Eskom	Guideline	Technology

Title:	**Reliability Engineering Analysis Guideline**	Unique Identifier:	**240-49230030**
		Alternative Reference Number:	**N/A**
		Area of Applicability:	**Engineering**
		Documentation Type:	**Guideline**
		Revision:	**3**
		Total Pages:	**11**
		Next Review Date:	**February 2024**
		Disclosure Classification:	**CONTROLLED DISCLOSURE**

APPROVED FOR AUTHORISATION
TECHNOLOGY ENGINEERING
DOCUMENT CENTRE ☎ X4962

Compiled by	Approved by	Authorised by
....	....	....
G.F Fuhnwi	**P. Phochana**	**S. Ndlovu**
Snr Technologist: System Design	**Chief Technologist: System Design**	**SC Chairperson**
Date: 08/02/2019	Date: 08/02/2019	Date: 2019/02/11

		Supported by TC
		....
		L. Fernandez
		TC Chairperson
		Date: 2019/02/14

PCM Reference: **Perform Design Analysis**

SCOT Study Committee Number/Name: **Design Integr, Reliability and Safety Eng SC**

CONTENTS

Page

FIGURES

1. INTRODUCTION

Reliability Engineering refers to the Engineering discipline which addresses reliability and maintainability of a product or system during its total lifecycle. Reliability Engineering Analysis refers to the different analyses to be used for specification, allocation, designing-for, evaluation and/or measurement of reliability and maintainability of a product or system. These analyses are primarily applicable during system design but can also be used during operations and maintenance.

2. SUPPORTING CLAUSES

2.1 SCOPE

This guideline contains concise descriptions for a number of Reliability Engineering Analysis. Detailed guidelines for some of these analyses have already been developed (e.g. Failure Mode and Effects Analysis). It is recommended that formal Eskom guidelines for the other analyses (e.g. aging/degradation analysis) be developed in future.

2.1.1 Purpose

The purpose of this document is to provide information for the different Reliability Engineering Analyses which may be used during the different lifecycle 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

Parties using this document shall apply the most recent edition of the documents listed in the following paragraphs.

2.2.1 Normative

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

2.2.2 Informative

[2] P.D.T. O'Connor and A. Kleyner, *Practical Reliability Engineering*, 5th edition, John Wiley, 2012

Definitions
Not applicable.

2.3 CLASSIFICATION

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

2.4 ABBREVIATIONS & ACRONYMS

Abbreviation or Acronym	Description
EMI	Electromagnetic Interference
EMC	Electromagnetic Compatibility
FMEA	Failure Mode and Effects Analysis

Abbreviation or Acronym	Description
FMECA	Failure Mode, Effects and Criticality Analysis
FRACAS	Failure Reporting and Corrective Action System
FTA	Fault Tree Analysis
RAM	Reliability, Availability and Maintainability
RCA	Root Cause Analysis

2.5 ROLES AND RESPONSIBILITIES

Not applicable.

2.6 PROCESS FOR MONITORING

Not applicable.

2.7 RELATED/SUPPORTING DOCUMENTS

[3] 240-49230100 Safety Engineering Analysis Guideline

[4] 240-49230111 HAZOP Analysis Guideline

[5] 240-50055960 Procurability Analysis Guideline

[6] 240-50056004 Constructability Analysis Guideline

[7] 240-49910508 Environmental Analysis Guideline

[8] 240-49230100 Safety Engineering Analysis Guideline

[9] 240-49230046 FMEA Guideline

3. INTRODUCTION

Reliability can be defined as "*the probability that an item will perform a required function without failure under stated conditions for a stated period of time*". Reliability Engineering refers to the specialised Engineering discipline which addresses the reliability of a product or system during its total lifecycle. It includes related aspects, such as maintainability, availability, safety, etc.

The objectives of Reliability Engineering, in the order of priority, are:

1. To apply engineering knowledge in order to prevent or reduce the likelihood or frequency of failures;
2. To identify and correct the causes of failures that occur, despite the efforts to prevent them;
3. To determine ways of coping with failures that occur, if their causes have not been corrected; and
4. To apply methods for estimating the likely reliability of new designs and for analysing reliability data.

The reason for the priority emphasis is that it is by far the most effective way of working, in terms of minimising costs and developing reliability products and systems. Proactive prevention of failure is always more cost-effective than reactive correction of failure.

Timeous execution of the *correct Reliability Engineering activities* is of utmost importance in achieving the required reliability. Therefore, inappropriate Reliability Engineering activities, executed too late during product or system development stages, are major contributing factors to an ineffective Reliability Engineering program. The Reliability Engineering effort should always be treated as an integral part of product or system development. The output from Reliability Engineering Analysis 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 Reliability 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 Reliability 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.[1] Figure 1 indicates what information relating to the specific project is necessary to select and tailor Reliability Engineering activities.

[1] Many design-for-reliability activities should in practice be performed by the Eskom Centres-of-Excellence.

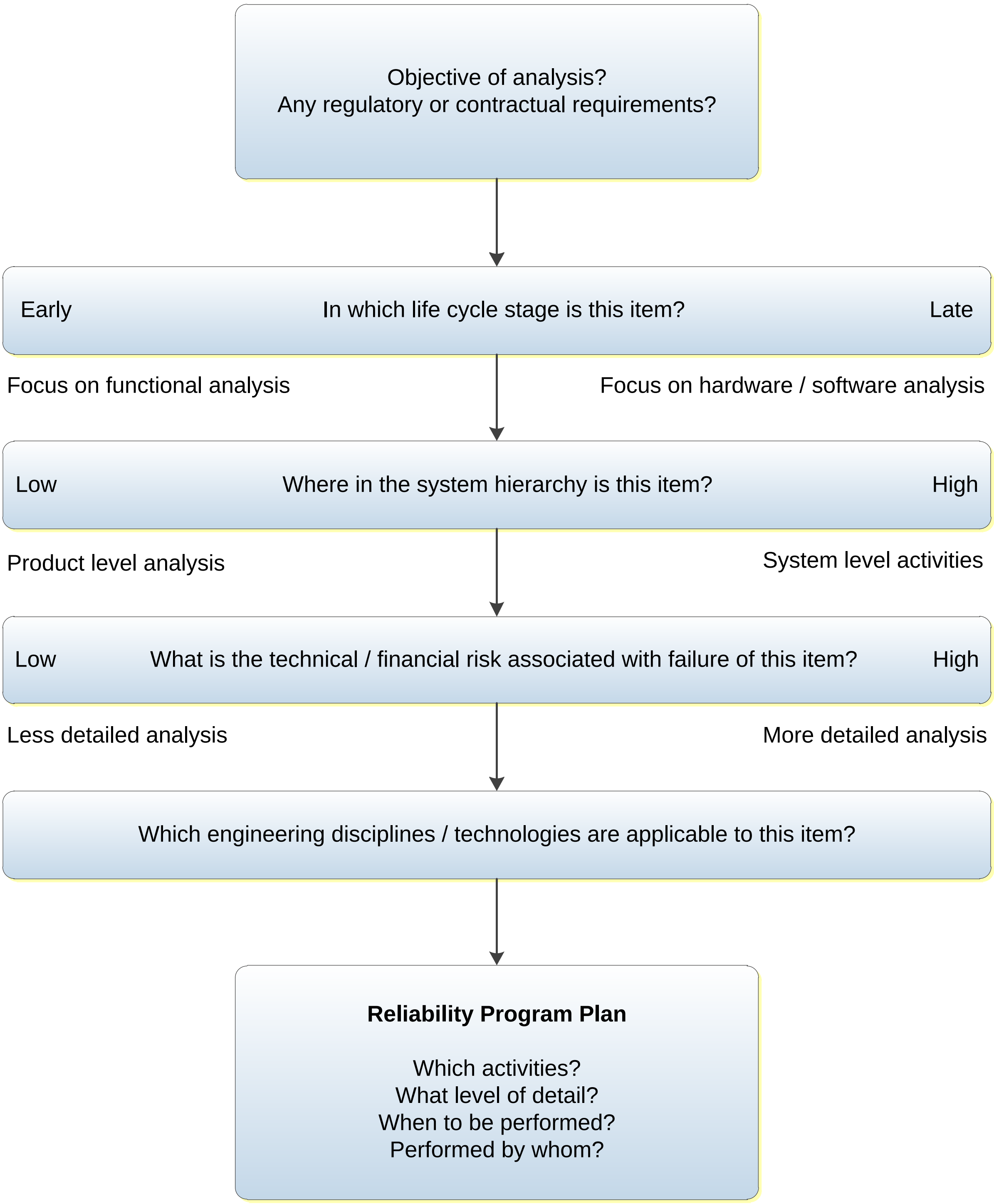

Figure 1: Reliability Program Plan Development

3.1 RELIABILITY ENGINEERING ANALYSIS

Reliability Engineering activities can be classified as either *management*[2] or *engineering* activities. This guideline refers primarily to Reliability Engineering activities and, more specifically, to Reliability Engineering Analysis.

3.1.1 Reliability, Availability and Maintainability specification

Reliability, Availability and Maintainability (RAM) specification refers to the specification of, primarily, quantitative reliability, availability and maintainability parameters. This activity should be performed as part of requirements analysis and, as such, be performed early during product or system development. It should include aspects such as RAM metrics, failure definitions, failure distributions, user profiles, environmental profiles, etc.

3.1.2 Reliability, Availability and Maintainability allocation

Reliability, Availability and Maintainability (RAM) allocation refers to the allocation (also known as apportionment) of, primarily, quantitative system reliability, availability and maintainability specifications to lowerlevel subsystems. This activity should be performed early during product or system development in order to influence the design processes.

3.1.3 Environmental analysis

Environmental analysis refers to the analysis required to determine detailed environmental conditions applicable to a specific product or system. It includes determination and documentation of both user and environmental profiles. It includes all operating and nonoperating environments (including storage), expected operating and nonoperating times (including maintenance) and environmental factors (e.g. temperature, humidity, vibration, shock, etc.).

Environmental analysis is described in more detail in a separate guideline, *Environmental Analysis Guideline*, Eskom document number 240-49910508.

3.1.4 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.

[2] Examples of management activities include Reliability Program Plan development, reliability training of personnel, establishment of preferred part lists, control of subcontractor reliability activities, etc.

3.1.5 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.

3.1.6 System RAM analysis

System RAM analysis refers to system evaluation in terms of reliability, availability, maintainability, lifecycle costs, etc. It includes development of reliability block diagrams, model verification, sensitivity analysis and the obtaining of reliability and maintainability (i.e. uptime and downtime) estimates. Typically, system RAM analysis can be performed using Monte Carlo simulation or Markov analysis. Generally, it is only applicable to higherlevel systems and not to product reliability. System RAM analysis can also be used for the facilitation of RAM allocation (or apportionment).

System RAM analysis is described in more detail in a separate guideline, *System RAM Analysis Guideline*, Eskom document number 240-52844017

3.1.7 Load-strength analysis

Load-strength analysis refers to the fundamental Reliability Engineering principle, in which, applied load should never exceed design strength. Therefore, load-strength analysis should be an inherent part of any design activity. It is used to determine the robustness of a design and it includes aspects such as definition of loading roughness and safety margin, interference between load and strength distributions, probabilistic design, safety factors (for mechanical design), derating factors (for electronic design), etc.

3.1.8 Aging / degradation analysis

Aging/degradation analysis refers to the analysis of health and usage parameters of an existing product or system. It requires comprehensive information on usage (e.g. operating time, power-up cycles, etc.), applicable failure mechanisms (e.g. corrosion, fatigue, etc.), material properties, environmental conditions, etc. to determine asset health. Condition monitoring (by providing realtime input) may be used to facilitate aging/degradation analysis. Aging/degradation analysis may also be supported by life data analysis (refer to *Life Data Analysis Guideline*, Eskom document number 240-49230067).

3.1.9 Life Data Analysis

Life Data Analysis refers to the application of statistical analyses to determine the reliability characteristics of either components or systems based on actual failure data. The required failure data may originate from component or system development (e.g. test data) or may be recorded during operations and maintenance using an appropriate FRACAS (Failure Reporting and Corrective Action System).

It is imperative to distinguish between component life data analysis (i.e. non-repairable items where data typically consists of individual times-to-failure) and system life data analysis (i.e. repairable systems where data typically consists of times of successive failures in a single system). Non-repairable items are typically analysed using Weibull analysis, while repairable systems may be analysed using the Laplace test.

Life data analysis is described in more detail in a separate guideline, *Life Data Analysis Guideline*, Eskom document number 240-49230067.

3.1.10 Reliability testing

Testing in Engineering can be divided into functional testing, reliability testing and safety testing. Reliability testing refers to practical testing of prototype or production units in order to determine reliability characteristics. Reliability testing is, therefore, not classified as an analysis but is frequently used to complement reliability analysis. Functional testing is used to confirm that the design meets the performance requirements (also called compliance or qualification testing). Reliability testing differs from functional testing, since it should focus on identifying potential design or production weaknesses (e.g. failure mechanisms). Typically, reliability testing is performed on products, while reliability growth monitoring may be applicable for systems during operations. The objective of safety testing is to verify compliance to safety and regulatory requirements.

3.1.11 Failure Reporting and Corrective Action System

All failures occurring during the product or system lifecycle should be reported and analysed to determine possible corrective action. FRACAS is an acronym used for the management and software application required to support these aspects. It should be initiated during product or system design but it is primarily used during operations and maintenance.

Failure Reporting and Corrective Action System is described in more detail in a separate guideline, *FRACAS Guideline*, Eskom document number 240-49910503.

3.1.12 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.

3.1.13 Electromagnetic Interference and Compatibility Analysis

Electromagnetic interference (EMI) refers to the disturbance of correct electronic circuit operation by changing electromagnetic fields or other electrical stimuli. These emissions may be received by other electronic products, causing malfunction of equipment. Electromagnetic compatibility (EMC) is the ability of products and systems to withstand these adverse effects and is sometimes called electromagnetic immunity. Both analysis and testing should be used to manage EMI and EMC during product or system design.

3.1.14 Human factors or ergonomics

Human factors or ergonomics refers to the multi-disciplinary field which integrates product or system design with psychology, statistics, operations research and anthropometry. It refers to the study of designing equipment that fits the human body and its cognitive abilities. Human factors or ergonomics is, therefore, concerned with the 'fit' between the user, equipment and their environments.

3.1.15 Additional design engineering analyses

Numerous other design engineering analyses can be successfully applied to aid in performing Reliability Analysis. Examples include the following:

a. Thermal analysis

b. Physics-of-failure

c. Fatigue analysis

d. Finite element analysis

e. Computational fluid dynamics

4. AUTHORISATION

This document has been seen and accepted by:

Name	Designation
Thabelo Mamphogoro	Snr Engineer Prof Engineer
Gert-Daniel Scholtz	Engineer
Peter Phochana	Chief Technologist
Godwin Fuhnwi	Senior Technologist
Selelepoo Ntoampe	Engineer
Siyabonga Ndlovu	System Design Middle Manager
Phinda Dlamini	Snr Advisor
Tony Haupt	Chief Engineer
Dustin Fransman	Snr Engineer
Amanda Dube	Snr Technician
Theo Kleynhans	Snr Engineer
Theunus Marais	Chief Engineer
Tebogo Mokwana	Snr Consultant Engineering
Phuti Ngoetjana	Snr Advisor
Nelisiwe Nhlapo	Senior Technologist

5. REVISIONS

Date	Rev.	Compiler	Remarks
November 2012	1	E Pininski	Final Document for Authorisation and Publication
November 2015	2	H Visagie	Final Rev 2 Document for Authorisation and Publication
May 2018	2.1	GF Fuhnwi	Updated Final Draft after Review Process
February 2019	3	GF Fuhnwi	Final Rev 3 Document for Authorisation and Publication

6. DEVELOPMENT TEAM

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

Reliability and Safety Engineering during Design Work Group

7. ACKNOWLEDGEMENTS

- RWA Barnard, Lambda Consulting, 082 344 0345
- E Pininski, Eskom, pininse@eskom.co.za