| Eskom | Guide | Nuclear Engineering |
|---|---|---|

Title: **Guideline for Safety Issue Catergorisation**

| | |
|---|---|
| Document Identifier: | **331-64** |
| Alternative Reference Number: | **KGA-046** |
| Area of Applicability: | **Nuclear Engineering** |
| Functional Area: | **Nuclear Analysis and Siting** |
| Revision: | **4** |
| Total Pages: | **39** |
| Next Review Date: | **December 2024** |
| Disclosure Classification: | **Controlled Disclosure** |

| **Compiled by** | **Functional Responsibility** | **Authorized by** |
|---|---|---|
| pAV | LJ Mahlangu | |
| **P Vymers** | **L Mahlangu** | **I Sekoko** |
| **Physicist, DPSA** | **Manager, DPSA** | **Middle Manager, NAS** |
| Date: 2021-12-15 | Date: 2021-12-15 | Date: 2021-12-25 |

## Nuclear Additional Classification Information

| | |
|---|---|
| Business Level: | **3** |
| Working Document: | **4** |
| Importance Classification: | **SR (S12001)** |
| NNR Approval: | **No** |
| Safety Committee Approval: | **No** |
| ALARA Review: | **No** |
| Functional Control Area: | **Nuclear Analysis and Siting** |

## Content Page

1. Introduction ........ 4
2. Supporting Clauses ........ 4
    2.1 Scope ........ 4
        2.1.2 Purpose ........ 4
        2.1.3 Applicability ........ 4
        2.1.4 Effective date ........ 4
    2.2 Normative/Informative References ........ 4
        2.2.2 Normative ........ 4
        2.2.3 Informative ........ 4
    2.3 Definitions ........ 5
    2.4 Abbreviations ........ 5
    2.5 Roles and Responsibilities ........ 6
    2.6 Process for Monitoring ........ 6
    2.7 Related/Supporting Documents ........ 6
3. Content ........ 6
4. Acceptance ........ 7
5. Revisions ........ 8
6. Development Team ........ 9
7. Acknowledgements ........ 9
Appendix A: WORK FLOW MATRIX ........ 10
APPENDIX B: SAFETY SIGNIFICANCE CATEGORIES ........ 13
APPENDIX C: PSA PROCESS ........ 15
1. INTRODUCTION ........ 15
2. RISK LEVELS AND MEASURES ........ 15
3. APPROACH ........ 16
    3.1 CRITERIA FOR OVERALL PSA RESULTS ........ 16
    3.3 CRITERIA FOR TEMPORARY CHANGES ........ 21
Appendix D: PSA PROCESS FORM (331-103) ........ 25
Appendix E: DETERMINISTIC PROCESS ........ 27
Appendix F: DETERMINISTIC PROCESS Form (331-104) ........ 30
Appendix G: OPERATIONAL PROCESS ........ 34
Appendix H: OPERATIONAL PROCESS Form (331-105) ........ 39

## 1. Introduction

This document provides guidelines for the categorisation of safety issues within Nuclear Engineering.

## 2. Supporting Clauses

### 2.1 Scope

Applicable to the categorising of nuclear safety issues at Koeberg Nuclear Power Plant.

### 2.1.2 Purpose

To provide guidance for categorising nuclear safety issues using risk and safety concepts.

### 2.1.3 Applicability

This document shall apply throughout Nuclear Engineering.

### 2.1.4 Effective date

Please see date of authorization.

### 2.2 Normative/Informative References

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

### 2.2.2 Normative

[1] ISO 9001 Quality Management Systems

### 2.2.3 Informative

[2] IAEA Safety Series No. 110: The Safety of Nuclear Installations

[3] IAEA Safety Series No. 12, 1998: Evaluation of the Safety of Operating Nuclear Power Plants Built to Earlier Standards

[4] INSAG-3: Basic Safety Principles for Nuclear Power Plants

[5] INSAG-4: Safety Culture

[6] NUMARC 93-01: Industry Guideline for Monitoring the Effectiveness of Maintenance at Nuclear Power Plants

[7] RD-0014: Emergency Preparedness and Response Requirements for Nuclear Installations

[8] RD-0022: Radiation Dose Limitation at Koeberg Nuclear Power Station

[9] RD-0024: Requirements on Risk Assessment and Compliance with Principle Safety Criteria for Nuclear Installations

[10] RG 1.174: An Approach for Using Probabilistic Risk Assessment in Risk-Informed Decisions on Plant-Specific Changes to the Licensing Basis

[11] TR-105396: EPRI PSA Applications Guide

### 2.3 Definitions

**2.3.1 Diversity:** the existence of redundant components or systems to perform an identified function, where such components or systems collectively incorporate one or more different attributes to achieve that function.

**2.3.2 Principal Safety Function:** a function to prevent the accident from occurring, or to protect the barriers, and can be related to the reliability of the system.

**2.3.3 Redundancy:** provision for more than the minimum number of elements or systems, such that the worst single failure does not result in the loss of the required safety function. Redundancy: provision for more than the minimum number of elements or systems, such that the worst single failure does not result in the loss of the required safety function.

### 2.4 Abbreviations

| Abbreviation | Explanation |
|---|---|
| **CDF** | Core Damage Frequency |
| **CDP** | Core Damage Probability |
| **EPRI** | Electric Power Research Institute |
| **FDF** | Fuel Damage Frequency (in the spent fuel pool) |
| **FDP** | Fuel Damage Probability (in the spent fuel pool) |
| **IAEA** | International Atomic Energy Agency |
| **INPO** | Institute of Nuclear Power Operators |
| **ETMM** | Engineering Technical Management Meeting |
| **LERF** | Large Early Release Frequency |
| **LERP** | Large Early Release Probability |
| **NNR** | National Nuclear Regulator |
| **NUMARC** | Nuclear Management and Resources Council |
| **PSA** | Probabilistic Safety Assessment |
| **QRA** | Qualitative Risk Assessment |
| **SFP** | Spent Fuel Pool |
| **UK HSE** | United Kingdom Health and Safety Executive |
| **US-NRC** | United States Nuclear Regulatory Commission |
| **WANO** | World Association of Nuclear Operators |

### 2.5 Roles and Responsibilities

QRA forms (Appendix D, F and H) shall be conducted according to the workflow given in Appendix A. The compiler of the QRA shall obtain a QRA number from the Access database on the LAN. This is the same database that is used for Safety Screenings, Safety Evaluations and Safety Justifications. The compiler shall keep the database up to date as the QRA progresses through the cycle of compilation/SME review/PSA review/Authorization/Presentation to ETMM/Archiving/Cancellation. PSA review/Authorisation, the name of the person performing the function, in sequence, tracks the progress of the database. The line manager who initiated the QRA is responsible for ensuring that the designated compiler tracks the progress or cancellation of the QRA via the Access database." The PSA manager is accountable for the QRA tracking database.

### 2.6 Process for Monitoring

QRA forms (Appendices D, F and H) are permanent plant records that must be stored for the lifetime of the station. The compiler shall create a record with KIS Reference PH5.3.3.4 and sent to TD&RM within four weeks of document approval.

### 2.7 Related/Supporting Documents

Not Applicable

## 3. Content

a) This guide uses PSA as the default process for categorisation of safety issues as described in Appendix C.

b) The process for QRA generation is described in Appendix A.

c) If the PSA group manager determines that the PSA process is not suitable, the deterministic process can be applied as described in Appendix E. The deterministic process is based on the defence-in-depth approach which consists of three main considerations:

- Frequency Categorisation
- Consequence Categorisation
- Principal Safety Function Capability Categorisation

The key elements for this approach are provided in the IAEA Safety Report Series No. 12, "Evaluation of the Safety of Operating Nuclear Power Plants Built to Earlier Standards" [3]. These elements are based on PSA concepts and have been combined in order to obtain the Koeberg approach set out in this guide.

d) If issues do not directly affect the plant then the operational process should be applied as described in Appendix G.

e) Once the overall evaluation is complete, the actions required in Appendix B should be considered. Since this guide is based on reference [11] more detailed guidance can be obtained from that guide.

## 4. Acceptance

This document has been seen and accepted by:

| Name | Designation |
|---|---|
| E Lamprecht | Senior Physicist |
| D Dreyer | Senior Physicist |

## 5. Revisions

| Date | Rev. | Compiler | Remarks |
|---|---|---|---|
| December 2021 | 4 | P Vymers | Editorial changes to:<br>Section 2.5: added information to facilitate tracking of QRA in Access database on the LAN |
| March 2021 | 3 | E Lamprecht | Full review as part of review cycle. Changes made are as follows:<br><br>- Section 3.3.2: now states that MEDIUM issues for SFP should not be entered into, owing to significant impact on average public risk; adds Level 2 counterpart to Level 1 instantaneous risk limit.<br>- Appendix C: adds guidance on gauging risk significance of SSCs and initiating events.<br>Editorial changes as follows:<br>- Minor error corrections performed<br>- Appendix A (work flow matrix, added Operational Process)<br>- Appendix D (form 331-103)<br>- Appendix E: added information to clarify the intent of a QRA as a risk assessment, with explicit guidance on how to select the consequence to eliminate a common source of error.<br>- Appendix F (form 331-104)<br>- Appendix H added (form 331-105,S11507, to address SE 39601-002 GA))<br>Safety Screening S11507.performed for update of 331-64 itself as well as for 331-103, 331-104, and for the creation of 331-105. |
| September 2017 | 2 | E Lamprecht | Editorial changes to:<br>- Appendix A (work flow matrix)<br>- Appendix D (form 331-103, screening S2017-0517)<br>- Appendix F (form 331-104, screening S2017-0518)<br>the intent of which is to relocate information from the forms to the work-flow matrix and to remove redundant information. Safety screening S2017-0519. |

| Date | Rev. | Compiler | Remarks |
|---|---|---|---|
| May 2016 | 1 | E Lamprecht | Full review as part of review cycle. Changes made are as follows:<br>- Added Section 5.1.2 to refer to Appendix A in body.<br>- Minor editorial changes to procedure 331-64<br>- Minor editorial changes to form 331-103<br>Safety screening S2016-0187 |
| June 2012 | 0 | A Rajkumar | This document was revised to align with the new procedure numbering scheme with only minor typographical changes made. |

## 6. Development Team

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

| Name | Designation or Business area |
|---|---|
| P Vymers | Physicist, DPSA |

## 7. Acknowledgements

Not applicable.

## Appendix A: WORK FLOW MATRIX

| **WORK FLOW RESPONSIBILITY MATRIX** | | | | | | | | | | | | | **APPENDIX A** |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | **ORGANISATION / FUNCTION** | | | | | | | | | | | | |
| R – Responsible<br>A – Approve<br>F – File<br>• – Outside Matrix Scope<br>Y/N or N/Y – Decision<br>C – Concur<br>I – Informed<br>S – Service<br>[ ] – Mandatory Requirement<br>( ) – As Appropriate/Required<br>Flow Path:<br>Main Flow Secondary Flow | COMPILER – AUTHORISED SAFETY EVALUATOR | REVIEWER – SUBJECT MATTER EXPERT OR AUTHORISED SAFETY EVALUATOR | COMPILER – PSA GROUP AUTHORISED SAFETY EVALUATOR | REVIEWER – PSA GROUP AUTHORISED SAFETY EVALUATOR | PSA GROUP MANAGER | LINE MANAGER | INITIATOR | ETMM | | | | | **NOTES & REFERENCES** |
| **ACTIVITIES** | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | |
| **A. INITIATION** | | | | | | | | | | | | | |
| 1. A plant issue or condition is identified that requires grading of its safety significance. | | | | | | | (R) | | | | | | |
| **B. PSA SCREENING** | | | | | | | | | | | | | |
| 1. Determine if the issue can be addressed using PSA. | | | | | [Y/N] | | | | | | | | Determination made by expert judgement. |
| **C. PSA PROCESS** | | | | | | | | | | | | | |
| 1. PSA group manager designates an authorised safety evaluator from the PSA group. | | | | | [R] | | | | | | | | Safety evaluators must be authorised according to the KFA-058 process. |
| 2. Obtain a QRA screening number. | | | [R] | | | | | | | | | | From Access database on the LAN (same as for Safety Screenings, SE, SJ). |
| 3. Perform safety issue categorisation using the PSA process in Appendix C. | | | [R] | | | | | | | | | | Results to be captured in 331-103 (Appendix D). |
| 4. Review of safety issue categorisation by the PSA group. | | (R) | | [R] | | | | | | | | | Safety evaluators must be authorised according to the KFA-058 process. PSA group review should include whether the QRA process, in accordance with this procedure, has been applied. Optional SME review as to whether PSA accurately and adequately addresses the plant issue. |
| 5. Authorised by PSA group manager. | | | | | [A] | | | | | | | | There is no formal requirement on who can authorize a QRA. |
| 6. Present to ETMM for information. | | | [R] | | | | | (I) | | | | | |

| **WORK FLOW RESPONSIBILITY MATRIX** | | | | | | | | | | | | | **APPENDIX A** |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| R – Responsible<br>A – Approve<br>F – File<br>• – Outside Matrix Scope<br>Y/N or N/Y – Decision<br>C – Concur<br>I – Informed<br>S – Service<br>[ ] – Mandatory Requirement<br>( ) – As Appropriate/Required<br>Flow Path:<br>Main Flow Secondary Flow | **ORGANISATION / FUNCTION**<br>COMPILER – AUTHORISED SAFETY EVALUATOR | REVIEWER – SUBJECT MATTER EXPERT OR AUTHORISED SAFETY EVALUATOR | COMPILER – PSA GROUP AUTHORISED SAFETY EVALUATOR | REVIEWER – PSA GROUP AUTHORISED SAFETY EVALUATOR | PSA GROUP MANAGER | LINE MANAGER | INITIATOR | ETMM | | | | | **NOTES & REFERENCES** |
| **ACTIVITIES** | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | |
| **PSA PROCESS (cont'd)** | | | | | | | | | | | | | |
| 7. Ensure a signed copy of 331-103 is stored with TD & RM. | | | [R] | | | | | | | | | | Within 4 weeks of authorisation, using KIS reference PH5.3.3.4. |
| **D. DETERMINISTIC / OPERATATIONAL PROCESS** | | | | | | | | | | | | | |
| 1. Line group manager designates an authorised safety evaluator to implement KGA-046. | | | | | | [R] | | | | | | | Safety evaluators must be authorised according to the KFA-058 process. |
| 2. Obtain a QRA screening number. | [R] | | | | | | | | | | | | From Access database on the LAN (same as for Safety Screenings, SE, SJ). |
| 3. Perform safety issue categorisation using the Deterministic process in Appendix E / Operational process in Appendix G | [R] | | | | | | | | | | | | Results to be captured in Deterministic Process form 331-104 (Appendix F) / Operational Process form (331-105 (Appendix H). |
| 4. Review of safety issue categorisation by SME or authorised safety evaluator. | | [R] | | | | | | | | | | | Safety evaluators must be authorised according to the KFA-058 process. |
| 5. Review of safety issue categorisation by the PSA group. | | | | [R] | | | | | | | | | Safety evaluators must be authorised according to the KFA-058 process. PSA group review should include whether the QRA process, in accordance with this procedure, has been applied. |
| 6. Authorised by line group manager. | | | | | | [A] | | | | | | | There is no formal requirement on who can authorize a QRA. |
| 7. Present to ETMM for information. | [R] | | | | | | | (I) | | | | | |

**CONTROLLED DISCLOSURE**

| WORK FLOW RESPONSIBILITY MATRIX | | | | | | | | | | | | | APPENDIX A |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| R – Responsible<br>A – Approve<br>F – File<br>• – Outside Matrix Scope<br>Y/N or N/Y – Decision<br>C – Concur<br>I – Informed<br>S – Service<br>[ ] – Mandatory Requirement<br>( ) – As Appropriate/Required<br>Flow Path:<br>Main Flow Secondary Flow | **ORGANISATION / FUNCTION** | | | | | | | | | | | | **NOTES & REFERENCES** |
| | COMPILER – AUTHORISED SAFETY EVALUATOR | REVIEWER – SUBJECT MATTER EXPERT OR AUTHORISED SAFETY EVALUATOR | COMPILER – PSA GROUP AUTHORISED SAFETY EVALUATOR | REVIEWER – PSA GROUP AUTHORISED SAFETY EVALUATOR | PSA GROUP MANAGER | LINE MANAGER | INITIATOR | ETMM | | | | | |
| **ACTIVITIES** | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | |
| 8. Ensure a signed copy of 331-104 / 331-105 is stored with TD & RM. | ↓ [R] | | | | | | | | | | | | Within 4 weeks of authorisation, using KIS reference PH5.3.3.4. |

# APPENDIX B: SAFETY SIGNIFICANCE CATEGORIES

| | Defence in Depth Classification Criteria | Actions Required |
|---|---|---|
| **DROP**<br>An issue which may have a negligible impact on plant safety | • No impact on defence in depth.<br>– or –<br>• ALARA principle met. | Plant operation can continue without the need for corrective measures. However, measures may be considered such as economic conventional safety, public perception, regulations, alignment, cost / benefit etc. |
| **LOW**<br>An issue which may have a small impact on plant safety | • A barrier is affected by the issue.<br>– or –<br>• One or more levels of defence are affected by the issue but the primary safety function capability to protect the barrier(s) is still considered robust for certain accident sequences in the design basis envelope[a] or adequate for certain accident sequences beyond the design basis envelope.<br>– or –<br>• The issue causes a new initiating event or an increase of the frequency of certain initiating events and challenges to safety systems and personnel, leading to a small impact on the risk.<br>– or –<br>• The level of operational performance and safety culture warrants improvement. | Plant operation can continue without the need for interim corrective measures. Corrective measures may be considered and implemented within a specified time schedule if shown to be reasonably practicable. |
| **MEDIUM**<br>An issue that has a significant impact on plant safety | • A barrier is degraded by the issue.<br>– or –<br>• One or more levels of defence are significantly affected by the issue but the primary safety function capability to protect the barrier(s) is adequate for certain accident sequences in the design basis envelope[a] or is inadequate for certain accident sequences beyond the design basis envelope.<br>– or –<br>• The issue causes a new initiating event or an increase of the frequency of certain initiating events and challenges to safety systems and personnel, leading to a significant impact on risk.<br>– or –<br>• The level of operational performance and safety culture is inadequate.[b] | Some interim corrective measures are usually necessary in the short term. Plant operation may continue for some limited time, depending on the risk after implementation of the interim corrective measures. Cost effective permanent corrective measures should be implemented. |

## APPENDIX B: SAFETY SIGNIFICANCE CATEGORIES (CONTINUED)

| | Defence in Depth Classification Criteria | Actions Required |
|---|---|---|
| **HIGH**<br>An issue that has a major impact on plant safety | • A barrier is seriously degraded by the issue.<br>– or –<br>• One or more levels of defence are lost because of the issue to that the primary safety function capability to protect the barrier(s) is inadequate for certain accident sequences in the design basis envelope.[a]<br>– or –<br>• The issue causes a new initiating event or an increase of the frequency of certain initiating events and challenges to safety systems and personnel, leading to a major impact on risk.<br>– or –<br>• The level of operational performance and safety culture is unacceptable.[b] | Immediate corrective measures are necessary to reduce the risk and plant shutdown should be considered. If immediate corrective measures cannot reduce the risk, the plant may need to be shut down until interim or permanent corrective measures which will reduce the risk are implemented. |

[a] The phrase "certain accident sequences in the design basis envelope" means the design basis accidents for current design practices, which may be more comprehensive than those of the original design basis, including small break loss of coolant accidents and related boundary conditions, the range of anticipated operational occurrences, startup, shutdown and refuelling operations.

[b] Although the levels of defence associated with the primary safety function capability already include elements of operational safety, the operational performance should emphasise the safety significance of shortcomings in human involvement. The terms used in this table are defined as: warrants improvement — improvements in operational performance are warranted in relation or procedural compliance, inadequate — poor procedural compliance or procedural quality; unacceptable — a significant shortfall in procedural compliance and quality.

# APPENDIX C: PSA PROCESS

## 1. INTRODUCTION

This guide defines the risk acceptance criteria for management decision making in response to Probabilistic Safety Analysis (PSA) results.

The risk acceptance criteria guidelines are not intended to be overly prescriptive. They are intended to provide an indication, in numerical terms, of what is internationally acceptable. Due to model incompleteness and uncertainties associated with these PSA models, the numerical results should not be used as the only tool to make definitive decisions when it comes to safety
evaluations / justifications. However PSA can be exclusively used for categorisation of safety issues when appropriate as this is not the basis of issue closure. For most risk-informed decisions, which could also include deterministic, engineering and economical evaluations, the decision-maker should award a lower bias to the PSA risk evaluation where greater uncertainties exist and so arrive at an integrated decision.

This guide does not define criteria for:

a) Permanent changes to OTS LCOs, which use unique criteria defined in RRM-10-0014 Rev 0b.

b) Risk monitor, as there is currently no international consensus of what criteria should be used for this type of application.

The criteria given in this guide are based on the risk incurred by all hazards. Where the PSA model lacks completeness, such as external events, adequate allowances must be made when using the risk criteria.

The results of the PSA Process should be captured and documented using the PSA Process Form (331-103).

## 2. RISK LEVELS AND MEASURES

The risk to the public and the worker imposed by the operation of Koeberg Nuclear Power Station is calculated using PSA techniques. Within PSA there are different measures that can be used to evaluate the risk of nuclear accidents. Typically, PSAs for Nuclear Power Plants analyse nuclear accident risks at three levels:

- Level 1 which considers the risk of Core Damage,
- Level 2 which considers the risk of Large Radioactive Releases, &
- Level 3 which considers the risk to the public and the workers.

## APPENDIX C: PSA PROCESS (CONTINUED)

Each of these levels has their own risk measures and different probabilistic safety criteria (PSC). The most common risk measure for Level 1 is Core Damage Frequency (CDF). For Level 2, the most common measure is Large Early Release Frequency (LERF). Finally, for Level 3, the measures are public and worker fatality risk. These risk measures are currently in use at Koeberg.

Currently, there are only formal NNR risk criteria for the overall Level 3 results. There is no formal Probabilistic Safety Criteria (PSC) for the other PSA levels.

Additionally, there is no formal guidance on what are acceptable criteria for temporary and permanent plant changes for any of the PSA levels.

### 3. APPROACH

The approach is based on the IAEA guidance where possible. Where guidance is not of sufficient detail, UK & US regulatory authorities and EdF's position is considered. Where the National Nuclear Regulator (NNR) or ESKOM has a formal position on risk limits, these limits shall be respected.

The framework for defining these PSCs is based on there generally being four PSC regions for each risk measure as defined by the IAEA: High, Medium, Low, Drop. The regions are described in Appendix B.

Regardless of the categorisation however the ALARA approach should be applied and cost / benefit considerations should be considered. For example, a simple procedure change may be considered mandatory for a Drop issue while design changes may be considered too costly for a low issue.

### 3.1 CRITERIA FOR OVERALL PSA RESULTS

The acceptability of the overall PSA results is evaluated against the appropriate probabilistic safety criteria (PSC). The PSA results used in the evaluation should include internal and external events, covering full power and shutdown conditions. Where model completeness does not exist, allowances should be made.

With the exception of the public and site personnel risk criteria measured as fatalities, which are regulatory requirements, all PSC should be used as guidance. These PSC should be compared to the mean of the risk measure.

Each of the criteria for each level is important and therefore should be compared for acceptability. The highest grading for any level should apply.

## APPENDIX C: PSA PROCESS (CONTINUED)

It is also important to ensure there is a balanced risk for all the probability safety measures. If there is a single accident group contributing significantly to the results all efforts should be made to reduce the risk generated from this accident group. Such an accident group identifies an area where a single change to the plant could significantly improve safety.

### 3.1.1 Level 3 Overall Probabilistic Safety Criteria

The NNR has defined formal tolerability safety criteria for the public and site personnel. INSAG has no guidance on targets for public health effects.

#### 3.1.1.1 Public Risk

| Average Public Risk | Category | Actions Required |
|---|---|---|
| **> $10^{-8}$ fatalities/(yr person)** | Intolerable | Violation of the Nuclear Installation License. Changes *must* be made to reduce risk. |
| **> $10^{-9}$ fatalities/(yr person)** | Tolerable | Changes *should* be made to reduce risk. |
| **≤ $10^{-9}$ fatalities/(yr person)** | Acceptable | No changes required, but ALARA principle still applicable. |

***Table 1:*** *Level 3 Average Public Probabilistic Safety Criteria*

| Peak Public Risk | Category | Actions Required |
|---|---|---|
| **> $5\times10^{-6}$ fatalities/yr** | Intolerable | Violation of the Nuclear Installation License. Changes *must* be made to reduce risk. |
| **> $5\times10^{-7}$ fatalities/yr** | Tolerable | Changes *should* be made to reduce risk. |
| **≤ $5\times10^{-7}$ fatalities/yr** | Acceptable | No changes required, but ALARA principle still applicable. |

***Table 2:*** *Level 3 Peak Public Probabilistic Safety Criteria*

These probabilistic safety criteria are formal NNR safety criteria given in license document RD-0024. These safety criteria are per site and are summarised in Tables 1 and 2.

The NNR's license document RD-0024 also specifies a target for bias against larger accidents. This aspiration is that the annual frequency f (N) of accidents affecting more than N fatalities be less than $AN^{-1}$, where A is constant derived from the total national population. A is derived by limiting the mean fatality probability per person per annum to $10^{-8}$, in the range of 1 to Np, where Np is an acceptable projection of the national population.

The NNR's license document RD-0024 also requires the ALARA principle to be applied to public risks.

## APPENDIX C: PSA PROCESS (CONTINUED)

### 3.1.1.2 Site Personnel Risk

| Average Site Risk | Category | Actions Required |
|---|---|---|
| **> $10^{-5}$ fatalities/(yr person)** | Intolerable | Violation of the Nuclear Installation License. Changes *must* be made to reduce risk. |
| **> $10^{-6}$ fatalities/(yr person)** | Tolerable | Changes *should* be made to reduce risk. |
| **≤ $10^{-6}$ fatalities/(yr person)** | Acceptable | No changes required, but ALARA principle still applicable. |

***Table 3:*** *Level 3 Average Site Personnel Probabilistic Safety Criteria*

| Peak Site Risk | Category | Actions Required |
|---|---|---|
| **> $5\times10^{-5}$ fatalities/yr** | Intolerable | Violation of the Nuclear Installation License. Changes *must* be made to reduce risk. |
| **> $5\times10^{-6}$ fatalities/yr** | Tolerable | Changes *should* be made to reduce risk. |
| **≤ $5\times10^{-6}$ fatalities/yr** | Acceptable | No changes required, but ALARA principle still applicable. |

***Table 4:*** *Level 3 Peak Site Personnel Probabilistic Safety Criteria*

These probabilistic safety criteria are formal requirements to be met according to RD-0024. These safety criteria are per site and are summarised in Tables 3 and 4.

This is comparable to one of the UK's Health & Safety principles which is the total predicted individual risk of death (early or delayed), to any worker on the plant, attributable to radiation doses from accidents. They specify that a Basic Safety Limit (equivalent to the tolerable or low risk category) of $10^{-4}$/yr, and a Basic Safety Objective (equivalent to the target risk criterion) of $10^{-6}$/yr.

The NNR's license document RD-0024 also requires the ALARA principle to be applied to site personnel risks.

### 3.1.2 Level 2 Overall Probabilistic Safety Criteria

| PSA Result | Category |
|---|---|
| **LERF > $10^{-5}$/yr** | High |
| **$10^{-6}$/yr < LERF ≤ $10^{-5}$/yr** | Medium |
| **$10^{-7}$/yr < LERF ≤ $10^{-6}$/yr** | Low |
| **LERF ≤ $10^{-7}$/yr** | Drop |

***Table 5:*** *Level 2 Overall Probabilistic Safety Criteria*

## APPENDIX C: PSA PROCESS (CONTINUED)

The Large Early Release Frequency is defined as involving the rapid, unscrubbed release of airborne aerosol fission products to the environment before the effective implementation of the off-site emergency response and protective actions. The LERF criteria apply to both core damage events and Spent Fuel Pool accidents.

The probabilistic safety criteria in Table 5 are based on IAEA, US-NRC and UK HSE standards, all of which are in general agreement.

The only significant difference being that the UK's HSE basic safety objective is $10^{-7}$/yr for large release frequencies. EdF uses an informal acceptance criterion that is similar to the target risk criteria, but does not have tolerable risk criteria. What is evident is that there is a general agreement that the LERF criteria should be an order of magnitude less than the CDF criteria.

### 3.1.3 Level 1 Overall Probabilistic Safety Criteria

| PSA Result | Tolerability |
|---|---|
| **CDF > $10^{-4}$/yr** | High |
| **$10^{-5}$/yr < CDF ≤ $10^{-4}$/yr** | Medium |
| **$10^{-6}$/yr < CDF ≤ $10^{-5}$/yr** | Low |
| **CDF ≤ $10^{-6}$/yr** | Drop |

***Table 6:*** *Level 1 Overall Probabilistic Safety Criteria*

The criteria in Table 6 are based on IAEA, US-NRC and UK's HSE standards, all of which are in general agreement. It should be highlighted that EdF have a policy to actively target their CDF to below $10^{-5}$/yr. IAEA Safety Series 12 suggests however that overall CDF should be less than $10^{-3}$/y.

This is in-line with INSAG-3 which states that the target core damage frequency for existing power plants should be below $10^{-4}$/yr, and for future plants should be below $10^{-5}$/yr.

## APPENDIX C: PSA PROCESS (CONTINUED)

### 3.2 CRITERIA FOR PERMANENT CHANGES

These probabilistic safety criteria evaluate the acceptability of permanent plant changes. Examples of such changes would be plant modifications and procedural changes.

Any changes should meet the necessary acceptance criteria for all three levels, where appropriate and practical. It is important to note that permanent changes resulting in increases in risk can be allowed which is in-line with the latest US-NRC regulation.

In addition to the criteria below, it must also be ensured that the overall risk criteria presented in the previous sections are respected.

Historically, there have been very few plant changes that result in a net overall increase in risk. However, recognising that the possibility of such a change may be proposed because of significant cost savings, or to reduce risk in other areas, not considered in the PSA, these criteria have been included.

#### 3.2.1 Level 3 Permanent Change Probabilistic Safety Criteria

There is no guidance nationally or internationally on probabilistic safety criteria for the evaluation of individual permanent changes. As the uncertainties at this level are relatively large, and in view of the general insensitivity of the Level 3 to most plant issues; a criteria at this level for permanent changes is not considered practical.

However, if any modification or permanent change were found to exceed the regulatory limits for the overall Level 3 results (tables 1 to 4) then the change would be considered unacceptable.

#### 3.2.2 Level 2 Permanent Change Probabilistic Safety Criteria

| Change in LERF | Tolerability |
|---|---|
| **$\Delta$LERF > $10^{-6}$/yr** | High |
| **$10^{-7}$/yr < $\Delta$LERF $\leq$ $10^{-6}$/yr** | Medium |
| **$10^{-8}$/yr < $\Delta$LERF $\leq$ $10^{-7}$/yr** | Low |
| **$\Delta$LERF $\leq 10^{-8}$/yr** | Drop |

***Table 7:*** *Level 2 Permanent Change Probabilistic Safety Criteria*

## APPENDIX C: PSA PROCESS (CONTINUED)

The criteria in Table 7 apply are based on NRC Regulatory Guide 1.174 and are more restrictive than EPRI's recommended criteria for permanent changes.

The criteria in Table 7 also apply to Spent Fuel Pool (SFP) uncovery accidents. Such accidents contribute to off-site releases but not core damage. They are significant because of the large radionuclide inventory in the SFPs and due to the Spent Fuel buildings not being leak tight.

If the permanent change results in a decrease in the Large Early Release Frequency (LERF), the change will be acceptable from a LERF perspective. If the change results in a very small increase in LERF ($\Delta$LERF < $10^{-8}$/yr) it is acceptable. However, if the change in LERF is greater than $10^{-7}$/yr, the proposed change is unacceptable.

### 3.2.3 Level 1 Permanent Change Probabilistic Safety Criteria

| Change in CDF | Tolerability |
|---|---|
| **$\Delta$CDF >$10^{-5}$/yr** | High |
| **$10^{-6}$/yr < $\Delta$CDF $\leq$ $10^{-5}$/yr** | Medium |
| **$10^{-7}$/yr < $\Delta$CDF $\leq$ $10^{-6}$/yr** | Low |
| **$\Delta$CDF $\leq$ $10^{-7}$/yr** | Drop |

***Table 8:*** *Level 1 Permanent Change Probabilistic Safety Criteria*

The criteria in Table 8 are in-line with NRC Regulatory Guide 1.174 and are more restrictive than EPRI's recommended criteria for permanent changes.

If the permanent change results in a decrease in CDF, the change will be acceptable from a CDF perspective. If the change results is a very small increase in CDF ($\Delta$CDF <$10^{-7}$/yr) it is acceptable. However, if the resultant change in CDF in greater than $10^{-6}$/yr, the change should be considered unacceptable.

## 3.3 CRITERIA FOR TEMPORARY CHANGES

A temporary change is any modification, event or configuration that may lead to the plant incurring additional risk for a limited time. Examples of temporary changes are once off technical specification exemptions, justification for limited continued operations and event significance evaluations.

## APPENDIX C: PSA PROCESS (CONTINUED)

They are quantified using core damage probability or large early release probability. These probability measurements are determined by multiplying the additional risk incurred for the change by the duration of the change.

i.e. CDP = ΔCDF x duration **or** LERP = ΔLERF x duration

These limits are also used to evaluate previous events as they are considered as temporary configurations as done in the EdF and the US-NRC accident sequence precursor programs. These programs evaluate the conditional core damage probability of events that have occurred in the US and France.

EdF currently have more restrictive internal limits, based on the LCO for evaluating the acceptance of existing forced or planned high risk configurations, as opposed to historical assessments. However, they have found their acceptance criteria very restrictive and are currently in the process of revising their criteria and its use.

These temporary change risk criteria are to evaluate individual plant changes. However, the cumulative impact of all individual temporary changes need to be assessed on an annual basis to ensure the overall PSA results reflect the real annual plant risk.

### 3.3.1 Level 3 Temporary Change Probabilistic Safety Criteria

There are no international or national acceptance limits for this type of change evaluation. As the uncertainties at this level are relatively large and because of the general insensitivity of the Level 3 PSA to most plant issues; criteria at this level for temporary changes are not considered practical.

### 3.3.2 Level 2 Temporary Change Probabilistic Safety Criteria

| Event LERP | Tolerability |
|---|---|
| **LERP >$10^{-5}$** | High |
| **$10^{-6}$ < LERP ≤ $10^{-5}$** | Medium** |
| **$10^{-7}$ < LERP ≤ $10^{-6}$** | Low |
| **$10^{-8}$ < LERP ≤ $10^{-7}$** | Possibly Low* |
| **LERP ≤ $10^{-8}$** | Drop |

***** Consider non PSA aspects to determine if Low or Drop***

***** Because of the significant impact on average public risk, temporary-change MEDIUM issues affecting the Spent Fuel Pool should not be entered voluntarily.***

***Table 9:** Level 2 Temporary Change Probabilistic Safety Criteria*

The criteria in Table 9 are based on the EPRI 'PSA Application Guide' criteria. These are an order of magnitude below the overall CDF criteria. There is no other guidance on acceptance and tolerable limits for temporary changes from any other reference. Because of the significant impact on average public risk of spent-fuel related problems, temporary-change MEDIUM issues affecting the Spent Fuel Pool should not be entered voluntarily.

## APPENDIX C: PSA PROCESS (CONTINUED)

The criteria in Table 9 also apply to the Spent Fuel Pool (SFP) uncovery accidents. Such accidents contribute to off-site releases but not core damage. They are significant because of the large radionuclide inventory in the SFP's and due to the Spent Fuel buildings not being leak tight.

A further criterion is to **ensure that the instantaneous or conditional configuration LERF, for the duration of the inoperability or event, does not exceed $10^{-4}$/yr.** See Section 3.3.3 for details on corresponding EPRI guidance for CDF, upon which this criterion is based.

### 3.3.3 Level 1 Temporary Change Probabilistic Safety Criteria

| Event CDP | Tolerability |
|---|---|
| **CDP > $10^{-4}$** | High |
| **$10^{-5}$ < CDP ≤ $10^{-4}$** | Medium |
| **$10^{-6}$ < CDP ≤ $10^{-5}$** | Low |
| **$10^{-7}$ < CDP ≤ $10^{-6}$** | Possibly Low* |
| **CDP ≤$10^{-7}$** | Drop |

**** Consider non PSA aspects to determine if Low or Drop***

***Table 10:*** *Level 1 Temporary Change Probabilistic Safety Criteria*

The criteria in Table 10 are based on the EPRI 'PSA Application Guide' criteria.

Both the US-NRC and EdF have accident sequence precursor programs which quantify the CDP of individual events that have occurred in the US and France. Both programs consider events with a CDP less than $10^{-6}$ as noteworthy but only events with a CDP greater than $10^{-4}$ to be risk significant which is in agreement with the EPRI criteria.

A further criterion, as suggested by the EPRI "PSA Application Guide", is to **ensure that the instantaneous or conditional configuration CDF, for the duration of the inoperability or event, does not exceed $10^{-3}$/yr**.

## 3.4 ACCEPTANCE GUIDELINES FOR IMPORTANCE MEASURES

For some applications, the baseline PSA results can be used to assess the risk significance (importance) of components, systems or structures independently of changes to the plant.

These criteria are relative measures and can be compared against the CDF, LERF and FDF results.

To classify equipment based on their importance to mitigate and prevent a nuclear accident, the criteria from NUMARC 93-01 are applied. This agrees with both the EPRI and NEI guidelines.

## APPENDIX C: PSA PROCESS (CONTINUED)

Equipment with an importance measure above any of the criteria in Table 11 should be classified as risk significant. Equipment with an importance measure below all of the criteria in Table 11 should be classified as non-risk significant provided that this can be supported deterministically.

| Risk Importance Measure | Criteria | Risk Category |
|---|---|---|
| **Risk Reduction Worth (RRW)** | | |
| **[or Risk Decrease Factor]** | | |
| - System Level | **> 1.05** | Risk Significant |
| - Component Level | **> 1.005** | Risk Significant |
| **Fussel-Vesely Importance (FV)** | | |
| - System Level | **> 0.05** | Risk Significant |
| - Component Level | **> 0.005** | Risk Significant |
| **Risk Achievement Worth (RAW)** | | |
| **[or Risk Increase Factor]** | | |
| - System Level | **> 2** | Risk Significant |
| - Component Level | **> 2** | Risk Significant |

***Table 11:*** *Component and System Risk Importance Measure Risk Significance Criteria*

It should be noted that the criteria for Risk Reduction Worth and Fussel-Vesely importance are effectively the same, as these measures are interrelated, but both are included for completeness. Since PSA quantification codes calculate both, only the Fussel-Vesely importance measure is discussed further.

For determining risk importance of components,

- the Fussel-Vesely Importance of a component is the sum of this measure over all basic events that represent failure modes of the component (including CCF)

- the Risk Achievement Worth of a component is the maximum of this measure over all basic events that present failure modes of the component (including CCF)

The same principle may be applied to systems.

Note that initiating events present a particular challenge because in the Koeberg PSA model these are generally modelled as “lumped” events and not by means of fault-trees that contain failure basic events. Therefore, any list of risk-significant components should be reviewed (e.g., by an expert panel) for hidden contributions from risk-significant initiating events, and adjusted accordingly. The risk significance of initiating events can be determined using the FV criteria in Table 11 and by substituting conditional top event probability (e.g., conditional CDP) for risk achievement worth.

## Appendix D: PSA PROCESS FORM (331-103)

| | | | | | |
|---|---|---|---|---|---|
| Eskom | **Nuclear Engineering PSA Process** | **Document Identifier** | 331-103 | **Rev** | 3 |
| | | **Effective Date** | **March 2021** | | |
| | | **Review Date** | **March 2024** | | |

***Note:*** *This QRA is to be completed in accordance with the guidelines provided in 331-64.*

| | | |
|---|---|---|
| **Title** | | **QRA Screening Number:** |
| **Issue Description** | | |
| **Type of Plant Change** | ☐ Permanent | ☐ Temporary |
| **Justification** | | |
| **Identify Applicable Criteria** | ☐ Public Risk (Level 3)<br>☐ ΔLERF/LERP (Level 2)<br>☐ ΔCDF/CDP (Level 1) | ☐ Site Personnel Risk (Level 3)<br>☐ ΔFDF/FDP (Level 2, SFP) |
| **Justification** | | |

**QRA - Overall PSA Evaluation**

| | | | **Result** | **High** | **Medium** | **Low** | **Drop** |
|---|---|---|---|---|---|---|---|
| **Overall PSA Criteria** | **Level 3** | Average Public Risk | | ☐ | ☐ | ☐ | ☐ |
| | | Peak Public Risk | | ☐ | ☐ | ☐ | ☐ |
| | | Average Site Risk | | ☐ | ☐ | ☐ | ☐ |
| | | Peak Site Risk | | ☐ | ☐ | ☐ | ☐ |
| | **Level 2** | LERF | | ☐ | ☐ | ☐ | ☐ |
| | **Level 2** | FDF (SFP) | | ☐ | ☐ | ☐ | ☐ |
| | **Level 1** | CDF | | ☐ | ☐ | ☐ | ☐ |
| **Permanent Change Criteria** | **Level 2** | ΔLERF | | ☐ | ☐ | ☐ | ☐ |
| | **Level 1** | ΔCDF | | ☐ | ☐ | ☐ | ☐ |
| | **Level 2** | ΔFDF (SFP) | | ☐ | ☐ | ☐ | ☐ |
| **Temporary Change Criteria** | **Level 2** | LERP | | ☐ | ☐ | ☐ | ☐ |
| | **Level 2** | FDP (SFP) | | ☐ | ☐ | ☐ | ☐ |
| | **Level 1** | CDP | | ☐ | ☐ | ☐ | ☐ |
| **Overall Evaluation** | | | | ☐ | ☐ | ☐ | ☐ |

## APPENDIX D: PSA PROCESS FORM (331-103) (CONTINUED)

| Eskom | Nuclear Engineering PSA Process | Document Identifier | 331-103 | Rev | 3 |
|---|---|---|---|---|---|
| | | Effective Date | March 2021 | | |
| | | Review Date | March 2024 | | |

| Comments |
|---|
| |
| **Document any Mitigating Actions to be taken (refer to Appendix B of 331-64)** |
| |

| | Name | Signature | Date | Designation / Group |
|---|---|---|---|---|
| Prepared By | | | | |
| PSA Group Review | | | | |
| Optional SME Review | | | | |
| Authorised By | | | | |

## Appendix E: DETERMINISTIC PROCESS

A QRA, conducted using the deterministic process, is logically equivalent to a single-branch event tree. The initiating event is a postulated condition or occurrence that will require an affected safety function to be actuated if an undesired consequence to be averted. Risk categorisation takes place considering the frequency of the initiating event, the capability of the affected safety function (or its likelihood of failing) and the consequence that will ensue if the initiating event occurs and the affected safety function fails.

### 1. Step 1: Determine Principal Safety Functions Affected

The first step in the judgement process is to identify which Principal Safety Function(s) are affected by the safety issue.

### 2. Step 2: Principal Safety Function Capability Categorisation

This step requires the greatest amount of judgement, experience and engineering skill. The objective is to assess the expected reliability of a principal safety function to prevent an accident or protect a barrier. For engineered principal safety functions compare physical margins with those specified in appropriate standards. For those requiring human action, consider time available, training, procedures, and environment.

The following rules are used to complete the Principal Safety Function Capability Categorisation in 331-104.

| Principal safety function Category | Guidance for Judgement |
|---|---|
| **Robust**<br>Safety Function | Safety function for EXPECTED/POSSIBLE initiating events achieved with either<br>• capacity and redundancy<br>• protection against common cause failures<br>• diversity<br>• safety margin<br>• not over reliant on programmatic activities |
| **Adequate**<br>Safety Function | Safety function can be achieved with<br>• questionable capacity only,<br>• OR, incomplete redundancy, incomplete protection against common cause failures, incomplete diversity as determined by current standards and practices,<br>• OR, over reliance on programmatic activities. |
| **Inadequate**<br>Safety Function | • Safety function cannot be achieved, or is unlikely to be achieved |

## APPENDIX E: DETERMINISTIC PROCESS (CONTINUED)

### 3. Step 3: Frequency Categorisation

Estimate the frequency of the initiating event associated with the safety issue under consideration. The initiating event could directly or indirectly be caused by the safety issue, or the safety issue may become relevant in the accident sequence after a particular initiating event occurs. The following rules which align with the Koeberg SAR are used to complete the Frequency Categorisation in 331-104.

| Frequency Category | Guidance for Judgement |
|---|---|
| **Expected**<br>Initiating Events and Transient Scenarios | Events that might reasonably be expected during the life of the plant (frequency > 1E-2/reactor-year). Consistent with anticipated operational occurrences. |
| **Possible**<br>Initiating Events and Design Basis Accident Scenarios | Events which have > 1% chance of occurring over the life of the plant (frequency > 1E-4/reactor-year). Consistent with design basis accidents. |
| **Unlikely**<br>Initiating Events and Beyond Design Basis Accident Scenarios | Events which have < 1% chance of occurring over the life of the plant (frequency < 1E-4/reactor-year). Not normally included in design basis accidents. |
| **Remote**<br>Initiating Events And Severe Accident Scenarios | Events which are very unlikely to occur (frequency <1E-6/reactor-year) |

### 4. Step 4: Consequence Categorisation

First, determine the potential consequences of the safety issue in terms of its impact on prevention (occurrence of initiating events) or mitigation of events which threaten one or more barriers controlling radioactive material. Second, use this knowledge to categorise the potential consequences of the safety issue based on the severity of the associated accident in terms of plant damage, radioactive release or exposure of plant personnel. The following rules (derived from RD-0014 and RD-0022) are used to complete the Consequence Categorisation of the form in 331-104. Because the QRA is a risk analysis,the consequence to be considered is that of the affected safety function being required and failing, *not* succeeding as is the case with SAR safety analysis.

| Consequence Category | Guidance for Judgement |
|---|---|
| **Tolerable**<br>Consequences of Transients and on-site radiological exposures | • Some plant damage.<br>• Releases leading to off-site doses not exceeding 1 mSv<br>• Doses to site personnel not exceeding 20 mSv |
| **Significant**<br>Consequences of Moderate and Serious Design Basis Accidents and off-site radiological exposures | • Serious, but contained plant damage<br>• Possible core damage<br>• Releases leading to off-site doses of the order of 1 – 10 mSv<br>• Site personnel doses 20 – 100 mSv |
| **Intolerable**<br>Consequences of Severe Accidents | • Severe core damage.<br>• Severe plant damage.<br>• Release of large fraction of fission products ( iodine thyroid dose > 100 mGy), acute and delayed health effects, off-site doses > 10 mSv<br>• Site personnel doses exceeding100 mSv |

## 5. Step 5: Safety Significance Judgement

The importance of the safety issue is established by completing page 2 of 331-104, using the results of Steps 1 – 4 above.

## Appendix F: DETERMINISTIC PROCESS Form (331-104)

| | | | | | |
|---|---|---|---|---|---|
| Eskom | Nuclear Engineering Deterministic Process | Document Identifier | 331-104 | Rev | 2 |
| | | Effective Date | March 2021 | | |
| | | Review Date | March 2024 | | |

| | | |
|---|---|---|
| Note: This QRA is to be completed in accordance with the guidelines provided in 331-64. | | |
| **Title** | | **QRA Screening Number:** |
| **Description** | | |
| **Affected Principal Safety Functions** | | |
| **Principal Safety Function Capability Category** | **Justification for Judgement** | |
| ☐ **Robust**<br>Achieved with either:<br>• capacity &redundancy<br>• protection against CCF<br>• diversity<br>• safety margin<br>• not over-reliant on programmatic activity | | |
| ☐ **Adequate**<br>Achieved with:<br>• questionable capacity only<br>• OR *incomplete* redundancy, protection against CCF or diversity as determined by current standards and practices<br>• OR over-reliance on programmatic activity | | |
| ☐ **Inadequate**<br>Cannot be achieved or is unlikely to be achieved. | | |

## APPENDIX F: DETERMINISTIC PROCESS FORM (331-104) (CONTINUED)

| Eskom | Nuclear Engineering Deterministic Process | Document Identifier | 331-104 | Rev | 2 |
|---|---|---|---|---|---|
| | | Effective Date | March 2021 | | |
| | | Review Date | March 2024 | | |

| Frequency Category | Justification for Judgement |
|---|---|
| ☐ **Expected**<br>Initiating Events and Transient Scenarios<br>F > 1E-2/ry | |
| ☐ **Possible**<br>Initiating Events and Design Basis Accident Scenarios<br>1E-4/ry ≥ F > 1E-2/ry | |
| ☐ **Unlikely**<br>Initiating Events and Beyond Design Basis Accident Scenarios<br>1E-6/ry ≥ F > 1E-4/ry | |
| ☐ **Remote**<br>Initiating Events and Severe Accident Scenarios<br>F < 1E-6/ry | |

## APPENDIX F: DETERMINISTIC PROCESS FORM (331-104) (CONTINUED)

| Eskom | Nuclear Engineering Deterministic Process | Document Identifier | 331-104 | Rev | 2 |
|---|---|---|---|---|---|
| | | Effective Date | March 2021 | | |
| | | Review Date | March 2024 | | |

| Consequence Category | Justification for Judgement |
|---|---|
| ☐ **Tolerable**<br><br>Consequences of Transients and On-Site Radiological Exposures<br><br>• Some plant damage<br>• Off-site doses ≤ 1mSv<br>• Site pers. doses ≤ 20 mSv | |
| ☐ **Significant**<br><br>Consequences of Moderate and Serious Design Base Accidents and Off-Site Radiological Exposures<br><br>• Serious but contained plant damage<br>• Possible core damage<br>• Off-site doses : 1 – 10 mSv<br>• Site pers. doses: 20 - 100 mSv | |
| ☐ **Intolerable**<br><br>Consequences of Severe Accidents<br><br>• Severe core camage<br>• Severe plant damage<br>• Large release (thyroid dose > 100 mGy), acute and delayed health effects<br>• off-site doses > 10 mSv<br>• Site pers. doses >100 mSv | |

**Please mark conclusion as *bold and underlined.***

| | **Potential Consequences** | Tolerable | | | Significant | | | Intolerable | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | **Safety Function Capability** | **Robust** | **Adequate** | **Inadequate** | **Robust** | **Adequate** | **Inadequate** | **Robust** | **Adequate** | **Inadequate** |
| **Event Frequency** | **Expected** | *Low* | *Low* | *Medium* | *Medium* | *High* | *High* | *High* | *High* | *High* |
| | **Possible** | *Drop* | *Drop* | *Low* | *Low* | *Medium* | *High* | *Medium* | *Medium* | *High* |
| | **Unlikely** | *Drop* | *Drop* | *Drop* | *Drop* | *Low* | *Low* | *Low* | *Low* | *Medium* |
| | **Remote** | *Drop* | *Drop* | *Drop* | *Drop* | *Drop* | *Drop* | *Drop* | *Low* | *Low* |

**CONTROLLED DISCLOSURE**

## APPENDIX F: DETERMINISTIC PROCESS FORM (331-104) (CONTINUED)

| Eskom | Nuclear Engineering Deterministic Process | Document Identifier | 331-104 | Rev | 2 |
|---|---|---|---|---|---|
| | | Effective Date | March 2021 | | |
| | | Review Date | March 2024 | | |

| Document any mitigating actions to be taken (refer to Appendix B of 331-64). |
|---|
| |

| | Name | Signature | Date | Designation / Group |
|---|---|---|---|---|
| Prepared By | | | | |
| SME Review | | | | |
| PSA Group Review | | | | |
| Authorised By | | | | |

## Appendix G: OPERATIONAL PROCESS

### 1. BACKGROUND

The operational process is only to be used when the impact on nuclear safety cannot be performed by neither deterministic nor the PSA process.

This appendix provides a framework for assessing the safety significance of operational issues.

Operational issues can be categorised into two groups: those that have a direct impact on the level of defence in depth and those that have an impact on the level of safety culture but whose impact on the level of defence in depth is diffuse, but no less significant.

IAEA Safety Series No. 110, “The Safety of Nuclear Installations”, establishes six fundamental principles for the safe operation and maintenance of nuclear power plants. These are:

(1) The design shall ensure that the nuclear installation is suited for reliable, stable and easily manageable operation. The prime goal shall be the prevention of accidents.

(2) The design shall include the appropriate application of the defence in depth principle so that there are several levels of protection and multiple barriers to prevent releases of radioactive materials, and to ensure that failures or combinations of failures that might lead to significant radiological consequences are of very low probability.

(3) Technologies incorporated in a design shall be proven or qualified by experience or testing, or both.

(4) The systematic consideration of the human-machine interface and human factors shall be included in all stages of design and in the associated development of operational requirements.

(5) The exposure of site personnel to radiation and releases of radioactive materials to the environment shall be made, by design, as low as reasonably achievable.

(6) A comprehensive safety assessment and independent verification shall be carried out to confirm that the design of the installation will fulfil the safety objectives and requirements before the operating organisation completes its submission to the regulatory body.

INSAG-3, “Basic Safety Principles for Nuclear Power Plants” and INSAG-4, “Safety Culture” describe the principal requirements for management responsibility to achieve the safe operation of nuclear power plants through the development and maintenance of a strong safety culture.

## APPENDIX G: OPERATIONAL PROCESS (CONTINUED)

Any review process will need to address operational performance and feedback, the adequacy of the safety management system, the development and maintenance of a strong safety culture, accident prevention and mitigation, quality assurance and radiological protection. These issues must be seen as a necessary foundation for the assessment of plant safety against current standards. For many plant specific safety issues, consideration must be given to the demands on the operator and the capability to meet them to achieve defence in depth. Equally, certain corrective actions may require administrative procedures and operator intervention, and human factor analysis may be required. A human factor assessment comprising an operational review, task analyses and human reliability assessment to support the PSA may be needed.

### 2. PREPARATION

The first phase of assessing the safety significance of operational issues is to obtain information on the current performance of the plant under consideration, within its generic type, both nationally and internationally. This can be obtained by using:

(1) Operational experience feedback, including performance indicators such as nuclear, radiological and industrial safety performance indicators.

(2) Quality assurance audits.

(3) International reviews, e.g. WANO or INPO peer evaluations, including comparisons with performance objectives and criteria.

(4) Review of the organisation’s safety management arrangements, including the framework for establishing and maintaining a sound safety culture.

(5) Review of the operating, maintenance and emergency procedures / activities.

### 3. ASSESSMENT

The second phase is to assess the safety significance of the findings against the criteria given in Appendix B. The first step is to divide the findings into those that impact directly on the level of defence in depth and those that impact on safety culture.

Issues affecting defence in depth include the following:

(1) Plant issues (i.e. equipment defects found during service). These issues can be assessed through their impact on fault trees and equipment failure frequencies.

## APPENDIX G: OPERATIONAL PROCESS (CONTINUED)

(2) Human factors issues (i.e. slips and abnormal events during operational activities related to poor procedures, plant layout, training, etc.). Human errors during manual activities can usually be modelled in fault trees and their significance assessed using human reliability analysis. However, cognitive activities and acts of commission (i.e. performing an unwanted action) are difficult to model and assess quantitatively. Qualitative judgements can be made using task analysis.

(3) Issues associated with operational and safety (maintenance, surveillance, engineering support and training) can have a direct bearing on the availability and reliability of safety components and systems, and should be classified accordingly even if the application of these assessment criteria for operational performance is more subjective.

Issues affecting safety culture include the following:

(1) Safety management issues, i.e. deficiencies in allocation of responsibilities, management structures, safety policy, and arrangements for audit and review. A good safety culture requires an effective framework for managing safety.

(2) Attitudes of individuals (i.e. partial or complete lack of a questioning attitude and of a rigorous and prudent approach). A good safety culture requires the commitment of individuals at all levels in responding to and benefiting from the safety management framework.

(3) Attitudes of the organisations (i.e. deficiencies in ensuring adequate resources for safety and in the commitment to a process of continuous improvement). Such a commitment is at the heart of a good safety culture.

Qualitative judgements on the adequacy of the safety culture can be made by assessing the safety management framework and the arrangements for promoting and monitoring safety culture. It is likely that a good safety culture will be present only if positive action is taken to promote it.

Assessing the safety management framework involves:

(1) Assessing the scope of the framework by reviewing the current arrangements against international best practices given in various sources such as INSAG-4, the WANO performance objectives and criteria, and the UK Health and Safety Executive booklet entitled Successful Health and Safety Management.

(2) Assessing the effectiveness of the framework by reviewing past performance to identify whether the system is adequately robust.

## APPENDIX G: OPERATIONAL PROCESS (CONTINUED)

Assessing the arrangements to promote and monitor safety culture involves:

(1) Assessing whether adequate arrangements exist to promote safety culture covering staff awareness and commitment, staff involvement and ownership, effective communications, etc.

(2) Assessing whether adequate arrangements exist to monitor safety culture by such methods as staff attitude surveys, safety culture and analysis of events, performance indicators, etc.

Because judgements on safety management and safety culture are very subjective, plant operators are encouraged to monitor their safety culture arrangements with an independent review. Such reviews could include WANO or INPO peer evaluations.

In particular, the WANO guidance on performance objectives and criteria for peer reviews comprehensively describes good international practices. The guidance sets out detailed objectives in each of the following areas:

- organisation and administration
- operations
- maintenance
- engineering support
- training and qualification
- radiological protection
- chemistry
- operating experience review
- emergency preparedness

Each area is expanded to describe detailed practices addressing both the management framework for safe operation and the attendant safety culture:

- operations organisation and administration
- conduct of operations
- plant status controls
- operating procedures and documentation
- operational facilities and equipment
- operator knowledge and performance

## APPENDIX G: OPERATIONAL PROCESS (CONTINUED)

### 4. IMPLEMENTATION

Actions taken to overcome weaknesses cover:

(1) Actions to improve the safety management framework – there are various sources of international best practice including INSAG-4, the WANO performance objectives and criteria, and the UK Health and Safety Executive booklet.

(2) Actions to improve the attitudes of individuals and organisations – it is essential that the cultural factors underlying the apparent weaknesses be identified by the appropriate use of root cause analysis techniques. These underlying factors are likely to be highly interdependent, and a mixture of corrective measures are likely to be required, relating to issues such as developing personnel, streamlining processes and simplifying organisational structures and responsibilities.

## Appendix H: OPERATIONAL PROCESS Form (331-105)

| | | | | | |
|---|---|---|---|---|---|
| Eskom | **Nuclear Engineering Operational Process** | **Document Identifier** | 331-105 | **Rev** | 1 |
| | | **Effective Date** | March 2021 | | |
| | | **Review Date** | March 2024 | | |

| | | |
|---|---|---|
| **Note: This QRA is to be completed in accordance with the guidelines provided in 331-64.** | | |
| **Title** | | **QRA Screening Number:** |
| **Description** | | |
| **Affected Operational Properties** | | |
| **Risk impact grading** | **Justification for Judgement** *(use Defence in Depth Classification Criteria in 331-64 Appendix B)* | |
| ☐ **High** Major impact on plant safety | | |
| ☐ **Medium** Significant impact on plant safety | | |
| ☐ **Low** Small impact on plant safety | | |
| ☐ **Drop** Negligible impact on plant safety | | |
| **Document any Mitigating Actions to be taken (refer to Appendix B of 331-64)** | | |

| | Name | Signature | Date | Designation / Group |
|---|---|---|---|---|
| **Prepared By** | | | | |
| **SME Review** | | | | |
| **PSA Group Review** | | | | |
| **Authorised By** | | | | |