PRT-CTRL-DIN

Protege GX DIN Rail Integrated System Controller

Installation Manual

Last Published: 20-Jan-26 1:02 PM

Contents

Introduction

This installation manual provides instructions and technical specifications for physical installation of the Protege GX DIN Rail Integrated System Controller module. 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 Integrated System 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 PRT-CTRL-DIN 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
- 8 high security monitored inputs
- 4 open collector outputs
- 2 Form C Relay outputs
- 1 USB Port
- Built-in offsite communications dialer (Contact ID or SIA)
- Industry standard DIN rail mounting

Controller Editions

There are two editions of the PRT-CTRL-DIN controller:

- The **PRT-CTRL-DIN-IP** can communicate alarms and upload information to remote systems over IP, using an ethernet or mobile internet connection.
- The **PRT-CTRL-DIN** can communicate alarms and upload information to remote systems over IP, using an ethernet or mobile internet connection. It also includes a built-in 2400bps modem dialer which allows it to communicate alarms and upload information to remote systems via PSTN using Contact ID or SIA protocols.

Installation Requirements

This equipment is to be installed in accordance with:

- The product installation instructions
- UL 294 - Access Control System Units
- UL 681 - Installation and Classification of Burglar and Holdup Systems
- UL 827 - Central-Station Alarm Services
- CAN/ULC-S301, Central and Monitoring Station Burglar Alarm Systems
- CAN/ULC-S302, Installation and Classification of Burglar Alarm Systems for Financial and Commercial Premises, Safes and Vaults
- CAN/ULC-S561, Installation and Services for Fire Signal Receiving Centres and Systems
- CAN/ULC-60839-11-1, Alarm and Electronic Security Systems – Part 11-1: Electronic Access Control Systems – System and Components Requirements
- The National Electrical Code, ANSI/NFPA 70
- The Canadian Electrical Code, Part I, CSA C22.1
- AS/NZS 2201.1 Intruder Alarm Systems
- The Local Authority Having Jurisdiction (AHJ)

Wiring

For UL/cUL installations, the following wiring specifications must be observed.

Earth Ground Wiring: Minimum 14AWG solid copper wire.

Input Wiring: Maximum distance of 300m (1000ft) from the connected module when using 22 AWG.

Aux Wiring: Minimum 22AWG, maximum 16AWG (depends on length and current consumption).

For wire/cable size, a maximum of 5% voltage drop at the terminals of the powered device must be observed.

Ethernet Wiring: CAT5e / CAT6. Maximum length 100m (330 ft).

Module Network Wiring:

- Minimum 24AWG (0.51mm) shielded twisted pair with characteristic impedance of 120Ω. Maximum length 900m (3000ft).
- CAT5e / CAT6 also supported for data transmission when using ground in the same cable. Maximum length 100m (330 ft).

Do not use extra wires in the cable to power devices.

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 that 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.

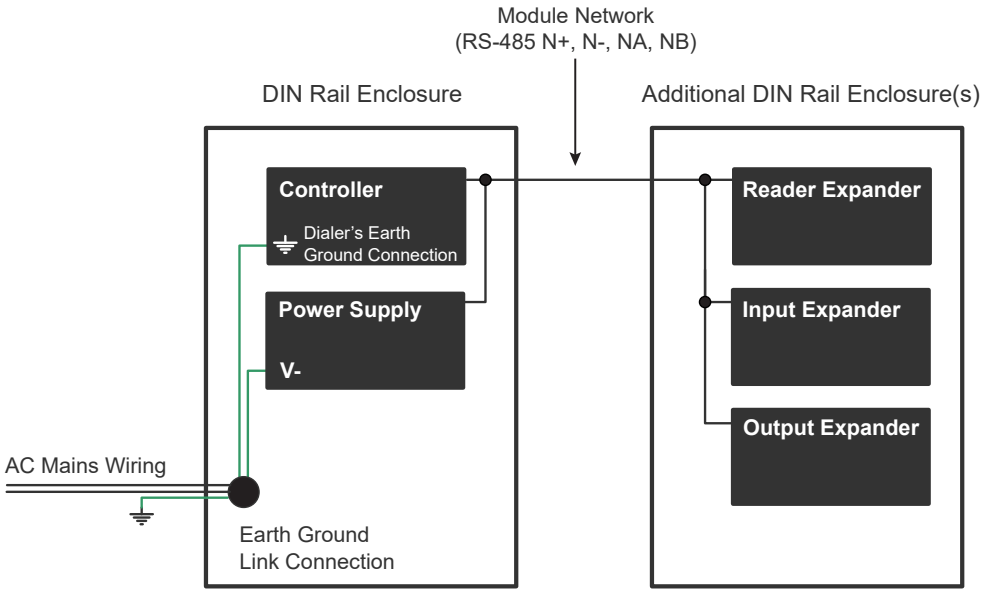
Warning: All cabinet internal covers and lids/doors must be connected to the cabinet's main ground point for electrical safety and static discharge protection.

Earth Ground Connection

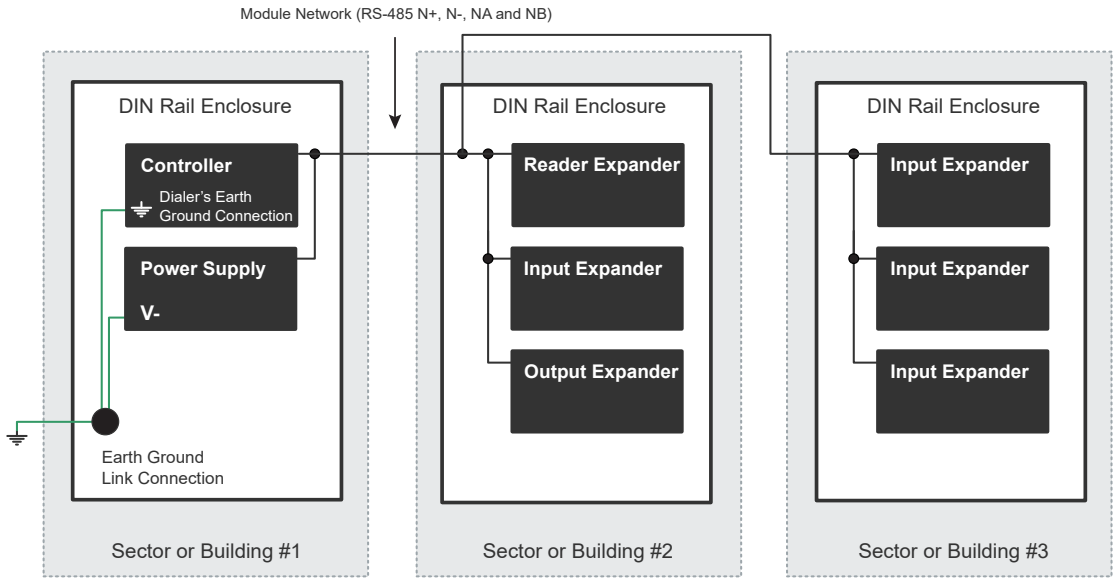
The DIN rail enclosure and the DIN rail modules must be grounded to a suitable single-point earth ground connection in the installation. A minimum 14AWG solid copper wire (or thicker, in accordance with local authorities) shall be used from the Protege system's earth connection points.

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)



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.

Location

Protege DIN rail modules must be installed indoors, within the protected area. Modules must be protected by a secure cabinet with tamper detection.

We recommend installing the cabinet in a location that provides easy access for wiring. Suitable locations include electrical rooms, communication equipment rooms and accessible areas of the ceiling. Ensure that there is adequate clearance around each device and that air flow to the vents is not restricted.

Protege DIN rail modules must not be installed outdoors. Ensure that the room does not exceed or fall below the operating temperature or humidity ranges listed in the Technical Specifications for each module. Do not mount cabinets on the exterior of a vault, safe or stockroom.

For UL/cUL installations, you must use a UL- or cUL-listed enclosure. See the full certification list in the UL/cUL-Listed Protege Enclosures document, available from the ICT website.

All cabinet installations of this type must be located **inside the Protected Area**. **Not** to be mounted on the exterior of a vault, safe or stockroom.

Mounting a DIN Rail Module

To mount a module onto DIN rail:

1. Position the 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.

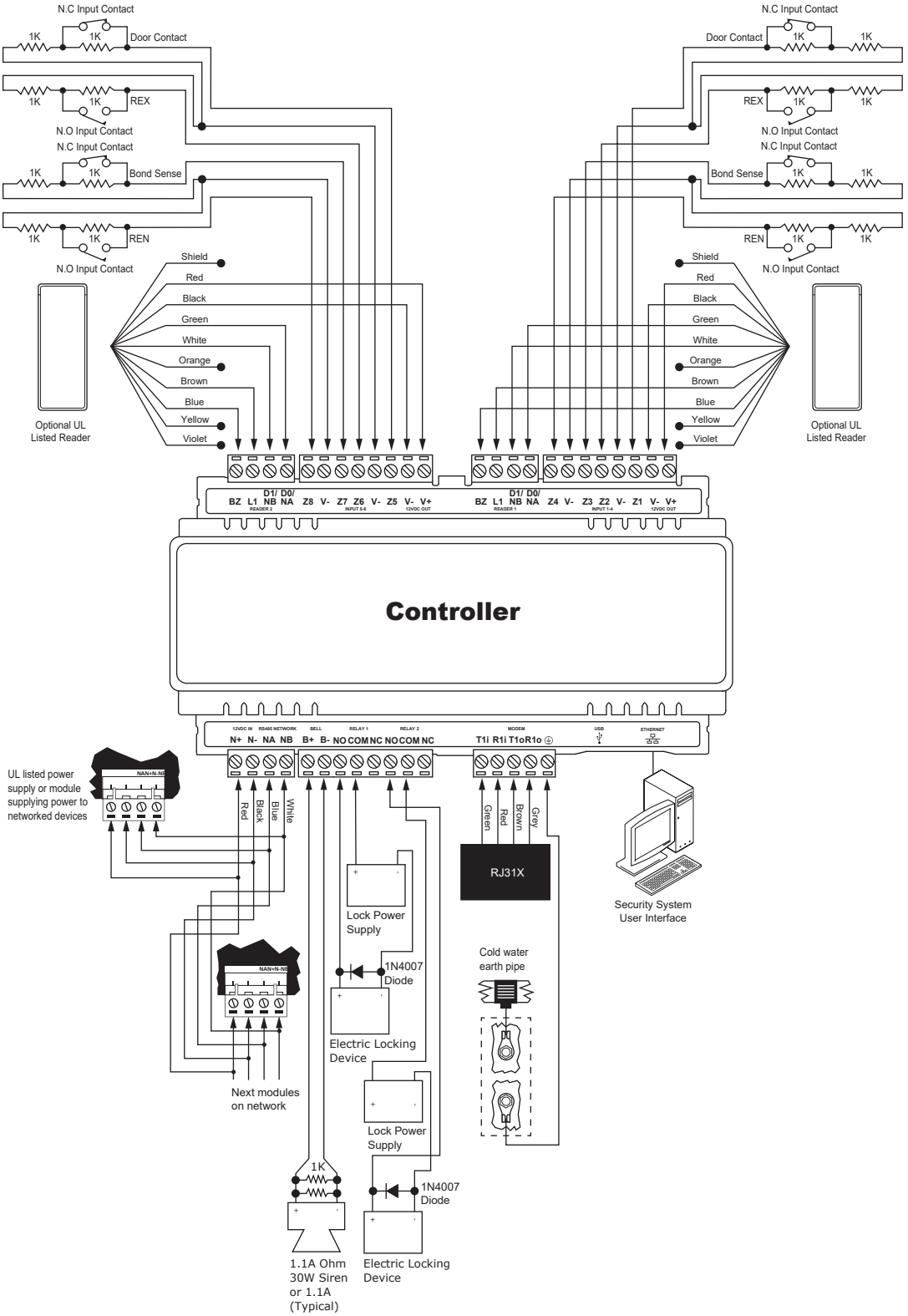
Removal

To remove the DIN rail module from the DIN rail mount:

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

Wiring Diagram

Notice: Incorrect wiring may result in damage to the unit.



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.

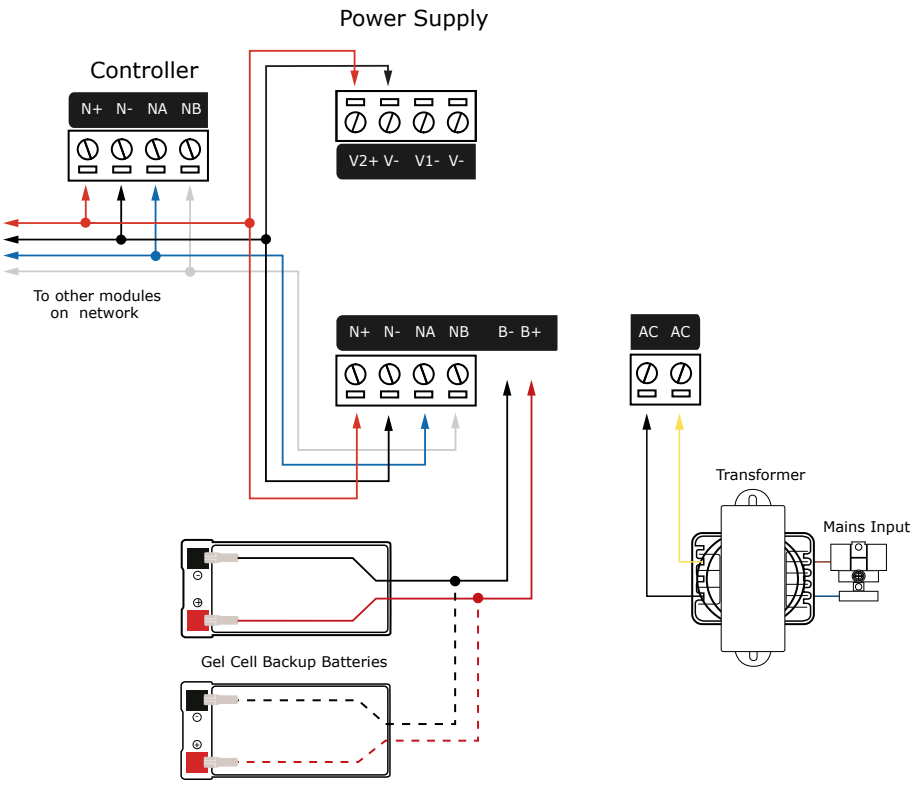
Termination of wiring to the module while power is applied or the battery is connected may cause serious damage to the unit and will VOID ALL WARRANTIES OR GUARANTEES.
Power the unit only after all wiring, configuration and jumper settings are completed.

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.

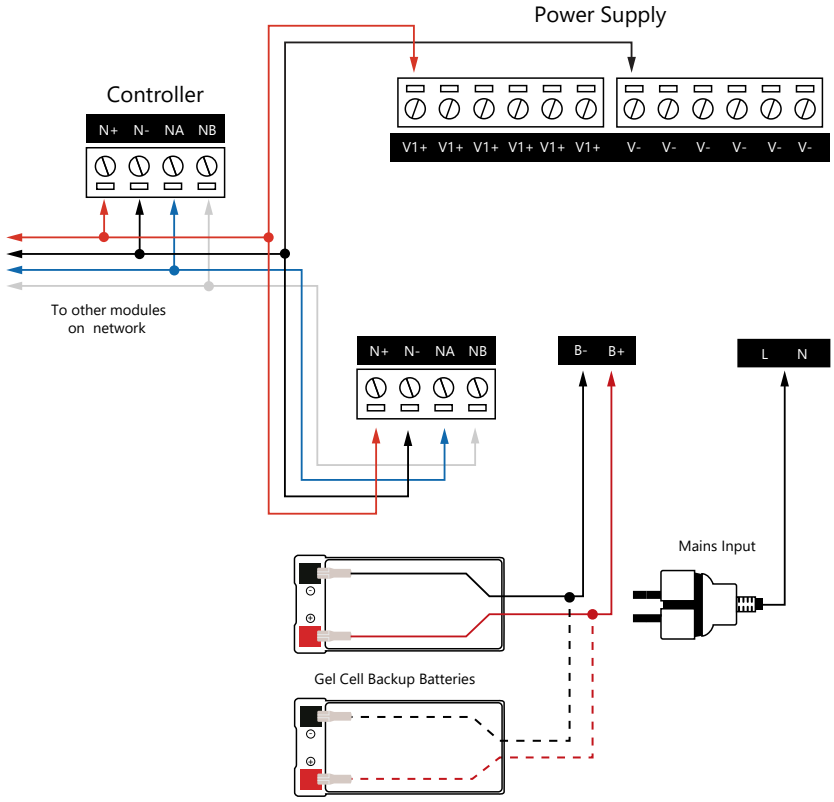
For UL applications, must be powered by a UL Listed (UL 603 or UL 294) power limited power supply capable of supplying at least 4 hours of standby power.

For cUL applications, must be powered by a cUL Listed (CAN/ULC S318 or CAN/ULC S319) power limited power supply capable of supplying at least 24 hours of standby power.

Example 2A Power Supply Connection:



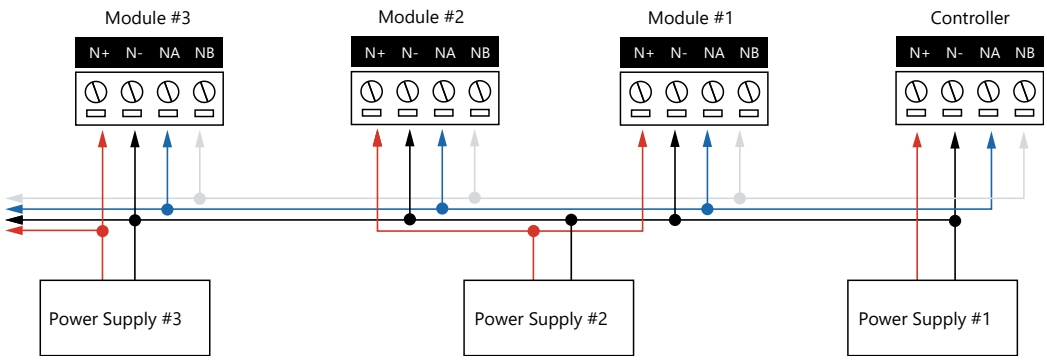
Example 4A Power Supply Connection:



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:



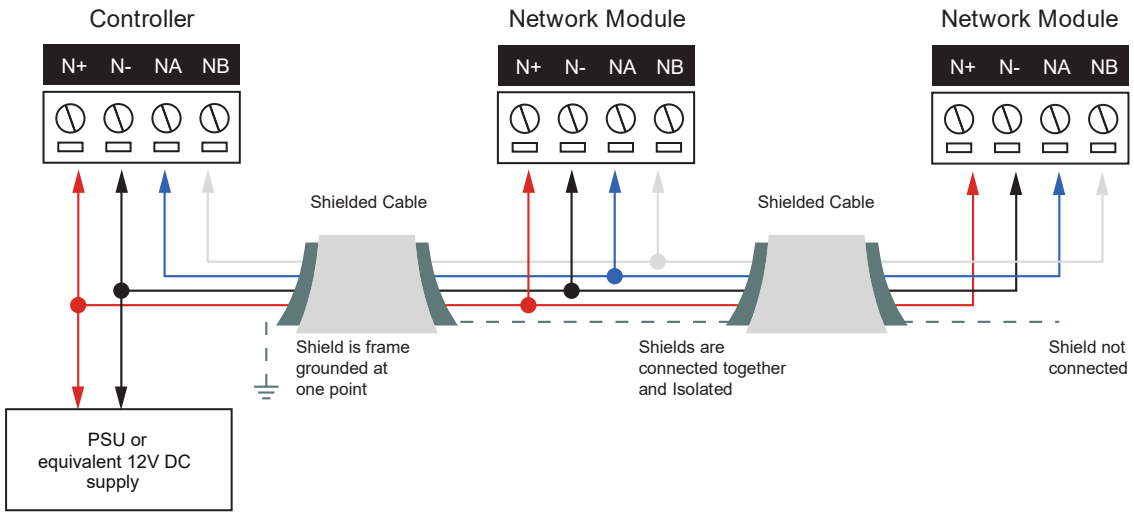
When using multiple power supplies it is important to ensure that all ground connections (V-) are connected between all power supplies and that no power connections (V+) are connected between any power supplies.

Auxiliary Outputs

The auxiliary outputs (V- V+) 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.

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:

- Minimum 24AWG (0.51mm) shielded twisted pair with characteristic impedance of 120Ω
- 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))

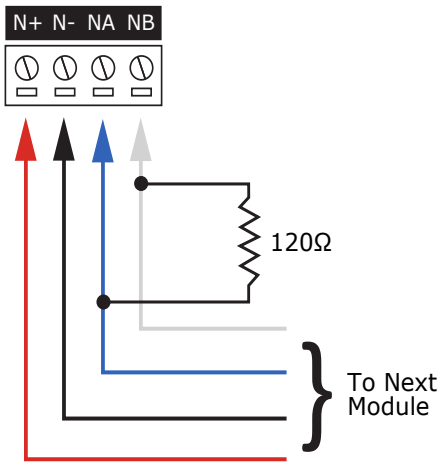
Warning: Unused wires in the cable must not be used to carry power to other devices.

End-of-Line (EOL) Resistors

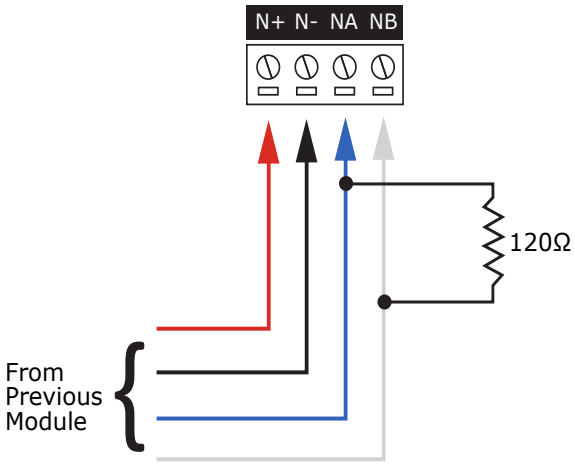
End-of-line resistors prevent signal reflections at the ends of the RS-485 network bus, improving signal strength and reducing data corruption.

You must insert a **120Ω resistor** 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



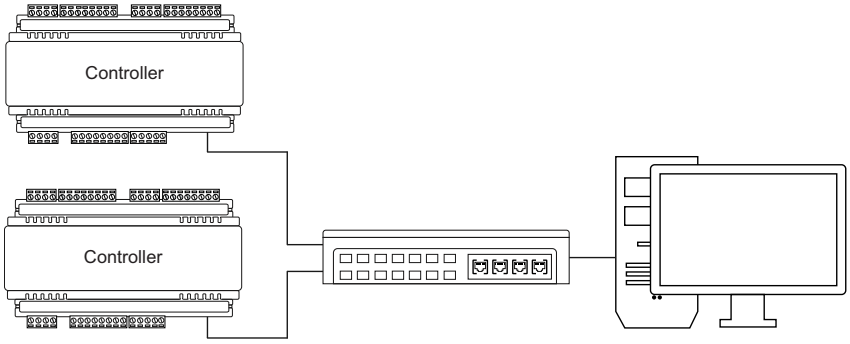
Ethernet 10/100 Network Interface

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.

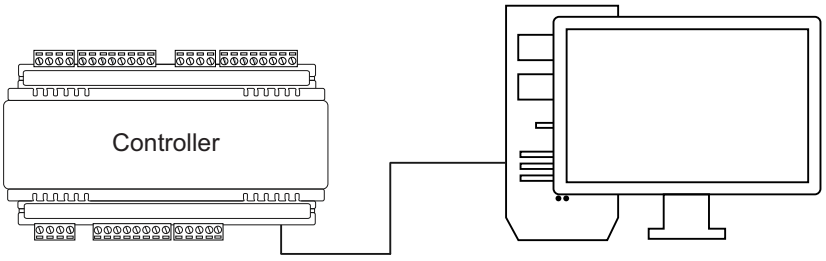
When installing an ethernet connection the module should be interfaced using a standard segment (<100m in length) and should be connected to a suitable ethernet hub or switch:

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:



- All network equipment such as hubs/routers/gateways used with the controller must comply with the UL and cUL standard requirements associated with a signal receiving center.
- The controller must be installed in the same room as the network equipment that provides it the network connection.

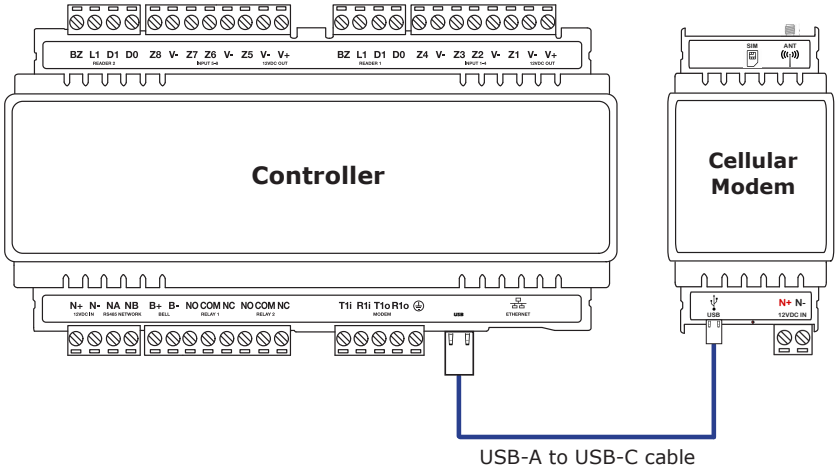
Cellular Modem/Router

The controller can communicate alarms and upload information to remote systems via mobile internet, using the Protege DIN Rail Cellular Modem (PRT-4G-USB) or a compatible third-party cellular router. The modem or router is connected to the controller's Type-A USB port.

Older Protege controllers without USB ports do not support this feature.

Protege DIN Rail Cellular Modem

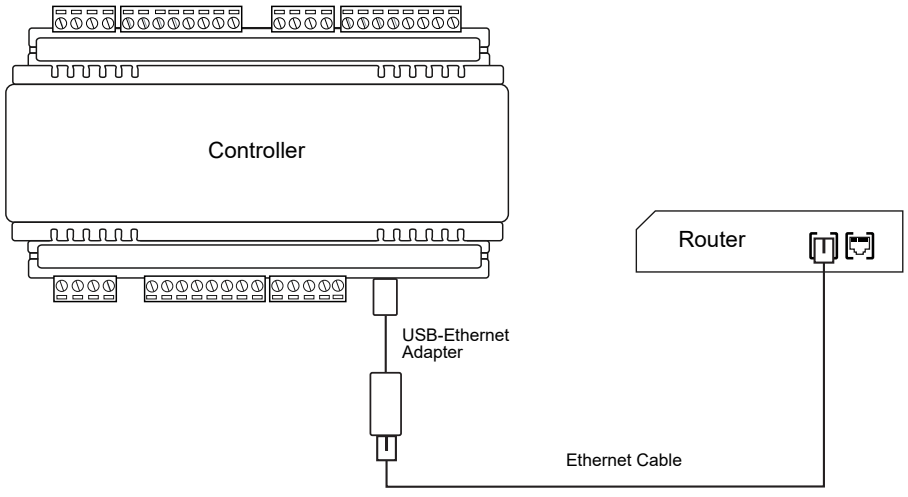
The Protege DIN Rail Cellular Modem can be connected directly to the controller using a USB-A to USB-C cable.



For more information, see the Protege DIN Rail Cellular Modem Installation Manual and Protege DIN Rail Cellular Modem Configuration Guide.

Third-Party Cellular Router

The controller can be connected to a third-party cellular router using a compatible USB-Ethernet adapter.

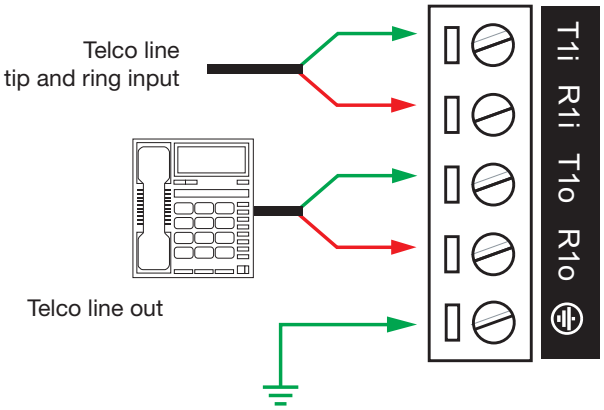


For information about compatible adapters and routers, see the controller configuration guide.

Connection to a third-party cellular router has not been evaluated by UL/cUL. Use the Protege DIN Rail Cellular Modem for UL/cUL installations.

Telephone Dialer

The controller provides the ability to communicate alarms and upload information to remote systems using the onboard 2400bps modem. The telephone line can be connected directly to the controller using the onboard telephone connection terminals.



Door Access Control

The controller provides access control functionality onboard without the requirement for additional hardware, allowing the connection of up to 4 reading devices controlling 2 doors with entry and exit readers. Each reader port can be independently configured to support one of the following protocols:

- ICT RS-485 (ICT readers only)
- OSDP (Open Supervised Device Protocol)
- Wiegand

Recommended Cabling

The recommended cable specifications for ICT RS-485 and OSDP are:

- Minimum 24AWG (0.51mm) shielded twisted pair with characteristic impedance of 120 ohm
- Maximum distance: 900m (3000ft)

Wiegand cables are **not** suitable for ICT RS-485 and OSDP connections. RS-485 communications over Wiegand data lines are affected by interference between the data wires, which can cause corrupted card reads and readers dropping offline. If you are transitioning a site from Wiegand to RS-485, we strongly recommend that you replace the existing Wiegand cables with shielded twisted pair cables.

The recommended cable specifications for Wiegand are:

- 22AWG alpha 5196, 5198, 18AWG alpha 5386, 5388
- Maximum distance: 150m (492ft)

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

Shield Connection

- Use a shielded cable to connect the card reader to the module port.
- Frame ground the shield to the metallic enclosure at one end only.
- 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 pigtail shield and cable shield wires should be joined at the reader pigtail splice.
- 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.

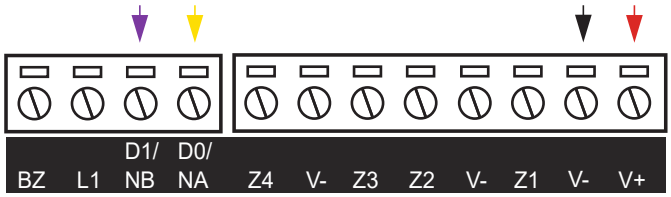
Always refer to the card reader manufacturer for detailed installation guidelines.

RS-485 Reader Connection

ICT readers can be connected to a Protege controller in RS-485 configuration. The following shows the connection of a single RS-485 reader for entry only.

Third-party RS-485 readers can only be connected using the OSDP protocol (see page 22).

Reader Port Connections



Reader Wiring Connections

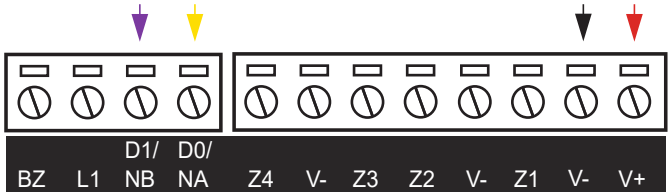
The reader should be connected using the wiring configuration outlined in the table below.

Reader Wire	Connection
12VDC+ positive	**V+** 12VDC positive
12VDC- negative	**V-** 12VDC negative
RS-485 **A**	**D0/NA** RS-485 A
RS-485 **B**	**D1/NB** RS-485 B
Shield (drain)	Frame grounded at one point only

RS-485 Reader Connection (Entry/Exit)

The following shows the connection of two RS-485 readers to provide an entry/exit configuration.

Reader Port Connections



Primary Reader Wiring Connections

The primary reader should be connected using the wiring configuration outlined in the table below.

Reader Wire	Connection
12VDC+ positive	**V+** 12VDC positive
12VDC- negative	**V-** 12VDC negative
RS-485 **A**	**D0/NA** RS-485 A
RS-485 **B**	**D1/NB** RS-485 B
Shield (drain)	Join the shield (drain) wires together. Frame grounded at one point only

Secondary Reader Wiring Connections

The secondary reader should be connected using the wiring configuration outlined in the table below.

Reader Wire	Connection
12VDC+ positive	Join to primary reader **12VDC+** positive wire
12VDC- negative	Join to primary reader **12VDC-** negative wire
RS-485 **A**	Join to primary reader RS-485 **A** wire
RS-485 **B**	Join to primary reader RS-485 **B** wire
Shield (drain)	Join the shield (drain) wires together. Frame grounded at one point only

RS-485 Reader Location

As two RS-485 readers can be connected to the same reader port, the reader **address** uniquely identifies each reader and determines which is the entry reader and which is the exit reader.

Configuration	Location
Reader address = **0**	Entry
Reader address = **1**	Exit

All ICT readers use address 0 (entry) by default, unless configured otherwise. The reader's address can be configured by applying the required reader address TLV setting to the reader programming.

For programming instructions, see the ICT Card Reader Configuration Guide, available from the ICT website.

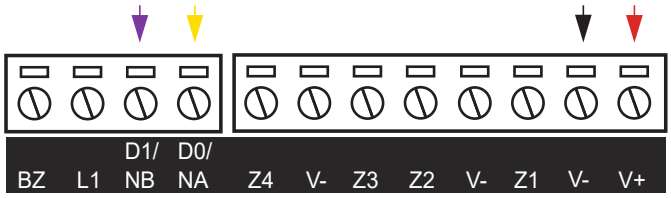
tSec readers are hardwired to use address 1 when the reader's **green** and **orange** wires are joined together. For more information, see the tSec reader installation manual.

OSDP Reader Connection

When using the OSDP protocol the reader is connected to the reader port using a standard RS-485 wiring configuration. The following shows the connection of a single OSDP reader for entry only.

Connection of two OSDP readers to provide an entry/exit configuration follows the same connection requirements as connecting two RS-485 readers (see previous page).

Reader Port Connections



This connection example shows wiring for ICT readers. Other readers may use different color configurations. Always refer to the card reader manufacturer for detailed installation guidelines, and see the table below.

Reader Wiring Connections

The reader should be connected using the wiring configuration outlined in the table below.

Reader Wire	Connection
12VDC+ positive	**V+** 12VDC positive
12VDC- negative	**V-** 12VDC negative
RS-485 **A**	**D0/NA** RS-485 A
RS-485 **B**	**D1/NB** RS-485 B
Shield (drain)	Frame grounded at one point only

Consult the manufacturer's documentation for wiring instructions for the specific reader being connected.

Connecting OSDP readers to Protege modules requires additional hardware configuration and system programming. For more information, see Application Note 254: Configuring OSDP Readers in Protege.

For more information about OSDP support on ICT card readers, including configuring readers for secure channel communications, see Application Note 321: Configuring ICT Readers for OSDP Communication.

OSDP Reader Location

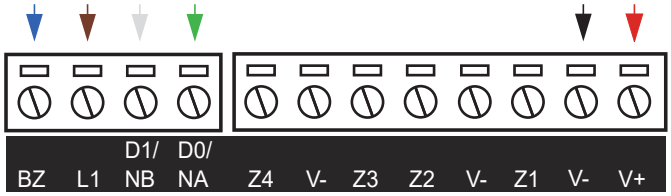
You can connect two OSDP readers to each Protege module's reader port. Each OSDP reader is configured as either an Entry or Exit reader in the **Reader location** setting of the associated **smart reader** record.

The default addresses are 0 for entry and 1 for exit. However, these can be any two unique addresses from 0-127. OSDP reader location is **not** determined by the reader address.

Wiegand Reader Connection

The following shows the connection of a single Wiegand reader for entry only.

Reader Port Connections



This connection example shows wiring for ICT readers. Other readers may use different color configurations. Always refer to the card reader manufacturer for detailed installation guidelines, and see the table below.

Reader Wiring Connections

The reader should be connected using the wiring configuration outlined in the table below.

Reader Wire	Connection
12VDC+ positive	**V+** 12VDC positive
12VDC- negative	**V-** 12VDC negative
Wiegand **Data 0**	**D0/NA** Wiegand Data 0
Wiegand **Data 1**	**D1/NB** Wiegand Data 1
Wiegand **LED** control	**L1** Wiegand LED control
Wiegand **beeper** control	**BZ** Wiegand beeper control
Shield (drain)	Frame grounded at one point only

Multiple Wiegand Reader Connection

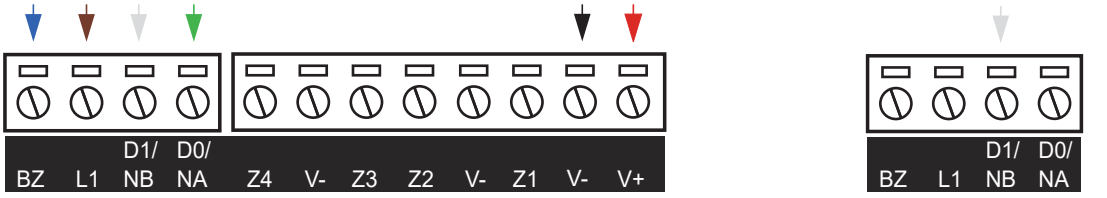
In multiple reader mode, the secondary card reader has all connections wired to the same reader port as the primary reader, except the Data 1 connection which is wired to the Data 1 input on the alternate reader port.

The normal primary reader connection operates as the **entry** reader, and the secondary reader that is multiplexed into the alternate reader port will operate as the **exit** reader.

To connect two Wiegand readers to a reader port the **Multiple reader input port 1/2** option must be enabled in the reader expander programming. When this option is disabled the reader port will only process a single reader.

The following shows the connection of two Wiegand readers to provide an entry/exit configuration.

Reader Port Connections



Primary Reader Port **Alternate Reader Port**

This connection example shows wiring for ICT readers. Other readers may use different color configurations. Always refer to the card reader manufacturer for detailed installation guidelines, and see the table below.

Entry Reader Wiring Connections

The entry reader should be connected using the wiring configuration outlined in the table below.

Reader Wire	Connection
12VDC+ positive	**V+** 12VDC positive
12VDC- negative	**V-** 12VDC negative
Wiegand **Data 0**	**D0/NA** Wiegand Data 0
Wiegand **Data 1**	**D1/NB** Wiegand Data 1
Wiegand **LED** control	**L1** Wiegand LED control
Wiegand **beeper** control	**BZ** Wiegand beeper control
Shield (drain)	Join the shield (drain) wires together. Frame grounded at one point only

Exit Reader Wiring Connections

The exit reader should be connected using the wiring configuration outlined in the table below.

Reader Wire	Connection
12VDC+ positive	Join to entry reader **12VDC+** positive wire
12VDC- negative	Join to entry reader **12VDC-** negative wire
Wiegand **Data 0**	Join to entry reader Wiegand **Data 0** wire
Wiegand **Data 1**	**D1/NB** Wiegand Data 1 (alternate reader port to entry reader)
Wiegand **LED** control	Join to entry reader Wiegand **LED** control wire
Wiegand **beeper** control	Join to entry reader Wiegand **beeper** control wire
Shield (drain)	Join the shield (drain) wires together. Frame grounded at one point only

Connecting 4 Wiegand Readers

Multiple reader mode allows the connection of 4 Wiegand readers controlling 2 doors, each with entry and exit readers. To connect 4 Wiegand reading devices:

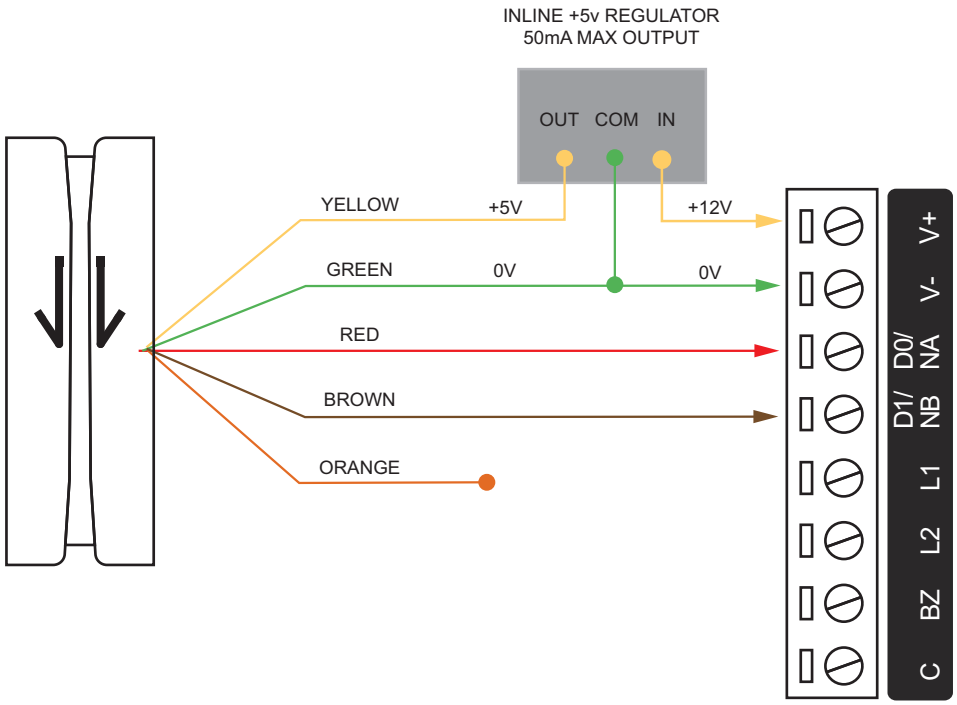
- Door 1 entry reader is connected to reader **port 1**
- Door 1 exit reader has its Wiegand Data 1 wire connected to the reader **port 2** D1 connection
- Door 2 entry reader is connected to reader **port 2**
- Door 2 exit reader has its Wiegand Data 1 wire connected to the reader **port 1** D1 connection
- The **Multiple reader input port 1** option is enabled in the reader expander programming (General | Options)
- The **Multiple reader input port 2** option is enabled in the reader expander programming (General | Options)

To connect two Wiegand readers to a reader port the **Multiple reader input port 1/2** option must be enabled in the reader expander programming. When this option is disabled the reader port will only process a single reader.

Magnetic Reader Connection

The controller allows the connection of standard magnetic track 2 format cards and provision is made in the software for a large number of formats. Formats include BIN number for ATM access control and first 4, 5 and 6 card numbers.

Magnetic Card Reader Interface:

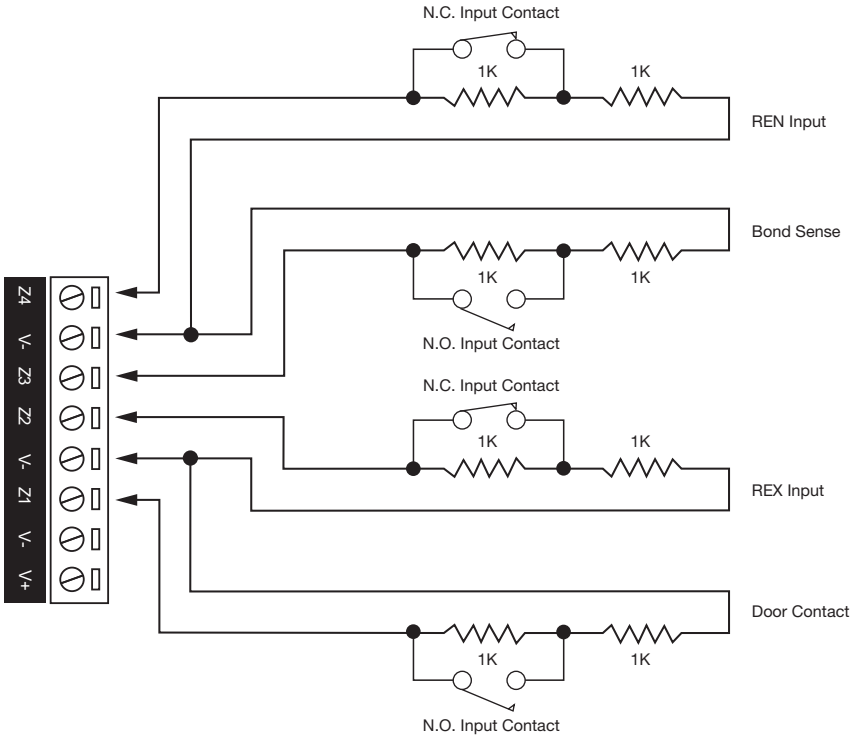


Magnetic card readers are typically operated by 5 volts. Before connecting the magnetic card reader to the controller, ensure that the supply voltage is correct and if required insert the inline 5 Volt regulator as shown in the diagram above.

The magnetic reader connection has not been evaluated for UL/cUL applications.

Door Contact Connection

The module allows the connection of up to 4 contacts for monitoring and controlling access control doors. Each input can be used for either the door function that is automatically assigned or as a normal input on the system. The following example shows the connection of a normally closed door position monitoring contact to monitor the open, closed, forced and alarm conditions of the door.



Inputs 1-4 and 5-8 can operate as either general purpose inputs or as onboard reader inputs. If used as general purpose inputs, make sure that these inputs are not defined in the onboard reader set up.

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
Input 3	Bond Sense, Port 1	General Purpose Input
Input 4	REN Input, Port 1	General Purpose Input
Input 5	Door Contact, Port 2	Door Contact, Port 2
Input 6	REX input, Port 2	REX Input, Port 2
Input 7	Bond Sense, Port 2	General Purpose Input
Input 8	REN Input, Port 2	General Purpose Input

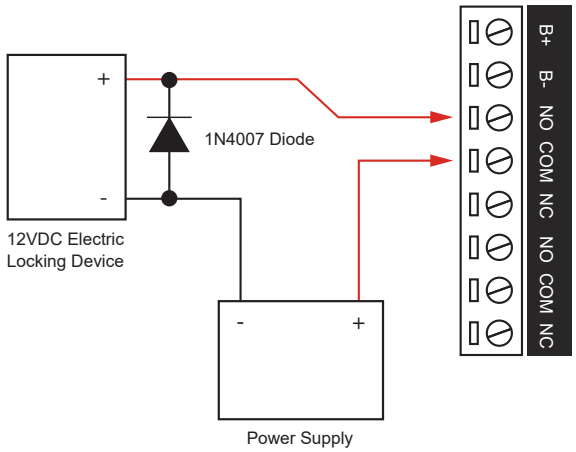
When connected the REX input can be programmed to operate regardless of the door contact state. The REX input can also be programmed to recycle the door alarm time to prevent nuisance alarms when the door is held open to permit longer entry.

When inputs are configured as bond sense and/or general purpose inputs (access control and burglar installations), remaining inputs cannot be used for fire.

Lock Output Connection

The controller provides relays on outputs 3 and 4. These are used for the Lock 1 (Output 3 CP001:03) and Lock 2 (Output 4 CP001:04) functions and are used to control electric door strikes and other lock control devices.

To use the lock outputs 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.



The locking device is connected to the **NO** terminal, as displayed above, for power to unlock / fail secure devices. For power to lock / fail safe devices the locking device is connected to the **NC** terminal.

The 1N4007 diode is supplied for lock output connections and **must** be installed at the electric strike terminals.

Warning: Relay outputs can switch to a maximum capacity of 7A. Exceeding 7A will damage the output.

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 1-4 and 5-8 as its door contact, REX, bond sense and REN inputs 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.

REX and REN devices must be listed to UL 294 for UL installations and CAN/ULC-S319 for cUL installations, and be compatible with the system.

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
Input 3	Bond Sense, Port 1	General Purpose Input
Input 4	REN Input, Port 1	General Purpose Input
Input 5	Door Contact, Port 2	Door Contact, Port 2
Input 6	REX input, Port 2	REX Input, Port 2
Input 7	Bond Sense, Port 2	General Purpose Input
Input 8	REN Input, Port 2	General Purpose Input

Onboard Reader Trouble Inputs

The onboard reader expander can monitor up to 16 trouble inputs used to report associated trouble conditions.

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

Input Number	Description	Default Trouble Group	Default Trouble Group Option
RDxxx:01-11	Reserved	None	None
RDxxx:12	Reader 1 Tamper	System	System Tamper
RDxxx:13	Reader 2 Tamper	System	System Tamper
RDxxx:14	Door 1 Lockout	Access	Too Many Attempts
RDxxx:15	Door 2 Lockout	Access	Too Many Attempts
RDxxx:16	Module Offline	System	Module Offline

Replace 'xxx' with the address of the module that you are programming.

Door Trouble Inputs

In addition to the trouble inputs of the module itself, the onboard reader can also monitor trouble inputs associated with connected doors. These are used for monitoring and reporting door troubles such as door forced and duress conditions.

Input Number	Description	Default Trouble Group	Default Trouble Group Option
Door xxx 01	Door Forced	Access	Forced Door
Door xxx 02	Door Left Open	Access	Left Open
Door xxx 08	Door Duress	None	None

'xxx' refers to the **Name** of the door in the Protege system.

Inputs

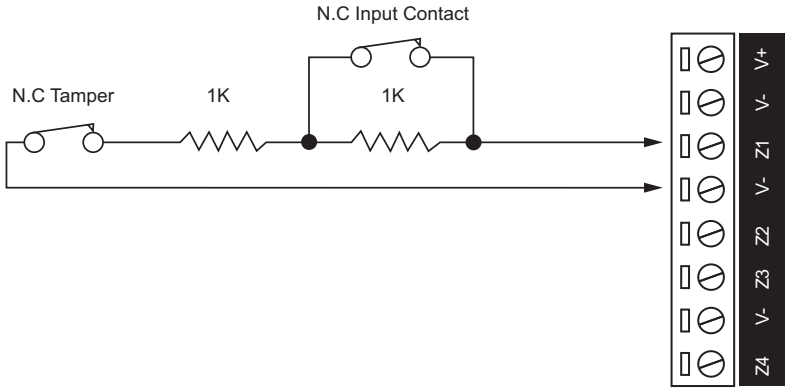
The controller has 8 onboard inputs for monitoring the state of devices such as magnetic contacts, motion detectors and temperature sensors. Devices connected to the inputs can be installed to a maximum distance of 300m (1000ft) from the module when using 22 AWG wire.

- Magnetic contacts shall be listed to UL 634 to comply with UL installation standards and ULC/ORD-C634 to comply with cUL installation standards.
- Motion detectors and temperature sensors shall be listed to UL 639 to comply with UL installation standards and ULC-S306 to comply with cUL installation standards.
- The controller has been evaluated for UL 294, UL 1076, UL 1610, UL 1635, CAN/ULC-S304, CAN/ULC-S319 and CAN/ULC-S559.

Inputs can be programmed using the Protege software. Inputs CP001:01 to CP001:08 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

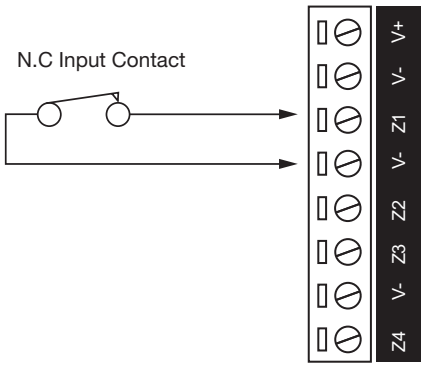


Inputs 1-4 and 5-8 can operate as either general purpose inputs or as onboard reader inputs. If used as general purpose inputs you must ensure that they are not defined in the onboard reader set up.

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 the EOL resistor configuration, the EOL resistor option must be configured based on the site requirements. Note 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
2k2	2k2	Open, Closed, Tamper, Short
4k7	2k2	Open, Closed, Tamper, Short
4k7	4k7	Open, Closed, Tamper, Short
5k6	5k6	Open, Closed, Tamper, Short
N/O alarm	5k6	Open, Closed, Tamper

The 5k6 Value 1 and Value 2 have not been evaluated by UL, cUL.

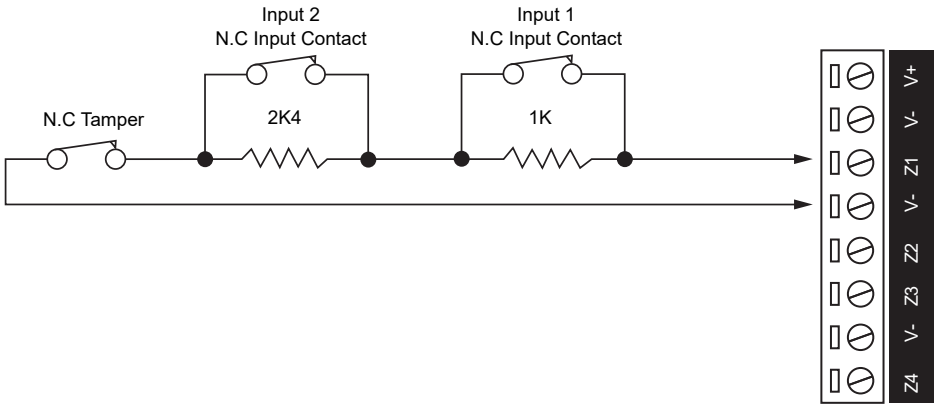
Duplex Inputs

The controller is able to support up to 16 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 9-16 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
5	Z3	1K
6	Z3	2K4
7	Z4	1K
8	Z4	2K4
9	Z5	1K
10	Z5	2K4
11	Z6	1K
12	Z6	2K4
13	Z7	1K
14	Z7	2K4
15	Z8	1K
16	Z8	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

Each controller can monitor up to 64 local 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 groups that they are associated with.

Input Number	Description	Default Trouble Group	Default Trouble Group Option
CP001:01	Reserved	-	-
CP001:02	12V Supply Failure	General	AC Failure
CP001:03	Reserved	-	-
CP001:04	Real Time Clock Not Set	General	RTC/Clock Loss
CP001:05	Service Report Test	-	-
CP001:06	Service Report Failure to Communicate	General	Reporting Failure
CP001:07	Phone Line Fault (modem model only)	General	Phone Line Lost
CP001:08	Auxiliary Failure	General	Power Fault
CP001:09	Bell Cut/Tamper	General	Bell/Output Fault
CP001:10	Reserved	-	-
CP001:11	Bell Current Overload	General	Bell/Output Fault
CP001:12	Reserved	-	-
CP001:13	Module Communication	System	Module Loss
CP001:14	Module Network Security	System	Module Security
CP001:15	Reserved	-	-
CP001:16	Reserved	-	-
CP001:17	Reserved	-	-
CP001:18	Reserved	-	-
CP001:19	Reserved	-	-
CP001:20	Report IP Reporting Failure	System	Hardware Fault
CP001:21	Reserved	-	-
CP001:22	Modbus Communication Fault	System	Hardware Fault
CP001:23	Protege System Remote Access	System	Hardware Fault
CP001:24	Installer Logged In	System	Hardware Fault
CP001:25	Reserved	-	-
CP001:26	Reserved	-	-
CP001:27	Reserved	-	-
CP001:28	Reserved	-	-
CP001:29	System restarted	System	Hardware Fault
CP001:30	Reserved	-	-
CP001:31	Reserved	-	-
CP001:32	3G Modem Link Lost (legacy 3G modem model only)	System	Hardware Fault
CP001:33	Controller Group Link Lost	System	Hardware Fault

Input Number	Description	Default Trouble Group	Default Trouble Group Option
| | | |	| |	|	|
CP001:64	Reserved	-	-

CP001:33 Controller Group Link Lost is not evaluated by UL, cUL.

Outputs

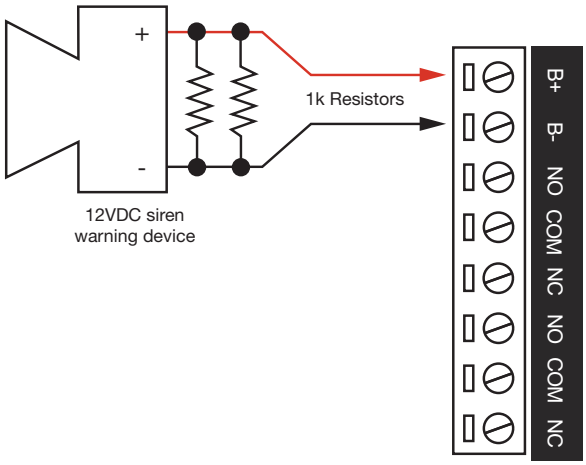
The controller has 7 onboard outputs. These outputs are used to activate bell sirens, lighting circuits, door locks, relay accessory products and other automation points. The first output on the controller has a special hardware design that allows it to monitor for fault conditions and is ideally suited to driving sirens or warning devices.

Bell/Siren Output

Not investigated by UL/cUL for local burglary applications.

The + and - terminals of the bell output (CP001:01) are used to power bells, sirens or any devices that require a steady voltage output. The bell output supplies 12VDC upon alarm and supports one 30-watt siren. The bell output uses an electronically fused circuit and automatically shuts down under fault conditions.

Connecting a Piezo siren may result in a dull noise being emitted. This is caused by residual current from the monitoring circuit. To prevent this occurring, connect two 1K resistors in parallel.

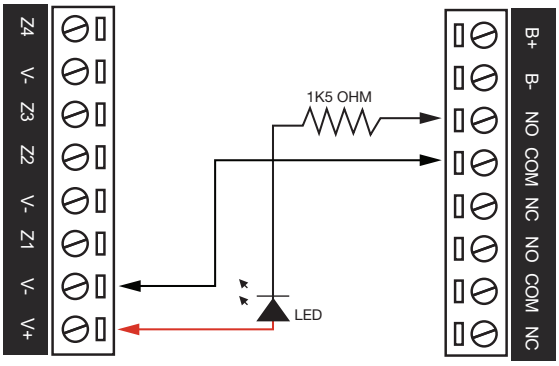


If the load on the bell terminals returns to normal, the controller reinstates power to the bell terminals on the next transition of the output.

When the bell output is not used, the appropriate trouble input will be activated. This can be avoided by connecting a 1K resistor (provided in the accessory bag) across the bell output. If the bell is not being used for another function, and the trouble input is not programmed in the system, a resistor is not required.

Relay Outputs

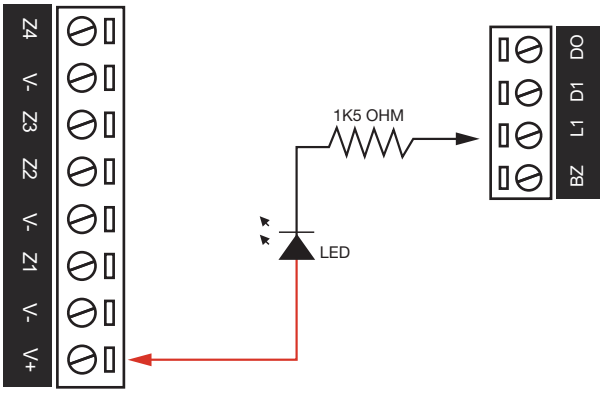
The relay outputs (CP001:03 and CP001:04) on the controller are Form C relays with normally open and normally closed contacts. These outputs can be used to activate larger relays, sounders and lights, etc.



Warning: Relay outputs can switch to a maximum capacity of 7A. Exceeding 7A will damage the output.

Reader Outputs

If readers are not attached to the reader ports then the Reader 1 L1 and BZ, and the Reader 2 L1 and BZ outputs can be used as general purpose outputs. These can be controlled by assigning the RDxxxGreen R1, RDxxx Beeper R1, RDxxxGreen R2 and RDxxx Beeper R2 outputs of whichever reader module has been configured as the onboard reader module. These are open drain outputs which switch to the V- reference.



Warning: The reader outputs can switch to a maximum capacity of 50mA. 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.

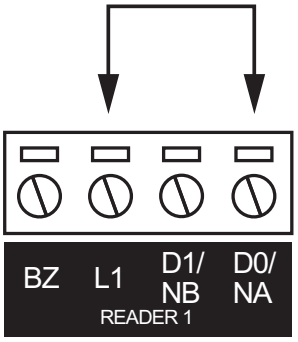
Once the settings have been changed you must save the settings by pressing the **[Arm]** key. You will be prompted to confirm the changes by pressing **[Enter]**. You must then restart the controller, either through the menu **[4], [2], [2]** or by cycling the power, for the settings to take effect.

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 will also temporarily disable HTTPS security, which may help resolve some connection issues.

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 **Reader 1** D0 input and **Reader 1** L1 output.



4. Power up the controller. Wait for the status indicator to begin flashing steadily.

Accessing the Controller

5. 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
   - **Use HTTPS**: Disabled
6. Connect to the controller by entering http://192.168.111.222 into the address bar of your web browser, and view or change the IP address and other network settings as required.

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

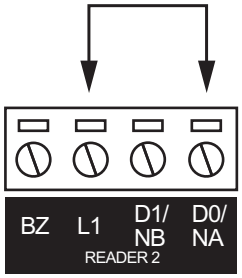
7. Remove the wire link(s) and power cycle the controller again.
   The controller will now use the configured network settings.

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

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 the **Reader 2** D0 input and the **Reader 2** L1 output.



4. Power up the controller. Wait for the status indicator to begin flashing steadily.
5. Remove the wire link **before making any changes to the controller's configuration**.

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 encryption keys used for secure sessions and pairing are deleted. This includes:
  - OSDP secure channel encryption keys for the controller **and** connected reader expanders
  - Protege wireless lock encryption keys
  - Pairing with Protege GX extended services
  - Pairing with Protege X
- All operator records are removed and the admin operator must be recreated.
- All other programming is removed.

After Defaulting a Controller

Before making any changes to the controller's configuration or upgrading the firmware, **remove the wire link used to default the 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. If you were using OSDP secure channel, put **all** OSDP card readers connected to the controller **and** its reader expanders into installation mode. Initiate installation mode on the controller and all connected reader expanders to re-establish the secure channel.

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

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

Modem Indicator

Modem model only.

The Modem indicator shows the status of the onboard modem.

State	Description
On (green)	Modem has control of telephone line
Off	Modem is not active

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

Bell Indicator

The Bell indicator shows the status of the bell output and the over current or circuit fault conditions.

State	Description
Off	Bell is connected, output is OFF
On (green)	Bell is ON
Single flash (green)	Bell is ON, the circuit is in over current protection
Two flashes (green)	Bell is OFF, the circuit to the siren/bell is cut, damaged or tampered

Relay Indicators

The relay indicators show the status of the lock output relays.

State	Description
Constantly on (red)	Relay output is ON
Constantly off	Relay output is OFF

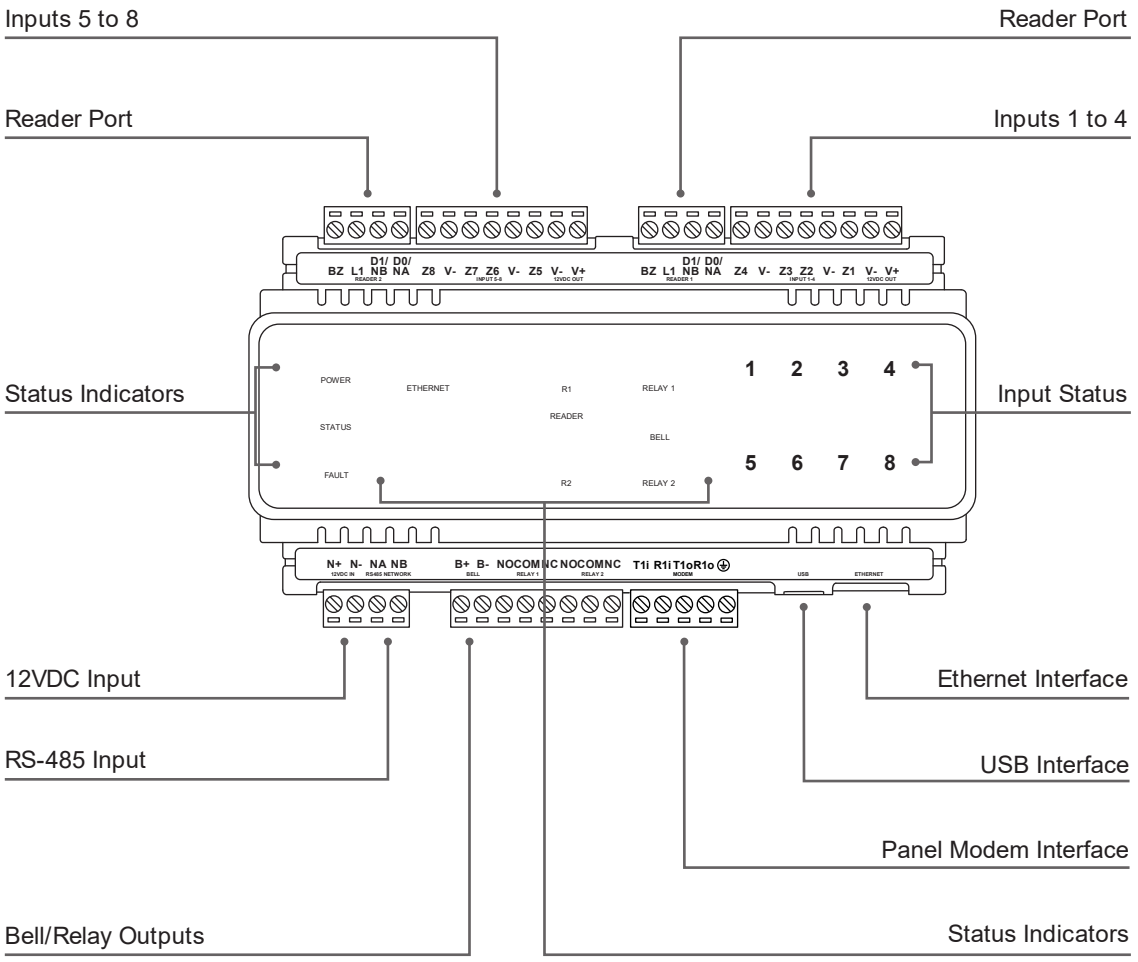
Input Indicators

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

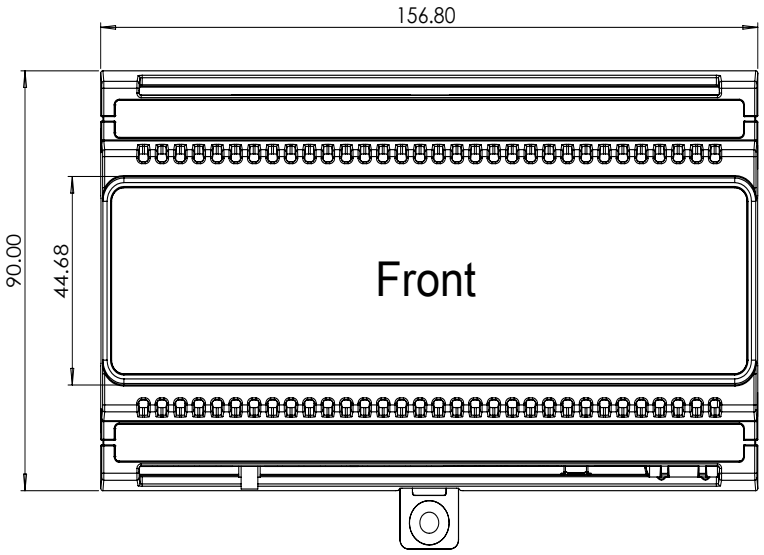
Mechanical Diagram

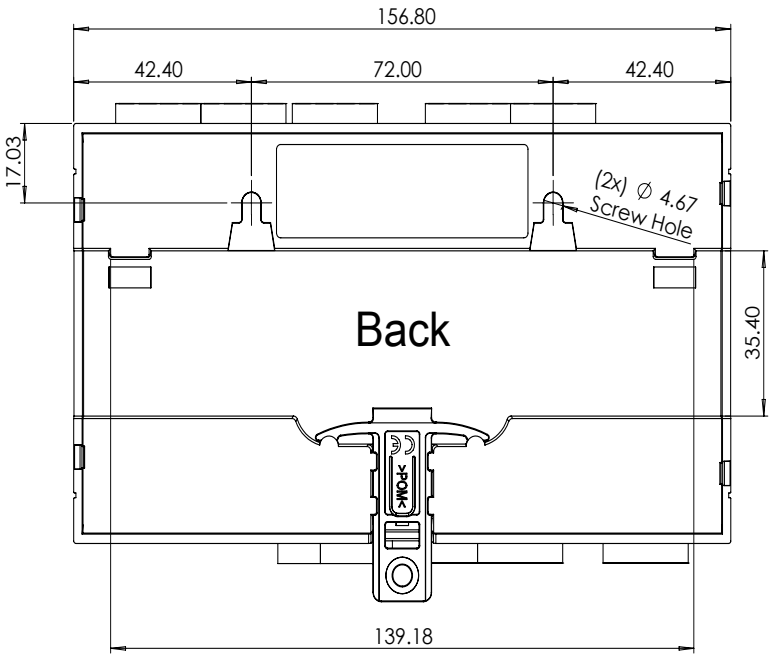
The mechanical diagram shown below outlines the essential details needed to help ensure the correct installation of the controller.



Mechanical Layout

The mechanical layout 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	
PRT-CTRL-DIN	Protege GX DIN Rail Integrated System Controller
Power Supply	
Operating Voltage	11-14V DC
Operating Current	120mA (Typical)
DC Output (Auxiliary)	10.45-13.85V DC 0.7A (Typical) Electronic shutdown at 1.1A
Bell DC Output (Continuous)	10.4-13.45V DC 8 ohm 30W Siren or 1.1A (Typical) Electronic shutdown at 1.6A
Bell DC Output (Inrush)	1500mA
Total Combined Current*	3.4A (max)
Electronic Disconnection	9.0V DC
Communication	
Ethernet	10/100Mbps ethernet communication link
RS-485	3 RS-485 communication interface ports - 1 for module communication, 2 for reader communication
USB	Type-A
Modem	2400bps modem communication
Readers	
Readers	2 reader ports, independently configurable for either Wiegand (up to 1024 bits configurable) or RS-485, allowing connection of up to 4 readers providing entry/exit control for two doors **
	RS-485 reader port connections support configuration for OSDP protocol
Inputs	
Inputs (System Inputs)	8 high security monitored inputs
Outputs	
Outputs	4 (50mA max) open collector outputs for reader LED and beeper or general functions
Relay Outputs	2 Form C relays - 7A N.O/N.C. at 30V AC/DC resistive/inductive
Dimensions	
Dimensions (L x W x H)	157 x 90 x 60mm (6.2 x 3.5 x 2.4")
Net Weight	360g (12.7oz)
Gross Weight	440g (15.5oz)
Operating Conditions	
Operating Temperature	UL/cUL 0° to 49°C (32° to 120°F) : EU EN -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 RDF 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 Bell output is connected in the same way.

** Each reader port supports either Wiegand or RS-485 reader operation, but not both at the same time. If combining reader technologies, they must be connected on separate ports.

The size of the conductor used for power supply should be adequate to prevent voltage drop of 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.

Current and Validation Example

The example shown below refers to the specifications needed to help ensure the correct installation of a Protege controller. Specifications should be validated to ensure that individual maximum currents and total combined current are not exceeded.

Example

External Devices Connected to Panel
4 EDGE PIR Motion Detectors (Inputs 1-4) connected on AUX1 Output
4 EDGE PIR Motion Detectors (Inputs 5-8) connected on AUX2 Output
1 30W Siren (1.1A (1100mA) @ 13.8VDC)

Current Consumption	
Total Combined Current before shutdown	3.4A (3400mA)
Operating Current	120mA (Typical)
DC Output (AUX1)	4 EDGE PIR Motion Detectors @ 15mA each (Total 60mA)
DC Output (AUX2)	4 EDGE PIR Motion Detectors @ 15mA each (Total 60mA)
Siren on Bell Output	1.1A (1100mA)
Total Consumption	1.34A (1340mA)

Validation		
Is the total DC Output (AUX1) current less or equal to 1.1A (1100mA)?	Yes, it is 60mA	✓
Is the total DC Output (AUX2) current less or equal to 1.1A (1100mA)?	Yes, it is 60mA	✓
Is the Bell current output less or equal to 1.1A (1100mA)?	Yes, it is 1.1A (1100mA)	✓
Is the total combined current less or equal to 3.4A (3400mA)?	Yes, it is 1.34A (1340mA)	✓

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.

ASIAL Class 5

This product is certified for AS/NZS 2201:2007 Class 5 installations as part of a compliant Protege GX or Protege WX system.

For more information, see the Protege GX / Protege WX AS/NZS 2201.1:2007 Class 5 Compliance Installer Guide, available from ICT.

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.

Task	Frequency	Description
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.
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 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.

UL and cUL Installation Requirements

Only UL / cUL listed compatible products are intended to be connected to a UL / cUL listed control system.

For installations where a secondary method of reporting is required, use the onboard 2400bps modem included with the modem controller model, or incorporate the PRT-4G-USB cellular modem module into the installation with the non-modem controller model.

UL/cUL Product Firmware Versions

UL/cUL has validated this controller with the following firmware versions:

- 2.08.XXXX
- 3.10.XXXX

To view the firmware version of your controller:

1. Connect to the controller using an ethernet segment or over the network.
2. Log in to the controller's web interface.
3. Navigate to **Application Software**. The **Current Version** displays the firmware version.

UL/cUL Enclosures

All UL/cUL installations must use an enclosure (cabinet) that is listed to the relevant UL or cUL standard.

ICT offers a range of UL- and cUL-listed enclosures that are suitable for installation of Protege DIN rail products and accessories such as batteries. For our enclosure listings, see one of the following locations:

- The UL/cUL-Listed Protege Enclosures reference document, available from the ICT website.
- UL Product iQ

Central Station Signal Receiver Compatibility List

- IP Receiver via Ethernet Port: ArmorIP Internet Monitoring Receiver. Internet monitoring software and interconnected with a (DAXW/C) central station automation system software and compatible receiving equipment.
- CID Receiver via Onboard Modem: Any UL and cUL listed receiver that uses the Contact ID protocol.

  Modem model only.

UL Operation Mode

UL operation mode should be enabled in Protege GX system settings. Select **Sites | Controllers | Options** and then select **Advance UL Operation** for the Protege GX system to operate in UL compliance mode.

This setting has the following effects:

- Adds a 10 second grace period following a failed poll before a module is reported as offline.

  Each module sends a poll message to the controller every 250 seconds. The module will be reported as offline if no poll has been received for the duration of this poll time plus the 10 second grace period.
- Suppresses reporting of all alarms and/or reportable events to a monitoring station within the first two minutes of the controller powering up. The system will continue to send poll messages as usual.

- Reports 'Input Tamper' events as 'Input Open' events when the area that the input is assigned to is armed. If the area is disarmed an 'Input Tamper' message will be sent.
- Limits the **Dial attempts** for reporting services to a maximum of 8.

This setting must be used in conjunction with the other configuration requirements as noted in this section.

cUL Compliance Requirements

CAN/ULC-60839-11-1

- The Protege controller and reader expander module are intended to be mounted within the enclosure (refer to UL/cUL Installation Cabinet Options), installed inside the protected premise, and are CAN/ULC-60839-11-1 Listed for Class I applications only.
- Exit devices and wiring must be installed within the protected area.
- For the Protege controller and reader expander module, all RS-485 and reader terminal connections must be made using shielded grounded cable.
- All readers must be connected with shielded, grounded cable.
- A bell or visual indicator used as an arming acknowledgment signal must be listed to a cUL security, signaling or fire standard. If intended to be mounted outside, it must be rated for outdoor use.
- Fail secure locking mechanisms shall only be installed where allowed by the local authority having jurisdiction (AHJ) and shall not impair the operation of panic hardware and emergency egress.
- If fire resistance is required for door assembly, portal locking device(s) must be evaluated to ULC-S533 and CAN/ULC-S104.
- Must be installed with CAN/ULC-60839-11-1 listed portal locking device(s) for cUL installations.
- If a flexible cord is used to connect to line voltage, strain relief must be provided for the cord inside the enclosure or at the knockout.
- The power supply is not intended to be mounted on the exterior of vault, safe, or stockroom.

CAN/ULC-S304

- **Auto Arming**

  Control units that support auto arming shall provide an audible signal throughout the protected area not less than 10 min prior to the auto arming taking place. The control unit shall allow authorized users to cancel the auto arming sequence and transmit such cancelation to the signal receiving center with the identification of the authorized user that canceled the action.

  The following options must be enabled in the Protege system when using the Auto Arming feature. When the defer warning time is programmed to 10 minutes, the output group will be activated 10 minutes before the system performs the Auto Arming in the associated Area.

  - The **Defer Output or Output Group** must be programmed. Refer to the section Areas | Outputs in the Operator Reference Manual for programming instructions.
  - The **Defer Warning Time** must be programmed to not less than 10 minutes. Refer to the section Areas | Configuration in the Operator Reference Manual.
  - The **Defer Automatic Arming** option must be enabled. Refer to the section Areas | Options (2) in the Operator Reference Manual.
- **Arming Signal**

  A bell or visual indicator used as an arming acknowledgment signal must be listed to a cUL security, signaling or fire standard. If intended to be mounted outside, it must be rated for outdoor use.
- **Double EOL Input Configuration**

  Only double EOL Input Configuration shall be used. Refer to the Inputs section of this manual and the section Inputs | Options in the Operator Reference Manual.
- **Multiplex System and Poll Time**

The Protege controller is compatible with the ArmorIP Internet Monitoring Receiver. Poll Time must be set to 40 seconds and the Grace Time must be set to 20 seconds.

In the Protege system, the reporting service must be configured to 40 seconds. The following options are required for the service selected as Report IP type:

- The **Log Polling Message** option must be enabled. Refer to the section Report IP | Options in the Operator Reference Manual.
- The **Poll Time** must be programmed to 40 seconds. Refer to the Report IP | General section in the Operator Reference Manual.

- **Central Station Signal Receiver**

  The common equipment of each signal receiving center control unit shall be limited to 1000 alarm systems.

- **Number of attempts**

  In the event of unsuccessful communication, a digital alarm communicator transmitter shall make a minimum of 5 and a maximum of 10 attempts. Where the maximum number of attempts to complete the sequence is reached, an indication of the failure shall be made at the premises.

  In the Protege system, the reporting service selected as Contact ID must have the number of attempts programmed to 5 attempts. The **Dial Attempts** option must be programmed. Refer to the section Contact ID | Settings in the Operator Reference Manual.

  If the PRT-4G-USB cellular modem is being used as the secondary reporting option in the installation, the Report IP service assigned to the cellular modem must be programmed as above.

- **Check-In Time**

  DACT communication channel check-in time is not to exceed 24 hrs.

- **Trouble Input Service Test Report**
  - The **Test Report Time** must be programmed. Refer to the section Controllers | Configuration in the Operator Reference Manual.
  - The **Generate Input Restore on Test Input** option must be enabled. Refer to the section Controller | Options in the Operator Reference Manual.
  - The **Test Report Time is Periodic** option must be enabled. Refer to the section Controller | Options in the Operator Reference Manual.

- **Primary Communication Channel**

  The first attempt to send a status change signal shall utilize the primary communication channel.

  An ethernet Report IP service must be used as the primary service. The backup service may use Contact ID over the phone line or Report IP over the cellular network if the PRT-4G-USB cellular modem is being used as the secondary communication channel.

  The following options are required:
  - The primary service (Report IP) must have the **Backup service** set to the secondary reporting service (Contact ID or Report IP over 4G modem). The **Service mode** must be set to 1 - Start with controller OS.
  - The backup service must have **Service operates as backup** enabled. For ULC-S304 P3 applications, **Enable offline polling** must be enabled and configured so that the backup service is monitored even when it is not active.
  - For Report IP services, the **Reporting protocol** must be set to Armor IP.
  - Refer to the Services section in the Operator Reference Manual.

- **Status Change Signal**

  An attempt to send a status change signal shall utilize both primary and secondary communication channels.

- **Local Annunciation if Signal Reporting Failure**

  Failure of the primary communication channel or secondary communication channel shall result in a trouble signal being transmitted to the signal receiving center within 240 seconds of the detection of the fault. Failure of either communication channel shall be annunciated locally within 180 seconds of the fault.

  The following options must be enabled in the Protege system:

- The **Ethernet Link Failure** trouble input must be programmed.
- The **Trouble Input Area** must be armed. Refer to the section Trouble Inputs | Areas and Input Types in the Operator Reference Manual.

- **Network and Domain Access**

  Neither the subscriber control unit nor the signal receiving center receiver shall be susceptible to security breaches in general-purpose operating systems.

  Network access policies should be set to restrict unauthorized network access and "spoofing" or "denial of service" attacks.

- **Ethernet Connections**

  All ethernet network connections shall be installed within the same room as the equipment.

- **Encryption**

  For active communications channel security, encryption shall be enabled at all times.

  The ArmorIP-E (UDP or TCP) protocol must be used and the Encryption Type must be set to AES-256.

  The following options must be enabled for the Report IP service in the Protege system.

  - The **Reporting Protocol** must be set to ArmorIP (UDP) Encrypted or ArmorIP (TCP) Encrypted. The AES key must be set as specified by monitoring station.
  - Refer to the section Report IP | General in the Operator Reference Manual.

- **Server Configuration**

  Where a server is employed for control over network addressing, encryption or re-transmission, such shall be designed to remain in the "on state" at all times.

  Communicators are not suitable for active communication channel security and medium or high risk applications unless such can be "online" at all times, have a minimum 128 bit encryption scheme, have encryption enabled, network and domain security implemented.

  Network access policies shall be set to restrict unauthorized network access and "spoofing" or "denial of service" attacks.

- **Internet Service Provider (ISP)**

  The Internet Service Provider (ISP) providing service shall meet the following requirements:

  - redundant servers/systems
  - back-up power
  - routers with firewalls enabled and
  - methods to identify and protect against "Denial of Service" attacks (i.e. via "spoofing")

- **Information Technology Equipment, Products or Components of Products**

  Products or components of products, which perform communications functions only, shall comply with the requirements applicable to communications equipment as specified in CAN/CSA-C22.2 No. 62368-1, Audio/video, information and communication technology equipment - Part 1: Safety requirements. Where network interfaces, such as the following, are internal to the subscriber control unit or receiver, compliance to CAN/CSA-C22.2 No. 62368-1 is adequate. Such components include, but are not limited to:

  - A) Hubs;
  - B) Routers;
  - C) Network interface devices;
  - D) Third-party communications service providers;
  - E) Digital subscriber line (DSL) modems; and
  - F) Cable modems.

- **Backup Power Requirements**

  Power for network equipment such as hubs, switchers, routers, servers, modems, etc., shall be backed up or powered by an uninterruptible power supply (UPS), stand-by battery or the control unit, capable of facilitating 24h standby, compliant with Clauses 16.1.2 and 16.4.1 of CAN/ULC-S304.

  For communications equipment employed at the protected premises or signal receiving center and intended to facilitate packet switched communications, as defined in CAN/ULC-S304, 24h back-up power is required.

- **Compromise Attempt Events**

ArmorIP detects the reception of any invalid packet on the programmed port as a potential system **compromise attempt**. Each compromise attempt sends a notification to the receiver, and logs a Compromise Attempt event under the Live Panel Events.

The event is sent with the following details:

- **Account Code** as defined in the Serial Receiver settings
- **Event Code** 0x163
- **Group Code** as defined in the Serial Receiver settings
- **Point Code** as defined in the Serial Receiver settings

Refer to the section Global Settings | Serial Receiver in the ArmorIP Version 3 Internet Monitoring Application User Manual.

For UL and cUL installations the Central Station Receiving software must have the Contact ID details as specified, programmed for the **Compromise Attempt** event.

- **Power Supply Mains Power Connection**

  If a flexible cord is used to connect to line voltage, strain relief must be provided for the cord inside the enclosure or at the knockout.

  The power supply is not intended to be mounted on the exterior of vault, safe, or stockroom.

CAN/ULC-S319

- The Protege controller and reader expander module are intended to be mounted within the enclosure (refer to UL/cUL Installation Cabinet Options), installed inside the protected premise, and are CAN/ULC-S319 Listed for Class I applications only.
- Exit devices and wiring must be installed within the protected area.
- For the Protege controller and reader expander module, all RS-485 and reader terminal connections must be made using shielded grounded cable.
- All readers must be connected with shielded, grounded cable.
- A bell or visual indicator used as an arming acknowledgment signal must be listed to a cUL security, signaling or fire standard. If intended to be mounted outside, it must be rated for outdoor use.
- Fail secure locking mechanisms shall only be installed where allowed by the local authority having jurisdiction (AHJ) and shall not impair the operation of panic hardware and emergency egress.
- If fire resistance is required for door assembly, portal locking device(s) must be evaluated to ULC-S533 and CAN/ULC-S104.
- Must be installed with CAN/ULC-S319 listed portal locking device(s) for cUL installations.
- If a flexible cord is used to connect to line voltage, strain relief must be provided for the cord inside the enclosure or at the knockout.
- The power supply is not intended to be mounted on the exterior of vault, safe, or stockroom.

CAN/ULC-S559

Signal Reporting

The reporting services and other components shall be programmed so as to meet the requirements of CAN/ULC-S559 for either an active or passive communication system.

This includes the following provisions:

- All signals must be transmitted to the fire signal receiving center within 60 seconds.
- An active communication system shall use one or more IP reporting services. Any fault in the primary reporting service must be detected and annunciated at the fire signal receiving center within 180 seconds.
- IP reporting services may utilize either the controller's onboard ethernet or the PRT-4G-USB cellular modem. The **Reporting Protocol** must be set to ArmorIP with at least 128 bit encryption. Either UDP or TCP may be used.

- A passive communication system shall use two or more communication channels. The primary channel is a Contact ID service over the phone line, with a test signal sent at least every 6 hours. The phone dialer must make a minimum of 5 and a maximum of 10 attempts to dial the receiving center in the event of a communication failure.
- In passive systems, a DAYR7-listed cellular alarm communicator (e.g. DSC LE4010) must provide the backup channel and phone line integrity monitoring. The alarm communicator must be installed and configured in accordance with the manufacturer's instructions for CAN/ULC-S559 (commercial fire reporting) installations.

Further details and programming instructions are provided in Application Note 362: CAN/ULC-S559 Fire Reporting in Protege Systems.

Central Station Signal Receiver

The signal receiving software must be ICT ArmorIP Version 3. It must meet the following requirements:

- The **Poll Time** must be set to 40 seconds and the **Poll Grace Time** must be set to 20 seconds.
- The maximum number of signal transmitting units connected to the ArmorIP Receiver shall not exceed 10000 simultaneous connections.
- The system shall be redundant. For up to 1000 accounts, two computers must be used. Each subsequent set of 1000 accounts requires another two computers.

For instructions and hardware requirements, see the ArmorIP Version 3 Internet Monitoring Application User Manual.

Ethernet Connections

All ethernet network connections shall be installed within the same room as the equipment.

External Wiring

All wiring extending outside of the enclosure must be protected by metal conduits.

Power Supply Mains Power Connection

If a flexible cord is used to connect to line voltage, strain relief must be provided for the cord inside the enclosure or at the knockout.

The power supply is not intended to be mounted on the exterior of vault, safe, or stockroom.

Backup Power

See your power supply installation manual for backup battery power requirements for the Protege system.

Telecom equipment (switches, modems, routers) requires 24hr of standby backup power.

Arming Signal

A bell or visual indicator used as an arming acknowledgment signal must be listed to a cUL security, signaling or fire standard. If intended to be mounted outside, it must be rated for outdoor use.

Keypad Wiring

The RS-485 connection to the keypad must be wired such that the shorts and other faults on the RS-485 line connection of the keypad will not cause the controller to malfunction.

Fire Zone Inputs

Inputs 1, 2 and 3 on the controller or input expander must be connected to the Fire, Supervisory and Trouble outputs on the fire alarm control panel, as indicated in the diagrams below.

- EOL resistors must be installed at the fire alarm control panel outputs. Typical input circuits are:

Value 1	Value 2	Monitored Status
1k	1k	Open, Closed, Tamper, Short
6k8	2k2	Open, Closed, Tamper, Short
10k	10k	Open, Closed, Tamper, Short
2k2	2k2	Open, Closed, Tamper, Short
4k7	2k2	Open, Closed, Tamper, Short
4k7	4k7	Open, Closed, Tamper, Short

  See the Inputs section of the controller or expander installation manual for connection diagrams.
- These inputs must have a fire area assigned, and the area must be armed. Areas used for fire reporting must not also be used for burglary.
- These inputs must be used exclusively for fire monitoring and cannot be programmed to activate the bell output.

Further details and programming instructions are provided in Application Note 362: CAN/ULC-S559 Fire Reporting in Protege Systems.

Trouble Monitoring

The following trouble inputs must have the system area assigned with the Trouble Silent input type.

- Controller Service Report Test
- Controller ContactID Reporting Failure
- Controller ReportIP Reporting Failure
- Power Supply (Analog Expander) Mains Failure

The 24 hour portion of the system area must be armed at all times.

Provided that the Power Supply Mains Failure trouble input is monitored and reported to the receiving center, it is not necessary to display a visible LED indication outside the cabinet when there is a mains power failure.

Further details and programming instructions are provided in Application Note 362: CAN/ULC-S559 Fire Reporting in Protege Systems.

Indicating Reporting Failures

Reporting failures must be indicated on the user interface for the system. There are two methods for achieving this:

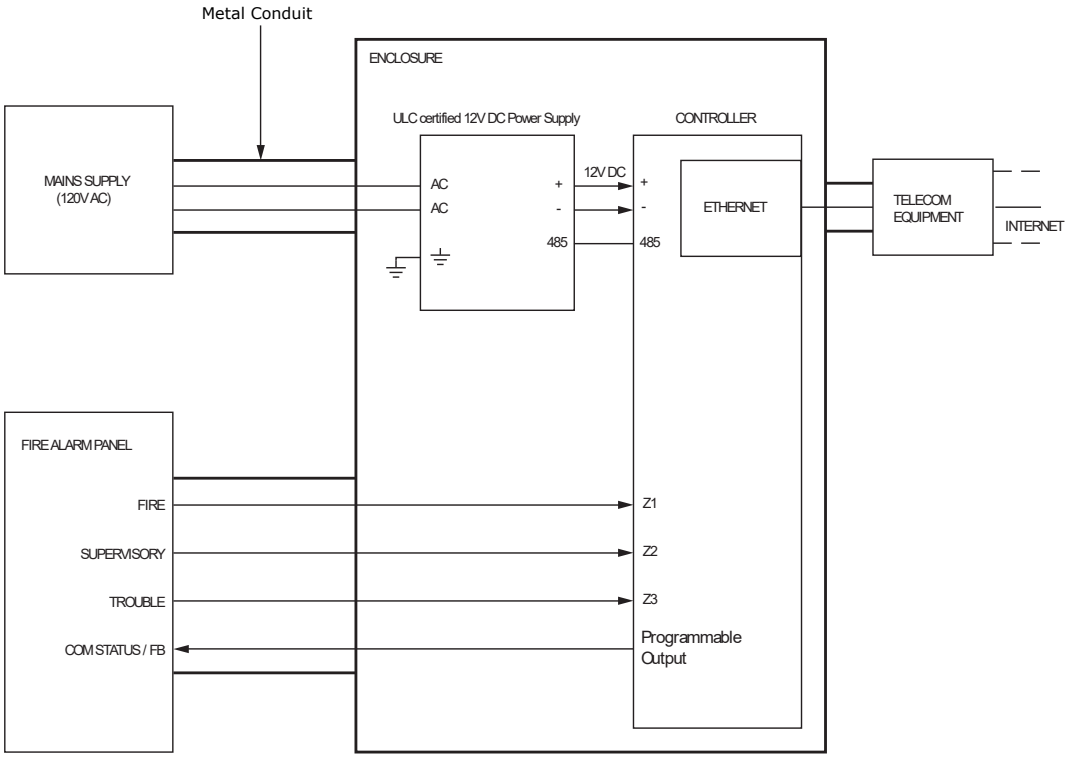
- Sites with keypads can display the trouble message on the keypad.
- If the fire alarm control panel has an COM Status input, it may be connected to any available dry relay contact on the controller or output expander. When there is a reporting failure, the relay will turn on to activate the COM Status indicator on the fire alarm control panel.

  Depending on how this relay is programmed, it may latch on when a reporting failure occurs. If so, a normally open monitoring reset button must be provided on controller input 4 to reset the relay output.

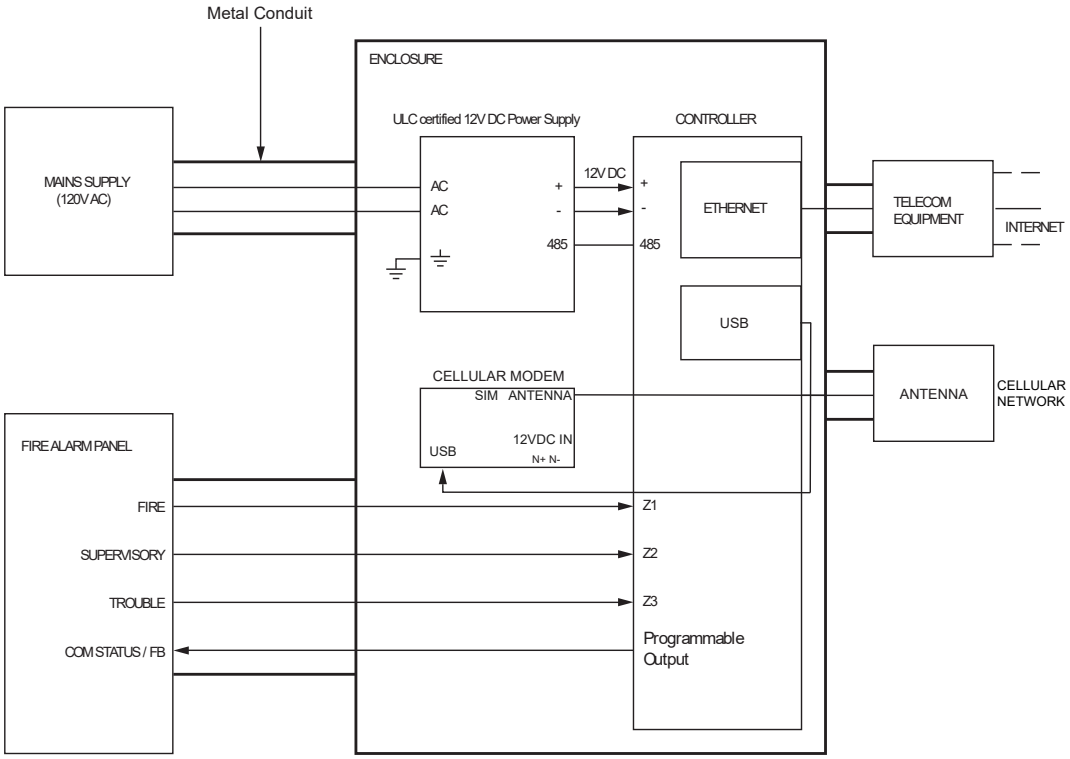
Further details and programming instructions are provided in Application Note 362: CAN/ULC-S559 Fire Reporting in Protege Systems.

Active/Passive Communication System Diagrams

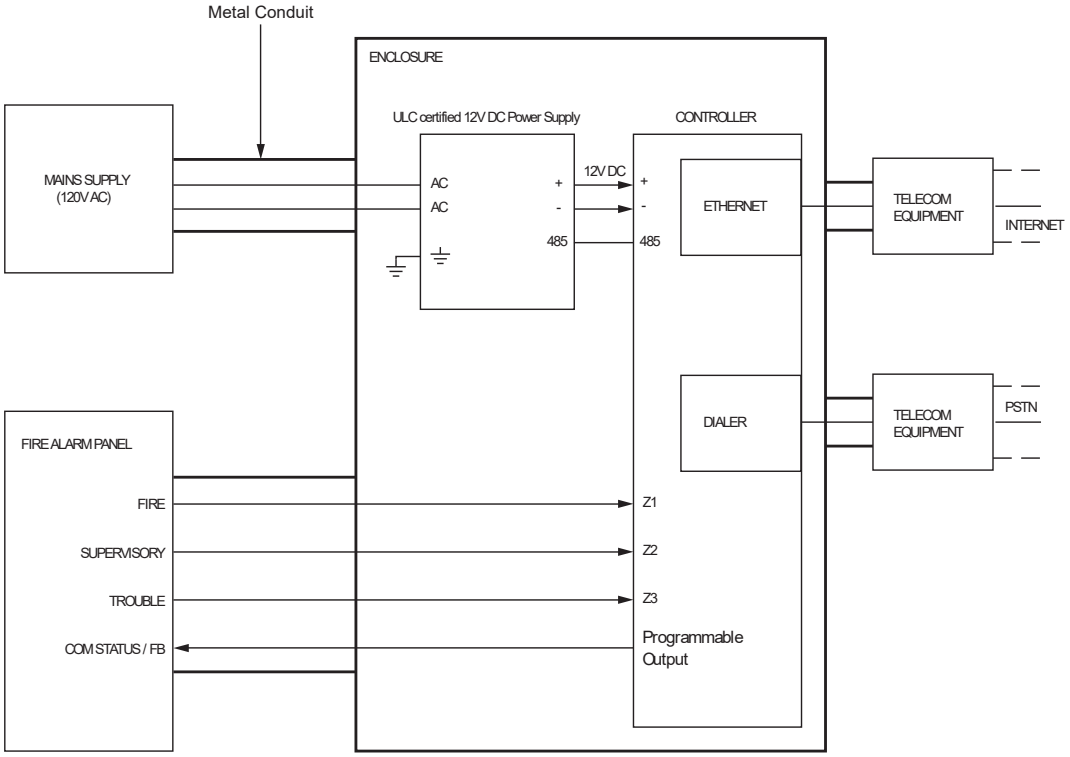
CAN/ULC-S559
CONTROLLER
ACTIVE COMMUNICATION



CAN/ULC-S559
CONTROLLER
ACTIVE COMMUNICATION: CELLULAR MODEM



CAN/ULC-S559
CONTROLLER
PASSIVE COMMUNICATION: MODEM DIALER



UL Compliance Requirements

UL1610

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.

- A local alarm sounding device, alarm housing, and control unit shall comply with the mercantile requirements in the Standard for Police Station Connected Burglar Alarm Units and Systems, UL365.
- A bell or visual indicator used as an arming acknowledgement signal must be listed to a UL security, signaling or fire standard. If intended to be mounted outside, it must be rated for outdoor use.
- Exit and entry delay must not exceed 60 seconds. To program the entry and exit delay time, refer to the section Areas | Configuration in the Operator Reference Manual.
- All ethernet network connections shall be installed within the same room as the equipment.
- Signals between the premises control unit and the receiving equipment, when not carried by wireless means, shall be protected by the following method:
  - Onboard modem telco connection must be dedicated to the Protege controller.

    Modem model only.
  - Ethernet connection to the Internet Service Provider (ISP) with a fixed IP Address must be dedicated to the Protege controller.
- To comply with the dual signal line transmission system requirement, both transmission lines (onboard modem and IP reporting) must be enabled. Signals shall be sent simultaneously to both the primary communications channel and the Backup Service.

  The Report IP and Contact ID services must be programmed and enabled within the Protege system. The following options are required:

- The **Contact ID Reporting Service** must be enabled and the **Service Mode** must be configured to start with the operating system.
- Refer to the section Contact ID in the Operator Reference Manual.
- The **Report IP Service** must be enabled as the primary communication channel, the **Service Mode** must be configured to start with the operating system, and the **Reporting Protocol** must be set to ArmorIP.
- Refer to the section Report IP in the Operator Reference Manual.

- When more than one means of signal transmission is used, loss of communication with the receiving system shall be annunciated at the receiver within 200 seconds. If a fault is detected on any of the signal transmission means, at least one of the signal transmission channels shall send a signal to the central-station to report the fault within 200 seconds.

  The Report IP and Contact ID services must be programmed and enabled within the Protege system.

  The Protege controller is compatible with the ArmorIP Internet Monitoring Receiver. Poll Time must be set to 40 seconds and the Grace Time must be set to 20 seconds.

  In the Protege system, the reporting service must be configured to 40 seconds. The following options are required for the service selected as Report IP type:
  - The **Poll Time** must be programmed to 40 seconds. Refer to the Report IP | General section in the Operator Reference Manual
  - The **Contact ID Reporting Service** must be enabled and the **Service Mode** must be configured to start with the operating system.
  - Refer to the section Contact ID in the Operator Reference Manual
  - The **Report IP Service** must be enabled as the primary communication channel, the **Service Mode** must be configured to start with the operating system, and the **Reporting Protocol** must be set to ArmorIP.
  - Refer to the section Report IP in the Operator Reference Manual.
  - The **Trouble Input Area** must be armed in 24h mode. Refer to the section Trouble Inputs | Areas and Input Types in the Operator Reference Manual.

  In the event of unsuccessful communication, a digital alarm communicator transmitter shall make a minimum of 5 and a maximum of 10 attempts. Where the maximum number of attempts to complete the sequence is reached, an indication of the failure shall be made at the premises.

  In the Protege system, the reporting service selected as Contact ID must have the number of attempts programmed to 5 attempts. The following options are required:
  - The **Dial Attempts** option must be programmed. Refer to the section Contact ID | Settings in the Operator Reference Manual.
- DACT communication channel check-in time is not to exceed 24 hrs.
- Trouble Zone Service Test Report
  - The **Test Report Time** must be programmed. Refer to the section Controllers | Configuration in the Operator Reference Manual.
  - The **Generate Input Restore on Test Input** option must be enabled. Refer to the section Controller | Options in the Operator Reference Manual.
  - The **Test Report Time is Periodic** option must be enabled. Refer to the section Controller | Options in the Operator Reference Manual.
  - ArmorIP detects the reception of any invalid packet on the programmed port as a potential system **compromise attempt**. Each compromise attempt sends a notification to the receiver, and logs a Compromise Attempt event under the Live Panel Events.

    The event is sent with the following details:
    - **Account Code** as defined in the Serial Receiver settings
    - **Event Code** 0x163
    - **Group Code** as defined in the Serial Receiver settings
    - **Point Code** as defined in the Serial Receiver settings

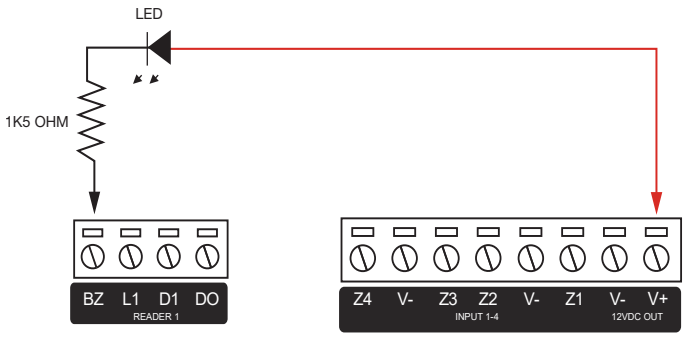
    Refer to the section Global Settings | Serial Receiver in the ArmorIP Version 3 Internet Monitoring Application User Manual.

For UL and cUL installations the Central Station Receiving software must have the Contact ID details as specified, programmed for the **Compromise Attempt** event.

- If a flexible cord is used to connect to line voltage, strain relief must be provided for the cord inside the enclosure or at the knockout.
- The power supply is not intended to be mounted on the exterior of vault, safe, or stockroom.

UL294

- The Protege controller and reader expander module are intended to be mounted within the enclosure (refer to UL/cUL Installation Cabinet Options), installed inside the protected premise, and are UL 294 Listed for Attack Class I applications only.
- Exit devices and wiring must be installed within the protected area.
- For the Protege controller and reader expander module, all RS485 and reader terminal connections must be made using shielded grounded cable.
- All readers must be connected with shielded, grounded cable.
- A bell or visual indicator used as an arming acknowledgment signal must be listed to a UL security, signaling or fire standard. If intended to be mounted outside, it must be rated for outdoor use.
- Fail secure locking mechanism shall only be installed where allowed by the local authority having jurisdiction (AHJ) and shall not impair the operation of panic hardware and emergency egress.
- If fire resistance is required for door assembly, portal locking device(s) must be evaluated to UL10B or UL10C.
- Must be installed with UL 1034 listed electronic locks for UL installations.
- AC power on shall be indicated by an external panel mount LED (Lumex SSI-LXH312GD-150) and fitted into a dedicated 4mm hole in the cabinet to provide external visibility. This shall be wired between 12V and a PGM output that is programmed to follow the AC trouble input as shown below:



- If a flexible cord is used to connect to line voltage, strain relief must be provided for the cord inside the enclosure or at the knockout.
- The power supply is not intended to be mounted on the exterior of vault, safe, or stockroom.

FCC Compliance Statements

FCC PART 15, WARNINGS: INFORMATION TO USER

This equipment complies with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

Changes or modifications not authorized by the party responsible for compliance could void the user's authority to operate this product.

This device complies with 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.

IMPORTANT INFORMATION

This equipment complies with Part 68 of the FCC Rules and the requirements adopted by the ACTA. Inside the cover of this equipment is a label that contains, among other information, a product identifier in the format US: AAAEQ##TXXXX. If requested, this number must be provided to the telephone company.

FCC REGISTRATION NUMBER:	US: 48DMM00BPRTCTRLDI
RINGER EQUIVALENCE NUMBER:	0.0
USOC Jack:	RJ-31X

Telephone Connection Requirements

A plug and jack used to connect this equipment to the premises wiring and telephone network must comply with the applicable FCC Part 68 rules and requirements adopted by the ACTA. A compliant telephone cord modular plug is provided with this product. It is designed to be connected to a compatible modular jack that is also compliant. See this document for details.

Ringer Equivalence Number (REN)

The REN is used to determine the number of devices that may be connected to a telephone line. Excessive RENs on a telephone line may result in the devices not ringing in response to an incoming call. In most but not all areas, the sum of RENs should not exceed five (5.0). To be certain of the number of devices that may be connected to a line, as determined by the total RENs, contact the local telephone company. For products approved after July 23, 2001, the REN for this product is part of the product identifier that has the format US: AAAEQ##TXXXX. The digits represented by ## are the REN without a decimal point (e.g., 03 is a REN of 0.3). For earlier products, the REN is separately shown on the label.

Incidence of Harm

If this equipment (Protege controller) causes harm to the telephone network, the telephone company will notify you in advance that temporary discontinuance of service may be required. But if advance notice isn't practical, the telephone company will notify the customer as soon as possible. Also, you will be advised of your right to file a complaint with the FCC if you believe it is necessary.

Changes in Telephone Company Equipment or Facilities

Modem model only.

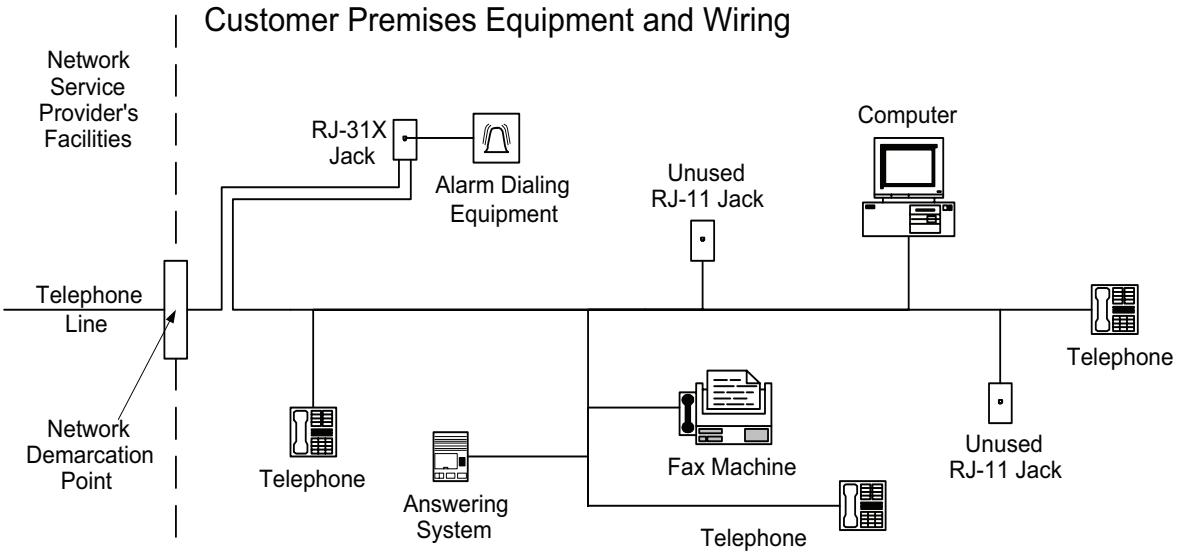
The telephone company may make changes in its facilities, equipment, operations or procedures that could affect the operation of the equipment. If this happens the telephone company will provide advance notice in order for you to make necessary modifications to maintain uninterrupted service.

Equipment Maintenance Facility

If trouble is experienced with this equipment (Protege controller), for repair or warranty information please contact Integrated Control Technology. If the equipment is causing harm to the telephone network, the telephone company may request that you disconnect the equipment until the problem is resolved. This equipment is of a type that is not intended to be repaired by the end user.

Additional Information

Connection to party line service is subject to state tariffs. Contact the state public utility commission, public service commission or corporation commission for information. Alarm dialing equipment must be able to seize the telephone line and place a call in an emergency situation. It must be able to do this even if other equipment (telephone, answering system, computer modem, etc.) already has the telephone line in use. To do so, alarm dialing equipment must be connected to a properly installed RJ-31X jack that is electrically in series with and ahead of all other equipment attached to the same telephone line. Proper installation is depicted in the figure below. If you have any questions concerning these instructions, you should consult your telephone company or a qualified installer about installing the RJ-31X jack and alarm dialing equipment for you.



Industry Canada Statement

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)

This product meets the applicable Industry Canada technical specifications. The Ringer Equivalence Number (REN) for this terminal equipment is 0.0. The Ringer Equivalence Number is an indication of the maximum number of devices allowed to be connected to a telephone interface. The termination on an interface may consist of any combination of devices subject only to the requirement that the sum of the RENs of all the devices does not exceed five.

L'indice d'équivalence de la sonnerie (IES) du présent matériel est de 0.0. Le présent materiel est conforme aux spécifications techniques applicables d'Industrie Canada. L'indice d'équivalence de la sonnerie (IES) sert à indiquer le nombre maximal de terminaux qui peuvent être raccordés à une interface téléphonique. La terminaison d'une interface peut consister en une combinaison quelconque de dispositifs, à la seule condition que la somme d'indices d'équivalence de la sonnerie de tous les dispositifs n'excède pas 5.

Controller REGISTRATION NUMBER	IC: 10012A-PRTCTRLDIN
Controller NUMÉRO D'ENREGISTREMENT	IC: 10012A-PRTCTRLDIN

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.

Designers & manufacturers of integrated electronic access control, security and automation products.
Designed & manufactured by Integrated Control Technology Ltd.