RSTi-OM Network-Based Devices

SECURE DEPLOYMENT GUIDE

EMERSON

Contents

Section 1 About this Guide

This document provides information that can be used to help improve the cybersecurity of systems that include RSTI-OM IO-Link Master (IOLM) from Emerson. It is intended for use by control engineers, integrators, IT professionals, and developers responsible for deploying and configuring RSTI-OM products.

Table 1: Catalog Numbers

Catalog Number	Description
OMIOLM001	IO-Link Master

1.1 Related Documents

Table 2: RSTi-OM Documentation

Description of Manual	GFK Number
RSTI-OM User Manual	GFK-3212
RSTi-OM Quick Start Guide	GFK-3213

1.2 Revisions in this Manual

Table 3: Revisions

Rev	Date	Description
A	Jun 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 the 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 the 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 protect 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 RSTi-OM IO-Link Master (IOLM) covered in this document was 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 RSTi-OM IOLM.

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 3.3, Ethernet Firewall Configuration and Section 6 Network Architecture and Secure Deployment.)
6. Enable and/or configure the appropriate security features on each configurable IOLM. (Refer to Section 5 Configuration Hardening.)
7. On each configurable IOLM, change every supported password to something other than its default value and disable unneeded secondary users. (Refer to Section 4.4, Password Management.)

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

8. Harden the configuration of each configurable IOLM, 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 is not needed on a particular device (refer to Section 4.4, Password Management), and by using appropriately configured and deployed network security devices (for example, firewalls and routers) to block every protocol (whether Protocols Supported

3.1.1 Ethernet Protocols

This section indicates which Ethernet protocols are supported by the IOLM. 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 4: Support Ethernet Protocols

	Protocol	RSTi-OM
		OMIOLM001
Link	ARP	Yes
	LLDP	Yes
Internet	IPv4	Yes
	ICMP	Yes
Transport	TCP	Yes
	UDP	Yes
Application Layer	DCE/RPC Client	No
	DCE/RPC Server	No
	PROFINET DCP client	Yes
	PROFINET DCP server	No
	PROFINET I/O	Yes
	HTTP Server	Yes
	HTTPS Server	Yes
	MRP	Yes
	SNMP v1 server	Yes
	SNMP v2c server	No
	NTP	Yes
	FTP	No
	OPC-UA	Yes
	MQTT	Yes
	Modbus TCP	Yes

3.1.2 Serial Protocols

In addition to Ethernet, RSTI-OM IOLM may also support communication over serial ports. 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-OM IOLM. 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 5: Serial Protocols

Protocol	OMIOLM001
IO-Link	Yes

3.2 PROFINET

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

3.2.1 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.

Table 6: IO Device Communication Paths

Protocol	PAC Machine Edition	I/O Device
PROFINET DCP	Client	Server

Supporting this path will allow PAC Machine Edition to directly discover all the IOLM devices that are connected to the same subnet as the computer. (Note that this protocol is not routable.) PAC 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.

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

3.2.2 Network Discovery and Device Identification

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

Table 7: Device IO 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.*

3.2.3 Using an I/O Device

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

Table 8: PROFINET IO Device Communication Paths

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.

Table 9: Required for Media Redundancy

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

3.3 Ethernet Firewall Configuration

Network-based and host-based firewalls should be configured to only allow expected and required network traffic. This section identifies the Ether Types and the TCP/UDP ports used by the protocols supported on RSTi-OM IOLM.

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

Note: *Refer to Figure 1 for a diagram showing firewall placement.*

3.3.1 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

Table 10: Link Layer Protocols

Protocol	ETHERNET Type
ARP	Eth Type 0x806
LLDP	Eth Type 0x88CC
MRP	Eth Type 0x88E3
PROFINET DCP Client	Eth Type 0x8892

Internet Layer Protocols

Table 11: Internet Layer Protocols

Protocol	ETHERNET Type	IP Protocol #
IPv4	Eth Type 0x0800	-
ICMP	-	IP Protocol #: 1
IGMP	-	IP Protocol #: 2

Transport Layer Protocols

Table 12: Transport Layer Protocols

Protocol	ETHERNET Type	IP Protocol #
TCP	-	IP Protocol #: 6
UDP	-	IP Protocol #: 17

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

3.3.2 Application Layer Protocols

The RSTi-OM IOLM can act 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 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.

Table 13 Application Layer Protocols

Protocol	Port Number
DCE/RPC Server	UDP Ports 34964 & 49152
HTTP / HTTPS	Port 80 / Port 443
PROFINET I/O	Dynamic UDP Ports > 49152
SNMP v1 Server	UDP port 161
Modbus TCP	TCP port 502
Discovery protocol	UDP port 4606
PN DCP Client	Ethernet Frame type - 34962
MRP	Ethernet Frame type - 35043
NTP	Port 123
FTP	N/A
OPC-UA	Port 4840
MQTT	Defined by server. MQTT server port (0-65535). Default 1883 or 8883 if TLS is enabled.

Section 4 Security Capabilities

This section describes the IO-Link Master 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 14: Security Capabilities

Security Capability	OMIOLM001
The predefined set of user accounts	Yes
Access Control List	Yes
Login Type	Plain text when using HTTP, Secured when using HTTPS
Firmware – Unsigned	Unsigned
Boot – Unsecured	Unsecured
Internal Firewall - No	No

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 IOLM, 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.

Table 15: Subjects Available on IOLM module

Interface	Functionality	Application Protocol	Subjects Available
IO link ports	Interface to IO-Link devices	IO-Link	All

Table 16: Subjects Available on IOLM Ethernet Network Interface

Interface	Functionality	Application Protocol	Subjects Available
Ethernet	PROFINET Server	PROFINET	Anonymous
	Modbus TCP Server	Modbus TCP	Anonymous
	OPC-UA Server	OPC-UA	Anonymous
	MQTT Client	MQTT	Anonymous
	Time Server	NTP	Anonymous

4.2.2 Specifying Access Rights

For each subject, IOLM provides predefined access rights. In some cases, those access rights can be partially restricted, while in other cases they either cannot be changed at all or can only be revoked by disabling the associated server/protocol. For in-depth details to configure user accounts, please consult *GFK-3212, RSTi-OM User Manual.*

Table 17: Access Rights on IOLM Controllers

Page	Admin	Operator	User
Log-in	Yes	Yes	Yes
Home	Yes	Yes	Yes
Diagnostics - All	Yes	Yes	Yes
Configuration - IO-Link Settings	Yes	Yes	View-only
Configuration - Modbus/TCP	Yes	Yes	View-only
Configuration - PROFINET IO	Yes	Yes	View-only
Configuration - OPC UA	Yes	Yes	View-only
Configuration - Network	Yes	View-only	No
Configuration - Misc	Yes	Yes	Yes
Configuration - Load/Save	Yes	Yes	View-only
Configuration - Clear Settings	Yes	No	No
Advanced - Software	Yes	No	No
Advanced - Accounts	Yes	No	No
Advanced - Log Files	Yes	Yes	Yes
Advanced - Licenses	Yes	Yes	Yes
Attached Devices - IO-Link Device Description Files	Yes	Yes	View-only
Attached Devices - IO-Link Device Configuration Summary	Yes	Yes	View-only
Attached Devices - IO-Link Device - Port	Yes	Yes	View-only

Only Admin can reset the controller to Factory Defaults.

4.2.3 Enforcement

Each of the RSTi-OM IOLM enforces the access rights for the data and services that it provides.

4.3 Authentication

The RSTi-OM IOLM from Emerson 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 an installation's security requirements. For more details, see Section *4.2.2, Specifying Access Rights.*

4.3.1 Server Protocols

This section summarizes the authentication mechanisms supported by RSTI-OM IOLM for each protocol. It is important to note that some RSTI-OM IOLM may only support a subset of the options listed here. Refer to Section 4.2.2 Specifying Access Rights, for more details.

Table 18: Server Protocols

Transport Medium	Functionality	Application Protocol	Subjects Available
Serial	IO-Link communication	IO-Link	None
Ethernet	Web Server	HTTP	None
	Web Server Firmware Update	HTTP	Admin

4.3.2 Authentication Supported by the PROFINET Protocol

The IOLM I/O specification does not define an authentication mechanism, so no authentication mechanism is officially supported on RSTI-OM T IOLM using 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 an installation's security requirements.

4.3.4 Recommendations

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

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.

Personnel Security Protection

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

Physical Security Perimeter Protection

All ICS hardware should be placed in locked cabinets, with policies and procedures to restrict access to the key.

1. 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.
2. 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.
3. Networks should always be physically segmented as suggested in the Reference Network Architecture diagram (Section 6.1) to avoid exposure to ICS networks.
4. Each ICS system asset should be visibly labeled by a unique identifier, with all expected asset identification compiled into an access-controlled list.

Electronic Security Perimeter Protection

5. All external access to an ICS network should be managed through a Virtual Private Network (VPN) or similar technology leveraging two-factor authentication.
6. 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.
7. 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.
8. 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.

9. 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.
10. 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 operational function.
11. 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.
12. Carefully protect sources of and access to credentials (user names, passwords) for all ICS equipment, including switches, routers, firewalls, IDS, IPS, etc.
13. 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 overtime should be compensated for with policies and procedures that require a history of unique passwords.

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

4.4 Password Management

As described in Section 4.2.1, Authorization Framework, each instance of a server has its 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.

4.4.1 Changing Passwords

IOLM module provides default user accounts – Admin, Operator & User with limitations according to the role. Users must ensure to set a different and strong password for all user accounts. The password should include a combination of small-case, upper-case, numeric, and symbol.

4.5 Confidentiality and Integrity

4.5.1 Communication Protocols

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

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

Encryption is not provided for any of the protocols. Therefore, compensating controls may be required to meet an installation's security requirements for protecting data in-flight.

Protocol-Provided Security Capabilities

Table 19: 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
	OPC-UA	Y	Y
	Modbus TCP	N	N
	SNMP	N	N
	NTP	N	N
	MQTT	N	N
Serial	IO-Link	N	N

4.5.2 Firmware Signatures

The RSTi-OM IOLM does not support firmware signatures.

4.5.3 Logging and Auditing

IOLM devices supplied by Emerson 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.

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 IOLM 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 IOLM product, all ports, users, services, and protocols that are not required for the intended application.

5.1 Physical Access

This can be done by placing the IOLM 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 IOLM's Ethernet Interface. These settings should be considered when configuring any IOLM 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 the Gateway IP Address set to all zeros:

Table 20: Disabling IP Routing

Service	Parameter name	Value
IP Routing	Gateway IP Address	0.0.0.0

For more information on these parameters, refer to the IOLM User Manual (GFK-3212).

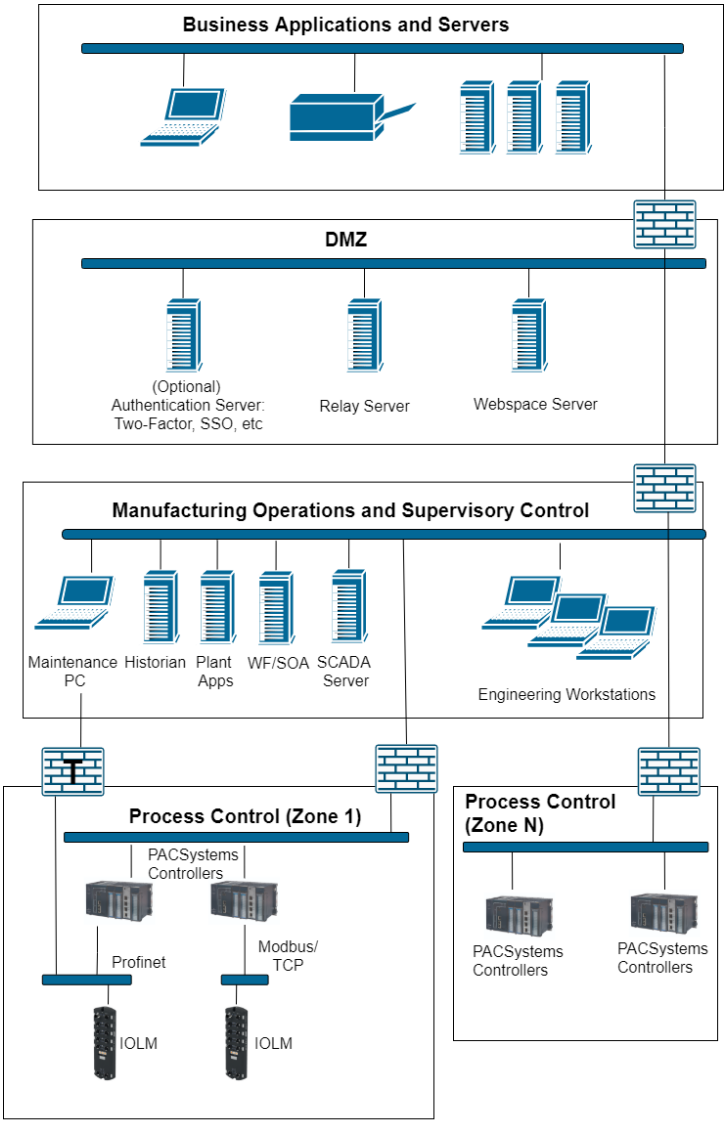
Section 6 Network Architecture and Secure Deployment

This section provides security recommendations for deploying an RSTi-OM controller in the context of a larger network.

6.1 Reference Architecture

The following figure illustrates a reference deployment of IO-Link Master.

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 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 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 IOLM be temporarily taken out of service.

Some installations require extensive qualification and/or commissioning to 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 guide 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 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 guide 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)

+39-0362-228-5555 (from Italy - if toll-free 800 option is unavailable or dialing from a mobile telephone)

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

Asia

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

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

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

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

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

EMERSON