



University of Wollongong

Electronic Monitoring and Access Control Design Standards
Version 1.08 – 25 March 2011



QUALITY SYSTEM

Reason for Issue:	Updated
Client:	University of Wollongong
Director Responsible:	Bruce Flint
Director's Signature:	
Primary Consultants:	Donny Yap
Issue:	Version 1.08 – 25 March 2011

CONFIDENTIAL

This document contains confidential information solely for use by the University of Wollongong. All reasonable precautionary methods in handling the document and the information contained herein should be taken to prevent any third party from obtaining access without the approval of the University of Wollongong.



VERSION CONTROL SYSTEM

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	2 nd 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 (I) 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



TABLE OF CONTENTS

1.	ELECTRONIC MONITORING AND ACCESS CONTROL	2
1.1	OVERVIEW	2
1.2	DESIGN PROCESS	3
1.3	FUNCTIONAL REQUIREMENTS	4
1.3.1	General	4
1.3.2	Perimeter Alarm Monitoring and Access Control	4
1.3.3	Lift Alarm Monitoring and Access Control	5
1.3.4	Internal Secure Area Alarm Monitoring and Access Control	5
1.3.5	Systems Interfacing	5
1.3.6	Paths of Egress	6
1.3.7	Operational Monitoring	6
1.3.8	Remote Arming Terminal	7
1.3.9	Building Lockdown Reader	7
1.4	STANDARDS	7
1.5	MINIMUM PERFORMANCE STANDARDS	8
1.6	DESIGN OF OPERATIONAL CONTROL STRATEGIES	9
1.6.1	Programming Alarm Parameters	11
1.7	INSTALLATION GUIDELINES	11
1.7.1	Electrical Cabling	11
1.7.2	Communication Cabling	11
1.7.3	Field Devices	12
1.7.4	Field Processing Units	12
1.7.5	Remote Arming Terminals	12
1.7.6	Operator Terminal	13
1.7.7	Labelling	13
1.8	DOCUMENTATION CONVENTIONS	13
1.9	DOOR ALARM NAMING CONVENTION	13
1.10	EQUIPMENT	14
1.10.1	Field Processing Units	14
1.10.2	Operator Terminal	15
1.10.3	Application Software	15
1.10.4	Alarm Devices	15
1.10.5	Access Reader	16
1.10.6	Electric Lock	17
1.10.7	V-Lock	18
1.10.8	Electric Strike	18
1.10.9	Detectors	18
1.11	WARRANTY	20
1.12	LIFE-CYCLE COSTING	20
	APPENDIX A – OPERATIONAL CONTROL STRATEGY SPREADSHEET	21



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 Cardax FT System. All hardware, software and field devices shall be Cardax FT compliant and approved.

1.1 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.



1.2 DESIGN PROCESS

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

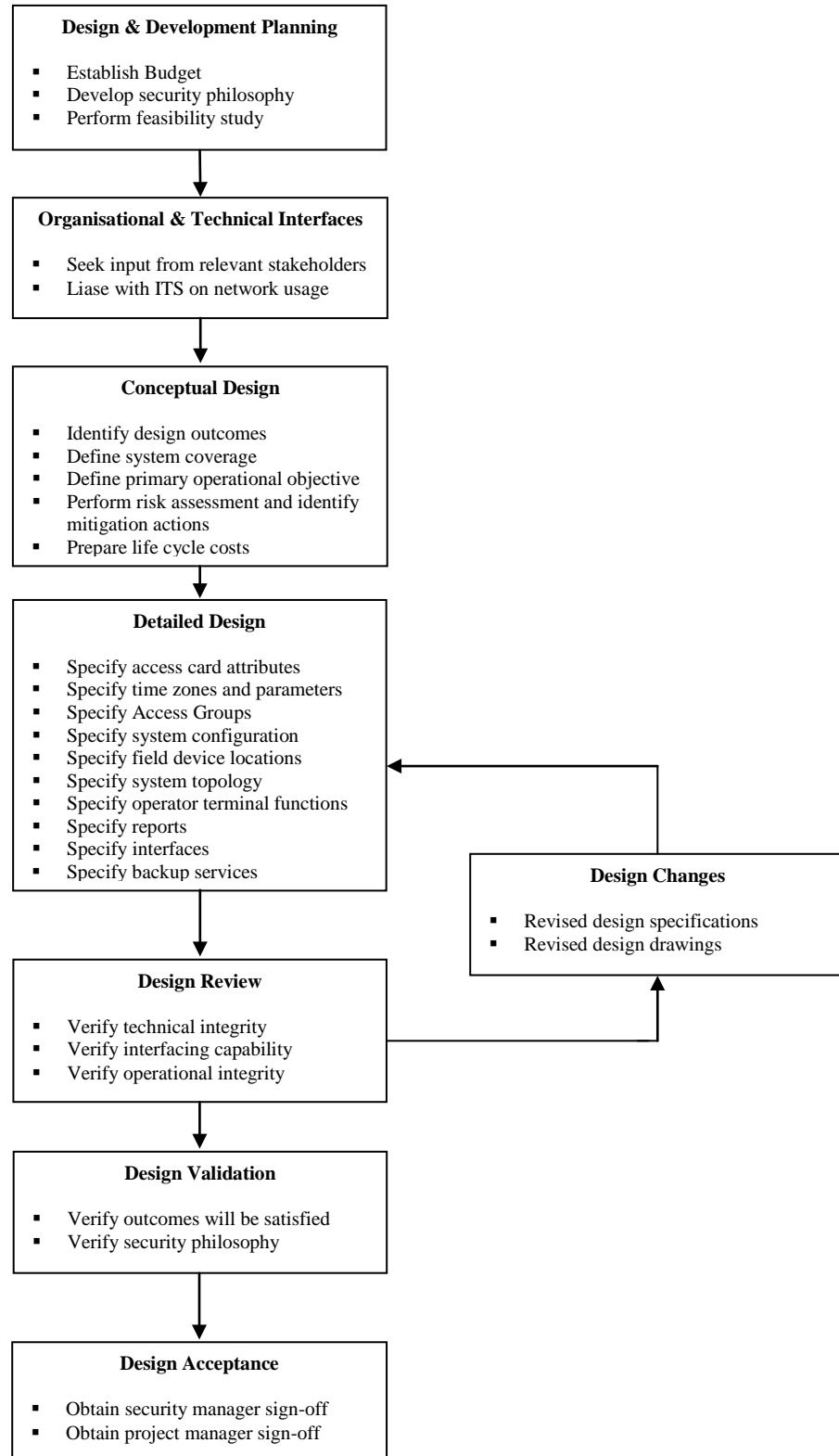


Figure 1.1 - Process Flow



1.3 FUNCTIONAL REQUIREMENTS

1.3.1 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.

1.3.2 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 Cardax FT 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 a v-lock or hook 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. Push buttons such those installed internally adjacent to the door should only be provided for automated doors which would require after-hours release.



1.3.3 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.

1.3.4 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 Cardax FT 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 a 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. Push buttons such those installed internally adjacent to the door should only be provided for automated doors which would require after hours release.

1.3.5 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 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 Interfaces

1.3.6 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.

1.3.7 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.



1.3.8 Remote Arming Terminal

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.

1.3.9 Building Lockdown Reader

At all satellite 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.

1.4 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

1.5 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



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

1.6 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:

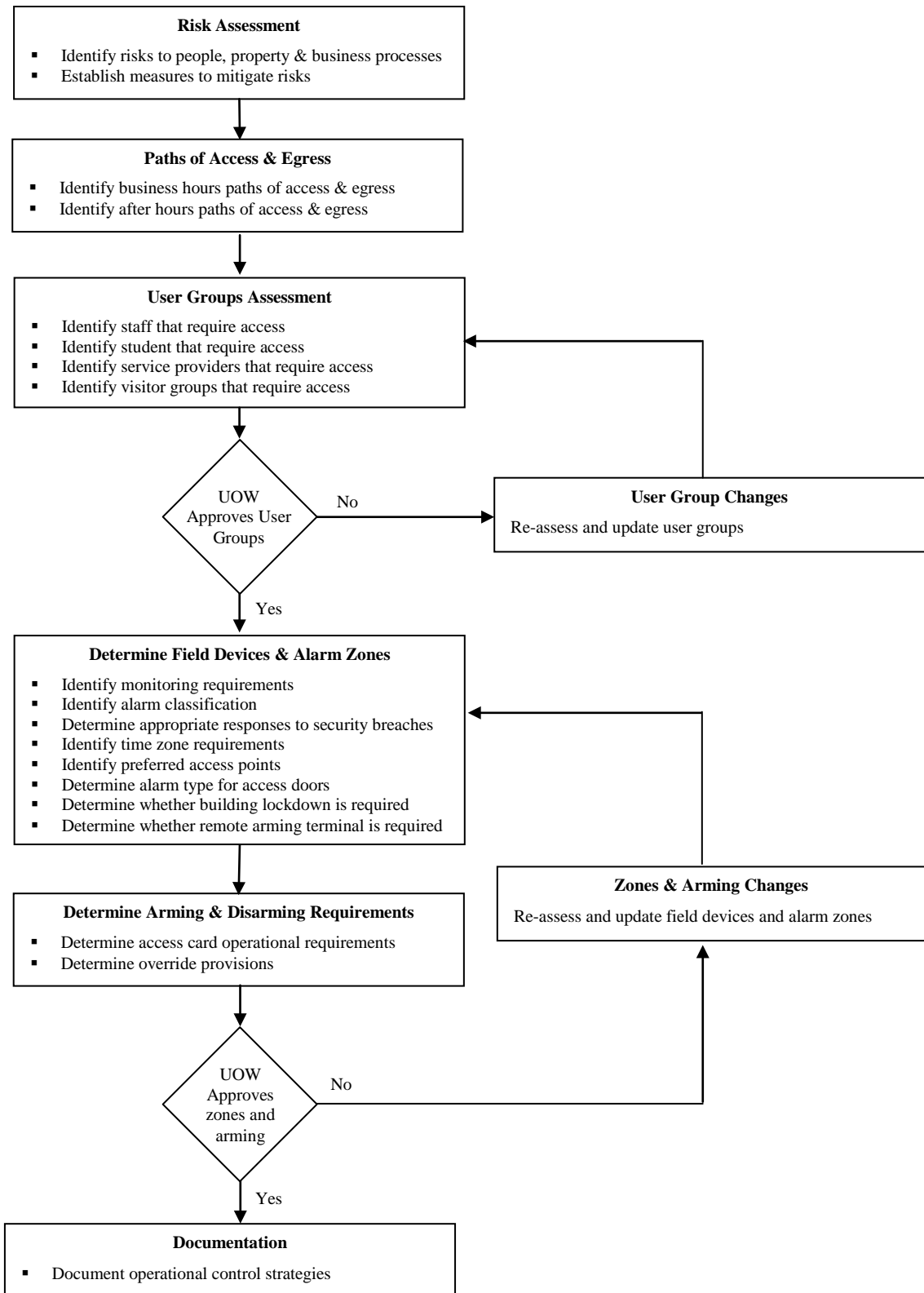


Figure 1.2 – Operational Control Strategies Process Flow



1.6.1 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 during after hours periods also transmitted to third party monitoring centre as either critical, very high or high alarm.

To enable the alarm to be transmitted to a third party monitoring centre a communications device must be provided at each site to enable dialup facility.

1.7 INSTALLATION GUIDELINES

1.7.1 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.

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.

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.

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

1.7.2 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.

1.7.3 Field Devices

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.

1.7.4 Field Processing Units

The FPU shall be installed in designated service areas where adequate access and ventilation is available. The location shall maintain separation from other building services such as electrical and fire systems.

The FPU cabinets 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.

1.7.5 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.



1.7.6 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.

1.7.7 Labelling

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

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

1.8 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.

1.9 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> <Door-Type> <Door-Number> will be used.



This convention will include the following terms:

- Building: B#;
- Ground: G;
- Perimeter: P;
- Roller Door: RD;
- Level: either G for Ground ; L1 for level 1, L2 for Level 2 etc; and
- Room: R.

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 identified as by the room number eg room G101 would be B32 G RG101. 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 North Corridor.

1.10 EQUIPMENT

1.10.1 Field Processing Units

Table 1.4 below contains the Cardax FT Controller Field Processing Units (FPU) that shall be used for monitoring and control functions.

Device	Function	Make	Model	Rating
Cardax FT Controller 3000	<ul style="list-style-type: none"> ▪ Network communications ▪ Reader control ▪ Maintains historical records 	Gallagher Security	Cardax FT Controller 3000	16 balanced inputs 8 relay outputs
Cardax FT Controller 5000	<ul style="list-style-type: none"> ▪ Network communications ▪ Reader control ▪ Monitors access control and security ▪ Maintains historical records 	Gallagher Security	Cardax FT Controller 5000	24 balanced inputs 8 relay outputs
Cardax FT Remote Alarming Terminal	<ul style="list-style-type: none"> ▪ Allows for monitoring, arming and disarming of alarm zones ▪ Networked to the Cardax FT Controller 3000 	Gallagher Security	Cardax FT Remote Alarming Terminal	100 inputs on any Cardax FT Controller
Cardax FT Controller 5000GL	<ul style="list-style-type: none"> ▪ Network communications ▪ Reader control ▪ Monitors access control and security ▪ Maintains historical records 	Gallagher Security	Cardax FT Controller 5000GL	4 balanced inputs 1 relay output

Table 1.4 - Field Processing Units



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

1.10.2 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	Model	Rating
Central Processing Unit	<ul style="list-style-type: none"> Operator terminal computer 	UOW lease standard	Pentium 4	3 Gigahertz
Visual Display Unit	<ul style="list-style-type: none"> Presents visual display of operations and data 	UOW lease standard	15 inch	50 Hertz

Table 1.5 - Operator Terminal Devices

1.10.3 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
Cardax FT Command Centre Software	<ul style="list-style-type: none"> Alarm management Access card programming System configuration Device control 	Gallagher Security	Cardax FT Command Centre	Microsoft SQL 2000

Table 1.6 - Application Software

1.10.4 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
1/2" Steel Door Contact	<ul style="list-style-type: none"> Door alarm 	General Electric	1076	100V
3/4" Steel Door Contact	<ul style="list-style-type: none"> Door alarm 	General Electric	1078	30V
3" Overhead Door Magnetic Contacts	<ul style="list-style-type: none"> Door alarm 	General Electric	2202	100V



Device	Function	Make	Model	Rating
3/8" Recessed Contact	<ul style="list-style-type: none"> Alarm devices 	General Electric	1015	30V
1" Surface Mount Miniature Self-Adhesive Contact	<ul style="list-style-type: none"> Alarm devices 	General Electric	1035	100V
1" Surface Mount Magnetic Contact	<ul style="list-style-type: none"> Door alarm 	General Electric	1038	100V
2.54" x 0.545" x 0.690" Surface Mount Designer Styled Terminal Contact	<ul style="list-style-type: none"> Door alarm 	General Electric	1285T	100V
3" Overhead Door Mount	<ul style="list-style-type: none"> Door alarm 	General Electric	2200	100V
3" Curtain Door Track Mount Contact	<ul style="list-style-type: none"> Door alarm 	General Electric	2302	100V
1.77"W x 2.90"L x 0.76"H Panic Switch	<ul style="list-style-type: none"> Alarm device 	General Electric	3040	100V

Table 1.7 - Alarm Devices

1.10.5 Access Reader

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

Device	Function	Make	Frequency	Rating
Cardax Prox Readers	<ul style="list-style-type: none"> Provides access through the use of a valid access card 	Generic*	125kHz	100V
Cardax Prox Readers	<ul style="list-style-type: none"> Provides access through the use of a valid access card and/or PIN access code 	Generic*	125kHz	100V
Cardax Prox Readers	<ul style="list-style-type: none"> Provides access through the use of a valid access card 	Prox 125	125kHz	100V
Cardax Prox Readers	<ul style="list-style-type: none"> Provides access through the use of a valid access card and/or PIN access code 	Prox Plus 125	125kHz	100V

Table 1.8 - Access Reader

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



1.10.6 Electric 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
Electric lock	<ul style="list-style-type: none"> ▪ Vestibule lock ▪ Non-monitored lock (reversible) 	Lockwood	3572/3582 N1	12V or 24V
Electric lock	<ul style="list-style-type: none"> ▪ Vestibule lock ▪ Monitored lock (reversible) 	Lockwood	3572/3582 M1	12V or 24V
Electric lock	<ul style="list-style-type: none"> ▪ Vestibule lock ▪ Key override ▪ Non-monitored lock (reversible) 	Lockwood	3572/3582 N2	12V or 24V
Electric lock	<ul style="list-style-type: none"> ▪ Vestibule lock ▪ Key override ▪ Monitored lock (reversible) 	Lockwood	3572/3582 M2	12V or 24V
Electric lock	<ul style="list-style-type: none"> ▪ Vestibule lock ▪ Key override ▪ Monitored key override (handed) 	Lockwood	3572/3582 M4/5	12V or 24V
Electric lock	<ul style="list-style-type: none"> ▪ Vestibule lock ▪ Key override ▪ Monitored lock (reversible) 	Lockwood	3572/3582 M2	12V or 24V
Electric lock	<ul style="list-style-type: none"> ▪ Vestibule lock ▪ Key override ▪ Monitored lock (reversible) 	Lockwood	3572ELEMO	4 balanced inputs 1 relay output
Electric lock	<ul style="list-style-type: none"> ▪ Vestibule lock ▪ Key override ▪ Monitored lock 	Lockwood	3582 M1	
Electric lock	<ul style="list-style-type: none"> ▪ Vestibule lock ▪ Key override ▪ Monitored lock (reversible) 	Lockwood	3582 M5	

Table 1.9 - Electric Lock



1.10.7 V-Lock

V-locks shall be used to secure the passive leaf of double leaf doors.

Device	Function	Make	Model	Rating
V-Lock	<ul style="list-style-type: none"> Secure passive leaf of double doors 	Padde	ES8000	12V
Vestibule Lock	<ul style="list-style-type: none"> Secure passive leaf of double door 	Abloy	EL413	12V

Table 1.10 - V-Lock

1.10.8 Electric Strike

Electric strikes provide automatic locking of doors. Table 1.11 below contains the preferred electric strikes.

Device	Function	Make	Model	Rating
Electric Strike Wide Lip	<ul style="list-style-type: none"> Electronic door locking 	Padde	ES320	12V
Electric Strike ANSI Lip	<ul style="list-style-type: none"> Electronic door locking High security 	Padde	ES3100	12V
Electric Strike Non-Monitored	<ul style="list-style-type: none"> Electronic door locking High security 	Padde	ES310	12V
Electric Strike Non-Monitored	<ul style="list-style-type: none"> Electronic door locking High security 	Padde	ES200	12V
Electric Strike Monitored	<ul style="list-style-type: none"> Electronic door locking Monitored 	Padde	ES2000	12V

Table 1.11 - Electric Strike

1.10.9 Detectors

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

Device	Function	Make	Model	Rating
200' Mirror Optic PIR	<ul style="list-style-type: none"> Detects heat 	General Electric	AP633	12V
200' Mirror Optic PIR	<ul style="list-style-type: none"> Detects heat 	General Electric	AP633A	12V
50' Mirror Optic PIR	<ul style="list-style-type: none"> Detects heat 	General Electric	AP450	12V
75' Mirror Optic PIR Single	<ul style="list-style-type: none"> Detects heat 	General Electric	AP475	12V



Device	Function	Make	Model	Rating
Curtain				
60' Ceiling Mount PIR	<ul style="list-style-type: none"> ▪ Detects heat 	General Electric	AP669RT	12V
50' Wireless PIR Motion Sensor	<ul style="list-style-type: none"> ▪ Detects heat 	General Electric	AP750W	12V
50' Mirror Optic PIR 2-in-1 Pet Immune	<ul style="list-style-type: none"> ▪ Detects heat 	General Electric	AP950 PI	12V
50' Mirror Optic PIR Antimasking High-Security Sensor	<ul style="list-style-type: none"> ▪ Detects heat 	General Electric	AP950 AM	12V
5.6" x 2.75" Audio converter	<ul style="list-style-type: none"> ▪ Detects movement by microwave channels 	General Electric	KTD336	12V
40' x 40' Optex Passive and Microwave Sensor	<ul style="list-style-type: none"> ▪ Detects movement 	General Electric	DX40	12V
40' x 40' Optex PIR / Microwave, Relay Output & Alarm Memory	<ul style="list-style-type: none"> ▪ Detects movement 	General Electric	DX40 Plus	12V
60' x 60' Optex Passive and Microwave Sensor	<ul style="list-style-type: none"> ▪ Detects movement 	General Electric	DX60	12V
60' x 60' Optex PIR / Microwave, Trouble Relay Output & Alarm Memory	<ul style="list-style-type: none"> ▪ Detects movement 	General Electric	DX60 Plus	12V
40' x 40' Optex PIR / Microwave W / Pet Immunity	<ul style="list-style-type: none"> ▪ Detects movement 	General Electric	MX40PI	12V
50' x 50' Optex Standard PIR/ Microwave Sensor	<ul style="list-style-type: none"> ▪ Detects movement 	General Electric	MX50T	12V

Table 1.12 - Detectors



1.11 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	12 Months
Electric Locks	12 Months
V-Locks	12 Months
Electric Strikes	12 Months
PIR Detectors	12 Months
Field Processing Units	12 Months
Operator Terminal	12 Months
Application Software	12 Months

Table 1.13 - Warranty Periods

1.12 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



APPENDIX A – OPERATIONAL CONTROL STRATEGY SPREADSHEET

Access Requirement	Security Measure	Access Group	Alarm Monitoring		Access Card Presentation			Override		Secure Period	Remote Arming Terminal	Building Lockdown	BCA Requirement		
			Force	Ajar	Single	Double	Dual	Manual	Auto				Local Smoke Detector	Break Glass	Fire Services
Front Door Point of Entry	Electric Lock & Card Reader	- Staff - Service Provider	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	1800 - 0600	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
			<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
			<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
			<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
			<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
			<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
			<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
			<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
			<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
			<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
			<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
			<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
			<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
			<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
			<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
			<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Table 1.14 - Spreadsheet