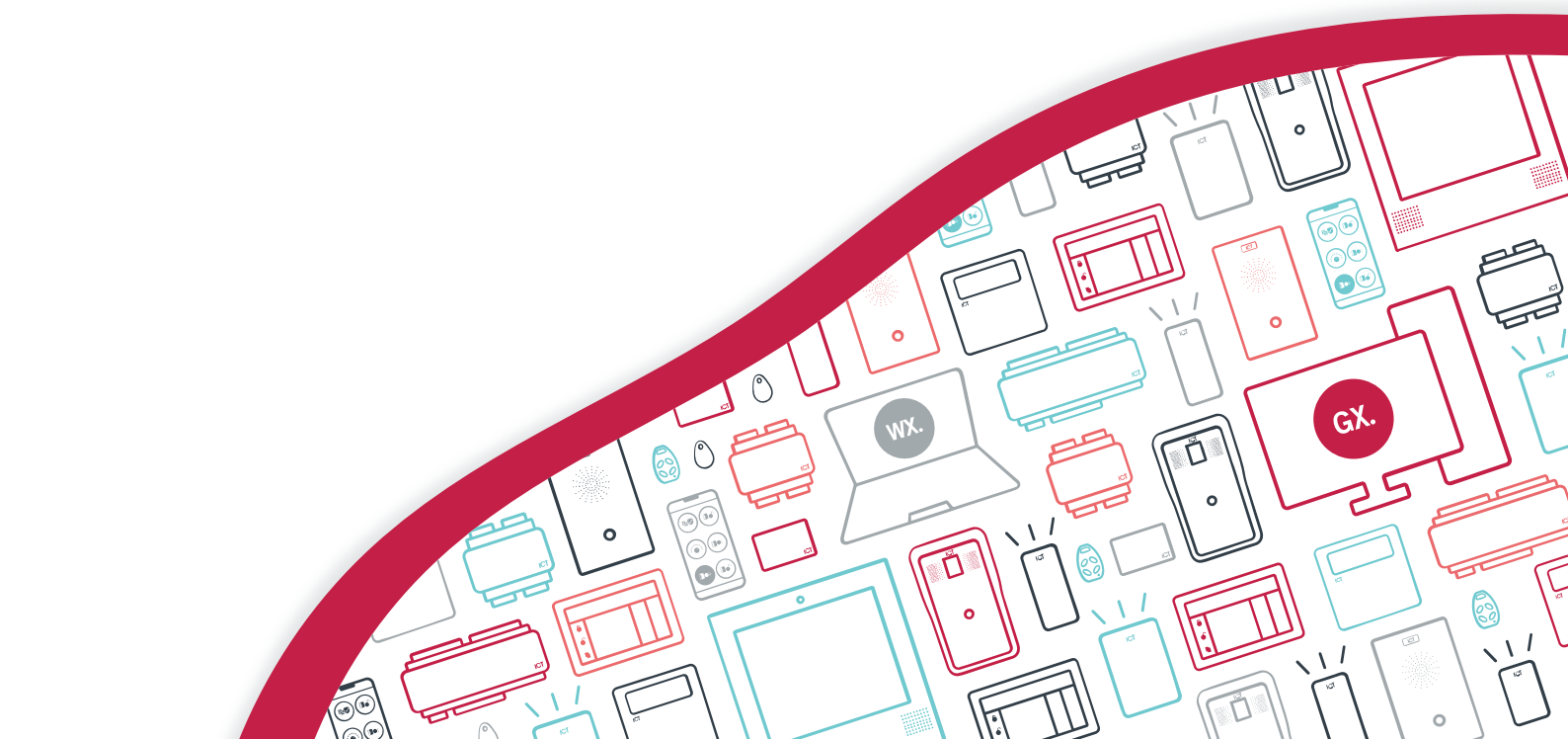
Protege GX / Protege WX

AS/NZS 2201.1:2007 Class 5 Compliance

Installer Guide



Last Published: 21-Jun-24 9:09 AM

Contents

Introduction

This manual outlines the required procedures for installing ICT Protege GX and Protege WX systems in compliance with AS/NZS 2201.1:2007 Class 5.

Personnel installing ICT systems must meet the following requirements to comply with AS/NZS 2201.1:2007 Class 5:

- Installers must be trained by ICT.
- Installers must be certified to AS/NZS 2201.1:2007 Class 5.
- Any installers carrying out the works must at minimum have an ACA Open Cabling Registration to install security cabling. Any individual and company must also hold certification from the equipment manufacturer that they are able to supply, install, commission and provide on-going warranty for the product being installed.
- The contractor and/or employee must also hold any relevant state or federal security industry licensing that may become required.

For specific installation information refer to the Installation Manual for each individual product (see page 28). For product programming reference information refer to the Protege GX or Protege WX Application Help or Reference Manual.

Refer to AS/NZS 2201.1:2007 for full details to confirm installation compliance. Standards are available for purchase online from:

- Standards New Zealand: https://shop.standards.govt.nz
- Standards Australia: https://www.standards.org.au

Heading numbers within this document refer to specific clauses within AS/NZS 2201.1:2007.

Compliance Documents

This document forms part of a suite of compliance documents. ASIAL's 'Class 5 Capability Certification' relies on ongoing compliance with:

- AS/NZS 2201.1:2007 by the manufacturer, installer and client.
- The equipment installation manuals and installer guide (this document).
- The equipment maintenance routine found in the controller installation manuals and installer guide (see page 20).
- The installer compliance statement.
- The client compliance statement.

1 - Scope and General

1.3 - Installer/Client Security Risk Assessment Prior to Installation

A risk assessment shall be conducted and documented by the installer in conjunction with the client. The classification of the intruder alarm system installation shall be selected from the following list with agreement from the client.

Risk assessment procedures shall follow the guidance provided by AS/NZS IEC 31000 Risk Management – Principles and Guidelines and AS/NZS IEC 31010 Risk Management – Risk Assessment Techniques.

All references to the requirements for the intruder alarm system installation refer to basic minimum requirements and the designers/installers of such a system should take into account the nature of the premises, the value of the contents, the degree of risk of intrusion, the threat to personnel and any other factors which may influence the choice of grade and content of such a system.

Security Risk Profile

Likelihood of Attack	Consequence of Attack				
	Minimal	Minor	Moderate	Major	Catastrophic
Very Likely	Class 2*	Class 3	Class 4	Class 5**	Class 5**
Likely	Class 2*	Class 3	Class 4	Class 5	Class 5**
Possible	Class 2*	Class 3	Class 3	Class 4	Class 5
Unlikely	Class 1*	Class 2*	Class 3	Class 4	Class 5
Very Unlikely	Class 1*	Class 2	Class 3	Class 4	Class 5

***** Class 1 and 2 are not in the scope of the ICT Protege GX or Protege WX system.

****** Risks in these cells cannot be addressed by an intruder alarm system alone.

Different areas within a single site may be different Classes. For example, a reception area might be installed at Class 3, while a vault or server room on the same site must be installed at Class 5. This is acceptable as long as the different spaces are monitored separately (i.e. different areas in the Protege system) and separately comply to the relevant standard.

2 - System Installation Requirements

2.2 - System Installation Requirements

2.2.1 - General

All equipment shall be installed in accordance with:

- The manufacturer's instructions (refer to the relevant product installation manual (see page 28))
- The standard AS/NZS 2201.1:2007
- The local Authority Having Jurisdiction (AHJ)
- Any other applicable standards necessary for a compliant installation

Mains Supplies

The switchboard circuit breaker from which power for the security systems is obtained shall be labeled as follows: `SECURITY SYSTEM - Do not switch off`.

The enclosure shall be wired with the mains entering from the rear, or via a metal conduit mounted in one of the knockouts on the side walls of the cabinet.

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

The electrical hazard warning sticker supplied with the Power Supply shall be applied to the cabinet internal cover of any enclosure containing a Power Supply.

2.2.2 - Control Equipment and Power Supply Location

Unless otherwise approved by the client in writing, the Protege modules, including the Power Supply, are intended to be mounted within ICT enclosures installed inside the protected premise, and are not to be mounted on the exterior of a vault, safe or stockroom.

Where practicable, the enclosures or modules shall not be visible outside the alarmed area.

2.2.3 - Mounting

All components shall be correctly mounted according to the instructions provided in the product manuals to minimize the risk of interference or damage.

All components and enclosures mounted to masonry shall be fixed in position using corrosion-resistant plugs or masonry anchors. All components and enclosures mounted to plaster board shall be fixed in position using purpose-designed corrosion-resistant wall anchors suitable for the weight loading.

Where possible, at least two fixings shall be made into one or more timber or steel studs. Bolts or machine screws, washers and anti-vibration devices shall be used where necessary for fixing into metal. Corrosion-resistant bolts, screws and washers suitable for the environment shall be used.

2.2.4 - Tamper Detection

ICT steel enclosures are fitted with a tamper switch, which is activated by opening the door and/or attempted removal from the wall. This switch shall be wired into the dedicated 24HR Tamper Alarm input terminal, TP, on the Power Supply, or any other system input designated and programmed as a 24HR Tamper Alarm.

To comply with Class 5, the enclosure must also be fitted with a DSC SS-102 Shockgard seismic vibration sensor. For more information, see Appendix 1 - Enclosure and Pre-tamper (Vibration) (page 26).

2.2.5 - Power Supply Equipment

Power Supply equipment and indicators shall be housed integrally with the control equipment or in separate enclosures conforming to the enclosure requirements of Clause 3.7 (see page 14). This excludes AC step-down transformers and solar cells, which may be mounted remotely.

ICT's range of enclosures are constructed from steel 1.2mm thick.

2.2.6 - Battery Marking

Each battery in the system must be legibly and indelibly marked with the month and year of installation. This information must be entered into the system site logs or maintenance records.

2.2.7 - Alarm Transmission Equipment

Should the alarm transmission equipment be housed in a separate enclosure, the enclosure shall comply with the enclosure requirements of Clause 3.7 (see page 14).

2.3 - Detection Devices

2.3.1 - General

Detection devices shall be installed in accordance with the manufacturer's requirements and AS 2201.3. The security alarm company shall make every reasonable effort to select the correct number, type and placement of detection devices to mitigate the agreed risk profile, selected in accordance with Clause 1.3 (see page 6).

The location of devices shall be carefully considered to minimize false detection signals.

2.3.2 - Inputs (Zoning)

Individual or addressable inputs (zones) shall be provided for each:

- Powered electronic detection device (e.g. movement detectors)
- Unpowered detection device (e.g. electromechanical devices such as reed switches)

However, a single input may be provided for multiple devices that are installed on common adjacent detection points (e.g. double doors or multiple windows within the same frame).

2.3.3 - End-of-line Supervision (EOL)

Where possible, EOL components or devices shall be terminated within detection devices. If this is not practical, they shall be terminated within a suitable junction box located immediately adjacent to the detection devices. Class 5 requires active end-of-line for EOL to be used.

The Protege Single Input Expander (PRT-ZX1) fulfills this requirement by means of secure encrypted RS-485 module communications.

The junction box shall also be fitted with tamper detection devices meeting the requirements of Clause 3.16.3.5 and the interconnecting cables shall not be visible.

2.4 - Audible Warning Devices

Audible alarms shall sound as required in response to an audible alarm output being generated by the control equipment and shall meet the requirements of Clause 3.16.2.9 (see page 16).

Class 1 and Class 2 installations are not in the scope of the ICT Protege GX or Protege WX system.

Note: Local laws may restrict the sound pressure level and duration differently from those specified in Clause 3.16.2.9.

2.5 - Environmental Conditions

2.5.2 - Special Environmental Conditions

The design and construction of the installation shall ensure that the reliability of the system is not compromised if any equipment, material or wiring is located in a position where it may be exposed to dampness, corrosion or other special conditions.

Where flammable or explosive gas or dust are reasonably expected to be present, any equipment installed shall comply with the requirements of the appropriate Australian/New Zealand standard(s) for equipment in use in such hazardous conditions.

HB 13: Electrical equipment for hazardous areas

As well as mandating AS/NZS 3000 Wiring Rules, the Electricity (Licensing) Regulations 1991 also mandate other standards, including AS/NZS 2381 (Electrical equipment for explosive atmosphere) and AS 2430 (Classification of hazardous areas). Clause 7.9 of the Wiring Rules outlines the special requirements for installation in hazardous areas.

The means by which areas are classified as hazardous are specified in AS 2430.1, AS/NZS 61241.3 and AS/NZS 2430.3. These standards relate to areas that are classified as being hazardous due to the presence of flammable gases and vapors and combustible dusts.

The electrical apparatus which is installed in hazardous areas must comply with AS/NZS 2381 and AS/NZS 61241.1.2 in terms of its selection and installation.

Where more than one code or regulation is applicable, the more stringent shall apply. It is the contractor's obligation to ensure that local, national or federal standards are met where applicable.

2.6 - Wiring

2.6.1 - General

Cable installation, identification and termination shall be performed in accordance with the manufacturer's technical installation guidance, in addition to the application codes ACIF S009, AS/NZS 3000 and the requirements of the relevant regulatory authorities.

In the absence of the manufacturer's recommendations on conductor application, the contractor shall ensure that the cable selected meets all technical requirements of the equipment to be installed.

Where practicable, wiring should be concealed, to reduce the risk of attack or damage. All cables should be run as a single cable run and terminated at either end to the control and remote equipment. Where a join cannot be avoided, a junction box must be used and clearly shown on the 'As Built' drawings.

This Clause refers to wiring with copper conductors, but does not exclude the use of other conductors, fiber optics or radio waves for the transmission of signals.

2.6.2 - Type of Wiring

(a) Minimum rating for wiring

Wiring shall have a total cross-sectional area not less than 0.20 mm^2 and an outer sheath insulation rating not less than 300 V RMS. Conductors shall be stranded, except for coaxial cables which may have a solid core.

For Class 3 systems and above the following applies:

- For single core and figure-eight cables, conductors shall have a minimum of 24 strands of diameter 0.20 mm.
- For multi-core shielded cables (three or more conductors), conductors shall have a minimum of seven strands of diameter 0.20 mm.
- For multi-core non-shielded cables (three or more conductors), conductors shall have 14 strands of diameter 0.20 mm.

(b) Load sizing

Wiring cable size must meet the minimum codes of practice for commercial security or low voltage installation. The larger cable specified shall apply. All data or instrumentation cable must be run in the maximum gauge possible and be an overall shielded type.

Cable sizing shall be sufficient to ensure that voltage drop is minimal. The voltage drop in the wiring runs shall not be enough to reduce the terminal voltage at the devices to 10% above the lower limit stated by the manufacturer.

(c) Open wiring

Open wiring, such as along walls, shall be supported by clips at distances not exceeding 500 mm. Segregation from other services shall be maintained to ensure works comply with the relevant standard. If required, additional supporting saddles, cleats, clips or insulators shall be provided. Wherever possible cabling shall be installed on cable tray or attached to dedicated catenary wires.

If exposed to view, install conduits in parallel runs with right angle changes of direction.

ICT recommends that open wiring should be permissible in enclosed, secure spaces under the floor, in the ceiling and wall cavities and on cableways only.

(d) Wiring within ceilings and under floors

Cables shall be supported at intervals not exceeding 1000mm using catenary wires or approved dedicated hangers fixed to the ceiling or under floor structure. Cabling shall not be secured to hangers provided by other services, pipes, ceiling rods, or other non-structural supports.

Cables shall be neatly grouped together such that cables do not rest at any point on the topside of the false ceiling, lighting fittings or other heat producing equipment.

Where tile ceiling support systems are utilized, PVC/PVC cable shall be fixed at intervals not exceeding 300mm in all spaces greater than 600mm deep. In spaces less than 600mm deep, PVC/PVC cables may be fixed at intervals not exceeding 1000mm.

Wiring shall be segregated from other wiring and electrical cables as specified in ACIF S009 or relevant requirements of the New Zealand Ministry of Economic Development (Radio Spectrum Management (RSM) Division).

(e) Flexible wiring

Where wiring is required to be attached to hinged or movable doors or windows, conductors shall be insulated, flexible and resistant to fracture.

For doors, a Power Transfer Module (commonly referred to as an EPT or PT) should be considered. This provides a flexible conduit hidden within a pocket that is concealed within the hinge side of the door. Power Transfers protect the wiring and allow larger gauge wires for powering door hardware.

Cable transfer devices must comply with the following minimum:

- Lockwood LC8810/11 lead covers, including a door recess box or approved equivalent. Cable transfer hinges, curly cord or exposed cable transfer units are not suitable.

  Note: If the opening angle of the door is more than 120° or the distance between hinge and doorframe is greater than 20mm, provide Lockwood LC8811 lead cover.

Flexible conductors shall comply with Clause 2.8 (see page 12).

2.6.3 - Stress on Conductors and Terminals

Cables shall be installed in a workmanlike manner parallel to walls, floors and ceilings as applicable. They shall be neatly loomed and cable tied to the catenary cable or enclosed in a conduit, tray or ducting. Install cables in a manner to eliminate the possibility of strain on the cable itself or on cable terminations.

2.6.4 - Protection of Wiring

Before commencing any works, the contractor shall refer to detailed design documentation for any project specific requirements regarding protection of wiring.

The cable shall be selected to ensure any adverse conditions such as, corrosion, heat, weather, mechanical damage, fumes etc., are adequately catered for. Wherever possible cabling shall be installed on cable trays or attached to dedicated catenary wires. Segregation from other services shall be maintained to ensure works comply with the relevant standard.

Where liable to damage, or exposed to weather, wiring shall be adequately protected by conduits, piping, ducts or cover strips, in accordance with ACIF S009 or the requirements of the relevant regulatory authority.

Additional wiring protection must be applied in the following cases:

- **Wiring to control equipment and external alarms**: For connection to control equipment and external alarms, wiring shall be arranged so that the wiring passes directly through the wall via ducting or conduits into the rear of the enclosure. Where this is not possible, the exposed wiring from the control equipment and external alarms must:
  - contain or incorporate a monitored circuit with a level of supervision in accordance with the classification of the system (e.g. Class 5 systems should follow Clause 3.16.6); and
  - be encased by conduit complying with AS/NZS 2053.1, piping or one-piece duct.
- **Wiring between buildings**: Aerial, underground and surface wiring between buildings and to external detection devices shall be installed in accordance with the appropriate provisions of ACIF S009 or relevant regulatory authority. It shall also meet the requires for Wiring to control equipment and external alarms above. In addition, aerial cables shall have surge protection devices in accordance with AS/NZS 1768(Int).

2.7 - Jointings

All cables should be run as a single cable run and terminated at either end to the control and remote equipment. Where a join cannot be avoided, joints should be concealed or must be contained in a junction box to reduce the possibility of tampering.

Joints between fixed wiring and flexible connections shall be mechanically supported to prevent acute bending or breakage of the conductors and clearly shown on the 'As Built' drawings.

All joints shall be mechanically and electrically sound, and shall be of one of the following forms:

- **Soldered joints**: The conductors shall be mechanically connected and soldered. The finished joint shall be covered with heat shrink to fully insulate each termination point. Heat shrink shall be installed for non-structured cabling as follows:
  - At each cable core and termination point
  - Across the main cable sheath of multi-core cables to fully insulate the cable termination and provide a secure cable connection
  - As directed by the Site Supervisor following inspection of the cabling and cable termination onsite
  - Application of the heat shrink shall not show any evidence of:
    - Ruptures, melting due to excess heat or breakages in the insulation provided by the heat shrink
    - Exposed cable cores, terminations of the outer cable sheath
    - Loosely applied heat shrink which does not form a secure connection or insulator
- **Clamped joints**: The conductor shall be secured in accordance with Clause 2.9 (see next page).

2.8 - Flexible Conductors and Connections

Movable parts of the alarm system shall be connected by flexible, fracture-resistant conductors that meet the following specifications:

- **Stranded construction**: Consisting of a total cross-sectional area of not less than 0.5 mm^2 and at least 16 strands of annealed high conductivity oxygen-free copper. Insulation shall be PVC or better, complying with the requirements for Grade V-75 of AS/NZS 3191 and having a minimum nominal radial thickness of 0.4 mm.
- **Tinsel construction**: Consisting of two or more cadmium-copper tapes evenly lapped on a suitable core of natural or synthetic fiber not less than 0.75 mm diameter, with a maximum resistance of 1.1 Ω/m at 20°C and a minimum breaking load of not less than 89 N. Insulation to be PVC or better, complying with the requirements for Grade V-75 of AS/NZS 5000.1 and having a nominal radial thickness of at least 0.18mm. Tinsel wires shall not be soldered.

  Note: The use of other flexible conductors, such as flexible printed circuit boards and flexible ribbon cable, is permitted if they comply with the requirements for the standard types above.

2.9 - Terminations

(a) Terminals

There shall be no loose wire strands or nicked or damaged wires. Wire strands shall be securely fastened.

Termination of all cables to equipment that requires a screw clamp, rising clamp or push to clip connection shall use a termination lug. The termination lug must comply with the manufacturer's technical installation guidelines and be of suitable gauge and size, meeting the requirements of Clause 3.8.

(b) Crimped

It is recommended that a strain relief type boot lace ferrule or pin clip device suitable for the size of conductor which requires manual crimping is used.

It is preferred that all installations and termination be made with a LeGRAND® ratchet type automatic termination tool, which cannot be released until the crimp is completed.

Crimped joints shall be used only on stranded cables.

(c) Plugs and Sockets

All ICT DIN Rail products are provided with keyed plug and sockets so that connections can only be made in one position.

(d) Soldered joints

Any connections requiring soldered joints shall be soldered using lead free solder and non-corrosive flux. ICT recommends RoHS lead free SN100C solder wire with no clean flux cores.

When soldering internal conductors, terminals, lugs, etc., the solder shall provide a good electrical bond between the conductor and the tag. Soldered terminations shall meet the following requirements:

- The solder is supported and held in position independently of the soldered joint
- Prior to soldering, the joint is mechanically sound
- The soldered joint shall not be subject to mechanical stress
- Care has been taken to avoid damage to the insulation and shorts caused by excessive solder
- No excess solder remains on the connection
- No solder droppings are left on or about the work

(e) Self-locking terminals or connectors

Connectors supplied with ICT products are of the self-locking type. Other connectors supplied or used within the system must also be of the self-locking type.

Conductors being terminated into screw or rising terminals must be correctly sized to match.

Stranded conductors being terminated in connectors designed for solid wire shall first be fitted with a soldered or, preferably, crimped ferrule of the correct size for the situation.

2.10 - Wire-Free Links

Not applicable. The system does not contain wire-free links.

2.11 - Commissioning

Following installation, all systems shall be completely commissioned by an engineer/technician with the appropriate qualifications to audit and give a certificate of compliance for the project.

Arrange with the client an appropriate time to perform the initial commissioning. In addition, if the system is being monitored, notify the alarm monitoring company before any testing begins so that they can place the system 'on test'. The monitoring center shall verify that the appropriate events are being communicated, interpreted and processed correctly.

The tests as a minimum shall include a full maintenance check as outlined in Section 5 (see page 20), including out of hours tests, to demonstrate the system's performance. The commissioning shall include:

- Testing of system components for correct function and operation.
- Demonstration that devices perform on site to at least the level stated in the manufacturer's performance specification for each device.
- Testing of the operation of alarm sectors and panel functions.
- Demonstration that the system functions under mains fail conditions.
- Demonstration of the operation of the battery and charger. This shall include, if possible, a full discharge/recharge over the designated time.

2.12 - Client Training

Following the successful commissioning of the system, client training can be carried out by qualified/certified personnel.

3 - Equipment Requirements

ICT system control and peripheral equipment comply with the requirements of this section.

The environmental operating conditions (see Clause 3.3) for each piece of equipment can be found in the relevant installation manual, in the Technical Specifications section. Below is a guide to standard environmental requirements:

- **Indoor Equipment**
  - **Environment IP Rating**: IP40
  - **Operating Temperature**: -10° to 55°C (14° to 131°F)
  - **Storage Temperature**: -10˚ to 85˚C (14˚ to 185˚F)
  - **Humidity**: 0%-93% non-condensing, indoor use only (relative humidity)
- **Outdoor Equipment**
  - **Environment IP Rating**: IP65
  - **Operating Temperature**: EU EN -40° to 70°C (-40° to 158°F)
  - **Storage Temperature**: -10˚ to 85˚C (14˚ to 185˚F)

ICT equipment is compliant with the relevant Australian and New Zealand EMC Standards (Clause 3.4) and meets the requirements of EN 55024 (now EN 55035) for immunity (Clause 3.5, tested and certified to the accepted EN 50130-4).

3.2 - Additional Functionality

The Protege system performs a wide range of functions in addition to intruder detection, such as access control, fire detection and building automation. Where the system is used for additional functions, it shall comply with the relevant Australian or New Zealand standards applicable to those functions.

3.7 - Enclosures

ICT DIN rail system components are intended to be mounted within the ICT range of attack resistant, powder coated, IP50 rated 1mm thick steel enclosures.

Other critical or vulnerable components must also be housed in protective enclosures of 1mm thick steel or 3mm polycarbonate.

3.10 - Instructions

General installation requirements for compliance with AS/NZS 2201.1:2007 Class 5 are available in this manual. Specific setup and installation details of ICT system components can be found in their respective installation manuals, which also include basic programming and operating information.

For full programming and operating instructions, see the Protege GX Operator Reference Manual or Protege WX Programming Reference Manual, or the Application Help.

3.11 - Power Supplies

The power supply for the system consists of a PSU (Power Supply Unit) or PSUs suitably sized to satisfy the system operating requirements. Any combination of ICT DIN Rail Power Supplies is permitted. These are available as 12V 2A, 4A and 8A.

The system Power Supply performance (as regards Clause 3.11.2) must be able to supply continuous, steady voltage within the range of –15% to +2% of the Power Supply's nominal output voltage under all current loads demanded by the system when operating on an external supply source. The Power Supply must be able to maintain the system when operating from battery power for the period specified in Table 3.14.2(A) or (B) as applicable.

Each PSU must include a battery that is suitably sized for the system to allow normal operation. Batteries shall comply with Clause 3.14 (see below). The backup battery must be capable of supplying enough power for the equipment to perform its designed function for at least two complete alarm sequences relevant to the equipment being powered at any time within the specified period.

ICT DIN Rail Power Supplies comply with all points of Clauses 3.11 and 3.12, providing low battery reporting (3.11.3) as well as automatic battery testing and fault reporting (3.11.4). Automatic battery health testing is performed every 10 minutes, providing indication and fault reporting. Battery charging is integral with the PSU (3.11.5, 3.11.6).

3.11.7 - Mains Supply Isolation Switch

The power supply shall be supplied by a dedicated electrical power source and have a dedicated circuit breaker. Do not use a switch controlled breaker or a switched electrical point to supply electrical power.

When the mains supply is installed in the enclosure as advised in section 2 (see page 7), a key and (optionally) a screwdriver are required to gain access to the mains connection.

3.12 - Power Supply Indications

The system shall indicate the current status of the mains supply and battery, and shall be configured to transmit any faults to the offsite monitoring center.

- **3.12.1 - Mains Indication**: The power indicator on the face of the Power Supply indicates whether the correct module input voltage is provided from the mains supply.

  The Mains Failure trouble input for each Power Supply shall be programmed into a system area which is monitored by a reporting service. When there is a mains failure, the trouble input will open and a 24HR alarm will be reported to the monitoring station.
- **3.12.2 - Charging Indication**: Not applicable, as Power Supplies are always connected to mains supply.
- **3.12.3 - Battery Indication**: The battery indicator on the face of the Power Supply indicates whether the battery is connected and functioning correctly. In addition, when the mains are disconnected and the battery is in use, it indicates whether the battery is low or normal.

  The Battery Low / Missing trouble input for each Power Supply shall be programmed into a system area which is monitored by a reporting service. When the battery is disconnected, low or faulty, the trouble input will open and a 24HR alarm will be reported to the monitoring station.

3.13 - Marking of Power Supply Equipment

Protege Power Supplies are supplied with a sticker label containing the following information:

- Name of manufacturer
- Model number of equipment

Further, the following information shall be clearly and indelibly marked on all modules:

- Input and output supply voltages, frequency and power or current
- Approval number(s)
- Type and capacity of replacement battery

3.14 - Battery Requirements

Batteries shall comply with the applicable Australian and/or New Zealand Standards.

The battery capacity required shall be calculated based on the size of the system.

Acceptable battery types include any 12 VDC VRLA battery designated for security use and equivalent to the Yuasa NP range. For example, Panasonic 12V DC VRLA battery LC-R, LC-RA, LC-XD, LC-P, LC-X, Redlite 12V7Ah VRLA Battery, etc.

3.16 - Equipment Classification

3.16.1 - General

This Clause specifies the requirements for all equipment.

References to control equipment also include any part of an intruder alarm system that controls or extends the capabilities of the control equipment, whether housed in the same enclosure or located remotely (e.g. Input Expanders, Output Expanders, etc.).

The classification of a system shall be the lowest classification of the equipment used in the system. To qualify as a Class 5 system, the system must meet the requirements of all lower classifications as well as those for Class 5.

3.16 - Requirements for Class 1-4

The following requirements apply to Class 1-4 installations and must be met in any Class 5 installation. The highest applicable standard for each category has been outlined here, as defined in Clauses 3.16.2-5.

Alarm Input Speed (Input Debounce)

To comply with 3.16.2.2, ICT control equipment must not be set to generate an alarm condition where the signal on any wired input (zone) lasts less than 100ms. The system shall generate an alarm condition in response to an uninterrupted signal lasting longer than 400ms.

The system default for the Alarm Input Speed is set to 500ms, adjustable up to 1 hour.

Input (Zone) Indication

The Protege system complies with the requirements for Clause 3.16.2.3 for input indication. Keypads connected to the system give visual and audible indications in the following situations:

- When an input is open (alarmed) during the arming process.
- When an input is bypassed (isolated) during the arming process.
- When an input is opened (alarmed) while the system is armed.

Further visual and audible indications for each function can be programmed by the installer as required.

To comply with Clause 3.16.3.3, a report shall be sent to the monitoring station when an area is armed with bypassed inputs, unless the client specifies otherwise in writing.

Alarm Processing

In compliance with Clauses 3.16.2.4 and 3.16.3.2, any area in the system can be armed for processing alarm conditions or disarmed to disable alarm processing (with the exception of system troubles and 24HR tamper conditions).

When arming, open inputs can be bypassed (isolated) temporarily. In this state the alarm condition will not be processed until the area is disarmed. This must be carried out manually by an authorized user or software operator.

In addition, areas can be stay armed (partial armed) so that alarms are not processed in a predefined set of inputs.

Alarm Warning Devices

To comply with Clause 3.16.2.9, alarm warning devices connected to the system must comply with the following requirements:

- **Audible alarm devices**:
  - Sound pressure level shall not be less than 90 dB(S) or greater than 130 dB(A) when measured from 1 metre.
  - The audible alarm shall not sound for a period longer than 5 minutes.
  - After timing out, the audible alarm shall not sound again until the area is disarmed and rearmed, or unless an alarm is generated in a different area.

    This requires specific programming. For a programming example, see Appendix 3 (see page 35).
- **Visual alarm devices**:
  - A visual warning device in the form of a flashing blue light shall be used in addition to the audible warning device.
  - This shall be activated when the audible alarm device is activated and may remain in operation beyond the duration of the audible alarm.
  - It shall be located outside or be visible from outside the area, in a location that minimizes the risk of incidental or deliberate damage.
- **Satellite sirens**:
  - Use of satellite sirens (alarm devices with integrated power supplies) is optional.
  - The power supply and battery used shall comply with the relevant provisions of Clauses 3.11-3.14 (see page 14).
  - Any wire links to the control equipment shall be monitored in accordance with Clause 3.16.2.2 or higher (see below).

The requirements of local legislation shall be followed if they differ from the above.

Tamper Detection

In compliance with 3.16.3.5, tamper detection devices shall be used with all control equipment enclosures, audible alarm device enclosures and remote arming stations that use relay contact outputs or similar. These shall be configured to generate a system alarm when tampering is detected, which must be reported to the offsite monitoring station except during maintenance (3.16.4.4).

In addition, for Class 4 compliance and above, an early warning tamper detection device is required in the control equipment enclosure.

For more information, see Appendix 1 - Enclosure and Pre-tamper (Vibration) (page 26).

Locking of Equipment Enclosures

To comply with Clause 3.16.5.7, all equipment enclosures shall be fitted with a camlock using a restricted key system that is protected by patent. Written authorization is required for the key to be replicated.

The installer must supply an M20x17mm flat type equivalent size camlock that meets the above requirements. The camlocks supplied with ICT enclosures are not sufficient.

3.16.6 - Class 5

The following system controllers meet the requirements for a Class 5 classification:

- Protege GX DIN Rail Integrated System Controller - IP only (PRT-CTRL-DIN-IP)
- Protege GX DIN Rail Integrated System Controller (PRT-CTRL-DIN)
- Protege WX DIN Rail Integrated System Controller - IP only (PRT-WX-DIN-IP)
- Protege WX DIN Rail Integrated System Controller (PRT-WX-DIN)
- Protege GX DIN Rail Single Door Controller (PRT-CTRL-DIN-1D)
- Protege WX DIN Rail Single Door Controller (PRT-WX-DIN-1D)
- Protege GX DIN Rail Single Door Controller with PoE (PRT-CTRL-DIN-1D-POE)
- Protege WX DIN Rail Single Door Controller with PoE (PRT-WX-DIN-1D-POE)

A full list of system components that meet the requirements for a Class 5 classification can be found in Appendix 2 (see page 28).

3.16.6.1 - General

In additional to the requirements for Class 1-4, or superseding them as applicable, the requirements of Clauses 3.16.6.2 to 3.16.6.5 apply to Class 5 equipment.

3.16.6.2 - Input (Zone) Supervision

All wired detection circuits such as door contacts, PIR sensors etc. are required to be continuously monitored using an active end-of-line module. Each input is a four state input capable of generating open, closed, tamper and short conditions.

The Protege Single Input Expander (PRT-ZX1) fulfills the requirements for active supervision and encryption by means of secure encrypted RS-485 module communications.

Only inputs wired to PRT-ZX1s are Class 5 compliant.

3.16.6.3 - Arming and Disarming

The Protege controller provides the means of on site disarming via RFID reader, keypad and/or biometric recognition system. Communication between each arming station and the control equipment is over a proprietary high speed protocol across an encrypted local area network and AES encrypted proprietary RS-485 module network. For active communications channel security, encryption is always enabled. The system allows the use of up to AES-256.

The recommended method of disarming for Class 5 systems is use of both a card or equivalent credential with a minimum of 900,000 combinations and a PIN of at least 6 digits in length (supports up to 8 digits).

This can be configured by enabling the **Keypad Login Requires Card** option (**Expanders | Keypads | Options 2**) and setting the **Reader 1/2 Keypad Type** to LCD Keypad (**Expanders | Reader Expanders | Reader 1/2**).

The Standard requires, at a minimum, use of a PIN or credential with at least 1000 unique combinations.

In addition, keypads used for disarming shall be configured with the **Lock Keypad on Excess Attempts** option enabled, such that it will only accept a maximum of 6 incorrect PIN attempts (default is 3 attempts). If this limit is met, the following shall occur:

- The keypad will not accept any further PIN attempts for at least 1 minute.
- The Too Many Attempts trouble input will be opened. This shall cause a system alarm and be reported to the offsite monitoring station.

3.16.6.4 - Remote System Access

Communication is over a proprietary high speed protocol across an encrypted local area network and AES encrypted proprietary RS-485 module network. For active communications channel security, encryption is always enabled. The system allows the use of up to AES-256.

3.16.6.5 - Alarm Transmission Equipment

Protege controllers comply with the requirements of AS 2201.5 for Class 5 transmission systems. For an example of compliant settings for an IP reporting service, see Appendix 3 (see page 36).

4 - General Operational Procedures and Responsibilities

4.1 - General Responsibilities

The installer will provide the following to the client at the time of system commissioning. Examples of this 'handover' documentation can be found in the additional documents provided by ICT.

- Site documentation in accordance with Clause 6.1 (see page 24).
- A maintenance log in accordance with Clause 6.2 (see page 24) and logbook in accordance with Clause 6.4 (see page 24) to record all visits, maintenance and works by the attending technician.
- Instructions for the correct operation of the system, including arming and disarming methods.
- Adequate training and demonstration of the system operating procedures.
- An adequate operating and maintenance manual in plain English covering the entire intruder alarm system as installed.
- A list detailing all detection devices, their physical locations and the system input that they correspond to.
- If the intruder alarm system allows authorized remote access for maintenance or operation, written advice about how and why this will be accessed.
- Details of all applicable warranties.
- Written maintenance instructions in accordance with Section 5 (see next page).
- Written advice of the client's responsibilities as per Clause 4.2 (see below).
- A completed and signed installer compliance statement. This document is provided by ICT as the ICT Class5 Installer Compliance Statement.

4.2 - Client Responsibilities

The installer will notify the client of their responsibilities in the handover documentation, as per Clause 4.2. The responsibilities of the client are as follows:

- Ensuring that all users of the intruder alarm system have appropriate training in its operation.
- Ensuring that the intruder alarm system is operated correctly and in accordance with the procedures agreed with the security alarm company.
- Ensuring that all detection devices are tested at least once per month (if practicable).
- Ensuring that the system remains in compliance with this standard. If the system is faulty or unable to perform its intended function for whatever reason, the client shall request that the security alarm company make appropriate changes to return the system to compliance.
- Completing, signing and retaining a client compliance statement. This document is provided by ICT as the ICT Class5 Client Compliance Statement.

5 - Maintenance and Service

ICT recommends regular maintenance and testing of Protege systems. AS/NZS 2201.1:2007 specifies that maintenance inspections for Class 3-5 systems must be carried out at least once every 12 months.

Any service preformed shall be recorded in the client's maintenance logbook (see page 24).

Peripheral Devices

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

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

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

Testing Frequency

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

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

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

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

Recommended Routine Maintenance Procedures

Preliminary Procedures

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

On Site Maintenance Procedures

Task	Frequency	Description
Check the equipment schedule and/or maintenance sheets	Once per year	Check the installation, location and siting of all equipment and devices against the 'as-built' documentation. Record and report any discrepancies.
Check wiring and cable protection	Once per year	Visually inspect all wiring and cable protection systems (conduits, trunking, etc.). Record any damage or deterioration.
Check for dust, moisture and vermin	Once per year	Check all equipment enclosures for dust, moisture, condensation and vermin. If excessive moisture or foreign matter is present, clear this out of the enclosure and take steps to prevent future accumulation.
Check the power supply	Once per year	Check that all power supplies are properly connected to a mains outlet and are operational.
Test the power supply DC output voltage	Once per year	Disconnect the backup batteries and test the DC voltages across the V+ and V- output terminals on all power supplies. The recommended voltage range is **12.4 - 14.0 VDC**.
Test expander module DC output voltage	Once per year	Test DC voltage across the V+ and V- output terminals on Protege controllers, input expanders and output expanders. The recommended voltage range is **10.4 - 14.0 VDC**.
Check battery connections	Once per year	Check that all power supplies have batteries fitted and connected correctly to the B+ and B- terminals, and that the batteries and connections show no visible signs of corrosion.
Test battery charge voltage	Once per year	Test the DC voltage across the B+ and B- terminals of all power supplies. The recommended voltage range is **13.4 - 13.8 VDC**. Note: When the mains power is restored following an AC fail condition, the battery charge voltage may fluctuate between **10.0 - 13.8 VDC** while the battery is recharging.
Replace battery	Once per 3-5 years, or as specified by the battery manufacturer	Replace each power supply battery as required with another of equivalent or better specifications. Record the installation date of the new battery in the system maintenance records and in a clearly visible location within the equipment enclosure or on the battery itself.
Check keypad keys	Once per year	Check the operation of every key on the keypad, that all keys are clearly legible and that the keypad backlighting is operational.
Check keypad display	Once per year	Check the operation of the keypad display to ensure that all characters display correctly on the screen and that the backlight is operational and at the correct brightness.
Test the primary reporting service	As agreed between monitoring company and client, but not less than once per year	**Note**: This procedure must be pre-arranged in consultation with the monitoring station. • Ensure that the system is 'on test'. • Perform an operation that triggers reporting. • Check that the system reports successfully.

Task	Frequency	Description
Test the backup reporting service	As agreed between monitoring company and client, but not less than once per year	**Note**: This procedure must be pre-arranged in consultation with the monitoring station. • Disable the primary reporting service. • Perform an operation that triggers a reportable alarm. • Check that the system correctly reports alarm to the backup reporting service after failing to communicate with the primary service. • Re-enable the primary reporting service.
Test system inputs and areas programmed to report	As agreed between monitoring company and client, but not less than once per year	**Note**: This procedure must be pre-arranged in consultation with the monitoring station. • Consult the maintenance sheets for a list of all inputs to be tested. • Activate each input by causing it to switch from the closed state to open (alarm) and back to closed. • Check the system event log for associated open/close events. • Check off each input on the maintenance sheet after successful testing and report any discrepancies. • Return all alarm areas to their pre-test states. • Obtain an activity report of all input opens/closes and area alarms/restores from the monitoring station. • Compare the monitoring station report with the system event log for the period to ensure that all tested inputs and areas reported correctly. Record and report any discrepancies. Special testing equipment and procedures may be required for smoke, heat, seismic glass-break and other detectors.
Test warning device outputs	As agreed between monitoring company and client, but not less than once per year May be performed alongside Input Testing (above)	**Note**: This procedure must be pre-arranged in consultation with the monitoring station. Test the operation of each audible and visible warning device. • Consult the maintenance sheets for a list of all outputs to be tested. • Arm any relevant areas. • Activate each warning device, either by user operation or by triggering an alarm which should cause activation. • Check that each warning device works as specified. Record and report any discrepancies. • Reset/Restore alarm areas to their previous state.

Software Maintenance Procedures

Task	Frequency	Description
Back up programming database	Recommended monthly	Backups of the programming database should be performed on a regular basis. It is vital that backups be stored offsite for disaster recovery. See the Operator Reference Manual for instructions on how to backup your database.
Back up events database	Recommended monthly	Backups or exports of recorded events should be performed on a regular basis. Verify that the backup file has been created. See the Operator Reference Manual for instructions on how to backup your database.

Follow-up Procedures

Task	Frequency	Description
Perform necessary system modifications	As required	Complete any modifications to the system resulting from the maintenance procedures. Record these in the maintenance sheets and report.
Obtain client sign off	At the conclusion of each maintenance visit	Obtain the signature of the client or the client's representative on the maintenance record.

5.2.2 - Emergency Service

The security alarm company shall always keep the client informed of their current after-hours or emergency contact details. If emergency service is required, an installer or technician shall attend the site within one working day. If this is not possible, the client shall be informed of any delay.

Any emergency service preformed shall be recorded in the client's maintenance logbook (see next page).

6 - Records and Reports

The following records and reports are required for a compliant system.

6.1 - Client and Equipment Records

When commissioning is completed, the initial records of equipment and system configuration shall be supplied to the client, providing an 'as-built' record of the system.

These records shall include all of the following:

- The address of the site and a floor plan.
- The position and type of each detection device.
- Description and wiring diagram of the installation.
- The position of any communication path and 240 VAC power outlets used by the system.
- The classification of the system in the form of a certificate. Any exceptions to compliance shall be noted.

A copy of this record shall be held by both the security alarm company and the client.

An example of this documentation is provided as AS_NZS_2201.1-2007_Class_5_Example_Site_Documents.docx.

6.2 - Maintenance Record

The security alarm company shall create and update a maintenance record, which covers all routine maintenance and emergency calls. This historical record shall be retained for a minimum of two years. A copy shall be signed by the client where possible, and provided to the client and relevant regulatory authorities on request.

The following details shall be included:

- The date and time of each visit.
- Any faults found, the action taken to resolve the issues and the cause, if known.
- Any work left outstanding after a maintenance visit.
- Record of any instance where it is necessary to temporarily disconnect, bridge or remove a detection device. This should include the reason and, if possible, the name and signature of the client's representative authorizing this action (see Clause 6.3 below).
- Record of any detection device that is not operating correctly.
- Any amendments to the installation or wiring diagrams.
- Record of any complaint received by the security alarm company or any other information that appears to require investigation. This should include the time and date that the information or complaint was received, any action taken to resolve the situation, and the time and date of that action.

6.3 - Authority for Disconnecting

No detection device shall be disconnected, bypassed or removed by the security alarm company without written authorization from the client. This authorization should be included in the site's maintenance record.

6.4 - Logbook

Technicians attending the site should maintain a logbook recording all visits, maintenance and work. This shall be kept inside the control equipment enclosure or in a secure location on the customer's premises. It shall include the following:

- The classification of the system, both at the time of installation and after any subsequent changes.
- The date and time of any visits, maintenance or works.
- The name and signature of each technician and the name of their company.
- The purpose of the visit (e.g. routine maintenance, emergency service, etc.).
- Details of any faults found or reported by the client.
- Recommendations for alterations or improvements, and details of any alterations or improvements that have been implemented.
- Details of any faults resolved or left unresolved during the visit.
- Record of any actions taken to mitigate unresolved faults (e.g. bypassing faulty inputs).
- Record of any battery replacement.

Appendix 1 - Enclosure and Pre-tamper (Vibration)

This section describes the method of mounting and dismounting ICT DIN Rail products in a DIN Rail enclosure, as well as the installation of the cabinet tamper switch and vibration sensor.

Mounting

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

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

1. Position the DIN rail module with the labeling in the correct orientation.
2. Hook the mounting tabs (opposite the tab clip) under the edge of the DIN rail.
3. Push the DIN rail module against the mount until the tab clips over the rail.

Removal

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

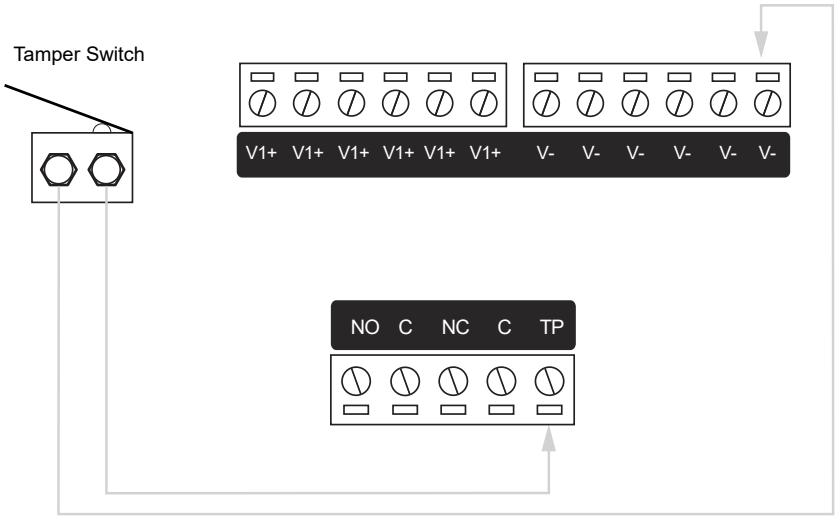
1. Insert a flat blade screwdriver into the hole in the module tab clip.
2. Lever the tab outwards and rotate the unit off the DIN rail mount.

Cabinet Tamper Switch

The enclosure tamper input notifies the monitoring station or remote computer that the enclosure has been opened. If the tamper switch is already mounted in your ICT enclosure, simply cut the cable tie once the enclosure is in place to allow the switch to actuate. Otherwise, mount the tamper switch to the enclosure with the bracket provided.

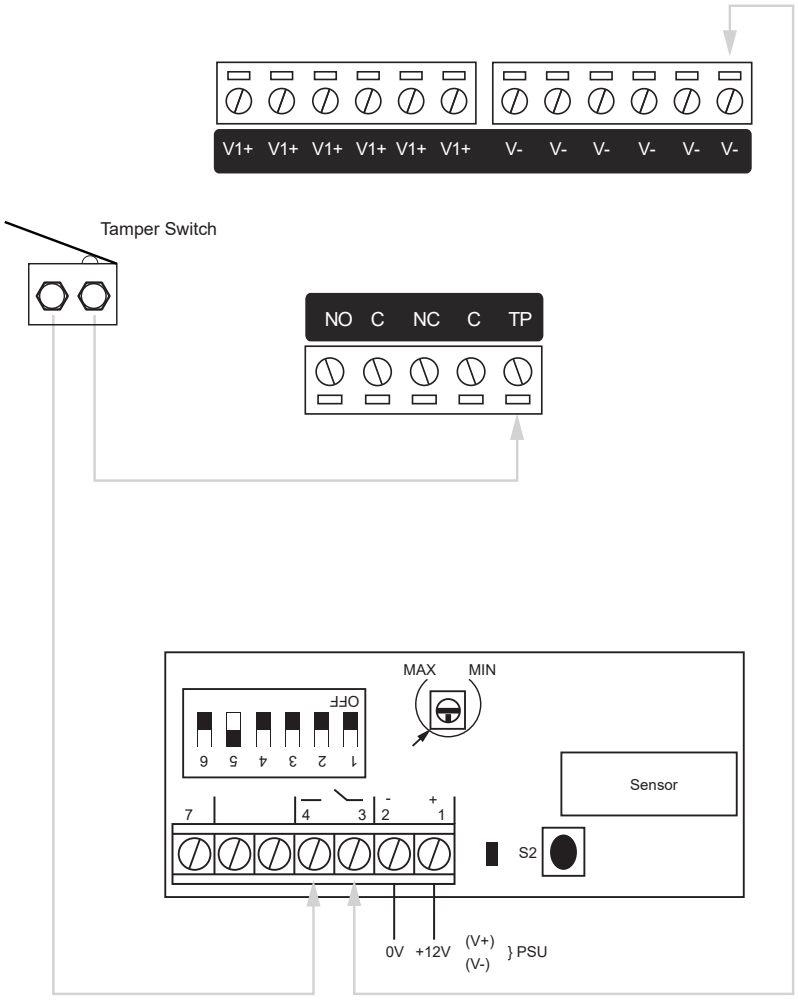
When the tamper input switch terminals are connected in series with the dedicated tamper input (TP) and V- terminal of the power supply, it will open the trouble input AExxx:01 on the power supply. Alternatively, connect the tamper switch to any other system input designated and programmed as a 24HR tamper alarm input.

Tamper Input Connection:



Vibration Sensor

Protection is provided by a DSC SS-102 Shockgard seismic vibration sensor mounted within the system enclosure.



Appendix 2 - Products Covered by AS/NZS 2201.1:2007 Class 5

The following products and installation manuals are covered by AS/NZS 2201.1:2007. The **Class** column indicates the highest standard that each unit complies to.

DIN Rail Products

Product Code	Description	Class	Installation Manual
PRT-CTRL-DIN-IP	Main system controller, control unit, DIN Rail	5	Protege GX DIN Rail Integrated System Controller (IP Only) Installation Manual
PRT-CTRL-DIN	Main system controller, control unit, in-built modem, DIN Rail	5	Protege GX DIN Rail Integrated System Controller Installation Manual
PRT-WX-DIN-IP	Main system controller, web enabled, decision and control unit, DIN Rail	5	ProtegeWX DIN Rail Integrated System Controller (IP Only) Installation Manual
PRT-WX-DIN	Main system controller, web enabled, decision and control unit, in-built modem, DIN Rail	5	Protege WX DIN Rail Integrated System Controller Installation Manual
PRT-CTRL-DIN-1D	Main system single door controller, control unit, DIN Rail	5	Protege GX DIN Rail Single Door Controller Installation Manual
PRT-WX-DIN-1D	Main system single door controller, decision and control unit, DIN Rail	5	Protege WX DIN Rail Single Door Controller Installation Manual
PRT-CTRL-DIN-1D-POE	Main system single door controller, control unit, DIN Rail, with power over ethernet (POE)	5	Protege GX DIN Rail Single Door Controller with PoE Installation Manual
PRT-WX-DIN-1D-POE	Main system single door controller, web enabled, decision and control unit, DIN Rail, with power over ethernet (POE)	5	Protege WX DIN Rail Single Door Controller with PoE Installation Manual
PRT-PSU-DIN-4A	12VDC 4A O/P Power Supply (AC Mains I/P 110-264VAC, 4765Hz), DIN Rail	5	Protege DIN Rail 4A Intelligent Power Supply Installation Manual
PRT-PSU-DIN-8A	12VDC 8A O/P Power Supply (AC Mains I/P 110-264VAC, 4765Hz), DIN Rail	5	Protege DIN Rail 8A Intelligent Power Supply Installation Manual
PRT-PSU-DIN-2A	12VDC 2A O/P Power Supply without 16VAC input transformer, DIN Rail	5	Protege DIN Rail 2A Intelligent Power Supply Installation Manual
PRT-RDM2-DIN-485	Reader Expander for 2 door access control, DIN Rail	5	Protege DIN Rail 2 Door Reader Expander Installation Manual
PRT-HRDM-DIN	Reader Expander for 2 door access control, Half DIN Rail (double stack)	5	Protege Half DIN Rail 2 Door Reader Expander Installation Manual

Product Code	Description	Class	Installation Manual
PRT-PX8-DIN	8 Output Expander, DIN Rail	5	Protege DIN Rail 8 Output Expander Installation Manual
PRT-HPX8-DIN	8 Output Expander, Half DIN Rail (double stack)	5	Protege Half DIN Rail 8 Output Expander Installation Manual
PRT-MNR2-DIN	COMMS Expander / Module Network Repeater, Half DIN Rail	5	Protege Module Network Repeater Installation Manual

Keypads

Product Code	Description	Class	Installation Manual
PRT-KLCD	LCD Keypad	5	Protege Alphanumeric LCD Keypad Installation Manual
PRT-KLCS	Touch Sense LCD Keypad, white	5	Protege Touch Sense LCD Keypad Installation Manual
PRT-KLCS-B	Touch Sense LCD Keypad, black	5	Protege Touch Sense LCD Keypad Installation Manual

Card Readers

See tables below (see page 31).

DIN Rail Cabinets and Accessories

Product Code	Description	Class	Installation Manual
EN-DIN-24	Metal box for every type of Protege DIN Rail module, with opening door tamper and remove from wall tamper 2x4 DIN Rail cabinet	5	
EN-DIN-23	2x3 DIN Rail cabinet	5	
EN-DIN-22	2x2 DIN Rail cabinet	5	
EN-DIN-12	1x2 DIN Rail cabinet	5	
EN-DIN-11	1x1.5 DIN Rail cabinet	5	
SS-102	Intrusion Shock Detector / Vibration Sensor (manufacturer DSC)	5	
12V 7Ah	Battery 12V 7Ah or (12V/18Ah)	5	

Other Components

Product Code	Description	Class	Installation Manual
PRT-ZX1	Single Input Expander	5	Protege Single Input Expander Installation Manual
	Personal RFID Cards/Tags	5	

Software

Product Code	Description	Class	Installation Manual
PRT-GX-SRVR	Protege GX System Management Suite	5	Protege GX Installation Manual

Product Code	Description	Class	Installation Manual
PRT-GX-WEB	Protege GX Web Client	5	Protege GX Web Client Installation Manual
AIP-V3-CORE	ArmorIP Version 3 Internet Monitoring Application	5	ArmorIP Version 3 Internet Monitoring Application User Manual

Card Readers

The ICT card readers below are compliant with the AS/NZS 2201.1:2007 Class 5 standard when wired in RS-485 configuration. When wired in Wiegand configuration, the readers are compliant with Class 4 and below.

tSec Readers

The readers named below are covered by the tSec Multi-Technology Card Reader with Bluetooth® Wireless Technology Installation Manual. For all readers, with and without keypad, environment class IVA applies.

Standard	117 x 46 x 18mm (4.61 x 1.81 x 0.71")				
	Keypad	125kHz	MIFARE/ DESFire/ NFC	Bluetooth® Technology	Vandal Resistant Cover*
PRX-TSEC-STD-B tSec Standard Multi-Technology Card Reader		✓	✓		
PRX-TSEC-STD-KP-B tSec Standard Multi-Technology Card Reader with Keypad	✓	✓	✓		
PRX-TSEC-STD-125-B tSec Standard 125kHz Card Reader		✓			
PRX-TSEC-STD-DF-B tSec Standard 13.56MHz Card Reader			✓		
PRX-TSEC-STD-DF-KP-B tSec Standard 13.56MHz Card Reader with Keypad	✓		✓		
PRX-TSEC-STD-BT-B **PRX-TSEC-STD-BT-W** tSec Standard Multi-Technology Card Reader with Bluetooth® Wireless Technology		✓	✓	✓	
PRX-TSEC-STD-KP-BT-B **PRX-TSEC-STD-KP-BT-W** tSec Standard Multi-Technology Card Reader with Keypad and Bluetooth® Wireless Technology	✓	✓	✓	✓	
PRX-TSEC-STD-KP-BT-B-VRC tSec Standard Multi-Technology Card Reader with Keypad, Vandal Resistant Cover and Bluetooth® Wireless Technology	✓	✓	✓	✓	✓
PRX-TSEC-STD-DF-BT-B tSec Standard 13.56MHz Card Reader with Bluetooth® Wireless Technology			✓	✓	
PRX-TSEC-STD-DF-KP-BT-B tSec Standard 13.56MHz Card Reader with Keypad and Bluetooth® Wireless Technology	✓		✓	✓	

* Keypad editions with vandal resistant cover included. Covers may be purchased separately for readers without keypads, but regular keypad editions do not support vandal resistant covers.

Extra	117 x 75x 18mm (4.61 x 2.95 x 0.71")				
	Keypad	125kHz	MIFARE/ DESFire/ NFC	Bluetooth® Technology	Vandal Resistant Cover*
PRX-TSEC-EXTRA-KP-B tSec Extra Multi-Technology Card Reader with Keypad	✓	✓	✓		
PRX-TSEC-EXTRA-125-B tSec Extra 125kHz Card Reader		✓			
PRX-TSEC-EXTRA-DF-B tSec Extra 13.56MHz Card Reader			✓		
PRX-TSEC-EXTRA-DF-KP-B tSec Extra 13.56MHz Card Reader with Keypad	✓		✓		
PRX-TSEC-EXTRA-BT-B **PRX-TSEC-EXTRA-BT-W** tSec Extra Multi-Technology Card Reader with Bluetooth® Wireless Technology		✓	✓	✓	
PRX-TSEC-EXTRA-KP-BT-B **PRX-TSEC-EXTRA-KP-BT-W** tSec Extra Multi-Technology Card Reader with Keypad and Bluetooth® Wireless Technology	✓	✓	✓	✓	
PRX-TSEC-EXTRA-KP-BT-B-VRC tSec Extra Multi-Technology Card Reader with Keypad, Vandal Resistant Cover and Bluetooth® Wireless Technology	✓	✓	✓	✓	✓
PRX-TSEC-EXTRA-DF-BT-B tSec Extra 13.56MHz Card Reader with Bluetooth® Wireless Technology			✓	✓	

***** Keypad editions with vandal resistant cover included. Covers may be purchased separately for readers without keypads, but regular keypad editions do not support vandal resistant covers.

Mini	85 x 46 x 17mm (3.35 x 1.81 x 0.67”)				
	Keypad	125kHz	MIFARE/ DESFire/ NFC	Bluetooth® Technology	Vandal Resistant Cover*
PRX-TSEC-MINI-B tSec Mini Multi-Technology Card Reader		✓	✓		
PRX-TSEC-MINI-125-B tSec Mini 125kHz Card Reader		✓			
PRX-TSEC-MINI-DF-B tSec Mini 13.56MHz Card Reader			✓		
PRX-TSEC-MINI-BT-B **PRX-TSEC-MINI-BT-W** tSec Mini Multi-Technology Card Reader with Bluetooth® Wireless Technology		✓	✓	✓	
PRX-TSEC-MINI-DF-BT-B tSec Mini 13.56MHz Card Reader with Bluetooth® Wireless Technology			✓	✓	

* Keypad editions with vandal resistant cover included. Covers may be purchased separately for readers without keypads, but regular keypad editions do not support vandal resistant covers.

TSL Readers

The readers named below are covered by the TSL Multi-Technology Card Reader Installation Manual. For all readers, with and without keypad, environment class IVA applies.

Standard	117 x 43 x 9.5mm (4.61 x 1.69 x 0.37")			
	Keypad	125kHz	MIFARE/ DESFire/ NFC	Bluetooth® Technology
TSL-STD-RR-HL TSL Standard Multi-Technology Card Reader with Bluetooth® Wireless Technology		✓	✓	✓
TSL-STD-RK-HL TSL Standard Multi-Technology Card Reader with Bluetooth® Wireless Technology and Keypad	✓	✓	✓	✓
TSL-STD-RR-H TSL Standard 13.56MHz Card Reader with Bluetooth® Wireless Technology			✓	✓
TSL-STD-RK-H TSL Standard 13.56MHz Card Reader with Bluetooth® Wireless Technology and Keypad	✓		✓	✓

Extra	117 x 75 x 9.5mm (4.61 x 2.95 x 0.37")			
	Keypad	125kHz	MIFARE/ DESFire/ NFC	Bluetooth® Technology
TSL-EXTRA-RR-HL TSL Extra Multi-Technology Card Reader with Bluetooth® Wireless Technology		✓	✓	✓
TSL-EXTRA-RK-HL TSL Extra Multi-Technology Card Reader with Bluetooth® Wireless Technology and Keypad	✓	✓	✓	✓
TSL-EXTRA-RR-H TSL Extra 13.56MHz Card Reader with Bluetooth® Wireless Technology			✓	✓
TSL-EXTRA-RK-H TSL Extra 13.56MHz Card Reader with Bluetooth® Wireless Technology and Keypad	✓		✓	✓

Mini	87 x 43 x 9.5mm (3.43 x 1.69 x 0.37")			
	Keypad	125kHz	MIFARE/ DESFire/ NFC	Bluetooth® Technology
TSL-MINI-RR-HL TSL Mini Multi-Technology Card Reader with Bluetooth® Wireless Technology		✓	✓	✓
TSL-MINI-RR-H TSL Mini 13.56MHz Card Reader with Bluetooth® Wireless Technology			✓	✓

Appendix 3 - Programming Examples

This appendix contains some examples of programming which may be required to achieve Class 5 compliance on site.

Programming Audible Alarm Devices

For Class 5 compliance, it is required that audible alarm devices such as sirens may be activated once when an area goes into alarm for the first time, but cannot be activated again until the area is disarmed, or a separate area goes into alarm.

An example of the configuration required to achieve this is given below (there may be other valid options). This programming will need to be repeated for each area that is using a siren.

Some field and menu names differ slightly between Protege GX and Protege WX. Use the option appropriate for your platform.

1. If you do not already have virtual outputs available, navigate to **Expanders | Output Expanders** and create a virtual output expander:
   - In Protege GX, ensure that the **Virtual Module** option is enabled.
   - Set the **Physical Address** to a value above existing physical expanders (e.g. 32).
   - In **Programming | Outputs**, rename the resulting outputs so that they include the term Virtual in their names.
2. Select a virtual output and give it a name similar to Alarm Memory VO.

   One virtual output is required per area. It is recommended that you add the area name to each output name.
3. Navigate to **Programming | Areas** and select each area that you are programming. Configure the following settings:
   - **Configuration** tab: Set the **Alarm 1 Time** / **Alarm Time** to 5 minutes.
   - **Outputs** tab:
     - Set **Bell Output** to the physical siren output.
     - Set **Alarm Memory Output** to the appropriate Alarm Memory VO.

   When the area goes into alarm for the first time, the siren will be activated for 5 minutes. At the same time, the Alarm Memory VO will be activated. The Alarm Memory VO will be deactivated when the area is disarmed.
4. Navigate to **Sites | Schedules** or **Scheduling | Schedules**. For each area, you need a schedule that will be valid when the Alarm Memory VO is OFF, and invalid when the Alarm Memory VO is ON. This means that the schedule will become invalid after the alarm is first activated in the area, until the area is disarmed.
   - Click **Add** and give the schedule a name similar to Siren Activation Schedule.

     It is recommended that you add the area name to each schedule name.
   - In the **Periods** section, tick all of the days in **Period 1**, and set the **Holiday Mode** to Ignore Holiday.
   - In the **Options** tab, enable **Validate Schedule if Qualify Output OFF**.

     Set the **Qualify Output** to Alarm Memory VO.
5. Navigate to **Programming | Input Types**. For every input type functionality that is used in an area (e.g. Instant, Delay), you must create a primary input type and a secondary input type.
   - The primary input type is used when the Siren Activation Schedule is valid, and activates the bell output in the area. Each area requires a unique primary input type.
   - The secondary input type is used when the Siren Activation Schedule is invalid, and does not activate the bell output in the area. There must be a secondary input type for each input type functionality, but there does not need to be one per area.

6. Create the primary input types that are required. There must be a unique set of primary input types in each area.
   - In the **Options (2)** tab, enable **Activate Bell Output** and **Activate Memory Output**.

   In Protege GX you can use the **Copy** button in the toolbar to duplicate the settings from an existing input type.

7. For each input type functionality in use, click **Add** to create a new secondary input type.
   - Duplicate the settings of one of the primary input types. In Protege GX you can use the **Copy** button in the toolbar.
   - In the **Options (2)** tab, disable **Activate Bell Output**.
8. Select each primary input type and set the following in the **General** tab:
   - **Operating Schedule**: Siren Activation Schedule
   - **Secondary Input Type**: The corresponding secondary input type created above.
9. Navigate to **Programming | Inputs**. Select each input that generates alarms and open the **Areas and Input Types** tab.
   - Set **Area 1** to the required area, and **Input Type 1** to the required primary input type.
   - Set **Area 2** to the same area as above, and **Input Type 2** to the corresponding secondary input type.
10. Wait for the settings to download to the controller. Disarm each area (including the 24HR portion) and rearm to implement the programming.

To test this programming, generate an alarm in the area by opening any input. All inputs are currently using the primary input type, so the first alarm will activate the bell output. The Alarm Memory VO turns on, which causes the Siren Activation Schedule to become invalid.

Since the Siren Activation Schedule is invalid, all inputs in that area are now using the secondary input type. Wait for the siren to time out, then open another input in the same area. The area will go into alarm again, but the bell output will not be activated.

Since each area has a unique Siren Activation Schedule, inputs in other areas are still using their own primary input types. Open an input in another area to generate an alarm. The bell output should be activated again.

Finally, disarm and rearm the area. This deactivates the Alarm Memory VO. When you open an input, the bell output should be activated again.

Service Settings for Class 5 Basic Communications

IP reporting communications are configured by programming a service in the Protege system. The following shows an example of appropriate configuration for Class 5 compliant communications:

- **Service Type**: Report IP
- **Service Mode**: 1 - Start with Controller OS
- **Client Code**: As required
- **Reporting Protocol**: Armor IP (UDP) Encrypted
- **Encryption Level**: AES 256 Bit, 192 Bit or 128 Bit.
- **Encryption Key**: The encryption key used to achieve the desired level of encryption.
  - For 256 bit encryption, the key should be exactly 32 characters long
  - For 192 bit encryption, the key should be exactly 24 characters long
  - For 128 bit encryption, the key should be exactly 16 characters long

  The key can be comprised of any combination of letters and numbers.
- **Poll Time**: 20 (seconds)
- **Ack Wait Time**: 5 (seconds)
- **Enable Offline Polling**: Yes
- Enter configuration for both the **Primary Channel Settings** and **Secondary Channel Settings**.
- **Switch Secondary IP Immediately**: Yes

The above settings comply with:

- **System Performance Dual Path (DP)**: AS/NZS 2201.5 Class 5 with redundancy of Class 2 (C5R2), Availability Class A5, D5, T5, S5.
- **System Performance Single Path (SP)**: AS/NZS 2201.5 Class 5, Availability Class A5, D5, T5, S5.

Disclaimer and Warranty

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

For warranty information, see our Standard Product Warranty.

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