Title	**Demonstrate knowledge of integrated electronic security system design, commissioning, and fault finding**		
Level	**4**	**Credits**	**25**

Purpose	People credited with this unit standard are able to demonstrate knowledge of: – security risks in the electronic security industry; – electronic security intruder alarm system design and commissioning; – electronic security access control system design and commissioning; – electronic security CCTV system design and commissioning; – integrated electronic security power supply system design and commissioning; – integrated electronic security digital wireless system design and commissioning; and are able to – use systematic techniques to identify location and causes of faults in an integrated electronic security system.

Classification	Electronic Engineering > Electronic Security

Available grade	Achieved

Guidance Information

1 This unit standard has been developed for learning and assessment off-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 Definitions
CCTV – closed circuit television.
CIF – common interchange format.
Component – a part of a larger system.
DVR – digital video recorder.
Environmental may include sunlight, heat sources, halogen lights, pets, drafts, insects, rodents, weather, electrical interference, lightning, radio interference.
IP – internet protocol.
NVR – network video recorder.
PIR – passive infra-red.
POE – power over ethernet.
PTZ – pan tilt zoom.

Resolution – covers range from CIF to megapixel.
REX – request to exit.
Risk – the chance of something happening that will have an impact upon objectives, measured in terms of consequences and likelihood.
Safe working practices – work practices designed to prevent personal injuries and damage to equipment and plant. This includes practices relating to personal attire and use of safety clothing and equipment, use of machinery and tools, and handling of materials and waste.
Threats – things or actions that present risks to people, assets, or events, and which, if untreated, may result in harm, fear, disruption, loss, damage, compromise or destruction.

4 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;
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 Act 1992;
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*;
Local territorial authority requirements;
and all subsequent amendments and replacements.

5 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.

6 Range
An *integrated security system* must include at least three of – access control, intruder alarm, closed circuit television (CCTV), intercom.

7 Knowledge of simple electronic and radio theory only is required, sufficient to understand the theory of electronic security equipment operation.

8 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

Demonstrate knowledge of security risks in the electronic security industry.

Range evidence of three different risks is required.

Performance criteria

1.1 The relationships between risks, threats, and vulnerabilities are explained in terms of the electronic security industry.

1.2 Security risks are explained in terms of an electronic security installation.

1.3 Options to minimise risks for an electronic security installation are described.

Outcome 2

Demonstrate knowledge of electronic security intruder alarm system design and commissioning.

Performance criteria

2.1 Programme functions are explained in terms of intruder alarm functions, and described in terms of their suitability for given situations.

Range intruder alarm functions may include but are not limited to – points and/or zones, areas, partitioning, common areas, zone doubling, duress, user authorisation, late working, auto arming, stay mode, bypass, isolate, walk test, time zone, entry delay, exit delay, siren time;
evidence of five programme functions is required.

2.2 The main management functions of an intruder alarm system are explained.

Range management functions may include but are not limited to – user programming, alarm activity reporting, user activity reporting, system time programming, system status, system test, off-site monitoring;
evidence of three management functions is required.

2.3 Safety and local body regulations are explained in relation to noise level of audible sounders.

Range may include but are not limited to – decibel rating for internal sounders, duration of external sounders in residential areas; evidence of two is required.

2.4 Influences that may affect components performance are explained.

Range influences may include but are not limited to – environmental, radio and/or cell transmitters;
evidence of five is required.

2.5 Advantages and disadvantages of components for given environments are explained.

Range components may include but are not limited to the following – internal audible device, external audible device, communications devices, PIR detector, microwave detector, point-to-point beam, dual and quad technology detector, reed switches, seismic sensors, glass beak detectors, outdoor detector;
evidence of five components is required.

2.6 Electronic intruder alarm systems are designed to meet given outcomes.

Range includes but is not limited to – design specification, site plan, equipment schedule, installation plan, installation timeline, system programming, testing and commissioning, documentation, client training;
system programming – minimum of five areas that operate on a varying ‘24 hours a day, 7 days a week’ cycle;
evidence is required for one domestic site and one commercial or industrial site;
commercial or industrial site must include a minimum of 46 detector devices.

Outcome 3

Demonstrate knowledge of electronic security access control system design and commissioning.

Performance criteria

3.1 Installer programming functions are explained in terms of providing an operational system.

3.2 Access control system management functions are described.

Range management functions may include but are not limited to – card programming, alarm activity reporting, card user activity reports, temporary card issue, holiday time scheduling, lost card control, fire evacuation reporting, user grouping, authorisation levels, lift floor levels, global access, restricted access, two person rule, blocked card, expiry dates, time schedules;
evidence of ten is required.

3.3 Safety issues relating to means of egress are described.

Range safety issues include but are not limited to – fire alarm override, building code compliance, emergency evacuation, lift access control, emergency break glass, lock type selection, emergency key override.

3.4 Environmental influences that may affect component performance are explained.

Range includes but is not limited to – wind and pressure loading, building movement.

3.5 Advantages and disadvantages of components are explained for given environments.

Range components may include but not limited to – electric strikes, electric mortise locks, electromagnetic locks, cable transfer hinges, egress switches, point-to-point beam, vehicle detection loop, credential reader (key, card, tag), radio and infra-red transmitters, mechanical door closer, automatic door closer, auto door, v-lock, turnstiles, vehicle barrier arm; vehicle arresting devices, REX, fire release, emergency door release;
one advantage and one disadvantage for each of ten components are required.

3.6 Access control systems are designed to meet given outcomes.

Range includes but not limited to – design specification, site plan, equipment schedule, cable schedule, power supply requirements, installation plan, installation timeline, system programming, testing and commissioning, documentation, client training;
evidence is required for two installations each with a minimum of twelve controlled doors and /or entry /exit points. Each installation must have a minimum of six user access requirements.

Outcome 4

Demonstrate knowledge of electronic security CCTV system design and commissioning.

Performance criteria

4.1 CCTV system functions are explained and their suitability for given situations are described.

Range may include but is not limited to – frames per second, images per second, motion detection, privacy zone, CIF, pixel, resolution, lines, image compression method, text insertion, archive, sequence time, multiplexer screen split, lenses, alarm triggers, matrix switching, event programming, image sensor; evidence of ten functions is required.

4.2 Component performance, interference, and lighting situations are described.

Range may include but is not limited to – illumination levels, shadows, direct sunlight, glare, rapid light fluctuation, scene contrast, colour rendering, infra red, fluorescent, high and low pressure sodium, incandescent, large vehicles, trees; evidence of five is required.

4.3 Advantages and disadvantages of different CCTV technologies are described.

Range dome cameras, full body cameras, analogue and digital cameras, infrared imaging cameras, fixed and auto iris lenses, DVR, NVR, matrix switch, virtual matrix, PTZ, megapixel.

4.4 CCTV system is designed to meet given outcomes.

Range CCTV system may include but is not limited to – cameras, lenses, housings, brackets, video monitors, power supply, matrix switchers, IP camera, network switch, system software, mega pixel cameras, PTZ, cable, DVR, NVR, lighting, access control interface;
system design documentation may include but is not limited to – design specification, site plan, equipment schedule, installation timeline, testing and commissioning, client training schedule; evidence is required for one commercial installation and one industrial installation each with a minimum of 12 cameras.

Outcome 5

Demonstrate knowledge of integrated electronic security power supply system design and commissioning.

Performance criteria

5.1 Advantages and disadvantages of power supply types are described.

Range power supply types may include but not limited to – linear, switchmode, POE;
evidence of two advantages and two disadvantages for each is required.

5.2 Management functions of a power supply are described.

Range mains fail, low battery, battery charging.

5.3 Advantages and disadvantages of centralised and distributed power supply systems are explained.

Range includes but is not limited to – fire alarm override, monitoring functions, mains reticulation, voltage drop.

5.4 Characteristics of three different backup battery technologies are described.

5.5 Environmental considerations that may affect component performance are explained.

Range includes but is not limited to – heat, corrosion, humidity, airflow.

5.6 Power supply system is designed to meet given outcomes for an integrated access control system.

Range access control system – sixteen access controlled doors, eight hours of standby power, commissioning documentation;
CCTV system – sixteen cameras;
power supply – to run the system and to recharge the batteries to more than 90% of battery capacity within 24hrs.

Outcome 6

Demonstrate knowledge of integrated electronic security digital wireless system design and commissioning.

Performance criteria

6.1 Digital microwave system design is explained as applied to an electronic security system.

Range Ethernet protocol, line of sight, transmitter range, interference, spectrum analysis, bit error rate, radio spectrum, environment, mounting considerations.

6.2 Safety issues relating to digital wireless systems are described.

Range microwave radiation, safe working practises.

6.3 A digital wireless radio system is designed to meet a given outcome.

Range includes but is not limited to – design specification, site plan, equipment schedule, installation plan, installation timeline, system programming, testing and commissioning, documentation, client training;
evidence of one system is required.

Outcome 7

Demonstrate and apply knowledge of systematic techniques to identify location and causes of faults in an integrated electronic security system.

Performance criteria

7.1 Techniques to diagnose faults in electronic security equipment are described.

Range techniques include but are not limited to – observation, simulation, measurement, function loss, comparison, frequency of occurrence, previous fault data, manufacturers' documentation and diagnostic data, built-in diagnostics.

7.2 Safety precautions to be observed during fault diagnoses in relation to personnel and equipment are identified and observed.

7.3 Systematic diagnostic techniques, fault symptom analysis, and test equipment are used to locate and identify the cause of faults in electronic security equipment.

Range diagnostic techniques may include but are not limited to – observation; simulation; measurement; function loss; comparison; frequency of occurrence; previous fault data; manufacturers' diagrams, servicing information, and diagnostic data; built-in diagnostics;
evidence of ten different faults on different electronic security equipment is required.

7.4 The integrity of the equipment is maintained and uncompromised during the diagnostic process.

7.5 The logic of the diagnostic techniques used to find each fault is explained.

Replacement information	This unit standard was replaced by unit standard 31598.

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	18 March 2011	31 December 2021
Review	2	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.