



PRT-KLCS

Protege Touch Sense LCD Keypad

Installation Manual



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 2003-2024. All rights reserved.

Last Published: 17-Jun-24 10:10 AM

Contents

Introduction	5
Installation Requirements	6
Mounting Instructions	7
Mounting with Surface Mount Box Accessory	7
Mechanical Layout	8
Mechanical Layout of Surface Mount Box Accessory	9
Configuration	10
Keypad Functions	10
Keypad Address	11
Backlight Brightness Setting	11
Default Configuration	11
Keypad Version Information	11
Communication	12
Connections	13
End of Line Termination (EOL)	13
Inputs	13
Trouble Inputs	15
Outputs	16
LED Indicators	17
Error Messages	19
Technical Specifications	20
New Zealand and Australia	21
European Standards	22
UK Conformity Assessment Mark	24
UL and cUL Installation Requirements	25
cUL Compliance Requirements	25
CAN/ULC-S304	25
CAN/ULC-S559	28
UL Compliance Requirements	32
UL1610	32
FCC Compliance Statements	34
Industry Canada Statement	35
Disclaimer and Warranty	36

Introduction

The Protege Touch Sense LCD Keypad provides a sleek, user friendly human interface to the Protege system, an advanced technology security product providing seamless and powerful integration of access control, security and building automation.

The current features of the keypad include:

- Securely login with user codes from 1 to 8 digits and support for card reader and PIN code operation.
- Intuitive menu function allows scrollable options according to user security level with quick access shortcut keys for the power user.
- Dual code and master code provider functions for secure ATM and banking vault area access with automatic timeout and delayed opening functions.
- Individual reportable duress code trouble for each Protege keypad.
- Activation of 3 reportable panic events (Panic, Medical and Fire).
- Smoke detector reset provided on Clear and Enter keys selectable for an output or output group.
- 4 inputs (duplex mode) can be used to perform any system alarm and automation functions with a dedicated enclosure tamper switch.
- 1 low current output for driving any signaling device.
- Capacitive touch sense keypad.
- Available in white or black.

Installation Requirements

This equipment is to be installed in accordance with:

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

Mounting Instructions

The keypad should be mounted in an accessible location, such as near an external door. Cables are intended to be run inside the wall. If cables are to be run through external conduits, you must use the surface mount box accessory (see below).

1. Select where to mount the keypad, ensuring that it is in an accessible location.
2. Hold the rear case against the wall and mark the mounting holes and cable entry area. The cable entry area should align with a hole cut through the plaster wall-board.
3. Use appropriate screws (not supplied) to affix the case to the wall.
4. Run the wiring. Refer to later sections of this manual for the electrical connections. Leave about 20cm (8") of wire protruding through the center of the mounted half of the case.
5. Connect the wiring to the keypad electronics.
6. Clip the upper rim of the front case over the upper rim of the rear case. Press gently on the front case until the lower rim slots over the lower rim of the rear case, lining up the screw hole at the bottom.
7. To complete the installation, use the M3 x 8mm Plastite screw provided with the keypad to secure and fasten the cases together.

Mounting with Surface Mount Box Accessory

The optional surface mount box accessory enables you to mount the keypad projected from the wall, allowing space for cables from external conduits. The surface mount box has the same height, width and screw positions as the standard keypad rear case, with additional depth.

To mount the keypad on a surface mount box:

1. Select where to mount the keypad, ensuring that it is in an accessible location.
2. Hold the surface mount box against the wall and mark the mounting holes.
3. Mark the entry point for the external conduit on the top, bottom or side of the surface mount box. This must be aligned in the **center** of the box side. Drill a hole to allow cable entry.

Warning: Do not drill a hole with a diameter greater than **20mm (0.8")** in the surface mount box. Do not drill off-center. Drilling too close to the edge of the surface mount box may cause structural damage.

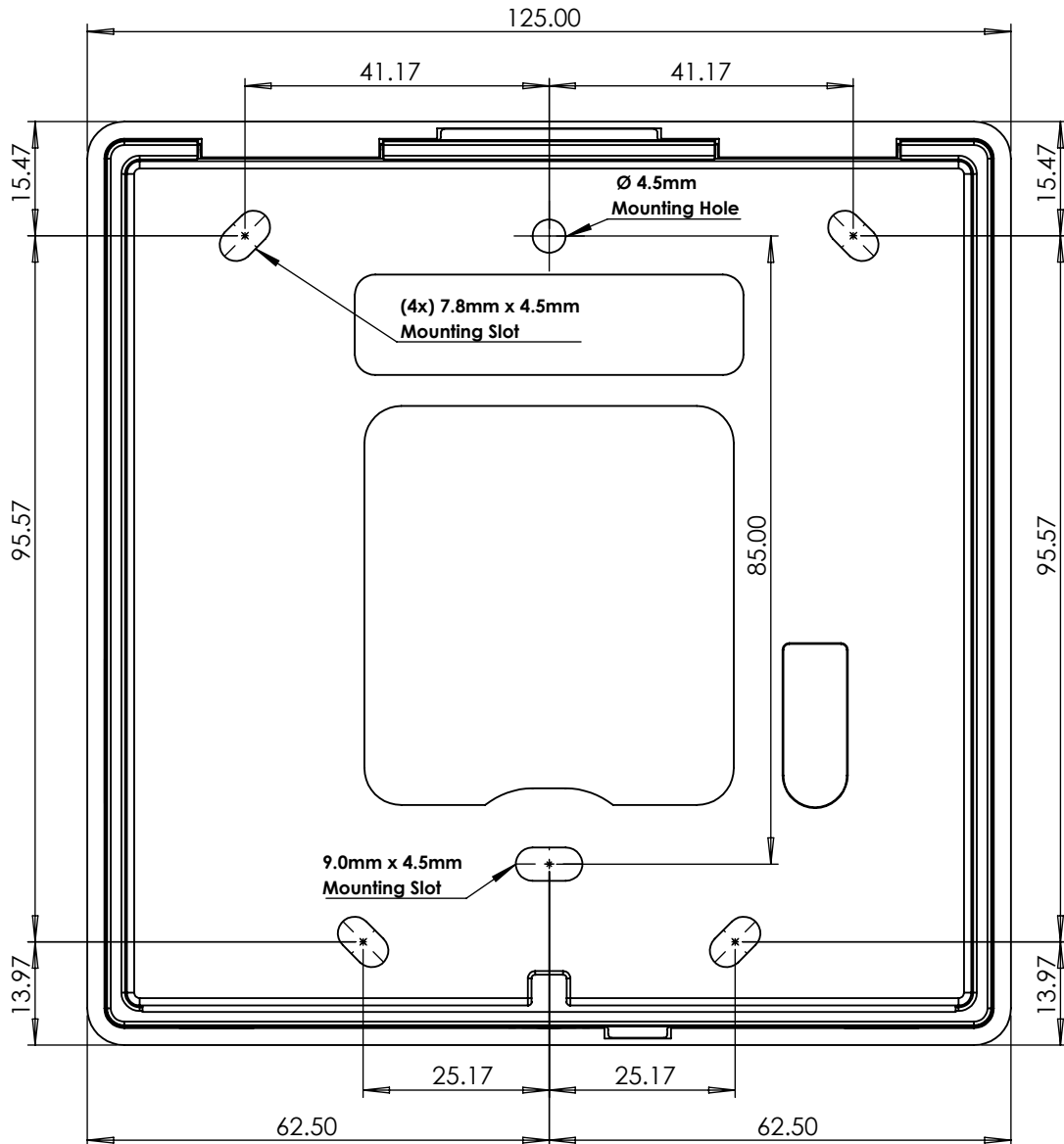
4. Use appropriate screws (not supplied) to affix the surface mount box to the wall.
5. Connect the wiring to the keypad electronics through the conduit hole.
6. Insert the short rod supplied with the surface mount box into the slot at the bottom left. This will connect to the keypad's tamper switch, causing it to open when the keypad is removed from the surface mount box or the surface mount box is removed from the wall.
7. Clip the upper rim of the front case over the upper rim of the surface mount box. Press gently on the front case until the lower rim slots over the lower rim of the surface mount box, lining up the screw hole at the bottom.
8. To complete the installation, use the M3 x 8mm Plastite screw provided with the keypad to secure and fasten the front case to the surface mount box.



The surface mount box accessory has not been evaluated for UL/cUL applications.

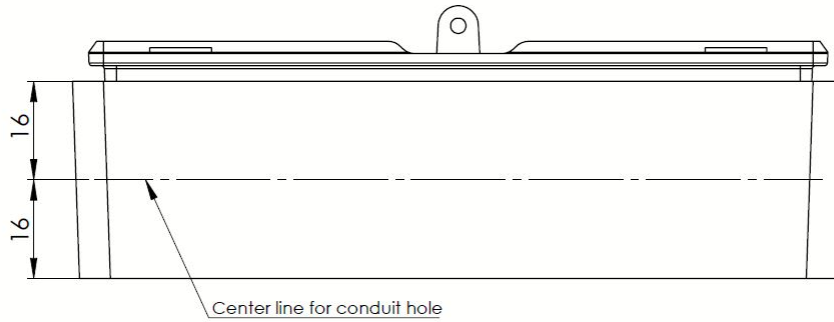
Mechanical Layout

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



Mechanical Layout of Surface Mount Box Accessory

The mechanical layout shown below outlines the essential details needed to help ensure the correct installation of the surface mount box accessory. All measurements are shown in millimeters.












Configuration

Before the keypad will communicate with the Protege system it must be assigned an address.

To program an address using the system configuration menu, apply power to the keypad. When the screen displays the keypad version information press the **[CLEAR]** key then press **[ENTER]**. A configuration menu is displayed. Scroll the available options by pressing the up and down keys and **[ENTER]** to select the menu item.

The configuration menu can only be accessed when the keypad powers up. It cannot be accessed when the keypad is operational.

Keypad Functions

Key	Function
0-9	The primary function of the numeric keys is to enter user codes. When controlling devices the [1] key turns the device on, the [2] turns the device off, and in the on state the [3] key latches the device.
	The [ARM] key is used to start the arming process for an area.
	The [DISARM] key is used to silence alarms, disarm the area, and cancel an arming sequence.
	The [MENU] key is used to access the menu and can be followed by menu shortcut selection key(s) that represent a menu item. When the [MENU] key is held for 2 seconds, the keypad will recognize it as the [FUNCTION] key, which can be programmed to unlock a door.
	The [STAY] key is used to initiate the stay arming process for an area.
	The [FORCE] key is used to force arm an area.
	The [MEMORY] key will take a user directly to the memory view menu.
	The [BYPASS] key can be pressed when an area is breached during an arming process to bypass the displayed input.
	The [CLEAR] key will log off the user currently logged in to the keypad. When pressed while not logged in the display will be refreshed.
	The [ENTER] key is used to confirm an action on the keypad, acknowledge memory and alarm information, and move to the next programming screen.
ARROW KEYS	The arrow keys are used to scroll the menu, move the focus of a program window to the next screen, and move the cursor when programming or editing values.

Keypad Address

The address selection sets the address of the keypad. This address must be a unique address in the Protege system that is below an address of 200.

```
Enter device  
address: 256
```

Use the numerical keys 0 to 9 to program the address and press **[ENTER]** to save the setting.

To exit without making changes press the **[MENU]** key.

Backlight Brightness Setting

The backlight brightness setting adjusts the brightness for the LCD screen and the keypad's LEDs.

```
Backlight  
[***** ]
```

Use the left and right keys to adjust the brightness and press **[ENTER]** to save the setting.

To exit without making changes press the **[MENU]** key.

Default Configuration

The default setting resets the keypad to the factory default settings.

```
Press [ENTER] to  
default keypad.
```

Press **[ENTER]** to default the keypad.

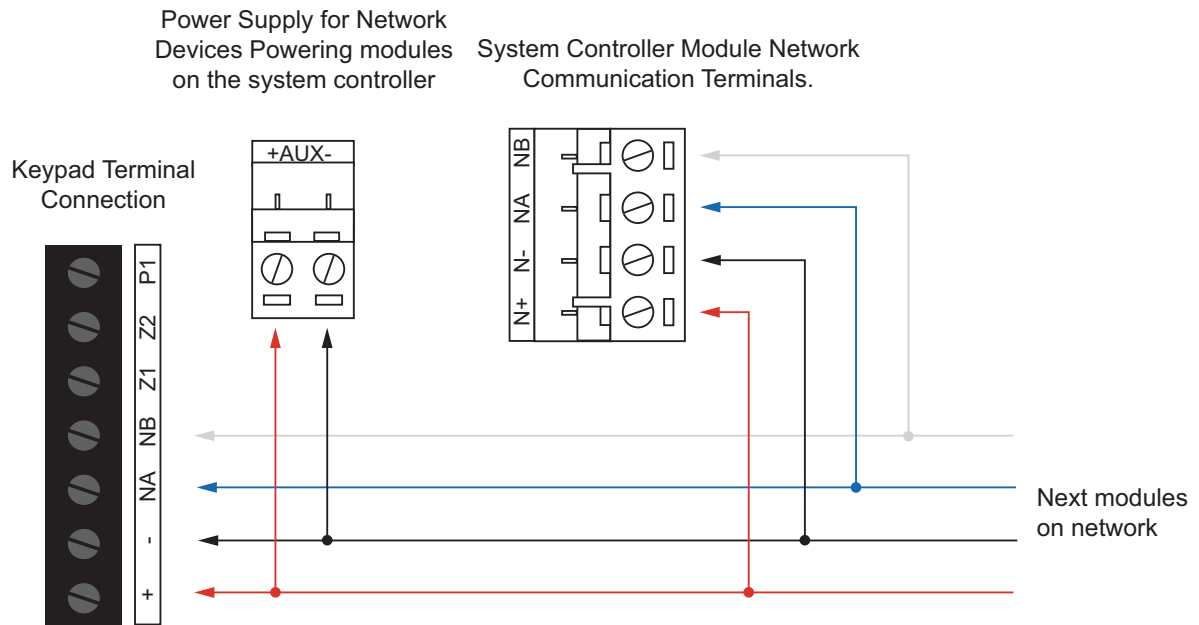
To exit without defaulting the keypad press the **[MENU]** key.

Keypad Version Information

The version menu option displays the version and build information about the keypad. The version information is displayed on two lines and can be scrolled. Press the **[MENU]** key to exit.

Communication

The Protege system incorporates encrypted RS-485 communications technology for its module network. Each system controller supports up to 250 keypads.



Connections

End of Line Termination (EOL)

The EOL (End of Line) jumper should be placed in the ON position when the keypad is inserted as the **first or last** module on the RS-485 network.



EOL Jumper OFF



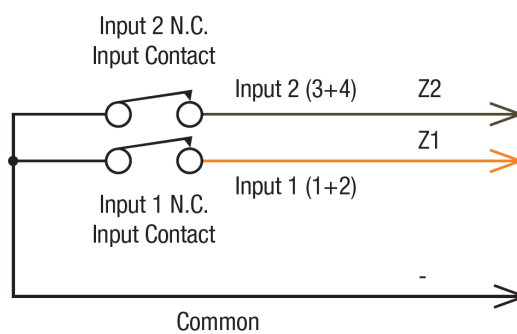
EOL Jumper ON

Inputs

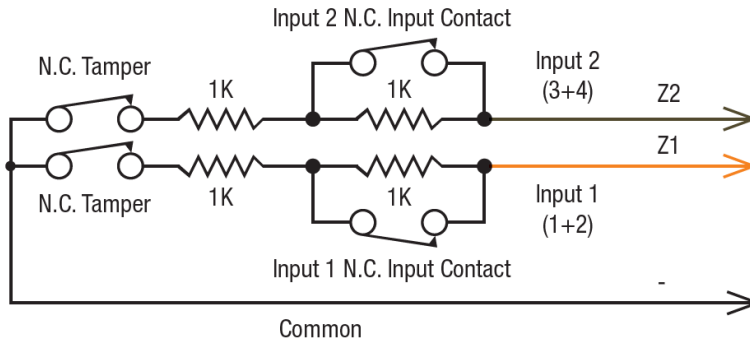
The keypad is capable of connecting to 4 inputs, each of which can be programmed to perform the required function in the Protege system.

The following diagrams show examples of the input wiring configuration settings that can be programmed under the input options within the Protege software.

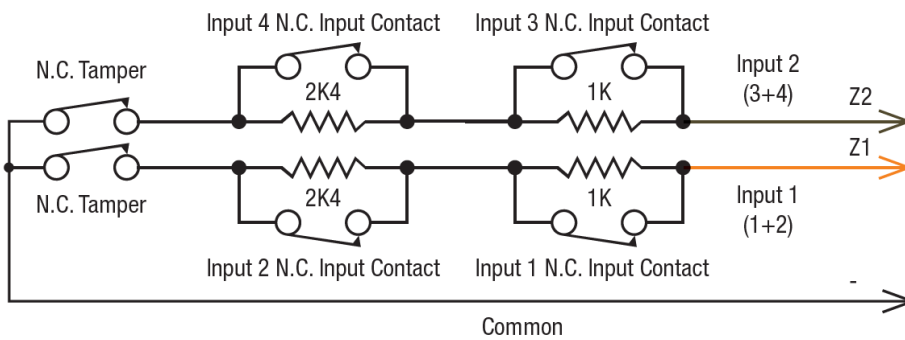
Input (No Resistors):



Input (1K and 1K):



Input Duplex Mode (1K and 2K4):



To utilize the input duplex mode configuration shown above, the **Duplex Inputs** setting must be enabled in the keypad programming (**Keypads | Options 2**).

Trouble Inputs

Each keypad can monitor up to 8 trouble inputs.

Trouble inputs are used to monitor the module status and in most cases are not physically connected to an external input.

The following table details the trouble inputs that are configured in the system and the trouble groups that they are associated with.

Trouble Input	Function	Default Trouble Group	Default Trouble Group Option
KPXXX:01	Module Tamper Opens when the keypad is removed from the wall.	System	Module Tamper
KPXXX:02	Reserved	-	-
KPXXX:03	User Panic Keys 1 and 3 are pressed together generating a panic message.	-	-
KPXXX:04	User Duress A user code with the duress option enabled has entered a code on the keypad.	-	-
KPXXX:05	Reserved	-	-
KPXXX:06	Reserved	-	-
KPXXX:07	Too Many Codes Too many incorrect codes have been entered at the keypad and it has been locked out for the programmed lockout time.	Access	Number of Attempts
KPXXX:08	Module Offline The keypad has either been removed from the system or lost communications.	System	Module Lost

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

The panic and duress features have not been evaluated for UL/cUL installations.

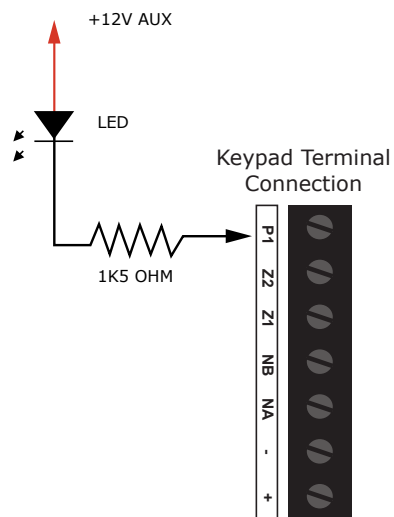
Outputs

The keypad has 4 programmable outputs. These outputs are used to control the 2 system status LED indicators, system beeper and the open collector output. The outputs can be activated and deactivated based on specific events or functions within the Protege system.

Output	Function
KPXXX:01	Open collector output on the keypad terminal block (P1)
KPXXX:02	Armed status indicator LED (red)
KPXXX:03	Disarmed status indicator LED (green)
KPXXX:04	Beeper output

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

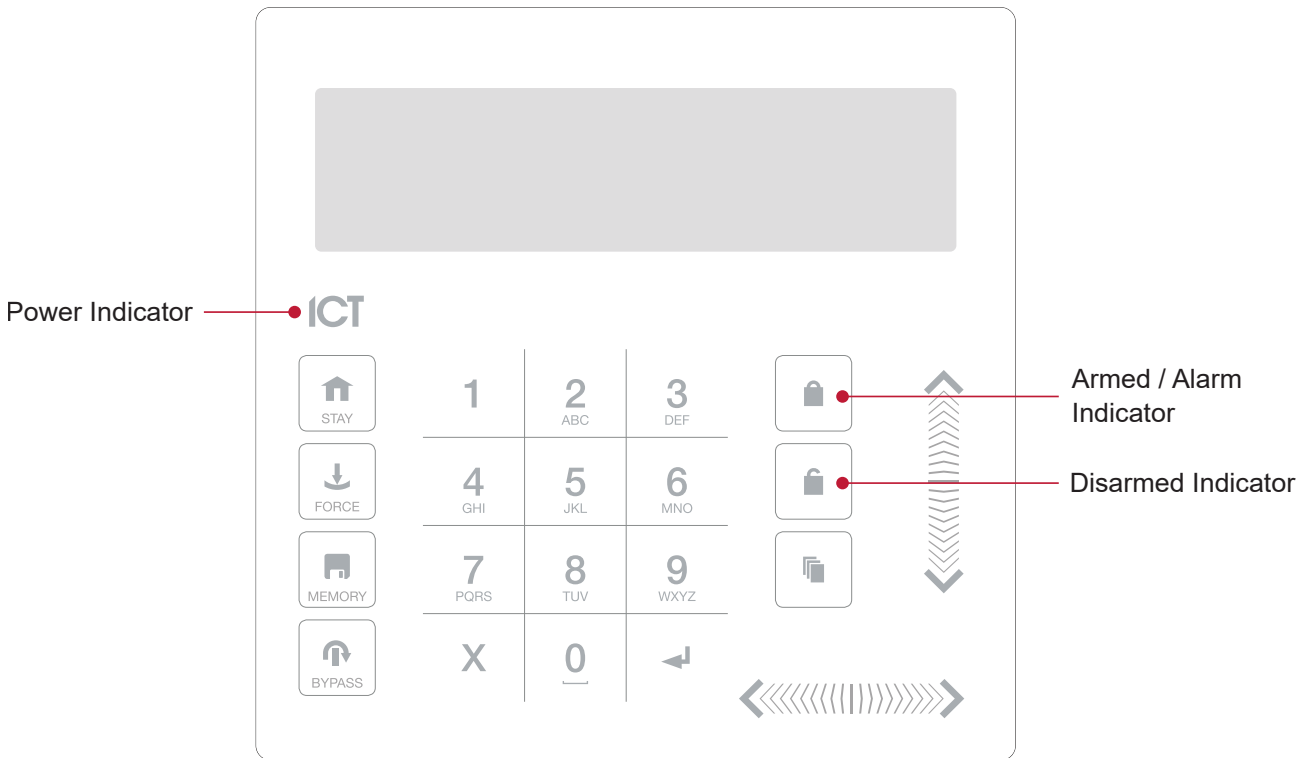
Example Open Collector Output Connection (P1):



Warning: The open collector output can switch to a maximum capacity of 50mA. Exceeding this amount will damage the output.

LED Indicators

The keypad features three status indicator lights showing the condition of the Protege system.



Confidentiality Mode

Keypads include a confidentiality mode where activation of the onboard output will cause all lights (Power, Disarm, Arm and LCD backlight) to turn off when the keypad is not in use.

When the onboard output is not activated, these lights serve their normal functions.

This feature must be enabled by entering the following command in the keypad programming:

ConfidentialMode = true

Confidentiality mode is available for keypads with firmware version 1.09.013 or later.

Power Indicator

When the power indicator **on**, the system is powered and operating normally. If there is a complete power failure this indicator will be **off**.

Disarmed Indicator

This indicator is programmable and can perform one or more functions in the Protege system. The following are common functions:

- To illuminate this LED when an area is disarmed, program it as the **Disarmed output** for the area.
- To illuminate the LED when an area is ready to arm (i.e. all inputs are closed), program it as the **Ready output** for the area.

Armed / Alarm Indicator

This indicator is programmable and can perform one or more functions in the Protege system. The following are common functions:

- To illuminate this LED when an area is armed, program it as the **Armed output** for the area.
- To flash this LED when an area is in alarm (until the alarm times out or the area is disarmed), add it to the **Bell output group** for the area. Use the **Bell pulse on/off time** settings to pulse the LED on and off.
- To flash this LED when an area has had an alarm (until the area is disarmed), program it as the **Alarm memory output** for the area. Use the **Alarm memory pulse on/off time** settings to pulse the LED on and off.

Error Messages

When the keypad attempts to register or communicate with the system controller after powering up, errors can be generated indicating access to the Protege system has been denied or was unsuccessful. This is a normal part of the Protege system.

Keypad Version Error

The version of the keypad is incorrect for the system controller. This error cannot be corrected without updating the keypad firmware. The event log in the system controller will display the version of the keypad and the version that is required if this error has occurred.

Please contact your distributor for information on how to update the firmware.

Keypad Address Too High

The address of the keypad that is programmed is beyond the maximum number of keypads that are allowed to connect to the controller. Press the **[EXIT]** key to restart the keypad. Set the keypad address to a lower value.

Duplicate Keypad Address

The address of the keypad is already programmed into the system controller. Press the **[EXIT]** key to restart the keypad then set the keypad address to a free address.

Security Violation

The system controller has security enabled and devices cannot be added to the Protege system. Remove the security setting for the system controller then press the **[EXIT]** key to restart the keypad.

Invalid Serial Number

The keypad has an invalid serial number programmed and cannot be registered on the Protege system. Return the keypad to your distributor. This error cannot be corrected without updating the keypad firmware.

Technical Specifications

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

Ordering Information	
PRT-KLCS	Protege Touch Sense LCD Keypad
Power Supply	
Operating Voltage	11VDC to 14VDC
Operating Current	60mA (95mA Max)
User Interface	
User Interface Display	Energy smart backlit LCD 16 x 2 alphanumeric display with enhanced viewing angle
User Interface Keypad	Combined 23 key capacitive touch keypad with 3 system status LEDs
Inputs and Outputs	
Inputs	2 standard or 4 using Input Duplex mode
Outputs	1 open collector (50mA Max) output. Programmable for all output functions. 3 system status LEDs 1 system beeper
Dimensions	
Dimensions (H x W x D)	125 x 125 x 20mm (4.92 x 4.92 x 0.79")
Net Weight	192g (6.8oz)
Gross Weight	243g (8.6oz)
Keypad with Surface Mount Box (H x W x D)	125 x 125 x 48mm (4.92 x 4.92 x 1.9")
Surface Mount Box Net Weight	110g (3.9oz)
Surface Mount Box Gross Weight	150g (5.3oz)
Operating Conditions	
Operating Temperature	UL/cUL 0° to 49°C (32° to 120°F) : EU EN -10° to 55°C (14° to 131°F)
Storage Temperature	-10° to 85° C (14° to 185° F)
Humidity	0%-93% non-condensing, indoor use only (relative humidity)

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

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

New Zealand and Australia

General Product Statement

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



European Standards

CE Statement

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

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



Information on Disposal for Users of Waste Electrical & Electronic Equipment

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

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

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

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

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

For business users in the European Union

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

Information on Disposal in other Countries outside the European Union

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

EN50131 Standards

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

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

Security Grade 4

Environmental Class II

Equipment Class: Fixed

Readers Environmental Class: IVA, IK07

SP1 (PSTN – voice protocol)

SP2 (PSTN – digital protocol)

SP6 (LAN – Ethernet) and DP1 (LAN – Ethernet + PSTN)

SP6 (LAN – Ethernet) and DP1 (LAN – Ethernet + USB-4G modem)

Tests EMC (operational) according to EN 55032:2015

Radiated disturbance EN 55032:2015

Power frequency magnetic field immunity tests (EN 61000-4-8)

EN50131

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

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

Anti Masking

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

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

To comply with EN 50131-1:

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

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

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

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

UK Conformity Assessment Mark

General Product Statement

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



UL and cUL Installation Requirements

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

cUL Compliance Requirements

CAN/ULC-S304

- **Auto Arming**

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

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

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

- **Arming Signal**

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

- **Double EOL Input Configuration**

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

- **Multiplex System and Poll Time**

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

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

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

- **Central Station Signal Receiver**

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

- **Number of attempts**

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

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

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

- **Check-In Time**

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

- **Trouble Input Service Test Report**

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

- **Primary Communication Channel**

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

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

The following options are required:

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

- **Status Change Signal**

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

- **Local Annunciation if Signal Reporting Failure**

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

The following options must be enabled in the Protege system:

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

- **Network and Domain Access**

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

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

- **Ethernet Connections**

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

- **Encryption**

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

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

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

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

- **Server Configuration**

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

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

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

- **Internet Service Provider (ISP)**

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

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

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

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

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

- **Backup Power Requirements**

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

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

- **Compromise Attempt Events**

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

The event is sent with the following details:

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

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

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

- **Power Supply Mains Power Connection**

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

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

CAN/ULC-S559

- **Signal Reporting**

Any fault of an active communication system shall be annunciated and recorded at the signal receiving center within 180 s of the occurrence of the fault.

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

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

In the ArmorIP Internet Monitoring Software the **Poll Time** must be set to 40 seconds and the **Grace Time** must be set to 20 seconds. Refer to the section Poll/Grace Time in the ArmorIP Version 3 Internet Monitoring Application User Manual.

- **Central Station Signal Receiver**

The maximum number of signal transmitting units connected to any transmission channel shall conform to the manufacturer's recommendations. The ArmorIP Receiver supports up to 10000 simultaneous connections.

Refer to the section Internet Connections Requirements in the ArmorIP Receiver Installation Manual for further details.

- **Number of attempts**

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

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

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

- **Check-In Time**

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

- **Trouble Input Service Test Report**

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

- **Ethernet Connections**

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

- **External Wiring**

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

- **Power Supply Mains Power Connection**

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

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

- **Arming Signal**

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

- **Keypad Wiring**

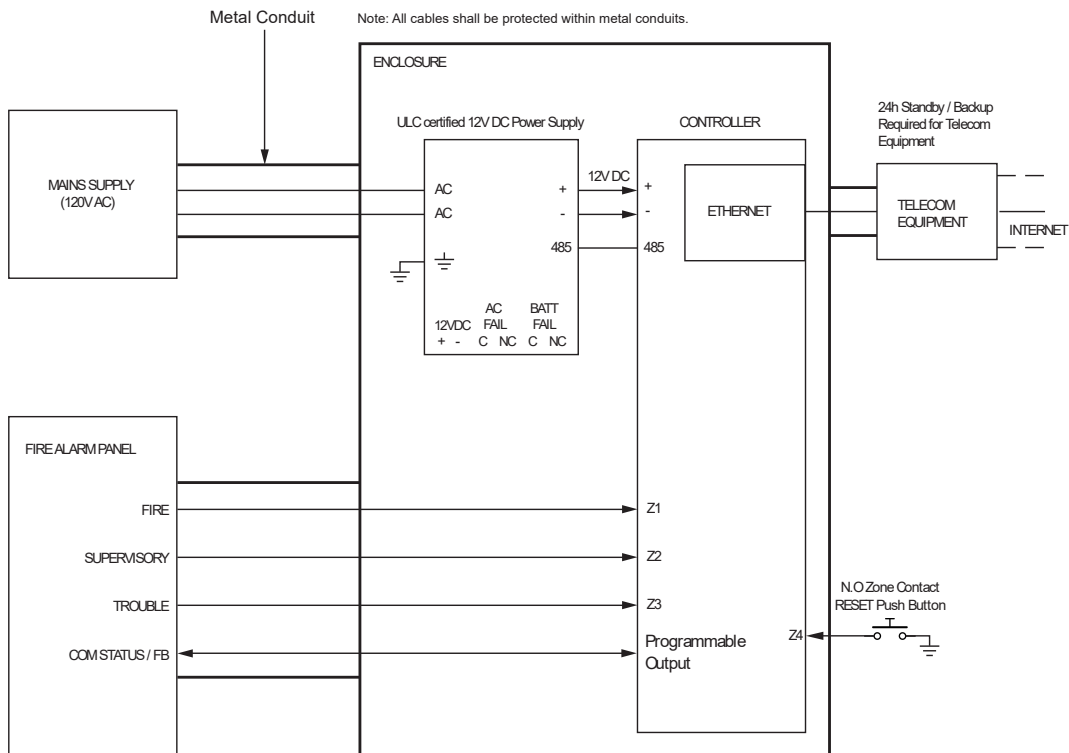
The RS-485 connection to the keypad must be wired such that the shorts and other faults on the RS-485 line connection of the keypad will not cause the controller to malfunction.

- **Fire Areas**

Fire areas shall be separated from burglar areas through area partitioning.

NOTE: Any available dry relay contact on the Protege controller or output expander may be used for the FACP system, provided the selected output is programmed as the Report OK output.

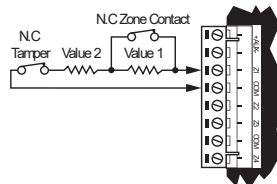
**CAN/ULC-S559
CONTROLLER
ACTIVE COMMUNICATION**



- * The AC FAIL output on the Power Supply **MUST** be programmed to follow the AC Trouble Input as follows:
AC FAIL = OPEN on fail
- * Fire zones shall be separated from burglar zones through area partitioning.
- * Fire zones Z1-Z3 shall be used exclusively for fire monitoring and cannot be programmed to activate the bell output
- * Fire Zone Z4 N.O. Push Button to be used as monitoring reset switch.

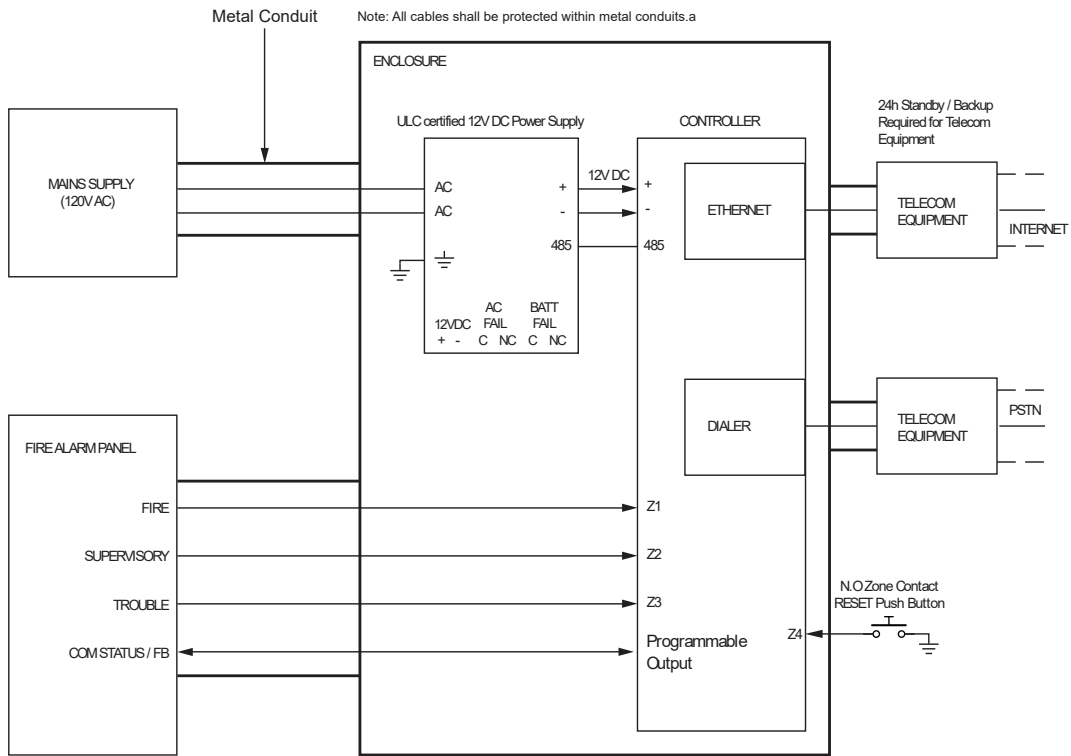
Typical Zone Circuits

EOL Resistor Zone Configuration		
Value 1	Value 2	Monitored Status
1K	1K	Open, Close, Tamper, Short
6K8	2K2	Open, Close, Tamper, Short
10K	10K	Open, Close, Tamper, Short
2K2	2K2	Open, Close, Tamper, Short
4K7	2K2	Open, Close, Tamper, Short
4K7	4K7	Open, Close, Tamper, Short



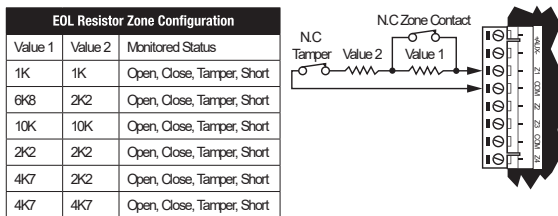
* EOL resistor must be installed at the Fire Alarm Control Panel Output.

CAN/ULC-S559
 CONTROLLER
 PASSIVE COMMUNICATION: MODEM DIALER



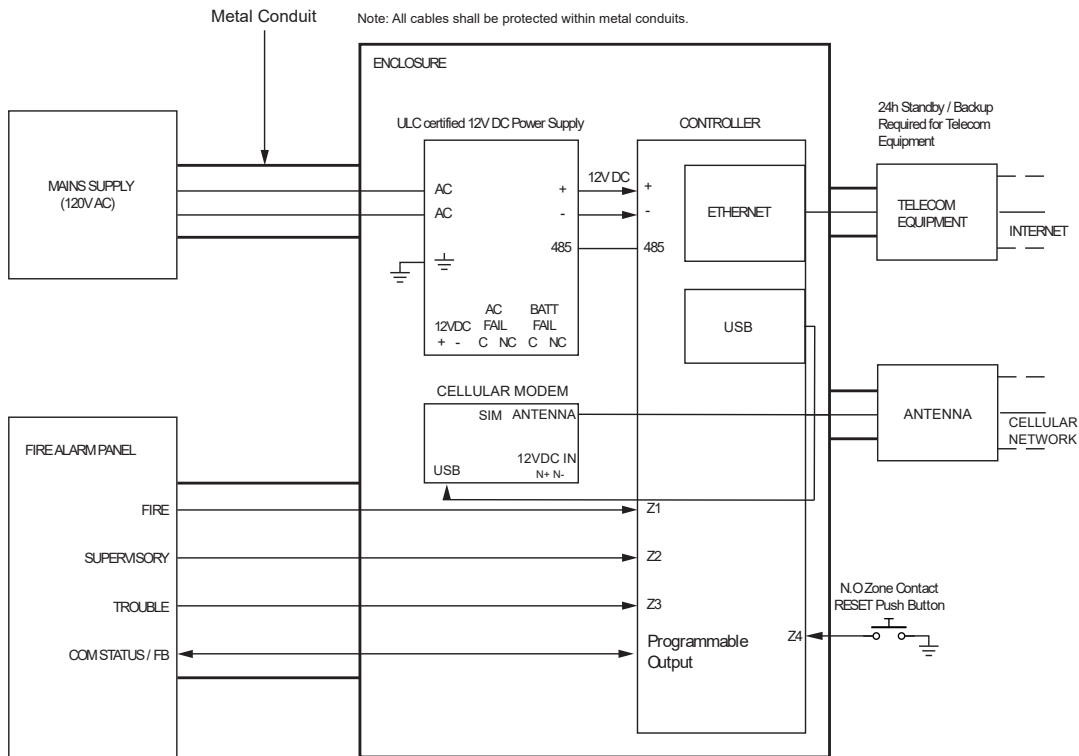
- * The AC FAIL output on the Power Supply MUST be programmed to follow the AC Trouble Input as follows:
 AC FAIL = OPEN on fail
- * Fire zones shall be separated from burglar zones through area partitioning.
- * Fire zones Z1-Z3 shall be used exclusively for fire monitoring and cannot be programmed to activate the bell output
- * Fire Zone Z4 N.O Push Button to be used as monitoring reset switch.

Typical Zone Circuits



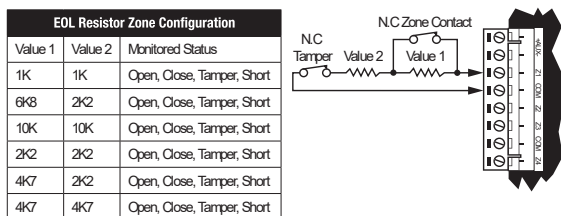
* EOL resistor must be installed at the Fire Alarm Control Panel Output.

CAN/ULC-S559
 CONTROLLER
 ACTIVE COMMUNICATION: CELLULAR MODEM



- * The AC FAIL output on the Power Supply MUST be programmed to follow the AC Trouble Input as follows:
 AC FAIL = OPEN on fail
- * Fire zones shall be separated from burglar zones through area partitioning.
- * Fire zones Z1-Z3 shall be used exclusively for fire monitoring and cannot be programmed to activate the bell output
- * Fire Zone Z4 N.O Push Button to be used as monitoring reset switch.

Typical Zone Circuits



* EOL resistor must be installed at the Fire Alarm Control Panel Output.

Fire area inputs must be programmed as follows:

- FACP Fire Alarm Signal input type must be programmed as Fire.
- Supervisory Trouble Signal input type must be programmed as 24 HR Silent.
- Trouble Signal input type must be programmed as 24 HR Silent.

Please refer to the section Inputs | Areas and Input Types in the Operator Reference Manual.

- All fire area inputs must be placed into an area and this area must be armed. Please refer to the section Inputs | Areas and Input Types in the Operator Reference Manual.
- COM Status

FACP system with a COM STATUS input must have this input connected to one of the dry relay contacts of the Relay1 or Relay2 outputs of the Protege controller and the selected output must be programmed as the Report OK output in the Contact ID Service.

Note: Any available dry relay contact on the Protege controller or output expander may be used for the FACP system, provided the selected output is programmed as the Report OK output.

Please refer to section Contact ID | Settings in the Operator Reference Manual.

- Fire inputs Z1-Z3 shall be used exclusively for fire monitoring and cannot be programmed to activate the bell output.

UL Compliance Requirements

UL1610

For Security Grade 4 installations, two forms of reporting are required. This can be satisfied using the onboard 2400bps modem included with the modem controller model, or through the incorporation of the PRT-4G-USB cellular modem module into the installation with the non-modem controller model.

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

Modem model only.

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

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

- The **Contact ID Reporting Service** must be enabled and the **Service Mode** must be configured to start with the operating system.
 - Refer to the section Contact ID in the Operator Reference Manual.
 - The **Report IP Service** must be enabled as the primary communication channel, the **Service Mode** must be configured to start with the operating system, and the **Reporting Protocol** must be set to ArmorIP.
 - Refer to the section Report IP in the Operator Reference Manual.
- When more than one means of signal transmission is used, loss of communication with the receiving system shall be annunciated at the receiver within 200 seconds. If a fault is detected on any of the signal transmission means, at least one of the signal transmission channels shall send a signal to the central-station to report the fault within 200 seconds.

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

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

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

- The **Poll Time** must be programmed to 40 seconds. Refer to the Report IP | General section in the Operator Reference Manual
 - The **Contact ID Reporting Service** must be enabled and the **Service Mode** must be configured to start with the operating system.
 - Refer to the section Contact ID in the Operator Reference Manual

- The **Report IP Service** must be enabled as the primary communication channel, the **Service Mode** must be configured to start with the operating system, and the **Reporting Protocol** must be set to ArmorIP.
- Refer to the section Report IP in the Operator Reference Manual.
- The **Trouble Input Area** must be armed in 24h mode. Refer to the section Trouble Inputs | Areas and Input Types in the Operator Reference Manual.

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

In the Protege system, the reporting service selected as Contact ID must have the number of attempts programmed to 5 attempts. The following options are required:

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

The event is sent with the following details:

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

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

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

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

FCC Compliance Statements

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

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

Operation is subject to the following two conditions:

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

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

Industry Canada Statement

ICES-003

This class A digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.

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

Disclaimer and Warranty

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

For warranty information, see our [Standard Product Warranty](#).

Submitted to UL 17-Jun-24

Designers & manufacturers of integrated electronic access control, security and automation products.
Designed & manufactured by Integrated Control Technology Ltd.
Copyright © Integrated Control Technology Limited 2003-2024. All rights reserved.

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