Frick Quantum HD Unity Hardening Requirements

GPS0053-CE-EN
Version 1.0
Rev A
Revised 2024-07-26

Johnson Controls

Introduction

Our practices provide peace of mind to our customers with a holistic cyber mind set beginning at initial project design concept, and is supported through deployment, including a rapid incident response to meet comprehensive and evolving cybersecurity environments.

This hardening document intends to provide cybersecurity requirements for the Frick Quantum HD Unity Control Panel for configuration and upgrade management.

As cybersecurity threats affect all connected devices, it is important to ensure that cybersecurity is considered throughout the planning, deployment and maintenance phases associated with a solution’s functional operation.

Legal disclaimer

The cybersecurity practices described in this guide are recommended practices to facilitate the secure installation and configuration of the products described herein. However, Johnson Controls cannot guarantee that the implementation of the cybersecurity practices or recommendations described in this guide will ensure the security of the relevant product or system, or prevent, or alter the potential impact of, any unauthorized access or damage caused by a cybersecurity incident. This guide is provided “as is”, and Johnson Controls makes no representation or warranty, expressed or implied, as to the efficacy of the cybersecurity practices or recommendations described within. Johnson Controls disclaims all liability for any damages that may occur because of, or despite, reliance on this guide or compliance with any cybersecurity practices or recommendations set forth herein.

Contents

1 Planning

This section helps plan for the implementation of security requirements for Frick Quantum HD Unity control panels.

1.1.0 Internet connectivity

Internet access increases your cybersecurity footprint and attack area which requires additional hardening steps. The hardening steps in section 2 must be taken to limit external access.

1.2.0 Hardening methodology

While most products provide onboard security safeguards, including secure-by-default settings, we recommend that the device is hardened according to the guidance outlined in section 2.

Generally, you should aim for a defense-in-depth strategy employing standard IT hardening methods and compensating controls as needed to be compliment with the base security features of each product.

2 Deployment

This section is designed to harden your attack surface before the new or upgraded system is turned over to runtime operations. Security hardening begins with careful planning prior to deployment.

2.1.0 Hardening

While many products include secure-by-default safeguards, additional hardening is usually required to meet the security requirements of the target environment. It is important to apply the correct level of protection as warranted by customer policies and other applicable regulations that may govern the application security settings for this deployment.

2.2.0 Hardening checklist

This checklist provides a list of hardening steps you may choose to go through. The actual steps you will take are based on the features required for your specific products and application environment.

To harden this product, complete the following tasks:

- ☐ Hardening Step 1: Disable unused network ports
- ☐ Hardening Step 2: Equipment network isolation
- ☐ Hardening Step 3: Software upgrades
- ☐ Hardening Step 4: Manage pin numbers

2.3.0 Configure network ports

Quantum HD Unity panels often communicate over Ethernet networks, but the type of communication will depend on the software features that are used. Use a network firewall to allow only approved communication. Below are steps to limit network traffic to just the services that are needed.

Hardening Step 1: Disable unused network ports

To decide what ports to open refer to the table below. Block all unused ports. For example, if you no longer need to use Modbus TCP and are not using port 502 for any other use, block port 502. NOTE: Before blocking ports, consult your Frick Factor and IT department.

Table 2.3.1

Network Port	Protocol	Int / Ext	Feature	Description
80	TCP	Internal	HTTP	Web browser HMI WebSockets
465, 587, or user configurable	TCP	External	Email	Email notification
502	TCP	Internal	Modbus	Used for Modbus messaging
44818	TCP	Internal	Allen-Bradley EtherNet/IP	Used for Rockwell Allen-Bradley messaging

2.4.0 Isolated internet

Connecting any system to the internet always increases cybersecurity risk. To harden your system, it is recommended that you do not connect the Quantum HD Unity panel directly to the internet.

However, features such as email or remote monitoring will require an internet connection. If remote monitoring connections are used outside the local network, they should be through a VPN or other secure remote connection.

Hardening Step 2: Equipment network isolation

Quantum HD Unity panels should communicate on a dedicated internal Ethernet equipment network that is isolated from other Ethernet networks and Internet connections. If connections to external networks are required, use a network firewall to only allow communication for specific services.

2.5.0 Apply upgrades

It is best practice to apply the most current software upgrades. These upgrades can include cybersecurity improvements as well as feature additions and other software improvements. Review the release notes and prioritize the benefits of the update. The overall benefit should include the improved protection that will lower the cybersecurity risk.

Hardening Step 3: Software upgrades

Review the Quantum HD Unity product page on the frickcontrols.com website for the latest software and upgrade procedure at the following link - https://frickcontrols.com/quantum-hd-unity-q6

2.6.0 Managing pin numbers

Pin numbers are used to control the level of access granted to users of the control panel. There are three levels of access that may be granted. Always grant access with the principle of Least Privilege. In general, this means:

- Only the minimum necessary rights should be assigned to a user that requests access
- Access rights should be in effect for the shortest duration necessary

Hardening Step 4: Manage pin numbers

Pin numbers should be reviewed and changed when specific events occur. For example:

- When new personnel need to access the control panel
- When personnel are no longer employed by the organization
- When personnel have changed roles, and have either increased or decreased responsibilities

During these events, immediately update the pin number. This ensures that people with the appropriate roles can access the panels with the correct privileges.