INNER RANGE PTY. LTD.

INCEPTION INSTALLER MANUAL
(CONTROL EQUIPMENT)

FOR
AS/NZS 2201.1:2007 CLASSES 1 to 3 COMPLIANCE
Australia and New Zealand

- **Before using this document please check that you have the latest version by visiting the 'Technician Downloads' pages from the 'TRAINING & SUPPORT' menu at www.innerrange.com; Or e-mail: publications@innerrange.com**
- **This manual is NOT exhaustive and is not a substitute for a detailed check against the Standard itself!**
- **Inner Range also produces products that are certified compatible with AS2201.1:2007 Class 5 Installations. Contact Inner Range for information.**

CONTENTS

1. INTRODUCTION

1.1 Overview

This document outlines the installation, commissioning and maintenance procedures for an Inner Range Inception system when installed in accordance with AS/NZS 2201.1:2007. Class 1, Class 2 or Class 3.

For an Inner Range Inception system to comply with the requirements of these Classes, the Inception products listed in the table in Section 1.2 must be utilized.

The core components of an Inner Range Inception system are:

- Inception Controller and Power Supply Unit
- Sealed Lead-Acid (gel) type backup battery.
- A network connection. (Via Ethernet cable or the optional WiFi adapter)
- A web browser.

Compatible Inner Range Integriti and Concept products provide the User interfaces, output expansion, communications port expansion, additional power supplies and LAN accessories.

The full range of Inception system equipment and the recommended minimum firmware version number for all relevant products are listed in the table in 1.2 'Inner Range Inception system equipment'.

AS/NZS 2201.1:2007.

This document describes how the listed Inner Range products and common peripheral devices must be installed to meet the requirements of AS/NZS 2201.1:2007. Classes 1 to 3. The Installer must be familiar with the requirements of this standard.

For requirements relating to third-party equipment and other aspects of the system design, installation, commissioning and maintenance the Installer must refer directly to the document "AS/NZS 2201.1:2007. Intruder Alarm Systems. Part 1: Client's premises--Design, installation, commissioning and maintenance."

The standards for detection devices used with an Intruder Alarm system are provided in:
AS 2201.3:1991 DETECTION DEVICES FOR INTERNAL USE.

Copies of these standards are available from Standards Australia and can be purchased on-line via the SAI Global Website: http://www.saiglobal.com/shop

1.2 Inner Range Inception system equipment.

Inception Control Equipment.

The following Inner Range control equipment may be utilized in an Inner Range Inception system installation. Inner Range or Third Party Arming station devices (Terminals) or Expansion devices not included in this list may also be compatible, but it is the responsibility of the Installer to ensure that any other product used, meets the requirements for the relevant Class of installation.

Part Number	Description	Minimum Firmware Version	Associated Documentation	Doc. Vers.
996300AU	Inception Controller (Controller & PSU)	5.2	Infiniti Class 1-3 Installer's Manual (This document) 636300. Installation Manual. Inception Quick Start Guide. Inception LAN Installation Guide. Inception Routine Maintenance Manual. Inception Tech Bulletin - Alarm Reporting Inception System Alarm Contact ID Map.	1.0 5.21 Feb 2019 1.0 1.0 1.0 2.9 (Mar 2018)
995200	Small Enclosure.	N/A		
995201I 995201PEI	Medium Enclosure. Medium Enclosure with 3A PSU	N/A N/A	635201OPT. Installation Manual. 635201PE. Installation Manual	1.0 2.0
995204 995204PE3 995204PE8	Wide Body Enclosure. Wide Body Encl. with 3A PSU Wide Body Encl. with 8A PSU	N/A N/A N/A	635204OPT. Installation Manual. 635204OPT + 636091 635204OPT + 636092	2.0
996090PCB&K	Inner Range 2A PSU		636090. Installation Manual	2.4
996091PCB&K	Integriti 3A Smart PSU		636091. Installation Manual	3.4
996092	Integriti 8A Smart PSU	4.03	636092. Installation Manual	1.5
999030	Inception WiFi Adapter	N/A		
999032	Inception USB Hub	N/A		
995000ML 995000MLWH	Elite LCD Terminal. Ivory. Elite LCD Terminal. White.	3.0	635000ML. Installation Manual.	2.0
995400 995400SI	EliteX Terminal. EliteX -SIFER Terminal.	3.1.0	635400. Installation Manual.	3.4
998530LT 998530	Inner Range T4000 Communicator	2.1.4	638530. Installation Manual	2.3
996797	T4000-Inception Interface Cable	N/A	636797. Installation Manual	1.0
994720 994720MF	Inner Range SIFER Reader Inner Range SIFER Reader Multi-format	1.16.0.14	634720. Installation Manual	4.4
996012PCB&K	Integriti SLAM	4.0.7	636012. Installation Manual	3.4
996005PCB&K	Integriti 8-Zone LAN Expander	3.1.1	636005. Installation Manual	4.0
996500PCB&K	Integriti UniBus 8 Input Exp.	1.0.3	636500. Installation Manual	2.0
996515PCB&K	Integriti UniBus 8 Relay Exp.	1.1.2	636515. Installation Manual	2.0
996540PCB&K	Integriti UniBus Lift Interface	1.0.0	636540. Installation Manual	2.0
995915	Mini LAN Hub. 8-way.	N/A	635915. Installation Manual	1.0
996088	LAN Ethernet Bridge	1.1.0	636088. Installation Manual	1.11
995087	Inner Range Fibre Modem-S	V2.0	635087. Installation Manual	2.0
995081	Inner Range Fibre Modem-M	V2.0	635081. Installation Manual	3.1
995080PCB&K	Inner Range LAN Isolator	V5.00	635080. Installation Manual	4.1
995041	Inner Range LAN Surge Diverter	N/A	635040. Installation Manual	1.1

Firmware/Document Versions

The Inner Range firmware and document version numbers listed in the table above imply that either the version number listed, or a later version of the firmware or document is acceptable.

Additional Documentation

This manual is to be used in conjunction with the AS/NZS 2201.1:2007 document and the Inception documentation associated with each of the products listed above.

Where any specifications, requirements or information in AS/NZS 2201.1:2007 differs from information in this manual, the AS/NZS 2201.1:2007 document takes precedence.
Likewise, where any specifications, requirements or information in this manual differs from information in the other Inner Range documentation listed above, the material in this manual takes precedence.

Equipment Configuration and Power Supply requirements

See section 2.3 h) Batteries for details of typical equipment configurations and the operating current required by compatible Inner Range products.

1.3 Risk Assessment.

AS2201.1:2007 requires that a risk assessment has been performed in accordance with the requirements for the relevant Class.
See AS/NZS 2201.1. Clause 1.3 and Appendix A.

When designing the system, select the number and type of detection devices that will be appropriate to mitigate the agreed risk profile selected.
This will determine the location and number of Expander Modules required in the system.

1.4 Power Supply

All Inner Range Inception system Controllers, LAN Modules and associated devices such as warning devices and door locks must be powered by Inner Range Power Supplies or other approved Power Supplies that meet the requirements of AS/NZS 2201.1.

Mains power must be sourced from a permanent external mains power supply.

See 2.3 c) for details.

1.5 Wire-free Systems

At present, the Inner Range Paradox or Inovonics RF Expander Module products have not been evaluated for AS2201.1 capability.

Compatible user credentials and readers connected to the RS485 Reader port on the Inception Controller or compatible LAN Access Modules may be used.

1.6 Disarming and Arming procedures

The options available for the Area Disarming and Arming procedures in an Inception system must be explained clearly to the client. Once determined, the agreed arming and disarming methods must be recorded and provided to the client. The information below describes the options and is provided to assist in this process.

NOTE: Owing to the level of protection available by an Inception system, adoption of the more secure options for disarming and arming are recommended.

Minimum Requirement for Disarming

Clause 3.16.2.6 sets out the minimum requirements for user credentials required in the on-site disarming procedure.
i.e. Any coded system with a minimum of 1000 unique combinations.
Use of a PIN Code OR an Inner Range SIFER Card to disarm an Area in an Inception system meets & exceeds the minimum requirements of this clause by employing:

1) The option to set a minimum user PIN Code length (i.e. 4 or more) to enforce the required minimum number of unique combinations.
2) Monitoring of incorrect PIN Code attempts and timed lockout option.
3) An extremely high number of unique credential combinations via the Inner Range SIFER Card data format.
4) An extremely high level of encryption on the SIFER Card Reader communications link.

More Secure option for Disarming (recommended)

Clauses 3.16.3.4 and 3.16.4.3 require that the keypad lockout feature is implemented and that options are available for Class 2 and Class 3 systems to employ the use of a higher number of unique combinations. The minimum requirement (Class 1) and options for all 3 Classes are shown in the table below.
Where practicable, use of one of the more secure options is recommended.

Requirement	**Class 1**	**Class 2**	**Class 3**
No. of unique code combinations.	≥1,000	≥9,000	≥900,000
'Minimum PIN Code length' setting.	4	4	6
Keypad lockout on max. 6 wrong code attempts.	Optional	Mandatory	Mandatory

Note that the Inception system also supports a Card + PIN option for disarming an Area for a higher level of credential security which you may also wish to offer the client.
For this method you would need to install a SIFER-Keypad, an EliteX-SIFER Terminal, or a Card Reader plus User Terminal (Elite or EliteX Terminal) at each location where disarming operations are required.

Options for Arming

There is no specified minimum credential requirement for on-site arming, however it would not be advisable to implement an arming procedure that could cause an Area to be armed unintentionally (e.g. A pushbutton requiring no user credential or a single card presentation as commonly used in access control operations)

Inception offers the following recommended options:

1) PIN Code arming at an Elite or EliteX LCD Terminal.
2) 3-Badge Arming using a Card Reader.

2. INSTALLATION

2.1 Equipment location

a) General

Install the control equipment and associated equipment such as alarm transmission equipment, within the alarmed area, and where practicable, where it is not visible from outside the alarmed area. i.e. Within the area monitored and protected by the intruder alarm system.

Install the equipment in a location that meets the environmental conditions specified in the relevant installation manual.

Inception control equipment includes the Controller, RS485 LAN Modules (including LCD Terminals), UniBus expansion boards and Power Supply equipment.

b) Arming Stations

e.g. Elite and EliteX LCD Terminals.
LCD Terminals have built-in tamper detection.

- Elite Terminals have a switch. Ensure that the tamper switch actuating lever is properly fitted as per the installation instructions and that the switch is operational.
- EliteX Terminals have an optical detection device. Ensure that the terminal is installed according to the installation instructions and that tamper detection is operational.

2.2 Wiring

a) General

All wiring described in this document must meet the following requirements.

The wiring requirements described in AS/NZS 2201.1:2007 Clause 2.6 must be followed.

Wiring must be installed and connected in accordance with:
AS/CA S009; Installation requirements for customer cabling (Wiring Rules)
Where equipment is required to interface with low voltage circuits, the wiring must comply with:
AS/NZS 3000; Electrical Installations (Australian/New Zealand Wiring Rules)

Wiring must be arranged to minimize the risk of attack or damage and where practicable, should be concealed.

Wiring and all associated materials must be chosen to suit the expected environmental conditions at the installed location.

Note that third party wire and cable recommendations provided in the individual installation manuals for the Inner Range products used in an Inception system are intended as a guide only and may, or may not, comply with the requirements of AS/NZS 2201.1.

b) Wire Rating

i) General.

Wire rating and size must be chosen according to the minimum ratings below, and also for the intended wire length and load such that at the maximum expected current, the voltage drop in the wiring will not reduce the terminal voltage at the devices to less than 10% above the lower operating voltage limit stated by the device manufacturer.

e.g. If a device's minimum operating voltage is 10 VDC, then at the maximum expected current, the wiring must not cause the voltage at the device to be less than 11 V DC..

ii) Minimum ratings

All wiring must have:

- A total cross-sectional area of at least 0.20mm^2 (24 AWG).
- An outer sheath insulation rating of at least 300V RMS.
- Stranded conductors in accordance with the following table. (Note: Coaxial cable may have a solid core)

Cable type.	Typical application	Stranding (No. of strands/Strand diam.)	
		Class 1 & Class 2	Class 3
Single core and Figure 8	Battery. Tamper switch. Reed-switch. Siren. Strobe. Beeper. Lock. Exit button. Arm button.	14/0.20mm	24/0.20mm
Multi-core cable. Un-shielded. (3 or more conductors)	PIR detector. Glass-break detector. Smoke Detector.	7/0.20mm	14/0.20mm
Multi-core cable. Shielded. (3 or more conductors)	Inception RS485 LAN. Card reader. Printer. PC. External modem.	7/0.20mm	7/0.20mm
Coaxial Cable (Core)		1/0.51mm Or 7/0.20mm	1/0.51mm Or 7/0.20mm

c) Inner Range Cables

The following Inner Range cables are either supplied with, or may be purchased for use with, an Inception system and meet the minimum ratings for Class 3 described in AS/NZS 2201.1 Clause 2.6 and summarized above.

Description	Part No.	Drawing P/N
SINGLE CORE & FIGURE 8		
Battery Lead Pair. 40cm	N/A	605051
Integriti Battery Lead. 60cm	N/A	605052
Integriti Heavy Duty Battery Lead.	999048	605055
Chassis Earth to PCB	N/A	605029
MULTICORE UNSHIELDED		
Integriti Smart PSU Cable 430mm	996792	605062
Integriti PSU Cable for 3rd Party PS	996794	605064
UniBus Patch Cable 150mm	996791SS	605061SS
UniBus Patch Cable 220mm	996791S	605060
UniBus Patch Cable 270mm	996791L	605061L
UniBus Patch Cable 475mm	996791LL	605061LL
UniBus Patch Cable 675mm	996791XL	605061XL
MULTICORE SHIELDED		
T4000-Inception Interface Cable	996797	606797

Other Inner Range cables may also be compatible, but it is the responsibility of the Installer to ensure that any other cable used, meets the requirements for the relevant Class.

d) Jointings

Avoid creating joints in wiring whenever possible.
If wiring joints are necessary, the requirements described in AS/NZS 2201.1:2007 Clause 2.7 must be followed.

e) Flexible Conductors and Connections

Wiring that connects movable parts of the intruder alarm system must meet the requirements described in AS/NZS 2201.1:2007 Clause 2.8. e.g. Wiring to control & monitor an electric mortise lock.

f) Terminations

All wiring connecting to Inception equipment must be terminated using:

- The cable provided with the product (e.g. UniBus patch cable, Smart PSU cable, Inception Battery Cable, etc.)
- The pre-assembled cable recommended by the manufacturer (e.g. T4000 Interface cable, etc.)
- The plug-on connectors provided in the installation kit (e.g. Zone Inputs, Relay outputs, RS485 LAN, Reader, Siren, etc.)

The termination requirements described in AS/NZS 2201.1:2007 Clause 2.9 must be followed.

2.3 Installing the control equipment.

a) Mounting the equipment

All Inception Controllers, Alarm Transmission equipment (e.g. Inner Range T4000 Communicator), LAN Modules and ancillary LAN devices, UniBus boards, Power Supplies and Batteries must be installed in:
- Inner Range Inception or Integriti enclosures.
- or 3rd party enclosures that meet all the requirements of AS/NZS 2201.1:2007 Clause 2.6.4, Clause 3.7 and Clause 3.16.3.5.

The Alarm Transmission device must be installed in the same enclosure as the Controller.

Control equipment enclosures must be installed indoors and within the alarmed area and should not be visible from outside the alarmed area. The installation environment should be maintained at a temperature of 0º to 50º Celsius and 15% to 85% Relative humidity (non-condensing).

Fix all enclosures and User Terminals securely to the mounting surface using corrosion-resistant bolts, screws and washers suitable for the environment, and in a position that minimizes the risk of interference or damage.

Use fixings in all the mounting holes provided in the equipment enclosures and User Terminals.

If fixing to a masonry surface, corrosion resistant plugs or masonry anchors must be used.
If fixing to plaster board, purpose-designed corrosion-resistant wall anchors suitable for the weight loading must be used and where possible, at least two fixings should be into one or more timber or steel studs.
If fixing into metal, bolts or machine screws, washers and anti-vibration devices must be used.

b) Equipment labelling

Inner Range equipment enclosures and Modules supplied from the factory in an Inner Range enclosure are supplied with an equipment label affixed to the enclosure cover.

The Inception Controller and other products to be installed in an enclosure may also be supplied with an adhesive label in the accessory kit. This label must be affixed to the outside of the equipment enclosure where it will be clearly visible, in addition to any existing label.

Part number and Serial number labels are affixed to Inception Controllers and printed circuit board (PCB) assemblies. The Inner Range manufacturer logo is printed on the Inception Controller and every PCB.

The equipment labels, part number and serial number labels described above must be legible and must not be removed.

Ensure that any enclosure containing a power supply also has the following information clearly and indelibly marked, if it is not already provided on one or more of the existing labels.
- Name of the manufacturer or supplier.
- Module number of the equipment.
- Input and Output supply voltages, frequency and power or current.
- Approval numbers.
- Type and capacity of replacement battery where applicable.

c) Power Supplies

i) Mains Supply Isolation Switches

AS/NZS 2201.1:2007 Clause 3.11.7 requires that mains isolation is provided by either a switched GPO located inside or adjacent to the control equipment enclosure, or an isolation switch located within the enclosure.

ii) Inception Controller Power Supply.

The Inception Controller must be powered by the supplied Power Supply Unit as described in the Inception Installation Manual.
The PSU should be installed in the same enclosure as the Controller and a suitable 12V sealed lead-acid battery connected to the 'BATT' connector terminals on the Inception Controller.

An alternative power supply must not be used, as battery testing requirements will not be able to be met.

iii) Integriti Power Supplies.

An Integriti Smart Power Supply is pre-installed in Integriti Powered Equipment Enclosures.

The power supply connector P2 must be connected to the main LAN Module in that enclosure using the supplied 10-way cable. e.g. An 8 Zone LAN Expander, SLAM, etc.
NOTE: Any enclosure containing a Smart Power Supply must have at least one LAN Module present in the same enclosure connected to the Power Supply via the P2 connection to provide power supply monitoring.

The 8A Smart Power Supply also provides a general purpose power supply output (T3) for powering other LAN Modules within the same enclosure and peripheral devices such as door locks. The connection between the power supply T3 and LAN Module "External Power" connector is made using the cable P/N: 996794. Integriti PSU Cable for 3rd Party PS.
The AC Fail and Battery Fail outputs on connector T4 of the 8A Power Supply must not be used. These states are monitored via the data link between the power supply and the host module.

d) Elite LCD Terminals

The physical Auxiliary outputs provided on an Elite LCD Terminal (X01 to X04) must not be used. If required, X02 may be used for LED4 control (if enabled) and X04 may be used for pulsing beeper control.

e) Standard LAN Access Modules (SLAM)

The Valid (VAL) and Invalid (INV) outputs provided on the SLAM PCB must not be used.

f) 8-32 Zone LAN Expander Module

The Integriti 8-32 Zone LAN Expander provides additional Zone Inputs, Siren outputs, Relay outputs, Smart Power Supply monitoring and Cabinet Tamper monitoring.
The Siren outputs are designed to directly drive 8 Ohm horn speakers.

g) Tamper detection

Integriti equipment enclosures are provided with a cabinet tamper switch device. This must be installed and monitored.

NOTE:
- Tamper detection devices are mandatory in Class 2 & 3 systems, and optional in Class 1 systems.
- Reporting of Tamper alarms is mandatory in Class 3 and optional in Class 1 & 2.

i) Tamper Switches.

Fit the supplied Tamper switch to all control equipment enclosures as per the installation instructions, and connect to the "TAMP/0V" input on a Controller or LAN Module installed inside the same enclosure.

Tamper detection devices must also be fitted to all audible warning device enclosures and any junction boxes used to house EOL supervision devices. The tamper detection device must be designed to activate prior to, or on opening of the enclosure; and prior to, or on removal of the enclosure from its mounting surface.

If the enclosure does not contain a Controller or LAN Module (e.g. A Siren enclosure, or an enclosure that only contains power supply equipment), the Tamper switch must be fitted with end-of-line resistors and connected to a Zone Input. *See "End-of-line Supervision" for details.*

ii) Terminals/Arming Stations

When installing Elite LCD Terminals, ensure that the tamper switch actuating lever is properly fitted as per the installation instructions and that the built-in Tamper switch is operational.
When installing EliteX LCD Terminals, follow the installation instructions and check that the optical tamper detection is operational.

iii) Securing equipment enclosures

The covers of all equipment enclosures must be secured with the screws supplied or an optional key lock.

h) Batteries

Choose appropriate 12V, 7AH-22AH, Valve-regulated, SLA (Sealed Lead Acid) or AGM (Absorbed Glass Matt) Batteries for every Power Supply. Non-rechargeable batteries must not be used. Batteries must have a charge rate specification of at least 0.2C

The following batteries have been tested by Inner Range and found to be suitable:

- AUSCELL No. 1. CJ12-18
- FUSION AGM BATTERIES. CBC12V22AH

Depending on the number of modules installed and peripheral devices being powered, an equipment enclosure may need to be fitted with two 18 AH batteries. This will require an Integriti Wide-body enclosure.

In the system design, the load on each Power Supply and the Battery capacity must be selected such that:

1) Under failure of the external mains supply, the system will continue to operate for:
    a. At least 16 hours with alarm transmission to a monitoring centre. (Note: Remote alarm monitoring is mandatory in Classes 2 & 3)
    b. At least 24 hours with local alarm monitoring only.
2) The battery will recharge sufficiently to achieve the backup capacity stated above within 48 hours after the external mains supply is restored.

If a power supply load is such that these requirements cannot be met, then the system design will require one or more additional battery-backed power supplies to distribute the load.

BATTERY CAPACITY GUIDE
This table provides a general guide to the battery capacity required for the typical enclosure configurations shown.

Integriti Class 5 Configuration	Description	Battery
Controller, Communicator and 8 Zone Expansion.	-Inception Controller and T4000 Communicator. -1x Integriti 8-Zone Expander. -Detection devices (up to 16), indicating devices, Readers and Arming stations with a total current draw of no more than 400mA.	18Ah
8 Zone Expansion.	-1x Integriti 8A Smart Power Supply. -1x Integriti 8-Zone Expander. -Detection devices (up to 8), indicating devices and Arming stations with a total current draw of no more than 500mA.	9Ah
16 Zone Expansion.	-1x Integriti 8A Smart Power Supply. -1x Integriti 8-Zone Expander. -1x Integriti UniBus 8-Zone Expander. -Detection devices (up to 16), indicating devices and Arming stations with a total current draw of no more than 900mA.	18Ah
Reader Expansion.	-1x Integriti 8A Smart Power Supply. -1x SLAM. -Readers and Arming stations with a total current draw of no more than 500mA.	9Ah

The Battery must comply with the requirements of AS/NZS 2201.1:2007 Clause 3.14.

Install the battery in each enclosure as per the relevant installation manual.

Mark every battery with the month and year of installation. Ensure that the marking is done so as to be legible and durable.

The current required by each Inner Range product is provided in the 'Current Consumption Guide' table below and also in each product's installation manual to assist the installer in calculating the current required for other configurations. For 3rd party equipment such as detection devices, sounders, locks, etc., the installer will need to consult the manufacturer's product documentation.

CURRENT CONSUMPTION GUIDE
This table provides a general guide to the operating current required for compatible Inner Range products.

Module or Device	Part Number	Power Supply Current Required.
Inception Controller	996300AU	85-150mA with Ethernet connected Add 25mA for each active Relay O/P.
Inception WiFi Adapter	999030	25-40mA
Inception 4-Port USB Hub	999032	20-40mA
Elite LCD Terminal	995000ML	20mA (Idle) 45mA (In use)
EliteX LCD Terminal EliteX-SIFER LCD Terminal	995400 995400SI	17mA (Idle). 50mA (Max) 72mA (Idle). 186mA (Max)
8-32 Zone LAN Expander Module	996005PCB&K	70mA (Idle) 110mA (Both Relays On)
Standard LAN Access Module (SLAM)	996012PCB&K	110mA (Idle) 175mA (Lock Relays On)
Inner Range SIFER Reader	994720 (Standard) 994720MF (Multi-format)	75mA to 150mA (Depends on LED configuration)
Inner Range SIFER-Keypad Reader	994725 (Standard) 994725MF (Multi-format)	75mA to 165mA (Depends on LED configuration)
UniBus 8 Zone Expander	996500PCB&K	75mA
UniBus 8 Relay Expander	996515PCB&K	45mA (Idle) 175mA (All Relays On)
UniBus 16 Floor Lift Interface	996540PCB&K	310mA
T4000 Security Communicator	998530LT (Lite) 998530 (Std)	120mA
Mini LAN Hub. 8-way.	995915	3mA
RS485 LAN/Reader Surge Diverter	995041	None
Inner Range Fibre Modem-S	995087	Approx. 160mA average.
Inner Range Fibre Modem-M	995081	Approx. 30mA average.
Inner Range LAN Isolator	995080PCB&K	Approx. 65mA average.

i) Outputs

Items of control equipment may provide one or more relay outputs, open collector outputs, 13.75V DC outputs or 5V DC outputs for controlling and/or powering peripheral devices such as alarm sounders, strobes, readers, door locks, indicator lamps, etc.

Do not exceed the current and voltage limits specified for each output.
The limits for each output are specified in the installation manual for the product. See the table in 1.2.

The following outputs are not suitable for AS/NZS 2201.1:2007 installations and must not be used:

- Elite LCD Terminal. Physical Auxiliary outputs X01 to X04. If required, the internal functionality offered by X02 & X04 may still be used. i.e. X02 may be used for LED4 control (if enabled) and X04 may be used for pulsing beeper control.
- Standard LAN Access Module (SLAM). Valid (VAL) and Invalid (INV) outputs.
- 8A Smart Power Supply. AC Fail and Battery Fail outputs on connector T4.

2.4 Installing the Detection Devices

a) General

Install all detection devices such that their location provides an optimized balance between intruder detection and the risk of detecting unwanted signals and interference.
e.g. A PIR must not be installed where movement outside the protected area (i.e. through a window), or sudden changes in temperature may cause a false alarm.
Refer to the detector manufacturer's installation instructions.

Connect or assign only one detection device to each Inception Zone Input address.
Note: If multiple unpowered detection devices of the same type are used to monitor a single entry point such as a double door or multiple windows within the same frame, then those devices may be connected or assigned to a single Zone Input address.

b) End-of-line supervision

End-Of-Line (EOL) Resistors must be installed on every detection device as described in the Inception installation manuals.
Install the EOL Resistors within the housing of the detection device whenever possible.
e.g. PIR detectors, Glass-break detectors, Smoke detectors, etc.

If not possible (e.g. Magnetic Reed switches), the EOL Resistors must be installed in a junction box located immediately adjacent to the detection device and fitted with tamper-detection devices in accordance with AS/NZS 2201.1:2007 Clause 3.16.3.5. (A tamper-detection device is not required for Class 1)
The interconnecting cables between the detection device and the junction box must not be visible.

When connecting the EOL Resistors to the detector and the Zone Input wiring, all joints must be either:

- Soldered and covered with a suitable insulating material.
- Clamped. i.e. Terminated in the clamping screw terminals of the detector.

2.5 Installing the Warning Devices

All warning devices must meet the requirements of AS/NZS 2201.1:2007 Clause 3.16.2.9.

CONTROL EQUIPMENT OUTPUTS.

- The Inception Controller provides up to 4 Auxiliary Relays which may be available to control devices such as a Strobe light, Satellite Siren or Piezo Siren device.
- The 8 Zone LAN Expander Module provides 2 dedicated Siren speaker outputs (External Siren and Internal Siren) and 2 Auxiliary Relays which may be available to control devices such as a Strobe light, Satellite Siren or Piezo Siren device.
- The UniBus Relay expansion board option can be fitted to an 8-Zone LAN Expander for additional Auxiliary Relay outputs.

Locate all warning devices so as to minimize the possibility of inadvertent damage or interference.

Check that the installation and programming recommendations for warning devices in this document do not contravene any legislation pertaining to these devices.

Install at least two audible alarm warning devices (e.g. 8 Ohm Siren Speakers &/or Piezo Siren Drivers) as per the instructions in the relevant installation manual.
Choose devices that provide a sound pressure level in the range of 90dB(A) to 130dB(A) @1metre.

Install at least one flashing blue strobe light outside, or where it will be clearly visible from outside the premises and connect it to a Controller or Zone Expander Module auxiliary relay output as per the instructions in the relevant installation manual.

Warning device enclosures must have tamper detection devices fitted. *See "Tamper Detection" above for details.*
(A tamper-detection device is not required for Class 1)

2.6 Installing Card Readers

Card Readers, or equivalent credential readers may be installed for disarming &/or arming the system.

If used, a card data format must be chosen that meets at least the minimum requirements for unique card/credential combinations described in 1.6 'Disarming and Arming procedures'.

Higher numbers of unique combinations are recommended according to the Class of installation and the options agreed to between the installer and the client.
e.g. For Class 3, a card data format that provides at least 900,000 unique card/credential numbers would be recommended. If a Wiegand format, the card number would need to be a minimum of 20 bits in length to meet this requirement.

The Inner Range SIFER Readers & Cards also meet and exceed these requirements.

Any additional or alternative device must be chosen and installed in accordance with the appropriate requirements for Arming Stations &/or Card Readers.

2.7 Installing Alarm Transmission equipment

Depending on the Class of the installation and the level of alarm transmission integrity required, a compatible, certified AS/NZS 2201.5 Alarm Communicator may be installed with the Inception Controller.
The Alarm Communicator should be installed in the same equipment enclosure, and must be installed in accordance with the requirements for the relevant Class.

If the Alarm Communicator is installed in a separate enclosure, the enclosure must comply with the requirements of Clause 3.7 (All Classes) and Clause 3.16.3.5 (Class 2 and Class 3)

The Inner Range T4000 Security Communicator is a suitable option.

If utilizing the T4000 Security Communicator, the alarm transmission plan must be chosen to comply with the relevant "Alarm transmission equipment" requirement for the relevant Class described in AS/NZS 2201.1:2007
The T4000 communications poll rate and supervision period is dependent on the transmission plan selected by the Central Monitoring station operator or Bureau technician using the Multipath-IP client software.

See the T4000 Installation manual for details of the Alarm Transmission plans relevant to each Class.

Refer to "AS/NZS 2201.5:2008. ALARM TRANSMISSION SYSTEMS" for full details.

T4000 wiring connections.

1) **Power Supply.**
   Connect T4000 'VIN +/0V' to the Inception 'VOUT +/0V' terminals next to the 'BATT' terminals. Ensure that no other devices are powered from the same 'VOUT' connector. Use 24/0.20 Figure 8 cable. Check for correct polarity. i.e. VIN+ to VOUT+ and VIN 0V to VOUT 0V.

2) **Serial Data.**
   Connect T4000 SERIAL (TTL) to the Inception Controller 'USB' connector (P1) using the Inception-T4000 interface cable P/N 996797. NOTE: If an Inception 4-port USB Hub is in use to provide additional USB connections, then the USB end of the cable may be connected to the Hub.

See "Reporting. (Dialler, GSM, etc.)" in the System Programming Notes section for reporting format details.

3. SYSTEM PROGRAMMING

The Inception browser includes a 'Commissioning Checklist' which provides the installer with a convenient and logical sequence for system programming and commissioning.

For ease of use, the programming notes below are provided in the same sequence offered by the Commissioning Checklist. The configuration menu location of the item is also shown in brackets.

3.1 Configure Network Settings.

(Configuration > General > Network)

The default network settings for Ethernet, Wi-Fi and Skytunnel access do not normally need to be changed unless a static IP address is required, the Wi-Fi Connection Mode needs to be changed or a connection method needs to be disabled.

3.2 Configure Date and Time Settings.

(Configuration > General > Date and Time)

Select the correct Time Zone and check other settings to ensure the system will be synced correctly and will operate and log events with the correct local time.

3.3 Configure System Settings and Compliance.

(Configuration > General > System)

a) GENERAL

END OF LINE. The default setting of "2k2 + 2k2 or 2k2 + 6k8" is recommended but other configurations may be chosen. End of line resistors are mandatory in all Classes and must be installed at the detector location.
AC FAIL REPORTING DELAY. Set to an appropriate duration, but not exceeding 90 minutes.
VERIFY SYSTEM HEALTH ON AREA ARM. Ensure that this option is enabled.
MODULE FAILED TIME: The default setting of 1 minute is recommended.
PREVENT SIREN RETRIGGER FROM SAME SOURCE. This option must be enabled.

b) STANDARDS COMPLIANCE

Not relevant to AS2201.1

c) PIN / PASSWORD POLICY

	Class 1 and Class 2	**Class 3**
MINIMUM USER PIN LENGTH	Not less than 4.	Not less than 6.
MAXIMUM USER PIN LENGTH	Same as Min. User PIN length or greater.	Same as Min. User PIN length or greater.
MINIMUM USER PASSWORD LENGTH	Not less than 4.	Not less than 6.
LOGIN ATTEMPTS BEFORE ACCOUNT LOCK	Not more than 6.	Not more than 6.
LOCKOUT DURATION	Not less than 1 minute.	Not less than 1 minute.

d) DURESS USER

Optional.

e) BATTERY TEST

Program Automatic Battery Testing to be performed on the Inception Controller and all LAN Modules that have an Integriti Smart Power Supply connected as follows:

Option	Class 1 & Class 2	Class 3
Test Frequency	As agreed with the Monitoring Centre &/or Client. A setting of "Each Week" is recommended. (i.e. Weekly testing)	Daily.
Test Day of Week	As agreed with the Monitoring Centre &/or Client.	Not relevant to Class 3.
Test Time of Day	Set to the time of day at which the Battery Testing is to start.	Set to the time of day at which the Battery Testing is to start.

d) EMAIL

Optional.

3.4 Setup Site Areas / Create Areas

(Configuration > Areas > Area Creation)

The Intruder Alarm system may be configured as a single Area, or multiple Areas as appropriate to the particular site if partial arming/disarming is required.

3.5 Perform Hardware Enrolment / Run Hardware Wizard

(Configuration > Hardware)

The Controller and each Module can be selected for editing.
Use the 'Create New' button to add Modules that are not yet in the system.

INCEPTION CONTROLLER

Inputs and Outputs:
Select the behavior and program a name for each of the Inputs and Outputs that are to be used on the controller.

Additional Components:

- Select the Cabinet Tamper Switch Type. For the tamper switches provided with the recommended Inner Range enclosures, select the "Open Circuit Secure" option. Tamper monitoring is mandatory for Class 2 and Class 3.
- The options "Power Supply connected to DC IN", "Backup Battery Connected to BATT" and "Enable Battery Testing" must all be enabled.
- A "Battery Test Duration" appropriate for the Power Supply load and Battery capacity of the Controller must be programmed.

LCD TERMINALS / ELITEX LCD TERMINALS

Module Settings:

- Poll Time. The default setting of 1 minute is recommended.
- Logon Security:
  Set the "Max Login Attempts" option to an appropriate value, but not greater than 6. (Mandatory if the Terminal is installed outside the protected area)
  Set the "Lockout Time" option to an appropriate value, but not less than 60 seconds. (Mandatory if the Terminal is installed outside the protected area)
  For Class 1 installations, this feature is optional, but nevertheless recommended.

- Alarm Message Sources. Ensure that this option is set to “All Areas”
- User Duress Reporting. Optional if Duress functionality is employed in the system.

Associations:
- Associated Area. Select the Area that this Terminal will be used to control.
- Associated Door/Side of Door. Optional if access control is implemented.

Terminal Inputs/Outputs:
- Enable Tamper Detection. Must be enabled for Class 2 or Class 3. Optional but recommended for Class 1.
- Enable and name any Inputs that will be used on this Module.

8 INPUT EXPANDERS

Module Settings:
- Poll Time. The default setting of 1 minute is recommended.

Inputs:
- Select the behavior and program a name for each of the Inputs that are to be used on the Expander.

Outputs:
- Select the behavior and program a name for each of the Outputs that are to be used on the Expander.

Lift Interfaces:
- Optional if Lift Access Control is used.

Additional Components:
- Select the Cabinet Tamper Switch Type. For the tamper switches provided with the recommended Inner Range enclosures, select the “Open Circuit Secure” option. Tamper monitoring is mandatory for Class 2 and Class 3.
- Internal Siren Wired/External Siren Wired. These options must be enabled for any 8-Zone Expander Siren output that is used in the system.
- If an Integriti Smart Power Supply is connected to the Expander:
    a) The options “Integriti Smart Power Supply Connected”, “Battery Connected to Integriti Smart Power Supply” and “Enable Battery Testing” must all be enabled.
    b) A “Battery Test Duration” appropriate for the Power Supply load and Battery capacity of the Module must be programmed.

STANDARD LAN ACCESS MODULES (SLAM)

Module Settings:
- Poll Time. The default setting of 1 minute is recommended.

Readers:
- Optional if Readers are used in the system.

Door 1 / Door 2:
- Optional if Door access control is used in the system.

Inputs and Outputs:
- Select the behavior and program a name for each of the Inputs and Outputs that are to be used on the SLAM.

Lift Interfaces:
- Optional if Lift Access Control is used.

Additional Components:
- Select the Cabinet Tamper Switch Type. For the tamper switches provided with the recommended Inner Range enclosures, select the “Open Circuit Secure” option. Tamper monitoring is mandatory for Class 2 and Class 3.
- If an Integriti Smart Power Supply is connected to the Expander:

a) The options “Integriti Smart Power Supply Connected”, “Battery Connected to Integriti Smart Power Supply” and “Enable Battery Testing” must all be enabled.
b) A “Battery Test Duration” appropriate for the Power Supply load and Battery capacity of the Module must be programmed.

3.6 Configure Intruder Detection

Link Inputs to Areas

(Configuration > Areas > Area Input Map)

All Intruder alarm Zone Inputs must be assigned to an appropriate Intruder Alarm Area under the relevant Input Type. This is done by simply adding the Intruder Zone Inputs to each of the pre-configured Intruder alarm input categories provided as shown below:

Input Type	Input Example
Primary (Entry Delay Start)	Intruder detector at a point of entry. e.g. Door Reed or PIR immediately inside a Door.
Handover (Entry/Exit Path)	Internal intruder detector which is in the Entry-Exit path, but not allowed to start an entry timer.
Intruder Inputs (Instant Alarm)	Internal intruder detector.

Edit Area Settings

(Configuration > Areas > Edit Areas)

Program the settings for each intruder alarm area.

a) GENERAL

NAME. Program a name that will identify the area clearly.

b) BASIC CONFIGURATION

ENTRY DELAY / EXIT DEALAY. Set appropriate Entry and/or Exit delay values.

c) MONITORING OPTIONS

REPORT OPENINGS. This option must be set to “Report Openings and Closings (Optional for Class 1)

d) INPUTS

MONITORED INPUTS. Check that the required Inputs have been assigned to the area. If any are missing they can be added by using the ‘Add Items’ button. If adding intruder alarm inputs, make sure the correct Input Type (Process Group) is chosen for each input. *See “Link Inputs to Areas” above.*
IGNORE MODULE HEALTH ISSUES. Ensure that this option is <u>not</u> enabled.

e) SIRENS

SIREN DEVICES / SIREN OUTPUTS. Assign one or more Siren Devices and/or Siren Outputs and select the Location for any Siren Outputs assigned.
Any Siren device or output assigned must be capable of controlling one or more Sirens that meet the requirements of the standard. *See ‘Installing the Warning Devices’ in the Installation section of this manual for more details.*
SIREN TIME. Program the Siren Timer for 5 minutes duration. (Unless a different value is specified by local legislation)

f) STROBES

STROBE OUTPUTS. Assign one or more Strobe Outputs.

Any Strobe output assigned must be capable of controlling one or more Strobes that meet the requirements of the standard. *See 'Installing the Warning Devices' in the Installation section of this manual for more details.*

g) AUTO-ARM

Optional.

h) INPUT AUTO-ISOLATION

AUTO-ISOLATE UNSEALED INPUTS ON USER ARM. This option should remain disabled.
AUTO-ISOLATE UNSEALED EXIT PATH INPUTS ON EXIT. This option should be disabled.

These options should not be enabled unless the system is configured to provide an audible and visual warning to the operator whenever one or more zone inputs are auto-isolated when arming.

3.7 Zone Inputs.

INPUT DEBOUNCE. The input de-bounce time for all wired Zone Inputs in an Inception system is 300mS.
This meets the requirements of AS/NZS 2201.1.

3.8 Module Health.

The "Ignore Module Health Issues" option MUST NOT be enabled.
This option is found in 'Edit Areas' under 'Inputs'. Check all Areas and ensure that the option is not enabled.

Ensure that a 'System Health Area Reporting ID' is configured.
This option is found in the 'Alarm Reporting' options. The default setting is Area 90.

3.9 Configure Permission Group and Roles.

NAME. Program a name to easily identify each Permission Group.
PERMISSIONS. Assign the appropriate entities (i.e. Areas, Doors and Outputs) to each permission group and for each entity define the types of operations allowed and when they are allowed.

3.10 Review and Configure Web Profiles.

Web Profiles must be configured to ensure that the Client cannot make changes to the system configuration that will cause the control equipment to be non-compliant with AS/NZS 2201.1:2007.
i.e. The client operations and view of operational status available via the software must be restricted to the operations and information normally available to the client via the intruder alarm system's user interfaces and indicating equipment.

ITEM MONITORING PERMISSIONS
Ensure that the "Input State" option is set to "View Only" or "None in all Web Page Profiles except for the 'Installer' Web Page Profile.

3.11 Review and Configure Terminal Profiles.

TERMINAL PERMISSIONS.
Ensure that the "Control Inputs" option is disabled in all Terminal Profiles except for the 'Installer' Terminal Profile.

INSTALLER MENU
Ensure that the 'Installer Menu' options are disabled in all Terminal Profiles other than the "Installer" Terminal Profile.

3.12 Create and Configure Users.

a) GENERAL

NAME. Program a name that will identify the User clearly.

b) CREDENTIALS

SECURITY PIN. User PIN Codes must be a minimum length as defined in 'Configure System Settings' above and as agreed in writing with the Client.

LCD TERMINAL PROFILE. The correct profile must be chosen for each User to ensure their LCD Terminal operation permissions are appropriate for their role and level of access.

ENABLE WEB LOGIN. If remote access via the web interface is required, Web Login must be enabled and an appropriate Username and Password that meets the minimum requirements must be programmed.
As described previously, User Passwords must be a minimum length.

To enforce password security, specific requirements for passwords are setup in the 'PIN/Password Policy'.

In order to meet the requirement of Clauses 3.16.2.7 and 3.16.4.5, the security policy must ensure that at least 9000 unique combinations (Class 1 and Class 2) or 900,000 unique combinations (Class 3) are available.
e.g. A password with a minimum length of 5 characters that supports both upper & lower case letters provides over 300 million combinations and will meet the requirement of these Clauses.

WEB PAGE PROFILE
The correct profile must be chosen for each User to ensure their Web Interface operation permissions are appropriate for their role and level of access.

c) PERMISSIONS

PERMISSIONS. Assign the appropriate entities (i.e. Areas, Doors and Outputs) to each permission group and for each entity define the types of operations allowed and when they are allowed.
Select an approThe correct profile must be chosen for each User to ensure their LCD Terminal operation permissions are appropriate for their role and level of access.

3.13 Remote Access and Reporting.

a) USER LOCKOUT.

The Inception Browser supports a user lockout feature by default to meet the requirements of Clause 3.16.2.7.
The settings for the operator lockout feature are predefined and cannot be edited.
On the 4th incorrect login attempt, the login dialogue is locked out for 90 seconds. With each subsequent incorrect attempt 5 seconds is added to the lockout timer up to a max of 3 minutes.

b) REMOTE ACCESS BY A THIRD PARTY SERVICE PROVIDER.

In accordance with Clauses 3.16.2.7 (b) and 3.16.4.5.2, unless otherwise agreed to in writing by the client, the system must be configured so that each remote access procedure will be authorized or manually initiated by the client.

If Client authorization of a third party service provider (Installer) is required, the Inception Controller must be configured so that one or more appropriate users representing the Client have the ability to control the 'Enable Web Login' option for any 'User' representing a third party service provider (Installer).
i.e. Their Web Profile must have the same "Profile Priority Level" and permission to Edit Users.

The recommended method for this is to create a User and a Web Page Profile that are only used for this purpose and not for the general day-to-day operation of the system.

I) Create a new Web Page Profile:

- Enter a name. e.g. Installer Authorization

- Under ‘Item Editing Permissions’, set ‘Users’ to the “Modify” option.
- Under ‘System Permissions’, set the ‘Profile Priority Level’ to the “Priority Five” option.
- Under ‘Dashboard Content’, enable the “User Shortcuts’.

II) Create a new User:
- Enter a name. e.g. System Owner
- Under ‘Credentials’, enable (check) the “Enable Web Login’ option.
- Under ‘Credentials’, enter a suitable user name (e.g. owner) and password of appropriate strength.
- Under ‘Credentials’, in ‘Web Page Profile’ assign the new Web Page Profile created above.

In order to implement this functionality, when the system has been commissioned and tested and has been handed over to the Client, the Client must ensure that the ‘Enable Web Login’ option is disabled (unchecked) for any third party service providers. *See procedure below.*

The Client can now authorize or disable Installer access to the browser as follows:

i) Logon to the browser with the special User logon created above.
ii) Select ‘Manage Users’ from the Dashboard.
iii) Select the User (e.g. “Installer”) that you wish to authorize or disable.
iv) Under ‘Credentials’, enable (check) or disable (uncheck) the “Enable Web Login’ option.
v) Click on the ‘Save’ button at the top of the page.
vi) Logout.

Note: When the Installer’s connection session has finished, the Client must remember to logon again and disable (uncheck) the ‘Enable Web Login’ for that User.

NOTE: If this functionality is implemented, the Client will require written instruction and training in this procedure.

c) Reporting to a Monitoring Centre

See the paragraph “Installing alarm transmission equipment” for additional information.

When installed and configured in accordance with AS/NZS 2201.1:2007 and AS/NZS 2201.5:2008; The Inner Range T4000 Security Communicator meets the requirements for the various Classes of Alarm Transmission requirements when an appropriate Data Plan is chosen. *See the T4000 Installation manual.*

Reporting formats and monitoring plans must be chosen in consultation with the Monitoring Centre.

Configuration > General > Reporting Format Configuration.
Ensure that the ‘System Health Area Reporting ID’ is programmed to an appropriate Area ID number.

4. ROUTINE MAINTENANCE AND SERVICE.

Routine maintenance on Intruder Alarm Systems installed in a client's premises must be performed in accordance with:
AS/NZS 2201.1:2007 SECTION 5. MAINTENANCE AND SERVICE.
AS/NZS 2201.1:2007 SECTION 6. RECORDS AND REPORTS.

Note that this standard requires that routine maintenance be performed at least every 24 months for Class 1 and Class 2, and at least every 12 months for Class 3.

The document "INCEPTION MANUFACTURER'S RECOMMENDED ROUTINE MAINTENANCE" may be used to assist with the requirements of AS/NZS 2201.1:2007 Clause 5.2.1.2

5. RECORDS AND REPORTS.

Client and equipment records, maintenance records, authorizations and logbooks must be performed and maintained in accordance with:
AS/NZS 2201.1:2007 SECTION 6. RECORDS AND REPORTS.

For the purposes of these records, it is required that the installer keep note of the details required below as the installation work is performed.

Client and equipment records must include the following information as a minimum:

1. The address and an outline plan of the alarmed premises showing any unusual features.
2. The position and type of each detection device.
3. Installation, description and wiring diagram.
4. The position of any communication path and 240 V a.c. power outlets associated with the intruder alarm system.
5. The classification referring to the premises or to each detection sector, if applicable, and which shall be in the form of a certificate confirming compliance with this Standard, and noting any exceptions/non-compliances, if applicable.

6. DOCUMENT REVISION HISTORY

Revision 1.0 25 September, 2023.

Disclaimer:

1. The manufacturer and/or its agents take no responsibility for any damage, financial loss or injury caused to any equipment, property or persons resulting from the correct or incorrect use of the system or its peripherals. The purchaser assumes all responsibility in the use of the system and its peripherals.
2. While every effort has been made to ensure the accuracy of this manual, the manufacturer assumes no responsibility or liability for any errors or omissions. Due to ongoing development, product specifications and the contents of this manual are subject to change without notice.

Document Part No: 636001AUC3

Please send any comments regarding this manual to publications@innerrange.com