UNIVERSITY OF WOLLONGONG AUSTRALIA

UOW FACILITIES MANAGEMENT DIVISION

Electronic Monitoring and Access Control Design Standards

Contents

1 Electronic monitoring and access control

Electronic monitoring and access control systems form part of the overall security strategy implemented by the University of Wollongong. Systems are used in conjunction with physical and operational security measures to protect people, property and processes.

The new electronic monitoring and access control system shall comprise of alarm monitoring and the capability to control access through the use of electronic locking devices and access card readers. The electronic monitoring and access control system used by UOW is the Gallagher System. All hardware, software and field devices shall be Gallagher compliant and approved.

2 Overview

This design standard outlines the functional, installation and technical requirements for a new electronic monitoring and access control system.

The designer shall use these standards as the basis for the system design, however it is incumbent upon the designer to ensure that the design satisfies site specific operational, logistical and performance requirements and meets UOW's security objective for the facility.

Where the designer considers that an alternate equipment type is preferred to the equipment type specified in the design standard, the designer will advise the principal of the functional, performance or cost benefit that will be achieved through the use of the alternate equipment type.

3 Definitions

Term	Definition
FPU	Field Processing Unit - controller
RAT	Remote arming terminal
UOW	University of Wollongong

4 Design process

This section overviews the design process. The process shall be followed to achieve UOW's desired outcomes.

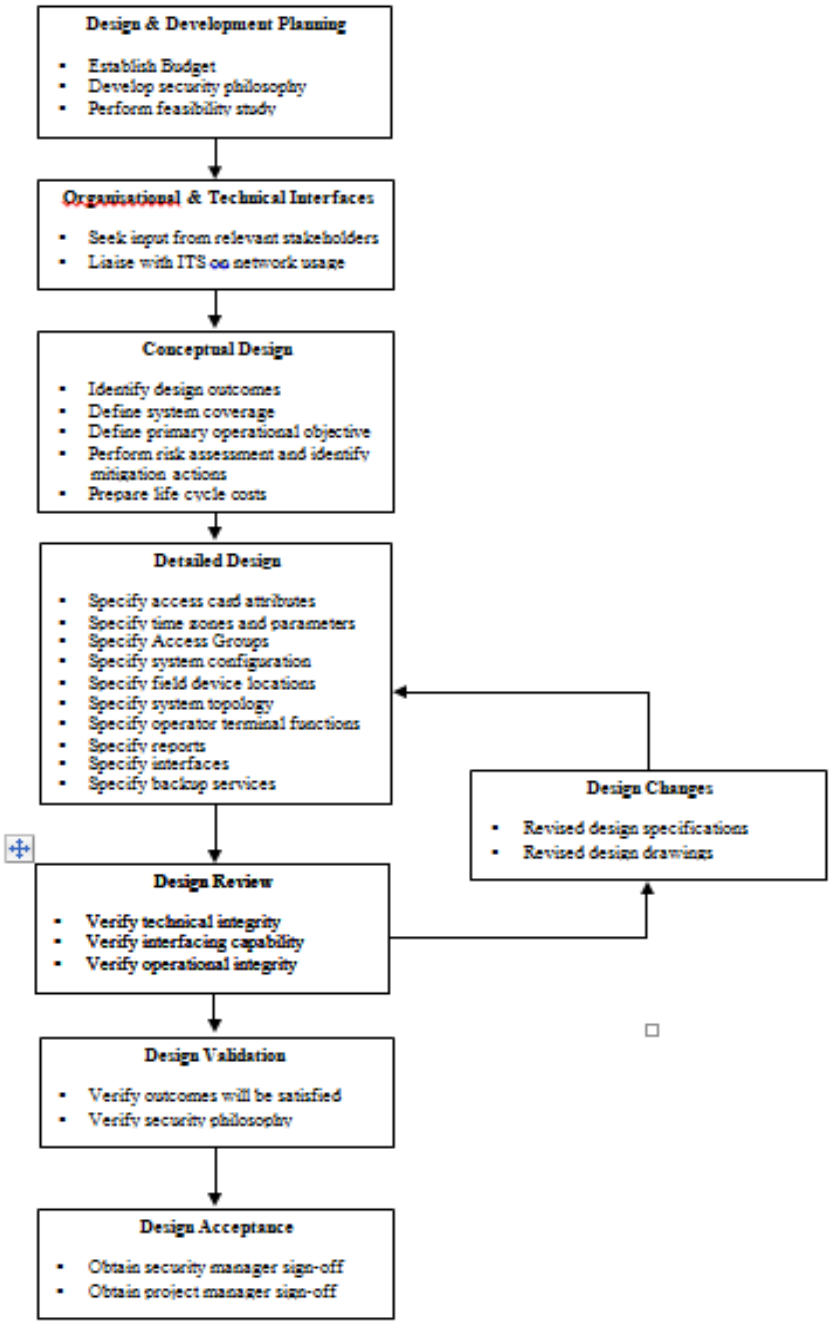


Figure 1.1 Process Flow

4.1 Functional requirements

4.1.1 General

The electronic monitoring and access control system shall be fully time programmable to permit defined access and establish secure periods to suit the requirements of the University of Wollongong.

The system shall be expandable to enable the connection of future sub- systems. The system shall permit monitoring and control functions to be performed from the operator terminal. The system shall support both the monitoring and control of all field devices.

Following are the primary system functions:

a. Perimeter alarm monitoring and access control;

b. Lift alarm monitoring and access control;

c. Internal secure area alarm monitoring and access control;

d. Systems interfacing;

e. Operational monitoring.

All equipment must be connected to the University Gallagher Command Centre head end via the University IP Network.

4.1.2 Perimeter Alarm Monitoring and Access Control

During secure periods, entry to the building via a perimeter door shall be achieved via the presentation of a valid access card. During non-secure periods, the electronic locking device shall be overridden by a programmed time schedule contained in the Gallagher controller field processing units.

The use of an access card shall provide temporary override of the electric locks. In double leaf doors, the second leaf should be secured using an electro-magnetic lock. The door status shall be secure, temporary access (access card use), or automatic access (programmed time schedule).

Perimeter doors shall be monitored for forced and door open too long alarms. The alarm condition shall be either normal, alarm or fault. Nuisance alarms shall be eliminated for general egress during secure periods through the provision of an alarm-shunting device integrated in the electric locks. REX (Request to Exit) push buttons such those installed internally adjacent to the door should only be provided for automated doors which would require after-hours release or on doors using an electro-magnetic lock to secure the door requiring emergency release. The REX shall be incorporated directly into the door wiring so that failure of the controller will not affect the release of the door. The UOW auto door standard must be consulted for further detail.

4.1.3 Lift Alarm Monitoring and Access Control

Where lift control forms part of the security strategy for a university building, lifts shall be controlled via the presentation of a valid access card during secure periods. The access card shall control a lift relay that provides temporary access to the designated floor(s).

The status of the lift relay shall be secure, temporary override (access card use), or programmed override. Where presentation of a valid card is required, only one floor call shall be latched in conjunction with the lift button. If any more floor calls are required, additional key presentation shall be required for each floor call. It shall not be possible to push two buttons at the same time and have them both latch.

The fire service overrides, passenger alarm button, car fault, stop and service override in each lift car shall be monitored by the system. The system shall generate a lift car specific high priority alarm if a fire service override, passenger alarm, car fault, service override or any other means has caused a lift car to be non-secured.

Where access is granted to a floor, by the card identification number, the users' name and destination floor shall be recorded in a history file with availability for a period of three (3) months.

4.1.4 Internal Secure Area Alarm Monitoring and Access Control

During secure periods, internal secure areas shall be accessed via the presentation of a valid access card. During non-secure periods, the electronic locking device shall be overridden by a programmed time schedule contained in the Gallagher controller field processing units.

The use of an access card shall provide a temporary override of an electric lock. In double leaf doors, the second leaf should be secured by an electro-magnetic lock. v-lock or hook lock. The door status shall be secure, temporary access (access card use), or automatic access (programmed time schedule).

Internal doors shall be monitored for forced entry, unlocked doors and doors open too long. The alarm condition shall be either normal, alarm or fault. Nuisance alarms shall be eliminated for general egress during secure periods through the provision of an alarm shunting device integrated in the electric locks. REX (Request to Exit) push buttons such as those installed internally adjacent to the door should only be provided for automated doors which would require after hours release or on doors using an electro-magnetic lock to secure the door requiring emergency release. The REX shall be incorporated directly into the door wiring so that failure of the control will not affect the release of the door.

4.1.5 Systems Interfacing

Where the electronic monitoring and access control system interconnects to other building services such as fire services, ventilation systems or automatic door and gate systems, an interface shall be provided that achieves optimum functionality, performance and reliability.

Low level interfaces shall comprise of a set of electrical contacts controlled via a signal from the Gallagher Cardax FT controller field processing unit. High level interfaces shall be provided using a standard protocol and an established software product that is fully compatible with the electronic monitoring and access control system and the service to be interfaced.

System to be Interfaced	Interface Type	Interface Responsibility
Fire	Low level	Security
Lift	Low level/high level	Security
Automatic doors	Low level	Security
Ventilation	Low level/high level	HVAC

Table 1.1 System interface

4.1.6 Fire Trip

Fire Trips must be connected via a normally open contact with an appropriate relay to “cut power” as required. Where fitted, the fire trip must have a separate contact to monitor when it is activated. This must be monitored as an input via the Gallagher system.

4.1.7 Paths of Egress

Where electronic locking is provided on doors that are located on paths of egress, an override mechanism must be installed so that occupants can evacuate the building safely and quickly. The mechanism must be functional in a fire or other emergency and comply with the BCA.

The override mechanism may involve direct connection to the fire panel, local smoke detectors, break glass or manual override.

All mortice locks must be configured ‘fail secure’ for entry. If a door on a path of egress is locked, ‘fail safe - open’ configuration is required, including a monitored double pole break glass.

4.1.8 Operational Monitoring

The security operator terminal is the human interface between the electronic monitoring and access control system and the operational security management team. The operator terminal shall be configured to monitor and control the status and condition of the entire system.

The operator terminal shall be programmed to perform the following functions:

a. Alarm management;
b. Device programming;
c. Access card programming;
d. Manual control of field devices;
e. Reporting;
f. Database management; and
g. Site plans showing all relevant features.

4.2 Monitoring – device/status/tamper

Gallagher equipment including power supplies, cabinets, etc must be fitted with status monitoring, tamper switches and other detection devices. This is to prevent interference with or the failure of the access control equipment. All devices must programmed so that an alarm is raised if a failure or abnormality occurs.

Equipment to be monitored include:

a. PSU Mains fail.
b. PSU Low battery.
c. Cabinet tamper for all cabinets including power supplies
d. Door open / door open too long
e. Door Not Locked (inc, bond sense)
f. Door forced
g. Break glass broken
h. Fire trip activated
i. Motion detector activation PIR
j. Motion detector tamper PIR
k. Glass Break detector tamper
l. Glass break detector activation
m. Wireless duress battery status
n. Button release
o. Open circuit tamper
p. Short circuit tamper
q. Input Open/Closed
r. Output On/Off.

4.2.1 Remote Arming Terminal (RAT)

Remote arming terminals shall be installed at nominated sites. The remote arming terminals shall provide activation and deactivation of alarm devices and alarm zones at each building. Remote arming terminals shall be operated using a proximity card reader. Current versions of Gallagher hardware RAT have a card reader in in the RAT.

4.2.2 Building Lockdown Reader & Duress Buttons

At all regional campuses and any specially nominated sites, a building lockdown reader will be installed. The purpose of this building lockdown reader is to enable administrative staff with the appropriate authorisation to lock all perimeter access points (and any nominated internal secure areas) during an emergency situation. This shall operate by the authorized user using a single swipe of the reader to lock down and double swipe to disarm the predetermined areas.

In certain circumstances a Duress or Panic button can be installed to provide covert operation and alarm generation. The button must be the duel button activation type. Wireless buttons must provide for low battery alarm.

Both systems must generate an immediate alarm back to the university's third party monitoring station.

4.3 Standards

The design shall comply with all relevant codes and standards. Table 1.2 below contains a list of the relevant codes and standards.

Issuing Body	Document Number	Title
Standards Australia	AS/ACIF S009: 2006-11-08	Installation requirements for customer cabling (wiring rules)
ABCB	BCA-2005	Australian Building Code of Australia
Institute of Electrical and Electronics Engineers	IEEE 802.3 IEEE 802.5	Broadband applications
Standards Australia	AS/NZS 1102.103:1997	Conductors and connecting devices
Standards Australia	AS 1345 - 1995	Identification of the contents of pipes, conduits and ducts
Standards Australia	AS 2053	Conduits and fittings for electrical installations
Standards Australia	AS 2201.1 - 1998	Systems installed in client's premises
Standards Australia	AS 2201.2 - 2004	Monitoring centres
Standards Australia	AS 2201.3 - 1991	Detection devices for internal use

Issuing Body	Document Number	Title
Standards Australia	AS 2201.4 - 1990	Wire-free systems installed in client's premises
Standards Australia	AS 2201.5 - 1992	Alarm transmission systems
Standards Australia	AS 2834 - 1995	Computer accommodation
Standards Australia	AS 3000	Wiring rules
Standards Australia	AS 3080:2003	Telecommunications installations - Generic cabling for commercial premises
Standards Australia	AS 3768 - 1990	Guide to the effects of the temperature on electrical equipment
Standards Australia	AS 3084:2003	Telecommunications installations - Telecommunications pathways and spaces for commercial buildings
Standards Australia	AS 3011	Electrical installations - Secondary batteries installed in buildings
TIA/EIA	TSB36	Specification for unshielded twisted pair cables
TIA/EIA	TSB40	Transmission specifications for unshielded twisted pair cables connecting hardware
UOW	OHS064	OH&S Consideration for Design (http://staff.uow.edu.au/workingsafely/design/OHS064-OHS_Design_Guidelines.pdf)

Table 1.2 - Codes and Standards

4.4 Minimum performance standards

The following minimum performance standards shall be achieved to ensure efficient operation of the electronic monitoring and access control system

Functions	Acceptable Limit
Presentation of access card to override door lock	<1s
Generation of door open too long alarm on operators terminal	<1s
Generation of forced entry alarm on operators terminal	<1s
Presentation of access card to override lift relay	<2s

Functions	Acceptable Limit
Generation of fire service alarm on operators terminal	<1s
Generation of lift alarm on operators terminal	<1s
Online display of historical report from report request	<5s

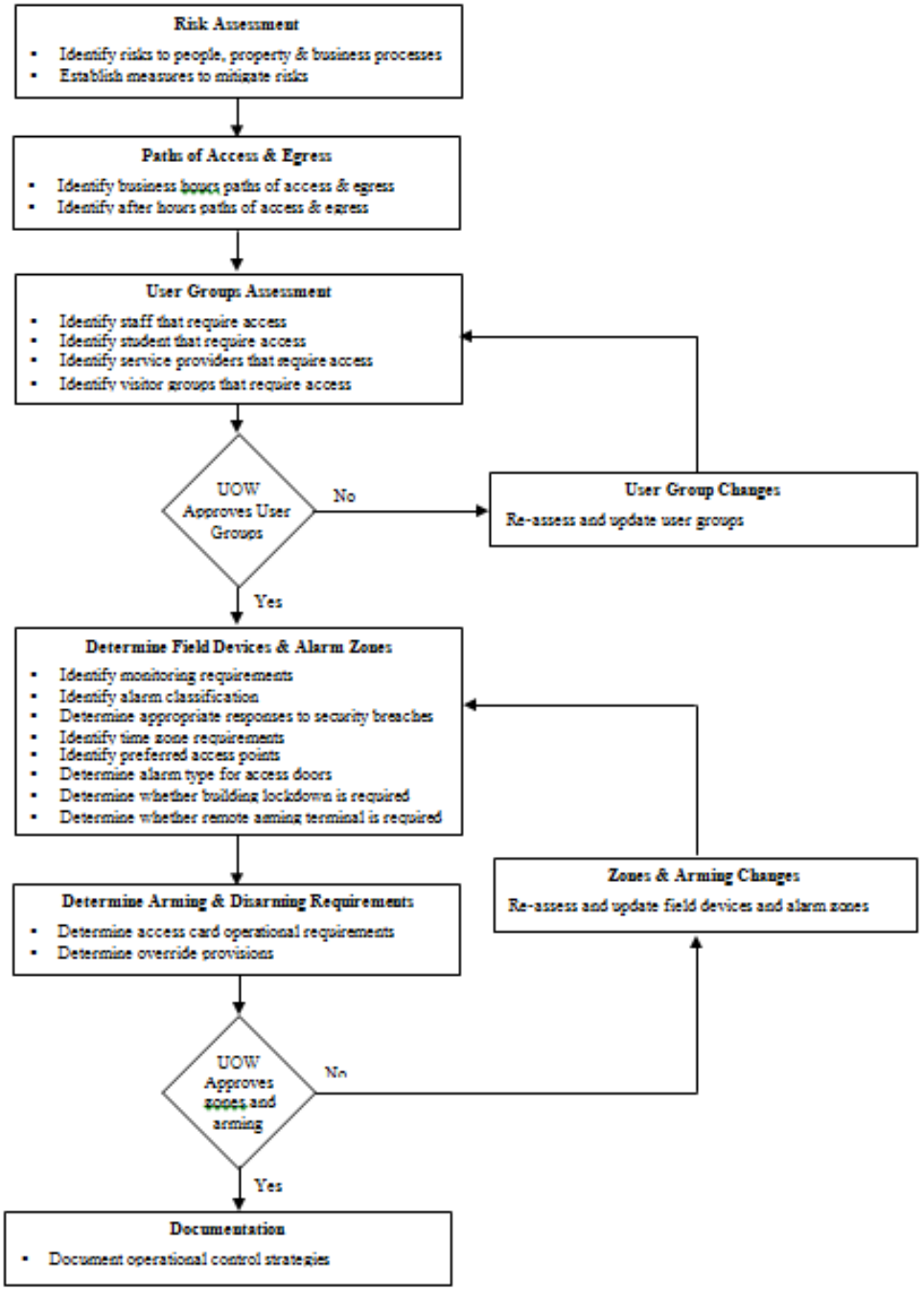
Table 1.3 - Minimum Performance Standards

4.5 Design of Operational Control Strategies

As part of the detailed design, the designer will liaise with UOW Security and appropriate business area managers to determine the operational control strategies for the specific building. This process will involve:

a. Identification of the risks to persons, property and business process;
b. Establishment of measures to mitigate the risks e.g. means of protection, detection and/or deterrence;
c. Identify paths of egress during business hours and after hour periods;
d. Identify staff, student, service provider and visitor groups that will require access to the building;
e. Identify monitoring requirements, alarm classification and the appropriate response to a security breach;
f. Identify the time zone requirements in terms of being on or off security and the periods over which the groups outlined in d. above will require access;
g. Identify the preferred access point through which access will be achieved during "security on" periods;
h. Identify whether access doors need to report a forced alarm and/or an ajar alarm. If the ajar alarm is required determine the time before the device enters an alarm stage;
i. Determine the access card operational requirements e.g. single presentation, double presentation, dual card device etc;
j. Determine override requirements e.g. to satisfy BCA requirements on a path of egress;
k. Determine methods for manually and/or automatically overriding the field device;
l. Determine whether building lockdown functionality or remote arming terminal functionality is required;
m. Identify special secure locations within a specific building that require increased security provisions, then repeat points (a) to (k) above;
n. Document the above in a spread sheet form and circulate to UOW Security and UOW business managers for sign-off. Refer to Appendix A for an outline of the spreadsheet to be used by the designer.

The following diagram outlines the process to determine the operational control strategies:



4.6 Programming Alarm Parameters

The system shall be programmed so that when a door which is configured for “door open too long” functionality is open for 20 seconds an audible warning alarm shall be sounded at the card reader. Should the door remain open for a further 200 seconds then a door open too long alarm will be generated at the operator’s terminal.

Forced alarms, door not locked alarms and door open too long alarms on doors which lead to critical areas will be generated on a 24 hour 7 day basis. Alarms to non-critical areas will only be generated from Monday through to Friday between the hours of 9:30PM and 7:30AM.

Zoned intruder alarms, panic alarms, duress alarms and armed hold-up alarms will be generated on a 24 hour 7 day basis.

Alarm will appear in the operators terminal alarm viewer and are transmitted to third party monitoring station as either critical, very high or high alarm.

To enable the alarm to be transmitted to a third party monitoring central station communication devices must be provided at each building. In 2017 with recent changes to telecommunications network (inclusive of NBN) communications should be via TCP/IP Network utilising Gallagher IP equipment and where determined in conjunction with UOW providing a GSM network should be considered for redundancy.

Alarm zone configuration shall be in accordance with the Gallagher Alarm Zone Action Plan and follow established UOW naming conventions.

4.7 Installation guidelines

4.7.1 Electrical Cabling

Electrical cabling shall be sized to meet the maximum demand of the proposed equipment and the potential additional equipment likely to be connected to the final sub-circuit. Cable type must be suitable for the application being used. Cables must be sized to factor in voltage drop and not exceed the manufacturers recommended maximum length. Generally internal cable should be a minimum 14/020 and either 4 or 6 core. For runs over 35 metres, power to locks is supplied by 2 core 1.5mm or larger stranded red and black TPS cable. External cabling should be rated for outdoor use and be gel filled cable to stop moisture ingress. All cabling shall provide for redundant cores to be installed and consideration should be to run 2 x 6 core cables to each lock. Cables terminating at field devices must allow a suitable extra length to easily remove any device for maintenance or replacement and to re-terminate cable if required.

Electrical cabling shall be installed such that stress does not occur to any part of the cable or to the connected equipment. Cables shall be securely supported and protected from mechanical damage by the use of suitable ducting or conduit minimum of 20mm diameter. Cabling run in a fire stair should be run in steel conduit or meet the requirements of the BCA and AS 3000. All cabling entry points should be fire sealed as required by building design standards.

All cabling installed between equipment or devices shall consist of one continuous length of cable. Cabling shall be concealed wherever possible in ceiling spaces, wall cavities, risers and the like. Terminations shall be made using soldered joints with heat-shrink to be used to protect joins and terminations instead of electrical tape.

Cables must be protected from mechanical damage when installed in metal framing such as doors and windows. Suitable plastic bushes or rubber grommets should be used at through frame holes and all burrs must be removed around entry points.

Device in-outs such as motion detectors, reed switches, etc. must be wired with individual common return wires.

All cables shall be identified at each end by approved labels fixed to cable sheaths or conduit, identifying the origin and destination.

Prior to the connection of equipment, cabling shall be tested for continuity, polarity and disturbance.

4.7.2 Communication Cabling

The type and size of communication cabling shall be selected to achieve optimum system performance. Where a different type of cabling for the primary control bus and secondary control bus produces optimum performance, the different cable types will only be used where compatibility is assured and manufacturer recommendations are satisfied.

Communication cabling shall be installed such that stress does not occur to any part of the cable or to the connected equipment. Cables shall be securely supported and protected from mechanical damage.

All cabling installed between equipment or devices shall consist of one continuous length of cable. Cabling shall be concealed wherever possible in ceiling spaces, wall cavities, risers and of the like.

All cabling shall meet the requirements of the BCA, relevant Australian Standard and the UOW standards for communications cabling.

Any work on the structured wiring on the communications must only be carried out by an IMTS approved contractor. Security installers are not authorised to work on the network and can only connect to cabling and equipment installed by an IMTS approved contractor.

It is usual practice for patch cables to be a different colour to standard patch cable colours.

4.7.3 Field Devices

The number of field devices installed per Field Processing Unit must not exceed the manufactures recommended maximum.

Access readers, electronic locking devices, alarm devices, lift relays etc shall be mechanically secured to protect against operational damage and ensure stability for continuous use.

Electrical terminations shall be permanent and insulated to protect against faults. Communication cable terminations shall be permanent and protected from interference.

Where possible, field devices shall be recessed and all external devices shall be weather resistant. External field devices should be mounted so that any cable entry points face down to prevent the ingress of moisture where possible.

4.7.4 Field Processing Units (FPU)

The FPUs shall be installed in designated service areas where adequate access and ventilation is available in a restricted, lockable and where appropriate, air conditioned area in a dedicated low voltage cupboard.. The location shall maintain separation from other building services such as electrical and fire systems. FPUs should be located on a per floor basis to avoid problems with fault finding and cable run lengths. Field devices should be connected to the FPU on the floor that they are installed on. Any cabinet will be installed only in general areas and not in offices or other restricted areas. The FPU cabinets shall be mechanically secured and cable entries shall be insulated to protect against cable damage. Gallagher Dual Cabinets, with 8amp PSU, must be used for all installations.

All outputs to field devices must be run through individual fuses that protect the cabling and device. The use of the “Jack Fuse PP8FR” fuse board provides this protection with the added benefit of a fire trip relay. Fuse boards are to be installed in the controller cabinet.

Gallagher FT 6000 controller with 8H module ONLY must be used for all installations.

8 input, IO and HD IO expansion boards must be used for all installations. Where necessary to increase capacity the use of a universal reader interface should be considered.

Electrical terminations shall be permanent and insulated to protect against faults. Communication cable terminations shall be permanent and protected from interference.

**All FSU’s must have a 240V electrical supply from a dedicated circuit and must not be mixed with other equipment on a circuit. This must be clearly labeled at the Electrical Distribution Board.

4.7.5 Batteries

Each FPU’s shall be provided with a sealed suitable for indoor use to backup battery as part of the installation. The battery will be sized to maintain operation of the FPU and the connected devices for a minimum of 4 hours under full load conditions with the maximum number of field devices connected.

All batteries must be marked with permanent ink indicating the date of installation (format dd/mm/yyyy) on the top of each battery.

4.7.6 Remote Arming Terminals

Remote arming terminals and associated proximity card reader shall be installed at the main entrance to each building. The remote arming terminals shall be mechanically secured and cable entries shall be insulated to protect against cable damage.

Electrical terminations shall be permanent and insulated to protect against faults. Communication cable terminations shall be permanent and protected from interference.

4.7.7 Operator Terminal

The operator terminal CPU, LCD screen and other peripheral devices shall be installed at the operational security work station. Interconnecting cables shall be protected from mechanical damage and permanently connected.

4.7.8 Labelling

FPUs and other major system components shall be clearly labelled using black lettering on white background self-adhesive engraved traffolyte labels, attached to a suitable fixed part of the equipment.

The sticker provided by Gallagher for every cabinet, controller and expansion board must be filled out and neatly fixed to the inside of the cabinet. The sticker must be written out in pencil and the naming conventions must copy details of the configuration sheet provided to the UOW FMD.

Every door with access control shall be clearly labelled using black lettering on white background self-adhesive engraved traffolyte labels, attached to the outside of the door mullion directly above the door.

Equipment labels shall identify the equipment in accordance with UOW's asset register convention.

4.7.9 Mounting

All equipment shall be mounted at heights and in locations that will facilitate ease of maintenance.

FSUs shall be mounted so that access is at ground level and at comfortable working height without the need for the use of a ladder. Clear access shall be provided to allow for the swing of doors as per AS3000.

Readers and break glass shall be mounted at a height that satisfies the BCA for disabled access.

Detectors should be mounted so that scaffold or EWP are not required for maintenance or replacement.

4.8 Documentation conventions

The designer will ensure that all drawings comply with UOW Drawing Standards and symbols programmed on security operator terminals are consistent with all other symbols currently in use:

The designer will specify the following:

- Unique Device ID;
- Location;
- Description of the device;

- Alarm zone that the devices connected to;
- Time parameters;
- Access parameters; and
- Remote operational parameters.

4.9 Door alarm naming convention

The designer will implement UOW's door numbering convention when assigning identification names to alarm points installed on the door or door frame. Perimeter doors shall be numbered as follows:

- Commence from the left hand side of the northern elevation of the building and then proceeding in a clockwise direction;

- Doors will be numbered consecutively apart from internal doors eg entrance to plant rooms, communications rooms etc. These doors will be named in accordance with the name on the architectural drawings;

- The convention, <Building> <Level> <Location> <Door-Number> <Door-Type> <Descriptor> will be used.

This convention will include the following terms:

External Door Number System					
Building Number	**Level**	**Location**	**Door** Number	**Door Type** (Omit if not listed)	**Descriptor** (Quick ID)
xx	Carpark x	Perimeter	1	Roller RD	eg Parent Room
	B		2	Auto	eg Bank
	G		3	Auto Swing	eg Supermarket
	1		4	Gate	eg Fire Stair
	2			Boom Gate	

Using the above convention for doors which occur in a clockwise direction, a typical example would be B32 GP1 for the first door, then followed by B32 GRD2, B32 GP3, B32 GP4 etc.

Double leaf doors will be identified as using the extensions A and B eg B32
GP1A and B32 GP1B.

Internal doors shall be numbered as follows:

- These doors will be named in accordance with the name on the architectural drawings;

- The convention, <Building> <Level> <Location> <Door-Number> <Door-Type> <Descriptor> will be used.

Internal Door Number System					
Building Number	**Level**	**Location**	**Door Number** (Common Spaces)	**Door Type** (Omit if not listed)	**Descriptor** (Quick ID)
xx	B	G01	0.1	Roller	eg Parent Room
	LG	101	0.2	Auto	eg Bank
	G	Plant	0.3	Auto Swing	eg Supermarket
	1	G99		Gate	eg Fire Stair
	2				

Internal doors shall be identified as by the room number eg a communications room would be B32 G RGP4 Comms. In relation to corridor access where there is more than one corridor eg north and south the convention is to identify the corridor following the level ID eg B32 L1 199.1 North Corridor.

4.10 Equipment

4.10.1 Field processing Units (FPU) & I/O Boards

Table 1.4 below contains the Gallagher FPU that shall be used for monitoring and control functions.

Device	Function	Make	Model	Rating
Field Processing Unit "Controller"	The interface between the Gallagher Command Centre Server and the distributed field hardware.	Gallagher	6000 High Spec. Part # C300101	
8H Module	The connective module between the Gallagher FPU and the distributed field hardware.	Gallagher	8H Part # C300182	8 HBUS Connections 24 Inputs 8 Relay Outputs 4 DC Outputs
HBUS 8 In 2 Out Door Module	Provide flexible, cost effective and secure input and output expansion options, and shared cabling with other HBUS devices over a distance of up to 500m (1640 ft.) at a speed of 1Mb/s.	Gallagher	Part # C300660	8 Inputs 2 Outputs 4 HBUS readers or HBUS terminals
HBUS 16 In 16 Out Board	Provide flexible, cost effective and secure input and output expansion options, and shared cabling with other HBUS devices over a distance of up to 500m (1640 ft.) at a speed of 1Mb/s.	Gallagher	Part # C300688	16 Inputs 16 Outputs 4 HBUS readers or HBUS terminals
HBUS 8 In 4 Out Board	Provide flexible, cost effective and secure input and output expansion options, and shared cabling with other HBUS devices over a distance of up to 500m (1640 ft.) at a speed of 1Mb/s.	Gallagher	Part # C300684	8 Inputs 4 Outputs 4 HBUS readers or HBUS terminals
HBUS 8 In Board	Provide flexible, cost effective and secure input and output expansion options, and shared cabling with other HBUS devices over a distance of up to 500m (1640 ft.) at a speed of 1Mb/s.	Gallagher	Part # C300680	8 Inputs 4 HBUS readers or HBUS terminals

Table 1.4 - Field Processing Units & Modules

A communications interface shall be provided where necessary for nominated alarms to be forwarded to a third party monitoring station as required.

4.10.2 Operator Terminal

The operator terminal provides the security operator with the ability to monitor and control field devices and to interrogate historical records and perform alarm and access card management. Table 1.5 below contains the devices of an operator terminal.

Device	Function	Make
Central Processing Unit	▪ Operator terminal computer	UOW lease standard
Visual Display Unit	▪ Presents visual display of operations and data	UOW lease standard

Table 1.5 - Operator Terminal Devices

4.10.3 Application Software

Application software supports the function of the operation system. Table 1.6 below contains details of the application software.

Device	Function	Make	Model	Platform
Gallagher Command Centre Software	▪ Alarm management ▪ Access card programming ▪ System configuration ▪ Device control	Gallagher Security	Gallagher Command Centre	As per Gallagher Specifications

Table 1.6 - Application Software

4.10.4 Alarm Devices

The alarm devices monitor the condition of doors, windows and other access points. Table 1.7 below contains alarm devices.

Device	Function	Make	Model	Rating
20mm reed switch and magnet	Alarm Device	n/a	n/a	n/a
Surface mount reed switch	Alarm Device	n/a	n/a	n/a

Table 1.7 - Alarm Devices

4.10.5 Access Reader & RAT

The access reader provides controlled access through nominated doors by comparing the access privileges stored in the FPUs. Table 1.8 below contains access reader specifications:

Device	Function	Make	Frequency	Rating
T15 Reader	Slim form footprint card reader using multi-technology reader options with mounting surfaces without spacers (even on metal). Supports Bluetooth use. Standard black	Gallagher	Supports: MIFARE DESFire EV2 MIFARE DESFire EV1 MIFARE Plus MIFARE Classic 125 kHz	
T20 RAT	Access reader and a management tool, able to read cards, accept PIN's and has the ability to interface directly with the security system to make control decisions.	Gallagher	Supports: MIFARE DESFire EV2 MIFARE DESFire EV1 MIFARE Plus MIFARE Classic 125 kHz	

Table 1.8 - Access Reader

** The access card reader must be compatible with UOW's current access card system 125kHz proximity card.*

4.10.6 Electric Mortice Lock

Electric Locks provide automatic locking of doors and should be used in preference to electric strikes and other locking mechanisms. Table 1.9 below contains the preferred electric locks.

Device	Function	Make	Model	Rating
Mortice Lock	Dead latched and Locked Door position/Reed switch Dual key override monitoring Request to exit/REX LED indication	Lockwood	3570	
Mortice Lock Narrow	Dead latched Door position/Reed switch Dual key override monitoring Request to exit/REX	Lockwood	3582	

Table 1.9 - Electric Lock

4.10.7 Electro Magnetic Lock (MAG Lock)

Device	Function	Make	Model	Rating
Mag Lock	Secure door leaf Monitored Lock	Lockwood	Z4	12V
Mag Lock	Secure door leaf Monitored Lock	Lockwood	Z8	12V

Table 1.10 – Electro Magnetic Lock

4.10.8 Electric Strike

Electric strikes are not prescribed. Contractor must liaise with FMD if necessity for electric strikes arises.

4.10.9 Detectors

Detectors are used to monitor movement within an environment. Table 1.12 below contains a list of detectors.

Device	Function	Make	Model	Rating
PIR Detector	Detects movement	Risco	iWise DT	12V
PIR Detector	Detects movement	Risco	Lunar DT 360^0	12V

Table 1.12 - Detectors

4.11 Warranty

The designer shall ensure that all components are supplied with the following minimum warranty periods:

System/Equipment	Warranty Period
Alarm Devices	12 Months
Access Readers	Limited Lifetime
Electric Mortice Locks	12 Months
Electro Magnetic Locks	12 Months
PIR Detectors	12 Months
Field Processing Units & Boards	5 Year
Operator Terminal	12 Months
Application Software	12 Months

Table 1.13 - Warranty Periods

4.12 Life-cycle costing

The designer shall prepare life-cycle costing as part of the conceptual system design. A ten-year period of financial interest shall be used as the basis of the life- cycle analysis. In the case of an electronic monitoring and access control system these costs will include:

- ☐ Initial cost of system equipment
- ☐ Installation costs
- ☐ Maintenance costs
- ☐ Software support and regular upgrades

- ☐ Licenses and statutory costs
- ☐ Cost of third-party support for interfaces

5 Version Control Table

Version	Release Date	Author/Reviewer	Approved By	Amendment
3	30/06/2017	David Anderson Manager Security Brent Michell Electrical Maintenance Officer Maintenance	David Anderson Manager Security	Version 3 Primary updates relate to references to later products and models of Gallagher controllers and card readers. Standard re-numbered. Various other minor amendments.
4	31/08/17	David Anderson	David Anderson Manager Security	Version 4 released
5	1/5/19	Brent Michel	David Anderson	Version 5 Update of Door Alarm Naming Convention Minor amendments.

5.1 APPENDIX A – OPERATIONAL CONTROL STRATEGY SPREADSHEET

Access	Security	Access Group	Alarm Monitoring		Access Card Presentation			Override		Secure	Remote Arming Terminal	Building	BC[illegible]		
			Force	Ajar	Single	Double	Dual	Manual	Auto				[illegible]	Glass	Fire Services
Point of Entry	Card Reader	Staff - Service Provider	☑	☑	☐	☑	☐	☐	☑	1800 - 0600	[illegible]	☑	[illegible]	☑	☑
			☐	☐	☐	☐	☐	☐	[illegible]		[illegible]	☐	[illegible]	[illegible]	☐
			☐	☐	☐	☐	☐	☐	[illegible]		[illegible]	☐	[illegible]	☐	☐
			☐	☐	☐	☐	[illegible]	☐	☐		[illegible]	☐	[illegible]	☐	☐
			☐	☐	[illegible]	☐	[illegible]	☐	☐		[illegible]	☐	[illegible]	[illegible]	☐
			☐	☐	[illegible]	☐	[illegible]	☐	[illegible]		[illegible]	[illegible]	[illegible]	☐	☐
			☐	☐	☐	☐	[illegible]	☐	☐		[illegible]	[illegible]	☐	☐	☐
			☐	☐	☐	☐	[illegible]	☐	☐		[illegible]	☐	☐	☐	☐
			[illegible]	☐	☐	[illegible]	[illegible]	☐	☐		☐	☐	☐	☐	☐
			[illegible]	☐	☐	[illegible]	[illegible]	☐	☐		☐	☐	☐	☐	☐
			[illegible]	☐	☐	[illegible]	[illegible]	☐	☐		☐	☐	☐	☐	☐
			[illegible]	☐	☐	☐	☐	☐	☐		☐	☐	☐	☐	☐
			[illegible]	☐	☐	☐	☐	☐	☐		☐	☐	☐	☐	☐
			☐	☐	☐	☐	☐	☐	☐		☐	☐	☐	☐	☐
			☐	☐	☐	☐	☐	☐	☐		☐	☐	☐	☐	☐
			☐	☐	☐	☐	☐	☐	☐		☐	☐	☐	☐	☐

6 Historical Version Control records

Section Modified	Description of Modification	Version	Organisation	Representative	Date
1.1; 1.8	The term "Design Engineer" changed to "Designer"	1.01	Asset Technologies Pacific	Donny Yap	10/08/06
1.8	Life Cycle Costings changed to Section 1.9	1.02	Asset Technologies Pacific	Tom Poyner	17/11/06
1.9	Section 1.8 changed to Warranty	1.02	Asset Technologies Pacific	Tom Poyner	17/11/06
1.4	"Australian Communications Authority" changed to "Standards Australia"	1.02	Asset Technologies Pacific	Tom Poyner	27/11/06
1.4	"TS 008/9" changed to "AS/ACIF S009:2006-11-08"	1.02	Asset Technologies Pacific	Tom Poyner	27/11/06
1.4	"ACA standards for cabling requirements" changed to "Installation requirements for customer cabling (wiring rules)"	1.02	Asset Technologies Pacific	Tom Poyner	27/11/06
1.7.5	2nd row of table 1.8 deleted	1.02	Asset Technologies Pacific	Tom Poyner	27/11/06
1.7.5	"Milfare" and "TIRIS" changed to "Generic*"	1.02	Asset Technologies Pacific	Tom Poyner	27/11/06
1.7.5	Clarification added to generic for compatibility with current electronic access system.	1.02	Asset Technologies Pacific	Tom Poyner	27/11/06
1.7.5	"Model" changed to "Frequency"	1.02	Asset Technologies Pacific	Tom Poyner	27/11/06
1.7.5	"Standard" and "Plus" changed to "125kHz"	1.02	Asset Technologies Pacific	Tom Poyner	27/11/06
Throughout	UOW Logo added to headers	1.02	Asset Technologies Pacific	Tom Poyner	28/11/06
1.2	Add risk assessment activity to conceptual design process.	1.02	Asset Technologies Pacific	Tom Poyner	1/12/06
1.4	Insert OH&S reference link	1.02	Asset Technologies Pacific	Tom Poyner	1/12/06
1.3.4	Paragraph added on remote arming terminals	1.02	Asset Technologies Pacific	Tom Poyner	1/12/06
1.6.5	Remote Arming Terminals added	1.02	Asset Technologies Pacific	Tom Poyner	1/12/06
Throughout	Amended Table #'s	1.03	University of Wollongong	David Anderson/ Chris Hewitt	18/7/07

Section Modified	Description of Modification	Version	Organisation	Representative	Date
1.7.5	Access Readers – added 2 more rows to table 1.4	1.04	University of Wollongong	David Anderson/ Chris Hewitt	30/4/08
1.7.1	Field Processing Units – added 2 more rows to table 1.4	1.04	University of Wollongong	David Anderson/ Chris Hewitt	30/4/08
1.7.6	Electric Locks – added 3 more lines to table 1.9	1.04	University of Wollongong	David Anderson/ Chris Hewitt	30/4/08
1.7.7	V Lock – added 1 more line to table 1.10	1.04	University of Wollongong	David Anderson/ Chris Hewitt	30/4/08
1.3.6	Path of Egress – inserted new section	1.05	University of Wollongong	David Anderson/ Chris Hewitt	15/06/10
1.6	Design of Operational Control Strategies - inserted new section	1.05	University of Wollongong	David Anderson/ Chris Hewitt	15/06/10
1.7	Installation Guidelines – renumbered section	1.05	University of Wollongong	David Anderson/ Chris Hewitt	15/06/10
1.8	Documentation Conventions – inserted new section	1.05	University of Wollongong	David Anderson/ Chris Hewitt	15/06/10
1.9	Equipment – renumbered section	1.05	University of Wollongong	David Anderson/ Chris Hewitt	15/06/10
1.9.6	Electric Lock – amended section	1.05	University of Wollongong	David Anderson/ Chris Hewitt	15/06/10
1.10	Warranty – renumbered section	1.05	University of Wollongong	David Anderson/ Chris Hewitt	15/06/10
1.11	Life-Cycle Costing – renumbered section	1.05	University of Wollongong	David Anderson/ Chris Hewitt	15/06/10

Section Modified	Description of Modification	Version	Organisation	Representative	Date
Appendix A	Appendix A – Inserted Table 1.14	1.05	University of Wollongong	David Anderson/ Chris Hewitt	15/06/10
1.6	Modify Figure 1.2	1.06	University of Wollongong	David Anderson/ Chris Hewitt	21/06/10
Appendix A	Modified Table 1.14	1.06	University of Wollongong	David Anderson/ Chris Hewitt	21/06/10
1.3.8	Inserted Remote Arming Terminal Section	1.07	University of Wollongong	David Anderson/ Chris Hewitt	27/07/10
1.3.9	Inserted Building Lockdown Reader Section	1.07	University of Wollongong	David Anderson/ Chris Hewitt	27/07/10
1.6	Inserted Sub-Clause (l) RAT and Lockdown Functionality	1.07	University of Wollongong	David Anderson/ Chris Hewitt	27/07/10
1.6	Updated Flow Diagram with RAT and Lockdown Functions	1.07	University of Wollongong	David Anderson/ Chris Hewitt	27/07/10
Appendix A	Inserted Columns for RAT and Building Lockdown	1.07	University of Wollongong	David Anderson/ Chris Hewitt	27/07/10
1.6.1	Programming Alarm Parameters	1.08	University of Wollongong	David Anderson/ Chris Hewitt	19/08/10
1.9	Door Alarm Naming Convention	1.08	University of Wollongong	David Anderson/ Chris Hewitt	19/08/10
Throughout	Amended Clause #'s	1.08	University of Wollongong	David Anderson/ Chris Hewitt	19/08/10
Throughout	Document updated to reflect name change from Buildings & Grounds (B&G) to Facilities Management Division (FMD) and rebranding logo	2	University of Wollongong	Yvonne Butcher	5/3/2012
Throughout	Document updated to reflect changes to controllers and card readers, etc. Interim update to major review	4	University of Wollongong	David Anderson	31/08/2017

4.8					