PRT-CTRL-DIN-1D

Protege GX DIN Rail Single Door Controller

Installation Manual

Last Published: 11-Jun-20 11:46 AM

Contents

Introduction

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

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

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

The current features of the Controller include:

- Internal industry-standard 10/100 Ethernet
- 32 Bit advanced RISC processor with 2Gb total memory
- 2 high security monitored inputs
- NIST Certified AES 128, 192 and 256 Bit Encryption

Single Door Controller Editions

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

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

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

Installation Requirements

This equipment is to be installed in accordance with:

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

Grounding Requirements

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

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

1. Safety
2. Component protection
3. Noise reduction

Safety Grounding

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

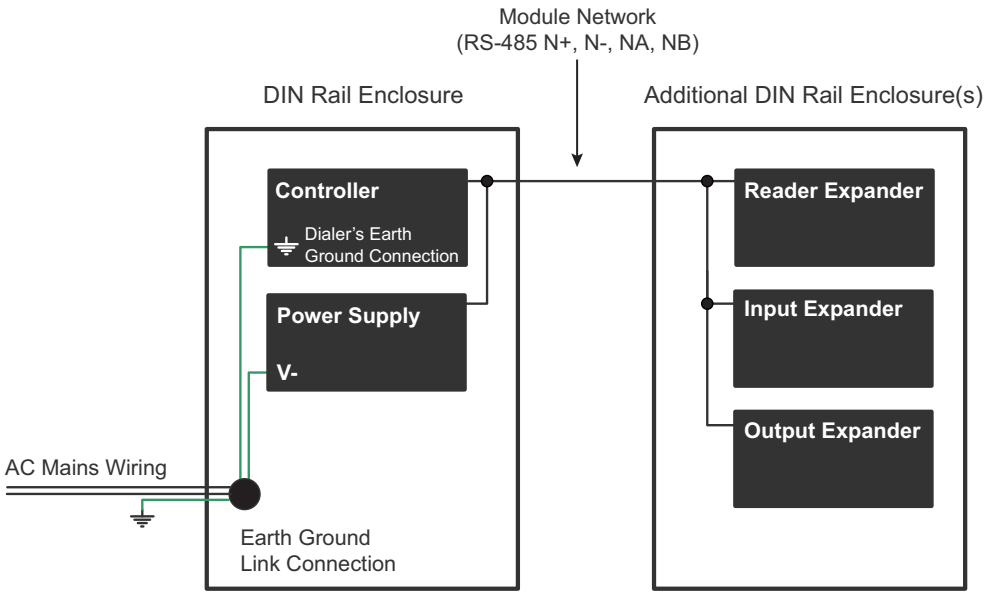
General safety dictates that all metal parts are connected to earth with separate copper wire or wires of the appropriate gauge.

Earth Ground Connection

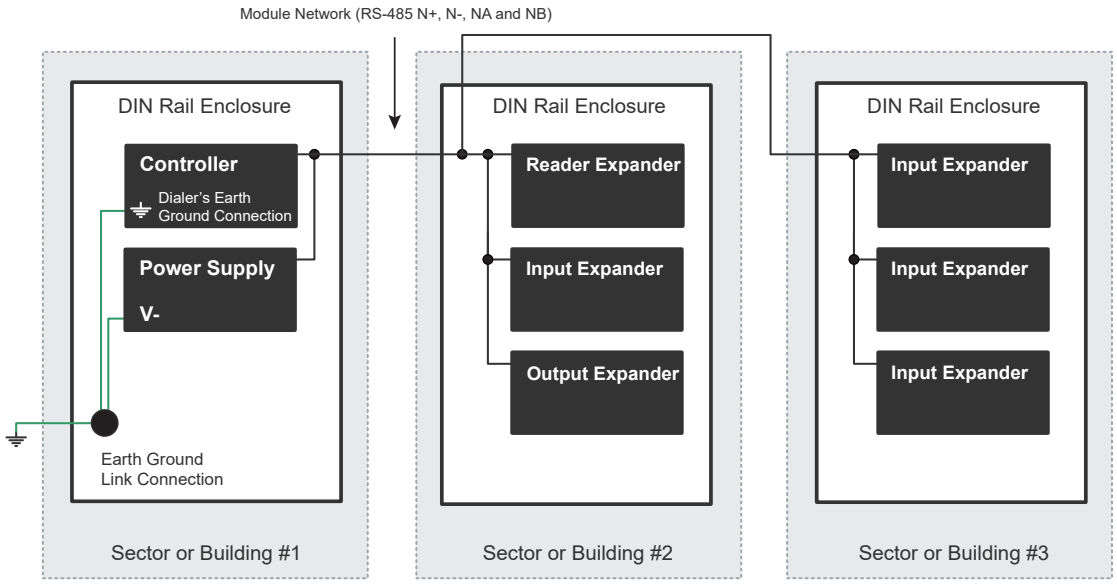
The DIN Rail enclosure and the DIN Rail modules must be grounded to a suitable single-point earth ground connection in the installation. A minimum 14AWG solid copper wire (or thicker, in accordance to local authorities) shall be used from the Protege system's earth connection points.

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)



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

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

Mounting

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

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

1. Position the DIN Rail module in the correct orientation, with the writing on the face the right way up.
2. Hook the mounting tabs (opposite the tab clip) under the edge of the DIN rail.
3. Push the DIN Rail module against the mount until the tab clips over the rail.

Removal

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

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

Connections

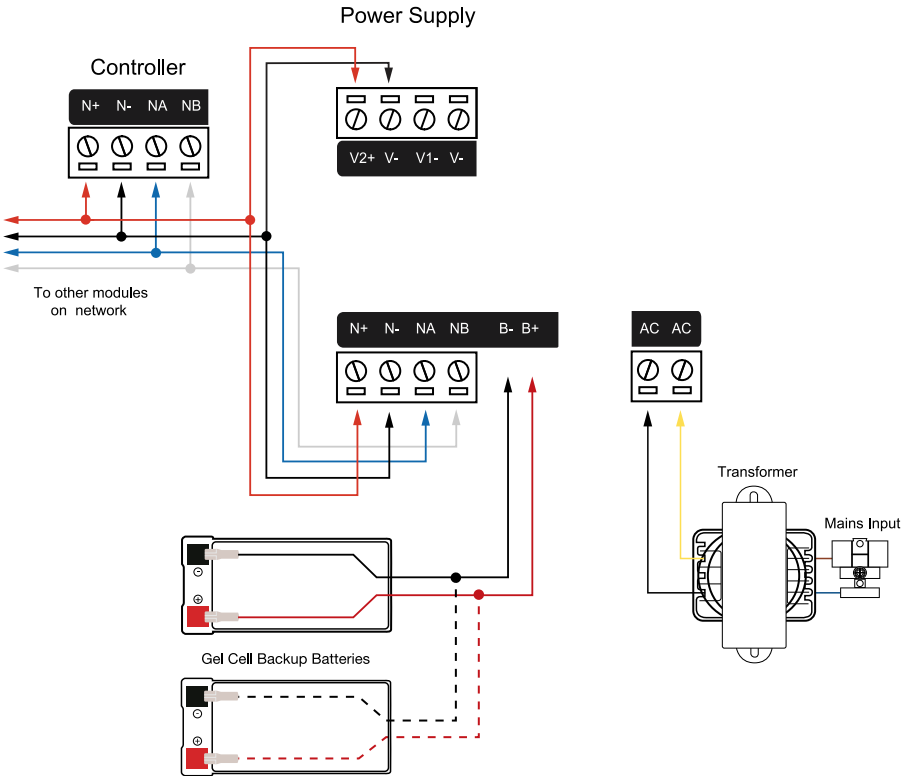
Power Requirements

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

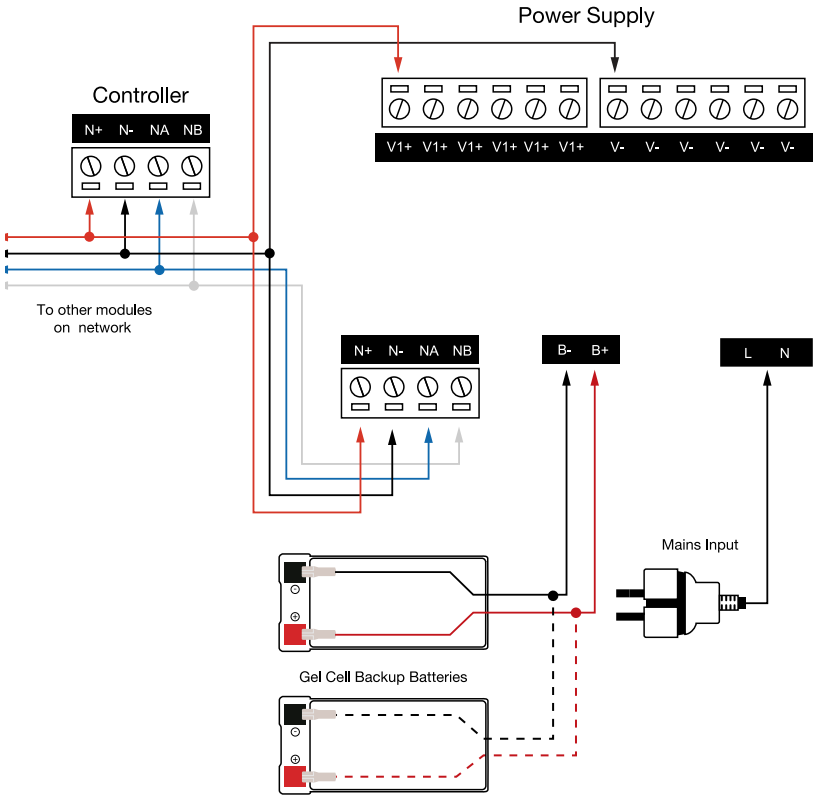
Termination of wiring to the module while power is applied or the battery is connected may cause serious damage to the unit and will VOID ALL WARRANTIES OR GUARANTEES. **Power the unit only after all wiring, configuration and jumper settings are completed.**

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

Example 2A Power Supply Connection:



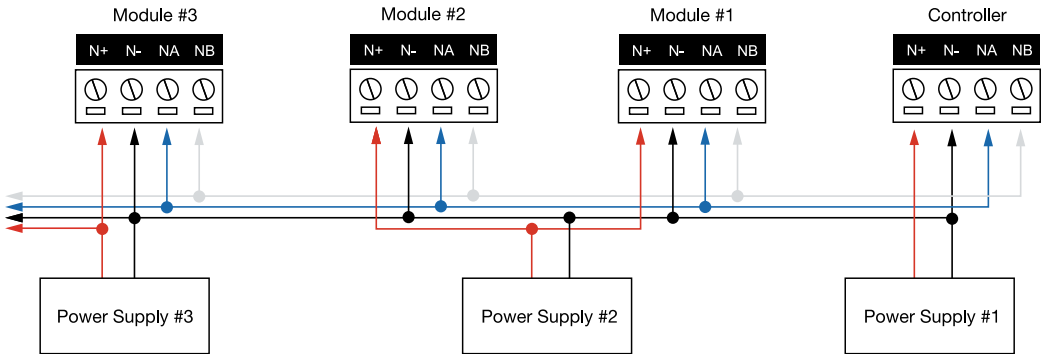
Example 4A Power Supply Connection:



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

Power over Ethernet (PoE)

PoE models only

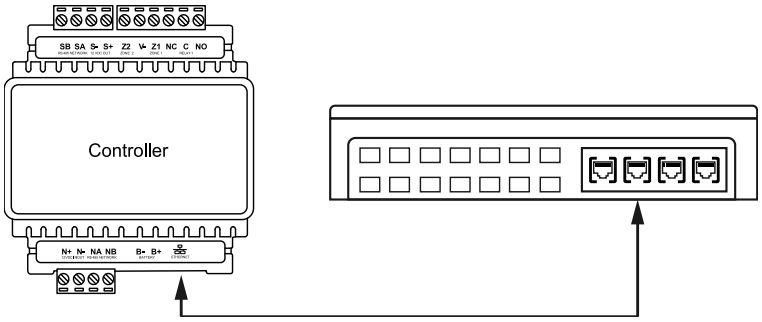
Power can be supplied to the Controller by a PoE Router connected to the Ethernet terminal.

There are two types of PoE Routers available:

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

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

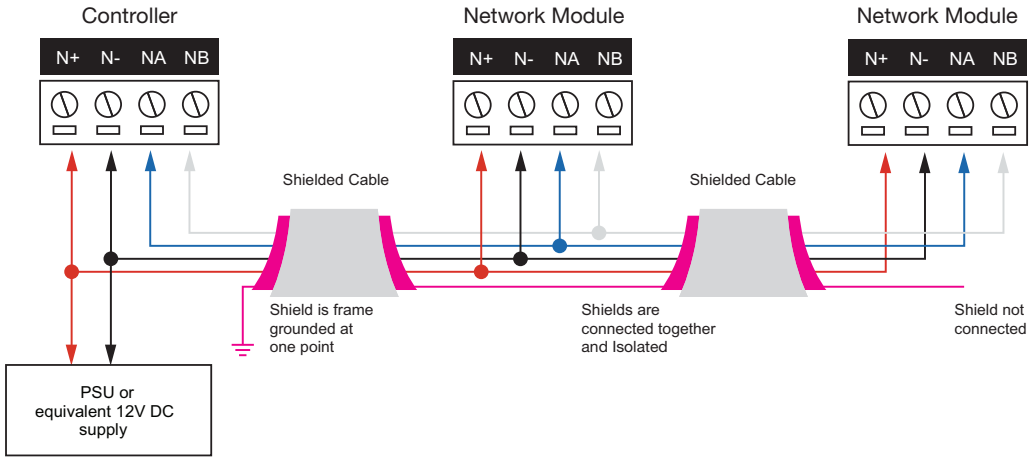
The use of a High Power Type 2 (PoE+) Router is necessary when the Controller is required to supply a combined auxiliary load of more than 600mA.



When using a PoE Router as power source for the Controller, the rating for the auxiliary outputs (S- S+) will be different to those when the Controller is being powered by an Integrated Control Technology Power Supply or a 12V DC supply. Please refer to the values outlined in the Technical Specifications below for more details.

Encrypted Module Network

The Controller incorporates encrypted RS-485 communications technology. Connection of the communications should be performed according to the following diagram.



Always connect the Controller's NA and NB terminals to the NA and NB terminals of the expansion devices and keypads. The N+ and N- must connect to a 12V power supply source capable of supplying the peak current drawn by all modules. If a shielded cable is used, the shield must be connected at only one end of the cable. **DO NOT** connect a shield at both ends.

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

Module Wiring

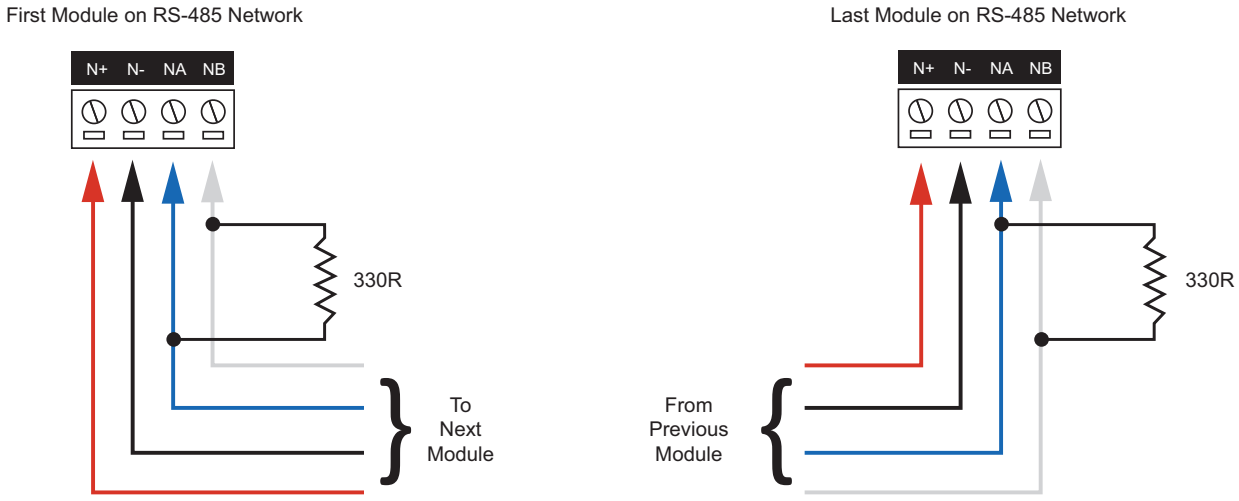
The recommended module network wiring specifications are:

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

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

End of Line (EOL) Resistors

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

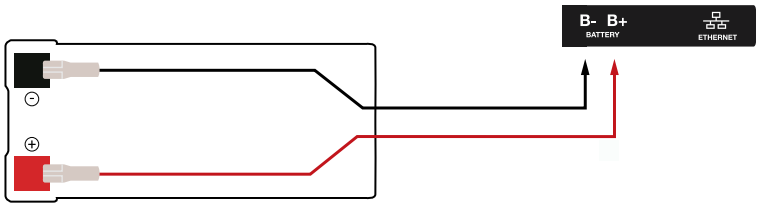


Backup Battery

PoE models only

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

Single Door Controller with PoE Battery Connection:



Gel Cell Backup Battery

Warning:

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

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

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

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

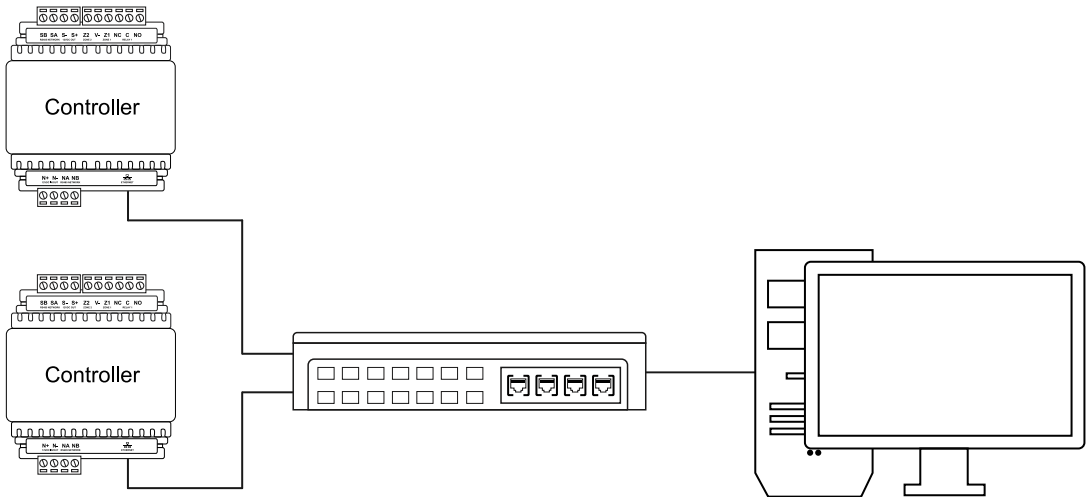
Ethernet 10/100 Network Interface

The communication between the Protege System and the Controller uses a 10/100 Ethernet network operating the TCP/IP protocol suite. The IP address of the Controller can be configured using an LCD Keypad terminal or via the built-in web interface. The default IP address is set to a static IP 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.

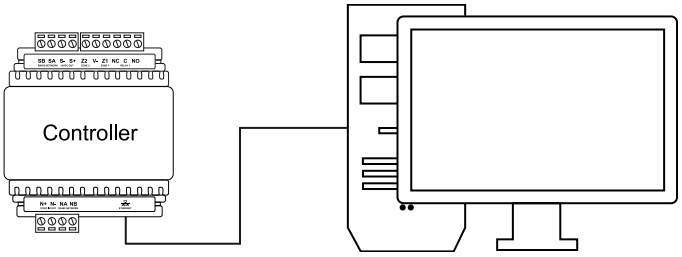
When installing an Ethernet connection the module should be interfaced using a standard segment (<100m in length) and should be connected to a suitable Ethernet hub or switch:

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:



Configuration

Configuring a Controller via the Web Interface

The controller's built-in web interface allows you to configure specific settings in order to get the controller online with a Protege GX server. These settings include:

- IP addressing – IP address, Subnet mask, Gateway and DNS settings
- Event Server addresses
- Event, Control and Download Port settings

In addition to this you can update the controller firmware and/or the firmware of connected expander modules from this interface, and control operator access to the controller.

When the controller is connected to the computer's network, the web interface can be accessed by entering its current IP address into the address bar of a browser, then logging in with valid credentials for that controller. The default IP address is **192.168.1.2**, the default username is **admin**, and the default password is **admin**.

When logging in to the controller web interface it is **highly recommended** that you change the default password. If this password is not changed, a warning will appear reminding you to do this on every subsequent login.

Home Page

Controller Status

- **Health**: Displays the Health Status of the controller. This is the same as the information displayed by the **Get Health Status** function in the Protege GX software.
- **Voltage**: Shows the voltage passing through the controller.
- **Memory Usage**: Shows the current memory usage of the controller, along with a breakdown of what that memory is being used for.
- **Status**: Displays the current Serial Number and IP Address of the controller.

Operator Details

- **Logged in as**: Show the username of the current operator.
- **Logged in at**: Shows the time and date that this operator logged in.

Options

- **Logout**: Log out and return to the login screen.
- **Change Password**: Change the password used by this user.
- **Display Theme**: Switch between the dark (dark background, white text) and light (white background, dark text) display themes for the web interface.

System Settings

This page can be saved or refreshed using the toolbar buttons in the top right. The **Restart** button can be used to reboot the controller, which is required to apply any changes to the fields marked with an asterisk *****.

- **Name**: Equivalent to the **Panel Name** in the Protege GX software. This name is currently not configurable via the controller web interface.
- **Serial Number**: The serial number of the controller.

- **HTTP Port***: The default port is **80**. This can be changed to any network port that is not occupied.
- **Use DHCP**: When enabled the Controller will use DHCP to dynamically allocate an IP address instead of using a static IP address. To use this there must be a DHCP server on the network you are attempting to connect to.
  - **IP Address***: The Controller has a built-in TCP/IP Ethernet device and it must be programmed with a valid TCP/IP address to allow communication. By default the IP address is set to **192.168.1.2**
  - **Subnet Mask***: Used in conjunction with the IP address, a netmask must be configured to allow access to the appropriate node on the subnet. By default this is set to a value of **255.255.255.0**
  - **Default Gateway***: Used in conjunction with the IP address, the gateway can be configured to allow access to a router for external communications beyond the subnet to which the Controller is connected. By default this is set to a value of **192.168.1.1**. Set this to **0.0.0.0** to prevent any external communication.
- **DNS Server***: The IP address of the DNS server being used by the controller. This is required if a DNS name is being used to connect to the Event Server below.
- **Event Server 1***: The IP address or DNS name of the Event Server.
- **Event Server 2/3***: Alternative paths to the Event Server (optional).
- **Event Port***: The default port is **22000**. This must match the port defined in **Global | Event Server** in the Protege GX software.
- **Download Port***: The default port is **21000**. This must match the port defined in **Sites | Controllers | General** in the Protege GX software.
- **Control Port***: The default port is **21001**. This must match the port defined in **Sites | Controllers | General** in the Protege GX software.

Hostname

- **Hostname**: If the controller is accessible via an external hostname it can be entered here. This is only required if the DDNS or HTTPS options (below) are being used.

Dynamic DNS

- **Enable DDNS**: The controller has an in-built DDNS (Dynamic Domain Name Server) application, which allows it to dynamically connect to an external hostname even if its external IP address is not static. Check this checkbox and enter the required details to activate DDNS.
- **DDNS Server**: Enter the name of the DDNS server which is being used. Currently Duck DNS (www.duckdns.org) and No-IP (www.noip.com) are supported DDNS providers.
- **DDNS Username/Password**: Enter the required credentials for your DDNS provider.
  - **Duck DNS**: The username should be left blank. The password is the **Token** generated by your Duck DNS account.
  - **No-IP**: The username and password are the credentials used to log in to your No-IP account.

HTTPS

This feature is only available with controller OS version 2.0.25 or higher.

- **Use HTTPS**: It is possible to connect to the controller via HTTPS, by using a signed HTTPS certificate to create an encrypted connection between controller and web browser. Check this checkbox and enter the required details to enable HTTPS.
- **HTTPS Port***: The default port is **443**. This can be changed to any port that is not occupied.
- **Use HTTPS Certificate**: This option will prompt you to load an HTTPS certificate onto the controller. This can be either a third-party certificate obtained from a Certificate Authority, or a self-signed certificate.
  - **Load Validation File**: Click to browse and upload a validation file (.txt format) provided by the Certificate Authority. This will be used by the CA to validate your domain name. Validating the domain this way requires your controller to be externally accessible via a hostname on external port 80.

    This step is not required when installing a self-signed certificate.

- **Install Certificate**: Click to browse and upload an HTTPS certificate in .pfx format. If the file is secured with an export password you will be prompted to enter it. **Restart the controller** to implement HTTPS.

Operators

Operators can be created, deleted and saved using the toolbar buttons in the top right. Note that these are operators for the controller's web interface and do not correspond to operators in the Protege GX software.

- **Name**: A name for the operator record in the web interface.

Configuration

- **Username/Password**: The operator's login credentials for the controller's web interface.
- **Change Password**: Click this button to change the password of the operator. It is recommended that you give each operator a secure password (see below).
- **Default Language**: Select a default language for the operator. This language will be displayed when the operator uses the web interface.

Operator Timeout

- **Enable Operator Timeout**: When this option is enabled, the operator will be automatically logged out of the web interface after a set period of inactivity.
- **Operator Timeout**: Set the length of time in minutes before the operator will be automatically logged out.

Application Software

Controller Software

- **Current Version**: Displays the current firmware version of this controller. Click on this field to display further version information.

Update Application Software

- **BIN File**: This section is used to update the firmware of the controller. Click **Choose File** to browse to the firmware file (.bin format) supplied by ICT, then click **Upload** to install the new firmware on the controller. This process will take approximately 10 minutes and the controller will not be able to perform its normal functions during this period. It is recommended that firmware updates are performed when the site is closed for maintenance or at times of low activity.

Update Module Firmware

- **Module**: This section is used to update the firmware of any module connected to the controller. Select the connected module that requires a firmware update from the dropdown.
- **Upload Firmware**: Click **Choose File** to browse to the firmware file (.bin format) supplied by ICT, then click **Upload Firmware** to install the new firmware on the selected module.

Warning: Updating module firmware will put the entire network into maintenance mode, preventing normal activity for the duration of the update process. Module firmware **must not** be updated remotely.

Creating a Secure Password

When changing the default password it is **highly recommended** that you create a very secure password.

As a guideline, a secure password should have these features:

- Minimum 8 characters in length
- Combination of upper and lower case letters
- Combination of numbers and letters
- Inclusion of special characters

Setting the IP Address

There are two methods for setting the IP address of a controller. The recommended method is using the built-in web interface:

1. With the controller connected to your network, type the current IP address into the address bar of your web browser. The default IP address is 192.168.1.2.

   If the current IP address is not known, it can be temporarily defaulted to 192.168.111.222 allowing you to view and/or change the IP address. See Temporarily Defaulting the IP Address in this document.

2. Enter the user name and password. The default user name is **admin** and the default password is **admin**.

   For security reasons it is **highly recommended** that you change this password before deployment.

3. Enter the required settings, save, then restart your controller by either cycling the power or clicking the **Restart** button at the top right.

Setting the IP Address from a Keypad

If the current IP address of the Controller is not known, it can be viewed and/or 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). 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.

Configuring a Controller via the Protege GX Software

To connect a Controller to the software, you must add it to the system programming.

Adding a Controller:

1. Login to Protege GX and navigate to **Sites | Controllers** from the main menu.
2. Click **Add** to display the Add Controller window.
3. Select the option that best suits your needs:
   - **Add controller with default records**: To add a single Controller record and automatically add the specified expander modules, doors and groups as required by your site.

- **Add an individual controller record**: To add just the Controller. Any expander modules, doors, groups and other programming must be added manually.
- **Add new controller based on an existing controller**: To duplicate the programming of a previously configured Controller.

4. Once added, the Controller will require configuration to define settings including the serial number and communication parameters.

You may need to restart the services to bring the Controller online. Open the **Services** application and restart the Protege GX services.

Adding a Controller with Default Records

If adding a Controller with default records, the **Add Controller** configuration window is displayed, enabling you to automatically add the expander modules, inputs, outputs and doors that your site will be using. All of these records can be edited or deleted at a later stage, or additional records can be added.

General

- **Name**: Defines the name of the Controller to be used as a reference when programming the system.
- **Count**: Defines the number of Controllers to be added. If more than one Controller is added, the subsequent Controllers are assigned default names that can be edited later.

Controller

- **Inputs**: Defines the number of onboard Controller inputs that you intend to use. Note that the Single Door (1D) Controller has only 2 onboard inputs, so the number selected here should only be set to 2. If you are using the onboard readers then some of the inputs may be used for their reader functions and not be required. By default, the number of inputs will be set to 16 as older versions of the Controller hardware have 16 onboard inputs.
- **Outputs**: The Single Door (1D) Controller has 1 onboard output. By default, the number of outputs is set to 4 for compatibility with older Controller hardware and should be left set to four. When the outputs are created they are assigned sequential output numbers 1 to 4. On the Single Door (1D) Controller the Relay 1 is output #3. Outputs #1, #2, and #4 are generated to maintain compatibility with older hardware and do not exist on the Single Door (1D) Controller.
- **Add Trouble Inputs**: Select this option to automatically add the Controller trouble inputs. Some trouble inputs will not be relevant to the DIN Rail Controller and can later be deleted. For further details refer to the section on trouble inputs.

Keypads, Input Expanders, Reader Expanders, and Output Expanders

Use these fields to add the relevant number of expanders that are connected to the module network of the site, and the number of inputs, outputs and trouble inputs that will be used. Note that if the onboard reader is used then it should be included in the number of Reader Expanders so that programming fields will be created for it. Refer to the Programming the Onboard Reader for further details.

Options

- **Create "Installer" Menu Group**: Creates a menu group with every menu enabled.
- **Create Floor Plan**: Create a floor plan including all inputs and outputs. This is useful for small sites with only a few inputs and outputs. For larger sites it is generally better to create the floor plans manually.

Doors

- **Doors**: Automatically creates the defined number of door records. Typically this would be two per Reader Expander.
- **Add Door Trouble Inputs**: Create Door Forced and Door Left Open trouble inputs.

- **Assign to Reader Expanders**: Assigns the first door to the Reader One programming of the first Reader Expander, the second door to the Reader Two programming of the first Reader Expander, the third door to the Reader One programming of the second Reader Expander, etc.
- **Assign Reader Lock Output to Door Configuration**: Assigns the Lock Output programming of the first door to the Reader One lock output on the first Reader Expander, the Lock Output programming of the second door to the Reader Two lock output on the first Reader Expander, the Lock Output programming of the third door to the Reader One lock output on the second Reader Expander, etc.
- **Assign Reader Beeper to Door Alarm Configuration**: Assigns the Pre Alarm Output and Left Open Alarm Output of the door programming to the beeper on the associated Reader Expander.

Adding a Controller Based on an Existing Controller

If adding a Controller based on an existing Controller, the **Copy Controller** configuration window is displayed, enabling you to define how the new Controller and associated records will be created:

- **Site (Copy From)**: Defines the site from which the programming should be copied.
- **Controller (Copy From)**: Defines the Controller from which the programming should be copied.
- **New Controller Name**: Defines the name to be assigned to the new Controller.
- **Prepend Controller name to all record names**: When enabled the name of the Controller will be added to the start of each record name. For example, if a door record is called Main Entrance and the new Controller is named CTRL2, the new door record would be CTRL2 Main Entrance.
- **Add Access Level and Door Group**: When enabled creates a door group (using the Controller name) containing all doors, and an access level containing this door group.
- **Copy Global Records**: When enabled copies the global records that are relevant to the original Controller.

Configuring a Controller

Once added, the Controller needs to be configured to define settings including the serial number and communication parameters.

Controllers | General Settings

General

- **Name**: The controller name identifies the module to the operator or system user, and should ideally describe the premises or building where the controller is installed.
- **Name (Second Language)**: The name of the controller in a second language (optional).
- **Record Group**: Defines the record group that the controller belongs to.

Communications

- **Serial Number**: The serial number of the controller. This can be obtained from the label on the side of the controller or from the configuration page of the built-in web interface.
- **IP Address:** The controller has a built-in TCP/IP Ethernet Device and it must be programmed with a valid TCP/IP Address to allow the software to connect. The default IP address is set to 192.168.1.2. Programming an IP address requires knowledge of the network and subnet that the controller will be connected to. ALWAYS consult the network or system administrator before programming these values.

  Programming the IP Address, Subnet Mask, and Default Gateway requires knowledge of the network and subnet that the system is connected to. You should always consult the network or system administrator before programming these values.
- **Dynamic IP Address Update**: When enabled, the incoming IP address of the controller is detected by the event server, and the IP address field is automatically updated.
- **Download Port:** When connecting to the controller using TCP/IP, this specifies the IP port to use. By default this is port 21000.

- **Download Server**: Defines the download server used by the controller.
- **Control and Status Request Port**: The IP port through which control commands will be sent. By default this is port 21001.
- **Last Known IP Address**: Shows the last IP address that the controller communicated to the server on. (Read only)
- **Last Downloaded**: Shows the date and time of the last download. (Read only)

Display

- **Panel Name:** The name used to identify the Controller in the IP reporting services.

Controllers | Configuration Settings

Configuration

- **Test Report Time (HH:MM):** The test report time, in conjunction with the **Test Report Time is Periodic** option, sets the time of the day or the period that the test report trouble input activates.

  When the **Test Report Time is Periodic** option is enabled, the time programmed will be used as a period between reports in hours and minutes; otherwise it is treated as a time of day.

- **Automatic Offline Time**: Allows the panel to update the users and other offline parameters on all intelligent modules at a set time of the day.
- **AC Restore Delay Time (seconds):** The AC Restore time allows the installer to program a time that AC must be present for after an AC Failure before restoring the AC Failure Trouble Input. Set this to a larger value for locations that experience frequent but short interruptions in power or that operates on a generator frequently. This setting is only relevant to older hardware which is supplied by an AC power source.
- **AC Fail Time (Seconds):** The AC Fail time allows the installer to program a time that AC mains voltage must have failed before activating the AC Failure Trouble Input. Set this to a larger value for locations that experience frequent but short interruptions in power or that operates on a generator frequently. This setting is only relevant to older hardware which is supplied by an AC power source.
- **Module UDP Port:** This is the UDP port that all Ethernet enabled modules will communicate with the Protege GX controller over. If this port is changed all modules will also need to be changed.
- **Modem Country:** The onboard modem must be configured for the region that the controller is being installed in to ensure correct operation.
- **Modem Backup Phone Number**: If Ethernet communication fails, the modem will dial this number to report events.
- **Default Language:** The controller supports multiple languages on the keypad and the serial event printers. The language selected here will be the default language for users who have no language selected and also for any events.
- **Download Retry Delay**: Defines the frequency (in seconds) at which the software sends programming updates to the controller.
- **Register as Reader Expander**: Used for programming the onboard reader. The onboard reader is programmed as and treated by the system as if it were a reader expander connected on the module network. This setting defines the address at which the onboard reader will be registered and must be distinct from any physical reader expanders connected to the module network.
- **Onboard Reader Lock Outputs**: Defines the output that will be activated upon successful door access. If set to none the lock output (if any) programmed under the associated reader expander will be used.
- **Touchscreen UDP Port**: The UDP port that a touchscreen will communicate over.

Encryption

- **Initialize Controller Encryption**: Enables encryption of the messages sent between the controller and the Protege GX server. Selecting this option performs a one-off process that randomly generates and begins using a 256 bit AES encryption key. Using an RSA algorithm, this key is exchanged and stored in both the

controller and the Protege GX database.

- **Disable Controller Encryption**: Instructs the software to stop using encryption. To avoid encryption being disabled accidentally or maliciously, this option will NOT change the encryption setting in the controller itself. To stop the controller from using encryption it must be hardware defaulted.
- **Encryption Enabled:** Read only field that indicates if encryption is enabled.

Controllers | Options Settings

For more information on the **Options** and **Misc Options** settings, refer to the Protege GX Online Help or the Protege GX Operator Reference Manual.

Controllers | Time Update Settings

- **Automatically Synchronize with an Internet Time Server**: Select this option to automatically synchronize the controller with an internet time server.
- **Primary SNTP Time Server:** IP address of the primary SNTP time server for the controller to update its time from.
- **Secondary SNTP Time Server:** IP address of the secondary SNTP time server for the controller to update its time from should it not be able to connect to the primary SNTP server.
- **Time Zone:** The current time zone that should be assigned to the controller. Offset from GMT.

When using a Time Server, the time provided is always in UTC (Coordinated Universal Time) which has no time zone and is not subject to any daylight saving time rules. This means that you must correctly configure the **Time Server**, the **time zone** that the controller is operating in, and the **daylight savings settings** for NTP to work correctly. Failure to configure any of these things will result in the time being inaccurate.

Controllers | Custom Reader Format Settings

Custom Reader Configuration

- **Custom Reader Type**: Defines the reader type. The data can be output as Wiegand (D0 and D1) or Magnetic Data (Clock and Data).
- **Bit Length**: The bit length defines the total number of bits that are sent by the card reader for each card badge.
- **Site Code Start**: The site code start defines the index where the site code data starts in the data transmitted. The count starts at zero.
- **Site Code End**: The site code end defines the index where the site code data ends in the data transmitted. The count starts at zero.
- **Card Number Start**: The card number start defines the index where the card number data starts in the data transmitted. The count starts at zero.
- **Card Number End**: The card number end defines the index where the card number data ends in the data transmitted. The count starts at zero.
- **Data Format**: The data format defines how the card number that is received from the card reader is handled. If the size of the site code and card number are less than 16 bits (e.g. Site Start – Site End is less than 16 bits) use 16 bit, otherwise use 32 bit. If unsure, use 32 bit.

Parity Options (1-4)

There can be up to 4 blocks of parity calculated over the received data.

- **Parity Type**: The parity type defines the method of calculating the parity for the block. This is either Even or Odd Parity.
- **Parity Location**: The parity location defines the position of the parity bit in the received data.
- **Parity Start**: Defines where the parity block starts in the received data.
- **Parity End**: Defines where the parity block ends in the received data.

Bit Options (1-4)

- **Set Bit**: A set bit defines a location in the received data that must always be set (or a logical '1'). The set bit defines the location of the bit in the received data.
- **Clear Bit**: A clear bit defines a location in the received data that must always be cleared (or a logical '0'). The clear bit defines the location of the bit in the received data.

Addressing Modules

Traditionally the network address of a module has been set using a bank of DIP Switches located on each individual module. The Protege system modules enable addresses to be configured electronically via the Protege GX software.

The factory default address of all DIN Rail modules is 254. If this address is not changed the module will not be able to register with the Controller.

To change the network address of a module:

1. Ensure the Controller is correctly powered and is communicating with the Protege GX software.
2. Connect the module(s) that require addressing to the module network. Make sure that the Power light on each module is on and that the Status light begins flashing rapidly.
3. Allow some time for the module(s) to attempt to register with the Controller.
   - If the module has the default address of 254 or has the same address as another module, the Fault light will begin flashing an error code.
   - If the module has been previously addressed and is not a duplicate then it will succeed in registering and the Status light will begin flashing at 1 second intervals.
4. Once all modules have completed the registration process (successful or not), open the Auto-addressing window in the software by right clicking on the Controller and selecting **Module Addressing**.
5. If the address can be changed electronically this is indicated in the Address can be changed column and the selector in the Address column is enabled. The Update and Find options will also be enabled. If it is not clear which module is which, click **Find** to instruct the respective module to flash its Status light for the specified period of time. Modules can also be identified by comparing the serial number on the label with that shown in the software. Ensure that you are clear which module is which before assigning addresses to them.
6. Enter an address for the relevant module(s) by selecting an option from the Address column. When an address has been selected but has not yet been updated on the module, it is shown in red. Modules can be updated individually by clicking the option in the Update column, or all at once using the **Update All** button. Allow about 5 seconds per module for the new address to be sent and registered.
7. Click **Refresh** to update the list and display the new addresses. The addresses change from red to gray to show that they have been read back from the Controller.
   - If the address has not changed, check the module is online and communicating and that is has finished attempting to register.
   - If the address has changed but the module is not shown as registered, check the address is in the valid address range and that it is not a duplicate of another module address.

Once all modules are online and registered with the desired addresses, the addressing process is complete.

Door Access Control

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

The recommended cable types for RS-485 are:

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

Important:

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

All ICT readers are shipped with single LED mode set as default and are fully compatible with the Protege system, such as tSec Standard Readers, tSec Mini Readers, etc.

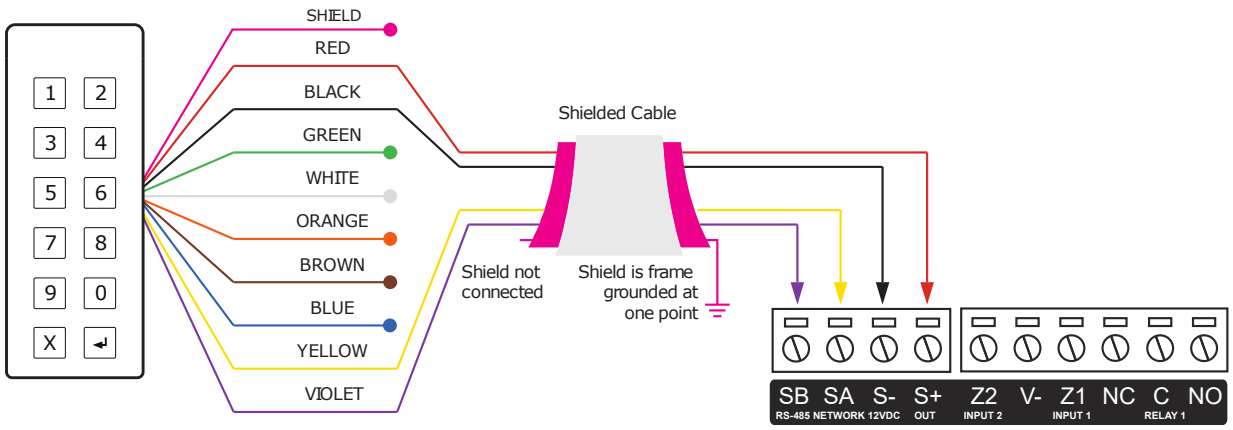
RS-485 Reader Locations

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

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

RS-485 Reader Connection (Entry Only)

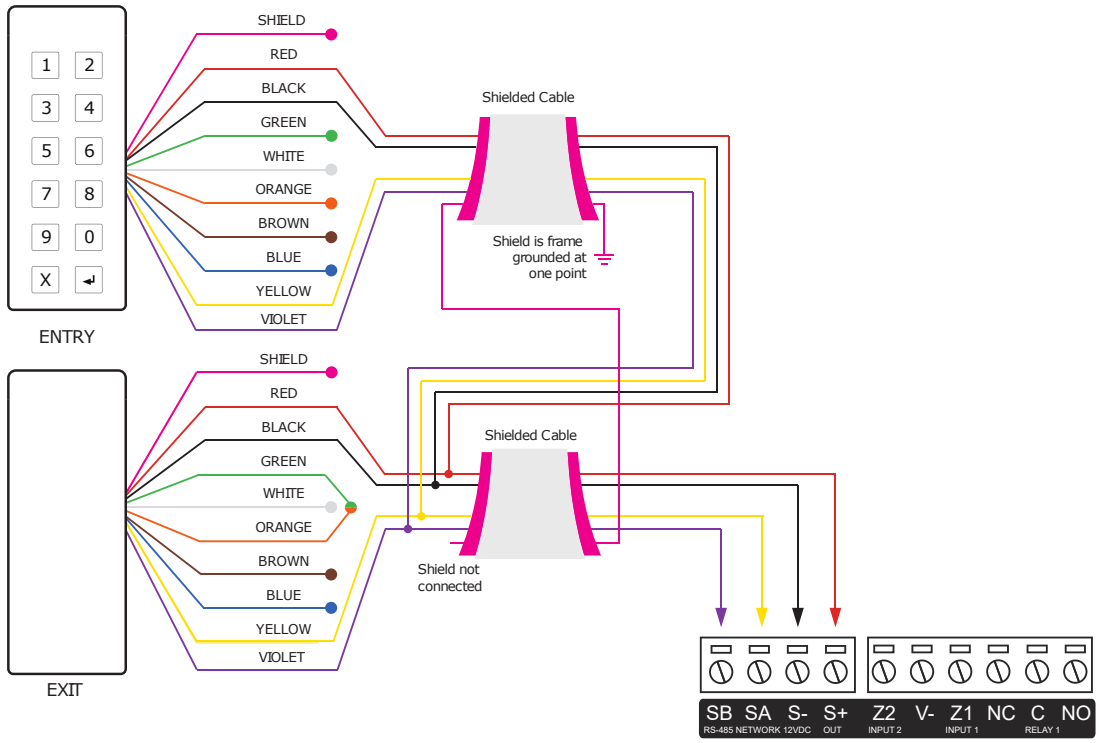
The following diagram shows the connection of a single RS-485 reader connected in entry only mode.



When the green and orange wires are not connected together, the reader defaults to an entry reader.

RS-485 Reader Connection (Entry/Exit)

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



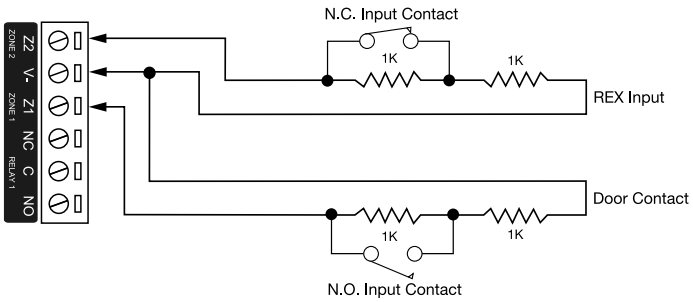
The exit reader has the **green** and **orange** wires connected together.

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

Door Contact Connection

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

Typical Configuration of Door Monitoring Contacts:



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

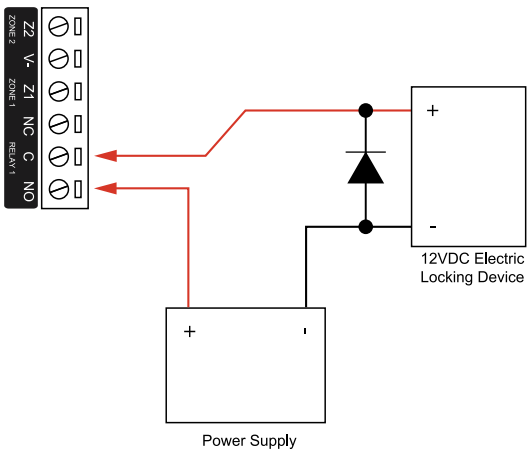
When connected the REX input can be programmed to operate regardless of the door contact state. The REX input can also be programmed to recycle the door alarm time to prevent nuisance alarms when the door is held open to permit longer entry.

Lock Output Connection

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

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

Typical Lock Output Connection:



Programming the Onboard Reader

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

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

The default settings are shown in the following table:

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

The controller's onboard reader port supports an RS-485 reader interface allowing ICT 485 readers to be configured. The option is available to select the onboard reader's port type to ICT 485 from the Reader Expander menu.

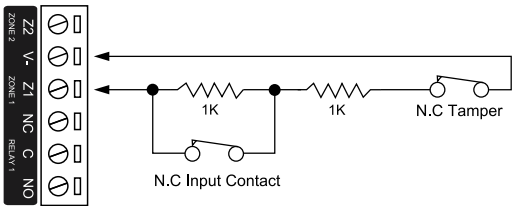
Inputs

The Controller has 2 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.

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

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

EOL Resistor Input Configuration:

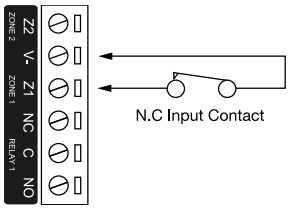


Inputs 1 and 2 can operate as either general purpose inputs or as onboard reader inputs. If used as general purpose inputs you must ensure that they are not defined in the onboard reader set up.

Each input can use a different input configuration. To program a large number of inputs with a certain 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 (OPEN) Alarm and (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
1k	1k	Open, Closed, Tamper, Short
1k	No Resistor	Open, Closed
<5K7	No Resistor	Open, Closed

Value 1	Value 2	Monitored Status
No Resistor	No Resistor	Open, Closed
2k2	6k8	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

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.

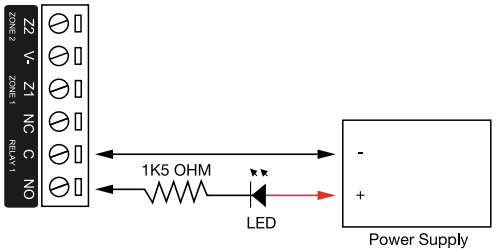
The following table details the trouble inputs that are configured in the Controller. The trouble type and group define the trouble that is generated by the trouble input when it is activated.

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

Outputs

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

Example Relay Connection:



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

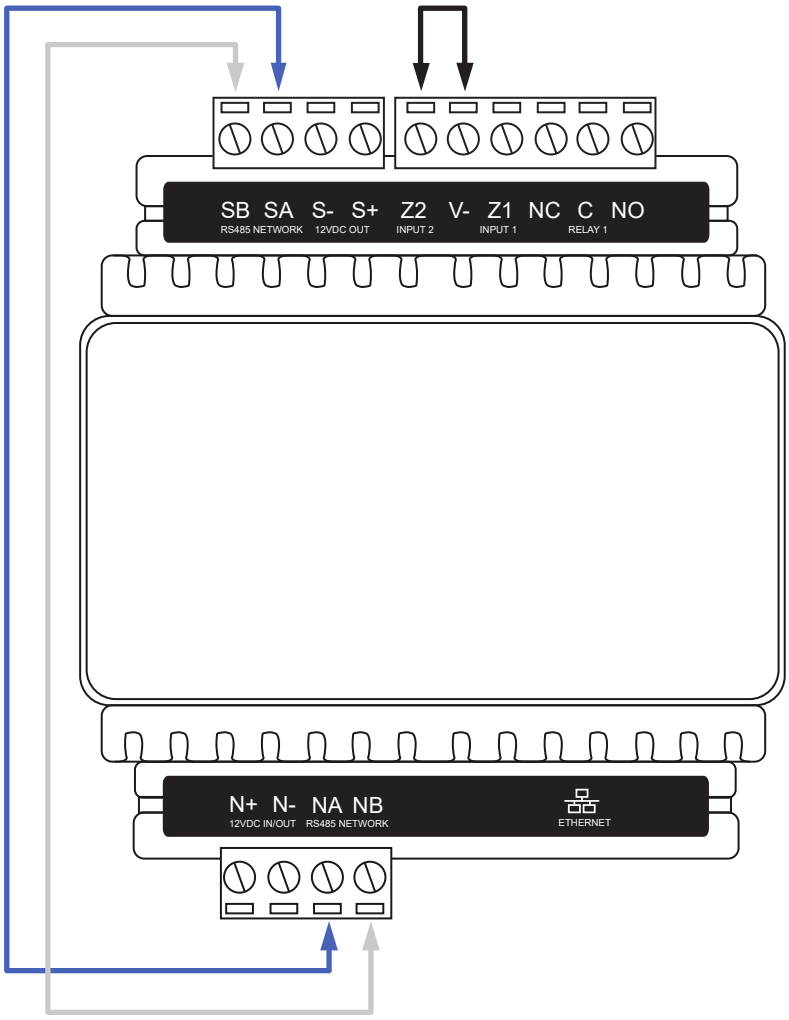
Hardware Configuration

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 resets 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 previously configured IP address is used again.

1. Remove power to the Controller by disconnecting the 12V DC input.
2. Wait until the power indicator is off.
3. Connect a wire link between **NA** of the module network and **SA** of the reader network, and between **NB** of the module network and **SB** of the reader network.
4. Connect **Input 2** to ground.



5. Power up the Controller.

1. When the Controller starts up it will use the following settings:
   - IP address : 192.168.111.222
   - Subnet Mask : 255.255.255.0

- Gateway : 192.168.111.254
- DHCP : disabled

2. Connect to the Controller by entering 192.168.111.222 into the address bar of your web browser, and view or change the IP address as required.

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

3. Remove the wire link(s) and power cycle to the Controller again.

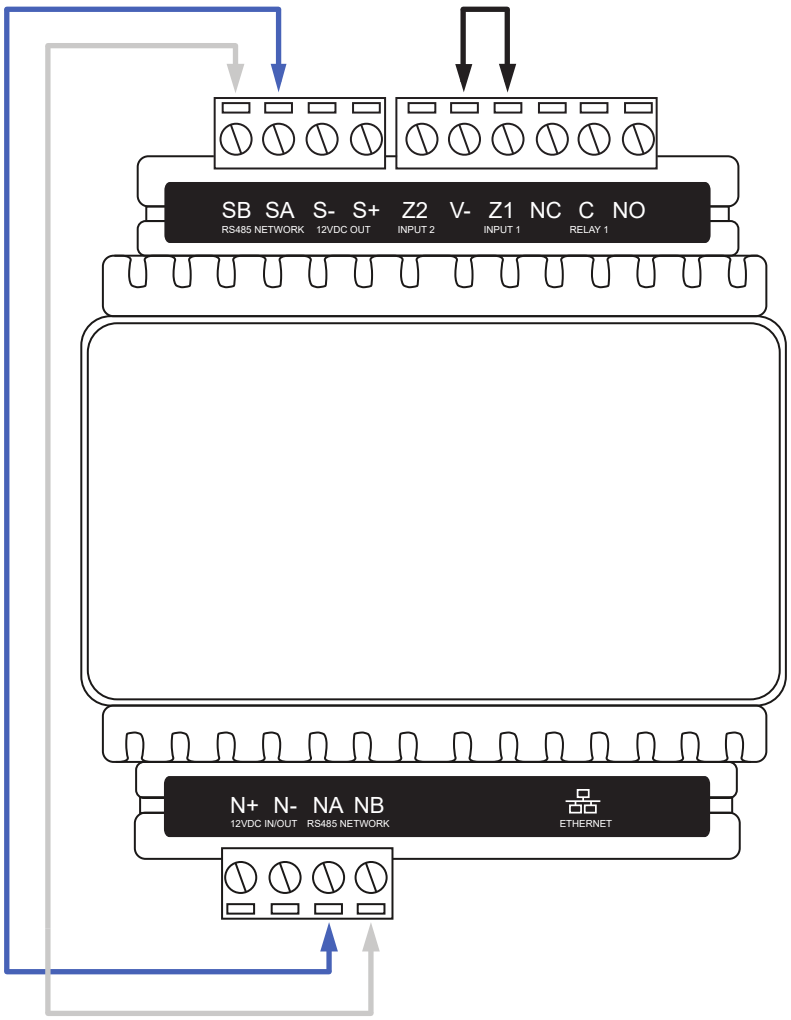
   You can now connect to the Controller using the newly configured (or now known) IP address.

Defaulting a Controller

The Controller can be set back to the factory default which resets all internal data and event information. This allows you to remove all programming and start afresh.

Defaulting a One-Door Controller

1. Remove power to the Controller by disconnecting the 12V DC input.
2. Wait until the power indicator is off.
3. Connect a wire link between **NA** of the module network and **SA** of the reader network, and between **NB** of the module network and **SB** of the reader network.
4. Connect **Input 1** to ground.



5. Power up the Controller.
6. Remove the wire link(s).

The system will now be defaulted with all programming and settings returned to factory configuration.

Defaulting the Controller does not reset the IP address. Refer to Configuring the IP Address for instructions on how to reset the address.

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	The Controller is operating normally

Fault Indicator

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

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

PoE Power Indicator

PoE models only

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

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

Battery Indicator

PoE models only

The Battery indicator shows the status of the backup battery.

State	Description (with mains power connected - power indicator on)
Flashing (red)	Backup battery is disconnected
On (red)	Backup battery failed its dynamic battery test
On (green)	Last backup battery dynamic test successful
State	**Description (with mains power disconnected - power indicator off)**
Flashing (red)	Mains has failed and the PSU is drawing power from the battery. State is Battery Low
Flashing (green)	Mains has failed and the PSU is drawing power from the battery. State is Battery Restore

Ethernet Link Indicator

The Ethernet indicator shows the status of the Ethernet connection.

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

Reader Data Indicators

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

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

Relay Indicator

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

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

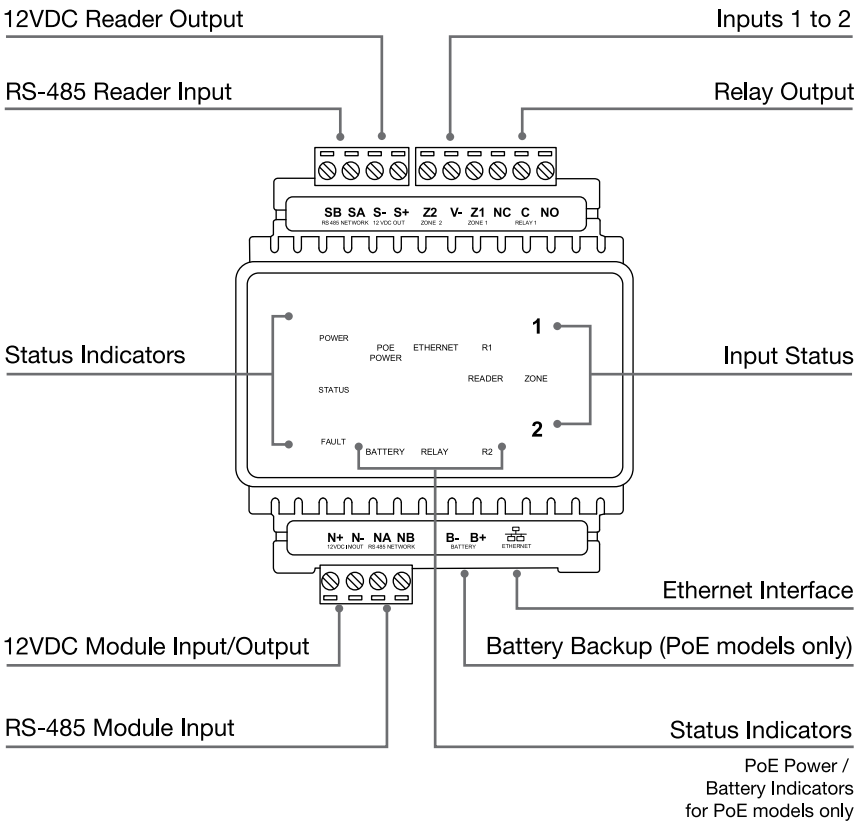
Input Indicators

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

State	Description
Constantly off	Input is not programmed
Constantly on (red)	Input is in an OPEN state
Constantly on (green)	Input is in a CLOSED state
Continuous flash (red)	Input is in a TAMPER state
Continuous flash (green)	Input is in a SHORT state

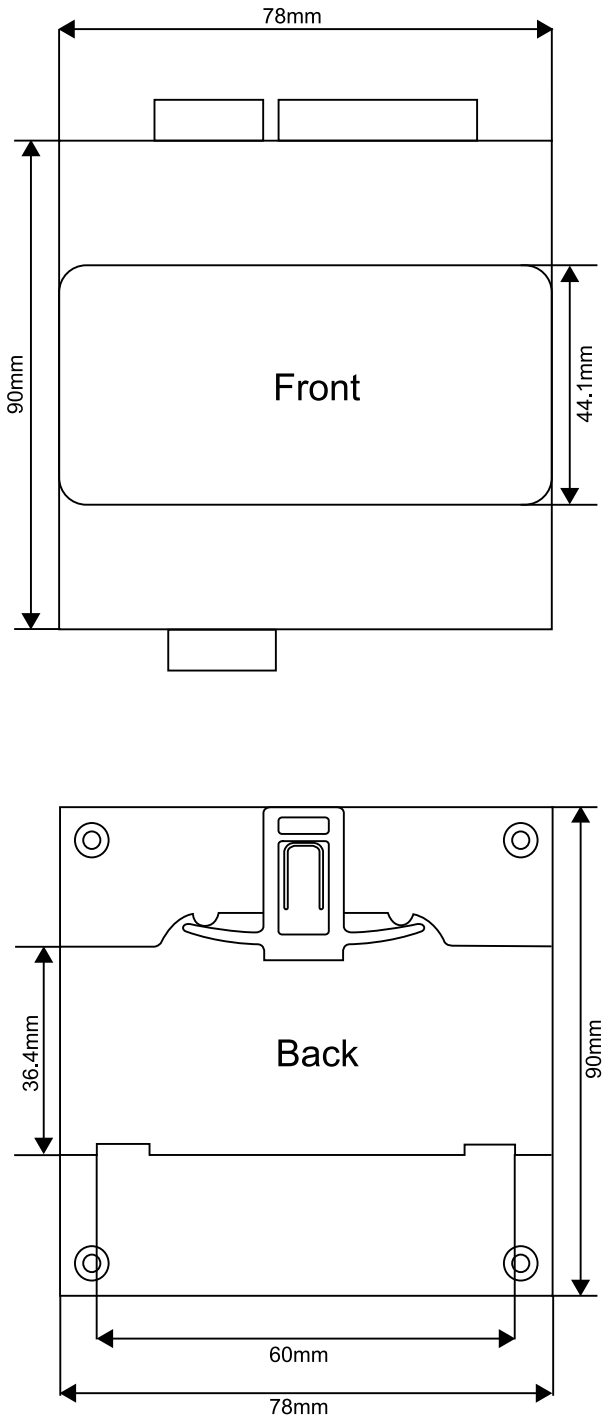
Mechanical Diagram

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



Mechanical Layout

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



Technical Specifications

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

Ordering Information		
Order Code	PRT-CTRL-DIN-1D	PRT-CTRL-DIN-1D-POE
Product Name	Protege GX DIN Rail Single Door Controller	Protege GX DIN Rail Single Door Controller with POE
Power Supply		
Operating Voltage	11-14V DC	
Operating Current	120mA (typical)	
DC Output	10.45-13.85VDC 0.7A (typical) electronic shutdown at 1.1A	13VDC +/- 0.5 0.7A (typical) electronic shutdown at 1.1A
Total Combined Current*	0.82A (Max)	0.6A total at outputs, inclusive of battery charging (PoE) / 1A total at outputs, plus battery charging (PoE+)
Electronic Disconnection	9.0VDC	
Battery		
Battery Charging	-	300mA (typical)
Battery Low	-	11.2VDC
Battery Restore	-	12.5VDC
Communications		
Communication (Ethernet)	10/100Mbps Ethernet communication link	
Communication (RS-485)	2 RS-485 communication interface ports - 1 for module communications, 1 for reader communications	
Readers		
Readers	1 RS-485 enabled reader port, allowing connection of up to 2 RS-485 capable readers providing entry/exit control for a single door	
	RS-485 reader port connections support configuration for OSDP protocol	
Inputs and Outputs		
Inputs	2 high security monitored inputs	
Relay Outputs	1 Form C Relay - 7A N.O/N.C. at 30 VAC/DC resistive/inductive	
Dimensions		
Dimensions (L x W x H)	78 x 90 x 60mm (3.07 x 3.54 x 2.36")	
Weight	167g (5.89oz)	205g (7.23oz)
Operating Conditions		
Operating Temperature	-10° to 55°C (14° to 131°F)	

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

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

The ICT implementation of OSDP conforms to a subset of the OSDP functionality. For specifications and reader configuration, refer to AN-254 Configuring OSDP Readers, available from the Integrated Control Technology website.

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

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

New Zealand and Australia

General Product Statement

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

Intruder Detection Maintenance Routine

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

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

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

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

Peripheral Devices

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

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

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

Testing Frequency

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

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

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

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

Recommended Routine Maintenance Procedures

Preliminary Procedures

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

On Site Maintenance Procedures

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

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.

Task	Frequency	Description
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.
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

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)

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.

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 , EN-DIN-24-ATTACK and EN-DIN-31 , 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.

FCC Compliance Statements

FCC Rules and Regulations CFR 47, Part 15, Class A

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

Operation is subject to the following two conditions:

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

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

Industry Canada Statement

ICES-003

This is a Class A digital device that meets all requirements of the Canadian Interference Causing Equipment Regulations.

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

Disclaimer and Warranty

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

For warranty information, see our Standard Product Warranty.

New Zealand
4 John Glenn Ave
Rosedale
Auckland 0632
Email: sales@ict.co
Toll free: (0800) 428 111
Ph: +64 9 476 7124

USA
5265 S Rio Grande Street
Suite 201
Littleton, CO 80120
Email: ussales@ict.co
Toll free: (855) 428 911
Ph: +1 720 442 0767

Canada
6201 Highway 7
Unit 7
Vaughan, Ontario, L4H 0K
Email: cansales@ict.co
Ph: +1 647 724 3428

Australia
Building 4
39-43 Duerdin Street
Notting Hill, VIC 3168
Email: ausales@ict.co
Ph: +61 426 145 907

EMEA
Email: emeasales@ict.co
Ph: +44 1625 800078

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