The Abdus Salam
International Centre for Theoretical Physics

United Nations
Educational, Scientific and
Cultural Organization

IAEA
International Atomic Energy Agency

2257-20

Joint ICTP-IAEA School of Nuclear Energy Management

8 - 26 August 2011

Safety Assessment

Javier Yllera
IAEA, Vienna
Austria

Safety Assessment of Nuclear Installations

IAEA/ICPT School of Nuclear Energy Management

Javier Yllera
Safety Assessment Section
Acting Section Head
Nuclear Safety and Security Department

16 August 2011

Contents

- Fundations of Nuclear Safety
- Need and Requirements for Safety Assessment
- The Safety Assessment Process
- Safety Analysis Methods: Deterministic and Probabilistic safetyanalysis

Foundations of Nuclear Safety

- **THE FUNDAMENTAL SAFETY OBJECTIVE:**
  - To protect people and the environment from harmful effects of ionizing radiation.
  - This objective has to be achieved for all stages in their lifetime without unduly limiting the application of technology.
- **THREE FUNDAMENTAL SAFETY FUNCTIONS**
  - Control of reactivity,
  - Removal of heat from the core,
  - Confinement of radioactive material
- **DEFENCE IN DEPTH**
  - Effective strategy in compensating for human errors and equipment failures
  - Based on several levels of protection and physical barriers for preventing the release of radioactive material to the environment

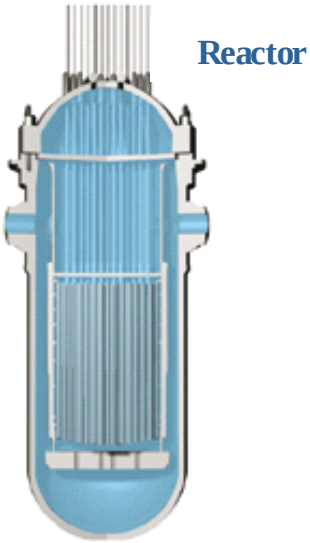
Need for Safety Assessment

- The **fundamental safety objective** is stated in the **Fundamental Safety Principles**
- The achievement of this objective is leads, inter alia, to the **requirement for a safety assessment** to be carried out:
  - **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 and whether the basic safety objectives and safety criteria established by the designer, the operating organization and the regulatory body, in compliance with the **requirements** for protection and safety as established in the International Basic Safety Standards for Protection against Ionizing Radiation and for the Safety of Radiation Sources, have been fulfilled.
  - 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.
  - A **graded approach** shall be used in determining the scope and level of detail of the safety assessment carried out consistent with the magnitude of the possible radiation risks arising from the facility or activity.

Fundamental Safety Functions (NPP)

Controlling reactor power

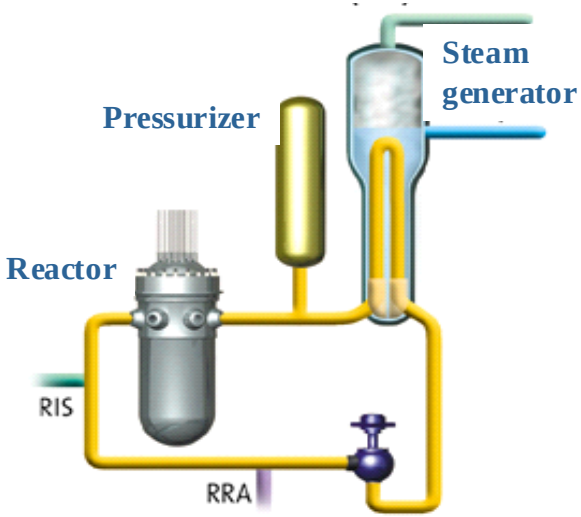
- Control rods
- Boron concentration



Cooling the core

Heat removal by:

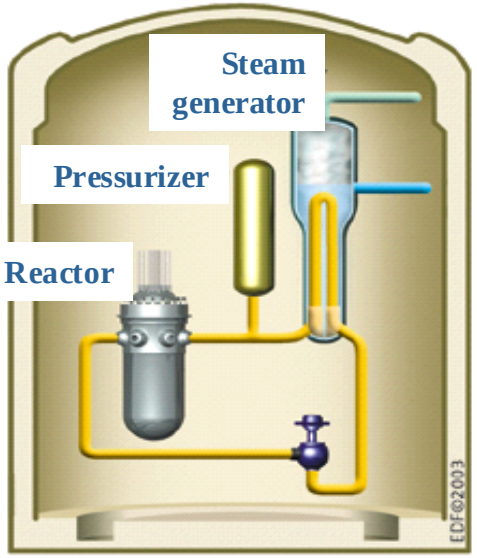
- Steam generators in operation
- Residual heat removal
- Safety injection



Confining radioactivity

By barriers like:

- Fuel and cladding
- Primary cooling system
- Containment building



Safety Functions

Controlling the Reactivity	Cooling the Fuel	Confining Radioactive Material
SF(1) to prevent unacceptability reactivity transient	SF(4) to maintain sufficient RCS inventory for non-LOCA accident	SF(10) to maintain acceptable cladding integrity in the core
SF(2) to maintain reactor in safe shutdown condition	SF(5) to maintain sufficient RCS inventory for all DB events	SF(11) to maintain RCS integrity
SF(3) to shutdown reactor as necessary	SF(6) to remove heat from the core under LOCA conditions	SF(12) to limit Ra-releases from the containment under accident condition
SF(18) to maintain subcriticality of fuel outside RCS	SF(7) to remove heat from the core under non-LOCA conditions	SF(13) to limit Ra-discharges from sources outside the containment
	SF(8) to transfer heat from safety systems to ultimate heat sink	SF(14) to limit Ra-discharges during operational states
SF(9) to ensure necessary service as a support for safety systems	SF(17) to remove decay heat from fuel outside the RCS	SF(16) to maintain control of Ra-releases from the fuel outside the RCS
SF(15) to maintain control Of environmental conditions within the plate	SF(19) to prevent failure of a system with potential Impairment of a SF	SF(20) to maintain integrity of the containment
		SF(21) to limit effects of Ra-releases on the public and environment

IAEA
International Atomic Energy Agency

Defence in Depth

A hierarchical deployment of different levels of equipment and procedures in order to maintain the effectiveness of physical barriers placed between a radiation source or radioactive materials and workers, members of the public or the environment, in operational states and, for some barriers, in accident conditions.

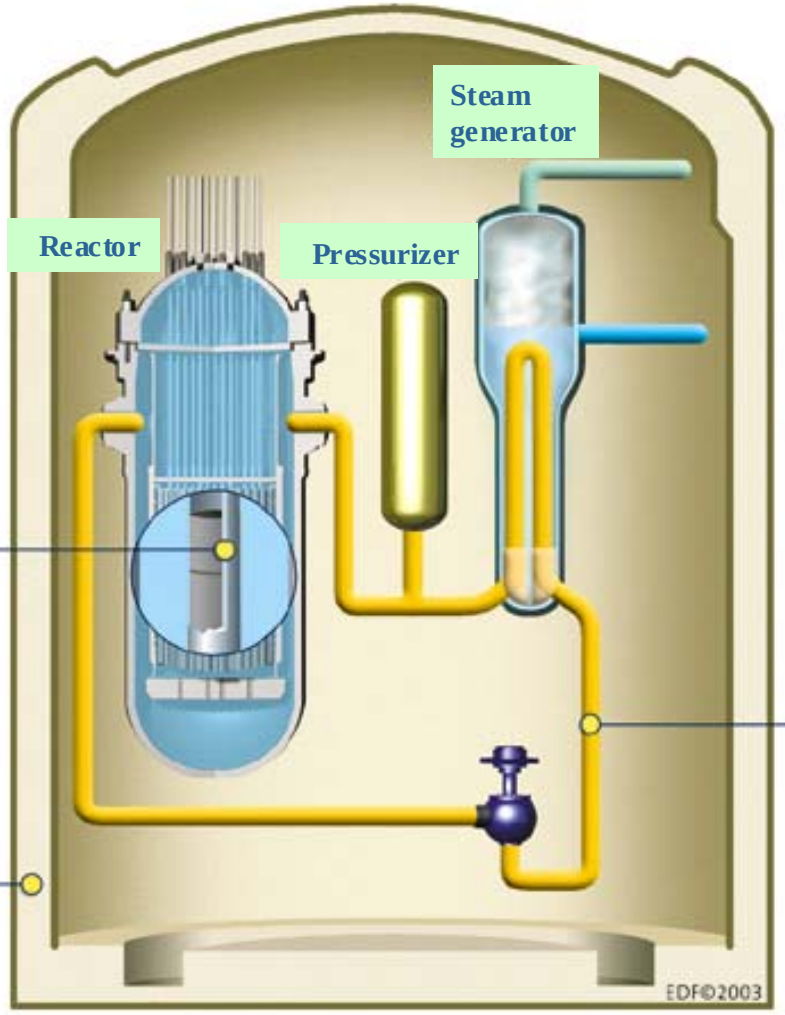
The objectives of defence in depth are:

- to compensate for potential human and component failures;
- to maintain the effectiveness of the barriers by averting damage to the facility and to the barriers themselves; and
- to protect the public and the environment from harm in the event that these barriers are not fully effective.

Levels of defence in depth (From INSAG-10)

Levels of defence	Objective	Essential means
Level 1	Prevention of abnormal operation and failures	Conservative design and high quality in construction and operation
Level 2	Control of abnormal operation and detection of failures	Control, limiting and protection systems and other surveillance features
Level 3	Control of accidents within the design basis	Engineered safety features and accident procedures
Level 4	Control of severe plant conditions including prevention of accident progression and mitigation of the consequences of severe accidents	Complementary measures and accident management
Level 5	Mitigation of radiological consequences of significant releases of radioactive materials	Off-site emergency response

Safety features: multiple barriers



First barrier

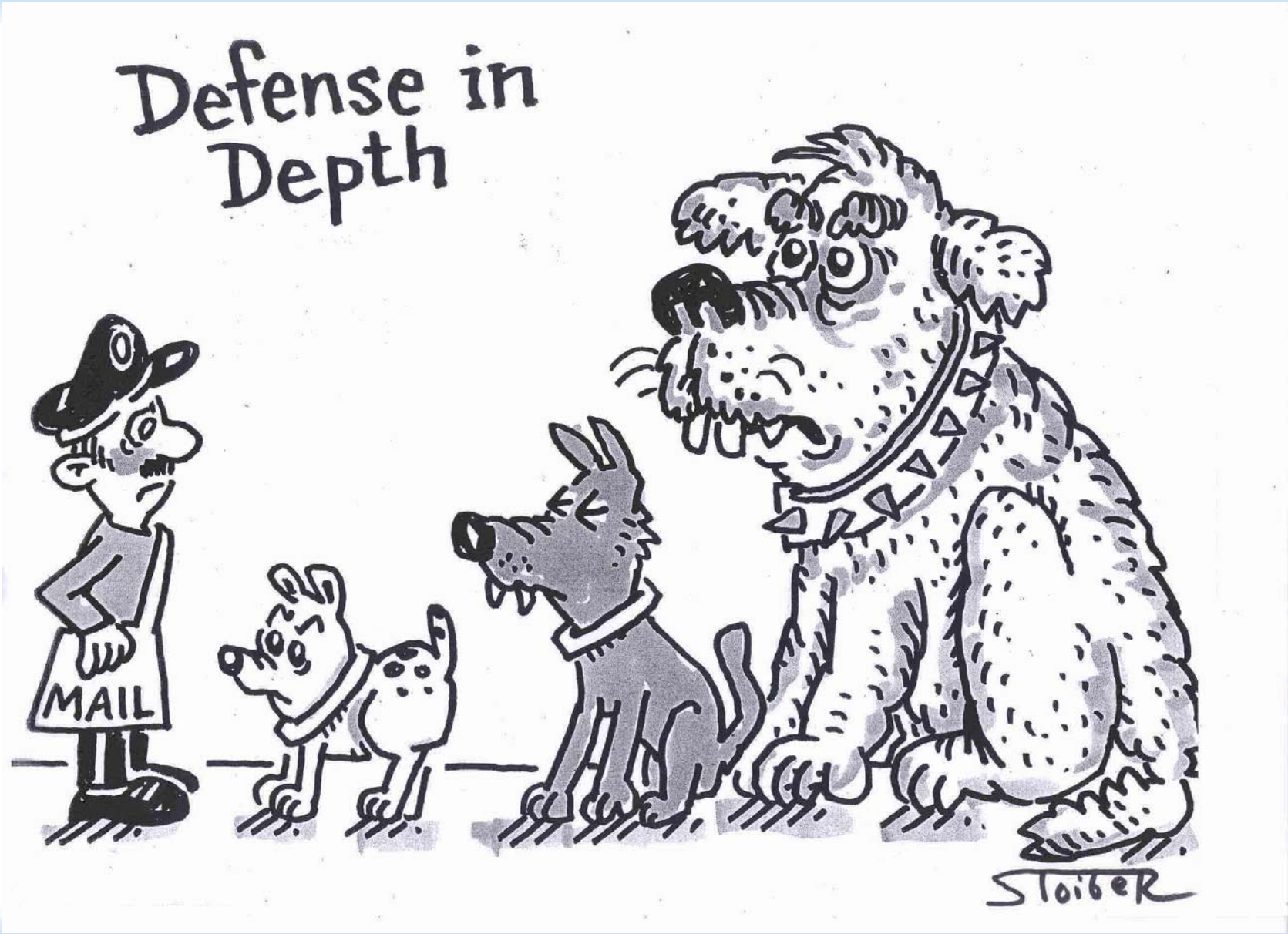
Fuel cladding

Second barrier

primary system

Third barrier

Containment building


Defense in Depth
MAIL
STOIBER

Requirements for Safety Assessment

- It has to be determined in the safety assessment whether **adequate defence in depth** has been provided, as appropriate, through a combination of several layers of protection (i.e. physical barriers, systems to protect the barriers, and administrative procedures) that would have to fail or to be bypassed before there could be any consequences for people or the environment.

- The safety assessment has to include a **safety analysis**, which consists of a set of different quantitative analyses for evaluating and assessing challenges to safety in various operational states, anticipated operational occurrences and accident conditions, by means of deterministic and also probabilistic methods. The scope and level of detail of the safety analysis are determined by use of a graded approach. Determination of the scope and level of detail of the safety analysis is an integral part of the safety assessment.

IAEA Safety Standards

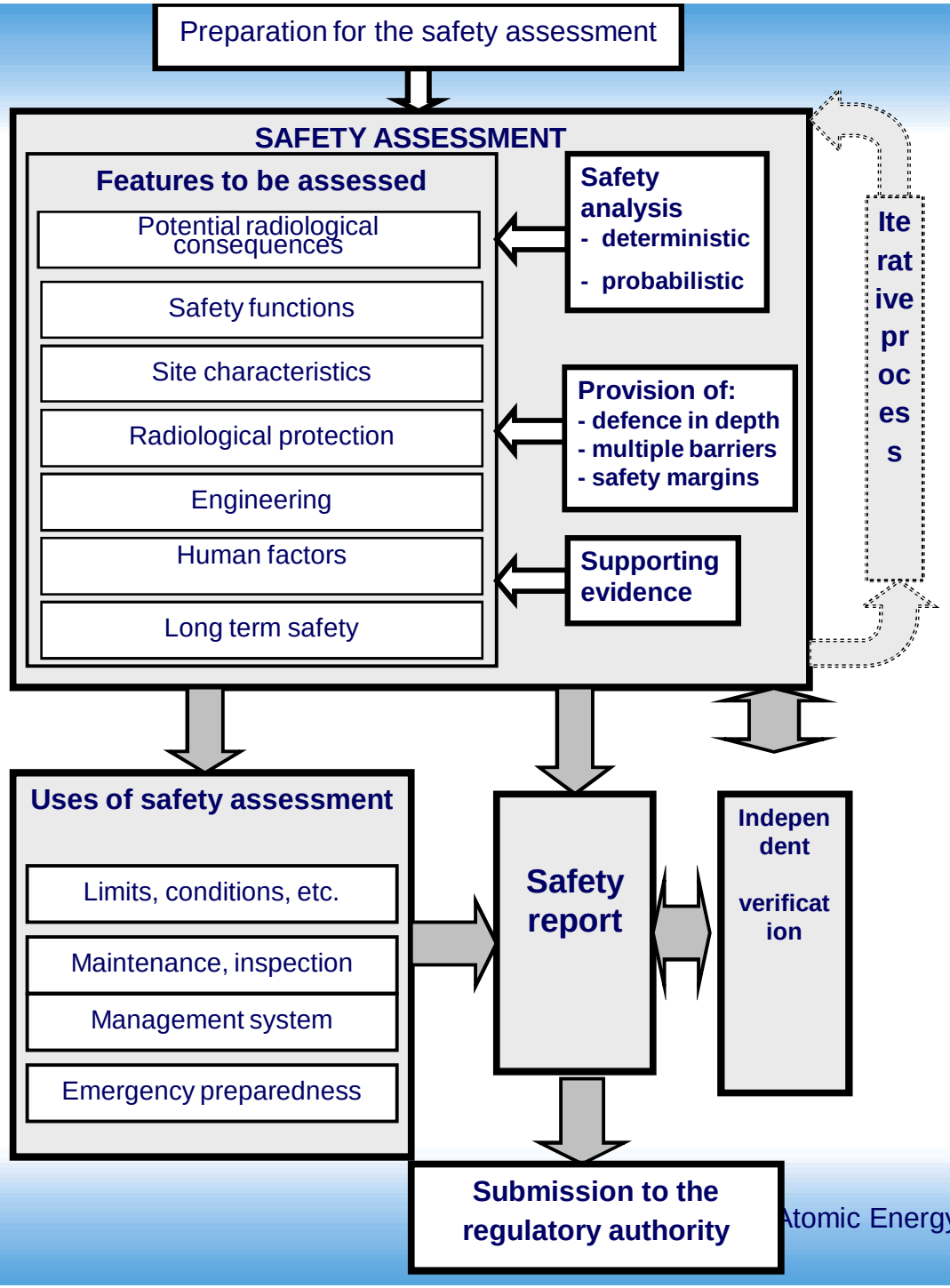
for protecting people and the environment

Safety Assessment for Facilities and Activities

General Safety Requirements Part 4

No. GSR Part 4

IAEA International Atomic Energy Agency



REQUIREMENTS FOR A SAFETY ASSESSMENT

(1 of 12)

OVERALL REQUIREMENTS

- Safety assessment shall be carried out for all applications of technology that give rise to radiation risks (facilities and activities).
- The responsibility for carrying out the safety assessment shall be with the person or organization authorized (licensed) to operate the facility or carry out the activity.
- The safety assessment shall have the primary purpose of determining whether an adequate level of safety has been achieved for a facility or activity and whether the basic safety objectives and safety criteria established by the designers, the operator and the regulatory authority have been complied with.
- The safety assessment shall include an assessment of the radiological protection provisions to determine whether the radiological risks are being controlled within specified limits and whether they have been reduced to a level that is as low as reasonably achievable.
- The safety assessment shall address all the radiation risks that arise from normal operation and from abnormal and accident conditions.
- The safety assessment shall be carried out as early as possible in the lifetime of the facility or activity and shall be updated as necessary as the facility or activity passes through the stages of its lifetime.

REQUIREMENTS FOR A SAFETY ASSESSMENT

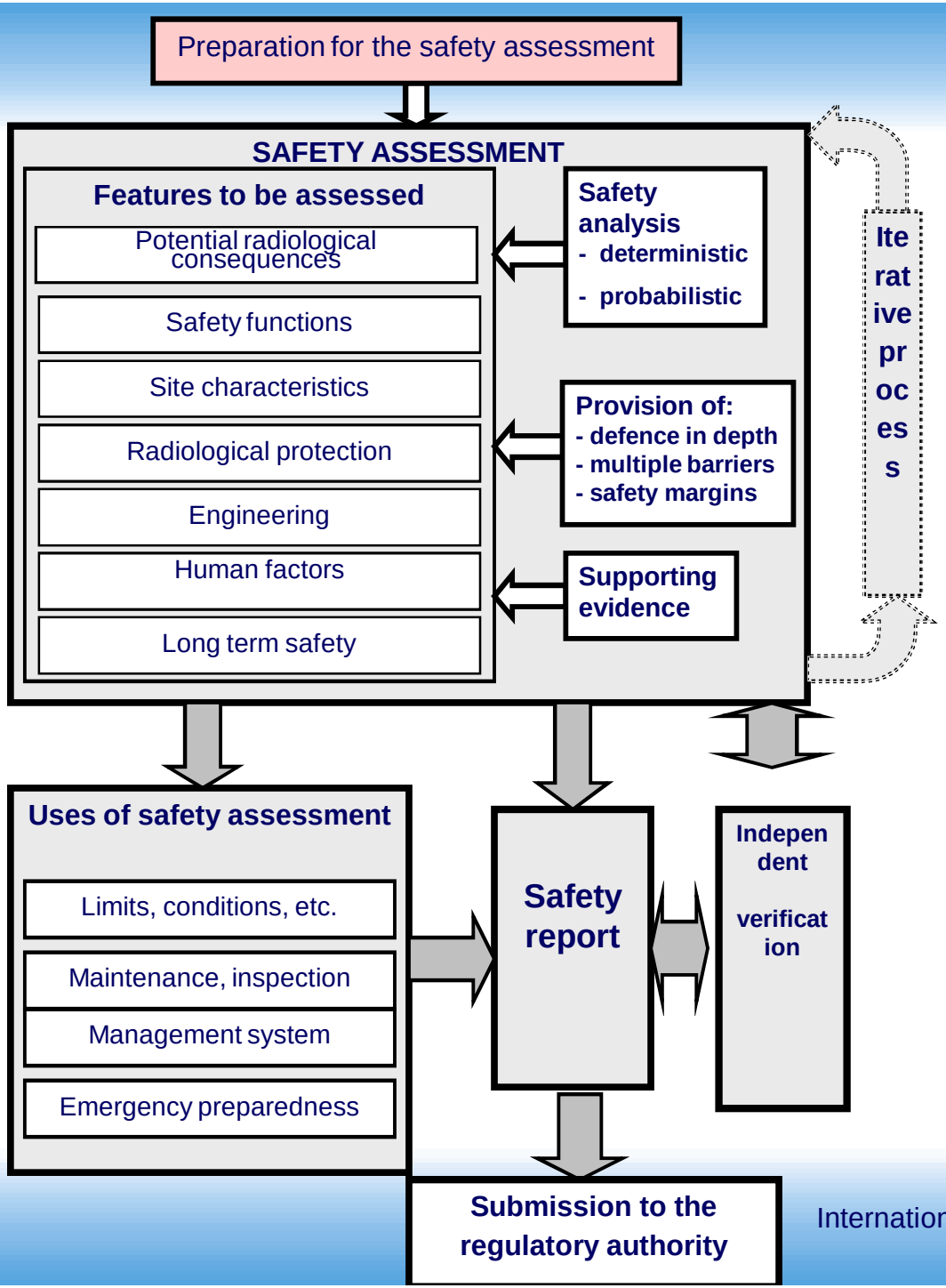
(2 of 12)

- The updating of the safety assessment shall also take account of operating experience including data relating to abnormal and accident conditions and accident precursors both from the facility or activity itself and from other similar facilities or activities.
- For facilities and activities that continue over long periods of time, the safety assessment shall be reviewed and repeated as necessary.
- The safety assessment shall identify all the safety measures necessary to control the potential radiological consequences. It shall determine whether the design and engineered safety features fulfill the safety functions required of them. It shall also determine whether appropriate measures have been taken to prevent abnormal or and accident conditions and whether the radiological consequences would be mitigated should they occur.
- The safety assessment shall address the radiation risks to all individuals and population groups.
- The safety assessment shall address the radiation risks now and in the future (i.e. waste).
- The safety assessment shall determine whether adequate defence in depth has been provided through a combination of several layers of protection, physical barriers, systems to protect the barriers and administrative procedures, which would have to be breached before harm could be caused to people or the environment.

REQUIREMENTS FOR A SAFETY ASSESSMENT

(3 of 12)

- In most cases, the safety assessment includes a **safety analysis**, which consists of a set of different analyses that quantitatively evaluates and assesses challenges to safety under various operational, abnormal and accident conditions, using **deterministic and probabilistic** methods as appropriate.
- The computer codes that have been used to carry out the safety analysis shall be verified and validated and this will form part of the supporting evidence presented in the safety report. In the management system, the operator and the regulatory authority shall seek improvements to the tools and data that are used.
- The results of the safety assessment shall be used to identify appropriate safety related improvements to the design and operation of the facility or activity. They allow the assessment of the safety significance of unresolved shortcomings or of planned modifications and to determine their priority. They are used to provide the basis for continued operation.

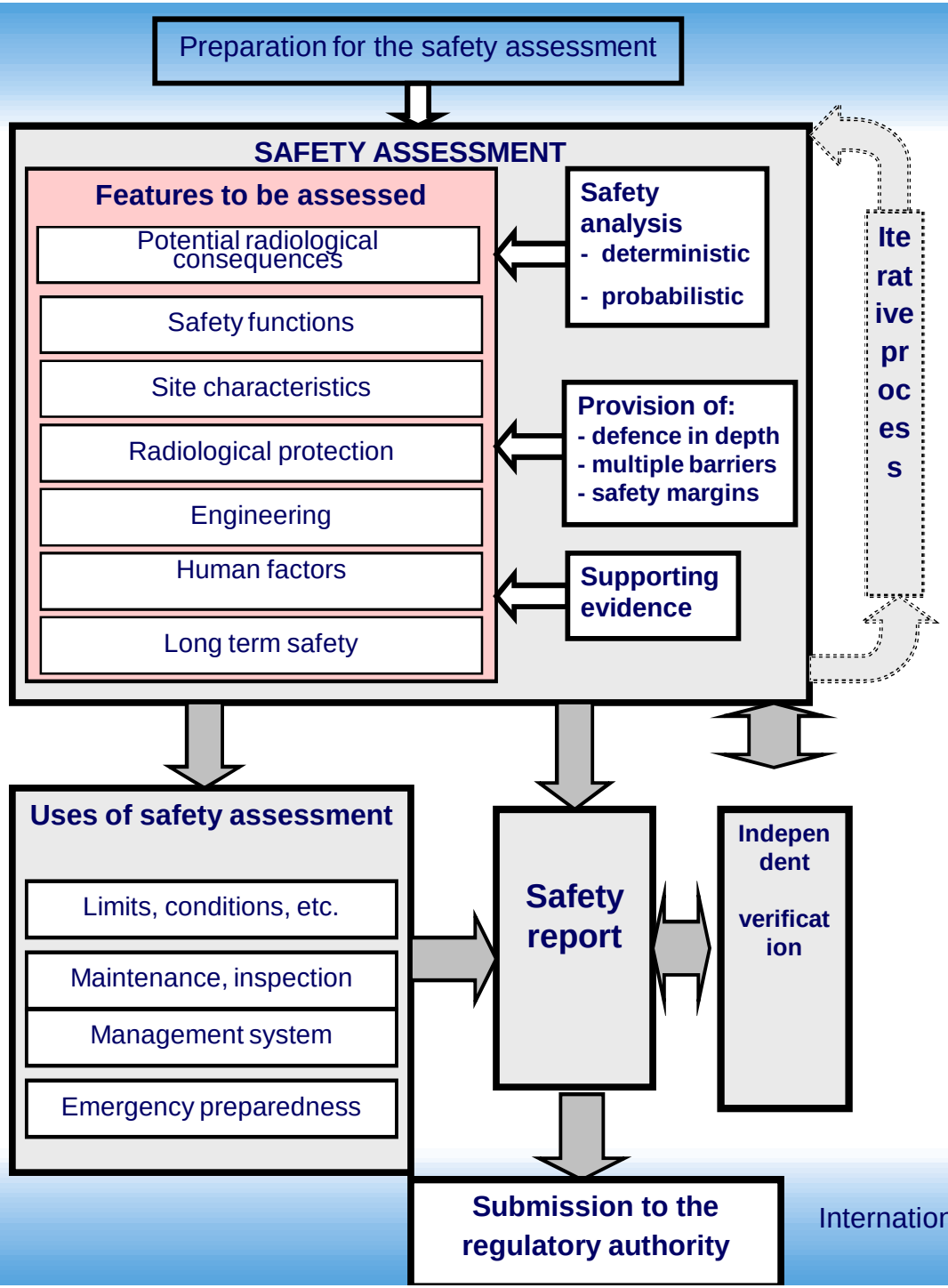

Preparation for the safety assessment
SAFETY ASSESSMENT
Features to be assessed
Potential radiological consequences
Safety functions
Site characteristics
Radiological protection
Engineering
Human factors
Long term safety
Safety analysis
- deterministic
- probabilistic
Provision of:
- defence in depth
- multiple barriers
- safety margins
Supporting evidence
Iterative process
Uses of safety assessment
Limits, conditions, etc.
Maintenance, inspection
Management system
Emergency preparedness
Safety report
Independent verification
Submission to the regulatory authority

REQUIREMENTS FOR A SAFETY ASSESSMENT

(4 of 12)

Preparation for the Safety Assessment

- The first stage in carrying out the safety assessment is to make the necessary preparations. This shall include ensuring that:
  - There are sufficient skilled and expert people available to carry out the work;
  - The required background material is available. This includes all the information relating to the design and operation of the facility or activity;
  - The necessary tools for carrying out the safety assessment are available. This includes the computer codes required for carrying out the safety analysis; and
  - The criteria to be used for judging whether the safety of the facility or activity is adequate have been defined.


Preparation for the safety assessment
SAFETY ASSESSMENT
Features to be assessed
Potential radiological consequences
Safety functions
Site characteristics
Radiological protection
Engineering
Human factors
Long term safety
Safety analysis
- deterministic
- probabilistic
Provision of:
- defence in depth
- multiple barriers
- safety margins
Supporting evidence
Iterative process
Uses of safety assessment
Limits, conditions, etc.
Maintenance, inspection
Management system
Emergency preparedness
Safety report
Independent verification
Submission to the regulatory authority

REQUIREMENTS FOR A SAFETY ASSESSMENT

(5 of 12)

Identification of the Potential Radiological Consequences

- The potential radiological consequences from the facility or activity shall be identified and assessed. This includes the radiation exposure to people and the release of radioactive material to the environment following the occurrence of abnormal or accident conditions that lead to a loss of control.

Assessment of Safety Functions

- All the safety functions associated with a facility or activity shall be identified and assessed. This shall include the safety functions associated with the engineered structures, systems and components, any natural barriers as applicable, and any human actions required to ensure the safety of the facility or activity.
- The assessment of the safety functions shall determine whether they will be carried out with an adequate level of reliability, there is no vulnerability to a single failure or to a common cause failure for engineered equipment, and any structure, system, component or barrier provided to carry out a safety function has an adequate level of redundancy, diversity, separation, segregation, equipment qualification, etc. as appropriate.

REQUIREMENTS FOR A SAFETY ASSESSMENT

(6 of 12)

Assessment of Site Characteristics

- An assessment of the site characteristics related to the safety of the facility or activity shall be carried out and include:
  - The physical and chemical characteristics that will affect the dispersion or migration of radioactive materials released in normal operation or due to an incident or accident;
  - The identification of the natural and man-made hazards of the area that have the potential to affect the safety of any facility or activity; and
  - The site demographic characteristics in regard to any siting policy of the Member State and the need to determine an emergency plan.
- The scope and level of detail of the site assessment shall be consistent with the potential radiological consequences from the facility or activity, the type of facility or activity to be carried out and the purpose of the assessment (i.e. whether it is to determine whether a new site is suitable for a facility or activity, the safety evaluation of an existing site, the long term assessment of a site for waste disposal, etc.) and will be reviewed periodically during the lifetime of the facility or activity.

REQUIREMENTS FOR A SAFETY ASSESSMENT

(7 of 12)

Assessment of the Radiological Protection Provisions

- The safety assessment shall determine whether adequate measures are in place for a facility or activity to control the occupational radiation exposure of people – as required by the Fundamental Safety Objective.
- The safety assessment shall determine whether adequate measures are in place to control the occupational radiation exposure within any relevant dose limit and that the protection is optimized such that the magnitude of individual doses, the number of people exposed and the likelihood of incurring exposures have all been kept as low as reasonably achievable, economic and social factors being taken into account.
- The safety assessment of the radiological protection provisions shall address normal operation of the facility or activity, and abnormal and accident conditions.

REQUIREMENTS FOR A SAFETY ASSESSMENT

(8 of 12)

Assessment of the Engineering

The safety assessment shall:

- determine whether, to the extent possible, a facility or activity uses structures, systems, components and procedures of robust and proven design with previous successful application. Relevant operational experience, including results of root cause analysis of abnormal and accident conditions where appropriate, shall be taken into account;
- identify the design principles that have been applied to the facility and determine whether these requirements have been met;
- determine whether, where appropriate, a suitable safety classification scheme has been formulated and applied to the structures, systems and components
  - Importance to safety, the severity of the consequences of their failure
  - Identification of the appropriate industry codes and standards and the regulatory requirements that need to be applied in the design, manufacturing, construction and inspection of the engineered features or to the development of procedures and in their management system.

REQUIREMENTS FOR A SAFETY ASSESSMENT

(9 of 12)

Assessment of the Engineering (continued)

The safety assessment shall:

- address the external hazards that could arise for a facility or activity, and determine whether an adequate level of protection is provided (natural external events and man-made events);
- address the internal hazards that could arise for a facility and determine whether the structures, systems and components are able to perform their function under the loads induced by the accidents that have been taken into account explicitly in the design of the facility;
- determine whether the materials used are suitable for their purpose with regard to the standards specified in the design and the operational conditions which arise during normal operation and following abnormal or accident conditions that have been taken into account explicitly in the design of the facility or activity.
- address whether preference has been given to a fail-safe design, or, if this is not possible, whether a means of detecting the failures that have occurred has been incorporated wherever possible;

REQUIREMENTS FOR A SAFETY ASSESSMENT

(10 of 12)

Assessment of the Engineering (continued)

The safety assessment shall:

- determine whether any time related aspects such as ageing, wear-out or life limiting factors, such as cumulative fatigue, embrittlement, corrosion, chemical decomposition and radiation-induced damage, have been adequately addressed;
- determine whether the equipment important to safety has been qualified so that it is able to perform its safety function in the conditions that it would experience during normal operation and following the abnormal and accident conditions that have been taken into account in the design;
- identify the provisions made and the procedures defined for the decommissioning the nuclear facility and the closure of a repository for the disposal of radioactive waste, and determine whether they are adequate from a safety point of view;
- determine whether compliance with the safety requirements has been demonstrated by an appropriate programme of research, analysis and testing complemented by a programme of monitoring during operation to account for operating experience feedback, and the results of safety analysis and safety research.

REQUIREMENTS FOR A SAFETY ASSESSMENT

(11 of 12)

Assessment of Human Factors

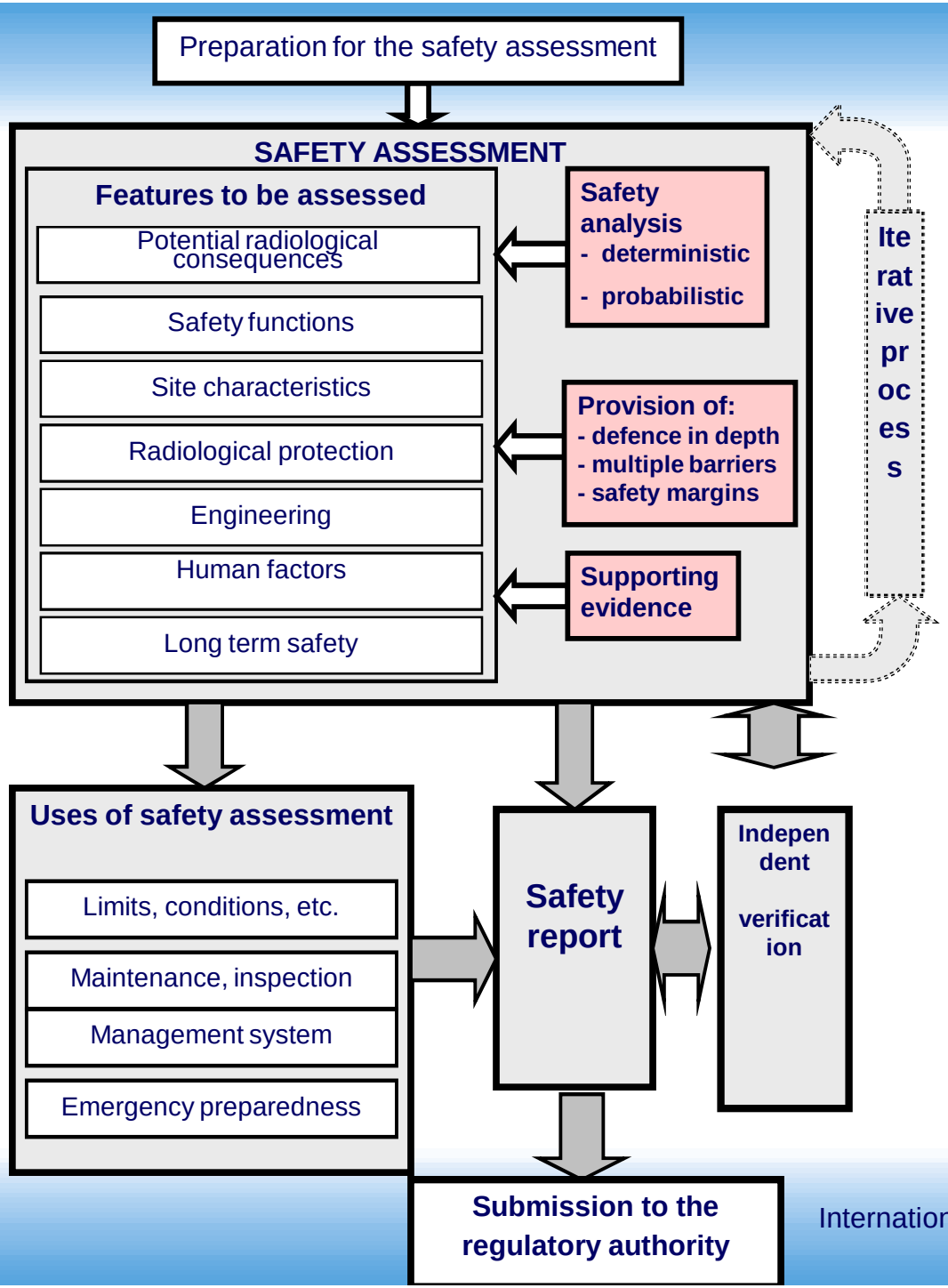
- To the extent that safety cannot be achieved by inherently safe design and engineered provisions, the safety assessment shall identify the procedures and measures that are necessary for all normal operational activities, in particular those required to implement the identified operational limits and conditions, and those required in response to abnormal and accident conditions.
- The safety assessment shall determine whether the requirements specified for personnel competences, associated training and minimum staffing levels for maintaining safety are adequate.
- The safety assessment shall determine whether the design and operation of any facility and the procedures for any activities have addressed the requirements to comply with human factors, including those related to the ergonomic design of all the areas, man-machine interfaces where human activities are carried out, and future decommissioning and closure activities.
- For facilities and activities already in existence, the safety assessments shall include aspects of safety culture where appropriate.

REQUIREMENTS FOR A SAFETY ASSESSMENT

(12 of 12)

Assessment of Long Term Safety (post-closure phase of a repository for the disposal of significant quantities of radioactive material)

- In the case of a repository for the disposal of significant quantities of radioactive waste, the anticipated and potential radiological effects on human health and the environment shall be considered for the post-closure phase. Potential radiological impacts following closure of the repository may arise from gradual processes, such as the degradation of barriers, and from discrete events that could affect waste isolation such as inadvertent human intrusion. The safety assessment shall address all aspects relevant for long term safety in order to provide a basis for giving reasonable assurance that the repository will meet the design objectives and safety requirements.
- In view of the uncertainties inherent in predicting future events, according to the Safety Standard for the geological disposal of radioactive waste, reasonable assurance of compliance with the safety requirements related to long term hazards is most likely to be achieved by the use of multiple lines of reasoning. This is achieved by supplementing the quantitative estimates of repository performance with other qualitative evidence that the repository will provide isolation of the wastes as designed.


Preparation for the safety assessment
SAFETY ASSESSMENT
Features to be assessed
Potential radiological consequences
Safety functions
Site characteristics
Radiological protection
Engineering
Human factors
Long term safety
Safety analysis
- deterministic
- probabilistic
Provision of:
- defence in depth
- multiple barriers
- safety margins
Supporting evidence
Iterative process
Uses of safety assessment
Limits, conditions, etc.
Maintenance, inspection
Management system
Emergency preparedness
Safety report
Independent verification
Submission to the regulatory authority

DEFENCE IN DEPTH AND SAFETY MARGINS

(1 of 2)

- The assessment of defence in depth shall determine whether adequate provisions have been made at each of the levels of defence in order to:
  - Prevent deviations from normal operation and, in the case of a repository, its desirable long-term evolution;
  - Detect and intercept deviations from normal operation and the desirable long-term evolution should they occur;
  - Control accidents within the limits inherent in the design;
  - Identify accident management measures to control severe accident (beyond design basis) conditions; and
  - Mitigate the radiological consequences of potential releases.
- The safety assessment shall identify the necessary layers of protection including physical barriers to confine the radioactive material at specific locations and the need for supporting administrative controls.

DEFENCE IN DEPTH AND SAFETY MARGINS

(2 of 2)

- In order to determine whether defence in depth has been adequately implemented the safety assessment shall determine whether:
  - The highest priority has been given to: reducing the number of challenges to the integrity of layers of protection and physical barriers; preventing the failure or bypass of a barriers; preventing failure of one barrier leading to the failure of another one; and preventing significant releases if failure of the barriers should occur;
  - The layers of protection and physical barriers are independent of each other as much as possible;
  - Special attention has been given to internal and external hazards that have the potential to adversely affect more than one barrier at once or to cause simultaneous failures of safety systems; and
  - Specific measures have been implemented to ensure the effectiveness of the required levels of defence.
- The safety assessment shall determine whether there are adequate **safety margins** in the design and operation of the facility or activity so that there is a wide margin to failure of any structures, systems or components for any of the abnormal or accident conditions that could occur.

SAFETY ANALYSIS

(1 of 4)

Scope of Safety Analysis

The safety analysis shall:

- assess the performance of a facility or activity in all operational states and, as necessary, in the post-operational phase and shall determine whether there is compliance with the safety requirements;
- address both the consequences arising from all normal operational conditions as well as the probabilities and consequences associated with all identified abnormal or accident conditions;
- identify the abnormal and accident conditions that challenge nuclear safety (all internal and external events and processes that may impact on physical barriers to confine the radioactive material or otherwise give rise to radiological risks;
- address the abnormal and accident conditions that arise during operation of the facility or activity. The aim shall be to determine the cause of the abnormal or accident conditions, its significance and determine the effectiveness of the proposed corrective action.

SAFETY ANALYSIS

(2 of 4)

Approaches to Safety Analysis

- The safety analysis shall incorporate deterministic and probabilistic approaches, as appropriate. Both can provide input into an integrated decision making process.
- The aim of the deterministic approach is to define and apply a set of conservative rules and requirements for the design and operation of a facility or activity. If these rules and requirements are met, they are expected to provide a high degree of confidence that the level of risk to workers and members of the public from the facility or activity will be acceptably low.
- Probabilistic safety analysis determine all significant contributors to the radiological risk from a facility or activity and to evaluate the extent to which the overall design is well balanced and meets probabilistic safety criteria if been defined. The probabilistic approach uses realistic assumptions whenever possible and is able to quantify uncertainties explicitly.
- With increasing quality of models and data it is possible to develop more realistic deterministic analysis and to make use of probabilistic information in selecting accident scenarios. Increasing emphasis is also being given to probabilistically specifying how compliance with the deterministic safety criteria is demonstrated, e.g. by specifying confidence intervals, and how safety margins are defined.

SAFETY ANALYSIS

(3 of 4)

Criteria for Judging Safety

- Criteria for judging safety shall be defined for the safety analysis that are sufficient to meet the fundamental safety objective and the fundamental principles given in and the requirements of the designers, operator and the regulatory authority.
- In addition, detailed criteria may be developed to assist in assessing compliance with these higher level objectives, including risk criteria which relate to the likelihood of abnormal or accident conditions occurring with significant radiological consequences.

Uncertainty and Sensitivity Analysis

- There will always be uncertainties associated with safety analysis (predictions) which depend on the exact nature of the facility or activity and the complexity of the safety analysis. To the extent practicable the results of a safety analysis shall be robust, i.e. tolerant to uncertainties.
- Uncertainties in the safety analysis shall be characterized with respect to their source, nature and degree, using quantitative methods, professional judgment or both. Uncertainties which may have implications on the outcome of the safety analysis and decisions made on that basis shall be addressed in uncertainty and sensitivity analyses.

SAFETY ANALYSIS

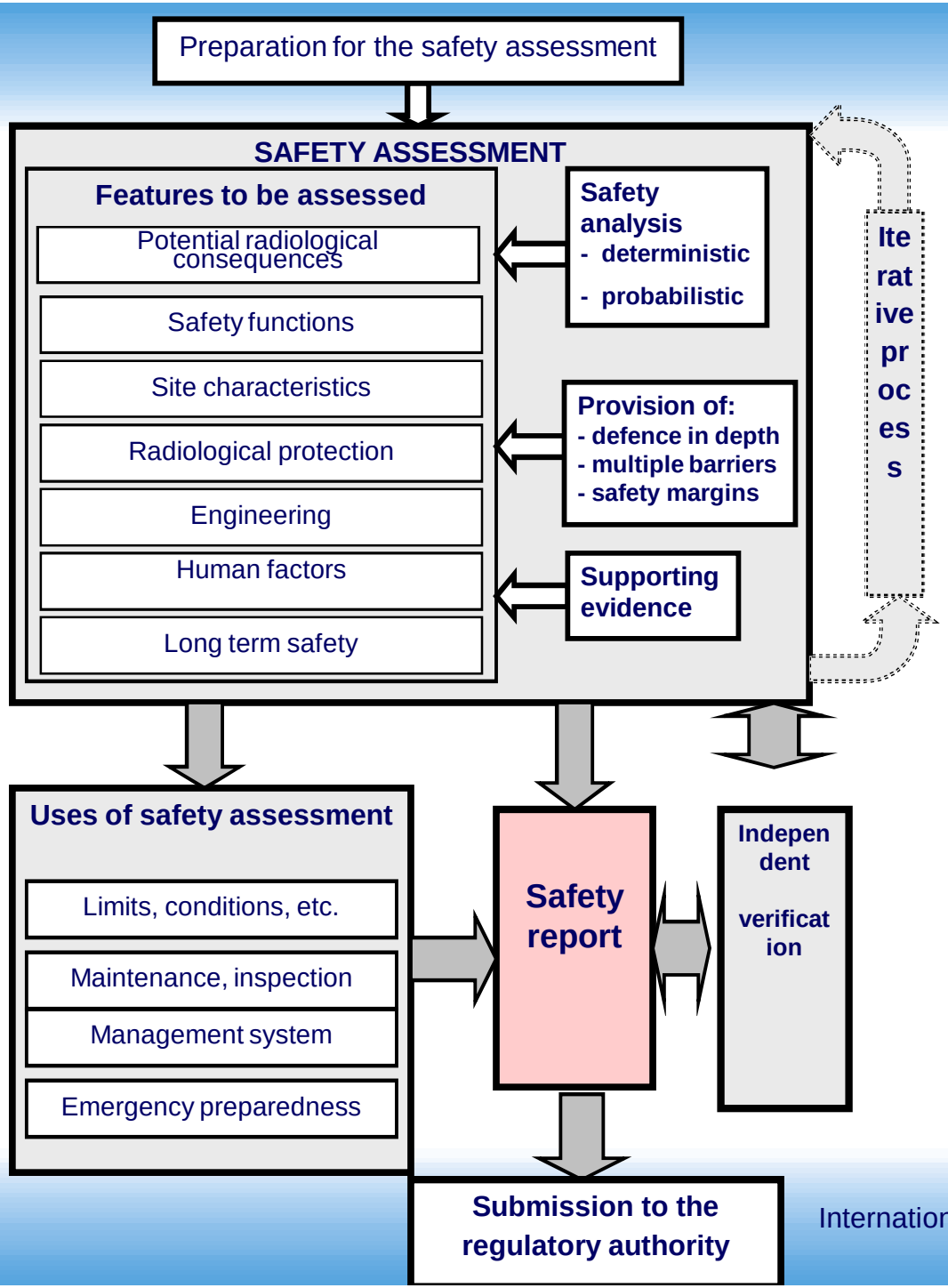
(4 of 4)

Use of Computer Codes

- The computer codes used in the safety analysis shall undergo a sufficient level of verification and validation.
  - Verification determines whether the controlling physical equations and data have been correctly translated into the computer code.
  - Validation determines whether the mathematical model is an adequate representation of the real system being modelled by comparing the predictions of the model with observations of the real system or experimental data. The validation process shall identify the uncertainties and shortcomings in the models and the underlying data basis and how these are to be taken into account in the safety analysis.

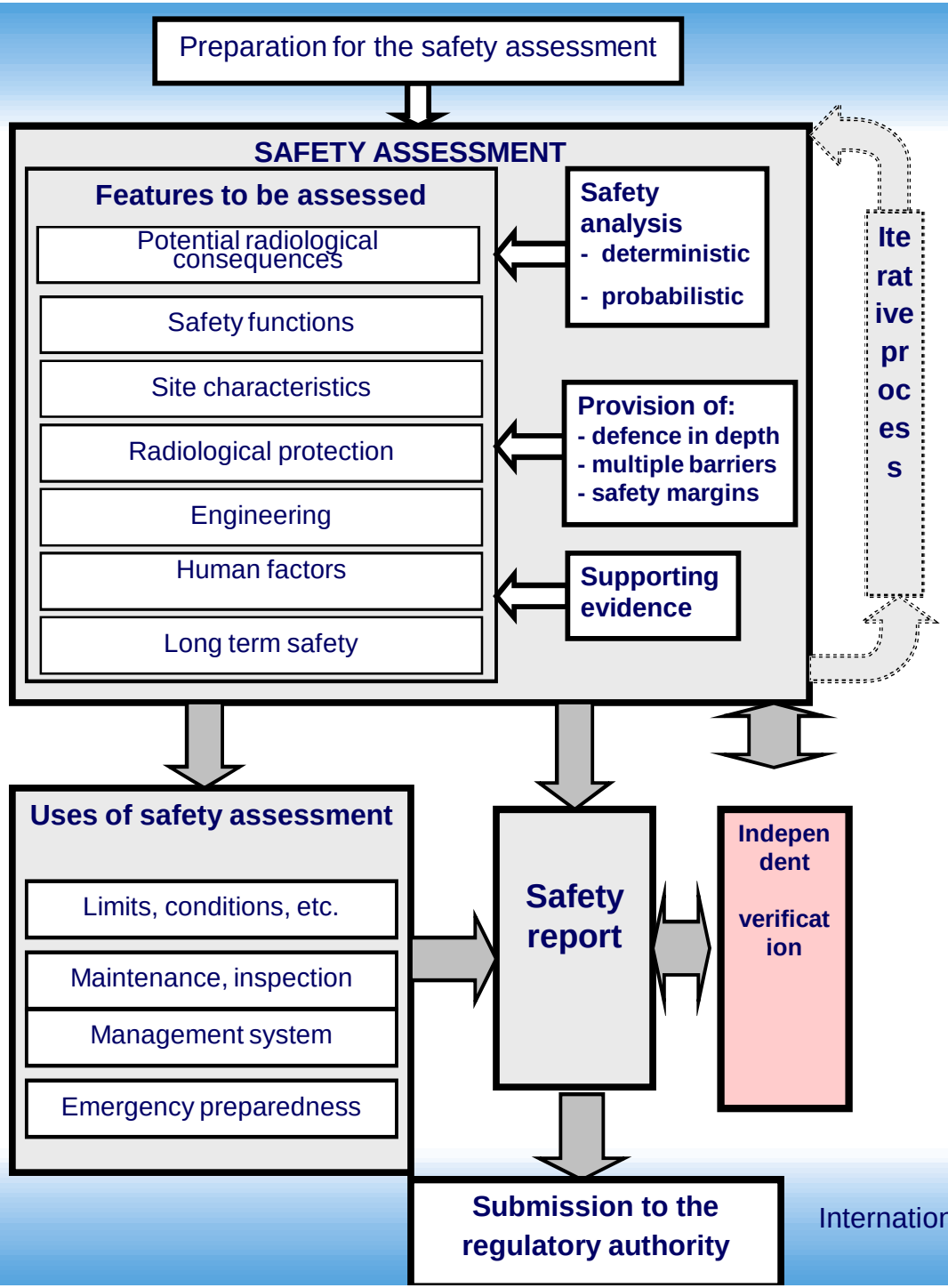
Use of Data from Operating Experience

- Operational safety performance data shall be collected and assessed, including records of incidents such as human errors, performance of safety systems, radiation doses, generation of radioactive waste and effluents. For complex facilities, the collection of data may be based on a set of safety performance indicators that have been established for the facility. Operational safety experience shall be used, as appropriate, to update the safety assessment and review management systems.


Preparation for the safety assessment
SAFETY ASSESSMENT
Features to be assessed
Potential radiological consequences
Safety functions
Site characteristics
Radiological protection
Engineering
Human factors
Long term safety
Safety analysis
- deterministic
- probabilistic
Provision of:
- defence in depth
- multiple barriers
- safety margins
Supporting evidence
Iterative process
Uses of safety assessment
Limits, conditions, etc.
Maintenance, inspection
Management system
Emergency preparedness
Safety report
Independent verification
Submission to the regulatory authority

SAFETY ASSESSMENT DOCUMENTATION

- The results and findings of the safety assessment shall be documented in the form of a **safety report** to present the assessment and the analysis that determine whether the nuclear facility or activity is in compliance with the fundamental safety principles and any other safety requirements set out in national laws and regulations.
- The quantitative and qualitative outcome of the safety assessment forms the basis of the safety report. It is supplemented by supporting evidence and reasoning for the robustness and reliability of the safety assessment and its assumptions.
- The safety analysis shall be documented with sufficient scope and detail and provide in particular:
  - A justification for the selection of events and processes addressed and for the definition of scenarios;
  - An overview and necessary details of the collection of data, the modeling and the assumptions;
  - Criteria used for the evaluation of the modeling results;
  - Results of the analysis addressing the performance of the facility or activity, incurred risks and prevailing uncertainties; and
  - Conclusions on the acceptability of the level of safety achieved and the identification of necessary improvements and additional measures.
- Safety report shall be retained until the nuclear facility has been fully decommissioned or the repository for nuclear waste has been closed.


Preparation for the safety assessment
SAFETY ASSESSMENT
Features to be assessed
Potential radiological consequences
Safety functions
Site characteristics
Radiological protection
Engineering
Human factors
Long term safety
Safety analysis
- deterministic
- probabilistic
Provision of:
- defence in depth
- multiple barriers
- safety margins
Supporting evidence
Iterative process
Uses of safety assessment
Limits, conditions, etc.
Maintenance, inspection
Management system
Emergency preparedness
Safety report
Independent verification
Submission to the regulatory authority

INDEPENDENT VERIFICATION

- **The operating organisation shall carry out an independent verification** to increase the level of confidence in the safety assessment before it is used by the operator or submitted to the regulatory authority.
- The independent verification shall be performed by individuals or a group of people that is separate from those carrying out the safety assessment. The aim shall be to determine whether the safety assessment has been carried out in a way that is consistent with the current state of the art for that type of facility or activity.
- Decisions about the scope and level of detail of the independent verification are subject to a graded approach and should reflect the level of risk, complexity and novelty of the facility or activity.
- The independent verification shall combine an overall review to determine whether the safety assessment carried out is comprehensive along with spot checks where a much more detailed review is carried out that focuses on those aspects of the safety assessment that have the highest impact on the risk from the facility or activity.
- The independent verification shall ensure that the models and data used are accurate representations of the design and operation.
- **A separate independent verification shall also be carried out by the regulatory authority** to determine whether the safety assessment meets their requirements.

GRADED APPROACH FOR SAFET ASSESSMENT

(1 of 2)

- **Resources devoted to safety have to be commensurate with the magnitude of the radiation risks** - graded approach needs to be applied in carrying out the safety assessments for the wide range of facilities and activities due to the very different levels of risk that they pose. This allows flexibility in the way that the radiation risks are assessed and controlled without unduly limiting the operation of facilities or the conduct of activities.
- A graded approach shall be used to determining the scope, extent, level of detail and the effort that needs to be devoted to the safety assessment carried out for any particular facility or activity.
- The **main factor in the application of the graded approach to the safety assessment shall be the magnitude of the radiation risks** to workers, members of the public and the environment arising from the facility or activity (releases during normal operation, the potential consequences for abnormal and accident conditions, and the possibility of very low probability events with potentially high consequences). A judgment then needs to be made on the scope, extent, level of detail and the effort that needs to be applied to any particular facility or activity.

GRADED APPROACH FOR SAFET ASSESSMENT

(2 of 2)

- The graded approach to safety assessment shall also take into account other relevant factors such as the maturity or complexity of the facility or activity.
  - The maturity relates to the use of proven practices and procedures, proven designs, data on operational performance of similar facilities or activities, uncertainties in the performance of the facility or activity, and availability of experienced manufacturers and constructors.
  - The complexity relates to the extent and difficulty of the effort required to construct a facility or implement a practice, of the number of the related processes requiring control, the extent to which radioactive materials have to be handled, the longevity of the radioactive materials, the reliability and complexity of systems and components and their accessibility for maintenance inspection, testing and repair.
- The application of the graded approach shall be reviewed as the safety assessment progresses and a better understanding is obtained of the level of risk arising from the facility or activity, and the scope, extent, level of detail and the effort applied adjusted accordingly. For example, as the safety assessment progresses, it may emerge that the likelihood of significant consequences is greater than originally considered and more effort and/or detail may be required to demonstrate compliance with the safety requirements, or vice versa.
- The graded approach shall also be applied to the requirements for updating the safety assessment.

THE MANAGEMENT, USE AND MAINTENANCE OF THE SAFET ASSESSMENT

(1 of 3)

- The safety assessment is one of the key requirements to enable the operator to manage facilities and activities safely. It is also a vital input to the safety report required to demonstrate compliance with regulatory requirements.
- The safety assessment in itself cannot achieve safety.
- Safety is only achieved if the input assumptions are valid, the derived limits and conditions are implemented and maintained and the assessment reflects the installation or activity as it actually is at any point in time.
- Safety assessments require to be updated to reflect such changes as knowledge, experience and understanding that also develop with time.
- The updating of safety assessments is also important in order to provide a baseline for the future evaluation of monitoring data and performance indicators and for radioactive waste facilities to provide an appropriate record for future site use. of safety assessments have been set out.
- The safety assessment shall be reviewed to identify the input assumptions that need to be complied with by appropriate safety management controls.

THE MANAGEMENT, USE AND MAINTENANCE OF THE SAFET ASSESSMENT

(2 of 3)

- The safety assessment shall be used to identify the limits and conditions that need to be implemented through suitable procedures and controls. These shall include means for monitoring to ensure that the limits and conditions are complied with at all times.
- The safety assessment shall be used to identify the maintenance and inspection programme that needs to be established using procedures and controls that are auditable in order to ensure that
  - Any necessary conditions are maintained; and
  - Any structures, systems and components maintain their integrity and functional capability over their required lifetime.
- The safety assessment shall be used to identify the procedures that need to be put in place for all operational activities significant to safety and for responding to abnormal and accident conditions. The safety assessment shall also be used to plan for on- and off-site accident management and emergency response.
- The safety assessment shall be used to identify the necessary competences for the staff involved with the facility or activity and this shall be used to inform their training, control and supervision.

THE MANAGEMENT, USE AND MAINTENANCE OF THE SAFET ASSESSMENT

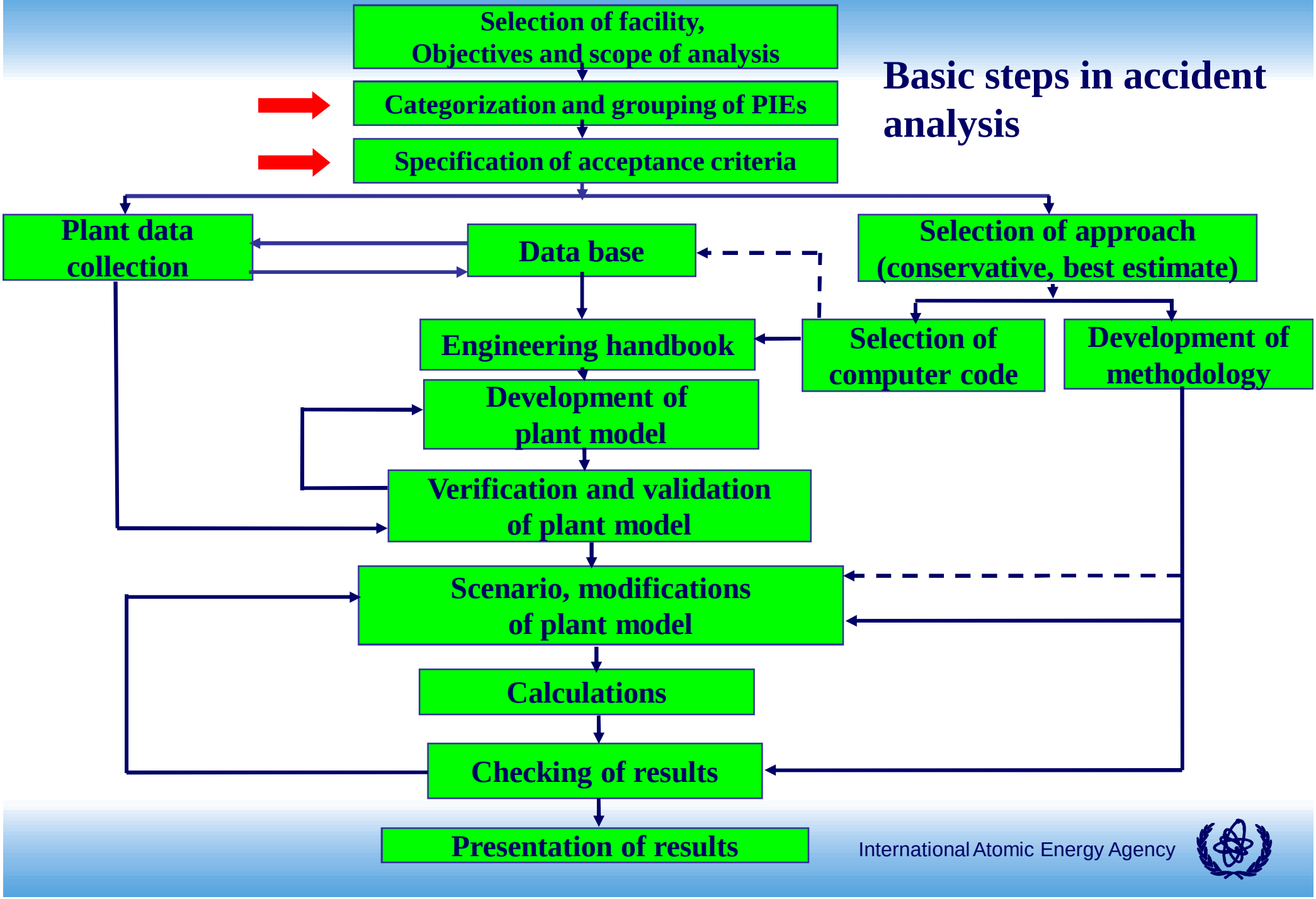
(3 of 3)

- The safety assessment shall be used as a basis for management decisions in an integrated risk informed approach.
- The processes by which safety assessment are produced shall be planned, organized, applied, audited and reviewed in a way that is commensurate with the importance to be placed upon the claims made in the resulting safety report.
- Safety assessments and the management systems that implement them shall be periodically reviewed in accordance with regulatory requirements. In addition, they shall be reviewed and updated:
  - When there is any significant change to the installation or activity;
  - When significant changes in knowledge and understanding occur;
  - When there is an emerging safety issue due to a regulatory concerns or an incident.
  - Periodically at a predefined period as specified by the regulatory authority but typically not less than one in ten years.

Overview of Deterministic Safety Analysis

- **The accident analysis Process**
- **Postulated initiating events:**
  - **Various safety aspects of initiating events**
  - **Grouping of initiating events based on safety aspects**
- **Acceptance criteria**
  - **General acceptance criteria (radiological criteria)**
  - **Specific acceptance criteria (criteria associated with integrity of barriers)**

Basic steps in accident analysis



Categorization of Postulated initiating events

- Categorization is important for systematic approach to analysis
- The most typical categories used in the design basis analysis are based on:
  - principal effect on potential degradation of fundamental safety functions
  - principal cause of the initiating event
  - frequency and potential consequences of the event

Categorization of PIEs based on the frequency

Occurrence (1/reactor-year)	*Characteristics*		*Terminology*
10^{-2} – 1 (Expected in the life of the plant)	Expected	Anticipated Operational Occurrences	Anticipated transients, transients, frequent faults, incidents of moderate frequency, upset conditions, abnormal conditions.
10^{-4} – 10^{-2} (Chance greater than 1% over the life of the plant)	Possible	Design Basis Accidents	Infrequent incidents, infrequent faults, limiting faults, emergency conditions.
10^{-6} – 10^{-4} (Chance less that 1% over the life of the plant)	Unlikely	Beyond Design Basis Accidents without core melt	Faulted conditions
$<10^{-6}$ (Very unlikely to occur)	Remote	Severe accidents	Faulted conditions

Categorization based on degradation of FSFs

- **increase in heat removal by the secondary side;**
- **decrease in heat removal by the secondary side;**
- **decrease in flow rate in the reactor coolant system;**
- **increase in flow rate in the reactor coolant system;**
- **anomalies in distributions of reactivity and power;**
- **increase in reactor coolant inventory;**
- **decrease in reactor coolant inventory;**
- **radioactive release from a subsystem or component**

Examples of normal operation regimes (IAEA)

- **Initial approach to reactor criticality;**
- **Normal reactor startup from shutdown through criticality to power;**
- **Power operation including both full and low power;**
- **Changes in the reactor power level including load follow modes if employed;**
- **Reactor shutdown from power operation;**
- **Shutdown in a hot standby mode;**
- **Shutdown in a cold shutdown mode;**
- **Shutdown in a refuelling mode or equivalent maintenance mode that opens major closures in the reactor coolant pressure boundary;**
- **Shutdown in other modes or plant configurations with unique temperature, pressure or coolant inventory condition**
- **Handling and storage of fresh and irradiated fuel**

Indicative list of PIEs leading to AOOs (IAEA)

- Increase in reactor heat removal: **inadvertent opening of steam relief valves; secondary pressure control malfunctions leading to an increase in steam flow rate; feedwater system malfunctions leading to an increase in the heat removal rate.**
- Decrease in reactor heat removal: **feedwater pump trips; reduction in the steam flow rate for various reasons (control malfunctions, main steam valve closure, TG trip, loss of external load, loss of power, loss of condenser vacuum).**
- Decrease in reactor coolant system flow rate: **trip of one main coolant pump; inadvertent isolation of one main coolant system loop**
- Reactivity and power distribution anomalies: **inadvertent control rod withdrawal; boron dilution due to a malfunction in the volume control system (for a PWR); wrong positioning of a fuel assembly.**
- Increase in reactor coolant inventory: **malfunctions of the chemical and volume control system.**
- Decrease in reactor coolant inventory: **very small loss of coolant accident (LOCA) due to the failure of an instrument line.**
- Release of radioactive material from a subsystem or component: **minor leakage from a radioactive waste system.**

Indicative list of PIEs leading to DBAs (IAEA)

- Increase in reactor heat removal: **steam line breaks.**
- Decrease in reactor heat removal: **feedwater line breaks.**
- Decrease in reactor coolant system flow rate: **trip of all main coolant pumps; main coolant pump seizure or shaft break.**
- Reactivity and power distribution anomalies: **uncontrolled control rod withdrawal; control rod ejection; boron dilution due to the startup of an inactive loop (for a PWR).**
- Increase in reactor coolant inventory: **inadvertent operation of emergency core cooling.**
- Decrease in reactor coolant inventory: **a spectrum of possible LOCAs; inadvertent opening of the primary system relief valves; leaks of primary coolant into the secondary system.**
- Release of radioactive material from a subsystem or component: **overheating of or damage to used fuel in transit or storage; break in a gaseous or liquid waste treatment system**

PIEs leading to BDBA or severe accidents (IAEA)

- **The severe accidents 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. These sequences should be selected by adding additional failures or incorrect operator responses to the DBA sequences (to include safety system failure).**
- **The most rigorous way of identifying severe accident sequences is to use the results of the Level 1 PSA. However, it might also be possible to identify representative or bounding sequences from an understanding of the physical phenomena involved in severe accident sequences, the margin existing in the design, and the amount of system redundancy remaining in the DBAs.**
- **Examples of severe accident initiators include the following:**
  - **Complete loss of the residual heat removal from the reactor core**
  - **LOCA with a complete loss of the emergency core cooling**
  - **Complete loss of electrical power for an extended period**

PIEs due to internal or external hazards (IAEA)

- **The analysis should pay special attention to internal and external hazards which could have the potential to adversely affect more than one barrier at once or to cause simultaneous failures of redundant equipment of safety systems.**
- **Internal hazards: fires, explosions, turbine missile impacts and floods of internal origin which could affect the safety of the reactor and cause failure of some of the safety system equipment which provides protection for that initiating event.**
- **Natural external hazards:**
  - **Extreme weather conditions (wind loading, atmospheric temperatures, rainfall and snowfall, extreme cooling water temperatures and icing)**
  - **Earthquakes**
  - **External flooding**
- **Human made external hazards**
  - **Aircraft crashes**
  - **Hazards arising from transportation and industrial activities (fire, explosion, missiles, release of toxic gases).**

Examples of PIEs during shutdown regimes

- **Reactivity accidents (homogenous or heterogenous boron dilution, connection of a non-operable loop)**
- **LOCA (interface LOCA, man induced LOCA, rupture in the primary RHR system)**
- **Loss of RHR due to degradation of primary circulation (RCS over-draining, injection of non-condensable, rapid cooldown with bubble formation)**
- **Loss of RHR due to equipment incl. support system failures**
- **Overpressurization of RCS (ECCS, pressurizer heaters)**
- **Spent fuel pool cooling events (spent fuel pool draining, leakage, loss of cooling)**
- **Damage of spent fuel during reload operations**
- **Heavy load drop accidents**

Grouping of initiating events based on safety aspects

Safety aspects of different initiating events

- Safety aspects: **different effects that may challenge the integrity of barriers against uncontrolled release of radioactivity**
- **Barriers can be challenged by** affecting the three fundamental safety functions **(control of reactivity, removal of heat from the fuel, confinement of radioactive materials)**
- **Some** potential safety aspects **are listed below, following the sequence of the four successive barriers, covering the full spectrum of consequences, from transients through design basis accidents to severe accidents**

Overview – examples of safety aspects (PWR)

I.

- **reactor power excursions due to reactivity insertion**
- **reactor re-criticality (local or global) after its shutdown**
- **fuel enthalpy and temperature rise**
- **local fuel melting**
- **major fuel melting and core degradation**

II.

- **reduction of the departure from nucleate boiling ratio (DNBR) due to reduced coolant flow or due to increased temperature or decrease of pressure**
- **boiling crisis due to loss of coolant inventory**
- **fuel cladding overheating**
- **zirconium-water reaction of the cladding**
- **deformation and/or damage of the fuel cladding**

Overview – examples of safety aspects (PWR)

III.

- primary or secondary system pressurization
- pressure waves acting on reactor internals
- pressurized thermal shock
- reactor vessel melt-through

IV.

- hydrogen production
- mechanical impact of the escaping coolant jet
- reaction forces of escaping coolant on plant components
- environmental impact of the escaping coolant on system and component qualification requirements (humidity, temperature and radiation)
- containment pressurization
- containment basemat melt-through
- direct radioactivity releases due to containment by-pass
- radioactivity releases from the containment

Grouping of initiating events

- A large number of PIEs is identified. It is not necessary to analyse all of these PIEs. The normal practice is to group them and, for each group, to **choose bounding cases** for analysis.

- Basis for grouping and advantages of grouping
  - the same safety aspects/dominant phenomena

- Similar methodology of analysis within the group
  - the 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

Grouping of initiating events

- **Single event may at the same time belong to several different groups, requiring different analyses**
- **Example: LOCA**
  - **degradation of core cooling**
  - **containment pressure build–up**
  - **radioactivity transport and environmental releases**
  - **pressurized thermal shock (PTS) due to ECCS**
  - **boron dilution (reactivity accident) due to boiling condensing regime**
  - **complete failure of the reactor scram in case of LOCAs may be studied as an ATWS sequence (not usual –ATWS only for AOOs as initiating events)**

Examples of group of internal PIEs for analysis

- **analysis of core cooling and system pressure for various events**
  - **Reactivity induced accidents**
  - **Decrease of reactor coolant flow**
  - **Increase of reactor coolant inventory**
  - **Increase of heat removal by the secondary side**
  - **Decrease of heat removal by the secondary side**
- **analysis for core cooling for LOCAs**
- **analysis of containment by-pass due to PRISE**
- **analysis of boron dilution**
- **analysis of RHR degradation during shutdown**
- **analysis of pressure-temperature transients in containments**
- **analysis of radioactivity transport during DBA**
- **analysis of ATWS**
- **analysis of BDBA**

Acceptance criteria

IAEA Safety glossary

Acceptance criteria: Specified bound on the value of a functional indicator or condition indicator used to assess the ability of a structure, system or component to perform its design function

Acceptance criteria

- Acceptance criteria should be developed for events and conditions within the plant operational states as well as accident conditions

- Acceptance criteria should be developed in two levels:
  - **Global/high level criteria** which relate to radiological consequences, usually expressed in terms of releases or doses and often defined in law or by the regulatory body.

  - **Detailed criteria which relate to integrity of barriers**. They are usually expressed in terms of limiting values of variables essential for integrity of barriers, such as pressures, temperatures, heat fluxes, stresses, etc.

- A high degree of conservatism is achieved by defining these acceptance criterion limits. Detailed criteria should be specified so that to ensure sufficient margin between the criterion and the physical limit for loss of integrity of a barrier against releases of the radioactivity.

- Typically proposed by the designer and subsequently approved by the regulatory body for use in the safety demonstration.

Conservative specification of acceptance criteria

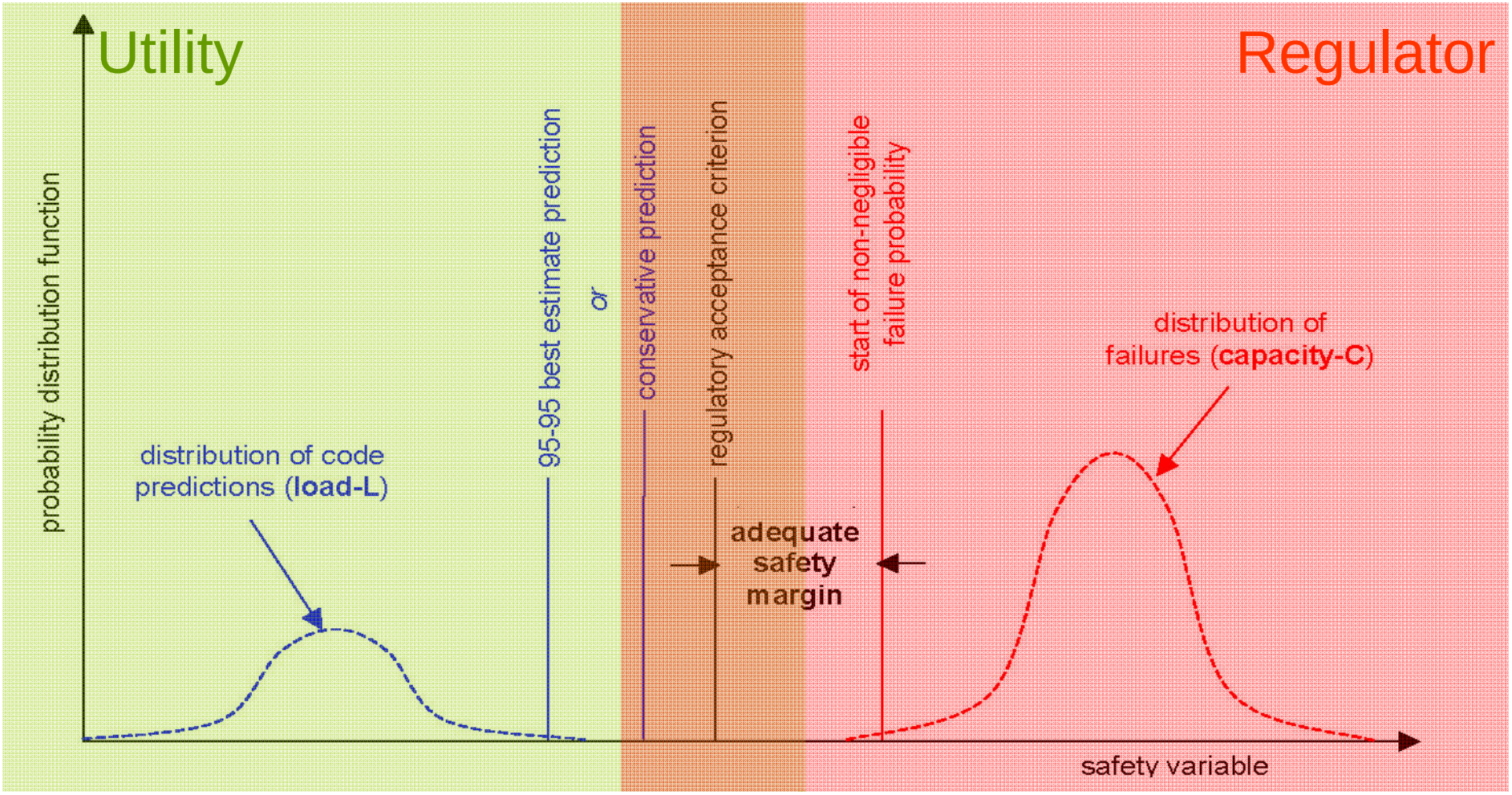
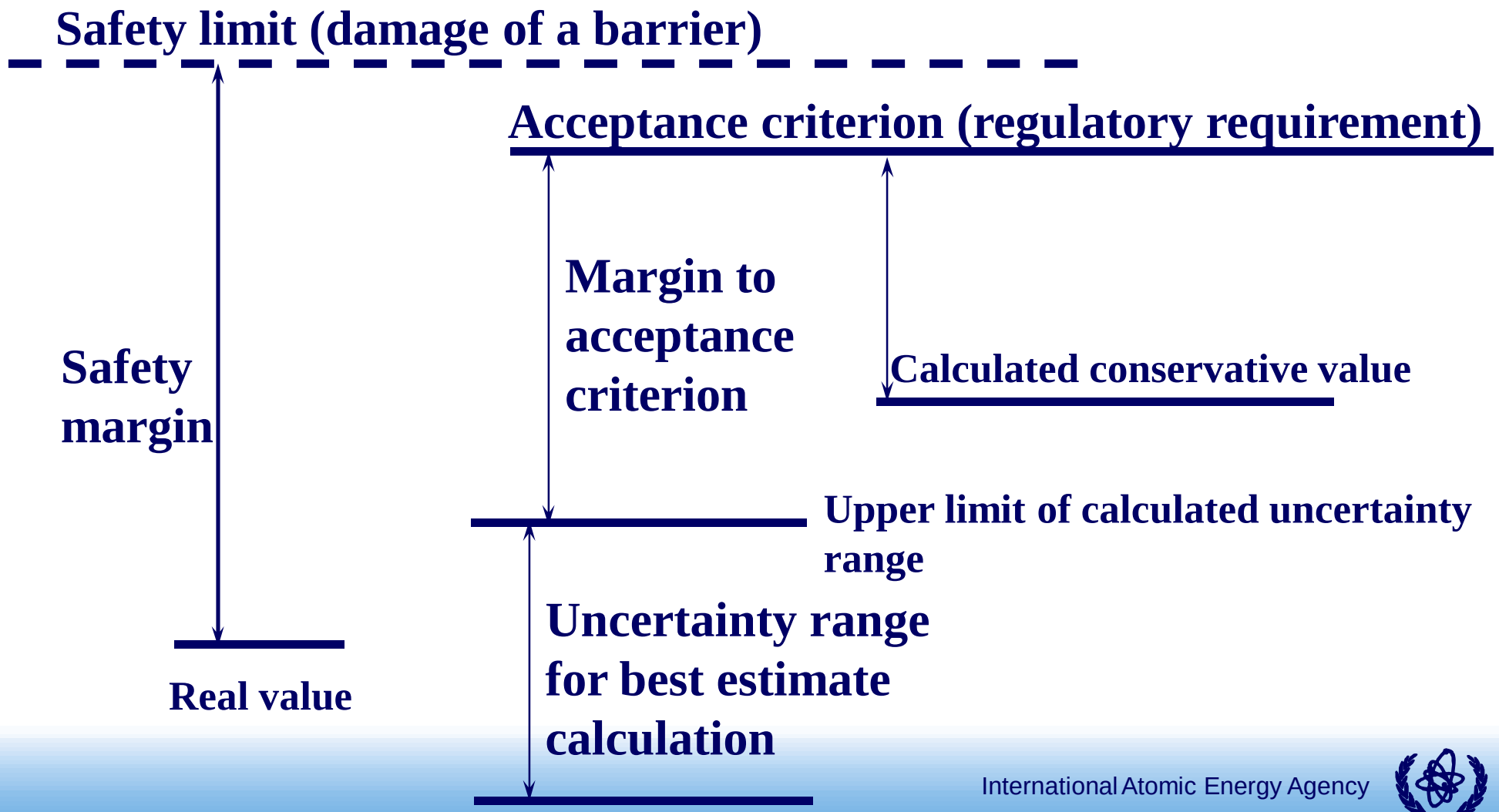


Illustration of safety margins



Acceptance criteria

- **Different criteria are generally needed to judge the vulnerability of individual barriers and for various aspects of the accident. More stringent criteria should be applied for events with a higher frequency of occurrence.**
- **The range and conditions of applicability of each specific criterion should be clearly specified.**
- **In particular, predicted radiological consequences strongly depend on conditions and assumptions for their evaluation. Acceptance criteria can significantly vary accordingly**
-

Global acceptance criteria

- 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.**
- 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.**
- 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.**

Global acceptance criteria

- Severe accidents: **the consequences can be defined in terms of effective dose to critical groups, or in terms of a surrogate measure such as a cumulative frequency of core damage or 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.**

General detailed acceptance criteria

- **An event should not generate a subsequent more serious plant condition without the occurrence of a further independent failure. Thus an anticipated operational occurrence by itself should not generate a DBA, and such an accident by itself should not generate a beyond design basis accident.**
- **There should be no consequential loss of function of the safety systems needed to mitigate the consequences of an accident.**
- **Systems used for accident mitigation should be designed to withstand the maximum loads, stresses and environmental conditions for the accidents analysed.**

General detailed acceptance criteria

- **The pressure in the primary and secondary systems should not exceed the relevant design limits for the existing plant conditions.**
- **The number of fuel cladding failures which could occur should be established for each type of PIE to allow the global radiological criteria to be met.**
- **In LOCAs with fuel uncovering and heatup, a coolable geometry and structural integrity of the fuel rods should be maintained.**
- **No event should cause the temperature, pressure or pressure differences within the containment to exceed values which have been used as the containment design basis.**

Set of detailed acceptance criteria

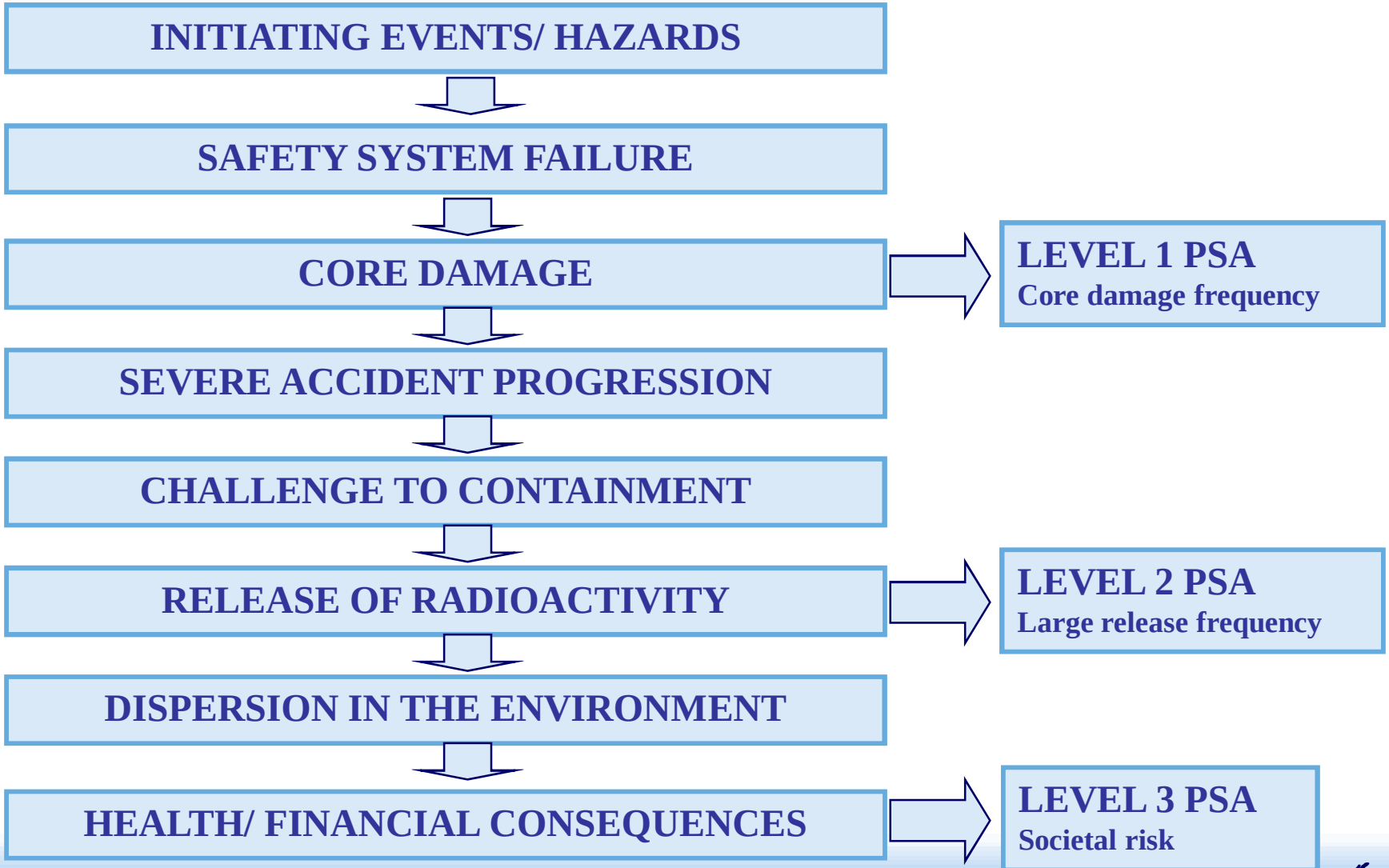
- **Criteria related to integrity of nuclear fuel matrix: maximum fuel temperature, radial averaged fuel enthalpy (with dependence on burn-up and composition of fuel / additives like burnable absorbers)**
- **Criteria related to integrity of fuel claddings: minimum DNBR, maximum cladding temperature, maximum local cladding oxidation)**
- **Criteria related to integrity of the whole reactor core: subcriticality, maximum production of hydrogen, maximum damage of fuel elements, maximum deformation of fuel assemblies (as required for cooling down, insertion of absorbers, and de-assembling)**

Set of detailed acceptance criteria

- **Criteria related to integrity of the RCS: maximum coolant pressure, temperature, pressure and temperature changes and resulting stresses-strains, no brittle fracture from a postulated defect of the RPV**
- **Criteria related to integrity of the secondary circuit (if relevant): maximum coolant pressure, maximum temperature, pressure and temperature changes in the secondary circuit equipment**
- **Criteria related to integrity of the containment and limitation of releases to the environment: maximum and minimum pressure, maximum pressure differences on containment walls, leakages, concentration of flammable gases, acceptable working environment for operation of systems**

Overview of Probabilistic Safety Analysis

PSA model overview



Levels of PSA

Level-1 PSA
- starts with an initiating event/ internal hazard/ external hazard
- identifies the safety systems failures that lead to core damage
- estimates core damage frequency
- identifies the strengths/ weaknesses of safety systems/ emergency procedures

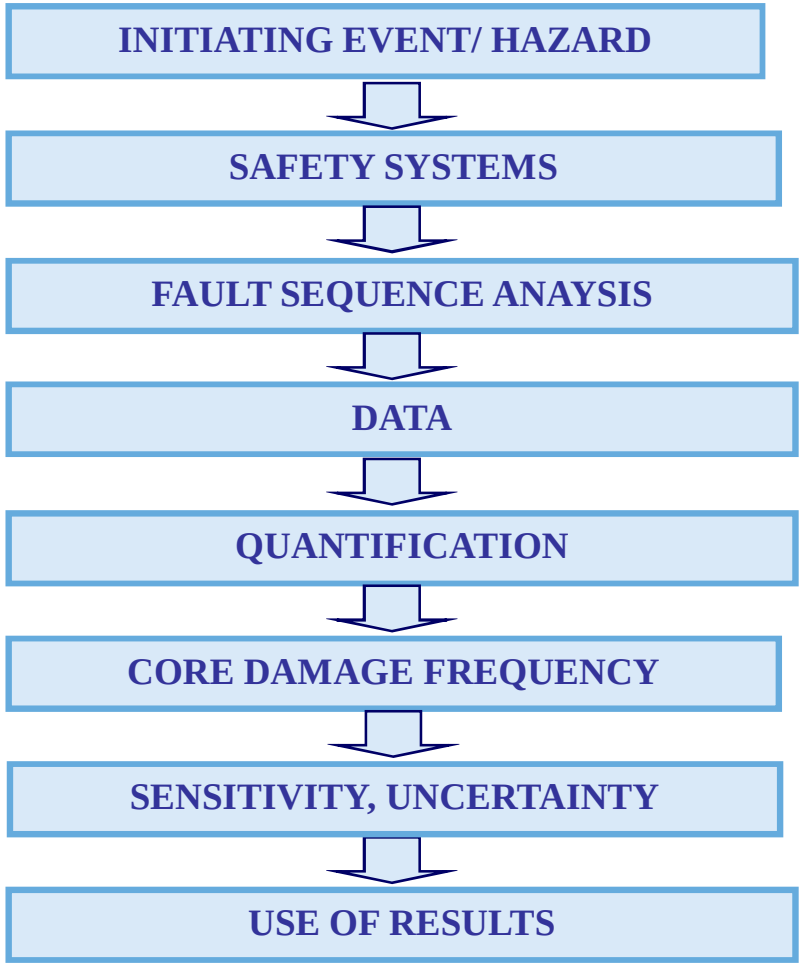
INTERFACE – Plant Damage States

Level-2 PSA
- models: phenomena that could occur following core damage; challenges to the containment integrity; transport of radioactive material in the containment
- considers the effectiveness of the design/ severe accident management measures to mitigate the effects of core damage
- estimates the frequency/ magnitude of a release of radioactive material to the environment

INTERFACE – Source Term Categories/ Release Categories

Level-3 PSA
- models the consequences of a release of radioactive material to the environment
- estimates the risks to public health and societal risks such as the contamination of land or food

Level 1 PSA process



Scope of PSA

Success criteria

Event trees/ fault trees

Initiating events; component failure …

PSA software

Analysis of Results

Identify weaknesses, plant improvements

PSA applications

Aims of the Level 1 PSA

- Determine Core Damage Frequency (CDF)
- Compare with risk criteria/ targets
- Identify weaknesses in design and operation
- Determine whether the risk is as low as reasonably practicable (ALARP)
- Use for PSA applications
  - risk-informed Tech Specs, in-service inspection, quality assurance, ..
  - PSA-based event analysis, …
- Provide an input into the Level 2 PSA

Scope of the Level 1 PSA

- Range of initiating events
  - internal initiating events - transients, LOCA, …
  - internal hazards - fire, flood, …
  - external initiators - earthquake, extreme weather conditions, …
- Modes of operation
  - full power, low power
  - shutdown, refuelling
- Sources of radioactivity on the plant
  - reactor core
  - irradiated fuel in transit/ storage
  - radioactive waste
- Modern practice is to carry out a full scope PSA that address all initiating events and hazards + all modes of operation + all sources of radioactivity (for Level 2 PSA)

Initiating events/ hazards (1)

- Identification of initiating events
  - Safety Analysis report
  - plant system analysis (FMEA, HAZOP, …)
  - analytical approach (Master Logic Diagram)
  - comparison with the PSAs for other plants
- Identification of internal hazards
  - potential for fire, flood, …
  - rotating machinery, stored energy, flammable gases, …
- Identification of external hazards
  - site surveys - geological faults, flooding potential, …
  - industrial activities - flammable gases, explosion, transport, …
  - survey of historical data - earthquakes, aircraft crash, …
  - meteorological data - extreme weather conditions, …
- Aim is that the set of initiating events/ hazards is complete/ comprehensive

Define safety system requirements

- Identify safety functions
  - reactivity control – reactor shutdown, hold down
  - decay heat removal – from the reactor core
  - primary circuit integrity
  - containment integrity
- Define success criteria
  - performance required for each safety system for each initiating event
  - combination of systems and number of trains required to operate
  - includes front line systems (SG feed, emergency core cooling, …) and support systems (electrical power, cooling water, …)
  - operator actions required for the initiating event/ hazard
- Success criteria justified by analysis
  - thermal hydraulic, neutronic, …

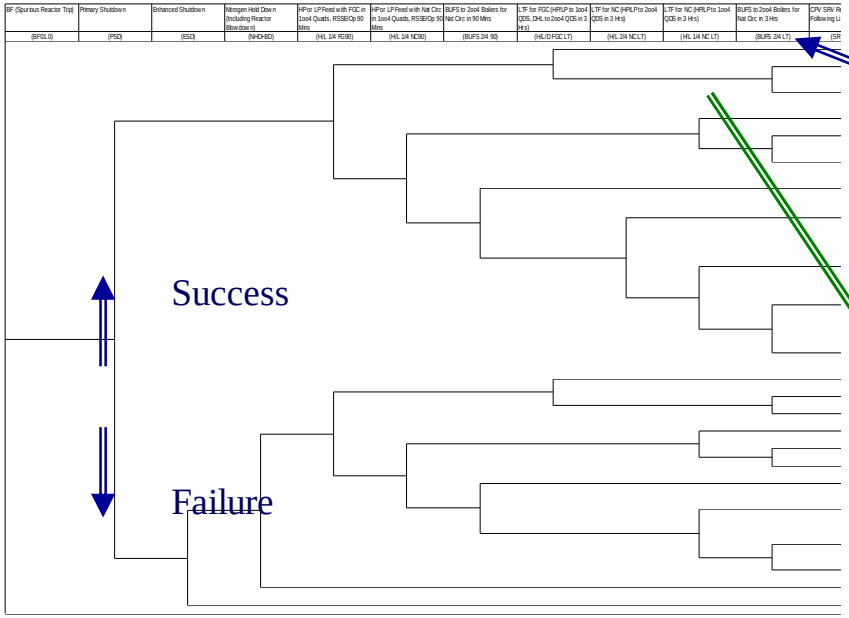
Fault sequence analysis

- Usually done by linked event tree/ fault tree analysis

- Analysis takes into account interdependencies:
  - common support systems
  - consequences of hazards
  - common cause failures
  - human error dependencies

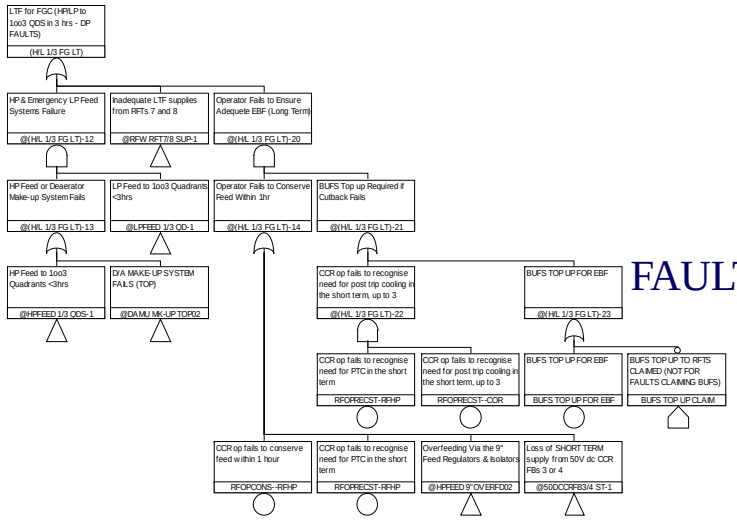
Fault sequence analysis

EVENT TREE



Safety function/ system

Fault trees linked to event trees



FAULT TREE

Fault sequence analysis normally done using linked event trees and fault trees

Modern PSA software allows PSA model to be constructed and analysed

Data required

- Data required
  - initiating event frequencies
  - component failure probabilities
  - common cause failure probabilities
  - human error probabilities
  - duration of maintenance outages

- Justification for data used
  - plant specific data (preferred option, plant data should be collected)
  - data from similar plants
  - generic data (may be all that is available)
  - expert judgement

Results of the Level 1 PSA

- Core damage frequency (CDF)

- Contributions to the CDF from:
  - initiating event groups
  - individual sequences/ cut sets

- Importance functions:
  - Fussel Vesely importance
  - Risk Achievement Worth/ Risk Reduction Worth

Use of results of the Level 1 PSA

- Comparison with risk criteria/ targets for CDF
  - typical targets CDF < 10^{-5} /year
- Identify areas where improvements required to plant
  - additional safety systems
  - additional redundancy/ diversity/ segregation/ equipment qualification
- Identify areas where improvements required to operation
  - better operating procedures, human-machine interfaces
  - better training
  - better management of risk
- PSA applications
  - Risk Informed Tech Specs, In-Service Inspection, Quality Assurance, …
  - maintenance planning
  - PSA-based event analysis