

Title: **Hazard and Operability Analysis Guideline**

Unique Identifier: **240-49230111**

Alternative Reference Number: **N/A**

Area of Applicability: **Engineering**

Documentation Type: **Guideline**

Revision: **1**

Total Pages: **30**

APPROVED FOR AUTHORISATION



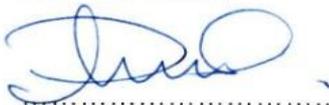
TECHNOLOGY ENGINEERING

DOCUMENT CENTRE ☎ x4962

Next Review Date: **April 2015**

Disclosure Classification: **CONTROLLED DISCLOSURE**

Process Owner

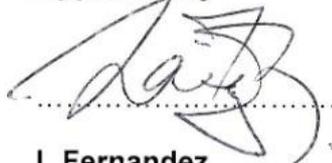


E Pininski

Chief Engineer: Systems Design (Reliability Engineering) (B2B Perform Design Analysis Process Owner)

Date: 27/11/2012

Approved by



L Fernandez

Senior Manager: Systems Integration (B2B Engineering Processes/System Lead

Date: 28/2/2013

Authorised by



D Odendaal

General Manager: Plant Engineering (B2B Engineering Tools Programme Lead)

Date: 4/3/2013

Governance



D Odendaal

TDAC Chairperson

Date: 4/3/2013

## CONTENTS

	Page
<b>1. INTRODUCTION</b> .....	<b>4</b>
<b>2. SUPPORTING CLAUSES</b> .....	<b>4</b>
2.1 SCOPE.....	4
2.1.1 Purpose.....	4
2.1.2 Applicability .....	4
2.2 NORMATIVE/INFORMATIVE REFERENCES .....	4
2.2.1 Normative.....	4
2.2.2 Informative .....	5
2.3 DEFINITIONS .....	5
2.3.1 Disclosure Classification .....	6
2.4 ABBREVIATIONS .....	6
2.5 ROLES AND RESPONSIBILITIES .....	6
2.6 PROCESS FOR MONITORING .....	6
2.7 RELATED/SUPPORTING DOCUMENTS .....	6
<b>3. HAZOP OVERVIEW</b> .....	<b>7</b>
3.1 HAZOP OBJECTIVES .....	7
3.2 HAZOP PRINCIPLES .....	8
3.2.1 Examination .....	8
3.2.2 Design representation.....	11
3.2.3 Design requirements and design intent .....	11
3.3 HAZOP PROCESS .....	12
3.3.1 Definition .....	13
3.3.2 Preparation .....	14
3.3.3 Execution .....	16
3.3.4 Documentation.....	18
3.4 GENERAL ASPECTS .....	20
3.4.1 Limitations of HAZOP .....	20
3.4.2 Relationship with other analyses .....	20
3.4.3 Hazard identification analyses during different system life-cycle stages .....	21
3.4.4 Audit.....	22
<b>4. AUTHORISATION</b> .....	<b>23</b>
<b>5. REVISIONS</b> .....	<b>23</b>
<b>6. DEVELOPMENT TEAM</b> .....	<b>23</b>
<b>7. ACKNOWLEDGEMENTS</b> .....	<b>23</b>
A.1 EXAMPLE GUIDE WORDS .....	24
A.2 HAZOP WORKSHEET .....	30

## FIGURES

<b>Figure 1: HAZOP analysis basic steps</b> .....	<b>12</b>
Figure 2: Flow chart of HAZOP execution procedure .....	17
Figure 3: Example of risk matrix.....	19

### CONTROLLED DISCLOSURE

When downloaded from the EDMS, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorised version on the system.

**TABLES**

Table 1: Examples of process / system parameters ..... 8  
Table 2: Examples of deviations and their meanings ..... 9  
Table 3: Guide word / element (or parameter) associations ..... 10  
Table 4: Severity and probability of occurrence classification ..... 19

**CONTROLLED DISCLOSURE**

When downloaded from the EDMS, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorised version on the system.

## 1. INTRODUCTION

Hazard and Operability 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).

## 2. SUPPORTING CLAUSES

### 2.1 SCOPE

This guideline describes the process of performing a HAZOP analysis. It provides guidance on HAZOP principles, the HAZOP process and the application of HAZOP during the different system life-cycle stages. The guideline also includes typical HAZOP guide words and a worksheet as an example.

This document is based on IEC 61822, *Hazard and Operability Studies (HAZOP Studies) – Application Guide*, which should be consulted as the primary informative reference when additional details are required. The typical guide words are based on the *Hazard and Operability Study Manual* published by Integrated Safety-Health-Environment Consultants.

#### 2.1.1 Purpose

The purpose of this document is to provide guidance on the principles of HAZOP analysis and the procedural steps necessary to consistently perform effective HAZOP 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*.

### CONTROLLED DISCLOSURE

When downloaded from the EDMS, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorised version on the system.

### 2.2.2 Informative

- [1] IEC 61882, *Hazard and operability studies (HAZOP studies) – Application guide*, 1<sup>st</sup> edition, May 2001
- [2] IEC 60812, *Analysis techniques for system reliability – Procedure for failure mode and effects analysis (FMEA)*, 2<sup>nd</sup> edition, January 2006
- [3] IEC 60300-3-9, *Dependability management – Part 3: Application guide – Section 9: Risk analysis of technological systems*, 1st edition, December 1995
- [4] IEC 61025, *Fault tree analysis (FTA)*, 2<sup>nd</sup> edition, December 2006
- [5] AS IEC 61165, *Application of Markov techniques*, 2008
- [6] Integrated Safety-Health-Environment Consultants, *Hazard and Operability Study Manual*, 1991
- [7] P.D.T. O'Connor and A. Kleyner, *Practical Reliability Engineering*, 5<sup>th</sup> edition, John Wiley, 2012
- [8] C.A. Ericson, *Hazard Analysis Techniques for System Safety*, John Wiley, 2005

## 2.3 DEFINITIONS

### a. Design Intent

The designer's desired or specified range of behaviour for elements and parameters.

### b. Deviation

Departure from the design intent.

### c. Element<sup>1</sup>

A constituent of a part which serves to identify the part's essential features.

### d. Guide Word

A word or phrase which expresses and defines a specific type of deviation from an element.

### e. Harm

Physical injury or damage to the health of people or damage to property or the environment.

### f. Hazard

Potential source of harm.

### g. Parameter<sup>2</sup>

The qualitative or quantitative property of an element.

---

<sup>1</sup> The word 'node' has the same meaning as 'element', and is often used in some industries.

<sup>2</sup> Examples of parameters are pressure, temperature, voltage, etc.

**h. Part<sup>3</sup>**

A section of the system, which is the subject of immediate analysis.

**i. Risk**

A combination of the probability of occurrence of harm and the severity of that harm.

**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
FTA	Fault Tree Analysis
HAZOP	HAZard and OPerability (analysis)
PHA	Preliminary Hazard Analysis

**2.5 ROLES AND RESPONSIBILITIES**

Not Applicable.

**2.6 PROCESS FOR MONITORING**

Not Applicable.

**2.7 RELATED/SUPPORTING DOCUMENTS**

Not Applicable.

---

<sup>3</sup> A part may be physical (e.g. hardware) or logical (e.g. step in an operational sequence).

### 3. HAZOP OVERVIEW

HAZOP analysis is a detailed hazard and operability problem identification process, carried out by a multi-disciplinary team under the guidance of an analysis leader. HAZOP deals with the identification of potential deviations from the design intent, examination of their possible causes and assessment of their consequences. Key features of the HAZOP examination include the following:

- a) The examination systematically uses a series of guide words to identify potential deviations from the design intent.
- b) The examination is carried out under the guidance of a trained and experienced analysis leader.
- c) The examination relies on specialists from various disciplines with appropriate skills and experience.
- d) Solutions to identified problems are not a primary objective of the HAZOP examination (hazards identified by HAZOP for further investigation should be analysed in detail).

There are many different tools and techniques available for the identification of potential hazards and operability problems, such as checklists, failure mode and effects analysis (FMEA), fault tree analysis (FTA), HAZOP, etc. Before commencing a HAZOP analysis, it should be confirmed that it is the most appropriate technique to be used. In making this judgement, consideration should be given to the purpose of the analysis, legal and regulatory requirements, possible severity of any consequences, appropriate level of detail, availability of relevant data and resources, etc.

#### 3.1 HAZOP OBJECTIVES

The primary objective of HAZOP is to:

- a) Identify potential hazards (i.e. potential sources of harm) in a system.
- b) Identify potential operability problems with a system.

Since hazard refers to physical injury or damage to the health of people or damage to property or the environment, HAZOP not only relates to the system itself.

## 3.2 HAZOP PRINCIPLES

### 3.2.1 Examination

The basis of HAZOP is “guide word examination”, which is a search for deviations from the design intent. To facilitate the examination, a system is divided into parts in such a way that the design intent for each part can be adequately defined. A part may be physical (e.g. hardware) or logical (e.g. operational sequence). The size of the part chosen is likely to depend on the complexity of the system and the severity of the hazard.

The design intent for a given part of a system is expressed in terms of elements. Elements may be discrete steps or stages in a procedure, individual signals and equipment in a control system, equipment or components in a process, material involved, etc. Therefore, the choice of elements may depend upon the particular application. Elements can often be usefully defined further in terms of parameters which can be either quantitative or qualitative.

Examples of process/system parameters are shown in Table 1. The list is purely illustrative, as the words employed in an actual HAZOP analysis will depend upon the system being analysed. Note that some parameter words may not appear to be related to any reasonable interpretation of the design intent. For example, one may question the use of the word ‘corrode’ on the assumption that no one would intend that corrosion should occur. However, most systems are designed with a certain life-span in mind and implicit in the design intent is that corrosion should not occur or, if it is expected, it should not exceed a certain rate. An increased corrosion rate, in such circumstances, would be a deviation from the design intent.

**Table 1: Examples of process / system parameters**

Flow (gas, liquid)	Temperature
Pressure	Level
Separate (settle, filter, centrifuge)	Composition
Reaction	Mix
Reduce (grind, crush)	Absorb
Corrode	Erode
Isolate	Drain
Vent	Purge
Inspection, surveillance	Maintain
Viscosity	Shutdown
Instruments	Start-up
Corrosion	Erosion
Vibration	Shock
Software data flow	Density
Voltage	Current
Ageing	

### CONTROLLED DISCLOSURE

When downloaded from the EDMS, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorised version on the system.

The HAZOP team examines each element (and parameter, where relevant) for deviation from the design intent which can lead to undesirable consequences. The identification of deviations from the design intent is achieved by a questioning process using predetermined guide words. Adjectives (or guide words), such as *more*, *no*, *less*, etc. are combined with process- or system-conditions, such as *flow*, *pressure*, etc. A HAZOP analysis looks for hazards resulting from potential deviations in design intent. The objective of the guide word approach is to stimulate imaginative thinking, to focus the analysis and elicit ideas and discussion, thereby maximizing the chances of analysis completeness. Examples of guide words and their meanings are shown in Table 2.

**Table 2: Examples of deviations and their meanings**

Deviation type	Guide word	Example interpretation for process industry	Example interpretation for Programmable Electronic System
Negative	NO	No part of the intention is achieved, e.g. no flow	No data or control signal passed
Quantitative modification	MORE	A quantitative increase, e.g. higher temperature	Data is passed at a higher rate than intended
	LESS	A quantitative decrease e.g. lower temperature	Data is passed at a lower rate than intended
Qualitative modification	AS WELL AS	Impurities present Simultaneous execution of another operation/step	Some additional or spurious signal is present
	PART OF	Only a part of the intention is achieved, i.e. only part of an intended fluid transfer takes place	The data or control signals are incomplete
Substitution	REVERSE	Covers reverse flow in pipes and reverse chemical reactions	Normally not relevant
	OTHER THAN	A result other than the original intention is achieved, i.e. transfer of wrong material	The data or control signals are incorrect
Time	EARLY	Something happens early relative to clock time, e.g. cooling or filtration	The signals arrive too early with reference to clock time
	LATE	Something happens late relative to clock time, e.g. cooling or filtration	The signals arrive too late with reference to clock time
Order or sequence	BEFORE	Something happens too early in a sequence, e.g. mixing or heating	The signals arrive earlier than intended within a sequence
	AFTER	Something happens too late in a sequence, e.g. mixing or heating	The signals arrive later than intended within a sequence

**CONTROLLED DISCLOSURE**

Guide word/element (or parameter) associations may be listed, as shown in Table 3. To achieve comprehensive hazard identification, it is necessary that the elements and their associated parameters cover all relevant aspects of the design intent and guide words cover all deviations. Combinations without credible deviations should be indicated as such on the list. Combinations with credible deviations are examined in detail and recorded to an agreed format (i.e. referenced in the HAZOP worksheet).

**Table 3: Guide word / element (or parameter) associations**

Guide word / element (or parameter)	Element 1			Element 2			Element 3		
	No	Yes	Ref	No	Yes	Ref	No	Yes	Ref
No voltage	X								
High voltage		X	1						
Low voltage	X								
Voltage transients		X	2						
Intermittent voltage		X	3						

Appendix 0 contains examples of guide words applicable to continuous processes, batch processes, manual tasks (operations and maintenance), electrical systems and mechanical systems. These guide words are provided in this document for guidance only and the analysis leader remains responsible to determine, use and record guide words applicable to the specific project.

### 3.2.2 Design representation

An accurate and complete design representation of the system under analysis is a prerequisite to examination. A design representation is a descriptive model adequately describing the system under analysis, its parts and elements, and identifying their parameters. The representation may be of the physical design or of the logical design and it should be made clear what is represented.

The design representation should convey the function of each part and element in a qualitative or quantitative manner. It should also describe the interactions of the system with other systems, with its operator/user and, possibly, with the environment. The conformance of elements or parameters to their design intent determines the correctness of operations and, in some cases, the safety of the system.

The representation of the system consists of two basic parts:

- System requirements; and
- Physical and/or logical description of the design.

The resulting value of a HAZOP analysis depends on the completeness, adequacy and accuracy of the design representation, including the design intent. Therefore, care should be taken in preparation of the information package. If HAZOP is being conducted in the operational or disposal phase, care should be taken to ensure that any modifications are reflected in the design representation. Before starting the examination, the team should review this information package and, if necessary, have it revised.

### 3.2.3 Design requirements and design intent

The design requirements consist of qualitative and quantitative requirements which the system has to satisfy and provide the basis for development of system design and design intent. All reasonable use and misuse conditions, which are expected by the user, should be identified. Both the design requirements and resulting design intent have to meet customer expectations.

The designer should not only consider what the equipment should do, but also ensure that it will not fail under any unusual set of conditions or that it will not wear-out during the specified life-time.

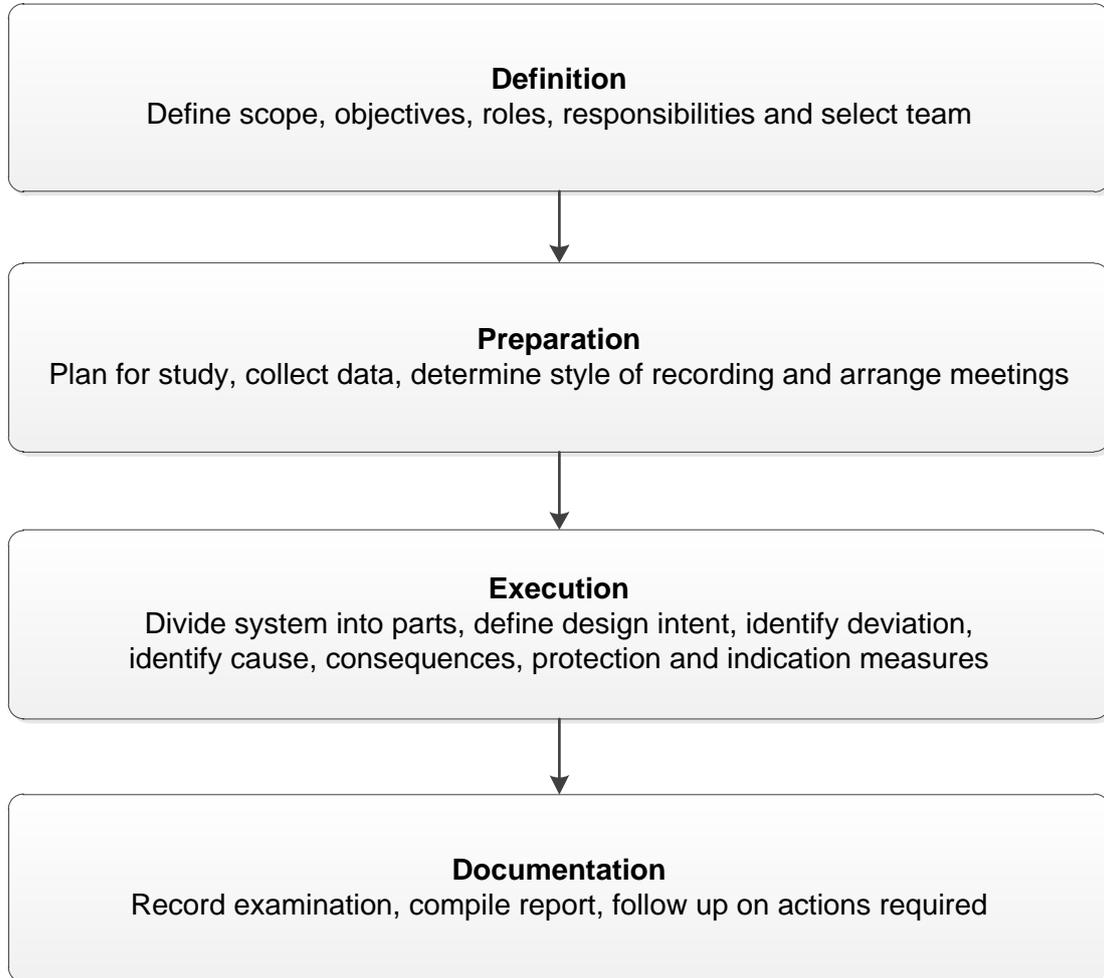
“Design intent“ should be correct and complete, as far as possible. In general, most documented design intents are limited to basic system functions and parameters under normal operating conditions. However, provisions for abnormal operating conditions and undesirable activities which may occur (e.g. severe vibrations, water hammer in pipes, voltage surges which may lead to failure) are rarely mentioned, but should be identified and considered during the examination. Furthermore, deterioration mechanisms, such as ageing, corrosion and erosion and other mechanisms which cause deterioration in material properties are not specifically stated. However, they have to be identified and considered in an analysis using appropriate guide words.

Expected life, reliability, maintainability and maintenance support should also be identified and considered together with hazards which may be encountered during maintenance activities, provided they are included in the scope of the HAZOP analysis.

## CONTROLLED DISCLOSURE

### 3.3 HAZOP PROCESS

HAZOP analysis consists of four basic sequential steps:



**Figure 1: HAZOP analysis basic steps**

### 3.3.1 Definition

#### Define scope, objectives, roles, responsibilities and select team

The scope of the HAZOP analysis will depend on a number of factors, including:

- a) Physical boundaries of system
- b) Number of design representatives available
- c) Level of design representatives available
- d) Scope of previous analyses (including HAZOP)
- e) Regulatory requirements

The following factors should be considered when defining objectives for the HAZOP analysis:

- a) Purpose for which results will be used
- b) Life-cycle stage of system
- c) Persons or property that may be at risk
- d) Potential operability problems
- e) Standards required of the system

A HAZOP analysis is a team effort, with each team member being chosen for a defined role. The team should be as small as possible, consistent with the relevant technical and operating skills and experience being available. Generally, this will involve at least four persons and rarely more than seven. Where a system has been designed by a contractor, the HAZOP team should contain personnel from both the contractor and the client.

Recommended roles for team members are as follows:

#### Analysis leader

- Not closely-associated with design team and project;
- Trained and experienced in leading HAZOP analyses;
- Responsible for communications between project management and HAZOP team;
- Plans analysis;
- Agrees to analysis team composition;
- Ensures analysis team is supplied with design representation package;
- Suggests guide words and guide word – element/parameter interpretations;
- Conducts/facilitates examination; and
- Ensures documentation of results.

#### Recorder

- Documents the proceedings of meetings; and
- Documents the hazards and problem areas identified, recommendations made and any actions for follow-up.

#### Designer

- Explains design and its representation; and
- Explains how a defined deviation can occur and corresponding system response.

**CONTROLLED DISCLOSURE**

**User**

- Explains operational context within which element under analysis will operate, operational consequences of deviation and extent to which deviations may be hazardous.

**Specialists**

- Provide expertise relevant to system and analysis; and
- May be called upon for limited participation.

**Maintainer**

- Provides maintenance information (when required).

**Operator**

- Provides operator information (when required).

The viewpoint of the designer and user is always required for the analysis. However, depending on the particular stage of the life-cycle in which the analysis is carried out, the type of specialists most appropriate for the analysis may vary. All team members should have sufficient knowledge of the HAZOP technique to enable them to participate effectively in the analysis or, at least, suitable introduction should be provided.

**3.3.2 Preparation****Plan for analysis, collect data, determine style of recording and arrange meetings**

The analysis leader is responsible for the preparation of an analysis plan that should contain the following:

- a) Objective and scope of analysis;
- b) List of participating members;
- c) Technical details:
  - Design representation divided into parts and elements (or parameters);
  - List of proposed guide words to be used; and
  - Interpretation of guide word/element (or parameters) combinations.
- d) List of appropriate references;
- e) Administrative arrangements;
- f) Form of recording required; and
- g) Templates that may be used in analysis.

The success of the HAZOP analysis firmly depends on the alertness and concentration of the team members and it is, therefore, important that the sessions are of limited duration and that there are appropriate intervals between sessions.

Typically, a design description may consist of some of the following documentation which should be clearly and uniquely identified, approved and dated:

- a) For all systems:
  - Design requirements and descriptions, flow sheets, functional block diagrams, control diagrams, electrical circuit diagrams, engineering data sheets, arrangement drawings, utilities specifications, operating and maintenance requirements.
- b) For process flow systems:
  - Piping and instrumentation diagrams, material specifications and standards equipment, piping and system layout.
- c) For programmable electronic systems:
  - Data flow diagrams, object-oriented design diagrams, state transition diagrams, timing diagrams, logic diagrams, etc.

In addition, the following information should be provided:

- a) boundaries of object of analysis and interfaces at these boundaries
- b) environmental conditions in which system will operate
- c) operating and maintenance personnel qualifications, skills and experience
- d) procedures and/or operating instructions
- e) operational and maintenance experience and known hazards with similar systems

In the planning stage of a HAZOP analysis, the analysis leader should propose an initial list of guide words to be used, and test the proposed guide words against the system and confirm their adequacy. The choice of guide words should be considered carefully, as a guide word which is too specific may limit ideas and discussion, and one which is too general may not focus the HAZOP analysis efficiently.

### 3.3.3 Execution

#### **Divide system into parts, define design intent, identify deviation, identify cause, consequences, protection and indication measures**

The analysis should follow the flow or sequence related to the subject of the analysis, tracing inputs to outputs in a logical sequence. Hazard identification techniques, such as HAZOP, derive their power from a disciplined step-by-step examination process. The sequence of examination is shown in Figure 2.

- a) The analysis leader explains the overall design to ensure that all team members have an adequate understanding of the design representation. The analysis leader selects a part of the design representation to be analysed. Thereafter, the design intent of that part is examined and the relevant elements and any parameters associated with these elements are identified.
- b) The analysis leader chooses an element and the first applicable guide word. Thereafter, the team examines the guide word interpretation in the context of the element to see if there is a credible deviation from the design intent. If a credible deviation is identified, it is examined for possible causes and consequences. In some applications, it is useful to categorise the deviations either in terms of the severity of the consequences or in terms of a relative risk-ranking based on the use of a risk matrix.
- c) The team should identify the presence of protection, detection and indication mechanisms for the deviation, which may be included within the selected part or form a portion of the design intentions of other parts. The presence of such mechanisms should not stop the potential hazard or operability problem being explored or listed or attempts being made to reduce the probability of its occurrence or mitigating its consequences.
- d) The analysis leader should summarise the results that are documented by the recorder. Where there is a need for additional follow-up work, the name of the person responsible for ensuring that the work is carried out should also be recorded.
- e) Thereafter, the process is repeated for any other interpretation of that guide word; then for another guide word, and then for each element of the part under analysis. After a part has been fully examined, it should be marked as completed. The process is repeated until all parts have been analysed.

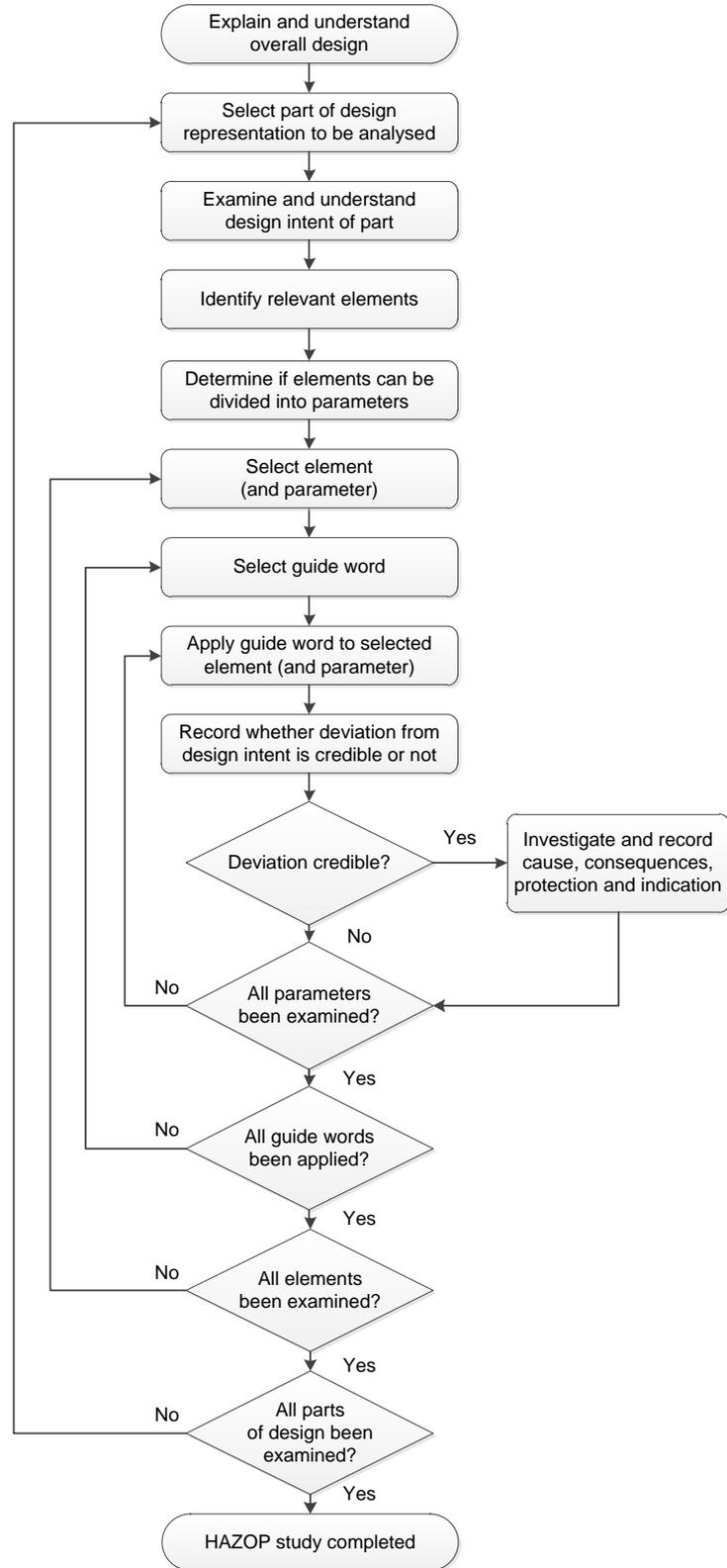


Figure 2: Flow chart of HAZOP execution procedure

**CONTROLLED DISCLOSURE**

When downloaded from the EDMS, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorised version on the system.

### 3.3.4 Documentation

#### Record examination, compile report, follow-up on actions required

The primary strength of HAZOP is that it presents a systematic, disciplined and documented approach. To achieve full benefits from a HAZOP analysis, it has to be properly documented and followed up. The analysis leader is responsible to ensure that suitable records are produced for each meeting.

Full recording of all results of applying each guide word/element combination to every part or element on the design representation is required. Although cumbersome, it provides the evidence that the analysis has been thorough and should satisfy the most stringent audit requirements.

HAZOP analyses are not aimed at redesigning a system nor is it usual for the analysis leader to have the authority to ensure that the analysis team's recommendations are acted upon.

Before any significant changes resulting from the findings of the HAZOP have been implemented, and once the revised documentation is available, the project manager should consider reconvening the HAZOP team to ensure that no new hazards or operability or maintenance problems have been introduced.

The output from a HAZOP analysis should include the following:

- a) Details of identified hazards and operability problems together with details of any provisions for their detection, and/or mitigation.
- b) Recommendations for any further analyses of specific aspects of the design using different techniques, if necessary.
- c) Actions required for addressing uncertainties discovered during the analysis.
- d) Recommendations for mitigation of the problems identified based on the team's knowledge of the system (if within the scope of the analysis).
- e) Notes which draw attention to particular points that need to be addressed in the operating and maintenance procedures.
- f) List of team members for each session.
- g) Guide word check lists.
- h) HAZOP worksheets.
- i) Risk matrix (if required).

Risk<sup>4</sup> can be defined as the combination of mishap severity and probability of occurrence. The severity and probability of occurrence classifications listed in Table 4 may be used for this purpose.

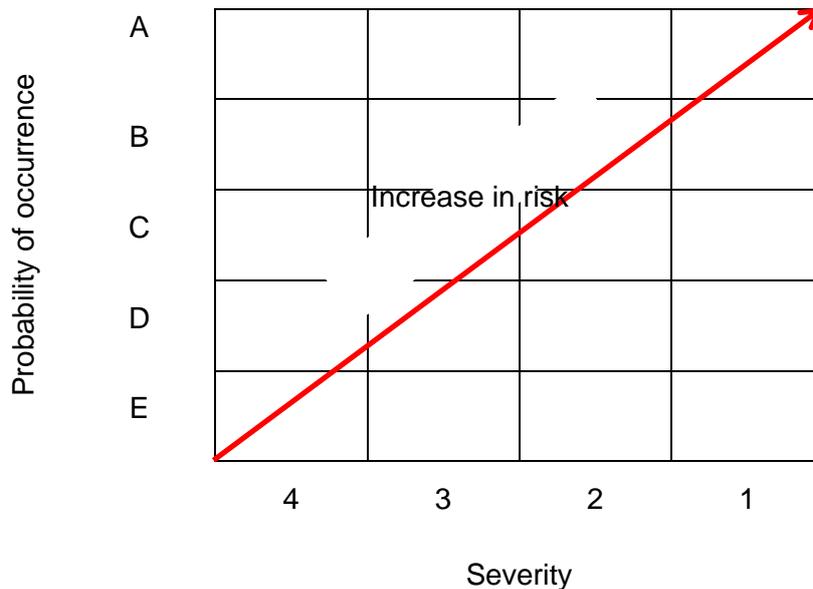
---

<sup>4</sup> Refer to *Failure Mode and Effects Analysis Guideline*, Eskom document number xyz for more information.

**Table 4: Severity and probability of occurrence classification**

Severity		Probability	
1	Catastrophic	A	Frequent
2	Critical	B	Probable
3	Marginal	C	Occasional
4	Negligible	D	Remote
		E	Improbable

A typical risk matrix may be compiled to show the results of the HAZOP in a graphical format, as shown in Figure 3. It is evident that risk increases with higher probability of occurrence and higher severity levels. *There are many risk matrices in existence but the most appropriate one for a given analysis depends on the particular application<sup>5</sup>. Therefore, risk should be managed in 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 (e.g. individual hazards) 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.*



**Figure 3: Example of risk matrix**

<sup>5</sup> IEC 60300-3-1, *Dependability management – Part 3-1: Application guide – Analysis techniques for dependability – Guide on methodology.*

### 3.4 GENERAL ASPECTS

#### 3.4.1 Limitations of HAZOP

HAZOP analyses have limitations that should be taken into account when considering a potential application:

- a) HAZOP is a hazard identification technique which considers system parts individually and methodically examines the effects of deviations on each part. Frequently, a serious hazard will involve the interaction between a number of parts of the system. In such cases, the hazard may need to be studied in more detail using techniques such as event tree and fault tree analyses.
- b) As with any technique for the identification of hazards or operability problems, there can be no guarantee that all hazards or operability problems will be identified in a HAZOP analysis. The analysis of a complex system should not, therefore, depend entirely upon HAZOP.
- c) Many systems are highly inter-linked and a deviation at one of them may have a cause elsewhere. Adequate local mitigating action may not address the real cause and still result in a subsequent mishap or accident.
- d) The success of a HAZOP analysis depends greatly on the ability and experience of the analysis leader and the knowledge, experience and interaction between team members.
- e) HAZOP only considers parts that appear on the design representation. Activities and operations which do not appear on the representation are not considered.

HAZOP is particularly useful for identifying weaknesses in systems (existing or proposed) involving the flow of materials, people or data, or a number of events or activities in a planned sequence or the procedures controlling such a sequence. As well as being a valuable tool in the design and development of new systems, HAZOP may also be profitably employed to examine hazards and potential problems associated with different operating states of a given system, e.g. start-up, standby, normal operation, normal shutdown and emergency shutdown.

#### 3.4.2 Relationship with other analyses

HAZOP may be used in conjunction with other analysis methods, such as FMEA and FTA. Such combinations may be utilised in situations when:

- a) The HAZOP analysis clearly indicates that the performance of a particular item of equipment is critical and needs to be examined in considerable depth (the HAZOP may then be usefully complemented by an FMEA of that item of equipment).
- b) Having examined single element/single parameter deviations by HAZOP, it can be decided to assess the effect of multiple deviations using FTA or to quantify the likelihood of the failures, again, using FTA.

FMEA and HAZOP analyses are both systematic inductive analysis methods, with many similarities. FMEA starts with identification of potential failure modes and, thereafter, determines the possible causes and the failure effects at higher system levels. HAZOP begins with identification of potential deviations from the design intent and then determines the possible causes and the consequences at higher system levels (including operations). Therefore, a major difference between the two analyses is the starting point of the analyses.

### CONTROLLED DISCLOSURE

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.

### 3.4.3 Hazard identification analyses during different system life-cycle stages

HAZOP analyses are most suitable in the later stages of detailed design, for examining operating facilities and when changes to existing facilities are made. However, HAZOP (and other methods of analysis) should be applied during all life-cycle stages of a system:

#### 1 Concept and definition stage

In this stage of a system’s life-cycle, the design concept and major system parts are decided, although the detailed design and documentation required to conduct the HAZOP do not exist. However, it is necessary to identify major hazards at this time to allow them to be considered in the design process and to facilitate future HAZOP analyses. To carry out these analyses, other methods, such as checklists, reviews of historical data, FMEA and FTA, may be used. Alternatively, a formal Preliminary Hazard Analysis may be performed.

Preliminary Hazard Analysis (PHA)<sup>6</sup> is an inductive method of analysis, in which, the objective is to identify the hazards, hazardous situations and events that can cause harm for a given activity, facility or system. Most commonly, it is carried out early in the development of a project when there is little information concerning design details or operating procedures and can often be a precursor to further analyses. It can also be useful when analysing existing systems or prioritising hazards where circumstances prevent a more extensive technique from being used. A PHA formulates a list of hazards and generic hazardous situations by considering parameters, such as:

- a) Materials used or produced.
- b) Equipment employed.
- c) Operating environment.
- d) Layout.
- e) Interfaces among system components
- f) Etc.

The method is completed with the identification of the possibilities that the accident happens, the qualitative evaluation of the extent of possible injury or damage to health that could result and the identification of possible remedial measures.

---

<sup>6</sup> IEC 60300-3-9, *Dependability management – Part 3: Application guide – Section 9: Risk analysis of technological systems*, 1st edition, December 1995

## 2 Design and development stage<sup>7</sup>

During this stage of a life-cycle, detailed design is developed, methods of operation are decided upon and documentation is prepared. The design reaches maturity and is frozen. The best time to carry out a HAZOP analysis is just before the design is frozen. At this stage, the design is sufficiently detailed to allow the questioning mechanism of a HAZOP to obtain meaningful answers. It is important to have a system that will assess the implications of any changes made after the HAZOP has been carried out. This system should be maintained throughout the life of the system.

## 3 Manufacturing and commissioning stage

It is advisable to carry out an analysis before the system is started up, if commissioning and operation of the system can be hazardous and proper operating sequences and instructions are critical or when there has been a substantial change of intent in a late stage. Additional data, such as commissioning and operating instructions should be available at this time. In addition, the analysis should also review all actions raised during earlier analyses to ensure that these have been resolved.

## 4 Operational stage

The application of HAZOP should be considered before implementing any changes that could affect the safety or operability of a system or have environmental effects. A procedure should also be put in place for periodic reviews of a system to counteract the effects of “creeping change”. It is important that the design documentation and operating instructions used in an analysis are up to date.

## 5 Decommissioning or disposal stage

An analysis of this stage may be required due to hazards that may not be present during normal operation. If records from previous analyses exist, this analysis can be carried out expeditiously. Records should be kept throughout the life of the system in order to ensure that the decommissioning issues can be dealt with expeditiously.

### 3.4.4 Audit

The program and results of HAZOP analyses may be subjected to internal company or regulatory authority audits. Criteria and issues which may be audited should be defined in the company's procedures. These may include: personnel, procedures, preparations, documentation and follow-up. A thorough check of technical aspects should also be included.

---

<sup>7</sup> The HAZOP process described in this document (e.g. Figure 2) refers primarily to the HAZOP analysis performed during the design and development stage.



## **A.1 EXAMPLE GUIDE WORDS**

The following checklists contain examples of guide word/deviations that may be used in the HAZOP analysis. The team leader should ensure that any other applicable guide word/deviations are also considered by the analysis team, recorded and analysed.

The example guide words are grouped under the following categories:

1. Continuous processes
2. Batch processes
3. Manual tasks (Operations and Maintenance)
4. Electrical systems
5. Mechanical systems





**3 MANUAL TASKS (OPERATIONS AND MAINTENANCE)**

Engineering drawing	(e.g. Drawing title, number, revision and date)								
Element identification	(e.g. Element #1)			(e.g. Element #2)			(e.g. Element #3)		
Guide word / element	Yes	No	Ref	Yes	No	Ref	Yes	No	Ref
Many operations									
Long haul / reach									
High rate / speed									
Late starting									
Increased energy									
High force / tension									
Heavy weight / load									
Few operations									
Short haul / reach									
Low rate / speed									
Early starting									
Decreased energy									
Low force / tension									
Light weight / load									
Stopped / interrupted									
Opposite direction									
Spillage while									
Impurities									
Inadequate conditions									
Partial completion									
Distortion									
Breakage									
Interference									
Loss of control									
System failure									
Human failure									
Distractions									
Repetitive actions									
Additional tasks									
Friction with									
Vibration with									
Wear of equipment									
Noise emission									
Toxic emission									
Heat radiation									
Nuclear radiation									
Wrong operation									
Other direction route									
Wrong material									
Instead maintenance									
Cleaning									
Checking									
Emergency									

**CONTROLLED DISCLOSURE**

When downloaded from the EDMS, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorised version on the system.

**4 ELECTRICAL SYSTEMS**

Engineering drawing	(e.g. Drawing title, number, revision and date)								
Element	(e.g. Element #1)			(e.g. Element #2)			(e.g. Element #3)		
Guide word / element	Yes	No	Ref	Yes	No	Ref	Yes	No	Ref
High voltage									
High current									
High power									
Leading power factor									
High frequency									
Increased temperature									
Surges / transients									
Low voltage									
Low current									
Low power									
Lagging power factor									
Low frequency									
Reduced temperature									
Slow response									
No current									
No voltage									
Spurious trips									
Reverse current									
Reverse polarity									
Stresses									
Shorting									
Distortion									
Breakage									
Interference									
Instrument failure									
Mechanical failure									
Service failure									
Human failure									
Arcing									
Burning									
Melting									
Wear/friction/impact									
Ingress of dust									
Noise emission									
Toxic emission									
Electromagnetic emission									
Loss of control									
Other direction/route									
Wrong unit									
Instead maintenance									
Checking									
Emergency									

**CONTROLLED DISCLOSURE**

When downloaded from the EDMS, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorised version on the system.

**4 MECHANICAL SYSTEMS**

Engineering drawing	(e.g. Drawing title, number, revision and date)								
Element	(e.g. Element #1)			(e.g. Element #2)			(e.g. Element #3)		
Guide word / element	Yes	No	Ref	Yes	No	Ref	Yes	No	Ref
High throughput / feed									
Long stroke / travel									
High rate / speed									
Increased temperature									
High tension / thrust									
High force / torque									
High pressure / load									
Low throughput / feed									
Short stroke / travel									
Low rate / speed									
Decreased temperature									
Low tension / thrust									
Low force / torque									
Low pressure / load									
Stoppage / interruption									
Opposite direction									
Backwards run									
Spillage while									
Loose rate									
Loose heat									
Gain rate									
Gain heat									
Incomplete execution									
Distortion									
Breakage									
Contaminate									
Interfere									
Failures while									
Expansion stress									
Contraction stress									
Vibration stress									
Depositing									
Built-up									
Wear with									
Pollution									
Emissions with									
Radiation with									
Loss of control									
Other direction route									
Wrong material									
Instead maintenance									
Checking									
Emergency									

**CONTROLLED DISCLOSURE**

When downloaded from the EDMS, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorised version on the system.

**A.2 HAZOP WORKSHEET**

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

Ref	Guide word / element (or parameter)	Cause	Consequence	Protection	Indication	Sev	Prob	Recommendation	Comments
1	High pressure	Pressure sensor faulty	Rupture of feeder pipes possible	Pressure relief valve installed	Pressure sensor analogue output monitored by control system continuous test function	2	C	Installation of dual redundant pressure sensor  Modification of control system to monitor out of range pressure measurements	Refer to Design Authority for implementation
2	High temperature	Temperature sensor faulty	Damage to feeder pipe connections possible	None	Temperature sensor analogue output monitored by control system continuous test function	2	D	Installation of dual redundant temperature sensor	Refer to Design Authority for implementation
etc.									

**CONTROLLED DISCLOSURE**

When downloaded from the EDMS, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorised version on the system.