GE
Intelligent Platforms

Operator Interface Products

QuickPanel+

Operator Interface

Secure Deployment Guide, GFK-2897

January 2014

GFL-002

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.

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. GE Intelligent Platforms assumes no obligation of notice to holders of this document with respect to changes subsequently made.

GE Intelligent Platforms 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.

* indicates a trademark of GE Intelligent Platforms, Inc. and/or its affiliates. All other trademarks are the property of their respective owners.

Contact Information

If you purchased this product through an Authorized Channel Partner, please contact the seller directly.

General Contact Information

Online technical support and GlobalCare	http://www.ge-ip.com/support
Additional information	http://www.ge-ip.com/
Solution Provider	solutionprovider.ip@ge.com

Technical Support

If you have technical problems that cannot be resolved with the information in this guide, please contact us by telephone or email, or on the web at www.ge-ip.com/support

Americas

Online Technical Support	www.ge-ip.com/support
Phone	1-800-433-2682
International Americas Direct Dial	1-780-420-2010 (if toll free 800 option is unavailable)
Technical Support Email	support.ip@ge.com
Customer Care Email	customercare.ip@ge.com
Primary language of support	English

Europe, the Middle East, and Africa

Online Technical Support	www.ge-ip.com/support
Phone	+800-1-433-2682
EMEA Direct Dial	+420-23-901-5850 (if toll free 800 option is unavailable or if dialing from a mobile telephone)
Technical Support Email	support.emea.ip@ge.com
Customer Care Email	customercare.emea.ip@ge.com
Primary languages of support	English, French, German, Italian, Czech, Spanish

Asia Pacific

Online Technical Support	www.ge-ip.com/support
Phone	+86-400-820-8208
	+86-21-3217-4826 (India, Indonesia, and Pakistan)
Technical Support Email	support.cn.ip@ge.com (China)
	support.jp.ip@ge.com (Japan)
	support.in.ip@ge.com (remaining Asia customers)
Customer Care Email	customercare.apo.ip@ge.com
	customercare.cn.ip@ge.com (China)

Contents

1 About this Guide

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

Secure deployment information is provided in this manual for the following QuickPanel+ products.

Family	Catalog Number	Description
QuickPanel+	IC755CSW07CDA	QuickPanel+ View & Control, 7" Color TFT Widescreen with Multi-touch Projected Capacitive Screen, GE Monogram Bezel, 24 VDC Powered

2 Introduction

This section introduces the fundamentals of security and secure deployment.

2.1 What is Security?

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

- Confidentiality: Ensure only the people you want to see 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.

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

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, GE Intelligent Platforms recommends taking a "Defense in Depth" approach to security.

2.3 What is Defense in Depth?

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

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

2.4 General recommendations

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

2.5 Checklist

This section provides a sample checklist to help guide the process of securely deploying QuickPanel+ 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. (See section 3, *Network Architecture & Secure Deployment*.)
5. Configure firewalls & other network security devices
6. Enable and/or configure the appropriate security features on each QuickPanel+ module.
7. On each QuickPanel+ module, change every supported password to something other than its default value.
8. Harden the configuration of each QuickPanel+ module, disabling unneeded features, protocols and ports.
9. Test / qualify the system.
10. Create an update/maintenance plan.

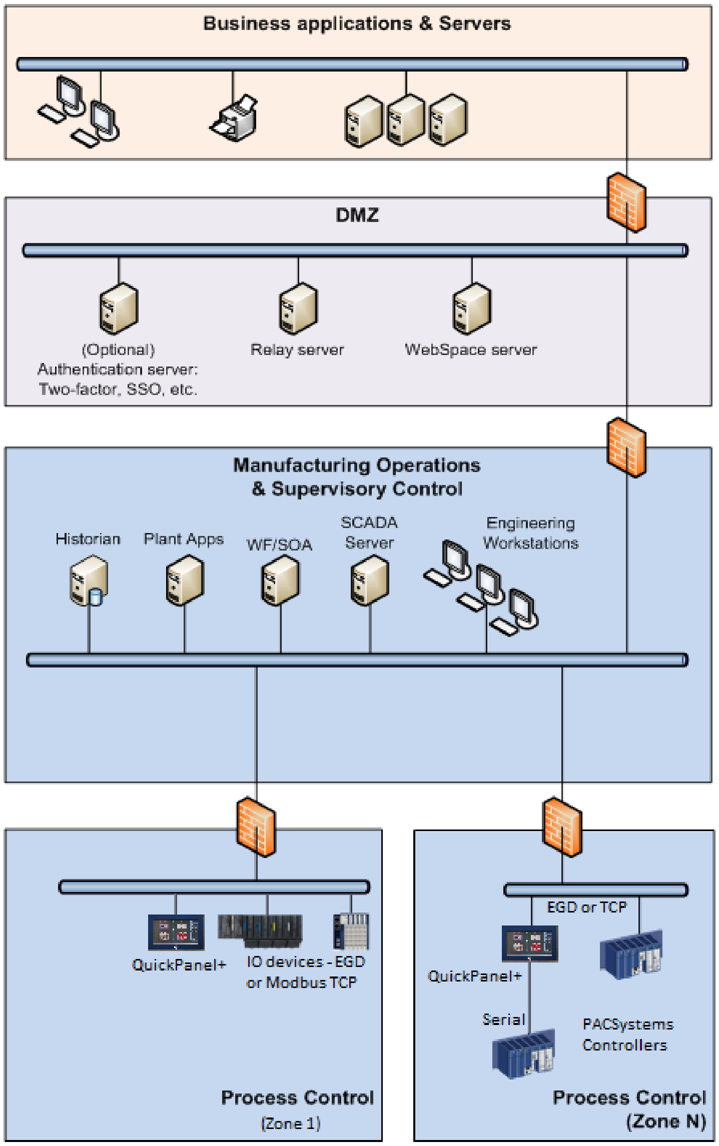
Note: Secure deployment is only one part of a robust security program. This document, including the checklist above, is limited to only providing secure deployment guidance. For more information about security programs in general, see section 4.5, *Additional Guidance*.

3 Network Architecture & Secure Deployment

This section provides security recommendations for deploying QuickPanel+ controllers in the context of a larger network.

3.1 Reference Architecture

The figure below shows a reference deployment of QuickPanel+ components.



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.

3.2 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.

3.3 Access to Process Control networks

Ethernet traffic from the Supervisory Control network to the Process Control networks should be restricted to support only the functionality that is required. If a particular protocol (such as Modbus TCP) doesn't need to be used between those regions, then the firewall should be configured to block that protocol. If, in addition to that, a controller doesn't have some other reason it needs to use that 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. Since communication to QuickPanel+ controllers will typically be initiated from a PC on the "untrusted" side of the Process Control network firewall, protecting a Process Control network using a NAT firewall may cause additional communication challenges. Before deploying NAT, carefully consider its impact on the required communications paths.

4 Other Considerations

4.1 Patch Management

A strategy for applying security fixes, including patches, firmware updates, and configuration changes, should be included in a facility's security plan. Applying these updates will often require that an affected QuickPanel+ controller be temporarily taken 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.

4.2 Real-time Communication

When designing the network architecture, it is important to understand what impact the network protection devices (such as firewalls) will have on the real-time characteristics of the communications traffic that must pass through them. In particular, the PROFINET IO, Ethernet Global Data, and 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.

4.3 TCP SYN Storm Denial of Service

In order to establish a TCP connection between a source host and destination host, a handshake sequence must occur. First, the source host sends 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, a block of memory is set up to hold the data of the established connection. If for some reason an ACK never comes back from the source host, a timeout occurs and the block of memory is allocated but unused. This behavior can be used in a well-known attack against TCP implementations, known as a TCP SYN 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.

4.4 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 QuickPanel+ 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.

4.5 Additional Guidance

4.5.1 Protocol-specific Guidance

Protocol standards bodies may publish guidance on how to securely deploy and use their protocols. Such documentation, when available, should be considered in addition to this document.

4.5.2 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 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 & operating a cyber-security program, including recommended technologies for industrial automation and control systems.

5 Related Documents

QuickPanel+ Operator Interface User's Manual, GFK-2847

QuickPanel+ Operator Interface Quick Start Guide, GFK-2893

GE Intelligent Platforms Information Centers

Headquarters:
1-800-433-2682 or 1-434-978-5100

Global regional phone numbers
are available on our web site
www.ge-ip.com

Additional Resources

For more information, please visit the GE Intelligent Platforms web site:

www.ge-ip.com