

**Protege Ethernet 2 Reader Expander
Installation Manual**

ICTProtege®.

The specifications and descriptions of products and services contained in this document were correct at the time of printing. Integrated Control Technology Limited reserves the right to change specifications or withdraw products without notice. No part of this document may be reproduced, photocopied, or transmitted in any form or by any means (electronic or mechanical), for any purpose, without the express written permission of Integrated Control Technology Limited. Designed and manufactured by Integrated Control Technology Limited. Protege® and the Protege® Logo are registered trademarks of Integrated Control Technology Limited. All other brand or product names are trademarks or registered trademarks of their respective holders.

Copyright © Integrated Control Technology Limited 2003-2016. All rights reserved.

Publication Date: June 2017

Contents

1	Introduction	5
2	Installation	6
2.1	Package Contents	6
2.2	Location and Mounting	6
2.3	Cabinet Tamper Switch	7
2.4	Earth Ground Connection	7
2.5	AC Power	8
2.6	Backup Battery	8
2.7	Status Indicator	9
2.8	Ethernet 10/100 Network Connection	9
2.9	Encrypted Module Network	10
2.10	Slave Device Network	12
2.11	RS-485 Biasing Settings	14
3	Communication Setup	15
3.1	Keypad Programming	15
	Network Mode	15
	Controller Connection	16
	DHCP Configuration	16
	Network UDP Port	16
	Module IP Address	16
	Module IP Subnet Mask	17
	Module IP Gateway	17
	Controller IP Address	17
3.2	Web Programming	17
	User Login	18
	Setup	18
	Network Setup	18
	Statistics	19
	Users	19
4	Door Access Control	20
4.1	Reader Connection	20
4.2	Multiple Wiegand Reader Connection	21
4.3	Magnetic Reader Connection	22
4.4	Door Contact Connection	22
4.5	Door Lock Connection	23

5	Zone Inputs	24
5.1	Zone Inputs - Reader	24
5.2	Trouble Zone Inputs	26
6	Programmable Outputs	27
6.1	Lock PGM Outputs (1 and 2)	27
6.2	Standard PGM Outputs (3 to 8)	28
6.3	PGM Beeper Outputs Special Functions (5 and 8)	29
7	Configuration Switch	30
7.1	Address Configuration	30
8	Status Indication	31
8.1	Status Indicator	31
8.2	Fault Indicator	31
8.3	Charge/Test Indicator	31
8.4	Auxiliary OK Indicator	31
8.5	AC OK Indicator	31
8.6	5V Isolated Power Indicator	32
8.7	Lock 1/Lock 2 Indicators	32
8.8	Network RX/TX Indicator	32
8.9	R1 and R2 Power Indicator	32
8.10	R1 and R2 Data Indicator	32
9	Error Code Indication	33
9.1	Error Code Display	33
10	Technical Specifications	34
11	New Zealand and Australia	35
12	European Standards	36
13	Ordering Information	38
14	Warranty	39
15	Contact	40

1 Introduction

The ICT Protege System is a powerful integrated alarm and access control management system designed to provide integration with building automation, apartment complex control and HVAC in one flexible package. Communication is over a proprietary high speed protocol across an encrypted local area network and AES Encrypted Proprietary RS-485 module network. Using modular-based hardware design, system installers have the flexibility to accommodate any installation from small to large, residential or commercial.

The PRT-RDE2-PCB Protege Ethernet Reader Expander extends the number of card reader inputs on the system by 2, number of zone inputs by 8 (4 zones used for door monitoring and control and up to eight can be used for extended functionality) and the number of PGM outputs by 8 (includes 2 monitored lock control outputs).

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 up to a distance of 900M (3000ft). Communication beyond this distance requires the use of a RS-485 Network Extender or the Slave Communications Port on a PRT-RDI2-PCB Protege Intelligent Reader Expander.

The current features of the Protege Ethernet 2 Reader Expander include:

- 4 Wiegand Reader Mode for 2 Entry/Exit Doors Per Reader Expander
- Secure Encrypted RS-485 Module Communications
- 8 Zone Inputs
- 2 Monitored Lock Control PGM Outputs
- 6 Open Collector PGM Outputs (Reader Control Outputs)
- 1.5A Switching Power Supply
- Intelligent Battery Charge and Monitoring
- Smart Reader Missing/Tamper Monitoring
- Online and Remote upgradeable firmware

For more information on the Protege Ethernet 2 Reader Expander and other Integrated Control Technology products please visit the ICT website (<http://www.ict.co>).

2 Installation

2.1 Package Contents

When receiving the PRT-RDE2-PCB Protege Reader Expander you should find the kit contains the items listed below. When receiving this product, you should find the kit contains the items listed below. If you do not have the correct contents, please contact your distributor immediately.

PRT-RDE2-PCB - Protege Reader Expander PCB Only

- Reader Expander Printed Circuit Board
- 6 X Plastic Mounting Standoffs
- 20 X 1K Ohm Resistors
- 2 X 1N4007 Lock Reverse EMF Protection Diodes
- Red/Black Backup Battery Wires

2.2 Location and Mounting

The Reader Expander is available as a PCB Only (Printed Circuit Board) or complete unit supplied with a metal cabinet. We recommend that the cabinet is used wherever possible as this provides the best mounting and installation solution as well as the required cable entry and termination space.

When installing the Reader Expander ensure that there is adequate clearance around all sides of the enclosure and air flow to the vents of the enclosure are not restricted.

We recommend the Reader Expander is installed in a location that will facilitate easy access for wiring. We also recommend that the Reader Expander is installed in electrical rooms, communication equipment rooms, closets or in an accessible area of the ceiling.

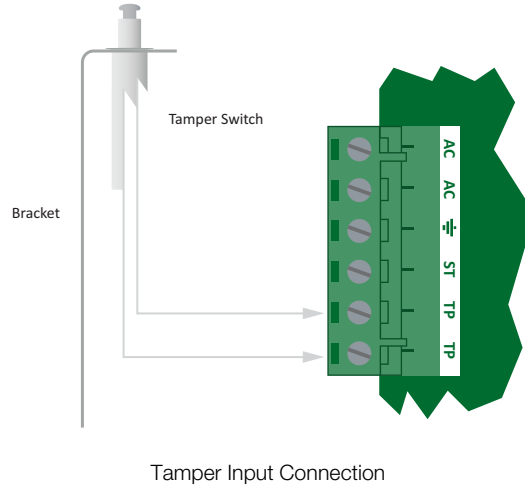
1. Insert the plastic stand-offs in to the locations to mount the PCB board.
2. Calculate the location and position of the enclosure and mark the holes for the keyhole points in the top left and right locations. This will allow you to screw in the screws and then hang the box on them adjusting the location to suit.
3. Ensure a solid fixing point and screw in the two screws. Before tightening the top screws insert the tamper bracket in the slot provided on the right side of the enclosure.
4. Fix the enclosure securely using the remaining mounting holes on the bottom left, right and centre of the enclosure.
5. Insert the PCB in to the enclosure and mount using the plastic standoffs inserted during step one.



Install the enclosure when the circuit board is NOT installed on the plastic stand-offs. This will reduce the risk of damage caused by debris during the installation process.

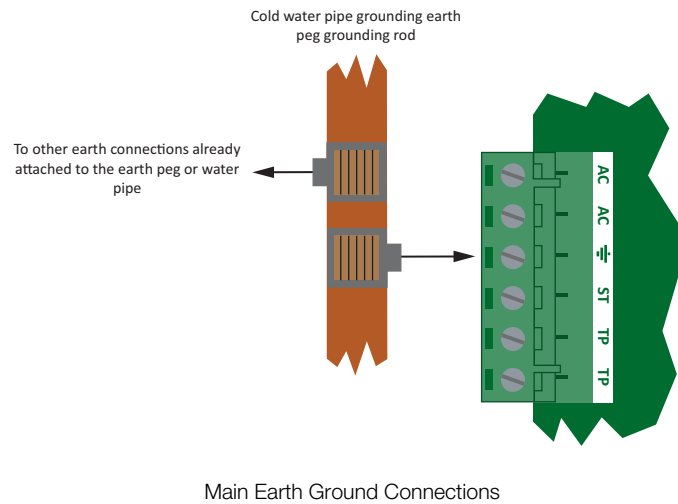
2.3 Cabinet Tamper Switch

The enclosure tamper input signals to the monitoring station or remote computer that the Reader Expander enclosure has been opened. The tamper input switch shall be mounted into the steel bracket provided and connected to the tamper connection terminals as shown in the diagram below. The tamper input opens and closes trouble zone RDxxx:01 on the Reader Expander.



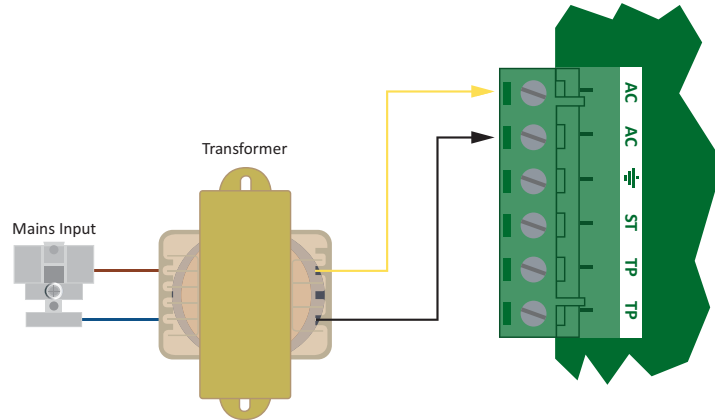
2.4 Earth Ground Connection

The Reader Expander has a connection for earth ground. For best results a cold water pipe should be used with a pipe wiring clamp. If a cold water pipe is not available, connect to a suitable ground connection in the installation. A minimum 14AWG solid copper wire shall be used from the Reader Expander's earth connection point to the clamp on the cold water pipe. If other earth clamps are present at the same connection point connect the clamp below the existing units.



2.5 AC Power

The Protege PGM Expander should be supplied by a dedicated electrical power source rated for a minimum 10Amp Load and have a dedicated circuit breaker. Do not use a switch controlled breaker or a switched electrical point to supply electrical power. Connect the primary of a 16.5VAC, 50/60Hz, 40VA Transformer to the electrical circuit and run the secondary to the AC input on the controller terminals.



AC Transformer 16VAC, 50/60Hz, 40VA MAX

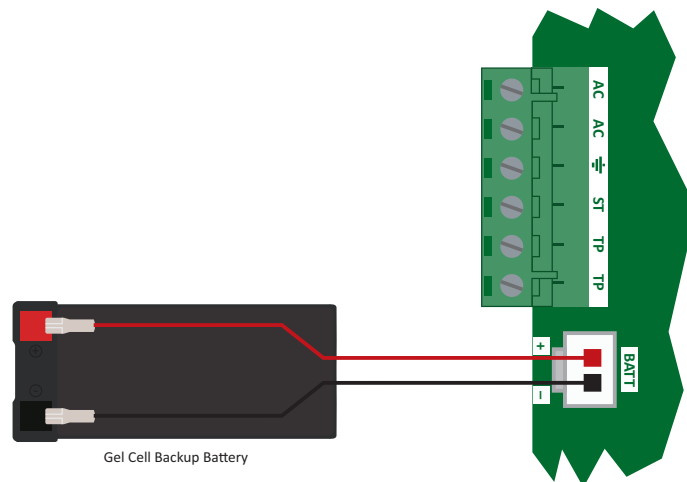
Specific regional regulations may allow the transformer to be mounted inside the enclosure. In this case wire the electrical circuit to the electrical termination point inside the enclosure and the secondary wires of the transformer to the AC Input on the controller.



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

2.6 Backup Battery

It is recommended that a minimum of a 4Ah 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- terminals. Connect the spade terminals to the battery as shown below. Connection of the battery in reverse will not damage the Reader Expander but will cause the battery fuse (5A Fast Blow) to blow and require replacement.



Battery Connection

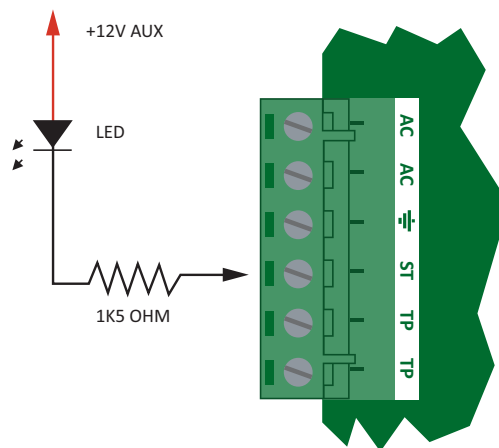
The battery test procedure uses a special algorithm to prevent deep discharge and increase battery endurance. A dynamic battery test is performed every ten minutes when AC power is present and a battery condition alarm will be generated if the battery is either disconnected or shows poor capacity. Battery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

If AC is not present the Protege Reader Expander will monitor the battery for a low voltage level and will activate the battery trouble zone. The next dynamic battery test will occur 30 minutes after AC power has been restored. This delay allows the battery to achieve optimal charging during the first 30 minutes when power is initially restored to the unit. Once the first test is completed the dynamic battery testing will return to 10 minute intervals.

When power is first applied to the Protege Reader Expander a dynamic battery test will be performed after 30 seconds, this allows the status and condition of the battery to be detected. On completion of this first test the normal testing period of 10 minutes will be resumed.

2.7 Status Indicator

The status output will activate according to the status indicator on the Protege Reader Expander and can be used to provide signalling or indication of the Reader Expander status outside the enclosure. The following diagram shows the connection of an LED indicator to the status output.



External Status LED Connection

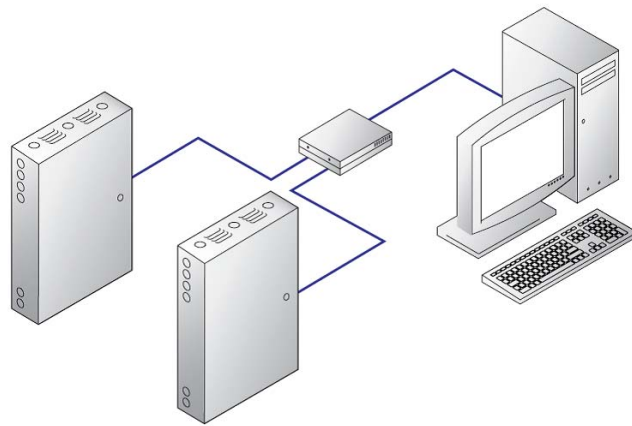
2.8 Ethernet 10/100 Network Connection

The communication between the PRT-RDE2 and the Protege System Controller can be via a 10/100 Ethernet network operating the encrypted UDP protocol suite. The IP address of the controller can be configured using the LCD Keypad Terminal or web interface. The default IP address for the PRT-RDE2 is set to a static IP address of 192.168.1.3 with a subnet mask of 255.255.255.0, and the default controller IP address the PRT-RDE2 will try to communicate on is 192.168.1.2.



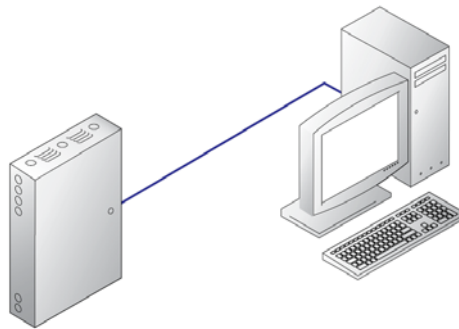
Installing the Protege Reader Expander on an active network requires knowledge of the configuration and structure for the network. Always consult the network or system administrator and ask them to provide you with a fixed IP address that can be assigned to the Protege Reader Expander.

When installing an Ethernet connection, the Protege Reader Expander 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

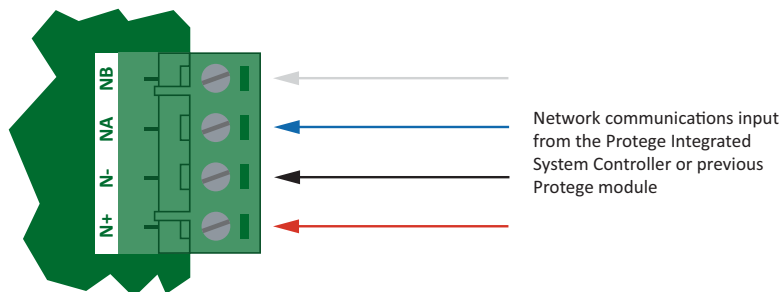
Temporary direct connections can be used for onsite programming by using a standard Ethernet crossover cable.



Ethernet 10/100 Direct Connection

2.9 Encrypted Module Network

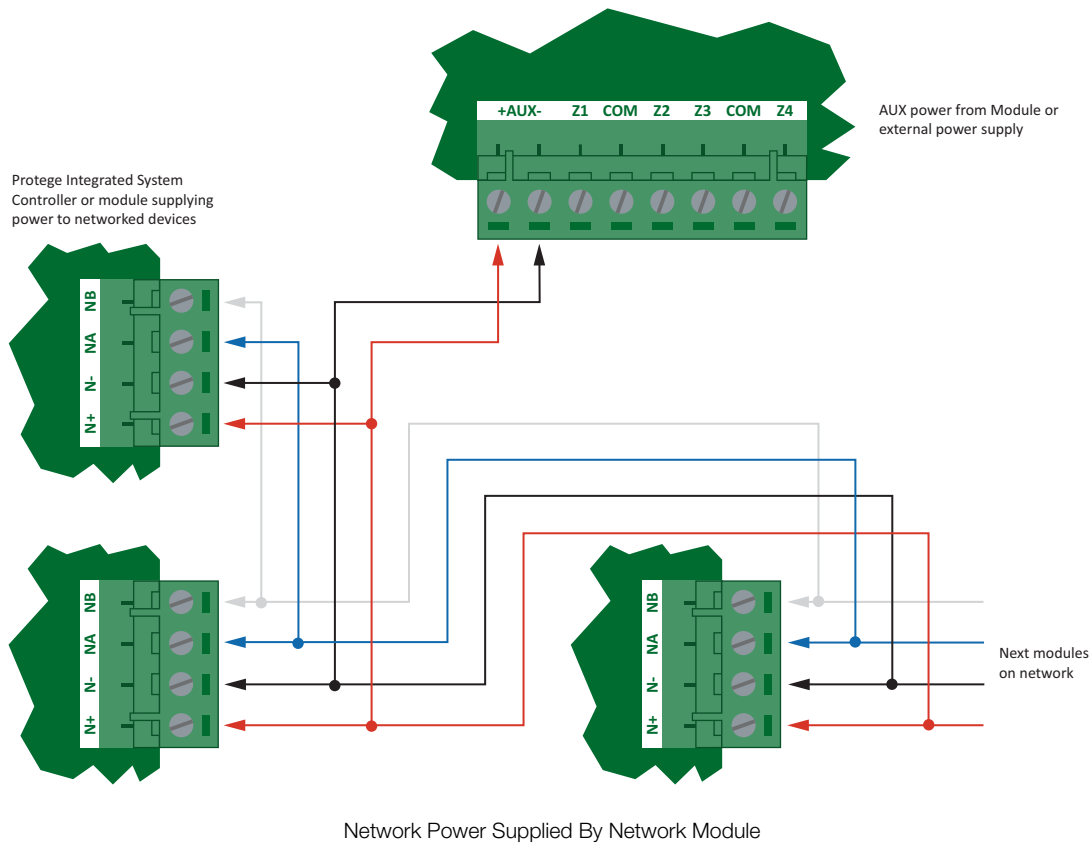
The Protege Reader Expander incorporates encrypted RS-485 communications technology. The isolated communications interface offers full galvanic isolation to prevent ground loop noise and cross phase ground differential between network devices.



Standard Communication Connection

Connection of the communications should be performed according to the diagram shown above. It is important that the N+ Network Communications Power be supplied from an independent battery backed power supply unit or a networked module capable of supplying the required voltage to all devices on the RS485 network.

Always connect the Reader Expanders NA and NB terminals to the NA and NB terminals of the communication network. The N+ and N- must go to a 12V power supply source as shown in the following diagram and connected at ONLY one +12V power source.



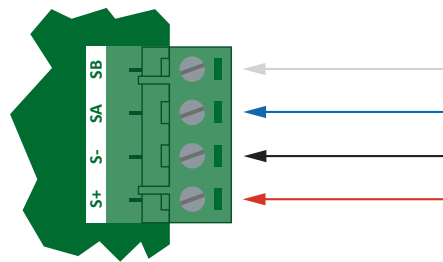
Warning: The 12V N+ and N- Communication input must be supplied from only ONE point. Connections from more than one 12V supply may cause failure or damage to the Reader Expander or device supplying network power.

i The EOL (End Of Line) jumper setting MUST be set in the ON position for the LAST module on the RS485 network. EOL is ON when the jumper is closest to the EOL text.

2.10 Slave Device Network

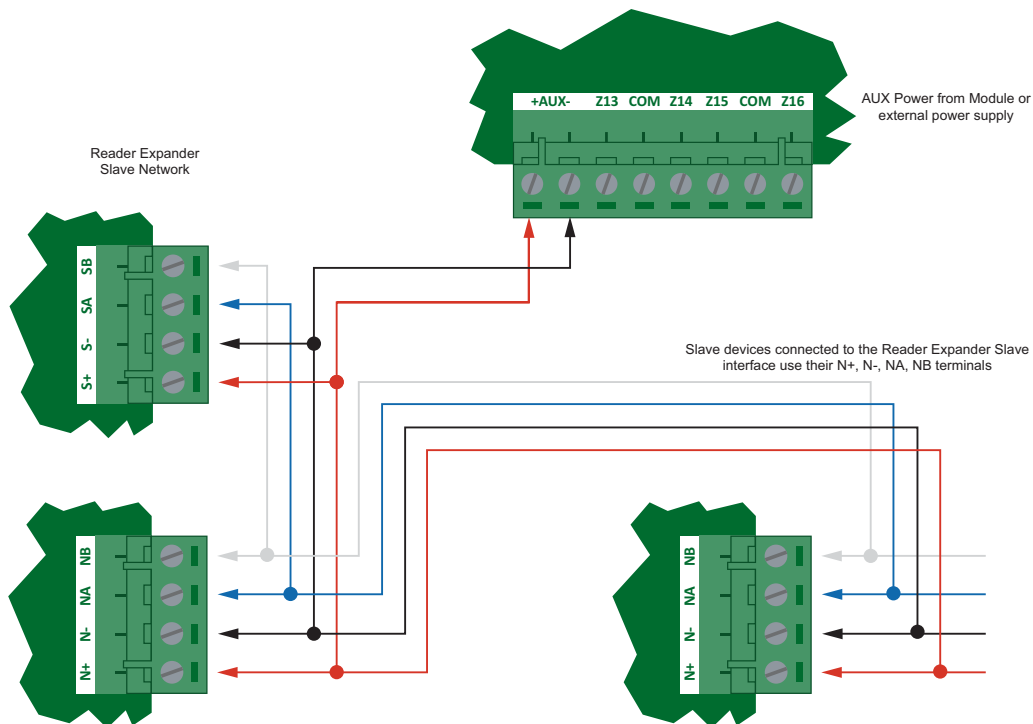
The Protege Reader Expander incorporates a secondary encrypted RS-485 communication interface that can be used to expand the functionality of the Reader Expander for the purpose of High Rise Elevator Control. A floor control module PRT-PX16 Protege 16 PGM Expander, set as a floor control device, is attached to the slave communication interface.

Connection of the communications shall be performed according to the following diagram. It is important that the S+ Slave Communications Power be supplied from an independent battery backed power supply unit or a module connected to the slave communication interface capable of supplying the required voltage to all devices on the slave RS485 network.



Slave Communications Connection

Always connect the Reader Expanders SA and SB terminals to the SA and SB terminals of the slave devices. The S+ and S- must go to a 12V power supply source as shown in the following diagram.



Slave Power Supplied by Module

The above diagram shows a power connection taken from the auxiliary power outputs on the Reader Expander's zone terminals. This connection is suitable for smaller systems provided that the:

- Maximum total output current,
- AUX DC output current,
- B1/B2 DC output current, and
- Total combined current

are ALL lower or equal to the values outlined in the Technical Specifications section. If these currents are exceeded, a separate power supply shall be used.



If an external power supply is required, a UL 603 or UL 294 listed power-limited power supply must be used to comply with UL installation standards, and a CAN/ULC-S318 or CAN/ULC-S319 listed power-limited power supply must be used to comply with ULC installation standards.



Warning: The 12V S+ and S- Communication input must be supplied from only ONE point. Connections from more than one 12V supply may cause failure or damage to the Reader Expander or device supplying slave communication power.

The recommended module network wiring specifications are:

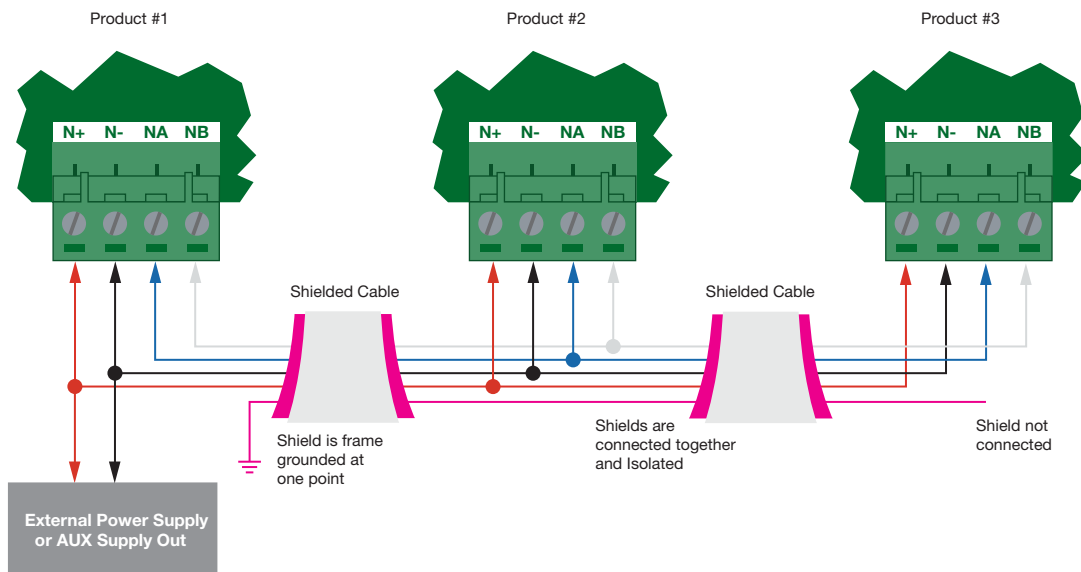
- CAT5e / CAT6 are also supported for data transmission when using ground in the same cable.
- 24AWG twisted pair with characteristic impedance of 120ohm
- Belden 9842 or equivalent.
- Maximum total length of cable is max 900m (3000ft)



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

Shielded Cables

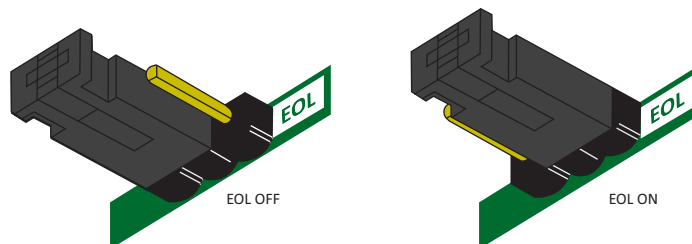
- Shielded cables can be used in noisy environments (with RF and electromagnetic interference).
- If a shielded cable is used, the shield must be connected at only one end of the cable. DO NOT connect a shield at both ends. Refer to the following diagram for the recommended shield connection.



Recommended Shield Connection



The EOL (End Of Line) jumper setting MUST be set in the ON position for the LAST slave module on the RS485 network. EOL is ON when the jumper is closest to the EOL text.



EOL Jumper

2.11 RS-485 Biasing Settings

The Protege Reader Expander has biasing settings for the module network. Biasing can be configured for either high or low (L indicates a low bias and H indicates high bias configuration). Both jumpers **MUST** be set to the same bias type.



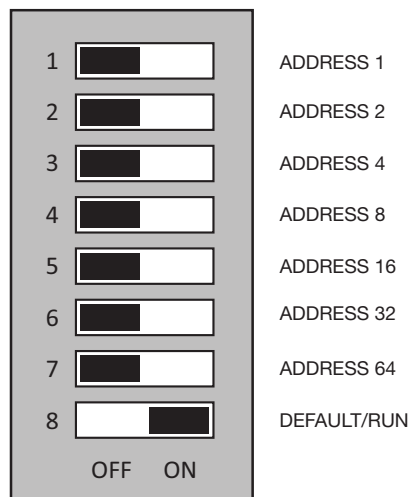
- Biasing shall only be set to LOW on ONE point on any single segment of the RS-485 network. All other devices on the same segment shall be set to the middle position which is no biasing.
- By default, the PRT-CTRL System Controller has the jumpers for the biasing set to low and the EOL jumper on. This is also the same default configuration for the slave communication port on the PRT-RDI2 Protege Intelligent Reader Expander.

3 Communication Setup

Before the Protege Reader Expander can communicate with the Protege System Controller the communications need to be setup. These settings are available from either a web interface or by using a Protege LCD Keypad. To program the reader expander using the web interface the IP address must be known.

3.1 Keypad Programming

To setup the basic communication parameters for the Protege Ethernet Reader Expander using a Protege LCD Keypad (PRT-KLCD) power the Reader Expander up with DIP Switch 8 turned on as shown below.



DIP Switch Setting for Keypad Configuration

Connect a PRT-KLCD module to the primary RS-485 port (NA and NB) that has a module address of 200 or greater. Make sure there are no other modules attached to this network, as in this mode the Reader Expander will simulate a Protege System Controller when in this programming mode.

Once the Keypad has registered with the Reader Expander the following screen will be displayed.

Network Mode

The network mode defines what communication method the Protege Reader Expander will use to communicate with the Protege System Controller. When Ethernet is selected the primary RS-485 port can be used as a network repeater and all received Protege communication will be sent to the System Controller of the Ethernet link.

Network Mode
Ethernet

Use the [1] and [3] keys to scroll the network mode selection and press [ENTER] to select the mode displayed.

Controller Connection

The controller connection defines how the reader expander finds the Protege System Controller on the network. This can be done either dynamically where the reader expander will find an available controller to connect to or statically. When connecting statically the Controller IP Address must be set (see below).

CTRL Connect
Static

Use the [1] and [3] keys to scroll the connection selection and press [ENTER] to select the connection displayed.



Do not use a dynamic controller connection when there is more than one controller on the network the reader expander is being connected to. You cannot guarantee which controller the reader expander will connect to.

DHCP Configuration

The Reader Expander can use DHCP to obtain an IP address. To use this feature select Enabled.

DHCP Usage
Disabled

Use the [1] and [3] keys to scroll the connection selection and press [ENTER] to select the connection displayed.

Network UDP Port

The Network UDP port defines the port the Reader Expander uses to connect to the Protege System Controller. This must be set the same as Protege System Controller.

Network UDP
port: 09450

Enter a network UDP port (00000 - 65535).

Module IP Address

The reader expander has a built in TCP/IP Ethernet Device and it must be programmed with a valid TCP/IP Address to allow it to connect to the system controller. By default the IP address is set to 192.168.1.2.

Programming an IP address requires knowledge of the network and subnet that the system controller will be connected to. ALWAYS consult the network or system administrator before programming these values.

IP Address
192.168.001.003

To modify the IP address use the decimal entry from (000 to 255), use the keypad as explained in section Entering Decimal Numbers in the Protege System Controller Reference Manual and press [ENTER].



When the Reader Expander is configured with DHCP enabled an IP address does not have to be entered. Once a DHCP address has been obtained it will be displayed. An IP address of 000.000.000.000 will be shown while the Reader Expander is trying to find a DHCP server.

Module IP Subnet Mask

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.

Programming an IP Netmask requires knowledge of the network and subnet that the system controller will be connected to. ALWAYS consult the network or system administrator before programming these values.

Subnet 255.255.255.000

To modify the subnet mask use the decimal entry from (000 to 255), use the keypad as explained in section Entering Decimal Numbers in the Protege System Controller Reference Manual and press [ENTER].

Module IP Gateway

In conjunction with the IP Address a gateway can be configured to allow access to a router for external communications beyond the subnet to which the reader expander is connected. By default this is set to a value of 0.0.0.0 to prevent any external communication.

Programming a, IP Gateway requires knowledge of the network and subnet that the system controller will be connected to. ALWAYS consult the network or system administrator before programming these values.

Gateway 000.000.000.000
--

To modify the IP gateway use the decimal entry from (000 to 255), use the keypad as explained in section Entering Decimal Numbers in the Protege System Controller Reference Manual and press [ENTER].

Controller IP Address

If the reader expander has been configured to connect to the Protege System Controller using a static IP address then this IP address of the Controller must be entered in this field. If a dynamic connection is being used the controller's IP address can be confirmed by viewing this field.

Controller IP 192.168.001.002
--

To modify the IP address use the decimal entry from (000 to 255), use the keypad as explained in section Entering Decimal Numbers in the Protege System Controller Reference Manual and press [ENTER].

3.2 Web Programming

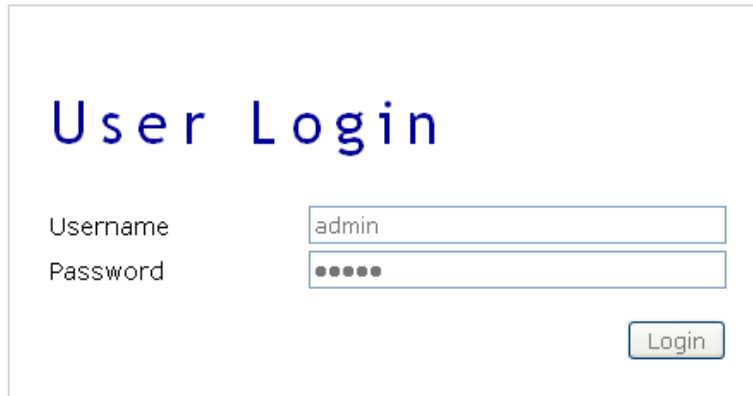
The Protege Reader Expander can be programmed using an internal web interface. To access this, open a web browser (such as Internet Explorer or Firefox) and type the IP address of the module into the address bar.



When attempting to view the webpage of the Reader Expander from a network that uses a Proxy Server, ensure the browsers connections options recognise local addresses.

User Login

To access to the reader expander programming you must login. By default the username is **admin** and the password **admin**. For maximum security, modify the password before completion of the installation.



User Login

Username

Password

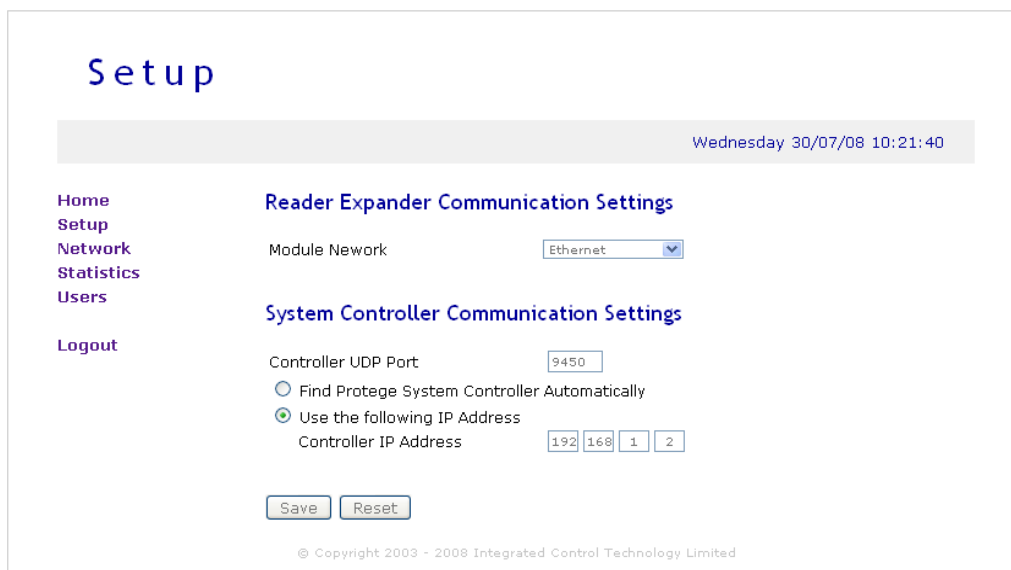
Login

Web Programming User Login Page

Setup

Once logged in the main page (index.php) will be displayed. Click the **Setup** link on the menu on the left to navigate to the setup page (setup.php).

All the options that are available through the keypad can be modified through the web page. Enter the details as appropriate.



Setup

Wednesday 30/07/08 10:21:40

Home
Setup
Network
Statistics
Users
Logout

Reader Expander Communication Settings

Module Network

System Controller Communication Settings

Controller UDP Port

Find Protege System Controller Automatically

Use the following IP Address

Controller IP Address

Save Reset

© Copyright 2003 - 2008 Integrated Control Technology Limited

Protege Reader Expander Basic Setup

Network Setup

The IP address, Subnet Mask and Gateway settings can also be programmed through the web pages. Click the **Network** link on the menu on the left to access this programming.

The reader expander will need to be restarted for any of these changes to take place.

Statistics

The statistics web page displays the reader expander's serial number and firmware versions.

Users

To restrict access to the reader expander it is recommended to change the password of the default user.

Select the checkbox of the user to be modified and click the **Edit** button as shown below. Up to two users can be programmed.



Once setup is complete turn DIP switch 8 off before restarting Reader Expander.

User Management

Wednesday 30/07/08 10:48:01

	User Name	Password
<input checked="" type="checkbox"/>	admin	admin
<input type="checkbox"/>		

[Edit](#)

© Copyright 2003 - 2008 Integrated Control Technology Limited

- Home
- Setup
- Network
- Statistics
- Users
- Logout

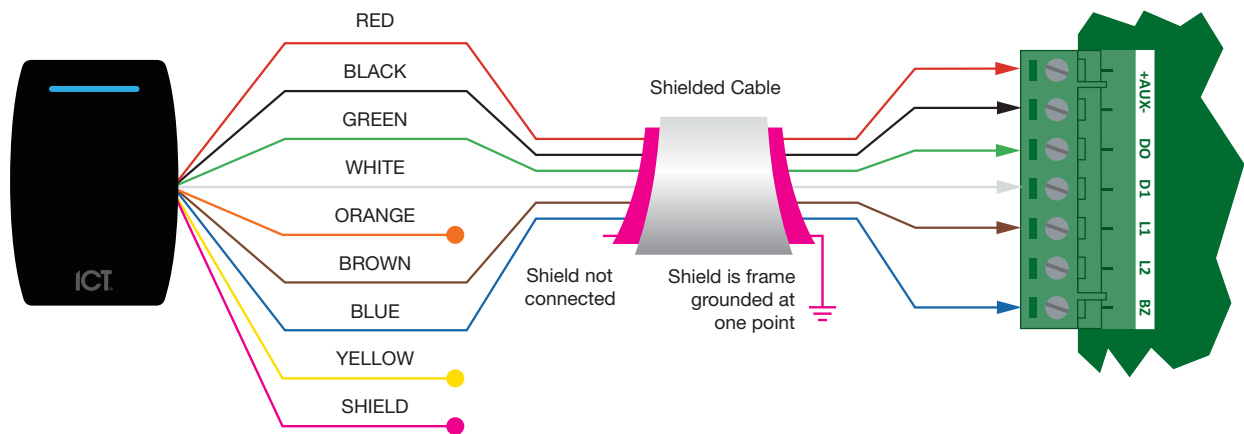
Web page User Programming

4 Door Access Control

The Reader Expander allows the control of two separate access controlled doors used for entry or exit only, and a single access controlled door using entry/exit.

4.1 Reader Connection

The Protege Reader Expander allows the connection of 2 reading devices or 4 Wiegand reading devices and the ability to control 2 doors (Entry or Exit Only) or 1 door (Entry and Exit). The following diagram shows the connection of standard Wiegand Reader with the Protege Reader Expander controlling an Access Door and Entry/Exit Door.



Standard Card Reader Connection

The card reader must be connected to the Controller port using a shielded cable. Always refer to the card reader manufacturer for detailed installation guidelines. The shield connection must only be connected at one end of the cable in the metallic enclosure (frame grounded). The beeper output on the Controller provides diagnostic information to the end user and installer when access is denied or the unit is operating offline.

Warning:



- Do not connect the shield to a AUX- or 0V connection.
- Do not join the shield and black wires at the reading device.
- Do not connect the shield to any shield used for isolated communication.

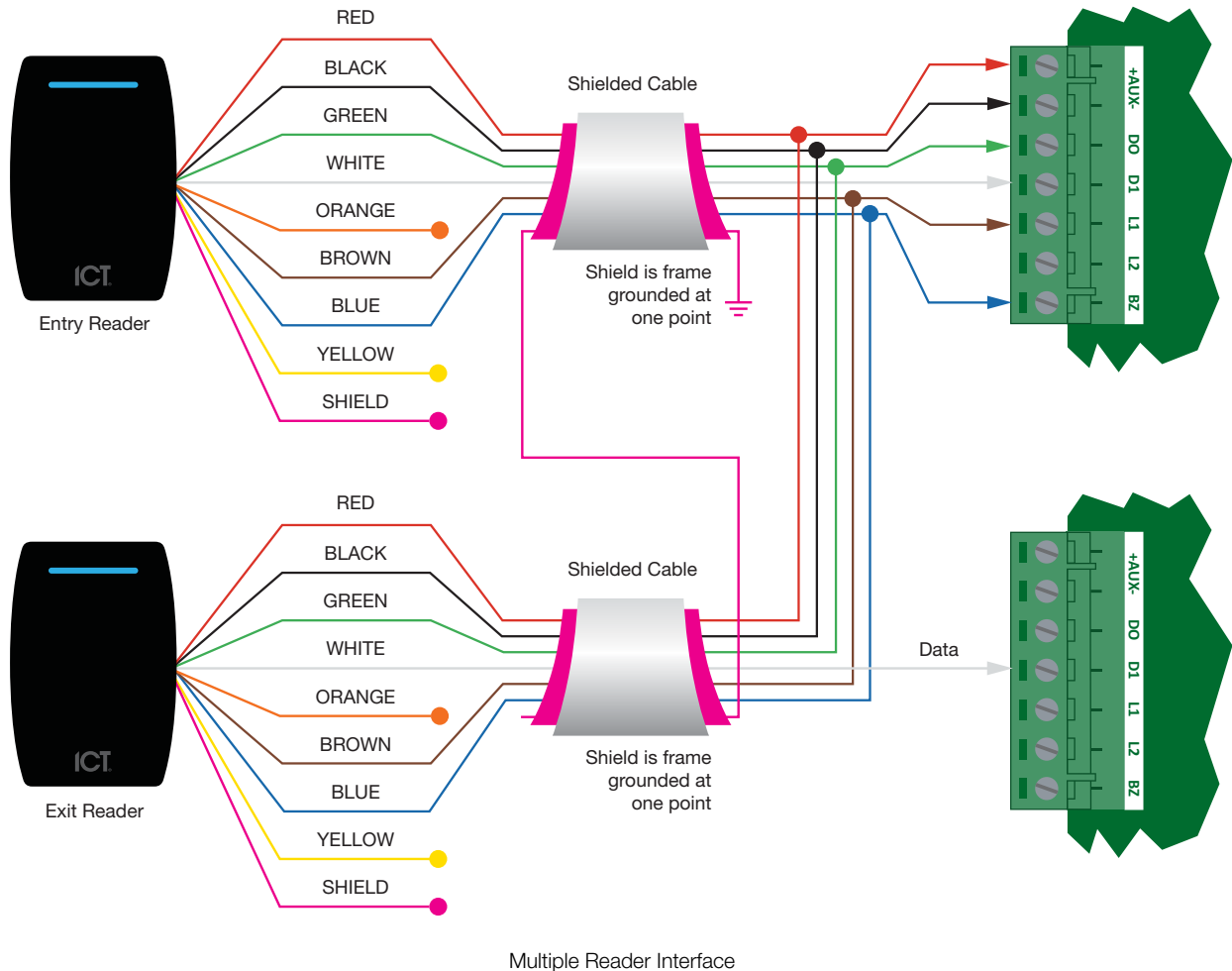


Compatible access control card reader communication formats are: 26-, 34-, 37-Bit Wiegand, RS-232, RS-485, and Smart RS-485.

4.2 Multiple Wiegand Reader Connection

When operating the reader expander in multiple reader mode the Protege Reader Expander allows the connection of 4 wiegand reading devices controlling two doors each with Entry/Exit readers.

When connecting Wiegand readers in multiple reader mode the secondary reader that is connected will have all connections wired to the same port as the primary card reader with the DATA 1 connection wired to the opposite reader connection DATA 1 input.



The card reader must be connected to the reader port using a shielded cable. Always refer to the card reader manufacturer for detailed installation guidelines. The shield connection must only be connected at one end of the cable in the metallic enclosure(frame grounded). The reader that is multiplexed in to the alternate reader port will operate as the exit reader and the normal reader connection shall be programmed to operate as the Entry Reader.

Warning:



- Do not connect the shield to a AUX- or 0V connection.
- Do not join the shield and black wires at the reading device.
- Do not connect the shield to any shield used for isolated communication.

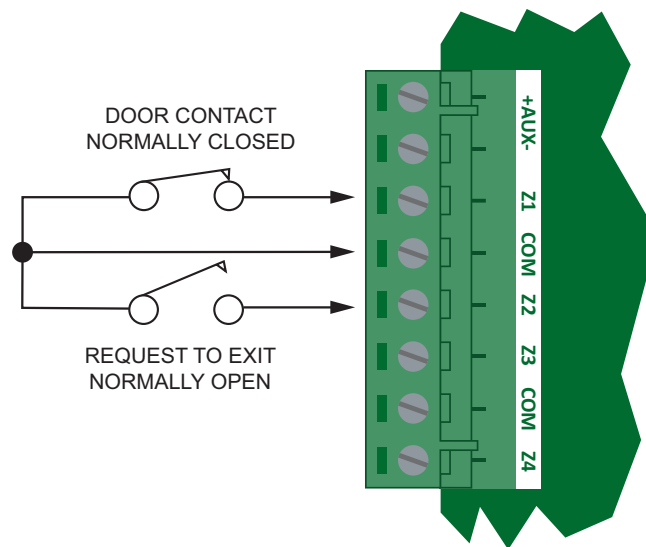
4.3 Magnetic Reader Connection

The Protege Reader Expander 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 (Bank Identification Number) for ATM access control, Full 16 Character decoding, and a range of first 4, 5 and 6 card number encoding.

For information on the use of magnetic readers please refer to Application Note AN 009 Connecting Magnetic Card Readers available at www.incontrol.co.nz.

4.4 Door Contact Connection

The Reader Expander allows the connection of up to 4 contacts for monitoring and controlling access control doors. Each zone on the Reader Expander can be used for the door function that is automatically assigned and as a normal zone 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.



Standard Door Contact Inputs



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.

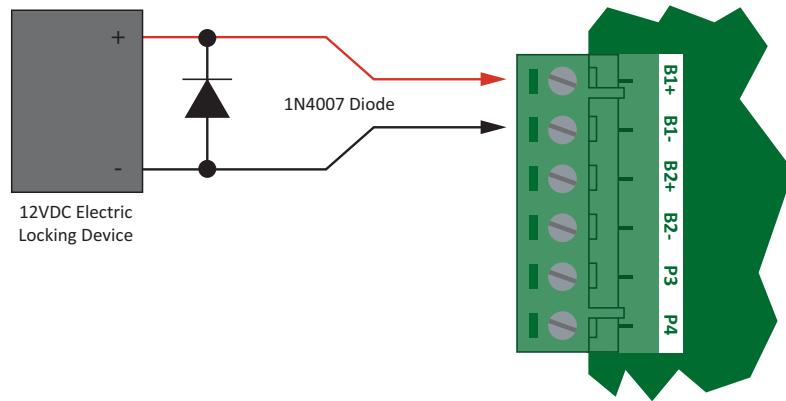


REX and REN devices must be listed to UL 294 for UL installations and CAN/ULC-S319 for ULC installations, and be compatible with the system.

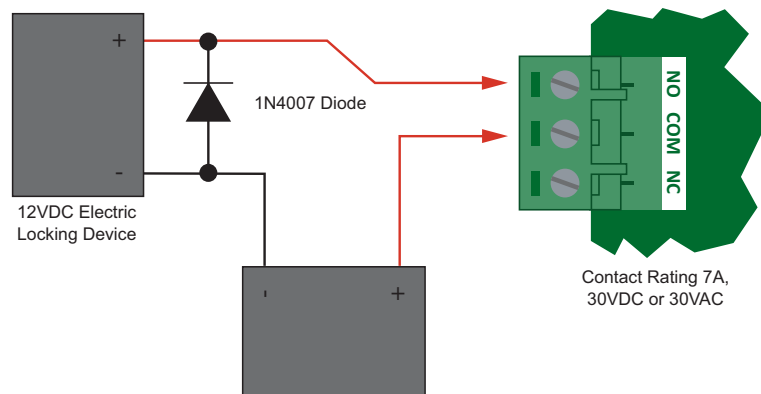
4.5 Door Lock Connection

The Protege Reader Expander provides a connection for 2 electric strike locks with full monitoring of the lock circuit for tamper and over current/fuse blown conditions. The door lock monitoring can be disabled if it is not required. For information on the LOCK control status, refer to the Indication section on page .

For locking devices that have different voltage or current requirements than is available at the L1+/- or L2+/- terminals, a FORM C relay contact is also provided, with the RELAY 1 contacts operating in parallel with L1 output and the RELAY 2 contacts operating in parallel with the L2 output.



Door Lock Powered Outputs



Door Lock Relay Outputs



- When using a door with an entry and exit reader, the LOCK output shall be connected to LOCK 1, and enable the swap lock option for the second reader input to allow the reader LED's to display the correct status.
- The 1N4007 diode (as shown in the above diagrams) is supplied with the Protege Reader Expander and MUST be installed at the electric strike terminals.



Class 1 wiring is required for NO relay circuit connection of 8-10A

5 Zone Inputs

The Protege Reader Expander has 8 Zone Inputs. The reader expander also monitors 16 trouble zones used to report trouble conditions. A trouble zone is in most cases not physically connected with a device, rather it is related within the system. For example, a module communication fault causes a trouble zone to open as a result of the communication failure.

5.1 Zone Inputs - Reader

The Protege Reader Expander can monitor the state of up to 8 zone inputs such as magnetic contacts, motion detectors and temperature sensors. Devices connected to these zones can be installed to a maximum distance of 300m (1000ft) from the Controller when using 22 AWG. The Controller supports normally opened and normally closed configurations with or without EOL resistors on a per zone configuration setting.

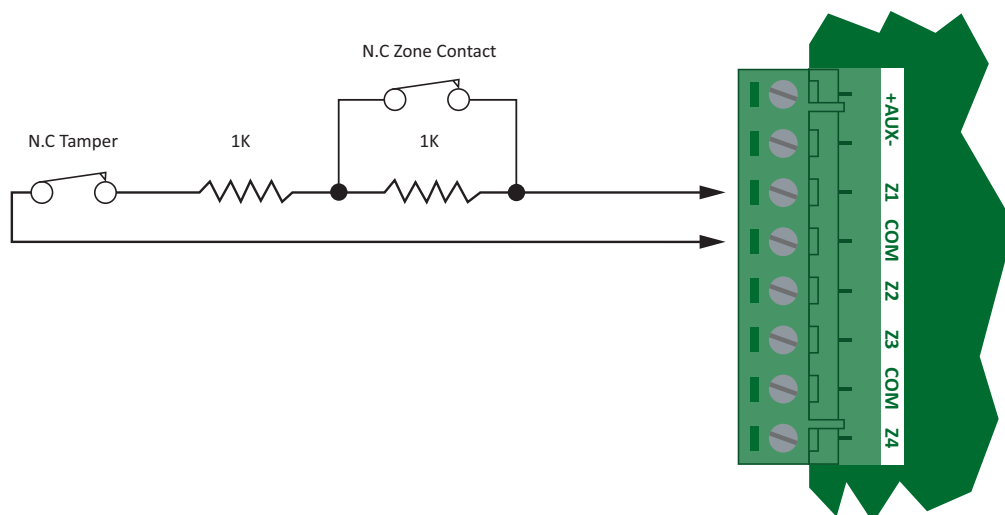


- Magnetic contacts shall be listed to UL 634 to comply with UL installation standards and ULC/ORD-C634 to comply with ULC installation standards.
- Motion detectors and temperature sensors shall be listed to UL 639 to comply with UL installation standards and ULC-S306 to comply with ULC installation standards.
- The PRT-RDI2-PCB has been evaluated for UL 294 and CAN/ULC-S319 standalone access control.

Zones can be programmed from the Protege LCD Keypad (PRT-KLCD) or using the Protege System Management Suite (PRT-SMGT). RD001:01 to RD001:08 represent Zone 1 to Zone 8 on the Protege Reader Expander (Substitute the module address for the appropriate address being programmed).

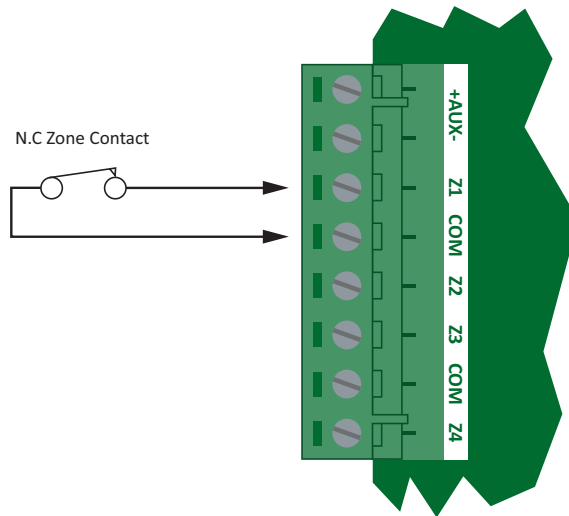
When using a zone with the EOL resistor configuration, the controller generates an alarm condition when the state of a zone changes and generates a tamper alarm condition when a wire fault (short circuit) or a cut wire (tampered) in the line occurs.

When using the EOL resistor configuration, the EOL resistor option must be turned on for the zone(s) so that the tamper and short states can be monitored (refer to Zones Section in the Protege Reference Manual).



EOL Resistor Zone Configuration

Each zone input can use a different input configuration. To program a large number of zones, with a single configuration type, use the Multiple Selection feature in the Protege System Management Suite application. 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.



Normally Closed Zone Configuration No Resistors

5.2 Trouble Zone Inputs

Each reader expander can monitor up to 16 trouble zones. Trouble zones are used to monitor the status of the reader expander and in most cases are not physically connected to an external zone. For example, trouble zone RD001:06 is used to monitor door 1 for a forced open condition and will generate an alarm state if the door is forced.

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

Zone Number	Description	Type	Group
RDxxx:01	Module Tamper	System Tamper	System
RDxxx:02	AC failure	Power Fault	General
RDxxx:03	Low Battery	Power Fault	General
RDxxx:04	Aux Failure	Power Fault	General
RDxxx:05	Lock Failure	Power Fault	General
RDxxx:06	Door 1 Forced	Forced Door	Access
RDxxx:07	Door 2 Forced	Forced Door	Access
RDxxx:08	Door 1 Left Open	Left Open	Access
RDxxx:09	Door 2 Left Open	Left Open	Access
RDxxx:10	Reader 1 Voltage	Power Fault	General
RDxxx:11	Reader 2 Voltage	Power Fault	General
RDxxx:12	Reader 1 Tamper	System Tamper	System
RDxxx:13	Reader 2 Tamper	System Tamper	System
RDxxx:14	Door 1 Lockout	Attempts	Access
RDxxx:15	Door 2 Lockout	Attempts	Access
RDxxx:16	Module Offline	Module Offline	System

Replace 'xxx' with the appropriate address of the Reader Expander that you are programming.

6 Programmable Outputs

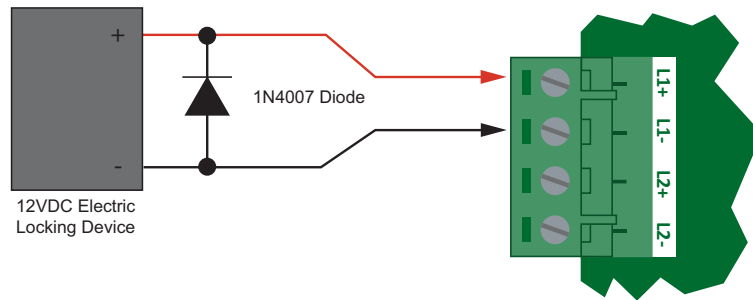
The Protege Reader Expander has 4 Programmable Outputs (PGMs). The PGMs are used to activate the Electric Door Locks, Sirens, Lighting Control and Relay Accessory Products.

6.1 Lock PGM Outputs (1 and 2)

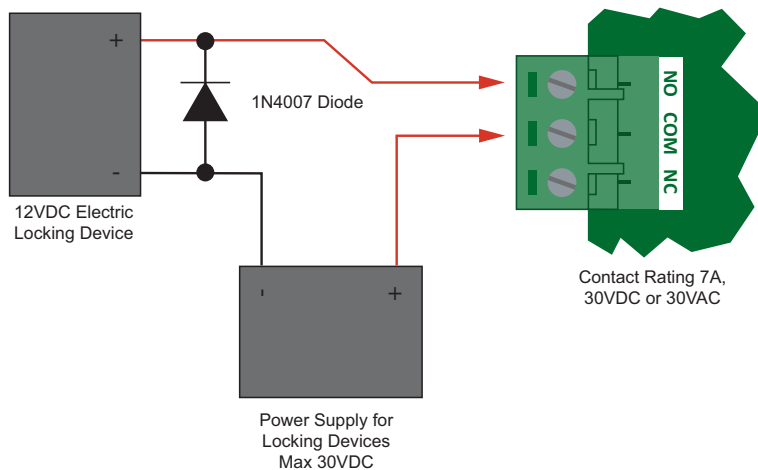
The + and - terminals of Lock 1 (PGM1 RD001:01) and Lock 2 (PGM2 RD001:02) are used to power electric door strikes and other lock control devices that require a steady voltage output. The lock outputs supply 12Vdc upon an unlock or activation and support up to 1000mA (1A) inrush and 700mA continuous operation. The lock output uses an electronically fused circuit and automatically shuts down if the current exceeds 1.1A.

If the load on the lock terminals returns to normal ($\leq 1A$), the reader expander will reinstate power to the lock terminals if they are activated.

For locking devices that have different voltage or current requirements than is available at the L1+/- or L2+/- terminals, a FORM C relay contact is also provided, with the RELAY 1 contacts operating in parallel with Lock 1 (PGM1 RD001:01) output and the RELAY 2 contacts operating in parallel with the Lock 2 (PGM2 RD001:02) output.



Lock Output PGM1/2 Connection (PGM 1 Shown)



Lock Output PGM1/2 Relay Outputs

When the lock output is not used, the appropriate trouble zone will be activated (refer to the Trouble Zone Input section). To avoid this, connect a 1k Ω resistor across the lock output. If the Lock is not being used for another function, and the trouble zone is not programmed in the system, no resistor is required.

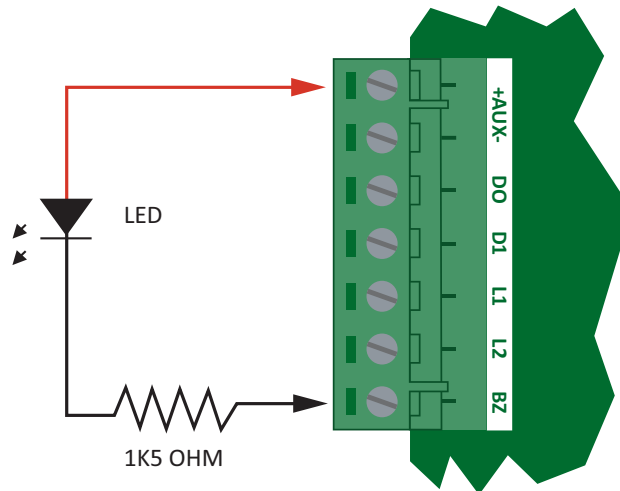
6.2 Standard PGM Outputs (3 to 8)

The PGM outputs 3, 4, 5, 6, 7 and 8 on the Protege Reader Expander are open collector outputs and switch to a ground connection.

The PGMs have a default pre-programmed function as detailed in the following table and are used to control the indicator and audible outputs on the attached reading device. These functions may be disabled by programming the appropriate setting in the reader expander configuration.

PGM Number	Description
RDxxx:03	LED 1 (Green) Reader 1
RDxxx:04	LED 2 (Red) Reader 1
RDxxx:05	BEEPER Reader 1
RDxxx:06	LED 1 (Green) Reader 2
RDxxx:07	LED 2 (Red) Reader 2
RDxxx:08	BEEPER Reader 2

Replace 'xxx' with the appropriate address of the Reader Expander that you are programming.



Example Open Collector Output Connection (LED)



The PGM outputs 3 to 8 can switch to a maximum capacity of 50mA each, exceeding this amount will damage the PGM output.

6.3 PGM Beeper Outputs Special Functions (5 and 8)

The PGM beeper outputs 5 and 8 on the provide special diagnostic information when a card is presented. The following table shows the beeper modes of operation.

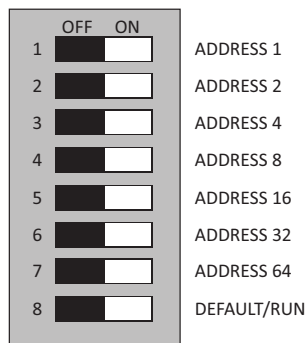
Function	Description
2 Beeps	Access Granted. The lock will activate and allow access to the door the card has been presented.
4 Beeps	Offline Access Granted. This is generated ONLY if the is operating offline and the mode of offline operation allows access.
1 Long Beep	Offline Access Denied. This is generated ONLY if the is operating offline and the mode of offline operation prevents this card from being allowed access.
1 Long Beep 1 Short Beep	Access Denied Card Number Not Known. The card number is not known in the system. The card that has been presented to the reader could not be matched to a valid user in the system.
1 Long Beep 2 Short Beeps	Access Denied Door Group. The user is denied access because they do not have access to the door. This error will also be generated if the door group is not set or the door group schedule is not valid.
1 Long Beep 3 Short Beeps	Access Denied Area Group. The user is denied access because they do not have access to the area that is being controlled by the door. If the area that the door is associated with is armed, and the user does not have this area in their area disarm group, they will be denied access. This also depends on the area group settings for the door.
1 Long Beep 4 Short Beeps	Access Denied Access Level. The user is denied access because they do not have a valid access level or the access level they are assigned is currently outside the programmed schedule.

7 Configuration Switch

The addressing of the Reader Expander allows up to 128 devices to be connected to the system controller. The 'CONFIG' configuration DIP switch allows each Reader Expander to have a unique address.

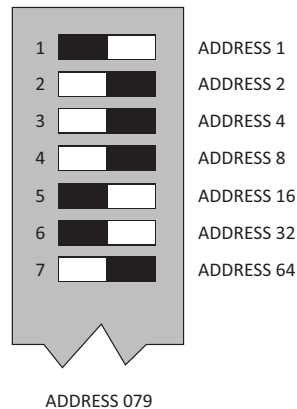
7.1 Address Configuration

The switch positions 1 to 7 select the device address from 1 to 128. When setting an address the Reader Expander must be powered down (Battery and AC) and restarted for the new address to take affect. When changing the address the Reader Expander will automatically default the internal configuration and require a network update. See the Protege System Reference Manual for information on performing a module update.



Reader Expander CONFIG Switch Functions

The device address is determined by adding the value of each switch that is selected in the ON position and then adding 1 to this value. In the example below the address 079 results in $(64+8+4+2) + 1 = 079$. Setting all address switches to OFF results in the default address of 001.



Reader Expander Configured For Address 079

8 Status Indication

The Reader Expander includes 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.

8.1 Status Indicator

The Status Indicator is located in the centre of the PCB and indicates the status of the Protege Reader Expander. If the Protege Reader Expander is operating normally the LED will indicate this by **FLASHING** at 1 second intervals. **FLASHING** rapidly at 250ms intervals indicates that the Reader Expander is attempting to register with the system controller, or that communication has failed and the Reader Expander is retrying the request.



When the fault indicator is ON the status indicator will show an error code. Refer to the section on Error Code Display for more information.

8.2 Fault Indicator

The fault indicator LED is identified by the text 'FAULT' and is located in the centre of the PCB. When the fault indicator is **FLASHING** the Reader Expander is operating in firmware update mode, or there is no firmware loaded. The fault indicator when **ON** indicates that an error has occurred while trying to register with the system controller. The status indicator will flash a number of times indicating an error code. Refer to the section on Error Code Display for more information.

8.3 Charge/Test Indicator

The charge and test indicator serves two functions; it will indicate that a Battery Test is in progress, and that Battery Charging is being performed. When AC is present the battery charging current will be indicated by a varying intensity level on this indicator. This indicator will be **ON** when a battery test is in progress by illuminating brightly for 30 seconds every 10 minutes.

This indicator is identified by the text **CHARGE/TEST**. This indicator does not function when AC is not present. For more information, refer to the section on Battery Backup.

8.4 Auxiliary OK Indicator

Auxiliary voltage is supplied to the AUX+ outputs through the auxiliary fuse. If auxiliary supply is normal the the **AUX OK** indicator will be illuminated. If the auxiliary fuse is damaged, the indicator will be off.

8.5 AC OK Indicator

When a valid AC input is provided, the **AC OK** indicator will illuminate. When the AC is disconnected or has failed, the indicator will be off.

8.6 5V Isolated Power Indicator

The Reader Expander communicates using an isolated RS-485 interface for optimal performance and this requires an isolated supply on the N+ and N- terminals. When a valid power supply is available the '5V ISO' indicator will be **ON** for the interface. The '5V ISO' indication is located at the top of the network isolated interface.

8.7 Lock 1/Lock 2 Indicators

The Lock 1 and Lock 2 indicators will show the status of the Lock Output and the over current or circuit fault conditions.

ON Lock is **ON**.

TWO FLASHES Lock is **ON**, the circuit is in Over Current Protection or the fuse has blown.

THREE FLASHES Lock is **OFF**, the circuit to the locking device is cut, damaged or tampered.

8.8 Network RX/TX Indicator

The Network Receive and Transmit Data indicators are located on the top right side of the PCB beside the network communication interface. The indicator shows when the Protege Reader Expander is transmitting and receiving information from the module communications interface and is identified by the text 'RX' and 'TX'. When the indicator is **ON** data is being transmitted or received.

8.9 R1 and R2 Power Indicator

The R1 and R2 power indicators are located beside the reader 1 and reader 2 connection terminals. Reader voltage is supplied to the R+ outputs through the reader fuse. If the reader supply is normal the indicator will be **ON**. If the indicator is **OFF** the reader fuse is damaged.

8.10 R1 and R2 Data Indicator

The R1 and R2 data indicators are located beside the reader 1 and reader 2 connection terminals. A short **FLASH** (<250 Milliseconds) on the Data Indicator will show that data was received but was not in the correct format. A long **FLASH** (>1 Second) indicates that the unit has read the data and the format was correct.

9 Error Code Indication

When the Reader Expander attempts to register or communicate with the system controller a registration error can be generated indicating that it was not successful.

9.1 Error Code Display

The following table is only valid if the FAULT indicator is **CONSTANTLY ON** and the STATUS indicator is **FLASHING RED**.

If the fault indicator is **FLASHING** the Reader Expander requires a firmware update or is currently in firmware update mode.

The status indicator will **FLASH RED** with the error code number. The error code number is shown with a 250ms **ON** and **OFF** period (duty cycle) with a delay of 1.5 seconds between each display cycle.

Flash	Error Description
1	Unknown Error Code The error code returned by the system controller could not be understood by the Reader Expander. Contact Integrated Control Technology.
2	Firmware Version The firmware version on the Reader Expander is not compatible with the system controller. To clear this error, update the module using the module update application.
3	Address Too High The Reader Expander address is above the maximum number available on the system controller. To clear this error change the address to one within the range set on the system controller, restart the Reader Expander by disconnecting the power.
4	Address In Use The Address is already in use by another Reader Expander. To clear this error set the address to one that is not currently occupied. Use the view network status command to list the attached devices, or the network update command to refresh the registered device list.
5	Controller Secured Registration Not Allowed Controller is not accepting any module registrations. To allow module registrations use the network secure command to change the secure setting to not secured.
6	Serial Number Fault The serial number in the device is not valid. Return the unit to the distributor for replacement.
7	Locked Device The Reader Expander or system controller is a locked device and cannot communicate on the network. Return the unit to the distributor for replacement.

10 Technical Specifications



The following specifications are important and vital to the correct operation of the PRT-RDI2-PCB Protege Intelligent Reader Expander. Failure to adhere to the specifications will result in any warranty or guarantee that was provided becoming null and void.

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

Power Supply	
AC Input Voltage	16VAC 50/60Hz @ 40VA (Max)
Operating Current	280mA (Typical)
DC Output (Auxiliary)	1.2A (Max)
Battery Charging	350mA/700mA
Battery Low	10.5VDC
Battery Restore	11.5VDC
Communication	
RS-485	Isolated Module Network
Outputs	
Lock Outputs	2 Outputs, 400mA (Max), 500mA Shutdown
PGM Outputs	6 (50mA Max) Open Collector
Status Output	50mA (Max) Open Collector
Inputs	
Zone	8 (500ms to 40sec Input Speed)
Tamper	1 (Normally Closed)
Trouble Zone	16
Dimensions	
PCB Dimensions	183mm X 234mm (7.2" X 9.2")
Enclosure	330mm X 406mm X 89mm (13" X 16" X 3.5")
Temperature	
Operating	5° - 55° Celsius (41° - 131° Fahrenheit)
Humidity	0%-85% (Non-Condensing)
Storage	-10° - 85° Celsius (14° - 185° Fahrenheit)



It is important that the unit is installed in a dry cool location that is not affected by humidity. Do not locate the unit in air conditioning or a boiler room that can exceed the temperature or humidity specifications.



The isolated communications interface on the Protege uses full galvanic isolation to prevent ground loop noise and cross phase ground differential. This is a very important feature of the product family and the correct connection of power to this isolated section will ensure the correct operation of the communications network. Failure to apply power to the communication interface will prevent the operation of the communication interface.

11 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.



12 European Standards

CE Statement

Conforms to European Union (EU) Low Voltage Directive (LVD) 2014/35/EC, Electro-Magnetic Compatibility (EMC) Directive 2014/30/EU and RoHS Recast (RoHS2) Directive: 2011/65/EU.

The CE mark indicates that this product complies with the European requirements for safety, health, environmental and customer protection.



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 was tested by the accredited testing laboratory No. 1172 of the company TESTALARM Praha s.r.o. and met the requirements and conditions for full compliance with EN50131 series of standards for equipment classification;

Security Grade 3

Environmental Class II

Equipment Class: Fixed

EN 50131-1:2006, EN 50131-3:2009, EN 50131-6:2008

Recognition class 2 (for readers without a keypad)

Recognition class 3 (for readers with a keypad)

Access class B

EN 50133-1:1998

ICT enclosure all products, CAB-JMB-NOT, has been tested and certified to EN50131. By design, the ICT enclosure for all products, CAB-FBY-NOT, complies with the EN50131 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.

EN 50131

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

Ensure for Grade 3 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 zone is not disarmed within 30 seconds, the entry delay has expired or another instant is violated, the main alarm will be triggered and reported.

To comply with EN 50131-1 neither Internals Only on Part Set Zone 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 for Anti Masking, detectors with a separate or independent mask signal should be used and the mask output should be connected to another input zone.

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

To comply with EN 50131-1:

- do not fit more than 10 unpowered detectors per zone,
- do not fit more than one non-latching powered detector per zone,
- do not mix unpowered detectors and non-latching powered detectors on a zone.

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: Only one battery can be connected and monitored per system. If more capacity is required, a single, larger battery must be used.

13 Ordering Information

Please use the following product codes when placing an order for the Protege Reader Expander.

- PRT-RDE2-PCB - Protege Reader Expander (PCB Only)

Includes Accessory Bag

To order the Protege Ethernet Reader Expander in a cabinet order the CAB-LRG large steel cabinet complete with transformer and tamper connections.

Manuals and additional literature are available on the ICT Website (<http://www.ict.co>).

14 Warranty

Integrated Control Technology (ICT) warrants its products to be free from defects in materials and workmanship under normal use for a period of two years. Except as specifically stated herein, all express or implied warranties whatsoever, statutory or otherwise, including without limitation, any implied warranty of merchantability and fitness for a particular purpose, are expressly excluded. ICT does not install or connect the products and because the products may be used in conjunction with products not manufactured by ICT, ICT cannot guarantee the performance of the security system. ICT's obligation and liability under this warranty is expressly limited to repairing or replacing, at ICT's option, any product not meeting the specifications. In no event shall ICT be liable to the buyer or any other person for any loss or damages whether direct or indirect or consequential or incidental, including without limitation, any damages for lost profits, stolen goods, or claims by any other party caused by defective goods or otherwise arising from the improper, incorrect or otherwise faulty installation or use of the merchandise sold.

15 Contact

Integrated Control Technology welcomes all feedback.

Please visit our website (<http://www.ict.co>) or use the contact information below.

Integrated Control Technology

P.O. Box 302-340
North Harbour Post Centre
Auckland
New Zealand

4 John Glenn Ave
Rosedale
North Shore City 0632
Auckland
New Zealand

Phone: +64-9-476-7124

Toll Free Numbers:

0800 ICT 111 (0800 428 111) - New Zealand

1800 ICT 111 (1800 428 111) - Australia

1855 ICT 9111 (1855 428 9111) - USA/Canada

Email: sales@incontrol.co.nz or support@incontrol.co.nz (<mailto:support@ict.co>)

Web: www.ict.co

APAC

Integrated Control Technology Limited
4 John Glenn Avenue, Rosedale, Auckland 0632
PO Box 302-340, North Harbour, Auckland 0751, New Zealand
Email: sales@ict.co Toll Free: (0800) 428 111 Phone: 64 (9) 476 7124

AMERICAS

Integrated Control Technology (USA) LLC
5265 S Rio Grande Street, Suite 201, Littleton, CO 80120
Email: ussales@ict.co Toll Free: (855) 428 9111 Phone: 720 442 0767

EMEA

Integrated Control Technology (Europe) Limited
St Mary's Court, The Broadway, Amersham, HP7 0UT, UK
Email: emeasales@ict.co Phone: 44 0 1494 590494

Designers & manufacturers of integrated electronic access control, security and automation products.

Designed & manufactured by Integrated Control Technology Ltd.

Copyright © Integrated Control Technology Limited 2003-2017. All rights reserved.

Disclaimer: Whilst every effort has been made to ensure accuracy in the representation of these products, 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 Integrated Control Technology policy of enhanced development, design and specifications are subject to change without notice

227-4035-250

www.ict.co

