Fire Panel Hardening Guide

GPS0056-CE-EN
Version 1.0
Rev B
Revised 2024-11-01

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 used in planning, deployment, and maintenance periods for Fire Panels.

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.

This guide provides hardening requirements for configuration and maintenance. It is broken down into three main sections depicting the overall process for hardening:

1. Planning	2. Deployment	3. Maintain
Provides an introduction, general knowledge, and overall guidance for you to prepare your system for security and hardening	Guides you through the execution and hardening steps based on the products and security features of the target system components	Provides a checklist for future checkpoints to keep your system safe and secure

Appendixes are included at the end for certification, additional Fire Panel literature, and acronyms used within this document.

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.

Table of Contents

1 Planning

This section helps plan for the implementation of security requirements for the Fire Panel solution.

1.1 Fire Panel solution overview

Fire Detection and Control Panels provide extensive installation, operator, and service features with point and module capacities suitable for a wide range of system applications. An on-board Ethernet port provides fast external system communications to expedite installation and service activity. A wide variety of functional modules are available to meet specific system requirements. Selections allow panels to be configured for either Stand-Alone or Networked fire control operation.

1.1.1 Deployment architecture

Johnson Controls Fire Panel solutions are comprised of several components to provide options for wired communications within the building, cellular communication and to cloud services which provide analytics and remote access for monitoring.

Over the next few pages, we will cover the common use cases for Fire Panels as shown in the table below:

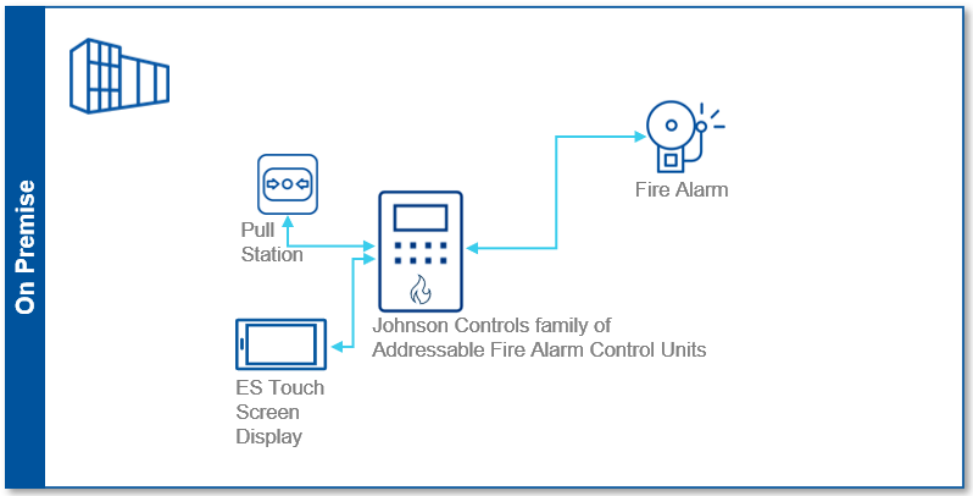
Use Case	Fire Panel Connection	Recommended usage*
1	Standalone	Simple installation with ES Touch screen display (TSD)
2	Connected	Remote connection to the panel
3	Networked	High-rise or multiple buildings
4	Networked over CNB**	Connecting 2 or more distinct fire networks
5	Central Station monitoring	24x7x365 monitoring

**These map to points (College campus or Hotel or High Rise/ Gov't Bldg./Sports Arena/Geographical areas [network])*
*** CNB = Customer Network Bridge*

Use Case 1

Use case 1 reflects a simple installation scenario using a standalone fire panel.

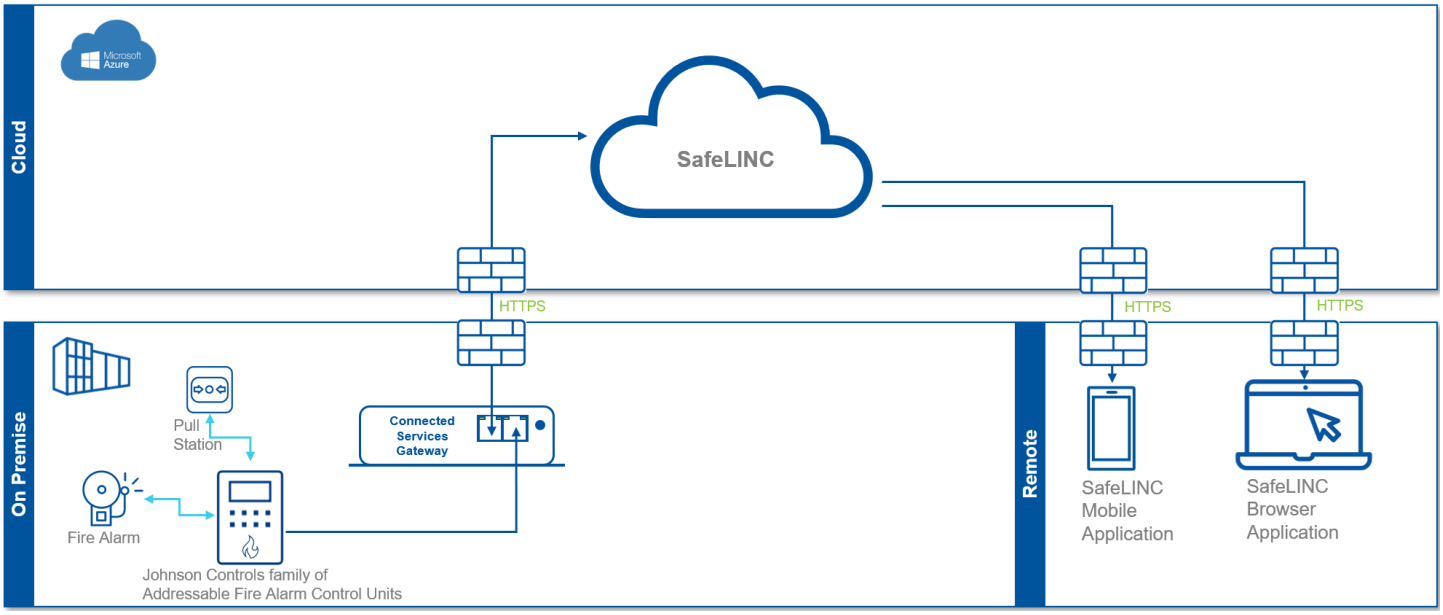
Figure 1.1.1.1: Standalone Fire Panel architecture



Use Case 2

Use case 2 reflects a scenario with a remote connection to the fire panel.

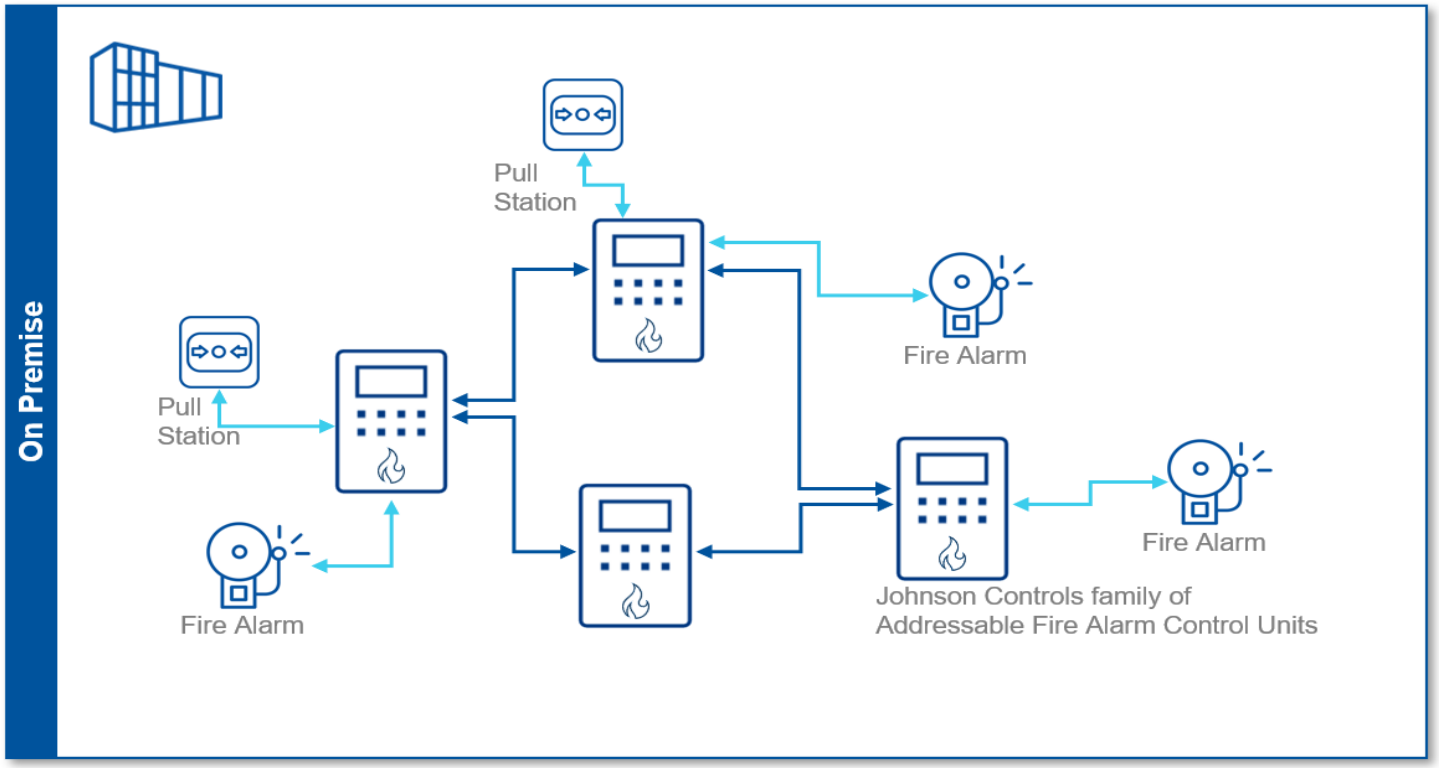
Figure 1.1.1.2: Connected Fire Panel architecture



Use Case 3

Use case 3 reflects a high-rise or multiple building scenario where multiple fire panels are interconnected.

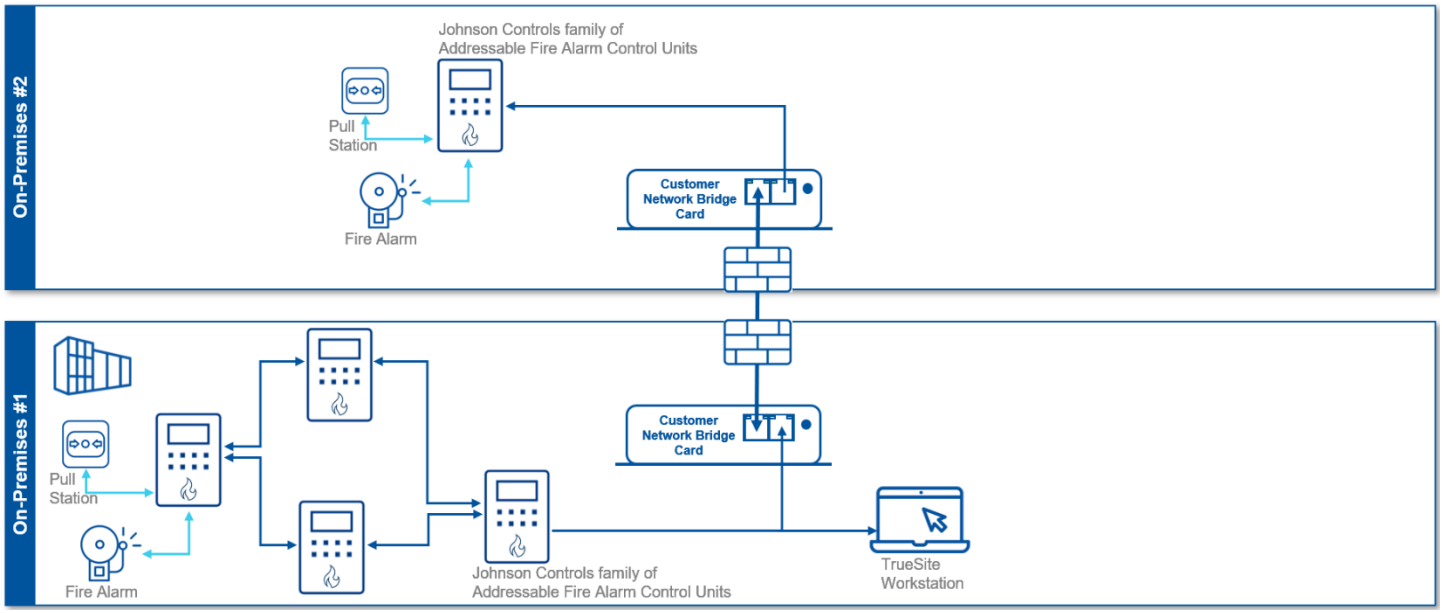
Figure 1.1.1.3: Networked Fire Panel architecture



Use Case 4

Use case 4 reflects a scenario where two end-user buildings are connecting their fire systems together using Customer Network Bridge, allowing for easier fire system monitoring without introducing cloud-based technologies

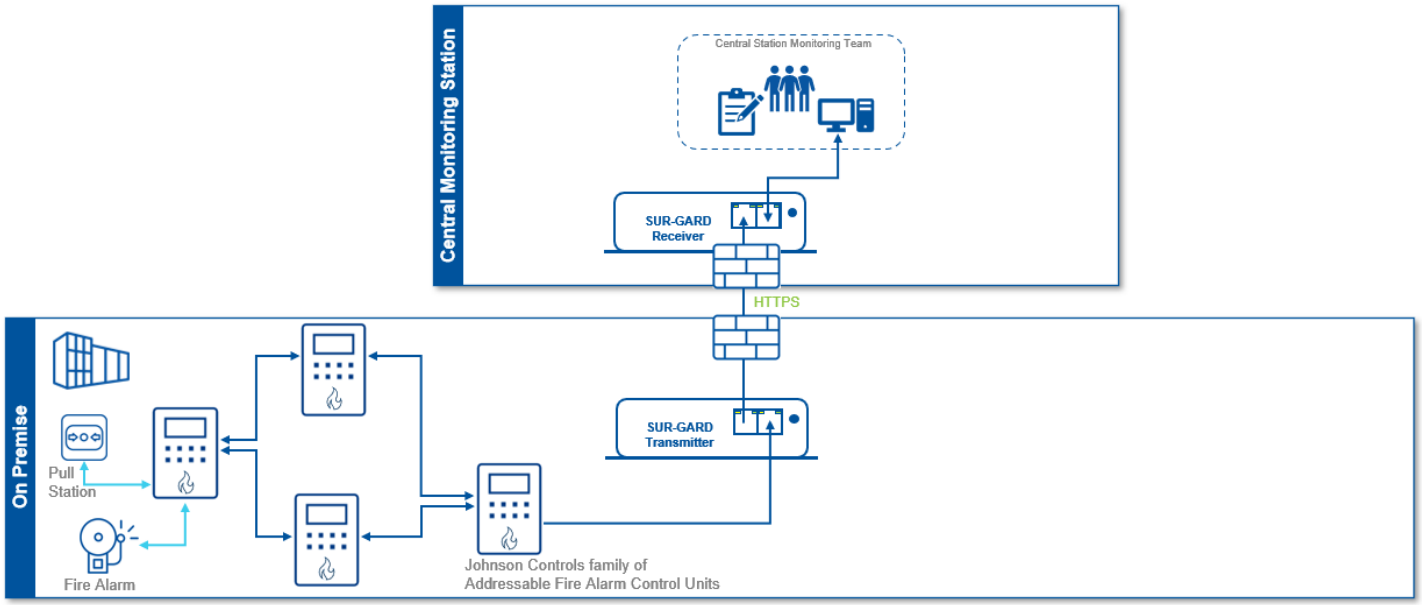
Figure 1.1.1.4: Connected and Networked Fire Panel architecture



Use Case 5

Use case 5 reflects a scenario where multiple fire panels are connected to a central monitoring service.

Figure 1.1.1.5: Central Station monitoring Connected and Networked Fire Panel architecture



1.1.2 Components

Fire Panel solutions consist of the following on premises components:

Fire Panels

Johnson Controls offers different fire alarm control panels with varying features such as audio, visual indication of alarms, priority 2 / CO, troubles, and supervisory conditions. All Johnson Controls fire panels are:

- Intelligent - Next-generation technology that's robust and cost-effective
- Flexible - Easy to install, configure, and expand
- Intuitive - A variety of programming options for fast setup and maintenance

Customers customize their solution by selecting **conventional** or **addressable** panels with the features they require. **Conventional** panels are easy to install, configurable, cost-effective, and meet a variety of customer and building needs. **Addressable** panels can pinpoint the source of a fire, alert, trouble, or other system event while offering a modular design and an intuitive interface.

Example panels are shown below in Table 1.1.2.1.

Table 1.1.2.1 Example Fire alarm control panels (not all inclusive)

Model	Type[1]	Overview	Recommended use
4004R	CONV	A programmable hazard-releasing panel in a compact, cost-effective package. Smart dual-condition design helps prevent accidental discharge.	Ideal for small facilities
4006, 4008	CONV	A conventional control panel Easy installation and configuration Has a built-in DACT to easily connect to a central monitoring facility.	Ideal for small facilities with straightforward fire protection needs
4007ES	ADDR	A small facility control panel with the features and benefits of addressability. Easy color touch screen interface. USB port for transferring panel information, and other functions.	Smaller version of the 4017ES recommend for small installations. Networkable with 4100ES and 4010ES control panels
4010ES	ADDR	An addressable control panel that's ideal for mid-sized buildings. Efficient operation and flexible design Compatible with TrueAlarm sensors and TrueAlert ES addressable notification appliances.	Recommended for medium sized installations Networkable with 4007ES and 4100ES control panels
4017ES	ADDR	Fire panel which includes audio and visual indications of alarms, and a newer CPU.	Small audio panel, recommended for small to medium sized installations
4100ES	ADDR	An advanced, addressable control unit for the largest and most complex facility requirements. Networkable, scalable, flexible, and an efficient design Integrated voice and audio signaling capabilities	Recommended for larger installations, such as Hotels, stadiums, and large complexes

[1] CONV = Conventional, ADDR = Addressable

For additional details on your specific fire panel, see the installation manual.

Touch Screen Display

The 8” color display with an annunciator (available for the 4100ES) which provides better display capabilities over the standard 2-line by 40-character display. The touch screen has two communication modes: serial bus and ethernet. Note: The ethernet port is dedicated to fire panel functions and not for network connectivity.

USB Drive

Used to install software on panels that provide a USB port.

Service Tech Laptop

Used to download and install software

Peripherals

Peripherals are devices that connect to the fire panel for various control and monitoring operations. Each customer installation is different and may include one or more groups of the following peripheral devices:

- Pull stations
- Horns
- Strobes
- Speakers
- Smoke detectors
- Control relays
- Sprinkler pumps
- And others…

Connected Services Gateway and Johnson Controls Cloud Services (Optional)

The Connected Services Gateway (CSG) is an all-in-one interface card that supports central station communication and enables SafeLINC Cloud Services. SafeLINC Cloud is intended to complement Central Station monitoring for fire alarm systems and enhance your ability to manage your fire and life safety systems effectively. SafeLINC Cloud is not a substitute for real-time Central Station monitoring of your fire alarm system.

1.1.3 Supporting components

Supporting components are those which are necessary for system operations but are not within the targeted scope of this document. This solution is supported by the following components:

Expansion Cards / Boards / Accessories

Expansion cards can be added to the fire panel to expand capabilities. See the installation manual for the specific fire panel to see which optional modules can be installed. An example of the modules include:

- IDNAC card (Integrated into the fire panel)
- IDNET card

- Zone/Relay module
- LED Module
- ES Net card (Ethernet, DSL, and Fiber Media)
- ES Touch screen display
- Connected Services Gateway (CSG)
- SUR-GARD transmitter
- And others…

TrueSite Workstation (TSW)

The Simplex TrueSite Workstation software is a PC-based application that provides head-end annunciation, floor plan display, system control, and information management. It is an integral part of an alarm system; it is a node on a fire panel network used to annunciate and control the points contained within the fire panel network.

1.2 Security feature set

Johnson Controls products are designed with built-in cybersecurity features out of the box. Some features are included and set by default while other features need the reader to go through steps for advanced hardening. Note: the features below will vary by the selection of panels in each solution.

Table 1.2.0.1: Feature summary table

Section	Type	Feature name	New feature
1.2.1	Secure communications	Digital certificate management	1.0
1.2.2	Monitor	Audit Logs	1.0
1.2.3	Alarms and alerts	Heartbeat Tamper switch User interface (UI)	1.0
1.2.4	Availability assurance	Power backup Data availability Panel recovery	1.0
1.2.5	Code validation	Secure boot	1.0

1.2.1 Digital certificate management

Field firmware (4017ES) updates are signed and protected.

1.2.2 Audit logs

Audit logs - Activity and events from fire panels are stored in both **Alarm** and **Trouble** audit log records which are enabled by default. Users can access these logs to view evidence of the activities that have affected the system and indicate the timestamped operation, procedure, or event. Log files cannot be deleted without elevated privileges.

1.2.3 Alarms and alerts

Heartbeat. Fire panels initiate a “heartbeat” or notification at periodical intervals that the network is connected and communicating properly. If a trouble event, such as a disconnection, circuit trouble, fault or network goes down, the heartbeat is not transmitted. The Central Station monitoring will know within a predetermined amount of time and will alert the contact person at that site and start troubleshooting the issue.
Note: The heartbeat time interval is a variable setting and can be customized per site.

Tamper Switch. Some products, such as the 4100ES, can be optionally equipped with a tamper switch. This option can be used when an audible alarm and logging of tampering activity is required.

User Interface. Fire panels have a screen or User Interface (UI) which shows system status, alarms, and alerts. The UI allows the technician, emergency professional or customer to perform acknowledge incoming events, diagnostic activities, system status, reports, updates, configuration, etc.
Some common functional alarm conditions are:

- Fire
  - Standard Fire & Smoke detection
- Priority 2 / CO alert
  - Standard Carbon Monoxide detection
- Supervisory
  - Abnormal conditions being monitored by the panel (ex: sprinkler tamper switches on valves)
- Trouble
  - (service mode, config mismatch, wrong device, duplicate device, device missing, open/short circuit)

1.2.4 Availability assurance

Fire panels have several built-in security safeguards to protect your system in the event of a power outage or system failure.

Power backup. Fire panels include backup batteries to ensure the system is running during a power loss.

Configuration of data availability. Log files and configuration are preserved in event of power outage

Panel recovery. A fire panel may have restoration functionality in the event of system crash or hang up.

1.2.5 Code validation

The 4017ES fire panel has secure boot enabled by default. When a secure boot enabled device starts or boots, the secure boot process validates each step, ensuring that each step of the boot sequence is validated. This protective measure helps to mitigate attacks on your hardware device during the start-up sequence. Secure boot prevents unsigned code from loading on to the fire panel.

1.3 Intended environment

Physical access and installation of devices can greatly impact cybersecurity.

Fire Panels. Fire panels are designed to be operated in an indoor, dry environment such as Commercial and Industrial buildings including the lobbies and hallways of schools, factories, hospitals, transportation buildings, as well as the utility closets of those structures.

Here is some general panel installation guidance:

- Install in areas free of corrosive vapors
- Install where the ambient temperature stays between 32 and 120 degrees F (0-49 degrees C)
- Install in lower operating humidity no higher than 93% RH, non-condensing @ 90°F (32°C)
- Please refer to the Installation Guide of the specific panel for additional details

Peripherals. Peripherals at each level will possess varying degrees of access (section 1.1.2). Peripherals need to be installed per the building and local codes. It is best to refer to the specific installation instructions for each peripheral.

1.3.1 Internet connectivity

Internet access increases your cybersecurity footprint and attack area which requires additional hardening steps. Fire panels do not need internet access to function locally.

If your solution includes cloud services such as SafeLINC, it will require an internet gateway CSG (Connected Services Gateway) card to communicate via the internet. In this scenario, the hardening steps in section 2 must be taken to limit external access. For more information on SafeLINC, see the SafeLINC 4100-0062 datasheet at this link - https://docs.johnsoncontrols.com/simplex/v/u/Simplex/en-US/Connected-Services-Gateway-Central-Station-Communication-and-SafeLINC-Cloud-Services/6. If this link does not work, start here and do a search - https://docs.johnsoncontrols.com/simplex

1.3.2 Integration with IT networks

Most Fire Panel installations will rely heavily on isolated networks. However, some installations will include the use of customer network bridge (CNB) card and an ES Net card. If these are present in your system, follow the steps in section 2 to open the applicable communication ports.

1.3.3 Integration with external systems

Fire panels are designed to integrate with monitoring services such as Central Station monitoring to deliver 24x7 events and alarms for review and if needed, emergency action. This is achieved by using a CSG card connected to a wired telephone line, wired ethernet or cellular connection.

1.4 Patch Policy

It is best practice to upgrade fire panels with the latest software to install the most recent security fixes.

Fire Panel support is provided for the latest version of the current release. When we discover a critical security vulnerability, we use commercially reasonable efforts to:

- Issue a **critical update** for the current version of the product as soon as is reasonably practicable

When we discover non-critical security vulnerability, we use commercially reasonable efforts to:

- Apply fixes for **high severity** vulnerabilities in the next immediate release
- Apply fixes for **medium severity** vulnerabilities in the next major release

This policy shall be limited to the commercial life of the product.

1.5 Hardening methodology

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

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

1.6 Data Communication

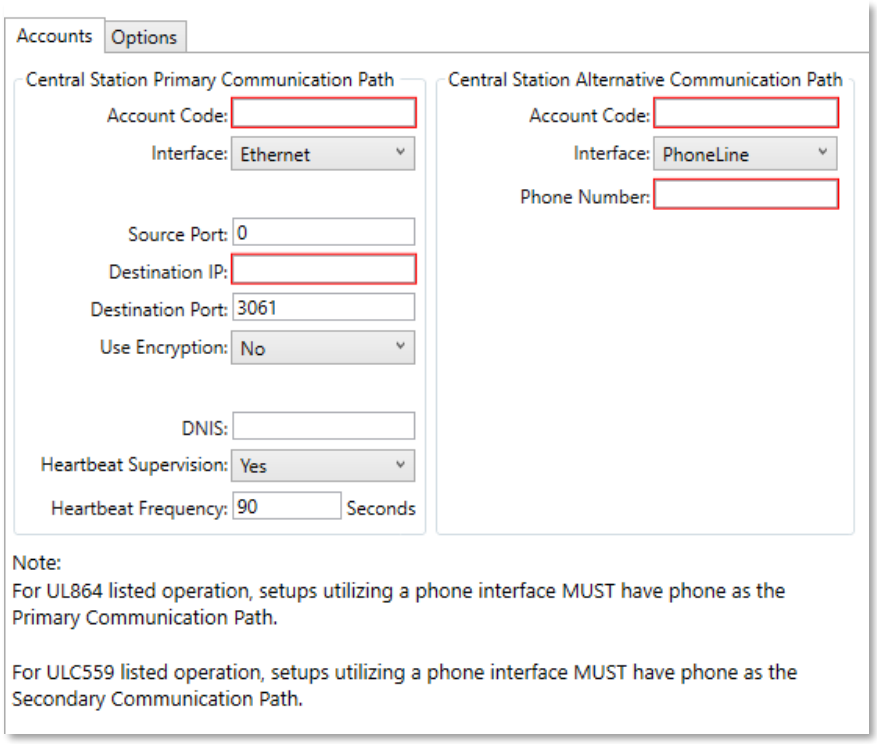
A data flow path is a detailed view of the architecture which will show each communication path and flow direction. This resource will be used to aid in the configuration of network security settings (rules) within routers, firewalls, and zero-trust architectures. The data flow path is useful for someone who is not as familiar with the process to break the communication paths to understand the processes for the basic to the more complex applications. Sections 1.6.1 through 1.6.3 illustrates the three data paths that fire panels can navigate.

1.6.1 Path 1 – Central Station monitoring.

CSG Configuration. Fire panels can be optionally monitored through a Central Station, which is a service that is always connected to the fire panels receiving outbound system status. This service will monitor, and proactively alert team members and first responders when needed.

Johnson Controls panels are designed to connect to third party monitoring solutions through a phone line, ethernet or cellular. For ethernet and cellular connections, third-party monitoring stations will require the user to configure the settings as presented within their specific product manual. Fire panels are configured with the initial settings as shown in figure 1.6.1.1. below. When configuring a panel for the first time, take special note of the boxes in red and change the defaults to ensure your panels connect properly.

Figure 1.6.1.1 Central Station monitoring default configuration



Port numbers

The ports to configure the Central Station device are shown below.

Table 1.6.2.1 Port number

Port	Protocol	Direction	Destination System	Process/Service	Description
1025	Proprietary	Outbound	Central Station server	Heartbeat	Heartbeat service

3061	Proprietary	Outbound	Central Station server	Communication	Send fire alarm events

1.6.2 Path 2 – Connecting to the SafeLINC Cloud.

Gateway Configuration - Gateway devices commissioned on on-premises networks should allow IP address prefixes to control connectivity between the IoT Hub, SafeLINC Cloud, and respective devices.

Device Gateway (IoT Hub) IP Addresses and Best practices

The Microsoft Azure cloud hosts the SafeLINC Cloud. Recommendations from Microsoft related to network configuration are available here: SafeLINC configurations - https://www.simplexfire.com/services/safelinc-connected-services-suite.

Note: The IoT hub IP address is subject to change without notice. To avoid disruption, always use the hostname when you configure firewall rules.

Port numbers

Gateways communicate with SafeLINC in Azure using protocols. Current gateway devices communicate with the protocol in Table 1. Table 1 shows a list of outbound ports that must be open in the network for a device to communicate and send data to the SafeLINC Cloud.

Table 1.6.2.1 Port number

Port	Protocol	Direction	Destination System	Process/Service	Description
5671	AMQP	Outbound	server	NotifyPI	SMTP client connection

The CSG (Connected Services Gateway) uses port 5671 to communicate with SafeLINC. Port 5671 should be open in the network to communicate with SafeLINC.

SafeLINC configuration. SafeLINC configurations for the firewall are as follows.

Note: IP addresses are subject to change from Microsoft.

Table 1.6.2.2 Regional configuration

	North America configuration	**EU configuration**
	IoT Hub and device gateway	
Host name	http://aihbtsfirestormprod001.azure-devices.net	http://aihbtsfirestormprod201.azure-devices.net
IP address	20.49.99.102	40.113.176.167
	SAFELINC_CLOUD-CSG	**Device provisioning and registration service**
Host name	aidpsbtsfirestormprod001.azure-devices-provisioning.net	http://aidpsbtsfirestormprod201.azure-devices-provisioning.net
IP address	20.49.109.137	20.49.109.137
Notes:	**Important:** When you configure firewall or network settings for a gateway device to the North American region SafeLINC cloud, the firewall and network must allow outbound connection on port 5671. You must allow DNS names: aihbtsfirestormprod001.azure-devices.net	**Important:** When you configure firewall or network settings for connecting devices to an EU region SafeLINC cloud, the firewall and network must allow outbound connection on port 5671. You must allow DNS names http://aihbtsfirestormprod201.azure-devices.net and

	andaidpsbtsfirestormprod001.azure-devices-provisioning.net or IP addresses: 20.49.99.102 and 20.49.109.137.	http://aidpsbtsfirestormprod201.azure-devices-provisioning.net or IP addresses 40.113.176.167 and 20.49.109.137.

SafeLINC Cloud is designed to complement Central Station monitoring, which is covered in use case 1.

1.6.3 Path 3 – Customer Network Bridge.

CNB configuration. CNB is a way of connecting fire panels together using the existing building infrastructure. This use case relies on the building owner or customer for the network connectivity. To have a working configuration this fire alarm system must be configured with specific IP addresses and a port that would be provided by the IT administrator. Once you have this information, a configuration file can be generated for each card by using the configurator – see figure 2.5.3 in hardening step 4.

The IT service would need to select two IP addresses, and a single port according to the following rules:

- Any IP address may be used, except local (169.254.n.n) and 0.0.0.0
- Port must be between 1 and 65535 inclusively

2 Deployment

This section is designed to help execute the deployment phase of your system. The contents within this section address how to initiate secure deployment for new installations, how to harden your attack surface and additional steps after commissioning required before the new or upgraded system is turned over to runtime operations.

2.1 Deployment overview

Security hardening begins prior to deployment with careful planning as outlined in section 1 of this guide. It is a good practice to review sections prior to deployment to fully understand the security feature set, its architecture, data flow and requirements before physically installing and making application specific configuration changes.

In this section more details are provided to help the installer prepare for deployment:

- Physical installation considerations
- Default security behavior
- Recommended knowledge level

Before you start the installation of your solution, consider the guidance in the following sections.

2.1.1 Physical installation considerations

Install hardware using the instructions provided in the installation guide. Fire panels are designed to be placed in open areas. However, the physical access to the device and physical installation of the device can impact the cybersecurity. To prevent unauthorized access, the fire panel headend should be placed in a room, cabinet or enclosure that can restrict access (for example, mechanical lock or physical access control).

2.1.2 Default security behavior

On the initial startup, certain functions will be enabled to facilitate the most common commissioning tasks. Make sure to review default access level privileges.

2.1.3 Recommended knowledge level

The person confirming that the proper hardening steps are executed should be experienced in your product's administration and networking technologies. If training for your product(s) exist, completion of the basic installation course is required, and any advanced installation course is recommended.

Note: Check with local regulations and standards to see if licensing is required for commissioning or configuring your fire panel solution (example NFPA license, or nicet.org).

2.2 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 to the correct level of protection as warranted by the customer policies and government regulations that may govern the application security settings for this deployment.

2.2.1 Hardening checklist

This checklist provides an example list of hardening steps you may select to go through. The actual steps you will take is based upon the features included within your specific environment as gathered in Section 1.

- ☐ Hardening Step 1: Disable unused ports
- ☐ Hardening Step 2: Harden Access Level Codes
- ☐ Hardening Step 3: (Optional) Harden the CSG card
  - ☐ Hardening Step 3.1: Harden the CSG card for Central Station Monitoring
  - ☐ Hardening Step 3.2: Harden the CSG card for SafeLINC
- ☐ Hardening Step 4: (Optional) Harden ES Net card with CNB

2.3.0 Communication port configuration

Ensure that the ports corresponding to your Fire Panel from section 1.6.0 are open that need to be open based on the features being used. Unused ports should be blocked unless they are specifically needed.

Hardening Step 1: Disable unused ports

To harden your system, block all ports that are not in use.

2.4.0 Access Level Codes

Numeric Codes are used to control the level of access granted to users of the fire panel. There are three levels of access that may be granted. Always grant access with the principle of Least privilege. 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 to do their job (example: accounts used during initial commissioning)

For additional details and a matrix of the roles and permissions assigned to each, refer to the specific programmer's manual for your panel

Hardening Step 2: Harden Access Level codes

Review Access Level codes in the current system and remove any codes that are no longer needed or unassigned to specific users.

2.5.0 Conditional configuration

In section 1, we learned about the specific components that your system is comprised of. The solution may contain an ES Net card with CNB, a CSG card, both cards or neither card.

- If you are using a **CSG card**, you will need to perform hardening step 2.1, 2.2 or both, depending on the features in use (Central Station monitoring or SafeLINC)
- If you are using an **ES Net card with CNB**, you will need to perform hardening step 3
- If you are not using either card, you may skip to section 3

Hardening Step 3: Harden the CSG card

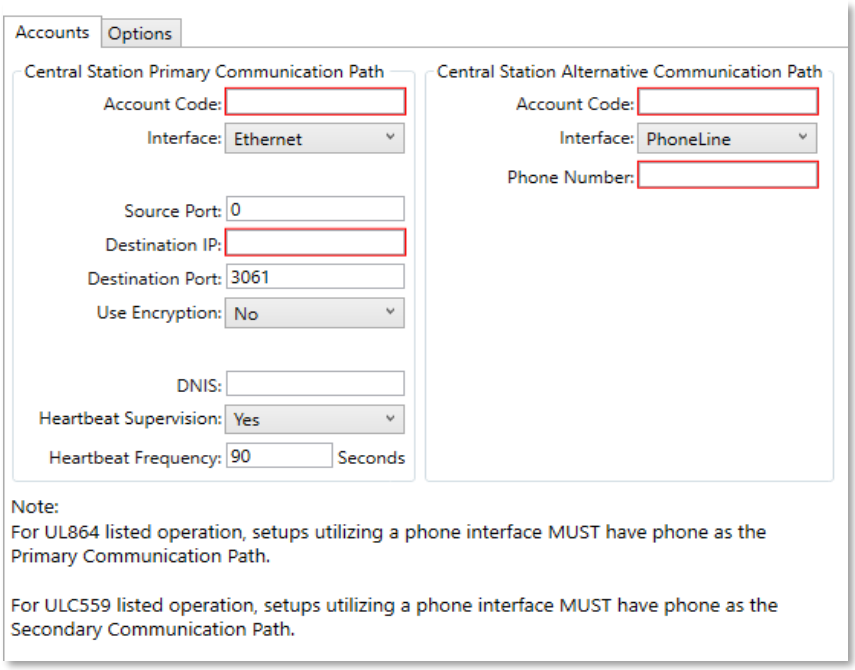
As mentioned in section 1.3.1, if your solution includes cloud services such as Central Station monitoring or SafeLINC, it will require a CSG card to communicate via the internet.

Hardening Step 3.1: Harden the CSG card for Central Station monitoring

To harden Central Station monitoring configuration:

1. Unblock communication port. This port is typically 3061. Verify this with the manual that came with your monitoring equipment.
2. Unblock heartbeat port. This port is typically 1025. Verify this port if the solution has a specific manual.
3. Configure CSG card using the Central Station configurator tool shown below in figure 2.5.1

Figure 2.5.1 – Central Station configurator

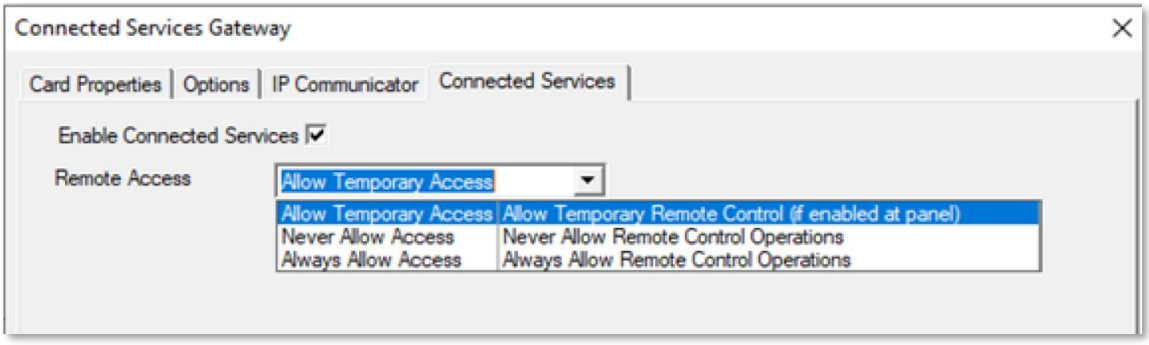


Hardening Step 3.2: Harden the CSG card for SafeLINC

To harden SafeLINC cloud service configuration:

a. Unblock port 5671
b. Enable remote access and select remote access category as shown below in figure 2.5.2

Figure 2.5.2 – Connected Services Gateway configuration

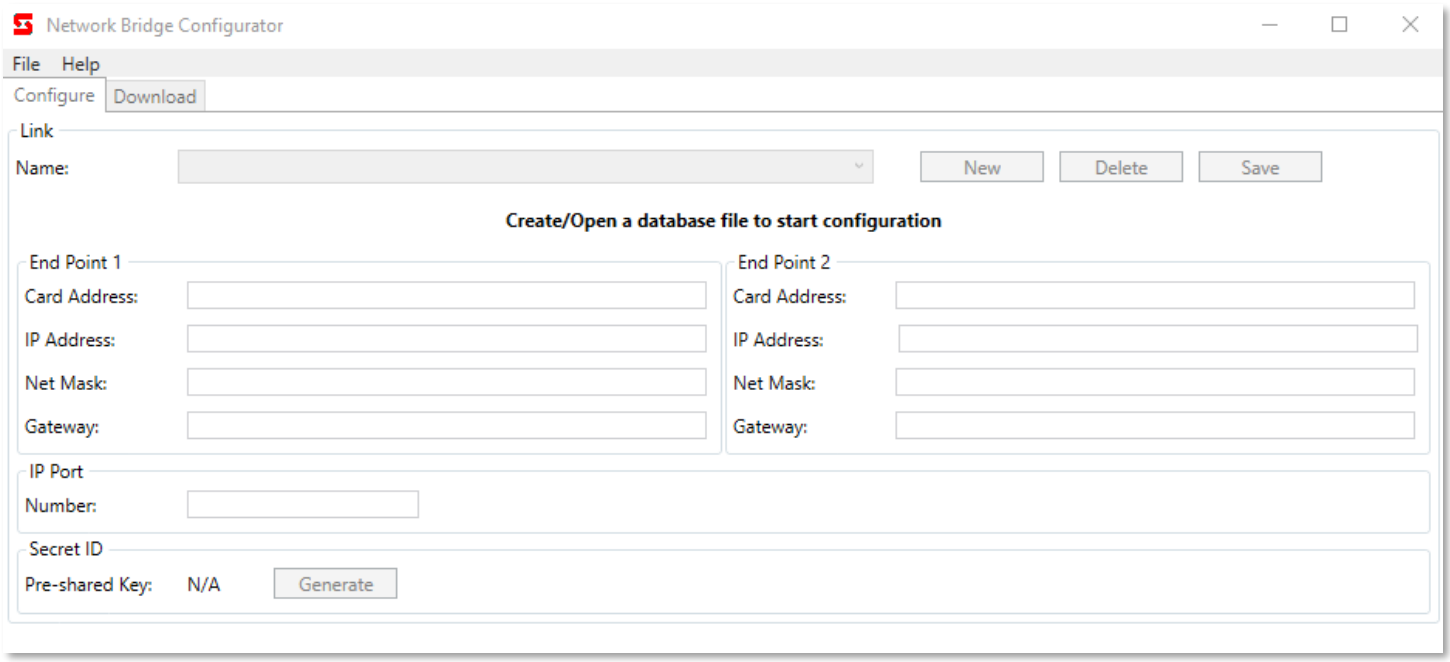


Hardening Step 4: Harden ES Net card with CNB

When connecting 2 fire panels within building networks, an ES Net card with CNB is installed. To harden this configuration:

1. Reserve a static IP address for each card and a common communication port from the building management / IT department.
2. Configure each CNB card to include a static IP address and the common communication port within the fire panel using the Network Bridge Configurator tool shown below in figure 2.5.3

Figure 2.5.3 – Network Bridge Configurator



3 Maintain

In section 1 we learned that many components work together to provide a custom solution. This section addresses how to monitor for potential cybersecurity issues and maintain protection levels as conditions change for several solutions. This means that some items in the checklist may not be part of your solution and/or within your contract. From the research you gathered in Section 1, and the terms within your contract, determine the items in table 3.1.1 that apply to your system and focus on only those items.

An audit that produces a report indicating low cybersecurity risk is a very positive result and suggests that the deployment was conducted with a high degree of care and consideration. However, new attack vectors, combined enhanced hacking tools and more advanced testing techniques may, in the future, disclose vulnerabilities with the technologies used.

The impacted technologies and their implementation may have been previously well regarded by cybersecurity experts. The discovery of vulnerabilities post the final deployment audit may not reflect the quality of the audit at the time. You may require a higher degree of protection for the environment as policies and regulations change over time.

3.1 Cybersecurity maintenance checklist

Continuously or periodically practice the following cybersecurity maintenance items. The frequency of their execution will depend on the policies and regulations which govern the site. The typical maintenance periods provided are a starting point and adjusted to best suit the target conditions of the deployed environment

See Table 3.1.1 **Cybersecurity maintenance checklist** on the following page.

Item	Description	Immediate	Base on Priority	Daily	Weekly	Monthly	Quarterly	Annual
1	*Backup event log data*							✓
2	*Update access level codes*	✓						✓
3	ES Programmer license (self-maintainer)	✓						✓
4	*Disable unused features, ports, and services*						✓	
5	*Check for and prioritize advisories or product notices*						✓	
6	*Plan and execute advisory recommendations*		✓					
7	*Check and prioritize software patches and updates*						✓	
8	*Plan and execute software patches and updates*		✓					
9	*Review updates to organizational policies*							✓
10	*Review updates to regulations*							✓
11	*Conduct security audits*							✓
12	*Update as built documentation*	✓						✓
13	*Update standard operating procedures*							✓
14	*Renew licensing agreements*							✓
15	*Renew support contracts*							✓
16	*Check for end-of-life announcements and plan for replacements*							✓
17	*Monitor for cyber attacks*	✓		✓				

Table 3.1.1 – Cybersecurity Maintenance Checklist

3.1.1 Backup event log data

Event log data can be the most valuable asset within the fire panel. It is recommended that backups are performed annually and before changing or modifying the system. Johnson Controls recommends performing this backup before the annual inspection. To backup event log data, choose from the following:

1. Review the Operator's manual.
   Print out the event logs.
   Store the event logs in a safe location or off site.

2. Review the Programmer's manual.
   Open the **IP File Transfer** tool.
   Download the event log files.
   Note: the manual refers to this as an "Upload" from the perspective of the panel, up to the PC.
   Store these files in a secure location, according to your organization's policies.

Action	Details	Suggested frequency
Backup historical data	Either (1) print out the event logs (See Operator's manual) or (2) download the event logs file using the **IP File Transfer** tool (See programmer's manual).	Annually

3.1.2 Update access level codes

Access codes should be reviewed and changed when specific events occur. For example:

- When new personnel need to access the fire panel
- When personnel are voluntarily or non-voluntarily terminated from employment
- When personnel have changed roles and have increased or decreased responsibilities

During these events, immediately update the access level codes. This ensures that people with the appropriate roles can access the panels with the correct privileges. It also ensures an older code can no longer be used to gain access, keeping your panel secure. Note: It is common practice that a passcode used with fire panels may be used by multiple users which needs to be considered when updating or removing codes.

Action	Details	Suggested frequency
Update access level codes	Depending on the event (add, delete, change) update the access level codes	Immediate and annually

3.1.3 ES Programmer license (self-maintainer)

To edit a fire panel's configuration, a software license is needed to run the **ES Programmer** tool. A license is assigned to a single Windows workstation at a time. When a license is no longer required, revoke it by:

- Deactivating the workstation
- Revoking the license from the server

Exception: If a machine is reassigned to a new employee, do not perform the steps to keep the current license. For additional information on this process, see the Fire Panel Programmer's manual.
Note: Workstation licenses need to periodically synchronize with the server to remain active.

Action	Details	Suggested frequency

R**e**view and u**pdate** E**S Programmer l**icenses	Depending on the event (add, delete, change) review, revoke and reassign ES Programmer licenses	Immediate and annually

3.1.4 Disable unused features, ports, and services

Reassess the need for optional features, ports, and services (SafeLINC Cloud or Central Station monitoring) that an authorized user does not require and disable them. This practice will lower the attack surface resulting in a higher level of protection.

Action	Details	Suggested frequency
Disabled unused features, **ports**, **and services**	Refer to your product Installation or User manuals. Also refer to sections 1.6 and 2.2.2 to disable unused ports	Quarterly

3.1.5 Check for and prioritize advisories or product notices

Find cybersecurity advisories for Fire Panels at https://www.johnsoncontrols.com/cyber-solutions/security-advisories with a registered user account (create a username and password). User account registration is open to JCI customers and authorized representatives. At the bottom of the page, register to receive product security advisories via email. Some Key points to consider:

- Determine if a Fire Panel is impacted by the conditions outlined in the advisories
- Based on how the system is deployed, configured, and used, will help determine if the advisory may or may not be of concern
- Referring to as-built documentation of the system will help with this assessment. A well good set of as-built documentation will identify the number of components impacted and their location.
- While advisories call attention to a cybersecurity issue, it is not always possible to take immediate action or execute the full recommendation described in the advisories. If so, prioritization will aid in your planning to ensure that any issue impacting your system is fully and appropriately addressed in order of priority.

Check for advisories or product notices from third party components such as networking equipment and operating systems by consulting with the respective vendor.

Action	Details	Suggested frequency
Check for and prioritize advisories	Refer to the link above that hosts Johnson Control's advisories and explore each quarter	Quarterly

3.1.6 Plan and execute advisory recommendations

Follow the plan determined in maintenance step 3.1.5. Consult with all parties who may be impacted by an advisory or downtime and choose the best time for deployment.

Action	Details	Suggested frequency
Plan and execute advisory recommendations	Plan and execute advisory recommendations from maintenance step 3.1.5	Based on priority

3.1.7 Check and prioritize patches and updates

While a patch or update may or may not relate to a security advisory, it is always best practice to apply the most current patches and updates. These patches and updates can include cybersecurity enhancements as well as fixes to known issues. Review the release notes and prioritize the benefits of the patch or update. The overall benefit should include the improved protection that will aid in lowering the cybersecurity risk. Be sure also to check for updates and patches of third-party components such as networking equipment and operating systems by consulting with the respective vendor.

Action	Details	Suggested frequency
Check for and prioritize patches and updates	Explore available patches and updates each quarter	Quarterly

3.1.8 Plan and execute software patches and updates

Follow the plan determined in maintenance step 3.1.7. Consult with all parties who may be impacted by patches, updates or downtime and choose the best time for deployment. Contact your local branch office for assistance.

Action	Details	Suggested frequency
Plan and execute software patches and updates	Plan and execute advisory recommendations from maintenance step 3.1.7	Base on priority

3.1.9 Review updates to organizational policies

Organizations may update their policies which include cybersecurity requirements. Changes to these policies can impact systems which complied prior to the change. Periodically check to see if policy changes were made and re-assess compliance with those policies.

Action	Details	Suggested frequency
Review organizational policy updates	Collect most recent security policies for your organization	Annual

3.1.10 Review updates to regulations

If a Fire Panel is deployed in a location that is governed by regulation, it is important to check to see if there are any updates to those regulations. In some cases, new regulations are introduced. Whether it is a review of an updated regulation to maintain compliance and a new regulation, an assessment of the changes should be conducted periodically.

Action	Details	Suggested frequency
Review updates to regulations	Collect most recent copies of regulations as applicable. Perform a gap analysis against the deployed configuration.	Annual

3.1.11 Conduct security audits

Periodic security audits are necessary as cybersecurity guidance, organizational policies, regulations, auditing processes, system use, and configuration and threats have likely changed since the last audit. By conducting periodic security audits, you can apply the latest knowledge and reveal gaps in protection previously undetected or created by changes in system use of configuration.

Action	Details	Suggested frequency

Conduct security audits	Perform the tasks listed on your Security audit checklist	Annual

3.1.12 Update as-built documentation

Be certain to keep the as-built documentation up to date if the system architecture or component configuration significantly changes. Updates are also usually required if you modify or add equipment. After every change, evaluate if the as-built documentation is out of date enough to initiate the documentation process.

Some installations may require updating the as-built documentation on a more frequent, periodic basis. Work with your local branch or building owner if you have questions.

Action	Details	Suggested frequency
Update as-built documentation	Update if the system architecture or component configuration significantly changes	As changes are made or annual

3.1.13 Update standard operating procedures

Including best practices for cybersecurity within standard operating procedures can complement the protection that the system can deliver on its own. Depending on the procedures an operator uses, they can create, prevent, or close a gap in protection. Therefore, it is important to update standard operating procedures periodically.

Action	Details	Suggested frequency
Update standard operating procedures	Collect standard operating procedures for use of Fire Panels within the organization	Annual

3.1.14 Renew licensing agreements

Assure that your software license supports the necessary functions required for your installation.

Action	Details	Suggested frequency
Renew licensing agreements	Collect active licensing details.	Annual

3.1.15 Renew support contracts

If you have any support contracts such Software Support Agreement (SSA) and Product Service Agreement (PSA), assure that these are up to date to eliminate any lapses in coverage.

Action	Details	Suggested frequency
Renew support contracts	Collect SSA and PSA details	Annual

3.1.16 Check for end-of-life announcements and plan for replacements.

Check with your local Johnson Controls branch for end-of-support announcements a.k.a. discontinuation information and plan for replacements or upgrades, including all operating systems and fire panels.

Action	Details	Suggested frequency
Check for discontinuation information and plan for replacements	Collect end-of-support details for your products through your local office	Annual

3.1.17 Monitor for cyber attacks

Monitoring site perimeters, networks and endpoints for cyber-attacks is a part of good cybersecurity operation. Ultimately it is the site owner's responsibility to:

- Review the many tools available to assist with real-time analytics-based detection
- Decide on and fully test the tool in a non-production environment
- Verify that Fire Panels continue to operate properly after installation of any security monitoring tools
- Only install software (or hardware) which aligns with the policies of the environment's owner

Action	Details	Suggested frequency
Monitor for cyber attacks	Determine which security monitoring tools and services to implement	Run continuously once implemented

Appendix A - Additional Fire Panel certification details

The certifications below are from datasheets listing the different agency approvals for our panels. For the latest updates, refer to the recent product specific datasheets (updated more frequently). Fire Panels are generally:

4100ES	• **UL 864**, Fire Detection and Control (UOJZ), Smoke Control Service (UUKL), Releasing Device Service (SYZV), Emergency Communication and Relocation Equipment (UOQY), Control Unit Accessories (UOXX) • **UL 1076**, Proprietary Alarm Units - Burglar (APOU) • **UL 2017**, Process Management Equipment (QVAX), Emergency Alarm System Control Units (FSZI) • **UL 1730**, Smoke Detector Monitor (UULH) • **UL 2572**, Mass Notification Systems (PGWM) • **CAN/ULC-S527** Control Units for Fire Alarm Systems (UOJZ7), Releasing Device Service (SYZV7), Control Unit Accessories (UOXX7) • **CAN/ULC-S559** Central Station Fire Alarm System Units (DAYR7) • **ULC/ORD-C1076** Proprietary Burglar Alarm Units and Systems (APOU7) • **ULC/ORD-C100** Smoke Control System Equipment (UUKL7)
4010ES	• **UL 864**, Control Units, System (UOJZ); Control Unit Accessories, System, Fire Alarm (UOXX); Control Units, Releasing Device Service (SYZV); Smoke Control System Equipment (UUKL) • **UL 1076**, Proprietary Alarm Units (APOU) • **UL 1730**, Smoke Detector Monitors and Accessories (UULH) • **UL 2017**, Emergency Alarm System Control Units, CO detection (FSZI); Process Equipment Management (QVAX) • **ULC-S527**, Control Units, System, Fire Alarm (UOJZ7); Control Unit Accessories, System, Fire Alarm (UOXX7); Control Units, Releasing Device Service (SYZV7) • **ULC-S559**, Central Station Fire Alarm System Units (DAYR7) • **ULC/ORD-C1076**, Proprietary Burglar Alarm System Units (APOU7) • **ULC/ORD-C100**, Smoke Control System Equipment, (UUKL7)
4007ES	• **UL 864** - Control Units, System (UOJZ); Control Unit Accessories, System, Fire Alarm (UOXX); Control Units, Releasing Device Service (SYZV) • **UL 2017** - Emergency Alarm System Control Units (CO detection), (FSZI) • **ULC-S559** - Central Station Fire Alarm System Units (DAYRC) • **ULC-S527** - Control Units, System, Fire Alarm (UOJZC); Control Unit Accessories, System, Fire Alarm (UOXXC); Control Units, Releasing Device Service (SYZVC)
4008, 4006 & 4004R	• **UL** Standard **86** • **ULC** Standard **S527**
4017ES	The 4017ES is seeking on top of these listings: • **UAE** Approval from UAE Civil Defense (based on the UL and FM reports) • **LVD 62368-1** Third Edition 13-Dec-2019 Audio/Video, Information and Communication Technology Equipment – Part 1: Safety Requirements • **OSHPD ICC-ES AC-156** Special Seismic Certification of Equipment and Components • **UL 1711** Fourth Edition 28-Dec-2006 Amplifiers for Protective Signaling Systems

Key to abbreviations

CSFM = California State Fire Marshall
FCC = Federal Communications Commission
FM = Factory Mutual
LVD = Low Voltage Directive
NFPA = National Fire Protection Association
UL = Underwriters Laboratories Inc.
ULC = Underwriters Laboratories of Canada
OSHPD = Office of Statewide Health Planning and Development
OTCR = Office of Technical Certification and Research
UAE = United Arab Emirates

Appendix B – Acronyms

Acronym	Description
CNB	Customer Network Bridge
CSG	Connected Services Gateway
DACT	Digital Alarm Communicator Transmitter
IDNAC	Intelligent Distributed Network Annunciation Circuit
IDNET	Intelligent Device Network
PSA	Product Service Agreement
SSA	Software Support Agreement
TSD	Touch Screen Display
TSW	TrueSite Workstation by Simplex ©

Appendix C - Additional Fire Panel Literature

Document title	Document number
4004R Fire Alarm installation, programming, and operating instructions	0579354
4006 Datasheet	S4006-0001
4007ES and 4007ES Hybrid Fire Alarm System Installation Manual	05791102
4007ES and 4007ES Hybrid Fire Alarm Systems	05791167
4007ES Operator’s Manual	05791165
4010ES Fire Alarm Operator's Manual	0579969
4010ES Fire Alarm System Installation Guide	0579989
4017ES Operator’s Manual	A16382A1M5
4017ES Panel Programmer’s Manual	A16382A1LN
4100ES Fire Alarm System Installation Guide	0574848
4100ES Fire Alarm System Operator’s Manual	0579197
ES Panel Programmer’s Manual For 4100ES and 4010ES Fire Alarm Control Panels	0574849

For additional information see this link - https://www.johnsoncontrols.com/fire-detection/control-units