AMS 10-63 Infrastructure Security

2023-27 Transmission Revenue Reset

PUBLIC

Document number	AMS 10-63
Issue number	10
Status	Approved
Approver	Paul Ascione
Approval Date	30/07/2020

ISSUE/AMENDMENT STATUS

Issue	Date	Author	Reviewed By	Approved by
5	22/11/2006	G Lukies D Postlethwaite	G Lukies D Postlethwaite	G Towns
6	18/01/2007	G Lukies D Postlethwaite	G Lukies D Postlethwaite	G Towns
7	17/03/2007	G Lukies D Postlethwaite	G Lukies D Postlethwaite	G Towns
8	11/1/2013	R Stanwix D Meade	R Stanwix D Meade	D Postlethwaite
9	19/10/2015	A Rogers D Postlethwaite S Goel	A Rogers D Postlethwaite S Goel	J Dyer
10	30/07/2020	A Payne-Billard F Lirios	S. Dick	P. Ascione

Disclaimer

This document belongs to AusNet Services and may or may not contain all available information on the subject matter this document purports to address.

The information contained in this document is subject to review and AusNet Services may amend this document at any time. Amendments will be indicated in the Amendment Table, but AusNet Services does not undertake to keep this document up to date.

To the maximum extent permitted by law, AusNet Services makes no representation or warranty (express or implied) as to the accuracy, reliability, or completeness of the information contained in this document, or its suitability for any intended purpose. AusNet Services (which, for the purposes of this disclaimer, includes all of its related bodies corporate, its officers, employees, contractors, agents and consultants, and those of its related bodies corporate) shall have no liability for any loss or damage (be it direct or indirect, including liability by reason of negligence or negligent misstatement) for any statements, opinions, information or matter (expressed or implied) arising out of, contained in, or derived from, or for any omissions from, the information in this document.

Contact

This document is the responsibility of Network Management Division of AusNet Services. Please contact the indicated owner of the document with any inquiries.

AusNet Services
Level 31, 2 Southbank Boulevard
Melbourne Victoria 3006
Ph: (03) 9695 6000

Table of Contents

1 Executive Summary 3
1.1 Risk 4
1.2 Principles 4
1.3 Strategies 4
2 Introduction 7
2.1 Purpose 8
2.2 Scope 8
2.3 Asset Management Objectives 8
3 Asset Description 10
3.1 Terminal Stations 10
3.2 Towers / Structures 15
3.3 Network Redundancy 15
3.4 Asset Age Profile 15
3.5 Asset Condition 16
3.6 Asset Performance 18
3.7 Asset Criticality 20
4 Other Issues 23
5 Risk Assessment 24
5.1 Terminal Stations 24
5.2 Transmission Lines 25
5.3 Inspection Testing Maintenance and Auditing 25
5.4 Contingency Plans 25
5.5 Program of Works 26
6 Asset Strategies 27
6.1 Terminal Stations 27
6.2 Transmission Lines 28

1 Executive Summary

This strategy forms part of AusNet Services' asset management strategy for the Victorian Electricity Transmission network. Its purpose is to maintain network safety, availability and security through effective and efficient management of the physical security of network infrastructure.

Commonwealth and state governments have imposed legal responsibility on the owners and operators of critical infrastructure; to take all necessary preventative security measures to ensure continuity of supply. This strategy focuses on security enhancements for terminal stations and transmission lines, forming part of the electricity transmission network in the state of Victoria. The main security threats to this network are:

- Safety – of untrained persons in the vicinity of energy-containing equipment.
- Malicious – motivated by revenge, fame, association or challenge.

- Criminal – profit driven; includes theft, fraud, sabotage or extortion.
- Terrorism – threat or use of force to influence government or public through fear or intimidation.[1]

1.1 Risk

This strategy is informed by site-specific risk assessments of major sites and generic assessments for the multiplicity of less significant installations. The 2018 Infrastructure Security Risk Assessment Tool (ISRAT) is used to assess physical security risks to public safety, network assets and the electrical energy they transmit. ISRAT is based on:

- National Guidelines for Unauthorised Entry Prevention, Energy Networks Australia, and
- ISO 31000:2009, "Risk Management – guidelines on principles and implementation of risk management".

1.2 Principles

AusNet Services' physical security control measures are founded on the following principles:

- Consistent risk identification and quantification.
- Defence in depth – increasing the number and sophistication of control measures commensurate with the degree of intrusion risk.
- Deterrence – measures to deflect would-be intruders towards other targets.
- Delay – measures to increase the time and effort required to successfully intrude.
- Detection – measures to promptly and reliably detect intrusion.
- Response – measures to promptly and appropriately deal with intruders and associated consequences.
- Contingency planning – measures to promptly recover service and minimise societal impact.

1.3 Strategies

The following summarises the key strategies for the management of infrastructure security of terminal stations and transmission lines:

1.3.1 Terminal Stations

1.3.1.1. New and major re-development projects

New greenfield terminal stations and substantial brownfield redevelopments shall incorporate, as a minimum, the following security measures:

- [C-I-C].

[1] A 'terrorist act' is an act or threat intended to advance a political, ideological or religious cause by coercing or intimidating an Australian or foreign government or the public; causing serious harm to people or property, creating a serious risk of health and safety to the public, disrupting trade, critical infrastructure or electronic systems – Criminal Code Act 1995 [Commonwealth].

1.3.1.2. High Risk

In conjunction with network augmentation and asset replacement projects at existing higher-risk terminal stations over the next decade:

[C-I-C]

1.3.1.3. Medium Risk

In conjunction with network augmentation and asset replacement projects at existing medium-risk terminal stations over the next decade:

[C-I-C]

1.3.1.4. Low Risk

In conjunction with network augmentation and asset replacement projects at existing lower-risk terminal stations over the next decade:

[C-I-C]

1.3.2 Transmission Lines

1.3.2.1. High Risk Lines

In conjunction with annual review and re-publishing of network contingency plans each year:
[C-I-C]

1.3.2.2. Low Risk Lines

In conjunction with annual review and re-publishing of network contingency plans each year:
[C-I-C]

2 Introduction

AusNet Services owns and operates the Victorian electricity transmission network, directly serving the energy needs of Australia's second largest economy and the National Electricity Market (NEM) via the national electricity transmission grid. This network transfers bulk power from NEM generators to the electricity distributors who service in excess of 2.4 million Victorian households and businesses. It interconnects high voltage customers such as the Portland Aluminium Smelter and the transmission networks of New South Wales, South Australia and Tasmania.

The Commonwealth and State governments have imposed legal responsibility on both the owners and operators of critical infrastructure, such as gas and electricity installations, to take all necessary preventative security measures to ensure continuity of supply. Owners and operators are expected to clearly recognise their responsibilities in safeguarding their installations as far as possible and to develop robust contingency plans to restore their services following a calamitous event (whether natural or man-made).

The Emergency Management (Critical Infrastructure Resilience) Regulations 2015 and the Victorian Emergency Management Act 2013 requires electricity and gas network owners and operators to prepare and maintain risk management plans which include:

- *the identification and assessment of emergency risks;*
- *the existing and planned actions or activities to manage each of the emergency risks; and*
- *the arrangements, processes and procedures that implement these actions or activities.*

The Electricity Safety Act requires AusNet Services to *design, construct, operate, maintain and decommission its supply network to minimise, as far as is practicable, the hazards and risks to the safety of any person arising from the supply network*.[2] What is considered "practicable" is determined by regard to:

a) the severity of the hazard or risk in question; and
b) state of knowledge about the hazard or risk and any ways of removing or mitigating the hazard or risk; and
c) the availability and suitability of ways to remove or mitigate the hazard or risk; and
d) *the cost of removing or mitigating the hazard or risk.*[3]

AusNet Services is also required to meet the requirements of clause 11.1 of the Electricity System Code[4] to:

(b) develop and implement plans for the acquisition, creation, replacement, maintenance, operation, refurbishment, repair, retirement and disposal of transmission network assets to, economically:
- *meet reasonable customer expectations of transmission services;*
- *comply with the laws and other performance obligations which apply to the provision of transmission services; and*
- *maintain transmission network service performance so as to minimise the risks associated with the failure of assets; and*

(c) develop, test or simulate and implement contingency plans to deal with events which have a low probability of occurring, but are realistic and would have a substantial impact on customers and generators connected to the licensee's transmission network.

Clause 6A.6.7 of the National Electricity Rules requires AusNet Services to propose capital expenditures necessary to:

- *meet or manage the expected demand for prescribed transmission services over that period;*
- *comply with all applicable regulatory obligations or requirements associated with the provision of prescribed transmission services;*
- *maintain the quality, reliability and security of supply of prescribed transmission services;*
- *maintain the reliability, and security of the transmission system through the supply of prescribed transmission services; and*
- *maintain the safety of the transmission system through the supply of prescribed transmission services.*

[2] Safety Act 1998, section 98(a).
[3] Electricity Safety Act 1998, section 3.
[4] Electricity System Code, Office of the Regulator General, October 2000.

Infrastructure Security

2.1 Purpose

This strategy outlines physical security requirements in accordance with the aims and objectives outlined in SPIRACS[5], reproduced below for convenience.

> "Security management involves the protection of AusNet Services assets (infrastructure, people, information) from natural or deliberate threats. Credible threats and vulnerabilities shall be identified and mitigated; robust security controls introduced; and contingency plans developed and maintained to minimise the effects of security incidents, should they occur.
>
> An effective security management capability is necessary to minimise risks from security threats, and ensure compliance with regulatory and contractual obligations. The SPIRACS Corporate Security Policy establishes the requirement for a security management capability in AusNet Services, and specifically defines the policy in which potential or actual security incidents are to be effectively identified and managed".

The objectives of security management are to:

- Minimise exposures to credible security threats,
- Ensure that only authorised and appropriately trained personnel have access to assets,
- Prevent unauthorised disclosure/access/loss/damage of corporate assets,
- Prevent loss of asset functionality for the community, clients and customers,
- Identify and respond to security incidents, and
- Minimise the impact of security incidents.

2.2 Scope

This document includes Strategies for the management of physical security infrastructure associated with the AusNet Services' electricity transmission network in Victoria. The scope of infrastructure covered by this document includes:

- Terminal stations; and
- Transmission lines.

This document does not include information technology security strategies: please refer to the Information and Communication Technology Strategy[6] for information on this topic.

This document does not include communication infrastructure security strategies, such as radio tower sites: please refer to the Communication Systems Strategy[7] for information on this topic.

2.3 Asset Management Objectives

As stated in *AMS 01-01 Asset Management System Overview*, the high-level asset management objectives are:

- Comply with legal and contractual obligations;
- Maintain safety;
- Be future ready;
- Maintain network performance at the lowest sustainable cost; and
- Meet customer needs.

As stated in *AMS 10-01 Asset Management Strategy -Transmission Network*, the electricity transmission network objectives are:

[5] SPIRACS – AusNet Services Incident Response and Contingency System.
[6] Information and Communication Technology Strategy CY2020 - CY 2024 Electricity Distribution Network, AusNet Services 2018
[7] AMS 10-56 Communication Systems, AusNet Services 2020

Infrastructure Security

- Maintain top quartile benchmarking;
- Maintain reliability;
- Minimise market impact;
- Maximise network capability;
- Leverage advances in technology and data analytics;
- Minimise explosive failure risk.

3 Asset Description

AusNet Services' electricity transmission network includes 42 unmanned terminal station and 12 power station switchyards and 155 transmission circuits formed from approximately 13,000 galvanised steel towers and 6,500 kilometres of EHV lines to transport electricity from power stations to electricity distributors and large customers.

To ensure that asset failures are unlikely to constrain supplies to customers or compromise the security of the National Electricity Market (NEM), this electricity transmission network employs high levels of redundancy in primary circuits and secondary circuits including:

[C-I-C]

Prior to 2006, these installations were designed and maintained to the security standards outlined in AS 2067[8] and ESAA guidelines[9] for design and maintenance of overhead lines. Since 2006 installations have been designed to the Energy Networks Association's (ENA's) national guidelines[10] and since 2010 designs have referenced AS 7000 for the design of overhead electrical lines[11].

3.1 Terminal Stations

AusNet Services owns and operates terminal stations located in neighbourhoods ranging from remote rural to urban industrial subdivisions. On average each terminal station supplies 55,000 customers. Electrical equipment within each terminal station is arranged in switchyards which typically contain air-insulated bus bars, power transformers, instrument transformers, circuit breakers, disconnectors, capacitor banks, Static VAr Compensators and associated low voltage electrical protection, control and instrumentation equipment.

3.1.1 Security Fence

The primary physical security feature for each terminal station is a chain wire mesh fence, fitted in many cases with an electric fence, barbed wire or barbed tape anti-climbing feature.

About 56 km of security fencing[12] encloses more than 532 hectares of land at over 60 individual sites. Early security fence design utilises a 2.5 m chain-wire panel mounted on galvanised posts (2.7 to 3m in height) topped with multiple strands of barbed wire. The lower edge of the chain-wire panel is usually buried with a stabilised cement plinth under the fence. This provides some resistance against burrowing and tunnelling.

The foundations and structural supports of fencing are designed to resist the manual efforts of potential intruders. Fencing utilises robust materials such as brick, masonry, chain wire mesh, sheet metal, weldmesh or steel palisade, arranged so as to minimise the possibility of unauthorised persons penetrating, scaling or undermining the fence.

The location, construction and use of gates are designed to complement the function of intruder-resistant fences. Particular attention is required to ensure locking devices and gateposts minimise scaling of the gate or fence.

Where motor vehicles are assessed as credible risk, vehicular barriers such as Armco railings, concrete barriers, drainage ditches or earth mounds are incorporated in the overall fencing design.

Where space permits at sites assessed as a higher risk of unauthorised access, 'clearance zones' are established immediately adjacent to security fencing to minimise the threat of scaling by use of nearby aids such as vegetation or stored materials. If space is restricted, the total effective height of fencing is increased in proportion to the risk of scaling.

[8] Australian Standard AS/NZS 2067 HV Installations.
[9] Guidelines for the Design and Maintenance of Overhead Lines C(b) 1 – 2003, Electricity Supply Association of Australia.
[10] National Guidelines for the Prevention of Unauthorised Access to Electricity Infrastructure, ENA Doc 015–2006
[11] Australian Standard AS/NZS 7000.
[12] Station design manual Vol.5 Section.5 – Civil designs security fencing and signage.

3.1.1.1. Higher Risk Sites

Where assessment indicates higher risks of unauthorised access; intruder-resistant fences may be constructed from Type 2 – Pipe rail security fencing[13] arranged as per SDM 05-1300[14] or equivalent weldmesh security panels, palisade panels, brick or masonry walls of a minimum 2.4 m in height with a concrete or cement stabilised crushed rock footing or kerb and a barbed tape anti-climbing device in flat loop or concertina configuration to bring effective fence height to greater than 2.9 m. At higher risk sites; existing intruder-resistant fences are enhanced with:

- a micro phonic or vibration-based perimeter detectors; or
- electric power fencing.

Figure 1 below illustrates a palisade security fence with a continuous concrete footing plinth and an electric power fence anti-climbing feature suitable for higher security risk sites.

Figure 1: Palisade Security Panel with Concrete Plinth and electric power fence

An electric power fence is located on the inside of the chain wire mesh or palisade panel. Its lowest wire is less than 150 mm above ground level and its upper wire is 2.9 m above ground level. In-riggers, out-riggers, barbed wire or barbed tape are not used in conjunction with an electric power fence. The electric power fence installation shown in Figure 2 below includes intrusion alarm monitoring via SCADA.

[13] Australian Standard AS 1725.1-2010 Chain link fabric fencing Part 1 Security fences and gates
[14] SDM 05-1300 Security Fencing & Signage Station Design Manual AusNet Services

Figure 2: Electric Power Fence inside Chain Wire Mesh Fence

3.1.1.2. Medium Risk Sites

Where existing terminal stations are assessed as a medium risk of unauthorised access, intruder resistant fencing may be of chain wire mesh construction to Type 2 - Pipe rail security fencing[15] arranged as per SDM 05-1300[16]. The minimum height of existing fence panels is 2.4 m. Each fence panel shall not be more than 50 mm from the ground. Risers fitted with flat looped short-barbed tape provide an anti-climbing feature to a minimum effective fence height of 2.9 m. At selected medium risk sites; existing intruder-resistant fences may be enhanced with a micro phonic or vibration-based perimeter detectors.

A combination of fence footings, kerbings or rails is used to restrict the ability of intruders to pass under the fence as shown in Figure 3 below.

Figure 3: Pipe rail security fence to AS 1725.1 with barbed tape anti-climb feature

3.1.1.3. Lower Risk Sites

For existing terminal stations assessed as a lower risk of unauthorised access, intruder resistant fencing may be of chain wire mesh construction to Type 2 - Pipe rail security fencing[17], arranged as per SDM 05-1300[18].

[15] Australian Standard AS 1725.1-2010 Chain link fabric fencing Part 1 Security fences and gates
[16] SDM 05-1300 Security Fencing & Signage Station Design Manual AusNet Services
[17] Australian Standard AS 1725.1-2010 Chain link fabric fencing Part 1 Security fences and gates
[18] SDM 05-1300 Security Fencing & Signage Station Design Manual AusNet Services

The minimum height of existing fence panels is 2.1 m. Each fence panel shall not be more than 50 mm from the ground. Outriggers, inriggers or risers fitted with multiple strands of barbed wire or short-barbed tape provide an anti-climbing feature to a minimum effective fence height of 2.4 m. A combination of fence footings, kerbings or rails is used to restrict the ability of intruders to pass under the fence as shown in Figure 4 below.

Figure 4: Pipe rail security fence to AS 1725.1 with barbed wire anti-climb feature

3.1.2 Access Systems

Electronic access control systems shall be installed on designated pedestrian gates and vehicle gates in each terminal station security fence and on designated external building doors leading to control and relay rooms.

Access controls are capable of giving specific permission to individual persons on a site-by-site basis and can be used to restrict access to certain times or under certain conditions. The electronic access control system provides access history and transmits alarm signals to the network operation centre when unauthorised access is attempted. Electronic proximity cards permit entry to authorised employees and contractors via an interface similar to that illustrated in Figure 5 below.

Figure 5: Electronic Access Control, User Interface

3.1.3 Intruder Detection System

These systems are installed on high risk sites so that if intruders are able to gain entry into these installations, the Control Room Security Desk is alerted of their presence and the appropriate authorities such as Police or Security Company is requested to attend the site and secure the area.

[C-I-C]

3.1.3.1. Site Perimeter

[C-I-C]

3.1.3.2. Site Interior

CCTV cameras may be installed to monitor access points, switchyards and buildings within selected higher security risk sites. Options include permanent installations to monitor sustained security risks and temporary installations to monitor time-specific risks such as construction projects. CCTV camera placement will be determined on a site specific basis.

CCTV cameras can operate in conjunction with intrusion detectors, security lighting and remote operation to detect, verify and assist the response to unauthorised access attempts. Access to the images from the cameras is restricted to authorised personnel, as per AusNet Services policy 'Use of Surveillance Camera Equipment'.

3.1.3.3. Building Interior

[C-I-C].

3.1.4 Station and Switchyard Lighting

Lighting is incorporated into the security system of a terminal station as it deters anti-social behaviour, unauthorised access, identifies intruders and assists personnel in responding to network events and unauthorised access attempts.

The standard and extent of lighting and the sophistication of lighting controls is matched to the assessed risk of unauthorised access. The entrances and the pathways within sites are capable of illumination to ensure night visibility for staff. Switchyards are lit to levels that enable operational activities to be performed. Remote activation of switchyard and building lighting from the network control room facilitates the response of security contractors to unauthorised access alarms.

Where credible security risks have been assessed, supplementary lighting will enable CCTV monitoring and facilitate response to unauthorised access attempts. When planning the installation or augmentation of operational and security lighting the following factors should be considered:

- Manual and remote activation.
- Restrike time for high-intensity discharge lamps.
- Light pollution on neighbouring properties and the night sky.

3.1.5 Signs warning of EHV equipment and of the dangers of unauthorised access

Station perimeter signage advises the public on site ownership, security warnings, and electrical hazards of the station and contact telephone numbers.

Australian Standards[19] require that key parts of the station installation are clearly, legibly, durably and uniquely labelled. Therefore, many equipment nameplates and signs have been installed in terminal stations to physically identify these assets. These operational nameplates help the safe and reliable operation and maintenance of other electrical assets.

[19] AS1319 – 1994: Safety signs for the occupational environment.

3.2 Towers / Structures

AusNet Services employs approximately 13,000 galvanised steel towers to support 155 individual EHV transmission circuits located throughout Victoria. These towers are predominantly of a lattice type construction whereby relatively small individual steel members are bolted in to a single structure from 20 m to 50 m in height.

3.2.1 Anti-Climbing Barriers

Towers are located in varying types of environment/settings. Urban environment where the population can walk to a structure, climbing deterrents or anti-climbing barriers comprised on steel mesh and barb wire held up by steel members are installed around the tower.

Access to the tower is via a corner door through the mesh that is controlled by a security padlock. Keys for these security locks are only issued to staff and contractors who are formally trained and authorised to climb these towers. Keys are managed from a single register to ensure effective control.

3.2.2 Passive Climbing Deterrents

To futher deter unauthorised climbing on the tower, a passive system has been introduced in that there are no climbing bolts aka step-dogs along the first two metres of the climbing leg. Workers authorised to climb the structure are provided by removable step bolts which they install prior to climbing, and remove after performing work on the sturcuture.

3.2.3 Signs warning of EHV equipment and of the dangers of unauthorised access

Similar to terminal stations, tower structures have signages which advises the public on site ownership, security warnings, and electrical hazards of the structure.

3.2.4 Fences

Fences are installed on tower sites located inside private land and/or where the structure is deemed needing further security in addition to what anti-climbing barrier provides. Only a handful of towers have security fences installed around them, in addition to the anti-climbing barriers which have gates that can be opened by the same key that is issued by the Security Team from the Control Room.

3.3 Network Redundancy

A key factor in the management of unauthorised access risks to transmission lines is the redundancy of individual circuits provided by the meshed and looped configuration of the Extra High Voltage (EHV) circuits in the National Electricity Market (NEM). The failure of a single transmission line on a day of average loadings will not cause supply outages to customers and single failures will have little impact on the re-scheduling of the many generators serving the NEM. It is only on the relatively few peak demand days each year that an outage of some circuits will constrain the optimium configuration of the NEM causing re-scheduling of generators and controlled load shedding to restore the NEM to secure status.

3.4 Asset Age Profile

In many cases existing infrastructure security designs date back to the initial station construction but partial or full replacement of some of these assets as part of the station rebuild works or station infrastructure projects have resulted in improved condition.

The age profile of the station security fence, shown in Figure 6 shows a much younger profile compared to that of the terminal stations, which is shown in Figure 7.

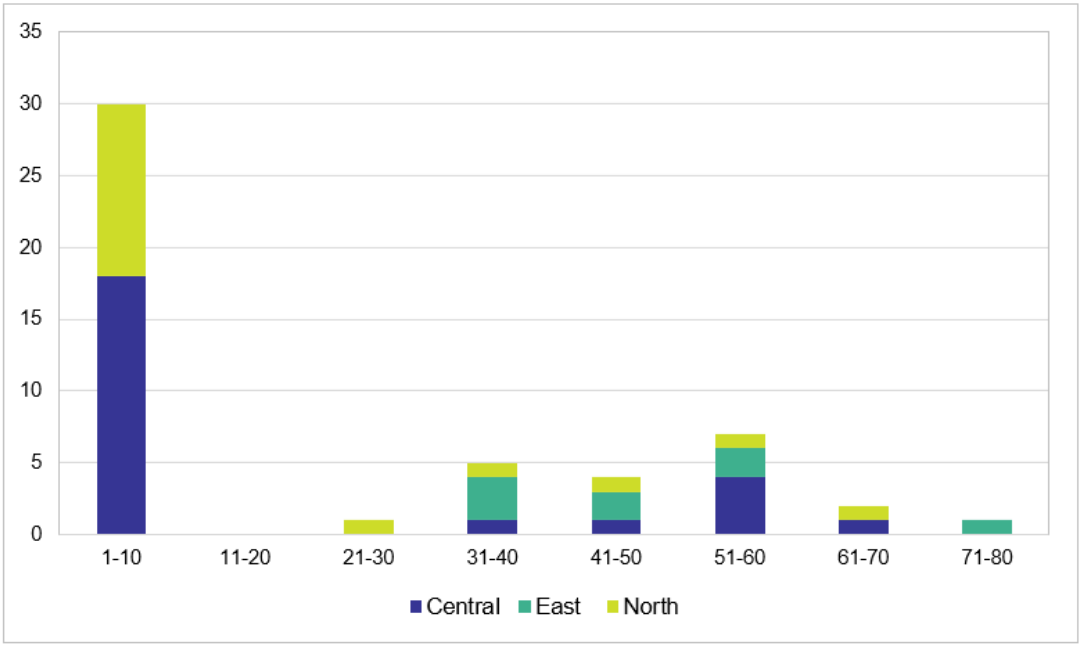

Figure 6: Security Fence Age Profile

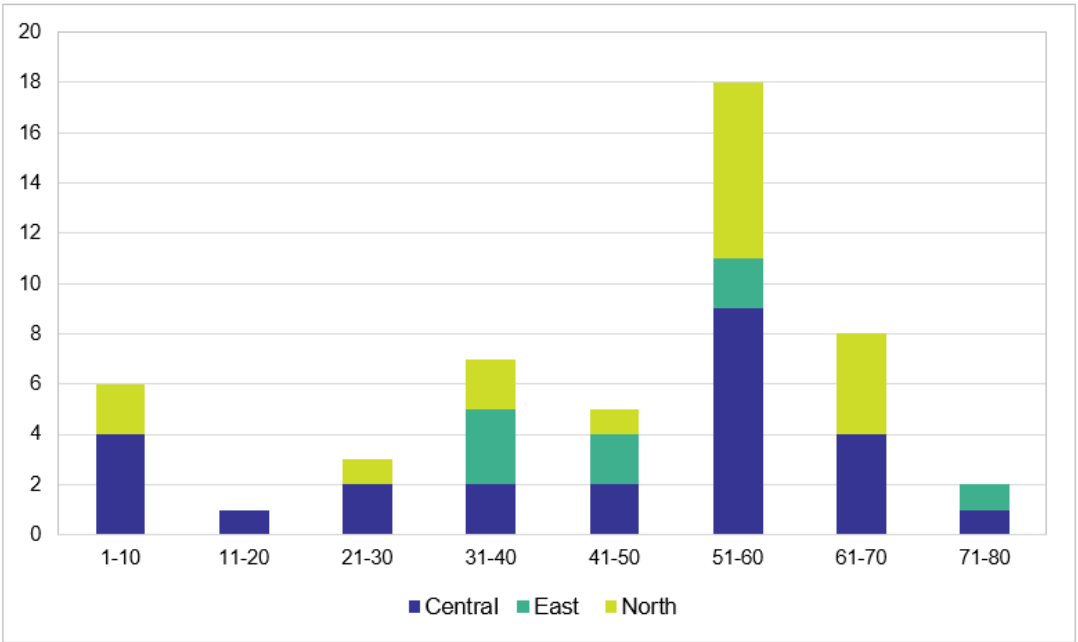

Figure 7: Zone Substation, Age Profile

3.5 Asset Condition

The condition of the terminatl stations' infrastructure security is in Average condition, even though majority of the stations' service life is beyond 50 years. This is due to recent upgrades/refurbishments of some of the assets in the stations during rebuilds and/or equipment replacement programs.

The condition of infrastructure security assets is influenced by several factors such as:

- Operating conditions;
- Climatic and environmental conditions;
- Differing designs and construction material;
- Past opportunities to integrate infrastructure security replacement works, together with civil infrastructure works into rebuild projects/programs.

Infrastructure Security

Infrastructure security assets in poor condition pose risks associated with breach in security. These issues are more prominent at stations which are near populated areas, or if the stations have a high profile image such as SMTS or ROTS which have multiple lines going into the yard.

The condition assessment for the infrastructure security in all terminal stations was formulated to inspect all major stations to be incorporated into the existing civil infrastructure maintenance program.

Infrastructure security assets are assigned condition scores which correspond to the remaining service potential (remaining life). Table 1 below lists details of condition scores including descriptions and the expected remaining service potential.

Table 1: Condition Scores

Condition	Description	Remaining Service Potential
C1	As New	90%
C2	Good	75%
C3	Average	50%
C4	Poor	25%
C5	Very Poor	10%

Details on the condition of infrastructure security assets in terminal stations and on transmission structures are covered in the sections below.

3.5.1 Station Fence

Over the past ten years, many stations were identified as critical security sites, and have been upgraded with electric power fencing constructed along with new chain wire mesh. These upgrades also involve the retrofit of razor tape topping and concrete footing plinths to existing security fences. Approximately half of terminal stations now have an electric fence, with eighty percent of the sites having been given a Very Good to Average (C1 to C3) condition score, while 20% of the sites are in Poor to Very Poor condition (C4 & C5) as shown in Figure 8 below.

Progressive fencing upgrades and replacement works are planned to ensure that all station security fences will meet industry design standards[20] by 2022. Refer to AMS 10-63: Infrastructure security for more details on the condition of these fences and proposed upgrade work programs.

[C-I-C]

Figure 8 – Condition profile of security fencing

[20] National Guidelines for Prevention of Unauthorised Access to Electricity Infrastructure – ENA DOC 015-2006.

3.5.2 Tower Security Fence

Unlike security fences for terminal stations, tower fences and anti-climbing barriers used on structures are assessed in a binary way – either they're working or defective. This is because tower structures are mostly isolated and are inspected at a longer intervals[21] compared to terminal stations, which requires these to remain operational until the next tower inspections.

3.6 Asset Performance

3.6.1 Suspended Failures

Defects in Infrastructure Security which are identified prior to a failure or fault are defined as suspended failures. Suspended failures are also referred to as "preventative actions" which are identified during routine stations inspections, or during Condition Assessment Inspecitons/ Line & Easement Inspections on transmission lines.

The station inspector raises a ZA notification in SAP and assigns appropriate priority rating (PT rating) to the issue commensurate to the risk of the asset failing. The following figures illustrates the top 10 items identified for the various Infrastructure Security components inside stations for the past years.

3.6.1.1. Station Security Fencing

Security fencing includes the electrical fence that has been installed in critical sites as determined by the security department in conjunction with Victoria Police. [C-I-C]

[C-I-C]

Figure 9 – Infrastructure Security, Suspended Failures, Terminal Stations

3.6.1.2. Tower Security

Tower security is primarily provided by the anti-climbing barriers installed around the structure at least 2-metres from ground level. Additional security measures are the waring signs around the structure as well as the absence of step bolts along fist 2-metres of the climbing leg.

As shown in Figure 10, the issues associated with tower security are mainly missing signage, followed by damaged fences, missing anti-climbing barriers, etc.

[21] Transmission structures can be inspected 3-yearly, 6-yearly or 9-yearly depending on the risks of failure for any component on the structure, e.g. conductor, groundwire, insulator or the structure itself.

[C-I-C]

Figure 10 – Infrastructure Security, Suspended Failures, Transmission Lines

3.6.2 Functional failures

Functional failures, also known as Faults, result in the system not being able to perform its intended purpose and therefore, appropriate action is necessary to maintain the performance and security of the system.

Similar to Suspended failures, assets that have experienced Functional failure are flagged in the system and a ZK notification (action required after a Fault) is raised. The following sections identify the functional failures that have occurred over the past five years.

3.6.3 Station Security Fencing

Security fencing faults primarily involve issues with [C-I-C] of ZK notifications, followed by [C-I-C] The rest of the cohort involve the monitoring equipment.

[C-I-C]

Figure 11 – Security fencing, functional failure

3.6.4 Tower Security

As mentioned in Section 3.6.1.2, tower security is composed of primarily the anti-climbing barriers together with the passive deterrent of not having climbing bolts near the base of the tower. On some towers where there is a higher risk of unauthorised access, security fences are installed around the tower. Often times, these deterrents are effective in their objective however, on are occasions, unauthorised access is not prevented.

One such event occurred in 20th April 2020, there were three base jumpers were able to gain access into T004 WMTS-FBTS 220 kV line. This tower, together with T003 and T005 are three of the tallest structures in the network with an average height of 100 metres. Fortunately, a member of the public called the Police and when one of the jumpers went down the tower, the authorities were able to stop their attempt which could have been fatal – as both circuits were alive.

Figure 12 below illustrates the number of functional failures in the transmission line network. (Note that the event that occurred in T004 is not included in the list because it was reported by a member of the public, thus no Notification was created in SAP).

[C-I-C]

Figure 12 – Security fencing, functional failures

3.7 Asset Criticality

The consequence of failure of any of the various components in Infrastructure Security in a Terminal Station and/or Transmission Line Structure can vary significantly, ranging from theft, asset damage for the building and structure, to the safety of untrained members of the public who has gained access into AusNet Services ' assets.

To get a quantitative value of the system's criticality, the economic impact of each potential outcome is considered and analysed. For this analysis, the condition of the security fence and anti-climbing barriers are assessed for the terminal stations and transmission structures, respectively.

The economic impact is calculated by adding these components shown in Table 2:

- Safety – of untrained persons in the vicinity of energy containing equipment
- Vandalis/Malicious – motivated by revenge, fame, association or challenge
- Criminal – profit driven; includes theft, fraud, sabotage or extortion
- Terrorism – use or threat of force or violence to influence government or public through fear or intimidation

Table 2: Security Threats by Installation Type

	Safety	Malicious	Criminal	Terrorism
Terminal Stations	Yes	Yes	Yes	Yes
Tower Lines	Yes			

3.7.1 Procedures

SPIRACS Volume 5 Part 2 'Security Management Framework' and Part 3 'Operational Security Policies, Standards & Procedures' contain information and references on the authorised policy and procedures to be employed when:

- Authorising employees and contractors to enter AusNet Services sites.
- Entering AusNet Services sites.
- Reporting unauthorised access events.
- Monitoring and responding to unauthorised access events.
- Inspecting, testing, maintaining and auditing physical security measures.
- Developing, exercising and maintaining contingency plans.

3.7.2 ISRAT

The 2018 versions of the Infrastructure Security Risk Assessment Tool (ISRAT) has been used to assess physical security risks and control measures in each terminal station[22] and generic risks for the multiplicity of transmission line towers[23]. ISRAT is a quantitative tool based on the principles in Energy Network Association's national guidelines and is consistent with the methodology from the international risk management standard ISO 31000. ISRAT can produce assessments of risk for safety, theft/malicious damage, and terrorism threats:

- During planning and design of new sites.
- Following an unauthorised access event.
- Where major changes are made to existing sites where security may be compromised.
- When neighbouring land is re-zoned or its main use is significantly changed.
- Where a risk assessment has not been carried out for five years.

3.7.3 Terminal Stations

2018 Terminal Station ISRAT calculates the consequences associated with unauthorised access events at terminal stations based on the following factors:

3.7.3.1. Theft and Vandalism

Site specific theft consequences are established from the average values via 2014 regional police and insurance company crime statistics. The theft and malicious damage effects, escalated to 2019 values, equates to [C-I-C] per event and is based on AusNet Services' historic event records.

3.7.3.2. Terrorism

The effect of a terror event has been calculated for each site based on equipment and circuit redundancy, the value of unserved energy following damage to a connection asset and the value of a generation market constraint following damage to an asset in the shared transmission network.

3.7.3.3. Safety

The safety effect of [C-I-C] per event is based on the present day value of a statistical life as per the Health Safety Executive[24] methodology. This represents a scenario wherein a member of the public gained access into the terminal station which resulted to a fatality.

3.7.4 Transmission Structures

As the safety infrastructure of transmission structures are not assessed in terms of condition, a qualitative analysis has been undertaken for these assets below and the results are shown in the Corporate Risk Matrix in Section 5: Risk Assessment. The 2018 Transmission Line ISRAT calculates the generic risks associated with unauthorised access events on transmission line towers based on the following factors:

[22] 2015 Terminal Station ISRAT.xlsx AusNet Services July 2015.
[23] 2015 Transmission Line ISRAT.xlsx AusNet Services July 2015.
[24] Page 6 ND Guidance on the Demonstration of ALARP TAS005 Health Safety Executive 2009 www.hse.gov.uk

3.7.4.1. Theft and Vandalism

The malicious damage probability of 1% per transmission line per annum is based on a scenario of one minor damage event on the 120 transmission circuits each year. The malicious damage effect of [C-I-C] per event is based on limited historic records of insulator vandalism, structural steel damage and foundation bolt removal.

.

3.7.4.2. Terrorism

The average terrorism probability has been based on the scenario of a terror event each 50 years which is equivalent to 0.05% per circuit per annum. The effect of a terror event has been calculated for each transmission line based on circuit redundancy, tower replacement costs, the value of unserved energy and the value of a generation market constraint in the shared transmission network

3.7.4.3. Safety

The average safety probability (0.1% per line per annum) has been based on the scenario of a single safety event on the 120 transmission circuits each decade. The safety effect of $20,000,000 per event is based on the present day value of a statistical life as per the Health Safety Executive[25] methodology.

3.7.5 Overall Criticality

The consequences of a fragile security system can be allocated into five criticality bands based on their economic impact as the result of the failure leading to unauthorised access into the station, or onto the transmisison structure. These asset criticalities or consequence impacts are irrespective of the likelihood of the actual failure of the security system.

The five criticality bands are tabulated given in Table 3 below:

Table 3 – Criticality Band

Criticality Band	Economic Impact due to a failure
1	<= 1 replacement cost
2	1 to 3 x replacement cost
3	3 to 10 x replacement cost
4	10 to 30 x replacement cost
5	>30x replacement cost

The criticality assessment compares calculated consequence cost over the replacement cost. For the infrastructure security, the criticality value is the ratio of the consequences of unauthorised access into a terminal station, or tower structures, and the cost to replace the system.

Figure 11 in *Section 5: Risk Assessment* presents the criticality matrix for the Infrastructure Security on Terminal Stations and Transmission Structures. The numbers indicate the quantity of terminal stations which have an Infrastructure Security under a specific condition score and have a consequence of failure within a particular Criticality Band.

[25] Page 6 ND Guidance on the Demonstration of ALARP TAS005 Health Safety Executive 2009 www.hse.gov.uk

4 Other Issues

These are other issues related to Infrastructure Security:

- The Security and Emergency Management Team is intending to produce a new document, Security of Operational Facilities, Functional Requirement Document" which shall be used as reference in upgrading the Infrastructure Security in Terminal Stations.
- Records for the infrastructure security systems inside terminal stations are inadequate and do not include up-to-date essential information such as installation date, material type, length, and asset specific condition.
- Increasing security standards and changes in neighbouring land usage often render the existing security fencing inadequate before reaching its nominal service life.

5 Risk Assessment

There are varying risks associated with the infrastructure security for terminal stations and transmission line structures, ranging from Theft & Malicious Damage, Safety of the public and Terrorism. Depending on the nature of the and scale of the deficiency, solution to rectify the issue can be by asset replacement, station or tower ACD refurbishment, or whole station rebuild.

5.1 Terminal Stations

For terminal stations, the integration of the station security fence refurbishment or replacement has proven to be most cost effective if incorporated into station rebuild projects. A semi-quantitative risk analysis was undertaken for each station by considering the stations that were given a condition rating of Poor to Very Poor (C4 to C5), using the criticality values from consequences of a breach in security divided by the unit rate for repair/replacement of the security infrastructure.

[C-I-C]

Figure 13: Infrastructure Security Risk Matrix

There are 5-terminal stations in risk Level A: the 3-terminal stations with C5 conditon fences are LY, MPS and YPS, while the terminal stations with C4 condition fence and Criticaltiy 4 are HOTS and LYPS Switch yard.

LY and LYPS switch yard are located inside the power station so don't require the same standard of fence security as High Risk Station fences, i.e. this is a fence within the power station fence. Meanwhile, MPS doesn't house any relevant assets so the fence doesn't need to be replaced, as long as the fence is still safe to operate. Hence, only HOTS and YPS are included in the proposed program of works for the coming period, shown in Section 5.5.

5.1.1 Higher Criticality Stations

The following terminal stations are currently classified as higher security risk in accordance with the Emergency Management (Critical Infrastructure Resilience) Regulations 2015 or the 2018 Terminal Station ISRAT:
[C-I-C]

5.1.2 Medium Criticality Stations

The following terminal stations are currently classified as medium security risk:
[C-I-C]

5.1.3 Lower Criticality Stations

The following terminal stations are currently classified as lower security risk:
[C-I-C]

5.2 Transmission Lines

For transmission structures, a qualitative risk assessment was undertaken in *Section 3.7.4 Transmission Structures*, and the results are used to provide a generic heat map of the security risks for a typical transmission line, as shown in Figure 144:

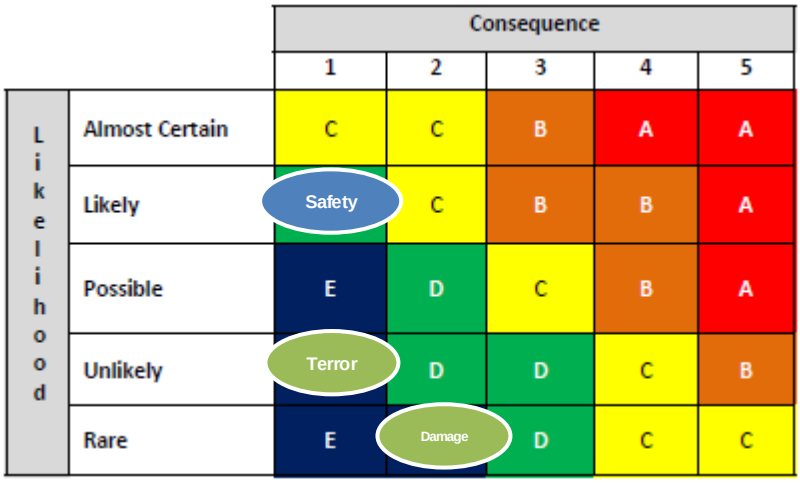

Figure 14: Generic transmission line security risks

5.2.1.1. Higher Risk Lines

The majority of transmission lines are currently classified as lower security risks principally due to the redundant nature of the meshed and looped circuits in the National Electricity Market. However, the following transmission lines are currently classified as higher security risk due to the co-location of redundant circuits on single towers: [C-I-C]

5.3 Inspection Testing Maintenance and Auditing

Commensurate with the assessed level of security risks:

- Sites are inspected regularly for indications of unauthorised entry.
- Control measures are inspected and tested to ensure functionality.

Inspections are carried out at intervals defined in the Standard Maintenance Instruction for on-site inspections. At times of heightened threat classification or alert, inspections may be required at more frequent intervals. Inspections include specific checks for indications of unauthorised entry to each site. Inspections also assess the condition and functionality of installed controls, especially fences, gates and building access points. Controls deemed to be in poor condition are reported and remedied within the timeframes specified by SPIRACS.

Periodic audits are conducted to confirm the integrity of the overall security system in accordance with the provisions established in SPIRACS. Audit scopes include:

- Recent security system performance.
- Compliance with established policy, procedures and standards.
- Relevancy and adequacy of established policy, procedures and standards.

5.4 Contingency Plans

A network contingency plan which includes a spare equipment holding review is prepared for the electricity transmission network each year. Whilst this plan is focussed on the recovery of service following plant failure or a natural disaster such as flood or fire; elements of this plan are suitable for response to unauthorised access events. In conjunction with SPIRACS these plans enable rapid deployment of skilled people, specialised construction equipment and spare equipment to safely restore electricity supplies.

For those sites assessed as a particularly high security risk; specific contingency plans to manage the recovery of service provision following an unauthorised access event may be prepared.

5.5 Program of Works

The proposed program of works for Regulatory Period 2022 to 2008 is provided in Table 4 below. The scope of works reflect the minimum acceptable standard for the stations and so if the station already has a particular item, the action is to assure that the existing system is functaional and meets accepted standards.

Table 4: Infrastructure Security, Program of Works

Name of Program	Scope of works	Stations
Infrastructure Security upgrade	CCTV installation; Remotely operated switchyard lights via SCADA.	[C-I-C]
	CCTV upgrade; Remotely operated switchyard lights via SCADA	[C-I-C]
	Security fencing with razor tape and plith; Remotely operated switchyard lights via SCADA.	[C-I-C]

NOTES:

1. + YPS is included in the Critical Infrastructure List.

6 Asset Strategies

6.1 Terminal Stations

6.1.1 New and major re-development projects

New greenfield terminal stations and substantial brownfield redevelopments shall incorporate, as a minimum, the following security measures:

[C-I-C]

6.1.2 High Risk

In conjunction with network augmentation and asset replacement projects at existing higher-risk terminal stations over the next decade:

[C-I-C]

6.1.3 Medium Risk

In conjunction with network augmentation and asset replacement projects at existing medium-risk terminal stations over the next decade

[C-I-C]

6.1.4 Low Risk

In conjunction with network augmentation and asset replacement projects at existing lower-risk terminal stations over the next decade:

[C-I-C]

6.2 Transmission Lines

6.2.1 High Risk Lines

In conjunction with annual review and re-publishing of network contingency plans each year:
[C-I-C]

6.2.2 Low Risk Lines

In conjunction with annual review and re-publishing of network contingency plans each year:
[C-I-C]