ENVIRONMENTAL IMPACT ASSESSMENT FOR THE PROPOSED NUCLEAR POWER STATION ('NUCLEAR-1') AND ASSOCIATED INFRASTRUCTURE

BEYOND-DESIGN-BASIS ACCIDENTS

September 2015

Prepared by: **J Slabbert**

Ψ PSI RISK CONSULTANTS CC

Prepared for: **Arcus GIBB Pty Ltd**

ARCUS GIBB ENGINEERING & SCIENCE

On behalf of: **Eskom Holdings SOC Ltd**

Eskom

DECLARATION OF INDEPENDENCE

I, Johan Slabbert, an independent consultant, hereby confirm my independence as a specialist and declare that I do not have any interest, be it business, financial, personal, or other, in any proposed activity, application, or appeal in respect of which Arcus GIBB was appointed as environmental assessment practitioner in terms of the National Environmental Management Act, 1998 (Act No. 107 of 1998), other than fair remuneration for work performed, specifically in connection with the Environmental Impact Assessment for the proposed conventional nuclear power station (‘Nuclear-1’). I further declare that I am confident in the results of the studies undertaken with information made available by Eskom and conclusions drawn as a result of it – as is described in my attached report.

JSlabbert

Full Name:	Johan Slabbert
Title / Position:	Nuclear Safety Analyst and Radiation Protection Specialist
Qualification(s):	BSc Hons; M.Phil, Environmental Management, EWI Post-graduate Training Course — Reactor Physics and Nuclear Fuel Management
Experience (years/months):	34 years in nuclear facilities safety analyses and radiological protection
Registration(s):	Pr Sci Nat (400028/96)

Table of Contents

List of Tables

List of Figures

Executive Summary

South Africa is considering the construction of a nuclear power plant (NPP) consisting of a combination of reactor units with a total electrical power capacity of up to 4 000 MWe and its associated infrastructure. The EIA makes provision for the potential future expansion of a NPP to allow for a total capacity of approximately 10 000 MWe on a site. It is envisaged that light water reactors (LWR) and specifically GEN III pressurised water reactors (PWR) will be the selected technology.

Accidents at NPPs have always been a concern of the public. This report provides an overview of some of the important NPP safety concepts that address this concern in the case of GEN III NPP designs. Safety analysis techniques applied to NPPs aim to provide confidence that safety principles promoted by the International Atomic Energy Agency (IAEA) and adopted by the South African National Nuclear Regulator will practically eliminate beyond-design-basis accidents (BDBAs), i.e. accidents that have the potential to release large quantities of radioactivity to the environment.

The Gen III NPP designs include distinctive safety characteristics in respect of sequences of events that could result in conditions outside the design basis of a NPP, known as design extension conditions. The results of safety analyses show that beyond-design-basis accidents that present a significant risk to the public and environment are practically eliminated as a result of provisions for design extension conditions. Examples of these safety characteristics are [1]:

- simpler designs making the reactors easier to operate and more tolerable of abnormal operating conditions;
- passive safety features in the design of the structures, systems, and components (SCCs) that avoid use of active control and relying on natural phenomena such as natural circulation of cooling media, e.g. cooling of the containment building to avoid overpressure;
- reduced probabilities for the failure of SCCs and a lower reactor core damage frequency (CDF) compared to earlier generation reactors (an order of magnitude reduction);
- new design features that provide mitigation to reduce the release of radioactivity to the environment significantly should the reactor core melt; and
- improved resistance to external hazards such as aircraft crash and extreme natural events.

Mitigation of off-site consequences in the case of GEN III NPPs should only be required in the most extreme and unlikely accident situations and then only with very limited consequences in space and time, i.e. emergency actions will be applied for short periods and in a small radius around the NPP.

There have been three major BDB reactor accidents in the history of civil nuclear power. Each of these accidents had a different impact on the public and the environment:

- Three Mile Island (USA 1979) – The reactor of unit 2 was severely damaged but radiation was contained and there were no adverse health or environmental consequences.
- Chernobyl (Ukraine 1986) – A destruction of reactor unit two caused by a steam explosion and a fire, an accident that killed 31 people in the early phase of the accident and had significant health and environmental consequences. The death toll has since increased.
- Fukushima (Japan 2011) – Three older generation boiling water reactors suffered severe damage and together with a fourth, were written off. The loss of cooling to the reactors as a result of the earthquake-induced tsunami resulted in failure to contain the radioactivity released from the damaged reactor cores.

Two of the three NPP BDBAs that were classified as severe accidents involving reactor core melts, were light water reactor designs that include reactor containment, the final barrier against a release of radioactivity to the environment during a BDBA. The NPP at Fukushima Daiichi in Japan were boiling water reactors that were subjected to a combination of extreme external events on 11 March 2011. The reactor containments withstood the challenges of the external events but not the subsequent internal explosions. When the pressurised water reactor at Three Mile Island reactor unit two in the United States suffered a BDBA, it had limited impact on the environment and people. It avoided the internal explosions that would have challenged the integrity of the reactor containment. The nuclear industry realised the importance of a robust reactor containment design. It has been one of the major safety enhancement areas in the design of Generation III / III+ reactors.

A comparison of the GEN III PWR reactor probabilities (expressed as an annual frequency) of a large radioactivity release during a BDBA that could result in radiological exposure of the public with a high fatality risk, indicates that the regulatory limit of the National Nuclear Regulator (NNR) will be met. The frequencies in Table E-1 can be compared to the NNR peak individual fatality risk of 5E-06 per year.

Table E-1: Core damage and large release fraction frequencies for GEN III NPPs

GEN III Reactor Designs for PWR	Light Water Reactor Type	Core Damage Frequency (events per reactor year)[1]	Large Radioactivity Release Frequency (events per reactor year)
AES-92	Pressurised Water Reactor (PWR)	6.10E-07	1.80E-08
AP1000	PWR	5.10E-07	3.90E-08
APR-1400	PWR	2.70E-06	8.20E-08
APWR	PWR	4.60E-06	8.10E-07
EPR	PWR	6.10E-07	3.90E-08

A new NPP to be built in South Africa will have to submit a safety analysis report that provides the evidence for this provisional conclusion. This evidence have to be based on an analysis of external and internal potential initiating events for purposes of accidents analyses, specific to the selected NPP design and specific site where it will be built.

The safety features of GEN III NPPs are significantly advanced when compared to the NPP designs that suffered BDBAs in the past. However, the lessons learnt from the Fukushima Daiichi accident will remain of paramount importance in the nuclear power industry. In a recently published report on the accident, the director general of the IAEA emphasised the culture that has to be entrenched in the nuclear industry:

> *"There can be no grounds for complacency about nuclear safety in any country. Some of the factors that contributed to the Fukushima Daiichi accident were not unique to Japan. Continuous questioning and openness to learning from experience are key to safety culture and are essential for everyone involved in nuclear power. Safety must always come first."*

[1] The US NRC requirement for calculated core damage frequency is 1E-04. Most current US plants have about 5E-05 and GEN III NPPs are about ten times better than this. The IAEA safety target for future plants is 1E-05.

Glossary

Terms

Cladding

The thin-walled metal tube that forms the outer jacket of a nuclear fuel rod. It prevents the corrosion of the fuel by the coolant and the release of fission products into the coolants. Aluminium, stainless steel, and zirconium alloys are common cladding materials.

Contamination

Radioactive substances on surfaces or within solids, liquids, or gases (including the human body), where their presence is unintended or undesirable, or the process giving rise to their presence in such places.

Coolant

A substance circulated through a nuclear reactor to remove or transfer heat. The most commonly used coolant is water. Other coolants include air, carbon dioxide, and helium.

Core

The central portion of a nuclear reactor containing the fuel elements and control rods.

Critical Group (also see Representative Person)

A group of members of the public (in the general population) which is reasonably homogeneous with respect to its exposure for a given radiation source and given exposure pathway and is typical of individuals receiving the highest dose by the given exposure pathway from the given source.

Dose

Absorbed Dose: It is the fundamental dose quantity given by:

$$D = \frac{d\bar{\varepsilon}}{dm}$$

Where $d\bar{\varepsilon}$ is the mean energy imparted to matter of mass dm by ionising radiation. The SI unit for absorbed dose is joule per kilogram ($\mathrm{Jkg^{-1}}$) and its special name is Gray (Gy).

Decay heat

The heat produced by the decay of radioactive fission products after the reactor has been shut down.

Committed Effective Dose: A weighted measure of the radiation energy received or absorbed by the whole body and measured in units of sievert (Sv); more specifically, the tissue-weighted sum of the equivalent doses in all specified tissues and organs of the body. The commitment period is taken to be 50 years for adults, and to age 70 years for children.

Annual Effective Dose: The total effective dose, E_T to a person is calculated according to the following formula:

$$E_T = H_p(d) + \sum_j e(g)_{j,ing} I_{j,ing} + \sum_j e(g)_{j,inh} I_{j,inh}$$

where $H_p(d)$ is the personal dose equivalent from exposure to penetrating gamma radiation during the year; $e(g)_{j,ing}$ and $e(g)_{j,inh}$ are the committed effective dose per unit intake by ingestion and inhalation for radionuclide j by the group of age g; and $I_{j,ing}$ and $\mathrm{I_{j,inh}}$ are the intakes via ingestion or inhalation of radionuclide j during the same period.

Exposure

The act or condition of being subject to ionising radiation. Public exposure is exposure incurred by members of the public from radiation sources, excluding any occupational or medical exposure and the normal local natural background radiation.

Potential exposure is exposure that is not expected to be delivered with certainty but that may result from an accident at a source or an event or sequence of events of a probabilistic nature, including equipment failures and operating errors.

Exposure pathway

A route by which radiation or radionuclides can reach humans and cause exposure. An exposure pathway may be very simple, e.g. external exposure from airborne radionuclides, or a more complex chain, e.g. internal exposure from drinking milk from cows that ate grass contaminated with deposited radionuclides.

Fuel rod

A long, slender tube that holds fuel (fissionable material) for nuclear reactor use. Fuel rods are assembled into bundles called fuel elements or fuel assemblies, which are loaded individually into the reactor core.

Gray (Gy)

The special name for the SI unit of absorbed dose:

$$1\ Gy = J\ kg^{-1}.$$

Nuclear damage

Any injury to or the death or any sickness or disease of a person, or other damage including any damage to or any loss of use of property or damage to the environment, which arises out of or results from, or is attributable to, the ionising radiation associated with a nuclear installation.

Pressure vessel

A strong-walled container housing the core of most types of power reactors.

Pressuriser

A tank or vessel that controls the pressure in a certain type of nuclear reactor.

Radiation (ionising)

The emission and propagation of energy through space or matter in the form of electromagnetic waves (e.g. gamma rays) or fast-moving particles such as alpha and beta particles and can cause ionisation in matter.

Radioactive

The condition of a material exhibiting the spontaneous decay of an unstable atomic nucleus into one or more different elements (e.g. uranium decays into various isotopes of radium, thorium, and lead).

Radioactive material

Material designated by the National Nuclear Regulator as being subject to regulatory control because of its radioactivity, often taking account of both activity and activity concentration.

Radiation effect

Stochastic effects of radiation: Malignant disease and heritable effects for which the probability of an effect occurring, but not its severity, is regarded as a function of dose without threshold.

Deterministic effect: Injury in populations of cells, characterised by a threshold dose and an increase in the severity of the reaction as the dose is increased further. Also termed tissue reaction. In some cases, deterministic effects are modifiable by post-irradiation procedures including biological response modifiers.

Reactor (nuclear)

A device in which nuclear fission may be sustained and controlled in a self-supporting nuclear reaction. There are several varieties, but all incorporate certain features, such as fissionable material or fuel, a moderating material (to control the reaction), a reflector to conserve escaping neutrons, provisions for removal of heat, measuring and controlling instruments, and protective devices.

Representative Person

An individual receiving a dose that is representative of the more highly exposed individuals in the population. This term is equivalent of, and replaces, “the average member of the Critical Group”.

Risk

A multi-attribute quantity expressing hazard, danger, or probability of harmful or injurious consequences associated with actual or potential exposures. It relates to quantities such as the probability that specific deleterious consequences may arise and the magnitude and character of such consequences.

Sievert (Sv)

The SI unit of equivalent dose and effective dose, equal to 1 J/kg. In this report it refers to effective dose, the summation of tissue equivalent doses, each multiplied by the appropriate tissue weighting factor.

Sites
The Eskom sites at Thyspunt, Bantamsklip, and Duynefontein being assessed for Nuclear Power Plants.

Steam Generator
The heat exchanger used in some reactor designs to transfer heat from the primary (reactor coolant) system to the secondary (steam) system. This design permits heat exchange with little or no contamination of the secondary system equipment.

Structures, systems, and components (SSCs)
A general term encompassing all of the elements (items) of a NPP that contribute to protection and safety, except human factors. Structures are the passive elements such as buildings, vessels, and shielding. A system comprises several components, assembled in such a way as to perform a specific (active) function. A component is a discrete element of a system.

Abbreviations

µSv	microsievert, 10^{-6} sievert (one millionth of a sievert)
ALARA	As Low As Reasonably Achievable
AOO	Anticipated Operational Occurrence
BDBA	Beyond-Design-Basis Accident
Bq	becquerel
Bq/ℓ	becquerel per litre
Bq/m^3	becquerel per cubic metre
CDF	Core Damage Frequency
CNS	Convention on Nuclear Safety
DBA	Design Basis Accident
DiD	Defence in Depth
DSA	Deterministic Safety Analysis
DSA	Deterministic Safety Analysis
DSR	Design Safety Review
EPR	European Pressurised Reactor
EUR	European Utility Requirement
GEN II, III	Generation II, III
GRSR	Generic Reactor Safety Review
Gy	Gray
IAEA	International Atomic Energy Agency
ICRP	International Commission on Radiological Protection
IEA	Environmental Impact Assessment
IEC	Incident and Emergency Centre
IES	Incident and Emergency System
INES	International Nuclear Event Scale
INIR	Integrated Nuclear Infrastructure Review
LERF	Large Early Release Fraction
LOCA	Loss of Coolant Accident
LWR	Light Water Reactor
mSv	millisievert, 10^{-3} sievert (one thousandth of a sievert)

NNR	National Nuclear Regulator
NPP	Nuclear Power Plant
OSART	Operational Safety Review Team
PCCS	Passive Containment Cooling System
PRIPE	Potential Radiological Impact on the Public and the Environment
PSA	Probabilistic Safety Analysis
PWR	Pressurised Water Reactor
RBMK	High Power Channel-Type Reactor
RSRP	Regulations on Safety Standards and Regulatory Practices
SSC	Structure, systems, and components
TMI	Three Mile Island
UK	United Kingdom
UNSCEAR	United Nations Scientific Committee on the Effects of Atomic Radiation
US NRC	United States (of America) Nuclear Regulatory Commission
USA	United States of America
WENRA	Western European Nuclear Regulators Association
Scientific notation for numbers	10 can be expressed as 1E01 or 1 × 10^1; 100 can be expressed as follows in scientific notation: 1E02 or 1 × 10^2; 0.1 is 1E-01 or 1 × 10^{-1} (one tenth); 0.01 is 1E-02 or 1 × 10^{-2}; etc.

1 INTRODUCTION

South Africa is considering the construction of a nuclear power plant (NPP) consisting of a combination of reactor units with a total electrical power capacity of up to 4 000 MWe and its associated infrastructure. The three sites included in the environmental impact assessment (EIA) are Thyspunt, Bantamsklip, and Duynefontein. The EIA makes provision for the potential future expansion of a NPP to allow for a total capacity of approximately 10 000 MWe on a site. It is envisaged that light water reactors (LWR) and specifically GEN III pressurised water reactors (PWR) will be the selected technology.

A fundamental safety question that concerns the public as well as the regulatory authorities, is how will a severe accident with a potentially large public health and environmental impact be avoided at the NPP, or, expressed in more simple terms, when things go wrong, how likely is a Fukushima-type accident? This report provides information to address this question. The report builds on information provided in Part 3 of the PRIPE report [1].

A plethora of sources exist on each of the topics in this report. An attempt is made to link with limited information some important NPP safety analysis concepts and BDBA examples from these sources. If required, the reader may consult the references for more detail on each topic. Of specific interest could be the detailed report by the director of the International Atomic Energy Agency on the Fukushima Daiichi accident, of which extracts are included in this report [2].

2 SCOPE

The reader is introduced to some of the important safety principles upon which NPP design and operation are based and how they relate to accidents that are defined as beyond-design-basis accidents (BDBAs).

The concept of defence in depth (DiD) and its application in the nuclear industry has been proven to be of cardinal importance as a result of lessons learnt from NPP accidents. DiD is discussed and the associated safety assessment methodologies. Mitigation of a potential severe accident at a NPP relies on the proper implementation of DiD to be demonstrated using various safety analysis methodologies in an integrated manner.

Three major NPP accidents demonstrated weaknesses in the application of the fundamental nuclear safety principles. Three Mile Island, Chernobyl, and Fukushima Daiichi are discussed. The aim of new GEN III NPP designs is to practically eliminate these BDBAs.

An overview of national and international compliance criteria for nuclear facilities (regulatory framework) is provided. The role of the International Atomic Energy Agency (IAEA) in the event of an accident is described, including the Agency’s role in developing lessons learned and revision of international recommendations for ensuring that the accident is not repeated.

3 PRINCIPLES FUNDAMENTAL TO SAFETY IN THE NUCLEAR INDUSTRY

The fundamental safety objective for NPPs and other nuclear facilities is to protect people and the environment from harmful effects of ionising radiation. Measures must be in place to [3]:

- control the radiation exposure of people and the release of radioactive material to the environment;
- restrict the likelihood of events that might lead to a loss of control over nuclear processes and sources of radiation; and
- mitigate the consequences of such events if they were to occur.

The IAEA has formulated ten *safety principles* on the basis of which safety requirements are developed and safety measures are implemented in order to achieve the fundamental safety objective. The ten safety principles are titled as follows [3]:

- Principle 1: Responsibility for safety
- Principle 2: Role of government
- Principle 3: Leadership and management for safety
- Principle 4: Justification of facilities and activities
- Principle 5: Optimisation of protection
- Principle 6: Limitation of risks to individuals
- Principle 7: Protection of present and future generations
- Principle 8: Prevention of accidents
- Principle 9: Emergency preparedness and response
- Principle 10: Protective actions to reduce existing or unregulated radiation risks

The focus in this report is on Principle 8 that deals with the prevention of accidents.

4 BEYOND-DESIGN-BASIS ACCIDENTS AND RELATED SAFETY CONCEPTS

4.1 Main safety functions

The *main safety functions* of a NPP are [4]:

- reactivity control (i.e. control of the nuclear fission process);
- heat removal from the reactor core; and
- confinement of radioactivity (the barriers between radioactivity and the environment of which the reactor building is the most important during accident conditions).

A BDBA can only occur when these *main safety functions* have been compromised and the NPP is outside its design basis and a severe accident occurs. The resulting risk to workers, the public, and the environment requires an introduction to some important NPP safety analysis concepts, such as:

- how risk is defined;
- what is meant by the design basis of a NNP;
- how is the design basis assessed; and

- how and when can events challenge the safety of a NPP that potentially result in consequences that are outside the design basis and cause a BDBA with a significant health risk.

Terms such as hazard, initiating event, accident, and risk relate to one another. A hazard is a characteristic of the site where a NPP is located or an aspect of the NPP that represents a potential for an accident. An initiating event is an occurrence that can potentially lead to an event sequence (a series of failures) that could involve human errors and/or a NPP structure, system, or component (SCC) failure. In the absence of high-quality safety systems, an event sequence can result in an accident. Unsuccessful mitigation of an accident can result in a severe accident and release of radioactivity to the environment. An initiating event can be as a result of an external hazard, e.g. an earthquake, or internal, e.g. a NPP operator error or loss of electrical supply to a cooling water pump. Aircraft, for example, represent an external hazard to a NPP. The probability of an initiating event such as an aircraft crashing into a NPP is determined by the distance to airports and aircraft traffic volumes in the vicinity of the NPP. The damage caused by the aircraft crash, the initiating event, set in motion a potential sequence of events involving failures of SSC that could compromise one or more of the main safety functions. In an extreme and low probability situation when all safety related SSCs malfunction and severe accident management procedures fail, a BDBA can occur. Figure 4-1 is a simple illustration of measures to protect a NPP against hazards. Tested safety principles in the nuclear power industry and regulatory criteria are conditions with which a NPP operator has to comply. The occurrence of initiating events that could result in challenges to the NPP safety and set in motion a sequence of events that could result in a BDBA, must be protected against by various independent safety-related SSCs.

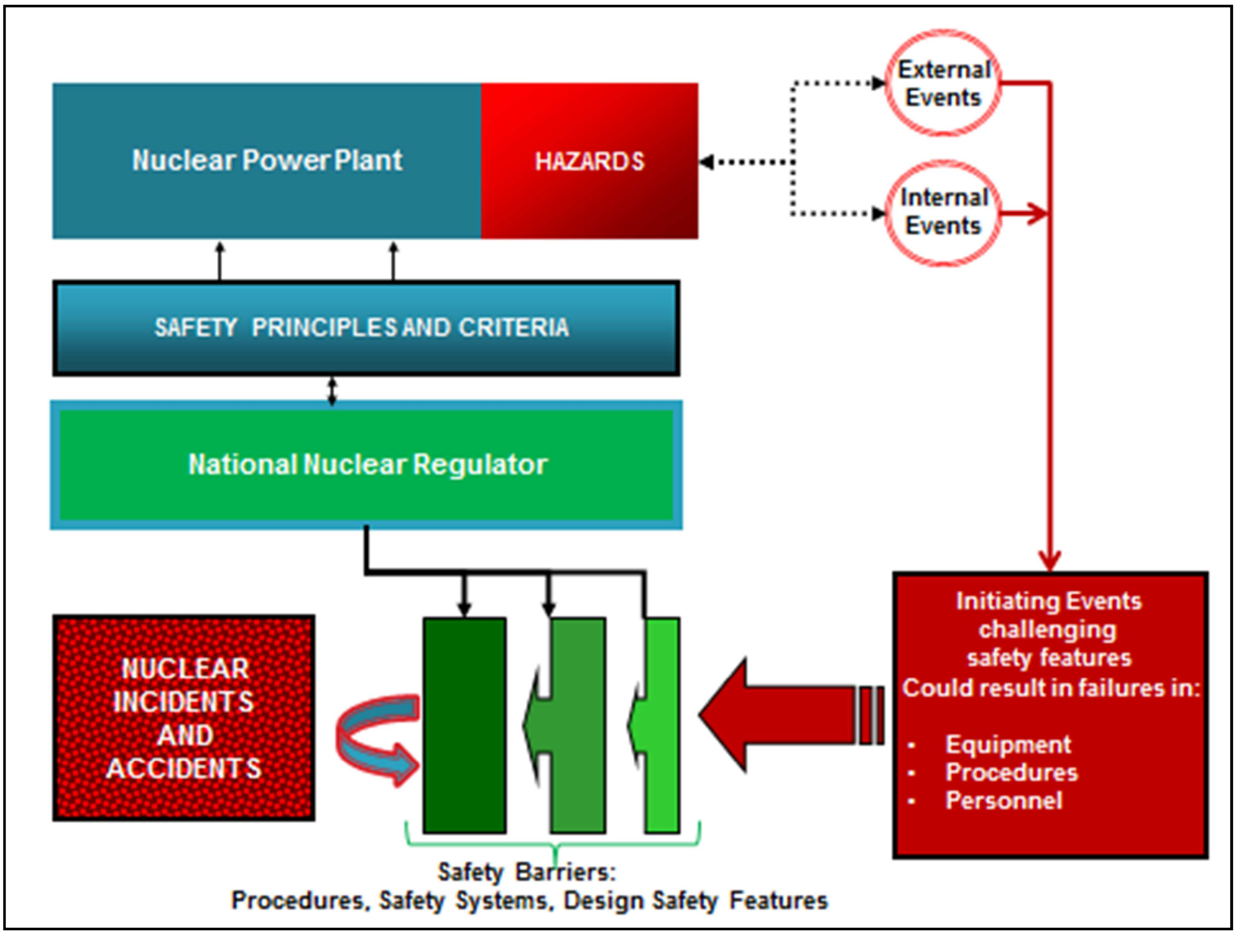

Nuclear Power Plant
HAZARDS
External Events
Internal Events
SAFETY PRINCIPLES AND CRITERIA
National Nuclear Regulator
NUCLEAR INCIDENTS AND ACCIDENTS
Initiating Events challenging safety features Could result in failures in:
• Equipment
• Procedures
• Personnel
Safety Barriers:
Procedures, Safety Systems, Design Safety Features

Figure 4-1: Hazards and nuclear incidents and accidents

Safety assessments of a highly complex technical nature are carried out to identify and define hazards, determine the likelihood of initiating events that could result from these hazards, and calculate the magnitude of the potential radioactivity releases and radiological risk. Safety assessments will identify a broad spectrum of potential exposure scenarios, ranging from those with little or no impact to those with a very high potential impact. The design and operation of a NPP have to be such that accidents with severe consequences have extremely low probabilities.

4.2 Design basis and design basis accident

The design basis of a NPP is information that identifies specific functions to be performed by SSCs of a NPP. It includes the specific values or range of values chosen for controlling parameters as reference bounds for design of these SSCs (e.g. pressure control and allowable maximum pressure in a pressure vessel) [4]. These values are derived from:

- general accepted state-of-the-art good engineering practices for achieving SSC functional goals; and
- requirements derived from analyses of the effects of postulated design basis accidents (DBAs), for which a SSC must meet its functional goals.

A design basis accident (DBA) is defined as an accident causing conditions for which a NPP is designed in accordance with established design criteria and conservative methodology, and for which releases of radioactive material and exposure are kept within acceptable limits determined by the National Nuclear Regulator (NNR). The design basis of a NPP therefore represents a range of conditions and events taken explicitly into account in the design, according to established criteria, such that the planned operation of safety systems will prevent operational and regulatory limits being exceeded. A primary objective is to manage all DBAs so that they have no or only minor radiological impact on or off the NPP site, and do not necessitate any off-site intervention measures. The DBAs are analysed in a conservative manner using conservative assumptions, models, and input parameters in the analysis [7].

4.3 Design extension conditions and beyond-design-basis accidents

A BDBA in a NPP results in accident conditions more severe than DBAs, and in earlier nuclear safety publications it was classified as an accident that is postulated to occur less frequently than a DBA (typically less frequent than 1E-06 per year). There has been a fundamental change in the definition of BDBA since the IAEA publication on design safety of NNPs was issued in 2012 [8]. It supersedes the earlier IAEA publication on NPP safety standards [9]. The changes are illustrated in Figure 4-2 and show the different NNP conditions, progressing from normal operation to BDBAs. The concepts illustrated in Figure 4-2 are briefly discussed.

<table>
<tr><td colspan="6">2000: IAEA Safety Requirements publication on Safety of Nuclear Power Plants: Design -Safety Standards Series No. NS-R-1</td></tr>
<tr><td colspan="2">Operational States</td><td colspan="4">Accident Conditions</td></tr>
<tr><td>Normal Operation</td><td>Anticipated Operational Occurrence</td><td>Design Basis Accidents</td><td colspan="3"><b><i>Beyond Design Basis Accidents</i></b></td></tr>
<tr><td colspan="3"></td><td></td><td><b><i>Severe Accidents</i></b></td><td></td></tr>
<tr><td colspan="3">Included in the design basis</td><td colspan="3"><b><i>Beyond Design Basis Accidents</i></b></td></tr>
</table>

<table>
<tr><td colspan="6">2012: IAEA Safety Standards Series No. SSR-2/1 Safety of Nuclear Power Plants Design: Specific Safety Requirements</td></tr>
<tr><td colspan="2">Operational States</td><td colspan="4">Accident Conditions</td></tr>
<tr><td>Normal Operation</td><td>Anticipated Operational Occurrence</td><td>Design Basis Accidents</td><td colspan="2"><b><i>Design Extension Conditions</i></b></td><td rowspan="2"><b><i>Conditions Practically Eliminated</i></b></td></tr>
<tr><td colspan="3"></td><td>No Reactor Core Melt</td><td><b><i>Severe Accidents - Reactor Core Melt</i></b></td></tr>
<tr><td colspan="5">Included in the design basis</td><td><b><i>Beyond Design Basis Accidents</i></b></td></tr>
</table>

Figure 4-2: NPP states and accident conditions

4.3.1 Definitions of NNP accident conditions prior to 2012

The first NPP state beyond that of normal operation is termed an anticipated operational occurrence (AOO). It is any deviation from normal operation which is expected to occur at least once during the operating lifetime of a NPP. An AOO does not cause any significant damage to safety related SCCs or lead to accident conditions. An example of an AOO is a loss of normal electrical power, a turbine trip or loss of power to a main pump providing cooling water to the reactor core. The reactor can be returned to normal operation in a prompt and safe manner. If an AOO is not controlled it may lead to a DBA.

In the original schematic of the 2000 version of NPP conditions shown in Figure 4-2, progression from a DBA led directly into the domain of BDBAs. When the unlikely progression of an accident sequence continues, a severe accident state is reached, i.e. when all safety systems and operator actions have failed to return the NPP to DBA conditions. A severe accident normally involves damage to a significant fraction of the nuclear fuel in a reactor as opposed to damage of only a few fuel rods. (There are a 157 fuel elements comprising 41 448 fuel rods in a Koeberg type reactor core, each with an *active length* of 3.66 m along which the nuclear power is generated). The consequences can range from a significant fraction of the nuclear fission products being released into the primary cooling water circuit or progress to an uncontrolled dispersion of radioactivity into the environment. The accidents at Three Mile Island and Fukushima Daiichi were both severe accidents, but with very different consequences (refer to § 6.2 and § 6.3). A severe accident thus starts when there is a mismatch between the power produced by the reactor fuel and the power evacuated from it, i.e. a loss of adequate cooling. Several phenomena are typical of a severe accident associated with earlier pressurised water reactors (PWR) designs, for example:

- Chemical reactions take place between the fuel rod cladding material (zirconium alloy) and superheated steam resulting in hydrogen formation. The potential for an explosion then exists, an event dramatically demonstrated during the Fukushima Daiichi accident.

- Heat-up of the reactor fuel result in deformation of the core, the fuel geometry is lost and insufficient cooling results.
- Debris is formed in the lower plenum of a reactor vessel. Melting of the debris form a liquid corium, which releases most of the nuclear fission products into the primary coolant.
- A large fraction of dispersible fission products can now enter the atmosphere of the containment building leaving the containment building thereby breaching the final barrier between the radioactivity and the environment.
- If the reactor vessel eventually fails, the corium interacts with the reactor building structure.

4.3.2 Definitions of NPP conditions after 2012

The concept of a design extension condition has now been introduced; refer to Figure 4-2. It is defined as accident conditions that are not evaluated in the same conservative manner as DBAs, but are still explicitly considered in the design process of the facility. Safety assessment of design extension conditions are carried out with best estimate methodologies in order to demonstrate that potential release of radioactive material are kept within acceptable limits. Design extension conditions include severe accident conditions. The IAEA defines requirement in terms of design extension conditions as follows [8]:

> “A set of design extension conditions are derived on the basis of engineering judgement, deterministic assessments and probabilistic assessments for the purpose of further improving the safety of the NPP 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 are 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.
>
> 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 design basis accident conditions, or to mitigate their consequences, as far as is reasonably practicable. This might require additional safety features for design extension conditions, or extension of the capability of safety systems to maintain the integrity of the containment.
>
> These additional safety features for design extension conditions, or this extension of the capability of safety systems, ***must ensure the capability for managing accident conditions in which there is a significant amount of radioactive material in the containment (including radioactive material resulting from severe degradation of the reactor core)***. The plant shall be designed so that it can be brought into a controlled state and the containment function can be maintained, with the result that ***significant radioactive releases would be practically eliminated***.
>
> The design extension conditions shall be used to define the design basis for safety features and for the design of all other items important to safety that are necessary for preventing such conditions from arising, or, if they do arise, for controlling them and mitigating their consequences. This could be done with a best estimate approach (more stringent approaches may be used according to States’ requirements).
>
> ***In particular, the containment and its safety features shall be able to withstand extreme scenarios that include, among other things, melting of the reactor core.*** These scenarios shall be selected using engineering judgement and input from probabilistic safety assessments.

> ***The design shall be such that design extension conditions that could lead to significant radioactive releases are practically eliminated. If not, for design extension conditions that cannot be practically eliminated, only protective measures that are of limited scope in terms of area and time shall be necessary for protection of the public, and sufficient time shall be made available to implement these measures**.”*

Design extension conditions are included in the NPP designs that have been considered for the Eskom sites. GEN III NPPs have distinctive characteristics in respect of design extension conditions. These include [9]:

- simpler designs making the reactors easier to operate and more tolerable of AOOs;
- passive safety features in the design of the SCCs that avoid use of active control and relying on natural phenomena such as natural circulation of cooling media e.g. cooling of the containment building to avoid overpressure;
- reduced SCCs failure probabilities and a lower reactor core damage frequency compared to earlier generation reactors (an order of magnitude reduction);
- new design features that provide mitigation should the reactor core melt to significantly reduce the release of radioactivity to the environment; and
- improved resistance to external hazards such as aircraft crash and extreme natural events.

5 ASSESSMENT OF NPP DESIGN TO PREVENT A BDBA

5.1 Defence in Depth

The primary means of preventing and mitigating the consequences of accidents is ‘defence in depth’ (DiD). DiD is implemented primarily through the combination of a number of consecutive and independent levels of protection that would have to fail before significant nuclear damage can occur. If one level of protection or barrier were to fail, the subsequent level or barrier would be available for protection. No single technical, human, or organisational failure should lead to nuclear damage. Any combination of failures that could give rise to nuclear damage must be of very low probability. The independent effectiveness of the different levels of DiD is essential [5].

Five levels of defence in depth are defined. These are:

- Level 1: The aim is to maintain normal NPP operation and prevent the occurrence of abnormal operation and SSC failures. This is done by producing a conservative design and ensuring a high quality of construction and operation.
- Level 2: The aim is to control abnormal operation (AOOs) and detect failures should they occur. This is done by incorporating control and surveillance systems.
- Level 3: The aim is to control accidents within the design basis should they occur. DBAs should not progress to design extension conditions. This is done by incorporating engineered safety features and developing emergency operating procedures.
- Level 4: The aim is to control severe plant conditions and it requires the prevention of accident progression and the mitigation of the consequences. This is done by incorporating severe accident management measures that have been developed for these NPP conditions.
- Level 5: The aim is to mitigate the radiological consequences of releases of radioactive material from the plant. This is done by developing off-site emergency response measures.

The different levels of protection in the DiD principle is illustrated in Figure 5-1.

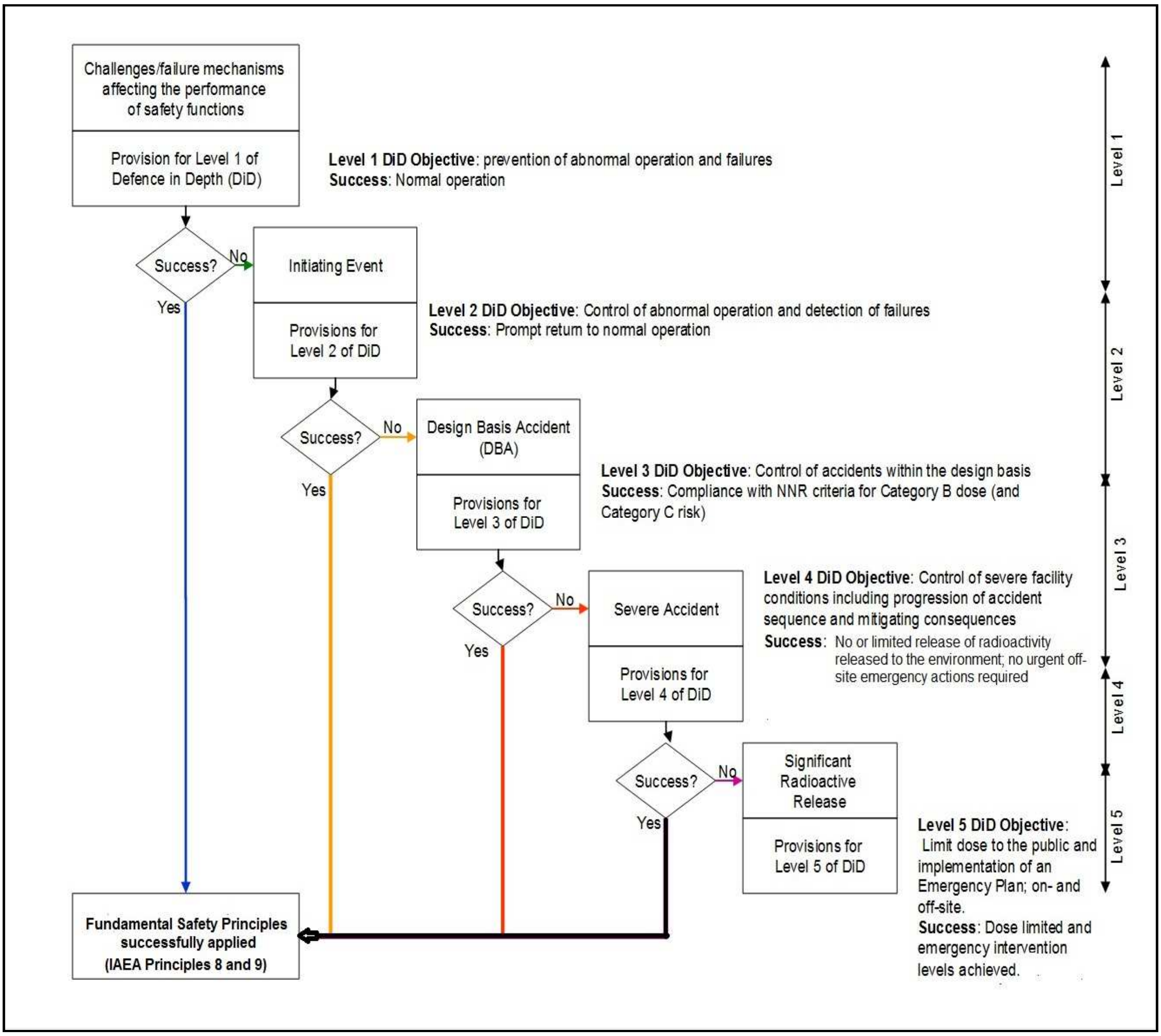

Challenges/failure mechanisms affecting the performance of safety functions
Provision for Level 1 of Defence in Depth (DiD)
Level 1 DiD Objective: prevention of abnormal operation and failures
Success: Normal operation
Success?
No
Yes
Initiating Event
Provisions for Level 2 of DiD
Level 2 DiD Objective: Control of abnormal operation and detection of failures
Success: Prompt return to normal operation
Success?
No
Yes
Design Basis Accident (DBA)
Provisions for Level 3 of DiD
Level 3 DiD Objective: Control of accidents within the design basis
Success: Compliance with NNR criteria for Category B dose (and Category C risk)
Success?
No
Yes
Severe Accident
Provisions for Level 4 of DiD
Level 4 DiD Objective: Control of severe facility conditions including progression of accident sequence and mitigating consequences
Success: No or limited release of radioactivity released to the environment; no urgent off-site emergency actions required
Success?
No
Yes
Significant Radioactive Release
Provisions for Level 5 of DiD
Level 5 DiD Objective: Limit dose to the public and implementation of an Emergency Plan; on- and off-site.
Success: Dose limited and emergency intervention levels achieved.
Fundamental Safety Principles successfully applied (IAEA Principles 8 and 9)
Level 1
Level 2
Level 3
Level 4
Level 5

Figure 5-1: Defence in Depth

5.2 Safety analysis methodologies

5.2.1 Introduction

A safety case, prepared for each NPP, requires a structure and content that have been agreed to by the NNR. It consists of a collection of arguments and evidence in support of the safety of a NPP and upon which a licence to construct and operate is issued, once approved by the NNR. A central part of the safety case is the technical safety analysis that considers potential initiating events that can lead to AOOs, DBAs, design extension conditions, and BDBAs. The results of a safety analysis must demonstrate compliance with regulatory criteria and international standards for nuclear safety (refer to § 8).

The safety analysis of a new NPP assesses, in a prospective manner, the risk of nuclear damage (refer to the glossary for a definition). For each potential scenario for accidental exposure to ionising radiation, a dose to the most highly exposed member of the public (the representative person) and the probability of the exposure scenario is calculated. This radiological health risk of an accident scenario

i can be expressed by combining the probability of the scenario ***p_i*** occurring and the probability of the health effects as a result radiological exposure, **C_i:**

$$R_i = p_i \times C_i$$

where:

R_i is the risk of a health effect.

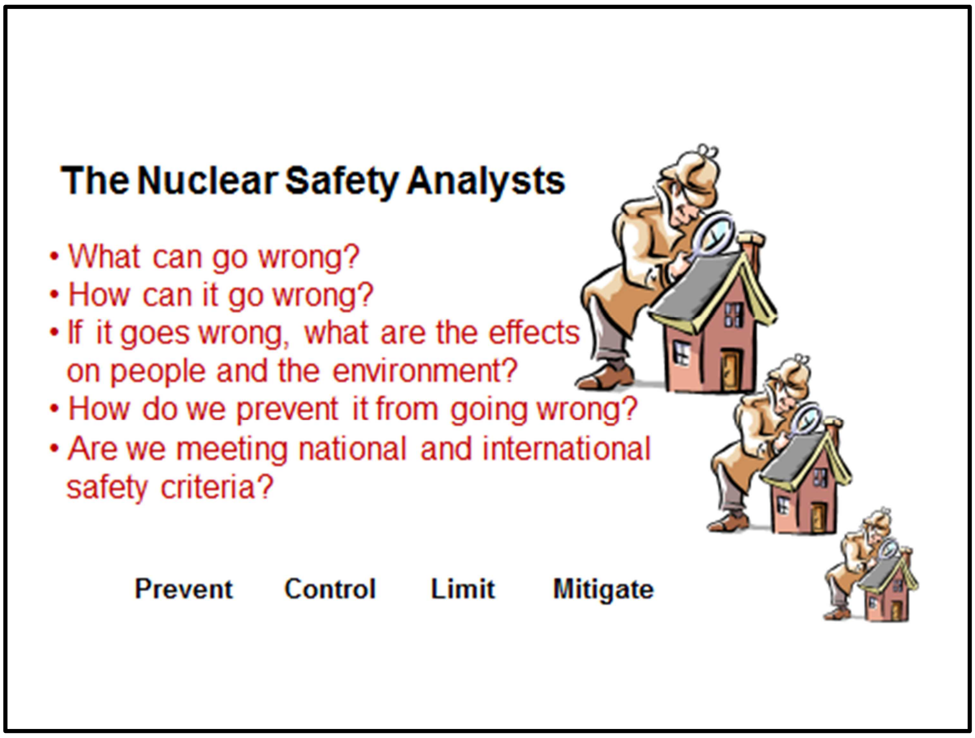
If accident scenarios that have been identified are mutually independent and their probabilities are low, the risks of all the scenarios could then be added to give the overall risk:

$$R = \sum_i \; p_i \times C_i$$

The NNR risk criteria are discussed in § 8.

The two most important safety analysis methods are briefly discussed and serve as examples of the rigorous processes involved. They are deterministic safety analysis (DSA) and probabilistic safety analysis (PSA) methods. DSA and PSA establish and confirm the design basis for the SSCs important to safety, e.g. reactor shutdown systems and emergency cooling systems that have to ensure the main safety functions of reactivity control and heat transfer from the reactor core.

A team of nuclear safety analysts apply DSA and PSA tools to all potential accident phenomena and SSC failures. They have to provide answers to some basic questions, for example those illustrated in Figure 5-2. They use DSA and PSA to demonstrate that the fundamental safety functions of a NPP are available with extremely high reliability.



The Nuclear Safety Analysts

- What can go wrong?
- How can it go wrong?
- If it goes wrong, what are the effects on people and the environment?
- How do we prevent it from going wrong?
- Are we meeting national and international safety criteria?

Prevent **Control** **Limit** **Mitigate**

Figure 5-2: Nuclear safety analysts at work

DSA and PSA are applied in an integrated manner. The two methodologies use different techniques and boundary conditions. Each methodology has strengths and limitations and used together, the limitations of each methodology is compensated for.

5.2.2 Deterministic safety analysis

The aim of a DSA is to study NPP behaviour under specific pre-determined operational and accident conditions to determine whether the design is adequate in respect of safety criteria applicable to these conditions [11]. A set of conservative rules and requirements, taking into account uncertainties in the performance of equipment and humans, are defined in the DSA. Compliance provides a high degree of confidence that the radiation dose and therefore health risk to workers and members of the public will be acceptably low.

The framework for DSA provides for DiD in a NPP design. The application of the DiD approach to the design and operation of NPPs provides multiple means of carrying out safety functions and multiple barriers in place to prevent the release of radioactive material from the plant. The aim in NPP design and its safety systems is to provide a large margin between the expected plant behaviour following an initiating event and the potential failure of any of the barriers to the release of radioactive material. These margins take account of uncertainties in the analysis methods and data. During a loss of coolant accident (LOCA), for example, the operation of emergency core cooling systems needs to ensure that there is a large margin between the conditions that would be reached in the reactor core and those that would lead to overheating of the fuel elements. There must be a high degree of confidence that nuclear fuel failures would not occur. Similarly, the operation of the reactor containment systems needs to ensure that there is a large margin between the temperature and pressure conditions reached in the containment following a severe accident and those that would lead to failure and a release of radioactivity to the environment.

DSA also assesses the application of the safety principles such as the single failure requirement, prevention of common cause failures, equipment qualification, and high levels of quality assurance amongst other safety requirements. Application of the single failure requirement ensures that SCCs providing a specific safety function are designed in such a way that no single failure prevents the safety function from being carried out by SSC important to safety. Therefore, the safety systems usually have more than one train of equipment that is capable of carrying out a specific safety function. The analysis that is carried out for design basis accidents assumes that the worst single failure occurs following the initiating event.

Common cause failures are provided for by redundancy, i.e. supplying additional and independent SCCs to perform the same safety function, preferably in different locations in the NPP (to avoid fire and flooding, for example, negating the redundancy measures). Diversity of safety equipment is another means of avoiding common cause failures. When high reliability is required, diverse means of carrying out the safety function need to be incorporated. Diversity is provided by using different physical processes, using different equipment, and in some cases, different manufacturers for redundant systems.

The main strength of DSA approach is that it has well-developed techniques and that there is a large body of international experience in its application. This information is made available to NPPs through research organisations, regulatory authorities, and especially by the IAEA.

There are some shortcomings in the deterministic approach of DSA. DSA only takes initiating event frequencies and component failure probabilities into account in an approximate way so that it is not always clear that a NPP has a balanced design; i.e. certain event sequences and accidents contribute disproportionately to the NPP risk. These shortcomings are compensated for by applying PSA.

5.2.3 Probabilistic safety analysis approach

A PSA is carried out during the design process of new NPPs and is maintained during the life of a NPP to evaluate any changes in operating procedures and SCCs. Its role is to study the accident sequences that include multiple SSC failures and human error. Its results have to verify safety criteria for core damage probability (CDF expressed as an annual frequency of occurrence), large early radioactivity release frequency in the case of a BDBA (LERF), and human health risk.

A PSA is typically carried out at three levels:

- Level 1 PSA: The initiating events and event sequences that can lead to damage of the reactor core and stored irradiated fuel are identified and the CDF is calculated. Level 1 provides insights into the strengths and weaknesses of the SSCs and operating procedures of the NPP and provides the following specific information:
  - identification of the dominant accident sequences leading to core damage;
  - identification of SSCs and human actions that are important for safety; and
  - assessment of dependencies between systems and between human actions and systems.
- Level 2 PSA: An analysis of accident phenomena is carried out, the ways in which radioactive releases from a NPP can occur are identified, and the magnitude and frequencies of these releases are calculated. The Level 2 PSA provides additional insights into the relative importance of accident prevention and mitigation measures to maintain, for example, reactor containment integrity or the use of other means to control releases. Some typical uses of Level 2 PSA are:
  - to gain insights into the progression of severe accidents and containment performance;
  - to identify specific vulnerabilities of the containment to severe accidents;
  - to identify major containment failure modes and to estimate the corresponding releases of radionuclides;
  - to provide a basis for the evaluation of off-site emergency planning strategies;
  - to provide a basis for the development of specific accident management strategies; and
  - to provide a basis for the prioritisation of safety research activities.
- Level 3 PSA: Public radiological health risk is estimated, as well as other societal risks such as the contamination of land or food. The regulatory risk criteria are discussed in § 8. The elements of a risk estimate include the following:
  - description of the radionuclides release source terms (from PSA Level 2);
  - environmental dispersion and deposition based on meteorological data as well as marine/river data;
  - exposure pathways;
  - population, agricultural, and economic data;
  - health effects, and
  - information to develop counter-measures to the consequences of BDBA.

The benefits of using PSA in an integrated manner with DSA are that the following characteristics of a NPP can be confirmed:

- The NPP design is balanced across all initiating events and ensures that any group of initiating events does not make a contribution to the risk that is much larger than others.
- The design is balanced across levels of DiD and it has been implemented adequately, something that is not possible using DSA alone; and

- The PSA models all initiating events, SSCs failures, and human errors in a single model so that the relative importance of each of them can be determined, something that is not possible with DSA.

5.3 External events

Fukushima Daiichi demonstrated the importance of events as a result of external hazards. They have a potential for affecting many different SSCs simultaneously. GEN III NPPs include safety features to cope with extreme external events based on lessons learnt from the Fukushima Daiichi accident. The safety features will be measures against the specific external hazards that exist at each of the three Eskom sites. The potential initiating events from external hazards at the sites will be included in the DSA and PSA of a new NPP. Examples of external hazards are illustrated Figure 5-3 [12].

Figure 5-3 Illustrations of some of the external hazards considered in the design of a NPP: tsunami, earthquake, severe weather phenomena, aircraft crash, solar flares, and chemical explosion

Combinations of external events also have to be considered, e.g. seismicity and flooding as experienced at Fukushima Daiichi. The Fukushima Daiichi NPP survived the earthquake of a magnitude that caused ground motion beyond the design basis of some NPP structures. It was the subsequent tsunami that resulted in a severe accident progressing into a BDBA. The framework for external event analysis is illustrated in Figure 5-4.

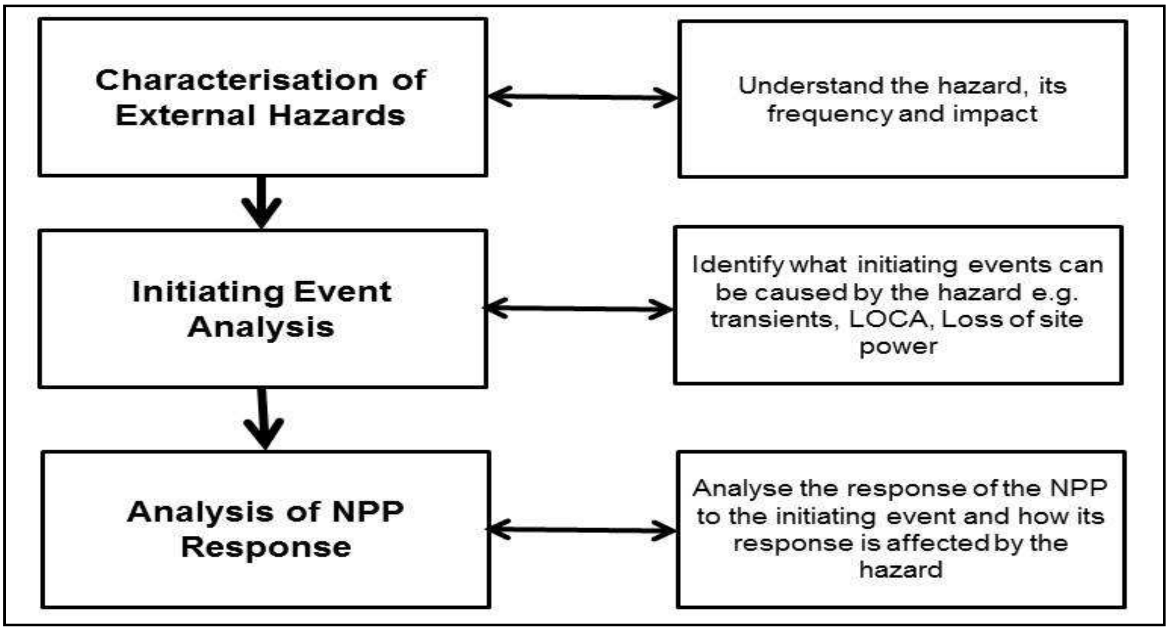

Characterisation of External Hazards
Understand the hazard, its frequency and impact
Initiating Event Analysis
Identify what initiating events can be caused by the hazard e.g. transients, LOCA, Loss of site power
Analysis of NPP Response
Analyse the response of the NPP to the initiating event and how its response is affected by the hazard

Figure 5-4: External event analysis

An example of how external events are considered in the design of a NPP is that of an aircraft crash. The NNR requires a design-specific assessment of the effects on a NPP of the impact of a large commercial or military aircraft [10]. It includes a probabilistic evaluation of the air traffic in the vicinity of a NPP.

Apart from a probabilistic assessment of aircraft crash frequencies, many designers of NPPs have studied the consequences of an aircraft crash more closely in a deterministic way, partly in response to the possibility of malevolent human actions such as the 9/11 terrorist event in New York. In response to this, some NPP designs now include double containment structures and reduced above-ground vertical profiles. It aims to also provide protection against malevolent human-induced external events that cannot be defined in a probabilistic manner in a PSA. A deterministic approach is also used to show that following the impact of a large commercial aircraft, considered to be a design extension condition, the reactor core remains cooled, the reactor building containment remains intact and spent fuel pool integrity is maintained [11].

An example of how the designs of GEN III reactors have evolved to include aircraft crash is that of the French EPR reactor. Originally, the EPR design basis considered the direct impact on the NPP of general aviation and military aircraft only. After the 9/11 event, the EPR design was enhanced to safely withstand a deliberate impact of a large commercial aircraft, including the consequences of a fuel fire following the impact [12].

Lessons learnt from the Fukushima Daiichi accident have been taken into account in the design of GEN III NPPs. External event reviews and so-called stress tests have also been carried out to identify potential weaknesses in currently operating NPPs should extreme external events be experienced. The insights obtained from the stress tests are used to strengthen the design basis and improve response to design extension conditions.

5.4 NPP safety road map

A limited number of elements of a NPP safety case have been discussed in § 5. The extent of the safety principles to be demonstrated throughout the life of a NPP life is illustrated in Figure 5-5 [13]. It shows the rigorous approach and extensiveness of safety analysis and safety provisions.

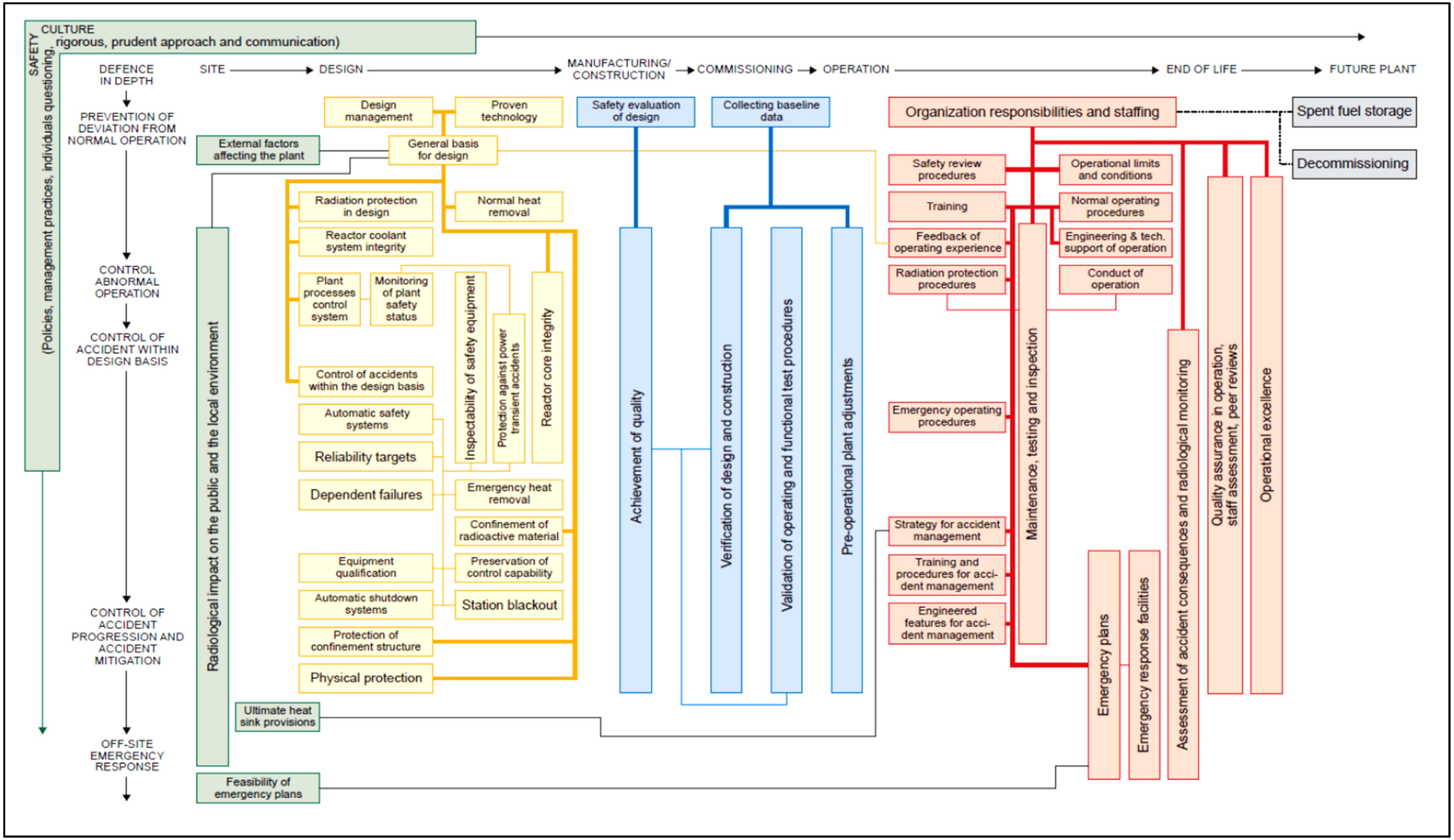

SAFETY CULTURE
(Policies, management practices, individuals questioning, rigorous, prudent approach and communication)
DEFENCE IN DEPTH
SITE
DESIGN
MANUFACTURING/ CONSTRUCTION
COMMISSIONING
OPERATION
END OF LIFE
FUTURE PLANT
PREVENTION OF DEVIATION FROM NORMAL OPERATION
CONTROL ABNORMAL OPERATION
CONTROL OF ACCIDENT WITHIN DESIGN BASIS
CONTROL OF ACCIDENT PROGRESSION AND ACCIDENT MITIGATION
OFF-SITE EMERGENCY RESPONSE
External factors affecting the plant
Radiological impact on the public and the local environment
Ultimate heat sink provisions
Feasibility of emergency plans
Design management
Proven technology
General basis for design
Radiation protection in design
Normal heat removal
Reactor coolant system integrity
Plant processes control system
Monitoring of plant safety status
Inspectability of safety equipment
Protection against power transient accidents
Reactor core integrity
Control of accidents within the design basis
Automatic safety systems
Reliability targets
Dependent failures
Emergency heat removal
Confinement of radioactive material
Equipment qualification
Preservation of control capability
Automatic shutdown systems
Station blackout
Protection of confinement structure
Physical protection
Safety evaluation of design
Achievement of quality
Collecting baseline data
Verification of design and construction
Validation of operating and functional test procedures
Pre-operational plant adjustments
Organization responsibilities and staffing
Safety review procedures
Training
Feedback of operating experience
Radiation protection procedures
Emergency operating procedures
Strategy for accident management
Training and procedures for accident management
Engineered features for accident management
Maintenance, testing and inspection
Operational limits and conditions
Normal operating procedures
Engineering & tech. support of operation
Conduct of operation
Emergency plans
Emergency response facilities
Assessment of accident consequences and radiological monitoring
Quality assurance in operation, staff assessment, peer reviews
Operational excellence
Spent fuel storage
Decommissioning

Figure 5-5: Safety principles and a NPP lifecycle

6 BEYOND-DESIGN-BASIS ACCIDENTS IN THE NUCLEAR POWER INDUSTRY: THREE MILE ISLAND, FUKUSHIMA DAIICHI, AND CHERNOBYL

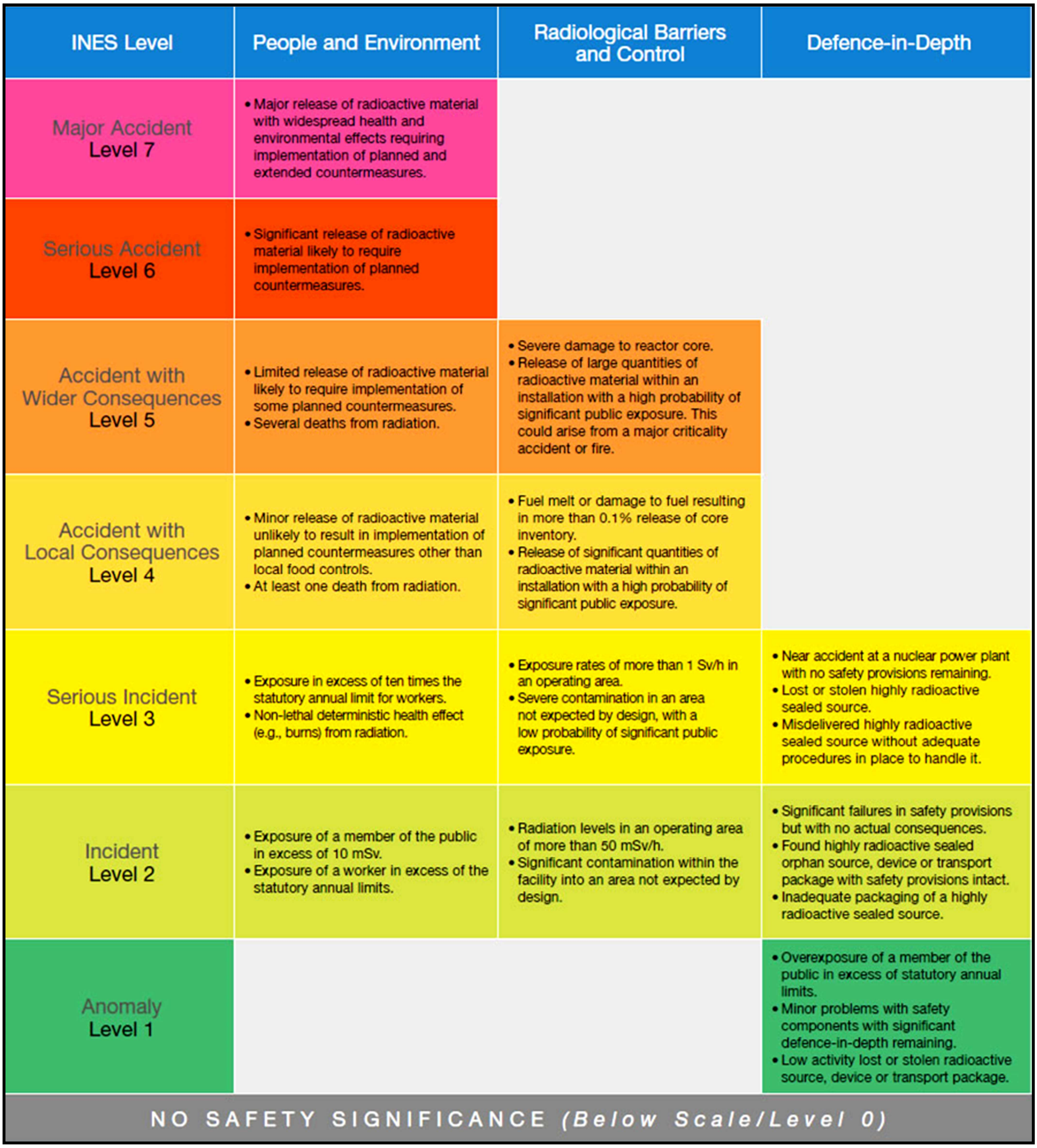
6.1 The International Nuclear Event Scale

The International Nuclear Event Scale (INES) system is briefly discussed to provide perspective on the three NPP accidents that are discussed in subsequent sections. It serves as a framework to categorise nuclear incidents and accidents and the severity of the consequences of these events [14].

The primary purpose of INES is to facilitate communication and understanding between the technical community, the media, and the public on the safety significance of nuclear and other radiological events and accidents. The aim is to keep both the public and nuclear authorities accurately informed on the occurrence and consequences of reported events. The INES levels are illustrated in Figure 6-1.

The accident at Three Mile Island was an INES Level 5 accident. It fits in the column titled “Radiological Barriers and Control” since severe damage was suffered by the reactor core but it had no significant impact on people and the environment.

The Chernobyl and Fukushima Daiichi accidents were both at Level 7. The Chernobyl accident resulted in widespread health effects that included worker deaths from radiation exposure, evacuation of a large number of people, and extensive environmental contamination. The Fukushima Daiichi accident resulted in environmental contamination and evacuation of people. No radiation deaths have been reported as a result of the Fukushima Daiichi accident.



INES Level	People and Environment	Radiological Barriers and Control	Defence-in-Depth
Major Accident Level 7	• Major release of radioactive material with widespread health and environmental effects requiring implementation of planned and extended countermeasures.		
Serious Accident Level 6	• Significant release of radioactive material likely to require implementation of planned countermeasures.		
Accident with Wider Consequences Level 5	• Limited release of radioactive material likely to require implementation of some planned countermeasures. • Several deaths from radiation.	• Severe damage to reactor core. • Release of large quantities of radioactive material within an installation with a high probability of significant public exposure. This could arise from a major criticality accident or fire.	
Accident with Local Consequences Level 4	• Minor release of radioactive material unlikely to result in implementation of planned countermeasures other than local food controls. • At least one death from radiation.	• Fuel melt or damage to fuel resulting in more than 0.1% release of core inventory. • Release of significant quantities of radioactive material within an installation with a high probability of significant public exposure.	
Serious Incident Level 3	• Exposure in excess of ten times the statutory annual limit for workers. • Non-lethal deterministic health effect (e.g., burns) from radiation.	• Exposure rates of more than 1 Sv/h in an operating area. • Severe contamination in an area not expected by design, with a low probability of significant public exposure.	• Near accident at a nuclear power plant with no safety provisions remaining. • Lost or stolen highly radioactive sealed source. • Misdelivered highly radioactive sealed source without adequate procedures in place to handle it.
Incident Level 2	• Exposure of a member of the public in excess of 10 mSv. • Exposure of a worker in excess of the statutory annual limits.	• Radiation levels in an operating area of more than 50 mSv/h. • Significant contamination within the facility into an area not expected by design.	• Significant failures in safety provisions but with no actual consequences. • Found highly radioactive sealed orphan source, device or transport package with safety provisions intact. • Inadequate packaging of a highly radioactive sealed source.
Anomaly Level 1			• Overexposure of a member of the public in excess of statutory annual limits. • Minor problems with safety components with significant defence-in-depth remaining. • Low activity lost or stolen radioactive source, device or transport package.
NO SAFETY SIGNIFICANCE (*Below Scale/Level 0*)			

Figure 6-1: General description of INES levels

6.2 Three Mile Island

The Three Mile Island unit 2 (TMI-2) reactor of the two-unit NPP, near Middletown in Pennsylvania in the USA, experienced a severe accident on 28 March 1979, resulting in a partial reactor core melt. A combination of equipment malfunctions, design-related problems, and operator errors led to the accident. The information on the accident that follows is a summary of the extensive information made available by the US Nuclear Regulatory Commission (US NRC) [15].

The initiating event to the accident took place about 04:00 when unit 2 experienced a system or component failure that prevented the main feedwater pumps from sending water to the steam generators, thus preventing heat removal from the reactor core; refer to Figure 6-2.

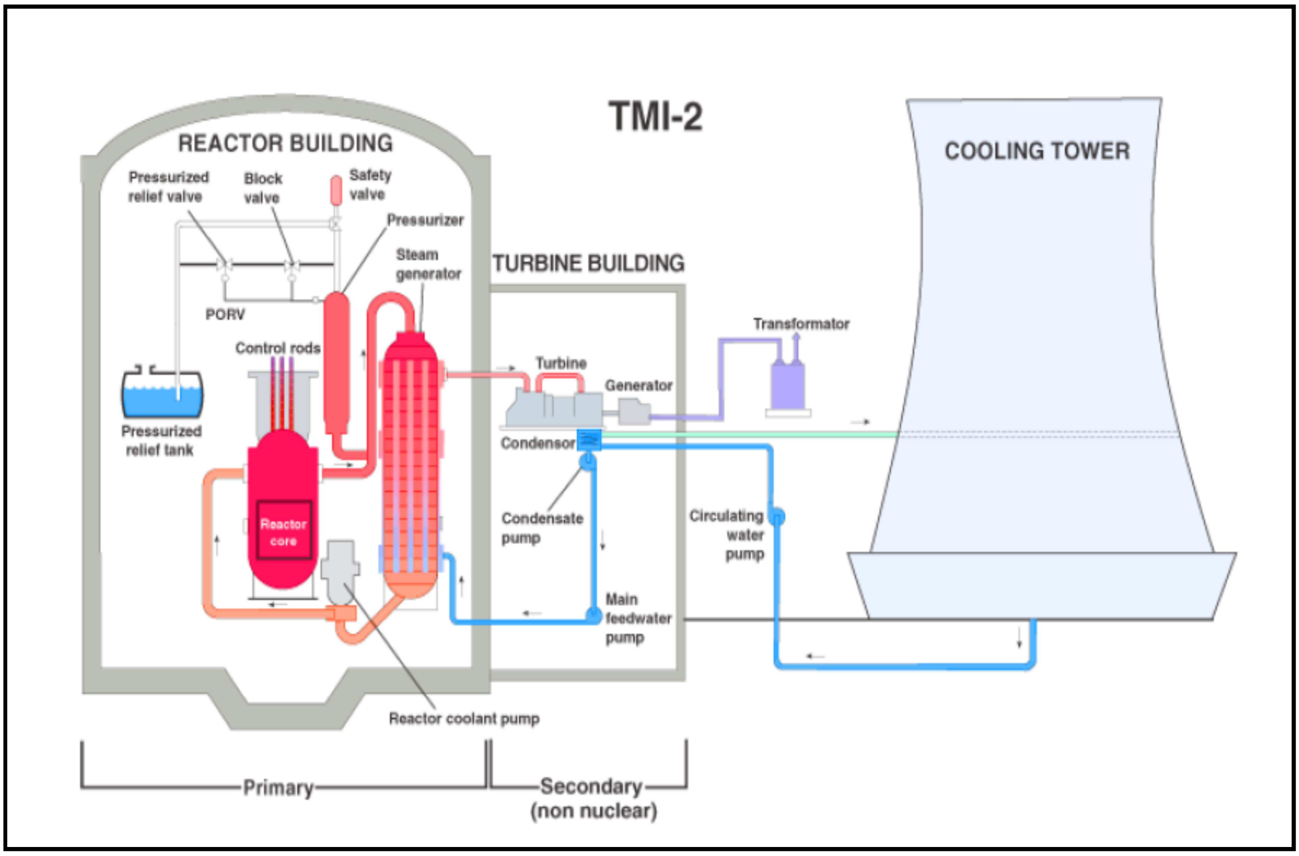


Figure 6-2: Three Mile Island Unit 2

This failure caused the plant's turbine generator and then the reactor itself to automatically shut down. Pressure began to rise in the primary system that contains the cooling water directly in contact with the reactor core. It carries the nuclear generated heat to the secondary system via the steam generators. In order to control that pressure, the pilot-operated relief valve located at the top of the pressuriser opened. The valve should have closed when the pressure fell to proper levels, but it failed in an open position. In terms of the DiD levels illustrated in Figure 5-1, one can describe it as unsuccessful DiD at Level 2. The reactor operators of TMI-2 were unaware that cooling water was pouring out of the open valve because of an instrumentation failure that did not indicate that the valve was stuck in the open position.

There were no other instruments available to reactor operators to provide additional information that compensate for the instrumentation failure. It was absolutely essential to preserve adequate water in the primary system to provide heat removal from the core. However, there was no instrument that showed how much water covered the reactor core. The operators assumed that as long as the pressuriser water level was high, the core was also properly covered with water. The reactor was in the midst of a LOCA unbeknownst to the operators.

Multiple alarms went off, and together with flashing warning lights, a very confusing situation existed in the control room. The operators then took actions that made conditions worse. The water escaping through the stuck valve reduced primary system pressure so much that the reactor coolant pumps had to be turned off to prevent dangerous vibrations. To prevent the pressuriser from filling up completely, the staff reduced the flow of cooling water being pumped into the primary system. These actions starved the reactor core of coolant, causing it to overheat.

The nuclear fuel pins that make up the nuclear fuel elements consist of a zirconium tube and enriched uranium fuel pellets. A large fraction of the fuel pins overheated and ruptured and the fuel pellets began to melt. It was later found that about half of the core melted during the early stages of the accident.

Late in the morning of 28 March, small releases of radioactive gases were measured off-site and caused concern of potential exposure to the local population. It was not yet realised that the core had melted but control measures were implemented to ensure adequate cooling of the core. Emergency response teams were mobilised and helicopters were employed to sample radioactivity in the atmosphere above the plant by midday. The White House was notified and at 11:00, all non-essential station personnel were instructed to vacate the premises.

By the evening of 28 March, the core appeared to be adequately cooled and the reactor appeared to be stable. But new concerns arose by Friday morning, 30 March. A significant release of radiation from the plant's auxiliary building when primary system pressure was relieved to avoid curtailing the flow of coolant to the core, caused a great deal of confusion and consternation. In an atmosphere of growing uncertainty about the condition of the plant, the governor of Pennsylvania consulted with the NRC about evacuating the population near the plant. It was agreed that it would be prudent for those members of society most vulnerable to radiation to evacuate the area. Pregnant women and pre-school-age children within a five-mile radius of the plant were advised to leave the area.

Within a short time, chemical reactions in the melting fuel created a large hydrogen bubble in the dome of the reactor pressure vessel, the container that holds the reactor core. There was concern that the hydrogen bubble might burn or even explode and rupture the pressure vessel. This could cause the reactor core to drop and result in a breach of containment. The hydrogen bubble was a source of intense scrutiny and great anxiety, both among government authorities and the population, throughout the day on Saturday, 31 March. The crisis ended when experts determined on Sunday, 1 April, that the bubble could not burn or explode because of the absence of oxygen in the pressure vessel. By that time, the size of the bubble had been greatly reduced, diminishing the hazard.

Although TMI-2 suffered a severe core meltdown, consequences outside the plant were minimal. Unlike the Chernobyl and Fukushima accidents, TMI-2's containment building remained intact and held almost all of the accident's radioactive material. The NRC conducted detailed studies of the accident's radiological consequences, as did the Environmental Protection Agency, the Department of Health, and other agencies. The approximately 2 million people around TMI-2 during the accident are estimated to have received an average radiation dose of only about 10 µSv above the usual background dose (global annual average is 2 400 µSv). Comprehensive investigations and assessments by several well-respected organisations such as the Columbia University and the University of Pittsburgh have concluded that in spite of serious damage to the reactor, the actual release had negligible effects on the physical health of individuals or the environment.

Major changes to reactor design and accident response were introduced as a result of the accident. Some of the major changes are the following:

- upgrading and strengthening of NPP design and equipment requirements. This includes fire protection, piping systems, auxiliary feedwater systems, containment building isolation, reliability of individual components (pressure relief valves and electrical circuit breakers), and the ability of plants to shut down automatically;

- identifying the critical role of human performance in plant safety led to a review and improvement of operator training and staffing requirements, followed by improved instrumentation and control for operating the plant;
- enhancing emergency preparedness and conducting response exercises on a regular basis;
- installing additional equipment at NPPs to mitigate accident conditions and monitor radiation levels and plant status; and
- enacting programmes by licensees for early identification of important safety-related problems, and for collecting and assessing relevant data so operating experience can be shared and quickly acted upon.

Lessons learnt from the Fukushima Daiichi accident (discussed in § 6.3) led to further improvements. The reactor containment building for example, the last barrier in the unlikely event of a severe accident, will now provide its safety function with even higher reliability than was the case during the TMI-2 accident. An example of how NPPs evolved since the TMI-2 accident is that of reactor containment designs. An example of a GEN III containment design is that of the Westinghouse AP1000 NPP and is illustrated in Figure 6-3 [16]. A passive containment cooling system (PCCS) cools the outer surface of a steel containment shell using natural circulation of air and water evaporation. The AP1000's ultimate heat sink is the atmosphere. This is in stark contrast to the relatively complex and mainly active cooling systems of GEN II PWRs.

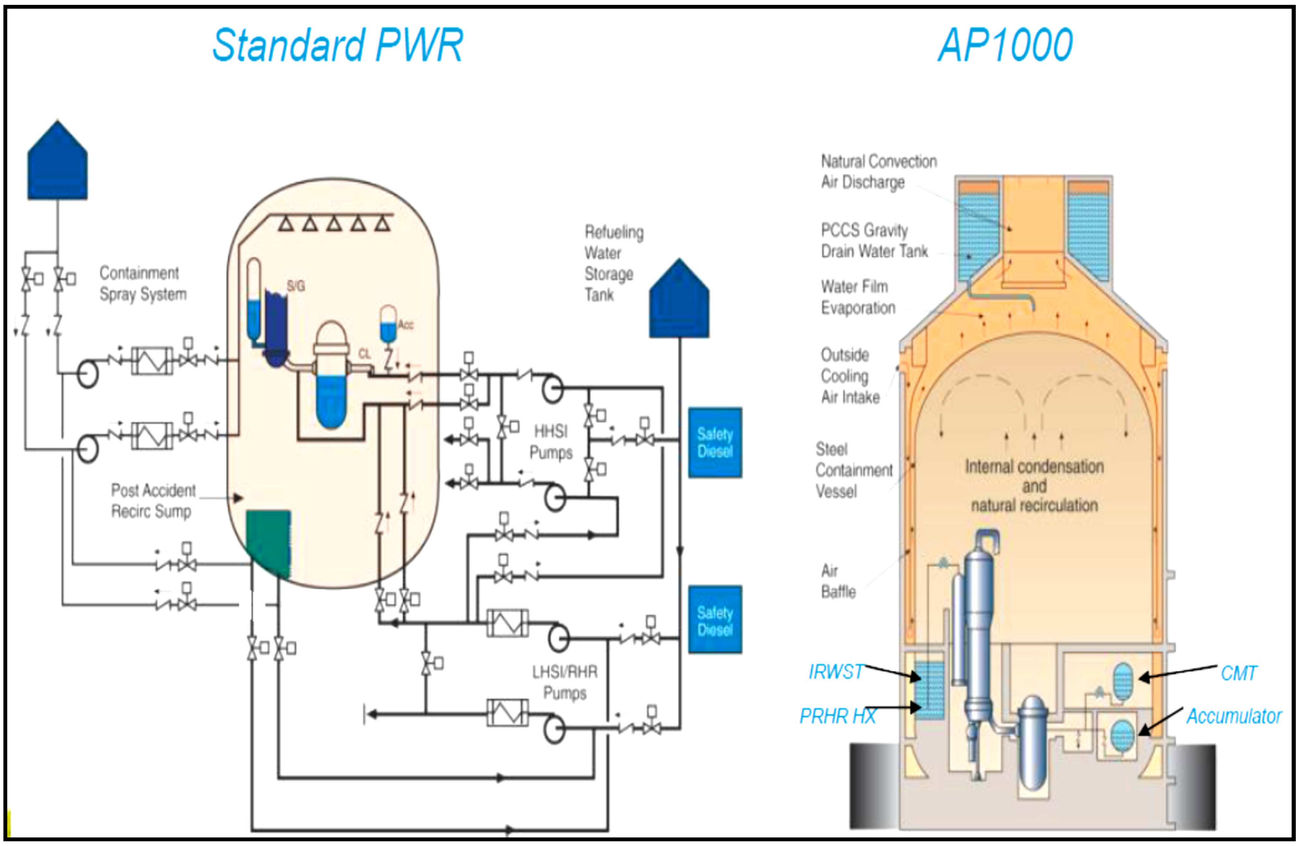

Standard PWR
AP1000
Containment Spray System
S/G
Acc
CL
Refueling Water Storage Tank
HHSI Pumps
Safety Diesel
Post Accident Recirc Sump
Safety Diesel
LHSI/RHR Pumps
Natural Convection Air Discharge
PCCS Gravity Drain Water Tank
Water Film Evaporation
Outside Cooling Air Intake
Steel Containment Vessel
Internal condensation and natural recirculation
Air Baffle
IRWST
PRHR HX
CMT
Accumulator

Figure 6-3: Advanced containment design of the AP1000 NPP and passive containment cooling system (PCCS)

6.3 Fukushima Daiichi

6.3.1 The initiating event and accident sequence

The Great East Japan Earthquake that struck on 11 March 2011 registered a massive magnitude 9. The epicentre of the earthquake in relation to the nearest Japanese NPPs is illustrated in Figure 6-4. The earthquake gave rise to a series of large tsunami waves. When these tsunami waves reached the eastern coast of Japan, extensive damage and loss of human life occurred over a wide area. It initiated the worst accident at a NPP since the Chernobyl disaster in 1986.

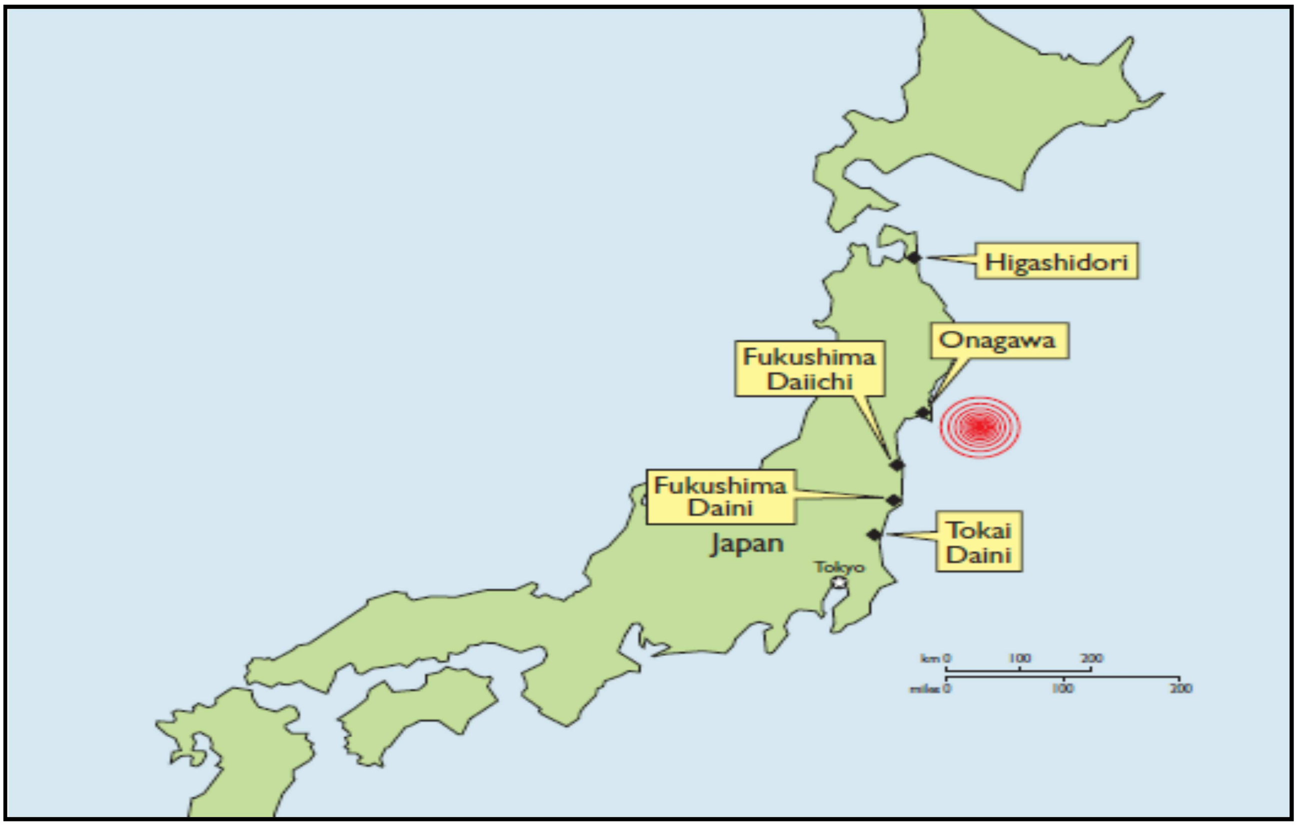


Figure 6-4: Japanese NPP locations in relation to the earthquake epicentre

The information presented here on the nuclear damage that followed consists of extracts from the recent and comprehensive report by the Director General of the IAEA [2]. The lessons learnt by the nuclear industry have been used to assess the safety of current operating NPPs and to influence the designs of new NPPs. It is recommended that readers who desire a more comprehensive technical discussion of the accident than what is presented here, access the report from the IAEA website [25].

The first tsunami waves reached the Fukushima Daiichi NPP about 40 minutes after the earthquake. The site was protected from the first wave by means of the barrier seawalls that were designed to protect against a maximum tsunami height of 5.5 m. The first waves had a 4 to 5 m run-up height. Run-up height is the height of the wave at the furthest inland point with respect to the normal sea level. Figure 6-5 illustrates the NPP layout and the relative height of the tsunami waves and NPP structures. About 10 minutes after the first wave, the second and largest wave, with a run-up height of 14 to 15 m, flowed over the seawalls and flooded the site. The flooding caused by the second tsunami wave initiated the accident sequence at Fukushima Daiichi that led to a BDBA rated at INES Level 7.

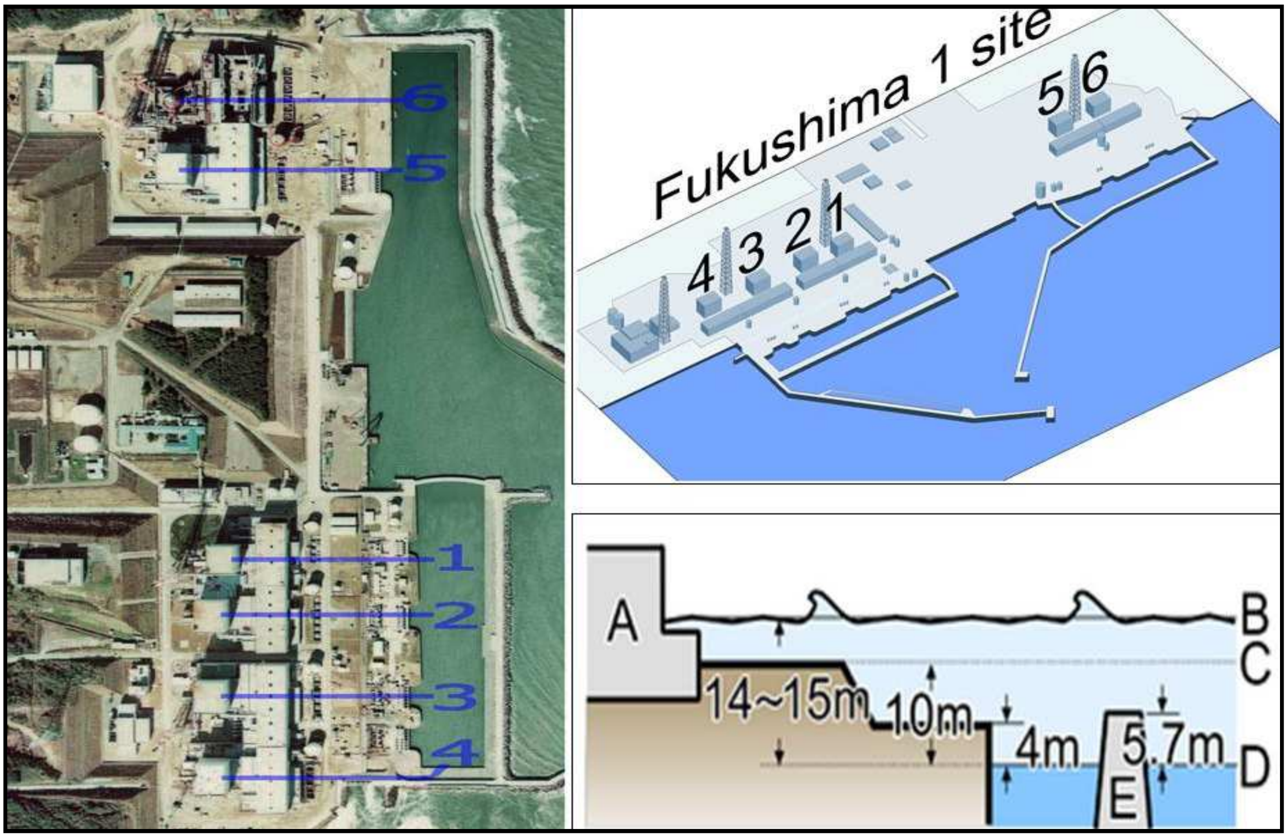


Figure 6-5: Layout of the Fukushima Daiichi NNP and height of the tsunami waves (A: the plant elevation; B: tsunami height; C: plant terrace height; D: normal sea level; E: height of seawalls)

Figure 6-6 illustrates the tsunami wave heights at different NPPs along the coast. Higher waves struck the Onagawa NPP but since its design basis allowed for higher tsunami waves, no accident resulted.

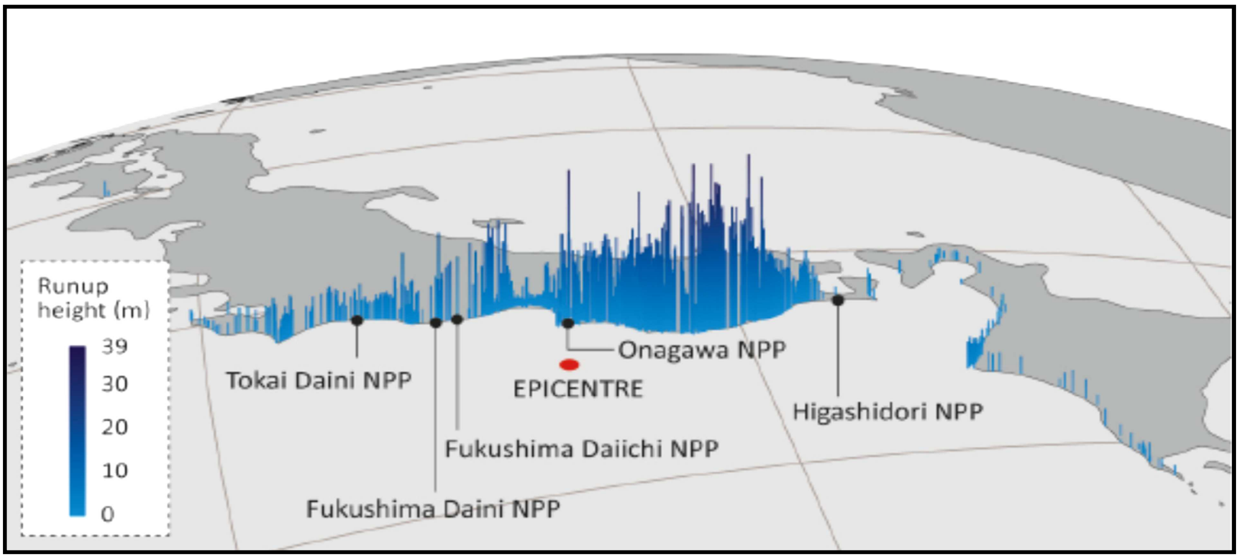


Figure 6-6: The variation of tsunami wave heights along the Japan coast

Figure 6-7 illustrates the main structures and systems of a NPP unit.

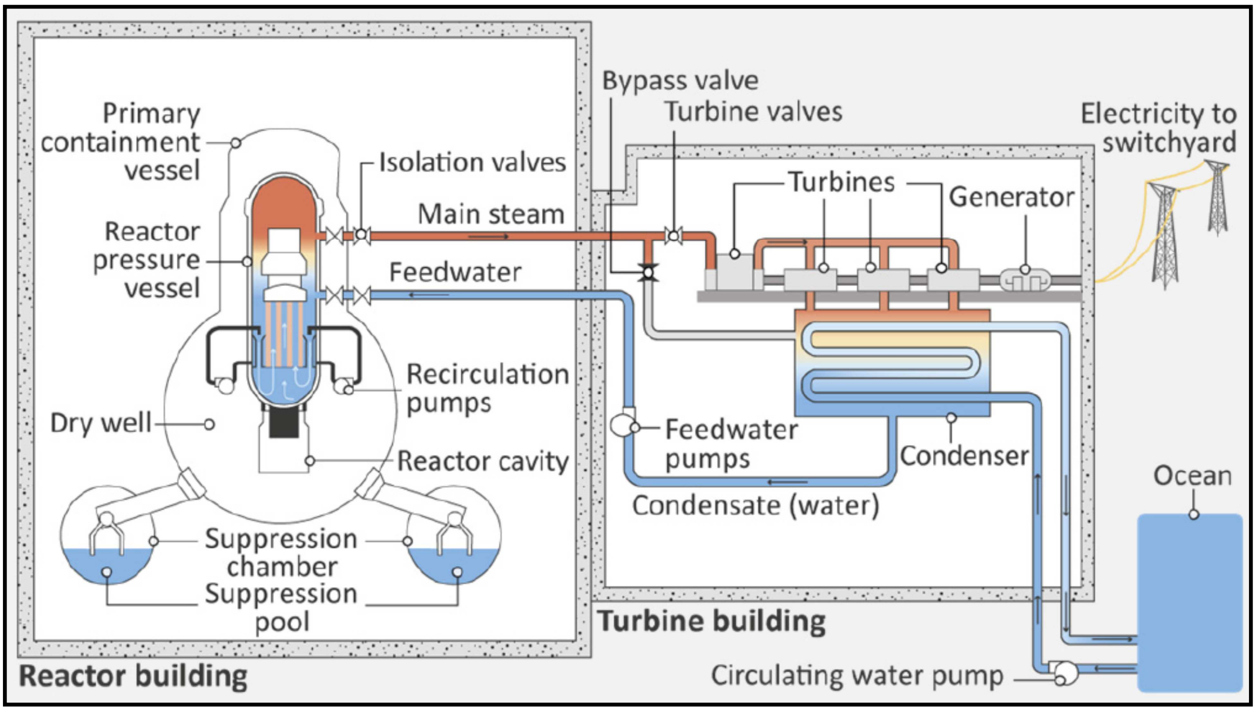


Figure 6-7 Diagram of a unit of the Fukushima Daiichi NPP

The wave flooded and damaged the unhoused seawater pumps and motors at the seawater intake locations on the shoreline. This meant that essential plant systems, including the water-cooled emergency diesel generators, could not be cooled to ensure their continuous operation. Water entered and flooded buildings, including all the reactor and turbine buildings, the common spent fuel storage building and diesel generator building. It damaged the buildings and the electrical and mechanical equipment inside at ground level and on the lower floors. The damaged equipment included the emergency diesel generators or their associated power connections, which resulted in the loss of emergency electrical power. Only one of the air-cooled emergency diesel generators, that of unit 6, was unaffected by the flooding. It remained in operation, continuing to supply emergency power to the safety systems of reactor unit 6, and allowing cooling of the reactor.

As a result of these events, units 1 to 5 lost all power, a situation referred to as a station blackout. The administration buildings and the seismically isolated building that contained the on-site emergency response centre were on a cliff at an elevation of approximately 35 m (which was the original topographical site elevation before the site area was excavated for placing the reactor units during construction).

Each reactor unit had a pair of emergency diesel generators, and unit 6 had an additional generator. Of those 13 emergency diesel generators, units 2, 4, and 6 each had one that was air cooled. Since they were air cooled, operability of these generators was not directly affected by the loss of cooling water caused by the damage to the seawater pumps.

The air-cooled emergency diesel generators of units 2, 4 (located in ground floor of the common spent fuel building), and unit 6 (located on the first floor of a separate diesel generator building at higher elevation) appeared to be unaffected by the flooding. However, the components (i.e. switchgear, power centres, panels, etc.) of the air-cooled emergency diesel generators of units 2 and 4, which were located in the basement of the common spent fuel building, suffered water damage.

NPPs are generally equipped with on-site back-up power sources (i.e. gas turbine generators or diesel engines) to withstand a station black-out for a limited period, varying between 4 and 72 hours. This grace period is based mainly on the time that it would take to restore power sources to the NPP and the capacity of the available measures. During that time, equipment such as batteries, current inverters and other secondary back-up power sources (e.g. gas turbines or diesel generators) is used.

The earthquake and heights of the tsunami waves significantly exceeded the characterisation of these external hazards that had been made when the NPP was originally designed. The seismic hazard and tsunami waves considered in the original design were evaluated mainly on the basis of historical seismic records and evidence of recent tsunamis in Japan. This original evaluation did not sufficiently consider tectonic-geological criteria, and no re-evaluation using such criteria was conducted. Prior to the earthquake, the Japan Trench was categorised as a subduction zone with a frequent occurrence of magnitude 8 class earthquakes; an earthquake of magnitude 9.0 off the coast of Fukushima Prefecture was not considered to be credible by Japanese scientists. However, similar or higher magnitudes had been registered in different areas in similar tectonic environments in the past few decades.

The design basis of the NPP included enough safety margin to provide for the seismic effects of the earthquake. There were no indications that the main safety features of the plant were affected by the vibratory ground motions generated by the earthquake. This was due to the conservative approach to earthquake design and construction of NPPs in Japan. However, the original design considerations did not provide comparable safety margins for extreme external flooding events, such as tsunami waves that were experienced.

6.3.2 The design basis and external events

The vulnerability of the Fukushima Daiichi NPP to external hazards had not been reassessed in a systematic and comprehensive manner during its lifetime. At the time of the accident, there were no regulatory requirements in Japan for such reassessments, and relevant domestic and international operating experience was not adequately considered in the existing regulations and guidelines. The regulatory guidelines in Japan on methods for dealing with the effects of events associated with earthquakes, such as tsunamis, were generic and brief, and did not provide specific criteria or detailed guidance. Before the accident, some reassessments of extreme tsunami flood levels were conducted using a consensus-based methodology developed in Japan in 2002. It indicated wave height values higher than the original design basis estimates. Based on the results, some compensatory measures were taken, but they proved to be insufficient at the time of the accident. A number of trial calculations were also performed before the accident, using wave source models or methodologies that went beyond the consensus-based methodology. Thus, a trial calculation using the source model proposed by the Japanese Headquarters for Earthquake Research Promotion in 2002, which used the latest information and took a different approach in its scenarios, envisaged a substantially larger tsunami than that provided for in the original design and in estimates made in previous reassessments. At the time of the accident, further evaluations were being conducted, but in the meantime, no additional compensatory measures were implemented. *The estimated values were similar to the actual tsunami flood levels recorded in March 2011.*

6.3.3 The current situation

Currently, it is presumed that the remains of the reactor cores (molten corium or fuel debris) are within the buildings, in a stable cooled condition by means of water circulation. A large water treatment plant was built to cope with the water contaminated by the core materials in the destroyed reactors. Also, there is considerable storage capacity built at the site to hold decontaminated water. Management of extensive water storage at various levels of radioactivity is becoming a challenge that has been given much media attention. Nitrogen is being injected into all three reactors to ensure inert atmosphere there and prevent any chance of further hydrogen explosions. Nuclear fuel in storage pools is being cooled and in a stable condition. It is believed not to have been significantly damaged. Removal of fuel from the storage pool in unit 4 began in November 2013 and was completed in December 2014.

6.3.4 Impact on the public

Significant amounts of radioactivity were released, but prompt evacuation limited the radiological exposure and dose low levels. Approximately 160 000 people were evacuated from their homes. Radiation was not expected to have any measureable effect on the health of the population and this was confirmed in 2013 by an estimation from the UN Scientific Committee on the Effects of Atomic Radiation (UNSCEAR) that no person in Fukushima prefecture would be exposed through the environment or their food to more than 10 mSv in their entire lifetime. This is one tenth of the level at which health effects are known to become more likely, and therefore no measureable increase in cancer rates is expected. The government continues to monitor the health of all Fukushima residents. Stress, anxiety, and the social problems associated with relocation have been repeatedly identified as the likely causes of ill health. Certain areas are still off limits but the Japanese government has lifted the evacuation order from other areas. Figure 6-8 illustrates the diminishing dose rates with time as radioactivity decays.

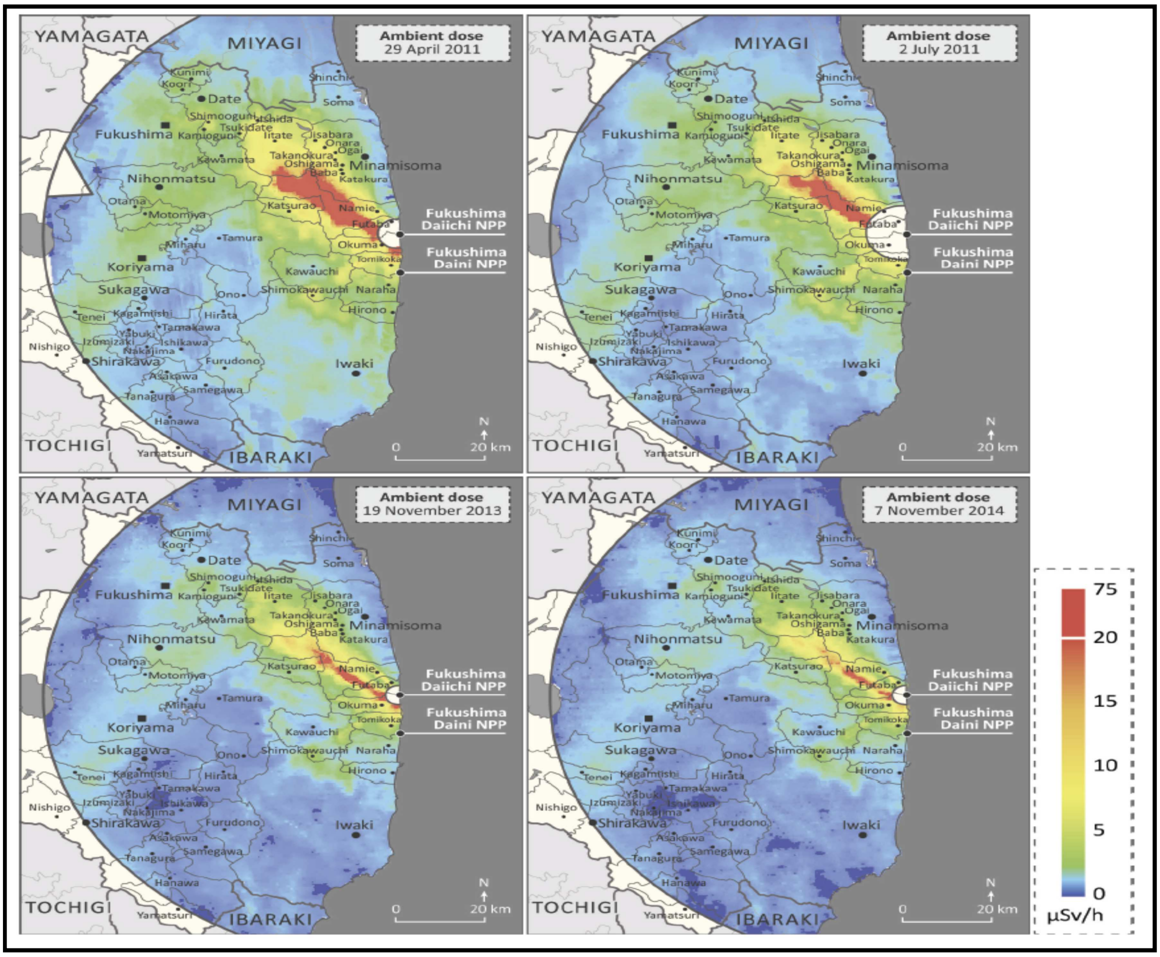


Figure 6-8: Measured aerial dose rates (µSv/h) from deposited radioactivity

6.3.5 Lessons learnt

Worldwide NPP operating experience has shown instances where natural hazards have exceeded the design basis for a NPP. In particular, the experience from some of these events demonstrated the vulnerability of safety systems to flooding. The lessons learnt are:

- The assessment of natural hazards needs to consider the potential for their occurrence in combination, either simultaneously or sequentially, and their combined effects on a NPP. The assessment of natural hazards also needs to consider their effects on multiple reactor units at a NPP.
- The safety of NPPs needs to be re-evaluated on a periodic basis to consider advances in knowledge, and necessary corrective actions or compensatory measures need to be implemented promptly.
- Operating experience programmes need to include experience from both national and international sources. Safety improvements identified through operating experience programmes need to be implemented promptly. The use of operating experience needs to be evaluated periodically and independently.

The design of the Fukushima Daiichi NPP provided equipment and systems for the first three levels of DiD, but external hazards such as tsunamis were not fully addressed. Consequently, the flooding resulting from the tsunami simultaneously challenged the first three protective levels of defence in depth, resulting in common cause failures of equipment and systems at each of the three levels. The common cause failures of multiple safety systems resulted in plant conditions that were not envisaged in the design. Consequently, the means of protection intended to provide the fourth level of defence in depth, that is, prevention of the progression of severe accidents and mitigation of their consequences, were not available to restore the reactor cooling and to maintain the integrity of the containment. The complete loss of power, the lack of information on relevant safety parameters due to the unavailability of the necessary instruments, the loss of control devices and the insufficiency of operating procedures made it impossible to arrest the progression of the accident and to limit its consequences. The lessons learnt are:

- The DiD principle remains valid, but implementation of DiD needs to be strengthened at all levels by adequate independence, redundancy, diversity, and protection against internal and external hazards. There is a need to focus not only on accident prevention, but also on improving mitigation measures.
- Instrumentation and control systems that are necessary during beyond-design-basis accidents need to remain operable in order to monitor essential NPP safety parameters and to facilitate NPP operations.

A review of the accident against the fundamental safety functions reveals the following:

- Following the earthquake, the first fundamental safety function, control of reactivity, was fulfilled in all six units at the Fukushima Daiichi NPP.
- The second fundamental safety function, removing heat from the reactor core and the storage pool for irradiated and spent fuel, could not be maintained because the operators had very little control over the reactors of units 1, 2, and 3 and the fuel pools as a result of the loss of most of the electrical systems. The loss of the second fundamental safety function was, in part, due to the failure to implement alternative water injection because of delays in depressurising the reactor pressure vessels. Loss of cooling led to overheating and melting of the fuel in the reactors.

- The confinement function was lost as a result of the loss electrical power, which rendered the cooling systems unavailable and made it difficult for the operators to use the containment venting system. Confinement is closely related in meaning to containment, but confinement is typically used to refer to the safety function of preventing the ‘escape’ of radioactive material, whereas containment refers to the means for achieving that function [4]. Venting of the containment was necessary to relieve pressure and prevent its failure. The operators were able to vent units 1 and 3 to reduce the pressure in the primary containment vessels. However, this resulted in radioactive releases to the environment. Even though the containment vents for units 1 and 3 were opened, the primary containment vessels for units 1 and 3 eventually failed. Lessons learnt in respect of containment are:
    - Robust and reliable cooling systems that can function for both design basis and beyond-design-basis conditions need to be provided for the removal of residual heat.
    - There is a need to ensure a reliable confinement function for beyond-design-basis accidents to prevent significant release of radioactive material to the environment.

Safety analyses conducted during the licensing process of the Fukushima Daiichi NPP and during its operation, did not fully address the possibility of a complex sequence of events that could lead to severe reactor core damage. In particular, the safety analyses failed to identify the vulnerability of the NPP to flooding and weaknesses in operating procedures and accident management guidelines. The probabilistic safety assessments did not address the possibility of internal flooding, and the assumptions regarding human performance for accident management were optimistic. Furthermore, the regulatory body had imposed only limited requirements for operators to consider the possibility of severe accidents. Lessons learnt are:

- Comprehensive probabilistic and deterministic safety analyses need to be performed to confirm the capability of a NPP to withstand applicable beyond-design-basis accidents and to provide a high degree of confidence in the robustness of the NPP design.
- Accident management provisions need to be comprehensive, well designed, and up to date. They need to be derived on the basis of a comprehensive set of initiating events and NPP conditions and also need to provide for accidents that affect several units at a multi-unit NPP.
- Training, exercises, and drills need to include postulated severe accident conditions to ensure that operators are as well prepared as possible. They need to include the simulated use of actual equipment that would be deployed in the management of a severe accident.

Before the accident, there was a basic assumption in Japan that the design of NPPs and the safety measures that had been put in place were sufficiently robust to withstand external events of low probability and high consequences. Because of the basic assumption that NPPs in Japan were safe, there was a tendency for organisations and their staff not to challenge the level of safety. The reinforced basic assumption among the stakeholders about the robustness of the technical design of NPPs resulted in a situation where safety improvements were not introduced promptly. The accident at the Fukushima Daiichi NPP showed that, in order to better identify NPP vulnerabilities, it is necessary to take an integrated approach that account for complex interactions between people, organisations, and technology. The lessons learnt are:

- In order to promote and strengthen safety culture, individuals and organisations need to continuously challenge or re-examine the prevailing assumptions about nuclear safety and the implications of decisions and actions that could affect nuclear safety.

- A systemic approach to safety needs to consider the interactions between human, organisational, and technical factors. This approach needs to be taken through the entire life cycle of nuclear installations' radioactive releases.

Finally, it is clear that in order to ensure effective regulatory oversight of the safety of nuclear installations, it is essential that the regulatory body be independent and possesses legal authority, technical competence, and a strong safety culture.

6.4 Chernobyl

A brief overview is presented here of the Chernobyl accident, an extract from [18]. It is important to note that the design of the Chernobyl nuclear reactors bears no resemblance to the PWR NPPs of the time of which the Three Mile Island NPP is an example. The Chernobyl accident does, however, provide valuable lessons in respect of the important concepts of DiD, nuclear safety culture, and how human errors contribute to accidents.

On 26 April 1986, a sudden surge of power during a reactor systems test destroyed unit 4 of the Chernobyl NPP in Ukraine, part of the Soviet Union at the time. The accident and the fire that followed released massive amounts of radioactive material into the environment. The NPP was not equipped with a reactor containment of similar quality to the design used in the West, such as at Three Mile Island.

The RBMK-1000 NPP design illustrated in Figure 6-9 is a Soviet-designed and built graphite moderated pressure tube type reactor, using slightly enriched uranium dioxide fuel. It is a boiling light water reactor, with two loops feeding steam directly to the turbines, without an intervening heat exchanger.

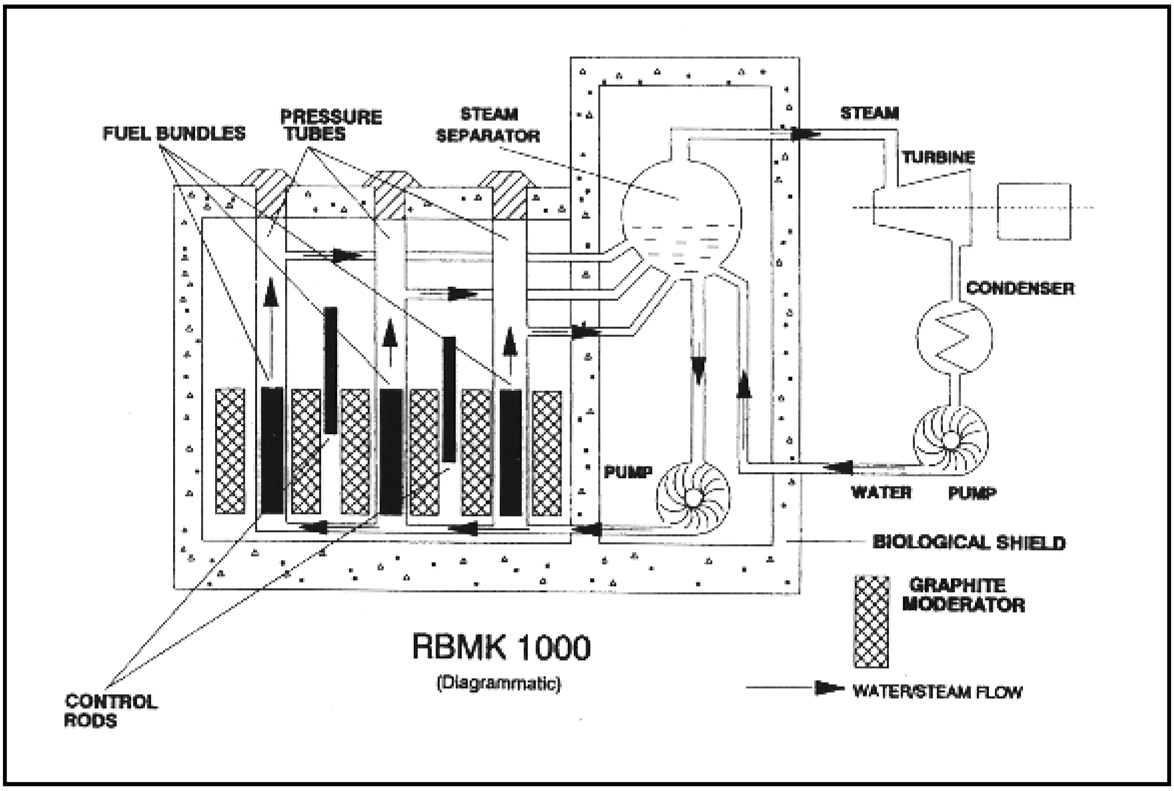


Figure 6-9: The RBMK 1000 reactor

One of the most important characteristics of the RBMK reactor is that it can possess a ‘positive void coefficient’, where an increase in steam bubbles (‘voids’) is accompanied by an increase in reactor core reactivity. As steam production in the fuel channels increases, the neutrons that would have been absorbed by the denser water, now produce increased fission in the fuel. (In Western GEN II and all GEN III PWR reactors, the void coefficient is negative.)

On 25 April, prior to a routine shutdown, the reactor crew at Chernobyl 4 began preparing for a test to determine how long turbines would spin and supply power to the main circulating pumps following a loss of main electrical power supply. A series of operator actions, including the disabling of automatic shutdown mechanisms, preceded the attempted test early on 26 April. By the time that the operator moved to shut down the reactor, the reactor was in an extremely unstable condition. A peculiarity of the design of the control rods caused a dramatic power surge as they were inserted into the reactor to shut it down. The interaction of very hot fuel with the cooling water led to fuel fragmentation along with rapid steam production and an increase in pressure. The design characteristics of the reactor were such that substantial damage to even three or four fuel assemblies can, and did, result in the destruction of the reactor.

Emergency crews responding to the accident used helicopters to pour sand and boron on the reactor debris. The sand was to stop the fire and additional releases of radioactive material; the boron was to prevent additional nuclear reactions. A few weeks after the accident, the crews completely covered the damaged unit in a temporary concrete structure, called the “sarcophagus,” to limit further release of radioactive material. The Soviet government also cut down and buried about a square mile of pine forest near the NPP to reduce radioactive contamination at and near the site.

After the accident, officials closed off the area within 30 kilometres (18 miles) of the NPP, except for persons with official business at the NPP and those people evaluating and dealing with the consequences of the accident and operating the undamaged reactors. About 115 000 people were evacuated from the most heavily contaminated areas in 1986 and another 220 000 people in subsequent years.

The Chernobyl accident’s severe radiation effects killed 28 of the site’s 600 workers in the first four months after the event. Another 106 workers received high enough doses to cause acute radiation sickness. Two workers died within hours of the reactor explosion from non-radiological causes. Another 200 000 clean-up workers in 1986 and 1987 received doses of between 10 mSv and 1 Sv. Chernobyl clean-up activities eventually required about 600 000 workers, although only a small fraction of these workers were exposed to elevated levels of radiation. Government agencies continue to monitor clean-up activities and the health of recovery workers.

Experts conclude some cancer deaths may eventually be attributed to Chernobyl over the lifetime of the emergency workers, evacuees, and residents living in the most contaminated areas. These health effects are far lower than initial speculations of tens of thousands of radiation-related deaths.

Chernobyl’s three other reactors were subsequently restarted but all eventually shut down for good, with the last reactor closing in 1999.

Many other international programmes were initiated following Chernobyl. The IAEA safety review projects for each particular type of Soviet reactor brought together operators and engineers from the West to focus on safety improvements. The Convention on Nuclear Safety adopted in Vienna in June 1994 is another outcome.

7 THE IAEA AND ITS ROLE IN THE EVENT OF AN ACCIDENT

The IAEA was established by the United Nations in 1957. One of its functions was to act as an auditor of world nuclear safety, and this role was significantly increased following the Chernobyl accident. The IAEA produces documents on a wide spectrum of nuclear and radiation safety issues. These documents are grouped according to the following hierarchy [3]:

- Safety Fundamentals: As the primary publication in the Safety Standards Series, the IAEA publication Fundamental Safety Principles (SF-1) establishes the fundamental safety objective and principles of protection and safety.
- Safety Requirements: An integrated and consistent set of stable Safety Requirements publications establish the requirements that must be met to ensure the protection of people and the environment, both now and in the future. The requirements are governed by the objectives and principles of the Safety Fundamentals. If they are not met, measures must be taken to reach or restore the required level of safety. Their format and style facilitate their use by member states for the establishment, in a harmonised manner, of their national regulatory framework.
- Safety Guides: IAEA Safety Guides provide recommendations and guidance on how to comply with the requirements. They indicate an international consensus that it is necessary to take the measures recommended (or equivalent alternative measures). The Safety Guides present international good practices, and increasingly they reflect best practices to help users striving to achieve high levels of safety.

The principal users of these documents are the regulatory authorities of IAEA member states. South Africa is a member state.

The international emergency preparedness and response framework is based on conventions that place specific obligations on the parties (members of IAEA) and the IAEA, with the aim of minimising consequences for health, property, and the environment. The following two conventions have specific relevance to BDBA:

- The Convention on Early Notification of a Nuclear Accident [19]: This Convention aims to strengthen international cooperation in order to provide relevant information about nuclear accidents as early as necessary in order that trans-boundary radiological consequences can be minimised. States parties commit that, in the event of a nuclear accident that may have trans-boundary radiological consequences, they will notify the IAEA and countries that may be affected, and provide relevant information on the development of the accident. The IAEA in turn forthwith informs states parties, member states, other states that may be physically affected, and relevant international organisations of a notification received and promptly provides other information on request. It therefore requires that, in the event of an accident, South Africa shall (i) notify, directly or through the IAEA, those states that are or may be physically affected and the IAEA of the nuclear accident, its nature, the time of its occurrence and its exact location where appropriate; and (ii) promptly provide the states referred to in (i) above, directly or through the IAEA, and the IAEA, with such available information relevant to minimising the radiological consequences in those states.
- The Convention on Assistance in the Case of a Nuclear or Radiological Accident [20]: This Convention sets out an international framework for co-operation among states parties and with the IAEA to facilitate prompt assistance and support in the event of nuclear accidents or radiological emergencies. The IAEA serves as the focal point for such cooperation by

facilitating the provision of assistance through channelling information, supporting efforts, and providing its available services.

The IAEA discharges its function during an accident through its Incident and Emergency System (IES). This system includes a 24-hour contact point and an operational focal point, the Incident and Emergency Centre (IEC). During the Fukushima Daiichi accident, the IAEA activated the IES following a notification from the IAEA's International Seismic Safety Centre soon after the earthquake struck on 11 March 2011. This notification indicated the occurrence of an earthquake, the potential for damage at four NPPs on the north-eastern coast of Japan, and the risk of a tsunami. The IAEA immediately established initial communication with the official contact point designated by Japan under the Early Notification Convention and the Assistance Convention. The IAEA established teams to evaluate key nuclear and radiological safety issues that a severe accident could take place. The IAEA laboratories reviewed environmental data provided by the Japanese authorities on monitoring of the marine environment and received terrestrial environment samples for independent analysis [21].

Internationally, NNP safety is supported by the IAEA Convention on Nuclear Safety (CNS) [22]. It was drawn up during a series of expert level meetings from 1992 to 1994 and was the result of considerable work by governments, national nuclear safety authorities, and the IAEA secretariat. Its aim is to legally commit participating states operating land-based NPPs to maintain a high level of safety by setting international benchmarks to which states would subscribe. The obligations of the parties cover for instance, siting, design, construction, operation, the availability of adequate financial and human resources, the assessment and verification of safety, quality assurance, and emergency preparedness.

The Convention is an incentive instrument and based on their common interest to achieve higher levels of safety. These levels are defined by international benchmarks developed and promoted through regular meetings of the parties. The Convention obliges parties to report on the implementation of their obligations for international peer review. This mechanism is the main element of the Convention. Under the Operational Safety Review Team (OSART) programme dating from 1982, international teams of experts conduct in-depth reviews of operational safety performance at a NPP. They review emergency planning, safety culture, radiation protection, and other areas. OSART missions are on request from the government, and involve staff from regulators.

The Convention entered into force in October 1996. As of September 2009, there were 79 signatories to the Convention, 66 of which are contracting parties, including all countries with operating NPPs.

The IAEA General Conference in September 2011 unanimously endorsed the Action Plan on Nuclear Safety that government ministers requested in June. The plan arose from intensive consultations with member states but not with industry, and was described as both a rallying point and a blueprint for strengthening nuclear safety worldwide. It contains suggestions to make nuclear safety more robust and effective than before, without removing the responsibility from national bodies and governments. It aims to ensure "adequate responses based on scientific knowledge and full transparency". Apart from strengthened and more frequent IAEA peer reviews (including those of regulatory systems), most of the 12 recommended actions are to be undertaken by individual countries and are likely to be well in hand already.

Following this, an extraordinary general meeting of 64 of the CNS parties in September 2012 gave a strong push to international collaboration in improving safety. National reports at future threeyearly CNS review meetings will cover a list of specific design, operational, and organisational issues stemming from Fukushima lessons. They include further design features to avoid long-term off-site contamination and enhancement of emergency preparedness and response measures, including better definition of national responsibilities and improved international cooperation. Parties should also report on measures to “ensure the effective independence of the regulatory body from undue influence”.

In February 2015, diplomats from 72 countries unanimously adopted the Vienna Declaration of Nuclear Safety, setting out “principles to guide them, as appropriate, in the implementation of the objective of the CNS to prevent accidents with radiological consequences and mitigate such consequences should they occur” but rejected Swiss amendments to the CNS as impractical. However, in line with Swiss and EU intentions, “comprehensive and systematic safety assessments are to be carried out periodically and regularly for existing installations throughout their lifetime in order to identify safety improvements. Reasonably practicable or achievable safety improvements are to be implemented in a timely manner”.

The IAEA perform NPP design safety reviews. An IAEA Design Safety Review (DSR) is performed at the request of a member state organisation to evaluate the completeness and comprehensiveness of a reactor’s safety documentation by an international team of senior experts. It is based on IAEA published safety requirements. If the DSR is for a vendor’s design at the pre-licensing stage, it is done using the Generic Reactor Safety Review (GRSR) module. IAEA Safety Standards applied in the DSR and GRSR at the fundamental and requirements level, are generic and apply to all nuclear installations. Therefore, it is neither intended nor possible to cover or substitute licensing activity, or to constitute any kind of design certification. DSRs have been undertaken in Pakistan, Ukraine, Bulgaria, and Armenia. GRSRs have been done on AP1000 (USA and UK), Atmea1, APR1400, ACPR-1000+, ACP1000, and AES-2006, and VVER-TOI.

An IAEA team of international experts has carried out a review of South Africa’s nuclear infrastructure – the first Integrated Nuclear Infrastructure Review (INIR) mission to a country that is already generating nuclear power, and the first in Africa. The mission was conducted from 30 January to 8 February 2013 [23].

8 THE SOUTH AFRICAN REGULATORY FRAMEWORK IN RESPECT OF NPP ACCIDENT RISK

The siting, construction, operation, decontamination, or decommissioning of any nuclear installation, including a NPP, as defined in the National Nuclear Regulator Act 1999, Act No. 47 of 1999 [24] must be authorised by way of a nuclear installation licence by the NNR. The principal requirements that must be met to ensure safety in all nuclear installations are defined in the Regulations on Safety Standards and Regulatory Practices published as Regulation No. R388 dated 28 April 2006 (RSRP) [25].

The NNR’s policy for regulating radiation safety is in line with international consensus and in accordance with standards and guidance provided by the IAEA. These fundamental principles lead to a system of radiation dose limitation for persons occupationally exposed to radiation and for members of the public. The NNR requires that the risks to both the workforce involved in licensed activities and the public should not exceed prescribed limits for both normal operation and for potential accidents, and that both individual and population risks be maintained as low as reasonably achievable, social and environmental factors being taken into consideration.

The NNR defines a nuclear accident as follows [25]:

> *"Any occurrence or succession of occurrences having the same origin and resulting in an unintended/unauthorised exposure to radiation or release of radioactive material, and which is capable of giving rise to an effective dose in excess of 1 mSv to the public off-site in a year, or in excess of 50 mSv to a worker on site received essentially at the time of the event, is regarded as a nuclear accident as defined in section 1(xiii) of the Act".*

The NNR requirements for risk assessment and principal safety criteria are defined in a regulatory requirements document RD-0024 [26]. The principal safety criteria refer to limits on the annual radiological risk to members of the public due to exposure as a result of accidents. The NNR requires assessment of all potential initiating events that could lead to exposure, including those that are demonstrated to be extremely unlikely, including events that are estimated to occur with an annual frequency of less than 1E-06 per year. This would then include design extension conditions and more infrequent events that could result in a BDBA. In this frequency range, events must be considered as part of the design where there are significant uncertainties on the related probability values.

In respect of risk limitation to members of the public, the following criteria must be applied in consideration of both design and all phases of operation of the site*:

- 5E-06 per year of peak individual risk for a member of the public due to all nuclear installations in South Africa;
- 1E-08 average per year per NPP site for the average member of the public;
- provisions to be provided against beyond category B events so that no cliff edge effects are to be expected, i.e. a small change in NPP conditions should result in an abrupt change for the worse; and
- risks must be optimised and be as low as reasonably achievable, the ALARA principle in radiation protection.
- The NNR has also generated regulations on licensing of sites for new nuclear installations [27][28]. It includes the following requirements pertinent to NNP accidents:
  - *"4(2) The proposed nuclear installation design(s), and the characteristics specific to the site: New nuclear installation(s) must reflect through their design, construction, and operation an acceptably low probability of postulated events that could result in release of quantities of radioactive material.*
  - *4(3) The site location and the engineered safety features of all nuclear installations, included as safety measures against the hazardous consequences of postulated events, must ensure an acceptably low risk of public exposure.*
  - *4(4) The site must be such that radiological doses and risks from normal operation and postulated events associated with all nuclear installations in the vicinity will be acceptably low.*
  - *4(5) Natural phenomena and potential man-made hazards must be appropriately accounted for in the design of the new nuclear installation(s), and that adequate emergency plans and nuclear security measures can be developed.*
  - *5(3) The characteristics of the site relevant to the design assessment, risk and dose calculations, including inter alia:*

    (a) external events;
    (b) meteorological data;
    (c) land use;

(d) population demographics;
(e) regional development;

- *5(4) A source term analysis that is representative of the overall potential hazards posed to the public and the environment owing to the new nuclear installation(s). A representative scope of internal and external events enveloping the new nuclear installation(s) must be taken into consideration."*

9 AN EXAMPLE OF INITIATIVES IN OTHER COUNTRIES TO IMPROVE NPP SAFETY – WESTERN EUROPE NUCLEAR REGULATOR ASSOCIATION AND EUROPEAN UTILITY REQUIREMENTS

Heads of regulators for nuclear safety within the European Union and Switzerland commenced co-operation in 1999 in the framework of Western European Nuclear Regulators Association (WENRA). It started with ten countries and has expanded since. Members with significant nuclear generating capacity include Germany, France, United Kingdom, and Sweden [28]. One of the objectives of WENRA is to develop a harmonised approach to nuclear safety and radiation protection issues. Objectives for new NPPs that include GEN III designs were defined and include the following [29]:

- increase the level of independence of the DiD levels at NPPs;
- extend NPP design beyond the traditional design basis in the area of reactor core melt prevention and mitigation, with emphasis on more robust containment buildings (design extension conditions); and
- consider systematically severe accidents from the beginning of the design process so that the following can be achieved primarily by design measures:
  - reduce the necessity for off-site measures such as evacuation, and the potential for long-term and large-scale land contamination; and
  - increase the protection against external hazards.

Severe accidents must be accounted for as part of the design and accidents with core melt that could lead to early or large releases of radioactivity to the environment have to be "practically eliminated". This implies that the possibility of certain NNP accident conditions occurring is considered to have been practically eliminated if it is physically impossible for the conditions to occur or if the conditions can be considered with a high degree of confidence to be extremely unlikely to arise.

The term BDBA is not interpreted the same for existing reactors and for new reactors. Several previously defined BDBA accident scenarios for existing reactors are now included in the design basis for new reactors, e.g. reactor core melt accidents are considered as "design basis extension" situations for new NPPs. The safety case for a new reactors therefore has to demonstrate reinforcement of the DiD principle. It also requires, amongst other safety measures, that the NPP confinement features be designed to cope with core melt accidents, also for a long period. This is typically is not the case for most of the currently operating NPPs.

For accidents with core melt that have not been practically eliminated, design provisions have to be taken so that only limited protective measures in area and time are needed for the public (no permanent relocation, no need for emergency evacuation outside the immediate vicinity of the NPP, limited sheltering, no long-term restrictions in food consumption). Sufficient time has to be available to implement these measures.

Independent of WENRA, the major European electricity producers formed an organisation to develop the European Utility Requirement (EUR) document [30]. This document proposes a common set of utility requirements for the GEN III / III+ NPPs using light water reactors (LWR). The EUR document sets common safety targets, which are consistent with the best European and international objectives. It states that these targets are values that are more restrictive than regulatory limits but are judged to be at a level that can be reasonably achieved by modern well-designed NPPs.

10 CONCLUDING STATEMENTS

GEN III NPP strengthened DiD provisions, based on technological advances and lessons learnt from the three major BDBAs in the nuclear power industry. Designs include safety features based on explicit consideration of severe accidents that include a reactor core melt. In earlier generation NPPs, these accidents are considered part of the BDBA classification and require extensive DiD level 5 safety provisions, i.e. limiting the dose through emergency plans when significant quantities of radioactivity are released to the environment. The design objective of GEN III reactors is to reduce potential radioactive releases to the environment, also in the long term, by following the qualitative criteria below:

- accidents with core melt which would lead to early or large releases have to be practically eliminated;
- for accidents with core melt that have not been practically eliminated, design provisions have to be taken so that only limited protective measures in area and time are needed for public protection; no permanent relocation, no need for emergency evacuation outside the immediate vicinity of the NPP, limited sheltering and no long-term restrictions in food consumption. Sufficient time is available to implement these measures.

These objectives in respect of severe accidents are achieved by having increased reliance on passive safety systems, when compared with designs of mostly active systems supported by human actions in GEN II NPPs. The use of passive systems avoids the consequences of events that disrupt external sources of electricity, cooling water, and other essential systems to return a NNP to a safe condition. The reactor core of some GEN III designs, for example, can be cooled by passive means through natural convection, heat radiation, and conduction. No external electricity is required, something that was essential to have prevented of the Fukushima Daiichi accident.

Design extension conditions are assessed to define the design basis for safety related SSCs. GEN III NPPs have distinctive characteristics that can be summarised as follows [32]:

- simpler design designs making the reactors easier to operate and more tolerable of abnormal operating conditions;
- passive safety features in the design of the SCCs that avoid use of active control and relying on natural phenomena such as natural circulation of cooling media, e.g. cooling of the containment building to avoid overpressure;
- reduced SCCs failure probabilities and a lower reactor core damage frequency compared to earlier generation reactors (an order of magnitude reduction);
- new design features that provide mitigation to significantly reduce the release of radioactivity to the environment should the reactor core melt; and
- improved resistance to external hazards such as aircraft crash and extreme natural events.

A comparison of the GEN III PWR of estimated annual frequencies of a large radioactivity release during a BDBA that could result in radiological exposure of the public and pose a high fatality risk, indicates that these NPP designs should be able to meet the regulatory limits of the NNR. The accident frequencies in Table E-1 (pg 6) can be compared to the NNR peak individual fatality risk of 5E-06 per year.

A NPP to be built in South Africa will have to submit a safety analysis report that provide the evidence for this provisional conclusion, based on an analysis of external and internal events for the specific design and specific site where it will be built.

11 REFERENCES

[1] Environmental Impact Assessment for the Proposed Nuclear Power Station (‘Nuclear-1’) and Associated Infrastructure, Assessment of the Potential Radiological Impact on the Public and the Environment. 2015. Vienna.

[2] International Atomic Energy Agency (2015), The Fukushima Daiichi Accident - Report by the Director General and Technical Volumes. Vienna.

[3] International Atomic Energy Agency (2006), Safety Standards Series No. SF-1, Fundamental Safety Principles: Safety Fundamentals. Vienna.

[4] International Atomic Energy Agency (2007), IAEA Safety Glossary - Terminology used in the Nuclear Safety and Radiation Protection 2007 Edition. Vienna.

[5] International Atomic Energy Agency (2012), Safety Standards Series No. SSR-2/1 – Safety of Nuclear Power Plants Design, Specific Safety Requirements. Vienna.

[6] International Atomic Energy Agency (2000), Safety Standards Series No. NSR. Vienna.

[7] Marques J.G., Evolution of Nuclear Fission Reactors: Third Generation and Beyond, Energy Conversion and Management 51 (2010) 1774-1780]

[8] International Atomic Energy Agency (2005), IAEA TECDOC-1436: Risk Informed Regulation of Nuclear Facilities: Overview of the current status, Vienna.

[9] http://static.onemansblog.com/wp-content/uploads/2011/03/Picture-of-Tsunami-Approaching-Japan-2011.jpg; https://en.wikipedia.org/wiki/2015_Tianjin_explosions#/media/File:2015_Tianjin_explosion_-_Crop.jpg

[10] National Nuclear Regulator (2012), PP-0014: Considerations of External Events for New Nuclear Installations, Rev 0. Centurion.

[11] International Atomic Energy Agency (2006), Advanced Nuclear Plant Design Options to Cope with External Events. TECDOC 1487. Vienna.

[12] EPR Aircraft Crash Design

[13] International Atomic Energy Agency (1999), Basic Safety Principles for Nuclear Power Plants : 75-INSAG-3 Rev. 1 / INSAG 12. A report by the International Nuclear Safety Advisory Group. Vienna.

[14] http://www-ns.iaea.org/tech-areas/emergency/ines.asp

[15] http://www.nrc.gov/reading-rm/doc-collections/fact-sheets/3mile-isle.html

[16] https://www.iaea.org/NuclearPower/Downloads/Technology/meetings/2011-Jul-4-8-ANRT-WS/2_USA_UK_AP1000_Westinghouse

[17] https://www.iaea.org/newscenter/news/iaea-releases-director-general%E2%80%99s-report-fukushima-daiichi-accident

[18] http://www.nrc.gov/reading-rm/doc-collections/fact-sheets/chernobyl-bg.html

[19] International Atomic Energy Agency (1986), Convention on Early Notification in Case of a Nuclear Accident. INFCIRC/335.Vienna

[20] International Atomic Energy Agency (1986), Convention on Assistance in the Case of Nuclear Accident or Radiological Emergency. INFCIRC/336.Vienna

[21] IAEA Report on Preparedness and Response for a Nuclear or Radiological Emergency in the Light of the Accident at the Fukushima Daiichi NPP, International Atomic Energy Agency Vienna, 2013

[22] International Atomic Energy Agency (1994), Convention on Nuclear Safety.

[23] International Atomic Energy Agency IAEA Generic Reactor Safety Review (GRSR) - Progress of IAEA SSs on NPP Design Javier Yllera Safety Assessment Section Department of Nuclear

[24] Republic of South Africa (1999), National Nuclear Regulator Act, 1999. Act No. 47 of 1999. Pretoria

[25] Department of Minerals and Energy (2006), R.388: Regulations in Terms of Section 36, Read with Section 47 of the National Nuclear Regulator Act, 1999 (Act No. 47 of 1999), on Safety Standards and Regulatory Practices. Government Gazette 28755. Pretoria

[26] National Nuclear Regulator (2008), RD-0024: Requirements on Risk Assessment and Compliance with Principal Safety Criteria for Nuclear Installations. Rev 0. Centurion

[27] Department of Energy (2011), R.927: The Regulations on Licensing of Sites for New Nuclear Installations, 2010. Government Gazette 34735. Pretoria

[28] http://www.wenra.org/about-us/

[29] Western European Nuclear Regulator's Association Safety Objectives for New Power Reactors Study by WENRA Reactor Harmonization Working Group December 2009 Reactor Harmonization Working Group

[30] European Utility Requirements Organisation (2001), European Utility Requirements for LWR Nuclear Power Plants. Volume 2 Rev C, and Volume 4, Rev B (2000). Available from: http://www.europeanutilityrequirements.org/eur.htm [Accessed: 12/03/12

[31] http://www.nrc.gov/about-nrc.html

[32] Marques J.G., Environmental Characteristics of the Current Generation III Nuclear Power Plants, WIREs Energy Environ 2013, 0: 1–18 doi: 10.1002/wene.81R