PRT-CTRL-DIN-1D

Protege GX DIN Rail Single Door Controller

Installation Manual

Last Published: 17-Jun-22 5:20 PM

Contents

Introduction

This installation manual provides instructions and technical specifications for physical installation of the Protege GX DIN Rail Single Door Controller. For system communication and programming information, see the Protege GX Integrated System Controller Configuration Guide, available from the ICT website.

About This Module

The Protege GX DIN Rail Single Door Controller is the central processing unit responsible for the control of security, access control and building automation in the Protege GX system. It communicates with all system modules, stores all configuration and transaction information, processes all system communication, and reports alarms and system activity to a monitoring station or remote computer.

Protege GX is an enterprise level integrated access control, intrusion detection and building automation solution with a feature set that is easy to operate, simple to integrate and effortless to extend.

Flexible module network architecture allows large numbers of modules to be connected to the RS-485 module network. Up to 250 modules can be connected to the Protege system in any combination to the network, over a distance of up to 900M (3000ft). Further span can be achieved with the use of a network repeater module.

The current features of the controller include:

- Internal industry standard 10/100 ethernet
- 32 Bit advanced RISC processor with 2Gb total memory
- Encrypted module network using RS-485 communication
- NIST Certified AES 128, 192 and 256 Bit Encryption
- Factory loaded HTTPS certificate
- OSDP configurable RS-485
- 2 high security monitored inputs
- 1 Form C Relay output
- Industry standard DIN rail mounting

Single Door Controller Editions

There are two editions of the PRT-CTRL-DIN-1D Controller:

- The PRT-CTRL-DIN-1D can be supplied power from a 12V DC power supply connected to the N+ and N- terminals.
- The PRT-CTRL-DIN-1D-POE can be supplied power from a 12V DC power supply connected to the N+ and N- terminals OR from a power over ethernet (PoE) router via the onboard ethernet terminal.

The features specific to the PoE interface described in this manual are only relevant if using the appropriate edition.

Installation Requirements

This equipment is to be installed in accordance with:

- The product installation instructions
- AS/NZS 2201.1 Intruder Alarm Systems
- The Local Authority Having Jurisdiction (AHJ)

Grounding Requirements

An effectively grounded product is one that is intentionally connected to earth ground through a ground connection or connections of sufficiently low impedance and having sufficient current-carrying capacity to prevent elevated voltages which may result in undue hazard to connected equipment or to persons.

Grounding of the Protege system is done for three basic reasons:

1. Safety
2. Component protection
3. Noise reduction

Safety Grounding

The object of safety grounding is to ensure that all metalwork is at the same ground (or earth) potential. Impedance between the Protege system and the building scheme ground must conform to the requirements of national and local industrial safety regulations or electrical codes. These will vary based on country, type of distribution system and other factors. The integrity of all ground connections should be checked periodically.

General safety dictates that all metal parts are connected to earth with separate copper wire or wires of the appropriate gauge.

Earth Ground Connection

The DIN rail enclosure and the DIN rail modules must be grounded to a suitable single-point earth ground connection in the installation. A minimum 14AWG solid copper wire (or thicker, in accordance with local authorities) shall be used from the Protege system's earth connection points.

The DIN rail enclosure includes an earth ground single-point link connection via the metallic enclosure. This single-point link is the Protege system's earth ground. All modules that have earth ground connections and that are installed in the same enclosure shall be connected to this single point. A single-point earth ground connection avoids the creation of ground loops in the system and provides a single reference point to earth ground.

DIN Rail Ground Connections (one or more cabinets installed in the same room)
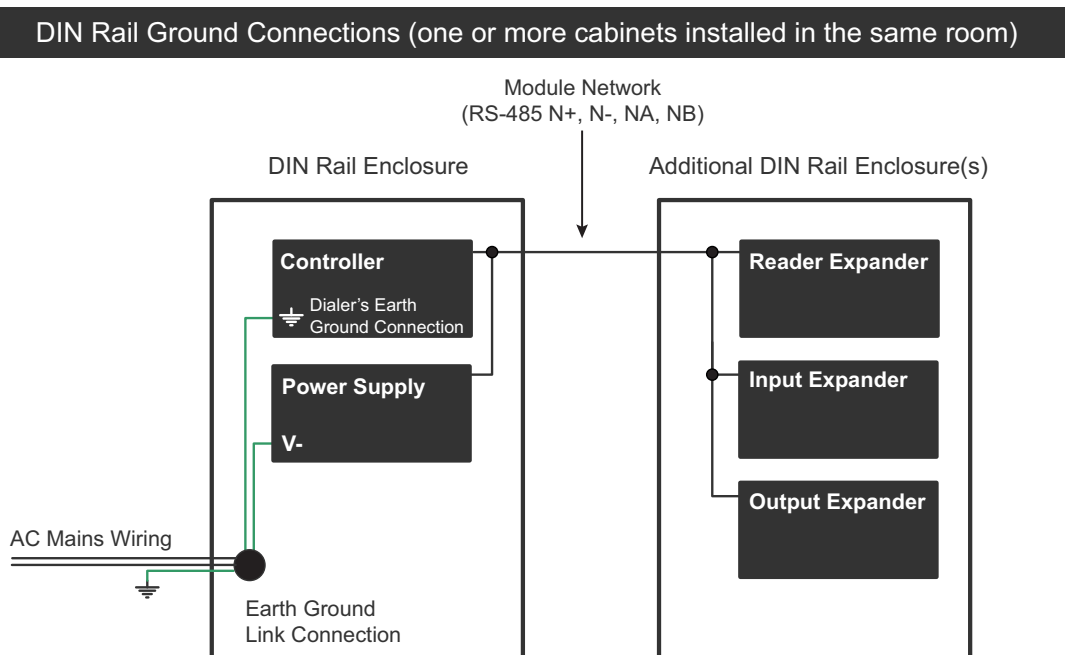
DIN Rail Ground Connections (multiple cabinets in different rooms, sectors, or buildings)

Module Network (RS-485 N+, N-, NA and NB)

DIN Rail Enclosure	DIN Rail Enclosure	DIN Rail Enclosure

Controller

⏚ Dialer's Earth
Ground Connection

Power Supply

V-

Earth Ground
Link Connection

Reader Expander

Input Expander

Output Expander

Input Expander

Input Expander

Input Expander

Sector or Building #1 — Sector or Building #2 — Sector or Building #3
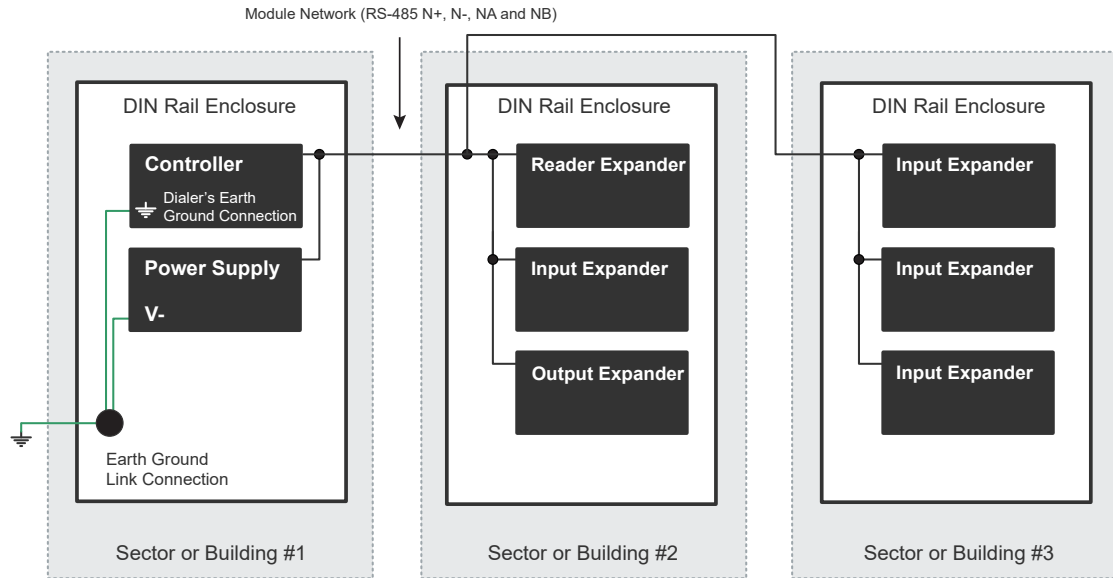
The Dialer's Earth Ground Connection applies to modem model controllers only.

Note that the DIN rail enclosure earth terminal is connected to the power supply V- terminal.

There must be only **one** single earth grounding point per system.

Mounting

Protege DIN rail modules are designed to mount on standard DIN rail either in dedicated DIN cabinets or on generic DIN rail mounting strip.

When installing a DIN rail module, ensure that there is adequate clearance around all sides of the device and that air flow to the vents of the unit is not restricted. It is recommended that you install the module in a location that will facilitate easy access for wiring. It is also recommended that the module is installed in an electrical room, communication equipment room, secure cabinet, or in an accessible area of the ceiling.

1. Position the DIN rail module with the labeling in the correct orientation.
2. Hook the mounting tabs (opposite the tab clip) under the edge of the DIN rail.
3. Push the DIN rail module against the mount until the tab clips over the rail.

Removal

A Protege DIN rail module can be removed from the DIN rail mount using the following steps:

1. Insert a flat blade screwdriver into the hole in the module tab clip.
2. Lever the tab outwards and rotate the unit off the DIN rail mount.

Connections

Power Requirements

Power is supplied to the controller by a 12V DC power supply connected to the N+ and N- terminals. The controller does not contain internal regulation or isolation and any clean 12V DC supply is suitable for this purpose.

> Termination of wiring to the module while power is applied or the battery is connected may cause serious damage to the unit and will VOID ALL WARRANTIES OR GUARANTEES.
> **Power the unit only after all wiring, configuration and jumper settings are completed.**

A battery backup must be connected to the module network to provide a monitored supply. The battery plays an important role in power conditioning and provides a continuous source of power in the event of a power outage.

Example 2A Power Supply Connection:
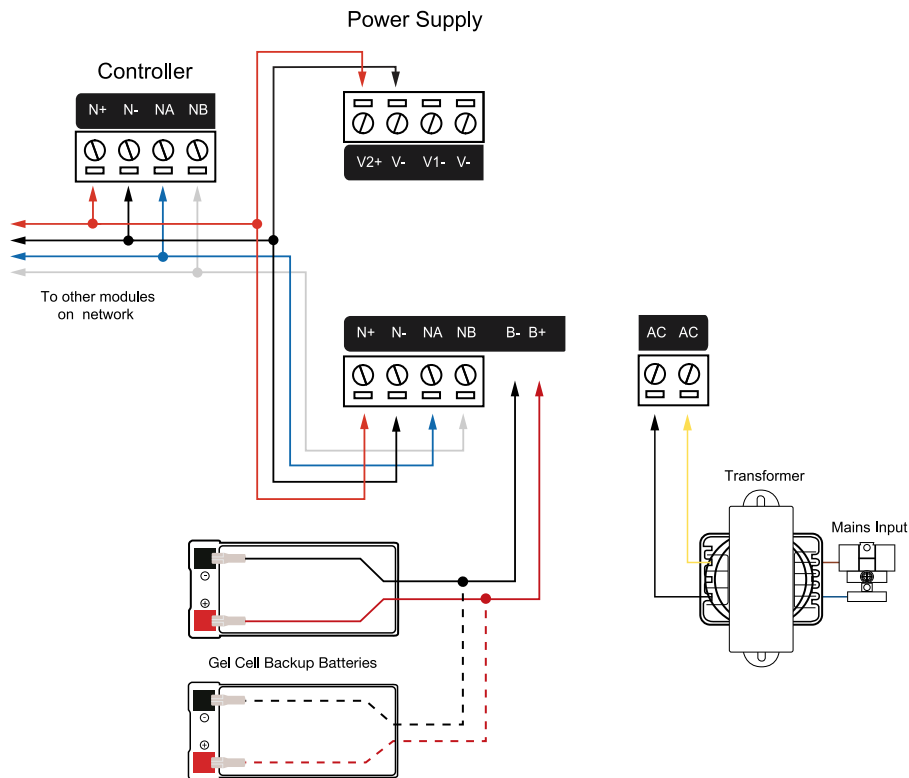
Example 4A Power Supply Connection:

Power Supply

Controller

N+   N-   NA   NB

V1+ V1+ V1+ V1+ V1+ V1+   V-   V-   V-   V-   V-   V-

To other modules
on network

N+   N-   NA   NB

B-   B+

L   N

Mains Input

Gel Cell Backup Batteries
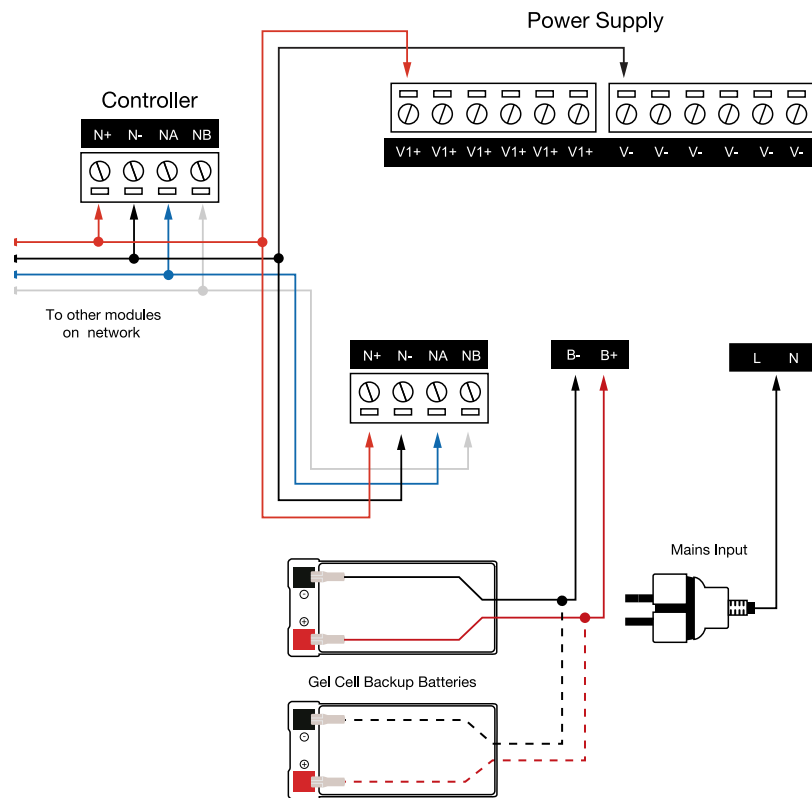
In a small installation this same power supply can be used to supply the module network as well, so long as the maximum load of the power supply is not exceeded. In larger installations, the power supply may need to be split to allow for load sharing between several supplies.

To comply with EN 50131-1 only one battery can be connected and monitored per system. If more capacity is required a single larger battery must be used.

Example Multiple PSU Connection:

Module #3   Module #2   Module #1   Controller

N+   N-   NA   NB   N+   N-   NA   NB   N+   N-   NA   NB   N+   N-   NA   NB

Power Supply #3   Power Supply #2   Power Supply #1
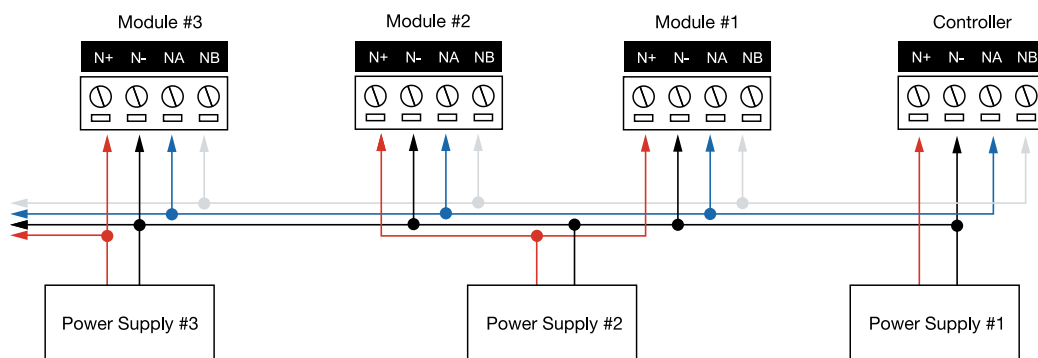
When using multiple power supplies it is important to ensure that all ground connections (V-) are connected between all power supplies and that no power connections (V+) are connected between any power supplies.

Auxiliary Outputs

The auxiliary outputs (S- S+) of the controller can be used to supply other equipment. Note that there is no onboard regulation or isolation for these outputs - they are a fused feed-through from the N+ N- input terminals. When using these outputs to supply other devices, be sure not to exceed the rating of the internal fuses as outlined in the Technical Specifications.

Power over Ethernet (PoE)

PoE model only

Power can be supplied to the controller by a PoE router connected to the ethernet terminal.

There are two types of PoE routers available:

- Low Power Type 1 (PoE) IEEE 802.3af, 12.95W Deliverable
- High Power Type 2 (PoE+) IEEE 802.3at, 25.5W Deliverable

When using a PoE router as the power source to the controller, the N+ and N- terminals become the network outputs that can be used for powering the module network. The auxiliary outputs (S- S+) should be used for powering readers and auxiliary loads such as locks.

The use of a High Power Type 2 (PoE+) router is necessary when the controller is required to supply a combined auxiliary load of more than 600mA.
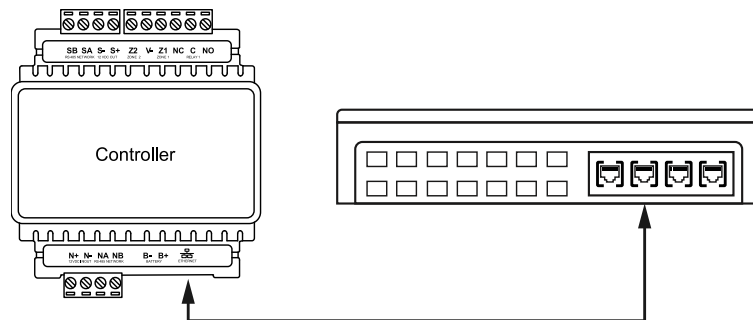
When using a PoE router as power source for the controller, the rating for the auxiliary outputs (S- S+) will be different to those when the controller is being powered by an Integrated Control Technology power supply or a 12V DC supply. Please refer to the values outlined in the Technical Specifications below for more details.

Encrypted Module Network

The controller incorporates encrypted RS-485 communications technology. Connection of the communications should be performed according to the following diagram.
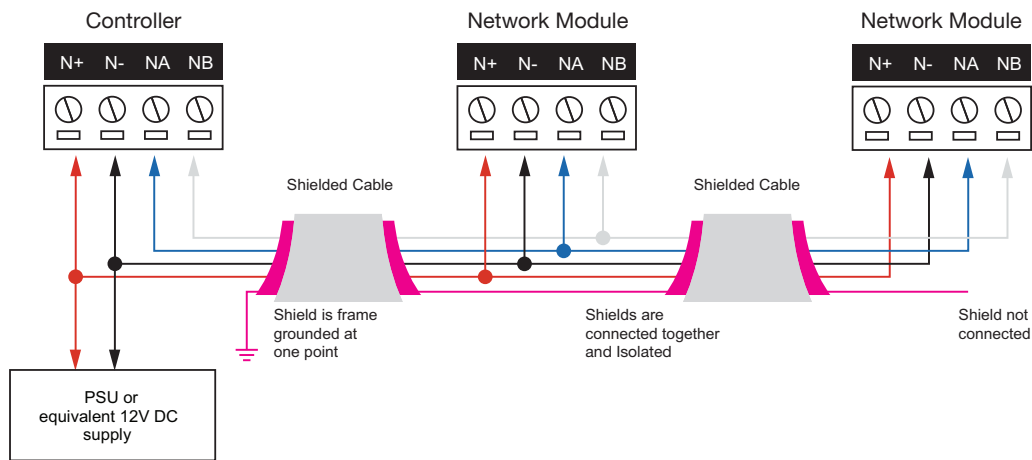
Always connect the controller's NA and NB terminals to the NA and NB terminals of the expansion devices and keypads. The N+ and N- must connect to a 12V power supply source capable of supplying the peak current drawn by all modules. If a shielded cable is used, the shield must be connected at only one end of the cable. **DO NOT** connect a shield at both ends.

The 12V N+ and N- communication input must be supplied from only **one** point. Connections from more than one 12V supply may cause failure or damage to the unit or the device supplying network power. Make sure that the power supply can supply enough current for the peak load drawn by **all modules** connected to the 12V supply, including the controller itself.

Module Wiring

The recommended module network wiring specifications are:

- Belden 9842 or equivalent
- 24AWG twisted pair with characteristic impedance of 120 ohm
- Maximum total length of cable is 900m (3000ft)
- CAT5e / CAT6 are also supported for data transmission when using ground in the same cable (to a maximum length of 100m (328ft))

**Warning:** Unused wires in the cable must not be used to carry power to other devices.

End of Line (EOL) Resistors

The 330 ohm EOL (End of Line) resistor provided in the accessory bag **must** be inserted between the NA and NB terminals of the **first** and **last** modules on the RS-485 network. These are the modules physically located at the ends of the RS-485 network cabling.

First Module on RS-485 Network
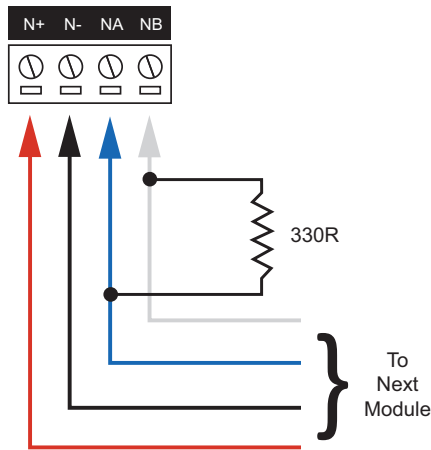
Last Module on RS-485 Network
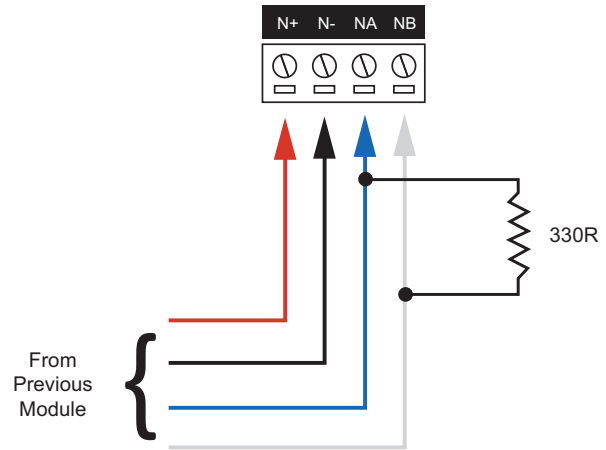
Backup Battery

PoE model only

It is recommended that a minimum of a 7Ah battery is used as the main backup battery. From the accessory bag provided, connect the RED and BLACK battery termination wires to the B+ and B- plugs. Connect the spade terminals to the battery as shown below. Connection of the battery in reverse will not damage the controller but will cause the battery fuse (5A resettable fuse) to open, requiring resetting by removal of all connections to the B+ and B- plugs for approximately 30 seconds.

Single Door Controller with PoE Battery Connection:

Gel Cell Backup Battery
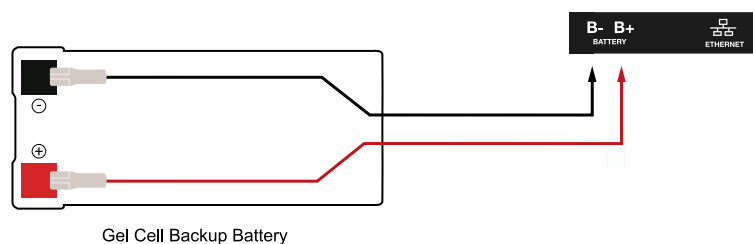
Warning:

- Only attach standard lead acid batteries.
- Do not connect the battery wires or B+ and B- plugs of the module to any other ancillary device (siren, lock, mag clamp, etc.).
- An incorrect connection may cause erroneous faults or serious damage to the module and will **VOID ALL WARRANTIES OR GUARANTEES**.

The battery test procedure uses a special algorithm to prevent deep discharge and increase battery endurance. A dynamic battery test is performed every ten minutes when mains power is present and a battery condition alarm will be generated if the battery is either disconnected or shows poor capacity. Battery fault conditions will activate the battery trouble input associated with the address assigned to the controller.

In addition to the dynamic battery test procedure, the controller performs a battery presence test every 60 seconds, which determines whether the presence of a backup battery is detected. Similarly, a battery condition alarm will be generated and the battery trouble input associated with the address assigned to the controller will also be activated.

To comply with EN 50131-1 only one battery can be connected and monitored per system. If more capacity is required a single larger battery must be used.

Ethernet 10/100 Network Interface

The communication between the Protege system and the controller uses a 10/100 ethernet network operating the TCP/IP protocol suite. The IP address of the controller can be configured using an LCD keypad terminal or via the built-in web interface. The default IP address is set to a static address of 192.168.1.2 with a subnet mask of 255.255.255.0. These IP address settings are commonly used for internal networks.

Installing the module on an active network requires knowledge of the configuration and structure for the network. Always consult the network or system administrator and ask them to provide you with a fixed IP address that can be assigned to the module.

When installing an ethernet connection the module should be interfaced using a standard segment (<100m in length) and should be connected to a suitable ethernet hub or switch:

Ethernet 10/100 Switch Hub Connection:
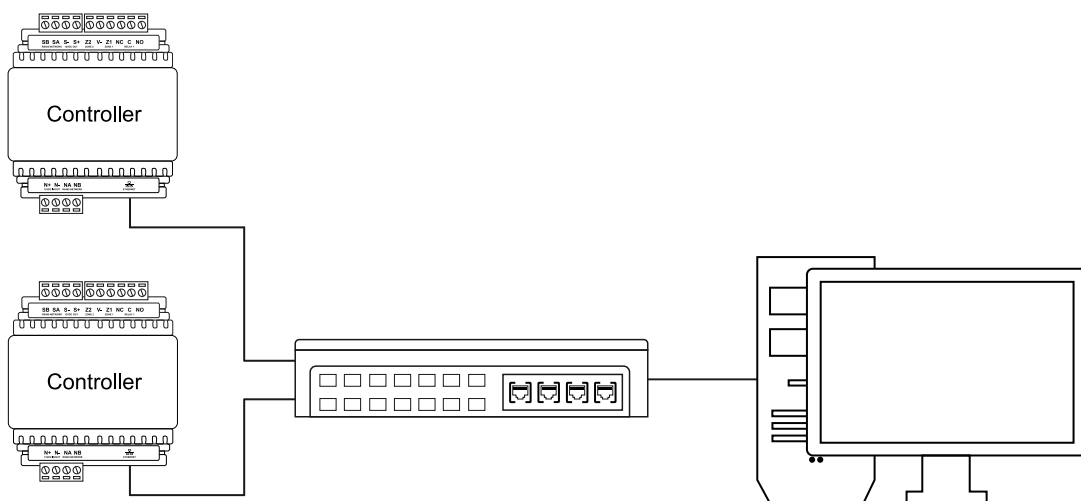
Temporary direct connections can be used for onsite programming by using a standard ethernet cable.

Ethernet 10/100 Direct Connection:
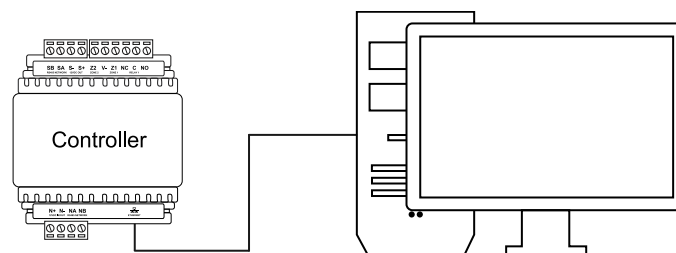
Door Access Control

The controller provides onboard access control allowing the connection of up to two RS-485 readers (configured for entry and exit) to a single door.

The recommended cable types for RS-485 are:

- Belden 9842 or equivalent
- 24 AWG twisted pair with characteristic impedance of 120ohm

Important:

- The card reader must be connected to the module port using a shielded cable.
- The shield must only be connected at one end of the cable in the metallic enclosure (frame grounded).
- Do not connect the cable shield to an AUX-, 0V or V- connection on the module.
- Do not connect the cable shield to any shield used for isolated communication.
- The reader and cable shield wires must be joined at the reader pigtail splice.
- Do not join the shield and black wires at the reading device.
- Do not terminate the reader shield wire inside the reader.

Note: The reader and cable shield wires must be joined at the reader pigtail splice for all MIFARE capable ICT card readers. Older readers which are internally grounded and third-party readers do not require the shield wires to be joined. For further information, contact ICT Technical Support.

Always refer to the card reader manufacturer for detailed installation guidelines.

All ICT readers are shipped with single LED mode set as default and are fully compatible with the Protege system.

RS-485 Reader Locations

As two RS-485 readers can be connected to the same RS-485 reader port, configuration of the **green** and **orange** wires uniquely identifies the reader, and determines which is the entry reader and which is the exit reader.

Location	Configuration
Entry	Green and orange wires **not** connected.
Exit	Green and orange wires connected together.

RS-485 Reader Connection (Entry Only)

The following diagram shows the connection of a single RS-485 reader connected in entry only mode.
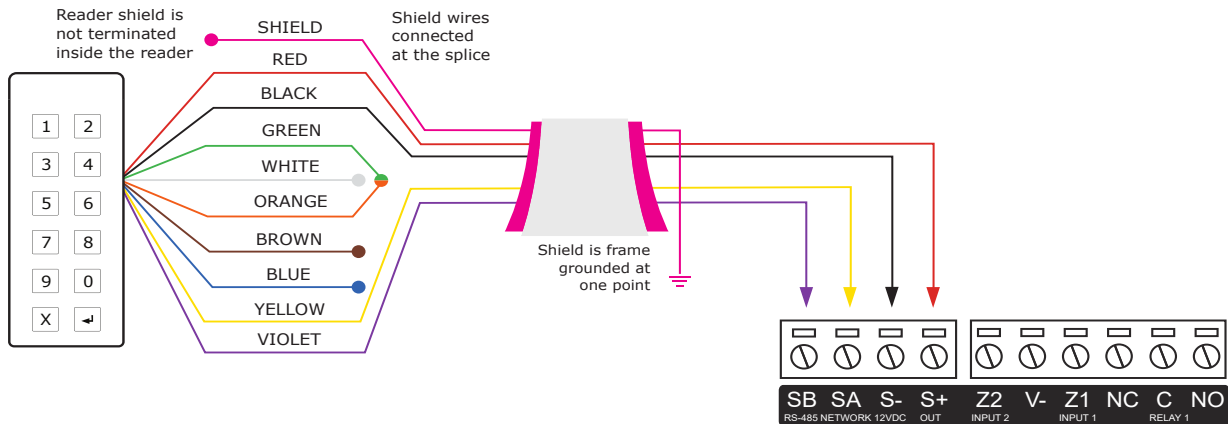
When the green and orange wires are not connected together, the reader defaults to an entry reader.

RS-485 Reader Connection (Entry/Exit)

The following diagram shows the connection of two RS-485 readers connected to provide an entry/exit configuration.
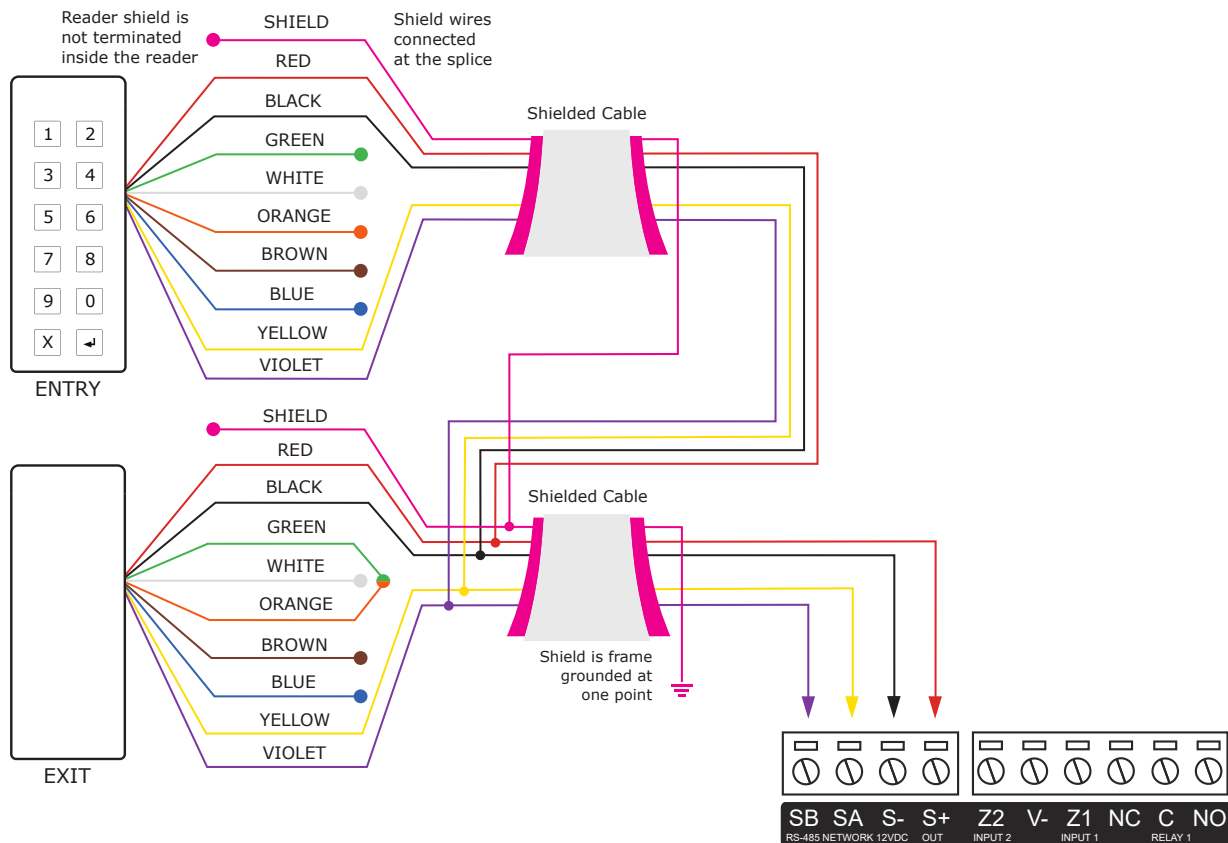
The exit reader has the **green** and **orange** wires connected together.

A 330 ohm EOL (End of Line) resistor may be required to be inserted between the NA and NB terminals of the reader and a second 330 ohm EOL resistor must then be inserted between the source NA and NB terminals at the other end of the wiring.

Door Contact Connection

The controller allows the connection of 2 contacts for monitoring and controlling the door.

Typical Configuration of Door Monitoring Contacts:
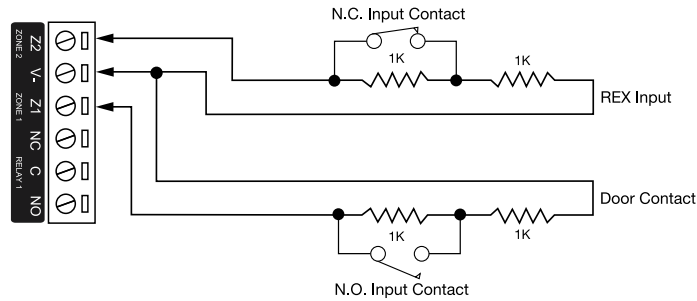
Each of these inputs can be used for either the door function that is automatically assigned or as a general purpose input. If used as general purpose inputs, make sure the inputs are not defined in the onboard reader setup.

Input	Access Control Function	Default Setting
Input 1	Door Contact, Port 1	Door Contact, Port 1
Input 2	REX Input, Port 1	REX Input, Port 1

When connected the REX input can be programmed to operate regardless of the door contact state. The REX input can also be programmed to recycle the door alarm time to prevent nuisance alarms when the door is held open to permit longer entry.

Lock Output Connection

The controller provides a connection for an electric strike lock using the integrated relay.

To use the lock output in conjunction with the onboard reader, the lock output for the door associated with the reader port must be configured to be the desired lock output on the controller. This is not configured by default.

Typical Lock Output Connection:
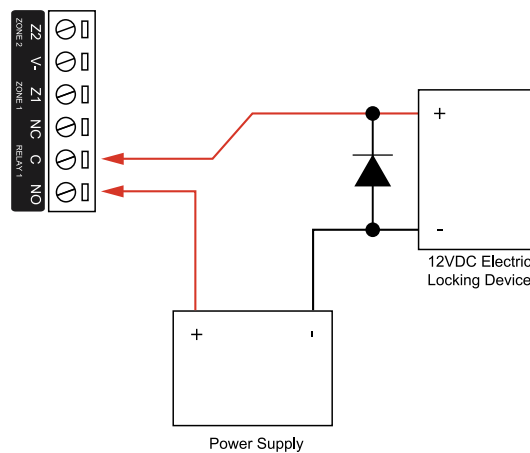
Programming the Onboard Reader

The onboard reader is programmed in exactly the same way as any other reader module. It can be thought of as if it were a normal reader expander module on a separate circuit board. By default the onboard reader is disabled. To enable it, configure the address at which you want it to register using the Protege user interface. Note that any physical reader expander module that is connected with the same address will be treated as a duplicate and will fail to register, so care should be taken to ensure the address is unique.

The onboard reader uses inputs 1 and 2 as its door contact and REX respectively. Any inputs that are not configured for use with the onboard reader may be used as general purpose inputs. If you wish to use an access control input as a general input, you will need to disable the associated function input in the door programming section of the Protege user interface.

The default settings are shown in the following table:

Input	Access Control Function	Default Setting
Input 1	Door Contact, Port 1	Door Contact, Port 1
Input 2	REX Input, Port 1	REX Input, Port 1

The controller's onboard reader port supports an RS-485 reader interface, allowing ICT RS485 readers to be configured. This can be set in the **Expanders | Reader expanders** menu.

Inputs

The controller has 2 onboard inputs for monitoring the state of devices such as magnetic contacts and motion detectors. Devices connected to the inputs can be installed to a maximum distance of 300m (1000ft) from the module when using 22 AWG wire.

Inputs can be programmed. Inputs CP001:01 and CP001:02 represent the controller's onboard inputs. Additional inputs are supported through the use of expansion modules.

The controller supports normally opened and normally closed configurations with or without EOL resistors. When using an input with the EOL resistor configuration, the controller generates an alarm condition when the state of an input changes between open and closed and generates a tamper alarm condition when a wire fault (short circuit) or a cut wire (tampered) in the line occurs. Inputs default to require the EOL resistor configuration.

EOL Resistor Input Configuration:
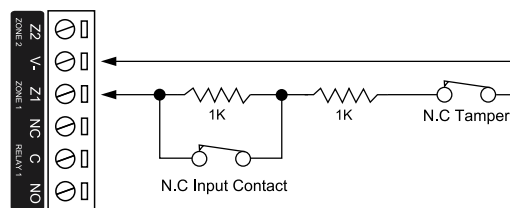
Inputs 1 and 2 can operate as either general purpose inputs or as onboard reader inputs. If used as general purpose inputs you must ensure that they are not defined in the onboard reader set up.

Each input can use a different input configuration. To program a large number of inputs with the same configuration use the multiple selection feature within the Protege software.

When using the 'No Resistor' configuration the controller only monitors the opened and closed state of the connected input device, generating the alarm (open) and restore (closed/sealed) conditions.

No EOL Resistor Input Configuration:
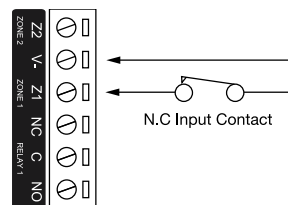
EOL Resistor Value Options

When using EOL resistor configuration, the EOL resistor option must be configured based on the site requirements. Note that these resistor options are supported on the controller but not all resistor options are supported on all Protege field modules.

Value 1	Value 2	Monitored Status
No Resistor	No Resistor	Open, Closed
1K	1K	Open, Closed, Tamper, Short
6K8	2K2	Open, Closed, Tamper, Short
10K	10K	Open, Closed, Tamper, Short

Value 1	Value 2	Monitored Status
2K2	2K2	Open, Closed, Tamper, Short
4K7	2K2	Open, Closed, Tamper, Short
4K7	4K7	Open, Closed, Tamper, Short
5K6	5K6	Open, Closed, Tamper, Short
No Resistor	5K6	Open, Closed

Duplex Inputs

The controller is able to support up to 4 inputs when duplex mode is enabled.

To enable this feature, check the **Duplex inputs** option in **Sites | Controllers | Options**. In addition, you will need to manually add additional inputs with addresses 3-4 in **Programming | Inputs**.

Duplex Input Configuration
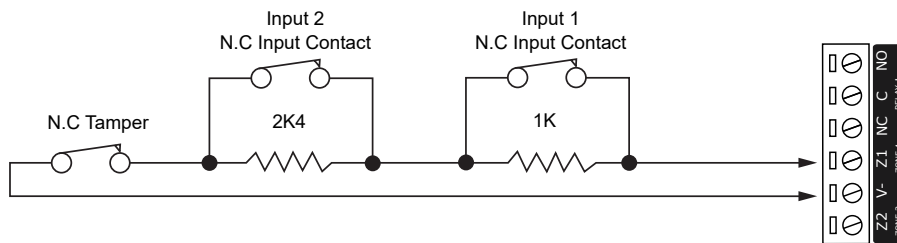
The following table indicates the position and resistor configuration corresponding to each input address:

Input Address	Position	Resistor
1	Z1	1K
2	Z1	2K4
3	Z2	1K
4	Z2	2K4

Enabling duplex inputs will not change the programming of any existing inputs. These must be reprogrammed or rewired to match the new addressing scheme.

Trouble Inputs

Trouble inputs are used to monitor the status of the controller and in most cases are not physically connected to an external input. These can then be used to report a message to a monitoring station, remote computer, keypad or siren.

The following table details the trouble inputs that are configured in the controller and the trouble type and group that they activate.

Input Number	Description	Type	Group
CP001:02	12V Supply Failure	Power Fault	General
CP001:04	Real Time Clock Not Set	RTC/Clock Loss	General
CP001:05	Service Report Test	-	-
CP001:08	Auxiliary Failure	Power Fault	General
CP001:13	Module Communication	Module Loss	System
CP001:14	Module Network Security	Module Security	System
CP001:20	Report IP Reporting Failure	Reporting Failure	System
CP001:22	ModBUS Communication Fault	Hardware Fault	System
CP001:23	Protege System Remote Access	Hardware Fault	System
CP001:24	Installer Logged In	Hardware Fault	System
CP001:29	System restarted	Hardware Fault	System
CP001:30	PoE Connection Lost (PoE model only)	Power Fault	General
CP001:31	Output Over-Current Failure (PoE model only)	Power Fault	General

Outputs

The controller has one onboard output (CP001:03) which is a Form C relay with normally open and normally closed contacts. This output can be used to activate larger relays, sounders, lights, locks etc.

Example Relay Connection:
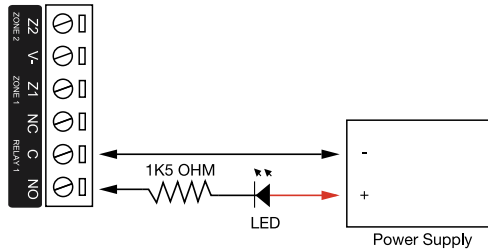
Warning: The relay outputs can switch to a maximum capacity of 7A. Exceeding this amount will damage the output.

Hardware Configuration

Configuring a Controller via the Web Interface

The controller's built-in web interface allows you to configure system communication and security settings, including login, IP address, subnet mask, gateway and DNS settings, as well as security certificates.

For information on using the controller's web interface to configure IP network and security settings, see the Protege GX Integrated System Controller Configuration Guide, available from the ICT website.

Setting the IP Address from a Keypad

If the current IP address of the controller is not known it can be viewed and changed using a Protege keypad.

1. Connect the keypad to the module network.

2. Log in to the keypad using any valid installer code. The default installer code is 000000.

   If the default code has been overridden and you do not know the new codes you will need to default the controller (see Defaulting the Controller in this document) to reset the code.

   Note that this will erase **all** existing programming as well as setting up the default installer code.

3. Once logged in select **Menu 4** (Install Menu) then **Menu 2** (IP Menu) and view or edit the IP address, network mask, and gateway as required.

Once the settings have been changed you must save the settings by pressing the **[Arm]** key. You will be prompted to confirm the changes by pressing **[Enter]**. You must then restart the controller, either through the menu **[4], [2], [2]** or by cycling the power, for the settings to take effect.

Temporarily Defaulting the IP Address

If the currently configured IP address is unknown it can be temporarily set to 192.168.111.222 so that you can connect to the web interface to view and/or change it.

This defaults the IP address for as long as power is applied, but does not save the change permanently. Once the link is removed and power is cycled to the unit the configured IP address is used.

1. Remove power to the controller by disconnecting the 12V DC input.

2. Wait until the power indicator is off.

3. Connect a wire link between **NA** of the module network and **SA** of the reader network, and between **NB** of the module network and **SB** of the reader network.

4. Connect **Input 2** to ground.
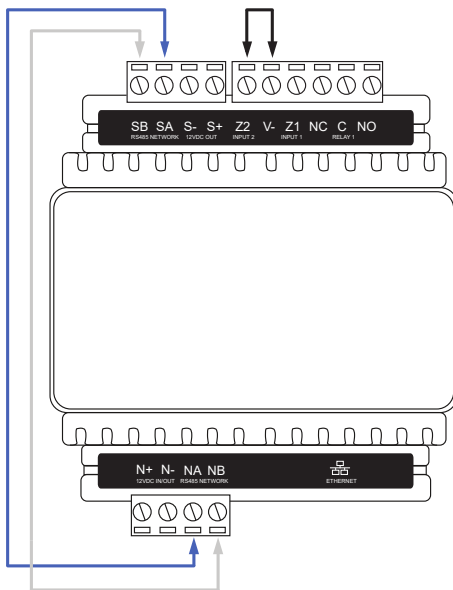
5. Power up the controller. Wait for the status indicator to begin flashing steadily.

6. When the controller starts up it will use the following temporary settings:

   - IP address : 192.168.111.222
   - Subnet Mask : 255.255.255.0
   - Gateway : 192.168.111.254
   - DHCP : disabled

7. Connect to the controller by entering https://192.168.111.222 into the address bar of your web browser, and view or change the IP address as required.

   Remember to change the subnet of your PC or laptop to match the subnet of the controller.

8. Remove the wire link(s) and power cycle the controller again.

   You can now connect to the controller using the configured IP address.

Defaulting a Controller

The controller can be factory defaulted, which resets all internal data and event information. This allows you to remove all programming and start afresh.

Defaulting the controller resets the IP address to the factory default IP of 192.168.1.2

Defaulting a One-Door Controller

1. Remove power to the controller by disconnecting the 12V DC input.

2. Wait until the power indicator is off.

3. Connect a wire link between **NA** of the module network and **SA** of the reader network, and between **NB** of the module network and **SB** of the reader network.

4. Connect **Input 1** to ground.
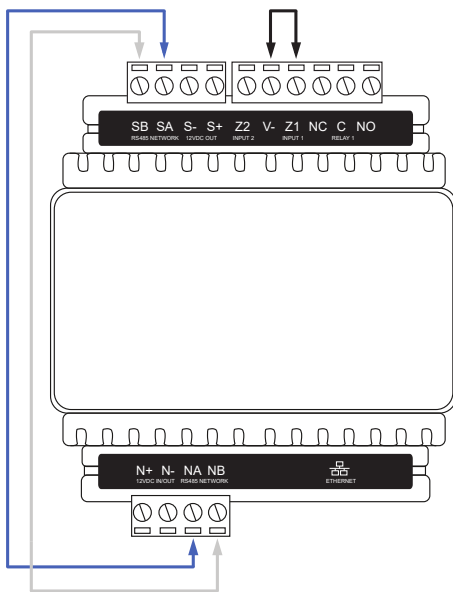
5. Power up the controller. Wait for the status indicator to begin flashing steadily.

6. Remove the wire link(s).

The system will now be defaulted with all programming and **System Settings** returned to factory configuration, including resetting the IP address and all network configuration, and removing all operator records.

- Defaulting the controller resets the IP address to the factory default IP of 192.168.1.2.

  Earlier versions of the controller firmware do not reset the IP address. If the controller is not available on 192.168.1.2 you will be able to connect to it via its previous IP address.

- Any configured system settings (e.g. **Default Gateway**, **Event Server**) are reset to their default values.

- Any custom HTTPS certificates are removed and the default certificate is reinstalled.

  Earlier versions of the controller do not have a default HTTPS certificate installed. If the controller is not available via HTTPS, connect to it via HTTP.

- All operator records are removed and the admin operator must be recreated.

- All other programming is removed.

After Defaulting a Controller

After defaulting a controller a number of essential steps will need to be performed to resume normal operation. Not all of the following steps will necessarily be required, depending on your site configuration:

1. Connect to the controller's web interface using HTTPS, unless it is an older controller with no default certificate loaded, then it will connect using HTTP.

2. Recreate the admin operator and log in to the controller's web interface.

   If you are not prompted to create the admin operator, the default username is admin with the password admin.

3. Reset the controller's IP address to its previous value.

4. Reconfigure any additional network settings.

5. Reinstall previously installed custom HTTPS certificates.

6. Restore any other system settings as required by your site configuration.

LED Indicators

Protege DIN rail modules feature comprehensive diagnostic indicators that can aid the installer in diagnosing faults and conditions. In some cases an indicator may have multiple meanings depending on the status indicator display at the time.

Power Indicator

The power indicator is lit when the correct input voltage is applied to the controller.

Note that this indicator may take several seconds to light up after power has been applied.

State	Description
On (green)	Correct input voltage applied
Off	Incorrect input voltage applied

Status Indicator

The status indicator displays the status of the controller.

State	Description
Flashing (green) at 1 second intervals	Controller is operating normally

Fault Indicator

The fault indicator is lit any time the controller is operating in a non-standard mode. During normal operation the fault indicator is off.

State	Description
Off	Controller is operating normally
On (red)	Controller is operating in a non-standard mode

PoE Power Indicator

PoE model only

The PoE power indicator shows the status of the PoE connection.

State	Description
On (green)	PoE+ connection applied
Flashing (green)	PoE connection applied
Off	No PoE connection applied

Battery Indicator

The battery indicator shows the status of the backup battery.

State	Description
Flashing (red)	Backup battery is disconnected
On (red)	Backup battery failed its dynamic battery test
On (green)	Last backup battery dynamic test successful

Ethernet Link Indicator

The ethernet indicator shows the status of the ethernet connection.

State	Description
On (green)	Valid link with a hub, switch or direct connection to a personal computer detected
Flashing (green)	Data is being received or transmitted
Off	Ethernet cable not connected, no link detected

Reader Data Indicators

The R1 and R2 indicators display the status of the data being received by the onboard readers.

State	Description
Short flash (red)	A SHORT flash (<250 milliseconds) will show that data was received but was not in the correct format
Long flash (red)	A LONG flash (>1 second) indicates that the unit has read the data and the format was correct

Relay Indicator

The relay indicator shows the status of the lock output relay.

State	Description
On (red)	Relay output is ON
Off	Relay output is OFF

Input Indicators

Whenever an input on the module is programmed with an input type and area, the input status will be displayed on the front panel indicator corresponding to the physical input number. This allows for easy test verification of inputs without the need to view the inputs from the keypad or the Protege software.

State	Description
Constantly off	Input is not programmed
Constantly on (red)	Input is in an open state
Constantly on (green)	Input is in a closed state
Continuous flash (red)	Input is in a tamper state
Continuous flash (green)	Input is in a short state

Mechanical Diagram

The mechanical diagram shown below outlines the essential details needed to help ensure the correct installation of the controller.
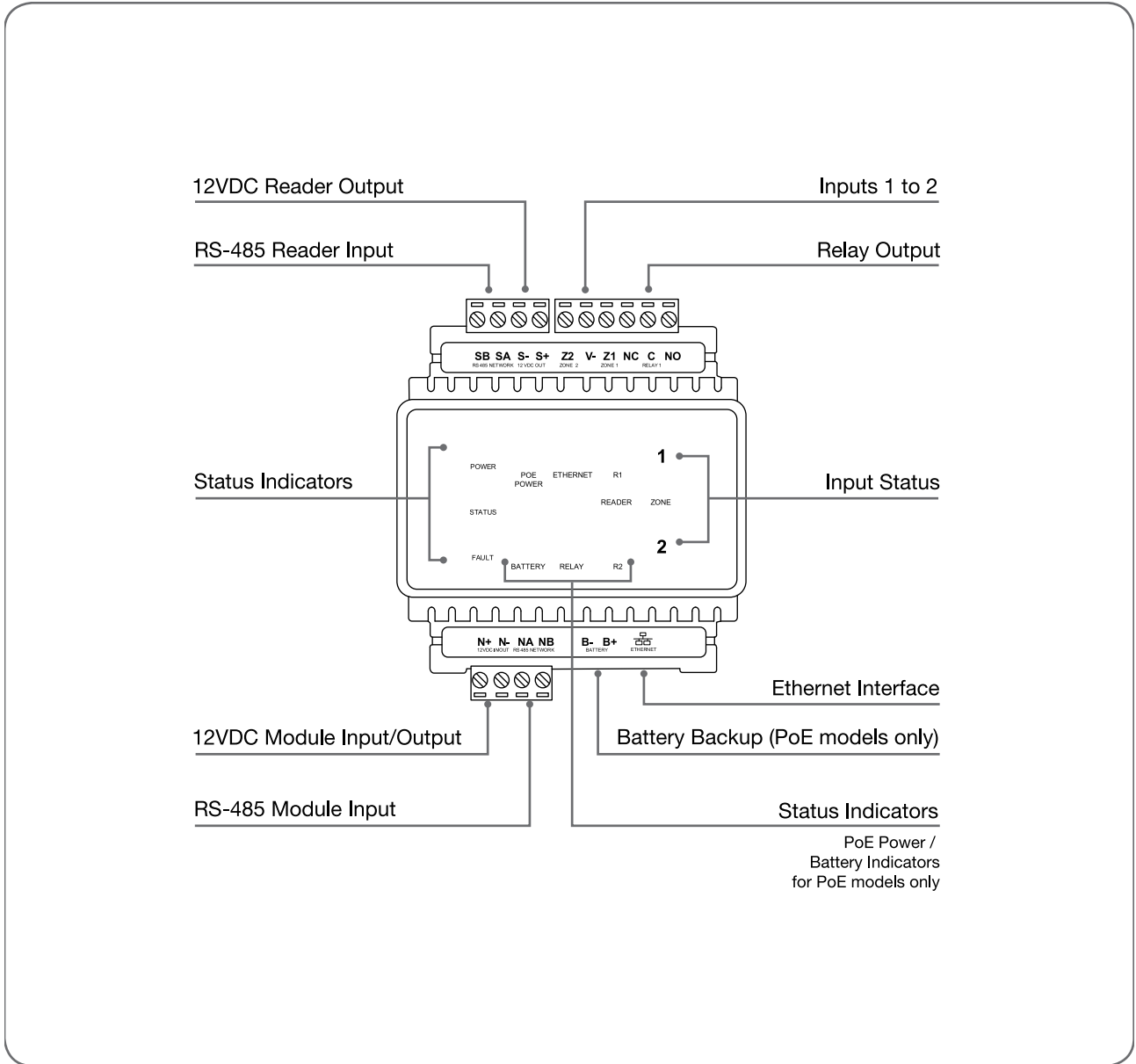
Mechanical Layout

The mechanical layout shown below outlines the essential details needed to help ensure correct installation and mounting. All measurements are shown in millimeters.

Technical Specifications

The following specifications are important and vital to the correct operation of this product. Failure to adhere to the specifications will result in any warranty or guarantee that was provided becoming null and void.

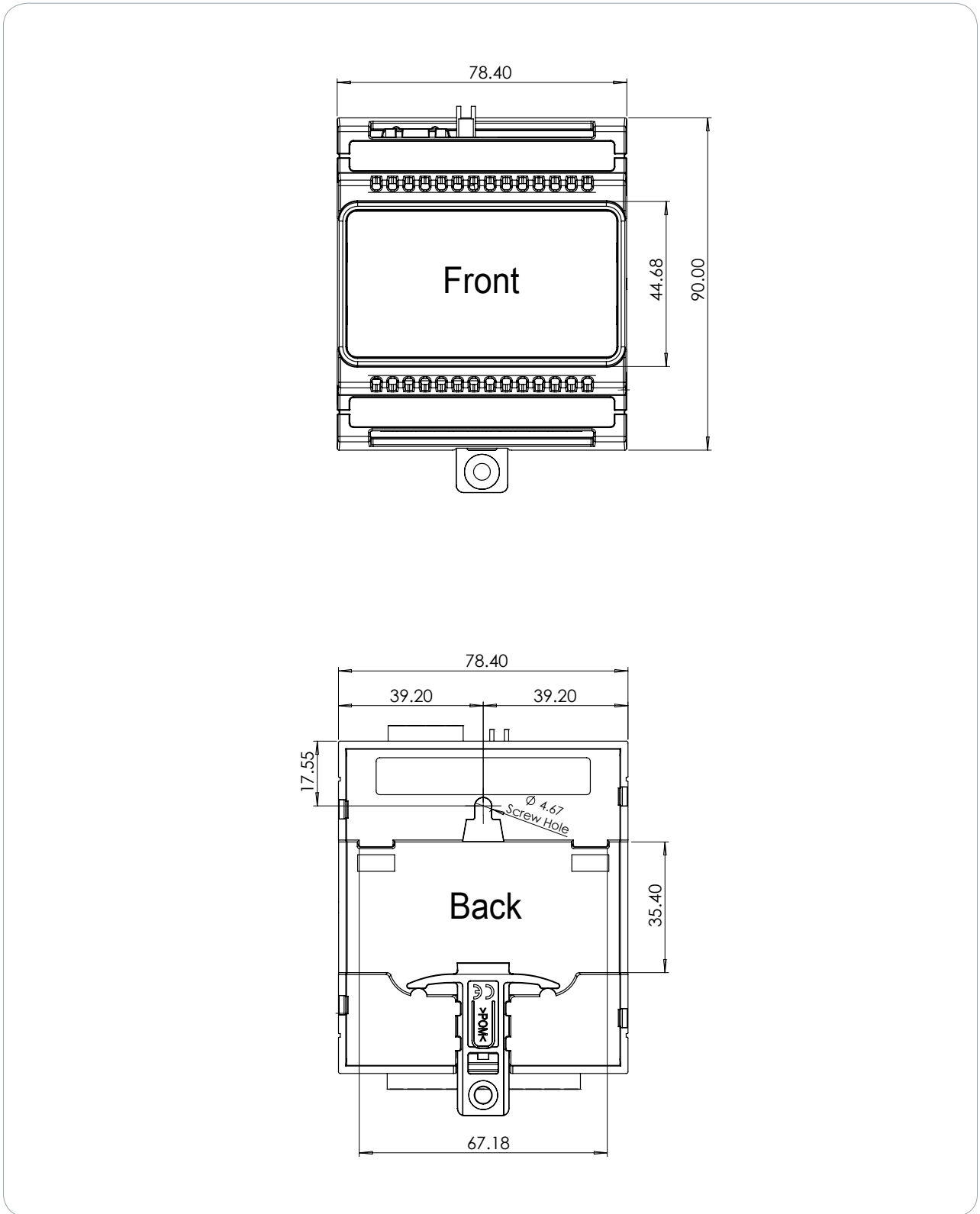| Ordering Information		
Order Code	PRT-CTRL-DIN-1D	PRT-CTRL-DIN-1D-POE
Product Name	Protege GX DIN Rail Single Door Controller	Protege GX DIN Rail Single Door Controller with POE
Power Supply		
Operating Voltage	11-14V DC	
Operating Current	120mA (Typical)	
DC Output	10.45-13.85VDC 0.7A (Typical) electronic shutdown at 1.1A	13VDC +/- 0.5 0.7A (Typical) electronic shutdown at 1.1A
Total Combined Current*	0.82A (Max)	0.6A total at outputs, inclusive of battery charging (PoE) / 1A total at outputs, plus battery charging (PoE+)
Electronic Disconnection	9.0VDC	
Battery		
Battery Charging	-	300mA (Typical)
Battery Low	-	11.2VDC
Battery Restore	-	12.5VDC
Communications		
Ethernet	10/100Mbps ethernet communication link	
RS-485	2 RS-485 communication interface ports - 1 for module communications, 1 for reader communications	
Readers		
Readers	1 RS-485 enabled reader port, allowing connection of up to 2 RS-485 capable readers providing entry/exit control for a single door	
	RS-485 reader port connections support configuration for OSDP protocol	
Inputs and Outputs		
Inputs	2 high security monitored inputs	
Relay Outputs	1 Form C Relay - 7A N.O/N.C. at 30 VAC/DC resistive/inductive	
Dimensions		
Dimensions (L x W x H)	78 x 90 x 60mm (3.07 x 3.54 x 2.36")	
Net Weight	170g (6oz)	210g (7.4oz)
Gross Weight	230g (8.1oz)	310g (10.9oz)
Operating Conditions		

Operating Temperature	-10° to 55°C (14° to 131°F)
Storage Temperature	-10˚ to 85˚C (14˚ to 185˚F)
Humidity	0%-93% non-condensing, indoor use only (relative humidity)
Mean Time Between Failures (MTBF)	560,421 hours (calculated using RFD 2000 (UTE C 80-810) Standard)

* The total combined current refers to the current that will be drawn from the external power supply to supply the expander and any devices connected to its outputs. The auxiliary outputs are directly connected via thermal resettable fuses to the N+ N- input terminals, and the maximum current is governed by the trip level of these fuses.

The ICT implementation of OSDP conforms to a subset of the OSDP functionality. For specifications and reader configuration, refer to Application Note 254: Configuring OSDP Readers, available from the ICT website.

The size of conductor used for the supply of power to the unit should be adequate to prevent voltage drop at the terminals of no more than 5% of the rated supply voltage.

Integrated Control Technology continually strives to increase the performance of its products. As a result these specifications may change without notice. We recommend consulting our website (www.ict.co) for the latest documentation and product information.

New Zealand and Australia

General Product Statement

The RCM compliance label indicates that the supplier of the device asserts that it complies with all applicable standards.

Intruder Detection Maintenance Routine

Integrated Control Technology recommends regular maintenance of the Protege system, including Protege controllers, expander modules and other connected devices.

The periodic routine maintenance procedures outlined in this section accord with AS/NZS standards for intruder detection systems:

- AS/NZS 2201.1-2007 SECTION 5 - MAINTENANCE AND SERVICE
- AS/NZS 2201.1-2007 SECTION 5 - RECORDS AND REPORT

Copies of these standards are available from Standards New Zealand, and can be purchased online from https://shop.standards.govt.nz.

Peripheral Devices

This section outlines specific routine maintenance procedures for Protege controllers and expander modules which are used for intruder detection. It does not include specific instructions for peripheral devices connected to the Protege system, such as motion detectors, smoke detectors and warning devices. Although many of these peripheral devices will be operated as part of the maintenance procedures described below, this may not meet the routine maintenance procedures recommended for those devices.

As a minimum, we recommend that you follow the AS/NZS 2201.1-2007 standards relating to:

- Detection devices for internal use (AS/NZS 2201.3 Part 3)
- Audible and visible alarm and warning devices

Testing Frequency

The maintenance procedures outlined below meet the requirements of AS/NZS 2201.1-2007, which specifies that testing of the intruder detection system must be carried out at least once a year. However, the testing frequency of detection devices, alarm warning devices and reporting operations should be determined according to the needs of the particular installation and local body regulations.

For some clients or sites it may be prudent to perform more frequent testing to ensure the integrity of the system. For example:

- Sites which require a higher rate of security or are heavily affected by environmental conditions may choose to have testing carried out more frequently.
- Very large sites with hundreds of detection devices may prefer to arrange multiple testing rounds per year, with a percentage of the devices tested in each round.

In contrast, sites where automated testing functions have been implemented may find that annual maintenance visits are adequate.

Recommended Routine Maintenance Procedures

Preliminary Procedures

Task	Frequency	Description
Notify the alarm monitoring company (place account 'on test')	As required prior to start of maintenance routine	If the system is monitored, the monitoring company must be notified before any testing begins (commonly referred to as placing the system 'on test'). In most circumstances you must be authorized to perform this task. The monitoring company may request a Technician or 'voice' code to identify you and the company that you represent.
Notify personnel on the premises	As required prior to start of maintenance routine	Prior to any test that may have an impact on personnel such as testing inputs or warning devices, ensure that all affected staff members are given any necessary notification, warning or instructions.

On Site Maintenance Procedures

Task	Frequency	Description
Check the equipment schedule and/or maintenance sheets	Once per year	Check the installation, location and siting of all equipment and devices against the 'as-built' documentation. Record and report any discrepancies.
Check wiring and cable protection	Once per year	Visually inspect all wiring and cable protection systems (conduits, trunking, etc.). Record any damage or deterioration.
Check for dust, moisture and vermin	Once per year	Check all equipment enclosures for dust, moisture, condensation and vermin. If excessive moisture or foreign matter is present, clear this out of the enclosure and take steps to prevent future accumulation.
Check the power supply	Once per year	Check that all power supplies are properly connected to a mains outlet and are operational.
Test the power supply DC output voltage	Once per year	Disconnect the backup batteries and test the DC voltages across the V+ and V- output terminals on all power supplies. The recommended voltage range is **12.4 - 14.0 VDC**.
Test expander module DC output voltage	Once per year	Test DC voltage across the V+ and V- output terminals on Protege controllers, input expanders and output expanders. The recommended voltage range is **10.4 - 14.0 VDC**.
Check battery connections	Once per year	Check that all power supplies have batteries fitted and connected correctly to the B+ and B- terminals, and that the batteries and connections show no visible signs of corrosion.
Test battery charge voltage	Once per year	Test the DC voltage across the B+ and B- terminals of all power supplies. The recommended voltage range is **13.4 - 13.8 VDC**. Note: When the mains power is restored following an AC fail condition, the battery charge voltage may fluctuate between **10.0 - 13.8 VDC** while the battery is recharging.

Task	Frequency	Description
Replace battery	Once per 3-5 years, or as specified by the battery manufacturer	Replace each power supply battery as required with another of equivalent or better specifications. Record the installation date of the new battery in the system maintenance records and in a clearly visible location within the equipment enclosure or on the battery itself.
Check keypad keys	Once per year	Check the operation of every key on the keypad, that all keys are clearly legible and that the keypad backlighting is operational.
Check keypad display	Once per year	Check the operation of the keypad display to ensure that all characters display correctly on the screen and that the backlight is operational and at the correct brightness.
Test the primary reporting service	As agreed between monitoring company and client, but not less than once per year	**Note**: This procedure must be pre-arranged in consultation with the monitoring station. • Ensure that the system is 'on test'. • Perform an operation that triggers reporting. • Check that the system reports successfully.
Test the backup reporting service	As agreed between monitoring company and client, but not less than once per year	**Note**: This procedure must be pre-arranged in consultation with the monitoring station. • Disable the primary reporting service. • Perform an operation that triggers a reportable alarm. • Check that the system correctly reports alarm to the backup reporting service after failing to communicate with the primary service. • Re-enable the primary reporting service.
Test system inputs and areas programmed to report	As agreed between monitoring company and client, but not less than once per year	**Note**: This procedure must be pre-arranged in consultation with the monitoring station. • Consult the maintenance sheets for a list of all inputs to be tested. • Activate each input by causing it to switch from the closed state to open (alarm) and back to closed. • Check the system event log for associated open/close events. • Check off each input on the maintenance sheet after successful testing and report any discrepancies. • Return all alarm areas to their pre-test states. • Obtain an activity report of all input opens/closes and area alarms/restores from the monitoring station. • Compare the monitoring station report with the system event log for the period to ensure that all tested inputs and areas reported correctly. Record and report any discrepancies. Special testing equipment and procedures may be required for smoke, heat, seismic glass-break and other detectors.

Task	Frequency	Description
Test warning device outputs	As agreed between monitoring company and client, but not less than once per year May be performed alongside Input Testing (above)	**Note**: This procedure must be pre-arranged in consultation with the monitoring station. Test the operation of each audible and visible warning device. • Consult the maintenance sheets for a list of all outputs to be tested. • Arm any relevant areas. • Activate each warning device, either by user operation or by triggering an alarm which should cause activation. • Check that each warning device works as specified. Record and report any discrepancies. • Reset/Restore alarm areas to their previous state.

Software Maintenance Procedures

Task	Frequency	Description
Back up programming database	Recommended monthly	Backups of the programming database should be performed on a regular basis. It is vital that backups be stored offsite for disaster recovery. See the Operator Reference Manual for instructions on how to backup your database.
Back up events database	Recommended monthly	Backups or exports of recorded events should be performed on a regular basis. Verify that the backup file has been created. See the Operator Reference Manual for instructions on how to backup your database.

Follow-up Procedures

Task	Frequency	Description
Perform necessary system modifications	As required	Complete any modifications to the system resulting from the maintenance procedures. Record these in the maintenance sheets and report.
Obtain client sign off	At the conclusion of each maintenance visit	Obtain the signature of the client or the client's representative on the maintenance record.

European Standards

CE Statement CE

Conforms where applicable to European Union (EU) Low Voltage Directive (LVD) 2014/35/EU, Electromagnetic Compatibility (EMC) Directive 2014/30/EU, Radio Equipment Directive (RED)2014/53/EU and RoHS Recast (RoHS2) Directive: 2011/65/EU + Amendment Directive (EU) 2015/863.

This equipment complies with the rules, of the Official Journal of the European Union, for governing the Self Declaration of the CE Marking for the European Union as specified in the above directive(s).

WEEE

Information on Disposal for Users of Waste Electrical & Electronic Equipment

This symbol on the product(s) and / or accompanying documents means that used electrical and electronic products should not be mixed with general household waste. For proper treatment, recovery and recycling, please take this product(s) to designated collection points where it will be accepted free of charge.

Alternatively, in some countries you may be able to return your products to your local retailer upon purchase of an equivalent new product.

Disposing of this product correctly will help save valuable resources and prevent any potential negative effects on human health and the environment, which could otherwise arise from inappropriate waste handling.

Please contact your local authority for further details of your nearest designated collection point.

Penalties may be applicable for incorrect disposal of this waste, in accordance with your national legislation.

For business users in the European Union

If you wish to discard electrical and electronic equipment, please contact your dealer or supplier for further information.

Information on Disposal in other Countries outside the European Union

This symbol is only valid in the European Union. If you wish to discard this product please contact your local authorities or dealer and ask for the correct method of disposal.

EN50131 Standards

This component meets the requirements and conditions for full compliance with EN50131 series of standards for equipment classification.

EN 50131-1:2006+A2:2017, EN 50131-3:2009, EN 50131-6:2008+A1:2014, EN 50131-10:2014, EN 50136-1:2012, EN 50136-2:2013, EN 60839-11-1:2013

This component meets the requirements and conditions for full compliance with EN50131-3 (2010) 8.10.1 and EN50131-1 (2006) 8.10 when connected to a compliant ARC (Alarm Reporting Centre).

Security Grade 4
Environmental Class II
Equipment Class: Fixed
Readers Environmental Class: IVA, IK07
SP1 (PSTN – voice protocol)
SP2 (PSTN – digital protocol),
SP6 (LAN – Ethernet) and DP1 (LAN – Ethernet + PSTN)
SP6 (LAN – Ethernet) and DP1 (LAN – Ethernet + USB-4G modem)

Tests EMC (operational) according to EN 55032:2015
Radiated disturbance EN 55032:2015
Power frequency magnetic field immunity tests (EN 61000-4-8)

EN50131

In order to comply with EN 50131-1 the following points should be noted:

- Ensure for Grade 3 or 4 compliant systems, the minimum PIN length is set for 6 digits.
- To comply with EN 50131-1 Engineer access must first be authorized by a user, therefore Installer codes will only be accepted when the system is unset. If additional restriction is required then Engineer access may be time limited to the first 30 seconds after the system is unset.
- Reporting delay –Violation off the entry path during the entry delay countdown will trigger a warning alarm. The warning alarm should not cause a main alarm signal and is not reported at this time. It can be signaled locally, visually and or by internal siren type. If the area is not disarmed within 30 seconds, the entry delay has expired or another instant input is violated, the main alarm will be triggered and reported.
- To comply with EN 50131-1 neither Internals Only on Part Set Input Alarm nor Internals Only on Part Set Tamper Alarm should be selected.
- To comply with EN 50131-1 Single Button Setting should not be selected.
- To comply with EN 50131-1 only one battery can be connected and monitored per system. If more capacity is required a single larger battery must be used.
- For Security Grade 4 installations, two forms of reporting are required. This can be satisfied using the onboard 2400bps modem included with the modem controller model, or through the incorporation of the PRT-4G-USB cellular modem module into the installation with the non-modem controller model.

Anti Masking

To comply with EN 50131-1 Grade 3 or 4 for Anti Masking, detectors with a separate or independent mask signal should be used and the mask output should be connected to another input.

I.e. Use 2 inputs per detector. One input for alarm/tamper and one input for masking.

To comply with EN 50131-1:

- Do not fit more than 10 unpowered detectors per input,
- Do not fit more than one non-latching powered detector per input,
- Do not mix unpowered detectors and non-latching powered detectors on an input.

To comply with EN 50131-1 the Entry Timer should not be programmed to more than 45 seconds.

To comply with EN 50131-1 the Bell Cut-Off Time should be programmed between 02 and 15 minutes.

EN 50131-1 requires that detector activation LEDs shall only be enabled during Walk Test. This is most conveniently achieved by using detectors with a Remote LED Disable input.

To comply with EN 50131-1, EN 60839-11 Security Grade 4 and AS/NZS2201.1 class 4&5 Vibration Detection for PreTamper Alarm, protection is provided by a DSC SS-102 Shockgard Seismic vibration sensor mounted within the system enclosure. Alarm output is provided by a pair of non-latching, N.C. (normally closed) relay contacts, opening for a minimum of 1 second on detection of an alarm connected in series with the 24Hr tamper input (TP) on the PSU (or any other system input designated/programmed as a 24Hr Tamper Alarm).

This relay is normally energized to give fail-safe operation in the event of a power loss. Indication of detection is provided by a LED situated on the front cover. The vibration sensor is fully protected from tampering by a N.C. micro switch operated by removal of the cover.

Enclosure EN-DIN-24 has been tested and certified to EN50131.

By design, the enclosures for all Integrated Control Technology products, EN-DIN-11, EN-DIN-12 and EN-DIN-24-ATTACK, comply with the EN 50131 standards. Tamper protection against removal of the cover as well as removal from mounting is provided by tamper switch.

Warning: Enclosures supplied by 3rd parties may not be EN50131-compliant, and should not be claimed as such.

UK Conformity Assessment Mark

General Product Statement

The UKCA Compliance Label indicates that the supplier of the device asserts that it complies with all applicable standards.

UK CA

UK PD 6662:2017 and BS 8243

Protege systems conform to PD 6662:2017 and BS 8243 at the security grade and notification option applicable to the system.

FCC Compliance Statements

FCC Rules and Regulations CFR 47, Part 15, Subpart B

This equipment complies with the limits for a Class A digital device, pursuant to Part 15 of the FCC rules.

Operation is subject to the following two conditions:

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

NOTE: THE GRANTEE IS NOT RESPONSIBLE FOR ANY CHANGES OR MODIFICATIONS NOT EXPRESSLY APPROVED BY THE PARTY RESPONSIBLE FOR COMPLIANCE. SUCH MODIFICATIONS COULD VOID THE USER'S AUTHORITY TO OPERATE THE EQUIPMENT.

Industry Canada Statement

ICES-003

This class A digital apparatus complies with Canadian ICES-003.
Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.

CAN ICES-3 (A)/NMB-3(A)

Disclaimer and Warranty

Disclaimer: Whilst every effort has been made to ensure accuracy in the representation of this product, neither Integrated Control Technology Ltd nor its employees shall be liable under any circumstances to any party in respect of decisions or actions they may make as a result of using this information. In accordance with the ICT policy of enhanced development, design and specifications are subject to change without notice.

For warranty information, see our Standard Product Warranty.