NOTIFIER®
by Honeywell

Cybersecurity Manual

Product Security



Document LS10217-000NF-E Rev: F
8/13/2021 ECN: 5066

Fire Alarm & Emergency Communication System Limitations

While a life safety system may lower insurance rates, it is not a substitute for life and property insurance!

An automatic fire alarm system—typically made up of smoke detectors, heat detectors, manual pull stations, audible warning devices, and a fire alarm control panel (FACP) with remote notification capability—can provide early warning of a developing fire. Such a system, however, does not assure protection against property damage or loss of life resulting from a fire.

An emergency communication system—typically made up of an automatic fire alarm system (as described above) and a life safety communication system that may include an autonomous control unit (ACU), local operating console (LOC), voice communication, and other various interoperable communication methods—can broadcast a mass notification message. Such a system, however, does not assure protection against property damage or loss of life resulting from a fire or life safety event.

The Manufacturer recommends that smoke and/or heat detectors be located throughout a protected premises following the recommendations of the current edition of the National Fire Protection Association Standard 72 (NFPA 72), manufacturer's recommendations, State and local codes, and the recommendations contained in the Guide for Proper Use of System Smoke Detectors, which is made available at no charge to all installing dealers. This document can be found at http://www.systemsensor.com/appguides/. A study by the Federal Emergency Management Agency (an agency of the United States government) indicated that smoke detectors may not go off in as many as 35% of all fires. While fire alarm systems are designed to provide early warning against fire, they do not guarantee warning or protection against fire. A fire alarm system may not provide timely or adequate warning, or simply may not function, for a variety of reasons:

Smoke detectors may not sense fire where smoke cannot reach the detectors such as in chimneys, in or behind walls, on roofs, or on the other side of closed doors. Smoke detectors also may not sense a fire on another level or floor of a building. A second-floor detector, for example, may not sense a first-floor or basement fire.

Particles of combustion or "smoke" from a developing fire may not reach the sensing chambers of smoke detectors because:

- Barriers such as closed or partially closed doors, walls, chimneys, even wet or humid areas may inhibit particle or smoke flow.
- Smoke particles may become "cold," stratify, and not reach the ceiling or upper walls where detectors are located.
- Smoke particles may be blown away from detectors by air outlets, such as air conditioning vents.
- Smoke particles may be drawn into air returns before reaching the detector.

The amount of "smoke" present may be insufficient to alarm smoke detectors. Smoke detectors are designed to alarm at various levels of smoke density. If such density levels are not created by a developing fire at the location of detectors, the detectors will not go into alarm.

Smoke detectors, even when working properly, have sensing limitations. Detectors that have photoelectronic sensing chambers tend to detect smoldering fires better than flaming fires, which have little visible smoke. Detectors that have ionizing-type sensing chambers tend to detect fast-flaming fires better than smoldering fires. Because fires develop in different ways and are often unpredictable in their growth, neither type of detector is necessarily best and a given type of detector may not provide adequate warning of a fire.

Smoke detectors cannot be expected to provide adequate warning of fires caused by arson, children playing with matches (especially in bedrooms), smoking in bed, and violent explosions (caused by escaping gas, improper storage of flammable materials, etc.).

Heat detectors do not sense particles of combustion and alarm only when heat on their sensors increases at a predetermined rate or reaches a predetermined level. Rate-of-rise heat detectors may be subject to reduced sensitivity over time. For this reason, the rate-of-rise feature of each detector should be tested at least once per year by a qualified fire protection specialist. Heat detectors are designed to protect property, not life.

IMPORTANT! Smoke detectors must be installed in the same room as the control panel and in rooms used by the system for the connection of alarm transmission wiring, communications, signaling, and/or power. If detectors are not so located, a developing fire may damage the alarm system, compromising its ability to report a fire.

Audible warning devices such as bells, horns, strobes, speakers and displays may not alert people if these devices are located on the other side of closed or partly open doors or are located on another floor of a building. Any warning device may fail to alert people with a disability or those who have recently consumed drugs, alcohol, or medication. Please note that:

- An emergency communication system may take priority over a fire alarm system in the event of a life safety emergency.
- Voice messaging systems must be designed to meet intelligibility requirements as defined by NFPA, local codes, and Authorities Having Jurisdiction (AHJ).
- Language and instructional requirements must be clearly disseminated on any local displays.
- Strobes can, under certain circumstances, cause seizures in people with conditions such as epilepsy.
- Studies have shown that certain people, even when they hear a fire alarm signal, do not respond to or comprehend the meaning of the signal. Audible devices, such as horns and bells, can have different tonal patterns and frequencies. It is the property owner's responsibility to conduct fire drills and other training exercises to make people aware of fire alarm signals and instruct them on the proper reaction to alarm signals.
- In rare instances, the sounding of a warning device can cause temporary or permanent hearing loss.

A life safety system will not operate without any electrical power. If AC power fails, the system will operate from standby batteries only for a specified time and only if the batteries have been properly maintained and replaced regularly.

Equipment used in the system may not be technically compatible with the control panel. It is essential to use only equipment listed for service with your control panel.

Alarm Signaling Communications:

- **IP connections** rely on available bandwidth, which could be limited if the network is shared by multiple users or if ISP policies impose restrictions on the amount of data transmitted. Service packages must be carefully chosen to ensure that alarm signals will always have available bandwidth. Outages by the ISP for maintenance and upgrades may also inhibit alarm signals. For added protection, a backup cellular connection is recommended.
- **Cellular connections** rely on a strong signal. Signal strength can be adversely affected by the network coverage of the cellular carrier, objects and structural barriers at the installation location. Utilize a cellular carrier that has reliable network coverage where the alarm system is installed. For added protection, utilize an external antenna to boost the signal.
- **Telephone lines** needed to transmit alarm signals from a premise to a central monitoring station may be out of service or temporarily disabled. For added protection against telephone line failure, backup alarm signaling connections are recommended.

The most common cause of life safety system malfunction is inadequate maintenance. To keep the entire life safety system in excellent working order, ongoing maintenance is required per the manufacturer's recommendations, and UL and NFPA standards. At a minimum, the requirements of NFPA 72 shall be followed. Environments with large amounts of dust, dirt, or high air velocity require more frequent maintenance. A maintenance agreement should be arranged through the local manufacturer's representative. Maintenance should be scheduled as required by National and/or local fire codes and should be performed by authorized professional life safety system installers only. Adequate written records of all inspections should be kept.

Limit-F-2020

Installation Precautions

Adherence to the following will aid in problem-free installation with long-term reliability:

WARNING - Several different sources of power can be connected to the fire alarm control panel. Disconnect all sources of power before servicing. Control unit and associated equipment may be damaged by removing and/or inserting cards, modules, or interconnecting cables while the unit is energized. Do not attempt to install, service, or operate this unit until manuals are read and understood.

CAUTION - System Re-acceptance Test after Software Changes: To ensure proper system operation, this product must be tested in accordance with NFPA 72 after any programming operation or change in site-specific software. Re-acceptance testing is required after any change, addition or deletion of system components, or after any modification, repair or adjustment to system hardware or wiring. All components, circuits, system operations, or software functions known to be affected by a change must be 100% tested. In addition, to ensure that other operations are not inadvertently affected, at least 10% of initiating devices that are not directly affected by the change, up to a maximum of 50 devices, must also be tested and proper system operation verified.

This system meets NFPA requirements for operation at 0-49º C/32-120º F and at a relative humidity 93% ± 2% RH (non-condensing) at 32°C ± 2°C (90°F ± 3°F). However, the useful life of the system's standby batteries and the electronic components may be adversely affected by extreme temperature ranges and humidity. Therefore, it is recommended that this system and its peripherals be installed in an environment with a normal room temperature of 15-27º C/60-80º F.

Verify that wire sizes are adequate for all initiating and indicating device loops. Most devices cannot tolerate more than a 10% I.R. drop from the specified device voltage.

Like all solid state electronic devices, this system may operate erratically or can be damaged when subjected to lightning induced transients. Although no system is completely immune from lightning transients and interference, proper grounding will reduce susceptibility. Overhead or outside aerial wiring is not recommended, due to an increased susceptibility to nearby lightning strikes. Consult with the Technical Services Department if any problems are anticipated or encountered.

Disconnect AC power and batteries prior to removing or inserting circuit boards. Failure to do so can damage circuits.

Remove all electronic assemblies prior to any drilling, filing, reaming, or punching of the enclosure. When possible, make all cable entries from the sides or rear. Before making modifications, verify that they will not interfere with battery, transformer, or printed circuit board location.

Do not tighten screw terminals more than 9 in-lbs. Over-tightening may damage threads, resulting in reduced terminal contact pressure and difficulty with screw terminal removal.

This system contains static-sensitive components. Always ground yourself with a proper wrist strap before handling any circuits so that static charges are removed from the body. Use static suppressive packaging to protect electronic assemblies removed from the unit.

Units with a touchscreen display should be cleaned with a dry, clean, lint free/microfiber cloth. If additional cleaning is required, apply a small amount of Isopropyl alcohol to the cloth and wipe clean. Do not use detergents, solvents, or water for cleaning. Do not spray liquid directly onto the display.

Follow the instructions in the installation, operating, and programming manuals. These instructions must be followed to avoid damage to the control panel and associated equipment. FACP operation and reliability depend upon proper installation.

Precau-D2-11-2017

FCC Warning

WARNING: This equipment generates, uses, and can radiate radio frequency energy and if not installed and used in accordance with the instruction manual may cause interference to radio communications. It has been tested and found to comply with the limits for class A computing devices pursuant to Subpart B of Part 15 of FCC Rules, which is designed to provide reasonable protection against such interference when devices are operated in a commercial environment. Operation of this equipment in a residential area is likely to cause interference, in which case the user will be required to correct the interference at his or her own expense.

Canadian Requirements

This digital apparatus does not exceed the Class A limits for radiation noise emissions from digital apparatus set out in the Radio Interference Regulations of the Canadian Department of Communications.

Le present appareil numerique n'emet pas de bruits radioelectriques depassant les limites applicables aux appareils numeriques de la classe A prescrites dans le Reglement sur le brouillage radioelectrique edicte par le ministere des Communications du Canada.

HARSH™, **NIS™**, and **NOTI•FIRE•NET™** are all trademarks; and **Acclimate® Plus™**, **FlashScan®**, **FAAST Fire Alarm Aspiration Sensing Technology®, Honeywell®**, **INSPIRE®**, **Intelligent FAAST®, NOTIFIER®**, **ONYX®**, **ONYXWorks®**, **SWIFT®**, **VeriFire®**, and **VIEW®** are all registered trademarks of Honeywell International Inc. **Microsoft®** and **Windows®** are registered trademarks of the Microsoft Corporation. **Chrome™** and **Google™** are trademarks of Google Inc. **Firefox®** is a registered trademark of The Mozilla Foundation.

©2021 by Honeywell International Inc. All rights reserved. Unauthorized use of this document is strictly prohibited.

Software Downloads

In order to supply the latest features and functionality in fire alarm and life safety technology to our customers, we make frequent upgrades to the embedded software in our products. To ensure that you are installing and programming the latest features, we strongly recommend that you download the most current version of software for each product prior to commissioning any system. Contact Technical Support with any questions about software and the appropriate version for a specific application.

Documentation Feedback

Your feedback helps us keep our documentation up-to-date and accurate. If you have any comments or suggestions about our online Help or printed manuals, you can email us.

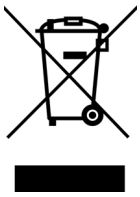
Please include the following information:

- Product name and version number (if applicable)
- Printed manual or online Help
- Topic Title (for online Help)
- Page number (for printed manual)
- Brief description of content you think should be improved or corrected
- Your suggestion for how to correct/improve documentation

Send email messages to:

FireSystems.TechPubs@honeywell.com

Please note this email address is for documentation feedback only. If you have any technical issues, please contact Technical Services.



This symbol (shown left) on the product(s) and / or accompanying documents means that used electrical and electronic products should not be mixed with general household waste. For proper treatment, recovery and recycling, contact your local authorities or dealer and ask for the correct method of disposal.

Electrical and electronic equipment contains materials, parts and substances, which can be dangerous to the environment and harmful to human health if the waste of electrical and electronic equipment (WEEE) is not disposed of correctly.

Disclaimer

In no event shall Honeywell be liable for any damages or injury of any nature or kind, no matter how caused, that arise from the use of the equipment referred to in this manual.

Strict compliance with the safety procedures set out and referred to in this manual, and extreme care in the use of the equipment, are essential to avoid or minimize the chance of personal injury or damage to the equipment.

The information, figures, illustrations, tables, and specifications contained in this manual are believed to be correct and accurate as of the date of publication or revision. However, no representation or warranty with respect to such correctness or accuracy is given or implied and Honeywell will not, under any circumstances, be liable to any person or corporation for any loss or damages incurred in connection with the use of this manual.

The information, figures, illustrations, tables, and specifications contained in this manual are subject to change without notice.

In no event shall Honeywell be liable for any equipment malfunction or damages whatsoever, including (without limitation) incidental, direct, indirect, special, and consequential damages, damages for loss of business profits, business interruption, loss of business information, or other pecuniary loss, resulting from any violation of the above prohibitions.

Copyright Notice

Microsoft, MS and Windows are registered trademarks of Microsoft Corp.

Other brand and product names mentioned in this manual may be trademarks or registered trademarks of their respective companies and are the sole property of their respective holders.

NOTIFIER is a registered trademark of Honeywell International Inc.

Find out more at www.notifier.com.

Table of Contents

Section 1: Introduction 7
1.1: Assumptions and Prerequisites 7
1.2: Applicable NOTIFIER Products 7
1.3: Applicable Physical Connections 7
Section 2: General 8
2.1: Threats 8
2.2: Unauthorized Access 8
2.3: Viruses and Other Malicious Software Agents 8
2.4: User Access and Passwords 8
2.5: Memory Media 8
2.6: Software and Firmware Updates 8
2.7: Computers and Access 8
2.8: Networks, Firewalls & VPN Connections 9
2.9: VPN Setup 12
2.9.1: Digital Signing 12
Section 3: Product Information 14
3.1: NCD/Fire Panels 14
3.2: PC NFN Gateways 14
3.3: ONYXWORKS-WS 14
3.4: Embedded Gateways 14
3.5: NFC-50/100 15
3.6: Smart Wireless Integrated Fire Technology (SWIFT) 15
3.7: VeriFire Tools 16

Section 1: Introduction

This guide is intended to provide information on security risks and solutions associated with day to day use of NOTIFIER products.

1.1 Assumptions and Prerequisites

This guide assumes a high degree of technical knowledge and familiarity with:

- PC administration and operations systems
- Networking systems and concepts
- Security issues and concepts

1.2 Applicable NOTIFIER Products

- N16
- NCA-2
- NCD
- NFS-320/SYS
- NFS2-640
- NFS2-3030
- DVC
- ONYXWORKS-WS
- HS-NCM
- NCM
- NFN-GW-PC-W
- NFN-GW-PC-F
- NFN-GW-PC-HNSF
- NFN-GW-PC-HNW
- BACNET-GW-3
- MODBUS-GW
- NFN-GW-EM-3
- LEDSIGN-GW
- CAP-GW
- VESDA-HLI-GW
- NFC-50/100
- SWIFT®
- VeriFire® Tools

1.3 Applicable Physical Connections

Physical connections referred to in this manual include:

- Touch Screen/Front Panel
- USB Ports
- RS-232 Port
- RS-485 Port
- Ethernet Port
- BroadR-Reach

Section 2: General

2.1 Threats

Security threats applicable to networked systems include unauthorized access, communication snooping, viruses and other malicious software agents.

2.2 Unauthorized Access

This threat includes physical access to the controller and intrusion into the network to which NOTIFIER equipment is connected. Unauthorized external access can result in the following:

- Loss of system availability
- Incorrect execution of controls causing damage to the equipment
- Incorrect operation and/or spurious alarms
- Theft or damage to the contents of the system
- The capture and modification, or deletion of data causing possible liability to the install site and Honeywell

Unauthorized access can result from lack of security of user name and password information. Uncontrolled access to the equipment, and uncontrolled, unsecured access to the network.

2.3 Viruses and Other Malicious Software Agents

Malicious Software includes the following:

- Viruses
- Spyware
- Worms
- Trojans

These may be present on a computer which is used for PC configuration software, such as VeriFire Tools or on a USB stick that is used to upload/download system data on an FACP.

The intrusion of malicious software agents can result in performance degradation, loss of system availability, and the capture, modification, or deletion of data, including configuration, and device logs. Viruses can be transferred by USB devices from other infected systems on the network or malicious Internet sites.

2.4 User Access and Passwords

Good password security practices should be followed. This includes ensuring the physical security of passwords and keeping passwords secure. For password protected products, observe the following good practice:

- Ensure physical security of passwords. Avoid writing user names and passwords where they can be seen by unauthorized personnel
- Make sure passwords contain characters, numbers, and a mix of lower and uppercase letters
- Passwords should be complex enough as to not be easily guessed, and should not contain phrases used in common speech
- Do not use personally identifiable information as a password, such as social security numbers, addresses, birth dates etc.
- Set the minimum level of access for each user. Do not provide users with privileges they do not need
- Ensure that users only use their credentials when accessing the programming level of the FACP
- Periodically audit user accounts and remove any that are no longer required

2.5 Memory Media

Use only authorized removable media that has been scanned and checked for viruses and malware using up to date anti-virus software.

Ensure that memory media is not used for other purposes to avoid risk of infection. Control access to media containing backups to avoid risk of tampering.

2.6 Software and Firmware Updates

System software and firmware updates may be offered from time to time. Ensure that your local representative has up to date contact details and periodically visit the NOTIFIER web site for up to date product information.

2.7 Computers and Access

Good security practice should be observed on any PC connecting to NOTIFIER equipment. Operating systems and software should be kept up to date by installing the manufacturers updates, as well as maintaining up to date anti-virus software on all computers which may be directly connected or via a network. Ensure that the computers are regularly scanned for viruses. Only allow files and software from trusted sources to be installed and used on associated computers to avoid malicious software installs. Use only authorized removable media, e.g. CD, DVD, external hard drives, USB memory sticks that have been scanned using up to date anti-virus software.

2.8 Networks, Firewalls & VPN Connections

Physical access to network nodes and infrastructure should be limited to authorized personnel to prevent tampering. Where enhanced system protection is desired, it is recommended to utilize conduit for network wiring (HS-NCM, NCM). Where access from untrusted networks is required, such as Internet access, **NOTIFIER strongly recommends** the use of a VPN to ensure the security of the connection.

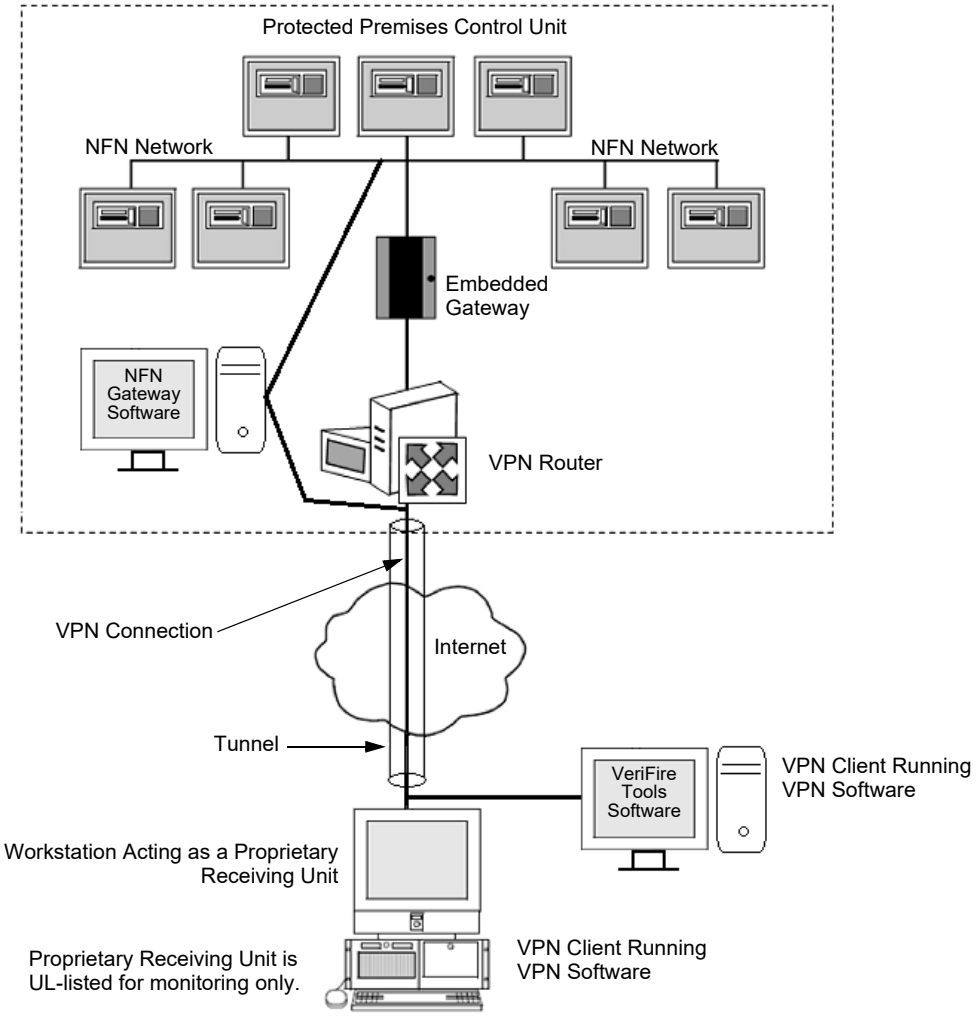
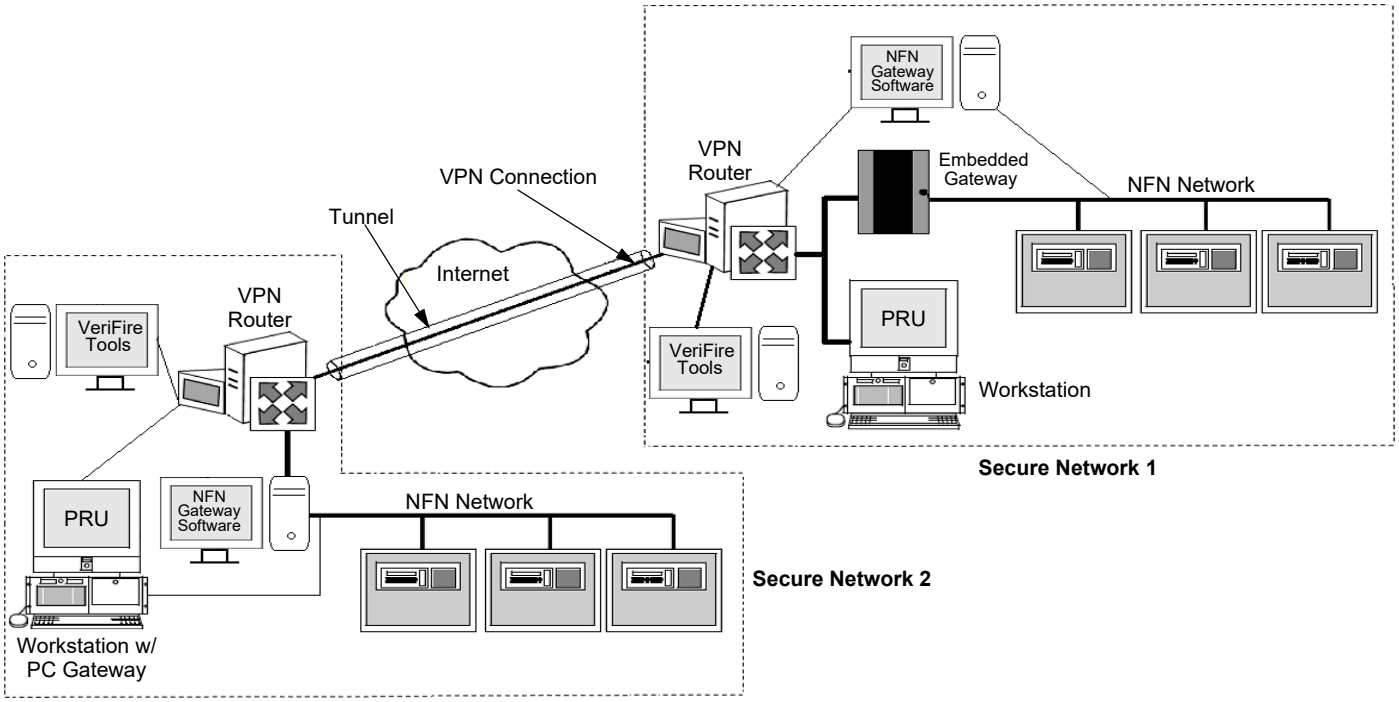
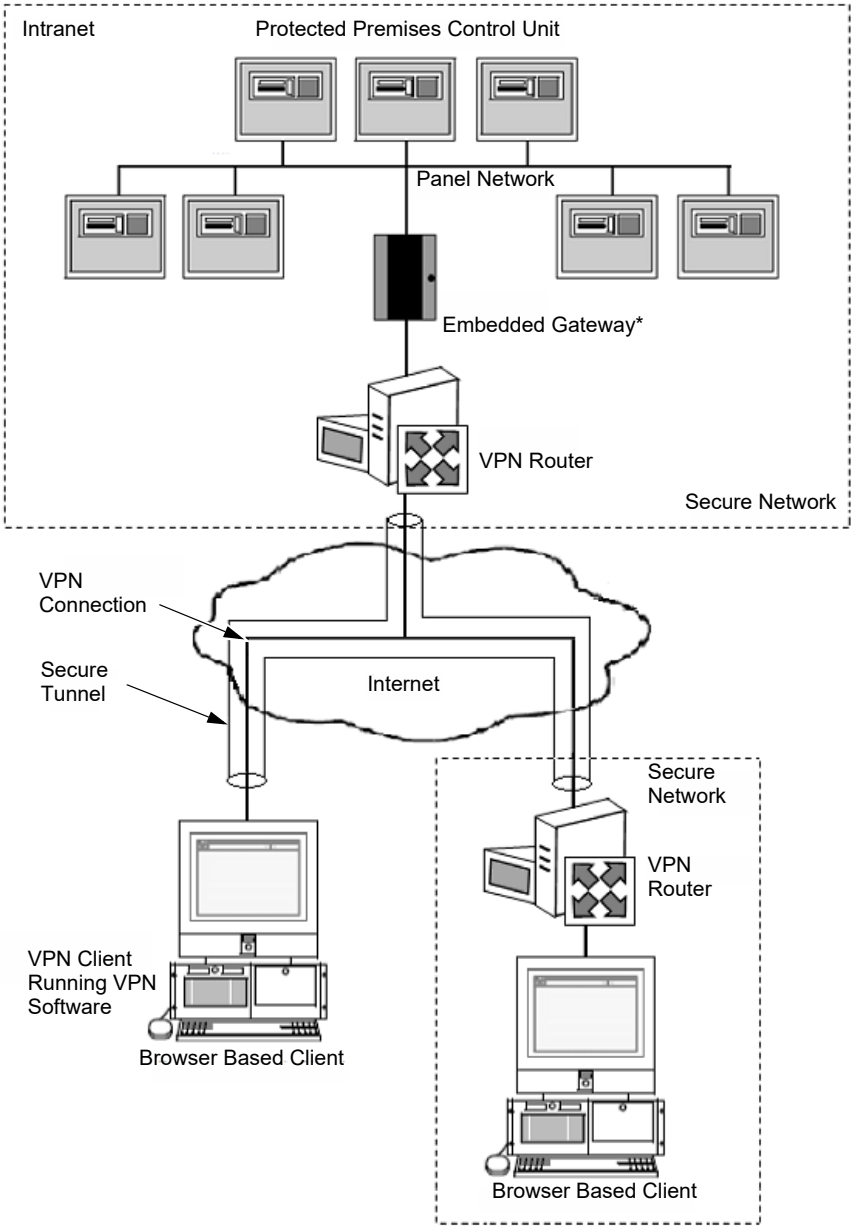


Figure 2.1 VPN Type 1



NOTE: VPN Software must be running on the Workstation/VeriFire Tools PC.

Figure 2.2 VPN Type 3



Note: *BACNET-GW-3, CAP-GW, LEDSIGN-GW, MODBUS-GW, NFN-GW-EM-3, and VESDA-HLI-GW

Figure 2.3 Embedded Gateway VPN Setup

2.9 VPN Setup

A Virtual Private Network (VPN) must be set up for any external (i.e. outside the site's intranet) communications including those for all gateways, the PC installed with VeriFire Tools, and remote workstations. A VPN protects the data from being seen or tampered with by bad actors via a secure connection across an insecure network such as the Internet. Set up a VPN as follows:

1. Use the VPN infrastructure provided by the IT department at your site.
2. Get the VPN services and respective credentials configured on the PCs with the help of the IT department.
3. Ensure that the VPN is turned-on (enabled) and running before starting or using any applications.
4. The end user or the commissioning engineer who configures the system should provide the following information to the IT department, so that these things are properly managed in the Firewall and/or VPN routers for external communications:
   - All the IP addresses and port information that are set up in the system such as the IP address of workstation(s), gateway-card(s) and any other IPs such as the time sync server, etc.
   - The workstation and VeriFire Tools IP port settings in the following table:

Setting	Port	Type	Direction	Purpose
Workstation	25	TCP	Out	SMTP
	123	UDP	In and Out	SMTP
	2004	TCP	N/A	(Internal) Workstation Plug-in Access
	2014	TCP	Out	Connection to DACR Gateway
	2017	TCP	Out	Connection to NFN Gateway
	2029	TCP	Out	Workstation Output Appliances (Signs)
	4016	TCP	In	Database Import/Export
VeriFire Tools	5000	TCP	Out	Connection to NFN Gateway

Table 2.1 IP Port Settings

2.9.1 Digital Signing

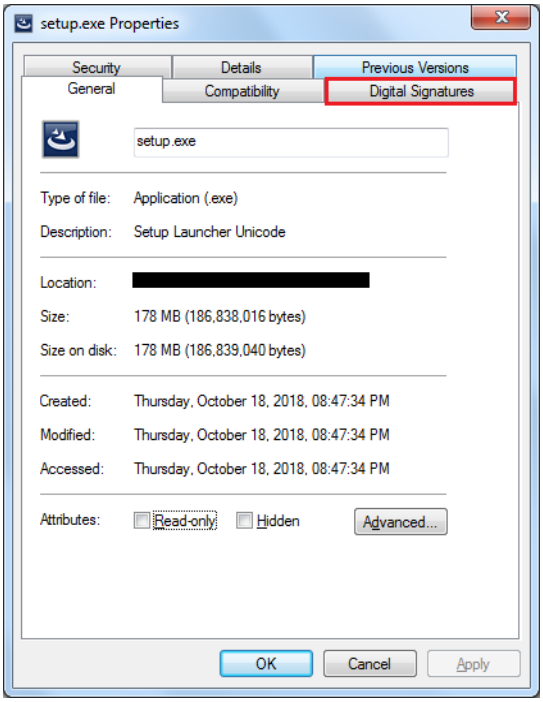
The application setup package is digitally signed using a certificate. A digital signature certificate is used to authenticate the identity of the sender/signer of a document/file and ensure that the original content of the document/file that has been sent is unchanged in transit.

The certification authority used for signing the product installer package is DigiCert® (DigiCert, Inc.).

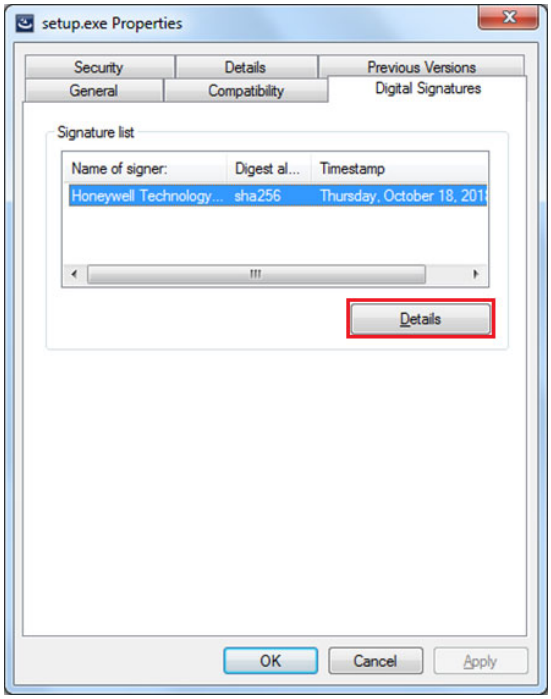
Website URL: www.digicert.com

If an installer package is digitally signed, perform the following steps:

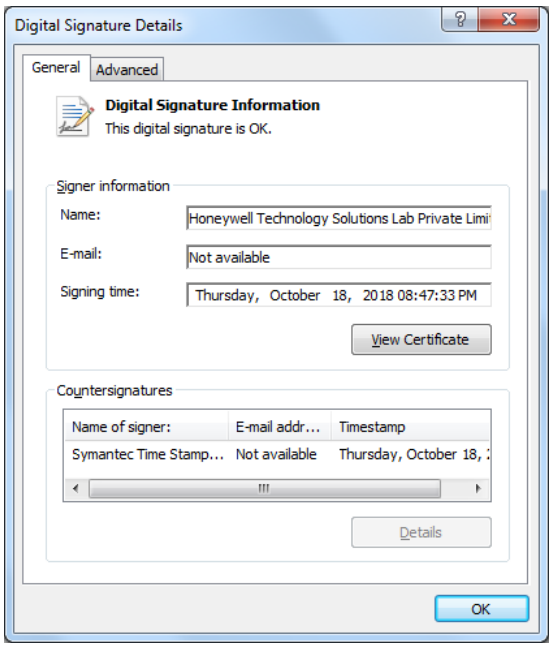
1. Right click the setup file and select **Properties**. Go to the **Digital Signatures** tab in the properties window. If you see signatures listed on the tab, you know that the file has been signed digitally.



2. Under Signature list, select the signature, and click **Details**.



3. You will see information regarding the Code Signing certificate that was used to sign the executable. On the next tab under **Countersignatures**, it will list an entry for a timestamping. If this field is blank, no timestamp exists on this code.



4. You may click on **View Certificate** to display the signature or click on the **Advanced** tab to display signature details as well.

Windows installer verifies the Digital Signatures of the installer packages before installing. To verify the signature manually, use the SignTool that comes with Windows SDK or the utility provided by DigiCert available for download at https://www.digicert.com/util/DigiCertUtil.exe.

Section 3: Product Information

CAUTION: CYBERSECURITY RISK
FAILURE TO COMPLY WITH THE RECOMMENDED SECURITY PRACTICES MAY PLACE YOUR SYSTEM AT RISK.

3.1 NCD/Fire Panels

The following Cybersecurity practice is highly recommended for the NCD/Fire Panels:

- When connecting VeriFire Tools to the NCD/Fire Panels, or connecting the NCD/Fire Panels to the NCM, visually inspect the USB and/or RS-232 port and cables to ensure it has not been tampered with as sensitive information is transmitted over these wires.

3.2 PC NFN Gateways

The following Cybersecurity practices are recommended for the PC NFN Gateways.

NFN-GW-PC-W, NFN-GW-PC-F, NFN-GW-PC-HNMF, NFN-GW-PC-HNSF, and NFN-GW-PC-HNW:

- The operating system should be set to download Windows updates, but not install them. This ensures that the update installation does not interfere with fire protection. A site-specific plan should be created that allows for the installation of the updates while minimizing impact to fire protection.
- Software updates should be installed as they become available. A site-specific plan should be created that allows for the installation of the updated software while minimizing impact to fire protection.
- Installation of any additional software is not recommended by Honeywell and requires the approval of the AHJ. If additional software is installed, a site-specific risk assessment should be performed to ensure the additional software does not compromise fire protection. If the additional software can restart the system, a plan must be developed to ensure fire protection is maintained.
- The IT infrastructure utilized for life safety communication should be physically or logically isolated from non-life safety infrastructure. Examples of such isolation could include a VLAN, VPN, or dedicated network. Refer to Figure 2.1, “VPN Type 1” on page 9 and Figure 2.2, “VPN Type 3” on page 10.

3.3 ONYXWORKS-WS

The following Cybersecurity practices are highly recommended for ONYXWORKS-WS:

- The operating system should be set to download Windows updates, but not install them. This ensures that the update installation does not interfere with fire protection. A site-specific plan should be created that allows for the installation of the updates while minimizing impact to fire protection.
- Workstation software updates should be installed as they become available. A site-specific plan should be created that allows for the installation of the updated software while minimizing impact to fire protection.
- An anti-virus program should be utilized with this system.
- Installation of any additional software is not recommended by Honeywell and requires the approval of the AHJ. If additional software is installed, a site-specific risk assessment should be performed to ensure the additional software does not compromise fire protection. If the additional software can restart the system, a plan must be developed to ensure fire protection is maintained.
- The IT infrastructure utilized for life safety communication should be physically or logically isolated from non-life safety infrastructure. Examples of such isolation could include a VLAN, VPN, or dedicated network. See Figure 2.1, “VPN Type 1” on page 9 and Figure 2.2, “VPN Type 3” on page 10.
- Each user of the workstation software should have their own user account so that actions taken by a user can be audited.
- The user accounts should be periodically reviewed to verify that users have the minimum access level required to perform their duties.
- The workstation database should be backed-up at regular intervals.

3.4 Embedded Gateways

The following Cybersecurity practices are highly recommended for Embedded Gateways BACNET-GW-3, MODBUS-GW, NFN-GW-EM-3, LEDSIGN-GW, CAP-GW, and VESDA-HLI-GW:

- Gateway application software updates should be installed as they become available. A site-specific plan should be created that allows for the installation of the updated software while minimizing impact to fire protection.
- The IT infrastructure utilized for life safety communication should be physically or logically isolated from non-life safety infrastructure. Examples of such isolation could include a VLAN, VPN, or dedicated network. See Figure 2.1, “VPN Type 1” on page 9, Figure 2.2, “VPN Type 3” on page 10, and Figure 2.3, “Embedded Gateway VPN Setup” on page 11.

3.5 NFC-50/100

The following Cybersecurity practices are highly recommend for the NFC-50/100:

- Install the NFC-50/100 panel in a secure location considering both software and hardware vulnerabilities.
- Change the default password to a unique password.
- Securely configure networks and firewalls.
- Develop a Disaster and Recovery Plan.
- Develop a Backup and Recovery Strategy.
- Install, configure, and maintain anti-virus software on all computers which access the panel.
- Keep the operating system updated and maintain version compatibility with the panel.
- Deliver all required system information upon delivery to the system owner.
- Train end-users on security maintenance tasks upon system delivery.
- For decommissioning, dispose of data securely.
- Ensure the Ethernet cable is removed from the NFC-50/100 when not being utilized for configuration.

3.6 Smart Wireless Integrated Fire Technology (SWIFT)

The following Cybersecurity practices are highly recommended when using SWIFT Tools:

- When using SWIFT Tools to update the firmware of the gateway or gateway devices, ensure updates are performed on a secure/encrypted Wi-Fi Network.
- Ensure the PC running SWIFT Tools has full disk encryption. Full encryption of any backed-up data is also recommended.
- The wireless gateway should be secured in a location which is only accessible to authorized personnel.
- When any SWIFT gateway or device is decommissioned from service, return the equipment to the factory default state.
- When installing or upgrading SWIFT Tools, be sure that the pop-up window “Do you want to allow this app to make changes to your device?” shows that the verified publisher is “Honeywell Technology Solutions Lab Private Limited” before selecting Yes. Otherwise, select “No” and contact Honeywell for a new SWIFT Tools installation package.

3.7 VeriFire Tools

CAUTION:

VERIFIRE TOOLS MUST BE CAUTIOUSLY USED ONLY BY TRAINED AND AUTHORIZED USERS OPERATING ON A PROTECTED LOCAL NETWORK.

The following Cybersecurity practices are highly recommended when using VeriFire Tools:

- Securely configure networks and firewalls.
- Install, configure, and maintain anti-virus software on all computers that access the panel.
- The IT infrastructure utilized for life safety communication should be physically or logically isolated from non-life safety infrastructure. Examples of such isolation could include a VLAN, VPN, or dedicated network. See Figure 2.1 on page 9 and Figure 2.2 on page 10.
- An anti-virus program should be used with this system.
- Installation of any additional software is not recommended by Honeywell and requires the approval of the AHJ. If additional software is installed, a site-specific risk assessment should be performed to ensure that the additional software does not compromise fire protection. If the additional software can restart the system, a plan must be developed to ensure fire protection is continued despite the restart.
- MS-Access database password protection is provided to protect against accidental damage. This would not provide protection against security researchers or targeted exploits.
- Develop a backup and recovery strategy.
- Develop a disaster and recovery plan.
- Ensure that an authorized person downloads the fire system firmware from the official website and that the same file is downloaded to the panel from VeriFire Tools by an authorized technician.

Manufacturer Warranties and Limitation of Liability

Manufacturer Warranties. Subject to the limitations set forth herein, Manufacturer warrants that the Products manufactured by it in its Northford, Connecticut facility and sold by it to its authorized Distributors shall be free, under normal use and service, from defects in material and workmanship for a period of thirty six months (36) months from the date of manufacture (effective Jan. 1, 2009). The Products manufactured and sold by Manufacturer are date stamped at the time of production. Manufacturer does not warrant Products that are not manufactured by it in its Northford, Connecticut facility but assigns to its Distributor, to the extent possible, any warranty offered by the manufacturer of such product. This warranty shall be void if a Product is altered, serviced or repaired by anyone other than Manufacturer or its authorized Distributors. This warranty shall also be void if there is a failure to maintain the Products and the systems in which they operate in proper working conditions.

MANUFACTURER MAKES NO FURTHER WARRANTIES, AND DISCLAIMS ANY AND ALL OTHER WARRANTIES, EITHER EXPRESSED OR IMPLIED, WITH RESPECT TO THE PRODUCTS, TRADEMARKS, PROGRAMS AND SERVICES RENDERED BY MANUFACTURER INCLUDING WITHOUT LIMITATION, INFRINGEMENT, TITLE, MERCHANTABILITY, OR FITNESS FOR ANY PARTICULAR PURPOSE. MANUFACTURER SHALL NOT BE LIABLE FOR ANY PERSONAL INJURY OR DEATH WHICH MAY ARISE IN THE COURSE OF, OR AS A RESULT OF, PERSONAL, COMMERCIAL OR INDUSTRIAL USES OF ITS PRODUCTS.

This document constitutes the only warranty made by Manufacturer with respect to its products and replaces all previous warranties and is the only warranty made by Manufacturer. No increase or alteration, written or verbal, of the obligation of this warranty is authorized. Manufacturer does not represent that its products will prevent any loss by fire or otherwise.

Warranty Claims. Manufacturer shall replace or repair, at Manufacturer's discretion, each part returned by its authorized Distributor and acknowledged by Manufacturer to be defective, provided that such part shall have been returned to Manufacturer with all charges prepaid and the authorized Distributor has completed Manufacturer's Return Material Authorization form. The replacement part shall come from Manufacturer's stock and may be new or refurbished. THE FOREGOING IS DISTRIBUTOR'S SOLE AND EXCLUSIVE REMEDY IN THE EVENT OF A WARRANTY CLAIM.

Warn-HL-08-2009.fm

NOTIFIER
12 Clintonville Road
Northford, CT 06472-1610 USA
203-484-7161
www.notifier.com

NOTIFIER®
by Honeywell