Part of Energy Queensland

Substation Standard

Network Physical Security – Design Reference

These standards created and made available are for the construction of Energy Queensland infrastructure. These standards ensure meeting of Energy Queensland's requirements. External companies should not use these standards to construct non-Energy Queensland assets.

If this standard is a printed version, to ensure compliance, reference must be made to the Energy Queensland internet site www.energyq.com.au to obtain the latest version.

Approver	Carmelo Noel General Manager Asset Standards
If RPEQ Sign-off required insert details below.	
Certified Person Name and Position Title	Registration Number
John Lansley Manager Substation Standards	RPEQ 6371

Abstract: This standard is designed to outline the security requirements for the design of Energy Queensland substations

Keywords: Fence, security, substations

Network Physical Security – Design Reference

CONTENTS

FIGURES

TABLES

1 Overview

1.1 Purpose

The purpose of This Document is to provide guidance to achieve a consistent approach to applying physical security controls for Network assets and is targeted at EQL internal stakeholders, consultants and architects for the design and application of physical security controls consisting of electronic security systems. This document is not intended to be a detailed design.

This Document does not cover physical security for Non-Network Assets such as corporate offices, depots, distribution centres, training centres, pole yards. Please refer to the Non-Network Physical Security Design Reference for guidance on the physical security controls available for Non-Network assets.

1.2 Scope

The scope of This Document is limited to guidance on the provision of physical security measures for Network Assets including:

- Bulk Supply Substations
- Zone Substations
- Commercial and Industrial Substation
- Standalone telecommunications sites.

This Document recognises that in some applications and circumstances logical security treatments (such as those implemented by the Digital Office) will also contribute to security risk reduction, as part of a layered approach.

Generation assets associated with isolated systems will be covered under separate documentation from the Renewables & Distributed Energy Group.

1.3 Asset/Risk Owners

The asset owner is accountable for the asset or group of assets with a responsibility to ensure control measures are implemented appropriately to reduce the risk exposure to an acceptable level.

1.4 Designers

This Document is a guidance document and is intended to be read at a high level only. Details on design and installation requirements associated with the implementation of security control measures may reside in sources flagged in Section 1.10 Reference sources.

It is the responsibility of the designer to complete all relevant site investigations and identify all relevant compliance requirements and approvals (both EQL and external) required to complete the design and construction of security measures referred to in This Document and any specific, relevant project or contract documentation.

1.6 Non-prescription

The physical security treatment measures detailed in This Document are not meant to be prescriptive in nature or requirement. Ultimately, the treatment of the security risks is achieved by applying the results of a security risk assessment and/or as per the general advice provided in This Document to ensure the ongoing availability, continuity and resilience of all Network Assets.

1.7 Audience

This document is primarily intended for:

- EQL Network planners, designers and project managers
- EQL Line Management
- EQL Operational Telecommunications staff.

Additionally, This Document should also be referred to by the following external stakeholders with respect to the design, implementation and management of security for Network Assets:

- Architects
- Builders
- Electrical Engineers
- Consultants
- any other organisation or person responsible for the design of physical security of EQL people or physical assets.

1.8 Limitations

This document does not contain any site-specific information, nor should it be considered a detailed or complete design.

It is the responsibility of the EQL designer, service provider, engineer or security system designer to complete all required site investigation and design in compliance with the requirements of this document and the contract for which they have been engaged by EQL.

1.9 Enquiries

Any enquiries are to be forwarded to corporatesecurity@energyq.com.au for review and response.

2 References

2.1 Legislation, regulations, rules, and codes

Queensland Electrical Safety Act, 2002 (Queensland Government)

Queensland Electrical Safety Regulation, 2013 (Queensland Government)

Queensland Electricity Act, 1994 (Queensland Government)

Queensland Electricity Regulation, 2006 (Queensland Government)

Queensland Work Health and Safety Act, 2011 (Queensland Government)

Queensland Work Health and Safety Regulation, 2011 (Queensland Government)

Queensland Government CPTED Part A & B Guideline

Information Privacy Act 2009 (Qld)

Public Records Act 2002 (Qld)

Security Providers Act 1993 (Qld)

Queensland Government CCTV Guidelines

Queensland Government Information Standard 18: Information Security

Queensland Government Information Security 31: Retention and disposal of public records

Queensland Government Information Standard 40: Recordkeeping

Managing CCTV records – Guideline for Queensland Public

Security of Critical Infrastructure Act 2018 (Federal Government)

Federal Government, Protective Security Policy Framework – PSPF

2.2 Energy Queensland controlled documents

Physical Security of Network Assets (STNW3434) – 8723887

Network Key Management Standard (STNW3435) - 8719649

Corporate Security - CCTV Guideline (R151) - 690969

Corporate Security - ID Card Guideline (R153) - 690523

Corporate Security – Access Control Guideline (R154) - 687278

Corporate Security - Security of Sites, Assets and Materials (R137) - 691300

Corporate Security – Physical Security Technical Reference (R296) - 691017

Enterprise Risk Management Standard (R271) - 689958

Risk Evaluation Matrix (R056) - 691861

2.3 Other sources

Intruder Alarm Systems, AS/NZS 2201 Set

CCTV, AS/NZS 4806:2008-Set

Lightning Protection, AS/NZS 1768:2021

Risk Management – Principles and Guidelines, AS/NZS ISO 31000:2018

Chain-link fabric security fencing and gates – General Requirements, AS 1725.1:2010

Substations and high voltage installation above 1kV ac, AS 2067:2016

Electric Security Fence, AS/NZS 3016:2002

Guards and Patrol Security, AS/NZS 4421:2011

National Guidelines for Prevention of Unauthorised Access to Electricity Infrastructure,

ENA DOC 015-2022

Security Risk Management Handbook, HB167:2006

A spreadsheet tool and reference guide which standardises the approach towards completing security risk assessments for EQL Network Assets, Network Security Risk Resolver Assessment Tool and accompanying guide

Provides guidance on achieving a consistent approach to determining physical security controls, Australian Government – Physical security management guidelines

A document which describes the business requirements for perimeter security across its asset base, Corporate Security - Perimeter Security Guideline (draft)

A document which describes the business requirements for physical security for EQL sites which are under construction, Corporate Security - Security in Construction Guideline (draft)

3 Definitions and abbreviations

3.1 Definitions

For the purposes of this standard, the following definitions apply.

Asset/Risk owner	The group responsible for management of the asset
Network Asset	Infrastructure directly used for the transmission/distribution of electrical energy, including communications infrastructure supporting these assets.
Primary Controls	Physical deterrents to unauthorised access such as fences, gates, locks etc
Secondary Controls	Surveillance, thermal cameras, alarms to detect unauthorised access
This Document	STNW3039

3.2 Abbreviations

This list does not include well-known unambiguous abbreviations, or abbreviations defined at their first occurrence within the text.

a.c.	Alternating current
CCTV	Closed circuit television system
ENA	Energy Networks Association
EQL	Energy Queensland Limited
GIS	Gas insulated switchgear
HV	High voltage
LED	Light emitting diode
MPLS	Multiprotocol label switching
MV	Medium voltage
MVA	Mega Volt Amp
OTN	Operational telecommunications network

PA	Public address
PE	Photo-electric
PTZ	Pan-tilt-zoom
QoS	Quality of service
QPS	Queensland Police Service
RTU	Remote terminal unit
SMS	Security management system
SOCI	Security of Critical Infrastructure Act - 2018
SRA	Security risk assessment
STPIS	Service Target Performance Incentive Scheme
VLAN	Virtual local area network
VOIP	Voice over internet protocol

4 Approach

4.1 General

Baseline security controls are identified as items or devices used to provide a minimum level of security, typical examples used are:

- Defined perimeter (i.e., fence, gates, doors etc.)
- Nominated entry points (i.e., doors or gates requiring restricted key system or access control for entry)
- Monitoring of entry points (i.e., reed switches on doors, detection devices)
- Surveillance (i.e., natural surveillance by maintaining clear unobstructed fence lines, continual observation by EQL staff and CCTV systems)
- Securing attractive or valuable items (i.e., locking copper and tools in secured containers).

4.2 Philosophy

This design reference provides guidance on the baseline requirements for the implementation of security measures within EQL owned or operated Network Assets (substations).

This document provides advice on the application of approved security controls relative to the operational areas associated with an asset or sub-asset (See Figure 1):

- Zone 1: The boundary of the Network Asset (e.g., substation perimeter), taking in all assets enclosed within the perimeter
- Zone 2: Facilities, control buildings, switch rooms, fully enclosed transformer rooms, sheds, generator compounds etc within Zone 1

- Zone 3: Equipment rooms with exposed HV terminals, and/or rooms within Zone 2 containing sensitive equipment in racks and/or enclosures.

(Note all HV enclosures shall comply with the requirements of AS2067, Electrical Safety Act, Energy Queensland rules and plant and equipment standards).

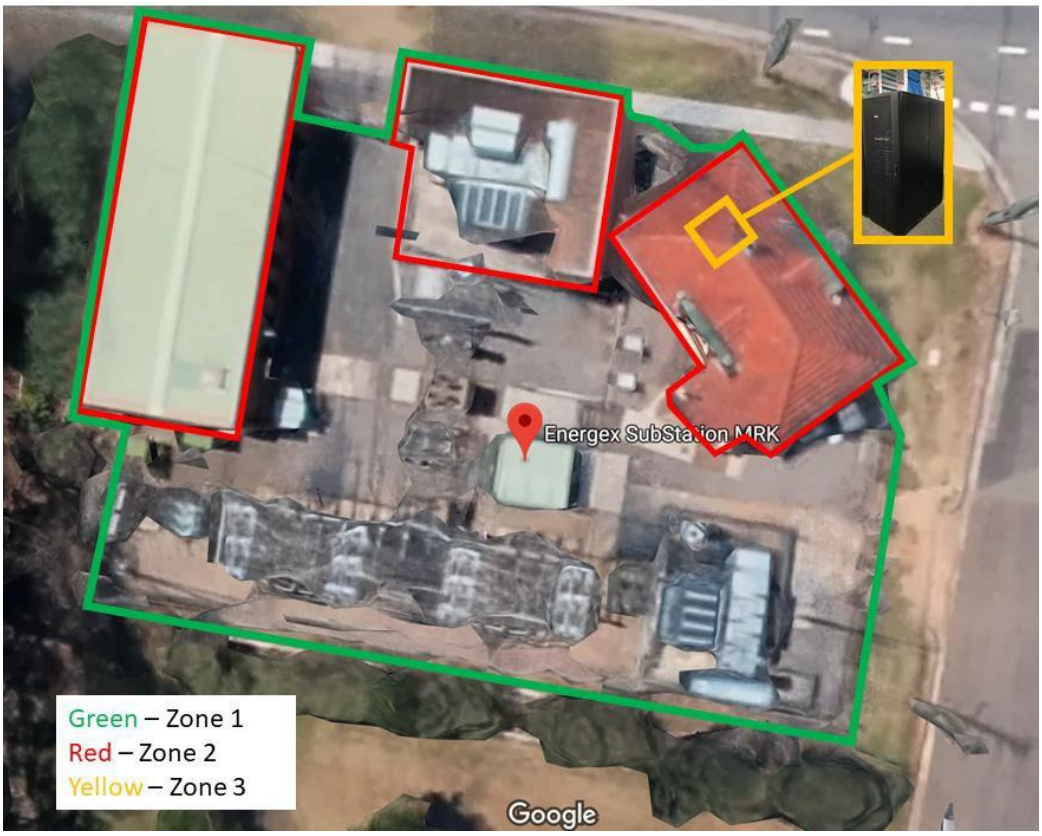

Figure 1 Definition of Zones in Substation

The level of security assurance is relative to the risk profiling, application of security controls and site management of security procedures. The zone type is the reference term used to identify operational areas, each with a range of recommended security controls. Generally, access to operational areas shall progressively increase through the application of multiple layers of physical and logical security controls, to increase the 'Security-in-Depth' of the Asset.

This Document also recognises that in some cases the application of multiple concentric security measures will not be achievable (for example, at a non EQL controlled site) and asset protection will be limited to standalone measures implemented at the discretion of the Asset/Risk Owner.

4.3 Security Risk Assessment (SRA)

A Security Risk Assessment must be completed prior to the project approval stage so that sufficient funds may be allocated to the project. The level of assessment depends on the classification of the asset (see Section 3.2)

- Critical - Refer to EQL Security Risk Assessment process for further details. To be conducted by Corporate Security team or their representative

- High, Significant or Limited – using the Resolver SRA tool.

All results shall be recorded in the Resolver database. The relevant manager identified in the risk assessment shall sign off on the level of security risk. Measures identified in Section 5 can be used to reduce the level of risk. See Section 11.2 of R271 for escalation and ownership of risk response.

Table 1 - Risk Response (ref Section 11.2 R271)

Risk Level	Sustainable	Minor	Medium	High	Extreme
Escalation & Ownership	Supervisor or Frontline Manager	Area or Department Manager	General Manager	Executive General Manager (escalation & ownership) Subsidiary Board and Risk and Compliance Committee (escalation for oversight)	EGM (escalation & ownership) CEO (Risk and Compliance Committee and EQL Board (escalation for oversight)
Action	Monitor the risk for any change. Maintain and / or monitor existing controls to ensure they continue to be effective. Monitor internal and external changes to the portfolio's environment.		Risk may be accepted with effective controls in place.	Activity must not commence or continue until the Risk Owner has approved the risk. If applicable, suspend or pause the activity so long as it is safe to do so.[5]	Suspend / terminate the activity immediately so long as it is safe to do so. Immediately report to the relevant EGM to report the risk to the CEO detailing control effectiveness and identified treatments to reduce the risk level.
	For health and safety risks demonstrate i.e., provide evidence and justification the risk is managed SFAIRP.		For health and safety risks demonstrate i.e., provide evidence and justification risk managed SFAIRP. For all other risks consider the EQL Risk Appetite to determine the appropriate response.		For health and safety risks, activity must not commence or continue until applied controls reduce the risk level.
			• If residual risk level within RAS, accept the risk and document the reasons. • If the residual risk level indicates a potential breach of the Board Approved Risk Appetite Statement, advise Risk Owner immediately. Risk Owner will need to make decision as to whether to accept the risk or not. If outside of RAS, a detailed Risk Management Action Plan including proposed controls / treatments to be implemented as soon as practicable to lower the residual risk to within appetite will be required. This will need to be supported by regular review of existing controls for effectiveness as well as monitoring and confirmation of effectiveness and timely implementation as per agreed action plan.		
Review	Annual Review		Six Monthly Review	Quarterly Review	Monthly Review

4.4 Primary Controls

Primary Controls are used to identify the property boundary and is defined by installation of a fence and access gates. The following documents detail the minimum design criteria for primary controls:

a) ENA DOC 015 – National Guidelines for the Prevention of Unauthorised Access to Electricity Infrastructure; and

b) AS 2067:2016 – Substations and High Voltage Installations Exceeding 1 kV a.c.

c) STNW3434 – Physical Security of Network Assets

Where not specifically directed by the results of a security risk assessment, EQL Network planners and designers shall refer all fence and gate design requirements to the above two standards and the relevant internal fence/gate specifications/drawings. The site risk assessment and/or business specific requirements may trigger additional security controls (referred to in ENA-015 as secondary security controls) as shown below.

This Document may also refer to Primary Controls associated with architectural elements of the Asset yet omits provision of any specific guidance on their implementation. Designers are required to identify and reference relevant EQL documentation with regards to architectural related Primary Controls.

4.5 Fences

Perimeter fences shall be one of the following types:

4.5.1 Chain-link Fence

Comply with the requirements of AS1725.1-2010, heavy duty with 50mm diamond construction. The addition of an electric fence behind the chain link fence may be a consideration where additional security may be required. For further details see drawings S10000301 (all sheets).

4.5.2 Anti-climb Fence

Where greater security is required, perimeter fencing shall be of the anti-climb variety. This can include:

- Solid brick walls with barbed wire topper
- Welded mesh (eg 358 Mesh)
- Corrugated mesh (eg. Corromesh 358)

The welded and corrugated mesh shall be made of high quality wire to AS4534-2006. The design and manufacture shall be to EN1022-2012 for high security applications.

Palisade fences are not acceptable for this application.

4.5.3 Temporary Fences

Where a temporary fence is required during project staging, refer to drawing S1000301-05 for details. Note that modular fence panels of similar height and barbed wire topping can be used between posts that are buried in ground and holes filled with compacted no fines concrete or stabilised sand.

4.5.4 Secondary fence mesh

As an additional measure to improve security on existing chain link fences, an option is to install a welded mesh fence material behind the existing chain-link fence wire from the bottom the fence to a height of 1.2m as per Figure 2 below:

Figure 2 - Secondary fence mesh installed on existing chain link fence

This measure is a deterrent to unauthorised access via cutting the chain link fencing, and can be used where there have been repeated break-ins in this manner. Provided this mesh is secured to

the existing posts,rails and fence with multiple secure metallic ties, no additional earthing to this mesh need be installed.

4.6 Key Management

Requirements for physical security of network assets are documented in STNW3434.

Key management is one control to manage access to network assets, and these requirements are documented in STNW3435 Network Key Management Standard and in R154 Access Control guidelines.

4.7 Secondary Controls

Secondary Controls consist of additional security hardware to assist in providing the management of authorised access or to add another layer of security to the primary control. ENA Doc-015 outlines typical secondary controls that can be implemented in substations. EQL Corporate Security can provide additional design input and advice for secondary controls where there may be site specific influences that do not fit within the standard substation design. Examples of secondary security controls may consist of:

a) Access Control Systems
b) Intrusion Detection Systems
c) Closed Circuit Television (CCTV)
d) Electric Fence/Fence Detection Systems
e) Intercom System and Public Address (PA) systems; and
f) Perimeter Intruder Detection Systems.

4.8 Communications and cabling

Security cameras, IP PA speakers and other networked secondary controls shall be installed on their own VLAN. In general, they will have their own network switch, although in cases where there are only one or two devices and there is room on the existing network switches these may be used, provided at least one port remains available on each switch for OTN use, Security systems in secondary buildings shall have a separate subnet as well. Further advice can be obtained from Telecommunications Department.

Preference is for cabling from the VLAN to secondary control devices to be fibre optic cables. If copper cable is used (Ethernet, RS485), it shall be screened or run in a separate conduit to power cables to avoid problems with electrical induction.

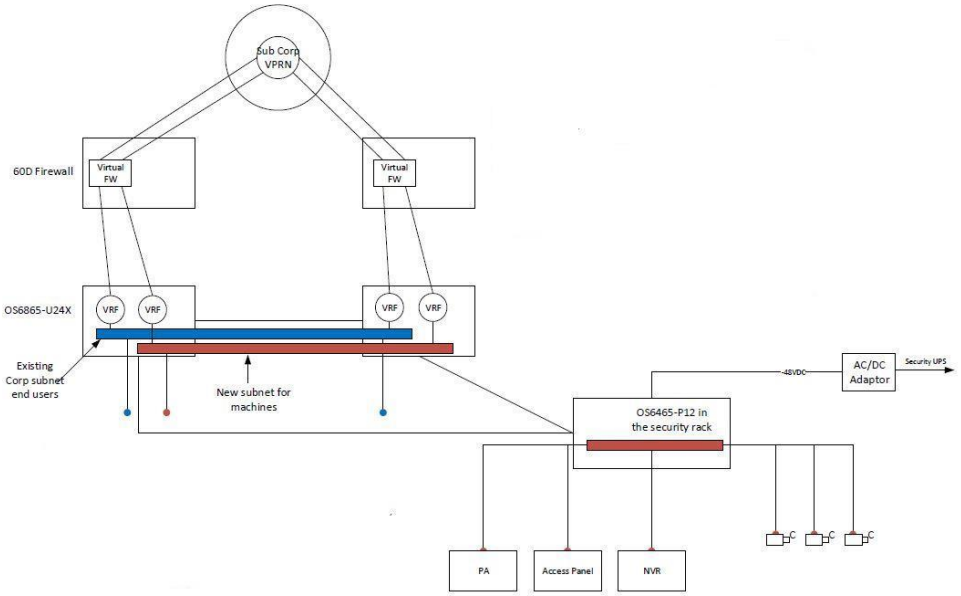

Figure 3: Typical Telecommunications configuration

5 Security Design Standards

The underlying principle in applying baseline physical security controls is to limit unauthorised access while being able to accurately identify and record details relating to authorised personnel access to Network assets.

This section provides a high-level view of 'Security-in-Depth' principles and how the asset classification, asset types and different work areas within these locations are required to have a diverse range of security controls.

5.1 Security-in-depth

EQL applies a 'Security-in-Depth' approach towards physical security controls to reduce the likelihood and severity of attacks from malicious actors and to ensure high-voltage enclosures are not readily accessible by unauthorised persons. A more resilient security environment is achieved by the layering of different types of physical security controls which will together provide greater protection of EQL people, assets and information.

Security controls when applied in a 'Security-In-Depth' approach shall be designed to Deter, Detect, Delay, Deny and Respond to a source of security threat.

The relationship between detecting the breach and the response process is illustrated in Figure 4:

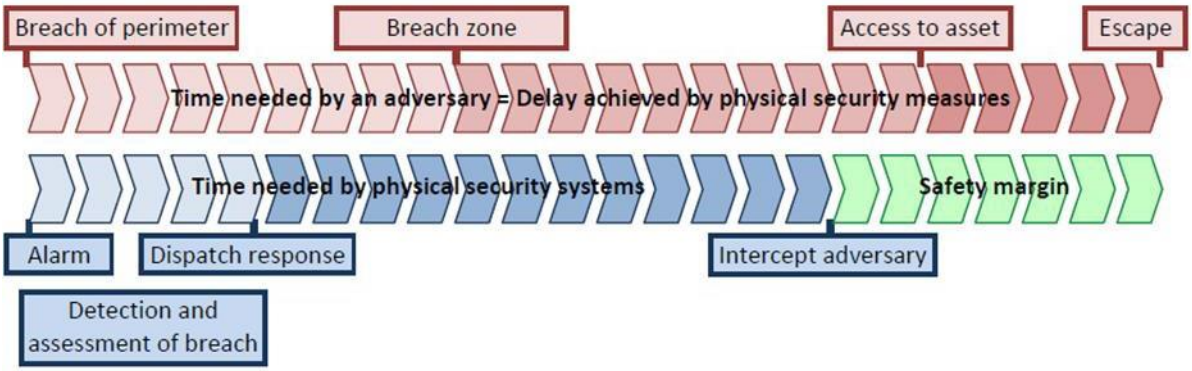

Figure 4: Breach and response

5.2 Asset classification and security controls

An EQL Network Asset can be classified as either:

- Critical
- High
- Significant; or
- Limited.

The classification of an EQL Network Asset is based on the level of importance it has to the business. The criterion used to determine Asset Classification has been developed by EQLs Corporate Risk Group and considers several factors influencing the organisations risk exposure in the event a Network Asset is lost, compromised or functionally degraded.

EQL Network Asset/Risk owners should refer to the following guidance published by the Corporate Risk Group when determining the classification of a Network Asset:

- EQL Standard R271 – Enterprise Risk Management Standard
- EQL Reference R056 – Risk Evaluation (Consequence & Likelihood) Matrix

The classification of the asset will carry implications for the protective security measures required for its protection. Additionally, certain assets may require a balanced approach as the asset may reside within certain locations/buildings/sites which do not fall into any specific category. In this case, EQL Corporate Security can provide guidance to the business and assess the security to determine the most appropriate security controls.

As a guide, the following table may offer criteria for evaluation of the asset classification:

Table 2 - Criticality guide

Asset Classification	Asset Type	Impact to Community
Critical	Installed transformer capacity ≥100MVA SVC: provides network stability for load and major embedded generation Connection asset market participant ≥100MVA Telecommunications sites containing centralised Telecommunication network management systems Key strategic node sites containing MPLS, Microwave and TDM (SDH / PDH) networks	≥ 20,000 customers or significant CBD loads Load at risk > 50MVA Major industrial customers whose production is critically affected by even short time outages (refineries, smelters) Severe community outrage at loss of service Outage would cause severe impact on CBD reliability/STPIS
High	Installed transformer capacity 50 – 99 MVA Connection asset market participant between 30 and 100MVA Telecommunications sites containing: • One or more MPLS nodes • Multiple DB2 / DB4 or DM2 PDH multiplex equipment • Single DN2 node	Between 10,000 to 20,000 customers Load at risk 25-50 MVA Major customers whose may have backup generation but may be affected by long time outages (hospitals, shopping centres) Community outrage if extended loss of service Outage would cause severe impact on urban reliability/STPIS
Significant	Installed transformer capacity 20 - 49 MVA Telecommunications sites containing: • MPLS long line switch / CE node • Single DB2 / DB4 or DM2 PDH node	2,500 to 10,000 customers Load at risk 10-25 MVA Community upset at loss of service Outage would cause moderate impact on urban or severe impact on rural reliability/STPIS
Limited	Installed transformer capacity <20 MVA Telecommunications sites containing simple modem	Less than 2 500 customers Load at risk < 10 MVA Community disquiet at loss of service Outage would cause moderate impact on rural reliability/STPIS

Where one criteria may be higher than another the higher classification shall be taken for the asset.

5.3 SOCI and Critical Electricity Assets

SOCI Act was enacted o protect the essential services all Australians rely on by uplifting the security and resilience of critical infrastructure. Critical electricity assets are defined as:

- a network, system, or interconnector for electricity transmission or distribution for at least 100,000 customers

Part 2A of this act requires entities to undertake a risk management program for the critical infrastructure asset. The responsible entity must report annually on its risk management program. To support this program, critical electricity assets should include where possible:

- Access control to monitor access
- Anti-climb security fencing to prevent unauthorised access
- Secondary controls such as video surveillance.

Further clarifications will be provided in future editions of this standard.

6 Security Zones

Following the classification of a Network Asset by the Asset/Risk owner, the Asset/Risk owner must assess the requirement for completion of a security risk assessment, including application of protective security zones to achieve an appropriate level of 'Security-in-Depth' for the site.

The table below outlines security zones typically associated with an Asset, based on their classification. It also provides guidance on when the security risk assessment process should be adopted, based on Asset classification (refer Figure 1 for definition of zones):

Table 3 - Security zones

Asset Classification	Zone 1	Zone 2	Zone 3	SRA
Critical	✓	✓	✓	Mandatory
High	✓	✓	✓	Highly recommended
Significant	✓	✓		Recommended
Limited	✓			Discretionary

6.1 Treatment guidance matrix

The matrix below establishes a series of baseline security treatments at the disposal of an EQL Asset/Risk owner to reduce inherent security risk exposure.

The EQL Asset/Risk owner is responsible for the selection and implementation of treatment measures, based on site limitations and constraints influencing inherent risk levels and the specific assets' operating environment.

Table 4 - Treatment matrix

TREATMENT/MEASURE	CRITICAL			HIGH			SIGNIFICANT			LIMITED		
	Z1	Z2	Z3	Z1	Z2	Z3	Z1	Z2	Z3	Z1	Z2	Z3
Chain-link perimeter fence to AS 2067 & AS 1725				●			●			●		
Anti-climb perimeter fence to ENA-015 & EN 10223-2012	●			●								
Gates to same standard as perimeter fence	●			●			●			●		
Commercial grade locking systems	●	●		●	●		●	●		●	●	
Protected padlock and chain	●			●			●			●		
Window grilles and locks		●			●			●		●		
External LED lighting with auto sensor PE	●			●								
Perimeter video surveillance, (PTZ)	●			●								
Asset video surveillance			●									
General video surveillance	●	●		●	●		●	●				
Electronic access control, entry reader	●	●		●	●		●	●		●		
Intruder alarm system coverage (perimeter)	●	●		●	●			●			●	
Intruder alarm system coverage (internal)		●			●			●			●	
TREATMENT/MEASURE	Z1	Z2	Z3	Z1	Z2	Z3	Z1	Z2	Z3	Z1	Z2	Z3

TREATMENT/MEASURE	CRITICAL			HIGH			SIGNIFICANT			LIMITED		
	Z1	Z2	Z3	Z1	Z2	Z3	Z1	Z2	Z3	Z1	Z2	Z3
Perimeter Intrusion Detection				●								
Electric Fencing System	●											
IP PA speaker for VoIP announcements	●			●			●					
Security signage	●	●		●	●		●	●		●		
Arm/disarm indicator	●	●		●	●		●	●		●		

7 Implementation Guidance

7.1 Security of 'Critical' assets

The table below provides guidance on the selection and implementation of physical security control measures associated with security zones for assets classified as 'Critical':

Table 5: Critical substation recommendations

No.	Function	Guiding Principles
1	Zone 1 – Generally operational areas within the perimeter fence/yard area containing outdoor HV plant and Zone 2 enclosures. Includes substation earth grid and connections, and any equipment stored permanently or temporarily at site.	Unless directed otherwise by the results of a security risk assessment, Zone 1 areas for 'Critical' Assets should be implemented as follows: • Anti-climb perimeter fencing to ENA-015 and Section 4.5.2, inclusive of anti-tunnel measures • Full height pedestrian gates to control primary pedestrian entry/egress • Electric fence for the full perimeter of the site (Note – shared fences may need to be solid to prevent landscaping from neighbours interfering with electric fence operation) • Primary perimeter entry/exit points to be monitored and controlled by the intruder detection and access control system, entry reader • All other perimeter gates are to have a protected padlock and chain based on EQL restricted keying system • Fixed CCTV cameras to view nominated access path from perimeter gate to entry doors of buildings • Fixed CCTV cameras to provide general coverage of typical movement areas around buildings • PTZ cameras located on buildings to provide as much coverage of the perimeter electric fence (maximum 2 x PTZ cameras) • Low level LED lighting operated by PE cell to support CCTV and natural surveillance • Arm/Disarm indicators as indicated by the specification or shown on standard drawings • External environmental enclosure to accommodate security equipment if the security equipment is not located inside the control buildings • IP PA speaker for voice announcements • Security and electric fence signage • All transformers are enclosed, or if outdoors have HV and LV cable boxes ***where practical***. Consideration given to indoor GIS and cable entry to eliminate exposed busbars ***where cost justifiable***.

No.	Function	Guiding Principles
2	Zone 2 – Facilities, control buildings, switch rooms, enclosed transformer compounds, sheds, generator compounds etc.	Unless directed otherwise by the results of a security risk assessment, Zone 2 areas for 'Critical' Assets should be implemented as follows: • All primary entry/exit perimeter doors to be provided with access control monitored and controlled by the EQL corporate intruder detection and access control system, entry reader • All other doors/openings to be provided with door monitoring device connected to the alarm system
		• Motion detectors to be provided to rooms with external windows or doors on ground floor; and higher floors if accessible from external of the building • Registered lock and key cylinders • Security signage • Arm/Disarm indicators as indicated by the specification or shown on standard drawings • All MV and GIS switchgear installed within Zone 2 secured building.
3	Zone 3 – Equipment rooms,	No specific additional security measures, unless specifically identified as part of a site risk assessment. If required additional measures could include: • CCTV oversight of the target asset

7.2 Security of 'High' assets

The table below provides guidance on the selection and implementation of physical security control measures associated with security zones for assets classified as 'High':

Table 6: High substation recommendations

No.	Function	Guiding Principles
1	Zone 1 – Generally operational areas within the perimeter fence/yard area containing outdoor HV plant and Zone 2 enclosures. Includes substation earth grid and connections, and any equipment stored permanently or temporarily at site.	Unless directed otherwise by the results of a security risk assessment, Zone 1 areas for 'Critical' Assets should be implemented as follows: • Either Chain-link perimeter fencing to ENA-015, inclusive of anti-climb and anti-tunnel measures, or • Anti-climb perimeter fencing to ENA-015 and Section 4.5.2, inclusive of anti-tunnel measures • Full height pedestrian gates to control primary pedestrian entry/egress • Where chain link fence used, electric fence for the full perimeter of the site (Note – shared fences may need to be solid to prevent landscaping from neighbours interfering with electric fence operation) • Primary perimeter entry/exit points to be monitored and controlled by the intruder detection and access control system, entry reader • All other perimeter gates are to have a protected padlock and chain based on EQL restricted keying system • Fixed CCTV cameras to view nominated access path from perimeter gate to entry doors of buildings • Fixed CCTV cameras to provide general coverage of typical movement areas around buildings • PTZ cameras located on buildings to provide as much coverage of the perimeter electric fence (maximum 2 x PTZ cameras) • Low level LED lighting operated by PE cell to support CCTV and natural surveillance • Arm/Disarm indicators as indicated by the specification or shown on standard drawings • External environmental enclosure to accommodate security equipment if the security equipment is not located inside the control buildings • IP PA speaker for voice announcements • Security and electric fence signage • All transformers are enclosed, or if outdoors have HV and LV cable boxes ***where practical***. Consideration given to indoor GIS and cable entry to eliminate exposed busbars ***where cost justifiable***.

No.	Function	Guiding Principles
2	Zone 2 – Facilities, control buildings, switch rooms, enclosed transformer compounds, sheds, generator compounds etc.	Unless directed otherwise by the results of a security risk assessment, Zone 2 areas for 'Critical' Assets should be implemented as follows: • All primary entry/exit perimeter doors to be provided with access control monitored and controlled by the EQL corporate intruder detection and access control system, entry reader • All other doors/openings to be provided with door monitoring device connected to the alarm system
		• Motion detectors to be provided to rooms with external windows or doors on ground floor; and higher floors if accessible from external of the building • Registered lock and key cylinders • Security signage • Arm/Disarm indicators as indicated by the specification or shown on standard drawings • All MV and GIS switchgear installed within Zone 2 secured building.
3	Zone 3 – Equipment rooms,	No specific additional security measures, unless specifically identified as part of a site risk assessment. If required additional measures could include: • CCTV oversight of the target asset

7.3 Security of 'Significant' assets

The table below provides guidance on the selection and implementation of physical security control measures associated with security zones for assets classified as 'Significant':

Table 7 - Significant substation recommendations

No.	Function	Guiding Principles
1	Zone 1 – Generally operational areas within the perimeter fence/yard area containing outdoor HV plant and Zone 2 enclosures. Includes substation earth grid and connections, and any equipment stored permanently or temporarily at site.	Unless directed otherwise by the results of a security risk assessment, Zone 1 areas for 'Significant' Assets should be implemented as follows: • Chain-link perimeter fencing to ENA-015, inclusive of anti-climb and anti-tunnel measures • Full height pedestrian gates to control primary pedestrian entry/egress • Primary perimeter entry/exit points to be monitored and controlled by the intruder detection and access control system, entry reader • All other perimeter gates are to have a protected padlock and chain based on EQL restricted keying system • Fixed CCTV cameras to view nominated access path from perimeter gate to entry doors of buildings • Fixed CCTV cameras to provide general coverage of typical movement areas around buildings • Low level LED lighting operated by PE cell to support CCTV and natural surveillance • Arm/Disarm indicators as indicated by the specification or shown on standard drawings • External environmental enclosure to accommodate security equipment if the security equipment is not located inside the control buildings • IP PA speaker for voice announcements • Security signage
2	Zone 2 – Facilities, control buildings, switch rooms, enclosed transformer compounds, sheds, generator compounds etc.	Unless directed otherwise by the results of a security risk assessment, Zone 2 areas for 'Significant' Assets should be implemented as follows: • 1 xl primary entry/exit perimeter doors to be provided with access control monitored and controlled by the EQL corporate intruder detection and access control system, entry reader • All other doors/openings to be provided with door monitoring device connected to the alarm system • Motion detectors to be provided to rooms with external windows or doors on ground floor; and higher floors if accessible from external of the building • Registered lock and key cylinders • Security signage • Arm/Disarm indicators as indicated by the specification or shown on standard drawings
3	Zone 3 – Equipment rooms,	No specific additional security measures, unless specifically identified as part of a site risk assessment

7.4 Security of 'Limited' assets

This Asset class will typically only require a single security zone, based on the profile and location of their operating environment. Unless specifically directed by the results of a security risk assessment, Assets of this classification will generally omit the provision of electronic security measures in favour of more robust physical security measures designed to delay or deny access to the Asset.

Stand-alone assets may require more simplistic controls such as pad-locks and signage; while assets in third party rooms/building may be able to have access control, CCTV and intrusion detection devices.

The table below provides guidance on the selection and implementation of physical security control measures associated with security zones for assets classified as 'Limited':

Table 8 - Limited substation recommendations

No.	Function	Guiding Principles
1	Zone 1 – Generally operational areas within the perimeter fence/yard area containing outdoor HV plant and Zone 2 enclosures. Includes substation earth grid and connections, and any equipment stored permanently or temporarily at site.	Unless directed otherwise by the results of a security risk assessment, Zone 1 areas for 'Limited' Assets should be implemented as follows: • Chain-link perimeter fence/cage/barrier to AS 2067 & AS 1725 including anti-climb and anti-tunnel, where appropriate • Access portals (gates, cage doors etc) to the same standard as the perimeter fence/cage/barrier • For stand-alone assets, all access panels and perimeter gate entrance to have a protected padlock and chain based on EQL restricted keying system • 1 x primary entry/exit perimeter doors to be provided with access control monitored and controlled by the EQL corporate intruder detection and access control system, entry reader • All other doors/openings to be provided with door monitoring device connected to the alarm system • Security signage

Appendix A

Revision History

Revision Date	Version Number	Author	Description of change/revision
29/05/2011	1	Corporate Security	Initial issue joint standard
June 2023	2	DC	Added STNW number, added reference to STNW3434 and 3435, updated template for ECM
April 2024	3	J Lansley	Update references, added fencing requirements in Section 4, added requirements for temporary fences during projects and secondary fences. Added SOCI requirements Section 5, update fence requirements Section 6 and 7,