Training Course
on the IAEA Safety Standards Overview

IAEA General Safety Requirements GSR Part 4 (Rev.1) Safety Assessment for Facilities and Activities

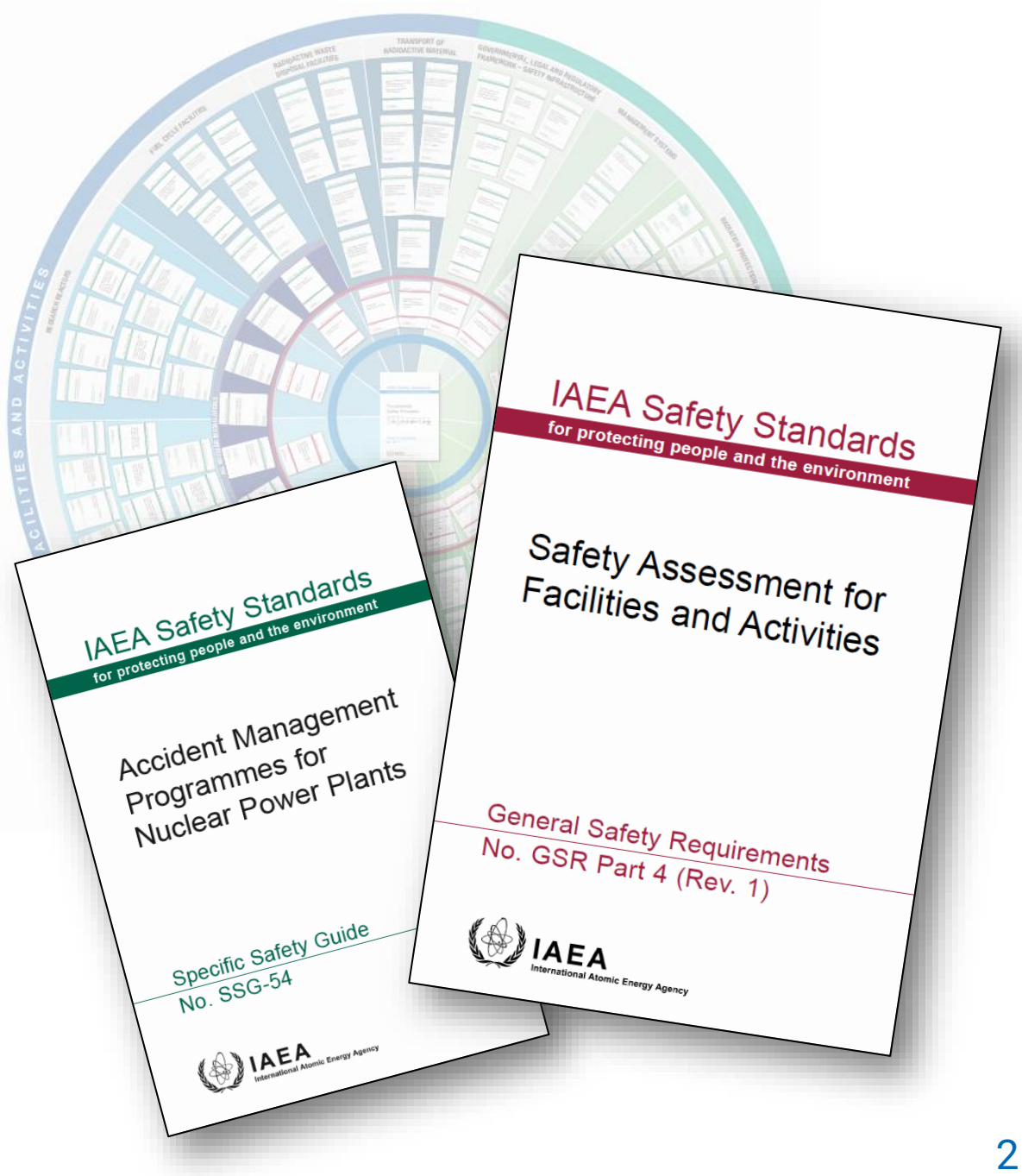
Jorge LUIS HERNANDEZ
Safety Assessment Section (SAS)
Division of Nuclear Installation Safety (NSNI)
Department of Nuclear Safety and Security, IAEA

Shinagawa Campus, Tokai University, Tokyo, Japan

04 -07, August 2026

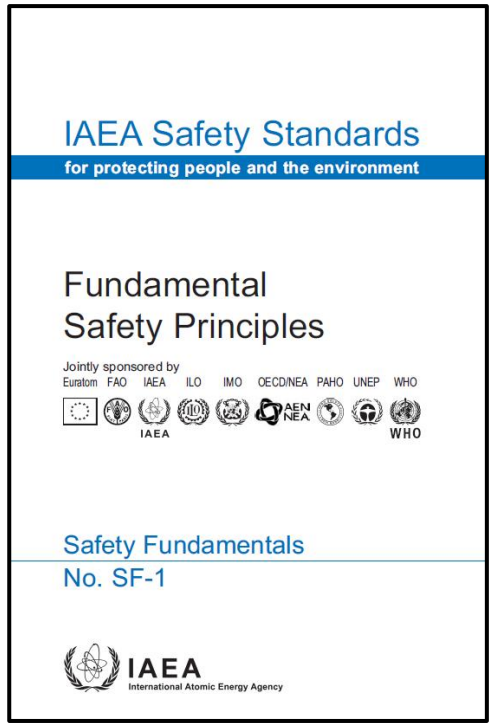
Outline

- INTRODUCTION
- REV.1 OF IAEA REQUIEMENTS ON SAFETY ASSESSMENT
  - GRADED APPROACH
  - SAFETY ASSESSMENT
  - MANAGEMENT, USE AND MAINTENANCE OF SAFETY ASSESSMENT
- IAEA SAFETY GUIDE ON ACCIDENT MANAGEMENT
- CONCLUSIONS



Introduction

INTRODUCTION



Safety shall be assessed for all facilities and activities consistent with a graded approach

Facility/activity may only be commissioned or commenced **once it has been demonstrated to the satisfaction of the regulatory body** that the proposed safety measures are adequate.

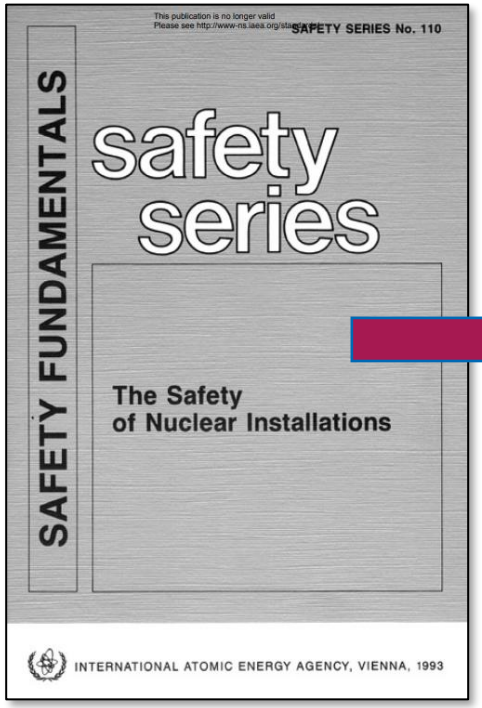
Safety assessment is **repeated in whole or in part** as necessary in order to take into account changed circumstances

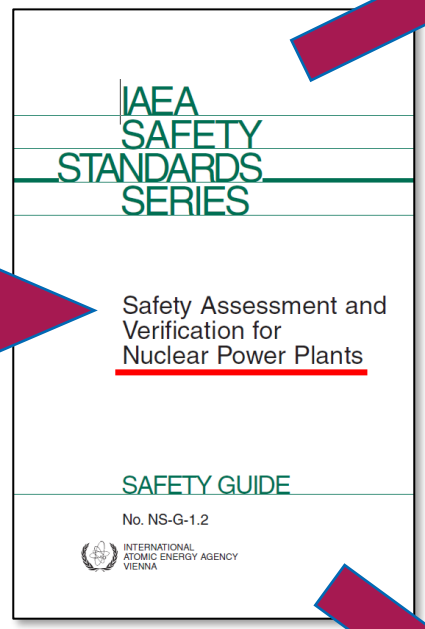
- application of new standards
- technological developments,
- feedback of operating experience
- modifications and the effects of ageing

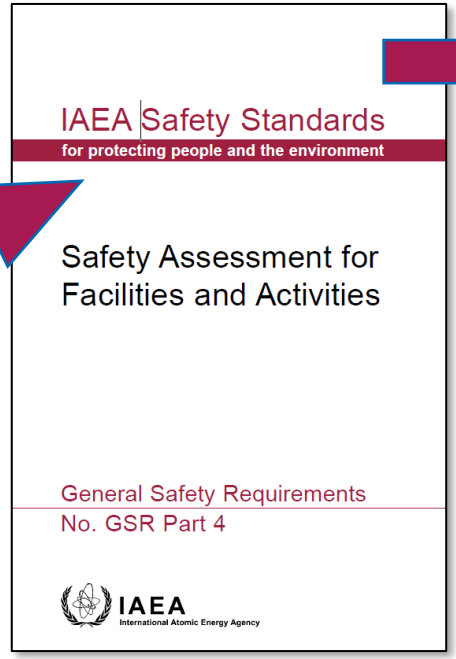
Continuation of such operations is subject to demonstrating to the satisfaction of the regulatory body that the **safety measures remain adequate.**

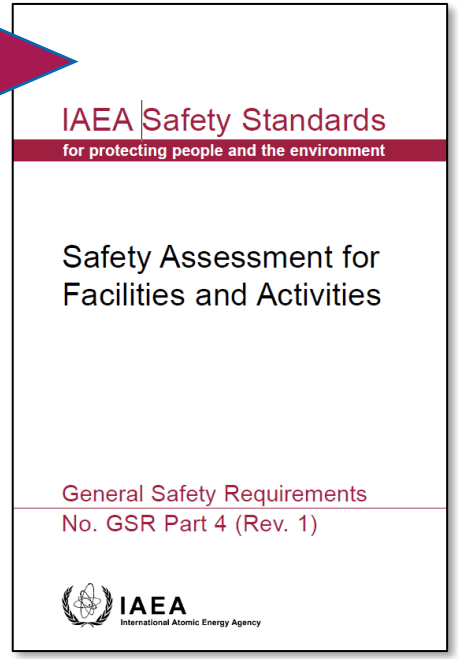
IAEA Requirements for Safety Assessment

General (facilities and activities)

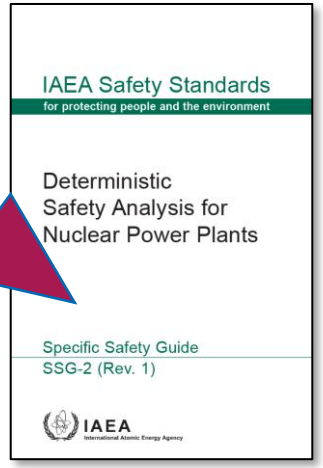


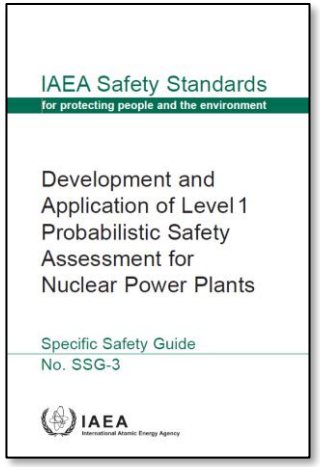


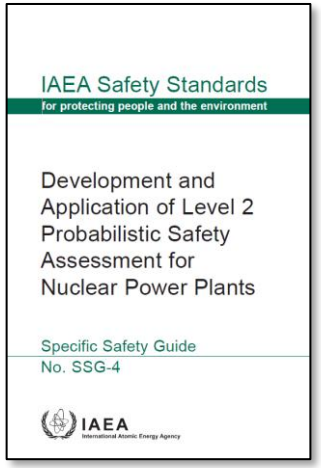




Specific (NPPs)





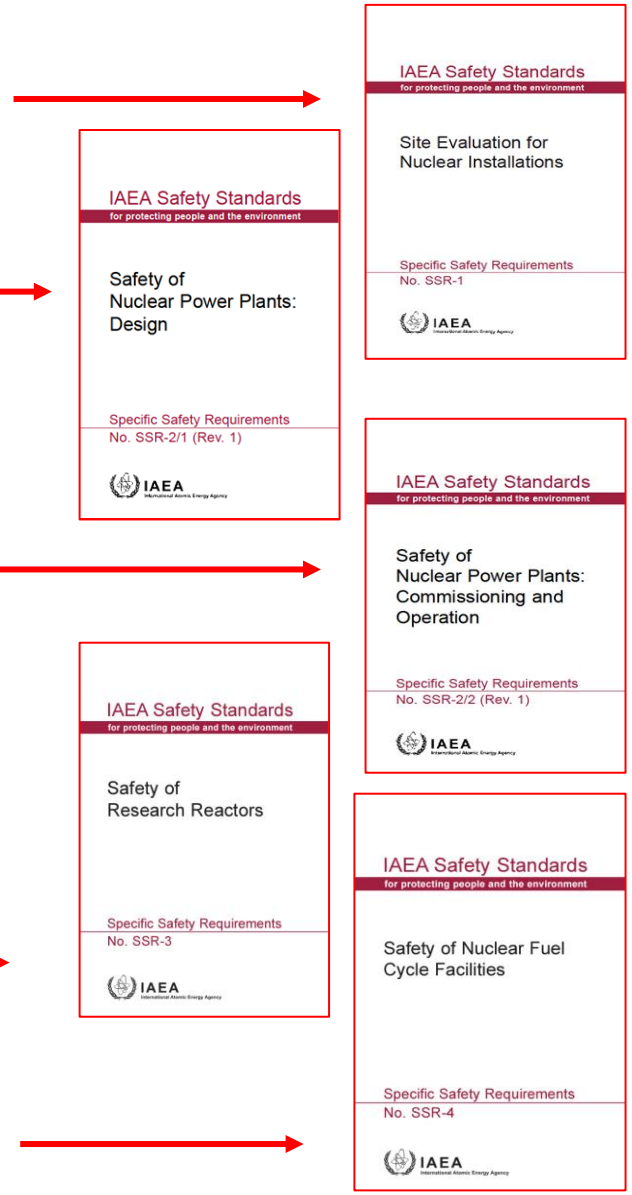


Facilities:
NPPs, research reactors, critical assemblies, fuel cycle facilities, irradiation facilities, etc.

Activities:
Production, use, import and export of radiation sources, transport of radioactive material, mining, decommissioning and dismantling of facilities, etc.

Requirements in relation to Safety Assessment referred from:

- **SSR-1 Site Evaluation for Nuclear Installations**
- **SSR-2/1 (Rev. 1) Safety of Nuclear Power Plants: Design**
- **SSR-2/2 (Rev. 1) Safety of Nuclear Power Plants: Commissioning and Operation**
  - **Operation**
  - **Plant Modifications**
  - **Maintenance, testing, surveillance and inspection programmes**
  - **Periodic safety review and long-term operation**
- **SSR- 3 Safety of Research Reactors**
- **SSR-4 Safety of Nuclear Fuel Cycle Facilities**



IAEA Safety Standards on Safety Assessment

General Safety Requirements are addressed in GSR Part 4 (facilities and activities – F&A)

NPP details in safety guides

- SSG-2 (Rev. 1) (DSA)
- SSG-3 (Rev. 1) and SSG-4 (Rev. 1) (PSA)
- SSG-61 (SAR)

Safety Approach

- Acceptance criteria/design limits
- Defense in Depth (DiD) and plant states
- Requirements for reliability

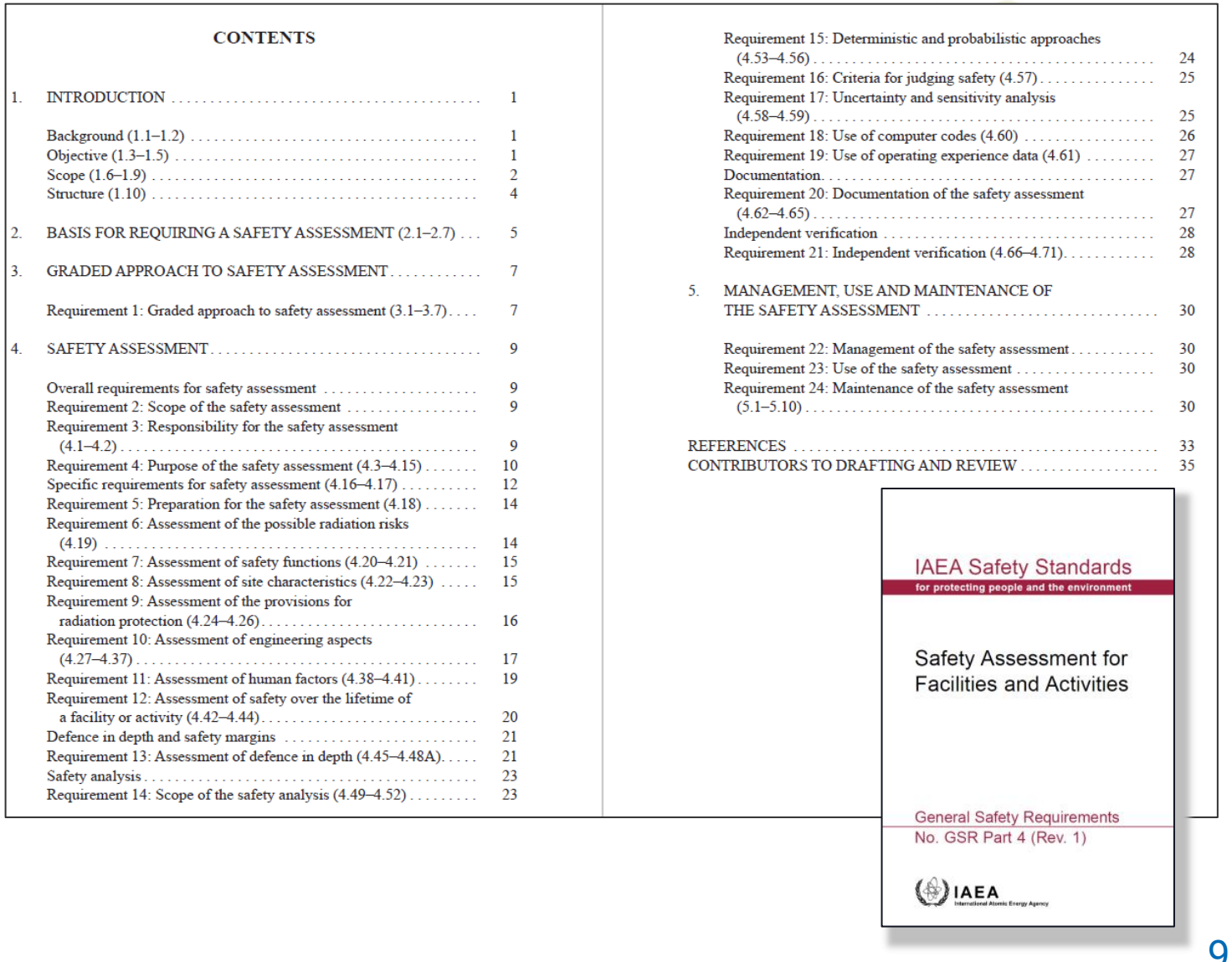
IAEA GSR Part 4 (Rev.1) Safety Assessment for Facilities and Activities

IAEA Safety Standards on Safety Assessment

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

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

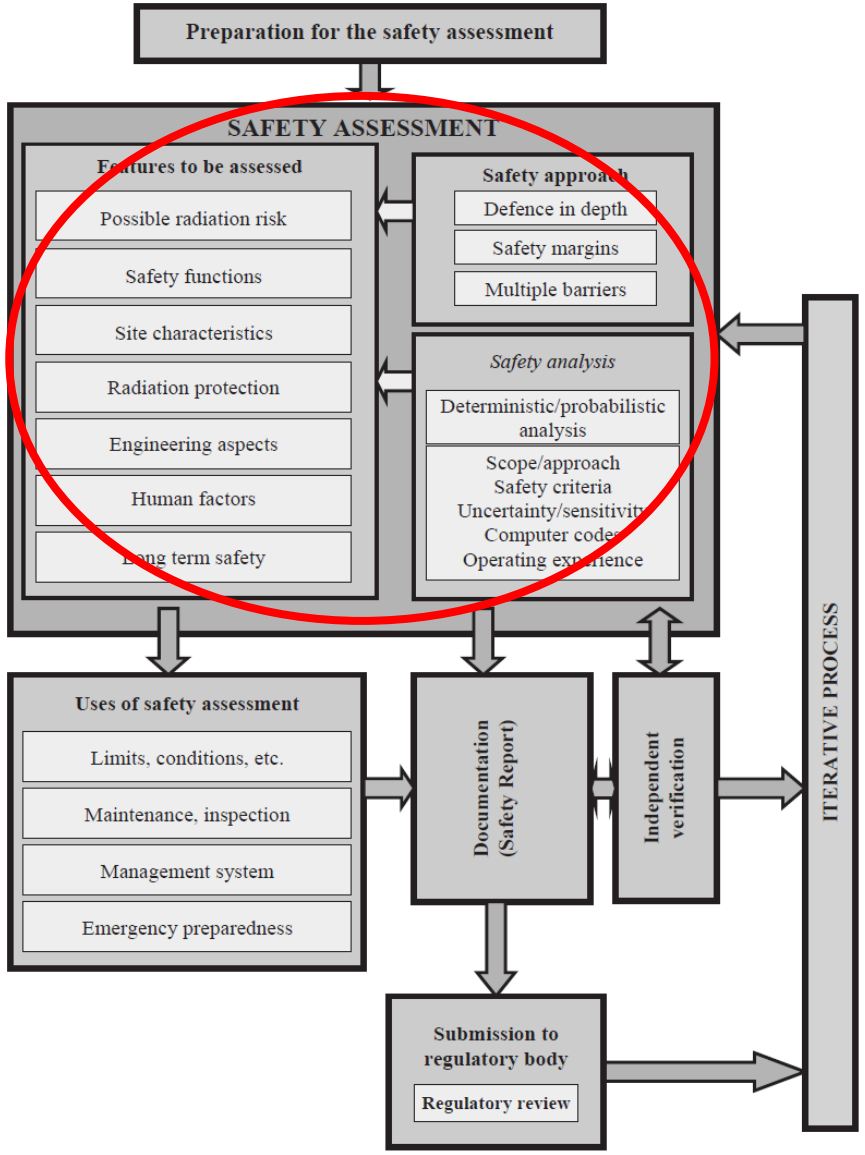
- Margins to withstand external events
- Margin to avoid cliff-edge effects
- Multiple facilities/activities at one site
- Cases where resources are shared
- Human factors in accident conditions



CONTENTS

IAEA Safety Standards on 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: Requirement 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

- Allows flexibility in the way that the possible radiation risks are assessed and controlled **without unduly limiting the operation.**
- **Graded approach used to determine:**
  - scope and level of detail
  - resources to be directed
- **Graded approach considers:**
  - magnitude of the possible risks
  - risks at all plant states
  - very low probability events with potentially high consequences
  - maturity or complexity of facility or activity

SAFETY ASSESSMENT: Requirement 1 (cont'd)

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

- **Maturity**
  - proven practices, procedures and designs
  - data on performance of F&A
  - uncertainties in the performance of F&A
  - continuing and future availability of experienced manufacturers and constructors.
- **Complexity**
  - efforts required to construct or do the F&A
  - processes for which control is necessary
  - radioactive material handling extent
  - longevity of the radioactive material
  - reliability and complexity of structures, systems and components (SSC)
  - accessibility of SSC for maintenance inspection, testing and repair

SAFETY ASSESSMENT: Requirement 1 (cont'd)

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

- **The application of the graded approach shall be reassessed** as the safety assessment progresses and a better understanding is obtained of the radiation risks arising from the facility or activity.
- The scope, level of detail and level of resources then **modified as necessary**
- Graded approach shall also be taken in **when updating the safety assessment.**

SAFETY ASSESSMENT: Requirement 2

Req. 2

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

Facilities:

- NPPs, research reactors, critical assemblies, fuel cycle facilities, irradiation facilities, etc.

Activities:

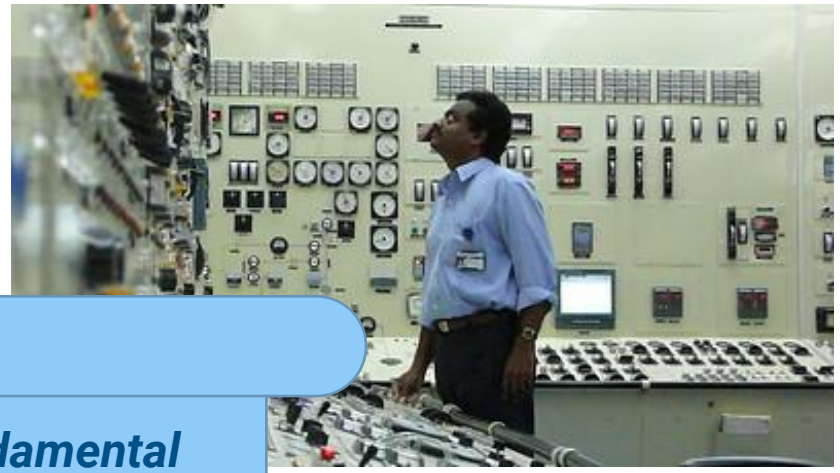
- Production, use, import and export of radiation sources, transport of radioactive material, mining, decommissioning and dismantling of facilities, etc.

SAFETY ASSESSMENT: Requirement 3

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.

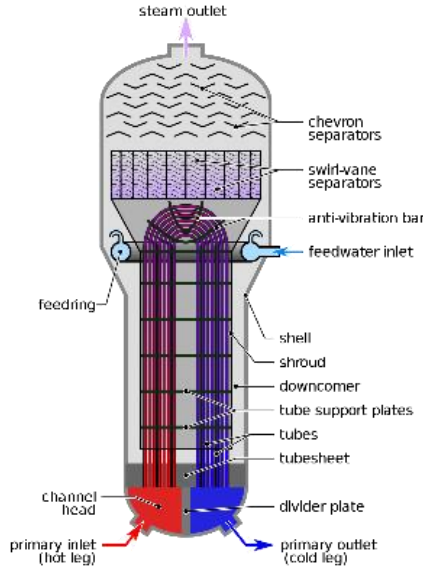


IAEA Fundamental Safety Principles

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

SAFETY ASSESSMENT: Requirement 3 (cont'd)

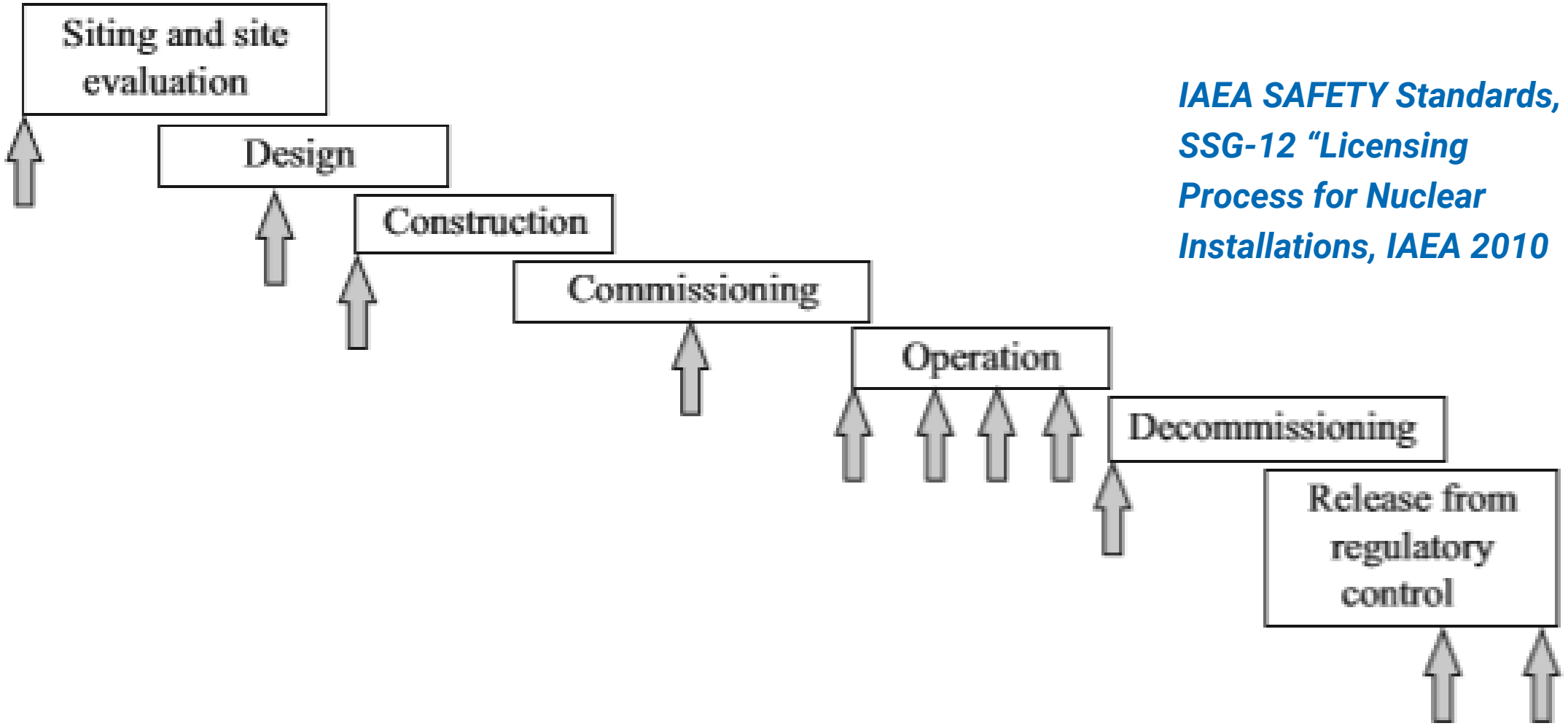
Other groups, such as **designers, manufacturers, constructors, employers, contractors, consignors** and **carriers**, also have legal, professional or functional responsibilities with regard to safety.



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

SF-1: Facility/activity may only be commissioned or commenced ***once it has been demonstrated to the satisfaction of the regulatory body***

Lifetime stage of nuclear installation (hold points)



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

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

SAFETY ASSESSMENT: Requirement 4

Req. 4

PURPOSE OF THE SAFETY ASSESSMENT

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.

SAFETY ASSESSMENT: Requirements 5-6

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.**

SAFETY ASSESSMENT: Requirement 7

Req. 7

ASSESSMENT OF SAFETY FUNCTIONS

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

- **All safety functions** associated with a facility or activity shall be specified and assessed
- Includes the functions associated with **SSCs, barriers, inherent safety features, human actions**
- An assessment is undertaken to determine **whether the safety functions** can be fulfilled for all plant states (including normal operation)
- SA shall determine whether SSCs and barriers performing the safety functions have an adequate level of **reliability, redundancy, diversity, separation, segregation, independence and equipment qualification and whether potential vulnerabilities have been identified and eliminated.**

SAFETY ASSESSMENT: Requirement 8

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

- **Evaluation of the site characteristics shall cover:**
  - Physical, chemical, radiological characteristics that will affect the dispersion or migration of radioactive material
  - Identification of natural and human induced events
  - Distribution of the population around the site.
- **Scope and level of detail** of the site assessment shall be consistent with the possible radiation risks associated with the facility or activity, the type of facility to be operated or activity to be conducted, and the purpose of the assessment
- The site assessment **shall be reviewed periodically** over the lifetime of the facility or activity

Which site characteristics would you expect to change and how are they relevant to safety assessment?

SAFETY ASSESSMENT: Requirements 9-10

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

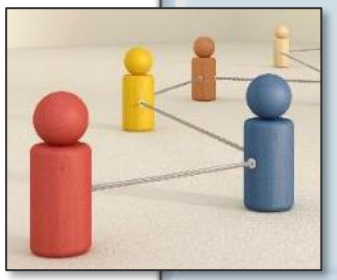
It shall be determined in the safety assessment whether a facility or activity uses, to the extent reasonable, **structures**, **systems** and **components** of **robust and proven design**

SAFETY ASSESSMENT: Requirement 11

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**



- **Human actions** (in all plant states) shall be assessed
- Whether personnel competences, training programmes and minimum staffing levels are adequate
- Whether human factors were addressed in the design (Human Machine Interface; HOF)
- Aspects of **safety culture** shall be included in the safety assessment as appropriate
  - *Challenging task, see Safety Report No.127 for considerations on Human and Organisational Factors (HOF)*

SAFETY ASSESSMENT: Requirement 12

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

- Safety assessment shall cover all the **lifetime stages (including design)**.
- Safety assessment includes activities that are carried out **over a long period of time, (e.g. decommissioning, dismantling)**
- For **disposal facility for radioactive waste** in significant quantities, radiation risks shall be considered for the post-closure phase.
  - Radiation risks following closure of the disposal facility may arise from gradual processes, e.g. degradation of barriers

SAFETY ASSESSMENT: Requirement 13

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**

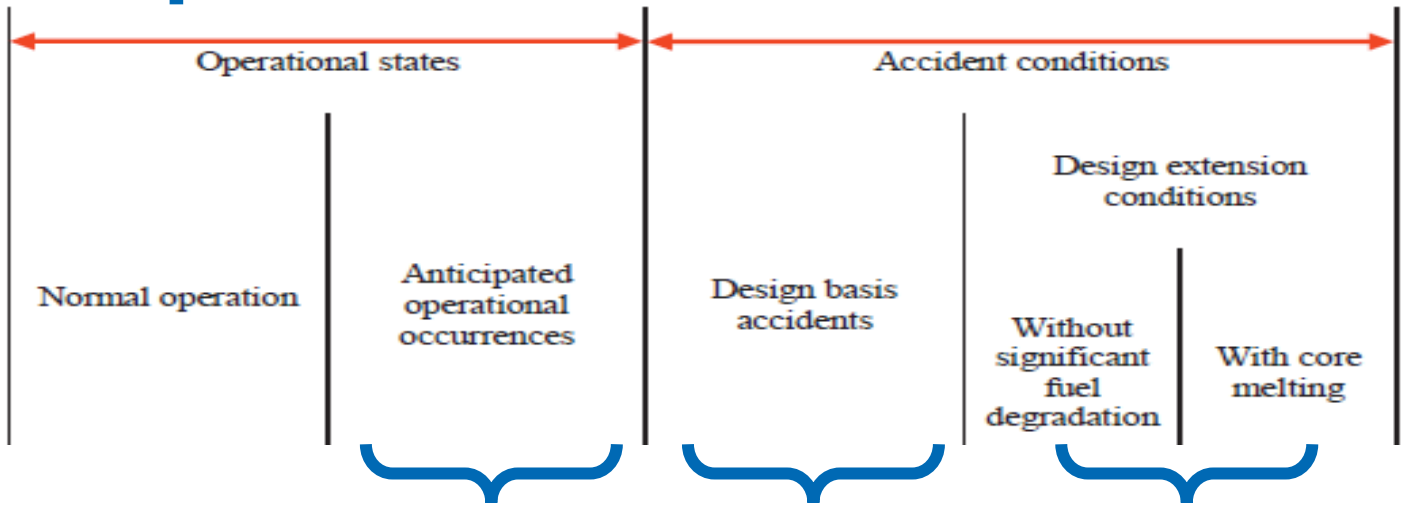
- **Whether adequate provisions have been made** at each of DiD levels to e.g. address deviations from normal operation (NO), control accidents within design limits, mitigate the consequences of accidents that exceed design limits
- **Idenfication of DiD layers of protection:** relevant safety functions, challenges to safety functions and mechanisms of these challenges, provisions to monitor or mitigate the consequences of mechanisms
- **Whether DiD is adequately implemented** (e.g. reducing number of challenges, DiD levels independence)
- **Whether there are adequate safety margins**
- Where practicable, SA shall confirm that there are adequate margins to **avoid cliff edge effects that would have unacceptable consequences.**

SAFETY ASSESSMENT: Requirement 14

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**.



- Whether the facility or activity is in compliance with the relevant **safety requirements and national regulatory requirements.**
- **All plant states** to be considered (considering frequencies and consequences)
- **Relevant operating experience** shall be taken into account in the safety analysis.

SAFETY ASSESSMENT: Requirement 15

Req. 15

DETERMINISTIC AND PROBABILISTIC APPROACHES

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

- Deterministic and probabilistic approaches **complement one another,** can be used together for integrated decision making
- **Deterministic:** to specify and apply a set of deterministic rules and requirements for the design and operation of facilities or for the planning and conduct of activities. **Conservative.**
  - high degree of confidence that the level of radiation risks to workers and members of the public will be acceptably low).
- **Probabilistic:** to determine all significant contributing factors to the radiation risks, to evaluate whether the design is well balanced and meets probabilistic safety criteria (if any). **Realistic.**

SAFETY ASSESSMENT: Requirements 16-18

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

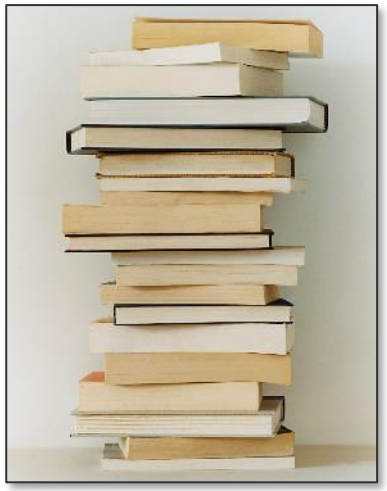
Any calculational methods and computer codes used in the safety analysis shall undergo verification and validation.

SAFETY ASSESSMENT: Requirements 19-21

Req. 19

USE OF OPERATING EXPERIENCE DATA

Data on operational safety performance shall be collected and assessed



Req. 20

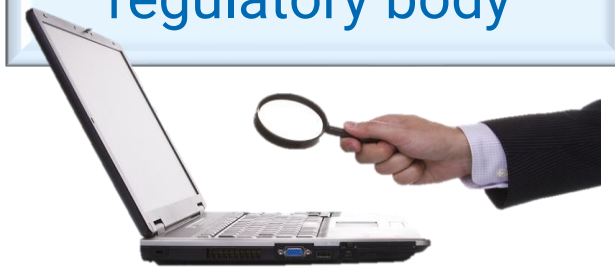
DOCUMENTATION OF THE SAFETY ASSESSMENT

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

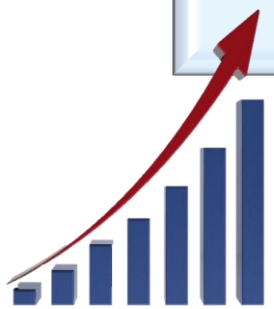


SAFETY ASSESSMENT: Requirements 22-23

Req. 22

MANAGEMENT OF THE SAFETY ASSESSMENT

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



Req. 23

USE OF THE SAFETY ASSESSMENT

Safety assessment results 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 all plant states;
- to specify the **necessary competences** for the staff involved in the facility or activity;
- to make **decisions in an integrated, risk informed approach**

SAFETY ASSESSMENT: Requirement 24

Req. 24

MAINTENANCE OF THE SAFETY ASSESSMENT

The safety assessment shall be periodically reviewed and updated

- The safety assessment in **itself cannot achieve safety**.
- Safety can only be achieved if the **input assumptions are valid**, derived limits and conditions are implemented and maintained, and the assessment reflects the facility or activity as it actually is at any point in time.
- Facilities and activities change over their lifetimes (e.g. **modifications, effects of ageing**).
- **Knowledge and understanding** also advance with time.
- The safety assessment shall be updated to reflect such changes and **to remain valid.**
- Updating the safety assessment is also important in order to provide a baseline for the **future evaluation of monitoring data and performance indicators**

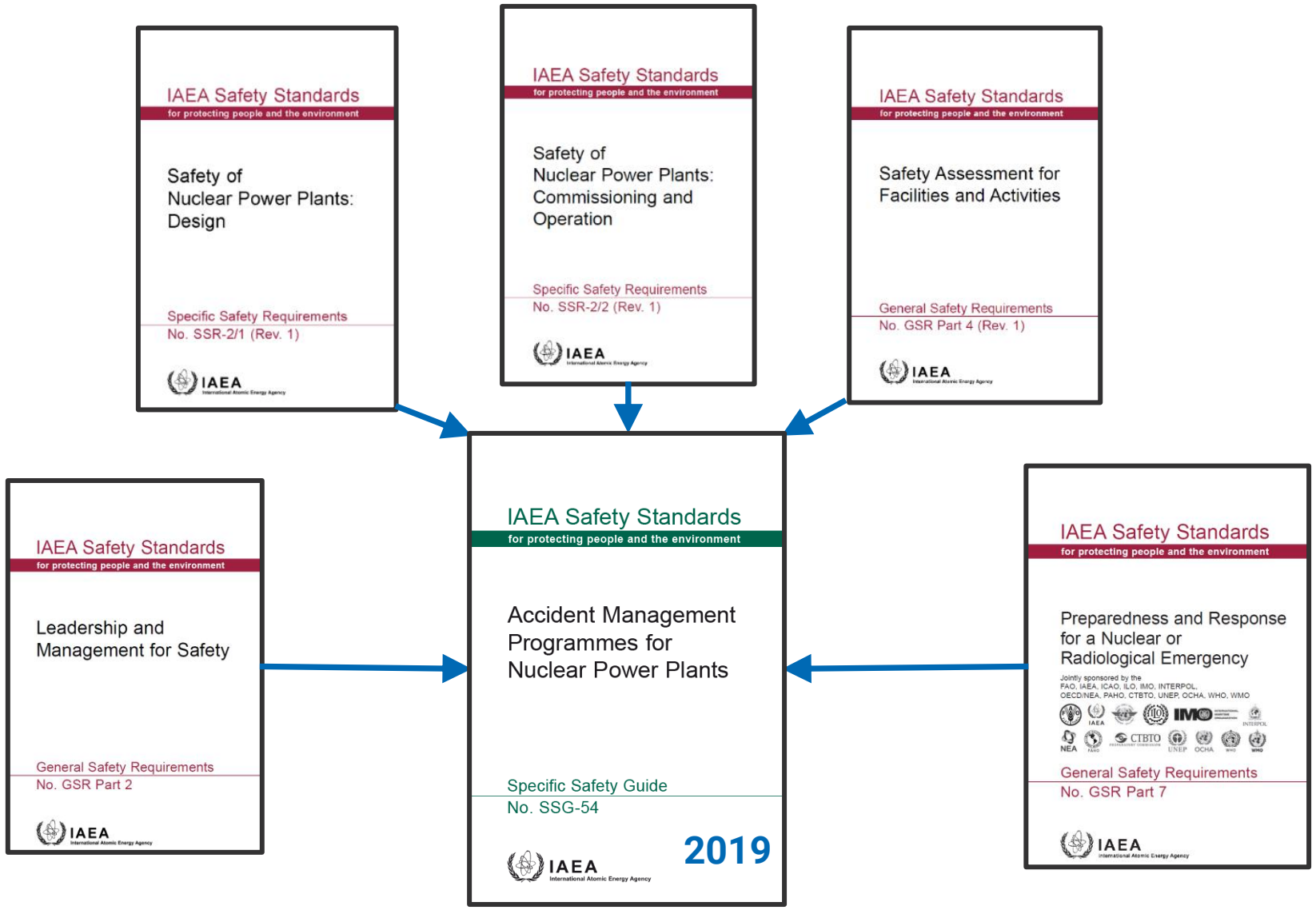
Concluding remarks

The IAEA General Safety Requirements – Safety Assessment for Facilities and Activities GSR Part 4 (Rev.1) (2016)

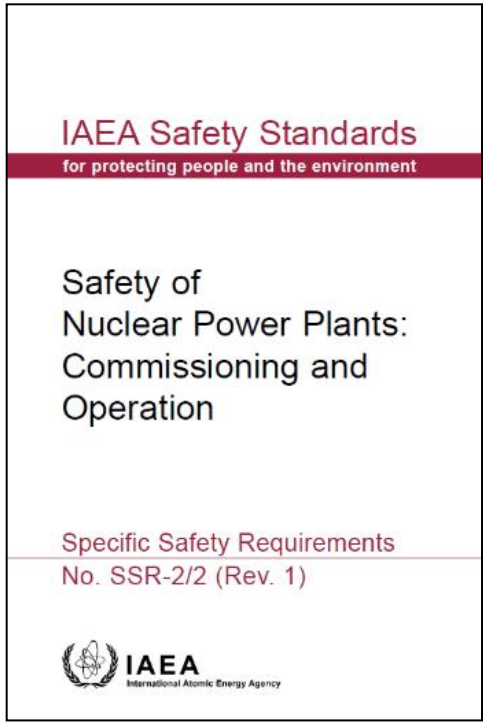
- **Reflects the international consensus** on safety assessment and graded approach
- **Wide scope:** all types of facilities and activities
- **Contains 24 requirements:** Graded approach, Safety Assessment aspects and Management of safety assessment
- **Supported by numerous Safety Guides:** e.g. DSA, PSA, non-reactor facilities
- **Next revision of GSR Part 4** is planned to be initiated in 2026

IAEA SSG-54
Accident Management Programmes for NPPs

SSG-54 interfaces with Safety Requirements



SSR-2/2 (Rev.1) Requirement 19
Accident Management Programme



The operating organization shall establish, and periodically review and as necessary revise, an Accident Management Programme (AMP).

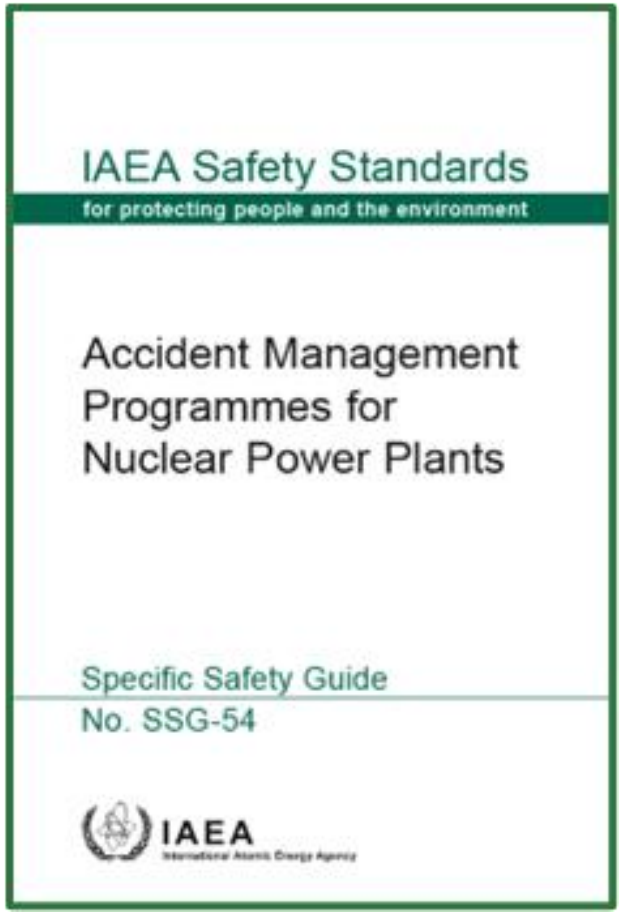
- "An AMP shall be established that covers the preparatory measures, procedures and guidelines, and equipment that are necessary for preventing the progression of accidents, including accidents more severe than design basis accidents, and for mitigating their consequences if they do occur.
- The AMP shall be documented and shall be periodically reviewed and as necessary revised"
- The AMP shall include instructions for the utilization of available equipment — safety related equipment as far as possible, but also items not important to safety (e.g. conventional equipment)". It shall include also contingency measures.
- The AMP shall include the technical and administrative measures necessary to mitigate the consequences of an accident".
- The AMP shall include training necessary for its implementation.

Accident management

- The IAEA Safety Glossary defines ‘accident management’ as **“The taking of a set of actions during the evolution of an accident to:**
  - **prevent escalation** to a severe accident;
  - **mitigate the consequences** of a severe accident;
  - achieve a **long term safe stable state**.”

- **Accident management program (AMP)** is needed for such measures and AMP:
  - encompasses plans and actions undertaken to ensure that plant personnel and other operating organization personnel are adequately prepared **to decide on and implement effective on-site actions**.
  - Essential aspect of DiD application of defence in depth and deals with accidents within and beyond the design basis
  - Needs to be **supported by appropriate safety assessment.**
  - Needs to be **well integrated with the arrangements for EPR**

SSG-54 structure



1. INTRODUCTION

2. GENERAL GUIDANCE FOR AN AMP

- AMP concept, main principles
- Forms of Accident Management Guidance
- Verification and Validation of AMP
- Accident Management for External Hazards and Multi-Unit sites
- Roles and Responsibilities and staffing

3. DEVELOPMENT AND IMPLEMENTATION OF A SEVERE ACCIDENT MANAGEMENT PROGRAMME (SAMP)

- Technical Bases, challenge mechanisms and plant capabilities
- Severe Accident Management Guidance (development, V&V, integration in EPR, hardware provisions)
- Analyses for Development of a SAMP
- Training, Exercises, Drills and updating of SAMP

4. EXECUTION OF THE ACCIDENT MANAGEMENT PROGRAMME

ANNEX: EXAMPLES OF SAMG IMPLEMENTATION IN NPPs

Accident management programmes

- An AMP should be developed and implemented for the prevention and mitigation of severe accidents, **irrespective of the frequency of accident sequences and of fission product releases considered in the design.**
- AMP should address **all modes and states of operation and all fuel locations,** including the spent fuel pool,
- AMP **should take into account possible combinations of events**
- **It should also consider external hazards** more severe than those considered for the design that could result in **significant damage to the infrastructure** on the site or off the site which would hinder actions
- AMP should be developed and **maintained consistent with the plant design** and its current configuration

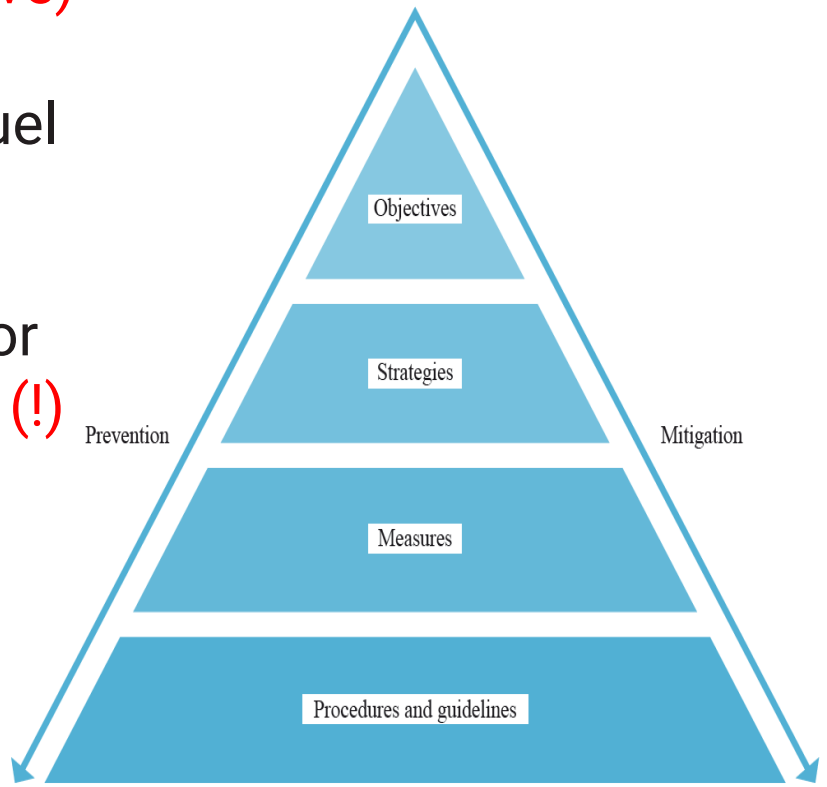
Forms of Accident Management Guidance

Preventive domain (before the onset of fuel rod degradation)

- Actions aimed at **controlling accident progression** to prevent significant fuel damage **or to delay it**
- Guidance is provided in the **form of procedures** (prescriptive)

Mitigatory domain (when a severe accident, i.e. significant fuel degradation, is imminent or in progress)

- Priority is given to mitigating the consequences: avoiding or **limiting fission product releases by containment integrity** (!)
- Guidance is provided in the form of guidelines
  - can be prescriptive for specific actions or
  - offer a range of actions that should be evaluated because of the uncertainties about on plant conditions and accident evolution.



Accident management programmes

Multiple strategies should be identified in preventive and mitigatory domains:

- **Preventing or delaying** the occurrence of fuel rod degradation;
- **Terminating the progress** of fuel rod degradation once it has started;
- **Maintaining the integrity of the reactor pressure vessel** to prevent melt-through especially at high pressure;
- **Maintaining the integrity of the containment** and preventing containment bypass;
  Highest priority
- Minimizing releases of radioactive material from the fuel or at other locations where releases of radioactive material could occur;
- Returning the plant to a long term safe stable state in which the fundamental safety functions can be preserved.

Prioritization of accident management strategies

Accident management strategies **should be prioritized** with account taken of the plant damage state and the existing and anticipated challenges, e.g.:

- **Time frames** and severity of challenges to the barriers
- **Availability of support functions**, as well as the possibility of their restoration.
- **Initial operating mode** of the plant
- **Adequacy of a strategy** in the given domain
- **Difficulty** of implementing several in parallel.
- **Long term implications** of or concerns about their implementation

Trigger should be either certain parameters reach thresholds or trending imminently

Uncertainties should be taken into account (e.g. time windows)

Suitable and effective measures should be derived that correspond to available hardware provisions (e.g. SSCs available, recovery, non-permanent equipment)

Main principles of accident management guidance

Accident management guidance should address the **full spectrum of events**:

- **Promoting consistent implementation** by all staff during an accident.
- **Using the SSCs that are not likely to fail** in the given conditions
- **Instrumentation available and its reliability** for evaluating plant conditions
- **Maintaining SFs** or **increase the margin to failure** or **extending time to failure**
- Adding components, including non-permanent equipment,
- **Human and organizational factors** (e.g. adverse conditions: radiation, lightning temperature, stress)
- **Command and control structure**, information sharing and cooperation

Supporting analyses for AMP

- Accident management procedures and guidelines **should be supported by technical basis documents**, which describe and explain the rationale of the various parts of procedure and guidelines.
- Severe accident management programme should be supported by **appropriate computational analysis showing the progression of representative accident** sequences to be addressed
- **Best estimate computer codes**, assumptions and data regarding initial and boundary plant conditions should be used with proper consideration of uncertainties for timing and severity of the phenomena

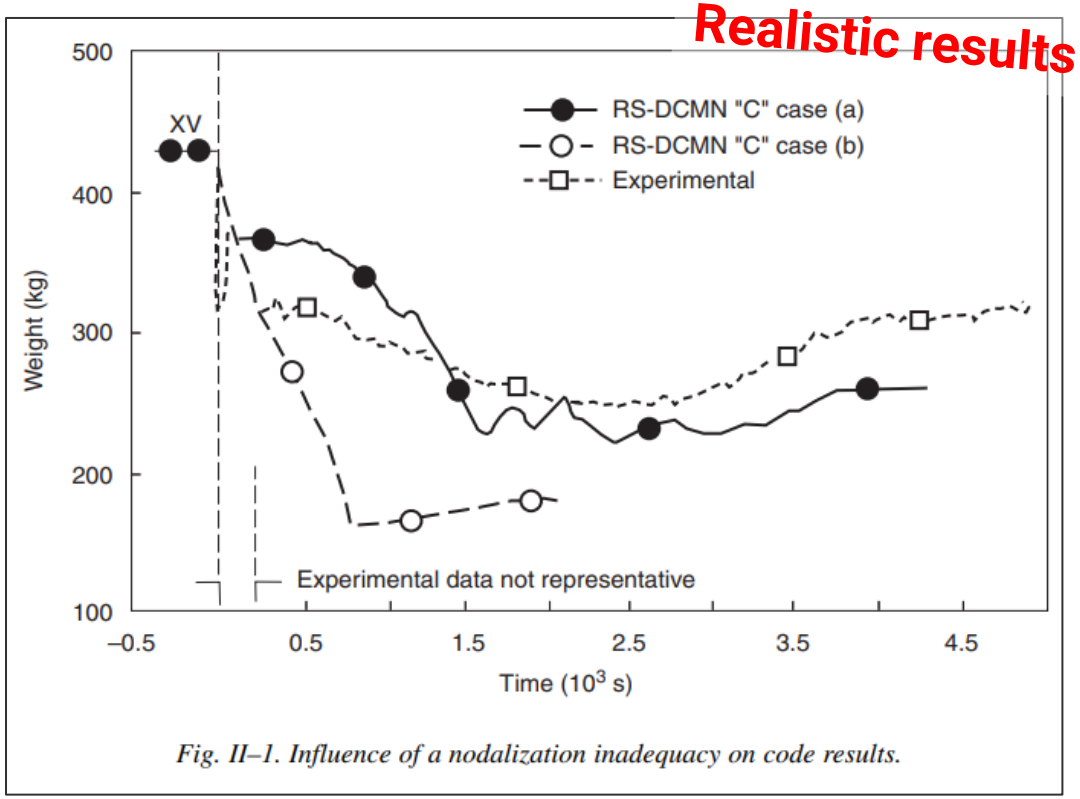


Fig. II–1. Influence of a nodalization inadequacy on code results.

Development of AM procedures and guidelines

Accident management procedures and guidelines should be developed to implement the strategies and measures in the **preventive and the mitigatory domains** (contains instructions on use of equipment, equipment limitations, cautions and benefits)

Preventive	Emergency Operating Procedures (EOPs)	Actions to prevent the escalation of an event into a severe accident
Mitigatory	Severe Accident Management Guidelines (SAMGs)	Actions to mitigate the consequences of a severe accident according to chosen strategies, addressing positive and negative consequences of proposed actions and different options

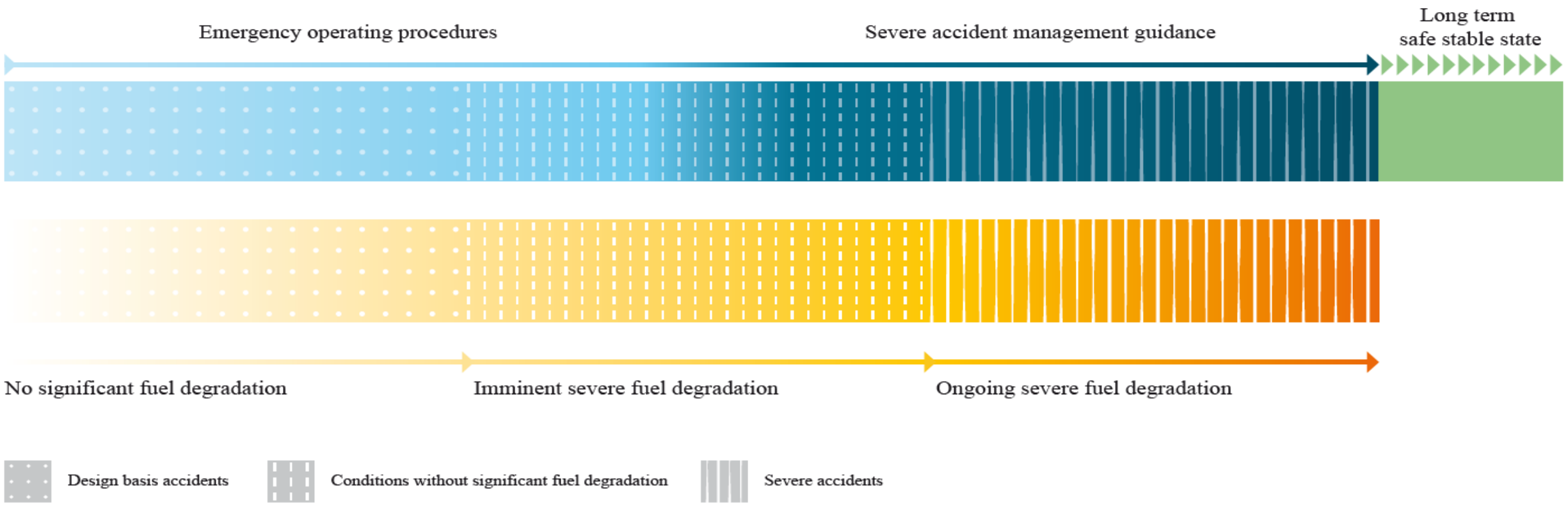
Which is more prescriptive?

The transition point from EOPs to SAMGs should be set with careful consideration of the timing and magnitude of subsequent challenges to the barriers.

Specific and measurable parameter values should be defined for the transition to the use of SAMGs, e.g. core exit temperature.

If the transition point is conditional criteria, the time necessary to confirm the transition point has been reached should be considered.

Summary of Accident management programme



What are the key differences between EOPs and SAMGs?

Hardware provisions for AM

- **Equipment in the mitigatory domain** should be focused on preserving the containment function or minimizing releases when the containment has failed
- To increase the equipment capability or its margin to failure:
  - **Monitoring essential containment** parameters (P,T, radiation, etc.)
  - **Ensuring the leak-tightness of the containment**, e.g. functionality of isolation devices and penetrations for a reasonable time.
  - **Establishing or restoring the ultimate heat sink** (removing heat from the containment and molten core)
  - **Control of combustible gases**, **fission products and other materials released**, including any necessary instrumentation;
  - **Monitoring and control of containment leakages** & fission product releases

Verification and validation (V&V) of AMP

Independent V&V processes should assess:

- accuracy and adequacy of the AMP guidance
- ability of personnel to follow and implement them

Verification process should confirm AMP guidance compatibility with referenced equipment, user aids and supplies.

Validation should be carried out to confirm that the specified actions can be followed by trained staff to manage emergency events.

Possible methods for validation of the SAMGs are the use of an engineering simulator (e.g. full scope simulator) and a tabletop method.

Scenarios should be developed that describe fairly realistic (complex) situations that would require the application of major portions of EOPs and SAMGs.

Responsibilities and lines of authorization

The roles of personnel involved in severe accident management should be considered. There are three categories of functions:

- **Evaluation/recommendation** (e.g. assessment of plant conditions, identification of potential actions, evaluation of the potential impacts of these actions, and recommendation of actions)
- **Decision making** / Authorization
- **Implementation of actions**

In an event that degrades into a severe accident, **transfer of responsibilities from the control room staff to a higher level of authority** should be made at some specified point in time.

Education and training

Specific objectives and training needs should be defined for each group involved in accident management, including:

- plant personnel
- management of the operating organization
- other decision making levels,
- regulatory personnel (where applicable)

Regulators, where they participate in utility decisions, should be trained so that they fully understand the basis of proposed utility decisions.

Exercises and drills should be based on appropriate scenarios that will require the application of a substantial number of procedures and guidelines.

Exercises and drills should reflect to the extent possible the expected conditions.

Updating and Managing Severe Accident Management Programme

Following should be reflected in EOPs and SAMGs during their update (this also related to the relevant organisational aspects of accident management):

- change in plant configuration,
- international research on severe accident phenomena
- exchange of information with peers

Development and update of a severe accident management programme should be the **responsibility of the operating organization.**

Operating organization should integrate all the elements of the severe accident management programme **within its management system.**

- so that the processes and activities that may affect safety are established and conducted coherently for the protection of site personnel, public, environment.

Concluding remarks

IAEA Specific Safety Guide SSG-54 - Accident management programme for NPPs (2019)

- **Provides recommendations on accident management for NPPs**
- **Contains "should" statements:** AMP concept, main principles, forms of Accident Management Guidance, V&V of AMP, roles and responsibilities, development and implementation of a severe accident management programme, training, exercises, drills and updating of SAMP
- **Interfacing with Safety Requirements: Design** (SSR-2/1 Rev.1), **Operation** (SSR-2/2 Rev.1) **Safety Assessment** (GSR Part 4 Rev.1), **Leadership and Management** (GSR Part 2) and **Preparedness and Response** (GSR Part 7)
- **Next revision of SSG-54** is planned to be initiated in 2028

Thank you!

Safety-Standards.Contact-Point@iaea.org

Annex

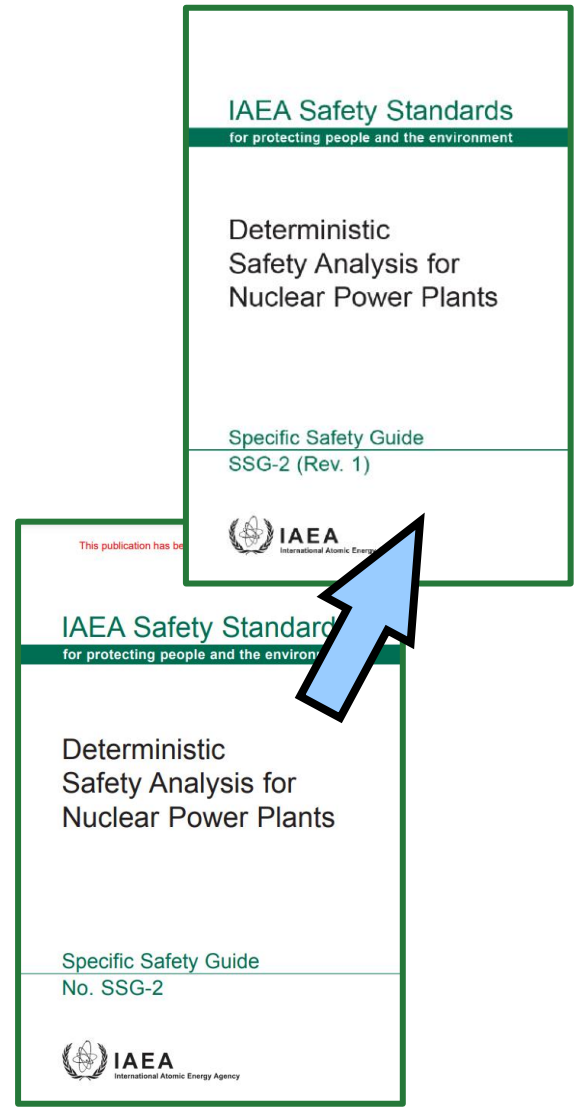
SSG-2 (Rev.1)
Deterministic Safety Analysis

IAEA Specific Safety Guide SSG-2 (Rev. 1): Deterministic Safety Analysis for NPPs

Recommendations and guidance for the conduct of DSA of NPPs (old and new) and its applications.

Main contents:

- Identification, categorization and grouping of Postulated Initiating Events and accident scenarios
- Computer codes and plant models for the analysis
- Selection of acceptance criteria
- Approaches for safety analysis of different plant states
- Safety margins and uncertainties
- Applications of deterministic analysis



Objectives of DSA are to:

- **CONFIRM** that safety functions can be performed with the necessary reliability and that the necessary SSC, in combination with operator actions, **are capable with adequate safety margins, to keep radiation doses and releases below acceptable limits**
- **DEMONSTRATE** that the barriers to the release will **maintain their integrity to the extent required**
- **CONTRIBUTE** to demonstrating that:
  - potential radiological consequences of different plant states **are acceptable**
  - possibility of certain conditions arising that could lead to an early or a large radioactive release can be **considered as 'practically eliminated'**

Characteristics of DSA

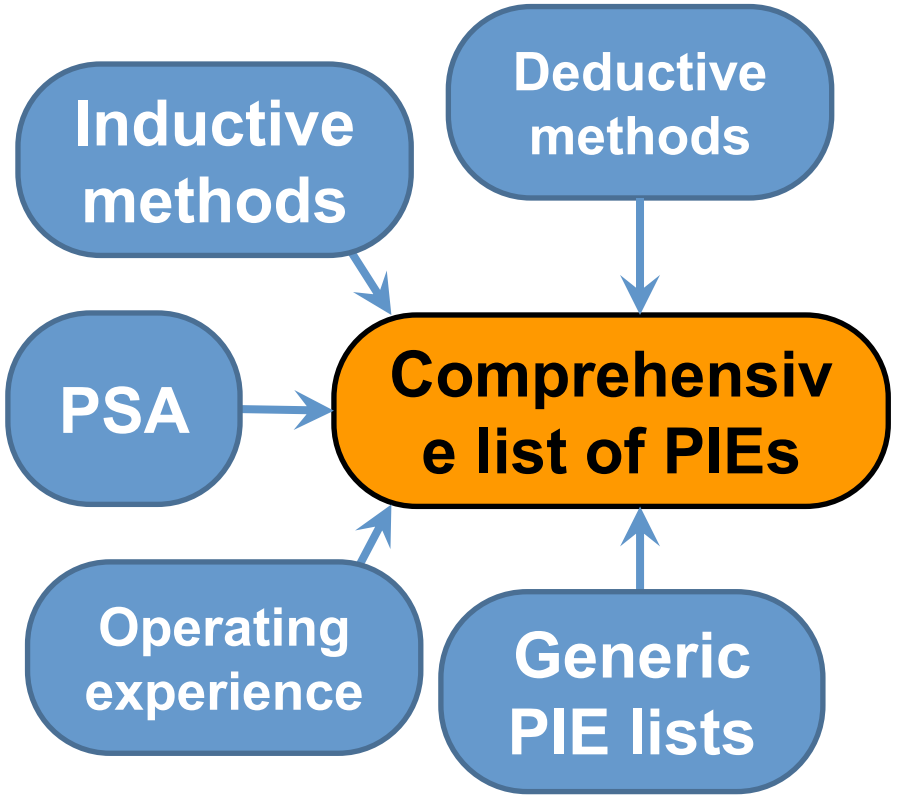
- DSA predicts the response of an NPP to normal operation and to a PIE alone or with additional postulated failures
- Analysis is performed using set of rules **specific for each plant state**
- The results of each analysis is compared with **different acceptance criteria specific for each plant state**
- The computations cover predetermined operating modes and plant states
- They address neutronic, thermohydraulic, radiological, and thermo-mechanical aspects, typically by means of computer codes

Identification of Postulated Initiating Events (PIEs)

Systematic approach should be applied to identify comprehensive set of PIEs such that all foreseeable events with the potential for serious consequences and significant frequency of occurrence are considered.

Combining methods

- **Analytical methods (inductive, deductive)**
  - Hazard and operability analysis (HAZOP)
  - Failure modes and effects analysis (FMEA)
  - Master logic diagrams (MLD)
- **Engineering judgement**
- **Comparison with lists of PIEs of similar plants**
- **Analysis of operating experience**
- **Insights and results from PSAs**



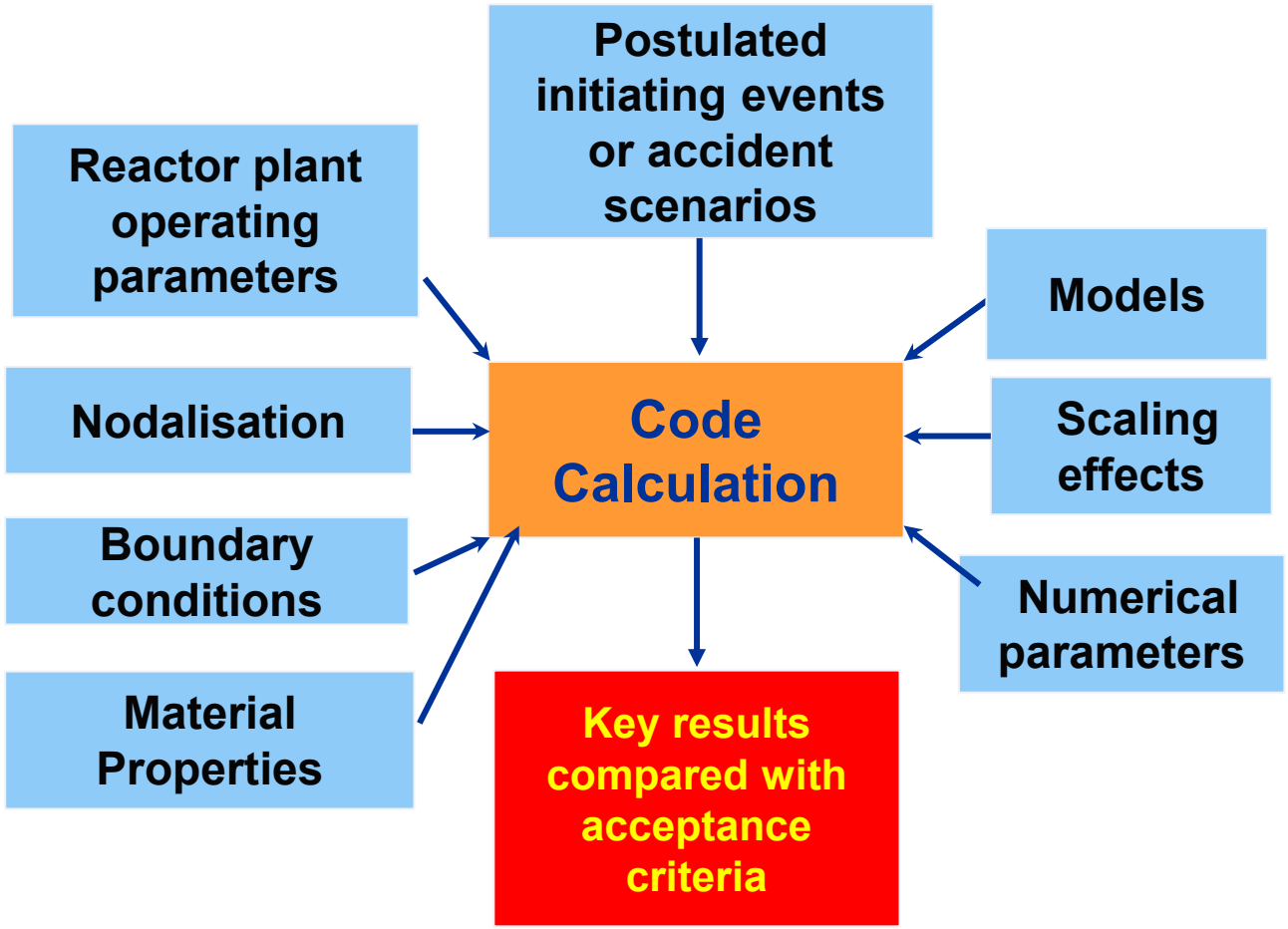
PIE Grouping

- To be grouped on the basis of **frequency of occurrence and impact on plant**
- **Grouping reduces the number of cases for analysis**, considering PIEs similar with respect to safety aspects and dominant phenomena and challenges to safety parameters
- Bounding cases representing the **most severe challenges** to systems and functions are identified from each group
- **PSA should support PIE categorization** in accordance with their frequency of occurrence

Categorization of PIEs

Plant State	*Occurrence (1/reactor-year)*	*Character.*	*Terminology*
Anticipated Operational Occurrences	$> 10^{-2}$ (Expected at least once during the lifetime of the plant)	Expected	Anticipated transients, transients, frequent faults, incidents of moderate frequency, upset conditions, abnormal conditions.
Design Basis Accidents	$10^{-4} - 10^{-2}$ (Chance greater than 1% over the life of the plant)	Possible	Infrequent incidents, infrequent faults, limiting faults, emergency conditions.
DECs without core melt	$10^{-6} - 10^{-4}$ (Chance less that 1% over the life of the plant)	Unlikely	DEC without core melt
DECs with core melt	$<10^{-6}$ (Very unlikely to occur)	Remote	DEC with core melt

Use of computer codes for DSA



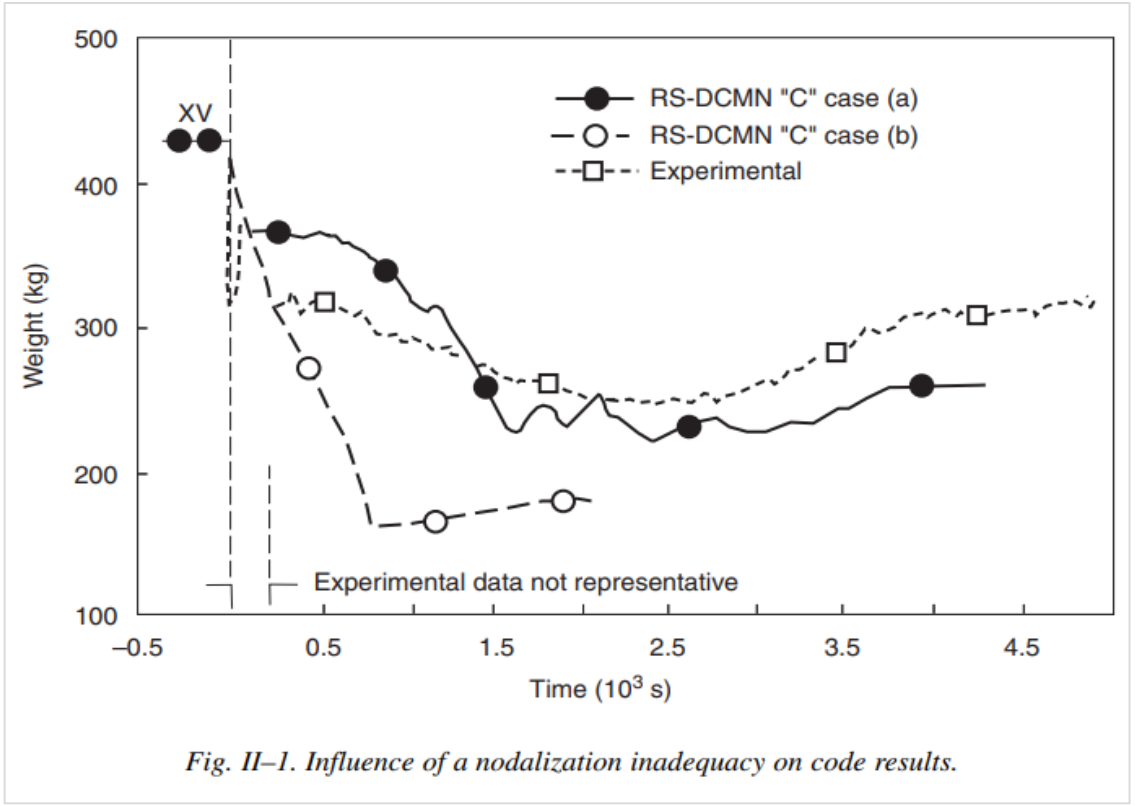
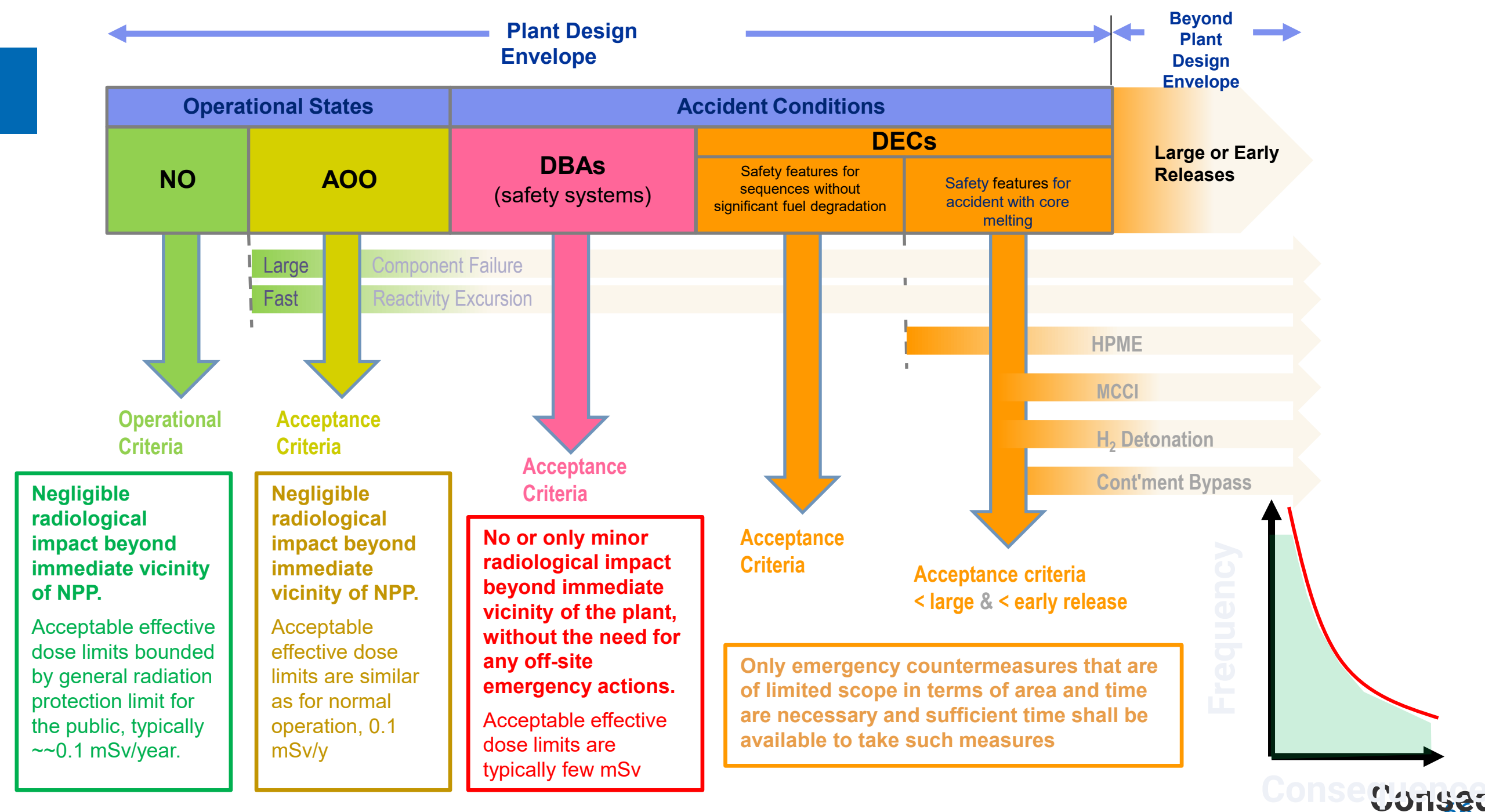


Fig. II–1. Influence of a nodalization inadequacy on code results.

Acceptance criteria for DSA

- **ACCEPTANCE CRITERIA:** values or conditions used to judge the acceptability of the results, expressed as qualitative terms or as quantitative limits.

- **THREE CATEGORIES OF CRITERIA:**
  - **Safety criteria:** criteria that relate either directly to the radiological consequences, or to the integrity of barriers
  - **Design criteria:** design limits for individual structures, systems and components, which are part of the design basis as important preconditions for meeting safety criteria
  - **Operational criteria:** rules to be followed by the operator during normal operation and anticipated operational occurrences


Plant Design Envelope
Beyond Plant Design Envelope
Operational States
Accident Conditions
NO
AOO
DBAs (safety systems)
DECs
Safety features for sequences without significant fuel degradation
Safety features for accident with core melting
Large or Early Releases
Large
Fast
Component Failure
Reactivity Excursion
HPME
MCCI
H2 Detonation
Cont'ment Bypass
Operational Criteria
Acceptance Criteria
Acceptance Criteria
Acceptance Criteria
Acceptance criteria < large & < early release
Negligible radiological impact beyond immediate vicinity of NPP.
Acceptable effective dose limits bounded by general radiation protection limit for the public, typically ~~0.1 mSv/year.
Negligible radiological impact beyond immediate vicinity of NPP.
Acceptable effective dose limits are similar as for normal operation, 0.1 mSv/y
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
Only emergency countermeasures that are of limited scope in terms of area and time are necessary and sufficient time shall be available to take such measures
Frequency
Consequence

Options for performing analysis

Option	Computer code type	Assumptions about 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

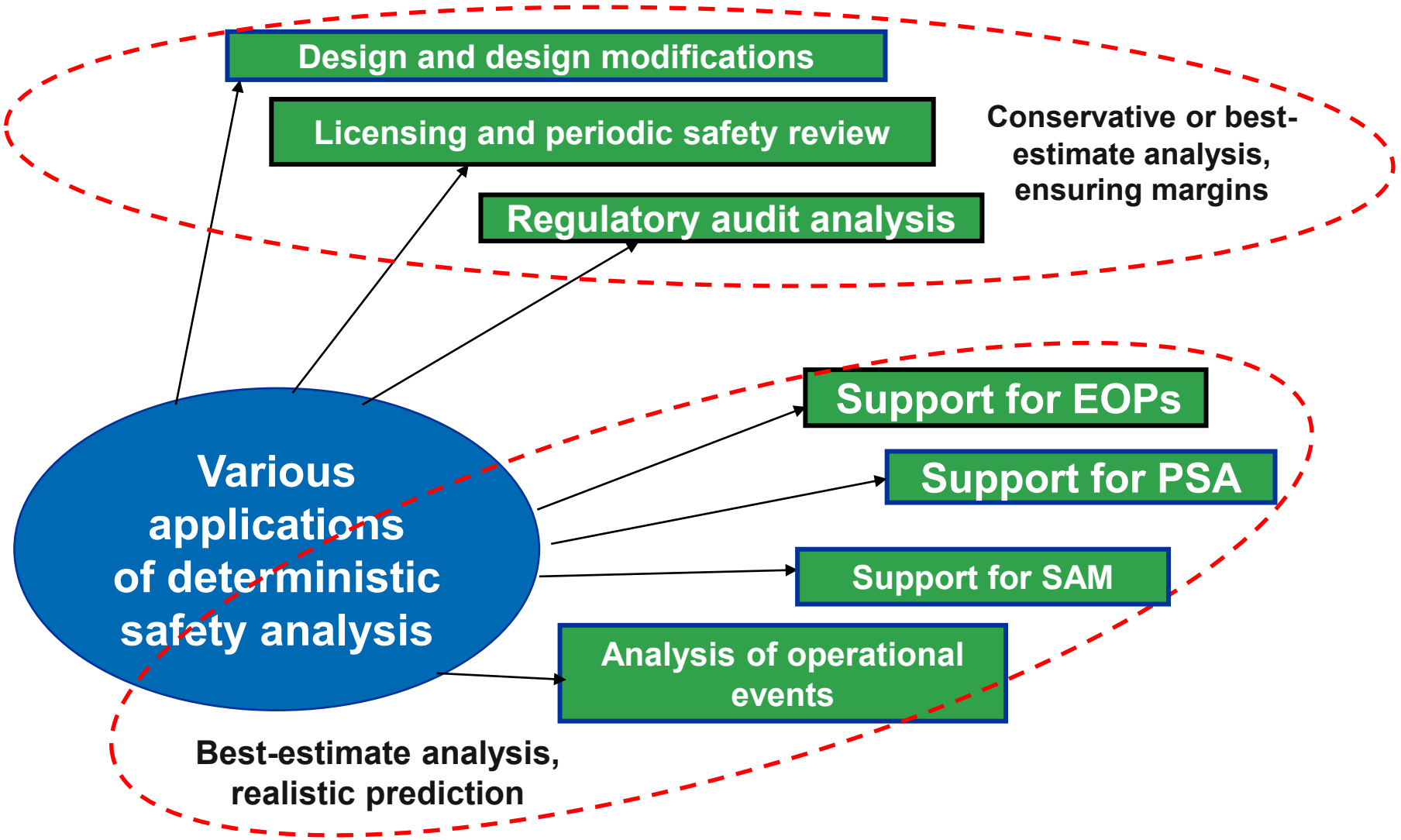
* For simplicity, the terms 'realistic approach' or 'realistic analysis' are used in this Safety Guide to mean best estimate analysis without quantification of uncertainties.

PSA could be used

Assumptions are critical: Example of Conservative Boundary Conditions for a DBA

- Most unfavorable single failure;
- Unavailability of some systems due to preventive maintenance;
- Most unfavorable break location;
- Range of break sizes resulting in highest peak cladding temperature;
- Conservative values for the reactivity feedback coefficients;
- Unfavorable time within the fuel cycle;
- Unfavorable values for the TH parameters
- Temperature conditions for the ultimate heat sink;
- Loss of off-site power;
- Unfavorable initial core power;
- Stuck control rod

Applications of deterministic analysis

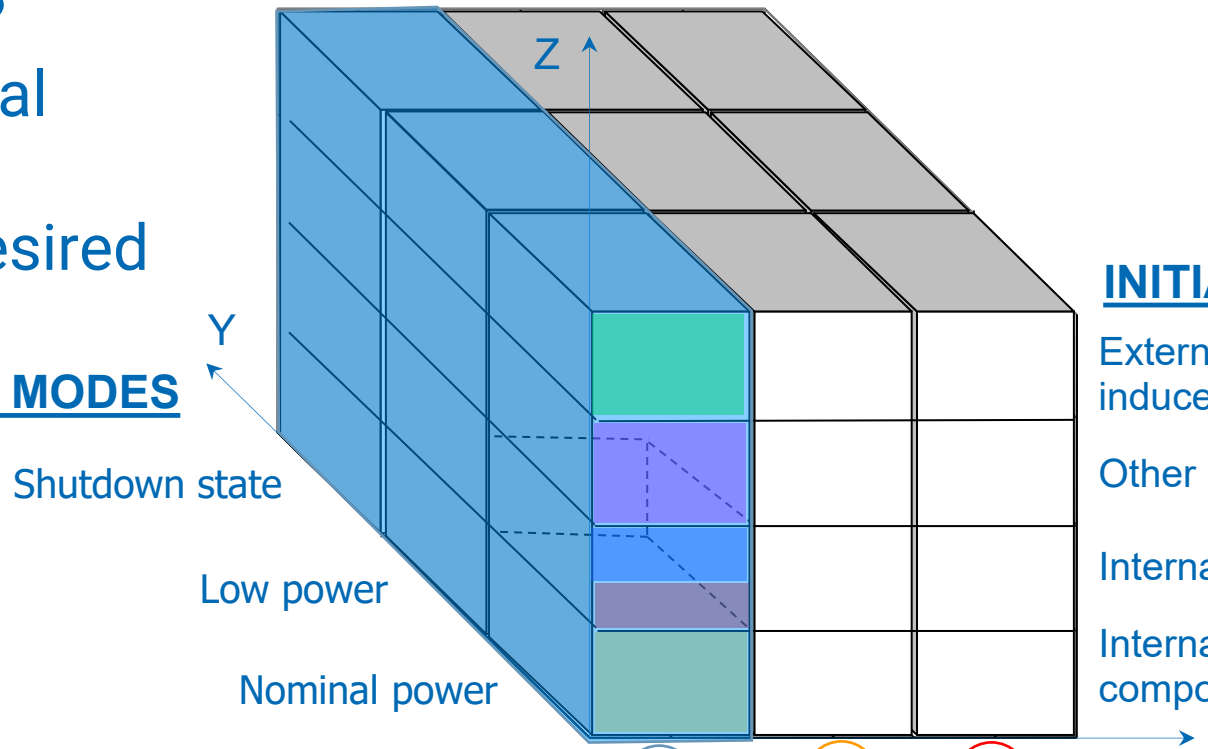


SSG-3 (Rev.1) and SSG-4 (Rev. 1)

Level 1 and Level 2 Probabilistic Safety Assessment

Scope of PSA

1. Which initiators?
2. Which operational states?
3. What is the undesired event?



OPERATING MODES

Shutdown state

Low power

Nominal power

INITIATING EVENTS AND HAZARDS

External hazards (natural and human-induced)

Other internal hazards

Internal fires and floods

Internal initiating events (caused by random component failures and human errors)

1 2 3

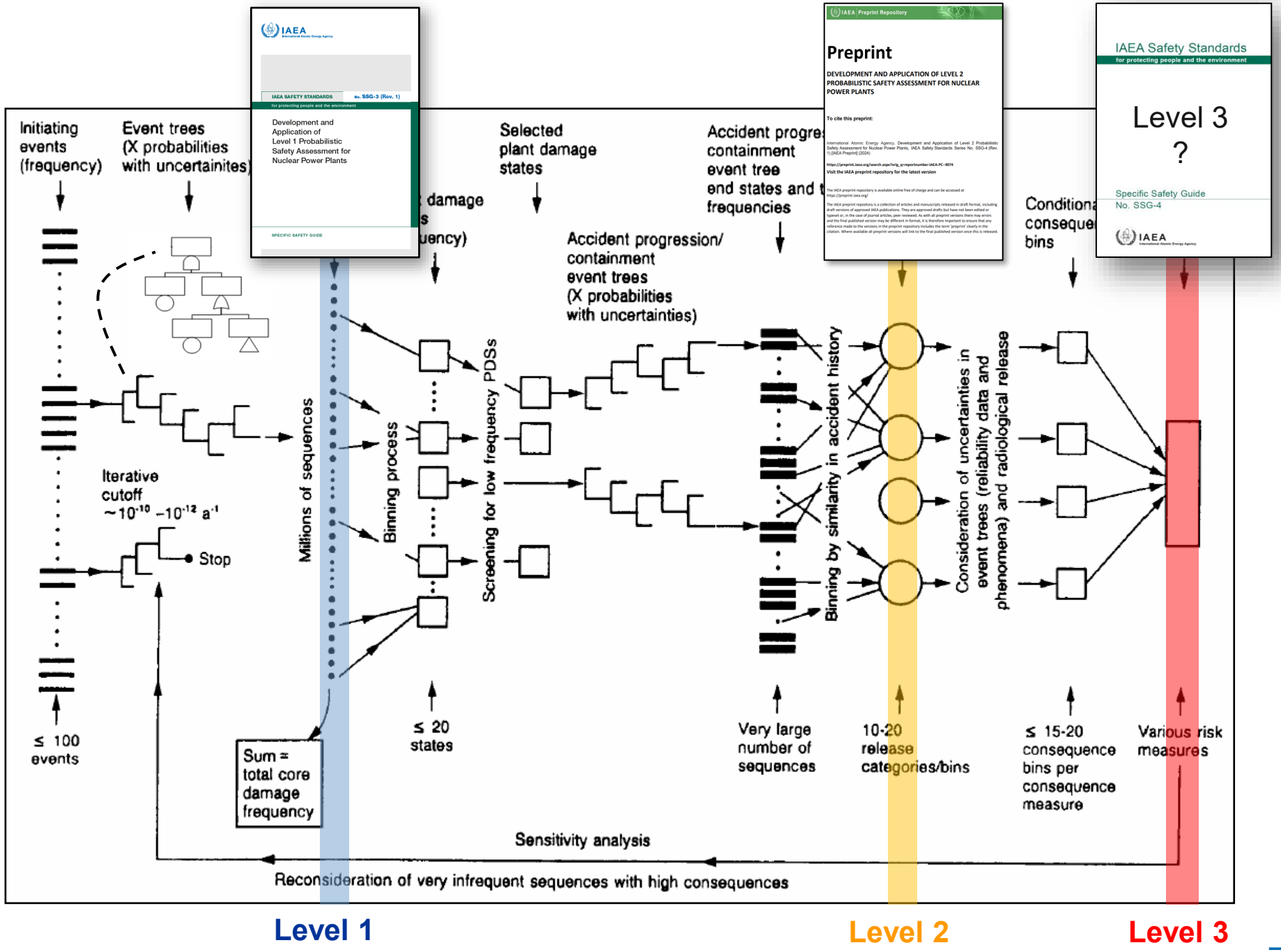
PSA LEVELS
(characterize the extent of accident scenario development)

Core damage frequency

Large early release frequency

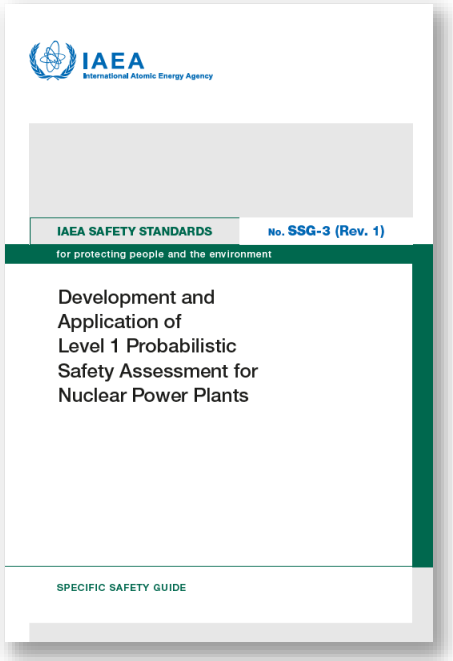
Individual risk of fatality

Overall PSA approach

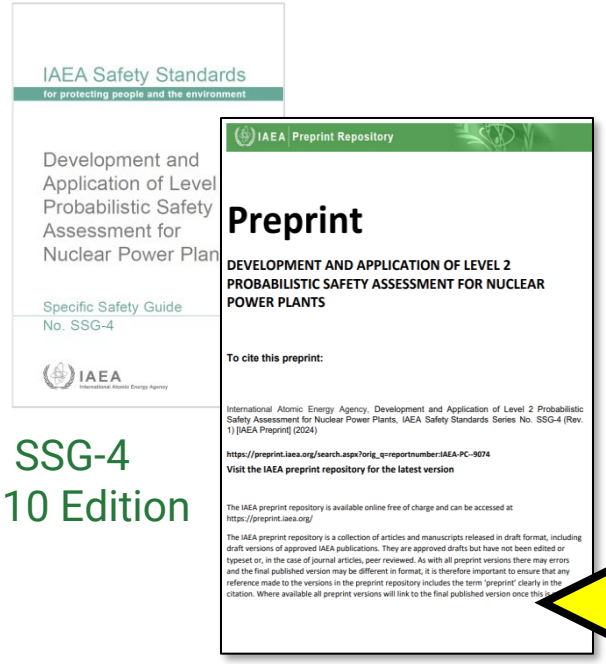


Probabilistic Safety Assessment
SSG-3 (Rev. 1) and SSG-4 (Rev. 1) and more…

SSG-3 (Rev.1)

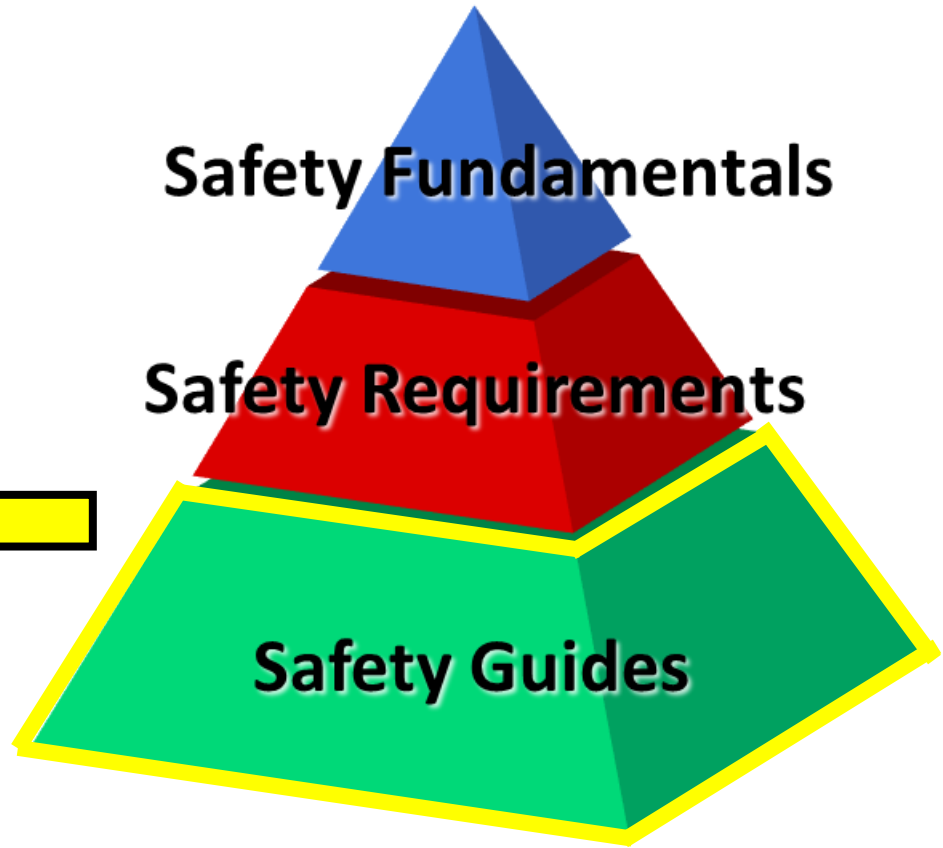


SSG-4 (Rev. 1)



SSG-4
2010 Edition

To be published in 2025



Development and Application of PSA Level 1 & Level 2

- **Scope:**
  - All hazards
  - All operational states
  - For reactor core only
  - Malicious acts excluded

- **No risk goals/criteria** provided (e.g. CDF, LERF), only as examples

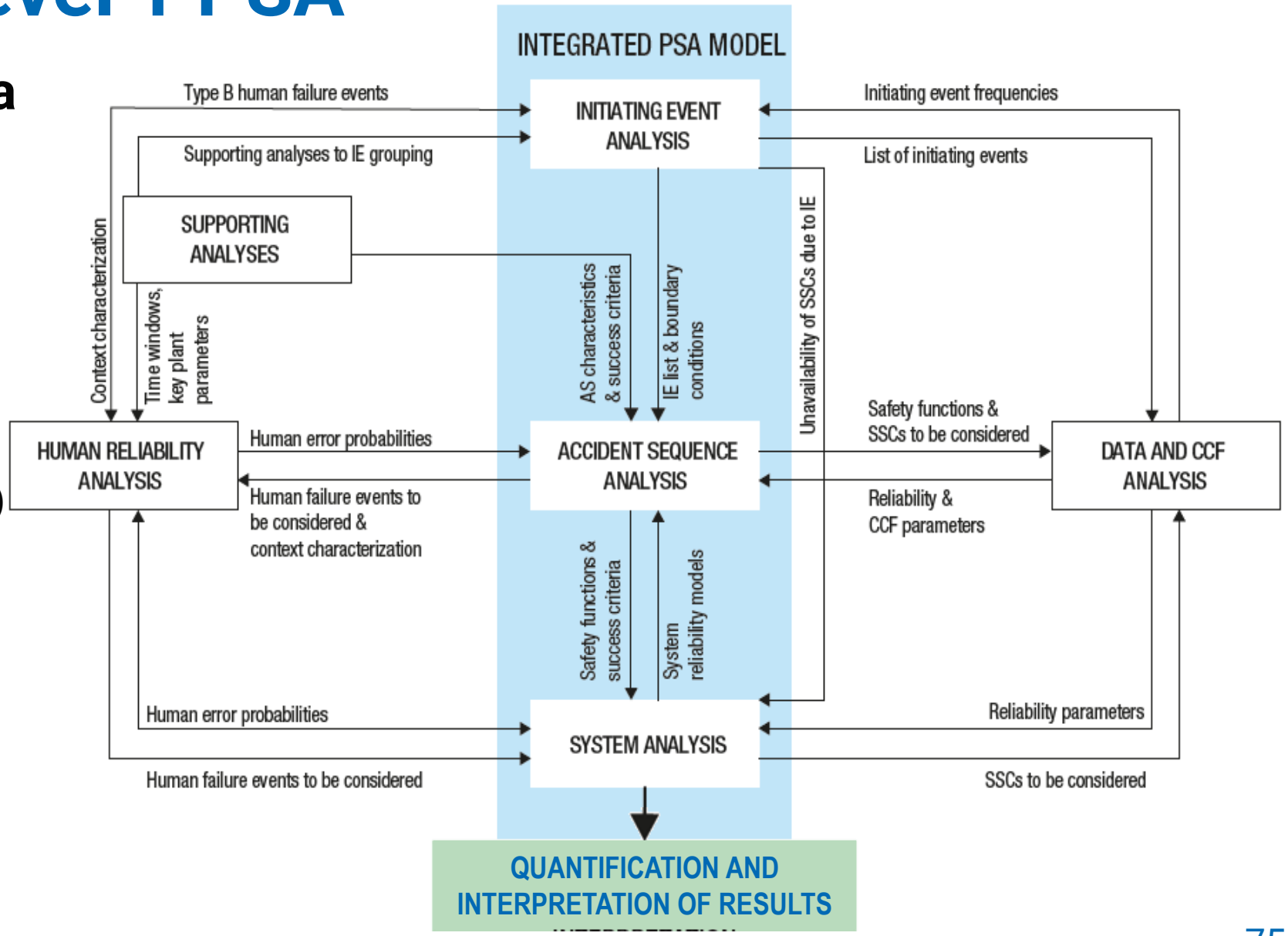
- **Supplemented with examples** & illustrative annexes (e.g. examples of plant operational states and associated initiating events)

SSG-3 (Rev.1): Level 1 PSA

Presents Level 1 PSA as a structured process

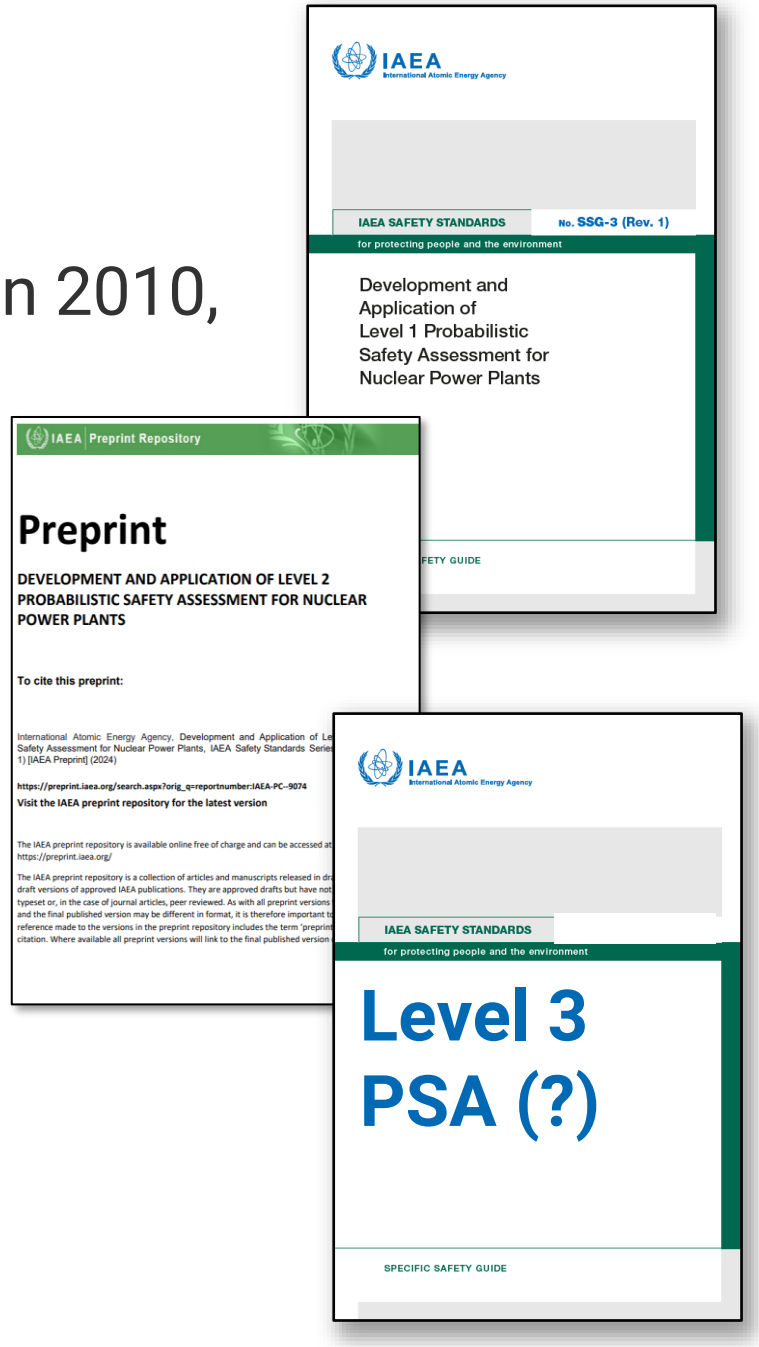
Recommendations on:

- L1 PSA project management and organization
- L1 PSA for internal events (major tasks – IE, accident analysis, system analysis, Human Reliability Analysis, etc.)
- L1 PSA for internal and external hazards
- PSA for Low Power and Shutdown States
- Multi-unit considerations and Spent Fuel Pool
- Use and Application of Level 1 PSA



Revision of PSA safety guides

- **SSG-3** (L1 PSA) and **SSG-4** (L2 PSA) published in 2010,
- **SSG-4 (Rev.1)** pre-print published
- **Scope**: L1&L2, all operating states, all hazards
- Currently under **revision**:
  - Spent Fuel Pool and Multi-unit considerations
  - Passive & software systems reliability
  - Modelling of the portable equipment
  - HRA developments (e.g. EOC)
  - More on combination of hazards
  - Recent developments in PSA applications
  - Feedback to current guides (e.g. from CPWG)
- Plans for New Safety Guide on **Level 3 PSA**



PSA scope

Undesirable event to be analyzed?

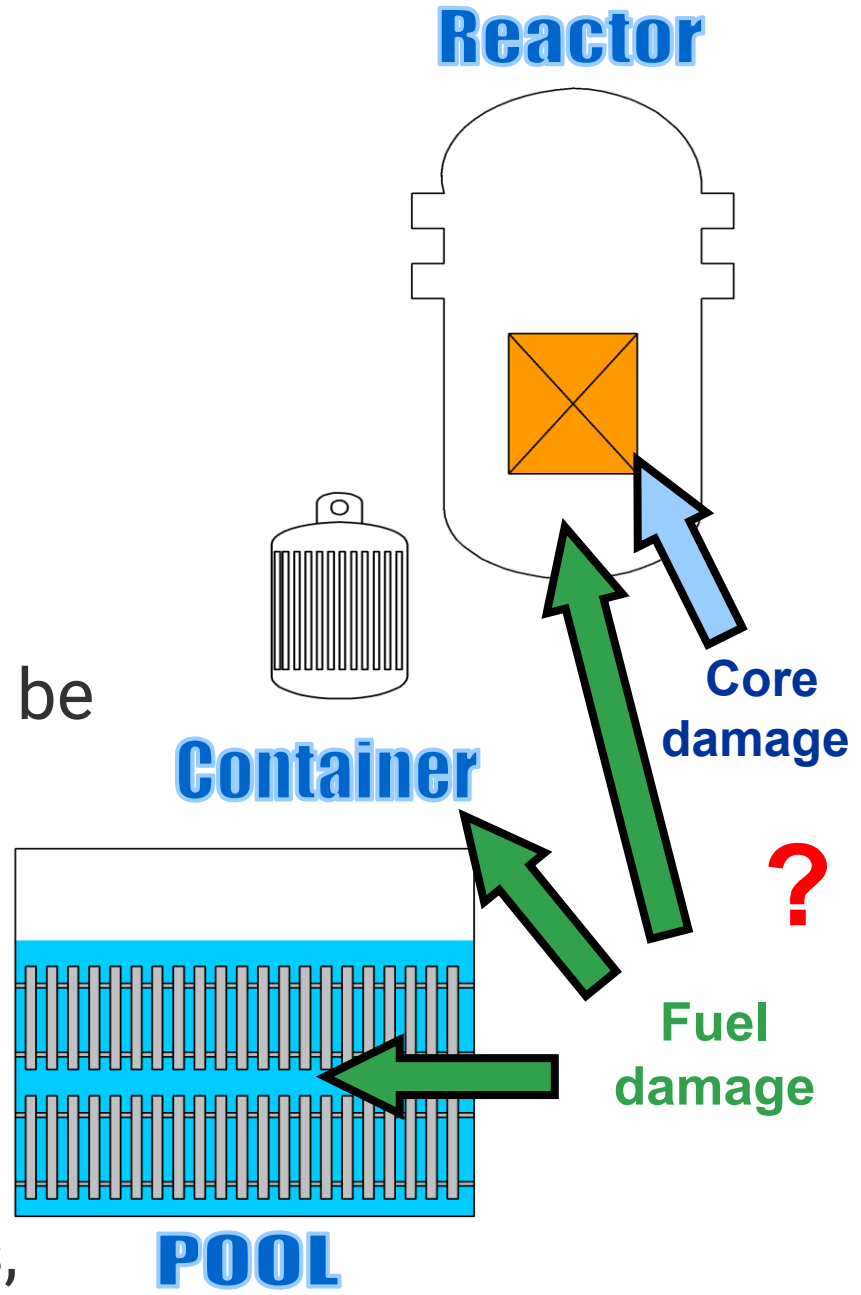
- Reactor core damage, spent fuel pool damage, radioactive release, etc.
- even financial losses could be analyzed
- Clear definition of undesirable event should be done (e.g. for CDF – 1200^{o}C, etc.)

Regimes to be analysed?

- Full power operation, low power operation, shutdown, etc.

Initiating events to be analysed?

- Internal events, fires, floods, seismic events, winds, etc.



Plant familiarization

- **The plant documentation, SAR and EOP** provide the basic information of the plant responses to the accidents
- **Discussions / interviews** with safety analysts and the utility staff
- **All members of the PSA team should be involved** in plant familiarization initially by the documentation review, then by plant visits
- **Regular contact with plant personnel** is maintained throughout the course of the study
- **Several confirmatory plant visits** during the analysis should be conducted

Initiating Events analysis

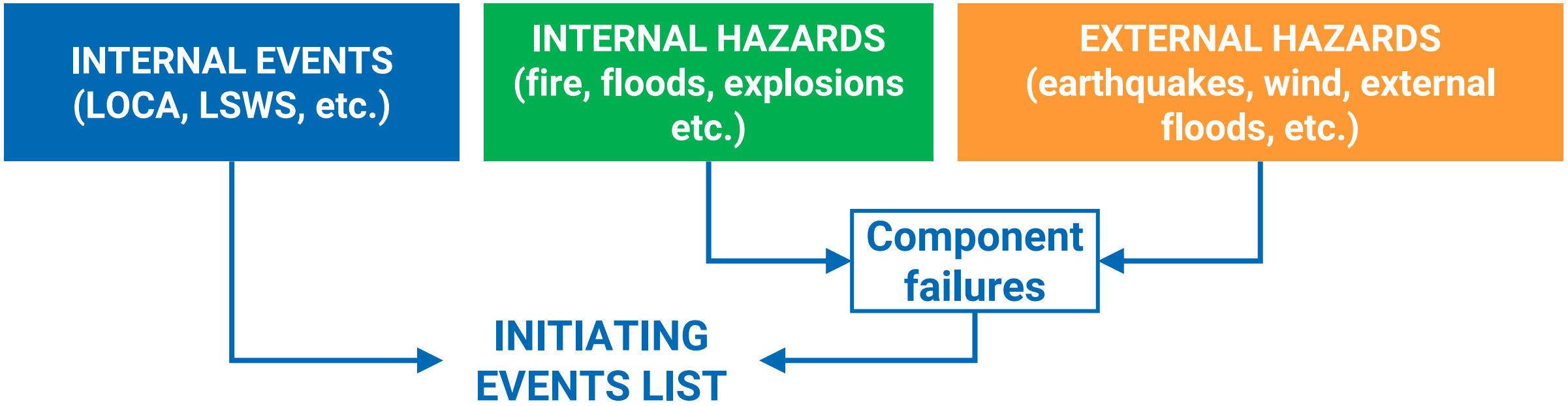
- **Initiating Events (IE) analysis is one of the key PSA tasks** which plays significant role for PSA quality
- **Main objectives** of IE analysis are
  - to identify a (reasonably) **complete** set of IEs
  - to group the identified initiating events so as to facilitate the efficient modeling of plant response

SSG-3 (Rev.1), para 5.11:

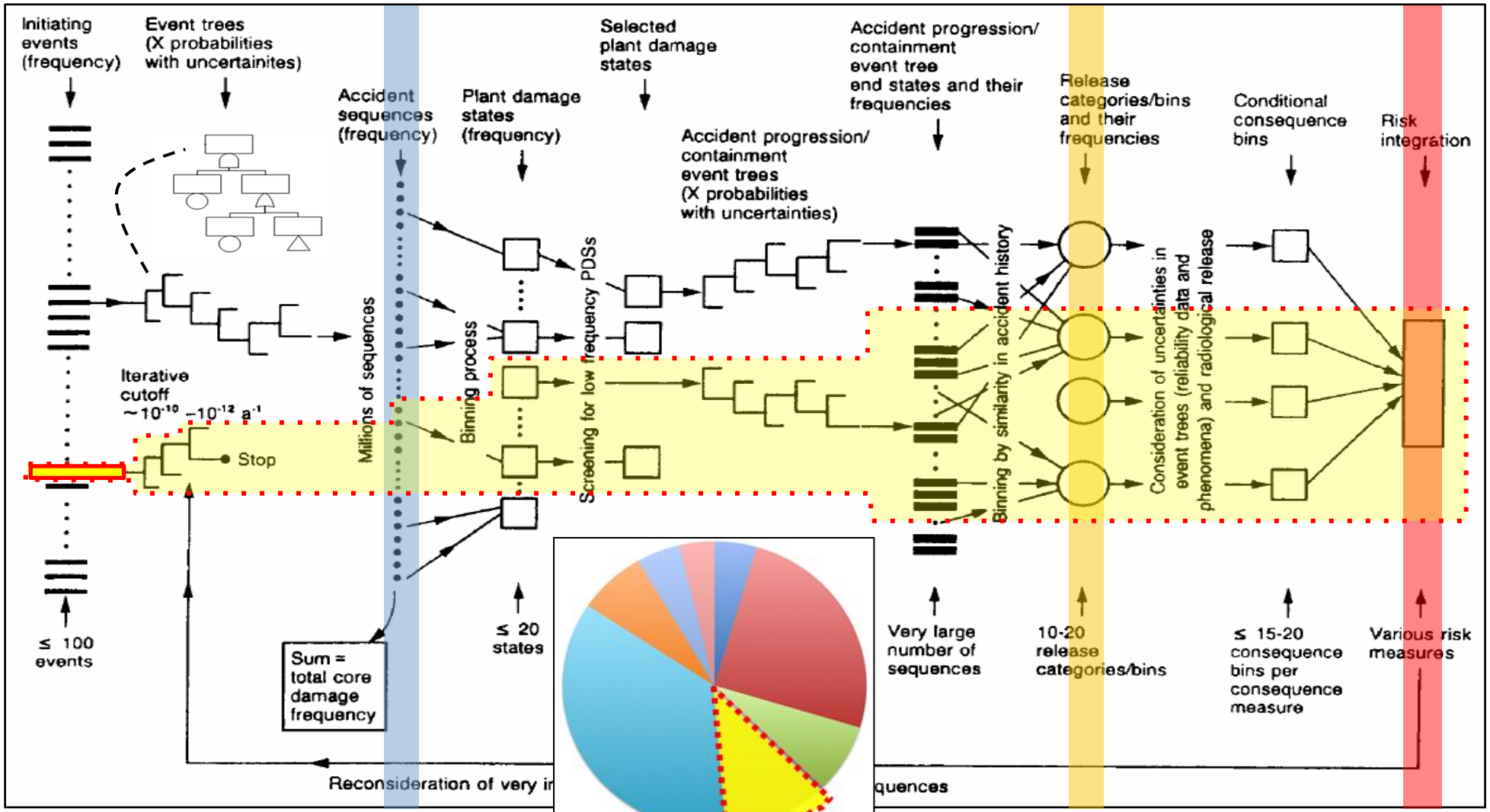
'"… An initiating event is an event that ***challenges normal operation*** *and which* ***necessitates successful mitigation*** *to prevent core damage or* ***can directly lead to core damage****."*

Initiating events analysis

- Initiating events at NPP are caused by **components failures or human errors (internal events)**
- Could be originated by **different type of hazards:** INTERNAL and EXTERNAL HAZARDS

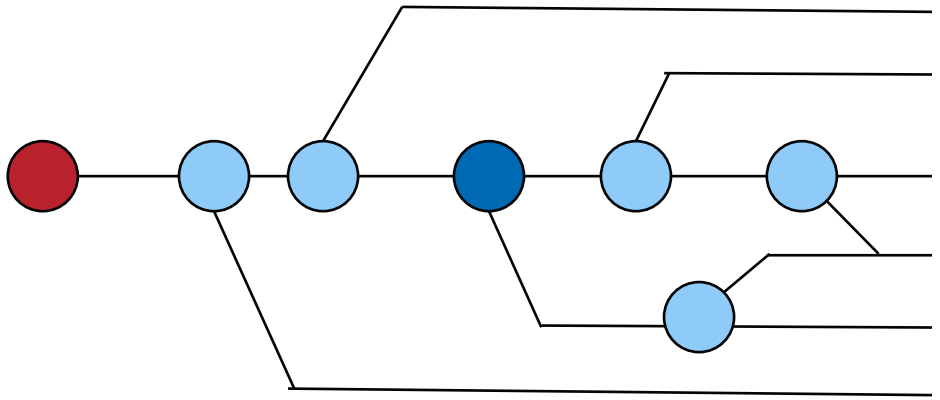


Role of IE analysis is critical



Accident sequence analysis

- Accident sequence is a **chain of events** that link initiator and consequences depending on the success or failure of the mitigating safety and safety related systems

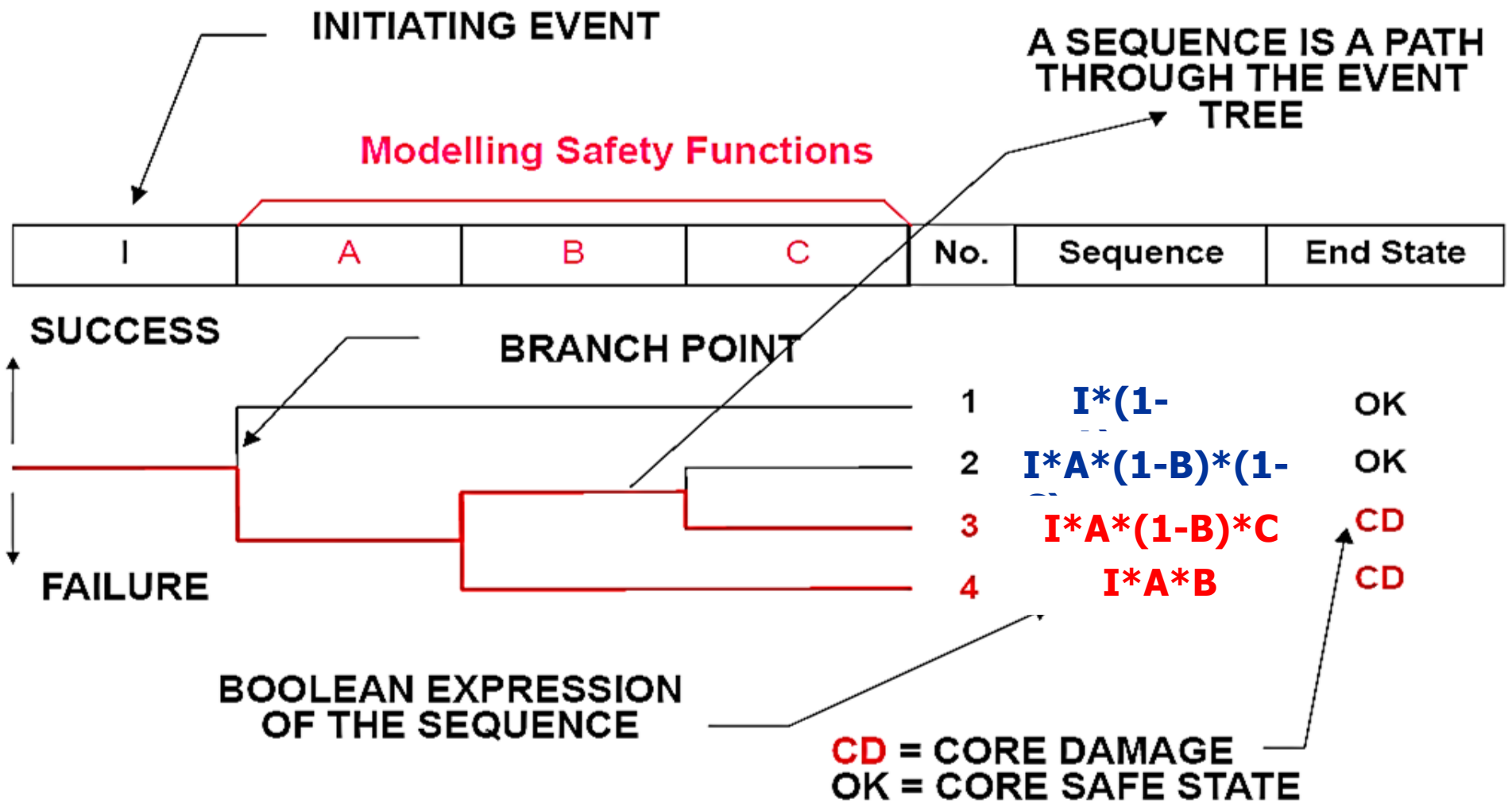


- Consideration of all non-negligible accident sequences in PSA model (in Level 1 PSA the sequences leading to core damage)

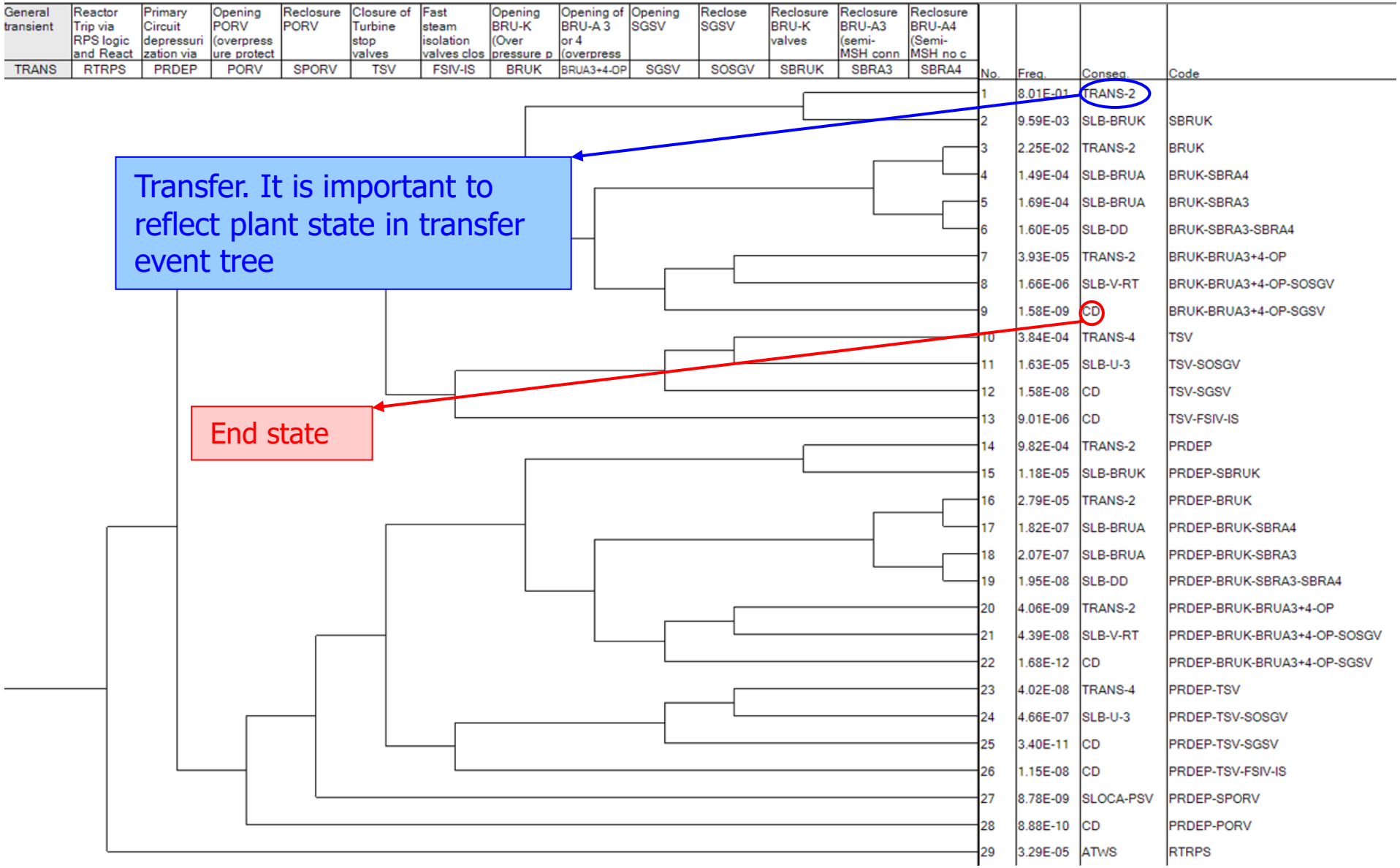
- One of the most used approaches for accident sequence modeling is **EVENT TREE METHOD**

Accident sequence analysis

***Event tree** is constructed based on success criteria identified for particular IE group*



Accident sequence analysis



Component boundary & data

Boundary for components should be defined according to the data analysis

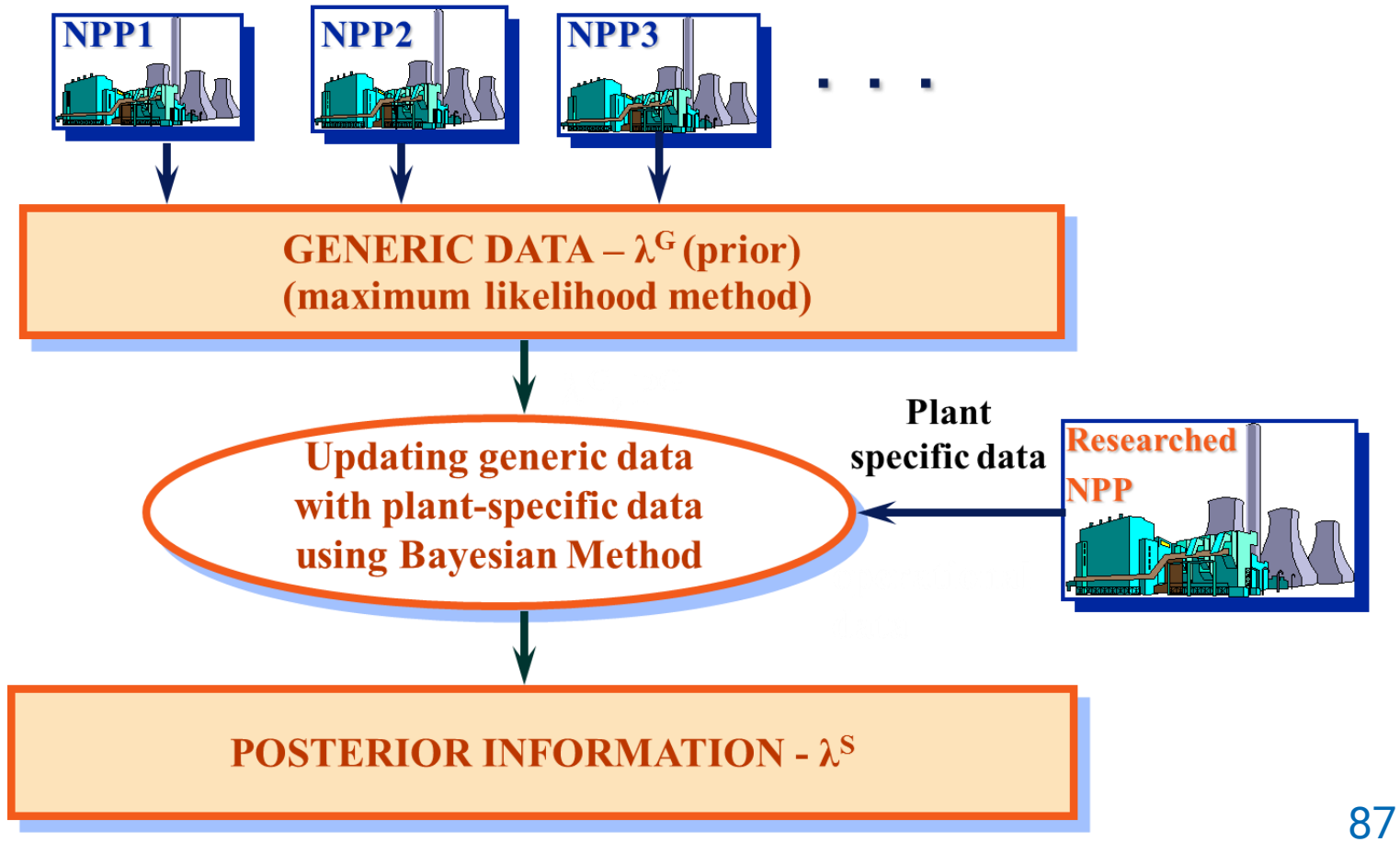
- this **boundary depends on the available data**

No component inside the boundary will be modelled

Data analysis

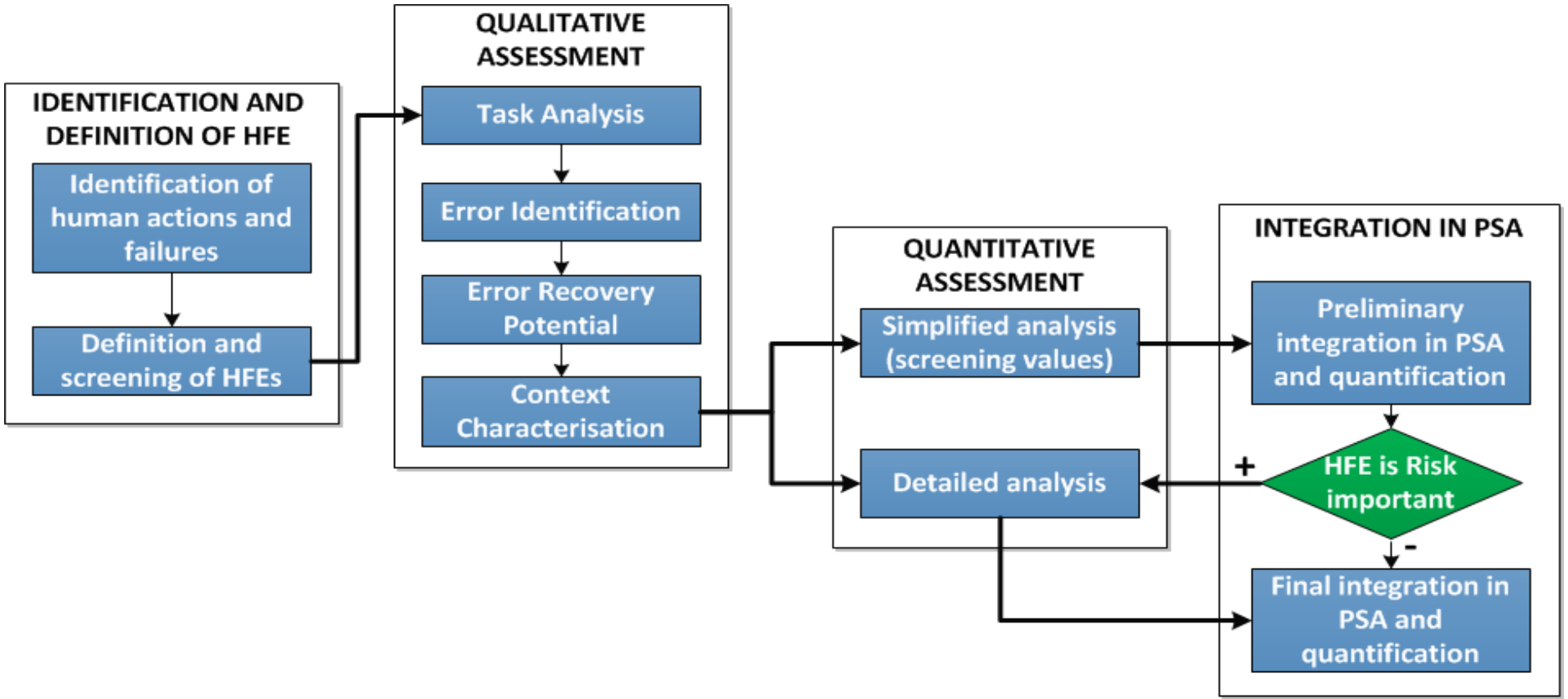
Objective: to provide quantitative information needed to estimate the core damage frequency. Specifically, this activity includes the estimation of:

- **IE frequencies**
- **Component reliability** (failure probability)
- **Component unavailability** due to maintenance
- **Component unavailability** due to testing
- **Common cause failure** probability
- **Human error probability** (next task HRA)



Human reliability

- **Human Reliability Analysis (HRA)** is a complex task designed to evaluate the human performance in the prevailing context
- Ensures that the key human interactions are **systematically identified, analyzed and incorporated in PSA**



Human reliability analysis

- **Several categories of human failure events should be considered**
  - **Type A** – Pre-initiator human errors (calibration, wrong test, etc.)
  - **Type B** – Human errors leading to IEs (human induced LOCA, usually calculated within Initiating Events Frequency; IEF)
  - **Type C** – Post-initiator human errors (failure to perform required actions in response to an initiator - failure of diagnosis or implementation - usually most critical human errors)
- **Recovery errors** (sub-Type of Type C) – represent operator failure to manually actuate or manipulate equipment that has failed to actuate automatically, or establish alternatives to failed functions

Errors of omission/ commission

ERROR OF OMISSION

- Failure to carry out a required procedure or a step in a procedure

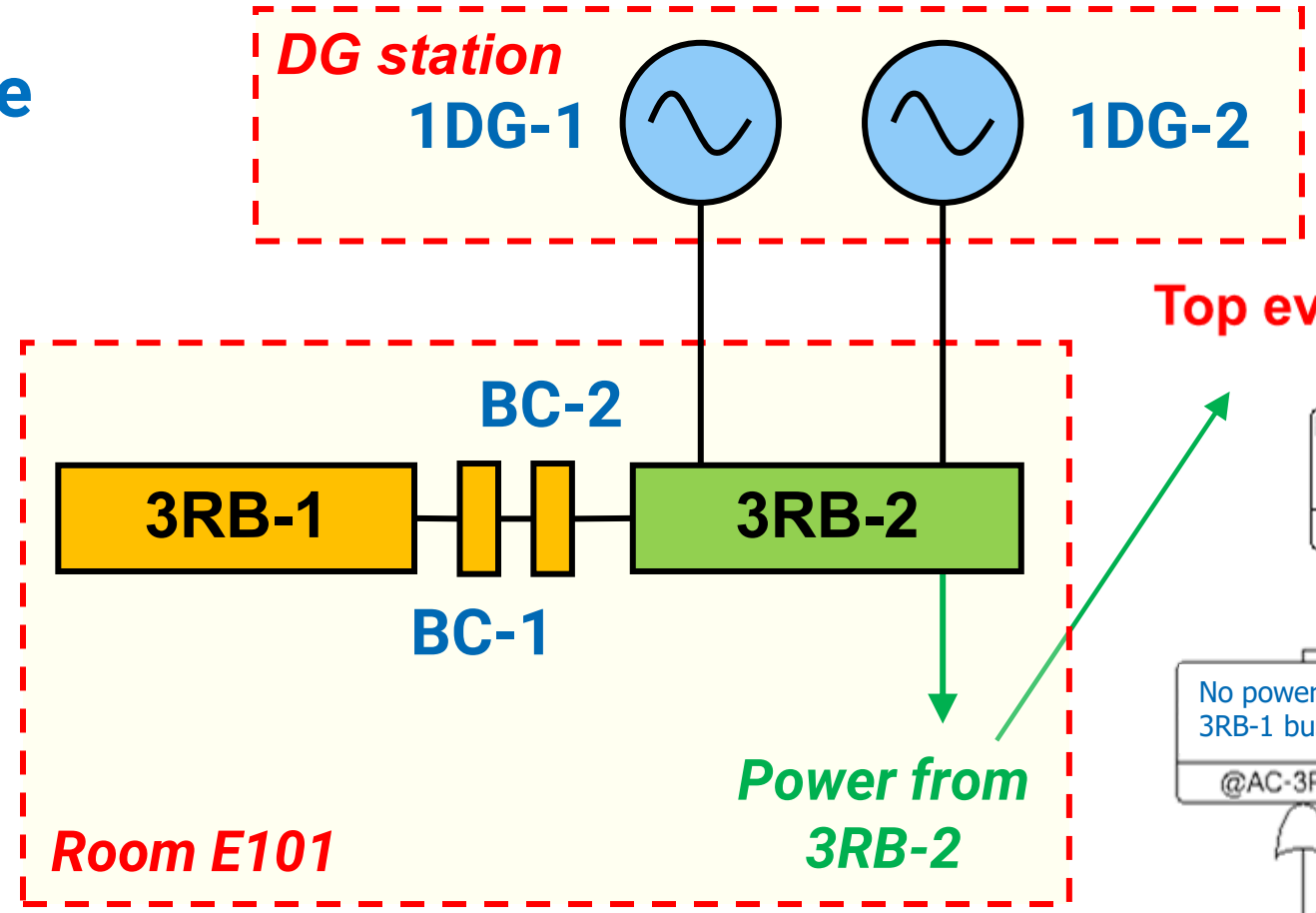
ERROR OF COMMISSION

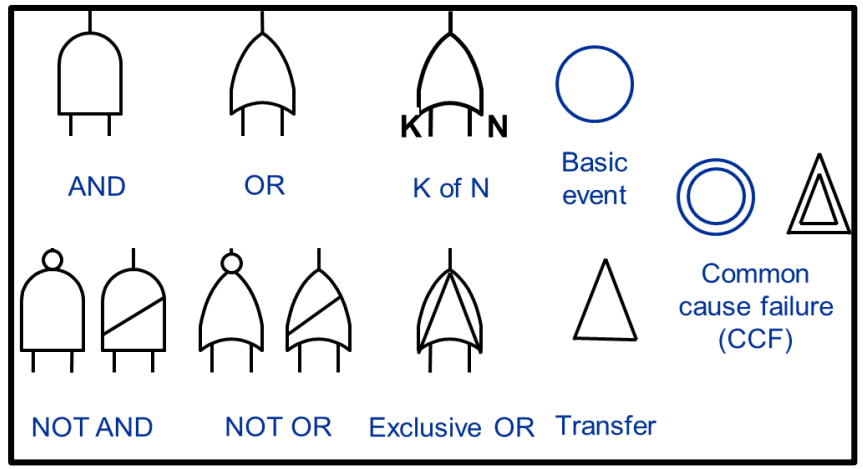
- Carries out an action incorrectly (opening valves in system A rather than system B)
- Carries out an additional, unrequired action (opening valves that are not required to be opened in the procedure being carried out)

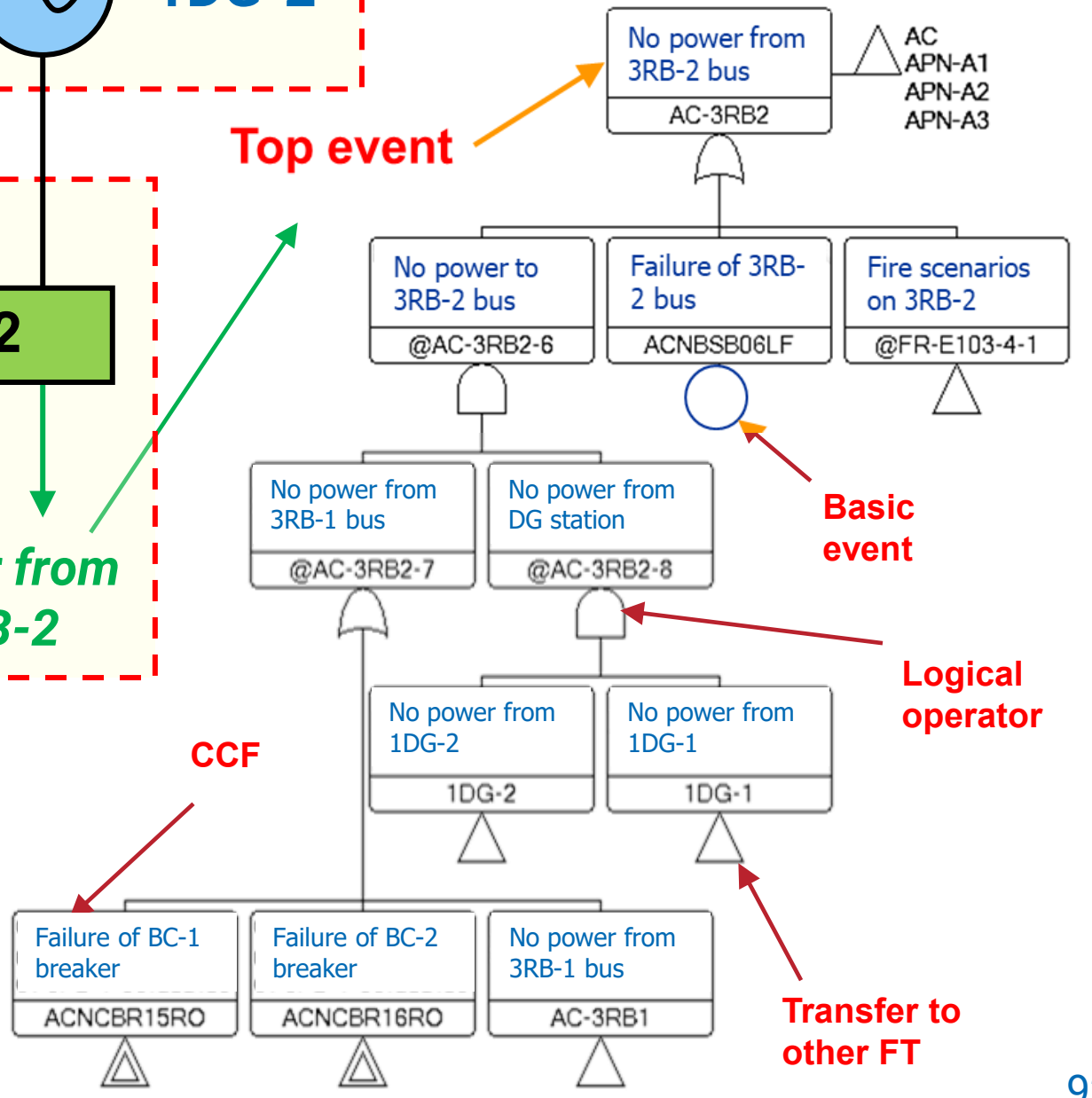
System analysis

- Aim of system analysis in PSA is to develop **logical model which reflects dependency of system operation from various factors**
- **Different methods** for system reliability model construction (fault tree method, GO-schemes, Markov chains, etc.)
- The most popular method is **FAULT TREE METHOD**
- It should contain:
  - Relevant **component failures**
  - Outages from **testing, maintenance and repairs**
  - **Human errors** including dependencies between human actions
  - Failures of **supplies and supports** (normally handled through transfers to the fault trees of supplies and supports)
  - **Common Cause Failures** (CCFs)
  - Failures **induced by Initiating event** (where applicable)

Fault tree example







Quick exercise:

52 cards are in the card deck

What is the probability that queen spades is among the cards that are with you ?

A) 0.33
B) 0.057
C) 1
D) 0

It is important to investigate the plant-specific information in detail

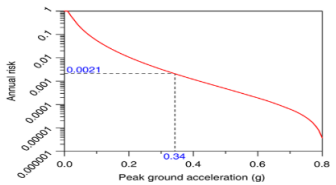
Internal & external hazards

Collection of information

Familiarization with the plant, collection of relevant information, walkdowns, etc.

Selection of hazards

Analysis of generic hazard lists, examination of plant buildings, development of plant-specific hazard list

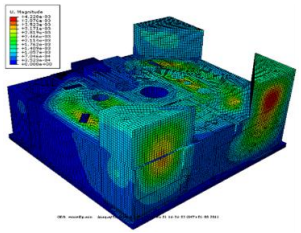


Hazards screening

Screening criteria, quantitative + qualitative screening, hazard parameterization (hazard curves)

Bounding assessment

Conservative assessment of selected hazards impact on NPP safety, selection of critical hazards for detailed analysis



Detailed analysis

Detailed analysis of accident scenarios aimed at realistic estimation of the potential damage

Level 1 & Level 2 PSA

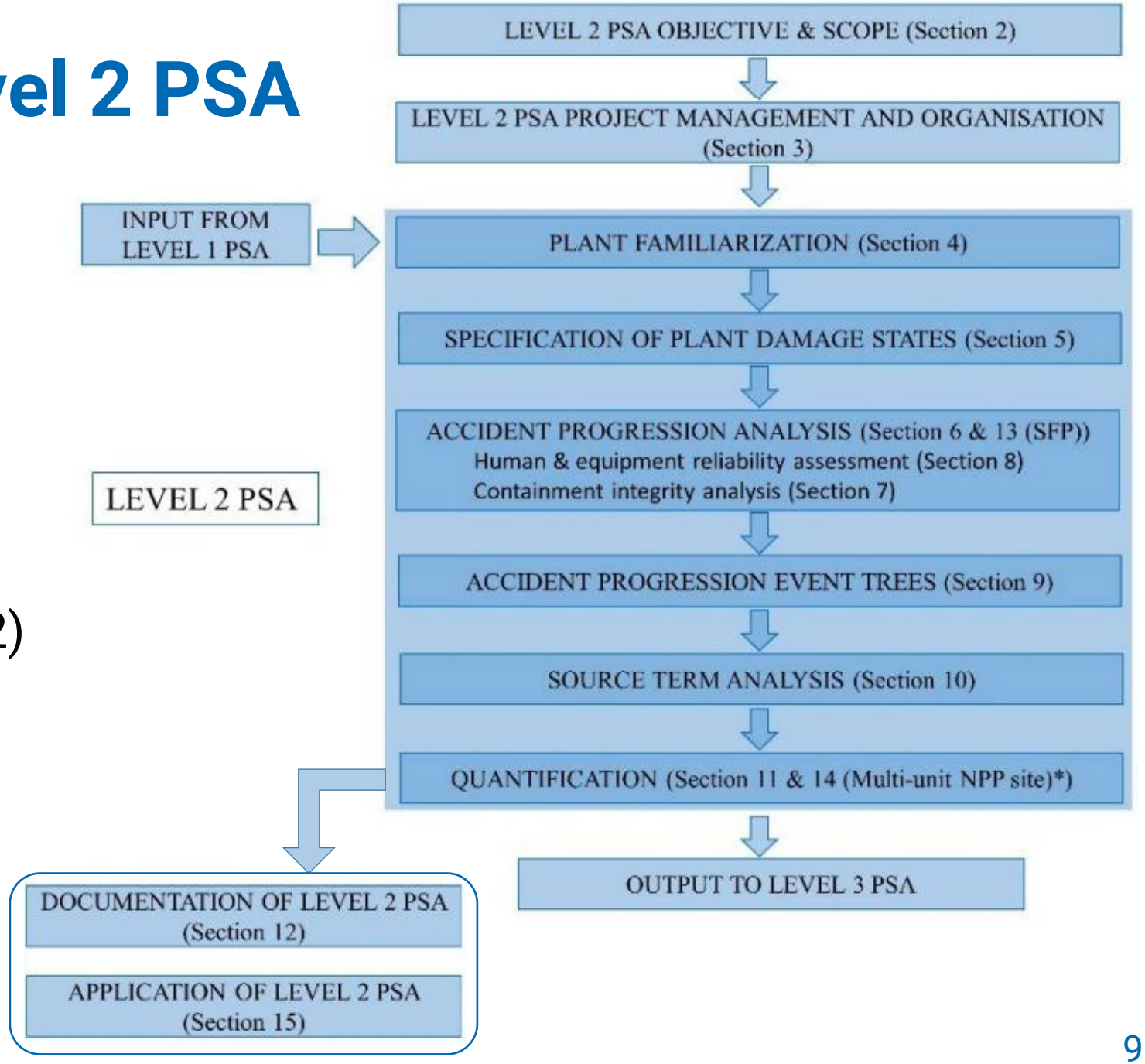
- **Level 2 requires more information than a Level 1 PSA generates**
  - Containment safeguards systems not usually needed to determine ‘core damage’
  - Level 1 event trees built from success criteria can ignore status of front-line systems that influence extent of core damage
- **Event trees create very large number of scenarios to evaluate**
  - Grouping of similar scenarios is a practical necessity
- **Quantification involves considerable subjective judgment**
- **Sensitivity and uncertainty**

SSG-4 (Rev. 1): Level 2 PSA

Presents Level 2 PSA as a structured process

Recommendations on:

- L2 PSA objective & scope
- L2 Project management
- Plant familiarization
- Plant Damage States (L1-L2)
- Accident progression & containment analysis
- Source term analysis
- Quantification
- Documentation & results
- Level 2 PSA applications

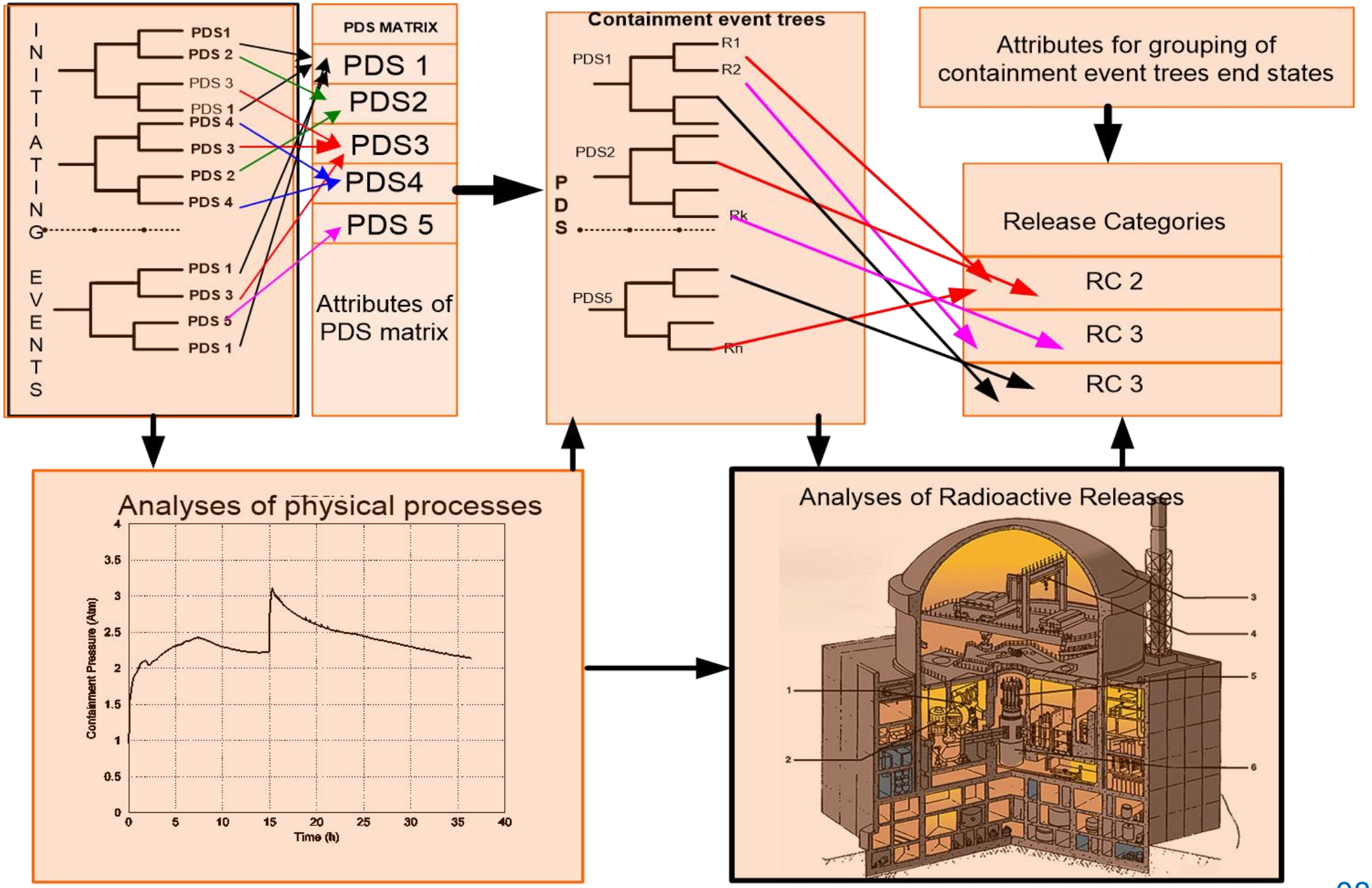


Level 2 PSA

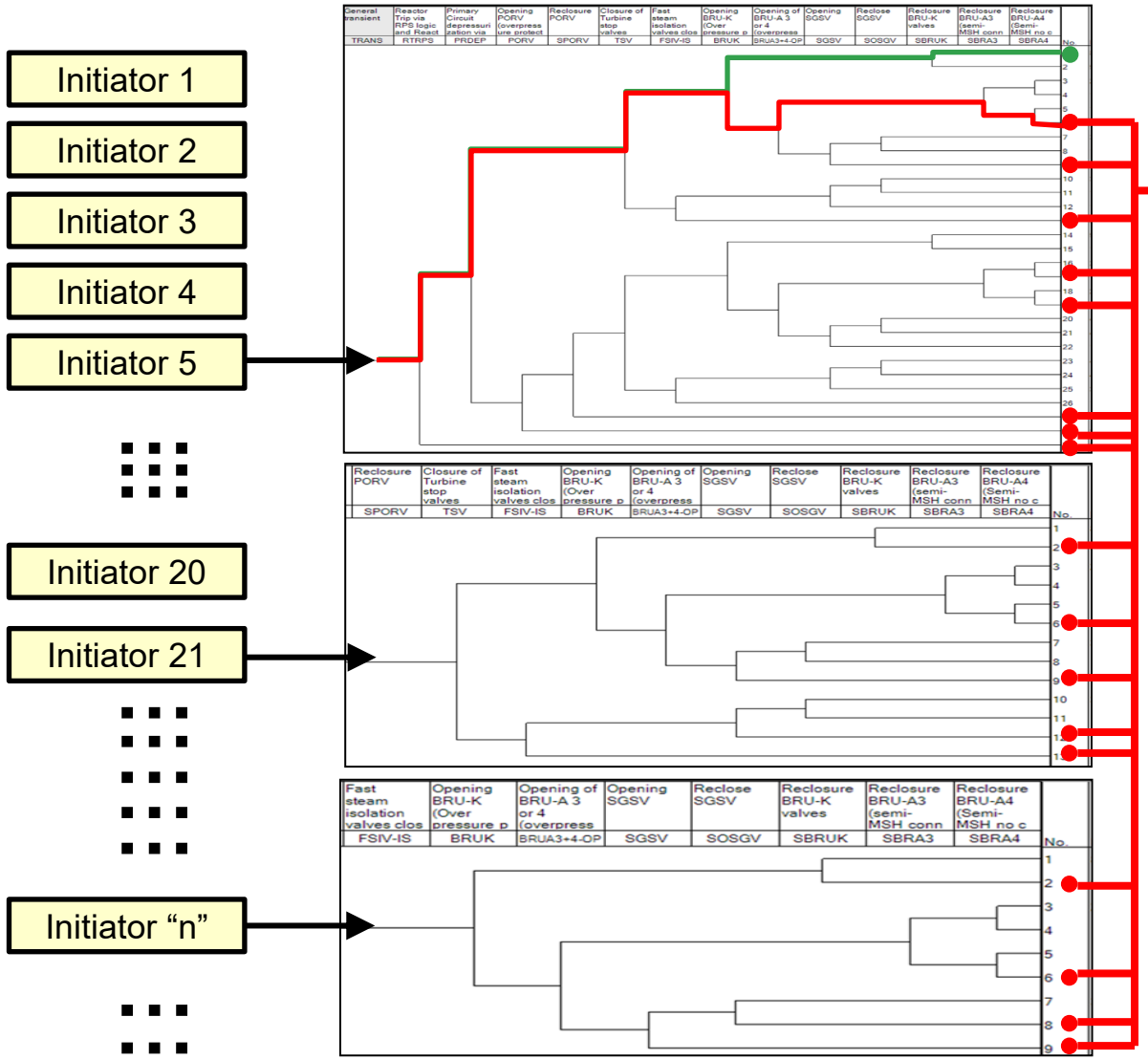
- Adequate level of expertise in the following
  - knowledge of the **design and operation** of the plant
  - knowledge of **severe accident phenomena**
  - knowledge of **containment challenges**, and
  - knowledge of **PSA techniques**

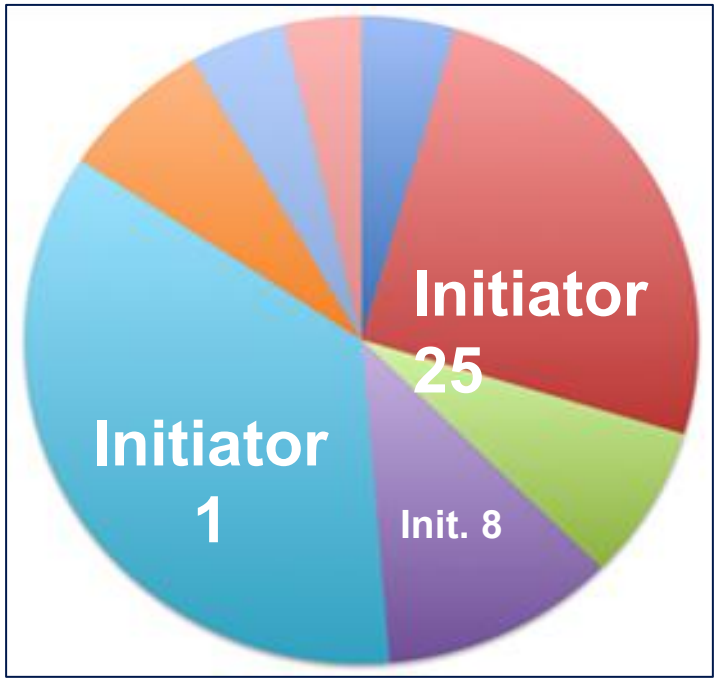
- *„...extensive participation of the plant engineers and utility personnel, or designers if performed at the design stage, and probabilistic safety analysts specialized in accident phenomena and other Level 2 PSA disciplines is essential.”*

Level 2 PSA

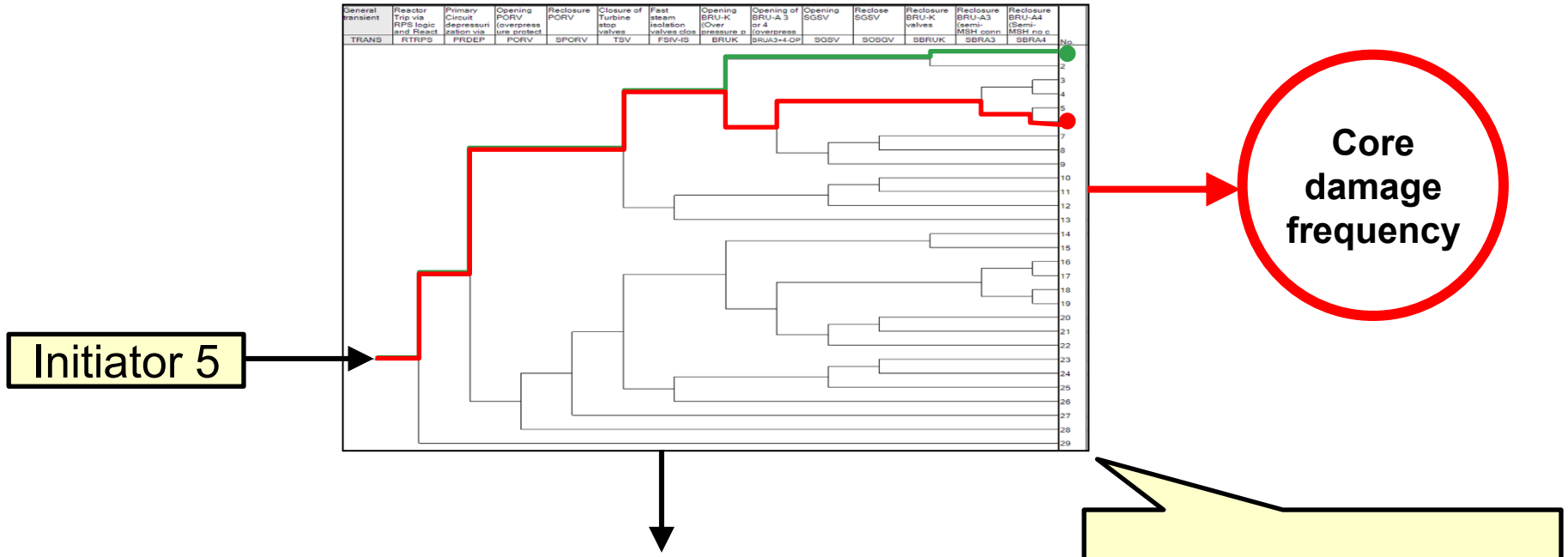

INITIATING EVENTS
PDS1
PDS 2
PDS 3
PDS 1
PDS 4
PDS 3
PDS 2
PDS 4
PDS 1
PDS 3
PDS 5
PDS 1
PDS MATRIX
PDS 1
PDS2
PDS3
PDS4
PDS 5
Attributes of PDS matrix
Containment event trees
PDS
PDS1
R1
R2
PDS2
Rk
PDS5
Rn
Attributes for grouping of containment event trees end states
Release Categories
RC 2
RC 3
RC 3
Analyses of physical processes
Containment Pressure (Atm)
Time (h)
Analyses of Radioactive Releases

Integral PSA model for NPP





Integral PSA model for NPP

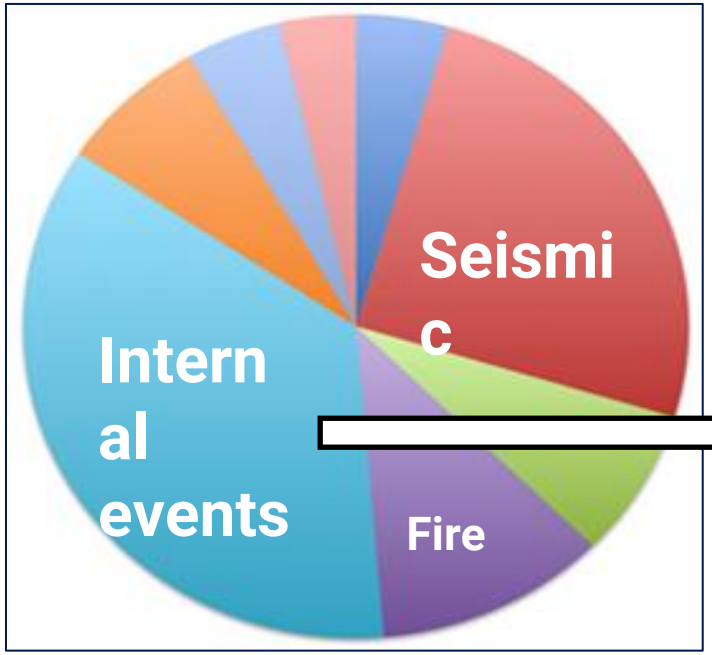


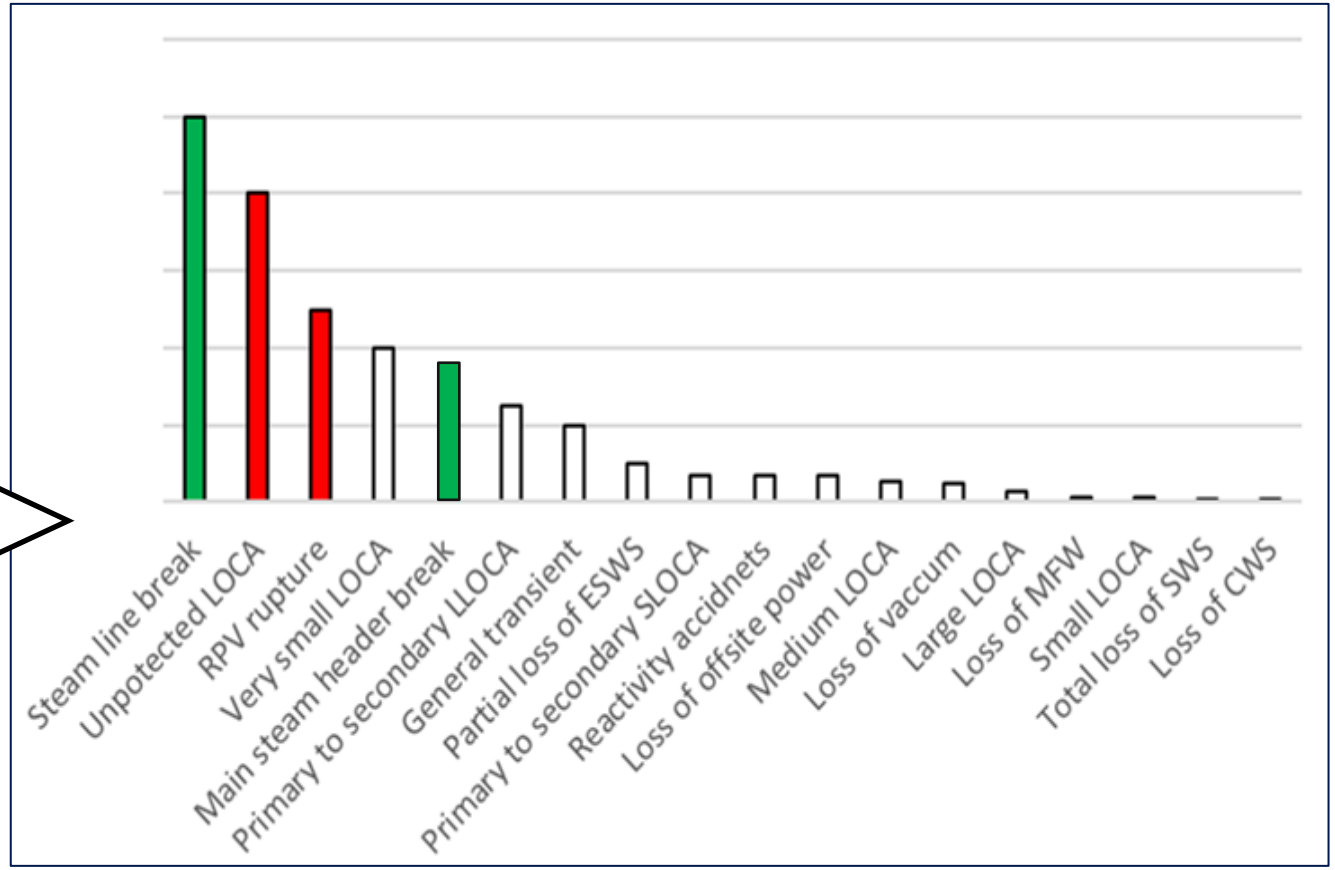
PSA MODELS TAKE INTO ACCOUNT

- Equipment failures
- Adverse conditions
- Unavailability due to maintenance
- Human errors
- Structural failures
- Other potential failures

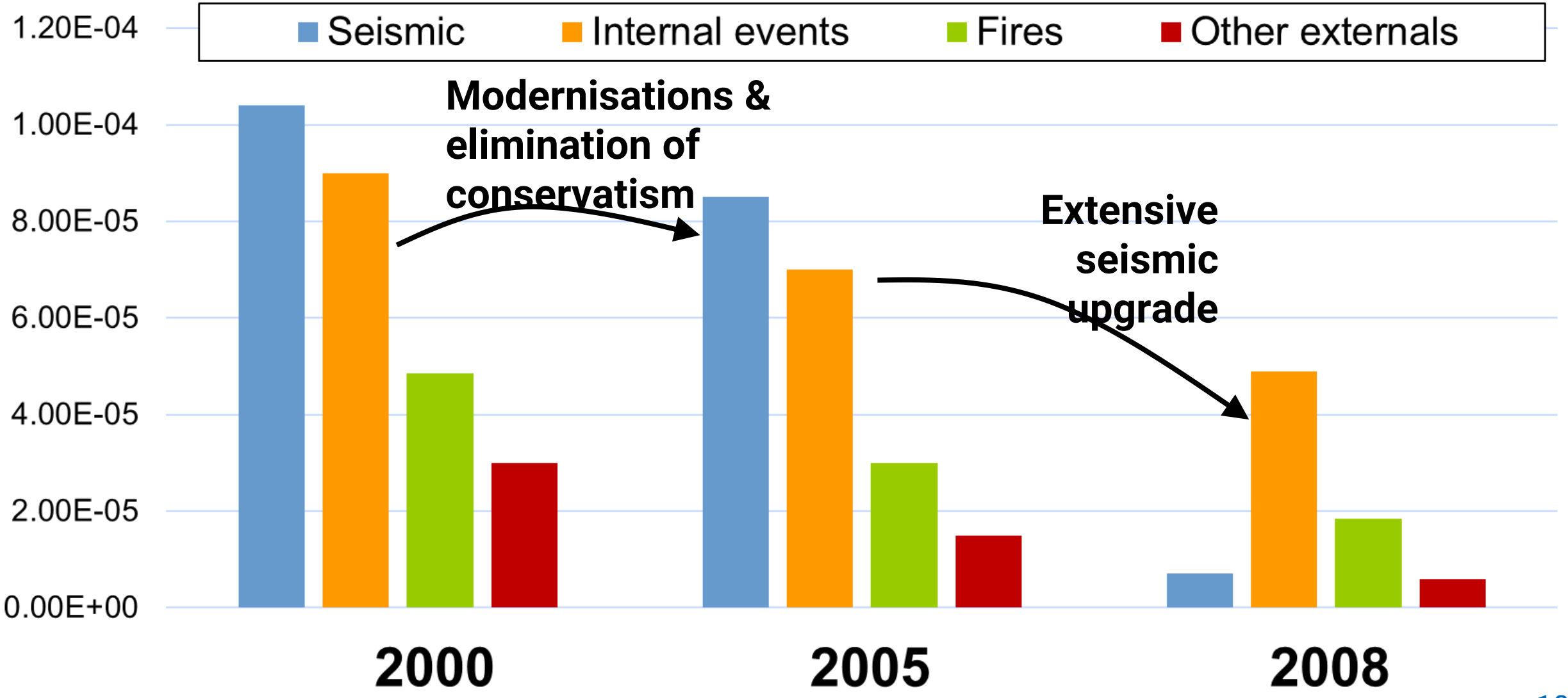
PSA results interpretation

Main outcome is the understanding of the risk profile and create basis for decision-making on risk reduction



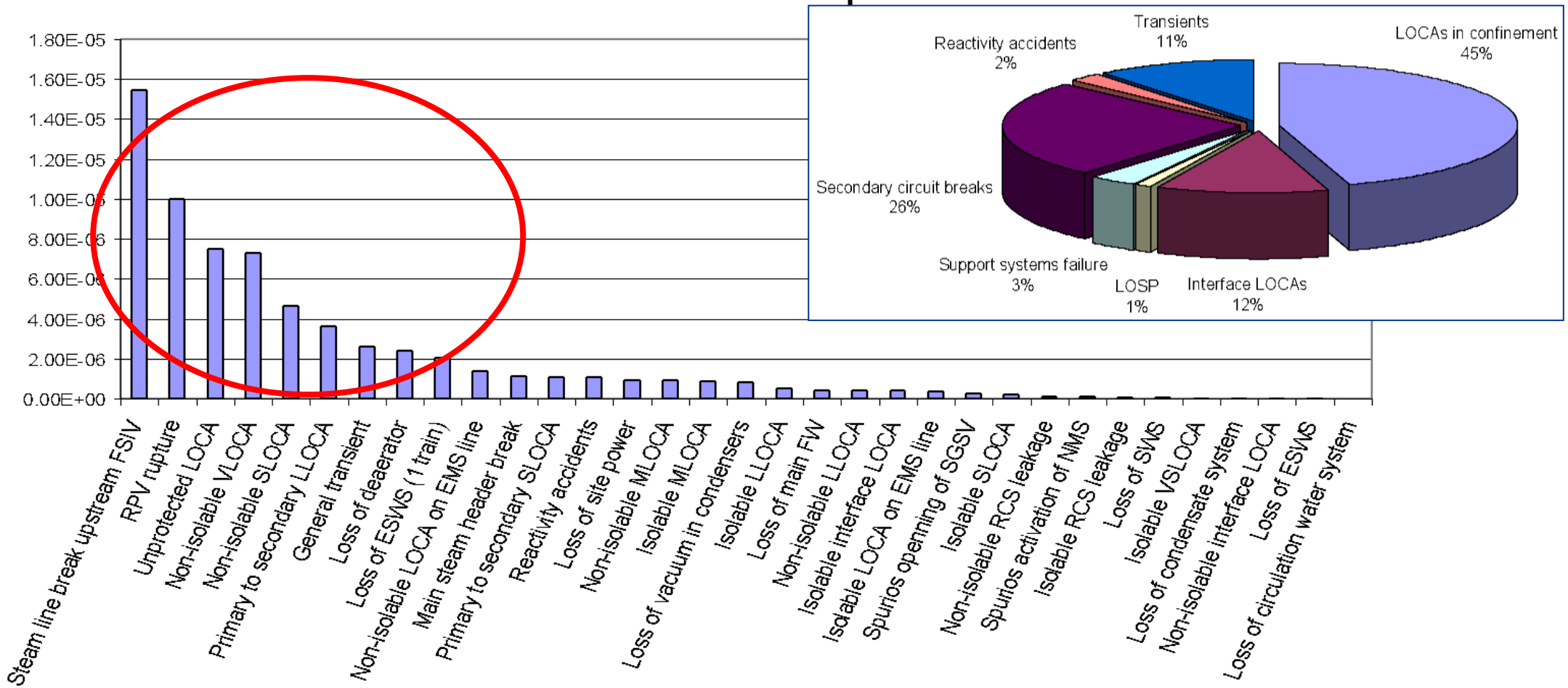


Example of evolvement of PSA results (e.g. CDF)



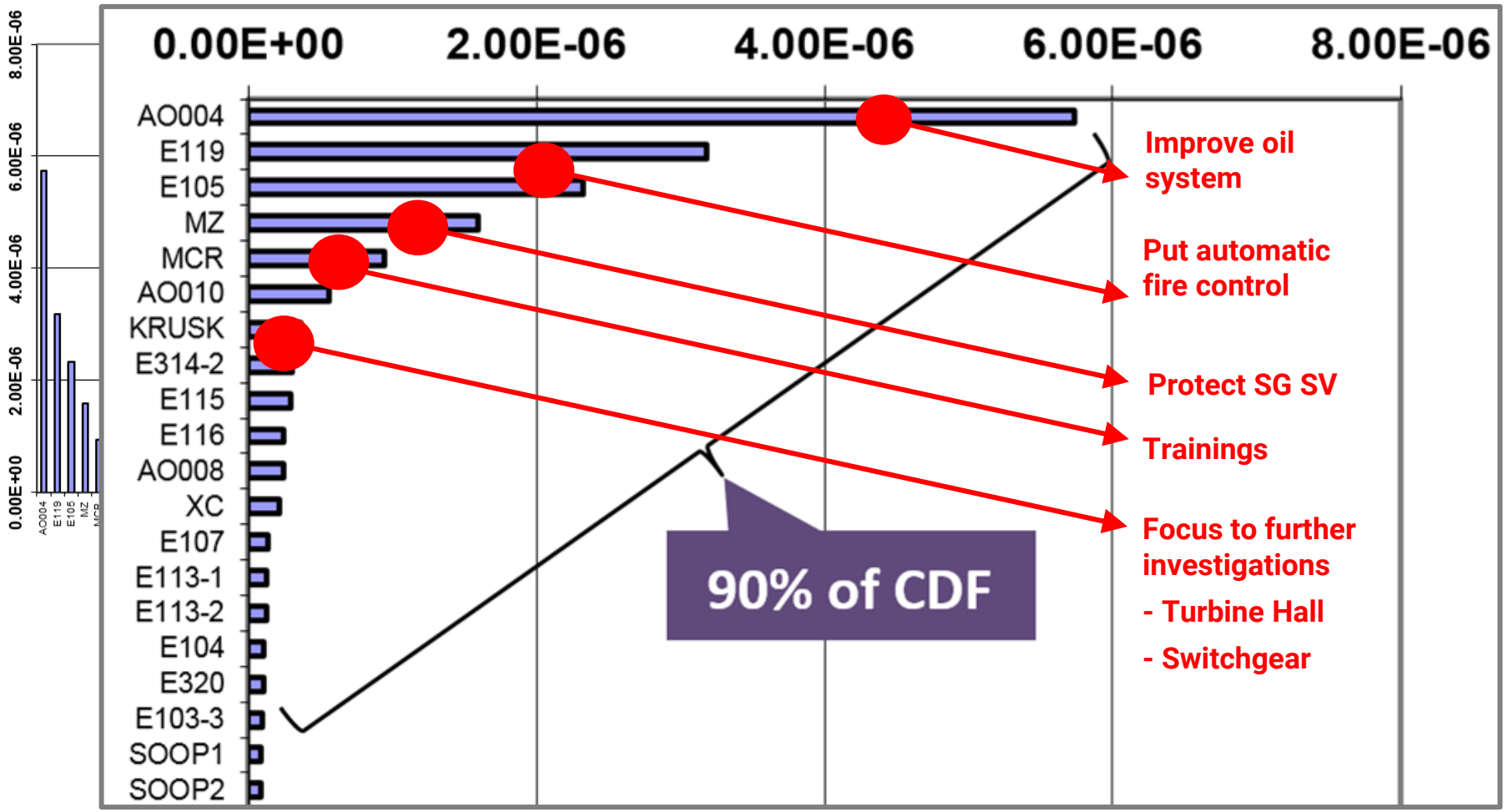
Quantification & Interpretation

- Risk profile should be carefully examined
- Recommendations are based on risk profile



Quantification & Interpretation

Example of risk profile for fires

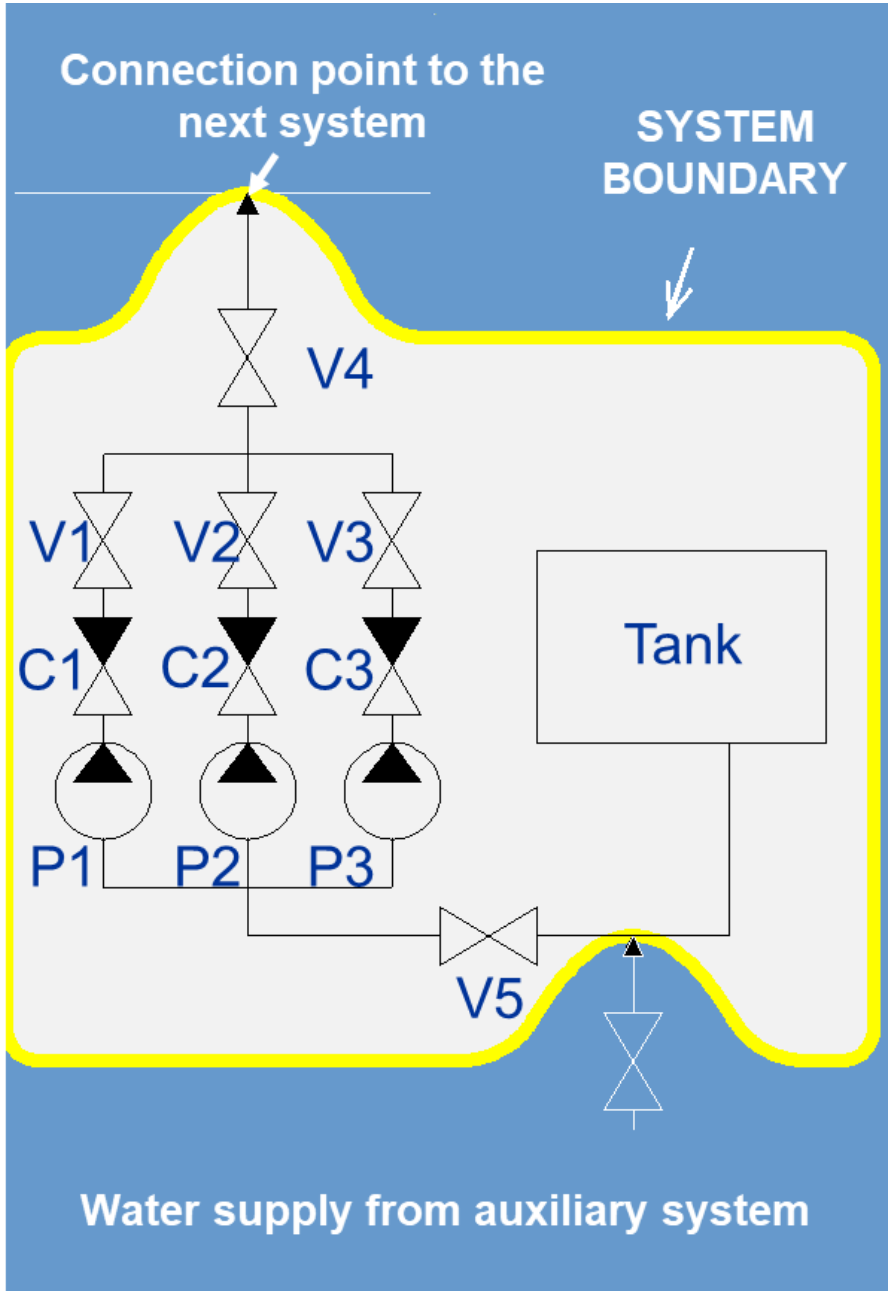


Concluding remarks

IAEA Specific Safety Guides SSG-3 (Rev.1) and SSG-4 (Rev.1) – Development and Application of Level 1 and Level 2 PSAs (2024-2025)

- **Provides recommendations on Level 1 and Level 2 PSA for NPPs** (methodology is applicable to other nuclear installations with judgement)
- **Contains should statements:** Level 1 and Level 2 PSA main tasks, as well as PSA applications and risk-informed decision making
- **Interfacing with Safety Requirements: Design** (SSR-2/1 Rev.1), **Operation** (SSR-2/2 Rev.1) **Safety Assessment** (GSR Part 4 Rev.1)
- **Safety Guide on Level 3 PSA** is planned to be initiated in 2025 (NUSSC-52 requested)

SHORT EXERCISE



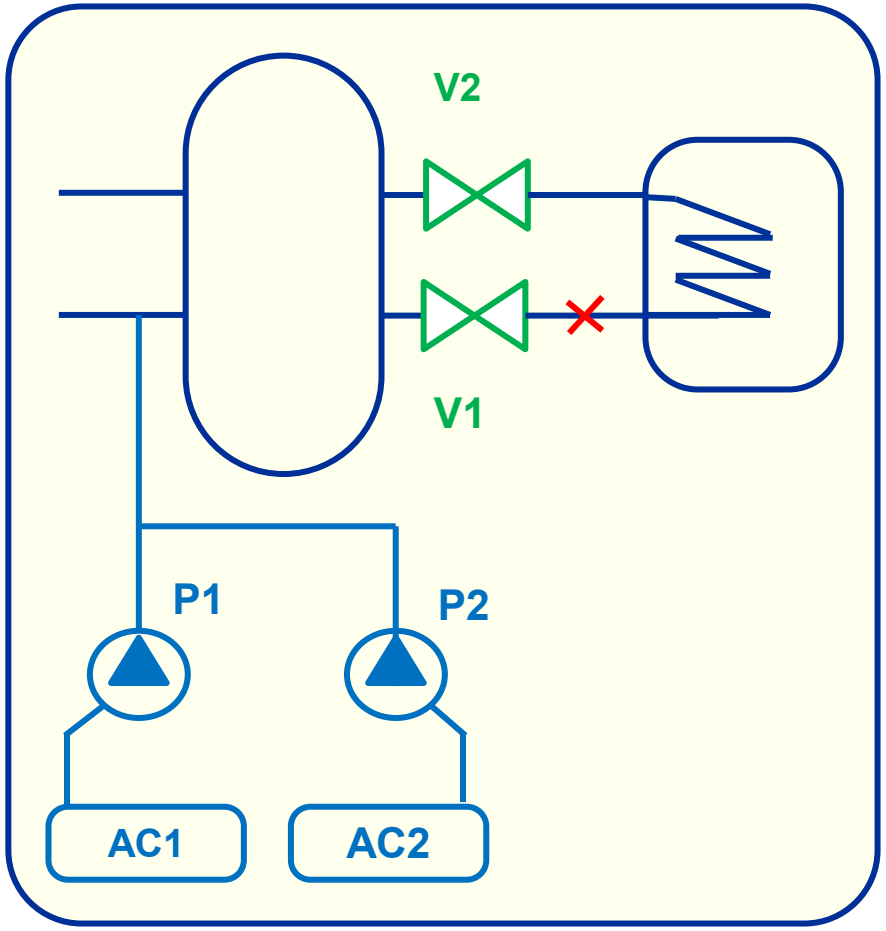
If success criteria 1 out of 3, minimal cutsets are:

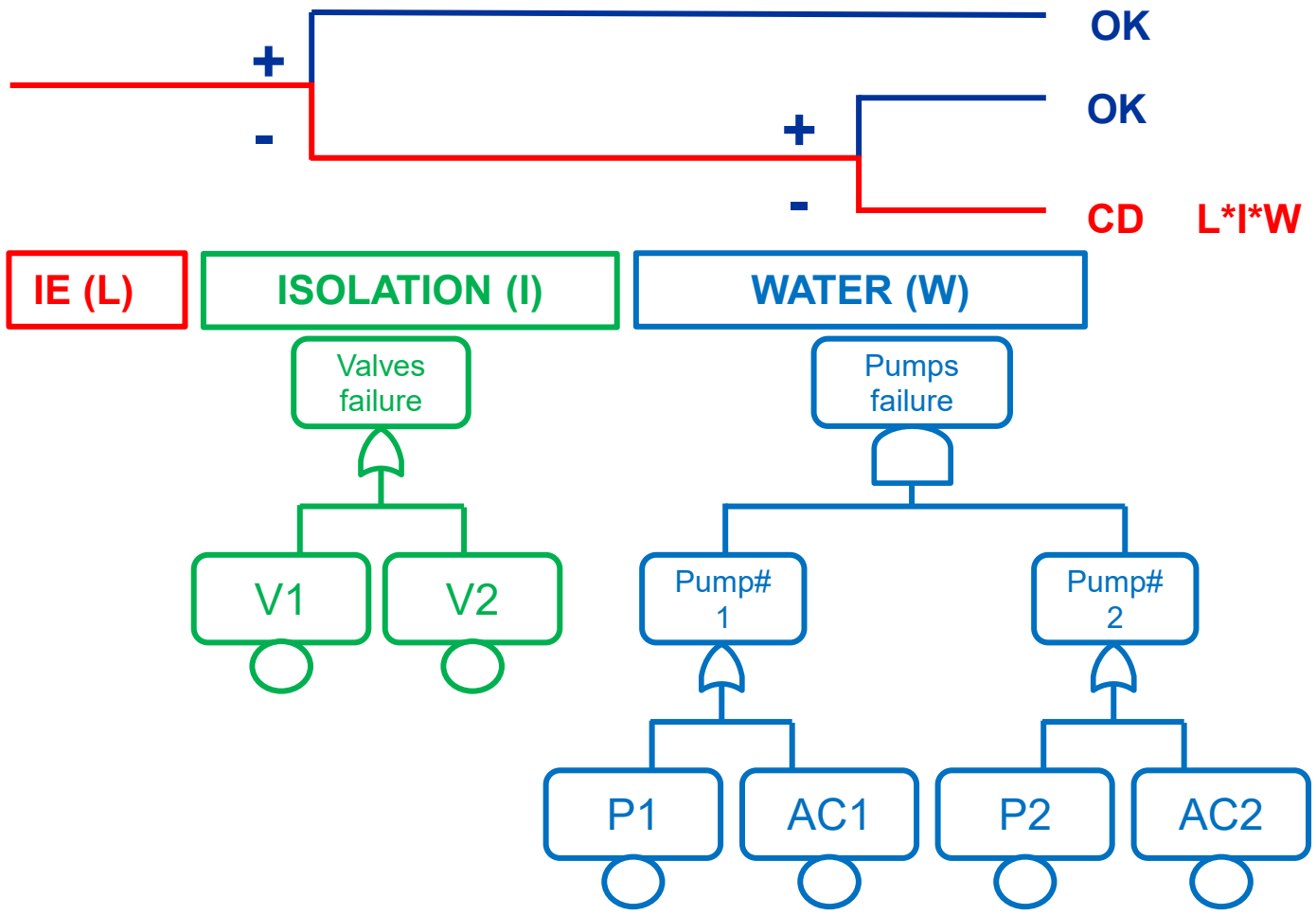
1) V1 x C2 x V3
2) …
3) ….

If success criteria 2 out of 3, minimal cutsets are:

1) V1 x V2
2) …
3) ….

Minimal cutsets: minimal combinations of failures that would lead to the failure of the system)





I=V1+V2

W=(P1+AC1)*(P2+AC2)=P1*P2+P1*AC2+AC1*P2+AC1*AC2

CD=L*I*W = L*(V1+V2)*(P1*P2+P1*AC2+AC1*P2+AC1*AC2)=

L*V1*P1*P2 + L*V1*P1*AC2 + L*V1*AC1*P2 + L*V1*AC1*AC2 +
L*V2*P1*P2 + L*V2*P1*AC2 + L*V2*AC1*P2 + L*V2*AC1*AC2