Eskom	**Manual**	**Nuclear Engineering**

Title: **Koeberg Accident Analysis Manual**

Document Identifier:	**331-195**
Alternative Reference Number:	**GGM-0907**
Area of Applicability:	**Nuclear Engineering**
Functional Area:	**NAS**
Revision:	**3**
Total Pages:	**70**
Disclosure Classification:	**Controlled Disclosure**

Compiled by	**Functional Responsibility**	**Authorized by**
Khoza	LJ Mahlangu	
	L Mahlangu	**I Sekoko**
Snr Physicist	**DPSA Manager**	**Middle Manager NAS**
Date: 2023-03-31	Date: 2023-03-31	Date: 2023-10-02

Nuclear Additional Classification Information

Business Level:	**3**
Working Document:	**3**
Importance Classification:	**CSR (S12185)**
NNR Approval:	**Yes**
Safety Committee Approval:	**No**
ALARA Review:	**No**
Functional Control Area:	**Nuclear Analysis and Siting**

Content

Page

Figures

Tables

1. Introduction

This manual describes the process for performing accident analyses for Koeberg Nuclear Power Station. It ensures that the appropriate methodologies, acceptance criteria and assumptions are used, and provides a licensing framework for Severe Accident Management Guidelines and associated plant modifications.

The nuclear safety criteria of ANS N-18.2 [1] were applied to Koeberg Nuclear Power Station during the design and construction phases. For this reason, ANS N-18.2 [1] is the default standard that shall be applied for all accident analysis and design purposes. Further information on the use of standards and the development of Dose Acceptance Criteria is provided in Section 3.5 and Appendix A.

The position of ANS N-18.2 [1] regarding the responsibilities of an owner or designer of a Pressurised Water Reactor (PWR) is of fundamental importance, and is quoted below:

> *"Ritualistic adherence to the criteria may not suffice for satisfying the requirement of assuring public health and safety. An owner or designer of a PWR has a responsibility, even at the design stage that goes beyond the degree of safety afforded by these criteria."*
>
> *"In certain areas there may now exist a capability of setting out more detailed criteria…"*

In acknowledgment of the above position, Eskom has adopted additional approaches, developed after the issue of ANS N-18.2 [1], which shall be applied over and above the mandatory requirements of ANS N-18.2 [1]. These additional approaches are also described in this document.

Conditions more complex and/or more severe than those postulated as design basis accidents (DBAs) can occur. These conditions shall be investigated as Design Extension Conditions (DEC) so that any reasonably practicable measures to improve the level of safety of a plant, compared to the level reached with the design basis, are identified and implemented.

The concept of Beyond Design Basis Accidents (BDBA) have evolved since Fukushima to be replaced by Design Extension Conditions (DEC) as part of Defence in Depth (DiD) [24], summarised in Appendix B [59]. The manual adopts the International Atomic Energy Agency (IAEA) approach on extending the DiD to include DECs. Together with DECs the concept of practical elimination is also adopted to deal with those accidents which are considered impossible or extremely unlikely to occur. This enhances the plant's capability to withstand more severe events or conditions than those considered in the design basis to further minimise the radiological releases harmful to the public and the environment as far as reasonably practicable. Other established, international assumptions and methods, justified by Eskom and accepted by the National Nuclear Regulator (NNR), may be incorporated.

2. Supporting Clauses

2.1 Scope

2.1.1 Purpose

The purpose of this manual is to provide the requirements and the process that shall be used for analysing accidents, whether design basis or design extension conditions. It provides guidance for this analysis and for when the plant is to be modified to prevent or mitigate the consequences of such an accident. This manual also provides guidance for identifying the process to be followed to determine the relevant design and nuclear safety criteria and the analyses required to be performed.

This manual includes all the approaches to and requirements for accident analysis in addition to those of the default standard, ANS N-18.2 [1].

This manual provides the licensing framework for accident related issues which include severe accident management guidelines and the emergency plan. Following the guidance in this manual will ensure that related licensing submissions address all the relevant safety issues in a systematic manner.

2.1.2 Applicability

This manual is applicable to all accident management related activities and accident analyses performed for Koeberg Nuclear Power Station. It shall be used in conjunction with the safety justification procedures, KSA-066 [15] and KGA-029 [28], and the safety evaluation process, KAA-709 [27].

The primary focus of this manual is directed at the reactor cores and spent fuel storage facilities, currently the spent fuel pools and dry cask facilities. The analysis of other radioactive sources should be done in accordance with RG-0019 [32].

2.1.3 Effective Date

This document shall be effective from the authorisation date.

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] ANSI/ANS N-18.2 (1973), Nuclear safety criteria for the design of stationary Pressurised Water Reactor plants

[2] ANSI/ANS-51.1 (1983), Nuclear Safety Criteria for the Design of Stationary Pressurized Water Reactor Plants

[3] ANSI/ANS-57.2 (1983), Design Requirements for Light Water Reactor Spent Fuel Storage Facilities at Nuclear Power Plants

[4] ANSI/ANS-58.21 (2007), External Events PRA Methodology

[5] ANSI/ANS-58.22 (2009), Low Power and Shutdown PRA Methodology, Draft

[6] ANSI/ANS-58.8 (1994), Time Response Design Criteria for Safety-Related Operator Actions

[7] ANSI/ANS-58.9 (1981), Single Failure Criteria for Light Water Reactor Safety-Related Fluid Systems

[8] ASME/ANS RA-Sa–2009 (2009), Standard for Level 1/Large Early Release Frequency Probabilistic Risk Assessment for Nuclear Power Plant Applications

[9] ASME/ANS-58.25 (2010), Radiological Accident Offsite Consequence Analysis (Level 3 PRA) to Support Nuclear Installation Applications, Draft

[10] IAEA General Safety Requirements Part 3 No. GSR Part 3 (2014), International Basic Safety Standards for Protection against Ionizing Radiation and for the Safety of Radiation Sources

[11] IAEA Safety Standards, Specific Safety Guide No. SSG-2 (2019), Deterministic Safety Analysis for Nuclear Power Plants

[12] INPO 09-003 (2009), Excellence in the Management of Design and Operating Margins

[13] KAA-811, The Integrated Koeberg Nuclear Emergency Plan

[14] KBA 00 22E 00 006, Nuclear Steam Supply System Design Transients

[15] KSA-066, Standard for Nuclear Design and Licensing Basis Evaluation

[16] NNR Letter k12131N, “Koeberg Nuclear Power Station: Technical Basis for the Koeberg Emergency Plan”, 17 July 2000

[17] NNR Letter k12131.1N, “Koeberg Nuclear Power Station: Technical Basis for the Koeberg Emergency Plan”, 28 February 2005

[18] RCC-P, Design and Construction Rules for System Design of 900 MWe PWR Nuclear Power Plants, Revision 4 – September 1991, Modified 1995

[19] RD-014, Emergency Preparedness and Response Requirements for Nuclear Installations

[20] RG-0016, Guidance on the Verification and Validation of Evaluation and Calculation Models used in Safety and Design Analyses

[21] RD-0022, Radiation Dose Limitation at Koeberg Nuclear Power Station

[22] RD-0024, Requirements on Risk Assessment and Compliance with principal Safety Criteria for Nuclear Installations compliance with the safety criteria of the NNR

[23] Regulations No. R. 388 (28 April 2008) in terms of Section 26, read with Section 47 of the National Nuclear Regulator Act (Act No. 47 of 1999) on Safety Standards and Regulatory Practices

[24] IAEA Safety Standards, Specific Safety Requirements No. SSR-2/1 (Rev. 1) (2016), Safety of Nuclear Power Plants: Design

[25] IAEA-TECDOC-1982, Current Approaches to the Analysis of Design Extension Conditions with Core Melting for New Nuclear Power Plants

[26] IAEA Safety Glossary, Terminology Used in Nuclear Safety and Radiation Protection, 2018

[27] KAA-709, Process for Performing Safety Evaluations, Screenings, and Safety Justifications

[28] KGA-029, Safety Justification Preparation

[29] Koeberg Safety Analysis Report

[30] Safety Analysis Report; EDF – 900 MWe Series – Accident Design Rules, Volume III, Chapter 4, Section 3.1

[31] NUREG-0800, U.S. NRC Standard Review Plan Section 4.2, "Fuel System Design" (2007)

[32] RG-0019, Interim Guidance on Safety Assessments of Nuclear Facilities, Rev 0

2.2.2 Informative

[33] ICRP Publication 68 (1994), Dose Coefficients for Intake of Radionuclides by Workers

[34] ICRP Publication 72 (1996), Age-dependent Doses to Members of the Public from Intake of Radionuclides

[35] ICRP Publication 26 (1977), Recommendations of the International Commission on Radiological Protection

[36] Radiological Protection.KGA-003, Guide for Classification of Plant Components, Structures and Parts

[37] 331-64, Guideline for Safety and Production Issue Categorisation

[38] OCDE / GD (97) 198 (1997), Level 2 PSA Methodology and Severe Accident Management

[39] U.S. NRC Regulatory Guide 1.183 (2000), Alternative Radiological Source Terms for Evaluating Design Basis Accidents at Nuclear Power Reactors

[40] U.S. NRC Regulatory Guide 1.196 (2003), Control Room Habitability at Light-Water Nuclear Power Reactors

[41] U.S. NRC Regulatory Guide 1.203 (2010), Transient and Accident Analysis Methods

[42] 10 CFR Part 50.67, Accident Source Term

[43] 10 CFR Part 100.11, Determination of Exclusion Area, Low Population Zone, and Population Center Distance.

[44] ICRP Publication 60 (1991), 1990 Recommendations of the International Commission on Radiological Protection

[45] Oak Ridge National Laboratory, http://www2.epa.gov/radiation/tools-calculating-radiation-dose-and-risk#tab-3 – DC_PAK3.02 software package, DCPAK 3.02 Abstract and User Guide to DCFPAK 3

[46] PNNL-18212 Rev. 1 (2011), Update of Gap Release Fractions for Non-LOCA Events Utilizing the Revised ANS 5.4 Standard

[47] U.S. NRC Staff Memorandum (26 July 2011), Technical Basis for Revised Regulatory Guide 1.183 (DG-1199) Fission Product Fuel-to-Cladding Gap Inventory (ADAMS Accession Number ML111890397)

[48] U.S. NRC Draft Regulatory Guide DG-1199 (2009), Alternative Radiological Source Terms for Evaluating Design Basis Accidents at Nuclear Power Reactors

[49] PSA-R-T16-18, Alternative Source Term (AST) Framework Document

[50] WENRA Safety Reference Levels for Existing Reactors (2020)

[51] WENRA Practical Elimination Applied to New NPP Designs – Key Elements and Expectations (2019)

[52] IAEA Safety Standards, Fundamental Safety Principles, No SF-1, 2006

[53] IAEA General Safety Requirements Part 2 No. GSR Part 2 (2016), Leadership and Management for Safety

[54] U.S. NRC Staff Memorandum (16 March 2015), Technical and Regulatory Basis for the Reactivity-Initiated Accident Interim Acceptance Criteria and Guidance, Revision 1 (ADAMS Accession Number ML14188C423)

[55] NUREG-1465 (1995), Accident Source Terms for Light Water Nuclear Power Plants.

[56] U.S. AEC (now U.S. NRC) TID-14844 (1962), Calculation of Distance Factors for Power and Test Reactor Sites.

[57] U.S. NRC Federal Register 61 FR 65157 (11 December 1996), Reactor Site Criteria Including Seismic and Earthquake Engineering Criteria for Nuclear Power Plants.

[58] U.S. NRC SECY-98-289 (15 December 1998), Proposed Amendments to 10 CFR Parts 21, 50, and 54 Regarding Use of Alternative Source Terms at Operating Reactors.

[59] IAEA-TECDOC-1791, Considerations on the Application of the IAEA Safety Requirements for the Design of Nuclear Power Plants

[60] EMB-895, Design Extension Condition Specifications and Surveillances

[61] IAEA Safety Report Series No. 52, Best Estimate Safety Analysis for Nuclear Power Plants: Uncertainty Evaluation, 2008

2.3 Definitions

2.3.1 Accident

Any unintended event, including operating errors, equipment failures and other mishaps, the consequences or potential consequences of which are not negligible from the point of view of protection and safety.

2.3.2 Acceptance Criteria

Acceptance criteria are used in deterministic safety analysis to assist in judging the acceptability of the results of the analysis as a demonstration of the safety of the nuclear power plant. The acceptance criteria can be expressed in general, qualitative terms or as quantitative limits. Three categories of criteria are recognized:

- Safety criteria: Criteria that relate either directly to the radiological consequences of operational states or accident conditions, or to the integrity of barriers against releases of radioactive material, with due consideration given to maintaining the safety functions.
- Design criteria: Design limits for individual structures, systems and components, which are part of the design basis as important preconditions for meeting safety criteria (see Requirement 28 of SSR-2/1 (Rev. 1) [1]).
- Operational criteria: Rules to be followed by the operator during normal operation and anticipated operational occurrences, which provide preconditions for meeting the design criteria and ultimately the safety criteria.

2.3.3 Analytical Margin

The difference between the analysed design limit and the ultimate capability or failure limit. This is typically an unanalysed region that cannot be used unless an analysis is performed to establish a new analysed design limit. Analytical margin consists of conservative assumptions and methodologies used to account for uncertainties in design, materials or fabrication. In some cases, an exact value for this margin cannot be specifically determined.

2.3.4 Analysed Design Limit

The limiting condition of a system or component from an engineering perspective. This value is typically found in engineering calculations and includes design margin. This provides a boundary that describes the analysed condition.

2.3.5 Beyond Design Basis External Events

Two levels of external hazards should be considered in the design and evaluation of SSC important to safety that are subjected to external events. The first level is the traditional design basis external events, and the second level is the Beyond Design Basis External Events (BDBEE). The frequency of exceedance of design basis events should be low enough that the design measures applied ensures a high degree of protection against external hazards. Beyond design basis external events intensities are defined at a level greater than the design basis external event in order to both ensure that there are no cliff-edge effects with respect to extreme hazards, and the plant design and mitigation strategies are capable of withstanding extreme events.

2.3.6 Cliff-Edge Effects

In a nuclear power plant, an instance of severely abnormal plant behaviour caused by an abrupt transition from one plant status to another following a small deviation in a plant parameter, and thus a sudden large variation in plant conditions in response to a small variation in an input, (IAEA Safety Glossary, 2018 [26]).

2.3.7 Coincident Occurrence

A simultaneous independent or low probability dependant occurrence other than single failure of nuclear safety-related equipment, common cause failures and multiple failures in nuclear safety-related equipment.

2.3.8 Common Cause Failure

Multiple failures of Structures, Systems and Components (SSCs) as a result of a single phenomenon.

2.3.9 Current Licensing Basis

Refers to the safety case applicable at any time during operation of the plant and all license-binding documentation and NNR licence documents.

2.3.10 Credible Combinations of Events

Those combination of events where it is considered that the multiple events could occur simultaneously, this would include:

- events induced by other events e.g. explosion creating fires;
- events that are typically co-related, e.g. high wind and heavy rain;
- relatively common events or long duration events that could occur simultaneously with a rare or other common event e.g. drought, jellyfish ingress.

Two or more independent rare events would typically not be considered a credible combination.

2.3.11 Design Basis

The range of conditions and events taken explicitly into account in the design of a facility, according to established acceptance criteria, such that the facility can withstand them without exceeding authorised limits by the planned operation of safety systems.

2.3.12 Design Basis Accidents (DBAs)

Accident conditions against which a nuclear power plant is designed according to established design criteria, and for which the damage to the fuel and the release of radioactive material are kept within authorised limits [11].

2.3.13 Design Extension Conditions

Postulated accident conditions that are not considered for design basis accidents, but that are considered in the design process of the facility in accordance with best estimate methodology, and for which releases of radioactive material are kept within acceptable limits. DECs are further subdivided into two categories, namely DEC without significant fuel degradation (DEC-A) and DEC with core melting (DEC-B) [26].

2.3.14 Design Margin

The difference between the analysed design limit and the operating limit. Design margin accounts for the following:

- design assumptions used in calculations;
- equipment tolerances such as pipe wall thickness, structural component dimensions and electrical relay actuation times;
- instrumentation tolerances;
- calculation round-off;
- allowance for degraded equipment performance.

2.3.15 Deterministic Safety Analysis

The deterministic safety analysis is used to confirm that safety functions can be fulfilled and that the necessary structures, systems and components, in combination with operator actions, are effective in keeping the releases of radioactive material from the plant below acceptable limits.

2.3.16 Expert Judgment

Information provided by a technical expert, in the expert's area of expertise, based on opinion or on an interpretation based on reasoning that includes evaluations of theories, models or experiments, (ASME/ANS RA-Sa-2009 [8]).

2.3.17 Extremely Unlikely with A High Degree of Confidence

The demonstration that an accident is extremely unlikely with a high degree of confidence should take account of the assessed frequency of the condition and of the degree of confidence in the assessed frequency. The uncertainties associated with the data and methods should be evaluated, including the use of sensitivity studies, in order to underwrite the degree of confidence claimed. The demonstration should not be claimed solely based on compliance with a general cut-off probabilistic value. Probabilistic and deterministic elements both are required for this demonstration.

It should be ensured that the provisions relied upon to demonstrate the extreme unlikeliness remain in place and valid throughout the plant lifetime. For example, in-service inspection and other periodic checks may be necessary.

All analytical methods applied should be validated against the specific phenomena in question, and verified [26].

2.3.18 External Hazards

Hazards or events unconnected with the operation of a facility or the conduct of an activity that could have an effect on the safety of the facility or activity. External hazards includes both natural and external human induced hazards, that could pose a threat to a nuclear plant [26].

2.3.19 Human Induced Hazards

These human induced external events are generated external to the plant or nuclear facility, that could pose a risk to the facility, such as aircraft crashes, explosions and large fires [26].

2.3.20 Independent Review

This is a complete review by authorised and technically competent personnel who have not participated in the development and are not responsible for the original compilation.

2.3.21 Limited Protective Measures

Limited protective measures [26] include:

- The offsite radiological impact of accidents that are not practically eliminated should only lead to limited protective measures in area and time.

- There should be no permanent human relocation, no long term restrictions in food consumption, no need for emergency evacuation outside the immediate vicinity of the nuclear facility, or only limited sheltering required.
- Iodine prophylaxis should only be limited in area and time
- Sufficient time should be available to implement these measures.

2.3.22 Low Population Zone

An area of low population density often required around a nuclear installation before it's built. The number and density of residents is of concern in emergency planning so that certain protective measures (such as notifications and instructions to residents) can be accomplished in a timely manner.

2.3.23 Margin

Conservatism included in operational limits and the design of every system, structure and component in a nuclear plant. In qualitative terms, margin is the difference between the actual (or predicted) and required performance of a component, system or structure. This conservatism may also be present in the analyses for an entire safety function.

2.3.24 Natural Hazards

These are all natural hazards that might affect the plant or facilities on the site, such as geological hazards, meteorological hazards, hydrological hazards and biological phenomena [26].

2.3.25 Operating Limit

The maximum or minimum operating value imposed on the operation of the system for a particular parameter. The limit is normally specified in facility configuration information (drawings, specifications, and databases) or included in technical specifications.

2.3.26 Operating Margin

The difference between the extreme of the normal operating range and the designed operating limit of the system. The Operations Department operates the plant within a range of normal operating limits

2.3.27 Practical Elimination

The possibly of the potential occurrence of certain hypothetical events sequences in scenarios could be considered to be excluded, practically eliminated, provided that it would be physically impossible for the relevant event sequences to occur or that these sequences "*could be considered with a high level of confidence to be extremely unlikely to arise*", (IAEA Safety Glossary, 2018 [26]).

2.3.28 Qualified Expert

An individual who, by virtue of certification by appropriate boards or societies, professional licences or academic qualifications and experience, is duly recognized as having expertise in a relevant field of specialization, e.g. medical physics, radiation protection, occupational health, fire safety, quality management or any relevant engineering or safety specialty, (IAEA No. GSR Part 3 [10]).

2.3.29 Radiological Dose Criteria

Radiological dose criteria, which relate to radiological consequences of plant operational states or accident conditions. These are usually expressed in terms of activity levels or doses, and are typically defined by law or by regulatory requirements.

2.3.30 Range of Normal Operation

Parameter range in which the system or component is normally operated. Typically, an alarm or an annunciation is in place that requires operator action if the range of normal operations is exceeded.

2.3.31 Safe Plant State

Plant state, following an anticipated operational occurrence or accident conditions, in which the reactor is subcritical and the fundamental safety functions can be ensured and maintained stable for a long time (IAEA, SSR 2/1).

2.3.32 Safety Analysis

This is part of the overall safety assessment, that is part of the systematic process that is carried out throughout the lifetime of the facility to ensure that all the relevant safety requirements are met by the proposed design (IAEA, SSR 2/1).

2.3.33 Severe Accident

An accident more severe than a design-basis accident which involves significant core degradation or significant fuel degradation in the spent fuel pool. The severity of the severe accident depends on the degree to which fuel is damaged and on the degree to which containment integrity is lost. The focus of a severe accident is to limit the release from the facility, such as protecting the containment building, in the case of the reactors. It reflects not only the ultimate internal condition of the plant, but also the extent of the radiological impact on the environment [26].

2.3.34 Single Failure Criterion

A failure that results in the loss of capability of a system or component to perform its intended safety function(s) and any consequential failure(s) that result from it. The single failure criterion is a criterion (or requirement) applied to a system such that it must be capable of performing its task in the presence of any single failure.

In the single failure analysis it may not be necessary to assume the failure of a passive component designed, manufactured, inspected and maintained in service to an extremely high quality, provided that it remains unaffected by the postulated initiating event. However, when it is assumed that a passive component does not fail, such an analytical approach should be justified, with account taken of the loads and environmental conditions, as well as the total period of time after the initiating event for which functioning of the component is necessary.

2.3.35 Technical Acceptance Criteria

The technical acceptance criteria, which relate to the integrity of barriers to releases of radioactive material (e.g. the fuel matrix, fuel cladding, reactor coolant system pressure boundary and containment). These are defined in regulatory requirements, or proposed by the designer subject to regulatory acceptance, for use in the safety demonstration.

2.3.36 Ultimate Capability

The point at which functional failure would be expected to occur in a system or component. This point is expected to be well above the analysed design limit, although the exact point of functional failure may be indeterminate.

2.4 Abbreviations

Abbreviation	Explanation
AST	Alternative Source Term
BDBA	Beyond Design Basis Accident
CEDE	Committed Effective Dose Equivalent
CFR	Code of Federal Regulations
CM	Calculation Model
DBA	Design Basis Accident
DEC	Design Extension Condition
DEC-A	Design Extension Condition without core melt (i.e. significant fuel degradation)
DEC-B	Design Extension Condition with core melt (i.e. severe accidents)
DDE	Deep Dose Equivalent
DiD	Defence in Depth
DNBR	Departure from Nucleate Boiling Ratio
EAB	Exclusion Area Boundary
ECA	Emergency Contingency Action (procedures)
ECC	Emergency Control Centre
EDE	Effective Dose Equivalent
EM	Evaluation Model
EMDAP	Evaluation Model Development and Assessment Process
EOP	Emergency Operating Procedure
EP	Emergency Plan
EPA	Environmental Protection Agency
FRP	Functional Restoration Procedure
IAEA	International Atomic Energy Agency
IE	Initiating Events
ICRP	International Commission on Radiological Protection
KNPS	Koeberg Nuclear Power Station
LOCA	Loss of Coolant Accident
LPZ	Low Population Zone
MSLB	Main Steam Line Break
NNR	National Nuclear Regulator
NRC	Nuclear Regulatory Commission
NSSS	Nuclear Steam Supply System
OE	Operating Experience
OTS	Operating Technical Specifications
PIE	Postulated Initiating Events
PRA	Probabilistic Risk Assessment (equivalent to PSA)

Abbreviation	Explanation
PSA	Probabilistic Safety Assessment
PSR	Periodic Safety Review
PWR	Pressurised Water Reactor
RAR	Risk Analysis Report
RIA	Reactivity Initiated Accident
SAM	Severe Accident Management
SAMGs	Severe Accident Management Guidelines
SAR	Safety Analysis Report
SBO	Station Blackout
SGTR	Steam Generator Tube Rupture
SRA	Safety Re-Assessment
SRSM	Safety Related Surveillances Manual
SSC	Structures, Systems and Components
TEDE	Total Effective Dose Equivalent
TSC	Technical Support Centre
U.S.	United States

2.5 Roles and Responsibilities

2.5.1 Nuclear Engineering Manager

The Nuclear Engineering Manager shall be responsible for the overall policies, standards, codes and practices related to the design of Koeberg Nuclear Power Station. This includes all safety analysis related to design basis accidents, design extension conditions, severe accidents, development of accident analysis procedures, deterministic and probabilistic safety analysis and the overall implementation thereof.

2.5.2 Koeberg Engineering Manager

The Senior Manager, Koeberg Engineering, shall be responsible for ensuring the development and management of accident procedures, including severe accidents, management and mitigation strategies and the bases thereof.

2.5.3 Safety Case Manager

The Safety Case Manager shall be responsible for the overall Safety Case and the Safety Analysis Report (SAR) for Koeberg, as well as for developing accident management procedures, including management and mitigation strategies, severe accidents and ensuring that all accidents covered within the scope of this manual are adequately integrated into the SAR.

2.5.4 Nuclear Analysis and Siting Manager

The Nuclear Site and Analysis Manager is responsible for conducting and documenting both the deterministic and probabilistic accident analysis for the plant, including the verification of its quality and completeness.

2.6 Process for Monitoring

The Koeberg Accident Analysis Process described in Section 3.1 shall be utilised to identify any deviations in the accident management related activities and accident analyses performed for Koeberg Nuclear Power Station. It shall be used in conjunction with the safety justification procedures, KSA-066 [15] and KGA-029 [28], and the safety evaluation process, KAA-709 [27], and any corrective actions shall be implemented as appropriate. The manual shall be updated / reviewed as and when the need arises to ensure its effectiveness by means of self-assessments and other appropriate tools and concurrence on such updates shall be made with the NNR. The analyses performed in accordance with this manual shall be carried out by competent personnel under controlled conditions using approved current procedures, instructions, drawings or other appropriate means that are periodically reviewed to ensure their adequacy and effectiveness.

The Periodic Safety Review (PSR) should review both the deterministic and probabilistic accident analyses to confirm that the accident analyses are comprehensive, in line with regulations and latest international norms.

2.7 Related/Supporting Documents

Not applicable

3. Deterministic Accident Analysis

The Fundamental Safety Principles establish one fundamental safety objective and ten safety principles that provide the basis for requirements and measures for the protection of people and the environment against radiation risks and for the safety of facilities and activities that give rise to radiation risks.

This fundamental safety objective has to be achieved, and the ten safety principles have to be applied, without unduly limiting the operation of facilities or the conduct of activities that give rise to radiation risks. To ensure that nuclear power plants are operated, and activities are conducted to achieve the highest standards of safety that can reasonably be achieved, measures have to be taken to achieve the following:

(a) To control the radiation exposure of people and radioactive releases to the environment in operational states;

(b) To restrict the likelihood of events that might lead to a loss of control over a nuclear reactor core, nuclear chain reaction, radioactive source, spent nuclear fuel, radioactive waste or any other source of radiation at a nuclear power plant;

(c) To mitigate the consequences of such events if they were to occur.

The deterministic safety analyses for a nuclear power plant predict the response to Postulated Initiating Events (PIE), hereafter referred to initiating events (IE). The analysis of these IE is performed in accordance with a specific set of rules and acceptance criteria is applied. Acceptance criteria are used in deterministic safety analysis to assist in judging the acceptability of the results of the analysis as a demonstration of the safety of the nuclear power plant. Typically, these focus on neutronic, thermohydraulic, radiological, thermo mechanical and structural aspects, which are often analysed with different computational tools.

Deterministic safety analysis shall mainly provide:

- Establishment and confirmation of the design basis for all items important to safety;
- Characterisation of the PIE that are appropriate for the site and the design of the plant;
- Analysis and evaluation of event sequences that result from PIE, to confirm the qualification requirements;
- Comparison of the results of the analysis with acceptance criteria, design limits, dose limits and acceptable limits for purposes of radiation protection;
- Demonstration that the management of anticipated operational occurrences and design basis accidents is possible by safety actions for the automatic actuation of safety systems in combination with prescribed actions by the operator.

The DEC analysis [50] shall:

- rely on methods, assumptions or arguments which are justified, and should not be unduly conservative;
- be auditable, paying particular attention where expert opinion is utilized, and take into account uncertainties and their impact;
- identify reasonably practicable provisions to prevent severe fuel damage (DEC-A) and mitigate severe accidents (DEC-B);
- evaluate potential on-site and off-site radiological consequences resulting from the DEC (given successful accident management measures);
- consider plant layout and location, equipment capabilities, conditions associated with the selected scenarios and feasibility of foreseen accident management actions;
- demonstrate, where applicable, sufficient margins to avoid “cliff-edge effects” that would result in unacceptable consequences; i.e. for DEC-A severe fuel damage and for DEC-B a large or early radioactive release;
- reflect insights from PSA level 1 and 2;
- take into account severe accident phenomena, where relevant and
- define an end state, which should where possible be a safe state, and, when applicable, associated mission times for SSCs.

3.1 Process for Analysing Accidents

The following process has been developed to ensure that a consistent and comprehensive approach is followed whenever:

- analysing an accident;
- modifying the plant, procedures and documents used to prevent an accident or mitigate the consequences of an accident;
- developing a safety case to demonstrate that the plant meets its design and safety criteria.

The Accident Analysis Process Chart (**Figure 1: Accident Analysis Process Chart**) is based on the SAR [29], ANS N-18.2 [1], ANSI/ANS-51.1 [2] and RCC-P [18] with insights from IAEA standards on safety analysis. Each applicable step in the Chart presented in a solid-lined box, shall be addressed. The Chart includes references to the relevant sections of this manual. The order is not important. However, the safety case shall cover all the relevant steps.

The anticipated frequency or probability of occurrence of the single initiating event, informed by available Operating Experience (OE), is a principal factor in determining how the accident shall be analysed. Guidance on determining this is given in Section 3.2. If the probability of occurrence falls within the probability of existing DBAs, the accident shall be analysed as such against the relevant safety criteria using conservative assumptions, applying the single failure criterion to demonstrate compliance with ANS N-18.2 [1] performance criteria. ANS-58.9 [7] provides additional guidance on the application of the single failure criterion. The plant design shall be capable of accommodating appropriate coincident occurrences. Examples of coincident occurrences include loss of offsite power and a stuck control rod assembly. The methodology employed for design basis accident analysis may be conservative, best estimate or combined analysis and shall demonstrate an overall conservative evaluation. Best estimate analysis shall include an evaluation of the uncertainties. Detail is given in Section 3.3. A design review of the plant (if required) shall be made against the design criteria associated with the relevant plant condition. Detail is provided in Section 3.5. The risk criteria as detailed in Section 4.1 shall, at all times, be respected. The deterministic analysis shall therefore be complemented by a probabilistic risk assessment depending on the type of analysis.

If the design and nuclear safety criteria cannot be met with the current plant design, a plant modification or procedure change shall be considered. The Safety Evaluation process will be followed in these cases to ensure the modification does not compromise the plant design basis. If a modification in accordance with the design base criteria is not feasible to meet the relevant design criteria, a specific case shall be made in the Safety Justification and approved by the Licensing Authority, taking credit for alternative measures, such as operating procedures, training, different design criteria and operating experience.

The original ANSI 18.2 based deterministic approach does not include explicit consideration of multiple failures in nuclear safety-related equipment and common cause failures. However, it is important to recognise that multiple failures in nuclear safety-related equipment (other than an initiating occurrence and a single failure) can occur. Through DEC, additional analyses or provisions are required to ensure that the probability and consequence of identifiable multiple failures in nuclear safety-related equipment or common cause failure using the process discussed under Section 3.2.5 are acceptably low.

However, for DECs the design basis as well as accident mitigation strategies such as provided in the EOP and SAMGs can be considered. Also, for DECs credit can be taken for mitigation as well, including portable equipment (where demonstrated to be deployable timeously), beyond design base accident procedures (i.e. ECA, FRP and SAMGs), or alternative mitigation that may not have been part of the original design consideration. Furthermore, it should be borne in mind that the public and worker risks must always comply with the criteria in RD-0024 [22] and the public and worker doses must comply with the criteria of Table 3.

Confirmation is required in the Safety Evaluation process that the additional design provisions for DECs do not compromise the design basis of the plant.

An evaluation shall be conducted to determine whether significant impact on the technical bases for the Emergency Plan (EP) exists [13]. If it is determined that this impact is significant, changes to the plant, its operating procedures and training should be considered. If this is not practicable then changes to the EP shall be implemented. If the changes cannot be effected, an alternative method of addressing the impact shall be developed and implemented.

SAMGs have been specifically developed to give the operating staff and technical support staff guidance on how to deal with severe accidents. If the evaluation of a specific severe accident (category of DECs) intervention shows that the intervention may not maintain the plant in a safe and stable state, 'severe accident' modifications may be required. Section 3.5 details the relevant nuclear safety and design criteria against which the modification shall be designed. Confirmation is required in the Safety Evaluation process that the severe accident modifications do not compromise the design basis of the plant.

The assumptions used in the deterministic and probabilistic safety analyses are detailed in Sections 3.4 and 4.2.

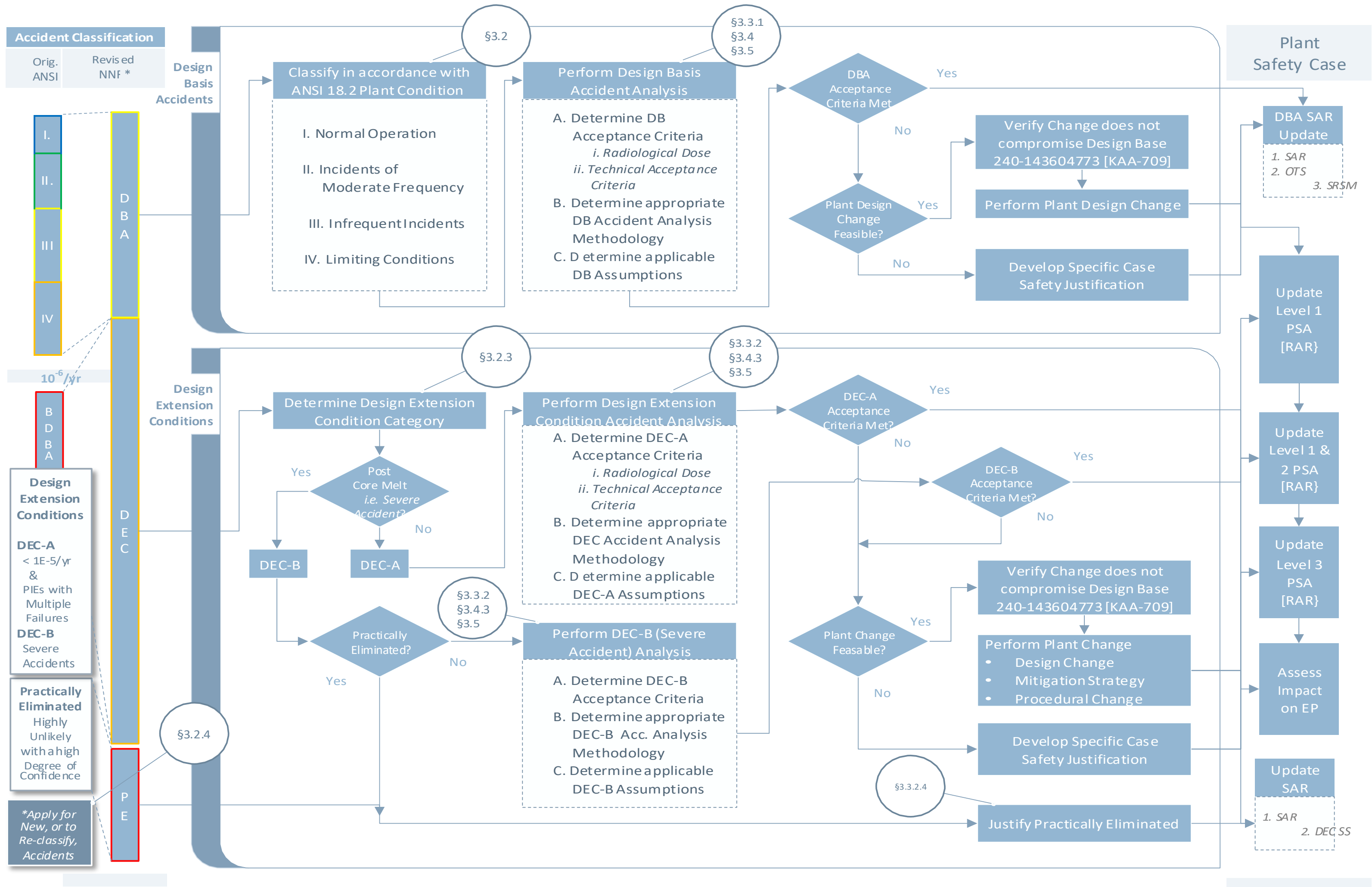


Figure 1: Accident Analysis Process Chart

3.2 Categorisation of Plant Conditions

3.2.1 Introduction

In accordance NNR RG-0019 [32] and IAEA, with the definition of plant states (considered in design) from IAEA SSR-2/1 (Rev. 1) [24], the plant states considered in the deterministic safety analysis should cover:

a) Normal operation;

b) Anticipated operational occurrences;

c) Design basis accidents;

d) Design extension conditions, including sequences without significant fuel degradation and sequences with core melting.

The deterministic safety analysis should address all PIE originating in any part of the plant and having the potential to lead to a radioactive release to the environment, both on their own and in combination with possible additional failures. For example, in the instrumentation systems for control and limitation of the plant variables (but also to the systems for normal operation and those for anticipated operational occurrences actuated by them) and the associated safety functions. The primary focus of this manual is directed at the reactor cores and spent fuel storage facilities, currently the spent fuel pools and dry cask facilities. The analysis of other radioactive sources should be done in accordance with RG-0019 [32].

The spectrum of normal operations and abnormal DBAs that Koeberg could be exposed to during the lifetime of the plant are identified in accordance with their frequency of occurrence, based on an analysis of frequency that takes uncertainty into account. Initially, four Plant Conditions were determined from these frequencies to which appropriate nuclear safety criteria are assigned in accordance with ANS N-18.2.

Table 1: Plant Condition Frequencies

Title	Definition	Frequency of Occurrence	Initiating Event Frequency (F) Range (y^{-1})
Condition I	Normal Operation	Frequently	Planned Operations
Condition II	Incidents of Moderate Frequency	During a calendar year for a plant	$F \geq 10^{-1}$
Condition III	Infrequent Incidents	Infrequently during life of plant	$10^{-1} > F \geq 10^{-2}$
Condition IV	Limiting Faults	Postulated but not expected to occur during life of plant	$10^{-2} > F \geq 10^{-6}$

Conditions more complex and/or more severe than those postulated as design basis accidents (DBAs) can occur. These conditions shall be investigated as Design Extension Conditions (DEC) so that any reasonably practicable measures to improve the level of safety of a plant, compared to the level reached with the design basis are identified and implemented.

The accident analysis manual has been further supplemented by with the introduction of the DEC, as specified in RD-0019 [32], and has been aligned with IAEA and therefore the concept of DEC-A and DEC-B has been introduced:

Table 2: DEC definitions

Definition	**Description**
DEC-A	DEC without core melt (i.e. significant fuel degradation)
DEC-B	DEC with core melt (i.e. severe accidents)

The NNR RG-0019 [32] requires that events (including combinations of events) with initiating event frequency equal to or greater than 10^{-5} per year of operation of the facility but less than 10^{-2} per year, be categorised as DBAs. All events (including combinations of events as well as multiple failures) with frequencies less than 10^{-5} per year, including severe accidents will be classified as DECs, unless previously analysed as a DBA. The complementary accidents originally derived from EDFs accident methodology will henceforth be categorised under DECs.

3.2.2 Design Basis Plant Conditions

For the original design basis for Koeberg, Plant Conditions were defined in accordance with their anticipated frequency of occurrence and consequence. The spectra of Plant Conditions are divided into four sections that define applicable nuclear safety criteria and design requirements. These are described in the SAR [29].

3.2.2.1 Condition I: Normal Operation (and Operational Transients)

> *"Condition I occurrences are operations that are expected frequently or regularly in the course of power operation, refuelling, maintenance, or manoeuvring of the plant.*
>
> *Condition I occurrences shall be accommodated with margin between any plant parameter and the value of that parameter which would require either automatic or manual protective action."*

ANS N-18.2 [1]

The reactor control system is designed to keep pressure within limits during Condition I and Condition II events. Pressure transients shall not challenge the pressuriser safety valves. Normal operation should typically include operating conditions such as:

a) Normal reactor startup from shutdown, approach to criticality and approach to full power;

b) Power operation, including full power and low power operation;

c) Changes in reactor power, including extended low power operations;

d) Reactor shutdown from power operation;

e) Hot shutdown;

f) Cooling down process;

g) Cold shutdown;

h) Refuelling during shutdown or during normal operation at power, where applicable;

i) Shutdown in a refuelling mode or maintenance conditions that open the reactor coolant or containment boundary;

j) Normal operation modes of the spent fuel pool;

k) Storage and handling of fresh fuel.

It should be taken into account that, in some cases during normal operation, the main plant parameters change owing to transfer to different plant modes or changes in the plant power output. A major aim of the analysis for transients occurring during normal operation should be to demonstrate that the plant parameters can be kept within the specified operational limits and conditions.

3.2.2.2 Condition II: Incidents of Moderate Frequency

> *"Condition II occurrences include incidents, any one of which may occur during a calendar year for a particular plant.*
>
> *Condition II incidents shall be accommodated with, at most, a shutdown of the reactor with the plant capable of returning to operation after corrective action.*
>
> *By itself a Condition II incident cannot generate a more serious incident of the Condition III or IV type without other incidents occurring independently. A single Condition II incident shall not cause consequential loss of function of any barrier to the escape of radioactive products."*

ANS N-18.2 [1]

For Condition II occurrences, the protection system must ensure reactor shut-down before the integrity of the first barrier is threatened, and the Nuclear Steam Supply System (NSSS) [14] must be able to return to power after corrective action.

Note that although the analyses of Condition II transients will show that in general the reactor coolant pressure peaks remain low enough not to threaten the integrity of the second barrier, the repeated load variations during the unit operating life affect the fatigue strength of the material. For this reason, this aspect of safety is logged in the NSSS Design Transients Manual which serves as an accounting tool for transients to ensure that the assumptions made with respect to material properties and margins to failure in the design analysis (design loads, number of fatigue cycles, hardness, ductility, fracture resistance and so forth) are not exceeded.

The integrity of each barrier (that is, the fuel cladding, the reactor coolant system pressure boundary and the containment) shall be analysed.

3.2.2.3 Condition III: Infrequent Incidents

> *"Condition III occurrences include incidents, any one of which may occur during the lifetime of a particular plant.*
>
> *A Condition III incident shall not, by itself, generate a Condition IV fault or result in a consequential loss of function of the reactor coolant system or reactor containment barriers."*

ANS N-18.2 [1]

The pressuriser safety and relief valves have been designed to ensure pressure boundary integrity by providing adequate relief capacity for Condition III and IV events.

The integrity of each barrier (that is, the fuel cladding, the reactor coolant system pressure boundary and the containment) shall be analysed.

3.2.2.4 Condition IV: Limiting Faults

"Condition IV occurrences are faults that are not expected to occur, but are postulated because their consequences would include the potential for the release of significant amounts of radioactive material. Condition IV faults are the most drastic that must be designed against, and thus represent the limiting design case.

A single Condition IV fault shall not cause a consequential loss of required functions of systems needed to cope with the fault including those of the reactor coolant system and the reactor containment system."

ANS N-18.2 [1]

3.2.3 Design Extension Condition (DEC-A and DEC-B)

Conditions more complex and/or more severe than those postulated as design basis accidents (DBAs) can occur. These conditions shall be investigated as Design Extension Conditions (DEC) so that any reasonably practicable measures to improve the level of safety of a plant.

Requirement 20 of IAEA SSR-2/1 (Rev. 1) [24] states that:

"A set of design extension conditions shall be derived on the basis of engineering judgement, deterministic assessments and probabilistic assessments for the purpose of further improving the safety of the nuclear power plant by enhancing the plant's capabilities to withstand, without unacceptable radiological consequences, accidents that are either more severe than design basis accidents or that involve additional failures. These design extension conditions shall be used to identify the additional accident scenarios to be addressed in the design and to plan practicable provisions for the prevention of such accidents or mitigation of their consequences if they do occur."

Two separate categories of design extension conditions should be identified:

- design extension conditions without core melt (DEC-A); and
- design extension conditions with core melt (i.e. severe accidents) (DEC-B).

Different acceptance criteria and different rules for deterministic safety analysis may be used for these two categories. The main technical objective of considering the design extension conditions is to provide assurance that the design of the plant is such as to prevent accident conditions not considered in design basis conditions, or to mitigate their consequences, as far as is reasonably practicable.

The requirements differ for fuel in the reactor core and for spent fuel in storage:

- Despite all reasonable preventive measures, DEC with severe core damage have to be considered with the purpose of identifying reasonably practicable mitigative measures.

- Measures for sufficiently mitigating the consequences of severe accidents in spent fuel storages could be difficult to implement. Therefore, it is the goal that such accidents are extremely unlikely with a high degree of confidence.

The design extension conditions shall regularly, and when relevant as a result of operating experience and significant new safety information, be reviewed, using both a deterministic and a probabilistic approach as well as engineering judgement to determine whether the selection of design extension conditions is still appropriate. Based on the results of these reviews needs and opportunities for improvements shall be identified and relevant measures shall be implemented.

3.2.3.1 DEC Selection Process

Representative event sequences of design extension conditions with core melting should be selected to identify the most severe plant parameters resulting from the phenomena associated with a severe accident. These parameters should be used in the deterministic analyses of the plant structures, systems and components to demonstrate the limitation of the radiological consequences of such severe accident sequences. The analysis of these sequences should provide the environmental conditions to be taken into account when assessing whether the equipment used in severe accidents is capable of performing its intended functions when necessary (see Requirement 30 of SSR-2/1 (Rev. 1) [24]).

Representative event sequences should be selected by considering additional failures or incorrect operator responses to design basis accident or design extension condition sequences and to the dominant accident sequences identified in the probabilistic safety analysis.

The following subsections introduce the specific selection processes for DEC-A and DEC-B.

3.2.3.1.1 DEC-A

The initial selection of sequences for design extension conditions without significant fuel degradation (DEC-A) should be based on the consideration of single IE of very low frequency or multiple failures, which cannot be considered, with a high degree of confidence, to be extremely unlikely to occur and which may lead to severe fuel damage in the core or in the spent fuel storage.

It shall cover:

- events occurring during all of the defined operational states of the plant;
- multiple failures (including common cause failures) [24] and;
- events resulting from internal or external hazards (beyond design basis external events).

Where applicable, all reactors and spent fuel storage on the site must be taken into account. Events potentially affecting all units on the site, potential interactions between units as well as interactions with other sites in the vicinity shall be assessed.

The final sets of conditions selected for DEC-A analysis shall be plant and site specific, developed on the basis of the following non-exhaustive list. Examples of initiation events can be seen in Appendix C.

Events and combinations of events that can be regarded as 'extremely unlikely with a high degree of confidence' (see definition), based on information available prior to the DEC selection process or on deliberations performed during this process, do not need to be considered further for the DEC selection. For example, this can apply to a particular natural hazard that is extremely unlikely by appropriate site selection; or failure of the RPV, if it is considered extremely unlikely due to design, manufacturing, quality control, etc. It may also concern some common cause failures (CCFs) which can be considered extremely unlikely with a high degree of confidence and thus are screened out, or large reactivity insertion.

For events or credible combinations of events, which cannot be considered with a high degree of confidence to be extremely unlikely to occur and which may lead to accident conditions more challenging than those included in the design basis accidents, the DEC-A analysis should be carried out in order to ensure that they are already sufficiently covered (provisions or measures already realised by the design of the plant), or to identify reasonably practicable measures (additional provision or measure to be implemented) to prevent severe fuel damage.

It is conceivable that for an existing plant the analysis of a potential DEC-A leads to the result that existing provisions are insufficient to prevent severe fuel damage and no further measures for improving the resistance of the plant on the prevention level are reasonably practicable. Although they are part of the DEC-A analysis, the corresponding events or combinations of events will not be covered by the set of representative DECs of category A for the existing plant. In these cases, it must be investigated if there are reasonably practicable means to mitigate their consequences within DEC-B.

The determination of PIE due to internal and external hazards should take account of effects and loads from events caused by relevant site specific internal and external hazards, individually and in combination [24]. Analysis of internal and external hazards differs from analysis of PIE and scenarios caused by a single failure or multiple failures in the nuclear power plant technological systems or by erroneous human actions having a direct impact on performance of fundamental safety functions. The hazards themselves do not represent IE but they are associated with loads, which can initiate such events.

The beyond design basis external events should be defined in the following ways:

(a) By adopting a lower annual frequency of exceedance than that specified for the design basis external event;

(b) By adopting a higher amplitude in the design basis external event loading conditions for all SSCs important to safety, or for a subset of SSCs ultimately necessary to prevent an early radioactive release or a large radioactive release. One approach is to add a factor of conservatism to the design basis external event loading conditions for such SSCs.

The analysis of hazards, which is performed by using probabilistic methods or appropriate engineering methods, should aim to demonstrate for each hazard, or credible combination of hazards that either:

a) The hazard can be screened out owing to its negligible contribution to risk;

b) The nuclear power plant design is robust enough to prevent any transition from the load caused by the hazard into an initiating event;

c) The hazard causes an initiating event considered in the design.

In cases where an initiating event is caused by a hazard, the analysis should credit only the functions of those structures, systems and components that are qualified for, or protected from, the hazard.

In determining PIE caused by site specific hazards for multiple unit plant sites, the possibility of affecting several or even all units on the site simultaneously should be taken into account [24]. Specifically, the effects from losing the electrical grid, those from losing the ultimate heat sink and the failure of shared equipment should be taken into account.

3.2.3.1.2 DEC-B

A set of category DEC-B events are to be identified to cover those situations where core melt or severe fuel damaged has occurred. This could be as a result of either the capability of the plant to prevent severe fuel damage being exceeded, or where measures provided are assumed not to function as intended.

The main goal in DEC-B is ensuring adequate confinement of radioactive substances, especially by protecting the containment integrity. The accident which has resulted in severe core damage, may involve reactor vessel breach and possibly containment failure. Special consideration should be given to the sequences that could lead to large or early releases to the environment (e.g. high pressure core melt), in order to reduce the threats or to show that these sequences become very unlikely to occur with a high degree of confidence, to the extent that it demonstrates that:

a) Isolation of the containment is possible in DEC. For those shutdown states where this cannot be achieved in due time, severe core damage shall be prevented with a high degree of confidence. If an event leads to bypass of the containment, severe core damage shall be prevented with a high degree of confidence;
b) Pressure and temperature in the containment is managed;
c) The threats due to combustible gases is managed;
d) The containment is protected from overpressure. If venting is to be used for managing the containment pressure, adequate filtration is provided;
e) High pressure core melt scenarios are prevented;
f) Containment degradation by molten fuel is prevented or mitigated as far as reasonably practicable;
g) Any radioactive release into the environment is limited in time and magnitude as far as reasonably practicable to:
    i. allow sufficient time for protective actions (if any) in the vicinity of the plant; and
    ii. avoid contamination of large areas in the long term.

For existing plants, it cannot be excluded that there are states with severe fuel damage which have to be postulated, and which:

- were not considered in the past;
- cannot be considered extremely unlikely with a high degree of confidence;
- do not lead to the identification of practicable additional measures of prevention (DEC-A) and/or mitigation (DEC-B) of severe accidents;
- lead to radiological consequences which exceed the acceptable limits (in particular, to large or early releases).

For DEC-B (severe accidents) a different approach from that for the selection of DEC-A is to be taken, since there will usually be a very large number of possible scenarios, based on a wide range of plant specific severe accident conditions and phenomena, which cannot all be captured at the start of a selection process. Accordingly, a list of IE needs to be established for DEC-A and DEC-B.

A set of severe fuel damage scenarios (severe accidents) should be selected for analysis in order to establish the design basis for the safety features for mitigating the consequences of such accidents. These should cover the different situations and conditions which can occur at the outset and during the course of a severe accident. These sequences should be selected in order to represent all of the main physical phenomena (e.g. primary circuit pressure, reactor decay heat or containment status) involved in core melt sequences.

The selection process of representative scenarios should make use of the PSA results, the overall understanding of the physical phenomena involved, the margins in the design and the systems' redundancy and diversity. As far as necessary, preliminary analyses of scenarios should be performed as part of the selection process.

These cases should be identified and judged on a case-by-case basis to determine whether the associated risk is acceptable. For cases where additional measures have been identified as practicable but are not sufficient to render large or early releases extremely unlikely with a high degree of confidence, a similar judgment must be made, taking into account the practicable measures.

Core melt conditions should be postulated regardless of the provisions implemented in the design. A low estimated frequency of occurrence for an accident with core melting is not a sufficient reason for failing to protect the containment against the conditions generated by such an accident. To exclude containment failure, the analysis should demonstrate that very energetic phenomena that may result from an accident with core melting are prevented (i.e. the possibility of the conditions arising may be considered to have been 'practically eliminated').

3.2.4 Classification of New Accidents and Re-classification to Design Basis

New events may be discovered that have not been previously analysed. These may be a combination of an initiating event with a single failure, or coincident occurrence(s), or both. The plant operating condition under which the event is to be analysed is classified according to its probability of occurrence, as well as the number of failures considered.

For DBAs, the frequency of the initiating event is the root of the classification, not the frequency of the event in its totality. A probabilistic assessment can be performed to determine the likelihood of the initiating event, and best estimate values are used.

For newly identified accidents, if the probability of occurrence is greater than or equal to 10^{-5} per year, the accident shall be categorised and analysed as a "design basis" event, and the associated design and nuclear safety criteria associated with the relevant Plant Condition I, II, III or IV is applied.

Existing classification and analysis of events will remain unchanged unless OE indicates a need to re-classify. This means that the Koeberg accident analysis will remain largely based on the original ANSI 18.2. For DBAs, only in cases where new accidents are to be included or a specific need to reclassify them is identified, will the events be reclassified in accordance with RG-0019. Therefore, previously analysed DBA events with an initiating frequency of between 10^{-6} and 10^{-5} per year will remain DBAs, however any new event with a frequency of lower than 10^{-5} per year will be classified as DECs.

Industry experience has shown that for some events there have been occurrences that place them in categories that are different to those in which they were initially placed for the original design and that were considered in original licensing considerations. It may be shown from experience feedback that certain initiating event frequencies have changed from those originally calculated. For events where the initiating frequency is higher than originally calculated, an assessment shall be performed to determine whether the increase in frequency is applicable to Koeberg. If it is determined that the increase in frequency is applicable to Koeberg, the event classification should be justified to remain as is or re-categorised into the appropriate Condition or Category.

If the frequency of occurrence is shown to be below 10^{-5} per year and not part of the existing design basis, the event shall be categorised and analysed using the design and nuclear safety criteria associated with DECs.

PIE taking place during plant operating modes of negligibly short duration may be excluded from deterministic safety analysis if the analysis and quantitative assessment confirm that their potential contribution to the overall risk, including the risk of conditions arising that could lead to an early radioactive release or a large radioactive release, is also negligible. Nevertheless, the need to prevent or mitigate these events with appropriate procedures or means should be addressed on a case-by-case basis.

3.2.5 Multiple Failures in Nuclear Safety-Related Equipment and Common Cause Failures

The design and safety evaluation of the Koeberg reactor plant systems and equipment were based on the acceptance criteria and requirements associated with the operating conditions or Plant Conditions described in the previous sections. The original ANSI 18.2 deterministic approach for design base accidents did not include explicit consideration of multiple failures in nuclear safety-related equipment and common cause failures. Accident scenarios involving coincident failures, including failures outside of the single failure criteria are not addressed by the ANS N-18.2 Standard [1]. However, the design of the plant shall nevertheless be capable of accommodating postulated coincident occurrences.

The NNR, state in RG-0019 [32] that “All events (including combinations of events as well as multiple failures) with frequencies of less than 10^{-5}, including severe accident conditions”, should be classified as DEC, while “Events (including combinations of events) equal to or greater than 10^{-5} per year of operation of the facility but less than 10^{-2}, should be classified as DBAs.”

Multiple failures are therefore dealt with as DECs. More specifically those events where it is required to demonstrate no core melt or severe fuel degradation will be classified as DEC-A, while any severe phenomena will be dealt with as DEC-B.

Design basis accidents requires that on one unit will have no adverse safety consequences on a neighbouring unit. DECs on one unit should not have adverse safety consequences on a neighbouring unit where practical.

3.2.6 Sharing of Safety Systems between Multiple Units

Each unit of a multiple unit nuclear power plant shall have its own safety systems, and shall have its own safety features for DECs, as far as the plant design permits.

To further enhance safety, means of allowing interconnections between the units shall be considered in the design, as per IAEA SSR-2/1, Requirement 33 [24].

3.3 Accident Analysis Methodology

Three methods of accident analysis are acceptable; these are Conservative Analysis, Combined Analysis and Best Estimate Analysis. When using the Best Estimate approach, the uncertainty analysis shall establish, with 95% or greater probability and 95% or greater confidence level, that the calculated results do not exceed the acceptance criteria.

There are advantages and disadvantages associated with each of these methods and certain accident progressions may be better suited to a particular method of analysis. The choice of analysis methodology shall therefore be justified for each accident analysed and shall demonstrate an overall conservative evaluation methodology.

Objectives of the Deterministic Safety Analysis are:

- demonstration of compliance with acceptance criteria for a given type of accident in all plant conditions;
- verification of the adequacy of the plant design and the capacity of the safety systems;
- determination of the remaining margin and eventually indication of how to gain margin;
- definition of a number of limits in the Operating Technical Specifications (OTS).

There are three ways of analysing anticipated operational occurrences and DBAs to demonstrate that the safety requirements are met:

3.3.1 DBA Analysis Method

3.3.1.1 Option 1: Conservative Analysis

This approach will involve the use of conservative computer codes, conservative assumptions regarding the availability of systems, and conservative input data for the initial and boundary conditions.

The concept of conservative methods was introduced in the early days of safety analysis to take account of uncertainties due to the limited capability of modelling, the limited knowledge of physical phenomena and to simplify the analysis. There are fundamental deficiencies associated with the use of conservative analysis. The methodology may be so conservative that important safety issues may be masked. A conservative approach often may not show margins to acceptance criteria which, in reality, could be used to obtain greater operational flexibility, and reduce unnecessary reactor scrams or actuations of the protection systems.

The conservative assumptions may sometimes lead to the prediction of an incorrect progression of events or unrealistic timescales, or it may exclude some important physical phenomena. The sequences of events that constitute the accident scenario, which are important in assessing the safety of the plant, may thus be overlooked. The unrealistic timescales may result in unnecessary, excessive operator burden.

It is important to note that for accident scenarios with large margins to the acceptance criteria, it may be appropriate for simplicity and economy to use a conservative analysis. In cases where a realistic analysis could demonstrate that important safety issues may be masked, the conservative licensing calculations should be accompanied by a best estimate analysis, without an evaluation of the uncertainties, to ensure that important safety issues are not being concealed by the conservative analysis.

Furthermore, conservative analysis (Option 1) is rarely used and is not suggested for current safety analysis, except in situations in which scientific knowledge and experimental support is limited. However conservative analysis (Option 1) remains relevant, as it may have been used in legacy analysis.

3.3.1.2 Option 2: Combined Analysis

This approach will involve the use of best estimate computer codes, conservative assumptions regarding the availability of systems and conservative input data for the initial and boundary conditions.

The combined analysis is the use of a best estimate computer code with conservative initial and boundary conditions, as well as conservative assumptions with regard to the availability of systems. Conservative initial and boundary conditions should be used to ensure that all uncertainties associated with the plant parameters are bounded. The evaluation of uncertainties in the results of the combined analysis are meant more in the deterministic (as opposed to statistical) sense which typically considers code to code comparisons, code to data comparisons and expert judgements (e.g., phenomena identification and ranking process) in combination with sensitivity studies. The complete analysis requires the use of sensitivity studies to justify the selection of conservative input data.

3.3.1.3 Option 3: Best Estimate Analysis plus Uncertainty

This approach allows the use of best estimate computer codes together with more realistic assumptions. A mixture of best estimate and partially unfavourable (i.e., somewhat conservative) initial and boundary conditions may be used, considering the very low probability that all parameters would be at their most pessimistic value at the same time. Conservative assumptions are usually made about the availability of systems. To ensure the overall conservatism required in analysis of design basis accidents, the uncertainties need to be identified, quantified and statistically combined. Option 3 contains a certain level of conservatism and is currently accepted for some design basis accidents and for conservative analyses of anticipated operational occurrences.

An evaluation of the uncertainties in the calculation results, with account taken of both the uncertainties in the input data and the uncertainties associated with the models in the best estimate computer code. The uncertainty analysis shall establish with 95% or greater probability and 95% or greater confidence level that the calculated results do not exceed the acceptance criteria. The result, which reflects conservative choices but has a quantified level of uncertainty, is used in the safety evaluation. Realistic input data is used only if the uncertainties or their probabilistic distributions are known. For those parameters whose uncertainties are not quantifiable with a high level of confidence, conservative values should be used.

3.3.1.4 Option 4: Realistic (Best Estimate without uncertainty)

This approach allows the use of best estimate models and computer codes, and best estimates of system availability and initial and boundary conditions. Option 4 is appropriate for realistic analysis of anticipated operational occurrences aimed at the assessment of control system capability and in general for best estimate analysis of design extension conditions, as well as for the purpose of justifying prescribed operator actions in realistic analysis.

3.3.2 DEC Analysis Method

Analysis of severe accidents should be performed using a realistic approach to the extent practicable. Since explicit quantification of uncertainties may be impractical due to the complexity of the phenomena and insufficient experimental data, sensitivity analyses should be performed to demonstrate the robustness of the results and the conclusions of the severe accident analyses.

For the deterministic and probabilistic analysis of DECs, including severe accidents (DEC-B), it is acceptable to use best estimate computer codes combined with realistic assumptions and initial and boundary conditions that reflect the likely plant configuration and conditions and the expected response of plant systems and operators in the analysed accident scenario, together with an evaluation of the uncertainties associated with the relevant phenomena. However, an uncertainty analysis is not always practicable or even possible, and should not necessarily be performed when determining what measures should be taken to mitigate the consequences of severe accidents. Where it is not possible to use realistic assumptions and / or initial and boundary conditions, reasonably conservative assumptions and / or initial and boundary conditions should be used in which the uncertainties in the understanding of the phenomena being modelled are considered and bounded based to the extent possible on available experimental data or expert judgement. Appropriate rules should be defined for testing and maintenance of systems or components necessary for design extension conditions to ensure their availability, paragraph 7.63 of SSG-2 [11].

Also, there shall be sufficient independent and diverse means including necessary power supplies available to remove the residual heat from the core and the spent fuel. At least one of these means shall be effective after events involving external hazards more severe than design basis events. Batteries shall have adequate capacity to provide the necessary DC power until recharging can be established or other means are in place.

There are a number of clear and basic differences regarding the treatment of DBA and DEC, including:

- Methodology of analysis:
  - Option 1 (Conservative analysis) or Option 3 (best estimate analysis plus uncertainties) for DBA, but best estimate analysis (with or without uncertainties) is acceptable and, in some cases, preferred (see DEC analysis guidance below) for DEC;
  - single failures criterion is used for DBA, but not necessary for DECs.
- Technical acceptance criteria:
  - Generally less restrictive and based on more realistic assumptions for DEC.
- Radiological consequences outside the exclusion area are within specified limits for DECs in accordance with RG-0019 [32] as opposed to, no radiological impact outside the site boundary or exclusion area in excess of 50 mSv for DBAs.

In principle, it is admissible to perform a DEC analysis without considering uncertainties. However, the consideration of uncertainties is useful to ensure that the results of a best estimate analysis constitute a meaningful basis for the planning of reasonably practicable improvement measures.

In addition, the general principle that radioactive releases harmful to the public and the environment have to be minimised as far as reasonably practicable must be followed.

3.3.2.1 Safe State Demonstration

For DEC-A, the “defined end state” would be a “safe state” as defined in IAEA SSR-2/1 [24]: “Plant state, following an anticipated operational occurrence or accident conditions, in which the reactor is subcritical and the fundamental safety functions can be ensured and maintained stable for a long time.”

However, in case of DEC-B, it is unlikely to reach such a safe state. Therefore, the DEC-B analysis should cover a reasonable period of time, until some other defined end state is reached. This could be a “controlled state after severe accident”. This is a state after a severe accident where decay heat removal is ensured, the damaged or molten fuel is stabilized, re-criticality is prevented and long term confinement is ensured to the extent that there is limited release of radioactive nuclides.

3.3.2.2 DEC Analysis Outcome

The outcomes of the DEC analyses should be used for:

- Identification of SSCs that are important to prevent severe fuel damage (DEC-A) or to prevent large or early releases (DEC-B).
- Identification of administrative and procedural measures (operator actions, EOPs, SAMGs etc.) that are important to prevent severe fuel damage (DEC-A) or to prevent large or early releases (DEC-B).
- Identification of reasonably practicable additional provisions (regarding SSCs as well as administrative and procedural features) to prevent severe fuel damage (DEC-A) or to prevent large releases and/or to allow sufficient time for protective actions for the public to be implemented (DEC-B).

3.3.2.3 Crediting SSCs

For the fulfilment (or re-establishment) of the fundamental safety functions in DEC-A and DEC-B, the use of mobile equipment on-site can be taken into account, as well as support from off-site, with due consideration for the time required for it to be available. Control, availability considering hazards, and testing of mobile equipment should be demonstrated for equipment credited for DEC analyses[1]. Furthermore, it is essential to demonstrate that SSCs (including mobile equipment and their connecting points, if applicable) required for the prevention of severe fuel damage or mitigation of consequences in DEC have the capacity and capability and are adequately qualified to perform their relevant functions for the appropriate period of time. If accident management relies on the use of mobile equipment, permanent connecting points, accessible (from a physical and radiological point of view) under DEC, shall be installed to enable the use of this equipment. The mobile equipment, and the connecting points and lines shall be maintained, inspected, adequately stored and tested. A systematic process shall be used to review all units relying on common services and supplies (if any), for ensuring that common resources of personnel, equipment and materials expected to be used in accident conditions are effective and sufficient for each unit at all times. In particular, if support between units at one site is considered in DEC, it shall be demonstrated that it is not detrimental to the safety of any unit.

[1] An implementation program (similar to that of the Safety Related Surveillances Manual (SRSM)), which will include compliance tracking tables, is being developed. This will provide an auditable record of all the testing and surveillances for all equipment listed in the DEC Specifications and Surveillances Manual [60].

Modifications required to prevent or mitigate the consequences of DECs may be designed to non-nuclear safety class design codes. However, the appropriateness of the design code selected shall be justified, and it shall be demonstrated that the proposed modification does not compromise the design basis of the plant and is commensurate with the risk benefit.

Non-permanent equipment should not be considered in demonstrating the adequacy of the nuclear power plant design. Such equipment is typically considered to operate for long term sequences and is assumed to be available in accordance with the emergency operating procedures or accident management guidelines. The time claimed for the availability of non-permanent equipment should be justified.

The requirements for SSCs credited in the DECs is to ensure independence between the levels of defence in depth, the normal operation systems, including control and limitation systems, should not be credited in DEC-A analysis. Reason being that:

- One given sequence is potentially intended to cover several kinds of postulated initiating event, and it may be difficult to demonstrate that the operational system is always available considering both the origin of the postulated initiating event and the multiple failures.
- The sequences often create degraded ambient conditions and the systems credited in the analysis should be adequately qualified for such conditions

In cases where an initiating event is caused by a hazard, the analysis should credit only the functions of those structures, systems and components that are qualified for, or protected from, the hazard [11]. Safety systems that are not affected by the failures assumed in the design extension conditions without significant fuel degradation sequence may be credited in the analysis. However, special attention should be paid to other factors affecting safety systems (e.g. sump screen blockage) and support systems (e.g. electrical, ventilation and cooling) when assessing the independence of safety systems with regard to the postulated failures (e.g. internal flooding) [11]. The accident sequences often create degraded ambient conditions and the systems credited in the analysis should be adequately qualified for such conditions [11]. Safety systems should not be credited in the analysis of severe accidents unless it is shown with reasonable confidence that:

- Their failure is not part of any scenario that the severe accident sequence is meant to cover;
- The equipment will survive realistic severe accident conditions for the period that is necessary to perform its intended function.

3.3.2.4 Additional Information and Practical Elimination

The representative event sequences for design extension conditions with core melting, in accordance with each acceptance criterion, should be analysed to determine limiting conditions, particularly those sequences that could challenge the integrity of the containment. The representative event sequences should be used to provide input to the design of the containment and of those safety features necessary to mitigate the consequences of such design extension conditions.

The following accidents are provided as a preliminary reference of design extension conditions with core melting (severe accidents):

a) Loss of core cooling capability, such as an extended loss of off-site power with partial or total loss of on-site AC power sources and/or the loss of normal access to the ultimate heat sink (exact sequence is design dependent);

b) Loss of reactor coolant system integrity, such as loss of coolant accidents without the availability of emergency core cooling systems or exceeding their capabilities.

Paragraph 2.13(4) of SSR-2/1 (Rev. 1) [24] states:
"The safety objective in the case of a severe accident is that only protective actions that are limited in terms of lengths of time and areas of application would be necessary and that off-site contamination would be avoided or minimized. Event sequences that would lead to an early radioactive release or a large radioactive release are required to be 'practically eliminated'."

PAIA section43(1).Redacted information contains research information of a third party

"The possibility of certain conditions arising may be considered to have been 'practically eliminated' if it would be physically impossible for the conditions to arise or if these conditions could be considered with a high level of confidence to be extremely unlikely to arise."

The event sequences for which specific demonstration of their 'practical elimination' is required should be classified as follows:

a) Events that could lead to prompt reactor core damage and consequent early containment failure, such as:
   i. Failure of a large pressure-retaining component in the reactor coolant system;
   ii. Uncontrolled reactivity accidents.
b) Severe accident sequences that could lead to early containment failure, such as:
   i. Highly energetic direct containment heating;
   ii. Large steam explosion;
   iii. Explosion of combustible gases, including hydrogen and carbon monoxide.
c) Severe accident sequences that could lead to late containment failure:
   i. Basemat penetration or containment bypass during molten core concrete interaction;
   ii. Long term loss of containment heat removal;
   iii. Explosion of combustible gases, including hydrogen and carbon monoxide.
d) Severe accident with containment bypass.
e) Significant fuel degradation in a storage fuel pool and uncontrolled releases.

The consequences of event sequences that may be considered to have been 'practically eliminated' are not part of the deterministic safety analysis. However, deterministic safety analysis contributes to the demonstration that design and operation provisions are effective in the 'practical elimination' of these sequences.

3.4 Assumptions Used for Deterministic Accident Analysis

3.4.1 Reactor Fuel and Core Analysis Requirements

The Reference Core concept is used for accident analysis. The following is a brief summary of the key aspects of the Reference Core concept.

The reference fuel assembly must be defined in such a way that it is bounding with respect to current and, as far as possible, future fuel types to be used. The reference fuel assembly is be used to define the boundaries of the safety analysis that the later successive reloaded batches have to meet in order to warrant the validity of the generic reference safety analyses. The reference fuel assembly will ensure that the current licensing basis safety analysis remains valid for other fuel designs.

The reference core, a loading pattern that is as bounding as possible for all desired in-core fuel management loading patterns, should be used to generate nuclear safety parameters for the accident and transient analysis, considering uncertainties and making adequate provisions for future in-core fuel management variations.

Should it be established that the specific core or fuel assembly are not within the predefined envelope of the reference core or reference fuel assembly, specific analyses will be performed to verify that the safety limits are still respected. Should this deviation be as a result of a generic change in core or fuel design, the relevant documentation will be updated to reflect a new reference core or fuel assembly incorporating these changes.

The reference core and reference fuel analysis will form part of the assessment base within the recommended Evaluation Model Development and Assessment Process (EMDAP) process, which is further described in Section 7.2 Safety-Relevant Calculations to Support Koeberg Licensing Basis.

3.4.2 Assumptions Used for the Analysis of Plant Conditions I to IV

The assumptions used in the analysis of Plant Condition I to IV occurrences shall represent the worst or most penalising case. For Plant Condition III and IV occurrences in particular, cognisance of the general considerations discussed in the sub-sections of Section 5.1 of U.S. NRC Regulatory Guide 1.183 [47] shall be taken.

Also, the selection of initial and boundary conditions should take account of geometric changes, fuel burnup and age-related changes to the nuclear power plant, such as fouling of steam generator. Conservative initial and boundary conditions should be selected from the ranges of parameters specified in the plant's operational limits and conditions. Input data and modelling assumptions should be selected not only for neutronic and thermohydraulic aspects of anticipated operational occurrences and design basis accidents, but also for radiological aspects. In selecting conservative input parameters for the analysis, the following should be considered:

(a) Intentional conservatisms might not always lead to the intended conservatism in the results, for example if different assumptions lead to compensatory effects and 'cancel out' conservatisms;

(b) The degree of conservatism can change during the course of the event and an assumption might not remain conservative throughout the whole transient;

(c) The use of some conservative assumptions might lead to misleading or unrealistic predicted sequences of events and timescales;

(d) If conservative values are selected based on engineering judgement, there is a high risk that such selection is not properly implemented by the user and that it does not lead to conservative results.

Parameters to which the analysis results are most sensitive should be identified. A sensitivity analysis should be performed with systematic variation of the key input variables to determine their influence on the results. These analyses should be used for the determination of the values of parameters that represent the greatest challenges to safety, and for demonstrating that realistically foreseeable changes in parameters do not lead to cliff edge effects. It should be taken into account that when sensitivity analyses are carried out by changing one parameter at a time, misleading results might be obtained because the possible compensatory or cumulative effects when several parameters change simultaneously are not necessarily reflected [11].

The required single failure criteria are contained in standards such as ANSI 18-2 [1] and IAEA SSR-2/1, Requirement 25 [24].

3.4.3 Assumptions Used for the Analysis of DECs

All assumptions must be identified and suitably justified.

For the analysis of severe accidents the safety systems should not be credited in the analysis unless it can be shown with reasonable confidence that a) their failure is not part of any scenario that the severe accident sequence is meant to cover or b) the equipment will survive realistic severe accident conditions for the period that is necessary to perform its intended function [11]. Considerations about the availability of equipment under severe accident conditions should include a) the circumstances of the applicable initiating event, including those resulting from external hazards e.g., station blackout and earthquakes and b) the environment e.g., pressure, temperature and radiation and time period for which the equipment is needed [11]. Non-permanent equipment should not be considered in demonstrating the adequacy of the nuclear power plant design, as for some DEC the equipment is typically considered to operate for long term sequences and is assumed to be available in accordance with the emergency operating procedures or accident management guidelines. Hence the time claimed for the availability of non-permanent equipment should be justified.

The following assumptions may be used for the analysis of DEC-A:

- The power level will be representative of the expected authorised mode of operation.
- Control devices are considered to be operating normally.
- Off-site electrical power supply remains available (except for Blackout scenario).
- Residual power is evaluated without any margin as a function of burn-up.
- The times at which the relevant systems are assumed to start-up are calculated realistically.

In general, the combined approach or the best estimate approach with quantification of uncertainties (best estimate plus uncertainty), as applicable for design basis accidents, may be used. However, in line with the general rules for analysis of design extension conditions, best estimate analysis without a quantification of uncertainties may also be used, subject to the demonstration that there are adequate margins to avoid cliff edge effects. This may be achieved by means of sensitivity analysis demonstrating, to the extent practicable, that when more conservative assumptions are made about dominant parameters, there are still margins for the loss of integrity of physical barriers.

For DEC-A single failure criterion does not need to be applied. Furthermore, the unavailability of safety features for DEC-A due to maintenance may not need to be considered.

For DEC-B expert judgement from recognised sources may be used where benchmarked models are not available. A realistic approach is recommended to the extent practicable, since explicit quantification of uncertainties may be impractical due to the complexity of the phenomena and insufficient experimental data, sensitivity analyses shall be performed to demonstrate the robustness of the results.

The following assumptions may be used in the analysis of severe accidents (DEC-B):

- Adequately qualified instrumentation shall be available for determining the status of plant (including spent fuel storage) and safety functions as far as required for making decisions. Operational and habitable control room (or another suitably equipped location) available during DEC in order to manage such situations.
- For instrumentation, no margin need be considered, but where possible, readings are validated by multiple/diverse means. However, instrumentation credited to operate during DEC with reasonable confidence (to be capable of performing their intended safety function under the expected environmental conditions), it shall be qualified under these environmental conditions and consequential effects on instrumentation accuracy due to post accident environmental conditions shall be considered.
- Credit can be taken for the recovery of failed systems or equipment (qualified to operate in such condition) if they are not failed as part of the accident sequence and if there is reasonable confidence that they will function in the accident conditions.
- Uncertainties regarding severe accident phenomena and the outcome of mitigating measures may be accommodated through the trade-off between positive and negative impacts.
- Sensitivity analysis performed can be taken into account (and conclusions drawn from it) in the results of the safety analysis.
- Single failure criterion does not need to be applied.
- Isolation of the containment to be achieved in DECs. For those shutdown states where this cannot be achieved in due time, severe core damage shall be prevented with a high degree of confidence. If an event leads to bypass of the containment, severe core damage shall be prevented with a high degree of confidence. Together with management of:
    - pressure and temperature in the containment;
    - threats due to combustible gases;
    - containment protected from overpressure. If venting is to be used for managing the containment pressure, adequate filtration shall be provide;.
    - high pressure core melt scenarios to be prevented and
    - containment degradation by molten fuel shall be prevented or mitigated as far as reasonably practicable.

3.4.4 Operator Actions in Accident Analyses

3.4.4.1 Operator Actions in Design Basis Accidents

Reliance on operator action as part of input to the definition and successful outcome of a design basis accident shall be minimized. Where operator action is implemented instead of automatic actions, its use will be justified.

Time critical operator actions credited within the first 30 minutes of Design Basis Accident (DBA) analyses shall be assessed for acceptability before credit may be assumed for the action in the analysis.

These operator actions must be validated according to both ANS-58.8 [6] and by simulation or dry run techniques. If the validation of the action is not successful by both of these methods, a different method of achieving the objective of the action shall be used. For example, the design may be changed or the action may be automated to:

- reduce the number of operator actions;
- reduce the number of manipulations that comprise the actions;
- reduce delays in the event time sequences;
- increase the time to reaching the limiting design requirement.

Where local operator actions are required to mitigate an accident progression the operator dose estimate shall be assessed to be below the occupational dose limit (i.e. a maximum annual effective dose of 50 mSv as prescribed in RD-0022 [21]).

The following is a summary of key aspects of the ANS-58.8 [6] standard. The table below shows the allowed time interval between the first indication of the DBA to the plant operators and the earliest time for which credit can be taken for initiation of a safety-related operator action. This time frame is called the Diagnosis Time Interval ($TI_{diagnosis}$).

Minimum Diagnosis Time Intervals	
Plant Condition	Minimum $TI_{diagnosis}$
II	5 minutes
III	10 minutes
IV	20 minutes

ANS-58.8 [6] uses 5 plant conditions. The ANS-58.8 [6] conditions 4 and 5 should be treated as plant condition IV as defined by the SAR.

The time interval during which the operator initiates and completes safety-related actions is called the Operator Response Time Interval ($TI_{operator}$). The following table provides the minimum time intervals allowed for operator actions. This table shows the Operator Response Time Intervals (minutes) for each plant condition and for actions taken outside of the control room:

Operator Response Time Intervals		
Plant Condition	Fixed	Variable*
II	1 +	n
III	3 +	n
IV	5 +	n
Actions outside control room	30 +	n

ANS-58.8 [6] uses 5 plant conditions. The ANS-58.8 [6] conditions 4 and 5 should be treated as plant condition IV as defined by the SAR.

*n signifies the number of discrete manipulations to complete a specific, single operator action.

The length of $TI_{operator}$ reflects both the complexity of the DBA (based on the fixed sub-interval) and the number of individual manipulations (based on the variable sub-interval) required to complete the action. The value of the sum of the fixed sub-interval and the variable sub-interval is the minimum time interval (in minutes) that ANS-58.8 [6] allows for operator action.

The assessment process and time requirements are given in ANS-58.8 [6]. Credit for safety-related operator actions may only be taken if sufficient information and feedback from safety-related displays and control instrumentation indicates that the required safety function has been successfully achieved prior to exceeding the design limit.

In accordance with ANS-58.8 [6], departures from the specified diagnosis time intervals and operator response time intervals may be justified by using performance data derived from empirical human performance data if a 95% confidence level is demonstrated for the time available to perform safety related operator actions. Exceptions to these acceptance criteria may be made on a case-by-case basis if the application of these acceptance criteria reduces overall plant safety. Documented justification for each exemption shall be included in the safety analysis.

3.4.4.2 Operator Actions in Design Extension Conditions

Operator actions can only be credited in the analyses of DECs where they have been assessed to confirm whether the time period allowed for the required operator action is reasonable and achievable, without excessively burdening operating staff. This assessment should be focused on simulation or dry run techniques, though the guidance of ANS-58.8 [6] may also be used. Where the assessment cannot justify sufficient time for the operator to perform the action without undue burden, a different method of achieving the objective of the action shall be used. For example, actions may be automated to reduce the delays in the event time sequences.

For DEC-B credit may be taken for operator action. The risk benefit of operator actions in SAMGs should be assessed and actions that would result in a significant risk reduction in all conditions applicable to the set of guidelines must be considered to be assigned a mandatory status. The operator actions are best estimate, consistent with SAM guidelines, with action times accounting for harsh environmental conditions such as radiation levels, temperature and possible delays due to infrastructure damage. Sensitivity studies could also be used to account for delays of the immediate actions performed from the main control room.

Where local operator actions are required to mitigate an accident progression the operator dose estimate shall be assessed to be below the emergency dose limit prescribed in RD-0022 [21].

3.4.5 Accident Analysis Period

The analysis period for design basis accidents shall begin with the accident initiation and end with the plant in a safe operating state.

The acceptance criteria for the safe operating state are:

- the reactor core is subcritical;
- adequate decay heat removal is achieved;
- containment environment control is sustainable.

The IAEA Safety Report Series No. 52 [61] defines a controlled safe state as a plant state in which:

- The core is and remains subcritical;
- The core is in a coolable geometry and there is no further fuel failure;
- Heat is being removed by the appropriate heat removal systems;
- Fission product releases from the containment have ceased, or further release can be bounded.

To reach the safe operating end state the operator actions described in the EOPs will be used. This phase of the analysis begins with the first required operator action and ends with the plant in a safe operating state. It should be assumed that all operator actions are carried out without error.

During this phase of the analysis, equipment may be identified as useful to achieve the safety objective of the analysis. Identified equipment shall then be assessed to ensure that credit can be taken for the use of this equipment. Such assessment shall include the consideration of the safety classification status of the identified equipment.

The safe operating end state may vary depending on the accident conditions. The determined end state must however be justified.

The end state chosen for each event analysis may vary depending on the event. For example, in the feedwater pipe rupture accident, the penalizing factor in this phase may be that there is no make up to the ASG tank available; hot shut down is therefore not a safe operating state. It should be verified that the ASG tank capacity is sufficient to take the unit to RRA conditions. A second example is a small or intermediate break LOCA where the safe operating state may be RRA Conditions or Low Head Safety Injection.

The approach followed by Eskom for determining the accident analysis period and the associated analysis requirements is based on the approach developed by EDF [30].

For DEC-B the time span covered by any scenario analysed and presented should extend up to the moment when the plant reaches a safe and stable end state [11]. It should furthermore be demonstrated that the plant can be brought into a controlled state in order for the containment function to be maintained, with the result that the possibility of plant states arising that could lead to an early radioactive release, or a large radioactive release is practically eliminated [24]. Safety features for DEC are required to be independent, as far as practicable, from safety systems used in more frequent accidents [24].

3.5 Design and Nuclear Acceptance Criteria for Accident Analysis

The accident analyses are intended to demonstrate the overall safety of the unit for all operating occurrences by grouping all types of incidents or faults into a limited number of typical accidents.

Acceptance criteria are used in deterministic safety analysis to assist in judging the acceptability of the results of the analysis as a demonstration of the safety of the nuclear power plant. The acceptance criteria are derived from standards such as ANSI 18.2 [1] and NUREG-800 [31].

In general, each accident corresponds to the most representative case or to the most serious of a certain type of transient as far as radiological consequences is concerned. Alternatively stated as:

- those situations in the plant that are assessed as having a high frequency of occurrence shall have a small consequence to the public;
- those extreme situations having the potential for the greatest consequence to the public shall be those having a very low probability.

Acceptance criteria should be established at two levels, as follows:

- radiological dose criteria, which relate to radiological consequences of plant operational states or accident conditions. These are usually expressed in terms of activity levels or doses, and are typically defined by law or by regulatory requirements.

- technical acceptance criteria, which relate to the integrity of barriers to releases of radioactive material (e.g. the fuel matrix, fuel cladding, reactor coolant system pressure boundary and containment). These are defined in regulatory requirements, or proposed by the designer subject to regulatory acceptance, for use in the safety demonstration.

3.5.1 Acceptance criteria for DBAs

Fuel damage (as determined by Departure from Nucleate Boiling Ratio (DNBR), fuel centreline temperature and cladding temperature acceptance criteria) is not expected during Condition I and Condition II events. It is not possible, however, to preclude a very small number of fuel rod failures during normal operation. The resulting activity is within the capability of the unit clean-up systems and is consistent with the unit design basis.

Condition III incidents shall not cause more than a small fraction[2] of the fuel elements in the reactor to be damaged, although sufficient fuel element damage might occur to preclude resumption of operation for a considerable outage time.

Condition III incidents shall meet the maximum annual effective public dose of 0.250 mSv (Case 1) noted in Table 3. Any Condition III incident that has a consequence that exceeds this public dose criteria shall be shown to meet the Case 2 dose criteria for Condition III incidents noted in Table 3.

The analysis of Conditions II and III has been used to verify the design basis for the reactor protection system including set-point values. Condition IV faults are the most drastic that must be designed against, and thus represent the limiting design case. For this reason, the analysis of Condition IV events determines the requirements of the safeguard systems to conform to the safety criteria. The safety of the unit can be demonstrated by checking that protection and safeguard systems come into operation during each accident early enough to ensure conformance with the safety criteria applicable to the specific accident involved.

The pressuriser safety and relief valves have been designed to ensure pressure boundary integrity by providing adequate relief capacity for Condition III and IV events. For Condition IV events, it shall be shown that the capacity of the safety valves is such that the maximum pressure does not exceed 110% of design pressure. Furthermore, for Condition IV events the integrity of each barrier (that is, the fuel cladding, the reactor coolant system pressure boundary and the containment) shall be analysed. For the rod ejection accident analysis, the fuel cladding DNBR acceptance criteria prescribed in NUREG-0800, Standard Review Plan Section 4.2 [31], shall be adopted.

The methodology for the application of the design criteria shall be that of ANS N-18.2 [1]. From SSG-2 the acceptance criteria for deterministic safety analysis typically includes:

- Criteria relating to the integrity of the nuclear fuel matrix: maximum fuel temperature and maximum radially averaged fuel enthalpy (taking into account burnup, fuel composition and additives, such as burnable absorbers, in both values);
- Criteria relating to the integrity of fuel cladding: minimum departure from nucleate boiling ratio; maximum cladding temperature; and maximum local cladding oxidation;
- Criteria relating to the integrity of the whole reactor core: adequate subcriticality; maximum production of hydrogen from oxidation of cladding; maximum damage of fuel elements in the core and maximum deformation of fuel assemblies (as required for cooling, insertion of control rods and removal of control rods);
- Criteria relating to the integrity of the nuclear fuel located outside the reactor: adequate subcriticality; adequate water level above the fuel assemblies; and adequate heat removal;

[2] *Fraction assumed to be < 5% for purposes of accident analysis*.

- Criteria relating to the integrity of the reactor coolant system: maximum coolant pressure; maximum temperature, pressure and temperature changes and resulting stresses and strains in the coolant system pressure boundary; and no initiation of a brittle fracture or ductile failure from a postulated defect of the reactor pressure vessel;
- Criteria relating to the integrity of the secondary circuit (if relevant): maximum coolant pressure; and maximum temperature, pressure and temperature changes in the secondary circuit equipment;
- Criteria relating to the integrity of the containment and limitation of releases to the environment: value and duration of maximum and minimum pressure; maximum pressure differences acting on containment walls; maximum leakages; maximum concentration of flammable or explosive gases; acceptable working environment for operation of systems; and maximum temperature in the containment, and

Also, for DBAs:

- An event should not generate a more serious plant condition without the occurrence of a further independent failure (in addition to any single failure assumed to meet the single failure criterion). Thus, an anticipated operational occurrence by itself should not generate a design basis accident, and a design basis accident should not generate a design extension condition;
- There should be no consequential loss of the overall function of the safety systems necessary to mitigate the consequences of an accident, although a safety system may be partially affected by the postulated initiating event;
- Systems used for accident mitigation should withstand the maximum loads, stresses and environmental conditions for the accidents analysed. This should be demonstrated by separate analyses covering environmental conditions and ageing (e.g. temperature, humidity, radiation or chemical environment), and thermal and mechanical loads on plant structures and components. The margins considered in the design for given loads should be commensurate with the probability of the loads;
- The pressure in the reactor and main steam systems should not exceed the relevant design limits for the existing plant conditions, in accordance with the overpressure protection rules. Additional overpressure analysis may be necessary to study the influence of the plant conditions on safety and relief valves;
- The number of fuel cladding failures should be limited for each type of postulated initiating event to allow the global radiological criteria to be met and to limit the level of radiation to below that used for equipment qualification;
- In design basis accidents with fuel uncovering and heating up, a coolable geometry and the structural integrity of the fuel assemblies (light water reactors) should be maintained;
- No event should cause the temperature, pressure or pressure differences between containment compartments to exceed values which have been used as the design basis for the containment.
- Subcriticality of nuclear fuel in the reactor after shutdown, in fresh fuel storage and in the spent fuel pool should be maintained. Temporary returns to criticality (e.g. steam line break in pressurized water reactors) may be acceptable for certain events and plant operating modes, provided that criteria for sufficient cooling of the fuel continue to be met;
- There should be no initiation of a brittle fracture or ductile failure from a postulated defect of the reactor pressure vessel during the plant design life for any postulated design basis accident, and
- Internal reactor components should withstand dynamic loads during design basis accidents so that safe shutdown of the reactor, reactor subcriticality and sufficient reactor core cooling are maintained.

The dose acceptance criteria applicable to plant condition events are summarised in Table 3.

Table 3: Dose Acceptance Criteria for Plant Condition Events

Plant Condition Categorization Scheme		Basis of Dose Criteria	Radiological Dose Criteria
Condition I Normal Operation		Annual dose permitted in normal operation per site as prescribed in RD-0024 [22].	Maximum annual effective dose of 0.250 mSv to a member of the critical group.
Condition II Moderate Frequency Incidents			
Condition III Infrequent Incidents	Case 1[c]	Occupational exposure as prescribed in RD-0024 [22].	The occupational exposure of any worker shall not exceed an average effective dose of 20 mSv per year, averaged over five consecutive years and a maximum effective dose of 50 mSv in any single year.
	Case 2[c], including coincident iodine spike cases[d]	10% of 10 CFR 50.67 as described in Appendix E (excluding control room habitability)[a]. Occupational exposure as prescribed in RD-0022 [21].	Maximum 2-hour TEDE of 25 mSv at the exclusion area boundary. Maximum TEDE of 25 mSv at the low population zone outer boundary for the entire period of the passage of the radioactive cloud resulting from the postulated fission product release. Maximum TEDE of 50 mSv for control room habitability for the duration of the limiting accident. The occupational exposure of any worker required to perform local operator actions to mitigate an accident progression shall not exceed a maximum annual effective dose of 50 mSv.
Condition IV Limiting Faults	All accidents, excluding LOCA and including pre-incident iodine spike cases[d]	25% of 10 CFR 50.67 as described in Appendix E (excluding control room habitability)[a]. Occupational exposure as prescribed in RD-0022 [21].	Maximum 2-hour TEDE of 63 mSv at the exclusion area boundary. Maximum TEDE of 63 mSv at the low population zone outer boundary for the entire period of the passage of the radioactive cloud resulting from the postulated fission product release. Maximum TEDE of 50 mSv for control room habitability for the duration of the limiting accident. The occupational exposure of any worker required to perform local operator actions to mitigate an accident progression shall not exceed a maximum annual effective dose of 50 mSv.
	LOCA	IAEA International Basic Safety Standards [IAEA No. GSR Part 3 [10]] maximum reference level for sources that are not under control[b] (excluding control room habitability)[a] Occupational exposure as prescribed in RD-0022 [21].	Maximum 2-hour TEDE of 100 mSv at the exclusion area boundary. Maximum TEDE of 100 mSv at the low population zone outer boundary for the entire period of the passage of the radioactive cloud resulting from the postulated fission product release. Maximum TEDE of 50 mSv for control room habitability for the duration of the limiting accident. The occupational exposure of any worker required to perform local operator actions to mitigate an accident progression shall not exceed a maximum annual effective dose of 50 mSv.
DECs		Radiological consequences outside the exclusion area are within specified limits. Offsite radiological consequences requires limited protective measures in area and time (NNR RG-019 [32]). N/A (apply risk criteria described in Section 4.1.1)	

(a) Control room habitability is assessed against 100% of 10 CFR 50.67 for the limiting accident (that is, the configuration that results in the maximum consequences to the control room operators) in accordance with Sections 2.3.2 and 2.4 of U.S. NRC Regulatory Guide 1.196. All Condition III and IV events shall be considered and evaluated when determining the limiting accident. Exceptions must be analysed and justified.

(b) While the basis is 10 CFR 50.67, a more conservative dose criterion for Condition IV LOCA from IAEA Basic Safety Standards has been applied.

(c) Any Condition III incident that exceeds the Case 1 dose criteria shall be shown to meet the Case 2 dose criteria with a best estimate initiating event frequency of less than 1E-2 per year (outside the normal operation frequency range as defined in RD-0024 [22]).

(d) The coincident and pre-incident iodine spike cases are applicable to the Main Steam Line Break (MSLB) and Steam Generator Tube Rupture (SGTR) accidents, which shall be evaluated in accordance with the accident-specific assumptions provided in Appendices E and F of U.S. NRC Regulatory Guide 1.183 and considering the major deviations described in Appendix E.

Further information on the use of standards and the development of Dose Acceptance Criteria for Condition III and IV are provided in Appendix E and F.

The same or similar acceptance and radiological dose criteria [32] as those for design basis accidents may be considered, where no radiological impact outside the site boundary or exclusion area in excess of 50 mSv at the lower end of the frequency scale is allowed. Radioactive releases should be minimised as far as reasonably achievable.

3.5.2 Acceptance Criteria for DECs

In DEC-A, the objective is that the plant shall be able to fulfil, the fundamental safety functions:

- control of reactivity, preferable continuously, but if lost, re-established after a justifiable transient period
- removal of heat from the reactor core and from the spent fuel, and
- confinement of radioactive material.

For DEC-A, the fundamental safety function of heat removal can be regarded as fulfilled if operation of the corresponding systems is interrupted for some time, but their function is restored without any relevant fuel damage occurring. In particular, when assessing the residual heat removal from the spent fuel pool, the thermal inertia which is provided by the water inventory of the pool has to be taken into account. However, all relevant cases of fuel inventory and decay heat power which are possible in the pool have to be duly considered, including the case of the reactor core being completely unloaded into the pool.

In DEC-B, the objective is that the plant shall be able to fulfil the function of confinement of radioactive material. To this end removal of heat from the damaged fuel shall be established.

For DEC-B, maintaining the fundamental safety function of confinement has the highest priority. The other fundamental safety functions are of importance insofar as they are required to support the confinement function. The irreversible loss of the confinement function, and the associated uncontrolled consequences, should be avoided. Severe accident management actions to prevent this irreversible loss of the confinement function which are leading to limited and controlled releases to the environment, are not considered as a loss of the confinement function if they are temporary, associated with specific predefined requirements (such as filtering of the releases) and do not lead to unacceptable off-site consequences, and thus are part of DEC-B measures.

The acceptance criteria for DEC-B include limitation of the containment pressure, containment water level, temperature and flammable gas concentrations, and stabilization of molten corium.

The analysis shall show compliance with risk criteria as stated in RD-0024 [22] and DEC acceptance criteria should meet the requirement as in IAEA SSR-2/1 [24] that the design shall be such that for design extension conditions, protective actions that are limited in terms of lengths of time and areas of application shall be sufficient for the protection of the public, and sufficient time shall be available to take such measures.

3.6 Accident Analysis Relating to the Spent Fuel Storage Facility

The spent fuel storage facility analysis shall comply with ANSI/ANS-57.2 [3]. The dose acceptance criteria for spent fuel storage facility events are presented in Table 3.

3.6.1 Acceptance Criteria for Spent Fuel Pool Criticality Analysis

3.6.1.1 If No Credit is taken for Soluble Boron

With the spent fuel storage racks loaded with fuel of maximum permissible reactivity and flooded with full-density unborated water, the maximum k_{eff} shall be less than or equal to 0.95, including mechanical and calculational uncertainties, with a 95% probability at a 95% confidence level.

3.6.1.2 If Partial Credit is taken for Soluble Boron

With the spent fuel storage racks loaded with fuel of maximum permissible reactivity and flooded with full-density unborated water, the maximum k_{eff} shall be less than 1.0, including mechanical and calculational uncertainties, with a 95% probability at a 95% confidence level.

In addition, the spent fuel storage racks loaded with fuel of maximum permissible reactivity and flooded with full-density water borated to the concentration required to maintain the 0.95 k_{eff} limit without consideration of accidents, the maximum k_{eff} shall be less than or equal to 0.95, including mechanical and calculational uncertainties, with a 95% probability at a 95% confidence level.[3]

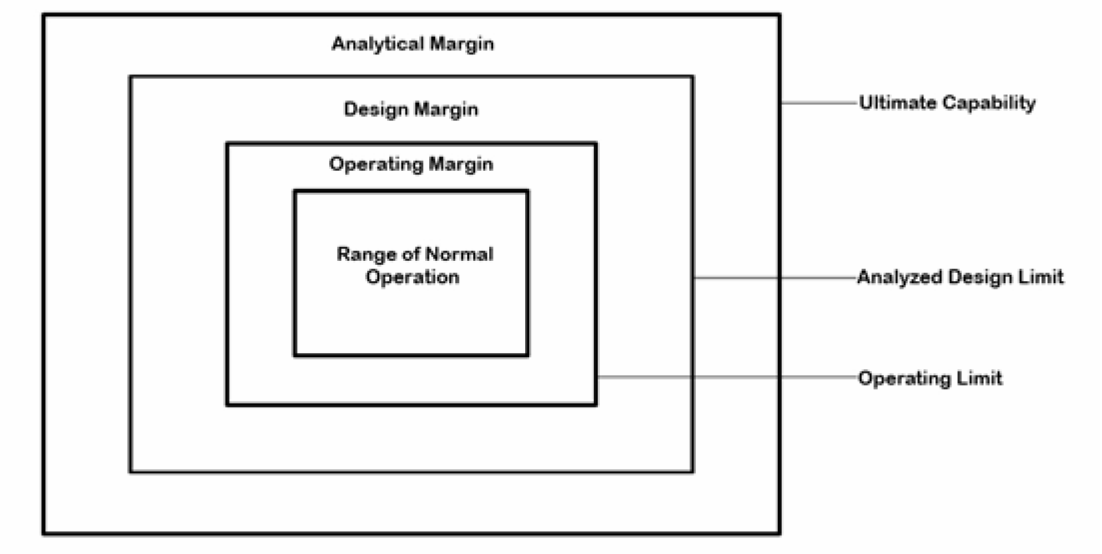
A boron dilution analysis shall be performed to ensure that sufficient time is available to detect and suppress the worst credible dilution event that can occur from the minimum technical specification concentration to the boron concentration required to maintain the 0.95 k_{eff} design limit.

Events leading to k_{eff} exceeding 0.95 must be shown to fall into the DEC category.

3.7 Margin Evaluation

The margin model shown below provides the basis for the principles of margins as provided by INPO 09-003 [12] and as accepted by Koeberg Nuclear Power Station (KNPS). Detailed explanations of the terms below are provided in Section 2.3 Definitions.

[3] *Guidance on regulatory requirements for criticality analysis of fuel storage at light-water reactor plants – Laurence Kopp US NRC WCAP 14416-NP-A Nov 1996.*



For the accident analyses, it is a requirement to provide an engineering document that includes a summary of the margins that exist between the calculated results from the limiting case and the corresponding acceptance criteria.

For DEC margin evaluation are to be performed to demonstrate, where applicable, if sufficient margins are available to avoid cliff-edge effects, early radioactive releases or large radioactive releases. In addition, sensitivity studies such as a delay of immediate actions performed from the main control room up to one hour from the beginning of core melt, assist to ensure margins with respect to possible cliff-edge effects. Expert judgement typically used to determine if the safety margins are sufficient.

Within the analysis of DEC, cliff-edge effects should be analysed and a sufficient margin to avoid those cliff-edge effects should be demonstrated wherever applicable.

The onset of severe fuel damage would be the cliff-edge effect for a DEC-A. What is considered as a sufficient margin to avoid a cliff-edge effect is to be decided on a case-by-case basis. Different kinds of margins may have to be considered, depending on the nature of the DEC.

The following examples illustrate this point for DEC-A:

- For certain multiple failure events like total Station Blackout (SBO), loss of primary ultimate heat sink and many other cases, the margin could be expressed in terms of the period of time available for measures to avoid severe fuel damage. The probability of these sequences may be taken into account.
- For events related to reactivity or loss of coolant, the margin could be expressed in terms of parameters such as fuel temperature or enthalpy release.
- For external hazards within DEC, margins could in addition be expressed in terms of frequency or severity.

For postulated DEC-B, the cliff edge effect should be understood in terms of a large increase of radiological consequences due to containment failure. A margin could be expressed in terms of likelihood or time delay of containment failure to occur.

4. Probabilistic Accident Analysis

4.1 Nuclear Safety Criteria for Probabilistic Accident Analysis

4.1.1 Nuclear Regulator's Licensing Criteria for Plant Personnel and Public Risk

The Nuclear Regulator's licensing criteria for plant personnel and public risk are presented in RD-0024 [22]. A summary is given in the table below.

Plant Personnel Risk	Accidents
Average Peak	1E-5 fatalities/annum 5E-5 fatalities/annum
Public Risk	**Accidents**
Average Peak	1E-8 fatalities/annum 5E-6 fatalities/annum

The requirements of NNR RD-0024 [22] shall be met. Where NNR RD-0024 [22] does not give instruction, ASME PSA standards, such as those listed in Appendix D, will be used as guides in the development of the PSA with the intent that the PSA should meet "Capability Category II" in areas impacting risk informed decisions.

4.2 Assumptions for Probabilistic Accident Analysis

Sensitivity and uncertainty analyses shall be performed on key sources of uncertainty that impact the PSA results and consequently may influence the decision being made or lead to noncompliance (see ASME/ANS RA-Sa-2009 [8] definition for 'assumption' and 'source of model uncertainty').

4.2.1 Core Damage Analyses (Level 1 PSA Studies)

Core damage analyses (and the Koeberg Level 1 PSA Study) are analyses that calculate the expected frequency of significant core damage.

The following assumptions shall apply:

- a severe accident is defined as one where significant core damage has occurred;
- when the reactor is initially at power, the power level is at 100% of full power;
- when the reactor is shut down, a best estimate decay heat value is used;
- when the reactor is in a low power state a realistic power value is used;
- the single failure criterion is not applied;
- the times at which the relevant systems are assumed to start-up are determined realistically;
- the times that relevant systems are assumed to run for are calculated realistically;
- best-estimate accident analysis codes and methodology for modelling are used;

- expert judgement may be used as a substitute for quantitative analysis in instances where the use of benchmarked codes or models is considered to be impractical, as stated in ASME/ANS RA-Sa-2009 [8];
- in accordance with ASME/ANS RA-Sa-2009 [8] (see SY-A22) non-safety related systems may be considered when appropriately supported;
- best estimate reliability, availability and maintainability component data are used;
- realistic system success criteria that can be derived using a best-estimate accident analysis code will be used;
- risk significant procedurised operator actions will be included;
- credit can be taken for the recovery of failed systems or equipment, where justifiable, which will usually be within accident scenarios which extend beyond 24 hours;
- the analysis can end when a controlled safe state is reached.

4.2.2 Containment Response and Source Term Analyses (Level 2 PSA Studies)

Containment response and source term analysis is performed for severe accident sequences, ultimately to determine the source term (that is, physical/chemical form and time history of the radio nuclide releases).

The following assumptions shall apply:

- best estimate probabilistic analysis techniques can be applied;
- expert judgement may be used as a substitute for quantitative analysis in instances where the use of benchmarked codes or models is considered to be impractical, as stated in ASME/ANS RA-Sa-2009 [8];
- best estimate severe accident analysis programs are used where practical and when their models include the relevant phenomena;
- in identifying the success paths of the event trees, the analysis can show that a controlled stable state is reached. An example of the details for a controlled stable state is given in Table 4.3-1 of OCDE / GD (97) 198;
- non-safety related systems may be considered where appropriate. Credit can be taken for the recovery of failed systems or equipment;
- where justifiable, credit can be taken for the use of systems or equipment beyond their design intent;
- uncertainties regarding severe accident phenomena and the outcome of mitigating measures may be accommodated through the trade-off between positive and negative impacts;
- credit may be taken for operator action;
- best estimate initial radioactive inventories are to be used;
- core damage sequences shall be grouped into plant damage states based on their accident progression attributes in a manner consistent with ASME/ANS RA-Sa-2009 (see HLR-LE-A and supporting requirements);

- the radionuclide release(s) shall be defined into release categories so as to support the offsite consequence analysis in a manner consistent with ASME/ANS-58.25 [9] (see HLR-RE-A and supporting requirements RE-A1 and RE-A2).

4.2.3 Off-Site Consequence Analyses (Level 3 PSA Studies)

Off-site consequence analyses (and the Koeberg Level 3 PSA Study) are analyses that calculate the impact of large accidental radioactive releases beyond the Koeberg site boundary.

The following assumptions shall apply:

- the beneficial effect of any administration of stable iodine tablets is ignored;
- the beneficial effect of sheltering is ignored;
- the beneficial effect of evacuation is ignored;
- the beneficial effect of relocation is ignored;
- the beneficial effect of decontamination of persons is ignored;
- the beneficial effect of decontamination of areas is ignored;
- the beneficial effect of body protection (for example, gloves, hats, raincoats) is ignored;
- the beneficial effect of respiratory protection (for example, the use of handkerchiefs and other items to cover the mouth and nose) is ignored;
- the beneficial effect of access control to affected areas is ignored;
- the beneficial effect of a food ban is given credit (for example, the ingestion pathway will not be considered) provided that the implementation of a food ban is demonstrated to be adequately addressed in a procedure and is credible;
- best estimate future population developments are to be taken into account wherever possible;
- the transient population is to be included in the demographic data if the information can be made available and if their numbers make a significant contribution to public risk;
- a best estimate off-site consequence code is used;
- best estimate initial radioactive inventories are used;
- best estimate release fractions are used;
- realistic meteorological data are used;
- realistic population estimates are used.

4.2.4 Worker Risk Analyses

Worker risk analyses are analyses that calculate the risk to the plant personnel from accidental radioactive releases. These accidental releases could typically occur from severe accidents, fuel handling accidents[4] and waste treatment accidents.

[4] In the case of fuel handling accidents covered by the design basis, conservative analyses are used as some of these can constitute Condition IV events.

The following assumptions shall apply:

- best estimate initial radioactive inventories are used;
- best estimate radioactive releases are used;
- best estimate plant personnel doses are used;
- best estimate plant personnel risk is calculated;
- best estimate dose calculation programs are used where practical and when their models include the relevant phenomena;
- stochastic and deterministic doses are considered;
- stochastic and deterministic risks are considered

5. Emergency Planning Technical Basis

Even though the potential for serious accidents, which could lead to a significant release of radioactivity around the Koeberg station is extremely low, it cannot however be eliminated entirely. It is therefore considered prudent and in accordance with regulatory requirements to put in place emergency response plans off-site that consider and implement emergency or remedial measures where the potential exists that any member of the public may receive more than an annual effective dose of 1 mSv resulting from such events [Regulations No. R. 388 [23]].

The EP requirements are based on the regulatory requirements set out in RD-014 [19] which specifies that the holder of a nuclear authorization must periodically conduct a comprehensive safety analysis which shall take into account potential accidents over a wide range of probabilities such that severe accidents are also considered. The safety analysis shall identify potential threats and determine the likelihood, nature and magnitude of the nuclear and radiological consequences. RD-014 [19], together with the current NNR approved EP Technical Basis methodology and approach as detailed in the NNR Report on the Technical Basis for the Koeberg Emergency Plan (issued and approved by the NNR via letter k12131N [16] and k12131.1N [17]), provides a technical basis for the EP in terms of planning zones, protective action strategies and timing for protective action implementation. The objectives of the protective actions are to prevent deterministic effects (early mortality or morbidity) and to reduce stochastic effects (principally cancer) as much as is reasonably practicable.

The development of the EP technical basis adopts an approach where both the deterministic analysis of the potential consequences of accidents and an analysis of the risk related to the entire spectrum of potential accidents are utilized. The deterministic analysis is used in the evaluation of accident scenarios taking into consideration the consequences of potential severe accidents for various weather patterns whereas risk insights from the PSA are used to determine the Reference Accident(s).

The technical basis for Emergency Planning is documented in the Koeberg SAR Part III Chapter 4 Section 2 [29].

6. Severe Accident Guidelines

It is predicted that the progression of events that lead to the potential for creating a radioactive release to the environment that exceeds the authorised limits will occur over a period of time. Early in the event sequence, the EP shall be activated and the Emergency Control Centre (ECC) and Technical Support Centre (TSC) staffed.

The Senior Reactor Operators shall be responsible for the implementation of the governing accident procedures until the pre-determined criteria are exceeded that indicate fuel damage has occurred. Once it is apparent that fuel damage has occurred, the TSC shall provide the Control Room crew with guidance in mitigation of the accident. To this purpose, the TSC shall use appropriate accident management guidelines, specific to severe accident phenomena.

7. Validation and Verification of Computer Software and Nuclear Safety-Related Calculations

7.1 Calculations Performed by Eskom to Support Koeberg Operation

To support the safe, reliable operation of KNPS, a wide range of accident analysis codes can be utilised. The code set currently identified for accident analysis includes those used for reactor neutronics, radiation and dose, thermal hydraulics, and so forth.

Examples of accident analysis codes currently employed by Eskom are:

- MAAP
- RELAP / SCDAP / SIM
- PC COSYMA

Subject to appropriate verification and validation, these codes can be used in the following applications:

- Accident management guidance;
- Emergency exercise scenario development;
- Equipment qualification;
- Incident investigation;
- Operator response investigation;
- PSA analyses;
- Reactor licensing activities;
- Training simulators;
- Containment performance;
- Plant support;
- Outage support;
- Spot checks to support reviews of safety, engineering and operational analysis;
- Risk-informed information for operation and engineering-related activities;

- Support for design basis and DECs and severe accident procedures;
- Support for operating procedures.

Use of these software codes and the performing of accident analysis for the above applications shall be subject to the following provisions:

- personnel performing analysis using software codes, such as MAAP and RELAP shall hold appropriate qualification(s) and relevant authorisation(s);
- all analyses shall be carried out in accordance with approved and controlled processes and procedures;
- verification and validation of the software code and its models shall be performed. The extent of applying this shall be dependent on the pedigree of the code(s) and its importance to the safety case;
- all software codes and analyses shall be developed within a formal Quality Assurance and verification and validation management system in accordance with approved and controlled processes and procedures. An auditable trail shall be evident for all data and phases in the development, validation and verification process;
- all software codes shall be authorised as fit for its intended use in each particular application and any limitations shall be specified;
- all analyses shall be reviewed internally and independent reviews shall be considered commensurate with the nature of the calculation and its importance to the safety case. All review comments and their resolution shall be documented;
- a complete description and justification of the models, analytical approaches, equations, approximations, assumptions and empirical correlations used, the limitations of the code, sensitivity studies and demonstration of solution convergences shall be documented to conform to the principal requirements given in RG-0016 [20].

7.2 Safety-Related Calculations to Support Koeberg Licensing Basis

This section is applicable for nuclear-safety relevant calculations to support licensing and to prove the KNPS safety case. An established and acceptable validation and verification approach will be undertaken which demonstrates compliance to RG-0016 [20] and other pertinent regulatory requirements.

The level of verification and validation undertaken will be dependent of the pedigree of the code and its importance to the safety case. For execution of the validation and verification process, it is recommended that the U.S. NRC EMDAP or KAA-737 (Guide KGF-001) to be followed.

In accident analysis, more than one calculation is required for determining the accident progression and consequences. This complete set of analyses required to evaluate the event behaviour and consequences is termed the Evaluation Model (EM). By definition, an EM is the calculation framework for evaluating the behaviour of the reactor system during a postulated transient or design basis accident which includes one or more computer program and all other information required for use in the target application. EMs comprise of Calculation Models (CMs) (each consisting of System Models, Software Products (SPs) and data) and the flow of data between CMs. Verification and validation activities will be performed to assess the adequacy of all the EMs, including all its constituents for nuclear safety-related calculations.

The EM development process shall be clearly defined and the application envelope for each EM shall be determined. The importance of constituent phenomena, processes and key parameters within that envelope requires adequate identification and concurrence. These requirements shall be clear, comprehensive and sufficient to permit an independent review.

The verification and validation of the EM is only completed when the verification and validation of the constituent components (CMs, SPs and data) has been concluded. The same applies to the Calculation Model (CM); the constituent SPs and data need to be verified and validated before the verification and validation of the CM can be completed. For the case where several EMs are used, the verification and validation process used must be consistent and systematic across all EMs. The complete EMs, in their entirety, shall conform to RG-0016 [20] to ensure that it predicts the consequences of an accident with sufficient accuracy and to a suitable degree of confidence.

The phenomena assessment process shall be used to identify and rank all phenomena associated with the EM developed to assess the event behaviour and consequences, and to expose the critical set of phenomena which have the greatest effect on the acceptance criteria. An assessment base shall be developed to validate and assess the adequacy of the EM. The assessment base consists of the collection of experimental data and other empirical evidence, which should include, as a minimum, the following records:

- separate effects tests developed to assess empirical correlations and other closure models;
- integral effects tests developed to assess system interactions and global code capability;
- plant normal operations and transient data (on-site data where applicable);
- benchmarking with other software codes and calculation methods;
- other experimental data to validate and verify input data.

Suitable provisions shall be made to account for any uncertainties arising with regards to nuclear safety related calculations using software, data or models with incomplete verification and validation. Uncertainty analysis will be performed, described and justified for each calculation model where applicable. The treatment of uncertainties whether aleatory or epistemic, and the criteria and methodology used for management of these uncertainties, shall be justified and comply with RG-0016 [20] and / or other governing international standards. Refer to Section 3.3, Section 3.4 and Section 3.5 for more information. Should any of these provisions become necessary in order to support incomplete verification and validation efforts, these will be clearly documented, controlled and justified to ensure that the design and nuclear safety criteria are not compromised.

8. Acceptance

This document has been seen and accepted by:

Name	Designation
Israel Sekoko	Middle Manager – Nuclear Analysis and Siting
Lufuno Mahlangu	Manager Engineering – Deterministic and Probabilistic and Safety Analysis
Shirley Movalo	Corporate Specialist Nuclear
Marc Maree	Acting Senior Manager – Nuclear Licensing
Innes Greeff	Senior Physicist – Reactor Fuel Engineering
Mvuseleli Hermanus	Manager Engineering – Koeberg Safety Case Group
Thavy Krishna	Senior Consultant – Nuclear Analysis and Siting
Emmanuel Lamprecht	Senior Physicist – Deterministic and Probabilistic and Safety Analysis

9. Revisions

Date	Rev.	Compiler	Remarks
	Rev 3	E Khoza	Revised to address NNR comment communicated through k29105N. The last paragraph under Section 3 was deleted since the DEC analysis assumption is covered in section 3.4.3. This means that the following has been deleted: In addition, for DEC analysis it should be assumed that the features to prevent core melting fail or are insufficient, and that the accident sequence will further evolve into a severe accident.
December 2022	331-195 Rev 3	R Steyn	Revised to address NNR comments received in k26709N and k28772N mainly including the following changes: • Incorporation of Design Extension Conditions (DECs) information • Clarity of Figure 1 improved and updated to reflect DEC • Inclusion of Section 5.2.2 (KAAM Rev. 1c) as it has been omitted in Section 3.2.2 in KAAM Rev. 2 • SC-14 (in k28772N): Control, availability considering hazards, and testing of mobile equipment should be demonstrated for equipment credited for DEC analyses. Additionally, GA 41045 text clarification provided in Section 3.2.2.4 (acceptance criteria for Condition IV incidents) and GA 40926 option information included for the selection of the analysis method (Section 3.4.1).

Date	Rev.	Compiler	Remarks
April 2020	331-195 Rev 2	Y Combrink	Updated to reflect the latest document template and changed organisation. Also added content for the following new sections: • Section 2.5 on Roles and Responsibilities. • Section 2.6 on Process for Monitoring; and • Section 2.7 on Related/Supportin g Documents.
March 2018	331-195 Rev 1c	Y Combrink	Revised to address the NNR comment received in k24031N.
October 2017	331-195 Rev 1b	Y Combrink	Revised to address NNR comments received in k23090N. Lastly, RD-0016 was replaced with / superseded by RG-0016.
July 2016	331-195 Rev 1a	Y Combrink	Revised to address NNR general review comments received in k21682N as per Eskom's response detailed in letter K-23090-E. The following additional changes have also been made: • Table 5.3.1 was improved to clarify the dose acceptance criteria applicable to the coincident and pre-incident iodine spike cases to be evaluated for MSLB and SGTR accidents in accordance with the accident-specific assumptions provided in Appendices E and F of U.S. NRC Regulatory Guide 1.183. • Section 5.5 was updated to describe the major deviations from the Alternative Source Term (AST) guidance provided in U.S. NRC Regulatory Guide 1.183 that shall be applied to the dose consequence assessment of Condition III and IV events as detailed in Revision 4 of the Alternative Source Term (AST) Framework Document (PSA-R-T16-18).
March 2015	331-195 Rev 1	T Booysen	Revised in accordance with NNR Comments k20566N Rev 1 and NNR Comments & Approval k21464N.

Date	Rev.	Compiler	Remarks
November 2012	331-195 Rev 0	T Booysen	In accordance with the Nuclear Engineering Document Management System the unique identifier 331-95 was allocated to replace 335-64. The Koeberg Accident Analysis Manual was updated as a major revision to 331-95 Revision 0 to take into account current developments in the field of accident analysis. Current developments for ensuring the stable and safe operation of nuclear reactors are closely related to the advances that are being made in safety analysis. Initially, rigorous conservative approaches to anticipated operational occurrences and design basis accidents were used in deterministic safety analyses. Licensing calculations used conservative codes with conservative input data, mostly owing to the difficulty of modelling complicated physical phenomena with limited computer capacity and a lack of adequate data. As more experimental data has become available, and with advances in code development the practice in many countries has moved towards a more realistic approach together with an evaluation of uncertainties. Advances have also been made in areas including evaluation of operator actions, radiological consequences of accidents and verification and validation of computer codes. The Koeberg Accident Analysis Manual has been updated to incorporate international best practices into the process for accident analysis for Koeberg Nuclear Power Station.
February 2011	335-64 Rev 0	A Rajkumar	In accordance with the Eskom Document Management System the unique identifier 335-64 was allocated.
March 2009	36-928 Rev 0	A Rajkumar	Updated numbering scheme from GGM-0907. Include Section 4.8 on use of Accident Analysis Code.

10. Development Team

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

- Ruan Steyn Nuclear Engineering
- Neil Foster Nuclear Engineering
- Louise Nieuwoudt Nuclear Engineering
- Jenna De Araujo Nuclear Engineering
- Cate Pretorius Nuclear Engineering

11. Acknowledgements

Not applicable.

Appendix A – Design Basis Standards

The nuclear safety criteria of ANS N-18.2 (1973) [1] were applied to Koeberg Nuclear Power Station during the design and construction phase. Therefore, unless an alternative is approved, this is the default design standard and accident analysis standard.

Although this standard has been withdrawn, it is not practical to perform a total backfit of the safety design criteria of later standards such as ANSI/ANS-51.1 [2] onto the existing plant, as ANS N-18.2 [1] was applied during the design phase of Koeberg. The general application of ANSI/ANS-51.1 [2] rules to future plant changes at Koeberg will inexorably result in loss of design configuration and integrity. It is feasible to apply later standards, including ANS-51.1 [2] acceptance criteria, to specific changes where it is possible to clearly bound or contain the design limits. However, such cases must be applied with caution as very few systems are without functional design interdependencies.

It is acknowledged that ANSI/ANS-51.1 [2] did represent an evolution of the ANS N-18.2 [1] requirements, and that there are significant parts of ANSI/ANS-51.1 [2] that are consistent with ANS N-18.2 [1] acceptance criteria. In line with the sentiments of ANS N-18.2 [1], clause 1.7, where the design criteria are not seen to be all encompassing and complete, the Eskom approach is to continue to apply ANS N-18.2 [1] acceptance criteria, and to support that with later standards, including sections of ANSI/ANS-51.1 [2], that augment or clarify ANS N-18.2 [1] rules.

Appendix B – Levels of DiD

Level of defence*	Objective	Essential design means	Essential operational means
Level 1	Prevention of abnormal operations and failures	Conservative design and high quality in construction of normal operation systems, including monitoring and control systems	Operational rules and normal operating procedures
Level 2	Control of abnormal operation and detection of failures	Limitation and protection systems and other surveillance features	Abnormal operating procedures/ emergency operating procedures
Level 3 3a	Control of design basis accidents	Engineered safety features (safety systems)	Emergency operating procedures
3b	Control of design extension conditions to prevent core melt	Safety features for design extension conditions without core melt	Emergency operating procedures
Level 4	Control of design extension conditions to mitigate the consequences of severe accidents	Safety features for design extension conditions with core melt Technical Support Centre	Complementary emergency operating procedures/severe accident management guidelines
Level 5	Mitigation of radiological consequences of significant releases of radioactive material	On-site and off-site emergency response facilities	On-site and off-site emergency plans

* Koeberg follows Approach 1 and focus on Level 1, 2 and 3, as described in TECDOC-1791 [59].

Appendix C – WENRA Examples of DBA, DEC and Practical Elimination events

DBAs:

- small, medium and large LOCA
- breaks in the main steam and main feed water systems
- forced decrease of reactor coolant flow
- steam generator tube rupture
- uncontrolled movement of control rods
- uncontrolled withdrawal/ejection of control rod

DEC-A:

- IE induced by earthquake, flood or other natural hazards exceeding the design basis events;
- IE induced by relevant human-made external hazards exceeding the design basis events;
- prolonged station black out (SBO; for up to several days);
  - SBO (loss of off-site power and of stationary primary emergency AC power sources);
  - total SBO (SBO plus loss of all other stationary AC power sources), unless there are sufficiently diversified power sources which are adequately protected;
- loss of primary ultimate heat sink, including prolonged loss (for up to several days);
- anticipated transient without scram (ATWS);
- uncontrolled boron dilution;
- total loss of feed water;
- LOCA together with the complete loss of one emergency core cooling function (e.g. HHSI or LHSI);
- total loss of the component cooling water system;
- loss of core cooling in the residual heat removal mode;
- long-term loss of active spent fuel pool cooling;
- multiple steam generator tube ruptures;
- loss of required safety systems in the long term after a design basis accident.

DEC-B:

- hydrogen explosion
- large steam explosion
- direct containment heating
- basemat melt

- vessel rupture
- containment bypass
- containment overpressure
- containment isolation failure

Practical elimination:

1. Events that could lead to prompt reactor core damage and consequent early containment failure:
    a. Failure of a large component in the reactor coolant system (RCS);
    b. Uncontrolled reactivity accidents.
2. Severe accident phenomena which could lead to early containment failure:
    a. Direct containment heating;
    b. Large steam explosion;
    c. Hydrogen detonation.
3. Severe accident phenomena which could lead to late containment failure:
    a. Molten core concrete interaction (MCCI);
    b. Loss of containment heat removal.
4. Severe accident with containment bypass;
5. Significant fuel degradation in a storage pool.

Appendix D – ASME PSA Standards for Guidance

Where NNR RD-0024 [22] does not give instruction regarding acceptance criteria for plant personnel and public risk, ASME PSA standards, such as those listed below, will be used as guides in the development of the PSA with the intent that the PSA should meet “Capability Category II” in areas impacting risk informed decisions.

- ASME/ANS RA-Sa–2009 ‘Standard for Level 1/Large Early Release Frequency Probabilistic Risk Assessment for Nuclear Power Plant Applications’ [8];
- ASME/ANS-58.25 (2010) ‘Radiological Accident Offsite Consequence Analysis (Level 3 PRA) to Support Nuclear Installation Applications, Draft’ [9];
- ANSI/ANS-58.21 (2007) ‘External-Events PRA Methodology’ [4];
- ANSI/ANS-58.22 (2009) ‘Low Power and Shutdown PRA Methodology, Draft’ [5].

Appendix E – Dose Consequence Assessment of Condition III and IV Events

The acceptance criteria for the assessment of the doses at the Exclusion Area Boundary (EAB) and the outer boundary of the Low Population Zone (LPZ) from all Condition III (Case 2) and IV events, excluding the LOCA event, shall be based on fractions from ANSI/ANS-51.1 [2] of the Total Effective Dose Equivalent (TEDE) criteria specified in 10 CFR 50.67 "Accident Source Term" [42] as presented in Table 3.

The dose acceptance criteria at the EAB and the outer boundary of the LPZ for the Condition IV LOCA event shall be based on the more conservative IAEA International Basic Safety Standards maximum TEDE reference level of 100 mSv instead of the TEDE criteria specified in 10 CFR 50.67.

In accordance with Sections 2.3.2 and 2.4 of U.S. NRC Regulatory Guide 1.196, control room habitability shall be assessed for the limiting accident against 100% of the TEDE criteria specified in 10 CFR 50.67. The limiting accident is the configuration that results in the maximum consequences to the control room operators. All Condition III and IV events shall be considered and evaluated when determining the limiting accident for control room habitability.

10 CFR 50.67 [42] specifies the following TEDE criteria:

- An individual located at any point on the boundary of the exclusion area for any 2-hour period following the onset of the postulated fission product release, would not receive a radiation dose in excess of 0.25 Sv TEDE.
- An individual located at any point on the outer boundary of the LPZ, who is exposed to the radioactive cloud resulting from the postulated fission product release (during the entire period of its passage), would not receive a radiation dose in excess of 0.25 Sv TEDE.
- Adequate radiation protection is provided to permit access to and occupancy of the control room under accident conditions without personnel receiving radiation exposures in excess of 0.05 Sv TEDE for the duration of the accident.

The assumptions and methods provided in U.S. NRC Regulatory Guide 1.183 [48] “Alternative Radiological Source Terms for Evaluating Design Basis Accidents at Nuclear Power Reactors” (July 2000) shall be used for determining compliance to the Condition III and IV dose acceptance criteria presented in with the following major deviations PSA-R-T16-18 [49]:

- Table 6 in U.S. NRC Regulatory Guide 1.183 [47] is replaced with the dose acceptance criteria for Condition III and IV events presented in . However, the analysis release durations for accidents noted in Table 6 of U.S. NRC Regulatory Guide 1.183 [47] remain applicable and are adopted in total when determining the TEDE at the outer boundary of the low population zone.
- The following dose conversion factors based on International Commission on Radiological Protection (ICRP) Publication 60 are used in determining the TEDE, which is the sum of the Committed Effective Dose Equivalent (CEDE) from inhalation and the Effective Dose Equivalent (EDE) from external exposure:
  - For members of the public, the adult exposure-to-CEDE conversion factors for inhalation provided in ICRP Publication 72 [34];
  - For operators, the adult exposure-to-CEDE conversion factors for inhalation provided in ICRP Publication 68 [33]; and

- For members of the public and operators, the adult air submersion effective conversion factors available from the U.S. Environmental Protection Agency (EPA) software and data package DCFPAK 3.0 (Dose Coefficient File Package) , Version 3.02 [45].

- Table 2 in U.S. NRC Regulatory Guide 1.183 [47] is replaced with the LOCA event total core inventory fractions released into containment that has been reduced by 60% as presented in the table below, consistent with the 60% reduction in the Condition IV LOCA event dose acceptance criteria at the EAB and the outer boundary of the LPZ specified in 10 CFR 50.67 (i.e., reduction from 250 mSv to 100 mSv TEDE) [42]:

Condition IV LOCA Event Total Core Inventory Fractions Released into Containment			
Radionuclide Group	**Gap Release Fraction**	**Early In-vessel Phase**	**Total**
Noble Gases	0.02	0.38	0.40
Halogens	0.02	0.14	0.16
Alkali Metals	0.02	0.10	0.12
Tellurium Metals	0.00	0.02	0.02
Ba, Sr	0.00	0.008	0.008
Noble Metals	0.00	0.001	0.001
Cerium Group	0.00	0.0002	0.0002
Lanthanides	0.00	0.00008	0.00008

- For non-LOCA events, Table 3 in U.S. NRC Regulatory Guide 1.183 [47] (applicable to both non-LOCA DBAs and Reactivity Initiated Accident (RIAs)) is replaced with the revised steady state gap release fractions presented in the table below, that were published in [PNNL 18212 Rev. 1] [46] and [U.S. NRC Staff Memorandum dated 26 July 2011 (ML111890397)] and provides the technical basis for the proposed revision to [U.S. NRC Draft Regulatory Guide DG-1199] [47] based on [PNNL-18212 Rev. 1] [46]:

Radionuclide Group	**Steady-State Gap Release Fraction for Non-LOCA Events**
I-131	0.08
I-132	0.09
Kr-85	0.38
Other Noble Gases	0.08
Other Halogens	0.05
Alkali Metals	0.50

- For RIAs, Table 3 in U.S. NRC Regulatory Guide 1.183 [47] is replaced with the combined (i.e., the sum of the revised steady-state gap release and transient-induced Fission Gas Release (FGR)) fractions presented in the table below, with the steady-state gap release fractions as presented in the table above and the transient-induced FGR fraction based on the correlation for peak pellet burnup ≥ 50 GWd/MTU provided in [U.S. NRC Staff Memorandum dated 16 March 2015 (ML14188C423)][5]:

Radionuclide Group	Combined Release Fraction for RIAs[a,b,c]
I-131	$0.08 + 0.33 \times [(0.26 \times \Delta H) - 5]/100$
I-132	$0.09 + 0.33 \times [(0.26 \times \Delta H) - 5]/100$
Kr-85	$0.38 + [(0.26 \times \Delta H) - 5]/100$
Other Noble Gases	$0.08 + 0.33 \times [(0.26 \times \Delta H) - 5]/100$
Other Halogens	$0.05 + 0.33 \times [(0.26 \times \Delta H) - 5]/100$
Alkali Metals	$0.50 + (2)^{0.5} \times [(0.26 \times \Delta H) - 5]/100$

a. ΔH = increased peak radial average fuel enthalpy during RIA (Δcal/g).
b. Assumes no fuel melting.
c. The calculated transient-induced FGR fraction contribution must be ≥ 0.

As stated in U.S. NRC Regulatory Guide 1.183 [47], the TEDE should be determined for the most limiting person at the EAB and in the LPZ.

It should be noted that the assumptions in U.S. NRC Regulatory Guide 1.183 [47] are often for severe accidents and so are very conservative with respect to design basis accident scenarios. Furthermore, since the dose consequences for all Condition III and IV events will be re-assessed according to U.S. NRC Regulatory Guide 1.183 [47] (that is, a full implementation that addresses all characteristics of the Alternative Source Term is pursued), a sensitivity/scoping analysis of the dose consequence assessment of Condition III and IV events is not required and shall not be performed[6].

---

[5] *Even though the additional factor of 0.33 applied in [PNNL 18212 Rev. 1] is not clearly included in [U.S. NRC Staff Memorandum dated 16 March 2015 (ML14188C423)], the factor of 0.33 applied to I-131 and other short lived radionuclides (with half-life less than 4.85 hours) to account for decay during diffusion was kept since ignoring (not crediting) decay during diffusion is considered to be overly conservative for RIAs. Lastly, the adjustment factor of (2)0.5 applied in [PNNL 18212 Rev. 1] is conservatively included for alkali metals.*

[6] *This follows from the Analysis Decision Chart and notes 2 and 3 in Appendix J of U.S. NRC Regulatory Guide 1.183, which states that sensitivity/scoping analysis should not comprise a significant part of the EAB, outer boundary of the LPZ and control room analysis, and scoping analysis may be used where a number of similar analyses are involved and generic conclusions can be drawn. However, scoping analysis should not be used for EAB / outer boundary of the LPZ / control room doses.*

Appendix F - Single TEDE Limit (10 CFR 50.67) versus Separate Whole Body and Thyroid Dose Limits (10 CFR 100.11)

Before proposing and accepting the final rule on 10 CFR 50.67 “Alternative Source Term” [42] in 61 FR 65157 (Federal Register, Vol. 61. No. 239, Rules and Regulations 65157), the U.S. NRC performed a comprehensive assessment, referred to as rebaselining, of several plants to develop a better understanding of the impacts of implementing the Alternative Source Term (AST) assumptions and methods described in U.S. Regulatory Guide 1.183 at operating plants. The results of this assessment and the proposed amendments are documented in:

- SECY-98-154 (30 June 1998), “Results of the Revised (NUREG-1465) Source Term Rebaselining for Operating Reactors”; and
- SECY-98-289 (15 December 1998), “Proposed Amendments to 10 CFR Parts 21, 50, and 54 Regarding use of Alternative Source Terms at Operating Reactors”.

SECY-98-289 and 61 FR 65157 document the U.S. NRC’s interpretation of the single TEDE limit and their reasons for doing away with a separate thyroid dose limit in 10 CFR 50.67 [42].

The 10 CFR 100.11 whole body and thyroid dose limits were largely predicated by the assumed source term from TID-14844 (1962) “Calculation of Distance Factors for Power and Test Reactor Sites” being predominantly noble gases and radioiodine and the assumed "single critical organ" method of modelling the internal dose from ICRP Publication 2 (1959) used at the time that 10 CFR 100.11 was originally published. The whole body dose comes primarily from noble gases, and the thyroid dose is based on inhalation of radioiodine. It assumes that the major contributor to dose will be radioiodine resulting in the thyroid dose generally being limiting. Although this may be appropriate with the TID-14844 source term, as implemented by U.S. NRC Regulatory Guides 1.3 and 1.4, it may not be true for the AST [U.S. NRC Regulatory Guide 1.183] [47] based on a more complete understanding of accident sequences and phenomenology.

The postulated chemical and physical form of radioiodine in the AST (being predominantly aerosol) is more amenable to mitigation and, as such, radioiodine may not always be the predominant radionuclide in an accident release and systems needed to remove iodine vapours (elemental iodine) are less important under conditions where iodine is an aerosol. The AST include a larger number of radionuclides than the TID-14844 source term. The whole body and thyroid dose criteria ignore the contribution from these additional radionuclides to dose. The U.S. NRC amended its radiation protection standards in 10 CFR 20 in 1991, to replace the “single critical organ” concept for assessing internal exposure with the TEDE concept that assesses the impact of all relevant nuclides upon all body organs (weighted by their relative importance of risk). TEDE is defined to be the Deep Dose Equivalent (DDE) for external exposure plus the CEDE for internal exposure. The DDE is comparable to the present whole body dose; the CEDE is the sum of the products of doses (integrated over a 50-year period) to selected body organs resulting from the intake of radioactive material multiplied by weighting factors for each organ that are representative of the radiation risk associated with the particular organ from ICRP Publication 26 (1977).

The 10 CFR 50.67 TEDE [42] limit therefore utilizes a risk consistent methodology to assess the radiological impact of all relevant nuclides upon all body organs. It promotes uniformity and consistency in assessing radiation risk that may not exist with the separate whole body and thyroid dose criteria. Although it is expected that in many cases the thyroid could still be the limiting organ and radioiodine the limiting radionuclide, this conclusion cannot be assured in all potential cases. The TEDE numerical value of 250 mSv was selected since it is equivalent to the risk of latent cancer fatality implied by the 10 CFR 100.11 dose limit of 250 mSv whole body and 3 Sv thyroid (although a numerical calculation would lead to a value of 270 mSv, the U.S. NRC concluded that a value of 250 mSv is sufficiently close, and that the use of 270 mSv rather than 250 mSv implies an unwarranted numerical precision).

Furthermore, the final rule in 61 FR 65157 notes that when the U.S. NRC requested comments on whether the TEDE limit should include an additional organ “capping” limitation (that is, an additional requirement that the dose to any individual organ not be in excess of some fraction of the total), there was a nearly unanimous opinion that no organ “capping” dose was required, since the TEDE concept already provided the appropriate weighting for all body organs.

Lastly, it is noteworthy that the IAEA International Basic Safety Standards, which forms the basis of the NNR regulations [Regulations No. R. 388 [23]] and requirements, prescribes a maximum reference level of 100 mSv TEDE for individuals that are exposed to sources that are not under control. The basis for a TEDE limit of 100 mSv is that it is sufficiently low to avoid the occurrence of all deterministic health effects and reduce the risk of stochastic health effects to acceptable levels. In order to comply with IAEA International Basic Safety Standards, Section 3.5 and Table 3 propose that the maximum dose acceptance criteria of 250 mSv TEDE prescribed in 10 CFR 50.67 [42] be reduced to 100 mSv TEDE.