PACSystems^{TM} Field Agent

SECURE DEPLOYMENT GUIDE

EMERSON.

Contents

Chapter 1: About this Guide 1

1.1 Applicable Products 1
1.2 Related Documentation 2
1.2.1 Product Landing Pages 2
1.2.2 Other Documentation 2
1.3 Revisions in this Manual 3

Chapter 2: Introduction 4

2.1 What is Security? 4
2.2 I have a Firewall. Isn't that Enough? 4
2.3 What is Defense in Depth? 4
2.4 General Recommendations 4
2.5 Sample Checklist 5

Chapter 3: Communication Requirements 6

3.1 Serial Communication 6
3.1.1 Application Layer Protocols 6
3.2 Ethernet Communication 7
3.2.1 Lower-level Protocols 7
3.2.2 Application Layer Protocols 8
3.3 Cellular Communication 9
3.3.1 4G LTE Cellular General Information 9
3.3.2 4G LTE Cellular on AT&T Private Network 9
3.3.3 4G LTE Cellular using Customer-Provided SIM 10
3.3.4 Recommendations 10
3.4 Wireless Local Area Network Communication 10
3.4.1 802.11 Wi-Fi Hotspot 10
3.4.2 Recommendations 11

Chapter 4: Security Capabilities 12

4.1 Access Control and Authorization 12
4.1.1 Authorization Framework 12
4.1.2 Enforcement 12
4.2 Authentication 13
4.2.1 Authentication Recommendations 13

4.3 Password Management 15
4.4 Firewall 15
4.4.1 MFA Firewall 17
4.4.2 EFA Firewall 18
4.4.3 VFA Firewall 18
4.4.4 Opening Additional Ports in the Firewall 19
4.5 Confidentiality and Integrity 19

Chapter 5: Configuration Hardening 21

5.1 General Field Agent Configuration Hardening 21
5.1.1 Configure Automatic Field Agent Updates 21
5.1.2 Update Predix Machine to the Latest Supported Version 21
5.1.3 Harden Access to each Industrial Data Source 22
5.2 MFA Configuration Hardening 23
5.2.1 MFA Network Configuration 23
5.2.2 Disable Predix Machine Web Console after Provisioning 23
5.2.3 Remove Unused Cellular Antennae 23
5.2.4 Remove Unused Wi-Fi Antennae 23
5.3 EFA Configuration Hardening 23
5.3.1 Disabling Configuration Mode 23
5.4 VFA Configuration Hardening 24
5.4.1 VFA Network Configuration 24
5.4.2 Disable Predix Machine Web Console after Provisioning 24
5.4.3 Change Predix User Account Password after Provisioning 24

Chapter 6: Reference Network Architecture 25

6.1 Remote Access and Demilitarized Zones (DMZ) 25
6.2 Field Agent to Cloud Communications 26
6.3 Field Agent to Industrial Data Source Communications 26

Chapter 7: Other Considerations 27

7.1 Patch Management 27
7.2 Protocol-Specific Guidance 27
7.3 Government Agencies & Standards Organizations 27

Warnings, Caution 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 to 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.

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

These instructions do not purport to cover all details or variations in equipment, nor to provide for every possible contingency to be met during installation, operation, and maintenance. The information is supplied for informational purposes only, and Emerson makes no warranty as to the accuracy of the information included herein. Changes, modifications, and/or improvements to equipment and specifications are made periodically and these changes may or may not be reflected herein. It is understood that Emerson may make changes, modifications, or improvements to the equipment referenced herein or to the document itself at any time. This document is intended for trained personnel familiar with the Emerson products referenced herein.

Emerson may have patents or pending patent applications covering subject matter in this document. The furnishing of this document does not provide any license whatsoever to any of these patents.

Emerson provides the following document and the information included therein as-is and without warranty of any kind, expressed or implied, including but not limited to any implied statutory warranty of merchantability or fitness for particular purpose.

Chapter 1: About this Guide

1.1 Applicable Products

This document provides information that can be used to help improve the cyber security of systems that include Field Agent products supplied by Emerson. It is intended for use by control engineers, integrators, IT professionals, and developers responsible for deploying and configuring Field Agent products.

Table 1: Applicable Products

Product Family	Catalog #	Description	Provisioning Connection	Data Source Connection	Cloud Connection
Mini Field Agent (MFA)	ICMFA000000	Field Agent as a standalone appliance for connecting to external data sources.	• Ethernet LAN	• Ethernet LAN	• Ethernet WAN
	ICMFA002US0 ICMFA002EU0	Field Agent as a standalone appliance for connecting to external data sources. Includes optional Wi-Fi hotspot for provisioning.	• Ethernet LAN • Wi-Fi hotspot with country codes and frequencies set per catalog number	• Ethernet LAN	• Ethernet WAN
	ICMFA001US1 ICMFA001UM1 ICMFA001EU1 ICMFA001AU1 ICMFA001AE1	Field Agent as a standalone appliance for connecting to external data sources. Includes optional Wi-Fi hotspot for provisioning and optional private cellular cloud connection on AT&T®.	• Ethernet LAN • Wi-Fi hotspot with country codes and frequencies set per catalog number	• Ethernet LAN	• Ethernet WAN • AT&T private cellular network per catalog number
	ICMFA001US0 ICMFA001UM0 ICMFA001EU0 ICMFA001AU0 ICMFA001AE0	Field Agent as a standalone appliance for connecting to external data sources. Includes optional Wi-Fi hotspot for provisioning and optional cellular cloud connection on customer-provided network.	• Ethernet LAN • Wi-Fi hotspot with country codes and frequencies set per catalog number	• Ethernet LAN	• Ethernet WAN • Cellular network per catalog number using customer-provided SIM
Embedded Field Agent (EFA)	IC695CPE400	Field Agent embedded in an Industrial Internet Control System running PACSystems*.	• Ethernet WAN in Configuration Mode only	• Virtual LAN through hypervisor • Ethernet WAN	• Ethernet WAN

Product Family	Catalog #	Description	Provisioning Connection	Data Source Connection	Cloud Connection
Virtual Field Agent (VFA)	ICVFA000000	Field Agent as a virtual machine image.	• Virtual LAN1 through hypervisor • Virtual LAN2 through hypervisor	• Virtual LAN1 through hypervisor • Virtual LAN2 through hypervisor	• Virtual WAN through hypervisor

1.2 Related Documentation

1.2.1 Product Landing Pages

Table 2: Product Landing Pages

Product	URL
Mini Field Agent	https://www.emerson.com/Industrial-Automation-Controls/support
CPE400 with Embedded Field Agent	https://www.emerson.com/Industrial-Automation-Controls/support
Virtual Field Agent	https://www.emerson.com/Industrial-Automation-Controls/support

1.2.2 Other Documentation

Table 3: Other Documentation

Document ID	Document Title
GFK-2993	Field Agents User Guide
GFK-3017	Mini Field Agent Upgrade Guide
GFK-3018	Field Agents Registration Guide
GFK-3019	Field Agent Machine Adapters User Guide
GFK-2830	PACSystems RXi, RX3i, RX7i and RSTi-EP Controller Secure Deployment Guide
GFK-2222	PACSystems RX7i, RX3i and RSTi-EP CPU Reference Manual
GFK-2314	PACSystems RX3i System Manual
GFK-2224	PACSystems RX7i, RX3i and RSTi-EP TCP/IP Ethernet Communications User Manual
GFK-2225	PACSystems TCP/IP Ethernet Communications Station Manager User Manual
GFK-2571	PACSystems RX3i & RSTi-EP PROFINET I/O Controller Manual
GFK-2572	PACSystems RX3i PROFINET Controller Command Line Interface Manual
GFK-2904	PROFINET IO Devices Secure Deployment Guide

1.3 Revisions in this Manual

Table 4: Revisions in this Manual

Rev	Date	Description
L	Sep 2019	Following Emerson's acquisition of this product, changes have been made to apply appropriate branding and registration of the product with required certification agencies. No changes to material, process, form, fit or functionality.
K	Sep 2018	Added information regarding the High-Performance Field Agent
J	Jul 2018	Updated the "Supported Ethernet Protocols" Added warning about Specter/Meltdown vulnerabilities
H	Apr 2018	Added new MFA model numbers. Added CAN bus to the MFA Added VPN protocol to the MFA
G	Feb 2018	Added Support for Ethernet/IP (CIP and PCCC protocols) and OSI PI Web Services.
F	Sep 2017	Added Contact Information section. Added MFA support for Modbus RTU over RS-232.
E	Jul 2017	Added information regarding the Ethernet Global Data protocol.
D	Jun 2017	Added information regarding Mini Field Agent Wi-Fi hotspot for provisioning and cellular cloud connection capability. Applied style guide.
C	May 2017	Added information regarding the Virtual Field Agent.
B	Apr 2017	Added information regarding the Embedded Field Agent.
A	Mar 2017	Created a new GFK from Chapter 3 of GFK-2993A, Field Agents User Guide.
-	Jan 2017	Initial Publication

In addition to these manuals, datasheets and product update documents describe individual devices and product revisions. The most recent documentation is available on the Emerson support website https://www.emerson.com/Industrial-Automation-Controls/support.

Chapter 2: Introduction

2.1 What is Security?

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

- Confidentiality: Ensure that only those people whom you want to see certain 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. As Emerson product vulnerabilities are discovered and fixed, security advisories are issued to describe each vulnerability in each product version as well as the version in which the vulnerability was fixed. Emerson Product Security Advisories can be found 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 such as 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 Emerson products and solutions.

- Care must be taken when connecting hardware to a wide area network including but not limited to a corporate network or the Internet at large. The network segmentation and firewall rules at each network interface must be carefully considered to reduce the allowed traffic to the bare minimum needed for operation. 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. Care must be taken to control, limit, and monitor all access, using, for example, virtual private networks (VPN) or Demilitarized Zone (DMZ) architectures. If a device is being used in a manner that does not require wide area network access, it is strongly recommended that the device not be connected to any wide area network to reduce attack surface.

- Harden system configurations by enabling/using the available security features, and by disabling unnecessary ports, services, functionality, and network file shares.
- Apply the latest Emerson product security updates, SIMs, and other recommendations.
- Apply 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 Sample Checklist

This section provides a sample checklist to help guide the process of securely deploying Emerson products.

1. Create or locate a network diagram.
2. Identify and record the required communication paths between nodes.
3. Identify and record the protocols required along each path, including the role of each node.
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 & other network security devices.
6. Enable and/or configure the appropriate security features on each Emerson product.
7. On each Emerson product, change every supported password to something other than its default value.
8. Harden the configuration of each Emerson product, 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.*

Chapter 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 device, and by using appropriately configured and deployed network security devices (e.g. firewalls, routers) to block every protocol (whether enabled or disabled) 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 chapter describes how the supported serial and Ethernet application protocols are used in each Field Agent and indicates the role of each participant in the communication. 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 to support only the required communications paths for each installation.

3.1 Serial Communication

This section indicates which serial interfaces are supported by each Field Agent.

Table 5: Available Serial Interfaces

Interface	Mini Field Agent	Embedded Field Agent	Virtual Field Agent
RS-232	Yes	No	No
RS-485	No	No	No
CAN	Yes	No	No
SDIO (microSD)	No	No	No
USB	No	No	No

3.1.1 Application Layer Protocols

While there are no Field Agent serial application protocol stacks included by default in any Field Agent type, support for some serial protocols can be enabled by deploying an associated Machine Adapter. The table below indicates the serial protocols supported by each Field Agent type, and which Machine Adapter must be deployed to enable this protocol support.

Table 6: Available Serial Protocols

Interface	Mini Field Agent	Embedded Field Agent	Virtual Field Agent
Modbus RTU over RS-232	Yes (Modbus RTU Machine Adapter)	No	No
CAN bus	Yes	No	No

3.2 Ethernet Communication

This section indicates which Ethernet protocols are supported by each Field Agent. Some of the supported protocols may not be required in each system, since the installation may only be using a subset of the available protocols.

Table 7: Supported Ethernet Protocols

OSI Layer	Protocol	Mini Field Agent	Embedded Field Agent	Virtual Field Agent
Link	ARP	Yes	Yes	Yes
Network	ICMP	Yes	Yes	Yes
	IGMP	Yes	Yes	Yes
	IPv4	Yes	Yes	Yes
	IPv6	Yes	Yes	Yes
Transport	TCP	Yes	Yes	Yes
	UDP	Yes	Yes	Yes
Application	DHCP Client	Yes	Yes	Yes
	DNS Client	Yes	Yes	Yes
	Ethernet Global Data	Yes	Yes	Yes
	Ethernet/IP® CIP	Yes	Yes	Yes
	Ethernet/IP PCCC	Yes	Yes	Yes
	HTTP Server	No	No	Yes
	HTTPS Server	Yes	Yes	Yes
	Modbus® TCP Master	Yes	Yes	Yes
	OPC® UA Client	Yes	Yes	Yes
	OSI PI Web Services	Yes	Yes	Yes
	VPN	Yes	Yes	Yes

3.2.1 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 8: Link Layer Protocols

Protocol	Ether Type
ARP	0x0806

Table 9: Internet Layer Protocols

Protocol	Ether Type	IP Protocol #
ICMP	0x0800	1
ICMP	0x0800	2
IPv4	0x0800	N/A
IPv6	0x86DD	N/A

Table 10: Transport Layer Protocols

Protocol	Ether Type	IP Protocol #
TCP	0x0800	6
UDP	0x0800	17

Note: *Each of these lower-level protocols is required by one or more of the supported Field Agent Application protocols.*

3.2.2 Application Layer Protocols

Field Agents can act as a server, responding to requests sent through any of several different protocols. They can also act as a client, sending requests to other servers using any of several different protocols. The following table, Application Layer Protocols, lists the protocols supported by Field Agents, along with any TCP or UDP ports that are leveraged by those protocols. This table could aid in configuring a firewall between each Field Agent and any clients or servers it communicates with. The table Supported Ethernet Protocols lists which of these protocols each Field Agent communicates with, when in a client or server role.

Table 11: Application Layer Protocols

Protocol	Server TCP Port	Destination UDP Port
DHCP		67 on server 68 on client
DNS	53	53 on server >1023 on client
Ethernet Global Data		18246
Ethernet/IP CIP	44818	
Ethernet/IP PCCC	44818	
HTTPS	443, 8443	
Modbus TCP	502	
OPC UA	4840, 4841	
OSI PI Web Services	443	
VPN	443	

3.3 Cellular Communication

Some Field Agents can leverage cellular communications. This section describes which cellular technologies are supported by each Field Agent type.

Table 12: Cellular Communication Support

Cellular	Mini Field Agent	Embedded Field Agent	Virtual Field Agent
4G LTE Cellular on AT&T Private Network	Yes	No	No
4G LTE Cellular using Customer-Provided SIM	Yes	No	No

Table 13: Supported Protocols over 4G LTE Cellular Connection

OSI Layer	Protocol	Mini Field Agent
Network	ICMP	Yes
	IGMP	Yes
	IPv4	Yes
	IPv6	Yes

3.3.1 4G LTE Cellular General Information

MFAs with catalog numbers ICMFA001US0, ICMFA001US1, ICMFA001EU0, and ICMFA001EU1 include cellular modems that can be configured for use as the communication path between the MFA and Predix* Cloud. However, these cellular-capable MFAs do not have the cellular modem enabled by default. Instead, the default cloud connection uses the wired Ethernet WAN port. By connecting to the Predix Machine Web Console though the MFA's LAN Ethernet interface (or Wi-Fi hotspot WLAN interface in Configuration Mode only), the cellular modem can be selected as the cloud connection setting in the Technician Console > Network Configuration page. When the cellular modem is enabled as the cloud connection and is connected to the cellular network, the internal MFA network routing prevents any outgoing traffic from using the wired Ethernet WAN interface. Similarly, if the cloud connection is set back to use the wired Ethernet WAN interface, the cellular modem is disabled, and the routing is switched to use the wired Ethernet WAN interface. The detailed instructions for enabling and disabling the MFA cellular modem and verifying the cellular connection can be found in the Field Agents User Guide, GFK-2993.

The cellular modem's IMEI and SIM's ICCID can be found printed on the MFA cover. These values and other cellular diagnostics are also available in the Technician Console > Cellular page in the Predix Machine Web Console.

3.3.2 4G LTE Cellular on AT&T Private Network

MFAs with catalog numbers ICMFA001US1, ICMFA001EU1, ICMFA001AE1, ICMFA001AU1, and ICMFA001UM1 include a cellular modem and an activated AT&T SIM card authorized to connect to a private cellular network, arranged through a partnership between Emerson and AT&T, with direct access to the Predix Cloud environment. The IP addresses assigned to connected MFAs are not Internet-routable, so there is no network path for a malicious third party on the Internet to attempt to initiate a connection to the MFA directly. Furthermore, this private network guarantees that any MFA network traffic destined to the Predix Cloud such as industrial data from a connected data source cannot be intercepted by a malicious third party on the Internet. However, MFAs have indirect Internet access by routing requests through the Predix Cloud environment.

3.3.3 4G LTE Cellular using Customer-Provided SIM

MFAs with catalog numbers ICMFA001US0, ICMFA001EU0, ICMFA001AE0, ICMFA001AU0, and ICMFA001UM0 include a cellular modem but no SIM. When using a customer-provided SIM, the corresponding APN connect string must be configured in the Technician Console > Cellular page in the Predix Machine Web Console. Since the customer-provided SIM may use a cellular network with direct Internet access, it is critical to perform a thorough security assessment of the MFA deployment considering the use and abuse cases of the application.

3.3.4 Recommendations

Emerson strongly recommends removing the cellular antennas from the MFA on models that support cellular if the MFA is configured to use wired Ethernet and is not expected to make use of the cellular modem.

3.4 Wireless Local Area Network Communication

Some Field Agents can leverage wireless communications for Wireless Local Area Networks (WLAN). This section describes which WLAN technologies are supported by each Field Agent type.

Table 14: Wireless Communication Support

Wireless Communication	Mini Field Agent	Embedded Field Agent	Virtual Field Agent
802.11 Wi-Fi Hotspot	Yes (only in Configuration Mode)	No	No

3.4.1 802.11 Wi-Fi Hotspot

With physical access to the Mini Field Agent (MFA), the Push Button interface can be used to enable Configuration Mode, which is documented in Section 2.2.1 of the Field Agents User Guide, GFK-2993. When Configuration Mode is enabled, the MFA broadcasts a Wi-Fi hotspot that can be used as a Local Area Network by nearby devices like laptops and smart phones. When devices connect to the Wi-Fi hotspot, they can use this WLAN to authenticate with the Predix Machine Web Console, if it is enabled, to perform device enrollment and read device diagnostics. In this way, the Wi-Fi hotspot provides the equivalent level of access to the MFA as a wired Ethernet connection on the LAN interface.

Each MFA uses a unique SSID that includes its serial number in the format shown below. To prevent accidental connection to a rogue Wi-Fi hotspot with the same or similar SSID, each MFA is assigned a unique Wi-Fi hotspot password that is printed on the MFA label near the serial number. Once connected to a MFA's Wi-Fi hotspot, the Predix Machine Web Console credentials are needed to interact with the MFA using its REST API.

While the MFA is in Configuration Mode with the Wi-Fi hotspot enabled, the MFA's green ON LED fades in and out slowly. Configuration Mode can be disabled by repeating the same steps taken to enable it, or by waiting one hour for Configuration Mode to automatically disable.

Table 15: Wi-Fi Hotspot Properties

Wi-Fi Hotspot Property	Value
SSID	mfa_<7-digital serial number> (e.g. mfa_td7s0sx)
Encryption Type	WPA2-PSK
Password	Printed on MFA label
Router IP Address	192.168.2.1
Router IP Subnet Mask	255.255.255.0
Number of Concurrent Client Connections	2
Client IP Address Assignment Range	192.168.2.20 - 192.168.2.21
DHCP Lease Duration	1 hour
Maximum Enabled Duration	1 hour

Clients connected to the MFA's Wi-Fi hotspot are provided IP addresses using DHCP and hostname resolution using DNS. Section 4.4.1of this document, MFA Firewall, describes the modifications made to the MFA's firewall to support DHCP and DNS when Configuration Mode is enabled.

Table 16: Supported Protocols over 802.11 Wi-Fi Hotspot in Configuration Mode

OSI Layer	Protocol	Mini Field Agent
Network	ICMP	Yes
	IGMP	Yes
	IPv4	Yes
	IPv6	No
Transport	TCP	Yes
	UDP	Yes
Application	DHCP Server	Yes
	DNS Server	Yes
	HTTPS Server	Yes

3.4.2 Recommendations

Emerson strongly recommends removing the Wi-Fi antenna from the MFA if the Wi-Fi hotspot feature will not be used. Similarly, Emerson strongly recommends removing the Wi-Fi antenna from enrolled and configured MFAs if there is no future expectation of using the Wi-Fi hotspot for diagnostics or reconfiguration.

Chapter 4: Security Capabilities

This chapter describes the Field Agent capabilities and security features that can be used as part of a defense-in-depth strategy to secure your system.

Table 17

Security Capability	Mini Field Agent	Embedded Field Agent	Virtual Field Agent
Predefined set of Subjects & Access Rights	Yes	Yes	Yes
Access Control List	Yes	Yes	Yes
Secure Remote Operations	Yes	Yes	Yes
Firmware Signatures	Yes	Yes	Yes
Software Firewall	Yes	Yes	Yes
Hardware Entropy Source	Yes	Yes	No
Hard Disk Encryption	No	Yes	No
Secure Boot	No	Yes	No

4.1 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).
2. Enforcement – Approving or rejecting access requests.

This section describes the Access Control capabilities supported by Field Agents, which includes its Authorization capabilities.

4.1.1 Authorization Framework

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

Table 18

Functionality	Application Protocol	Subjects Available
Predix Machine Web Console	HTTPS	“Predix” user

4.1.2 Enforcement

The Field Agent enforces the access rights for the data and services that it provides. An unprivileged user account is leveraged to run Predix Machine and the related services on the Field Agent. This account provides only the minimum privileges needed to operate these services.

4.2 Authentication

The Field Agent provides password-based authentication for all supported server protocols. The following tables provide a summary of authentication mechanisms supported by the Field Agent for each protocol.

Table 19: Authentication supported by Field Agent Servers

Functionality	Application Protocol	Authentication Supported
Predix Machine Web Console	HTTPS	Username and Password

Table 20: Authentication supported by Field Agent Clients

Functionality	Application Protocols	Authentication Supported
Lookup IP addresses by hostname	DNS	None
Read data from a Modbus TCP slave	Modbus TCP	None
Read data from an OPC UA server	OPC UA	Username and Password, Certificates
Ethernet Global Data Consumption	Ethernet Global Data	None
Ethernet Global Data Production	Ethernet Global Data	None
Read data from Ethernet/IP server	Ethernet/IP	None
Read data from an OSI PI server	OSI PI REST API	Username and Password

4.2.1 Authentication Recommendations

Emerson strongly recommends that authentication be used for every enabled protocol that supports authentication, and that all default passwords be changed. 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.

The following table provides recommended actions to mitigate the risk of external or internal entities accessing a facility network and sending unauthorized messages.

Table 21

Item	Recommendations
Personnel Security Protection	All individuals with permission to physically access end customer systems should have background checks and be trained in the proper use and maintenance of the systems.
Physical Security Perimeter Protection	Whenever possible, there should be no physical network path from a facility network to the Internet. It should not be possible for an attacker to reach a facility network from any Internet-facing computer.
	Networks should always be physically segmented as suggested in the Reference Network Architecture diagram (Figure 1) to avoid exposure to facility network.

Item	Recommendations
	Each asset should be visibly labeled by a unique identifier, with all expected asset identification compiled into an access-controlled list.
Electronic Security Perimeter Protection	All external access to a facility network should be managed through a Virtual Private Network (VPN) or similar technology leveraging two-factor authentication.
	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.
	If one network node such as MDI servers 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.
	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.
	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.
	To limit the impact of the compromise of any single user account, it is recommended to divide administrator privileges into several user accounts, each for its own operational function.
	To limit the impact of the compromise of any single set of credentials (user name, password) for any end customer equipment, it is recommended to never re-use credentials for different tools or purposes.
	Carefully protect sources of and access to credentials (user names, passwords) for all end customer equipment, including switches, routers, firewalls, IDS, IPS, etc.

Item	Recommendations
	Enforce a policy of rotating credentials for end customer equipment periodically and after personnel changes. Note that products with no support for enforcement of unique passwords over time should be compensated for with policies and procedures that require a history of unique passwords.
Passwords	Recommendations on password complexity and management can be found in NIST 800-118, Guide to Enterprise Password Management.

4.3 Password Management

Each instance of a server has its own instances of the predefined subjects. Therefore, passwords for each subject must be separately managed for each instance of a given kind of server.

Emerson strongly recommends the use of long (10 characters or more), complex passwords wherever passwords are used for authentication. Recommendations on password complexity and management can be found in NIST 800-118, Guide to Enterprise Password Management.

Table 22: Changing Passwords

Functionality	Authenticated Subjects	How Passwords Are Assigned
Predix Machine Web Console	"Predix" user	Auto-prompted upon first login using the default password (predix2machine). Configurable in the Web Console User Administration page.
Predix Machine Web Console	Additional users are created in the Web Console User Administration page	Passwords are assigned and modified in the Web Console User Administration page.

4.4 Firewall

Each Field Agent has a built-in firewall that is configured to block all incoming traffic other than the protocol types specified in the following tables by default. All outgoing traffic generated by the Field Agent is permitted through the firewall, as is incoming traffic related to an outgoing request. The firewall is configured to block all forwarded traffic, which prevents devices on the same network as the Field Agent from using it as a direct gateway to the wide area network. Refer to Section 0, Opening Additional Ports in the Firewall for instructions and considerations when an application or Machine Adapter needs additional ports opened in the firewall for operation.

4.4.1 MFA Firewall

The default MFA firewall does not permit any incoming TCP or UDP traffic on the Wide Area Network (WAN) port or the cellular interface on MFA catalog numbers that support cellular communications. The MFA firewall does permit incoming (1) HTTPS traffic (TCP port 8443) on the Local Area Network (LAN) port to enable Predix Machine Web Console access for provisioning and diagnostics and (2) EGD traffic (UDP port 18246) on the LAN port for the EGD Machine Adapter. Both the LAN and WAN ports permit incoming ICMP traffic.

Table 23: Incoming Traffic Permitted Through MFA Firewall with Configuration Mode Disabled

Network Interface	Protocol	Port Number
Wide Area Network (WAN)	ICMP	N/A
Local Area Network (LAN)	ICMP	N/A
Local Area Network (LAN)	HTTPS	8443/TCP
Local Area Network (LAN)	EGD	18246/UDP

When Configuration Mode is enabled, the MFA's Wi-Fi hotspot becomes active and temporarily modifies the firewall to permit incoming HTTPS traffic (TCP ports 443 and 8443) on the Wireless Local Area Network (WLAN) interface. TCP port 8443 is used to enable Predix Machine Web Console access for provisioning and diagnostics. TCP port 443 is used to enable a connected device like an iPhone to use the MFA as a gateway to the Predix Cloud APIs to create devices in EdgeManager, deploy software, and issue commands. All incoming HTTPS traffic on WLAN TCP port 443 is forwarded to the network interface used for the cloud connection, which is either the WAN Ethernet port or the cellular modem depending on the MFA configuration.

The Wi-Fi hotspot also includes a DHCP server that assigns connected clients IP addresses, and a DNS forwarding service that provides connected client with indirect hostname resolution. These services require permitting incoming DHCP traffic on WLAN UDP ports 67 and 68 and incoming DNS traffic on WLAN TCP and UDP port 53. All incoming DNS traffic on WLAN TCP and UDP port 53 is forwarded to the network interface used for the cloud connection, which is either the WAN Ethernet port or the cellular modem depending on the MFA configuration. The WLAN interface also permits incoming ICMP traffic.

Table 24: Incoming Traffic Permitted Through MFA Firewall with Configuration Mode Enabled

Network Interface	Protocol	Port Number
Wide Area Network (WAN)	ICMP	N/A
Local Area Network (LAN)	ICMP	N/A
Local Area Network (LAN)	HTTPS	8443/TCP
Local Area Network (LAN)	EGD	18246/UDP
Wireless LAN (WLAN)	ICMP	N/A
Wireless LAN (WLAN)	HTTPS	443/TCP, 8443/TCP
Wireless LAN (WLAN)	DNS	53/TCP, 53/UDP

Network Interface	Protocol	Port Number
Wireless LAN (WLAN)	DHCP	67/UDP, 68/UDP

4.4.2 EFA Firewall

The default EFA firewall does not permit any incoming TCP or UDP traffic on the Wide Area Network (WAN) port but does permit incoming ICMP traffic. Since the EFA does not have a Local Area Network (LAN) port, the WAN port must be used to access the Predix Machine Web Console for provisioning and diagnostics. To enable incoming HTTPS traffic (TCP port 8443) on the WAN port, the EFA must be placed into Configuration Mode using the Push Button interface in a process described in the Field Agents User Guide, GFK-2993. Configuration Mode is disabled automatically after one hour unless disabled manually earlier using the Push Button.

Table 25: Incoming Traffic Permitted Through EFA Firewall with Configuration Mode Disabled

Network Interface	Protocol	Port Number
Wide Area Network (WAN)	ICMP	N/A

Table 26: Incoming Traffic Permitted Through EFA Firewall with Configuration Mode Enabled

Network Interface	Protocol	TCP Port
Wide Area Network (WAN)	ICMP	N/A
Wide Area Network (WAN)	HTTPS	8443/TCP

4.4.3 VFA Firewall

The default VFA firewall does not permit any incoming TCP or UDP traffic on the Wide Area Network (WAN) port but does permit incoming ICMP traffic. The VFA firewall does permit incoming HTTPS traffic (TCP port 8443) on the Local Area Network (LAN) ports to enable Predix Machine Web Console access for provisioning and diagnostics. Both the LAN ports and WAN port permit incoming ICMP traffic.

Table 27: Incoming Traffic Permitted Through VFA Firewall

Network Interface	Protocol	Port Number
Wide Area Network (WAN)	ICMP	N/A
Local Area Network (LAN1/2)	ICMP	N/A
Local Area Network (LAN1/2)	HTTPS	8443/TCP

4.4.4 Opening Additional Ports in the Firewall

Some applications and Machine Adapters may require opening one or more of the user or registered TCP or UDP ports (starting at port number 1024). If a Machine Adapter requires connecting to a server on another device, a port does not need to be opened in this Field Agent's firewall since outgoing client requests are permitted by default. For example, the OPC UA Machine Adapter acts as a client that connects to an external OPC UA server, so the default firewall does not need to be modified in this case. However, if an application or Machine Adapter requires listening on a port for incoming network traffic, the firewall needs to be modified to permit incoming traffic on this port. For example, the EGD Machine Adapter requires UDP port 18246 to be opened in the Field Agent's firewall.

Currently, the MFA and VFA support opening additional ports through the firewall on Local Area Network (LAN) interfaces. The EFA also supports opening additional ports, but since there is no dedicated LAN interface on the EFA, the ports are opened on the WAN interface. Opening ports on the EFA WAN is intended for use cases involving an EFA connected to a LAN from which data is being collected. Whenever EFA WAN ports are opened, it is the responsibility of the customer to set up and configure proper routers and firewalls between the LAN and the Internet to limit outgoing traffic to only what is required for the EFA to communicate with the EdgeManager and the Time Series database.

Refer to the Field Agent Machine Adapters User Guide, GFK-3019, for the list of required ports to be opened for each supported Machine Adapter. Refer to the Field Agents User Guide, GFK-2993, for instructions for modifying the default firewall rules to open additional ports in the section How to Open Ports on a Field Agent.

In order to minimize the surface area for attacks on the Local Area Network, Emerson strongly recommends evaluating the possible security impact of each port to be opened, and only opening the minimum set of ports required to support the deployed applications and Machine Adapters. Furthermore, Emerson strongly recommends limiting the protocols used to the minimum set required for the intended application and adding additional compensating security controls whenever using insecure protocols that cannot be otherwise removed from the deployment.

4.5 Confidentiality and Integrity

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 it was malicious.

Following are the communications protocols supported by Field Agents provide either of these features, as detailed in the table below. Therefore, compensating controls may be required to meet an installation's security requirements for protecting data in-flight.

Table 28: Protocol-Provided Security Capabilities

Protocol	Data Encryption	Message Authentication Codes
Ethernet Global Data	No	No
DHCP	No	No
DNS	No	No
HTTPS	Yes	Yes
Modbus TCP	No	No
OPC UA	Yes	Yes
VPN	Yes	Yes

Chapter 5: Configuration Hardening

This chapter is intended to assist in reducing the potential attack surface by providing information that can be used to harden the configuration of Field Agents that are present in an installation. Configuration Hardening should be considered in addition to enabling and using security features such as Authentication, Access Control, and Authorization.

In general, Emerson recommends disabling all services and protocols that are not required for the intended application.

5.1 General Field Agent Configuration Hardening

5.1.1 Configure Automatic Field Agent Updates

Each Field Agent can update its Linux® operating system components and configuration manually or automatically. Emerson strongly recommends that customers keep the Linux packages on each Field Agent up-to-date. The instructions for performing or scheduling Field Agent updates are provided in the Field Agents User Guide, GFK-2993. Note that Predix Machine is not updated by the Field Agent Updater. Predix Machine must be updated through EdgeManager for EdgeManager to track the history of Predix Machine updates, in order to provide an auditable history of Configuration and Application updates per Field Agent.

5.1.2 Update Predix Machine to the Latest Supported Version

As new versions of Predix Machine are released by GE Digital, they are integrated into the various Field Agents distributed by Emerson. They are validated and released as officially supported versions. Due to resource constraints, performance optimizations, and security considerations, the default Predix Machine container is heavily customized to the profile of each Field Agent. In many cases, deploying a Predix Machine container built by a customer without customizations to a Field Agent can cause Predix Machine to fail to run, requiring a factory reset. For this reason, Emerson publishes Configuration and Application Templates that are pre-built, pre-validated Predix Machine containers on top of which customer modifications can be applied. Emerson also publishes migration packages for upgrading from one major version of Predix Machine to another.

Updating within a Predix Machine Minor Version

A pair of Configuration and Application Templates are published for each supported version of Predix Machine per Field Agent. The latest version of these Templates for a given minor version of Predix Machine (for example, 16.2) will contain all the latest patches from GE Digital (for example, 16.2.5). Emerson strongly recommends deploying the latest Configuration and Application Template for a given minor version of Predix Machine to patch all known defects and security vulnerabilities. Links to the Field Agent Configuration and Application Templates can be found on each Field Agent Landing Page referenced in Section 1.2.1, Product Landing Pages.

Upgrading to a New Predix Machine Major Version

Upgrading a Field Agent to a new major version of Predix Machine (for example migrating from 16.2.3 to 17.1.1) can be done two ways. If the Field Agent is enrolled and Reachable in EdgeManager, the Field Agent can be remotely upgraded by deploying an upgrade package from EdgeManager. If the Field Agent is not enrolled or not Reachable in EdgeManager, an offline upgrade can be applied in the Field Agent Updater page of the Predix Machine Web Console, which requires Local Area Network access. Links to the documentation for both upgrade processes can be found on each Field Agent Landing Page referenced in Section 1.2.1, Product Landing Pages.

5.1.3 Harden Access to each Industrial Data Source

When configuring a Field Agent to consume industrial data from a data source like an OPC UA Server or Modbus TCP Slave, it is important to configure the visibility of variables or registers such that only those tags that are expected to be consumed are readable by the Field Agent and other network nodes. For example, OPC UA variables in the PACSystems CPUs can be left unpublished, published internally to other components of the User Application, published as External Read-Only, or published as External Read/Write. Variables should not be published as External Read-Only unless they need to be read by a Field Agent or another network node. Variables should not be published as External Read/Write unless they need to be read and written to by a Field Agent or another network node. Refer to the User Guide or Secure Deployment Guide for the specific industrial data source to learn how to restrict the visibility of available variables and registers.

The OPC UA Machine Adapter and Modbus TCP Machine Adapter provided with Predix Machine in each Field Agent can only be configured to read industrial data. If the Field Agent is using only these default Machine Adapters, Emerson strongly recommends that all published variables and registers be only published as read-only. Predix Machine also includes APIs for writing to OPC UA variables and Modbus TCP registers. These APIs enable application developers to write custom application bundles to manipulate tags published as read/write. If such an application is in use, Emerson strongly recommends limiting the variables and registers published as read/write to the minimum set needed by the application.

As an additional layer of security, Emerson strongly recommends enabling authentication for read and write operations on industrial data sources wherever supported. For example, PACSystems CPUs should have Enhanced Security enabled with passwords protecting PRIV Levels 2, 3, and 4. With this set, an attacker on the network would be unable to, for example, write to any OPC UA variables that are accidentally published as read/write on a PACSystems OPC UA Server without knowing the PRIV Level 2 password.

If more granular control of specific read and write operations to industrial data sources is required, an application level firewall with knowledge of industrial protocols (like the Wurldtech OpShield*) can be placed in-line between the industrial data source and Field Agent. The firewall can be configured to enforce policies that whitelist specific Field Agents from reading or writing to specific OPC UA variables or Modbus TCP registers.

5.2 MFA Configuration Hardening

5.2.1 MFA Network Configuration

The Field Agents User Guide, GFK-2993, provides instructions for configuring the MFA's Wide Area Network (WAN) and Local Area Network (LAN) IP addresses. It is strongly recommended that the WAN and LAN interfaces each be configured for separate network subnets with no overlap.

5.2.2 Disable Predix Machine Web Console after Provisioning

The Predix Machine Web Console is a tool for local Field Agent management, maintenance, and diagnostics that is enabled by default and hosted by a web server accessible only on the MFA's Local Area Network (LAN). If the MFA is placed into Configuration Mode using the Push Button interface, the MFA's Wireless Local Area Network (WLAN) Wi-Fi hotspot can also be used to access the Predix Machine Web Console until Configuration Mode is either automatically disabled after one hour or manually disabled earlier. Detailed instructions for accessing and logging into the Predix Machine Web Console are in the Field Agents User Guide, GFK-2993.

Each Field Agent can be remotely instructed to disable or enabled the Predix Machine Web Console from the Predix EdgeManager. Emerson recommends disabling the Web Console from EdgeManager after the provisioning process is complete to minimize the attack surface by eliminating the local web server as a potential attack vector. Detailed instructions for Field Agent Commands including the command to disable the Web Console from EdgeManager are in the Field Agents User Guide, GFK-2993.

5.2.3 Remove Unused Cellular Antennae

Emerson strongly recommends removing the cellular antennas from the MFA on models that support cellular if the MFA is configured to use wired Ethernet and is not expected to make use of the cellular modem.

5.2.4 Remove Unused Wi-Fi Antennae

Emerson strongly recommends removing the Wi-Fi antenna from the MFA if the Wi-Fi hotspot feature will not be used. Similarly, Emerson strongly recommends removing the Wi-Fi antenna from enrolled and configured MFAs if there is no future expectation of using the Wi-Fi hotspot for diagnostics or reconfiguration.

5.3 EFA Configuration Hardening

5.3.1 Disabling Configuration Mode

The Predix Machine Web Console is a tool for local Field Agent management, maintenance, and diagnostics that is enabled by default and hosted by a web server. Since the EFA does not have a Local Area Network (LAN) port, the Wide Area Network (WAN) port must be used to access the Web Console. To enable Web Console access on the WAN port, the EFA must be placed into Configuration Mode using the Push Button interface in a process described in the Field Agents User Guide, GFK-2993.

Once the Web Console has been used for provisioning or diagnostics, Configuration Mode should be disabled to minimize the attack surface by eliminating access to the web server as a potential attack vector. Configuration Mode can be disabled using the Push Button in a process described in the Field Agents User Guide, GFK-2993. Configuration Mode is disabled automatically after one hour unless disabled manually earlier using the Push Button.

5.4 VFA Configuration Hardening

5.4.1 VFA Network Configuration

The Field Agents User Guide, GFK-2993, provides instructions for configuring the VFA's Wide Area Network (WAN) and Local Area Network (LAN) IP addresses. It is strongly recommended that the WAN and LAN interfaces each be configured for separate network subnets with no overlap.

5.4.2 Disable Predix Machine Web Console after Provisioning

The Predix Machine Web Console is a tool for local Field Agent management, maintenance, and diagnostics that is enabled by default and hosted by a web server accessible only on the VFA's Local Area Network (LAN). Detailed instructions for accessing and logging into the Predix Machine Web Console are in the Field Agents User Guide, GFK-2993.

Each Field Agent can be remotely instructed to disable or enabled the Predix Machine Web Console from the Predix EdgeManager. Emerson recommends disabling the Web Console from EdgeManager after the provisioning process is complete to minimize the attack surface by eliminating the local web server as a potential attack vector. Detailed instructions for Field Agent Commands including the command to disable the Web Console from EdgeManager are in the Field Agents User Guide, GFK-2993.

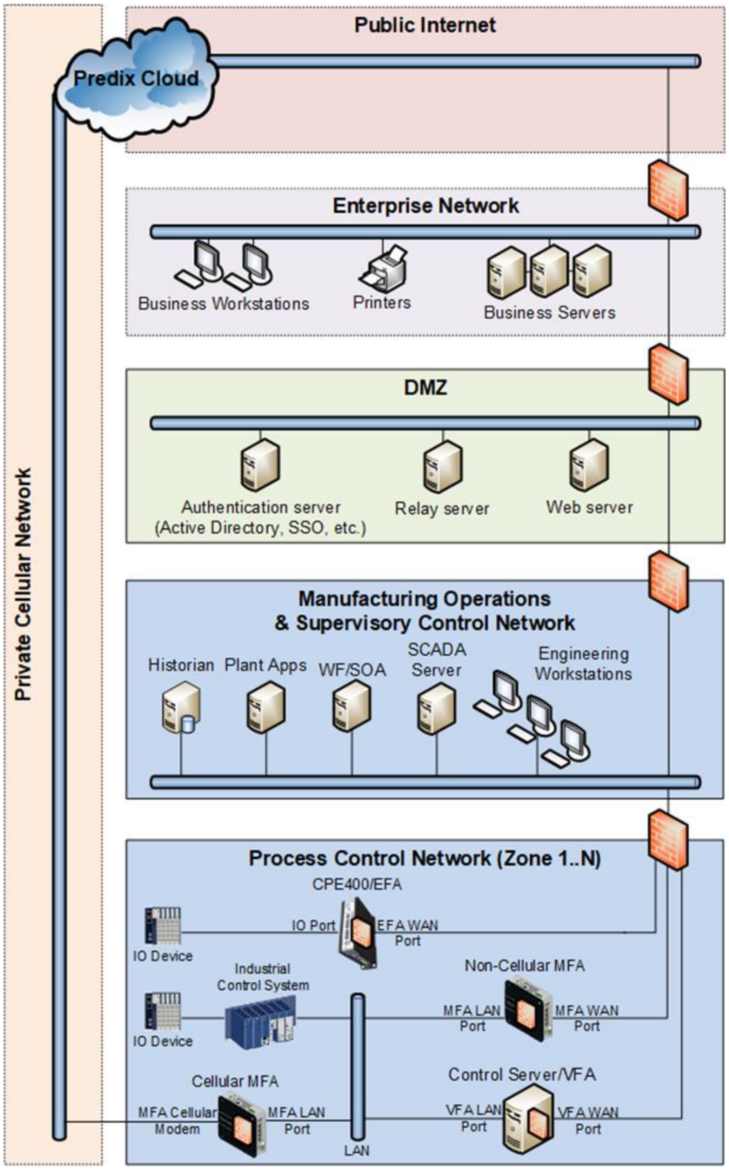
5.4.3 Change Predix User Account Password after Provisioning

It is strongly recommended that the Predix user account have its password changed after provisioning. From the Linux command line, the "passwd" utility can be used to change the account password. For example, to change the password to "example" execute the command: passwd example. Recommendations on password complexity and management can be found in NIST 800-118, Guide to Enterprise Password Management.

Chapter 6: Reference Network Architecture

The following figure represents a typical deployment of a Field Agent for a large industrial application. However, the level of segmentation will vary based on the level of risk assessed for the application.

Figure 1: Field Agents SDG Reference Network Diagram



6.1 Remote Access and Demilitarized Zones (DMZ)

The Manufacturing Zone networks (which include the Manufacturing Operations, Supervisory Control, and Process Control networks) are segregated from other untrusted networks such as the Enterprise network (also referred to as the Business network, Corporate network, or Intranet) and the Internet using a Demilitarized Zone (DMZ) architecture. The Process Control networks have limited exposure to traffic from higher-level networks, including other networks in the Manufacturing Zone, as well as from other Process Control networks. The Enterprise network may also reside behind a separate DMZ.

A DMZ architecture uses two firewalls to isolate servers that are accessible from untrusted networks. The DMZ should be deployed such that only specific (restricted) communication is allowed between the Emerson devices and the DMZ, and between the Cloud / Internet and the DMZ.

6.2 Field Agent to Cloud Communications

Ethernet traffic from the Cloud/Internet to the Field Agent should be restricted to support only the functionality that is required. If a protocol is not needed between those regions, then the firewall should be configured to block that protocol.

Note: *Network Address Translation (NAT) and Port Address Translation (PAT) firewalls typically do not expose all the devices on the "trusted" side of the firewall to devices on the "untrusted" side of the firewall. Further, NAT/PAT 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 initial provisioning communication to Field Agents may be initiated from a PC on the "untrusted" side of the Process Control network firewall, protecting a Process Control network using a NAT/PAT firewall may cause additional communication challenges. Before deploying NAT/PAT, carefully consider its impact on the required communications paths.*

⚠ WARNING

All field agents permit users to upload code, which could be used to exploit the Specter/Meltdown vulnerabilities.

6.3 Field Agent to Industrial Data Source Communications

Emerson recommends avoiding the use of a Field Agent's Wide Area Network (WAN) port for communicating with industrial data sources like control systems. This practice is normally unnecessary since, for example, the MFA has a Local Area Network (LAN) for this purpose and the EFA communicates directly with its connected control system over the hypervisor virtual network.

However, there may be situations where it is necessary to use a Field Agent's WAN port to communicate with an industrial data source. In such situations, Emerson strongly recommends structuring the network in such a way that does not bridge or otherwise expose the entire Process Control Network to the Manufacturing Operations & Supervisory Control Network and/or DMZ. Special care must be taken to ensure the firewall between the Process Control Network and higher-level networks is configured to block access to any control systems or other industrial data sources from the Manufacturing Operations & Supervisory Control Network.

Chapter 7: Other Considerations

7.1 Patch Management

A strategy for applying security fixes, including patches, firmware updates, and configuration changes, should be included in a facility's security plan. Applying these updates may require that an affected Field Agent be temporarily taken out of service.

Some installations require extensive qualification 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 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 Government Agencies & 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 industrial control systems and related equipment. Below is a list of common standards and regulations to consider when designing a system's security policy and architecture. Such documentation, when appropriate, should be considered in addition to this document.

- ISA/IEC 62443 (formerly ISA99) for critical infrastructure
- NIST 800-53 for federal information systems
- ISO 27001 for information security management
- ISO 27002 for information security management
- ISO 27019 for information security management of electric systems
- NERC CIP V5 for critical infrastructure specific to electric systems
- NIST Cyber Security Framework for critical infrastructure

Technical Support & Contact Information

Home link: http://www.emerson.com/industrial-automation-controls

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

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™