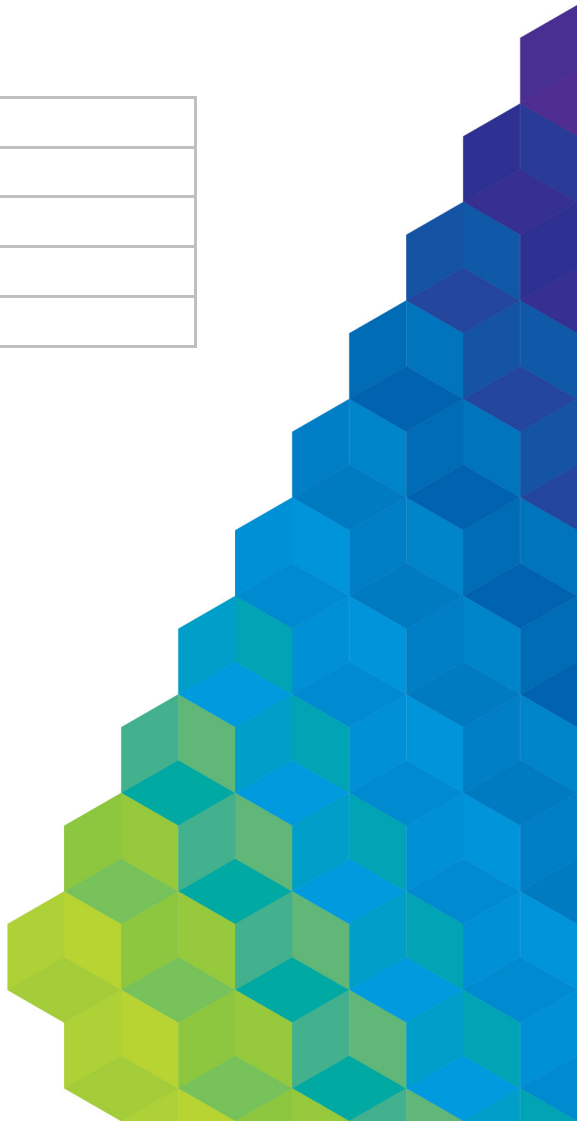
AMS – Victorian Electricity Transmission Network

Infrastructure Security (PUBLIC VERSION)

Document number	AMS 10-63
Issue number	9
Status	Approved
Approver	J. Dyer
Approval Date	19/10/2015



ISSUE/AMENDMENT STATUS

Issue	Date	Description	Author	Approved
5	22/11/06	Editorial review.	G. Lukies D. Postlethwaite	G. Towns
6	18/01/07	Review and Update.	G. Lukies D. Postlethwaite	G. Towns
7	17/03/07	Editorial review.	G. Lukies D. Postlethwaite	G. Towns
8	11/01/13	Review and Update.	R. Stanwix D. Meade	D. Postlethwaite
9	19/10/15	Fundamental review including update of risk assessments.	A. Rogers D. Postlethwaite S. Goel	J. Dyer

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 the Asset Management Division, AusNet Services. Please contact the indicated owner of the document with any inquiries.

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

Table of Contents

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 2015 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

Strategies for the management of infrastructure security of terminal stations and transmission lines are contained in Section 8.

[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].

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.

[2] Electricity 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

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.*

3 Objective

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.

[5] SPIRACS – AusNet Services Incident Response and Contingency System.

4 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, [C.I.C]: please refer to the Communication Systems Strategy[7] for information on this topic.

[6] Information and Communication Technology Strategy CY2016 – CY 2020 Electricity Distribution Network, AusNet Services 2014.

[7] AMS 10-56 Communication Systems, AusNet Services 2015.

5 Asset Summary

AusNet Services' electricity transmission network includes 43 [C.I.C] terminal station and power station switchyards and 120 transmission circuits formed from 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:

- EHV electrical equipment is arranged in redundant circuits within each terminal station;
- EHV transmission lines are arranged in redundant meshed and looped circuits throughout Victoria;
- Protection, control and instrumentation functions are duplicated or backed up; and
- Data streams are transmitted by redundant circuits over duplicated routes.

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].

5.1 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.

Large power transformers and smaller instrument transformers, located within each switchyard usually have exposed high voltage (HV) and extra high voltage (EHV) connections at heights exceeding 4 m. Transformer designs do not include any [C.I.C].

Circuit breakers and disconnectors are predominantly of the air-insulated type with exposed HV and EHV conductors located upon supporting structures at heights exceeding 4 m. [C.I.C].

Capacitor banks and other reactive compensation equipment is usually located within locked chainwire mesh enclosures or a purpose designed building. These enclosures add an additional layer of security control to unauthorised access attempts.

Freestanding [C.I.C] are located within each switchyard. They are usually constructed of brickwork with sheet metal roofs. However, there are some [C.I.C] buildings constructed from sheet metal cladding in regional areas. Each [C.I.C].

A minority of terminal stations; located on small metropolitan Melbourne sites, have metal-enclosed gas-insulated switchgear located in conventional switchyards or within purpose designed buildings. In these cases the dead-front design of the equipment mitigates the safety risks associated with unauthorised persons approaching energised equipment.

The primary physical security feature for each terminal station is [C.I.C], fitted in many cases with [C.I.C] feature.

[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.

[C.I.C] to switch yard gates and control room doors and primary electrical equipment. [C.I.C] is restricted to trained personnel and managed via a single [C.I.C].

Signs warning of EHV equipment and of the dangers of unauthorised access and showing contact phone numbers are displayed at all sites. [C.I.C] alarms are common. Response systems include [C.I.C], attendance by police and contracted security agents and contingency plans.

5.2 Tower Lines

AusNet Services employs approximately 13,000 galvanised steel towers to support 120 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 [C.I.C].

Transmission lines comprising a single three-phase circuit or in some cases two three-phase circuits are predominantly located in dedicated easements within private property. Access to easements is controlled by [C.I.C]. Access to individual towers is controlled by [C.I.C] on each tower. [C.I.C].

[C.I.C] are only issued to staff and contractors who are formally trained and authorised to climb these towers. [C.I.C] are managed from [C.I.C] to ensure effective control.

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 EHV circuits in the 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. [C.I.C].

6 Risk Management

6.1 Threats

Geographically dispersed in all types of neighbourhood, [C.I.C] elements of the electricity transmission network present diverse security challenges. With potential impacts on members of the public, the local community and on the commercial viability of network owners / operators, these security threats have been classified as:

- 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 – use or threat of force or violence to influence government or public through fear or intimidation.

6.2 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; and
- Developing, exercising and maintaining contingency plans.

6.3 ISRAT

The 2015 versions of the Infrastructure Security Risk Assessment Tool (ISRAT) has been used to assess physical security risks and control measures in each terminal station[12] and generic risks for the multiplicity of transmission line towers[13]. 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; and
- Where a risk assessment has not been carried out for five years.

[12] 2015 Terminal Station ISRAT.xlsx AusNet Services July 2015.

[13] 2015 Transmission Line ISRAT.xlsx AusNet Services July 2015.

6.4 Risks

6.4.1 Terminal Stations

2015 Terminal Station ISRAT calculates the risks associated with unauthorised access events at terminal stations based on the following factors:

- [C.I.C].
- [C.I.C].
- [C.I.C].

The heat map below (Figure 1) illustrates the generic 2015 security risks for a typical terminal station:

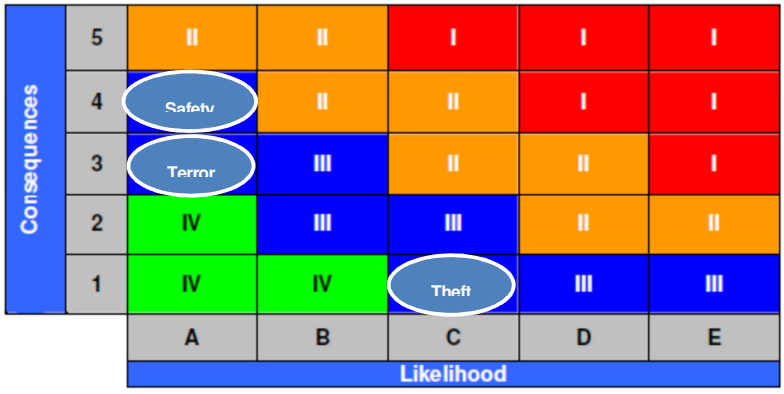


Figure 1 – 2015 Generic terminal station security risks

6.4.1.1. Higher Risk 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 2015 Terminal Station ISRAT:
[C.I.C].

6.4.1.2. Medium Risk Stations

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

6.4.1.3. Lower Risk Stations

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

6.4.2 Transmission Lines

2015 Transmission Line ISRAT calculates the generic risks associated with unauthorised access events on transmission line towers based on the following factors:

- [C.I.C].
- [C.I.C].
- [C.I.C].

The heat map below (Figure 2) illustrates the generic 2015 security risks for a typical transmission line:

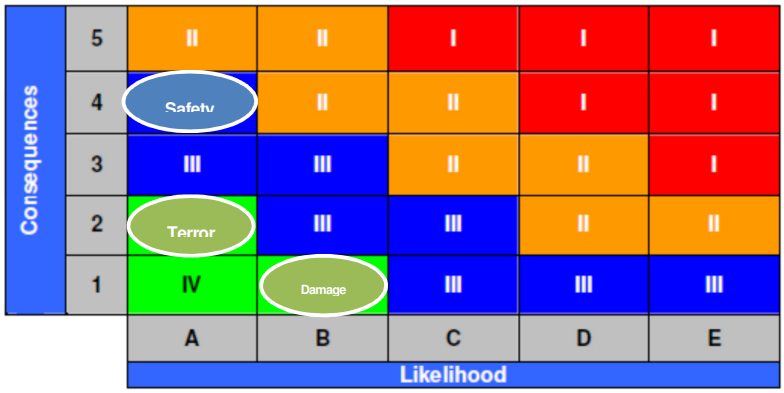


Figure 2 – 2015 Generic transmission line security risks

6.4.2.1. 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 [C.I.C].

7 Control Measures

7.1 Principles

Controls limit the extent of, and define the response to, a breach of security. It is acknowledged that, with portable power tools widely available, it is impractical to prevent determined persons from gaining unauthorised access to every site. Nevertheless, AusNet Services employs a range of security controls to deter would-be intruders, to delay and detect unauthorised entry events and to promptly respond to and/or recover from the impact of such entry. 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.

Sites are defined in a manner that discourages anti-social behaviour such as loitering, littering, graffiti and vandalism, which frequently precede unauthorised entry. Definition includes site delineation using [C.I.C] and extends to signs requesting that third parties report inappropriate behaviour.

Territorial reinforcement aims to deflect intruders toward softer targets through the use of obvious physical security measures such as [C.I.C] and extends to prompt removal of graffiti and repair of vandalism and the use of electronic security warning signs. To deflect potential intrusion attempts, sites are maintained in a neat and tidy manner with vegetation regularly trimmed, grasses mown and litter removed.

The contents of sites are securely stored. [C.I.C]

Natural surveillance involves surveillance zones through landscaping, where trees are pruned up and shrubs are trimmed down, to provide visibility of access points, site perimeter, buildings and equipment. This allows neighbours, staff or legitimate passers-by to scrutinise the activities of potential intruders. In particular, trees and shrubs are not established such that they mask visibility of the site perimeter or the switchyard interior.

7.2 [C.I.C]

7.2.1 Principles

[C.I.C] is designed to exclude persons not equipped with tools and delay access by those equipped with tools from selected areas of infrastructure sites.

The foundations and structural supports of [C.I.C] are designed to resist the manual efforts of potential intruders. [C.I.C] utilises robust materials such [C.I.C], arranged so as to minimise the possibility of unauthorised persons penetrating, scaling or undermining the [C.I.C].

The location, construction and use [C.I.C] are designed to complement the function of [C.I.C]. Particular attention is required to ensure [C.I.C] minimise scaling of the [C.I.C].

Where motor vehicles are assessed as credible risk, vehicular barriers such [C.I.C] are incorporated in the overall [C.I.C] design.

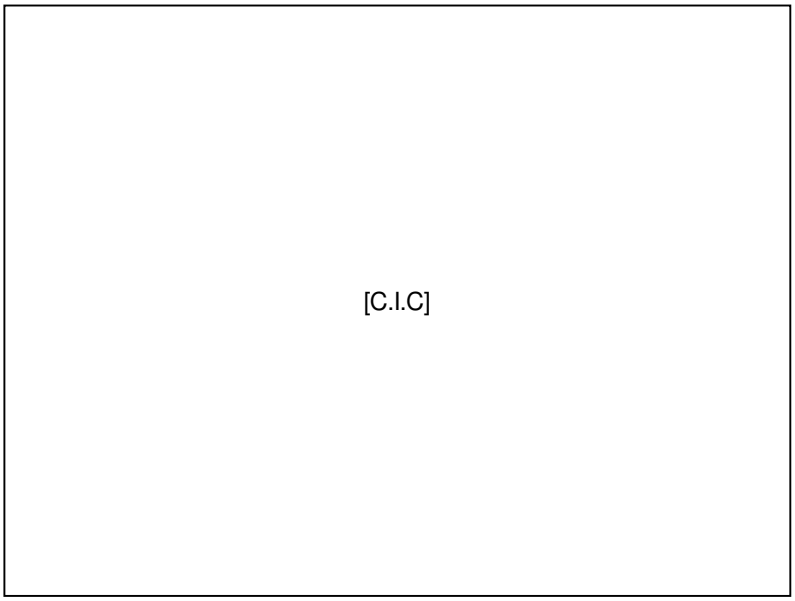
Where space permits at sites assessed as a higher risk of unauthorised access, 'clearance zones' are established immediately adjacent to [C.I.C] to minimise the threat of scaling by use of nearby aids such as vegetation or stored materials. If space is restricted, the total effective [C.I.C] is increased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

7.2.2 Higher Risk Sites

Where assessment indicates higher risks of unauthorised access; [C.I.C] may be constructed from [C.I.C][14] arranged as per SDM 05-1300[15] or equivalent [C.I.C]. At higher risk sites; existing [C.I.C] are enhanced with:

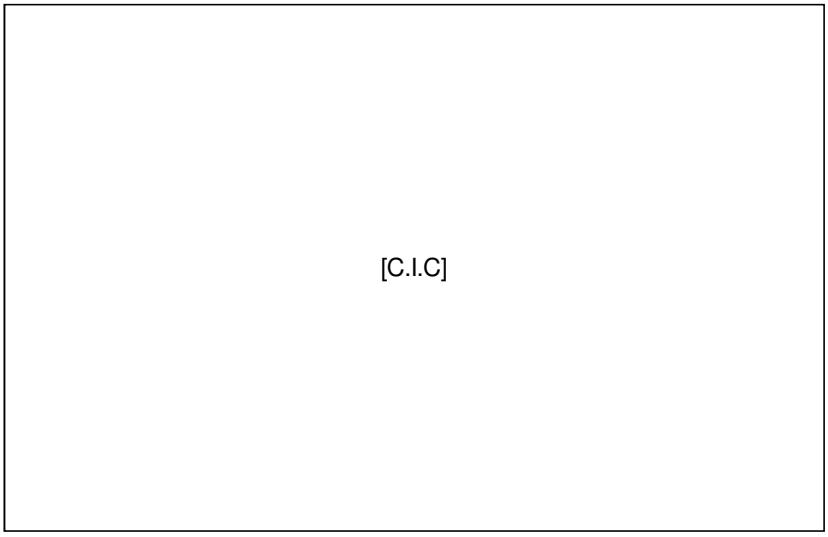
- [C.I.C]
- [C.I.C].

Figure 3 below illustrates a [C.I.C] with a continuous [C.I.C] feature suitable for higher security risk sites.



[C.I.C] is located on the inside of [C.I.C]. [C.I.C] installation shown in Figure 4 below includes [C.I.C].

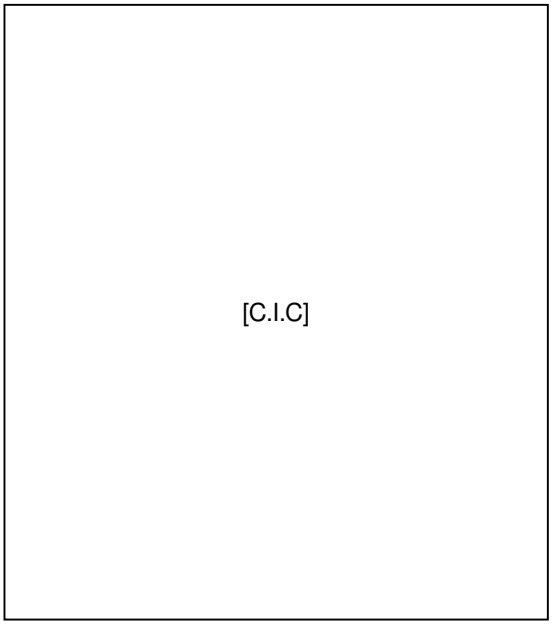
[14] [C.I.C].
[15] [C.I.C].



7.2.3 Medium Risk Sites

Where existing terminal stations are assessed as a medium risk of unauthorised access, [C.I.C][16] arranged as per SDM 05-1300[17]. [C.I.C]. At selected medium risk sites; [C.I.C] may be enhanced with [C.I.C].

A combination of [C.I.C] is used to restrict the ability of intruders to pass [C.I.C] shown in Figure 5 below.



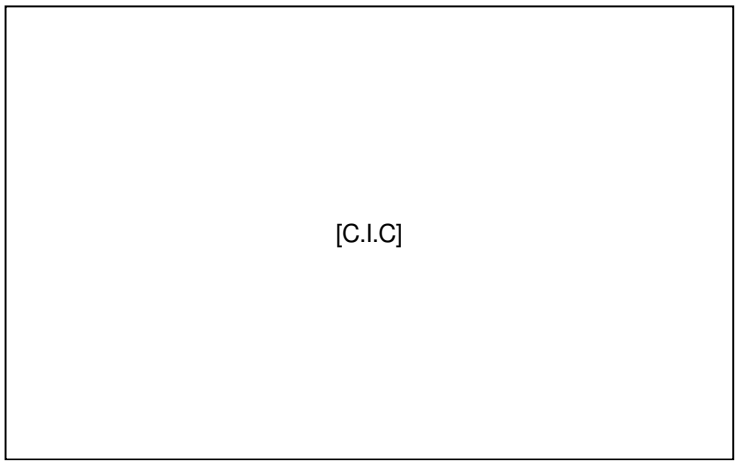
[16] [C.I.C].

[17] [C.I.C].

7.2.4 Lower Risk Sites

For existing terminal stations assessed as a lower risk of unauthorised access, [C.I.C]

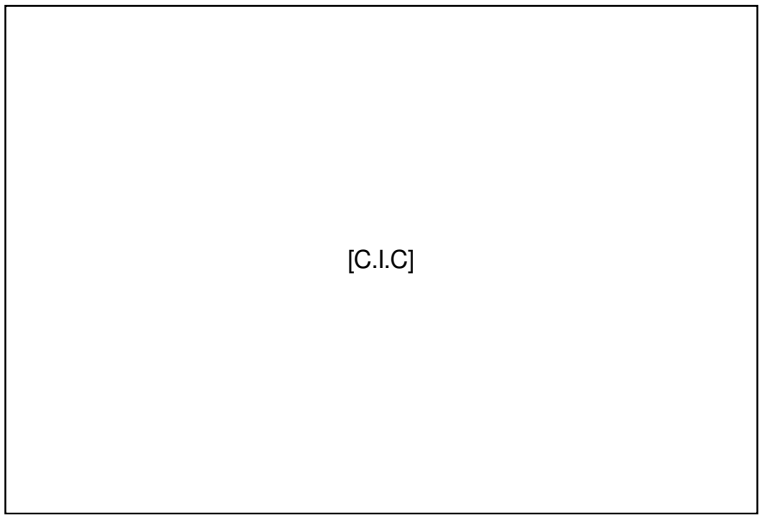
[C.I.C]. A combination of [C.I.C] is used to restrict the ability of intruders to pass [C.I.C] as shown in Figure 6 below.



7.3 [C.I.C]

[C.I.C] systems shall be installed on designated pedestrian gates and vehicle gates in each terminal station [C.I.C] and on designated external building doors leading to control and relay rooms.

[C.I.C] 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. [C.I.C]. [C.I.C]permit entry to authorised employees and contractors [C.I.C] similar to that illustrated in Figure 7 below.



7.4 Buildings

Buildings are to be constructed of robust materials such as brick, masonry or sheet metal cladding, arranged so as to minimise the possibility of unauthorised persons penetrating, scaling or undermining the building. Roofs are made of steel sheeting securely fastened to prevent removal. Building designs feature minimal climbing aids such as down-pipes, windowsills and architectural features.

External doors in new and re-furbished installations are [C.I.C]. Door strength and fire rating are not to be compromised by vents or windows; hardware has [C.I.C]. External openings to [C.I.C] similar to those shown in the following Figure 8 below.

Figure 8 – [C.I.C] Existing Windows

7.5 Locks and Keys

The operation of electrical equipment within switchyards shall be controlled by locksets and padlocks complying with AS 4145.

Entry points at terminal stations shall be minimised. The permanent removal of non-essential or under-utilised gates shall be considered. Entry points to terminal stations that are not fitted with [C.I.C] are secured with locksets and padlocks complying with AS 4145 – Mechanical Locksets for doors in buildings. Keys are only issued to staff, contractors and agents who are formally trained and authorised to enter specific areas and sites. [C.I.C].

Periodic replacement of locks and padlocks and re-issue of new keys to authorised persons is the most economic and pragmatic technique for managing lost, misplaced and stolen mechanical keys.

7.6 Signage

Installations are signed at entrance points and at regular intervals along the site boundary or security perimeter to achieve the following objectives:

- Display ownership of the property;
- Mandate controlled access by authorised persons;
- Provide contact phone numbers for emergencies, to report suspicious activity or seek return of lost property such as sports balls;
- Warn of occupational hazards such as HV or extreme operating pressures; and
- Warn of the use of electronic surveillance and alarms, and the use of security measures such as barbed tape, electric power fencing and Data Dot marking.

Signs are placed where they are noticeable and the message is clearly visible. They are secured in a tamper-resistant manner in locations that do not compromise other occupational hazard signs. As per AS 1319, where [C.I.C] tools are used, this is also signed along the perimeter.

7.7 Intrusion Detection

Commensurate with the level of assessed security risk, intrusion detectors shall be installed to detect and verify unauthorised access attempts. The Network Operation Centre shall monitor intrusion alarms and respond in accordance with procedures established in SPIRACS Volume 5 Part 2 Security Management Framework and AS 2201 and AS 4421.

7.7.1 Site Perimeter

[C.I.C] perimeter detectors such as the [C.I.C] installed on existing security fences as stand-alone systems or in conjunction with [C.I.C]to detect attempts to penetrate, scale or undermine the security fence.

7.7.2 Site Interior

[C.I.C] installed to monitor access points, switchyards and buildings within [C.I.C] sites. Options include permanent installations to monitor sustained security risks and temporary installations to monitor time-specific risks such as construction projects. [C.I.C] placement will be determined on a site specific basis.

[C.I.C] can operate in [C.I.C]to detect, verify and assist the response to unauthorised access attempts. Access to [C.I.C] is restricted to authorised personnel, as per AusNet Services' policy [C.I.C]

7.7.3 Building Interior

[C.I.C] and [C.I.C] may be used [C.I.C] to detect unauthorised access.

7.8 Lighting

Security for terminal stations incorporates lighting designed to:

- Deter nearby anti-social behaviour;
- Deter unauthorised access;
- Facilitate identification of unauthorised access activity; and
- Assist staff and security personnel in responding to network events and unauthorised access attempts.

The standard and extent of lighting and the sophistication of lighting controls is matched [C.I.C]. 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.

[C.I.C], supplementary lighting will enable [C.I.C] and facilitate response to unauthorised access attempts. When planning [C.I.C] the following factors should be considered:

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

7.9 Patrols and Monitoring

Security guards are contracted to monitor equipment and materials at construction sites and to respond to security events at operational sites. The extent and sophistication of security monitoring is [C.I.C]

7.10 Inspection Testing Maintenance and Auditing

Commensurate with the assessed level of security risks:

- Sites are inspected for indications of unauthorised entry; and
- 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. [C.I.C], 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, [C.I.C]. 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; and
- Relevancy and adequacy of established policy, procedures and standards.

7.11 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.

8 Strategies

8.1 Terminal Stations

8.1.1 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].
- [C.I.C].
- [C.I.C].
- [C.I.C].
- [C.I.C].
- [C.I.C].
- [C.I.C].
- [C.I.C].
- [C.I.C].

8.1.2 High Risk

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

- [C.I.C].
- [C.I.C].
- [C.I.C].
- [C.I.C].
- [C.I.C].
- [C.I.C].
- [C.I.C].
- [C.I.C].
- [C.I.C].
- [C.I.C].
- [C.I.C].

8.1.3 Medium Risk

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

- [C.I.C].
- [C.I.C].
- [C.I.C].
- [C.I.C].
- [C.I.C].
- [C.I.C].
- [C.I.C].
- [C.I.C].
- [C.I.C].

8.1.4 Low Risk

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

- [C.I.C].
- [C.I.C].
- [C.I.C].
- [C.I.C].
- [C.I.C].
- [C.I.C].
- [C.I.C].
- [C.I.C].

8.2 Transmission Lines

8.2.1 High Risk Lines

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

- [C.I.C]
- [C.I.C].

8.2.2 Low Risk Lines

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

- [C.I.C].