DO NOT PRINT THIS PAGE

This Manual is to be
Printed in Color
on 8.5” x 11” stock.

Slice IO Products

RSTi-EP Slice IO
Network Adapter

Secure Deployment Guide
GFK-2972B
April 2018

Warnings, Cautions and Notes as Used in this Publication

Warning

Warning notices are used in this publication to emphasize that hazardous voltages, currents, temperatures, or other conditions that could cause personal injury exist in this equipment or may be associated with its use.

In situations where inattention could cause either personal injury or damage to equipment, a Warning notice is used.

Caution

Caution notices are used where equipment might be damaged if care is not taken.

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

This document is based on information available at the time of its publication. While efforts have been made to be accurate, the information contained herein does not purport to cover all details or variations in hardware or software, nor to provide for every possible contingency in connection with installation, operation, or maintenance. Features may be described herein which are not present in all hardware and software systems. GE assumes no obligation of notice to holders of this document with respect to changes subsequently made.

GE makes no representation or warranty, expressed, implied, or statutory with respect to, and assumes no responsibility for the accuracy, completeness, sufficiency, or usefulness of the information contained herein. No warranties of merchantability or fitness for purpose shall apply.

* indicates a trademark of General Electric Co. and/or its affiliates. All other trademarks are the property of their respective owners.

Contact Information

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

General Contact Information

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

Technical Support

If you have technical problems that cannot be resolved with the information in this guide, please contact us by telephone or email, or on the web at www.geautomation.com/support

Americas

Online Technical Support	www.geautomation.com/support
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	www.geautomation.com/support
Phone	+800-1-433-2682
EMEA Direct Dial	+420-23-901-5850 (if toll free 800 option is unavailable or if 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	www.geautomation.com/support
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

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

Secure deployment information is provided in this manual for the following RSTi-EP network adapter.

Family	Catalog Number	Description
RSTi-EP network adapter	EPXPNS001/101	*PROFINET Network Adapter, 2 Cu RJ45 Ports, 1024 bytes (Input + Output) / 101- Redundancy Capable [NAP S2 Type]*
	EPXMBE001	*Modbus TCP Network Adapter, 2 Cu RJ45 Ports, 2048 bytes (Input + Output)*
	EPXMBE101	*Modbus TCP Single/Dual Network Adapter, 2 Cu RJ45 Ports, 2048 bytes (Input + Output)*
	EPXETC001	*EtherCAT Network Adapter, 2 Cu RJ45 Ports, 1024 bytes (Input + Output)*

1.1 Related Documents

GFK-2958	RSTi-EP User Manual
GFK-2816	PACSystems RXi Distributed I/O Controller User Manual
GFK-2222	PACSystems CPU Reference User Manual
GFK-2571	PACSystems PROFINET Controller User Manual
GFK-2224	PACSystems RX7i and RX3i TCP/IP Ethernet Communications User Manual

1.2 Revisions to this Manual

Rev	Date	Description
B	Apr-2018	*EPXPNS101 Catalogue addition*
A	Nov 2017	*EPXMBE101 catalogue addition*
-	Dec 2015	*Initial draft*

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

Note: As GE 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-PlatformsSecurity-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 recommends taking a "Defense in Depth" approach to security.

2.3 Defense in Depth

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

For example, if a system is protected because it is on a network protected by a firewall, the attacker only needs to circumvent the firewall to gain unauthorized access. However, if there is an additional layer of defense, say a username/password authentication requirement, now the attacker needs to find a way to circumvent both the firewall and the username/password authentication.

2.4 General Recommendations

Adopting the following security best practices should be considered when using GE 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 GE product security updates, SIMs, and other recommendations.
- Apply all of the latest operating system security patches to control systems PCs.
- Use anti-virus software on control systems PCs and keep the associated anti-virus signatures up-to-date.
- Use whitelisting software on control systems PCs and keep the whitelist up-to-date.

2.5 Checklist

This section provides a sample checklist to help guide the process of securely deploying RSTi-EP network adapter.

1. Create or locate a network diagram.
2. Identify and record the required communication paths between nodes.
3. Identify and record the protocols required along each path, including the role of each node.
4. Revise the network as needed to ensure appropriate partitioning, adding firewalls or other network security devices as appropriate. Update the network diagram.
5. Configure firewalls and other network security devices
6. Enable and/or configure the appropriate security features on each RSTi-EP Network adapter.
7. On each RSTi-EP Network adapter, change/create every supported password to something other than its default value.
8. Harden the configuration of each RSTi-EP Network adapter, disabling unneeded features, protocols and ports.
9. Test / qualify the system.
10. Create an update/maintenance plan.

Note: Secure deployment is only one part of a robust security program. This document, including the checklist above, is limited to only providing secure deployment guidance. For more information about security programs in general, see section 6.6, *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 may be enhanced by limiting the protocols allowed and the paths across which they are allowed, to only what is needed. This can be accomplished by disabling every communication protocol that is not needed on a particular device (refer to chapter 5, Configuration Hardening), and by using appropriately configured and deployed network security devices (for example, firewalls and routers) to block every protocol (whether disabled or not) that doesn't need to pass from one network/segment to another.

GE 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 PROFINET I/O, Modbus TCP and EtherCAT 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 RSTi-EP network adapter. Note that some of the supported protocols may not be required in a given system, since the installation may only be using a subset of the available protocols.

Supported ETHERNET Protocols

	Protocol		RSTi-EP		
		EPXPNS001/101	EPXMBE001	EPXMBE101	EPXETC001
Link	ARP	✓	✓	✓	
	LLDP	✓			
Internet	IPv4	✓	✓	✓	
	ICMP	✓	✓	✓	
Trans	TCP	✓	✓	✓	
	UDP	✓	✓	✓	
Application Layer	DCE/RPC Client	✓			
	DCE/RPC Server	✓			
	PROFINET DCP Client				
	PROFINET DCP Server	✓			
	PROFINET I/O	✓			
	MRP	✓			
	SNMP v1 Server	✓			
	MODBUS/TCP		✓	✓	
	EtherCAT				✓
	http	✓	✓	✓	✓

3.1.2 Serial Protocols

In addition to Ethernet, RSTi-EP Network adapter products 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 RSTi-EP Network adapter modules. Note that some of the supported protocols may not be required in a given system, since the installation may only be using a subset of the available protocols.

Protocol	EPXPNS001/101	EPXMBE001	EPXMBE101	EPXETC001
Application-specific†	✓	✓	✓	✓
ASCII Terminal				
Modbus RTU Slave				
SNP Slave				

†The Network adapter uses serial port for accessing the web server application. The USB-LAN interface driver is installed and network adapter connects over ethernet when connected over USB.

3.2 Web Server

This section describes the communication paths needed to support common operations on a Web Server.

Using a Web Server

With default settings each type of network adapter offers web server access only via USB port. For that multiple IP addresses can be parametrized. Please note that this is a virtual DHCP server. To avoid network disruption no other network device with the same subnet ID should be connected to the PC.

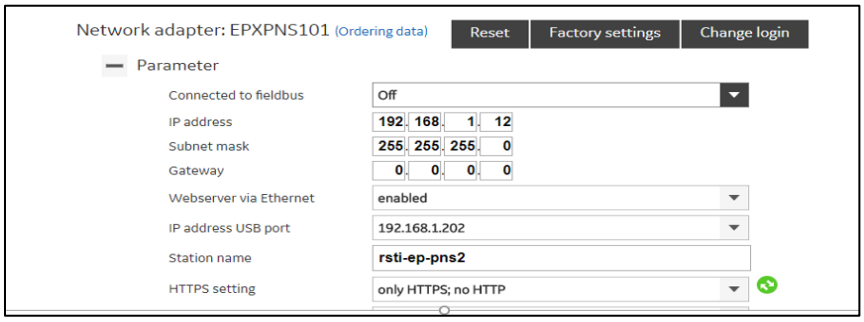
Using network adapter for Ethernet-based fieldbus systems – recognizable by the RJ45 socket – web server access can be realized alternatively via Ethernet. This function must be enabled in the web server in the couplers parameter setup.

Any changes of the IP settings on either USB port or Ethernet port will not be effective until restarting the coupler.

Webserver Capabilities

- Simulate the operation of the RSTi-EP remote node
- Query the status of network adapter and each of the module
- Display the parameters of network adapter and modules, and change them for testing purposes
- Access diagnostic information
- Operate the station in Force mode for testing purposes
- The EPXPNS101 Network Adaptor and higher revisions of other Network Adaptors like EPXPNS001, EPXPMBE101, EPXMBE001, EPXETC001, supports both HTTP and HTTPS interface. Please check the IPI documents for these devices for more information. This is a configurable option in the Webserver parameters.

Note: It is strongly recommended to use HTTPS protocol for connecting to the Network Adaptor Webserver by setting the “HTTPS setting” parameter as below.



Operating instructions

- Assign username and strong password when prompted during the first power-up of out-of-box module
- GE recommends that Webserver be used only with USB-Serial Cable and not use Webserver over ethernet even when the Network is considered to intrusion safe.
- Limitation and safe-guarding of control IO network is required to prevent data corruption by un-identified external access

3.3 PROFINET

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

Installing an IO device

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

Protocol	Proficy Machine Edition	IO device
PROFINET DCP	Client	Server

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

Network Discovery and Device Identification

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

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

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

Using an IO device

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

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

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

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	IO controller	IO device
MRP	Bi-directional	Bi-directional

3.4 EtherCAT

Installing an IO device

Commissioning, adding, or replacing an IO device requires configuring of IO device on the master and downloading the configuration to the master. The EtherCAT master controller configures slave device on the sequence as configured. The sequence of configuration and drop on the Ethernet network should match as the device are auto-addressed. Doing this requires supporting the following communication path.

Protocol	Master Controller	IO device
EtherCAT	Client	Server

Network Discovery and Device Identification

Auto discovery based on the configuration and the installation of the EtherCAT network devices.

Protocol	Local IO controller	Remote IO controllers and IO devices
EtherCAT	Client	Server

Using an IO device

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

Protocol	IO controller	IO devices
EtherCAT	Client	Server

3.5 Modbus/TCP

Installing an IO device

Commissioning, adding, or replacing an IO device requires assigning of IP address and other details via the webserver application over USB.

Protocol	IO device
TCP/IP (over USB interface)	Server

Network Discovery and Device Identification

Device identification is made by assigned IP address.

Protocol	Remote IO controllers and IO devices
TCP/IP (over Ethernet Interface)	Server

Using an IO device

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

Protocol	IO devices
Modbus TCP	Server

4 Secure Capabilities

This section describes the capabilities of the RSTi-EP network adapter and security features that can be used as part of a defense-in-depth strategy to secure your control system.

4.1 Capabilities by Product

This section provides a summary view of the security capabilities supported on each RSTi-EP network adapter module.

Security Capability	EPXPNS001/ 101	EPXMBE001	EPXMBE101	EPXETC001
Predefined set of Subjects and Access Rights				
Encoded Login	✓	✓	✓	✓
Secure Login (SRP-6a)				
Access Control List				
Firmware Signatures				

4.2 Access Control and Authorization

The Access Control process can be divided into two phases:

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

This section describes the Access Control capabilities supported by RSTi-EP network adapter, which includes its Authorization capabilities.

4.2.1 Authorization framework

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

RSTi-EP network adapter provide only one default user for authorization.

Subjects Available on GE RSTi-EP Network Adapter

	Functionality	Application Protocol	Subjects Available
Ethernet	Web Server	HTTP & HTTPS [Configurable Parameter]	
	Parameter Update	HTTP & HTTPS [Configurable Parameter]	***Authorization required for modification of parameters***
	Firmware Update	HTTP & HTTPS [Configurable Parameter]	***Authorization required***
Micro USB	Firmware Update	HTTP & HTTPS [Configurable Parameter]	***Authorization required***

	Functionality	Application Protocol	Subjects Available
	Parameter Update	HTTP & HTTPS [Configurable Parameter]	***Authorization required for modification of parameters***

Note: The EPXPNS101 Network Adaptor and higher revisions of other Network Adaptors like EPXPNS001, EPXPMBE101, EPXMBE001, EPXETC001, supports both HTTP and HTTPS interface. Please check the IPI documents for these devices for more information. This is a configurable option in the Webserver parameters.

4.3 Authentication

RSTI-EP network adapter provides password-based authentication for some operations via Web Server.

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 RSTi-EP network adapter for each protocol. It is important to note that some RSTi-EP network adapter only support a subset of the authentication options listed as follows.

Authentication available on RSTi-EP Network Adapter

	Functionality	Application Protocol	Subjects Available
Ethernet	Web Server	HTTP & HTTPS	
	Parameter Update	HTTP & HTTPS	***Authentication required for modification of parameters***
	Firmware Update	HTTP & HTTPS	***Authentication required***
Micro USB	Firmware Update	HTTP & HTTPS	***Authentication required***
	Parameter Update	HTTP & HTTPS	***Authentication required for modification of parameters***

Note: The EPXPNS101 Network Adaptor and higher revisions of other Network Adaptors like EPXPNS001, EPXPMBE101, EPXMBE001, EPXETC001, supports both HTTP and HTTPS interface. Please check the IPI documents for these devices for more information. This is a configurable option in the Webserver parameters.

4.4 Password Management

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

Access Mechanism/Utility	Authenticated Subjects	How Passwords are assigned
Web server	Firmware updates Parameter updates	During initial login or from the 'change login' menu

4.5 Confidentiality and Integrity

RSTi-EP network adapters provide encryption of password when being set and transferred from webserver application to the network adapter.

4.6 Logging

RSTi-EP network adapters log events and will provide in *.wmi format which is accessible from 'Save Service file' menu on the web server application. The internal events logged in service file and stored in binary format with the extension *.wmi which is not in plain-text.

5 Network Architecture and Secure Deployment

This section provides security recommendations for deploying RSTi-EP Network adapter in the context of a larger network.

5.1 Reference Architecture

The following figure displays a reference deployment of RSTi-EP Network adapter.

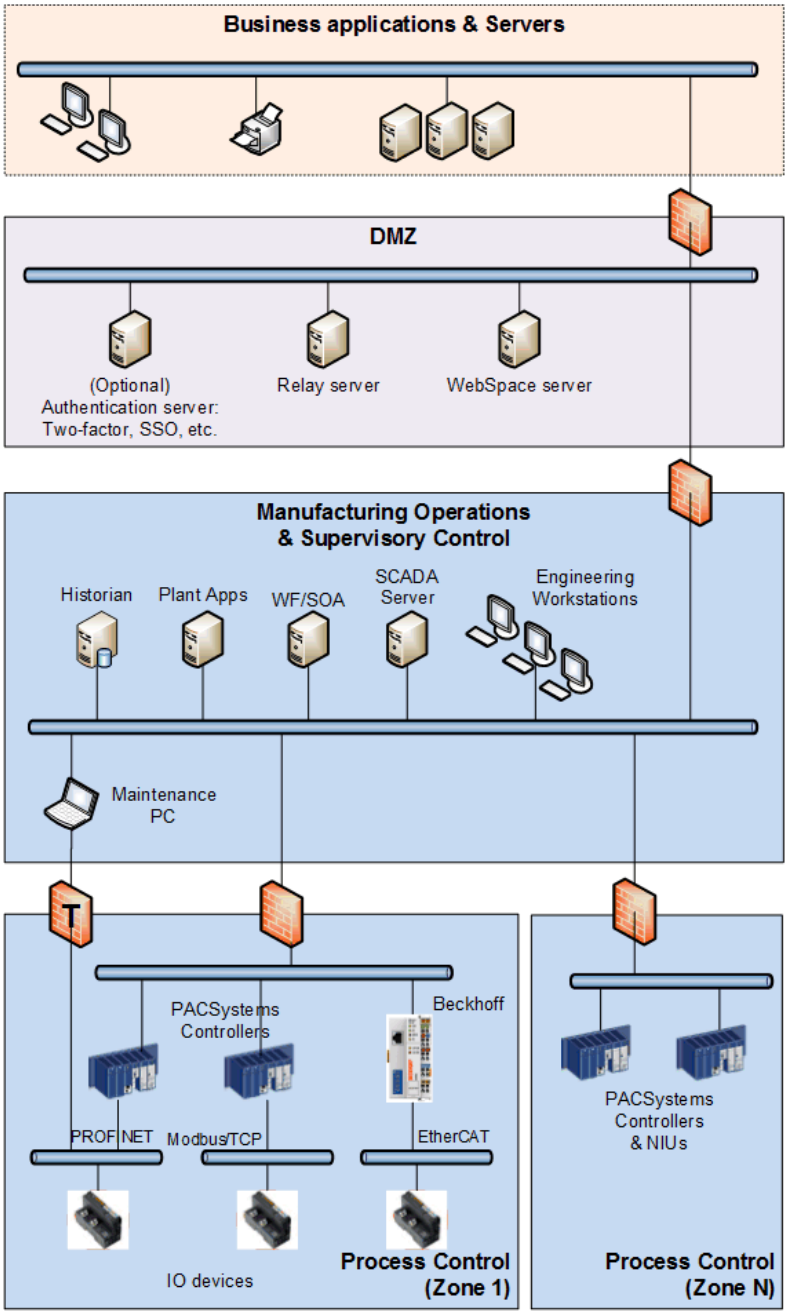


Figure 1: Network Architecture

The Manufacturing Zone networks (which include the Manufacturing Operations, Supervisory Control, and Process Control networks) are segregated from other untrusted networks such as the enterprise network (also referred to as the business network, corporate network, or intranet) and the internet using Demilitarized Zone (DMZ) architecture. The Process Control networks have limited exposure to traffic from higher-level networks, including other networks in the Manufacturing Zone, as well as from other Process Control networks.

5.2 Remote Access and Demilitarized Zones (DMZ)

DMZ architecture uses two firewalls to isolate servers that are accessible from untrusted networks. The DMZ should be deployed such that only specific (restricted) communication is allowed between the business network and the DMZ, and between the control network and the DMZ. The business network and the control networks should ideally not communicate directly with each other.

If direct communication to a control network is required from the business network or from the internet, carefully control, limit and monitor all access. For example, require two-factor authentication for a user to obtain access to the control network using Virtual Private Networking (VPN) and even then, restrict the allowed protocols/ports to just the minimum set required. Further, every access attempt (successful or not) and all blocked traffic should be recorded in a security log that is regularly audited.

5.3 Access to Process Control networks

Ethernet traffic from the Supervisory Control network to the Process Control networks should be restricted to support only the functionality that is required. If a particular protocol (such as Modbus TCP) does not need to be used between those regions, then the firewall should be configured to block that protocol. If, in addition to that, a controller does not have some other reason it needs to use that protocol, then – in addition to blocking it at the firewall – the controller itself should be configured to disable support for the protocol.

Note: Network Address Translation (NAT) firewalls typically do not expose all of the devices on the "trusted" side of the firewall to devices on the "untrusted" side of the firewall. Further, NAT firewalls rely on mapping the IP address/port on the "trusted" side of the firewall to a different IP address/port on the "untrusted" side of the firewall. Since communication to RSTi-EP network adapters will typically be initiated from a PC on the "untrusted" side of the Process Control network firewall, protecting a Process Control network using a NAT firewall may cause additional communication challenges. Before deploying NAT, carefully consider its impact on the required communications paths.

6 Other Considerations

6.1 Patch Management

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

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

6.2 Real-time Communication

When designing the network architecture, it is important to understand what impact the network protection devices (such as firewalls) will have on the real-time characteristics of the communications traffic that must pass through them. In particular, the PROFINET IO, EtherCAT, and Reliable Datagram Service protocols are generally expected to operate with small, known, worst-case bounds on their communications latency and jitter. As a result, network architectures that require real-time communications to pass through such devices may limit the applications that can be successfully deployed.

6.3 Web interface

The web server uses a simple token value to authenticate. Any attacker that can observe network traffic is able to capture the token value, and provide it in requests to impersonate a legitimate user. If not properly mitigated, this can lead to attack against the application resulting in denial of service on the destination host.

The attacks on web server can be mitigated by keeping the web server behind the firewall and disabling the access to web server over Ethernet. It is strongly advised to disable the web server access over Ethernet to minimize the attacks due to cross-site scripting, session hijacking and input validation.

6.4 Denial of Service due to Fuzzing – PROFINET/MODBUS-TCP/EtherCAT protocols

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

It is recommended to use the firewall to protect the device from unauthorized access.

6.5 Denial of Service due to Storm - PROFINET/Modbus-TCP protocols

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

Most mid-range to high-end firewalls today have the capability to detect storms which originate from devices in a less-trusted security zone/network, and should be used to mitigate the effects of Denial of service attacks due to storms.

6.6 Additional Guidance

6.6.1 Protocol-specific Guidance

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

6.6.2 Government Agencies and Standards Organizations

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

6.6.3 Industrial I/O Communication Protocol Specific Guidance

Industrial I/O communication protocols such as Profinet, Modbus and others, are vulnerable to the threat of cyber-attack. Consequently, the owner should take precautions to limit exposure to the effects of malicious and accidental Denial of Service and other threats.

The recommended defense in depth mitigations might include all or a combination of the following:

1. Industrial firewall that features Industrial Protocol inspection
2. Network access control measures that restrict access to the I/O network
3. Industrial intrusion detection devices capable of recognizing and reporting malicious attacks on I/O protocols
4. Ensuring physical access is restricted to authorized individuals only

GE Information Centers

Headquarters:
1-800-433-2682 or 1-434-978-5100

Global regional phone numbers
are available on our web site
www.ge-ip.com

Additional Resources

For more information, visit the GE web site:

www.ge-ip.com

GFK-2972A