12 – Security, CCTV and Access Control

Version	Date	Authors	Summary of Changes
1.01	4 April 2012	Alex Chryss	
1.02	15 January 2013	Ben Crossling	Changed references to Project Lead
2.0	26 October 2015	Ross McLoughlin	General Revision
3.0	19 December 2023	Joe Ducie	General Revision

Security Systems General

Closed Circuit Television Systems General

Access Control General

Security Systems General

12.01 The Campus and Buildings Requirements Manual (the CBRM, the Requirements or the Manual) documents the minimum design and construction requirements for new, refurbishment or repurposed building works, landscapes and engineering/infrastructure projects on buildings, facilities and campuses of the Australian National University (the ANU or the University). The Requirements are prepared for the direction of a Consultant, Designer or Project Manager in the preparation of project specific documentation and in the delivery of project works.

12.02 Notwithstanding any Consultant's particular discipline or area of responsibility, each Consultant and/or designer shall consider the document in its entirety. The complete CBRM consists of the following Sections which may be referred to within this Section:

Campus and Building Requirements Manual	
Section 01	General Requirements
Section 02	Architectural Requirements
Section 03	Roads, Car Parking & Civil Works
Section 04	Soft Landscaping
Section 05	Roofing, Roof Fabric & Roof Safety
Section 06	Building Management Systems
Section 07	Electrical Services
Section 08	Fire Protection Systems
Section 09	Hydraulic Systems
Section 10	Mechanical Services
Section 11	Lifts, Cranes & Vertical Transportation Systems
Section 12	Security, CCTV & Access Control

Principles of Security Levels

12.03 The appropriate level of security shall be established during the design phase of the project.

12.04 The degree of damage, which could be caused to the ANU through personal injury; loss of or damage to property (including intellectual property); or interruption of a critical service determines the basis for the level of security for buildings, or areas within buildings.

12.05 The ANU has a policy on site security that is predicated upon electronic access control for all perimeter doors on campus. Through a process of risk assessments during design and throughout the life of the building additional security requirements may be identified to attain the appropriate level of security risk management.

12.06 All perimeter doors shall be electronically secured and monitored to ANU specifications (available separately) with backup manual locking to protect against long term power outages. Internal doors maybe locked electronically or using a keying system appropriate for the area. Electronic security devices shall be used internally when risk assessments indicate a higher level of security is required. The type and location of any electronic security device shall be subject to discussion with the Principal's Representative (the Principal or the Principal's Project Manager) during the early design stage.

Application to Building Design

12.07 Design principles having security implications include the following:

- electronic access control systems;
- passenger lift control functions;
- design of the building façade;
- design of accessible low level windows;
- design of internal areas to ensure that high security functions are grouped together;
- external lighting; and
- profile of usage e.g. afterhours access, types of research and teaching, security risks for visitors, students or staff members emanating from the activities within the building.

Crime Prevention through Environmental Design (CPTED) Principles

12.08 CPTED is to be incorporated into the design of new buildings (and major refurbishments) in accordance with the policy: http://policies.anu.edu.au/policies/security_buildings_and_site/policy

12.09 Where major building renovations or changes to building usage are intended, a security design consistent with the ANU's principles shall be provided.

12.010 Where applicable, refer to the Principal's Representative for a security risk assessment and Section.07 Electrical Services for guidance on luminaires and Section.08 Fire Protection Systems.

Peripheral Security

12.011 External lighting shall be provided to all buildings to ensure that:

- the main external entrance is well lit; and
- all perimeter doors and other ground floor points of access are properly illuminated.

12.012 Security lighting from the building shall extend to adjacent car parks and associated illuminated pedestrian path.

12.013 The building façade shall be designed to minimise recesses, alcoves, columns and the like that may be a security hazard.

12.014 Plant room access shall be isolated from the main building security perimeter to ensure that service personnel need not enter secured areas to access the plant room.

12.015 Main entry doors shall be the principle access for all people entering or leaving the building.

12.016 Standard doors located on the building's façade shall be fitted with magnetic locking devices wherever possible. Where reed switches are used, they should detect door open/closed status. Where double doors are installed, the inactive leaf shall be secured with a lockable panic bolt, keyed to the building's master key system. A suitable door-closing mechanism shall be installed on each active door leaf.

12.017 Electromechanical doors shall be fitted with the appropriate actuator linked to the electronic access control system.

12.018 Door actuators shall have the following features:

- Automatic door controllers are required to be serviced by the ANU service provider and are required to have universal service access.
- battery back-up for a minimum of 8 hours in the event of mains power failure. In the event of a power failure, the battery back-up system should keep the doors locked and secure unless there is a fire alarm;
- the ability to physically monitor doors when open and closed;
- contain a separate electric lock for positive locking;
- the ability to monitor the status of the electric lock;
- Automatic safety reversing of doors;
- self-checking safety Photoelectric Beams (P.E. Beams); and
- afterhours access via an electronic control system and manual override.

12.019 Emergency exit doors shall have the following features:

- no external door furniture;
- all door furniture shall allow for single handed operation;
- doors shall be hung to open out with triple hinges of a secure design and construction;
- door closing mechanism to ANU specification; and
- doors shall be of solid core construction (fire rated as necessary).

12.020 External doors shall be secured by an electronic lock linked to the fire alarm and/or the ANU central monitoring station.

12.021 Where keyed locks are accepted by the ANU, reed switches shall be installed to monitor door open/closed status.

12.022 Electronic access systems shall meet the ANU specifications and integrate into existing monitoring arrangements, be fully monitored and programmable to lock/open doors as required by a user defined schedule. Magnetic card swipe readers shall allow access/egress outside normal business hours. All fire exit doors (access controlled) shall have connections between the fire and Cardax system as appropriate to ensure compliance with fire trip requirements.

Internal Security

12.023 The level of security required by the ANU and the building user through a risk assessment process shall determine the level of security systems used within buildings.

12.024 Generally, areas shall be zoned according to their security requirements with high security areas grouped together. The principles outlined in test required shall be utilised when establishing the security requirements for access to each zone within a building.

12.025 Internal exit doors shall be keyed to the building's master key and lock system.

12.026 Additional security devices may be required within specific areas and may include the following:

- electric door strikes;
- key override switches;
- emergency release latches;
- request-to-exit push buttons;
- duress alarm buttons;
- break glass units;
- passive infra-red detectors;
- communications systems; and
- Closed circuit television (CCTV).

Closed Circuit Television Systems General

12.028 The ANU will review and ensure compatibility of any proposed and designed CCTV system based upon the IP CCTV System detailed below. The system shall be a Geutebruck (or equal equivalent capable of system continuity and consistency) fully IP CCTV System, installed by a certified installer.

12.029 Provide an IP based CCTV surveillance system to permit overall visual surveillance by ANU Security of public and secure areas. The system will comprise of network switches, backbone cabling, IP CCTV Cameras, server and monitor and all required brackets and housings in order to ensure system is operational. All cameras shall be powered using power over Ethernet (PoE) in network switches.

12.030 Design all interface equipment and any necessary lightning protection and other items to make the system completely operational.

12.031 Provide a complete and separate Local Area Network (LAN) backbone to facilitate the transferring and communication of all video and data between equipment. Liaise with the Principal's Representative on system design and setup including the installation of relevant client software. All elements within the CCTV system are to support IPv6.

12.032 All CCTV control, monitoring and recording equipment shall be housed within the Leonard Huxley Datacentre, or other location nominated by ANU Security.. Equipment racks are to be included in system design.

12.033 All necessary system design, programming (i.e. videotext, point descriptors, display maps, alarm message text) is to be included.

Cameras

12.034 Camera images are to provide clean, roll-free switching and image stability. All cameras shall be fully compatible and integrated with the Geutebruck software, in appropriate domes or external grade housings as locations dictate. Cameras shall be provided with Activity Detection and Video Motion Detection inside the camera.

Lenses

12.035 All lenses used are to be constructed of colour corrected glass optics and have steel body construction. To accommodate any changes in lighting, all lenses are to be identical in make and model and be Direct Coupled (DC) Auto Iris types. Lenses are to be of reputable manufacture that has been operating in the optics industry for over the past ten years. Acceptable types include Pentax, Computar, Fujinon, Navitar and Panasonic. Final selection of focal length will be made on site by the Consultant system designer.

Camera Housings

12.036 All Camera housings are to conform to the following:

- minimum internal dimensions to accommodate the camera and lens;
- fit with tamper locks to prevent unauthorised access;
- fit with tamper switch to be monitored by security system;

- completely sealed to protect against environmental damage and condensation;
- any dome housing utilising tint is not to reduce light input by more than 1 F stop;
- all external housings are to be mounted at a minimum of 3.0 m off ground level. Any housing below this height must be a high security type; and
- all internal cameras are to be mounted at a minimum of 2.2 m off ground level.

12.037 Camera mounting is to conform to the following:

- all cabling to the camera is to be concealed within the mounting bracket;
- utilise any accessories e.g. ceiling/wall/pole mount brackets, as required by the situation;
- all cameras mounted on brackets are to provide manual adjustment of position of +30º to -90º tilt and 360º pan;
- be firmly locked into the desired position and be rigidly supported to prevent any vibrations and movement; and
- the housings tendered are to be demonstrated to the Consultant system designer prior to install for evaluation.

Internal Dome Housing

12.038 All cameras to be mounted internally are to be placed in a housing conforming to the following as a minimum:

Internal Dome Housing	
Style	Flush/recess mount dome housing
Construction	1.2 mm extruded aluminium, mild steel camera bracket
Lens	3 mm optically clear acrylic dome with no distortion in any section
Black inner liner	Tinted dome option
Finish	Polyester powder coated, colour to suit environment
Rating	IP55, IK06
Mounting	Upper section flange mounted to fixed ceiling or tiles
Camera Access	3 x spring clips to remove lower dome hemisphere
Cable Entry	1 x 20 mm poly(vinyl chloride*)* (PVC) gland on top rear
Internal Dimensions (WxHxD)	To accommodate proposed camera and lens combination

External Dome Housing

12.039 All fixed cameras to be mounted externally on a penetrable ceiling or eave and are to be placed in a weather proofed housing and fitted with heaters as appropriate for Canberra climate as detailed. Housing to further conform to the following:

External Dome Housing	
Style	Flush/recess mounted dome housing
Construction	1.6 mm extruded aluminium, mild steel camera bracket
Lens	3 mm MR10 GE Lexan (Polycarbonate) optically clear polycarbonate dome with no distortion in any section. Black inner liner Tinted dome option
Finish	Polyester powder coated, colour to suit environment
Rating	IP66, IK10
Mounting	Flush – upper section flange mounted to fixed ceiling Surface – housing to be secured to surface
Camera Access	4 x M6 Stainless steel security screw to remove lower dome hemisphere
Cable Entry	1 x 20 mm PVC gland on top rear
Thermostatic Controlled Heater	Factory Option. 7 W nominal (Canberra – minus 5°C operability)
Thermostatic Controlled Fan	Factory Option. 7 W nominal
Internal Dimensions (WxHxD)	To accommodate proposed camera and lens combination

External Tubular Housing

12.040 All cameras to be mounted externally on a wall or a non-penetrable ceiling and are to be placed in a housing conforming to the following:

External Tubular Housing	
Style	Tubular housing mounted on adjustable manual pan/tilt bracket. Mounted on suitable wall bracket
Construction	1.6 mm extruded aluminium
Lens	6 mm MR10 GE Lexan (Polycarbonate)
Finish	Polyester powder coated, colour to suit environment
Rating	IP66, IK10

Mounting	Upper section flange mounted to fixed ceiling or tiles
Camera Access	4 x M6 Stainless steel security screws, flip top construction
Cable Entry	2 x 20 mm PVC cable compression glands
Sunshield	Adjustable along length of body
Thermostatic Controlled Heater	Factory Option. 7 W nominal
Thermostatic Controlled Fan	Factory Option. 7 W nominal
Internal Dimensions (WxHxD)	To accommodate proposed camera and lens combination
Weight	Approximately 4 kg

Power Supplies

Power over Ethernet

12.041 Where possible, all cameras are to be powered from the same point (circuit) in order to maintain synchronization and avoid ground loops. All cameras are to utilise the IEEE802.3af PoE standard for the supply of power. Further, support for IEEE802.3at is preferable.

12.042 PoE is to be supplied from associated network hardware such as switches.

Server and Network Video Recorder

12.043 The complete CCTV system comprises a complete CCTV management server and software package that will allow the operator full control of the various components within. The entire system is to be controlled via a Graphic User Interface (GUI) front end. The system will encompass a server and client machines for each operator as needed. The system will be a Geutebruck GeViScope-IP/SE and be provided with the following:

- the GUI will provide a dynamic interface allowing real-time updating of indicators such as all text, position of cameras and alarm statuses via multi coloured icons;
- the GUI must allow for the display of multiple cameras from multiple sources on the one screen. Cameras are to be listed in a tree format to the side of the viewing area. Multiple screen layouts are to be provided. Populated layouts are to be able to be saved retaining server and camera number and position for each spot;
- the GUI must be provided with MultiMap with as many individually designable maps for intuitive operation of the entire system as desired;
- display live camera images by the clicking of an icon on the map screen;
- incorporate programmable ‘macros’. Each macro is to have a minimum of five steps;
- the GUI will use password protection to allow login and logout. The user management system will allow for multiple permission levels so as to restrict functionality from certain users. An event log will allow all actions on the server to be recorded. This must be retained for a minimum 31 days on a separate physical backup location identified by the ANU;

- it shall be possible to display the video images in any combination on the overview monitor (e.g. 25, 16, 8, 4 way split, one quad and graphic display per screen, multi-images per screen, or any other combination). The content and orientation of the information shown on these screens shall be flexible allowing for live video, data, maps and other forms of visual cues to be displayed in a variety of formats. As a minimum, up to 16 separate live (real time) images at 4CIF each, shall be displayed per overview monitor;
- all recorders, switchers, control systems and other primary equipment shall be time synchronised to maintain time continuity across all components;
- all equipment (where practical) shall be assembled off site and fully tested prior to installation and operation;
- provide full 32bit SDK for high level integration;
- video motion detection shall be provided on the camera rather than on the server. When in dormant state, a camera's image shall be recorded at five frames per second at 4CIF. When movement is detected, the camera's full frame rate at 4CIF shall be recorded;
- the system shall be provided with a minimum 4 TB activated database size. Footage shall be stored on the server until either dumped to the ANU campus wide archive storage. Recorded footage can be overwritten with new footage once the local storage is full;
- the system shall be integrated into the ANU campus wide archive storage and configured to dump it's footage on a 24 hour cycle; and
- the system shall be provided with a suitable monitor, keyboard and mouse.

Monitors

12.044 Provide a 19" (48 cm) TFT display with 1 x DVI-D and 1 x VGA input for use in combination with Geutebruck video surveillance systems. The operator monitor is to comply with the following minimum:

Monitors	
Size	19" active matrix TFT LCD
Display Colours	Over 16 Million colours.
Resolution	1280 x 1024 @ 60 Hz.
Pitch	0.26 mm dot pitch or better.
Brightness	300 cd/m white luminance- typical
Contrast Ratio	800:1 contrast ratio- typical
Response Time	5 ms or less
Viewing Angle	176/170 viewing angle (H/V) minimum
Video Input	VGA - 15pin D-sub. and DVI-D

Case	Black Plastic
Stand	Detachable, Adjustable
Power Consumption	37 W (<2 W in power save mode)

Networking Equipment

12.045 It is the Consultant's responsibility to ensure that the network infrastructure is designed and installed correctly to allow for the IP traffic expected by their solution. The network is to be designed to allow for the simultaneous recording and viewing of all documented cameras (at 25 frames per second at 4CIF) from the main server.

12.046 A separate LAN is to be created for the interconnection of all IP based CCTV system components. As a guide, the private architecture will entail:

- all cameras and encoders are to be connected via TCP/IP to an edge network switch with POE (IEEE 802.3af supply to each port);
- all edge switches will be connected to the core switch(s) by optical fibre cabling;
- the management PC, Network attached storage, client machines, printers and all other peripherals are to be directly connected to the switch(s) via a Gigabit connection;
- the system shall be capable of performing at full capacity across multiple nodes and switches within the network;
- a single port is to be connected to the ANU's WAN for integration into the Campus Security Network. To be either Cisco or HP; Conform to C-Tick, CE Mark, FCC Part 15 Class A;
- provide LEDs for speed, link, PoE and activity on each port. Support switch latency of < 20µs for 64byte frame;
- be rack mountable;
- edge switches to be Layer 2 management and located in the Communications Room closest to the camera location. Each Communications Room shall be provided with provided with four spare switch ports for future cameras;
- core switch to be Layer 3 management and located in the ground floor main Communications Room; and
- be provided with a minimum five year warranty.

Access Control General

12.047 The ANU access control system is based upon the Cardax (Gallagher) access control system. The proximity readers utilise Mifare Plus (128 bit AES encryption).

12.048 The ANU requires compliance with *AS 14443 Identification cards – Contactless integrated circuit(s) cards – Proximity Cards* on this component with important additional requirements.

12.049 The access control system will also need to comply with any specific project requirements issued by the ANU in addition to the CBRM, relevant Australian Standards and codes as applicable. Consultants are required to refer to Section.07 Electrical Systems of the CBRM and the ANU Information Technology Services (ITS) Cabling Specification.

Australian Electronic Standards

Unless otherwise stated in this specification all installations must comply with the following Australian standards.

- AS/NZS IEC 60839.11.1:2019 – Electronic access control systems
- AS/NZS 2201.1:2007 Intruder alarm systems
- AS/NZS 3000:2018 Amd 1:2020 Electrical installations (known as the Australian/New Zealand Wiring Rules)
- AS/CA S009:2020 - Installation requirements for customer cabling (Wiring Rules)
- AS/CA S008:2020 - Requirements for customer cabling products

Persons carrying out cabling works on campus must hold a current cabling license.

Communications cabling shall only be carried out by an ANU approved communications contractor.

12.050 Consultants are also advised to ascertain from the Principal’s Representative the level of interfacing between the Cardax system and other security and building systems at the time of project design. Consultants are also to apply the principles of the ANU Security: Buildings and Site policy.

Requirement

12.051 Access card specifications will need to comply with AS 14443 for proximity cards used with the Cardax or equal equivalent system.

12.052 The ANU has specified a minimum requirement of 128 bit AES encryption for the proximity card system chosen - Mifare Desfire EV3. (X configuration).

Replacement of Existing Hardware Where Required

12.053 Clear descriptions of how the work would be accomplished within buildings with areas of possible concern clearly explained in a series of compliance statements.

Functional Overview - Electronic Access Control System - Campus Wide System

12.054 The system shall provide a means to control access through nominated doors having electric locking door status monitoring and access control readers. Access rights associated with a presented access card shall be checked for validity based on card, access area, access time and any other access management function defined in this specification; as stored in intelligent field controllers. Access shall be granted or denied, dependent on the access privilege. Access rights shall be programmed in a variety of ways to allow flexibility.

12.055 The system shall provide access control in elevators as identified in schedules enabling the access of each cardholder to have access to any combination of floors over specified time periods. The interface to the elevator manufacturer's equipment shall be by either low level interface (relay outputs) or preferably by a high level (data) interface.

12.056 The system shall monitor the condition of inputs. The system shall be able to be programmed to apply a variety of conditions to the way in which these inputs are monitored and shall enunciate the condition of such inputs in accordance with such programming.

12.057 The system shall provide a fully functional intruder alarm system including entry and exit delays where intruder detection sensors are connected to system inputs. The intruder alarm systems component shall be fully integrated with the access control aspects of the system. It shall be possible to set (secure) or unset (unsecure) areas from any access control reader associated with an area, or via Remote Arming Terminals (RAT's) or as required from defined central control locations.

12.058 Intercom functionality shall be integrated with a card reader, enabling a card reader user to talk to an operator as and when required, and an operator to talk directly to the card reader user. All intercom communications shall utilise the common Integrated Security system network and communications cabling infrastructure; and be fully integrated with the access control system.

12.059 The system shall provide an integrated software facility for the design and production of photo ID cards.

12.060 The system shall be 'OPC Alarms and Events' enabled using Microsoft COM and DCOM enabling integration of event data with other third party OPC enabled automation and business systems.

12.061 The system shall allow data exchange with other applications using REST API protocols for schedule changes, and card record changes. The system shall be capable of carrying out the data exchange on a batch or real time processing basis.

12.062 The system server shall be Microsoft Windows (enterprise edition) compatible. If an alternative operating system is designed, full details must be supplied on how the alternative meets the ANU criteria.

12.063 All system communications must be totally integrated with either existing or new firewalled LAN/WAN networks using the ANU IP numbering scheme.

12.064 Connection to Intelligent Field Controllers (IFCs) shall be achieved using Ethernet cabling supporting 10baseT and TCP/IP protocols. The network connection must be on-board the IFC. Interface transceiver units (10BaseT to RS485, RS232 and the like) are not acceptable.

12.065 Remote IFCs not permanently connected to the network can be connected via a PSTN service, using TCP/IP protocols.

12.066 Connection from the remote IFC to the server shall be either via dialup to an Internet Service Provider (ISP) using encrypted TCP/IP; and then via an approved firewall through into the IT environment or via dialup directly to a remote arming station (RAS) connection to the Server

12.067 All system software upgrades shall be downloadable through the network to the IFC.

12.068 All data communication internal to the system on the TCP/IP network between IFC's and between IFC's and the Server shall be encrypted using symmetrical session keys and an industry-standard encryption algorithm to a minimum of 40 Bits (Secure Socket Layer). Session keys shall be changed on a regular basis at intervals no longer than 24 hours.

12.069 The system shall report all events to the operator(s) as configured and shall produce and maintain a log of all system events, alarms and operator actions.

12.070 The system shall provide a means for an operator to extract information relative to the event log and system configuration and produce this information in the form of printed reports, screen displays or ASCII files.

12.071 The system shall provide for a Windows based User Interface with Site Plans and interactive icons representing the location and real-time status of access control, and alarm monitoring equipment.

12.072 The system must provide emergency evacuation reporting.

12.073 All equipment shall have the following approvals:

- FCC Part 15;
- CE approval BS EN 50130; and
- CE approval BS EN 55022.

12.074 Encoders and readers shall also meet:

- CE ETS 300 683 Short Range Devices; and/or
- C-Tick RFS29.

12.075 The system software shall be written in a fully structured, fully validated and commercially available language that provides a strictly controlled development environment.

12.076 Comprehensive backup and archiving facilities shall be incorporated as an integral part of the system software.

12.077 The system shall include system division suitable for multi-tenanted buildings. Operators shall only be able to access those parts of the system which fall within their division and operator privileges.

12.078 IFCs must support peer to peer communications for input and output communications between IFC's. Systems that require the main server for communications between panels are unacceptable.

1) Programming - Gallagher

12.079

12.080 Permission to program within Gallagher Command Centre and Configuration client must be sort via the ANU Unisafe Operations Manager.

12.081

12.082 System programmers must hold a Gallagher channel partnership, individual certification and ACT security license.

12.083

11.1) Programming Notes

Consistency

12.084 Gallagher programming must match existing conventions. Programmers must take time to familiarise themselves with the existing programming style and replicate this for new works.

12.085

Icons

12.086 Some Command Centre items have custom icon sets including:

- Power supply Inputs
- Fire inputs
- Sirens
- Break glass units
- Duress buttons

12.087 New programming must make use of the same icons.

12.088

Controller Alarm Zones

12.089 Each controller must have its own alarm zone. Alarm zones, as a general rule should not be shared across controllers. Dedicated alarm zones shall be used for alarm systems.

12.090

Access Programming

12.091 Gallagher integrators shall not program or modify cardholders, cards or access groups. Assigning access and making user changes shall be performed by ANU staff only.

12.092

12.093 Please provide ANU Unisafe two weeks' notice for access permission work.

12.094

Nuisance Alarms

12.095 System items that are undergoing modification or installation should be programmed such that regular nuisance alarms do not feature in the alarm stack. Remove alarm zones until items are fully commissioned.

12.096

De-commissioning

12.097 Decommissioned items shall be fully deleted from the system. This includes all hardware items, access zones and any items featuring in Command Centre site viewers. No items shall be left, un-allocated in the hardware tree.

12.098

Divisions

12.099 When programming new items care must be taken to assign them to the correct division.

12.0100

Log and Event

12.0101 All general inputs and outputs shall at minimum shall use the 'log and event' action plan. Note that if the input type already logs an alarm by default, then the action plan should not be modified.

12.0102

Cross Controller Programming

12.0103 Site items that are inherently associated with each other, such as door or alarm components must be connected to the same controller. Alarm zones and other connections must also be associated with the same controller.

12.0104

12.0105 Cross controller connections and programming, such as a reader on one controller and the exit button for the same door on another controller will be rejected. Similarly, area alarm sensors, sirens and keypads shall be connected to a single controller wherever possible.

12.0106

11.2) Doors

Access Zones

12.0107 Generally, each door will have a matching access zone. It is not usually permitted to share a single access zone between multiple doors. Access zones will not normally be associated with an alarm zone for general door use.

12.0108

Doors

12.0109 In general doors shall be programmed with an alarm zone, entry access zone, open and unlock inputs, readers and a lock output. Most doors shall not feature an exit access zone. This allows any ANU card holder to exit the door.

12.0110

Advanced Tab

12.0111 Retry the lock shall be disabled.

12.0112 DOTL warning = 20 seconds

12.0113 DOTL alarm = 120 seconds

12.0114 Door forced shall be enabled for doors without a free handle exit

12.0115 Automatic door will have the confirmed as closed timer extended to 1000 milliseconds.

12.0116

Scheduled Alam Zone

12.0117 Doors in general office/teaching buildings shall be programmed with a scheduled alarm zone.

12.0118

12.0119 This scheduled alarm zone shall disable DOTL and door not locked alarms from 0800 to 1600 to help prevent nuisance alarms in the alarm stack.

12.0120

12.0121 At least one scheduled alarm zone shall be programmed per building and shall be associated with a local controller.

12.0122

12.0123 Allow to work with the building manager and ANU security to identify doors that should not use the scheduled alarm zone.

12.0124

11.3) Alarm Priorities and Mimic Panel

Alarm Priorities

12.0125 Default alarm priorities shall be used for most items. Specific alarms shall be assigned higher priorities. These specific alarms include but are not limited to:

12.0126

12.0127 Critical Priority

- Duress
- Intrusion
- Controller offline
- Fire, power and battery alarms
- Smoke alarms
- Freezer/Fridge alarms

12.0128

12.0129 Very High Priority

- Cabinet tamper
- Break glass activations

12.0130

12.0131 Other events may be allocated specific alarm priorities after confirming with the ANU Security operations manager.

12.0132

12.0133 Custom action plans have been created for common alarms and are to be used when appropriate, for adding or modifying associated site items.

12.0134

01. Break Glass Alarms - Campus Wide
02. Gallagher Panel Inputs - Campus Wide

12.0135 Campus Wide DNL Never Action Plan

12.0136 Campus Wide DNL Scheduled Action Plan

12.0137 Campus Wide DOTL Never Action Plan

12.0138 Campus Wide DOTL Scheduled Action Plan

12.0139 Campus Wide Forced Door Scheduled Action Plan

12.0140 Campus Wide Input Scheduled Action Plan

12.0141

Mimic Panel

12.0142 Several specific alarm sources must trigger the ANU control room mimic panel. There are custom action plans available for this purpose. These sources include.

- Break glass alarms
- Intrusion
- Duress activations
- Power
- BMS

Readers

12.0143 All readers installed on campus in new installations are required to be Cardax (or equal ANU approved equivalent) T-15 Multitech, Mifare Desfire (X configuration) proximity readers, charcoal grey in colour or to match existing installation.

Key Pads

12.0144 Keypads, including combined card reader/keypads shall be Gallagher T30 Multi Tech in black.

T30 keypads are typically used where a pin is required for entry via an access-controlled door or gate.

Terminals

12.0145 Terminals for arming/disarming shall be Gallagher T20 in black. Where access control is also required the terminal shall be Gallagher T20 Multi Tech in black.

Lock Types

12.0146 The locking devices controlled by these systems shall be either the Magna lock type or the Padde ES2000 type. Some variations may be encountered, such as automatic doors, all documentation is to be provided to the Principal's Representative for review prior to final specification.

12.0147 Padde EML6 for single leaf doors. Incorporating bond sense, LED on lock and 1500 LBS holding force.

12.0148 Padde EML10 for double leaf doors. Incorporating bond sense, LED on lock and 1500 LBS holding force.

Locking Style

12.0149 All locks shall be the fail to safe type (power on to lock).

12.0150 All Magna lock types shall be fitted with tamper proof screws if on the non-secure side and to include appropriate mounting equipment for inward and outward swing doors.

12.0151 All Electric strikes shall be fitted with a diode across the coil to reduce "Back EMF". Strikes shall also have high strength striker cover plates securely mounted to protect the tongue and lock mechanism from being forced or manipulated. Where an electric strike is fitted, the coil sense (LSS) and tongue sense (DSS) shall be monitored in series via a single input and programmed as the "unlock" input. Tongue sense shall not be used as the "open" input or as an egress input under any circumstance.

12.0152

12.0153 Where the door features a free handle exit, the door forced option will be disabled within programming.

12.0154

12.0155 All electric strikes shall be configured as fail safe unless specified otherwise and/or approval is given by the ANU Unisafe team.

12.0156

12.0157 Unused wires from the electric strike must additionally insulated so the ends cannot contact any metal surface.

12.0158

12.0159 The use of pre-load electric strikes in new builds shall be avoided in favour of a correctly installed strike and door hardware. In new builds the door should not place excessive pressure on the strike. Pre-load electric strikes may be used to solve issues during retrofits.

12.0160 Magna lock types (unless otherwise approved) shall always be installed on the secure side of a door.

12.0161 An additional manual lock set will be provided (where none pre-exists) to ensure that the door can be secured should the access or power system fail (cylinder and key format to be specified by the ANU).

Electromechanical Locks

12.0162 Electromechanical locks shall not be used on campus. Repairs to existing electromechanical locks or replacement of doors that feature electromechanical locks shall be cause for a full replacement with an electromagnetic lock.

Fire Trip

12.0163 Access control doors shall be interfaced to the buildings fire indication panel to provide an egress path in the event of a fire. Detection of fire by the FIP anywhere in the building shall trigger the fire trip interface.

12.0164 Fire trip Interfaces shall be via a dedicated power distribution module complete with integral fire trip relay. Individual outputs from the PDM shall be configurable to either fire tripped power or standard power. A secondary contact on the fire trip interface relay shall be monitored via a separate input to the EACS controller to provide an alarm to the control room in the event of a fire relay activation.

Break Glass Units

12.0165 All electric locks installed must have a Green break glass unit mounted adjacent to the door at 900-1200 mm above finished floor level. Fracturing/breaking the glass or plastic must initiate a direct break in lock power to allow free egress and produce an individual alarm on the Command Centre e.g. Glass broken.

12.0166 Green KAC type break glass units shall be used complete with plastic re-settable inserts on all access control doors excepting those with free handle exit. On activation the positive side of the lock power circuit must be interrupted thus releasing the electric lock.

12.0167 A second contact of the break glass unit shall be monitored via a separate input to the security controller. This input shall be programmed to raise an alarm in the Command Centre alarm stack if the break glass unit is activated. The campus wide break glass action plan shall be used.

12.0168 Under normal circumstances the break glass input be shall not be used as a remote release or emergency input in the door programming.

12.0169 Note that a break glass unit fitted to the door does not negate the need for a fire trip.

12.0170

12.0171 The break glass (Green) shall be key resettable dual pole units utilising plastic inserts.

12.0172 The initiation of free egress via communication input is not permitted.

Reed Switches

- Sentrol type flush type;
- 19 or 25 mm; and
- Only be surface mount where flush mount is not suitable.

Power Supplies

12.0173 Low voltage power supplies shall be self-contained and installed within the secure equipment cabinets. The power supplies shall be a switch mode with a minimum capacity of 2 A and shall have stand by batteries capable of sustaining continuous operation for at least eight hours in the event of a mains supply failure. Power supplies to incorporate mains fail and battery low indications.

12.0174 Power supplies shall not be loaded greater than 65% of their rated capacity for new installations and 80% for additions to existing power supplies. This load shall be calculated using the assumption that all locks and relays are powered.

12.0175 As part of commissioning documentation for new works, a power supply load calculation must be submitted showing a per device break down of current draw per power supply. Device technical data sheets shall be used to derive this current calculation.

12.0176 The 1A auxiliary output featured on Gallagher 8A power supplies shall not be used to power controllers or electric locks.

12.0177

12.0178 All power supplies will be Austel Approved 240 V/12 V DC.

12.0179 All power supplies must have their mains and battery condition monitored and shall activate an alarm on the Cardax or equal equivalent System if a problem occurs for example loss of mains (240 V) and/or low battery alarm.

12.0180 The ANU prefers the use of linear power supplies to reduce any possible interfaces to the facilities electronic equipment used in high technology buildings.

12.0181 The minimum specifications as above shall be utilised when supplying linear units.

12.0182 Details must be provided in the material list of the capacity and type of each power supply included to meet the tender requirement.

12.0183 Power supplies shall be scaled up in output capacity so as to have the ability to recharge the connected battery/s from a fully discharged condition without tripping or failing.

Batteries

12.0184 EACS power supplies shall be provided with a backup battery capable of maintaining full system operation for a minimum of 8 hours. The power supply battery charging circuit must be capable of charging a flat battery to full charge within 24 hours.

12.0185 On installation, back up batteries will be clearly marked with an installation date and an expected replacement date. Replacement dates will be two years post installation.

12.0186 Cables connecting batteries to power supplies must be sized to handle the maximum current draw of the power supply plus 20%.

12.0187 EDAM BA006 (or equal equivalent) minimum 12 V 7 A per hour capacity (sealed unit).

12.0188 Be monitored by the power supply for low battery alarm.

12.0189 Battery capacity scaling shall be considered in lieu of multiple minimum sized units.

Equipment Cabinets

12.0190 New building designs that include a single large 'Rittal' style cabinet are preferred. Gallagher dual cabinets are acceptable for smaller installations.

12.0191 New cabinets shall have approximately 20% spare capacity. That is, as a guide, space for the addition of expanders to accommodate 20% more doors/inputs/outputs.

12.0192 Cabinets shall feature cable management such as slotted trunking and shall be kept neat and tidy.

12.0193 Gallagher Dual cabinets shall not contain more than one controller. Double stacking of controllers or expanders will not be permitted.

12.0194 Security cabinets shall be centrally located. Ideally one security cabinet shall serve an entire building, or, in the case of large buildings, one security cabinet shall serve an entire floor.

12.0195 Distributed cabinets and controllers located at doors shall be avoided.

12.0196 Security cabinets will ideally be located within a dedicated security room or riser. Cabinets may also be located within a communication room. Care must be taken that cabinet locations do not impede travel paths or access to racks within communication rooms.

12.0197 Cabinets must be accessible without needing a ladder. The top edge of security cabinets shall not be mounted above 1800mm AFFL. Space for additional cabinets and future expansion should be considered when installing new cabinets.

12.0198 All equipment cabinets are to be tamper monitored to both the door and to the rear-mounting surface.

12.0199 All wiring inside the enclosure shall conform to Australian Standards and Section.07 Electrical Systems.

Time Controlled Access Doors (TCR)

12.0200 All doors installed without readers will comply with Section.02 Architectural Requirements.

12.0201 Each TCR will have the reader cable installed and located above the door for future reader connection.

12.0202 Hardware allocation should allow for the future connection of the reader to the system.

Request to Exit Button

12.0203 Any exit buttons specified will meet the *AS 1428 Design for Access and Mobility* suite of standards for location and operation.

The request to exit button shall be an approved button assembly equal equivalent to the EX16 specification.

Press to exit buttons shall be wired to an individual EACS input. The normally open contact shall be used for connection to the security controller.

Exit buttons that directly cut lock power or directly control an automatic door shall not be accepted.

Electrical light switch style exit buttons are not to be used.

12.0204

Security Alarms

12.0205 Within the ANU Campus there were two options for installing alarms systems, the first is to utilise the Gallagher access control system and the second is the stand alone alarm system. The ANU will, where possible replace existing stand-alone security/intruder detection panels with an integrated access control and intruder alarm system. For all new systems an integrated access control and intruder alarm system is to be designed.

12.0206 For alarm system indication there are a minimum of two approved means:

a) RAT indication or equivalent
b) Red indicator located above the reader

Cardax System or Equivalent Intruder System

12.0207 Connection to a relay interface output board with security devices such as detectors or reed switches. These devices will be set up with an alarm zone that can be controlled by a reader and/or a RAT and/or a Schedule (timeframe).

12.0208 The ANU will assess the capability of the intruder component system in relation to alarm management and the functionality for remote arming and disarming

Security Panel Option

12.0209 The ANU reserves the right for site installations with specific needs to retain the separate panel installation in such sites on campus the equipment shall:

- be RAT, C&K Sierra Type or approved alternative;
- supply a normal contact that can interface into the Cardax or equal equivalent;
- have only one detection device per zone (unless otherwise briefed and advised by the ANU); and
- not have its installers combination code changed from factory default.

Glass Break Detectors

12.0210 Dual flex/audio detection separate microphone.

12.0211 Minimum 7.6 m detection range.

Detectors

12.0212 Dual Technology PIR and Microwave.

12.0213 Selectable pulse count and walk test facility.

Duress Buttons

12.0214 DURE001 PAB 11-117 Holds Up with Centre Push (or equal equivalent); they must lock on and be able to be reset manually through use of a key.

12.0215 Duress buttons deployed on campus are also connected directly to inputs in the Gallagher system. This allows duress alarms to be reported and actioned upon by ANU Unisafe.

12.0216

Conduits

12.0217 Internal

a) Shall be rigid LD-UPVC of minimum 25 mm diameter.
b) All fittings, draw boxes, bends and couplings are to be purpose made.
c) Shall be joined using an approved solvent cement.
d) Shall be secured using metal saddles spaced at 600 mm (maximum) centres and within 150 mm of all fittings.
e) Shall be installed so that cables can be drawn in at draw boxes only. Inspection elbows shall not be classified as draw points.
f) Shall be filled with cables to not more than 60% of its capacity.

Cable Duct

a) Shall be fitted with removable covers.
b) Shall be fitted with the manufacturer’s standard bends, elbows, couplings and reducers.
c) Shall be manufactured from extruded PVC when exposed. When concealed cavities and ceiling spaces maybe metal.
d) Shall be filled with cables to not more than 60% of its capacity.
e) Shall not be used on external building installations

12.0218 External

a) All conduits installed externally of a building shall be steel conduit (plated or painted depending on environment) to prevent tampering.
b) Where possible, all visible conduit and duct routes shall be identified on contractual documentation.

12.0219 Fixings

a) Shall comprise corrosive resistant metal thread screws or bolts into expanding type masonry anchors for fixing to concrete or masonry.
b) Shall comprise tapered woodscrews for fixing to timber (full thread).
c) Shall comprise metal expanding anchors for fixings to gyprock.
d) All fixings to be corrosive resistant.

External Reader Fixing and Installation Rating

12.0220 All card reader installations on buildings and facilities (including under awnings, verandas, porticos and under crofts) shall meet or exceed an IP65 rating.

Network and 240 V Construction and Responsibility

12.0221 The ANU builds and supports its campus IT Network and electrical reticulation in buildings.

12.0222 The access control system currently operates in a virtual private network with an ANU controlled IP range. The network resides behind an ANU administered firewall. Power over Ethernet is available in some part of the network.

12.0223 Cabling and Ethernet wall plug installation is managed by Network Services within ANU ITS.

12.0224 Network cabling shall comply with the ANU ITS Cabling Specification. Note that Ethernet cables shall comply with CAT6 specifications.

Naming Convention - Gallagher

An extensive naming convention has been implemented for the programming of all devices withing Gallagher command centre. This naming convention must be adhered to when programming changes and new works.

Please refer to Command Centre Configuration Client for more examples and ensure naming matches existing conventions. Unnecessary capitalisation shall be avoided.

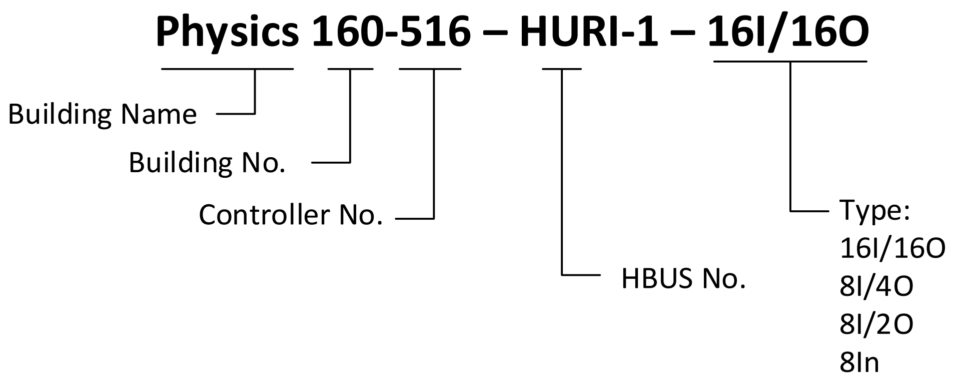
Controllers & Expanders

Controllers

Controller numbers are unique and will be provided by the ANU Unisafe operations manager. Do not program the next sequential controller number without permission as it may already be reserved for other works.

Expanders

HBUS expander name examples are shown below.



12.0225

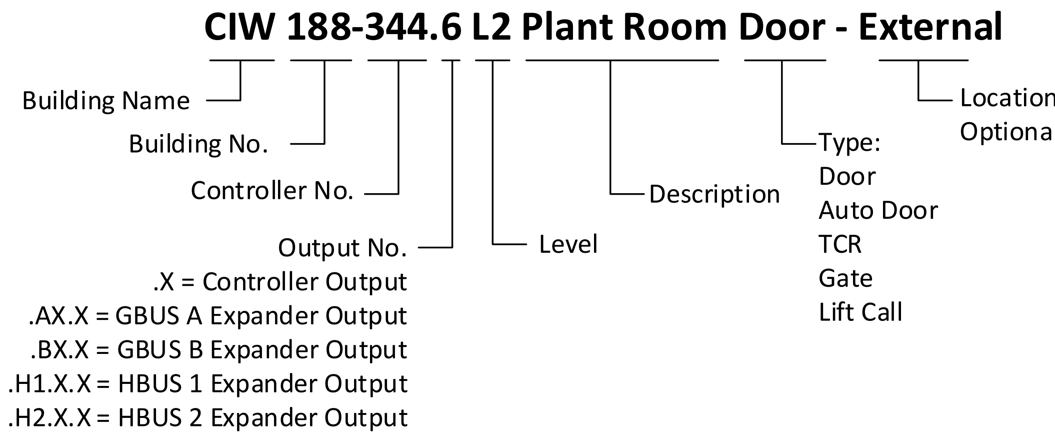
12.1) Doors

Door programming uses the Gallagher controller and lock output number to create a unique identifier within the system. This number is also used for devices related to the door can be used to quickly search and find items.

12.0226 Door Labelling

The unique identifier for each door must be applied as a Traffolyte label above the external card reader or, in the case of a TCR door, to the break glass or exit device.

12.0227 Door Naming Example


CIW 188-344.6 L2 Plant Room Door - External
Building Name
Building No.
Controller No.
Output No.
.X = Controller Output
.AX.X = GBUS A Expander Output
.BX.X = GBUS B Expander Output
.H1.X.X = HBUS 1 Expander Output
.H2.X.X = HBUS 2 Expander Output
Level
Description
Type:
Door
Auto Door
TCR
Gate
Lift Call
Location
Optiona

12.0228

12.0229 Door Peripherals & Access Zones

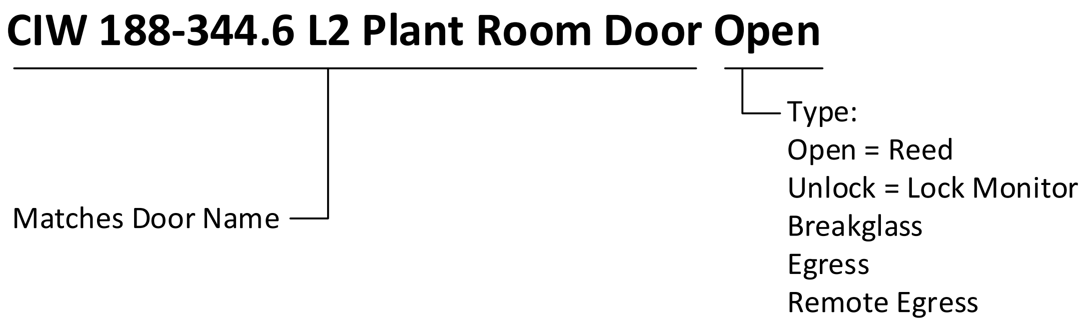
Inputs and outputs related to doors, readers and access zone names shall be derived from the door name and shall contain the same number and name prefix. Examples below.

Access zone names shall be the same as the door name.

Other door related items such as logic block and macros should also contain the full door number.

Adding the door number is essential and allows operators to search and find any competent related to a single door just by entering the controller and output number.

12.0230 Door Input Example



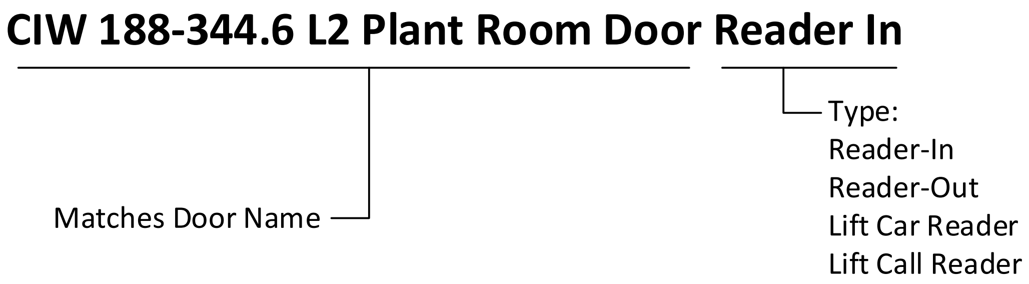
CIW 188-344.6 L2 Plant Room Door Open

Matches Door Name

Type:
Open = Reed
Unlock = Lock Monitor
Breakglass
Egress
Remote Egress

12.0231

12.0232 Reader Example



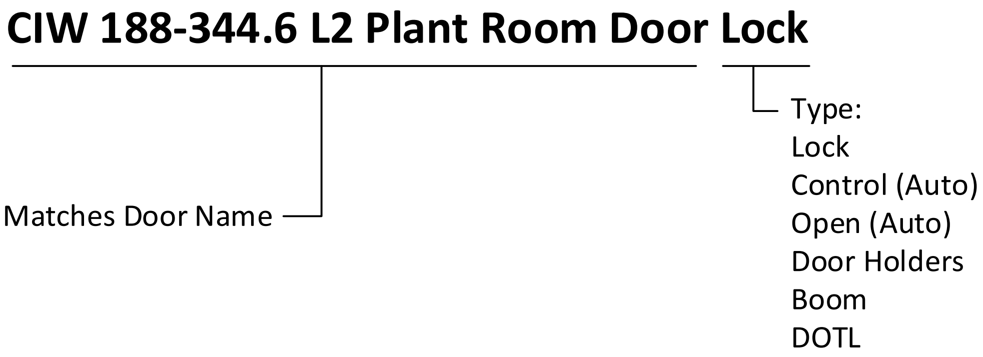
CIW 188-344.6 L2 Plant Room Door Reader In

Matches Door Name

Type:
Reader-In
Reader-Out
Lift Car Reader
Lift Call Reader

12.0233

12.0234 Door Output Example



CIW 188-344.6 L2 Plant Room Door Lock

Matches Door Name

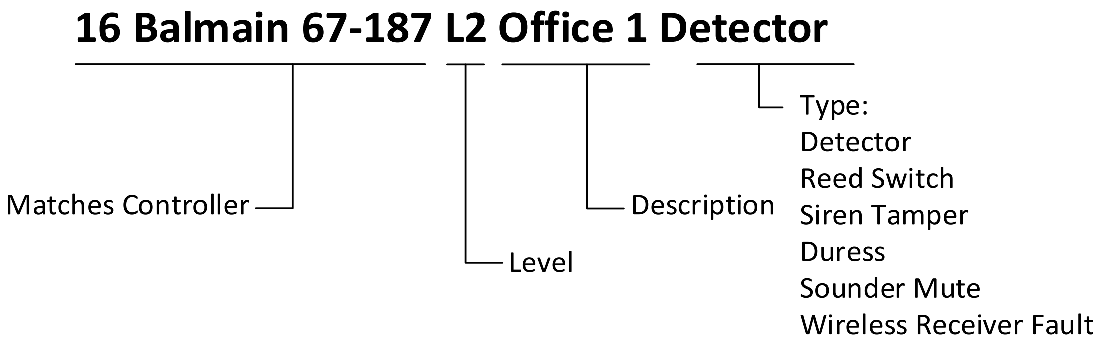
Type:
Lock
Control (Auto)
Open (Auto)
Door Holders
Boom
DOTL

12.0235

12.2) Inputs

Alarm, duress and system inputs shall contain the building name, building name and controller number.

12.0236 Input Example – Alarm



16 Balmain 67-187 L2 Office 1 Detector

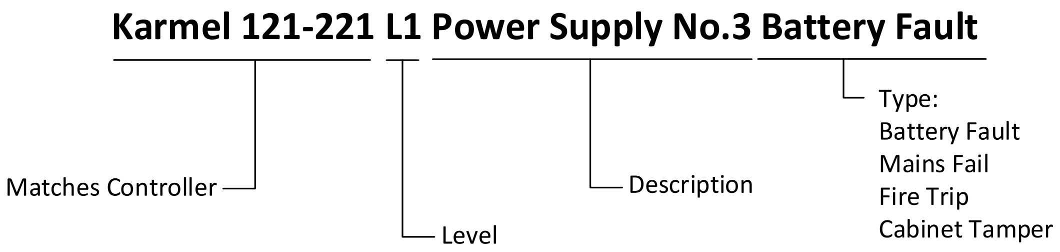
Matches Controller

Level

Description

Type:
Detector
Reed Switch
Siren Tamper
Duress
Sounder Mute
Wireless Receiver Fault

12.0237 Input Example – System

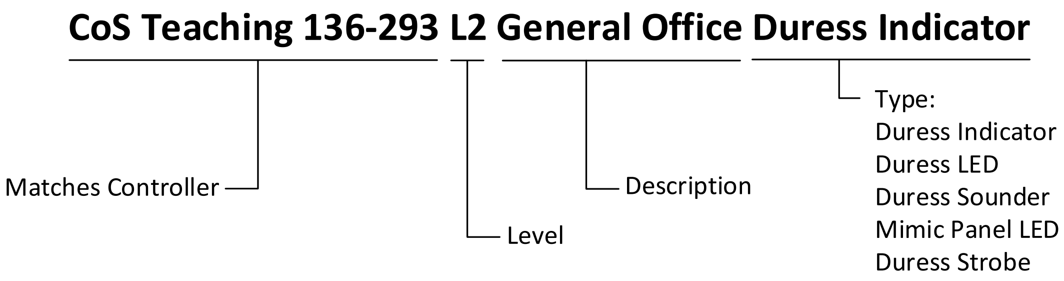

Karmel 121-221 L1 Power Supply No.3 Battery Fault
Matches Controller
Level
Description
Type:
Battery Fault
Mains Fail
Fire Trip
Cabinet Tamper

12.3) Outputs

12.0239 Alarm, duress and system outputs shall contain the building name, building name controller and expander number.

12.0240 Output Example – Duress

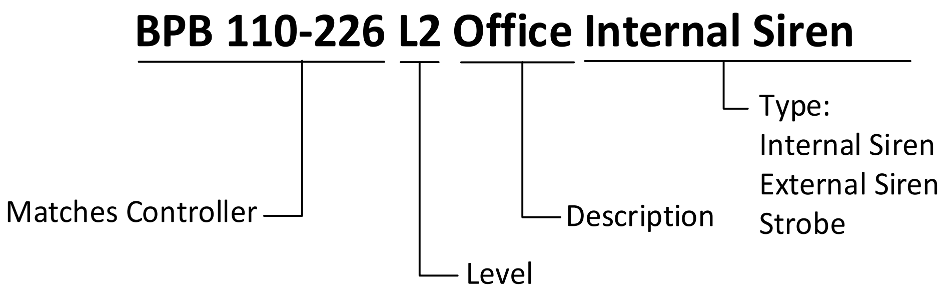
12.0241



12.0242

12.0243 Output Example – Alarm

12.0244



ANU Preferred Equipment Lists

12.01 ANU Security have identified preferred equipment to be used to reduce service complexity and deliver a consistent, reliable outcome. This equipment should be specified and used wherever possible. Alternative equipment solutions will require written approval from the Unisafe operations manager.

AccessControl

Part Description	Part No.	Supplier/Brand	Notes
	Access Control Peripherals		
Press to Exit Button – Green Mushroom	v	Smart	
Emergency Break Glass Unit Resettable	WG2200SGEDR	KAC	
Emergency Break Glass Insert	WF1	KAC	Must be used
Recessed Reed Switch 19mm	SD70	Tane	
Rare earth magnet (channel magnet)	1840N	Sentrol/UTC/GE	
Roller Reed Switch	2205A	Sentrol/UTC/GE	
Electric Strike - Monitored	ES20M	LOX	
Electric Strike – Pre-load	ES9000	Padde Lockwood	
Electric Strike - Rim	ES15M	FSH	
Electromagnetic Lock Standard - Monitored	EM5700M	LOX	
Electromagnetic Lock Low Profile – Monitored	EM3500M	LOX	
Electromagnetic Lock Sliding Door - Monitored	EM3500FM	LOX	
Electromagnetic Lock - Weather Proof	EM5000	LOX	
Boom Gate	Magnetic.Access	Magnetic Automation	

Gallagher

Part Description	Part No.	Supplier/Brand	Notes
	Gallagher		
Controller 6000 - Standard	Gallagher	C300100	
Controller 7000* – RS485	Gallagher	C400010	Normal Use
Controller 7000* – PoE+	Gallagher	C400020	Special Use Only
HBUS Module – 8H	Gallagher	C300182	
High Density Input/Output Expander	Gallagher	C300688	HBUS
8 In 4 Out Expander	Gallagher	C300684	HBUS
8 In Expander	Gallagher	C300680	HBUS
Universal Reader Interface	Gallagher	C300665	HBUS
Reader – T15 MultiTech Black	Gallagher	C305480	HBUS
Reader + Keypad – T30 MultiTech Black	Gallagher	C300490	HBUS
Terminal + Reader – T20 MultiTech Black	Gallagher	C300460	HBUS

Power Supply and Distribution

Power Supply & Distribution		
Power Supply – 8A	C200440	Gallagher
Power Supply – 8A	PB256	Powerbox
Power Supply – 16A	PB251	Powerbox
Fire Trip, Fused PDM	PP8FR	Jack Fuse
Fused PDM	PP10HD	Jack Fuse

Cabling

Cable			
HBUS Cable – Indoor	C303900	Gallagher	Readers, Terminals & Expanders
HBUS Cable – External	C303901	Gallagher	Readers, Terminals & Expanders
4 Core Security 14/020		Various	Inputs
6 Core Security 14/020		Various	Inputs & auto door control
Twin, double insulated .88mm^2			Electric Strikes*
Twin, Double insulated 1mm^2			Electromagnetic Locks*
Twin, Double insulated 1.5mm^2			Electromagnetic Locks*

SALTO

Salto		
XS4 One	EB750Z00IMBB6	Salto
XS4 One IP55	EB750Z00IMBB65	Salto
XS4 Original+	AM650Z00IMBB6	Salto
XS4 Original+ IP56	AM650Z00IMBB6E5	Salto
NEOXX Padlock	NBP4P60150CPB0	Salto
NEO Cylinder Aus Oval	NMA1100N00CSBN	Salto
NEO Cylinder Aus Oval IP66	NMA1100N00CSBNR	Salto
Update point reader XS4 2.0 Square	WRDB0E4B	Salto
Mullion Reader XS4 2.0	WRDB0M4B	Salto
Online control unit	CU42E0AUS	Salto
Auxiliary control unit	CU4200AUS	Salto
BLUEnet wireless gateway	GATEWAYW3CAUS	Salto
BLUEnet node	RFNODE3W	Salto

Duress

Duress			
Indoor Duress button Cash/Desk	PAB1	Sprint	Supply key
Indoor ‘Duress’ button	SMART4372DUR	SMART	Must use shroud
Indoor ‘Press For Assistance’ button	SMART4372PFA	SMART	Must use shroud
Outdoor/Freezer duress button IP65*	242-0845	RS PRO	Must use shroud
Duress button shroud	LPXAU158	Levato	
Duress Audible/Visual Indicator	AI673	Aritech	

*Outdoor RS PRO duress button must feature separate label with appropriate text. E.G. “Press for Assistance”

Intrusion Detection

Intrusion Detection			
Motion Detector 90° Dual Tech 15m	RK825DTGLUSC	Risco Iwise	
Motion Detector 90° Ceiling Bracket	RA900000000A	Risco Iwise	
Motion Detector 90° Wall Bracket	RA910000000A	Risco Iwise	Includes corner mount
Motion Detector 360°	PA6810E	Takex	
Alarm Arming Indicator	AI673	Aritech	
Screamer Flush Mount	WPO5	Sprint	
Siren Strobe Combination	PWP16BLACK	Firefly	White or Black