IAEA
International Atomic Energy Agency
Atoms for Peace and Development

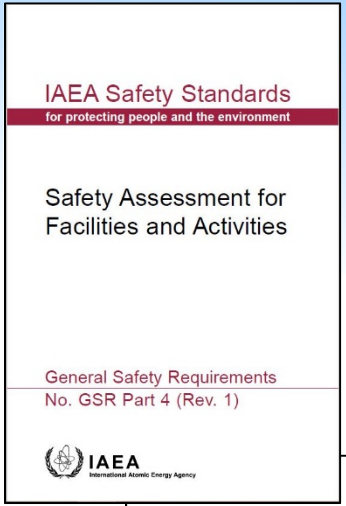
International Training Course
on the IAEA Safety Standards
at Tokai University, 11-14 March 2024

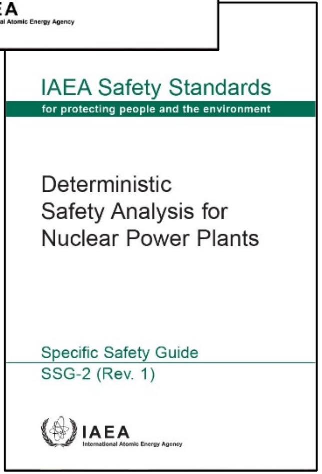
Safety Assessment for Facilities and Activities - GSR Part 4 (Rev.1) & Deterministic Safety Analysis for Nuclear Power Plant - SSG-2 (Rev.1)

Jorge LUIS HERNANDEZ
Senior Nuclear Safety Officer (NPP Design Safety)
Safety Assessment Section (SAS), Division of Nuclear Installation Safety (NSNI)
Department of Nuclear Safety and Security
IAEA

Outline

- SAFETY ASSESSMENT
  - INTRODUCTION TO IAEA GENERAL SAFETY REQUIREMENTS GSR PART 4 (REV. 1)
  - OVERVIEW OF REQUIREMENTS
  - RECOMMENDATIONS FOR PERFORMING AND VERIFYING DETERMINISTIC SAFETY ANALYSIS FOR NPPS SSG-2 (REV. 1)
- CONCLUSIONS

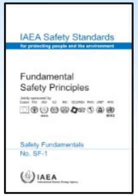

IAEA Safety Standards
for protecting people and the environment
Safety Assessment for Facilities and Activities
General Safety Requirements
No. GSR Part 4 (Rev. 1)
IAEA
International Atomic Energy Agency


IAEA Safety Standards
for protecting people and the environment
Deterministic Safety Analysis for Nuclear Power Plants
Specific Safety Guide
SSG-2 (Rev. 1)
IAEA
International Atomic Energy Agency

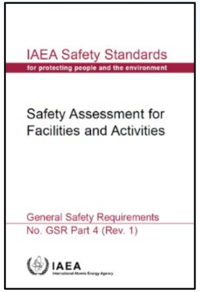
The safety assessment process
Introduction

Safety assessment

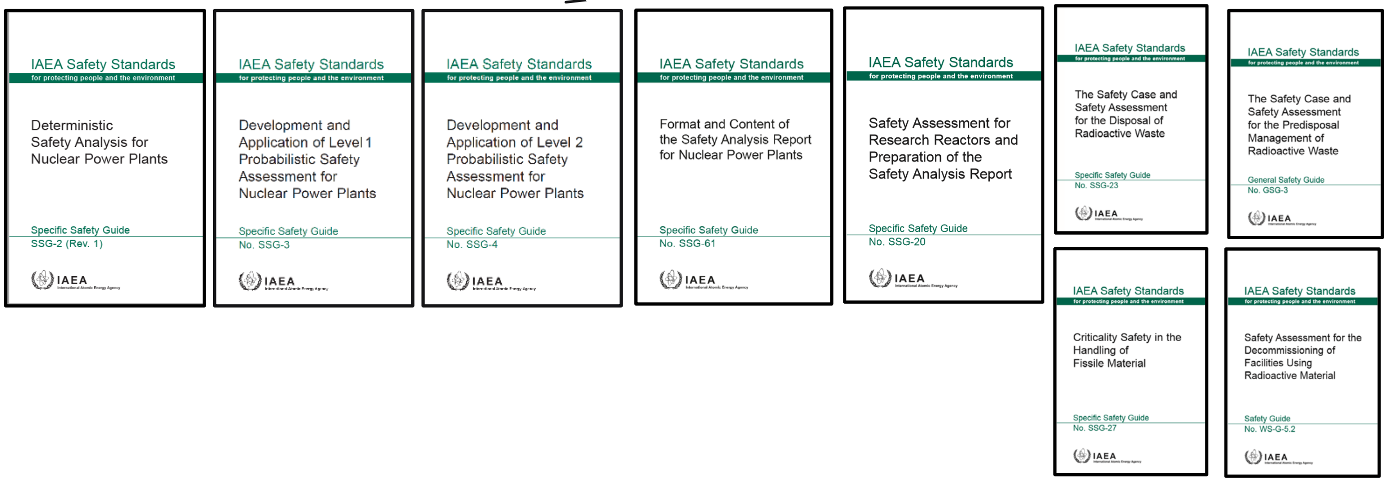
Safety objectives and safety principles



Functional conditions required for safety



Guidance on how to fulfil the requirements



Safety assessment

IAEA

Requirements for conducting the safety assessment are defined in the General Safety Requirements (GRS Part 4 (Rev.1), 2016)

IAEA Safety Standards
for protecting people and the environment

Safety Assessment for Facilities and Activities

General Safety Requirements
No. GSR Part 4 (Rev. 1)

IAEA
International Atomic Energy Agency

CONTENTS

Revised after the Fukushima Daiichi nuclear accident. The changes introduce reinforcements related to:

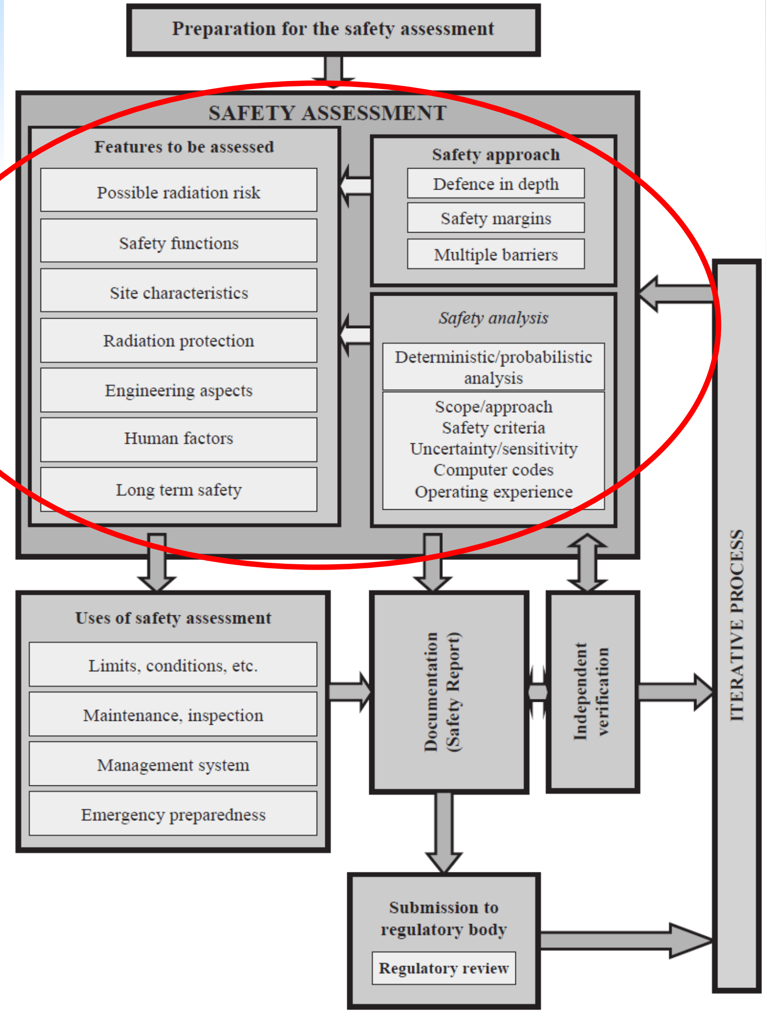
- Margins to withstand external events
- Margin to avoid cliff-edge effects
- Multiple facilities/activities at one site
- Cases where resources are shared
- Human factors in accident conditions

Safety assessment

Is the systematic process that is carried out throughout the lifetime of the facility or activity to ensure that all the relevant safety requirements are met by the proposed or actual design.

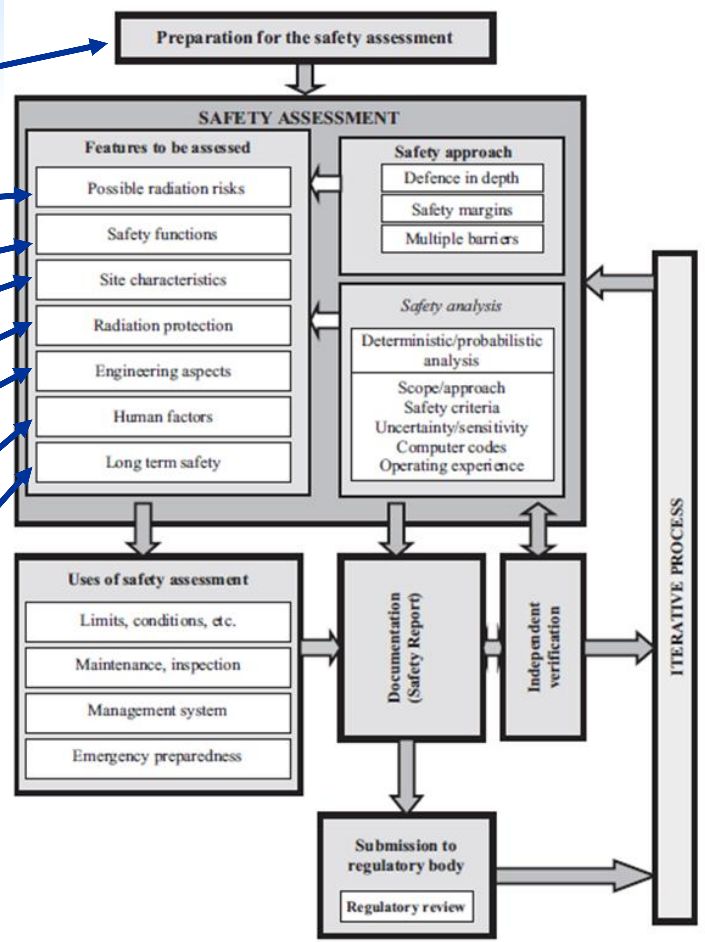
For an authorized facility, it includes siting, design and operation of the facility.

Safety assessment includes, but is not limited to, the **formal safety analysis**.



Safety assessment

1. Preparation for the safety assessment, in terms of assembling the expertise, tools and information required to carry out the work;
2. Identification of the possible radiation risks resulting from normal operation, anticipated operational occurrences or accident conditions
3. Identification and assessment of a comprehensive set of safety functions;
4. Assessment of the site characteristics that relate to the possible radiation risks;
5. Assessment of the provisions for radiological protection;
6. Assessment of engineering aspects to determine whether the safety requirements for design relevant to the facility or activity have been met;
7. Assessment of human factor related aspects of the design and operation of the facility or the planning and conduct of the activity;
8. Assessment of safety in the longer term, which is of particular concern when ageing effects might develop and might affect safety margins, decommissioning and dismantling of facilities, and closure of repositories for radioactive waste.



GSR Part 4, Revision 1

Req. 1

GRADED APPROACH

A graded approach shall be used in determining the scope and **level of detail** of the safety assessment carried out in a particular State **for any particular facility or activity**, consistent with the **magnitude of the potential radiation risks** arising from the facility or activity

SCOPE

SCOPE OF SAFETY ASSESSMENT

A safety assessment shall be carried out for **all applications of technology** that give rise to radiation risks — that is, for all types of facilities and activities

Req. 2

GSR Part 4, Revision 1

FACILITIES

- NPP
- Other nuclear reactors (research reactors and critical assemblies)
- Enrichment facilities and fuel fabrication facilities;
- Conversion facilities used to generate UF6;
- Storage and reprocessing plants for irradiated fuel;
- Facilities for radioactive waste management where radioactive waste is treated, conditioned, stored or disposed of;
- Any other places where radioactive materials are produced, processed, used, handled or stored;
- Irradiation facilities for medical, industrial, research and other purposes, and any places where radiation generators are installed;
- Facilities where the mining and processing of radioactive ores (such as ores of uranium and thorium) are carried out.

ACTIVITIES

- The production, use, import and export of radiation sources for industrial, research, medical and other purposes;
- The transport of radioactive material;
- The decommissioning and dismantling of facilities and the closure of disposal facilities for radioactive waste;
- The close-out of facilities where the mining and processing of radioactive ore was carried out;
- Activities for radioactive waste management such as the discharge of effluents;
- The remediation of sites affected by residual radioactive material from past activities.

Req. 2

GSR Part 4, Revision 1

Req. 3

RESPONSIBILITY FOR SAFETY ASSESSMENT

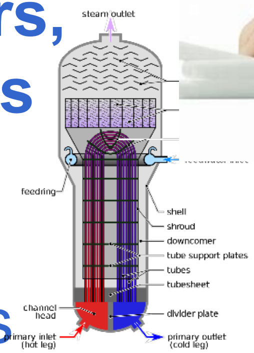
The responsibility for carrying out the safety assessment shall rest with the **responsible legal person**, i.e. the person or organization responsible for the facility or activity.

IAEA Fundamental Safety Principles

*"The **licensee** retains the **prime responsibility** for safety throughout the lifetime of facilities and activities, and this responsibility **cannot be delegated**."*

GSR Part 4, Revision 1

Other groups, such as **designers, manufacturers, constructors, employers, contractors, consignors** and **carriers**, also have legal, professional or functional responsibilities with regard to safety.



The regulatory authority shall review and assess submissions on safety from the operators both prior to authorization and periodically during operation as required.

Granting of Authorization (Licence)

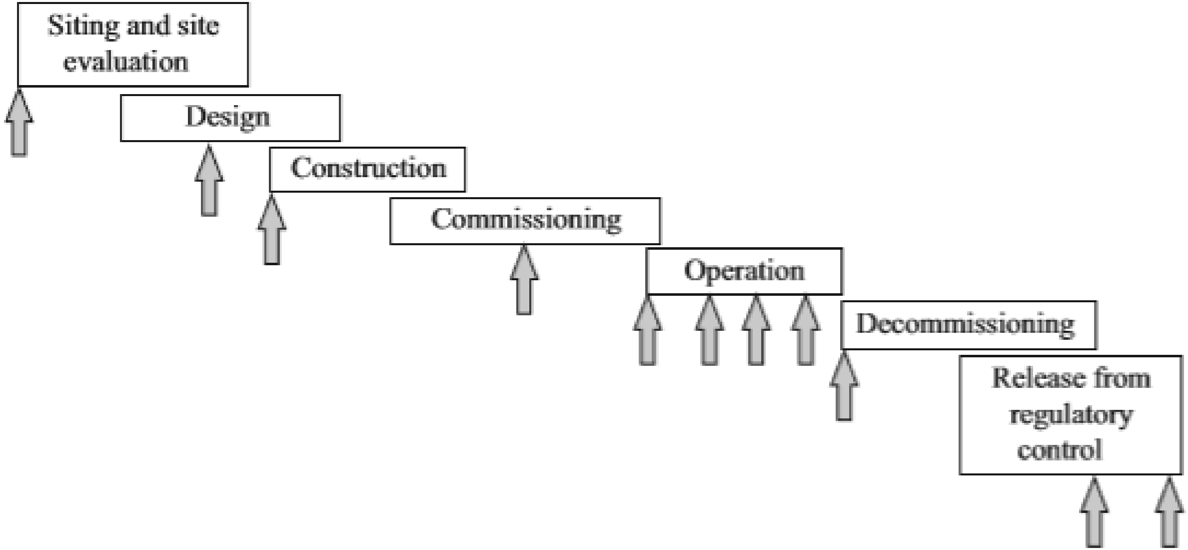


FIG. 1. Stages in the lifetime of a nuclear installation; the arrows indicate where hold points may be imposed.

IAEA SAFETY Standards, SSG-12 "Licensing Process for Nuclear Installations, IAEA 2010

Granting of Authorization (Licence)

Format and content of submission set-up by the regulator

Safety assessment performed by the applicant to demonstrate the level of safety

Communications with the designer/vendor

Independent review of the safety assessment by support organizations

Communications with other involved organizations

Regulatory Review and assessment

- Regulatory authority
- Independent review of the safety assessment by support organizations

REGULATORY DECISION
- granting of authorization
- authorization with conditions
- refusal of authorization

Purpose and scope of the safety assessment

GSR Part 4, Revision 1

PURPOSE OF THE SAFETY ASSESSMENT

Req. 4

The primary purposes of the safety assessment shall be:

- to determine whether an **adequate level of safety** has been achieved for a facility or activity

- whether the basic **safety objectives and safety criteria** established by the designer, the operating organization and the regulatory body have been **fulfilled**

> in compliance with the requirements for radiation protection and safety as established in the International Basic Safety Standards for Protection against Ionizing Radiation and for the Safety of Radiation Sources

GSR Part 4, Revision 1

Req. 5

PREPARATION FOR THE SAFETY ASSESSMENT

The **first stage** of carrying out the safety assessment shall be to ensure that the **necessary resources, information, data, analytical tools** as well as **safety criteria** are **identified** and are **available**.

Req. 6

ASSESSMENT OF THE POTENTIAL RADIATION RISKS

The **possible radiation risks** associated with the facility or activity shall be **identified** and **assessed**

GSR Part 4, Revision 1

Req. 7

ASSESSMENT OF SAFETY FUNCTIONS

All **safety functions** associated with a facility or activity shall be **specified and assessed**

Req. 8

ASSESSMENT OF SITE CHARACTERISTICS

An assessment of the **site characteristics** relating to the safety of the facility or activity shall be carried out

GSR Part 4, Revision 1

Req. 9

ASSESSMENT OF THE PROVISIONS FOR RADIATION PROTECTION

It shall be determined in the safety assessment for a facility or activity whether **adequate measures** are in place to protect **people and the environment** from harmful effects of ionizing radiation

Req. 10

ASSESSMENT OF ENGINEERING ASPECTS

It shall be determined in the safety assessment whether a facility or activity uses, to the extent reasonable, **structures, systems** and **components** of **robust and proven design**

GSR Part 4, Revision 1

Req. 11 ASSESSMENT OF HUMAN FACTORS

Human interactions with the facility or activity shall be **addressed** in the safety assessment and it shall be determined whether **the procedures and safety measures** that are **provided** for all **normal operational activities**, in particular those that are necessary for implementation of the operational limits and conditions, and those that are required in response to anticipated operational occurrences and accidents, ensure an **adequate level of safety**

Req. 12 ASSESSMENT OF SAFETY OVER THE LIFETIME OF A FACILITY OR ACTIVITY

The safety assessment shall cover **all the stages in the lifetime** of a facility or activity in which there are possible radiation risks

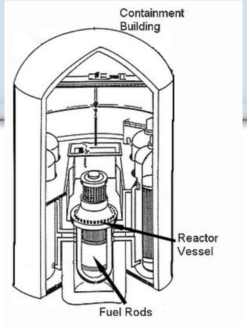
Performing the safety assessment

GSR Part 4, Revision 1

Req. 13

ASSESSMENT OF DEFENCE IN DEPTH

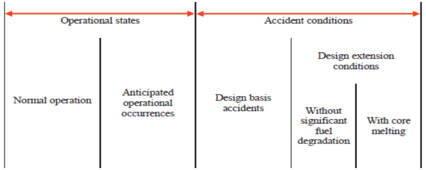
It shall be determined in the assessment of defence in depth whether adequate provisions have been made at **each of the levels of defence in depth**



Req. 14

SCOPE OF THE SAFETY ANALYSIS

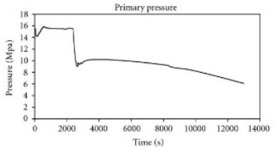
The performance of a facility or activity in **all operational states** and, as necessary, in the post-operational phase shall be **assessed in the safety analysis**.

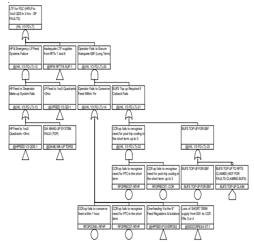


Req. 15

DETERMINISTIC AND PROBABILISTIC APPROACHES

Both deterministic and probabilistic approaches shall be included in the safety analysis





GSR Part 4, Revision 1

Req. 16

CRITERIA FOR JUDGING SAFETY

Criteria for judging safety shall be defined for the safety analysis

Req. 17

UNCERTAINTY AND SENSITIVITY ANALYSIS

Uncertainty and sensitivity analysis shall be performed and taken into account in the results of the safety analysis and the conclusions drawn from it

Req. 18

USE OF COMPUTER CODES

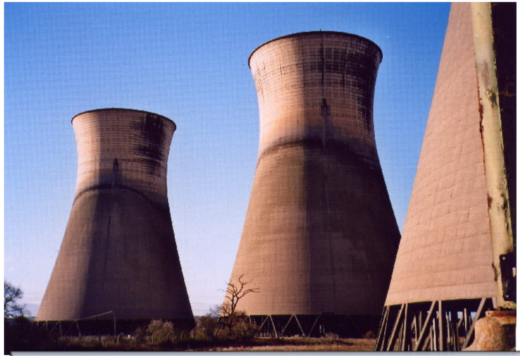
Any calculational methods and computer codes used in the safety analysis shall undergo verification and validation.

GSR Part 4, Revision 1

Req. 19

USE OF OPERATING EXPERIENCE DATA

Data on operational safety performance shall be collected and assessed



Req. 20

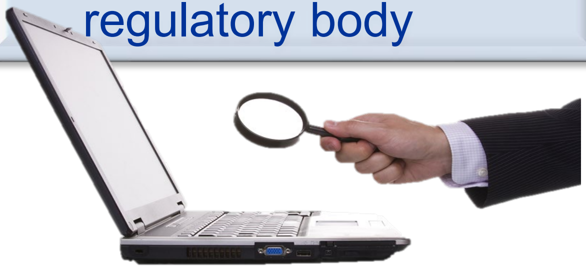
DOCUMENTATION OF THE SAFETY ASSESSMENT

The results and findings of the safety assessment shall be documented

Req. 21

INDEPENDENT VERIFICATION

The operating organization shall carry out an independent verification of the safety assessment before it is used by the operating organization or submitted to the regulatory body



GSR Part 4, Revision 1

MANAGEMENT OF THE SAFETY ASSESSMENT

Req. 22

The processes by which the safety assessment is produced shall be planned, organized, applied, audited and reviewed

USE OF THE SAFETY ASSESSMENT

Req. 23

The results of the safety assessment shall be used:

- to specify the programme for maintenance, surveillance and inspection;

- to specify the procedures to be put in place for all operational activities significant to safety and for responding to anticipated operational occurrences and accidents;

- to specify the necessary competences for the staff involved in the facility or activity;

- to make decisions in an integrated, risk informed approach

GSR Part 4, Revision 1

MAINTENANCE OF THE SAFETY ASSESSMENT

Req. 24

The safety assessment shall be periodically <u>reviewed and updated</u>

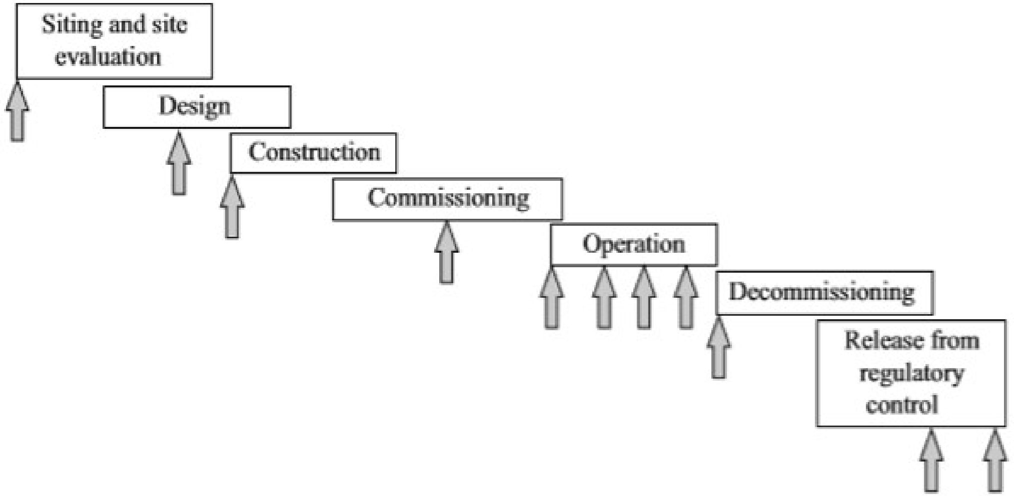


FIG. 1. Stages in the lifetime of a nuclear installation; the arrows indicate where hold points may be imposed.

Deterministic safety analysis for NPPs (SSG-2 (Rev.1))

Safety Guide Contents

Chapter 1: Background, objective, scope and structure

Chapter 2 : Terminology and main parts of the analysis

Chapter 3 : Identification, categorization and grouping of initiating events and accident scenarios to be analysed

Chapter 4: Acceptance criteria to be used in DSA. Rules to establish them and their use.

Chapter 5: Computer codes. Selection, validation and verification of codes, plant models. for development, verification and validation, selection and use of computer codes and plant models and input data.

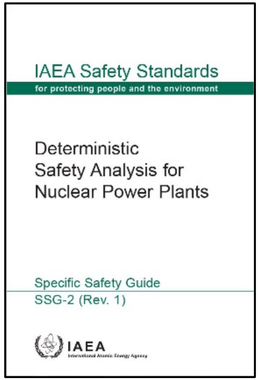
Chapter 6: Analysis approaches for different plant states: conservative, best estimate with quantification of uncertainties.

Chapter 7: More specific guidance on DSA for different plant states: NO, AOOs, DBAs and DEC, including severe accidents

Chapter 8: Documentation, review, and update of DSA

Chapter 9: Independent verification

Annex: Applications of DSA

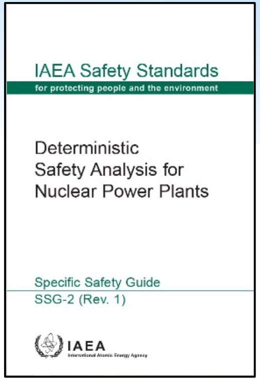


Deterministic safety analysis: Areas of application

Deterministic Safety Analysis

Deterministic safety analysis (DSA) is the analytical evaluation of physical NPP performance for all plant states. Confirming or demonstrating that:

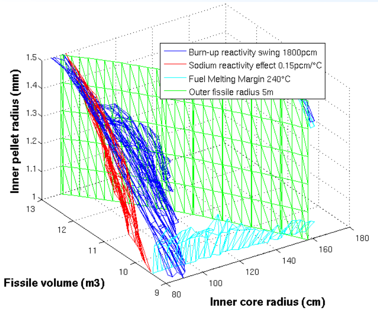
- Safety functions can be achieved by the proposed engineering design with the necessary reliability;
- Structures, systems and components are capable and sufficiently effective to prevent an uncontrolled release of radioactive substances and to keep them below acceptable limits for all plant states by maintain their integrity to the extent required;
  - Characterization of the appropriate Postulated Initiating Events (PIEs);
- The characteristics of potential radioactive release (source terms) for different plant states are determined and acceptable;
  - Analysis and evaluation of the event sequences resulting from the PIEs;
  - Plant event sequences that could lead to an early radioactive release or a large radioactive release are ‘practically eliminated’;
- Validity and compliance of:
  - the operational limits and conditions with the design assumptions;
  - the results with acceptance criteria and limits.

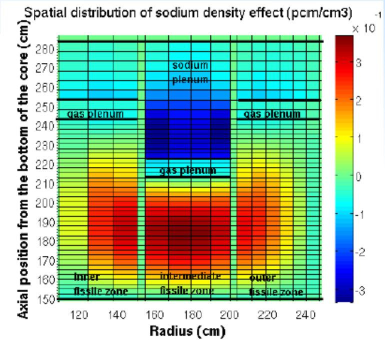


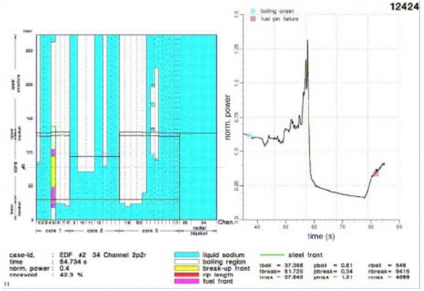
Technical areas of Deterministic Safety Analysis

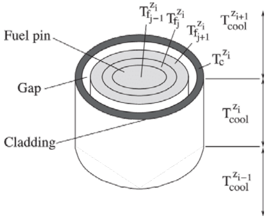
Technical areas concerned by DSA

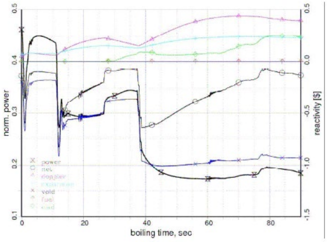
- Reactor physics
- System thermal-hydraulics
- Fuel behavior
- Material science
- Severe accidents
- Containment behavior
- Atmospheric dispersion
- Equivalent dose
- …

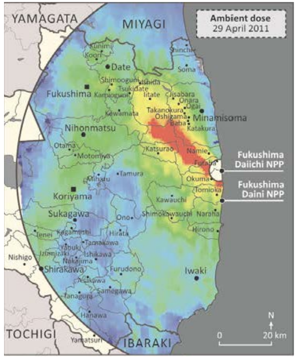












Deterministic safety analysis for NPPs

Postulated Initiating Events & Accident Scenarios

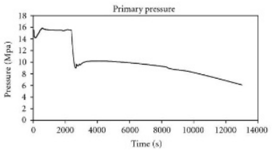
Identification

Categorization

Grouping

Acceptance Criteria

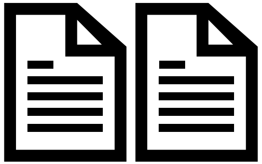
Computer Codes



Conducting DSA

Option	Computer code type	Assumptions on systems availability	Type of initial and boundary conditions
1. Conservative	Conservative	Conservative	Conservative
2. Combined	Best estimate	Conservative	Conservative
3. Best estimate plus uncertainty	Best estimate	Conservative	Best estimate; partly most unfavourable conditions
4. Realistic	Best estimate	Best estimate	Best estimate

Approaches



Documenting DSA results

Independent Verification & Review

Identification, categorisation and grouping of PIEs and accident scenarios

Updated plant states definition within SSR-2/1 (Rev. 1)

IAEA

Req. 13 **CATEGORIES OF PLANT STATES**

Plant states shall be **identified** and shall be grouped into a limited number of **categories** according to their frequency of occurrence.

- **Normal operation**;
- **Anticipated operational occurrences**, which are expected to occur over the operating lifetime of the plant;
- **Design basis accidents**;
- **Design extension conditions**, including accidents with core melting.

Criteria shall be assigned to **each plant state**, such that **frequently** occurring plant states shall have no, or only minor, radiological consequences and plant states that could give rise to serious consequences shall have a very low frequency of occurrence.

Operational states		Accident conditions		Large or Early Releases
Normal Operation NO	Anticipated Operational Occurrences AOO	Design Basis Accidents DBA	Design Extension Conditions DEC	Practical Elimination

DSA for Normal Operation

Objective: Confirm NPP operation within specified operational limits and conditions

- System requirements
  - Contribution to the performance and maintain of the three fundamental safety functions.
  - Number of trains required
  - Modes of operation
- Functional criteria or values of process variables (Max/Min)
  - Service conditions
  - Environmental conditions
- Surveillance, monitoring and testing criteria (normal)
  - Range
  - Setup points

DSA for PIEs & Accident Scenarios

Objective: Confirm or demonstrate that NPP design is capable and sufficiently effective to achieve and maintain the three fundamental safety functions with the necessary reliability in case of Postulated Initiating Events and Accident Scenarios by:

- maintaining the integrity of barriers (compliance with technical acceptance criteria) to prevent an uncontrolled release of radioactive substances;
- And if it occurs, keeping them below acceptable limits (compliance with radiological acceptance criteria) and Practical Elimination concept;

PIEs: Set of initiating failures

Prediction of the plant behaviour in plant states other than N.O. (AOO, DBA, DEC) based on **plant specific list of PIEs**

- Target: anticipate all foreseeable events with potential for **serious consequences** or with significant frequency of occurrence
- Due account of operating experience feedback, including operating experience from the actual or similar NPP

Set of PIEs defined to cover all **credible failures**

- of structures, systems and components of the plant, arising from internal and external hazards
- initiated by operator errors

PIEs: Consequential failures

Consideration as a part of the PIE of all **consequential failures** that a given PIE could originate

INITIATING EVENT

- **Failure** of part of an **electrical distribution system**
  - Analysis should assume the **unavailability** of all the **equipment powered** from it
- **Energetic event**
  - Analysis should include consideration of **potential failure** of the **equipment** that could be **affected** by such an event
- **Internal hazards**
  Failures caused by **external hazards**
  - Definition of induced PIE should include **failure** of all **equipment:**
    - **Not designed to withstand the effects** of the event
    - **Not protected** from it

Grouping of PIEs (1/2)

Not necessary to analyse all PIEs
→ grouping event sequences, taking into account PIEs' physical evolution

Basis for grouping

- similar **challenge** to the safety functions and barriers
- similar **mitigating** systems to drive the plant to a safe state

Bounding sequences are chosen to represent and referred to when dealing with the group

- Same assumptions criteria and initial conditions are selected and applied to all PIEs grouped under the same representative event sequence

Grouping of PIEs (2/2)

Similar **methodology** of analysis **within the group**:

- same computer code applicable
- similar acceptance criteria and/or similar initial conditions
- applying similar methodologies with the results being presented in similar form
- it is possible for each group to identify the worst accident (bounding case) which can significantly reduce number of needed calculations

Categorization of PIE based on frequency

TABLE II–1. EXAMPLE OF ANTICIPATED OPERATIONAL OCCURRENCES AND DESIGN BASIS ACCIDENT CATEGORIES USED IN SOME STATES

Plant state	Alternative names used in some States	Indicative frequency range (per year)
Anticipated operational occurrences	Faults of moderate frequency: DBC-2, PC-2	$f > 10^{-2}$
Design basis accidents	Infrequent faults: DBC-3, PC-3 Limiting faults: DBC-4, PC-4	$10^{-2} > f > 10^{-4}$ $10^{-4} > f > 10^{-6}$

Note: DBC — design basis condition; PC — plant condition. The designations DBC-1 and PC-1 are used for normal operation. Some other accidents for which the frequency is $<10^{-6}$ need to be considered because they are representative of a type of risk from which the reactor has to be protected.

Identification of PIEs leading to DECs

DEC result from sequences in which the safety systems have malfunctioned and some of the barriers to the release of radioactive material have failed or have been bypassed

Identification by using:

- **the results of Level 1 PSA**
- **representative sequences of severe accidents**

Examples of DEC initiators:

- Complete loss of the residual heat removal from the reactor core
- LOCA with a complete loss of the high- or low-pressure emergency core cooling
- Complete loss of electrical power for an extended period

DEC without significant Fuel Degradation

Selection based on consideration of single **initiating events of very low frequency** or **multiple failures**, to meet acceptance criteria on prevention of core damage

A deterministically derived **list** of DECs without significant fuel degradation to be developed including:

- Initiating events that could lead to situations **beyond the capability** of safety systems designed for DBAs
- **AOO** or **frequent DBAs** combined with **multiple failures** that prevent the safety systems from performing their intended function to control the PIE; failures of supporting systems are implicitly included
- **Credible PIEs** involving multiple failures causing the loss of a safety system while this system is used to fulfil its function as part of normal operation

DEC Sequences with Core Melting (1/2)

Selection to establish the design basis for the safety features for mitigating the consequences

- to represent all main physical phenomena involved

Assumptions

- insufficiency of features to prevent core melting failures
- accident sequence will further evolve into a severe accident
- ➢ Selection of **representative sequences** considering additional failures / incorrect operator responses to DBA/DEC sequences and to dominant accident sequences identified in PSA

Representative sequences

- analysed to determine limiting conditions, particularly those that could challenge the integrity of containment
- used to provide input to design of containment and of safety features necessary to mitigate consequences of such DECs

DEC Sequences with Core Melting (2/2)

List of DECs: Preliminary Reference

- Loss of core cooling capability
- Loss of reactor coolant system integrity

Low estimated frequency of occurrence: not sufficient reason for failing to protect the containment

- **Postulate** core melt conditions regardless of provisions implemented
- To exclude containment failure → Demonstration that resulting **very energetic phenomena** with core melting are **prevented**

Selection of **representative sequences** to identify the most severe plant parameters, to be used in DSA to demonstrate **limitation of radiological consequences**

Typical equipment qualification programmes not always applicable: ‘**survivability assessment**’ is acceptable

Practical elimination: Safety Standards

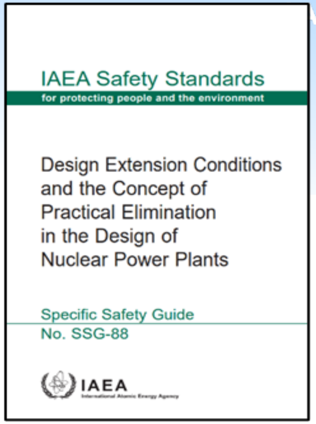
SSR-2/1 (Rev. 1), Par 2.13 (4)

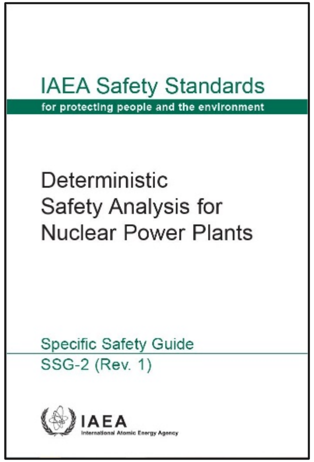
*"The safety objective in the case of a severe accident is that only **protective actions** that are **limited** in terms of lengths of time and areas of application would be **necessary** and that **off-site contamination** would be **avoided** or minimized. Event sequences that would lead to an **early radioactive release** or a **large radioactive release** are required to be '**practically eliminated**' "*

- Radioactive release for which off-site protective actions would be **necessary** but would be **unlikely** to be **fully effective** in due time
- Radioactive release for which off-site protective actions that are **limited in terms of lengths** of time and areas of application would be **insufficient** for the protection of people and of the environment
- It would be **physically impossible** for the conditions to **arise** or if these conditions could be considered with a **high level of confidence to be extremely unlikely to arise**

Conditions to be Practically Eliminated

- Hypothetical accident sequences
- Events that could lead to prompt reactor core damage and consequent early containment failure
  - Failure of a large component in the reactor coolant system
  - Uncontrolled reactivity accidents
- Severe accident sequences that could lead to early containment failure
  - Highly energetic direct containment heating
  - Large steam explosion
  - Explosion of combustible gases, including hydrogen and carbon monoxide
- Severe accident sequences that could lead to late containment failure
  - Basemat penetration or containment bypass during MCCI
  - Long term loss of containment heat removal
  - Explosion of combustible gases, including hydrogen and carbon monoxide
- Severe accident with containment by pass
- Significant fuel degradation in storage fuel pool, uncontrolled releases





Acceptance criteria for Deterministic Safety Analysis

Acceptance criteria for DSA

- In DSA, tool to judge the **acceptability** of the **results, to** demonstrate the safety of the NPP
- **General**, **qualitative** terms or as **quantitative** limits
- **SSG-2 (Rev. 1)**: only **safety acceptance criteria** are addressed; they may include margins with respect to safety criteria

1. **Safety criteria**
   - relate either directly to:
     - radiological consequences of operational states or accident conditions;
     - integrity of barriers against releases of radioactive material due consideration to maintaining safety functions
2. **Design criteria**
   - design limits for individual structures, systems and components, which are part of the design basis as important preconditions for safety criteria
3. **Operational criteria**
   - rules for operator during N.O. and AOO, providing preconditions for design and safety criteria

Acceptance criteria for DSA

Safety acceptance criteria:

High level (radiological) criteria

defined by **law / regulatory requirements**	expressed in terms of **activity levels / doses**	related to **radiological consequences**

Detailed (derived) technical criteria

defined in **regulatory requirements** / proposed by the **designer**	related to **integrity of barriers**

Acceptance criteria for DSA

- **More frequent** conditions (N.O. or AOO): **More restrictive** acceptance criteria

- **Less frequent** events (DBA, DEC): **Less restrictive** acceptance criteria

AOO
- no consequential failure of any of the physical barriers and no fuel damage

DBAs, DECs
- barriers to the release of radioactive material from the plant should maintain their integrity to the extent required

DECs (core melting)
- containment integrity should be maintained, and containment bypass should be prevented to ensure prevention of an early radioactive release or a large radioactive release

Acceptance criteria for DSA

Technical acceptance criteria: **integrity** of…

a)Nuclear fuel matrix
- maximum fuel temperature, maximum radially averaged fuel enthalpy

•Fuel cladding
- minimum departure from nucleate boiling ratio, maximum cladding temperature, maximum local cladding oxidation

•Whole reactor core
- adequate subcriticality, maximum production of hydrogen from oxidation of cladding, maximum damage of fuel elements in the core, maximum deformation of fuel assemblies, calandria vessel integrity

•Nuclear fuel located outside the reactor
- adequate subcriticality, adequate water level above the fuel assemblies and adequate heat removal

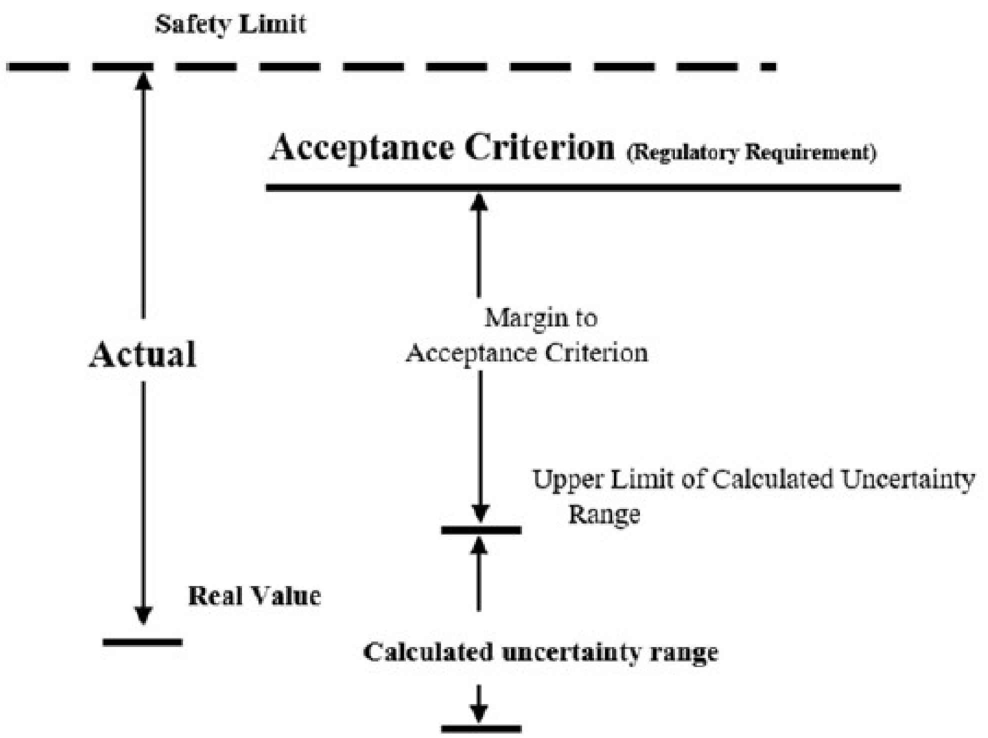
•Reactor coolant system
- maximum coolant pressure, maximum temperature-pressure-temperature changes and resulting stresses and strains in the coolant system pressure boundary,…

•Secondary circuit (if relevant)
- maximum coolant pressure, maximum temperature-pressure-temperature changes in secondary circuit equipment

•Containment / limitation of releases to the environment
- value and duration of maximum and minimum pressure, maximum pressure differences acting on containment walls, maximum leakages, maximum concentration of flammable or explosive gases,…

•Other component necessary to limit radiation exposure
- maximum pressure, temperature and heat-up rate

Conservative specification of acceptance criteria



For LOCA design basis accident conditions, the regulatory criteria are for example:

- Peak clad temperature (1204°C)
- Maximum clad oxidation (17% of clad thickness)
- Maximum hydrogen generation (not to exceed deflagration or detonation limits for containment integrity)
- Coolable geometry of core

IAEA-TECDOC-1909 Considerations on Performing Integrated Risk Informed Decision Making
IAEA-TECDOC-1332 Safety Margins of Operating Reactors (2003)

Global acceptance criteria

Associated with radiological consequences

Normal operation

- criteria typically expressed as effective dose limits for the plant staff and for the members of the public, and acceptable releases from the plant.
- **Acceptable dose** limits are of order of **~0.1 mSv per year**

Anticipated operational occurrences

- criteria more restrictive than for design basis accidents since their frequencies are higher.
- **Acceptable dose** limits per each event are comparable with **annual dose limits for normal operation**

Design basis accidents

- either no off-site radiological impact or only minor radiological impact outside the exclusion area. Very restrictive dose limits in order to exclude the need for off-site emergency actions.
- **Acceptable dose** limits are typically of order of few **(1-5) mSv per year**

Global acceptance criteria

Associated with radiological consequences

Severe accidents:

The consequences can be defined in terms of **effective dose to critical groups**, or in terms of **radioactivity release** into the **environment** above a specified threshold

The criteria are intended to ensure that there will be neither short term nor long term health effects following a severe accident:

- Typical effective dose limits are of order of several tens or hundreds of mSv; the value strongly depends on conditions considered for determination of doses
- Optionally, radiological criteria can be expressed in terms of acceptable releases of selected radioisotopes (I131, Cs137) or groups of radioisotopes

Acceptance criteria and levels of DiD

Level of defence	Objective	Associated plant state	Criteria for maintaining integrity of barriers	Criteria for limitation of radiological consequences
Level1	Prevention of abnormal operation and failures	Normal operation	No failure of any of the physical barriers except minor operational leakages	Negligible radiological impact beyond immediate vicinity of NPP. Acceptable effective dose limits are bounded by general radiation protection limit for the public (1 mSv /year commensurate with natural background), typically ~~0.1 mSv/year.
Level 2	Control of abnormal operation and detection of failures	Anticipated operational occurrence	No failure of any of the physical barriers except minor operational leakages	Negligible radiological impact beyond immediate vicinity of the plant. Acceptable effective dose limits are similar as for normal operation, limiting the impact per event and for the period of 1 year following the event (0.1 mSv/y)
Level 3a	Control of design basis accidents (DBAs)	Design basis accident	No consequential damage of the RCS, maintaining containment integrity, limited damage of the fuel	No or only minor radiological impact beyond immediate vicinity of the plant, without the need for any off-site emergency actions. Acceptable effective dose limits are typically few mSv/y. (1-5)
Level 3b	Control of DECs without significant fuel degradation	Design extension conditions without significant fuel degradation	No consequential damage of the RCS, maintaining containment integrity, limited damage of the fuel.	The same or similar radiological acceptance criteria as for the most unlikely design basis accidents.
Level 4	Control of DECs with core melt (mitigation of consequences of severe accidents)	Design extension conditions with core melt (severe accident)	Maintaining containment integrity both in an early as well as late phase, and practical elimination of fuel melt when the containment is disabled or by-passed	Radiological acceptance criteria ensuring that only emergency countermeasures that are of limited scope in terms of area and time are necessary
Level 5	Mitigation of radiological consequences of significant releases	Accidents with releases requiring implementation of emergency countermeasures	Containment integrity severely impacted, or containment disabled or bypassed	Off-site radiological impact necessitating emergency countermeasures

Approaches and Options for performing Deterministic Safety Analysis

Approaches and options for performing DSA

Option	Computer code type	Assumptions on systems availability	Type of initial and boundary conditions
1. Conservative	Conservative	Conservative	Conservative
2. Combined	Best estimate	Conservative	Conservative
3. Best estimate plus uncertainty	Best estimate	Conservative	Best estimate; partly most unfavourable conditions
4. Realistic	Best estimate	Best estimate	Best estimate

1) Conservative Accident Analysis

Assumed plant conditions and physical models are set conservatively

- Parameters: allocated values with an unfavourable effect in relation to specific acceptance criteria
- In the past, commonly adopted to simplify and compensate for limited modelling of phenomena with large conservatisms
- Assumption: to bind many similar transients in a way that acceptance criteria would be met for all bounded transients

Rarely used, as computer codes allowed to calculate results corresponding more accurately to experimental results and recorded event sequences in NPP

- **Not suggested** for current safety analysis, **except** in situations when scientific knowledge and experimental support is limited
- Still relevant, as it may have been used in legacy analyses

2) Combined Accident Analysis

Base: use of **'best estimate' models** and **computer codes** instead of conservative models and codes

Best estimate codes are used in combination with **conservative initial** and **boundary conditions,**
and with conservative assumptions regarding the availability of systems

- Assumptions:
  1. all **uncertainties** associated with the code models are **well established**
  2. plant **parameters** used are conservative based on operating experience

Complete analysis requires use of **sensitivity studies** to justify the selection of conservative input data

Commonly used for **DBAs** and for conservative analysis of **AOOs**

3) Best estimate plus uncertainty

Allows the use of best estimate **computer codes** together with more **realistic assumptions**

- Possible use of a mixture of best estimate and partially unfavourable initial and boundary conditions
- Usual conservative assumptions on availability of systems

Need to identify, quantify and statistically combine the uncertainties to ensure overall conservatism required

Accepted for some **DBAs** and for conservative analyses of **AOOs**

Mixture of Options 2 and 3 is often employed

Analyses performed according with Options 1, 2 and 3 are considered conservative, with decreasing conservatism from 1 to 3

Conservative approach for assuring safety margins

- The aim of the **deterministic approach** (to safety assessment) is to **specify** and **apply a set of conservative deterministic rules and requirements for the design and operation of facilities or for the planning and conduct of activities**

  - When these rules and requirements are met, they are expected to provide a **high degree of confidence** that the level of radiation risks to workers and members of the public arising from the facility or activity will be **acceptably low**

  - This conservative approach provides a way of **compensating for uncertainties** in the performance of equipment and the performance of personnel, by providing a **large safety margin**

4) Realistic Accident Analysis

Use of best estimate **models** and **codes** and **best estimates** of system availability and **initial and boundary conditions**

Appropriate for

- realistic analysis of **AOOs** aimed at assessment of control system capability
- best estimate analysis of **DECs**
- justifying prescribed operator actions in realistic analysis

Deterministic analysis for operating events that may necessitate a **short term relaxation** of regulatory requirements may also rely on best estimate modelling

Sources of uncertainties

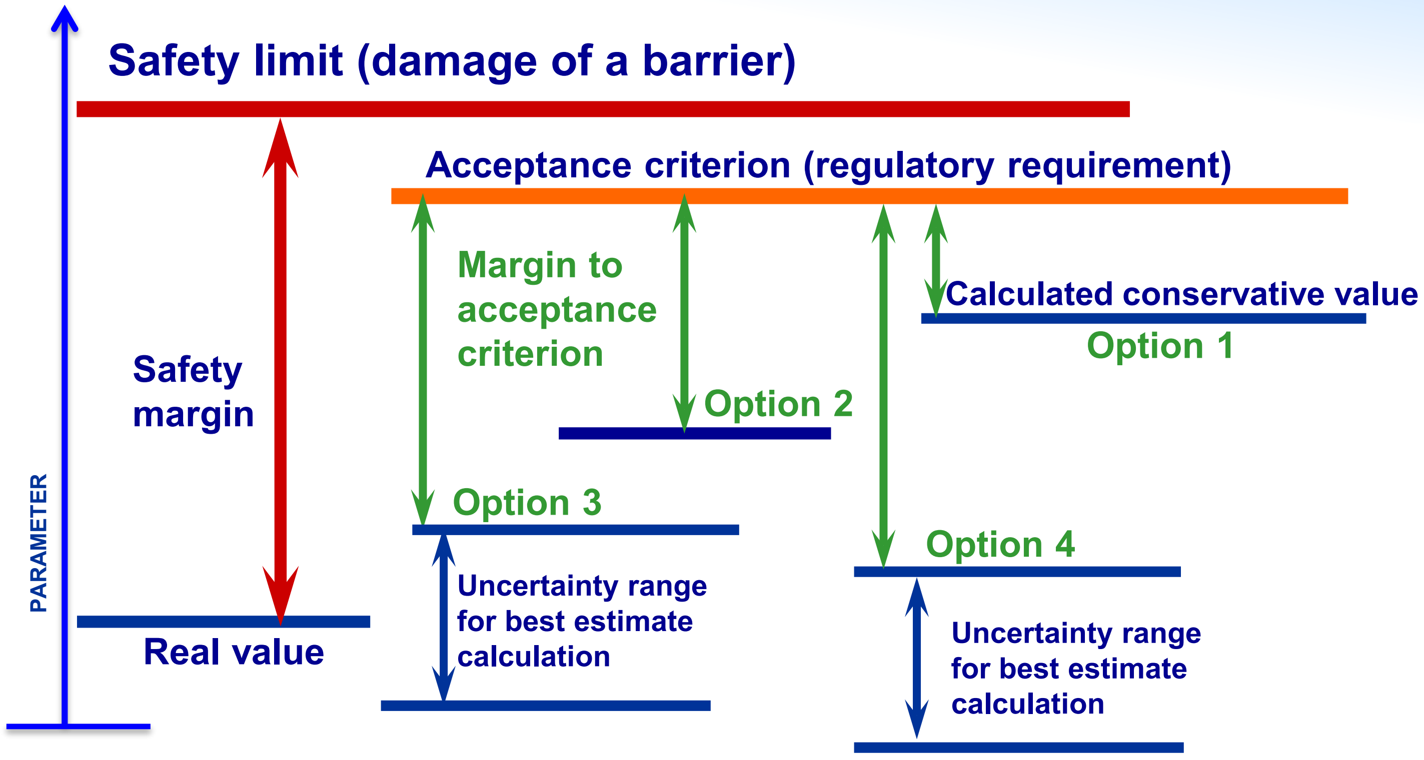
Code or model uncertainty: Uncertainty associated with the models and correlations, the solution scheme, model options, unmodelled processes, data libraries and deficiencies of the computer program.

Representation or simulation uncertainty (user effects): Uncertainty in representing or idealizing the real plant, such as that due to the inability to model the complex geometry accurately, three dimensional effects, scaling, control and system simplifications.

Plant uncertainty: Uncertainty in measuring or monitoring the real plant, such as reference plant parameters, instrument error, set points, instrument response.

Scaling uncertainty: Using data from scaled experiments.

Safety margins



Methodology for Analysis

Conservative approach is typically required for…

- Design and design modifications
- Licensing (design basis)
- Regulatory audit calculations

Best estimate is appropriate for…

- Design (control systems)
- Analysis of operational events.
- Licensing (Design Extension Conditions)
- Support for EOP, AM and emergency planning
- PSA related analysis

Determination of Source Term

Determination of the source term (1/3)

To predict **dispersion** of material, **impact** on environment and **exposure** for plant staff and public

Source term: “amount and isotopic composition of radioactive material released (or postulated to be released) from a facility”; it is necessary to determine

- **sources** of radiation
- **inventories** of radionuclides produced
- **mechanisms** by which radioactive material can travel from source through installation and be released

Simulation codes to predict, under accident conditions

- **fission product release** from fuel elements
- **transport** through primary system and containment/spent fuel pool building, and related **chemistry** affecting this transport
- **form** of release of radioactive material

Determination of the source term (2/3)

Reasons for evaluating the source term

- Confirm that design is **optimized** so that the source term is so low as reasonably
- Support ‘**practical elimination**’ of plant event sequences that could lead to an early radioactive release or a large radioactive release
- Demonstrate that **design** ensures respect of requirements for radiation protection
- Basis for **emergency** arrangements to **protect** human life, health, property and environment
- Support **specification** of conditions for **qualification** of **equipment** to withstand accidents
- Provide **data** for **training** activities on emergency arrangements
- Support design of **safety features** to mitigate severe-accidents consequence

General rules apply also to determine the source term: associated aspects are introduced to remind of the applicability of general rules to this specific application

Determination of the source term (3/3)

Separate analyses of source term for failures for which the phenomena that would affect the source term would be different

- Accidents in **manipulation** of irradiated fuel
- **Accidents** bypassing the **containment** or accidents taking place **outside** the containment
- **Loss of coolant** accidents with release of **reactor coolant** and **fission products** from the core to the containment
- Accidental releases from the **systems for treatment** and **storage** of **gaseous and liquid** radioactive waste

For many accidents, important release of radionuclides would be from the reactor **core** > into the reactor **coolant system** and then > into the **containment**

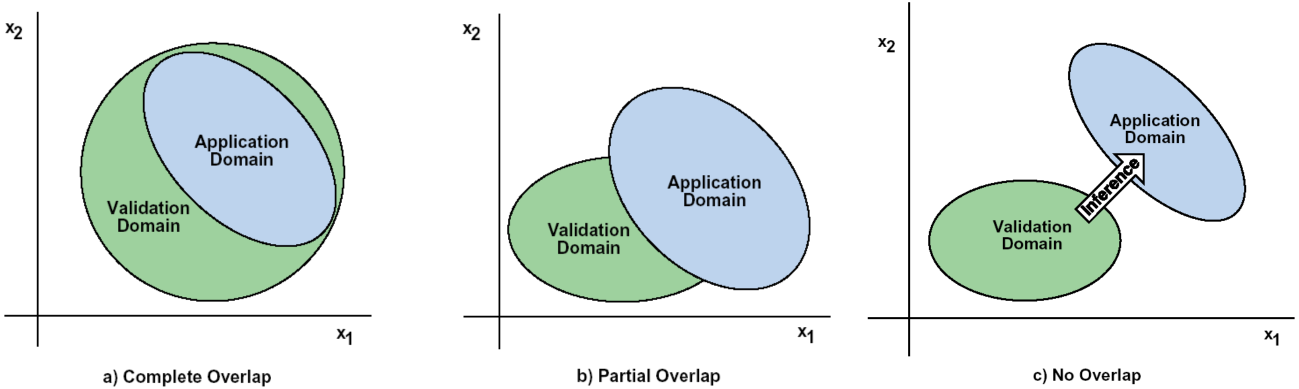
- Evaluation of source term should include predicting this behaviour of the radionuclides, until their release

USE OF COMPUTER CODES FOR DETERMINISTIC SAFETY ANALYSIS

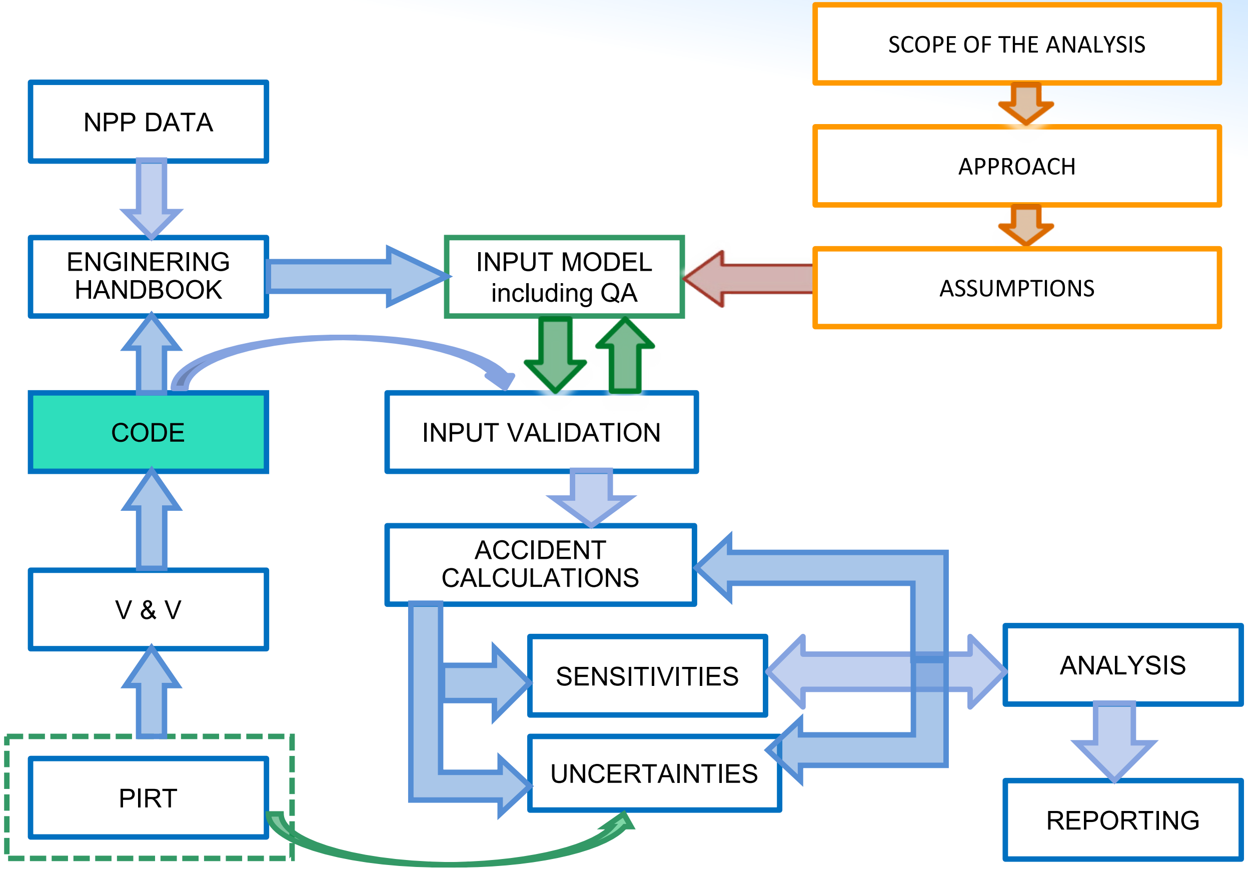
Computer code

Verification and validation, depending on the type of application and purpose of the analysis:

- Appropriate and adequate
- Able to simulate the analyzed facility and PIE



Safety Analysis Methodology



Code verification and validation (1/2)

GSR Part 4, Req. 18, § 4.60 "Any calculation methods and computer codes used in the safety analysis shall undergo verification and validation to a sufficient degree…

•VERIFICATION

- The code represents the **mathematical model** of the real system AND it conforms to the **code documentation**
  - Numerical methods
  - transformation of equations into numerical scheme to provide solutions
  - user options and restrictions
- in **accordance with specifications**

•VALIDATION

- Mathematical **models** used are an adequate representation of the real system being modelled
- Comparison of outputs with observations of the real system or experimental data

Code verification and validation (2/2)

- **VERIFICATION**
- **Comparison of the source coding** with its **description** in the documentation ("*doing thing right*")
- **VALIDATION**
- **Code assessment** against **relevant experimental data** to demonstrate the **applicability/accuracy** to **predict phenomena** expected to occur ("*doing right thing*")

PERFORMING DETERMINISTIC SAFETY ANALYSIS FOR DIFFERENT PLANT STATES

Overview of level of Conservatism

Plant state	Conservatism		Operator actions
	Code	Plant parameters & System performances	
Normal operation	BE	Conservative	BE
AOO (realistic)	BE	BE	BE
DBA + AOO (conservative)	BE*	Conservative	30 minutes
	BE + uncertainties	BE + uncertainties	30 minutes
DEC w/o significant fuel degradation	BE*	Conservative	30 minutes
	BE + uncertainties	BE + uncertainties	30 minutes
	BE*	BE**	BE
DEC w/ core melt	BE*	Conservative	>30 minutes
	BE*	BE**	BE

- BE*: sensitivities have to prove conservatism
- BE**: sensitivities needed to show no cliff-edge effect

Overview of Analysis Rules: Systems Credited

Plant state	Systems credited in the analysis			SFC	Maintenanc e (if allowed)
	Control & Limitation	Safety	DEC		
Normal operation	Operating	Not activated	Not activated	No	Yes
AOO (realistic)	Operating	Not activated	Not activated	No	No
DBA + AOO (conservative)	Fail	Yes	Not activated	Yes	Yes
DEC w/o significant fuel degradation	Fail	Yes if not affected by sequence	Yes	No	Possibly no
DEC with core melt	Fail	No except if fully independent from sequence	Yes except if not fully independent from sequence	No	Possibly no

Example of Conservative Boundary Conditions for a DBA: LOCA

Most unfavourable single failure;

Unavailability of some systems due to preventive maintenance;

Most unfavourable break location;

Range of break sizes resulting in highest peak cladding temperature;

Loss of off-site power;

Unfavourable initial core power;

Conservative values for the reactivity feedback coefficients;

Unfavourable time within the fuel cycle;

Unfavourable values for the thermal-hydraulic parameters;

Temperature conditions for the ultimate heat sink;

Stuck control rod.

BEPU Approach – Cons and Pros (1/2)

CONS

Time consuming – comprehensive data, high number of calculations

High requirements on the computation tools (high computer power, large data storage space)

Selection of uncertain parameters and definition of probabilistic distribution functions difficult due to the lack of information

Definition of uncertain parameters usually based on expert judgment leading to a possible user effect

Extensive experimental/operational data needed to reference applied values

Uncertainty bands often too broad (typically non-symmetrical), not only due to statistical nature of processes, but also due to limited knowledge of phenomena and of probability distribution of input parameters

BEPU approach – cons and pros (2/2)

CONS

Uncertainty methods sometimes provide bands for few parameters, others to be recalculated conservatively

Treatment of uncertainties when using several codes in sequence complicated; coupling of codes needed

PROS

Prediction of ‘realistic’ response of the plant

Safety margins are quantified

Several acceptance criteria evaluated in one step

Statistically sound evaluation of combined influence of input parameters

Close links to experimental results justifying or supporting the application of procedures or guidelines

DOCUMENTING THE RESULTS OF DETERMINISTIC SAFETY ANALYSIS

Documenting results of DSA

The information should be sufficient and comprehensive,:

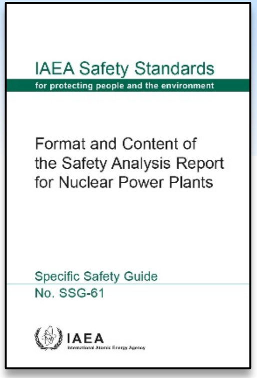
- to justify and confirm the design basis for items important to safety;
- to ensure that the overall plant design is capable of meeting the established acceptance criteria / limits;
- to enable an independent verification of the safety analyses.

describe:

- the scope, the approach, the process, the data, the assumptions, the criteria, <u>the results</u>, the uncertainties, etc.

and identify additional documents.

Quality Assurance



Documenting results of DSA

The documentation of the results should typically include the following information:

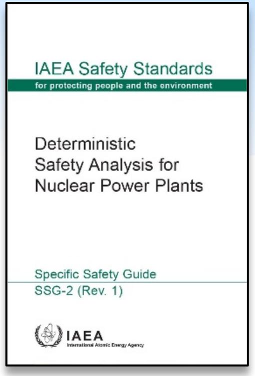
a) A chronological description of the main events as they have been calculated;

b) A description and evaluation of the accident on the basis of the parameters selected;

c) Figures showing plots of the main parameters calculated;

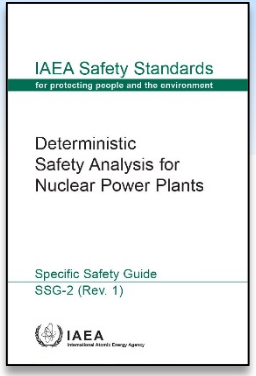
d) Conclusions on the acceptability of the level of safety achieved and a statement on compliance with all relevant acceptance criteria, including the adequacy of margins;

e) Results of sensitivity analyses, as appropriate.



INDEPENDENT VERIFICATION OF RESULTS OF DETERMINISTIC SAFETY ANALYSIS

Independent verification of DSA results



Internal

-QA during design process

External

Final design:

-by or on behalf of operating organization before submitted to the regulatory authority

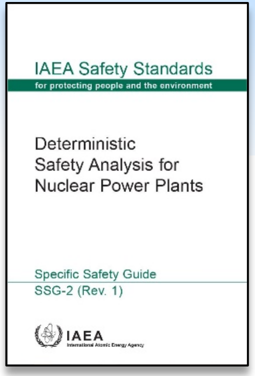
-by or on behalf of the regulatory authority

Narrow scope, focus on most significant issues and requirements

Independent verification of DSA results

The verification should include, as appropriate:

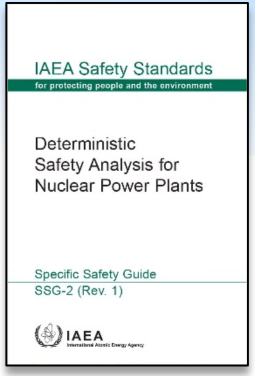
a) Compliance with the requirements of reference documents;
b) Completeness of the documentation;
c) Correctness of input data;
d) Selection of initiating events or accident scenarios;
e) Selection of acceptance criteria;
f) Selection of the safety analysis method;
g) Selection of safety analysis computer codes and adequacy of code validation;
h) Selection of assumptions for ensuring safety margins;
i) Adequacy of the description and evaluation of the analysis results.



Independent verification of DSA results

The verification should confirm:

a) How the safety analysis were performed;
b) PIEs and accident scenarios representativeness;
c) Consideration of consequential failures and event combinations;
d) V&V of computer codes;
e) Appropriate computational models:
f) Assumptions and data;
g) Adequate sensitivity and uncertainty evaluations;
h) Plant systems in different plant states;
i) Acceptance criteria & limits;
j) Acceptability of independent calculations;
k) Discrepancies found do not question conclusions.



DSA: Areas of Application

a) Design
b) Licensing purposes
c) Independent verification
d) Periodic Safety Review
e) Plant modifications
f) Events exceeding normal operation limits
g) Development / Validation of EOPs
h) Development of SAMGs
i) Demonstration of success criteria and development of accident sequences (Level 1 PSA & Level 2 PSA)

Conclusions

Conclusion (1/2)

Conducting the deterministic safety analyses should be led to questioning yourself whether you are convinced that for all plant states it is confirmed or demonstrated that:

- Fundamental safety functions can be achieved and maintained by the proposed engineering design with the necessary reliability;
- Structures, systems and components are capable and sufficiently effective to prevent an uncontrolled release of radioactive substances and to keep them below acceptable limits for all plant states by maintain their integrity to the extent required;
- The identification and characterization of Postulated Initiating Events (PIEs) is appropriated;

Conclusion (2/2)

Conducting the deterministic safety analyses should be led to questioning yourself whether you are convinced that for all plant states it is confirmed or demonstrated that (cont'):

- The characteristics of potential radioactive release (source terms) for different plant states are determined and acceptable;
  - Analysis and evaluation of the event sequences resulting from the PIEs;
  - Plant event sequences that could lead to an early radioactive release or a large radioactive release are 'practically eliminated';
- Validity and compliance of:
  - the operational limits and conditions with the design assumptions;
  - the results with acceptance criteria and limits.

Terminology

Conservative model: Pessimistic estimate for a physical process relative to specific acceptance criteria

Conservative code: A combination of models aimed to provide a pessimistic bound to the processes related to specific acceptance criteria

Conservative data: Plant parameters, initial plant conditions, equipment availability, operator actions and accident sequence assumptions chosen to give a pessimistic result

Best estimate model: A model which provides a realistic estimate of a physical process to the degree consistent with the currently available data and knowledge of phenomena

Best estimate code: A combination of the best estimate models necessary to provide a realistic estimate of the overall response of the plant during an accident.

Best estimate data: Most likely plant parameters, initial plant conditions, equipment availability, operator actions and accident sequence assumptions

PIEs: other examples (1/2)

Other failures are assumed in DSA for **conservatism** or for the purpose of **DiD**

- **Distinction** between these failures and those part of, or directly caused by, PIEs
- To limit the number of analyses, some failures may be added to **bound** a **set** of **similar events**

PIEs should **include** only failures

- directly leading to **challenge safety functions**
- threatening integrity of **barriers** to radioactive material releases

Hazards should not be considered as PIEs by themselves, but **associated loads** should be considered **potential causes** of PIEs

PIEs: other examples (2/2)

Set of PIEs should be identified using a **systematic and structured approach**:

- Use of analytical methods (HAZOP,…)
- Comparison with list of PIEs from similar NPP
- Analysis of similar plants' operating experience data
- Insights and results from PSA

Certain limiting faults have been considered as DBAs

- representatives of accidents that the reactor has to be protected against, not excluded from DBA unless careful analysis and quantitative assessment of their potential contribution to the overall risk indicate it

Failures in supporting systems impeding systems necessary for N.O. → PIEs, if they require **actuation of reactor protection systems** or **safety systems**

Examples of N.O. regimes

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

b) **Power operation**

    a) Including full power and low power operation

c) **Changes in reactor power**

    a) Including load follow modes and return to full power after an extended period at low power, if applicable

d) **Reactor shutdown from power operation**

e) **Hot shutdown**

f) **Cooling down process**

g) **Cold shutdown**

h) **Refuelling during shutdown or during normal operation at power**

i) **Shutdown in a refuelling mode**

    a) Or maintenance conditions that open the reactor coolant or containment boundary

j) **Normal operation modes of the spent fuel pool**

k) **Storage and handling of fresh fuel**

Indicative list of PIEs leading to AOOs

a) **Increase or decrease in the heat removal from the reactor coolant system**
b) **Increase or decrease in the flow rate of the reactor coolant system**
c) **Anomalies in reactivity and power distribution in the reactor core, or anomalies in reactivity in fresh or spent fuel in storage**
d) **Increase or decrease in the reactor coolant inventory**
e) **Leaks in the reactor coolant system with potential by-pass of the containment**
f) **Leaks outside the containment**
g) **Reduction in or loss of cooling of the fuel in the spent fuel storage pool**
h) **Loss of cooling of fuel during on-power refuelling**
   a) Pressurized heavy water reactor
i) **Release of radioactive material from a subsystem or component**
   a) Typically from treatment or storage systems for radioactive waste

Indicative list of PIEs leading to DBAs

a) **Increase in heat removal from the reactor** (e.g. Steam line breaks)

b) **Decrease in heat removal from the reactor** (e.g. Loss of feedwater)

c) **Decrease in flow rate of the reactor coolant system** (e.g. Seizure or shaft break of main coolant pump; trip of all coolant pumps

d) **Anomalies in reactivity and power distribution** (e.g. Uncontrolled withdrawal of control rod (or control rod bank); ejection of control rod (pressurized water reactor); rod drop accident (boiling water reactor); boron dilution due to the startup of an inactive loop (pressurized water reactor)

e) **Decrease in reactor coolant inventory** (e.g. A spectrum of possible loss of coolant accidents; inadvertent opening of the primary system relief valves; leaks of primary coolant into the secondary system)

f) **Reduction in or loss of cooling of the fuel in the spent fuel storage pools** (e.g. Break of piping connected to the water of the pool)

g) **Loss of cooling of fuel during on-power refuelling** (e.g. Pressurized heavy water reactor)

h) **Loss of moderator circulation or decrease in or loss of moderator heat sink** (e.g. Pressurized heavy water reactor)

i) **Release of radioactive material due to leak in reactor coolant system** with potential containment by-pass, or from a subsystem or component (e.g. Overheating of or damage to used fuel in transit or storage; break in a gaseous or liquid waste treatment system)

j) **End-shield cooling failure** (e.g. Pressurized heavy water reactor)

List of DECs: Preliminary Reference

Very low frequency initiating events typically not considered DBAs

- Multiple steam generator tube ruptures
- Main steam line break and induced steam generator tube ruptures

AOOs/DBAs combined with multiple failures in safety system

- Anticipated transient without scram
- Station blackout
- Total loss of feed water
- ...

SSG-2 (Rev. 1), § 3.41

PIEs involving multiple failures

- Total loss of the component cooling water system or of the essential service water system
- Loss of the residual heat removal system during cold shutdown or refuelling
- …

IAEA
International Atomic Energy Agency
Atoms for Peace and Development

How to contact us

Safety.Standards@iaea.org

IAEA
International Atomic Energy Agency
Atoms for Peace and Development

Thank you!