Secure Deployment Guide

GFK-3188A

Jan 2021

PACSafe™ Secure Deployment Guide

EMERSON

Contents

Section 1: About this Guide 1
1.1 Related Documents 1
1.2 Revisions in this Manual 1
Section 2: Introduction 2
2.1 What is Security? 2
2.2 I have a firewall. Isn’t that enough? 2
2.3 What is Defense in Depth? 2
2.4 General recommendations 3
2.5 Checklist 3
Section 3: Communication Requirements 5
3.1 Protocols Supported 5
3.1.1 Ethernet Protocols 5
3.1.2 USB Protocols 6
3.2 USB Application Protocol 6
3.3 Ethernet Servers 7
3.4 Ethernet Firewall Configuration 7
3.4.1 Lower-level Protocols 7
3.4.2 Application Layer Protocols 8
3.4.3 Protocols Reserved for Future Use 8
Section 4: Security Capabilities 9
4.1 Capabilities by Product 9
4.2 Access Control and Authorization 9
4.2.1 Authorization Framework 10
4.2.2 Specifying Access Rights 10
4.2.3 Enforcement 11
4.3 Authentication 11
4.3.1 Summary 11
4.3.2 Recommendations 11
4.4 Password Management 12
4.5 Communications Protocols 12
4.6 Logging and Auditing 13
Section 5: Configuration Hardening 14
5.1 USB Port, LCD UI and Physical Access 14
5.2 Ethernet Interface 14
Section 6: Network Architecture and Secure Deployment 15
6.1 Reference Architecture 15
6.2 Remote Access and Demilitarized Zones (DMZ) 16
6.3 Access to Process Control networks 16
Section 7: Other Considerations 17
7.1 Configuration Management 17
7.2 Real-time Communication 17
7.3 Additional Guidance 17
7.3.1 Protocol-specific Guidance 17
7.3.2 Government Agencies and Standards Organizations 17
General Contact Information 18
Technical Support 18

Section 1: About this Guide

Safety control is a critical and required part of any safety system. This is because safety controllers ensure that your safety measures 1) do not fail, or 2) if failure is inevitable, fail in a predictable safe way. A safety controller is often an ideal safety control solution, because it provides more functionality than a safety relay, at a lower cost than a safety PLC.

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

Secure deployment information is provided in this manual for the following catalog numbers.

Catalog Number	Description
IC225SXE262	PACSafe Configurable Safety Controller with Expansion
IC225SXF262	PACSafe Configurable Safety Controller with Expansion & Display
IC225SSE262	PACSafe Standalone Configurable Safety Controller
IC225SSF262	PACSafe Standalone Configurable Safety Controller with Display
IC225SSE102	PACSafe Standalone Configurable Safety Controller with Relay Outputs
IC225SDL910	PACSafe Single Relay, Dual Channel Output Module
IC225SDL920	PACSafe Double Relay, Dual Channel Output Module
IC225SDD841	PACSafe 8-Channel Input Module
IC225SDD842	PACSafe 16-Channel Input Module
IC225SDL720	PACSafe 2-Pair Output Module
IC225SDL740	PACSafe 4-Pair Output Module

1.1 Related Documents

Description of Manual	GFK Number
PACSafe Configurable Safety Relay Quick Start Guide (QSG)	GFK-3183
PACSafe Configurable Safety Relay User Manual	GFK-3184
PACSafe Interface Module User Manual	GFK-3195

1.2 Revisions in this Manual

Rev	Date	Description
A	Jan 2021	Initial Release

Section 2: Introduction

This section introduces the fundamentals of security and secure deployment.

2.1 What is Security?

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

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

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

Note: *As Emerson product vulnerabilities are discovered and fixed, security advisories are issued to describe each vulnerability in a specific product version, as well as the version in which the vulnerability was fixed. Emerson product security advisories are available at the following location:*

https://www.emerson.com/Industrial-Automation-Controls/support

2.2 I have a firewall. Isn’t that enough?

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

Therefore, Emerson recommends taking a “Defense in Depth” approach to security.

2.3 What is Defense in Depth?

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

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

2.4 General recommendations

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

- The controllers and supervisory level computers covered in this document were not designed for or intended to be connected directly to any wide area network, including but not limited to a corporate network or the Internet at large. Additional routers and firewalls (such as those illustrated in Section 6.1: Reference Architecture) that have been configured with access rules customized to the site's specific needs must be used to access devices described in this document from outside the local control networks. If a control system requires external connectivity, care must be taken to control, limit, and monitor all access, using, for example, virtual private networks (VPN) or Demilitarized Zone (DMZ) architectures.
- Harden system configurations by enabling/using the available security features, and by disabling unnecessary ports, services, functionality, and network file shares.
- Apply all of the latest Emerson product security updates, SIMs, and other recommendations[1].
- 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 Configurable Safety Controllers.

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 3.4: Ethernet Firewall Configuration and Section 6: Network Architecture and Secure Deployment.)
6. Enable and/or configure the appropriate security features on each Configurable Safety Relay module. (Refer to Section 5: Configuration Hardening.)

[1] This recommendation does not apply to the PACSafe controllers. A certified safety controller cannot have its firmware modified without invalidating safety certifications.

7. On each Configurable Safety Controller module, change every supported password to something other than its default value and disable unneeded secondary users. (Refer to Section 4.4: Password Management.)
8. Harden the configuration of each Configurable Safety Controller module, disabling unneeded features, protocols and ports. (Refer to Section 5: Configuration Hardening.)
9. Test/qualify the system.
10. Create an update/maintenance plan.
11. Implement physical access controls to restrict access to authorized individuals.

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

Section 3: Communication Requirements

Communication between different parts of a control system is, and must be, supported. However, the security of a control system 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, and by using appropriately configured and deployed network security devices (for example, firewalls, routers) to block every protocol (whether disabled or not) that doesn't need to pass from one network/segment to another.

Emerson recommends limiting the protocols allowed by the network infrastructure to the minimum set required for the intended application. Successfully doing this requires knowing which protocol is needed for each system-level interaction.

This section describes how the supported serial and Ethernet application protocols are used by IC225S* controllers 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.

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 specific installation.

3.1 Protocols Supported

3.1.1 Ethernet Protocols

This section indicates which Ethernet protocols are supported, by IC225S* controllers. 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.

Table 1: Support Ethernet Protocols

Network Layer	Protocol	IC225S*
Link	ARP	✓
Network	IPv4	✓
	IGMP[2]	☒
	ICMP	✓
Transport	TCP	✓
	UDP	✓
Application	Modbus TCP	✓
	PROFINET	✓
	Ethernet/IP[3]	☒

[2] Not used. Reserved for future use.
[3] Not used. Reserved for future use.

3.1.2 USB Protocols

In addition to Ethernet communication, IC225S* controllers support communication over a direct USB connection.

Table 2: Supported USB Protocols

Interface	Protocol	IC225S*
USB	USB CDC with Application-Specific Driver	✓

3.2 USB Application Protocol

The IC225S* USB Application protocol is a proprietary protocol that provides access to services supported by the IC225S* controllers over USB. This is the only protocol used by the programming software when communicating with an IC225S* controller. It supports many different operations, including:

- Upload/download a confirmed configuration
- Confirm a new configuration
- Reset controller to factory defaults
- Enable and configure network interface
- Live application monitoring
- Configure controller user access and passwords
- View and optionally clear a log of any faults that have occurred in the controller
- Reset controller to factory defaults
- View Configuration log

USB Application Protocol is transported over a direct USB 2.0 CDC connection using a standard USB 2.0 - compliant cable.

3.3 Ethernet Servers

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

Table 3: IC225S* Server Capabilities

Interface	Functionality	Required Application Protocols	Example Clients
Ethernet	PROFINET	PROFINET	Other controllers
	Modbus/TCP Server	Modbus/TCP	Other controllers

3.4 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 IC225S* controllers.

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.

Table 4: Link Layer Protocols

Protocol	EtherType
ARP	0x0806
PROFINET	0x8892

Table 5: Internet Layer Protocols

Protocol	EtherType	IP Protocol #
IPv4	0x0800	(n/a)
ICMP	0x0800	1
IGMP[4]	0x0800	2

[4] Not used. Reserved for future use.

Table 6: 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 IC225S* Controllers.

3.4.2 Application Layer Protocols

The following is the list of TCP and UDP port numbers for the Application layer protocols supported by IC225S* Controllers.

Table 7: Application Layer Protocols

Protocol	TCP Port	UDP Port	IC225S*
Modbus TCP	502	-	✓
PROFINET	-	34964 49152	✓
Ethernet/IP[5]	44818	2222 44818	☒

3.4.3 Protocols Reserved for Future Use

The preceding sections document several protocols as not used by IC225S* Controllers. While present to a limited degree, they are not configurable. **These ports are reserved for future use and should be blocked by the firewall**.

[5] Not used. Reserved for future use.

Section 4: Security Capabilities

This section describes IC225S* controller 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 supported security capabilities.

Table 8: Security Capabilities

Security Capability	IC225S*
Predefined set of Subjects and Access Rights	✓
Access Control List	✓

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 IC225S* controllers, 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.

IC225S* controllers, however, do not provide such a facility – there is no support for creating additional User IDs. A User ID does not even have to be specified to authenticate. In this case, authorization is based on the functionality being used and the password that is provided for authentication. However, the authentication features supported on IC225S* Controllers implicitly define a fixed set of subjects, which are identified here.

The subjects defined and supported by IC225S* server protocol are indicated in the following table.

Table 9: Subjects Available on IC225S* Controllers

Interface	Functionality	Application Protocol	Subjects Available
USB	Configuration and Live Monitoring Requests	USB Application	Anonymous User 1 User 2 User 3

Table 10: Subjects Available on IC225S* Ethernet Network Interface

Interface	Functionality	Application Protocol	Subjects Available
Ethernet	PROFINET Server	PROFINET	Anonymous
	Modbus TCP Server	Modbus TCP	Anonymous

4.2.2 Specifying Access Rights

For each subject, IC225S* controllers provide 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.

Table 11: Access Rights on IC225S* Controllers

Capability	User 1	User 2	User 3
Application Configuration	RW	RW	RW
Live Monitoring	R	R	R
Network Configuration	RW	RW	RW
Configuration Log	R	R	R
Fault Log	RD	RD	RD
User Passwords	RWD	-	-
Reset to Factory Defaults	A	-	-

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

The User 1 has the ability to prohibit any subject from reading or writing the Application configuration and/or Network Configuration. Only User 1 can reset controller to Factory Defaults.

4.2.3 Enforcement

The IC225S* controller enforces the access rights for the data and services that it provides. Thus, the IC225S* controller ensures that the Application and Network Configuration can only be updated by a user with the access rights to write the Application Configuration.

4.3 Authentication

The IC225S* controller provides simple, 4-digit password-based authentication which must be used in in combination with physical presence to modify its configuration, clear its logs and change the user passwords. The password is either entered on the LCD UI, if available, or provided to programming software when programming the controller using a USB cable. Compensating controls may be needed to satisfy a specific installation's security requirements.

4.3.1 Summary

This section summarizes the authentication mechanisms supported by IC225S* controllers for each interface.

Table 12: Authentication Available on IC225S* Controllers

Interface	Functionality	Authentication Options
LCD	Import Configuration from XM	Password
	Write Configuration to XM	Password
	Clear Fault Log	None
Programming Software (USB)	Read Configuration	None
	Write Configuration	Password
	Read Fault or Configuration Logs	None
	Live Monitoring	None
Ethernet	PROFINET Server	None
	MODBUS TCP Server	None

4.3.2 Recommendations

Augment simple user and password authentication scheme by limiting access to untrusted users.

The IC225S* controller requires physical access to the controller's micro USB connector to change the application configuration and application logic. Physical access is either through a direct connection using the USB port to a PC running the programming software or by inserting an XM card.

To secure the controller, physical access to it must be restricted by placing the controller in a secure physical environment such as a locked cabinet.

4.4 Password Management

As described in the Section 4.2.1: Authorization Framework, IC225S* controller has a set of predefined subjects. The passwords for each subject must be explicitly managed. The programming software enforces unique passwords for each subject.

IC225S* controller fixes password length at 4 numeric characters. Emerson strongly recommends the use of non-default, non-predictable passwords.

Table 13: Authentication Supported by IC225S* Controller

Functionality	Authenticated Subjects	How Passwords are assigned
Configuration Requests	User 1 User 2 User 3	All these passwords are controlled by User 1.

For more detailed information on assigning these passwords, refer to the PACSafe Configurable Safety Relay User Manual (GFK-3184).

4.5 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 IC225S* Controllers provide either of these features, as detailed in the following tables. Therefore, compensating controls may be required to meet an installation’s security requirements for protecting data in-flight.

Table 14: Protocol-Provided Security Capabilities on IC225S* Controller

Interface	Protocol	Data Encryption	Message Authentication Codes
USB	System Configuration Protocol	N	N

Table 15: Protocol-Provided Security Capabilities on IC225S* Ethernet Network Interface Unit

Interface	Protocol	Data Encryption	Message Authentication Codes
Ethernet	PROFINET	N	N
	Modbus TCP	N	N

4.6 Logging and Auditing

The IC225S* controllers do not provide a dedicated security log embedded within the controller. However, the IC225S* Controller does log configuration update events in a small (10 entry) configuration log table. Each entry includes the time and date that the configuration was confirmed, using the date and time of the configuration change as maintained on the PC. Also included is the configuration name and the confirmation CRC.

This configuration log can be viewed using the programming software. The log is read-only and cannot be reset or exported from the controller. Resetting the controller to factory defaults also generates an entry in the log table.

IC225S* controller also has a fault log. Most of the events that are logged in the IC225S* Controller fault log 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. Fault logs do not get retained after the power is removed. Fault log can be viewed either through the programming software or on the LCD UI.

Section 5: Configuration Hardening

This section is intended to assist in reducing the potential attack surface by providing information that can be used to harden the configuration of the IC225S* 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.

Emerson recommends disabling, on each IC225S* product, all ports, users, services, and protocols that are not required for the intended application.

5.1 USB Port, LCD UI and Physical Access

To reduce the potential attack surface, limit the physical access to the USB Port and LCD UI by limiting the physical access to the controller. This can be done by placing the controller in a physically secure environment, such as a locked cabinet.

5.2 Ethernet Interface

This section provides information to use when hardening the configuration of the IC225S* controller's Ethernet Interface. These settings should be considered when configuring any IC225S* Ethernet Interface.

If your deployment does not need to access devices that are not on the Process Control Network, routing should be disabled by setting Gateway IP Address set to all zeros:

Table 16: Disabling IP Routing

Service	Parameter name	Value
IP Routing	Gateway IP Address	0.0.0.0

These settings are specified within the hardware configuration that is downloaded to the IC225S* controller.

Ethernet interface can also be completely disabled using the programming software.

For more information on these parameters, refer to the IC225S* Controller User Manual (GFK-3184).

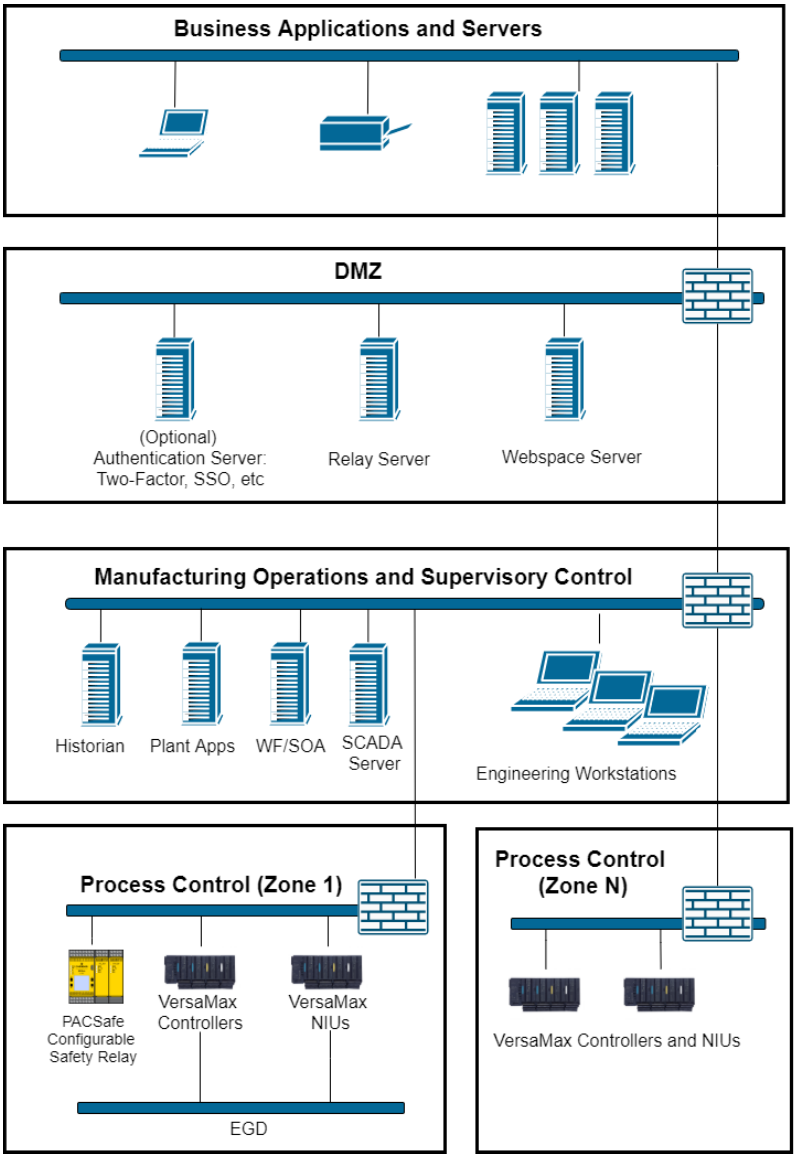
Section 6: Network Architecture and Secure Deployment

This section provides security recommendations for deploying an IC225S* controller in the context of a larger network.

6.1 Reference Architecture

The following figure illustrates a reference deployment of IC225S* controllers.

Figure 1: Sample 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 other networks, including other networks in the Manufacturing Zone and from other Process Control networks.

6.2 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.

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. If a particular protocol is not used between those regions, then the firewall should be configured to block that protocol. If a specific controller does not use that protocol, then it should be blocked at the firewall, and 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 the Configurable Safety Relay controller will typically be initiated from a PC on the “untrusted” side of the Process Control network firewall, protecting a Process Control network using a NAT firewall may cause additional communication challenges. Before deploying NAT, carefully consider its impact on the required communications paths.*

Section 7: Other Considerations

7.1 Configuration Management

A strategy for applying security fixes, including configuration changes, should be included in a facility's security plan. Applying these updates will often require that an affected IC225S* controller be temporarily taken out of service.

Some installations require extensive qualification and/or commissioning 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.

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.

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 cyber-security with Control Systems. Such documentation, when appropriate, should be considered in addition to this document. Similarly, the International Society of Automation publishes the ISA-99 specifications to provide guidance on establishing and operating a cyber-security program, including recommended technologies for industrial automation and control systems.

General Contact Information

Home link:	http://www.emerson.com/industrial-automation-controls
Knowledge Base:	https://www.emerson.com/industrial-automation-controls/support

Technical Support

Americas
Phone: 1-888-565-4155
1-434-214-8532 (If toll free option is unavailable)

Customer Care (Quotes/Orders/Returns): customercare.mas@emerson.com
Technical Support: support.mas@emerson.com

Europe
Phone: +800-4444-8001
+420-225-379-328 (If toll free option is unavailable)

Customer Care (Quotes/Orders/Returns): customercare.emea.mas@emerson.com
Technical Support: support.mas.emea@emerson.com

Asia
Phone: +86-400-842-8599
+65-6955-9413 (All other Countries)

Customer Care (Quotes/Orders/Returns): customercare.cn.mas@emerson.com
Technical Support: support.mas.apac@emerson.com

Any escalation request should be sent to: mas.sfdcescalation@emerson.com

Note: If the product is purchased through an Authorized Channel Partner, please contact the seller directly for any support.

Emerson reserves the right to modify or improve the designs or specifications of the products mentioned in this manual at any time without notice. Emerson does not assume responsibility for the selection, use or maintenance of any product. Responsibility for proper selection, use and maintenance of any Emerson product remains solely with the purchaser.