Eskom	Guideline	Technology

Title: Failure Mode and Effects Analysis Guideline

Unique Identifier:	240-49230046
Alternative Reference Number:	N/A
Area of Applicability:	Engineering
Documentation Type:	Guideline
Revision:	1
Total Pages:	26
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: 6/3/2013

Governance

D Odendaal

TDAC Chairperson

Date: 4/3/2013

CONTENTS

Page

FIGURES

TABLES

1. INTRODUCTION

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. Since FMEA determines the severity of potential failure modes, it provides input to mitigating measures to reduce risk. It is, therefore, primarily applicable during system design and is, typically, performed as an important part of a comprehensive reliability or safety program plan.

2. SUPPORTING CLAUSES

2.1 SCOPE

This guideline describes the process of performing FMEA (Failure Mode and Effects Analysis) and FMECA (Failure Mode, Effects and Criticality Analysis).[1] It provides guidance on the principles of the analysis and the procedural steps necessary to perform an analysis. The guideline also includes an applicable example.

This document is primarily based on IEC 60812, *Analysis techniques for system reliability – Procedure for Failure Mode and Effects Analysis (FMEA)*, which should be consulted as an informative reference when more details are required.

2.1.1 Purpose

The purpose of this document is to provide guidance on the principles of FMEA and the procedural steps necessary to consistently perform effective FMEA's 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 60812, *Analysis techniques for system reliability – Procedure for failure mode and effects analysis (FMEA)*, 2nd edition, January 2006

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

[1] All general descriptions for FMEA also apply to FMECA, since FMECA is an extension of FMEA.

[4] IEC 61025, *Fault tree analysis (FTA),* 2nd edition, December 2006

[5] IEC 61078, *Analysis techniques for dependability – Reliability block diagram method.*

[6] IEC 61882, *Hazard and operability studies (HAZOP studies) – Application guide*, 1st edition, May 2001

[7] AS IEC 61165, *Application of Markov techniques, 2008*

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

[9] J. Mowbray, *Reliability-centered Maintenance*", 2nd edition, Industrial Press, 1997

[10] C.A. Ericson, *Hazard Analysis Techniques for System Safety*, Wiley, 2005

[11] J.B. Bowles, *Fundamentals of Failure Modes and Effects Analysis*, tutorial presented at 2012 Annual Reliability and Maintainability Symposium, USA.

[12] C.S. Carlson, *Lessons Learned for Effective FMEAs*, tutorial presented at 2012 Annual Reliability and Maintainability Symposium Tutorial, USA.

2.3 DEFINITIONS

A - Item

Any part, component, device, sub-system, functional unit, equipment or system that can be individually considered.

B - Failure

The termination of the ability of an item to perform a required function.

C - Failure Cause

The process or mechanism responsible for initiating the failure mode.

D - Failure Criticality

A combination of the severity of a failure effect and the probability of occurrence of that specific failure mode.

E - Failure Effect

The consequence of a failure mode in terms of the operation, function or status of the item.

F - Failure Mode

The manner in which an item fails.

G - Failure Probability of Occurrence

The expected probability (or frequency) of failure mode occurrence.

H - Failure Severity

An indication of significance of the effect of a failure mode on the item operation, item environment or item operator.

I - Fault[2]

The state of an item characterised by the inability to perform a required function, excluding the inability during preventive maintenance or other planned actions or due to lack of external resources.

J - System

A set of inter-related or interacting elements.

2.3.1 Disclosure Classification

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

2.4 ABBREVIATIONS

Abbreviation	Description
FMEA	Failure mode and effects analysis
FMECA	Failure mode, effects and criticality analysis
FTA	Fault tree analysis
HAZOP	Hazard and operability (study)
Prob	Probability (or frequency) of failure mode occurrence
RCM	Reliability-centred maintenance
Sev	(Failure mode) severity

2.5 ROLES AND RESPONSIBILITIES

Not Applicable.

2.6 PROCESS FOR MONITORING

Not Applicable.

2.7 RELATED/SUPPORTING DOCUMENTS

Not Applicable.

3. FMEA OVERVIEW

Failure Mode and Effects Analysis (FMEA) is a systematic procedure for the analysis of a system to identify potential failure modes, failure causes and subsequent failure effects on system performance.

[2] A fault is often the result of a failure of the item itself, may exist without prior failure.

FMECA (Failure Mode, Effects and Criticality Analysis) is an extension of FMEA 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 should be performed by a team of knowledgeable persons who are qualified to identify and assess the consequences of various failure modes. Typically, the process is facilitated by an experienced FMEA team leader (also known as an FMEA facilitator).

FMEA is applicable at various levels of system decomposition, from the highest system-level down to functional-level and even to individual part-level. The level of analysis should be determined prior to execution of the analysis and different levels may be used for a specific analysis (e.g. sub-systems with safety implications may require analysis at lower levels). Regardless of whether a functional or hardware FMEA is performed, the process uses inductive logic to analyse a system in a “bottom-up” approach.

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 FMEA may be cost-effective. FMEA is an iterative process that takes place concurrently with the design process.

FMEA identifies and analyses individual failure modes and their effects on the system. Each failure mode is treated as independent. FMEA is, therefore, unsuitable for consideration of dependent failures or failures resulting from a combination (or sequence) of events. To analyse these situations, other methods and techniques, such as Fault Tree Analysis or Markov Analysis, may be required.

FMEA should be tailored to meet both industry- and project-specific requirements. FMEA worksheets (e.g. FMEA software application) requiring specific entries should be tailored for the specific application. If severity levels of failure modes are defined, they may be defined differently for different systems or different system levels.

FMEA is useful to analyse a system (Design FMEA), to analyse a process (Process FMEA) and to analyse an operation (Operator FMEA). Although this guideline primarily refers to Design FMEA, the principles are similar for all types of analyses.

FMEA is frequently listed as one of the most powerful reliability (and safety) engineering tools used by many different industries.

3.1 FMEA OBJECTIVES

The primary objective of an FMEA is to identify reliability (and safety) critical failure modes. Since FMEA identifies (and rank) potential failure modes, it can be effectively used to:

a) Support the system design process in terms of reliability and safety (e.g. early detection of design deficiencies, redundancy considerations, component selection, design margins and part derating, failure avoidance, test requirements, etc.)

b) Support the system design process in terms of maintainability (e.g. design of built-in test equipment and failure indications, testability analysis, diagnostic flowcharts, etc.)

c) Support the system design process in terms of supportability (e.g. list of failure modes is primary input to supportability analysis process (including RCM process))

d) Support the technical risk management process (e.g. risk mitigation, product safety litigation, management focus on critical items, etc.)

3.2 FMEA PRINCIPLES

FMEA is a systematic procedure for the analysis of a system to identify potential failure modes, causes and subsequent effects on system performance. FMEA is, therefore, an analysis technique that answers questions such as:

a) What can fail?

b) How does it fail?

c) How frequently will it fail?

d) What are the effects of the failure?

e) What is the reliability (or safety) consequence of the failure?

Therefore, FMEA is performed by identifying potential failure modes and by documenting failure causes, failure effects, compensating provisions, failure severity (and failure probability (in the case of FMECA)). Typically, these data entries are captured in an FMEA software application (e.g. similar to worksheet). *Since FMEA should be tailored according to the purpose and objectives of the specific project, not all analyses will record the same information.* For example, some analyses may not include “failure cause”, while others may include additional information (e.g. “test method”). A typical FMEA may include the following:

a) Reference number

b) Function/item

c) Failure mode

d) Failure cause

e) Failure effects

f) Detection method

g) Compensating provisions

h) Severity

i) Probability of occurrence

j) Comments/recommendations

3.2.1 Reference number

All failure modes should have a unique reference number, typically derived from the system or functional breakdown structure. This number is used to provide traceability (e.g. criticality matrix reference, corrective action list, etc.).

3.2.2 Function / item

All failure modes relate to functions or hardware items on the system or functional breakdown structure and the names of these functions or items should be used on the worksheet.

3.2.3 Failure mode

Potential failure modes for the system (i.e. the manner in which an item fails) should be identified by the FMEA team. Conceptually, there are three types of failure modes:

a) Functional (where analysis is performed on functions (at any indenture level))

b) Hardware (where analysis is performed on hardware (at any indenture level))

c) Combination of both functional and hardware approaches

At a high functional level, almost all failure modes can be classified as one or more of the following:

a) Failure during operation

b) Failure to operate at a prescribed time

c) Failure to cease operation at a prescribed time

d) Premature operation

However, these general failure modes should be expanded into more specific failure modes applicable to the system under analysis. It is important to ensure that potential failure modes are not omitted for lack of data and that initial FMEA results are improved when more detailed design information becomes available. Although specific failure modes can be obtained from databases, typically, they are generated per analysis by a knowledgeable FMEA team.

Much of the duplicative work associated with FMEA can be eliminated by grouping failure modes into equivalence groups consisting of all the failure modes that exhibit identical consequences[3]. Thereafter, these “equivalent failure modes” may be analysed once only and referenced under a single reference number. Such a group is shown in Figure 1, where “A open input”, “A no output”, “B open”, “C open input” and “C no output” all have the same failure effects. It may, therefore, be analysed as a single equivalent failure mode.

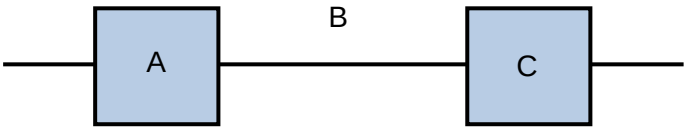

Figure 1: Equivalent failure modes

3.2.4 Failure causes

The most likely causes for each potential failure mode should be identified and described. Since a failure mode can have more than one cause, the most likely potential independent causes for each failure mode need to be identified and described. Failure cause is closely related to failure mechanism (i.e. what caused the failure mode to occur).

The identification and description of failure causes is not always necessary for all failure modes identified in the analysis. Identification and description of failure causes as well as suggestions for their mitigation should be done on the basis of the failure effects and their severity. The more severe the effects of failure modes, the more accurately identified and described the failure causes should be.

[3] The use of “equivalent failure modes” is not recommended if the FMEA is required as input to a supportability analysis.

Failure causes may be determined from analysis of field failures or failures in test units. When the design is new and without precedent, failure causes may be established by eliciting the opinion of experts.

Examples of general failure causes include the following:

a) Manufacturing defects
b) Wear-out or end-of-life (e.g. fatigue or corrosion)
c) Design weakness (e.g. insufficient design margins)
d) Environmental (e.g. lightning)
e) Inferior or faulty maintenance actions
f) Incorrect operation

Depending on the specific FMEA objectives, the description for failure cause is also occasionally used to simply identify lower-level failure modes. For example, for a transmission assembly consisting of both gearbox and electric motor, “gearbox failure” may be the cause of “transmission assembly failure”.

3.2.5 Failure effects

Failure effects are the consequence of a failure mode in terms of the operation, function or status of a system[4]. Failure effects can be described at different system indenture levels:

a) Local failure effect
b) Next higher-level failure effect
c) End failure effect (also known as system failure effect)

Most FMEA’s define failure effects at these three levels, however, two levels may be sufficient for some analyses (e.g. lower-level products).

“Local failure effect” refers to the effects of the failure mode on the system element under consideration (i.e. same indenture level). “Next higher-level failure effect” refers to the effect of the failure mode on the system element at a next higher-indenture level. “End failure effect” refers to the effect of the failure mode on the highest system level. When identifying end effects, the impact of a possible failure on the highest system level is defined and evaluated by the analysis of all intermediate levels. The end effect described may be the result of multiple failures.

Examples of general end failure effects include the following:

a) Total system failure
b) Degradation in system performance
c) Potential injury to personnel
d) No effect

[4]Although “failure effect” can generally be defined as the “consequence of a failure mode”, it should be noted that these terms are actually not the same. A failure effect describes “what happens when a failure mode occurs”, whereas a failure consequence answers the question “how does it matter?”

For an example of failure cause, failure mode and failure effects, refer to the reliability block diagram shown in Figure 1:

a) Failure mode: “B open”

b) Failure cause: “Corrosion”

c) Local failure effect: “No input to C”

d) End failure effect: “Total system failure”

Where computer-aided engineering software applications are used in the design process, these can normally be used to facilitate the determination of failure effects (especially for complex designs).

3.2.6 Detection method

For each failure mode, the FMEA team should determine if the failure mode can be detected by the operator or maintainer of the system. Failure detection methods may include the implementation of built-in-test equipment, the establishment of a special checkout procedure before system operation or by inspection during maintenance activities. It may be implemented at start-up of the system or continuously during operation or at prescribed intervals. Not all failure modes will have detection methods and some failure modes will be obvious to the operator or maintainer (e.g. visual).

3.2.7 Compensation provisions

Compensating provisions are any design features at a given system level or other provisions that have the ability to prevent or reduce the effect of the failure mode. The FMEA should, therefore, show the behaviour of such a feature in the presence of the specific failure mode. Other provisions against failure that need to be recorded in the FMEA include the following:

a) Redundant items that allow continued operation if one or more elements fail

b) Alternative means of operation

c) Monitoring or alarm devices

d) Any other means of permitting effective operation or limiting damage

3.2.8 Severity classification

Severity is an indication of the significance of the effect of a failure mode on item operation. The classification of severity is highly dependent on the specific system and is developed in consideration of several factors:

a) Nature of the system in relation to possible effects on users or environment resulting from failure

b) Functional performance of the system or process

c) Any contractual requirements imposed by the customer

d) Government or industry safety requirements

e) Requirements implied by a warranty

Table 1: Severity classification

Class	Severity	Consequence to persons, system or environment
1	Catastrophic	A failure mode which could potentially result in the failure of the system's primary functions and, therefore, cause serious damage to the system and its environment and/or personal injury. Descriptive keywords: System loss, injury or death.
2	Critical	A failure mode which could potentially result in the failure of the system's primary functions and, therefore, cause considerable damage to the system and its environment, but does not constitute a serious threat to life or injury. Descriptive keyword: Operation loss.
3	Marginal	A failure mode which could potentially degrade system performance function(s) without appreciable damage to the system or threat to life or injury. Descriptive keyword: Operation disruption.
4	Insignificant	A failure mode which could potentially degrade the system's functions but will cause no damage to the system and does not constitute a threat to life or injury. Descriptive keyword: Unscheduled maintenance.

3.2.9 Probability of occurrence

FMEA does not include probability of occurrence (and, therefore, also not criticality). FMECA, as an extension of FMEA, includes the probability of occurrence (or frequency) of each failure mode to determine the criticality of that failure mode. When using published information regarding probability of failure or expected failure rates, it is important to realise the limitations of published failure rate data. In particular, care should be taken to consider the operational profile (environmental, mechanical and/or electrical stresses applied) of each component that contributes to its probability of occurrence.

Probability of occurrence of the failure modes can be estimated from:

a) Failure data for similar items
b) Failure data from component life tests
c) Available databases of failure rates
d) Field failure data

e) Best engineering estimates

The probability of failure can be used in either a qualitative or quantitative FMECA.

A quantitative analysis requires information on failure rate per failure mode[5]. This is usually calculated using the expected failure rate for the item and the failure mode ratio, i.e. percentage of time an item is expected to fail in a specific failure mode. Quantitative analysis results in criticality numbers (also known as Risk Priority Numbers) which can be used to rank criticality.

A qualitative FMECA is based on relative estimates of probability of occurrence, with typical values for probability of occurrence shown in Table 2.

Table 2: Probability of occurrence

Class	Description	Probability of Occurrence
A	Frequent	$P \geq 20\%$
B	Probable	$10\% \leq P < 20\%$
C	Occasional	$1\% \leq P < 10\%$
D	Remote	$0.1\% \leq P < 1\%$
E	Improbable	$0 \leq P < 0.1\%$

The probabilities shown in Table 2 serve as example and may be used as default values or adjusted to satisfy specific project requirements. Experience has shown that these (or similar) probabilities, used as relative measures, provide for adequate criticality analysis. It is, therefore, usually not worthwhile to attempt accurate quantification of individual probabilities. Failure mode probability, based on best available knowledge or engineering estimates, is usually sufficient for an effective analysis. However, more detailed analysis may be required for failure modes with higher risk implications, e.g. safety.

3.2.10 Comments

It is recommended that the analysis worksheet should make provision for recording of comments per failure mode (where applicable). These comments or remarks should be entered by either the FMEA team or subsequent user of the analysis, e.g. systems engineer or project manager. Comments are also useful to document decisions on corrective actions.

[5] Quantitative FMECA is not recommended for typical Eskom projects.

3.3 FMEA PROCESS

The FMEA process consists of the following four basic steps:

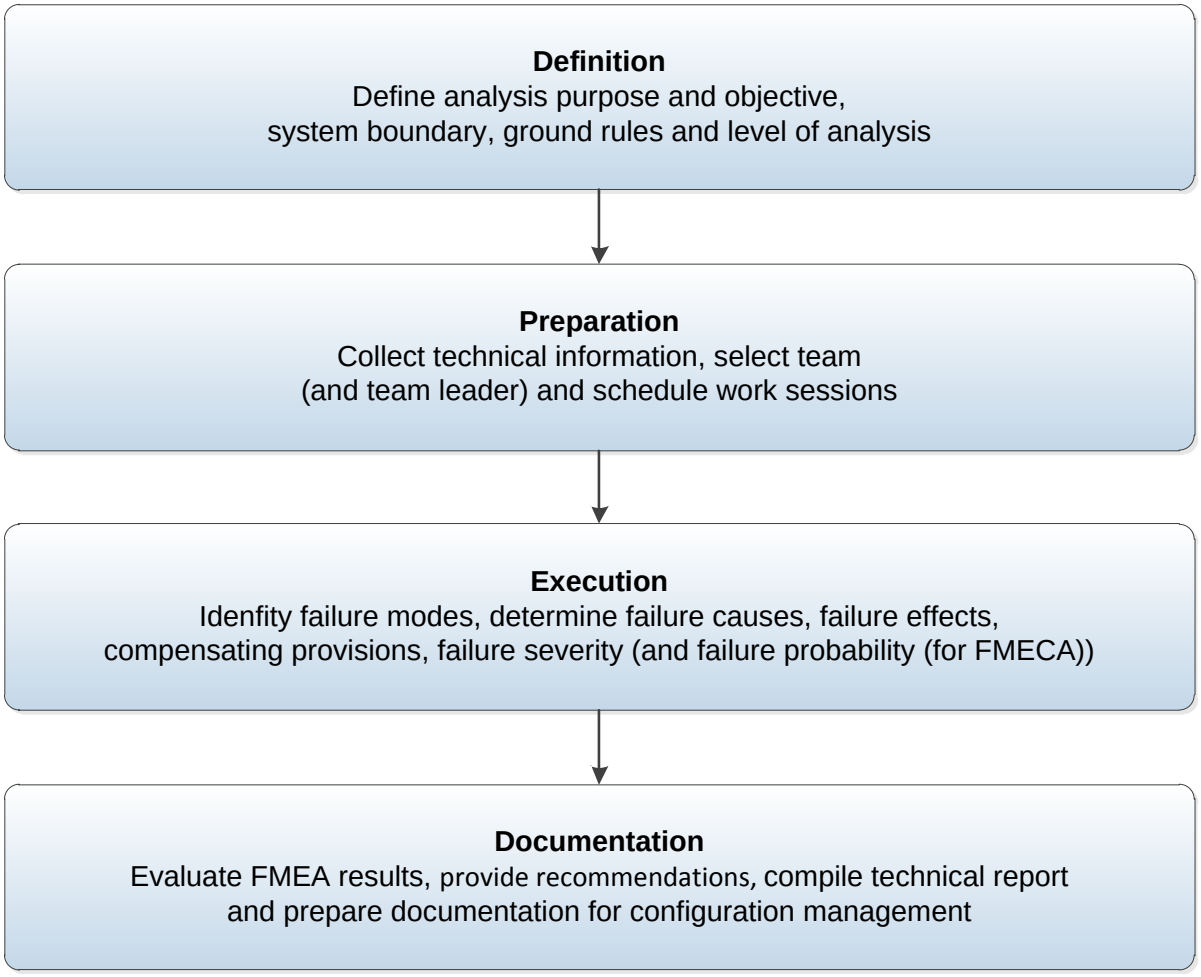

Figure 2: FMEA basic steps

3.3.1 Definition

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

Typically, the requirement for performing FMEA 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 FMEA 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 ground rules may include, among others, analysis viewpoint and redundancy considerations. The analysis viewpoint will determine the severity classification used for the analysis. For example, an analysis performed from a reliability viewpoint will assign different severity levels to individual failure modes than an analysis performed from a safety viewpoint. It is also necessary to decide whether redundancy (if applicable) is considered in the analysis (since it will determine the end failure effects and, therefore, the severity of individual failure modes).

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).

FMEA on a complex system may be very extensive and time-consuming. The effort may be reduced if the system includes sub-systems which are identical or similar to those used in a previous design. The analysis should use information on those sub-systems, where possible. However, care should be taken to ensure that the previous analyses are valid for the new design, i.e. same environmental and use profiles.

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. It is the responsibility of the FMEA study leader to manage the challenges of detail. 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 failure and subsequent 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)

3.3.2 Preparation

Collect technical information, select team (and team leader) and schedule work sessions

Since FMEA should be performed by a team of knowledgeable persons during work sessions, adequate planning for the analysis is necessary. The FMEA team should consist of persons representing different disciplines, such as project management, systems engineering, design engineering, production or construction, operations, maintenance, etc. The composition of the team will have a major impact on the quality of the FMEA results, since the identification of unwanted failure effects can frequently be attributed to dynamic interaction between team members.

It should be emphasised that the FMEA team should consist of knowledgeable persons. It is essential that they have sufficient technical knowledge of and experience with the (or similar) systems to both identify potential failure modes and to determine the consequences of those identified failure modes.

Furthermore, a prerequisite for effective FMEA is a sound knowledge of the principles of FMEA. Therefore, adequate training of the FMEA team is necessary, not only to ensure that everybody understands the FMEA process, but also to ensure that the team can avoid typical FMEA mistakes.

Typically, the FMEA process is facilitated by an experienced FMEA team leader, also known as an FMEA facilitator. The team leader should not only be experienced in the FMEA process but should also be trained in facilitation techniques and should also be able to manage different personalities of team members. Furthermore, the team leader should also have the ability to motivate all members to contribute to the process, e.g. a design engineer may be reluctant to discuss failure modes relating to his design.

All relevant technical information on the system should be collected prior to the work sessions, 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. reliability block diagram indicating series and parallel blocks)

d) Environmental and use profiles

e) Operating procedures

f) Test and evaluation results (if available)

g) Reliability and safety data on similar items

h) Other analysis results (e.g. HAZOP studies (if available))

It is recommended that the FMEA is performed during a number of work sessions, each focusing on a specific part of the analysis (e.g. analyse one sub-system at a time). The duration of the individual work sessions should be limited to a maximum of a few hours, due to the tedious nature of the analysis. An analysis performed uninterrupted for a long period of time (e.g. whole day) will prove to be very ineffective and will have a negative impact on the motivation of the FMEA team.

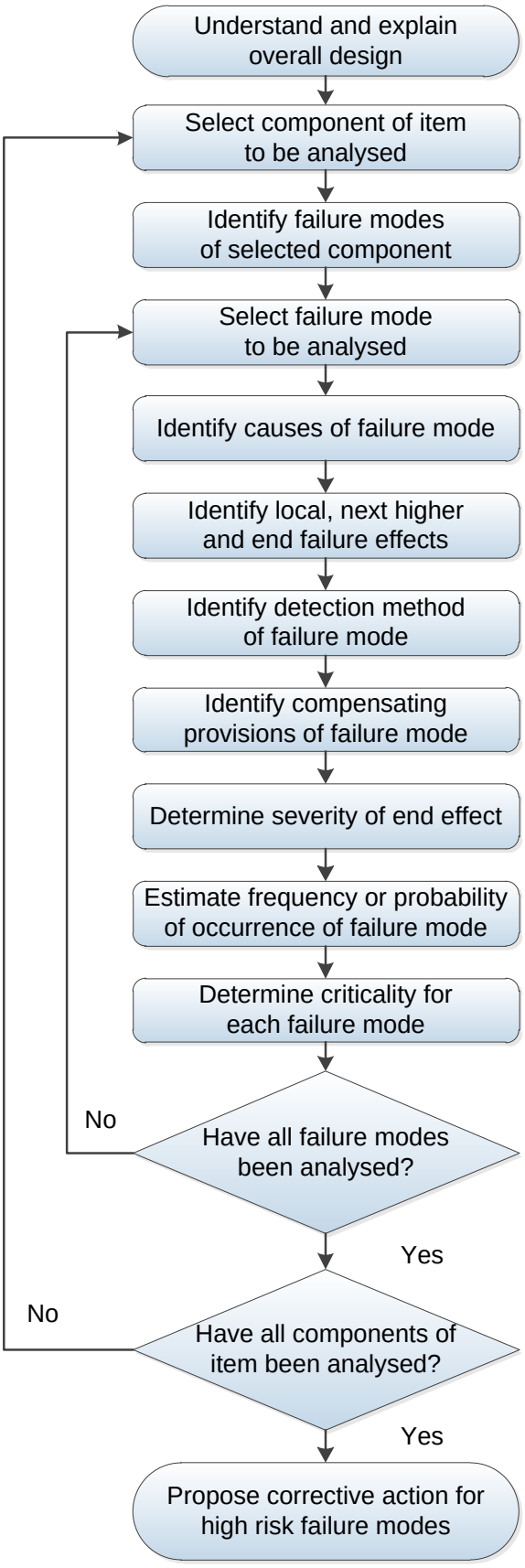

Figure 3: FMEA execution sequence diagram

3.3.3 Execution

Identify failure modes, determine failure causes, failure effects, compensating provisions, failure severity (and, in the case of FMECA, failure probability)

FMEA is executed by identifying potential failure modes and by documenting failure causes, failure effects, compensating provisions, failure severity (and, in the case of FMECA, failure probability). These data entries are captured in an FMEA software application (e.g. worksheet type application). Appendix A shows a typical FMEA worksheet.

FMEA execution starts with the identification of failure modes for a given item (chosen based on the level of analysis required). Generally, it is easier to identify a number of failure modes relating to the specific item and then to determine the failure causes, failure effects, etc. However, some FMEA teams may prefer to complete all entries, per failure mode, and then move on to the next failure mode. Since this is a matter of preference, the end results should be the same.

It is seldom possible to complete all entries immediately and the team will, invariably, have to re-visit some entries at a later stage, e.g. further detail information may be required to understand some failure effects. FMEA frequently becomes a highly-iterative process.

Although useful analysis can be performed using a worksheet software application, it is not recommended. Among other useful features, FMEA software applications can prevent the use of different phrases with the same meaning. For example, ‘failure of system’ and ‘system failure’ are the same failure effect, although, the use of two different phrases will impede further analysis of the FMEA results.

Depending on individual personalities, design engineers may be reluctant to contribute to the identification of potential failure modes. A possible solution to this problem is to change the negative question of “how can it fail?” into a positive question, such as “what can you do to make it fail?”. The response to the latter question is usually sufficient to generate a number of potential failure modes.

3.3.4 Documentation

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

A Criticality Matrix should be compiled to show the results of a qualitative FMEA, in a graphical format, as shown in Figure 4. It is evident that criticality increases with higher probability of occurrence and higher severity levels.

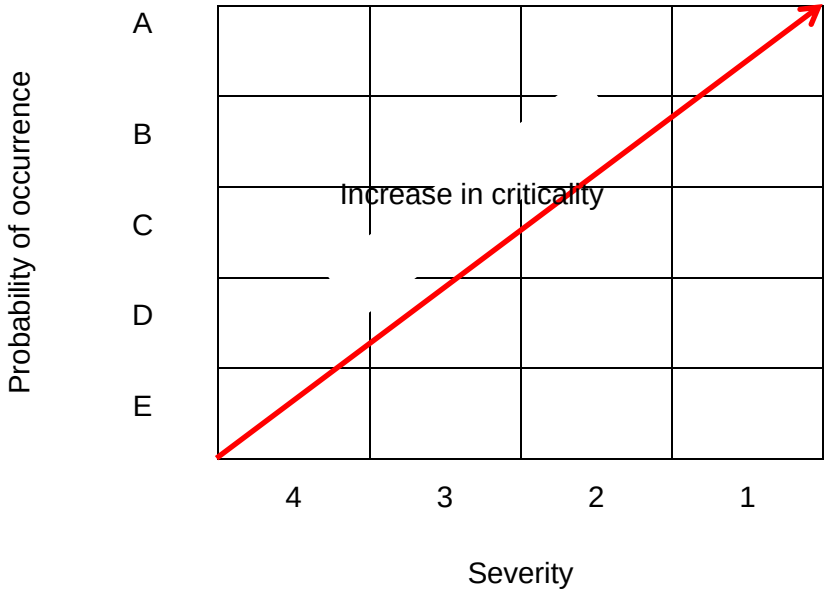

Figure 4: Criticality Matrix

There are many risk matrices in existence but the most appropriate one for a given analysis depends on the particular application[6]*.* Therefore, risk should be managed within its context. Some companies assign descriptions, such as “unacceptable”, “undesirable” and “acceptable” to sections of the Criticality Matrix. This practice can easily result in inferior engineering decisions and is, therefore, not recommended. The results of the analysis (i.e. individual failure mode criticalities) should rather be evaluated by persons to whom specific responsibilities are assigned (e.g. system engineer, project manager, etc.) in relation to all project-specific risks.

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

The FMEA 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) Criticality matrix
f) Recommendations
g) Detailed worksheets (e.g. Annexure)

3.4 GENERAL ASPECTS

3.4.1 Limitations of FMEA

FMEA may be difficult and tedious for complex systems with multiple functions, multiple operating modes and different repair and maintenance policies.

Difficulties and errors may occur when FMEA attempts to analyse several levels in a hierarchical structure (especially if redundancy is considered). Therefore, it is preferable for an FMEA to be restricted to two or three hierarchical levels. *More specifically, care should be taken not to "hide" a failure mode with high criticality value by developing it into two (or more) lower-level failure modes, each having a lower criticality value.*

Relationships between individual failure modes cannot be effectively presented in FMEA, since FMEA assumes independency of failure modes. This deficiency becomes even more pronounced for software/hardware interactions and human interactions (i.e. combinations of failure modes should rather be analysed using Fault Tree Analysis (FTA)).

FMEA does not adequately identify common-cause failures, i.e. single failures that will cause failure in multiple elements of a system. In fault-tolerant systems, common-cause failures are, therefore, rarely identified by FMEA since they require more than one component failure.

When FMEA is performed on complex systems, failure effects (and severity) often depend on functionality of embedded software. Unless the analysis team includes a person with substantial knowledge on system software, determination of failure effects will be difficult or impossible.

Generally, FMEA is not recommended for the analysis of software. However, FMEA on software may be used when a functional approach is taken, especially when the analysis focuses on interfaces between functions.

FMEA has limitations when human errors are analysed, especially since many system failures can be contributed to human errors in combination with other failure modes. Also, operational and maintenance failures are likely to be missed during the FMEA unless the FMEA team is skilled in human reliability analysis and recognises component failure modes due to human interaction.

3.4.2 Relationship with other analyses

3.4.2.1 Fault Tree Analysis

The relationship between FMEA and FTA should be well understood to select the applicable approach for the system under consideration. As shown in Figure 5, 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. 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. FTA not only shows the interdependency between faults (i.e. system failure logic), but can also be used to quantify the probability of top event occurrence.

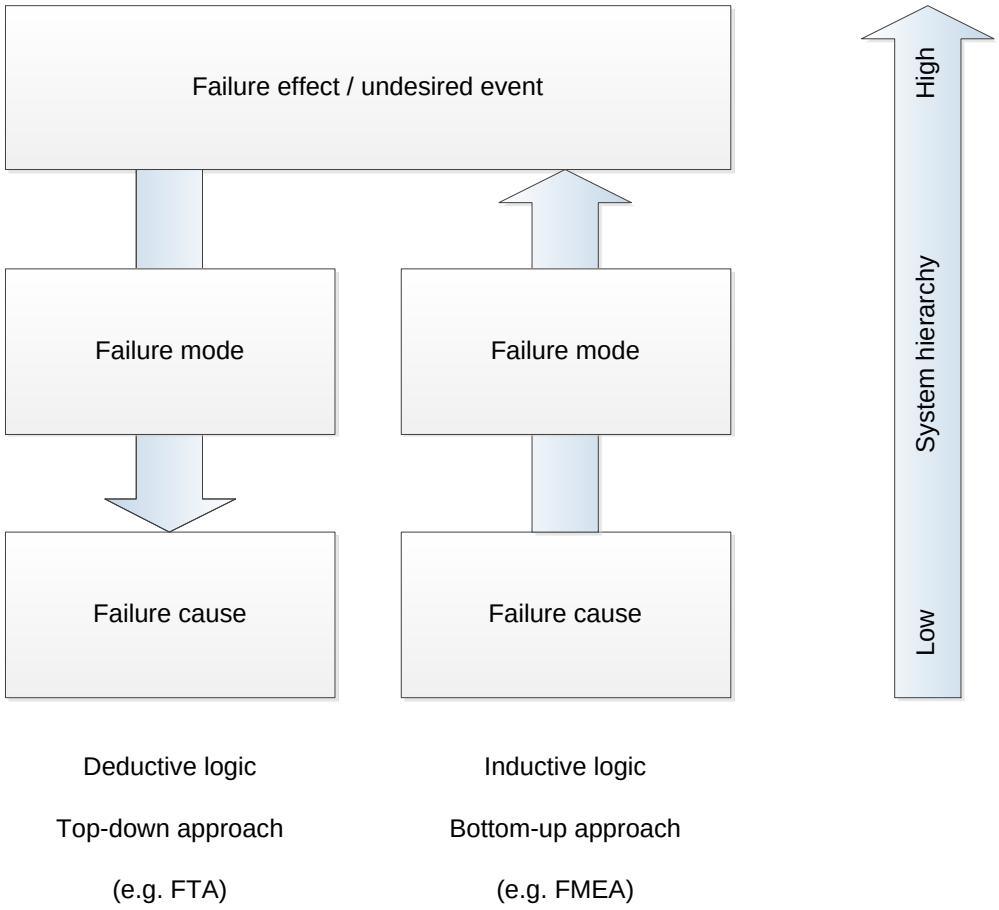

Figure 5: Deductive vs. inductive logic

Therefore, FMEA and FTA complement each other and both analyses are frequently required for a specific project. The following general guidelines may be useful to select between FMEA and FTA when only one analysis is to be performed:

Consider FMEA:

- When knowledge of system behaviour is limited;
- When system consists primarily of series configurations;
- When comprehensive knowledge of the failure modes is required;
- When analysing lower-level sub-systems and assemblies;
- To identify unacceptable effects of failures; and
- To analyse new designs when failure characteristics are unknown.

Consider FTA:

- When failure of system can have safety issues;
- When multiple failure modes in combination can lead to system failure;
- When calculation of probability of top event occurrence is required;
- When system contains of several parallel configurations (i.e. redundancy); and
- When diagnostic flowcharts are required.

3.4.2.2 Reliability-Centred Maintenance

Reliability-Centred Maintenance (RCM) is a process used to determine the maintenance requirements of a physical asset in its operating context. Typically, RCM implements a process where the following is considered:

- What are the functions of the asset in its operating concept?
- How can it fail to fulfil these functions?
- What causes each functional failure?
- What happens when each failure occurs?
- In what way does each failure matter?
- What can be done to prevent each failure? and
- What should be done if a suitable preventive task cannot be found?

It is evident that RCM includes an FMEA process, where failure modes are identified and the effects, thereof, determined. RCM also considers specific aspects, such as hidden failures, impact of failure on the environment, impact of failure on the safety of personnel, impact of failure on the operational capability, etc.

3.4.2.3 HAZOP studies

FMEA and HAZOP studies are both systematic inductive analysis methods, with many similarities. FMEA starts with identification of potential failure modes and then determines the possible causes and failure effects at higher system levels. HAZOP starts with identification of potential deviations from the design intent and then determines the possible causes and consequences at higher system levels (including operations). Therefore, a major difference between the two analyses is the starting point of the analyses. FMEA defines a failure mode as “the manner in which an item fails”, while HAZOP specifically focuses on deviations which are defined as “departures from the design intent”. Another difference is that HAZOP is always performed from a safety viewpoint, while FMEA may or may not be performed from a safety viewpoint.

3.4.2.4 Supportability analysis

An output of FMEA is a complete list of potential failure modes, which is an input to a supportability analysis. A design FMEA will frequently show lower-level failure modes, e.g. part level, while the supportability analysis may only require failure modes at a higher–level, e.g. level at which maintenance will be performed. In theory, a design FMEA can be used to initiate a supportability analysis (by using the failure mode list, although at a higher system level).

3.4.3 Management of FMEA

3.4.3.1 Applicability

Since FMEA can be very time-consuming and inefficient, it should be judiciously applied and should never be included in project plans indiscriminately.

3.4.3.2 Timing

Execution of FMEA 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 FMEA should begin at the earliest conceptual stage.

3.4.3.3 Updates and configuration management

The FMEA 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.

FMEA results, including source data and FMEA software application version used, should be put under configuration management for future use and updating, when required. Configuration management of all relevant documents is of utmost importance since FMEA results may be required for litigation purposes.

3.4.3.4 Sub-contractors

Execution of FMEA by Eskom sub-contractors should be carefully managed to ensure:

- Compliance with this FMEA 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 FMEA execution (including definition of ground rules), monitoring of the process during FMEA execution, provision of FMEA example, mandatory use of specific software application, etc. Close cooperation of sub-contractors is essential to ensure successful integration of individual analyses (if required).

3.4.3.5 Best practice FMEA process

Without a documented FMEA process, actual results will be dependent on individual personalities and results will vary from project to project. Therefore, a company-specific “best practice” FMEA process is necessary.

3.4.3.6 Criticality reduction

Failure modes with unacceptable criticality values should be considered for reduction of either failure mode probability of occurrence or failure mode severity. Failure mode probability of occurrence can be reduced by using one or more failure avoidance methods, e.g. selection of higher quality part, and failure mode severity can be reduced by using one or more risk mitigation methods, e.g. use of redundancy.

3.4.3.7 Combination of lower-level FMEA’s

Individual FMEA’s for items on the same hierarchical level and performed using the same ground rules can, in theory, be combined into one larger analysis. However, whenever complex systems are designed by several sub-contractors, the individual FMEA’s cannot be integrated into a higher-level system FMEA. The primary reason is that system-level information (e.g. end effect, severity, redundancy, etc.) is generally not available to lower-level sub-contractors. Integration of lower-level FMEA’s into a higher-level system FMEA is, therefore, not feasible and should not be performed.

3.4.3.8 Quality objectives

Typical FMEA mistakes made by design teams have been researched and published in available literature. These mistakes were analysed to define the following FMEA quality objectives which may be used to measure the effectiveness of an analysis:

- The FMEA drives system design or process improvements as the primary objective;
- The FMEA addresses all high-risk failure modes with effective and executable action plans;
- The design verification plan considers failure modes from the FMEA;
- The FMEA scope includes integration and interface failure modes in both block diagrams and analysis;
- The FMEA consider all major “lessons learned” as input for failure mode identification;
- The FMEA is completed during the “window of opportunity”, where it can most effectively impact the system or process design;
- The right people participate in the FMEA team throughout the analysis and are adequately trained in the process;
- The FMEA document is complete, including “corrective actions” and final risk assessment; and
- The time spent by the FMEA team is an effective and efficient use of time with value-added result.

4. AUTHORISATION

This document has been seen and accepted by:

Name	Designation
	Document Approved by TDAC ROD on 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
- E Pininski, Eskom, pininse@eskom.co.za

7. ACKNOWLEDGEMENTS

Not applicable.

APPENDIX A:

A.1 EXAMPLE: FMECA WORKSHEET

The following imaginary example should be replaced with a relevant Eskom example using the selected software application.

Ref	Function / item	Failure mode	Failure cause	Failure effects			Detection method	Compensating provisions	Sev	Prob	Comments / recommendation
				Local	Next higher	End					
1.1	Pressure sensor, number XYZ	No output	Mechanical or electrical damage	No pressure input to analogue-to-digital converter of control system	Control system inhibits start-up sequence	No effect	Control system start-up test function	Visual alarm on operator console	2	D	None
1.2	Pressure sensor, number XYZ	Out of range output	Electrical damage	Out of range pressure input to analogue-to-digital converter of control system	Control system initiates shutdown sequence	Over-pressure of vessel possible	Control system continuous test function	Visual and audible alarm on operator console	2	E	Dual redundant safety relief valves
1.3	Pressure sensor, number XYZ	Inaccurate output	Electrical damage	Inaccurate pressure input to analogue-to-digital converter of control system	Incorrect control of pressure system	Over or under-pressure of vessel possible	None	None	1	D	Periodic preventive maintenance (including sensor calibration)
etc.											