PACEdge™

SECURE DEPLOYMENT GUIDE

EMERSON™

Contents

Warnings and 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 exist in this equipment or may be associated with its use.

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

⚠ CAUTION

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

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

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 the 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 a particular purpose.

Section 1: About this Guide

⚠CAUTION

Emerson provides these general recommendations and guidelines to aid the end-user in managing security risk associated with the operation of an Emerson PACEdge System (hardware with pre-installed PACEdge Software). It is entirely the owner's responsibility to ensure the security of the Linux OS and any associated applications deployed on the platform.

1.1 Applicable Products

This document provides information that can be used to help improve the cybersecurity of systems that include Linux Operating Systems supplied by Emerson Automation & Controls. It is intended for use by control engineers, integrators, IT professionals, and developers responsible for deploying and configuring products with an embedded, customer-accessible Linux OS.

Table 1: Product Description

Product	Description	Provisioning Connection	Data Source Connection	Cloud Connection
PACEdge 2.2.0	PACEdge v2.2.0 release. **Main Updates:** Support for Movicon v4.2 Updated Node-RED to version v2.2.2 Updated Grafana to version v9.0.2 Updated Telegraf to version v1.23.2 Updated other applications to newer versions Another Improved PACEdge usability	Ethernet LAN, USB	Ethernet LAN, USB	Ethernet LAN
PACEdge 2.1	Linux-based Edge software, running on Industrial PC	Ethernet LAN, USB	Ethernet LAN, USB	Ethernet LAN

1.2 Related Documentation

This section provides information on related documents. These documents include product landing pages and related documents that contain additional information.

1.2.1 Product Landing Pages

Table 2: Landing Page Reference

Product	URL
PACEdge	https://emerson-mas.force.com/communities/en_US/Article/PACEdge-Landing-Page

1.2.2 PACEdge Documentation

Document ID	Document Title
GFK-3074	PACEdge RXi2-LP Quick Start Guide
GFK-3178	PACEdge User's Manual
GFK-3187	RXi2-BP User's Manual
GFK-3196	PACEdge RXi2-BP Quick Start Guide
GFK-3197	PACEdge Secure Deployment Guide
GFK-3199	RXi2-BP Quick Start Guide
GFK-3200	RXi2-BP Secure Deployment Guide
GFK-3053	RX3i Rackless CPUs with PACEdge Quick Start Guide

1.3 Revisions in this Manual

Table 3: Product Revision

Rev	Date	Description
C	Nov 2022	Updates to support PACEdge 2.2.0
B	Aug 2021	PACEdge 2.1 adds support to IPCs and CPE400/CPL410
A	Sep 2020	Initial Publication

The most recent documentation is available on the Emerson technical support website listed at the end of this document.

Section 2: Introduction

Section 2 is intended to show why it is important to secure Emerson products. It explains what security means and why it is important not to rely only on a firewall. Readers can expect to learn about the Defense in Depth concept and its general recommendations. An example checklist is also provided, which should help to securely deploy the Emerson product.

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 the appropriate care in securing their Emerson products and solutions. As Emerson's 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 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 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.

- Edge devices span both control networks and wide area networks (WAN), potentially extending to include access to the Internet as a whole. Network segmentation and firewall rules must be carefully considered to reduce the allowed traffic to the bare minimum needed for operation. Care must be taken to control, limit, and monitor all access, using, for example, virtual private networks (VPN) or Demilitarized Zone (DMZ) architectures. All communication endpoints should be considered individually, and if a specific protocol or the device as a whole does not require wide-area network access, it is strongly recommended that the relevant protocols be restricted to the most limited network possible.
- 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 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.*

Section 3: Communication Interfaces

Communication between different parts of a control system 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, and by using appropriately configured and deployed network security devices (for example, firewalls, routers) to block every protocol (whether disabled or not) that does not 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 first describes the supported protocols.

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 a particular installation.

3.1 Ethernet Communication

This section indicates which Ethernet protocols are supported by PACEdge products by default. As access to the operating system is not limited, additional protocols can be installed by the user.

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: Supported Ethernet Protocols

OSI Layer	Protocol
Link	ARP
Network	ICMP
	IGMP
	IPv4
	IPv6
Transport	TCP
	UDP
Application	DHCP
	DNS
	HTTP
	HTTPS
	OPC® UA
	SSH/SCP/SFTP
	MQTT

3.1.1 Lower-level Protocols

The following are the details of the lower-level Ethernet communication layers.

Table 5: Link Layer Protocols

Protocol	EtherType
ARP	0x0806

Table 6: Internet Layer Protocols

Protocol	EtherType	IP Protocol #
ICMP	0x0800	1
IGMP	0x0800	2
IPv4	0x0800	N/A
IPv6	0x86DD	N/A

Table 7: Transport Layer Protocols

Protocol	EtherType	IP Protocol #
TCP	0x0800	6
UDP	0x0800	17

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

3.1.2 Application Layer Protocols

Embedded open Linux can act as a server, responding to requests sent through several different protocols. It can also act as a client, sending requests to other servers using several different protocols. The following table, Application Layer Protocols, lists the protocols supported by embedded open Linux, along with any TCP or UDP ports that are leveraged by those protocols. This table could aid in configuring a firewall between the embedded Linux Controller and any clients or servers it communicates with. This table lists which of these protocols are being used.

Table 8: Application Layer Protocols

Protocol	TCP Port	UDP Port
HTTP	80	-
HTTPS	443, 9090	-
SSH	22	-
MQTT	1883	-
OPC UA Server	62841,62859,62871	-
DNS	53	53

Note: Cockpit's Navigator Plugin requires access to current files/directories on the machine to be able to visualize them in the Cockpit UI. This triggers temporary system-level Unix Ports to be opened to initially read the information on the operating system and to be displayed in the Browser within the Cockpit UI.

3.1.3 OPC UA Port Forwarding Feature

The OPC UA Port Forwarding feature creates a temporary tunnel from one Ethernet interface to the other on one specific port. This tunnel exposes OPC UA Server on one network to be accessible on the other network. The consequences and risks of this temporary exposure need to be considered when using this feature. Care should be taken not to leave the port open longer than necessary. To use this feature, administrator rights are needed and a security mechanism will automatically close the port after a **maximum** of 60 minutes. For detailed usage instructions, please refer to GFK-3187, PACEdge User Manual.

3.2 Remote Access Technologies

PACEdge User Manual documents few remote access technologies that have been tested with the product. If a remote connection to the device is required, please consider using one of the documented methods in order to minimize cyber security risks.

⚠ CAUTION

In general, caution should be taken when opening ports, as there are major security risks in doing so without the appropriate precautions and technical knowledge.

Section 4: Security Capabilities

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

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 PACEdge, 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 9: Authorization Framework

Functionality	Application Protocol	Subjects Available	PACEdge System
PACEdge Home Page	HTTPS	-	No
PACEdge Application Pages	HTTPS	**admin** user **developer** user **service** user **operators** user	Yes
Remote Login	SSH	**admin** user	Yes

4.1.2 Enforcement

PACEdge enforces access rights for the data and services that it provides. An unprivileged user account **admin** is leveraged by default to allow login. This account provides pseudo privileges to allow complete system administration. Emerson recommends adding less privileged users for non-administrative tasks.

4.2 Authentication

PACEdge provides password-based authentication for most server protocols. The following tables provide a summary of authentication mechanisms supported by PACEdge for each protocol.

Table 10: Authentication supported by default Servers

Functionality	Application Protocol	Authentication Supported
PACEdge Home Page	HTTPS	No authentication
PACEdge Application Pages	HTTPS	Username and Password
OS Remote Login	SSH	Username and Password

Table 11: Authentication supported by default Clients

Functionality	Application Protocols	Authentication Supported
Lookup IP addresses by hostname	DNS	None
Read data from an OPC UA server	OPC UA	Username and Password, Certificates
Inter-application communication, pub/sub mechanism	MQTT	Username and Password, RBAC*

*For more information please visit:
https://mosquitto.org/documentation/dynamic-security/

4.2.1 Privileged Users

As Linux is part of PACEdge it should be mentioned that the superuser root has all rights and permissions to all files and programs.

As root therefore potentially can cause great damage to a PACEdge system, it is common practice not to allow root to log in. Instead, ordinary users are provided with additional rights via the **superuser do** (sudo documentation: https://www.sudo.ws/) mechanism. This powerful tool can be configured (/etc/sudoers.d) to assign privileges fine-granularly to users on a per-program

basis. To execute a command requiring privileges, a sudo user needs to prepend **sudo** to the command.

Emerson recommends providing users only with the minimum privileges required for their tasks.

Table 12: Embedded Linux Default Users

User	Authentication	Sudo	Sudo Auth.	Linux
admin	Username and Password	Yes	Yes	Yes
root	Disabled	NA	NA	Yes
developer	Disabled	Yes	Yes	Yes
service	Disabled	Yes	Yes	Yes
operators	Disabled	NA	NA	Yes

4.2.2 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.

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 the facility network.
	Each asset should be visibly labeled by a unique identifier, with all expected asset identification compiled into an access-controlled list.
	The devices should be physically protected from unauthorized access.

Item	Recommendations
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, 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.
	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.

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

4.3 Password Management

The passwords of PACEdge should be changed at the first login. 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 Special Publication 800-63-3, Digital Identity Guidelines (https://pages.nist.gov/800-63-3/sp800-63b.html).

Details on password management can be found in GFK-3178, PACEdge User Manual.

Firewall

A firewall is a network security mechanism filtering network traffic according to predefined firewall rules. With a firewall the user can, for example, limit Linux access to specified IP Addresses or services (ports).

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.

4.3.1 PACEdge System Firewall

PACEdge has native firewall support. However, it is worth noting that the user should be cautious about using it without proper configuration. An improperly configured firewall may result in user lockouts from the operating systems. Emerson advises using firewalls with extreme caution and only with appropriate expertise.

4.3.2 PACEdge System Default Network Services

A network service is a program running in the background, monitoring network connections from remote clients and providing data services to those clients.

The default setup of Linux with PACEdge instantiates a minimal set of network services:

Table 13: Default Network Services

Service	Protocol	Accepted Addresses	Port	Program
SSH	TCP IPV4/IPV6	From all	22	sshd
HTTP	TCP IPV4/IPV6	From all	80 Redirected to HTTPS	PACEdge
HTTPS	TCP IPV4/IPV6	From all	443, 9090	PACEdge
ICMP	IPV4/IPV6	From all	N/A	Kernel IP Stack
OPC UA	IPV4/IPV6	From all	62841, 62859, 62871	PACEdge
MQTT	IPV4/IPV6	From all	1883	PACEdge
NTP	UDP	-	123	NTP
DNS	IPV4/IPV6	-	53	DNS

Every network service offered to remote clients also may be an attack vector by exploiting bugs in the implementation of this service. To minimize the vulnerability to attacking the surface of your PACEdge system, only start as few services as necessary and limit access to the remaining services by firewall rules or appropriate service configuration.

4.4 Confidentiality and Integrity

Some communications protocols provide features that help protect data while it is “in-flight” – or 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.

The following are the communications protocols supported by PACEdge and their capabilities. Note that in some cases additional security mechanisms may be required to meet an installation's security requirements for protecting data in-flight.

Table 14: Protocol-Provided Security Capabilities

Protocol	Data Encryption	Message Authentication Codes
DHCP	No	No
DNS	No	No
HTTPS	Yes	Yes
OPC UA	Yes	Yes
MQTT	No	No

4.4.1 PACEdge Integrity

Industrial PCs that PACEdge is installed on do support Secure UEFI Boot technology, which users can configure and enable. Secure UEFI Boot would protect the integrity of the GRUB boot loader, however, Linux operating system and PACEdge applications are meant to be frequently updated and are open for user modifications. Such updates and modifications will cause security hashes to change and therefore are difficult to protect using static secure boot chain technologies. Emerson, therefore, cannot guarantee the security or integrity of the Linux components. It is the responsibility of the user to ensure that only trustworthy drivers and applications are being installed into Linux and that existing Linux files have not been tampered with.

One possibility to ensure the integrity of Linux is to regularly create hashes of monitored files and compare them with externally stored reference values or implement remote attestation

Low-Level Security Technologies

Some low-level security technologies come with the hardware. Some examples are Secure Boot, Measured Boot, and Secure Flash. For details, please refer to the secure deployment guide (SDG) for the specific hardware. A list of documentation is provided in Section 0,

Related Documentation.

UEFI Password

Unified Extensible Firmware Interface (UEFI) is the interface between the operating system and the IPC's firmware, which initializes and configures the hardware components of an IPC. The UEFI offers menus to modify hardware and firmware options. As these settings directly influence the hardware behavior, e.g. the device the IPC boots from, these settings are also security-relevant. To avoid unauthorized changes in UEFI settings, access to the menus can be restricted by password. By default, this password is not activated, but Emerson strongly recommends making use of the security advantages of an enabled password. You can change/activate the UEFI password by hitting the F2 button of an attached keyboard during boot and then selecting the Security menu and the Password change entry.

SSH

SSH allows secure transfer protocols using encryption only. Encryption keys are therefore automatically exchanged between the server and the client. So, if establishing an SSH client connection for the first time, the user will be asked to accept the remote host's public key. Accepted public keys are stored in a client database to be used in future communications. If a fake server tries to masquerade as a known server whose public key is already stored in the client database, SSH tools will warn about a key change, thus enabling the user to identify the fraud.

Note: *It is recommended to disable port forwarding for the SSH server.*

PACEdge System SSH

The SSH-Host-Key-Pairs (public and private) are stored in the directory /etc/ssh. These keys are not populated at the time of delivery. Therefore, new SSH-Keys are generated automatically during the first boot or whenever Linux detects missing keys during bootup. Users may use these generated keys or create new ones with the ssh-keygen command.

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 configurations that are present in a PACSystem. 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 Harden Access to each Industrial Data Source

When implementing applications consuming industrial data from a data source like an OPC UA Server 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 application 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 an embedded Linux application 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.

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 are required, an application-level firewall with knowledge of industrial protocols can be placed in line between the industrial data source and Field Agent. The firewall can be configured to enforce policies that whitelist specific devices from reading or writing to specific OPC UA variables.

5.2 PACEdge System 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 PACEdge.

5.2.1 Network Configuration

DHCP as well as a static IP address is configured by default. Further information can be found in the PACEdge User's Manual.

5.2.2 PACEdge Encrypted Communication

The connection to PACEdge is encrypted by default. To make sure, that the communication between PACEdge and other Devices is encrypted properly, only TLS v1.2 or newer is allowed. For the encryption, Traefik and Cockpit use self-signed certificates (SHA 256, RSA 2048 bit, 3650 days validity) by default. The private keys and certificates can be replaced by a customer-generated X.509 keypair.

Replace the certificate with an x509 certificate example (self-signed):

```
openssl req -new -x509 -sha256 -newkey rsa:4096 -nodes -keyout
/etc/ssl/PACEdgeServerPK.pem -days 3650 -out
/etc/ssl/PACEdgeServerCert.crt -subj "/C=DE/ST=BY/L=AUG
/O=Emerson/OU=PACEdge/CN=PACEdge.Emerson.com"

cp /etc/ssl/PACEdge/PACEdgeServerCert.crt
/etc/ssl/PACEdge/PACEdgeServer.crt

sudo sh -c "cat /etc/ssl/PACEdge/PACEdgeServerPK.pem >>
/etc/ssl/PACEdge/PACEdgeServer.crt"

chgrp cockpit-ws /etc/ssl/PACEdge/PACEdgeServer.crt

chmod 440 /etc/ssl/PACEdge/PACEdgeServer.crt

chmod 400 /etc/ssl/PACEdge/PACEdgeServerPK.pem
```

Reboot the system

5.2.3 PACEdge system Linux OS Update

PACEdge is based on the Linux operating system, which is continuously being developed and updated. New cyber security threats and their mitigations are being continuously introduced and it is important to keep the operating system up to date. PACEdge supports a few methods to update Linux operating system.

The main update method, well suited for systems that do not have internet connectivity, is to install the latest PACEdge software version. Users can get information about PACEdge software updates by periodically checking the SFDC website or by activating automated notifications.

The alternative method is to connect PACEdge to the Internet and use Cockpit to perform an automated Linux operating system update.

It is also possible to update the Linux manually by monitoring the Ubuntu update and security mailing lists for relevant announcements. Following are some of the mentioned mailings lists:

- https://lists.ubuntu.com/ (general)
- https://lists.ubuntu.com/mailman/listinfo/ubuntu-security-announce (security)
- https://lists.ubuntu.com/mailman/listinfo/Focal-changes (ubuntu 20.04 updates)

Depending on the software repositories configured in /etc/apt/sources.list file and in the /etc/apt/sources.list.d directory, new software packages are typically downloaded from external repositories. A working Internet connection is therefore required to install or update packages.

Upgrading a system also can include the Linux Kernel and the initial RAM disk, both located in the /boot directory. If a new Kernel or RAM disk has been installed by the manual upgrade, make sure the symbolic links /boot/vmlinuz and /boot/initrd.img are pointing to the latest Kernel (RAM disk version).

Note: Please perform a complete PACEdge backup, as described in the PACEdge User's Manual, before performing upgrades.

Note: *There is always a risk of damage to the Linux installation when upgrading the system, especially if the Kernel is being updated. Therefore, automatic Linux updates are deactivated by default. If you want to upgrade your system manually and not with the official releases consider performing such an upgrade in a protected environment before attempting such an upgrade on a production system.*

5.2.4 PACEdge Home Page WEB Server

PACEdge's home page is hosted by an internal web server. This server is listening to ports 80 (HTTP), and 443 (HTTPS), whereas access to port 80 is redirected to HTTPS protocol. The Web server provides an overview of the PACEdge services. All shown services can be accessed by clicking on the icons. The access to the web server is not protected by default, but to use individual services valid credentials are needed.

If a service is not needed for the use case, it is strongly recommended to disable it.

5.2.5 Cockpit

The cockpit offers a graphical user interface to manage Linux PCs. It can be reached via Browser on Port 9090. The cockpit uses the same credentials as the Linux system. The cockpit can be used as a graphical tool to perform Linux component updates.

Note: Do NOT change the root password!

5.3 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 device be temporarily taken out of service.

Some installations require extensive qualifications 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.

***Note**: Automatic updates are deactivated by default. Please check regularly for available security updates.*

5.4 Protocol-Specific Guidance

Protocol standards bodies may publish guidance on how to securely deploy and use their protocols.

5.5 Logging

In addition to the above-mentioned IDS and IPS log options for the network, the log options available on the device should also be used. This helps to monitor the system and can also be useful for error diagnosis.

For all PACEdge services logging is activated by default. The Linux logs can be seen in the Cockpit interface logs. All other logs can be seen in Portainer when clicking on the containers.

5.6 Self-written extensions

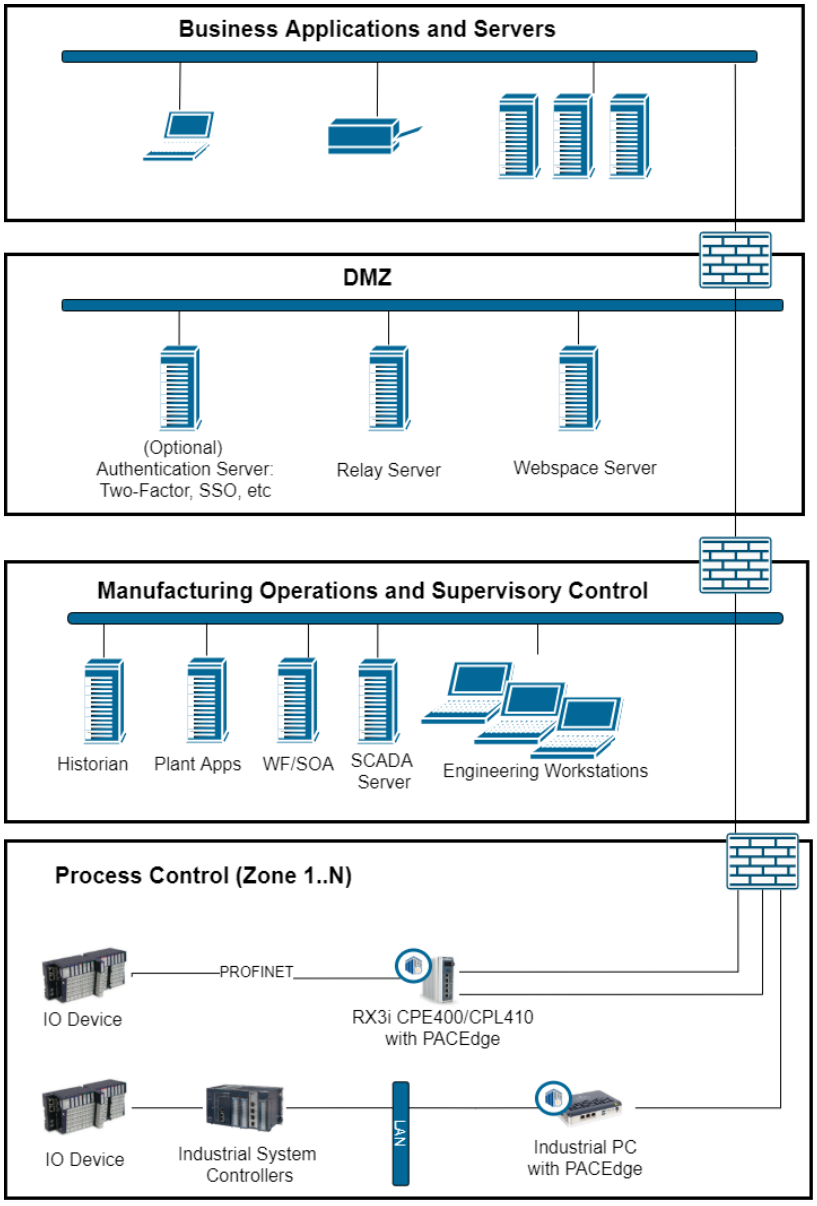
PACEdge provides many possibilities to write customized extensions for the functionality of the system. There are a couple of general security aspects which should be considered:

- Databases with sensitive data should be stored encrypted and secured by a strong password
- All communications should be encrypted (Database connections, etc.)
- Secure coding should be used for self-written extensions to prevent vulnerabilities

Section 6: Reference Network Architecture

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

Figure 1: Information Architecture



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 PACEdge to Cloud/Internet Communications

Ethernet traffic from the Cloud/Internet to PACEdge 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 PACEdge 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.*

6.3 PACEdge to Industrial Data Source Communications

Emerson recommends avoiding the use of network ports for simultaneous communication with industrial data sources like control systems and Wide Area Networks (Cloud).

However, there may be situations where it is necessary to use a port to communicate with an industrial data source and the Internet. 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.

Section 7: Other Considerations

7.1 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.

- ISA/IEC 62443 (formerly ISA99) for critical infrastructure
- T 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 Cybersecurity Framework for critical infrastructure

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 the toll-free 800 option is unavailable or dialing from a mobile)

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 the proper selection, use, and maintenance of any Emerson product remains solely with the purchaser.

EMERSON