Eskom	Guideline	Technology

Title: **System Reliability, Availability and Maintainability Analysis Guideline**

Unique Identifier:	**240-52844017**
Alternative Reference Number:	**N/A**
Area of Applicability:	**Engineering**
Documentation Type:	**Guideline**
Revision:	**3**
Total Pages:	**16**
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 : **Reliability & Safety SC**

CONTENTS

FIGURES

1. INTRODUCTION

System Reliability, Availability and Maintainability (RAM) Analysis refers to system evaluation in terms of reliability, availability, maintainability, life-cycle costs, throughput, etc. It includes modelling of the system using reliability block diagrams, model verification and assigning of reliability and maintainability (i.e. uptime and downtime) data to individual blocks. Reliability block diagrams show the relationship between subsystems in terms of success paths (i.e. series, parallel and other complex configurations). System RAM Analysis is typically performed using Monte Carlo simulation where a deterministic model is repeatedly evaluated.

2. SUPPORTING CLAUSES

2.1 SCOPE

This guideline describes the process of performing System RAM Analysis using Monte Carlo simulation. It provides guidance on the principles of the analysis and the procedural steps necessary to perform an analysis.

2.1.1 Purpose

The purpose of this document is to provide guidance on the principles of System RAM Analysis and the procedural steps necessary to consistently perform effective system analyses on 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] IEC 61078, *Analysis techniques for dependability – Reliability block diagram method*

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

2.3 DEFINITIONS

Not Applicable

2.3.1 Disclosure Classification

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

2.4 ABBREVIATIONS

Abbreviation	Description
BOM	Bill of Materials
FMEA	Failure Mode and Effects Analysis
FTA	Fault Tree Analysis
MTBF	Mean Time Between Failure
MTTF	Mean Time To Failure
RAM	Reliability, Availability and Maintainability
RBD	Reliability Block Diagram

2.5 ROLES AND RESPONSIBILITIES

Not Applicable.

2.6 PROCESS FOR MONITORING

Not Applicable.

2.7 RELATED/SUPPORTING DOCUMENTS

Not Applicable.

3. SYSTEM RAM ANALYSIS OVERVIEW

During the initial stages of system design, block diagrams are typically developed where each block represents a sub-system of the total system. A *schematic block diagram* shows how the sub-systems are physically connected, while a *functional block diagram* shows the flow of power, material, information, etc. through the system. Similarly, system reliability and availability may be analysed using a Reliability Block Diagram (RBD). The connections between sub-systems in a RBD indicate the ways in which the system will *function as required* and do not necessarily indicate the actual physical connections. Therefore, a RBD shows the relationship between sub-systems in terms of success paths (i.e. series, parallel and other complex configurations). A RBD is usually developed using schematic or functional block diagrams of the system as a starting point.

System RAM (Reliability, Availability and Maintainability) Analysis refers to system evaluation in terms of reliability, availability, maintainability, life-cycle costs, throughput, etc. It includes modelling of the system using reliability block diagrams, model verification and assigning of reliability and maintainability (i.e. uptime and downtime) data to individual blocks. It is generally only applicable to higher level systems, and not to lower levels sub-systems. System RAM Analysis is typically performed using Monte Carlo simulation where a deterministic model is repeatedly evaluated.

System RAM Analysis typically consists of the development of a system model, the verification of the developed model, and finally the use of the verified model. As such, it follows a highly-iterative process of model development, model verification and model use.

The analysis should be initiated as soon as possible, even as early as concept stage. If performed early in the development cycle, implementation of design changes to overcome deficiencies identified by the System RAM Analysis may be cost-effective.

3.1 MONTE CARLO SIMULATION

Monte Carlo simulation is an analysis method where a deterministic model is repeatedly evaluated using sets of random numbers as inputs. For example, for the parametric model $y=f(x_1, x_2, x_3, \ldots, x_n)$, the input values $x_1, x_2, x_3, \ldots, x_n$ are generated (or sampled) and the respective output values of y are recorded for further analysis. The random values are generated to follow an arbitrary statistical distribution which simulates the process of sampling from an actual population. The distribution for each input parameter is chosen based on best available knowledge about that input parameter. Typical distributions may include the normal distribution, exponential distribution, Weibull distribution or any other statistical distribution. The data generated by simulation is typically presented as histogram or probability distribution function.

In addition to other statistical distributions, the following basic distributions are frequently used in Monte Carlo analysis:

The uniform or rectangular distribution is a distribution with constant probability over an interval. The triangular distribution is defined as a three-point distribution with a minimum, most likely and maximum values, and is often used as an engineering approximation of the normal distribution.

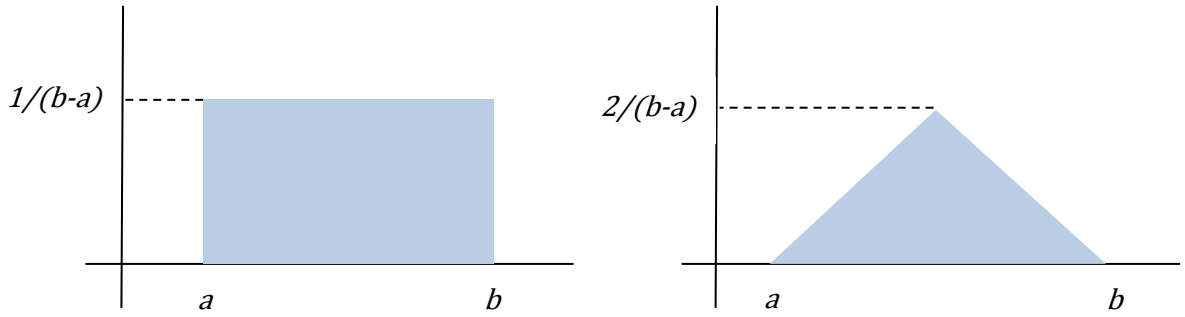


Figure 1: Rectangular and triangular failure distributions

A spreadsheet application can be used to perform basic Monte Carlo simulations[1]. In this case, a basic formula is calculated repeatedly to generate the required output values. However, for complex real-life problems, more sophisticated modelling can be performed using a commercially available Monte Carlo simulation package. The number of Monte Carlo simulation runs required to achieve 'stability' of the output depends on the complexity of the deterministic model, the variance of the input parameters and the required accuracy of the output.

[1] *Practical Reliability Engineering* (5th edition) contains Microsoft Excel functions for statistical distribution sampling.

3.2 SYSTEM RAM ANALYSIS PROCESS

The System RAM Analysis process consists of the following four basic steps:

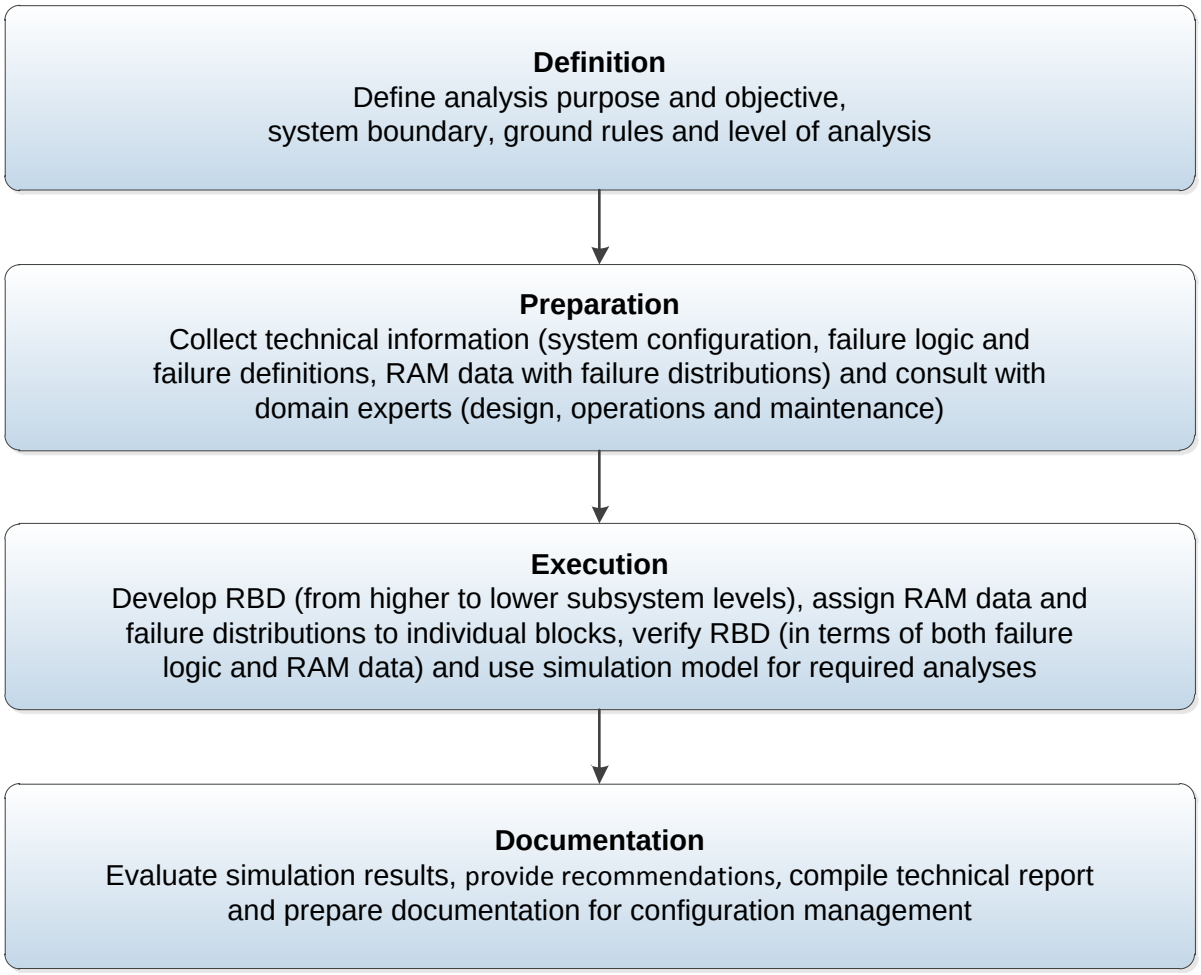


Figure 2: System RAM analysis basic steps

3.2.1 Definition

Define analysis purpose and objective, system boundary, ground rules and level of analysis

Typically, the requirement for performing System RAM Analysis will be stated in the overall project plan, with higher-level analysis objectives listed, e.g. what are the expectations for the analysis. The purpose and objectives of the specific System RAM Analysis should be derived from these higher-level objectives, defined and documented prior to execution of the analysis. The definition of purpose and objectives is important since it will have a direct influence on the ground rules and the system boundary.

Analysis basic rules may include, among others, analysis viewpoint and redundancy considerations.

The system boundary forms the physical and functional interface between the system and its environment, including other systems with which the system interacts. Systems and/or sub-systems outside this boundary should explicitly be defined for exclusion. For complex systems, it may be advantageous to define the system boundary in terms of a functional rather than physical viewpoint (i.e. hardware).

It is important to determine the system indenture level that will be used for the analysis. For example, systems can be broken down into functions or sub-systems, replaceable units, individual parts, etc. Excessive time on lower-risk systems should be avoided. The following guidelines may be useful to determine the level of analysis:

a) Level of analysis should be determined by the purpose and objectives of the analysis

b) Level of analysis should be determined by the availability of design information

c) Analysis at the highest system level tends to lead to obvious results (e.g. no or little new knowledge is generated on system behaviour)

d) Analysis at the lowest system level (i.e. parts) tends to lead to extensive unnecessary analysis (i.e. no value-added information generated)

e) Less detailed analysis may be justified for a system based on a mature design (i.e. known reliability and/or safety record)

f) More detailed analysis may be required for new technology, new design (where risk is a concern), new application of existing technology, systems with potential safety issues, systems with a history of significant field failure problems, potential for important regulation issues, supplier capability concerns, etc.

g) Level of analysis may be determined by the specified or intended maintenance and repair level (e.g. line replaceable item level)

3.2.2 Preparation

Collect technical information (system configuration, failure logic and failure definitions, RAM data with failure distributions) and consult with domain experts (design, operations and maintenance)

System RAM Analysis is typically performed by an analyst who should have both sufficient technical knowledge of the system and experience in system analysis / modelling. However, since a system normally consists of a variety of different sub-systems from different engineering disciplines, the analyst should consult with domain experts from all relevant disciplines (e.g. design, operations and maintenance).

All relevant technical information on the system should be collected prior to analysis execution, including:

a) System specification (e.g. functional breakdown with performance requirements)

b) Sub-system interaction (e.g. functional block diagram indicating relationship between sub-systems)

c) Redundancy configuration (e.g. series / parallel blocks, active / standby redundancy)

d) Environmental and use profiles

e) Operating procedures

f) Maintenance procedures

g) Failure logic (e.g. sequence of required events, etc.)

h) Failure definitions (e.g. degraded operation, etc.)

i) RAM parameters (e.g. probability of success, repair time, etc.)

j) RAM data

k) RAM data failure distributions (e.g. Weibull parameters)

l) Operating and maintenance costs (for Life Cycle Cost Analysis)

m) Process parameters (for Throughput Analysis)

n) Other technical information (e.g. P&IDs, PFDs, load sharing, system states, operating phases, duty cycles, start-up / shutdown sequences, etc.)

o) Other reliability analysis results (e.g. FMEA and FTA)

RAM data can be obtained (or predicted) from the following sources:

a) Similar equipment

b) Life data analysis (from operational failure data)

c) Life data analysis (from test failure data)

d) Incident and accident investigations

e) Manufacturer failure data

f) Generic reliability data bases

g) Engineering judgement

3.2.3 Execution

Develop RBD (from higher to lower subsystem levels), assign RAM data and failure distributions to individual blocks, verify model (in terms of both failure logic and RAM data) and use simulation model for required analyses

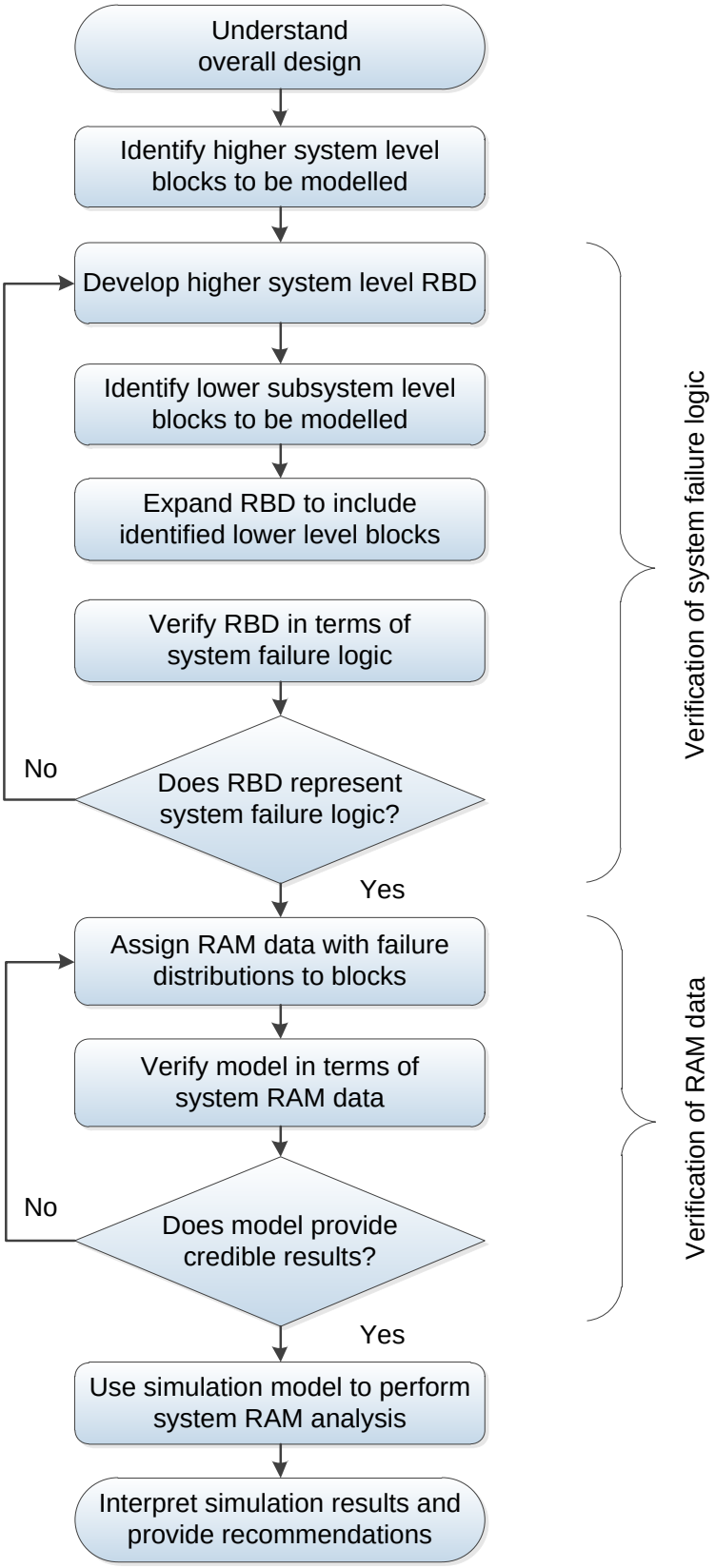
The System RAM Analysis execution sequence diagram is shown in Figure 3

System RAM Analysis typically consists of the development of a system model, the verification of the developed model, and finally the use of the verified model. As such, it follows a highly-iterative process of model development, model verification and model use.

The required RBD should always be developed from a system viewpoint, starting with the identification of higher system level blocks to be modelled. The RBD should accurately model the system failure logic, and should include all redundancies in the system. Based on the objectives of the analysis, lower system level blocks should then be identified, and the RBD should be expanded to include these lower level blocks. Verification of the RBD in terms of failure logic may be supported by FMEA results (if available). Subsequently, RAM data is assigned to the individual blocks, and the model is verified in terms of the expected system RAM based on the assigned data. Therefore, model verification should be based on both system failure logic and RAM data.

The developed simulation model can then be used for a variety of analyses:

a) Reliability analysis
b) Availability analysis
c) Maintainability analysis
d) RAM optimization
e) RAM allocation
f) Life Cycle Cost analysis
g) Throughput analysis
h) Resource planning
i) ‘What-if’ analysis
j) Sensitivity analysis



Note: As part of the first steps, one should also define model failure

Figure 3: System RAM analysis execution sequence diagram

3.2.4 Documentation

Evaluate simulation results, provide recommendations, compile technical report and prepare documentation for configuration management

The System RAM Analysis should be documented in a technical report, which should at least include the following:

a) Summary of analysis and recommendations

b) References (e.g. engineering drawings with revision status)

c) Purpose and objective, system boundary, ground rules and level of analysis

d) System definition (including functional and/or reliability block diagrams)

e) RAM data and failure distributions (including source of data and motivation for assumptions)

f) Simulation results

g) Recommendations

3.3 GENERAL ASPECTS

3.3.1 Limitations of system ram analysis

System RAM Analysis is a powerful analysis to evaluate a system in terms of availability, process throughput, etc. The development and use of a simulation model provides the opportunity to estimate system performance during system design. However, both analyst and user of simulation results should be aware of the following limitations.

3.3.1.1 'Bottom-up' simulation model development

System analysis, by definition, should focus on the system as a whole. Therefore, any simulation or other model used for System RAM Analysis should be developed 'top-down', and be expanded to lower levels where required. A common pitfall to avoid is 'bottom-up' simulation model development, which is a relative easy approach when the system Bill of Materials is used for system definition. This approach frequently results in far too many lower level blocks which may not contribute to the overall objective of the analysis.

3.3.1.2 Modelling of series configurations

Monte Carlo simulation may not be the preferred approach to analyse a system consisting mainly of blocks connected in a series configuration. These systems can easily be analysed using a simple deterministic approach (e.g. spreadsheet application). The analyst should also remember that a large number of 'high reliability' items connected in series will result in 'low system reliability'. For example, connecting only 10 identical items with reliability of 95% will result in a system reliability of only 60%.

3.3.1.3 Assuming exponential failure distribution

Due to simplicity of analysis, analysts frequently assume a constant hazard (or failure rate) for all blocks in a system. This implies that failures are exponentially distributed, which may be totally incorrect. Subsequent system results may therefore be invalid. This assumption should especially be viewed with suspicion for Eskom equipment, where wear-out failure mechanisms may be dominant.

Note: MTTF (or MTBF) is frequently used as an indicator of "average life" of an item, which may be completely incorrect. The exponential distribution describes the situation where the hazard (or failure) rate is constant. It can be shown that the mean value of the exponential distribution (i.e. MTTF (or MTBF)) is $1/\lambda$, and that 63.2% of items will have failed by t = MTTF (or MTBF).

Note: The probability of a 20 year male person dying within one year is 0.002 (or 0.2%)[2]. This person is clearly in the 'useful life' period on the bathtub curve, implying that the exponential failure distribution may be a valid assumption. However, it can easily be shown that in this case, the 'MTTF' is equal to 500 years. This example serves to highlight a mistake frequently made by engineers to use MTTF (or MTBF) as indicator of life expectancy.

3.3.1.4 Unrealistic reliability predictions

Unless the actual failure mechanisms (e.g. fatigue, corrosion, etc.) are known and applicable to the specific environment, it is not possible to perform accurate reliability predictions. Reliability predictions used for System RAM Analysis should therefore always be viewed with caution, and a worst case approach may be beneficial when simulation results are to be used for important design decisions.

3.3.2 Relationship with other analyses

3.3.2.1 Fault Tree Analysis

For system reliability analysis, Fault Tree Analysis (FTA) provides an alternative to reliability block diagram analysis. It is broader in scope than reliability block diagrams and differs from reliability block diagrams in several aspects. It is a top-down, deductive analysis structured in terms of events rather than components and the perspective is on faults rather than reliability. All failures are faults, however, not all faults may be considered failures. For example, a human error resulting in an incorrect switch being set would be treated as a fault although it would not normally be an inherent equipment failure mode. An advantage of focussing on failures is that failures are usually easier to define than non-failures and there may be far fewer ways in which a failure can occur, as opposed to the numerous ways in which non-failures can occur.

System reliability (or availability) can be calculated from either reliability block diagram or fault tree. For example, analysis of a system consisting of series components can be performed using an "OR" gate. Similarly, parallel components in a reliability block diagram can be analysed using an "AND" gate. Some commercial software packages for system analysis combine both RBD and FTA approaches.

[2] South African statistical data, 2010

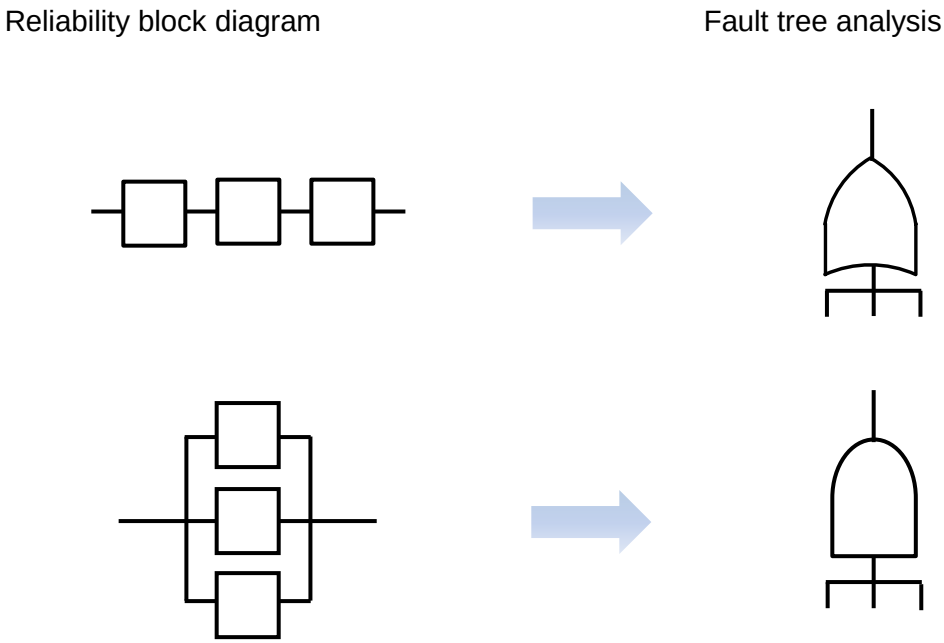


Figure 4: Relationship between RBD and FTA

3.3.2.2 Failure Mode and Effects Analysis

Failure Mode and Effects Analysis (FMEA) is a systematic bottom-up procedure for the analysis of a system to identify potential failure modes, failure causes and subsequent failure effects on system performance. Therefore, FMEA results can be used to facilitate the development of reliability block diagrams, especially for model verification in terms of failure logic.

3.3.2.3 Markov Analysis

A system or component can be in one of two states (e.g. failed or non-failed) and the probabilities associated with these states can be defined on a discrete or continuous basis. The probability of being in one or the other state at a future time can be evaluated using state-space analysis. In reliability, the failure probability and the probability of being returned to an available state are the variables of interest. Markov analysis is a state-space analysis technique which can be used for this analysis.

3.3.2.4 A Stochastic Model

A stochastic model is a tool for estimating probability distributions of potential outcomes by allowing for random variation in one or more inputs over time. The random variation is usually based on fluctuations observed in historical data for a selected period using standard time-series technique.

3.3.3 Management of system ram analysis

3.3.3.1 Applicability

Since System RAM Analysis can be time-consuming. It should be judiciously applied and should never be included in project plans indiscriminately. Since it is used to analyse systems, it is generally only applicable to evaluate complex systems. Simple systems (e.g. series systems) can be analysed using simple deterministic calculations.

3.3.3.2 Timing

Execution of System RAM Analysis early in the development process is essential to achieve the potential benefits from the process, e.g. to prevent costly redesigns at later stages. Therefore, it is strongly recommended that System RAM Analysis should begin at the earliest conceptual stage.

3.3.3.3 Updates and configuration management

The System RAM Analysis should be updated during the different development stages as more detail design information becomes available and should also be updated during the operations and maintenance stages, whenever design or operating changes are implemented.

System RAM Analysis results, including source data and simulation software application version used, should be put under configuration management for future use and updating, when required.

3.3.3.4 Sub-contractors

Execution of System RAM Analysis by Eskom sub-contractors should be carefully managed to ensure:

- Compliance with this System RAM Analysis guideline;
- Achievement of expected results; and
- Consistency of results between different sub-contractors.

These objectives can be supported by application-specific training, facilitation during initial analysis execution (including definition of ground rules), monitoring of the process during analysis execution, provision of simulation model example, mandatory use of specific software application, etc. Close cooperation of sub-contractors is essential to ensure successful integration of individual analyses (if required).

4. AUTHORISATION

This document has been seen and accepted by:

Name	Designation
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 for Authorisation and Publication
February 2019	2.1	G Fuhnwi	Final Draft Document after Review Process
February 2019	3	G 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 (Retired)