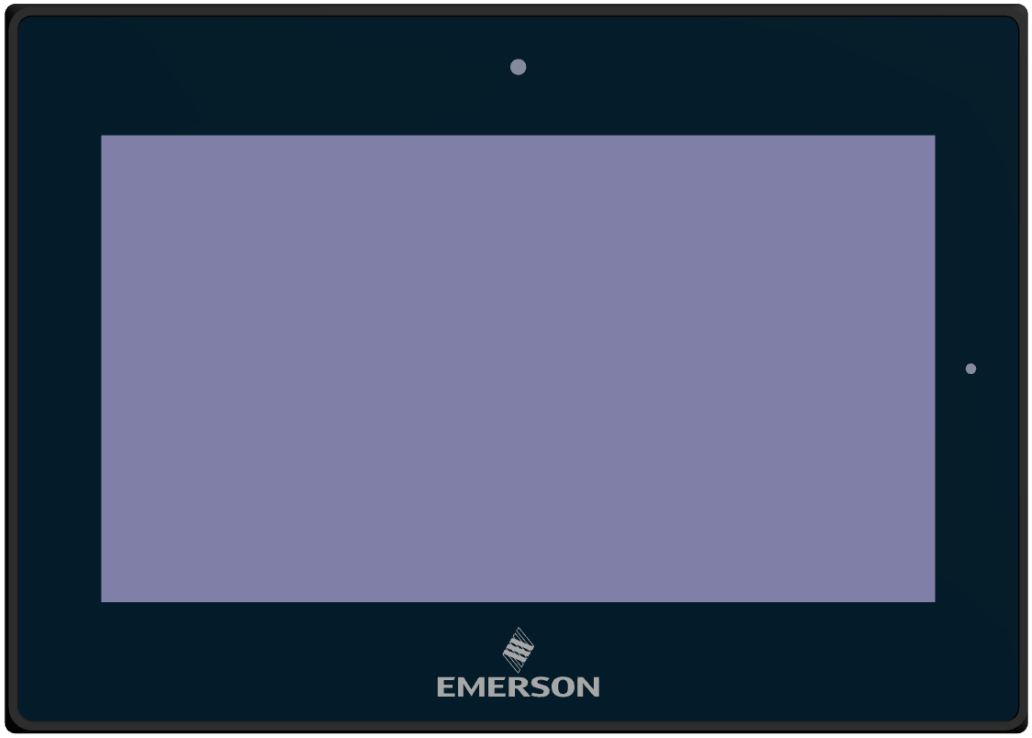
GFK-3076A
June 2019

Web Panel

SECURE DEPLOYMENT GUIDE



EMERSON

WARNINGS, CAUTIONS AND 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.

Attention

Indicates a procedure, condition, or statement that should be strictly followed to improve these applications.

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

This document is based on information available at the time of its publication. While efforts have been made to be accurate, the information contained herein does not purport to cover all details or variations in hardware or software, nor to provide for every possible contingency in connection with installation, operation, or maintenance. Features may be described herein which are not present in all hardware and software systems. Intelligent Platforms, LLC assumes no obligation of notice to holders of this document with respect to changes subsequently made.

Intelligent Platforms, LLC makes no representation or warranty, expressed, implied, or statutory with respect to, and assumes no responsibility for the accuracy, completeness, sufficiency, or usefulness of the information contained herein. No warranties of merchantability or fitness for purpose shall apply.

About this Guide

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

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

Product	Catalog Number	Product Description
7” RXi – Web Panel	IC757CSW07WHMI	Web Panel 7” Wide Screen
10” RXi – Web Panel	IC757CSS10WHMI	Web Panel 10” Standard
12” RXi – Web Panel	IC757CSS12WHMI	Web Panel 12” Standard
15” RXi - Web Panel	IC757CSS15WHMI	Web Panel 15” Standard
19” RXi – Web Panel	IC757CSS19WHMI	Web Panel 19” Wide Screen
24” RXi – Web Panel	IC757CSS24WHMI	Web Panel 24” Wide Screen

Related Documents

Document No.	Description
SR_XXXX	Web Panel SecurityRequirements_AIS

Revisions to this Manual

Revision	Date	Description

Introduction

This section introduces the fundamentals of security and secure deployment.

Security and Security Deployment

Security

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

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

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

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, Intelligent Platforms LLC recommends taking a “Defense in Depth” approach to security.

Defense in Depth

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

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

General Recommendations

Adopting the following security best practices should be considered when using Intelligent Platforms LLC 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 GE Intelligent Platforms 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.

Check List

This section provides a sample check list to help guide the process of securely deploying Web Panel 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 Web Panel module.
7. For each Web Panel module, change every supported password to something other than its default value.
8. For each Web Panel module, assign a unique device name to that module.
9. Harden the configuration of each Web Panel module, disabling unneeded features, Protocols and ports.
10. Test/ qualify the system.
11. 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.*

Notes

Communication Protocols

This chapter describes how the supported application protocols for Ethernet and serial ports are used with Web Panel. 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.

Intelligent Platforms, LLC 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.

Supported Protocols

Ethernet Protocols

This section indicates which Ethernet protocols are supported by the Web Panel.
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	Web Panel
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	—
	SRTP server	—
	Telnet server	✓
—	LPR /LPD & SMB	—

Media	Protocol	Web Panel
—	PCL5	—

Serial Protocols (RS-232, RS-485)

Protocol	Web Panel
Application-specific†	—
ASCII Terminal	—
Modbus RTU Slave	—
SNP Slave	—

USB Protocols

Web Panel 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	Web Panel
Application-specific†	—
USB†	—
USB To Serial‡	—
USB To Ethernet‡	—
USB to Wi-Fi‡	—

Server

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

Functionality		Required Application Protocols	Example Clients
Ethernet			
Serial			

Client

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

Functionality		Required Application Protocols	Example Servers
Ethernet			

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, in order to support only the required communications paths for any particular installation.

All unused networking ports other than HTTP, HTTPS, SSH will be disabled.

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 Web Panel.

Link Layer Protocols

Protocol	Ethernet Type
ARP	0x0806
LLDP	0x88cc

Internet Layer Protocols

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

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 >1023 on client
DNS	53	53 on server >1023 on client
Control – Warm Standby	12399	—
FTP	—	—
HTTP	80	—
HTTPS	443	—
SNMP	—	—
SSH	22	—

Security Capabilities

External Storage

The Web Panel provides an SD 3.0, MMC, SDIO cards lot 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 SD card, physically insert the media into the Web Panel, and boot from SD storages.

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, FTP service is disabled in Web Panel where as SSH service is enabled for the user to login and look to the log files.

Note: The web Panel only acts as user interface display rendering device, the user activities are done and controlled by web servers, so the critical system logo should be put on the web servers, not on Web Panel.

User Access Control (UAC)

Web Panel will provide list privileges to all the files and directory in the system to make sure not all the files and directories are readable/writable/executable by everyone.

Web Panel will make sure files that are readable, writable, and executable only by root user should be owned and group-owned by root. The file system only can be modified by root user, and the browser only has none-root user access right.

Web Panel will use appropriate security options like nosuid, nodev, noexec, ro while mounting the filesystem.

The chromium web browser in Web Panel will run under normal user privilege.

Configuration Hardening

Server Default States

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

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

Ethernet Interface

Interface	Availability
Bootp Client	Not Available
FTP Server	Not Available
IP Routing	Available
DNS Client	Available
SNTP Client	Available. On console key-in “systemctl stop ntpdate.service”
Web Server	Not Available.

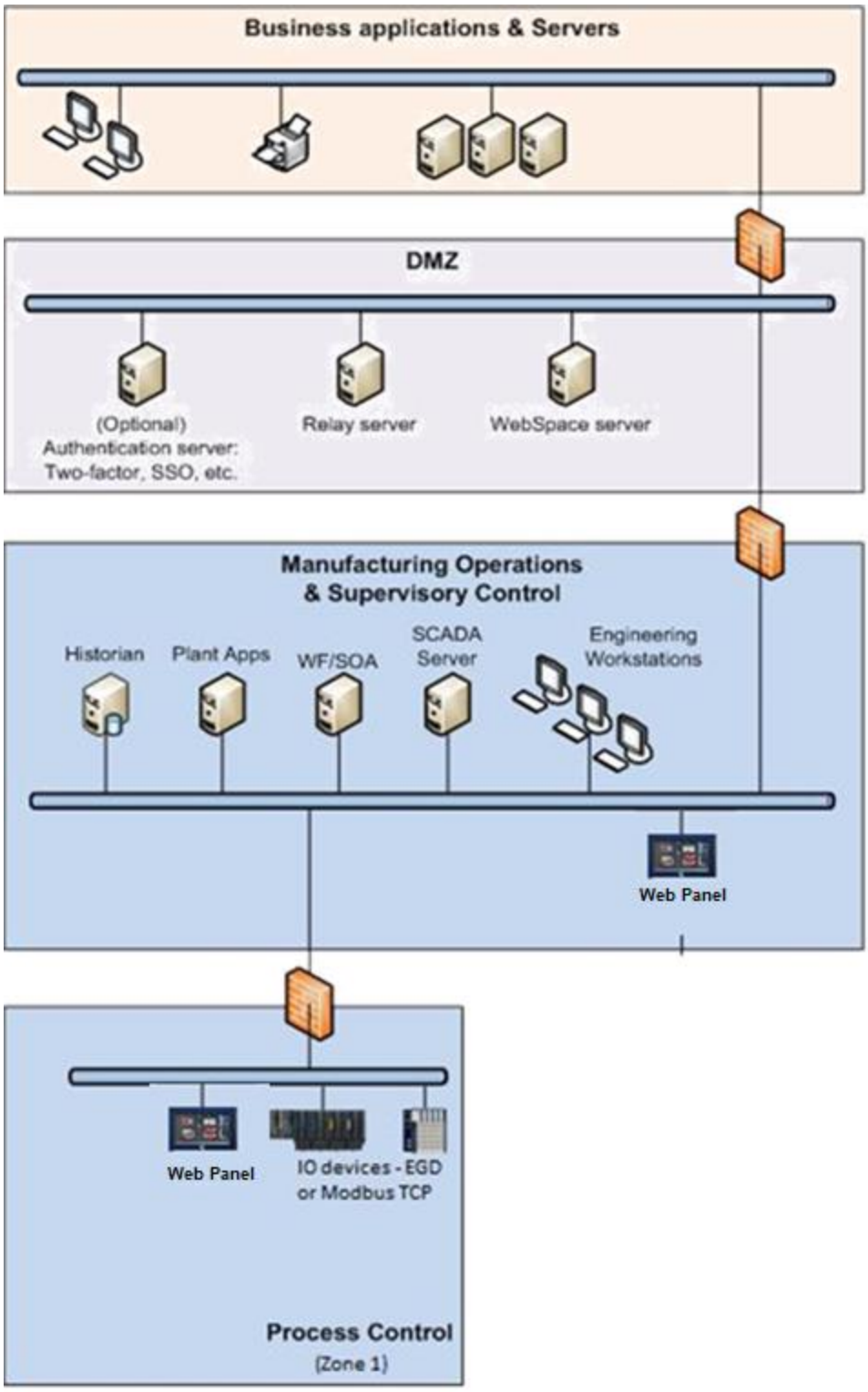
Device/ Web Configuration

Device/ Web browser	Enabled/ disabled
Access to physical memory via /dev/mem and /dev/kmem	Disabled. Web Panel Application doesn’t have root access rights.
Web browser plug-ins	No plug-in available in Chromium web browser.
Web browser extensions	Except the following, browser won’t allow to add more extensions, • LAN port IP setting • LCD backlight adjustment setting
Web browser security configuration	Only HTTPS protocol configuration Enabled.
SD-Card/USB configuration	Only HID keyboard and mouse devices can be detected and used on USB port, the USB host port for embedded Linux system is without autoplay/autorun capability.

Network Architecture & Secure Deployment

This chapter provides security recommendations for deploying Web Panel 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.



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, 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.

Notes

Optional Security Features

Security boot

Secure boot will be enabled and cannot be disabled once the OTP (one-time program) fuse been burned to prevent malicious attacker for running compromised bootloader/ operation. The system only can be booted with the image been signed by the keys of security boot, the keys is programmed in hardware OTP fuses, which cannot be modified.

TPM (Trusted Platform Module) interface is only available for x86 systems, not on ARM systems, the TPM module works with LPC (Low pin count) hardware interface, which is only available on x86 CPU.

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 Web Panel services to be taken to out of service.

Finally, some installations require extensive qualification 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 a SYN packet to the destination host. If the destination host is listening for the SYN packet, it will respond with a 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 (Web Panel 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 Web Panel 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.

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

Contact Information:

North & South America
18703 GH Circle
PO Box 508
Waller, Texas 77484
USA
T +1 281 727 5300

2500 Park Avenue West
Mansfield, Ohio 44906
USA
T +1 419 529 4311

9009 King Palm Drive
Tampa , Florida 33619
USA
T +1 813 630 2255

4112-91A Street
Edmonton, Alberta T6E5V2
Canada
T +1 780 450 3600

Av. Hollingsworth,325
Iporanga
Sorocaba, SP 18087-105
Brazil
T +55 15 3238 3788

Europe
Asveldweg 11
7556 BT Hengelo(O)
The Netherlands
T +31 74 256 1010

Siemensring 112
D-47877 Willich
Germany
T +49 2154 499 660

30/36 Allee du Plateau
93250 Villemomble
France
T +331 48 122610

6 Bracken Hill
South West Industrial Estate
Peterlee, Co Durham
SR82LS, United Kingdom
T +44 191 518 0020

3 Furze Court
114 Wickham Road
Fareham, Hampshire
PO167SH ,United Kingdom
T +44 132 984 8900

Via Montello 71/73
20038 Seregno
Italy
T +39 0362 2285207

Selska cesta 93
10000 Zagreb
Croatia
T +385 913654292

ul. Konstruktorska str 11A
02-673 Warsaw
Poland
T +48 22 4589237

Hungári körút 166-168
H-1146 Budapest
Hungary
T +36 14624034

Hajkova 2747/22
130 00 Praha 3
Czech Republic
T +42 2 81002666

Zelezniciarska 13
811 04 Bratislava
Slovakia
T +42 1252442071

Blegistrasse 21,
P.O. Box 1046
CH 6341 Baar
Switzerland
T +41 (41) 7686215

2-4, Gara Herastrau St.
District 2, Nova Building,
5th floor 020334 Bucharest
Romania
T +40 212062506

Icerenkoy MAh. Topcu Ibrahim Sk.
No:13 K:4 Icerenkoy
Istanbul, Turkey
T +90 2165739848408

Middle East & Africa
2 Monteer Road, Isando
Kempton Park, 1600
South Africa
T +27 11 974 3336

PO Box 17033
Jebel Ali Free Zone
Dubai,
United Arab Emirates
T +971 4883 5235

Asia Pacific
19, Kian Teck Crescent,
Singapore 628885
T +65 6501 4600

471 Mountain Highway
Bayswater, Victoria 3153
Australia
T +61 3 9721 0200

9/F Gateway Building
No.10 Ya Bao Road
Chaoyang District
Beijing, P.R. China
T +86 10 5821 1188

No 15 Xing Wang Road
Wuqing Development Area
Tianjin 301700
P.R. China
T +86 22 8212 3300

Lot 13112, Mukim Labu,
Kawasan Perindustrian Nilai
71807 Nilai, Negeri Sembilan
Malaysia
T +60 6 799 2323

Delphi B Wing, 601 & 602
6th Floor, Central Avenue
Powai, Mumbai 400076
India
T +91 22 6662 0566

NOF Shinagawa Konan Building
1-2-5, Higashi-shinagawa
Shinagawa-Ku, Tokyo
140-0002 Japan
T +81 3 5769 6873

Please visit our website for up to date product data.

www.Emerson.com

EMERSON™