Title	**Design electronic security access control systems**		
Level	**4**	**Credits**	**25**

Purpose	People credited with this unit standard are able to: – identify client's access control systems requirements; – select components for access control systems; – select access control peripheral devices; – prepare detailed access control system design plans; – install, commission, and hand over access control systems as designed; and – prepare a test and maintenance schedule for access control system installations.

Classification	Electronic Engineering > Electronic Security

Available grade	Achieved

Guidance Information

1 This unit standard has been developed for learning and assessment on-job.

2 Persons working or intending to work as a security officer or in related security employment may require a Security Guards Licence or, if an employee of a Security Guard Licence holder, a Certificate of Approval to be the Responsible Employee of a Security Guard. These licences are issued by the Registrar of Private Investigators and Security Guards.

3 References – Specific to Electronic Security Industry
New Zealand Security Association (Inc), *Code of Practice for Alarm Monitoring Centres*, 2007;
New Zealand Security Association (Inc), *Code of Practice for Closed Circuit Television Surveillance Systems*, 2006;
New Zealand Security Association (Inc), *Code of Practice for Electronic Access Control*, 2008;
New Zealand Security Association (Inc), *Code of Practice for Intruder Alarm Systems*, 2007;
NZS/AS 2201.1:2007, *Intruder alarm systems – Client's premises—Design, installation, commissioning and maintenance*;
NZS/AS 2201.2:1992, *Intruder alarm systems – Central stations*;
NZS/AS 2201.4:1990, *Intruder alarm systems – Wire-free systems installed in client's premises*;
NZS/AS 2201.5:2008, *Intruder alarm systems – Alarm transmission systems*;
NZS 4301.3:1993, *Intruder alarm systems – Detection devices for internal use*;
and all subsequent amendments and replacements.

References – General to Electronic Security Industry
Building Act 2004;
Electricity (Safety) Regulations 2010;
Electricity Regulations 1997;
Health and Safety in Employment Act 1992;
Health and Safety in Employment Regulations 1995;
Private Investigators and Security Guards Act 1974;
Privacy Act 1993;
AS/NZS 3000:2007, *Electrical installations (known as the Australian/New Zealand Wiring Rules)*;
NZS 4512:2003, *Fire detection and alarm systems in buildings*;
NZS 4514:2009, *Interconnected smoke alarms for houses*;
Telecommunications Act 2001;
Local territorial authority requirements;
and all subsequent amendments and replacements.

4 Guidelines for connection of intruder alarm systems to telephone lines are contained in *Access Standards Newsletters* issued periodically by Telecom NZ Ltd, available from www.telepermit.co.nz.

5 Range
- a Three separate access control systems, at least one of which will have a minimum of 24 controlled doors, and two will have a minimum of 12 controlled doors.
- b Each controlled door will include PC/software interface.

6 All activities and evidence presented for all outcomes and performance criteria in this unit standard must be in accordance with relevant legislation, policies, procedures, ethical codes and standards, and industry practice; and where appropriate, manufacturers' instructions, specifications, and data sheets.

Outcomes and performance criteria

Outcome 1

Identify client's access control systems requirements.

Performance criteria

1.1 The client's objectives and budget are identified.

1.2 A schematic block drawing is prepared to graphically represent the scope and location of the proposed access control system.

1.3 The block drawing is used to confirm with the client that all access control objectives have been identified.

1.4 Specification is reviewed and specific programming requirements are identified and documented.

Outcome 2

Select components for access control systems.

Performance criteria

2.1 System components are selected to meet all installation requirements, and are mutually compatible.

2.2 Interconnection methods are specified to integrate system components.

2.3 Power supply capacity and cabling is confirmed to support load as specified.

Outcome 3

Select access control peripheral devices.

Range may include – peripheral devices include but are not limited to – electric strikes, electric mortise locks, electromagnetic locks, V-Locks, power bolts, cable transfer hinges, door furniture, egress switches, point-to-point beam, vehicle detection loop, credential reader (key, card, tag), radio and infra-red transmitters, automatic door closer, vehicle barrier, request to exit device, emergency release device;
evidence of ten different devices across the three different installations is required.

Performance criteria

3.1 Devices are selected to meet all installation requirements with regard to the operating environment.

3.2 Device positions are selected to maximise system effectiveness and reliability.

Outcome 4

Prepare detailed access control system design plans.

Performance criteria

4.1 The locations of all system components are identified in the plans.

4.2 Unique references to all components and cabling are included in the plans.

4.3 The wiring schedule is included in the plans providing all details for requisition and installation of cable support systems and cables.

4.4 A parts list is included in the plans for requisition and installation of components and devices.

4.5 Detailed system programming documentation is developed.

4.6 The plans meet client's objectives and budget.

Outcome 5

Install, commission, and hand over access control systems as designed.

Performance criteria

5.1 Cabling systems are installed in accordance with design plans.

5.2 Selected components and devices are installed in accordance with design plans.

5.3 System is powered-up and tested for initial operation.

5.4 System is programmed to client's operational requirements and system specifications.

5.5 System is commissioned and handed over to client.

5.6 Equipment operation, warranty, and service options are communicated to the customer in accordance with the equipment documentation.

5.7 Handover documentation is completed in the agreed format, and in accordance with customer and enterprise requirements.

Outcome 6

Prepare a test and maintenance schedule for access control system installations.

Performance criteria

6.1 Functional tests to confirm system operation are specified in the schedule.

6.2 Frequency and details of subsequent maintenance testing are listed in the schedule.

6.3 A list of essential spare parts is specified in the schedule.

6.4 System updates are provided for in the schedule.

6.5 The frequency of future design reviews is specified in the schedule to confirm the continuing suitability of the system to the client.

Replacement information	This unit standard was replaced by unit standard 31599.

This unit standard is expiring. Assessment against the standard must take place by the last date for assessment set out below.

Status information and last date for assessment for superseded versions

Process	Version	Date	Last Date for Assessment
Registration	1	27 April 2000	31 December 2012
Revision	2	11 March 2004	31 December 2012
Review	3	18 March 2011	31 December 2021
Review	4	24 January 2019	31 December 2021

Consent and Moderation Requirements (CMR) reference	0003

This CMR can be accessed at http://www.nzqa.govt.nz/framework/search/index.do.