Honeywell

Honeywell Connected Life Safety Services

CLSS Gateway

HON-CGW-MBB

Installation and User Manual

LS10248-000HW-E

ECN: 00055952

REV. K | May 2025

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-ofrise feature of each detector should be tested at least once per year by a qualified fire protection specialist. Heat detectors are designed to protect property, not life.

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

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

• An emergency communication system may take priority over a fire alarm system in the event of a life safety emergency.

• Voice messaging systems must be designed to meet intelligibility requirements as defined by NFPA, local codes, and Authorities Having Jurisdiction (AHJ).

• Language and instructional requirements must be clearly disseminated on any local displays.

• Strobes can, under certain circumstances, cause seizures in people with conditions such as epilepsy.

• Studies have shown that certain people, even when they hear a fire alarm signal, do not respond to or comprehend the meaning of the signal. Audible devices, such as horns and bells, can have different tonal patterns and frequencies. It is the property owner's responsibility to conduct fire drills and other training exercises to make people aware of fire alarm signals and instruct them on the proper reaction to alarm signals.

• In rare instances, the sounding of a warning device can cause temporary or permanent hearing loss.

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

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

Alarm Signaling Communications:

• **IP connections** rely on available bandwidth, which could be limited if the network is shared by multiple users or if ISP policies impose restrictions on the amount of data transmitted. Service packages must be carefully chosen to ensure that alarm signals will always have available bandwidth. Outages by the ISP for maintenance and upgrades may also inhibit alarm signals. For added protection, a backup cellular connection is recommended.

• **Cellular connections** rely on a strong signal. Signal strength can be adversely affected by the network coverage of the cellular carrier, objects and structural barriers at the installation location. Utilize a cellular carrier that has reliable network coverage where the alarm system is installed. For added protection, utilize an external antenna to boost the signal.

• **Telephone lines** needed to transmit alarm signals from a premise to a central monitoring station may be out of service or temporarily disabled. For added protection against telephone line failure, backup alarm signaling connections are recommended.

The most common cause of life safety system malfunction is inadequate maintenance. To keep the entire life safety system in excellent working order, ongoing maintenance is required per the manufacturer's recommendations, and UL and NFPA standards. At a minimum, the requirements of NFPA 72 shall be followed. Environments with large amounts of dust, dirt, or high air velocity require morefrequent 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.

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 32ºC ± 2ºC (90ºF ± 3ºF). 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. Usestatic 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.

FCC REQUIREMENTS

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 online

Help or printed manuals, you can email us.

Please include the following information:

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

Send email messages to:

FireSystems.TechPubs@honeywell.com

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

TABLE OF CONTENTS

SECTION 1: GENERAL INFORMATION

1.1 ABOUT THIS MANUAL

This *CLSS Gateway Installation and Users' Manual* provides detailed procedures about installation, deployment, and upgrade of the gateway. The manual describes:

- the fixed CLSS Gateway,
- its installation environment,
- mounting and connecting the gateway circuit board to a fire detection panel, and
- initial gateway configurations

1.1.1 USING THIS MANUAL

This manual is written with the understanding that the user is trained in the operations and services required for this product.

1.1.2 USAGES

In this manual, product name usages are as below:

- The *CLSS Gateway* may also be referred as the *gateway*
- The *Connected Life Safety Services* mobile App may also be referred as the *CLSS App*
- The *CLSS Site Manager* may also be referred as *the Cloud*
- The term CLSS Gateway may refer to HON-CGW-MBB and CGW-MB, unless otherwise specified

1.2 INFORMATION SOURCES

Honeywell offers suitable information sources based on informational requirements.

1.2.1 TRAINING MODULES

Training modules are available when logged onto:

https://fire.us.honeywell.com/#/help-videos (For USA)

https://fire.eu.honeywell.com/#/help-videos (For Europe)

1.2.2 RELATED DOCUMENTS

The following table lists documents related to the CLSS Gateway:

Table 1.1
Related Document List

Product	For This Purpose...	Refer to...
CLSS Gateway:		
	Quick Installation and Setup	CLSS Gateway Quick Installation Guide P/N: 50151848-001
	Get comprehensive installation and configuration details	CLSS Gateway Installation and Users' Manual (This document) P/N: LS10248-000HW
	Configure for Honeywell Alarm Transmission Service	Supplement for Honeywell Alarm Transmission Service P/N: LS10248-152HW

Product	For This Purpose...	Refer to...
Gent Vigilon Panels:		
COMPACT-24-N	Installation	Installation Instructions - Vigilon Compact Panel Based Fire Detection and Alarm System P/N: 4188-1026
COMPACT-PLUS	Installation	Installation Instructions - Vigilon Compact Plus Panel Based Fire Detection and Alarm System P/N: 4188-1101
VIGPLUS-24 or VIGPLUS-72	Installation	Installation instructions Vigilon Plus 4/6 Loop Control Panel Based Fire Detection and Alarm System P/N: 4188-1100
Notifier Panels:		
NCA-2	Installation	NCA-2 Installation Manual P/N: 52482
NFS-320	Installation	NFS-320 Installation Manual P/N: 52745
	Programming	NFS-320 Programming Manual P/N: 52746
	Operation	NFS-320 Operations Manual P/N: 52747
	UL Listing Information	NFS-320 and NFS-320SYS Listing Document P/N: 52745LD
NFS-3030	Installation	NFS2-3030 Installation Manual P/N-52544
	Programming	NFS2-3030 Programming Manual P/N-52545
	UL Listing Information	NFS2-3030 UL Listing Document P/N: LS10006-051NF-E
NFS-640	Installation	
	Programming	
	UL Listing Information	
NFS2-640	Installation	
	Programming	
	Operation	
	UL Listing Information	
NFS2-3030	Installation	NFS2-3030 Installation Manual P/N-52544
	Programming	NFS2-3030 Programming Manual P/N-52545
	UL Listing Information	NFS2-3030 UL Listing Document P/N: LS10006-051NF-E
N16	Installation, Programming, Operation	N16 Instruction Manual P/N: LS10239-000NF-E
	UL Listing Information	N16 UL Listing Document P/N: LS10239-051NF-E
VeriFire® Tools:		

Product	For This Purpose...	Refer to...
	Software Installation	VeriFire® Tools Product Installation Guide P/N: 51690
	On-line Help	VeriFire® Tools Help Files
CLSS-Enabled LTE Commercial Fire Alarm Communicator:		
	Install and get started quickly	Getting Started with CLSS P/N: QHW-62051
	Installation and Operation	CLSS-Enabled LTE Commercial Fire Alarm Communicator Installation and Operating Guide P/N: LS10265-000HW-E
CLSS Connector Utility:		
	Install the utility and onboard the CLSS Gateway with a Central Monitoring Station	CLSS Central Station Onboarding Guide P/N: LS10378-000HW-E
CLSS Horizon:		
	Installation and Operation	CLSS Horizon Cloud Connected GUI Installation and Operation Manual P/N: LS10252-000HW-E
CLSS Central Station:		
	For events and their descriptions	Contact IDs for Central Station Quick Reference Sheet P/N: LS10378-351HW-E

1.3 ABBREVIATIONS USED

Table 1.2
Abbreviations List

Abbreviation	Description
CLSS	Connected Life Safety Services
DACT	Digital Alarm Communicator Transmitter
ESD	Engineered Systems Distributor
LTE	Long-Term Evolution The wireless broadband communication standard for mobile devices and data terminals.
NFN	NOTI-FIRE-NET™ The network interface for NOTIFIER™ Intelligent Fire Alarm Control Panels
NUP	NOTIFIER Universal Protocol The Universal Protocol by NOTIFIER for all fire alarm panel communications. This protocol enables direct transfer of data between the panels and networks, without the need to translate.
OC	Ownership Code The code that confirms ownership of the gateway
POTS	Plain Old Telephone Services
PSTN	Public Switched Telephone Network
TTL	Transistor-Transistor Logic A physical connection for performing both the logic gating and amplifying functions on the serial data.

Abbreviation	Description
UART	Universal Asynchronous Receiver/Transmitter A physical connection that converts and provides serial data for the panel and parallel data for the gateway.
USB	Universal Serial Bus

1.4 APPROVALS

UL
S35608
FCC

FCC ID: PV3CGWMB

Compliance Statements:

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

01. This device may not cause harmful interference.
02. This device must accept any interference received, including, an interference that may cause undesired operation.

Caution Statements:

• Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.
• This equipment should be installed and operated with a minimum distance of 20 cm between the radiator and your body.

Industry Canada (IC) Statement

IC ID: 1609A-CGWMB

Compliance Statements: This device complies with Industry Canada license-exempt RSS standard(s). Operation is subject to the following two conditions: 1) This device may not cause interference., 2) This device must accept any interference, including interference that may cause undesired operation of the device.

Déclarations de conformité: Le présent appareil est conforme aux CNR d'Industrie Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes : (1) l'appareil ne doit pas produire de brouillage, et (2) l'utilisateur de l'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.

Caution Statements:

• This equipment complies with radio frequency exposure limits set forth by Industry Cananda for an uncontrolled environment.
• This equipment should be installed and operated with a minimum distance of 20 cm between the device and the user or bystanders.

Déclarations de mise en garde:

• Cet équipement est conforme aux limites d'exposition aux radiofréquences défines par Indstrie Canada pourun environment non contrôlé.
• Cet équipement doit être installé et utilisé aven un minimum de 20 cm de distance dispositif et l'utilisateur ou des tiers.

Intertek

ID: 104270338NYM-001

NFPA Compliance (USA)

Install the CLSS Gateway in accordance with the *National Fire Protection Association Installation Standard* NFPA 72.

CSFM

CSFM ID: 7300-1637:0504

FDNY

COA# 2020-TMCOAP-000121-AMND
COA# 2020-TMCOAP-000122-AMND
COA# 2021-TMCOAP-001761-CERT
COA# 2021-TMCOAP-006279-AMND

1.5 WARNINGS AND CAUTIONS IN THIS MANUAL

WARNING: These instructions contain procedures to follow to avoid injury and damage to equipment. It is assumed that the user of this manual has been suitably trained and is familiar with the relevant regulations.

CAUTION: USERS MUST FOLLOW THE PROCESSES AND USAGES APPROVED AS PER THE REGULATORY COMPLIANCE. A CHANGED OR MODIFIED USAGE NOT EXPRESSLY APPROVED BY COMPLIANCE COULD VOID THE USER'S AUTHORITY TO OPERATE THE CLSS Gateway.

1.6 THE PRODUCT STANDARDS

CE This gateway's panel is CE Marked to show that it conforms to the requirements of the following European Community Directives:

Electro Magnetic Compatibility (EMC) Directive	2014/30/EU
Low Voltage Directive (LVD)	2014/35/EU
Radio Equipment Directive	2014/53/EU
RoHS Directive	2011/65/EU
Safety LVD Directive	2014/35/EU
Green Directive	2011/65/EU, (EU) 2015/863
WEEE Directive	2012/19/EU

1.7 DISCLAIMER

Images in the document are for reference purpose only and are subject to change. All trademarks, service marks, word marks, design marks, and logos are property of their respective owners.

SECTION 2: OVERVIEW

CLSS Gateway is an embedded and intelligent gateway for connected buildings. It enables system maintenance providers as well as end users to remotely manage connected fire detection systems. The gateway also supports them to ensure compliance.

2.1 OPERATION

The gateway acts as a portal among fire alarm panels, *CLSS Site Manager*, and peripheral devices. The gateway connection with the fire alarm panel enables reading the inventory and transmitting the data. Connection with the *CLSS Site Manager* facilitates remotely monitoring and managing the fire detection systems.

2.2 HONEYWELL CONNECTED LIFE SAFETY SERVICES

The software suite enables remote management of fire detection systems. It monitors the building's fire system events in real-time and notifies users about the events immediately. It also supports periodic maintenance activities and helps in reports generation.

2.3 GATEWAY BOARD LAYOUT

The illustration below points out those parts that are used for connections and trouble shooting.

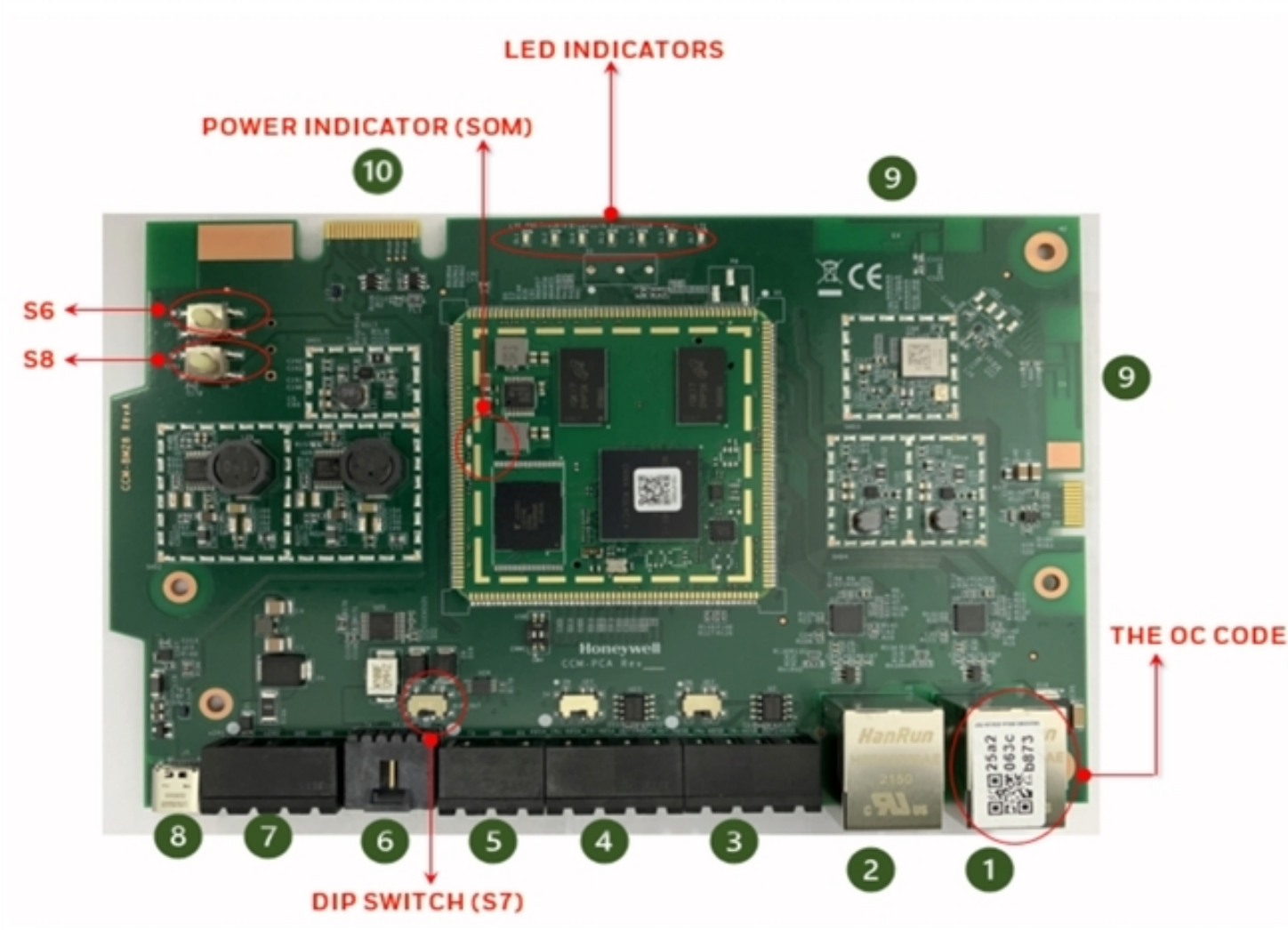


Figure 2-1: Printed Circuit Board: Layout

2.3.1 CONNECTING INTERFACES

Figure 2-2: The LED Indicators on the Gateway uses numbered labels to show the location of the interfaces for connections. This manual uses these numbered labels at various places for your convenience.

The table below uses these numbered labels to describe the type and usage of the interfaces.

Table 2.1 Gateway Interface Details

Number in the Figure	Interface Type	Interface Name	Label Name	Usage
1	Ethernet 1	J4	J4	Primary Ethernet port (Eth1) that can permanently connect the gateway board with the CLSS Gateway services or a Modbus client/server. The Ownership Code (OC) on it confirms the ownership of the board. It should be registered in the *CLSS Site Manager* during the first time installation of the CLSS Gateway. Cable: CAT 5 standard Ethernet cable with RJ45 connector
2	Ethernet 2	J3	J3	Secondary Ethernet port (Eth0) providing a TCP/IP connection to a configuration computer. Cable: CAT 5 standard Ethernet cable with RJ45 connector
3	RS-485B	P5	P5	Receives the alarm data and device data from an RS-485 port of a panel.
4	RS-485A	P1	P1	Receives the alarm data and device data from an RS-485 port of a panel.
5	UART/TTL	P4	P4	Receives the alarm data and device data from a UART/TTL port of a panel.
6	NUP (RS-232)	P7	P7	Transfers fire-related and device-related data from the panel to the *CLSS Site Manager* through the gateway. It also helps in administering the fire detection system. Connects the gateway board to a panel's RS-232 port. If the connected panel supplies power, the gateway would get power from the panel through the RS-232 port.
7	Power	P2	P2	Connects to an external 24-volt DC power when required. It uses a power-limited, regulated, power-supply-listed connection for fire-protective signaling. Twisted-unshielded pair, 12 to 18 AWG (3.31 mm² to 0.82 mm²) It is used only when the gateway board is connected with: • A network card or • When power is not supplied to the NUP connector
8	USB	J5	J5	Receives the alarm data and device data from a USB port of a panel.
9	Wireless Aerial		E4	Wireless antenna
10	Cellular		4D	40-pin connector for the compatible cellular module.

2.3.2 LED INDICATORS

The LED indicators on the gateway board use different colors to identify the operational status of the gateway. To know the location of the LED indicators on the gateway board, refer to Figure 2-1: Printed Circuit Board: Layout .

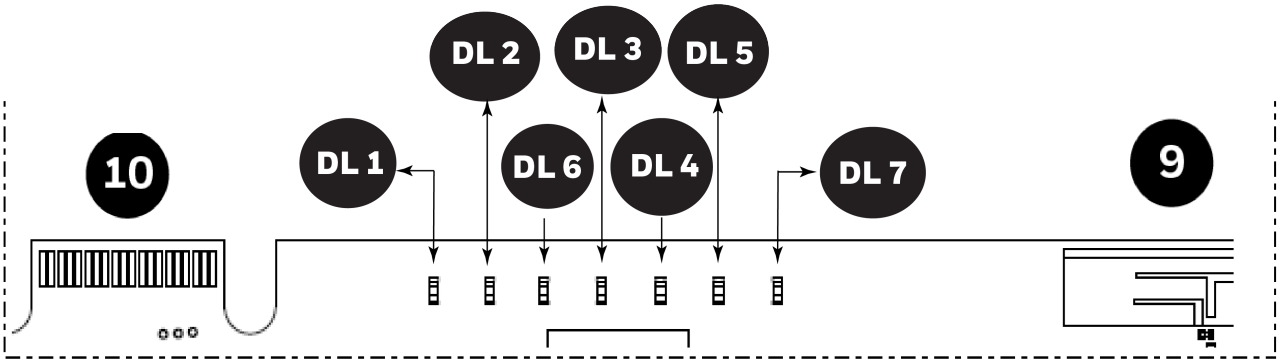


Figure 2-2: The LED Indicators on the Gateway

Table 2.2
LED Indicators and Their Messages

SOM Power-Indicating LED Indicates the gateway board's received power status. See "Power Indicator" in Figure 2-1: Printed Circuit Board: Layout .	
green	**ON** The circuit board is receiving 24V power from its power source. **OFF** The circuit board is *not* receiving power.
DL1 LTE Power LED Indicates the power supply status for cellular communications	
green	**ON** The LTE radio device is receiving power from the circuit board. **OFF** The LTE radio device is *not* receiving power.
DL2 Trouble LED Indicates the gateway's operational status	
amber	**OFF** There are no issues. **FLASHING SLOW** (flashes once per 1 second) There are communication issues with the panel or the Internet connectivity. **ON** There is a critical error in the system. To fix the issues, you can refer to the 6.2 Troubleshooting section, which discusses about some possible issues and their solutions.
DL6 Mobile Connectivity LED Indicates the status of mobile communications between the gateway and the CLSS App.	
Blue	**FLASHING SLOW** (flashes once per 1 second) The gateway is connected to the CLSS App. **FLASHING FAST** (flashes once per 0.25 second) The gateway is ready for the CLSS App connection. **OFF** The mobile connectivity is disabled.
DL3 Panel Connectivity LED Indicates the connection status of the panel	
green	**FLASHING SLOW** (flashes once per 1 second) The panel is connected with the gateway board. **FLASHINGFAST** (flashes once per 0.2 second) The gateway is fetching the inventory data. **ON** Configuration mode is enabled for configuring the gateway network settings. **OFF** The gateway is *not* communicating with the panel.
DL4 CLSS Site Manager Connectivity LED Indicates the gateway connection status with *CLSSSite Manager*	

green	**ON** The gateway is downloading the firmware from the *CLSSSite Manager*. **FLASHINGSLOW** (flashes once per 1 second) The gateway is connected with *CLSS Site Manager*. **FLASHINGFAST** (flashes once per 0.2 second) The gateway is connected with Internet, but not connected with the *CLSS Site Manager*. **OFF** The gateway is *not* connected with Internet.
DL5 **Wireless Connectivity LED** Indicates the gateway wireless connectivity status	
green	**FLASHING SLOW** (flashes once per 1 second) The wireless connectivity is enabled for the *CLSS Site Manager* connection. **OFF** The wireless connectivity is disabled.
DL7 **Cellular Connectivity LED** Indicates the LTE radio connection status	
green	**FLASHING SLOW** (flashes once per 1 second) The LTE radio is transmitting data. **FLASHING FAST** (flashes once per 0.2 second) The LTE radio may have a connectivity issue, which requires attention. **OFF** There is no cellular connection.

2.3.3 SWITCHES ON THE GATEWAY BOARD

Below table informs about the switches on the gateway board. To locate the switches on the gateway board, refer to Figure 2-1: Printed Circuit Board: Layout .

Table 2.3
Gateway Board Switches

Switches	Purpose
S6	For securely configuring the gateway's settings Pressing the switch for six seconds switches the gateway board to the configuration mode.
S7	For changing the direction of the 24V power of the NUP/RS-232 connector NUP_IN: The gateway board receives power through its NUP/RS-232 port. NUP_OUT: The gateway board receives power through its power supply port, which is connected to an external power supply source.
S8	For enabling mobile pairing Pressing the switch for ten seconds enables mobile pairing.

Tamper Switches	
Tamper 1	For alerting whenever the gateway enclosure door is opened It is located at the front-side of the gateway, next to the LED indicators.
Tamper 2	For alerting whenever the gateway board is removed from the enclosure It is located at the backside of the gateway.

2.4 CLSS GATEWAY PARTS

Part Number	Description
HON-CGW-MBB	CLSS Gateway with enclosure
CGW-MB	CLSS Gateway board
CGW-BB	CLSS Gateway enclosure
50160636-001	CLSS Gateway kit. It includes a 30” NUP cable and a NOTIFIER lock and key set.
32351718-001	10 ft NUP Serial (RS-232) cable kit
CCM-VZ-HON	CLSS Verizon cell module
CCM-ATT-HON	CLSS AT&T cell module

SECTION 3: SECURITY RECOMMENDATIONS

3.1 FOR USERS

An administrator should:

- Regularly review the user roles and permissions for a CLSS account
- Immediately remove users who should no longer have access to CLSS

A technician should:

- Use discretion to allow or deny a location access request.
- Disconnect the *CLSS App* from the *CLSS Gateway*, once the required activity is completed.
- Turn OFF the location access in the CLSS App's **Security Settings**, when location access is not required.

3.2 FOR PREVENTING POTENTIAL RISKS

Security threats applicable to networked systems include unauthorized access, communication snooping, viruses, and other malicious software agents. Please refer to below sections to understand and implement appropriate security controls to avoid/mitigate the potential risks.

3.2.1 UNAUTHORIZED ACCESS

Unauthorized access results from unsecured user name and password, uncontrolled access to the equipment, or uncontrolled and unsecured access to the network.

It results the following:

- Loss of system availability
- Incorrect execution of controls causing damage to the equipment
- Incorrect operation, spurious alarms, or both
- Theft or damage to the contents of the system
- Capture and modification or deletion of data causing possible liability to the installation Site and Honeywell

3.2.2 USER ACCESS AND PASSWORDS

Observe the following good practices:

- The password has one numerical, one upper case, one lower case, and one special character whenever any user registers or changes the credentials.
- Enforce a password change periodically
- Do now allow any dictionary words as passwords
- Check passwords against known common weak password databases
- Do not allow common and predictable passwords though they meet other requirements. For example: P@SSw0rd
- Not allow usernames, service names, or any such context-specific words
- Passwords should be complex and not easily guessed; and, should not contain phrases used in common speech.
- Do not use personally identifiable information as a password, such as social security numbers, addresses, birth dates.
- Provide only the minimum level of access and privileges for each user.
- Ensure physical security of passwords. Avoid and warn against writing user names and passwords where they can be seen by unauthorized personnel.
- Periodically audit user accounts and remove any that are no longer required.

3.2.3 MEMORY MEDIA

Use only authorized removable media.

Use an up-to-date anti-virus software to scan the removable media and check for viruses and malware.

Ensure that the memory media is not used for other purposes to avoid risk of infection.

Control access to media containing backups to avoid risk of tampering.

3.2.4 SOFTWARE AND FIRMWARE UPDATES

System software and firmware updates may be offered from time to time.

Ensure that your local representative:

- Has the up-to-date contact details, and
- Periodically visits the Honeywell web site for up-to-date product information
- Regularly updates the software/firmware of the devices to the latest available version to get important security updates

3.2.5 VIRUSES AND OTHER MALICIOUS SOFTWARE AGENTS

Malicious Software include the following:

- Viruses
- Spyware
- Worms
- Trojans

These may be present in a computer using a Monitoring Station Software or in a USB pen drive, which is used to copy data to computer.

The intrusion of malicious software agents can result in performance degradation, loss of system availability, and the capture, modification, or deletion of data — including configuration and device logs.

USB devices from other infected systems on the network or malicious Internet sites can also transfer viruses.

3.2.6 NETWORK AND FIREWALL SETUP

Inbound (In) Port: The port another computer uses to access a gateway functionality. An application on the gateway will be actively listening on this port for client connections.

Outbound (Out) Port: The gateway uses outbound ports to connect to Internet or *CLSS Site Manager*. The Cloud services in the *CLSS Site Manager* will be listening on these ports waiting for a connection from the gateway.

By default, block all inbound and outbound connections and allow only the ports listed in the below table:

Port Number	Type	IN/OUT	Purpose/Remarks
53	UDP and TCP	Out	DNS Rsolution
443	TCP	In/Out	HTTPS Communication
2020	TCP	In/Out	Alarm Transmission

NOTE: Please refer to the respective feature section (LCH/Modbus/Bacnet) for additional ports (if any) that need to be whitelisted based on the use-case.

Ensure that access to the below endpoints is allowed by your Organization's IT/Firewall team to enable Gateway's connectivity to CLSS Platform Services:

Reigon	URL/End-Points
Global	https://gaprodpkisystemauthenticationv2.sentience.honeywell.com/ https://gaprodregui.sentience.honeywell.com/ https://sentgaprod.blob.core.windows.net
Europe	https://t02aprodfileupload.sentience.honeywell.com/ https://sentt02aprodfu.blob.core.windows.net https://sentt02aprodv2.azure-devices.net/ https://iotvnextprodhbteu.blob.core.windows.net/ https://t02aprodcloudapp.sentience.honeywel.com
US	https://t01aprodfileupload.sentience.honeywell.com/ https://sentt01aprodfu.blob.core.windows.net https://sentt01aprodv2.azure-devices.net/ https://iotvnextprodhbt.blob.core.windows.net/ https://t01aprodcloudapp.sentience.honeywell.com

Reigon	URL/End-Points
US Alarm Transmission	https://honprodeast.rrmsalarm.com https://honprodwest.rrmsalarm.com https://honrtprodeast.firesignals.us https://honrtprodwest.firesignals.us

3.2.6.1 Best Practices

3.2.6.1.1 Network Security

Open protocols, unencrypted connections, and unauthenticated sites are risks.

Ensure the following:

- Required firewalls and VPN connections are in place
- The logging systems monitor malicious activity and perform regular audits
- Unused services and ports are disabled
- Security patches are up to date
- Users have only minimum required privileges for files and folders

3.2.6.1.2 Connecting to Wireless networks.

Whenever connecting to a Wi-Fi network:

- Make sure that the access point/ hotspot uses a strong password for network access.
- Access point should upgrade any WiFi Protected Access (WPA) protocol to WPA2 or higher. WPA is vulnerable to intrusion and can no longer be trusted.

3.2.6.1.3 Connected Devices

In case of use of ethernet port for connecting the Gateway to a Fire-Panel/ Vesda-Detector:

01. If the Gateway connects to the Fire panel/ Vesda Detector over Ethernet port 2 and connects to CLSS Cloud or LCH over Ethernet port 1, the IP addresses of these two ethernet ports should be in different subnets.
02. For connections from Gateway to Fire panel/ Vesda Detector over ethernet, the use of a short point-to-point (peer-to-peer) cable is recommended.
03. Further, the interface connecting to CLSS Cloud must be monitored/ managed by the Organization's IT team with the necessary firewall controls in place to detect/ avoid any network attacks.

For example, if Ethernet port 2 and fire panel are in the 192.168.10.0/24 subnet, then use 192.168.1.0/24 subnet for Ethernet Port1/ WLAN for CLSS Cloud connectivity or LCH.

NOTE: When using Vesda detectors, adhere to the Xtralis security guidelines: https://xtralis.com/file/9584

SECTION 4: INSTALLATION

You can use a fixed gateway in the fire detection system.

CAUTION: This section refers to the fixed gateway P/N: HON-CGW-MBB. For instructions on mounting the portable gateway, P/N: CGW-MB, refer to the NBB-2 installation document LS10250-000NF-E

CAUTION: The gateway must be installed indoors in a dry location.

CAUTION: Install as per the local building as well as customer-specific requirements. For example, installing and operating the gateway with its wireless technology might be restricted near medical equipment, fuels, or chemicals. Ensure that there are no conflicts.

4.1 WALL MOUNTING THE FIXED GATEWAY

It is recommended to keep the gateway within 1 meter (3-feet) from the connected panel or the network card. The minimum distance between the gateway and the panel should be 30 cm.

NOTE: In a low LTE signal area, you may choose to use external aerials.

CAUTION: The equipment is suitable for mounting at a maximum height of 9.9 feet only.

Follow the instructions below to mount the gateway enclosure:

01. Open the package and take out the contents.
02. Inspect the contents for damage. If there is any damage, do not proceed with installation. Return the package.
03. Place the right-side door edge on a flat surface for support.
04. At the right-side door edge, punch out a hole for the door locking screw or for an optional keyed lock (see"Screw Hole Knock Out" below).

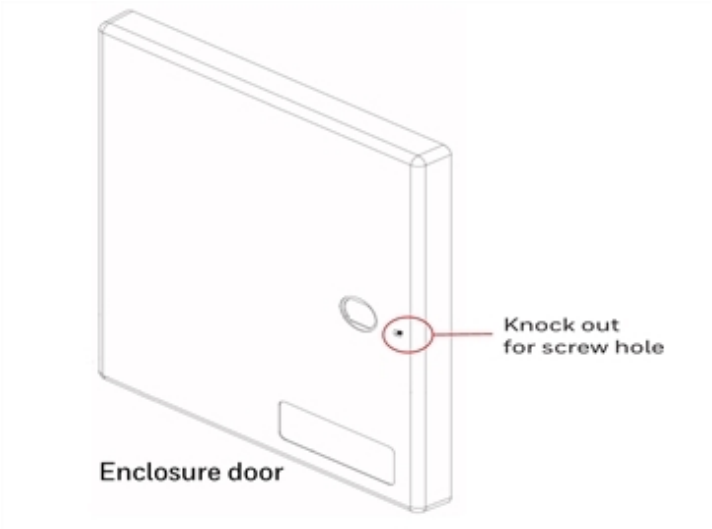


Figure 4-1: Screw Hole Knock Out

05. Depending upon the wall construction, select suitable screws to mount the enclosure.
06. Place the backbox on the wall where the enclosure is to be mounted.

07. Confirm that the placement of the backbox allows the door to swing open freely.
08. Mark and pre-drill the hole for the top mounting bolt (see"Mounting the Backbox" below).

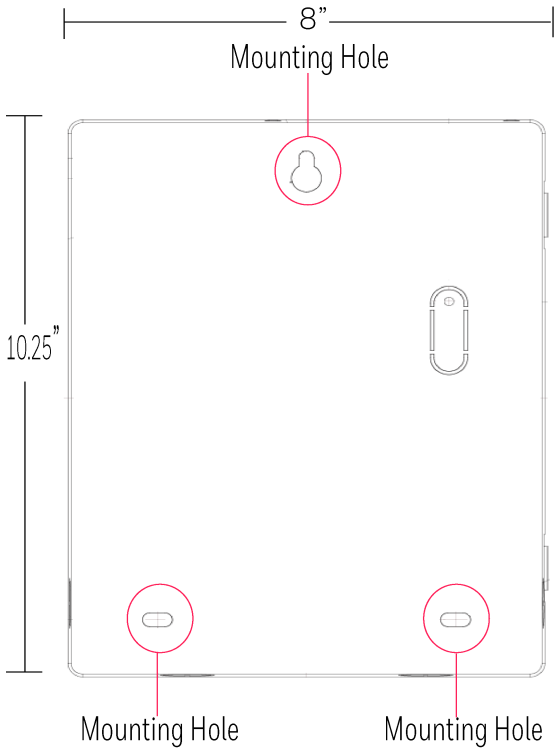


Figure 4-2: Mounting the Backbox

09. Remove the backbox.
10. In the top mounting hole, insert the mounting screw.
11. Tighten the screw, leaving space for hanging the enclosure.
12. Mount the backbox over the top screw and level it.
13. Mark the locations for the two lower mounting holes.
14. Remove the backbox and drill the mounting holes.
15. Mount the backbox over the top screw, then install the remaining fasteners.
16. Tighten all fasteners securely.

4.2 MOUNTING THE PORTABLE GATEWAY

Section reserved for future functionality.

4.2.1 MOUNTING ONTO THE CHASSIS

Section reserved for future functionality.

4.3 GATEWAY BOARD CONNECTION OPTIONS

The gateway board can be connected with a cellular module, wireless aerials, the *CLSS Site Manager*, a configuration computer, a panel, a mobile device, and an external power supply.

Figure 4-3: Gateway Connections - Top Side illustrates the connection options at the top side of the gateway board.

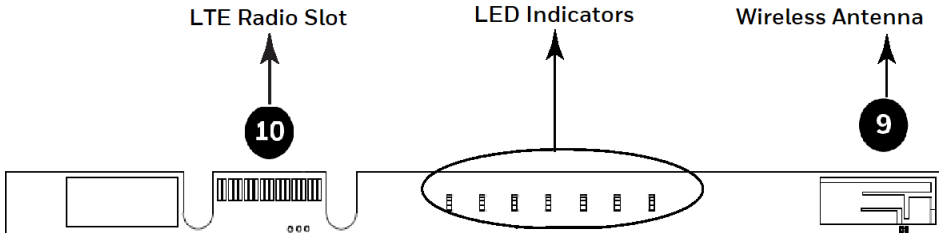


Figure 4-3: Gateway Connections - Top Side

Figure 4-4: Gateway Connection Options - Bottom Side illustrates the gateway connection options at the bottom side of the gateway board.

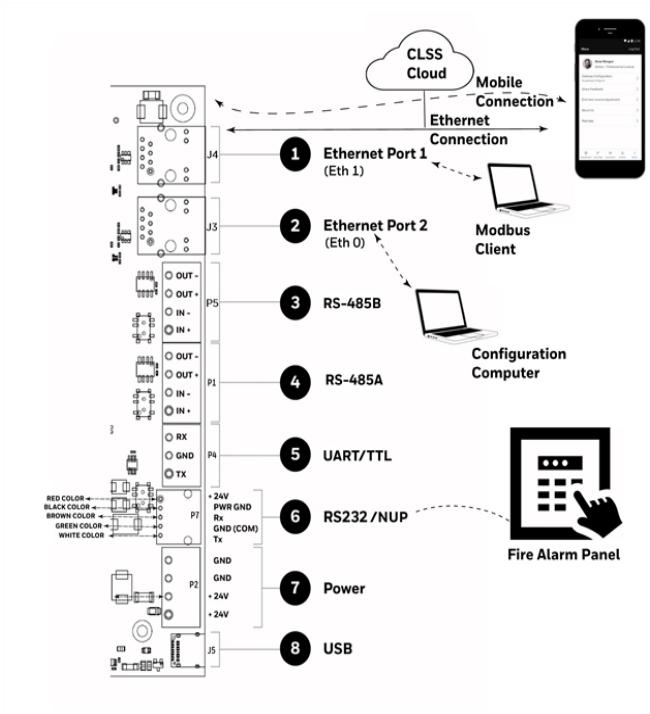


Figure 4-4: Gateway Connection Options - Bottom Side

4.3.1 CONNECTING TO A FIRE ALARM PANEL

To know about supported panel variants, their connection options, and commissioning procedure, refer to the Appendix C: Connecting to the Panels .

4.3.2 INSTALLING A SINGLE SIM CELLULAR MODULE (CCM-ATT-HON, CCM-VZ-HON,CCM-EU)

To use *CLSS Site Manager* and to provide value-added alarm transmission services with a cellular connection, plug in the cellular module onto the gateway board.

4.3.2.1 Compatibility Requirements

To ensure proper operation, these cellular module shall be compatible with the CLSS Gateway.

To know more about the supported devices, refer to Appendix D: Compatible Cellular Modules .

4.3.2.2 Before Installing a Cellular Module

• If installing on an existing operational gateway, inform the operator and local authority that the gateway will be temporarily out of service.
• Disconnect power to the gateway.

4.3.2.3 Precautions for Service Quality

• Carefully select the installation location of the CLSS Gateway.
• Do not mount the gateway on or near metal objects. This includes steel cabinets, metal walls, steel beams, steel roofs or roofing girders, foil backed insulated walls, and duct works.
• During the installation, periodically monitor the signal quality via the CLSS App to predict QoS (Quality of Service) of the LTE radio over time.
If the installation location does not offer good QoS, try the following options:

01. Move the gateway to achieve the best QoS. Typically, moving it to a higher placement offers the best QoS.
02. Use an optional antenna external aerial connection. Antenna must be located in the same room as the CLSS Gateway enclosure. Refer to the 4.3.2.8 Installing the External Aerials for Single Sim Cellular Module (CCM-ATT-HON, CCM-VZ-HON,CCM-EU) for details.

4.3.2.4 To Install a Single Sim Cellular Module (CCM-ATT-HON, CCM-VZ-HON,CCM-EU)

The installation involves plugging the cellular module onto the gateway board, and securing the mounted device with a retention strap. The strap will compress the RF ground system between the cellular modules and the gateway board assembly.

01. Switch OFF the gateway.
02. Punch out the appropriate knockouts on the enclosure for the aerials (see Figure 4-5: Knockouts on the Enclosure).

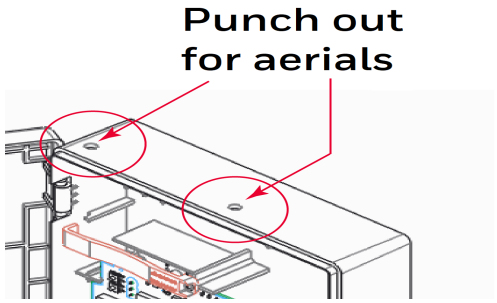


Figure 4-5: Knockouts on the Enclosure

03. Open the enclosure door.

04. On the top edge of the gateway, plug the cellular module onto the 40-pin expansion slot (see Figure 4-6: Installing the Cellular Module).
Do not use the screw on the top edge of the Cellular module. It will adversely affect the radio performance. Refer to the Do Not Use This Screw shown in Figure 4-4: Gateway Connection Options - Bottom Side .

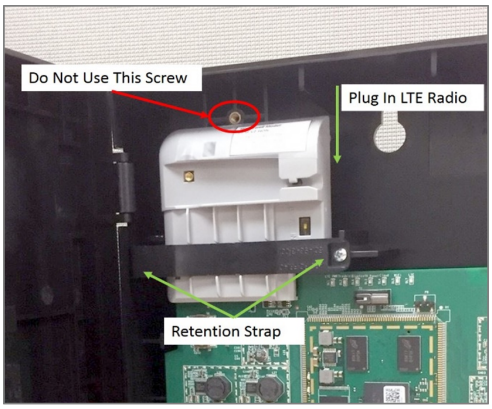


Figure 4-6: Installing the Cellular Module

05. Secure the cellular module with the retention strap and a screw, which come with the module (see Figure 4-6: Installing the Cellular Module).
Failure to use the retention strap may adversely affect the aerial performance.

4.3.2.5 How to Install a CLSS Gateway Single Sim Cellular Module (CCM-ATT-HON, CCM-VZ-HON,CCM-EU)

The installation involves plugging the cellular module onto the gateway board and securing the mounted device with a retention strap. The strap will compress the RF ground system between the cellular modules and the gateway board assembly. The CLSS Gateway has a two on board indicators to identify the cellular module installed (DL1) and Cellular Connection (DL7) refer to the table below.

LED Indicator	State	Definition
DL1	ON	The cellular module is installed and receiving power.
	OFF	The cellular module is not installed.
DL7	Flashing Slow	(Flashes once per 1 second) The LTE radio is transmitting data.
	Flashing Fast	(Flashes once per 0.2 second) The LTE radio may have a connectivity issue, which requires attention.
	OFF	There is no cellular option

4.3.2.6 Verifying the CLSS Gateway Cellular Signal Strength

Once the CLSS Gateway is activated through the CLSS Mobile app, to check the signal strength of the CLSS Gateway Cellular Module you can log into the CLSS Site Manager or CLSS Mobile App. After you log into the CLSS, navigate to the specific customer/site to view the CLSS Gateway Diagnostics tab. Honeywell recommends that the signal strength rating should be a 3 (Good) or above for a consistent good connection. If the signal rating is lower than 3, reposition the antenna and monitor the signal strength bars in the CLSS App.

NOTE: The signal bar shown is in the rating format

Signal Level	Signal Status	Rating
	Excellent	4
	Good	3
	Poor	2
	Bad	1
Not Connected	**No Signal**	0

4.3.2.7 Replacing the SIM Card in Single Sim Cellular Module (CCM-ATT-HON, CCM-VZ-HON,CCM-EU)

The cellular module comes with a factory-mounted SIM card. If necessary, replace it as follows:

01. Open the gateway door.
02. Remove the NUP cable or the 24v DC power cable to switch OFF the gateway board.
03. Remove the retention strap screw and the retention strap (see"Installing the Cellular Module" on the previous page).
04. Slide the cellular module upward to disconnect it from the gateway board.
05. Carefully remove the back cover of the cellular module.
    Find the SIM card holder and slide its door to unlock (see "Unlock or Lock Movement" below).

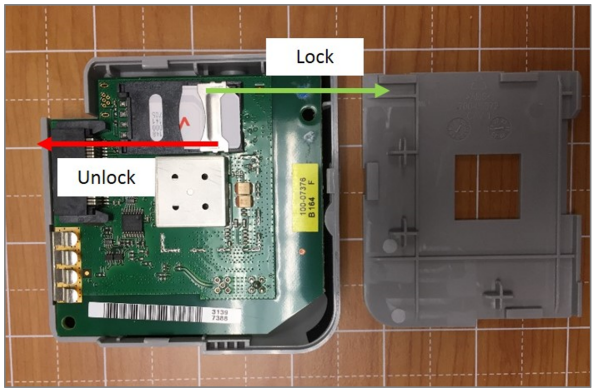


Figure 4-7: Unlock or Lock Movement

06. Remove the old SIM card and replace it with the new card.
07. Slide the card holder door back and lock it (see "Unlock or Lock Movement" above).
08. Place the bottom cover onto the communicator and snap it closed.

4.3.2.8 Installing the External Aerials for Single Sim Cellular Module (CCM-ATT-HON, CCM-VZ-HON,CCM-EU)

In a low LTE signal area, using an external aerial may boost the signals.

When installing an aerial, ensure that:

- The aerial is within its granted FCC directional gain limitations

FCC ID: RI7LE910NAV2, IC: 5131A-LE910NAV2		
BAND	**FREQUENCY**	**DIRECTIONAL GAIN**
Band 12 and 13	699 – 787 MHz	6.63 dBi
Band 5	824 – 894 MHz	6.63 dBi
Band 4	1710 -1745 MHz	6.00 dBi
Band 2	1850 – 1990 MHz	8.51 dBi

CCM-VZ-AN and CCM-VZ-HON RI7LE910SVV2, IC: 5131A-LE910SVV2		
BAND	**FREQUENCY**	**DIRECTIONAL GAIN**
Band 13	746 – 787 MHz	6.63 dBi
Band 4	1710 -1745 MHz	6.63 dBi
Band 2	1850 – 1990 MHz	8.51 dBi

- The installation is in accordance with the manufacturer's instructions

To Install an External Antenna

01. Switch the SW1 switch on the cellular module to EXT.
02. Connect the internal coax adapter to the module.
03. Route the coax adapter cable through the knock out on the enclosure.
04. Tighten the nuts at both sides of the knock out.
05. Take the external antenna.
06. Thread the antenna onto the antenna connector and tighten it.
07. (If there is a magnet at the bottom of the antenna) Attach the magnet to the top wall of the enclosure.
    Or
    (Optional) Use a double-sided adhesive tape to secure the attachment.

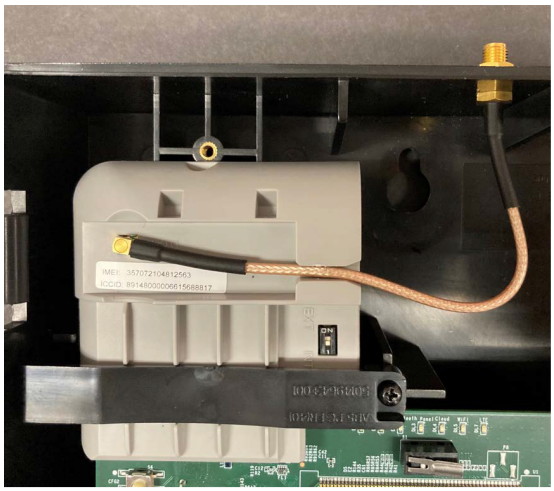


Figure 4-8: Installing an External Antenna

4.3.3 INSTALLING A DUAL SIM CELLULAR MODULE

The CLSS Dual SIM 4G LTE Cellular Module for the CLSS Gateway provides global connectivity and ensures stable network performance even in harsh signal conditions. It features a dual SIM design, and a high-performance antenna included with the module for greater range and reliability. The module supports redundant cell carriers (e.g., Verizon and AT&T in the US) and allows automatic SIM switching if the primary carrier signal fails, ensuring continuous and reliable network connectivity. Additionally, optional accessories are available: Diversity antenna kit, Outdoor Antenna kits with up to 25 or 50 feet of cable length, ideal for buildings with low signal penetration, such as schools and basement installations.

4.3.3.1 Dual SIM 4G LTE Module – Included Parts

Figure 4-9: Dual SIM Cell Module

Figure 4-11: Retention Strap with Screw

Figure 4-13: Quick Start Guide

Figure 4-10: Primary Antenna

Figure 4-12: SMA to MMCX cable

4.3.3.2 CLSS Dual SIM 4G LTE Cellular Module Installation steps

NOTE: Please ensure that the CLSS Gateway firmware version is 4.6.0.80 or higher for the Gateway to detect the new CLSS Dual SIM 4G LTE Cellular Module. If the current CLSS Gateway firmware version is older, please upgrade to version 4.6.0.80 or higher via the local web page or over-the-air (OTA) via the Wi-Fi or Ethernet interface, if available.

Figure 4-14: CLSS Gateway with Dual SIM Cellular Module

01. Switch OFF the gateway.
02. Open the enclosure door.
03. Punch out the appropriate knockouts on the enclosure for the aerials see Figure 4-15: Knouckouts on the Enclosure

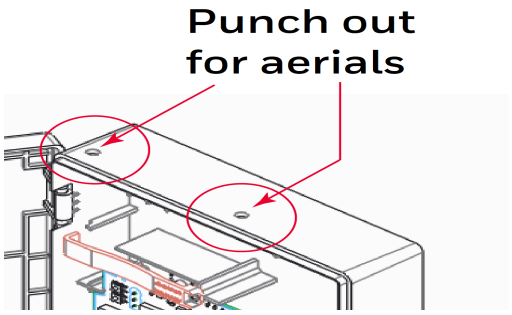


Figure 4-15: Knouckouts on the Enclosure

04. On the top edge of the gateway, plug the new CLSS Dual SIM 4G LTE Cellular Module onto the 40-pin expansion slot.
05. Secure the cellular module with the retention strap and a screw, which come with the module.
06. Use the MMCX to SMA cable and connect the SMA Connector to Gateway enclosure knockouts and tighten the hex nut and washer.
07. Connect MMCX male connector of the cable to Cellular module's primary antenna connector.
08. Install the Primary Antenna with SMA jack as shown in Figure 4-17: Installing Primary Antenna with SMA cable
09. Slowly and gently adjust the primary antenna position vertically from 0 to 90 degrees and rotate it 0 to 180 degrees azimuth to achieve maximum signal strength.
10. Connect the Gateway to the Panel via the respective cable.
11. Connect 24 VDC power supply or the Panel power output to the Gateway to switch ON the CLSS Gateway.

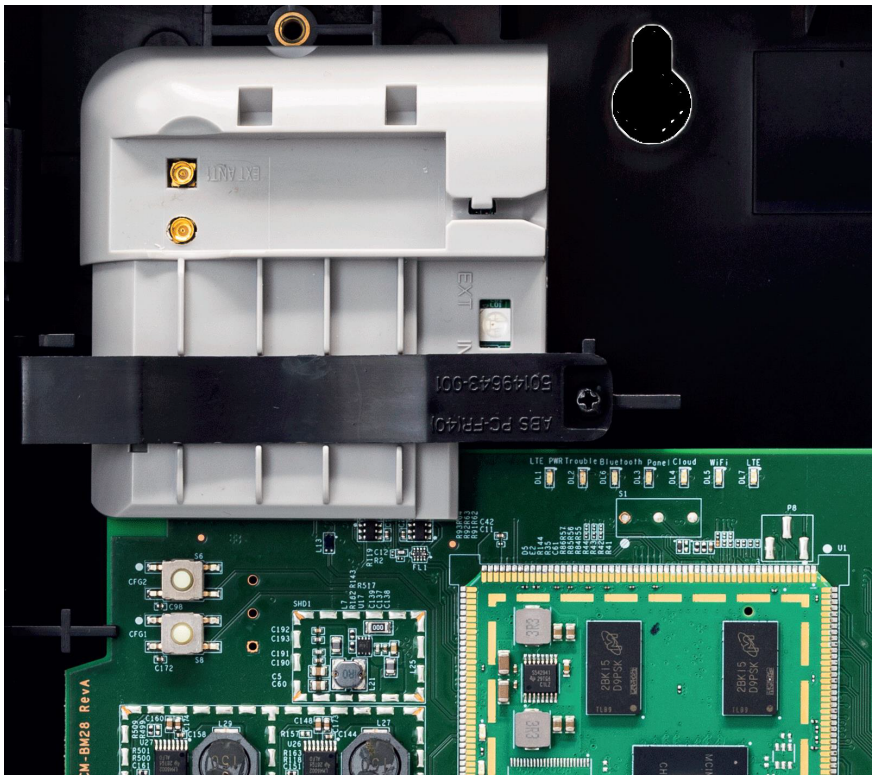


Figure 4-16: Installing the CCM2 cell module

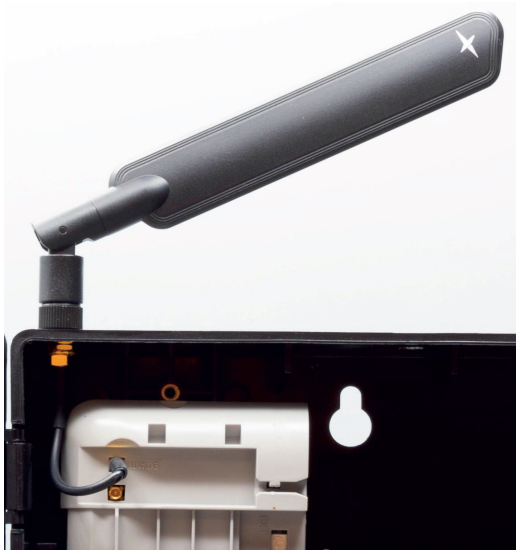


Figure 4-17: Installing Primary Antenna with SMA cable

4.3.3.3 Commissioning the CLSS Gateway with Cellular module

01. Check that the Cellular module LED is solid green. This indicates that the module is connected to the cell tower.
02. Check the status LEDs of the CLSS Gateway.
    i. LTE PWR (DL1) must be ON (solid green).
    ii. LTE (DL7) must be blinking slow.
03. Continue with Commissioning and installation of CLSS Gateway to a specific site/building by following the “fixed gateway installation” using the CLSS mobile app.

4.3.3.4 Troubleshooting

01. Cellular module LED
    a. Solid Green: Cellular module is connected to cell tower.
    b. OFF: CLSS Gateway not powered or cellular module is not connected to the Gateway.
    c. Blinking Red: Cellular module attempting to connect to cell tower.
02. CLSS Gateway LED for Cellular module
    a. DL1 – LTE POWER:
        i. Solid Green: Cellular module is detected and powered.
        ii. OFF: No cellular module detected or powered
    b. DL7 – LTE
        i. Blinking Slow (once every 2 seconds): The cellular module is connected to the Internet with a stable connection.
        ii. Blinking Fast (once every 0.5 seconds): The cellular module is connected to the Internet with an average connection.
        iii. OFF: The cellular module has no network connectivity.

NOTE: For average or weak network connection to cellular module.
1. Slowly and gently adjust the primary antenna position vertically from 0 to 90 degrees and rotate it 0 to 180 degrees azimuth to achieve maximum signal strength.
2. Optional accessories are available: Diversity antenna kit (CCM2-ANTKITEXT2), Outdoor Antenna kits with up to 25 feet (CCM2-ANTKIT-OUT25) or 50 feet (CCM2-ANTKIT-OUT50) of cable length to improve signal strength.

4.3.3.5 DIVERSITY / SECONDARY ANTENNA KIT (CCM2-ANTKITEXT2)

Secondary / Diversity Antenna can be used with cellular modules to improve signal quality and reliability in below scenarios:

01. Poor Signal Conditions: In areas with weak or fluctuating signals, a diversity antenna can help by providing an alternative signal path, reducing the chances of dropped connections.Diversity antennas can help maintain a stable connection by switching between antennas to find the best signal.
02. Multipath Interference: In environments where signals can reflect off buildings and other structures, causing interference, diversity antennas can help by selecting the signal with the least interference.
03. Improved Data Rates: Using multiple antennas can enhance data rates through techniques like MIMO (Multiple Input Multiple Output), which utilizes multiple antennas to transmit and receive more data simultaneously.
04. Enhanced Coverage: In large areas or buildings, diversity antennas can help ensure better coverage by picking up signals from different directions.

NOTE: If still problems persist, it may be necessary to try an outdoor antenna SKU to further improve signal reception.

SKU	Description	Kit Includes
CCM2-ANTKIT-EXT2	Diversity/Secondary Antenna Kit	mmcx to sma cable130mm CCD095174250D000130 SMA Bulkhead Female to SMA PLUG GOLD Male CCD01120T551D002000 cable tag/Nylon Cable Clips Wall Hanging (5 pcs)
		Indoor Antenna TG.55.8113
		L Bracket for Wall mounting Chipboard screw (5x60) - 2 pcs Plastic wall plugs - 2 pcs

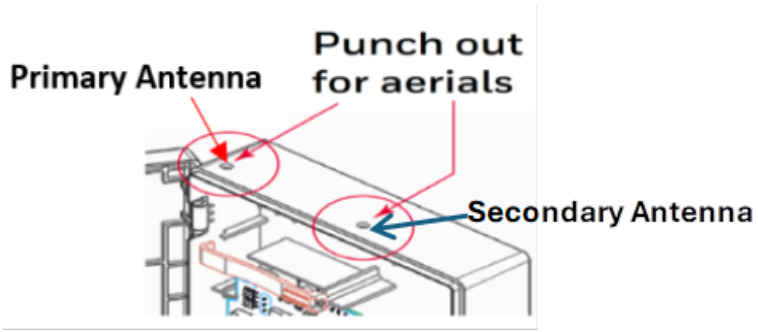


Figure 4-18: Installing Secondary / Diversity Antenna kit

4.3.3.6 OUTDOOR ANTENNA KIT (CCM2-ANTKIT-OUT25, CCM2-ANTKIT-OUT50)

01. Indoor Antenna included default with the unit can be replaced by Outdoor Antenna Kit by connecting to the Cellular Module Primary Antenna connector.
02. The maximum length of cable and antenna placement acceptable should be determined considering the signal strength rating seen in the Gateway Cellular Module after the install.Honeywell recommends that the signal strength rating should be Good or Excellent for a consistent reliable cellular connection. Maximum loss should be 3 dB.

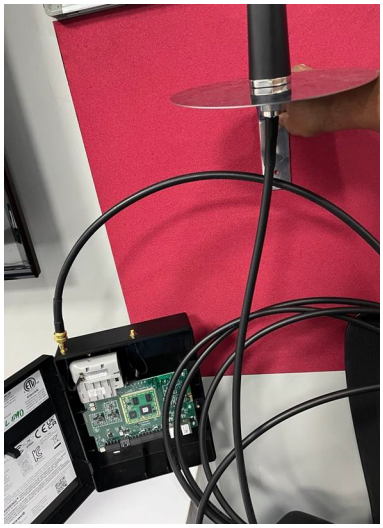


Figure 4-19: Installing Outdoor Antenna kit

NOTE: 1.Once the Gateway Cellular Module is activated, you can check the signal strength shown in the CLSS App or Site Manager.
2.Once the Gateway Cellular Module is activated, you can check the additional cellular details in the Mobile App advanced screen.

SKU	Description	Kit Includes
CCM2-ANTKITOUT25	Optional Outdoor antenna kit with 25' cable	25' RF Cellular Antenna low loss Coax Cable (CFD-400/TGC-400) Coaxial SMA male to N-Male CCD07340T005D007620
		N--Type female-based Antenna TLS.01.1F21
		20cm Ground Plane
		L – Bracket for Wall mounting Chipboard screw(5x60) - 2pcs plastic wall plugs - 2 pcs
		Cable tag/Nylon Cable Clips Wall Hanging (20 pcs)
CCM2-ANTKITOUT50	Optional Outdoor antenna kit with 50' cable	50' RF Cellular Antenna low loss Coax Cable (CFD-400/TGC-400) Coaxial SMA male to N-Male CCD07340T005D015240 N-Type female-based Antenna TLS.01.1F21 20cm Ground Plane
		L – Bracket for Wall mounting
		Chipboard screw(5x60) - 2pcs Plastic wall plugs - 2 pcs
		Cable tag/Nylon Cable Clips Wall Hanging (35 pcs)

SECTION 5: CONFIGURATIONS

The gateway settings control the gateway's communications with the mobile, panel, detectors, and *CLSS Site Manager*.

5.1 COMMISSIONING THE GATEWAY

You can commission the CLSS Gateway for an already added customer or for a new customer.

5.1.1 THE COMMISSIONING STEPS

Step 1: Connect to the IP network through the Ethernet 1 port of the gateway for the *CLSS Site Manager*.

Step 2: Send the panel's topology onto the *CLSS Site Manager*.

Refer to the 5.1.2 Exporting Panel's Topology Data section.

Step 3: Connect the gateway to a panel.

Refer to the Appendix C: Connecting to the Panels section.

Step 3: Configure the gateway to use the connected panel.

Refer to the Section 5: Configurations section. (The current section)

Steps 4: Inspection and maintenance of the gateway.

5.1.2 EXPORTING PANEL'S TOPOLOGY DATA

The first-time commissioning of the gateway includes uploading the panel's topology data to the *CLSS Site Manager*.

NOTE: The topology data is exported using the supported panel manufacturer's programming tool. To know about their recommended tool for exporting and related configurations, refer to the panel's documentation.

5.1.2.1 To Export the Topology Data

01. Using the tool, which the panel manufacturer recommends, export the panel's topology data into your configuration computer.
02. From the configuration computer, log into the *Connected Life Safety Services* application.
03. Ensure that the relevant *customer*, *site*, and *building* details are available in the application.
04. Select the building where the panel is located.
05. Go to the building's inventory page.
06. Click on the **Config File** button, find the exported topology data file, and select that file.
07. Wait for the upload success message.
08. Confirm that the inventory page shows details of the panel's connected devices.

5.1.3 TO CONFIGURE VIA THE WIRELESS CONNECTION

01. In the mobile device, download the *Connected Life Safety Services* App from Play Store or App Store.
02. Install the App.
03. From the Honeywell on-boarding email, note down the login credentials.
04. On the mobile device, log into the *CLSS* App.

05. On the App's dashboard, at the right bottom, tap the **More** icon (see Figure 5-1: CLSS App Dashboard).

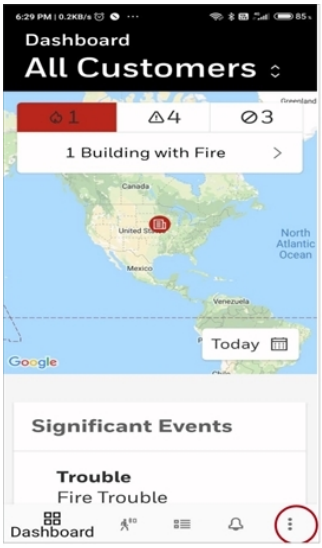


Figure 5-1: CLSS App Dashboard

06. Tap **Gateway Configuration**.
07. Follow the on-screen instructions for mobile connectivity.

> **NOTE:** Based on the gateway you are configuring, select either *Portable Gateway* or *Fixed Gateway*.

08. Wait for the App to connect with the gateway, the fire alarm panel, Internet, and *CLSS Site Manager*. The App notifies you when configuration is completed.
09. On the dashboard, from the **All Customers** option, find the required *customer* > *site*.
10. Tap on the specific building.
11. To commission the gateway, tap on **CONNECT GATEWAY** and follow the on-screen instructions (see Figure 5-2: Building Details Page .)

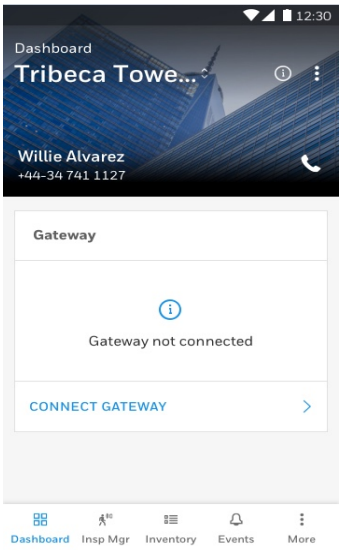


Figure 5-2: Building Details Page

NOTE: In the *Connected Life Safety Services* App, the option to enable the control functionality is available for 60 minutes, which can be extended.

NOTE: At the end of 60 minutes, the user will have the option to extend the session. If not extended, the session will expire after 60 minutes and the user must enable a new session of control functionality within the *Connected Life Safety Services* App.

5.2 VERIFYING THE GATEWAY CONNECTIONS

While configuring the gateway, confirm that the LEDs indicate successful connections as shown in Figure 5-3: Connection Indicators .

If the LED is indicating differently, refer to 2.3.2 LED Indicators section to know the operational status. If necessary, refer to the Section 6: Post-Installation Activities section to fix the problem or contact Honeywell Technical Support.

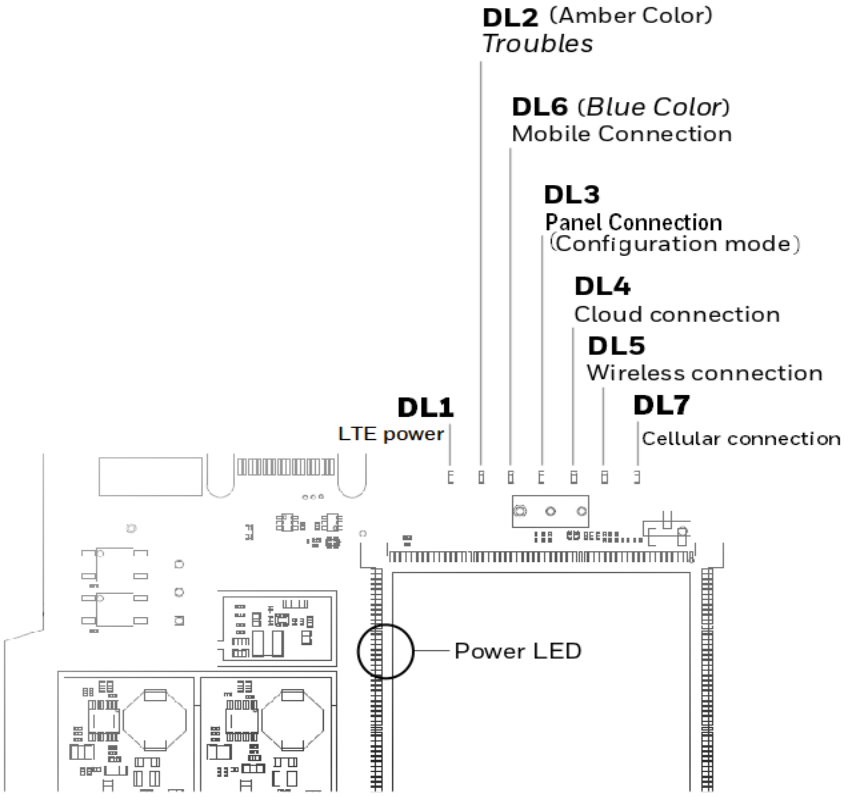


Figure 5-3: Connection Indicators

LED Indicator	State	Meaning
Power-Indicating LED	ON	Successful power connection
DL1	ON OFF	ON - The cellular module is installed and receiving power. OFF - The cellular module is not installed.
DL2	OFF	There are no issues
DL6	Flashing fast[1]	Successful mobile connection
	Flashing slow[2]	Ready for connection
	OFF	Disabled mobile connection

LED Indicator	State	Meaning
DL3	ON	The gateway is in the configuration mode
	Flashing fast	The gateway is getting the inventory data
	Flashing slow	The gateway is communicating with the panel
DL4	Flashing slow	The gateway is communicating with *CLSS Site Manager*
	Flashing fast	The gateway has the Internet connectivity, but not the *CLSS Site Manager* connectivity
DL5	Flashing slow	The gateway has wireless connection with *CLSS Site Manager*
DL7	OFF	There is no cellular connection.
	Flashing slow	The LTE radio is transmitting data for the cellular connection.
	Flashing fast	The LTE radio has connectivity issues.

[1]FLASHING FAST = 0.2 second ON and 0.2 second OFF
[2]FLASHING SLOW = 1 second ON and 1 second OFF

5.3 PANEL BRAND AND CONNECTION SETTINGS

When the mobile App is connected with the *CLSS Site Manager*, you can change the panel brand's communication settings.

NOTE: You can change the connection settings using either the CLSS mobile App or the *Gateway Configuration Tool*.

5.3.1 TO CHANGE THE CONNECTION SETTINGS

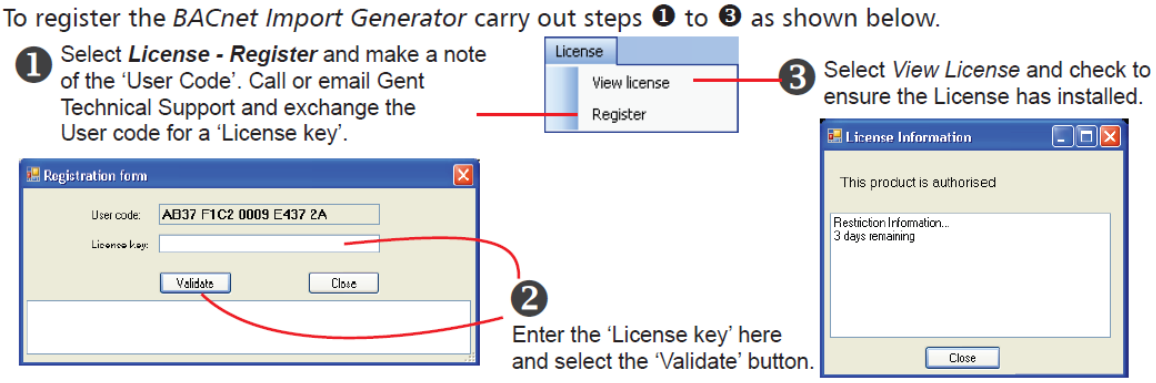
01. To change the newly connected panel's settings:
    a. Select the Customer and the Site.
    b. Tap on your connected gateway from the list of gateways.
    OR
    To change the previously connected panel's settings:
    a. Tap the three dots at the top right on the mobile App.
    b. Tap **Install Fixed Gateway**.
    c. Select the Customer and the Site.
    d. Tap on your connected gateway from the list of gateways.
02. Tap on the **Panel Brand & Connection** option on the **Gateway Summary** screen.
03. Tap on **Panel Brand**.
04. Change the panel brand, if required.
05. Tap **NEXT**.
06. Select the connection type for the panel from the **Connection Type** screen.
07. Tap **APPLY**.
08. Tap **Panel Type** on the **Gateway Summary** screen.
09. Change the values for the panel brand on the **Communication Settings** screen.
10. Tap **SAVE**.
    If an ANN BUS connects the gateway with the panel, the field name is shown as **ANN BUS Address**. For direct panel connections, the field name shown is **Address**.

5.3.2 IMPORTING THE GENT PANEL'S INVENTORY

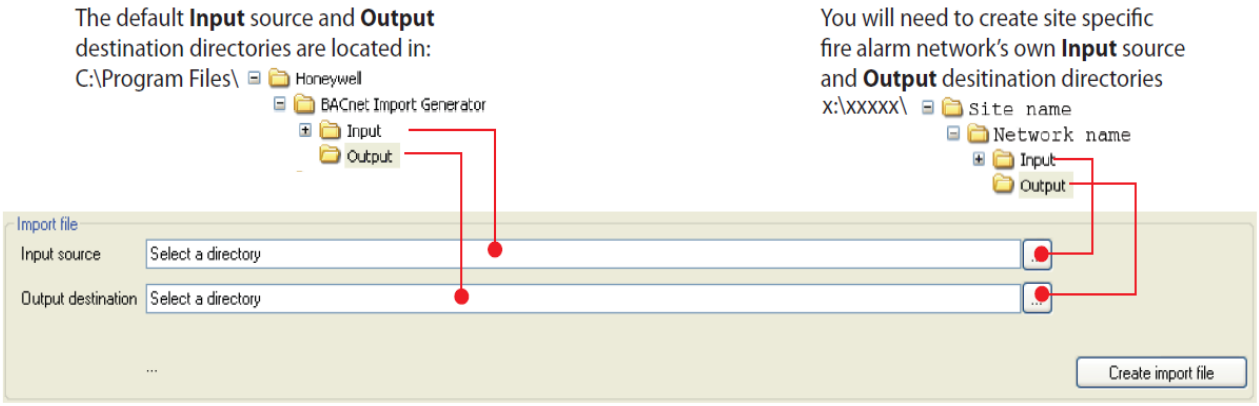
The `.dat` file has configuration details of all the devices and panels in the Gent panel network along with their addresses.

01. Run the *BACnet Import Generator* tool.

02. Follow the below process to register the *BACnet Import Generator*:

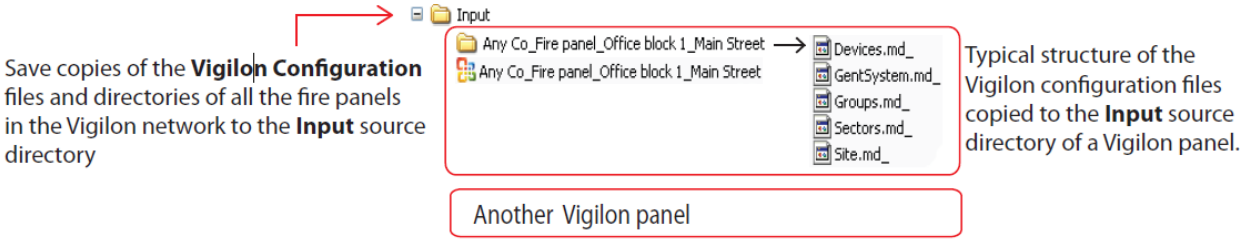


03. Create an *Input* folder and an *Output* folder.



> **NOTE:** The *Input* folder will store Vigilon configuration settings. The *Output* folder will store the `GENTGW.ini`, `GentComm.ini`, and `BacnetImport.dat` files.

04. Copy the panel's configuration files into the *Input* folder.



05. Click **Create Import File**.

06. Check that the `BACnetImport.dat` file appears in the *Output* folder.

5.3.3 TO CONFIGURE THE PANEL'S CONNECTION SETTINGS

CLSS gateway details are provided through the *Gateway Configuration Tool*, a web page-based configuration tool running on the gateway.

01. On the CLSS Gateway board, find the S6 button.
02. Connect the Ethernet cable to Eth0 and the Laptop to enable web configuration.
03. Press the S6 button for a minimum of 6 seconds and then release it. It will switch the gateway to configuration mode.

    The LED indicator DL3 turns ON and SOLID indicating that the configuration is enabled.

NOTE: The web configuration is available only on *Eth0*.

04. Open the Configuration Computer connected to the *Eth0* port of the gateway.

NOTE: The static IP of the *Eth0* port is *192.168.10.190*.

05. In the Chrome browser, enter the following URL: https://192.168.10.190:9443/config/index.html
06. Do the following if any security warning is shown. Otherwise, go to step 7.
    a. Click the *Advanced* link below the error message.
    b. Agree to proceed.
07. In the **Gateway Configuration Tool** page, enter the password.

NOTE: The default password is: Welcome123

08. Click **Gateway Settings** (see Figure 5-4: Gateway Settings Screen).

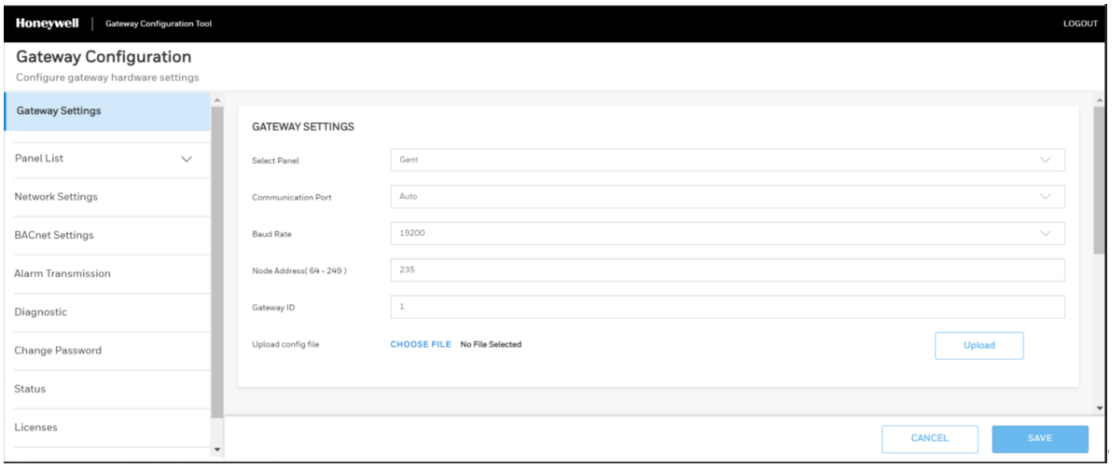


Figure 5-4: Gateway Settings Screen

09. Provide the required gateway settings details:

Table 5.1
Table 5.1 Gateway Settings Details

Field	Description
Select Panel	Select the panel brand to which gateway is connected.
Communication Port	Select the panel port to which the gateway is connected. Options are: Auto, RS-232, or TTL.
Baud Rate	Select the Baud Rate assigned for the panel. It could be 9600, 19200, 38400, 57600, or 115200.
Node Address	Specify the gateway address between 64 to 249. The default node address is 235. **Important**: Each gateway in its network of gateways should have its own node address.
Upload Config File	Click to upload a file for the generation of IFOM inventory. The file format is different for different panel brands. Refer to the 5.3.2 Importing the Gent Panel's Inventory section to generate Gent panel's inventory.

NOTE: Availability of the above fields depends upon the panel brand.

5.4 HONEYWELL CLSS ALARM TRANSMISSION SERVICES

The CLSS Gateway enables the central monitoring service providers, fire department, and its building occupants to have the quickest response possible to an event. The building occupants are given early, personalized guidance to safety.

This service also increases the first-time fix rate for all service providers. Its predictions about certain upcoming needs reduce business disruptions as well.

This special service is available only to select service providers. For more details, contact Honeywell Technical Support.

5.4.1 COMMUNICATION MANAGEMENT

- The communication path between the gateway and the Central Station is supervised. The default supervision timing is 5 minutes.
- In case of an AC failure, the CLSS Gateway communicates to the central station after 120-minutes.

5.4.2 CENTRAL STATION COMMUNICATION

The CLSS Gateway receives events from a listed Fire Alarm Control Unit and transmits events using cellular, wireless, or Ethernet to Honeywell's Network Operations Center (NOC). All signals from the CLSS Gateway are delivered to Honeywell's NOC, which routes the events to the appropriate central monitoring station over an IP network.

5.4.3 ACTIVATING THE CENTRAL STATION COMMUNICATION

In the *CLSS Site Manager*, the service provider administrator should activate the central station communication. It is a one-time activity, which can be done for an operational gateway or for a newly installed gateway.

NOTE: Before activating the central station communication, ensure that the CLSS Gateway has no communication failures. During a connection failure, the CLSS Gateway cannot send event data to the *CLSS Site Manager* or the NOC.
For example, if the gateway's Ethernet cable is disconnected, its fire panel will display *UDACT Trouble*. Only after restoring the connection and clearing the trouble, the *CLSS Site Manager* or the NOC can receive events again.

5.4.3.1 Adding a Central Station to the CLSS Account

Only those central stations added in the external accounts of the CLSS Site Manager can receive alarms the gateway sends. Therefore, a service provider administrator should first perform this one-time activity and add the accounts.

NOTE: Using the credentials given, you can log onto the *CLSS Site Manager* available on https://fire.honeywell.com and enable this feature. Honeywell recommends Chrome browser for using the *CLSS Site Manager*.

01. Log onto the CLSS *Site Manager.*
02. Click on the profile icon at the top right and click **External Accounts**.
03. Click **ADD NEW** under the **Central Stations** section.
04. Follow the on-screen instructions to add the central station account.

5.4.3.2 Install a Fixed Gateway at the Site

To enable central station communications, a CLSS Gateway must be installed.

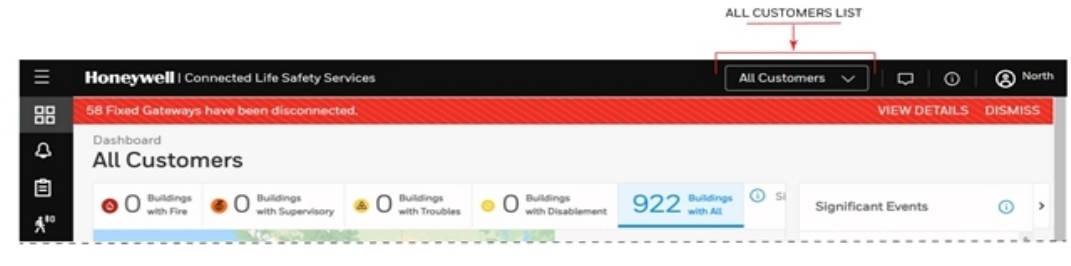
NOTE: You can skip this procedure if you are activating the central station communication for a CLSS Gateway that is already installed.

01. Log into the *Connected Life Safety Services* App in your mobile device.
02. Tap the three horizontal dots icon at the top-right side on the **All Customers** dashboard.
03. Select **Install Fixed Gateway** from the pop-up menu.
04. Follow the on-screen instructions to complete the gateway installation in the App.

5.4.3.3 Configuring the Central Station Communication

A technician or a service provider administrator can configure the central station communication of the CLSS Gateway.

01. Log onto the CLSS Site Manager.
02. Select the customer from the **All Customers** list at the top-right side.



03. Select the customer, select the site, and then select the building requiring alarm transmission.

04. Click the **FEATURE ACTIVATION** icon at the left navigation bar.

05. Select **Installed Gateways** and then go to the **INSTALLED GATEWAYS** section.

> **NOTE:** To view only those gateways not yet activated, select **Show only Gateways without activations** at the right side.

06. Find the CLSS Gateway requiring alarm transmission from the gateway list shown.
07. Click on the specific CLSS Gateway of the building.
08. Click on the **Connected Gateway** activation card inside the selected gateway.
09. Click **Configure Now**.
10. Select the central station to configure from the central stations list.
11. Follow the on-screen instructions to enable the alarm transmissions.
12. Download the central station report.

> **NOTE:** A central station report provides inventory and contact ID of a building. The report gives details, which the central station requires.

5.4.3.4 Verifying the Central Station Communication Configurations

After configuring for the central station communication, call the central station to confirm that the alarm transmission for the building is activated.

5.4.4 DUAL PATH COMMUNICATION FOR ALARM TRANSMISSION

While configuring the central station communication, you can choose a single path or two paths for alarm transmissions. Reporting options are: LTE cellular only, IP only, IP Primary with LTE cellular backup, or LTE Cellular Primary with IP backup.

NOTE: Alarms will be sent through two among the following ports: Ethernet, Wireless, or Cellular.

5.4.4.1 Supervision Period

Dual paths are monitored for integrity at an interval period as per NFPA 72 requirements. In case of a failure, both the local premises and the central station receive a failure report with a unique code as in the central station report.

5.4.4.2 Transmission Options

Path Options	Supervision Interval
Single Path	
Cellular	5 Minutes
	60 Minutes
IP [1]	5 Minutes
	60 Minutes
Dual Path	
IP [1] and Cellular	5 Minutes
	60 Minutes
[1]IP can be an Ethernet or a wireless connection	

5.4.4.3 Test Time Interval

The test time interval specifies the frequency when the *CLSS Gateway* should send a test event to its Central Station to confirm that the gateway is active. By default this is set to 24 hrs test, but you canchange it and specify the testing interval.

A supervisory device performs the additional-level supervising of the paths and performs this test. It can send only supervisory events and not the status events.

Examples:

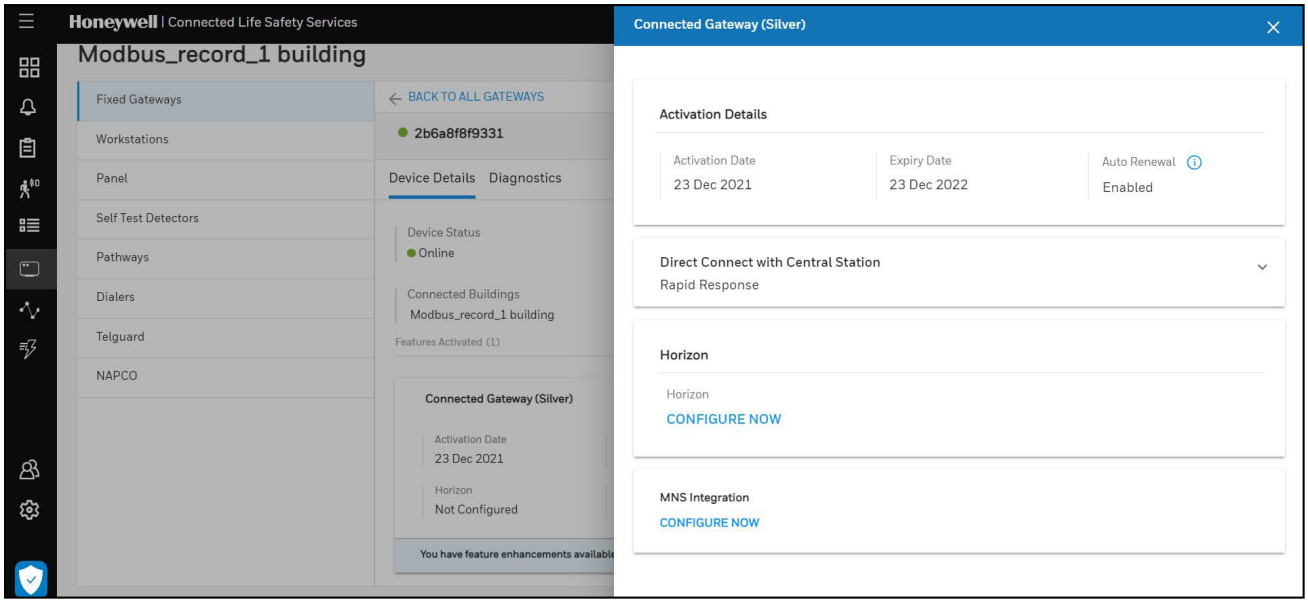
Event Code	Description
602	Periodic Test Event With No Trouble

5.4.4.4 Test Interval Options

Path Options	Interval Period
Single Path	
Cellular	1 Hour
	6 Hours
	24 Hours[1]
IP[2]	1 Hour
	6 Hours
	24 Hours[1]
Dual Path	
IP[2] and Cellular	1 Hour
	6 Hours
	24 Hours[1]
[1]24 hours is the default interval. [2]IP can be an Ethernet or a Wireless connection	

5.4.4.5 To Specify the Test Time Interval

01. Go to your **Customer** > **Site** > **Building** in *CLSS Site Manager*.
02. Click  at the left side for feature activation.
03. Find and click the required gateway from the **FIXED GATEWAYS** page.
04. Click **CONFIGURE NOW** at the bottom right.
05. Click and expand the **Direct Connect with Central Station** section.



06. Click  to edit the settings.
07. Select the test event frequency from the **Test Time Interval** field.
08. Click **APPLY**.

SECTION 6: POST-INSTALLATION ACTIVITIES

The system maintenance provider is responsible for the maintenance and upkeep of the CLSS Gateway. The maintenance involves avoiding potential issues, making regular backups, restoring data when required, collecting data for troubleshooting, and other activities.

6.1 UPGRADING THE GATEWAY FIRMWARE

CLSS Service Manager notifies the gateway administrators when a new firmware is launched. The administrators can perform the upgrade at a planned time.

CAUTION: Before upgrading ensure to get permission from the site. The reboot after the upgrade should be at a mutually planned time without affecting the operation.

The upgrade happens in the background while the system is running. After the upgrade the gateway will reboot.

CAUTION: prevent any disturbance to the power cable of the gateway during the upgrade

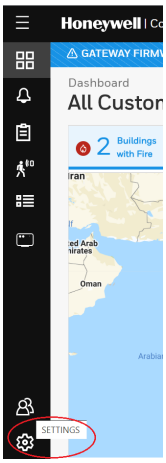
6.1.1 TO UPGRADE BEFORE COMMISSIONING THE GATEWAY

01. Connect the gateway to Internet.

    NOTE:
    The Internet connection can be either wireless or LAN.
    The LED indicator DL4 on the gateway flashing Green confirms Internet connection.

02. Log onto the *CLSS Site Manager*.
03. Click **VIEW** on the notification at the top.

    Or
    Click the **SETTINGS** icon at the bottom left.



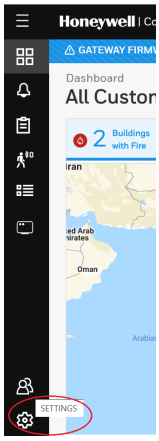
04. Click **Gateway Management** in the **Settings** page.
05. Click **Add Gateway** on top.
06. Enter the OC of the gateway in the **Add Gateway** dialog and click **ADD**.
07. Wait for the registration to complete.

08. Enter the OC of the gateway in the **Search OC** field to find the gateway to update.
    Or
    Scroll across to find the gateways to update.
09. Click **Update**.

6.1.2 TO UPGRADE AFTER COMMISSIONING THE GATEWAY

01. Log onto the *CLSS Site Manager*.
02. Click **VIEW** on the notification at the top.

    Or
    Click the **SETTINGS** icon at the bottom left.



03. Click **Gateway Management** in the **Settings** page.
04. Enter the OC of the gateway in the **Search OC** field to find the gateway to update.
    Or
    Scroll across to find the gateways to update.
05. Click **Update**.

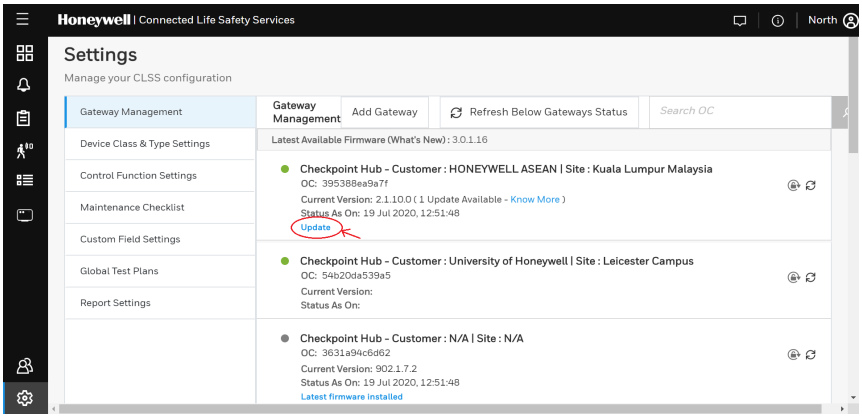


Figure 6-1: Firmware Upgrade

6.1.3 TO LOCALLY UPGRADE WITH A PC

01. On the gateway side, connect an Ethernet cable to the Ethernet port (J3). The port is labeled as 2 in Figure 4-4: Gateway Connection Options - Bottom Side .
02. On the configuration computer side, connect the Ethernet cable to the configuration computer's Ethernet port. Configuration computer/ laptop needs to be configured for static IP in the same subnet of the configuration page IP. As the configuration page IP is 192.168.10.190, a sample laptop side IP configuration can be: IP: 192.168.10.100; Subnet mask: 255.255.255.0;
03. On the gateway board, find the S6 button.
04. To switch to the configuration mode, press and hold the S6 button for a minimum of 6 seconds, and then release it. The LED indicator DL3 turns ON and SOLID, indicating that the configuration is enabled.
05. Open the Chrome browser and enter the following IP address for the configuration tool: **https://192.168.10.190:9443/config/index.html**
06. In the **Sign In** page, enter the password. The default password is: Welcome123
07. In the list of settings options, click **Diagnostic**.
08. In the **GATEWAY FIRMWARE UPGRADE** section, click **Choose File**.
09. Select the firmware image file and click **Choose**.
10. Once the chosen file is uploaded, click **Upgrade**.

6.1.4 TO VERIFY THE UPGRADE

01. After the restart, log into the configuration tool.
02. Click **Diagnostic**.
03. Click **About** and verify that the new version of the gateway firmware is shown.

6.1.5 LED INDICATIONS DURING THE UPGRADE

While the gateway is downloading the firmware, the Green-color LED indicator DL4 will be ON.

If an LED is indicating differently, refer 2.3.2 LED Indicators to determine the operational status. If necessary, refer to the 6.2 Troubleshooting section to fix the problem or contact Honeywell Technical Support.

6.2 TROUBLESHOOTING

Issues that may occur during the gateway's operation can be resolved on your own using the tables below or by contacting Honeywell Technical Support. The issues can be either LED-indicated issues or other issues.

6.2.1 TO TROUBLESHOOT LED-INDICATED ISSUES

When an LED status indicates issues, refer to the below table to determine their possible fixes.

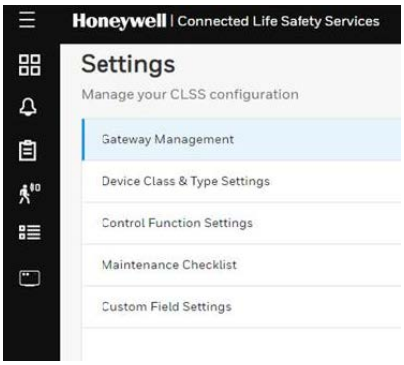
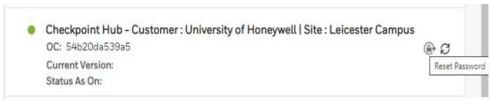
Table 6.1
LED-Indicated Issues and Possible Fixes

Power LED Status	Other LEDs' Status	Possible Fixes
SOM: Power LED-Indicated Issues		
OFF	All other LEDs are OFF	Ensure that the gateway board's power source is supplying the required 24V DC power.
ON	All other LEDs are OFF	Do the following: 01. Remove all the connected cables. 02. Wait for one minute. 03. Reconnect all the cables. 04. Ensure that the gateway board is getting its 24V DC power. If the above steps do not fix the issue, contact Honeywell Technical Support.
DL2: Trouble LED-Indicated Issues		
ON and SOLID Amber	Any	It is a critical issue. Contact Honeywell Technical Support.
Flashing Amber once per second	• **DL3** The panel LED is OFF • **DL4** The *CLSS Site Manager* LED is flashing once per second	Check the following and correct if necessary: • The cable connections at the gateway's port and at the panel's port • The cable connecting the gateway board and the panel
Flashing Amber once per second	• **DL3** The panel LED is flashing once per second • **DL4** The *CLSS Site Manager* LED is OFF	Check the following and correct if necessary: • Internet connectivity • Eth1 cable connections at the gateway board side and at the panel side • The Eth1 cable
DL3: Panel LED-Indicated Issues		
OFF	**DL2** The Trouble LED is OFF	Check the following and correct if necessary: • The cable connections at the gateway board side and at the panel side • The Eth2 cable connecting the gateway board and the panel
DL4: *CLSS Site Manager* LED-Indicated Issues		
Flashing Green every 0.25 second	• **DL3** The panel LED is flashing once per second • **DL2** The Trouble LED is OFF	• Associate the gateway board with the user account. • Ensure that the user account is active. • Ensure that the panel's date and time are correct.
DL5: Wireless LED-Indicated Issues		
OFF	• **DL3** The panel LED is flashing once per second • **DL4** The *CLSS Site Manager* LED is OFF	• Ensure that the WLAN settings in the gateway configuration tool are correct. • Ensure that the building's IP network has Internet and *CLSS Site Manager* connectivity.
DL6: Mobile LED-Indicated Issues		
OFF	• **DL3** The panel LED is flashing once per second • **DL4** The *CLSS Site Manager* LED is OFF	01. On the gateway board, find the S8 button. To find the S8 button, refer to Figure 2-1: Printed Circuit Board: Layout . 02. Press the S8 button until the LED indicator DL6 flashes fast, indicating enabled mobile connectivity.

6.2.2 TO TROUBLESHOOT OTHER ISSUES

If there are issues, which are not shown by the LEDs, refer to the below table to determine their possible fixes.

Table 6.2
Events-Related Issues

Issue Description	Possible Causes	Possible Fixes
Panel events are not displayed on the *Connected Life Safety Services* App	The gateway is dissociated.	Associate the gateway board with the user account.
	The user account is not associated with the gateway.	Ensure that the user account is active.
	The panel's date and time are incorrect.	Ensure that the panel's date and time are correct.
Active event sync failed	Attempting to get *Active Events* from an ESSER panel using a *Remote Access* connection would fail. The *Remote Access* connection on RS232 does not get *Active Events*.	To get *Active Events*, make a WINMAG connection on RS232 or RS485 in the ESSER panel. Refer to the C.3 ESSER Panels section to make a WINMAG connection.
There is a need to reset the default password of the *Gateway Configuration Tool*	Forgot the *Gateway Configuration Tool*'s password	To reset to the default password: 01. Log into the *CLSS Site Manager*: https://www.fire.honeywell.com 02. Click on the settings icon at the bottom-left section. 03. Click **Gateway Management** in the **Settings** section.  04. Find the gateway whose configuration tool password needs to be reset. 05. To ensure that the gateway is online, check that there is a green icon before the gateway name. 06. Click on the reset password icon at the right-side of the gateway name.  07. To confirm the reset, click **CONTINUE** on the message displayed. 08. Wait for the confirmation message. 09. Log in using the default password: Welcome123

Issue Description	Possible Causes	Possible Fixes
There is a need to reset the gateway board to its factory default settings	An unusual situation requires reverting to factory default settings.	Contact the Honeywell Tech Support for a guided procedure.
The CLSS App could not pair with the gateway.	The gateway firmware is not updated to 2.1.11.16 or above.	Upgrade the firmware to 2.1.11.16 or above.
Trouble IN SYSTEM ANN-PRI COMM FAULT DDEV #: ALL DEVICES	The ANN-PRI communication cable is not connected to the panel.	Connect the ANN-PRI communication cable with the panel.
Fuse of the Gent Compact panel is tripping frequently	The panel is facing power overload	Replace the panel's fuse with a fuse for 1A power. To know the fuse upgrade steps, refer C.8.6 Vigilon Series Panels .
Fuse of the Gent Compact panel is tripping frequently	The panel is facing power overload	Replace the panel's fuse with a fuse for 1A power. To know the fuse upgrade steps, refer C.8.6 Vigilon Series Panels .

SECTION 7: MODBUS COMMUNICATIONS

The CLSS Gateway can use a third-party client to monitor the nodes inside a Modbus LAN network, and send alarm and event data of these nodes for the CLSS users.

NOTE: The Modbus interface provides supplementary data to the third party client.
The Modbus details in this section are related to the NOTIFIER-UL panel.

7.1 OPERATION

The CLSS Gateway acts as a slave device to a Modbus master application and offer the Modbus monitoring functionalities to the CLSS Gateway users.

NOTE: The Modbus master application communicates with one or more panels over an NFN or a high-speed NFN network.

7.2 FUNCTIONALITY

With Modbus configurations the CLSS Gateway can:

- Support Modbus Application Protocol Specification V1.1b.
- Monitor up to 10 FACPs.

NOTE: Additional FACPs require additional CLSS Gateways to the network.

- Support a maximum of 2 Modbus clients or masters.

7.3 RECOMMENDED CYBERSECURITY PRACTICES

- Follow the highly-recommended cybersecurity practices specified in the *Cybersecurity Manual* (LS10217-000NF-E).

CAUTION: FAILURE TO COMPLY WITH THE RECOMMENDED SECURITY PRACTICES is a CYBERSECURITY RISK to YOUR SYSTEM.

- Ensure that all the network security best practices discussed in 3.2.6.1 Best Practices are followed.

7.4 REQUIRED SOFTWARE

- Chrome™
- Java™ version 6 or above

7.5 IP REQUIREMENT

7.5.1 IP PORT SETTINGS

The following IP ports must be available for the CLSS Gateway:

Table 7.1 Required IP Ports

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

7.5.2 IP RESTRICTIONS FOR THE GATEWAY

• Assign a static IP address.

NOTE: Dynamic Host Configuration Protocol (DHCP) is supported, but not recommended.
Before using DHCP with LAN for Intranet connection, consult the network administrator of the Site.

• Following are not supported:
  • Web access through an HTTP proxy server
  • Use of a NAT (Network Address Translation)

7.6 BANDWIDTH CALCULATION

Use the following information to calculate the network bandwidth CLSS Gateway usage requires and how it will impact the network.

Table 7.2 Total Required Bandwidth for 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 7.3 Total Required Bandwith for 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

7.6.1 REQUIREMENTS FOR THE CALCULATION

• 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 CLSS Gateway network bandwidth requirement based on polling rate:

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

7.7 SYSTEM ARCHITECTURE

An Internet or Intranet IP network connection is needed for the architectures described here.

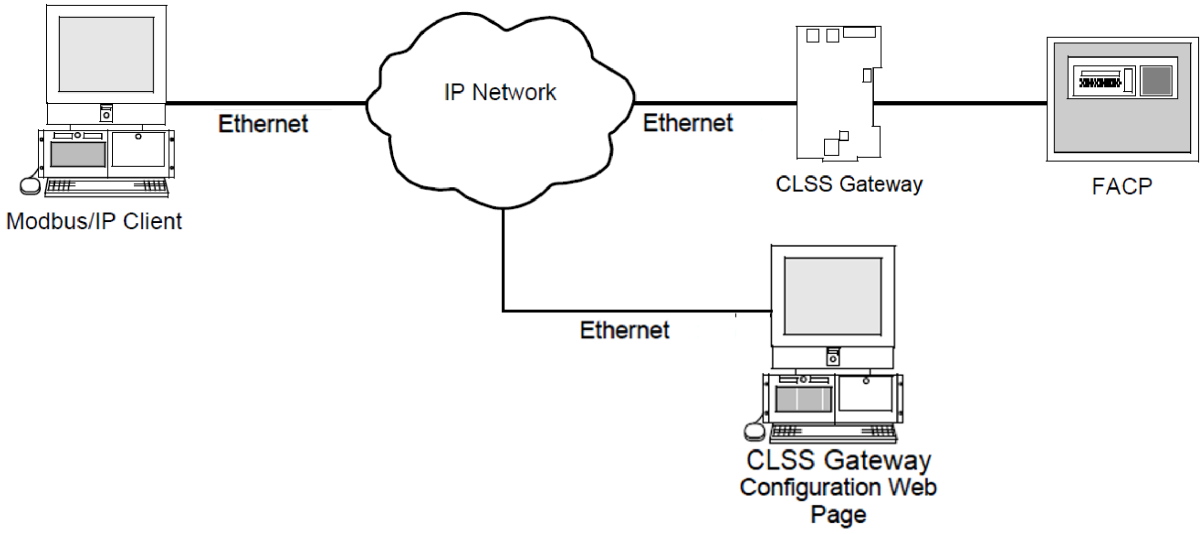


Figure 7-1: Single Panel Architecture

7.7.1 NETWORK OF PANELS

Below illustration shows a sample topology. Refer to the Appendix C: Connecting to the Panels section for panel-specific connection details.

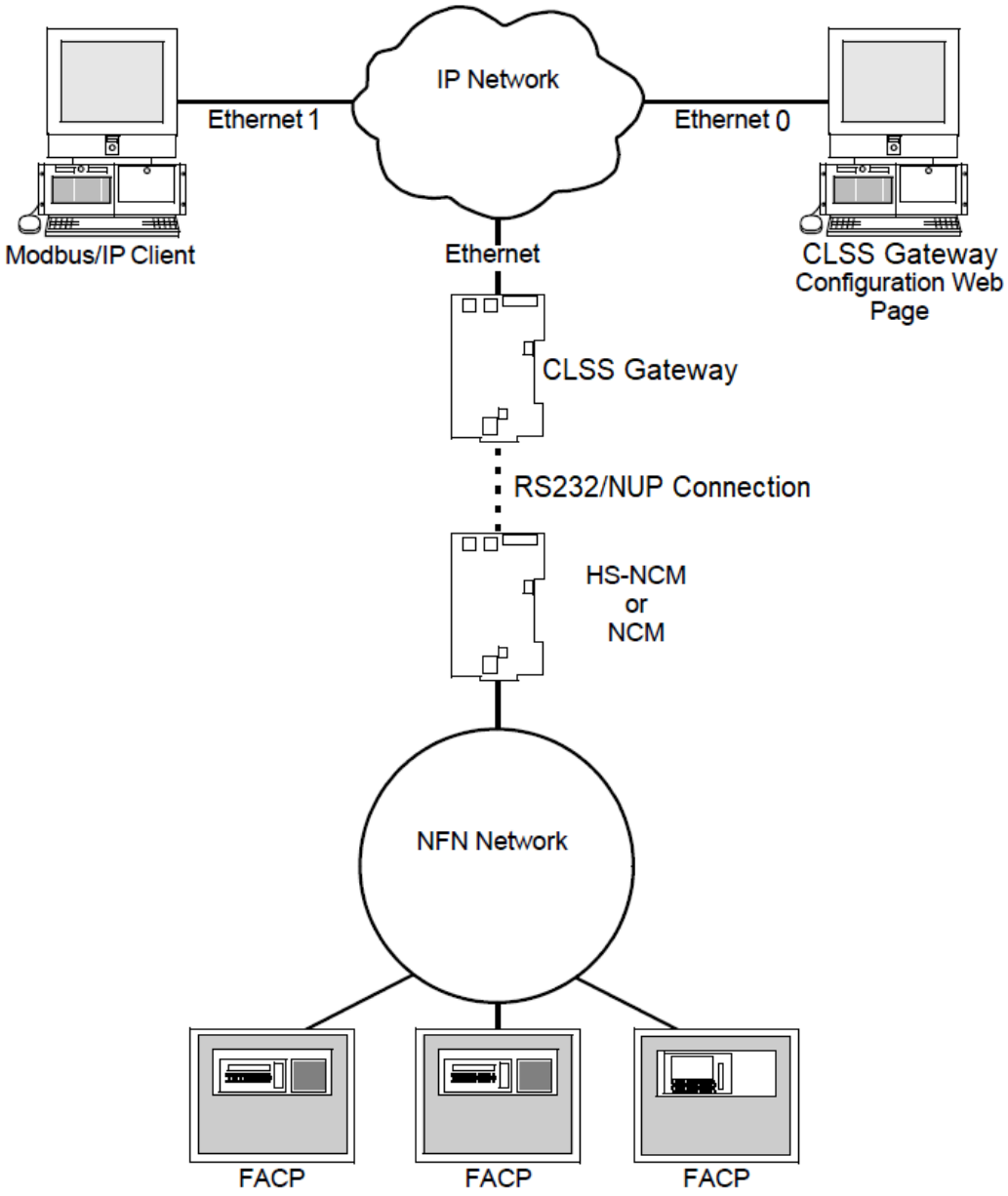


Figure 7-2: NFN Network Architecture

7.7.2 REDUNDANCY

A redundant gateway is a second gateway, which communicates with a Modbus client.

CAUTION: The First and Second gateways must have different node numbers and different ip addresses.

An Example

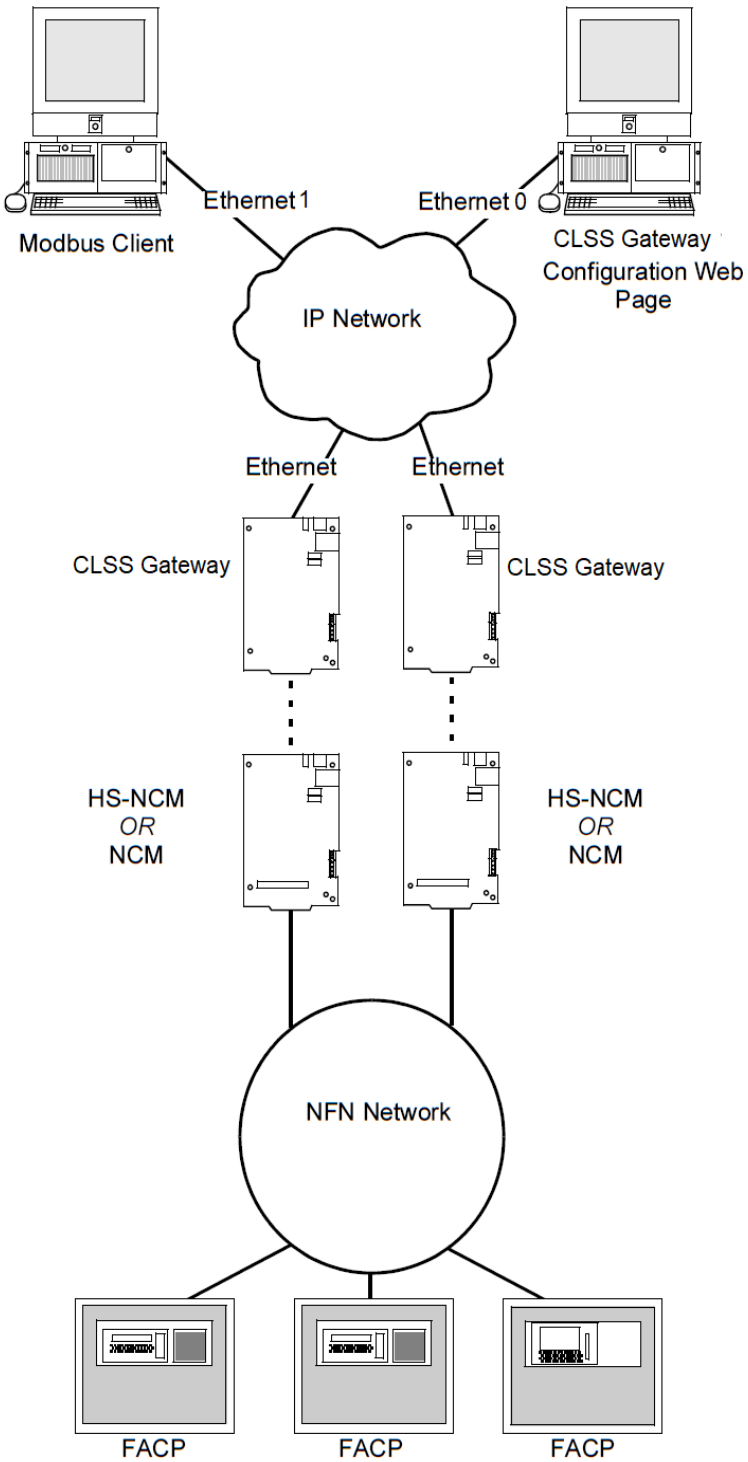


Figure 7-3: Redundant CLSS Gateways

7.8 NFN LEGACY MODBUS GATEWAY

A panel's network might already be using a Modbus gateway in its network. You can add the CLSS Gateway to the network or replace the legacy Modbus gateway with the CLSS Gateway.

7.8.1 REPLACING THE MODBUS GATEWAY (MODBUS-GW)

Following changes occur when the CLSS Gateway replaces the Modbus Gateway in the network.

NOTE: To know the Modbus Gateway values of the following, refer to the document: *LS10015-000NF-E Rev. C2*.

7.8.1.1 The Mapping of Registers

The CLSS Gateway and the Modbus Gateway have different mapping of registers.

Example:

The register range for loop-1 detectors:

- In the Modbus Gateway: 40001 to 40200
- In the CLSS Gateway: 40001 to 40300

Change the client-side scripting as required to change to the registry mapping of the CLSS Gateway.

For register mapping details for the CLSS Gateway, refer to the 7.21 Register Mapping section.

7.8.1.2 Device Types

The device types are different for these two gateways.

Example:

Device Type value of Heat detector:

- In the Modbus Gateway: 1
- In the CLSS Gateway: 0100H

For device type details for the CLSS Gateway, refer to the 7.29 Device Types section.

7.8.1.3 System Troubles

There are new troubles in the CLSS Gateway, and some of the system trouble names are different.

Example 1: New Troubles

- In the CLSS Gateway: 460016-12th bit is *Workstation Failure*.

Example 2: Different trouble name

- In the Modbus Gateway: The *General PS Fault* and the *Power Supply Trouble* are two different events.
- In the CLSS Gateway: The 460015 - 8th bit is one single event for these two.

For system trouble details for the CLSS Gateway, refer to the 7.30 System Troubles Register Map section.

7.8.1.4 Using Both the CLSS Gateway and the Modbus Gateway

Ensure the following:

- The *Node Number* of the CLSS Gateway should be different from other gateways in the network.
- The *IP address* of the CLSS Gateway should be different from other gateways and devices in the network.

NOTE: The changes described in the 7.8.1 Replacing the Modbus Gateway (Modbus-GW) section are applicable for this setup also.

7.9 AGENCY LISTINGS AND APPROVALS

- UL/ULC Listed: S35608
- CSFM: 7300-1637:0504
- FDNY: COA#000121, COA#000122

7.9.1 AGENCY RESTRICTIONS AND LIMITATIONS

CLSS Gateway is UL 864 and ULC-S527 listed for supplementary use only.

7.10 STANDARDS

7.10.1 COMPLIANCE

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

Underwriters Laboratories
- UL 864 - Control Units for Fire Alarm Systems, Tenth Edition

Underwriters Laboratories Canada
- CAN/ULC S527-19 - Standard for Control Units for Fire Alarm Systems, Fourth Edition

7.10.2 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

Underwriters Laboratories Canada
- CAN/ULC S527 - 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

7.11 COMPATIBLE EQUIPMENT

The CLSS Gateway is compatible with the following equipment:

Table 7.4 Compatible Equipment List

Type	Equipment
Fire Panels	• AFP 3030 • AFP2800 • AM-MA Series • GW-FCI S3 • GW-FCI E3 • N16 (INSPIRE) • NFS-3030 • NFS-320 • NFS-640 • NFS2-3030 • NFS2-640 • NOTIFIER-EN ID3000 • NOTIFIER-EN Pearl • XLS 120 • XLS 140-2 • XLS 2000 • XLS 3000
Network Cards	• NCM-F, NCM-W • HS-NCM-MF, HS-NCM-MFSF, HS-NCM-SF, HS-NCM-W, HS-NCM-WMF, HS-NCM-WSF • HS-NCM-W-2, HS-NCM-WMF-2, HS-NCM-WSF-2, NFN-GW-PC-NHW-2

Type	Equipment

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	Unmonitored but network compatible. • Legacy Gateway • DVC • NCA-2 • NCD • NFN-GW-EM-3 • NFN-GW-PC-F • NFN-GW-PC-HNMF • NFN-GW-PC-HNSF • NFN-GW-PC-HNW • NFN-GW-PC-HNW-2 • NFN-GW-PC-W • NWS-3 • PC NFN Gateways • VESDA-HLI-GW

7.12 MODBUS FEATURE ACTIVATION

Purchase the required number of Modbus support on *CLSS Site Manager* and then activate that feature in CLSS App.

NOTE: Purchase should be within the number of tokens available.

7.12.1 TO PURCHASE THE MODBUS SUPPORT

01. Log onto *CLSS Site Manager*.
02. Click on your account name and select **Manage Access**.

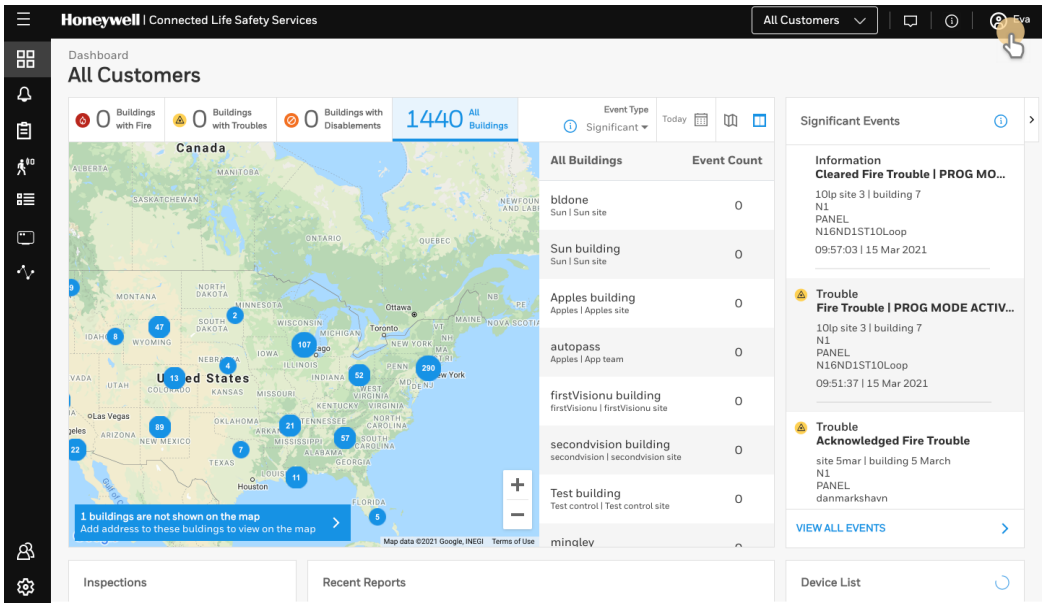


Figure 7-4: Selecting Manage Access

03. Click **Features** on the **Manage Access** page.
04. Click **Gateway** under the **Features** section.
05. Note down the purchased number under **Available Features**.

06. Click **PURCHASE** at the top right side.

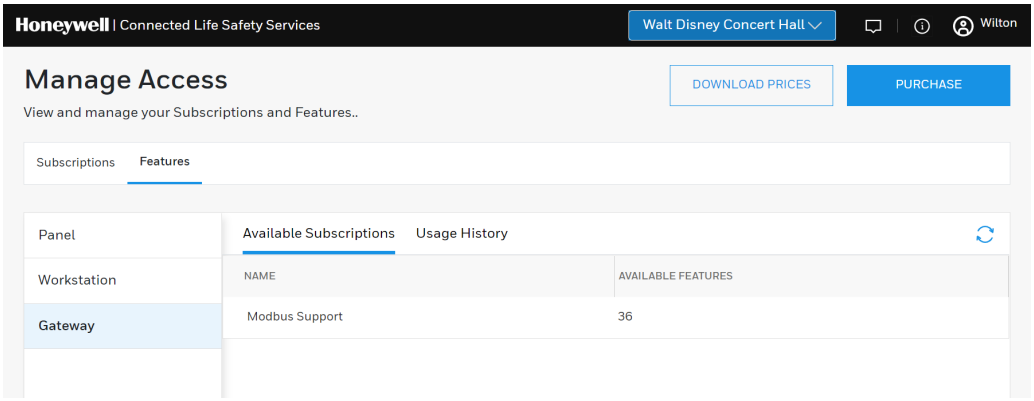


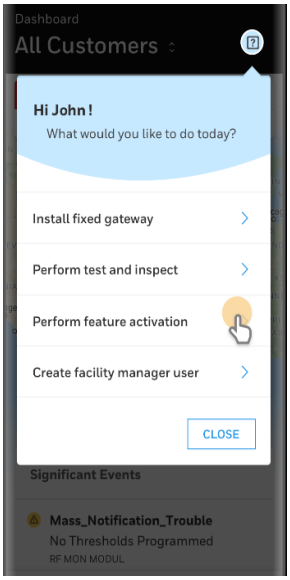
Figure 7-5: Purchasing the Modbus Support

07. Scroll down to find **Modbus Support** in the **Features** tab.
08. Enter the number of support required in the **Modbus Support** field.
09. Click **PURCHASE**.
10. Read the **Confirmation** message and if acceptable, click **CONFIRM**.
    Or
    Click **CANCEL** and repeat the steps from 8 to 10.
11. Wait for the purchase to complete and refresh the page, if required.
12. Verify that the purchased number under **Available Features** is correct.

7.12.2 TO ACTIVATE THE MODBUS SUPPORT

NOTE:
- The gateway must be already installed. If not, install the fixed gateway.
- All the network settings should be configured while installing.

01. Tap **Perform Feature Activation** on the CLSS App's welcome message.



02. Feature Activation: The First Step

03. Tap **Fixed Gateways**.
04. Select the site of the gateway.
05. Find and tap the OC of the gateway.
06. Tap **ADD ACTIVATION**.
07. Tap **Modbus Support** under the **One Time Activations**.
08. Tap **ACTIVATE**.
09. Wait for the activation successful message.

7.13 INSTALLATION AND CONFIGURATIONS

The CLSS Gateway can communicate with the Modbus client in an Ethernet LAN.

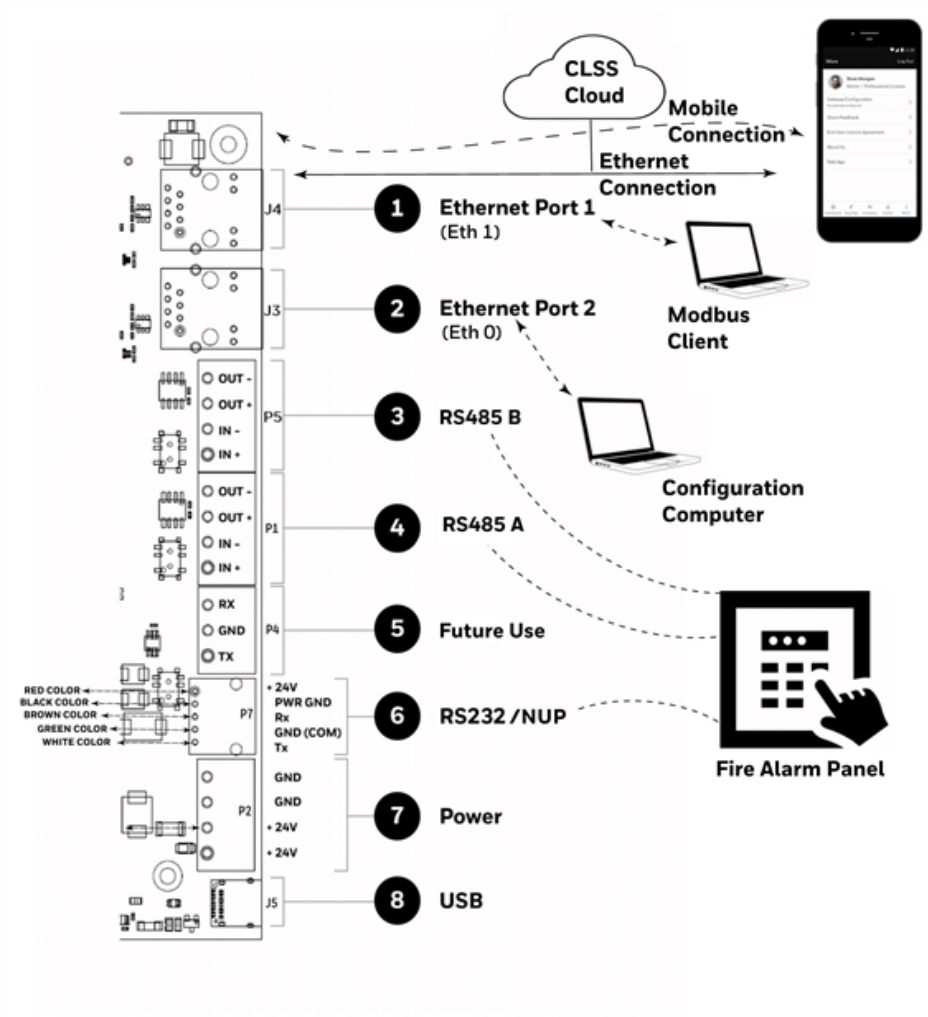
7.14 THE IP SETTINGS

The following information applies to IP settings:

- You can use only the *eth1* port for connections to Modbus clients. For more details, refer to 7.16 To Configure the Modbus Settings .
- Each CLSS Gateway is shipped with a default node number of 235.
- The computer used to configure the CLSS Gateway must establish an IP connection to the gateway. Consult with a network administrator if unsure how to make this connection.
- Connecting more than one CLSS Gateway prior to reconfiguring the IP address will result in an IP address conflict.

7.15 TO CONNECT WITH THE MODBUS CLIENT

01. At the CLSS Gateway side, connect an Ethernet cable to the Ethernet Port 1.



02. At the Modbus client side, connect the other end of the Ethernet cable to the system running the Modbus client.

7.16 TO CONFIGURE THE MODBUS SETTINGS

01. On the CLSS Gateway board, find the S6 button.
02. Press the S6 button for a minimum of 6 seconds and then release it. It will switch the gateway to configuration mode. The LED indicator DL3 turns ON and SOLID indicating that the configuration is enabled.
03. Connect the Ethernet cable to *Eth0* for enabling web configuration.

NOTE: The web configuration is available only on *Eth0*.

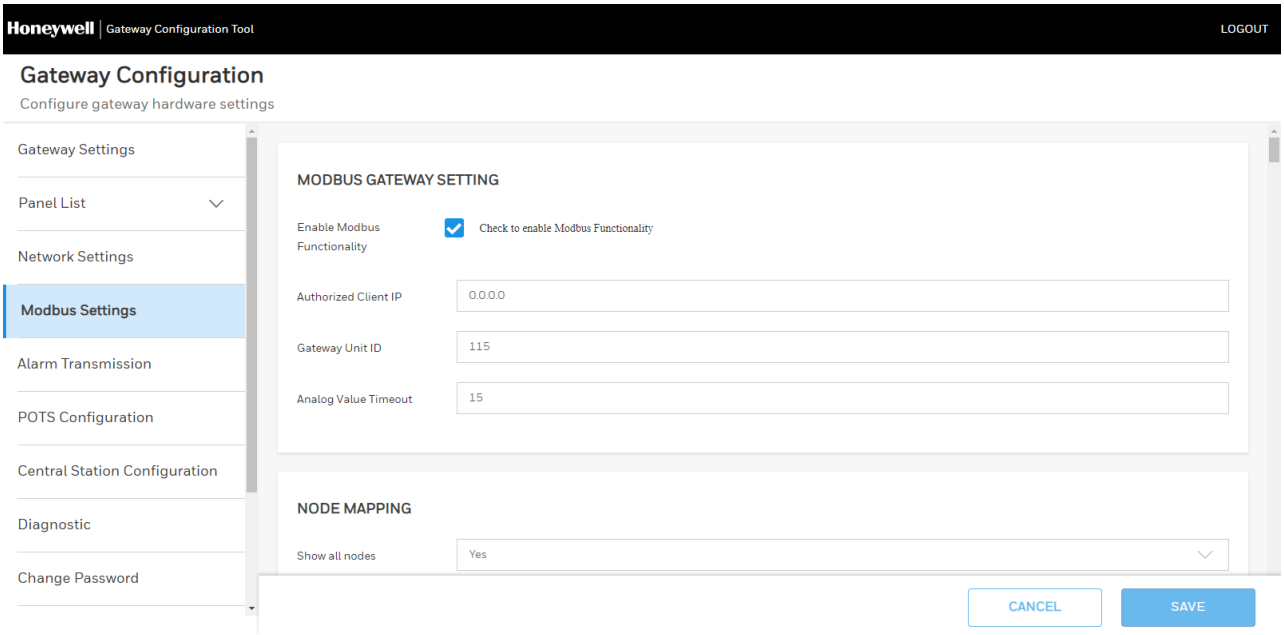
04. Open the Configuration Computer connected to the *Eth0* port of the gateway.

NOTE: The static IP of the *Eth0* port is *192.168.10.190*.

05. In the Chrome browser, enter the following URL: https://192.168.10.190:9443/config/index.html
06. Do the following if any security warning is shown. Otherwise, go to step 7.
    a. Click the *Advanced* link below the error message.
    b. Agree to proceed.
07. In the **Gateway Configuration Tool** page, enter the password.

> **NOTE:** The default password is: Welcome123

08. Go to the **Network Settings** in the **Gateway Settings** section.
09. Assign the *Eth1* port with a static IP address for the Modbus connection.
10. Connect the Ethernet cable between the *Eth1* port of CLSS gateway and its LAN device.
11. Find and click **Modbus Settings** in the **Gateway Settings** section.



12. In the **MODBUS GATEWAY SETTING** page, provide the required details for the Modbus client.

Table 7.5 Settings for Modbus Client Communications

Field	Description
Authorized Client IP	This is an optional security feature. • 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 CLSS Gateway configuration web page as normal. Or • Enter 0.0.0.0 to allow up to 2 clients to connect at a given time.

Field	Description
Gateway Unit ID	Displays the unit ID that the CLSS Gateway 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 CLSS Gateway 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* *Only for Notifier UL NFS 3030-2 panel.	Enter the minimum frequency (in seconds) at which the CLSS Gateway 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 CLSS Gateway stops polling the points in question. Once the time out period expires without the CLSS Gateway 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. Default value is 15 seconds.
NODE MAPPING	
Show All Nodes	• Select **Yes** to display all the nodes in the network. • Select **No** to display only the nodes that the panel monitors in the network.
Node Status	Shows the operational status of each nodes displayed. It would be *Online* or *Offline*. **Note**: The Gamewell-FCI, AM-MA Series, and NOTIFIER EN panels do not yet support this feature.
Node ID	Displays the number of each node in the network.
Node Type	Shows the brand name of the node. For example, NFS2-3030.
Node Unit ID	Displays the unit ID that each 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 (1-240). 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 CLSS Gateway 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 the *Show All Nodes* mode. If an *Unknown* node comes on line and is found to be of the wrong type for the CLSS Gateway to monitor, its Monitored field is automatically set to *No*. Some nodes in the node list are not usable by the CLSS Gateway and therefore are not configurable and do not have a unit ID.
Monitoring	• Select **Yes** to monitor the node. • Select **No** if the node is not to be monitored. At a given time, up to 10 nodes* can be monitored. * Excluding the CLSS Gateway.
MODULES MAPPING* * Modules mapping for channels is only for Notifier EN (ID3000 and Pearl) panels and AM-MA Series panels.	
Normal	300 detectors and 300 modules with 12 channels

Field	Description
Special	300 detectors, and • 1 - 15 modules with 12 channels • 16 - 40 modules with 3 channels • 41 - 300 modules with 2 channels
MODBUS TOOLS	
Control Functionality	01. Go to **Modbus Tools** in **Modbus Settings**. 02. Enable or disable as needed in the control functionality. 03. Read the UL Void message shown, if enabled. 04. Click **Save** to save it. 05. Wait until the CLSS Gateway shows the changes.
CSV REPORTS DOWNLOAD	
Actual Points	Click **Download** to download details of points (detectors and modules), which the panel monitors. The downloaded details will be in the CSV format.
All Points	Click **Download** to download details of monitored and unmonitored points. The downloaded details will be in the CSV format.
CONNECTED CLIENTS	
Show Connected Clients	Click **Show** to view all the clients connected to the Modbus master application.

13. Click **SAVE**.
14. Press the S6 button again until the LED indicator DL3 changes from ON to flashing.

NOTE: The configuration changes are enabled only after the gateway changes from the configuration mode to operational mode.

7.17 TO CONFIGURE THE MODBUS CLIENT

01. Open the Modbus master application you are using.
02. Specify the IP address of *Eth1* port of the CLSS Gateway.
03. Specify the port that the Modbus client is using in the **Service Port** field.

7.18 MODBUS COMMAND SUPPORT

The CLSS Gateway 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)

7.18.1 EXCEPTION RESPONSES

The CLSS Gateway sends exception responses to its Modbus clients as appropriate (e.g., invalid command, invalid data, etc.). For more information, refer to 7.27 Exception Responses .

7.18.2 MODBUS ADDRESSING

The CLSS Gateway uses Modbus addressing within the following guidelines:

- The CLSS Gateway operates similarly to a Modbus bridge. Each CLSS Gateway can support up to ten panels on a network. The Modbus master addresses each fire panel in the panel's network with a Unit ID.
- The Unit ID used in the CLSS Gateway must be in the range 1 to 240. This is a Modbus range limitation.

• The Unit ID should match the node number of the node, which is being addressed. For example, a Unit ID of 127 addresses node 127.
• The CLSS Gateway 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 000001–065536
  • 1x Discrete Input 10001–165536
  • 3x Input Register 300001–365536
  • 4x Holding Register 400001–465536

For more information on Modbus addressing, refer to 7.21 Register Mapping

7.19 CLSS GATEWAY CONTROL FEATURE

7.19.1 ENABLING THE CONTROL

CAUTION: UL LISTING
Enabling control voids the UL listing of the CLSS Gateway.

CLSS gateway control is enabled through a web page-based configuration tool running on the gateway. Enable control as follows:

01. Start the web browser on a computer that is in the same IP network as the CLSS Gateway.
    Note: Chrome is the recommended browser.
02. Enter the following URL in the browser:
    https://192.168.10.190:9443/config/index.html
03. Do the following if any security warning is shown. Otherwise, go to step 4.
    • Click the **Advanced** link below the error message.
    • Agree to proceed.
04. In the **Gateway Configuration Tool** page, enter the password.
05. Go to **Modbus Tools** in **Modbus Settings**.
06. Enable or disable as needed in the control functionality.
07. Read the **UL Void** message shown, if it is enabled.
08. Click **Save**.
09. Wait until the CLSS Gateway shows the changes.
10. Check that the changes are correct.

7.19.2 CONTROL COMMANDS

Using the CLSS Gateway you can send relevant command values to the holding registers of Points, Panels, and Zones. For detailed register mapping information refer to the 7.21 Register Mapping section.

The following tables display the values representing all the command types for nodes, points, and zones.

7.19.2.1 For NOTIFIER UL

Table 7.6 Device Commands

Command	Value	Holding Register
Acknowledge	0x0100	Use Device/Module Holding Register Address
Disable	0x0200	
Enable	0x0400	
Activate*	0x0800	
Deactivate*	0x1000	
* Activate and Deactivate work only for output-controlled modules like control and relay.		

Table 7.7 Panel Commands

Command	Value	Holding Register
Reset	0x0001	20001
Silence	0x0002	

Table 7.8 Zone Commands

Command	Value	Holding Register
Disable	0x0200	Use Zone Holding Register Address
Enable	0x0400	
Activate*	0x0800	
Deactivate*	0x1000	
* Activate and Deactivate work only for output-controlled modules like control and relay.		

Different panels support different zone types. Refer to Table 7.9 Zone Command Availability by Panel table for information about zone types supported

Table 7.9 Zone Command Availability by Panel

Panel Type	Enable/ Disable	Activate/ Deactivate	Enable/ Disable	Activate/ Deactivate	Enable/ Disable	Activate/ Disactivate
	General Zone		Logic Zones		Trouble/Release Zones	
AFP-2800	Yes	No	No	No	No	No
AFP-3030	Yes	No	No	No	No	No
N16	Yes	Yes	Yes	No	No	No
NFS-320	Yes	No	No	No	No	No
NFS-640	Yes	No	No	No	No	No
NFS2-640	Yes	No	No	No	No	No
NFS-3030	Yes	No	No	No	No	No
NFS2-3030	Yes	Yes	Yes	No	No	No
XLS 120	Yes	No	No	No	No	No
XLS 140-2	Yes	No	No	No	No	No
XLS 2000	Yes	No	No	No	No	No
XLS 3000	Yes	Yes	Yes	No	No	No

7.19.2.2 Generic Commands List

Table 7.10 Device Commands

Commands	Value	Gamewell-FCI	AM-MA Series	Notifier EN	Holding Register
Commands	Value	Gamewell-FCI	AM-MA Series	Notifier EN	Holding Register
Enable[1]	0x0400	No	Yes	Yes	Use Device/Module Holding Register Address
Disable[1]	0x0500	No	Yes	Yes	
Acknowledge Trouble	0x0b00	Yes	No	No	
Acknowledge Alarm	0x0c00	Yes	No	No	
Acknowledge CO and Gas Alarm	0x0d00	Yes	No	No	

[1]Enable and disable for channels are available in AM-MA Series panels only. Enable and disable for devices are available for all AM-MA Series and NOTIFIER EN brands, but not available for Gamewell-FCI panels.

Table 7.11 Zone Commands

Commands	Value	Gamewell-FCI	AM-MA Series	Notifier EN	Holding Register
Enable	0x0600	No	Yes	Yes	Use Zone Holding Register Address
Disable	0x0700	No	Yes	Yes	
Zone mode	0x1500	No	No	Yes	

Table 7.12 Panel Commands

Commands	Value	Gamewell-FCI	AM-MA Series	Notifier EN	Holding Register
Disable sounder	0x0013	No	No	Yes	20001
Enable sounder	0x0014	No	No	Yes	20001
Reset	0x0000	Yes	Yes	Yes	20001
Silence	0x0001	Yes	Yes	Yes	20001
Unsilence	0x000A	Yes	No	No	20001
Deactivate Buzzer	0x000E	No	Yes	Yes	20001
Terminate test[1]	0x0012	No	No	Yes	20001
Walk test - Sounder On	0x000F	No	No	Yes	20001
Walk test - No sounder On	0x0010	No	No	Yes	20001
Walk test - off	0x0011	No	No	Yes	20001

Only for Zone tests.

7.20 NOTIFIER UL: ANALOG VALUES AND TRENDING

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. Refer to 7.20.1 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 CLSS Gateway has had enough time to get the analog values and load the registers. Thereafter the CLSS Gateway continues to poll the points. The analog value in the CLSS Gateway 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 CLSS Gateway 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 15 seconds.
    - The gateway makes a request for a point (or points) that is not *exactly the same as the initial request*. The CLSS Gateway 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.

7.20.1 ANALOG VALUE USE CASES

Use Case 1: A client requests analog values from the points L1M1 through L1M10 every 10 seconds.
Result: The CLSS Gateway sends back zeros in response to the first request for analog values from the points L1M1 through L1M10. The CLSS Gateway sends back actual values on the second request from the client 5 seconds later. The CLSS Gateway 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 CLSS Gateway sends back zeros in response to the first request for analog values from the points L1M1 through L1M10. The CLSS Gateway sends back actual values on the second request from the client 10 seconds later. The CLSS Gateway 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 CLSS Gateway will stop polling the NFN after the Analog Value Time Out expires.

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 CLSS Gateway sends back zeros in response to the first request for analog values from the points L1M1 through L1M10. The CLSS Gateway 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, gateway waits till the timeout happens and then the CLSS Gateway immediately sends back zeros in response to the first analog value request from these points and starts polling L1M20 through L1M22. The CLSS Gateway 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 CLSS Gateway sends back zeros in response to the first request for analog values from the points L1M1 through L1M10. The CLSS Gateway sends back actual values in response to the second request from the client 10 seconds later. The CLSS 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 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 CLSS Gateway 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.

7.21 REGISTER MAPPING

7.21.1 REGISTER MAPPING OVERVIEW

The CLSS Gateway 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.

CAUTION: Ack Block and Ack alarm are not applicable for Notifier EN (ID3000 and Pearl) panels and AM-MA Series panels.

7.21.1.1 Point Status Holding Registers

CAUTION: A Limitation - for Notifier EN (ID3000 and Pearl) panels, Parent modules and their channels will not get initiated with the register value 0x1400. However, they will continue to receive the events.

Each of the point status holding registers is divided into an upper and lower byte as described below. See Table 7.13 Point Status Holding Register: Bit Definitions table for detailed information about point status holding registers.

- **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', see 7.28 CLSS Gateway Active Event Code 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, but the upper byte will contain a '0'.

The only possible active event type for zones is Non-Fire Activation (71H). 7.28 CLSS Gateway Active Event Code

Table 7.13 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 Code** (When Bit 11 is set to 1, see 7.28 CLSS Gateway Active Event Code .)							
	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. **AckFireAlarm** (Bit 8): The fire alarm on this point is acknowledged. Not applicable for zones.															

Refer to Table 7.14 Point Status Holding Register Point Addresses table for details of the holding register addresses and the channels. Each holding register range is for either detectors or modules.

Table 7.14 Point Status Holding Register Point Addresses

Start Address	End Address	Address
400001	400300	L1D1–L1D300
400301	400600	L1M1–L1M300
400601	400900	L2D1–L2D300
400901	401200	L2M1–L2M300
401201	401500	L3D1–L3D300
401501	401800	L3M1–L3M300
401801	402100	L4D1–L4D300
402101	402400	L4M1–L4M300
402401	402700	L5D1–L5D300
402701	403000	L5M1–L5M300
403001	403300	L6D1–L6D300
403301	403600	L6M1–L6M300
403601	403900	L7D1–L7D300
403901	404200	L7M1–L7M300
404201	404500	L8D1–L8D300
404501	404800	L8M1–L8M300
404801	405100	L9D1–L9D300
405101	405400	L9M1–L9M300
405401	405700	L10D1–L10D300
405701	406000	L10M1–L10M300

NOTE: On the AFP-2800, output activation status is not reported to the CLSS Gateway and therefore the bits and event type will always indicate a non-active state.

7.21.1.2 Point Device Type Input Registers

CAUTION: A Limitation - for Notifier EN (ID3000 and Pearl) panels, Parent modules and their channels are not shown in the CSV file and in the device type registers.

NOTE: If the point is not present in the panel programming, all bits in the byte will contain a value of *1* or *FFFFH*.

There are 6000 point device type holding registers. Each register address consists of two bytes representing a detector or module.

NOTE: For Gamewell-FCI panels, the user-defined data types and the CSV file would not have Device Types.

Table 7.15 Point Device Type Input 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 7.29 Device Types)																

Table 7.16
Input Register Addresses of the Point Device Types

Start Address	End Address	Address
300001	300300	L1D1–L1D300
300301	300600	L1M1–L1M300
300601	300900	L2D1–L2D300
300901	301200	L2M1–L2M300
301201	301500	L3D1–L3D300
301501	301800	L3M1–L3M300
301801	302100	L4D1–L4D300
302101	302400	L4M1–L4M300
302401	302700	L5D1–L5D300
302701	303000	L5M1–L5M300
303001	303300	L6D1–L6D300
303301	303600	L6M1–L6M300
303601	303900	L7D1–L7D300
303901	304200	L7M1–L7M300
304201	304500	L8D1–L8D300
304501	304800	L8M1–L8M300
304801	305100	L9D1–L9D300
305101	305400	L9M1–L9M300
305401	305700	L10D1–L10D300
305701	306000	L10M1–L10M300

7.21.1.3 Zones/Panel Circuits Status Holding Registers

CAUTION: Gamewell-FCI panels do not support Zones. Notifier EN (ID3000 and Pearl) panels and the AM-MA Series panels support only the General Zones.

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

- **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', see 7.28 CLSS Gateway Active Event Code

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', but the upper byte will contain a '0'.

Table 7.17 Zones/Panel Circuits Holding Registers: 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 7.28 CLSS Gateway Active Event Code .)							
	When individual upper byte bits are set to 1, the following definitions apply: **AckBlock** (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 this table.

Table 7.18 Register and Zone Addresses for Zone Types

Zone Type	Register Address	Zone Address
General Zones	408001–410000	Z 1,2,3,4,5,6,7,8,...2000
Logic Zones	410001–412000	Z 1,2,3,4,5,6,7,8,...2000
Trouble Zones	412001–412100	Z 1,2,3,4,5,6,7,8,...100
Releasing Zones	412101–412200	Z 1,2,3,4,5,6,7,8,...100

The holding register addresses and the panel circuits contained in these addresses are detailed in Table 7.19 Register Addresses for Panel Circuits .

Table 7.19 Register Addresses for Panel Circuits

Register Address	Panel Circuits
414001–414008	P1.1–P1.8
414009–414016	P2.1–P2.8
414017–414024	P3.1–P3.8
414025–414032	P4.1–P4.8
414033–414040	P5.1–P5.8
414041–414048	P6.1–P6.8
414049–414056	P7.1–P7.8
414057–414064	P8.1–P8.8
414065–414072	P9.1–P9.8
414073–414080	P10.1–P10.8
414081–414088	P11.1–P11.8
414089–414096	P12.1– P12.8

The maximum panel circuit points by fire panel is described in Table 7.20 Supported Circuits by Panel .

Table 7.20 Supported Circuits by Panel

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

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

7.21.1.4 Channel Status Holding Registers

Each channel status holding register is arranged into an *Upper Byte* and *Lower Byte* as described in the Table 7.21 Channel Status Holding Register: Bit Definitions :

• **Upper Byte**: Has general status information about the point.
• **Lower Byte**: Primarily used when bit 11 in the upper byte is a '1', which means the channel is active. Any Fire, Security, Critical Process, Medical, Mass Notification, or Supervisory alarm state identifies the active state in this gateway.

Refer to 7.28 CLSS Gateway Active Event Code for detailed information about the active point.

All of the lower byte will be zeroes if the device is not in an active state.

If the channel is not present in the panel programming, all bits in the Lower Byte will have a '1' or the value FFH, but the Upper Byte will have a '0'.

Specifically, the lower byte contains the actual active event for this channel. An active state is defined in this gateway as any Fire, Security, Critical Process, Medical, Mass Notification, or Supervisory alarm state.

If the channel is not present in the panel programming, all bits in the lower byte will contain a '1' or the value FFH, but the upper byte will contain a '0'.

Table 7.21 Channel 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 Code** (When Bit 11 is set to 1, see 7.28 CLSS Gateway Active Event Code .)							
	When individual upper byte bits are set to 1, the following definitions apply: **Ack Block** (Bit 15): All events on this channel, other than fire alarm, are acknowledged. Not applicable for zones. **Prealarm** (Bit 14): The channel is in a prealarm state. Not applicable for zones. **Trouble** (Bit 13): The channel is in a trouble state. Not applicable for zones. **InActive** (Bit 12): The channel is not active. **Active** (Bit 11): The channel is active and there will be an active event type in the lower byte. **Enable** (Bit 10): The channel is enabled. **Disable** (Bit 9): The channel is disabled. **Ack Fire Alarm** (Bit 8): The fire alarm on this channel is acknowledged.															

Refer to the 7.21.1.5 Mapping for Channels section for details of the holding register addresses and the channels. Each holding register address range is for channels.

7.21.1.5 Mapping for Channels

The holding register addresses for the channels are described below.

• **Normal Mapping**

Table 7.22 Holding Register Addresses for Normal Mapping

Start Address	End Address	Address
421001	424600	L1M1 - L1M300
424601	428200	L2M1 - L2M300
428201	431800	L3M1 - L3M300
431801	435400	L4M1 - L4M300
435401	439000	L5M1 - L5M300

Start Address	End Address	Address
439001	442600	L6M1 - L6M300
442601	446200	L7M1 - L7M300
446201	449800	L8M1 - L8M300
449801	453400	L9M1 - L9M300
453401	457000	L10M1 - L10M300

Table 7.23 Input Register Addresses for Normal Mapping

Start Address	End Address	Address
321001	324600	L1M1 - L1M300
324601	328200	L2M1 - L2M300
328201	331800	L3M1 - L3M300
331801	335400	L4M1 - L4M300
335401	339000	L5M1 - L5M300
339001	342600	L6M1 - L6M300
342601	346200	L7M1 - L7M300
346201	349800	L8M1 - L8M300
349801	353400	L9M1 - L9M300
353401	357000	L10M1 - L10M300

- **Special Mapping**

Table 7.24 Holding Register Addresses for Special Mapping

Start Address	End Address	Address
421001	421775	L1M1 - L1M300
421776	422550	L2M1 - L2M300
422551	423325	L3M1 - L3M300
423326	424100	L4M1 - L4M300
424101	424875	L5M1 - L5M300
424876	425650	L6M1 - L6M300
425651	426425	L7M1 - L7M300
426426	427200	L8M1 - L8M300
427201	427975	L9M1 - L9M300
427976	428750	L10M1 - L10M300

Table 7.25 Input Register Addresses for Special Mapping

Start Address	End Address	Address
321001	321775	L1M1 - L1M300
321776	322550	L2M1 - L2M300
322551	323325	L3M1 - L3M300
323326	324100	L4M1 - L4M300
324101	324875	L5M1 - L5M300
324876	325650	L6M1 - L6M300
325651	326425	L7M1 - L7M300
326426	327200	L8M1 - L8M300
327201	327975	L9M1 - L9M300
327976	328750	L10M1 - L10M300

• **Channel Device Type Input Registers**

> **NOTE:** If the channel is not present in the panel programming, all bits in the byte will contain a value of *1* or *FFFFH*.

There are 57000 channel device type input registers for normal mapping. 7750 device type input registers for special mapping. Each register address consists of two bytes representing a detector or module.

Table 7.26 Channel Device Type Input Registers

	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 7.29 Device Types)																

7.21.2 GAMEWELL-FCI: CAM TEXT EVENT HOLDING REGISTERS

Each of the point status holding registers is divided into an upper and lower byte as described in Table 7.27 CAM Text Event Holding Register Bit Definitions .

• **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', 7.28 CLSS Gateway Active Event Code for detailed information about the active point. The lower byte will be all 0's if the point 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', but the upper byte will contain a '0'.

The holding register address and the CAM Text Event contained in the address are detailed in the following table.

Table 7.27 CAM Text Event 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 Code** (When Bit 11 is set to 1, see 7.28 CLSS Gateway Active Event Code .)							
	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. **AckFireAlarm** (Bit 8): The fire alarm on this point is acknowledged. Not applicable for zones.															

Table 7.28 CAM Test Events Register Address

Start Address	End Address	CAM Text
415001	416000	CAM1 – CAM 1000

7.21.2.1 Bell Circuits Status Holding Registers

NFS2-640 and NFS-320 Only

Each of the bell circuits status holding registers is divided into an upper and lower byte as described in Table 7.29 Bell Circuits Holding Register Bit Definitions .

• **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', 7.28 CLSS Gateway Active Event Code 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', but the upper byte will contain a '0'.

Table 7.29 Bell 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 7.28 CLSS Gateway Active Event Code .)							
	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 7.30 Bell Circuit Holding Register Addresses table.

Table 7.30 Bell Circuit Holding Register Addresses

Start Address	End Address	Device Address
406001	406001	Bell Circuit 1
406002	406002	Bell Circuit 2
406003	406003	Bell Circuit 3
406004	406004	Bell Circuit 4

Bell Circuits Device Type Input Registers

NOTE: If the point is not present in the panel programming, all bits in the byte will contain a value of *1* or *FFFFH*.

Each bell circuits device type holding register address consists of two bytes as defined in Table 7.31 Bell Circuits Device Type Input Register Bit Definitions representing a bell circuit as shown in Table 7.32 Bell Circuit Device Type -Input Register Addresses .

Table 7.31 Bell Circuits Device Type Input 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 7.29 Device Types)																

Table 7.32 Bell Circuit Device Type -Input Register Addresses

Start Address	End Address	Device Address
306001	306001	BellCircuit1
306002	306002	BellCircuit2
306003	306003	BellCircuit3
306004	306004	BellCircuit4

7.21.2.2 Panel Status Holding Register

The panel status holding register is divided into an upper and lower byte as described below and in Panel Status Holding Register Bit Definitions representing one register address as shown in Panel Status Holding Register Addresses.

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

Table 7.33 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 7.34 Panel Status Holding Register Addresses

Start Address	End Address	Description
420001	420001	Panel Status Holding Register

7.21.2.3 Analog Values Input Registers

Analog values listed in Input Register Analog Values are only available for 4–20 mA modules. Refer to Input Register Analog Values for details regarding analog values.

Table 7.35 Input Register Analog Values

Start Address	End Address	Analog Value (16 bits)
310001	310300	L1M1–L1M300
310301	310600	L2M1–L2M300
310601	310900	L3M1–L3M300
310901	311200	L4M1–L4M300
311201	311500	L5M1–L5M300
311501	311800	L6M1–L6M300
311801	312100	L7M1–L7M300
312101	312400	L8M1–L8M300
312401	312700	L9M1–L9M300
312701	313000	L10M1–L10M300

Panel and System Troubles Holding Registers

One hundred 16-bit registers are Reserved for panel troubles and one register is assigned as an overall panel trouble indicator as shown in Panel and System Troubles Holding Register Addresses.

Table 7.36 Panel and System Troubles Holding Register Addresses

Start Address	End Address	Description
460000	460000	Panel Trouble Summary (Total number of Trouble bits set for the node)
460001	460100	Panel Troubles

A single bit is Reserved for each trouble in the system. The assignment of bits to trouble codes is shown in 7.30 System Troubles Register Map .

7.21.3 GENERAL COUNTERS

The General Counters are Registers used for having a count of different events in a Loop based on detectors or modules.

Table 7.37 The General Counters

Counters	Loop Detectors	Loop Modules	Loop Detectors	Loop Modules
	Loop 1		Loop 2	
Loop alarms Lx	414101	414106	414112	414117
Loop Troubles Lx	414102	414107	414113	414118
Loop Prealarms Lx	414103	414108	414114	414119

Counters	Loop Detectors	Loop Modules	Loop Detectors	Loop Modules
Loop Disables Lx	414104	414109	414115	414120
Loop tests Lx	414105	414110	414116	414121
Active NONAS Lx		414111		414122
	Loop 3		**Loop 4**	
Loop alarms Lx	414123	414128	414134	414139
Loop Troubles Lx	414124	414129	414135	414140
Loop Prealarms Lx	414125	414130	414136	414141
Loop Disables Lx	414126	414131	414137	414142
Loop tests Lx	414127	414132	414138	414143
Active NONAS Lx		414133		414144
	Loop 5		**Loop 6**	
Loop alarms Lx	414145	414150	414156	414161
Loop Troubles Lx	414146	414151	414157	414162
Loop Prealarms Lx	414147	414152	414158	414163
Loop Disables Lx	414148	414153	414159	414164
Loop tests Lx	414149	414154	414160	414165
Active NONAS Lx		414155		414166
	Loop 7		**Loop 8**	
Loop alarms Lx	414167	414172	414178	414183
Loop Troubles Lx	414168	414173	414179	414184
Loop Prealarms Lx	414169	414174	414180	414185
Loop Disables Lx	414170	414175	414181	414186
Loop tests Lx	414171	414176	414182	414187
Active NONAS Lx		414177		414188
	Loop 9		**Loop 10**	
Loop alarms Lx	414189	414194	414200	414205
Loop Troubles Lx	414190	414195	414201	414206
Loop Prealarms Lx	414191	414196	414202	414207
Loop Disables Lx	414192	414197	414203	414208
Loop tests Lx	414193	414198	414204	414209
Active NONAS Lx		414199		414210

7.21.4 GATEWAY INFORMATION INPUT REGISTERS

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

The CLSS Gateway records some status and configuration information for debugging and technical support purposes. This information is stored in some Reserved gateway registers as outlined below.

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

Table 7.38 Gateway Information Input Registers

Start Address	End Address	Description
360001	360100	Information/Debug information

Start Address	End Address	Description
320001	320015	Node Status: 1 = On Line 0 = Off Line The CLSS Gateway tracks status of network nodes under Modbus feature monitoring.
360016	360016	Gateway major version number
360017	360017	Gateway minor version number
360018	360018	Gateway feature number
360019	360019	Gateway build number

7.21.5 NODE STATUS DETAILS

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

Table 7.39 Node Status Details

Address	Bit Number															
	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
320001	N15	N14	N13	N12	N11	N10	N9	N8	N7	N6	N5	N4	N3	N2	N1	N0
320002	N31	N30	N29	N28	N27	N26	N25	N24	N23	N22	N21	N20	N19	N18	N17	N16

7.21.5.1 For Gamewell Panel Status

Table 7.40 System Trouble

Register	Bit No.	System Trouble Name
460051	4	Node Missing

7.21.5.2 For Pearl Panel Status

Table 7.41 System Trouble

Register	Bit No.	System Trouble Name
4600060	15	NETWORK DOMAIN RING OR SUBNET LOST

7.22 READ DEVICE IDENTIFICATION (0X2B/0X0E)

This function code allows reading the identification and additional information about the CLSS Gateway.

Table 7.42 Objects and Their Details

Object ID	Object Name / Description	Value
0x00	VendorName	Honeywell
0x01	ProductCode	HON-CGW-MBB
0x02	MajorMinorRevision	V1.0 (*Example*)
0x03	VendorUrl	www.fire.honeywell.com
0x04	ProductName	CLSS
0x05	ModelName	CLSS Gateway
0x06	UserApplicationName	Modbus Service
0x07	MappingVersion	V1.0 (Example)

7.23 TROUBLESHOOTING

7.23.1 WHAT ARE SOME BASIC GUIDELINES WHEN INSTALLING A CLSS GATEWAY?

• 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 CLSS Gateway 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.

7.23.2 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.

7.23.3 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 toolthat 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.

7.23.4 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.

7.23.5 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.

7.23.6 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.

7.23.7 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.

7.23.8 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.

7.23.9 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.

7.24 CONVERSION TO MODBUS RTU

CLSS Gateway (acting as a Modbus slave) interfaces with a Modbus master through Modbus TCP protocol. For a Modbus RTU master to interface with the CLSS Gateway, use Moxa MGate MB3180 and convert the Modbus TCP protocol to the Modbus RTU (Serial) protocol.

7.24.1 HARDWARE CONFIGURATION

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

7.24.2 SOFTWARE CONFIGURATION

Configure the CLSS Gateway as a node in the NFN network with a node number.

CAUTION: Ensure that the NFN network configurations are Unchanged.

Refer to the *NOTI•FIRE•NET™ Network Systems Interface Manual (P/N 51584)* or the *High Speed NOTI•FIRE•NET™ Instruction Manual (P/N 54013)* for details about network configuration.

When configuring the network, refer to the settings specified in " MGate MB3180 Configuration Settings" on the next page table. Settings not specified should be tailored to your network requirements. Refer to the *MGate MB3000 Modbus Gateway User’s Manual* for details.

01. Connect the MB3180 to a configuration computer through an Ethernet cable as shown in "Connect a Configuration Computer" below.

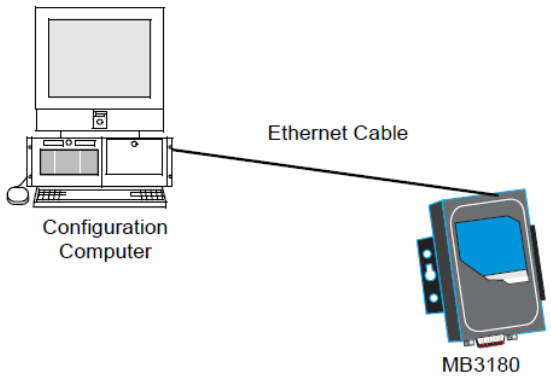


Figure 7-6: Connect a Configuration Computer

02. Run the *MGate Manager* installation software (MGM_Setup_Verx.x_Build_xxxxxxxx.exe) found on the Software CD shipped with the MGate MB3180.
03. Wait for the installation to complete.
04. Run *MGate Manager*.
05. Power up the MB3180.
06. Ensure that the Ready and Ethernet lights are ON.
07. Configure the MB3180 for the network.
08. Wait for the configuration to complete.
09. Click **OK**.
10. Click **Exit**.

Table 7.43 MGate MB3180 Configuration Settings

Tab	Setting
Mode	RTU Master Mode
Slave ID Map	The MGate MB3180 accepts the Modbus Unit ID as a virtual slave ID and monitors devices with these virtual slave IDs. By default, the CLSS Gateway assigns a Modbus Unit ID to each node on the NFN network. The ID is equal to node number of the node. They can be changed, but should be within 1 to 99. Refer to the 7.16 To Configure the Modbus Settings section for more information about changing a Modbus Unit ID.
Modbus	Initial Delay: 0 ms Response Time-out: 1000 ms

7.25 CONNECTING THE MOXA MGATE MB3180 INTERFACE

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

01. Connect the RTU master to the Serial port (RS-232, RS-485, or RS-422) of MB3180.
02. Connect the MB3180 to the CLSS Gateway.
    Figure 7-7: Connection Through Crossover Ethernet Cable and Figure 7-8: Connection Through a Router show possible configurations for connecting the CLSS Gateway to the Moxa interface.
03. Power up the system.

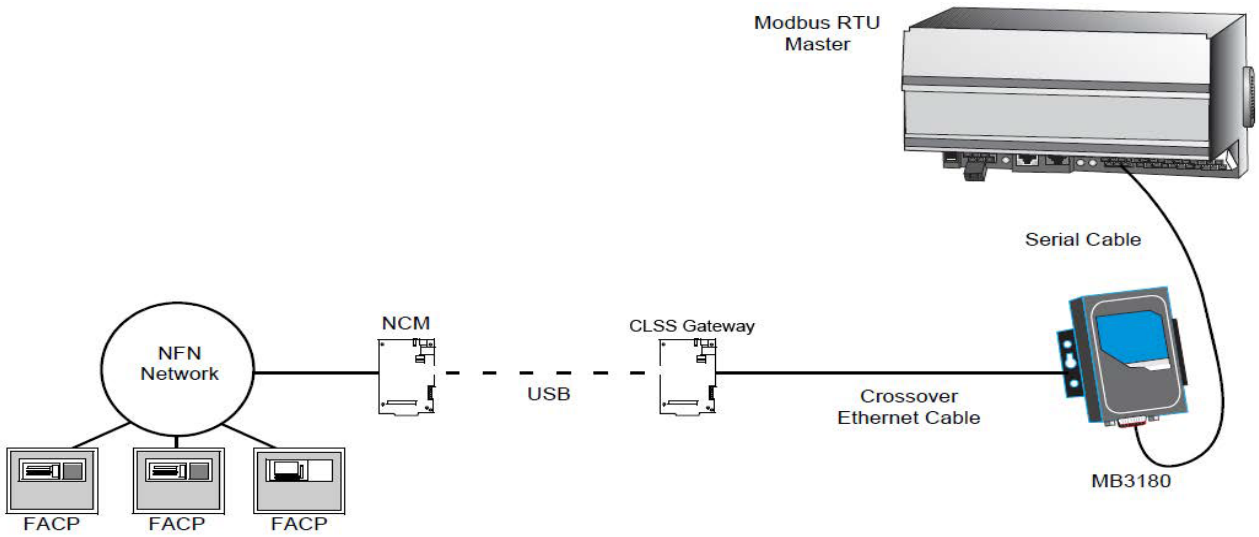


Figure 7-7: Connection Through Crossover Ethernet Cable

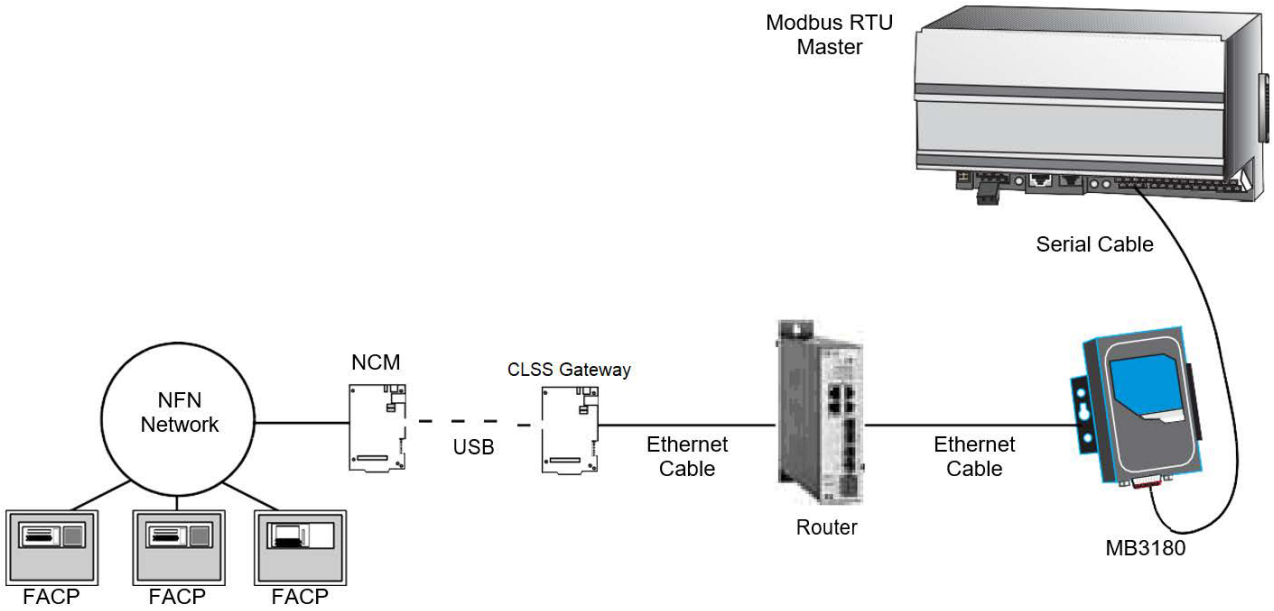


Figure 7-8: Connection Through a Router

7.26 SYSTEM TROUBLE

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

7.27 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. The table describes the exception codes sup- ported and the possible causes.

Table 7.44 Exception Codes and Their Details

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 CLSS Gateway 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

7.28 CLSS GATEWAY ACTIVE EVENT CODE

All events are mapped into Modbus event categories which are stored in the Modbus register.

Table 7.45 Event Code and Event Details

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

Event	Modbus Register Value
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
For Gamewell-FCI	
General Alarm	18H
Gas Alarm	22H
CO Supervisory	42H

NOTE: 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 7.21 Register Mapping .

7.29 DEVICE TYPES

Device types are organized into the following categories:

- Detectors (1–50) - Table 7.46 Device Type Values - Detectors
- Modules (51–150) - Table 7.47 Device Type Values – Modules

Table 7.46 Device Type Values - Detectors

Device Type	Value	Device Type	Value
Not Identified	0000H	Wireless Smoke Photo Tracking	0311H
Heat	0100H	Smoke Laser Latching	0400H
Heat (rate of rise)	0101H	Smoke Laser Tracking	0401H
Heat (fixed)	0102H	Duct Smoke Laser Latching	0402H
Heat (high heat)	0103H	Duct Smoke Laser Tracking	0403H
Wireless Heat	0110H	Air Reference Laser	0404H
Wireless Heat (rate of rise)	0111H	Smoke (Harsh)	0500H
Wireless Heat (fixed)	0112H	Smoke (Beam)	0501H
Wireless (high heat)	0113H	Smoke Multi	0600H
Smoke Ion Latching	0200H	Smoke Acclimate	0601H

Device Type	Value	Device Type	Value
Smoke Ion Tracking	0201H	Wireless Smoke Multi	0610H
Duct Smoke Ion Latching	0202H	Wireless Smoke Acclimate	0611H
Duct Smoke Ion Tracking	0203H	CO Alarm	0700H
Smoke Photo Latching	0300H	Fire/CO	0701H
Smoke Photo Tracking	0301H	Photo/CO	0702H
Duct Smoke Photo Latching	0302H	CO/Photo/Thermal/IR	0703H
Duct Smoke Photo Tracking	0303H	Aspiration	0801H
Smoke (Photo Flame)	0304H	Aspir. Ref	0802H
Wireless Smoke Photo Latching	0310H		

Table 7.47 Device Type Values - Modules

Device Type	Value	Device Type	Value
Not Identified	0000H	Acknowledge Switch	0041H
Heat Detection Circuit	0001H	Wireless Acknowledge Switch	0042H
Wireless Heat Detection Circuit	0002H	All Call Page	0043H
Conventional Smoke	0003H	Drill Switch	0044H
Wireless Conventional Smoke	0004H	Wireless Drill Switch	0045H
Smoke Detection	0005H	Evacuate Switch	0046H
Wireless Smoke Detection	0006H	Wireless Evacuate Switch	0047H
Monitor	0010H	Signals Silence Switch	0048H
Wireless Monitor	0011H	Wireless Signals Silence Switch	0049H
Pull Station	0012H	Reset Switch	004AH
Wireless Pull Station	0013H	Wireless Reset Switch	004BH
Monitor Tracking	0014H	Fire Control	0050H
Wireless Monitor Tracking	0015H	Hazard	0051H
Normally Closed Monitor	0016H	Wireless Hazard	0052H
Wireless Normally Closed Monitor	0017H	Medical	0053H
Normally Closed Monitor Tracking	0018H	Wireless Medical	0054H
Wireless Normally Closed Monitor Tracking	0019H	Relay	1002H
Disable	001AH	Wireless Relay	1003H
Wireless Disable	001BH	Non-reset Control	1004H
Waterflow	0020H	Wireless Non-Reset Control	1005H
Wireless Waterflow	0021H	Bell Circuit	1010H
Sprinkler System	0022H	Strobe Circuit	1011H
Access Monitor	0030H	Horn Circuit	1012H
Wireless Access Monitor	0031H	Speaker Circuit	1013H
Area Monitor	0032H	Speaker	1014H
Wireless Area Monitor	0033H	Telephone	1015H
Equipment Monitor	0034H	Isolated Speaker	1016H
Wireless Equipment Monitor	0035H	Isolated Notification Appli-ance Circuit	1017H
Hold Up	0036H	Releasing Circuit	1020H
Wireless Hold Up	0037H	Releasing Circuit ULC	1021H
Tamper	0038H	Releasing Form C	1022H
Wireless Tamper	0039H	Releasing Bell	1023H
Secure/Access	003AH	Releasing Audible	1024H

Device Type	Value	Device Type	Value
Telephone Page	0040H	Instant Release	1030H
Weather	0055H	Alarms Pending	1031H
Wireless Weather	0056H	Control Notification Appliance Circuit	1032H
Positive Alarm Sequence Inhibit Input	0060H	General Alarm	1033H
Abort Switch	0061H	General Supervisory	1034H
Manual Release	0062H	General Trouble	1035H
Manual Release Delay	0063H	General Pending	1036H
Second Shot	0064H	Trouble Pending	1037H
Audio System	0070H	Form C Reset	1038H
Power Supply	0071H	Relay Feedback	1040H
Wireless System	0072H	Relay Form C Feedback	1041H
Bi-Directional Amplifier/Distributed Antenna System	0073H	Control Feedback	1042H
Process Monitor	0080H	ECS/MNS General	1050H
Process Auto	0081H	ECS/MNS Control	1051H
4-20mA sensor	0090H	ECS/MNS Strobe	1052H
Wireless 4-20mA sensor	0091H	ECS/MNS Speaker	1053H
Feedback	00A0H	ECS/MNS Relay	1054H
Feedback Tracking	00A1H	Auxiliary	1060H
Hydrant	00A2H	Door Holder	1061H
Control	1000H	AAM Sounder	1062H
Wireless Control	1001H	TYPE 5 Control	1063H

7.30 SYSTEM TROUBLES REGISTER MAP

Register	Bit No.	System Trouble Name	Bit No.	System Trouble Name
460001	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 / FLASH IMAGE ERROR	15	ANNUN. 1 TROUBLE
460002	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

Register	Bit No.	System Trouble Name	Bit No.	System Trouble Name
460003	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
460004	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
460005	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
460006	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
460007	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

Register	Bit No.	System Trouble Name	Bit No.	System Trouble Name
460008	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
460009	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
460010	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
460011	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
460012	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

Register	Bit No.	System Trouble Name	Bit No.	System Trouble Name
460013	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
460014	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
460015	0	STYLE 4 SHORT A LOOP 7	8	GENERAL PS FAULT / POWER SUPPLY TROUBLE
	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
460016	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	WORKSTATION FAILURE
	5	DVC COMM LOSS	13	NETWORK MAPPING LIMIT EXCEEDED
	6	POWER SUPPLY CABLE NOT CONNECTED	14	INVALID NODE TYPE
	7	TM4 TROUBLE	15	DISPLAY NODE LIMIT EXCEEDED
460017	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

Register	Bit No.	System Trouble Name	Bit No.	System Trouble Name
460018	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
460019	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
460020	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
460021	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
460022	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

Register	Bit No.	System Trouble Name	Bit No.	System Trouble Name
460023	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
460024	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
460025	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
460026	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
460027	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

Register	Bit No.	System Trouble Name	Bit No.	System Trouble Name
460028	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
460029	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
460030	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
460031	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
460032	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 / HISTORY 80% FULL	13	LOOP 9-10 COMM FAILURE
	6	EBI STATUS	14	TEST PROGRAM UPDATE
	7	SOFTWARE MISMATCH	15	Reserved

Register	Bit No.	System Trouble Name	Bit No.	System Trouble Name
460033	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
460034	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
460035	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
	7	TRANSMIT/RECIEVE ERROR ABOVE LIMIT ON LOOP 10	15	TOO MANY DEVICES ON LOOP 8
460036	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

Register	Bit No.	System Trouble Name	Bit No.	System Trouble Name
460037	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	Reserved
	5	DAL No Answer / DAL DEVICE NO ANSWER	13	Reserved
	6	LOCAL MIC TROUBLE	14	AMPLIFIER LIMIT
	7	LOCAL PHONE TROUBLE	15	AMPLIFIER SUPERVISION
460038	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
460039	0	DAL DOWNLOAD IN PROGRESS	8	PRIMARY AMP 1 HARDWARE FAIL
	1	FIRE VOICE TROUBLE	9	PRIMARY AMP 2 HARDWARE FAIL
	2	FIRE VOICE NO ANSWER	10	PRIMARY AMP 3 HARDWARE FAIL
	3	PHONE CHANNEL LIMIT EXCEEDED	11	PRIMARY AMP 4 HARDWARE FAIL
	4	NCM SMIFFER MODE ACTIVE	12	BACKUP AMP 1 HARDWARE FAIL
	5	LOCAL CONNECTION LIMIT EXCEEDED	13	BACKUP AMP 2 HARDWARE FAIL
	6	HARDWARE MISMATCH	14	BACKUP AMP 3 HARDWARE FAIL
	7	Reserved	15	BACKUP AMP 4 HARDWARE FAIL
460040	0	DSBUS 1 COMMFAIL	8	PRIMARY AMP 2 LIMIT
	1	DSBUS 2 COMMFAIL	9	PRIMARY AMP 3 LIMIT
	2	DSBUS 3 COMMFAIL	10	PRIMARY AMP 4 LIMIT
	3	DSBUS 4 COMMFAIL	11	BACKUP AMP 1 LIMIT
	4	AA TROUBLE BUS FAIL	12	BACKUP AMP 2 LIMIT
	5	NFN PAGING CHANNEL LIMIT EXCEEDED	13	BACKUP AMP 3 LIMIT
	6	BACKUP AMP LIMIT	14	BACKUP AMP 4 LIMIT
	7	PRIMARY AMP 1 LIMIT	15	PRIMARY AMP 1 OVERCURRENT
460041	0	PRIMARY AMP 2 OVERCURRENT	8	PRIMARY AMP 2 TRIP
	1	PRIMARY AMP 3 OVERCURRENT	9	PRIMARY AMP 3 TRIP
	2	PRIMARY AMP 4 OVERCURRENT	10	PRIMARY AMP 4 TRIP
	3	BACKUP AMP 1 OVERCURRENT	11	BACKUP AMP 1 TRIP
	4	BACKUP AMP 2 OVERCURRENT	12	BACKUP AMP 2 TRIP
	5	BACKUP AMP 3 OVERCURRENT	13	BACKUP AMP 3 TRIP
	6	BACKUP AMP 4 OVERCURRENT	14	BACKUP AMP 4 TRIP
	7	PRIMARY AMP 1 TRIP	15	DSBUS 1 AC FAIL

Register	Bit No.	System Trouble Name	Bit No.	System Trouble Name
460042	0	DSBUS 2 AC FAIL	8	DSBUS 2 LOW BATT
	1	DSBUS 3 AC FAIL	9	DSBUS 3 LOW BATT
	2	DSBUS 4 AC FAIL	10	DSBUS 4 LOW BATT
	3	DSBUS 1 HIGH BATT	11	DSBUS 1 SELF TEST FAIL
	4	DSBUS 2 HIGH BATT	12	DSBUS 2 SELF TEST FAIL
	5	DSBUS 3 HIGH BATT	13	DSBUS 3 SELF TEST FAIL
	6	DSBUS 4 HIGH BATT	14	DSBUS 4 SELF TEST FAIL
	7	DSBUS 1 LOW BATT	15	PRIMARY AMP 1 FAIL
460043	0	PRIMARY AMP 2 FAIL	8	BACKUP AMP 1 NOT INSTALLED
	1	PRIMARY AMP 3 FAIL	9	BACKUP AMP 2 NOT INSTALLED
	2	PRIMARY AMP 4 FAIL	10	BACKUP AMP 3 NOT INSTALLED
	3	BACKUP AMP 1 FAIL	11	BACKUP AMP 4 NOT INSTALLED
	4	BACKUP AMP 2 FAIL	12	MODBUS COMMUNICATIONS FAULT
	5	BACKUP AMP 3 FAIL	13	VESDANET TROUBLE
	6	BACKUP AMP 4 FAIL	14	(Reserved)
	7	BACKUP AMP NOT INSTALLED	15	DOOR INTERLOCK FAULT
460044	0	ANNUN 01 TYPE MISMATCH	8	ANNUN 09 TYPE MISMATCH
	1	ANNUN 02 TYPE MISMATCH	9	ANNUN 10 TYPE MISMATCH
	2	ANNUN 03 TYPE MISMATCH	10	ANNUN 11 TYPE MISMATCH
	3	ANNUN 04 TYPE MISMATCH	11	ANNUN 12 TYPE MISMATCH
	4	ANNUN 05 TYPE MISMATCH	12	ANNUN 13 TYPE MISMATCH
	5	ANNUN 06 TYPE MISMATCH	13	ANNUN 14 TYPE MISMATCH
	6	ANNUN 07 TYPE MISMATCH	14	ANNUN 15 TYPE MISMATCH
	7	ANNUN 08 TYPE MISMATCH	15	ANNUN 16 TYPE MISMATCH
460045	0	ANNUN 17 TYPE MISMATCH	8	ANNUN 25 TYPE MISMATCH
	1	ANNUN 18 TYPE MISMATCH	9	ANNUN 26 TYPE MISMATCH
	2	ANNUN 19 TYPE MISMATCH	10	ANNUN 27 TYPE MISMATCH
	3	ANNUN 20 TYPE MISMATCH	11	ANNUN 28 TYPE MISMATCH
	4	ANNUN 21 TYPE MISMATCH	12	ANNUN 29 TYPE MISMATCH
	5	ANNUN 22 TYPE MISMATCH	13	ANNUN 30 TYPE MISMATCH
	6	ANNUN 23 TYPE MISMATCH	14	ANNUN 31 TYPE MISMATCH
	7	ANNUN 24 TYPE MISMATCH	15	ANNUN 32 TYPE MISMATCH
460046	0	DISPLAY COMM LOSS	8	LOOP CARD 1 COMM LOSS
	1	ALARM DEVICES DISABLED	9	LOOP CARD 2 COMM LOSS
	2	SMOKE CONTROL DISABLED	10	LOOP CARD 3 COMM LOSS
	3	PANEL HAS REBOOTED	11	LOOP CARD 4 COMM LOSS
	4	ZONES DISABLED BY BRIGADE	12	LOOP CARD 5 COMM LOSS
	5	ALARM SIGNAL	13	LOOP CARD 6 COMM LOSS
	6	KERNEL CORRUPTED	14	LOOP CARD 7 COMM LOSS
	7	CHANGE SERVICE TOOL PASSWORD	15	LOOP CARD 8 COMM LOSS

Register	Bit No.	System Trouble Name	Bit No.	System Trouble Name
460047	0	LOOP CARD 9 COMM LOSS	8	PMB 4 COMM LOSS
	1	LOOP CARD 10 COMM LOSS	9	PMB 5 COMM LOSS
	2	CHANGE MASTER USER PASSWORD	10	Recovery Partition Application Active
	3	PASSWORD DATABASE CORRUPTED	11	AIO COMM CLASS A TROUBLE
	4	Default database. Please program.	12	AC Failure (LSB is PMB address 1-5)
	5	PMB 1 COMM LOSS	13	Earth Fault (LSB is PMB address 1-5)
	6	PMB 2 COMM LOSS	14	Earth Fault Switch Mismatch (LSB is PMB address 1-5)
	7	PMB 3 COMM LOSS	15	Battery Low (LSB is PMB address 1-5)
460048	0	Battery High (LSB is PMB address 1-5)	8	AIO Address 5 Comm Loss (LSB is 0 for router, 1-15 for peripheral)
	1	Battery Deep-Discharge (LSB is PMB address 1-5)	9	AIO Address 6 Comm Loss (LSB is 0 for router, 1-15 for peripheral)
	2	Charger Fail (LSB is PMB address 1-5)	10	AIO Address 7 Comm Loss (LSB is 0 for router, 1-15 for peripheral)
	3	Power Supply Failure (LSB is PMB address 1-5)	11	AIO Address 8 Comm Loss (LSB is 0 for router, 1-15 for peripheral)
	4	AIO Address 1 Comm Loss (LSB is 0 for router, 1-15 for peripheral)	12	AIO Address 9 Comm Loss (LSB is 0 for router, 1-15 for peripheral)
	5	AIO Address 2 Comm Loss (LSB is 0 for router, 1-15 for peripheral)	13	AIO Address 10 Comm Loss (LSB is 0 for router, 1-15 for peripheral)
	6	AIO Address 3 Comm Loss (LSB is 0 for router, 1-15 for peripheral)	14	(Reserved)
	7	AIO Address 4 Comm Loss (LSB is 0 for router, 1-15 for peripheral)	15	(Reserved)
460049	0	POTS Card No Answer / Missing	8	Ethernet 1 No Connectivity
	1	POTS Line 1 Failure	9	Ethernet 2 No Connectivity
	2	POTS Line 2 Failure	10	CLSS Cloud Communication Failure
	3	POTS Call (Alarm Routing) Failure	11	Ethernet/WiFi Alarm Routing Failure
	4	POTS Software Mismatch	12	Cellular Alarm Routing Failure
	5	Cellular Card No Answer / Missing	13	(Reserved)
	6	Cellular Card No Connectivity	14	(Reserved)
	7	WiFi No Connectivity	15	(Reserved)
460050	0	NAC Key Card Fault 1	8	NAC Key Card Fault 3
	1	NAC Key Card Fault 2	9	NAC Key Card Fault 4
	2	Municipal Circuit Supervision	10	Access Denied
	3	Internal Power Supply Fault	11	Walk Test
	4	Ground Fault Positive	12	POTS Call Secondary Failure
	5	Ground Fault Negative	13	DACT Fault
	6	Auxiliary Trouble 61	14	DACT Timeout 1
	7	24VDC FAULT	15	Access Granted 1

Register	Bit No.	System Trouble Name	Bit No.	System Trouble Name
460051	0	Access Granted 2	8	LCD80 Supervisory 3
	1	Access Granted 3	9	LCD80 Supervisory 4
	2	Access Granted 4	10	LCD80 Supervisory 5
	3	Access Granted 5	11	LCD80 Supervisory 6
	4	Node Missing	12	LCD80 Supervisory 7
	5	Node Extra	13	LCD80 Supervisory 8
	6	LCD80 Supervisory 1	14	LCD80 Supervisory 9
	7	LCD80 Supervisory 2	15	LCD80 Supervisory 10
460052	0	LCD80 Supervisory 11	8	Auxiliary Trouble 35
	1	Auxiliary Trouble 28	9	Auxiliary Trouble 36
	2	Auxiliary Trouble 29	10	Auxiliary Trouble 37
	3	Auxiliary Trouble 30	11	Auxiliary Trouble 38
	4	Auxiliary Trouble 31	12	Auxiliary Trouble 39
	5	Auxiliary Trouble 32	13	Auxiliary Trouble 40
	6	Auxiliary Trouble 33	14	Auxiliary Trouble 41
	7	Auxiliary Trouble 34	15	Auxiliary Trouble 42
460053	0	Auxiliary Trouble 43	8	LCD80 Supervisory 51
	1	LCD80 Supervisory 44	9	LCD80 Supervisory 52
	2	LCD80 Supervisory 45	10	LCD80 Supervisory 53
	3	LCD80 Supervisory 46	11	LCD80 Supervisory 54
	4	LCD80 Supervisory 47	12	LCD80 Supervisory 55
	5	LCD80 Supervisory 48	13	LCD80 Supervisory 56
	6	LCD80 Supervisory 49	14	LCD80 Supervisory 57
	7	LCD80 Supervisory 50	15	LCD80 Supervisory 58
460054	0	LCD80 Supervisory 59	8	Auxiliary Trouble 16
	1	Network Ground Fault	9	Auxiliary Trouble 17
	2	Drill	10	Auxiliary Trouble 18
	3	Communication Error/Transmission Fault	11	Auxiliary Trouble 19
	4	Auxiliary Trouble 12	12	Auxiliary Trouble 20
	5	Auxiliary Trouble 13	13	Auxiliary Trouble 21
	6	Auxiliary Trouble 14	14	Auxiliary Trouble 22
	7	Auxiliary Trouble 15	15	Auxiliary Trouble 23
460055	0	Auxiliary Trouble 24	8	Speaker Circuit Short 5
	1	Auxiliary Trouble 25	9	Speaker Circuit Short 6
	2	Auxiliary Trouble 26	10	Speaker Circuit Short 7
	3	Auxiliary Trouble 27	11	Speaker Circuit Short 8
	4	Speaker Circuit Short 1	12	Speaker Circuit Open 1
	5	Speaker Circuit Short 2	13	Speaker Circuit Open 2
	6	Speaker Circuit Short 3	14	Speaker Circuit Open 3
	7	Speaker Circuit Short 4	15	Speaker Circuit Open 4

Register	Bit No.	System Trouble Name	Bit No.	System Trouble Name
460056	0	Speaker Circuit Open 5	8	Auxiliary Trouble 60
	1	Speaker Circuit Open 6	9	Tornado Alert
	2	Speaker Circuit Open 7	10	SLC! Disconnect
	3	Speaker Circuit Open 8	11	SLC2 Disconnect
	4	Amplifier Failure 1	12	Battery LOW
	5	Amplifier Failure 2	13	STYLE 6 ON LOOP 1
	6	Amplifier Failure 3	14	STYLE 6 ON LOOP 2
	7	Amplifier Failure 4	15	STYLE 6 ON LOOP 4
460057	0	STYLE 6 ON LOOP 5	8	LOSS OF PART LOOP3
	1	STYLE 6 ON LOOP 6	9	LOSS OF PART LOOP4
	2	STYLE 6 ON LOOP 7	10	LOSS OF PART LOOP5
	3	STYLE 6 ON LOOP 8	11	LOSS OF PART LOOP6
	4	STYLE 6 ON LOOP 9	12	LOSS OF PART LOOP7
	5	STYLE 6 ON LOOP 10	13	LOSS OF PART LOOP8
	6	LOSS OF PART LOOP1	14	LOSS OF PART LOOP9
	7	LOSS OF PART LOOP2	15	LOSS OF PART LOOP10
460058	0	LOSS OF ENTIRE LOOP1	8	LOSS OF ENTIRE LOOP9
	1	LOSS OF ENTIRE LOOP2	9	LOSS OF ENTIRE LOOP10
	2	LOSS OF ENTIRE LOOP3	10	HOLD UP ZONE TROUBLE
	3	LOSS OF ENTIRE LOOP4	11	CPU POWER RESTART LOOP1
	4	LOSS OF ENTIRE LOOP5	12	CPU POWER RESTART LOOP2
	5	LOSS OF ENTIRE LOOP6	13	CPU POWER RESTART LOOP3
	6	LOSS OF ENTIRE LOOP7	14	CPU POWER RESTART LOOP4
	7	LOSS OF ENTIRE LOOP8	15	CPU POWER RESTART LOOP5
460059	0	CPU POWER RESTART LOOP6	8	DEVICE ZERO PRESENT LOOP5
	1	CPU POWER RESTART LOOP7	9	DEVICE ZERO PRESENT LOOP6
	2	CPU POWER RESTART LOOP8	10	DEVICE ZERO PRESENT LOOP7
	3	CPU POWER RESTART LOOP9	11	DEVICE ZERO PRESENT LOOP8
	4	CPU POWER RESTART LOOP10	12	DEVICE ZERO PRESENT LOOP9
	5	DEVICE ZERO PRESENT LOOP2	13	DEVICE ZERO PRESENT LOOP10
	6	DEVICE ZERO PRESENT LOOP3	14	RS232 LINK FAULT
	7	DEVICE ZERO PRESENT LOOP4	15	BATTERY LOW VOLTAGE
460060	0	BATTERY FAILURE	8	CLOCK SET TO AFTER AD2099
	1	MAIN CPU WATCHDOG OPERATED	9	AUXILIARY TROUBLE
	2	CPU EPROM CHECKSUM ERROR	10	CONFIGURATION NEEDS EXPANSION
	3	SOFTWARE FAILURE	11	CONFIGURATION NEEDS RS485 CARD
	4	CPU/DISPLAY HARDWARE FAULT	12	EXTERNAL PSU FAULT
	5	SOUNDER CIRCUIT FAULT	13	EXTERNAL PSU LOW SYSTEM VOLTAGE
	6	OUTPUT DIRVER FAULT	14	NETWORK ZONE DUPLICATION
	7	GENERAL FAULT	15	NETWORK DOMAIN RING OR SUBNET LOST

Register	Bit No.	System Trouble Name	Bit No.	System Trouble Name
460061	0	INCOMPATIBLE LOOP1 DEVICE AND LIB	8	INCOMPATIBLE LOOP9 DEVICE AND LIB
	1	INCOMPATIBLE LOOP2 DEVICE AND LIB	9	INCOMPATIBLE LOOP10 DEVICE AND LIB
	2	INCOMPATIBLE LOOP3 DEVICE AND LIB	10	ID2NET PARTIAL OPEN/SHORT CIRCUIT FAULT
	3	INCOMPATIBLE LOOP4 DEVICE AND LIB	11	ID2NET: PHASE REVERSAL FAULT
	4	INCOMPATIBLE LOOP5 DEVICE AND LIB	12	ID2NET: CHANNEL INVERSION FAULT
	5	INCOMPATIBLE LOOP6 DEVICE AND LIB	13	TOO MANY CLIP ADDRESSES
	6	INCOMPATIBLE LOOP7 DEVICE AND LIB	14	SENSOR AT ADDRESS OUT OF RANGE LOOP1
	7	INCOMPATIBLE LOOP8 DEVICE AND LIB	15	SENSOR AT ADDRESS OUT OF RANGE LOOP2
460062	0	SENSOR AT ADDRESS OUT OF RANGE LOOP3	8	NEW AUXILIARY SUPPLY
	1	SENSOR AT ADDRESS OUT OF RANGE LOOP4	9	FAT/FBF MISSING FAULT
	2	SENSOR AT ADDRESS OUT OF RANGE LOOP5	10	ID2NET DUPLICATE NODE
	3	SENSOR AT ADDRESS OUT OF RANGE LOOP6	11	LOOP IN BOOTLOADER 1
	4	SENSOR AT ADDRESS OUT OF RANGE LOOP7	12	LOOP IN BOOTLOADER 2
	5	SENSOR AT ADDRESS OUT OF RANGE LOOP8	13	LOOP IN BOOTLOADER 3
	6	SENSOR AT ADDRESS OUT OF RANGE LOOP9	14	LOOP IN BOOTLOADER 4
	7	SENSOR AT ADDRESS OUT OF RANGE LOOP10	15	LOOP IN BOOTLOADER 5
460063	0	LOOP IN BOOTLOADER 6	8	AIO ADDR 4 ALARM DISCONNECT
	1	LOOP IN BOOTLOADER 7	9	AIO ADDR 5 ALARM DISCONNECT
	2	LOOP IN BOOTLOADER 8	10	AIO ADDR 6 ALARM DISCONNECT
	3	LOOP IN BOOTLOADER 9	11	AIO ADDR 7 ALARM DISCONNECT
	4	LOOP IN BOOTLOADER 10	12	AIO ADDR 8 ALARM DISCONNECT
	5	AIO ADDR 1 ALARM DISCONNECT	13	AIO ADDR 9 ALARM DISCONNECT
	6	AIO ADDR 2 ALARM DISCONNECT	14	AIO ADDR 10 ALARM DISCONNECT
	7	AIO ADDR 3 ALARM DISCONNECT	15	POWER SUPPLY NO SERVICE 1
460064	0	POWER SUPPLY NO SERVICE 2	8	POWER SUPPLY PROGRAM CORRUPT 5
	1	POWER SUPPLY NO SERVICE 3	9	POWER SUPPLY DATABASE CORRUPT 1
	2	POWER SUPPLY NO SERVICE 4	10	POWER SUPPLY DATABASE CORRUPT 2
	3	POWER SUPPLY NO SERVICE 5	11	POWER SUPPLY DATABASE CORRUPT 3
	4	POWER SUPPLY PROGRAM CORRUPT 1	12	POWER SUPPLY DATABASE CORRUPT 4
	5	POWER SUPPLY PROGRAM CORRUPT 2	13	POWER SUPPLY DATABASE CORRUPT 5
	6	POWER SUPPLY PROGRAM CORRUPT 3	14	POWER SUPPLY DATABASE INCOMPATIBLE 1
	7	POWER SUPPLY PROGRAM CORRUPT 4	15	POWER SUPPLY DATABASE INCOMPATIBLE 2

Register	Bit No.	System Trouble Name	Bit No.	System Trouble Name
460065	0	POWER SUPPLY DATABASE INCOMPATIBLE 3	8	LOOP NO DATABASE 6
	1	POWER SUPPLY DATABASE INCOMPATIBLE 4	9	LOOP NO DATABASE 7
	2	POWER SUPPLY DATABASE INCOMPATIBLE 5	10	LOOP NO DATABASE 8
	3	LOOP NO DATABASE 1	11	LOOP NO DATABASE 9
	4	LOOP NO DATABASE 2	12	LOOP NO DATABASE 10
	5	LOOP NO DATABASE 3	13	LOOP DATABASE INCOMPATIBLE 1
	6	LOOP NO DATABASE 4	14	LOOP DATABASE INCOMPATIBLE 2
	7	LOOP NO DATABASE 5	15	LOOP DATABASE INCOMPATIBLE 3
460066	0	LOOP DATABASE INCOMPATIBLE 4	8	RELEASING ZONE LICENSE EXCEEDED
	1	LOOP DATABASE INCOMPATIBLE 5	9	GENERAL ZONE LICENSE EXCEEDED
	2	LOOP DATABASE INCOMPATIBLE 6	10	ZONE CODING LICENSE NOT PRESENT
	3	LOOP DATABASE INCOMPATIBLE 7	11	LOGIC ZONE LICENSE EXCEEDED
	4	LOOP DATABASE INCOMPATIBLE 8	12	NETWORK DISPLAY LICENSE NOT PRESENT
	5	LOOP DATABASE INCOMPATIBLE 9	13	CLIP LICENSE NOT PRESENT
	6	LOOP DATABASE INCOMPATIBLE 10	14	CUSTOM ACTION LICENSE EXCEEDED
	7	Service Mode Enabled	15	ADVANCED LOGIC LICENSE NOT PRESENT
460067	0	WATER RELEASING ZONE LICENSE EXCEEDED	8	AIO ADDR 1 RELAY VOLTAGE FAULT 5
	1	DCC LICENSE NOT PRESENT	9	AIO ADDR 1 RELAY VOLTAGE FAULT 6
	2	GROUND FAULT INDICATION LICENSE NOT PRESENT	10	AIO ADDR 1 RELAY VOLTAGE FAULT 7
	3	AIO ADDR 1 RELAY VOLTAGE FAULT 0	11	AIO ADDR 1 RELAY VOLTAGE FAULT 8
	4	AIO ADDR 1 RELAY VOLTAGE FAULT 1	12	AIO ADDR 1 RELAY VOLTAGE FAULT 9
	5	AIO ADDR 1 RELAY VOLTAGE FAULT 2	13	AIO ADDR 1 RELAY VOLTAGE FAULT 10
	6	AIO ADDR 1 RELAY VOLTAGE FAULT 3	14	AIO ADDR 1 RELAY VOLTAGE FAULT 11
	7	AIO ADDR 1 RELAY VOLTAGE FAULT 4	15	AIO ADDR 1 RELAY VOLTAGE FAULT 12
460068	0	AIO ADDR 1 RELAY VOLTAGE FAULT 13	8	AIO ADDR 2 RELAY VOLTAGE FAULT 5
	1	AIO ADDR 1 RELAY VOLTAGE FAULT 14	9	AIO ADDR 2 RELAY VOLTAGE FAULT 6
	2	AIO ADDR 1 RELAY VOLTAGE FAULT 15	10	AIO ADDR 2 RELAY VOLTAGE FAULT 7
	3	AIO ADDR 2 RELAY VOLTAGE FAULT 0	11	AIO ADDR 2 RELAY VOLTAGE FAULT 8
	4	AIO ADDR 2 RELAY VOLTAGE FAULT 1	12	AIO ADDR 2 RELAY VOLTAGE FAULT 9
	5	AIO ADDR 2 RELAY VOLTAGE FAULT 2	13	AIO ADDR 2 RELAY VOLTAGE FAULT 10
	6	AIO ADDR 2 RELAY VOLTAGE FAULT 3	14	AIO ADDR 2 RELAY VOLTAGE FAULT 11
	7	AIO ADDR 2 RELAY VOLTAGE FAULT 4	15	AIO ADDR 2 RELAY VOLTAGE FAULT 12

Register	Bit No.	System Trouble Name	Bit No.	System Trouble Name
460069	0	AIO ADDR 2 RELAY VOLTAGE FAULT 13	8	AIO ADDR 3 RELAY VOLTAGE FAULT 5
	1	AIO ADDR 2 RELAY VOLTAGE FAULT 14	9	AIO ADDR 3 RELAY VOLTAGE FAULT 6
	2	AIO ADDR 2 RELAY VOLTAGE FAULT 15	10	AIO ADDR 3 RELAY VOLTAGE FAULT 7
	3	AIO ADDR 3 RELAY VOLTAGE FAULT 0	11	AIO ADDR 3 RELAY VOLTAGE FAULT 8
	4	AIO ADDR 3 RELAY VOLTAGE FAULT 1	12	AIO ADDR 3 RELAY VOLTAGE FAULT 9
	5	AIO ADDR 3 RELAY VOLTAGE FAULT 2	13	AIO ADDR 3 RELAY VOLTAGE FAULT 10
	6	AIO ADDR 3 RELAY VOLTAGE FAULT 3	14	AIO ADDR 3 RELAY VOLTAGE FAULT 11
	7	AIO ADDR 3 RELAY VOLTAGE FAULT 4	15	AIO ADDR 3 RELAY VOLTAGE FAULT 12
460070	0	AIO ADDR 3 RELAY VOLTAGE FAULT 13	8	AIO ADDR 4 RELAY VOLTAGE FAULT 5
	1	AIO ADDR 3 RELAY VOLTAGE FAULT 14	9	AIO ADDR 4 RELAY VOLTAGE FAULT 6
	2	AIO ADDR 3 RELAY VOLTAGE FAULT 15	10	AIO ADDR 4 RELAY VOLTAGE FAULT 7
	3	AIO ADDR 4 RELAY VOLTAGE FAULT 0	11	AIO ADDR 4 RELAY VOLTAGE FAULT 8
	4	AIO ADDR 4 RELAY VOLTAGE FAULT 1	12	AIO ADDR 4 RELAY VOLTAGE FAULT 9
	5	AIO ADDR 4 RELAY VOLTAGE FAULT 2	13	AIO ADDR 4 RELAY VOLTAGE FAULT 10
	6	AIO ADDR 4 RELAY VOLTAGE FAULT 3	14	AIO ADDR 4 RELAY VOLTAGE FAULT 11
	7	AIO ADDR 4 RELAY VOLTAGE FAULT 4	15	AIO ADDR 4 RELAY VOLTAGE FAULT 12
460071	0	AIO ADDR 4 RELAY VOLTAGE FAULT 13	8	AIO ADDR 5 RELAY VOLTAGE FAULT 5
	1	AIO ADDR 4 RELAY VOLTAGE FAULT 14	9	AIO ADDR 5 RELAY VOLTAGE FAULT 6
	2	AIO ADDR 4 RELAY VOLTAGE FAULT 15	10	AIO ADDR 5 RELAY VOLTAGE FAULT 7
	3	AIO ADDR 5 RELAY VOLTAGE FAULT 0	11	AIO ADDR 5 RELAY VOLTAGE FAULT 8
	4	AIO ADDR 5 RELAY VOLTAGE FAULT 1	12	AIO ADDR 5 RELAY VOLTAGE FAULT 9
	5	AIO ADDR 5 RELAY VOLTAGE FAULT 2	13	AIO ADDR 5 RELAY VOLTAGE FAULT 10
	6	AIO ADDR 5 RELAY VOLTAGE FAULT 3	14	AIO ADDR 5 RELAY VOLTAGE FAULT 11
	7	AIO ADDR 5 RELAY VOLTAGE FAULT 4	15	AIO ADDR 5 RELAY VOLTAGE FAULT 12
460072	0	AIO ADDR 5 RELAY VOLTAGE FAULT 13	8	AIO ADDR 6 RELAY VOLTAGE FAULT 5
	1	AIO ADDR 5 RELAY VOLTAGE FAULT 14	9	AIO ADDR 6 RELAY VOLTAGE FAULT 6
	2	AIO ADDR 5 RELAY VOLTAGE FAULT 15	10	AIO ADDR 6 RELAY VOLTAGE FAULT 7
	3	AIO ADDR 6 RELAY VOLTAGE FAULT 0	11	AIO ADDR 6 RELAY VOLTAGE FAULT 8
	4	AIO ADDR 6 RELAY VOLTAGE FAULT 1	12	AIO ADDR 6 RELAY VOLTAGE FAULT 9
	5	AIO ADDR 6 RELAY VOLTAGE FAULT 2	13	AIO ADDR 6 RELAY VOLTAGE FAULT 10
	6	AIO ADDR 6 RELAY VOLTAGE FAULT 3	14	AIO ADDR 6 RELAY VOLTAGE FAULT 11
	7	AIO ADDR 6 RELAY VOLTAGE FAULT 4	15	AIO ADDR 6 RELAY VOLTAGE FAULT 12

Register	Bit No.	System Trouble Name	Bit No.	System Trouble Name
460073	0	AIO ADDR 6 RELAY VOLTAGE FAULT 13	8	AIO ADDR 7 RELAY VOLTAGE FAULT 5
	1	AIO ADDR 6 RELAY VOLTAGE FAULT 14	9	AIO ADDR 7 RELAY VOLTAGE FAULT 6
	2	AIO ADDR 6 RELAY VOLTAGE FAULT 15	10	AIO ADDR 7 RELAY VOLTAGE FAULT 7
	3	AIO ADDR 7 RELAY VOLTAGE FAULT 0	11	AIO ADDR 7 RELAY VOLTAGE FAULT 8
	4	AIO ADDR 7 RELAY VOLTAGE FAULT 1	12	AIO ADDR 7 RELAY VOLTAGE FAULT 9
	5	AIO ADDR 7 RELAY VOLTAGE FAULT 2	13	AIO ADDR 7 RELAY VOLTAGE FAULT 10
	6	AIO ADDR 7 RELAY VOLTAGE FAULT 3	14	AIO ADDR 7 RELAY VOLTAGE FAULT 11
	7	AIO ADDR 7 RELAY VOLTAGE FAULT 4	15	AIO ADDR 7 RELAY VOLTAGE FAULT 12
460074	0	AIO ADDR 7 RELAY VOLTAGE FAULT 13	8	AIO ADDR 8 RELAY VOLTAGE FAULT 5
	1	AIO ADDR 7 RELAY VOLTAGE FAULT 14	9	AIO ADDR 8 RELAY VOLTAGE FAULT 6
	2	AIO ADDR 7 RELAY VOLTAGE FAULT 15	10	AIO ADDR 8 RELAY VOLTAGE FAULT 7
	3	AIO ADDR 8 RELAY VOLTAGE FAULT 0	11	AIO ADDR 8 RELAY VOLTAGE FAULT 8
	4	AIO ADDR 8 RELAY VOLTAGE FAULT 1	12	AIO ADDR 8 RELAY VOLTAGE FAULT 9
	5	AIO ADDR 8 RELAY VOLTAGE FAULT 2	13	AIO ADDR 8 RELAY VOLTAGE FAULT 10
	6	AIO ADDR 8 RELAY VOLTAGE FAULT 3	14	AIO ADDR 8 RELAY VOLTAGE FAULT 11
	7	AIO ADDR 8 RELAY VOLTAGE FAULT 4	15	AIO ADDR 8 RELAY VOLTAGE FAULT 12
460075	0	AIO ADDR 8 RELAY VOLTAGE FAULT 13	8	AIO ADDR 9 RELAY VOLTAGE FAULT 5
	1	AIO ADDR 8 RELAY VOLTAGE FAULT 14	9	AIO ADDR 9 RELAY VOLTAGE FAULT 6
	2	AIO ADDR 8 RELAY VOLTAGE FAULT 15	10	AIO ADDR 9 RELAY VOLTAGE FAULT 7
	3	AIO ADDR 9 RELAY VOLTAGE FAULT 0	11	AIO ADDR 9 RELAY VOLTAGE FAULT 8
	4	AIO ADDR 9 RELAY VOLTAGE FAULT 1	12	AIO ADDR 9 RELAY VOLTAGE FAULT 9
	5	AIO ADDR 9 RELAY VOLTAGE FAULT 2	13	AIO ADDR 9 RELAY VOLTAGE FAULT 10
	6	AIO ADDR 9 RELAY VOLTAGE FAULT 3	14	AIO ADDR 9 RELAY VOLTAGE FAULT 11
	7	AIO ADDR 9 RELAY VOLTAGE FAULT 4	15	AIO ADDR 9 RELAY VOLTAGE FAULT 12
460076	0	AIO ADDR 9 RELAY VOLTAGE FAULT 13	8	AIO ADDR 10 RELAY VOLTAGE FAULT 5
	1	AIO ADDR 9 RELAY VOLTAGE FAULT 14	9	AIO ADDR 10 RELAY VOLTAGE FAULT 6
	2	AIO ADDR 9 RELAY VOLTAGE FAULT 15	10	AIO ADDR 10 RELAY VOLTAGE FAULT 7
	3	AIO ADDR 10 RELAY VOLTAGE FAULT 0	11	AIO ADDR 10 RELAY VOLTAGE FAULT 8
	4	AIO ADDR 10 RELAY VOLTAGE FAULT 1	12	AIO ADDR 10 RELAY VOLTAGE FAULT 9
	5	AIO ADDR 10 RELAY VOLTAGE FAULT 2	13	AIO ADDR 10 RELAY VOLTAGE FAULT 10
	6	AIO ADDR 10 RELAY VOLTAGE FAULT 3	14	AIO ADDR 10 RELAY VOLTAGE FAULT 11
	7	AIO ADDR 10 RELAY VOLTAGE FAULT 4	15	AIO ADDR 10 RELAY VOLTAGE FAULT 12

Register	Bit No.	System Trouble Name	Bit No.	System Trouble Name
460077	0	AIO ADDR 10 RELAY VOLTAGE FAULT 13	8	AIO ADDR 1 ISOLATED VOLTAGE FAULT 5
	1	AIO ADDR 10 RELAY VOLTAGE FAULT 14	9	AIO ADDR 1 ISOLATED VOLTAGE FAULT 6
	2	AIO ADDR 10 RELAY VOLTAGE FAULT 15	10	AIO ADDR 1 ISOLATED VOLTAGE FAULT 7
	3	AIO ADDR 1 ISOLATED VOLTAGE FAULT 0	11	AIO ADDR 1 ISOLATED VOLTAGE FAULT 8
	4	AIO ADDR 1 ISOLATED VOLTAGE FAULT 1	12	AIO ADDR 1 ISOLATED VOLTAGE FAULT 9
	5	AIO ADDR 1 ISOLATED VOLTAGE FAULT 2	13	AIO ADDR 1 ISOLATED VOLTAGE FAULT 10
	6	AIO ADDR 1 ISOLATED VOLTAGE FAULT 3	14	AIO ADDR 1 ISOLATED VOLTAGE FAULT 11
	7	AIO ADDR 1 ISOLATED VOLTAGE FAULT 4	15	AIO ADDR 1 ISOLATED VOLTAGE FAULT 12
460078	0	AIO ADDR 1 ISOLATED VOLTAGE FAULT 14	8	AIO ADDR 2 ISOLATED VOLTAGE FAULT 5
	1	AIO ADDR 1 ISOLATED VOLTAGE FAULT 15	9	AIO ADDR 2 ISOLATED VOLTAGE FAULT 6
	2	AIO ADDR 2 ISOLATED VOLTAGE FAULT 0	10	AIO ADDR 2 ISOLATED VOLTAGE FAULT 7
	3	AIO ADDR 2 ISOLATED VOLTAGE FAULT 1	11	AIO ADDR 2 ISOLATED VOLTAGE FAULT 8
	4	AIO ADDR 2 ISOLATED VOLTAGE FAULT 2	12	AIO ADDR 2 ISOLATED VOLTAGE FAULT 9
	5	AIO ADDR 2 ISOLATED VOLTAGE FAULT 3	13	AIO ADDR 2 ISOLATED VOLTAGE FAULT 10
	6	AIO ADDR 2 ISOLATED VOLTAGE FAULT 4	14	AIO ADDR 2 ISOLATED VOLTAGE FAULT 11
	7	AIO ADDR 1 ISOLATED VOLTAGE FAULT 14	15	AIO ADDR 2 ISOLATED VOLTAGE FAULT 12
460079	0	AIO ADDR 2 ISOLATED VOLTAGE FAULT 13	8	AIO ADDR 3 ISOLATED VOLTAGE FAULT 5
	1	AIO ADDR 2 ISOLATED VOLTAGE FAULT 14	9	AIO ADDR 3 ISOLATED VOLTAGE FAULT 6
	2	AIO ADDR 2 ISOLATED VOLTAGE FAULT 15	10	AIO ADDR 3 ISOLATED VOLTAGE FAULT 7
	3	AIO ADDR 3 ISOLATED VOLTAGE FAULT 0	11	AIO ADDR 3 ISOLATED VOLTAGE FAULT 8
	4	AIO ADDR 3 ISOLATED VOLTAGE FAULT 1	12	AIO ADDR 3 ISOLATED VOLTAGE FAULT 9
	5	AIO ADDR 3 ISOLATED VOLTAGE FAULT 2	13	AIO ADDR 3 ISOLATED VOLTAGE FAULT 10
	6	AIO ADDR 3 ISOLATED VOLTAGE FAULT 3	14	AIO ADDR 3 ISOLATED VOLTAGE FAULT 11
	7	AIO ADDR 3 ISOLATED VOLTAGE FAULT 4	15	AIO ADDR 3 ISOLATED VOLTAGE FAULT 12
460080	0	AIO ADDR 3 ISOLATED VOLTAGE FAULT 13	8	AIO ADDR 4 ISOLATED VOLTAGE FAULT 5
	1	AIO ADDR 3 ISOLATED VOLTAGE FAULT 14	9	AIO ADDR 4 ISOLATED VOLTAGE FAULT 6
	2	AIO ADDR 3 ISOLATED VOLTAGE FAULT 15	10	AIO ADDR 4 ISOLATED VOLTAGE FAULT 7
	3	AIO ADDR 4 ISOLATED VOLTAGE FAULT 0	11	AIO ADDR 4 ISOLATED VOLTAGE FAULT 8
	4	AIO ADDR 4 ISOLATED VOLTAGE FAULT 1	12	AIO ADDR 4 ISOLATED VOLTAGE FAULT 9
	5	AIO ADDR 4 ISOLATED VOLTAGE FAULT 2	13	AIO ADDR 4 ISOLATED VOLTAGE FAULT 10
	6	AIO ADDR 4 ISOLATED VOLTAGE FAULT 3	14	AIO ADDR 4 ISOLATED VOLTAGE FAULT 11
	7	AIO ADDR 4 ISOLATED VOLTAGE FAULT 4	15	AIO ADDR 4 ISOLATED VOLTAGE FAULT 12

Register	Bit No.	System Trouble Name	Bit No.	System Trouble Name
460081	0	AIO ADDR 4 ISOLATED VOLTAGE FAULT 13	8	AIO ADDR 5 ISOLATED VOLTAGE FAULT 5
	1	AIO ADDR 4 ISOLATED VOLTAGE FAULT 14	9	AIO ADDR 5 ISOLATED VOLTAGE FAULT 6
	2	AIO ADDR 4 ISOLATED VOLTAGE FAULT 15	10	AIO ADDR 5 ISOLATED VOLTAGE FAULT 7
	3	AIO ADDR 5 ISOLATED VOLTAGE FAULT 0	11	AIO ADDR 5 ISOLATED VOLTAGE FAULT 8
	4	AIO ADDR 5 ISOLATED VOLTAGE FAULT 1	12	AIO ADDR 5 ISOLATED VOLTAGE FAULT 9
	5	AIO ADDR 5 ISOLATED VOLTAGE FAULT 2	13	AIO ADDR 5 ISOLATED VOLTAGE FAULT 10
	6	AIO ADDR 5 ISOLATED VOLTAGE FAULT 3	14	AIO ADDR 5 ISOLATED VOLTAGE FAULT 11
	7	AIO ADDR 5 ISOLATED VOLTAGE FAULT 4	15	AIO ADDR 5 ISOLATED VOLTAGE FAULT 12
460082	0	AIO ADDR 5 ISOLATED VOLTAGE FAULT 13	8	AIO ADDR 6 ISOLATED VOLTAGE FAULT 5
	1	AIO ADDR 5 ISOLATED VOLTAGE FAULT 14	9	AIO ADDR 6 ISOLATED VOLTAGE FAULT 6
	2	AIO ADDR 5 ISOLATED VOLTAGE FAULT 15	10	AIO ADDR 6 ISOLATED VOLTAGE FAULT 7
	3	AIO ADDR 6 ISOLATED VOLTAGE FAULT 0	11	AIO ADDR 6 ISOLATED VOLTAGE FAULT 8
	4	AIO ADDR 6 ISOLATED VOLTAGE FAULT 1	12	AIO ADDR 6 ISOLATED VOLTAGE FAULT 9
	5	AIO ADDR 6 ISOLATED VOLTAGE FAULT 2	13	AIO ADDR 6 ISOLATED VOLTAGE FAULT 10
	6	AIO ADDR 6 ISOLATED VOLTAGE FAULT 3	14	AIO ADDR 6 ISOLATED VOLTAGE FAULT 11
	7	AIO ADDR 6 ISOLATED VOLTAGE FAULT 4	15	AIO ADDR 6 ISOLATED VOLTAGE FAULT 12
460083	0	AIO ADDR 6 ISOLATED VOLTAGE FAULT 13	8	AIO ADDR 7 ISOLATED VOLTAGE FAULT 5
	1	AIO ADDR 6 ISOLATED VOLTAGE FAULT 14	9	AIO ADDR 7 ISOLATED VOLTAGE FAULT 6
	2	AIO ADDR 6 ISOLATED VOLTAGE FAULT 15	10	AIO ADDR 7 ISOLATED VOLTAGE FAULT 7
	3	AIO ADDR 7 ISOLATED VOLTAGE FAULT 0	11	AIO ADDR 7 ISOLATED VOLTAGE FAULT 8
	4	AIO ADDR 7 ISOLATED VOLTAGE FAULT 1	12	AIO ADDR 7 ISOLATED VOLTAGE FAULT 9
	5	AIO ADDR 7 ISOLATED VOLTAGE FAULT 2	13	AIO ADDR 7 ISOLATED VOLTAGE FAULT 10
	6	AIO ADDR 7 ISOLATED VOLTAGE FAULT 3	14	AIO ADDR 7 ISOLATED VOLTAGE FAULT 11
	7	AIO ADDR 7 ISOLATED VOLTAGE FAULT 4	15	AIO ADDR 7 ISOLATED VOLTAGE FAULT 12
460084	0	AIO ADDR 7 ISOLATED VOLTAGE FAULT 13	8	AIO ADDR 8 ISOLATED VOLTAGE FAULT 5
	1	AIO ADDR 7 ISOLATED VOLTAGE FAULT 14	9	AIO ADDR 8 ISOLATED VOLTAGE FAULT 6
	2	AIO ADDR 7 ISOLATED VOLTAGE FAULT 15	10	AIO ADDR 8 ISOLATED VOLTAGE FAULT 7
	3	AIO ADDR 8 ISOLATED VOLTAGE FAULT 0	11	AIO ADDR 8 ISOLATED VOLTAGE FAULT 8
	4	AIO ADDR 8 ISOLATED VOLTAGE FAULT 1	12	AIO ADDR 8 ISOLATED VOLTAGE FAULT 9
	5	AIO ADDR 8 ISOLATED VOLTAGE FAULT 2	13	AIO ADDR 8 ISOLATED VOLTAGE FAULT 10
	6	AIO ADDR 8 ISOLATED VOLTAGE FAULT 3	14	AIO ADDR 8 ISOLATED VOLTAGE FAULT 11
	7	AIO ADDR 8 ISOLATED VOLTAGE FAULT 4	15	AIO ADDR 8 ISOLATED VOLTAGE FAULT 12

Register	Bit No.	System Trouble Name	Bit No.	System Trouble Name
460085	0	AIO ADDR 8 ISOLATED VOLTAGE FAULT 13	8	AIO ADDR 9 ISOLATED VOLTAGE FAULT 5
	1	AIO ADDR 8 ISOLATED VOLTAGE FAULT 14	9	AIO ADDR 9 ISOLATED VOLTAGE FAULT 6
	2	AIO ADDR 8 ISOLATED VOLTAGE FAULT 15	10	AIO ADDR 9 ISOLATED VOLTAGE FAULT 7
	3	AIO ADDR 9 ISOLATED VOLTAGE FAULT 0	11	AIO ADDR 9 ISOLATED VOLTAGE FAULT 8
	4	AIO ADDR 9 ISOLATED VOLTAGE FAULT 1	12	AIO ADDR 9 ISOLATED VOLTAGE FAULT 9
	5	AIO ADDR 9 ISOLATED VOLTAGE FAULT 2	13	AIO ADDR 9 ISOLATED VOLTAGE FAULT 10
	6	AIO ADDR 9 ISOLATED VOLTAGE FAULT 3	14	AIO ADDR 9 ISOLATED VOLTAGE FAULT 11
	7	AIO ADDR 9 ISOLATED VOLTAGE FAULT 4	15	AIO ADDR 9 ISOLATED VOLTAGE FAULT 12
460086	0	AIO ADDR 9 ISOLATED VOLTAGE FAULT 13	8	AIO ADDR 10 ISOLATED VOLTAGE FAULT 5
	1	AIO ADDR 9 ISOLATED VOLTAGE FAULT 14	9	AIO ADDR 10 ISOLATED VOLTAGE FAULT 6
	2	AIO ADDR 9 ISOLATED VOLTAGE FAULT 15	10	AIO ADDR 10 ISOLATED VOLTAGE FAULT 7
	3	AIO ADDR 10 ISOLATED VOLTAGE FAULT 0	11	AIO ADDR 10 ISOLATED VOLTAGE FAULT 8
	4	AIO ADDR 10 ISOLATED VOLTAGE FAULT 1	12	AIO ADDR 10 ISOLATED VOLTAGE FAULT 9
	5	AIO ADDR 10 ISOLATED VOLTAGE FAULT 2	13	AIO ADDR 10 ISOLATED VOLTAGE FAULT 10
	6	AIO ADDR 10 ISOLATED VOLTAGE FAULT 3	14	AIO ADDR 10 ISOLATED VOLTAGE FAULT 11
	7	AIO ADDR 10 ISOLATED VOLTAGE FAULT 4	15	AIO ADDR 10 ISOLATED VOLTAGE FAULT 12
460087	0	AIO ADDR 10 ISOLATED VOLTAGE FAULT 13	8	AIO ADDR 1 HARDWARE FAILURE 5
	1	AIO ADDR 10 ISOLATED VOLTAGE FAULT 14	9	AIO ADDR 1 HARDWARE FAILURE 6
	2	AIO ADDR 10 ISOLATED VOLTAGE FAULT 15	10	AIO ADDR 1 HARDWARE FAILURE 7
	3	AIO ADDR 1 HARDWARE FAILURE 0	11	AIO ADDR 1 HARDWARE FAILURE 8
	4	AIO ADDR 1 HARDWARE FAILURE 1	12	AIO ADDR 1 HARDWARE FAILURE 9
	5	AIO ADDR 1 HARDWARE FAILURE 2	13	AIO ADDR 1 HARDWARE FAILURE 10
	6	AIO ADDR 1 HARDWARE FAILURE 3	14	AIO ADDR 1 HARDWARE FAILURE 11
	7	AIO ADDR 1 HARDWARE FAILURE 4	15	AIO ADDR 1 HARDWARE FAILURE 12
460088	0	AIO ADDR 1 HARDWARE FAILURE 13	8	AIO ADDR 2 HARDWARE FAILURE 5
	1	AIO ADDR 1 HARDWARE FAILURE 14	9	AIO ADDR 2 HARDWARE FAILURE 6
	2	AIO ADDR 1 HARDWARE FAILURE 15	10	AIO ADDR 2 HARDWARE FAILURE 7
	3	AIO ADDR 2 HARDWARE FAILURE 0	11	AIO ADDR 2 HARDWARE FAILURE 8
	4	AIO ADDR 2 HARDWARE FAILURE 1	12	AIO ADDR 2 HARDWARE FAILURE 9
	5	AIO ADDR 2 HARDWARE FAILURE 2	13	AIO ADDR 2 HARDWARE FAILURE 10
	6	AIO ADDR 2 HARDWARE FAILURE 3	14	AIO ADDR 2 HARDWARE FAILURE 11
	7	AIO ADDR 2 HARDWARE FAILURE 4	15	AIO ADDR 2 HARDWARE FAILURE 12

Register	Bit No.	System Trouble Name	Bit No.	System Trouble Name
460089	0	AIO ADDR 2 HARDWARE FAILURE 13	8	AIO ADDR 3 HARDWARE FAILURE 5
	1	AIO ADDR 2 HARDWARE FAILURE 14	9	AIO ADDR 3 HARDWARE FAILURE 6
	2	AIO ADDR 2 HARDWARE FAILURE 15	10	AIO ADDR 3 HARDWARE FAILURE 7
	3	AIO ADDR 3 HARDWARE FAILURE 0	11	AIO ADDR 3 HARDWARE FAILURE 8
	4	AIO ADDR 3 HARDWARE FAILURE 1	12	AIO ADDR 3 HARDWARE FAILURE 9
	5	AIO ADDR 3 HARDWARE FAILURE 2	13	AIO ADDR 3 HARDWARE FAILURE 10
	6	AIO ADDR 3 HARDWARE FAILURE 3	14	AIO ADDR 3 HARDWARE FAILURE 11
	7	AIO ADDR 3 HARDWARE FAILURE 4	15	AIO ADDR 3 HARDWARE FAILURE 12
	0	AIO ADDR 3 HARDWARE FAILURE 13	8	AIO ADDR 4 HARDWARE FAILURE 5
460090	1	AIO ADDR 3 HARDWARE FAILURE 14	9	AIO ADDR 4 HARDWARE FAILURE 6
	2	AIO ADDR 3 HARDWARE FAILURE 15	10	AIO ADDR 4 HARDWARE FAILURE 7
	3	AIO ADDR 4 HARDWARE FAILURE 0	11	AIO ADDR 4 HARDWARE FAILURE 8
	4	AIO ADDR 4 HARDWARE FAILURE 1	12	AIO ADDR 4 HARDWARE FAILURE 9
	5	AIO ADDR 4 HARDWARE FAILURE 2	13	AIO ADDR 4 HARDWARE FAILURE 10
	6	AIO ADDR 4 HARDWARE FAILURE 3	14	AIO ADDR 4 HARDWARE FAILURE 11
	7	AIO ADDR 4 HARDWARE FAILURE 4	15	AIO ADDR 4 HARDWARE FAILURE 12
460091	0	AIO ADDR 4 HARDWARE FAILURE 13	8	AIO ADDR 5 HARDWARE FAILURE 5
	1	AIO ADDR 4 HARDWARE FAILURE 14	9	AIO ADDR 5 HARDWARE FAILURE 6
	2	AIO ADDR 4 HARDWARE FAILURE 15	10	AIO ADDR 5 HARDWARE FAILURE 7
	3	AIO ADDR 5 HARDWARE FAILURE 0	11	AIO ADDR 5 HARDWARE FAILURE 8
	4	AIO ADDR 5 HARDWARE FAILURE 1	12	AIO ADDR 5 HARDWARE FAILURE 9
	5	AIO ADDR 5 HARDWARE FAILURE 2	13	AIO ADDR 5 HARDWARE FAILURE 10
	6	AIO ADDR 5 HARDWARE FAILURE 3	14	AIO ADDR 5 HARDWARE FAILURE 11
	7	AIO ADDR 5 HARDWARE FAILURE 4	15	AIO ADDR 5 HARDWARE FAILURE 12
460092	0	AIO ADDR 5 HARDWARE FAILURE 13	8	AIO ADDR 6 HARDWARE FAILURE 5
	1	AIO ADDR 5 HARDWARE FAILURE 14	9	AIO ADDR 6 HARDWARE FAILURE 6
	2	AIO ADDR 5 HARDWARE FAILURE 15	10	AIO ADDR 6 HARDWARE FAILURE 7
	3	AIO ADDR 6 HARDWARE FAILURE 0	11	AIO ADDR 6 HARDWARE FAILURE 8
	4	AIO ADDR 6 HARDWARE FAILURE 1	12	AIO ADDR 6 HARDWARE FAILURE 9
	5	AIO ADDR 6 HARDWARE FAILURE 2	13	AIO ADDR 6 HARDWARE FAILURE 10
	6	AIO ADDR 6 HARDWARE FAILURE 3	14	AIO ADDR 6 HARDWARE FAILURE 11
	7	AIO ADDR 6 HARDWARE FAILURE 4	15	AIO ADDR 6 HARDWARE FAILURE 12

Register	Bit No.	System Trouble Name	Bit No.	System Trouble Name
460093	0	AIO ADDR 6 HARDWARE FAILURE 13	8	AIO ADDR 7 HARDWARE FAILURE 5
	1	AIO ADDR 6 HARDWARE FAILURE 14	9	AIO ADDR 7 HARDWARE FAILURE 6
	2	AIO ADDR 6 HARDWARE FAILURE 15	10	AIO ADDR 7 HARDWARE FAILURE 7
	3	AIO ADDR 7 HARDWARE FAILURE 0	11	AIO ADDR 7 HARDWARE FAILURE 8
	4	AIO ADDR 7 HARDWARE FAILURE 1	12	AIO ADDR 7 HARDWARE FAILURE 9
	5	AIO ADDR 7 HARDWARE FAILURE 2	13	AIO ADDR 7 HARDWARE FAILURE 10
	6	AIO ADDR 7 HARDWARE FAILURE 3	14	AIO ADDR 7 HARDWARE FAILURE 11
	7	AIO ADDR 7 HARDWARE FAILURE 4	15	AIO ADDR 7 HARDWARE FAILURE 12
460094	0	AIO ADDR 7 HARDWARE FAILURE 13	8	AIO ADDR 8 HARDWARE FAILURE 5
	1	AIO ADDR 7 HARDWARE FAILURE 14	9	AIO ADDR 8 HARDWARE FAILURE 6
	2	AIO ADDR 7 HARDWARE FAILURE 15	10	AIO ADDR 8 HARDWARE FAILURE 7
	3	AIO ADDR 8 HARDWARE FAILURE 0	11	AIO ADDR 8 HARDWARE FAILURE 8
	4	AIO ADDR 8 HARDWARE FAILURE 1	12	AIO ADDR 8 HARDWARE FAILURE 9
	5	AIO ADDR 8 HARDWARE FAILURE 2	13	AIO ADDR 8 HARDWARE FAILURE 10
	6	AIO ADDR 8 HARDWARE FAILURE 3	14	AIO ADDR 8 HARDWARE FAILURE 11
	7	AIO ADDR 8 HARDWARE FAILURE 4	15	AIO ADDR 8 HARDWARE FAILURE 12
460095	0	AIO ADDR 8 HARDWARE FAILURE 13	8	AIO ADDR 9 HARDWARE FAILURE 5
	1	AIO ADDR 8 HARDWARE FAILURE 14	9	AIO ADDR 9 HARDWARE FAILURE 6
	2	AIO ADDR 8 HARDWARE FAILURE 15	10	AIO ADDR 9 HARDWARE FAILURE 7
	3	AIO ADDR 9 HARDWARE FAILURE 0	11	AIO ADDR 9 HARDWARE FAILURE 8
	4	AIO ADDR 9 HARDWARE FAILURE 1	12	AIO ADDR 9 HARDWARE FAILURE 9
	5	AIO ADDR 9 HARDWARE FAILURE 2	13	AIO ADDR 9 HARDWARE FAILURE 10
	6	AIO ADDR 9 HARDWARE FAILURE 3	14	AIO ADDR 9 HARDWARE FAILURE 11
	7	AIO ADDR 9 HARDWARE FAILURE 4	15	AIO ADDR 9 HARDWARE FAILURE 12

Register	Bit No.	System Trouble Name	Bit No.	System Trouble Name
460096	0	AIO ADDR 9 HARDWARE FAILURE 13	8	AIO ADDR 10 HARDWARE FAILURE 5
	1	AIO ADDR 9 HARDWARE FAILURE 14	9	AIO ADDR 10 HARDWARE FAILURE 6
	2	AIO ADDR 9 HARDWARE FAILURE 15	10	AIO ADDR 10 HARDWARE FAILURE 7
	3	AIO ADDR 10 HARDWARE FAILURE 0	11	AIO ADDR 10 HARDWARE FAILURE 8
	4	AIO ADDR 10 HARDWARE FAILURE 1	12	AIO ADDR 10 HARDWARE FAILURE 9
	5	AIO ADDR 10 HARDWARE FAILURE 2	13	AIO ADDR 10 HARDWARE FAILURE 10
	6	AIO ADDR 10 HARDWARE FAILURE 3	14	AIO ADDR 10 HARDWARE FAILURE 11
	7	AIO ADDR 10 HARDWARE FAILURE 4	15	AIO ADDR 10 HARDWARE FAILURE 12
460097	0	AIO ADDR 10 HARDWARE FAILURE 13	8	AIO ADDR 1 EXTRA DEVICE 5
	1	AIO ADDR 10 HARDWARE FAILURE 14	9	AIO ADDR 1 EXTRA DEVICE 6
	2	AIO ADDR 10 HARDWARE FAILURE 15	10	AIO ADDR 1 EXTRA DEVICE 7
	3	AIO ADDR 1 EXTRA DEVICE 0	11	AIO ADDR 1 EXTRA DEVICE 8
	4	AIO ADDR 1 EXTRA DEVICE 1	12	AIO ADDR 1 EXTRA DEVICE 9
	5	AIO ADDR 1 EXTRA DEVICE 2	13	AIO ADDR 1 EXTRA DEVICE 10
	6	AIO ADDR 1 EXTRA DEVICE 3	14	AIO ADDR 1 EXTRA DEVICE 11
	7	AIO ADDR 1 EXTRA DEVICE 4	15	AIO ADDR 1 EXTRA DEVICE 12
460098	0	AIO ADDR 1 EXTRA DEVICE 13	8	AIO ADDR 2 EXTRA DEVICE 5
	1	AIO ADDR 1 EXTRA DEVICE 14	9	AIO ADDR 2 EXTRA DEVICE 6
	2	AIO ADDR 1 EXTRA DEVICE 15	10	AIO ADDR 2 EXTRA DEVICE 7
	3	AIO ADDR 2 EXTRA DEVICE 0	11	AIO ADDR 2 EXTRA DEVICE 8
	4	AIO ADDR 2 EXTRA DEVICE 1	12	AIO ADDR 2 EXTRA DEVICE 9
	5	AIO ADDR 2 EXTRA DEVICE 2	13	AIO ADDR 2 EXTRA DEVICE 10
	6	AIO ADDR 2 EXTRA DEVICE 3	14	AIO ADDR 2 EXTRA DEVICE 11
	7	AIO ADDR 2 EXTRA DEVICE 4	15	AIO ADDR 2 EXTRA DEVICE 12
460099	0	AIO ADDR 2 EXTRA DEVICE 13	8	AIO ADDR 3 EXTRA DEVICE 5
	1	AIO ADDR 2 EXTRA DEVICE 14	9	AIO ADDR 3 EXTRA DEVICE 6
	2	AIO ADDR 2 EXTRA DEVICE 15	10	AIO ADDR 3 EXTRA DEVICE 7
	3	AIO ADDR 3 EXTRA DEVICE 0	11	AIO ADDR 3 EXTRA DEVICE 8
	4	AIO ADDR 3 EXTRA DEVICE 1	12	AIO ADDR 3 EXTRA DEVICE 9
	5	AIO ADDR 3 EXTRA DEVICE 2	13	AIO ADDR 3 EXTRA DEVICE 10
	6	AIO ADDR 3 EXTRA DEVICE 3	14	AIO ADDR 3 EXTRA DEVICE 11
	7	AIO ADDR 3 EXTRA DEVICE 4	15	AIO ADDR 3 EXTRA DEVICE 12

Register	Bit No.	System Trouble Name	Bit No.	System Trouble Name
460100	0	AIO ADDR 3 EXTRA DEVICE 13	8	AIO ADDR 4 EXTRA DEVICE 5
	1	AIO ADDR 3 EXTRA DEVICE 14	9	AIO ADDR 4 EXTRA DEVICE 6
	2	AIO ADDR 3 EXTRA DEVICE 15	10	AIO ADDR 4 EXTRA DEVICE 7
	3	AIO ADDR 4 EXTRA DEVICE 0	11	AIO ADDR 4 EXTRA DEVICE 8
	4	AIO ADDR 4 EXTRA DEVICE 1	12	AIO ADDR 4 EXTRA DEVICE 9
	5	AIO ADDR 4 EXTRA DEVICE 2	13	AIO ADDR 4 EXTRA DEVICE 10
	6	AIO ADDR 4 EXTRA DEVICE 3	14	AIO ADDR 4 EXTRA DEVICE 11
	7	AIO ADDR 4 EXTRA DEVICE 4	15	AIO ADDR 4 EXTRA DEVICE 12
460101	0	AIO ADDR 4 EXTRA DEVICE 13	8	AIO ADDR 5 EXTRA DEVICE 5
	1	AIO ADDR 4 EXTRA DEVICE 14	9	AIO ADDR 5 EXTRA DEVICE 6
	2	AIO ADDR 4 EXTRA DEVICE 15	10	AIO ADDR 5 EXTRA DEVICE 7
	3	AIO ADDR 5 EXTRA DEVICE 0	11	AIO ADDR 5 EXTRA DEVICE 8
	4	AIO ADDR 5 EXTRA DEVICE 1	12	AIO ADDR 5 EXTRA DEVICE 9
	5	AIO ADDR 5 EXTRA DEVICE 2	13	AIO ADDR 5 EXTRA DEVICE 10
	6	AIO ADDR 5 EXTRA DEVICE 3	14	AIO ADDR 5 EXTRA DEVICE 11
	7	AIO ADDR 5 EXTRA DEVICE 4	15	AIO ADDR 5 EXTRA DEVICE 12
460102	0	AIO ADDR 5 EXTRA DEVICE 13	8	AIO ADDR 6 EXTRA DEVICE 5
	1	AIO ADDR 5 EXTRA DEVICE 14	9	AIO ADDR 6 EXTRA DEVICE 6
	2	AIO ADDR 5 EXTRA DEVICE 15	10	AIO ADDR 6 EXTRA DEVICE 7
	3	AIO ADDR 6 EXTRA DEVICE 0	11	AIO ADDR 6 EXTRA DEVICE 8
	4	AIO ADDR 6 EXTRA DEVICE 1	12	AIO ADDR 6 EXTRA DEVICE 9
	5	AIO ADDR 6 EXTRA DEVICE 2	13	AIO ADDR 6 EXTRA DEVICE 10
	6	AIO ADDR 6 EXTRA DEVICE 3	14	AIO ADDR 6 EXTRA DEVICE 11
	7	AIO ADDR 6 EXTRA DEVICE 4	15	AIO ADDR 6 EXTRA DEVICE 12
460103	0	AIO ADDR 6 EXTRA DEVICE 13	8	AIO ADDR 7 EXTRA DEVICE 5
	1	AIO ADDR 6 EXTRA DEVICE 14	9	AIO ADDR 7 EXTRA DEVICE 6
	2	AIO ADDR 6 EXTRA DEVICE 15	10	AIO ADDR 7 EXTRA DEVICE 7
	3	AIO ADDR 7 EXTRA DEVICE 0	11	AIO ADDR 7 EXTRA DEVICE 8
	4	AIO ADDR 7 EXTRA DEVICE 1	12	AIO ADDR 7 EXTRA DEVICE 9
	5	AIO ADDR 7 EXTRA DEVICE 2	13	AIO ADDR 7 EXTRA DEVICE 10
	6	AIO ADDR 7 EXTRA DEVICE 3	14	AIO ADDR 7 EXTRA DEVICE 11
	7	AIO ADDR 7 EXTRA DEVICE 4	15	AIO ADDR 7 EXTRA DEVICE 12

Register	Bit No.	System Trouble Name	Bit No.	System Trouble Name
460104	0	AIO ADDR 7 EXTRA DEVICE 13	8	AIO ADDR 8 EXTRA DEVICE 5
	1	AIO ADDR 7 EXTRA DEVICE 14	9	AIO ADDR 8 EXTRA DEVICE 6
	2	AIO ADDR 7 EXTRA DEVICE 15	10	AIO ADDR 8 EXTRA DEVICE 7
	3	AIO ADDR 8 EXTRA DEVICE 0	11	AIO ADDR 8 EXTRA DEVICE 8
	4	AIO ADDR 8 EXTRA DEVICE 1	12	AIO ADDR 8 EXTRA DEVICE 9
	5	AIO ADDR 8 EXTRA DEVICE 2	13	AIO ADDR 8 EXTRA DEVICE 10
	6	AIO ADDR 8 EXTRA DEVICE 3	14	AIO ADDR 8 EXTRA DEVICE 11
	7	AIO ADDR 8 EXTRA DEVICE 4	15	AIO ADDR 8 EXTRA DEVICE 12
460105	0	AIO ADDR 8 EXTRA DEVICE 13	8	AIO ADDR 9 EXTRA DEVICE 5
	1	AIO ADDR 8 EXTRA DEVICE 14	9	AIO ADDR 9 EXTRA DEVICE 6
	2	AIO ADDR 8 EXTRA DEVICE 15	10	AIO ADDR 9 EXTRA DEVICE 7
	3	AIO ADDR 9 EXTRA DEVICE 0	11	AIO ADDR 9 EXTRA DEVICE 8
	4	AIO ADDR 9 EXTRA DEVICE 1	12	AIO ADDR 9 EXTRA DEVICE 9
	5	AIO ADDR 9 EXTRA DEVICE 2	13	AIO ADDR 9 EXTRA DEVICE 10
	6	AIO ADDR 9 EXTRA DEVICE 3	14	AIO ADDR 9 EXTRA DEVICE 11
	7	AIO ADDR 9 EXTRA DEVICE 4	15	AIO ADDR 9 EXTRA DEVICE 12
460106	0	AIO ADDR 9 EXTRA DEVICE 13	8	AIO ADDR 10 EXTRA DEVICE 5
	1	AIO ADDR 9 EXTRA DEVICE 14	9	AIO ADDR 10 EXTRA DEVICE 6
	2	AIO ADDR 9 EXTRA DEVICE 15	10	AIO ADDR 10 EXTRA DEVICE 7
	3	AIO ADDR 10 EXTRA DEVICE 0	11	AIO ADDR 10 EXTRA DEVICE 8
	4	AIO ADDR 10 EXTRA DEVICE 1	12	AIO ADDR 10 EXTRA DEVICE 9
	5	AIO ADDR 10 EXTRA DEVICE 2	13	AIO ADDR 10 EXTRA DEVICE 10
	6	AIO ADDR 10 EXTRA DEVICE 3	14	AIO ADDR 10 EXTRA DEVICE 11
	7	AIO ADDR 10 EXTRA DEVICE 4	15	AIO ADDR 10 EXTRA DEVICE 12
460107	0	AIO ADDR 10 EXTRA DEVICE 13	8	AIO ADDR 1 MUNICIPAL FAULT 5
	1	AIO ADDR 10 EXTRA DEVICE 14	9	AIO ADDR 1 MUNICIPAL FAULT 6
	2	AIO ADDR 10 EXTRA DEVICE 15	10	AIO ADDR 1 MUNICIPAL FAULT 7
	3	AIO ADDR 1 MUNICIPAL FAULT 0	11	AIO ADDR 1 MUNICIPAL FAULT 8
	4	AIO ADDR 1 MUNICIPAL FAULT 1	12	AIO ADDR 1 MUNICIPAL FAULT 9
	5	AIO ADDR 1 MUNICIPAL FAULT 2	13	AIO ADDR 1 MUNICIPAL FAULT 10
	6	AIO ADDR 1 MUNICIPAL FAULT 3	14	AIO ADDR 1 MUNICIPAL FAULT 11
	7	AIO ADDR 1 MUNICIPAL FAULT 4	15	AIO ADDR 1 MUNICIPAL FAULT 12

Register	Bit No.	System Trouble Name	Bit No.	System Trouble Name
460108	0	AIO ADDR 1 MUNICIPAL FAULT 13	8	AIO ADDR 2 MUNICIPAL FAULT 5
	1	AIO ADDR 1 MUNICIPAL FAULT 14	9	AIO ADDR 2 MUNICIPAL FAULT 6
	2	AIO ADDR 1 MUNICIPAL FAULT 15	10	AIO ADDR 2 MUNICIPAL FAULT 7
	3	AIO ADDR 2 MUNICIPAL FAULT 0	11	AIO ADDR 2 MUNICIPAL FAULT 8
	4	AIO ADDR 2 MUNICIPAL FAULT 1	12	AIO ADDR 2 MUNICIPAL FAULT 9
	5	AIO ADDR 2 MUNICIPAL FAULT 2	13	AIO ADDR 2 MUNICIPAL FAULT 10
	6	AIO ADDR 2 MUNICIPAL FAULT 3	14	AIO ADDR 2 MUNICIPAL FAULT 11
	7	AIO ADDR 2 MUNICIPAL FAULT 4	15	AIO ADDR 2 MUNICIPAL FAULT 12
460109	0	AIO ADDR 2 MUNICIPAL FAULT 13	8	AIO ADDR 3 MUNICIPAL FAULT 5
	1	AIO ADDR 2 MUNICIPAL FAULT 14	9	AIO ADDR 3 MUNICIPAL FAULT 6
	2	AIO ADDR 2 MUNICIPAL FAULT 15	10	AIO ADDR 3 MUNICIPAL FAULT 7
	3	AIO ADDR 3 MUNICIPAL FAULT 0	11	AIO ADDR 3 MUNICIPAL FAULT 8
	4	AIO ADDR 3 MUNICIPAL FAULT 1	12	AIO ADDR 3 MUNICIPAL FAULT 9
	5	AIO ADDR 3 MUNICIPAL FAULT 2	13	AIO ADDR 3 MUNICIPAL FAULT 10
	6	AIO ADDR 3 MUNICIPAL FAULT 3	14	AIO ADDR 3 MUNICIPAL FAULT 11
	7	AIO ADDR 3 MUNICIPAL FAULT 4	15	AIO ADDR 3 MUNICIPAL FAULT 12
460110	0	AIO ADDR 3 MUNICIPAL FAULT 13	8	AIO ADDR 4 MUNICIPAL FAULT 5
	1	AIO ADDR 3 MUNICIPAL FAULT 14	9	AIO ADDR 4 MUNICIPAL FAULT 6
	2	AIO ADDR 3 MUNICIPAL FAULT 15	10	AIO ADDR 4 MUNICIPAL FAULT 7
	3	AIO ADDR 4 MUNICIPAL FAULT 0	11	AIO ADDR 4 MUNICIPAL FAULT 8
	4	AIO ADDR 4 MUNICIPAL FAULT 1	12	AIO ADDR 4 MUNICIPAL FAULT 9
	5	AIO ADDR 4 MUNICIPAL FAULT 2	13	AIO ADDR 4 MUNICIPAL FAULT 10
	6	AIO ADDR 4 MUNICIPAL FAULT 3	14	AIO ADDR 4 MUNICIPAL FAULT 11
	7	AIO ADDR 4 MUNICIPAL FAULT 4	15	AIO ADDR 4 MUNICIPAL FAULT 12
460111	0	AIO ADDR 4 MUNICIPAL FAULT 13	8	AIO ADDR 5 MUNICIPAL FAULT 5
	1	AIO ADDR 4 MUNICIPAL FAULT 14	9	AIO ADDR 5 MUNICIPAL FAULT 6
	2	AIO ADDR 4 MUNICIPAL FAULT 15	10	AIO ADDR 5 MUNICIPAL FAULT 7
	3	AIO ADDR 5 MUNICIPAL FAULT 0	11	AIO ADDR 5 MUNICIPAL FAULT 8
	4	AIO ADDR 5 MUNICIPAL FAULT 1	12	AIO ADDR 5 MUNICIPAL FAULT 9
	5	AIO ADDR 5 MUNICIPAL FAULT 2	13	AIO ADDR 5 MUNICIPAL FAULT 10
	6	AIO ADDR 5 MUNICIPAL FAULT 3	14	AIO ADDR 5 MUNICIPAL FAULT 11
	7	AIO ADDR 5 MUNICIPAL FAULT 4	15	AIO ADDR 5 MUNICIPAL FAULT 12

Register	Bit No.	System Trouble Name	Bit No.	System Trouble Name
460112	0	AIO ADDR 5 MUNICIPAL FAULT 13	8	AIO ADDR 6 MUNICIPAL FAULT 5
	1	AIO ADDR 5 MUNICIPAL FAULT 14	9	AIO ADDR 6 MUNICIPAL FAULT 6
	2	AIO ADDR 5 MUNICIPAL FAULT 15	10	AIO ADDR 6 MUNICIPAL FAULT 7
	3	AIO ADDR 6 MUNICIPAL FAULT 0	11	AIO ADDR 6 MUNICIPAL FAULT 8
	4	AIO ADDR 6 MUNICIPAL FAULT 1	12	AIO ADDR 6 MUNICIPAL FAULT 9
	5	AIO ADDR 6 MUNICIPAL FAULT 2	13	AIO ADDR 6 MUNICIPAL FAULT 10
	6	AIO ADDR 6 MUNICIPAL FAULT 3	14	AIO ADDR 6 MUNICIPAL FAULT 11
	7	AIO ADDR 6 MUNICIPAL FAULT 4	15	AIO ADDR 6 MUNICIPAL FAULT 12
460113	0	AIO ADDR 6 MUNICIPAL FAULT 13	8	AIO ADDR 7 MUNICIPAL FAULT 5
	1	AIO ADDR 6 MUNICIPAL FAULT 14	9	AIO ADDR 7 MUNICIPAL FAULT 6
	2	AIO ADDR 6 MUNICIPAL FAULT 15	10	AIO ADDR 7 MUNICIPAL FAULT 7
	3	AIO ADDR 7 MUNICIPAL FAULT 0	11	AIO ADDR 7 MUNICIPAL FAULT 8
	4	AIO ADDR 7 MUNICIPAL FAULT 1	12	AIO ADDR 7 MUNICIPAL FAULT 9
	5	AIO ADDR 7 MUNICIPAL FAULT 2	13	AIO ADDR 7 MUNICIPAL FAULT 10
	6	AIO ADDR 7 MUNICIPAL FAULT 3	14	AIO ADDR 7 MUNICIPAL FAULT 11
	7	AIO ADDR 7 MUNICIPAL FAULT 4	15	AIO ADDR 7 MUNICIPAL FAULT 12
460114	0	AIO ADDR 7 MUNICIPAL FAULT 13	8	AIO ADDR 8 MUNICIPAL FAULT 5
	1	AIO ADDR 7 MUNICIPAL FAULT 14	9	AIO ADDR 8 MUNICIPAL FAULT 6
	2	AIO ADDR 7 MUNICIPAL FAULT 15	10	AIO ADDR 8 MUNICIPAL FAULT 7
	3	AIO ADDR 8 MUNICIPAL FAULT 0	11	AIO ADDR 8 MUNICIPAL FAULT 8
	4	AIO ADDR 8 MUNICIPAL FAULT 1	12	AIO ADDR 8 MUNICIPAL FAULT 9
	5	AIO ADDR 8 MUNICIPAL FAULT 2	13	AIO ADDR 8 MUNICIPAL FAULT 10
	6	AIO ADDR 8 MUNICIPAL FAULT 3	14	AIO ADDR 8 MUNICIPAL FAULT 11
	7	AIO ADDR 8 MUNICIPAL FAULT 4	15	AIO ADDR 8 MUNICIPAL FAULT 12
460115	0	AIO ADDR 8 MUNICIPAL FAULT 13	8	AIO ADDR 9 MUNICIPAL FAULT 5
	1	AIO ADDR 8 MUNICIPAL FAULT 14	9	AIO ADDR 9 MUNICIPAL FAULT 6
	2	AIO ADDR 8 MUNICIPAL FAULT 15	10	AIO ADDR 9 MUNICIPAL FAULT 7
	3	AIO ADDR 9 MUNICIPAL FAULT 0	11	AIO ADDR 9 MUNICIPAL FAULT 8
	4	AIO ADDR 9 MUNICIPAL FAULT 1	12	AIO ADDR 9 MUNICIPAL FAULT 9
	5	AIO ADDR 9 MUNICIPAL FAULT 2	13	AIO ADDR 9 MUNICIPAL FAULT 10
	6	AIO ADDR 9 MUNICIPAL FAULT 3	14	AIO ADDR 9 MUNICIPAL FAULT 11
	7	AIO ADDR 9 MUNICIPAL FAULT 4	15	AIO ADDR 9 MUNICIPAL FAULT 12

Register	Bit No.	System Trouble Name	Bit No.	System Trouble Name
460116	0	AIO ADDR 9 MUNICIPAL FAULT 13	8	AIO ADDR 10 MUNICIPAL FAULT 5
	1	AIO ADDR 9 MUNICIPAL FAULT 14	9	AIO ADDR 10 MUNICIPAL FAULT 6
	2	AIO ADDR 9 MUNICIPAL FAULT 15	10	AIO ADDR 10 MUNICIPAL FAULT 7
	3	AIO ADDR 10 MUNICIPAL FAULT 0	11	AIO ADDR 10 MUNICIPAL FAULT 8
	4	AIO ADDR 10 MUNICIPAL FAULT 1	12	AIO ADDR 10 MUNICIPAL FAULT 9
	5	AIO ADDR 10 MUNICIPAL FAULT 2	13	AIO ADDR 10 MUNICIPAL FAULT 10
	6	AIO ADDR 10 MUNICIPAL FAULT 3	14	AIO ADDR 10 MUNICIPAL FAULT 11
	7	AIO ADDR 10 MUNICIPAL FAULT 4	15	AIO ADDR 10 MUNICIPAL FAULT 12
460117	0	AIO ADDR 10 MUNICIPAL FAULT 13	8	AIO ADDR 1 BUZZER SUPERVISORY 5
	1	AIO ADDR 10 MUNICIPAL FAULT 14	9	AIO ADDR 1 BUZZER SUPERVISORY 6
	2	AIO ADDR 10 MUNICIPAL FAULT 15	10	AIO ADDR 1 BUZZER SUPERVISORY 7
	3	AIO ADDR 1 BUZZER SUPERVISORY 0	11	AIO ADDR 1 BUZZER SUPERVISORY 8
	4	AIO ADDR 1 BUZZER SUPERVISORY 1	12	AIO ADDR 1 BUZZER SUPERVISORY 9
	5	AIO ADDR 1 BUZZER SUPERVISORY 2	13	AIO ADDR 1 BUZZER SUPERVISORY 10
	6	AIO ADDR 1 BUZZER SUPERVISORY 3	14	AIO ADDR 1 BUZZER SUPERVISORY 11
	7	AIO ADDR 1 BUZZER SUPERVISORY 4	15	AIO ADDR 1 BUZZER SUPERVISORY 12
460118	0	AIO ADDR 1 BUZZER SUPERVISORY 13	8	AIO ADDR 2 BUZZER SUPERVISORY 5
	1	AIO ADDR 1 BUZZER SUPERVISORY 14	9	AIO ADDR 2 BUZZER SUPERVISORY 6
	2	AIO ADDR 1 BUZZER SUPERVISORY 15	10	AIO ADDR 2 BUZZER SUPERVISORY 7
	3	AIO ADDR 2 BUZZER SUPERVISORY 0	11	AIO ADDR 2 BUZZER SUPERVISORY 8
	4	AIO ADDR 2 BUZZER SUPERVISORY 1	12	AIO ADDR 2 BUZZER SUPERVISORY 9
	5	AIO ADDR 2 BUZZER SUPERVISORY 2	13	AIO ADDR 2 BUZZER SUPERVISORY 10
	6	AIO ADDR 2 BUZZER SUPERVISORY 3	14	AIO ADDR 2 BUZZER SUPERVISORY 11
	7	AIO ADDR 2 BUZZER SUPERVISORY 4	15	AIO ADDR 2 BUZZER SUPERVISORY 12
460119	0	AIO ADDR 2 BUZZER SUPERVISORY 13	8	AIO ADDR 3 BUZZER SUPERVISORY 5
	1	AIO ADDR 2 BUZZER SUPERVISORY 14	9	AIO ADDR 3 BUZZER SUPERVISORY 6
	2	AIO ADDR 2 BUZZER SUPERVISORY 15	10	AIO ADDR 3 BUZZER SUPERVISORY 7
	3	AIO ADDR 3 BUZZER SUPERVISORY 0	11	AIO ADDR 3 BUZZER SUPERVISORY 8
	4	AIO ADDR 3 BUZZER SUPERVISORY 1	12	AIO ADDR 3 BUZZER SUPERVISORY 9
	5	AIO ADDR 3 BUZZER SUPERVISORY 2	13	AIO ADDR 3 BUZZER SUPERVISORY 10
	6	AIO ADDR 3 BUZZER SUPERVISORY 3	14	AIO ADDR 3 BUZZER SUPERVISORY 11
	7	AIO ADDR 3 BUZZER SUPERVISORY 4	15	AIO ADDR 3 BUZZER SUPERVISORY 12

Register	Bit No.	System Trouble Name	Bit No.	System Trouble Name
460120	0	AIO ADDR 3 BUZZER SUPERVISORY 13	8	AIO ADDR 4 BUZZER SUPERVISORY 5
	1	AIO ADDR 3 BUZZER SUPERVISORY 14	9	AIO ADDR 4 BUZZER SUPERVISORY 6
	2	AIO ADDR 3 BUZZER SUPERVISORY 15	10	AIO ADDR 4 BUZZER SUPERVISORY 7
	3	AIO ADDR 4 BUZZER SUPERVISORY 0	11	AIO ADDR 4 BUZZER SUPERVISORY 8
	4	AIO ADDR 4 BUZZER SUPERVISORY 1	12	AIO ADDR 4 BUZZER SUPERVISORY 9
	5	AIO ADDR 4 BUZZER SUPERVISORY 2	13	AIO ADDR 4 BUZZER SUPERVISORY 10
	6	AIO ADDR 4 BUZZER SUPERVISORY 3	14	AIO ADDR 4 BUZZER SUPERVISORY 11
	7	AIO ADDR 4 BUZZER SUPERVISORY 4	15	AIO ADDR 4 BUZZER SUPERVISORY 12
460121	0	AIO ADDR 4 BUZZER SUPERVISORY 13	8	AIO ADDR 5 BUZZER SUPERVISORY 5
	1	AIO ADDR 4 BUZZER SUPERVISORY 14	9	AIO ADDR 5 BUZZER SUPERVISORY 6
	2	AIO ADDR 4 BUZZER SUPERVISORY 15	10	AIO ADDR 5 BUZZER SUPERVISORY 7
	3	AIO ADDR 5 BUZZER SUPERVISORY 0	11	AIO ADDR 5 BUZZER SUPERVISORY 8
	4	AIO ADDR 5 BUZZER SUPERVISORY 1	12	AIO ADDR 5 BUZZER SUPERVISORY 9
	5	AIO ADDR 5 BUZZER SUPERVISORY 2	13	AIO ADDR 5 BUZZER SUPERVISORY 10
	6	AIO ADDR 5 BUZZER SUPERVISORY 3	14	AIO ADDR 5 BUZZER SUPERVISORY 11
	7	AIO ADDR 5 BUZZER SUPERVISORY 4	15	AIO ADDR 5 BUZZER SUPERVISORY 12
460122	0	AIO ADDR 5 BUZZER SUPERVISORY 13	8	AIO ADDR 6 BUZZER SUPERVISORY 5
	1	AIO ADDR 5 BUZZER SUPERVISORY 14	9	AIO ADDR 6 BUZZER SUPERVISORY 6
	2	AIO ADDR 5 BUZZER SUPERVISORY 15	10	AIO ADDR 6 BUZZER SUPERVISORY 7
	3	AIO ADDR 6 BUZZER SUPERVISORY 0	11	AIO ADDR 6 BUZZER SUPERVISORY 8
	4	AIO ADDR 6 BUZZER SUPERVISORY 1	12	AIO ADDR 6 BUZZER SUPERVISORY 9
	5	AIO ADDR 6 BUZZER SUPERVISORY 2	13	AIO ADDR 6 BUZZER SUPERVISORY 10
	6	AIO ADDR 6 BUZZER SUPERVISORY 3	14	AIO ADDR 6 BUZZER SUPERVISORY 11
	7	AIO ADDR 6 BUZZER SUPERVISORY 4	15	AIO ADDR 6 BUZZER SUPERVISORY 12
460123	0	AIO ADDR 6 BUZZER SUPERVISORY 13	8	AIO ADDR 7 BUZZER SUPERVISORY 5
	1	AIO ADDR 6 BUZZER SUPERVISORY 14	9	AIO ADDR 7 BUZZER SUPERVISORY 6
	2	AIO ADDR 6 BUZZER SUPERVISORY 15	10	AIO ADDR 7 BUZZER SUPERVISORY 7
	3	AIO ADDR 7 BUZZER SUPERVISORY 0	11	AIO ADDR 7 BUZZER SUPERVISORY 8
	4	AIO ADDR 7 BUZZER SUPERVISORY 1	12	AIO ADDR 7 BUZZER SUPERVISORY 9
	5	AIO ADDR 7 BUZZER SUPERVISORY 2	13	AIO ADDR 7 BUZZER SUPERVISORY 10
	6	AIO ADDR 7 BUZZER SUPERVISORY 3	14	AIO ADDR 7 BUZZER SUPERVISORY 11
	7	AIO ADDR 7 BUZZER SUPERVISORY 4	15	AIO ADDR 7 BUZZER SUPERVISORY 12

Register	Bit No.	System Trouble Name	Bit No.	System Trouble Name
460124	0	AIO ADDR 7 BUZZER SUPERVISORY 13	8	AIO ADDR 8 BUZZER SUPERVISORY 5
	1	AIO ADDR 7 BUZZER SUPERVISORY 14	9	AIO ADDR 8 BUZZER SUPERVISORY 6
	2	AIO ADDR 7 BUZZER SUPERVISORY 15	10	AIO ADDR 8 BUZZER SUPERVISORY 7
	3	AIO ADDR 8 BUZZER SUPERVISORY 0	11	AIO ADDR 8 BUZZER SUPERVISORY 8
	4	AIO ADDR 8 BUZZER SUPERVISORY 1	12	AIO ADDR 8 BUZZER SUPERVISORY 9
	5	AIO ADDR 8 BUZZER SUPERVISORY 2	13	AIO ADDR 8 BUZZER SUPERVISORY 10
	6	AIO ADDR 8 BUZZER SUPERVISORY 3	14	AIO ADDR 8 BUZZER SUPERVISORY 11
	7	AIO ADDR 8 BUZZER SUPERVISORY 4	15	AIO ADDR 8 BUZZER SUPERVISORY 12
460125	0	AIO ADDR 8 BUZZER SUPERVISORY 13	8	AIO ADDR 9 BUZZER SUPERVISORY 5
	1	AIO ADDR 8 BUZZER SUPERVISORY 14	9	AIO ADDR 9 BUZZER SUPERVISORY 6
	2	AIO ADDR 8 BUZZER SUPERVISORY 15	10	AIO ADDR 9 BUZZER SUPERVISORY 7
	3	AIO ADDR 9 BUZZER SUPERVISORY 0	11	AIO ADDR 9 BUZZER SUPERVISORY 8
	4	AIO ADDR 9 BUZZER SUPERVISORY 1	12	AIO ADDR 9 BUZZER SUPERVISORY 9
	5	AIO ADDR 9 BUZZER SUPERVISORY 2	13	AIO ADDR 9 BUZZER SUPERVISORY 10
	6	AIO ADDR 9 BUZZER SUPERVISORY 3	14	AIO ADDR 9 BUZZER SUPERVISORY 11
	7	AIO ADDR 9 BUZZER SUPERVISORY 4	15	AIO ADDR 9 BUZZER SUPERVISORY 12
460126	0	AIO ADDR 9 BUZZER SUPERVISORY 13	8	AIO ADDR 10 BUZZER SUPERVISORY 5
	1	AIO ADDR 9 BUZZER SUPERVISORY 14	9	AIO ADDR 10 BUZZER SUPERVISORY 6
	2	AIO ADDR 9 BUZZER SUPERVISORY 15	10	AIO ADDR 10 BUZZER SUPERVISORY 7
	3	AIO ADDR 10 BUZZER SUPERVISORY 0	11	AIO ADDR 10 BUZZER SUPERVISORY 8
	4	AIO ADDR 10 BUZZER SUPERVISORY 1	12	AIO ADDR 10 BUZZER SUPERVISORY 9
	5	AIO ADDR 10 BUZZER SUPERVISORY 2	13	AIO ADDR 10 BUZZER SUPERVISORY 10
	6	AIO ADDR 10 BUZZER SUPERVISORY 3	14	AIO ADDR 10 BUZZER SUPERVISORY 11
	7	AIO ADDR 10 BUZZER SUPERVISORY 4	15	AIO ADDR 10 BUZZER SUPERVISORY 12
460127	0	AIO ADDR 10 BUZZER SUPERVISORY 13	8	AIO ADDR 1 HARDWARE MISMATCH 5
	1	AIO ADDR 10 BUZZER SUPERVISORY 14	9	AIO ADDR 1 HARDWARE MISMATCH 6
	2	AIO ADDR 10 BUZZER SUPERVISORY 15	10	AIO ADDR 1 HARDWARE MISMATCH 7
	3	AIO ADDR 1 HARDWARE MISMATCH 0	11	AIO ADDR 1 HARDWARE MISMATCH 8
	4	AIO ADDR 1 HARDWARE MISMATCH 1	12	AIO ADDR 1 HARDWARE MISMATCH 9
	5	AIO ADDR 1 HARDWARE MISMATCH 2	13	AIO ADDR 1 HARDWARE MISMATCH 10
	6	AIO ADDR 1 HARDWARE MISMATCH 3	14	AIO ADDR 1 HARDWARE MISMATCH 11
	7	AIO ADDR 1 HARDWARE MISMATCH 4	15	AIO ADDR 1 HARDWARE MISMATCH 12
	0	AIO ADDR 1 HARDWARE MISMATCH 13	8	AIO ADDR 2 HARDWARE MISMATCH 5
	1	AIO ADDR 1 HARDWARE MISMATCH 14	9	AIO ADDR 2 HARDWARE MISMATCH 6
	2	AIO ADDR 1 HARDWARE MISMATCH 15	10	AIO ADDR 2 HARDWARE MISMATCH 7

Register	Bit No.	System Trouble Name	Bit No.	System Trouble Name
460128	3	AIO ADDR 2 HARDWARE MISMATCH 0	11	AIO ADDR 2 HARDWARE MISMATCH 8
	4	AIO ADDR 2 HARDWARE MISMATCH 1	12	AIO ADDR 2 HARDWARE MISMATCH 9
	5	AIO ADDR 2 HARDWARE MISMATCH 2	13	AIO ADDR 2 HARDWARE MISMATCH 10
	6	AIO ADDR 2 HARDWARE MISMATCH 3	14	AIO ADDR 2 HARDWARE MISMATCH 11
	7	AIO ADDR 2 HARDWARE MISMATCH 4	15	AIO ADDR 2 HARDWARE MISMATCH 12
460129	0	AIO ADDR 2 HARDWARE MISMATCH 13	8	AIO ADDR 3 HARDWARE MISMATCH 5
	1	AIO ADDR 2 HARDWARE MISMATCH 14	9	AIO ADDR 3 HARDWARE MISMATCH 6
	2	AIO ADDR 2 HARDWARE MISMATCH 15	10	AIO ADDR 3 HARDWARE MISMATCH 7
	3	AIO ADDR 3 HARDWARE MISMATCH 0	11	AIO ADDR 3 HARDWARE MISMATCH 8
	4	AIO ADDR 3 HARDWARE MISMATCH 1	12	AIO ADDR 3 HARDWARE MISMATCH 9
	5	AIO ADDR 3 HARDWARE MISMATCH 2	13	AIO ADDR 3 HARDWARE MISMATCH 10
	6	AIO ADDR 3 HARDWARE MISMATCH 3	14	AIO ADDR 3 HARDWARE MISMATCH 11
	7	AIO ADDR 3 HARDWARE MISMATCH 4	15	AIO ADDR 3 HARDWARE MISMATCH 12
460130	0	AIO ADDR 3 HARDWARE MISMATCH 13	8	AIO ADDR 4 HARDWARE MISMATCH 5
	1	AIO ADDR 3 HARDWARE MISMATCH 14	9	AIO ADDR 4 HARDWARE MISMATCH 6
	2	AIO ADDR 3 HARDWARE MISMATCH 15	10	AIO ADDR 4 HARDWARE MISMATCH 7
	3	AIO ADDR 4 HARDWARE MISMATCH 0	11	AIO ADDR 4 HARDWARE MISMATCH 8
	4	AIO ADDR 4 HARDWARE MISMATCH 1	12	AIO ADDR 4 HARDWARE MISMATCH 9
	5	AIO ADDR 4 HARDWARE MISMATCH 2	13	AIO ADDR 4 HARDWARE MISMATCH 10
	6	AIO ADDR 4 HARDWARE MISMATCH 3	14	AIO ADDR 4 HARDWARE MISMATCH 11
	7	AIO ADDR 4 HARDWARE MISMATCH 4	15	AIO ADDR 4 HARDWARE MISMATCH 12
460131	0	AIO ADDR 4 HARDWARE MISMATCH 13	8	AIO ADDR 5 HARDWARE MISMATCH 5
	1	AIO ADDR 4 HARDWARE MISMATCH 14	9	AIO ADDR 5 HARDWARE MISMATCH 6
	2	AIO ADDR 4 HARDWARE MISMATCH 15	10	AIO ADDR 5 HARDWARE MISMATCH 7
	3	AIO ADDR 5 HARDWARE MISMATCH 0	11	AIO ADDR 5 HARDWARE MISMATCH 8
	4	AIO ADDR 5 HARDWARE MISMATCH 1	12	AIO ADDR 5 HARDWARE MISMATCH 9
	5	AIO ADDR 5 HARDWARE MISMATCH 2	13	AIO ADDR 5 HARDWARE MISMATCH 10
	6	AIO ADDR 5 HARDWARE MISMATCH 3	14	AIO ADDR 5 HARDWARE MISMATCH 11
	7	AIO ADDR 5 HARDWARE MISMATCH 4	15	AIO ADDR 5 HARDWARE MISMATCH 12

Register	Bit No.	System Trouble Name	Bit No.	System Trouble Name
460132	0	AIO ADDR 5 HARDWARE MISMATCH 13	8	AIO ADDR 6 HARDWARE MISMATCH 5
	1	AIO ADDR 5 HARDWARE MISMATCH 14	9	AIO ADDR 6 HARDWARE MISMATCH 6
	2	AIO ADDR 5 HARDWARE MISMATCH 15	10	AIO ADDR 6 HARDWARE MISMATCH 7
	3	AIO ADDR 6 HARDWARE MISMATCH 0	11	AIO ADDR 6 HARDWARE MISMATCH 8
	4	AIO ADDR 6 HARDWARE MISMATCH 1	12	AIO ADDR 6 HARDWARE MISMATCH 9
	5	AIO ADDR 6 HARDWARE MISMATCH 2	13	AIO ADDR 6 HARDWARE MISMATCH 10
	6	AIO ADDR 6 HARDWARE MISMATCH 3	14	AIO ADDR 6 HARDWARE MISMATCH 11
	7	AIO ADDR 6 HARDWARE MISMATCH 4	15	AIO ADDR 6 HARDWARE MISMATCH 12
460133	0	AIO ADDR 6 HARDWARE MISMATCH 13	8	AIO ADDR 7 HARDWARE MISMATCH 5
	1	AIO ADDR 6 HARDWARE MISMATCH 14	9	AIO ADDR 7 HARDWARE MISMATCH 6
	2	AIO ADDR 6 HARDWARE MISMATCH 15	10	AIO ADDR 7 HARDWARE MISMATCH 7
	3	AIO ADDR 7 HARDWARE MISMATCH 0	11	AIO ADDR 7 HARDWARE MISMATCH 8
	4	AIO ADDR 7 HARDWARE MISMATCH 1	12	AIO ADDR 7 HARDWARE MISMATCH 9
	5	AIO ADDR 7 HARDWARE MISMATCH 2	13	AIO ADDR 7 HARDWARE MISMATCH 10
	6	AIO ADDR 7 HARDWARE MISMATCH 3	14	AIO ADDR 7 HARDWARE MISMATCH 11
	7	AIO ADDR 7 HARDWARE MISMATCH 4	15	AIO ADDR 7 HARDWARE MISMATCH 12
460134	0	AIO ADDR 7 HARDWARE MISMATCH 13	8	AIO ADDR 8 HARDWARE MISMATCH 5
	1	AIO ADDR 7 HARDWARE MISMATCH 14	9	AIO ADDR 8 HARDWARE MISMATCH 6
	2	AIO ADDR 7 HARDWARE MISMATCH 15	10	AIO ADDR 8 HARDWARE MISMATCH 7
	3	AIO ADDR 8 HARDWARE MISMATCH 0	11	AIO ADDR 8 HARDWARE MISMATCH 8
	4	AIO ADDR 8 HARDWARE MISMATCH 1	12	AIO ADDR 8 HARDWARE MISMATCH 9
	5	AIO ADDR 8 HARDWARE MISMATCH 2	13	AIO ADDR 8 HARDWARE MISMATCH 10
	6	AIO ADDR 8 HARDWARE MISMATCH 3	14	AIO ADDR 8 HARDWARE MISMATCH 11
	7	AIO ADDR 8 HARDWARE MISMATCH 4	15	AIO ADDR 8 HARDWARE MISMATCH 12
460135	0	AIO ADDR 8 HARDWARE MISMATCH 13	8	AIO ADDR 9 HARDWARE MISMATCH 5
	1	AIO ADDR 8 HARDWARE MISMATCH 14	9	AIO ADDR 9 HARDWARE MISMATCH 6
	2	AIO ADDR 8 HARDWARE MISMATCH 15	10	AIO ADDR 9 HARDWARE MISMATCH 7
	3	AIO ADDR 9 HARDWARE MISMATCH 0	11	AIO ADDR 9 HARDWARE MISMATCH 8
	4	AIO ADDR 9 HARDWARE MISMATCH 1	12	AIO ADDR 9 HARDWARE MISMATCH 9
	5	AIO ADDR 9 HARDWARE MISMATCH 2	13	AIO ADDR 9 HARDWARE MISMATCH 10
	6	AIO ADDR 9 HARDWARE MISMATCH 3	14	AIO ADDR 9 HARDWARE MISMATCH 11
	7	AIO ADDR 9 HARDWARE MISMATCH 4	15	AIO ADDR 9 HARDWARE MISMATCH 12
	0	AIO ADDR 9 HARDWARE MISMATCH 13	8	AIO ADDR 10 HARDWARE MISMATCH 5
	1	AIO ADDR 9 HARDWARE MISMATCH 14	9	AIO ADDR 10 HARDWARE MISMATCH 6
	2	AIO ADDR 9 HARDWARE MISMATCH 15	10	AIO ADDR 10 HARDWARE MISMATCH 7

Register	Bit No.	System Trouble Name	Bit No.	System Trouble Name
460136	3	AIO ADDR 10 HARDWARE MISMATCH 0	11	AIO ADDR 10 HARDWARE MISMATCH 8
	4	AIO ADDR 10 HARDWARE MISMATCH 1	12	AIO ADDR 10 HARDWARE MISMATCH 9
	5	AIO ADDR 10 HARDWARE MISMATCH 2	13	AIO ADDR 10 HARDWARE MISMATCH 10
	6	AIO ADDR 10 HARDWARE MISMATCH 3	14	AIO ADDR 10 HARDWARE MISMATCH 11
	7	AIO ADDR 10 HARDWARE MISMATCH 4	15	AIO ADDR 10 HARDWARE MISMATCH 12
460137	0	AIO ADDR 10 HARDWARE MISMATCH 13	8	AIO ADDR 1 DUPLICATE ADDRESS 5
	1	AIO ADDR 10 HARDWARE MISMATCH 14	9	AIO ADDR 1 DUPLICATE ADDRESS 6
	2	AIO ADDR 10 HARDWARE MISMATCH 15	10	AIO ADDR 1 DUPLICATE ADDRESS 7
	3	AIO ADDR 1 DUPLICATE ADDRESS 0	11	AIO ADDR 1 DUPLICATE ADDRESS 8
	4	AIO ADDR 1 DUPLICATE ADDRESS 1	12	AIO ADDR 1 DUPLICATE ADDRESS 9
	5	AIO ADDR 1 DUPLICATE ADDRESS 2	13	AIO ADDR 1 DUPLICATE ADDRESS 10
	6	AIO ADDR 1 DUPLICATE ADDRESS 3	14	AIO ADDR 1 DUPLICATE ADDRESS 11
	7	AIO ADDR 1 DUPLICATE ADDRESS 4	15	AIO ADDR 1 DUPLICATE ADDRESS 12
460138	0	AIO ADDR 1 DUPLICATE ADDRESS 13	8	AIO ADDR 2 DUPLICATE ADDRESS 5
	1	AIO ADDR 1 DUPLICATE ADDRESS 14	9	AIO ADDR 2 DUPLICATE ADDRESS 6
	2	AIO ADDR 1 DUPLICATE ADDRESS 15	10	AIO ADDR 2 DUPLICATE ADDRESS 7
	3	AIO ADDR 2 DUPLICATE ADDRESS 0	11	AIO ADDR 2 DUPLICATE ADDRESS 8
	4	AIO ADDR 2 DUPLICATE ADDRESS 1	12	AIO ADDR 2 DUPLICATE ADDRESS 9
	5	AIO ADDR 2 DUPLICATE ADDRESS 2	13	AIO ADDR 2 DUPLICATE ADDRESS 10
	6	AIO ADDR 2 DUPLICATE ADDRESS 3	14	AIO ADDR 2 DUPLICATE ADDRESS 11
	7	AIO ADDR 2 DUPLICATE ADDRESS 4	15	AIO ADDR 2 DUPLICATE ADDRESS 12
460139	0	AIO ADDR 2 DUPLICATE ADDRESS 13	8	AIO ADDR 3 DUPLICATE ADDRESS 5
	1	AIO ADDR 2 DUPLICATE ADDRESS 14	9	AIO ADDR 3 DUPLICATE ADDRESS 6
	2	AIO ADDR 2 DUPLICATE ADDRESS 15	10	AIO ADDR 3 DUPLICATE ADDRESS 7
	3	AIO ADDR 3 DUPLICATE ADDRESS 0	11	AIO ADDR 3 DUPLICATE ADDRESS 8
	4	AIO ADDR 3 DUPLICATE ADDRESS 1	12	AIO ADDR 3 DUPLICATE ADDRESS 9
	5	AIO ADDR 3 DUPLICATE ADDRESS 2	13	AIO ADDR 3 DUPLICATE ADDRESS 10
	6	AIO ADDR 3 DUPLICATE ADDRESS 3	14	AIO ADDR 3 DUPLICATE ADDRESS 11
	7	AIO ADDR 3 DUPLICATE ADDRESS 4	15	AIO ADDR 3 DUPLICATE ADDRESS 12

Register	Bit No.	System Trouble Name	Bit No.	System Trouble Name
460140	0	AIO ADDR 3 DUPLICATE ADDRESS 13	8	AIO ADDR 4 DUPLICATE ADDRESS 5
	1	AIO ADDR 3 DUPLICATE ADDRESS 14	9	AIO ADDR 4 DUPLICATE ADDRESS 6
	2	AIO ADDR 3 DUPLICATE ADDRESS 15	10	AIO ADDR 4 DUPLICATE ADDRESS 7
	3	AIO ADDR 4 DUPLICATE ADDRESS 0	11	AIO ADDR 4 DUPLICATE ADDRESS 8
	4	AIO ADDR 4 DUPLICATE ADDRESS 1	12	AIO ADDR 4 DUPLICATE ADDRESS 9
	5	AIO ADDR 4 DUPLICATE ADDRESS 2	13	AIO ADDR 4 DUPLICATE ADDRESS 10
	6	AIO ADDR 4 DUPLICATE ADDRESS 3	14	AIO ADDR 4 DUPLICATE ADDRESS 11
	7	AIO ADDR 4 DUPLICATE ADDRESS 4	15	AIO ADDR 4 DUPLICATE ADDRESS 12
460141	0	AIO ADDR 4 DUPLICATE ADDRESS 13	8	AIO ADDR 5 DUPLICATE ADDRESS 5
	1	AIO ADDR 4 DUPLICATE ADDRESS 14	9	AIO ADDR 5 DUPLICATE ADDRESS 6
	2	AIO ADDR 4 DUPLICATE ADDRESS 15	10	AIO ADDR 5 DUPLICATE ADDRESS 7
	3	AIO ADDR 5 DUPLICATE ADDRESS 0	11	AIO ADDR 5 DUPLICATE ADDRESS 8
	4	AIO ADDR 5 DUPLICATE ADDRESS 1	12	AIO ADDR 5 DUPLICATE ADDRESS 9
	5	AIO ADDR 5 DUPLICATE ADDRESS 2	13	AIO ADDR 5 DUPLICATE ADDRESS 10
	6	AIO ADDR 5 DUPLICATE ADDRESS 3	14	AIO ADDR 5 DUPLICATE ADDRESS 11
	7	AIO ADDR 5 DUPLICATE ADDRESS 4	15	AIO ADDR 5 DUPLICATE ADDRESS 12
460142	0	AIO ADDR 5 DUPLICATE ADDRESS 13	8	AIO ADDR 6 DUPLICATE ADDRESS 5
	1	AIO ADDR 5 DUPLICATE ADDRESS 14	9	AIO ADDR 6 DUPLICATE ADDRESS 6
	2	AIO ADDR 5 DUPLICATE ADDRESS 15	10	AIO ADDR 6 DUPLICATE ADDRESS 7
	3	AIO ADDR 6 DUPLICATE ADDRESS 0	11	AIO ADDR 6 DUPLICATE ADDRESS 8
	4	AIO ADDR 6 DUPLICATE ADDRESS 1	12	AIO ADDR 6 DUPLICATE ADDRESS 9
	5	AIO ADDR 6 DUPLICATE ADDRESS 2	13	AIO ADDR 6 DUPLICATE ADDRESS 10
	6	AIO ADDR 6 DUPLICATE ADDRESS 3	14	AIO ADDR 6 DUPLICATE ADDRESS 11
	7	AIO ADDR 6 DUPLICATE ADDRESS 4	15	AIO ADDR 6 DUPLICATE ADDRESS 12
460143	0	AIO ADDR 6 DUPLICATE ADDRESS 13	8	AIO ADDR 7 DUPLICATE ADDRESS 5
	1	AIO ADDR 6 DUPLICATE ADDRESS 14	9	AIO ADDR 7 DUPLICATE ADDRESS 6
	2	AIO ADDR 6 DUPLICATE ADDRESS 15	10	AIO ADDR 7 DUPLICATE ADDRESS 7
	3	AIO ADDR 7 DUPLICATE ADDRESS 0	11	AIO ADDR 7 DUPLICATE ADDRESS 8
	4	AIO ADDR 7 DUPLICATE ADDRESS 1	12	AIO ADDR 7 DUPLICATE ADDRESS 9
	5	AIO ADDR 7 DUPLICATE ADDRESS 2	13	AIO ADDR 7 DUPLICATE ADDRESS 10
	6	AIO ADDR 7 DUPLICATE ADDRESS 3	14	AIO ADDR 7 DUPLICATE ADDRESS 11
	7	AIO ADDR 7 DUPLICATE ADDRESS 4	15	AIO ADDR 7 DUPLICATE ADDRESS 12
	0	AIO ADDR 7 DUPLICATE ADDRESS 13	8	AIO ADDR 8 DUPLICATE ADDRESS 5
	1	AIO ADDR 7 DUPLICATE ADDRESS 14	9	AIO ADDR 8 DUPLICATE ADDRESS 6
	2	AIO ADDR 7 DUPLICATE ADDRESS 15	10	AIO ADDR 8 DUPLICATE ADDRESS 7

Register	Bit No.	System Trouble Name	Bit No.	System Trouble Name
460144	3	AIO ADDR 8 DUPLICATE ADDRESS 0	11	AIO ADDR 8 DUPLICATE ADDRESS 8
	4	AIO ADDR 8 DUPLICATE ADDRESS 1	12	AIO ADDR 8 DUPLICATE ADDRESS 9
	5	AIO ADDR 8 DUPLICATE ADDRESS 2	13	AIO ADDR 8 DUPLICATE ADDRESS 10
	6	AIO ADDR 8 DUPLICATE ADDRESS 3	14	AIO ADDR 8 DUPLICATE ADDRESS 11
	7	AIO ADDR 8 DUPLICATE ADDRESS 4	15	AIO ADDR 8 DUPLICATE ADDRESS 12
460145	0	AIO ADDR 8 DUPLICATE ADDRESS 13	8	AIO ADDR 9 DUPLICATE ADDRESS 5
	1	AIO ADDR 8 DUPLICATE ADDRESS 14	9	AIO ADDR 9 DUPLICATE ADDRESS 6
	2	AIO ADDR 8 DUPLICATE ADDRESS 15	10	AIO ADDR 9 DUPLICATE ADDRESS 7
	3	AIO ADDR 9 DUPLICATE ADDRESS 0	11	AIO ADDR 9 DUPLICATE ADDRESS 8
	4	AIO ADDR 9 DUPLICATE ADDRESS 1	12	AIO ADDR 9 DUPLICATE ADDRESS 9
	5	AIO ADDR 9 DUPLICATE ADDRESS 2	13	AIO ADDR 9 DUPLICATE ADDRESS 10
	6	AIO ADDR 9 DUPLICATE ADDRESS 3	14	AIO ADDR 9 DUPLICATE ADDRESS 11
	7	AIO ADDR 9 DUPLICATE ADDRESS 4	15	AIO ADDR 9 DUPLICATE ADDRESS 12
460146	0	AIO ADDR 9 DUPLICATE ADDRESS 13	8	AIO ADDR 10 DUPLICATE ADDRESS 5
	1	AIO ADDR 9 DUPLICATE ADDRESS 14	9	AIO ADDR 10 DUPLICATE ADDRESS 6
	2	AIO ADDR 9 DUPLICATE ADDRESS 15	10	AIO ADDR 10 DUPLICATE ADDRESS 7
	3	AIO ADDR 10 DUPLICATE ADDRESS 0	11	AIO ADDR 10 DUPLICATE ADDRESS 8
	4	AIO ADDR 10 DUPLICATE ADDRESS 1	12	AIO ADDR 10 DUPLICATE ADDRESS 9
	5	AIO ADDR 10 DUPLICATE ADDRESS 2	13	AIO ADDR 10 DUPLICATE ADDRESS 10
	6	AIO ADDR 10 DUPLICATE ADDRESS 3	14	AIO ADDR 10 DUPLICATE ADDRESS 11
	7	AIO ADDR 10 DUPLICATE ADDRESS 4	15	AIO ADDR 10 DUPLICATE ADDRESS 12
460147	0	AIO ADDR 10 DUPLICATE ADDRESS 13	8	Trouble reporting
	1	AIO ADDR 10 DUPLICATE ADDRESS 14	9	Hardware Compromised
	2	AIO ADDR 10 DUPLICATE ADDRESS 15	10	HISTORY FLASH ERROR
	3	LOOP LICENSE EXCEEDED	11	NETWORK INSTALLATION MODE
	4	POWER SUPPLY LICENSE EXCEEDED	12	Reserved
	5	PANEL UPGRADE NOT PRESENT	13	Reserved
	6	ALARM SIGNAL LICENSE NOT PRESENT	14	Reserved
	7	ZONE VIEW LICENSE NOT PRESENT	15	Reserved

Register	Bit No.	System Trouble Name	Bit No.	System Trouble Name
360050	0	LOGIC ZONE LICENSE EXCEEDED	8	POWER SUPPLY DATABASE INCOMPATIBLE (LSB is PMB address 1-5)
	1	NETWORK DISPLAY LICENSE NOT PRESENT	9	Reserved
	2	CLIP LICENSE NOT PRESENT	10	Reserved
	3	CUSTOM ACTION LICENSE EXCEEDED	11	Reserved
	4	ADVANCED LOGIC LICENSE NOT PRESENT	12	Reserved
	5	POWER SUPPLY NO SERVICE (LSB is PMB address 1-5)	13	Reserved
	6	POWER SUPPLY PROGRAM CORRUPT (LSB is PMB address 1-5)	14	Reserved
	7	POWER SUPPLY DATABASE CORRUPT (LSB is PMB address 1-5)	15	Reserved
360051	0	Reserved	8	Reserved
	1	LOOP NO DATABASE (LSB is loop address 1-10)	9	Reserved
	2	LOOP DATABASE INCOMPATIBLE (LSB is loop address 1-10)	10	Reserved
	3	LOOP IN BOOTLOADER (LSB is loop address 1-10)	11	Reserved
	4	Reserved	12	Service Mode Enabled
	5	Reserved	13	Trouble reporting
	6	Reserved	14	Health check over Ethernet
	7	Reserved	15	Health check over wi-fi
360052	0	Hardware Compromised	8	AIO ADDR 6 BUZZER SUPERVISORY (LSB is 0 for router, 1-15 for peripheral)
	1	RLD Programming Mode Activated (LSB is AIO router address 1-10)	9	AIO ADDR 7 BUZZER SUPERVISORY (LSB is 0 for router, 1-15 for peripheral)
	2	RLD DATABASE MISMATCH (LSB is AIO router address 1-10)	10	AIO ADDR 8 BUZZER SUPERVISORY (LSB is 0 for router, 1-15 for peripheral)
	3	AIO ADDR 1 BUZZER SUPERVISORY (LSB is 0 for router, 1-15 for peripheral)	11	AIO ADDR 9 BUZZER SUPERVISORY (LSB is 0 for router, 1-15 for peripheral)
	4	AIO ADDR 2 BUZZER SUPERVISORY (LSB is 0 for router, 1-15 for peripheral)	12	AIO ADDR 10 BUZZER SUPERVISORY (LSB is 0 for router, 1-15 for peripheral)
	5	AIO ADDR 3 BUZZER SUPERVISORY (LSB is 0 for router, 1-15 for peripheral)	13	AIO ADDR 1 HARDWARE MISMATCH (LSB is 0 for router, 1-15 for peripheral)
	6	AIO ADDR 4 BUZZER SUPERVISORY (LSB is 0 for router, 1-15 for peripheral)	14	AIO ADDR 2 HARDWARE MISMATCH (LSB is 0 for router, 1-15 for peripheral)
	7	AIO ADDR 5 BUZZER SUPERVISORY (LSB is 0 for router, 1-15 for peripheral)	15	AIO ADDR 3 HARDWARE MISMATCH (LSB is 0 for router, 1-15 for peripheral)

Register	Bit No.	System Trouble Name	Bit No.	System Trouble Name
360053	0	AIO ADDR 4 HARDWARE MISMATCH (LSB is 0 for router, 1-15 for peripheral)	8	AIO ADDR 2 HARDWARE FAILURE (LSB is 0 for router, 1-15 for peripheral)
	1	AIO ADDR 5 HARDWARE MISMATCH (LSB is 0 for router, 1-15 for peripheral)	9	AIO ADDR 3 HARDWARE FAILURE (LSB is 0 for router, 1-15 for peripheral)
	2	AIO ADDR 6 HARDWARE MISMATCH (LSB is 0 for router, 1-15 for peripheral)	10	AIO ADDR 4 HARDWARE FAILURE (LSB is 0 for router, 1-15 for peripheral)
	3	AIO ADDR 7 HARDWARE MISMATCH (LSB is 0 for router, 1-15 for peripheral)	11	AIO ADDR 5 HARDWARE FAILURE (LSB is 0 for router, 1-15 for peripheral)
	4	AIO ADDR 8 HARDWARE MISMATCH (LSB is 0 for router, 1-15 for peripheral)	12	AIO ADDR 6 HARDWARE FAILURE (LSB is 0 for router, 1-15 for peripheral)
	5	AIO ADDR 9 HARDWARE MISMATCH (LSB is 0 for router, 1-15 for peripheral)	13	AIO ADDR 7 HARDWARE FAILURE (LSB is 0 for router, 1-15 for peripheral)
	6	AIO ADDR 10 HARDWARE MISMATCH (LSB is 0 for router, 1-15 for peripheral)	14	AIO ADDR 8 HARDWARE FAILURE (LSB is 0 for router, 1-15 for peripheral)
	7	AIO ADDR 1 HARDWARE FAILURE (LSB is 0 for router, 1-15 for peripheral)	15	AIO ADDR 9 HARDWARE FAILURE (LSB is 0 for router, 1-15 for peripheral)
360054	0	AIO ADDR 10 HARDWARE FAILURE (LSB is 0 for router, 1-15 for peripheral)	8	AIO ADDR 8 EXTRA DEVICE (LSB is 0 for router, 1-15 for peripheral)
	1	AIO ADDR 1 EXTRA DEVICE (LSB is 0 for router, 1-15 for peripheral)	9	AIO ADDR 9 EXTRA DEVICE (LSB is 0 for router, 1-15 for peripheral)
	2	AIO ADDR 2 EXTRA DEVICE (LSB is 0 for router, 1-15 for peripheral)	10	AIO ADDR 10 EXTRA DEVICE (LSB is 0 for router, 1-15 for peripheral)
	3	AIO ADDR 3 EXTRA DEVICE (LSB is 0 for router, 1-15 for peripheral)	11	AIO ADDR 1 DUPLICATE ADDRESS (LSB is 0 for router, 1-15 for peripheral)
	4	AIO ADDR 4 EXTRA DEVICE (LSB is 0 for router, 1-15 for peripheral)	12	AIO ADDR 2 DUPLICATE ADDRESS (LSB is 0 for router, 1-15 for peripheral)
	5	AIO ADDR 5 EXTRA DEVICE (LSB is 0 for router, 1-15 for peripheral)	13	AIO ADDR 3 DUPLICATE ADDRESS (LSB is 0 for router, 1-15 for peripheral)
	6	AIO ADDR 6 EXTRA DEVICE (LSB is 0 for router, 1-15 for peripheral)	14	AIO ADDR 4 DUPLICATE ADDRESS (LSB is 0 for router, 1-15 for peripheral)
	7	AIO ADDR 7 EXTRA DEVICE (LSB is 0 for router, 1-15 for peripheral)	15	AIO ADDR 5 DUPLICATE ADDRESS (LSB is 0 for router, 1-15 for peripheral)
360055	0	AIO ADDR 6 DUPLICATE ADDRESS (LSB is 0 for router, 1-15 for peripheral)	8	Reserved
	1	AIO ADDR 7 DUPLICATE ADDRESS (LSB is 0 for router, 1-15 for peripheral)	9	Reserved
	2	AIO ADDR 8 DUPLICATE ADDRESS (LSB is 0 for router, 1-15 for peripheral)	10	Reserved
	3	AIO ADDR 9 DUPLICATE ADDRESS (LSB is 0 for router, 1-15 for peripheral)	11	Reserved
	4	AIO ADDR 10 DUPLICATE ADDRESS (LSB is 0 for router, 1-15 for peripheral)	12	Reserved
	5	HISTORY FLASH ERROR	13	Reserved
	6	Reserved	14	Reserved
	7	Reserved	15	Reserved

SECTION 8: THE BACNET FEATURE

The BACnet feature of the CLSS Gateway provides communications between a panel(s) network and a BACnet client, which is using the BACnet communication protocol.

The CLSS Gateway acts like any other node on a panel network. It can communicate with a single panel or network of panels directly or through a network control module.

NOTE: The BACnet communication protocol is an *American National Standard (ANSI/ASHRAE 135-2012)*.

The CLSS BACnet client will present the physical fire devices in the network as BACnet objects. The CLSS Gateway manages their object database. As events occur, the object properties are updated in real-time, and messages are sent to the appropriate BACnet report destination.

The BACnet clients may make requests to read properties of the BACnet objects. Those properties are the values of the device status and programming.

After a user subscribes for event notifications, the BACnet client receives events from each subscribed panel.

Large networks can use many CLSS Gateways. Each CLSS Gateway in a large network can support up to 16 panels with a combined maximum of 15, 000 objects.

The BACnet client workstation front-end must conform to *BACnet Standard Annex J* for IP and support objects mentioned in the 8.13 BACnet PIC Statement .

NOTE: This manual is written with the understanding that its user is trained in BACnet operations and services. The information provided here is solely for the configuration of the Gateway to communicate event information to an existing BACnet network.

8.1 AGENCY LISTINGS

8.1.1 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 Code

Underwriters Laboratories

• UL-864—Control Units for Fire Alarm Systems, 10th Edition

Underwriters Laboratories Canada

• CAN/ULC-S527-19—Standard for Control Units for Fire Alarm Systems, Fourth Edition

8.2 INSTALLATION

This product is intended to be installed in accordance with the following regulatory agencies.

8.2.1 LOCAL

• AHJ—Authority Having Jurisdiction
• National Fire Protection Association
• NFPA 70—National Electrical Code
• NFPA 72—National Fire Alarm Code
• NFPA 101—Life Safety Code

8.2.2 CANADA

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

CAUTION: Improper installation, maintenance, and lack of routine testing could result in system malfunction.

8.3 COMPATIBLE EQUIPMENT

The CLSS Gateway is compatible with the following equipment:

Table 8.1
CLSS-Compatible Equipment List

Type	Equipment
Fire Panels	**NOTIFIER Panels** • NFS-320 • NFS-640 • NFS2-640 • NFS-3030 • NFS2-3030 • AFP2800 • AFP 3030 • N16 (INSPIRE) **Honeywell Panels** • XLS 120 • XLS 140-2 • XLS 2000 • XLS 3000 **GENT Panels** • COMPACT-24-N • COMPACT-PLUS • VIGPLUS-24 • VIGI-24 • VIGI-72
Network Cards	• NCM-W, NCM-F • HS-NCM-W, HS-NCM-SF, HS-NCM-MF, HS-NCM-WSF, HS-NCM-WMF, HS-NCM-MFSF • NFN-GW-PC-NHW-2, HS-NCM-WMF-2, HS-NCM-WSF-2, HS-NCM-W-2
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	Unmonitored but network compatible.
	
	• DVC
	• NCA-2
	• NCD
	• NWS-3
	• Legacy Gateway
	• NFN-GW-PC-HNW-2
	• 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
	• VESDA-HLI-GW

8.4 CLSS GATEWAY PARTS

Part Number	Description
HON-CGW-MBB	CLSS Gateway with enclosure
CGW-MB	CLSS Gateway board
CGW-BB	CLSS Gateway enclosure
50160636-001	CLSS Gateway kit. It includes a 30” NUP cable and a NOTIFIER lock and key set.
32351718-001	10 ft NUP Serial (RS-232) cable kit
CCM-VZ-HON	CLSS Verizon cell module
CCM-ATT-HON	CLSS AT&T cell module

8.5 SYSTEM REQUIREMENTS

The CLSS Gateway can monitor up to 16 panels. All of these panels should have a combined maximum of 15,000 objects only. This includes all detectors, monitor modules, control modules, bell circuits, and so on.

Refer to the panel manual for details about wiring limitations.

Access the configuration web page from a computer in the same IP subnet as the CLSS Gateway with latest version of Google Chrome™. JAVA® version 6 or higher must also be installed and enabled.

8.6 RECOMMENDATIONS

Ensure the following to prevent troubles:

- The LED indicators on the CLSS Gateway board confirm normal operations of the gateway.
- The BACnet functionality is correctly configured and enabled in the CLSS Gateway.
- The IP addresses and subnet mask entered in the **Network Settings** of the **CLSS Gateway Configuration Tool** are correct.
- Correct IP address as well as net mask are specified in the Configuration Computer allowing it to connect with the CLSS Gateway in the building.
- When the CLSS Gateway and the BACnet client are in different network, the gateway as a foreign device is enabled; and, the IP address and port of the BBMD device* is correctly entered.

*BBMD = BACnet Broadcast Management Devices (BBMDs)

8.7 SYSTEM ARCHITECTURE

These are connections options for the CLSS Gateway architecture.

An Internet or Intranet IP network connection is used with both architectures.

8.7.1 IP RESTRICTIONS FOR THE GATEWAY

- Assign a static IP address.

> **NOTE:** DHCP is supported, but not recommended.
> Before using DHCP with LAN for Intranet connection, consult the network administrator of the Site.

- Following are not supported:
    - Web access through an HTTP proxy server
    - Use of a NAT (Network Address Translation)

8.7.2 IP REQUIREMENTS

8.7.2.1 IP Port Settings

The following IP ports must be available to the CLSS Gateway:

Ports Range	Type	Direction	Purpose
53	UDP and TCP	Output	DNS Resolution: The optional web portal feature in the CLSS Gateway must resolve “www.evanceservices.com” for communications to the eVance server.
80	TCP	Input	Web Based Configuration
443	TCP	Input	HTTPS Communications: The CLSS Gateway accepts connections on Port 443 for configuration of the BACnet feature. Typically, this incoming connection is local to the site intranet and not externally from the Internet.
		Output	The optional web portal feature in the BACnet Gateway communicates out to the eVance server on the Internet (www.evanceservices.com) when configured for eVance operations.
47808 to 47823	UDP	Input/Output	BACnet feature communications

8.7.3 SINGLE PANEL ARCHITECTURE

Direct panel connection — a connection is made directly to a supported fire panel or annunciator. Refer to Figure 8-1: Single Panel Connecting to BACnet via CLSS Gateway for connection topology details.

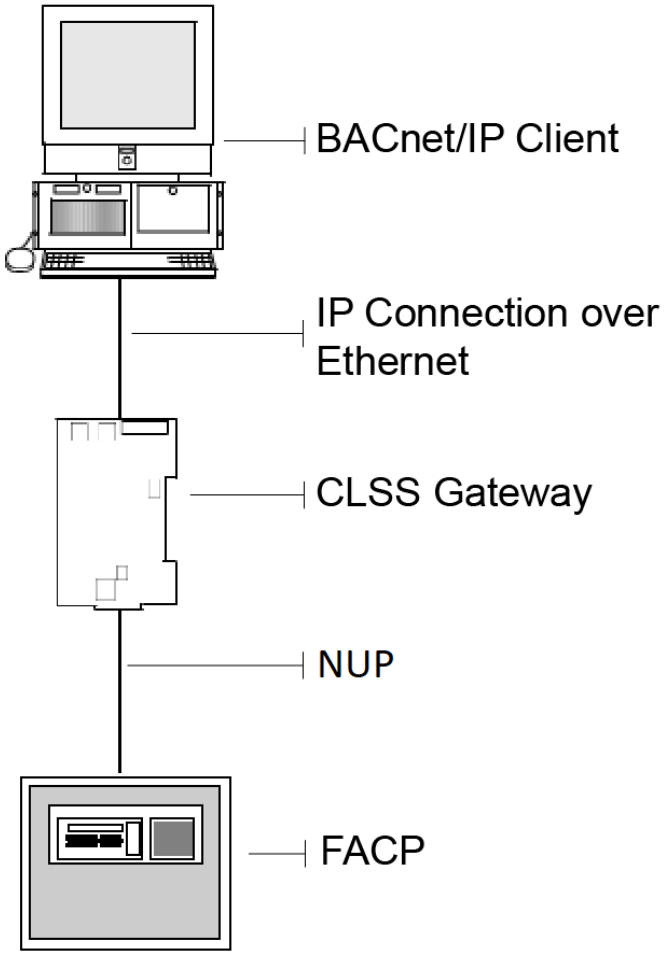


Figure 8-1: Single Panel Connecting to BACnet via CLSS Gateway

Refer to 8.3 Compatible Equipment for supported panels and annunciators.

8.7.4 MULTI-PANEL NETWORK ARCHITECTURE

The CLSS Gateway can connect to a NUP, RS232, USB, or TTL port available on a panel and interact with that panel's network.

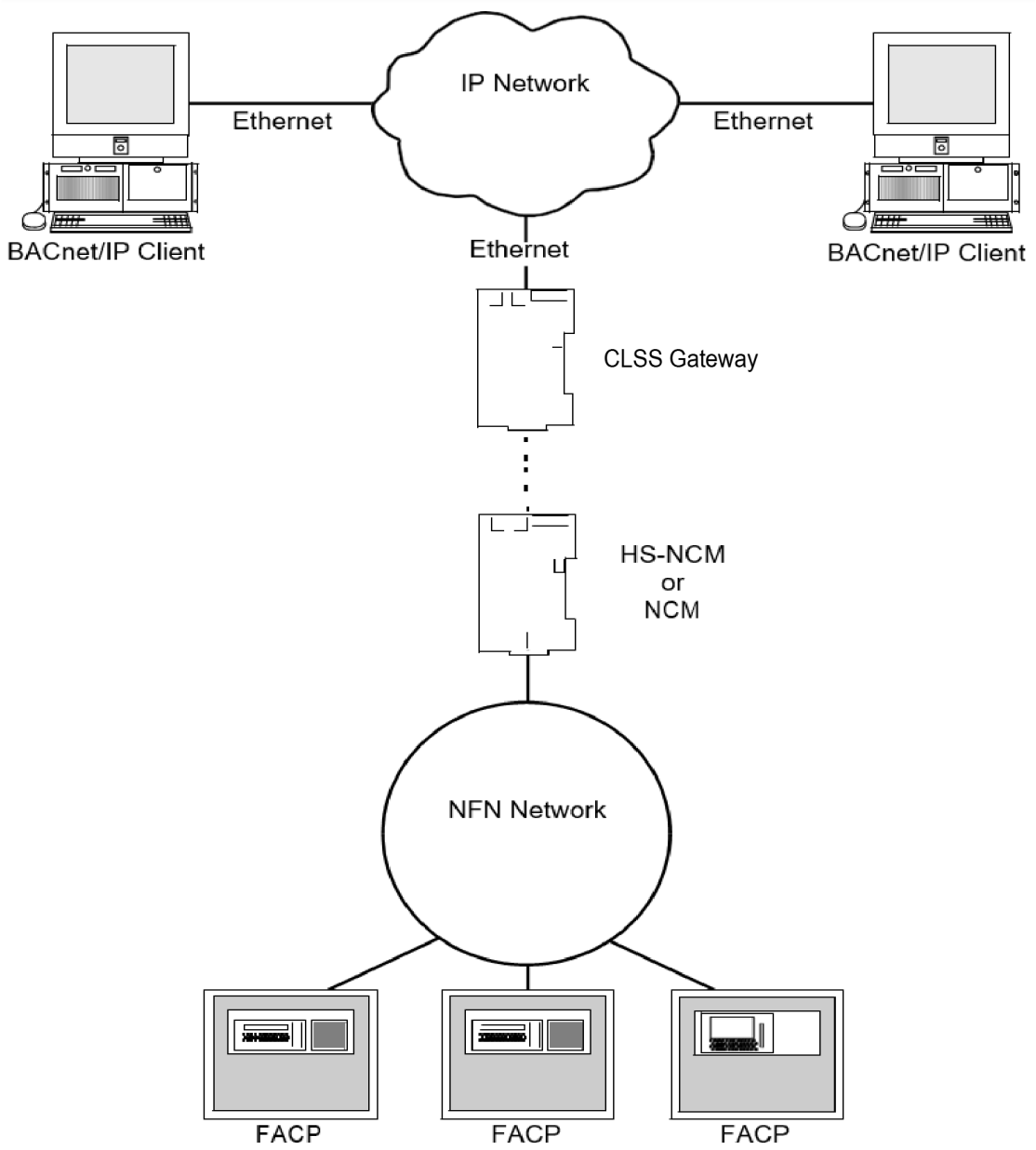


Figure 8-2: Gateway Connected with Multiple Panels

8.8 BACNET FEATURE ACTIVATION

Purchase the required number of BACnet features on *CLSS Site Manager* and then activate them in the CLSS App.

NOTE: Purchase should be within the number of tokens available.

8.8.1 TO PURCHASE THE BACNET SUPPORT

01. Log onto *CLSS Site Manager*.
02. Click on your account name and select **Manage Access**.

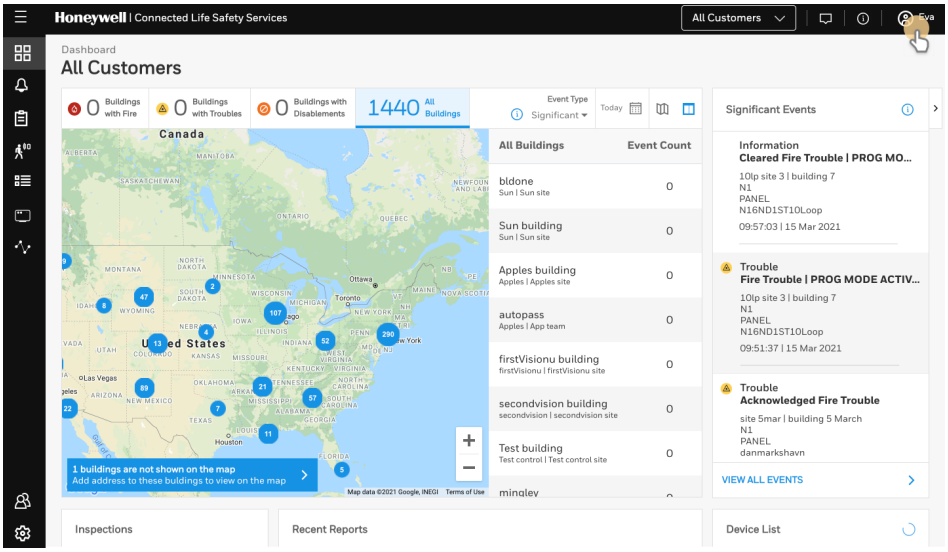


Figure 8-3: Selecting Manage Access

03. Click **Features** on the **Manage Access** page.
04. Click **Gateway** under the **Features** section.
05. Note down the purchased number under **Available Features**.
06. Click **PURCHASE** at the top right side.
    Purchasing the BACnet Support
07. Scroll down to find **BACnet Support** in the **Features** tab.
08. Enter the number of support required in the **BACnet Support** field.
09. Click **PURCHASE**.

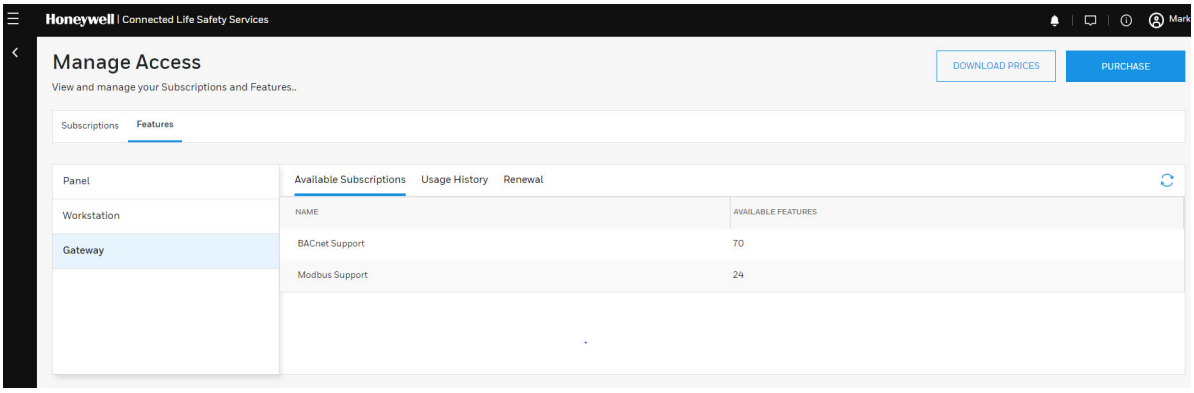


Figure 8-4: Purchasing the BACnet Support

10. Read the **Confirmation** message and if acceptable, click **CONFIRM**.
    Or
    Click **CANCEL** and repeat the steps from 8 to 10.
11. Wait for the purchase to complete and refresh the page, if required.
12. Verify that the purchased number under **Available Features** is correct.

8.8.2 TO ACTIVATE THE BACNET SUPPORT

NOTE:
- The gateway must be already installed. If not, install the fixed gateway.
- All the network settings should be configured while installing.

01. Tap **Perform Feature Activation** on the *CLSS* App's welcome message.

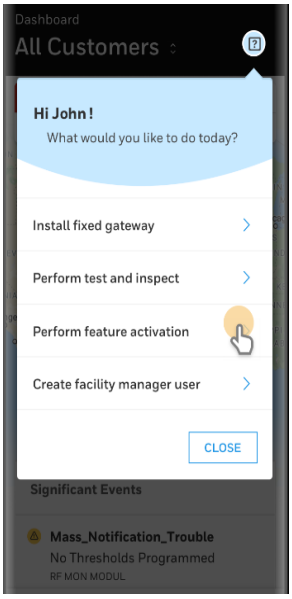


Figure 8-5: Feature Activation: The First Step

02. Tap **Fixed Gateways**.
03. Select the site of the gateway.
04. Find and tap the OC of the gateway.
05. Tap **ADD ACTIVATION**.
06. Tap **BACnet Support** under the **One Time Activations**.
07. Tap **ACTIVATE**.
08. Wait for the activation successful message.

8.9 CONFIGURING THE BACNET NETWORK SETTINGS

8.9.1 INSTALLATION AND CONFIGURATIONS

The CLSS Gateway can communicate with the BACnet client in an Ethernet LAN.

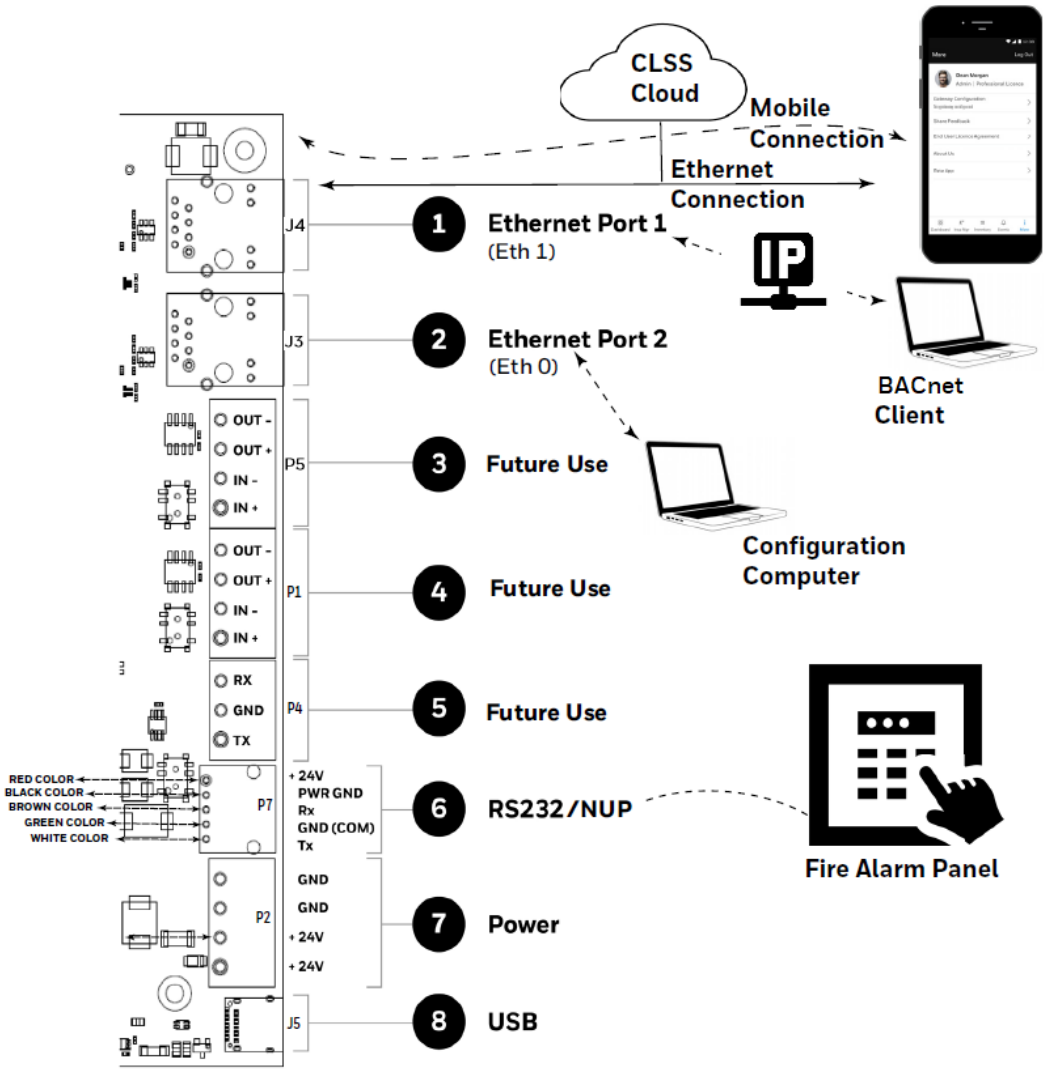
8.9.2 THE IP SETTINGS

The following information applies to IP settings:

• You can use only the *Eth1* port for connections to BACnet clients. For more details, refer to 8.10.1 To Configure the BACnet Settings .
• Each CLSS Gateway is shipped with a default node number of 235.
• The computer used to configure the CLSS Gateway must establish an IP connection to the gateway. Consult with a network administrator if unsure how to make this connection.
• Connecting more than one CLSS Gateway prior to reconfiguring the IP address will result in an IP address conflict.

8.10 TO CONNECT WITH THE BACNET CLIENT

01. At the CLSS Gateway side, connect an Ethernet cable to the Ethernet Port 1.
02. Connect the other end of the Ethernet cable to the IP network.



03. Connect the system running the BACnet client to the same IP network.

8.10.1 TO CONFIGURE THE BACNET SETTINGS

Using the web-based *Gateway Configuration Tool*, configure the BACnet settings for the *CLSS Gateway* to use the BACnet application.

CAUTION: If you are reconfiguring an existing setup, any new changes to the panel's device configuration file, NODE address, or gateway id will require manual removal of the database. It will automatically restart the BACnet application.

Configure the BACnet settings as follows:

01. On the CLSS Gateway board, find the S6 button.
02. Press the S6 button for a minimum of 6 seconds and then release it. It will switch the gateway to configuration mode. The LED indicator DL3 turns ON and SOLID indicating that the configuration is enabled.
03. Connect the Ethernet cable to *Eth0* for enabling web configuration.

NOTE: The web configuration is available only on *Eth0*.

04. Open the Configuration Computer connected to the *Eth0* port of the gateway.

NOTE: The static IP of the *Eth0* port is *192.168.10.190*.

05. In the Chrome browser, enter the following URL: https://192.168.10.190:9443/config/index.html
06. Do the following if any security warning is shown. Otherwise, go to step 7.
    a. Click the *Advanced* link below the error message.
    b. Agree to proceed.
07. In the **Gateway Configuration Tool** page, enter the password.

NOTE: The default password is: Welcome123

08. Go to the **Network Settings** in the **Gateway Settings** section.
09. Provide the required gateway settings details:

Table 8.2
Table 8.1 Gateway Settings Details

Field	Description
Select Panel	Select the brand of panel to which gateway is connected
Communication Port	Select the type of port gateway is connected to panel **Auto**: Automatically detects the port **RS232**: Select RS232 if gateway is connected via RS232 **TTL**: Select TTL if gateway is connected via TTL
Baud Rate	Select the Baud Rate to which panel is configured among 9600, 19200, 38400, 57600, 115200
Node Address	Enter the Node Address for gateway. For a Gent panel the address can be between 64 to 249. For a NOTIFIER panel the address can be between 1 to 240. The default node address is 235. **Note**: The node address should be different from the gateway in the same network.
Gateway ID	Enter the Gateway ID. It should be within 1 to 100. **Important**: It is applicable only for Gent panels. **Note**: It should be different from the node address in the same network.
Upload file	Upload a file using which IFOM inventory will be generated. For different panel type, the file format will be different. Only for Gent panels, it is a *.dat file. Refer to 5.3.3 To Configure the Panel's Connection Settings section to know how to generate a *.dat file)

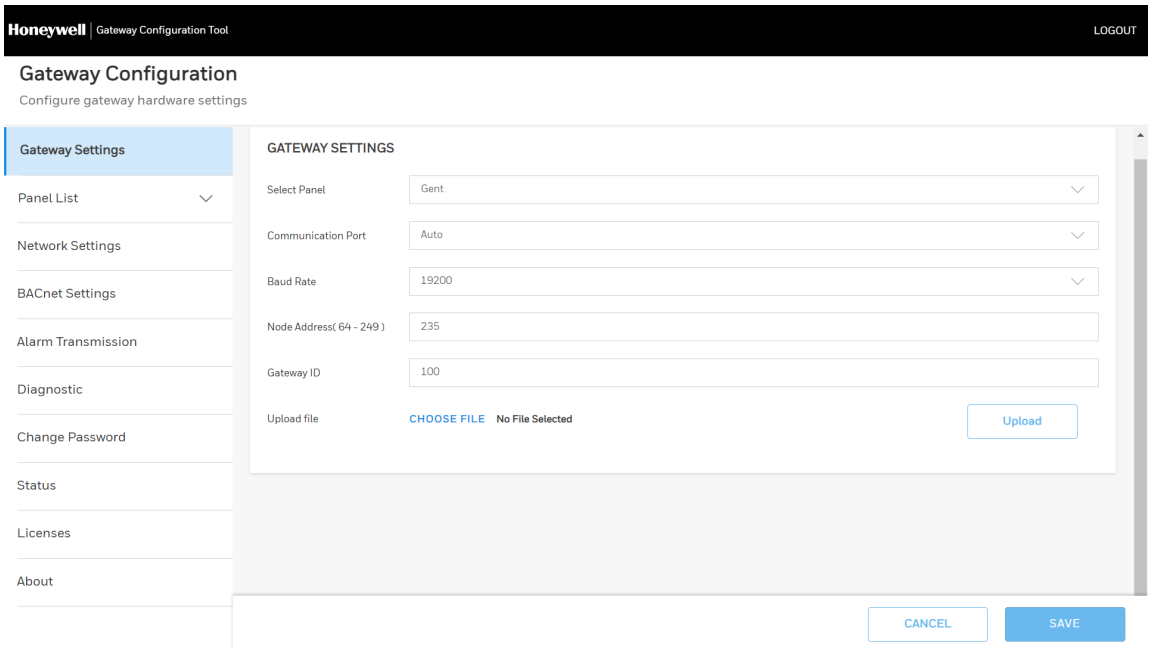
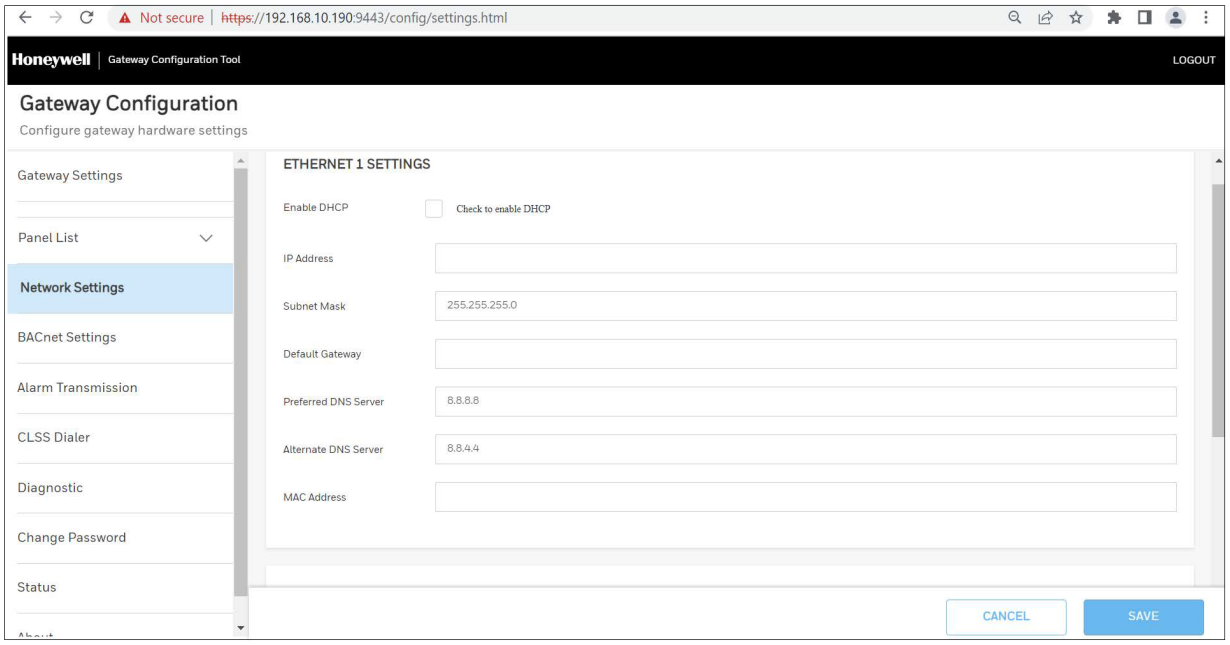


Figure 8-6: Gateway Settings for BACnet

10. Assign the *Eth1* port with a static IP address for the BACnet connection.



11. Connect the Ethernet cable between the *Eth1* port of CLSS gateway and its LAN device.

12. Find and click **BACnet Settings** in the **Gateway Settings** section as shown in"BACnet Gateway Settings Screen" below.

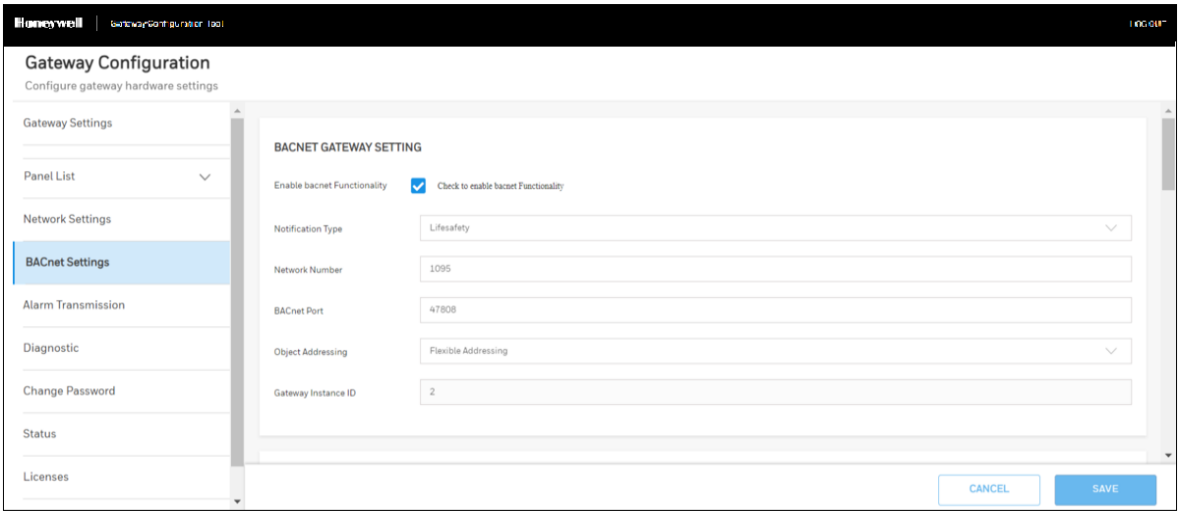


Figure 8-7: BACnet Gateway Settings Screen

13. Specify the required values as in the following table:

Table 8.3
Table 8.2 Gateway Settings

Fields	Action
Enable BACnet functionality	Select to enable the BACnet application.
Notification Type	Select Life Safety or Multi-state suitable to the customer requirement.
Network Number	Specify a network number of this BACnet gateway. It helps to identify the gateway when multiple gateways are in the network. Sometimes two or more gateways in the same network might use the BACnet feature. Each of them should have its own unique network number. Ensure that the difference between any two network numbers is at least 100.
BACnet Port	Specify the BACnet port. The universal default port number is 47808. Its range can be: 47808 - 47823 (0xBAC0 - 0xBACF)
Object Addressing	Select the addressing type. Options: Standard Addressing or Flexible Addressing. **Note**: Flexible addressing is available only for Gent panels. Standard addressing is available for NOTIFIER panels.
Gateway Instance ID	This is a read only property. It shows the instance number of Gateway on the client. The instance number is calculated using the Gateway ID value given in the Gateway settings.
FOREIGN DEVICE CONFIGURATION (Optional)	
Foreign Device	Select to enable the foreign device.
IP Address	Enter the BBMD Server IP address.
Port	Enter the BBMD Port number.
Register Time	Specify the time in seconds. As per this value, the device will periodically re-register with the BBMD to maintain full participation in the BACnet/IP network. **Note**: Maximum value is 30 seconds.
NODE MAPPING	
Automatic Mapping	Select Yes to view the first 16 nodes identified in the network. Select No to disable automatic mapping. **Note**: A reboot is needed, if the value is changed.

Fields	Action
Show all nodes(Yes/No)	Select Yes to view both online as well as offline nodes. Select No to view only the online and monitored nodes.
Monitoring(Yes/No)	Select Yes from the *Monitoring* column in the table. The client will show the selected nodes. Select No from the *Monitoring* column in the table to disable the monitoring.
BACK UP AND RESTORE	
Configuration Backup	Click to download a configuration settings as a backup file.
CHOOSE FILE	Click and select an already downloaded backup file.
Upload BACnet backup file	Click to upload and apply the configuration settings of the backup file. **Note**: Before uploading, ensure that the file name is: BacnetBackup.tar.gz
TOOLS AND GATEWAY ACTIVITY	
Delete Object Database	Click to delete the BACnet database in the gateway.
EVENT PRIORITIES **(Only for GENT Panels. Changing Event Priorities is Not Recommended.)**	
Reliable Fire Alarm	Set Priority between range 0-31.
Panic Alarm	Set Priority between range 0-31.
LifeSafety PreAlarm	Set Priority between range 0-31.
General Alarm	Set Priority between range 0-31.
Life Safety Return To Normal	Set Priority between range 0-31.
Property Process Alarm	Set Priority between range 32-63.
Property Return to Safety Alarm	Set Priority between range 32-63.
Fire Supervision	Set Priority between range 64-95.
General Supervision	Set Priority between range 64-95.
Early Warning Alert	Set Priority between range 64-95.
Fields	Action
Supervisory Return To Normal	Set Priority between range 64-95.
Process Trouble	Set Priority between range 96-127.
Fire Trouble	Set Priority between range 96-127.
Trouble return to normal	Set Priority between range 96-127.
Equipment Supervision and Monitoring	Set Priority between range 128-191.
System Status Active	Set Priority between range 192-255.
Set to default	Click to set the priorities to default.

14. Click **SAVE**.
15. Do the following if you reconfigured panel's device configuration file, node address, or gateway ID:
    a. Find and click **BACnet Settings** in the **Gateway Settings** section.
    b. Go to the **TOOLS** section and click **Delete** to delete the database.
16. Wait for the BACnet application restart to complete.

8.11 REPLACING THE BACNET-GW

The CLSS Gateway and the Legacy Gateway have different object addressing schemes. Refer to the 8.3 Compatible Equipment section for the supported objects details.

Ensure that the replacing CLSS Gateway has correct object addresses and the old object mappings of Legacy Gateway are removed.

Refer to the 8.13 BACnet PIC Statement section for the CLSS Gateway object addressing details.

01. Ensure that the BACnet feature in the CLSS Gateway is licensed.
02. Go to CLSS Gateway Web Configuration Tool.
03. Click the **BACnet Settings** tab.
04. Ensure that the below BACnet settings are same in the CLSS Gateway:
    • Static IP address
    • BACnet Port Number
    • Foreign device configurations
    • Node mapping
    • Network Number
05. Delete the replaced BACnet gateway related objects on the BACnet client.
06. Connect the CLSS Gateway.
07. Rediscover the BACnet objects.
    Or
    Restart the BACnet client.
08. Modify the client graphics according to the rediscovered objects.

8.12 USING BOTH THE CLSS GATEWAY AND THE LEGACY BACNET GATEWAY

The CLSS Gateway and the Legacy Gateway have different addressing schemes. Ensure that they are assigned with their own addressing scheme.

Refer to the 8.13 BACnet PIC Statement section for the CLSS Gateway object addressing details.

01. Ensure that the BACnet feature in the CLSS Gateway is licensed.
02. Go to CLSS Gateway Web Configuration Tool.
03. Click the **BACnet Settings** tab.
04. Configure the BACnet settings in the new CLSS Gateway.
05. Refer to the 8.10.1 To Configure the BACnet Settings section for the configuring procedure.
06. Connect the CLSS Gateway and rediscover the BACnet objects.
07. Modify the client graphics according to the new instance numbers (object addresses).

For the *CLSS Gateway* object addressing details, refer to the 8.13 BACnet PIC Statement . section.

CAUTION: The Node Number of the CLSS Gateway should be different from other gateways in the network.

CAUTION: The IP address of the CLSS Gateway should be different from other gateways and devices in the network.

8.13 BACNET PIC STATEMENT

8.13.1 PROTOCOL IMPLEMENTATION CONFORMANCE STATEMENT (NORMATIVE)

8.13.1.1 BACnet Protocol Revision: 14

Product Description

This product presents Fire Panel and Annunciator nodes (operating as part of a Fire Panel network or stand-alone) and their associated objects as BACnet objects. Event notification for Alarms, Troubles, and other states are sent to registered BACnet client workstations.

It also support the following control functionalities of the Gent panels:

Silence/Unsilence, Reset and Mute panels, Enable/Disable loop devices, Zones, Sectors and Command builds, and Activate/De-activate Command builds.

This product presents VESDA-Air is an indoor air quality (IAQ) measurement system piggybacking on VESDA-E smoke detection systems and their associated objects as BACnet objects. Event notification for Faults (stax/cartridge faults) and other states are sent to registered BACnet client workstations.

BACnet Standardized Device Profile (Annex L):

☐ BACnet Operator Workstation (B-OWS)

☐ BACnet Building Controller (B-BC)

☑ BACnet Advanced Application Controller (B-AAC)

☐ BACnet Application Specific Controller (B-ASC)

☐ BACnet Smart Sensor (B-SS)

☐ BACnet Smart Actuator (B-SA)

BACnet Interoperability Building Blocks Supported (Annex K)

Data Sharing	Device & Network Management	Scheduling	Alarm & Event Management	Trending
DS-RP-B	DM-DDB-B		AE-ACK-B	
DS-RPM-B	DM-DOB-A			
	DM-DOB-B		AE-ASUM-B	
	DM-LM-B			
DS-WP-B	DM-LM-B		AE-N-I-B	
DS-WPM-B			AE-INFO-B	
			AE-LS-B*	
*DM-RD-B and AE-LS-B are supported for the Gent panels only.				

Segmentation Capability

☑ Segmented requests supported, Window Size 1024 Max

☑ Segmented responses supported, Window Size 1024 Max

Standard Object Types Supported - Life Safety Point/Life Safety Zone

	BACnet Enumeration	BACnet LifeSafetyState	Fire Panel State
Present Value	0	IssQuiet	Normal
	1	IssPreAlarm	PreAlarm
	2	IssAlarm	Fire Alarm, Security Alarm (Life/Property), Critical Process Alarm, (Life/Property), Medical Emergency, IB Smash Glass, Panic Alarm
	3	IssFault	Security Trouble, Fire Trouble, Non-Fire Trouble, Fire Device or Zone, Disabled, Non-Fire Device Disabled
	7	IssActive	Non-Fire Activation
	22	IssSupervisory	Supervisory (Equipment), Supervisory (Guard's Tour)
Tracking Value	0	IssQuiet	Normal
	1	IssPreAlarm	PreAlarm
	2	IssAlarm	Fire Alarm, Security Alarm (Life/Property), Critical Process Alarm (Life/Property), Medical Emergency, IB Smash Glass, Panic Alarm
	3	IssFault	Security Trouble, Fire Trouble, Non-Fire Trouble, Fire Device or Zone, Disabled, Non-Fire Device Disabled
	7	IssActive	Non-Fire Activation
	22	IssSupervisory	Supervisory (Equipment), Supervisory (Guard's Tour)

	BACnet Enumeration	BACnet Event State	Fire Panel State
Event State	0		Normal
	1	EsNormal	Security Trouble, Fire Trouble, Non-Fire Trouble, Fire Device Disabled, Non-Fire Device Disabled
	2	EsOffNormal	All statuses other than normal and fault.

	BACnet Enumeration	BACnet Reliability	Fire Panel State
Reliability	0	reNoFaultDetected	All statuses other than trouble.
	7	re_UnreliableOther	Security Trouble, Fire Trouble, Non-Fire Trouble

	BACnet Enumeration	BACnet Mode	Fire Panel State
Mode	0	IsmOff	Power-Up State
	11	IsmEnabled	Set if point has been disabled and subsequently enabled since startup.
	12	IsmDisabled	Fire Device or Zone Disabled, Non-Fire Device Disabled
Silence State	0	ssUnsilenced	Audibles Unsilenced
	1	ssAudiblesSilenced	Audibles Silenced
Operation Expected	0		N/A
Maintenance Expected	N/A	N/A	N/A

	BACnet Event Transition Bit	BACnet Mode	Fire Panel State
Event Enable		toOffNormal	
		toFault	
		toNormal	
Proprietary Property 1001	REAL	N/A	% Alarm
	REAL	N/A	Drift Compensation Percent (ONYX Series Panels Only)

	Boolean	BACnet Status Flag	Fire Panel State
Status Flags	0,0,0,0	Normal	Normal
	1,0,0,0	InAlarm	Fire Alarm, Security Alarm (Life/Property), Critical Process Alarm (Life/Property), Medical Emergency, PreAlarm, IB Smash Glass, Panic Alarm
	0,1,0,0	Fault	Security Trouble, Fire Trouble, Non-Fire Trouble
	0,0,0,1	OutOfService	Fire Device or Zone Disabled, Non-Fire Device Disabled
	1,0,0,1	InAlarm, OutOfService	If device is in Alarm state (Fire Alarm, Security Alarm (Life/Property), Critical Process Alarm (Life/Property), Medical Emergency, PreAlarm, IB Smash Glass, Panic Alarm) and also device goes to disable state (Fire Device or Zone Disabled, Non-Fire Device Disabled)
	0,1,0,1	Fault, OutOfService	If device is in trouble state (Security Trouble, Fire Trouble, Non-Fire Trouble)and also device goes to disable state (Fire Device or Zone Disabled, Non-Fire Device Disabled)
Out of Service	0	FALSE	All statuses other than disable
	1	TRUE	Fire Device or Zone Disabled, Non-Fire Device Disabled

Standard Object Types Supported - Multi-State Input /Multi-State Output / Multi-State Value

	BACnet Enumeration	BACnet Event State	Fire Panel State
Present Value	1	None	Normal
	2	None	All statuses other than those included in 3 and 4 below.
	3	None	Security Trouble, Fire Trouble, Non-Fire Trouble
	4	None	Fire Device or Zone Disabled, Non-Fire Device Disabled
Event State	0	EsNormal	Normal
	1	EsFault	Security Trouble, Fire Trouble, Non-Fire Trouble, Fire Device Disabled, Non-Fire Device Disabled
	2	EsOffNormal	All statuses other than normal and fault.

	BACnet Enumeration	BACnet Reliability	Fire Panel State
Reliability	0	reNoFaultDetected	All statuses other than trouble.
	7	re_UnreliableOther	Security Trouble, Fire Trouble, Non-Fire Trouble

	Boolean	BACnet Status Flag	Fire Panel State
Status Flags	0,0,0,0		Normal
	1,0,0,0	InAlarm	Fire Alarm, Security Alarm (Life/Property), Critical Process Alarm (Life/Property), Medical Emergency, PreAlarm, IB Smash Glass, Panic Alarm
	0,1,0,0	Fault	Security Trouble, Fire Trouble, Non-Fire Trouble
	0,0,0,1	OutOfService	Fire Device or Zone Disabled, Non-Fire Device Disabled
	1,0,0,1	InAlarm, OutOfService	If device is in Alarm state (Fire Alarm, Security Alarm (Life/Property), Critical Process Alarm (Life/Property), Medical Emergency, PreAlarm, IB Smash Glass, Panic Alarm) and also device goes to disable state (Fire Device or Zone Disabled, Non-Fire Device Disabled)
	0,1,0,1	Fault, OutOfService	If device is in trouble state (Security Trouble, Fire Trouble, Non-Fire Trouble)and also device goes to disable state (Fire Device or Zone Disabled, Non-Fire Device Disabled)
Out of Service	0	FALSE	All statuses other than disable
	1	TRUE	Fire Device or Zone Disabled, Non-Fire Device Disabled

Supported - Binary Output

	BACnet Enumeration	BACnet LifeSafetyState	Fire Panel State
Present Value	0	bpv_InActive	Non-Fire Trouble, Non-Fire Device Disabled, Normal
	1	Bpv_Active	Non-Fire Activation

	BACnet Enumeration	BACnet Event State	Fire Panel State
Event State	0	EsNormal	Normal
	1	EsFault	Non-Fire Trouble, Non-Fire Device Disabled
	2	EsOffNormal	Non-Fire Activation

	BACnet Enumeration	BACnet Reliability	Fire Panel State
Reliability	0	reNoFaultDetected	Non-Fire Activation, Non-Fire Device Disabled, Normal
	7	re_UnreliableOther	Non-Fire Trouble

	Boolean	BACnet Status Flag	Fire Panel State
Status Flags	0,0,0,0	Normal	Normal
	1,0,0,0	InAlarm	Non-Fire Activation
	0,1,0,0	Fault	Non-Fire Trouble
	0,0,0,1	OutOfService	Non-Fire Device Disabled
	1,0,0,1	InAlarm, OutOfService	If device is in Alarm state (Non-Fire Activation) and also device goes to disable state (Non-Fire Device Disabled)
	0,1,0,1	Fault, OutOfService	If device is in trouble state (Non-Fire Trouble) and also device goes to disable state (Non-Fire Device Disabled)
Out of Service	0	FALSE	All statuses other than disable
	1	TRUE	Non-Fire Device Disabled

Supported - Binary Value Object

	BACnet Enumeration	BACnet Event State	Fire Panel State
Present Value	0	bpv_InActive	Trouble, Device Disabled, Normal
	1	Bpv_Active	
Event State	0	EsNormal	Normal
	1	EsFault	Trouble, Device Disabled
	2	EsOffNormal	Activation

	BACnet Enumeration	BACnet Reliability	Fire Panel State
Reliability	0	reNoFaultDetected	Activation, Device Disabled, Normal
	7	re_UnreliableOther	Trouble

	Boolean	BACnet Status Flag	Fire Panel State
Status Flags	0,0,0,0		Normal
	1,0,0,0	InAlarm	
	0,1,0,0	Fault	
	0,0,0,1	OutOfService	Device Disabled
	1,0,0,1	InAlarm, OutOfService	If device is in Alarm state (Activation) and also device goes to disable state (Device Disabled)
	0,1,0,1	Fault, OutOfService	If device is in trouble state (Trouble) and also device goes to disable state (Device Disabled)
Out of Service	0	FALSE	All statuses other than disable
	1	TRUE	

Supported – Group Object

This Object type is only supported for Interface devices. Interface devices consist of multiple channels (Maximum 12 channels). Interface device comes under Group object and channels are created as MSI/MSO object.

List Of Group Members	**Fire Panel State**
	This property holds the interface device channel objects (MSI/MSO)
Present Value	**Fire Panel State**
	This property holds the interface device channel objects (MSI/MSO) present values. It is an array.

Standard Object Types Supported -NotificationClass

Write Property/Add List element required for Intrinsic Reporting.

Data Link Layer Options:

☑ BACnet IP, (Annex J)

☑ BACnet IP, (Annex J), Foreign Device ISO 8802-3, Ethernet (Clause 7)

☐ ANSI/ATA 878.1, 2.5 Mb. ARCNET (Clause 8)

☐ ANSI/ATA 878.1, RS-485 ARCNET (Clause 8), baud rate(s)

☐ MS/TP MASTER (Clause 9), baud rate(s)

☐ MS/TP SLAVE (Clause 9), baud rate(s)

☐ Point-To-Point, EIA 232 (Clause 10), baud rate(s)

☐ Point-To-Point, modem, (Clause 10), baud rate(s)

☐ LonTalk, (Clause 11), medium

☐ Other

B.10.1 Device Address Binding

Is static device binding supported?

(This is currently necessary for two-way communication with MS/TP slaves and certain other devices.)

☑ Yes

☐ No

B.10.2 Networking Options

Router, Clause 6 - List all routing configurations, e.g., ARCNET-Ethernet, Ethernet-MS/TP, etc. BACnet to Proprietary ARCnet Fire Network

Annex H, BACnet Tunneling Router over IP BACnet Broadcast Management Device (BBMD)

Does the BBMD support registrations by Foreign Devices?

Yes ☑ No

B.10.3 Character Sets Supported

Indicating support for multiple character sets does not imply that they can all be supported simultaneously.

☑ ANSI X3.4

☐ IBM/Microsoft DBCS

☐ ISO 8859-1

☐ ISO 10646 (UCS-2)

☐ ISO 10646 (ICS-4)

☐ JIS C 6226

B.10.4 Supported Non-BACnet Equipment/Networks

This product supports communications between NOTIFIER®/GENT® Fire Panels and Annunciator nodes compatible with network v 5.0 and later operating in a network or stand-alone configuration.

This product supports communications between VESDA Detectors and other nodes compatible with VESDAnet.

8.13.1.2 Equations for Object IDs (Instance Numbers)

Standard Addressing – Device Object Instance Number (Default):

> **NOTE:** NOTIFIER panels use this addressing method.

In the CLSS BACNET-GW, each node has 15,000 object IDs available to it. For each node, multiply its node number by 15,000 and add the offset calculated below based on what type of point it is. These numbers define the 22 bits of the BACnet Object Identifier field.

Examples:

Node 15, L01D025 -> (15 x 15000) + ((1 - 1) x 1000) + (25 - 1) = 225024

Node 201, L02M014 -> (201 x 15000) + ((2 - 1) x 1000) + (14 + 299) = 3016213

Node 114, Annunciator 001 -> (114 x 15000) + (1 + 699) = 1711699

Node 20, ZONE0002 -> (20 x 15000) + (2 + 10000) = 310002

Flexible Addressing – Device Object Instance Number:

This is used by GENT panels. It is a default option for GENT panels.

For each node, use following formula to get base address **Gateway ID + X + 1 .** Here X Initial value is zero and will get incremented for each panel. Add the offset calculated below based on what type of point it is. These numbers define the 22 bits of the BACnet Object Identifier field.

> **NOTE:** Gateway ID is user configurable. Gateway ID + X + 1 should be in the range 0 to 4194303. If there are multiple gateways make sure that one gateway range (Gateway ID + X + 1) is not conflicting with other.

Examples:

GatewayID 1,Node 15 (First Panel Discovered), L01D025 ,
1+1+ 1+ ((1 - 1) x 1000) + (25 - 1) = 27

GatewayID 1, Node 201 (Second panel discovered), L03M014,
1+2+1+((3 - 1) x 1000) + (14 + 299) = 2317

Below point offset equations related to points or devices under a panel is common for standard addressing and flexible addressing.
Detectors = ((Loop - 1) x 1000) + (Detector Address - 1)
Modules = ((Loop - 1) x 1000) + (Module Address + 299) + Panel#

SECTOR (Multi State Output)
(((Loop - 1) * 50) + Sector Address + 16000)

Interface Device (Group Object)
Detectors = ((Loop - 1) x 1000) + (Detector Address - 1)
Modules = ((Loop - 1) x 1000) + (Module Address + 299) + Panel#
Example:
L01D200 = ((Loop - 1) x 1000) + (Detector Address - 1) = 0 + 199 = GO199

IO channels (Multi State Input or Multi State Output)
((Loop - 1) x 3000) + 18000 + ((#Point_Address - 1) * 12) + #CHANNEL_ADDR (1 to 12)
Example:
L01D200 Channel 1, -> ((1-1) x 3000) + 18000 + ((200 - 1) * 12) + 1 = MSO20389
L01D200 Channel 2, -> ((1-1) x 3000) + 18000 + ((200 - 1) * 12) + 2 = MSO20390
L01D200 Channel 12, -> ((1-1) x 3000) + 18000 + ((200 - 1) * 12) + 12 = MSI20400

Panel Circuits (BINARY_OUTPUT)
(Panel# x 10) + (circuit# - 1) + 650

Bell Circuits or NAC Circuits (BINARY_OUTPUT)
(BELL_CIRCUIT# + 790)

Zones (MULTI_STATE_INPUT or LIFE_SAFETY_ZONE)
ZONE (1-2000) => (ZONE# + 10000)
Logic Zones (MULTI_STATE_INPUT or LIFE_SAFETY_ZONE)
LZONE (1-2000) => (LZONE# + 12000)
Special Zones (MULTI_STATE_INPUT or LIFE_SAFETY_ZONE)
FZONE (0-47) => (FZONE# + 14000)
Trouble Zones (MULTI_STATE_INPUT or LIFE_SAFETY_ZONE)
TZONE (1-99) => (TZONE# +14100)
Releasing Zones (MULTI_STATE_INPUT or LIFE_SAFETY_ZONE)
RZONE (0-9) => (RZONE# + 14050)
Command Build(BINARY_VALUE)
#COMMAND_BUILD_NUM + 15000
DAA Speaker Circuit
(DAA# - 1) x 4 + (Spk# - 1) + 2600

AFP 2800 Specific

// AZF 1 and 2
(AZF# + 3600)

// R00M003I 1-4
(R00M003I# + 3602)

// Relays 1 through 8
(Relay# + 3606)

// XR Relays 1-64
(XR Relay# + 3620)

System Troubles or Generic Panel Points

(System Trouble# + 14200)
800 addresses are dedicated to system troubles or generic panel points. Bucketized the troubles as mentioned below.

Generic Panel Points

System Trouble Object	Count	Address	Point Type
PMB 1-5	5	1-5	MSI/LSP
AIO 1-12	12	6-17	MSI/LSP
PANEL	1	18	MSI/LSP
RESET	1	19	MSI/LSP
NETWORK_A	1	20	MSI/LSP
NETWORK_B	1	21	MSI/LSP
CPU	1	22	MSI/LSP
GROUND	1	23	MSI/LSP
BATTERY	1	24	MSI/LSP
ACPOWER	1	25	MSI/LSP
WALKTEST	1	26	MSI/LSP
LOOP 1-10	10	27-36	MSI/LSP

System Trouble Object	Count	Address	Point Type
ANNUN 1-32	32	37-68	MSI/LSP
DBUS 1-4	4	69-72	MSI/LSP
PRIMARY AMP 1-4	4	73-76	MSI/LSP
BACKUP AMP 1-4	4	77-80	MSI/LSP
BACKUP AMP	1	81	MSI/LSP
DAL	1	82	MSI/LSP
POTS	1	83	MSI/LSP
POTS1	1	84	MSI/LSP
POTS2	1	85	MSI/LSP
CELLULAR	1	86	MSI/LSP
ETH1	1	87	MSI/LSP
ETH2	1	88	MSI/LSP
ETH-WIFI	1	89	MSI/LSP
CLSS CLOUD	1	90	MSI/LSP
ZONE LICENSE	1	91	MSI/LSP
NETWORK DISPLAY LICENSE	1	92	MSI/LSP
LICENSE	1	93	MSI/LSP
AUDIO LIBRARY	1	94	MSI/LSP
DATABASE	1	95	MSI/LSP
VOICE	1	96	MSI/LSP
LIMIT EXCEED	1	97	MSI/LSP
MIC	1	98	MSI/LSP
PHONE	1	99	MSI/LSP
AMPLIFLIER	1	100	MSI/LSP
FFT	1	101	MSI/LSP
HISTORY	1	102	MSI/LSP
CHARGER	1	103	MSI/LSP
MASTER ALARM 1	1	104	MSV
MASTER ALARM 2	1	105	MSV
PSU	1	106	MSI/LSP
AUXILIARY RELAY 1	1	107	MSV
AUXILIARY RELAY 2	1	108	MSV
MONITORED INPUT	1	109	MSI/LSP

Input, Output, and ZoneNotify (NOTIFICATION_CLASS)

These objects will always be the same object ID on each device. You do not need to add the Node Number offset.

INPUTNOTIFY = 1
OUTPUTNOTIFY = 2
ZONENOTIFY = 3

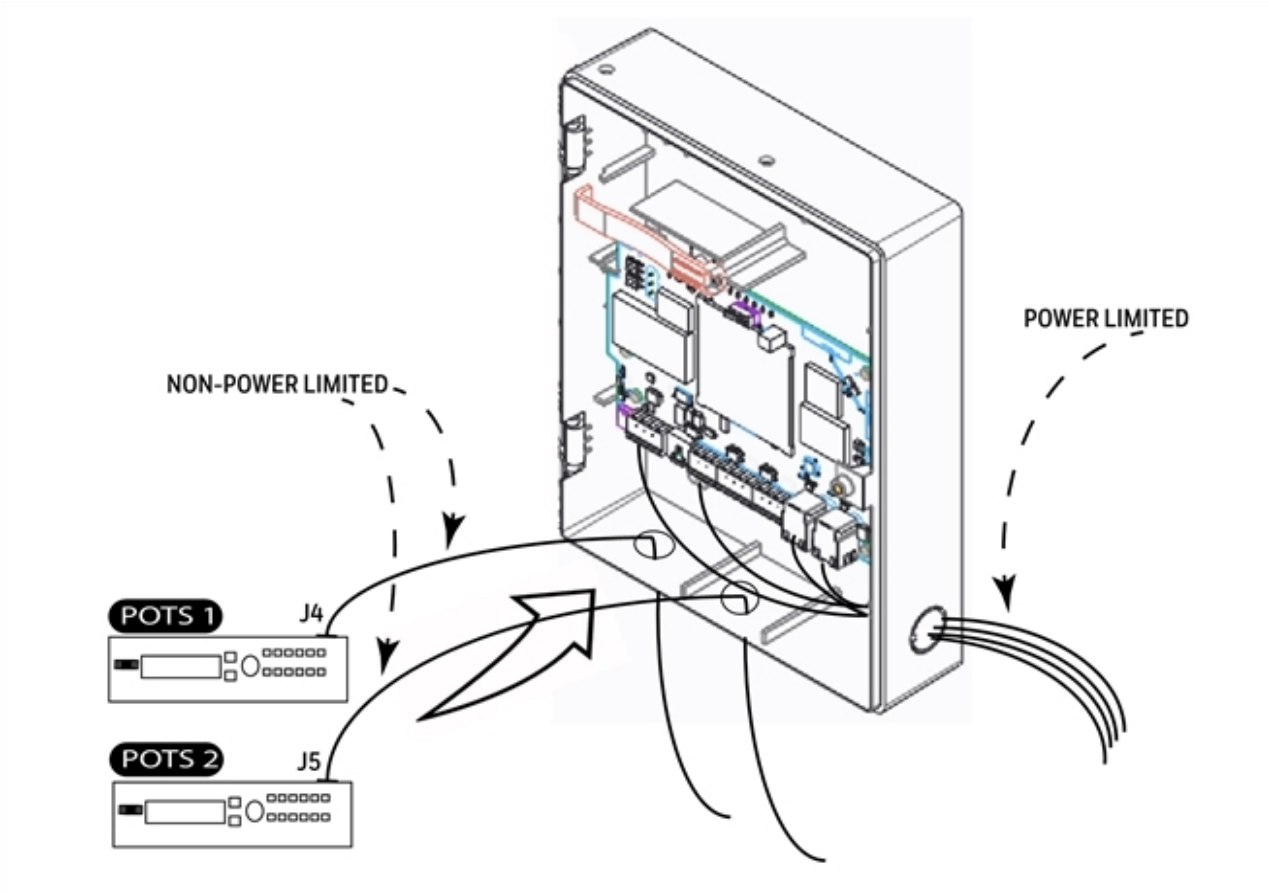
APPENDIX A: GATEWAY OPERATING CONDITIONS

Table A.1 Operational Requirements

Power Requirements	
Working voltage range	18V - 30V DC
Current	For HON-CGW-DACT: 180mA (maximum) For HON-CGW-MBB: 140mA (maximum) **NOTE**: The power requirement varies with the number of interfaces used.
Location Requirements	
Room Temperature	15 - 27° C (60 - 80° F)
Operational Temperature	0°C - 49°C (32°F - 120°F)
Relative humidity	93% ± 2% RH (Non-condensing) at 32°C ± 2°C (90° F ± 3°F)

CAUTION: Extreme temperature ranges and humidity may adversely affect the useful life of the system's standby batteries and the electronic components. Therefore, it is recommended that this system and its peripherals be installed in an environment with a normal room temperature of 15 - 27° C (60 - 80° F).

A.1 WIRINGS AND POWER



APPENDIX B: MODULATIONS AND POWER USED

Radio devices operating on the below frequencies should not be installed next to each other.

Target Power that Meets Spectrum Mask and EVM Compliance

Table B.1
Table B.1 Wireless Power Specifications

2.4 GHz TX Power Specifications							
IEEE 802.11	**Mod**	**Rate**	**BW**	**Channel**	**Spec (TYP)**	**Units**	**Tol. (dB)**
11b	CCK, DSSS	1 to 11 Mbps	20 MHz	1-13	17.5	dBM	+/-2.0
11g	OFDM	6 to 54 Mbps	20 MHz	1-13	15	dBM	+/-2.0
11n	OFDM	MCS 0-7	20 MHz	1-13	15	dBM	+/-2.0
5 GH z TX Power Specifications							
Std	**Mod**	**Rate**	**BW**	**Channel**	**Spec (TYP)**	**Units**	**Tol. (dB)**
11a	OFDM	6-54 Mbps	20 MHz	36-48 52-64 100-144	15	dBM	+/-2.0
11n	OFDM	MCS 0-7	20 MHz	36-48 52-64 100-144	15	dBM	+/-2.0

APPENDIX C: CONNECTING TO THE PANELS

C.1 GATEWAY BOARD CONNECTIONS

The gateway board can connect with a cellular module, wireless aerials, the *CLSS Site Manager*, a configuration computer, a panel, a mobile device, and an external power supply.
"Gateway Connections - Top Side" below illustrates the connection options at the top side of the gateway board.

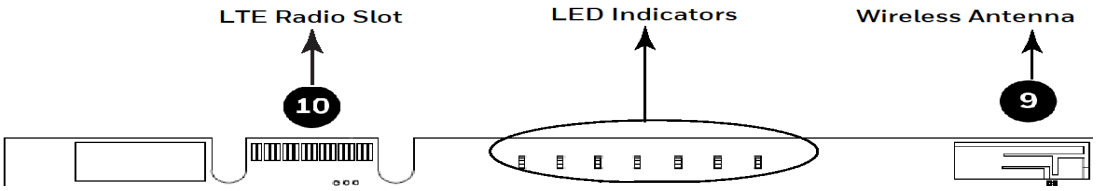


Figure C-1: Gateway Connections - Top Side

"Gateway Connection Options - Bottom Side" below illustrates the gateway connection options at the bottom side of the gateway board.

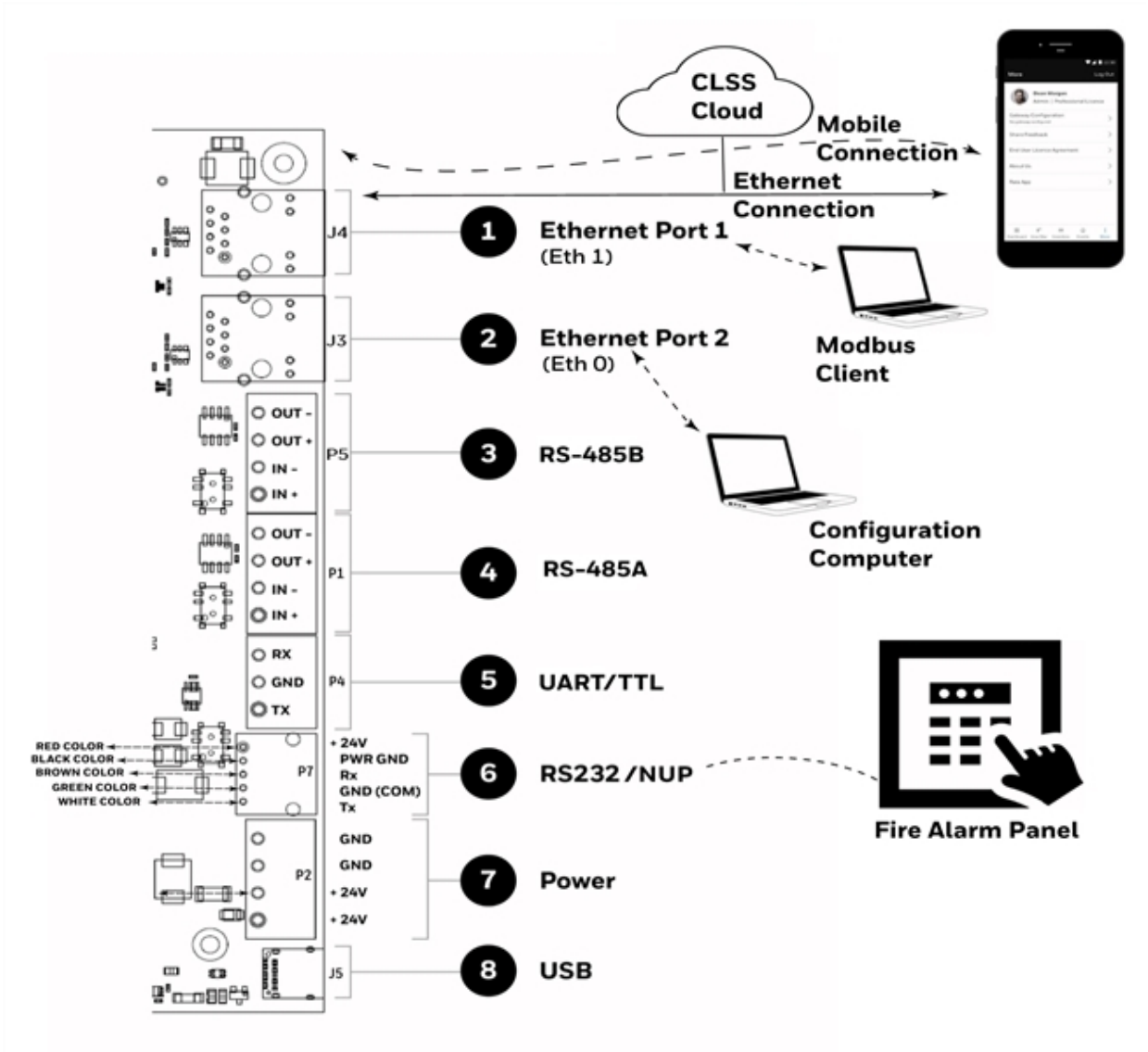


Figure C-2: Gateway Connection Options - Bottom Side

C.1.1 CONNECTING TO A FIRE ALARM PANEL

The panel sends data from all its devices to the connected CLSS Gateway. The data transmission is based on the connection type and the panel compatibility.

While the gateway is working do not remove connections to the gateway, *CLSS Site Manager*, and the panel.

When the gateway is communicating to a central station through cellular connection, it uses the primary Ethernet connection for *CLSS Site Manager* communications.

The interfaces of the gateway board and the panels must be connected only with compatible cables, devices, and wirings.

The total power a panel can distribute among its connected devices is limited. Therefore, before connecting the CLSS Gateway to a panel, ensure that the panel can continue to supply the required power to the gateway as well as other connected peripherals. Refer to the panel and other peripherals' documents to know their power requirements.

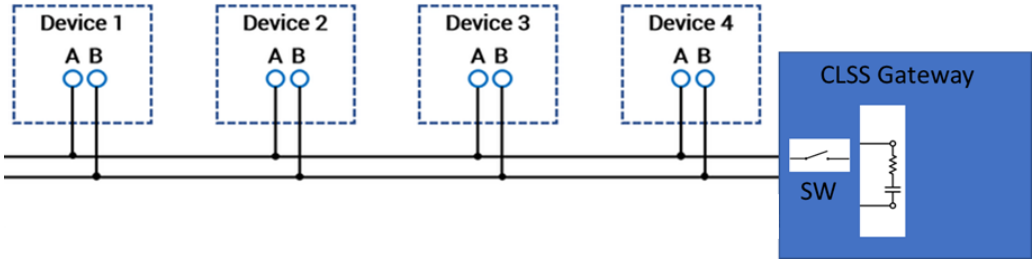
C.1.2 IMPROVING THE SIGNAL FIDELITY

An RS-485 loop of a panel with long cable and multiple devices may affect the signal fidelity. The gateway at the end of such an RS-485 loop can improve the signal fidelity with its termination resistor.

To enable the termination resistor on the gateway board:

If RS-485A is connected, switch the S4 switch to ON. If RS-485B is connected, switch the S5 switch to ON.

When there are no signal issues or when the gateway is not at the end of the loop, ensure that the S4 and S5 switches are switched to OFF.



C.2 SUPPORTED PANELS

The CLSS Gateway supports the following panel variants:

- C.3 ESSER Panels
- C.4 Farenhyt Panels
- C.5 Fire-Lite® Panels
- C.6 FireWarden Panels
- C.7 Gamewell-FCI Panels
- C.8 Gent Panels
- C.9 Morley-IAS Panels
- C.12 NOTIFIER® UL
- C.13 NOTIFIER® European Panels (EN)
- C.15 AM Series Panels
- C.16 Triga Panels
- C.17 VESDA® Detectors

C.3 ESSER PANELS

A *remote access* connection on RS-232 provides *inventory synchronization*. A *WINMAG* connection on RS-232 or on RS-485 provides *active events*.

You can have either the *remote access* connection or the *WINMAG connection* or both.

Refer to "To Make a Remote Access Connection on RS-232" below for the *remote access* connection on RS-232. Refer to "To Make a WINMAG Connection on RS-232" on page 147 for the WINMAG connection.

C.3.1 CONNECTION OPTIONS

The gateway operates only with the ESSER fire alarm control panels listed in the table below:

Table C.1 ESSER Panel Connection Options

Fire Alarm Panel Models	RS-485	UART/TTL	RS-232	USB
ESCOM	No	No	Yes	No
FlexES Control	Yes	No	Yes[1]	No
IQ8Control C	Yes[2]	No	Yes[1 or 3]	No
IQ8Control M	Yes[2]	No	Yes[1 or 3]	No
CMSI	No	No	No	Yes[4]

[1]Use a TTY-RS-232 converter (764856.10).
[2] Use the RS-485 module (784871) along with SEI-2 Card (Serial Essernet® Interface) (784850).
[3]Use the RS-232 module (772386) along with SEI Card (Serial Essernet® Interface) (784856).Use the OTG to RS232 converter (CLSS-CMSI-USB)
[4]Use the add-on I/O card (VIG-IOC-DOM) on the panel

C.3.2 MINIMUM REQUIRED VERSIONS

- ESCOM Panel: 02.06.011
- FlexES Panel: 4.07R001
- IQ8 Panel: 03.13R000
- CMSI8000 Panel: 4.06
- CLSS Gateway: 3.1.4.78

C.3.3 TO MAKE A REMOTE ACCESS CONNECTION ON RS-232

Using an RS-232 cable, you can connect to the TTY port of the panel's serial interface.

On the Gateway Side

Connect the RS-232 cable with pre-formed connector to the RS-232 port of the gateway board.
The RS-232 port in the gateway board is labeled as 6 in the "Gateway Connection Options - Bottom Side" on page 142.

On the TTY-RS-232 Converter Side

From the gateway:

- Connect the Rx wire to the Tx pin of the TTY-RS-232 converter.
- Connect the Tx wire to the Rx pin of the TTY-RS-232 converter.

On the Panel Side

- For FlexES Panels
- For IQ8 Panels

For FlexES Panels

Connect as below:

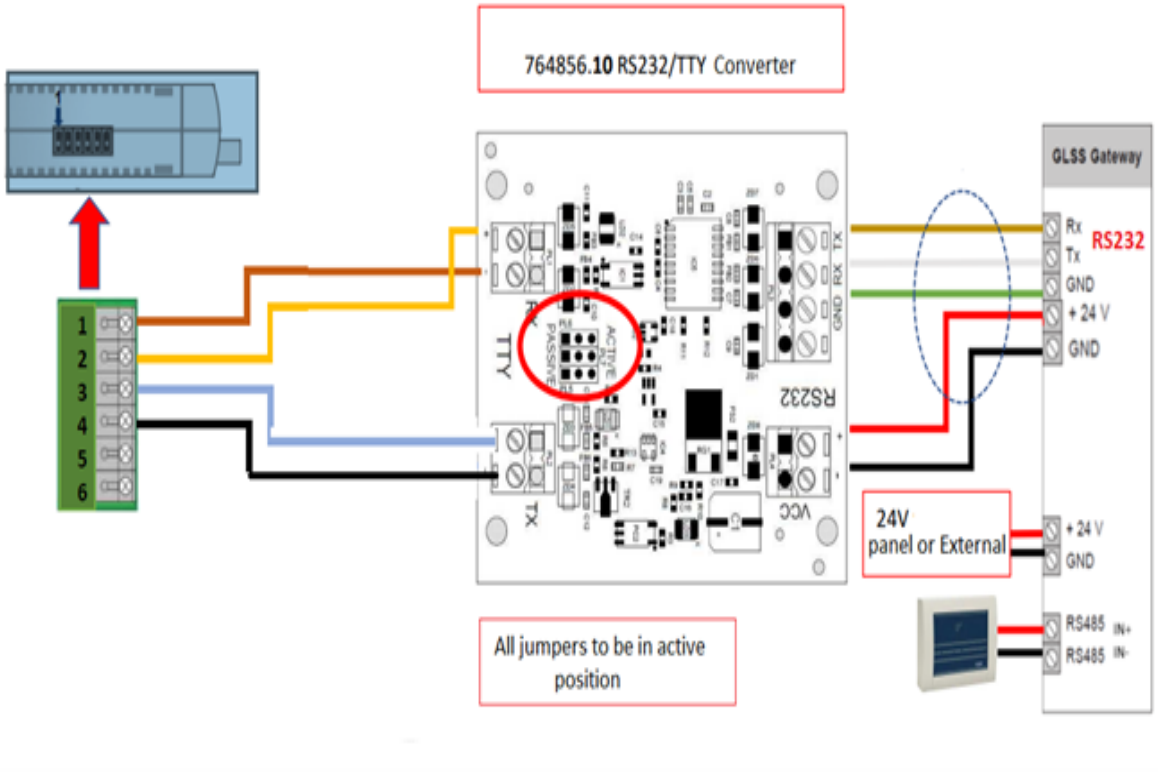
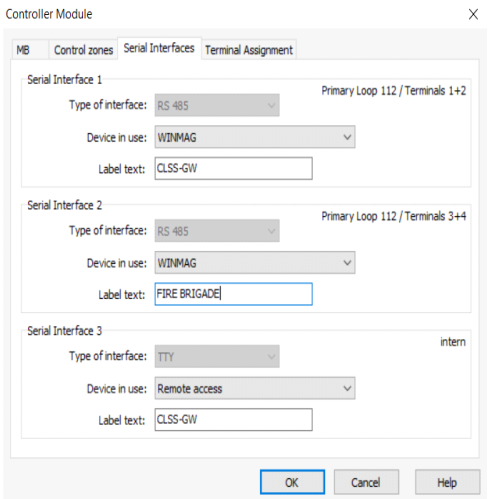


Figure C-3: RS-232 Connection on a FlexES Panel

Tools 8000 Settings for FlexES Panels

01. Select the **Serial Interfaces** tab in Tools 8000.
02. Go to the **Serial Interface 3** section.
03. Select *Remote Access* from the **Device in use** list.
04. Click **OK**.



For IQ8 Panels

Using an RS-232 cable, you can connect to the RS-232 port on the panel's serial interface.

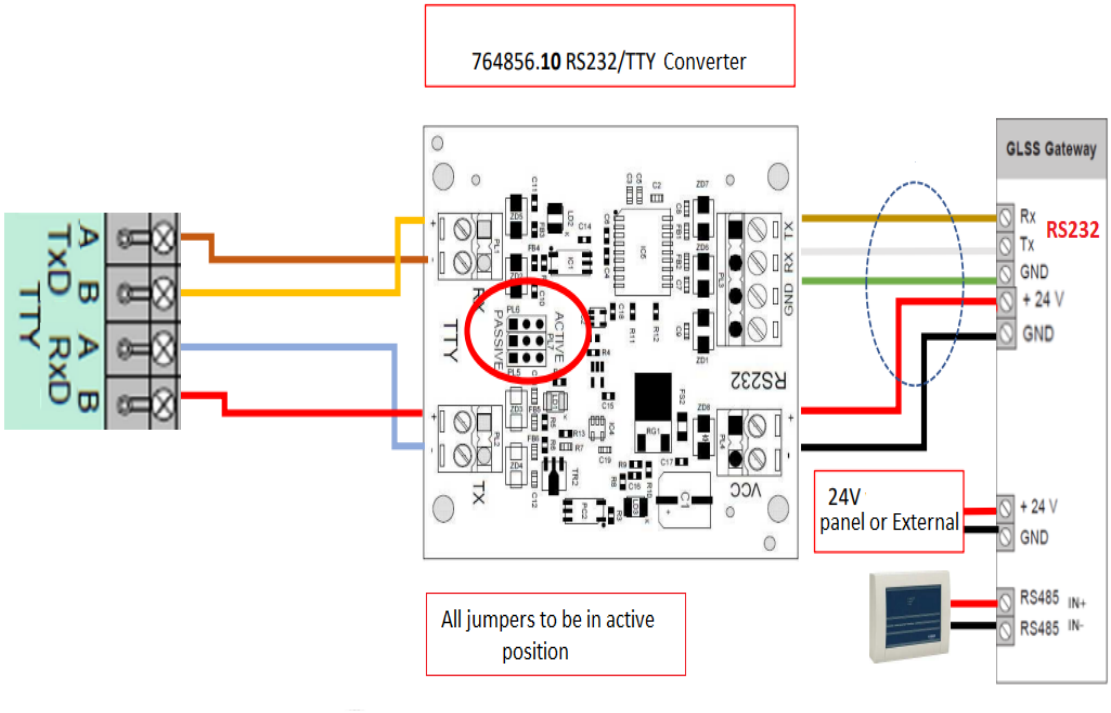
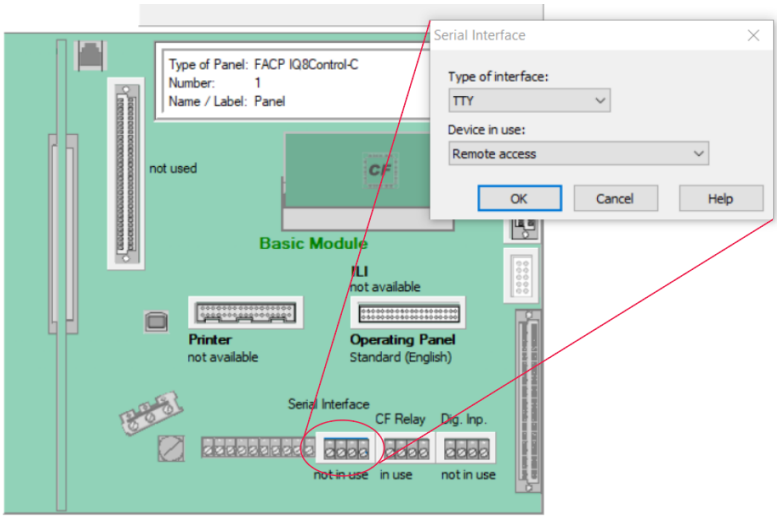


Figure C-4: RS-232 Connection on an IQ8 Panel

Tools 8000 Settings for IQ8 Panels

01. Double click on **Serial Interface** in Tools 8000.
02. Select *RS-232* from the **Type of interface** list.
03. Select *Remote Access* from the **Device in use** list.
04. Click **OK**.



C.3.4 TO MAKE A WINMAG CONNECTION ON RS-232

Using an RS-232 cable the CLSS Gateway and the panel are connected.

The RS-232 port in the gateway board is labeled as 6 in the "Gateway Connection Options - Bottom Side" on page 142.

On the Gateway Side

Connect to an RS-232 port of the gateway board.

On the Panel Side

• For ESCOM Panels

For ESCOM Panels

• Connect the White wire to the RxD+ pin.
• Connect the Brown wire to the TxD+ pin.
• Connect the Green wire to the 0V pin.

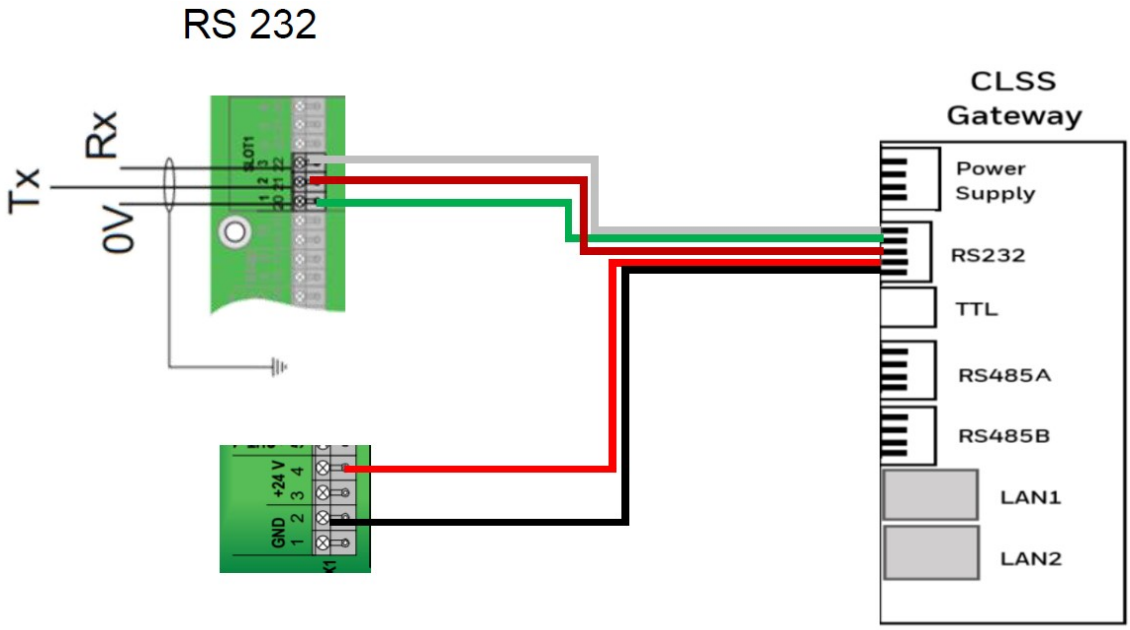


Figure C-5: Wiring Diagram: RS232 Connection for an ESCOM Panel

C.3.4.1 Power Connection

Using the RS-232 cable, the gateway can connect to the 24V DC power supply module of the ESCOM panel.

NOTE: Use the details given on the power supply module of the panel.

NOTE: The panel's power supply to the gateway must be within +24V DC power.

On the Gateway Side

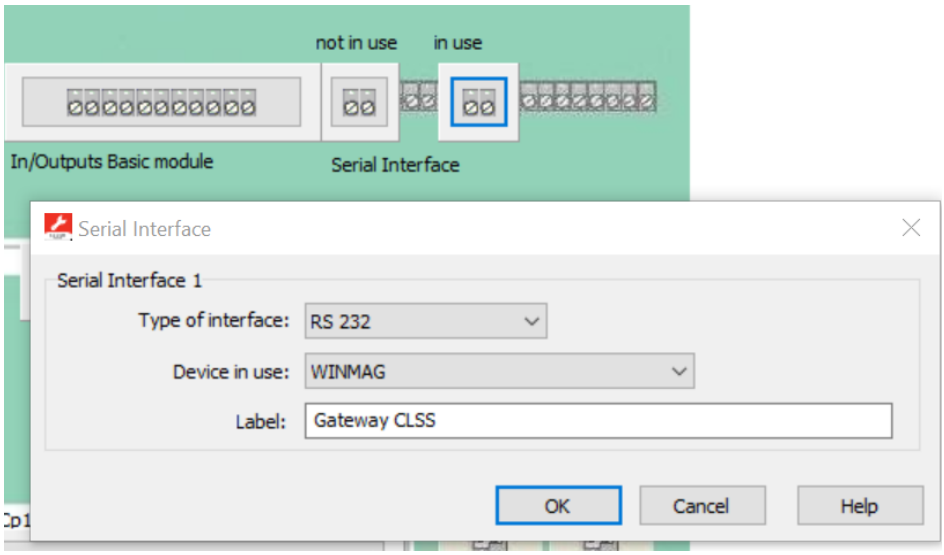
• Connect the +ve wire to the +ve pin of the power supply port.
• Connect the -ve wire to the -ve pin of the power supply port.

On the Panel Side

• Connect the +ve wire to the +24 pin of the power supply module.
• Connect the -ve wire to the Gnd pin of the power supply module.

Tools 8000 Settings for ESCOM Panels

01. Select the **Serial Interfaces** tab on Tools 8000.
02. Click **in use**.
03. Go to the **Serial Interface 1** section in the **Serial Interface** dialog.
04. Select *RS 232* from the **Type of Interface** list.
05. Select *WINMANG* from the **Device in use** list.
06. Enter the gateway name in the **Label** field.
07. Click **OK**.



C.3.5 IQ8(FRENCH VERSION) PANEL CONNECTION DIAGRAM USING RS232

This connection is applicable for panel versions. Serial interface module to be used for enabling the connection and its part number – 784842.F0

IQ8C M-512 without UGA	808296F
IQ8C M-RACK 512 without UGA	808295F
IQ8C µ-512 with UGA	808297F
IQ8C µ-RACK with UGA	808298F

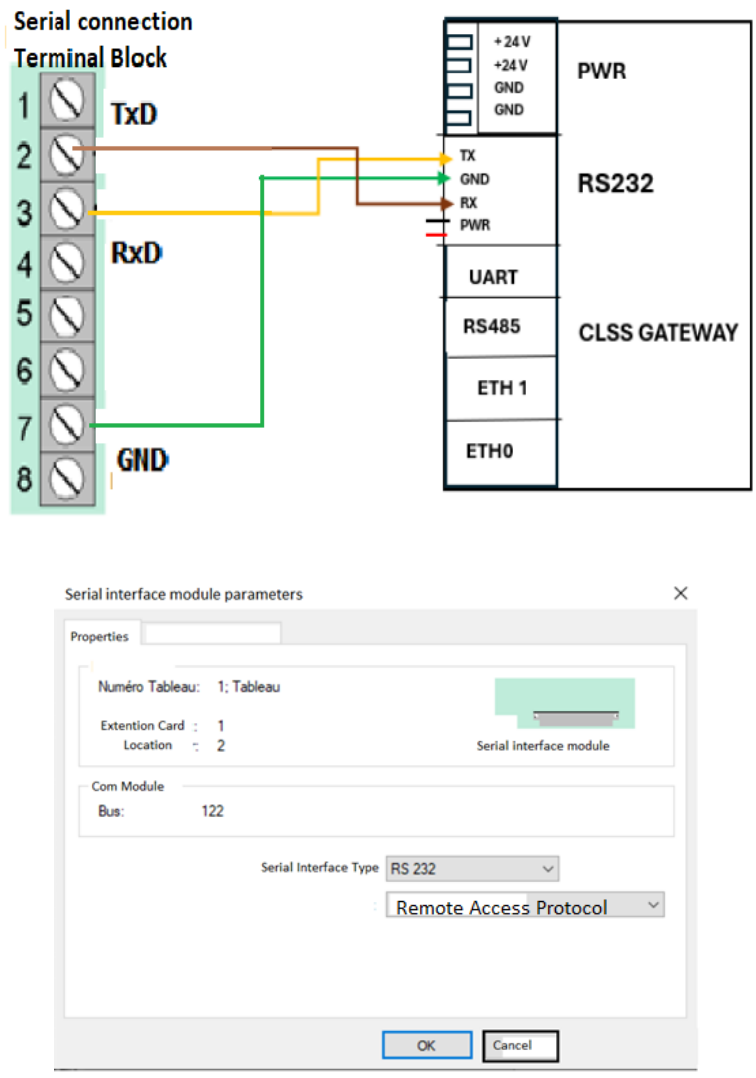


Figure C-6: Wiring Diagram: RS232 Connection for an IQ8 Panel

C.3.5.1 Power Connection

For FlexES Panels

Using a power cable, the gateway can connect to the 24V DC power supply module of the FlexES panel.

> **NOTE:** Use the details given on the power supply module of the panel.

> **NOTE:** The panel's power supply to the gateway must be within +24V DC power.

On the Gateway Side

- Connect the +ve wire to the +ve pin of the power supply port.
- Connect the -ve wire to the -ve pin of the power supply port.

On the Panel Side

- Connect the +ve wire to the +Ub pin of the power supply module.
- Connect the -ve wire to the Gnd pin of the power supply module.

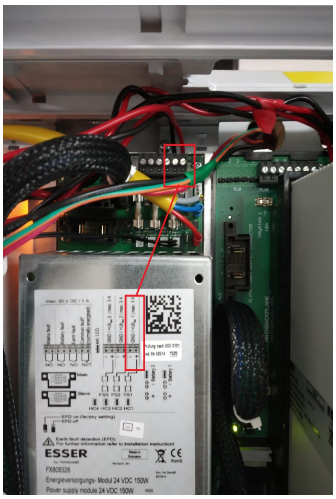
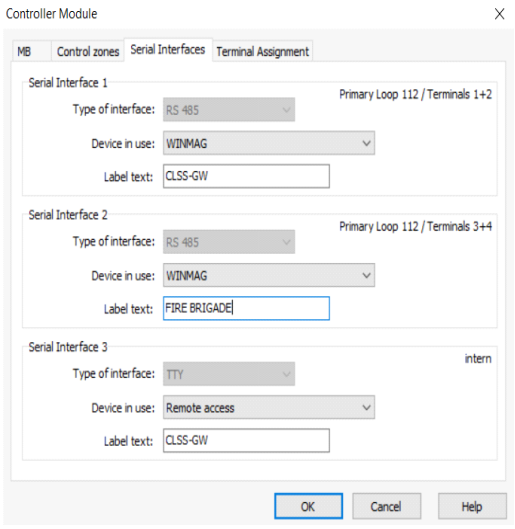


Figure C-7: FlexES Panel Power Connectors

Tools 8000 Settings for FlexES Panels

01. Select the **Serial Interfaces** tab in Tools 8000.
02. Go to the **Serial Interface 1** section.
03. Select *WINMANG* from the **Device in use** list.
04. Go to the **Serial Interface 3** section.
05. Select *Remote Access* from the **Device in use** list.
06. Click **OK**.



C.3.6 TO MAKE A WINMAG CONNECTION USING AN SEI 2 CARD

Using an RS-485 cable, you can connect to the additional RS-485 module (784871) on the panel's serial interface port.

The RS-485 ports in the gateway board are labeled as 3 and 4 in the Figure C-2: Gateway Connection Options - Bottom Side .

On the Gateway Side

Connect to an RS-485 port of the gateway board.

On the Panel Side

• For IQ8 Panels

For IQ8 Panels

Using an SEI2 Card Connect to the RS-485 (784871) module in the panel as below:

In the RXD port of the panel's SEI-2 card:

- Connect the In+ wire to the RXD+ pin.
- Connect the In- wire to the RXD- pin.

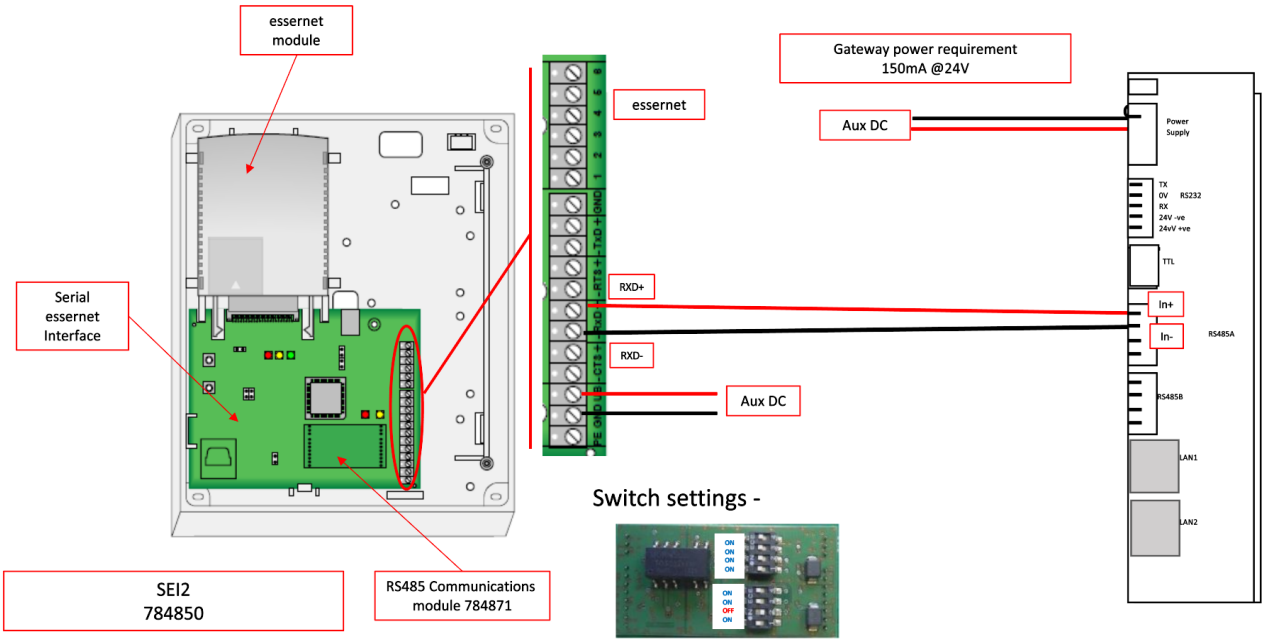


Figure C-8: Wiring Diagram: RS-485 to SEI2 Connection

C.3.7 POWER CONNECTION

Using a power cable, the gateway can connect to the 12V DC power supply module of the panel.

> **NOTE:** Although the gateway is capable of receiving 24V DC power, it can work with the 12V DC power of the IQ8 panel. Ensure that the power supply to the gateway is within +12V DC power.

On the Gateway Side

- Connect the +ve wire to the +ve pin of the power supply port.
- Connect the -ve wire to the -ve pin of the power supply port.

On the Panel Side

- Connect the +ve wire to the +UBext pin of the SEI-2 card.
- Connect the -ve wire to the GND pin of the SEI-2 card.

C.3.8 POWER CONNECTION

Using a power cable, the gateway can connect to the 12V power supply module of the IQ8 panel.

> **NOTE:** Use the details given on the power supply module of the panel.

> **NOTE:** Although the gateway is capable of receiving 24V DC power, it can work with the 12V DC power of the IQ8 panel. Ensure that the power supply to the gateway is within +12V DC power.

On the Gateway Side

- Ensure that the RS-232 cable is connected in the RS-232 port of the gateway.
- Switch the S7 Switch next to the RS-232 port towards *NUP_IN*.

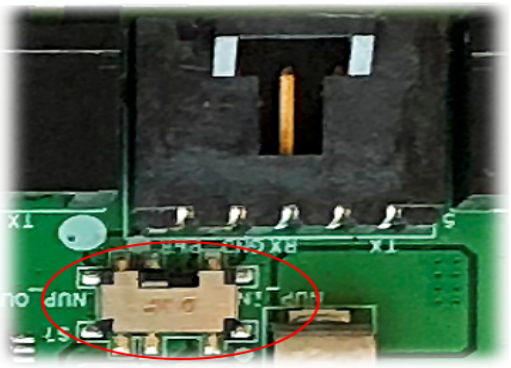


Figure C-9: The S7 Switch

On the Panel Side

- Connect the +ve wire to the +Ub pin of the SEI card.
- Connect the -ve wire to the Gnd pin of the SEI card.

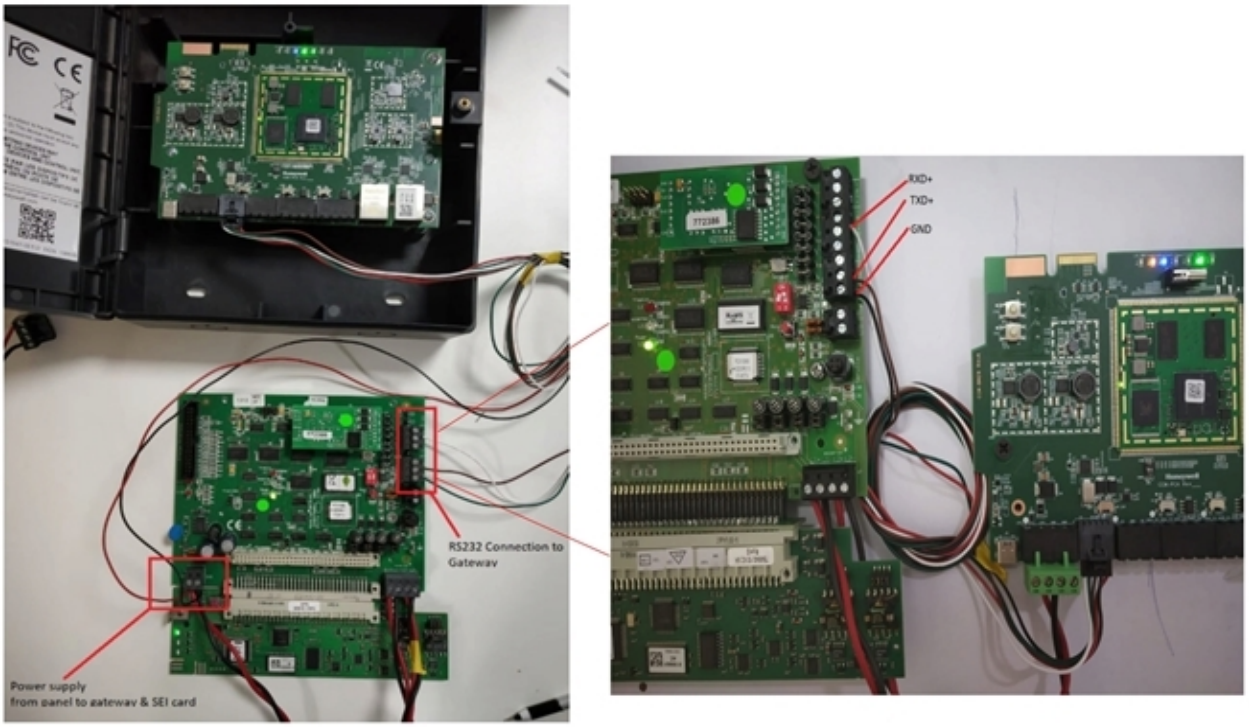


Figure C-10: IQ8 Panel RS-232 Power Connectors

C.3.9 TO MAKE A WINMAG CONNECTION ON RS-485

Using an RS-485 cable the CLSS Gateway and the panel are connected.

The RS-485 ports in the gateway board are labeled as 3 and 4 in the "Gateway Connection Options - Bottom Side" on page 142.

On the Gateway Side

Connect to an RS-485 port of the gateway board.

On the Panel Side

- For FlexES Panels
- C.3.6 To Make a WINMAG Connection Using an SEI 2 Card

For FlexES Panels

- Connect the +ve wire to the Terminal 1 of the panel.
- Connect the -ve wire to the Terminal 2 of the panel.

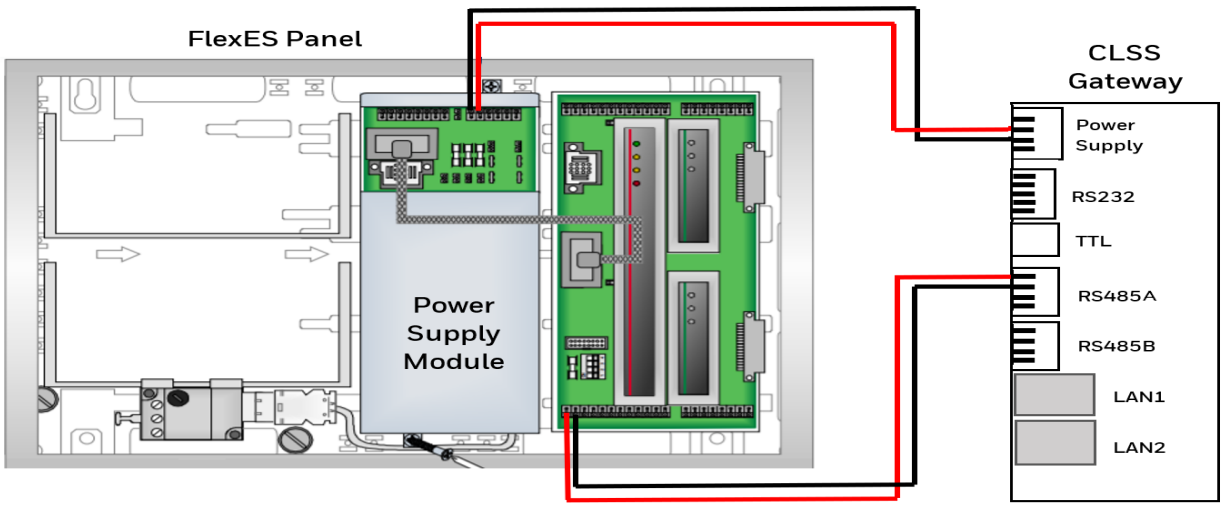
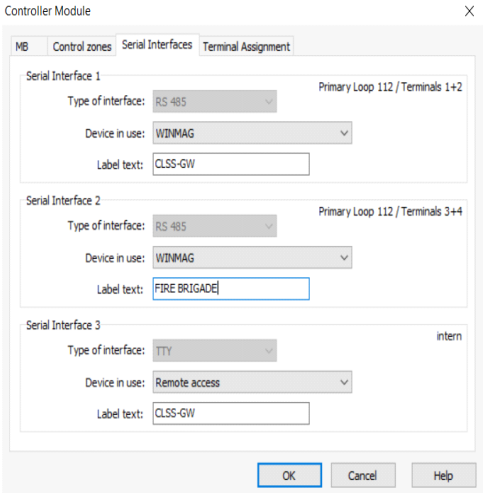


Figure C-11: Wiring Diagram: RS-485 Connections for a FlexES Panel

Tools 8000 Settings for FlexES Panels

01. Select the **Serial Interfaces** tab on Tools 8000.
02. Go to the **Serial Interface 1** section.
03. Select *WINMANG* from the **Device in use** list.
04. Click **OK**.
05. Go to the **Serial Interface 3** section.
06. Select *Remote Access* from the **Device in use** list.



C.3.10 TO MAKE A CMSI CONNECTION USING AN OTG-RS232 CABLE

Using an OTG-RS232 cable, connect the CLSS Gateway and the panel as shown in Figure C-12: CMSI Connections .

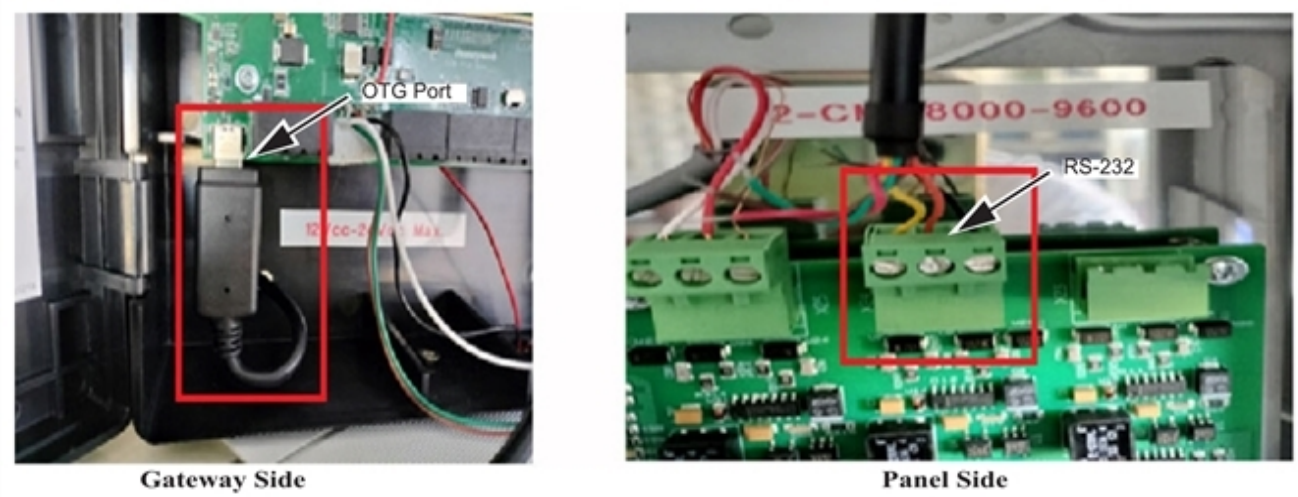


Figure C-12: CMSI Connections

CMSI 8000 Settings for CMSI Panel

• Add the UAE settings on the panel and enable them as shown in Figure C-13: CMSI Panel Settings .

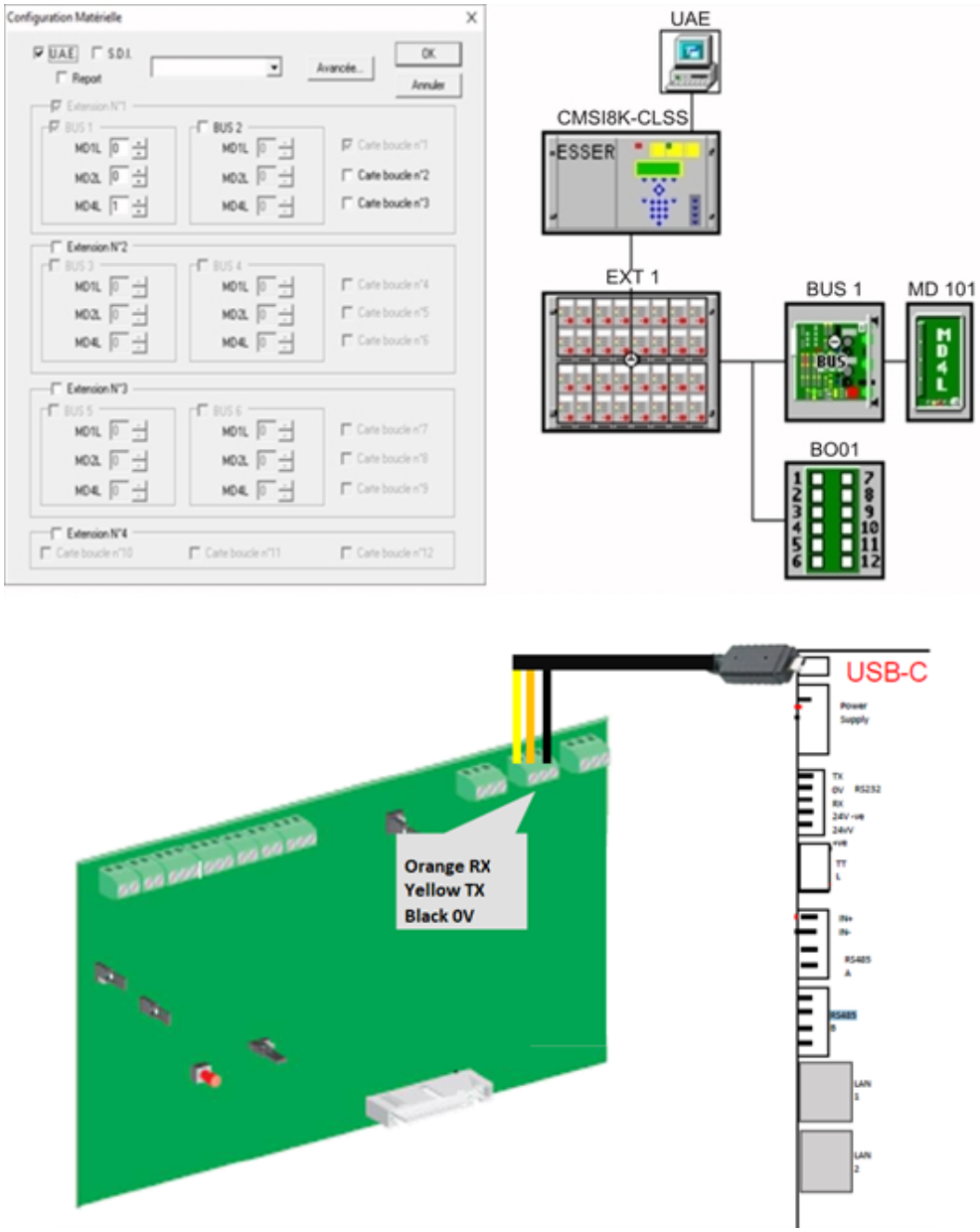


Figure C-13: CMSI Panel Settings

C.4 FARENHYT PANELS

C.4.1 CONNECTION OPTIONS

The gateway operates only with the Farenhyt fire alarm control panels listed in the table below:

Table C.2 Farenhyt Panel Connection Options

Fire Alarm Panel Modes	RS-485	UART/TTL	RS-232	USB
Panel firmware version: 6.05.03				
IFP-75	Yes	No	No	No
IFP-300	Yes	No	No	No
IFP-300ECS	Yes	No	No	No
IFP-2100	Yes	No	No	No
IFP-2100ECS	Yes	No	No	No
Panel firmware version: 5.0				
IFP-50	Yes	No	No	No
IFP-100	Yes	No	No	No
IFP-100ECS	Yes	No	No	No
IFP-1000	Yes	No	No	No
IFP-1000ECS	Yes	No	No	No
IFP-2000	Yes	No	No	No
IFP-2000ECS	Yes	No	No	No

CAUTION: When supporting the alarm transmission, it is recommended that the Farenhyt panel should use secondary ANN bus channel with Class A wiring.
If the alarm transmission service is *not* used, the panel can USE either the primary or the secondary ANN bus channel for the CLSS Gateway connection.

C.4.2 MINIMUM REQUIRED VERSIONS

• For the CLSS Gateway: 3.3.4.12

C.4.3 TO USE AN RS-485 CONNECTION

Using an RS-485 cable the CLSS Gateway connects with the annunciator primary terminal of the panel.

CAUTION: Connect either the CLSS gateway or the ANN S/P G module with the panel. Both of them should not be connected together with the panel.

On the Gateway Side

At the RS-485 A port in the gateway board:

• Connect the A connector to the IN+ pin of the RS-485 A port.
• Connect the B connector to the IN- pin of the same RS-485 A port.

The RS-485 ports in the gateway board are labeled as 3 and 4 in the Figure C-2: Gateway Connection Options - Bottom Side .

On the Panel Side

At the S-BUS board in the ANN-BUS PRI terminal:

• Connect the RS-485 +ve wire to the A port.
• Connect the RS-485 -ve wire to the B port.

C.4.4 POWER CONNECTION

On the Gateway Side

In the power supply port (labeled 7 in the Figure C-2: Gateway Connection Options - Bottom Side):

- Connect the Red wire to the +24V pin.
- Connect the Black wire to the Gnd pin.

On the Panel Side

In the power board of the panel:

- Connect the Red wire to the +ve pin.
- Connect the Black wire to the -ve pin.

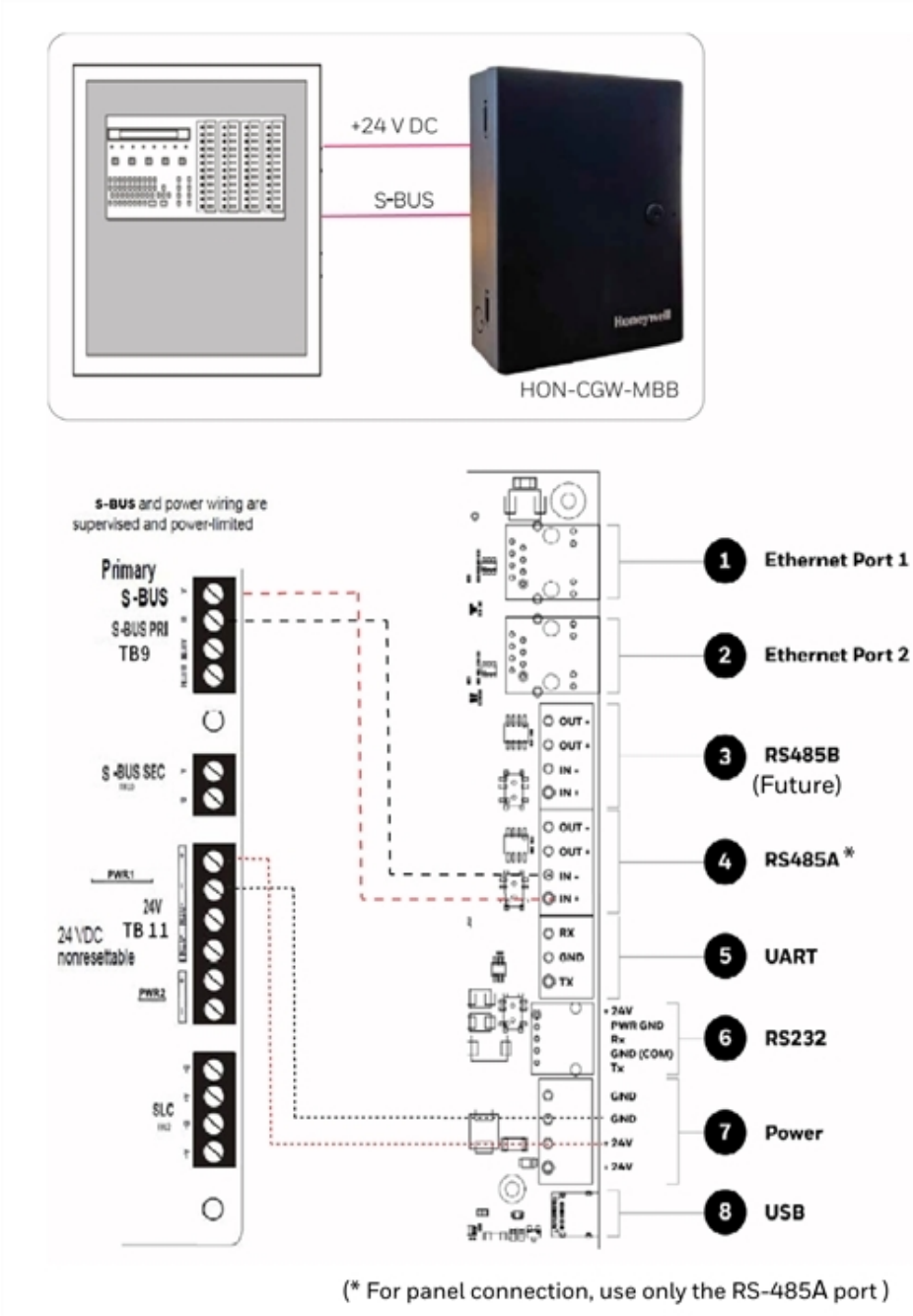


Figure C-14: Farenhyt Panel: RS-485 Connections

C.4.5 PROGRAMMING FOR ANNUNCIATOR (ANN-PRI)

Programming enables the panel to recognize the CLSS gateway and the annunciator.

CAUTION: Before programming, ensure that the ANN-PRI communication cable is connected with the panel.

C.4.6 TO PROGRAM FOR ANNUNCIATOR

Using the keypad on the panel, you select options on the screens.

01. On the panel, press the **Enter** button on the keypad.
02. View the panel screen options.
03. On the keypad, press **7** to select 7 = PROGRAMMING MODE.
04. Enter the panel's password in the PROGRAMMING screen.
    The default password is: 00000000
05. Select the panel connected with the gateway, if it is a standalone panel.
    OR
    Navigate in the list of panels and select the panel connected with the gateway if it is a multi-panel network.
06. Select 1 = MODULE.
07. Select 2 = ADD MODULE.
08. Select the module of the gateway from the list. Example: 5824-Serial/Parallel/IO
09. Select the module type.
10. Select 1 = EDIT MODULE to enter the module details.
11. Provide the **Module ID** details.
12. Navigate to next menu.
13. Select Output Port = PARALLEL.
14. Select Event Logging = YES.
15. Navigate to next menu.
16. Select Baud Rate = 19200.
17. Keep the default values for other fields.
18. Review the entered details.
19. Save the changes.

C.5 FIRE-LITE® PANELS

C.5.1 CONNECTION OPTIONS

The gateway operates only with the Fire-Lite fire alarm control panels as listed in the table below:

Table C.3 Fire-Lite Panel Connection Options

Fire Alarm Panel Models	RS485	UART/TTL	RS232	USB
ES50X	Yes	No	No	No
ES200X	Yes	No	No	No
MS-9600LS	Yes	No	No	No
MS-9600UDLS	Yes	No	No	No
MS-9050	Yes	No	No	No
MS-9200	Yes	No	No	No

C.5.2 TO USE AN RS485 CONNECTION

Using an RS485 cable the CLSS Gateway connects with the annunciator primary terminal of the panel.

Connect either the CLSS gateway or the ANN S/P G module with the panel. Both of them should not be connected together with the panel.

On the Gateway Side

At the RS485 port in the gateway board:

- Connect the A connector to the IN+ pin of the RS485 port.
- Connect the B connector to the IN- pin of the same RS485 port.

The RS485 ports in the gateway board are labeled as 3 and 4 in the Figure C-15: Fire-Lite Panel: RS485 Connections .

On the Panel Side

At the TB9 port in the ANN-BUS PRI terminal:

- Connect the RS485 +ve wire to the A port.
- Connect the RS485 -ve wire to the B port.

C.5.3 POWER CONNECTION

Using a power cable, the gateway connects to the 24V DC power supply port of the panel.

On the Gateway Side

In the power supply port (labeled 7 in the Figure C-15: Fire-Lite Panel: RS485 Connections):

- Connect the Red wire to the +24V pin.
- Connect the Black wire to the Gnd pin.

On the Panel Side

In the TB11 port of the panel:

- Connect the Red wire to the +ve pin.
- Connect the Black wire to the -ve pin.

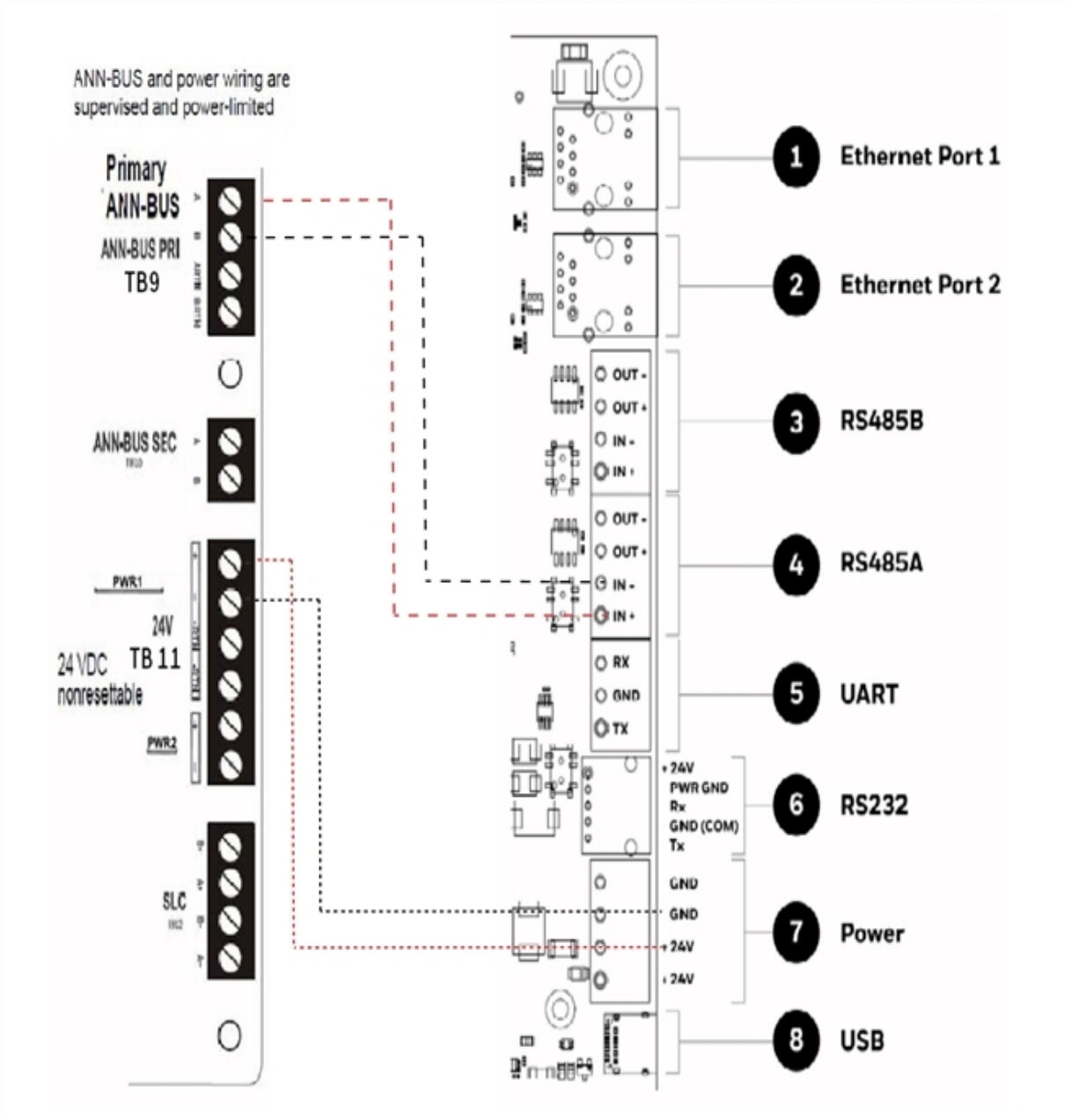


Figure C-15: Fire-Lite Panel: RS485 Connections

C.5.4 PROGRAMMING FOR ANNUNCIATOR (ANN-PRI)

Programming enables the panel to recognize the CLSS gateway and the annunciator.

Before programming, ensure that the ANN-PRI communication cable is connected with the panel.

C.5.5 TO PROGRAM FOR ANNUNCIATOR

Using the keypad on the panel, you select options on the screens.

01. On the panel, press the **Enter** button on the keypad.
02. View the panel screen options.
03. On the keypad, press **2** to select 2 = PROGRAMMING MODE.

04. Enter the panel's password in the PROGRAMMING screen.
    The default password is: 00000000
05. Press the down arrow button to select 2 = POINT PRGORAM.
06. Select 3 = FUTURE USE and then select 3 = ANNUNCIATORS.
07. Select 1 = PRIMARY on the ANN-BUS SELECT screen.
08. Ensure 1 = ENABLED YES on the ANN PRIMARY screen.
09. Select 2 = MODULES INSTALLED.
10. Select 1 = ADDR. 1-1 NONE on the ANN-BUS MODULES screen.
11. Ensure 1 = TYPE NONE on the ANN-BUS MODULE 1-1 screen.
12. Press the down arrow button once to go back to the ANN-BUS MODULE TYPE screen.
13. Press the down arrow button to go to the next screen.
14. Select 2 = ANN-S/PG MODULE.
15. On the keypad, press the **Esc** key three times to go back to the ANN/BUS SELECT screen.
16. Select 3 = ANN-BUS OPTIONS.
17. Press 1 = ANN-S/PG OPTIONS on the ANN-BUS screen.
18. Ensure the following settings on the ANN-S/PG OPTIONS screen:
    1 = PORT PAR
    2 = PRINTER SUPV YES
    3 = OFFLINE TIMER 0
19. Press the **Esc** button continuously until the main screen appears.

The panel saves the changes and resets.

C.5.6 TO VERIFY THE CHANGES

It is a good practice to confirm that the panel reflects the changes you did.

01. Use the keypad and go to the ANN-BUS MODULES screen.
02. Check that 1 = ADDR.1-1 ANN-S/PG on the ANN-BUS MODULE 1-1 screen.
03. Check that no ANN primary fault is reported on the main screen.

C.6 FIREWARDEN PANELS

C.6.1 CONNECTION OPTIONS

The gateway operates only with the FireWarden fire alarm control panels listed in the table below:

Table C.4 FireWarden Panel Connection Options

Fire Alarm Panel Models	RS-485	UART/TTL	RS-232	USB
FireWarden-50X	Yes	No	No	No
FireWarden-50	Yes	No	No	No
FireWarden-100-2	Yes	No	No	No
FireWarden-100X	Yes	No	No	No

When supporting the alarm transmission, it is recommended that the FireWarden panel should use secondary ANN bus channel with Class A wiring.
If the alarm transmission service is *not* used, the panel can USE either the primary or the secondary ANN bus channel for the CLSS Gateway connection.

C.6.2 MINIMUM REQUIRED VERSIONS

- For the Panel: 1.03.006
- For the CLSS Gateway: 3.0.3.116

C.6.3 TO USE AN RS-485 CONNECTION

Using an RS-485 cable the CLSS Gateway connects with the annunciator primary terminal of the panel.

CAUTION: Connect either the CLSS gateway or the ANN S/P G module with the panel. Both of them should not be connected together with the panel.

On the Gateway Side

At the RS-485 port in the gateway board:

- Connect the A connector to the IN+ pin of the RS-485 port.
- Connect the B connector to the IN- pin of the same RS-485 port.

The RS-485 ports in the gateway board are labeled as 3 and 4 in the Figure C-2: Gateway Connection Options - Bottom Side .

On the Panel Side

At the TB9 port in the ANN-BUS PRI terminal:

- Connect the RS-485 +ve wire to the A port.
- Connect the RS-485 -ve wire to the B port.

C.6.4 POWER CONNECTION

On the Gateway Side

In the power supply port (labeled 7 in the Figure C-2: Gateway Connection Options - Bottom Side):

- Connect the Red wire to the +24V pin.
- Connect the Black wire to the Gnd pin.

On the Panel Side

In the TB11 port of the panel:

- Connect the Red wire to the +ve pin.
- Connect the Black wire to the -ve pin.

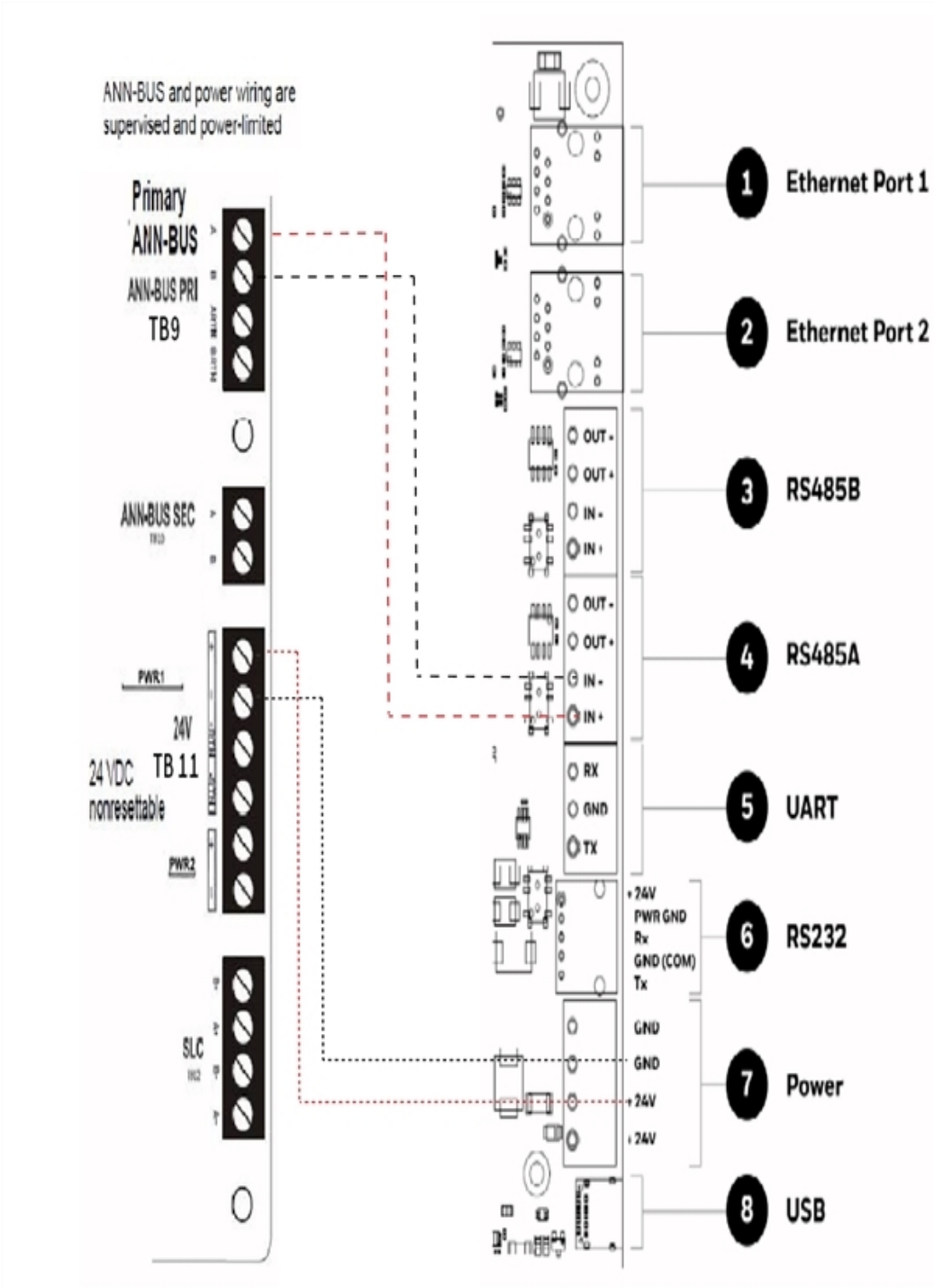


Figure C-16: FireWarden Panel: RS-485 Connections

C.6.5 PROGRAMMING FOR ANNUNCIATOR (ANN-PRI)

Programming enables the panel to recognize the CLSS gateway and the annunciator.

Before programming, ensure that the ANN-PRI communication cable is connected with the panel.

C.6.6 TO PROGRAM FOR ANNUNCIATOR

Using the keypad on the panel, you select options on the screens.

01. On the panel, press the **Enter** button on the keypad.
02. View the panel screen options.
03. On the keypad, press **2** to select 2 = PROGRAMMING MODE.
04. Enter the panel's password in the PROGRAMMING screen.
    The default password is: 00000000
05. Press the down arrow button to select 2 = POINT PRGORAM.
06. Select 3 = FUTURE USE and then select 3 = ANNUNCIATORS.
07. Select 1 = PRIMARY on the ANN-BUS SELECT screen.
08. Ensure 1 = ENABLED YES on the ANN PRIMARY screen.
09. Select 2 = MODULES INSTALLED.
10. Select 1 = ADDR. 1-1 NONE on the ANN-BUS MODULES screen.
11. Ensure 1 = TYPE NONE on the ANN-BUS MODULE 1-1 screen.
12. Press the down arrow button once to go back to the ANN-BUS MODULE TYPE screen.
13. Press the down arrow button to go to the next screen.
14. Select 2 = ANN-S/PG MODULE.
15. On the keypad, press the **Esc** key three times to go back to the ANN/BUS SELECT screen.
16. Select 3 = ANN-BUS OPTIONS.
17. Press 1 = ANN-S/PG OPTIONS on the ANN-BUS screen.
18. Set CLASS A to YES if your ANN Bus wiring is Class A topology, otherwise set it as NO.
19. Ensure the following settings on the ANN-S/PG OPTIONS screen:
    1 = PORT PAR
    2 = PRINTER SUPV YES
    3 = OFFLINE TIMER 0
20. Press the **Esc** button continuously until the main screen appears.
    The panel saves the changes and resets.

C.6.7 TO VERIFY THE CHANGES

It is a good practice to confirm that the panel reflects the changes you did.

01. Use the keypad and go to the ANN-BUS MODULES screen.
02. Check that 1 = ADDR.1-1 ANN-S/PG on the ANN-BUS MODULE 1-1 screen.
03. Check that no ANN primary fault is reported on the main screen.

C.6.8 TO USE PANEL'S PRINTER PORT CONNECTION

Some FireWarden panels support data transfer through their printer terminal.

> **NOTE:** Compatible CLSS Gateway firmware versions: 2.1.11.16 and above

On the Gateway Side

• Connect the serial cable into the RS-232 port of the gateway.

The RS-232 port is labeled as 6 in the Figure C-18: FireWarden Panels: Printer Port Connections .

On the Panel Side

Connect the serial cable in the DB9 serial port of the ANN-S/PG module on the panel.

CAUTION: Ensure that only the ANN-s/pg is connected and not the clss gateway. only one of these two can be connected. both of them must not be connected together.

C.6.9 POWER CONNECTION

On the Gateway Side

- Connect to the 24V DC external power supply.
- Switch the S7 Switch next to the RS-232 port towards *NUP_OUT*.

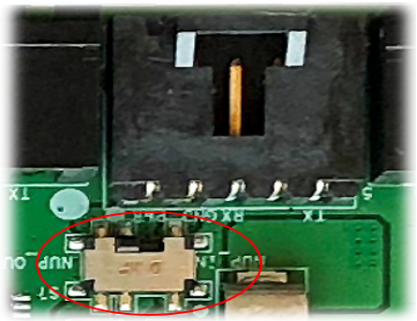


Figure C-17: The S7 Switch

On the Panel Side

Connect the power cable to a 24V DC external power source or the panel's power supply.

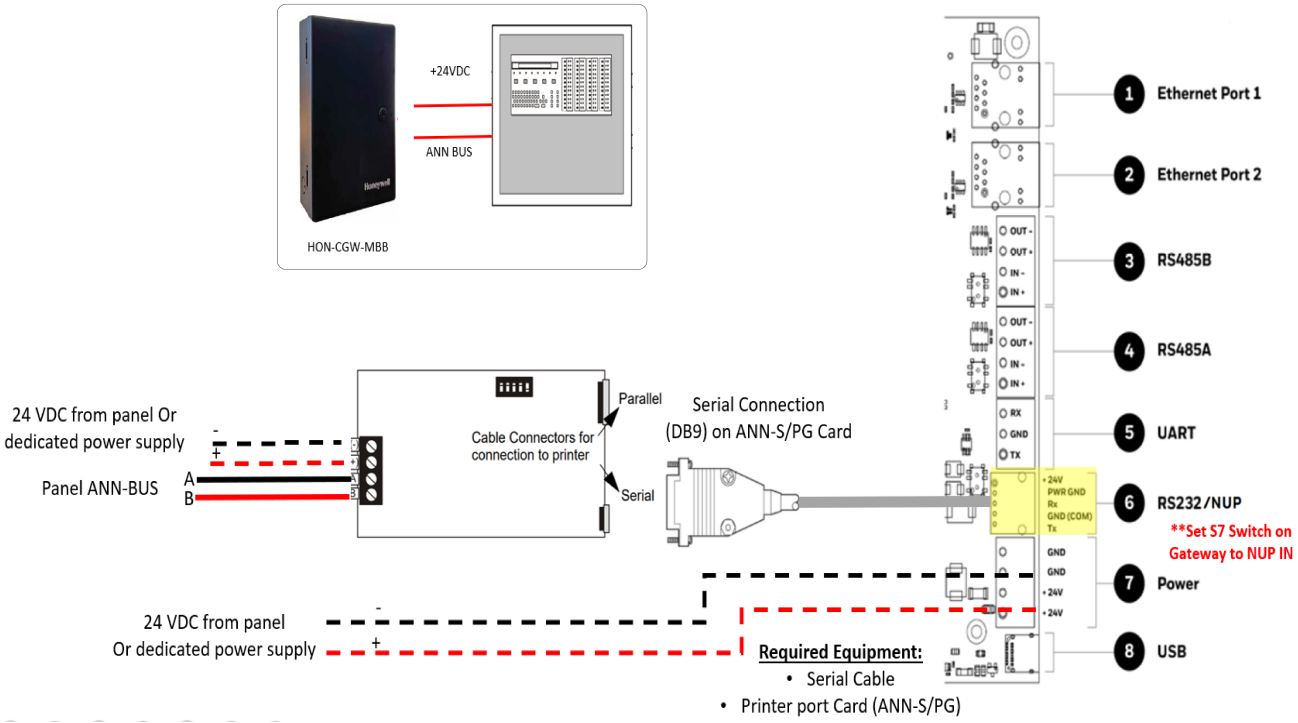


Figure C-18: FireWarden Panels: Printer Port Connections

C.7 GAMEWELL-FCI PANELS

C.7.1 CONNECTION OPTIONS

Each variant of the Gamewell-FCI panel offers various connection options.

The gateway operates only with the Gamewell-FCI fire alarm control panels listed in the table below:

Table C.5 Gamewell-FCI Panel Connection Options

Fire Alarm Panel Models	RS-485	UART/TTL	RS-232	USB	Ethernet
E3 Series Panels					
ILI-MB-E3	Yes	No	No	Yes	No
ILI-S-E3	No	No	No	Yes	No
ILI95-MB-E3	Yes	No	No	Yes	No
ILI95-S-E3	No	No	No	Yes	No
S3 Series Panels					
SLP-E3	Yes	No	No	Yes	Yes

CAUTION: Do not install DACT-E3 and the CLSS Gateway together on an ILI-MB-E3 circuit board or an ILI95-MB-E3 circuit board. You can use DACT-E3 on a different node within the network.

C.7.2 MINIMUM REQUIRED VERSIONS

- E3 Series: 7.00.106
- S3 Series: 7.00.106
- CLSS Gateway: 3.1.4.72
- LCD-SLP (Display Panel): 2.12.090
- NGA-K: 7.00.100

C.7.3 LIMITATION(S)

The *CLSS Gateway* only with firmware version 3.3.4.14 or above supports CAM text messages. Currently, these messages may show the *Device Type* as *Unavailable* on *Cloud-Connected Horizon*. It is planned to show this information in a future release.

Following Gamewell panel versions support the CAM text messages:

- E3 Series: 7.02.001
- S3 Series: 7.02.001
- LCD-SLP:7.01.001
- NGA-K: 7.01.001

C.7.4 TO USE PANEL'S PRINTER PORT CONNECTION

Gamewell panels support data transfer through their RS-485 connection. The transferred data is stored in the *CLSS Site Manager*.

On the Gateway Side

01. Connect the + (24 V) wire to the IN+ pin of an RS-485 port.
02. Connect the - (GND) wire to the IN- pin of an RS-485 port.

The RS-485 ports are labeled as 3 and 4 in the Figure C-18: FireWarden Panels: Printer Port Connections .

On the Panel Side

- E3 Series Panel
- S3 Series Panel

E3 Series Panel

At the TB3 terminal of the panel,

- Connect the +ve wire to the TB3-1 pin.
- Connect the -ve wire to the TB3-2 pin.

At the TB6 terminal of the panel,

- Connect the GND wire to the TB6-1 pin.
- Connect the TxD wire to the TB6-2 pin.
- Connect the SUPV wire to the TB6-3 pin.
- Connect the RxD wire to the TB6-4 pin.

C.7.5 POWER CONNECTION

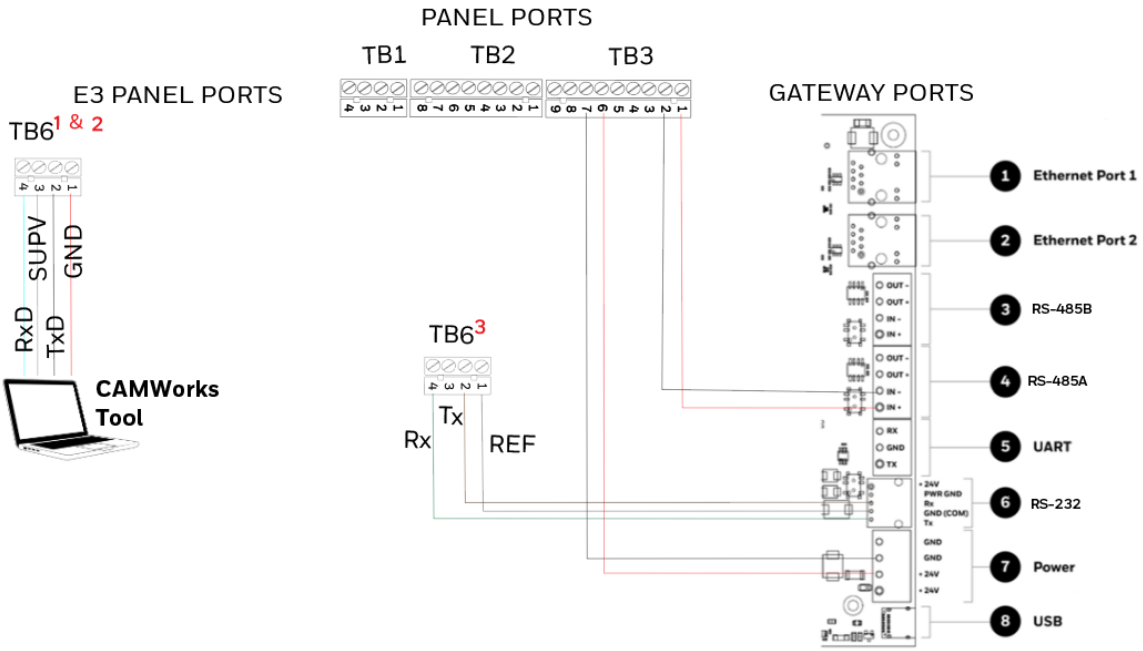
On the Gateway Side

Ensure that the power cable is connected with the power port of the gateway.

The power port is labeled as 7 in the Figure C-18: FireWarden Panels: Printer Port Connections .

On the Panel Side

- Connect the Red wire to the +ve pin in the TB3 port.
- Connect the Black wire to the -ve pin in the TB3 port.



1 Disconnect the CAMWorks Tool after downloading the configuration file. Then, connect RS-232 to TB6 for Control Functionality.

2 If the computer has a serial port, connect it with the RS-232 to DB9 converter (P/N: 75267). If the computer does not have a serial port, connect the converter with the USB port of the computer.

3 Control Functionality

Figure C-19: E3 Panel: Gateway Connections

TB6 and RS-232 Connections

The pin connections are as below:

TB6 Pins	RS-232 Pins	Description
TB6-1	RS-232 GND	*For Programming*. GND connects to the **Red** lead on the download cable of P/N 75267. For Printer port, GND connects to printer DB-9 and PIN-5.
TB6-2	RS-232 TxD	*For Programming*. TxD connects to the **Black** lead on the download cable of P/N 75267. For Printer port, TxD connects to printer DB-9 and PIN-2.
TB6-3	RS-232 Supervision	For optional printer supervision. For Printer port, SUPV connects to printer DB-9 and PIN-4.
TB6-4	RS-232 RxD	*For Programming*. RxD connects to the **Green** lead on the download cable of P/N 75267. For Printer port, RxD connects to printer DB-9 and PIN-3.

S3 Series Panel

At the TB3 terminal of the panel,

- Connect the +ve wire to the TB3-1 pin.
- Connect the -ve wire to the TB3-2 pin.

At the TB5 terminal of the panel,

- Connect the GND wire to the TB5-1 pin.
- Connect the TxD wire to the TB5-2 pin.
- Connect the SUPV wire to the TB5-3 pin.
- Connect the RxD wire to the TB5-4 pin.

C.7.6 POWER CONNECTION

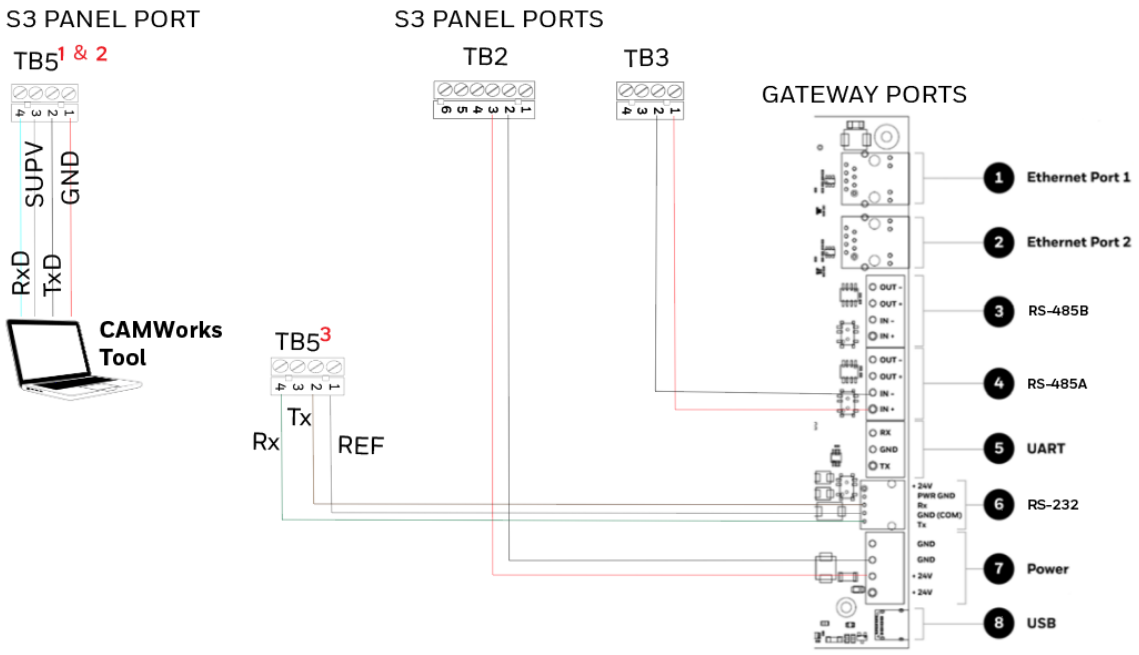
On the Gateway Side

Ensure that the power cable is connected with the power port of the gateway.

The power port is labeled as 7 in the "FireWarden Panels: Printer Port Connections" on page 165.

On the Panel Side

- Connect the Red wire to the +ve pin in the TB2 port.
- Connect the Black wire to the -ve pin in the TB2 port.



1 Disconnect the CAMWorks Tool after downloading the configuration file. Then, connect RS-232 to TB5 for Control Functionality.

2 If the computer has a serial port, connect it with the RS-232 to DB9 converter (P/N: 75267). If the computer does not have a serial port, connect the converter with the USB port of the computer.

3 Control Functionality

Figure C-20: S3 Series: Gateway Connections

TB5 and RS-232 Connections

The pin connections are as below:

TB5 Pins	RS-232 Pins	Description
TB5-1	RS-232 GND	*For Programming*. GND connects to the **Red** lead on the download cable of P/N 75267. For Printer port, GND connects to printer DB-9 and PIN-5.
TB5-2	RS-232 TxD	*For Programming*. TxD connects to the **Black** lead on the download cable of P/N 75267. For Printer port, TxD connects to printer DB-9 and PIN-2.
TB5-3	RS-232 Supervision	For optional printer supervision. For Printer port, SUPV connects to printer DB-9 and PIN-4.
TB5-4	RS-232 RxD	*For Programming*. RxD connects to the **Green** lead on the download cable of P/N 75267. For Printer port, RxD connects to printer DB-9 and PIN-3.

C.8 GENT PANELS

C.8.1 CONNECTION OPTIONS

The gateway operates only with the Gent fire alarm control panels listed in the table below:

Table C.6 Gent Panel Connection Options

Fire Alarm Panel Models	RS-485	UART/TTL	RS-232	USB
COMPACT-24-N	No	No	Yes	Yes
COMPACT-PLUS	No	No	Yes	Yes
VIGPLUS-24	No	Yes	Yes[1]	Yes
VIGPLUS-72	No	Yes	Yes[1]	Yes
VIG1-24	No	Yes	Yes[1]	Yes
VIG1-72	No	Yes	Yes[1]	Yes
[1]Use the add-on I/O card (VIG-IOC-DOM) on the panel				

NOTE: The add-on I/O card (VIG-IOC-DOM) is ordered separately.

C.8.2 COMPACT SERIES PANELS

For a fixed gateway we recommend using the RS-232 connection. For a portable gateway, we recommend using the USB connection.

To Use a RS-232 Connection

Certain Gent panel variants can directly communicate through the RS-232 connection.

On the Gateway Side

- Connect the RS-232 cable with pre-formed connector to the RS-232 port of the gateway board.
- The RS-232 port is labeled as 6 in the Figure C-2: Gateway Connection Options - Bottom Side .

On the Panel Side

- The baud rate should be 19200.

At the PB6 terminal of the panel,

- Connect the White wire to a Rx1 or Rx2 pin.
- Connect the Brown wire to a Tx1 or Tx2 pin.
- Connect the Green wire to the 0V pin.

Connect either the Tx1 and Rx1 *or* the Tx2 and Rx2.

If Tx1 and Rx1 are connected, select the Port 1 settings in the panel for communication. If Tx2 and Rx2 are connected, select the Port 2 settings in the panel for communication.

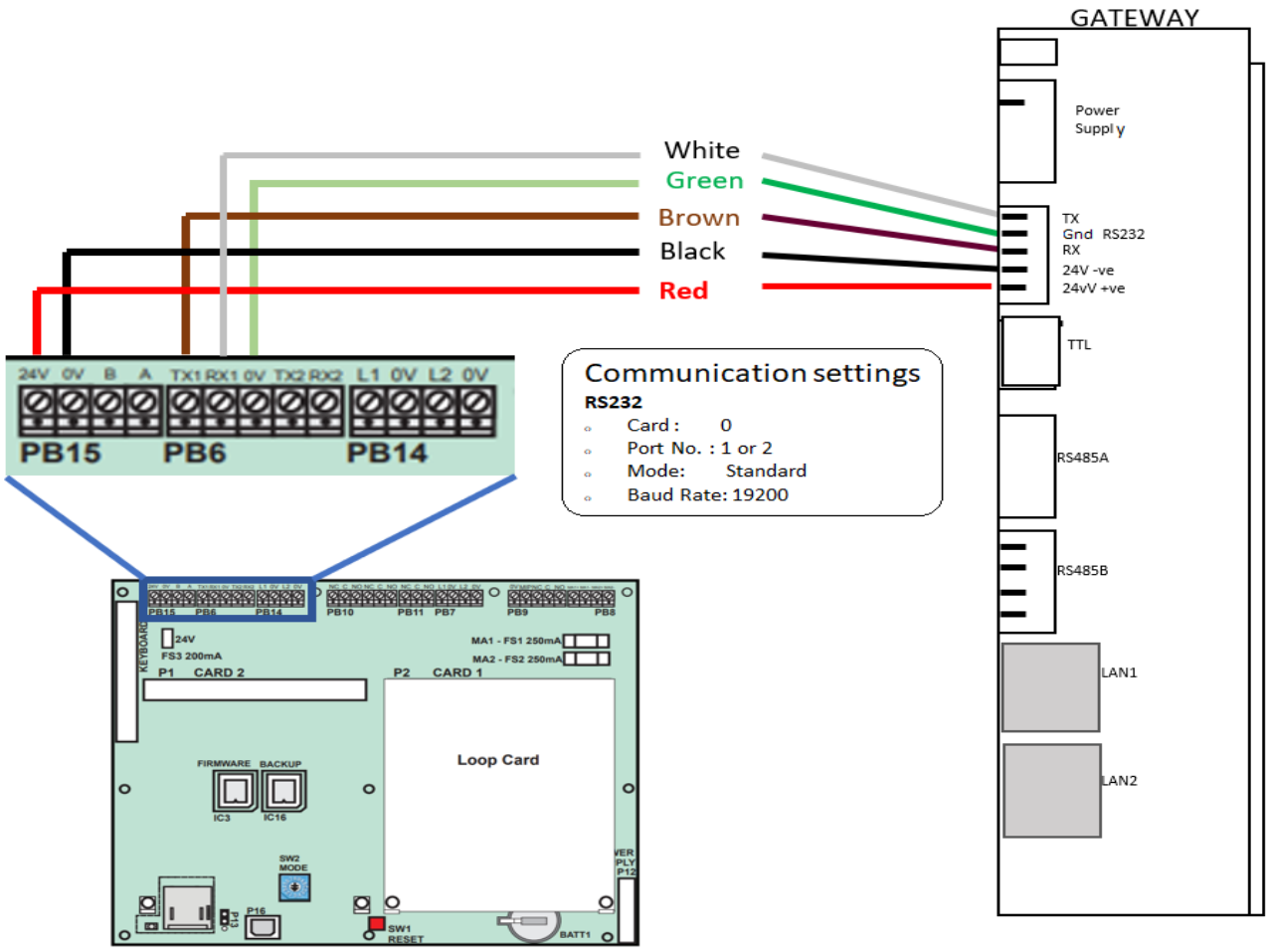


Figure C-21: COMPACT Panels: RS-232 Connections on the PB6 Terminal

C.8.3 POWER CONNECTION

On the Gateway Side

- Ensure that the RS-232 cable is connected with the RS-232 port of the gateway.
- Ensure that the S7 switch next to the RS-232 port is switched towards *NUP_IN*.

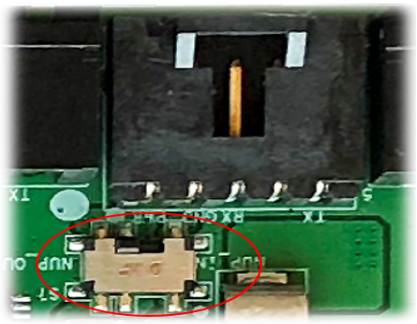


Figure C-22: The S7 Switch

On the Panel Side

At the PB15 terminal of the panel,

- Connect the Red wire (+ve) to the +24V pin.
- Connect the Black wire (-ve) to the 0V pin.

C.8.4 TO USE A USB CONNECTION

On the Gateway Side

- Connect the USB-C side of the cable to the USB port of the gateway.
- The USB port is labeled as 8 in the figure Figure C-2: Gateway Connection Options - Bottom Side .

On the Panel Side

Connect the USB-B side of the cable to the USB port of the panel.

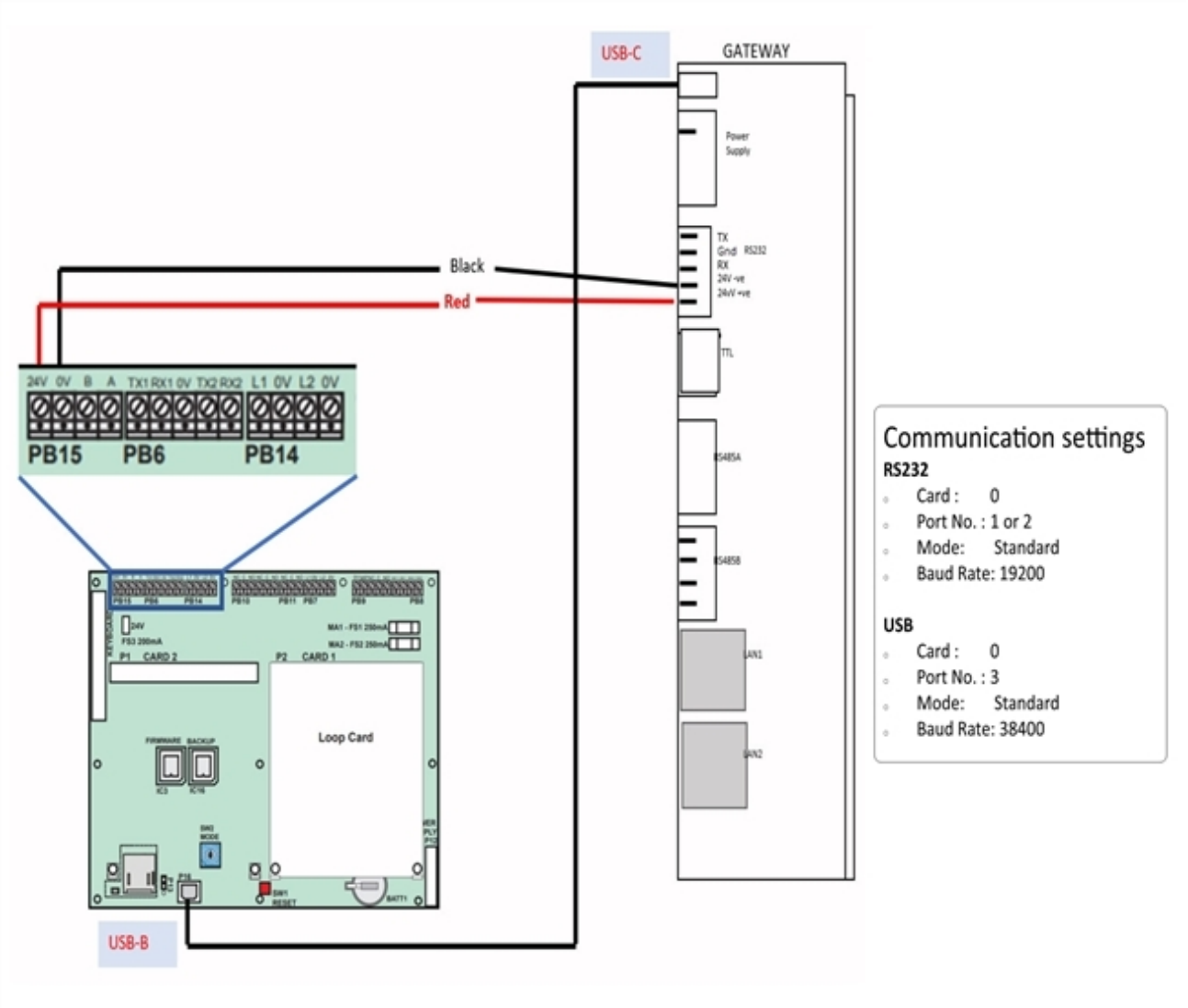


Figure C-23: Compact Panels: USB Connection

C.8.5 POWER CONNECTION

In the PB15 terminal on the panel,

- Connect the gateway to a 24V DC internal power source of the panel.
- The external power supply must be dedicated and not shared with any other devices.
- The panel's power supply to the gateway must be within +24V DC power.

C.8.6 VIGILON SERIES PANELS

For a fixed gateway, we recommend using a UART/TTL connection. If it is not available, use a RS-232 connection.

To Use a UART/TTL Connection

On the Gateway Side

• Connect the male UART/TTL cable to the Rx (Red), Gnd (Silver), and Tx (White) UART/TTL terminals of the gateway.

The UART/TTL port is labeled as 5 in Figure C-2: Gateway Connection Options - Bottom Side .

On the Panel Side

• Within the panel, find the backplane PCB board (see Figure C-24: Vigilon Panels: UART/TTL Connection).
• Connect the 3.5mm phono socket to the P11 connector on the panel's PCB.

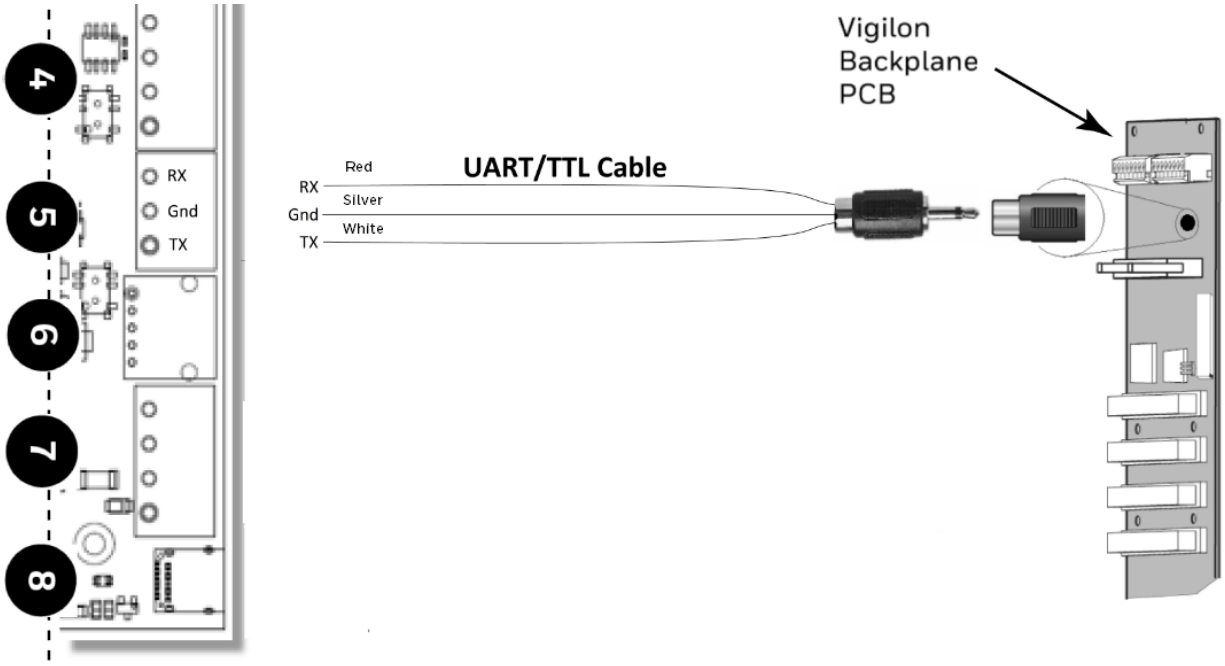


Figure C-24: Vigilon Panels: UART/TTL Connection

C.8.7 POWER CONNECTION

On the Gateway Side

Connect the power cable to a 24V DC external power source.

> **NOTE:** The external power supply must be dedicated and not shared with any other devices.

> **NOTE:** The panel's power supply to the gateway must be within +24V DC power.

To Use an RS-232 Port via an I/O Card

Using an add-on I/O card (VIG-IOC-DOM), certain Vigilon panel variants can communicate with the CLSS Gateway.

• The I/O card has a rotary switch, which should point to 5.
• The baud rate of the I/O card should be 19200.

On the Gateway Side

• Connect the RS-232 cable to the RS-232 port of the gateway.

The RS-232 port is labeled as 6 in the "Gateway Connection Options - Bottom Side" on page 142.

On the Panel Side

- Inside the panel enclosure, find the backplane PCB board.
- Insert the I/O card into the P2 Card 15.
- Insert the I/O card into P8 Card 6

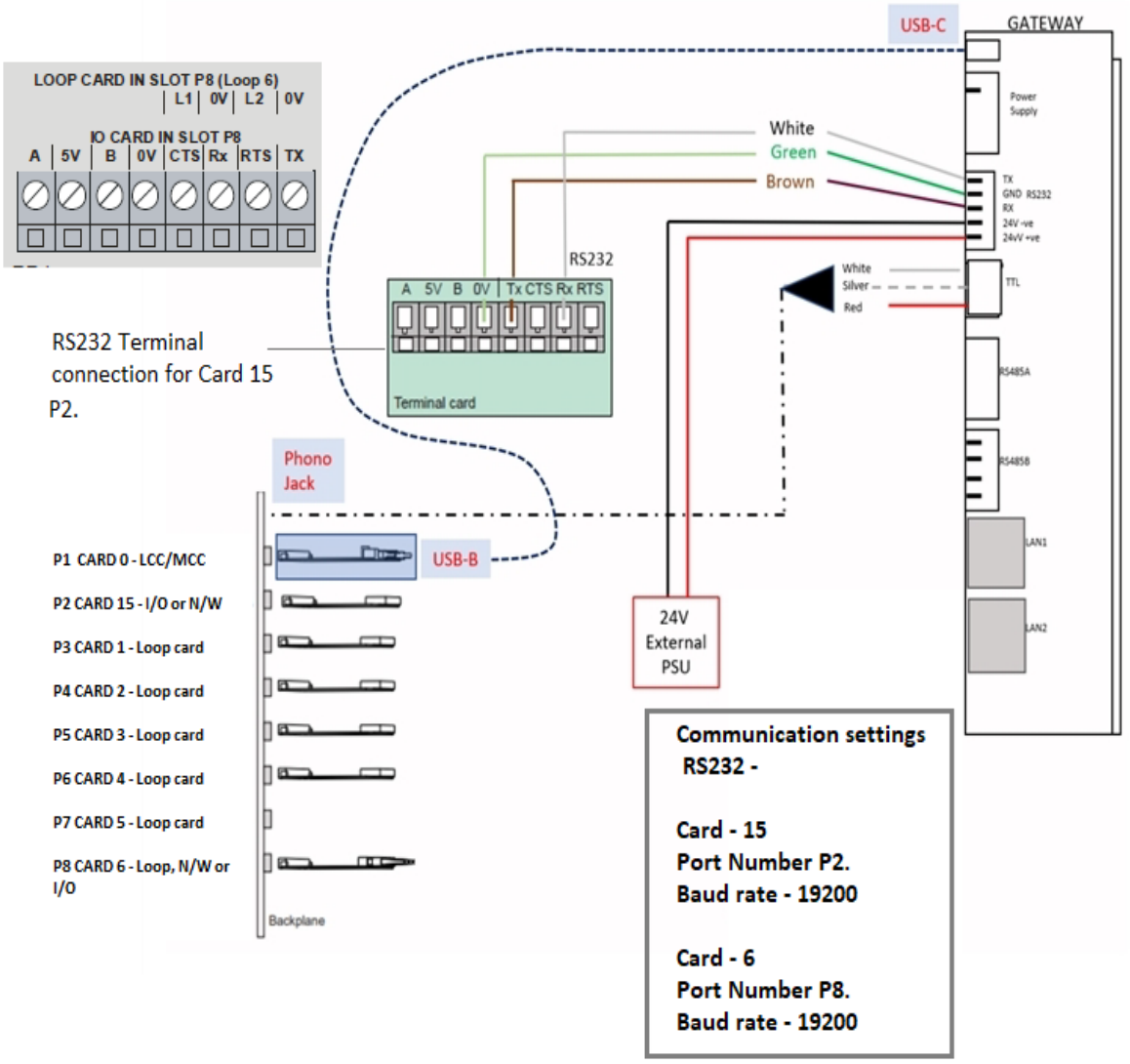


Figure C-25: Vigilon Panels: I/O Card Connection

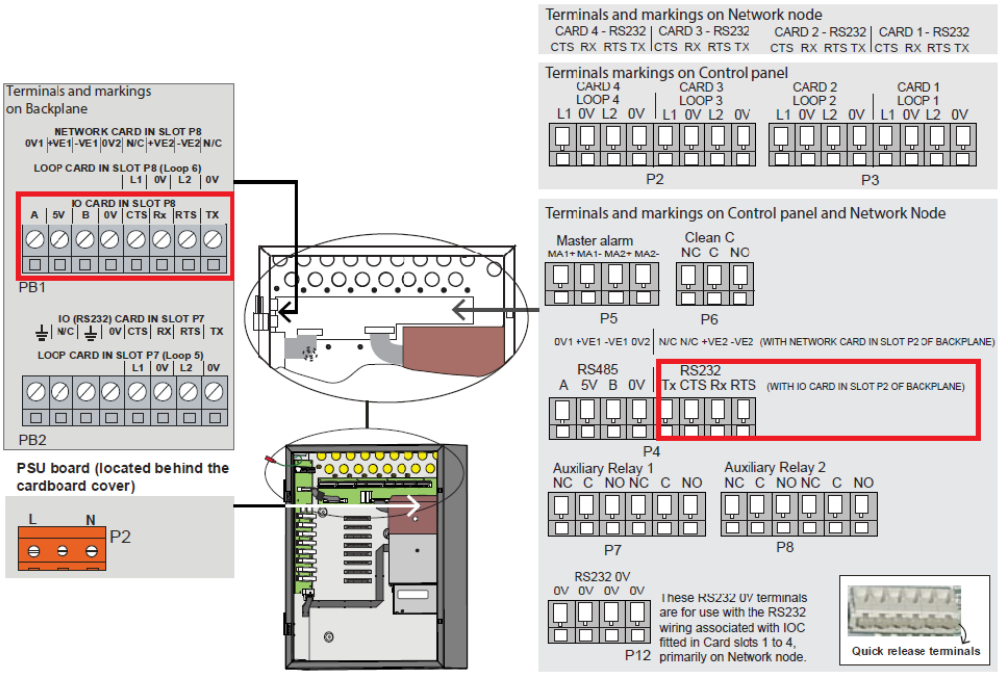


Figure C-26: Vigilon Terminal Card Connection Details

For the P2 Card 15-Connected I/O Card:

- In the panel, find the RS-485/RS-232 (P4) connectors on the main control board.
- Connect the RS-232 cable to the Tx (Brown), Rx (White), and 0V (Green) terminals of the RS-485/RS-232 (P4) connectors.

C.8.8 POWER CONNECTION

NOTE: The external power supply must be dedicated and not shared with any other devices.

NOTE: The panel's power supply to the gateway must be within +24V DC power.

On the Gateway Side

- Connect to the 24V DC external power supply.
- Ensure that the S7 switch next to the RS-232 port is switched towards *NUP_OUT*.

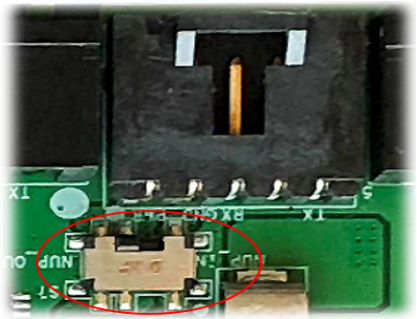


Figure C-27: The S7 Switch

On the Panel Side

Connect the power cable into the 24V DC external power supply.

C.8.8.1 To Use a USB Connection

On the Gateway Side

- Connect the USB-C side of the cable to the USB port of the gateway.
- The USB port is labeled as 8 in the figure Figure C-2: Gateway Connection Options - Bottom Side .

On the Panel Side

In the MCC card on the panel:

- Connect the USB-B side of the cable. Refer to the figure Figure C-25: Vigilon Panels: I/O Card Connection .

C.8.9 POWER CONNECTION

Connect the gateway to a 24V DC external power source.

NOTE: The external power supply must be dedicated and not shared with any other devices.

NOTE: The panel's power supply to the gateway must be within +24V DC power.

C.9 MORLEY-IAS PANELS

C.9.1 CONNECTION OPTIONS

The gateway operates only with the Morley-IAS fire alarm control panels listed in the table below:

Table C.7 Morley-IAS European Panel Connection Options

Fire Alarm Panel Models	RS-485	UART/TTL	RS-232	USB
DXc	No	No	Yes[1]	No

[1]Use the serial communication card (P/N: 795-122) on the panel

NOTE: Compatible CLSS Gateway firmware versions: 3.0.2.30 and above.

C.9.2 TO USE AN RS-232 CONNECTION

Morley-IAS panel variants use an RS-232 connection with the CLSS Gateway.

On the Gateway Side

- Connect the RS-232 cable with pre-formed connector t o the RS-232 port of the gateway board.
- The RS-232 port is labeled as 6 in the Figure C-2: Gateway Connection Options - Bottom Side .

On the Panel Side

- C.10 Morley DXc Panels

NOTE: In a network of panels, connect the gateway to the master panel.

C.10 MORLEY DXC PANELS

In the SK1 terminal of the panel:

- Connect the White wire to the RxD+ pin.
- Connect the Green wire to the Gnd pin.
- Connect the Brown wire to the TxD+ pin.

C.10.1 POWER CONNECTION

The gateway's RS-232 port can receive its power either from an external power source or from the non-resettable internal power of the panel.

NOTE: The external power supply must be dedicated and not shared with any other devices.

NOTE: The panel's power supply to the gateway must be within +24V DC power.

For the External Power Supply:

On the Gateway Side

- Connect to the 24V DC external power supply or to the panel's 24V DC power port.
- Ensure that the S7 switch next to the RS-232 port is switched towards *NUP_OUT*.

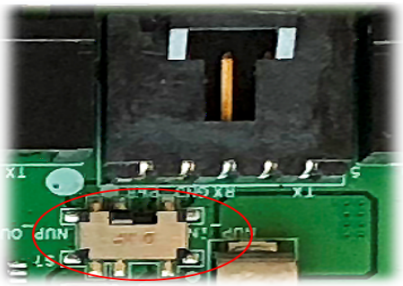


Figure C-28: The S7 Switch

On the Panel Side

In the SK4 or SK5 terminal,

• Connect the RS-232 cable for the non-resettable internal power.

C.11 MORLEY MAX PANELS

C.11.1 CONNECTION OPTIONS

The gateway operates with the MA Series fire alarm control panels listed in the table below:

Table C.8
MA Series Panel Connection Options

Fire Alarm Panel Models	RS-485	UART/TTL	RS-232	USB
MA-8000	No	No	Yes[1]	No
MA-2000	No	No	Yes[1]	No
MA-1000	No	No	Yes[1]	No
1 Use the Terminal Board AW80US0				

NOTE: The panel can be a stand alone panel of part os a network of panels.

C.11.2 MINIMUM REQUIRED VERSIONS

For the Panel/CPU1: V1.0.703

For the CLSS Gateway: 3.0.4.56

To Use an RS-232 Connection to establish connection between panel and gateway

In terms of hardware, the MA-2000 and MA-8000 control panels consist of two main boards: AW80FR0 (front) and AW80US0 (terminals board) (check the manual for further board schemes, be careful not to confuse with the AW80FR1 and AW80US1 which are used in the MA-1000) On the AW80US0 terminals board, the reference connector for TPP serial communication is CNS:

- CNS is a double-row connector.
- the useful terminals for the TPP connection are 4, 5, 6 (Note are in the lowest row).
- these terminals are used for both RS232 and RS485 connection

CNS-4 RS485_H RS232_TX
CNS-5 GND GND
CNS-6 RS485_L RS232_RX

Switch

On the AW80FR0 front board via SW5 (4-way dip switch or slide switch) it is possible to set RS232 / RS485.

If the customer has the first hardware version of the AW80FR0 v01s front board: SW5 is a 4-way dip switch.

RS232 SW5 1..4: ON ON OFF

RS485 SW5 1..4: OFF ON ON For all hardware versions subsequent to AW80FR0 v02s (inclusive)

SW5 is a slide switch and the settings

RS232 / RS485 are clearly marked on the board itself.

To switch RS232 <--> RS485

- Switch off the control unit
- Disconnect from CNS-4, CNS-5, CNS-6 the device acting as External Equipment
- Set SW5 correctly.
- Connect the device acting as External Equipment properly to CNS-4, CNS-5, CNS-6
- Switch on the control panel.

CNS Connector 9+9 poles 2 horizontal staggered planes pitch 5 (1-9 row below 10-18 row above)			
01	RS485H1		RS485-1 signal A+
02	GNDIS1		GND RS485-1 isolated
03	RS485L1		RS485-1 signal B-
04	RS485H2	RS232 TX2	RS485-2 A+ signal
05	GNDIS2	GNDIS2	GND RS485-2 isolated
06	RS485L2	RS232 RX2	RS485-2 signal B-
07	RS485H3	RS232 TX3	RS485-3 A+ signal
08	GNDIS3	GNDIS3	GND RS485-3 isolated
09	RS485L3	RS232 RX3	RS485-3 signal B-

Figure C-29: CNS Connectors on AW80US0 Board of Panel

CNU		
01	LA1 +	Loop 1 + side A
02	LA1 -	Loop 1 - side A
03	LB1 +	Loop 1 + side B
04	LB1 -	Loop 1 - side B
05	LA2 +	Loop 2 + side A
06	LA2 -	Loop 2 - side A
07	LB2 +	Loop 2 + side B
08	LB2 -	Loop 2 - side B
09	+24V USR	+ 24 Vcc User
10	GND USR	GND User

Figure C-30: CNU Connector on AW80US0 Board of Panel

Communication

Valid both for RS-232 and RS-485:

Baud Rate (Fixed) :38400
Number of bits (Fixed) : 8
Stop Bits (Fixed): 1
Parity (Fixed): none

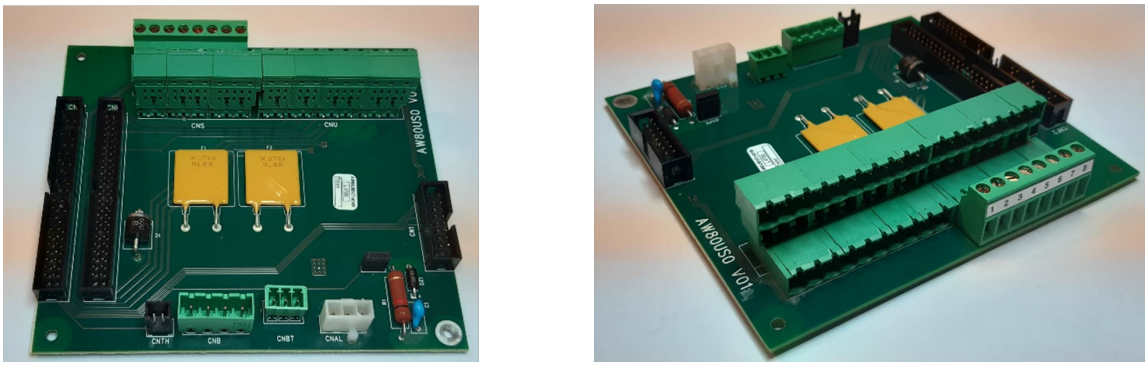


Figure C-31: Terminals of AW80US0 v01

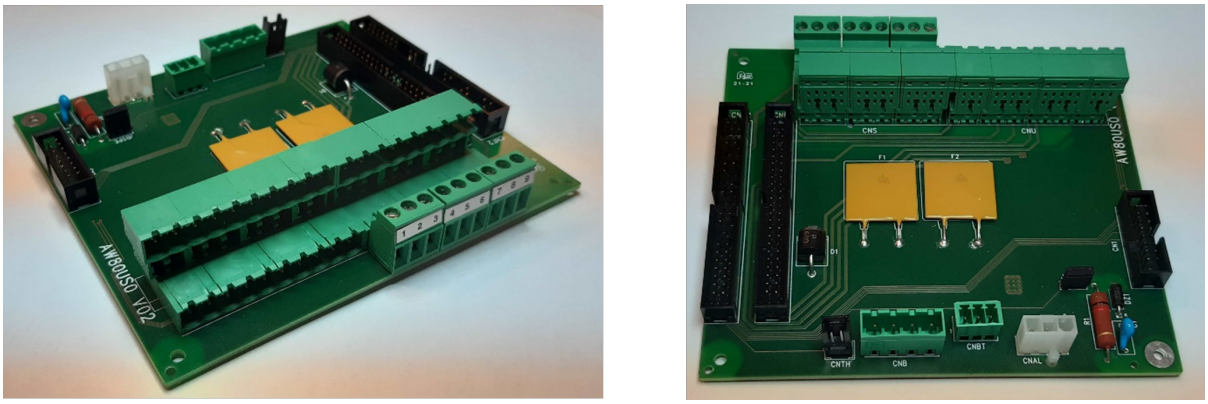


Figure C-32: Terminals of AW80US0 v02

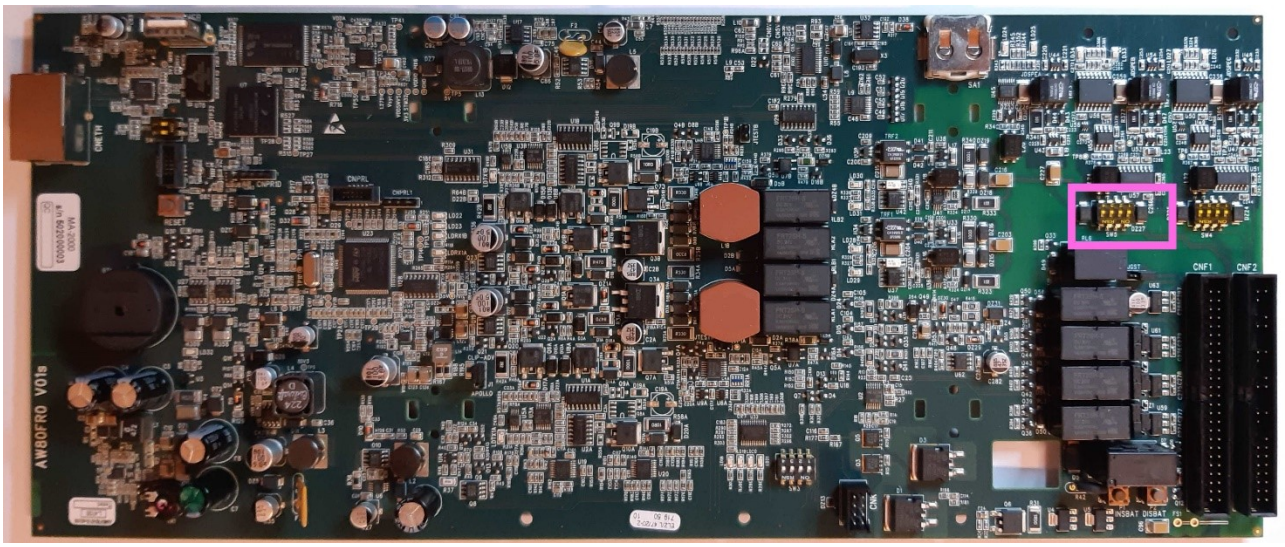


Figure C-33: 4-Way Dip Switch

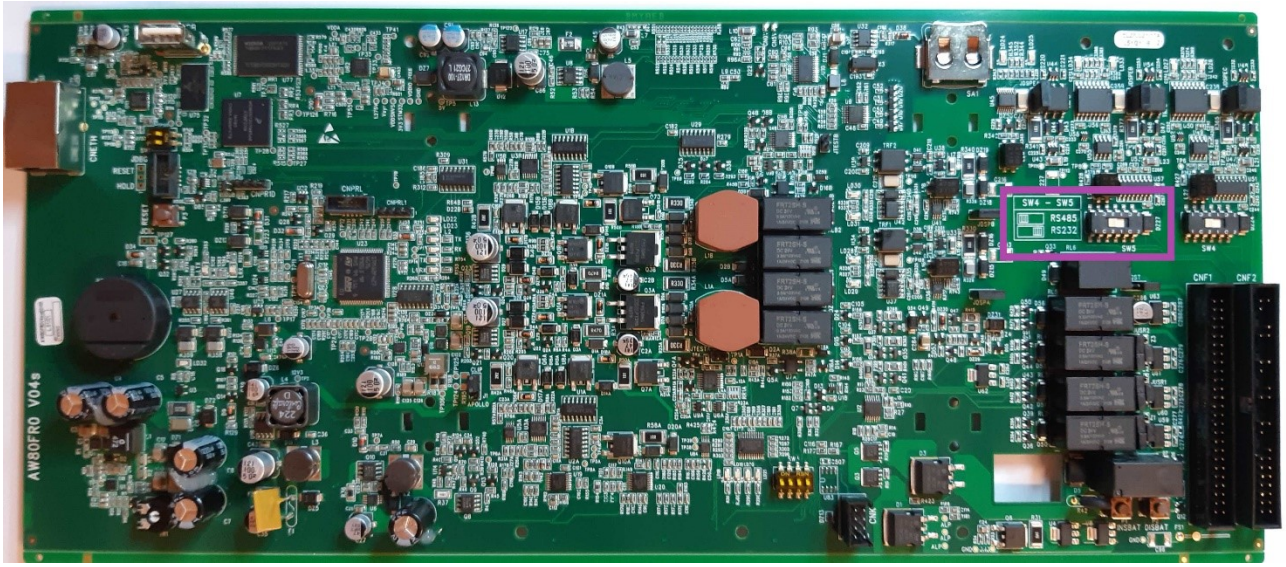


Figure C-34: Slide Switch

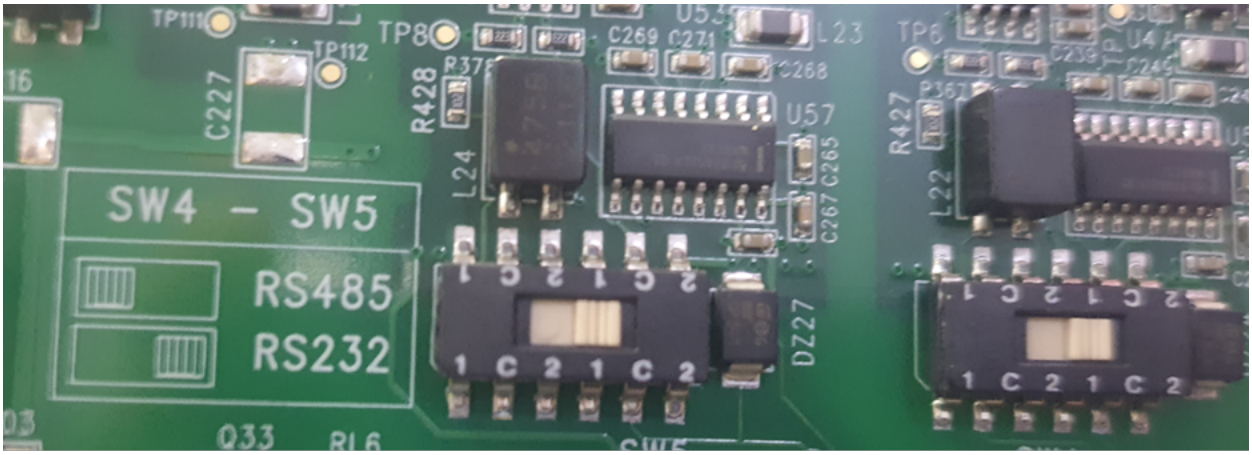


Figure C-35: Slide Switch Detail

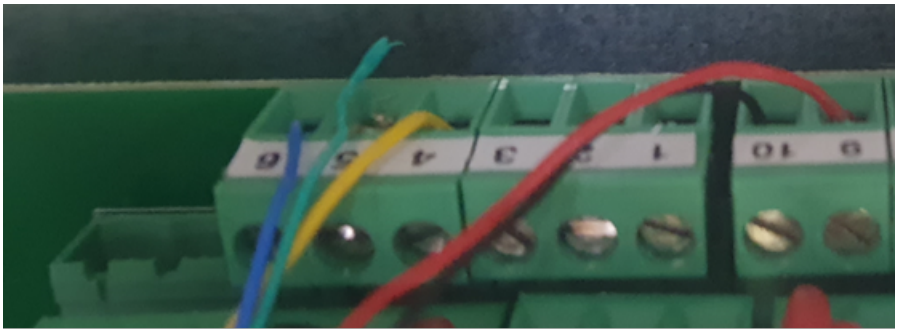


Figure C-36: Panel Side RS232 and Power Cable Connection

Panel side RS232 lines will be connected to CNS-4(TX), CNS-5(GND), and CNS-6(RX) on AW80US0 board. Power line +ve (CNU-9) and GND- (CNU-10).

Using an RS-232 cable the CLSS Gateway and the panel are connected. The RS-232 port in the gateway board is labeled as 6 in the Figure C-2: Gateway Connection Options - Bottom Side

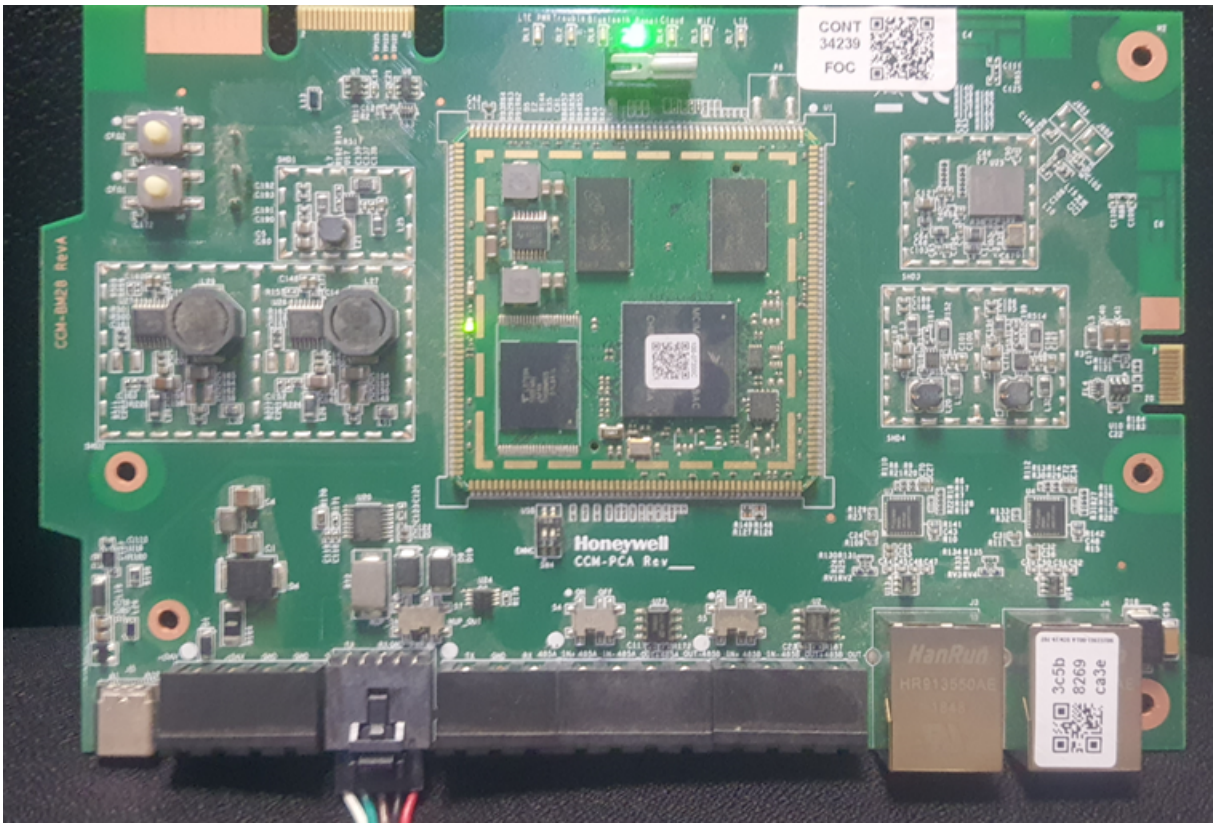
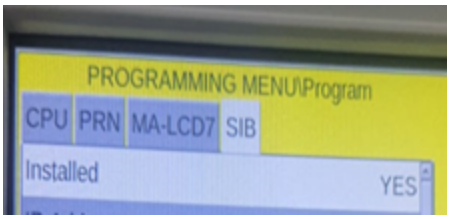


Figure C-37: Gateway Board with RS232 Connection

In the panel HMI, please select the below option to enable the serial communication over TPP.



On the Gateway Side

Connect to an RS-232 port of the gateway board

On the Panel Side

• MA8000, MA2000, MA1000 Panels

MAX Panels

1. Connect the RS232 RX pin of GW to CNS connector TX pin 4.
2. Connect the GND pin of GW to CNS connector GND pin 5.
3. Connect the RS232 TX pin of GW to CNS connector RX pin 6.
4. Connect the GW power line +ve terminal to +ve of CNU connector Pin 9.
5. Connect the GW power line GND terminal to GND pin of CNU connector pin 10.

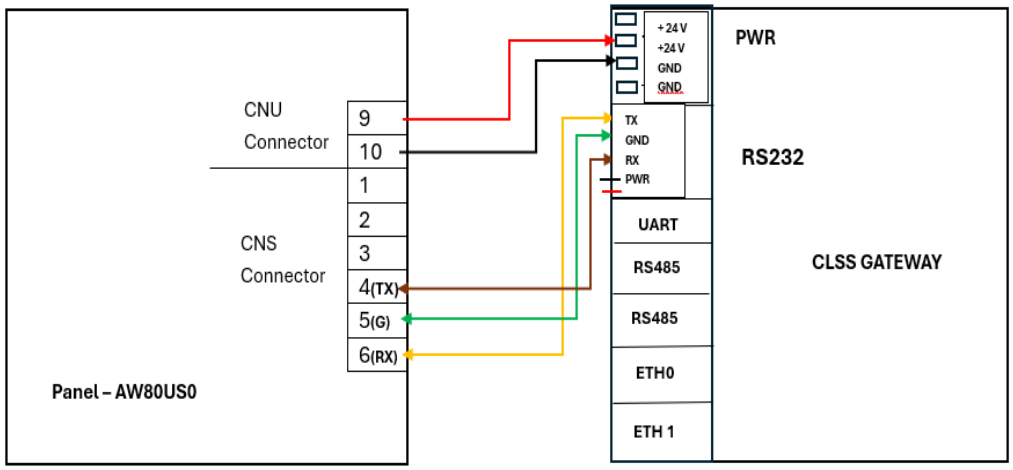


Figure C-38: Wiring Diagram: RS-232 Connection with MORLEY MAX Panel

To Upload Panel Configuration File to Cloud

Before installing the gateway, configuration file of the panel set up needs to be uploaded to cloud.

Steps involved in uploading the configuration file:

• Connect the USB drive into the panel as shown in Figure C-39: USB Drive Connected in Panel to Retrieve Configuration File

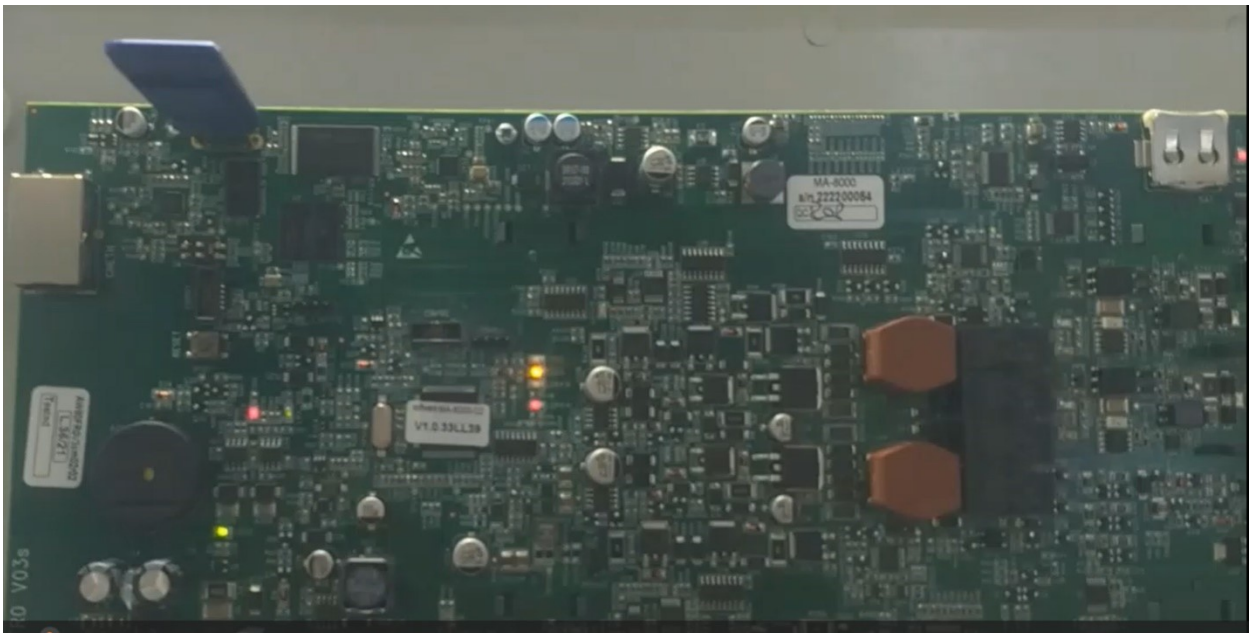


Figure C-39: USB Drive Connected in Panel to Retrieve Configuration File

• Locate the dip switch in the panel and move the SWITCH 1 to the upwards position.

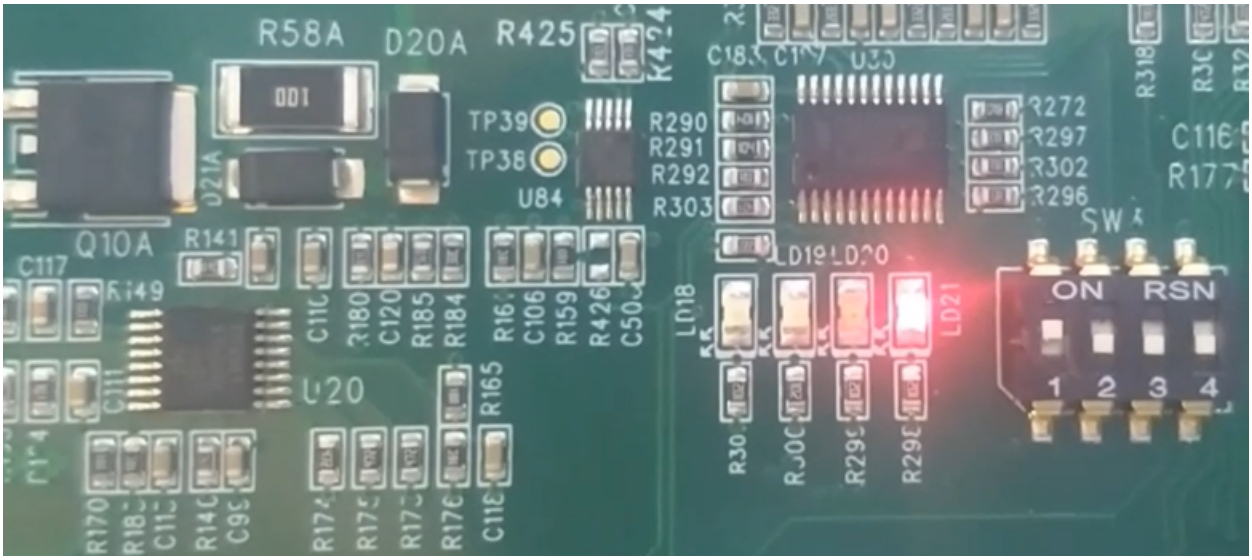


Figure C-40: Switch Position to Retrieve Configuration File

• At this stage panel will display message – “Export configuraiton done” message in its UI.
• Now press press over text to quit this window in panel UI, at this step configuration file in .BIN format is copyied into the USB drive.
• Copy this configuration file from USB drive into your PC/laptop.
• Open Morley MA1000-02 Morley-IAS tool as shown in Figure C-41: Morley - IAS Tool . And import the .BIN configuration file into this tool as shown in Figure C-42: Config File Import into Morley IAS Tool for converting the file into XML formal which can be uploaded to CLSS.

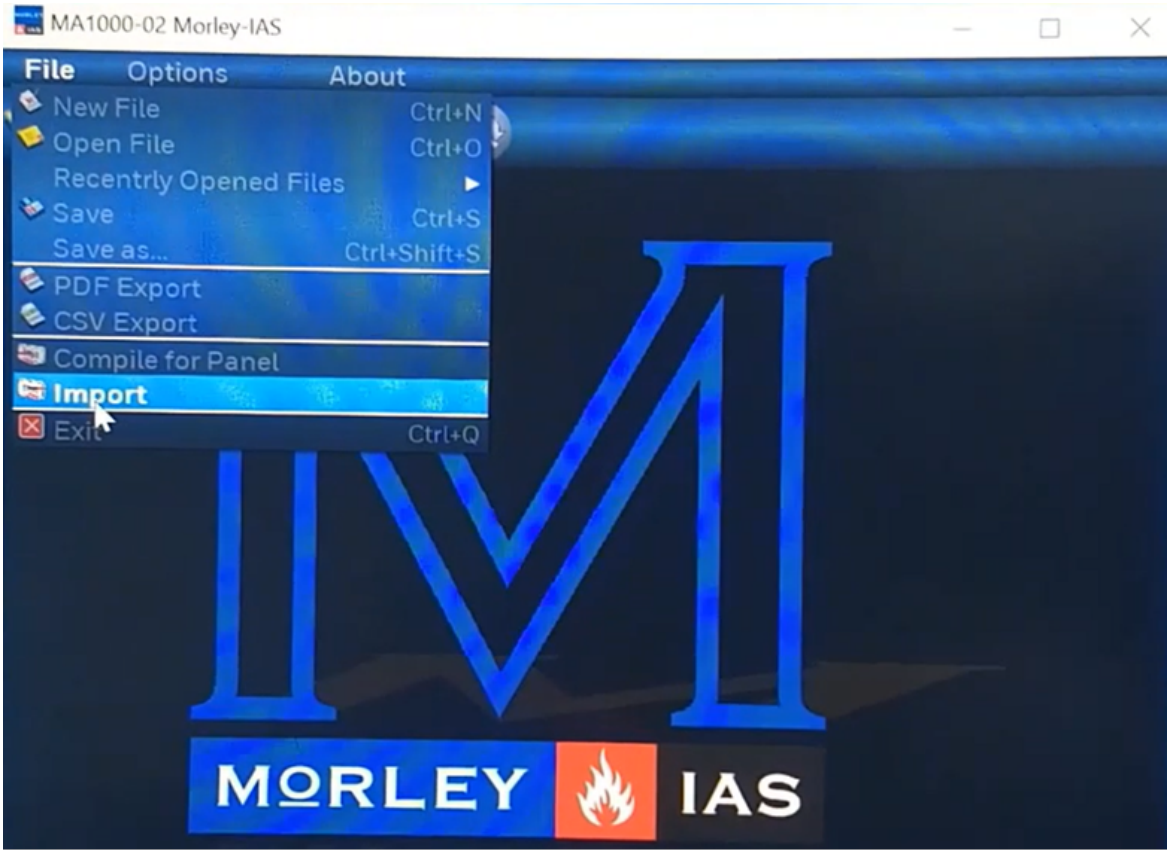


Figure C-41: Morley - IAS Tool

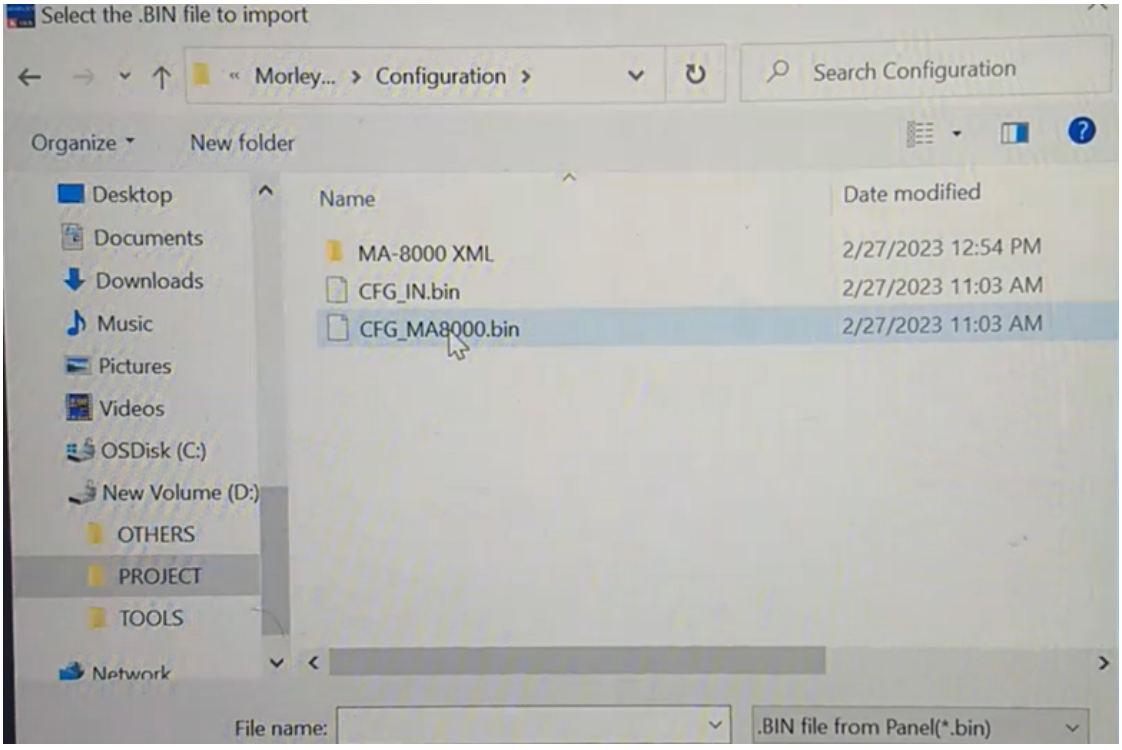


Figure C-42: Config File Import into Morley IAS Tool

• Now export the file into CSV format as shown in Figure C-43: Configuration File Export into CSV Format

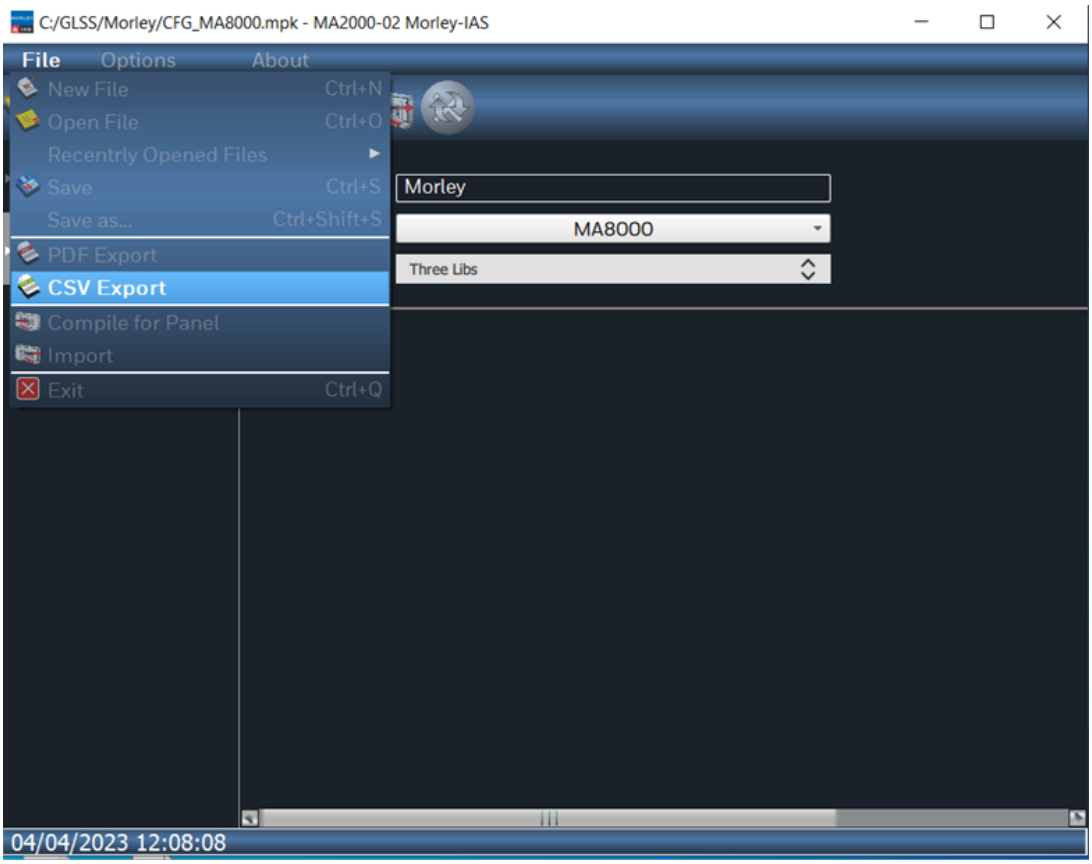


Figure C-43: Configuration File Export into CSV Format

• Select the required folder and export the file as shown in Figure C-44: Configuration File Export

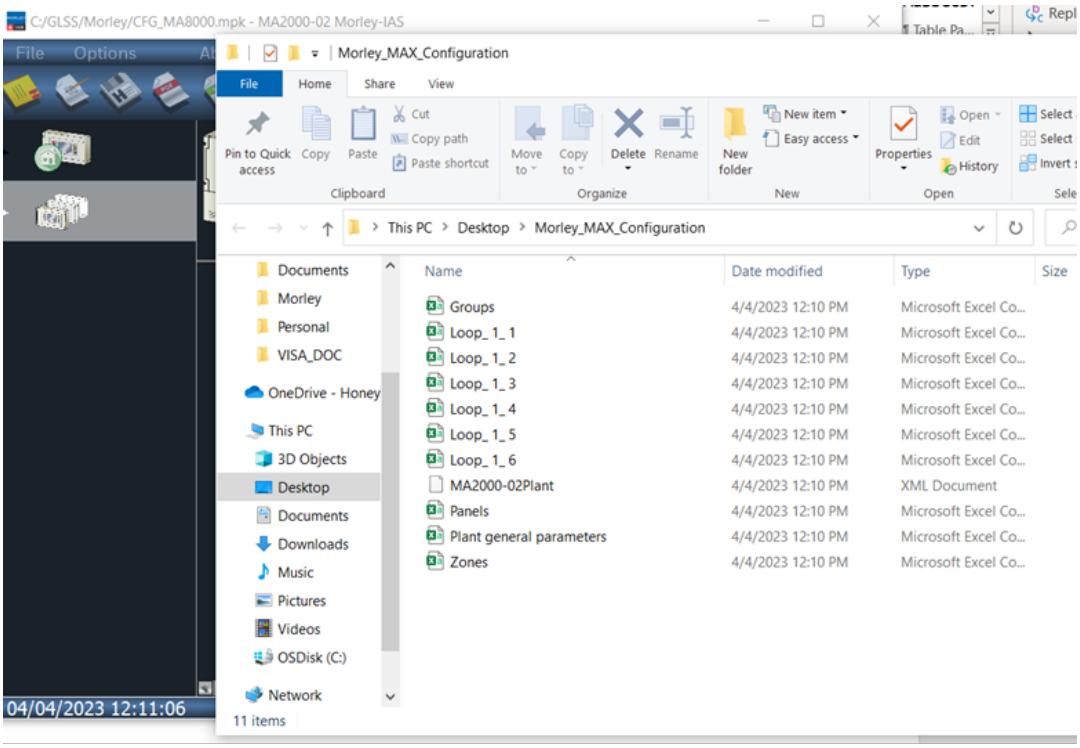


Figure C-44: Configuration File Export

• Now from the configuration export folder shows all the details of the panel set up with devices attached to it. Select the XML format of the configuration file and upload that to CLSS as shown in Figure C-45: Configuration File Upload to CLSS

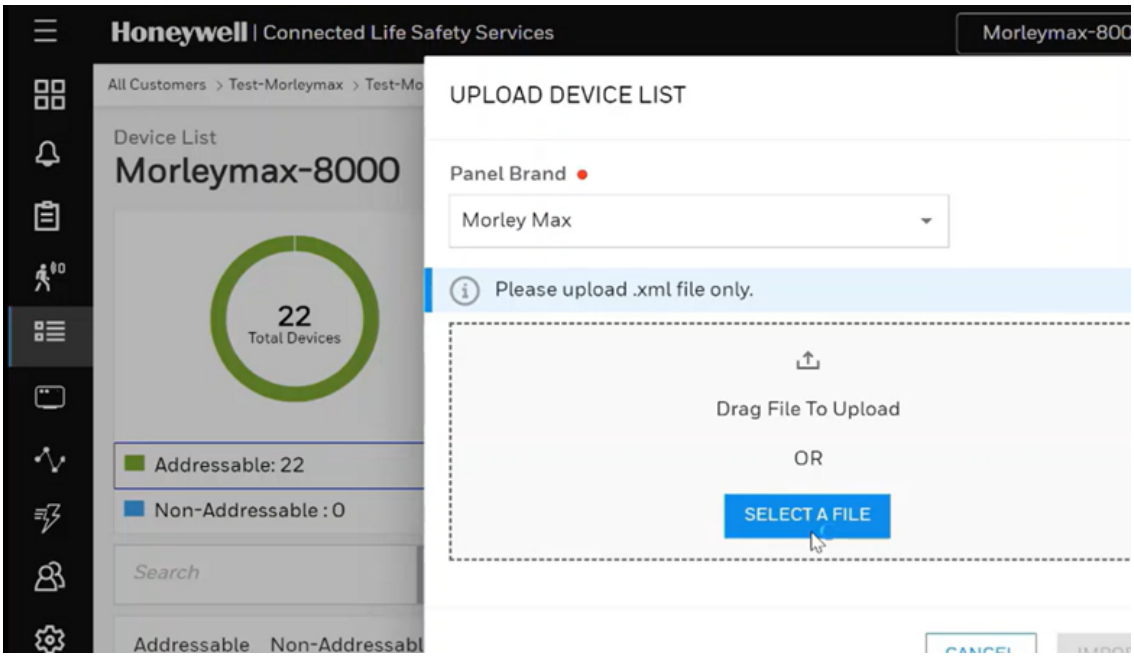


Figure C-45: Configuration File Upload to CLSS

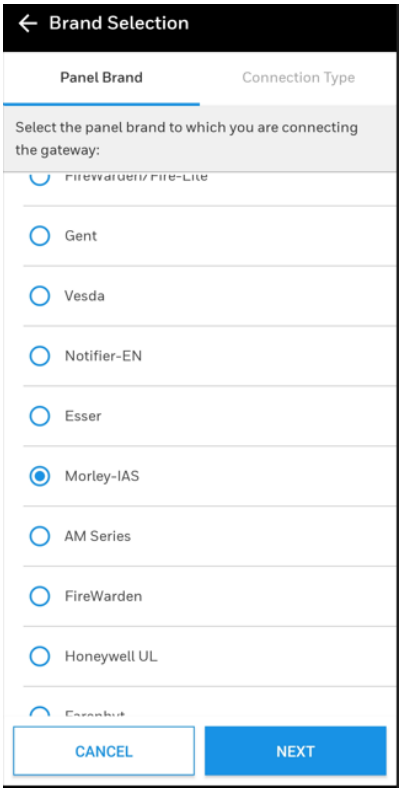


Figure C-46: Panel Brand Selection for Morley MAX Panel Series

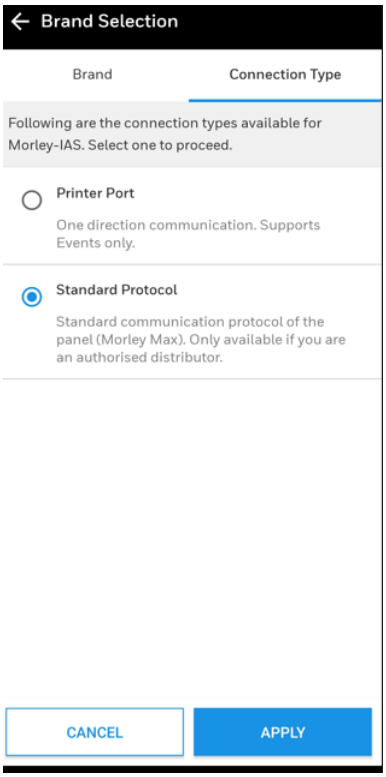


Figure C-47: Standard Protocol Selection for Morley MAX Series Panel

C.12 NOTIFIER® UL

C.12.1 CONNECTION OPTIONS

The gateway operates only with the NOTIFIER fire alarm control panels listed in the table below:

Table C.9 NOTIFIER UL Panel Connection Options

Fire Alarm Panel Models	RS-485	UART/TTL	NUP	USB
ONYX Panels				
NFS-320	No	No	Yes	No
NFS-640	No	No	Yes	No
NFS2-640	No	No	Yes	No
NFS-3030	No	No	Yes	No
NFS2-3030	No	No	Yes	No
INSPIRE Panels				
N16E	No	No	Yes	No
N16X	No	No	Yes	No
NCM-W	No	No	Yes	No
NCM-F	No	No	Yes	No
HSNCM-W	No	No	Yes	No
HSNCM-MF	No	No	Yes	No
HSNCM-SF	No	No	Yes	No
HSNCM-WMF	No	No	Yes	No
HSNCM-WSM	No	No	Yes	No
HSNCM-MFSF	No	No	Yes	No

C.12.2 TO USE A NUP CONNECTION

Some NOTIFIER panel variants use a NUP connection with the CLSS Gateway.

On the Gateway Side

• Connect the NUP cable to the NUP port of the gateway board.
The NUP port is labeled as 6 in the Figure C-48: Stand-alone Panel: NUP Connection .

On the Panel Side

In the NUP socket of the panel:

• Stand-alone Panel: Connect the NUP cable.

Direct Connection with the Panel

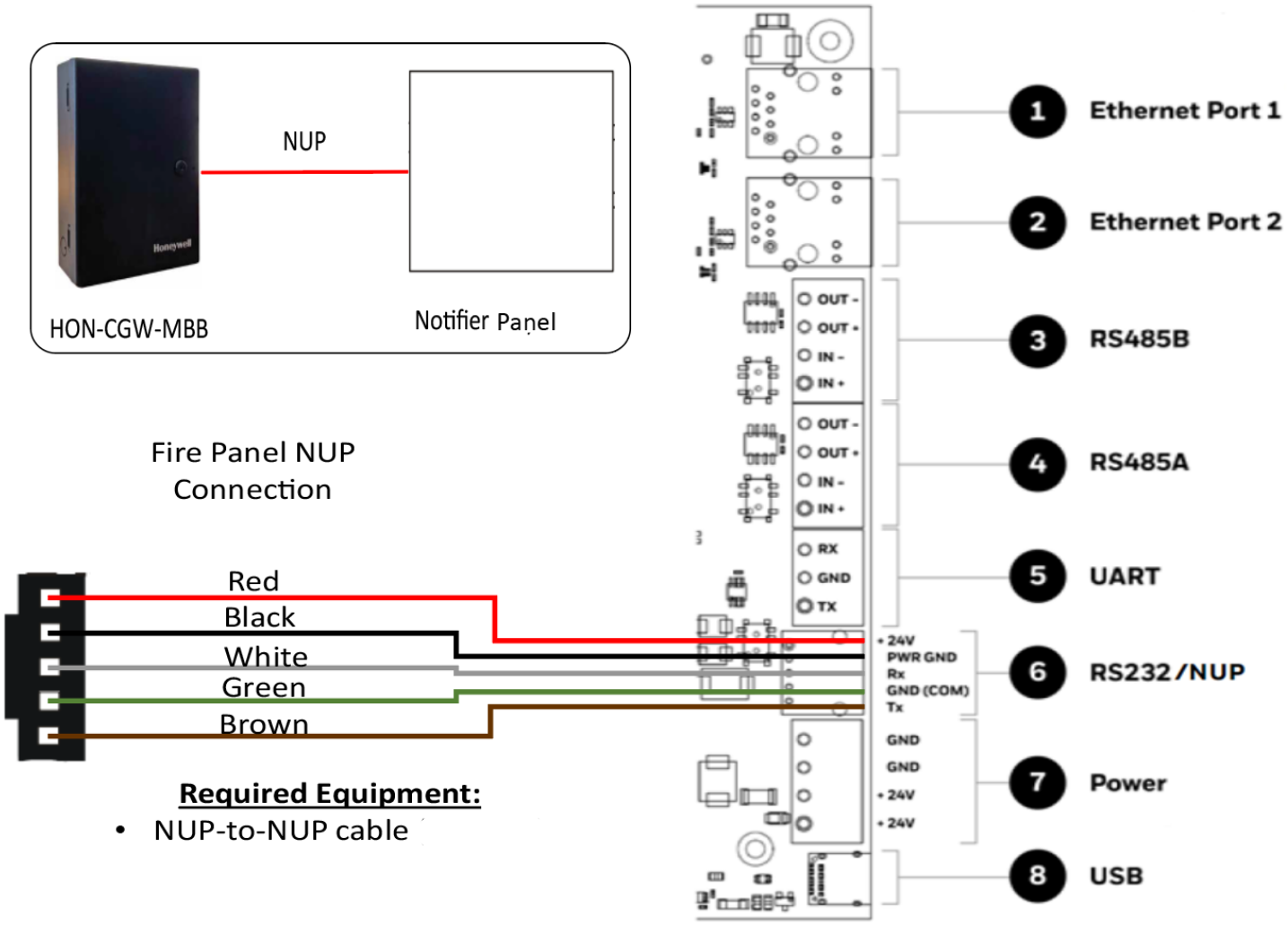


Figure C-48: Stand-alone Panel: NUP Connection

Connection through an NCM Card

Using required network cards the gateway can connect to a Standard-speed Network of Panels or High-speed Network of Panels.

Standard-speed Network of Panels

Add an additional standard NCM card to the panel for the gateway connection.

> **NOTE:** For the standard-speed network, each device should have its NCM card on the panel with an available port.

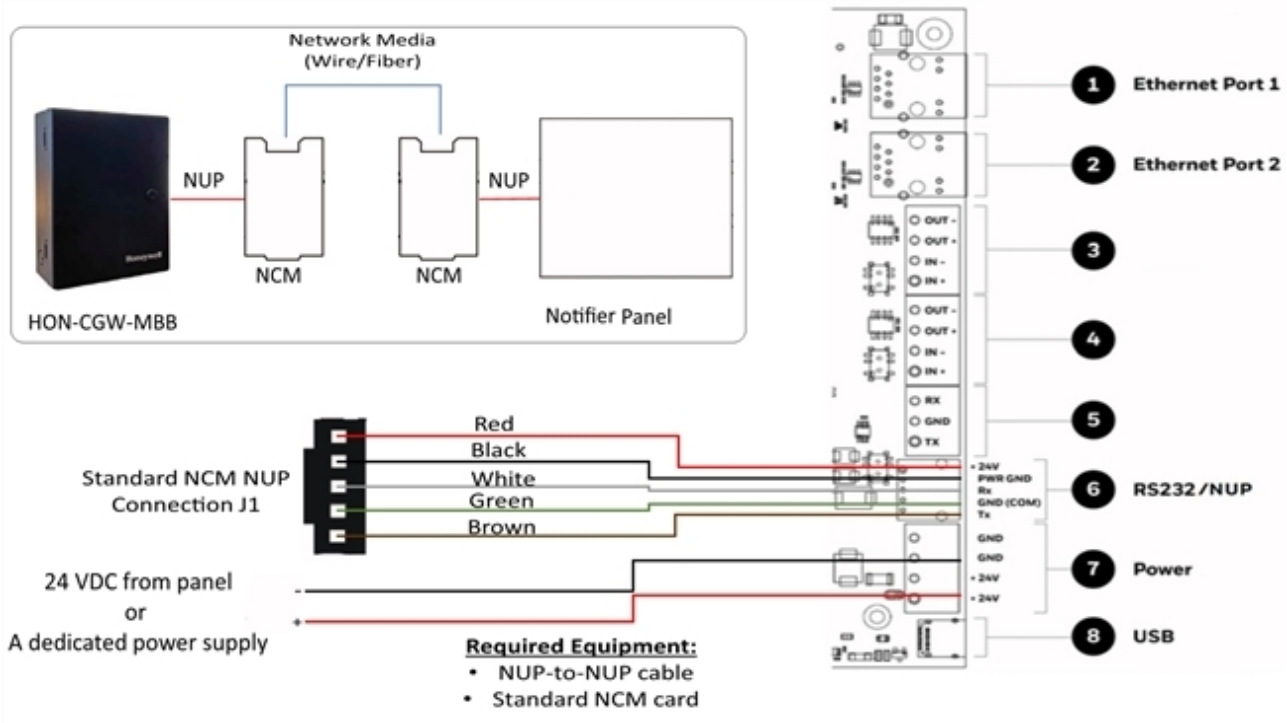


Figure C-49: Standard-speed Network Panel: NUP Connection

High-speed Network of Panels

Connect the NUP cable into an open NUP port of the HS-NCM card on the panel. If no NUP port is available, an additional HS-NCM card must be added and connected.

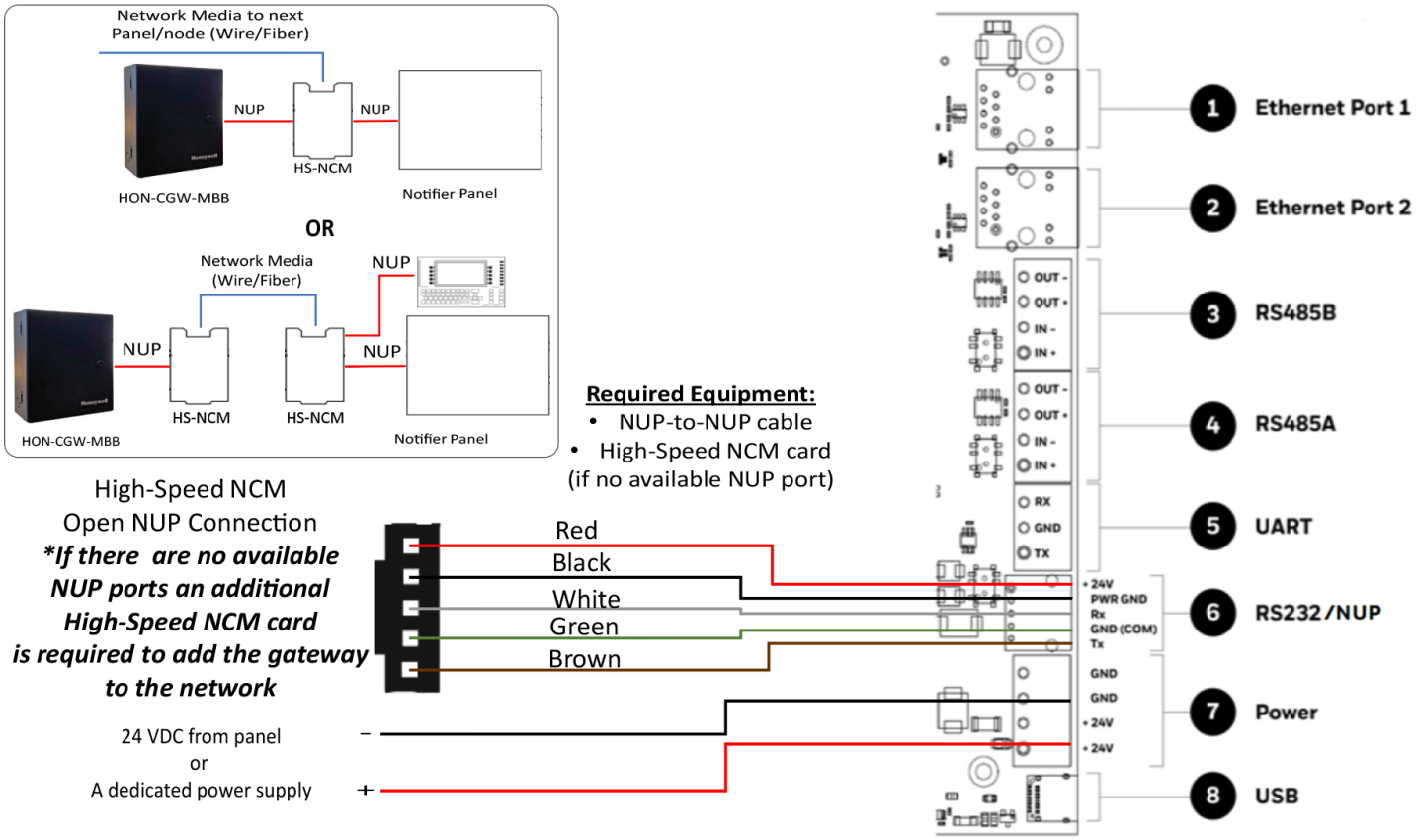


Figure C-50: High-speed Network Panel: NUP Connection

Connection through a DVC Card

Connect the NUP port of the gateway and the DVC with a NUP cable. Then, connect the NUP port of the DVC and the panel.

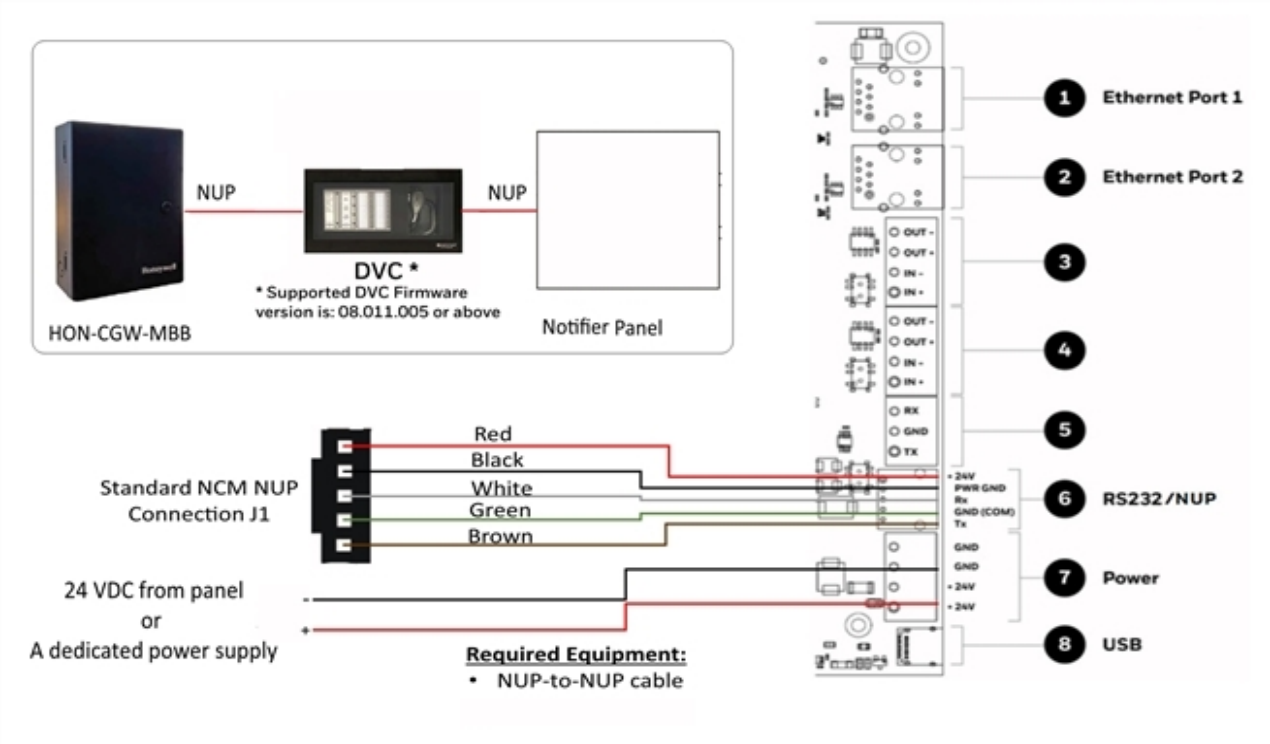


Figure C-51: Gateway Connection to Panel via DVC

N16 or NFS2-3030: Disconnection Messages

Disconnection Between the Gateway and the DVC		
Panel Message	[*GW_NODE_NUMBER*] OFF NETWORK	
Central Station Message	[*DVC_NODE_NUMBER*] COMMUNICATION LOSTOR [*FIRE PANEL_NODE_NUMBER*] COMMUNICATION LOST NETWORK MODULE COMMUNICATION LOST	
 CLSS GATEWAY  DVC  N16 or NFS2-3030 PANEL		
Panel Message	[*DVC_NODE_NUMBER*] COMMUNICATION LOST	
Central Station Message	[*FIRE PANEL_NODE_NUMBER*] COMMUNICATION LOST	
Disconnection Between the Gateway, DVC, and the Panel		
 CLSS GATEWAY  DVC  N16 or NFS2-3030 PANEL		
Panel Message	DVC COMMUNICATION LOST	[*FIRE PANEL_NODE_NUMBER*] COMMUNICATION LOST
Central Station Message		NETWORK MODULE COMMUNICATION LOST

C.12.3 POWER CONNECTION

NOTE: The external power supply must be dedicated and not shared with any other devices.

NOTE: The panel's power supply to the gateway must be within +24V DC power.

On the Gateway Side

Stand-alone Panel:

- Ensure that the NUP cable is connected with the NUP port of the gateway.
- Find the S7 switch next to the NUP port, and switch it towards *NUP_IN*.

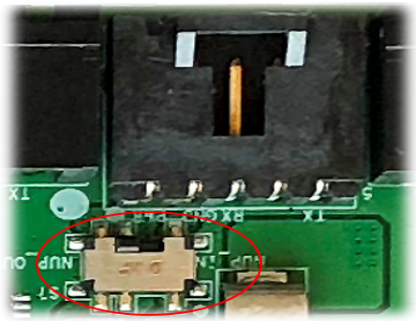


Figure C-52: The S7 Switch

High-speed or standard-speed network of panels:

- Connect to the +24V external power source or to the internal power supply of the panel.
- To power the HS-NCM or NCM over NUP from the gateway:
    - Find the S7 switch next to the NUP port, and switch it towards *NUP_OUT*.

On the Panel Side

- Stand-alone Panel: Ensure that the NUP cable is connected with the NUP port (J1) of the panel.
- Network of Panels: Connect to a +24V external power source or to the panel's power supply port.

C.13 NOTIFIER® EUROPEAN PANELS (EN)

C.13.1 CONNECTION OPTIONS

The gateway operates only with the NOTIFIER fire alarm control panels listed in the table below:

Table C.10 NOTIFIER European Panel Connection Options

Fire Alarm Panel Models	RS-485	UART/ TTL	NUP (RS-232)	USB	Ethernet
Pearl	Yes	No	Yes[1]	No	No
ID3000	No	No	Yes[2]	No	No
Inspire Notifier EN	No	No	Yes[3]	No	Yes

[1]Use the serial communication card (P/N: 124-426) on the panel
[2]Use the serial communication card (P/N: 124-300) on the panel
[3]Inspire Notifier EN panel version after Inspire Notifier EN 1.2 release supports ethernet connection on panel.

NOTE: Compatible CLSS Gateway firmware versions: 3.0.2.30 and above.

C.13.2 TO USE A NUP CONNECTION

Some NOTIFIER EN panel variants use a NUP connection with the CLSS Gateway.

On the Gateway Side

• Connect the NUP cable with a pre-formed connector to the NUP port of the gateway board.

Refer to Figure C-2: Gateway Connection Options - Bottom Side where the NUP port is labeled as 6. It is the P7 pin on the gateway board.

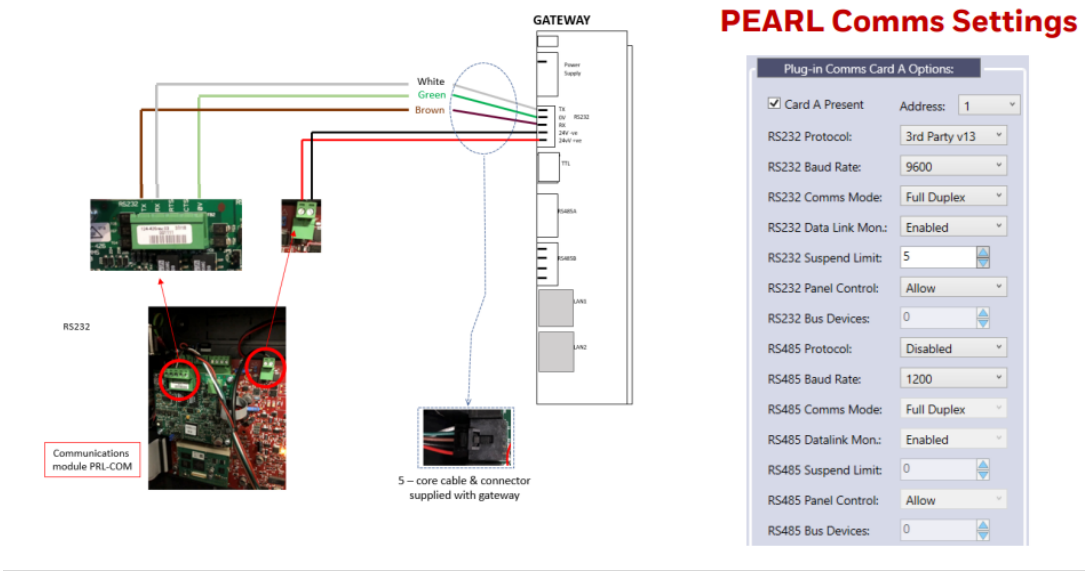
On the Panel Side

• Pearl Panel
• ID3000 Panel

Pearl Panel

In the TB2 terminal at the communication card on the panel:

- Connect the White wire to the RxD+ pin.
- Connect the Green wire to the Gnd pin.
- Connect the Brown wire to the TxD+ pin.



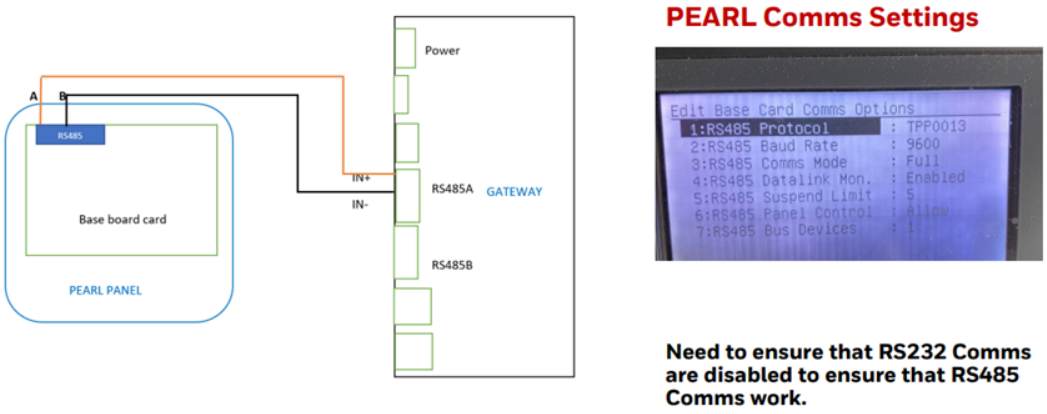


Figure C-53: Pearl Panel Setting and Connection with CLSS Gateway

ID3000 Panel

In the SK1 terminal at the communication card on the panel:

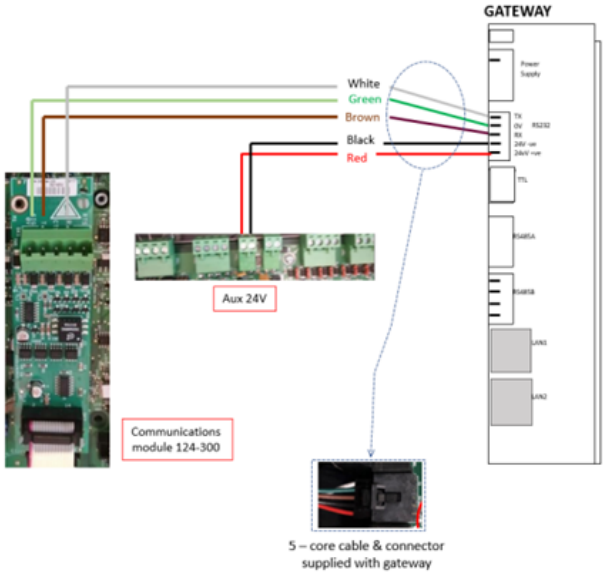
- Connect the White wire to the RxD+ pin.
- Connect the Green wire to the Gnd pin.
- Connect the Brown wire to the TxD+ pin.

OR

At the RS232/FT35 terminal of the panel:

- Connect the White wire to RxD pin.
- Connect the Green wire to GND pin.
- Connect the Brown wire to TxD pin.

The RS232/FT35 is a diagnostic port, which also supports data transmission between the panel and the gateway.



ID3K Comms Settings

Baud Rate	9.6Kb/s
Comms Protocol	TPP V 11 (bidirectional)

Configuring the Isolated RS232 Output

1. Open Panel settings on the ID3000
2. Select 17. Isolated RS232 Port Setup
3. Select Mode of Operation as 3rd Party RS232
4. Select Protocol 011A
5. Select Full Duplex
6. Select Enabled for Controls
7. Select Enabled for Fault Monitoring
8. Select Logged for Communications Stopped Fault to Appear
9. Select Timeout to 20 seconds

Figure C-54: ID3K Panel Setting and Connection with CLSS Gateway

C.13.3 TO USE AN RS-485 CONNECTION

Some NOTIFIER panel variants use an RS-485 connection with the CLSS Gateway.

Only a standalone panel can have an RS-485 connection.

On the Gateway Side

- Connect +ve wire to RS485 IN+ port.
- Connect -ve wire to RS485 IN- port.

Refer to Figure C-2: Gateway Connection Options - Bottom Side where the RS-485B and RS-485A ports are labeled as 3 and 4. They are the P5 and P1 pins on the gateway board.

On the Panel Side

- "Pearl Panel" below

Pearl Panel

At the TB6 terminal of the panel's board:

- Connect the +ve wire to the A pin.
- Connect the -ve wire to the B pin.

C.13.4 POWER CONNECTION

The gateway can receive its power either from an external power source or from the non-resettable internal power of the panel.

> **NOTE:** The external power supply must be dedicated and not shared with any other devices.

For the External Power Supply:

> **NOTE:** The panel's power supply to the gateway must be within +24V DC power.

On the Gateway Side

- Connect to the 24V DC external power supply or to the panel's 24V DC power port.
- Ensure that the S7 switch next to the RS-232 port is switched towards *NUP_OUT*.

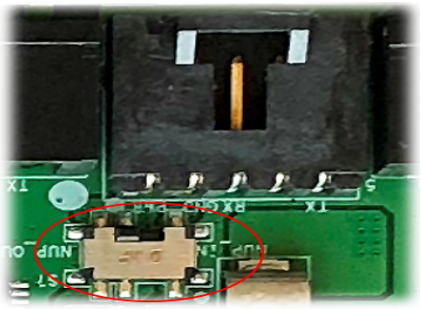


Figure C-55: The S7 Switch

On the Panel Side

Pearl Panels: At the TB7 terminal of the panel's board:

- Connect the +ve wire to the +ve pin.
- Connect the -ve wire to the -ve pin.

ID3000 Panels: At the SK4 terminal of the panel's board:

- Connect the +ve wire to the +ve pin.
- Connect the -ve wire to the -ve pin.

External Power Supply

Use this option if the gateway is *not* receiving the power from the panel.

On the Gateway Side

- Connect to the power port of the gateway.

Refer to Figure C-2: Gateway Connection Options - Bottom Side where the power port on the gateway is labeled as 7. It is the P2 pin on the gateway board.

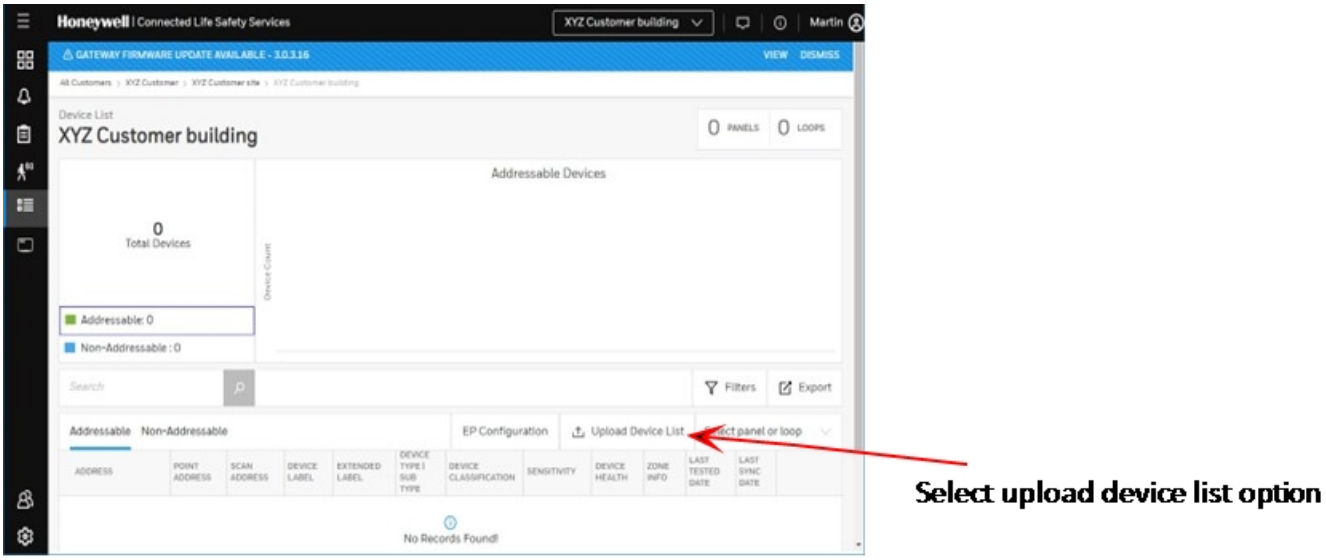
On the External Power Supply Side

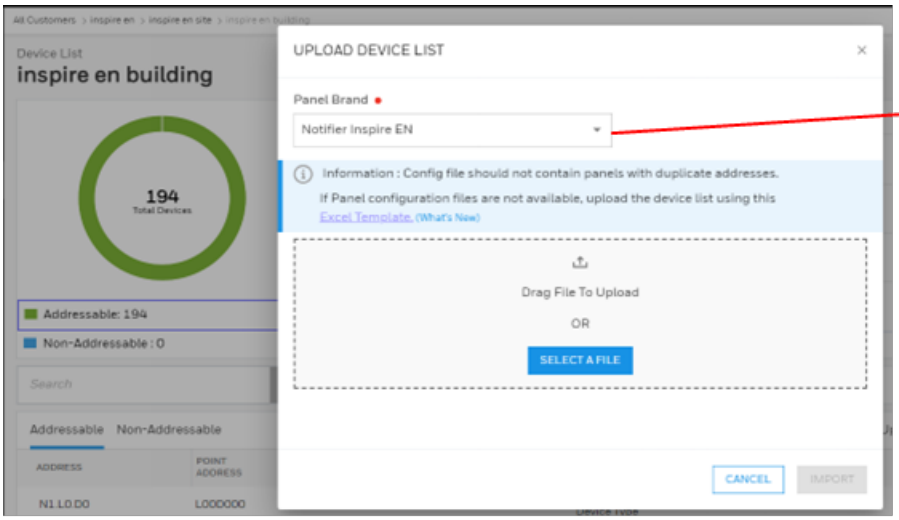
- Connect to the 24V DC external power supply.

C.14 NOTIFIER INSPIRE EN

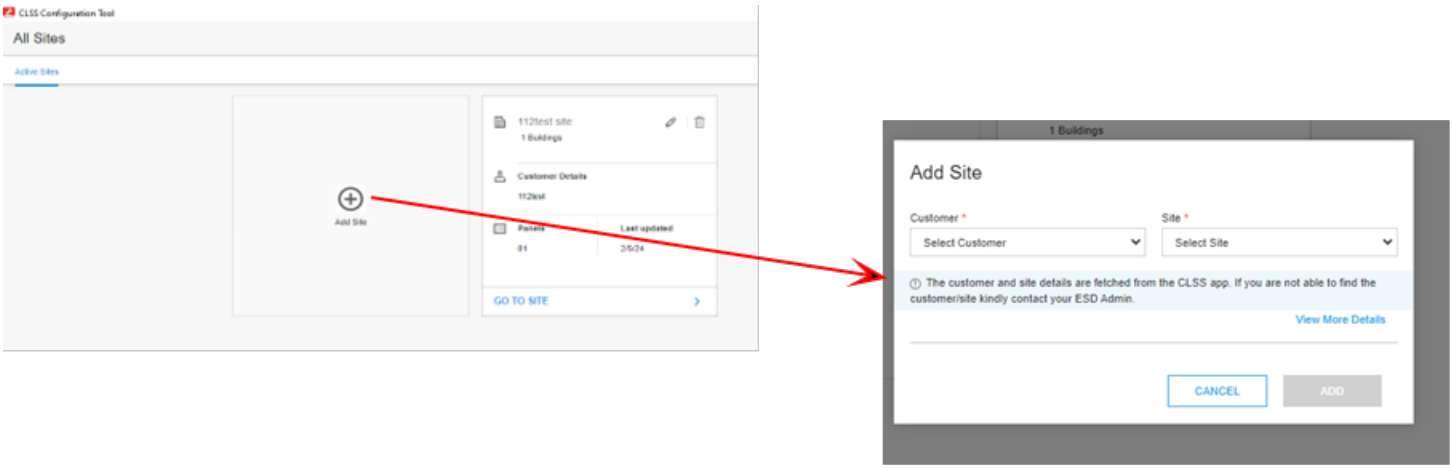
Gateway to panel connection details

Import Device Configuration

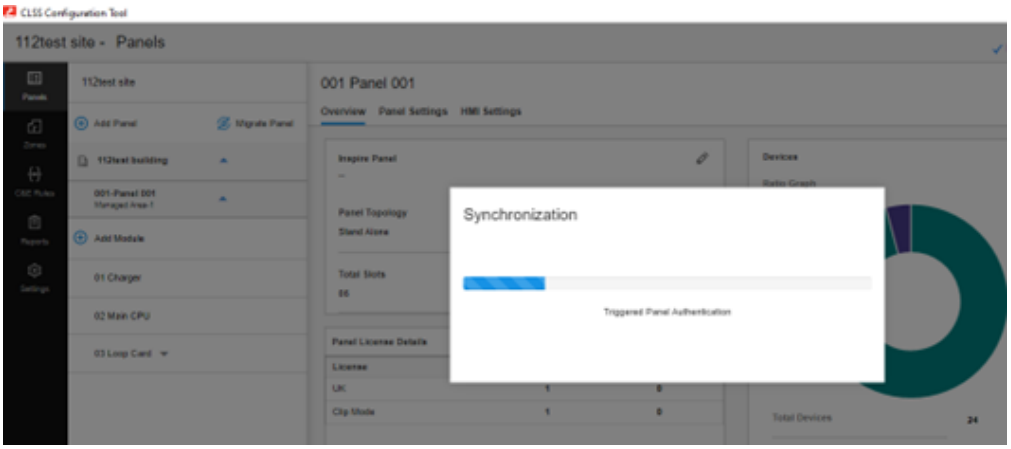


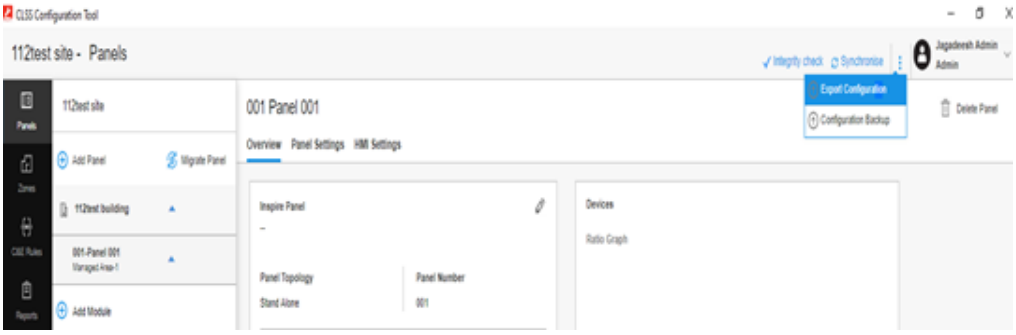


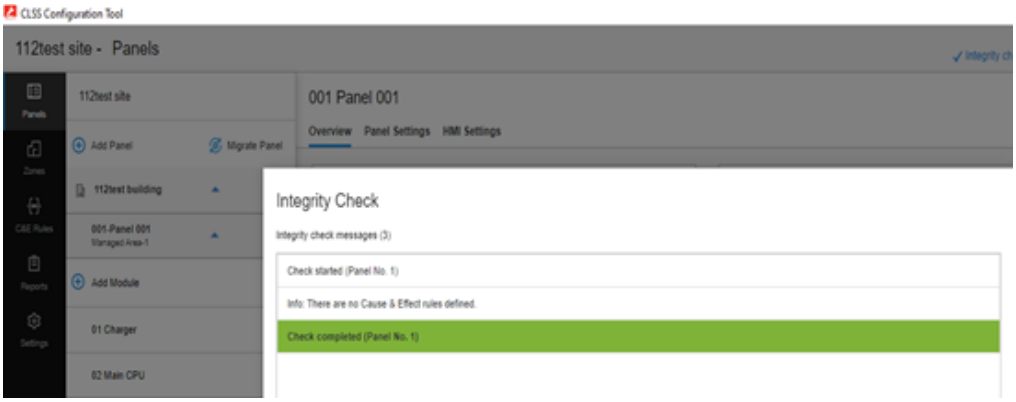
Automatic upload through Inspire EN "CLSS Configuration Tool"

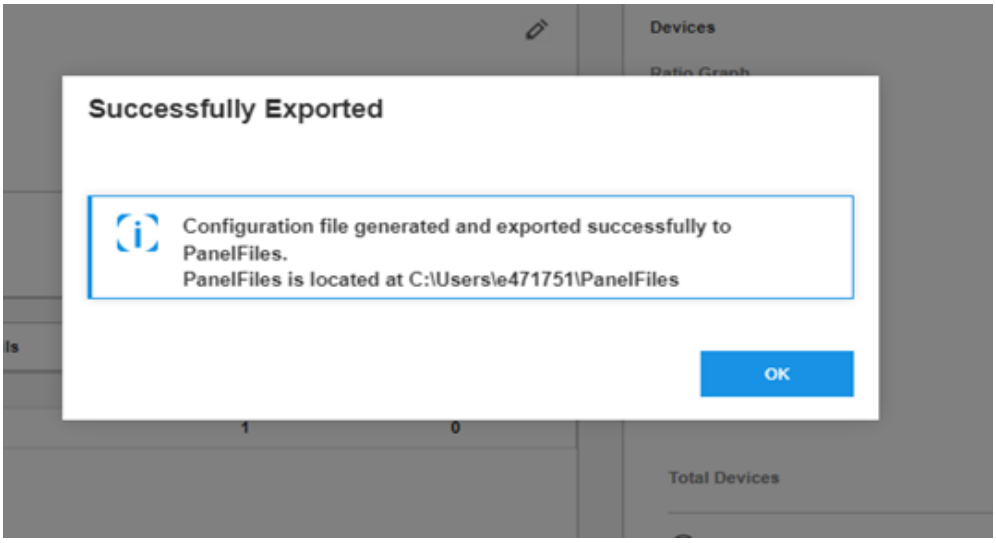


Extracting the configuration manually, saving it in PC and then performing a manual upload of zip file.









C.15 AM SERIES PANELS

C.15.1 CONNECTION OPTIONS

The gateway operates only with the AM Series fire alarm control panels listed in the table below:

Table C.11 AM Series Panel Connection Options

Fire Alarm Panel Models	RS-485	UART/TTL	RS-232	USB
AM1000CL[2]	Yes	No	Yes[1]	No
AM2000CL[2]	Yes	No	Yes[1]	No
AM6000CL[2]	Yes	No	Yes[1]	No
AM8200N[3]	Yes	No	No	No
AM8100[3]	Yes	No	No	No

[1]Use the SIB 8200 board
[2]AM1000CL, AM2000CL and AM6000CL Use the Terminal Board AW80US0
[3]AM8200N and AM8100 have RS485connectors on AW70PC0 board.

NOTE: AM8200N can be networked with AM8200N panels. All other panels are stand alone.

NOTE: The panel can be a stand alone panel or part of a network of panels.

C.15.2 MINIMUM REQUIRED VERSIONS

- For the Panel/CPU1and LIB (AM2000CL, AM6000CL): CPU.V1.0.49 and LL51-
- For the Panel/CPU1 and LIB: CPU.V1.0.50 and LL51-
- For the CLSS Gateway: 3.5.5.32

C.15.3 TO USE AN RS-232/RS-485 CONNECTION TO ESTABLISH CONNECTION BETWEEN PANEL (AM1000CL, AM2000CL, AM6000CL, AM8200N, AND AM8100) AND GATEWAY

On the AW80US0 terminals of the panel board, the reference connector for TPP serial communication is CNS:

- CNS is a double-row connector.
- the useful terminals for the TPP connection are 4, 5, 6 (Note are in the lowest row).
- these terminals are used for both RS232 and RS485 connection

CNS-4 RS485_H RS232_TX
CNS-5 GND GND
CNS-6 RS485_L RS232_RX

Switch

On the AW80FR0 front board via SW5 (4-way dip switch or slide switch) it is possible to set RS232 / RS485.

If the customer has the first hardware version of the AW80FR0 v01s front board: SW5 is a 4-way dip switch.

RS232 SW5 1..4: ON ON OFF
RS485 SW5 1..4: OFF ON ON For all hardware versions subsequent to AW80FR0 v02s (inclusive)
SW5 is a slide switch and the settings.
RS232 / RS485 are clearly marked on the board itself.

To switch RS232 <--> RS485:

- Switch off the control unit
- Disconnect from CNS-4, CNS-5, CNS-6 the device acting as External Equipment
- Set SW5 correctly.
- Connect the device acting as External Equipment properly to CNS-4, CNS-5, CNS-6
- Switch on the control panel.

Note – CNS 7, 8 and 9 can also be used for RS232/RS485 connection.

Panel side RS232 lines will be connected on to CNS– 4/CNS -7(TX), CNS-5/ CNS-8(GND) and CNS-6/ CNS-9(RX) on AW80US0 board. Power line +ve (CNU-9) and GND- (CNU-10).

Panel side RS485 lines will be connected on to CNS– 4/CNS -7(+ve), and CNS-6/ CNS-9(-ve) on AW80US0 board.

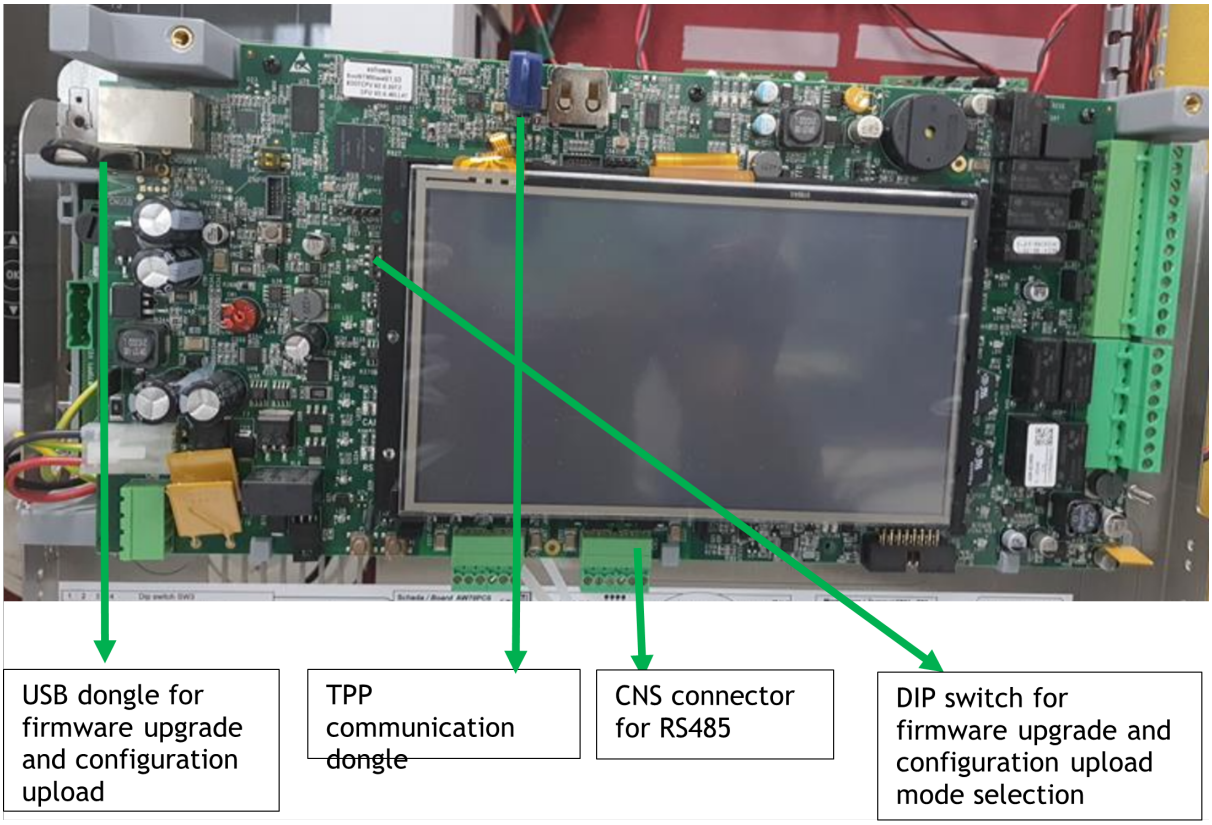


Figure C-56: AM8200N/AM8100 Block Diagram

Table C.12 RS485 pin details in CNS terminal for AM8200 and AM8100N panels

CNS Terminal		
Pin Numbers	**Details**	
1	LIN + 1	RS485 COMMUNICATOR
2	GNDIS 1	
3	LIN - 1	
4	LIN + 2	RS485 per LCD-8200
5	GNDIS 2	
6	LIN - 2	

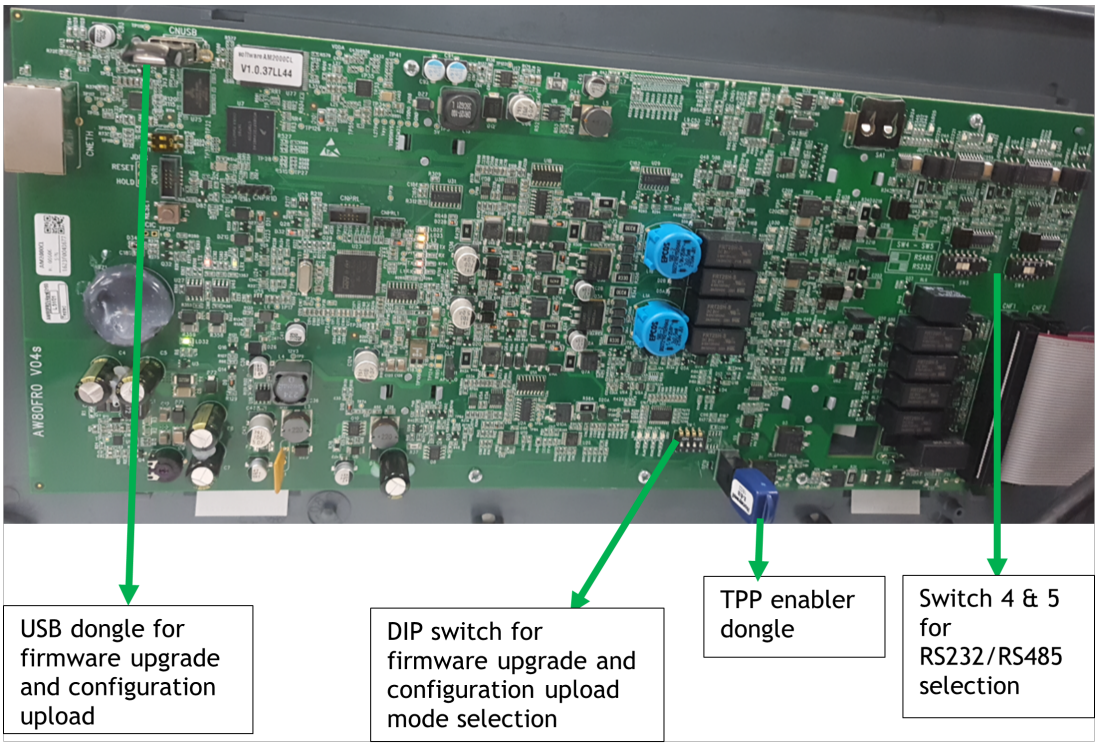
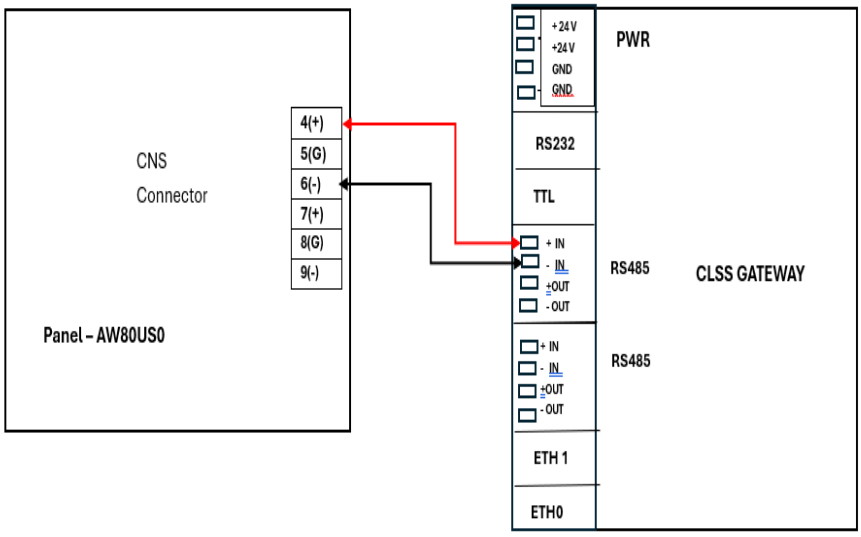


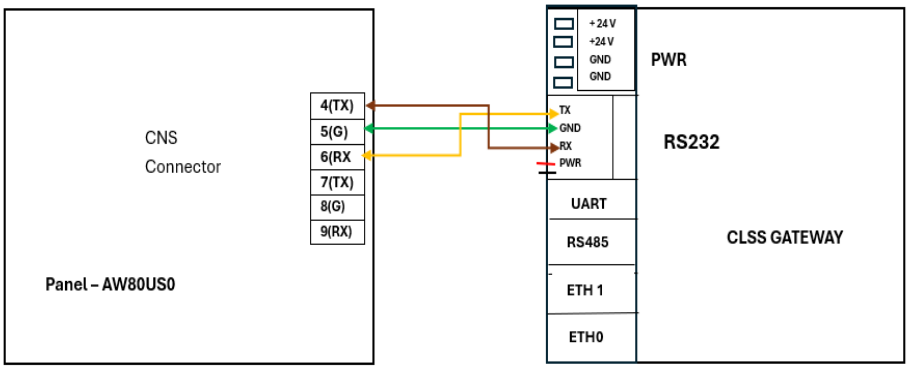
Figure C-57: AM CL Series Block Diagram

Figure C-58: CNS Connectors on AW80US0 Board for AM-CL series panels



NOTE: Pin 4 and 6 or 7 and 9 can be used in AW80US0 board for RS485 connection

Figure C-59: AM_CL series RS485 Connection Diagram



NOTE: Pin 4,5,6 or 7,8,9 can be used in AW80US0 for RS232 connection

Figure C-60: AM_CL series panels Connection Diagram using RS232

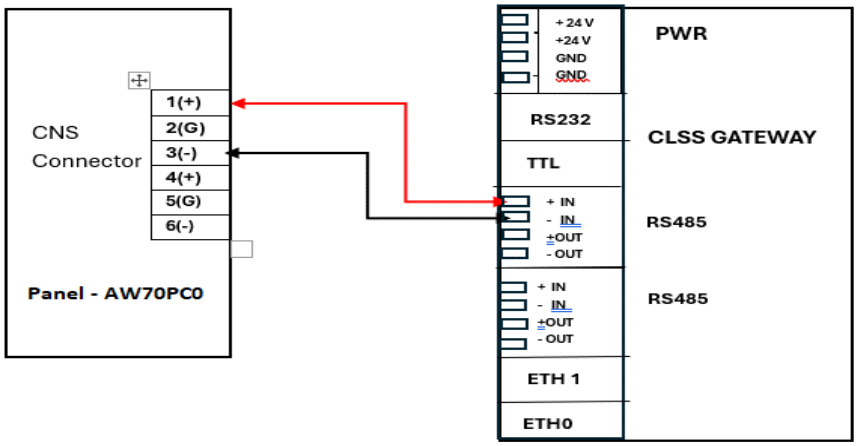


Figure C-61: AM8200N and AM8100 panels Connection Diagram using RS485

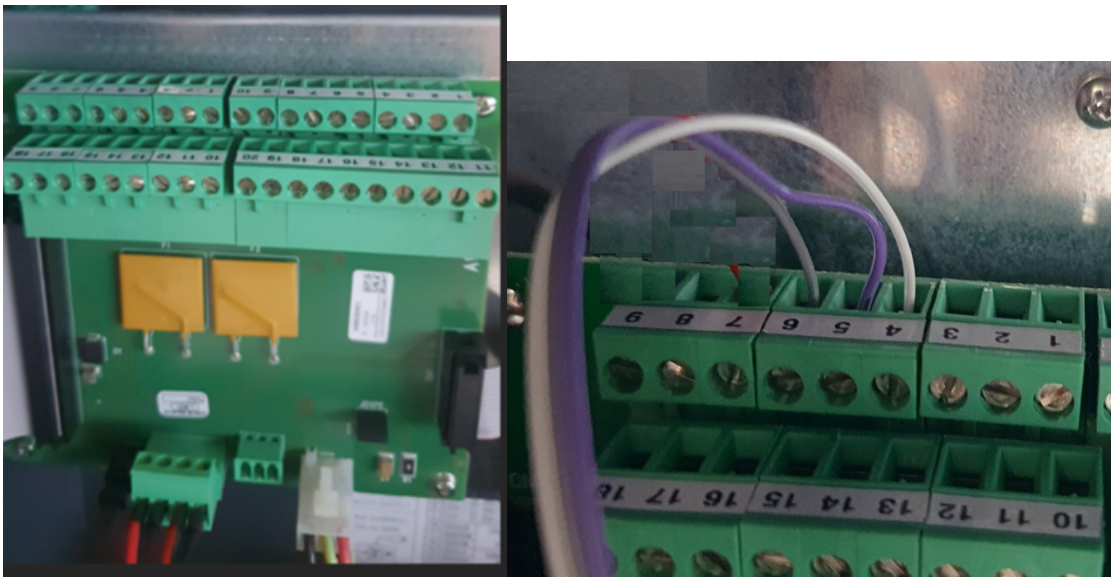


Figure C-62: CNS Connector on AW80US0 Board of Panel with RS-232 Connection AM CL Series Panel

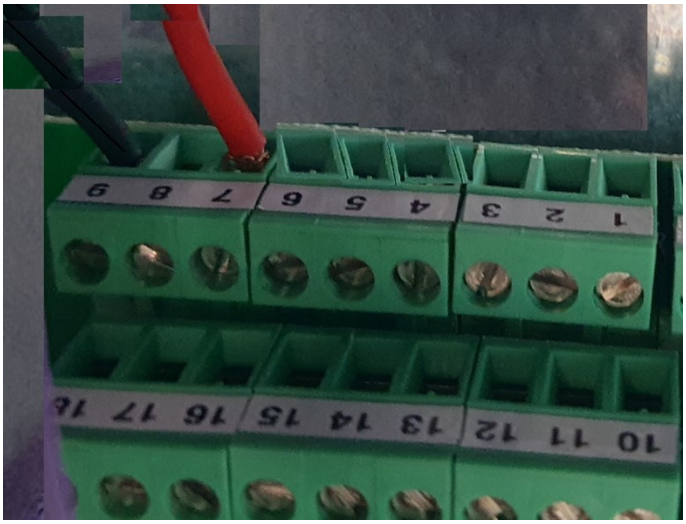


Figure C-63: CNS Connector on AW80US0 Board of Panel with RS-485 AM CL Series Panels

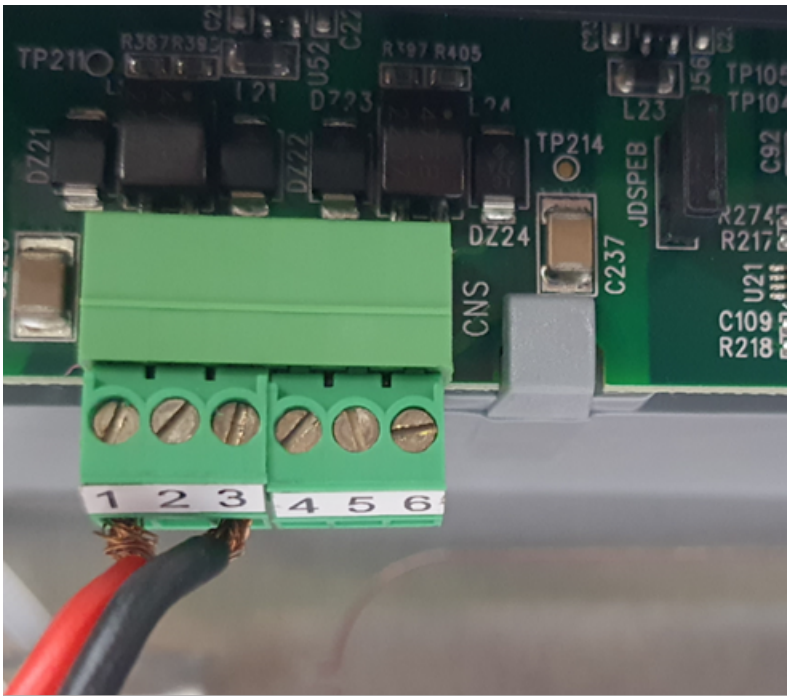


Figure C-64: CNS Connector on AM70PC0 Board of Panel with RS-485 Connection AM8200N/AM8100 Series Panel

Communication

Valid both for RS-232 and RS0485:

Baud Rate (Fixed): 38400
Number of Bits (Fixed): 8
Stops Bits (Fixed): 1
Parity (Fixed): none

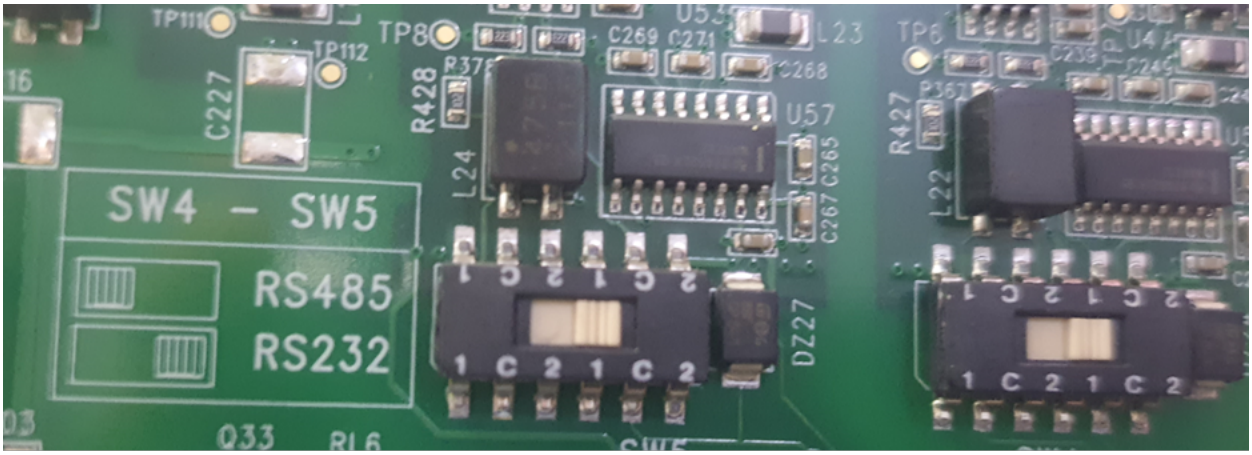


Figure C-65: Slide Switch Detail for RS-232/RSA-485 Selction AM CL Panels

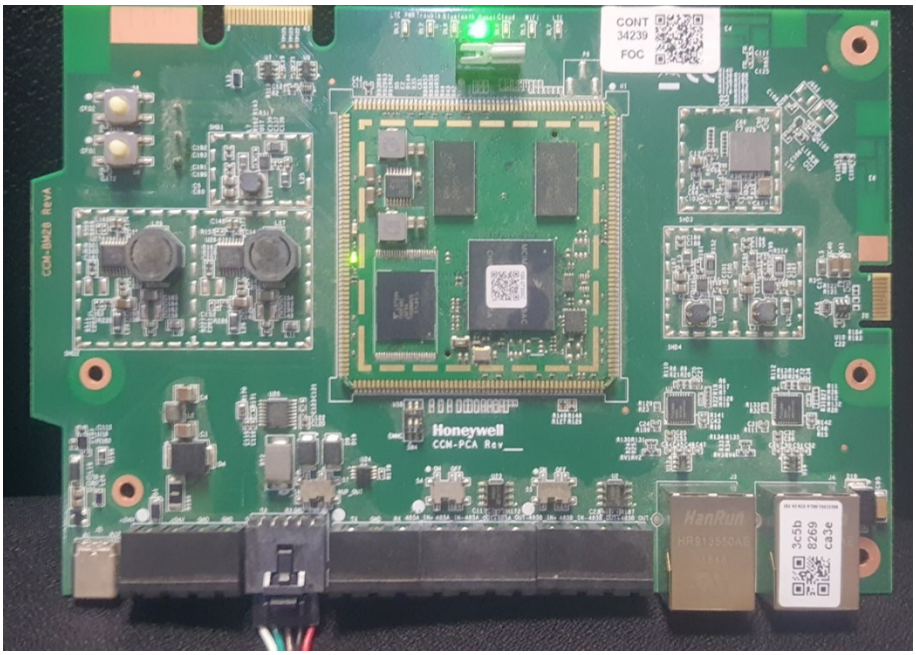


Figure C-66: Gateway Board with RS-232 Connection

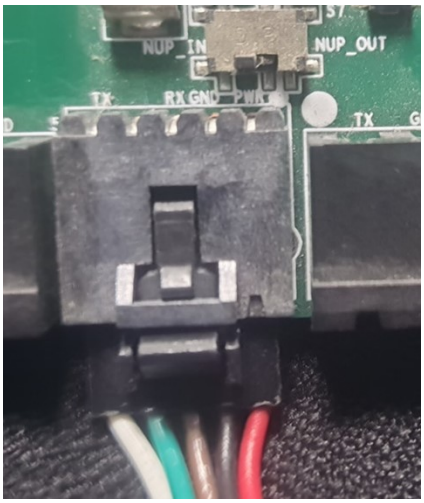


Figure C-67: Gateway RS-232 and Power Connection Detail

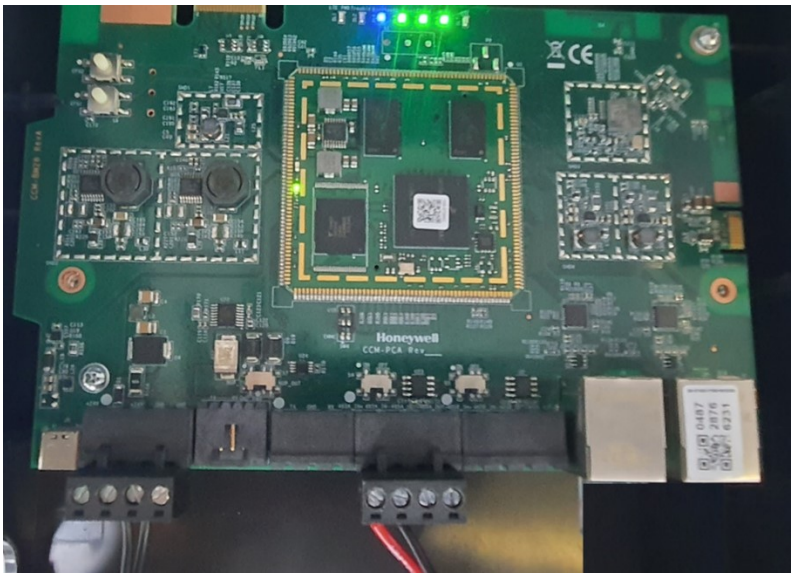
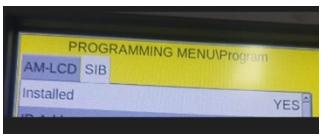


Figure C-68: Gateway Board with RS-485 Connection

Enabling the Serial Communication in Panel

Go to panel programming manu, SIB to be installed.



C.15.4 TO UPLOAD PANEL CONFIGURATION FILE TO CLOUD

Before installing the gateway, configuration file of the panel set up needs to be uploaded to cloud.

Steps involved in uploading the configuration file:

• Connect the USB drive into panel as shown in

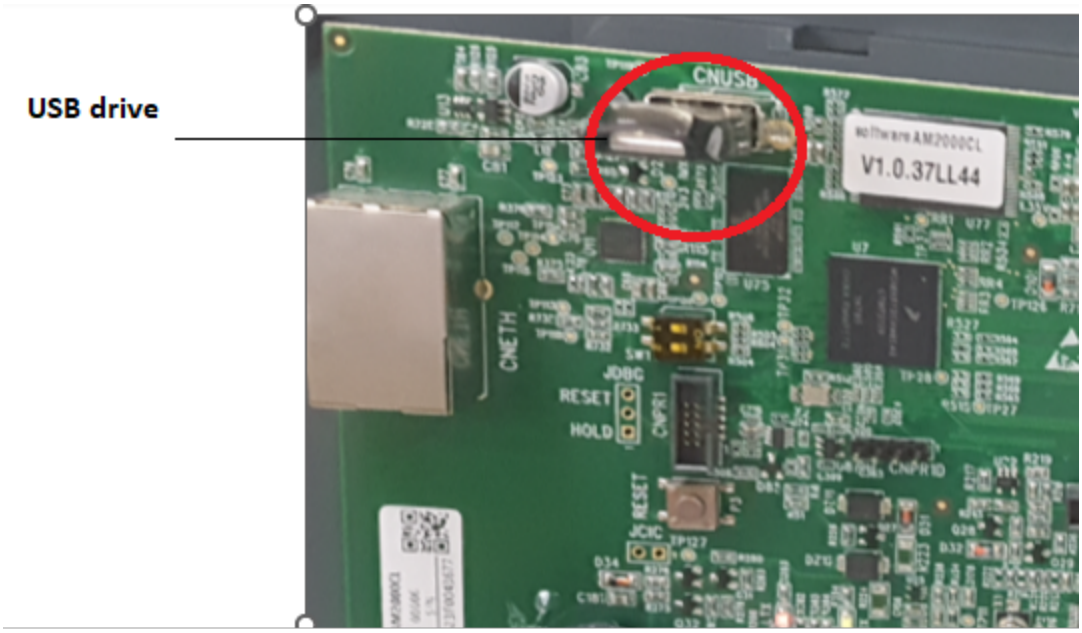


Figure C-69: USB Drive Connected in Panel to Retrieve Configuration File

• Locate the dip switch in the panel and move the SWITCH 1 to upwards position.

Figure C-70: Switch Position to Retrieve Configuration File in AM CL Series Panels

Figure C-71: Switch Position to Retrieve Configuration File in AM8200N/Am8100 Series Panel

• At this stage panel will display message – “Export configuraiton done” message in its UI.
• Now press press over text to quit this window in panel UI, at this step configuration file in .BIN format is copyied into the USB drive.
• Copy this configuration file from USB drive into your PC/laptop.
• Open AM 1000CL Notifier IT tool as shown in Figure C-72: AM CL Series Tool and import the .BIN configuration file into this tool as shown in Figure C-73: AM8200N/AM8100 Series Tool for converting the file into XML formal which can be uploaded to CLSS.

Figure C-72: AM CL Series Tool

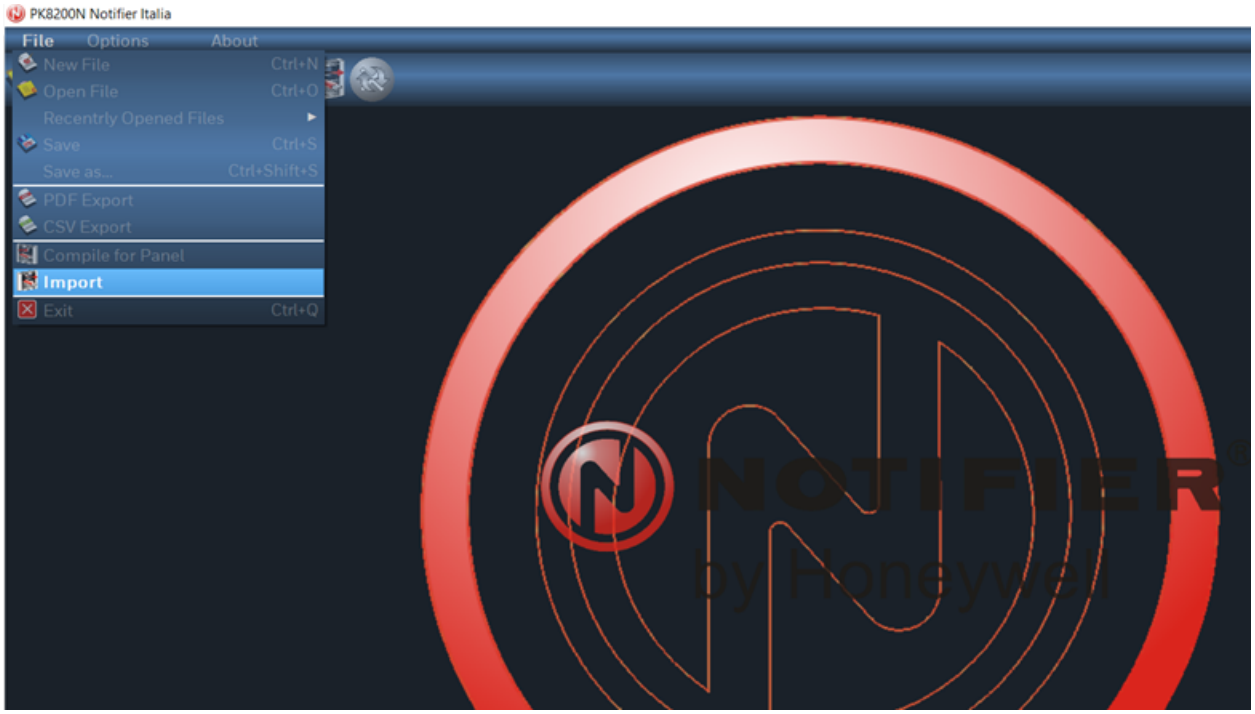


Figure C-73: AM8200N/AM8100 Series Tool

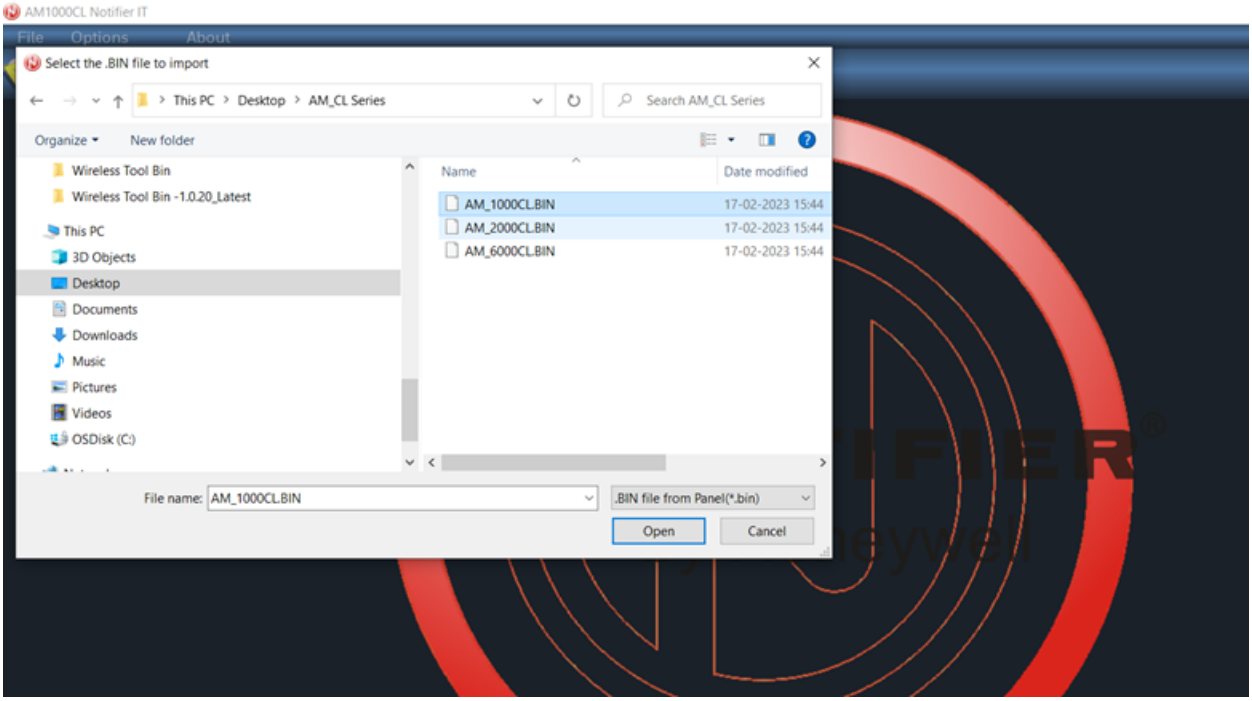


Figure C-74: Config File Import into AM CL Series Tool

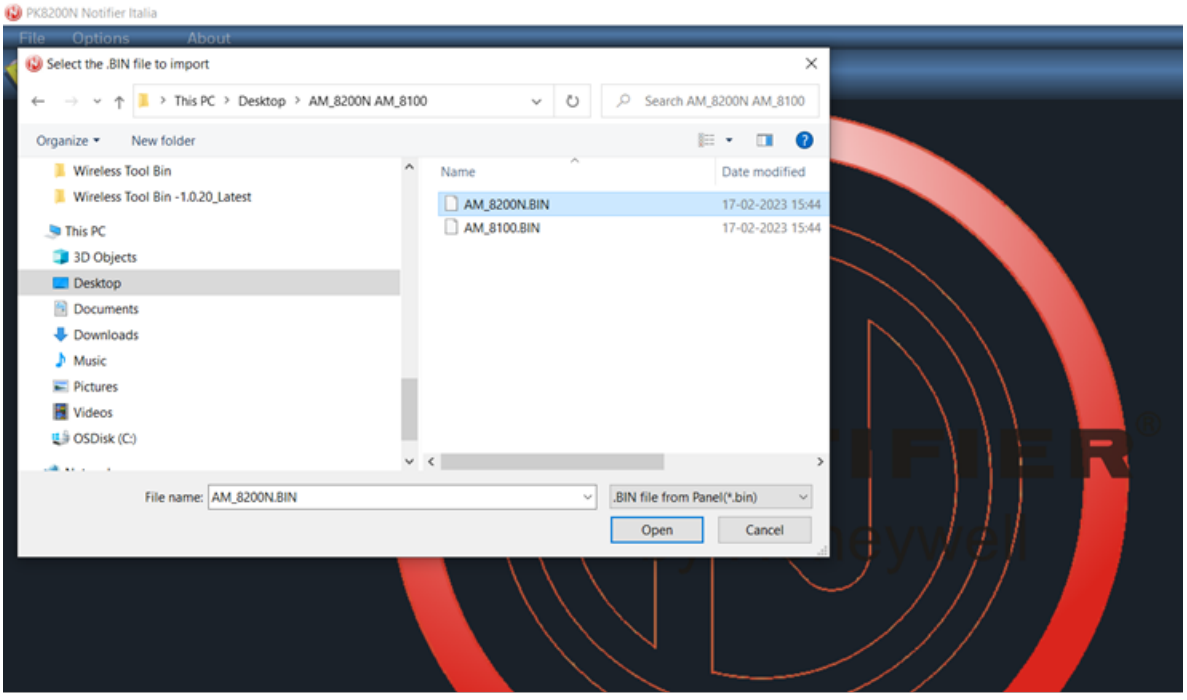


Figure C-75: Config File Import into AM8200N Tool

• Now export the file into CSV format as shown in Figure C-76: Configuration File Export Into CSV Format

Figure C-76: Configuration File Export Into CSV Format

• Now from the configuration export folder shows all the details of the panel set up with devices attached to it. Select the XML format of the configuration file and upload that to CLSS as shown in Figure C-77: Configuration File Upload to CLSS

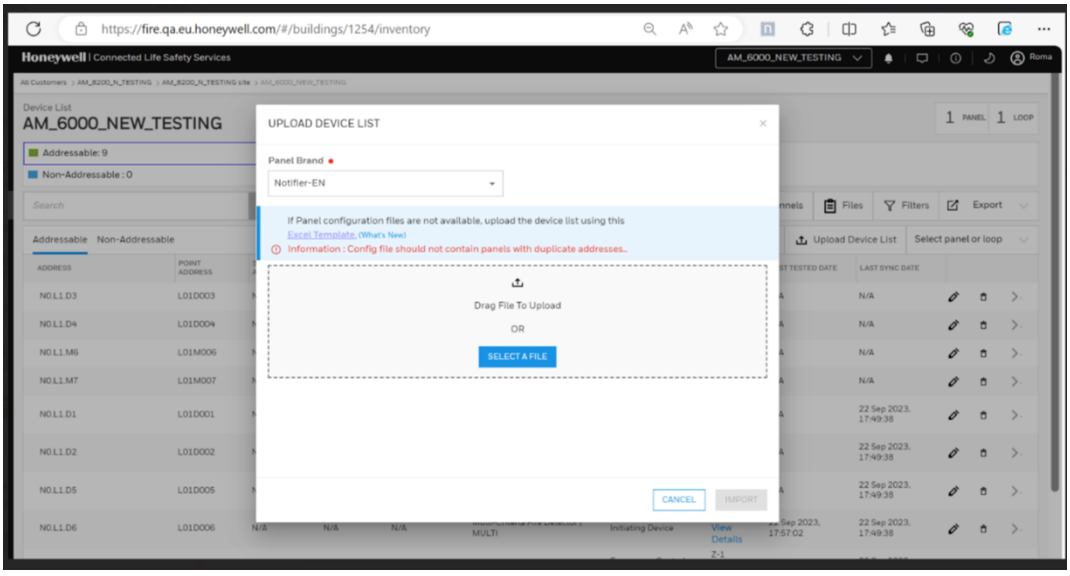


Figure C-77: Configuration File Upload to CLSS

C.15.5 PANEL FIRMWARE UPGRADE METHOD

- Connect the USB drive into panel which has the required panel firmware in it.
- Locate the dip switch in the panel and move the SWITCH 4 to upwards position

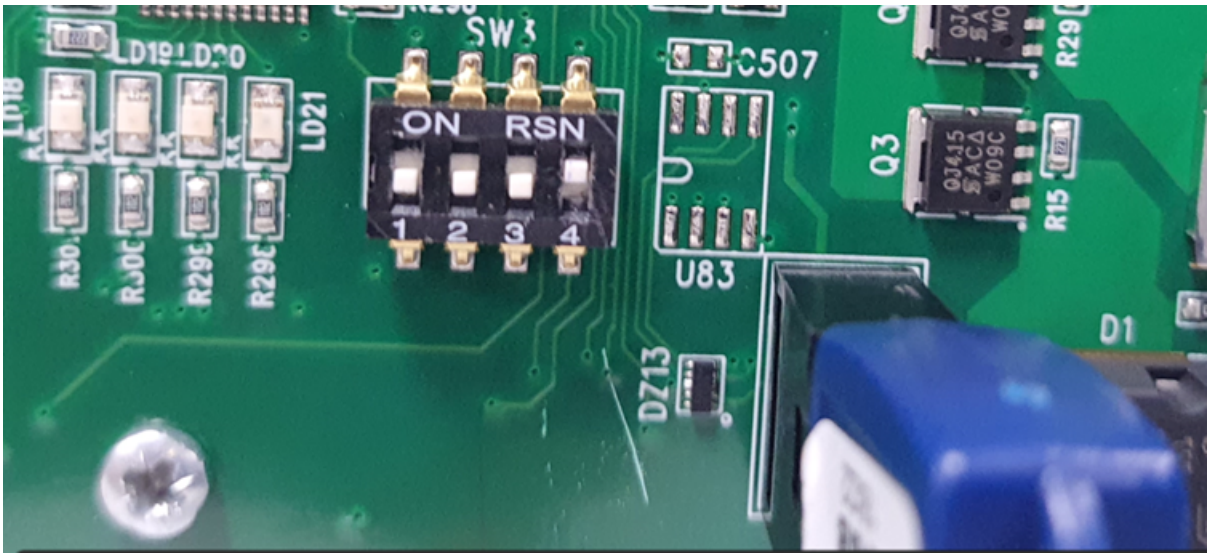


Figure C-78: Switch Position for Firmware Upgrade in AM CL Series Panel

Figure C-79: Switch Position for Firmware Upgrade in AM8200N/8100 Series Panel

• Choose firmware upgrade option from panel utility menu option.

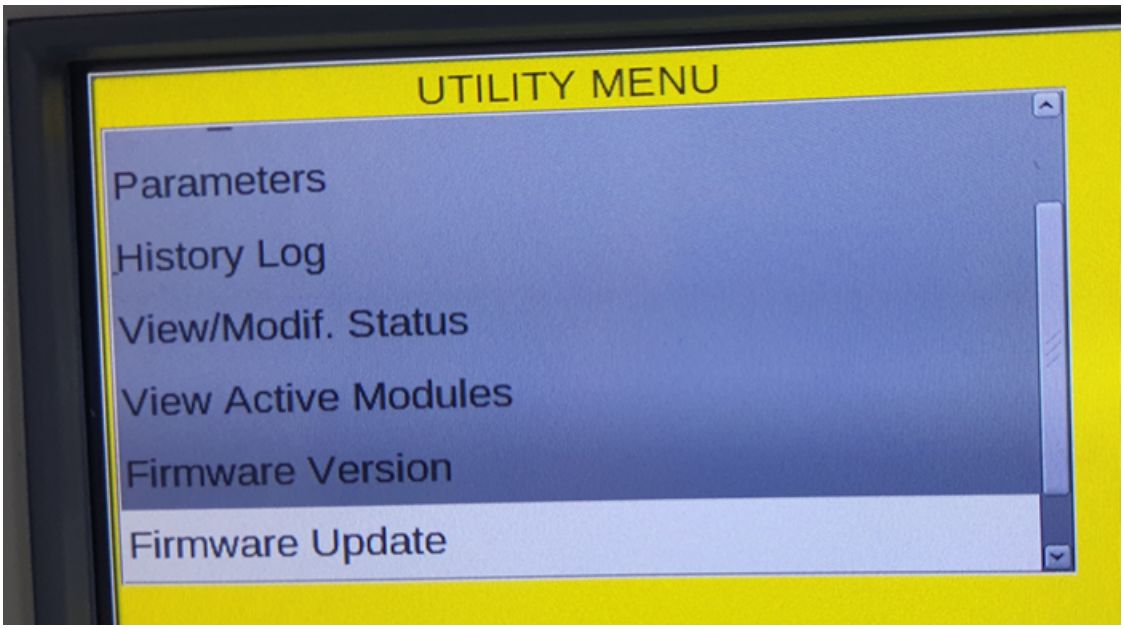


Figure C-80: Panel Firmware Upgrade Menu Option

C.16 TRIGA PANELS

C.16.1 CONNECTION OPTIONS

The gateway operates only with the Triga fire alarm control panels listed in the table below:

Table C.13 Triga Panel Connection Options

Fire Alarm Panel Models	RS-485	UART/TTL	RS-232	USB
TR-75R	Yes	No	No	No
TR-75B	Yes	No	No	No
TR-2100R	Yes	No	No	No
TR-2100B	Yes	No	No	No
TR-R2100R	Yes	No	No	No
TR-R2100B	Yes	No	No	No
TR-2100ECSR	Yes	No	No	No
TR-2100ECSB	Yes	No	No	No

CAUTION: When supporting the alarm transmission, it is recommended that the TRIGA panel should use secondary ANN bus channel with Class A wiring.
If the alarm transmission service is *not* used, the panel can USE either the primary or the secondary ANN bus channel for the CLSS Gateway connection.

C.16.2 MINIMUM REQUIRED VERSIONS

- For the Panel: 6.05.01
- For the CLSS Gateway: 3.1.4.74

C.16.3 TO USE AN RS-485 CONNECTION

Using an RS-485 cable the CLSS Gateway connects with the annunciator primary terminal of the panel.

CAUTION: Connect either the CLSS gateway or the ANN S/P G module with the panel. Both of them should not be connected together with the panel.

On the Gateway Side

At the RS-485 A port in the gateway board:

- Connect the A connector to the IN+ pin of the RS-485 A port.
- Connect the B connector to the IN- pin of the same RS-485 A port.

The RS-485 ports in the gateway board are labeled as 3 and 4 in the Figure C-2: Gateway Connection Options - Bottom Side .

On the Panel Side

At the S-BUS board in the ANN-BUS PRI terminal:

- Connect the RS-485 +ve wire to the A port.
- Connect the RS-485 -ve wire to the B port.

C.16.4 POWER CONNECTION

On the Gateway Side

In the power supply port (labeled 7 in the Figure C-2: Gateway Connection Options - Bottom Side):

- Connect the Red wire to the +24V pin.
- Connect the Black wire to the Gnd pin.

On the Panel Side

In the power board of the panel:

- Connect the Red wire to the +ve pin.
- Connect the Black wire to the -ve pin.

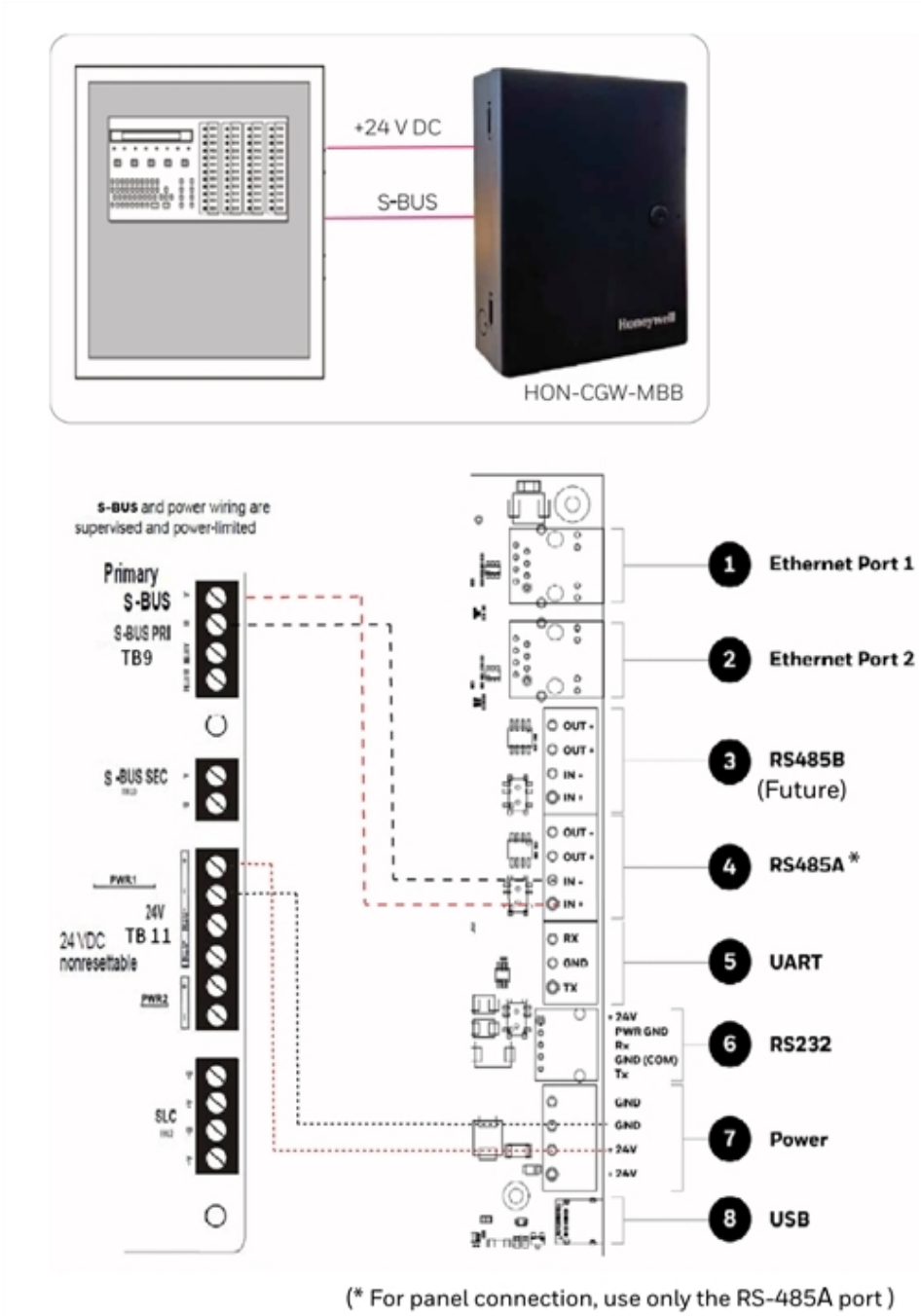


Figure C-81: Triga Panel: RS-485 Connections

C.16.5 PROGRAMMING FOR ANNUNCIATOR (ANN-PRI)

Programming enables the panel to recognize the CLSS gateway and the annunciator.

CAUTION: Before programming, ensure that the ANN-PRI communication cable is connected with the panel.

C.16.6 TO PROGRAM FOR ANNUNCIATOR

Using the keypad on the panel, you select options on the screens.

01. On the panel, press the **Enter** button on the keypad.
02. View the panel screen options.
03. On the keypad, press **7** to select 7 = PROGRAMMING MODE.
04. Enter the panel's password in the PROGRAMMING screen.
    The default password is: 00000000
05. Select the panel connected with the gateway, if it is a standalone panel.
    OR
    Navigate in the list of panels and select the panel connected with the gateway if it is a multi-panel network.
06. Select 1 = MODULE.
07. Select 2 = ADD MODULE.
08. Select the module of the gateway from the list.
09. Select the module type.
10. Select 1 = EDIT MODULE to enter the module details.
11. Provide the **Module ID** details.
12. Navigate to next menu.
13. Select Output Port = PARALLEL.
14. Select Event Logging = YES.
15. Navigate to next menu.
16. Select Baud Rate = 19200.
17. Keep the default values for other fields.
18. Review the entered details.
19. Save the changes.

C.17 VESDA® DETECTORS

C.17.1 CONNECTION OPTIONS

The gateway operates with VESDA detectors and sends alarm data to users.

C.17.2 MINIMUM REQUIRED VERSIONS

- For VESDA-E: All VESDA-E detector versions
- For the CLSS Gateway: 3.3.4.12

C.17.3 TO USE AN ETHERNET CONNECTION

Using an Ethernet cable the CLSS Gateway and the VESDA detectors are connected.

The CLSS Gateway can connect with a VESDA-E detector or a VESDA Detector Connector.

The CLSS Gateway uses a Host IP address, which is the subsequent next address of the VESDA-E detector's Host IP address. For example, if the VESDA detector IP address is 192.168.10.*69*, then the CLSS Gateway would automatically have the IP address 192.168.10.*70*. Therefore, do not assign the next host IP address to any other devices in the network.

C.17.3.1 Before Connecting

01. In the Configuration Computer:
    - Install the VSC Tool (with a valid license) on the Configuration Computer.
    - Connect the USB ports of the Configuration Computer and the detector with a Type B cable.
02. In the detector:
    - Using the VSC Tool, configure the respective parameters, including the authentication password.
    - Using the VSC Tool, create a connection profile for Ethernet.
    - If detector connector is used, ensure that the detectors are connected with the detector connector.
03. In the CLSS Gateway: Ensure that the gateway is connected with *CLSS Site Manager* via Ethernet or Wireless.

On the Gateway Side

- Connect the Ethernet cable to the Ethernet port 2 of the gateway.

Refer to Figure C-2: Gateway Connection Options - Bottom Side where it is labeled as the Ethernet Port 2. It is the J3 pin on the gateway board.

On the Detector Side

- Connect the Ethernet cable to the Ethernet port of the detector.

C.17.4 POWER CONNECTION

The gateway can receive the 24V DC power from an external power supply.

The detector's power supply to the gateway must be within +24V DC power.
Ensure that the battery backup capacity of a connected smoke detector is correctly calculated. power that the gateway also would consume should be considered in the calculation.

On the Gateway Side

- Connect the Red wire to the +ve pin of the power supply port.
- Connect the Black wire to the -ve pin of the power supply port.

C.17.4.1 External Power Supply

On the Gateway Side

- Connect to the power port of the gateway.
- Refer to Figure C-2: Gateway Connection Options - Bottom Side where the power port on the gateway is labeled as 7. It is the P2 pin on the gateway board.

On the External Power Supply Side

- Connect to the 24V DC external power supply.

APPENDIX D: COMPATIBLE CELLULAR MODULES

The cellular modules offer value-added services for mobile devices connected with the CLSS Gateway.

Figure D-1: A Cellular Module

To know about installing this device onto the gateway, refer to "Installing A Single SIM Cellular Module (CCM-ATT-HON, CCM-VZ-HON,CCM-EU)" on page 16.

D.1 OPERATION

The cellular modules are plug-and-play devices, which receive power from the CLSS Gateway and provide a cellular communication path.

D.2 SUPPORTED MODULES

Table D.1 Modules and Frequencies

Brand Name	Verizon Cellular Module	AT&T Cellular Module	EU - Cellular Module
Module Name	CCM-VZ-HON	CCM-ATT-HON	CCM-EU
Model	LE910-SV1	LE910B1-NA	LE910-EU1
Supported Regions	North America	North America	Europe
Frequency Details			
4G bands (MHz)	• B2 (1900) • B4 (AWS1700) • B13 (700)	• B2 (1900) • B4 (AWS1700) • B5 (850) • B12/B13 (700)	• B1 (2100) • B3 (1800) • B7 (2600) • B8 (900) • B20 (800)
3G bands (MHz)	-	• B2 (1900) • B5 (850)	-

Brand Name	Verizon Cellular Module	AT&T Cellular Module	EU - Cellular Module
Module Name	CCM-VZ-HON	CCM-ATT-HON	CCM-EU
Model	LE910-SV1	LE910B1-NA	LE910-EU1
2G bands (MHz)	-	-	• B3 (1800) • B8 (900)
Replaceable SIM Card	Yes	Yes	Yes

D.3 STANDARDS AND CODES

RED Directive 2014/ 53/ EU

- Health and Safety of the User
- Electromagnetic Compatibility
- Effective use of spectrum allocated

D.4 APPROVALS

Supported cellular module details are below:

Model: CCM-ATT-HON

Region: USA
Contains FCC ID: RI7LE910NAV2
Contains IC: 5131A-LE910NAV2

Model: CCM-VZ-HON

Region: USA
Contains FCC ID: RI7LE910SVV2
Contains IC: 5131A-LE910SVV2

Model: CCM-EU

Region: Europe
R&TTE/GCF

APPENDIX E: THIRD-PARTY COMMUNICATOR INTEGRATION

E.1 AES COMMUNICATOR INTEGRATION

The CLSS Gateway can send events to an AES® communicator (Model # 7707) to deliver the events to a central station. This integration enables AES communication without a PSTN dialer providing more rapid event delivery.

Events are reported to the Central Station using Contact ID* format.

*Refer: Document LS10378-351HW-E Honeywell Contact IDs for events and their descriptions.

The AES device is connected to CLSS Gateway using Eth0 (J3 connector) Interface. The communication data is encrypted using TLS 1.3 protocol.

Central station reports can be generated from CLSS Site Manager by uploading the configuration file to the CLSS Site Manager.

E.2 SYSTEM TOPOLOGY

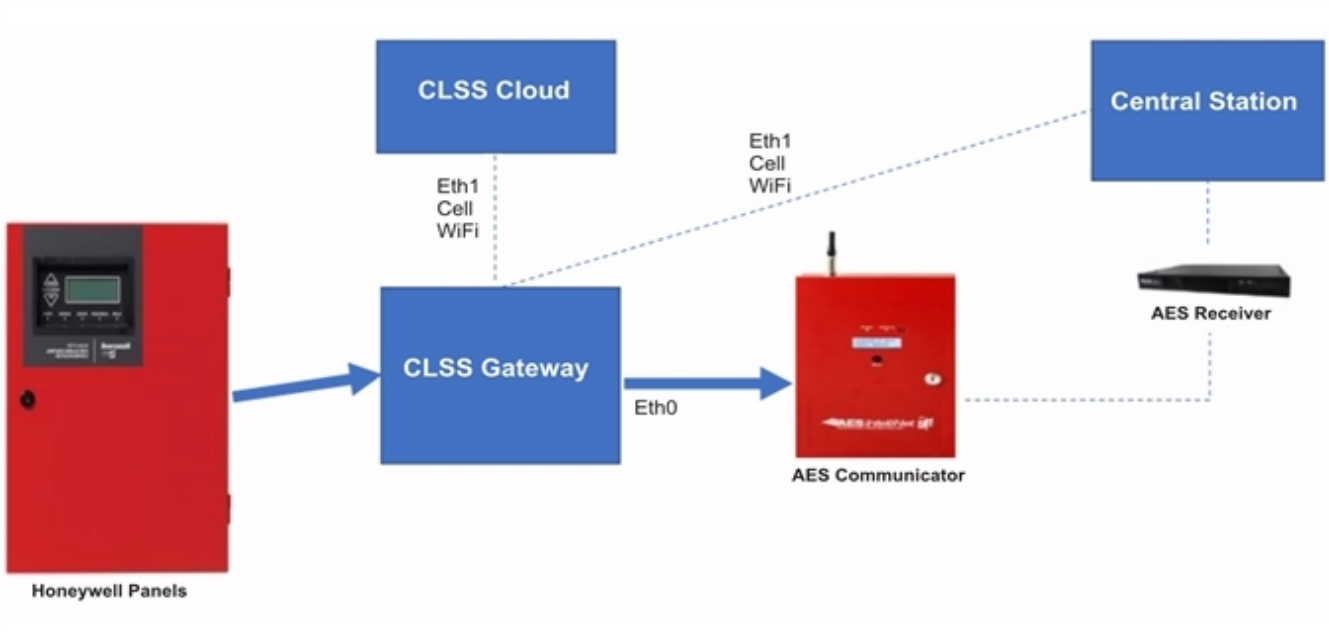


Figure E-1: System Topology - AES Communicator

E.3 CONNECTING TO THE AES COMMUNICATOR

Connect the AES communicator (Model # 7077) to the gateway as shown in Figure E-2: CLSS Gateway-AES Communicator Connections .

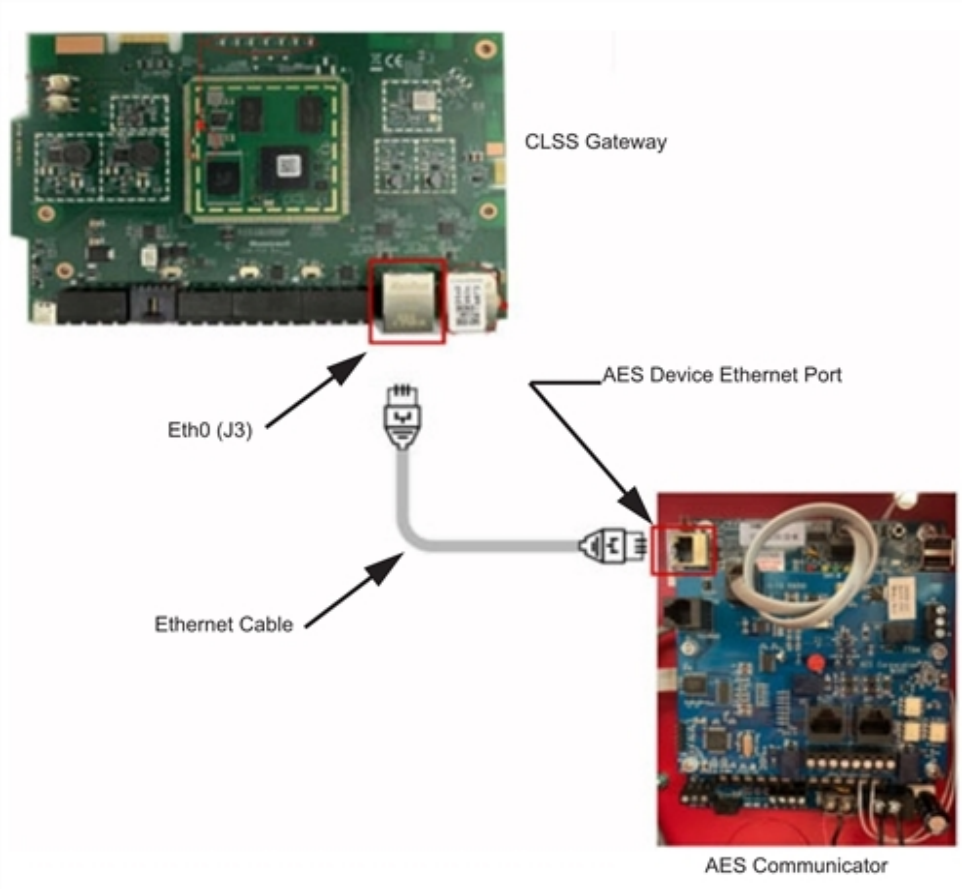


Figure E-2: CLSS Gateway-AES Communicator Connections

E.4 RECOMMENDED CYBERSECURITY PRACTICES

Cybersecurity risk. FAILURE TO COMPLY WITH THE RECOMMENDED SECURITY PRACTICES IS A CYBERSECURITY RISK TO YOUR SYSTEM.

It is recommended that the CLSS Gateway is directly connected to the AES communicator using an Ethernet cable, Do not use any Ethernet router or Ethernet switch for this connection.

E.5 CONFIGURATION AND ACTIVATION

AES device should be configured for CLSS using the AES IntelliNet® tool. Once configured, the user enables AES communication after completion of the fixed gateway installation flow using the CLSS Mobile app. Enable Gateway-to- AES communication as follows:

01. Navigate to the Activations screen and click on the card **Connected Gateway (Silver)** as shown in Figure E-3: AES Activation Card .
02. In the Activation Details screen (Figure E-4: AES Enable Card), click **ENABLE NOW**.
03. Follow the on-screen instructions to enable the AES communicator.

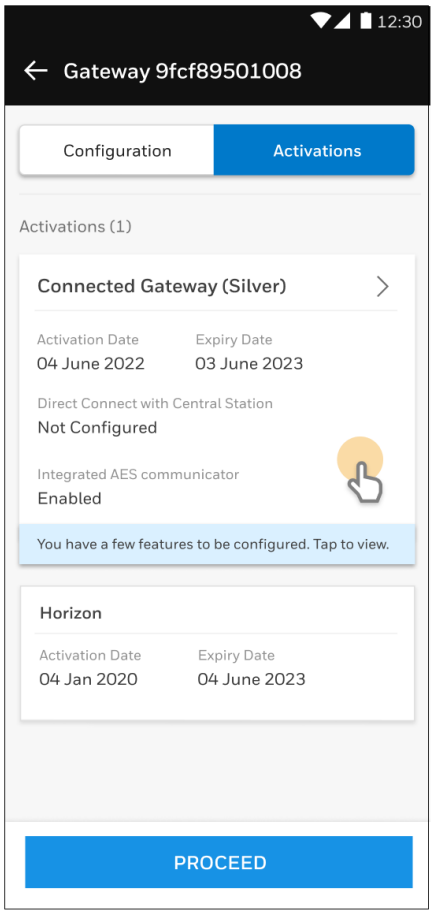


Figure E-3: AES Activation Card

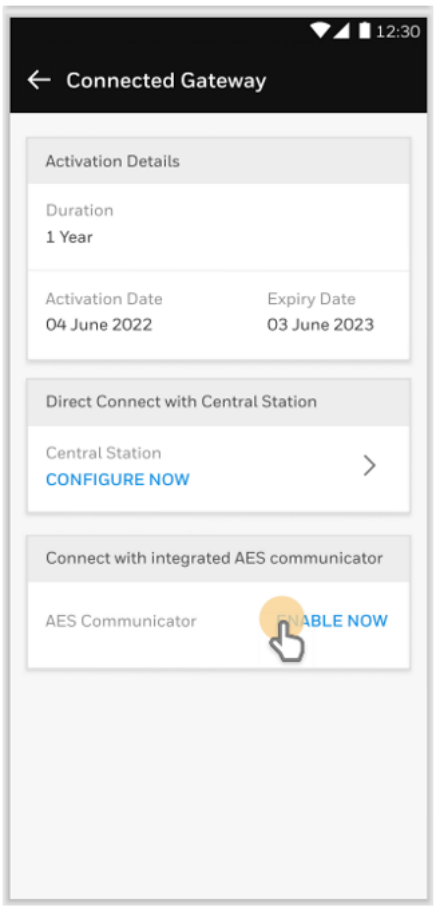


Figure E-4: AES Enable Card

E.6 GENERATING CENTRAL STATION REPORT USING SITE MANAGER

Generate central station reports from the CLSS Site Manager by uploading the configuration file to site manager as follows:

01. Log onto the CLSS Site Manager.
02. Click **All Customers** and select the customer name from the list (see Figure E-5: Site Manager - All Customers List).

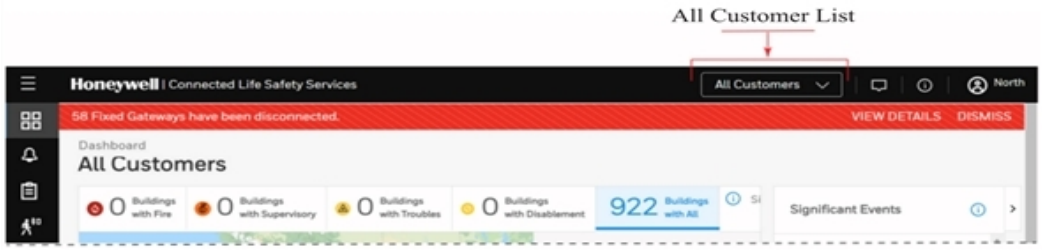


Figure E-5: Site Manager - All Customers List

03. Select the site and then select the building.
04. Click the feature activation icon at the left navigation bar (see Figure E-6: Feature Activation Icon Location).

Figure E-6: Feature Activation Icon Location

05. Navigate to the gateway and click **CONFIGURE NOW** (see Figure E-7: Configure Gateway).

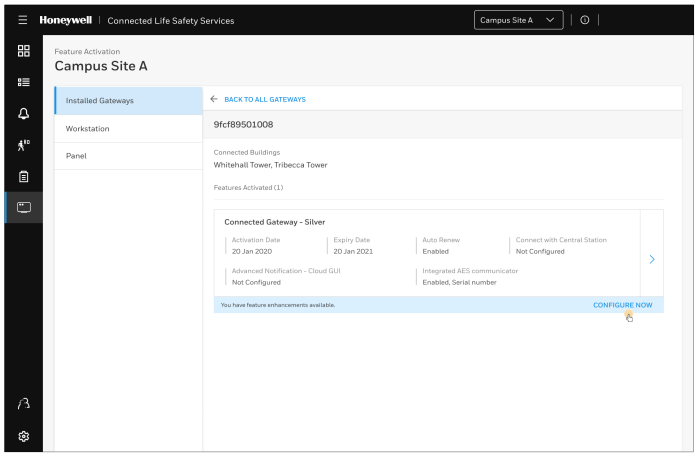


Figure E-7: Configure Gateway

06. Follow the on-screen instructions to download the central station report.

APPENDIX F: LAN-CONNECTED CLSS HORIZON

The *LAN-Connected CLSS Horizon* is a monitoring-only workstation, which allows multiple users to monitor their buildings, one or more networks, and life-safety systems.

LCH supports Control command also.

When connected with a *CLSS Gateway* using an Ethernet LAN, the *CLSS Horizon* receives events from the gateway's fire panels and shows them on a PC. Its display is GUI (Graphical User Interface).

The connection to the mobile device is wireless or cellular.

F.1 FUNCTIONALITY

The *LAN-Connected CLSS Horizon* translates the protocols and facilitates communications between a workstation and the connected FACPs, NFN network, or high-speed NFN network; to protocols used by the workstation.

F.2 CLSS HORIZON TOPOLOGY

01. Connect an Ethernet cable to the first Ethernet port (Eth1) of the gateway.
    The Ethernet port is labeled as 1 in "Connections to the LAN-Connected Horizon" on page 230.
02. Connect the other end of the Ethernet cable to the Computer running the *CLSS Horizon* application.

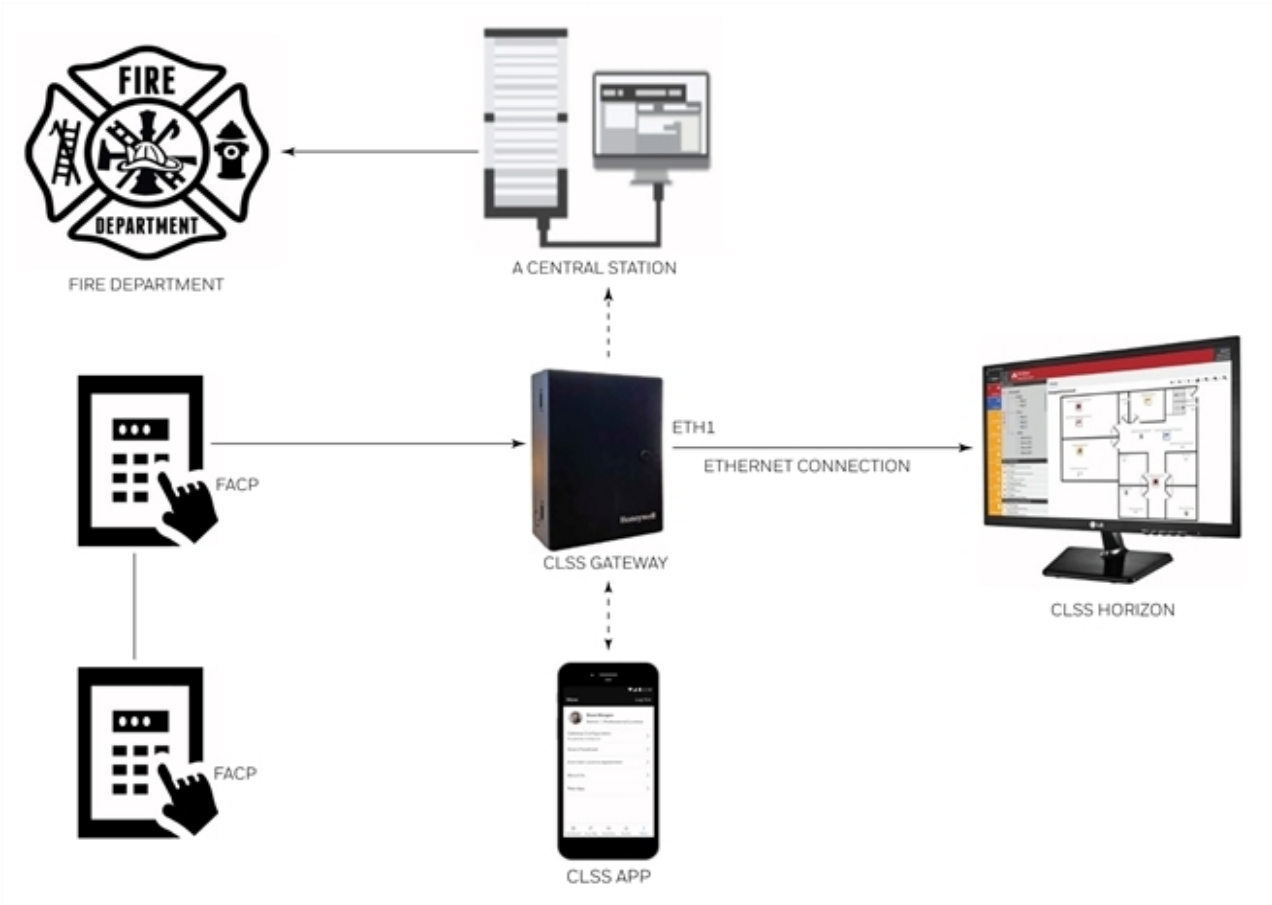


Figure F-1: LAN-Connected CLSS Horizon

F.3 IP REQUIREMENTS

F.3.1 IP PORT SETTINGS

The following IP ports must be available for the CLSS Gateway:

Table F.1
Required IP Ports

Port	Type	Direction	Purpose
53	UDP and TCP	Out	DNS Resolution
80	TCP	In	Web Based Configuration
123	UDP	Out	SNTP
443	TCP	In/Out	HTTPS Communications
2017	TCP	In	Connection from Workstation (Events and Commands)
4016	TCP	In	Upgrades
5100	TCP	5100	Voice Paging

F.3.2 IP RESTRICTIONS FOR THE GATEWAY

- Must have a static IP address
- Following are not supported:
    - DHCP
    - Web access through an HTTP proxy server
    - Use of a NAT (Network Address Translation)

F.4 COMPATIBLE EQUIPMENT

The CLSS Gateway is compatible with the following equipment:

Table F.2 Compatible Equipment List

Type	Equipment
Fire Panels	• N16 (INSPIRE) • NFS-320 • NFS2-640 • NFS2-3030
Network Cards	• NCM-F • NCM-W • HS-NCM-MF • HS-NCM-MFSF • HS-NCM-SF • HS-NCM-W-2 • HS-NCM-WMF-2 • HS-NCM-WSF-2
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-2

Type	Equipment
Other Products	Unmonitored but network compatible. • Legacy Gateway • DVC • NCA-2 • NCD • NFN-GW-EM-3 • NFN-GW-PC-F • NFN-GW-PC-HNMF • NFN-GW-PC-HNSF • NFN-GW-PC-HNW • NFN-GW-PC-HNW-2 • NFN-GW-PC-W • NWS-3 • PC NFN Gateways • VESDA-HLI-GW

F.5 CONNECTING THE LAN-CONNECTED HORIZON

01. At the CLSS Gateway side, connect an Ethernet cable to Ethernet Port 1.
02. At the LAN-Connected Horizon side, connect the other end of the Ethernet cable to the Ethernet port.

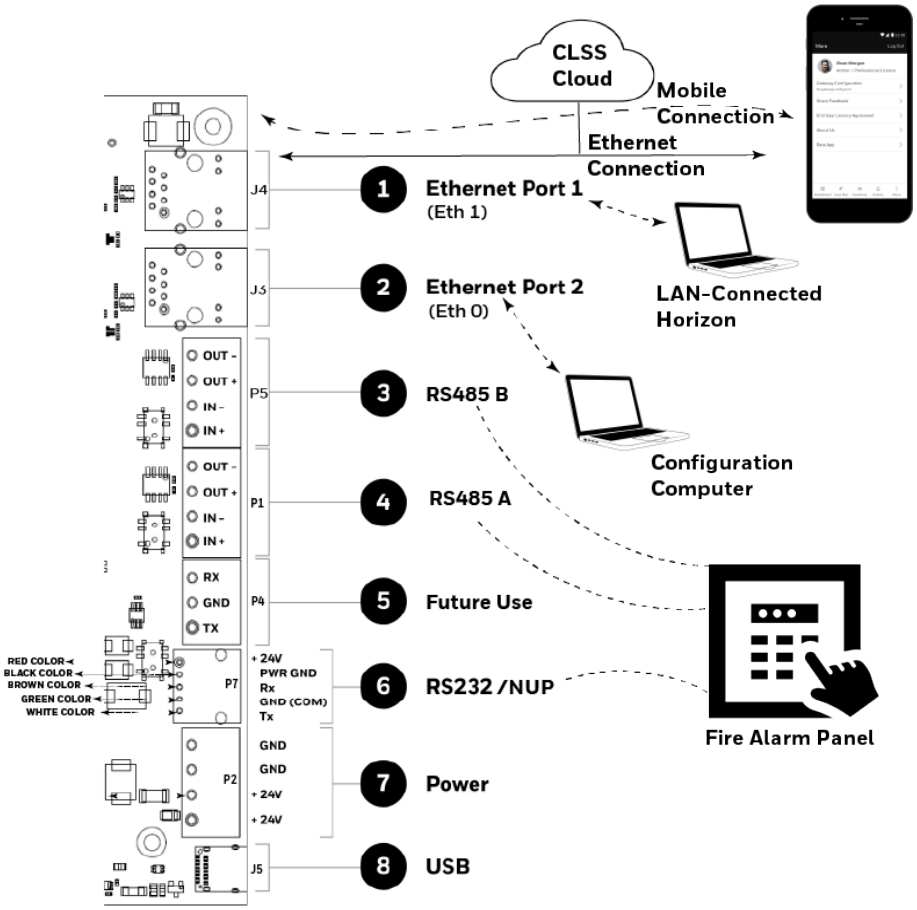


Figure F-2: Connections to the LAN-Connected Horizon

F.6 CONFIGURATION SETTINGS

You can configure the Ethernet settings either using the *CLSS* App or the *CLSS Gateway Configuration Tool*.

F.6.1 TO CONFIGURE USING THE CLSS APP

You install a fixed gateway when the gateway is not connected to the Internet.

01. Log into the *CLSS* App.
02. Tap the three dots at the top right on the dashboard.
03. Tap **Install Fixed Gateway**.
04. Select the Customer and then the Building.
05. Wait for the App to discover the gateway.
06. Pair with the discovered gateway.
07. Go to the **Configuration** tab.
08. Tap **CONFIGURE** at the *Ethernet (ETH1)*.
09. Provide the static IP address and other details in the **SETTINGS** page.
10. Tap **APPLY** and then tap **CONTINUE**.
11. Read the confirmation message and tap **YES, CONTINUE**.
12. Tap **NEXT**.
13. Wait for the panel connection success message.
14. Tap **+ADD ACTIVATION** in the **Activations** tab.
15. Find and select **LAN Connected Horizon** and **LAN Connected Horizon Panel Support**.
16. Read the informational message and tap **OKAY, GOT IT**.
17. Tap **ACTIVATE**.
18. Read the activation confirmation details and tap **CONFIRM**.
19. Wait for the activation success message.

F.6.2 TO CONFIGURE USING THE CONFIGURATION TOOL

The laptop or computer connected to the gateway for configuring is known as the *Configuration Computer*. It is recommended to connect the *Configuration Computer* always directly to the gateway board.

This configuration method is required only in the following cases:

- To time sync the fire panels with the LAN-Connected Horizon workstation
- To generate a secure gateway certificate for gateways manufactured on or before May 2021

01. Connect an Ethernet cable to the second Ethernet port (Eth0) of the gateway.
    The port is labeled as 2 in Figure F-2: Connections to the LAN-Connected Horizon .
02. Connect the other end of the Ethernet cable to the configuration computer's Ethernet port.
03. Ensure that your configuration computer's IP is in the range of 192.168.10.xxx
    a. In windows Search bar, type "Control panel" and click on the control panel Application
    b. In Network and internet select **View network status and tasks**.
    c. Click on **Change adapter settings** will get the below screen.
    d. Right click on the ethernet and click **Properties**.
    e. Select 'Internet Protocol Version 4' and click on **Properties**.

f. Select the **Use the following ip address** and enter:
IP Address: 192.168.10.100
Subnet mask: 255.255.255.0
Default gateway: 192.168.10.1

g. Click “OK”.

04. On the gateway board, find the S6 button.
To find the S6 button, refer to Figure 2-1: Printed Circuit Board: Layout .

05. Press the S6 button until the LED indicator DL3 turns ON, indicating enabled configuration mode.

06. Open the Chrome browser and enter the following IP address of the configuration tool:
https://192.168.10.190:9443/config/index.html
As the gateway comes with a self-signed certificate, the Chrome browser may warn that the connection is not private. You can proceed with the connection and configure the gateway.

07. If the Chrome browser warns about the connection, click **Advanced** and then click **Proceed to 192.168.10.190 (unsafe)**.

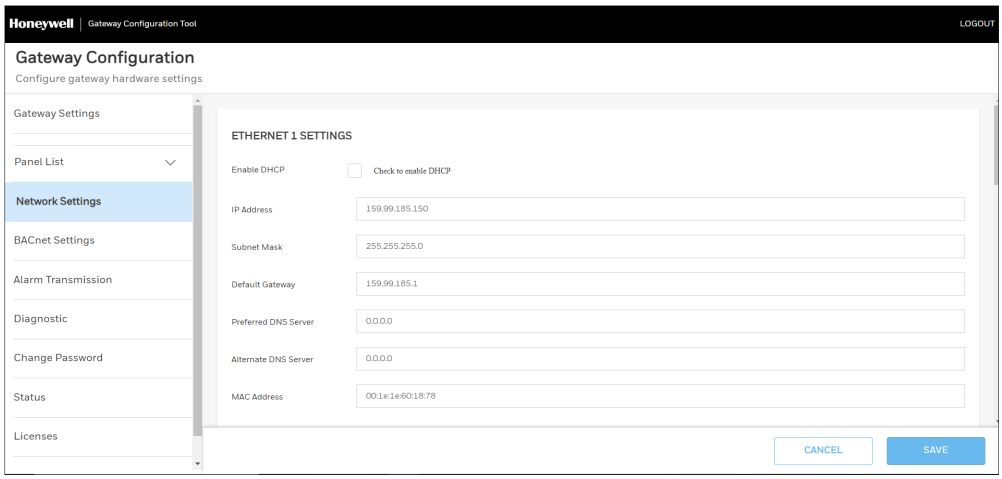
08. In the login page, enter the given password.
The default password is: *Welcome123*

09. Click **SIGN IN**.

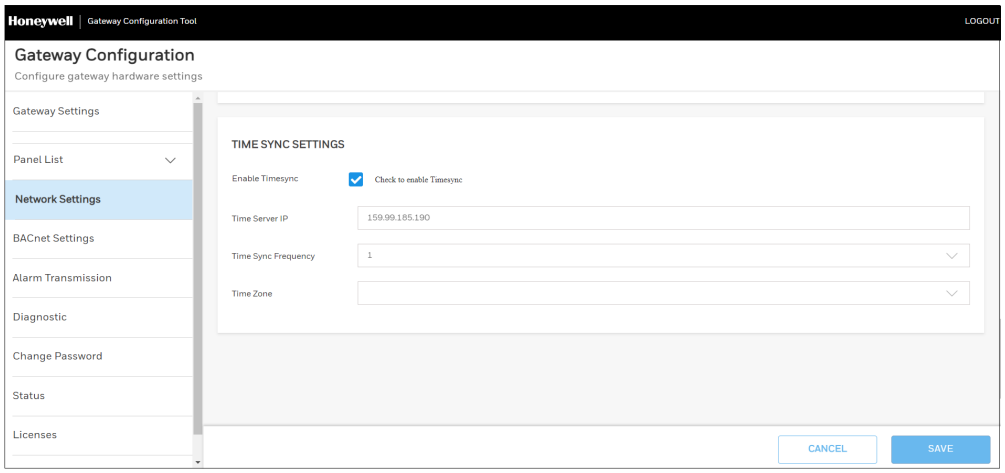
10. On the first login, the gateway mandates a password change. Change the password.

11. In the **Gateway Settings** section, enter the gateway-related values, and then click **SAVE**.

12. Scroll down to **Network Settings**, and in the **ETHERNET 1 SETTINGS** section, provide the static IP address details and then click **SAVE**.



13. Scroll down to **Network Settings**, and in the **TIME SYNC SETTINGS** section, click on the **Enable Timesync** checkbox, provide the Time Server details, and then click **SAVE**.

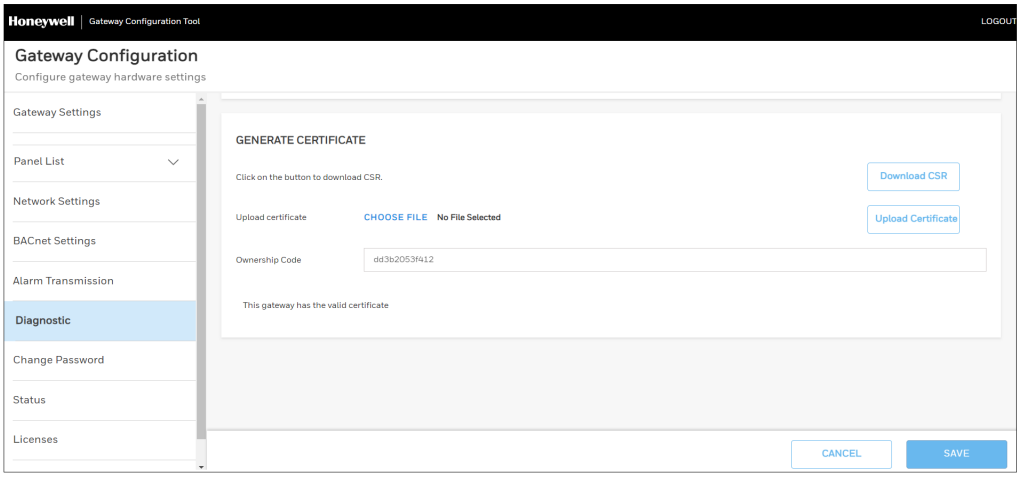


14. Scroll down, and in the **WLAN SETTINGS** dialog, specify the wireless settings values, and then click **SAVE**.

F.6.3 TO PROVIDE SERVER CAPABILITY TO THE GATEWAY

A *CLSS Gateway* released on May 2021 or earlier acts as a client to the panels, Cloud, and other networked systems. You can make it a master to other systems in the network with a server certificate.

01. Log in to *CLSS Gateway Configuration Tool* using the steps 1 to 9 in the F.6.2 To Configure Using the Configuration Tool section.
02. Click **Diagnostic** in the **Gateway Settings** section.



03. Click **Download CSR**.
04. Log on to *CLSS Site Manager*.
05. Go to **Settings** and click **Horizon Certificate Management**.
06. Click **UPLOAD CSR** and select the certificate downloaded.
07. Click **GENERATE**.
08. Wait for the certificate generation success message.

F.7 TO CONFIGURE THE GATEWAY IN CLSS HORIZON

01. Log into the *CLSS Horizon* application.
02. Go to **System** and then **Networks** on the menu bar.
03. Provide the *CLSS Gateway* details and click **OK**.

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.

12 Clintonville Rd
Northford, CT 06472
(203) 484-7161

140 Waterside Rd
Leicester LE5 1TN, UK
+44 (0) 203 4091779

Honeywell