NOTIFIER®
by Honeywell

Modbus Gateway

MODBUS-GW

Installation and Operation Manual

Document LS10015-000NF-E Rev: C2
4/30/2019 ECN: 19-0599

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.

Telephone lines needed to transmit alarm signals from a premises to a central monitoring station may be out of service or temporarily disabled. For added protection against telephone line failure, backup radio transmission systems 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-D2-2016

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.

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 on-line help or manuals, please email us at FireSystems.TechPubs@honeywell.com.

On-Line Help – Please include the following information:

- Product name and version number (if applicable)
- Topic title
- The content you think should be corrected/improved
- Detailed suggestions for correction/improvement

Documents – Please include the following information:

- Document part number and title
- Page number and paragraph
- The content you think should be corrected/improved
- Detailed suggestions for correction/improvement

Please Note: If you have any technical issues, please contact Technical Services.

Manual Usage

This manual is written with the understanding that the user has been trained in the proper operations and services for this product. The information provided in this manual is intended to assist the user by describing the configurations and how they affect operations.

Table of Contents

Section 1 Product Overview

1.1 Operation

The MODBUS-GW provides a communication link between stand alone FACPs or FACPs communicating over an NFN or a high-speed NFN to a Modbus master application. The MODBUS-GW operates as a Modbus slave device.

1.2 Functionality

The MODBUS-GW:

- Communicates with the NFN network through an HS-NCM or NCM that is on that NFN network or a direct connection to a single FACP.
- Supports Modbus Application Protocol Specification V1.1b.
- Monitors up to 4 FACPs. Additional MODBUS-GWs may be added to an NFN network to accommodate additional FACPs.
- Supports a maximum of two Modbus masters.

1.3 Recommended Cybersecurity Practices

Highly recommended cybersecurity practices for the MODBUS-GW are specified in the *Cybersecurity Manual* (LS10217-000NF-E).

CAUTION: CYBERSECURITY RISK

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

1.4 Required Software

Chrome™ is required for use with the MODBUS-GW.

1.5 Environmental Requirements

This product meets the following requirements for operation:

- Temperature - 0°C to 49°C (32°F - 120°F)
- Relative Humidity - 93 ±2% non-condensing at 32 ±2°C (90 ±3°F)

However, it is recommended that this product be installed in an environment with a normal room temperature of 15-27º C (60-80º F).

1.6 IP Requirements

1.6.1 IP Port Settings

The following IP ports must be available to the MODBUS-GW:

Port	Type	Direction	Purpose
80	TCP	In	Web Based Configuration
443	TCP	In	HTTPS Communications
502	TCP	In	Modbus
4016	TCP	In	Upgrades

1.6.2 IP Restrictions

The following restrictions apply:

- The MODBUS-GW must have a static IP address. Dynamic Host Configuration Protocol (DHCP) is not supported.
- Web access via an HTTP proxy server is not supported.

1.7 Bandwidth Calculation

Use the following information to calculate the network bandwidth MODBUS-GW usage requires and how it will impact the network.

Table 1.1 Modbus TCP Request

Description	Bytes
Ethernet Header	14
IP Header	20
TCP Header	20
MBAP Header	7
Message—5 bytes Function code (1) **+** Start Address (2) **+** Quantity of Registers (2)	5
Total Bytes	*66*

Table 1.2 Modbus TCP Response

Description	Bytes
Ethernet Header	14
IP Header	20
TCP Header	20
MBAP Header	7
Message—Function code (1) + Byte Count (1) + Max 100 registers of each 2 Bytes (200)	202
Total Bytes	*263*

1.7.1 Calculating the Bandwidth Requirement

- One request and response pair requires 329 Bytes (66 + 263).
- If a client is polling at one second intervals, then request and response are both possible in one second.
- A request and response pair creates network traffic of 329 Bytes per second (329 **x** 1).
- In other words, a request and response pair creates network traffic of 2632 bits per second (329 **x** 8).
- Therefore, the network must be able to accommodate at least 0.0027 Mbps data flow.
- Once every five seconds, an analog request adds a small amount of network traffic.
- Formula for MODBUS-GW network bandwidth requirement based on polling rate:

  Bandwidth Requirement = (329 **x** (1000/**polling rate in milliseconds**) **x** 8) / (10^6) **Mbps**

1.8 System Architecture

An Internet or Intranet IP network connection is used with the architectures described in Figures 1.1 and 1.2.

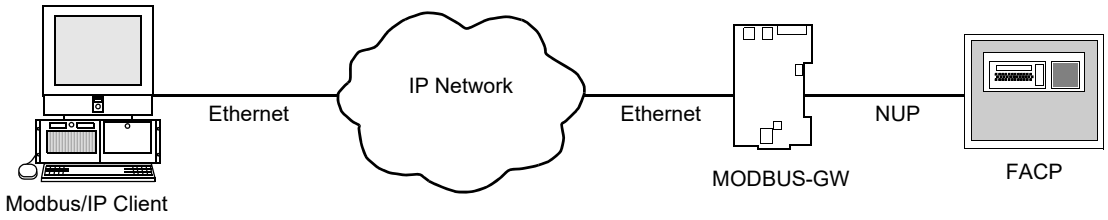


Figure 1.1 Single Panel Architecture

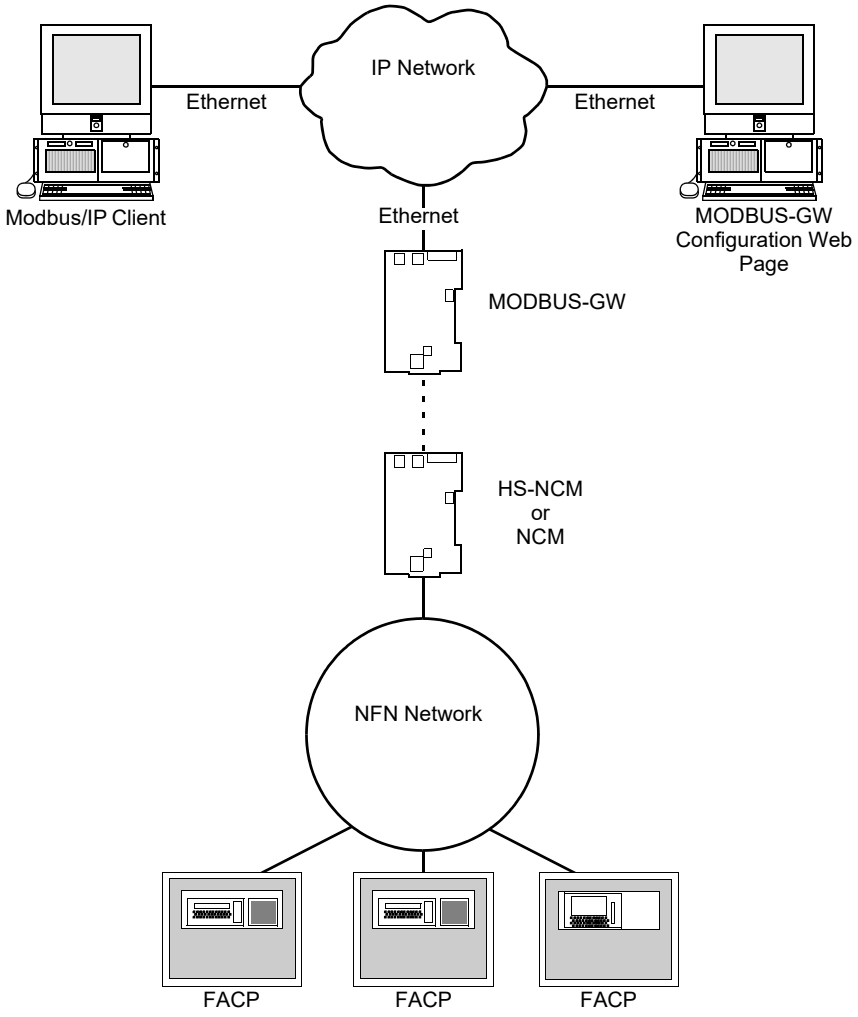


Figure 1.2 NFN Network Architecture

1.8.1 Redundancy

A redundant gateway is a second gateway which communicates with a Modbus client. The second gateway must have a separate and unique IP address from the first gateway. An example system is shown in Figure 1.3.

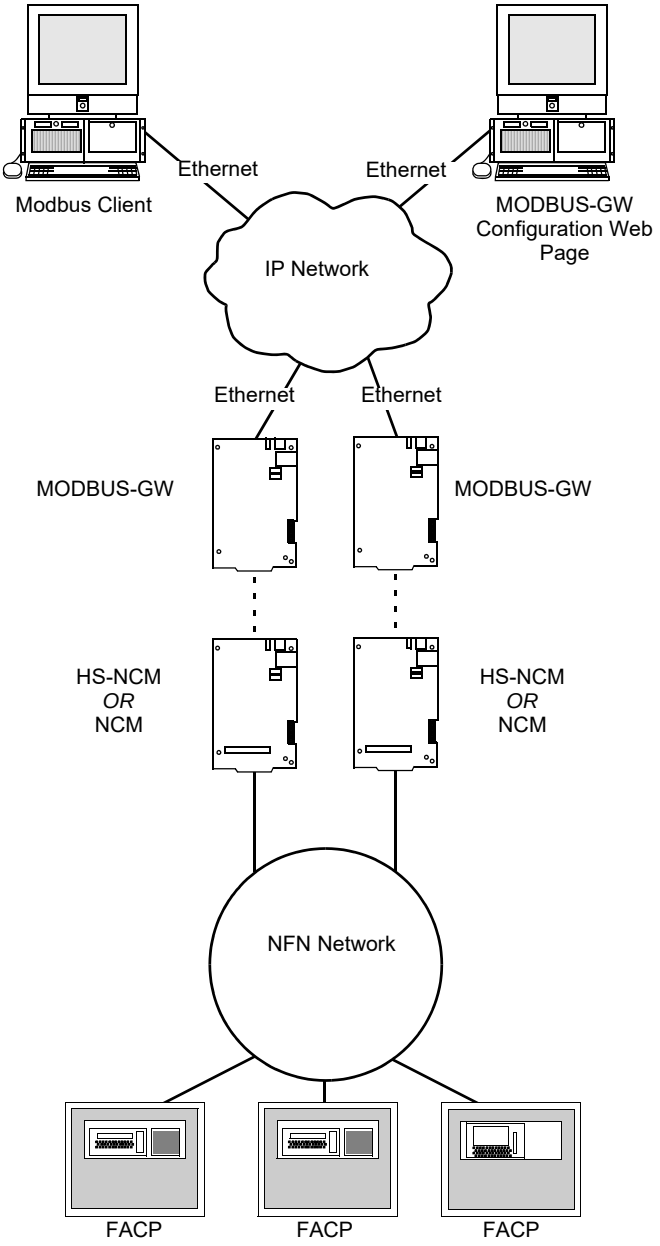


Figure 1.3 Redundant Modbus Gateways

1.9 Agency Listings

1.9.1 Standards

■ **Compliance** - This product has been investigated to, and found to be in compliance with, the following standards:

National Fire Protection Association

- NFPA 72 National Fire Alarm and Signaling Code

Underwriters Laboratories

- UL 864 Control Units for Fire Alarm Systems, Tenth Edition
- UL 2017 General Purpose Signaling Devices and Systems, Second Edition
- UL 2572 Mass Notification Systems, Second Edition

Underwriters Laboratories Canada

- CAN/ULC S527-11 Standard for Control Units for Fire Alarm Systems, Third Edition
- CAN/ULC S559-13 Standard for Equipment for Fire Signal Receiving Centres and Systems, Second Edition

■ **Installation** - This product is intended to be installed in accordance with the following:

Local

- AHJ Authority Having Jurisdiction

National Fire Protection Association

- NFPA 70 National Electrical Code
- NFPA 72 National Fire Alarm and Signaling Code
- NFPA 101 Life Safety Code

Underwriters Laboratories Canada

- CAN/ULC S524 Installation of Fire Alarm Systems
- CAN/ULC S561 Installation and Services for Fire Signal Receiving Centres and Systems

Canada

- CSA C22.1 Canadian Electrical Code, Part I, Safety Standard for Electrical Installations

1.9.2 Agency Restrictions and Limitations

- MODBUS-GW is UL 864 listed for supplementary use only.
- MODBUS-GW is UL 2572 listed for supplementary use only and cannot be used to trigger mass notification announcements.

1.10 Compatible Equipment

The MODBUS-GW is compatible with the following equipment:

Table 1.3 Compatible Equipment

Type	Equipment
Fire Panels:	• NFS-320 • NFS2-640 • NFS2-3030
Network Cards:	• NCM-W, NCM-F • HS-NCM-W, HS-NCM-SF, HS-NCM-MF, HS-NCM-WSF, HS-NCM-WMF, HS-NCM-MFSF
Gateways:	• NFN-GW-EM-3 • PC NFN Gateways: – NFN-GW-PC-F – NFN-GW-PC-W – NFN-GW-PC-HNMF – NFN-GW-PC-HNSF – NFN-GW-PC-HNW
Other Products:	• BACNET-GW-3 • DVC • NCA-2 • NCD • NWS-3 • VESDA-HLI-GW

1.11 PCB Board Type Supported by Software Version 4.30 and Later

Software version 4.30 and later does not support EMPCA board types. Only EMPCB board types are supported.

Section 2 Installation

2.1 Required Equipment

2.1.1 MODBUS-GW Assembly:

The following components are shipped with the MODBUS-GW:

- MODBUS-GW Printed Circuit Board
- Surge Suppressor (P/N PNET-1)
- NUP-to-NUP Cable (P/N 75577) - Used to connect the MODBUS-GW board to an NCM-W or NCM-F board or supported panel.
- Wire Leads-to-NUP Cable (P/N 75583) - Used to connect 24V power from the MODBUS-GW board to an NCM-W or NCM-F board.
- USB Cable (P/N 75665) - Used to connect the MODBUS-GW board to an HS-NCM board:
  - HS-NCM-W
  - HS-NCM-MF
  - HS-NCM-WMF
  - HS-NCM-SF
  - HS-NCM-WSF
  - HS-NCM-MFSF

2.1.2 Network Components:

- High-speed Network Communication Module (HS-NCM) - Used to facilitate network communication between the MODBUS-GW and a high-speed NFN network (sold separately).

  OR

- Network Communication Module (NCM) - Used to facilitate network communication between the MODBUS-GW and an NFN network (sold separately).

  OR

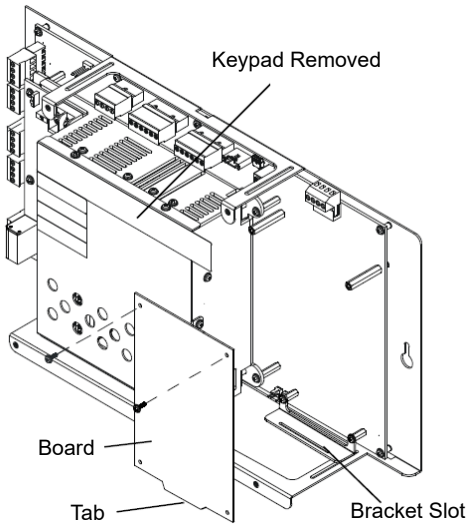
- Compatible FACP with NUP port.

2.1.3 Customer Supplied Equipment:

- Computer - Used to run a web browser to configure the MODBUS-GW. Refer to 1.4, "Required Software" for recommended browsers.
- Ethernet Patch Cable - Used for connecting to the Local Area Network (LAN).

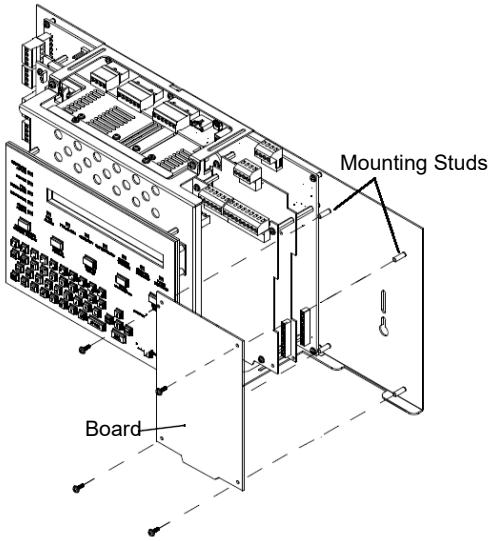
2.2 Board Installation

The MODBUS-GW may be installed in a CAB-3 or CAB-4 cabinet as shown below.



Install bracket on 1/2” standoffs. Place the board’s tab in the bracket slot and screw the board to the top of the standoffs. May be stacked in front of or behind another board using standoffs of adequate length to clear the rear board.

Figure 2.1 NFS-320 Series Installation



Mount in 4th column of the NFS2-640 Series chassis. Mount chassis to backbox before installing the board in rear position. May be mounted in front of another board using standoffs of adequate length to clear the rear board.

Figure 2.2 NFS2-640 Series Installation

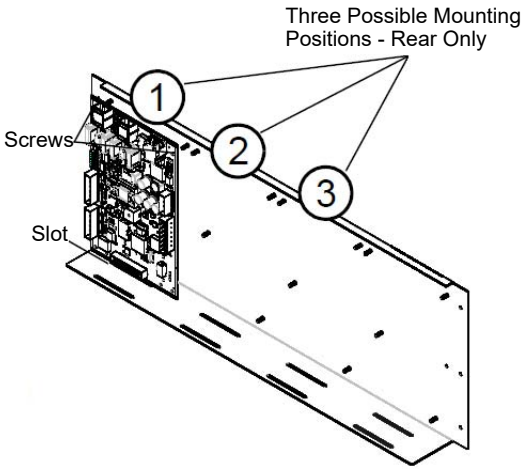


Figure 2.3 CHS-4L Installation

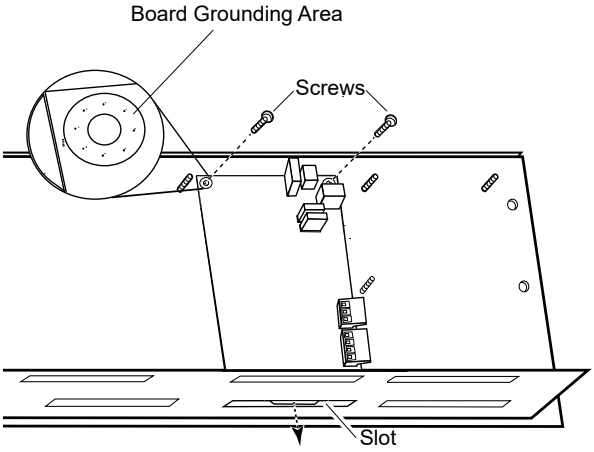


Figure 2.4 Securing the Board

2.3 Connections

2.3.1 Connecting the MODBUS-GW

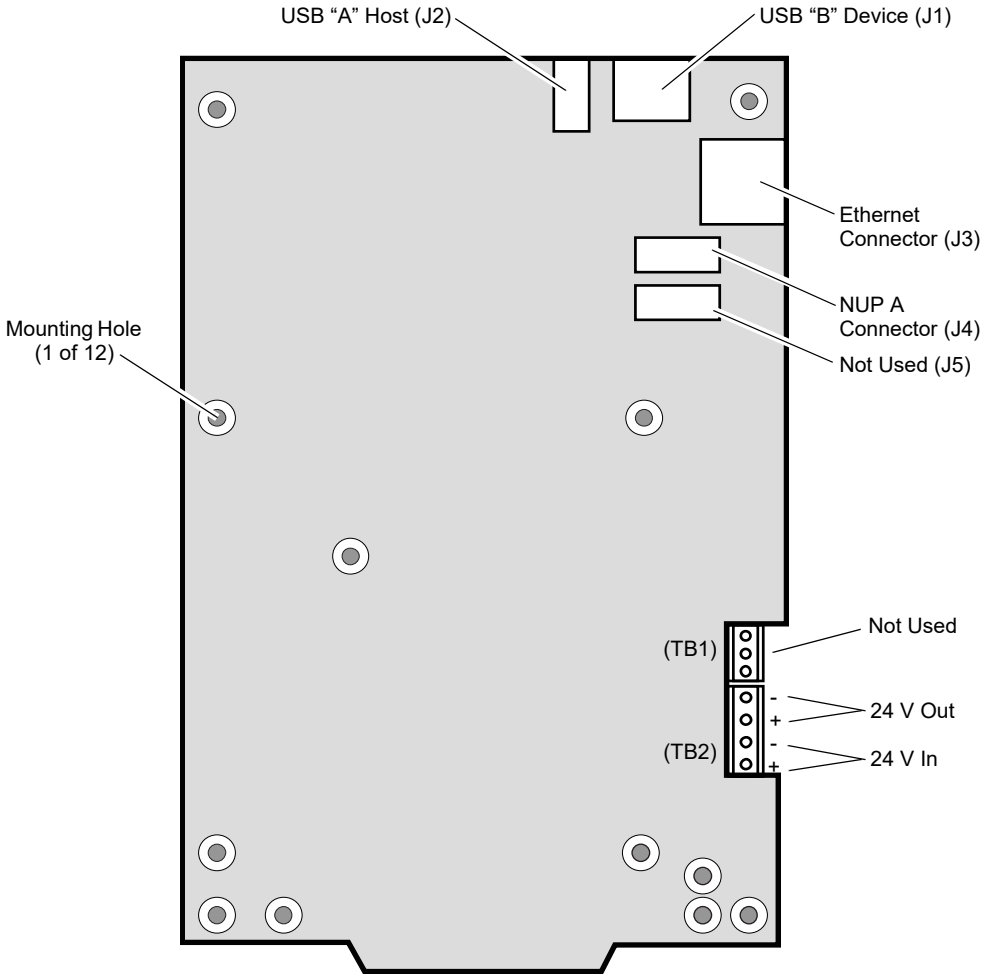


Figure 2.5 MODBUS-GW Connections

Table 2.1 Connection Specifications

Reference Designator	Description	Circuit Class	Specifications
TB2	DC Power	2	Power Source - FACP or UL 1481 listed 24 VDC regulated power supply Nominal Voltage: 24 VDC, Regulated Current: 125 mA Locate in same cabinet or use close nipple fitting
J1	USB B	2	Locate in same cabinet or use close nipple fitting
J2	USB A	2	Locate in same cabinet or use close nipple fitting
J3	Ethernet	2	Line Impedance 100 ohm Max Distance 328.083 ft. (100 m)
J4	NUP A	2	RS-232 Locate in same cabinet or use close nipple fitting
• All wiring from the power supply is power limited, and a separation of at least 1/4-inch (6.35 mm) must be maintained between power limited and non-power limited wiring. • All interconnects are power limited. • Ethernet connections are power limited and supervised except for ground faults.			

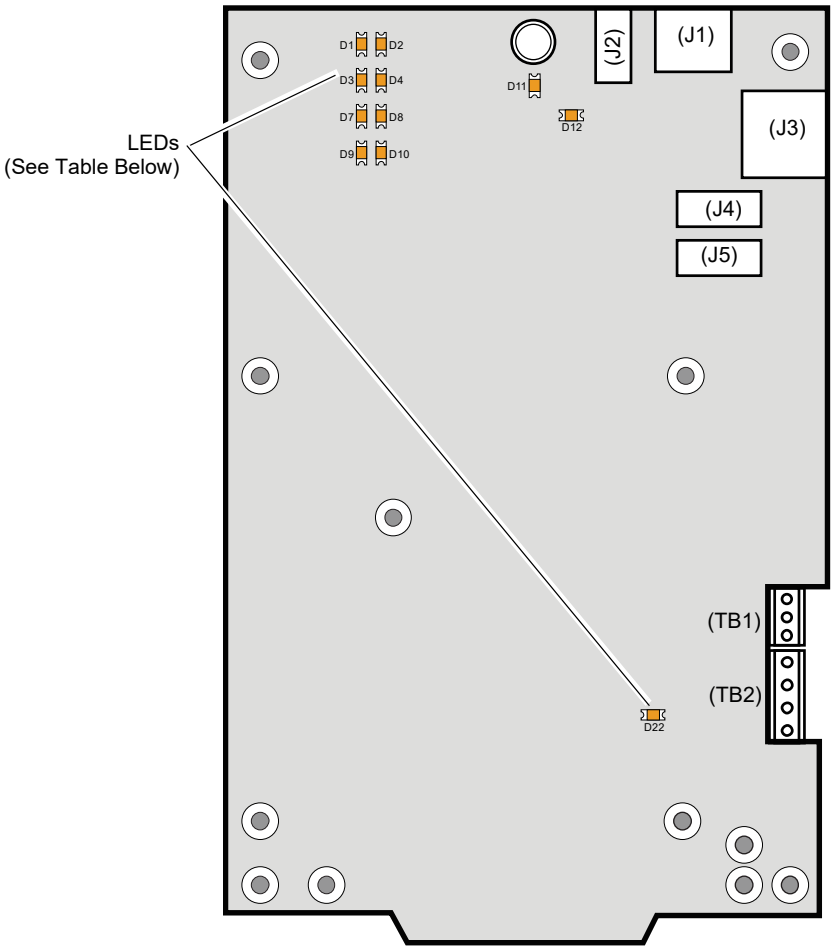


Figure 2.6 MODBUS-GW LEDs

Table 2.2 LED Definitions

Reference Designator	Label	Description
D1	ACTIVE	Active/Lit indicates that WinCE is running.
D2	NUPA RX	Blinks when data is received on the NUP A port (J4).
D3	PROGRAM	Not Used
D4	NUPB RX	Not Used
D7	USB B	Active/Lit indicates a device is connected to the USB B port (J1).
D8	NUPA TX	Blinks when data is sent on the NUP A port (J4).
D9	USB A	Active/Lit indicates a device is connected to the USB A port (J2).
D10	NUPB TX	Not Used
D11	DATA	Blinks to indicate data transmission to or from the Ethernet port (J3).
D12	LINK	Active/Lit indicates an Ethernet connection.
D22	WDT FAIL	Active/Lit indicates the system has undergone a reset due to a Watchdog circuit activating.

2.3.2 Connecting to a Standard NCM

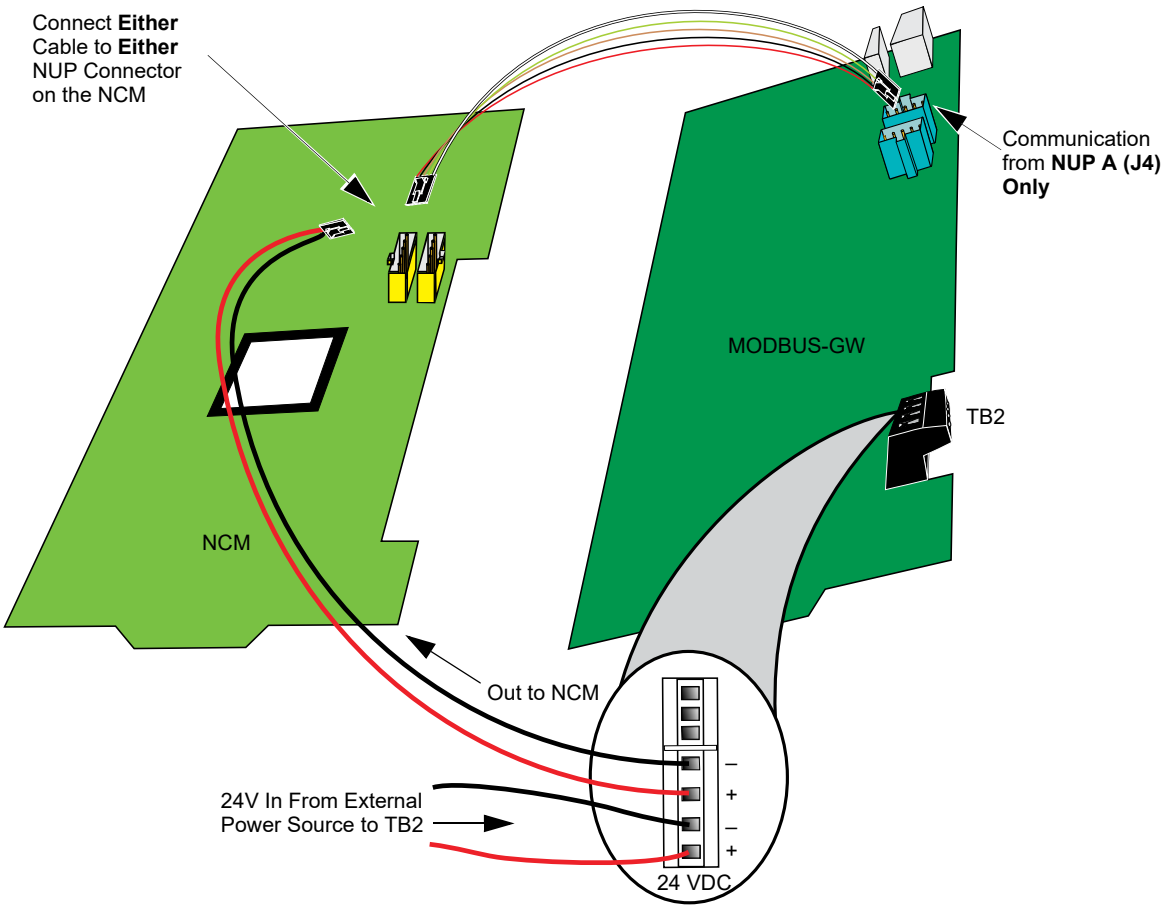


Figure 2.7 Routing Power and Communication to a Standard NCM

Table 2.3 Standard NCM Connections

Type	Connection
NCM-W	Twisted pair wire
NCM-F	Fiber-optic cable

2.3.3 Connecting to an HS-NCM

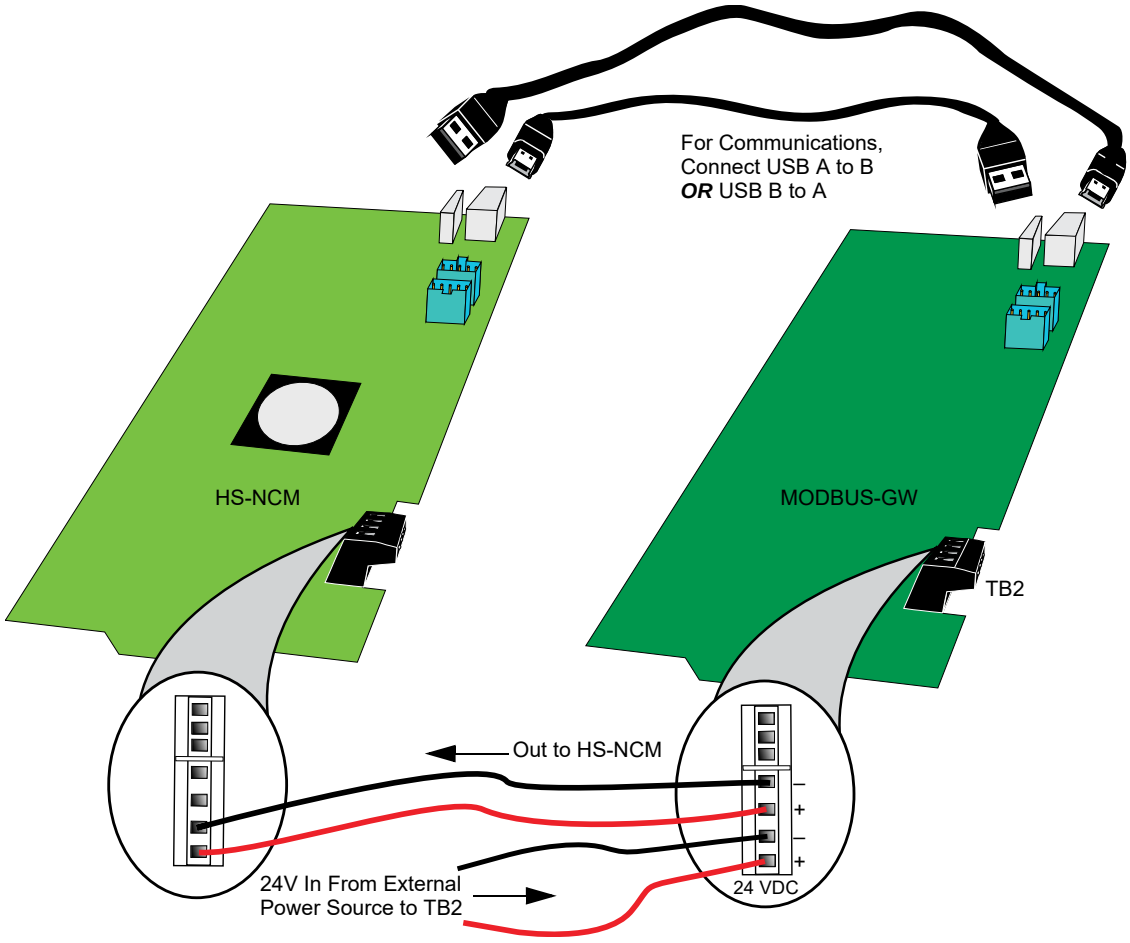


Figure 2.8 Routing Power and Communication to an HS-NCM

Table 2.4 HS-NCM Connections

Type	Connection
HS-NCM-W	Twisted pair wire
HS-NCM-SF	Single mode fiber-optic cable
HS-NCM-MF	Multimode fiber-optic cable
HS-NCM-WSF	Twisted pair wire, Single mode fiber-optic cable
HS-NCM-WMF	Twisted pair wire, Multimode fiber-optic cable
HS-NCM-MFSF	Multimode fiber-optic cable, Single mode fiber-optic cable

2.3.4 Connecting to a Fire Alarm Control Panel (FACP)

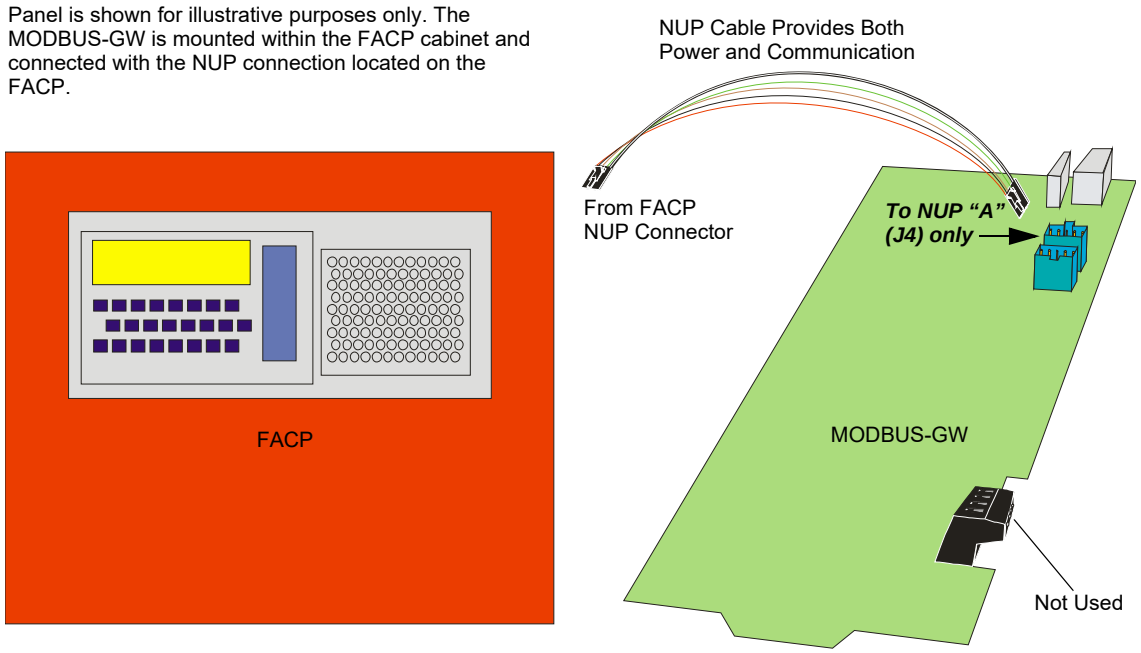


Figure 2.9 Connecting to an FACP

2.3.5 Connecting to the PNET-1 Surge Suppressor

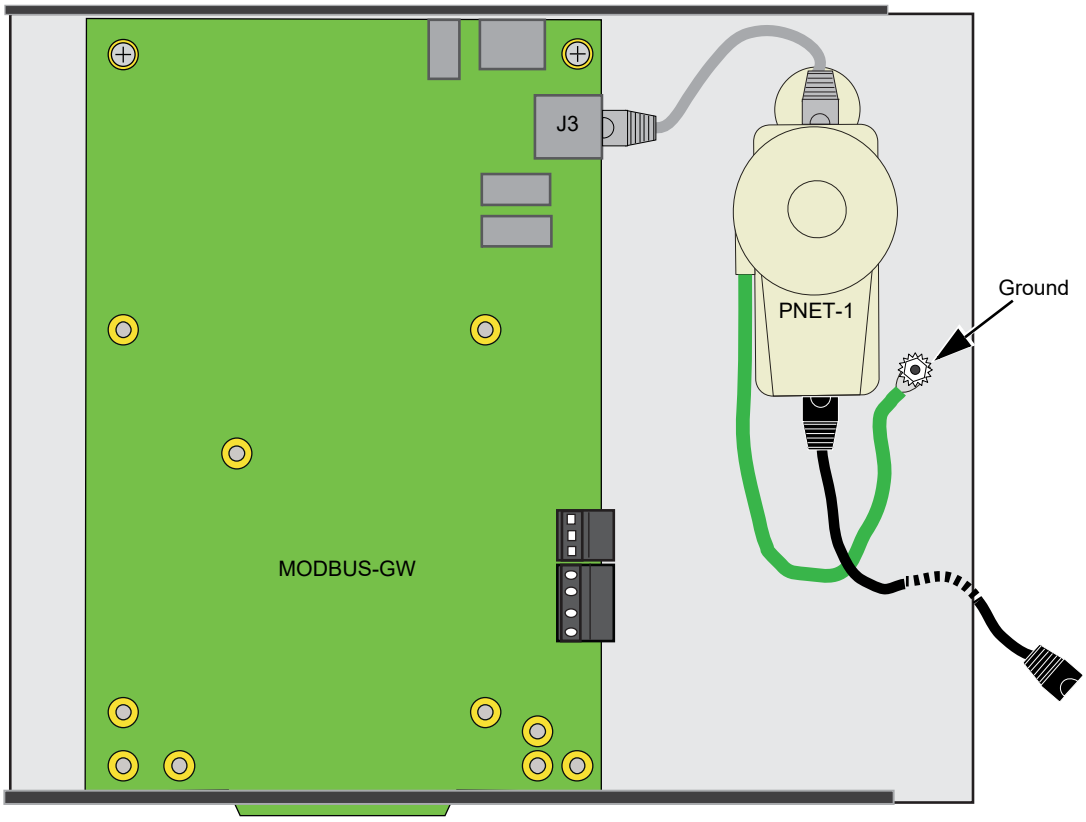


Figure 2.10 Connecting to the PNET-1

2.4 System Power

Table 2.5 Power Requirements

Power	Requirement
Input Voltage (Nominal)	24 VDC
Input Current @ 24 VDC	125 mA

2.5 Testing and Maintenance

Testing and maintenance should be performed according to the *Testing and Maintenance* section of NFPA-72 and CAN/ULC S536.

Section 3 Configuration

3.1 Configuration Web Page

Configuration of the MODBUS-GW is through a web page running on the MODBUS-GW. Supported web browsers are listed in 1.4, "Required Software".

The following information applies to IP settings:

- Each MODBUS-GW is shipped with a default IP address of 192.168.1.2 and a default node number of 240.
- The computer used to configure the MODBUS-GW must be able to establish an IP connection to the gateway. Consult with a network administrator if unsure how to make this connection.
- Connecting more than one MODBUS-GW prior to reconfiguring the IP address will result in an IP address conflict.
- Refer to Appendix A, "Gateway Settings" for instructions on resetting and reviewing the IP settings of the MODBUS-GW.

3.2 Configuring the MODBUS-GW

3.2.1 Logging into the Web Page

Log into the MODBUS-GW as follows:

1. Start the web browser.
2. Navigate to the IP address of the gateway **(default http://192.168.1.2)**.
3. If a security warning appears, select the option to continue anyway. Refer to 3.3, "Security Certificate" for more information.
4. Log into the web page:
   a. If the password has already been established, enter the password and click **OK**.
   b. If any of the following conditions is true, go to Step 5:
      - A new gateway from the factory.
      - An upgrade of a gateway from a previous version for which the password has not been set (i.e. still using the default password).
      - After a factory reset of the gateway.
5. To set a new password:
   a. Enter the default password, 00000000 (eight zeros) and click **OK**. The Set Device Password dialog box appears.
   b. Reenter the default password.
   c. Enter a new password.
   d. Reenter the new password to confirm.
   e. Click **OK**.

3.2.2 Basic Configuration Tool Layout

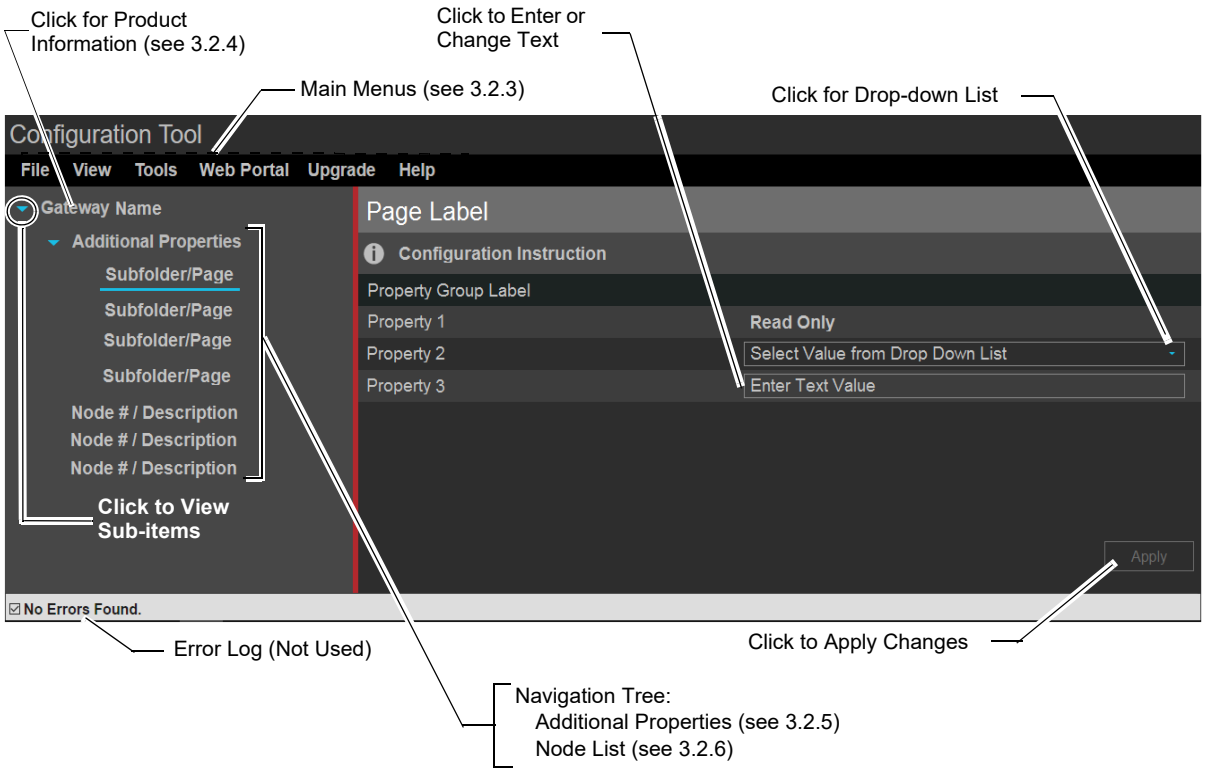


Figure 3.1 Basic Configuration Tool Layout

3.2.3 Main Menus

The following table describes the options available in the configuration tool main menus (see Figure 3.1).

Table 3.1 Main Menus

Menu	Option	Description
File	Reboot	Reboots the MODBUS-GW.
View	Refresh Node List	Refreshes the node list in the MODBUS-GW navigation tree.
	Connected Clients	Opens the Connected Clients screen. This screen displays IP addresses for Modbus clients connected to the MODBUS-GW.

Table 3.1 Main Menus *(Continued)*

Menu	Option	Description
Tools	Set Device Password	Displays a dialog box allowing the user to change the current password. • Passwords are case sensitive. • Alpha and numeric characters are supported. • Eight (8) characters minimum, 64 characters maximum. • Default: 00000000 (eight zeros)
	Backup...	Click to download a backup file (.bkp) from the gateway to the PC running the browser. Save or move the file to an appropriate location so it can be used, if necessary, to restore the gateway settings.
	Restore...	Browse to (or search for) the backup file on the PC running the browser. Click **Open** and then **Send**. An on-screen message indicates a successful restoration.
	Send PFX Key File	Opens a dialog box allowing the user to upload an SSL Certificate File. Browse for the file, enter the password (if required), and click **Send**. Refer to 3.3, "Security Certificate".
	Control	Displays a dialog box allowing the user to enable the Control feature. Note: UL certification is voided if Control is enabled.
	Create CSV Report	Downloads a comma separated value (CSV) register map report in standard file format to the PC running the browser. Hover over the label and select one of the following options: • **With All Points** – The report contains information about all possible points on all configured panels on the network. • **With Actual Points** – Recommended. The report contains detailed information about only the points that are configured and mapped on the network. Once downloaded, the user can access the file.
Upgrade	Firmware	Opens the Send Archive File dialog box. Click the **Choose** button and select the filename that begins with "**MGNUW**" and has the extension".AR". Click **Open** and then click **Send**. An on-screen message indicates a successful upgrade. It is recommended that the browser be restarted after the upgrade.
Help	Legal	Displays legal information pertaining to the MODBUS-GW.
	About	Displays software version information.
	Advance Diagnostics	Used for informational/diagnostic purposes.

3.2.4 Product Information

The following information displays when initially opening the configuration tool. It may also be accessed by clicking the first entry in the navigation tree (see Figure 3.1).

Table 3.2 Product Information

Property	Value
Type	Displays the gateway type by name.
Version	Displays the gateway version number.
Board Type	Displays the hardware model type.
Kernel Version	Displays additional software version information.
Boot Version	Displays additional software version information.

3.2.5 Additional Properties

The following table describes the options available under Additional Properties in the navigation tree (see Figure 3.1). After configuring the settings, click **Apply** in the lower-right corner of the window.

Table 3.3 Additional Properties

Navigation Tree Label	Property	Value
IP Address Settings	**IP Address Settings**	
	IP Address	Enter the IP address of the MODBUS-GW. (Default is 192.168.1.2) Note: If a new IP address is entered, the user must enter the new IP address in the browser address bar to log into the gateway at its new address.
	Subnet Mask	Enter the subnet address of the MODBUS-GW. (Default is 255.255.255.0)
	IP Gateway	Enter the IP address of the default gateway for the host network. (Default is 0.0.0.0)
	MAC Address	Displays the Media Access Control (MAC) address of the gateway Ethernet port and is not configurable.
NFN Settings	**General Information**	
	Connection Port	Displays the type of connection port used (Serial, USB, etc.).
	Connection Type	Displays how the gateway is connected to the NFN.
	NCM Version	Displays the NCM version number. Note: This property does not appear when there is no NFN connection.
	NCM Status Bits	Displays the NCM status, which can be: Piezo, UPS Failure, Network Fail Port A, Network Fail Port B, High Speed Audio, NCM Sniffer Mode Active, Local Connection Limit Exceeded, or None. Note: This property does not appear if there is no NFN connection.
	Fire Network Time Policy	Displays “Unsynced” since MODBUS-GW does not synchronize time with the network.
	Node Settings	
	Node	Enter the NFN node number of the MODBUS-GW. (Default is 240)
	Panel Label	Enter the panel label.
	Network Settings	
	Channel A Threshold	• Select **High** for a high-noise NFN network. • Select **Low** for a low-noise NFN network.
	Channel B Threshold	• Select **High** for a high-noise NFN network. • Select **Low** for a low-noise NFN network.
	Class X	• Select **Yes** for a Class X SLC (Signaling Line Circuit) configured NFN network. • Select **No** for a Class B SLC configured NFN network (default).

Table 3.3 Additional Properties *(Continued)*

Navigation Tree Label	Property	Value
Node Mapping	**Node Mapping**	
	Authorized Client IP	This is an optional security feature. The options are: • Enter the authorized client IP address. The gateway only responds to requests from the client at that IP – no other Modbus clients may communicate with the gateway. However, any computer running a browser in the local network will still be able to access the MODBUS-GW configuration web page as normal. • Leave the field blank to allow any client to request data. The MODBUS-GW only communicates with one client at a time. Once MODBUS-GW accepts a client's request to connect, it does not accept any other request to connect until the original client has disconnected.
	Gateway Unit ID	Displays the unit ID that the MODBUS-GW uses in the Modbus network. This is a configurable property of the nodes. By default, the Modbus Unit ID for a monitored node is set to be the same as the NFN Node ID. If for any reason the unit ID needs to be changed, click the value and enter the new unit ID number. Since each unit ID in the Modbus network needs to be unique, change this number only if there is a conflict in the unit IDs in the Modbus network. Note: Each of the 240 possible nodes on the NFN network (except for gateways, web servers, and DVCs) is automatically assigned a Modbus Unit ID. When a new unit ID number for a node is entered, the old unit ID number is reassigned to whichever node previously used the new unit ID number. However, the MODBUS-GW configuration web page does accept a new unit ID number that is currently being used by a monitored node. In order to reassign a unit ID number used by a monitored node, first assign a new unit ID number for the monitored node.
	Analog Value Timeout	Enter the minimum frequency (in seconds) at which the MODBUS-GW expects to receive continuing polls from clients seeking analog values from 4-20 mA devices. When a client that had been polling a set of analog values fails to re-poll the values within the time out period, the MODBUS-GW stops polling the points in question. Once the time out period expires without the MODBUS-GW receiving a repeated poll, any further poll received will be treated as a new poll, and the first read will be considered an initialization read (for more information, refer to "4.4, "Analog Values and Trending". (Default is 20 seconds)
	Show Online or Mapped Nodes - Show All Nodes	The property label toggles between "Show All Nodes" and "Show Online or Mapped Nodes" depending on the mode selected. Select **Yes** to display the list of nodes in the mode indicated by the property label.

Table 3.3 Additional Properties *(Continued)*

Navigation Tree Label	Property	Value
Node Mapping *(Continued)*	**Node**	
	Node List	**Node Column** Displays the node numbers and names of nodes on the NFN network. **Monitored Column:** • Select **Yes** to monitor the node. • Select **No** if the node is not to be monitored. **Unit ID Column:** Displays the unit ID that the node uses on the Modbus network. If for any reason the node unit ID needs to be changed, click the value and enter the new Modbus network unit ID number (1-255). Since each unit ID in the Modbus network needs to be unique, change this number only if there is a conflict between unit IDs in the Modbus network. If a unit ID number is changed to a number already assigned to another node, the node currently having that unit ID number swaps the unit ID number with the node that was changed. Example: The node assigned Unit ID #214 is changed to be Unit ID #5. The result is that the node that was Unit ID #214 is now #5 and the node that was Unit ID #5 is now #214. However, the MODBUS-GW configuration web page does accept a new unit ID number that is currently being used by a monitored node. In order to reassign a unit ID number used by a monitored node, first assign a new unit ID number for the monitored node. **Notes:** • The “Unknown” nodes can only be seen in “Show All Nodes” mode. • If an “Unknown” node comes on line and is found to be of the wrong type for the MODBUS-GW to monitor, its Monitored field is automatically set to “No”. • Some nodes in the node list are not usable by the MODBUS-GW and therefore are not configurable and do not have a unit ID.

3.2.6 Node List

Click the desired node label in the navigation tree area of the configuration tool screen (see Figure 3.1) to view information about that node. The information displayed is dependent on the node type. Labels for off-line nodes display in red text.

Since the MODBUS-GW monitors itself, it also appears as a monitored node in the navigation tree. The MODBUS-GW may be listed as a BACnet Gateway in the navigation tree. As described in Table 3.4, the MODBUS-GW displays general register mapping information only, since unlike FACPs it does not connect directly to network points.

Table 3.4 Node List Display

Property	Value
Node	Displays the NFN network node number of the monitored node.
Version	Displays software version information about the monitored node and the devices used to connect it to the NFN network.
Register Information	Displays register address information for the monitored node. If the “Register Type” property displays, click the field and select how register information is displayed from the drop-down list. The options are: **Analog Value** – Displays a map of the registers storing the analog values from 4–20 mA modules, if any, connected to the node. **Device Type** – Displays a map of the registers storing device type information for points attached to the node. **Status** – Displays a map of the registers storing status information for points attached to the node.

3.3 Security Certificate

The MODBUS-GW communicates with the browser using secure communications facilitated by a self-signed security certificate. Using the self-signed security certificate will cause the browser to display warnings similar to the following:

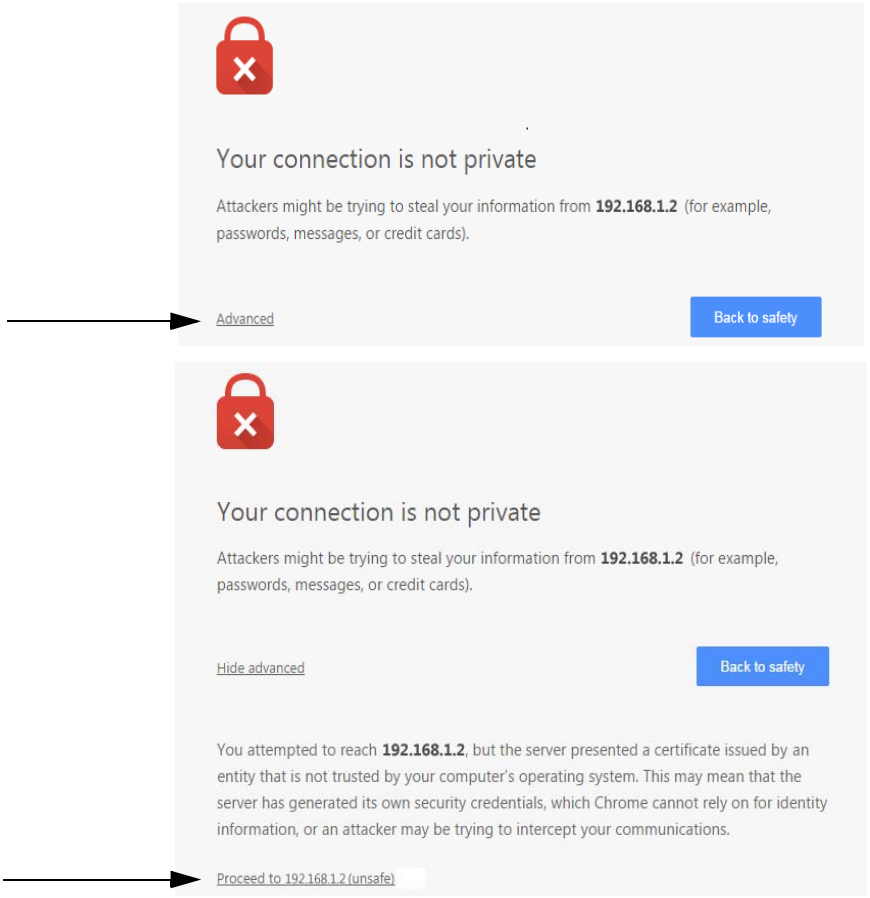


Figure 3.2 Chrome Security Warning Example

The browser warning is displayed upon each connection to the gateway. The warning may be removed by obtaining a security certificate from a security authority. The certificate may originate from a local certificate authority or a commercial certificate authority if the gateway is directly connected to the Internet with a unique IP address. Regardless of which type of certificate authority is selected, the IP address of the gateway must be provided. The certificate is specific to the specified IP address. If the IP address is changed, a new certificate will be required. In addition, the certificates have an expiration date. Once the certificate expires, a new certificate needs to be sent to the gateway. If the certificate expires, a different warning is displayed by the browser.

The security certificate must be in the PFX format. The PFX file is uploaded to the gateway using the **Tools > Send PFX Key File** option in the gateway configuration tool. It may be necessary to install a file on each PC used to configure the gateway to fully resolve the security configuration.

The MODBUS-GW includes a self-signed security certificate. The certificate is generated with a three year expiration. In addition, the certificate is generated using the default IP address of the gateway, 192.168.1.2. A certificate authority may be used to create a valid certificate based on the IP address of the MODBUS-GW. If a certificate authority is not available, a local IT administrator may use a security certificate generation application such as OpenSSL to generate the certificate.

The site network administrator may be able to assist with any additional details regarding security certificates.

Section 4 Operation

4.1 Panel and Gateway Synchronization

When making programming changes to a panel, it is important to verify that the MODBUS-GW has synchronized with these changes. This assures reliable data from the gateway. There are several ways in which a MODBUS-GW synchronizes with a panel:

- The gateway attempts to compare its database with the panel database every 24 hours. If there is a difference, the gateway synchronizes with the panel.
- If the gateway receives a message from the panel that it has been reprogrammed through a programming tool or from the front panel, the gateway will attempt to resynchronize.
- If the gateway is reset, the power is cycled or the panel connectivity is lost and reapplied.

Resynchronization includes the following processes:

- The gateway updates all of its device type registers to match the panels.
- The gateway updates the device status registers to ensure the gateway provides accurate state data.

If the panel and panel network are not completely stable while the gateway is resynchronizing, the gateway aborts resynchronization.

4.2 Modbus Command Support

4.2.1 Modbus Commands

The MODBUS-GW supports the following Modbus commands:

- Read Input Registers (0x04)
- Read Holding Registers (0x03)
- Write Single register (0x06)
- Read Device Identification supported 43 / 14 (0x2B / 0x0E)

4.2.2 Exception Responses

The MODBUS-GW sends exception responses to its Modbus clients as appropriate (e.g., invalid command, invalid data, etc.). For more information, refer to Appendix B, “Exception Responses”.

4.3 Modbus Addressing

The MODBUS-GW uses Modbus addressing within the following guidelines:

- The MODBUS-GW operates similarly to a Modbus bridge. Each MODBUS-GW can support up to four panels on an NFN network. Each fire panel being addressed by the Modbus master on the NFN network is identified by the Unit ID.
- The Unit ID used in the MODBUS-GW must be in the range 1 through 247. This is a Modbus range limitation. The Unit ID should match the node number of the NFN node that is being addressed. For example, a Unit ID of 127 addresses NFN node 127.
- The MODBUS-GW communicates on standard Modbus IP port 502.

NOTE: Communication on Modbus IP port 502 is not configurable and is a Modbus norm.

- Standard register types and reference ranges are:
  - 0x Coil 00001–09999
  - 1x Discrete Input 10001–19999
  - 3x Input Register 30001–39999
  - 4x Holding Register 40001–49999

For more information on Modbus addressing, refer to Section 5, “Register Mapping”.

4.4 Analog Values and Trending

4.4.1 Trending of Analog Values

Trending of analog values is supported on all of the panels/networks 4–20 mA modules. The only limitation is that the gateway will only actively read analog values for up to 10 analog modules at a time. All the analog values on all the modules can be read as long as a separate poll is sent for these points in groups of up to 10 points at a time, following the rules outlined below. Reference 4.4.2, "Analog Value Use Cases" for clarity on this issue.

- Accept a poll for up to any 10 analog (4–20 mA) points per gateway.
  - Requests for more points than this are rejected with an exception code.
  - If any of the points in the request are not 4–20 mA modules then the gateway rejects the request with an exception code.
- The first poll for analog values is an initialization poll. This initialization poll informs the gateway to start acquiring analog values for these points at 5 second intervals.
  - Points are only polled on the NFN if the 4–20 mA module is in at least the first level of alarm status. If the point is normal then the gateway returns a value of zero.

NOTE: The first response to an analog point poll is zero. This response is an initialization confirmation from the gateway.

- Upon receiving the initialization confirmation, the client can begin polling the analog points. The client should wait 5 seconds after the initialization request to insure that the MODBUS-GW has had enough time to get the analog values and load the registers. Thereafter the MODBUS-GW continues to poll the points. The analog value in the MODBUS-GW are updated no faster than once every 5 seconds.
  - Points are polled if the device is in at least the first level of alarm status. Zero is returned for devices not in alarm status.
  - When a point being polled enters normal status, polling for that point on the NFN is terminated and the analog value register for that point is filled with zeros.
- The MODBUS-GW ceases polling the analog points when:
  - The client does not make a request for these exact same points over a period defined in the Modbus Configuration Tool as “Analog Value Time Out”. The default is 20 seconds.
  - The gateway makes a request for a point (or points) that is not *exactly the same as the initial request*. The MODBUS-GW first sends an initial confirmation for the new set of analog points, and then begins polling those points at 5 second intervals.
- When a 4–20 mA module is in fault, the analog value register for that point is filled with zeros.

4.4.2 Analog Value Use Cases

Use Case 1: A client requests analog values from the points L1M1 through L1M10 every 10 seconds.

Result: The MODBUS-GW sends back zeros in response to the first request for analog values from the points L1M1 through L1M10. The MODBUS-GW sends back actual values on the second request from the client 5 seconds later. The MODBUS-GW continues to poll these devices as long as the client continues to send analog value requests for points L1M1 through L1M10 at a rate faster than the Analog Value Time Out.

Use Case 2: A client requests analog values from the points L1M1 through L1M10. After 10 minutes of polling on a 10 second interval, the client stops requesting analog values for these points.

Result: The MODBUS-GW sends back zeros in response to the first request for analog values from the points L1M1 through L1M10. The MODBUS-GW sends back actual values on the second request from the client 10 seconds later. The MODBUS-GW continues to poll these devices as long as the client continues to send analog value requests for points L1M1 through L1M10. When the client stops polling at 10 minutes, the MODBUS-GW will stop polling the NFN after the Analog Value Time Out expire**s.**

Use Case 3: A client requests analog values from the points L1M1 through L1M10. After 10 minutes of polling on a 10 second interval, the client requests analog values from the points L1M20 to L1M22.

Result: The MODBUS-GW sends back zeros in response to the first request for analog values from the points L1M1 through L1M10. The MODBUS-GW sends back actual values on the second request from the client 10 seconds later. The Gateway continues to poll these devices as long as the client continues to send analog value requests for the points L1M1 through L1M10. When the client sends a request for analog values from the points L1M20 through L1M22, the MODBUS-GW immediately sends back zeros in response to the first analog value request from these points and starts polling L1M20 through L1M22. The MODBUS-GW only polls the points specifically requested.

Use Case 4: A client requests analog values from the points L1M1 through L1M10. After 10 minutes of polling on a 10 second interval, the client requests analog values from the points L1M5 through L1M12.

Result: The MODBUS-GW sends back zeros in response to the first request for analog values from the points L1M1 through L1M10. The MODBUS-GW sends back actual values in response to the second request from the client 10 seconds later. The MODBUS-GW continues to poll these devices as long as the client continues to send analog value requests for the points L1M1 through L1M10. When the client sends a request for analog values from the points L1M5 through L1M12, the gateway immediately sends back zeros in response to the first analog value request from points L1M11 and L1M12 (since these are newly requested points) and it sends back actual values in response to the continuing analog value requests for points L1M5 through L1M10 (since it already has been polling these points). The gateway stops polling points L1M1 through L1M4 and starts polling points L1M5 through L1M12.

Use Case 5: A client requests analog values from the points L1M1 through L1M15.

Result: The MODBUS-GW sends back an exception response because it can only process requests for up to 10 analog values at a time. The client should request and receive values for L1M1 through L1M10 and then send a request for L1M11 through L1M15. Note that the first request for analog values from a valid range of points is considered an initialization request, which returns zeros.

Section 5 Register Mapping

5.1 Register Mapping Overview

The MODBUS-GW uses 16-bit registers. One Modbus Input register and one Modbus Holding Register are allocated for each device address. These registers represent a contiguous address mapping of all devices and points.

5.2 Point Status Holding Registers

Each of the point status holding registers are divided into an upper and lower byte as described below and in Table 5.1.

- **Upper Byte**: The upper byte contains general status information about the point.
- **Lower Byte:** The lower byte is primarily used when bit 11 in the upper byte is a '1' (or active). When bit 11 is a '1', refer to Appendix C, "MODBUS-GW Active Event Types" for detailed information about the active point. The lower byte will be all 0's if the device is not in an active state.

  Specifically, the lower byte contains the actual active event for this point. An active state is defined in this gateway as any Fire, Security, Critical Process, Medical, Mass Notification, or Supervisory alarm state. If the point is not present in the panel programming, all bits in the lower byte will contain a '1' or the value FFH. The only possible active event type for zones is Non-Fire Activation (71H). See Appendix C.

Table 5.1 Point Status Holding Register Bit Definitions

	Upper Byte								Lower Byte							
Bit No.	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
Bit Name	Ack Block	Prealarm	Trouble	InActive	Active	Enable	Disable	Ack Fire Alarm	**Active Event Type** (When Bit 11 is set to 1, the register value is 71H. See Appendix C.)							
	When individual upper byte bits are set to 1, the following definitions apply: • **Ack Block** (Bit 15): All events on this point, other than fire alarm, are acknowledged. Not applicable for zones. • **Prealarm** (Bit 14): The point is in a prealarm state. Not applicable for zones. • **Trouble** (Bit 13): The point is in a trouble state. Not applicable for zones. • **InActive** (Bit 12): The point is not active. • **Active** (Bit 11): The point is active and there will be an active event type in the lower byte. • **Enable** (Bit 10): The point is enabled. • **Disable** (Bit 9): The point is disabled. • **Ack Fire Alarm** (Bit 8): The fire alarm on this point is acknowledged. Not applicable for zones.															

The holding register addresses and the points contained in these addresses are detailed in Table 5.2. Each range of holding registers is used for either detectors or modules.

Table 5.2 Point Status Holding Register Device/Module Addresses

Start Address	End Address	Address
40001	40200	L1D1–L1D159
40201	40400	L1M1–L1M159
40401	40600	L2D1–L2D159
40601	40800	L2M1–L2M159
40801	41000	L3D1–L3D159
41001	41200	L3M1–L3M159
41201	41400	L4D1–L4D159
41401	41600	L4M1–L4M159
41601	41800	L5D1–L5D159
41801	42000	L5M1–L5M159
42001	42200	L6D1–L6D159
42201	42400	L6M1–L6M159
42401	42600	L7D1–L7D159
42601	42800	L7M1–L7M159
42801	43000	L8D1–L8D159
43001	43200	L8M1–L8M159
43201	43400	L9D1–L9D159
43401	43600	L9M1–L9M159
43601	43800	L10D1–L10D159
43801	44000	L10M1–L10M159

NOTES:

- There are unused registers on every loop in order to make the register addresses easier to remember and allow for future expansion *(e.g. registers 40159 through 40200 are not used).
- On the AFP-2800, output activation status is not reported to the MODBUS-GW and therefore the bits and event type will always indicate a non-active state. AFP-2800 activations from the Modbus client are not supported.

5.3 Point Device Type Holding Registers

There are 2000 point device type holding registers. Each register address consists of two bytes (upper and lower) as defined in Table 5.3 representing two detectors or modules as shown in Table 5.4. Devices in the upper byte have even number points; devices in the lower byte have odd number points.

Table 5.3 Point Device Type Holding Register Bit Definitions

	Upper Byte								Lower Byte							
Bit No.	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
Device Types (see Appendix D)																

Table 5.4 Point Device Type Holding Register Addresses

Start Address	End Address	Devices In Upper Byte	Devices In Lower Byte
44001	44100	Loop 1 Detector 2,4,6,8,10...158	Loop 1 Detector 1,3,5,9,11...159
44101	44200	Loop 1 Module 2,4,6,8,10...158	Loop 1 Module 1,3,5,9,11...159
44201	44300	Loop 2 Detector 2,4,6,8,10...158	Loop 2 Detector 1,3,5,9,11...159
44301	44400	Loop 2 Module 2,4,6,8,10...158	Loop 2 Module 1,3,5,9,11...159
44401	44500	Loop 3 Detector 2,4,6,8,10...158	Loop 3 Detector 1,3,5,9,11...159
44501	44600	Loop 3 Module 2,4,6,8,10...158	Loop 3 Module 1,3,5,9,11...159
44601	44700	Loop 4 Detector 2,4,6,8,10...158	Loop 4 Detector 1,3,5,9,11...159
44701	44800	Loop 4 Module 2,4,6,8,10...158	Loop 4 Module 1,3,5,9,11...159
44801	44900	Loop 5 Detector 2,4,6,8,10...158	Loop 5 Detector 1,3,5,9,11...159
44901	45000	Loop 5 Module 2,4,6,8,10...158	Loop 5 Module 1,3,5,9,11...159
45001	45100	Loop 6 Detector 2,4,6,8,10...158	Loop 6 Detector 1,3,5,9,11...159
45101	45200	Loop 6 Module 2,4,6,8,10...158	Loop 6 Module 1,3,5,9,11...159
45201	45300	Loop 7 Detector 2,4,6,8,10...158	Loop 7 Detector 1,3,5,9,11...159
45301	45400	Loop 7 Module 2,4,6,8,10...158	Loop 7 Module 1,3,5,9,11...159
45401	45500	Loop 8 Detector 2,4,6,8,10...158	Loop 8 Detector 1,3,5,9,11...159
45501	45600	Loop 8 Module 2,4,6,8,10...158	Loop 8 Module 1,3,5,9,11...159
45601	45700	Loop 9 Detector 2,4,6,8,10...158	Loop 9 Detector 1,3,5,9,11...159
45701	45800	Loop 9 Module 2,4,6,8,10...158	Loop 9 Module 1,3,5,9,11...159
45801	45900	Loop 10 Detector 2,4,6,8,10...158	Loop 10 Detector 1,3,5,9,11...159
45901	46000	Loop 10 Module 2,4,6,8,10...158	Loop 10 Module 1,3,5,9,11...159

5.4 Zones/Panel Circuits Status Holding Registers

Each of the zones/panel circuits status holding registers are divided into an upper and lower byte as described below and in Table 5.5.

- **Upper Byte**: The upper byte contains general status information about the zone or panel circuit.
- **Lower Byte:** The lower byte is primarily used when bit 11 in the upper byte is a '1' (or active). When bit 11 is a '1', refer to Appendix C, "MODBUS-GW Active Event Types" for detailed information about the active zone or panel circuit. The lower byte will be all 0's if the zone/panel circuit is not in an active state.

  Specifically, the lower byte contains the actual active event for this zone or panel circuit. An active state is defined in this gateway as any Fire, Security, Critical Process, Medical, Mass Notification, or Supervisory alarm state. If the zone or panel circuit is not present in the panel programming, all bits in the lower byte will contain a '1' or the value 'FFH'.

Table 5.5 Zones/Panel Circuits Holding Register Bit Definitions

	Upper Byte								Lower Byte							
Bit No.	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
Bit Name	Ack Block	Prealarm	Trouble	InActive	Active	Enable	Disable	Ack Fire Alarm	Active Event Type (When Bit 11 is set to 1, see Appendix C.)							
	When individual upper byte bits are set to 1, the following definitions apply: • **Ack Block** (Bit 15): All events on this zone/panel circuit, other than fire alarm, are acknowledged. • **Prealarm** (Bit 14): The zone/panel circuit is in a prealarm state. • **Trouble** (Bit 13): The zone/panel circuit is in a trouble state. • **InActive** (Bit 12): The zone/panel circuit is not active. • **Active** (Bit 11): The zone/panel circuit is active and there will be an active event type in the lower byte. • **Enable** (Bit 10): The zone/panel circuit is enabled. • **Disable** (Bit 9): The zone/panel circuit is disabled. • **Ack Fire Alarm** (Bit 8): The fire alarm on this zone/panel circuit is acknowledged.															

The holding register addresses and the zones contained in these addresses are detailed in Table 5.6.

Table 5.6 Zones

Zone Type	Register Address	Zone Address
General Zones	46001–47000	Z 1,2,3,4,5,6,7,8,...1000
Logic Zones	47001–49000	Z 1,2,3,4,5,6,7,8,...2000
Trouble Zones	49001–49100	Z 1,2,3,4,5,6,7,8,...100
Releasing Zones	49101–49110	Z 1,2,3,4,5,6,7,8,9,10

The holding register addresses and the panel circuits contained in these addresses are detailed in Table 5.7.

Table 5.7 Panel Circuits

Register Address	Panel Circuits
49111–49118	P1.1–P1.8
49119–49126	P2.1–P2.8
49127–49134	P3.1–P3.8
49135–49142	P4.1–P4.8
49143–49150	P5.1–P5.8
49151–49158	P6.1–P6.8
49159–49166	P7.1–P7.8
49167–49174	P8.1–P8.8
49175–49182	P9.1–P9.8
49183–49190	P10.1–P10.8
49191–49198	P11.1–P11.8
49199–49206	P12.1– P12.8

The maximum panel circuit points by fire panel is described in Table 5.8.

Table 5.8 Supported Circuits by Panel

Panel	Max. Panel Circuits Points
NFS-320	Not Supported
NFS-640	8
NFS2-640	Not Supported
NFS-3030	12
NFS2-3030	Not Supported

5.5 Bell Circuits Status Holding Registers

■ NFS2-640 and NFS-320 Only

Each of the bell circuits status holding registers are divided into an upper and lower byte as described below and in Table 5.9.

- **Upper Byte**: The upper byte contains general status information about the bell circuit.
- **Lower Byte:** The lower byte is primarily used when bit 11 in the upper byte is a '1' (or active). When bit 11 is a '1', refer to Appendix C, "MODBUS-GW Active Event Types" for detailed information about the active bell circuit. The lower byte will be all 0's if the bell circuit is not in an active state.

  Specifically, the lower byte contains the actual active event for this bell circuit. An active state is defined in this gateway as any Fire, Security, Critical Process, Medical, Mass Notification, or Supervisory alarm state. If the bell circuit is not present in the panel programming, all bits in the lower byte will contain a '1' or the value 'FFH'.

Table 5.9 Zones/Panel Circuits Holding Register Bit Definitions

	Upper Byte								Lower Byte							
Bit No.	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
Bit Name	Ack Block	Prealarm	Trouble	InActive	Active	Enable	Disable	Ack Fire Alarm	Active Event Type (When Bit 11 is set to 1, see Appendix C.)							
	When individual upper byte bits are set to 1, the following definitions apply: • **Ack Block** (Bit 15): All events on this bell circuit, other than fire alarm, are acknowledged. • **Prealarm** (Bit 14): The bell circuit is in a prealarm state. • **Trouble** (Bit 13): The bell circuit is in a trouble state. • **InActive** (Bit 12): The bell circuit is not active. • **Active** (Bit 11): The bell circuit is active and there will be an active event type in the lower byte. • **Enable** (Bit 10): The bell circuit is enabled. • **Disable** (Bit 9): The bell circuit is disabled. • **Ack Fire Alarm** (Bit 8): The fire alarm on this bell circuit is acknowledged.															

The holding register address and the bell circuit contained in the address is detailed in Table 5.10.

Table 5.10 Bell Circuit Holding Register Addresses

Start Address	End Address	Device Address
49400	49400	Bell Circuit 1
49401	49401	Bell Circuit 2
49402	49402	Bell Circuit 3
49403	49403	Bell Circuit 4

5.6 Bell Circuits Device Type Holding Registers

Each bell circuits device type holding register address consists of two bytes (upper and lower) as defined in Table 5.11 representing two bell circuits as shown in Table 5.12.

Table 5.11 Bell Circuits Device Type Holding Register Bit Definitions

	Upper Byte								Lower Byte							
Bit No.	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
Device Types (see Appendix D)																

Table 5.12 Bell Circuit Device Type Holding Register Addresses

Start Address	End Address	Device Address	Device Address
49410	49410	Bell Circuit 2	Bell Circuit 1
49411	49411	Bell Circuit 4	Bell Circuit 3

5.7 Panel Status Holding Register

The panel status holding register is divided into an upper and lower byte as described below and in Table 5.13 representing one register address as shown in Table 5.14.

- **Silence**: The fire alarm control panel is silenced when this bit is set to 1.
- **Reset**: Not used.

Table 5.13 Panel Status Holding Register Bit Definitions

	Upper Byte								Lower Byte							
Bit No.	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
Bit Name	Not Used														Silence	Reset

Table 5.14 Panel Status Holding Register Addresses

Start Address	End Address	Description
49500	49500	Panel Status Holding Register

5.8 Analog Values Input Registers

Analog values listed in Table 5.15 are only available for 4–20 mA modules. Refer to 4.4, "Analog Values and Trending" for details regarding analog values.

Table 5.15 Input Register Analog Values

Start Address	End Address	Analog Value (16 bits)
30001	30200	L1M1–L1M159
30201	30400	L2M1–L2M159
30401	30600	L3M1–L3M159
30601	30800	L4M1–L4M159
30801	31000	L5M1–L5M159
31001	31200	L6M1–L6M159
31201	31400	L7M1–L7M159
31401	31600	L8M1–L8M159
31601	31800	L9M1–L9M159
31801	32000	L10M1–L10M159

5.9 Panel and System Troubles Input Registers

Sixty-four 16-bit registers are reserved for panel troubles and one register is assigned as an overall panel trouble indicator as shown in Table 5.16.

Table 5.16 Panel and System Troubles Input Register Addresses

Start Address	End Address	Description
35000	35000	Panel Trouble Summary (Total number of Trouble bits set for the node)
35001	35064	Panel Troubles

A single bit is reserved for each trouble in the system. The assignment of bits to trouble codes is shown in Appendix E, “System Troubles”.

5.10 Gateway Information Input Registers

NOTE: Information/debug values are used by the MODBUS-GW Unit ID only. All other nodes reject reads in this address range.

The MODBUS-GW records some status and configuration information for debugging and technical support purposes. This information is stored in some reserved gateway registers as outlined below and in Table 5.17.

- Gateway Modbus Address
- Gateway IP Address
- Gateway Version Number
- Gateway Status

Table 5.17 Gateway Information Input Register Addresses

Start Address	End Address	Description
35100	35500	Information/Debug information
35100	35115	Node Status: • 1 = On Line • 0 = Off Line The MODBUS-GW tracks the node status of all nodes on the NFN network.
35116	35116	Gateway major version number
35117	35117	Gateway minor version number
35118	35118	Gateway build
35119	35119	Gateway Status: • 1 = On Line • 0 = Off Line

5.10.1 Node Status Details

Each nodes status is represented by a bit in a register. If the bit is set, the node is on line. Table 5.18 provides an example of how this is represented in a register.

Table 5.18 Node Status Example

	Bit Number															
Address	**15**	**14**	**13**	**12**	**11**	**10**	**9**	**8**	**7**	**6**	**5**	**4**	**3**	**2**	**1**	**0**
35100	N16	N15	N14	N13	N12	N11	N10	N9	N8	N7	N6	N5	N4	N3	N2	N1
35101	N32	N31	N30	N29	N28	N27	N26	N25	N24	N23	N22	N21	N20	N19	N18	N17

5.10.2 Read Device Identification (0x2B/0x0E)

This function code allows reading the identification and additional information about the MODBUS-GW as shown in Table 5.19.

Table 5.19 43/14 (0x2B/0x0E) Read Device Identification

Object ID	Object Name / Description	Value
0x00	VendorName	Notifier
0x01	ProductCode	1
0x02	MajorMinorRevision	V1.0 (*Example*)
0x03	VendorUrl	www.notifier.com
0x04	ProductName	Modbus Gateway
0x05	ModelName	Modbus Gateway
0x06	UserApplicationName	Modbus Gateway

Section 6 Troubleshooting

6.1 What are some basic guidelines I should use when installing a MODBUS-GW?

- Polling should be done slowly to start.
- Use Modscan® to debug the system rather than a more complicated client. Verify that registers are being updated as events happen on the NFN network/panel.
- Make sure gateway can be pinged from the same computer on which the client application is being installed.
- Check and double check the power supplies as well as all cabling.
- Make sure the client supports Unit IDs.
- Stop the client from sending a subsequent request until after it receives a response from the gateway.
- Make sure the client accepts all exception responses. Including 0xA and 0xB.
- Use Wireshark® to debug IP traffic.
- Be sure only one client is polling the gateway.
- Check the MODBUS-GW configuration tool and be sure that the Authorized Client IP address is set to **0.0.0.0**. If using the Authorized Client IP security feature, confirm that the address in the gateway matches the address in the Modbus client.

6.2 How fast can the Modbus client poll the gateway?

The polling rate is a function of several variables. Some issues that will determine the maximum poll rate are:

- The size of the NFN network that is being monitored.
- The number of points on the panels.
- The event activity on the NFN network/panel (i.e. VeriFire downloads).
- Requests for analog values are much slower than other requests
- If only a partial response form the gateway is seen in the Modbus client, try increasing the “response time out” value in the client to a larger value. If the value is set to 5 seconds or more, this should be adequate. The exact response time out will depend on IP network delays and routing. On a small IP network, the gateway responds to a read of 100 register in less than 1 second.

The gateway also has some processing overhead in order to do such things as maintain the registers.

6.3 How can I tell if the gateway is running?

- Ping the gateway from the computer on which the Modbus client is running.
- Use Wireshark to analyze the data on the IP network.
- Modscan was one tool that was used during development to test the gateway. It is designed primarily as a testing device for verification of correct protocol operation in new or existing systems.

6.4 How do I recover a lost password from the gateway?

If the password for the gateway is lost, programming changes cannot be made. In this situation, the gateway settings must be reset. Refer to Appendix A, “Gateway Settings” for instructions.

6.5 What is an “initialization read” for analog values?

This is the first read of up to 10 analog values from a 4–20 mA module. This first read tells the gateway that it should begin a polling routine for the analog values in this request. The first response from the initialization will usually be all zeros. Subsequent responses will have the actual values.

6.6 How many analog values can I read at a time?

Ten analog values can be read at one time. An initialization read must be performed.

6.7 Why do I get an exception code when trying to read an analog value?

There are several reasons why an exception code is received when requesting an analog value:

- The point from which an analog value is being requested is not a 4–20 mA analog input module.
- At least one of the points in the group of points from which an analog value is being requested is not a 4–20 mA analog input module.
- More than 10 analog values have been requested in a single request.

6.8 Why do I get all zeros when I read an analog value?

There are several reasons a zero reading from an FMM-4-20 Analog Input Module is received:

- The first read for an analog value from the gateway initializes the polling routine in the gateway to retrieve analog values from the NFN network. The first response will usually be all zeros. This is normal. The subsequent polls of an analog value for the same point or group of points will return actual values. As long as the same points continue to be polled at a rate faster than the Analog Poll Time Out, then the gateway will continue to poll the same points.
- The gateway does not actually take an analog value reading unless the module has reached the first threshold and therefore it will return a zero reading.
- If the client polls the gateway too quickly after the initialization poll then the gateway may still return zeros.
- If the client polls the analog values slower than the Analog Poll Time Out, then the gateway may return all zeros.

6.9 What is the “Analog Value Polling Time Out”?

This is how long a gateway will continue to poll analog points after the last client read request of the points. As long as the client makes analog reads of the same points faster than the Analog Value Polling Time then the gateway will continue to poll these points. If the client polls slower than the Analog Value Polling Time then the gateway may return readings of zero because this will be considered an initialization read.

6.10 System Trouble

For information about system trouble information stored in holding registers, refer to 5.9, "Panel and System Troubles Input Registers".

Appendix A Gateway Settings

NOTE: The procedures in this appendix require the use of a USB flash memory drive.

A.1 Viewing Existing IP Settings

1. Connect the flash drive to the MODBUS-GW.
2. Reboot the gateway.

   A file is created that matches the configured IP address of the gateway, followed by the extension "**.txt**" (e.g., **192.168.1.2.txt**). If the file already exists on the drive, it will be altered to match the gateway configuration. The file contains additional information such as the MAC address of the gateway.
3. Connect the drive to a PC and view the files.

   The flash drive should contain a file that matches the configured IP address of the gateway, followed by the extension "**.txt**" (e.g., **192.168.1.2.txt**). If the file already exists on the drive, it has been altered to match the gateway configuration. The file contains additional information such as the MAC address of the gateway.

A.2 Resetting Factory Default Values

1. Connect the flash drive to a PC and create a file named "**default.ldc"**. The contents of the file is not significant; however, ensure that the file does not have an additional hidden file extension. This file will be automatically deleted from the flash drive by the gateway.
2. Eject the flash drive from the PC.
3. Disconnect power from the gateway.
4. Disconnect the communication cable to the gateway USB port (if present) and connect the flash drive.
5. Reconnect the 24 VDC power supply to the gateway.
6. After approximately one minute, disconnect the flash drive from the USB port and (if necessary) reconnect the cable removed in Step 4.
7. Connect the flash drive to the PC and verify that the file named **192.168.1.2.txt** is on the drive.
   - If the file is on the flash drive, the reset has been accomplished.
   - If the file **is not** on the flash drive:
     – The flash drive may not have been connected during the reboot period or was removed early.
     – The flash drive is not seen as a valid drive by the hardware.
     – A software error has occurred and technical support may need to be contacted.

Appendix B Exception Responses

If a Modbus master device sends an invalid command or attempts to read an invalid holding register, an exception response is generated. The exception response follows the standard packet format. The high order bit of the function code in an exception response is 1. The data field of an exception response contains the exception error code. Table B.1, “Exception Codes” describes the exception codes supported and the possible causes.

Table B.1 Exception Codes

Exception Code	Conditions	Exception Name
0x01	• Protocol Identifier in Modbus packet does not match Modbus protocol. Protocol Identifier in Modbus should always be “0”. • Function code sent by the client is not supported by the MODBUS-GW or the FACP. • A Control command was sent to the gateway. Contact customer service.	Illegal function
0x02	• Register address range specified by the client is not supported by the FACP. • Register address range requested is valid but the device (e.g. Detector, Module, Zone, etc.) is not present in the specified FACP. • Analog Value is requested from a register which is not associated with a 4–20 mA device.	Illegal data address
0x03	• Number of registers requested exceeds the maximum allowed limit. The maximum number of registers that a client can read at one time is 100. The exception to this is for analog values where the maximum number of registers a client can read at one time is 10. • Invalid Data written to the register when sending commands.	Illegal data value
0x0A	Unit ID specified in the request packet is not configured for monitoring.	Gateway path failed
0x0B	FACP is off line or there is a communication problem on the panel and/or NFN.	Gateway target failed

Appendix C MODBUS-GW Active Event Types

All NFN events are mapped into Modbus event categories which are stored in the Modbus register. Events are mapped as shown in Table C.1.

Table C.1 Event Type Categories

Event	Modbus Register Value
No Active Status (see note)	00H
Mass Notification Alarm, High Priority	05H
Fire Alarm	10H
Security Alarm (Life)	11H
Critical Process Alarm (Life)	12H
Medical Emergency (Life)	13H
CO Alarm	14H
Mass Notification Alarm, Low Priority	15H
Security Alarm (Property)	20H
Critical Process (Property)	21H
Mass Notification Supervisory, High Priority	25H
Supervisory Signal (Guard's Tour)	30H
Supervisory Signal (Equipment)	40H
Mass Notification Supervisory, Low Priority	45H
Disabled Alarm (AFP2800 Panel Only)	52H
Disabled Active (AFP2800 Panel Only)	55H
Non-Fire Activation	71H
Non-Fire Activation (no acknowledgment required)	72H
CO Alarm & Fire Alarm	EAH
CO Supervisory	EBH
CO Supervisory & Photo Supervisory	ECH
CO Supervisory & Fire Alarm	EDH
CO Alarm & Photo Supervisory	EEH
Device Not Present	FFH

NOTES:

- Multiple states are possible for a device. For example, a device connected to a Fire Alarm Control Panel may be both Active and Disabled. Also, a device may be in the Trouble and Fire Alarm states at one time.
- "No Active Status" does not indicate the point/device is in a normal state. The holding register for the point or device contains more detail. For more information, refer to Section 5, "Register Mapping".

Appendix D Device Types

Device types are organized into the following categories:

- Detectors (1–50) - Table D.1
- Monitor Modules (51–150) - Table D.2
- Control Modules (151–250) - Table D.3

Table D.1 Device Type Values – Detectors

DEVICE TYPE	Value
HEAT DETECTOR	1
ION DETECTOR	2
PHOTO DETECTOR	3
LASER DETECTOR	4
OMNI DETECTOR	5
PHOTO DETECTOR	6
ASPIRATION	7

Table D.2 Device Type Values – Monitor Modules

DEVICE TYPE	Value	DEVICE TYPE	Value
MONITOR MODULE	51	MEDIC ALERT	79
HEAT DETECT	52	NON FIRE	80
MONITOR	53	PAS INHIBIT	81
PULL STATION	54	POWER MONITR	82
RF MON MODUL	55	PROCESS MON	83
RF PULL STA	56	PROCESS AUTO	84
SMOKE CONVEN	57	RESET SWITCH	85
SMOKE DETECT	58	SIL SWITCH	86
WATERFLOW	59	TELE PAGE	87
WATERFLOW S	60	TORNADO ALRT	88
ACCESS MONTR	61	TROUBLE MON	89
AREA MONITOR	62	ABORT SWITCH	90
AUDIO SYSTEM	63	MAN RELEASE	91
EQUIP MONITR	64	MANREL DELAY	92
HOLD UP	65	SECOND SHOT	93
RF SUPERVSRY	66	SECURITY T	94
SECURITY L	67	NC MONITOR	95
LATCH SUPERV	68	NC SUP T	96
TRACK SUPERV	69	NC SUP L	97
SPRINKLR SYS	70	NC NON FIRE	98
SYS MONITOR	71	SECURE/ACCESS	99
TAMPER	72	DISABLE MON	100
ACK SWITCH	73	4-20mA	101
ALLCALL PAGE	74	CO MONITOR MOBILE	102
DRILL SWITCH	75	MASS NOTIFICATION TRACKING SUPERVISORY	103
EVACUATE SW	76	MASS NOTIFICATION LATCHING SUPERVISORY	104

Table D.2 Device Type Values – Monitor Modules *(Continued)*

DEVICE TYPE	Value	DEVICE TYPE	Value
FIRE CONTROL	77	MASS NOTIFICATION TROUBLE MON	105
HAZARD ALERT	78	MASS NOTIFICATION MONITOR	106

Table D.3 Device Type Values – Control Modules

DEVICE TYPE	Value	DEVICE TYPE	Value
CONTROL	151	ALARMS PEND	168
RELAY	152	CONTROL NAC	169
BELL CIRCUIT	153	GEN ALARM	170
STROBE CKT	154	GEN SUPERVIS	171
HORN CIRCUIT	155	GEN TROUBLE	172
AUDIBLE CKT	156	GENERAL PEND	173
SPEAKER	157	TROUBLE PEND	174
REL END BELL	158	FORM C RESET	175
(blank)	159	ISOLATED SPK	176
RELEASE CKT	160	ISOLATED NAC	177
REL CKT ULC	161	RELAY FDBACK	178
RELEA.FORM C	162	REL FORM C FB	179
REL AUDIBLE	163	MASS NOTIFICATION GENERAL	180
NONRESET CTL	164	MASS NOTIFICATION CONTROL	181
TELEPHONE	165	MASS NOTIFICATION STROBE	182
REL CODE BELL	166	MASS NOTIFICATION SPEAKER	183
INSTANT RELE	167	MASS NOTIFICATION RELAY	184

Appendix E System Troubles

Table E.1 System Troubles Register Map

Register	Bit No.	System Trouble Name	Bit No.	System Trouble Name
35001	0	GROUND FAULT	8	INTERNAL RAM ERROR
	1	AC FAIL	9	EXTERNAL RAM ERROR
	2	BATTERY	10	PROGRAM CORRUPTED
	3	STYLE 6 POS. LOOP 1	11	NO DEV. INST ON L1
	4	STYLE 6 POS. LOOP 2	12	PANEL DOOR OPEN
	5	CORRUPT LOGIC EQUAT	13	AUXILIARY TROUBLE
	6	LCD80 SUPERVISORY	14	TERM. SUPERVISORY
	7	EPROM ERROR	15	ANNUN. 1 TROUBLE
35002	0	ANNUN. 1 NO ANSWER	8	ANNUN. 5 NO ANSWER
	1	ANNUN. 2 TROUBLE	9	ANNUN. 6 TROUBLE
	2	ANNUN. 2 NO ANSWER	10	ANNUN. 6 NO ANSWER
	3	ANNUN. 3 TROUBLE	11	ANNUN. 7 TROUBLE
	4	ANNUN. 3 NO ANSWER	12	ANNUN. 7 NO ANSWER
	5	ANNUN. 4 TROUBLE	13	ANNUN. 8 TROUBLE
	6	ANNUN. 4 NO ANSWER	14	ANNUN. 8 NO ANSWER
	7	ANNUN. 5 TROUBLE	15	ANNUN. 9 TROUBLE
35003	0	ANNUN. 9 NO ANSWER	8	ANNUN.13 NO ANSWER
	1	ANNUN.10 TROUBLE	9	ANNUN.14 TROUBLE
	2	ANNUN.10 NO ANSWER	10	ANNUN.14 NO ANSWER
	3	ANNUN.11 TROUBLE	11	ANNUN.15 TROUBLE
	4	ANNUN.11 NO ANSWER	12	ANNUN.15 NO ANSWER
	5	ANNUN.12 TROUBLE	13	ANNUN.16 TROUBLE
	6	ANNUN.12 NO ANSWER	14	ANNUN.16 NO ANSWER
	7	ANNUN.13 TROUBLE	15	ANNUN.17 TROUBLE
35004	0	ANNUN.17 NO ANSWER	8	ANNUN.21 NO ANSWER
	1	ANNUN.18 TROUBLE	9	ANNUN.22 TROUBLE
	2	ANNUN.18 NO ANSWER	10	ANNUN.22 NO ANSWER
	3	ANNUN.19 TROUBLE	11	ANNUN.23 TROUBLE
	4	ANNUN.19 NO ANSWER	12	ANNUN.23 NO ANSWER
	5	ANNUN.20 TROUBLE	13	ANNUN.24 TROUBLE
	6	ANNUN.20 NO ANSWER	14	ANNUN.24 NO ANSWER
	7	ANNUN.21 TROUBLE	15	ANNUN.25 TROUBLE
35005	0	ANNUN.25 NO ANSWER	8	ANNUN.29 NO ANSWER
	1	ANNUN.26 TROUBLE	9	ANNUN.30 TROUBLE
	2	ANNUN.26 NO ANSWER	10	ANNUN.30 NO ANSWER
	3	ANNUN.27 TROUBLE	11	ANNUN.31 TROUBLE
	4	ANNUN.27 NO ANSWER	12	ANNUN.31 NO ANSWER
	5	ANNUN.28 TROUBLE	13	ANNUN.32 TROUBLE
	6	ANNUN.28 NO ANSWER	14	ANNUN.32 NO ANSWER
	7	ANNUN.29 TROUBLE	15	NETWORK FAIL PORT A

Table E.1 System Troubles Register Map *(Continued)*

Register	Bit No.	System Trouble Name	Bit No.	System Trouble Name
35006	0	NETWORK FAIL PORT B	8	UDACT TROUBLE
	1	NETWORK FAILURE	9	UDACT NO ANSWER
	2	ADV WALK TEST	10	PROG MODE ACTIVATED
	3	CHARGER FAIL	11	LOADING NO SERVICE
	4	GROUND FAULT LOOP 2	12	BASIC WALK TEST
	5	STYLE 6 NEG. LOOP 1	13	NFPA 24HR REMINDER
	6	STYLE 6 NEG. LOOP 2	14	NVRAM BATT TROUBLE
	7	GROUND FAULT LOOP 1	15	(Reserved)
35007	0	Reserved	8	OPTION MODULE
	1	Reserved	9	STYLE 6 ON LOOP 3
	2	Reserved	10	AVPS. TROUBLE
	3	Reserved	11	NAM CCBE PROG. LOST
	4	Reserved	12	MAN. EVAC INITIATED
	5	Reserved	13	MAN. EVAC RECEIVED
	6	Reserved	14	(Reserved)
	7	Reserved	15	(Reserved)
35008	0	ANNUN.33 TROUBLE	8	ANNUN.37 TROUBLE
	1	ANNUN.33 NO ANSWER	9	ANNUN.37 NO ANSWER
	2	ANNUN.34 TROUBLE	10	ANNUN.38 TROUBLE
	3	ANNUN.34 NO ANSWER	11	ANNUN.38 NO ANSWER
	4	ANNUN.35 TROUBLE	12	ANNUN.39 TROUBLE
	5	ANNUN.35 NO ANSWER	13	ANNUN.39 NO ANSWER
	6	ANNUN.36 TROUBLE	14	ANNUN.40 TROUBLE
	7	ANNUN.36 NO ANSWER	15	ANNUN.40 NO ANSWER
35009	0	ANNUN.41 TROUBLE	8	ANNUN.45 TROUBLE
	1	ANNUN.41 NO ANSWER	9	ANNUN.45 NO ANSWER
	2	ANNUN.42 TROUBLE	10	ANNUN.46 TROUBLE
	3	ANNUN.42 NO ANSWER	11	ANNUN.46 NO ANSWER
	4	ANNUN.43 TROUBLE	12	ANNUN.47 TROUBLE
	5	ANNUN.43 NO ANSWER	13	ANNUN.47 NO ANSWER
	6	ANNUN.44 TROUBLE	14	ANNUN.48 TROUBLE
	7	ANNUN.44 NO ANSWER	15	ANNUN.48 NO ANSWER
35010	0	ANNUN.49 TROUBLE	8	ANNUN.53 TROUBLE
	1	ANNUN.49 NO ANSWER	9	ANNUN.53 NO ANSWER
	2	ANNUN.50 TROUBLE	10	ANNUN.54 TROUBLE
	3	ANNUN.50 NO ANSWER	11	ANNUN.54 NO ANSWER
	4	ANNUN.51 TROUBLE	12	ANNUN.55 TROUBLE
	5	ANNUN.51 NO ANSWER	13	ANNUN.55 NO ANSWER
	6	ANNUN.52 TROUBLE	14	ANNUN.56 TROUBLE
	7	ANNUN.52 NO ANSWER	15	ANNUN.56 NO ANSWER

Table E.1 System Troubles Register Map *(Continued)*

Register	Bit No.	System Trouble Name	Bit No.	System Trouble Name
35011	0	ANNUN.57 TROUBLE	8	ANNUN.61 TROUBLE
	1	ANNUN.57 NO ANSWER	9	ANNUN.61 NO ANSWER
	2	ANNUN.58 TROUBLE	10	ANNUN.62 TROUBLE
	3	ANNUN.58 NO ANSWER	11	ANNUN.62 NO ANSWER
	4	ANNUN.59 TROUBLE	12	ANNUN.63 TROUBLE
	5	ANNUN.59 NO ANSWER	13	ANNUN.63 NO ANSWER
	6	ANNUN.60 TROUBLE	14	ANNUN.64 TROUBLE
	7	ANNUN.60 NO ANSWER	15	ANNUN.64 NO ANSWER
35012	0	GROUND FAULT LOOP 3	8	STYLE 6 NEG. LOOP 3
	1	GROUND FAULT LOOP 4	9	STYLE 6 NEG. LOOP 4
	2	GROUND FAULT LOOP 5	10	STYLE 6 NEG. LOOP 5
	3	GROUND FAULT LOOP 6	11	STYLE 6 NEG. LOOP 6
	4	GROUND FAULT LOOP 7	12	STYLE 6 NEG. LOOP 7
	5	GROUND FAULT LOOP 8	13	STYLE 6 NEG. LOOP 8
	6	GROUND FAULT LOOP 9	14	STYLE 6 NEG. LOOP 9
	7	GROUND FAULT LOOP 10	15	STYLE 6 NEG. LOOP 10
35013	0	STYLE 6 POS. LOOP 3	8	PRINTER SUPERVISORY
	1	STYLE 6 POS. LOOP 4	9	BUZZER SUPERVISORY
	2	STYLE 6 POS. LOOP 5	10	CRT SUPERVISORY
	3	STYLE 6 POS. LOOP 6	11	PRINT QUEUE FULL
	4	STYLE 6 POS. LOOP 7	12	MEMORY LOSS
	5	STYLE 6 POS. LOOP 8	13	PRINTER COVER OPEN
	6	STYLE 6 POS. LOOP 9	14	PRINTER PAPER OUT
	7	STYLE 6 POS. LOOP 10	15	PRINTER OFF LINE
35014	0	Workstation Fan Failure	8	STYLE 4 SHORT A LOOP 3
	1	UPS Failure	9	STYLE 4 SHORT B LOOP 3
	2	MANUAL MODE ENTERED	10	STYLE 4 SHORT A LOOP 4
	3	NCM COMM LOSS	11	STYLE 4 SHORT B LOOP 4
	4	STYLE 4 SHORT A LOOP 1	12	STYLE 4 SHORT A LOOP 5
	5	STYLE 4 SHORT B LOOP 1	13	STYLE 4 SHORT B LOOP 5
	6	STYLE 4 SHORT A LOOP 2	14	STYLE 4 SHORT A LOOP 6
	7	STYLE 4 SHORT B LOOP 2	15	STYLE 4 SHORT B LOOP 6
35015	0	STYLE 4 SHORT A LOOP 7	8	GENERAL PS FAULT
	1	STYLE 4 SHORT B LOOP 7	9	STYLE 6 SHORT LOOP 1
	2	STYLE 4 SHORT A LOOP 8	10	STYLE 6 SHORT LOOP 2
	3	STYLE 4 SHORT B LOOP 8	11	STYLE 6 SHORT LOOP 3
	4	STYLE 4 SHORT A LOOP 9	12	STYLE 6 SHORT LOOP 4
	5	STYLE 4 SHORT B LOOP 9	13	STYLE 6 SHORT LOOP 5
	6	STYLE 4 SHORT A LOOP 10	14	STYLE 6 SHORT LOOP 6
	7	STYLE 4 SHORT B LOOP 10	15	STYLE 6 SHORT LOOP 7

Table E.1 System Troubles Register Map *(Continued)*

Register	Bit No.	System Trouble Name	Bit No.	System Trouble Name
35016	0	STYLE 6 SHORT LOOP 8	8	TM4 NO ANSWER
	1	STYLE 6 SHORT LOOP 9	9	TM4 DISABLED
	2	STYLE 6 SHORT LOOP 10	10	SELF TEST FAILED
	3	NODE xxx COMMUNICATIONS FAILURE	11	NETWORK INCOMPATIBILITY
	4	NCM PIEZO BATTERY FAILURE	12	Not Used
	5	DVC COMM LOSS	13	Not Used
	6	POWER SUPPLY CABLE NOT CONNECTED	14	Not Used
	7	TM4 TROUBLE	15	Not Used
35017	0	ANNUN. 65 TROUBLE	8	ANNUN. 69 TROUBLE
	1	ANNUN. 65 NO ANSWER	9	ANNUN. 69 NO ANSWER
	2	ANNUN. 66 TROUBLE	10	ANNUN. 70 TROUBLE
	3	ANNUN. 66 NO ANSWER	11	ANNUN. 70 NO ANSWER
	4	ANNUN. 67 TROUBLE	12	ANNUN. 71 TROUBLE
	5	ANNUN. 67 NO ANSWER	13	ANNUN. 71 NO ANSWER
	6	ANNUN. 68 TROUBLE	14	ANNUN. 72 TROUBLE
	7	ANNUN. 68 NO ANSWER	15	ANNUN. 72 NO ANSWER
35018	0	ANNUN. 73 TROUBLE	8	ANNUN. 77 TROUBLE
	1	ANNUN. 73 NO ANSWER	9	ANNUN. 77 NO ANSWER
	2	ANNUN. 74 TROUBLE	10	ANNUN. 78 TROUBLE
	3	ANNUN. 74 NO ANSWER	11	ANNUN. 78 NO ANSWER
	4	ANNUN. 75 TROUBLE	12	ANNUN. 79 TROUBLE
	5	ANNUN. 75 NO ANSWER	13	ANNUN. 79 NO ANSWER
	6	ANNUN. 76 TROUBLE	14	ANNUN. 80 TROUBLE
	7	ANNUN. 76 NO ANSWER	15	ANNUN. 80 NO ANSWER
35019	0	ANNUN. 81 TROUBLE	8	ANNUN. 85 TROUBLE
	1	ANNUN. 81 NO ANSWER	9	ANNUN. 85 NO ANSWER
	2	ANNUN. 82 TROUBLE	10	ANNUN. 86 TROUBLE
	3	ANNUN. 82 NO ANSWER	11	ANNUN. 86 NO ANSWER
	4	ANNUN. 83 TROUBLE	12	ANNUN. 87 TROUBLE
	5	ANNUN. 83 NO ANSWER	13	ANNUN. 87 NO ANSWER
	6	ANNUN. 84 TROUBLE	14	ANNUN. 88 TROUBLE
	7	ANNUN. 84 NO ANSWER	15	ANNUN. 88 NO ANSWER
35020	0	ANNUN. 89 TROUBLE	8	ANNUN. 93 TROUBLE
	1	ANNUN. 89 NO ANSWER	9	ANNUN. 93 NO ANSWER
	2	ANNUN. 90 TROUBLE	10	ANNUN. 94 TROUBLE
	3	ANNUN. 90 NO ANSWER	11	ANNUN. 94 NO ANSWER
	4	ANNUN. 91 TROUBLE	12	ANNUN. 95 TROUBLE
	5	ANNUN. 91 NO ANSWER	13	ANNUN. 95 NO ANSWER
	6	ANNUN. 92 TROUBLE	14	ANNUN. 96 TROUBLE
	7	ANNUN. 92 NO ANSWER	15	ANNUN. 96 NO ANSWER

Table E.1 System Troubles Register Map *(Continued)*

Register	Bit No.	System Trouble Name	Bit No.	System Trouble Name
35021	0	ANNUN. 97 TROUBLE	8	ANNUN. 101 TROUBLE
	1	ANNUN. 97 NO ANSWER	9	ANNUN. 101 NO ANSWER
	2	ANNUN. 98 TROUBLE	10	ANNUN. 102 TROUBLE
	3	ANNUN. 98 NO ANSWER	11	ANNUN. 102 NO ANSWER
	4	ANNUN. 99 TROUBLE	12	ANNUN. 103 TROUBLE
	5	ANNUN. 99 NO ANSWER	13	ANNUN. 103 NO ANSWER
	6	ANNUN. 100 TROUBLE	14	ANNUN. 104 TROUBLE
	7	ANNUN. 100 NO ANSWER	15	ANNUN. 104 NO ANSWER
35022	0	ANNUN. 105 TROUBLE	8	ANNUN. 109 TROUBLE
	1	ANNUN. 105 NO ANSWER	9	ANNUN. 109 NO ANSWER
	2	ANNUN. 106 TROUBLE	10	ANNUN. 110 TROUBLE
	3	ANNUN. 106 NO ANSWER	11	ANNUN. 110 NO ANSWER
	4	ANNUN. 107 TROUBLE	12	ANNUN. 111 TROUBLE
	5	ANNUN. 107 NO ANSWER	13	ANNUN. 111 NO ANSWER
	6	ANNUN. 108 TROUBLE	14	ANNUN. 112 TROUBLE
	7	ANNUN. 108 NO ANSWER	15	ANNUN. 112 NO ANSWER
35023	0	ANNUN. 113 TROUBLE	8	ANNUN. 117 TROUBLE
	1	ANNUN. 113 NO ANSWER	9	ANNUN. 117 NO ANSWER
	2	ANNUN. 114 TROUBLE	10	ANNUN. 118 TROUBLE
	3	ANNUN. 114 NO ANSWER	11	ANNUN. 118 NO ANSWER
	4	ANNUN. 115 TROUBLE	12	ANNUN. 119 TROUBLE
	5	ANNUN. 115 NO ANSWER	13	ANNUN. 119 NO ANSWER
	6	ANNUN. 116 TROUBLE	14	ANNUN. 120 TROUBLE
	7	ANNUN. 116 NO ANSWER	15	ANNUN. 120 NO ANSWER
35024	0	ANNUN. 121 TROUBLE	8	ANNUN. 125 TROUBLE
	1	ANNUN. 121 NO ANSWER	9	ANNUN. 125 NO ANSWER
	2	ANNUN. 122 TROUBLE	10	ANNUN. 126 TROUBLE
	3	ANNUN. 122 NO ANSWER	11	ANNUN. 126 NO ANSWER
	4	ANNUN. 123 TROUBLE	12	ANNUN. 127 TROUBLE
	5	ANNUN. 123 NO ANSWER	13	ANNUN. 127 NO ANSWER
	6	ANNUN. 124 TROUBLE	14	ANNUN. 128 TROUBLE
	7	ANNUN. 124 NO ANSWER	15	ANNUN. 128 NO ANSWER
35025	0	REMOTE DISPLAY 1 TROUBLE	8	REMOTE DISPLAY 5 TROUBLE
	1	REMOTE DISPLAY 1 NO ANSWER	9	REMOTE DISPLAY 5 NO ANSWER
	2	REMOTE DISPLAY 2 TROUBLE	10	REMOTE DISPLAY 6 TROUBLE
	3	REMOTE DISPLAY 2 NO ANSWER	11	REMOTE DISPLAY 6 NO ANSWER
	4	REMOTE DISPLAY 3 TROUBLE	12	REMOTE DISPLAY 7 TROUBLE
	5	REMOTE DISPLAY 3 NO ANSWER	13	REMOTE DISPLAY 7 NO ANSWER
	6	REMOTE DISPLAY 4 TROUBLE	14	REMOTE DISPLAY 8 TROUBLE
	7	REMOTE DISPLAY 4 NO ANSWER	15	REMOTE DISPLAY 8 NO ANSWER

Table E.1 System Troubles Register Map *(Continued)*

Register	Bit No.	System Trouble Name	Bit No.	System Trouble Name
35026	0	REMOTE DISPLAY 9 TROUBLE	8	REMOTE DISPLAY 13 TROUBLE
	1	REMOTE DISPLAY 9 NO ANSWER	9	REMOTE DISPLAY 13 NO ANSWER
	2	REMOTE DISPLAY 10 TROUBLE	10	REMOTE DISPLAY 14 TROUBLE
	3	REMOTE DISPLAY 10 NO ANSWER	11	REMOTE DISPLAY 14 NO ANSWER
	4	REMOTE DISPLAY 11 TROUBLE	12	REMOTE DISPLAY 15 TROUBLE
	5	REMOTE DISPLAY 11 NO ANSWER	13	REMOTE DISPLAY 15 NO ANSWER
	6	REMOTE DISPLAY 12 TROUBLE	14	REMOTE DISPLAY 16 TROUBLE
	7	REMOTE DISPLAY 12 NO ANSWER	15	REMOTE DISPLAY 16 NO ANSWER
35027	0	REMOTE DISPLAY 17 TROUBLE	8	REMOTE DISPLAY 21 TROUBLE
	1	REMOTE DISPLAY 17 NO ANSWER	9	REMOTE DISPLAY 21 NO ANSWER
	2	REMOTE DISPLAY 18 TROUBLE	10	REMOTE DISPLAY 22 TROUBLE
	3	REMOTE DISPLAY 18 NO ANSWER	11	REMOTE DISPLAY 22 NO ANSWER
	4	REMOTE DISPLAY 19 TROUBLE	12	REMOTE DISPLAY 23 TROUBLE
	5	REMOTE DISPLAY 19 NO ANSWER	13	REMOTE DISPLAY 23 NO ANSWER
	6	REMOTE DISPLAY 20 TROUBLE	14	REMOTE DISPLAY 24 TROUBLE
	7	REMOTE DISPLAY 20 NO ANSWER	15	REMOTE DISPLAY 24 NO ANSWER
35028	0	REMOTE DISPLAY 25 TROUBLE	8	REMOTE DISPLAY 29 TROUBLE
	1	REMOTE DISPLAY 25 NO ANSWER	9	REMOTE DISPLAY 29 NO ANSWER
	2	REMOTE DISPLAY 26 TROUBLE	10	REMOTE DISPLAY 30 TROUBLE
	3	REMOTE DISPLAY 26 NO ANSWER	11	REMOTE DISPLAY 30 NO ANSWER
	4	REMOTE DISPLAY 27 TROUBLE	12	REMOTE DISPLAY 31 TROUBLE
	5	REMOTE DISPLAY 27 NO ANSWER	13	REMOTE DISPLAY 31 NO ANSWER
	6	REMOTE DISPLAY 28 TROUBLE	14	REMOTE DISPLAY 32 TROUBLE
	7	REMOTE DISPLAY 28 NO ANSWER	15	REMOTE DISPLAY 32 NO ANSWER
35029	0	SYSTEM INITIALIZATION	8	Reserved
	1	POWER SUPPLY COMM FAILURE	9	Reserved
	2	Reserved	10	Reserved
	3	Reserved	11	Reserved
	4	Reserved	12	Reserved
	5	Reserved	13	Reserved
	6	Reserved	14	Reserved
	7	Reserved	15	Reserved
35030	0	Reserved	8	Reserved
	1	Reserved	9	Reserved
	2	Reserved	10	Reserved
	3	Reserved	11	Reserved
	4	Reserved	12	Reserved
	5	Reserved	13	Reserved
	6	Reserved	14	Reserved
	7	Reserved	15	Reserved

Table E.1 System Troubles Register Map *(Continued)*

Register	Bit No.	System Trouble Name	Bit No.	System Trouble Name
35031	0	Reserved	8	Reserved
	1	Reserved	9	Reserved
	2	Reserved	10	Reserved
	3	Reserved	11	Reserved
	4	Reserved	12	Reserved
	5	Reserved	13	Reserved
	6	Reserved	14	Reserved
	7	Reserved	15	Reserved
35032	0	Reserved	8	NO POWER SUPPLY INST
	1	Reserved	9	LOOP 1-2 COMM FAILURE
	2	LINK PROTECTOR PRIMARY STATUS	10	LOOP 3-4 COMM FAILURE
	3	LINK PROTECTOR SECONDARY STATUS	11	LOOP 5-6 COMM FAILURE
	4	LINK PROTECTOR NOT PRESENT	12	LOOP 7-8 COMM FAILURE
	5	EVENT BUFFER 80% FULL	13	LOOP 9-10 COMM FAILURE
	6	EBI STATUS	14	TEST PROGRAM UPDATE
	7	SOFTWARE MISMATCH	15	HISTORY 80% FULL
35033	0	LOOP CONTINUITY TEST FAIL LOOP 1	8	LOOP CONTINUITY TEST FAIL LOOP 9
	1	LOOP CONTINUITY TEST FAIL LOOP 2	9	LOOP CONTINUITY TEST FAIL LOOP 10
	2	LOOP CONTINUITY TEST FAIL LOOP 3	10	UNPROGRAMMED DEVICE ON LOOP 1
	3	LOOP CONTINUITY TEST FAIL LOOP 4	11	UNPROGRAMMED DEVICE ON LOOP 2
	4	LOOP CONTINUITY TEST FAIL LOOP 5	12	UNPROGRAMMED DEVICE ON LOOP 3
	5	LOOP CONTINUITY TEST FAIL LOOP 6	13	UNPROGRAMMED DEVICE ON LOOP 4
	6	LOOP CONTINUITY TEST FAIL LOOP 7	14	UNPROGRAMMED DEVICE ON LOOP 5
	7	LOOP CONTINUITY TEST FAIL LOOP 8	15	UNPROGRAMMED DEVICE ON LOOP 6
35034	0	UNPROGRAMMED DEVICE ON LOOP 7	8	IR ENABLED ON LOOP 5
	1	UNPROGRAMMED DEVICE ON LOOP 8	9	IR ENABLED ON LOOP 6
	2	UNPROGRAMMED DEVICE ON LOOP 9	10	IR ENABLED ON LOOP 7
	3	UNPROGRAMMED DEVICE ON LOOP 10	11	IR ENABLED ON LOOP 8
	4	IR ENABLED ON LOOP 1	12	IR ENABLED ON LOOP 9
	5	IR ENABLED ON LOOP 2	13	IR ENABLED ON LOOP 10
	6	IR ENABLED ON LOOP 3	14	TRANSMIT/RECIEVE ERROR ABOVE LIMIT ON LOOP 1
	7	IR ENABLED ON LOOP 4	15	TRANSMIT/RECIEVE ERROR ABOVE LIMIT ON LOOP 2
35035	0	TRANSMIT/RECIEVE ERROR ABOVE LIMIT ON LOOP 3	8	TOO MANY DEVICES ON LOOP 1
	1	TRANSMIT/RECIEVE ERROR ABOVE LIMIT ON LOOP 4	9	TOO MANY DEVICES ON LOOP 2
	2	TRANSMIT/RECIEVE ERROR ABOVE LIMIT ON LOOP 5	10	TOO MANY DEVICES ON LOOP 3
	3	TRANSMIT/RECIEVE ERROR ABOVE LIMIT ON LOOP 6	11	TOO MANY DEVICES ON LOOP 4
	4	TRANSMIT/RECIEVE ERROR ABOVE LIMIT ON LOOP 7	12	TOO MANY DEVICES ON LOOP 5
	5	TRANSMIT/RECIEVE ERROR ABOVE LIMIT ON LOOP 8	13	TOO MANY DEVICES ON LOOP 6
	6	TRANSMIT/RECIEVE ERROR ABOVE LIMIT ON LOOP 9	14	TOO MANY DEVICES ON LOOP 7

Table E.1 System Troubles Register Map *(Continued)*

Register	Bit No.	System Trouble Name	Bit No.	System Trouble Name
35035	7	TRANSMIT/RECIEVE ERROR ABOVE LIMIT ON LOOP 10	15	TOO MANY DEVICES ON LOOP 8
35036	0	TOO MANY DEVICES ON LOOP 9	8	MISMATCHED LOOP TYPE ON LOOP 7
	1	TOO MANY DEVICES ON LOOP 10	9	MISMATCHED LOOP TYPE ON LOOP 8
	2	MISMATCHED LOOP TYPE ON LOOP 1	10	MISMATCHED LOOP TYPE ON LOOP 9
	3	MISMATCHED LOOP TYPE ON LOOP 2	11	MISMATCHED LOOP TYPE ON LOOP 10
	4	MISMATCHED LOOP TYPE ON LOOP 3	12	Ground Fault Port A
	5	MISMATCHED LOOP TYPE ON LOOP 4	13	Ground Fault Port B
	6	MISMATCHED LOOP TYPE ON LOOP 5	14	Amplifier Trouble
	7	MISMATCHED LOOP TYPE ON LOOP 6	15	AUXIN Trouble
35037	0	DIGIN Trouble	8	ANALOG OUTPUT A TROUBLE
	1	FFT TROUBLE	9	ANALOG OUTPUT B TROUBLE
	2	REMOTE MIC Trouble	10	ANALOG OUTPUT C TROUBLE
	3	DAP Port A Failure	11	ANALOG OUTPUT D TROUBLE
	4	DAP Port B Failure	12	FLASH IMAGE ERROR
	5	DAL No Answer	13	POWER SUPPLY TROUBLE
	6	LOCAL MIC TROUBLE	14	AMPLIFIER LIMIT
	7	LOCAL PHONE TROUBLE	15	AMPLIFIER SUPERVISION
35038	0	DAL ADDRESS CONFLICT	8	MAPPING IN PROGRESS LOOP 7
	1	DEVICE SERVICING REQUIRED	9	MAPPING IN PROGRESS LOOP 8
	2	MAPPING IN PROGRESS LOOP 1	10	MAPPING IN PROGRESS LOOP 9
	3	MAPPING IN PROGRESS LOOP 2	11	MAPPING IN PROGRESS LOOP 10
	4	MAPPING IN PROGRESS LOOP 3	12	DATABASE CORRUPTED
	5	MAPPING IN PROGRESS LOOP 4	13	AUDIO LIBRARY CORRUPTED
	6	MAPPING IN PROGRESS LOOP 5	14	DATABASE INCOMPATIBLE
	7	MAPPING IN PROGRESS LOOP 6	15	AUDIO LIBRARY INCOMPATIBLE
35039	0	DAL DOWNLOAD IN PROGRESS	8	PRIMARY AMP 1 TROUBLE
	1	FIRE VOICE TROUBLE	9	PRIMARY AMP 2 TROUBLE
	2	FIRE VOICE NO ANSWER	10	PRIMARY AMP 3 TROUBLE
	3	PHONE CHANNEL LIMIT EXCEEDED	11	PRIMARY AMP 4 TROUBLE
	4	NCM SMIFFER MODE ACTIVE	12	BACKUP AMP 1 TROUBLE
	5	LOCAL CONNECTION LIMIT EXCEEDED	13	BACKUP AMP 2 TROUBLE
	6	HARDWARE MISMATCH	14	BACKUP AMP 3 TROUBLE
	7	DAL DEVICE NO ANSWER	15	BACKUP AMP 4 TROUBLE
35040	0	DSBUS 1 COMMFAIL	8	Reserved
	1	DSBUS 2 COMMFAIL	9	Reserved
	2	DSBUS 3 COMMFAIL	10	Reserved
	3	DSBUS 4 COMMFAIL	11	Reserved
	4	AA TROUBLE BUS FAIL	12	Reserved
	5	NFN PAGING CHANNEL LIMIT EXCEEDED	13	Reserved
	6	Reserved	14	Reserved

Table E.1 System Troubles Register Map *(Continued)*

Register	Bit No.	System Trouble Name	Bit No.	System Trouble Name
35040	7	Reserved	15	Reserved
35041	0	Reserved	8	Reserved
	1	Reserved	9	Reserved
	2	Reserved	10	Reserved
	3	Reserved	11	Reserved
	4	Reserved	12	Reserved
	5	Reserved	13	Reserved
	6	Reserved	14	Reserved
	7	Reserved	15	Reserved
35042	0	Reserved	8	Reserved
	1	Reserved	9	Reserved
	2	Reserved	10	Reserved
	3	Reserved	11	Reserved
	4	Reserved	12	Reserved
	5	Reserved	13	Reserved
	6	Reserved	14	Reserved
	7	Reserved	15	Reserved
35043	0	Reserved	8	Reserved
	1	Reserved	9	Reserved
	2	Reserved	10	Reserved
	3	Reserved	11	Reserved
	4	Reserved	12	Reserved
	5	Reserved	13	Reserved
	6	Reserved	14	Reserved
	7	Reserved	15	Reserved
35044	0	Reserved	8	Reserved
	1	Reserved	9	Reserved
	2	Reserved	10	Reserved
	3	Reserved	11	Reserved
	4	Reserved	12	Reserved
	5	Reserved	13	Reserved
	6	Reserved	14	Reserved
	7	Reserved	15	Reserved
35045	0	Reserved	8	Reserved
	1	Reserved	9	Reserved
	2	Reserved	10	Reserved
	3	Reserved	11	Reserved
	4	Reserved	12	Reserved
	5	Reserved	13	Reserved
	6	Reserved	14	Reserved

Table E.1 System Troubles Register Map *(Continued)*

Register	Bit No.	System Trouble Name	Bit No.	System Trouble Name
35045	7	Reserved	15	Reserved
35046	0	Reserved	8	Reserved
	1	Reserved	9	Reserved
	2	Reserved	10	Reserved
	3	Reserved	11	Reserved
	4	Reserved	12	Reserved
	5	Reserved	13	Reserved
	6	Reserved	14	Reserved
	7	Reserved	15	Reserved
35047	0	Reserved	8	Reserved
	1	Reserved	9	Reserved
	2	Reserved	10	Reserved
	3	Reserved	11	Reserved
	4	Reserved	12	Reserved
	5	Reserved	13	Reserved
	6	Reserved	14	Reserved
	7	Reserved	15	Reserved
35048	0	Reserved	8	Reserved
	1	Reserved	9	Reserved
	2	Reserved	10	Reserved
	3	Reserved	11	Reserved
	4	Reserved	12	Reserved
	5	Reserved	13	Reserved
	6	Reserved	14	Reserved
	7	Reserved	15	Reserved

Appendix F Conversion to Modbus RTU

Modbus Gateway (acting as a Modbus slave) interfaces with a Modbus master through Modbus TCP protocol. The Moxa MGate MB3180 can be used to convert Modbus TCP protocol to Modbus RTU (Serial) protocol so that a Modbus RTU master can interface with the MODBUS-GW.

F.1 Hardware Configuration

Refer to the *Moxa MGate MB3180 Quick Installation Guide* for hardware configuration of the MB3180.

F.2 Software Configuration

Configure the MODBUS-GW as a node in the NFN network with a node number. Make sure the NFN network is stable. For details about network configuration, consult the *NOTI•FIRE•NET™ Network Systems Interface Manual* (P/N 51584) or *High Speed NOTI•FIRE•NET™ Instruction Manual*, (P/N 54013).

1. Connect the MB3180 to a configuration computer through an Ethernet cable as shown in Figure F.1.

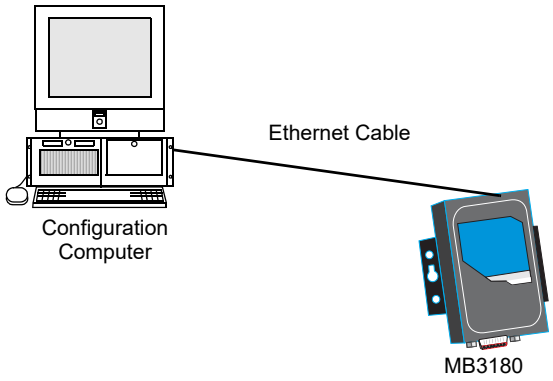


Figure F.1 Connect a Configuration Computer

2. Run the MGate Manager installation software (MGM_Setup_Ver*x.x*_Build_*xxxxxxxx*.exe) found on the Software CD shipped with the MGate MB3180.
3. Once the software has been installed, run MGate Manager.
4. Power up the MB3180. Make sure the “Ready” and “Ethernet” lights are on.
5. Configure the MB3180 for the network. The settings specified in Table F.1 are required. Settings not specified should be tailored to your network requirements. Refer to the *MGate MB3000 Modbus Gateway User’s Manual* for details.
6. When finished configuring, click **OK** to save the settings and **Exit** to close the MGate Manager.

Table F.1 MGate MB3180 Configuration Settings

Tab	Setting
Mode	RTU Master Mode
Slave ID Map	The MGate MB3180 monitors devices with virtual slave IDs in the range 1–99. By default, Modbus Gateway assigns each node on the NFN network a Modbus Unit ID equal to its node number. (The MGate MB3180 accepts the Modbus Unit ID as a virtual slave ID.) These numbers can be changed to fall within the range 1–99, but no more than 99 devices can be monitored. For more information about changing Modbus Unit IDs, refer to 3.2.5, "Additional Properties" under Node Mapping, Gateway Unit ID.
Modbus	Initial Delay: 0 ms Response Time-out: 1000 ms

F.3 Connecting the Moxa MGate MB3180 Interface to the MODBUS-GW

NOTE: The configuration used must have the approval of the AHJ (Authority Having Jurisdiction).

1. Connect the RTU master to the Serial port (RS232, RS485, RS422) of the MB3180.
2. Connect the MB3180 to the MODBUS-GW. Figures F.2 and F.3 show possible configurations for connecting the MODBUS-GW to the Moxa interface.
3. Power up the system.

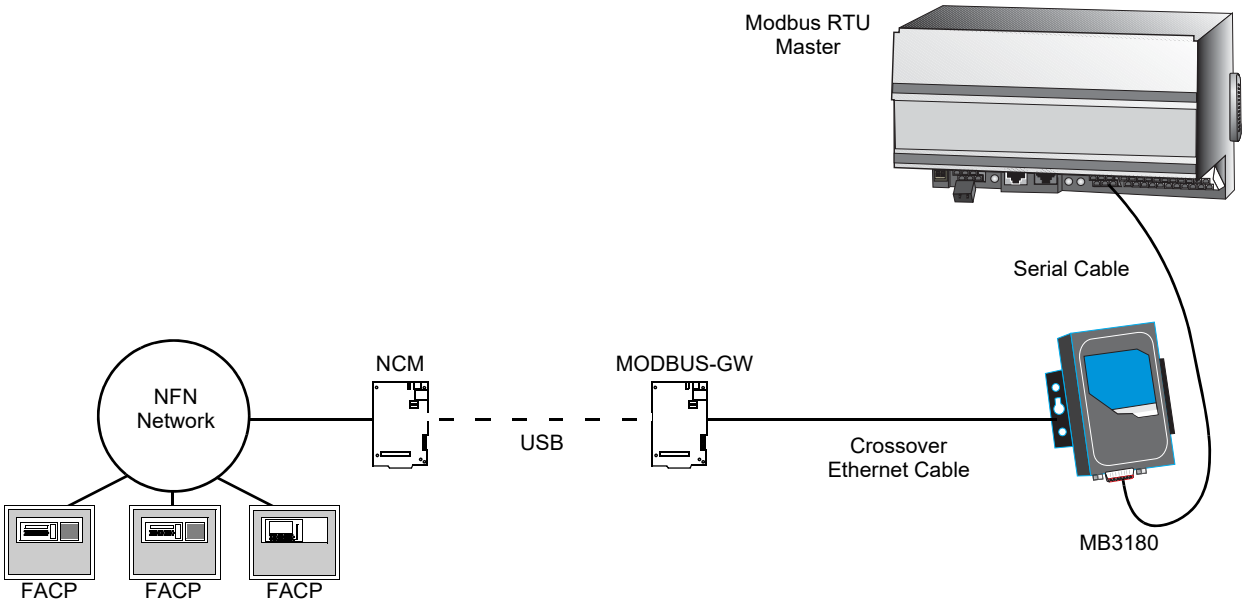


Figure F.2 Connection Through Crossover Ethernet Cable

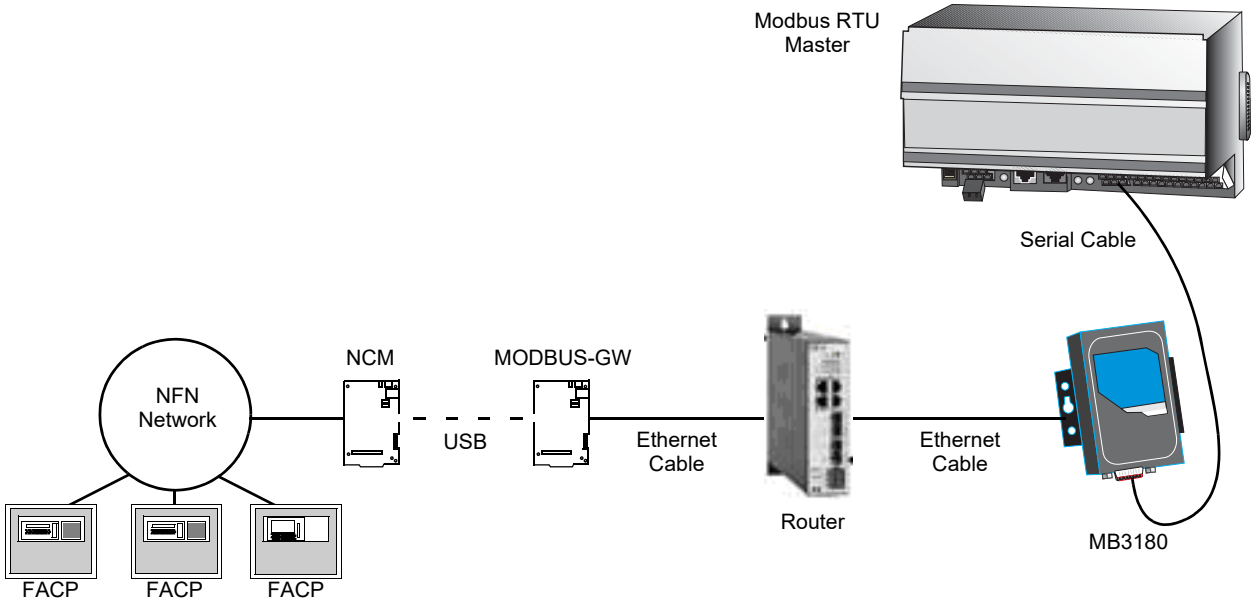


Figure F.3 Connection Through a Router

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