IAEA

60 Years

Atoms for Peace and Development

Probabilistic Safety Assessment: An Introduction.

Shahen Poghosyan, Simone Massara
Safety Assessment Section
Division of Nuclear Installation Safety
Department of Nuclear Safety and Security

ANSN Workshop on Safety Review and Assessment for Licensing NPPs
Daejeon, Republic of Korea, 27-31 May 2019

Learning objectives

Upon completion of this session, participants will be able to:

- Become familiar with the concept of **risk** and with main **methodological aspects** of Probabilistic Safety Assessment (PSA)
- Understand the **benefits of PSA** in the identification of the risk profile of a NPP, as a mean to orient further design actions aiming at reducing/balancing the total risk

Outline

- Concept of risk & introduction to PSA
- Methodology
- Risk-informed decision making and PSA applications
- Support to capacity building offered by IAEA

Concept of risk
& Introduction to PSA

Concept of risk

- The notion of risk is widely used in everyday life
- Colloquially, risk is associated with danger, hazard, exposure-to-death, injury, loss, or other ***negative*** consequences:
  - Risk implies a ***potential*** for harm
  - If the danger is actually realized, then it is no longer risk but actual death, injury, loss or other harmful consequence
- Risk is ***inescapable*** - it is inseparably associated with human existence

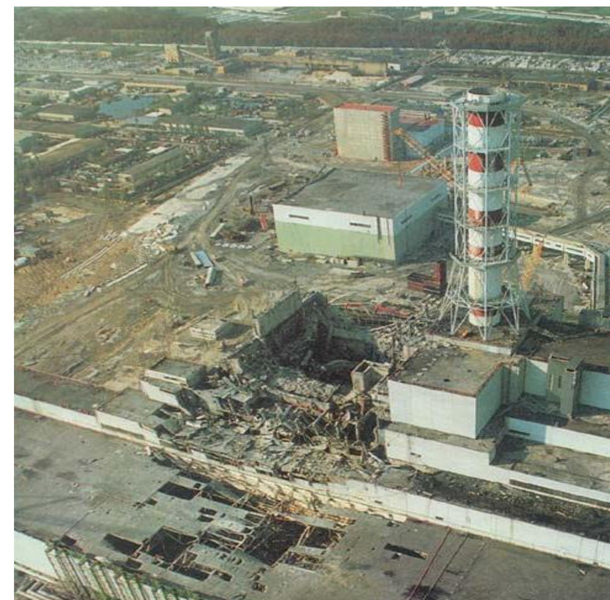
Concept of risk

IAEA 60 Years Atoms for Peace and Development

- A ***hazard*** is a potential condition that causes:
  - injury or death to people,
  - loss of or damage to equipment, property, etc.
- Hazard is characterized by
  - ***magnitude* (severity)** and
  - ***frequency of occurrence*** of the hazard with specified magnitude
- Risk is measure of a consequences from the hazards
- Risk is characterized by:
  - the ***magnitude* (*severity*)** of the adverse *consequence*(s) that can potentially result from the given hazard, and
  - by the ***frequency* of occurrence** of the given adverse consequence(s)
- **Safety** is maintained by ensuring that risks are maintained as low as reasonably practicable (ALARP, cf. INSAG-25)
  - Under the ALARP concept, measures to reduce risks should be applied unless there is a gross disproportion between the achievable level of risk reduction and the effort needed to reduce it (cf. INSAG-25)

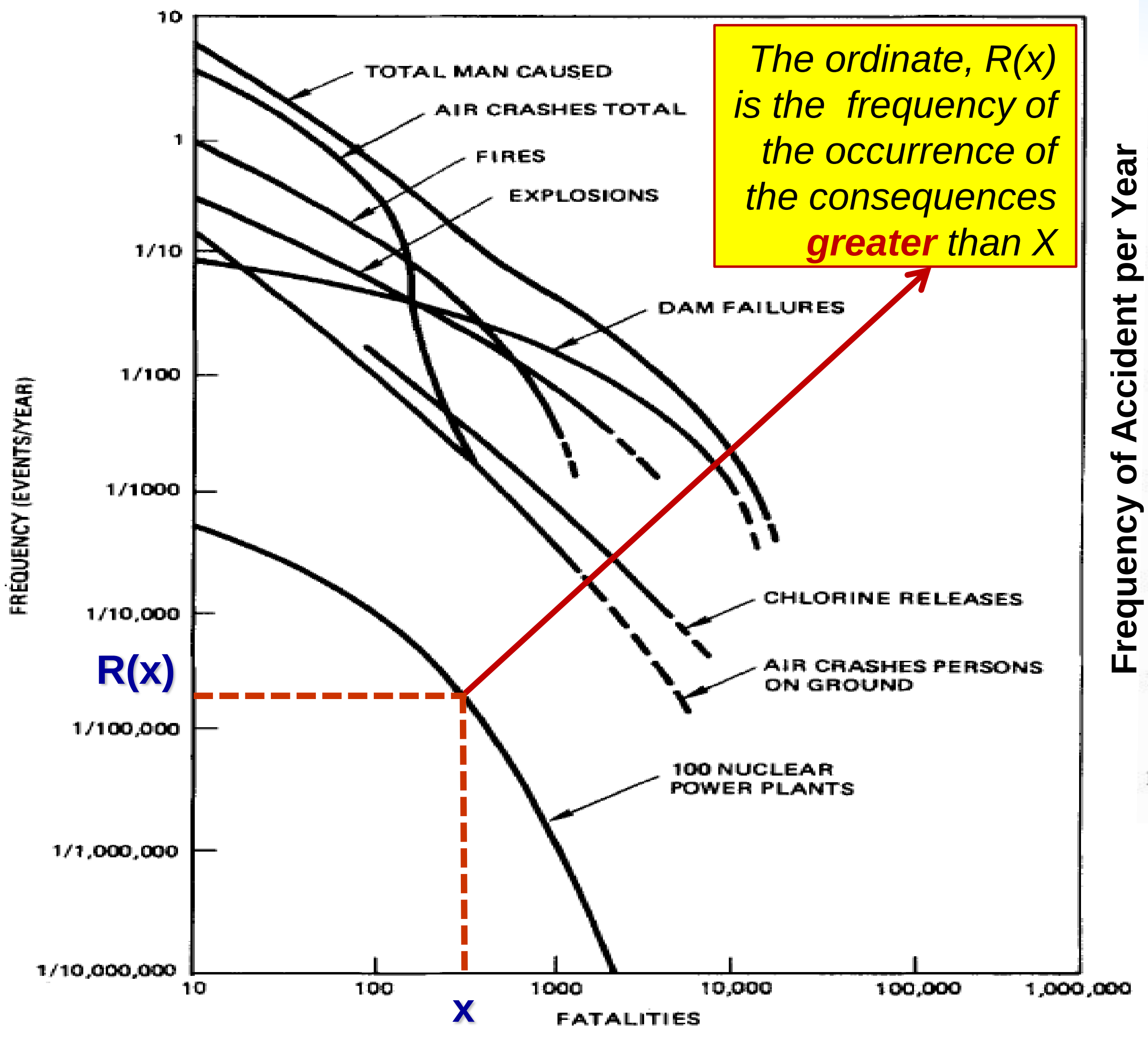
Concept of risk

- Risk can result from natural causes like illness or from natural disaster like earthquakes, floods, tsunamis volcanic eruptions, hurricanes, etc.
- Risk can also result from the side effect of human's technological achievement
- Legislation has the responsibility to protect human and property from the harm associated with technical installations and regulate the associated risk
- Industrial activities such as those in a nuclear installation may have risks of various types
- Risks may be borne by the site personnel, by people living near the installation and/or by the whole society – the environment may also suffer harm if radioactive material is released

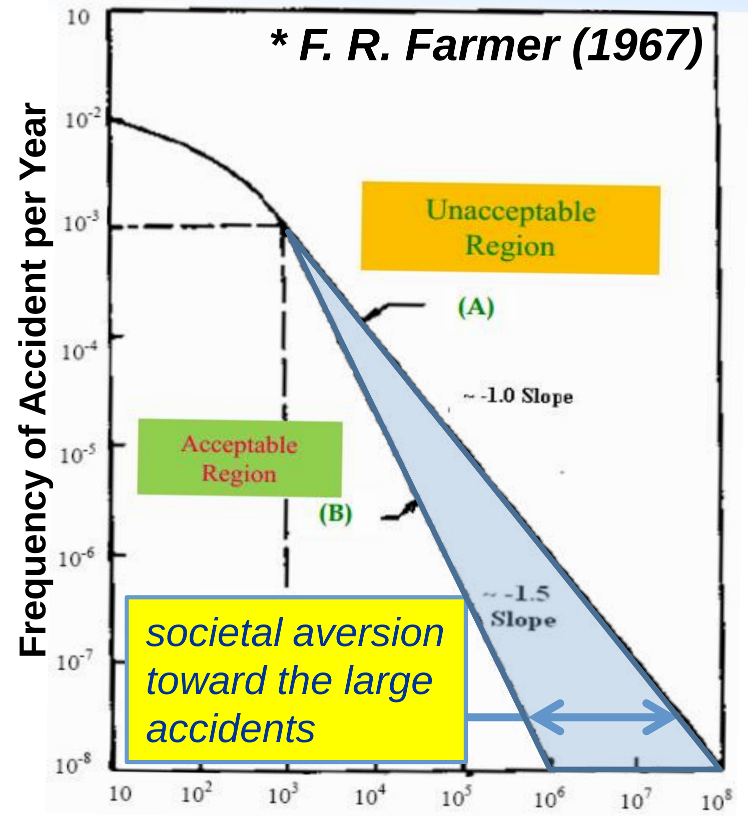


- Consequently, it is necessary to limit the radiation risk to which people and the environment are subject for all reasonably foreseeable circumstances

Farmer's curve



Frequency of fatalities due to man-caused events.



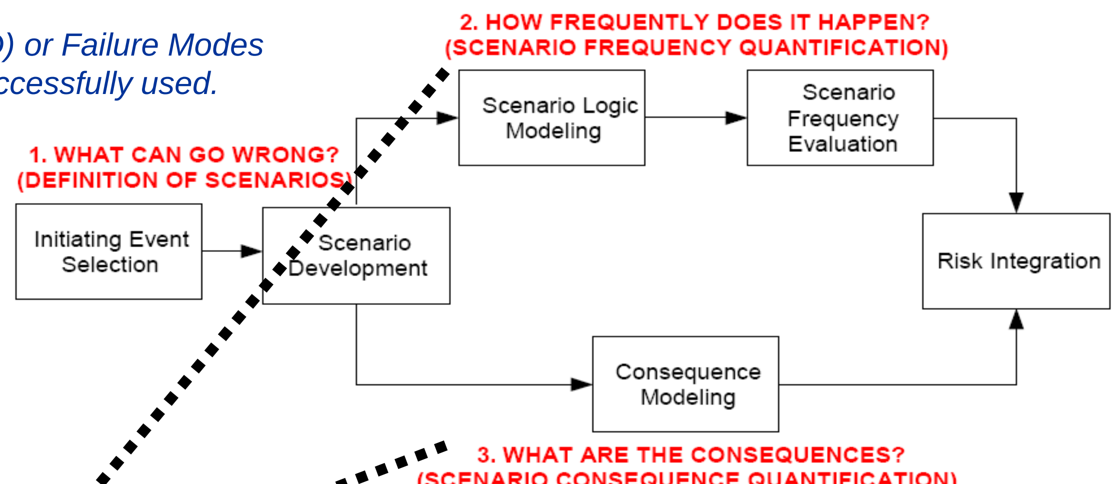
Equivalent Ground-Level Release of 131I (Curies)

Probabilistic Safety Assessment

- Risk assessment answers three basic questions:
  1. **What** can go wrong?
  2. **How frequently** does it happen?
  3. What are the **consequences**?

The answer to this question is obtained by using Boolean Logic methods (event tree analysis (ETA) and fault tree analysis (FTA)) for model development and by probabilistic or statistical methods for the quantification portion of the model analysis.

Answer to this question requires technical knowledge of the possible causes leading to detrimental outcomes of a given activity or action.
Logic tools like Master Logic Diagrams (MLD) or Failure Modes and Effects Analyses (FMEA) are usually successfully used.



The answers to both questions are obtained by developing and quantifying accident scenarios, which are chains of events that link the initiator to the end-point detrimental consequences:
- *Typically executed through DSA best-estimate analyses*

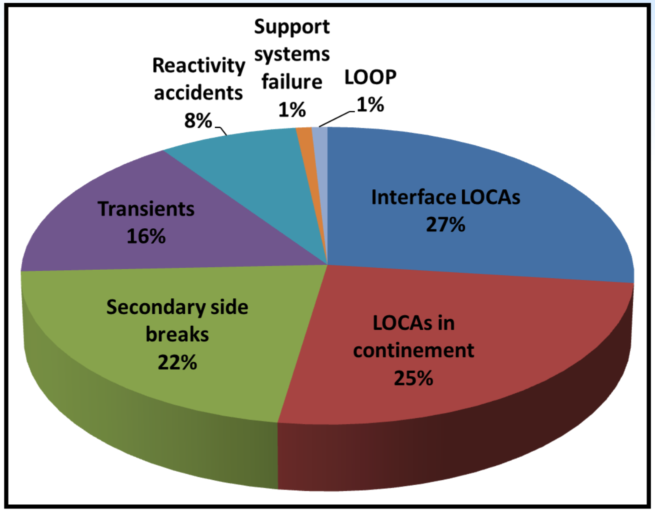
Probabilistic Safety Assessment

- The most famous risk assessment technique for NPPs is Probabilistic Safety Assessment (PSA)
  - Allow to analyze entire spectrum of possible accident scenarios
  - Allow to obtain risk profile for NPP

- Probabilistic Safety Assessment (PSA) or Probabilistic Risk Assessment (PRA) ?
  - It depends on the undesirable event. If risk is analyzed – in other words, the undesirable events are latent fatalities or acute fatalities – then the proper name is PRA.
  - If only core damage events or containment failures are analyzed, then PSA is more appropriate. PRA is primarily used in the United States. In other countries most people use PSA, although now the terms are being used interchangeably.

Probabilistic Safety Assessment

- The most famous risk assessment technique for NPPs is Probabilistic Safety Assessment (PSA)
  - Allow to analyze entire spectrum of possible accident scenarios
  - Allow to obtain risk profile for NPP



- Probabilistic Safety Assessment (PSA) or Probabilistic Risk Assessment (PRA) ?
  - It depends on the undesirable event. If risk is analyzed – in other words, the undesirable events are latent fatalities or acute fatalities – then the proper name is PRA.
  - If only core damage events or containment failures are analyzed, then PSA is more appropriate. PRA is primarily used in the United States. In other countries most people use PSA, although now the terms are being used interchangeably.

Objective of PSA

- Estimation of the frequency for undesirable event
- Identification of the initiating events and dominant accident sequences with the highest contribution to the undesirable event frequency (risk profile)
- Identification of weaknesses or vulnerabilities in plant systems design and operation
- Preparing input for safety-related decision making

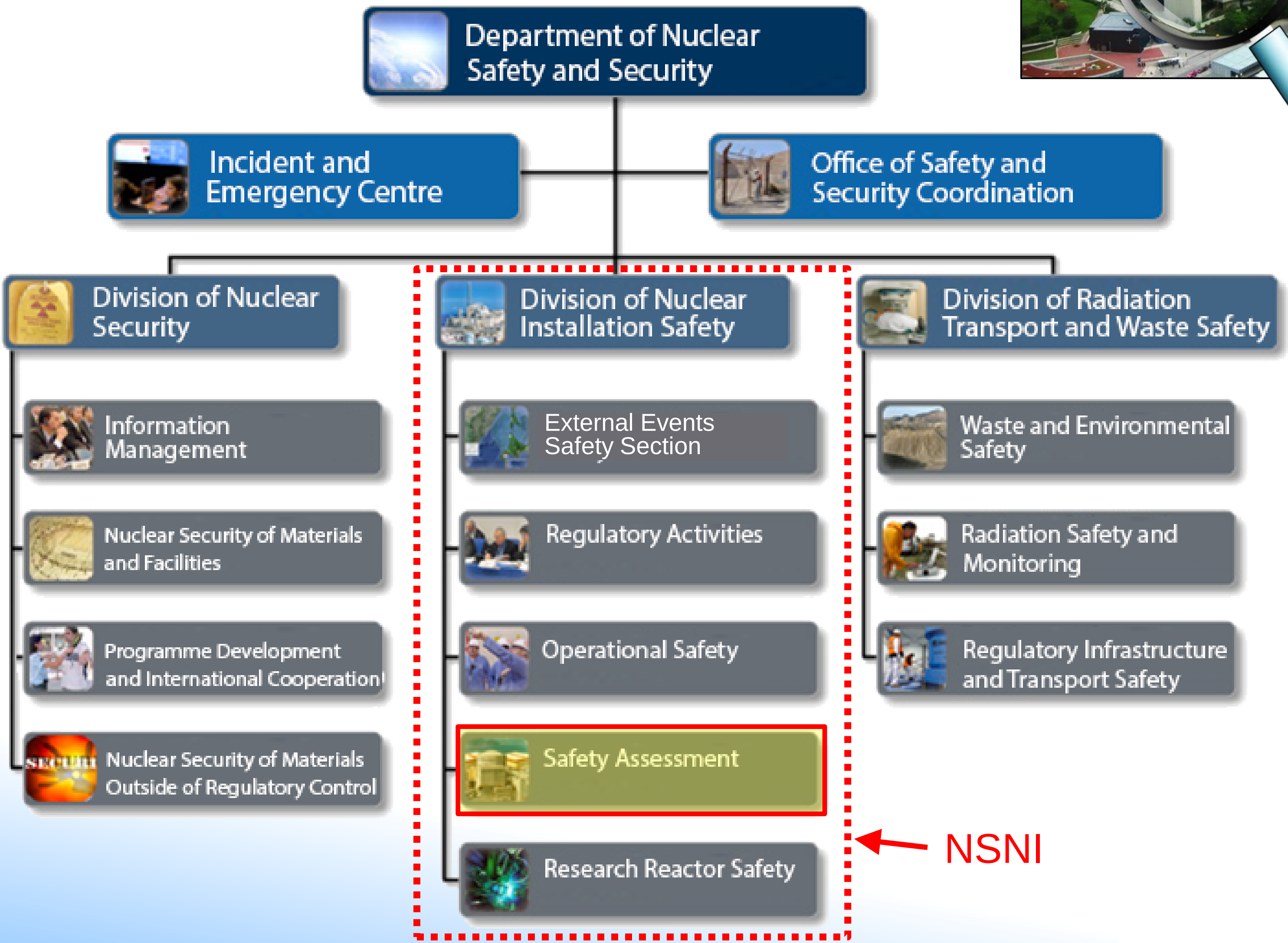
Can you spot any weaknesses?

Objective of PSA

Can you (still) spot any weaknesses?

If not… PSA can help!

IAEA Department of Nuclear Safety and Security



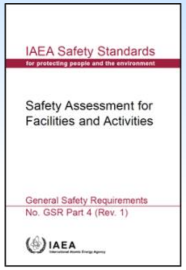
IAEA publications on PSA

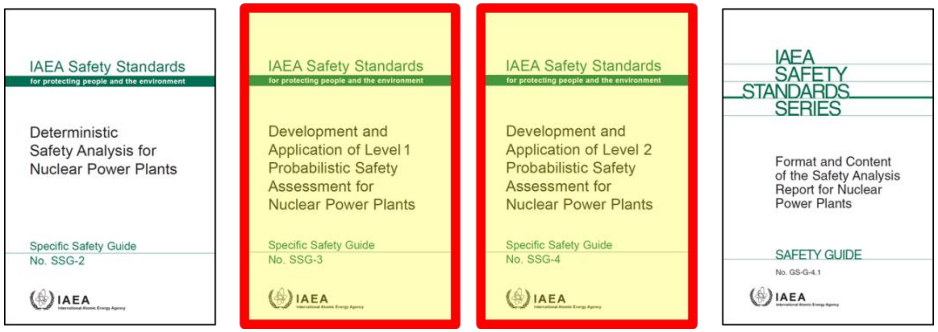
Safety objectives and safety principles

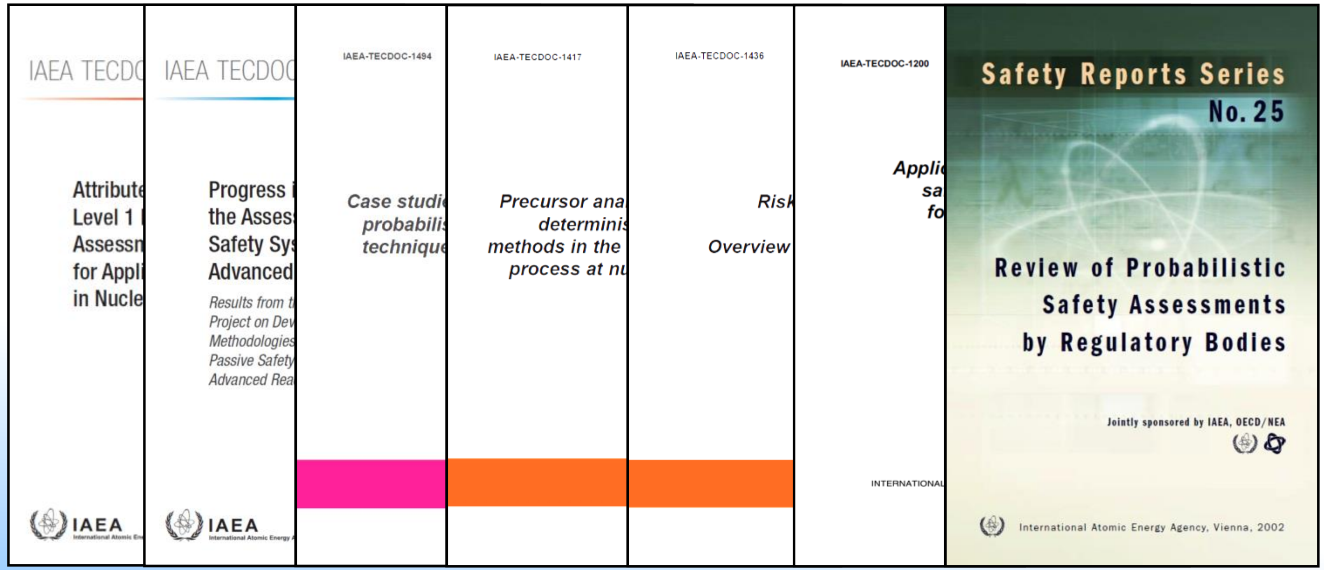
Functional conditions required for safety

Guidance on how to fulfil the requirements

to support SG



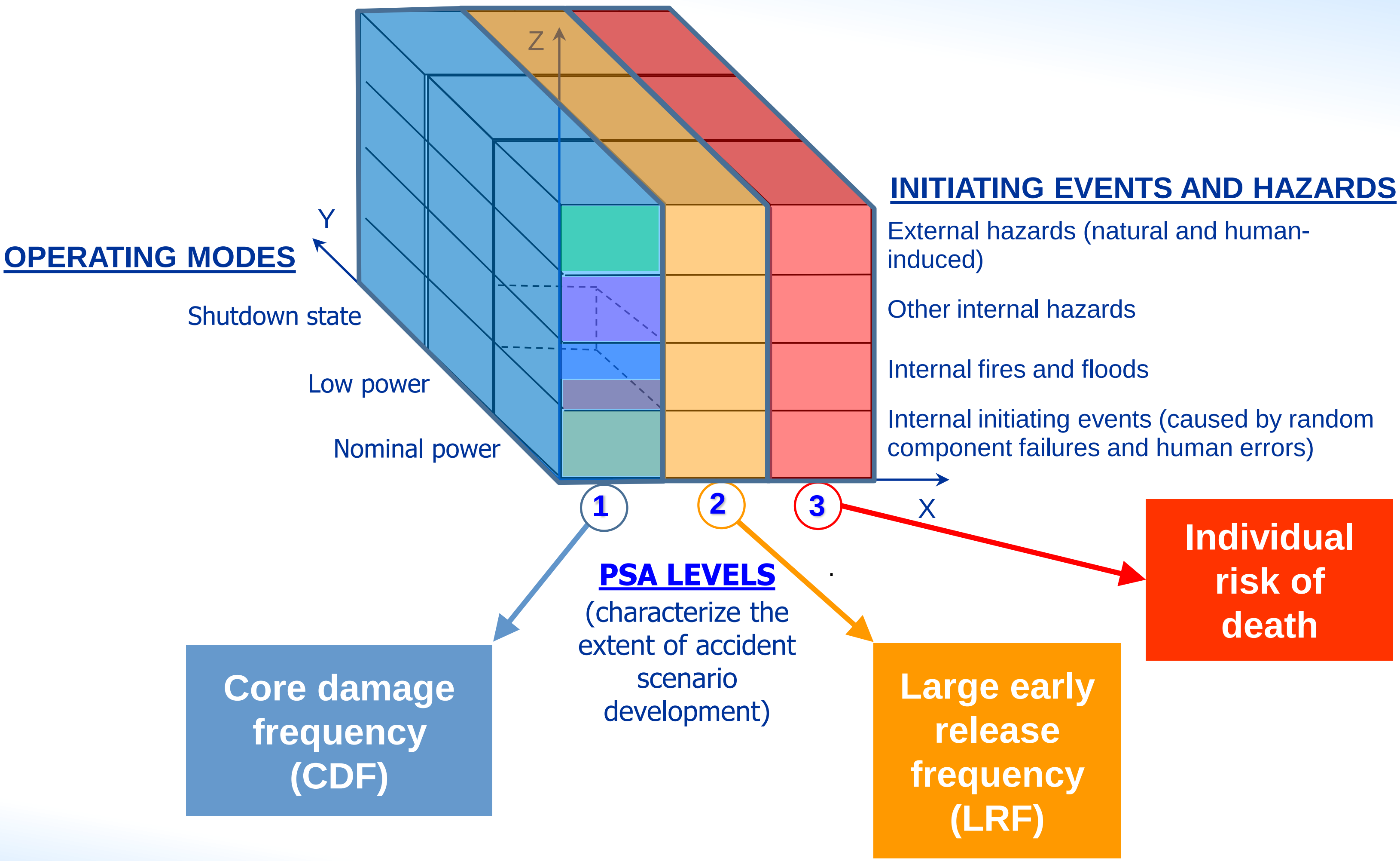




...under development
- Human Reliability
- Risk aggregation
- Multiunit PSA
- IRIDM
- Seismic PSA
- Use of Tsunami PSA
- CANDU PSA
- Research reactors PSA

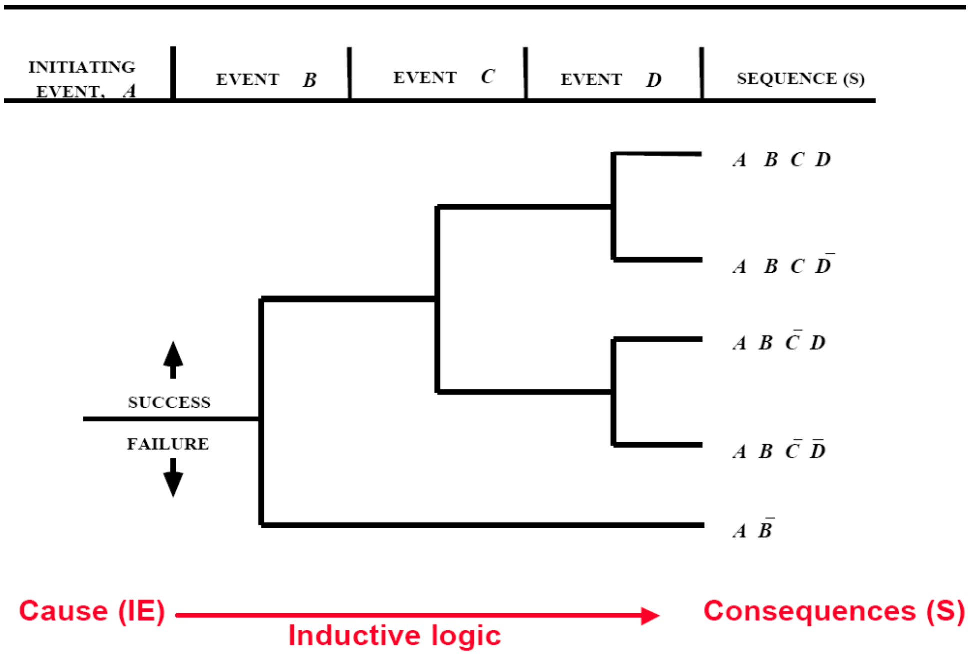
PSA methodology

Probabilistic Safety Assessment

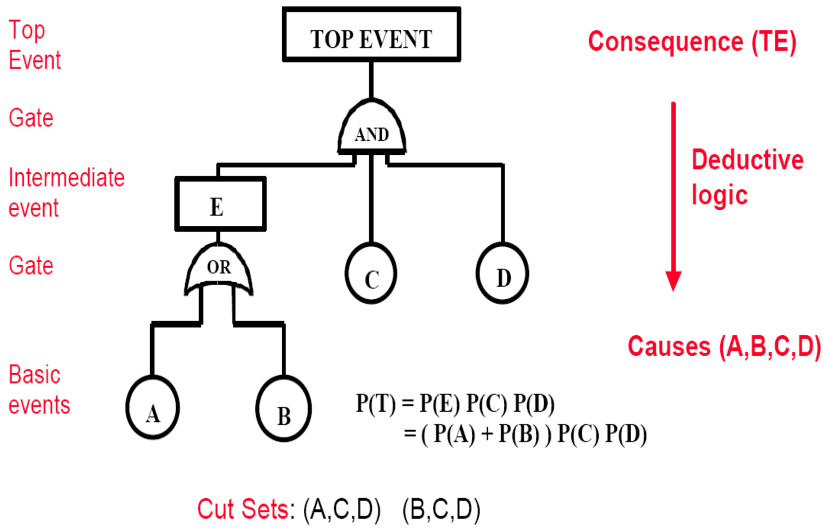


General methodology of PSA

Event tree



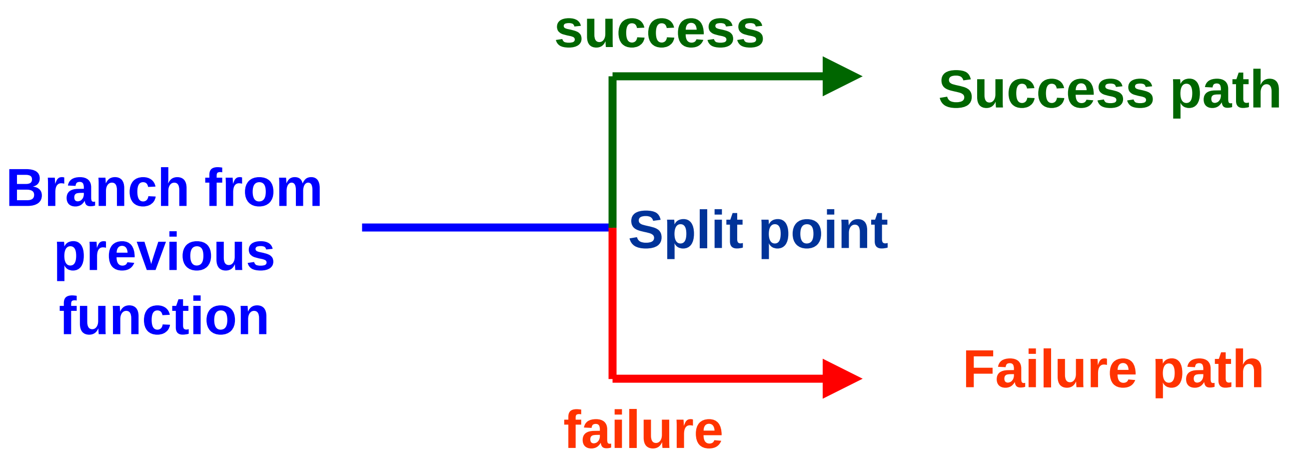
Fault tree



Boolean logic tools include *inductive* logic methods like *event tree analysis* (ETA*)* and *deductive* methods like *fault tree analysis* (FTA)

Overview of Event Tree technique (1 / 2)

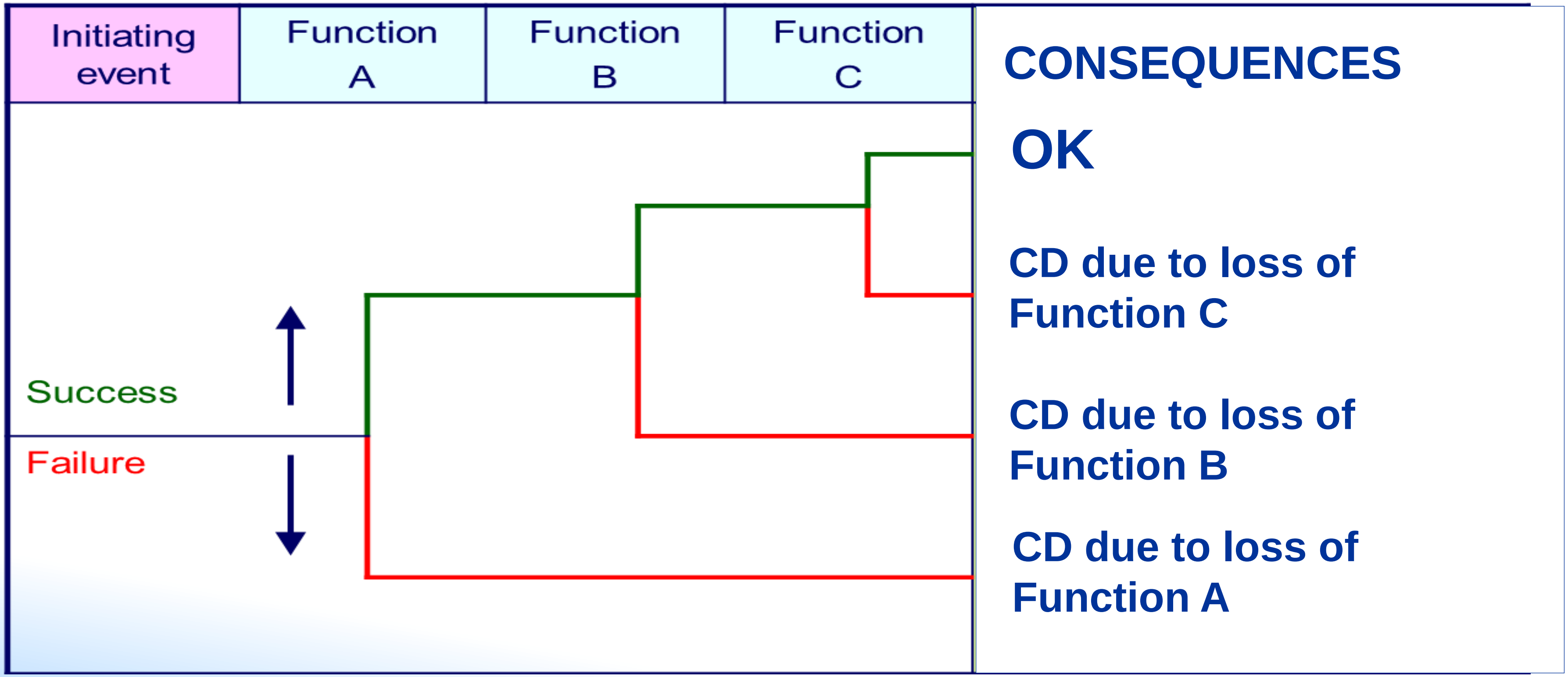
- **Event trees are developed by combining the success or failure of safety functions or systems for each initiating event**



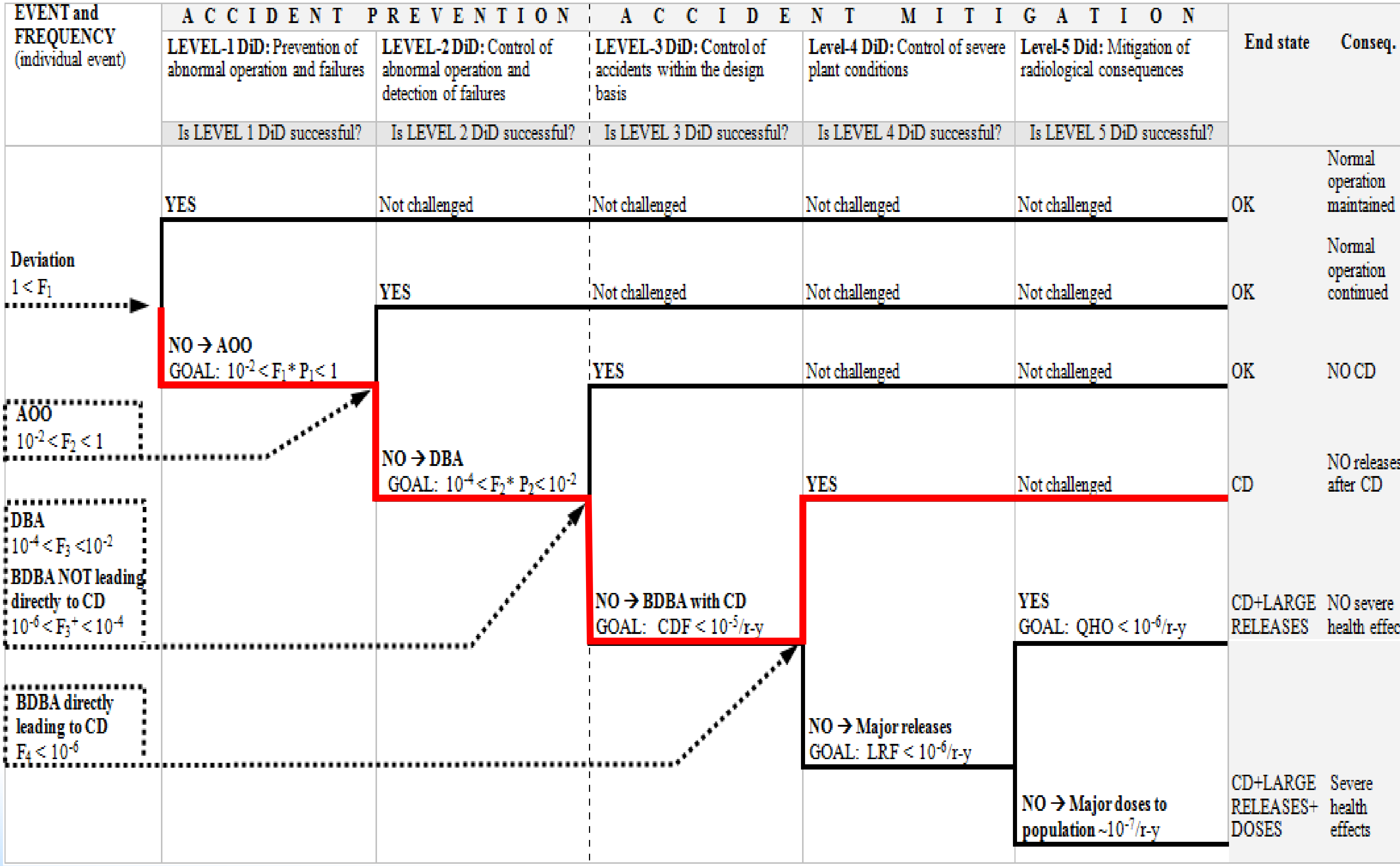
- **At split point the function is successful if the path is upward, the function fails if the path is downward**

Overview of Event Tree technique (2 / 2)

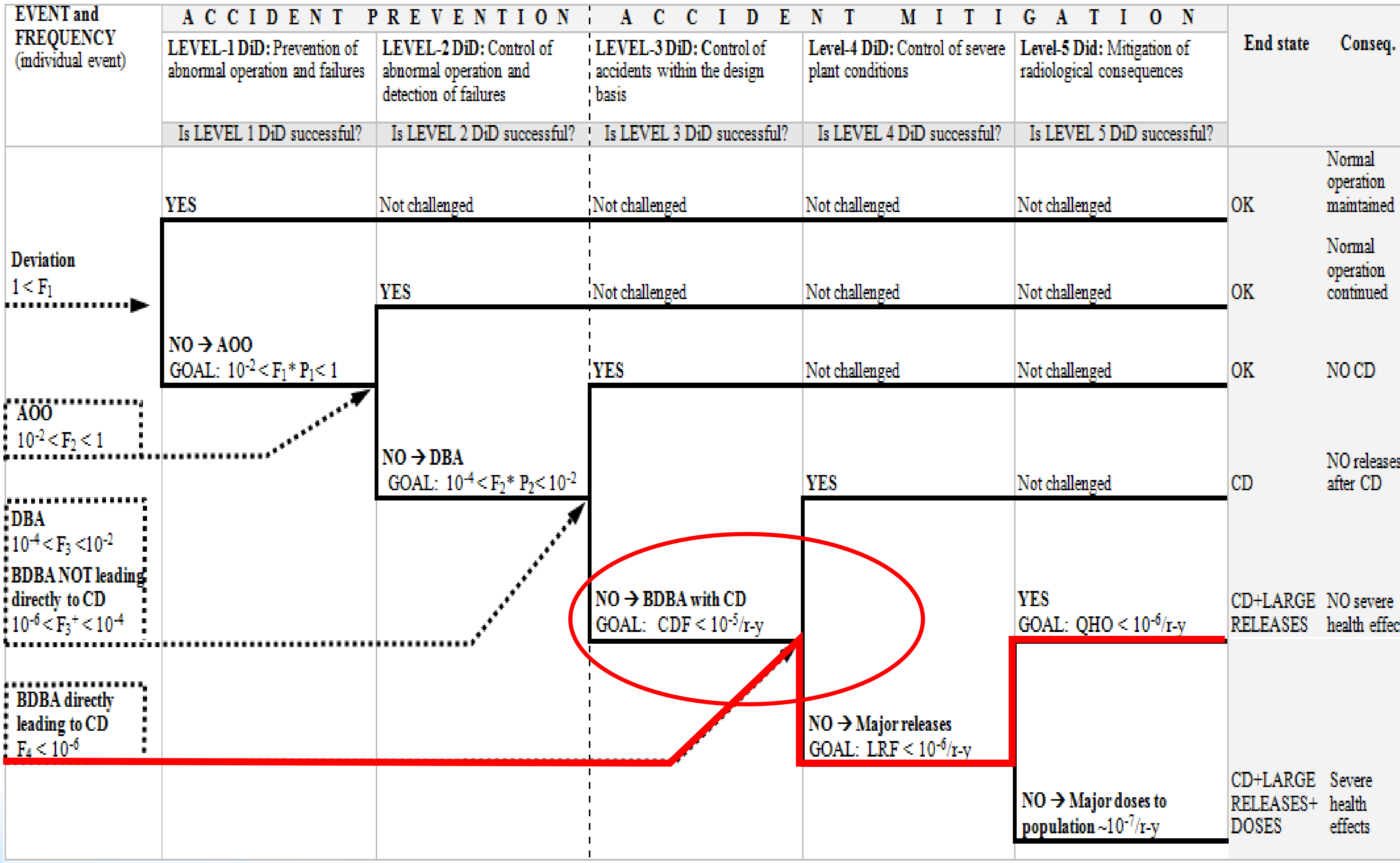
- Accident sequence – a chain of events linking the initiator and possible consequences
  - ✓ Depending on the success or failure of the modelling functions
- Main consequences considered in Level 1 PSA:
  - ✓ Plant safe state (OK), core damage (CD)



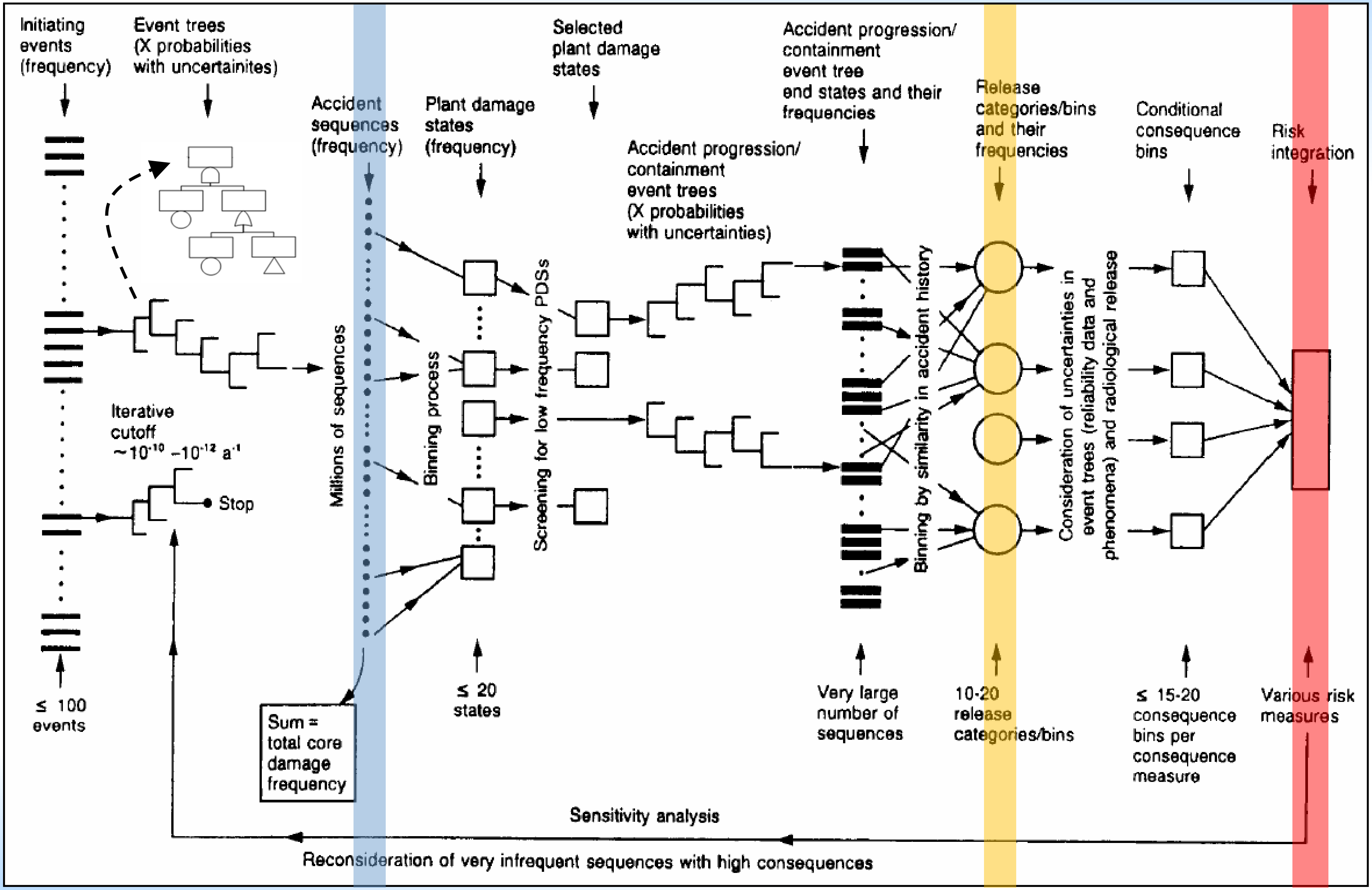
Concept of DiD illustrated through Event Tree



Concept of DiD illustrated through Event Tree



Probabilistic Safety Assessment

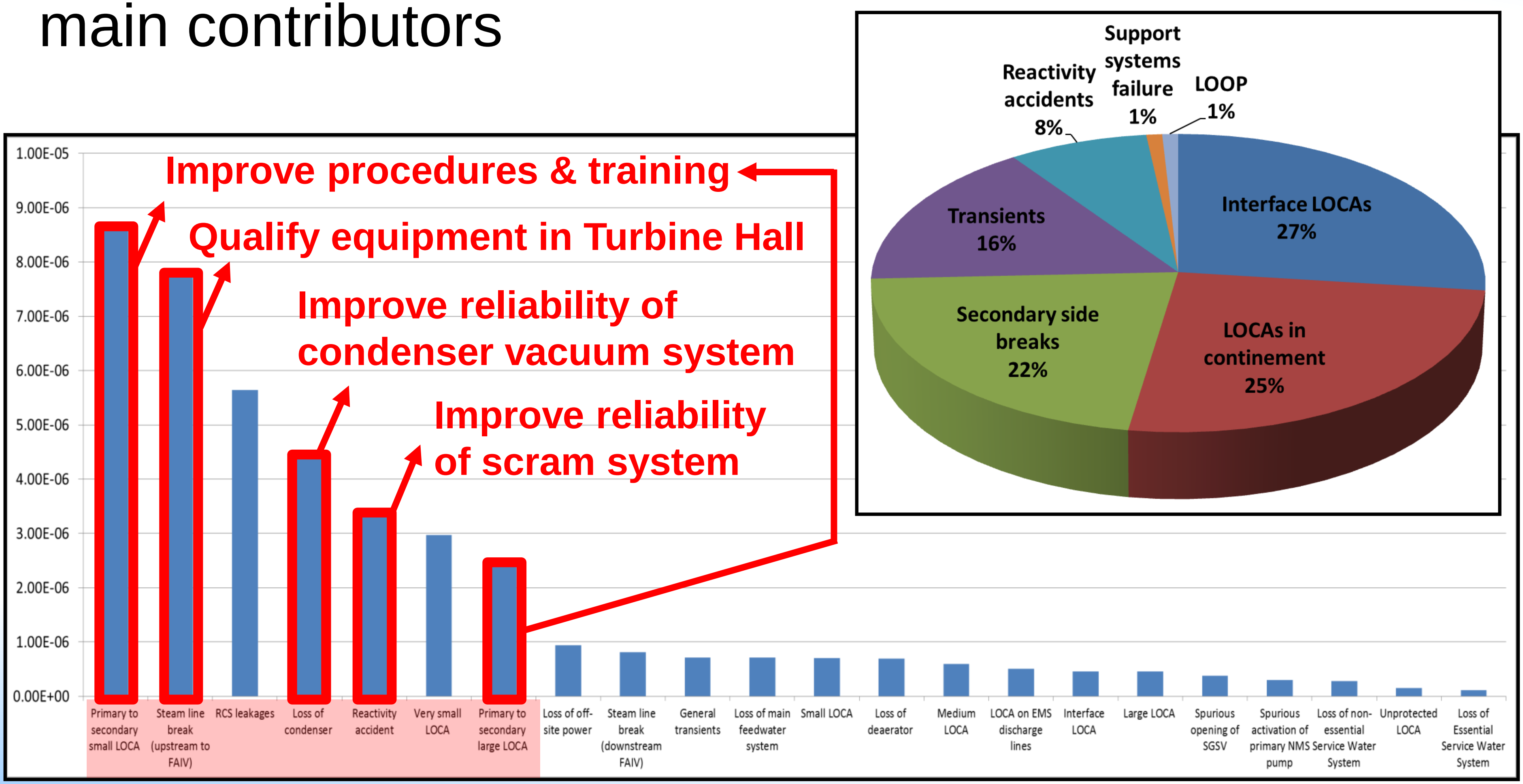


Level 1 Level 2 Level 3

Risk-informed decision making and PSA applications

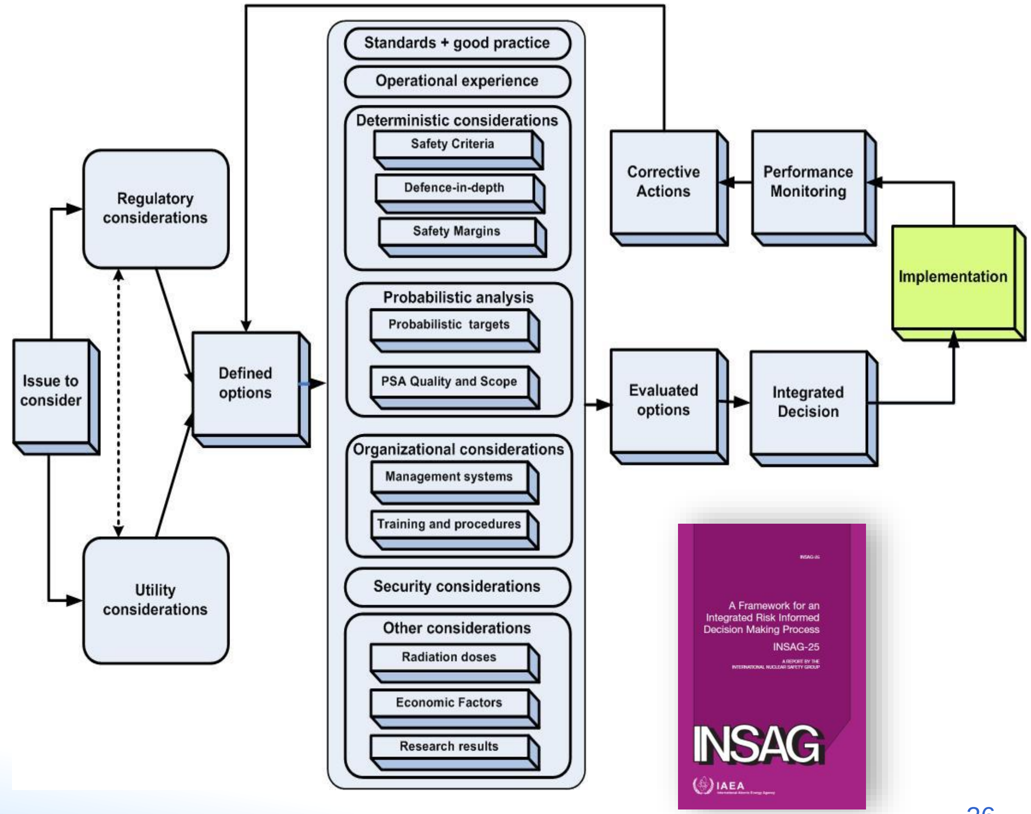
PSA results

Risk profile should be carefully examined. Further recommendations are based on the investigation of main contributors



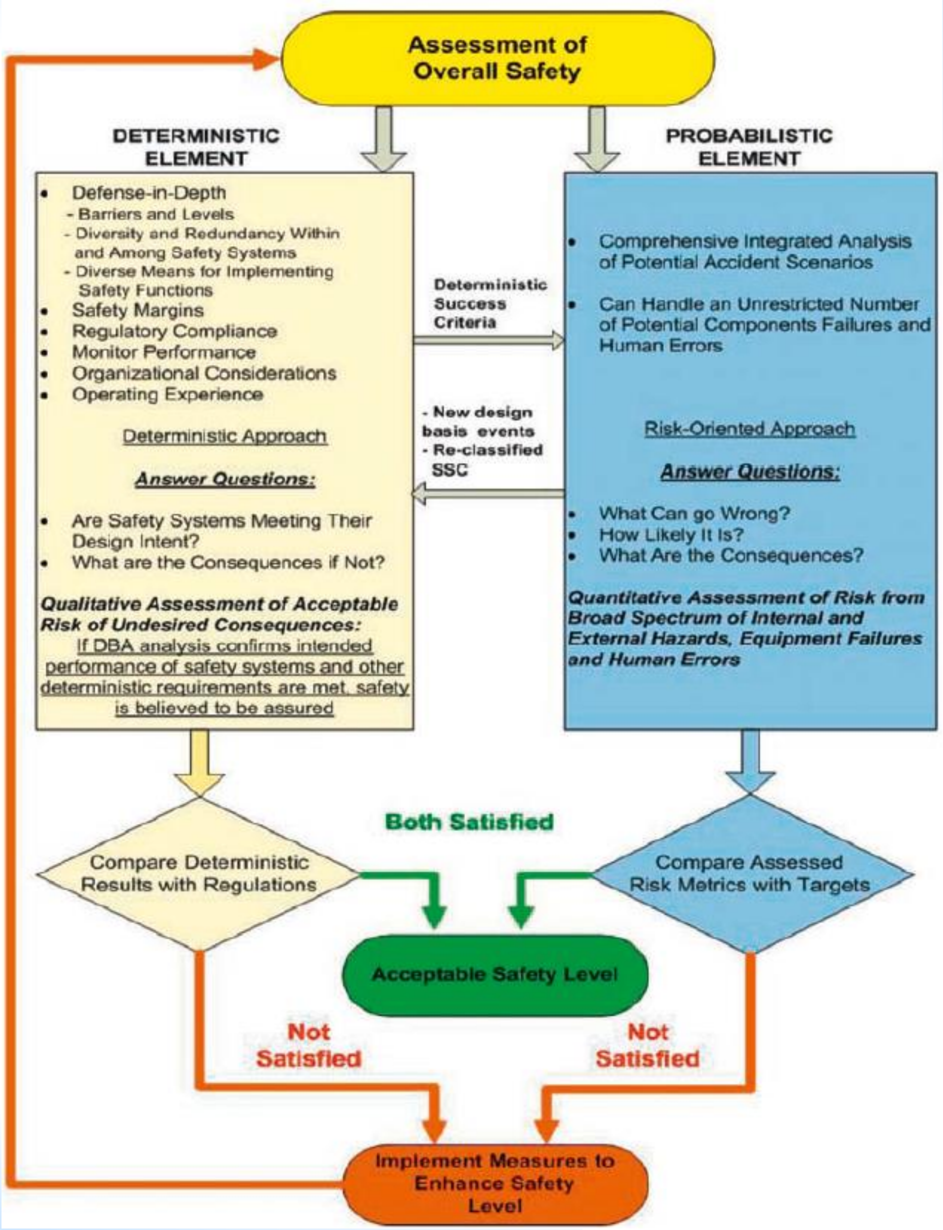
Integrated Risk Informed Decisions Making process (IRIDM)

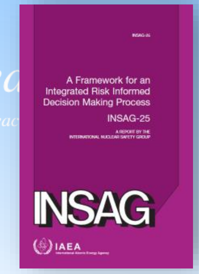
- **IRIDM process** is a systematic decision-making process that takes account of all relevant safety aspects in making a safety decision
- Objective: to provide principles and suggest approaches to apply IRIDM process
- Follows main principles listed in INSAG-25 report



IRIDM: Integration of deterministic and probabilistic elements

- Iterative process, before getting to a final safety decision
- The process can result in the identification of new design basis events and new criteria for deterministic safety classification of SSCs
- IRIDM involves the integration of various elements so that the overall resolution of the issue under consideration is commensurate with its risk significance and the efforts needed to implement it

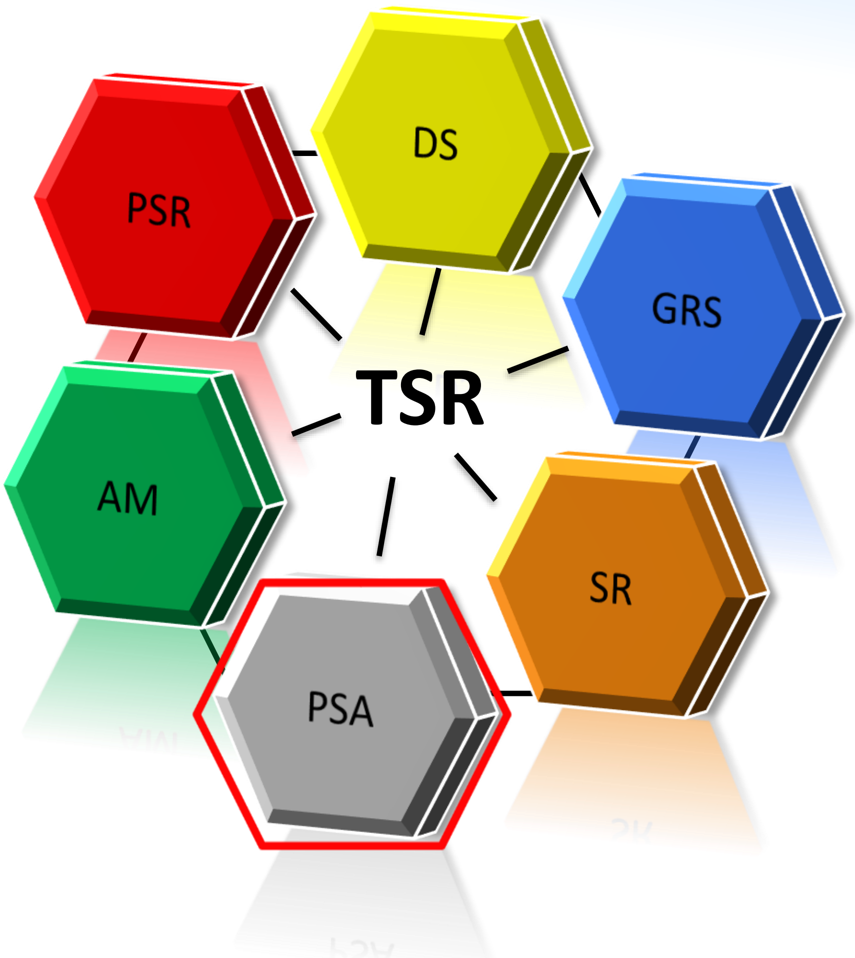




Capacity Building on PSA

Technical Safety Review (TSR)

The TSR Peer Reviews incorporates IAEA safety assessment and design safety technical review services to address the needs of Member States at most stages of development and implementation of the nuclear power programme.



Technical Safety Review of PSA

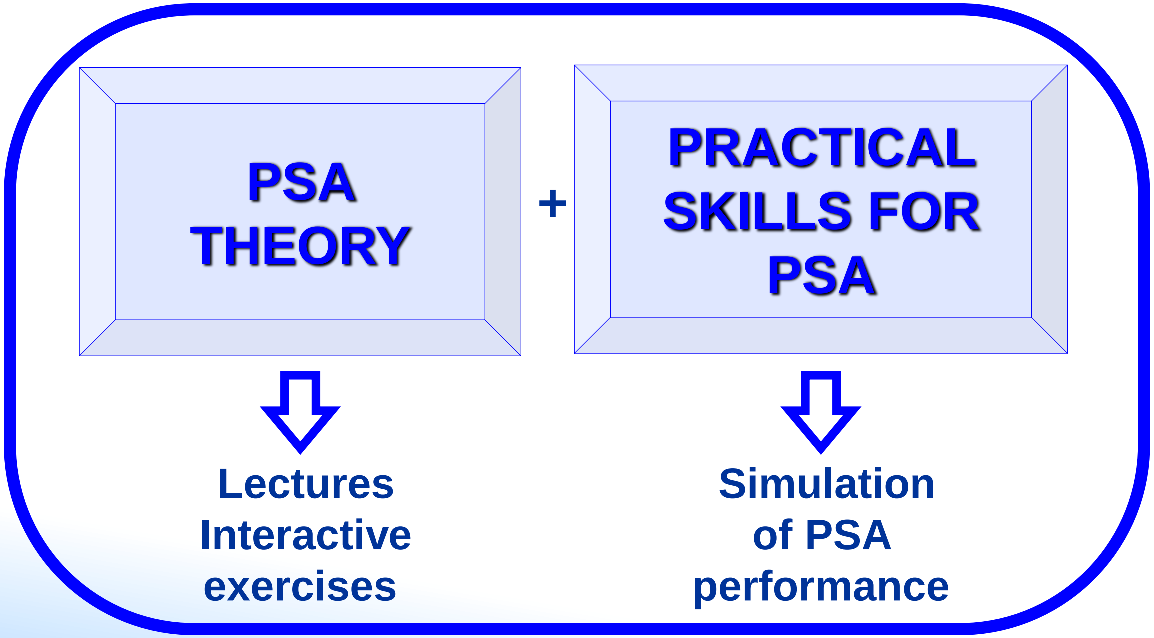
IAEA 60 Years Atoms for Peace and Development

- **DESCRIPTION**
  - Conducted to review the PSA documentation submitted to the IAEA against relevant IAEA SS:
    - GSR Part 4: General Safety Requirements on Safety Assessment for Facilities and Activities, supported by:
      - SSG-3: Development and Application of Level 1 Probabilistic Safety Assessment for NPPs
      - SSG-4: Development and Application of Level 2 Probabilistic Safety Assessment for NPPs
- **OBJECTIVE**
  - To assist in the review of the technological and methodological aspects modelled in the PSA, as well as PSA applications to enhance safety
- **PROCESS**
  - The process includes preparatory work by the review team and review meetings that usually last two weeks. Funded by the requesting party or through technical cooperation projects
- **DELIVERABLE**
  - Report that summarizes the observations of the review and includes, if needed, a set of recommendations to improve the adherence of the PSA documentation to the IAEA safety standards

More info: https://nucleus.iaea.org/sites/gsan/services/Pages/IPSART.aspx

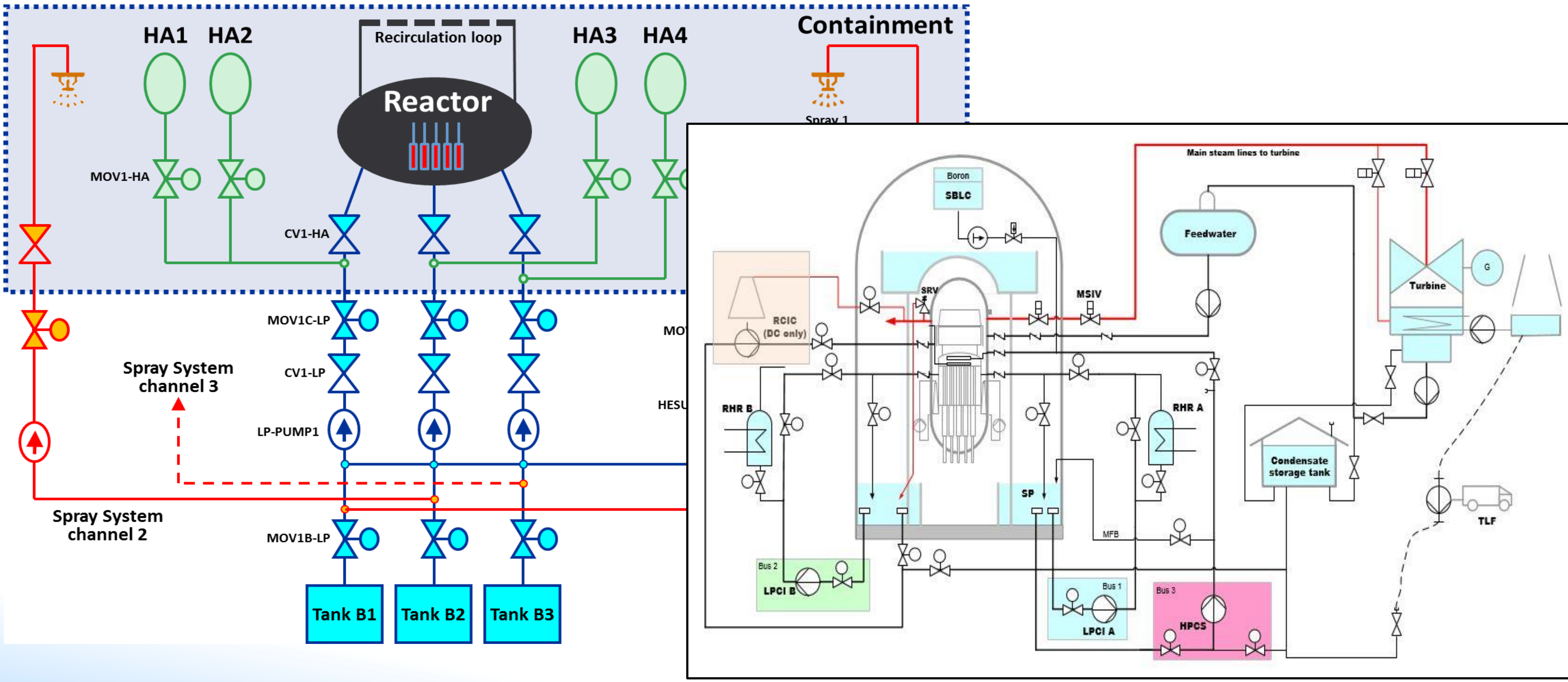
Education & Trainings

- Full scope PSA education & trainings for different type of audience
- PSA newcomers have issues with hands-on modeling experience
- Practical education & trainings are very efficient



Education & Trainings

- The trainees are the PSA team doing a PSA for a NPP
- Artificial NPP: simplified safety systems, artificial data



** Examples are available for PWR and BWR, could be adjusted for the needs of a Member State*

Education & Trainings: Process

- Developing pieces of the PSA model in groups
  - Splitting modelling tasks between the groups of trainees (ETs, FTs)
  - Independent work & interaction between the groups
  - Integration of the results (integral plant model in PSA software)
  - Documenting the analysis
- ‘Living’ agenda

Summary

Summary

- Safety is maintained by ensuring that risks are maintained As Low As Reasonably Practicable
- PSA is a tremendously powerful tool to determine the risk profile and assessing weaknesses of a NPP:
  - Guiding the optimization of the NPP design in the design phase, in an iterative process involving DSA and PSA
    - The optimized design is the one featuring an as **flat as possible distribution of risk profile,** because this confirms an optimal use of technical and financial resources
  - During the safety assessment for licensing purposes
- IAEA services in PSA capacity building: Technical Service Review and practical & theoretical trainings
  - Contact: Shahen Poghosyan, S.Poghosyan@iaea.org

…Thank you for your attention

S.Massara@iaea.org