Eskom	**Guide**	**Nuclear Engineering**

Title: **Safety Justification Preparation**

Document Identifier:	**240-156067953**
Alternative Reference Number:	**KGA-029**
Area of Applicability:	**Nuclear Engineering**
Functional Area:	**Engineering**
Revision:	**1**
Total Pages:	**15**
Next Review Date:	**July 2024**
Disclosure Classification:	**Controlled Disclosure**

Compiled by	**Supported by**	**Authorized by**
A Rijnsburger	**Mvuseleli Hermanus**	**B Mashele**
Senior Advisor C&I	**KSCG Manager**	**Senior Manager - Nuclear Engineering**
Date: 2021-06-29	Date: 2021-07-23	Date: 2021-07-26

Nuclear Additional Classification Information

Business Level:	**3**
Working Document:	**3**
Importance Classification:	**CSR- S11003**
NNR Approval:	**No**
Safety Committee Approval:	**No**
ALARA Review:	**No**
Functional Control Area:	**Koeberg Safety Case Group**

Content

Page

1. Introduction

This guide aims to provide guidance for the compilation of a Safety Justification.

The Safety Analysis Report (SAR) demonstrates the inherent safety of the plant design and plant operation. The SAR supports the defence-in-depth principle, the As Low As Reasonably Achievable (ALARA) approach, adherence to National Nuclear Regulator (NNR) safety criteria and the use of automatic protection and safeguards systems, and thus ensures that there is no unacceptable risk to the health and safety of the operators and the general public resulting from plant operation. The General Operating Rules (GOR) support the plant design and operation (including design extension conditions), and are in agreement with the SAR.

The Safety Evaluation Process determines whether there is a conflict or potential conflict with the assumptions or statements made in the SAR. If there is a conflict, or an apparent conflict, then a Safety Evaluation is required to determine whether the change poses an Unreviewed Safety Question (USQ). Where a USQ exists, the activity may be stopped or a Safety Justification may be compiled to put forward arguments why the activity or condition is, or should be included, within the design basis and the licensing basis.

2. Supporting Clauses

2.1 Scope

This document shall apply throughout Eskom Holdings Limited Divisions.

2.1.1 Purpose

To provide guidelines for the preparation of a nuclear Safety Justification to support the implementation of activities or continued operation with conditions that may be in conflict with the Koeberg SAR.

2.1.2 Applicability

This document is applicable to Nuclear Operating Unit (NOU).

2.1.3 Effective date

This document is effective from the authorisation date.

2.2 References

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

2.2.1 Normative References

[1] 238-8 Nuclear Safety and Quality Manual

[2] 335-2 KNPS Management Manual

[3] 331-3 Nuclear Engineering Document and Records Management Work Instruction

[4] 240-143604773 [KAA-709] The Safety Evaluation Process

[5] KSA-011 The Requirements for Controlled Documents

[6] 331-134 Screening and Safety Evaluation Guide

[7] NIL-01 Nuclear Installation Licence (NNR) for Koeberg Nuclear Power Station

2.2.2 Informative References

[8] GGW-1064 The Use of Licensing Frameworks at Koeberg Nuclear Power Station

[9] 240-143501787 Koeberg Nuclear Licensing Processes

[10] KAA-501 Project Management Process for Koeberg Nuclear Power Station Modifications

[11] 331-88 Temporary Alterations to Plant, Plant Structures or Operating Parameters that Affect the Design Base

[12] 331-177 Process and Responsibilities for the Development and Implementation of the In-service Inspection Programme

[13] KAA-647 Control of Non-Routine Testing and Infrequently Performed Activities

[14] 240-149081050 [KAA-689] Control of the Operating Technical Specifications

[15] 240-119744497 Control of the Safety Analysis Report

[16] KAA-768 Safety, Health and Environmental Risk Assessment and Programme

[17] 331-86 Design Changes to Plant, Plant Structures or Operating Parameters

[18] 240-143370657 Control of the Safety Related Surveillance Manual

[19] 331-94 Importance Category Classification Listing

[20] KTA-001 Training and Qualification Requirements for Nuclear Safety Review Committees

[21] 240-146088803 Training and Qualifications Requirements for Safety Screenings and Evaluators

[22] 10CFR50 Title 10 of the Code of Federal Regulations, Part 50

[23] 331-195 Koeberg Accident Analysis Manual

[24] KSA-066 Standard for Nuclear Design and Licensing Basis Evaluations

[25] 238-34 to 238-54 Radiation Protection Standards

[26] SAR Safety Analysis Report

[27] USNRC Regulatory Guides 1.174 An Approach For Using Probabilistic Risk Assessment In Risk-Informed Decisions On Plant-Specific Changes To The Licensing Basis

[28] USNRC Regulatory Guides 1.175 An Approach For Plant-Specific, Risk-Informed Decision Making: In-service Testing

[29] USNRC Regulatory Guides 1.176 An Approach For Plant-Specific, Risk-Informed Decision Making: Graded Quality Assurance

[30] USNRC Regulatory Guides 1.177 An Approach For Plant-Specific, Risk-Informed Decision Making: Technical Specifications

[31] USNRC Regulatory Guides 1.178 An Approach For Plant-Specific Risk-Informed Decision Making For In-service Inspection Of Piping

2.3 Definitions

2.3.1 Design Basis

That information which identifies the specific functions to be performed by a structure, system, or component (SSC) of a nuclear installation, and the specific values or ranges of values chosen for controlling parameters as reference bounds for design. These values may be:

- restraints derived from generally accepted state of the art practices for achieving functional goals or
- requirements derived from analysis (based on calculations and / or experiments) of the effects of a postulated accident for which a structure, system, or component must meet its functional goals.

The design basis stipulates the following:

- the function of the SSC
- the fundamental process that satisfies the function
- essential SSC parameters of the stated functions and processes
- the basic safety margins to be included in the design
- interfaces with other SSCs
- accident and incident scenario expectations
- environmental considerations and impacts
- applicability of industry codes and standards

2.3.2 General Operating Rules (GOR)

These define the safety documentation that prescribes how the safety requirements described in the SAR are met. They include: Operating Technical Specifications (OTS), The Radiation Protection Standards 238-34 to 238-54, Safety Related Surveillance Manual (SRSM), Koeberg Chemistry Specifications (KCS), Emergency Plan, Koeberg Nuclear Power Station (KNPS) Management Manual (335-2) and Emergency Operating Procedures.

2.3.3 Unreviewed Safety Question (USQ)

An actual or potential Unreviewed Safety Question is determined to be involved if an evaluation determines that:

- the frequency of occurrence or the consequences of an accident or malfunction of equipment important to safety previously evaluated in the safety analysis documents results in a more than minimal increase;
- a possibility for an accident (or malfunction) of a different type with a different result than any evaluated previously in the safety analysis documents is created;
- the design basis limit for a fission product barrier is exceeded or altered, or the method of evaluation used in the design basis or accident analysis is altered.
- there is a more than minimal increase in baseline risk in the Koeberg Risk Assessment;
- there is or would be a more than minimal impact on the Emergency Operating Procedures, Severe Accident Management Guidelines or Emergency Plan.

Please note that this list is not exhaustive.

2.4 Abbreviations

Abbreviation	Explanation
ALARA	As Low As Reasonably Achievable
ALARP	As Low as Reasonably Practicable
CDF	Core Damage Frequency
DPSA	Deterministic, Probabilistic Safety Assessment
EDF	Electricité de France
EP	Emergency Planning
EPR	Engineering Problem Report
FMEA	Failure Modes and Effects Analysis
GOR	General Operating Rules
IAEA	International Atomic Energy Agency
INSAG	International Nuclear Safety Advisory Group
IPD-K	Integrated Plant Design-Koeberg
KCS	Koeberg Chemistry Specifications
NNR	National Nuclear Regulator
NOU	Nuclear Operating Unit
OTS	Operating Technical Specifications
PSA	Probabilistic Safety Analysis
QRA	Qualitative Risk Assessment
SAMG	Severe Accident Management Guidelines
SAR	Safety Analysis Report
SRSM	Safety Related Surveillance Manual
SSC	Systems, Structures or Components
USQ	Un-reviewed Safety Question

2.5 Roles and Responsibilities

The preparation of a Safety Case is the responsibility of the team project managing the activity that requires a Safety Justification. The Safety Justification may be performed by another person, but the project manager of the activity retains overall responsibility. The Koeberg Licensing Group is responsible for liaising with the NNR to establish the licensing strategy or approach to be adopted.

In the case of complex justifications a team may be required to produce the Safety Justification by providing inputs in the area of their particular expertise.

Reviewers, by signing the Safety Justification, signify that in their area of expertise they have conducted a thorough review of the justification and support its conclusions.

Personnel or teams performing the independent review must not have been involved in the production of the Safety Justification.

2.6 Process for Monitoring

The process for Monitoring is inherent to the review and approval process.

3. Contents of a Safety Justification

3.1 General

3.1.1 A Safety Justification is treated as an amendment to the existing design and licensing basis. Therefore, each element of the current safety analysis that is affected by the proposed change or new condition needs to be analysed and justified.

3.1.2 For cases where an existing, or potential USQ exists, the associated Safety Justification is argued under the headings as defined in Appendix 2 of KSA-066. Section 3.3 provides guidance for what information should be provided under these headings.

- Applicable to the preparation of nuclear Safety Justifications required as a result of:
  - ✓ a USQ as determined by a Safety Evaluation;
  - ✓ a condition needing a Justification for Continued Operation;
  - ✓ any other activity which has a potential impact on nuclear safety.
- Not applicable to:
  - ✓ plant or procedure changes that do not alter previously analysed limits as specified in OTS, the SRSM or KCS, or do not pose a USQ;
  - ✓ experiments or tests that do not alter previously analysed limits as specified in OTS, the SRSM, KCS or the SAR, or are contained in authorised procedures

3.2 Cover Page

In accordance with Appendix 1.

Reviews by the DPSA Group and Integrated Plant Design-Koeberg (IPD-K) are compulsory. Additional reviews by other relevant groups will be done if appropriate.

Specialist reviews may be required in the areas of Emergency Planning (EP) section and Accident Management for Design Extension conditions.

3.3 Headings

3.3.1 Executive Summary

- Description of Change - Give the purpose and background of the problem or change requiring the Safety Justification. Make reference to the Safety Evaluation and explain the existing or potential USQ.
- Motivation for Change - Give the reason why the change or new condition is being implemented or accepted.
- Conclusion - This should show that the objective of the Safety Justification has been adequately addressed, and through deterministic and probabilistic methods, the proposed change or new condition has been demonstrated to be safe. In addition, any

corrective actions required to support the conclusion of the Safety Justification should be included in this section. For Justifications for Continued Operation, the validity or lifetime of the Safety Justification should be clearly spelt out.

3.3.2 Applicable Regulations and Standards

- This section should identify those aspects of the design and licensing bases that may be affected by the proposed change or new condition, including, but not limited to, rules and regulations, Safety Analysis Report (SAR), Technical Specifications (OTS), licensing conditions, and licensing commitments.
- In general, applicable regulations and criteria can be found in relevant SAR chapters.
- Possible regulations and standards should not be confined to nuclear safety requirements. Other regulations and standards (e.g. industrial safety, health and environmental.) may also be applicable.

3.3.3 NNR Safety Criteria

Reference should be made to applicable NNR safety criteria referenced in the Koeberg Nuclear Licence.

3.3.4 Evaluations and Reviews

Reference should be made to applicable Safety Screenings, Safety Evaluations, Engineering Problem Reports (EPRs), etc. as well as to groups or individuals that have reviewed the Safety Justification.

3.3.5 Deterministic Analysis

3.3.5.1 Defence-in-Depth

Levels of defence (see SAR I-4.3.2.2.1 and IAEA SSR-2/1):

- the first level is provided by a maximum inherent ability of the station to function safely during normal operation, through conservative design and quality of fabrication,
- the second level is provided by postulating, despite the care taken with regard to the first level, a certain number of abnormal transients and incidents, and designing each unit with protection systems which are able to stop the development of an accident, and to place each unit in a safe shutdown condition,
- the third level is provided by postulating hypothetical accidents which may affect the integrity of fission product barriers.
- the fourth level is provided by the Emergency Operating Procedures for coping with design extension conditions, and the Severe Accident Management Guidelines.
- the fifth level is provided by the Emergency Plan:

  (1) The change or new condition should be consistent (individually and cumulatively) with defence-in-depth philosophy. In this regard the intent is to ensure that the philosophy of defence-in-depth is maintained, not to maintain the way defence-in-depth is achieved.

(2) The defence-in-depth philosophy has traditionally been applied in reactor design and operation to provide multiple means to accomplish safety functions and to prevent the release of radioactive material. It has been, and continues to be, an effective way to account for uncertainties in equipment and human performance.

(3) If a comprehensive risk analysis is done, the defence-in-depth philosophy can be used to help determine the appropriate extent of defence-in-depth (e.g. balance between core damage prevention, containment failure and consequence mitigation) to ensure protection of public health and safety.

(4) When a comprehensive risk analysis is not or cannot be done, traditional defence-in-depth considerations should be used or maintained to account for uncertainties. The justification should consider the intent of the general design criteria, national standards and engineering principles, such as the single failure criterion. Further, the Safety Justification should consider the impact of the proposed change on preventive and mitigative barriers to core damage, containment failure or bypass, and the balance among defence-in-depth attributes.

(5) Defence-in-depth consists of a number of elements as summarised below. These elements can be used as guidelines for making that assessment. Other equivalent acceptance guidelines may also be used.

(6) Consistency with the defence-in-depth philosophy is maintained if:

- A reasonable balance is preserved amongst prevention of core damage, prevention of containment failure, and consequence mitigation.
- Over-reliance on programmatic activities to compensate for weaknesses in plant design is avoided.
- System redundancy, independence and diversity are preserved, commensurate with the expected frequency, consequences of challenges to the system, and uncertainties (e.g. no risk outliers).
- Defences against potential common cause failures are preserved, and the potential for the introduction of new common cause failure mechanisms is assessed.
- Independence of barriers is not degraded.
- Defences against human errors are preserved.
- The intent of the General Design Criteria in 10CFR50 Appendix A is maintained as documented in SAR I-4.3.2.3.

3.3.5.2 Single Failure Criterion

Each of the safeguard systems is designed to tolerate a single failure during the period of recovery following an incident without loss of its protection function. This period of recovery consists of two segments, the short-term period and the long-term period.

During the short-term period, the single failure is limited to a failure of an active component in either the safeguard system or its support systems to perform its function as required. Should the single failure occur during the long-term period, rather than the short-term period, the safety related systems are designed to tolerate an active failure or a passive failure without loss of their protection function.

More details on the single failure criterion, as applied in Koeberg's design, can be found in SAR, sub-section I-4.3.2.2.2.

(1) The Safety Justification should assess whether the change or new condition has an impact on the Single Failure Criterion of the SSC(s) involved.

3.3.5.3 Safety Margins

(1) The Safety Justification should assess whether the impact of the change or new condition is consistent with the principle that safety margins are sufficiently maintained. Here also, the compiler is expected to choose the method of engineering analysis appropriate for evaluating whether sufficient safety margins would be maintained with the change or new condition. An acceptable set of guidelines for making that assessment is summarised below. Other equivalent acceptance guidelines may also be used.

(2) With sufficient safety margins:

- Codes and standards, or their alternatives, approved for use by the NNR are met.
- Safety analysis acceptance criteria in the design and licensing basis (e.g. SAR and supporting analyses.) are met, or proposed revisions provide sufficient margin to account for analysis and data uncertainty.

(3) The US NRC has developed application-specific guidelines reflecting this general guidance (Regulatory Guides 1.174 to 1.178).

3.3.5.4 Engineering Practice

(1) The scope and quality of the engineering analyses conducted to justify the proposed change or new condition should be appropriate for the nature and scope of the change, should be based on the as-built and as-operated and maintained plant, and should reflect relevant internal and external operating experience. Any engineering studies, use of codes and standards, etc. should be included in this section.

(2) Depending on the complexity and impact of the change or new condition, a Failure Modes & Effects Analysis (FMEA) may be appropriate. Such an analysis is conducted to ensure that malfunctions of any one component do not adversely affect the safety function or analysis of the system, or any interfacing systems, or if safety is adversely affected, that the effect is still considered to be safe. The impact on existing design base accident analyses needs to be identified and addressed.

(3) This section should also include details and show the acceptability of any compensatory actions or continued monitoring required to reduce the risk impact of the proposed change or new condition. In addition, consideration should be given to the development of an implementation and monitoring plan to ensure that the Safety Justification continues to reflect the actual reliability and availability of SSCs affected by the proposed change or new condition.

3.3.5.5 Radiological Safety

This section should show that any radiological safety implications associated with the change or new condition have been analysed and have been shown to be acceptable in terms of existing regulations and criteria.

3.3.5.6 ALARA and ALARP

(1) ALARA - The results of any ALARA review should be summarised here, including any compensatory actions that will be required to minimise doses to personnel, impact on the environment, etc.

(2) ALARP - The results of any cost benefit analyses of different solutions could be included here.

3.3.5.7 Accident Prevention and Mitigation

(1) This section should be used to show that the impact of the proposed change or new condition has been evaluated against applicable design basis accidents and assumptions and found to be acceptable.

(2) If there is an impact, then the results of new accident analyses should be summarised, including details of any new measures taken to prevent or mitigate the consequences of the accident(s).

(3) Analyses for preventing conventional (industrial) accidents could also be included in this section. This could include any contingency plans for problems experienced during or after implementation of the proposed change or new condition.

3.3.6 Probabilistic Safety Assessment

(1) Probabilistic Safety Assessment may be used to address the principle that proposed increases in Core Damage Frequency (CDF) and risk is small and remains within regulatory limits. The necessary sophistication of the evaluation, including the scope of the Probabilistic Safety Analysis (PSA) (e.g. internal events only and full power only.) depends to some extent on the contribution that the risk assessment makes to the integrated decision-making, which depends to some extent on the magnitude of the potential risk impact.

(2) For changes or new conditions that may have a more substantial impact, an in-depth and comprehensive PSA, appropriate to derive a quantified estimate of total impact, will be required to provide adequate justification.

(3) In other applications, calculated risk-importance measures, or bounding estimates, are adequate. In still others, a qualitative assessment (e.g. a QRA in accordance with 331-64) of the impact of the change or new condition on the plant's risk may be sufficient.

(4) The quality of a PSA used to support an application is measured in terms of its appropriateness with respect to scope, level of detail, and technical acceptability. The scope, level of detail, and acceptability of the PSA should be commensurate with the application for which it is intended, and the role the PSA results play in the integrated decision process. The more emphasis that is put on the risk insights and on the PSA results in the decision-making process, the more requirements have to be placed on the PSA in terms of both scope and how well the risk and the change in risk are assessed. Conversely, emphasis on the PSA scope, level of detail and technical acceptability can be reduced if the proposed change or new condition results in a risk decrease, or is very small, or if the decision could be based mostly on traditional engineering arguments, or if compensating measures are proposed such that it can be convincingly argued that the change in risk is very small.

(5) One over-riding requirement is that the PSA should realistically reflect the actual design, construction, operational practices, and operational experience of the plant.

3.3.7 Accident Management / Emergency Plan

(1) Accident Management - Analyses against the requirements of the Accident Analysis Manual (331-195) should be included in this section.

(2) Emergency Plan - This section should be used to show that the impact of the proposed change or new condition has been evaluated and found to be acceptable against the technical basis of the Emergency Plan. Any impact should be summarised, including details of any new measures taken to improve the effectiveness of the Emergency Plan.

3.3.8 Severe Accident Management

(1) This section should be used to show that the impact of the proposed change or new condition has been evaluated and found to be acceptable against applicable beyond-design basis accidents and assumptions.

(2) If there is an impact, then the results of new analyses should be summarised, including details of any new measures taken to prevent, or mitigate the consequences of the accident(s) [including required updates to Severe Accident Management Guidelines (SAMGS).

3.3.9 References

Details of all reference documents used to compile the safety justification should be included in this section. Where possible, details should also include unique identification numbers (in the case of national or international standards or regulations, the applicable year of issue should be mentioned).

3.3.10 Attachments

Details of all attachments to the safety justification should be listed in this section. Such attachments could include calculation sheets, stress analysis printouts, PSA assessments.

3.3.11 "Tools" that can be used in the Process of Performing Safety Justifications

- PSA
- EPR
- World / EDF experience and standards
- Computational codes (e.g. thermohydraulic, mechanical and civil)
- Expert judgement (based on qualification)

4. Acceptance

This document has been seen and accepted by:

Name	Designation
Isaac Malgas	Middle Manager – Engineering
H Bosman	Senior Engineer – DPSA
Ravid Goldstein	Middle Manager – Engineering

5. Revisions

Date	Rev.	Compiler	Remarks
July 2021	1	A Rijnsburger	Procedure updated to new 240-156067953 document format. Safety Screening S11003.

6. Development Team

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

- Cate Pretorius
- Mvuseleli Hermanus
- Arij Rijnsburger

7. Acknowledgements

Not Applicable

Appendix 1 – Cover Page Format

Rev		Page	

KOEBERG NUCLEAR POWER STATION

SAFETY JUSTIFICATION NO: ______________________________

TITLE: ____

____

____

Prepared by: _________________________

Reviewed by: _________________________

IPD-K Review: _________________________

Risk Review: _________________________

Approved by: _________________________

Date: _________________________