Eskom	Guideline	Technology

Title: **Safety Engineering Analysis Guideline**

Unique Identifier:	**240-49230100**
Alternative Reference Number:	**N/A**
Area of Applicability:	**Engineering**
Documentation Type:	**Guideline**
Revision:	**1**
Total Pages:	**14**
Next Review Date:	**April 2015**
Disclosure Classification:	**CONTROLLED DISCLOSURE**

APPROVED FOR AUTHORISATION
☑ TECHNOLOGY ENGINEERING
DOCUMENT CENTRE ☎ X4962

Process Owner	Approved by	Authorised by
E Pininski	L Fernandez	D Odendaal
Chief Engineer: Systems Design (Reliability Engineering) (B2B Perform Design Analysis Process Owner)	Senior Manager: Systems Integration (B2B Engineering Processes/System Lead	General Manager: Plant Engineering (B2B Engineering Tools Programme Lead)
Date: 27/11/2012	Date: 28/2/2013	Date: 4/3/2013

Governance

D Odendaal
TDAC Chairperson

Date: 4/3/2013

CONTENTS

FIGURES

1. INTRODUCTION

Safety Engineering refers to the Engineering discipline that addresses safety of a product or system during its total life-cycle. Safety Engineering analysis, therefore, refers to the different analyses available to specify, design-for and evaluate safety of a product or system. Primarily, it is applicable during system design but can also be used during operations and maintenance.

2. SUPPORTING CLAUSES

2.1 SCOPE

This guideline contains concise descriptions concerning a number of Safety Engineering analyses. Detailed guidelines for some of these analyses have already been developed, e.g. Fault Tree Analysis. However, it is recommended that formal Eskom guidelines for the other analyses (e.g. Fire Hazard Analysis) be developed in future.

2.1.1 Purpose

The purpose of this document is to provide an overview of the different safety analyses which may be used during the different life-cycle stages of Eskom assets.

2.1.2 Applicability

This document shall apply throughout Eskom Holdings Limited Divisions. The intended users of this guideline include both Eskom technical personnel and sub-contractors. It is applicable, primarily, during system design but can also be used during operations and maintenance (e.g. analysis of upgrades or modifications).

2.2 NORMATIVE/INFORMATIVE REFERENCES

2.2.1 Normative

[1] ISO 9001, *Quality Management Systems*.

2.2.2 Informative

[2] C.A. Ericson, *Hazard Study Techniques for System Safety*, John Wiley, 2005

[3] IEC 60300-3-1, *Dependability management – Part 3-1: Application guide – Analysis techniques for dependability – Guide on methodology*

2.3 DEFINITIONS

NONE

2.3.1 Disclosure Classification

Controlled Disclosure: Controlled Disclosure to external parties (either enforced by law, or discretionary).

2.4 ABBREVIATIONS

Abbreviation	Description
CCFA	Common Cause Failure Analysis
FMEA	Failure Mode and Effects Analysis
FMECA	Failure Mode, Effects and Criticality Analysis
FRACAS	Failure Reporting and Corrective Action System
FTA	Fault Tree Analysis
RAM	Reliability, Availability and Maintainability
RCFA	Root Cause Failure Analysis
SIL	Safety Integrity Level

2.5 ROLES AND RESPONSIBILITIES

Not Applicable.

2.6 PROCESS FOR MONITORING

Not Applicable.

2.7 RELATED/SUPPORTING DOCUMENTS

Not Applicable.

3. INTRODUCTION

Safety Engineering refers to the specialised Engineering discipline which addresses safety of a product or system during its total life-cycle. It includes aspects related to the design, production (i.e. manufacturing and/or construction), operation (including maintenance) and disposal of the product or system. Safety should always be addressed from a systems viewpoint. Inadequate safety measures may have unacceptable implications for the equipment, people and/or environment. “People” denotes both the general public and personnel, such as operators and maintainers.

Safety Engineering is closely related to Reliability Engineering, which has the prevention (or reduction of the likelihood) of failure as the primary objective. A major difference between the two disciplines is that Reliability Engineering is generally concerned with the prevention of failures from a reliability and availability viewpoint, while Safety Engineering is always concerned with the prevention of harmful incidents and accidents.

This difference in viewpoint is important to understand, since some analyses (e.g. Failure Mode and Effects Analysis and Fault Tree Analysis) can be applied successfully for both Reliability Engineering and Safety Engineering objectives. Also, in theory, a product or system should never be analysed simultaneously for reliability and safety. In many cases, a trade-off is required when both reliability and safety is required.

3.1 SAFETY CONCEPTS

3.1.1 Risk management

Safety Engineering, which addresses safety of equipment, people and the environment as primary concern, can be seen as part of the overall discipline of Risk Management[1]. The relationship between the different elements of risk management is shown in Figure 1. Similarly, this model is applicable to Safety Engineering, where a safety analysis should be followed by a safety evaluation (i.e. safety assessment). Safety management consists of the reduction of the likelihood of occurrence (or control) of hazards, as identified by appropriate safety analyses.

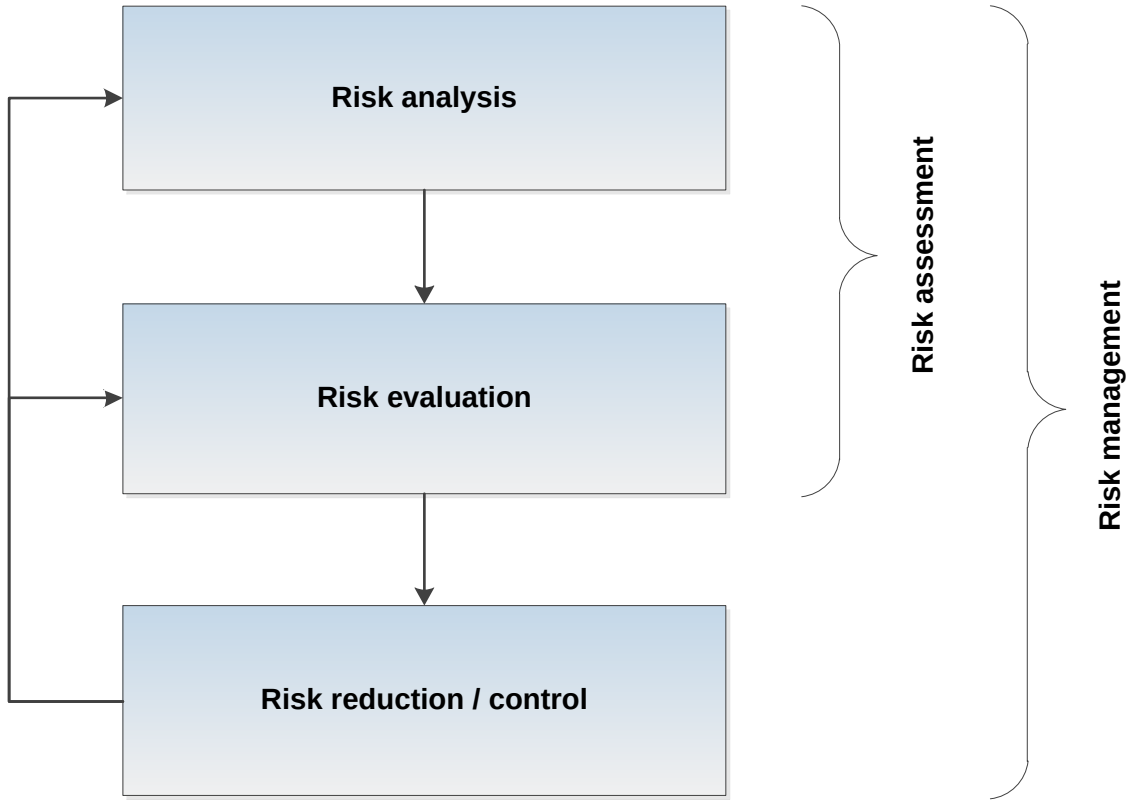

Figure 1: Relation between risk assessment and risk management

[1] IEC 60300-3-1, *Dependability management – Part 3-1: Application guide – Analysis techniques for dependability – Guide on methodology*

3.1.2 Hazard principles

3.1.2.1 Hazard consists of three components

A hazard consists of three basic components, as shown in Figure 2. Each of the following components must be present to constitute a hazard:

1 **Hazardous element** is the basic hazardous resource creating the impetus for the hazard (e.g. flammable material).

2 **Initiating mechanism** is the trigger or initiator event(s) or mechanism(s) that can cause transition of the hazard from a dormant state to an active mishap or accident.

3 **Target or threat** is the person or item that is vulnerable to injury and/or damage. It describes the expected consequential damage and loss, and determines the severity of the mishap event.

Figure 2: Definition of hazard

These concepts can be illustrated by the following example:

A worker can be electrocuted (target or threat) by touching exposed contacts (initiating mechanism) in an electrical panel containing high voltage (hazardous element).

It should be noted that the three hazard components are occasionally called source (hazardous element), mechanism (initiating mechanism) and outcome (target or threat).

3.1.2.2 Hazards, mishaps and risks are not random events

Mishaps and accidents are not random events but are deterministic events. Mishaps and accidents do not just happen but are the result of a unique set of conditions. A hazard is a potential condition that can result in a mishap or accident. This means that mishaps can be predicted via hazard identification and that mishaps can be prevented or controlled via hazard elimination or mitigation. Hazard identification should include all process, hardware, software and human aspects.

A hazard is the precursor to a mishap or accident and defines a potential event, while a mishap or accident is the occurred event. This results in a direct relationship between a hazard and a mishap or accident. A hazard and a mishap, or accident, are two separate states of the same phenomenon, linked by a state transition that must occur. A hazard is a "potential event" at the one end of the spectrum that may be transformed into an "actual event" at the other end of the spectrum. Generally, the state transition is characterised by 1) some sort of an energy build-up in the transition phase, and 2) a point of no return for the mishap occurring. The risk of a mishap or accident is defined by both the probability of occurrence and the severity of the consequences. The relationship between hazard, state transition, mishap and risk is shown in Figure 3.

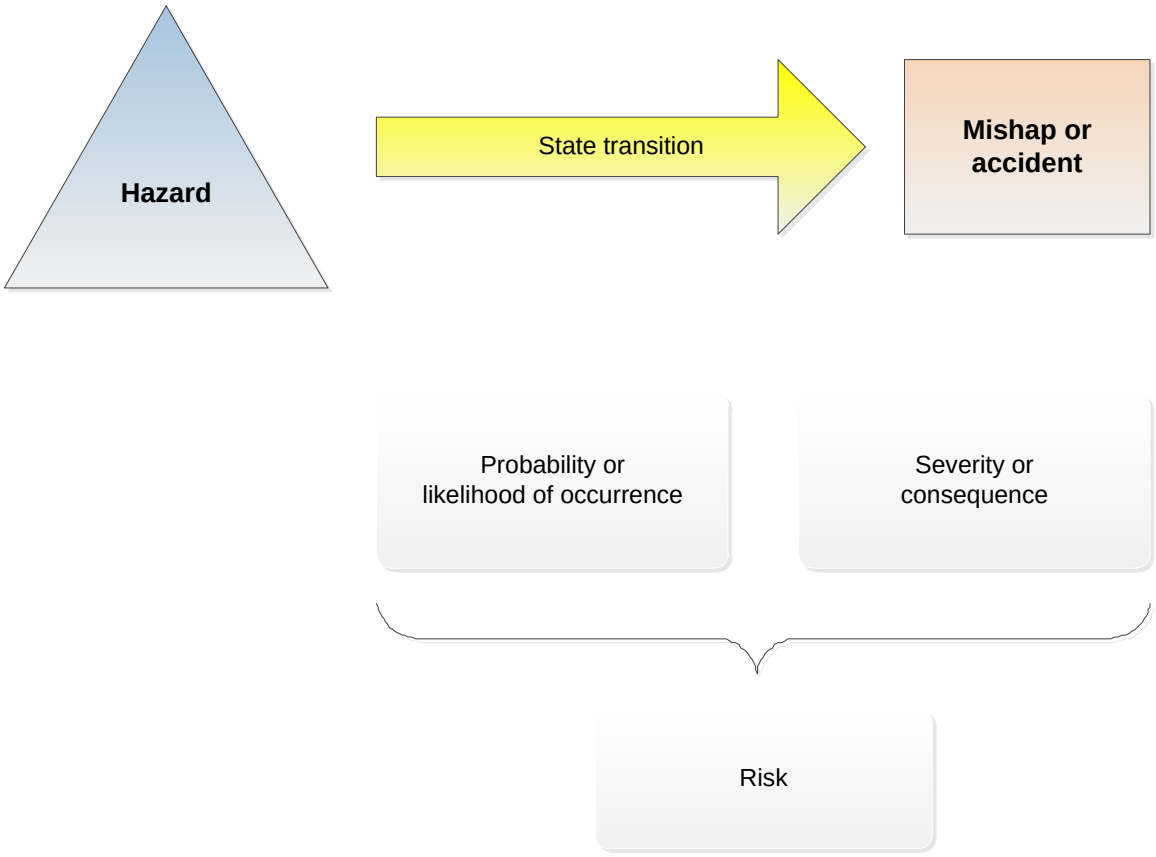

Figure 3: Transition of hazard to mishap or accident

3.1.2.3 Hazards are created during design

Hazards exist in systems because 1) they are unavoidable (e.g. hazardous elements are required in the system), or 2) they are the result of inadequate design safety considerations. Systems with hazardous elements will always have hazards that cannot be eliminated. These hazards are usually well known and the system mishap risk can be managed to an acceptable level. In order to reduce risk, the hazards should first be analysed (using appropriate hazard analysis methods). Frequently, however, hazards are inadvertently injected into the system design through design errors or lack of foresight. These issues are more difficult to identify and analyse (again using appropriate hazard analysis methods).

3.1.2.4 Inductive and deductive logic

Depending on the specific safety analysis, it can be based on either deductive or inductive logic. As shown in Figure 4, Failure Mode and Effects Analysis (FMEA) is an inductive "bottom-up" approach to failure analysis, i.e. it starts with individual functional or hardware failure modes and identifies the failure effects at higher system levels. Fault Tree Analysis (FTA) is a deductive "top-down" approach to failure analysis, i.e. it starts with an undesirable end effect (or top event) and identifies lower-level failure modes (or faults) which can cause the top event.

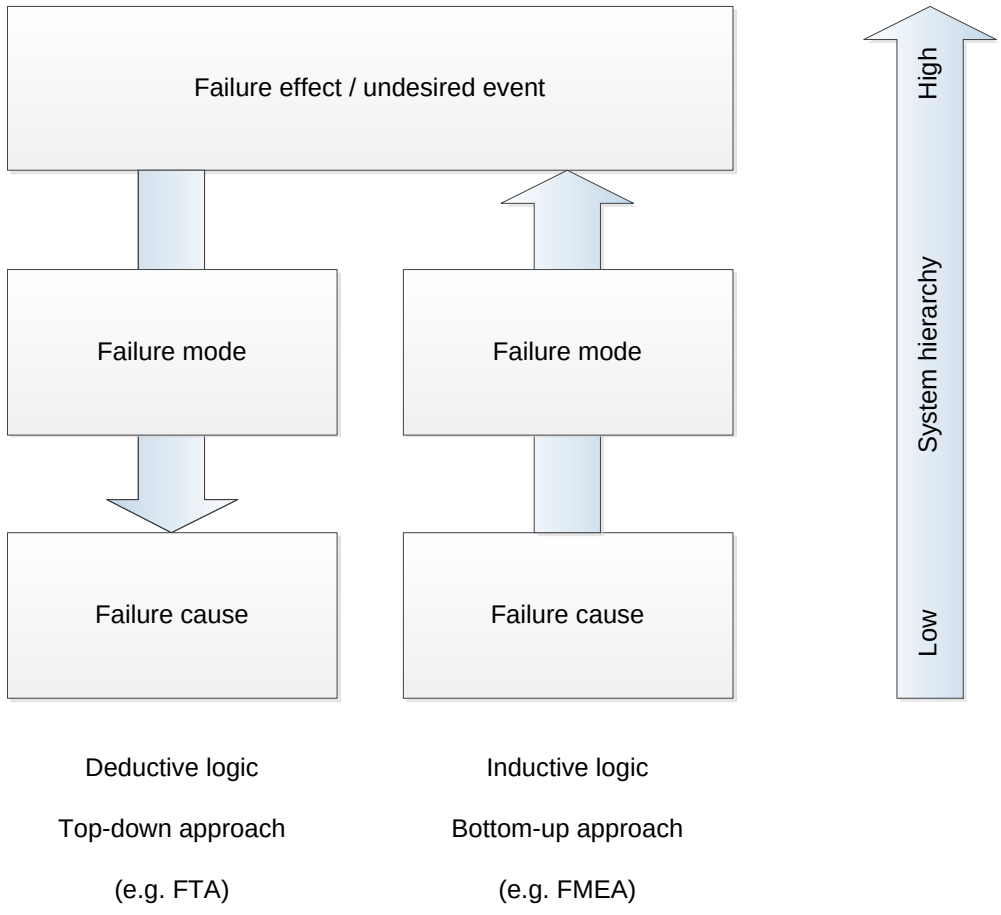

Figure 4: Deductive vs. inductive logic

3.2 SAFETY ANALYSIS

Timeous execution of the correct Safety Engineering activities is of utmost importance in achieving the required safety. Therefore, inappropriate Safety Engineering activities, executed too late during product or system development stages, are major contributing factors to an ineffective Safety Engineering program. The Safety Engineering effort should always be treated as an integral part of product or system development. The output from Safety Engineering analyses is an essential input to other project management activities (such as design reviews) and should, therefore, be scheduled for timeous completion.

Due to the fact that numerous different Safety Engineering activities are available, the appropriate activities should be selected and tailored according to the objectives for the specific project. The selected and tailored activities should be documented in a Safety Program Plan. A typical plan should indicate which activities to be performed, the planned timing of the activities, the level of detail required for the activities and the persons responsible for execution of the activities.[2]

3.2.1 HAZOP analysis

Hazard and Operability (HAZOP) analysis is a structured and systematic analysis of a defined system, with the objective to identify potential hazards in the system and to identify potential operability problems with the system. The resulting knowledge on potential hazards and operability problems is necessary to determine appropriate remedial measures. HAZOP analysis (also known as HAZOP study or HAZOP) deals with the identification of potential deviations from the design intent, examination of their possible causes and assessment of their consequences. The analysis is carried out by a multi-disciplinary team under the guidance of a HAZOP analysis leader. It is considered a mandatory process in many industries (e.g. process industries).

HAZOP analysis is described in more detail in a separate guideline, *HAZOP Guideline*, Eskom document number 240-49230111.

3.2.2 Fault tree analysis

Fault Tree Analysis (FTA) is a top-down analysis used to identify potential reliability and safety problems in complex systems. The analysis starts with the definition of a top event, and proceeds by showing how this top event can be caused by individual or combined lower-level failures or events. Typically, the top event describes an unwanted or undesirable system failure mode. Therefore, a fault tree is a diagram that graphically shows combinations of failures or events leading to a defined system failure.

Fault tree analysis is described in more detail in a separate guideline, *Fault Tree Analysis Guideline*, Eskom document number 240-49230125.

[2] Many safety engineering activities should in practice be performed by the Eskom Centres-of-Excellence.

3.2.3 Failure mode and effects analysis

Failure Mode and Effects Analysis (FMEA) is a bottom-up analysis of a product or system to identify potential failure modes, failure causes and subsequent failure effects on system performance. FMECA (Failure Mode, Effects and Criticality Analysis) is an extension of FMEA in order to include a means of ranking the severity of the identified failure modes. This is done by combining failure severity with probability of failure occurrence to provide failure criticality.

FMEA is described in more detail in a separate guideline, *Failure Mode and Effects Analysis Guideline*, Eskom document number 240-49230046.

3.2.4 Functional safety

Automatic protection equipment is frequently used to safeguard people, equipment and the environment from potentially hazardous events. The optimal design of such automatic protection equipment is known as “functional safety”.

IEC standards can be used as reference to achieve functional safety during system design. IEC 61508 is a basic safety standard which is based on two fundamental concepts. The safety life-cycle refers to a detailed engineering design process intended to reduce or eliminate failures due to systematic errors. Probabilistic failure performance analysis, quantified in order of magnitude levels (called safety integrity levels (SIL)), is intended to address random errors.

IEC 61511 is applicable to process industries, IEC 62061 addresses machinery safety and IEC 61513 deals with the nuclear industry. Since IEC 61508 is a standard and not a regulation or law, compliance is not always legally required. However, in many instances, compliance is identified as best practice and, thus, can be cited in liability cases.

3.2.5 Root cause failure analysis

Root Cause Failure Analysis (RCFA) refers to a structured approach to identify the factors that resulted in the nature, magnitude, location and timing of an unwanted failure mode. Knowledge on the root cause of failures is essential to recommend corrective actions to mitigate or prevent recurrence of similar failures. Root Cause Failure Analysis may be used as part of a continuous improvement program or it may be mandatory, following a serious incident or accident.

Root Cause Failure Analysis is described in more detail in a separate guideline, *Root Cause Failure Analysis Guideline*, Eskom document number 240-49910497.

3.2.6 Common cause failure analysis

Common Cause Failure Analysis (CCFA) is an analysis for identifying common causes of multiple failure events. A common cause failure is a single-point failure that destroys independent redundant designs. Therefore, the objective of CCFA is to discover common cause vulnerabilities in the system design that can result in the common failure of redundant subsystems and to develop design strategies to mitigate these types of hazards. Common cause failures are not always obvious, which make them difficult to identify. The potential for this type of event exists in any system architecture that relies on redundancy or uses identical components or software in multiple subsystems.

3.2.7 Fire hazard analysis

Basic approaches to fire safety design acknowledge that fire prevention is an important facet of overall fire safety. Fire hazard analysis refers to the comprehensive evaluation of the causes of, impacts from and consequences of fire in a specific location. It is a process, in a building or a structure, considering the effects of engineered systems, administrative programs and manual intervention. Fire hazard analysis is, thus, more extensive than simple fire inspections and other traditional fire prevention techniques.

By combining fire hazards analysis with risk assessment, system design and performance-based analyses, specific fire prevention needs can be identified and effective controls can be developed. Fire hazard analysis is performed whenever fire or life safety design or evaluation is undertaken. When making decisions regarding the capabilities of engineered systems, the design must consider the type, quantity and location of combustibles in the area protected.

3.3 APPLICABLE LEGISLATION

Safety, health and environmental legislation contains a vast number of safety-related requirements which should be considered during system design. Although legislation (and any related regulations) cannot be seen as analyses, they are referenced as essential inputs to any system design process. Note that the following list is not comprehensive and should be updated with current legislation and applied according to the requirements of a specific project.

3.3.1 Safety and Health Legislation

a) Occupational Health and Safety Act 85 of 1993
b) Hazardous Substances Act 15 of 1973
c) National Building Regulations and Building Standards Act 103 of 1997
d) National Road Traffic Act 93 of 1996
e) Water Services Act 108 of 1997
f) National Standards Act 29 of 1993

3.3.2 Environmental Legislation

a) Atmospheric Pollution Prevention Act No 45 of 1965
b) Environment Conservation Act no 73 of 1989
c) National Environmental Management Act 107 of 1998
d) Mountain Catchment Areas Act 63 of 1970
e) National Forests Act 84 of 1998
f) National Water Act 36 of 1998

3.3.3 National Standards

The following National Standards are referred to from the Occupational Health and Safety Act Regulations):

a) SANS 347, Categorisation and Conformity Assessment Criteria for all Pressure Equipment
b) SABS 099, Construction of Air Receivers
c) SABS 219, Construction of welded steel cylinders for LP Services
d) SANS 10087, Handling, storage and distribution of LPG in domestic, commercial and industrial installations
e) SABS 1545 – 1 & 2, Lifts and Service Lifts
f) SABS 0147, Refrigeration and Air-conditioning Installations
g) SABS 0108, The Classification of Hazardous Locations and the Selection of Electrical Apparatus for Use in Such Areas

3.3.4 Occupational Health and Safety Act 85 of 1993

The Occupational Health and Safety Act currently contains 21 sets of regulations, of which the following 11 regulations have relevance to system design:

a) Asbestos regulations
b) Construction regulations
c) Driven machinery regulations
d) Electrical installation regulations
e) Electrical machinery regulations
f) Environmental regulations
g) Facilities regulations
h) Driven machinery regulations
i) Lift, escalator and passenger conveyor regulations
j) Noise induced hearing loss regulations
k) Pressure equipment regulations

4. AUTHORISATION

This document has been seen and accepted by:

Name	Designation
	Document approved by TDAC ROD 31 January 2013

5. REVISIONS

Date	Rev.	Compiler	Remarks
November 2012	1	E Pininski	Final Document for Authorisation and Publication.

6. DEVELOPMENT TEAM

The following people were involved in the development of this document:

- RWA Barnard, Lambda Consulting, 082 344 0345
- B Magner, Magallan Risk Services, 083 550 0957
- E Pininski, Eskom, pininse@eskom.co.za

7. ACKNOWLEDGEMENTS

NONE