PRT-RDM2-PCB

Protege Mini 2 Reader Expander

Installation Manual

ICTProtege®

Publication Date: March 2015

Contents

1 Introduction

Thank you for purchasing the Protege Mini 2 Reader Expander by Integrated Control Technology. The Protege System is an advanced technology security 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 whether it's small, large, residential or commercial.

The Reader Expander extends the number of card reader inputs on the system by 2 or 4 when using Multiple Reader mode, number of zone inputs by 8 (four 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 relay 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, over a distance of up to 900M (3000ft). Further span can be achieved with the use of a network repeater module.

Locking a network prevents the removal, substitution or addition of modules to the module network effectively preventing any tampering with the system.

The current features of the 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 lock FORM C Relay PGM outputs
- 6 open collector PGM outputs (Reader Control outputs)
- Smart reader missing/tamper monitoring
- Online and remote upgradeable firmware

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.

- Reader Expander Printed Circuit Board
- Protege Mini 2 Reader Expander Installation Manual
- 18 1K Ohm resistors
- 2 1N4007 lock reverse EMF protection diodes
- 6 Plastic mounting standoffs

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

1.1 Document Conventions

	Indicates a warning or cautionary message
	Indicates an important note or advisory information
	Indicates a hint or suggestion
[TEXT]	Bold text enclosed in brackets is used to show a section number or address of a programmable option or information on programming shortcut sequences

2 Installation

2.1 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.

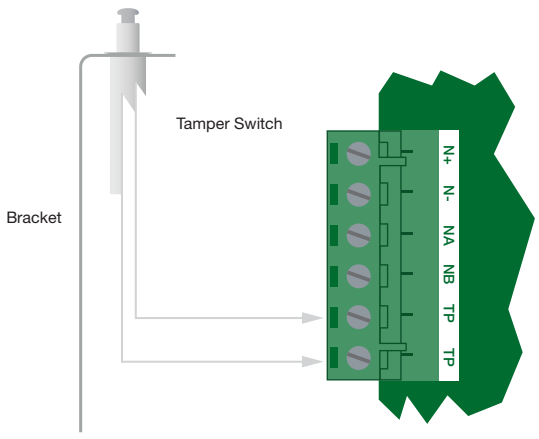
We recommend the Reader Expander is installed in a location that will facilitate easy access for wiring. We also recommend that the Reader Expander is installed in electrical rooms, communication equipment rooms, closets or in an accessible area of the ceiling.

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.

2.2 Cabinet Tamper Switch

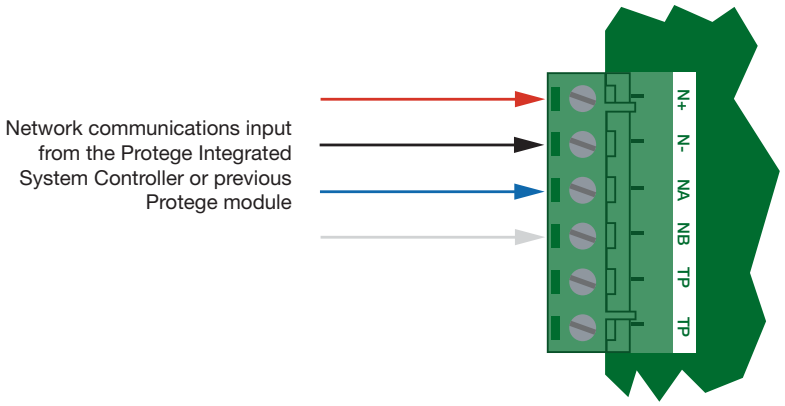
The enclosure tamper input signals to the monitoring station or remote computer that the Reader Expander enclosure has been opened. The tamper input switch shall be mounted into the steel bracket provided and connected to the tamper connection terminals as shown in the diagram below. The tamper input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



Tamper Input Connection

2.3 DC Power and Encrypted Module Network

The Reader Expander incorporates encrypted RS-485 communications technology, and both module and network power are supplied by the N+ and N- terminals.

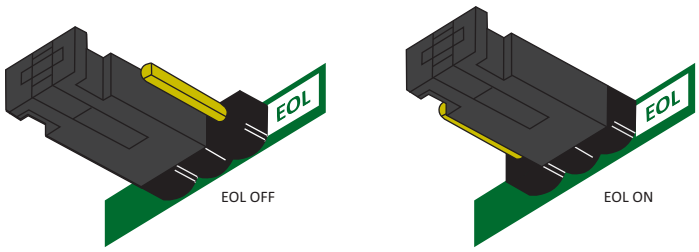


Standard Communication Connection

Connection of the communications and DC supply should be performed according to the diagram shown above. It is important that the N+ Network Communications Power be 12VDC supplied from an independent battery backed power supply unit such as the PRT-PSU-DIN or a networked module capable of supplying the required voltage to all devices on the RS485 network.

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.
- Under no circumstances should you power the locking devices that are connected to the Reader Expander from the N+ and N- network communication power supply. A separate power supply MUST be used to power the locking devices.



EOL Jumper

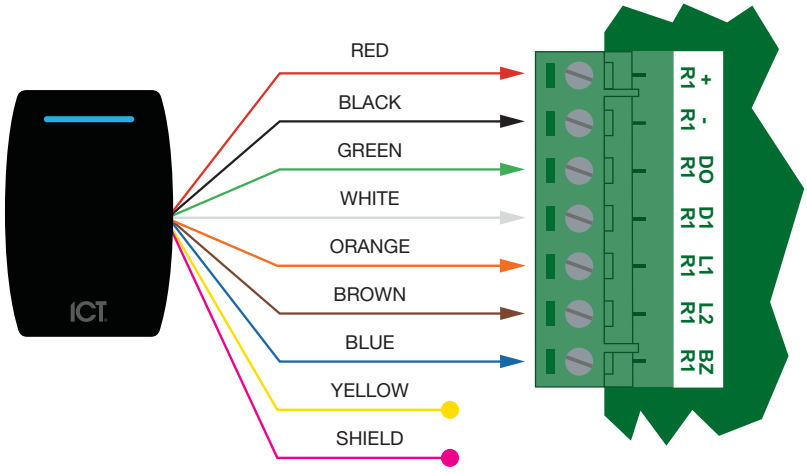
The EOL (End Of Line) jumper should be placed in the ON position when the Reader Expander is inserted as the FIRST or LAST module on the RS485 network. EOL is ON when the jumper is placed closest to the EOL text.

3 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.

3.1 Reader Connection

The Reader Expander allows the connection of 2 magnetic clock and data 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 a standard Wiegand Reader with the Reader Expander controlling an access door and entry/exit door.



Standard Reader Connection

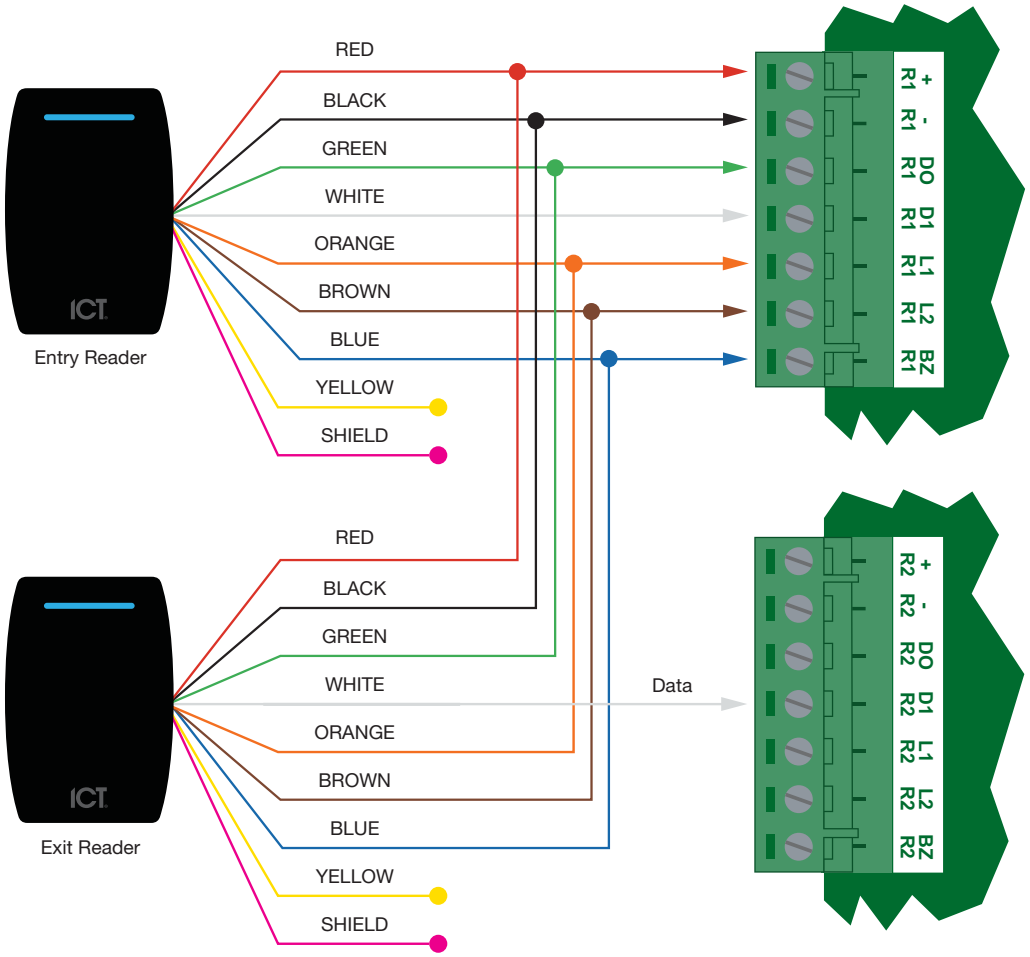
Warning: The shield connection on the card reading device that is connected to the reader port should NOT be connected to the R1-, R2- or a 0V connection. Do not join the shield and black wires at the card reading device. The shield should not be connected to any shield used for isolated communication. Always refer to the card reader manufacturer for detailed installation guidelines.

The beeper output on the Reader Expander provides diagnostic information to the end user and installer when access is denied or the unit is operating offline. Refer to PGM Beeper Outputs Special Function Operation (see page 15) for further details.

3.2 Multiple Wiegand Reader Connection

When operating in multiple reader mode the Reader Expander allows the connection of 4 reading devices for entry/exit control of doors per reader input.

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.



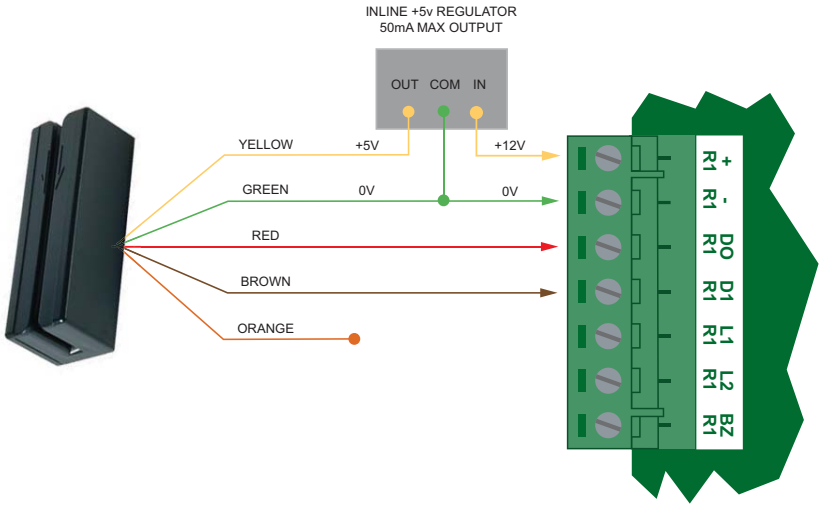
Multiple Reader Interface

Warning: The shield connection on the card reading device that is connected to the reader port should NOT be connected to the R1-, R2- or a 0V connection. Do not join the shield and black wires at the card reading device. The shield should not be connected to any shield used for isolated communication. Always refer to the card reader manufacturer for detailed installation guidelines.

The secondary reader when connected will ALWAYS function as the exit reader.

3.3 Magnetic Reader Connection

The 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 number for ATM access control and first 4, 5 and 6 card numbers.

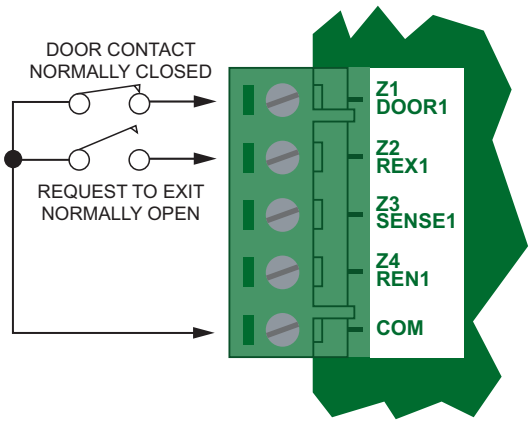


Magnetic Card Reader Interface

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

3.4 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.

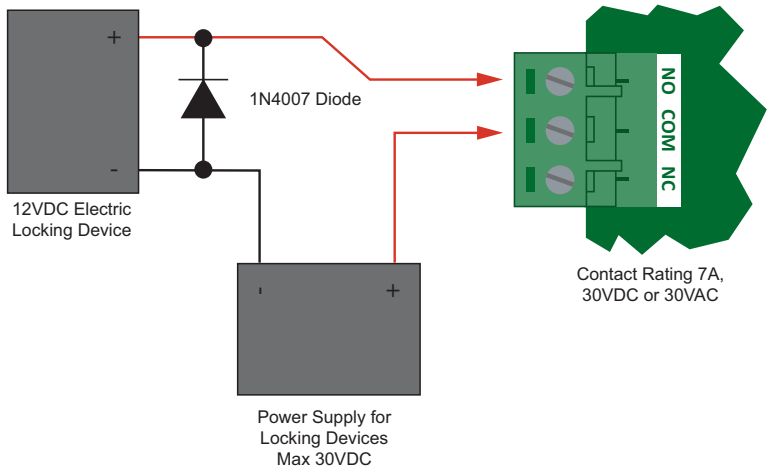


Standard Door Contact Inputs

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.

3.5 Door Lock Connection

The Reader Expander provides two lock output relays that can be used to switch electric locks.



Door Lock Outputs

- When using a door with an entry and exit reader, the LOCK output should 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 shown in the above diagram is supplied with the Reader Expander and MUST be installed at the electric strike terminals.

4 Zone Inputs

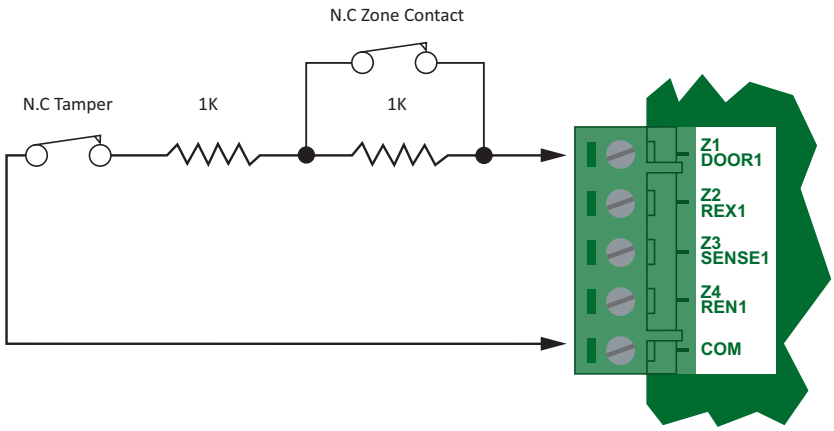
The Reader Expander has 8 zone inputs. The Reader Expander also monitors 16 trouble zones used to report trouble conditions such as module communication problems.

4.1 Zone Inputs

The Reader Expander can monitor the state of up to 8 zone inputs EOL monitored or dry contact devices such as magnetic switches, PIR motion detectors and temperature thermostats. Devices connected to these zones can be installed to a maximum distance of 300m (1000ft) from the Reader Expander when using 22 AWG wire. Each zone input may be individually configured for normally opened and normally closed configurations with or without EOL resistors for tamper and short condition monitoring.

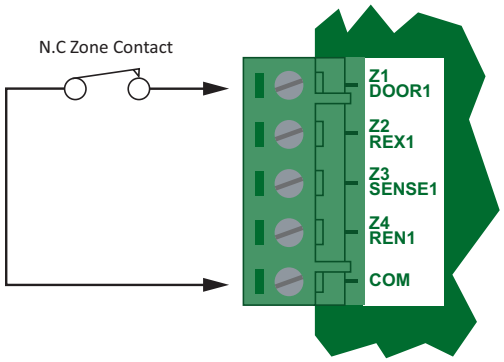
When using a zone with the EOL resistor configuration, the controller generates an alarm condition when the state of a zone changes between open and closed and generates a tamper alarm condition when a wire fault (short circuit) or a cut wire (tampered) in the line occurs.

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



EOL Resistor Zone Configuration

Each zone input can use a different input configuration. When using the No Resistor configuration, the system 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

4.2 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. 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	Reserved	None	None
RDxxx:04	Aux Failure	Power Fault	General
RDxxx:05	Reserved	None	None
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	Reserved	None	None
RDxxx:11	Reserved	None	None
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

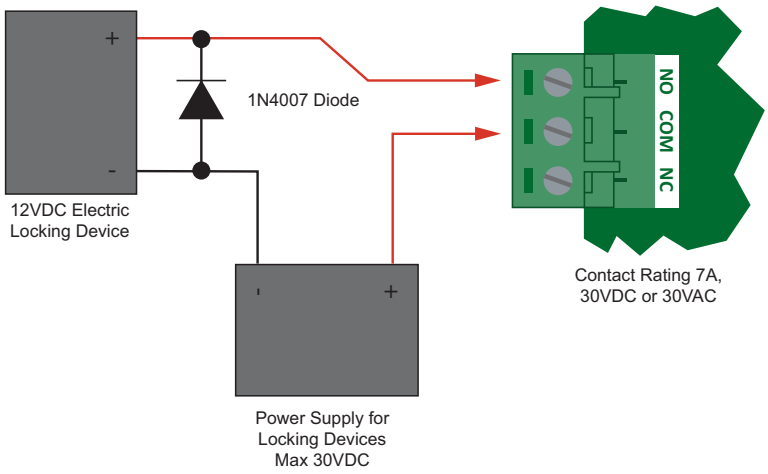
Replace 'xxx' with the appropriate address of the Reader Expander that you are programming.

5 Programmable Outputs

The Reader Expander has 8 Programmable Outputs (PGMs). These PGMs are used to activate bell sirens, lighting circuits, door locks, relay accessory products, and other automation points.

5.1 Lock PGM Outputs (1 and 2)

Relays are provided on PGM output 1 and 2. These are used for the Lock 1 (PGM1 RD001:01) and Lock2 (PGM2 RD001:02) functions and are used to control electric door strikes and other lock control devices. The lock relay will switch a maximum current of 7A resistive.



Lock Output PGM1/2 Connection

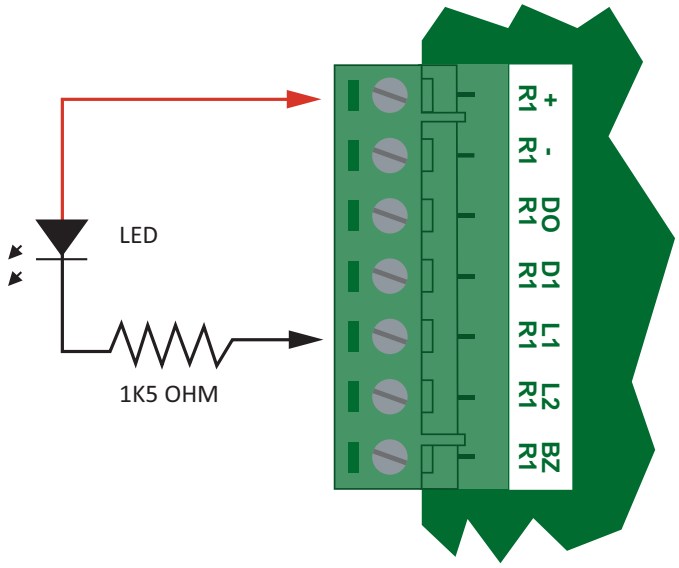
5.2 Standard PGM Outputs (3 To 8)

The PGM outputs 3, 4, 5, 6, 7 and 8 on the 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)

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

5.3 PGM Beeper Outputs Special Functions (5 and 8)

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

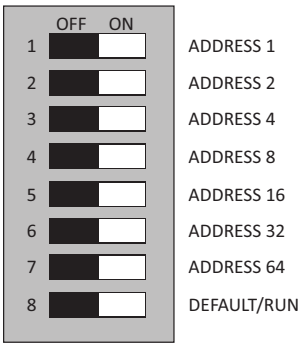
Function	Description
2 Beeps	Access Granted. The lock will activate and allow access to the door the card has been presented.
4 Beeps	Offline Access Granted. This is generated ONLY if the reader expander is operating offline and the mode of offline operation allows access.
1 Long Beep	Offline Access Denied. This is generated ONLY if the reader expander 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.

6 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.

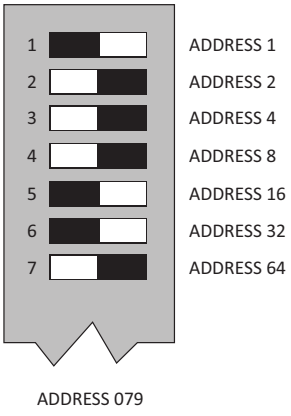
6.1 Address Configuration

The settings of the switch positions (1 to 7) determine the address assigned to the Reader Expander, a value from 1 to 128. When setting an address the Reader Expander must be powered down and restarted for the new address to take effect. 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 (1 to 7) that is set in the ON position and then adding 1 to this value. In the following example, the device address is determined by performing the addition (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

7 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.

7.1 Status Indicator

The Status indicator displays module status of the Reader Expander. FLASHING rapidly at 250ms intervals indicates that the Reader Expander is attempting registration with the controller. FLASHING at 1 second intervals will indicate that the Reader Expander has successfully registered with the controller.

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

7.2 Fault Indicator

The Fault indicator is lit any time the module is operating in a non-standard mode. When the Fault indicator is FLASHING the Reader Expander is operating in boot mode awaiting firmware update. When the Fault indicator is ON the Reader Expander is in error state and will flash an error code with the Status indicator. Refer to the Error Code Display section to determine the error.

7.3 RLY 1/RLY 2 Indicators

The RLY 1 and RLY 2 indicators will show the status of the respective lock output relays.

ON	Relay output is ON.
OFF	Relay output is OFF

7.4 RDRMON Indicator

Reader/Auxiliary voltage is supplied to the R1+ and R2+ outputs through the auxiliary fuse. If the reader/auxiliary supply is normal then the RDRMON indicator will be ON. If the fuse is damaged, the indicator will be OFF.

7.5 R1 and R2 Data Indicator

The R1 and R2 data indicators display the status of the data being received on their respective reader terminals. A short FLASH (<250 Milliseconds) on the R1/R2 data indicators will show that data was received but was not in the correct format. A long FLASH (>1 Second) indicates that the Reader Expander has read the data and the format was correct.

8 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.

8.1 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.

9 Technical Specifications

The following specifications are important and vital to the correct operation of the 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	
DC Input Voltage	12VDC (+/-10%)
R1/R2 DC Output Voltage	12VDC 700mA (Typical) Electronic Shutdown at 1.1A
Operating Current	40mA (Typical) 110mA (Max, All Relays Activated)
Low Voltage Cut-out	8.7VDC
Low Voltage Restore	10.5VDC
Communication	
RS-485	Isolated Module Network
Outputs	
Lock Outputs	2 FORM C Relay Outputs, 7A 250V Max
PGM Outputs	6 (50mA Max) Open Collector
Inputs	
Zone	8 (10ms to 1hr Input Speed Programmable)
Tamper	Dedicated Hardware Tamper Input
Trouble Zone	16
Dimensions	
PCB Dimensions	96mm X 217mm (3.78" X 8.54")
Weight	156g (5.50oz)
Temperature	
Operating	5˚- 55˚ Celsius (41˚ - 131˚ Fahrenheit)
Storage	-10˚- 85˚ Celsius (14˚ - 185˚ Fahrenheit)
Humidity	0%-85% (Non-Condensing)

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.

10 New Zealand and Australia

The C-Tick compliance label indicates that the supplier of the device asserts that it complies with all applicable standards. The SCN establishes a traceable link between a device and the supplier responsible for placing it on the Australian market.

11 European CE and EN 50131

European Standards CE

Conforms to European Union (EU) Low Voltage Directive (LVD) 73/23/EEC (amended by 93/68/EEC) and Electro-Magnetic Compatibility (EMC) Directive 89/336/EEC (amended by 92/31/EEC and 93/68/EEC). The CE mark indicates that this product complies with the European requirements for safety, health, environmental and customer protection

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 authorised 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.

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.

12 Ordering Information

Please use the following product codes when placing an order for the Protege Mini 2 Reader Expander.

- PRT-RDM2-PCB

To order the Reader Expander in a cabinet, order the CAB-MED steel cabinet complete with transformer and tamper connections separately.

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

13 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.

14 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

11 Canaveral Drive
Albany
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

Web: www.ict.co

Integrated Control Technology Limited

11 Canaveral Drive, Albany, Auckland 0632
P.O. Box 302-340, North Harbour, Auckland 0751, New Zealand
Email: support@incontrol.co.nz **Phone:** +64 (9) 476 7124 **Fax:** +64 (9) 476 7128
Designers & manufacturers of integrated electronic access control, security & automation products.
Designed & manufactured by Integrated Control Technology Limited.

www.incontrol.co.nz

227-4070-001