

Network Asset Risk Assessment Methodology

CONTROLLED DOCUMENT

Summary

The Network Asset Risk Assessment Methodology outlines the way network asset risks are analysed and assessed, to support the investment decision making process supporting the programs of work whilst ensuring a safe reliable network.

Revision no:	4	TRIM No:	D2016/00457	Approval/ Review Date:	16 November 2021
Business function:	Strategic Asset Management			Document type:	Procedure
Process owner:	Head of Asset Management				
Author:	Peter Gaudron, Asset Management System Specialist				
Reviewers:	Adam Hoare, Digital Infrastructure Asset Manager Charles Kurniawan, Transmission Lines and Cables Asset Manager Evan Lamplough, Substations Asset Manager Debashis Dutta, Asset Analytics and Insights Manager Edward Luk, Asset Works Program Strategy Manager Stephen Antoon, Senior Network Performance Engineer				
Approver:	Andrew McAlpine (Acting), Head of Asset Management				

A printed copy of this document may not be the current version. Please refer to the Wire to verify the current version.

Contents

1. Purpose	5
2. Scope.....	5
3. Definitions	5
4. Background	7
5. Framework	8
6. Process Description	10
6.1. Process.....	10
6.2. Investment Analytics	12
6.2.1. Overview.....	12
6.2.2. Systems.....	12
6.2.3. Risk Acceptance Criteria	14
6.2.4. Risk Quantification.....	14
6.2.5. As Low As Reasonably Practicable (ALARP).....	16
6.2.6. Regulatory Obligations – Network Safety	19
6.2.7. Sensitivity Analysis of the Risk Output.....	19
6.3. Asset Health Framework	20
6.4. Asset Criticality Framework.....	20
6.5. Cyber-Security Risk Assessment.....	21
6.6. Network Safety Formal Safety Assessment.....	21
6.6.1. Overview.....	21
6.6.2. Threat/control/consequence mapping.....	21
6.6.3. Control Criticality and Effectiveness.....	23
6.6.4. Critical Control Management.....	24
7. Integration with asset management strategies and plans	25
7.1. Maintenance plans	25
7.2. Renewal and maintenance strategies.....	25
7.3. Interaction with the Prescribed Network Capital Investment Process	25
7.3.1. Need and Opportunity Screening Assessment (NOSA)	26
7.3.2. Investment options	26
7.4. Interaction with Portfolio Investment.....	27
8. Accountability.....	27

9. Implementation	28
10. Monitoring and review	28
11. Change from previous version	28
12. References	28

List of Tables

Table 1 – Alignment to Transgrid’s Strategic Pillars.....	7
Table 2 – Asset Risk Systems.....	13
Table 3 – Determination of network safety risk reduction benefit.....	17
Table 4 – Option Evaluation.....	18
Table 5 – ALARP Test Option Evaluation.....	18
Table 6 – Bow Tie Component Definitions.....	22
Table 7 – Risk treatment effectiveness measures.....	24
Table 8 – PoA Inputs.....	37
Table 9 – LoB Inputs.....	40
Table 10 – Borg-Scale Expertise.....	40
Table 11 – Borg Scale Expertise Ratings.....	41
Table 12 – Borg Scale Expertise Ratings and Scores to carry out Cyber Attacks.....	41
Table 13 – CoB Inputs.....	42

List of Figures

Figure 1 – Decision Framework and Criteria.....	8
Figure 2 – Transgrid Risk Management Framework.....	9
Figure 3 – Risk Assessment Process.....	10
Figure 4 – Investment Analytics Base Risk Calculation.....	12
Figure 5 – Risk quantification methodology.....	15
Figure 6 – Elements of Threat Consequence Mapping.....	22
Figure 7 – Interaction between the NRAM and the investment process.....	26
Figure 8 – Australia’s National Terrorism Threat Level.....	38
Figure 9 – Cyber security incident reports received by the ACSC (1 June 2020 to 30 June 2021).....	39
Figure 10 – AEMO Market Subsector Criticality Bands.....	39

List of Appendices

Appendix A - Risk Calculation Methodology

Appendix B - Cyber Security Risk Assessment

Appendix C - Risk Assessment Methodology Framework – Full Version

1. Purpose

The purpose of the Network Asset Risk Assessment Methodology (NRAM) is to:

- Identify the threats, consequence, and controls required to manage network asset risks and ensure delivery of a safe and reliable network.
- Analyse and evaluate network asset risks in a systematic and consistent manner, to support the investment decision making process, and to provide a safe and efficient network to benefit the consumer and stakeholders.
- Support timely, effective, and efficient asset management investment decision making and to manage changing risk.
- Support the achievement of the asset management objectives and ultimately the corporate objectives.

2. Scope

The NRAM is applicable to the analysis and assessment of network safety and commercial risk for network assets, including:

- Substation assets
- Transmission Line assets
- Underground Cable assets
- Digital Infrastructure assets
- Security System assets
- Network Property assets
- Cyber Security Risk for Operational Technology

This framework is applied to in-service assets and replacement evaluation but may be applied to other assets such as augmentation as deemed necessary

3. Definitions

Key terms and definitions relating to this document.











Term	Definition
AEMO	Australian Electricity Market Operator
ALARP / SFAIRP	As Low As Reasonably Practicable (ALARP) / So Far As Is Reasonably Practicable (SFAIRP). Refer 6.2.5.
Conditional Failure	The inability of an asset to satisfy the operational/conditional limitations placed on it.
Consequence of Failure (CoF)	The credible cost consequence if the event eventuates. The preferred method is to perform quantitative risk analysis using range of credible consequences and align these to respective Likelihood of consequences Where a singular consequence of failure is used this should be based on the likely worst case scenario (as distinct from the maximum possible case).
Functional Failure	The inability of an asset to perform its required function.

Failure Mode	The way in which an asset failure occurs. e.g. conductor drop, tap changer failure, protection relay failure.
Life Ending Failure	Type of failure that destroys an asset beyond repair or when repair is uneconomical. Life ending failures can be catastrophic or non-catastrophic.
Likelihood	The chance of something happening.
Likelihood of Consequence (LoC)	The likelihood that the full value of the consequence event eventuates given the hazardous event has actually occurred. For quantitative risk analysis the Likelihood of Consequence will be determined for each of a range of credible consequences.
Loss of Control Event	A point in time which describes the release or loss of control over a Hazard that creates an undesired system state. Typical events identified at Transgrid are: <ul style="list-style-type: none"> • Loss of control of electricity • Loss of control of heat • Loss of control of third party activities that result in infringement of safe approach distances, entry to work sites, asset damage or injury.
Network Safety	The safety aspects of risk arising from the network associated with designing, building, operating, maintaining and disposing network assets that pose a risk to workers, the public, the environment (including Bushfire) and property.
Probability of Failure (PoF)	Annual probability of a Life Ending Failure occurring.
Risk	The effect of uncertainty on achieving Transgrid's objectives. Risk is measured in terms of impact and likelihood. Uncertainty can have positive and negative effects on objectives.
Risk Assessment	A systematic process of risk analysis and evaluation.
Risk Consequence	The outcome of an event expressed qualitatively or quantitatively, affecting Transgrid's objectives. There may be a range of possible outcomes associated with an event; these could have a positive or negative impact on objectives. The outcomes are categorised as financial, environmental (Inc. bushfire), reputational, safety (worker and public), compliance, and/or financial.
Risk Tolerance	The level of risk Transgrid is willing to accept, which is in accordance with the Risk Appetite Statement and Risk Management Framework approved by the Board.
Threat	A possible direct cause that will potentially realise the loss of control of a hazard by initiating a top event. Top events are identified undesirable event that either has the potential to cause or results in an outcome that prevents the achievement of the corporate and asset management objectives. Threats are selected from the Formal Safety Assessment following a hazards review. The most significant threats are: <ul style="list-style-type: none"> • Structure Failure • Conductor Drop • Explosive Asset Failure • Unauthorised Access • Third Party Activity • Unplanned outage • Environment High Consequence Incidents Refer to the Formal Safety Assessments for more detail.

4. Background

The Network Risk Assessment Methodology is the guiding document for management of risk within the Asset Management System. It is developed to be consistent with the requirements of the corporate Risk Management Framework and to deliver on Transgrid’s strategic objectives. The overriding principle is to provide benefit to the consumer and Transgrid’s stakeholders in accordance with Transgrid’s strategic pillars and aligned asset management objectives. Table 1 shows Transgrid’s current corporate strategic pillars and asset management objectives.

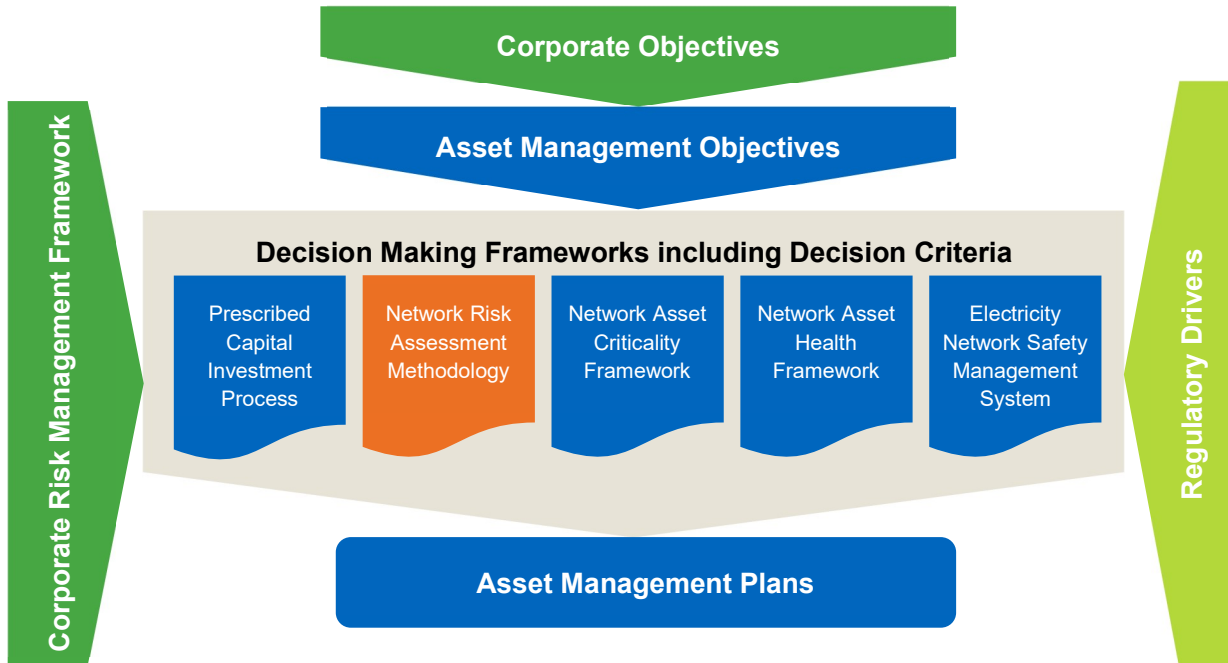
Table 1 – Alignment to Transgrid’s Strategic Pillars

Strategic Pillar		Asset Management Objective	
 <p>Deliver safe, reliable, and low cost power</p>		 <p>Maintain Network Safety Risk</p>	
		 <p>Maintain Network Reliability</p>	
		 <p>Manage assets efficiently without compromising security holder and consumer value</p>	
		 <p>Improve capability to support future energy system development</p>	
		 <p>Ensure accessible, relevant asset management information is available to inform business-wide decisions</p>	
 <p>Advocate for the energy system of the future</p>		 <p>Leverage AM to support new technologies and innovations that improve or grow our business</p>	
 <p>Invest in new infrastructure and services to support the energy transition</p>		 <p>Support sustainable growth of the asset base by providing the right assets in the right place</p>	

5. Framework

The NRAM forms the core of the network risk and investment analysis decision making framework at Transgrid as shown in Figure 1.

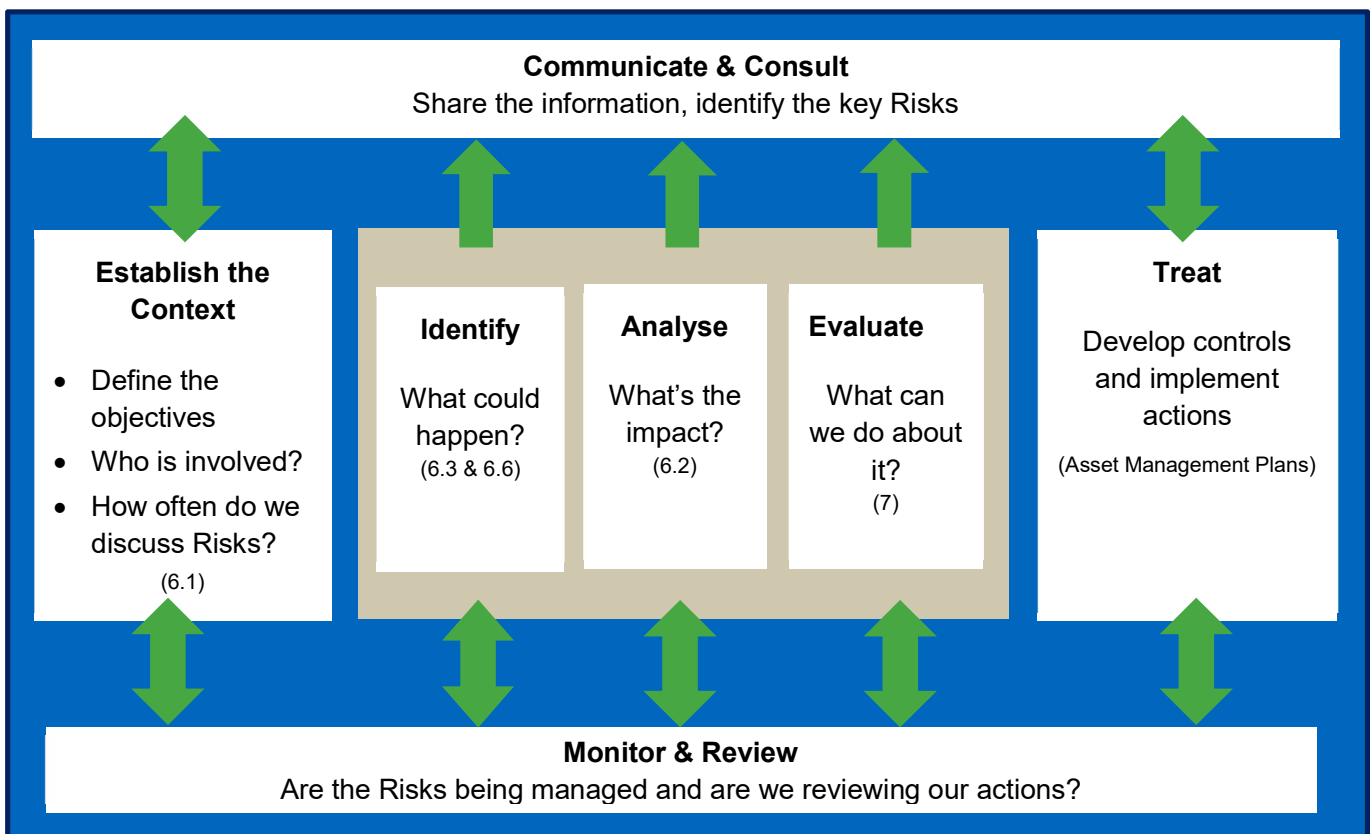
Figure 1 – Decision Framework and Criteria



The key principles of the NRAM are to provide a documented, systematic, and consistent process for the analysis and assessment of asset risks in order to ensure that Transgrid delivers a safe and reliable network that benefits its stakeholders. This analysis is performed to be consistent with the requirements of Transgrid's corporate Risk management Framework and the international standard ISO 31000 as shown in Figure 2. The NRAM Aligns to this framework through:

- Identifying the context for risk evaluation through a defined process referring to the key commercial and regulatory drivers and resultant outcomes required (Refer 6.1).
- Identify the threats, controls, consequences, and high potential incidents required to manage risk through the Formal Safety Assessment process (Refer 6.6).
- Analyse the risk factors associated with an asset based on criticality and to assist in making investment and maintenance decisions (Refer 6.3 and 6.4).
- Evaluate, and quantify the risk associated with an asset in monetary terms to assist in making investment and maintenance decisions (Refer 6.2).
- Integrating the outputs of this assessment into asset management plans that define asset operations, replacement, and maintenance plans.

Figure 2 – Transgrid Risk Management Framework



The risk assessment outcomes from the NRAM are used:

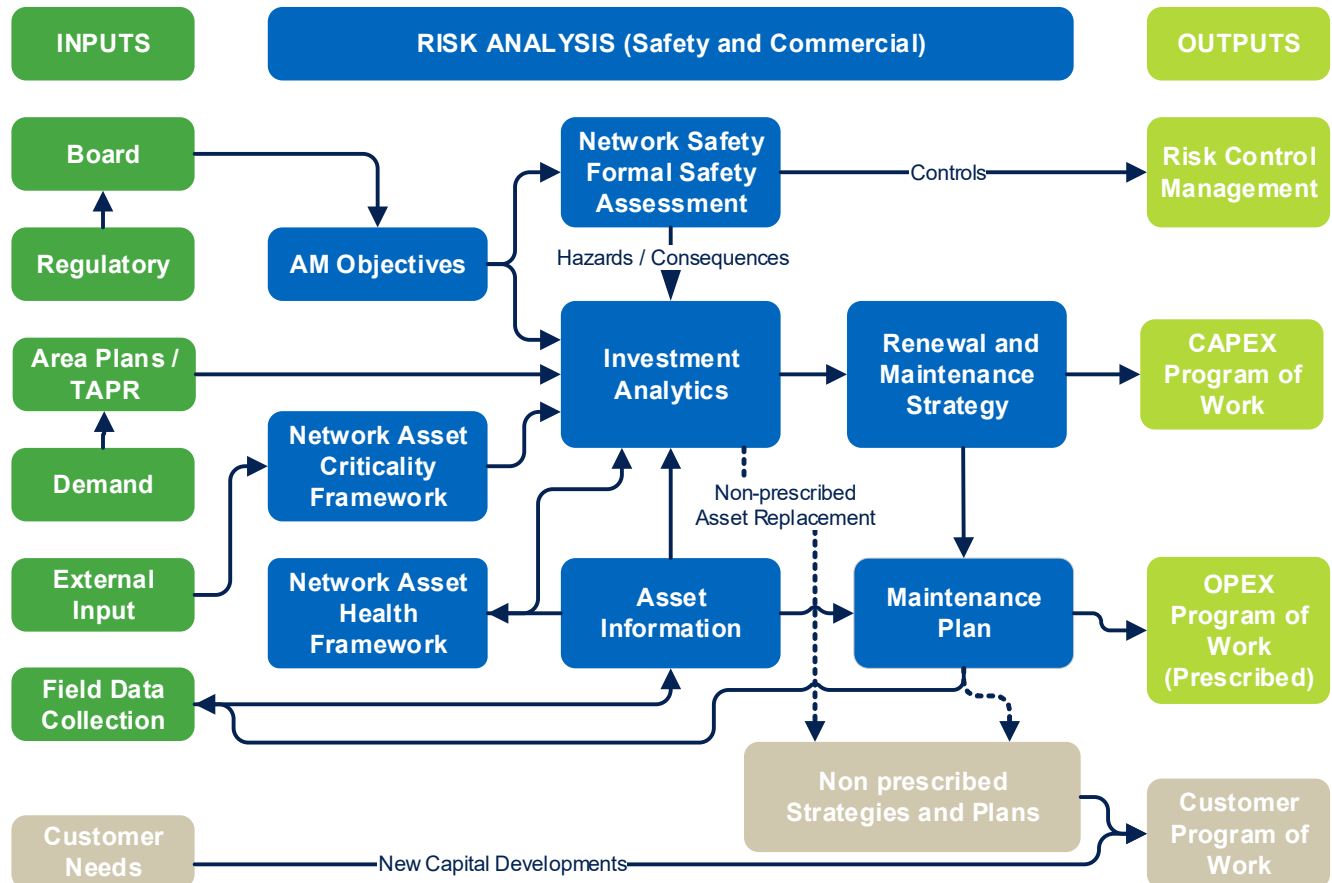
- To facilitate the requirement to minimise risk As Low as Reasonably Practicable (ALARP) as required by work health and safety and electricity safety regulations through identification of the controls required to deliver a safe and reliable network by:
 - Mapping of the threats that could lead to the occurrence of a Loss of Control Event through to its consequences
 - Identification of hazards, controls, and escalators which may cause control ineffectiveness to manage these threats through consultation and engagement with subject matter experts based on failure mode and root cause analysis.
 - Identification and modelling of terminal asset failures that could lead to the occurrence of undesired outcomes, and understanding the asset components, failure modes and associated root causes of the event.
 - Quantification of asset risk based on asset health and failure information to develop efficient capital and operating programs of work.
- To support asset management investment decisions in alignment with regulatory guidance by:
 - Input of controls and activities to the asset management strategies and plans to deliver the asset management and corporate objectives.
 - Input to the development of the Need and Opportunity Screening Assessment (NOSA). These NOSAs are the starting point for investment decision making as part of the investment process.
 - Developing risk scores to assist in prioritisation of maintenance replacement activities for assets.
 - Enabling the most efficient selection and timing of investment options by quantitative comparison of the risk reduction benefit (and cost) of alternative investment options (maintenance, refurbishment, replacement, timing, etc.) as part of the options analysis undertaken in the investment process.

6. Process Description

6.1. Process

Figure 3 shows the risk assessment process that is applied to transform the stakeholder requirements into actions within capital and operating programs of work and risk management actions. A detailed view of this process is shown in Appendix A.

Figure 3 – Risk Assessment Process



The components of this process consist of:

Inputs

The need and justification for safety management investment includes any combination of the following considerations:

- Regulatory Guidance from the Australian Energy Regulator (AER).
- Requirements of the board (asset owners) communicated through the Asset Management objectives.
- Compliance obligation in terms of Acts, Regulations, mandatory and good practice industry standards.
- Changes in network demand for network capacity for generators, industry and consumer end-users.
- External input factors such as environment, national and international economic factors, consumer, and government risk appetite.
- Characteristics of the Asset Portfolio to handle demand and external factors.

For activities where Transgrid is providing non-prescribed services:

- Customer needs through the contractual agreement to engage Transgrid to build and operate assets on its behalf.

Risk Analysis

Risk analysis consists of the following components:

- Guidance frameworks and processes including:
 - Network Asset Criticality Framework for documenting the methodology for quantifying the consequences associated with network assets.
 - Network Asset Health Framework for documenting the methodology for mapping asset health information to Probability of Failure for Transgrid assets.
- Electricity Network Safety Management
 - Identification of the hazards and threats that can lead to a loss of control event.
 - Identification of preventive and mitigative controls required to manage the loss of control event.
 - Articulation of the required controls through documented Formal Safety Assessments.
 - Identification of appropriate metrics around threats, loss of control events, control effectiveness etc. that can be used to monitor the performance of the safety management system.
- Asset investment analysis
 - Quantification of risk reduction benefit.
 - Requirement to eliminate the risk and if not, reduce it to ALARP
 - Lifecycle cost benefits
 - Obsolescence and end-of-technical life
 - Stakeholder requirements
 - Other benefits.
- Asset Information collection and storage related to the assets including:
 - Asset attribution including geospatial information.
 - Replacement cost
 - Network augmentation requirements
 - Historic failure, outage, defect, and corrective data.
 - Condition data from field inspection for input health and risk models.
 - Failure modes based on asset attributes.
 - Asset criticality based on network configuration and geospatial information
 - Tacit knowledge
- Artefacts to articulate the results of the network risk analysis:
 - Formal Safety Assessment including details of the required risk controls and High Potential Incidents required to control risk and monitor the performance of the safety management system.
 - Renewal and Maintenance Strategy to aggregate the investment needs required to maintain network integrity over the short and long term.
 - Maintenance Plan detailing the preventive and predictive maintenance requirements of the network.

Outputs

The outputs of the risk analysis are input into the following business activities:

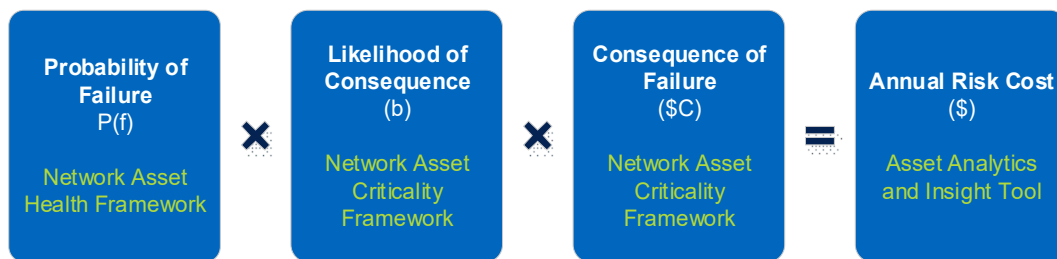
- Network and strategic risk management in alignment with the corporate Risk Management Framework.
- Capital program of work and budget with a 5 year plan and longer term capital forecast, associated short term capital programs, and capital budget.
- Asset Management program of works and (Operating) budget.
- Customer program for maintenance and replacement of non-prescribed assets.

6.2. Investment Analytics

6.2.1. Overview

Investment analytics is performed to ensure that Transgrid's investments are performed systematically using quantified risk assessment techniques in order to deliver benefits to Transgrid's Stakeholders including consumers, government and stakeholders. This is performed to be consistent with Section 5 of the *AER Asset Replacement Guidelines*¹ and is based on an underlying calculation of a monetised Risk Cost as shown in Figure 4. Indicated against each step is the primary procedure covering quantification of the necessary inputs. The specific application of this formula is explained in 6.2.4.

Figure 4 – Investment Analytics Base Risk Calculation



In performing this analysis Transgrid considers the following consequence areas:

- Financial (including costs of non-compliance)
- Environmental (including bushfire)
- Reputational (Social License)
- Safety (Worker and Public)
- Reliability

These are aligned with Transgrid's corporate Risk Management Framework. Refer to Transgrid's Network Asset Criticality Framework for further details.

6.2.2. Systems

The systems that support the application of the NRAM include:

- Isograph Availability Workbench for identification of failure modes of assets and calculation of probabilities of failure based on the failure modes of assets.
- Asset Analytics and Investment Tool for risk quantification, risk forecasting and register of risk assessments.
- Enterprise Resource Planning system for management of work.

¹ Industry practice application note, Asset replacement planning, January 2019, Australian Energy Regulator

- Asset Inspection Manager for collection of asset inspection data and issues requiring rectification from the field.
- Bow-Tie XP for development of Bow-Tie models.

The data required to support the application of the NRAM will need to be defined and captured to facilitate the use of these tools.

Table 2 – Asset Risk Systems

System	Provider	Description
Enterprise Resource Planning (ERP)	ABB Ellipse	Manages information related to: <ul style="list-style-type: none"> • Work management (Preventive and corrective) • Equipment work history • Asset maintenance costing
Capital cost estimation	MTwo	Contains cost information used to develop capital cost estimates for capital projects for input to the replacement analytics model.
Asset Analytics and Insights Tool	PowerPlan	Consolidates asset, asset replacement cost, asset maintenance costs, asset health, probability of failure, and criticality information to determine quantified risk costs for asset along with optimal replacement timing analysis using NPV analysis.
Reliability Analytics	Isograph Availability Workbench	Consolidates asset failure information to develop statistical failure distributions (Such as Weibull) for various asset classes and types.
Asset Inspection (Field)	Asset Inspection Manager	Assists with collection of: <ul style="list-style-type: none"> • Asset issues that may result in failure. • Quantified asset condition information through inspection sets that are used to feed into Asset Health models.
Online Information	Pi Historian	Collects real time information from online condition monitoring equipment.
Threat Analysis	Bow-Tie XP	Provides a systematic way to identify hazards, the threats that may result in a loss of control, and the controls put in place to prevent or mitigate the consequences of a loss of control event. This process through Transgrid's formal safety assessment process identifies the significant hazards, threats and events that relate to the risks analysed in replacement analysis.
Corporate Risk	CAMMS	Repository for risk information related to Transgrid's Principal and Operational risks.

6.2.3. Risk Acceptance Criteria

This document is aligned with the corporate Risk Management Framework document and Transgrid Risk Appetite Statement by:

- Coherence in asset risk assessment with corporate risk assessment process.
- Asset risk is evaluated against the risk acceptance criteria for the Principal Risks:
 - Health, Safety, and Environment, which has a risk appetite level of As Low As Reasonably Practicable.
 - Network Reliability, which has a risk appetite level of Medium and there is an expectation this is managed As Low As Reasonably Practicable with the Transgrid having no tolerance for a material loss of supply event.
 - Network Safety which have a risk appetite level of High and with the Transgrid having no tolerance for network safety events that could result in loss of life, permanent disability or significant environmental damage. Network safety regulations require these risks to be eliminated, and if not reasonably practicable to be reduced As Low As Reasonably Practicable.
- The risk acceptance criteria applied as per the Electricity Network Safety Management System Description document.

6.2.4. Risk Quantification

Risk is quantified by multiplying likelihood and consequence. The monetary value of risk (per year) for an individual asset failure resulting in an undesired outcome, is the likelihood (probability) of failure (in that year with respect to its effective age), as determined through modelling the failure behaviour of an asset (Asset Health), multiplied by the consequence (cost of the impact) of the undesired outcome occurring, as determined through the consequence analysis (Asset Criticality). Where multiple key hazards are applicable to an asset, the value of risk for each of these are summed to give the total value of risk associated with an asset. The equation for this quantitative risk assessment methodology is shown below.

By forecasting the likelihoods and consequence costs into the future, an annual forecast of the value of risk of an asset failure resulting in a Loss of Control and subsequent outcome is determined using:

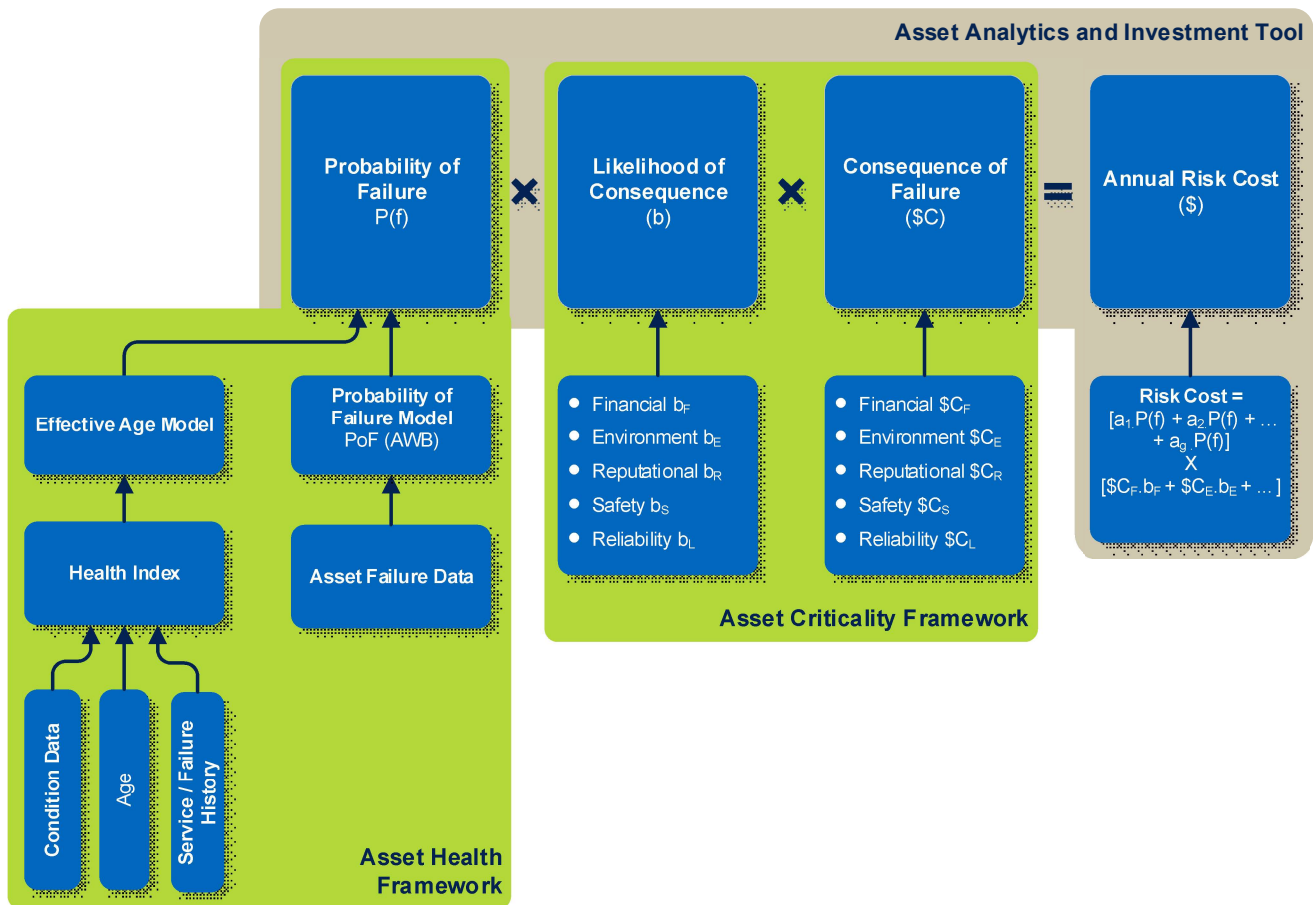
$$\text{Monetised value of risk (\$)} = \sum_{K=0}^{\gamma} P(\alpha_K) \cdot (\$C_1 \cdot \beta_1 + \$C_2 \cdot \beta_2 + \dots + \$C_i \cdot \beta_i)$$

Where:

- $P(\alpha_K)$ is the likelihood of failure attributable to failure mode K
- $\$C_i$ is the consequence category related to the failure mode for each category defined in Section 6.2.1.
- β_i is the likelihood of consequence related to the failure mode consequence $\$C_i$

A diagrammatic representation of the equation is shown below including the inputs that are required to develop the inputs to the risk cost calculation.

Figure 5 – Risk quantification methodology



The risk value is used to identify assets that require further attention and investigation, and determine the most suitable and timely investment option to manage asset risk to an acceptable level. By quantifying risk across all critical network assets, a view of the organisations asset risk profile can be determined. This can be utilised to analyse the impact on the risk profile of different funding scenarios and to broadly estimate the long-term replacement expenditure.

Appendix A provides the methodology for calculating Risk Cost for the following threats:

- Conductor Drop
- Earthing System Failure
- Unauthorised Tower Climbing
- Low Spans
- Supply Interruption
- Asset Explosion
- Unauthorised Substation Entry
- Protection Asset Failure

The risk value is also used as an input to prioritise and optimise capital investment at a portfolio level across Transgrid.

6.2.5. As Low As Reasonably Practicable (ALARP)

Transgrid operations are principally in NSW and are required to abide by:

- As an electricity network operator the Electricity Supply (Safety and Network Management) Regulation 2014 (the Regulation). This regulation requires that a network operator must take all reasonable steps to ensure that the planning, design, construction, commissioning, compliance, maintenance, renewal and decommissioning of its network (or any part of its network) is safe and mandates for network operators to comply with AS5577 'Electricity Network Safety Management Systems'. This regulation requires hazards associated are identified, recorded, assessed and managed by eliminating **safety risks so far as is reasonably practicable (SFAIRP)**, and if it is not reasonably practicable to do so, by reducing those risks to **as low as reasonably practicable (ALARP)**. The objective of the regulation is to support:
 - The safety of the public and persons near or working on the network.
 - The protection of property and network assets.
 - Management of safety aspects arising from the protection of the environment, including protection from ignition of fires by electricity networks.
 - Management of safety aspects arising from the loss of electricity supply.
- As an employer, the Work Health and Safety Regulation 2017 requires:
 - Elimination of health and safety risks so far as is reasonably practicable; and
 - If it is not reasonably practicable to eliminate risks to health and safety – minimise those risks SFAIRP.

The definition of 'practicable' is principally the same under both the Electricity Supply (Safety and Network Management) and HSE regulations and require that in order to manage risk all reasonable controls must be applied. The following extract of the NSW Safety Act defining the requirements for demonstrating practicable. Within this document, compliance with SFAIRP and ALARP are considered synonymous and referred to as ALARP.

"...in relation to a duty to ensure health and safety, means that which is, or was at a particular time, reasonably able to be done in relation to ensuring health and safety, taking into account and weighing up all relevant matters including:

- (a) the likelihood² 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 the person concerned knows, or ought reasonably to know, about:*
 - (i) the hazard or the risk, and*
 - (ii) 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 available ways of eliminating or minimising the risk, including whether the cost is grossly disproportionate to the risk."*

As Transgrid develops assets in other jurisdictions it is bound to also comply with the relevant regulations in that area.

² Note that Victorian Electricity Safety Act excludes likelihood in defining practicable.

In performing network analytics it is necessary to show that solutions are reducing risk to ALARP, and acceptable controls such as maintenance or capital expenditure are based on the reduction of risk to ALARP. This is achieved by the application of disproportionality factors on risk consequences when performing risk based calculations. These factors have been selected based on guidance from AER³ and HSE UK⁴ and are generally in the range of 1 to 10, the latter being for risks that involve high value widespread consequences such as nuclear accidents.

Transgrid use the following factors to demonstrate credible options, including the proposed option, satisfies ALARP once the scope of the options applies the hierarchy of controls.

Network safety risk reduction benefit should be calculated as:

$$Network\ Safety\ Risk\ Reduction\ (\$) = R \times \Delta\$Reliability\ Risk + S \times \Delta\$Safety\ Risk + B \times \Delta\$Bushfire\ Risk$$

where Δ is the pre-investment risk minus the post-investment risk.

Table 3 – Determination of network safety risk reduction benefit

Risk	Consequence Severity	Disproportionality Multiplier
Safety (S)	Potential for single fatality (Transgrid staff). e.g. explosive failure of plant	3
Safety (S)	Potential for multiple fatalities (Transgrid staff and the public). e.g. conductor drop	6
Bushfire (B)	Potential for multiple fatalities (Transgrid staff and public) and extensive property damage.	6
Environment (E) (Excluding Bushfire)	Potential for serious, long term, widespread environmental damage. (SF6 loss or oil spills)	3 ⁵
Reliability (R)	Potential for multiple fatalities (public only) due to interruption to electricity supply	0.1

The multipliers (S and B) represent the organisation's obligation to spend more than the value of the safety and bushfire risk avoided to reduce the risk, and the proportion that would be deemed reasonable by an objective third party (e.g. courts). For example, it may be deemed reasonable for an organisation to spend \$3 for every \$1 of risk reduction (a multiple of 3). The multiple also reflects the severity of the consequence of the risk. For example, a bushfire has the potential to cause extensive harm, including a great number of fatalities and extensive property damage, while an explosive plant failure in a substation has a much more limited potential impact. As such, it is not unreasonable to say an organisation would be expected to spend a greater multiple to reduce and manage the bushfire risk, as compared to the multiple used for the explosive plant failure risk.

The ALARP concept will be consistently applied to decision making across all life cycle stages of network assets (plan, build, maintain, operate, and replace or decommission), in addition to other considerations such as legislation (Work Health and Safety Act), and industry guidelines and standards.

³ Australian Energy regulator, Industry practice application note, Asset replacement planning - January 2019

⁴ HSE (Health and Safety Executive, United Kingdom), 2001, Reducing Risks, Protecting People, Her Majesty's Stationery Office, London, www.hse.gov.uk/risk/theory/r2p2.pdf.

⁵ Note that the AAIT includes Bushfire (B) and Environmental (E) risk in the one category Environmental and so only applies one disproportionality multiplier. To account for the different multipliers non bushfire risk including SF6 leakage and oil leaks will have the risk outcomes halved in performing risk analysis.

In the context of REPEX, ALARP is demonstrated in the Options Evaluation Report stage. The scoping of the credible options considers the hierarchy of controls. The credible options are tested for economic viability (positive net present value of option) and application of the disproportionality test, all of which is referred to as cost benefit analysis. The cost benefit analysis should consider the cost of each feasible option and the associated network safety risk reduction benefit (pre-investment risk minus post-investment risk). The difference in pre and post-investment risk is multiplied by the appropriate disproportionality multiplier, taking into consideration the type of risk and severity of the consequence of the risk. If the cost benefit analysis returns a positive result, the option is considered for implementation. The option that provides the maximum network safety risk reduction benefit and is most economical is proposed for DG1.

Example: A 132kV Transmission Line with numerous condition based issues, including deteriorating wooden poles, insulators, and conductors.

The options evaluated to address the condition issues are shown in Table 4.

Table 4 – Option Evaluation

Option	Option Description	Capital (\$m)	NPV (\$m)
A	Replace poor condition wooden poles with concrete poles.	6.8	31.4
B	Replace all wooden poles with concrete poles.	35.2	37.9
C	Replace all wooden poles with concrete poles and replace the conductor.	43.3	30.8

Option B provides the highest NPV of all the considered options. However there is a need to remediate condition issues in order to manage network safety risk levels to ALARP. The ALARP evaluation for each options are shown in Table 5.

Table 5 – ALARP Test Option Evaluation

Option	Network Safety Risk Reduction (\$m)	Annualised Capex (\$m)	Reasonably Practicable
A	0.40	0.36	Yes
B	1.65	1.90	No
C	1.83	1.87	No

The result of the ALARP evaluation is that Option A is above the ALARP threshold, so that work needs to be completed to manage our safety obligations and community expectations.

Option A would be the preferred option if the ‘non ALARP’ options have a negative or lower NPV or do not address the safety risk. In this case, Option B mitigates the risks associated with Option A and has additional benefits, resulting in Option B as the preferred option.

Where greater than 50% of the pre-investment network safety risk is comprised of reliability related safety risk, it is not necessary to apply the disproportionality test. This is because the overall economic cost benefit analysis inherently ensures that the network safety risk is being reduced to ALARP in circumstances where the primary driver for investment is reliability risk.

It should also be noted that AS 5577 requires that an option that provides the greatest safety and bushfire risk reduction benefit should be progressed irrespective of cost, until an acceptable level of residual risk is achieved (where Reasonably Practicable to do so). The assessment a particular risk is unacceptable is an inherent part of the risk assessment process and is based on expectations as represented through

accepted industry standards and guidelines. This applies both in relation to level of acceptability of the residual risk, and the application of appropriate controls in order to minimise the risk to ALARP. In doing so, Transgrid notes that consideration of the availability and suitability of ways to eliminate or minimise the risk, as is required under relevant safety legislation and, may at times require assessment based on non quantified risk, beyond the earlier mentioned disproportionality methodology.

In the capital works program, projects driven by the ALARP requirement should be the highest priority. A project in the capital works program driven by the ALARP requirement can only be removed, rescheduled, or in any other way modified with a risk assessment signed off at the appropriate level as per delegations of authority.

High Consequence / Low Likelihood ‘Black Swan Events’

In evaluating risks, edge cases may materialise where outcomes are considered unacceptable by societal standards and as such must have controls in place that are not justified under the standard disproportionality, VSL and VCR factors given in this document. This will generally be due to foreseeable threats and consequences that are not in line with the risk profiles that the standard factors were developed upon. In-line with AER guidance, alternative values may be used. These must be supported with sufficient evidence to justify their use over accepted values and be consistent with AER or industry guidance where available.

6.2.6. Regulatory Obligations – Network Safety

Cases may originate where the need is based on a requirement to meet regulatory obligations and the societal obligations imposed by this. Where the need is identified by this requirement, it shall be clearly identified and the description of the identified need should cite the relevant sections of the law or regulation where safety standards or obligations are imposed. In the case of upgrading safety controls where the risk cannot be fully quantified, it needs to be clearly indicated why the existing control is no longer meeting expectation as an effective control.

Where the ALARP criteria is met (as per the NRAM), the relevant sections of the law or regulations should be quoted as:

- Under the Electricity Supply (Safety and Network Management) Regulation 2014 Section 5 ‘A network operator must take all reasonable steps to ensure that the design, construction, commissioning, operation and decommissioning of its network (or any part of its network) is safe.’

In general the application of regulatory obligations cannot be applied to like for like replacement and quantified risk analysis with stated disproportionality is required.

6.2.7. Sensitivity Analysis of the Risk Output

The risk outputs of the NRAM can be calibrated and checked for sensitivity at the portfolio level. This is achieved by varying the key inputs to the risk calculation simultaneously and observing the degree of variability within the risk output and comparing the estimated number of failures and risk consequences with historical values.

Sensitivity of the risk output should be checked by developing suitable statistical distributions of the below key inputs:

- Value of customer reliability
- Value of statistical life
- Load at Risk

- Disproportionality factors
 - ALARP safety multiplier
 - ALARP bushfire multiplier
 - ALARP reliability multiplier
- Probability of failure
- OPEX and other benefits
- Discount rate

These inputs are considered important as they predominantly drive the overall risk output. Distributions are to be developed based on actual samples although alternative methods are acceptable in case of insufficient data.

6.3. Asset Health Framework

The following summarises the main concepts required in Asset Health management and its input to asset effective age input to the risk models. The scope of the framework is shown in Figure 5.

Asset Health is used to estimate the effective age of an asset, and to forecast the associated likelihood of failure of the asset now and into the future. The modelling takes input from current and historical asset information including, failure, defect, maintenance and condition data, and operational/performance information. The inputs to the Asset Health model are given weightings according to their significance to overall longevity of the asset. The failure behaviour of these assets is modelled by determining a statistical distribution and parameters that best fit the time to failure (or any other indicator of failure) of past failures, as determined by examining historical failure data. Asset Health is used as an input to the likelihood input to the risk assessment.

Asset Health supports the risk assessment by placing every major asset in a conditional state by comparing its health information (such as nameplate information, condition information, inspection/test results, defect/corrective maintenance data, and advice from maintenance staff) to the end-of-life criteria and thresholds for the asset type. These criteria and thresholds have been established from past experience with assets that have reached end-of-serviceable-life, expert advice and global best practice. The conditional states map to an age (termed the effective age), and probability of failure, based on an understanding of the expected health of the asset at these ages, in respect of the end-of-life criteria and thresholds.

A detailed framework and procedure for Asset Health management is provided in the 'Network Asset Health Framework' document.

6.4. Asset Criticality Framework

Asset criticality expresses the consequences of an undesired outcome.

shows the scope of Asset Criticality in the Risk Assessment process. Asset criticality considers the severity of the consequences following the asset failure (or Loss of Control Event) occurring, and the likelihood the consequence will eventuate. The analysis leverages experience with past events, accepted research/publications and best judgement to determine an economic value of the impact. Asset Criticality is used as an input to the consequence input to the risk assessment.

The analysis of the severity of the consequence assigns an economic value to the likely worst case impact in respect of the areas of consequence the organisation is concerned about. The analysis of the likelihood

of the consequence is used to determine the probability of the impact eventuating for the non-financial areas of consequence. This is to account for the fact that the combination of and economic value of consequences varies with and is dependent on the nature of the undesired outcome.

The broad areas of consequence are aligned with the corporate risk management framework.

6.5. Cyber-Security Risk Assessment

Cyber-security is a growing risk and has been identified as a component of Transgrid's Security Strategic Risk 'Protective and Cyber Security Risk' reported to the board.

Cyber security risk is evaluated based on protection from threat actors and utilises a specific evaluation methodology. This cyber-security risk assessment methodology and criticality framework to Operational Technology (OT) assets is included in Appendix B.

6.6. Network Safety Formal Safety Assessment

6.6.1. Overview

Network Safety Formal Safety Assessment is performed as a means of identifying:

- Credible threats that have the capacity for Transgrid to lose control of material hazards.
- Potential consequences from loss of control of the hazard.
- Preventive and mitigative controls that prevent loss of control, or mitigate the consequences respectively.

Transgrid perform network Safety Formal Safety Assessment in accordance with *AS5577 'Electricity Network Safety Management Systems'* that is required to meet its statutory regulation requirements for ensuring:

- (a) the safety of the public, and persons near or working on the network;
- (b) the protection of property and network assets;
- (c) safety aspects arising from the protection of the environment, including
- (d) protection from ignition of fires by electricity networks; and
- (e) safety aspects arising from the loss of electricity supply.

The outputs of Network Safety Formal Safety Assessments are used as inputs to the following processes:

- Risk controls for application in the design, construction, operations, maintenance, and disposal phases through actions defined in the relevant asset management plans.
- Threats, consequences, and Loss of Control Events that provide criteria and risk factors to be considered in Investment Analytics.

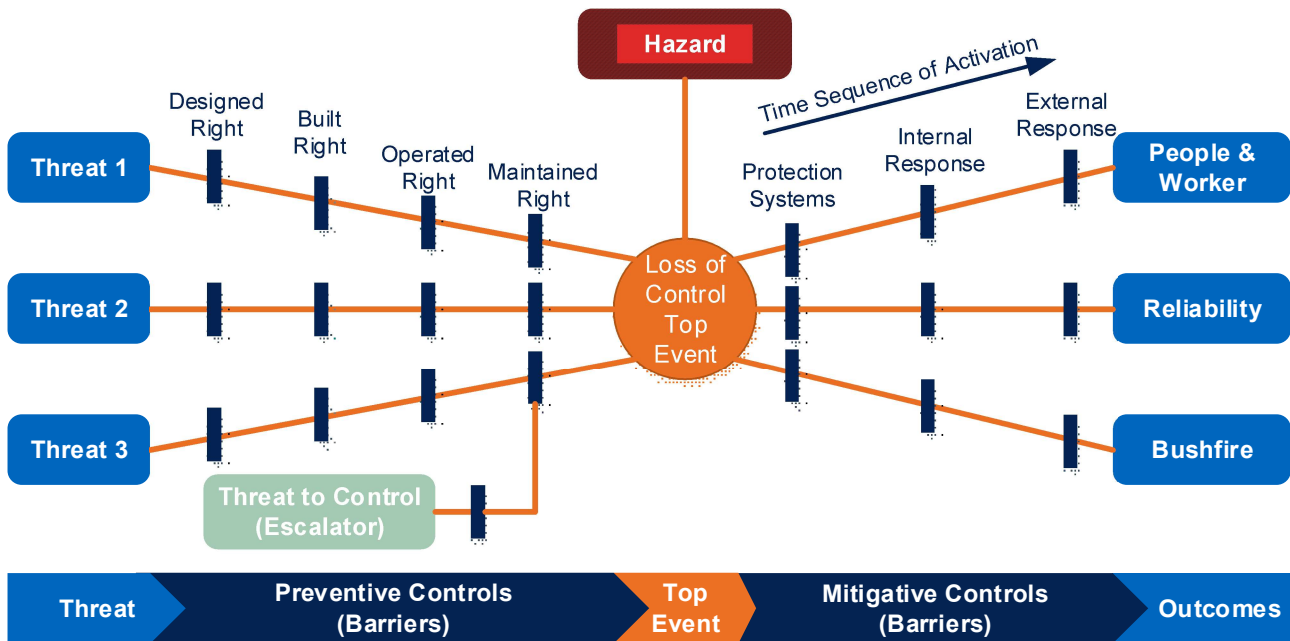
For details of the relevant asset management plans refer to the Electricity Network Safety Management System Description and supporting Formal Safety Assessment documents.

6.6.2. Threat/control/consequence mapping

Transgrid utilises the Bow-Tie method for identifying hazards, the threats that may lead to the loss of control of the hazards, the consequences that may occur from the loss of control and the preventive and mitigative controls required to prevent undesired outcomes. The framework for this analysis is shown in Figure 6.

The mapping exercise provides a visual representation of elements of the NRAM and how they contribute to the overall risk assessment, and what controls are in place to manage the risk. This identifies gaps and assess the effectiveness of the controls, and if necessary, a change or implementation of new the controls to manage the risks.

Figure 6 – Elements of Threat Consequence Mapping



The definitions for the core components of this process are shown in Table 6.

Table 6 – Bow Tie Component Definitions

Component	Description
Hazard	<p>The condition, object or activity with the potential of causing injuries to personnel, damage to equipment or structures, loss of material or reduction of ability to perform a prescribed function.</p> <p>For transmission physical asset risks represents potentially damaging energies (conditions and activities) in or adjacent to the network where the loss of control will result in potential damage and adverse outcomes. Typical hazards at Transgrid include:</p> <ul style="list-style-type: none"> • Electricity (risk from the network) • Vegetation (risk to the network) • Construction and maintenance activities • Public industrial and recreational activities adjacent to the network. • Social stressors (Resulting in sabotage, suicide, etc.)
Top Event (Loss of Control point)	A point in time which describes the release or loss of control over a Hazard that creates an undesired system state.
Threat	A possible direct cause that will potentially realise the loss of control of a hazard by initiating a top event
Consequences	A potential event resulting from the loss of control of a Hazard, which directly results in loss or damage.

Component	Description
	To align with AS5577 requirements the consequences shall generally be categorised to outcomes of: <ul style="list-style-type: none"> • Bushfire • Public Safety • Worker Safety • Reliability (safety related aspects) • Damage to property and the environment.
Preventive Controls	Any measure taken which acts against some undesirable force or intention to maintain a desired state. The preventive controls shall be identified in the order that they would occur during the life cycle stages of the asset. More than one control can be identified during each life cycle phase.
Mitigative Controls	These controls are considered to reduce the likelihood of the top event developing into a consequence or mitigating the severity of the consequence. The mitigative controls shall be identified in the time sequence that they will become active. e.g. automatic protection systems will generally occur first, followed by control room operators and then if required emergency response procedures will be activated internally and externally.
Escalator	A condition that leads to increased risk by defeating or reducing the effectiveness of controls (a control decay mechanism).
Escalation Factor Controls	A control that manages the conditions which reduce the effectiveness of other controls.

Reference: <https://www.caa.co.uk/Safety-initiatives-and-resources/Working-with-industry/Bowtie/Bowtie-elements>

6.6.3. Control Criticality and Effectiveness

When identifying controls, it is accepted that there is a level of uncertainty as to the criticality and effectiveness of the identified controls. This uncertainty is managed through:

Control Criticality

A control shall be identified as critical where failure of it has a reasonable probability of not preventing a threat to materialise or mitigate an undesired outcome from occurring.

Not all controls will have the same importance to the management of a specific threat. Identifying a controls significance according to criticality provides benefits such as:

- Focusing attention for the purpose of communication to stakeholders.
- Highlighting which controls require a greater depth of detail in terms of escalation factor consideration.

Standard controls are still required for the management of the threat (otherwise there would be no reason to have them) and their importance should not be disregarded. For example, having several standard controls failing in sequence may be just as significant a problem as having one critical control failure.

To assist with the decision as to whether a control should be classified as critical or standard, consider the following questions:

- If the control were absent or rated as 'partially effective', would you be thinking of stopping the operation?

- If the control were absent or only rated as 'partially effective' would it be likely to be rated as a material or non-material non-compliance in a system audit?

Control Effectiveness

Control effectiveness refers to the probability that will effectively act in preventing or mitigating the magnitude of an undesired outcome. The effectiveness of controls shall be evaluated based on its ability to prevent the undesired outcome considering the controls design, application, and its classification in the hierarchy of controls.

Table 7 – Risk treatment effectiveness measures

Risk treatment effectiveness	Qualitative description
Effective	Controls are well designed for the risk, address the root causes and Management believes that they are effective and reliable at all times.
Partially effective	While the design of controls may be largely correct in that they treat most of the root causes of the risk, they are not currently very effective, or Some of the controls do not seem correctly designed in that they do not treat root causes, those that are correctly designed are operating effectively.
Ineffective	Significant control gaps either due to design or issues discovered at implementation. Either controls do not treat root causes or they do not operate at all effectively.

6.6.4. Critical Control Management

Critical Control Management (CCM) is a process focused in improving control over rare but potentially catastrophic events. These sorts of events are known within Transgrid as High Potential Incidents. CCM recognises that prevention of High Potential Incidents requires specific attention at the highest level of an organisation and is based on:

- Having clarity on the controls that really matter
- Defining the performance required of those controls
- Defining what needs to be checked to ensure these controls are performing as intended
- Assigning accountability for undertaking the identified checks
- Reporting to an appropriate level within the organisation to ensure actions can be taken proactively to prevent a High Potential Incident.

The CCM approach uses bowties to provide a link between High Potential Incidents and an identified smaller number of critical controls, then establishing measurement and reporting of control effectiveness. It supports the development of an effective safety culture through more productive and insightful “visible leadership” interactions between managers and the workforce.

CCM is currently managed through regular review and sign off of controls within the CAMMS Incident and Risk system.

7. Integration with asset management strategies and plans

The asset management strategies and plans use a risk based approach guided by the Network Asset Risk Management Framework.

7.1. Maintenance plans

Transgrid's asset management challenge is the balance of risks against the direct costs of ownership (including undertaking maintenance work), and the performance of the assets. As such the objective identification, assessment, and evaluation of the risks associated with the asset through the consideration of its failure modes and root causes, likelihood of failure, performance, and consequence of failure is required. This asset risk is then controlled ALARP through the setting of appropriate maintenance activities and frequencies. This is supported by an appropriate spares holding to control outage durations.

A copy of the maintenance and spares plans for each asset class is available on The Wire.

7.2. Renewal and maintenance strategies

When the risk associated with an asset cannot be managed through maintenance activities, and has exceeded the organisation's tolerance, the asset is identified for replacement, refurbishment, or disposal if no longer required. An assessment and evaluation of the risks associated with the asset through the consideration of its failure modes and root causes, likelihood of failure, performance, and consequence and criticality of failure is undertaken. The asset risk is managed through the development of credible, renewal, refurbishment, and disposal options to manage asset risk to ALARP.

Transgrid generally prioritises replacement, refurbishment, and disposal projects based on a descending order of risk.

A copy of the renewal and maintenance strategies for each asset class is available on The Wire.

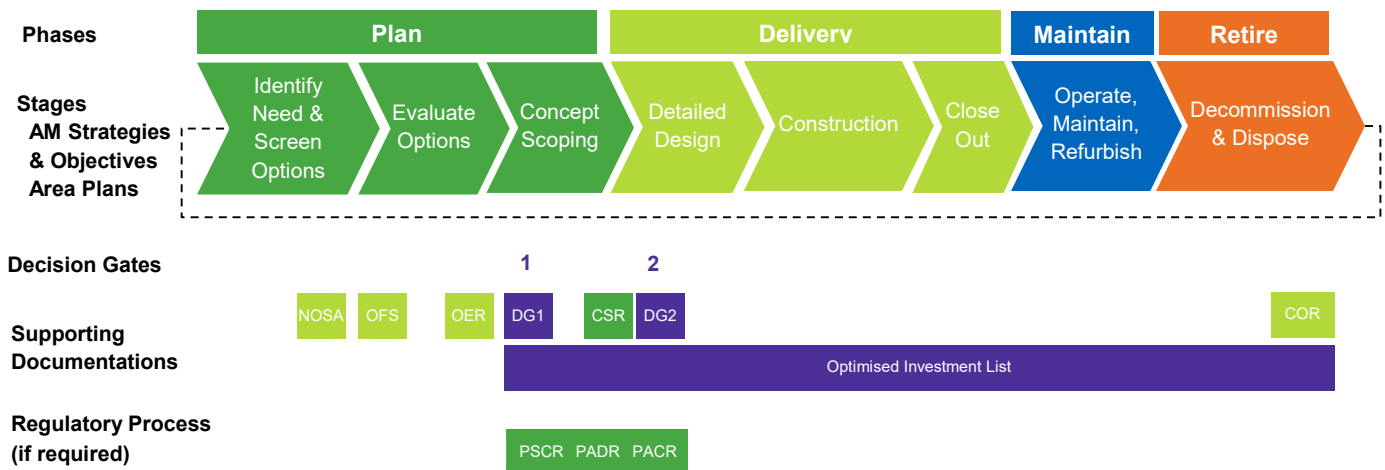
7.3. Interaction with the Prescribed Network Capital Investment Process

The NRAM identifies the risk value from the likelihood and consequence of asset failure. The risk value is then used to determine the appropriate treatment, including replacement where justified.

The risk value is used to prioritise projects to ensure Transgrid's overall risk exposure remains acceptable. In justifying investment decisions and prioritisation of projects when there are constraints on resources.

The interaction between the NRAM and investment process is shown below in Figure 7.

Figure 7 – Interaction between the NRAM and the investment process



The Prescribed Network Capital Investment Process is used to manage all capital investment options (replacement, refurbishment, or disposal) to manage asset risk to ALARP. The asset risk from current or emerging asset failure is assessed and evaluated according to the methodology in this framework, and used to identify where capital investment is required to manage the risk.

7.3.1. Need and Opportunity Screening Assessment (NOSA)

The identified risk is documented in a Need and Opportunity Screening Assessment (NOSA). The NOSA captures the asset risk associated with an asset, or group of assets, including the quantum of risk as determined through the methodology in this framework. In addition to the risk, the NOSA considers a range of factors including:

- Condition and health of the asset.
- Technical end of life or obsolescence of the asset, including availability of spares, ongoing manufacturer/supplier support.
- Compliance with Regulations and standards, such as the National Electricity Rules, security, safety, environmental and reliability.
- Operational and reliability performance of the asset, including maintenance and lifecycle costs, defects and faults.
- Other benefits.

7.3.2. Investment options

The NOSA is followed by an options identification and analysis process to identify credible options and evaluate options to address and/or mitigate the identified risks. The quantum of the risk reduction benefit (post investment risk minus the pre investment risk) for each credible option is determined via the methodology in this framework, and documented as part of each option. The scoping of proposed credible options takes into account the hierarchy of controls and the assessment of whether more can be done once the preferred option is selected. The preferred and selected option satisfies ALARP.

The outcome of this process is the Options Evaluation Report (OER) and subsequent approval of the preferred option. The preferred solution is considered to be that which meets Transgrid's constraints, addresses the investment drivers, and manages the risk to ALARP to satisfy the accepted level of risk.

A Decision Gate 1 is then prepared for approval of the proposed investment solution and commencement of the project. A Project Approval Document (PAD) / Decision Gate 2 will provide full approval to proceed with the project.

7.4. Interaction with Portfolio Investment

The NRAM guides a consistent and robust risk management process at the asset level. The outputs of the risk assessment and quantification are used as input to prioritise and optimise capital expenditure by balancing risk, cost, performance, value, capacity and constraints across the business, including the conflicting requirements of asset management and system planning. As such, the risk assessment and quantification at the asset level is consistent and compatible with the broader portfolio level approach. This approach is further defined in the Prescribed Network Capital Investment Process.

8. Accountability

Role	Responsibilities and Accountabilities
EM / Network Planning and Operations	<ul style="list-style-type: none"> • Implement the controls to manage asset risks in accordance with the corporate Risk Management Framework • Oversight of the processes for the identification and management of asset risks, including the Network Asset Risk Management Framework and the investment process.
Asset Management Committee	<ul style="list-style-type: none"> • Review and endorse the Network Asset Risk Management Framework • Oversight of the processes by which asset risks are managed • Monitoring the performance of Asset Management in managing the asset risks.
Head of Asset Management	<ul style="list-style-type: none"> • Ensure asset risk is being effectively managed • Approve and ensure the Network Asset Risk Management Framework is fit for purpose • Ensure consistent, effective and efficient implementation of the Network Asset Risk Management Framework • Monitor the development of Need and Opportunity Statements and investment options • Endorse Need and Opportunity Statements and investment options • Approve asset management strategies and plans.
Asset Systems and Compliance Manager	<ul style="list-style-type: none"> • Develop and refine the Network Asset Risk Management Framework • Establish and maintain a register of asset risks.
Asset Analytics and Insights Manager	<ul style="list-style-type: none"> • Develop the analytics capability and IT tools to facilitate the application of the Network Asset Risk Management Framework
Asset Managers	<ul style="list-style-type: none"> • Identify High Potential Incidents and risks • Apply the NRAM Framework to assess and evaluate asset risk • Manage the asset risks • Develop Need and Opportunity Statements • Develop investment options to address the asset risks • Develop the asset management strategies and plans.

9. Implementation

The NRAM will be implemented through:

- Discussions with managers during the various asset management committee and working group meetings
- Analysis and assessment of asset risk
- Development of Need and Opportunity Screening Assessments (NOSA)
- Consideration, analysis and evaluation of investment options through the investment process
- Development of the asset management strategies and plans
- Prioritisation and optimisation of capital expenditure at a portfolio level
- The Asset Analytics and Investment Tool (AAIT).

10. Monitoring and review

The NRAM is reviewed by the Asset Management Committee in accordance with the standard meeting schedule.

Asset risks are monitored and reviewed by the relevant Asset Manager at least annually via the refresh of the relevant Asset Renewal and Maintenance Strategy, or in response to an emerging issue, incident, or change in risk tolerance.

11. Change from previous version

Revision no.	Approved by	Amendment
0	Gerard Reiter, EGM/Asset Management	15 December 2015
1	Lance Wee, Manger / Asset Strategy	16 December 2016
2	Lance Wee, Manger / Asset Strategy	29 March 2017
3	Lance Wee, Head of Asset Management	2 September 2020
4	Andrew McAlpine (Acting), Head of Asset Management	Reformat into new template and update

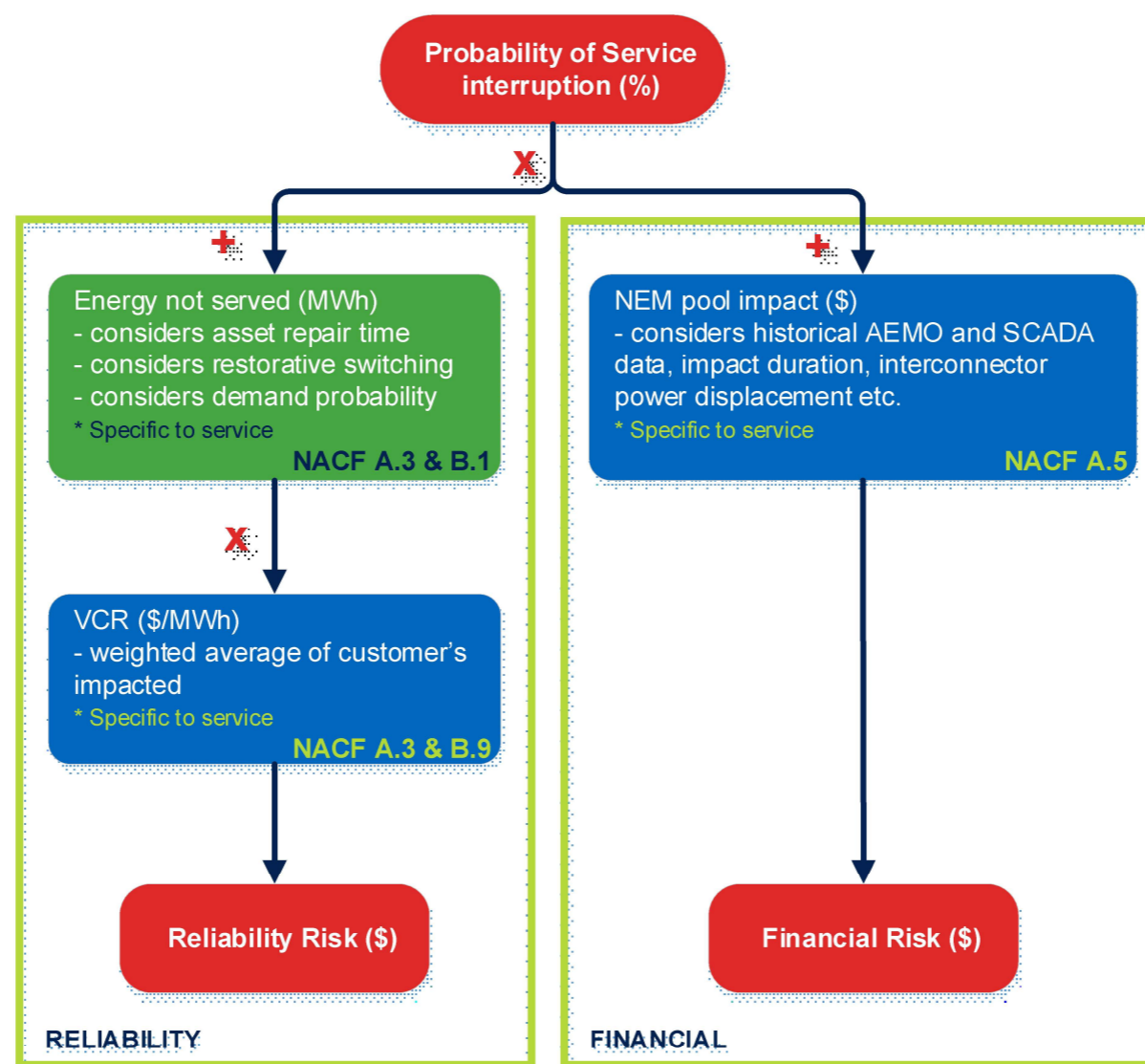
12. References

- Corporate Risk Management Framework
- Prescribed Network Capital Investment Process
- Network Asset Strategy
- Network Asset Health Framework
- Network Asset Criticality Framework

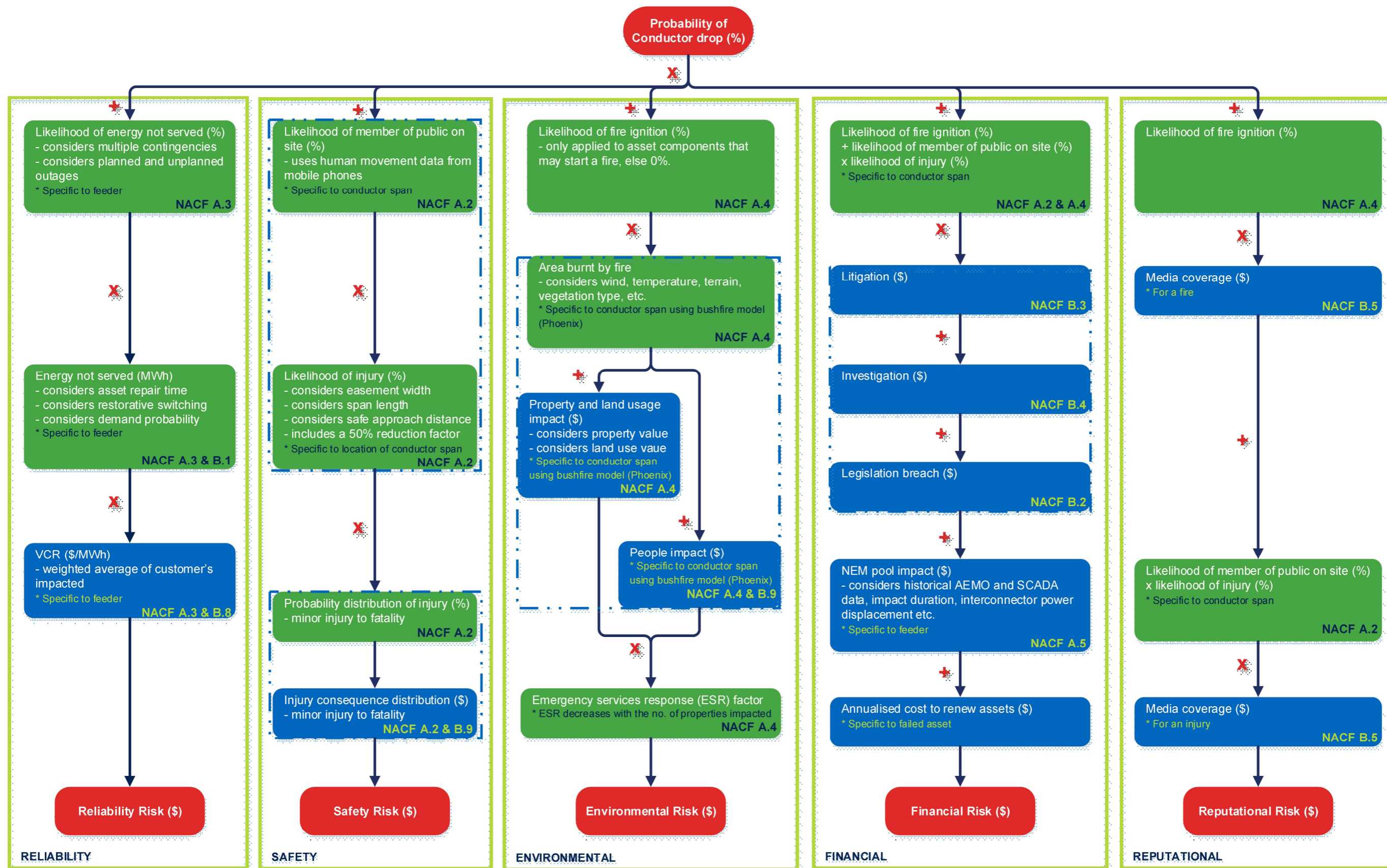
Appendix A - Risk Calculation Methodology

The following figures provide the basis on which risk cost calculations are performed for Transgrid's material hazardous events.

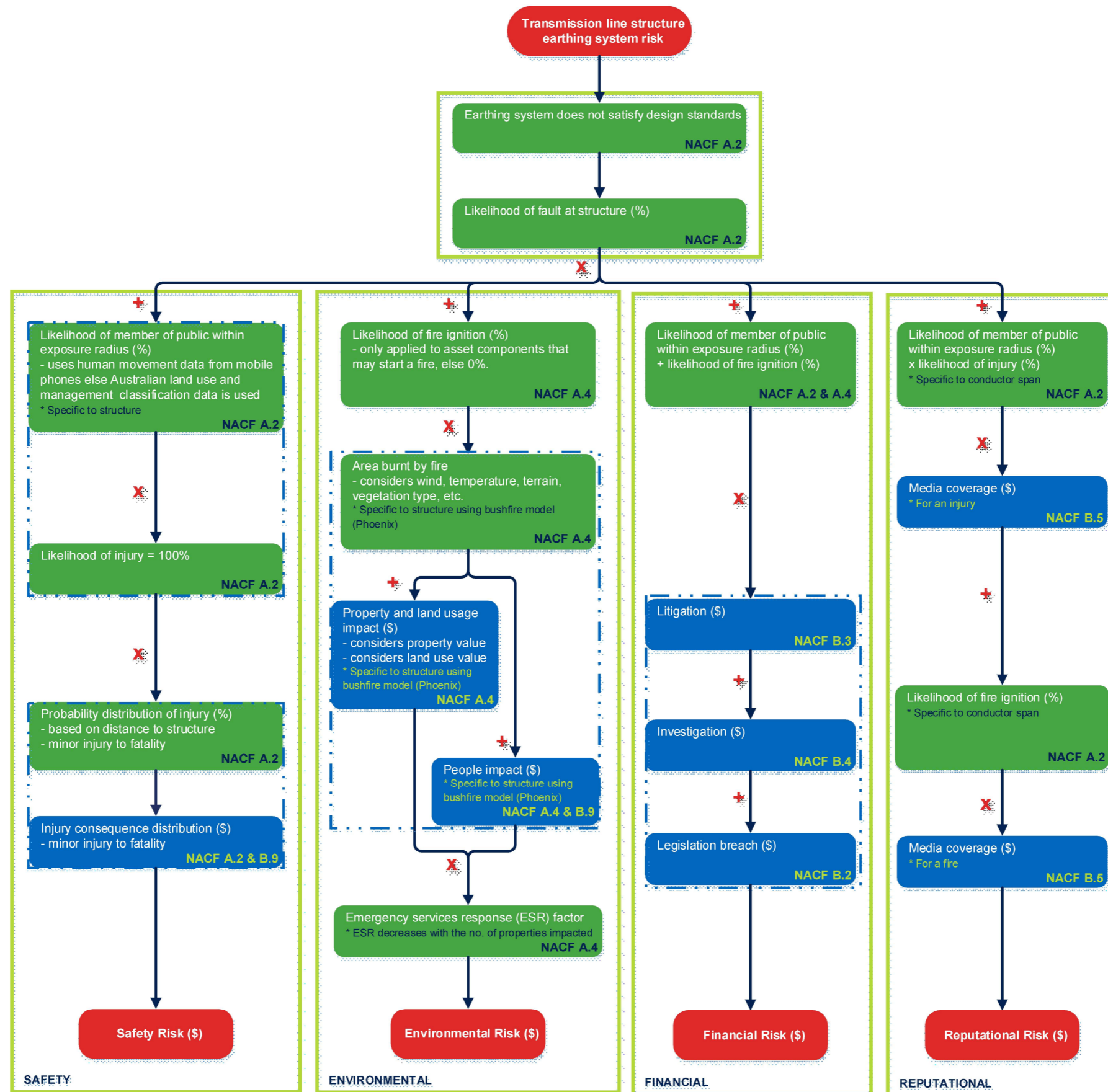
A.1 Supply Interruption



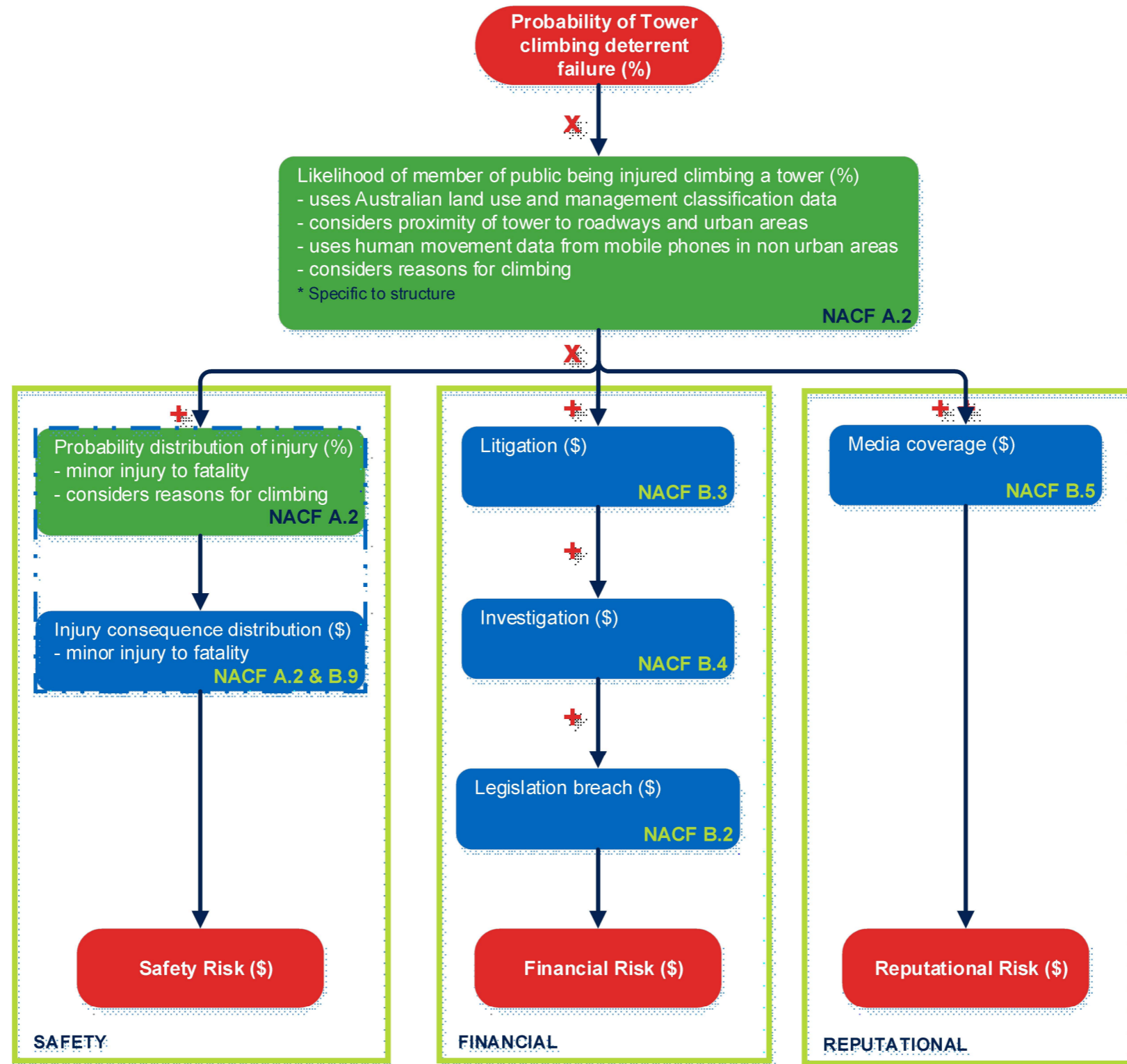
A.2 Conductor Drop



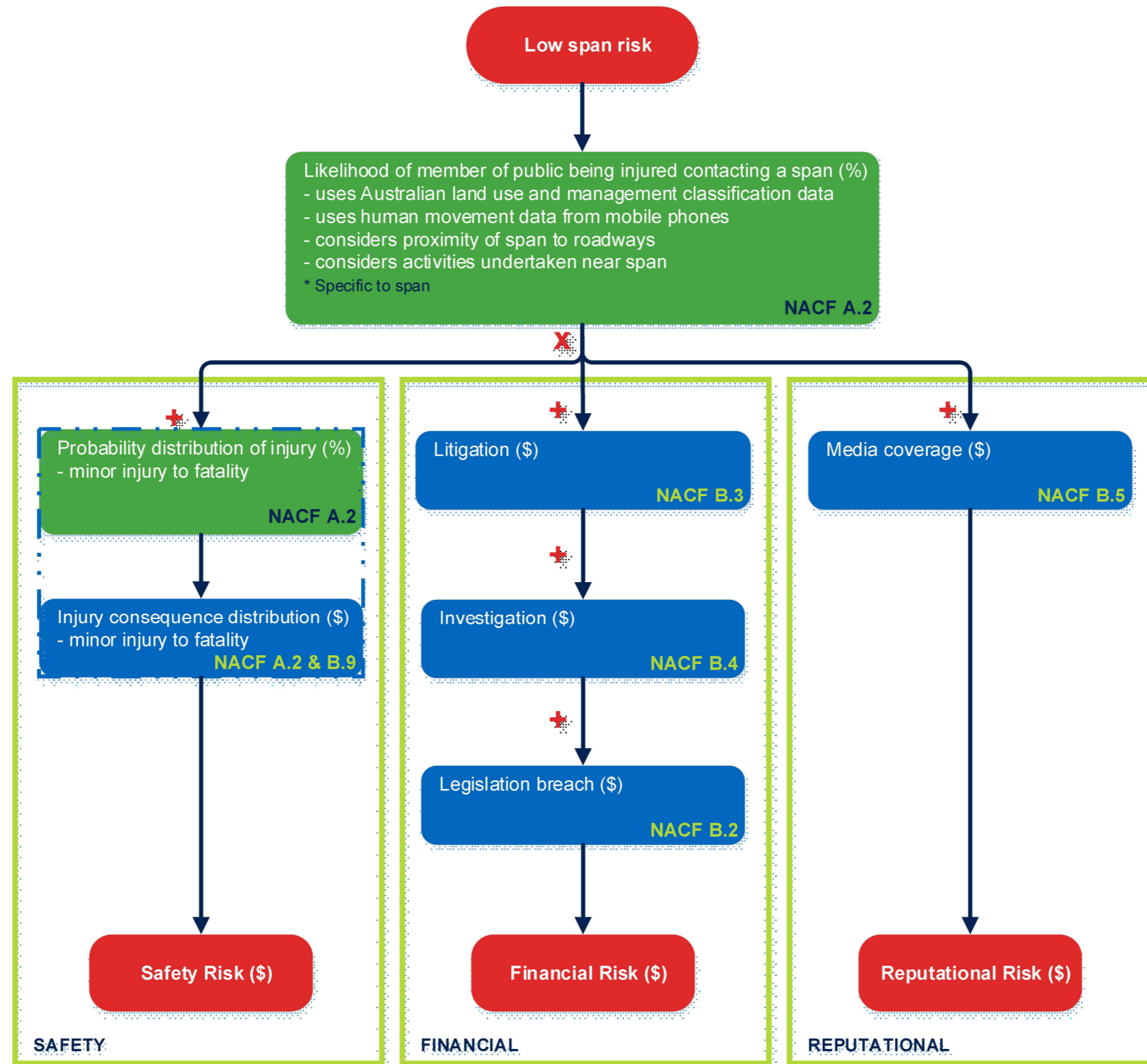
A.3 Earthing System Failure



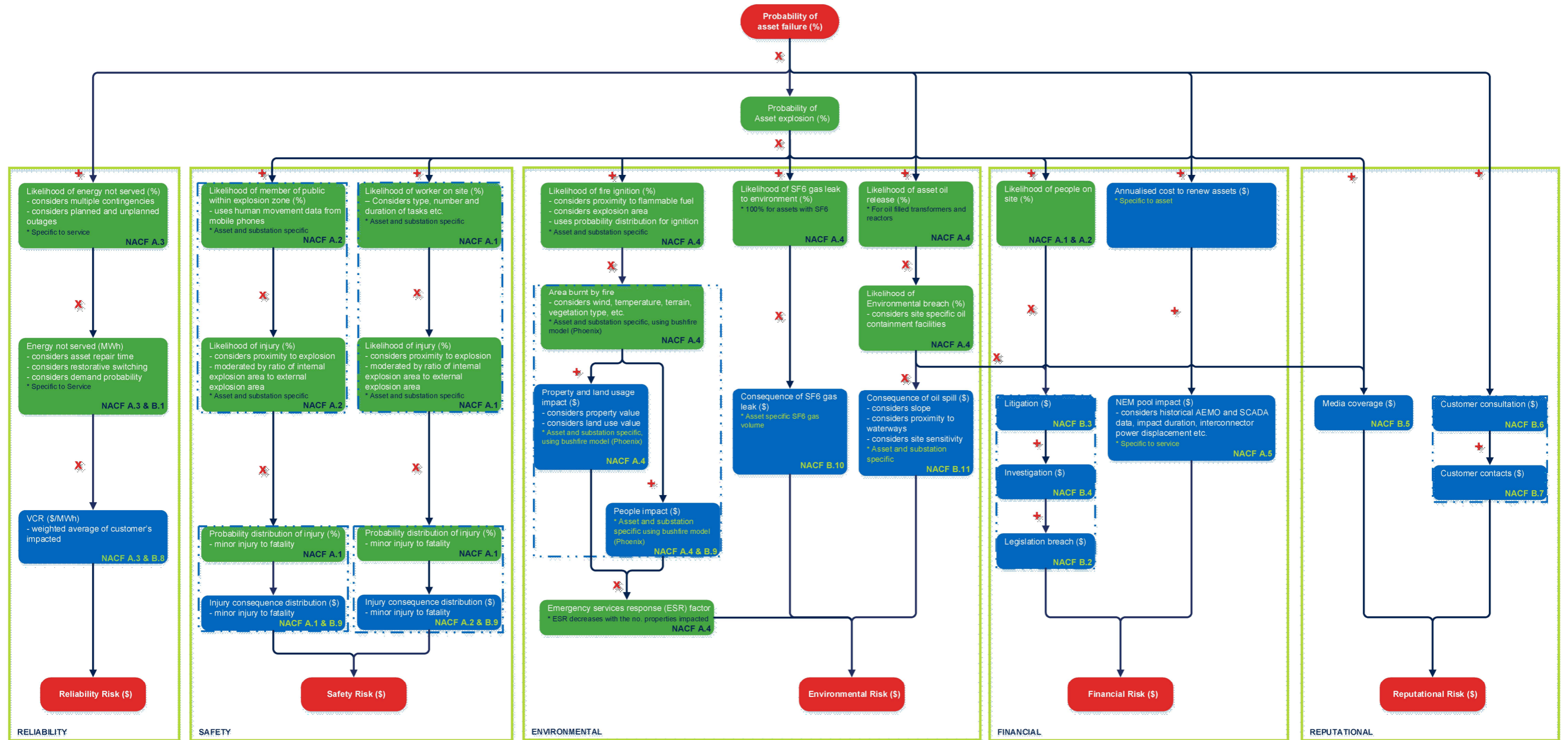
A.4 Unauthorised Tower Climbing



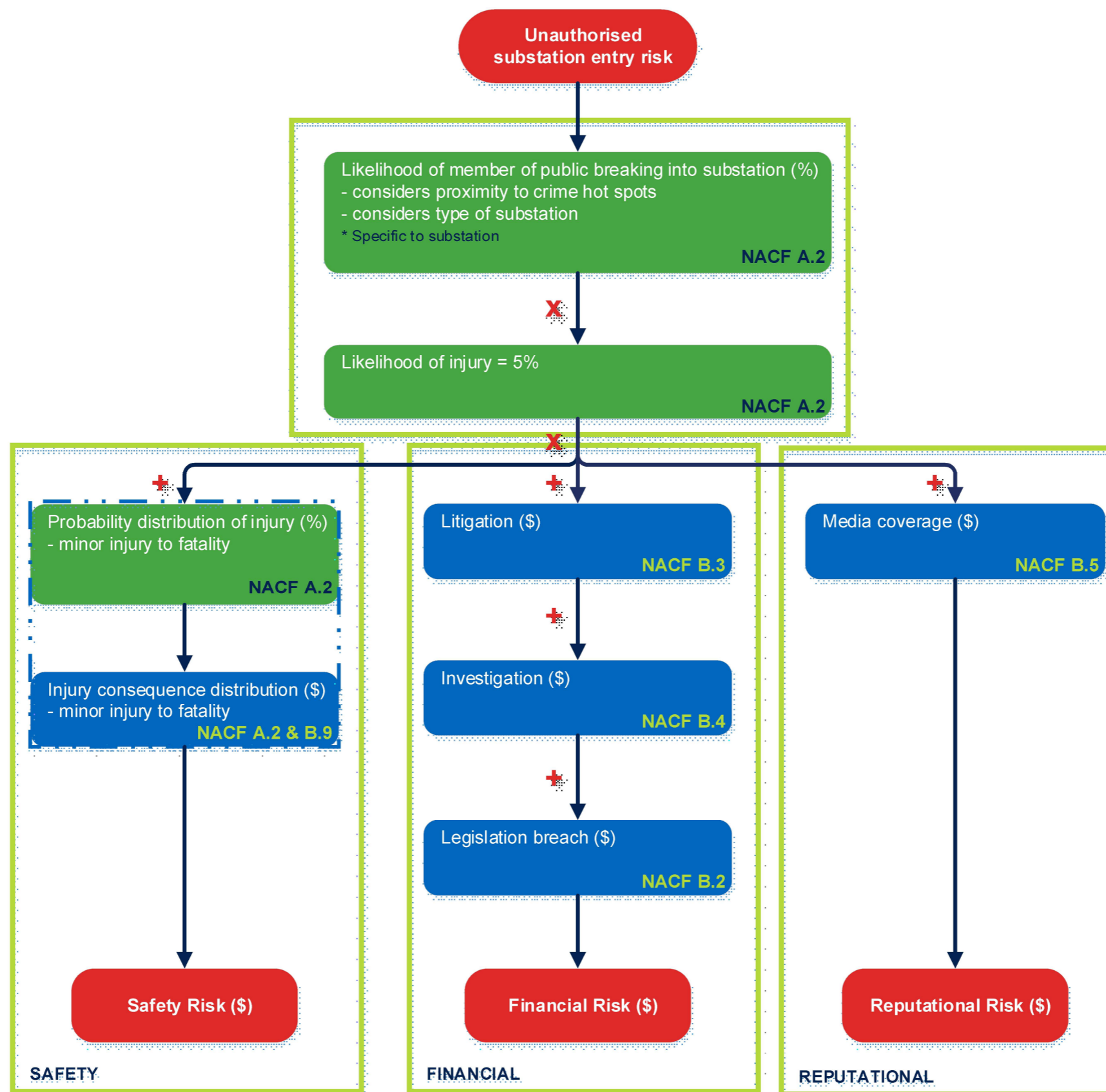
A.5 Low Span Risk



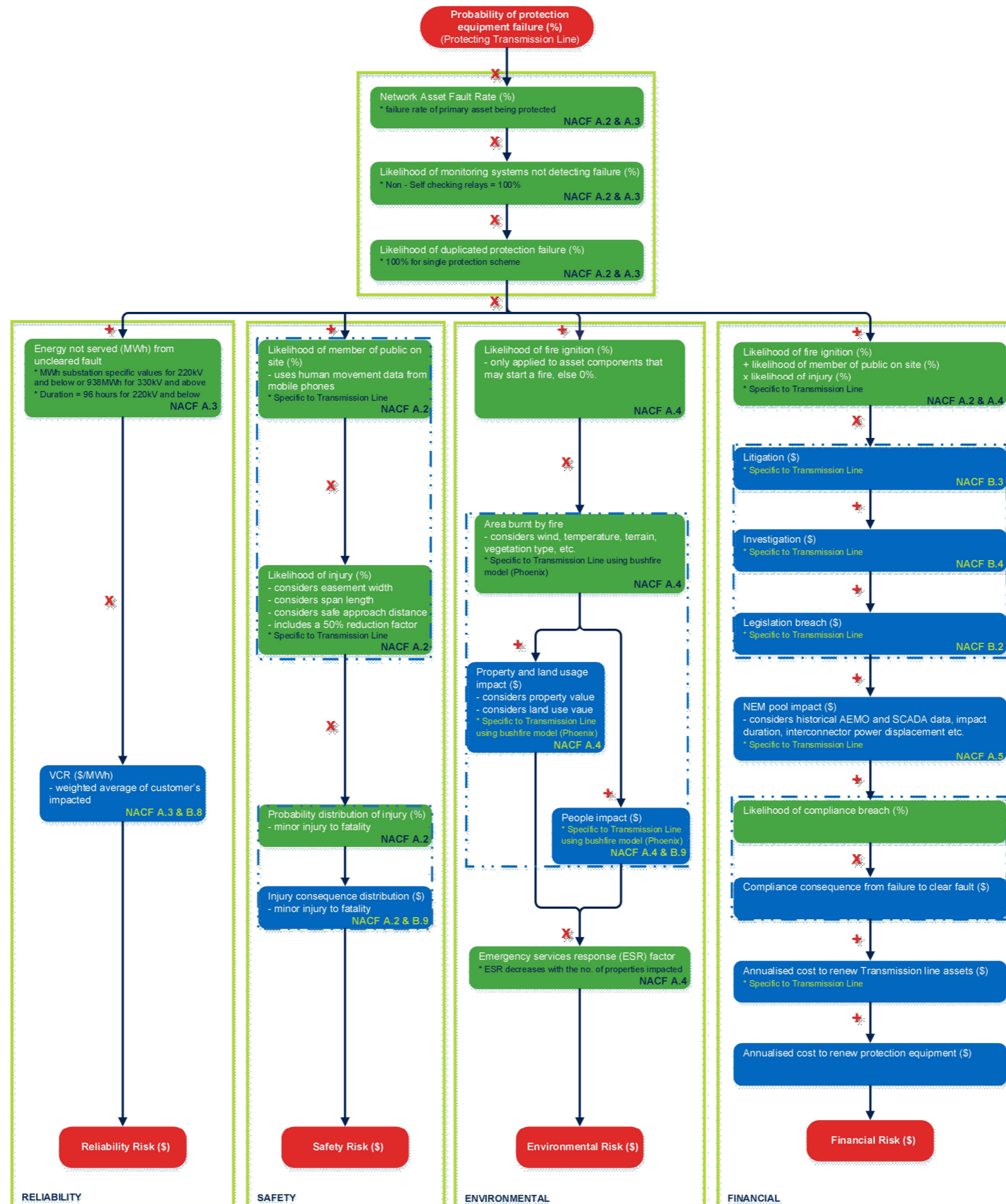
A.6 Asset Explosion



A.7 Unauthorised Substation Entry



A.8 Protection Asset Failure



Appendix B - Cyber Security Risk Assessment

B.1 Principles

Within the context of OT cyber security, the monetised value of risk is more simply expressed as follows:

$$\text{Monetised value of risk (\$)} = PoA \times LoB \times CoB$$

Where:

- *PoA* - Probability of Attack
- *LoB* - Likelihood of system Breach
- *CoB* - Consequence of system Breach

As part of continuous improvement this approach is expected to be further refined as more defined methods of quantification are developed..

B.2 Probability of Attack Considerations

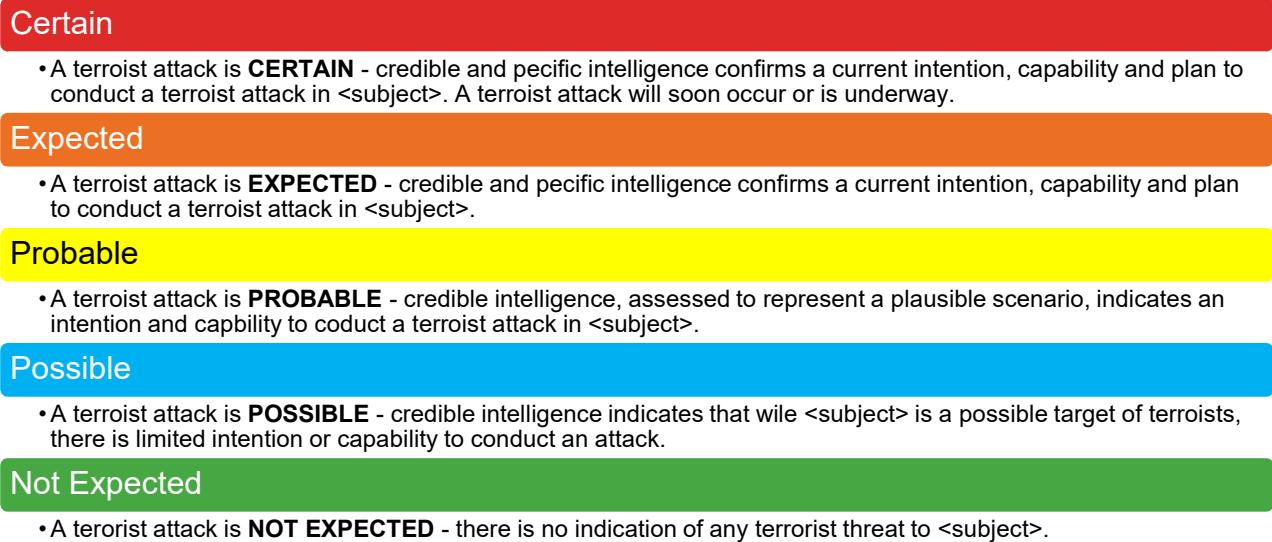
PoA is a qualitative assessment of the external cyber-security threats to Transgrid. The assessment is based on a number of information artefacts disseminated by various Australian security and advisory agencies. Factors used to assess PoA are outlined in Table 8 below.

Table 8 – PoA Inputs

Information Category	Usage	Module
Security Agency Assessments: <ul style="list-style-type: none"> • Australian Security Intelligence Organisation (ASIO): National Threat Assessment Centre • Australian Signals Directorate: Australian Cyber Security Centre (ACSC) • Other artefacts 	<ul style="list-style-type: none"> • National threat level • Specific threat to Australia's energy sector 	PoA assessment
Regulator Assessments: <ul style="list-style-type: none"> • Australian Energy Market Operator (AEMO) subsector criticality bands 	Regulatory assessment on criticality ranking	PoA assessment
Subject Matter Expert inputs <ul style="list-style-type: none"> • Chief Information Security Officer (CISO) 	Probability of Attack	PoA assessment

Australia's National Terrorism Threat Level is a scale of five levels providing advice about the likelihood of an act of terrorism occurring in Australia. When the threat level changes, government agencies release advice on what the level means and generic information regarding threats and potential targets. This threat is regularly reviewed in line with the security environment and intelligence. Terrorism threat levels are described below in Figure 8.

Figure 8 – Australia's National Terrorism Threat Level



The Australian Cyber Security Centre (ACSC) regularly release an Energy Sector snapshot report designed to inform decisions about investment and key focus areas within the critical infrastructure sector. The key PoA input published within this snapshot is the summary of cyber security incidents reported from within the energy sector.

This metric is used in combination with the national terrorism threat level to qualitatively assess the probability of attack to Transgrid's operations. Figure 9 below shows an extract of this table published in a 2019 report.

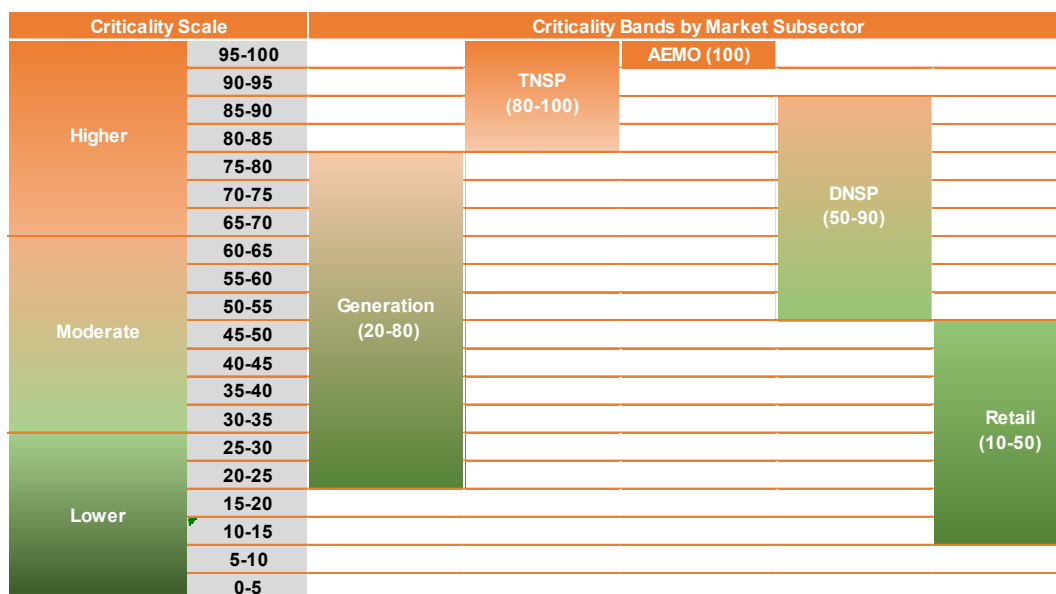
Figure 9 – Cyber security incident reports received by the ACSC (1 June 2020 to 30 June 2021)

Incident Type	Member(s) of the public	Small Organisation(s) Sole Traders	Medium-sized Organisations (s) Schools	State Government Academia/ R&D Large Organisation(s) Supply Chain	Federal Government / National infrastructure Supply Chain to CNI	National security Aus essential service(s) CNI Significant number impacted
Sustained disruption of essential systems and associated services	C6	C5	C4	C3	C2	C1
Exfiltration or deletion/damage of key sensitive data or intellectual property	C6	13	22	25	14	C1
Malware, beaoning or other active network intrusion; temporary system / service disruption	5	75	107	204	44	8
Low-level malicious attack – targeted reconnaissance, phishing, non-sensitive data loss	58	83	198	300	299	1
Scanning or reconnaissance	16	11	11	90	51	10

Source: www.cyber.gov.au

The third factual based input in the derivation of PoA is an energy market subsector criticality ranking published by the Australian Energy Market Operator (AEMO). This ranking provides insights into what portions of Australia’s energy networks are at highest risk of attack based on their criticality within the National Electricity Market (NEM). As an example, Figure 10 below from this publication ranks TNSP’s in the highest criticality band second only to AEMO.

Figure 10 – AEMO Market Subsector Criticality Bands



B.3 Likelihood of Breach Considerations

Likelihood of a breach is based on the qualitative assessment of Transgrid’s cyber security defences and the ability to repel threats effectively. This is outlined in Table 9 below:

Table 9 – LoB Inputs

Information Category	Usage	Module
Asset Information	<ul style="list-style-type: none"> Assessment of Transgrid cyber security system with regards to redundancy, maturity, functionalities, capabilities, monitoring, controls, protection, defences Assessment of expertise required to breach Transgrid cyber security system utilising the BORG cyber attack rating 	LoB assessment
Subject Matter Expert inputs Chief Information Security Officer (CISO)	<ul style="list-style-type: none"> Likelihood of Breach 	LoB assessment

In order to derive Likelihood of breach the Borg-Scale methodology⁶ has been chosen as an appropriate method. The Borg-Scale categorises cyber attackers into 5 main types namely:

- Vindictive Insiders
- Financial Criminals
- Ethno-nationalists
- Ideological Militants
- Nation States

The Borg-Scale identifies four specific areas of expertise necessary to successfully perform a cyber-security attack:

Table 10 – Borg-Scale Expertise

Expertise	Description
Business	Intimate knowledge of specific high value targets allowing attacker to benefit
Access	Ability to devise entry into relevant information systems and obtain desired information
Process	Knowledge of specific inputs to produce desired disruption
Programming	Ability to execute an attack to produce desired disruption

⁶ Estimating the Likelihood of Cyber Attacks When There’s “Insufficient Data”, Scott Borg

Table 11 is the qualitative assignment of comparative scores for demarcation of the 8 levels of attacker expertise.

Table 11 – Borg Scale Expertise Ratings

Expertise Ratings for Cyber Attacks (BORG Scale)		Comparative Score
Level Seven Expertise	Nearly unique intellectual gifts or knowledge of highly secret systems	1,000,000
Level Six Expertise	Deep insider experience or very elite, specialised training	100,000
Level Five Expertise	Substantial industry experience after a mid-level degree	10,000
Level Four Expertise	Solid mid-level university degree in the relevant subject	1,000
Level Three Expertise	Relevant undergraduate coursework	100
Level Two Expertise	Sustained interest in a relevant discipline	10
Level One Expertise	A few days of web surfing by an intelligent student	1
Level Zero Expertise	No special skill or knowledge whatsoever	0

Table 12 provides a guide as to the level of expertise required in each four areas of expertise, for various types of cyber security attacks.

Table 12 – Borg Scale Expertise Ratings and Scores to carry out Cyber Attacks

Some Minimum Expertise Ratings and Scores					
	Business Expertise	Access Expertise	Process Expertise	Program Expertise	Total Score
Common Worms and Viruses	Zero 0	Three 100	Zero 0	Two 10	110
Typical Credit Card Cyber Fraud	Three 100	Three 100	Two 10	Three 100	310
Larger criminal Enterprise Attack	Three 100	Four 1000	Four 1000	Three 100	2,200
Significant Infrastructure Attack	Three 100	Four 1000	Six 100,000	Five 10,000	111,100
National Cyber Assault Component	Five 10,000	Six 100,000	Six 100,000	Six 100,000	310,000

B.4 Consequence of Breach Considerations

Consequence of a breach is based on a combination of both qualitative and quantitative assessment of the impacts of cyber security breaches. This will generally be in line with the Network Asset Criticality Framework. The broad risk categories typically contributing to the cyber security risk calculation are outlined in Table 13 below.

Table 13 – CoB Inputs

Information Category	Usage	Module
Load Loss	Energy Not Served Event	CoB assessment
ENS Penalty	ENS Penalty	CoB assessment
Service Interruption	Customer Type	CoB assessment
Litigation	Litigation Type	CoB assessment

Appropriate risks will be selected based on the threat environment and types of attacks expected. Please refer to the Network Asset Criticality Framework for sample quantification of categories.

Appendix C - Risk Assessment Methodology Framework – Full Version

