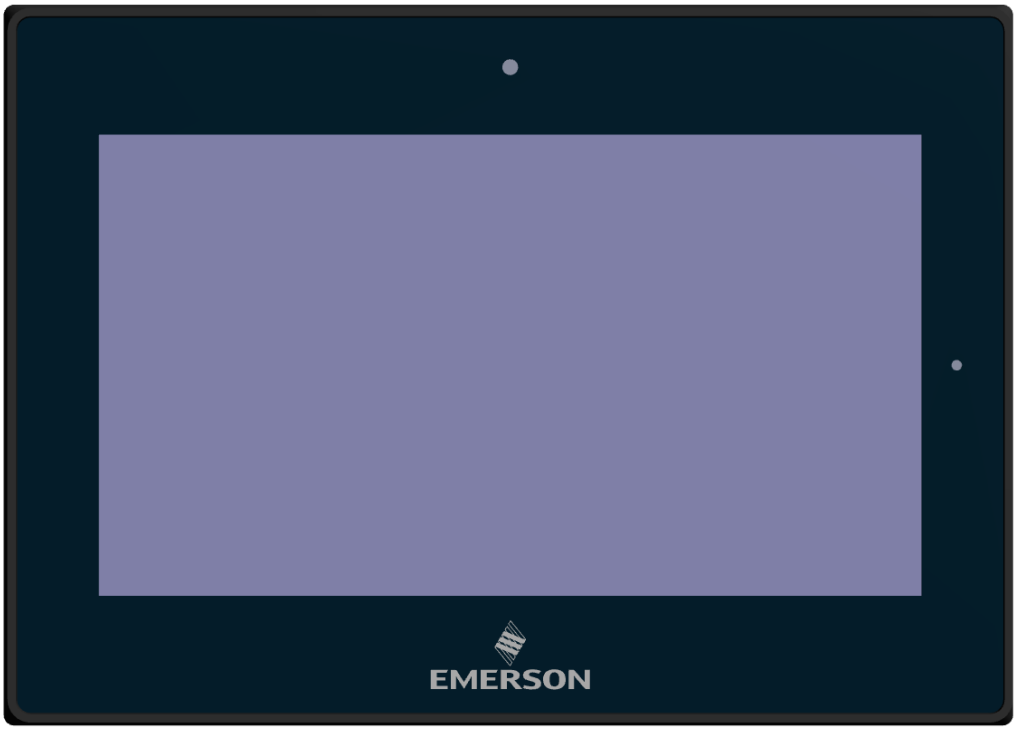
# PANEL PC

## SECURE DEPLOYMENT GUIDE




EMERSON

# 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 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.

# Contents

# Section 1: About this Guide

This document provides information that can be used to help improve the cybersecurity of systems that include the RXi– Panel PC products. It is intended for use by control engineers, integrators, IT professionals, and developers responsible for deploying and configuring PanelPC products. Secure deployment information is provided in this manual for the following PanelPC products.

Secure deployment information is provided in this manual for the following Panel PC Products.

## 1.1 Related Documents

| Document No. | Description |
|---|---|
| GFK-3071 | RXi Industrial Monitors Quick Start Guide |
| GFK-3072 | RXi Panel PC Quick Start Guide |
| GFK-3073 | RXi Web Panel Quick Start Guide |
| GFK-3138 | RXi Industrial Displays User Manual |

## 1.2 Revisions to this Manual

| Revision | Date | Description |
|---|---|---|
| B | Dec-2020 | • Added Server/Client Protocol tables<br>• Updated Related Documentation table<br>• Updated Application Layer Protocol table<br>• Updated to conform to Emerson's style guidelines.<br>• Updated Contact Us information |
| A | Jun-2019 | Initial Release |

# Section 2: Introduction

This section introduces the fundamentals of security and secure deployment.

## 2.1 Security and Security Deployment

### 2.1.1 Security

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

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

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

### 2.1.2 Firewall

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

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

### 2.1.3 Defense in Depth

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

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

### 2.1.4 General Recommendations

Adopting the following security best practices should be considered when using Emerson products and solutions.

- Deploy and configure firewalls to limit the exposure of control system networks to other networks, including internal business networks and the Internet. If a control system requires external connectivity, care must be taken to control, limit, and monitor all access, using, for example, virtual private networks (VPN) or Demilitarized Zone (DMZ) architectures.

- Harden system configurations by enabling/using the available security features, and by disabling unnecessary ports, services, functionality, and network file shares.
- Apply all of the latest Emerson product security updates, SIMs, and other recommendations.
- Apply all of the latest operating system security patches to control systems PCs.
- Use anti-virus software on control systems PCs and keep the associated anti-virus signatures up-to-date.
- Use whitelisting software on control systems PCs and keep the whitelist up-to-date.

### 2.1.5 Check List

This section provides a sample checklist to help guide the process of securely deploying Panel PC 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. (Refer to the chapter *Network Architecture & Secure Deployment*.)
5. Configure firewalls and other network security devices.
6. Enable and/or configure the appropriate security features on each Panel PC module.
7. For each Panel PC module, change every supported password to something other than its default value.
8. For each Panel PC module, assign a unique device name to that module.
9. Harden the configuration of each Panel PC module, disabling unneeded features,
10. Protocols and ports.
11. Test/ qualify the system.
12. Create an update/ maintenance plan.

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

# 2.2 Communication Protocols

This chapter describes how the supported application protocols for Ethernet and serial ports are used with Panel PC. Lower-level Ethernet protocols are not discussed here but are instead assumed to be supported when needed by the application protocol.

The security of a control system can be enhanced by limiting the protocols allowed, and the paths across which they are allowed. This can be accomplished by disabling all communication protocols that aren't needed on a particular device, and by using appropriately configured and deployed network security devices (firewalls, routers) to block any protocol (whether disabled or not) that doesn't need to pass from one network/ segment to another.

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

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. The intent should be to support only the required communications paths for the specific installation.

## 2.2.1 Supported Protocols

### Ethernet Protocols

This section indicates which Ethernet protocols are supported by the Panel PC.

Note that some of the supported protocols may not be required in a given system, since the installation may only be using a subset of the available protocols.

| Media | Protocol | Panel PC |
|---|---|---|
| Link | ARP | ✓ |
| | LLDP | ✓ |
| Internet | IPv4 | ✓ |
| | Ipv6 | ✓ |
| | ICMP | ✓ |
| | IGMP | ✓ |
| Trans | TCP | ✓ |
| | UDP | ✓ |
| Application Layer | BOOTP Client | — |
| | DCE/RPC Client | ✓ |
| | DNS Client | ✓ |
| | FTP server | ✓ |
| | HTTP server | ✓ |
| | MRP | — |
| | SNMP v1 & v2c server | ✓ |
| | SNTP client | ✓ |
| | SRTP client | ✓ |

| Media | Protocol | Panel PC |
|---|---|---|
| | SRTP server | ✓ |
| | Telnet server | ✓ |
| — | LPR /LPD & SMB | ✓ |
| — | PCL5 | ✓ |

## Serial Protocols (RS-232, RS-485)

| Protocol | Panel PC |
|---|---|
| Application-specific† | ✓ |
| ASCII Terminal | ✓ |
| Modbus RTU Slave | ✓ |
| SNP Slave | ✓ |

## USB Protocols

Panel PC supports USB based communications with the available following ports.

- 2 X USB2.0
- 1 X USB2.0

USB Protocols supported are as indicated below.

| Protocol | Panel PC |
|---|---|
| Application-specific† | ✓ |
| USB† | ✓ |
| USB To Serial‡ | ✓ |
| USB To Ethernet‡ | ✓ |
| USB to Wi-Fi‡ | ✓ |

## 2.2.2 Server

This section summarizes the available communication-centric functionality, where the communication is initiated by another PC.

| Functionality | | Required Application Protocols | Example Clients |
|---|---|---|---|
| Ethernet | View OPC Server | OPC | OPC Client |
| | EGD Consumption | Ethernet Global Data | Other controllers |
| | Process EGD Commands | Reliable Datagram Svc | Other controllers |
| | Modbus TCP Slave | Modbus TCP | HMI Other controllers third-party Masters |
| | Web Proprietary Server (TRAPI Server) | HTTP | Web browser on PC |
| | File Transfer (FTP server) | FTP | ftp.exe on PC |
| | Web Server | HTTP | — |
| | Logic OPC Server | OPC | OPC Client |
| | Print Spooler | LPR | Print |
| | TRAP and SNMP SET Requests | SNMP | SNMP Manager/NMS |
| Serial | View OPC Server | OPC (SNP/SNPX) | OPCClient (Runtime) |
| | QP+(View) | Modbus | QuickPanel+ /QP |

## 2.2.3 Client

This section summarizes the available communication-centric functionality, where the communication is initiated by the Panel PC. The servers involved in these communications are selected by the user application and/or configuration.

| | Functionality | Required Application Protocols | Example Servers |
|---|---|---|---|
| Ethernet | SRTP | SRTP | Other controllers |
| | Modbus TCP | Modbus TCP | 3rd-party device Other controllers |
| | EGD Production | Ethernet Global Data | Other controllers |
| | Send EGD Commands | Reliable Datagram Svc | Other controllers |
| | Time Synchronization | SNTP | SNTP server |
| | Lookup IP addresses by | DNS | DNS server |
| | PAC Machine Edition Historian Collector | Collector Shell/ihapi55 | Historian Server |
| | QP+ on PanelPC target | View Networking | PC |
| | Printing on PanelPC | LPR / TCP IP | Print Server on PC |
| | SNMP GET/GETNEXT | SNMP | SNMP Manager/NMS |

## 2.2.4 Ethernet Firewall Configuration

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

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

Panel PC firewall/network profile is set to public. This profile is most restrictive and secure.

Clients for Microsoft Network (The Client for Microsoft Networks is an essential networking software component for the Microsoft Windows family of operating systems. A Windows computer must run the Client for Microsoft Networks to remotely access files, printers, and other shared network resources on a Windows server). This feature is disabled in Panel PC. This can be achieved by Unchecking **Allow Remote Assistance connections to this computer** option In Ethernet Properties → Networking.

The following protocols/ drivers are disabled by default in Panel PC.

- File and Printer Sharing for Microsoft Networks
- QoS Packet Scheduler
- Microsoft Network Adapter Multiplexor Protocol
- Microsoft LLDP Protocol Driver
- Link-Layer Topology Discovery Mapper IO Driver
- Link-Layer Topology Discovery Responder
- IPv6
- Registration of IPv4 address in DNS
- NetBIOS over TCP/IP

### 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 in the following tables. Each of these lower-level protocols is required by one or more of the application protocols supported on the Panel PC.

Table 1: Link Layer Protocols

| Protocol | Ethernet Type |
|---|---|
| ARP | 0x0806 |
| LLDP | 0x88cc |

Table 2: Internet Layer Protocols

| Protocol | Ethernet Type | IP Protocol |
|---|---|---|
| IPv4 | 0x0800 | N/A |
| ICMP | | 1 |
| IGMP | | 2 |

Table 3: Transport Layer Protocols

| Protocol | Ethernet Type | IP Protocol |
|---|---|---|
| TCP | 0x0800 | 6 |
| UDP | | 17 |

## Application Layer Protocols

| Protocol | Server TCP Port | Dest UDP Port |
|---|---|---|
| DCE/RPC | — | 34964 on server<br>>1023 on client |
| DNS | 53 | 53 on server<br>>1023 on client |
| **View Runtime Server** | 12397 | — |
| **Control Runtime Server** | 12396 | — |
| **TRAPI Server** | 57176 | — |
| **View Networking** | 22739, 22740 | — |
| Control – Warm Standby | 12399 | — |
| **Ethernet Global Data** | — | 18246 |
| FTP | 21 | — |
| HTTP | 80, 8080 | — |
| **Modbus TCP** | 502 | — |
| SNTP | — | 123 |
| **SRTP** | 18245 | — |
| SNMP | 161 | 161, 162 |
| SSH | 22 | — |

### Firewall with Advanced Security

By default, all the listening ports of Windows are disabled in the firewall. Only required ports are enabled by default.

- The Internet Group Management Protocol (IGMP) is a communications protocol used by hosts and adjacent routers on IPv4 networks to establish multicast group memberships. Mostly used for online streaming video and gaming. IGMP is disabled by default in Panel PC.
- UPnP protocol is used for ease of configuration, for example, computer games running on the system can auto-configure the system firewall to let external players on the internet join in. If an attacker gains access to the system, he can use this feature to compromise the firewall settings. UPnP port 1900 is disabled in Panel PC.
- SMB protocol is used for file and printer sharing and, also as inter-process communication. Attackers exploit this feature using worms that could gain complete control of the system. SMB v1 protocol is disabled in Panel PC.
- Software restriction policy is enabled in Panel PC.

## 2.2.5 Security Capabilities

### External Storage

The Panel PC provides an SD 3.0, MMC, SDIO card slot for external storage. The cards can be used as a buffer media to transfer data. It is up to the user to decide how he wants to archive/protect the data on the SD card.

### Firmware Updates

The current mechanism to upgrade the firmware is to copy the required files into the media (USB), physically insert the media into the Panel PC, and boot from USB storage then update BIOS in DOS or UEFI.

### List Privileges

List privilege means to configure the system so that it is only capable of doing things that it is expected to do, and nothing else. In simple terminology disable all features that are not normally needed by the product.

By default, services that are not required like FTP, SSH login is disabled in Panel PC. User enables those services if it is required for user application. There will be at least one user login without administrative rights in Panel PC.

Run As Administrator feature is disabled in Panel PC, so even if an attacker gets entry with list privilege system, the user will be not able to escalate privileges of normal user to administrator. Edit registry has to be used to disable the feature.

## User Access Control (UAC)

UAC is turned to maximum security level by default in Panel PC.

## Stop/disable DCOM

It is mostly used for implementing a remote procedure call(RPC) mechanism in windows. DCOM has known vulnerabilities and can be easily exploited using tools like Metasploit.

Unless otherwise required by the application, DCOM is disabled by default in Panel PC.

Use Registry DCOMCNFG.EXE to achieve this.

## Configuration Hardening

Due to security concerns, the following servers are disabled/ enabled by default on the Panel PC device:

- FTPserver - Disabled
- HTTPserver - Disabled
- SNTP client - Enabled

## Ethernet Interface

| Interface | Availability |
|---|---|
| Bootp Client | Not Available. BIOS PXE Enable + DHCP server(third party) |
| FTP Server | Available and can be turned ON using Windows features. |
| IP Routing | Available. Use regedit.exe(IP Enable Router = 1) & services.mac(Routing and Remote Access Service) |
| DNS Client | Available. Use regedit.exe(Dnscache) |
| SNTP Client | Available. Use regedit.exe set SNTP server |
| Web Server | Available. Use Windows features to turn ON. |

## Network Devices and Features

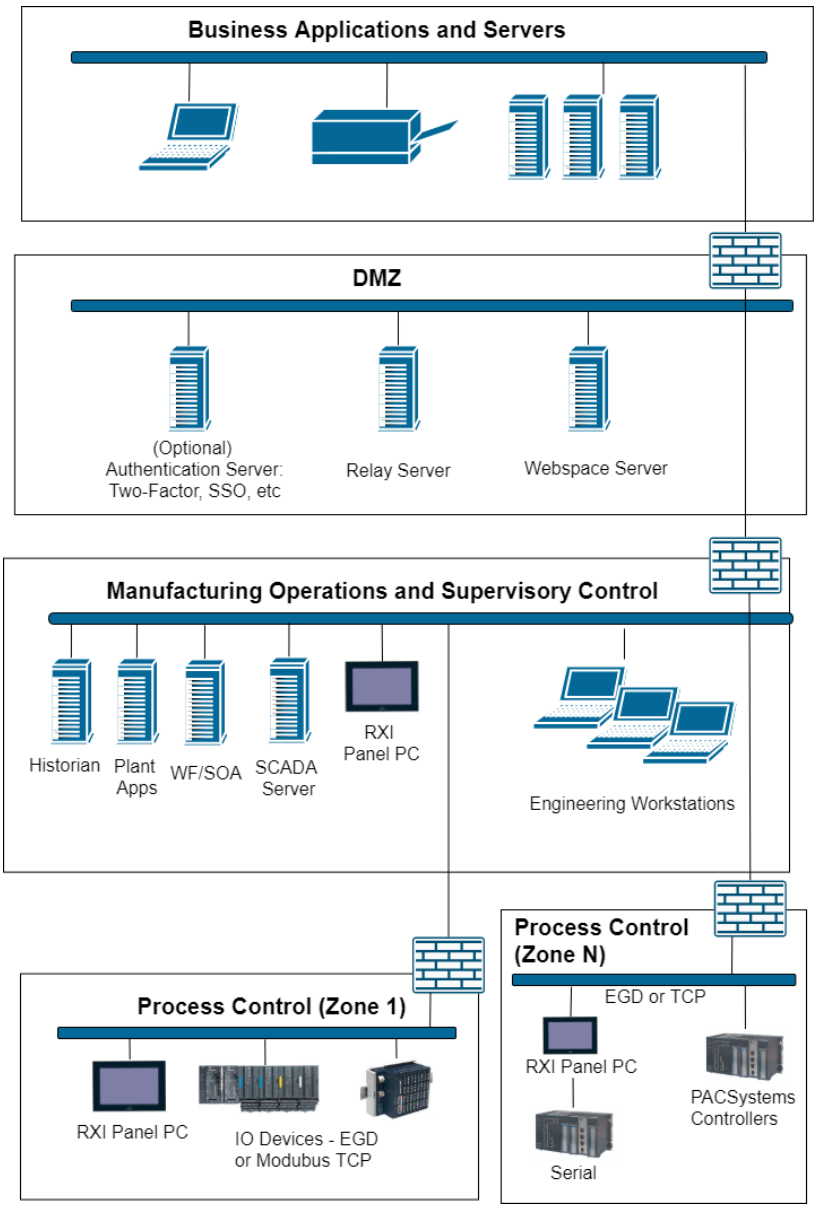
| Device/ Feature | Enable/ Disable |
|---|---|
| Remote Desktop Device Redirector Bus | Disabled. User “Device Manager” |
| Microsoft Kernel Debug Network Adapter | Disabled. bcdedit /debug off (default not show in “Device Manager”) |
| Autoplay for USB | Disabled. Use Edit Group Policy Option. |
| On Drive Access | Disabled. |
| DEP (Data Execution Prevention) | Enabled. |
| Remote Assistance | Disabled. |
| Flash/ filter ActiveX | Disabled. |

# Network Architecture & Secure Deployment

This chapter provides security recommendations for deploying RXi Panel PC in the context of a larger network.

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

**Figure 1: Network Architecture**



## Remote Access and Demilitarized Zones (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 business network and the DMZ, and between the control network and the DMZ. The business network and the control networks should ideally not communicate directly with each other.

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

## Access to Process Control Networks

Ethernet traffic from the Supervisory Control network to the Process Control networks should be restricted to support only the functionality that is required. If a particular protocol (such as Modbus TCP) doesn't need to be used between those regions, then the firewall should be configured to block that protocol. Additionally, if a controller has no other reason to use that particular protocol, then – in addition to blocking it at the firewall – the controller itself should be configured to disable support for the protocol.

Note: Network Address Translation (NAT) firewalls typically do not expose all of the devices on the trusted side of the firewall to devices on the untrusted side of the firewall. Further, NAT firewalls rely on mapping the IP address/port on the trusted side of the firewall to a different IP address/port on the untrusted side of the firewall.

## 2.2.6 Optional Security Features

### UEFI Security boot

BIOS password will be enabled as default to prevent the execution of the bootloader/ operation system which is not trusted by Emerson. Once it is enabled, then the Security boot cannot be disabled.

Use TPM Function (Trusted Computing -> Security Device Support = Enable(Default)) & OS TPM Setting (TPM.MSC) to use Trusted Platform Module (TPM) to store keys used in the system for security.

## 2.2.7 Other Considerations

### Patch Management

A strategy for applying security fixes, including patches, firmware updates, and configuration changes, should be included in a facility's security plan. Applying these updates will often require that an affected Panel PC services be taken to out of service.

Finally, 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.

### Real-time Communication

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

### TCP SYN Storm Denial of Service

To establish a TCP connection between a source host and destination host, a handshake sequence must occur. First, the source hosts end an SYN packet to the destination host. If the destination host is listening for the SYN packet, it will respond with an SYN/ACK packet. The source host then acknowledges with an ACK packet and the connection between source host and destination host is established.

During the response of the SYN/ACK from the destination host (Panel PC in this case), a block of memory is setup to contain the data of the established connection. If for some reason an ACK is never received from the source host, a timeout occurs, and the block of memory winds up being allocated but unused. This behavior can be used in a well-known attack against TCP implementations, known as a TCPSYN Storm. In a TCP SYN Storm, the attacker will continually send a SYN packet to a destination host, without sending an ACK. If not properly mitigated, this can

eventually consume all the memory on the destination host that is used to manage legitimate connections, resulting in a denial of service on the destination host.

TCP SYN Storm attacks can be detected and mitigated by monitoring source host SYN packets that do not have accompanying source host ACK response packets. Most mid-range to high-end firewalls today have this capability and should be used to mitigate the effects of TCP SYN Storm Denial of service attacks that originate from devices in a less-trusted security zone/network.

### Gratuitous ARP

The purpose of an ARP (Address Resolution Protocol) request is to associate an IP address with a physical address (MAC). A host can obtain a physical address by broadcasting an ARP request on the TCP/IP network. This is a required capability when using IPv4 communication on a Panel PC device.

The ARP protocol also allows hosts to broadcast unsolicited ARP replies, which is known as Gratuitous ARP (GARP). There is generally no need for Gratuitous ARP and there are well-known attacks (such as man-in-the-middle) that rely on it. An Ethernet switch that blocks gratuitous ARP packets can help mitigate ARP-based attacks.

## 2.2.8 Additional Guidance

### 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.

### Government Agencies and Standards Organizations

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

# General Contact Information

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

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

# Technical Support

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

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

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

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

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

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

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

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

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



EMERSON