Honeywell

# MAXPRO Intrusion Series

## Integrated Security Systems

800-23044-1 Rev. B8
March 2024

# Installation and Setup Guide

# Disclaimer

Honeywell International Inc. (“HII”) reserves the right to make changes in specifications and other information contained in this document without prior notice, and the reader should in all cases consult HII to determine whether any such changes have been made. The information in this publication does not represent a commitment on the part of HII.

HII shall not be liable for technical or editorial errors or omissions contained herein; nor for incidental or consequential damages resulting from the furnishing, performance, or use of this material. HII disclaims all responsibility for the selection and use of software and/or hardware to achieve intended results.



Web Address: www.honeywellaidc.com



For patent information, refer to www.hsmpats.com.

# TABLE OF CONTENTS

# Copyright Notice



# Document Conventions

The following typographic conventions are used in this document:

| Convention | Description |
|---|---|
| Bold | Used to denote emphasis. Used for names of menus, menu options, toolbar buttons |
| Italic | Used to denote references to other parts of this document or other documents. Used for the result of an action. |

The following icons are used in this document:

| Icon | Description |
|---|---|
| | Note. This icon indicates information of special interest that will help the reader make full use of the product, optimize performance, etc. Failure to read the note will not result in physical harm to the reader, or damage to equipment or data. |
| | Caution! This icon indicates danger to equipment. The danger can be loss of data, physical damage to the equipment, or permanent corruption of configuration details. |
| | Warning! This icon indicates danger of physical harm to the reader. Not following instructions may lead to death or permanent injury. |
| | Warning! This icon indicates danger of electric shock. This may lead to death or permanent injury. |
| EN | Indicates information for EN compliant installations. |

# Environmental Information

This symbol on our product shows a crossed-out "wheelie-bin" as required by law regarding the Waste of Electrical and Electronic Equipment (WEEE) disposal. This indicates your responsibility to contribute in saving the environment by proper disposal of this Waste

i.e. Do not dispose of this product with your other wastes. To know the right disposal mechanism please check the applicable law.

CHAPTER

# 1 ABOUT THIS DOCUMENT

## 1.1 Scope

This document provides full instructions for installing the hardware and for initial programming of a MAXPRO Intrusion Control Panel and its associated peripherals.

You can find the full programming information in the help file within the MAXPRO Cloud configuration tool, and in the MAXPRO Cloud Configuration Guide (doc. no. 800-24096-1).

This Installation and Setup Guide covers the following topics:

- The installation of the MAXPRO Intrusion (MPI) hardware:
  - Cabinet for Control Panel or Remote Power Supply
  - MPI Control Panel
  - MPI peripherals: Keypads, Remote Power Supply, Door Control Module, Relay Module, and Zone Expander
  - LTE module
  - V-Plex devices.
- Summary information for configuration in MAXPRO Cloud
- Testing and commissioning, hand-over to the customer
- Technical specifications of all MPI hardware
- Agency information

| | |
|---|---|
|  | **Caution: For instructions on maintaining compliance with the EN 50131 I&HAS standards, see *Instructions for Compliance*, page 182 .** |

This Installation and Setup Guide does not cover:

- Full configuration instructions for MAXPRO Cloud. For details, see the *MAXPRO Cloud Configuration Guide* (doc. no. 800-24096-1).
- Cybersecurity of the MAXPRO Intrusion installation. For details, see th *MAXPRO Intrusion Security Manual* (doc. no. 800-25507).
- The daily usage of the MAXPRO Intrusion system. For details, see the *MAXPRO Intrusion User Guide* (doc. no. 800-23041-1).

## 1.2 Audience

This Installation and Setup Guide is primarily intended for installers of the MAXPRO Intrusion systems.

## 1.3 More Info

You can find the latest versions of this document and any referenced document on the Honeywell support site www.mywebtech.com, or on the MAXPRO Intrusion Support pages.

Need a quick link to information for your device? Scan the QR code on the info card of the device, and it will take you to the appropriate page with Installation Guides and other information:

CHAPTER

# 2 INTRODUCTION

## 2.1 The MAXPRO Intrusion Solution

The MAXPRO® Intrusion (MPI) Series Control Panels provide integrated intrusion and access control functionality for applications ranging from small, standalone sites to large multi-site projects. The system is configured through MAXPRO® Cloud and can be managed by the end customer using the MAXPRO Cloud web and mobile apps, depending on the user's authority level within the control panel.

You need to set up a dealer account within MAXPRO Cloud before installing a MAXPRO Intrusion system. See www.maxprocloud.com for more details.

This document covers the following control panel models:

- MPIP2000 Series: MPIP2000E and MPIP2100E control panels
- MPIP3000 Series: MPIP3000E and MPIP3100E control panels.

## 2.2 System Features

| | |
|---|---|
|  | **Note:** *All references in this manual for number of inputs, outputs, areas, etc., use the MPIP3100x2 Control Panel features. The table further below lists the differences between the various control panels.* |

### 2.2.1 Overview and Panel Model Comparison

The MAXPRO Intrusion Series Control Panels provide the following features:

- Touch screen keypad control with either PIN or card user login
- Selectable zone supervision styles and EOL resistor values
- Access control with integrated operation of false alarm prevention
- Hardwired zone expansion with V-Plex sensors and IB2 bus modules
- Supervision of all bus-connected devices, auxiliary outputs, alarm sounders, and communicators
- Programmable relays and trigger outputs
- Schedule and event based automated operation including auto- arming/disarming
- MPIP3100E model will be available soon
- MPIP3100x model available soon.
- Flexible Permission Groups for multi-site intrusion and access applications

- Flexible multi-site system management
- Web and mobile applications available
- Integrates with MAXPRO Cloud video devices
- On-board IP for connection to MAXPRO Cloud, central station reporting, and third party integration.
- Optional digital cellular communicator (4G/LTE). Can be used for single or dual path reporting.
- Remote diagnostics for faster trouble resolution. The table below compares all current MPI Control Panel models.

***Table 1 : Control Panel Model Comparison***

| Feature | MPIP2000E | MPIP2100E | MPIP3000E | MPIP3100E[1] |
|---|---|---|---|---|
| Inputs (Zones) | | | | |
| Max. inputs | 60 | 150 | 300 | 600 |
| On-board inputs (total)[2] | 10 | 10 | 10 | 10 |
| On-board inputs suited for 2- wire smoke | 2 | 2 | 2 | 2 |
| Outputs | | | | |
| Max. outputs | 60 | 100 | 200 | 300 |
| On-board trigger outputs | 4 | 4 | 4 | 4 |
| On-board relay outputs | 1 | 1 | 2 | 2 |
| Auxiliary power outputs (12 VDC) | 1 | 1 | 2 | 2 |
| Monitored siren output | No | No | No | No |
| Siren power output (12 VDC) | 1 | 1 | 1 | 1 |
| Loudspeaker driver for internal siren | 1 | 1 | 1 | 1 |
| Areas and Doors | | | | |
| Areas | 10 | 30 | 60 | 120 |
| Doors | 10 | 30 | 60 | 60 |

MPIP3100E model will be available soon.

The total number of on-board inputs includes the normal inputs and the inputs that are suitable for 2-wire smoke devices. The inputs that are suitable for 2-wire smoke devices can also be used as normal inputs.

| Feature | MPIP2000E | MPIP2100E | MPIP3000E | MPIP3100E[1] |
|---|---|---|---|---|
| Users | | | | |
| Users | 500 | 2,000 | 5,000 | 10,000 |
| Permission Groups | 30 | 50 | 100 | 300 |

| | | | | |
|---|---|---|---|---|
| Events Log[2] | | | | |
| Intrusion | 1,500 | 1,500 | 1,500 | 1,500 |
| Access | 6,000 | 10,000 | 10,000 | 10,000 |
| Programming | | | | |
| Schedules | 30 | 50 | 100 | 200 |
| Holidays (per year) | 255 | 255 | 255 | 255 |
| Controller rules | 30 | 50 | 100 | 200 |
| Bus Network | | | | |
| On-board IB2 data bus lines | 1 | 1 | 2 | 2 |
| On-board V-Plex sensor bus lines | 1 | 1 | 2 | 2 |
| Power Supply | | | | |
| Max. constant current | 3.0 A | 3.0 A | 3.0 A | 3.0 A |
| Battery charging capacity[3] | 36 Ah | 36 Ah | 36 Ah | 36 Ah |
| Communication Paths | | | | |
| IP/Ethernet | 1 on board | 1 on board | 1 on board | 1 on board |
| Radio communication (4G/ LTE) | Optional | Optional | Optional | Optional |
| Central Station Signaling Protocols | | | | |
| Contact ID | Yes, via Maxpro receiver software package or other receiver compatible with Honeywell ISOM protocol | | | |
| SIA DC-03 | Yes, via Maxpro receiver software package or other receiver compatible with Honeywell ISOM protocol | | | |
| SIA DC-03 | Yes, Maxpro receiver software package or native SIA DC-09 IP protocol implementation in Control Panel with SIA DC-03 message Format. | | | |

MPIP3100E model will be available soon

The system stores the events log in the control panel memory. You cannot delete the events log. In order to preserve mandatory events as required by the standards, the system copies the required events into separate tables. You can view the content of these tables using the Export Log feature in MAXPRO Cloud. For mandatory intrusion and hold-up events, export the burglary event log. For communication events, export the SPT log. The system retains a minimum of 1500 events for intrusion and hold-up events, and a minimum of 1000 events for communication events. Due to buffering there will often be more events in the exported file.

With the MPI medium-sized cabinet (MPIBXM35), you can use a battery capacity of up to 18 Ah. If you need more battery capacity, you need to install a second tamper-protected cabinet with the second battery.

## 2.2.2 Inputs and Output

- Provides 10 on-board hardwire zones.

- Supports up to 16 two-wire smoke detectors on zones 9 and 10 (32 in total).
- Four-wire smoke detector reset through use of on-board relay.
- Low-voltage trigger outputs.
- Outputs can be programmed to activate in response to system events (alarm condition), or at a specific time of day, or manually.
- Battery sensing hardware that monitors two batteries independently and can sense when either battery voltage is too low. Prevents deep discharge from occurring.
- System expansion is available via V-Plex and IB2 bus:
- Zone expansion is possible via V-Plex sensors or zone expanders connected to the IB2 bus.
- Output expansion is possible via V-Plex devices or relay modules connected to the IB2 bus.

### 2.2.3 IB2 Bus for Expansion Modules

The Intellibus 2 (IB2) bus is the main 4-wire communication bus on which keypads, relay modules, zone expanders, and other peripheral devices are connected to the system. IB2 characteristics include:

- Guaranteed performance of up to 46 IB2 bus devices per bus.
- Provides free wiring topology (chain, star, or spur configuration).
- Does not require end-of-line resistors.
- Unique device IDs embedded within each device for easy enrolling on the system.

Each IB2 bus device is individually supervised.

Easy device swapping feature from MAXPRO Cloud. For an overview of compatible IB2 devices, see *Parts List*, page 191.

### 2.2.4 V-Plex Bus for Individual I/O

V-Plex is a two-wire addressable multiplex loop that allows V-Plex sensors to be connected and individually supervised by the system. In addition, some V-Plex sensors have the ability to send special signals to the control panel for special conditions, such as masking of the PIR. Characteristics of the V-Plex bus include:

Provides 128 mA current on each loop.

Supports a maximum of 128 devices in each V-Plex data bus provided cumulative current consumption of all devices in the data bus is less than 128mA.

For V-Plex smart PIRs, you can enable the Smart Contact functions. This allows the PIR to detect a mask condition in the disarmed state.

For an overview of compatible V-Plex devices, see *Parts List*, page 191.

### 2.2.5 Alarm Notification and Communication to the Central Monitoring Station

For alarm notification, the MPI control panels provide:

- Connections for sounders. For details, see *Wiring Alarm Sounders*, page 46.

An Alarm Transmission System (ATS) using the on-board Ethernet connection or the optional digital cellular radio (4G/LTE module). For a list of events that the system can transmit, see Events, page 149.

**EN** The system supports notification options A, B, C, D, and E for Grade 3, D and Grade 2 F for as listed in EN 50131-1, table 10. For the EN 50136 ATS ratings for Ethernet and/or cellular radio, see the specifications table in MPI Control Panel, page 161.

The communication method is pass-through (*Ref. EN 50136-2 Section 6.1.3*).

The system can communicate with the central monitoring station (CMS) via the MAXPRO Receiver software package, or via other receivers compatible with Honeywell ISOM protocol, or via native SIA DC-09 IP protocol in control panel with the SIA DC-03 message format.

### 2.2.6 Configuration

MAXPRO Cloud for system configuration and management. The system is designed to connect automatically to MAXPRO Cloud on start-up. The system requires an INTERNET connection via the Ethernet network or via the 4G/LTE module.

### 2.2.7 Areas (Partitioning)

- Provides control of up to 120 separate areas independently, each functioning as if it had its own separate control.
- You configure each keypad with a home area, but you can configure it to annunciate alarms from neighboring areas as well.
- Provides an ATM area that needs two levels of authorization:

First, the master user needs to initiate the ATM disarm period (Access window).

Then, only the ATM user can disarm the ATM area within the disarm period.

It is the responsibility of the ATM User to arm the ATM area before leaving the premise. When the ATM user disarms an ATM area, ATM re- arm period (configurable up to 90 minutes) is initiated. If the ATM user does not re-arm the ATM area before leaving the premise, the ATM area will be automatically re-armed once the configured re-arm time period expires. For the last 5 minutes of ATM re-arm time period, there will be an indicating sound in the AMS. The cadence of this sound will increase as time nears closer to expiring.

| | |
|---|---|
|  | **Notes:** The ATM Disarm Initiate can be done by a Master User through AMS/ MPC. The ATM area can be disarmed by the ATM user only through AMS.<br>In case of an alarm, a Master User can disarm an ATM area, clear the alarm and re-arm an ATM area. After a Master has disarmed an ATM area, an installer will be able to clear troubles in the ATM areas and re-arm the ATM area. An installer can't disarm an ATM area and can't Initiate Disarm Period. In case of Alarms/Troubles in an ATM area, ATM users won't be able to disarm an ATM area.<br>It is not recommended that you configure an ATM area as the home area of the AMS. An ATM area has to be an associated area of the AMS. An ATM area can't be associated to Common Lobby (for future).<br>In the ATM area, only the addition of a Seismic Zone Type is allowed. |

### 2.2.8 Access Control

- Supports up to 60 doors.
- Supports up to 10,000 access cards.
- Provides up to 300 access/intrusion permission groups.
- Automatic blocking of access if the area behind the door is armed.
- Allows disarm-and-access at the door reader for users with disarming rights.
- Stores access control events in the event log.

### 2.2.9 Scheduling

- Can automate system functions, such as access control periods, arming, disarming, and activation of outputs (e.g., lights).
- Provides up to 200 schedules.

### 2.2.10 Event Log

The event log is available on the keypad and in MAXPRO Cloud. For an overview of the events, see Events, page 149.

The system stores the events log in the control panel memory. You cannot delete the events log.

In order to preserve mandatory events as required by the standards, the system copies the required events into separate tables. You can view the content of these tables using the Export Log feature in MAXPRO Cloud. This feature is available from the control panel's **Overview** page:

- For mandatory intrusion and hold-up events, export BURG EVENT LOG.
- For communication events, export SPT LOG.
- For diagnostics events, export DIAGNOSTIC LOG.

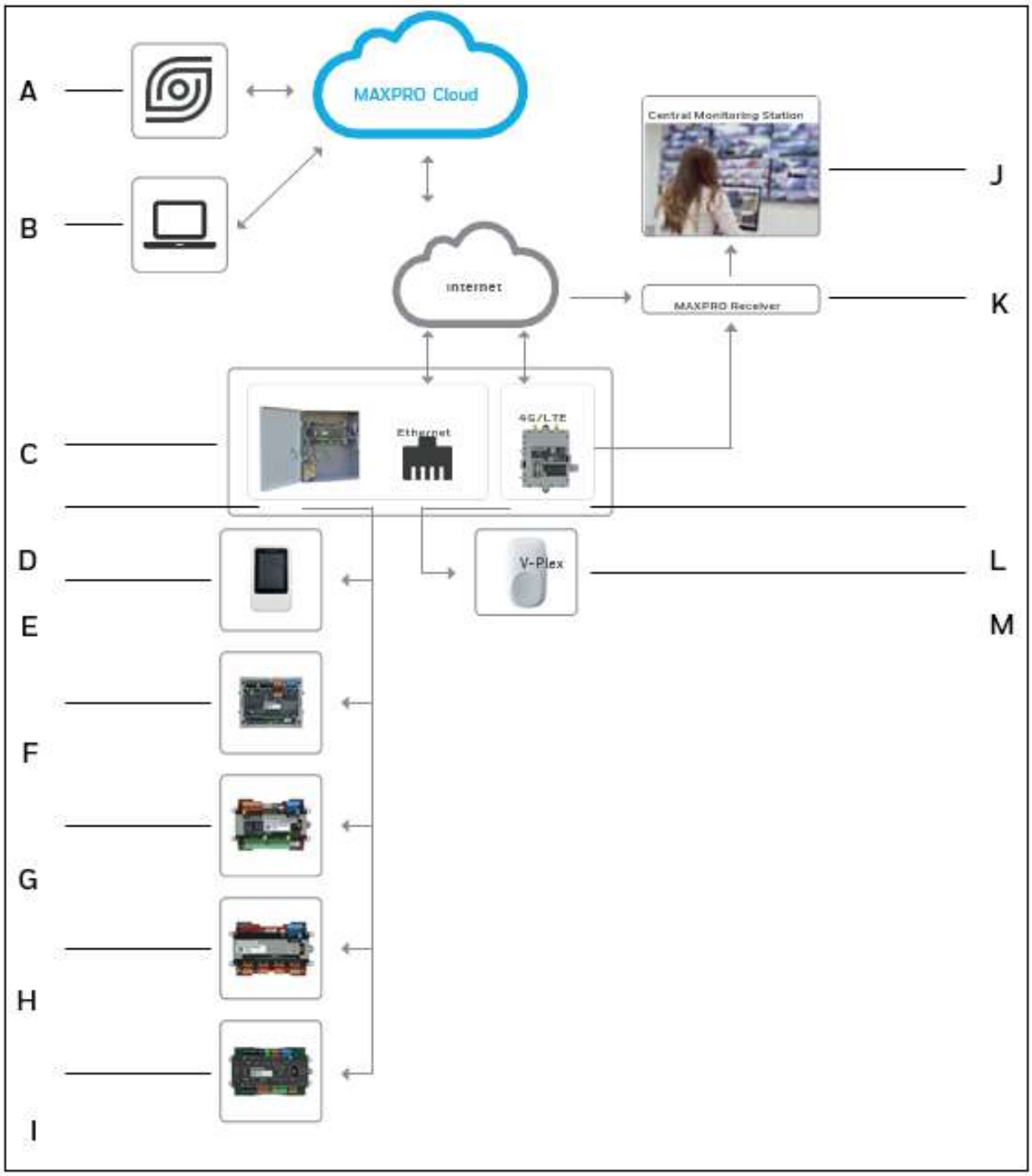
The system retains up to 5000 events for intrusion and hold-up events, up to 1000 events for communication events, and up to 1000 events for diagnostic log. Due to buffering there will often be more events in the exported file.

### 2.2.11 Indications

MAXPRO Intrusion provides indications such as messages, beeps and other sounds on the keypad and sounders. The system displays or annunciates the indication as the initiating event occurs.

1. The actual number is also limited by the number of devices that can be connected to the IB2 bus. An installer can choose any mix of devices. The system guarantees performance of up to 46 devices per bus.

## 2.3 General Architecture




| | |
|---|---|
| A | MAXPRO Cloud mobile app |

| | |
|---|---|
| B | MAXPRO Cloud web app |
| C | MAXPRO Intrusion Control Panel in cabinet with built-in Ethernet and optional 4G/LTE module.<br><br>IB2 modules can be stacked in the cabinet for saving space and quick connectivity. For details, see *About the Cabinet*, page 24. |
| D | IB2 bus with IB2 devices.<br><br>The system guarantees performance of up to 46 IB2 devices per IB2 bus. The MPIP3000 series supports two IB2 buses. |

| | |
|---|---|
| E | MAXPRO Intrusion keypad |
| F | MAXPRO Intrusion Remote Power Supply. The Remote Power Supply needs to be installed in a cabinet. |
| G | MAXPRO Intrusion Zone Expander |
| H | MAXPRO Intrusion Relay Module |
| I | MAXPRO Intrusion Door Control Module |
| J | Central Monitoring Station |
| K | MAXPRO Receiver software |
| L | V-Plex loop with V-Plex devices.<br><br>Not all V-Plex devices may be available in all regions. Contact your local Honeywell Intrusion Sales Representative for more information. The MPIP3000 series supports two V-Plex loops. |
| M | V-Plex motion detection |

CHAPTER

# 3 INSTALLATION

This chapter describes how to mount and wire the MPI Control Panel.

## 3.1 Installation and Setup – General Workflows

Installing a brand-new system or changing an existing system requires slightly different steps. Both procedures are explained in the sections below.

### 3.1.1 Initial Installation and Setup

The recommended work flow for the initial installation and setup of an MPI system requires the following steps:

| Step | For details, see |
|---|---|
| Mounting the cabinet that houses the control panel. | Mounting the Cabinet, page 30 |
| Installing the control panel in the cabinet | *Installing the Control Panel*, page 32 |
| Wiring the control panel: tamper switches, network communication (wired and cellular), inputs (zones) and outputs (triggers), and alarm sounders. | Overview of Control Panel Connectors, page 34 following, until Wiring Outputs, page 47 |
| Installing an MPI Keypad on the IB2 bus. Each control panel requires at least one keypad. | MPI Keypads MPIKTSMF, MPIKTSPRX, page 60 |
| Wiring additional devices on the IB2 bus and/or the V-Plex loops. | Installing IB2 Bus Devices, page 59<br>Installing V-Plex Devices, page 107 |

| | |
|---|---|
| Providing power to the system: AC power supply and backup batteries. This includes wiring the AC power supply to the cabinet's power adapter, calculating the control panel load and determining the corresponding required backup battery capacity, and installing the batteries. | Powering the System, page 111<br>*Note:*<br>You must install at least 1 battery. |
| Registering the control panel in MAXPRO Cloud using the panel's MAC address. | *Connecting to MAXPRO Cloud*, page 119. |
| Applying power to the system (switching on the AC power supply). | |
| Configuring the control-panel, and registering and configuring other devices in MAXPRO Cloud | *Configuration in MAXPRO Cloud*, page 123. |
| Changing the default user codes for the keypads (Installer and Master PIN code) | *MAXPRO Cloud onlinehelp* |
| Testing and commissioning the system | *Testing and Commissioning*, page 141. |

### 3.1.2 Updating or Expanding an Existing Installation

Adding or replacing modules in an existing installation requires the following steps:

| Step | For details, see |
|---|---|
| The installer logs on to MAXPRO Cloud and switches to Installer Mode. This will prevent trouble events going to the central monitoring station during maintenance work. | *MAXPRO Cloud onlinehelp* |
| The customer grants the installer access to the system. | *MAXPRO Intrusion User Guide* (doc. no. 800-23041-1). |

| | |
|---|---|
| The installer shuts down the control panel using the SHUTDOWN button.<br><br>This makes sure that the system can save all necessary data and statuses in the flash memory. It disables the inputs and outputs, but does not remove power (from the AC power) | Shutting Down the Panel Securely, page 121 |
| The installer adds, removes, or replaces the required modules. | |
| The installer registers and configures the new peripheral devices in MAXPRO-Cloud | *Configuration in MAXPRO Cloud*, page 123. |
| The installer tests and commissions the system | *Testing and Commissioning*, page 141 |

### 3.1.3 Swapping Devices

When swapping devices, the system can remember the settings of the old device and immediately apply them to the new device

| | |
|---|---|
|  | ***Note:*** *You can only swap identical devices. The new device must be on the same data bus as the old one. If not, the system will give a mismatch error when trying to swap the device in MAXPRO Cloud.* |

To swap a device for an identical one, proceed as follows:

1. Shut down the control panel using the SHUTDOWN button.
2. Swap the device: remove the old hardware and replace it by the new one.

| | |
|---|---|
|  | ***Note:*** *For quick and easy swapping, the colored terminal blocks on all MPI devices are removable. You can leave the existing wiring in place, and just pull the terminal blocks upwards to detach them from the old device. When the new device is placed, plug the terminal blocks back on the new device.* |

3. Restart the panel.
4. In MAXPRO Cloud, go to the old device's page and click Edit.
5. Click Replace Device. For swapping the control panel, click Replace Controller.
6. Enter the unique identifier of the new device: the serial number for the device, or the MAC address for the panel.
7. Click Confirm.

8. Click Save and Sync.
9. Restart the panel.

| | |
|---|---|
| | **Note:** *When swapping a control panel, check with the CMS to make sure that it can identify the new panel and receive its notifications.* |

# 3.2 Mounting the Cabinet

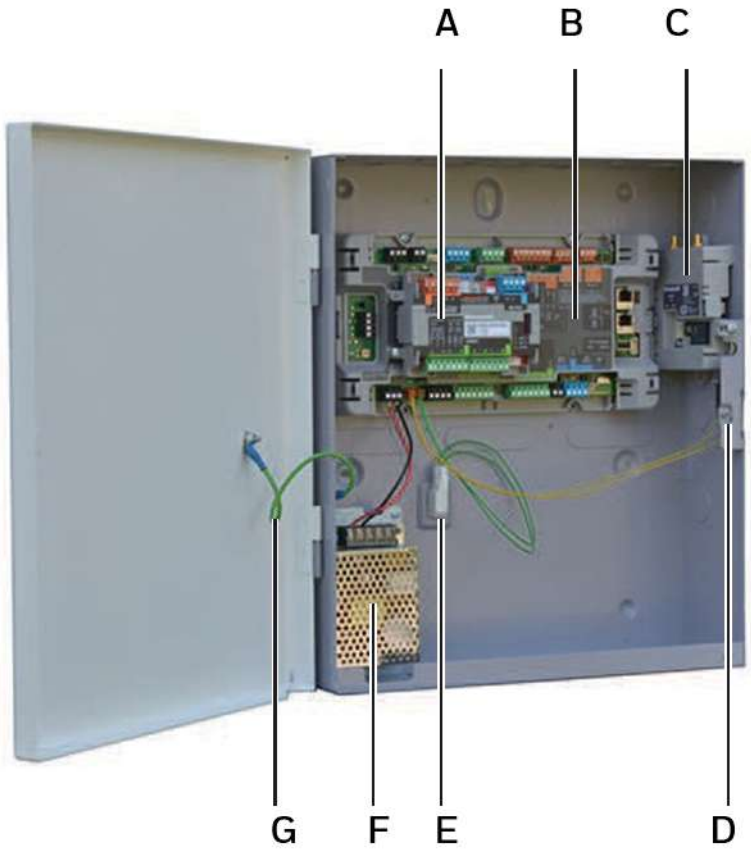
## 3.2.1 About the Cabinet

The MPI cabinet is suitable for housing an MPI Control Panel or a Remote Power Supply, and comes with a built-in AC power adapter. It comes with two tamper switches (lid and off-wall). Furthermore, the cabinet can house up to two backup batteries (18 Ah max. capacity). The cabinet can contain:

- An MPI Control Panel + optionally:
  - one additional device on top of the main board holder: either a Zone Expander or a Relay Module.
  - an LTE module.
- An MPI Remote Power Supply (RPS) + optionally:
  - up to two additional devices; one to the right of the RPS and one on top of the RPS holder. Suitable devices are: Door Control Modules, Zone Expanders, and Relay Modules.

You can find a few example configurations below.

The image below shows a cabinet with a Control Panel (B), a Zone Expander (A) on top, and the 4G/LTE Module (C) on the right-hand side.




| | |
|---|---|
| A | Zone Expander |
| B | Control Panel |
| C | 4G/LTE Module |
| D | Lid tamper switch |
| E | Off-wall tamper switch |
| F | AC power adapter |
| G | Earth lead |

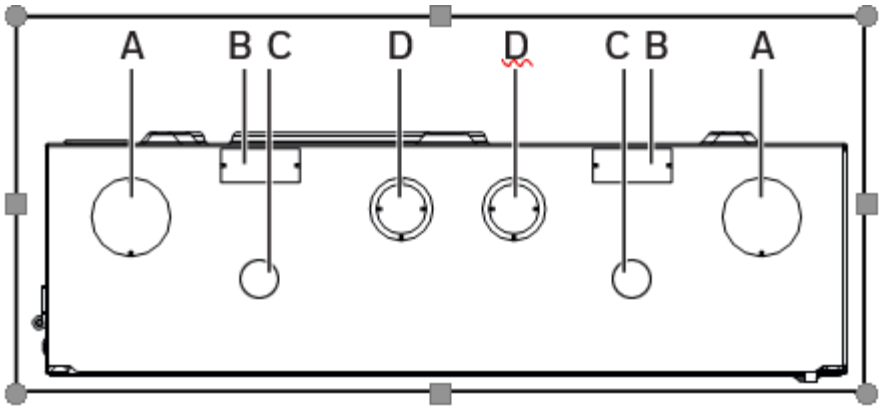
The image below shows a cabinet with a Remote Power Supply (H), a Zone Expander (I) on top, and a Door Control Module (C) to the side.


| | |
|---|---|
| H | Remote Power Supply |
| I | Zone Expander |
| J | Door Control Module |

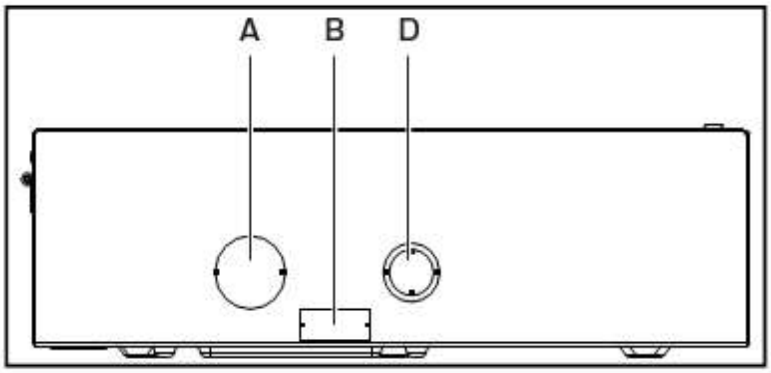
## 3.2.2 Cabinet Parts

The illustrations below show the parts of the cabinet.

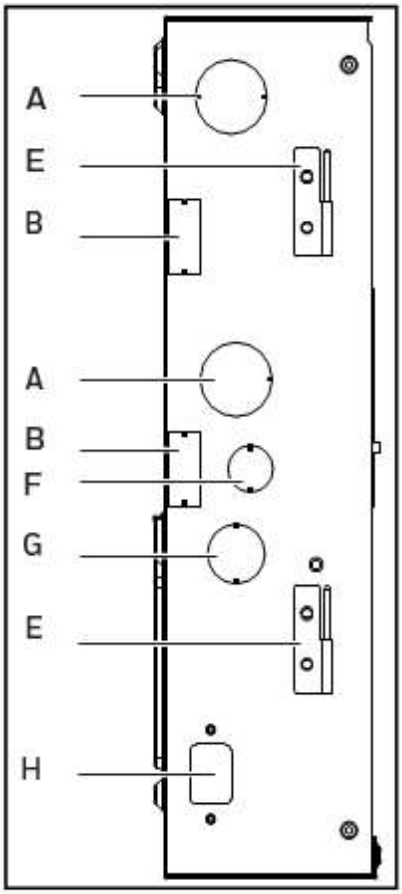
Top:



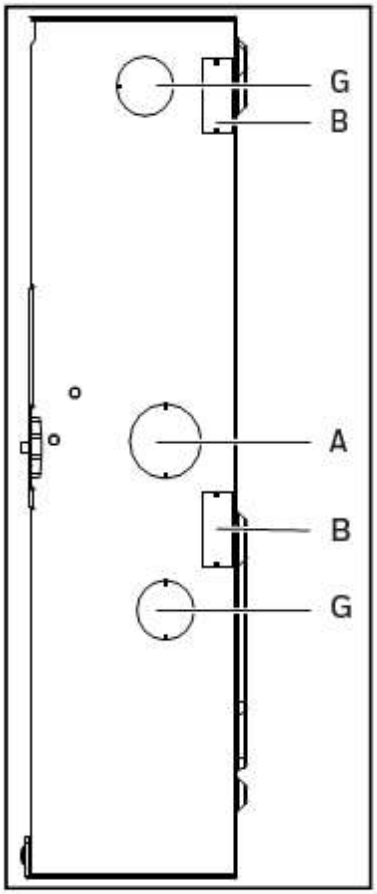
Bottom



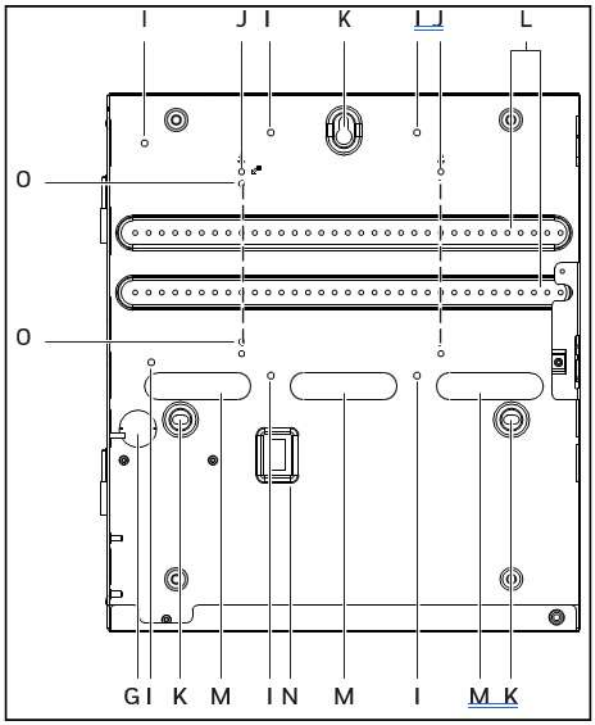

Left:




Right:



Back:

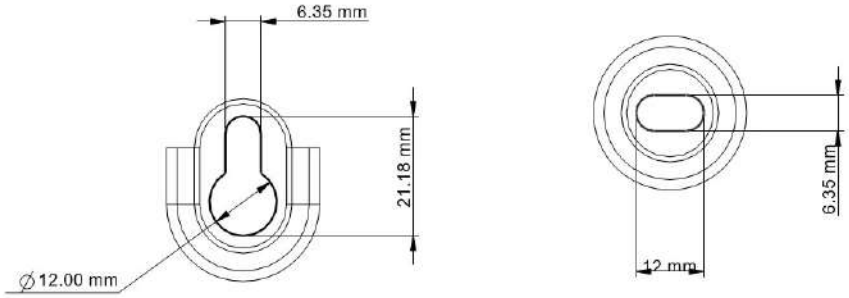



| # | Purpose | Dimensions |
|---|---|---|
| A | Wiring knockout, extra large (x 6) | Diameter 35 mm |
| B | Wiring knockout, rectangular (x 7) | 35 mm x 15 mm |
| C | Knockout for optional 4G/LTE module's antenna (x 2) | Diameter 16.8 mm |
| D | Knockout with folded edge (x 3) | Diameter 28 mm – 22 mm |
| E | Hinge (x 2) | |
| F | Wiring knockout, small (x 1) | Diameter 22 mm |
| G | Wiring knockout, large (x 4) | Diameter 28 mm |
| H | Wiring knockout for AC power inlet (x 1) | 27.8 mm x 20.2 mm |
| I | Attachment point for cable tie (x 6) | |
| J | Screw hole for mounting MPI Control Panel (x 2 above and x 2 below mounting rails) | Diameter 4 mm |
| K | Screw hole for mounting cabinet on wall (x 3) | See detail illustration further below. |
| L | Mounting rails for MPI modules (x 2) | |

| | | |
|---|---|---|
| M | Wiring knockout (x 3) | 80 mm x 20 mm |
| N | Wall tamper knockout (x 1) | 11.2 mm x 22.90 mm |
| O | Screw hole for mounting MPI Remote Power Supply (x 1 above and x 1 below mounting rails) | Diameter 4 mm |

| | |
|---|---|
| | **Caution:** ***If you are using cable glands or blanking plugs, make sure they match the knockout/conduit size to provide accurate (cable) protection. If using non-metal materials, make sure they comply with UL 94 V-0 .*** |

Detailed dimensions of the screw holes for cabinet mounting are indicated below:




## 3.2.3 Mounting the Cabinet

| | |
|---|---|
| | **Warning: If mounting the cabinet higher than 2 m above the ground, take the necessary safety precautions to prevent personal injury.** |

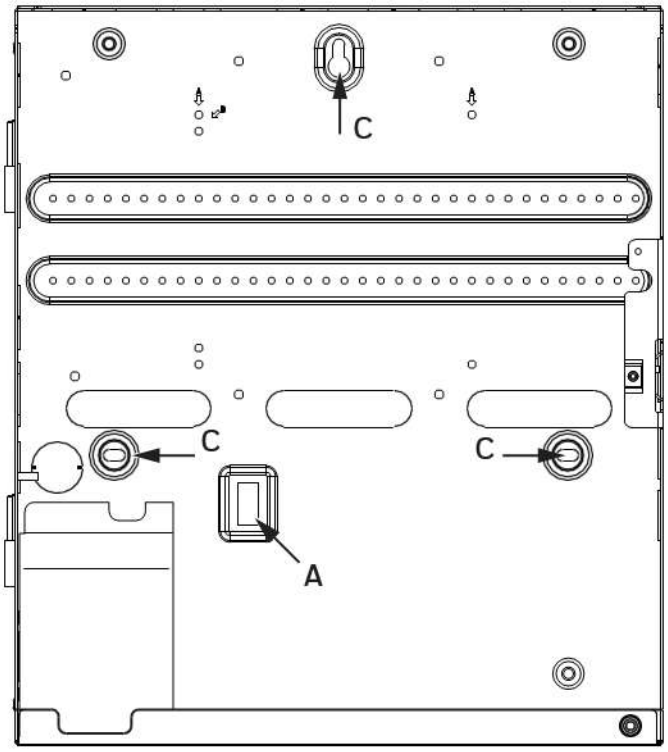
To mount the cabinet, proceed as follows:

1. Find a place for the cabinet on a sturdy wall in a clean, dry area that is not readily accessible to the general public.
2. Remove the cabinet lid by disconnecting the earth lead and sliding the lid off its hinges.
3. Remove the metal knockouts for the wiring entries that you will be using. For an overview of the available wiring entries and their sizes, see *Cabinet Parts*, page 26.

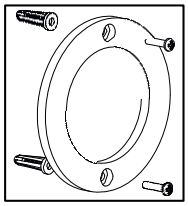
| | |
|---|---|
| | **Caution: If you are using cable glands or blanking plugs, make sure they match the knockout/conduit size to provide accurate (cable) protection. If using non-metal materials, make sure they comply with UL 94 V-0.** |

4. Temporarily remove the wall tamper switch from its knockout (A) in the back of the cabinet.

5. On the wall, mark the positions of the 3 mounting screw holes (C) and the wall tamper knockout (A). Mark the center of the tamper knockout.

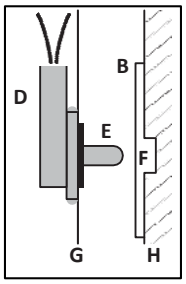



6. Take the large washer from the cabinet's accessory bag, remove the liner from the adhesive side, and stick the washer to the wall around the wall tamper mark. The center of the washer must coincide with the center of the wall tamper knockout. This will make sure that the wall tamper switch fits neatly through the washer. The washer prevents tampering with the switch.

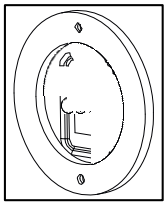


7. If necessary, fix the washer to the wall using the included plugs and screws.
8. Drill holes for the mounting screws of the cabinet.
9. Where you marked the position of the tamper knockout, drill a hole that is 2 mm deep and 8 mm in diameter. This will allow the plunger (E) of the wall tamper switch to protrude into that recess (F), preventing tampering with the switch.

B = washer fixed to the wall; D = wall tamper switch; E = plunger; F = recess in the wall; G = cabinet back plate; H = wall.



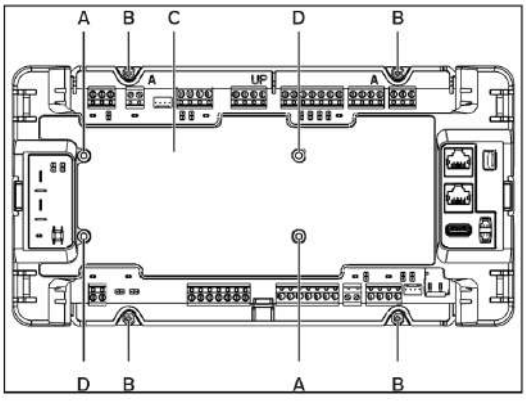

10. Place the wall tamper switch back in its knockout in the back of the cabinet.
11. Using three screws (not supplied), mount the cabinet to the wall. The wall tamper switch must fit neatly through the washer on the wall.



12. After completing the installation, slide the cabinet lid back on its hinges, and reconnect the earth lead.

# 3.3 Installing the Control Panel

## 3.3.1 Panel Parts




| | |
|---|---|
| A | Positioning pin (x 2) for stacked MPI module (optional). |
| B | Mounting screw holes (x 4) |
| C | Info card |

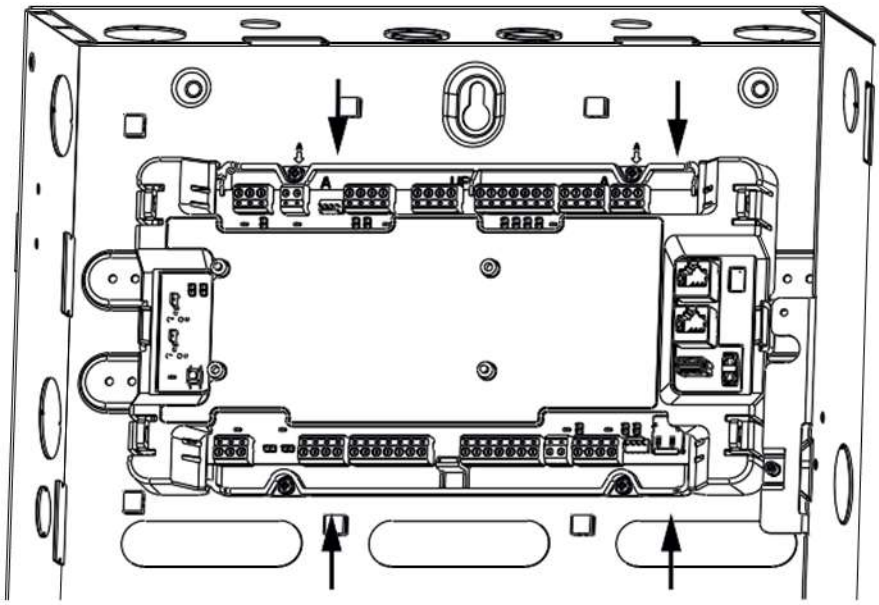
| | |
|---|---|
| D | Positioning pin with screw hole (x 2) for stacked MPI module (optional). |

### 3.3.2 Mounting the Control Panel in the Cabinet

| | |
|---|---|
| ⚠ | **Warning: High voltage is present in the cabinet's built-in AC power adapter!** |

To mount the control panel in the cabinet, proceed as follows:

1. Position the control panel over the screw holes in the cabinet and click it into position.
2. Secure the control panel to the mounting rails in the cabinet using the 4 screws supplied with the control panel.

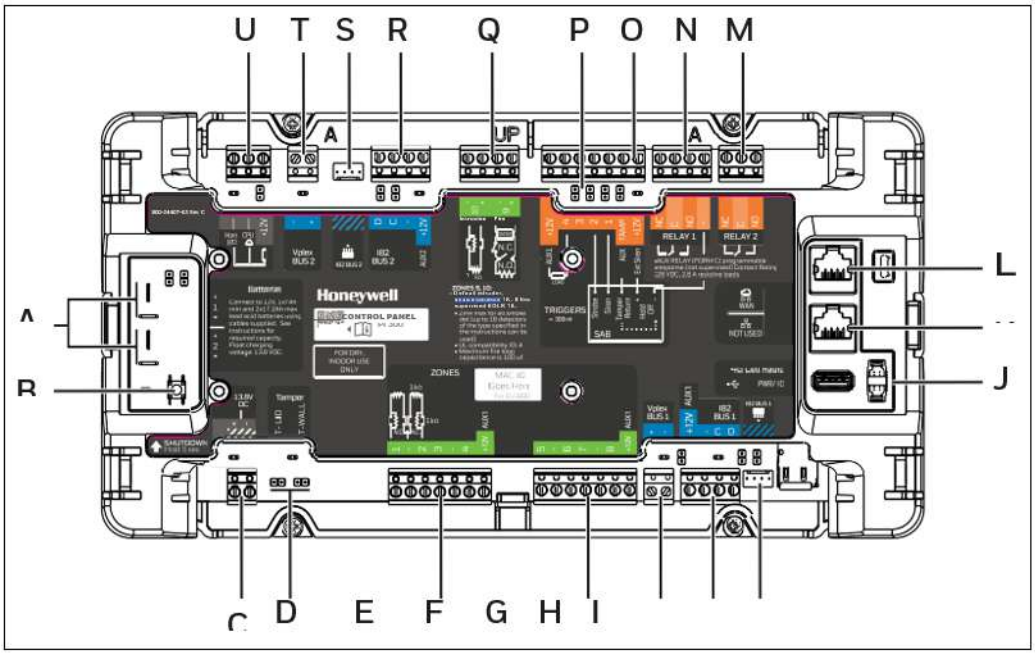


### 3.3.3 Options

You can mount a Zone Expander or Relay Module on top of the main circuit board holder. For details, see *Cabinet Mounting with Control Panel or Remote Power Supply*, page 102.

# 3.4 Overview of Control Panel Connectors

Below is a general overview of the connectors and terminals on the control panel. Detailed instructions are in the sections and chapters further below. The image below is for the MPIP3000 series. Not all connectors and terminals may be available on the MPIP2000 series.




| # | Item | Terminal or connector | Connect with |
|---|---|---|---|
| A | Batteries 1/2 | + | + terminal on backup battery 1/2 |
| | | – | – terminal on backup battery 1/2 |
| B | SHUTDOWN | (button) | Press the SHUTDOWN button for 5 seconds to shut down the panel. For details, see *Shutting Down the Panel Securely*, page 121 . |
| C | 13.8 VDC | + | Input voltage: V+ terminal on cabinet's built-in AC power adapter |
| | | – | Input voltage: V– terminal on cabinet's built-in AC power adapter |
| D | Tamper | T-LID | Cable from the cabinet's lid tamper switch |
| | | T-WALL | Cable from the cabinet's wall tamper switch |
| E | Zones 1–4 | For zones 1–4 (sensor contact inputs). For details, see Wiring Inputs (Zones), page 39 | |

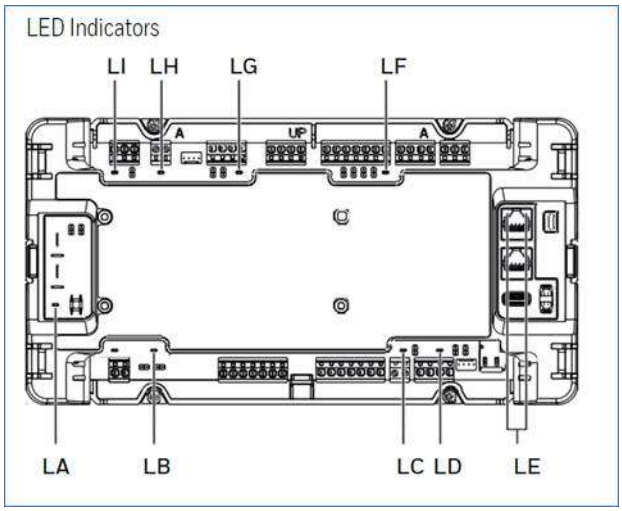
| | | | |
|---|---|---|---|
| F | Zones 5–8 | For zones 5–8 (sensor contact inputs). For details, see Wiring Inputs (Zones), page 39 | |
| G | V-plex BUS 1 | + | V-Plex bus 1 + |
| | | – | V-Plex bus 1 – |

| | | | |
|---|---|---|---|
| H | IB2 BUS 1 | +12V AUX1 | 12 VDC supply terminal for devices connected to IB2 bus 1. |
| | | – | 0 VDC supply terminal for devices connected to IB2 bus 1. |
| | | C | IB2 bus C |
| | | D | IB2 bus D |
| I | IB2 bus 1 | Quick connect plug for IB2 BUS 1 (can be used for module stacked on top of main board; quick connect cable is included). | |
| J | 4G Cell radio | USB and PWR/IO | Connectors for the 4G/LTE module |
| K | For future use. Do not use. | | |
| L | Ethernet | WAN | Network with INTERNET connection to the cloud. |
| M | Relay 2 | NC | Normal Closed terminal, output relay 2 |
| | | C | Common terminal, output relay 2 |
| | | NO | Normal Open terminal, output relay 2 |
| | | Relay 2 is only available on the MPIP3000 series. | |
| N | Relay 1 | NC | Normal Closed terminal, output relay 1 |
| | | C | Common terminal, output relay 1 |
| | | NO | Normal Open terminal, output relay 1 |
| | | – | Spare 0 VDC connector. |
| O | Triggers | For outputs. For details, see Wiring Outputs (Triggers), page 95.<br>Can also be used for a self-activating bell. For details, see Installing a Self-Activating Bell (SAB), page 46 | |
| P | Jumpers for low-voltage triggers. For details, see Wiring Outputs (Triggers), page 95. | | |
| Q | Zones 9, 10 | For zones (sensor contact inputs). Can be used for 2-wire smoke sensors or as double-balanced zones.<br>For details, see Wiring Inputs (Zones), page 39 | |

| | | | |
|---|---|---|---|
| R | IB2 BUS 2 | +12V AUX2 | 12 VDC supply terminal for devices connected to IB2 bus 2 |
| | | – | 0 VDC supply terminal for devices connected to IB2 bus 2 |
| | | C | IB2 bus C |
| | | D | IB2 bus D |
| | | IB2 BUS 2 is only available on the MPIP3000 series. | |
| S | IB2 bus 2 | Quick connect plug for IB2 BUS 2 (can be used for module stacked on top of main board; quick connect cable is included).<br>Only available on the MPIP3000 series. | |
| T | V-plex BUS 2 | + | V-Plex bus 2 + |
| | | – | V-Plex bus 2 – |
| | | V-plex BUS 2 is only available on the MPIP3000 series. | |
| U | Horn 8 Ω | Output to loudspeaker (min. 8 ohm), for alarm and entry/exit tones. | |
| | CPU | CPU failure output (watchdog): can be connected to a piezo sounder or LED to indicate a total system failure. | |
| | +12V | Auxiliary 12 VDC output | |

**Caution: Do not use any terminals that are labeled NOT USED.**

# 3.5 Overview of Control Panel LEDs




| # | LED Color | Description |
|---|---|---|
| LA | Red | Shutdown: on when control panel is active and while shutting down; is off when panel has shut down. |
| LB | Green | Power input available on main board. |
| | Off | No power available on main board. |
| LC | Green | V-Plex 1: loop OK. |
| | Off | V-Plex 1: loop shorted or data bus not running. |
| LD | Green | AUX1/IB2 bus 1: power on AUX1 is available. |
| | Off | PTC for AUX1 is resetting, or other trouble on the bus. |
| LE | Amber (left) | Ethernet amber LED (left): network connection is working. |
| | Green (right) | Ethernet green LED (right): flashes when the system is sending or receiving data over the network. |
| LF | Green | Ext. siren power (AUX3): power is available. |
| | Off | PTC for AUX3 is resetting. |
| LG | Green | AUX2/IB2 bus 2: power on AUX2 is available. |
| | Off | PTC for AUX2 is resetting, or other trouble on the bus. |
| | This LED is only available on the MPIP3000 series. | |
| LH | Green | V-Plex 2: loop OK. |
| | Off | V-Plex 2: loop shorted or data bus not running. |
| | This LED is only available on the MPIP3000 series. | |

| | | |
|---|---|---|
| LI | Red | Processor fault. |
| | Off | Processor OK. |

# 3.6 Connecting the Cabinet Tamper Switches

The cabinet comes with two tamper switches: one to prevent removal of the cabinet from the wall and one to prevent opening of the cabinet lid. Use the included cables to connect the tamper switches to the control panel (D, page 34)

| From | To Control Panel Terminal |
|---|---|
| Tamper switch in cabinet lid | T-LID |
| Tamper switch in cabinet back | T-WALL |

The system will report tamper events on Area 1, the system area.

- If Area 1 is disarmed, the system will report the tamper event as a fault condition.
- If Area 1 is armed, the system will report the tamper event as an alarm.

You can bypass the tamper switches by fitting a jumper on the tamper inputs on the control panel.

**Caution: Bypassing tamper inputs may invalidate compliance with local regulations.**

# 3.7 Network Connection (Ethernet)

## 3.7.1 Connecting to the Network

The Ethernet connection provides the main connection to internet for alarm signaling to the central monitoring station and communication with MAXPRO Cloud.Connect the main board (L, page 35) to the network that provides the internet connection using a standard Ethernet cable. Clip both ferrite beads over the cable. Position them as close as possible to the Ethernet connector on the control panel.

- The amber LED is illuminated when the network connection is working.
- The green LED flashes when the system is sending or receiving data over the network.

Upon first start-up, MAXPRO Cloud will automatically try and connect to the control panel. By default, the system uses dynamic IP addressing (DHCP). If connection should fail, you can edit the settings using the keypad and set up the IP network manually. For details, see *Connecting to MAXPRO Cloud*, page 119. You can view the network settings in MAXPRO Cloud.

## 3.7.2 Securing the Network

Make sure that the routers and firewalls in the network are set up correctly: network address translation (port forwarding), firewall settings, etc. If not, the control panel will not be able to send alarm and other information to MAXPRO Cloud. The table below lists the port numbers and services that are required for communication:

| Port No. | Protocol | Function |
|---|---|---|
| 53 | UDP | DNS server |

| | | |
|---|---|---|
| 123 | UDP | Used to synchronize time |
| 443 | TCP (TLS 1.2) | MAXPRO Cloud communication ISOM |

**Caution: For a secure network connection, please follow instructions for the network and firewall as described in the *MAXPRO Intrusion Security Manual* (doc. no. 800-25507).**

***Note:*** *Trouble and tampering signaling is disabled while the system is in Installer Mode. If you are on-line with the panel, but in Normal mode, all alarms report immediately. All other reports are delayed until you complete the session. The keypads remain active when on-line with a control panel but are inactive during actual uploading or downloading sessions. The keypads will indicate that the system is running in Installer Mode: the text Installer service mode appears in the top left corner of the display.*

# 3.8 Wiring Inputs (Zones)

***Note:*** *This section applies to the zones on the MPI Control Panel and the connected IB2 bus devices. It is not applicable to V-Plex devices. For wiring V-Plex devices, see Installing V-Plex Devices, page 107.*

## 3.8.1 Overview

The control panel offers 10 zones (sensor inputs). Zones 9 and 10 can be used for 2-wire smoke detectors.

## 3.8.2 Zone Wiring Types

Wire the required zones (*E*, page 34, F, page 35, and Q, page 35) or terminate them using resistors.

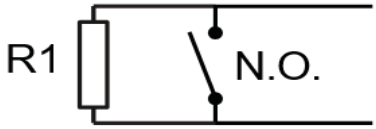
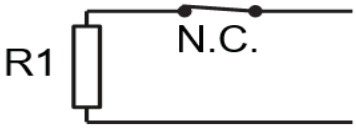
***Note:*** *Any unused hardwire zones should always have a 1K resistor wired across the zone terminals to terminate them.*

Possible wiring types are:

- Supervised EOLR (normal open or normal closed)
- Double balanced
- Triple balanced.

- No EOLR (normally open or normally closed) All types are described in detail further below.

*Supervised EOLR*

| R1 N.O. | R1 N.C. |
|---|---|
|  |  |
| For a normally open circuit, you wire the sensor (N.O.) in parallel to the EOL resistor R1. | For a normally closed circuit, you wire the sensor (N.C.) in series with the EOL resistor R1. |

| State at input terminals | Message to the system |
|---|---|
| Short circuit | Alarm |
| R1 ohms | Ready |
| Open circuit | Alarm |

Acceptable EOL values for R1 are defined in the table below. The electrical bands for each R1 value are indicated below:

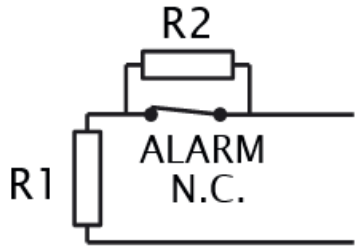
| | 0 → Ohm<br>Alarm < Ready < Alarm | | |
|---|---|---|---|
| R1 = 1K | 500 ? | | 1,500 ? |
| R1 = 2K/2K2 | 1,000 ? | | 3,000 ? |
| R1 = 3K3 | 2,000 ? | | 4,000 ? |
| R1 = 5K6 | 2,800 ? | | 8,400 ? |

For example, for R1 = 2K, the system will go in:

- Alarm state if the resistance falls below 1,000 ohms.
- Ready state if the resistance is between 1,000 and 3,000 ohms.
- Alarm state if the resistance is above 3,000 ohms.

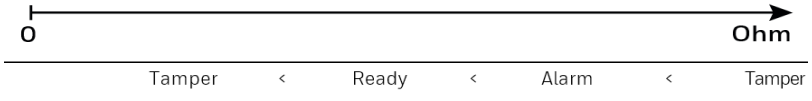
| | |
|---|---|
| | **Note:** *Resistor tolerance 1% or better.*<br>*Capable of up to 100 ohms resistance.* |

*Double Balanced*




| State at input terminals | Message to the system |
|---|---|
| Short circuit | Tamper |
| R1 ohms | Ready |
| R1 + R2 ohms | Alarm |
| Open circuit | Tamper |

Acceptable EOL values for R1 and R2 are defined in the table below. The electrical bands for each R1/R2 value are indicated below:




| | | | |
|---|---|---|---|
| R1 = 1K; R2 = 1K | 800 Ω | 1,500 Ω | 12,000 Ω |
| R1 = 2K; R2 = 2K | 1,500 Ω | 3,000 Ω | 15,000 Ω |
| R1 = 2K2; R2 = 4K7 | 1,500 Ω | 3,000 Ω | 15,000 Ω |
| R1 = 4K7; R2 = 4K7 | 4,000 Ω | 6,000 Ω | 12,000 Ω |

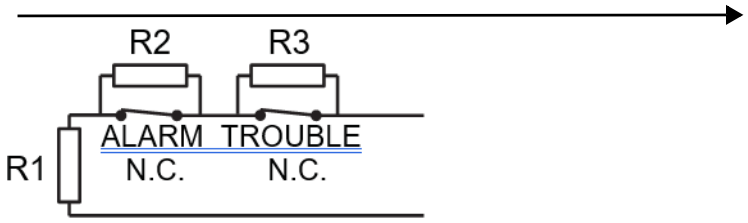
For example, for R1 = R2 = 1K, the system will go in:

- Tamper state if the resistance falls below 800 ohms.
- Ready state if the resistance is between 800 and 1,500 ohms.

- Alarm state if the resistance is between 1,500 and 12,000 ohms.
- Tamper state if the resistance is above 12,000 ohms.

| | |
|---|---|
| | **Note:** *Double balanced with 1K resistors is the default zone supervision configuration for the control panel's zones 9 and 10 when used as intrusion zones (default). Resistor tolerance 1% or better. Capable of up to 100 ohms resistance.* |

*Triple Balanced*

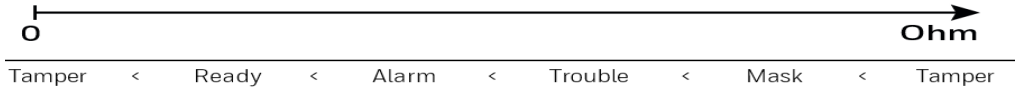



| State at input terminals | Message to the system |
|---|---|
| Short circuit | Tamper |
| R1 ohms | Ready |
| R1 + R2 ohms | Alarm |
| R1 + R3 ohms | Trouble |
| R1 + R2 + R3 ohms | Mask condition (trouble when system is disarmed; alarm when system is armed) |
| Open circuit | Tamper |

Acceptable values for R1, R2, and R3 are:

- R1 = 1K
- R2 = 1K
- R3 = 3K.

The electrical bands are indicated below:



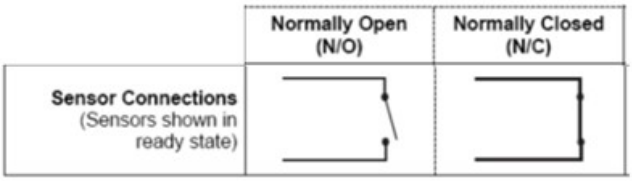

| | | | | |
|---|---|---|---|---|
| 800 Ω | 1,800 Ω | 2,500 Ω | 4,500 Ω | 10,000 Ω |

With R1 = R2 = 1K and R3 = 3K, the system will go in:

- Tamper state if the resistance falls below 800 ohms.
- Ready state if the resistance is between 800 and 1,800 ohms.
- Alarm state if the resistance is between 1,800 and 2,500 ohms.
- Trouble state if the resistance is between 2,500 and 4,500 ohms.
- Mask condition if the resistance is between 4,500 and 10,000 ohms.
- Tamper state if the resistance is above 10,000 ohms.

| | |
|---|---|
| | **Note:** *Triple balanced is the default zone supervision configuration for the control panel's zones 1–8.*<br>*You cannot use triple balanced with the control panel's zones 9 and 10.*<br>*Resistor tolerance 1% or better.*<br>*Capable of up to 100 ohms resistance.* |

*No EOLR (Normally Open or Normally Closed)*




*No EOLR (Normally Closed)*

| State at Input Terminals | Message to the System |
|---|---|
| Short Circuit Open Circuit | Ready |
| | Alarm |

For example, the system will go in:

- Ready state if the resistance is below 1,200 ohms.
- Alarm state if the resistance is above 1,200 ohms No EOLR (Normally Open)

For example, the system will go in:

- Alarm state if the resistance is below 1,200 ohms.
- Ready state if the resistance is above 1,200 ohms

## 3.8.3 Using 2-Wire Smoke Detectors on Zone 9 and 1 0

*About Zones 9 and 10*

By default, zones 9 and 10 are configured as intrusion zones; with default supervision double balanced with 1K resistors. However, you can also use these zones as fire zones with 2-wire smoke detectors. If you switch zone 9 or 10's response type to fire, the system automatically sets the supervision configuration to Supervised EOLR with a 1K resistor. You can change the resistor value if needed; the supervision type is fixed to Supervised EOLR.

Zones 9 and 10 can each support up to 16 two-wire smoke detectors if you configure them as fire zones. The zones provide 12 VDC power to the sensors (10–14.5 VDC).

You cannot use triple-balanced supervision with zones 9 and 10.

| | |
|---|---|
|  | ***Note:*** *The alarm current on zones 9 and 10 supports only one smoke detector in the alarmed state* |

**EN** The control panel is currently not EN 54 certified.

*Compatible 2-Wire Smoke Detectors*

| Detector type | Device model no. |
|---|---|
| Ionization smoke detector | System Sensor 1151 |
| Photoelectric smoke detector | System Sensor 2W-B |
| Photoelectric smoke detector with thermal sensor | System Sensor 2WT-B |
| Photoelectric smoke detector with thermal sensor and sounder | System Sensor 2WTA-B |
| Photoelectric smoke detector with thermal sensor and Form C relay | System Sensor 2WTR-B |
| Photoelectric smoke detector | System Sensor 2151 |
| Photoelectric smoke detector with heat sensor | System Sensor 2151T |
| Heat Detector | System Sensor 5151 |

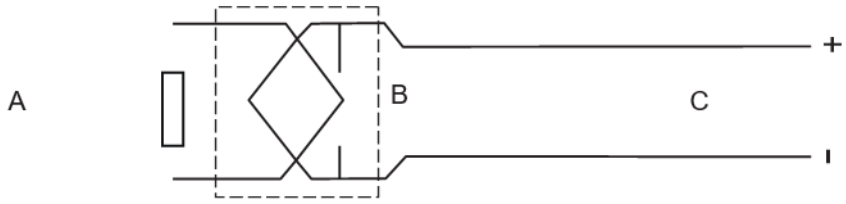
***Note:*** *Not all listed devices may be available in all regions. Contact your local Honeywell Intrusion Sales Representative for availability in your region*

*Wiring Fire Zones*

**Caution: You must use EOL resistors on fire zones when configured for use with smoke sensors, and across the loop wires of each zone at the last detector. Do not use the – (negative) terminals on zones 9 and 10 for anything else than the zone wiring itself. They are not connected to the common ground.**

Connect 2-wire smoke detectors across zone 9 or 10 terminals (+ and –) as shown below. Observe proper polarity when connecting the detectors.

You must connect the EOL resistor across the loop wires at the last detector.




A = End of line resistor; B = 2-wire smoke detector; C = terminals of zone 9/10.

| State at input terminals | Message to the system |
|---|---|
| Short circuit | Alarm |
| X ohms (EOLR value) | Ready |
| Open circuit | Trouble |

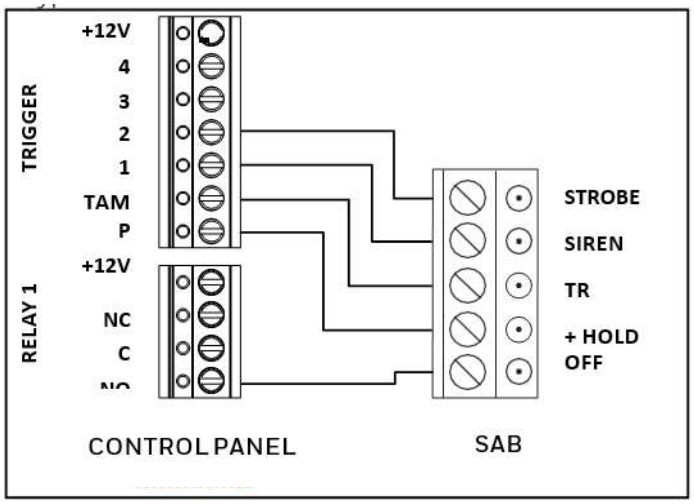
# 3.9 Wiring Alarm Sounders

## 3.9.1 Overview

The following alarm sounder outputs are available on the control panel:

- An output to a self-activating bell (SAB). For details, see *Installing a Self-Activating Bell (SAB)*, page 46.
- The Horn output to a loudspeaker for an internal siren. For details, see *Horn Output*, page 47.

## 3.9.2 Installing a Self-Activating Bell (SAB)




The SAB terminals allow for connecting an external siren with tamper protection. The illustration below shows a typical 5-wire connection.

| From control panel terminal | To SAB terminal |
|---|---|
| Trigger 2 | Strobe |

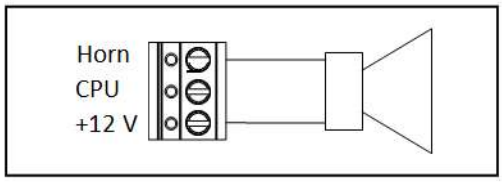
| | |
|---|---|
| Trigger 1 | Siren / Bell |
| TAMP (AUX) | Tamper return / TR |
| +12V (Ext Siren) | Hold off + / +Ve |
| – (on Relay 1 terminal block) | Hold off – / –Ve |

The default settings in MAXPRO Cloud are suitable for this SAB configuration: Trigger Output 1 = Exterior Siren; and Trigger Output 2 = Strobe. If you have wired up the SAB as shown, you do not need to change the settings.

### 3.9.3 Horn Output

The horn terminal (*U*, page 36) allows for connecting an 8-ohm loudspeaker to function as an internal siren, and to produce alarm and entry/exit tones. It gives a louder repeat of the keypad tones.

Wire the loudspeaker between the Horn 8Ω (–) and the +12V (+) terminals.




| | |
|---|---|
| | **Note:** *The horn output does not produce the confirmation of arming ding* |

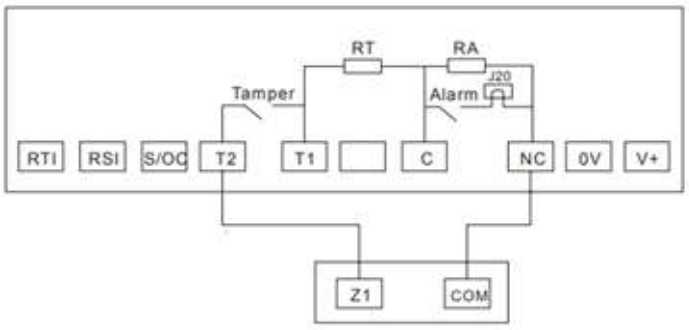
#### *Wiring Outputs*

The control panel offers the following outputs:

- Four programmable low-voltage trigger outputs (O, page 35) for arming LEDs, smoke detector power reset, etc.
  - Wire the AUX1 +12V terminal to the output device, and then use one of the trigger terminals 1 to 4 to switch to ground. The outputs will switch to ground when activated.
  - Max. current is 300mA for each trigger. For outputs that require a known state (logical 0/ 1), you can customize the outputs to use a pull-up resistor by fitting jumpers on the outputs.
- Two relay outputs, 28 VDC, 2.8 A max., resistive loads
  - Wire the relays between the common C terminal and the normal closed NC or normal open NO terminals.

## 3.10 Wiring Seismic Sensors

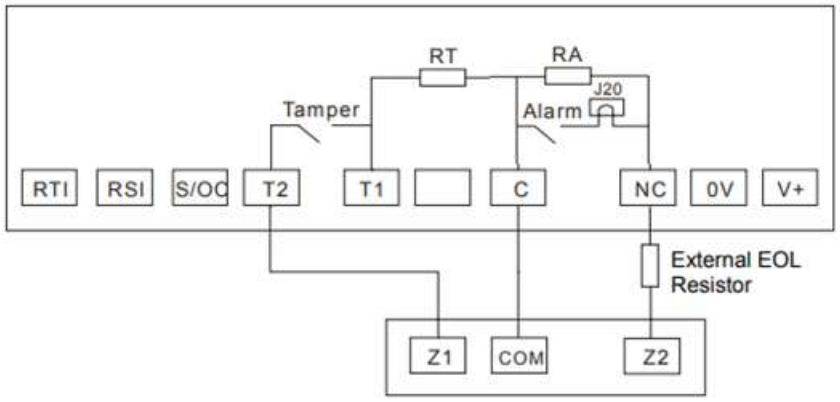
### 3.10.1 Single zone for alarm and tamper of seismic sensor




Z1 = Seismic as response type

Wiring type: It is recommended to use Double balanced/ Triple balanced.

### 3.10.2 Alarm and Tamper configured to two loops

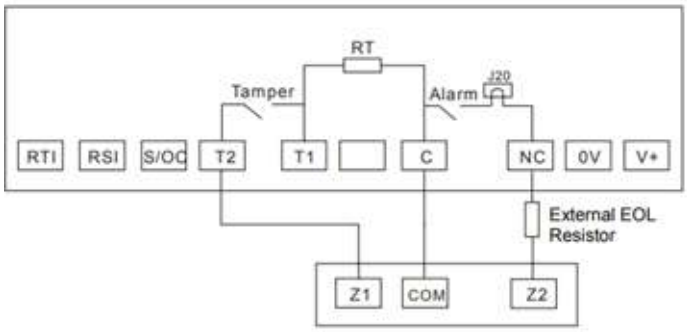



Z1 = Tamper as response type

Z2 = Seismic as response type

Wiring type: It is recommended to use Double balanced/Triple Balanced.

### 3.10.3 Alarm and Tamper configured to two loops with supervised EOLR




Z1 = Tamper as response type

Z2 = Seismic as response type

EOL = Supervised EOLR

Wiring type: It is recommended to use Supervised EOLR.

| | |
|---|---|
| | ***Note:*** *When this wiring diagram is used, RT can still be used for tamper loop, but the jumper on RA needs to be removed. Also, the external EOL resistor has to be connected to alarm loop.* |

CHAPTER

# 4 INSTALLING THE 4G/LTE MODULE MPICLTEE

The MPI 4G/LTE Module is an optional/primary communication module intended for use with the MPI Control Panel.

Communication Path settings in MPC enables you to select the desired communication path such as:

- Single Path Ethernet
- Dual Path - Ethernet Primary and Cellular Secondary
- Single Path Cell Radio

*For example*, if you select Single Path Cell Radio as the communication path, MPC and delivery of alarms and other messages to the central monitoring station will happen through 4G communication.

## 4.1 About the 4G/LTE Module

The MPI 4G/LTE Module is an optional communication module intended for use with the MPI Control Panel. It can provide a full backup path for the Ethernet connection, providing cellular radio communication for delivery of alarms and other messages to the central monitoring station.

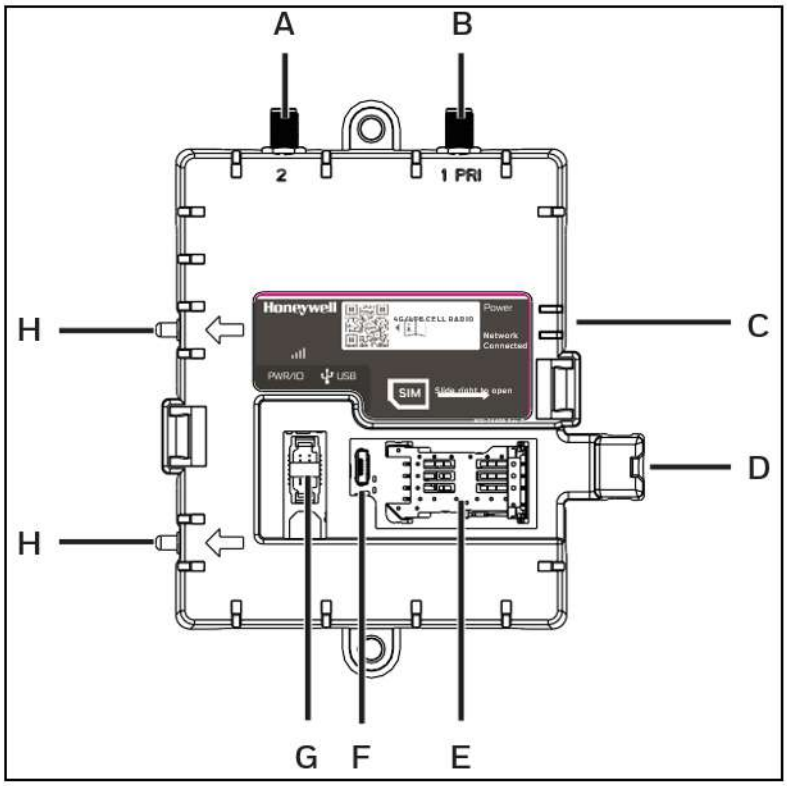
The 4G/LTE Module comes with two sets of SMA cable + SMA isolator + SMA antenna to support receive diversity. For details, see *Receive Diversity Antenna System*, page 57

Communication requires a valid data SIM card (2FF mini-SIM).

| | |
|---|---|
|  | **Caution: Shut down the control panel and disconnect power, including the battery or batteries, before installing the module. Removing power from the module without properly shutting down the control panel, can result in permanent damage to the module. For the correct shutdown procedure, see Disconnecting/Reconnecting, page 56.** |

# 4.2 Installation

## 4.2.1 Parts Overview



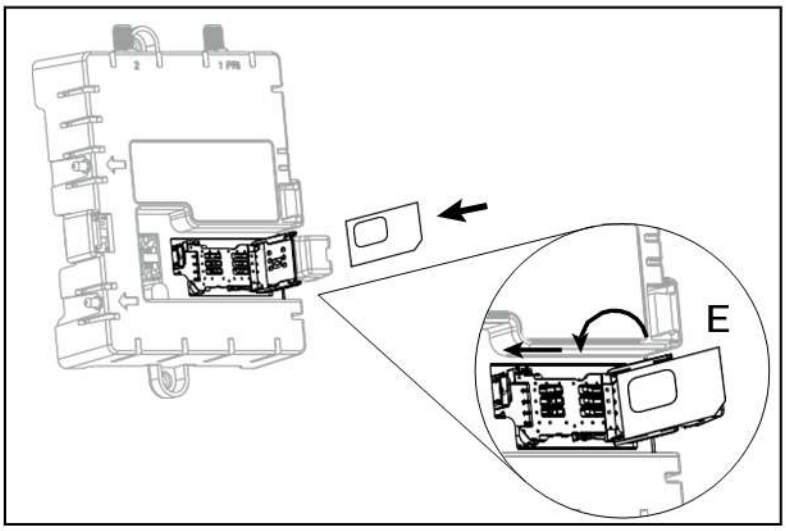

| | |
|---|---|
| A | Secondary antenna SMA connector (indicated as 2 on the device) |
| B | Primary antenna SMA connector (indicated as 1 PRI on the device) |
| C | Power and network LEDs. For details, see LED Indicators, page 58. |
| D | Mounting screw hole |
| E | SIM card holder (for 2FF mini-SIM) |
| F | Micro USB connector |
| G | I/O, Power & Ground cable connector |
| H | Alignment pegs (x 2) |

### 4.2.2 Installing the SIM Card

| | |
|---|---|
| | **Note:** *The MPICLTEE model comes without SIM card. Please purchase and activate a suitable SIM card (2FF mini-SIM) from your preferred provider.* |

To install the SIM card, proceed as follows:

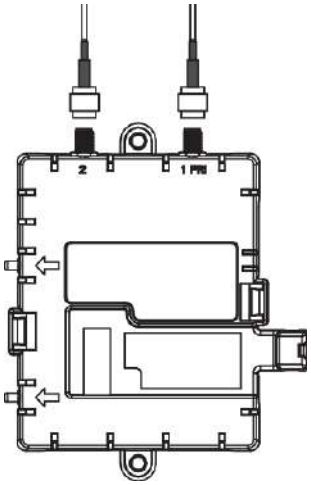
- On the LTE module, slide the SIM card holder door (E) to the right to unlock, then flip the door open.




- Slide the SIM card in the door as shown in the illustration.
- Close the SIM card holder door and slide it to the left to lock.

### 4.2.3 Installing the SMA Cables on the 4G/LTE Module

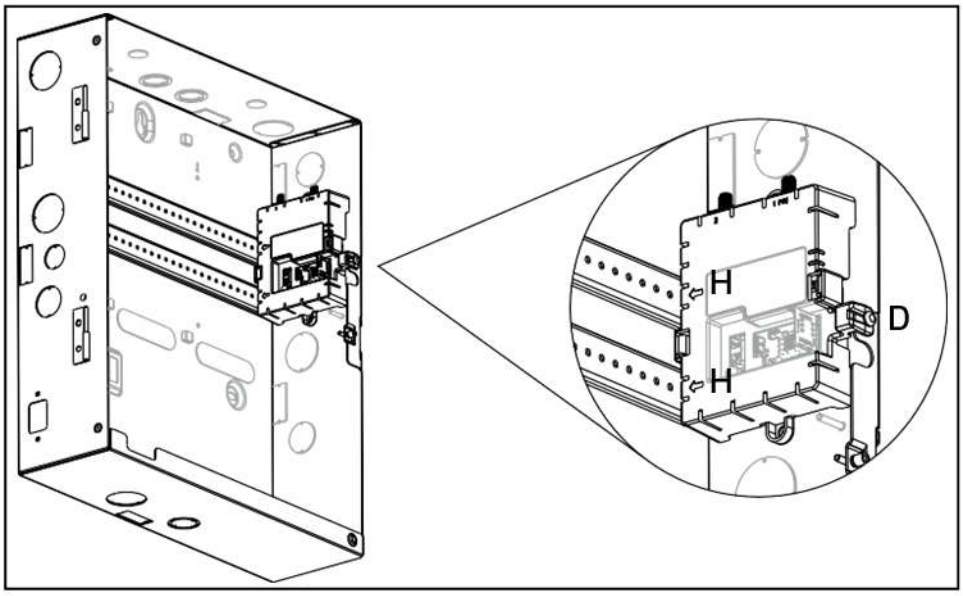
To install the SMA cables on the 4G/LTE module, proceed as follows



- Thread the SMA cables onto the primary (B) and secondary (A) antenna connectors.
- Securely tighten the connectors being careful not to overtighten.

### 4.2.4 Installing the 4G/LTE Module in the Cabinet

To install the 4G/LTE module in the cabinet, proceed as follows:

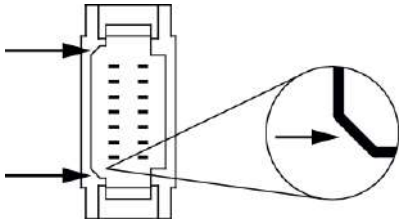


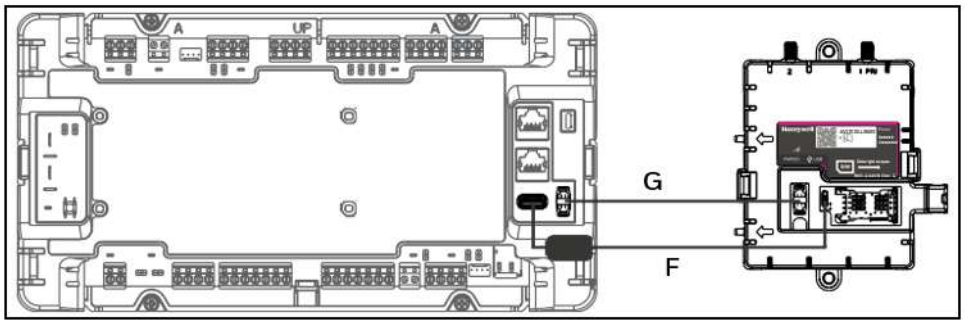

- Insert the alignment pegs (H) in the cabinet mounting holes (second set from the right). Use the indicator arrows on the module housing as a guide. Note: For clarity, the control panel and the SMA cables in the illustration below have been omitted.
- Fix the module in place using the screw (D).

### 4.2.5 Connecting to the MPI Control Panel

To connect the 4G/LTE module to the control panel, proceed as follows:

- Connect the module's PWR/IO and USB connectors (F and G) to the MPI Control Panel using the included cables.

| | |
|---|---|
| ⚠ | **Caution: Insert the plugs into the PWR/IO connectors very gently; do not apply any pressure if the plugs don't enter immediately. If you do apply pressure, you will bend the pins in the connectors. Make sure to align the chamfered corners of plug and connector correctly.**  |

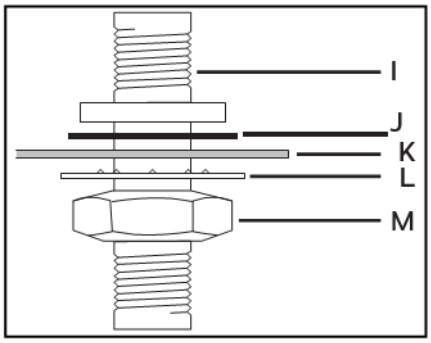



- Clip the ferrite bead over the USB cable (F). Position it as close as possible to the USB port on the control panel.

### 4.2.6 Installing the SMA Isolators on the MPI Cabinet

To install the SMA isolators, proceed as follows:

- Remove the antenna knockouts from the top of the MPI cabinet
- Place the flat washer (J) on top of the cabinet knockouts, then insert the SMA isolator (I) through the knockouts.



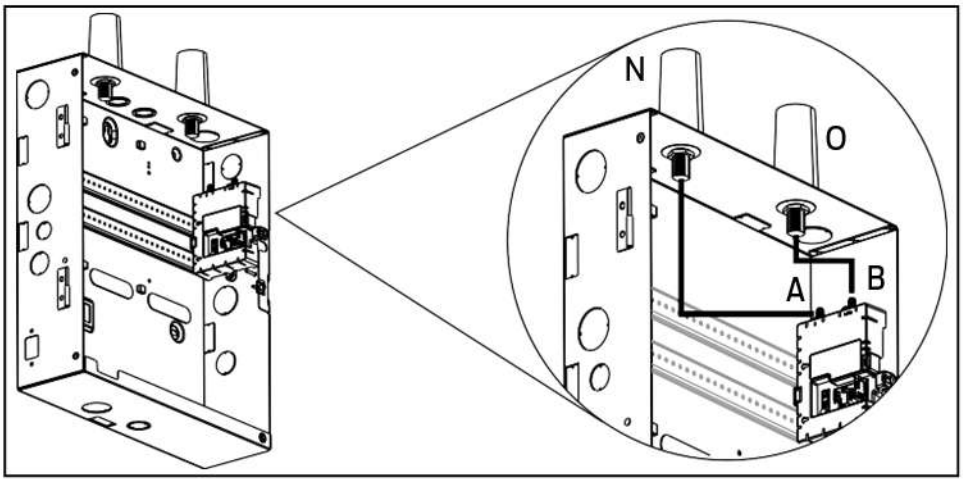

(SMA isolator; J: flat washer; K: cabinet wall; L: lock washer; M: nut)

- On the inside of the cabinet: slide the lock washers (L) over the SMA isolators and fix in position using the nuts (M).

### 4.2.7 Connecting the Primary and Secondary Antennas

To connect the antennas, proceed as follows:

- Mount the primary antenna (O) on the SMA isolator on the right-hand side of the MPI cabinet. Use an SMA cable to connect it to the primary connector (B) on the module.




- Connect the secondary antenna (N) on the SMA isolator on the left-hand side of the MPI cabinet. Use an SMA cable to connect it to the secondary connector (A) on the module.

### 4.2.8 Configuration in MAXPRO Cloud

- Log on to MAXPRO Cloud. Go to the appropriate customer, site, and control panel (= "controller" in MAXPRO Cloud). Click the **Communication Path** tab.
- Click the Edit button (top right), and then click the GSM Settings switch to turn it on. Under GSM Settings, fill in the **Access Point Name** (APN) and – if required – the user name and password from your provider. Click **Save**.
- For more information on communication settings and transmission paths, see the MAXPRO *Cloud Configuration Guide* (doc. no. 800-24096-1).

## 4.3 Disconnecting/Reconnecting

| | |
|---|---|
| ⚠ | **Caution: Removing power from the LTE module without properly shutting down the control panel can result in permanent and irreparable damage to the module. Always follow the procedure below if you need to disconnect/reconnect the module.** |

To disconnect the LTE module, proceed as follows:

- On the control panel, press the SHUTDOWN button for 5 seconds.
- Wait for the control panel to shut down completely (= the shutdown LED on the panel is off).
- You can now disconnect the LTE module and remove any cables. To reconnect the LTE module, proceed as follows:
- Reconnect all cables carefully.
- On the control panel, press the SHUTDOWN button once. The control panel will power up.

## 4.4 Receive Diversity Antenna System

The primary antenna is used for transmit and receive. The secondary antenna is the diversity antenna (receive only). The radio automatically determines and selects the receive path that provides the best Quality of Service (QoS).

Install the antennas depending on the reception requirements, using any of the options below.

- Standard installation: Use both primary and secondary antennas, mounted on top of the MPI cabinet. Install the primary antenna on the right-hand side, and the secondary antenna on the left-hand side.
- Option 1: Use both primary and secondary antennas, mounted either remotely or on top of the MPI cabinet in any combination. If mounting remotely, use approved coax cables to connect the antennas to the 4G/LTE module. For details on cabling, see Cable Type Requirements, page 175.
- Option 2: Use the primary antenna only, mounted either on top of the MPI cabinet or remotely.

## 4.5 Swapping the SIM Card

If you need to change the SIM card in the LTE module, you must restart the control panel. If not, the new SIM card will not work.

To swap the SIM card in the LTE module, proceed as follows:

- Swap the SIM card.
- Restart the panel using the SHUTDOWN button. For details, see *Shutting Down the Panel Securely*, page 121.
- Check the LTE module settings in MAXPRO Cloud and test the communication.

**Caution: If you change the Access Point Name (APN) for the LTE module in MAXPRO Cloud (for example when changing providers), you have to restart the control panel for the changes to take effect.**

## 4.6 LED Indicators

| LED | Function |
|---|---|
| Power (green) | Device is powered. |
| Network Connected (yellow) | Network connection status:<br>▪ Short flash every 4 seconds: idle, normal state.<br>▪ Short flash every 2 seconds: data transfer in progress.<br>▪ Fast flash (0.5s on, 0.5s off): no network or connection issue. |

## 4.7 RF Exposure

| | |
|---|---|
|  | **Warning: The antenna(s) used for this device must be installed to provide a separation distance of at least 20 cm (7.8 inches) from all persons and must not be co- located or operating in conjunction with any other antenna or transmitter except in accordance with FCC and ISED multi-transmitter product procedures.** |

## 4.8 Learn wireless detectors

Wireless Sensors can be learned provided that at least one RF Portal is configured onto the system.

For more information on enrolling RF Devices, refer **To configure the zones (Auto enrollment)** and **To configure the RF Zones (Manual Enrollment)** sections appearing in *MPI Configuration Guide*.

CHAPTER

# 5 INSTALLING IB2 BUS DEVICES

## 5.1 About IB2 Devices

The system guarantees performance of up to 46 devices per IB2 bus. Practically, the actual number of devices you can use depends on:

The control panel model. For details on the capabilities of each control panel model, see Overview and Panel Model Comparison, page 13.

The maximum current you can draw from the auxiliary outputs on the control panel. However, you can expand the capability using MPI Remote Power Supplies. For details on the maximum current draws on the auxiliary outputs, see Specifications, page 162.

The system will automatically provide a module number (address) for each device upon registration in MAXPRO Cloud.

For an overview of compatible IB2 devices, see *Parts List*, page 191.

| | |
|---|---|
|  | ***Note:*** *The control panel polls the IB2 bus and will report issues (for example, a missing module) within 10 seconds. The restore event is raised within 45 seconds. Upon a short-circuit on the IB2 bus power, the system will generate 'AUX low' and 'AUX fuse' events. Upon a short on the data bus, the system will generate a 'Module missing' event.* |

## 5.2 Cable Specifications

Suitable cable types for wiring devices on IB2 buses:

- 4-core alarm cable 22/4 STR CM/CL2); 100 ohms/km max.
- CAT 5E cable: UTP 24 AWG.Configuration and cable runs:

| | |
|---|---|
|  | **Caution: Use of other types of cables than those listed are at the installer's risk. Other types of cable than the ones mentioned above, including copper-clad aluminum and screened cable, significantly reduces usable distance and are not recommended.** |

- Free wiring topology, fully loaded bus.

- 3.65km/12,000ft–totalvolumeofcable(totallengthregardlessof topology).

| | |
|---|---|
|  | **Note:** *The minimum voltage required at each device is 11.5 VDC (with the control panel running on 13.8 VDC from the AC power adapter). If necessary, you can add MPI Remote Power Supplies to boost the voltage on the IB2 bus. For details, see* *MPI Remote Power Supply MPIPSU35, page 89.* |

# 5.3 MPI Keypads MPIKTSMF, MPIKTSPRX

## 5.3.1 About the MPI Keypads

The MAXPRO Intrusion Keypads are designed to provide a simple day-to-day interface with MPI Control Panels. Each keypad connects to the IB2 communication bus. The system keypad enrolls during the control panel's initial power up sequence or, if already operational, cycling power to the control panel. The system keypad is the first keypad that you touch after powering up. Each control panel requires at least one keypad.

The MPI keypads combine a touch screen keypad with a card reader into one housing. They are primarily intended for use where you need a PIN or a card to arm/disarm the intruder alarm system. They are not intended for door control, as they do not contain a door strike relay. However, you could program limited door functions using Controller Rules.

## 5.3.2 Features

- Two control options: Standard user (PIN) code or proximity card reader.
- LCD graphical display and built-in sounder (adjustable volume; different sounds for Fire, Burglary, CO alarms, and troubles).
- Multi-area control.
- View current system and zone status based on the keypad's assigned area.
- Global warming and disarming for all areas.
- Connects to the IB2 bus; enols by sending the serial number and device type information to the control panel.
- Provides a proximity card reader capable of reading up to 40-bit cards (tags) at a distance of 3 cm (1.5 in).

| | |
|---|---|
|  | **Note:** *Cards are programmable through MAXPRO Cloud only .* |

- MIFARE (Classic 32-bit and DESFire 56-bit) card type support.
- Lid and off-wall tamper protection.

## 5.3.3 Operational Commands

- User authorization
- Arm/disarm (set/unset), and reset
- View faults, troubles, and alarms
- Bypass zones
- View and operate other areas

- View activity log
- View zone status
- Run zone walk test, siren test

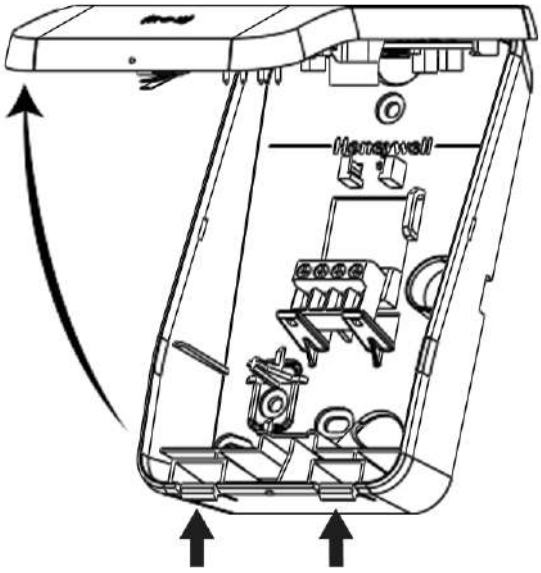
| | |
|---|---|
| | **Note:** *Besides using the keypad, the customer can arm/ disarm the system using the mobile app, via Visual Management in MAXPRO Cloud, or automatically using Schedules in MAXPRO Cloud.*<br>*Usage of mobile app will render the system non-compliant to EN 50131-3.* |

### 5.3.4 Mounting and Wiring

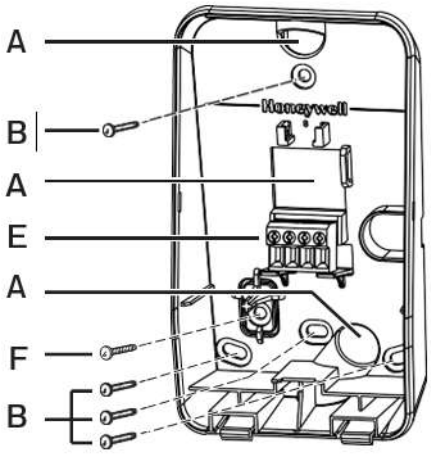
| | |
|---|---|
| | **Note:** *For details on using the optional keypad wall mounting plate, see* *Using the Optional Wall Mounting Plate, page 63.* |

To mount and wire the keypad, proceed as follows:

- Find a flat, vertical surface in a convenient location.
- Separate the back plate from the lid: press the two tabs at the bottom of the keypad, and remove the lid.

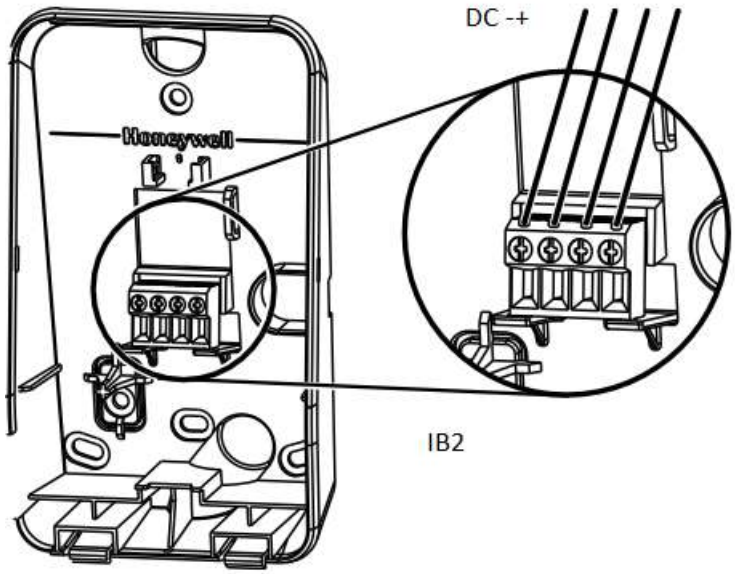


- Place the back plate on the wall at the desired location and mark the position of the mounting holes. There are 4 mounting holes available (B). Use the one at the top, and at the bottom you can use the one in the middle, or the two at the edges, depending on your needs.




| | | | |
|---|---|---|---|
| A | Opening for wiring (x 3) | E | IB2 bus connector |
| B | Mounting screw holes (x 4) | F | Tamper screw (x 1). Required for off-wall tamper protection. |

- Remove the back plate from the wall, and then drill the holes as required.
- Screw the back plate to the wall using the large screws, while running the wiring through the available openings.
- Screw the tamper screw (F) into the wall. This screw provides off-wall tamper protection.



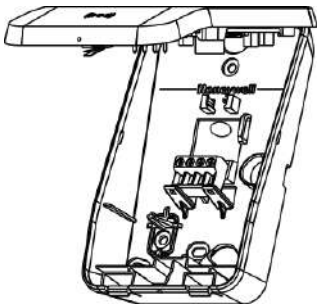
- Connect the keypad to the desired IB2 bus (H, page 29) on the control panel. Wiring from bus to control panel is as follows:

| Keypad terminal | To IB2 bus on Control Panel |
|---|---|
| + | +12V |
| – | – |
| C | C |
| D | D |

| | |
|---|---|
| ⚠ | **Caution: If you are using two CAT5E cables for incoming and outgoing wiring through the narrower wiring openings, the cables may get crushed. This may damage the wiring and cause system malfunctions. In this case, strip off the cables' outer covers so that only the cores are entering the enclosure. As an alternative, you can use (thinner) standard alarm cables for wiring.** |

Use cable ties to bundle and fix wiring, making sure that there is no excess wiring. The PCB holder has various attachments point for this purpose.

Click the lid back in place and fix it using the small lid screw (G).



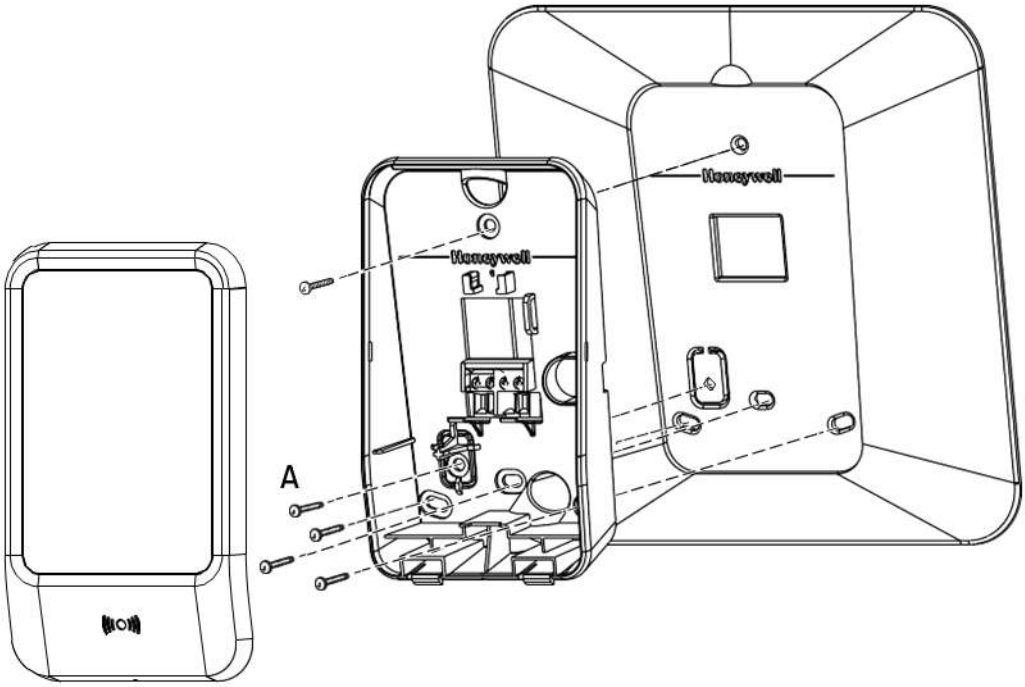
| | |
|---|---|
| ⚠ | **Caution: Make sure to fix the lid using the screw. This will keep the lid firmly in place, providing proper protection to the device.** |

## 5.3.5 Using the Optional Wall Mounting Plate

| |
|---|
| **EN** Usage of wall mounting plate will render the system non-compliant to EN 50131-3. |

The MAXPRO Intrusion Keypad Wall Mounting Plate MPIKW1 is an optional plate that you can mount between the keypad and the wall. You can use this plate, for example, to cover any mounting holes from legacy devices when upgrading an existing system.

The illustration below shows how to mount the keypad when using the optional wall plate: A =




tamper screw. Required for off-wall tamper protection.

## 5.3.6 Programming

| | |
|---|---|
| | **Note:** *The local settings (on the keypad) are limited to LCD brightness and sound level. For details, see the MAXPRO Intrusion User Guide (doc. no. 800-23041-1). All additional keypad settings are configured in MAXPRO Cloud.* |

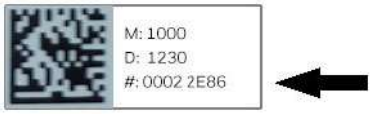
### *Module Assignment*

MAXPRO Cloud will automatically detect IB2 bus devices in Installer Mode. It registers the device with the unique identifier on the label attached to the device.

To register the device in MAXPRO Cloud, proceed as follows:

1. Log into MAXPRO Cloud. Go to the appropriate customer, site, and control panel (= "controller" in MAXPRO Cloud).
2. Switch **CONTROLLER MODE** to Installer to scan for new devices.
3. After scanning, click **VIEW ALL**.

4. In the New Devices list, select the desired device. You can recognise the device by its unique identifier (see the label on the device).




5. Specify the basic settings for the device (Device Name, Areas), and then click Register. The system has automatically filled in the IB2 bus ID and the device's serial number.
6. After registering, fill in the device's Settings tab (and other tabs if applicable) to fully configure the device. Settings that apply to all the keypads connected to the control panel, are available in the Controller settings page. For a summary of settings, see Configuration in MAXPRO Cloud, page 56. For details, see the MAXPRO Cloud online help.
7. After a successful connection, the screen goes to sleep mode. Touch the LCD display to wake up the keypad and log on with a personal user code or ID card.

## 5.3.7 LED Indicators

| LED Colour | Icon | Function |
|---|---|---|
| Green | ✓ | Area is ready to arm: All zones in the keypad's home area are in their normal state; the area is ready for arming. |
| Red | 🛡 | Area armed: The keypad's home area is armed. |
| | | **EN** To comply with EN 50131 standards, the red Area armed LED is disabled in Europe. |
| Green | ○ | Power: Power is present. |

**EN** For systems compliant with EN 50131, the keypad shall not display any details about the system state until a user has logged on to the keypad.

There is an option in MPC to control this behavior, for all keypads attached to the control panel. In the control panel's Settings screen, make sure that the option Show Alert Details on Arming Station Sleep Screen is set to Disabled. (This is the default setting.) If the site has multiple control panels, check the setting for each control panel.

If you enable the option, the keypad will display the event details (area and zone name) on the sleep screen.

***Note:*** *The keypad will indicate a warning message when the connection to the control panel is lost ("Keypad not connected").*
*Icon indications are not visible if the LED is not lit.*

## 5.3.8 PIN Codes

For the first panel registered with MAXPRO Cloud (MPC) under a customer, the MPC will automatically generate and configure the random installer PIN code and master PIN code to the panel. All the subsequent registered panels under same customer gets downloaded with the same already generated random PIN codes. Without MPC connection, if the panel is powered on, then for the first time using the arming station the user can configure the temporary installer PIN which will be overridden post registration with MPC.

If you login as customer admin, MPC provides the option to modify the master code at the customer level in MPC. The MPC will automatically download the modified PIN codes to all

the control panels under that customer. If you login as dealer admin, you can modify Installer code.

| | |
|---|---|
|  | **Caution: The default PIN length is 6 digits. However, you can set the PIN length between 4 and 6 digits. 6-digit PIN codes must be used for EN 50131-1 compliant installations and that failure to do so will render the system non-compliant.** |

### 5.3.9 Using the Keypad

This section describes the actions that only installers can perform on the keypad. For the actions that are available to end users (customers), see the *MAXPRO Intrusion User Guide* (doc. no. 800-23041-1).

### 5.3.10 Installer Access to the Keypad

You, as an installer, cannot log on to the keypad until the customer has granted you access. If you need access to different keypads, the customer has to grant you access on each keypad individually

| | |
|---|---|
|  | ***Note:*** *After restarting the panel, the installer access on the keypad is automatically blocked again. Logging on to a keypad automatically disarms the keypad's home area. Installers can only disarm areas if they armed the areas themselves. So if the home area of the keypad is armed, then installers can only log on to the keypad if they have armed that area themselves. If someone else has armed the area, then the system will deny installer access to the keypad.* |

To log on to the keypad:

- Using a PIN code:
  - Tap the screen to wake.
  - Tap again to display the pin pad.
  - Type your PIN code.
- Using a card: swipe the card along the bottom of the keypad.
  - If there is no activity on the keypad for 30 seconds, the system will log out the user automatically.

### 5.3.11 Network Settings

If you experience any issues, you can check the network settings using the keypad. Proceed as follows:

- Tap **Menu > Installer tools**

Enables you to tap and choose between Network Settings and/or NTP Settings.

- Tap **Menu > Installer tools > Network settings**.

If connection is OK, it will show green tick marks with the Internet connection check and MPC registration check messages.

If not, tap Enter Manual Mode to enter Manual mode. Tap Next to scroll through the screens and view or edit the current network settings.

- Tap **Menu > Installer tools > NTP Settings**.

| | |
|---|---|
|  | ***Note:*** *Both primary and secondary server are URL and not IP addresses.* |

-**Primary NTP**: By default, NTP server primary URL is set to **pool.ntp.org**.

| | |
|---|---|
|  | ***Note:*** *It is mandatory for the Installer to provide the primary URL and not to leave the field empty.* |

**Secondary NTP**: By default, NTP server secondary URL is set to **time.honeywell.com**.

If desired, you can now edit the NTP URL configuration via AMS (Keypad) to enable connection to locally hosted NTP server.

| | |
|---|---|
|  | ***Note:*** *Usage of incorrect URL is not monitored by Honeywell. Ensure to provide the correct URL for seamless usage of NTP settings.* |

## 5.3.12 Factory Default

You can use the factory default function on the keypad to delete the control panel configuration and reset all values to the factory settings. This will also delete all keypad users, except the default Installer and Master user.

If you want to remove a control panel from an installation, or decommission it, you must execute this function on the keypad before you delete the control panel from MAXPRO Cloud. For details, see Decommissioning a Control Panel after Resetting to Defaults, page 68. You can also use factory defaulting to try and resolve issues with the control panel, for example if the configuration is corrupted. In this case, you can reset the control panel configuration to default values using the keypad, and then use MAXPRO Cloud to restore the control panel's configuration. For details, see *Restoring the* Restoring the Panel's Configuration after Resetting to Defaults, page 69

To reset the control panel to factory defaults, proceed as follows:

1. Tap **Menu > Factory default**. A warning appears on the keypad screen.
2. Proceed as follows:
   - Tap **Continue** to confirm.
   - Tap **Back** to cancel. The system resets the control panel's settings and restarts the panel. Control panel's settings and restarts the panel.

### *Decommissioning a Control Panel after Resetting to Defaults*

Before decommissioning or uninstalling a control panel, make sure to execute the factory default function on the keypad to clear all data in the control panel before removing it.

| | |
|---|---|
|  | **Caution: When you delete a control panel, the system also deletes all devices, areas, and zones associated with the control panel. It also disassociates (but does not delete) the Schedules, Permission Groups, and People associated with the control panel.** |

To further decommission a control panel after resetting to factory defaults, proceed as follows:

1. Shut down the panel using the SHUTDOWN button. For detailed instructions, see Shutting Down the Panel Securely, page 121.
2. In MAXPRO Cloud, go to the appropriate customer and site, and then click Controllers to see the list of control panels.
3. Select the desired control panel, and then click the **Delete** button. The system displays a warning screen indicating the implications of deleting the control panel.
4. Select all check boxes, and then click **CONFIRM**.

| | |
|---|---|
|  | **Caution: You must physically destroy any decommissioned and faulty (unusable or permanently damaged) MPI control panel hardware.** |

### *Restoring the Panel's Configuration after Resetting to Defaults*

If you reset a control panel to the factory defaults via the keypad, MAXPRO Cloud keeps a backup of the configuration in the cloud. If the configuration on the control panel would become corrupt, you can reset the control panel to the factory defaults, and then restore its configuration using MAXPRO Cloud.

To restore the control panel's configuration after resetting to factory defaults, proceed as follows:

1. Log on to MAXPRO Cloud as a user with role Installer, and open the control panel's Settings page.
2. Click the **Edit** button, and then, under Advanced Settings, click the **REDOWNLOAD CONFIG** button.
3. Click **Yes** to confirm. The system will switch the panel to Installer mode and restore the configuration to the panel. You can check if restoring is finished on the control panel's Overview page: CONFIGURATION SYNC STATUS will display Up to Date.

# 5.4. MPI Door Control Module MPIDC1

## 5.4.1 About the MPI Door Control Module

The MAXPRO Intrusion Door Control Module (DCM) is a single door access control module and connects to an MPI Control Panel. It provides access and egress to the protected premises. Adding more than one DCM increases the number of access points and each communicates with an MPI Control Panel via the IB2 communication bus. The module may be mounted remotely in its own enclosure, or together with an MPI Remote Power Supply in a cabinet.

## 5.4.2 Features

Access control:

- Compatible with two Wiegand readers
- One programmable 12 VDC relay for door lock
- Selectable entry (access) vs. exit (egress) reader[1]
- Outputs to control reader, reader buzzer, and up to three reader LEDs.
- Supports up to the last 500 cards in reduced capability mode. Intrusion:

1. Exit reader will be available soon.

   – Door is usable as entry/exit door as part of the intrusion protection, using the door status monitor input. Only one magnetic contact required for access and intrusion functionality.

Tamper protection:

- Lid and off-wall tamper protection.
- Bypass able through MAXPRO Cloud.
- Tampers for both readers. Card formats, Wiegand:
- HID cards: 26, 32, 34, 35, and 48 bit.
- MIFARE cards: Classic 32-bit, MIFARE DESFire EV2 38-bit, and 56-bit.
- EM4102 cards 26, 40 bit.

### 5.4.3 Inputs and Outputs

Inputs:

- Input wiring is configurable.
- Door Status Monitor (DSM): input for door contact. For access monitoring and intrusion alarms. Can be used as an entry/exit zone for intrusion protection. In this case:
- When the area is disarmed, the DSM will work as a standard DSM; for example, causing a door forced alarm if the door is opened illegally.
- When arming/disarming, the DSM will follow the entry/exit route rules.
- Request to Exit (RTE): request to exit button.

Outputs:

- Door Strike/Lock: relay dedicated for the door lock.
- Selectable 12 VDC feed for the relay NC/NO contact using a jumper. In this case, the circuit current is limited to 1.5 A. For details, see *Relay Jumper*, page 74.
- LED R: controls the reader red LED (door blocked, e.g. area is armed)
- LED Y: controls the reader yellow LED
- LED G: controls the reader green LED
- BUZZ: controls the reader buzzer.
- The buzzer output provides audible notifications for the following events:
- Card presented: Short beep for .1 seconds.
- Valid card (ID) presented: Door unlocked will present one long beep for one second.
- Command rejected (request for access or request to arm): three short beeps.
- Door Forced or Door Held: continuous tone until door is closed or event is cancelled.

### 5.4.4 Mounting

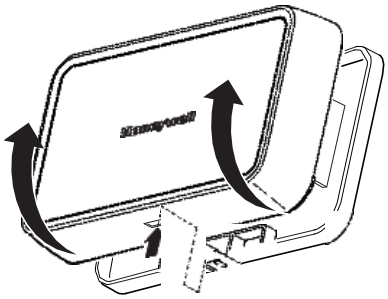
You can install the Door Control Module against a wall in its own enclosure, or you can install up to two Door Control Modules in a cabinet, next to and/or stacked on top of an MPI Remote Power Supply.

The procedure below is for mounting the device on the wall in its own enclosure. For installing in a cabinet, see *Cabinet Mounting with Control Panel or Remote Power Supply*, page 102.

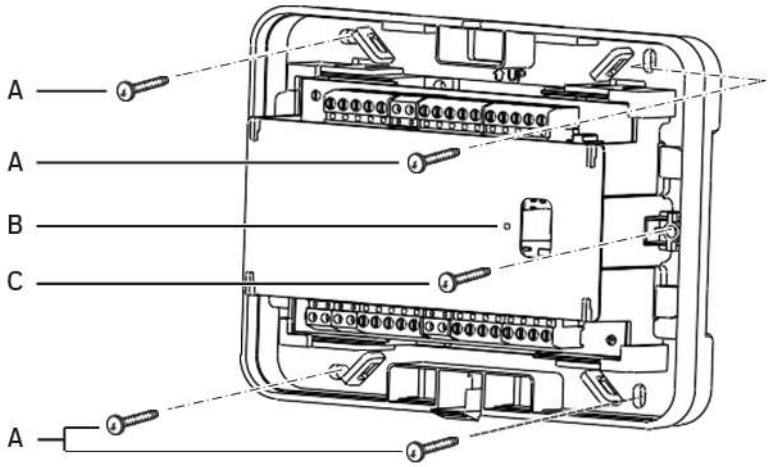
| | |
|---|---|
| | **Note:** *The Door Control Module is only suitable for mounting in a cabinet with an MPI Remote Power Supply, not with an MPI Control Panel.* |

To mount the device on the wall in its own enclosure, proceed as follows:

1. Press the tab at the bottom of the lid and remove the lid.



2. Fix the device to the wall using the 4 large screws ( A).



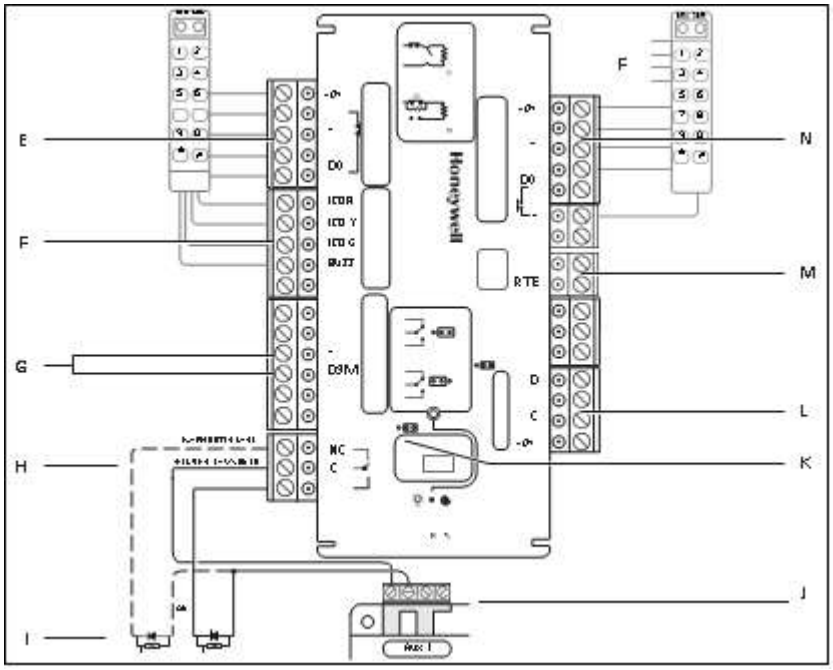

| | | | |
|---|---|---|---|
| A | Mounting screw (x 4) | C | Tamper screw (x 1). Required for off-wall tamper protection. |
| B | LED indicator | | |

3. Screw the tamper screw (C) into the wall. This screw provides off-wall tamper protection.
4. For wiring, see Summary of Connections, page 81.
5. Use cable ties to bundle and fix wiring, making sure that there is no excess wiring. The PCB holder has various attachments point for this purpose.

6. Click the lid back in place and fix it using the small lid screw (D).

| | |
|---|---|
| ⚠ | **Caution: Make sure to fix the lid using the screw. This will keep the lid firmly in place, providing proper protection to the device.** |

## 5.4.5 Summary of Connections




| # | Item | Terminal or connector | Connect to |
|---|---|---|---|
| E | ENTRY<br>Reader (Reader 1) | +12V | Entry reader power input [+]. |
| | | – | Entry reader input [–] for power and tamper |
| | | D0 | Entry reader data 0 |
| | | D1 | Entry reader data 1 |
| | | T | Entry reader tamper. |

| | | | |
|---|---|---|---|
| F | Triggers | LED R | Entry reader red LED. If used: exit reader red LED. |
| | | LED Y | Entry reader yellow LED. If used: exit reader yellow LED. |
| | | LED G | Entry reader green LED. If used: exit reader green LED. |
| | | BUZZ | Entry reader buzzer. If used: exit reader buzzer. |
| | | – | Reader LEDs and buzzer [–] terminal. |

| | | | |
|---|---|---|---|
| G | Door status monitor | – | Door status monitor [–] terminal. |
| | | DSM | Door status monitor. |
| | | Default supervision: triple balanced. For details and more options, see Wiring Inputs (Zones), page 39. Terminate using resistors if not used.<br>Can be used as an entry/exit zone for intrusion protection. | |
| H | Door Strike/Lock (relay) | NC | Normal Closed terminal |
| | | C | Common terminal |
| | | NO | Normal Open terminal |
| | | For door lock only: magnetic lock OR door strike. | |
| I | Transient protection for magnetic lock or door strike | | |
| J | Auxiliary power supply for door strike/lock relay. | | |
| K | Jumper | Jumper for door strike/lock relay: 12 VDC feed for the relay NC/NO contact if jumper is positioned over pins 1 and 2. For details, see further below. | |
| L | IB2 BUS | +12V | 12 VDC supply terminal |
| | | – | 0 VDC supply terminal |
| | | C | IB2 bus C |
| | | D | IB2 bus D |
| M | Request to exit (RTE), optional | RTE | To request to exit button |
| | | – | To request to exit button [–] terminal. |
| | | Default supervision: triple balanced. For details and more options, see Wiring Inputs (Zones), page 39. Terminate using resistors if not used. | |

| | | | |
|---|---|---|---|
| N | EXIT Reader (Reader 2), optional | +12V | Exit reader power input [+]. |
| | | – | Exit reader power input [–] |
| | | D0 | Exit reader data 0 |
| | | D1 | Exit reader data 1 |
| | | T | Exit reader tamper. |
| | | – | Exit reader tamper [–] |

| | |
|---|---|
| ⚠ | **Caution: Do not use any terminals that are labeled NOT USED.** |

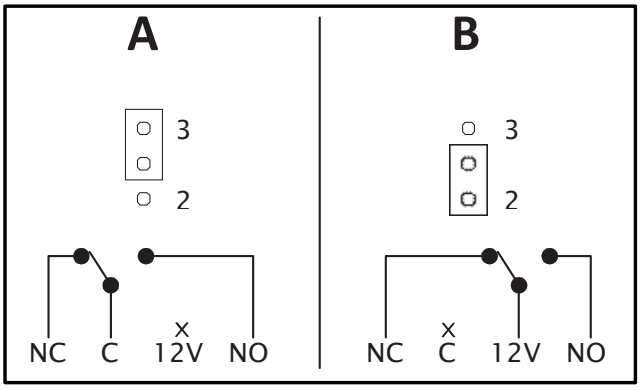
### *Minimum Connections*

The DCM simply needs wiring to the IB2 data bus, and the following minimum connections:

- Attach a Wiegand reader to the ENTRY Reader terminals.
- Attach the door lock to the Door Strike/Lock terminals.
- Attach a request to exit button to the RTE terminals.
- Attach a door contact to the DSM terminals.

Optionally, you can connect the reader buzzer and red LED control lines to the appropriate terminals on the DCM to give extra feedback.

### *Relay Jumper*

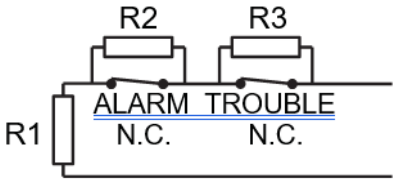



- A: jumper in position 2–3 (default). Normal relay operation ('dry contact')
- B: jumper in position 1–2. Feeds 12 V to the NC/NO terminals of the relay ('wet contact'). Note that the relay's common pin C is open in this case. When using this configuration, the current is limited to 1.5 A.

**Tip**: when using option B, use an MPI Remote Power Supply MPIPSU35 to provide additional current to the module.

### 5.4.6 Default Zone Configurations

For the Door Status Monitor and the Request to Exit button, triple balanced is the default zone supervision setting (R1 = R2 = 1K; R3 = 3K; resistor packs included). For details, see *Triple Balanced*, page 42.




For more information on the zone supervision settings, see *Zone Wiring Types*, page 39.

### 5.4.7 Programming

MAXPRO Cloud will automatically detect IB2 bus devices in Installer Mode. It registers the device with the unique identifier on the label attached to the device.

To register the device in MAXPRO Cloud, proceed as follows:

1. Log into MAXPRO Cloud. Go to the appropriate customer, site, and control panel (= "controller" in MAXPRO Cloud).
2. Switch CONTROLLER MODE to Installer to scan for new devices.
3. After scanning, click VIEW ALL.
4. In the New Devices list, select the desired device. You can recognize the device by its unique identifier (see the label on the device).


5. Specify the basic settings for the device (Device Name...), and then click Register. The system has automatically filled in the IB2 bus ID and the device's serial number.
6. After registering, fill in the device's Settings tab (and other tabs if applicable) to fully configure the device. For a summary of settings, see *Configuration in MAXPRO Cloud*, page 56. For details, see the MAXPRO Cloud online help.

## 5.4.8 LED Indicators

| LED Colour | Indication | Function |
|---|---|---|
| Green | Steady blink (0.1s on, 0.9s off) | Power and IB2 communication good |
| Red | Steady | Powered but not communicating on IB2 |
| – | Off | No power or communication |

## 5.4.9 Using luminAXS Readers with the DCM

### *Features*

The MPI Door Control Module is compatible with the Honeywell luminAXS readers. The following functionality is available:

- Access and intrusion (arm/disarm) functions.
- Buzzer and status LEDs (green, yellow, red).
- Light ring indications:
- Standby mode: blue.
- Entering access mode (area disarmed): colour switches briefly to green, then goes back to standby mode.
- Entering intrusion mode (area armed): colour switches briefly to yellow, then goes back to standby mode.
- Upon reading card: colour switches briefly to white.
- Cards, key fobs, and PIN code.

### *Operation*

Access

- In access mode (area is disarmed), you can unlock the door via card swipe or PIN code. Upon reading the card, the reader will beep and the light ring changes briefly to white.
- If access is allowed, the ring light changes briefly to green, and the green status LED will light up.
- If access is denied, the ring light changes briefly to red, and the red status LED will light up.

Intrusion

- If authorized, you can arm and disarm the area behind the door via card swipe.

To arm:

- You can triple swipe the card.
- On reader models with lock/unlock keys, you press the lock key and then swipe your card.

The reader will beep, and the ring light will briefly change to white upon reading the card. During the exit delay, the yellow status LED will light up, and the ring light changes to yellow. The system will unlock the door, allowing you to leave the area. Upon arming, the reader will beep twice.

If the system cannot arm the area, the reader will beep three times, the red status LED will light up, and the ring light changes to red.

To disarm:

- You can swipe your card.
- On reader models with lock/unlock keys, you press the unlock key and then swipe your card.

If you are authorized to disarm the area, the system will disarm the area and unlock the door. The yellow status LED will briefly light up, and the ring light briefly changes to yellow, then goes to standby mode.

If you are not authorized to disarm the area, the system will keep the area armed and the door locked. The reader will beep three times, the red status LED will light up, and the ring light changes to red.

When using luminAXS readers with MAXPRO Intrusion, take the following into account:

- On the 16-key model: the F, I, x, and v keys are not functional.

When using PIN codes: you do not need to confirm the PIN code by pressing the v key on the reader. The system decides when to validate the PIN code using the PIN length (set in MAXPRO Cloud). For example, if the PIN length is set to 4 digits, the system will validate after you have typed 4 digits.

- You cannot use PIN codes for arming/disarming, only cards.
- If the area behind the door is armed, the system will not allow access (unlock the door). You must disarm the area first.

### *Cards*

For usage with MPI, use MIFARE DESFire EV2 cards and key fobs (recommended LuminAXS 38-bit preprogrammed with diversified key encryption). In MAXPRO Cloud, set the DCM card type to LuminAXS 38-Bit Desfire.

| | |
|---|---|
|  | ***Note:*** *You can use the MIFARE DESFire EV2 cards and key fobs also with the MPIKTSMF keypad. The cards are not compatible with the MPIKTSPRX keypad.* |

You add cards to the system via MAXPRO Cloud (People).

### *Connections*

For mounting the luminAXS readers, see the luminAXS installation guide. The table below indicates how to wire the luminAXS readers to the DCM.

| DCM | | luminAXS reader | | |
|---|---|---|---|---|
| Entry reader | +12V | Entry reader | +U_b | Red wire |
| Entry reader | – | Entry reader | 0 V / GND | Black wire |
| Entry reader | D0 | Entry reader | Data 0 | Green wire |
| Entry reader | D1 | Entry reader | Data 1 | White wire |
| Entry reader | T | Entry reader | Tamper line | Purple wire |
| Triggers | LED R | Do not connect | | |

| | | | | |
|---|---|---|---|---|
| Triggers | LED Y | Entry or exit reader | Input Intrusion mode | Pink wire |
| Triggers | LED G | Entry + exit reader | Input LED green | Orange wire |
| Triggers | BUZZ | Entry + exit reader | Input Buzzer | Yellow wire |
| Triggers | – | Entry + exit reader | 0 V / GND | |
| Exit reader[1] | +12V | Exit reader | +U_b | Red wire |
| Exit reader | – (power) | Exit reader | 0 V / GND | Black wire |
| Exit reader | D0 | Exit reader | Data 0 | Green wire |
| Exit reader | D1 | Exit reader | Data 1 | White wire |
| Exit reader | T | Exit reader | Tamper line | Purple wire |
| Exit reader | – (tamper) | Exit reader | 0 V / GND | |
| Not supported | | Entry reader | Input hold line | (Blue wire) |

***Note:*** *To drive the luminAXS status LEDs (green, yellow, red), you only need to connect the DCM's LED G (green LED terminal). The luminAXS reader's built-in intelligence takes care of driving all three status LEDs (green, yellow, red) and the ring light.*
*The signal on the Input Intrusion Mode terminal on the luminAXS reader (pink wire) indicates if the area is armed or disarmed, so that the system can correctly allow or deny access to the area.*

# 5.5 MPI Relay Module MPIEOP4

## 5.5.1 About the MPI Relay Module

The MAXPRO Intrusion (MPI) Relay Module provides four additional programmable, unsupervised relays for use with MPI Control Panels. The module may be mounted remotely in its own enclosure, or together with an MPI Control Panel or MPI Remote Power Supply in a cabinet.

## 5.5.2 Features

- Provides four non-supervised relays
- Status LEDs
- Lid and off-wall tamper protection, by passable through MAXPRO Cloud programming.

## 5.5.3 Mounting

You can install the Relay Module against a wall in its own enclosure, or:

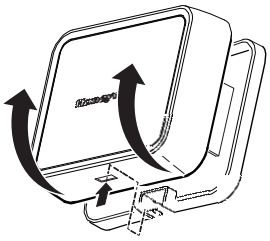
- You can install up to two Relay Modules in a cabinet on top of and/or next to an MPI Remote Power Supply.

- You can install one Relay Module in a cabinet on top of the MPI Control Panel.

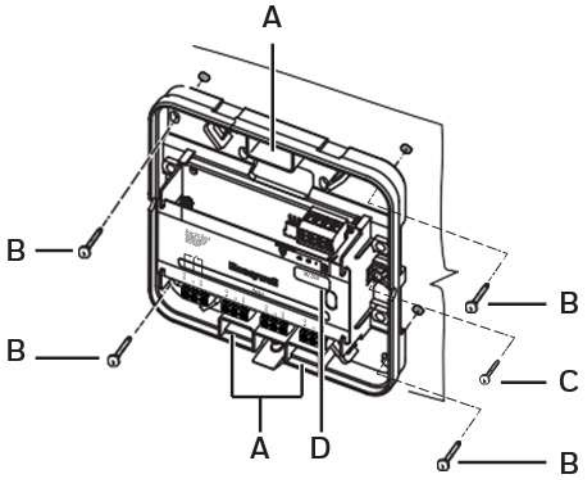
The procedure below is for mounting the device on the wall in its own enclosure. For installing in a cabinet, see *Cabinet Mounting with Control Panel or Remote Power Supply*, page 102.

To mount the device on the wall in its own enclosure, proceed as follows:

Press the tab at the bottom of the lid and remove the lid.



Fix the device to the wall using the 4 large screws (A).



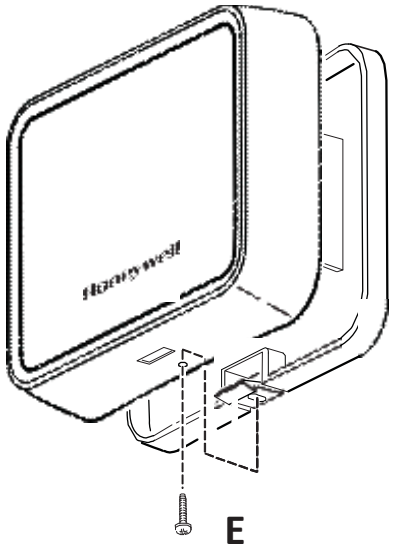

| | | | |
|---|---|---|---|
| A | Opening for wiring (x 3) | D | LED indicator |
| B | Mounting screw (x 4) | E | Lid screw (x 1) |
| C | Tamper screw (x 1). Required for off-wall tamper protection. | | |

Screw the tamper screw (C) into the wall. This screw provides off-wall tamper protection.

For wiring, see *Summary of Connections*, page 72.

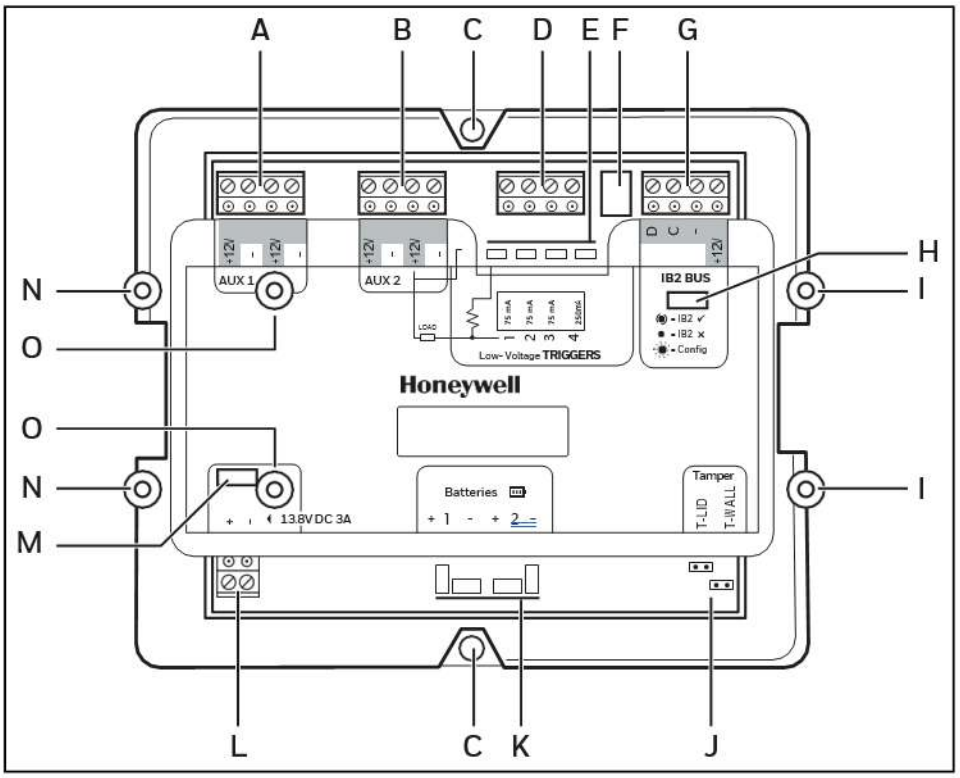
Use cable ties to bundle and fix wiring, making sure that there is no excess wiring. The PCB holder has various attachments point for this purpose.

Click the lid back in place and fix it using the small lid screw (E).




| | |
|---|---|
| ⚠ | **Caution: Make sure to fix the lid using the screw. This will keep the lid firmly in place, providing proper protection to the device.** |

## 5.5.4 Summary of Connections

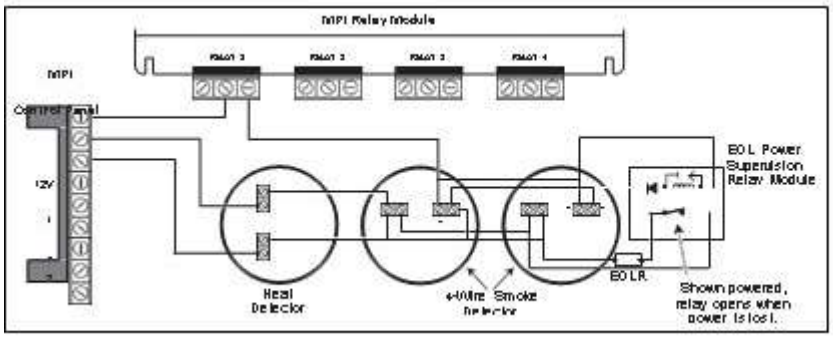



| # | Item | Terminal or connector | Connect to |
|---|---|---|---|
| F | Quick connect plug for IB2 BUS. Can be used if module is stacked on top of Control Panel or Remote Power Supply. | | |
| G | IB2 BUS | +12V | 12 VDC supply terminal |
| | | – | 0 VDC supply terminal |
| | | C | IB2 bus C |
| | | D | IB2 bus D |
| H | Relay 1–4 | NC | Normal Closed terminal |
| | | C | Common terminal |
| | | NO | Normal Open terminal |
| | | Wire the relays between the common C terminal and the normal closed NC or normal open NO terminals. | |

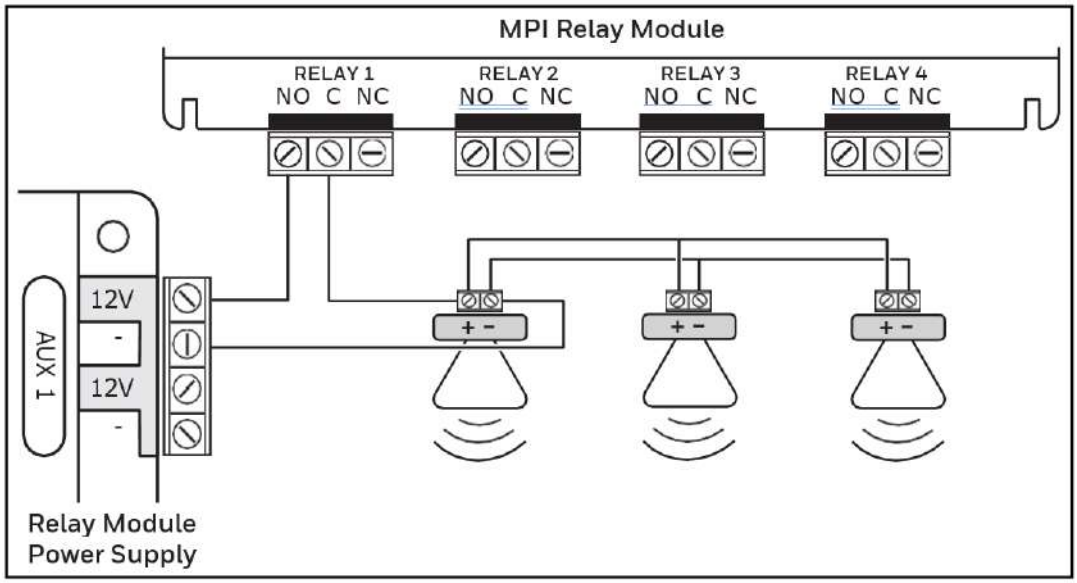
## 5.5.5 Example Functions

### *Relay Function = Smoke Detector Reset*

To use a relay for resetting smoke detectors, wire as follows:




To use a relay for adding additional sirens/sounders, wire as follows:




| | |
|---|---|
| ⚠ | **Caution: The schematic above shows a non-supervised siren configuration. It is not intended for primary notification appliances.** |

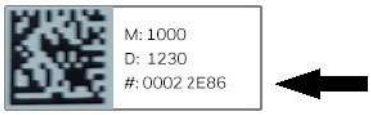
## 5.5.6 Programming

### *Module Assignment*

MAXPRO Cloud will automatically detect IB2 bus devices in Installer Mode. It registers the device with the unique identifier on the label attached to the device.

To register the device in MAXPRO Cloud, proceed as follows:

1. Log into MAXPRO Cloud. Go to the appropriate customer, site, and control panel (= "controller" in MAXPRO Cloud).
2. Switch CONTROLLER MODE to Installer to scan for new devices.
3. After scanning, click VIEW ALL.
4. In the New Devices list, select the desired device. You can recognize the device by its unique identifier (see the label on the device).




5. Specify the basic settings for the device (Device Name...), and then click Register. The system has automatically filled in the IB2 bus ID and the device's serial number.
6. After registering, fill in the device's Settings tab (and other tabs if applicable) to fully configure the device. For a summary of settings, see *Configuration in MAXPRO Cloud*, page 56. For details, see the MAXPRO Cloud online help.

### *Output Configuration*

You configure the outputs on the Relay Module in the same way as for the Control Panel.

### 5.5.7 LED Indicators

| LED Colour | Indication | Function |
|---|---|---|
| Green | Steady blink (0.1s on, 0.9s off) | Power and IB2 communication good |
| Red | Steady | Powered but not communicating on IB2 |
| – | Off | No power or communication |

## 5.6 MPI Zone Expander MPIEIO84E

### 5.6.1 About the MPI Zone Expander

The MAXPRO Intrusion (MPI) Zone Expander module (MPIEIO84E) provides eight additional hardwired zones for use with MPI Control Panels.

Furthermore, it offers four additional low-voltage trigger outputs. The module may be mounted remotely in its own enclosure, or together with an MPI Control Panel or MPI Remote Power Supply in a cabinet.

### 5.6.2 Features

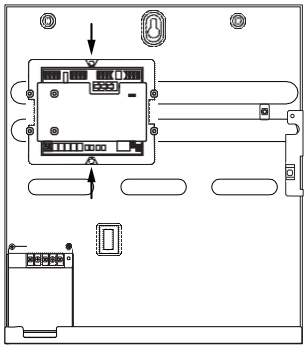
- Provides eight hard-wired zones for burglary and fire inputs. The zones support the following zone wiring types:
  - Supervised EOLR, normal open or normal closed
  - Double Balanced
  - Triple Balanced.
- Provides four programmable low-voltage trigger outputs (i.e. arming LEDs, smoke detector power reset, etc.).

- The outputs switch to ground when activated. For outputs that require a known state (logical 0/1), you can customize the outputs to use a pull-up resistor by fitting jumpers on the outputs.
- Lid and off-wall tamper protection, bypass able through MAXPRO Cloud programming.

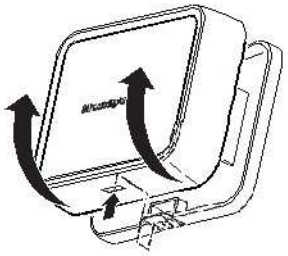
### 5.6.3 Mounting

You can install the Zone Expander against a wall in its own enclosure, or:

- You can install up to two Zone Expander modules in a cabinet on top of and/or next to an MPI Remote Power Supply.



- You can install one in a cabinet on top of the MPI Control Panel.

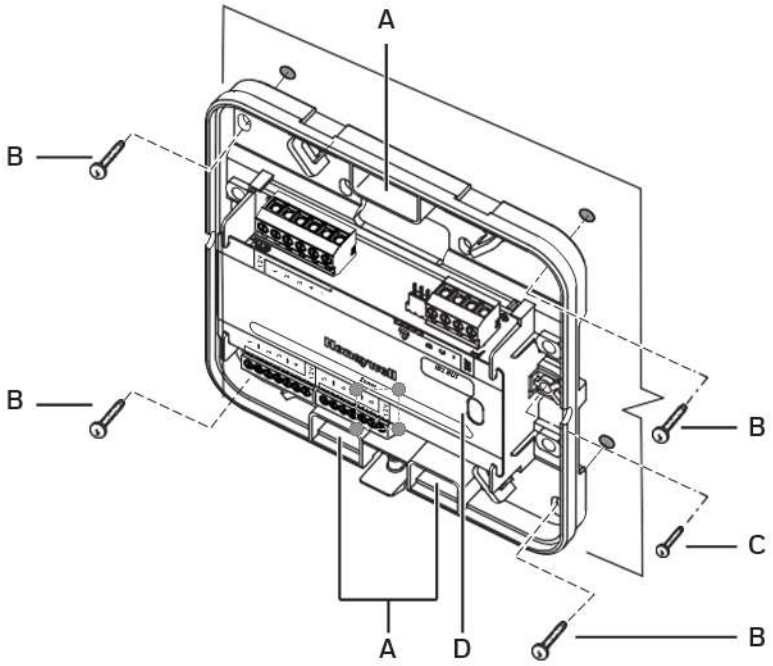


The procedure below is for mounting the device on the wall in its own enclosure. For installing in a cabinet, see *Cabinet Mounting with Control Panel or Remote Power Supply*, page 102.

To mount the device on the wall in its own enclosure, proceed as follows:

- Press the tab at the bottom of the lid and remove the lid.

- Fix the device to the wall using the 4 large screws (B).



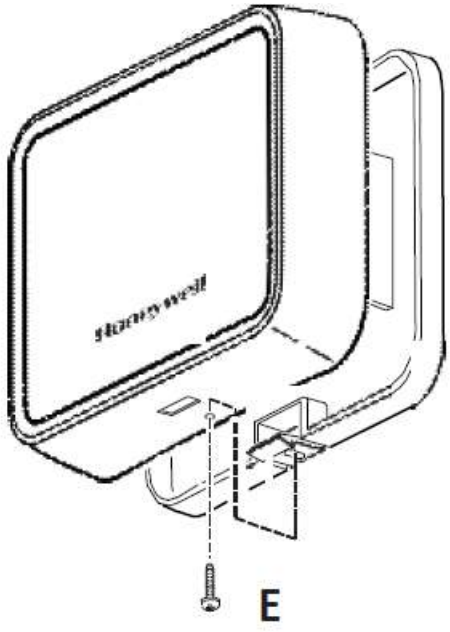

| | | | |
|---|---|---|---|
| A | Opening for wiring (x 3) | C | Tamper screw (x 1). Required for off-wall tamper protection. |
| B | Mounting screw (x 4) | D | LED indicator |

- Screw the tamper screw (C) into the wall. This screw provides off-wall tamper protection.

For wiring, see Summary of Connections, page 72 .

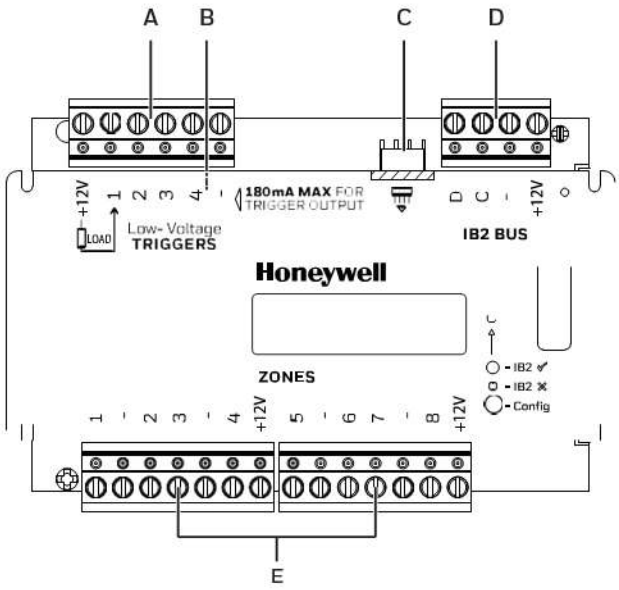
Use cable ties to bundle and fix wiring, making sure that there is no excess wiring. The PCB holder has various attachments point for this purpose.

Click the lid back in place and fix it using the small lid screw (E).




| | |
|---|---|
| ⚠ | **Caution: Make sure to fix the lid using the screw. This will keep the lid firmly in place, providing proper protection to the device.** |

## 5.6.4 Summary of Connections




| # | Item | Terminal or connector | Connect to |
|---|---|---|---|
| A | Triggers (outputs) | +12V 1–4 | Wire the +12V terminal to the output device, and then use one of the trigger terminals 1 to 4 to switch to ground. The outputs will switch to ground when activated. |
| B | Jumpers | For outputs requiring logical state (0/1), fit jumpers on the outputs to use a pull-up resistor. Lift the info card to have access to the jumpers. | |
| C | Quick connect plug for IB2 BUS. Can be used if module is stacked on top of control panel or remote power supply. | | |
| D | IB2 BUS | +12V | 12 VDC supply terminal |
| | | – | 0 VDC supply terminal |
| | | C | IB2 bus C |
| | | D | IB2 bus D |
| E | Zones | +12V | Auxiliary 12 VDC. |
| | | | For zones (sensor contact inputs). Wire between the [–] terminals and the terminals 1–8.<br>Default supervision: triple balanced. For details and more options, see *Wiring Inputs (Zones)*, page 39.<br>Terminate unused zones using resistors. |

## 5.6.5 Wiring the Zones

The zones are suitable for both burglary and fire inputs.

| | |
|---|---|
| ⚠ | **Caution: Make sure to select the appropriate zone wiring type, depending on the zone function (burglary, fire).** |

You wire the zones in the same way as the zones on the Control Panel. For details, see Zone Wiring Types, page 39.

## 5.6.6 Wiring the Trigger Outputs

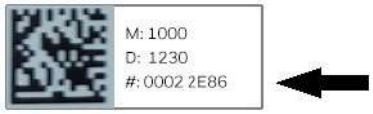
Wire the +12V terminal to the output device, and then use one of the trigger terminals 1 to 4 to switch to ground. The outputs will switch to ground when activated.

Max. current is 180 mA for each trigger. For outputs that require a known state (logical 0/1), you can customize the outputs to use a pull-up resistor by fitting jumpers on the outputs. To reach the jumpers, lift up the info card.

## 5.6.7 Programming

Module Assignment

- MAXPRO Cloud will automatically detect IB2 bus devices in Installer Mode. It registers the device with the unique identifier on the label attached to the device.
- To register the device in MAXPRO Cloud, proceed as follows:
- Log into MAXPRO Cloud. Go to the appropriate customer, site, and control panel (= "controller" in MAXPRO Cloud).
- Switch CONTROLLER MODE to Installer to scan for new devices.
- After scanning, click VIEW ALL.
- In the New Devices list, select the desired device. You can recognize the device by its unique identifier (see the label on the device).




- Specify the basic settings for the device (Device Name...), and then click Register. The system has automatically filled in the IB2 bus ID and the device's serial number.
- After registering, fill in the device's Settings tab (and other tabs if applicable) to fully configure the device. For a summary of settings, see Configuration in MAXPRO Cloud, page 56. For details, see the MAXPRO Cloud online help.

### *Zone and Output Configuration*

You configure the zones and outputs (triggers) on the Zone Expander in the same way as for the Control Panel.

## 5.6.8 LED Indicators

| LED Colour | Indication | Function |
|---|---|---|

| | | |
|---|---|---|
| Green | Steady blink (0.1s on, 0.9s off) | Power and IB2 communication good |
| Red | Steady | Powered but not communicating on IB2 |
| – | Off | No power or communication |

# 5.7 MPI Remote Power Supply MPIPSU35

## 5.7.1 About the MPI Remote Power Supply

The MPI Remote Power Supply is a supplemental smart power supply. In the event the total current draw of all modules connected to the control panel's auxiliary output is exceeded, the Remote Power Supply (RPS) provides additional 12 VDC power outputs to those modules and peripherals requiring additional power (such as door control modules, keypads, motion detectors, glass break detectors, sounders, etc.). Furthermore, it provides four programmable low-voltage trigger outputs.

## 5.7.2 Features

Outputs

- Provides two independents, fully protected monitored 12 VDC power outputs (AUX1, AUX2). Each output supports 1.5 A.
- In the event a short on an output exists, the built-in PTCs isolate the shorted loop from the other outputs.

Backup Batteries

- Supports up to two backup batteries (combined 36 Ah max.).
- Provides battery supervision.
- Automatically detects connected battery(ies), monitors and reports connection status (on power-up or in installer mode); monitors the terminal voltage of each battery independently.
- Disconnects battery when voltage falls below a specific voltage threshold (deep discharge protection).

| | |
|---|---|
|  | **Caution: Replace the battery or batteries according to the manufacturer's specifications and schedule. Dispose of used batteries according to local regulations.** |

### *Control Integration*

Monitors the auxiliary power supply voltages and communicates the status to MAXPRO Cloud.

System Expansion

The cabinet can hold extra modules including the RPS's batteries, and up to two additional devices; one to the right of the RPS and one on top of the RPS holder.

Suitable devices are: Door Control Modules, Zone Expanders, and Relay Modules.

For an example, see About the Cabinet, page 24.

Tamper

Provides two tamper switches (lid and off-wall). You can bypass the tamper switches by fitting a jumper on the required tamper input.

| | |
|---|---|
|  | **Caution: Bypassing the tamper will render the system non-compliant to EN 50131-3.** |

Triggers

Provides four programmable low-voltage trigger outputs.

The outputs switch to ground when activated. For outputs that require a known state (logical 0/1), you can customize the outputs to use a pull-up resistor by fitting jumpers on the outputs.

## 5.7.3 Monitoring/Reporting Options

There is a Diagnostics section for each RPS in MAXPRO Cloud. The system will generate and report the events. The following status information is available on the RPS's Diagnostics tab:

- Incoming power supply voltage.
- Total load current.
- Reports the sum of the AUX1 and AUX2 power output currents.
- Battery charge current.
- Reports the sum of the charge current for both batteries; or charger failure if unable to charge.
- Individual monitoring and reporting for AUX1 and AUX2. Reports output voltage, and circuit protection (fuse) status. The PTCs for each of the AUX outputs serve as automatic resetting fuses.
- Individual monitoring and reporting for each battery.

Each battery is tested and reported individually once every hour. Reports voltage and fuse status.

| | |
|---|---|
|  | ***Note:*** *The PTC on trigger 4 is not monitored. For the position of trigger 4, see Summary of Connections, page 72. The measured values (voltages, currents, resistance values) in the Diagnostics screen are indicative values only and intended for relative comparison purposes. They are not calibrated readings.* |

## 5.7.4 Mounting

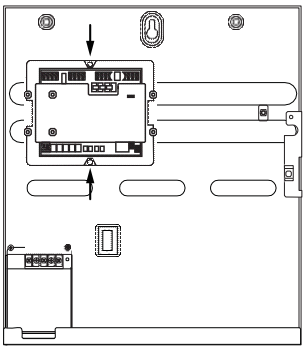
| | |
|---|---|
|  | **Warning: High voltage is present in the cabinet's built-in AC power adapter!** |

### *Installation in the Cabinet*

To mount the RPS in the cabinet, proceed as follows:

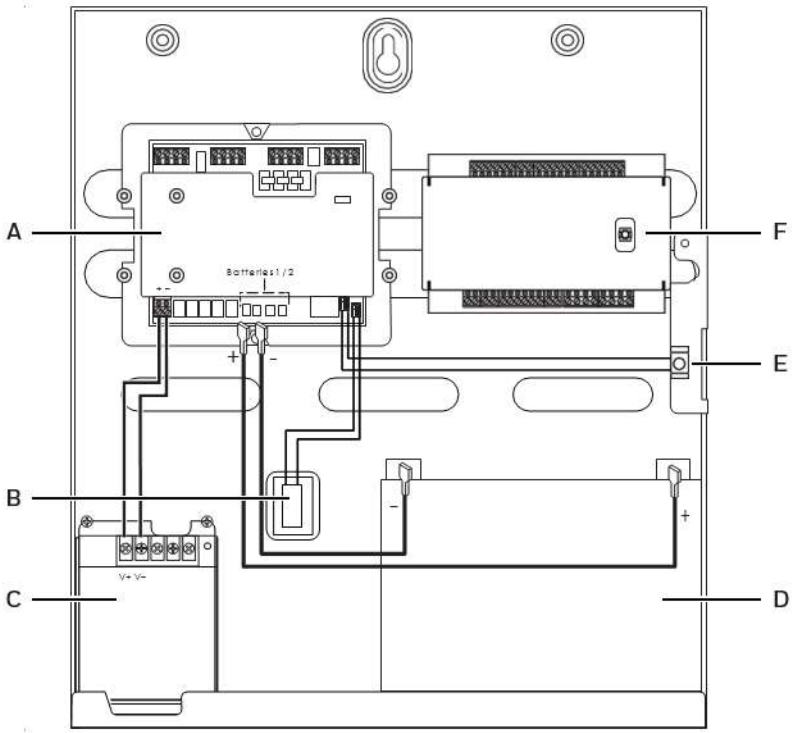
- For instructions on installing the cabinet and wiring the AC power adapter, see Mounting the Cabinet, page 30 and *Wiring the AC Power Supply in the Cabinet*, page 111.
- Position the RPS over the screw holes in the cabinet (O, page 35) and click it into position.

- Secure the RPS to the mounting rails in the cabinet using the 2 screws supplied with the RPS.



Connect the input voltage, cabinet tamper switches, and backup batteries as described below.

| Connection | From | To RPS |
|---|---|---|
| Power | V+ and V– terminals on cabinet's built-in AC power adapter | + and – terminals (13.8VDC) |
| | For detailed instructions on connecting input voltage to the RPS, see *Powering the Main Board*, page 113. | |
| Cabinet tamper switches | Lid tamper switch | T-LID |
| | Wall tamper switch | T-WALL |
| Backup batteries | + and – terminals on backup batteries | + and – terminals Batteries 1 and Batteries 2. |
| | For detailed instructions on installing backup batteries, see Battery Installation, page 117. | |




| | | | |
|---|---|---|---|
| A | Remote Power Supply | D | Backup battery |
| B | Wall tamper switch | E | Lid tamper switch |
| C | Cabinet's built-in AC power adapter | F | Optional:additionalMPI module. For details, see further below. |

**Note:** *The cabinet provides several knockouts for leading wires to/from devices, in the back of the cabinet or at the sides. For details, see Cabinet Parts, page 26.*

Optional: you can install up to 2 extra modules in the cabinet with the RPS:

- One to the right of the RPS (example in illustration further above).
- One on top of the RPS.

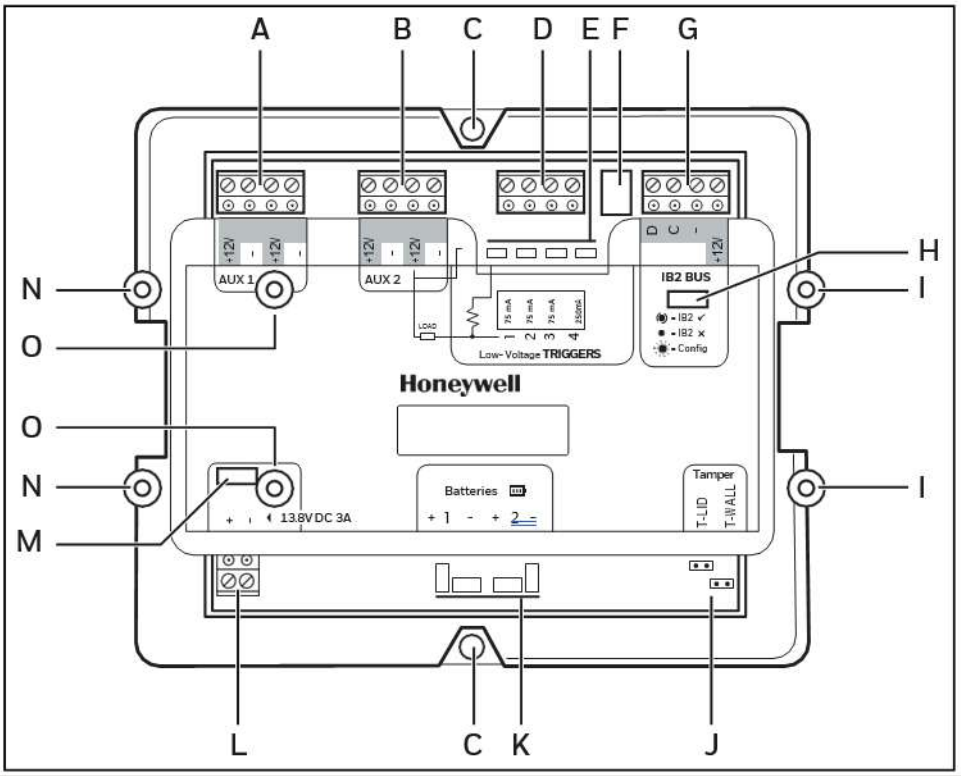
Suitable extra modules are: Door Control Modules, Zone Expanders, and Relay Modules. Before installing extra modules, wire the connections to the RPS first. If you stack another module on top of the RPS, the module will cover the info card indicating the RPS connectors. In this case, fix the RPS spare info card to the inside of the cabinet lid. For details, see Cabinet Mounting with Control Panel or Remote Power Supply, page 102 .

### *Installing Backup Batteries*

For details on determining the required battery capacity and installing the batteries, see *Installing Backup Batteries*, page 93.

## 5.7.5 Summary of Connection

Δ




| # | Item | Terminal or connector | Connect with |
|---|---|---|---|
| A | AUX 1 | +12V | Auxiliary 12 VDC output; connect to the |
| | | – | device that you want to power via auxiliary |
| | | (x 2) | output 1. |
| | | | The board has two sets of terminals on |
| | | | AUX 1. |
| B | AUX 2 | +12V | Auxiliary 12 VDC output; connect to the |
| | | – | device that you want to power via auxiliary |
| | | (x 2) | output 2. |
| | | | The board has two sets of terminals on |
| | | | AUX 2. |

| | | | |
|---|---|---|---|
| C | Screw hole (x 2) | Screw holes for mounting the Remote Power Supply in the cabinet. One at the top, one at the bottom. | |
| D | Triggers (x 4) | 1–4 | For outputs. For details, see Wiring Outputs (Triggers), page 95. |
| E | Jumpers (x 4) | Jumpers for the triggers. | |

| | | | |
|---|---|---|---|
| F | Quick connect plug for IB2 BUS (can be used for module stacked on top of main board; quick connect cable is included). | | |
| G | IB2 BUS | +12V | 12 VDC supply terminal for devices connected to the IB2 bus. |
| | | **Caution:** This output is for keypads and other IB2 bus expansion modules. Do not connect this to the +12V of the control panel or any other power supply. For details, see IB2 Bus Connection, page 95. | |
| | | – | 0 VDC supply terminal for devices connected to the IB2 bus. |
| | | C | IB2 bus C |
| | | D | IB2 bus D |
| H | IB2 bus LED | For details, see IB2 Bus LED Indicators, page 97. | |
| I | Positioning pin (x 2) for stacked MPI module (optional). The top pin has a screw hole for fixing the stacked module. | | |
| J | Tamper | T-LID | Cable from the cabinet's lid tamper switch. |
| | | T-WALL | Cable from the cabinet's wall tamper switch. |
| K | Batteries 1/2 | + | + terminal on backup battery 1/2 |
| | | – | – terminal on backup battery 1/2 |
| | | **Note** : You must install at least one battery. | |
| L | 13.8 VDC | + | Input voltage: V+ terminal on cabinet's built-in AC power adapter |
| | | – | Input voltage: V– terminal on cabinet's built-in AC power adapter |
| M | Power LED indicator | – Green: Power input available on main board.<br>– Off: Power input not available on main board. | |
| N | Positioning pin (x 2) for stacked MPI Door Control Module (optional). The bottom pin has a screw hole for fixing the stacked module. | | |

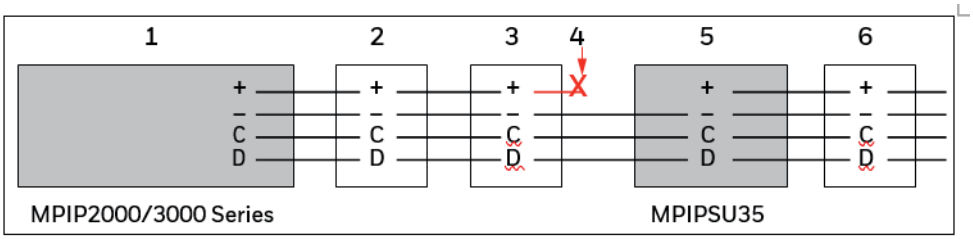
| | |
|---|---|
| O | Positioning pin (x 2) for stacked MPI Zone Expander or MPI Relay Module (optional). The bottom pin has a screw hole for fixing the stacked module. |

| | |
|---|---|
| ⚠ | **Caution: Incorrect wiring of the AC power supply input (13.8 VDC) may cause permanent and irreparable damage to the main board.** |

## 5.7.6 IB2 Bus Connection

To correctly wire the IB2 bus and the devices when using an MPI Remote Power Supply, see the illustration below.

| | |
|---|---|
| ⚠ | **Caution: IB2 Bus +12 VDC output: this output is for keypads and other IB2 bus expansion modules. Do not connect this to the +12V of the control panel or any other power supply.** |




| | | | |
|---|---|---|---|
| 1 | Control Panel | 4 | Do NOT connect incoming +12V to the RPS's IB2 bus! |
| 2 | Device on IB2 bus | 5 | Remote Power Supply |
| 3 | Device on IB2 bus | 6 | Device on IB2 bus after Remote Power Supply |

## 5.7.7 Wiring Outputs (Triggers)

The Remote Power Supply has four programmable low-voltage trigger outputs (D, page 94): for arming LEDs, smoke detector power reset, etc. Wire the AUX +12V terminal to the output device, and then use one of the trigger terminals 1 to 4 to switch to ground. The outputs will switch to ground when activated. The max. currents are:

- 75 mA each for triggers 1–3.

- 250 mA for trigger 4.

| | |
|---|---|
| ⚠ | **Caution: The PTC on trigger 4 is not monitored.** |

For outputs that require a known state (logical 0/1), you can customise the outputs to use a pull-up resistor by fitting jumpers (E, page 94) on the outputs.

You can program the triggers using MAXPRO Cloud. For details, see the *MAXPRO Cloud Configuration Guide* (doc. no. 800-24096-1).

## 5.7.8 Programming

### *Programming Options*

The following options are programmable:

- Triggers (Outputs)
- Options in MAXPRO Cloud: The system automatically assigns an output number to each trigger that you configure. Furthermore, you can specify the Output Name, the Start Trigger and Stop Trigger, additional settings for the pulse stop trigger, Areas, and Output Polarity.
- Hardware options: The outputs switch to ground when activated. For outputs that require a known state (logical 0/1), you can customise the outputs to use a pull-up resistor by fitting jumpers on the outputs.

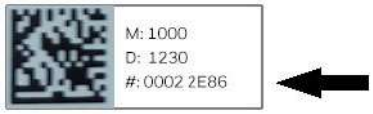
| | |
|---|---|
| 🗒 | ***Note:*** *Trigger programming on the Remote Power Supply is identical as for the triggers on the Control Panel.* |

### *Programming*

MAXPRO Cloud will automatically detect IB2 bus devices in Installer Mode. It registers the device with the unique identifier on the label attached to the device.

To register the device in MAXPRO Cloud, proceed as follows:

1. Log into MAXPRO Cloud. Go to the appropriate customer, site, and control panel (= "controller" in MAXPRO Cloud).
2. Switch CONTROLLER MODE to Installer to scan for new devices. After scanning, click VIEW ALL.
3. In the New Devices list, select the desired device. You can recognise the device by its unique identifier (see the label on the device).




4. Specify the basic settings for the device (Device Name...), and then click Register. The system has automatically filled in the IB2 bus ID and the device's serial number.

5. After registering, fill in the device's Settings tab (and other tabs if applicable) to fully configure the device. For a summary of settings, see Configuration in MAXPRO Cloud, page 56. For details, see the MAXPRO Cloud online help.

| | |
|---|---|
|  | ***Note:*** *In Installer Mode, the system will detect how many batteries are connected, and it will lock the correct number on exiting Installer Mode.* |

### 5.7.9 IB2 Bus LED Indicators

| LED Colour | Indication | Function |
|---|---|---|
| Green | Steady blink (0.1s on, 0.9s off) | Power and IB2 communication good |
| Red | Steady | Powered but not communicating on IB2 |
| – | Off | No power or communication |

#### *Maintenance*

The RPS, batteries, and AC power adapter (in the cabinet) do not contain any user serviceable components. No further calibration checks or adjustments are required.

## 5.8 MPI Transceiver (RF Portal)

### 5.8.1 About MPI Transceiver (RF Portal)

The RF Portal is a wireless transceiver for the Honeywell V2 and Alpha transmitter range. The RF Portal allows the control panel to receive signals from wire-free detectors and radio keyfobs.

One RF Portal will allow the control panel to assign wire-free detectors to detection zones. However, multiple RF Portals can be used to increase coverage.

On an MPI system, a maximum of eight RF Portals can be connected to the IB2 Bus to support up to 192 zones.

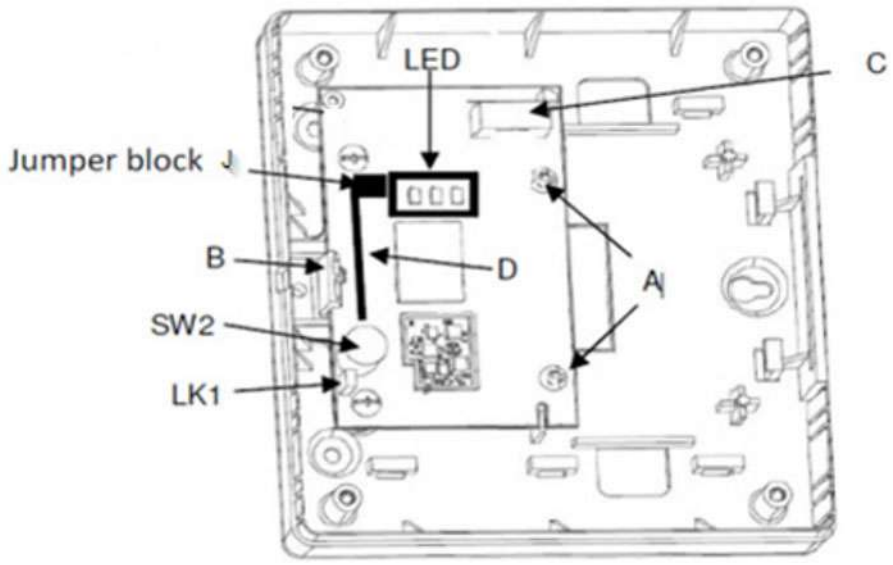
To avoid radio traffic congestion do not exceed 24 wireless sensors per RF Portal. A good guideline is 16 sensors per RF Portal.

| | |
|---|---|
| | **Notes:**<br>• Sensors which can be switched between V2 and Alpha mode should be set for Alpha mode.<br>• RF Portals should NOT be located within 30 cm of the mains cable, control panel, power RIO or any other metal object, consumer units, broadband routers or television sets.<br>• RF Portals should not be located in cellar locations or any other location below ground level as poor reception is likely.<br>• RF Portals should be mounted with the antenna in a VERTICAL orientation for best reception. |

## 5.8.2 Features

### 5.8.2.1 PCB Layout

The following image shows the layout of the PCB in the mounting box.




### 5.8.2.2 Tamper By-pass Link

The Tamper By-pass Link (LK1) must be removed to allow the cover tamper to function through the operation of switch (SW2).

### 5.8.2.3 LEDs

The red BUS LED gives power and communication status of the RF Portal as per the table below

| | |
|---|---|
| 0.1s on / 0.9s off | Good communication |
| 1.5s/on 1.5s off | Not Configured |

| | |
|---|---|
| Slow Flash | Bad communication |
| Off | No Power |

The green RX LED will blink upon receipt of valid signals. If an RF 'jam' condition occurs (continuous interference), the LED will light continuously and will switch off again only when the jam condition clears.

The yellow TX LED is on when the RF Portal is transmitting.

### 5.8.2.4 RF Portal Jumper Settings

To select mode of operation, select the appropriate setting on the Jumper block **(J)**.

| | Open | Closed | Availability |
|---|---|---|---|
| 1 | α1+α2 | α1+V2 | Yes. Protocol Selection |
| 2 | - | Russian | Not Used |
| 3 | Ant1+2 | Ant1 | Not Used |
| 4 | | | Not Used |
| 5 | - | Rx Tool | Refer to section"RAG indicator" below |
| 6 | - | Tx Tool | Refer to section"RAG indicator" below |

### 5.8.2.5 Connecting the RF Portal

Power can be supplied from the control panel power supply or from a remote power supply if the distance causes a large voltage to drop on the cable.

Connect Power to the RF Portal, observing polarity, +ve &-ve on terminal **(C)**.

| # | Item | Terminal or connector | Connect to |
|---|---|---|---|
| H | Quick connect plug for IB2 BUS. Can be used if module is stacked on top of control panel or remote power supply. | | |
| I | IB2 BUS | +12V | 12 VDC supply terminal |
| | | - | 0 VDC supply terminal |
| | | C | IB2 bus C |
| | | D | IB2 bus D |

Keep all cables away from the antenna location **(D)**.

## 5.8.3 Configuring the RF Portal

Refer to the relevant control panel instructions for instructions on registering the RF Portal onto the system.

### 5.8.3.1 Attaching the Cover

Place the cover over the plastic base then firmly attach with the four self-tapping screws provided.

## 5.8.4 Mounting the Plastic Base

Before mounting the base it is recommended that a survey is carried out to determine the suitability of the site for RF installation.

**Notes:**

- The antenna **(D)** must be orientated vertically.
- The plastic base is mounted using three screws. (Note these are not provided with the installation kit).
- The plastic base must be mounted before attaching the PCB as access to the mounting holes will be restricted.

## 5.8.5 Mounting (Refer to PCB Layout image)

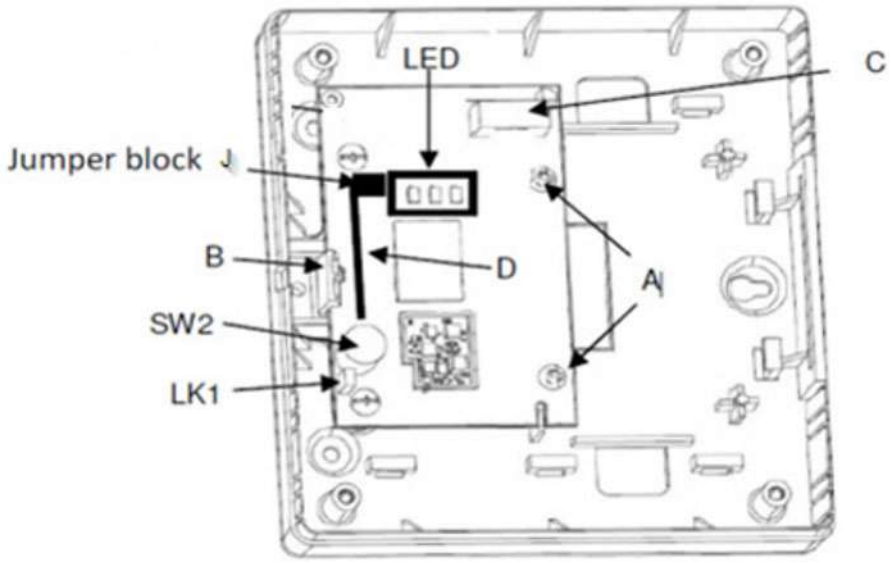
1. Either remove one of the knockouts in the side of the plastic base or in the centre of the base (see doc ref: 800-02456).
2. Fit the two plastic supports for the PCB from the underside of the plastic base **(A)**.
3. Using three screws, attach the plastic base loosely to a wall or electrical mounting box.
4. Bring the cable from the control panel into the base through the relevant knockout hole.
5. Firmly secure the plastic base with the three screws.

## 5.8.6 Attaching the PCB

1. Place the PCB over the two plastic supports and the two pillars **(A)**.
2. Pull back the clip **(B)** then press the PCB firmly into place.
3. To allow the cover tamper switch **(SW2)** to function, remove the by-pass link **(LK1)**.

**Caution:** ***Failure to remove the by-pass link (LK1) will render the system non-compliant*** **to EN 50131-3.**

4. Attach the cover tamper spring over the lid tamper switch **(SW2)**.




## 5.8.7 Signal Strength (RAG indicator)

The RF portal has an inbuilt signal strength indicator, (3 Strengths are indicated - See below). This allows the installer to assess the suitability of location for an RF Portal during the install process.

Descriptions for this and the operational modes are given below.

### 5.8.7.1 Tx Mode

- Ensure mode selection Jumpers 1 to 4 are in the desired configuration.
- Ensure mode selection Jumper 5 is not fitted (open).
- Fit RF portal mode selection Jumper No 6 (closed).
- Repower RF Portal.
- The amber LED will flash every 3 seconds indicating that an RF message has been transmitted.

### 5.8.7.2 Rx Mode

- Ensure mode selection Jumpers 1 to 4 are in the desired configuration.
- Ensure mode selection Jumper 6 is not fitted (open).
- Fit RF portal mode selection Jumper No 5 (closed).
- Repower RF Portal.
- All 3 LEDs will begin to flash in unison. This indicates that there is no signal received.
- When an RF message has been received the LED corresponding to the received signal strength range will flash then settle in the ON state.
- The received signal ranges and their respective LED indications are as follows:
  - Signal level 0-2 = RED
  - Signal level 3-6 = AMBER
  - Signal level 7-10 = GREEN

- If the RF portal does not receive an RF message within 10 seconds all 3 LEDs will go back to flashing in unison.

| | |
|---|---|
| | **Note:** *This product has been tested for compliance by BRE Global Ltd. UK to: EN 50131-3:2009 Grade 2, ACE Type B, Environmental Class II.* |

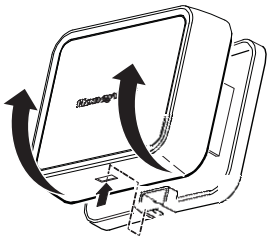
## 5.9 Cabinet Mounting with Control Panel or Remote Power Supply

You can install IB2 modules in a cabinet with a Control Panel or a Remote Power Supply, instead of in their own enclosure. The following options exist:

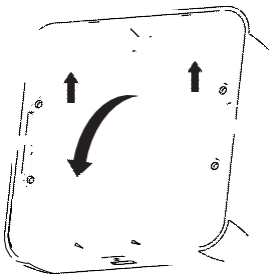
- In a cabinet with a Control Panel: you can install one module on top of the Control Panel. Suitable modules are: Relay Modules and Zone Expanders.
- In a cabinet with a Remote Power Supply: you can install up to two modules; one to the right of the RPS and one on top.
  Suitable modules are: Relay Modules, Zone Expanders, and Door Control Modules.

To mount a module in the cabinet, proceed as follows:

1. Before mounting a module in the cabinet, wire the connections to the panel/RPS main board first.
2. If you stack another module on top, the stacked module will cover the info card indicating the panel/RPS connectors. In this case, fix the panel/RPS spare info card to the inside of the cabinet lid.
3. Press the tab at the bottom of the lid and remove the lid.



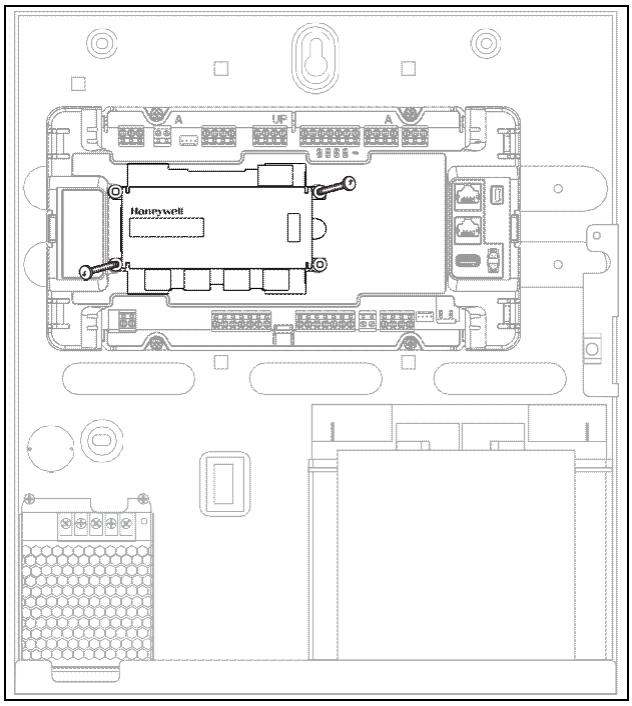
4. Gently remove the module from its enclosure: with the back facing towards you, push the two tabs upwards and then rotate the module towards you.



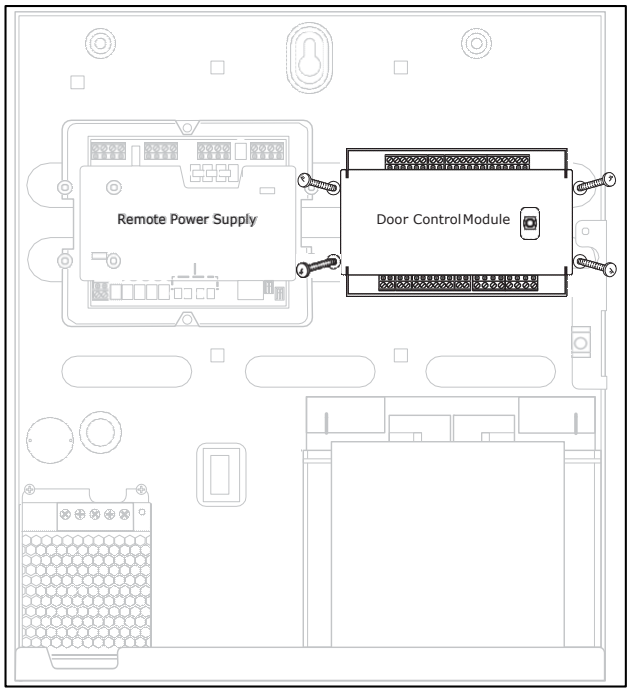
| | |
|---|---|
| | ***Note:*** *You may have to remove the info card before removing the module from its enclosure.* |

5. Mount the module in the cabinet as follows:

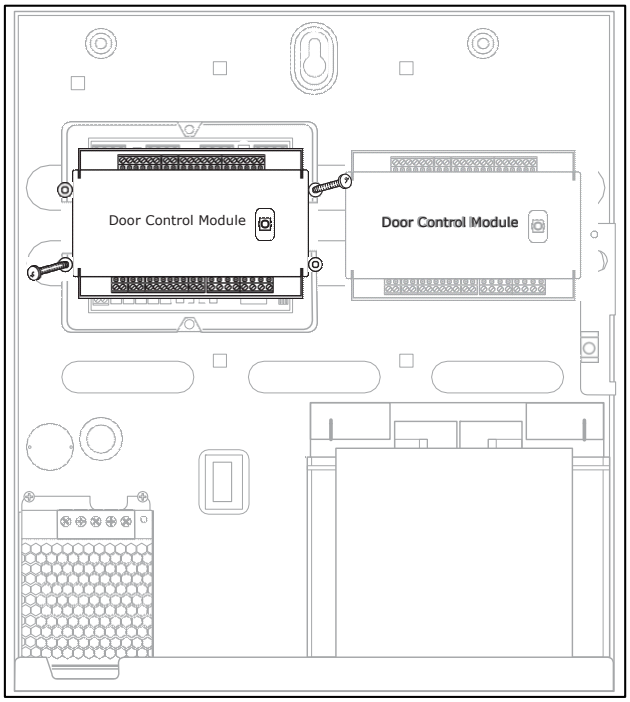
- On top of the Control Panel: fit the module over the positioning pins on the panel, and fix the module using 2 screws (top right, bottom left).



- To the right of the RPS: fix the module to the mounting rails in the cabinet using 4 screws. The example below shows a DCM.




- On top of the RPS: fit the module over the positioning pins on the RPS, and fix using 2 screws (top right, bottom left). The example below shows a DCM.



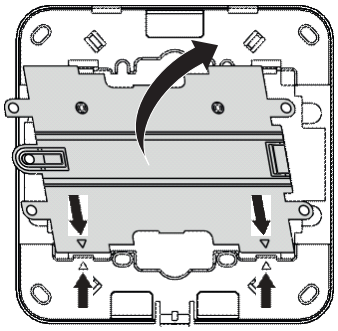

6. Wire the module in the normal way. Tip: you can use a quick connect cable (supplied with the panel or RPS) to connect the module to the IB2 Quick connector

7. If mounting in a cabinet, the module's built-in tamper switches (lid and off-wall) will go into alarm. To prevent this, disable its built-in tampers in MAXPRO Cloud.

| | |
|---|---|
| | **Note:** *If mounting in a cabinet, you do not use the module's tamper screw.* |

Placing a Module Back in its Enclosure To place the module back in its enclosure:

- Align the arrows on the back of the enclosure with the arrows on the back of the module, then rotate the module and click it into place.



CHAPTER

# 6 INSTALLING V-PLEX DEVICES

## 6.1 About V-Plex Devices

For an overview of compatible V-Plex devices, see *Parts List*, page 191.

The V-Plex loop is a multiplex loop (or polling loop) that supports low-current addressable sensors, as well as single, and dual, . The V-Plex loop provides both power and data to the V-Plex devices, and is constantly monitoring the status of all zones enabled on the loop. The maximum current draw of all devices on the V-Plex loop cannot total more than 128 mA.

***Note:*** *V-Plex devices that can be programmed via either DIP switches or the built-in unique serial number must be set for the serial number mode operation. DIP switch zone devices are not supported; the MPI control panel only supports devices in serial mode.*

You must wire all devices on the V-Plex loop in parallel to the [+] and [–] V-Plex loop terminals of the control panel. You can wire the peripherals on the V-Plex loops in a daisy-chain, free star, or spur configuration.

Notes on Wiring

- For new V-Plex loop installations, always use twisted pair wiring. In many cases, you may use existing non-twisted pair wiring, but it is more susceptible to interference from other sources, and may be problematic in installations with long wire runs or in high noise environments.
- Always locate V-Plex loop wiring at least 6 inches (15 cm) away from AC power, telephone, or intercom wiring. The V-Plex loop carries data between the control panel and the devices; interference on this loop can cause an interruption of communication. The V-Plex loop can also cause outgoing interference on the intercom or phone lines. If this spacing cannot be achieved, shielded wire must be used. (Note that the maximum total wire length supported is cut in half when shielded wire is used).
- Recommendation if using parallel wire runs: do not draw more than 64 mA on any individual wire run. This will enhance the reliability of the system.

When Using Multiple Loops (MPIP3000 Series Only)

- When using two V-Plex loops (MPIP3000 series panels only), always connect/configure devices to loop 1 (Vplex BUS 1) first. Do not use loop 2 (Vplex BUS 2) if there are no devices on loop 1.
- Multi-loop V-Plex devices must be kept together on the same loop, either loop 1 (Vplex BUS 1) or loop 2 (Vplex BUS 2). You cannot deploy them across different loops.
- The control panel only supervises loop 1.

Notes on Inputs and Outputs

- V-Plex outputs are always physically part of a V-Plex input device. The output is always associated with the zone number allocated to the input side of the V-Plex device. The system supervises the outputs for connectivity and lid tamper via the zone side of the device.
- You need to define a zone first before you can define an output. To add a zone, you need to enter the device's serial number in MAXPRO Cloud.
- Supported V-Plex outputs are trigger/relay style outputs only.

# 6.2 V-Plex Connections

## 6.2.1 Supervision

- The MPI system supervises the V-Plex polling loop. The system can annunciate a short circuit on the V-Plex loop on the keypads and in MAXPRO Cloud. It will also monitor each of the configured devices for presence.
- If it is a single zone, only that zone will display a trouble condition.
- If the area is armed when a device fails, and the zone is a burglary zone, the system will go into alarm.

| | |
|---|---|
|  | **Note:** *A short or open circuit on the V-Plex loop itself prevents an area from being armed, unless all zones on that loop are bypassed.* |

## 6.2.2 V-Plex Loop Short

The system will indicate the V-Plex loop short when there is a physical short, a low voltage on the loop, or too much current (exceeding 128 mA).

- The panel recognizes a short when the voltage on the V-Plex loop drops to 4.5 VDC or below.
- Isolate this by checking voltage on the V-Plex loop with wires connected and with all wires removed.
  Note that the voltage normally fluctuates between 8.5 and 14 VDC.

## 6.2.3 Limitations of V-Plex Cable Runs

### *Determining the Maximum Wire Length per V-Plex Loop*

To determine the maximum wire length per V-Plex loop, proceed as follows:

1. Use Table 2 <XREF>(further below) for unshielded cable and Table 3 <XREF>for shielded cable.
2. Determine the maximum load of each device, and add them together to determine the maximum wire length from the tables.

*Example*:

The 4190SN requires 2.0 mA. The total load for ten 4190SNs on the same loop would be 20 mA.

3. Locate the row in the table selected in step 1 <XREF>corresponding to the sum of all device currents determined in step 2.<XREF>

*Example*:

A total load current of 20 mA.

4. Determine the maximum wire length from the size, or gauge, of the wire used.

*Example*:

- The maximum wire length of No. 20 AWG wire for a total device load of
- 20 mA is 2,380 meters if you use either unshielded (Table 2)<XREF> or shielded (Table 3)<XREF> wire.
- If you use No. 18 AWG wire instead, the maximum allowable wire length would be 3,657 meters for unshielded cable, and 1,829 meters for shielded wire.

***Table 1 : V-Plex loop wiring distance (metre) using unshielded twisted pair (or non-metal conduit***

| Total Load (mA @ 11.5 VDC) | Wire Gauge | | | |
|---|---|---|---|---|
| | 22 AWG | 20 AWG | 18 AWG | 16 AWG |
| 1–16 | 3,657 | 3,657 | 3,657 | 3,657 |
| 17–24 | 1,478 | 2,380 | 3,657 | 3,657 |
| 25–32 | 1,109 | 1,783 | 2,822 | 3,657 |

| Total Load (mA @ 11.5 VDC) | Wire Gauge | | | |
|---|---|---|---|---|
| | 22 AWG | 20 AWG | 18 AWG | 16 AWG |
| 33–40 | 887 | 1,426 | 2,258 | 3,584 |
| 41–48 | 737 | 1,188 | 1,880 | 2,987 |
| 49–56 | 634 | 1,021 | 1,612 | 2,560 |
| 57–64 | 555 | 893 | 1,411 | 2,240 |
| 65–72 | 494 | 792 | 1,253 | 1,993 |
| 73–80 | 442 | 713 | 1,128 | 1,792 |
| 81–88 | 402 | 649 | 1,027 | 1,630 |
| 89–96 | 369 | 594 | 942 | 1,493 |
| 97–104 | 341 | 548 | 868 | 1,377 |
| 105–112 | 317 | 509 | 808 | 1,280 |
| 113–120 | 295 | 475 | 753 | 1,195 |
| 121–128 | 277 | 445 | 704 | 1,121 |

***Table 2 : V-Plex loop wiring distance (metre) using shielded twisted pair (or metal conduit); one side of the shield to ground***

| Total Load (mA @ 11.5 VDC) | Wire Gauge | | | |
|---|---|---|---|---|
| | 22 AWG | 20 AWG | 18 AWG | 16 AWG |
| 1–16 | 1,829 | 1,829 | 1,829 | 1,829 |

| | | | | |
|---|---|---|---|---|
| 17–24 | 1,478 | 1,829 | 1,829 | 1,829 |
| 25–32 | 1,109 | 1,783 | 1,829 | 1,829 |
| 33–40 | 887 | 1,829 | 1,829 | 1,829 |
| 41–48 | 737 | 1,188 | 1,829 | 1,829 |
| 49–56 | 634 | 1,021 | 1,612 | 1,829 |
| 57–64 | 555 | 893 | 1,411 | 1,829 |
| 65–72 | 494 | 792 | 1,253 | 1,829 |
| 73–80 | 442 | 713 | 1,128 | 1,792 |
| 81–88 | 402 | 649 | 1,027 | 1,630 |
| 89–96 | 369 | 594 | 942 | 1,493 |
| 97–104 | 341 | 548 | 868 | 1,377 |
| 105–112 | 317 | 509 | 808 | 1,280 |
| 113–120 | 295 | 475 | 753 | 1,195 |
| 121–128 | 277 | 445 | 704 | 1,121 |

### 6.2.4 Wiring Notes and Recommendations

- Twisted, stranded, non-shielded cable is recommended. Avoid sharp bends in the wire.
- Shielded cable, running Aux power in the same jacket, and/or running wire in metallic conduit increases the capacitance of the wire run, which limits distances.
- Avoid running the cable near keypad wiring, intercom, or AC power lines, or anything emitting RF noise.
- V-Plex devices that can be programmed via either DIP switches or the built- in unique serial number must be set for the serial number mode operation. DIP switch zone devices are not supported; the MPI control panel only supports devices in serial mode.
- Shielded wire should have one end of the shield to good Earth Ground.

### 6.2.5 Load

The maximum load on one or more V-Plex loops with a single supporting control panel is 128 mA.

CHAPTER

# 7 POWERING THE SYSTEM

## 7.1 Wiring the AC Power Supply in the Cabinet

| | |
|---|---|
|  | **Caution:** ***This product is not suitable for installation, maintenance, or connection by the user. A competent, qualified installer must carry out installation and maintenance .*** |

| | |
|---|---|
|  | **Warning: A means of isolation from the AC power supply must be provided within two meters of the control panel. Where live and neutral supplies can be identified, a fused spur (fused outlet) with a 3 A fuse must be fitted on the live circuit. Where live and neutral circuits cannot be readily identified, 3 A fuses must be fitted on both circuits.**<br>**During installation, make sure the control panel is disconnected from the AC power supply.** |

| | |
|---|---|
|  | ***Note:*** *Upon a total power failure, the control panel will ignore and not transmit alarm or supervisory information for a stabilization period of 120 seconds following restoration of power. Within 60 seconds at the end of the stabilization period, the control panel shall initiate the transmission of a power restoration signal code, if the system supervision report is enabled in MAXPRO Cloud.* |

| | |
|---|---|
|  | ***Caution:*** ***No other connections to the AC power supply terminals are permitted than the ones described in the procedures in this document. All wiring must be in accordance with local regulations.***<br>***Incorrect wiring of the AC power supply may cause permanent and irreparable damage to the main board of the Control Panel or Remote Power Supply. .*** |

The cabinet AC power adapter does not contain any user serviceable components. No further calibration checks or adjustments are required.

| | |
|---|---|
|  | ***Note:*** *You can add up to 2 backup batteries (max. 18 Ah, up to 2 x 9 Ah) in one cabinet. For instructions and further specifications, see* *Installing Backup Batteries, page 93.* |

| | |
|---|---|
|  | ***Note:*** *For 36 Ah battery capacity, you need to install 2 x 18 Ah batteries. You will need a second tamper-protected cabinet to house the second battery. You connect the second battery to the Battery 2 terminals on the control panel in the first cabinet.* |

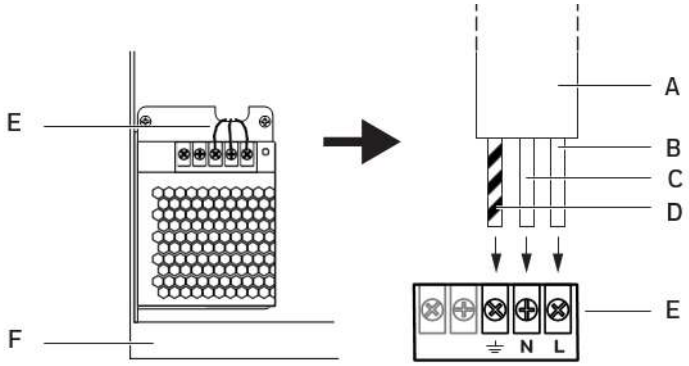
The AC power cable used must be a three-core type (with green/yellow earth insulation) of adequate current carrying capacity. Follow local laws and regulations regarding cable types and length.

To wire the AC power supply to the cabinet's AC power adapter, proceed as follows:

Route the AC power cable from the conduit through a suitable hole in the cabinet walls (back or left-hand side panel).

Wire the AC power cable (A) to the cabinet AC power adapter (E) as follows:

| AC power supply wire | Connect to terminal on AC power adapter |
|---|---|
| Line (B) | L |
| Neutral (C) | N |
| Earth (D) | ⏚ |




| | | | |
|---|---|---|---|
| A | AC power cable | D | Earth wire (typically yellow/green) |
| B | Line wire (typically brown) | E | Cabinet's AC power adapter |
| C | Neutral wire (typically blue) | F | Cabinet |

## 7.2 Powering the Main Board

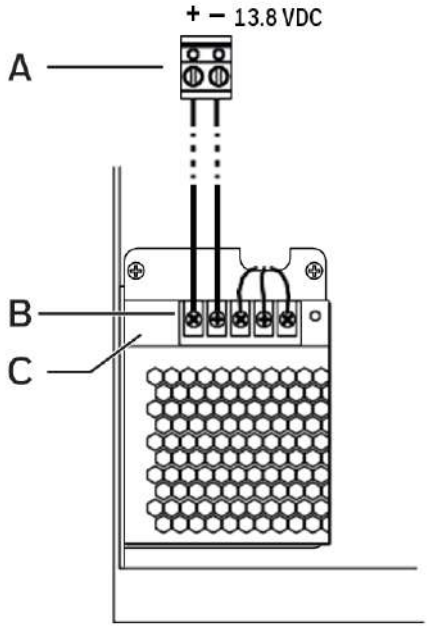
The cabinet's AC power adapter outputs (B, see image below) are pre-wired with red and black leads and a terminal block at the end to connect to the

13.8 VDC input pins (A, see image below) of the main board of the control panel or RPS. Slide the terminal block over the input pins, making sure the connections are as follows:

| From AC power adapter terminal | To main board terminals (13.8 VDC) |
|---|---|
| V– (black lead) | – |
| V+ (red lead) | + |

| | |
|---|---|
| ⚠ | ***Caution: Incorrect wiring of the AC power supply input may cause permanent and irreparable damage to the control panel's main board.*** |

The green LED (C) on the AC power adapter will light up when AC power is present.




.

| | |
|---|---|
| ⚠ | ***Caution:*** ***No other connections to the AC power supply terminals are permitted than the ones described in the procedures in this document. All wiring must be in accordance with local regulations.***<br>***Incorrect wiring of the AC power supply may cause permanent and irreparable damage to the main board of the Control Panel or Remote Power Supply.*** |

## 7.3 Installing Backup Batteries

Each Control Panel and each Remote Power Supply need at least one backup battery to ensure continued operation in case of a power failure. You can install up to 2 backup batteries (max. 18 Ah, up to 2 x 9 Ah) inside one cabinet. You can place the battery or batteries on the bottom of the cabinet, to the right of the built-in AC power adapter.

| | |
|---|---|
| 🗒 | ***Note:*** *For 36 Ah battery capacity, you need to install 2 x 18 Ah batteries. You will need a second tamper-protected cabinet to house the second battery. You connect the second battery to the Battery 2 terminals on the control panel in the first cabinet.* |

The sections below provide instructions for calculating the control panel load, so that you can determine the required battery capacity for your application

## 7.3.1 Determining the Load

### *Maximum Load on Control Panel*

To determine the load on the control panel, add the currents for the following items:

- AUX 1:
  - devices on IB2 bus 1 (if powered by the control panel and not by an extra remote power supply)
  - devices using the AUX1 +12V terminals
  - devices using the auxiliary +12V at the top left of the panel (U, page 36).
- AUX 2: devices on IB2 bus 2 (if powered by the control panel and not by an extra remote power supply).
- AUX 3: the external siren or any other device using the Ext. Siren +12V, and (optionally) the 4G/LTE module.
- V-Plex 1 and V-Plex 2: devices on the V-Plex loops.

### *Maximum Load on Remote Power Supply*

To determine the load on a remote power supply, add the currents for the following items:

- AUX 1 = devices using the auxiliary power on the AUX1 terminals.
- AUX 2 = devices using the auxiliary power on the AUX2 terminals.
- Devices on the IB2 bus.

## 7.3.2 Maximum Current Draw

### *On the Control Panel*

The following table shows the (theoretical) maximum current that may be drawn from each individual output on the control panel:

| Output | Maximum Current Draw |
|---|---|
| Auxiliary 1 (AUX1 +12V, IB2 bus 1, AUX +12V at top left of panel) | MPIP2000E series: 1,500 mA max. / MPIP3000E series: 1,100 mA max. |
| Auxiliary 2 (AUX2 +12V, IB2 bus 2 – MPIP3000 series only) | MPIP3000E series: 1,100 mA max. |
| Auxiliary 3 (Ext. siren, optional 4G/LTE module) | 1,100 mA max. |
| V-Plex 1 | 128 mA |
| V-Plex 2 (MPIP3000 series only) | 128 mA |

### *On the MPI Remote Power Supply*

For the MPI Remote Power Supply, the maximum current that may be drawn from each individual output (AUX1 and AUX2) is 1,500 mA.

## 7.3.3 Determining the Size of the Standby Battery

The total maximum allowed loads on the panel and remote power supply depend on the battery capacity, and the security norm you need to comply with.

The table below lists the advised loads to meet regulations based on using a battery at 100% capacity and allowing for activation of a sounder as per the regulation. Loads need to be adjusted if the battery is at less than 100%. There is no restriction other than the permitted load on capacity of battery used.

For the purposes of calculation, an allowance of 400 mA to activate the sounder has been included, but not the standby current of the sounder. When calculating the total load, remember to include the standby current of the sounder.

### *For the Control Panel*

| Battery Capacity | 7 Ah | 14 Ah | 17/18 Ah | 36 Ah |
|---|---|---|---|---|
| EN 50131 Grade 3; recharge 24 h | – | 210 mA | 350 mA | 950 mA |

| | |
|---|---|
|  | **Note:** *The 36Ah battery must not be used with EN 50131 compliant installations. Doing so will render the Installation non-compliant with the requirements of EN 50131-3.* |

### *For the Remote Power Supply*

| Battery Capacity | 7 Ah | 14 Ah | 17/18 Ah | 36 Ah |
|---|---|---|---|---|
| EN 50131 Grade 3; recharge 24 h | 190 mA | 425 mA | 525 mA | 1150 mA |

| | |
|---|---|
|  | **Note:** *The 36Ah battery must not be used with EN 50131 compliant installations. Doing so will render the Installation non-compliant with the requirements of EN 50131-3.* |

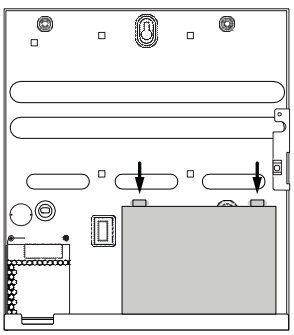
## 7.3.4 Battery Installation

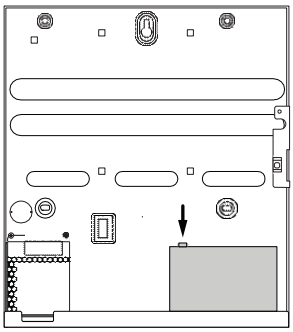
| | |
|---|---|
|  | ***Caution: Position the battery or batteries in the cabinet only as shown in the diagrams. Look carefully at the battery terminals position. This will prevent issues caused by: terminals touching the painted or unpainted metal surface. terminals touching each other even with shrouded connections. terminals touching another part including an adjacent battery.*** |

| | |
|---|---|
|  | ***Caution: You must install and replace batteries according to the manufacturer's specifications and schedule. Install batteries only in well ventilated areas. For safety precautions, maintenance, handling and recycling information, refer to the battery manufacturer's safety data sheet. (For the batteries recommended in this document, please refer to the Yuasa website.) Dispose of used batteries according to local regulations.*** |

Using a Single Battery To install a single battery, proceed as follows:

1. Place the battery horizontally on the bottom of the cabinet. If the battery terminals are both on the same side, position the battery with the terminals on the left-hand side.



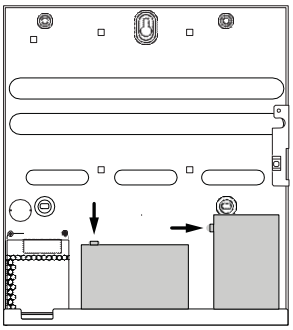


2. Connect the battery to the Batteries 1 terminals. Use the included battery leads.

| From battery terminal | To main board terminal |
|---|---|
| + | Batteries 1 + (red lead) |
| – | Batteries 1 – (black lead) |

Using Two Batteries To install two batteries, proceed as follows:

1. Position one battery horizontally, on the left, with the terminals on the left-hand side.
2. Position the other battery on its side, with the terminals at the top.



3. Connect the batteries to Batteries 1 and Batteries 2 terminals. Use the included battery leads.

| Battery | From battery terminal | To main board terminal |
|---|---|---|
| Battery 1 | + | Batteries 1 + (red lead) |
| | – | Batteries 1 – (black lead) |
| Battery 2 | + | Batteries 2 + (red lead) |
| | – | Batteries 2 – (black lead) |

| | |
|---|---|
| | **Note:** *In MAXPRO Cloud, the Multiple Battery Sensing feature will default to 2 batteries on fresh start-up. In Installer Mode, the system will detect how many batteries are connected, and it will lock the correct number on exiting Installer Mode.*<br>*In MAXPRO Cloud, you can specify the capacity of each installed battery. This allows the system to estimate the maximum runtime on battery if AC power is lost.* |

For systems that require more than 18 Ah battery capacity, you have to install a second tamper-protected cabinet to put a second battery.

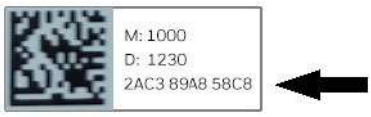
# 7.4 Connecting to MAXPRO Cloud

## 7.4.1 Workflow

After wiring all the devices and attaching power supplies (AC power and batteries) to the system, you will first register the control panel in MAXPRO Cloud, before finally applying power up the system. Make sure that you have connected at least one battery and one keypad.

To register the control panel in MAXPRO Cloud, proceed as follows:

1. On your PC, open your web browser and go to mymaxprocloud.eu/MPC/Signin. If you do not have an account yet, click Sign up to register as a new dealer. Sign in to MAXPRO Cloud after you receive a confirmation email from Honeywell.
2. In MAXPRO Cloud, click the Menu button ☰, and then click Customers.
3. Click Add a customer, and fill in the required data for the customer. In the Customer Name box, enter the name of your MPI customer. In the Site Name box, enter a name for the site where you installed the MPI system.
4. Click the newly created site.
5. Click Add Controller to add the MPI control panel.
6. In the Controller type box, select the exact model of your control panel (MPIP2000E, MPIP2100E, MPIP3000E, MPIP3100E). You can find the exact model name on the sticker on the panel's box, and on the sticker on the panel's plastic mounting bracket.
7. In the MAC ID box, type the control panel's MAC address. You can find the MAC address on the label on the control panel. Type the MAC address without spaces or special characters, for example 2AC389A858C8.




8. In the Time zone box, select the time zone for the control panel.

| | |
|---|---|
| | ***Caution:*** ***Make sure that you select the correct time zone. If not, MAXPRO Cloud will not be able to connect to the control panel.*** |

9. Click ADD CONTROLLER.
10. Once you have added the control panel in MAXPRO Cloud, apply power to the control panel. The control panel will automatically attempt to connect to the server and register. This process typically takes a few minutes. You can follow the progress on the display of the system keypad. If you have wired several keypads to the control panel, the system keypad is the first keypad that you touch after powering up. The display will show any failure points. If registration is successful, the connection status on MAXPRO Cloud will change to green. In case you experience any issues, see *Troubleshooting*, page 120. In the following steps, you will let the system discover the MPI peripherals that are connected to the control panel. You can then formally register the system keypad which was temporarily registered on first power-up, and all other keypads and peripherals.
11. Switch MAXPRO Cloud to Installer mode, as follows: in the Controller screen, under CONTROLLER MODE, click Installer, and then click Yes to confirm. The system will automatically scan for new devices connected to the control panel.
12. When scanning is finished, click VIEW ALL to switch to the Devices page. In the New Devices list, you can select and register each new device by giving it a dedicated description and setting any other required parameters.

For detailed instructions, see the MAXPRO Cloud online help.

| | |
|---|---|
|  | ***Note:*** *For initial setup, no programming is required using the keypad. You will configure the system in MAXPRO Cloud.*<br>*For the first panel registered with MAXPRO Cloud (MPC) under a customer, the MPC will automatically generate and configure the random installer PIN code and master PIN code to the panel. All the subsequent registered panels under same customer gets downloaded with the same already generated random PIN codes. Without MPC connection, if the panel is powered on, then for the first time using the arming station the user is able to configure the temporary installer PIN which will be overridden post registration with MPC.*<br>*If you login as customer admin, MPC provides the option to modify the master code at the customer level in MPC. The MPC will automatically download the modified PIN codes to all the control panels under that customer. If you login as dealer admin, you can modify Installer code.* |

## 7.4.2 Troubleshooting

When you apply power to the system, all devices will power up. The system keypad (the first keypad that you touch after powering up the panel) will temporarily register with the control panel in order to facilitate the connection to the server. When the splash screen disappears from the system keypad display, the keypad will display a series of messages, indicating the progress of the connection to the server. If any point fails, the screen will offer to enter Manual Mode and indicate an error message to help determine the cause. Consider the corrective actions detailed below:

- Internet connection check: this message indicates if the panel has made a connection to the local network and has obtained an IP address, and if the panel was able to connect to internet. If this fails, check the items below:
  - The network cable connection: the amber LED on the Ethernet port must be flashing.
  - Is port 443 open on the router for the site?

- Is a proxy server required for Internet access on the site? If so, enter Manual Mode on the keypad to add the proxy server details.

- MPC registration check: this message indicates if the panel is registered in MAXPRO Cloud and is connected to the cloud. If this message fails, check the following:
  - Is a site created yet in MAXPRO Cloud using the MAC address of the panel? For instructions, see *Workflow*, page 119.

### 7.4.3 Using Manual Mode on the Keypad

If the control panel fails to connect to internet and/or to the MAXPRO Cloud server, you can use Manual Mode on the keypad to enter connection details manually.

If connection fails, proceed as follows:

1. On the keypad, tap Enter Manual Mode. The Local Network screen appears.
2. If you want to manually assign an IP address to the panel, provide the following information:
   - PANEL IP ADDRESS: type the desired IP address for the panel.
   - GATEWAY IP ADDRESS: type the gateway IP address for the network segment where the panel resides.
   - SUBNET MASK ADDRESS: type the subnet mask for the network segment where the panel resides.
3. Tap Next to continue.
   The DNS Setup screen appears.
4. If required, type the network's DNS IP address, and then tap Next to continue.
   The APN Setup screen appears.
5. If required, type the Access Point Name (APN) address, and then tap Next to continue.
   The Proxy Setup screen appears.
6. If required, provide the following information for the proxy server:
   - Proxy Address: type the URL for the desired proxy server.
   - User Name: type the user name for logging on to the proxy server.
   - Password: type the password for logging on to the proxy server.
7. Tap Next to continue.
   The Register Server Setup screen appears.
8. The server address is normally filled in correctly for your region. Leave this setting as is.
9. Tap SAVE. The system will try and connect to internet and the MAXPRO Cloud server using the new settings.
10. You must now add the Controller to MPC.

## 7.5 Shutting Down the Panel Securely

The SHUTDOWN button on the panel () allows you to shut down the control panel securely. This makes sure that the system can save all necessary data and statuses in the flash memory. Shutting down the panel disables the inputs and outputs, and switches off the IB2 buses, the AUX outputs, and the PTCs. It does not remove power from the panel (from the AC power adapter or the batteries).

You have to shut down the control panel in the following situations:

- Before disconnecting the LTE Module.
- Before installing or removing peripherals on the IB2 bus.

To shut down the control panel securely, proceed as follows:

1. On the control panel, press the SHUTDOWN button for 5 seconds.
2. Wait for the control panel to shut down completely. The shutdown LED will go out; the keypad screen will go black and all keypad LEDs will go out.
3. You can now add or remove IB2 bus devices, or disconnect the LTE module.To restart the control panel, briefly press the SHUTDOWN button again. The system is ready again when the keypad screen displays the current time and date.

CHAPTER

# 8 CONFIGURATION IN MAXPRO CLOUD

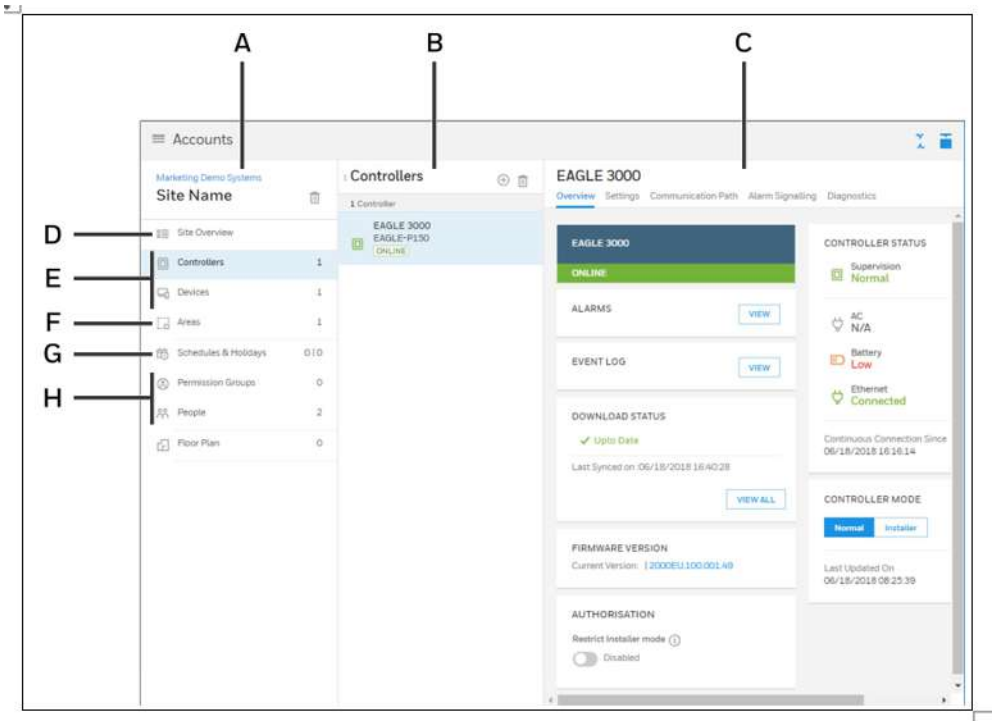
MAXPRO Cloud allows the installing dealer to program the system remotely, and allows the end customer to monitor and control the security system remotely.

This chapter introduces the MAXPRO Cloud user interface, and provides a summary of the settings for the MPI Control Panel and peripherals. The settings information is arranged per screen in MAXPRO Cloud. This document does not contain instructions for setting up an account, rules, reports, firmware updates, alarm handling, camera viewer, MAXPRO Cloud user management, subscriptions, or any other item.

For more detailed information, see the MAXPRO Cloud Configuration Guide and online help. To access the online help: click the Help button in the top right corner of the MAXPRO Cloud screen, and then select Help.

# 8.1 MAXPRO Cloud User Interface

Below is an overview of the main parts of the MAXPRO Cloud's user interface.




| | |
|---|---|
| A | Left column: to select the aspect of an integrated site configuration that you want to work on. |
| B | Middle column: to select the individual item to focus on. |
| C | Right column: contains the detailed information and configuration options of the item as selected in the other columns. The information and options can be split over several tabs. |
| D | General site settings |
| E | Configuration of inputs and outputs, and all peripherals. |
| F | Area specific configuration. |
| G | Schedule definitions. |
| H | Configuration of site users. |

# 8.2 Site Settings

Each site in MAXPRO Cloud can contain multiple control panels. Certain settings apply to all control panels and all peripherals in the site. In MAXPRO Cloud, go to the desired customer and Site Overview page.

### 8.2.1 Overview Tab

This tab shows the customer details.

### 8.2.2 Settings Tab

This tab allows you to set:

- Authority levels for resetting and overriding events.
- For access control with the MPI Door Control Modules, the card type is defined here for the whole site = identical for all DCMs connected to all control panels in the site.

## 8.3 Control Panel Settings

### 8.3.1 Overview Tab

The control panel's Overview tab displays:

- The status of the control panel (online or offline).
- The sync status of configurations. The system syncs the changes automatically when you exit Installer Mode.
- The authorisation status: indicates if the Installer mode is restricted. If that is the case, the customer has to grant the installer access to the system using the keypad.
- Buttons for viewing alarms and the event log, and for switching to Installer mode.
- The current firmware version.

***Note:*** *You can update the MPI firmware using the Firmware option in the menu. For detailed instructions, see* *Updating the Firmware, page 138**. Remember to test all functionality after updating.*

### 8.3.2 About Installer Mode

**Caution: After commissioning the installation, when you have enabled the Restrict Installer Mode setting in MAXPRO Cloud, you can only enter Installer Mode with permission from your customer. The customer authorises the Installer Mode using the keypad. For details, see the MAXPRO Cloud User Guide (doc. no. 800-25754-1).**

- Upon entering Installer Mode, MAXPRO Cloud will automatically scan for new devices connected to the control panel.
- In Installer Mode, the system will not report any alarms or faults. This allows you to add or remove peripherals and batteries, change the configuration (=settings that change the operation of the system) without generating false alarms.

There is one exception: tamper events. Enter the Installer code on the keypad to reset the tamper alarm.

- In Installer Mode, the keypad will indicate Installer service mode in the top left corner of the display.

| | |
|---|---|
|  | **Note:** *You cannot enter Installer Mode if there are armed areas. You must disarm all areas before you can enter Installer Mode.*<br>*You cannot exit Installer Mode if there are faults or tamper events active. You must solve all faults and tampers, and then acknowledge the events in MPC before you can exit Installer Mode.*<br>*Concurrent configuration restriction : Multiple Installer can view the panel configuration at a time. But it is restricted to only one Installer to modify the configuration at a time.*<br>*End Installer Session: An active Installer session via MPC can be ended by the Master user through AMS menu option.* |

## 8.3.3 Settings Tab

This tab displays:

- Control Panel information and general settings
- General settings for all keypads (arming stations) that are connected to the panel: Language, Fail Attempt Limit, and Lock Out Time. Settings for individual keypads are available in the Devices page.
- PIN Entry confirmation: After keying the PIN in the Keypad, you will have to tap the green tick in the arming station or # key in the DCM Reader for the PIN entry to be acknowledged and to proceed with login.
- Backup battery capacity
- Burglary alarm confirmation settings
- Date and time formats
- Reporting and system supervision options.

### *System Supervision Controls*

The system supervision controls allow you to choose which parts of the system you want to supervise. For example, if you are not using a V-Plex loop, you can switch off supervision to prevent trouble events for the loop.

**EN** Switching off supervision options may invalidate compliance with local regulations.

## 8.3.4 Communication Path Tab

The system will set up the Ethernet path automatically using DHCP where possible. In some network environments, for example when using a proxy server, you must enter the network settings manually via the keypad on start- up.

The system will automatically attempt to communicate over Ethernet where available. If there is no Ethernet connection to the internet, the system will switch to an LTE module path if this is configured. The system will switch back to Ethernet when the Ethernet internet connection is restored.

The system supports two independent network connections by adding the optional LTE module MPICLTEE. This provides Ethernet path and LTE path options. The LTE path can sometimes be referred to as cell path, or 3G/4G path.

The system monitors the Ethernet network interface independently in the hardware. It uses a PHY circuit that will generate an Ethernet line fail event when the local connection is removed (see *Events*, page 149).

The system monitors the LTE network interface whenever the connection is not active. The panel sends an AT command request to the LTE module every 6 seconds to confirm that a data connection is present. If there is no data connection available, the system records a line fail event.

The Communication Path tab has two subtabs:

- Communication Path: for the communication paths settings.
- Communication Test: allows you to test the communication paths.

**EN** EN ATS classification according to EN 50136-2: up to SP5 (Single Path Ethernet), DP4 (Dual Path Ethernet Primary/Cell Radio Secondary), SP3 (Single Path Cell Radio) depending on the Path Supervision Period for Primary and Path Supervision Period for Backup settings.

For systems that must meet DP4 (Dual Path Ethernet Primary/Cell Radio Secondary), set the Path Supervision Period for Primary to 90 seconds, and Path Supervision Period for Backup to 5 hours. If the primary path fails, the backup path will automatically step up to 90 seconds.

For systems that must meet SP3 (Single Path Cell Radio), set the Path Supervision Period to 30 minutes.

For systems that must meet SP5 (Single Path Ethernet), set the Path Supervision Period to 90 seconds.

You have to set up the LTE path manually. Make sure that you have inserted a valid data SIM card into the module. Typically, you need to specify only an Access Point Name (APN) for the network service provider of the chosen SIM card. In some regions, you may need additional APN logon details. Check with your local service provider for the necessary information.

**Caution: If you change the APN for the LTE module (for example when changing providers), you have to restart the control panel for the changes to take effect.**

## 8.3.5 Alarm Signalling Tab

The Alarm Signalling tab allows you to define one or more Alarm Reporting schemes. Each scheme consists of defining a Central Station account number, a set of events to be signalled, the areas to be involved, and the destination (alarm receivers). Typically, you only need to create a single alarm signalling report which will cover all the areas in the system. You can define a primary and secondary (backup) receiver (IP address or URL of the Central Station). However, it is possible to create multiple reports, each of which can contain different sets of events, areas, and destinations, and each with a different account number.

***Note:*** *Area 1 is the 'system' area: the system reports all panel and system events (such as tampers, battery low...) on Area 1.*

### 8.3.6 Diagnostics Tab

The Diagnostics tab is only available when the control panel is online. It provides details on:

- Power: incoming voltage, total load current, and estimated battery run time.

Furthermore, it provides details on the AUX ouputs and the backup batteries.

- LTE module (Cell radio)
- Communications channels.

| | |
|---|---|
|  | ***Note:*** *The measured values (voltages, currents, resistance values) in the Diagnostics screen are indicative values only and intended for relative comparison purposes. They are not calibrated readings.* |

## 8.4 Device Status

The Devices page, Configured Devices displays the list of configured devices on the IB2 bus. It indicates the current status of each device.

## 8.5 Control Panel Input/Output Settings

To configure the inputs and outputs on the Control Panel, go the Devices page, and select Panel I/O. You will find a tab for zones (inputs), for outputs, and a diagnostics tab.

### 8.5.1 Zones Tab

For each of the 10 zones, it displays:

Zone information, such as zone number and name

Settings, such as zone response type, area, and if the zone is bypassable.

Advanced settings, such as the zone supervision type and EOL resistor values.

### 8.5.2 Outputs Tab

For each output (1–9) it displays:

- Output information, such as output number and name
- Settings, such as start trigger and area(s).
- Advanced settings, such as stop trigger, pulse settings, and output polarity.

### 8.5.3 Diagnostics Tab

The Diagnostics tab is only available if the control panel is online.

It displays the current zone status and measured resistance value for each of the 10 zones.

It also displays the minimum and maximum resistance value measured, with date and time.

Click Refresh to refresh the diagnostic data.

| | |
|---|---|
|  | ***Note:*** *The measured values (voltages, currents, resistance values) in the Diagnostics screen are indicative values only and intended for relative comparison purposes. They are not calibrated readings.* |

# 8.6 Keypad Settings

In the Configured IB2 Devices section, you can find the information and settings for the individual keypads:

- Keypad information, such as serial number, name, and IB2 bus.
- Settings, such as home and associated areas.
- Settings that apply to all the keypads connected to the control panel, are available in the Control Panel settings. For details, see *Settings Tab*, page 125.

# 8.7 Door Control Module Settings

The following settings are available for each individual Door Control Module:

## 8.7.1 Overview Tab

The Overview tab hows the name of the Door Control Module and a diagram of the door configuration.

## 8.7.2 Settings Tab

This tab displays:

- DCM information, such as serial number, name, and IB2 bus.
- Settings, such as the area, the operation in reduced capability mode, door open times, Card/PIN usage, on-board tamper switch, triple swipe, settings for entry/exit reader or RTE buttons.

| | |
|---|---|
|  | ***Note:*** *The card type is set on site level (Site > Settings > Miscellaneous). For details, see Site Settings, page 124.* |

## 8.7.3 I/O Tab

This tab displays:

- Settings for the door status monitor, such as zone supervision type and EOL resistor values.
- Settings for the RTE button.
- Settings for the door lock relay.

# 8.8 Relay Module Settings

The following settings are available for each individual Relay Module:

## 8.8.1 Settings Tab

This tab displays:

- Device information, such as serial number, name, and IB2 bus.
- Settings, such as the on-board tamper switch.

## 8.8.2 Outputs Tab

This tab displays for each relay:

- Output information, such as output number and name

- Settings, such as start trigger and area(s).
- Advanced settings, such as stop trigger, pulse settings, and output polarity.

# 8.9 Remote Power Supply Settings

The following settings are available for each individual Remote Power Supply:

## 8.9.1 Settings Tab

This tab displays:

Device information, such as serial number, name, and IB2 bus.

Settings, such as the backup battery capacities.

## 8.9.2 Outputs Tab

For each output (trigger):

- Output information, such as output number and name
- Settings, such as start trigger and area(s).
- Advanced settings, such as stop trigger, pulse settings, and output polarity.

## 8.9.3 Diagnostics Tab

The Diagnostics tab is only available when the Remote Power Supply is online.

It provides details on:

- Power: incoming voltage, toal load current, and estimated battery run time.
- Details on the AUX ouputs and the backup batteries.

| | |
|---|---|
|  | ***Note:*** *The PTC on trigger 4 is not monitored. The measured values (voltages, currents, resistance values) in the Diagnostics screen are indicative values only and intended for relative comparison purposes. They are not calibrated readings.* |

# 8.10 Zone Expander Settings

The following settings are available for each individual Zone Expander:

## 8.10.1 Settings Tab

This tab displays:

- Device information, such as serial number, name, and IB2 bus.
- Settings, such as the on-board tamper switch.

## 8.10.2 Zones Tab

For each of the 8 zones:

- Zone information, such as zone number and name
- Settings, such as zone response type, area, and if the zone is bypassable.
- Advanced settings, such as the zone supervision type and EOL resistor values.

## 8.10.3 Outputs Tab

For each output (1–4):

- Output information, such as output number and name
- Settings, such as start trigger and area(s).
- Advanced settings, such as stop trigger, pulse settings, and output polarity.

# 8.11 V-Plex devices

The V-Plex devices page allows you set the device's zones, outputs, and run diagnostics on the V-Plex loop(s). For smart PIRs, you can enable the Smart Contact setting, allowing the PIR to detect a mask condition in disarmed state.

# 8.12 RF Devices

Under **RF devices**, you can start adding sensors for every zone. If the sensor is unable to communicate with the wireless transceiver, there is a 20 min wait, post which an RF activity failure event is activated. You cannot edit/modify **Area** settings when this event is active.

## 8.12.1 Zones tab

For each of the zone:

- Zone information, such as zone number , zone name, serial number, loop number
- Settings, such as zone response type, area, and if the zone is bypassable.

## 8.12.2 Diagnostics Tab

The **Diagnostics** tab displays details about the RF Sensors/Devices.

It provides details on:

- **Signal Strength**: Received signal strength.
- **Number of Supervisions missed**: Sensor missing supervision count is based on how many hours sensor has not communicated. The count resets once the communication is restored. .

For more details, refer to **RF Sensors** section in *MPI Configuration Guide*.

# 8.13 Areas

The following settings are available for each area:

## 8.13.1 Settings Tab

This tab displays:

- Area information, such as area number and name
- Settings, such as area type, entry and exit delays, and settings for alarm sounders, arming/disarming, and bypassing zones.

> **EN** For EN 50131-1 compliance, set the bell timeout to max. 15 minutes. Note that local/national requirements may demand a different value. Check your local/national regulations.

| | |
|---|---|
| | **Note:** *Area 1 is the 'system' area: the system reports all panel and system events (such as tampers, battery low...) on Area 1.* |

### 8.13.2 Sensors Tab

Displays all the sensors that are assigned to the current area.

### 8.13.3 Outputs Tab

Displays all the outputs that are assigned to the current area.

### 8.13.4 System Area

When you register a control panel in MAXPRO Cloud, the system automatically creates one area for it, Area 1, and assigns the control panel to this area. This is the system area: the system will report all panel and system events on Area 1. For example: communication failures, battery low, tamper events...

In case of a panel tamper event (lid, off-wall), the system will report the tamper event as a fault if Area 1 is disarmed, and as an alarm if Area 1 is armed.

MAXPRO Cloud sorts the area list on area number, not on area name. Even if you have renamed Area 1, it will still appear at the top of the area list (or at the bottom if you sort the list in descending order). The list displays the area number:


### 8.13.5 Delete Area

The area delete feature provides the Installer with an option to delete an Area from the controller. If the area is not associated to any entity such as zone, output, etc., you can directly delete the selected area. But, if the area is associated with any entity, then, the associations are listed in MPC page. The installer must manually disassociate the entities and then delete the area.

| | |
|---|---|
| | **Note:** *Area Delete option is not applicable for Default Area. Multiple areas cannot be deleted at a time.* |

## 8.14 Scheduling and Holidays

The scheduling and holidays features allow certain operations to be automated, such as arming and disarming. The system comes with two default schedules (always on and always off), but you can define any schedule you need. You define schedules on the customer level in MAXPRO Cloud. Once a schedule is defined, you can use it on every site, every control panel... of that customer.

Holidays allow you to define 'exception days' in a fixed schedule. For example, you want to allow access to a group of users on all week days, except on holidays such as New Year.

You can assign schedules to:

- areas, for automatic arming and disarming
- permission groups, for restricting access

- rules and controller rules, for automating tasks.

## 8.15 DCM Door Schedule

MPI Door Control Module (DCM) door unlock period can be controlled based on schedule. An Area needs to be in the disarmed state for door unlock schedule to execute. Door lock command from MPC will take priority over the schedule.

## 8.16 Permission Groups

Permission Groups allow you to quickly assign the same set of permissions to different people. A Permission Group is a set of access rules to areas and doors, according to a schedule. You define Permission Groups on the customer level in MAXPRO Cloud. Once a Permission Group is defined, you can use it on every site, every control panel... of that customer. For details, see the *MAXPRO Cloud Configuration Guide* (doc. no. 800-24096-1).

## 8.17 People

### 8.17.1 General

The Control Panel allows up to 10,000 users (People). You define users on the customer level in MAXPRO Cloud. Once you have defined a user, it is available for every site, every control panel... of that customer.

One user code can grant access to different sites, areas, and doors via Permission Groups. Furthermore, you can define a role (Intrusion Authority) for the user code, to control access to functions such as arming/disarming, silencing alarms, etc.

You assign each site user a 6-digit numeric (0–9) PIN code in the range from 001000 to 999999. This sequence of numbers provides a total of 999,000 available codes. PIN codes in the range from 000000 to 000999 are reserved.

| | |
|---|---|
|  | **Caution: The default PIN length is 6 digits. However, you can set the PIN length between 4 and 6 digits. 6 digit PIN codes must be used for EN 50131-1 compliant installations and that failure to do so will render the system non-compliant. You define the PIN length on customer level: all PIN codes for all sites will have the same length. Make sure that you specify the PIN length before you define any people. If not, you will need to change all the configured people's PIN codes manually.**<br>**If the panel is powered ON without the MPC connection, then, for the first-time usage of the arming station, the user can configure the temporary installer PIN. Post the panel registration in MPC, this PIN is overridden.** |

You can also assign a card to a user. Compatible cards use 26 bits or more, providing a minimum of 67,108,864 ($2_{26}$) different card numbers. There are no reserved card number ranges.

Also, selecting Learn Card feature enables you to assign a card instantly (through AMS or DCM), without knowing the card number in advance.

You set the Installer User and Master User codes on customer level. The system will automatically download the new codes to each of the customer's control panels once connected to MAXPRO Cloud.

- To change the Installer code: as an installer, log on to MPC to your Dealer account with an Admin role. Under Customers, select the desired customer, and then change the Installer PIN on the customer's Settings tab.
- To change the Master code: the customer must log on to MPC with the Master Admin credentials. They can change the Master PIN under My Sites, on the Overview page, on the Settings tab. Only the Master Admin user can change the Master PIN.

You can create additional Installer and Master codes for each control panel in the normal way for creating people and credentials. For details on programming people, see the *MAXPRO Cloud Configuration Guide* (doc. no. 800-24096-1).

MAXPRO Cloud holds the main user database. It operates as one database across the End Customer's account. The user's name is the unique reference. No two users can share both the same First and Last Name.

## 8.17.2 Intrusion Authority Levels

You have to assign a role, or level of authority, to each end user of the system. This authorizes the end user for certain system functions. An end user can have different levels of authority within different areas.

The following levels of authority are available:

- Installer
- Master
- Employee
- Security Guard
- Janitor
- Duress.
- ATM User

***Note:*** *The permissions for the Installer as described in the table below, are only available if the customer's Administrator authorises them by setting the dealer privileges in MAXPRO Cloud. For example, the Administrator can allow or deny installers from arming and/or disarming areas. The dealer privileges are valid for all the customer's sites.*

For details on the permissions of each level, go to any person's Permission tab, and click the Info button ⓘ above the Intrusion Authority box.

For MAXPRO Intrusion, the authorisations are defined as follows:

| Function | Authority Levels | | | | | | |
|---|---|---|---|---|---|---|---|
| | Installer | Master | Daily employee | Security guard | Janitor | Duress | ATM User |
| General Functions | | | | | | | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| Arm | Yes | Yes | Yes | Yes | Yes | Yes | Yes, but only<br>ATM<br>Area<br> |
| Disarm | Yes, but only if armed by same code | Yes | Yes | Yes | Yes | Yes | Yes, but only<br>ATM<br>Area |
| Bypass zones[1] | Burglary only | Burglary only | Burglary only | Burglary only | No | No | Yes, but only<br>ATM<br>Area<br>Seismic<br>Zone(s) |
| Cancel (silence) alarms and events | | | | | | | |
| Residential Fire alarms | Yes | Yes | Yes | Yes | No | No | No |
| Burglary, medical, panic, and non- security[2] alarms | Only if armed by the installer | Yes | Yes | Yes | Yes | Yes | No |
| Confirmed alarms | Only if armed by the installer | Yes | Yes | Yes | Yes | Yes | No |
| Troubles | Yes | Yes | Yes | Yes | Yes | Yes | No |
| Tampers | Yes | Yes | Yes | Yes | Yes | Yes | No |

If the zone is bypassable. Fire zones are never bypassable.

An example of a non-security alarm: an alarm from a sensor in a freezer indicating that the temperature is too high.

| Function | Authority Levels | | | | | | |
|---|---|---|---|---|---|---|---|
| | Installer | Master | Daily employee | Security guard | Janitor | Duress | ATM User |
| Reset | | | | | | | |
| Residential Fire alarms | Yes | Yes | Yes | Yes | No | No | No |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| Burglary alarms | Yes | Yes | Yes | Yes | No | No | No |
| Panic/ holdup alarms | Yes | Yes | Yes | Yes | No | No | No |
| Confirmed alarms | Yes | No | No | No | No | No | No |
| AC power troubles | Yes | Yes | Yes | Yes | No | No | No |
| System battery troubles | Yes | No | No | No | No | No | No |
| Single comms path troubles | Yes | Yes | Yes | Yes | No | No | No |
| ATS and fail to comms troubles | Yes | Yes | Yes | Yes | No | No | No |
| Interconnection Faults | Yes | No | No | No | No | No | No |
| Sensor masked | Yes | Yes | Yes | Yes | No | No | No |
| Other troubles | Yes | No | No | No | No | No | No |
| Tampers | Yes | No | No | No | No | No | No |
| Override | | | | | | | |
| AC power troubles | Yes | Yes | Yes | Yes | No | No | No |
| System battery troubles | Yes | Yes | Yes | Yes | No | No | No |
| Single comms path troubles | Yes | Yes | Yes | Yes | No | No | No |
| ATS and fail to comms troubles | Yes | No | No | No | No | No | No |
| Sensor masked | Yes | Yes | Yes | Yes | No | No | No |
| Other troubles | Yes | Yes | Yes | Yes | No | No | No |

| Function | Authority Levels | | | | | | |
|---|---|---|---|---|---|---|---|
| | Installer | Master | Daily employee | Security guard | Janitor | Duress | ATM User |
| Tampers | Yes | No | No | No | No | No | No |
| Other Actions | | | | | | | |
| View log | Yes | Yes | No | Yes | No | No | No |
| Run siren and walk test | Yes | Yes | No | Yes | No | No | No |

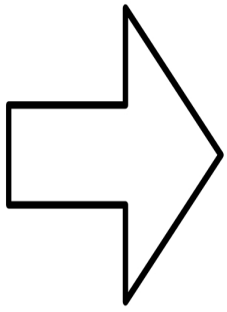
***Note:*** *Default settings are EN 50131-1 compliant. Once you modify these default settings, you will render the system non-compliant to EN 50131-1.*

## 8.18 Controller Rules

Controller rules allow the system to perform automated actions within the control panel, based on complex logical combinations of events. A controller rule has two parts:

- **If**: a logic combination of conditions which must be true to trigger the rule. You can use up to three conditions, combining them by AND or OR logic. You cannot combine AND and OR logic in one rule; you have to choose one.
- **Then**: A list of actions which the system will carry out when the logical combination of conditions becomes true. You can use up to three actions.

When the conditions become true, the system will carry out the defined actions once, and in sequence. However, as this happens almost immediately, the order of the actions is only important if one of the actions is a 'wait' action. Wait actions enable you to carry out two separate actions with a defined time interval between them.

| IF | | THEN |
|---|---|---|
| Condition 1 is true |  | Perform action 1 |
| AND/OR | | Followed by |
| Condition 2 is true | | Perform action 2 |
| AND/OR | | Followed by |
| Condition 3 is true | | Perform action 3 |

.The controller rules run from the control panel, and are not affected by the connection with MAXPRO Cloud. Controller rules are separate from the standard Rules in MAXPRO Cloud.

For details on programming controller rules, see the *MAXPRO Cloud Configuration Guide* (doc. no. 800-24096-1).

**EN** Using rules (standard Rules or Controller Rules) for automating tasks may render the system non-compliant Check all the rules that you program for compliance with product standards.

## 8.19 Floor Plan

Floor plans allow you to visualise a site and its zones. For details, see the MAXPRO Cloud Configuration Guide.

## 8.20 Clock Synchronisation

Initially, the panel will sync the time with Network Time Protocol (NTP) server. Post the registration with MPC, periodically (everyday) MPC will sync the time with control panel.

***Note:*** *At any instance, when MPC connection is not available and if the control panel is restarting, then, the panel will sync the time with NTP server.*

## 8.21 Updating the Firmware

Honeywell regularly provides firmware updates for your MPI system, which you can easily download via MAXPRO Cloud. When new firmware for the MPI system is available, a notification message appears in MAXPRO Cloud.

If your system contains multiple control panels, you need to perform the update for each control panel.

***Note:*** *The firmware update may include updates for the MPI control panel and peripherals. Depending on the number of devices that need updating, the entire process may take around 10 hours.*
*Honeywell recommends to use the Ethernet connection (instead of the cell radio connection) for performing firmware upgrades.*

To update the firmware, proceed as follows:

1. First, download the firmware using MAXPRO Cloud: in the control panel's Overview page, click the New Firmware Available button.
2. Select the desired control panel and firmware version, and then click Update.
   The system starts downloading the selected firmware version. The Current version column indicates progress.
3. For Update action, the corresponding status is Downloading. Once the download is 100%, the status changes to Authorize on Arming Station.

4. Once the manager level user selects Authorize on Arming Station, the corresponding status changes to Updating and the Panel reboots.
5. After panel reboot, in case of any peripheral pending for update, the Peripherals Pending Update, No Action Needed Now message appears.
6. Make sure the control panel is in Normal mode. If the control panel is in Installer mode, then switch it back to Normal mode first.
7. Go to the system keypad and log on. The keypad will display a message that new firmware is available.
8. Tap Update.

| | |
|---|---|
|  | ***Note:*** *If you want to postpone the new firmware installation, tap Postpone. The next time you log on to the keypad, the system will display the screen for installing the new firmware again.* |

The system starts installing the new firmware for the control panel. The message in the top left corner of the keypad indicates that the system is updating. When finished, the control panel will automatically restart.

9. When the control panel has restarted, log on to the system keypad again. The keypad will display a message to confirm that the firmware has been upgraded.
10. Tap OK to confirm the message. The home screen will indicate that the control panel has been restarted.
11. Tap View Items and reset the event. The firmware update will appear in the control panel's event log.
    If there are updates for the peripherals, the system will download these in the background after the control panel update has completed. This may take around 10 hours, depending upon the size of the system. You can safely use the control panel and the peripherals during this period. When the peripheral updates are ready to install, the keypad will again display a message the next time a user logs on, indicating that new firmware is available for installation.
12. When the peripheral updates are ready to install: tap Update. The system applies the firmware to all relevant peripherals. The system will be ready for use within 5 minutes.
13. If applicable, repeat for other control panels.

| | |
|---|---|
|  | ***Note:*** *You can click View Details for the list of peripherals pending update.*<br>*Failed: After 5 auto-update attempts, the device moves from Pending state to Failed state. The auto-update attempts are spaced every 24hrs after the first update attempt. Once the panels and peripherals are updated, the update or failure events are available in:*<br>*-ISP Events screen*<br>*-Controller Overview SPT log*<br>*-AMS activity log*<br>*Updated: Lists all the peripherals that have been updated.*<br>*Pending: Lists all the peripherals pending for an update.* |

CHAPTER

# 9 TESTING AND COMMISSIONING

## 9.1 Battery Test

The system runs the following battery tests:

- If AC power is present, the control panel runs a brief battery test every 60 minutes to determine if the battery or batteries are connected.
- It runs an extended battery test every 4 hours to check on the battery's condition. The extended test begins 4 hours after exiting Installer Mode.
- If the control panel finds that the battery voltage is low (less than approximately 11.2 V), it generates a low battery warning. It will log the warning, display it on the keypad, and report it to the central station. When the battery level is normal again, the system will send a Restore report to the central station.

## 9.2 Burglary Walk Test

The Burglary Walk Test causes the system to sound keypad beeps in response to faults on zones, so you can check proper zone operation without triggering alarms. You perform the test in disarmed mode, using the keypad. The system will send 'start of walk test' and 'end of walk test' messages to the central station.

| | |
|---|---|
|  | ***Note:*** *You perform a Burglary Walk Test for each area individually. The system will not send alarms for that area during the test. Other areas are still operative and will cause the external sounder and communicator to activate if an alarm condition occurs.* |

To run the burglary walk test, proceed as follows:

- Log on to the keypad, and tap Menu > Test modes > Walk test standard sensors.
- Tap the desired area, and then tap Start test. They keypad displays the list of untested zones in that area.
- Activate each zone in the area. The keypad produces a double beep when you activate each zone. The system moves the tested zones to the tested zones list.
- After testing all the zones in the area, you can:
- Tap View Tested to see the tested zones. Then tap Back to return to the list of areas.Tap New Test to return to the Test modes menu.
- Repeat for all areas and all zones.

- Tap Done to finish.

| | |
|---|---|
|  | ***Note:*** *If there is more than one keypad for the area, all keypads indicate that the Burglary Walk Test is in progress. During the test, all keypads will beep once every 30 seconds.*<br>*The system automatically exits the Burglary Walk Test mode if there is no activity (no doors or windows are opened and closed, no motion detectors are activated, etc.) for 30 minutes. During the last 5 minutes, all keypads in the area display a message that the system is about to exit Walk Test mode, and they beep twice every 15 seconds. After that, the system returns to normal operation.* |

## 9.3 Armed Burglary System Test

Besides the standard burglary walk test, you shall also perform a test while the system is armed, to check if the system produces the required alarm sounds and sends the alarm messages to the CMS.

| | |
|---|---|
|  | ***Note:*** *The system sends alarm messages to the CMS during the armed system tests. Notify the CMS that you will be performing a test.* |

To perform an armed system test, proceed as follows:

- Notify the CMS that you will perform a test of the system.
- Using the keypad, arm the system.
- Fault one or more zones.
- Using the keypad, silence any alarm sounder(s).
- Rearm the system.
- Repeat arming/faulting/silencing/rearming until you have tested all zones. Check at least the following items:
- Check that entry/exit delay zones provide the assigned delay times.
- If a zone has been programmed for audible alarm, check if the system produces the required alarm sounds (on the keypad, on the alarm sounders). If the zone has been programmed for silent alarm, there are no audible alarms or displays, but the system will send a report to the CMS.
- Notify the CMS that all tests are finished, and verify results with them.

## 9.4 Smoke Detector Test

You must test all smoke detectors monthly. To run a smoke detector test, proceed as follows:

- Press the TEST button located on the detector. If the TEST button does not cause the detector to activate, you must replace it immediately.

## 9.5 Siren Test

The siren test on the keypad allows you to test all alarm sounders (and any related strobe lights). You can perform the test per area, or for all areas at once.

To run the siren test, proceed as follows:

1. Log on to the keypad, and tap **Menu > Test modes > Siren test**.
2. Tap the desired area, or tap **All Areas** to test the alarm sounders in all areas.
3. Tap **Test**. The system activates the alarm sounders and any related strobes in the selected area or areas.
4. Check if the alarm sounders and strobes work as required.
5. Tap **Stop** to deactivate the alarm sounders and related strobes.

To run the siren test, with alternate Power Supply :

1. MPC output programming for Onboard relay output new start trigger - Siren Test to be added. The selected default action should be **Reflex**, to map with Siren test performed on AMS which is a latched action.
2. When Siren test is stopped at AMS, Relay output should deactivate.
3. Current Siren test should continue to work for specific Area, All Areas triggering test command to all Sirens configured in the system.
4. Installer should be recommended to wire only Battery enabled Sirens via relay output and no other device like smoke bomb, etc.
5. In case of multiple battery enabled Sirens are installed (for different Areas), Installer uses same relay output in output programming for Siren test. When Siren test is started for 1 Area, all Sirens connected to this relay will have primary power source cut off.
6. Installer should be able to configure relays in Relay module, Vplex and Relay 5_6(Onboard) for Siren Test. ZE & PSU are not applicable as they support voltage triggers.

| | |
|---|---|
|  | ***Note:*** *Instructions: During the Siren test Sirens connected to +12Vdc of panel or PSU AND with a battery as secondary power supply, should be tested upon secondary Power supply (its battery). Therefore the main power supply (+12Vdc of panel or PSU) should be disconnected.*<br>*This relay will be activated by an output configured with Siren Test start Trigger. Output action will be reflex (latched) matching to Siren test which is also latched action. When User does stop siren test output also will deactivate getting siren back with primary power source.*<br>*Installer can use and configure relays in relay module, Vplex, Relay 5 & 6 (onboard) with Siren Test.* |

## 9.6 Walk test

1. Log on to the keypad, and tap **Menu > Test modes > Walk test RF sensors**.
2. Tap the desired area, and then tap **Start test**. They keypad displays the list of untested zones in that area.
3. Activate (tamper/trip sensors) each zone in the area. The keypad produces a double beep when you activate each zone. The system moves the tested zones to the tested zones list.
4. After testing all the zones in the area, you can:

- Tap **View Tested** to see the tested zones. Then tap **Back** to return to the list of areas.
- Tap **New Test** to return to the Test modes menu.
- Repeat for all areas and all zones.

| | |
|---|---|
|  | ***Note:*** *Honeywell recommends you to start the RF walk test with system in Installer mode and check if the signal strength of RF sensors is either medium or high, as this is recommended for good installation.* |

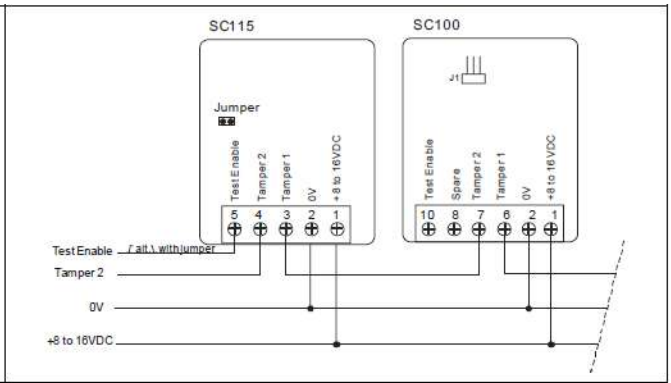
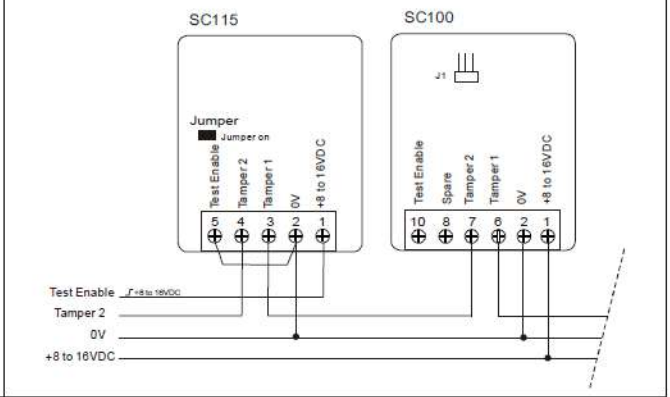
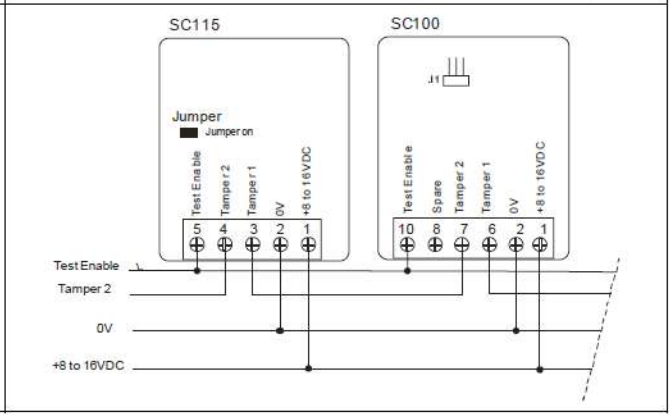
## 9.7 Seismic Testing

The Seismic sensors are connected to vaults so that protections for vaults can be quickly set up without extensive custom programming. It is not possible to perform a walk test for Seismic Zones

To run the seismic test, proceed as follows:

1. Seismic" zone which behaves as 24-hour intrusion/burglary alarm zone must be configured from MPC.
2. "Seismic" output must be configured from MPC. When test mode is on, a signal low from the output of the control panel activates the test device in the sensor (internal/ external). The Seismic output is pulsed and is used to activate the remote self-test function on Seismic sensors (internal), or the output can be used in conjunction with the "test enable" input on External Test Transmitter.

| | |
|---|---|
|  | ***Note:*** *MPI supports Wiring Type A, B, and C between seismic sensor and seismic simulator (External/Internal Test transmitter). Please refer the wiring for Type A, B and C below.* |

| | |
|---|---|
| A: **Use an active low or active high Test Enable signal** to start SC115. SC100 will acknowledge a successful test by generating an alarm signal within 5 ~ 60 seconds. |  |
| B: **Apply voltage** (+8 ~16VDC) to start SC115. SC100 will acknowledge a successful test by generating an alarm signal within 5 ~ 60 seconds. |  |
| C: **Use an active low Test Enable signal only** to start SC115 and SC100 remote test sequence. SC100 will acknowledge a successful test by generating an alarm signal within 1 second. |  |

3. Seismic Test can be activated periodically based on schedule from MPC. Seismic Test should be scheduled such that it doesn't coincide with arming/disarming of ATM areas. Seismic Test can also be activated manually from MPC/AMS.
4. Seismic Test is applicable per area. The output should be assigned to an area so that all Seismic zones in that area will go into the test mode when the output is activated.
5. When Seismic Test is initiated, the alarm action gets bypassed momentarily for the duration of the test and is not communicated to CMS/ARC.
6. The specific vibration test output for the area is switched ON for 55 seconds to enable the sensors to activate the vibration modules.
7. Each Seismic zone in the area is activated within 55 seconds to confirm a successful test.
8. If any zone within the area does not give an alarm activation, it is regarded as faulty and a trouble condition is generated and signaled to CMS/ARC.

9. Once the test routine is finished, all the Seismic zones are restored and brought back into service immediately. If the zone does not restore, then a trouble condition is generated and transmitted to the CMS/ARC.

10. Arming/disarming of non-ATM areas is not affected by Seismic Test.

11. Seismic output can't be configured for Macros/Controller Rules.

CHAPTER

# 10 IMPORTANT INFORMATION

## 10.1 To the Installer

Regular maintenance and inspection (at least annually) by the installer and frequent testing by the user are vital to continuous satisfactory operation of any alarm system.

You, as an installer, should assume the responsibility of developing and offering a regular maintenance program to the user as well as informing the user of the proper operation and limitations of the alarm system and its component parts. You must include recommendations for a specific program of frequent testing (at least weekly) to ensure the system's proper operation at all times.

Furthermore, maintain proper documentation of the installation. Note the devices that were installed, when they were installed, and where they were installed. Keep track of the last time any maintenance or testing was performed, as well as which maintenance or test tasks were performed. Finally, document any changes to the system.

## 10.2 Turning the System over to the User

Once the system is fully set up, tested, and approved; and before turning the system over to the user:

- Make sure that the default user PIN codes (Installer and Master code) have been changed. If not, anyone knowing the default codes can log on to the keypad and make (unauthorised) changes to the system. For details on changing the default PIN codes, see the MAXPRO Cloud online help.
- Make sure that the customer has enabled the Restrict Installer Mode setting in MAXPRO Cloud (go to My Sites, then select the desired site, then select the desired control panel; repeat for each control panel). With this setting enabled, the customer has to grant access to an installer before they can log on and start Installer Mode to make changes to the system. This will prevent unauthorised changes to the system once it has been set up and approved. The customer can use the keypad to allow and block access for the installer.

**EN** The customer must enable the Restrict Installer Mode option in MAXPRO Cloud before you hand over the system to them. If you leave the system with the customer in a non-compliant condition, you must remove any product labels stating compliance.

- Fully explain the operation of the system to the customer by going over each of its functions, as well as the User Guide supplied. Explain the operation of each zone (entry/exit, intruder, interior, fire, etc.). Be sure the customer understands how to operate any emergency feature(s) programmed into the system.

## 10.3 Contacting Technical Support

PLEASE, before you call Technical Support, be sure you:

Read the instructions!

- Check all wiring connections.
- Determine that the power supply and/or backup battery are supplying proper voltages.
- Verify your programming information where applicable.
- Verify that all keypads and devices are registered properly in MAXPRO Cloud.
- Note the proper model number of the devices, and the firmware version (if known) along with any documentation that came with the product.
- If you receive a warning or error message, note down the exact message text.
- Note your Honeywell customer number and/or company name.
- Having this information handy will make it easier for us to serve you quickly and effectively.

CHAPTER

# 11 EVENTS

## 11.1 Event Notification Priority

Normally, the system sends all events to the CMS in chronological order.

If multiple events occur simultaneously, the system prioritises the event transfer as follows:

- Fire
- Duress (panic/hold-up)
- Silent PA
- PA
- 24 hour
- Burglar
- Other alarms
- All others
- Audio alarms.

Special case: AC power fail event

In case of an AC power fail event, the panel immediately logs the event and reports it to MAXPRO Cloud. However, the system will not immediately send the event to the CMS. Instead, it is delayed by a random time between 40 and 50 minutes. This prevents nuisance alarms for short AC power interruptions, and prevents that the CMS is flooded with such alarms in case of a general power outage in a region.

Alarm Sounds The system produces different alarm sounds for different alarm types:

- Fire alarm: 3 long tones in succession, repeated after 1.5 seconds.
- CO alarm: 4 short tones in succession, repeated after 5 seconds.
- Intrusion alarm: steady tone

## 11.2 Indications

The system provides general indications when permitted as the events occur. It displays the indications that you access on a keypad (by viewing alerts) in the following order, and then ordered by time of occurrence:

- Fire
- Duress (panic/hold-up)
- Burglar
- Trouble
- Other alarms

## 11.3 Event Reporting per Area

If the system only has one area, then all events are reported and logged on Area 1, the system area.

In a system with multiple areas, event reporting is as follows:

- All system events are reported on Area 1, the system area. System events are: communication with peripherals, battery status, tampers...
- All events regarding access control on the DCM are reported on the area that is associated with the DCM.

A few examples:

- A battery low event on a Remote Power Supply will report to Area 1 (battery low = system event).
- A tamper event on a Door Control Module will report to Area 1 (tamper = system event).
- A door status event on a Door Control Module will report on the DCM's area.

# 11.4 MPI Events and Contact ID Codes

## 11.4.1 Events List

| MPI Event | CID # |
|---|---|
| Medical Alarm | 1100 |
| Fire Alarm | 1110 |
| Panic Alarm | 1120 |
| duress PIN entered | 1121 |
| 24 Hour silent holdup alarm | 1122 |
| alarm intruder - not used? | 1130 |
| alarm perimeter | 1131 |
| alarm interior | 1132 |
| alarm 24 hour | 1133 |
| alarm entry exit | 1134 |
| alarm day/night | 1135 |
| alarm outdoor | 1136 |
| open circuit trouble | 1137 |
| interconnection trouble | 1137 |
| Input device constant voltage Tamper | 1137 |
| open circuit trouble | 1137 |
| Tamper | 1137 |
| Intrusion Verifier | 1139 |
| exp mod tamper caused by mod missing | 1143 |
| aux bell tamper | 1143 |
| Equipment fail (assuming non-burglary) | 1150 |
| General alarm | 1150 |
| AC Loss | 1301 |
| Fuse Failure detected | 1301 |
| fuse reset failed for mains | 1301 |
| High voltage condition detected | 1301 |
| Low voltage condition detected | 1301 |
| AC Loss | 1301 |
| AC Power disabled | 1301 |
| Battery Failure detected | 1302 |

| | |
|---|---|
| Low battery | 1302 |
| Fuse for Battery Failure detected | 1302 |
| Battery Module disabled | 1302 |
| Bell/Sounder Trouble | 1321 |
| Bell/Sounder Trouble conflict with 321 | 1321 |
| expansion module tamper | 1341 |
| module missing | 1341 |
| wall tamper | 1341 |
| General alarm restore | 1350 |
| 24 Hour trouble | 1354 |
| 24 Hour trouble Cell (RF Jam) | 1354 |
| 24 Hour trouble(Lan Fault) | 1354 |
| Comm Path Supervision Fault | 1358 |
| Fire Trouble | 1373 |
| Cross zoneTrouble | 1378 |
| Sensor Trouble | 1380 |
| open circuit trouble | 1383 |
| Input device constant voltageTamper | 1383 |
| Sensor Tamper | 1383 |
| bell aux tamper | 1383 |
| Smoke Detector High Sensitivity | 1385 |
| Smoke Detector Low Sensitivity | 1386 |
| Partition unset event | 1401 |
| burglary cancel | 1406 |
| Remote Disarm | 1407 |
| Door Forced open restore | 1421 |
| Early Armed | 1451 |
| Late Disarmed | 1452 |
| Failed to Arm/close the system with in Access Window | 1453 |
| Exit error | 1457 |
| recent close | 1459 |
| lockout -multiple attemptfailure tamper | 1461 |
| Zone Bypassed | 1570 |
| Fire Zone Bypassed | 1571 |

| | |
|---|---|
| Panic Zone Bypassed | 1572 |
| Burglary bypass | 1573 |
| Burglary  Zone Bypassed | 1573 |
| Burglary walk test started | 1607 |
| panel program entry | 1627 |
| panel program exit | 1628 |
| fire silence | 1912 |
| CO silence | 1912 |
| Medical Alarm Restored | 3100 |
| Fire Alarm Restored | 3110 |
| Panic Alarm Restored | 3120 |
| 24 Hour silent holdup alarm restore | 3122 |
| alarm restore event | 3130 |
| alarm perimeter | 3131 |
| alarm interior restore | 3132 |
| alarm 24 hour restore | 3133 |
| alarm entry exit restore | 3134 |
| alarm day/night restore | 3135 |
| alarm outdoor restore | 3136 |
| open circuit trouble restore | 3137 |
| interconnection trouble restore | 3137 |
| constant voltage  trouble  restore | 3137 |
| open circuit trouble restore | 3137 |
| short circuit trouble restore | 3137 |
| Tamper restore | 3137 |
| exp mod tamper  caused by mod missing restore | 3143 |
| aux bell tamper restore | 3143 |
| Equipment fail restore (assuming non-burglary) | 3150 |
| Carbon Monoxide Detector  Restored | 3162 |
| Fire Verifier | 3200 |
| AC Restoral | 3301 |
| Fuse Restoral | 3301 |
| Battery Failure restored | 3302 |
| Fuse for Battery Failure restored | 3302 |

| | |
|---|---|
| Battery module enabled | 3302 |
| Battery Failure restored | 3302 |
| Battery charger restored | 3302 |
| Bell/Sounder Trouble Restore | 3321 |
| modules missing restore | 3341 |
| wall tamper restore | 3341 |
| expansion module tamper restore | 3341 |
| 24 Hour restore | 3354 |
| 24 Hour restore Cell(RF Jam) | 3354 |
| 24 Hour restore(Lan Fault) | 3354 |
| Comm Path Supervision Restore | 3358 |
| Fire Trouble Restored | 3373 |
| Cross zoneTrouble Restore | 3378 |
| Sensor Trouble Restore | 3380 |
| open circuit trouble restore | 3383 |
| Sensor Tamper Restore | 3383 |
| bell aux tamper restore | 3383 |
| open circuit trouble restore | 3383 |
| constant voltage trouble restore | 3383 |
| short circuit trouble restore | 3383 |
| Smoke Detector High Sensitivity Restored | 3385 |
| Smoke Detector Low Sensitivity Restored | 3386 |
| Partition Full event | 3401 |
| Auto Armed | 3403 |
| Alarm cancel event | 3406 |
| arm instant | 3441 |
| Partition Partset instant event | 3441 |
| Early Armed | 3451 |
| Late Armed | 3452 |
| Rearm after alarm | 3463 |
| Zone Unbypassed | 3570 |
| Fire Zone Unbypassed | 3571 |
| Panic Zone Unbypassed | 3572 |
| Unbypass Panic | 3573 |

| | |
|---|---|
| Burglary walk test end | 3607 |
| Burglary Zone detected fault during walk test | 3613 |
| Burglary Zone restored during walk test | 3613 |

### 11.4.2 Zone Identifiers

The system will send either a user identifier or a zone identifier together with the event code. The zone identifiers are defined as follows:

| Event | Zone ID |
|---|---|
| Event related to IB2 peripherals | 8xx range* |
| Event related to reader zones | 7xx range** |
| Primary path supervision fault | 951 |
| Primary path supervision fault restore | 951 |
| Secondary path supervision fault | 952 |
| Secondary path supervision fault restore | 952 |
| ATS fault | 950 |
| ATS fault restore | 950 |
| Event reporting failure | 960 |
| Event reporting failure restore | 960 |

*Range xx is the IB2 peripheral identifier (01–92).

**Range xx is the reader identifier

# 11.5 MPI Events and SIA Codes

| MPI Event | SIA Code |
|---|---|
| AC Restoral | AR |
| Fuse Restoral | AR |
| Aux rail restore | AR |
| AC Loss | AT |
| Fuse Failure detected | AT |
| High voltage condition detected | AT |
| Low voltage condition detected | AT |
| Alarm audible | BA |
| Alarm perimeter | BA |
| Alarm interior | BA |
| Alarm 24 hour | BA |
| Alarm entry exit | BA |
| Burglary bypass | BB |
| Burglary cancel | BC |
| Cross zone Trouble | BG |
| Cross zone Trouble Restore | BJ |
| Cross zone alarm | BM |
| Alarm audible restore | BR |
| Alarm restore event | BR |
| Alarm perimeter | BR |
| Alarm interior restore | BR |
| Alarm 24 hour restore | BR |
| Alarm entry exit restore | BR |
| Burg Bypass restore | BU |
| Intrusion Verifier | BV |
| Auto Armed | CA |
| Late Armed | CJ |
| Early Armed | CK |
| Partition Full event | CL |
| Remote Arm | CQ |
| Recent close | CR |

| | |
|---|---|
| Failed to Arm/close the system with in Access Window | CI |
| Door Forced open | DF |
| Lockout -multiple attempt failure tamper | DK |
| Door Forced open restore | DR |
| Door Propped open restore | DR |
| Door Propped open | DT |
| Exit error alarm | EE |
| Fire Alarm | FA |
| Carbon Monoxide Detected | GA |
| Fire silence | FC |
| CO silence | FC |
| Fire Trouble Restored | FJ |
| Fire Alarm Restored | FR |
| Carbon Monoxide Detector Restored | GR |
| Fire Trouble | FT |
| Duress PIN entered | HA |
| 24 Hour silent holdup alarm | HA |
| Hold up Bypass | HB |
| Hold up Trouble Restore | HJ |
| 24 Hour silent holdup alarm restore | HR |
| Hold up Trouble | HT |
| Unbypass Panic | HU |
| Panic Verify | HV |
| 24 Hour restore | IA |
| 24 Hour trouble | IR |
| Medical Alarm | MA |
| Medical Bypass | MB |
| Medical Trouble Restore | MJ |
| Medical Alarm Restored | MR |
| Medical Trouble | MT |
| Medical Unbypass | MU |
| 24 Hour restore Cell(RF Jam) | NR |
| 24 Hour restore(Lan Fault) | NR |
| 24 Hour trouble Cell (RF Jam) | NT |

| | |
|---|---|
| 24 Hour trouble(Lan  Fault) | NT |
| Auto Disarmed | OA |
| Untyped alarm is silenced | OC |
| Panic alarm is silenced | OC |
| tamper alarm is silenced | OC |
| panic alarm is silenced at area level by user | OC |
| Late Disarmed | OJ |
| Early Armed | OK |
| Partition  unset event | OP |
| Remote Disarm | OQ |
| Area Reset | OR |
| Panic Alarm | PA |
| Panic Zone Bypassed | PB |
| Sensor Trouble Restore | PJ |
| Panic Alarm Restored | PR |
| Sensor Trouble | PT |
| Panic Zone Unbypassed | PU |
| panel program entry | RB |
| Automated Test/outbound connection  is established | RP |
| panel program exit | RS |
| Manual Test/outbound connection is established | RX |
| Open circuit tamper alarm | TA |
| Communication failure alarm | TA |
| Tamper alarm | TA |
| Exp mod tamper caused by mod  missing | TA |
| Aux tamper alarm | TA |
| Expansion module tamper alarm | TA |
| Open circuit tamper alarm restore | TR |
| Communication failure alarm restore | TR |
| Exp mod tamper caused by mod  missing alarm restore | TR |
| Aux tamper alarm restore | TR |
| Expansion module tamper alarm restore | TR |
| Tamper Bypass | TB |
| Burglary walk test end | TE |

| | |
|---|---|
| Open circuit trouble restore | TT |
| Tamper alarm restore | TJ |
| Modules missing restore | TJ |
| Wall tamper restore | TJ |
| Sensor Tamper Restore | TJ |
| Aux tamper restore | TJ |
| Burglary walk test started | TS |
| Module missing | TT |
| Wall tamper | TT |
| Sensor Tamper | TT |
| Aux tamper trouble | TT |
| Tamper unbypass | TU |
| Comm Path Supervision Fault | YC |
| Comm Path Supervision Restore | YK |
| Battery Failure restored | YR |
| Fuse for Battery Failure restored | YR |
| Battery charger restored | YR |
| Battery Failure detected | YT |
| Low battery | YT |
| Fuse for Battery Failure detected | YT |
| Low System Battery | YT |
| Battery charger Failed | YT |

CHAPTER

# 12 SPECIFICATIONS

## 12.1 MPI Control Panel

MPIP2000 Series (MPIP2000E, MPIP2100E), MPIP3000 Series (MPIP3000E, MPIP3100E[1])
Intended for mounting in an MPI Cabinet.

| | |
|---|---|
|  | ***Note:*** *All interconnections on the MPI control panel are specific wired connections as defined in EN 50131-3 Annex A.* |

## 12.1.1 Specifications

| Board power | | |
|---|---|---|
| Input voltage | 14 VDC nominal (13.6–14.5 VDC) | |
| Current consumption, typical[2] | MPIP2000E series: 230 mA<br>MPIP3000E series: 270 mA | |
| Current consumption, max.[3] | MPIP2000E series: 290 mA<br>MPIP3000E series: 400 mA | |
| Backup battery | Up to 2 x 12 VDC sealed lead acid (SLA) battery | |
| Recommended batteries | Yuasa NP7-12FR (7A Ah) / Yuasa NP17-12IFR (17 Ah) / Yuasa NP18-12FR (17.2 Ah)<br>For permitted combinations, see specification for the cabinet:<br>MPI Cabinet, page 165 | |
| Battery protection | System has protection for charging and reverse polarity connection. | |
| Battery low voltage[4] | 11.2 VDC | |
| Battery deep discharge protection[5] | 10.5 VDC | |

MPIP3100E model will be available soon

Typical current consumption is for the panel circuit board only and does not include any current drawn from the auxiliary outputs.

Max. current consumption is for the panel circuit board only and does not include any current drawn from the auxiliary outputs.

The voltage at which the system will issue the low battery warning.

The voltage at which the system will disconnect the backup batteries from the circuit.

| Minimum supported battery voltage[1] | 9.5 VDC |
|---|---|
| Zones (inputs) (x 10) | |
| Voltage | 3.3 VDC |
| Resistance tolerance | 1 % max. |
| V-Plex | |
| Voltage | 8.5–14 VDC (fluctuating) |
| Current (max.) | 128 mA (each; second V-Plex loop available on MPIP3000 Series only) |
| Auxiliary outputs | |

| | |
|---|---|
| Power rating | 13.8 VDC nominal (10.2–14.4 VDC)<br>In the event of a failure, overvoltage protection will operate at<br>16.5 VDC. |
| AUX 1 (AUX1, IB2 bus 1) | MPIP2000E series: 1.5 A max. / MPIP3000E series: 1.1 A max. |
| AUX 2 (AUX2, IB2 bus 2) | MPIP2000E series: not fitted / MPIP3000E series: 1.1 A max. |
| AUX 3 (Ext. siren, 4G/ LTE module) | MPIP2000E series: 1.1 A max. / MPIP3000E series: 1.1 A max. |
| Total current available for AUX outputs | The combined load from all auxiliary outputs and devices depends on panel model and battery capacity, and must not exceed the maximums as given in the table in *Current Ratings<XREF>* on page 165<XREF>. |
| Auxiliary low power output fault | 10.0 VDC |
| Auxiliary high power output fault | 14.5 VDC |
| Circuit protection | All circuits are power limited using PTCs. |
| Low-voltage trigger outputs (x 4) | |
| Trigger output voltage | 13.8 VDC (0 VDC with switched) |
| Max. current | 300 mA per output |
| Relay outputs | |
| Relay 1<br>Relay 2 (where fitted) | Voltage free; contact rating 28 VDC, 2.8 A max.; resistive loads |
| Communication | |
| On-board Ethernet | EN 50136-1 SP5 (Single Path Ethernet) |

1 The voltage at which the system will treat the battery as if it is not there and will not recharge it.

| | |
|---|---|
| With optional LTE module MPIPCLTEE | EN 50136-1 DP4 (Dual Path Ethernet Primary/Cell Radio Secondary)<br>SP3 (Single Path Cell Radio) |
| Encryption | TLS V1.2BC |
| Communication method | Pass-through (Ref. EN 50136-2 Section 6.1.3) |

| | |
|---|---|
| IP alarm receiver | Maxpro receiver software package or other receiver compatible with Honeywell ISOM protocol or native SIA DC-09 IP protocol in control panel with SIA DC-03 message format.<br>**Note**: Use IP receivers only; dial-up receivers are not suitable. |
| Environmental | |
| Operating temperature | –10 to +50 °C / Indoor use only |
| Humidity | Max. 93% RH non-condensing |
| Ingress and impact protection | See specification for the cabinet: *MPI Cabinet* on page 166<XREF>. |
| Physical | |
| Dimensions (W x D x H) | Including cabinet: 36 cm x 41 cm x 11 cm<br>Without cabinet: 28 cm x 14.5 cm x 4.2 cm (including mounting bracket)<br>As shipped: 35.6 cm x 19.5 cm x 7.8 cm |
| Weight | MPIP2000E series: 502 g; MPIP3000E series: 535 g<br>As shipped: MPIP2000E series: 833 g; MPIP3000E series: 865 g |

**Compliance**

This product has been tested for compliance by BRE Global Ltd. UK to: EN 50131-3:2009 Grade 3, Environmental Class II

EN 50131-6:2017 Type A

EN 50136-2:2013 Category SP5 (Single Path Ethernet), DP4 (Dual Path Ethernet Primary/Cell Radio Secondary), SP3 (Single Path Cell Radio)

EN 50131-10:2014 Type Z

when used in conjunction with MAXPRO Intrusion enclosure MPIBXM35. Note: The MPIP3100E control panel is not part of certification.

## 12.1.2 Current Ratings

The table below lists the advised loads to meet regulations based on using a battery at 100% capacity and allowing for activation of a sounder as per the regulation. Loads need to be adjusted if the battery is at less than 100%. There is no restriction other than the permitted load on capacity of battery used.

For the purposes of calculation, an allowance of 400 mA to activate the sounder has been included, but not the standby current of the sounder. When calculating the total load, remember to include the standby current of the sounder.

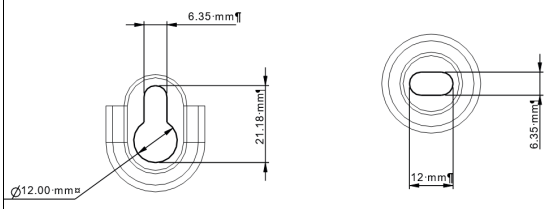
| Battery Capacity | 7 Ah | 14 Ah | 17/18 Ah | 36 Ah |
|---|---|---|---|---|
| EN Grade 3; recharge 24 h | – | 210 mA | 350 mA | 950 mA |

| | |
|---|---|
| | **Note:** *For 36 Ah battery capacity, you need to install 2 x 18 Ah batteries. You will need a second tamper-protected cabinet to house the second battery. You connect the second battery to the Battery 2 terminals on the control panel in the first cabinet.* |

## 12.2 MPI Cabinet

MPIBXM35

Type A power supply as per EN 50131-6 when used with MPI Control Panel (MPIPxxxx) or MPI Remote Power Supply (MPIPSU35)

| Electrical | |
|---|---|
| Input voltage (AC power supply) | 110–230 VAC; 50–60 Hz |
| DC output | 13.8 VDC ± 1% |
| Ripple (max.) | 120 mVp-p |
| Recommended batteries | Yuasa NP7-12FR (7 Ah); up to 2, or Yuasa NP17-12IFR (17 Ah) x 1, or Yuasa NP18-12FR (17.2 Ah) x 1 |
| Physical | |
| Dimensions (H x W x D) | 41 cm x 36 cm x 11 cm<br>As shipped: 43.5 cm x 37.5 cm x 11.5 cm |
| Mounting holes |  |

| | |
|---|---|
| Weight | 5.1 kg approx. (includes AC power adapter) As shipped: 5.4 kg approx. |
| Operating temperature | –10 to +50 °C / Indoor use only |
| Humidity | Max. 93% RH non-condensing |
| Ingress and impact protection | EN 60529:1992+A2:2013: IP30* / EN 62262:2002: IK06* |

The installation must be in accordance with local regulations and must conform to EN62368-1.

| | |
|---|---|
|  | ***Note:*** ** Certification test is in progress.* |

The AC power adapter does not contain any user serviceable components. No further calibration checks or adjustments are required.

For correct installation of the off-wall tamper switch, see Mounting the Cabinet, page 30.

**Compliance**

This product has been tested for compliance by BRE Global Ltd. UK to: EN 50131-3:2009 Grade 3, Environmental Class II when used with certified MAXPRO Intrusion control panels or peripherals.

# 12.3 MPI Remote Power Supply

MPIPSU35

Intended for mounting in an MPI Cabinet.

## 12.3.1 Specifications

| Board power | |
|---|---|
| Input voltage | 14 VDC nominal (13.6–14.5 VDC) |
| Idle current[1] | 35 mA |
| Max. current[2] | 35 mA |
| Backup battery | Up to 2 x 12 VDC sealed lead acid (SLA) battery |

Idle current consumption is for the RPS circuit board only and does not include any current drawn from the auxiliary outputs.

Maximum current consumption is for the RPS circuit board only and does not include any current drawn from the auxiliary outputs.

| | |
|---|---|
| Recommended batteries | Yuasa NP7-12FR (7A Ah) / Yuasa NP17-12IFR (17 Ah) / Yuasa NP18-12FR (17.2 Ah)<br>For permitted combinations, see specification for the cabinet: MPI Cabinet, page 165. |
| Battery protection | System has protection for charging and reverse polarity connection. |
| Battery low voltage[1] | 11.2 VDC |
| Battery deep discharge protection[2] | 10.5 VDC |

| | |
|---|---|
| Minimum supported battery voltage[3] | 9.5 VDC |
| Auxiliary outputs | |
| AUX1, AUX2 | 13.8 VDC nominal (10.2–14.4 VDC)<br>In the event of a failure, overvoltage protection will operate at<br>16.5 VDC.<br>1.5 A max. per auxiliary output |
| Total current available for AUX outputs | The combined load from all auxiliary outputs and devices depends on battery capacity, and must not exceed the maximums as given in the table in *Current Ratings* on page 169<XREF>. |
| AUX low power output fault | 10.0 VDC |
| AUX high power output fault | 14.5 VDC |
| Circuit protection | All circuits are power limited using PTCs. |
| Low-voltage trigger outputs (x 4) | |
| Trigger output voltage | 13.8 VDC (0 VDC with switched) |
| Max. current | Triggers 1–3: 75 mA per output<br>Trigger 4: 250 mA |
| Environmental | |
| Operating temperature | –10 to +50 °C / Indoor use only |
| Humidity | Max. 93% RH non-condensing |
| Ingress and impact protection | See specification for the cabinet: *MPI Cabinet* on page 166<XREF>. |

The voltage at which the system will issue the low battery warning.

The voltage at which the system will disconnect the backup batteries from the circuit.

The voltage at which the system will treat the battery as if it is not there and will not recharge it.

| Physical | |
|---|---|
| Dimensions (W x D x H) | 15.7 cm x 12.7 cm x 4.2 cm<br>As shipped: 23.5 cm x 16.3 cm x 7.5 cm |
| Weight | 250 g<br>As shipped: 440 g |

**Compliance**

This product has been tested for compliance by BRE Global Ltd. UK to: EN 50131-3:2009 Grade 3, Environmental Class II

EN 50131-6:2017 Type A

when used in conjunction with certified MAXPRO Intrusion enclosure MPIBXM35.

### 12.3.2 Current Ratings

The table below lists the advised loads to meet regulations based on using a battery at 100% capacity and allowing for activation of a sounder as per the regulation. Loads need to be adjusted if the battery is at less than 100%. There is no restriction other than the permitted load on capacity of battery used.

For the purposes of calculation, an allowance of 400 mA to activate the sounder has been included, but not the standby current of the sounder. When calculating the total load, remember to include the standby current of the sounder.

| Battery Capacity | 7 Ah | 14 Ah | 17/18 Ah | 36 Ah |
|---|---|---|---|---|
| EN Grade 3; recharge 24 h | 190 mA | 425 mA | 525 mA | 1150 mA |

| | |
|---|---|
| | ***Note:*** *For 36 Ah battery capacity, you need to install 2 x 18 Ah batteries. You will need a second tamper-protected cabinet to house the second battery. You connect the second battery to the Battery 2 terminals on the control panel in the first cabinet.* |

## 12.4 MPI Keypad

Keypads MPIKTSMF, MPIKTSPRX

| Electrical | |
|---|---|
| Input voltage | 13.8 VDC nominal (10–14.5 VDC) |
| Current, idle | MPIKTSMF: 100 mA / MPIKTSPRX: 75 mA |
| Current, max. (display and buzzer on) | MPIKTSMF: 130 mA / MPIKTSPRX: 110 mA |
| Sounder | Full Power, -3 dB, -6 dB, and -9 dB (85 dB at 10 cm) |
| Card support | |

| | |
|---|---|
| MPIKTSMF card types | MIFARE (Classic 32-bit and DES-Fire 56-bit); reading CSN only<br>MIFARE DESFire EV2 cards and keyfobs (recommended LuminAXS 38-bit preprogrammed with diversi-fied key encryption)<br>EM4102 ASK 125 kHz; up to 40 bits |
| MPIKTSPRX card types | EM4102 ASK 125 kHz; up to 40 bits |
| Environmental | |
| Operating temperature | –10 to +50 °C / Indoor use only |
| Humidity | Max. 93% RH non-condensing |
| Ingress and impact protection | EN 60529:1992+A2:2013: IP30*<br>EN 62262:2002: IK06* |
| Physical | |
| Dimensions (W x H x D) | 8.45 cm x 13.96 cm x 4.01 cm<br>As shipped: 9.3 cm x 16.7 cm x 5 cm |
| Weight | 169 g<br>As shipped: 244 g |
| Other | |
| Ancillary Control Equipment (ACE) | Type B |
| Options | MPIKW1: MAXPRO Intrusion Key-pad Wall Mounting Plate |

### Compliance

This product has been tested for compliance by BRE Global Ltd. UK to: EN 50131-3:2009 Grade 3, Environmental Class II.

| | |
|---|---|
|  | **Caution:** ***The MPIKW1 keypad wall mounting plate is not part of the certification. Use of the mounting plate will render the system non- compliant with EN 50131-3 .*** |

Option: Keypad Wall Mounting Plate MPIKW1

| | |
|---|---|
| Dimensions (W x D x H) | 17.8 cm x 17.6 cm x 0.5 cm<br>As shipped: 17.8 cm x 17.8 cm x 3.5 cm |
| Weight | 47 g<br>As shipped: 90 g |

# 12.5 MPI Door Control Module

MPIDC1

| Board power | |
|---|---|
| Input voltage | 13.8 VDC nominal (10–14.5 VDC) |
| Current, idle | 60 mA |
| Current, max.[1] | 185 mA (relays active) |
| Access control | |
| Reader power | 13.7 VDC; 1 A |
| Wiegand data | 5 VDC |
| Card types | Wiegand:<br>• HID cards: 26, 32, 34, 35, and 48 bit<br>• MIFARE cards: Classic 32 bit and DESFire 56 bit; reading CSN only<br>• MIFARE DESFire EV2 cards and keyfobs (with luminAXS readers), recommended LuminAXS 38-bit preprogrammed with diversified key encryption)<br>• EM4102 ASK 125 kHz; up to 40 bits.<br>**Note**: Card type is set on site level (all DCMs in the site). |

- Max. current consumption is for the DCM circuit board only and does not include any current drawn from the auxiliary outputs / relays.

| Relays | |
|---|---|
| Door Strike/Lock | 12–30 VDC; 3 A max. ('dry contact'); dedicated for door lock (magnetic lock or door strike).<br>Current-limited to 1.5 A with 12 VDC on NC/NO PIN ('wet contact') |
| Trigger outputs (x 4) | |
| LED R, LED Y, LED G, BUZZ | 50 mA each (switch to ground); |
| Zones (inputs) | |
| RTE (request to exit) | Default triple balanced |
| DSM (door status monitor) | Default triple balanced |
| Environmental | |

| | |
|---|---|
| Operating temperature | –10 to +50 °C / Indoor use only |
| Humidity | Max. 93% RH non-condensing |
| Ingress and impact protection | EN 60529:1992+A2:2013: IP30*/ EN 62262:2002: IK06* |
| Physical | |
| Dimensions (W x D x H) | With enclosure: 18 cm x 14 cm x 4 cm Without enclosure: 13 cm x 8.6 cm x 2.6 cm As shipped: 21.5 cm x 15.0 cm x 4.5 cm |
| Weight | With enclosure: 356 g Without enclosure: 120 g As shipped: 453 g |
| Other | |
| Ancillary Control Equipment (ACE) | Type B |

**Compliance**

This product has been tested for compliance by BRE Global Ltd. UK to: EN 50131-3:2009 Grade 3, Environmental Class II.

## 12.6 MPI Relay Module

MPIEOP4

| Board power | |
|---|---|
| Input voltage | 13.8 VDC nominal (10–14.5 VDC) |
| Current, idle | 15 mA |
| Current, max.[1] | 185 mA (relays active) |
| Relays (x 4) | Contact rating 28 VDC; max. 2.8 A (resistive load) |
| **Environmental** | |
| Operating temperature | –10 to +50 °C / Indoor use only |
| Humidity | Max. 93% RH non-condensing |
| Ingress and impact protection | EN 60529:1992+A2:2013: IP30* / EN 62262:2002: IK06* |
| **Physical** | |
| Dimensions (W x H x D) | With enclosure: 14.6 cm x 14.6 cm x 3.4 cm As shipped: 17.5 cm x 15.5 cm x 4.0 cm |
| Weight | With enclosure: 256 g As shipped: 332 g |

| Other | |
|---|---|
| Ancillary Control Equipment (ACE) | Type B |

1 Max. current consumption is for the Relay Module circuit board only and does not include any current drawn from the relays

**Compliance**

This product has been tested for compliance by BRE Global Ltd. UK to: EN 50131-3:2009 Grade 3, Environmental Class II.

## 12.7 MPI Zone Expander

MPIEIO84E

| Board power | |
|---|---|
| Input voltage | 13.8 VDC nominal (10–14.5 VDC) |
| Current, idle | 35 mA |
| Current, max. | 60 mA (all zones active) |
| Zones (inputs) (x 8) | |
| Voltage | 3.3 VDC |
| Resistance tolerance | 1 % max. |

1 Max. current consumption is for the Relay Module circuit board only and does not include any current drawn from the relays.

| Trigger outputs (x 4) | |
|---|---|
| Trigger voltage | 13.7 VDC (0 VDC with switched) |
| Max. current (per output) | 180 mA |
| Environmental | |
| Operating temperature | –10 to +50 °C / Indoor use only |
| Humidity | Max. 93% RH non-condensing |
| Ingress and impact protection | EN 60529:1992+A2:2013: IP30* / EN 62262:2002: IK06* |
| Physical | |
| Dimensions (W x H x D) | With enclosure: 14.6 cm x 14.6 cm x 3.4 cm As shipped: 17.5 cm x 15.5 cm x 4.0 cm |
| Weight | With enclosure: 263 g As shipped: 341 g |
| Other | |

| | |
|---|---|
| Ancillary Control Equipment (ACE) | Type B |

**Compliance**

This product has been tested for compliance by BRE Global Ltd. UK to: EN 50131-3:2009 Grade 3, Environmental Class II.

## 12.8 MPI Transceiver (RF Portal)

| Specifications | |
|---|---|
| Width | 164mm |
| Height | 152mm |
| Dept | 39mm |
| Weight of housing + PCBA | 250g |
| Weight of PCB only | 45g |
| Humidity | 0-85% |
| Operating temperature | -10°C to +40°C |
| Nominal Supply voltage | 12V DC |
| Current: Nominal | 35mA |
| Current: Maximum | 40mA |

**Compliance**

This product has been certified by BRE Global Ltd. UK to: EN 50131-3:2009 and EN 50131-5-3:2017 Grade 2, ACE Type B, Environmental Class II.

## 12.9 MPI 4G/LTE Module

MPICLTEE

Intended for mounting in an MPI Cabinet.

| LTE module | |
|---|---|
| Input voltage | 14 VDC nominal (13.85–14.5 VDC) |
| Current, idle | 45 mA |
| Current, max. (transmitting) | 240 mA |
| Frequency bands | LTE Category 1 2G GSM LTE Bands: 1, 3, 8, 20, 28<br>2G GSM Bands: GSM 900 and DCS 1800 |

| | |
|---|---|
| SIM Card | 2FF mini-SIM<br>SIM card not included; please purchase and activate a SIM card from your preferred provider. |
| Antennas (x 2) | |
| Type | Wideband, Dipole 4G LTE |
| Frequencies | 698–960 MHz, 1575.42 MHz, 1710–2700 MHz |
| Polarization | Linear |
| Peak gain | 3 dBi |
| VSWR | < 2:1 |
| Impedance | 50 Ohms |
| Connector type | SMA-M, Hinged |
| Environmental | |
| Operating temperature | –10 to +50 °C / Indoor use only |
| Humidity | Max. 93% RH non-condensing |
| Physical | |
| Dimensions (W x H x D) | LTE module: 97.6 mm x 108 mm x 25.4 mm Each antenna: 168.4 mm x 49 mm<br>As shipped: 24.5 cm x 16.5 cm x 8 cm |
| Weight | LTE module: 97 g As shipped: 393 g<br>Each antenna: 45.3 g |

### Compliance

This product has been tested for compliance by BRE Global Ltd. UK to: EN 50136-2:2013 (For category, please see the installation guide for the certified Control Panel.)

EN 50131-10:2014 Type Y when used with certified MAXPRO Intrusion MPIP Control Panel in MPIBXM35 enclosure.

# 12.10 Cable Type Requirements

| Function | Signal(s) | Type | Max. Length | Interior / Exterior |
|---|---|---|---|---|
| AC power | 110/230 VAC | As per local laws and regulations | | Interior |

| | | | | |
|---|---|---|---|---|
| Zone | Sensor contact input | Twisted pair or better (core min. 0.182 mm² / 24 AWG) | 100 m / 328 ft | Interior |
| Inter unit wiring | IB2 | ▪ 4-core alarm cable (22/4 STR CM/CL2);<br>100 ohms/km max.<br>▪ CAT5E UTP 24 AWG. | 3.65 km / 12,000 ft (see also note below) | Interior |
| | V-Plex | See Limitations of V-Plex Cable Runs, page 108. | | Interior |
| Ethernet | | CAT5E shielded | 100 m / 328 ft | Interior |
| Aerial extension leads[1] | 4G LTE | 50 ohm low-loss SMA M to F coaxial | As per cable manufac-turer's rec-ommendatio n | Interior |
| External siren (SAB) | Power, trigger, tamper, and fault | As per manufac-turer's recommenda-tion | 100 m / 328 ft | Interior |

1: The aerial extension cables are not part of the LPCB approval.

| | |
|---|---|
|  | **Caution:** ***IB2 bus wiring: Use of other types of cables than those listed are at the installer's risk .*** |

This page is intentionally left blank.

CHAPTER

# 13 GLOSSARY

| | |
|---|---|
| ARC | Alarm Receiving Centre |
| ATP | Alarm Transmission Path |
| ATS | Alarm Transmission System |
| CMS | Central Monitoring Station |
| CSN | Card Serial Number |
| DCM | Door Control Module |
| Entry delay | Entry delay defines the delay time that allows users to enter the premises through a door that has been programmed as an entry delay door and disarm the system without setting off an alarm. The system must be disarmed within this period or an alarm will occur. |
| EOLR | End of Line Resistor |
| Exit delay | Exit delay defines the delay time that allows users to leave the premises through a door that has been programmed as an entry/exit delay door after arming the system without setting off an alarm. The user must leave within this period or an alarm will occur. |
| MPC | MAXPRO Cloud |
| MPI | MAXPRO Intrusion |
| RPS | Remote Power Supply |
| PTC | Positive Temperature Coefficient. PTC thermistors protect against over-current. |
| SPPS | Supplementary Prime Power Source |
| VSWR | Voltage Standing Wave Ratio |

CHAPTER

# 14 LIMITATIONS OF THE ALARM SYSTEM

WARNING!

THE LIMITATIONS OF THIS ALARM SYSTEM

While this System is an advanced wireless security system, it does not offer guaranteed protection against burglary, fire or other emergency. Any alarm system, whether commercial or residential, is subject to compromise or failure to warn for a variety of reasons. For example:

- Intruders may gain access through unprotected openings or have the technical sophistication to bypass an alarm sensor or disconnect an alarm warning device.
- Intrusion detectors (e.g., passive infrared detectors), smoke detectors, and many other sensing devices will not work without power. Battery-operated devices will not work without batteries, with dead batteries, or if the batteries are not put in properly. Devices powered solely by AC will not work if their AC power supply is cut off for any reason, however briefly.
- Signals sent by wireless transmitters may be blocked or reflected by metal before they reach the alarm receiver. Even if the signal path has been recently checked during a weekly test, blockage can occur if a metal object is moved into the path.
- A user may not be able to reach a panic or emergency button quickly enough.
- While smoke detectors have played a key role in reducing residential fire deaths in the United States, they may not activate or provide early warning for a variety of reasons in as many as 35% of all fires, according to data published by the Federal Emergency Management Agency. Some of the reasons smoke detectors used in conjunction with this System may not work are as follows. Smoke detectors may have been improperly installed and positioned. Smoke detectors may not sense fires that start where smoke cannot reach the detectors, such as in chimneys, in walls, or roofs, or on the other side of closed doors. Smoke detectors also may not sense a fire on another level of a residence or building. A second floor detector, for example, may not sense a first floor or basement fire. Finally, smoke detectors have sensing limitations. No smoke detector can sense every kind of fire every time. In general, detectors may not always warn about fires caused by carelessness and safety hazards like smoking in bed, violent explosions, escaping gas, improper storage of flammable materials, overloaded electrical circuits, children playing with matches, or arson.

Depending on the nature of the fire and/or location of the smoke detectors, the detector, even if it operates as anticipated, may not provide sufficient warning to allow all occupants to escape in time to prevent injury or death.

- Passive Infrared Motion Detectors can only detect intrusion within the designed ranges as diagrammed in their installation manual. Passive

Infrared Detectors do not provide volumetric area protection. They do create multiple beams of protection, and intrusion can only be detected in unobstructed areas covered by those beams. They cannot detect motion or intrusion that takes place behind walls, ceilings, floors, closed doors, glass partitions, glass doors, or windows. Mechanical tampering, masking, painting or spraying of any

material on the mirrors, windows or any part of the optical system can reduce their detection ability. Passive Infrared Detectors sense changes in temperature; however, as the ambient temperature of the protected area approaches the temperature range of 90º to 105ºF (32º to 40ºC), the detection performance can decrease.

- Alarm warning devices such as sirens, bells or horns may not alert people or wake up sleepers if they are located on the other side of closed or partly open doors. If warning devices are located on a different level of the residence from the bedrooms, then they are less likely to waken or alert people inside the bedrooms. Even persons who are awake may not hear the warning if the alarm is muffled by noise from a stereo, radio, air conditioner or other appliance, or by passing traffic. Finally, alarm-warning devices, however loud, may not warn hearing-impaired people.
- Telephone lines needed to transmit alarm signals from a premise to a central monitoring station may be out of service or temporarily out of service. Telephone lines are also subject to compromise by sophisticated intruders.
- Even if the system responds to the emergency as intended, however, occupants may have insufficient time to protect themselves from the emergency situation. In the case of a monitored alarm system, authorities may not respond appropriately.

This equipment, like other electrical devices, is subject to component failure.

Even though this equipment is designed to last as long as 20 years, the electronic components could fail at any time.

The most common cause of an alarm system not functioning when an intrusion or fire occurs is inadequate maintenance. This alarm system should be tested weekly to make sure all sensors and transmitters are working properly. The security keypad (and remote keypad) should be tested as well.

Wireless transmitters (used in some systems) are designed to provide long battery life under normal operating conditions. Longevity of batteries may be as much as 4 to 7 years, depending on the environment, usage, and the specific wireless device being used. External factors such as humidity, high or low temperatures, as well as large swings in temperature, may all reduce the actual battery life in a given installation. This wireless system, however, can identify a true low battery situation, thus allowing time to arrange a change of battery to maintain protection for that given point within the system.

Installing an alarm system may make the owner eligible for a lower insurance rate, but an alarm system is not a substitute for insurance. Homeowners, property owners and renters should continue to act prudently in protecting themselves and continue to insure their lives and property. We continue to develop new and improved protection devices. Users of alarm systems owe it to themselves and their loved ones to learn about these developments.

CHAPTER

# 15 COMPLIANCE AND APPROVALS

## 15.1 EU Directives

- Low Voltage Directive 2014/35/EU
- Radio Equipment Directive 2014/53/EU
- Electromagnetic Compatibility Directive 2014/30/EU
- RoHS Directive 2011/65/EU.

## 15.2 Product Standards

For particular CE standards and RoHS compliance, please see the product's Declaration of Conformity (DoC). The DoC is available at www.mywebtech.com.

For compliance statements of each the MPI modules, see *Specifications*, page 161.

## 15.3 Product Certification

### Product Certification (EU)


Cert/LPCB ref. 042ce.

For information on product certification and requirements, see the quick install guides of the individual MAXPRO Intrusion devices and read all of section 15.

# 15.4 Instructions for Compliance

**EN** If you leave the system with the customer in a non-compliant condition, you must remove any product labels stating compliance.

If the customer account has multiple sites, you must check the settings for all sites. If a customer site has multiple control panels, you must check the setting for all control panels.

## 15.4.1 Control Panel Settings

### *System Supervision Controls*

The system supervision controls allow you to choose which parts of the system you want to supervise. For example, if you are not using a V-Plex loop, you can switch off supervision to prevent trouble events for the loop.

Switching off supervision options may invalidate compliance with local regulations.

### *Communication Paths*

EN ATS classification according to EN 50136-2: up to SP5 (Single Path Ethernet), DP4 (Dual Path Ethernet Primary/Cell Radio Secondary), SP3 (Single Path Cell Radio) depending on the Path Supervision Period for Primary and Path Supervision Period for Backup settings for the panel in MAXPRO Cloud.

For systems that must meet DP4 (Dual Path Ethernet Primary/Cell Radio Secondary), set Path Supervision Period for Primary to 90 seconds, and Path Supervision Period for Backup to 5 hours. If the primary path fails, the backup path will automatically step up to 90 seconds.

For systems that must meet SP3 (Single Path Cell Radio), set the Path Supervision Period to 30 minutes.

For systems that must meet SP5 (Single Path Ethernet), set the Path Supervision Period to 90 seconds.

Also set the Alarm Reporting Limit (Per Zone) to Unlimited.

### *Communication Delay to the ARC*

Set Communication Delay to ARC to at least 30 seconds.

### *Event Log*

Set Event Log Limit to 3.

### *Restricting Access to the System Configuration*

The customer Administrator must enable the Restrict Installer Mode option in MAXPRO Cloud (control panel setting) before you hand over the system to the customer. This prevents you, the installer, from making any changes in MAXPRO Cloud to the customer's system without their authorisation.

MAXPRO Cloud has an option that allows for changing People's PIN codes after they have been created. For compliance, this option must be disabled. This is the default setting. To verify, go to the customer account in MAXPRO Cloud, to the Settings tab. Under User Settings, make sure that the checkbox Allow PIN Change for all panel users is cleared.

Furthermore, the customer's Administrator must also set the dealer privileges (My sites; tab Settings), defining which operational tasks are allowed for the installer (arming/disarming, acknowledging alarms...). The dealer privileges are valid for all customer sites.

## 15.4.2 Keypad

### *Keypad Settings*

You specify the settings below on control panel level: they are valid for all keypads connected to that control panel.

### *MPIKW1*

The MPIKW1 keypad wall mounting plate is not part of the certification. Use of the mounting plate will render the system non-compliant with EN 50131-3.

### *User ID Settings: Fail Attempt Limit*

For Grade 3 applications, set Fail Attempt Limit to 3 or less.

### *User ID Settings: Lockout Time*

Set Lockout Time to 90 seconds or more.

### *System State Indication*

For systems compliant with EN 50131, the keypad shall not display any details about the system state until a user has logged on to the keypad.

Set Show Alert Details on Arming Station Sleep Screen to Disabled.

### *Logging on to the Keypad*

You shall not use proximity card and tags as the sole means of authorisation on the keypads in an EN 50131 compliant system.

## 15.4.3 DCM Settings

Use the Door Status Monitor (DSM) with the triple-balanced zone supervision. For details, see Triple Balanced, page 42. In MAXPRO Cloud, make sure that Zone Supervision Type for the DSM is set to Triple Balanced. (The default setting is Triple Balanced.)

## 15.4.4 Area Settings

### *Entry Delays*

Set Entry Delay and Entry Delay Extended to 45 seconds or less.

### *Abort Window*

For all areas in the system, set Abort Window (In Seconds) to a minimum of 30 seconds. If not, the system will not be compliant with EN standards.

| | |
|---|---|
|  | **Caution:** ***For EN compliance, the Abort Window must be a minimum of 30 seconds. If not, it will render the system non-compliant to EN 50131-1 .*** |

### *Restart Exit Time*

If enabled when the panel is armed the normal exit delay begins. After the user exits, closes the door and then re-enters the premise, the exit delay time restarts to the programmed value.

| | |
|---|---|
|  | **Caution:** ***Use of this feature will render the system non-compliant with EN 50131-1 standards .*** |

### *Auto-stay Arm on no Exit*

If enabled, this allows the system to automatically arm in stay mode if the exit door is not opened/closed.

| | |
|---|---|
|  | **Caution:** ***Use of this feature will render the system non-compliant with EN 50131-1 standards .*** |

### *Bypassing Zones*

For each area, the setting Remove bypass on disarming allows you to automatically unbypass any bypassed zone in that area when you disarm it. For EN compliance, a bypassed zone shall always be unbypassed automatically.

Set Remove bypass on disarming to Enabled.

| | |
|---|---|
|  | **Note:** *Enabling Force Bypass for user renders the system non-compliant to EN 50131-1.* |

### *Bell Timeout*

Set Bell Timout 15 minutes or less.

Note that local/national requirements may demand a different value. Check your local/national regulations.

### *Automatic Arming/Disarming*

When automatically arming/disarming an area (using an auto arming schedule or a rule), the system can provide a notification indication in advance that the area is about to arm. The keypads that have the area set as home area will start beeping, allowing the users to leave the area before it is armed, and preventing false alarms.

You can set the time of the a notification indication using the Prewarning Period (in Mins) setting for the area. This defines how many minutes before arming the keypads will start to beep. For EN compliance, the setting must not be 0. If you set Prewarning Period (in Mins) to 0, the area will arm without any advance warning. The default setting is 15 minutes.

When using automatic arming/disarming for an area, you must select the Force bypass option for that area. This makes sure that the system can automatically bypass any zones that stop the area from arming, and then arm the area so that it is protected. If a non-bypassable zone stops the area from arming, then the system will not arm the area, and it will notify the CMS that the area is not armed.

***Simple Arm/Disarm***

Simple Arm/Disarm feature enables the end user to easily arm or disarm all areas that they have access to.

When using simple arm/disarm for an area, you must select the Force bypass option for that area. This makes sure that the system can automatically bypass any zones that stop the area from arming, and then arm the area so that it is protected. If a non-bypassable zone stops the area from arming, then the system will not arm the area, and it will notify the CMS that the area is not armed.

| | |
|---|---|
| | ***Note:*** *Simple Arm/disarm for a user can be activated by disabling Area Choice for Arm/Disarm. Enabling Simple Arm/Disarm for user renders the system non-compliant to EN 50131-1* |

### 15.4.5 Using Rules for Automating Tasks

Using Rules (standard Rules or Controller Rules) for automating tasks may render the system non-compliant. Check all the rules that you program for compliance with product standards.

### 15.4.6 Installation Location

You must install all MAXPRO Intrusion modules (cabinets and control panels, keypads, remote power supplies, door control modules, relay modules, and zone expanders) within a secured intrusion area.

## 15.5 Instructions for Compliance – Sweden

### 15.5.1 Compliance with SSF 1014

In MAXPRO Cloud, for each area, set Abort Window (In Seconds) to 0 seconds.

## 15.6 Disclaimer

Honeywell MAXPRO Cloud and MAXPRO Intrusion log-in system is fully compliant with standard (EN 50131). Any other authentication log-in system that might be implemented by the Customer to access to MAXPRO Intrusion, in order to meet the requirements set forth by standard EN50131 must comply with the following requirements:

User password must have at least 100,000 different combinations;

After 3 failed log in attempts the user must be then be subject to a minimum account lockout time of 90 seconds;

Lockout after 3 failed attempts and then, following expiration of a lockout period, lockout after 1 failed attempt;

When any user has been subject to an account lockout, a user specific lockout event needs to be logged in the MAXPRO Intrusion Panel.

Failure to meet the authorisation requirements will render any installed system non-compliant to EN50131-3. Honeywell will not be liable - and customer will hold Honeywell harmful, releasing Honeywell from any claim, consequence and liability - for any unauthorized, fraudulent, unlawful access to MAXPRO Cloud and MAXPRO Intrusion made from any authentication log- in system implemented, maintained and managed by the Customer.

### 15.6.1 Dual Authentication

This feature will provide a higher level of security. Once enabled for an area, any user accessing that area by means of the arming station or card reader will be required to swipe their card and enter a PIN code in any sequence before access is granted.

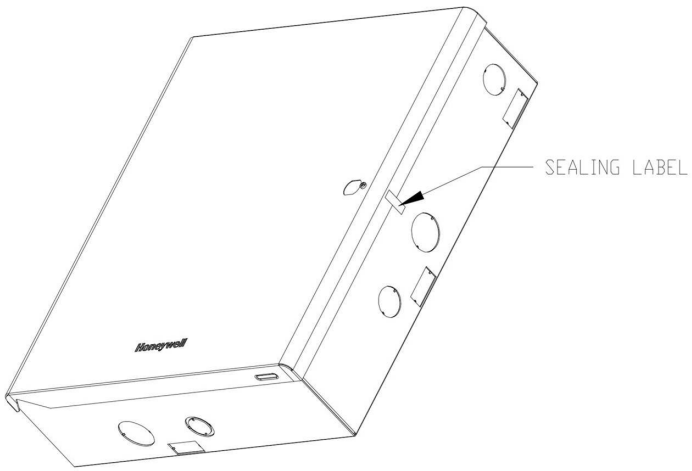
## 15.7 NF&A2P Requirements

### 15.7.1 Sealing Tape

Control units are sealed using non-reusable adhesive security seals reference 800-25741 (a model is supplied with the control unit).

The sealing tape should go over enclosure front cover and base overlap where visible to installer and is used as a tamper security indication.

After the user installs control panel in, close the door, user needs to stick sealing label on the top case and back case as shown.



## 15.7.2 Current requirement listing

The following table lists the maximum current available from AUX outputs to guarantee 60 hours as per NF&A2P Grade 3 standards.

| Control Panels | Battery Quantity | Total Battery Capacity | Maximum current available from AUX outputs | |
|---|---|---|---|---|
| MPIP2xxx | 1 | 17.2 Ah | In standby | 0 mA* |
| | 2 | 34.4 Ah | In standby | 225 mA |
| | | | In alarm | 625 mA |
| MPIP3xxx | 2 | 34.4 Ah | In standby | 185 mA |
| | | | In alarm | 515 mA |
| *__Note__: When only one 17Ah battery is used with the panel, a RPS module (with one or two 17Ah Batteries) can be used for peripherals connection.<br>YUASA NP18-12B (12V / 17.2Ah) used for validation. | | | | |

| Remote Power Supply | Battery Quantity | Total Battery Capacity | Maximum current available from AUX outputs | |
|---|---|---|---|---|
| MPIPSU35 | 1 | 17.2 Ah | In standby | 205 mA |
| | | | In alarm | 345 mA |
| | 2 | 34.4 Ah | In standby | 420 mA |
| | | | In alarm | 1120 mA |
| **Note**: YUASA NP18-12B (12V / 17.2Ah) used for validation. | | | | |

| Battery type (Battery not supplied) |
|---|
| YUASA NP17-12I(FR) (12V/17Ah)<br><br>YUASA NP18-12B (12V/17.2Ah) |

| | |
|---|---|
|  | ***Note:*** *For 36 Ah battery capacity, you need to install 2 x 18 Ah batteries. You will need a second tamper-protected cabinet to house the second battery. You connect the second battery to the Battery 2 terminals on the control panel in the first cabinet.* |

## 15.7.3 Cyber security requirements

| | |
|---|---|
| | **Note:** *The two factor authentication has to be activated in the MPC Web portal to conform with NF&A2P Cyber Security.* |

| | |
|---|---|
| | **Note:** *To conform with IP30, the keypad must be installed at least 10 cm from an outgoing wall corner.* |

### Product Certification (NF&A2P)

**Certification Body**: CNPP Cert.
**Contact Address**: Route de La Chapelle Réanville
CS22265
27950 SAINT MARCEL
**Tel**: +33 (0)2.32.53.63.63
**Fax**: +33 (0)2.32.53.64.46
**Website**: www.cnpp.com
**Email**: *certification@cnpp.com*

**Certification Body**: AFNOR Certification
**Contact Address**: 11, rue Francis de Pressensé
93571 LA PLAINE Saint Denis Cedex
**Tel**: +33 (0)1.41.62.80.00
**Fax**: +33 (0)1.49.17.90.00
**Website**: www.marque-nf.com
**Email**: *certification@afnor.org*

**Certification Process**: NF324-H58 / EN 50131-3 / RTC 50131-3 / EN 50131-6 / RTC 50131-6 / EN 50131-10 / RTC 50131-10 / EN 50136-2 et RTC Cyber

# 15.8 INCERT Requirements

## 15.8.1 Current requirement listing

To fulfill INCERT Grade 3, 60 hr, alternative power supply requirement limits below must be followed.

| Control Panels | Battery Quantity | Total Battery Capacity | Maximum current available from AUX outputs | |
|---|---|---|---|---|
| MPIP2xxx | 1** | 17.2 Ah | In standby | 0 mA* |
| | 2 | 34.4 Ah | In standby | 180 mA |
| | | | In alarm*** | 535 mA |
| MPIP3xxx**** | 2 | 34.4 Ah | In standby | 185 mA |
| | | | In alarm*** | 515 mA |

*__Note__: When only one 17Ah battery is used with the panel, a RPS module (with one or two 17Ah Batteries) can be used for peripherals connection. YUASA NP18-12B (12V / 17.2Ah) used for validation.

**__Note__: INCERT has not evaluated single battery setup.

***__Note__: In alarm, value is only for information. Not covered by INCERT.

****__Note__: Panel configuration related to maximum power consumption.

| Remote Power Supply | Battery Quantity | Total Battery Capacity | Maximum current available from AUX outputs | |
|---|---|---|---|---|
| MPIPSU35 | 1* | 17.2 Ah | In standby | 150 mA |
| | | | In alarm | 375 mA |
| | 2 | 34.4 Ah | In standby | 420 mA |
| | | | In alarm** | 1120 mA |

__Note__: YUASA NP18-12B (12V / 17.2Ah) used for validation.

*__Note__: INCERT has not evaluated single battery setup.

**__Note__: In alarm, value is only for information. Not covered by INCERT.

## 15.8.2 Additional System Settings Requirement

Exit Error must be set to **Disable/Enabled** to conform with INCERT requirements.

CHAPTER

# 16 PARTS LIST

| Part No. | Product Name | Remark |
|---|---|---|
| Control Panels | | |
| MPIP2000E | MAXPRO Intrusion MPIP2000E Controller | Needs cabinet |
| MPIP2100E | MAXPRO Intrusion MPIP2100E Controller | Needs cabinet |
| MPIP3000E | MAXPRO Intrusion MPIP3000E Controller | Needs cabinet |
| MPIP3100E[1] | MAXPRO Intrusion MPIP3100E Controller | Needs cabinet |
| Cabinets with AC Power Adapter | | |
| MPIBXM35 | MAXPRO Intrusion cabinet and PSU; medium-size; 3.5 A | |
| Communication Module | | |
| MPICLTEE | MAXPRO Intrusion 4G/LTE module (Europe) | |
| MAXPRO Cloud | | |
| MPC-I003 | MPC monthly fee for MPI 2000 & MPI 3000 Intrusion Panels management (per panel) | |
| MPC-IDC0 | MPC monthly fee for MPI Door Control Intrusion Panels management (per door) | |
| MAXPRO Receiver Software | | |
| MPICRX | MAXPRO Intrusion Receiver Full Capacity Licence (beyond 100 connections. Trial version also available.) | |
| IB2 Bus Devices | | |
| Expansion Power Supply | | |
| MPIPSU35 | MAXPRO Intrusion expansion PSU 3.5 A | Needs cabinet |
| I/O Wired Expanders | | |
| MPIEIO84E | MAXPRO Intrusion Zone Expander Module, 8 hard-wired zones + 4 triggers | |

| | | |
|---|---|---|
| MPIEOP4 | MAXPRO Intrusion Relay Module, 4 relays | |
| Keypads | | |
| MPIKTSMF | MAXPRO Intrusion Touchscreen Keypad MIFARE | |
| MPIKTSPRX | MAXPRO Intrusion Touchscreen Keypad Proximity | |
| MPIKW1 | MAXPRO Intrusion Keypad Wall Mounting Plate | Optional |

1 MPIP3100E model will be available soon

| Part No. | Product Name | Remark |
|---|---|---|
| Access Control Modules | | |
| MPIDC1 | MAXPRO Intrusion 1 Door Control Module (1 door, up to 2 readers) | |
| Access Readers | | |
| luminAXS | | |
| LU4500BHONA | luminAXS MIFARE Wiegand reader | |
| LU4516BHONA | luminAXS MIFARE 16 key Wiegand reader (with lock/unlock keys) | |
| LU4502BHONA | luminAXS MIFARE 2 key Wiegand reader (with lock/unlock keys) | |
| LU45BHONA | luminAXS MIFARE Wiegand reader (no light ring) | |
| V-Plex Devices[2] | | |
| FG1625SN | Interior Glass Break Detector | |
| 269SN | Hold up switch | |
| Interior Motion Detection and Motion Detection | | |
| DT8016AF4-SN / DT8016AF5-SN | DUAL TEC motion sensor with anti-mask | |
| DT8016MF4-SN / DT8016MF5-SN | DUAL TEC motion sensor | |
| DT8320AF4-SN / DT8320AF5-SN | DUAL TEC ceiling mount motion sensor with mirror optics and anti-mask | |
| DT8320F4-SN / DT8320F5-SN | DUAL TEC ceiling mount motion sensor with mirror optics | |
| IS3016A-SN | Passive Infrared motion sensor with anti-mask | |
| IS3016M-SN | Passive Infrared motion sensor | |
| IS4190-SN | | |

| Other Sensors[3] | | |
|---|---|---|
| 2-Wire Smoke Detectors | | |
| 4190-SN | Two-loop zone expansion module | |
| 1151 | Ionization smoke detector (System Sensor) | |
| 2W-B | Photoelectric smoke detector (System Sensor) | |
| 2WT-B | Photoelectric smoke detector with thermal sensor (System Sensor) | |
| 2151 | Photoelectric smoke detector (System Sensor) | |

Entry reader only; exit reader function will be available soon. Not all listed V-Plex devices may be available in all regions. Check the specifications and security grading in the sensor's datasheet, and contact your local Honeywell Intrusion Sales Representative for availability in your region. Not all listed devices may be available in all regions.

| Part No. | Product Name | Remark |
|---|---|---|
| 2151T | Photoelectric smoke detector with heat sensor (System Sensor) | |
| CO Detectors | | |
| CO1224T | Carbon Monoxide Detector (System Sensor) | |
| CO1224TR | Carbon Monoxide Detector (System Sensor) | |
| Hold-up Devices | | |
| 264 | Hardwired money clip (Resideo) | |
| 266 | Footrail (Resideo) | |
| 268 | Hold-up switch (Resideo) | |
| 269 | Hardwired hold-up switch (Resideo) | |
| 269R | Hardwired hold-up switch, stainless steel (Resideo) | |
| 270R | Hardwired hold-up switch (Resideo) | |
| Alarm Sounders | | |
| AS-121575W | Fire horn/strobe (Wheelock) | |
| P2RK, P4RK | Fire horn/strobe (System Sensor) | |

| Literature | |
|---|---|
| 800-23044-1 | MPI Installation and Setup Guide |
| 800-23040-1 | MPI Control Panel Quick Install Guide |

| | |
|---|---|
| 800-23148-1 | MPI Door Control Module Quick Install Guide |
| 800-23149-1 | MPI Remote Power Supply Quick Install Guide |
| 800-23150 | MPI Keypads Quick Install Guide |
| 800-25981 | MPI Keypad Mounting Plate Quick Install Guide |
| 800-23151-1 | MPI Zone Expander Quick Install Guide |
| 800-23154 | MPI Relay Module Quick Install Guide |
| 800-23041-1 | MAXPRO Intrusion User Guide |
| 800-25485-1 | MPI 4G/LTE Module Quick Install Guide |
| 800-24875-1 | MPI Cabinet Quick Install Guide |
| 800-25507 | MPI Security Manual |
| 800-24096-1 | MAXPRO Cloud Configuration Guide for Installers |
| 800-24095 | MAXPRO Cloud Mobile App Guide |
| 800-24094 | MAXPRO Cloud Quick Start Guide |
| 800-25754-1 | MAXPRO Cloud End User Guide |
| 800-25755 | MAXPRO Receiver (MPIRCX) Installation and User Guide |

CHAPTER

# 17 SUPPORT AND PATENT

## INFORMATION

For the latest documentation and online support information, please go to:

https://www.security.honeywell.com/

# HONEYWELL COMMERCIAL SECURITY

Aston Fields Road

Whitehouse Industrial Estate

Runcorn

Cheshire

WA7 3DL

United Kingdom Tel: +44 (0)8448 000 235

www.security.honeywell.com



**800-23044-1 Rev. B8 March 2024**