
Asset Risk Assessment Overview

Asset Management System

PUBLIC

Document number	AMS 01-09
Issue number	1
Status	APPROVED
Approver	John Dyer
Date of approval	3 October 2019

Asset Risk Assessment Overview

ISSUE/AMENDMENT STATUS

Issue	Date	Description	Author	Approved
1	03/10/2019	Original issue.	A Dickinson	J Dyer

Disclaimer

This document belongs to AusNet Services and may or may not contain all available information on the subject matter this document purports. Information contained in this document is subject to review and AusNet Services may amend this document at any time. Amendments will be indicated in the Amendment Table, but AusNet Services does not undertake to keep this document up to date.

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

Contact

This document is the responsibility of Regulatory and Network Strategy department, Regulated Energy Services division of AusNet Services. Please contact the indicated owner of the document with any inquiries.

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

Asset Risk Assessment Overview

Table of Contents

ISSUE/AMENDMENT STATUS	2
1 INTRODUCTION	5
1.1 Purpose	5
1.2 Scope.....	5
1.3 Background.....	5
1.3.1 Risk Definitions.....	5
1.3.2 Risk Management Framework	5
1.3.3 Risk Management Process	6
1.3.4 Risk Assessment.....	7
2 OVERVIEW OF RISK ASSESSMENT TECHNIQUES	8
2.1 General Considerations.....	8
2.2 Risk Identification.....	8
2.3 Risk Analysis	8
2.3.1 Qualitative	8
2.3.2 Semi-quantitative Analysis	9
2.3.3 Quantitative Analysis.....	9
2.4 Risk Evaluation	10
2.5 Applicability of Risk Assessment Techniques	10
3 DESCRIPTION OF RISK ASSESSMENT TECHNIQUES	11
3.1 Bow-tie Analysis	11
3.2 Brainstorming.....	11
3.3 Consequence/Likelihood Matrix	11
3.4 Cost-Benefit Analysis (CBA).....	12
3.5 Event Tree Analysis.....	13
3.6 Failure Mode and Effect Analysis (FMEA) and Failure Modes, Effects and Criticality Analysis (FMECA)	13
3.6.1 Overview.....	13
3.6.2 Failure Mode and Effects Analysis (FMEA)	13
3.6.3 Failure Mode, Effects and Criticality Analysis (FMECA)	14
3.7 Fault Tree Analysis.....	14
3.8 Monte Carlo Simulation	15
4 DETERMINING CONSEQUENCE	16
4.1 Bushfire.....	17
4.2 Safety.....	17
4.3 Supply	18
4.4 Environment.....	19
4.5 Collateral Damage	19
4.6 Reactive Repair/Replacement.....	19
5 DETERMINING LIKELIHOOD	20
5.1 Overview	20
5.2 Asset Condition Scores	20
5.3 Probability of Failure – Weibull Analysis	20
5.3.1 Overview.....	20

Asset Risk Assessment Overview

5.3.2	Estimating Weibull Parameters	21
5.3.3	Small Population Assets.....	21
6	RISK BASED ASSET MANAGEMENT	23
6.1	High Volume, Low Value Assets	23
6.2	Low Volume, High Value Assets	23
APPENDIX A	BOW-TIE RISK ASSESSMENT TEMPLATE	24
APPENDIX B	DISPROPORTIONALITY FACTORS	25
B.1	Background.....	25
B.2	Disproportionality Factors used by AusNet Services	25
APPENDIX C	SAFETY EFFECTS COSTS	27
APPENDIX D	ENVIRONMENTAL EFFECTS COSTS	28
APPENDIX E	COLLATERAL DAMAGE EFFECTS COSTS	29

Asset Risk Assessment Overview

1 Introduction

1.1 Purpose

This document describes the risk assessment process used by AusNet Services to identify and assess the highest risks associated with network assets.

These risk assessments are used to inform the development of optimised inspection, maintenance and replacement programs, forecast future asset replacement capital and operational expenditure and assist in the prioritisation of work.

1.2 Scope

This document applies to assessing risks associated with all network assets within the three regulated businesses in the development of asset management strategies.

Risks associated with projects are governed by Portfolio Management and Review (PM&R) processes and are not included in the scope of this document.

1.3 Background

1.3.1 Risk Definitions

AS/NZS ISO 31000 Risk Management defines *risk* as the 'effect of uncertainty on objectives'.

ISO Guide 73:2009 Risk Management – Vocabulary defines the level of risk (3.6.1.8) as:

Magnitude of a risk or combination of risks, expressed in terms of the combination of consequences and their likelihood.

Consequence is defined as the 'outcome of an event affecting objectives', where an event is defined as an 'occurrence or change of a particular set of circumstances'.

Likelihood is defined as the 'chance of something happening'.

1.3.2 Risk Management Framework

AusNet Services maintains a risk management system that has been designed in accordance with *ISO 31000:2018 Risk Management – Guidelines* to ensure risks are effectively managed to provide greater certainty for our security holders, employees, customers, suppliers and the communities in which we operate.

The Risk Management Framework sets out the overarching philosophy, principles, requirements and responsibilities for a sound approach of risk oversight, management and ongoing internal control assurance required within AusNet Services.

The Framework addresses the following:

- Governance and responsibilities;
- Risk management principles and methodology;
- How AusNet Services assesses and manages risk; and
- How AusNet Services monitors and reports on risk.

The framework is a blue print to manage risk consistently across AusNet Services. The asset management system is the primary mechanism by which risk reduction controls are implemented.

Asset Risk Assessment Overview

Risks are rated and prioritised under the following categories:

- Health and Safety (Employee and Public);
- Environment and Community;
- Reputation;
- Customers;
- Regulation, Legal and Compliance;
- Management Impact and People; and
- Financial Impact.

By adopting common metrics across the broad range of business risks and investment portfolios, AusNet Services can more effectively manage business risks and optimise network outcomes and objectives.

AusNet Services' risks are identified, assessed and managed at all levels in the organisation through network design and operation, incident investigation, asset condition monitoring and performance analysis, workshops, meetings and one-on-one interviews.

RM 10-01-1 Risk Assessment Process and Criteria provides details on AusNet Services' risk assessment process and the criteria underpinning analysis.

1.3.3 Risk Management Process

Figure 1 provides an overview of the risk management process.

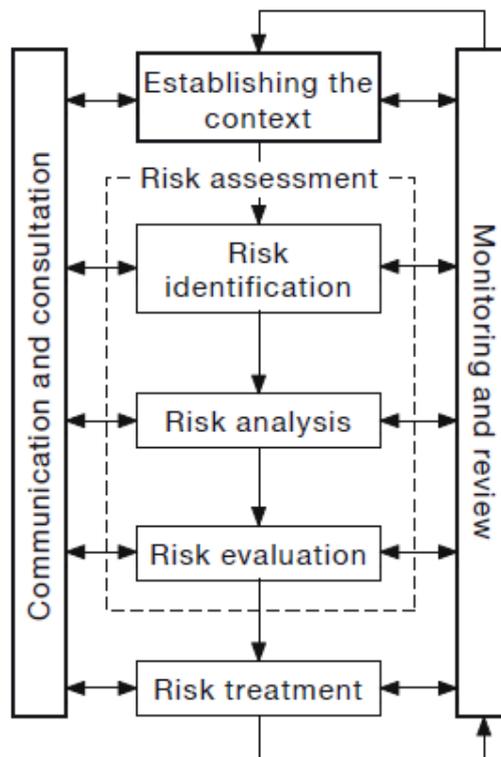


Figure 1: Risk Management Process from AZ/NZS ISO 31000

Asset Risk Assessment Overview

The three stages of the risk assessment process are shown within the dashed box, namely:

1. **Risk identification** – the process of finding, recognising and describing the risks;
2. **Risk analysis** – the process to comprehend the nature of the risk and determine the level of the risk; and
3. **Risk evaluation** – the process of comparing the results of risk analysis with risk criteria to determine whether the risk is acceptable to the organisation.

1.3.4 Risk Assessment

The purpose of risk assessment is to provide information and analysis to support decisions on how to treat particular risks and how to choose between options where there is uncertainty.

Risks are assessed at the following organisational and functional levels:

- Business Level Risks;
- Operational Level Risks; and
- Asset Related Risks.

Different tools and techniques may be appropriate for different needs and situations.

Business Level Risks

At the business (strategic) level of the organisation risks are typically identified by the executive management team, with input from senior management and endorsement by the Group Risk Committee (GRC) and the Audit and Risk Management Committee (ARMC). They are high level risks that overarch or aggregate the more detailed risks discussed below.

Operational Level Risks

At the operational level risks are typically identified by operational personnel, including managers and field personnel, depending upon the complexity and scope of the risk.

Routine risks, such as those faced by workers performing daily tasks, are assessed as part of the process of undertaking work. Other non-routine risks may be identified and addressed directly through instigation of a review using AusNet Services' Issue Management System and complex risks may be referred through the Network Safety Management Committee.

Asset Related Risks

Asset related risks are typically identified by engineers in Network Engineering, with input from field personnel. This occurs at the acquisition or design stages, through analysis of asset condition and performance data, and from incident investigations.

It is the assessment of these asset related risk which lie within the scope of this document.

Asset Risk Assessment Overview

2 Overview of Risk Assessment Techniques

2.1 General Considerations

Risk analysis is undertaken in varying degrees of detail, dependent upon the impact of the event, the purpose of the analysis and the availability and quality of asset data and information.

The following points should be particularly noted when undertaking risk assessments:

1. The risk assessment process should be systematic and structured
2. Risk assessment methods should be logically and mathematically correct
3. Risk assessments should be based on best available evidence
4. People with appropriate knowledge and competency should be involved
5. Uncertainty should be explicitly addressed
6. The form and rigour of risk assessment should be appropriate for the decision to be made
7. Human and cultural factors should be taken into account when assessing risks.

2.2 Risk Identification

The purpose of risk identification is to anticipate what might happen or what situations might exist that might affect the achievement of objectives.

Techniques used by AusNet Services for risk identification include:

- Bow-tie analysis;
- Brainstorming;
- Event tree analysis;
- Failure mode and effects analysis (FMEA) and failure mode, effects and criticality analysis (FMECA); and
- Fault tree analysis.

2.3 Risk Analysis

Risk analysis is about developing an understanding of the risk – the causes and sources of risk, their consequences and the likelihood that those consequences can occur.

Techniques used in analysing risk can be:

- Qualitative;
- Semi-quantitative; or
- Quantitative.

Risks can be assessed to different degrees of depth and detail and using one or many techniques ranging from simple to complex.

The choice of technique is highly dependent on context and the form of assessment and its output should be consistent with the risk criteria developed as part of establishing the context.

2.3.1 Qualitative

Qualitative analysis involves using qualitative and quantitative information to better understand risks.

Qualitative analysis is often used first to provide a general indication of the level of risk associated with an event or asset class and to reveal the major risk parameters.

Asset Risk Assessment Overview

Subsequently, more specific semi-quantitative or quantitative analysis is undertaken on the major risk parameters.

Results of qualitative analysis can be used to help identify risk treatment strategies or to compare options which involve several risks of different types or levels that cannot be measured on the same quantitative scale.

Qualitative techniques used by AusNet Services for risk analysis include:

- Bow-tie analysis;
- Consequence/likelihood matrices;
- Event tree analysis; and
- Fault tree analysis.

2.3.2 Semi-quantitative Analysis

The form of qualitative analysis where numerical, ordinal or interval scales are used to rate the consequence and/or likelihood is referred to as semi-quantitative analysis.

AusNet Services uses semi-quantitative risk analysis to assess overall network risk and specific high level risks, such as reliability, health and safety, environment, physical security and regulatory compliance.

In the analysis of high-level situations where there are large numbers of contributing factors and influencing control the AusNet Services Risk Management Framework is employed.

Semi-quantitative risk analysis is more objective than qualitative analysis techniques and consumes less time and resources than quantitative analysis. As far as is reasonably practicable, efforts are made to quantify individual contributing factors and influencing controls.

The objective is to produce a more expanded ranking scale than is usually achieved in qualitative analysis.

Semi-quantitative techniques used by AusNet Services for risk analysis include:

- Consequence/likelihood matrices; and
- Failure mode and effects analysis (FMEA) and failure modes, effects and criticality analysis (FMECA)

2.3.3 Quantitative Analysis

Quantitative risk analysis is the most objective risk analysis technique.

Quantitative analysis uses representative numerical values to model consequences and/or event probabilities, frequencies or distribution of values.

From this, numerical values of the probability of outcomes, the extent or level of consequence and their likelihood and/or the level of risk can be derived.

Where accurate and reliable data, covering significant periods is available, AusNet Services uses this fully quantitative approach to assess both network performance and asset failure risks.

Full quantitative analysis may not always be possible or desirable, due to insufficient information about the subject of analysis, lack of data, level of uncertainty or variability that cannot be correctly interpreted mathematically.

Asset Risk Assessment Overview

Quantitative techniques used by AusNet Services for risk analysis include:

- Cost-benefit analysis;
- Event tree analysis;
- Failure mode and effects analysis (FMEA) and failure modes, effects and criticality analysis (FMECA);
- Fault tree analysis; and
- Monte Carlo simulation.

2.4 Risk Evaluation

Risk evaluation uses the information generated by risk identification and risk analysis to make decisions about which risks need treatment and the priority for treatment implementation.

Ethical, legal, financial and other considerations, including perceptions of risk, are also inputs into the decision.

It is important to note that the risk analysis informs risk evaluation, but does not make the decisions.

2.5 Applicability of Risk Assessment Techniques

Table 1 is an extract from Table A1 *SA/SNZ HB 89:2013 Risk Management – Guidelines on risk assessment techniques*, which provides an assessment of the applicability of each technique to the specific elements of the AS/NZS ISO 31000 risk assessment process.

Table 1: Applicability of tools and techniques used for risk assessment¹

Tool/ technique	Risk Identificatio n	Control Analysis	Risk Analysis			Risk evaluation
			Consequen ce	Likelihood	Level of Risk	
Bow tie analysis	A	SA	A	A	A	A
Brainstorming	SA	A	NA	NA	NA	NA
Consequence/ likelihood matrix	SA	A	SA	SA	SA	A
Cost-benefit analysis	NA	A	A	NA	A	SA
Event tree analysis	A	SA	SA	A	A	A
FMEA/ FMECA	SA	A	SA	SA	SA	A
Fault tree analysis	A	A	NA	SA	A	A
Monte Carlo simulation	NA	A	A	SA	SA	SA

Notes:

- SA = Strongly applicable – common usage of tool
- A = Applicable – can be used in this context
- NA = Not applicable

¹ Extract from Table A1 in SA/SNZ HB 89:2013 Risk Management – Guidelines on risk assessment techniques

Asset Risk Assessment Overview

3 Description of Risk Assessment Techniques

3.1 Bow-tie Analysis

Bow-tie analysis is a simple way of describing and analysing the pathways of risk from causes to consequences. It displays an event showing a range of possible causes and consequences.

It is used when the situation does not warrant the complexity of a full fault tree or event tree analysis, or when the focus is on ensuring that there is a barrier or control in place for each failure pathway.

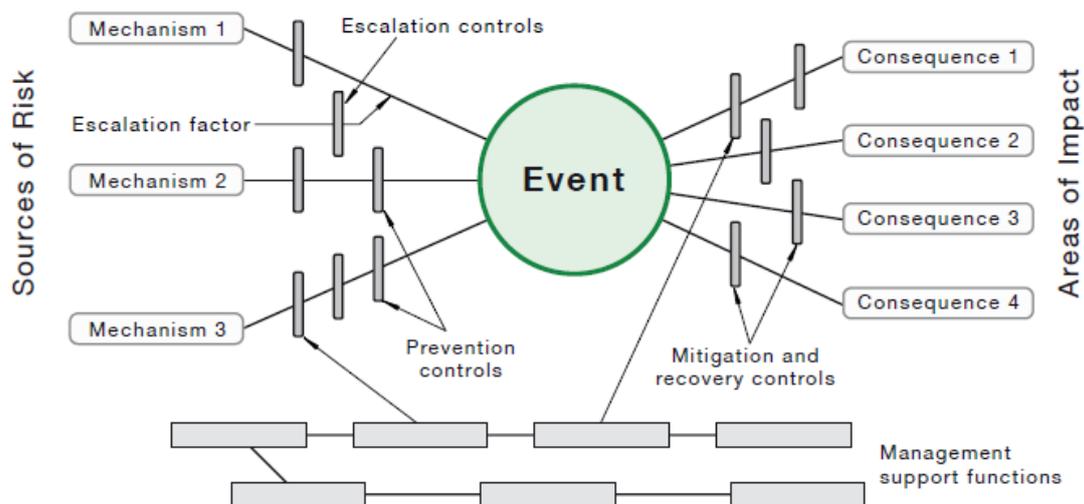


Figure 2: Example of a Bow Tie Diagram (from SA/SNZ HB 89:2013)

A template for conducting bow-tie analysis is given in Appendix A.

3.2 Brainstorming

Brainstorming involves stimulating and encouraging free-flowing conversation amongst a group of knowledgeable people to identify risk, sources of risk, potential failure modes, criteria for decisions and/or options for treatment.

Brainstorming can be used in conjunction with other risk assessment techniques or at any stage of the risk management process to encourage imaginative thinking.

3.3 Consequence/Likelihood Matrix

The consequence/likelihood matrix is a means of combining qualitative or semi-qualitative ratings of consequence and likelihood to produce a level of risk or risk rating.

It is commonly used as a screening tool when many risks have been identified to determine which need further or more detailed analysis, which risks need treatment first, or which risks need to be referred to a higher level of management.

It may be used in situations where there is insufficient data for detailed analysis, or the situation does not warrant the time and effort for a more quantitative analysis.

RM 10-01-1 Risk Assessment Process and Criteria provides guidance on AusNet Services' risk assessment process and the criteria underpinning analysis using a consequence/likelihood matrix.

Table 2 is the corporate risk level matrix, reproduced from RM 10-01. It can be seen that there is a skew so that risks with the highest levels of consequence, even if the likelihood is

Asset Risk Assessment Overview

low, are rated as extreme or very high – this is typical of organisations with a risk attitude that is strongly adverse to high consequence events.

Table 2: AusNet Services Risk Level Matrix

		Consequence				
		1	2	3	4	5
Likelihood	Almost Certain	C	C	B	A	A
	Likely	D	C	B	B	A
	Possible	E	D	C	B	A
	Unlikely	E	D	D	C	B
	Rare	E	E	D	C	C

In situations where there may be limited failure or asset data, AusNet Services has developed the risk matrix given in Table 3 to guide asset replacement decisions.

Table 3: Asset Replacement Risk Matrix

		Condition				
		C1	C2	C3	C4	C5
Criticality	>100 times replacement cost					
	<=100 times replacement cost					
	<=30 times replacement cost					
	<=10 times replacement cost					
	<=3 times replacement cost					

The condition of the assets is obtained from the asset health reports and the criticality determined based on the consequences of failure of the asset. The scaling for the criticality has been selected so that Condition C5 assets in the ‘red’ area of the matrix are economic to replace on a cost-benefit basis.

3.4 Cost-Benefit Analysis (CBA)

Cost-benefit analysis (CBA) can be used during risk evaluation where total expected costs are weighed against the total expected benefits in order to choose the best option.

Quantitative CBA aggregates the monetary value of all costs and all benefits to all stakeholders that are included in the scope and it adjusts for different time periods in which the costs and benefits accrue.

The net present value (NPV) which is produced becomes an input into decisions about risk.

Further details of AusNet Services’ economic assessment process can be found in *AMS 10-24 Asset Renewal Planning Guideline* and *AMS 20-16 Distribution Network Planning Standards and Guidelines*.

Asset Risk Assessment Overview

3.5 Event Tree Analysis

Event tree analysis is produced to model the possible outcomes that could occur from a given initiation event and the status of mitigating factors. It can be applied both qualitatively and quantitatively.

Event tree analysis can be used for modelling, calculating and ranking different accident scenarios following the initiating event.

An example event tree is given in Figure 3.

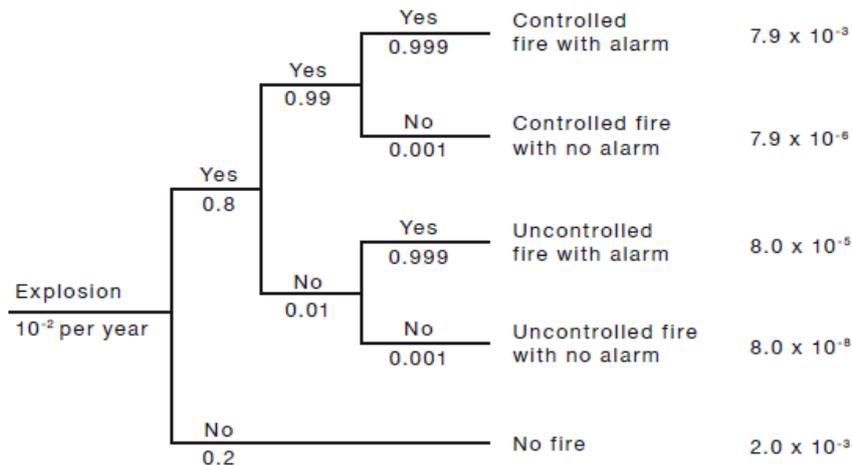


Figure 3: Example of an Event Tree (from SA/SNZ HB 89:2013)

3.6 Failure Mode and Effect Analysis (FMEA) and Failure Modes, Effects and Criticality Analysis (FMECA)

3.6.1 Overview

Failure Mode and Effects Analysis (FMEA) is a technique used to identify the ways in which components, systems, processes or procedures can fail to fulfil their objectives.

FMEA identifies the following:

- All potential failure modes of the various parts of a system
- The effects these failures may have on the system
- The mechanisms of failure
- How to avoid the failures and/or mitigate the effects of the failures on the system.

Failure Mode, Effects and Criticality Analysis (FMECA) extends FMEA so that each fault mode identified is ranked according to its importance, or criticality.

FMEA and FMECA need information about the elements of the system in sufficient detail for meaningful analysis of the ways in which each element can fail.

3.6.2 Failure Mode and Effects Analysis (FMEA)

A Failure Mode and Effects Analysis (FMEA) is often the first step of a system reliability study. It involves reviewing as many components, assemblies, and subsystems as possible to identify failure modes, and their causes and effects. For each component, the failure modes and their resulting effects on the rest of the system are recorded in a specific FMEA worksheet.

It is a systematic method to identify primary and secondary functions of the system and the failure modes that prevent the system from performing its designed purpose.

Asset Risk Assessment Overview

A FMEA can be a qualitative analysis, but may be put on a quantitative basis when mathematical failure rate models are combined with a statistical failure mode ratio database.

The steps to developing a FMEA are:

1. Define the scope and objective of the study
2. Assemble the team
3. Understand the system to be analysed
4. Break down the system into components
5. Define the function of each component

For each component:

1. How can each part fail?
2. What mechanisms might produce these modes of failure?
3. What are the effects if the failure did occur?
4. Is the failure in the safe or unsafe direction?
5. What inherent provisions are provided in the design to compensate for the failure?
6. How is the failure detected?

In FMECA, the study team goes on to classify each of the identified failure modes according to its criticality.

3.6.3 Failure Mode, Effects and Criticality Analysis (FMECA)

Failure Mode, Effects and Criticality Analysis (FMECA) is an extension of FMEA, which aims to rank each potential failure mode according to the combined influence of its severity classification of the consequences and probability of failure based on the best available data.

It is a bottom up analytical method which is used to chart the probability of failure modes against the severity of their consequences.

The result highlights failure modes with relatively high probability and severity of consequences, allowing remedial efforts to be directed where it will produce the greatest value.

3.7 Fault Tree Analysis

Fault tree analysis is a technique for identifying and analysing factors that can contribute to a specified undesired event (called the 'top event').

Causal factors are deductively identified, organised in a logical manner and represented pictorially in a tree diagram.

A fault tree may be used to identify potential causes and pathways to failure and to calculate the probability of the top event given knowledge of the probabilities of causal events.

An example fault tree is given in Figure 4.

Asset Risk Assessment Overview

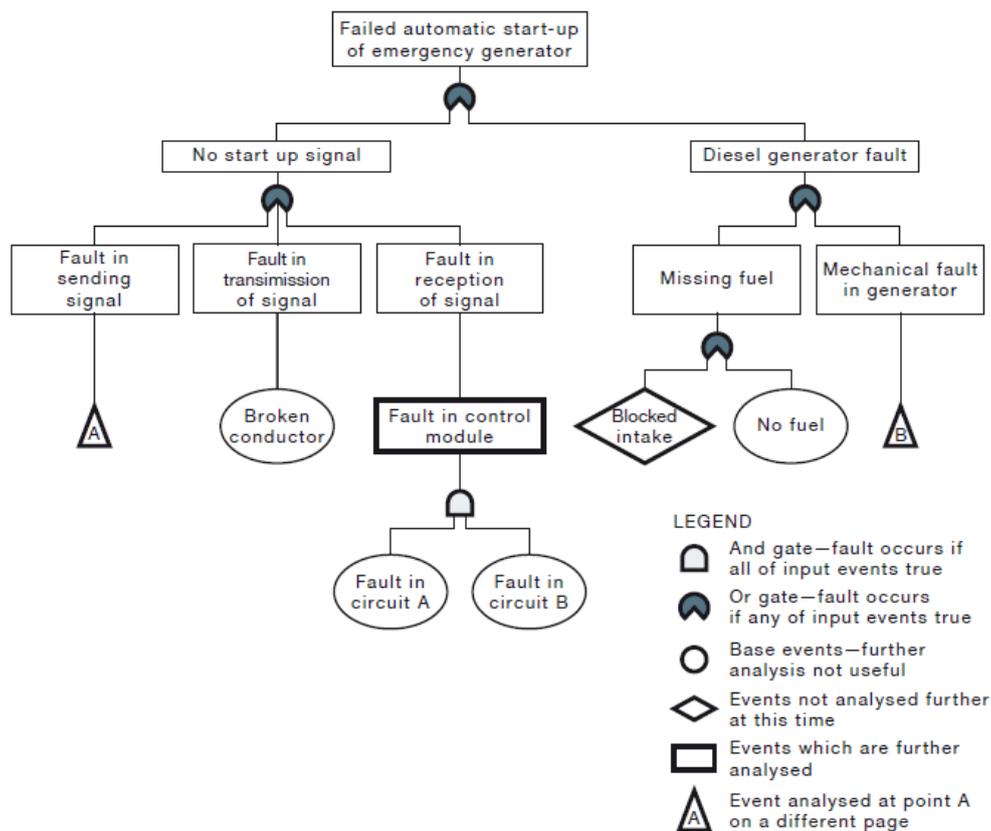


Figure 4: Example of Fault Tree (from SA/SNZ HB 89:2013)

3.8 Monte Carlo Simulation

Many systems are too complex for the effects of uncertainty on them to be modelling using analytical techniques, however they can be evaluated by considering the inputs as random variables and running a number (N) of calculations (called simulations) by sampling the input in order to obtain N possible outcomes of the result.

Monte Carlo simulation is a technique that provides probabilistic solutions to problems expressed mathematically. Using random numbers and trial and error, it repeatedly calculates the equations to arrive at a solution. The result may be given as a probability distribution or some statistic value, such as the mean.

AusNet Services uses Isograph's Availability Workbench (AWB) to perform Monte Carlo simulations to assess the risk associated with asset replacement and maintenance programs.

Further details on assessing the risks associated with asset replacement and maintenance programs can be found in *AMS 01-07 Reliability Centred Maintenance Application Guide*.

Asset Risk Assessment Overview

4 Determining Consequence

AS/NZS ISO 31000 Risk Management defines the level of risk the magnitude of a risk, or combination of risks, expressed in terms of the combination of consequences and their likelihood.

When looking at asset failure risk, there is a possibility that a given consequence, or failure effect, may occur but it is not always certain that it will occur. The probability an asset failure will result in a given consequence is known as ‘likelihood of consequence’.

Figure 5 shows the relationship between the level of risk, the probability of asset failure, the probability the asset failure results in a given consequence and the consequence.

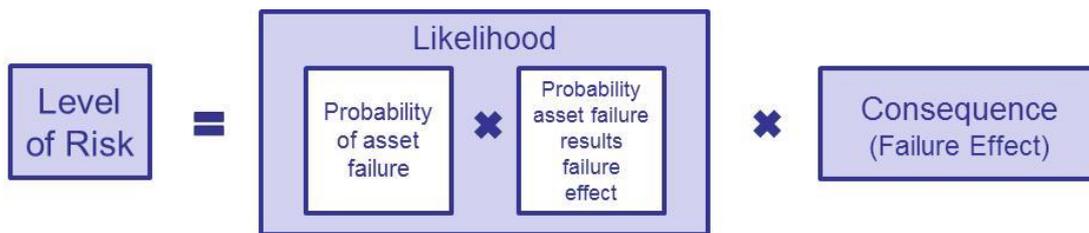


Figure 5: Relationship between level of risk, likelihood and consequence

Figure 6 illustrates the factors contributing to the likelihood of consequence for a fatality resulting from an explosive asset failure.

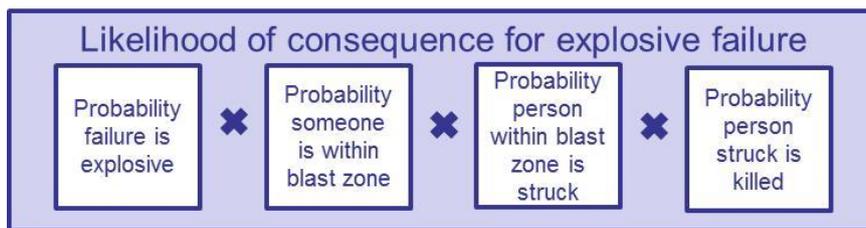


Figure 6: Likelihood of consequence for explosive failure

Rearranging the equation given in Figure 5, the failure effect cost is calculated by multiplying the probability a failure will result in a given failure effect by the estimated cost of that consequence (Figure 7).

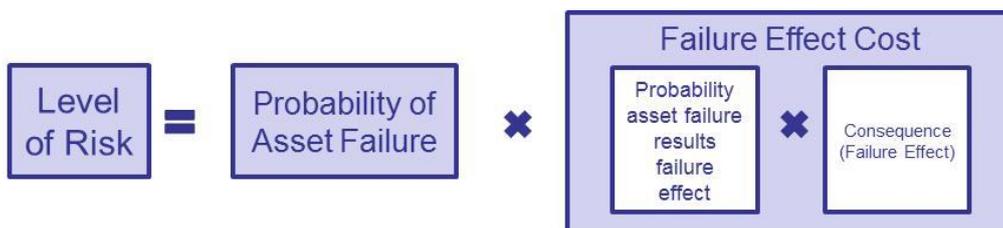


Figure 7: Relationship between probability of asset failure and failure effect cost

The consequences of failure considered in asset risk analysis include:

- Bushfire
- Safety
- Supply
- Environment
- Collateral Damage
- Reactive repair/replacement

Asset Risk Assessment Overview

These broadly align with the asset management objectives to ensure that the assets are supporting the organisation in achieving its goals.

The notable exception is the objective of complying with legal and contractual obligations. Compliance with legal and contractual obligations is seen as mandatory, and not subject to a risk analysis, aligning with our corporate value 'We do what's right'.

4.1 Bushfire

The failure effect cost for bushfire is the product of:

- Probability of fire ignition
- Probability of unfavourable weather conditions
- Expected house loss
- Bushfire loss value

This data is sourced from the Victorian Bushfire Royal Commission (VBRC) Final Report, government departments, Bureau of Meteorology and CSIRO.

The bushfire loss value is comprised of all the costs identified in the VBRC Final Report, scaled by the number of properties lost. The cost of fatalities is included, but is separated out to allow for the inclusion of disproportionality factors, as per the approach to calculating the failure effect cost for safety (Section 4.2).

The ENA is undertaking further work to establish the costs associated with bushfire ignition from electricity assets, and this work may be adopted by AusNet Services in the future.

AMS Continual Improvement Report – A methodology for quantifying bushfire risk costs provides details on how the bushfire failure effect costs are calculated.

4.2 Safety

The failure effect cost for safety is the product of:

- Likelihood of consequence
- Value of statistical life
- Value of Lost Time Injury
- Disproportionality factor

The likelihood of consequence is sourced from the *DNO Common Network Asset Indices Methodology* (Table 215).

The value of statistical life is sourced from the *Australia Government Best Practice Regulation Guidance Note Value of statistical life*, escalated to current year dollars.

The value of a lost time injury is source from Safe Work Australia's *The Cost of Work-related Injury and Illness for Australian Employers, Workers and the Community (2012-13)* (November 2015), Table 2.3b Electricity, Gas, Water and Waste Services.

The disproportionality factors provide guidance on the reasonableness of costs associated with safety risk mitigation measures to meet the requirements of the *Electricity Safety Act 1998*. They are a measure of society's expectation of how much should be spent to prevent a fatality. Higher values of disproportionality are justified when the consequences or likelihood are higher. They may also be higher when there is a low level of trust that a risk is being adequately managed.

Refer to Appendix B for further information on disproportionality factors.

Refer to Appendix C for safety effects costs calculations.

Asset Risk Assessment Overview

4.3 Supply

The failure effect cost for supply risk is the product of:

- Value of customer reliability (VCR)
- Expected Unserved Energy (EUE)

The value of customer reliability (VCR) is set by the Australian Energy Market Operator (AEMO) and provides a measure, in dollars per kilowatt-hour, of the value different types of customers place on having a reliable electricity supply.

The values currently used were set by AEMO in 2014 and are indexed to CPI.

In response to a Rule Change proposal from the Council of Australian Governments (COAG), the AEMC amended the NER to give the AER responsibility of determining the values different customers place on having a reliable supply. This rule change became effective on 5 July 2018.

The AER is currently conducting a review into VCR. The AER must publish their first VCR by 31 December 2019.

The VCR values for each class of customer are combined with the customer mix at each connection point, which is periodically reviewed and adjusted, to provide an economic value for electricity network investment evaluation at each connection point.

The Value of Unserved Energy failure effect is calculated by multiplying the expected unserved energy (kWh) by the value of VCR (\$/kWh) specified for the relevant transmission network connection point or, where relevant, zone substation.

Probabilistic planning requires the estimation of expected unserved energy for a given demand projection. Demand forecasts are produced each year for the next 10 years at AusNet Services transmission connection points, zone substations and distribution feeders for both summer and winter periods.

The demand forecasts are produced for the 'medium' economic growth scenario and include both 50% probability of exceedance (POE) of the maximum demand and 10% POE of the maximum demand.

The EUE calculation for sub-transmission network planning, including zone substation augmentations is as follows:

$$EUE = [w_{10} \times EAR_{D10} + w_{50} \times EAR_{D50}] \times Pr(f) \times MTTR$$

Where:

EAR_{D10} = Energy At Risk using 10%POE demand forecast

EAR_{D50} = Energy At Risk using 50%POE demand forecast

w_{10} = 0.30 (Weighting applied to 10%POE)

w_{50} = 0.70 (Weighting applied to 50%POE)

$Pr(f)$ = Probability of Failure

$MTTR$ = Mean Time To Repair (ie the mean time to restore supply)

In addition to the energy at risk in the event of an asset failure, the supply risk also includes a component for the energy at risk for any forecast load above the rating of the site when in a system normal configuration.

Asset Risk Assessment Overview

4.4 Environment

The failure effect cost for environment is the product of:

- Probability of an uncontrolled release of oil, gas or smoke
- Expected environmental cost of a single release event

Refer to Appendix D for environmental effects costs calculations for station assets.

The expected environmental cost for lines assets is assumed to be negligible.

4.5 Collateral Damage

The failure effect cost for collateral damage is the product of:

- Probability of failure being explosive
- Probability of equipment being damaged if failure is explosive (damage factor)
- Expected collateral damage cost

Refer to Appendix E for collateral damage effects costs calculations for station assets.

The expected collateral damage cost for lines assets is assumed to be negligible.

4.6 Reactive Repair/Replacement

The failure effect cost for reactive repair/replacement is the cost of replacing the asset. It is assumed that all failures result in the requirement to replace the asset.

The unit rates developed for project and business case estimation are used for the reactive replacement costs.

Asset Risk Assessment Overview

5 Determining Likelihood

5.1 Overview

As the condition of an asset deteriorates the risk of asset failure increases. Often this deterioration is linked to the age of the asset (i.e. the asset deteriorates over time), but asset condition is also influenced by other factors such as the loading on the asset, the environment it is installed in and frequency of operation.

In the absence of any meaningful condition information, asset age can be used as a proxy for condition.

5.2 Asset Condition Scores

AusNet Services uses condition monitoring to gather data for assets using a variety of techniques to create several measures of condition, known as 'asset health indices'.

These asset health indices are combined into a single 'condition score' on a scale of 1 to 5. The condition score range is consistent across asset types and relates to the expected remaining asset life.

Table 4 provides an overview of the asset condition scores.

Table 4: Condition Score Definition

Condition Score	Rating Scale	Condition
C1	Very Good	The asset is in very good condition with no past history of significant defects or failures.
C2	Good	Deterioration has minimal impact on asset performance. Minimal short term asset failure risk.
C3	Average	Functionally sound showing some wear with minor failures, but asset still functions safely at adequate level of service.
C4	Poor	Advanced deterioration – plant and components function but require a high level of maintenance to remain operational.
C5	Very Poor	The asset is in very poor condition, is maintenance intensive and is approaching end of life.

Where there is sufficient asset failure history, this can be combined with the condition data, to determine a probability of asset failure.

5.3 Probability of Failure – Weibull Analysis

5.3.1 Overview

The Weibull distribution can be used to model failure data regardless of whether the failure rate is increasing, decreasing or constant. It is flexible and adaptable to a wide range of data and a life distribution can be modelled even if not all of the items have failed.

The two-parameter Weibull distribution is the most widely used distribution for life data analysis.

The instantaneous failure rate, $\lambda(t)$, (sometimes referred to as hazard rate, $h(t)$) of the two parameter Weibull distribution is given in Equation 1.

Asset Risk Assessment Overview

$$\lambda(t) = \beta \cdot \frac{t^{\beta-1}}{\eta^{\beta}}$$

Equation 1: Two parameter Weibull Instantaneous Failure Rate²

Where:

t = time

η (eta) = characteristic life or scale parameter

β (beta) = shape parameter

The shape parameter indicates the rate of change of the instantaneous failure rate with time.

Three ranges of the shape parameter are salient:

- For $\beta = 1.0$, the Weibull distribution is identical to the exponential distribution and the instantaneous failure rate, then becomes a constant equal to the reciprocal of the scale parameter, η .
- For $\beta > 1.0$, the instantaneous failure rate is increasing; and
- For $\beta < 1.0$, the instantaneous failure rate is decreasing.

A shape parameter of $\beta=3.44$ is a fair approximation of a normal distribution.

The characteristic life, η , is the time at which 63.2% of the items are expected to have failed. This is true for all Weibull distributions, regardless of the shape parameter.

5.3.2 Estimating Weibull Parameters

Isograph's Availability Workbench software has a Weibull module which can be used to estimate Weibull parameters based on asset failure data.

Failure data consists of historical failures (ZK notifications in SAP and OMU work orders in SAP or Power On Fusion) that have been coded to their corresponding failure mode.

To model a particular failure mode, in addition to the details of actual failures, the following data needs to be included in the data set as 'suspended' failures to accurately predict the natural failure rate of the asset:

- Asset failures where the failure mode was different to the failure mode being modelled;
- Defects detected during asset inspections (ZA notifications in SAP) and rectified prior to failure; and
- All in-service assets.

The correlation co-efficient, ρ (rho), is a measure of how well the estimated parameters fit the data. The closer to 1, the better the data fit. A value of ρ of less than 0.9 is a sign of poor correlation and the data should be reviewed for competing failure modes.

Use of failure data relies on having statistically significant volumes of failures. This means that it is better suited to high population assets such as poles.

It is not as suitable for small population assets such as power transformers, where failure data may be scarce. Parameter estimation for these types of assets is Section 5.3.3.

5.3.3 Small Population Assets

Small population assets rely on asset condition, where failure probability is derived from a condition assessment.

² International Electro Technical Commission standard IEC 61649 (2008)

Asset Risk Assessment Overview

The condition of each asset is assessed on a five-point scale (C1, C2, C3, C4 and C5) to objectively establish its current position within the life cycle and hence the remaining service potential and associated probability of failure.

Table 5: Relationship between Condition Score and Remaining Service Potential

Condition Score	Remaining Service Potential (RSP%) ³
C1	95
C2	70
C3	45
C4	25
C5	15

A relationship is created between condition, remaining service potential (RSP%) and the failure rate, $\lambda(t)$, of the asset depending on its position within the asset life cycle and its characteristic life.

A β beta value of 3.5 is used as a default, unless additional modelling has been carried out for a specific asset class. This β beta value is consistent with a long life asset with wear out pattern represented by a normally distributed probability density function.

The characteristic life, η , is estimated by calibrating the estimated number of failures for the current in service population against actual failures (corrective maintenance) and pre-emptive replacements (preventative replacements) observed in recent history.

The calibration method is illustrated in Table 6.

Table 6: Circuit Breakers: Relationship between Condition, RSP% and Failure Rate (r(t))

CLASSIFICATION (All)												Condition 1 Age	2.25
												Condition 1 Hours	19710
												AGE	45
												Weibull	0
Row Labels	Count of ASSET	Cause	Condition	RSP%	Remaining Life	Age	Useful Life	BETA	PBF	Failures	2014		
C1	471	Circuit Breaker Failure	1	95	42.75	2.25	45	3.5	0.004%	0.02	0.00%		
C2	141	Circuit Breaker Failure	2	70	31.5	13.5	45	3.5	0.38%	0.54	0.38%		
C3	59	Circuit Breaker Failure	3	45	20.25	24.75	45	3.5	1.74%	1.03	1.74%		
C4	154	Circuit Breaker Failure	4	25	11.25	33.75	45	3.5	3.79%	5.83	3.79%		
C5	178	Circuit Breaker Failure	5	15	6.75	38.25	45	3.5	5.18%	9.22	5.18%		
Grand Total	1003												
											Estimated failures per year:	16.65	16.65
											Percentage of Fleet:	1.66%	1.66%
											Sanity Check (Asset Fleet/Usful Life):	22.29	

In Table 6, the number of assets in each phase of the life cycle is multiplied by the probability of failure associated with that phase of the life cycle. The resulting sum of estimated failures per year (in this case, 16.65 replacements per annum) predicted by the model is then compared to historical corrective and preventative replacements rates.

³ AMS Continual Improvement Report: Risk Analysis for Terminal Station Assets (2017)

Asset Risk Assessment Overview

6 Risk Based Asset Management

Broadly speaking, AusNet Services' assets can be divided into:

- High volume, low value assets in public places
- Low volume, high value assets in secure fenced areas, such as terminal and zone substations

6.1 High Volume, Low Value Assets

The low replacement cost for high volume, low value assets in public places means maintenance, repair or replacement are rarely an economic option for managing this type of asset.

Typically, high volume, low value assets in public places are managed using inspection programs to trigger condition-based replacements.

Public safety, bushfire and supply interruption risks are used to inform the business rules governing asset inspection intervals and replacement criteria of these inspection programs.

FMEA/FMECA techniques are useful for understanding asset functions and failure modes.

Monte Carlo simulation techniques using purpose built software, such as Availability Work Bench, are valuable in optimising inspection intervals based on risk.

Further information can be found in *AMS 01-07 Reliability Centred Maintenance Application Guide*.

6.2 Low Volume, High Value Assets

The replacement cost for low volume, high value assets means that maintenance, repair and refurbishment become viable economic options in the management of this type of asset.

Historically, inspection and maintenance intervals for low volume, high value assets have been based on a combination of manufacturer recommendations, industry experience and failure rates.

FMEA/FMECA and Monte Carlo simulation techniques are increasingly being used to further optimise the maintenance of these assets.

The fundamental principle underpinning the management of low volume, high value assets is the stabilisation of risk.

Fleet risk models are used to quantify the risks associated with these assets.

These risk models consider the risks associated with safety, environmental damage, collateral damage, supply and reactive asset replacement combined with probabilities of failure based on asset condition.

Depending on the assets and the information available on them, these risk models may include:

- Consequence/likelihood matrix
- Cost-benefit analysis
- Monte Carlo simulation

The decision to replace an asset is made when the risk benefit gained by replacing the asset is greater than the cost of replacement.

Asset Risk Assessment Overview

Appendix B Disproportionality Factors

B.1 Background

Safety legislation requires investment 'as far as practicable' – that is, invest until the costs are disproportionate to the benefits.

Disproportionality factors (DF) are used to provide guidance on a cut off of when to stop spending money to reduce safety risk; when the cost is disproportionate to the risk reduction.

According to the UK's Health and Safety Executive (HSE), DFs that may be considered gross vary from upwards of 1 depending on a number of factors including the magnitude of the consequences and the frequency of realising those consequences, i.e. the greater the risk, the greater the DF. A DF of greater than 10 is unlikely.

HSE submission to the 1987 Sizewell B Inquiry⁴ suggesting that a factor of up to 3 (i.e. costs three times larger than benefits) would apply for risks to workers; for low risks to members of the public a factor of 2, for high risks a factor of 10.

HSE has not formulated an algorithm which can be used to determine when the degree of disproportion can be judged as 'gross'; the judgement must be made on a case by case basis.

It is generally understood that the greater the risk, the more that should be spent in reducing it, and the greater the bias on the side of safety.

Additionally, the choice of DF may be higher when there is a low level of trust between the duty-holder and the community they operate in. In these circumstances, when trust levels are low, there may be an expectation to spend more to reduce risks.

B.2 Disproportionality Factors used by AusNet Services

The DFs given in Table 7 are to be applied to fatalities caused by electrical infrastructure, excluding fatalities caused by a bushfire started by electrical infrastructure. These values have been selected following a review of values used across the electricity industry within Australia and by other industries across Australia and internationally.

Table 7: Disproportionality Factors – Fatality caused by Electrical Infrastructure (excluding bushfire start)

Scenario	Disproportionality Factor
Public Trespass	1
Single Fatality (public or worker)	3
Multiple Fatality (public or worker)	6

Table 8 gives the disproportionality factors to be used when assessing the risk of a fatality cause by a bushfire started by electrical infrastructure.

⁴ The Sizewell B Inquiry was public inquiry conducted between January 1983 and March 1985 into a proposal to construct a nuclear power station in the UK.

Asset Risk Assessment Overview

Table 8: Disproportionality Factors – Fatalities due to bushfires started by electricity assets

Scenario	Disproportionality Factor
Asset in LBRA	1
Asset in HBRA	3
Asset in REFCL Area	6
Asset in Codified Area ⁵	10

The disproportionality factors for fatalities due to bushfires started by electrical infrastructure have been selected considering the weighting scale for the geographic dimension of the Ignition Risk Unit (IRU) calculation (Table 9) as a guide of the community’s expectation around preventing bushfires and the resulting fatalities.

Table 9: IRU Geographic Multiplier

Category	Description	Weight
Low	LBRA	0.2
High	HBRA	1.0
Severe	Areas covered by REFCL	4.6
Extreme	Codified	19.8

Figure 8 shows the location of each of these IRU geographic categories within Victoria.

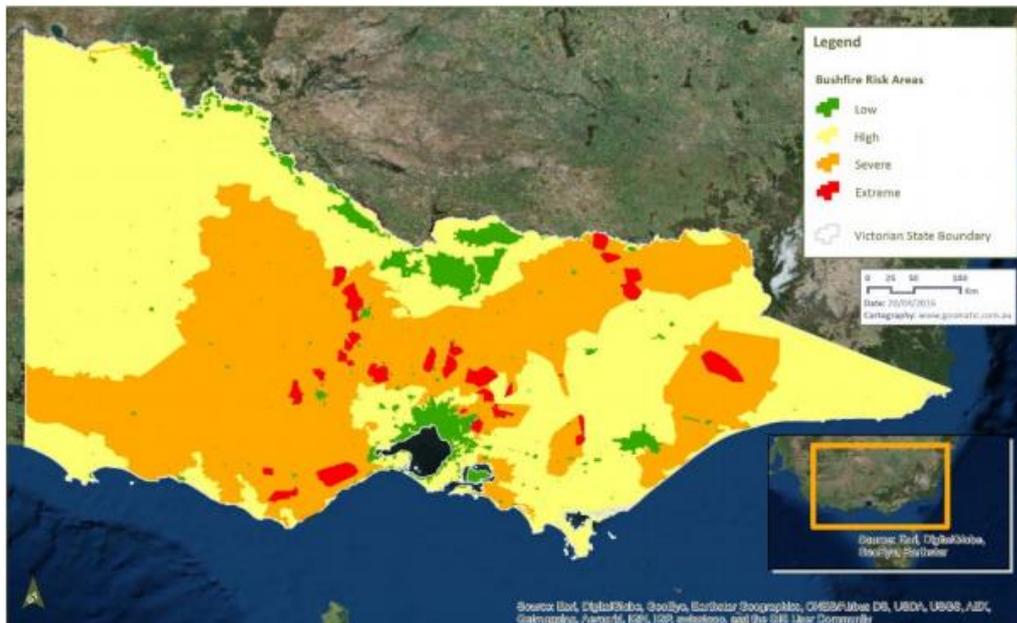


Figure 8: IRU Geographical Multiplier Category Locations

Note that there will be situations where engineering knowledge/judgement will determine that different values of DF should be used, such as for LBRA at a boundary location with HBRA.

⁵ Areas defined as ‘electric line construction areas’ by the Electricity Safety (Bushfire Mitigation) Regulations 2013

Asset Risk Assessment Overview

Appendix C Safety Effects Costs

Table 10 gives safety effect costs in 2014 dollars assuming:

- The reference safety probabilities given in the *DNO Common Network Asset Indices Methodology*
- The value of statistical life of [C.I.C] in 2014 dollars, as per the *Best Practice Regulation Guidance Note Value of Statistical Life*
- The value of lost time accident of [C.I.C] per event for Electricity, Gas, Water and Waste Services, as per Safe Work Australia's *The Cost of Work-related Injury and Illness for Australian Employers, Workers and the Community (2012-13)*, Table 2.3b
- A disproportionality factor of 3, for a single fatality of either a member of the public or a worker

Table 10: Safety Effects Cost

Asset Type	Lost Time Accident ⁶	Death or Serious Injury to Public ⁶	Death or Serious Injury to Staff ⁶	Safety Effects Cost (in 2014 dollars)
Pole	0.000272	0.00001088	0.00000544	C.I.C
Tower	0.000136	0.00000544	0.0000272	
Conductor	0.000544	0.00002176	0.0001088	
Circuit Breaker (<132kV)	0.0002603	0.000115	0.001960616	
Circuit Breaker (≥132kV)	0.0004164	0.0000575	0.003136986	
Transformer (<132kV)	0.0002603	0.00023	0.001960616	
Transformer (≥132kV)	0.0004164	0.0000575	0.003136986	

⁶ From Table 215 of *DNO Common Network Indices Methodology*, Health and Criticality Version 1.1, 30 January 2017

Asset Risk Assessment Overview

Appendix D Environmental Effects Costs

For oil-filled assets, the following average environmental clean-up costs per event are assumed:

- PCB-free oil: [C.I.C]
- PCB contaminated oil: [C.I.C]

It is assumed that all explosive failures of oil-filled assets result in an environmental incident.

Probabilities of explosive failure for various assets are given in Table 10 in Appendix E.

Thus, the environmental effects cost is calculated as the probability of explosive failure multiplied by the average clean-up cost.

For example, the probability of explosive failure for a $\geq 220\text{kV}$ bulk oil circuit breaker is 0.05. If the circuit breaker is PCB-free the environmental effect cost is [C.I.C]. If the circuit breaker contains PCB-contaminated oil, the environmental effect cost is [C.I.C].

For capacitor banks, the environmental effects costs are calculated based on the following assumptions:

- 5% of cans leak on capacitor bank failure
- Cost per can to clean up is [C.I.C]
- Number of cans ranges from 24 to 540 (average 156)

For example, a 24-can capacitor bank would have an environmental effect cost of

$0.05 \times 24 \times [\text{C.I.C}]$.

Asset Risk Assessment Overview

Appendix E Collateral Damage Effects Costs

Table 11 to Table 14 gives collateral damage effect costs for various types of equipment assuming a collateral damage cost of [C.I.C] per damage event, including consequential supply outages.

The 'damage factor' is a site specific factor between 0 and 1 that reflects the likelihood that adjacent plant by be damaged depending on the site layout and proximity to other equipment. This is assumed to be 0.5 unless more specific information is available.

Table 11: Current Transformer Collateral Damage Cost

Current Transformer Type	Voltage (kV)	Probability of Explosive Failure	Damage Factor	Collateral Damage Cost
Live Tank – Oil-filled – Porcelain	≥220	0.10	0.5	C.I.C
	≥66 to <220	0.05	0.5	
	≥22 to <66kV	0.01	0.5	
Dead Tank – Oil-filled – Porcelain	≥220	0.05	0.5	
	≥66 to <220	0.05	0.5	
	≥22 to <66kV	0.01	0.5	
Oil-filled – Polymer	≥220	0.01	0.5	
	≥66 to <220	0.01	0.5	
	≥22 to <66kV	-	0.5	
SF6	≥220	0.01	0.5	
	≥66 to <220	-	0.5	
	≥22 to <66kV	-	0.5	

Table 12: Voltage Transformer Collateral Damage Cost

Voltage Transformer Type	Voltage (kV)	Probability of Explosive Failure	Damage Factor	Collateral Damage Cost
CVT Porcelain	≥220	0.10	0.5	C.I.C
	≥66 to <220	0.05	0.5	
	≥22 to <66kV	-	0.5	
CVT Polymer	≥220	0.01	0.5	
	≥66 to <220	0.01	0.5	
	≥22 to <66kV	-	0.5	
MVT	≥220	-	0.5	
	≥66 to <220	0.02	0.5	
	≥22 to <66kV	0.01	0.5	

Asset Risk Assessment Overview

Table 13: Circuit Breaker Collateral Damage Cost

Circuit Breaker Type	Voltage (kV)	Probability of Explosive Failure	Damage Factor	Collateral Damage Cost
Bulk Oil	≥220	0.05	0.5	C.I.C
	≥66 to <220	0.02	0.5	
	≥22 to <66kV	0.01	0.5	
Minimum Oil	≥220	0.02	0.5	
	≥66 to <220	0.01	0.5	
	≥22 to <66kV	-	0.5	
SF6 – Live Tank	≥220	0.01	0.5	
	≥66 to <220	-	0.5	
	≥22 to <66kV	-	0.5	
SF6 – Dead Tank	≥220	-	0.5	
	≥66 to <220	-	0.5	
	≥22 to <66kV	-	0.5	

Table 14: Surge Arrester Collateral Damage Cost⁷

Surge Arrester Type	Voltage (kV)	Probability of Explosive Failure	Damage Factor	Collateral Damage Cost
Porcelain ≥30years	≥220	0.05	1	C.I.C
	≥66 to <220	0.05	0.4	
	≥22 to <66kV	0.05	0.3	
Porcelain <30 years	≥220	0.01	1	
	≥66 to <220	0.01	0.4	
	≥22 to <66kV	0.01	0.3	
Polymer	≥220	0.002	1	
	≥66 to <220	0.002	0.4	
	≥22 to <66kV	0.002	0.3	

⁷ Email from SME (N Boteju) 15/04/2016