ElectraNet

Substation Physical Security

Document Number: 1-11-FR-02

VERSION 1.0 June 2018

This functional requirements document is in line with the organisation's 1-11-ACS-03 Substation Physical Security Asset Class Strategy

Contents

1. Definitions

In this document the following words and expressions will have the following meanings:

Item	Meaning
ac	Alternating current
authorised person	A person with technical knowledge or sufficient experience who has been approved, or has the delegated authority to act on behalf of the organisation, to perform the duty concerned.
AS	Australian Standard, as publication by Standards Australia (Standards Association of Australia).
CCTV	Closed Circuit Television
Contractor	A contractor engaged by ElectraNet or a Customer (including a third party IUSA provider engaged by a Customer or any contractor engaged by such third party IUSA provider) to perform any design, construction or related services in relation to assets or infrastructure which are connected, or to be connected, to ElectraNet's transmission network
CPTED	Crime prevention through environmental design. Is the concept that good design and effective use of the physical environment can lead to a reduction in the fear and incidence of crime against people or property. ElectraNet requires substation design to embrace the principles and techniques of CPTED and actively apply the discipline across all facets of substation design.
Customer	A party who wants to establish or modify a connection to ElectraNet's transmission network but does not include a third party IUSA provider
defence in depth	The defence in depth principle is the integration of protective security into a tiered security system. Layers of protection secure an asset in the centre of the layers from an attack by an external source. Defence in depth provides a number of barriers to deter, detect, delay and respond to security related incidences. Barriers may include geography or topography surrounding the premises (water, rough terrain, gullies), perimeter (fences, gates detection systems, security lighting), space between perimeter, building, equipment (sterile zones), building fabric and equipment support structures (strength of walls, roofs, floors, windows, doors, trapdoors, and enhancements such as security patrols, static guards, intruder alarms, security lighting), space inside buildings (foyers, corridors, intruder detection, static guards), secure rooms (doors, walls, ceilings, floors, intruder detection equipment, locks, hardware, structural strength, insulated equipment and covers).
ENA	Energy Network Association
EPR	Earth Potential Rise. Voltage between an earthing system and a remote earth.
HDG	Hot Dip Galvanized

Item	Meaning
HV or high voltage	Nominal voltage exceeding 1000 volts alternating current or exceeding 1500 volts direct current.
Natural Surveillance	A design concept directed primarily to facilitate observation of the site by employees, neighbours and the general public so that the risk of detection is reinforced and maximises the opportunities for public safety. This principle is promoted by features that maximise visibility of people, parking areas and yard spaces and building entrances (including at night with adequate night-time lighting). Some common measures include: Clear sightlines, particularly along perimeter fences, around buildings and structure, and in between transmission infrastructure, Elimination of hidden or blind spaces, alcoves or voids where an assailant may conceal themselves, Passive surveillance of fence lines from the street scape and surrounding areas.
primary control measures	These include reducing the risk by using insulated / covered conductors, limiting access to exposed conductors, physical barriers such as fences or buildings, strengthened doors and door frames, using appropriate key, locking and control access measures and inspecting and maintaining the primary control measures.
procedural control measures	Procedural control measures support the primary and secondary control measures to ensure the ongoing effectiveness of these control measures and the security processes. Procedural control measures are not limited to security management, security policies and procedures, security risk assessment, control measure inspection testing and audit.
property fencing	Fencing designed to delineate land holder property ownership boundaries.
PVC	Polyvinyl chloride.
risk management	The management of risk in accordance with AS/NZS ISO 31000 Risk management - Principles and guidelines.
SCADA	Supervisory Control And Data Acquisition.
secondary control measures	These include intruder alarms systems, perimeter detection and deterrent systems, communication of alarms, CCTV, security lighting, event monitoring and reporting, response, regular security patrols, education awareness and training, graffiti clean-up, signage, site appearance and on-site storage.
security system	Consists of security components such as building, perimeter and yard physical security, access control and alarm system, closed circuit television, electronic key system, auxiliary systems and coordination.
SP	Security Purpose.
Standard Drawing	A drawing developed by ElectraNet as a complete design to be used for construction. Standard Drawings are not intended to be revised or renumbered.

Item	Meaning
substation perimeter fencing	These are fences that enclose the actual substation and are treated as security fences.
target hardening	Target hardening is the concept of opportunity reduction. Most target hardening measures are designed as a visible signal to would be offenders that the site is well protected, attempts to force entry will be time consuming and that there is a greater opportunity that apprehension will occur.
Template Drawing	A drawing developed by ElectraNet as the basis for design. Template Drawings are intended to be revised and renumbered as required to complete the design.
territorial reinforcement	The physical design should create and extend a sphere of influence to reinforce a sense of ownership. This aims to develop a territorial 'control' of a space, discouraging potential offenders from attempting to breach the secure perimeter. This reinforcement is supported with features that define property lines and clearly distinguish private spaces from public spaces, through the use of landscape plantings, pavement/pathway design and CPTED perimeter lines. Some common measures include: Clearly defining and designating areas with respect to their intended use. Use of common design elements, such as lighting, signage, paving etc. Clear borders of controlled/restricted spaces. People accessing a substation site should clearly recognise it as ElectraNet ‘space’ or Contractor 'space' (as applicable). Effective use of signage, for example, CCTV in use, restricted access, ElectraNet property notices or Contractor property notices (as applicable), etc.
third party IUSA	Has the same meaning as defined in the National Electricity Rules

2. Purpose

The purpose of this document is to describe the functional requirements for Substation Physical Security measures and their integration into a substation.

3. Scope

This document states the functional requirements with regard to Substation Physical Security measures, covering design, construction, operational and maintenance as well as the integration into a high voltage substation.

4. Referenced Documents

The table below lists applicable legislations, standards, referenced documents:

Legislation	
SAEA	Electricity Act 1996 (SA)
SAER	South Australia Electricity (General) Regulations 2012 (SA) under the SAEA
NER	National Electricity Rules
ETC	Electricity Transmission Code TC/08
SAA HB59:1994	Ergonomics - The human factor A practical approach to work systems design
Standards	
AS 1289:various	Methods of Testing Soils for Engineering Purposes
AS 1379:2007	Specification and supply of Concrete
AS 1725.1:2010	Chain link fabric fencing - Security fences and gates - General requirements
AS/NZS 2053.2:2001 (R2016)	Conduits and fittings for electrical installations - Rigid plain conduits and fittings of insulating material
AS 2342:1992 (R2013)	Development, testing and implementation of information and safety symbols and symbolic signs
AS 2423:2002	Coated steel wire fencing products for terrestrial, aquatic and general use
AS/NZS 3000:2007	Electrical Installations (known as the Australian/New Zealand Wiring Rules)
AS/NZS 3679.1:2016	Structural steel - Part 1: Hot-rolled bars and sections
AS 4145.1:2008	Locksets Part 1: Glossary of Terms
AS 4506:2005	Metal finishing - Thermoset powder coatings
AS/NZS 4680 :2006	Hot–dip galvanized (zinc) coatings on fabricated ferrous articles
AS 5577:2013	Electricity network safety management systems
AS/NZS ISO 31000:2009	Risk management - Principles and guidelines
BS1722 - 12:2016	Fences part 12: Steel palisade fences – manufacturing and installation - specification
ENA DOC 015-2006	National guidelines for prevention of unauthorised access to electricity infrastructure
ElectraNet's Documentation	
1-11-FR-01	Substation Earthing

1-11-FR-12	Substation Signage
1-11-ADM-12	Substation Signage
1-11-FR-13	Substation Electromagnetic Coordination

5. Physical Security

5.1 Physical Security Functional

5.1.1 Definitions and Requirements

5.1.1.1 The site specific documentation must define which type of fence is required, as well as the number and type of access gates on a per project basis. This will cover the number of vehicle access gates, whether they will be manually or electrically operated as well as the requirement for personnel access gates.

5.1.1.2 The design for the (perimeter) security fencing for each site must consider the following:

a) Land ownership boundaries;

b) Ensuring appropriate HV Clearances are maintained;

c) Underground cables and services locations;

d) Property or boundary fence requirements;

e) Access to garden areas (weed spraying), towers, etc.;

f) Access around the perimeter for patrols and maintenance (allow a minimum of 5m for this function);

g) Terrain;

h) Storm-water run-off from the substation site, including swales and detention ponds;

i) Use of storm-water drainage trenches for vehicle diversion;

j) Storm water movements created by concrete strips;

k) The installation of perimeter security (Consider future requirements. Allow a minimum of 5m for perimeter security installation);

l) Vegetation issues;

m) Retaining walls;

n) Adjacent buildings;

o) Adjacent fencing and isolation panel requirements;

p) Gate requirements and positioning;

q) Entry roads and their configuration to prevent ram raiding;

r) Climb points created by stobie poles etc.;

s) Security during installation (e.g. temporary fencing location);

t) The recommendations of any ‘Site Specific Earth Study’;

u) Hazard identification and mitigation; and

v) Safety In Design principles.

5.1.1.3 The security system must be safe, simple, minimise ongoing operation and maintenance costs with a capital cost proportionate to the risks involved.

5.1.1.4 Physical security controls must be fit for their intended purpose as defined by the functional requirements.

5.1.1.5 The security system must incorporate CPTED principles including natural surveillance and territorial reinforcement.

5.1.1.6 The security system must utilise CPTED as a design strategy.

5.1.1.7 Target hardening measures must be incorporated into the design.

5.1.1.8 Defence in depth principles must be utilised in the security system providing deterrence, detection, delay and response to security related incidences.

5.1.1.9 Security principles must be aligned with the current Security Risk Management Body of Knowledge which includes the principles of Defence in Depth and CPTED. Each layer in the Defence in Depth strategy must also employ the principles of:

a) Deter (Deter the intruder from entry to that layer);

b) Detect (Detect them as soon as they commence entry to that layer);

c) Delay (Delay their entry for as long as possible to that layer); and

d) Deploy (Deploy your response force, Police, Security Patrol, callout staff at the first layer of detection).

5.1.1.10 Total delay time for all layers must exceed the deployment response time from the first layer of detection.

5.1.1.11 Security principles must be aligned with the ENA Document, “National guidelines for prevention of unauthorised access to Electricity Infrastructure” ENA DOC 015-2006.

5.1.1.12 All substations sites must be laid out in a manner that cater for the construction of a property boundary fence and a substation security fence. For metropolitan areas it is not acceptable to have a substation security fence on the property boundary.

5.1.1.13 The minimum separation between property boundary and security fences must be 5 metres.

5.1.1.14 For metropolitan areas the minimum requirement for the property boundary fence is to install a medium security chainmesh fence as defined in this document. All access gates must have locking systems consistent with this document.

5.1.1.15 For rural areas the minimum requirement for the property boundary fence is to establish a post and wire stock fence. There is no requirement to have locks on the access gates however this may change depending on requirements of neighbouring property owners.

5.1.1.16 All substations sites must be designated as needing either medium or high security perimeter fencing. Breaching of a high security fence designs must take more effort than for a medium security design.

5.1.1.17 Chainmesh fencing, complying with the requirements of ElectraNet's Standard Drawings and AS 1725, must be used at sites requiring medium security fencing.

5.1.1.18 The Type 258 Weldmesh High Security Fence System, complying with the requirements of ElectraNet's Standard Drawings, must be used at sites requiring high security fencing.

5.1.1.19 The Weldmesh fences designs must comply with the relevant parts of BS1722, part 12, applicable to SP fencing. This standard defines the minimum requirements to be met for High Security Sites. Where this document is silent on an issue dealing with high security fencing, then BS1722 part 12 will apply.

5.1.1.20 Gates must provide the same level of security as provided by the fence and must be constructed using the same types of material as the fence.

5.1.1.21 The security system must provide a full spectrum of appropriate and benchmarked security controls to protect the general public, ElectraNet employees, contractors, assets at site and the reputation of ElectraNet.

5.1.1.22 When capacitor banks or other items of plant are installed involving air cored reactors and safety clearances to ground will not be met, then these items must be installed inside a compound consisting of a chainmesh and an interlocked personnel access gate. If necessary isolation panels must be installed to ensure that circulating currents are minimised.

5.1.2 Safety Requirements

5.1.2.1 The issue of keys and access control must be limited to authorised persons.

5.1.2.2 Signs used must be appropriate to the site and not contribute to any misunderstanding in relation to the hazards that may exist at the site.

5.1.2.3 Signs must comply with AS 1319, AS 2342 and AS/NZS 3000.

5.1.2.4 Signs must be assessed for appropriateness and may be a combination of words and symbols.

5.1.2.5 Farmers' fences or other types of fences owned by third parties, as well as ElectraNet owned property fences, must not connect directly to the security fencing. Isolation panels must be used in as many locations as necessary to reduce the transfer of unsafe potentials (voltages) to third party assets.

5.1.2.6 Isolation Panels must be installed where:

a) A change of earthing system exists along a security fence;

b) An abutting fence exists; and

c) A substation earthing system design requires this for EPR reductions.

5.1.2.7 Where isolation panels are used, they must have a minimum width of 3 metres.

5.1.2.8 Property boundary fence type must take into account:

a) Proximity to population, especially children;

b) Presence of containment and storage ponds; and

c) Requirements for perimeter security.

5.1.2.9 Signs on electrical infrastructure are required to warn of the hazard, deter access or other unwanted activity, and provide contact details to the public, and meet legal obligations arising from duty of care to the public and staff.

5.1.2.10 Where temporary fencing is required to maintain the security of the site then it must be designed and installed such that it meets the minimum requirements of the fence that it is interfacing with.

5.1.2.11 Locking and unlocking of the gate must be able to occur from either side of the closed gate. ElectraNet may vary this depending on site requirements.

5.1.2.12 Fence climb points are to be minimised through design.

5.1.2.13 The security fence must provide a maximum through visibility.

5.1.2.14 Hinges must be designed so that gates in all types of fence cannot be lifted off of the hinge and any gate removal must be done with the aid of tools.

5.1.2.15 A substation must have a maximum of one electrically operated vehicle access gate.

5.1.2.16 Where electrically operated access gates are to be used, the fence design must incorporate a personnel gate ‘adjacent to’ (not within) the vehicle gate.

5.1.2.17 For electrically operated gates, the operator control key switch of the electric vehicle access gate must be located on the far side of the adjacent personnel gate to prevent an operator from standing in the path of the closing gate.

5.1.2.18 For electrically operated gates the locking bar containing the padlock must slide open and closed and must not be fixed to prevent “spearing” of a person or vehicle in the path of the closing gate.

5.1.2.19 The electrically operated vehicle access gate design must incorporate visual and audible warning devices that the gate is about to open or close.

5.1.2.20 Signs are to be manufactured and installed such that they are conspicuous, legible, indelible and fitted securely.

5.1.2.21 The earthing of fences and gates must be in accordance with the requirements of the main substation earthing system design.

5.1.2.22 Gates must be designed such that they open inwards into the substation, and be provided with facilities that prevent the gates from opening outwards. If the site topography requires that the gates open outward, then the substation earth grid will need to be extended in a manner to ensure personnel safety when opening and closing the gates.

5.1.3 Design Requirements General

5.1.3.1 Risks associated with the introduction of new technology are to be minimised.

5.1.3.2 A holistic approach to security must be undertaken to existing and potential future vulnerabilities in the substation environment.

5.1.3.3 As a first layer of security, the security system must deter or displace criminal activity. First layer security involves a physical barrier such as the perimeter fence and signage.

5.1.3.4 In the event that an offender is not deterred, systems must detect the breach. The breach must be detected early and involves detection technology or active surveillance.

5.1.3.5 The security system must delay the offender from the intended target or purpose of theft or damage. The effectiveness of the defence strategy is directly proportional to the delay factors. It can be achieved by installing multiple layers of security. Inner fences surrounding the target, physically secured outbuildings and adequately secured building and equipment form part of the delay strategy. The total delay time in all layers in the system must exceed the response time of the deployed person from the first detection.

5.1.3.6 Site criticality, location and environmental factors will determine the holistic approach to the site security program.

5.1.3.7 Control measures must be taken to minimise unauthorised access and associated consequences which include warning signs, security lighting, security fencing, locking devices, barriers, sterile zone electronic detection and warning devices.

5.1.3.8 The three levels of control measures in ENA 015 must be utilised in minimising the risk of contact with electricity for unauthorised access to substations. The three levels are defined as primary control measures, secondary control measures and procedural control measures. The combination of these measures ensures a defence in depth approach is adopted in relation to the prevention of unauthorised access to electrical assets. Primary control measures provide physical protection and therefore provide a greater level of protection than secondary or procedural control measures.

5.1.3.9 Primary control measures, secondary control measures and procedural control measures must be reviewed on a regular basis or as required and continually improved.

5.1.3.10 The security system must utilise a combination of primary control measures, secondary control measures and procedural control measures to prevent unauthorised access.

5.1.3.11 A User (trained and authorised person to enter substations) must become unauthorised in the event of lost access accreditation (including failing to complete the required transmission asset access training within the required time frames).

5.1.3.12 The number of physical access controls for ElectraNet sites must be kept to a minimum to reduce the risk of loss, damage, complexity, and errors in the physical access controls.

5.1.3.13 The requirement for auxiliary and support equipment must either not be required or kept to a minimum.

5.1.3.14 The security system must be ElectraNet specific and must not be able to be duplicated by any third party.

5.1.3.15 Security measures for buildings and refurbishments must be considered early during the design and concept phases.

5.1.3.16 In accordance with AS 2067, AS 62271.201, AS/NZS 61439.1, AS 60529 and AS 62271.200 access to electrical equipment within substations must be restricted by methods such as full insulation, barrier, enclosure, safety section clearance and access by authorised personnel.

5.1.3.17 Locks, keys and security credentials must be limited to authorised persons.

5.1.3.18 The security system must be configurable to enable all alarms to be disabled on site from the main entry point, or via ElectraNet's SCADA system or via the proprietary management system.

5.1.3.19 An effective means must be provided to limit access to authorised personnel only.

5.1.3.20 The security system must facilitate unrestrained exit in the case of an emergency. This must be provided using pushbutton to activate an electric mortice lock or equivalent suitable device on the personnel gate adjacent to the electrically operated vehicle gate and connected to the security system with appropriate alarms.

5.1.3.21 Where possible clear lines of sight must be provided such that the substation is visible from the streetscape.

5.1.3.22 SCADA interface must be provided to the master security cubicle.

5.1.3.23 The access control system must limit entry to a substation to people with authorisation and a need to enter.

5.1.3.24 The security system must impede unauthorised or accidental access into a substation.

5.1.3.25 The security system must permit unimpeded egress from any building and from within the substation.

5.1.3.26 Access control hardware must be configurable for fail-secure operation from the insecure side and fail-safe from the secure side.

5.1.3.27 The design must remove the incentive for gaining access to site by limiting the amount of copper that can easily be removed.

5.1.3.28 The design must increase the physical barriers at the site to make entry to the site more difficult.

5.1.3.29 The design must increase the likelihood of detection of unauthorised access.

5.1.3.30 The Security system must be interface-able with motion detector sensors within the substation and permit verification through internal CCTV.

5.1.4 Design Requirements – Fences and Gates

5.1.4.1 All fences and gates must be designed for a minimum service life of 30 years.

5.1.4.2 Each switching station (substation without transformers) requires a minimum of one set of vehicle access gates and a pedestrian access gate as part of the perimeter fencing.

5.1.4.3 Each substation, where transformers are present, must have a minimum of two sets of vehicle access gates and a pedestrian access gate adjacent to the main vehicle access gate as part of the perimeter fencing.

5.1.4.4 A fire risk assessment, to be carried out for each site, must be used to determine the placement of all access gates.

5.1.4.5 Where a substation containing transformers is deemed to need high security perimeter fencing, one of the sets of vehicle access gates must be electrically operable.

5.1.4.6 The electrically operable vehicle access gate must not introduce any climb points.

5.1.4.7 Padlocking of the electrically operated vehicle access gate remains a requirement. ElectraNet may vary this depending on site specific requirements.

5.1.4.8 The property fence must delineate the block of land owned by ElectraNet.

5.1.4.9 The requirements of the property fence are developed as part of the Development Approval process and considers vegetation and topography requirements to provide a buffer between the substation and surrounding area. The development of this buffer must take into account the principles of CPTED which is a part of the overall Security Risk Management Principles and body of knowledge.

5.1.4.10 The perimeter fence must minimise the number of vehicular and pedestrian gates and achieve a physical barrier that surrounds the entire site.

5.1.4.11 With reference to AS 1725 the chain mesh fence design is to be based on a Type 2 – Pipe rail security fence, Type 2-B-R/B-T. i.e. bottom rail only, no top rail and barbed top.

5.1.4.12 For chainmesh fence designs all posts and pipes used for fencing must comply with the Class 1 requirements of AS 1725.

5.1.4.13 For chainmesh fence designs when bracing panels (or strainer assemblies) are used, all bracing must use diagonal brace stays set into concrete footings. All brace stays must be on the longitudinal axis of the fence

5.1.4.14 All galvanising must be to code W10Z/HG (heavy galvanised) as a minimum for chainmesh fencing.

5.1.4.15 Where Weldmesh fencing is required, all nuts, bolts and washers must meet the requirements of BS1722 part 12 regarding fasteners.

5.1.4.16 Where Weldmesh fencing is required, the sheet design must use Weldmesh Type 258 anti-climb/cut; high security fence sheeting of fixed aperture (3"x0.5").

5.1.4.17 The Weldmesh fencing must be made from materials like Carbon steel or Stainless Steel (Type 304 or SS-316).

5.1.4.18 The Weldmesh fencing must be of welded construction supplied in sheets, rolls or panels cut to size and easy to connect to the substation earthing system.

5.1.4.19 The Weldmesh fencing must be provided with the choice of Galvanized, Green PVC or Black PVC powder-coated finishes.

5.1.4.20 Anti-Climbs are to be used where buildings form part of the boundary fence. Site specific solutions will be required.

5.1.4.21 In some situations items will exist adjacent to fences that can be used as climb points, e.g. Stobie Poles. In these circumstances anti-climbs are to be fitted.

5.1.4.22 Anti-climbing barriers and tamper evident barriers must resist covert entry.

5.1.4.23 A 300 mm tall reinforced concrete strip, with a burial depth of 200 mm must be installed longitudinally under the entire length perimeter fence in order to prevent entry by burrowing animals and to deter people from digging under the fence. Where sandy soils are encountered the size and depth of this strip may need to be increased.

5.1.4.24 Where chainmesh fencing is used, the gap between the top of the concrete strip and the underside of the bottom fence rail must not exceed 50 mm.

5.1.4.25 Building materials and surfaces must be vandal resistant and facilitate timely repair.

5.1.4.26 Design of gates must provide a similar level of security as the fence. Locking devices and gateposts must not aid scaling of the gate or fence.

5.1.4.27 Vehicle access gates must be hinged or tracked / rolling according to site conditions and the expected frequency of operation.

5.1.4.28 Weldmesh fence installations utilising cantilevered or rolling gates must be capable of electrical operation.

5.1.4.29 The ‘commercial’ standard gate operator mechanism manufactured by “Gate Drive Systems” is suitable for the gate type and dimensions installed are to be utilised.

5.1.4.30 An electrical interlock must be designed that will prevent the gate drive system from electrically operating while the gate padlock remains in place. This operation will normally be provided by the use of a proximity sensor adjacent to the padlock and wired into the gate drive supply. Positioning of the proximity sensor must be such that only short shank padlocks can be used. Long shank padlocks must not be used.

5.1.4.31 230V power must be made available to the gate from the substation essential power and light distribution board.

5.1.4.32 The electric vehicle access gate system must include an engraved stainless steel lock front that has the ‘open’ and ‘close’ key switch directions the same as the gate ‘open’ and ‘close’ direction of travel.

5.1.4.33 Any change to the electrically operated gate design must be approved by ElectraNet with a documented risk assessment for its ‘security’ and ‘operating’ functions.

5.1.4.34 The gate operator must be of the following type: Model – ‘GDS 630E Li Pro’ with the following requirements.

a) Cast iron industrial grade gearbox;

b) 750W 3 phase induction motor;

c) ‘Prostar’ Inverter with limit positioning control;

d) 100% duty cycle;

e) 630mm/sec opening speed with ramp up and ramp down control;

f) Proximity lock reader with isolation output;

g) ‘Dead man’ control with SAP/ElectraNet lock system;

h) Strobe/buzzer lock release indicator;

i) HDG chassis;

j) Grade 316 Stainless steel cover with manual door handle release;

k) Back up battery system to prevent loss of settings during power outages or maintenance; and

l) Ability to switch to manual control on loss of power or gate drive failure.

5.1.4.35 Electric gate vehicle access gates audible and visual warning devices must be activated upon removal of the padlock securing the vehicle access gate, and only stop after the padlock has been reapplied after the gate has been closed.

5.1.4.36 Substation entry points must be appropriately secured.

5.1.4.37 Fence and gate climb points are to be minimised through design.

5.1.4.38 The security fence must provide a maximum through visibility.

5.1.4.39 Hinges must be designed so that gates in chainmesh fences cannot be lifted off of the hinge without the use of tools.

5.1.4.40 Hinges must be designed so that gates in Weldmesh fences cannot be lifted off of the hinge without the use of tools.

5.1.5 Requirements for Security Fence Locking Systems

5.1.5.1 Two types of locking systems are in use throughout the ElectraNet owned substations. All substations must utilise the CyberKey lock and key system manufactured by Videx. Some substations still use the more traditional mechanical lock and key systems but will be changed over to CyberKey in the future.

5.1.5.2 All new substations must use the CyberKey lock and key system, where the same locking system is to be used for all gates forming part of the substation security fence as well as for all entry/exit doors for buildings located within the substation and critical field cubicles where used.

5.1.5.3 All remotely located telecommunications buildings, ie for telecommunications sites located outside substations, must use the CyberKey lock and key system.

5.1.5.4 The detailed functional requirements for the CyberKey lock and key system are covered in document 1-11-FR-03.

5.1.5.5 The CyberLock system also provides padlocks that are a direct replacement for a conventional padlock. Wherever a padlock is used the shackle on it must be kept as short as possible unless specifically approved by ElectraNet. A 25mm shackle must be used for all applications. Equipment design must take this into account at all times. Longer shackles must only be used with the express permission of ElectraNet.

5.1.5.6 As with all devices in the system, cylinders and padlocks must be programmed into the CyberAuditWeb database prior to being used. All locks must be procured by ElectraNet and programmed before being issued to the Contractor or a third party IUSA provider for installation by suitably qualified tradespeople.

5.1.5.7 Locks and padlocks are all programmed for installation in a specific location. There must be no moving of padlocks from the designated location to another location as this will destroy the ability to control access in the case of an exclusion zone for example. The padlock must have a lanyard fitted that will secure the padlock to the nominated location and prevent relocation of the lock.

5.1.5.8 Where weldmesh fencing is to be installed, all gates must have lock boxes fitted to ensure that bolt cutters cannot be used, from either inside or outside the substation to cut the padlock shackle. The lock boxes must be manufactured and positioned such that only the body of a padlock will protrude beyond the enclosure. No part of the padlock shackle must protrude beyond the enclosure on either side of the box. Sufficient room must be allowed inside the lock box to provide room for the keys and lock to be accessed from either side of the gate.

5.1.6 Design Requirements Capacitor Bank / Air Cored Reactor Bank Compounds

5.1.6.1 The safety fencing around these compounds must be designed to meet the requirements of a chainmesh perimeter fence which only has a single personnel access gate, or as otherwise agreed with ElectraNet on a site specific basis.

5.1.6.2 The placement of the fence must be such that a person standing outside the fence must not experience electric and magnetic fields exceeding the occupational levels as defined in document 1-11-FR-13 under all operating conditions which includes power system faults within the compound.

5.1.6.3 The placement of the fence must ensure that the requirement minimum magnetic clearances to earthed structures as specified by the equipment manufacturer are met.

5.1.6.4 The design of the earthing system for the compound fencing must minimise or eliminate the presence of circulating currents.

5.1.6.5 The personnel access gate must be fitted with a safety interlocking system to ensure that entry cannot be gained until the equipment within has been de-energised earthed correctly via the appropriate switchgear.

5.1.6.6 The interlocking system must prevent re-energisation of the plant within the compound until the personnel access gate has been securely locked after the work has been completed.

5.1.6.7 The preferred method for interlocking will be via the use of a Castel key system

5.1.6.8 There is no requirement for a concrete strip to be installed under the fence for this type of application.

5.1.6.9 There is no requirement to install vehicle access gates for this type of application.

5.1.7 Constructability Requirements

5.1.7.1 For Brownfield substations where an existing fence is to be replaced, a temporary security fencing may need to be installed during the removal of the existing fence and erection of the new security fence. Security of the substation from unauthorised access must be maintained at all times. Temporary fencing must provide the same level of security as the currently installed fence.

5.1.7.2 Temporary fence earthing is required to the standard of the original fence. Substation portable earth leads or equivalent fault rated leads may be used for this purpose.

5.1.8 Operability Requirements

5.1.8.1 All signage must comply with the applicable requirements of 1-11-FR-12, 1-11-ADM-12 and the associated Standard Drawings and Template Drawings with respect to security systems and fencing.

5.1.8.2 Enclosure locks, keys and security keys must be limited to authorised persons.

5.1.8.3 Property fences must provide for a minimum of 5 m distance with no obstructions, from the substation security fence to allow for vehicles to traverse around the perimeter and also to facilitate the possible future implementation of perimeter security.

5.1.8.4 The Weldmesh security fence must be interface-able and compatible with electronic alarm and security detection systems associated with electricity substations.

5.1.8.5 Lock boxes are required over all gate padlocks where Weldmesh fences are installed. Slides for padlocking are to be located such that lock box function exists on both sides of the gate.

5.1.8.6 The electric vehicle access gate must have a drive mechanism that can be switched to manual operation.

5.1.8.7 Electric vehicle access gate operator control is required via a key switch for the full gate opening and closing change of state (dead man switch).

5.1.9 Maintainability Requirements

5.1.9.1 All surface finishes applied to the fencing materials must meet the expected design life for the fence.

5.1.9.2 Substation perimeter fences will not necessarily be located on ElectraNet property boundaries, but generally inside the property boundary.

5.1.9.3 Each building must have a designated entrance door.

5.1.10 Availability Requirements

5.1.10.1 Anti-tamper design must be provided for all components of the electrically operated vehicle access gate.

5.1.11 Environmental Requirements

5.1.11.1 The Weldmesh fence must provide adequate aesthetic appeal to blend with the surrounding and limit visual impact.

5.1.11.2 Vegetation planting must provide aesthetic appeal but must not provide total visual block into the substation. There will be sufficient visual connection from the exterior of the substation into the substation CPTED.

ElectraNet

Contact Us

52–55 East Terrace, Adelaide,
South Australia 5000
PO Box, 7096, Hutt Street Post Office,
Adelaide, South Australia 5000

Phone **+61 8 8404 7966** or toll-free **1800 243 853**

Fax **+61 8 8404 7956**

Visit us online **electranet.com.au**