L

Electricity Network Safety Management System

July 2019

Electricity Network Safety Management System

July 2019

Table of Contents

Overview

In NSW the operation of each Electricity Network Operator (including Ausgrid) is governed by the *Electricity Supply Act 1995* (the Act) and associated regulations. *The Electricity Supply (Safety and Network Management) Regulation 2014* (**the Regulation**) is one of these regulations and came into force on 1 September, 2014. This Regulation requires that an Electricity Network Safety Management System (**ENSMS**) be put into place for each Network Operator that complies with the Regulation and AS5577 – *Electricity Network Safety Management Systems*.

Ausgrid is responsible for appropriately managing risks relating to its electricity network as safely as reasonably practicable. Ausgrid has implemented an ENSMS in accordance with AS5577 as required by the Regulation to document the activities undertaken to address these responsibilities. AS5577 requires that when developing the ENSMS, the Electricity Network Operator (e.g. Ausgrid) shall utilise a Formal Safety Assessment (**FSA**) undertaken in compliance with AS5577.

The ENSMS covers all interactions with the electrical network, minimising the risk to people working on or near the network, the public, property and equipment as well as the environment, by addressing the management of the following aspects of the electrical network:

- Design;
- Construction;
- Commissioning;
- Operations;
- Maintenance; and
- Decommissioning.

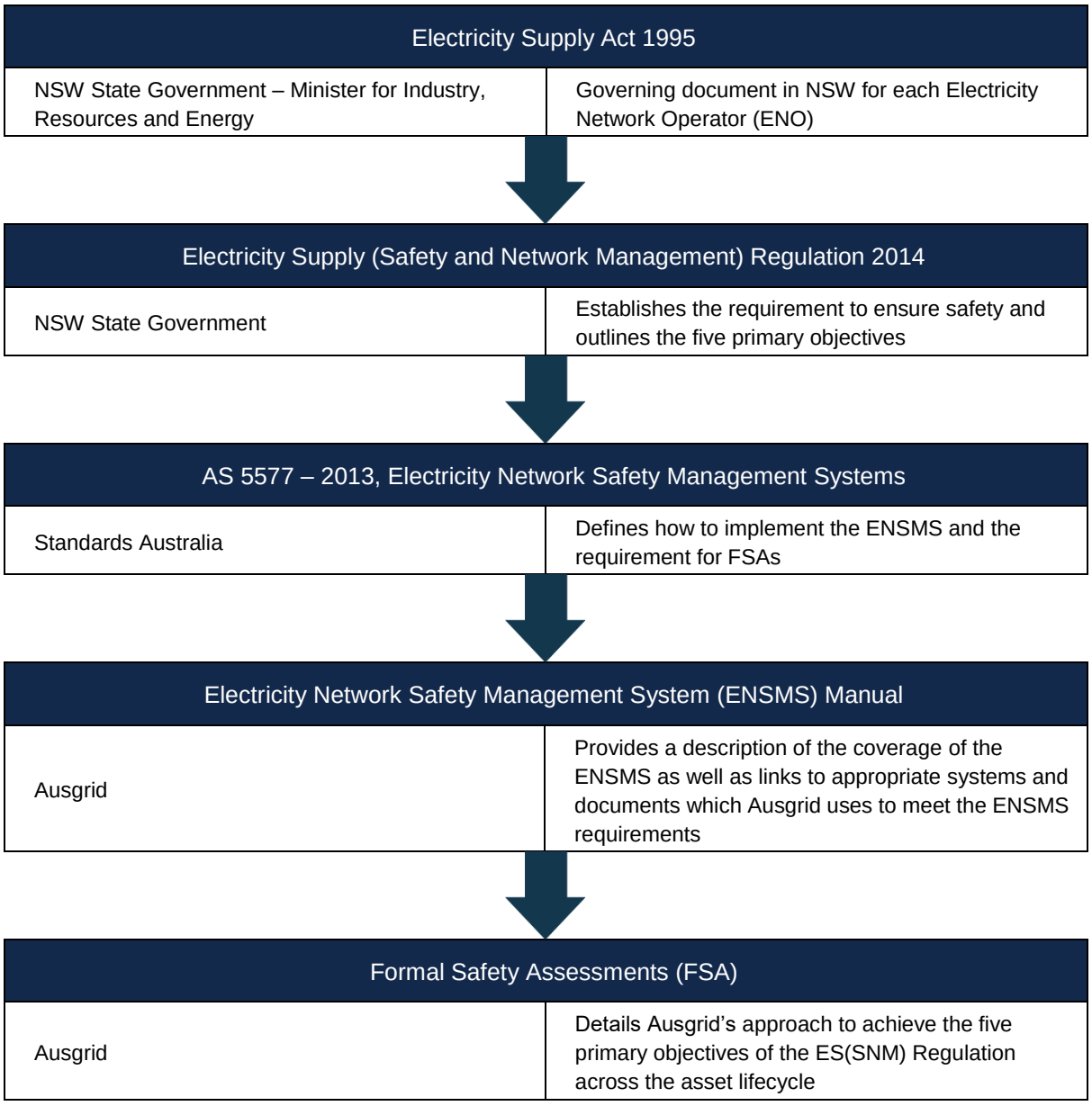
Description

Ausgrid's ENSMS is a large collection of inter-related strategies, policies, procedures, Formal Safety Assessments (**FSAs**), plans and standards which govern our activities in relation to the safety and management of our electricity network. A range of such documents can be found at the following links:

- www.ausgrid.com.au/ASPs-and-Contractors/Technical-documentation
- www.ausgrid.com.au/Industry/Regulation
- www.ausgrid.com.au/Industry/Regulation/Network-reports-and-plans

Regulatory environment

Figure 1: ENSMS Document hierarchy and purpose



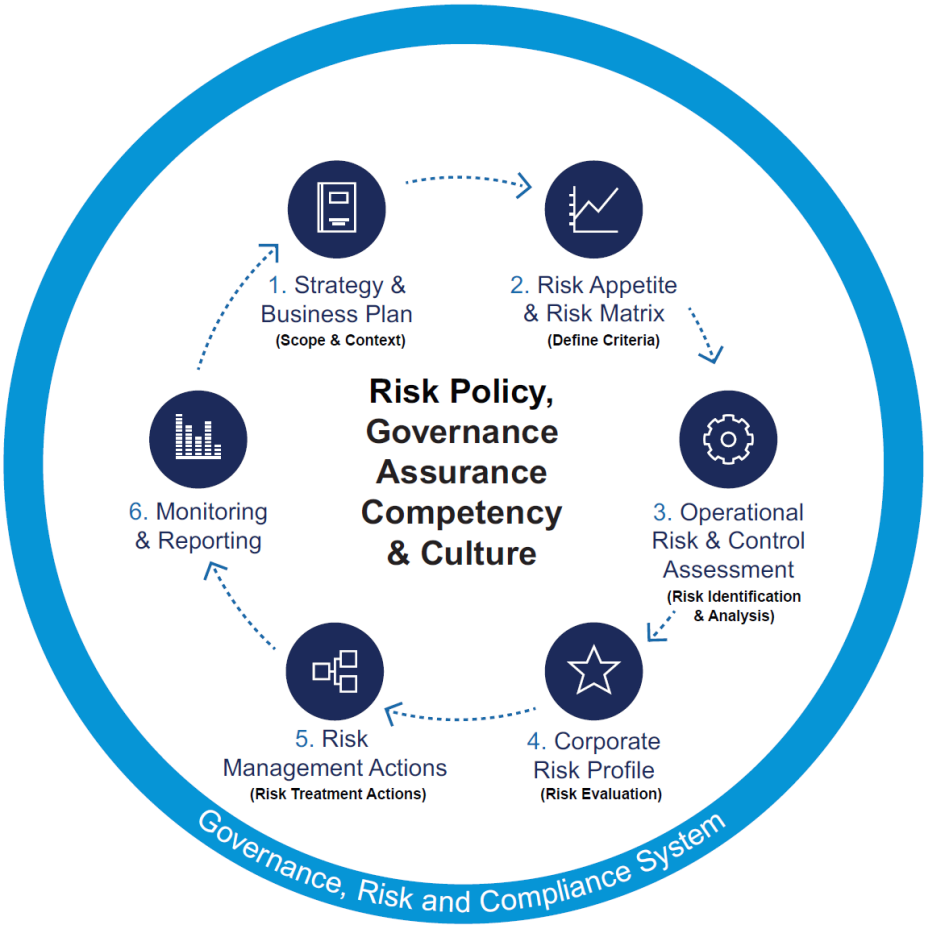
Ausgrid operates within a regulated environment, where:

- The Independent Pricing and Regulatory Tribunal NSW (**IPART**) regulates the business from a technical and safety perspective (which includes the requirement for an ENSMS and for Formal Safety Assessments);
- The Australian Energy Regulator (**AER**) regulates the business from an economic prudency and efficiency perspective;
- SafeWork NSW regulates the business with regards to safety compliance to the Work Health & Safety (**WHS**) Act and Regulation.

Risk Management

Ausgrid is committed to implementing an integrated risk management framework that is embedded into all critical processes and systems for making decisions. This enables the organisation to challenge assumptions and biases before decisions are made. The appropriate action can be taken to reduce the uncertainty around the achievement of our objectives.

Figure 2 – Ausgrid's Risk management framework



Ausgrid undertakes risk assessments on the activities and assets relating to its operations. Ausgrid is always looking for better ways to manage its risks, striving for best industry practice and considers the use of emerging technologies. Awareness of emerging risks and emerging technologies is obtained through participation at industry forums and events, interaction with suppliers and contractors, media reports, interaction with other network operators and analysis of Ausgrid data, audits and incident investigations.

Risk criteria

In compliance with the Regulation and AS5577 it is required that network safety risks be eliminated so far as is reasonably practicable (**SFAIRP**) and if not reasonably practicable to do so, then reduced to as low as reasonably practicable (**ALARP**).

Reasonably practicable', means that which is, or was at a particular time, reasonably able to be done to ensure safety, taking into account and weighing up all relevant matters including:

a) the likelihood of the hazard or the risk concerned occurring; and

b) the degree of harm that might result from the hazard or the risk; and

c) what is known, or ought reasonably be known, about the hazard or risk, and about the ways of eliminating or minimising the risk; and

d) the availability and suitability of ways to eliminate or minimise the risk; and

e) after assessing the extent of the risk and the available ways of eliminating or minimising the risk, the cost associated with the available ways of eliminating or minimising the risk, including whether the cost is grossly disproportionate to the risk.

The process for determining what is reasonably practicable is consistent with the risk management process as described in AS31000 and involves a systematic process to:

a) identify hazards associated with the network at each stage in the lifecycle;

b) if necessary, assess the risks to the primary objectives associated with the hazards;

c) identify and implement available and suitable control measures to eliminate or minimise the risks; and

d) review the effectiveness of the control measures.

Asset risk assessment

Risk assessment is the overall process of hazard or risk identification, risk analysis and risk evaluation. Ausgrid performs its risk assessment systematically using the principles and guidance contained in ISO31000 applied iteratively and collaboratively, drawing on the knowledge and views of stakeholders.

Risk identification

During the identification phase, the hazardous events, causes (threats) and consequences are determined. A range of techniques have been employed to identify hazards including available internal data, industry data and stakeholder engagement. The use of alternative techniques includes stakeholder input. The risk identification phase includes the involvement of stakeholders with the prerequisite technical expertise in the relevant areas, such as designers, operations and maintenance personnel, and safety and risk management experts.

Risk analysis

Risk analysis provides a link between the identified threats, the hazards and the consequences that could eventuate should a hazardous situation occur. It provides a means for generating an understanding of the risks and developing knowledge on the ways in which the risk can occur.

A variety of supporting techniques have been applied to support the risk assessment process. The technique selected is dependant on the level of detail required to gain the most thorough understanding of the risk given the available information.

The main considerations in the selection of the risk analysis method for each hazard and consequence are that the technique should:

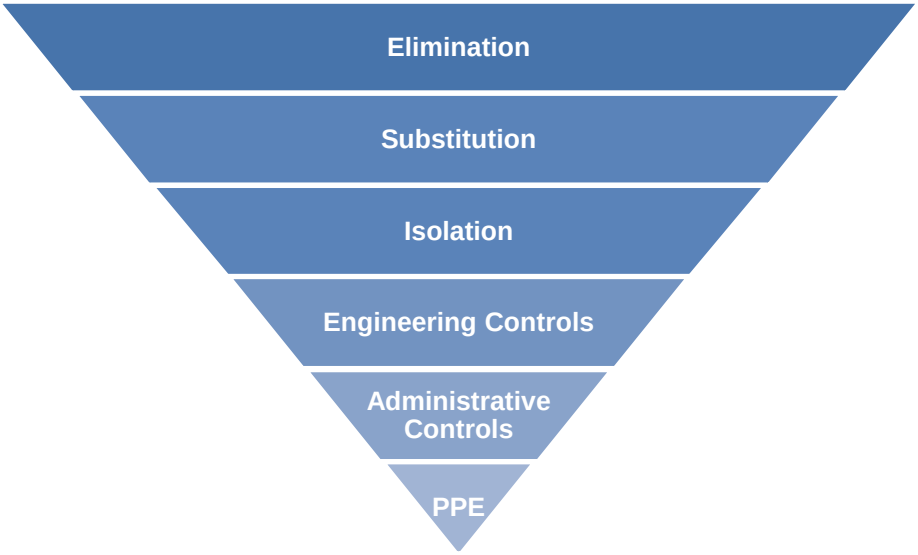
- be suitable for the type and complexity of the hazard;
- assist in understanding and selecting control measures;
- differentiate between consequences outcomes on a risk basis (i.e. likelihood and consequence); and
- assess the potential effect of risk reduction measures.

Risk evaluation

In taking all reasonable steps in ensuring the network is safe, eliminating the risk is the most effective control. Where a risk cannot be practicably eliminated, evaluation informs the treatment options for controlling the risk so that the residual risk is as low as reasonably practicable. Residual risks are considered reasonably practicable where the available treatment options for eliminating or minimising are grossly disproportionate to the risk. The risks and treatments should be monitored and periodically reviewed for acceptability and with no other or new available practicable ways for eliminating or minimising the risk.

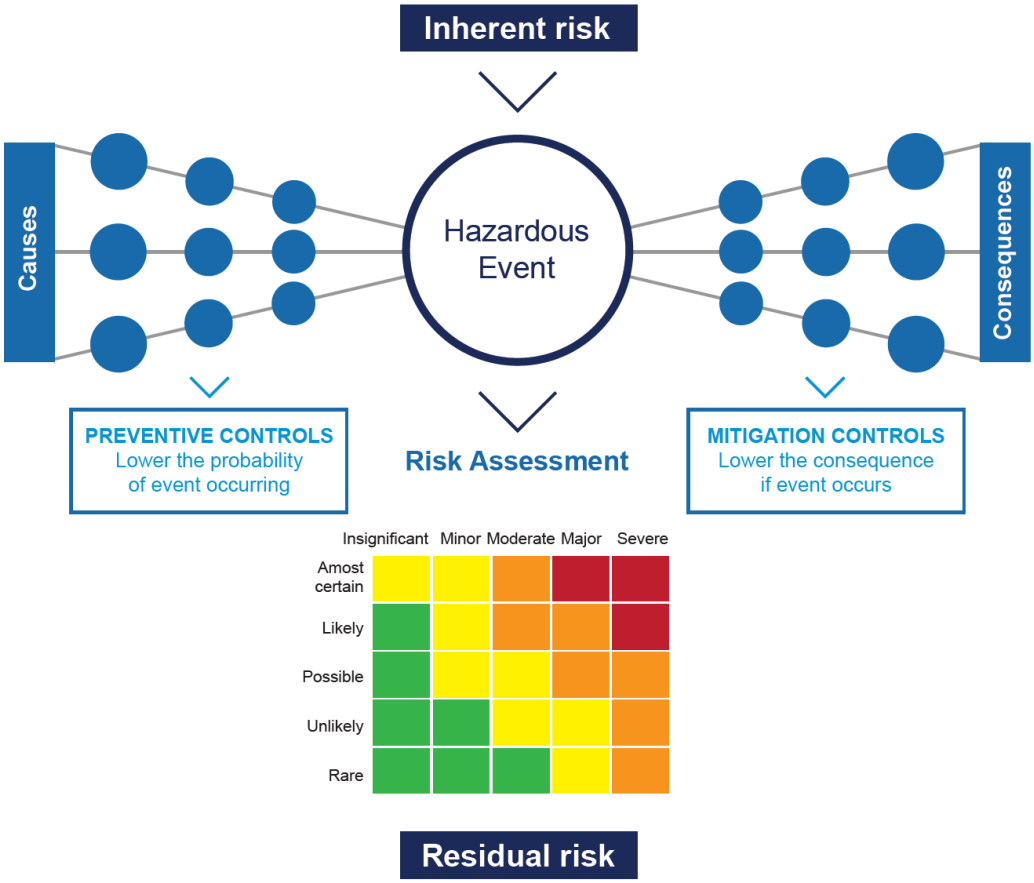
The ways of controlling risks can be ranked from the highest level of protection and reliability to the lowest as shown in **Figure 3**. Elimination of a risk is the most effective method of control and if this is not reasonably practicable to achieve, implementation of additional controls should be considered based upon their practicability. This ranking order is referred to as the hierarchy of controls and comprises elimination, substitution, isolation, engineering controls, administrative controls and finally use of personal protective equipment.

Figure 3 – Hierarchy of Controls



Bow Ties provide a visual representation of the hazards and, consequences, with their associated mitigating and preventative controls. These models are best utilised when there are multiple controls contributing to the residual risk outcome and provides a view of overall control effectiveness.

Figure 4: Risk analysis diagram (Bow tie)



Risk monitoring and review

Ausgrid monitors and reviews its risks and controls including:

- Monitoring of performance;
- Learnings from incidents and audits;
- Consideration of suitability and effectiveness;
- Investigating new technologies / controls
- Comparison against industry good practice; and
- Whether it would be reasonably practicable to implement additional or more effective controls.

These reviews provide assurance that its risks are eliminated or minimised through continual improvement and maintaining currency. Monitoring the residual risk of each of the threats so that the risk is appropriately managed through:

- Process and performance monitoring;
- Industry involvement and stakeholder engagement;
- Incident recording and investigation; and
- Revision of risk assessments.

Key risk terminology

Key terminology applied in the risk assessment are defined as follows:

- **Hazards** – Hazards are broadly defined as a source of potential harm arising from activities performed throughout the asset lifecycle. These include overhead line assets, underground mains assets, substation equipment, streetlighting assets and communication infrastructure and the asset lifecycle activities associated with these assets.
- **Causes** – factor that could lead to a hazardous event occurring. e.g. overhead conductor failure, vegetation falling into electricity mains
- **Hazardous events** – an event which has the potential to cause harm. e.g. public exposed to an overhead conductor failure, vehicle striking a power pole, power outage, bushfire caused by an asset failure
- **Controls** – Measures that modify the risk including:
  - Preventative controls – a treatment to reduce the likelihood of a hazardous event. e.g. overhead conductor minimum clearance distances, tree trimming, replacement of poor condition assets, design standards, personal protective equipment, training
  - Mitigating controls – a treatment to reduce the likelihood of a consequential outcome following a hazardous event. e.g. protection systems to isolate supply upon overhead conductor failure, incident response procedures
- **Escalators** – a scenario that increases the risk likelihood, including:
  - Loss of control escalators increase the likelihood of a hazardous event occurring. e.g. extreme weather increases the likelihood of overhead conductor failure or an electricity outage
  - Consequence escalators increase the likelihood of a high-consequence scenario following a hazardous event. e.g. an overhead conductor failure in a heavily vegetated region adjacent to a densely populated area increases the likelihood of a high consequence event
- **Consequences** – Outcome following a hazardous event, for example:
  - Near miss e.g. no injury occurrence.
  - Public safety incident e.g. electrocution following contact with failed overhead conductor on the ground
  - Network worker incident e.g. worker injured from falling into an open excavation whilst installing new underground cabling
  - Property damage e.g. bushfire started due to a network asset contacting vegetation
  - Environmental safety incident e.g. release of asbestos fibres into the environment following the failure of a network asset

- Loss of supply incident. e.g. outage of electricity supply leads to life support customer requiring medical care, street lighting outage contributes to pedestrian being struck by a motor vehicle

- **ALARP** – As low as reasonably practical
  - The measure of whether ALARP has been achieved is through the reduction of risk to a level that is acceptable.
  - Concepts such as the ALARP triangle are common approaches used to evaluate the level of risk against acceptable thresholds.
- **SFAIRP** - So far as is reasonably practicable
  - The measure of whether SFAIRP has been achieved if the cost of reducing the risk is grossly disproportionate to the benefit gained.
  - The concept of SFAIRP contains the explicit assumption that there are alternate controls that can reduce the risk but that some of alternatives may not be practical.
  - An important part of the process of demonstrating SFAIRP is the identification and evaluation of additional controls that offer lower risk.

Formal Safety Assessment

Ausgrid has a suite of six FSAs sitting under its ENSMS Manual. Refer **Table 1**. The FSAs outline the risks associated with the electrical network as well as the controls that are used to eliminate these risks So Far As Is Reasonably Practicable (SFAIRP) or reduce them to As Low As Reasonably Practicable (ALARP).

Table 1: Alignment of FSA documents to the primary objectives of the Regulation

Primary objective	Associated FSAs
The safety of members of the public	Public Safety FSA
The safety of persons working on networks	Worker Safety FSA
The protection of property (whether or not belonging to a network operator)	Property FSA
The management of safety risks arising from the protection of the environment (for example, preventing bushfires that may be ignited by network assets)	Bushfire FSA
	Environment (safety) FSA
The management of safety risks arising from loss of electricity supply	Loss of Supply (safety) FSA

The FSA structure has been guided by the risk assessment approaches within:

- The Australian Standard for Risk Management (AS/NZS ISO 31000:2009) – in effect, AS5577 applies the principles of ISO 31000 to eliminate the primary objective risks SFAIRP or reduce them to ALARP.
- The SafeWork NSW Codes of Practice – as they relate to managing risks associated with electricity. The code of practice is designed as a practical guide to achieving the standards of health, safety and welfare required under the WHS Act and WHS Regulations and therefore, in most cases, following an approved code of practice would achieve compliance with the duties in the Act, particularly in relation to the subject matter of the code.
- The International Standard for Environmental Management Systems (EMS) (ISO 14001) – requires identifying and planning actions to address risks and opportunities related to environmental aspects, compliance obligations, other issues or other needs and expectations of interested parties.
- The International Standard for Asset Management Systems (AMS) (ISO55001) – considers the end to end lifecycle management of assets in achieving a balance between risk, cost and performance.

Controls

Ausgrid implements a range of preventative and mitigative controls over the asset life cycle to achieve the primary objectives of the Regulation. Our FSAs include the following main controls:

- Planning standards, network design standards and technical specifications so that we only install suitable assets on the electrical network and configure the network to cater for redundancy and foreseeable circumstances. These include protection devices and systems, warning and isolation systems, containment and suppression systems.
- Virus, malicious code, malware protection, system design and processes to help protect the network from cyber attacks.
- Maintenance tasks and inspection programs to help maintain assets in good order and to address defects or poor condition assets while operating the network. This includes regular substation equipment condition monitoring & inspections and preventative tasks such as tree trimming to help keep vegetation away from overhead lines.
- Investing in the network to address poor condition or non-compliant network assets and overloaded network assets that are presenting an unacceptable network or safety risk.
- Policies, network standards, procedures, work instructions, rules, guidelines, job planning, environmental impact assessments, environmental management plans, worksite risk management, contractor management, fleet and plant management and safe work method statements so that workers work safely on or near the network.
- Protective personal equipment (PPE) to help prevent injury.
- Training, learning and development, auditing programs and supervision of workers so they are competent, aware of hazards and able to respond following an incident including licensing and authorisation processes, isolation and permitting processes, lock out and tag out processes, injury management and first aid.
- Operating practices on total fire ban days to help prevent and minimise the impact of bushfires.
- Raising public awareness of electrical network hazards through various media channels including Dial Before You Dig (DBYD) service for underground cable safety, overhead power line safety, school children electricity safety education programs, safety around fallen power lines, bushfire risk and electrical hazard awareness for emergency personnel.
- Using lessons learnt from investigations and audits to improve performance.
- Emergency response, incident management processes and responses to recover from incidents.

Public Safety FSA

Scope

This FSA evaluates risks specifically in relation to safety of the public, whereby:

- The public is any person not carrying out lifecycle activities related to electricity network assets (as defined within AS 5577); and
- Public safety relates to preventing harm to a member of the public attributable to Ausgrid's electricity network assets or activities (located within its distribution district).

Ausgrid has considered the following Public Safety threats and has implemented controls to manage these risks.

Public safety threats and threat scenarios

Threat scenarios	Threats
Asset failure	• Asset failure • Inadequate street lighting (traffic accidents) • Inadequate street lighting (increased crime rates)
Unsafe design	• Slips, trips and falls • Vehicle impact with ground mounted asset (e.g. poles, pillars, distribution substations)
Unauthorised access	• Unauthorised access to assets • Unauthorised operation of assets • Malicious damage • Encroachment (vegetation) • Encroachment (structures)
Electrical contact	• Electrical contact • Contact with overhead conductor (e.g. cranes, boats, aircraft) • Contact with underground cable • Encroachment (vegetation) • Encroachment (structures) • Earthing system failure
Asset lifecycle activities	• Construction work • Mobile plant • Traffic management • Driving • Slips, trips and falls • Road rage • Equipment (network workers) • Human error (operational)

Worker Safety FSA

Scope

This FSA evaluates risks specifically in relation to worker safety; whereby:

- A worker is any person carrying out lifecycle activities related to electricity network assets (as defined within AS 5577); and
- Worker safety relates to preventing harm to a worker attributable to Ausgrid's electricity network assets (located within its distribution district) or activities.

Ausgrid has considered the following Worker Safety threats and has implemented controls to manage these risks.

Worker safety threats and threat scenarios

Threat scenarios	Threats
Network fatal threats	• Exposure to electrical discharge • Exposure to chemicals / materials • Fall from heights • Motor vehicle accidents • Contact with mobile plant • Falling / moving objects • Crane activities • Collapse of excavation • Breach of controlled worksite (by vehicles outside the work area)
Operational threats	• Manual tasks • Mental stress • Release of pressurised substance • Slips, trips and falls • Environmental exposure (hot / cold) • Exposure to non-ionising radiation (EMF) • Confined spaces • Striking object • Sound / sound pressure • Bio hazard (dogs, bees, needles) • Occupational violence
Other threats	• Cyber security • Breach of confidential information • Operation over water • Aerial operations • Remote working • Working alone • Working underground (e.g. tunnels)

Threat scenarios	Threats
	• Not fit for work • Human error • Asset failure • Plant failure • Exposure to Fibre-optic (laser + sharps) • Non-approved materials • Malicious damage • Explosive work tools

Property FSA

Scope

This FSA evaluates risks specifically in relation to the protection of property, categorised as follows:

- Ausgrid damage to third party assets / property
- Third party damage to Ausgrid assets / property
- Ausgrid damage to Ausgrid assets / property
- External “natural” damage to Ausgrid assets / property
- Loss or damage to Ausgrid network data and information.

Ausgrid has considered the following Property Protection threats and has implemented controls to manage these risks.

Property protection threats and threat scenarios

Threat scenarios	Threats
Ausgrid damage to third party assets / property	• Asset failure • fallen overhead assets • explosive equipment • HV injection to LV • earthing system failure • assets not fit for purpose • vehicle impact • human error • access track damage • livestock fatality • reverse polarity • clearance encroachment • damage during construction or maintenance activities
Third party damage to Ausgrid assets / property	• Vehicle impact • inadvertent access • human error • construction or mining vibration • electrical contact with assets (cranes into overhead or cable strikes) • clearance encroachment • terrorism • sabotage • vandalism • theft • damage during construction or maintenance activities

Threat scenarios	Threats
Ausgrid damage to Ausgrid assets / property	• Asset failure, • fallen overhead assets • explosive equipment • HV injection to LV • earthing system failure • assets not fit for purpose • vehicle impact • human error • damage during construction or maintenance activities
External "natural" damage to Ausgrid assets / property	• Erosion • localised flooding • localised fire • subsidence • weather
Loss or damage to Ausgrid network data and information	• Cyber-attack • IT equipment failure

Environment FSA

Scope

This FSA:

- evaluates risks specifically in relation to protection of the environment from carrying out lifecycle activities related to electricity network assets (as defined within AS 5577);
- covers all activities, products and services carried out by the company which may impact on the environment, including those carried out by contractors and accredited service providers (ASPs).

Ausgrid has considered the following Environmental Protection safety threats and has implemented controls to manage these risks.

Environmental protection safety threats and threat scenarios

Threat scenarios	Threats
Pollution	• Loss of integrity of fluid filled cable • Loss of integrity of operating oil filled equipment • Inadequate storage or handling of oils, fuels and chemical • Inadequate management of dewatering activities • Inadequate management of works involving ground disturbance
Unauthorised development	• Absent or inadequate Environmental Impact report (incorporating necessary permissions) • Inadequate management of works impacting flora/fauna
Contamination and waste	• Inadequate management of contaminated sites • Inadequate storage and handling of Polychlorinated biphenyls (PCB)contaminated materials • Inadequate management of pesticide usage • Inadequate management of waste
Emissions	• Intrusive release of dust, gas or fumes • Excessive noise generated by operational equipment • Excessive noise associated with construction activity • Breach of electric magnetic fields requirements
Hazardous chemicals / materials	• Inadequate management of asbestos • Inadequate management of lead • Inadequate management of synthetic mineral fibre • Inadequate management of hazardous chemicals

Bushfire FSA

Scope

This FSA evaluates safety risks specifically in relation to bushfires initiated from Ausgrid's electricity network assets (located within its distribution district) or activities.

Ausgrid has considered the following Bushfire prevention threats and has implemented controls to manage these risks.

Bushfire prevention threats and threat scenarios

Threat scenarios	Threats
Asset failure	• Pole top components equipment e.g. cross arms, insulators • Conductor failure • Pole failure
Asset contact with vegetation	• Vegetation grows into overhead mains • Vegetation blows into overhead mains • Vegetation blows into or falls into overhead mains
Animal contact with assets	• Possum, bird or bat contacting overhead mains
Third party damage to Ausgrid assets	• Vehicle striking pole • Crane striking overhead mains
Conductor clashing	• Overhead bare wire mains clashing between phases
Protection reclosing	• Reclosing devices
Asset life cycle activities	• Grinding, welding, brazing or oxy cutting • Vehicle or machinery inadvertently starts a fire

Loss of Supply FSA

Scope

This FSA evaluates safety risks arising from loss of electricity supply.

- The hazard event of a “loss of electricity supply” relates to the loss of supply to network assets or customers located in Ausgrid’s electricity network assets (located within its distribution district).
- The loss of an upstream supply from our transmission service provider’s network is included in this FSA as some of the controls identified are common with maintaining security of our network and translate to affecting Ausgrid’s customers.

Those who may be reliant on electrical supply include:

- General customers - e.g. residential, commercial, industrial.
- Key customers – these predominantly relate to supply to infrastructure e.g. telecommunications, water supply or waste.
- Critical Infrastructure – e.g. hospitals, motorway tunnels with ventilation, airports.
- Vulnerable customers – e.g. customers reliant on life support equipment.

Out of scope

- Loss of electricity supply events that originate from within a private network or customer installation beyond the metering point as defined in the NSW Service and Installation Rules (SIR) and Australian Standards AS3000 (Wiring Rules) where the loss of supply event only impacts the associated private network customer are not assessed and evaluated as part of this FSA.
- Those customers who are reliant on powered equipment need to be adequately prepared to ride out a momentary interruption. This may include temporary back-up supply, including uninterruptible power supply (UPS) when developing their continuity or actions plans. Due to the customer’s responsibilities, momentary interruptions have also been excluded from scope of this FSA.

Ausgrid has considered the following Loss of Supply threats and has implemented controls to manage these risks.

Loss of Supply threats and threat scenarios

Threat scenarios	Threats
Asset failure	• Asset defect or asset condition
Forced outage (external issue)	• Directed or automatic under frequency load shedding • Loss of upstream supply
Forced outage (capacity constraint)	• Overloads
Human error	• Operator error • Technician error • System mapping error
Externally caused (nature)	• Flora / fauna • Weather
Externally caused (people)	• 3rd party activity • Terrorism • Vandalism • Embedded generation / customer equipment • Cyber security
Planned Interruption	• Maintenance, Construction, Augmentation, Connections • External request (customer, TNSP, DNSP, generator, construction)