UNIVERSITY OF WOLLONGONG AUSTRALIA

University of Wollongong

Closed Circuit Television Design Standard

Version 6 – 18 November 2016

VERSION CONTROL SYSTEM

Section Modified	Description of Modification	Version	Organisation	Representative	Date
Throughout	First Issue	1.01	University of Wollongong	Chris Hewitt / David Anderson	09/02/07
Throughout	Final Issue	1.02	University of Wollongong	Chris Hewitt / David Anderson	07/03/07
Title	Revised Title	1.03	University of Wollongong	Chris Hewitt / David Anderson	27/9/07
Section 9	Amended re Mini Dome Camera	1.04	University of Wollongong	Chris Hewitt / David Anderson	19/11/07
9.1.1	Fixed IP Cameras – Added information to Table 5	1.05	University of Wollongong	Chris Hewitt / David Anderson	30/4/08
9.3	Video Management & Storage Software – added Table 7	1.05	University of Wollongong	Chris Hewitt / David Anderson	30/4/08
Throughout	Updates to camera list, control strategy design process, system description and installation practices.	1.06	University of Wollongong	Chris Hewitt / David Anderson	26/10/10
Throughout	Updated frame rate and head end responsibilities	1.07	University of Wollongong	Chris Hewitt / David Anderson	24/12/10
8.1.1	Fixed IP Cameras – Added camera information to Table 5	1.07	University of Wollongong	Chris Hewitt / David Anderson	24/12/10
8.1.2	PTZ IP Cameras – Added camera information to Table 6	1.07	University of Wollongong	Chris Hewitt / David Anderson	24/12/10
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
3.1 3.2.1 3.3 6.2.2 7. 8.1 8.2 8.3.1	Clarified wording Clarified wording Added requirement for HD in high risk areas Clarified wording Rectified section numbering Updated camera selection table Identified preference for PoE Identified DVTel naming convention preference	3	Asset Technologies Pacific	Donny Yap	12/10/12
7.1.3 7.1.4 8.0	7.1.3 becomes 7.1.4 7.1.3 provides advice on preferred DVTEL supplier in Australia. Note: Software compatibility camera equipment – PTZ version 6.2. Caveat.	4	University of Wollongong	David Anderson	22/11/14
1.2 1.2 & 8.0 2.1 & 7.1.2 7.1.3 8. 8.1.1 8.1.2 8.2 Throughout	Updated location of security control room Identified impact of DVTel's acquisition by FLIR Inserted industrial Ethernet requirements Updated distributor information Inserted camera model / feature naming method Updated fixed IP camera selection table Updated PTZ IP camera selection table Updated PoE considerations Clarified wording and inserted current UOW logo	5	Asset Technologies Pacific	Antony Straubhaar	28/10/16

Section Modified	Description of Modification	Version	Organisation	Representative	Date
6.3.1 7.1.4	Updated locations Updated security contractor requirements	6	Asset Technologies Pacific	Antony Straubhaar	06/12/16

Contents

1 Overview

Closed circuit television (CCTV) systems form part of the overall security strategy implemented by the University of Wollongong (UOW).The systems are used to provide the following key functions:

a. Real time surveillance;

b. Recording of real time events and historical video data for video evidence of a security event; and

c. Provide a deterrent to criminal and unacceptable behaviour.

To obtain optimum performance the CCTV systems may be interfaced with other building services, in particular electronic monitoring and access control systems.

This document shall be used as the design standard for all future CCTV installations and upgrades at UOW. The CCTV Design Standard shall be used in conjunction with UOW's Documentation Standard, Electrical Services Design Standard and UOW's Specification for Voice and Data.

1.1 Objective

The objective of this design standard is to outline the functional, installation and technical requirements for UOW's CCTV system. The designer shall use this standard as the basis for new systems or extensions to the existing system at UOW. Whilst the design standard provides guidance on the minimum acceptable standard to UOW, it is incumbent upon the designer to ensure that the final design satisfies site-specific operational, logistical and performance requirements and meets UOW's security objective for the facility. (ie. a superior standard may be required to satisfy specific objectives)

Prior to undertaking the conceptual design, a risk analysis must be performed to determine the level of risk anticipated for the specific area. Where risks are identified that it is appropriate to use CCTV as part of the mitigation strategy, the environmental conditions and occupancy profile will also be taken into consideration.

1.2 System Description

The CCTV system installed at UOW is an Internet Protocol (IP) CCTV system. The system utilises digital technology for recording and for transmitting video images via UOW's Local Area Network (LAN). The IP CCTV system allows the flexibility for additional cameras to be added to the system at any time and be viewed on any workstation on the campus with a network connection and software licence.

The CCTV system currently utilised by UOW is a DVTel (now FLIR Systems) IP CCTV system. The cameras comprise digital IP cameras as well as older analogue cameras that are interfaced using analogue to digital converters.

The operator's terminal and control equipment are located within building 39, located on Northfields Avenue. The system utilises UOW's IT network to transmit digital images from the IP cameras to monitors for viewing and servers for recording purposes.

2 Design Process

The process shown below in Figure 1 shall be followed to achieve UOW's desired outcomes:

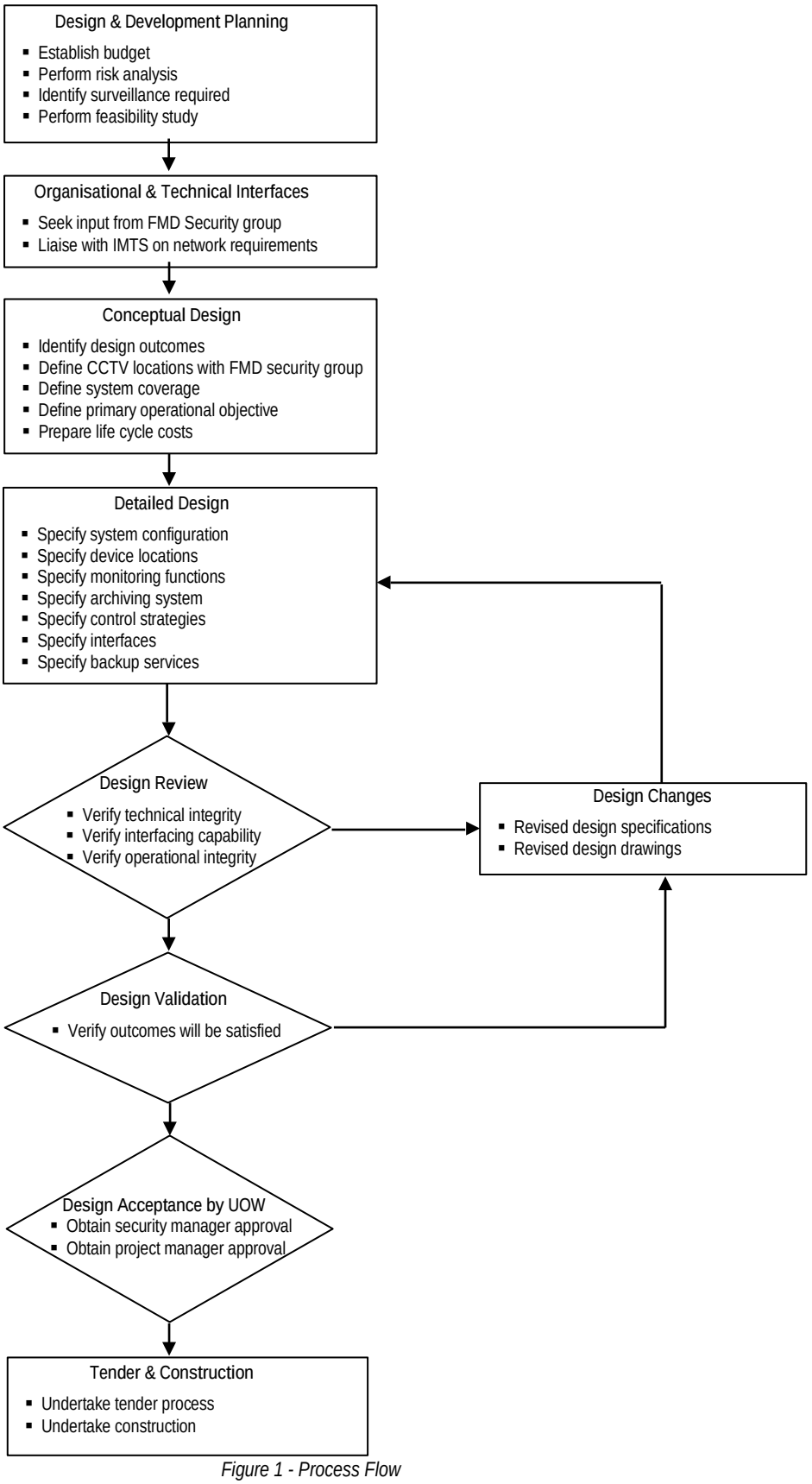

Figure 1 - Process Flow

2.1 Design of Configuration Parameters & Control Strategies

As part of the detailed design, operational control strategies shall be developed to ensure efficient utilisation of the equipment. The designer shall liaise with UOW Security and business area managers to identify the design priorities. The design spreadsheet attached in Appendix A shall be completed as part of the following procedure for extending or designing a new system:

a. Identify the location in which surveillance is required and assess the associated risks;

b Identify the primary subject in the location of surveillance and the type of view required. The primary subject may be a fixed point of interest (eg. an Automatic Teller Machine, Point of Sale Terminals, Laboratory entrance etc) or a general subject of interest (eg. Outdoor bar area)

c. Determine the primary purpose of surveillance. The different surveillance purposes include:
   i. Historical analysis - where the primary purpose is to record video evidence for later analysis;
   ii. Deterrence - where the camera is overtly visible as a means of deterring undesirable behaviour;
   iii. Real-time surveillance - where the camera is actively monitored by staff; and
   iv. Object video analysis - where the footage is analysed by software for alarm conditions.

d. Identify the period during which surveillance is required. Cameras in some locations may not be required out-of-hours, whilst others requiring 24/7 operation may require the consideration of after-hours illumination.

e. Identify the lighting sources in the area.

f. Nominate the camera features required based on the camera purpose and lighting sources available. The feature options include:
   i. Pan tilt zoom;
   ii. IR sensitivity;
   iii. IR lamp (integrated);
   iv. Thermal sensitivity;
   v. Tamper proof enclosure; and
   vi. Weatherproof enclosure.

g. Specify the PTZ home location, if applicable. If used, this will likely be a view of the primary subject.

h. Nominate the monitoring features required. These include:
   i. Capability to activate a monitor display on alarm activation;
   ii. Alarm ID for integration if applicable;
   iii. Whether the camera should be included as part of an existing video monitor rotation.

i. Determine the field of vision required, and correspondingly, the percentage of the screen that the subjects will occupy. This will determine whether the video can be used for observation, detection, recognition or identification.

j. Determine the rate of motion of subjects within the field of vision.

k. Identify the frame rate required for recording purposes.

l. Calculate the network bandwidth required to support the video and the associated hard disk storage requirements.

m. Where external IP cameras are to be installed in such a manner that they will not be affixed to a building, then the cameras shall be connected using industrial Ethernet. The design, protocols and specifications shall be developed in consultation with IMTS, taking into consideration UOW's requirements for rugged connectors, cables, low latency, better determinism etc.

n. Prepare and submit a budget of all equipment required for approval.

3 Functional Requirements

3.1 General

The IP CCTV system shall operate in all light conditions, including low light environments and shall automatically compensate for changing light conditions. In higher security installations or where the control strategy calls for video motion detection, the systems must be configurable to identify activity of interest, and discriminate this from spurious movement occurring under normal environmental conditions.

The system shall provide alarm condition detection/activation and fully interface with the electronic monitoring and access control system.

External camera and communication devices shall be mounted within housings that are rated to IP66 and function satisfactorily in all weather conditions.

The IP CCTV system shall be designed with a scalable architecture to allow expansion through the installation of additional cameras, control, network and storage devices. There shall be no limit on the number of workstations located throughout the UOW IT network.

3.2 Surveillance

The CCTV system cameras shall produce sharp, detailed and stable images on the monitor in sufficient detail to provide positive identification of individuals within the protected areas under all conditions of light.

Where required, wide coverage public areas shall be viewed with pan, tilt and zoom (PTZ) IP cameras, to provide close up images and tracking of events.

Fixed position and fixed focus IP cameras shall be used where a specific risk has been identified in a particular area and it is important that should an event occur it is viewed in real time or recorded.

The cameras shall be fitted with automatic light compensation devices to provide compensation for variations over a wide range of scene brightness. Where a camera must operate in total darkness, the nature of the possible events will be analysed to determine whether the situation requires a special application camera such as one that uses infra-red illumination.

Where identified in the risk analysis, cameras with “Wide Dynamic Range” shall be installed and connected into the video signal lines to overcome the possibility of the camera being blinded deliberately or accidentally by bright lights.

The suppression device shall remove unwanted highlights allowing the automatic iris control compensation to adjust to the true ambient high level.

3.2.1 Operational Surveillance

The security operator workstation is the interface between the IP CCTV system and the operational security management team. The video signal from each camera shall be transmitted over the University’s IT network and be viewed on any workstation with a network connection.

Camera switching shall be fast and efficient with not more than 0.5 seconds delay between switching from one camera to another.

Prior to selecting the CCTV monitor(s), control strategies will be developed to ensure maximum efficiency in terms of operational surveillance. The existing cameras and monitors will be considered in developing new control strategies and where appropriate, existing strategies will be modified to accommodate the new installation.

The design objective should be to minimise the number of monitors required by implementing control strategies including alarm activation, environmental sensing, intelligent programming and sequencing, and thereby reduce the dependency on the security operators to identify alarm conditions.

The security operator workstation shall be programmed to perform the following functions:

- Alarm management;
- Manual control of cameras;
- Automatic sequencing and control;
- Display of activated cameras;
- Reporting; and
- Database management.

The IP CCTV system shall be capable of allowing PTZ camera control from a workstation without the need for a dedicated operator keyboard. This shall be achieved through the use of DVTel / FLIR User Licences to allow camera control via a computer keyboard and mouse.

3.3 Video Data Management

Video data from fixed and PTZ IP cameras will be analysed using software as the video data is streamed into the operator workstation. An alarm signal will be flagged if an intruder or abnormality is detected.

Video shall be streamed from each camera at a fixed rate of 12 frames per second at a resolution of D1-PAL (720x576) for the purposes of viewing and recording. In areas of increased risk with a higher likelihood of requiring visual identification of persons, a high definition camera shall be installed and video streamed at not less than 720p and preferably 1080p. The increased storage requirements and bandwidth for the use of high definition video must be taken into account and approval obtained from UOW Security prior to activating this mode.

All IP CCTV cameras connected to the system shall digitally record for a minimum of 30 days and additional storage shall be considered for event recording. All abnormalities shall be digitally recorded for a period of no less than 30 days, and shall be capable of being utilised appropriately by the police in evidence and stored, copied and viewed without interfering with recording.

The system shall provide for video buffering of all alarm points and shall provide pre-alarm and post-alarm recording when an alarm has occurred.

Video storage capacity shall be considered at the beginning of the design process of the IP CCTV system to ensure UOW Security Service and UOW IMTS are familiar with the new installation, as well as additional equipment and additional storage requirements needed for the new system to operate at its optimum performance level.

The storage capacity of the IP CCTV system shall be confirmed and approved by UOW IMTS prior to installation occurring and additional storage requirements determined in consequence to the new installation. Approval of the new installation and final decision on any additional storage requirements must be obtained from the UOW Security Supervisor. The designer must incorporate into their installation budget any additional storage requirements which will be costed and provided by UOW IMTS.

3.4 Systems Interfacing

The IP CCTV system may be interfaced with the intercom system and the electronic monitoring and access control system depending on the requirements of the specific installation. This is shown in Table 1 below.

Where PTZ cameras are used in these circumstances the cameras shall be programmed to respond to the event conditions and automatically re-orientate to monitor the location of the event.

System to be Interfaced	Interface Type	Interface Responsibility
Electronic Monitoring and Access Control	High/Low level	Security contractor
Intercom System	Low level	Security contractor

Table 1 – Systems Interfacing

4 Standards

The design shall comply with the latest versions of all relevant codes and standards in force at the time of specification. Where the designer considers a standard to be inappropriate to the circumstances, the designer shall advise the principal and seek direction. Table 2 below contains a list of the relevant codes and standards.

Issuing Body	Document Number	Title
AUSTEL	AUSTEL	Australian Telecommunication Authority requirements
Australian Communications Authority	TS 008/9	ACA Standards for cabling requirements
BCA	BCA	Building Code of Australia requirements
CIBSE	LG6:1992	Chartered Institution of Building Services Engineers. The outdoor environment
Institute of Electrical and Electronics Engineers	IEEE 802.5 IEEE 802.3af IEEE 802.3at	Broadband applications Power Over Ethernet
Standards Australia	AS/NZS CISPR 14.1:2003	Electromagnetic compatibility - Requirement for household appliance, electric tools and similar apparatus - Emission
Standards Australia	AS/ACIF S009:2006	Installation requirements for customer cabling
Standards Australia	AS/NZS 1102.103:1997	Conductors and connecting devices
Standards Australia	AS 1125	Conductors in insulated electric cables and flexible cords

Issuing Body	Document Number	Title
Standards Australia	AS 1345	Identification of the contents of pipes, conduits and ducts
Standards Australia	AS 1367:2000	Coaxial cabling systems for the distribution of analogue television and sound signals in single and multiple unit installations
Standards Australia	AS 1939	Degrees of protection provided by enclosures for electrical equipment.
Standards Australia	AS 2053	Conduits and fittings for electrical installations
Standards Australia	AS 2834 - 1995	Computer accommodation
Standards Australia	AS 3000	Wiring Rules
Standards Australia	AS 3008	Electrical installations - Selection of cables
Standards Australia	AS 3011	Electrical installations - Secondary batteries installed in buildings
Standards Australia	AS 3080	Telecommunications installations - Generic cabling for commercial premises
Standards Australia	AS 3084	Telecommunications installations - Telecommunications pathways and spaces for commercial buildings
Standards Australia	AS 3085	Telecommunications installations – Administration of communications cabling systems – Basic requirements
Standards Australia	AS 3768 - 1990	Guide to the effects of the temperature on electrical equipment
Standards Australia	AS 4251	Electromagnetic compatibility (EMC) – Generic Emission Standard
Standards Australia	AS 4252	Electromagnetic compatibility - General immunity standard
Standards Australia	AS 4806	Closed Circuit Television (CCTV) Standards
Standards Australia	AS 61000	Electromagnetic compatibility (EMC)
UOW	ITS.ITS.001	Specification for Voice and Data
UOW	B&G-MAI-STA-013	Documentation Design Standard
UOW	B&G-MAI-STA-014	Electrical Design Standard

Issuing Body	Document Number	Title
UOW	B&G-MAI-STA-011	Building Elements Design Standard
UOW	B&G-MAI-STA-015	EMAC Design Standard

Table 2 – Relevant Standards

5 Minimum Performance Standards

The following minimum performance standards shall be achieved to ensure efficient operation of the CCTV system:

Functions	Worst Case Response (seconds)
Real time camera view displayed on display monitor at the operator workstation	0.5s
Switching to a different camera view on the display monitor at the operator workstation	1s
Real time video data analysis	1s
Display of historical report from report request	5s

Table 3 - Minimum Performance Standards

6 Installation Guidelines

6.1 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 physical strain does not occur to any part of the cable or to the connected equipment. Cables shall be securely supported and protected from mechanical damage.

The installation or normal use of the cabling does not expose carrier personnel, cabling providers, customers or other persons to any danger.

The
installation or normal use of the cabling does not adversely affect the integrity (proper end-to-end functioning) of a telecommunications network.

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.

6.1.1 Conduit/Duct

All exposed internal cabling shall be installed in PVC conduits and/or duct. Conduit and duct for internal installations shall be of PVC construction with white colour, unless an existing colour scheme is in use, whereby the conduit/duct shall match the existing equipment.

External cabling shall be installed in HDPE or PVC conduit. Underground cabling shall be installed at a minimum depth of 500mm. Cable marking tape with integrated tracer wire shall be installed above the conduit to facilitate future services location.

6.2 Communication Cabling

Communications cabling shall be part of an overall structured cabling system, compliant with UOW IMTS' Specification for Voice and Data Cabling. The type and size of communication cabling shall be selected to achieve optimum system performance.

Communication cabling shall be installed such that physical strain does not occur to any part of the cable or to the connected equipment. Cables shall be securely supported on cable trays or (where exposed) enclosed and protected from mechanical damage within conduits or duct.

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.

6.2.1 Qualifications

Personnel installing and commission cabling shall be ACMA licensed.

6.2.2 Conduit / Duct

Conduit and duct for internal installations shall be of PVC construction with white colour, unless an existing colour scheme is in use, whereby the conduit/duct shall match the existing equipment.

External cabling shall be installed in HDPE or PVC conduit. Conduit joins shall be sealed to prevent water entering and accumulating within the conduit and/or tracking back into the camera enclosure.

Underground cabling shall be installed at a minimum depth of 500mm. Cable marking tape with integrated tracer wire shall be installed above the conduit to facilitate future services location.

6.3 Cameras

6.3.1 Locations

Surveillance coverage shall be determined from an operational and risk analysis performed as part of the design and development planning phase. The risk analysis must consider the specific use and functionality of the building, facility or space and consider the views of the building operator and University Security Manager. The following camera locations shall be used as a minimum guide:

Entry & Exit Points

- Building entry / exit points at all levels;
- Library entry / exit points;
- Computer lab entry / exit points;
- Vehicle entry / exit points;
- Carpark general (internal), lane and external areas;
- Traffic control on Ring Road, driveways and boom gates; and
- Locations where intruders may gain entry without force.

Interaction Points

- Areas where staff, students and the public interact such as reception desks and help points;
- Reception desks;
- Mail distribution points;
- Client interaction points; and
- Areas where monetary transactions take place.

Assembly Areas

- Areas where students assemble / meet in large numbers such as external forecourts, internal common areas and social spaces, transport hubs etc;
- Lift lobbies at all levels;
- Library general floor areas; and
- Computer lab general areas.

Storage Areas

- Warehouse areas;
- Bike stores;
- Loading docks; and
- Areas where dangerous or valuable goods are stored.

Isolated Areas

- Building perimeters;
- Secluded areas;
- Areas where staff work alone or in small numbers on shifts; and
- Corridors in business or accommodation facilities or public areas provide access to sensitive areas.

General Areas

- Locations with duress/panic buttons;
- Locations of potential risky student behaviour;
- Locations that deter theft; and
- Circulation points inclusive of fire stairs/lift access.

6.3.2 Recommended Object Sizes

All IP CCTV equipment shall meet minimum requirements listed in *AS4806: Closed Circuit Television (CCTV) Parts 1, 2, 3 and 4*. Where CCTV is specified for an intended purpose, the design shall conform to the following requirements: A person of nominal height 1.6m shall occupy a portion of the image according to Table 4 below:

Purpose	Percentage of Screen (Vertical Element)
Face identification	100%
Face recognition	50%
Intrusion detection	10%
Crowd control	5%
License plate recognition (letter height)	5%

Table 4 – CCTV Object Size Requirements

6.3.3 Cabling and Termination

Cameras and cabling shall be mechanically secured and protected from mechanical damage. Terminations shall be permanent and insulated to protect against faults and from interference.

6.3.4 Internal IP Cameras

Internal IP cameras shall be fitted with opaque tinted acrylic domed housing to physically protect the cameras as well as to prevent observation of camera direction. Where specified, vandal proof housings shall be provided and installed.

6.3.5 External IP Cameras

External IP cameras shall be fitted inside enclosures that are IP66 rated and shall be weatherproof, robust, tamper resistant and fitted with sun shields. Thermostatically controlled internal blowers shall be provided to circulate air for maximum cooling during high ambient temperature conditions. Thermostatically controlled internal heaters shall be used during low ambient temperature conditions.

6.4 Operator Workstation

The operator workstation CPU, LCD monitors and other peripheral devices shall be installed at the location deemed to view the CCTV cameras. Interconnecting cables shall be protected from mechanical damage and permanently connected.

The LCD monitors shall be mounted adjacent to one another to provide easier viewing of the screens.

6.5 Labelling

Major system components (including every camera and IP network point) shall be clearly labelled using black lettering on white background self adhesive permanent engraved labels (eg. Traffolyte), attached to a suitable fixed part of the equipment or (where equipment is recessed or concealed) the building fabric.

Equipment labels shall identify the equipment in accordance with UOW's asset register convention. IP network points must be labelled in accordance with UOW IMTS' Specification for Voice and Data.

7 UOW & Security Contractor's Responsibilities

7.1 General

The IP CCTV system installed throughout the UOW campuses is made up of a number of components which together allow the system to function. The responsibility of these components is generally divided between the UOW IMTS department and the security contractor for any small or major works involving existing infrastructure. In the case of new building projects the Architects and consultants preparing specifications for any successful Builder will be responsible for ensuring that all design aspects for cabling works and camera designs are completed in consequence of these standards and to UOW IMTS standards and specifications.

7.1.1 UOW IMTS Department

The UOW IMTS department are responsible for the following components of the IP CCTV system:

- The Local Area Network (LAN)
- Workstations
- Monitors
- Servers
- Network connection ports
- Network switches
- Archiver servers or Hard disk drives (HDDs)
- Assignment of IP address

7.1.2 Security Installation Contractor

The security contractor is responsible for the following components of the IP CCTV system:

- Cameras
- Power Supplies
- Cabling
- CCTV System Management Software
- Camera licenses
- Software/User licenses
- Connection to network ports

Whilst UOW IMTS is responsible for providing CCTV head end server hardware, the security contractor remains responsible for installation, configuration, test and commissioning of the hardware and software.

The security contractor will also be responsible for ensuring the design meets UOW's minimum performance standards and functional requirements and is compliant with relevant standards. Where industrial Ethernet is to be used as part of the work, such as when external IP cameras are to be installed away from buildings, then the security contractor must consult with UOW's IMTS department to ensure that the specifications are appropriate. IMTS approved contractors shall be used.

7.1.3 Sole Australian Distributor

Security Contractors (integrators) are advised that all DVTel (now FLIR) cameras and camera licences must be sourced from Q Security Systems as it is the sole Australian distributor of these items.

7.1.4 Security Maintenance Contractor

Unless otherwise specified, maintenance of the CCTV equipment installed shall be performed by UOW's nominated security maintenance contractor. The security installation contractor shall be required to address issues during the warranty and defects liability period, irrespective of the contractor selected to perform the regular maintenance services.

The security maintenance contractor must be qualified to a suitable level to meet UOW standards and all relevant legislative, standard and code requirements. The security maintenance contractor must also maintain confidentiality, which will be enforceable during and after any engagement, and ensure procedures are implemented to achieve compliance with the requirements.

8 Equipment

UOW currently operates two DVTel systems with the main system utilising DVTel version 6.1 whilst the smaller system utilises DVTel 6.2. UOW intends to upgrade to version 6.3 and consolidate both systems into a single system in the short term. Contractors should check with UOW Project Officers on cameras specified for various projects until further advised that UOW has upgraded its software package and is subsequently able to update its selection of camera products. Fixed cameras should be compatible with version 6.1 and PTZ cameras should be compatible with version 6.2.

Since being acquired by FLIR Systems in December 2015, the availability of DVTel branded equipment is limited and is in the process of being transitioned to the new FLIR product line. The equipment identified in this section include those that are currently available as well as FLIR Systems equipment that is compatible with UOW's systems and is of equivalent or greater performance to that currently installed for UOW.

8.1 Cameras

A market review has been undertaken and identified fixed IP cameras that are suitable for installation. The specific models can be identified using a naming convention that has been designed to depict the key features of the equipment.

Table 5 below identifies the model naming convention used for the fixed IP cameras that were previously supplied under DVTel (now FLIR) and which include specific models deemed suitable for UOW:

	Fixed IP Camera Naming Convention & Features								
	Type	-	Series	Camera Resolution	Included Analytics	-	Lens Option	Environmental	IR Illuminator
Format	XX	-	XX	X	X	-	X	X	X
Content and Meaning	CF: Fixed	-	42: Quasar Series 52: IOI Series	1: HD 720p 2: HD 1080p 5: HD 1440p	1: Intelligent Multi-zone VMD and Tamper Detection 2: Advanced IOI analytics	-	0: Day / night	0: Indoor 1: Outdoor	N/A
	CM: Mini Dome Camera (pan / tilt)	-	31: Ariel II 42: Quasar 43: Quasar (low profile)			-	0: 3-9mm Auto Iris 1: 3-9mm Motorised Auto Focus	0: Indoor Tamper Resistant 1: Outdoor Vandal with heater/fan	I: 90 ° Illuminator

Table 5 – Naming convention for Fixed IP Cameras rebranded from DVTel to FLIR

Table 6 below identifies the model naming convention used for the PTZ IP cameras that were previously supplied under DVTel (now FLIR) and which include specific models deemed suitable for UOW:

	PTZ IP Camera Naming Convention & Features							
	Type	-	Series	Camera Resolution	Included Analytics	-	Lens Option	Environmental
Format	XX	-	XX	X	X	-	XX	X
Content and Meaning	CP: PTZ Camera	-	42: Quasar Series	2: HD 1080p	1: Intelligent Multi-zone VMD and Tamper Detection	-	20: Optical zoom 20x 30: Optical zoom 30x	0: Indoor Tamper Resistant 1: Outdoor IP66 Vandal with Heater/Fan

Table 6 – Naming convention for PTZ IP Cameras rebranded from DVTel to FLIR

Models in the FLIR IP series are being released and will progressively supersede the previous generation of models whilst providing increased resolution, analysis capabilities and additional functionality. This is likely to take place over the next three years.

8.1.1 Fixed IP Cameras

Table 7 below identifies the fixed IP cameras and housings that have been deemed suitable for installation:

Equipment Type & Performance				Equipment Deemed Suitable	
Device	Sensor	Lens	Power	Make	Model
Indoor					
Fixed colour day/night IP camera in box	HD 1080P, wide dynamic range	Auto iris	24 VAC ±10% or 802.3af PoE	FLIR Quasar	CF-4221-00(1)
	HD 1440P, wide dynamic range	Auto iris	24 VAC ±10% or 802.3af PoE	FLIR Quasar	CF-4251-00
Fixed colour day/night IP camera in low profile vandal-proof minidome (pan and tilt)	HD 1080P, wide dynamic range	Auto iris	802.3af PoE	FLIR Quasar	CM-4321-01
Fixed colour day/night IP camera in vandal-proof minidome (can pan and tilt) with motorised lens	HD 1080P, wide dynamic range	Auto iris	802.3af PoE	FLIR Ariel II	CM-3102-11
Fixed colour day/night IP camera in bullet enclosure with motorised lens	HD 1080P, wide dynamic range	Auto iris	24 VAC ±10% or 802.3af PoE	FLIR IP	N437VDL
Outdoor					
Fixed colour day/night IP camera in box with IOI analytics functions (e.g. loitering, stopped vehicle, camera tampering etc)	HD 720P, wide dynamic range	Auto iris	24 VAC ±10% or 802.3af PoE	FLIR IOI	CF-5212(1)
	HD 1080P, wide dynamic range	Auto iris	24 VAC ±10% or 802.3af PoE	FLIR IOI	CF-5222(1)
Fixed colour day/night IP camera in vandal-proof minidome with motorised lens	HD 1080P, wide dynamic range	Auto iris	24 VAC ±10% or 802.3af PoE	FLIR IP	N437VDL/P
Fixed colour day/night IP camera in box	HD 1080P, wide dynamic range	Auto iris	24 VAC ±10% or 802.3af PoE	FLIR Quasar	CF-4221-01(1)
	HD 1440P, wide dynamic range	Auto iris	24 VAC ±10% or 802.3af PoE	FLIR Quasar	CF-4251-01
Fixed colour day/night IP camera in vandal-proof minidome (can pan and tilt)	HD 1080P, wide dynamic range	Auto iris	24 VAC ±10% or 802.3af PoE	FLIR Quasar	CM-4221-01
	HD 1080P, wide dynamic range	Auto iris	802.3af PoE	FLIR Ariel II	CM-3102-01
Fixed colour day/night IP camera in vandal-proof minidome (can pan and tilt) with motorised lens (to be used where the camera is difficult to access)	HD 1080P, wide dynamic range	Auto iris	24 VAC ±10% or 802.3af PoE	FLIR Quasar	CM-4221-11
Housing(2)					
Indoor fixed mount bracket	N/A	N/A	N/A	FLIR	CF-X100-00
Pole mount for outdoor fixed box camera housing	N/A	N/A	N/A	FLIR	CF-X200-POLE
Outdoor fixed camera housing - heater / blower includes bracket mount	N/A	N/A	24 VAC ±10%	FLIR	CF-X200-01

Table 7 – Suitable fixed IP cameras and housings.

Note 1 – Lenses available for the CF-4221 and CF-5222 series of fixed IP cameras include auto-iris, varifocal lenses with focal ranges of 3.1 - 8mm (CF-L131-31), 8 - 50mm (CF-L131-08-50), 8 - 80mm (CF-L131-08) and 12.5 - 50mm (CF-L131-12). The lens shall be selected to suit the location and required coverage and be determined in consultation with UOW.
Note 2 - Housing type and size shall be selected to suit the camera and lens combination.

8.1.2 PTZ IP Cameras

The PTZ IP cameras listed in Table 8 below are deemed suitable for installation:

Equipment Type & Performance				Equipment Deemed Suitable	
Device	Sensor	Lens	Power	Make	Model
Pan, tilt, zoom colour day/night IP camera with indoor dome	HD 1080P, wide dynamic range	Auto iris Auto focus 20x zoom	24 VAC ±10% or 802.3at PoE	FLIR Quasar	CP-4221-20x (CP-4221-200)
Pan, tilt, zoom colour day/night IP camera with outdoor dome	HD 1080P, wide dynamic range	Auto iris Auto focus 20x zoom	24 VAC ±10% or 802.3at PoE	FLIR Quasar	CP-4221-20x (CP-4221-201)
Pan, tilt, zoom colour day/night IP camera with indoor / outdoor dome	HD 1080P, wide dynamic range	Auto iris Auto focus 30x zoom	24 VAC ±10% or 802.3at PoE	FLIR Quasar	CP-4221-301
	HD 1080P, wide dynamic range	Auto iris Auto focus 30x zoom	24 VAC ±10%	FLIR IP	DNZ30TL2RP
	HD 1080P, wide dynamic range	Auto iris Auto focus 30x zoom	24 VAC ±10% or 802.3at PoE	FLIR IP	N336ZD3/P

Table 8 – Suitable PTZ IP cameras

The proposed use of other types of fixed or PTZ cameras shall be referred to UOW and the final selection shall be approved by UOW Security Management.

8.2 CCTV Power Supplies

The use of Power over Ethernet (where supported by the network infrastructure) is preferred. The security contractor should consult with UOW's IMTS department as part of the design process with respect to the specific requirements, taking into consideration factors such as Ethernet cable type (e.g. Category 6), cable length (typically up to 100m), power sourcing equipment availability, PoE standard (IEEE 802.3af or IEEE 802.3at) etc.

Where external power supplies are used, the equipment shall meet the following minimum criteria:

- The power supplies will provide a 24VAC fused output via screw terminals
- Capacity should be 80% maximum load
- No plug packs shall be used
- Individually fused
- Each output circuit will have an Individual status LED indicator
- Mains input shall be fused
- The power supplies shall be CE and C-Tick approved
- Provision of mains power to PSU shall be the responsibility of the security contractor.

8.3 Video Management and Storage Software

8.3.1 General

The CCTV management software is DVTEL Latitude Network Video Management System (NVMS). The IP CCTV systems to be installed at UOW campuses shall connect to this system.

Device	Function	Model
LAT6-NT	Video management and storage software solution	DVTel Version 6
Server	Video management and storage	Windows Server 2003

Table 9 – Video Management & Storage Software

The naming of cameras added to an existing system must by consistent with the established convention, unless otherwise approved by UOW Security.

8.4 Communication & Switching Components

The communication of the IP CCTV system is provided by UOW IMTS, therefore the UOW IMTS department is responsible for supplying the hardware, network connections, and the maintenance of equipment for IP CCTV servers and software.

It is the contractor's responsibility to liaise with UOW IMTS for any network requirements, to provide UOW IMTS with time lines for installation of any additional network equipment and to identify the costs associated during the IP CCTV design stage at UOW. In addition, the contractor is to ensure the IP CCTV system design is compliant with the latest revision of the UOW Specification for Voice and Data.

9 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 IP closed circuit television system these costs shall 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

10 APPENDIX A – CONTROL STRATEGY DESIGN SPREADSHEET

Camera ID	Location	Primary Subject	Primary Purpose of Surveillance (Historical Analysis, Deterrence, Real-time Surveillance or Object Video Analysis)	Period of Surveillance	Lighting Source	Camera Features Require							Monitoring Features Required			Recording Features Required
						Pan Tilt Zoom	IR Sensitivity	IR Lamp	Thermal Sensitivity	Tamper proof enclosure	Weatherproof enclosure	PTZ Home Location	Activate Display on Alarm	Alarm ID	Include in Video Rotation	Frames per second required
C107	Food Court	ATM	Historical analysis	24/7	Food court lighting	☐	☑	☑	☐	☑	☐	N/A	☑	123	☑	25
						☐	☐	☐	☐	☐	☐		☐		☐	
						☐	☐	☐	☐	☐	☐		☐		☐	
						☐	☐	☐	☐	☐	☐		☐		☐	
						☐	☐	☐	☐	☐	☐		☐		☐	
						☐	☐	☐	☐	☐	☐		☐		☐	
						☐	☐	☐	☐	☐	☐		☐		☐	
						☐	☐	☐	☐	☐	☐		☐		☐	
						☐	☐	☐	☐	☐	☐		☐		☐	
						☐	☐	☐	☐	☐	☐		☐		☐	
						☐	☐	☐	☐	☐	☐		☐		☐	
						☐	☐	☐	☐	☐	☐		☐		☐	

Table A1 - Control Strategy Design Spreadsheet