NARSIS Workshop

aining on Probabilistic Safety Assessment for Nuclear Facilit

September 2-5, 2019, Warsaw, Poland

PSA: Main Elements and Role in the Process of Safety Assessment and Verification

Ivan Vrbanic, APOSS, Croatia

Overview

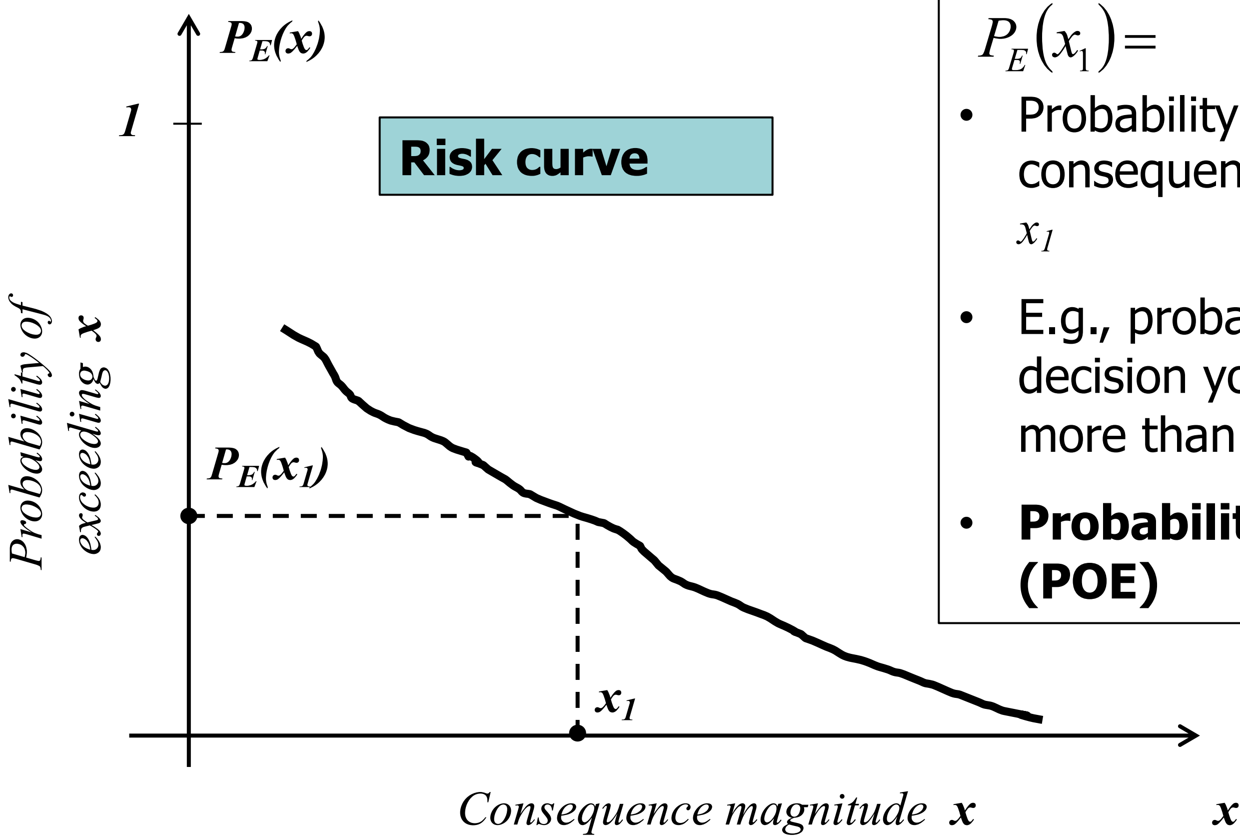
- Risk curve
- Definition of risk in engineer’s terms
- Risk control (risk management)
- Risk modeling – probabilistic safety (risk) assessment (PSA)
- Main technical elements of PSA
- A word on combined use of deterministic safety analyses and PSA in design safety verification

Introduction

- Exposure to a possibility of undesired consequences represents **risk**
- To possible undesired consequences you can be exposed:
  - Once / in a single specific occasion (e.g. single specific and important decision to be made)
  - Periodically or occasionally (e.g. decisions or actions of repetitive nature);
  - Continuously (e.g. natural hazards such as earhquake).
- For different people, risk means different things
  - Definition, i.e. formulation of term "risk" for an **engineer**.

Risk Curve

- Mathematical formulation of (single exposure)



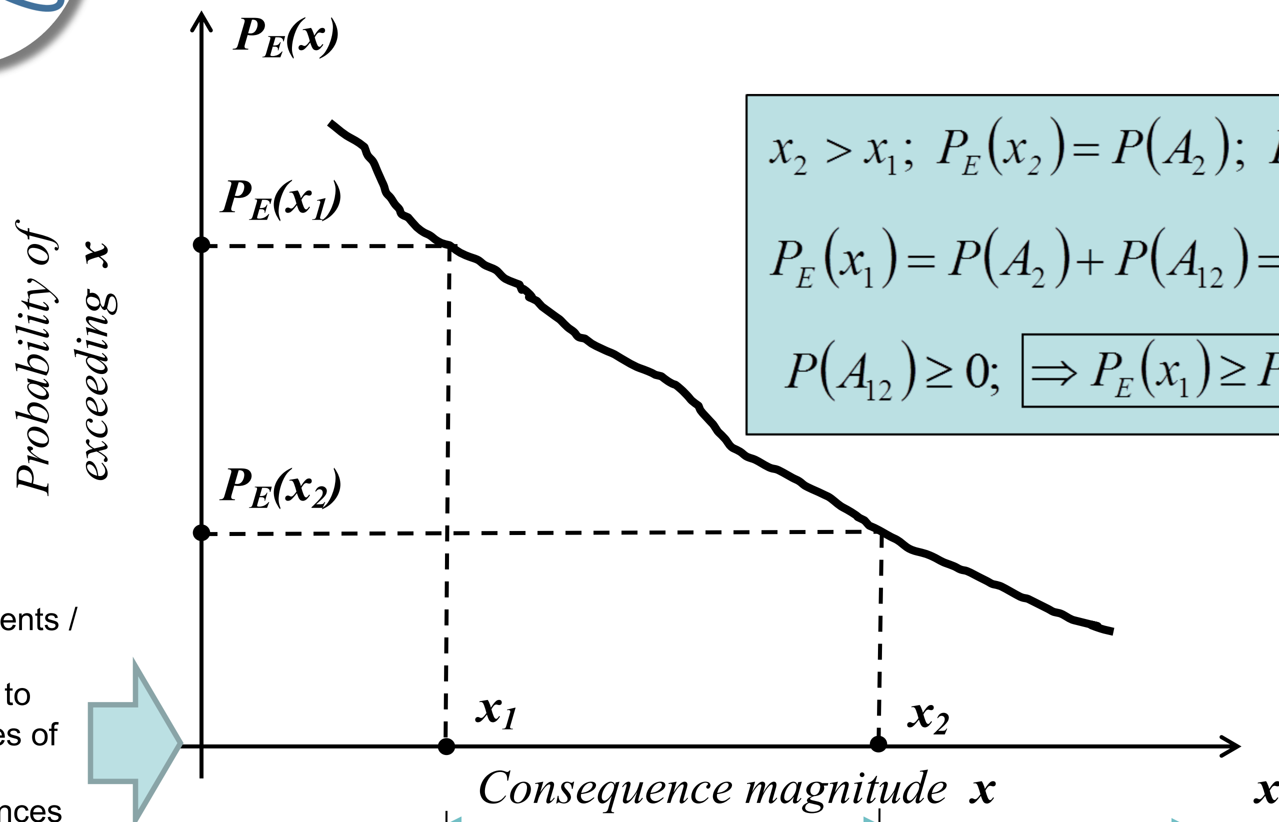
$P_E(x_1) =$

- Probability that undesired consequence exceeds magnitude x_1
- E.g., probability that because of decision you are making you loose more than 100 kEUR
- **Probability of Exceeding (POE)**

Risk Curve

- Important to notice: risk curve is, mathematically, a **decreasing** curve
  - Larger consequences → smaller probabilities
  - (next page)

Risk Curve



$$x_2 > x_1;\; P_E(x_2) = P(A_2);\; P_E(x_1) = P(A_1)$$

$$P_E(x_1) = P(A_2) + P(A_{12}) = P_E(x_2) + P(A_{12})$$

$$P(A_{12}) \geq 0;\; \boxed{\Rightarrow P_E(x_1) \geq P_E(x_2)}$$

Sort all events / scenarios according to magnitudes of their consequences

All events / scenarios with consequence magnitude $x_1 \leq x < x_2$ $(set\ A_{12})$

All events / scenarios with consequence magnitude $x_2 \leq x$ $(set\ A_2)$

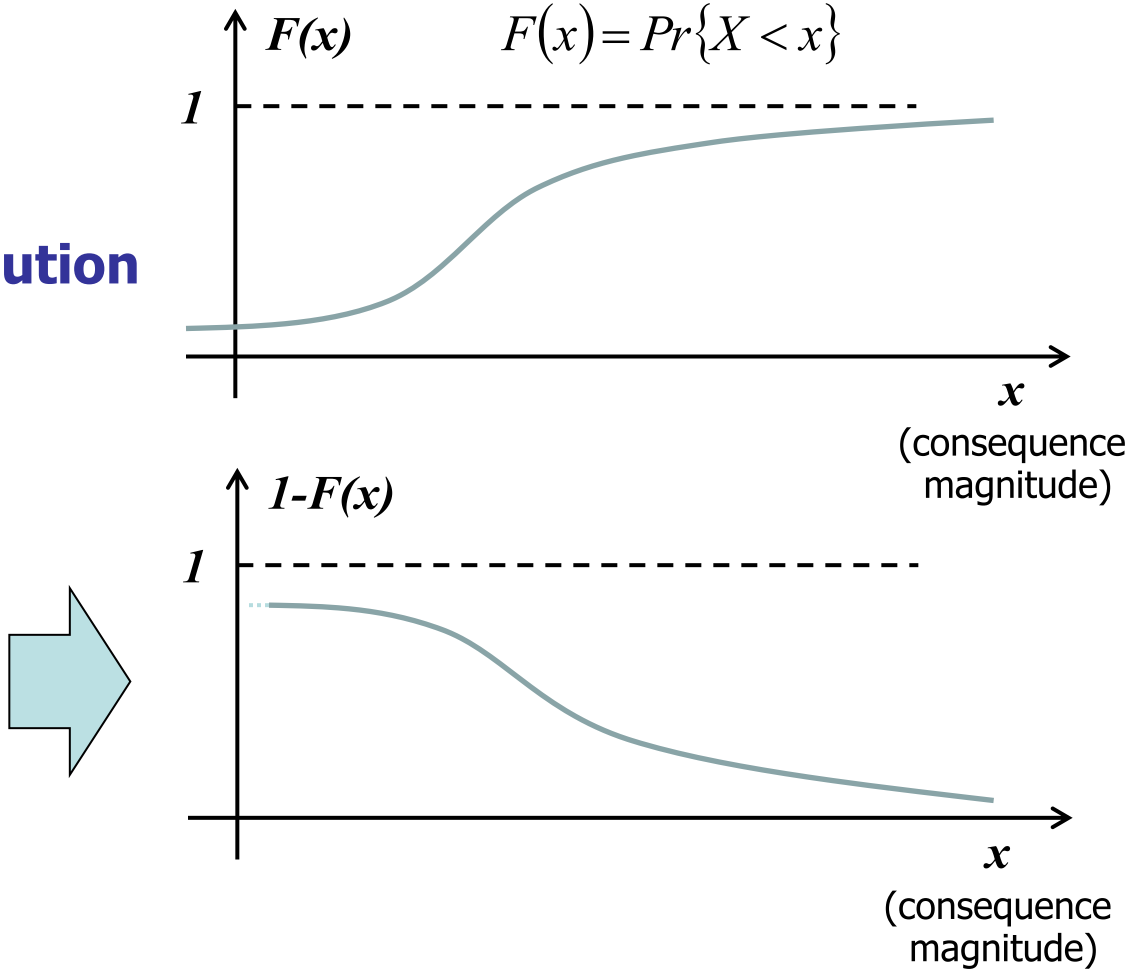
All events / scenarios with consequence magnitude $x_1 \leq x$ $(set\ A_1)$

Risk Curve

- Note:
  - Risk curve as **Complementary Cumulative Distribution Function (CCDF)**

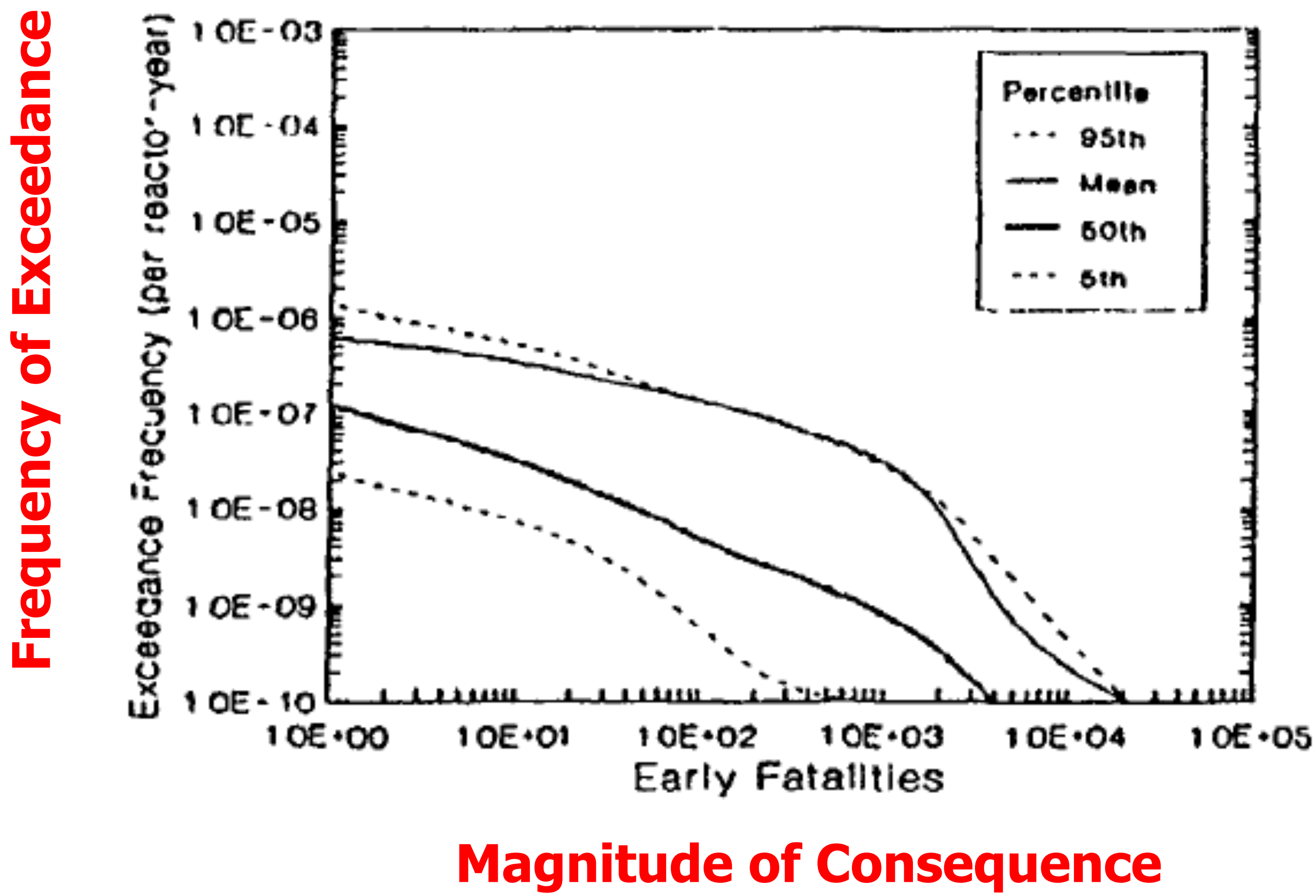
By definition:

$$F(x) = Pr\{X < x\}$$



Risk Curve

- Example (CCDF) from NUREG-1150



Risk Definition

- **Probability of occurrence (POO)** of event with consequence magnitude between x_1 and x_2:

$$P_O(x_1, x_2) = P_E(x_1) - P_E(x_2); \quad x_2 > x_1$$

  - Infinitesimal case:

$$P_O(x, x+dx) = -dP_E(x)$$

Risk Definition

- For technical engineering, **definition of risk** is derived from the general principle:
  - Risk increases with probability of harmful events and magnitude of undesired consequences
- Thus, risk from event with consequence x:

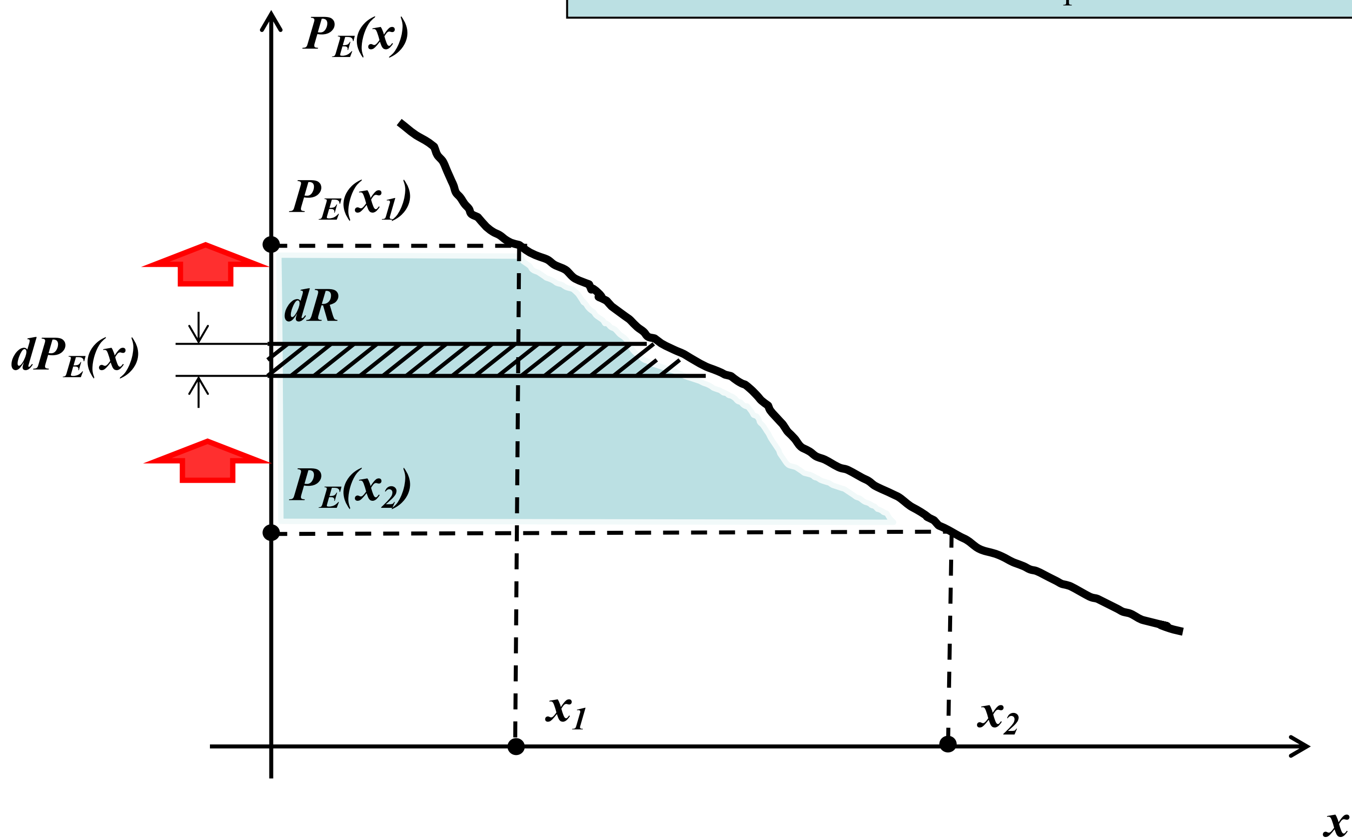
$$dR(x) = P_O(x, x + dx)\, x = -dP_E(x)\, x$$

- And risk from event with consequence between x_1 and x_2:

$$R(x_1, x_2) = -\int_{x=x_1}^{x=x_2} x \, dP_E(x)$$

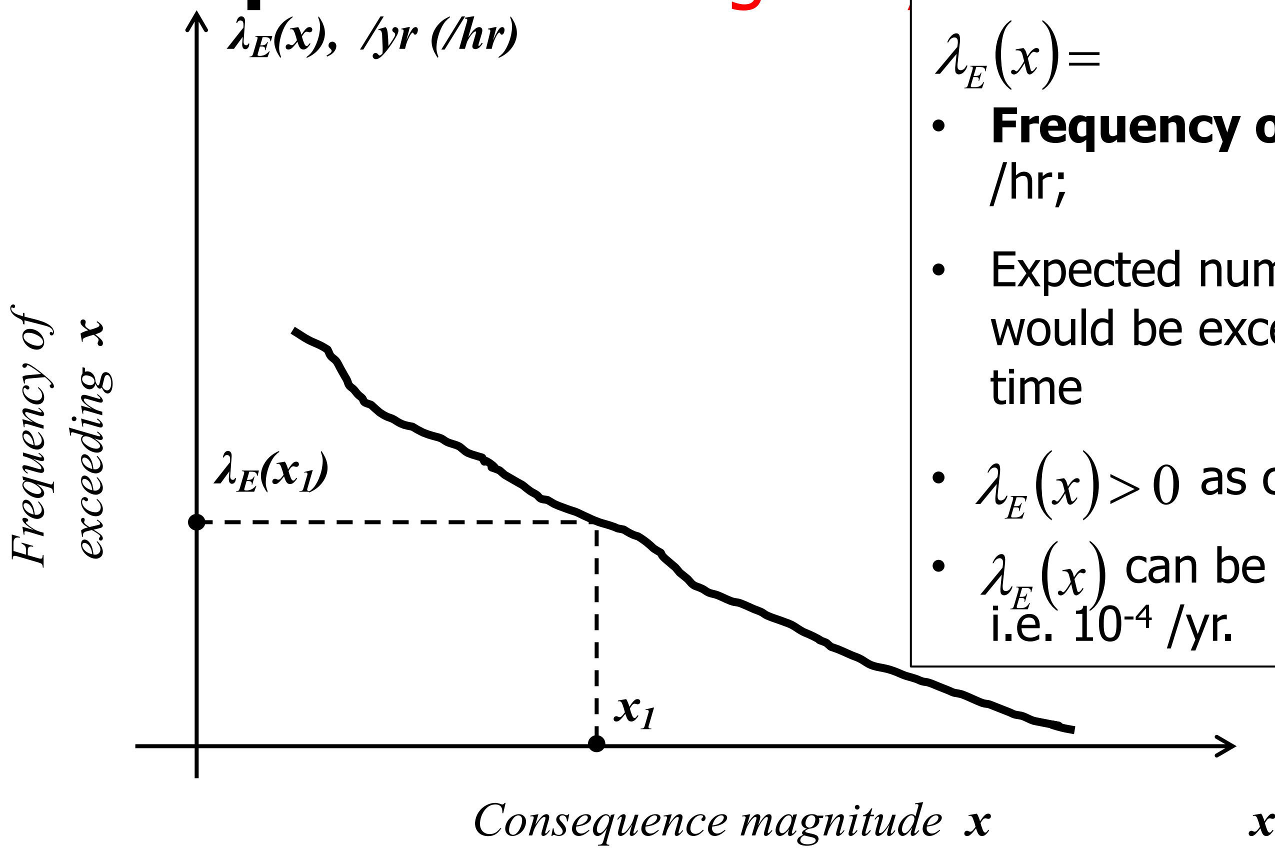
Risk Definition

$$R(x_1, x_2) = -\int_{x=x_1}^{x=x_2} x \, dP_E(x) = \int_{P_E(x_2)}^{P_E(x_1)} x \, dP_E(x)$$



Risk at Continuous Exposure

- Mathematical formulation of risk at **continuous exposure**: analogously



$\lambda_E(x) =$

- **Frequency of exceeding (FOE)**, /yr, /hr;
- Expected number of times magnitude x would be exceeded during a unit of time
- $\lambda_E(x) > 0$ as compared to $0 < P_E(x) < 1$
- $\lambda_E(x)$ can be 10 /yr or once in 10^4 yr, i.e. 10^{-4} /yr.

Risk at Continuous Exposure

- Like with $P_E(x)$, curve inevitably decreases:
  - If $x_2 > x_1$, then $\lambda_E(x_2) \leq \lambda_E(x_1)$
  - Specifically:

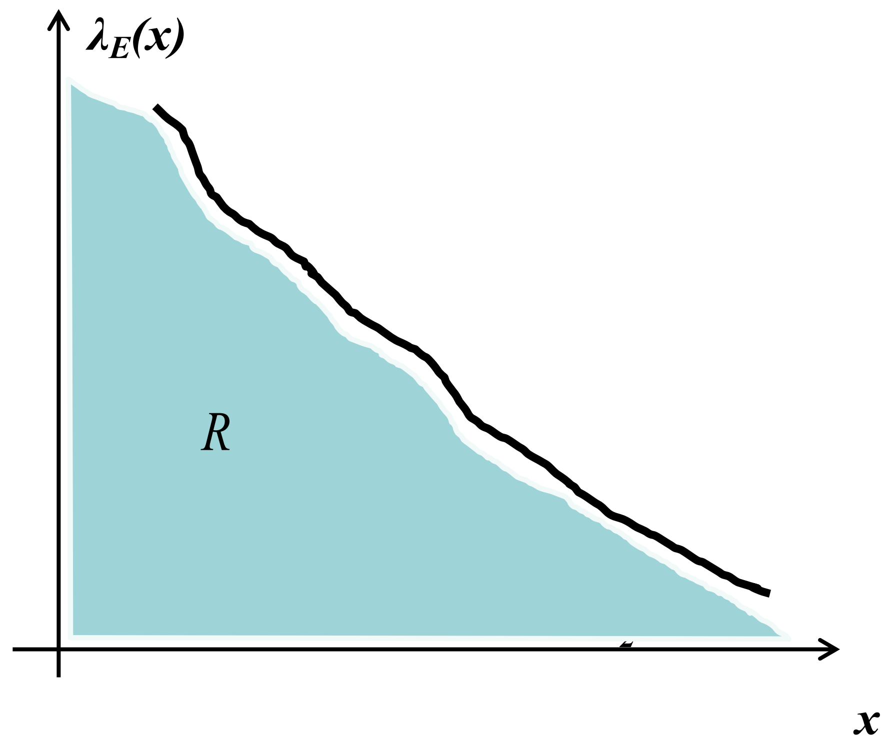
$$\boxed{\lambda_E(x_1) = \lambda_O(x_1, x_2) + \lambda_E(x_2)}$$

  - Where $\lambda_O(x_1, x_2)$ **frequency of occurrence** of events / scenarios with consequence magnitude between x_1 and x_2

Risk at Continuous Exposure

- Risk definition is analogous.
- Total risk:

$$R = -\int_{x \to -\infty}^{x \to \infty} x \, d\lambda_E(x)$$



Risk – Engineer's Definition

- **Simplification** of "risk" definition for practical engineering applications:
  - Risk from a **class of events (scenarios)**
  - Assume there is a class of events producing **approximately same** consequence, or such events for which the consequence can be **averaged** or **represented**

$$R(x_1, x_2) = \left| \int_{x=x_1}^{x=x_2} \bar{x}\, d\lambda_E(x) \right| = \bar{x} \left| \int_{x=x_1}^{x=x_2} d\lambda_E(x) \right| = \lambda_{tot}\bar{x}$$

Risk – Engineer's Definition

- Simplified, for practical purposes, definition:

Risk = Probability x Consequence

Risk = Frequency x Consequence

- Usually provided in literature on practical engineering applications
- Applies to **classes of events**
  - Typically, used for risk management in the form of some kind of **risk matrix** (which represents simplified risk curve)

Example: Consideration of Risk in NPP Safety Applications

- Risk Curve:
  - Usually, simplified by means of **predefined classes of consequences or conditions**
- Examples of most frequently used:
  - Reactor core damage;
  - Large release;
  - Large early release;
- However, others also in use, e.g.:
  - Entering BDB condition;
  - Boiling of coolant in reactor / cavity during shutdown modes;
  - Spent fuel pool (SFP) boiling;
  - Fuel uncovering in SFP
  - ...

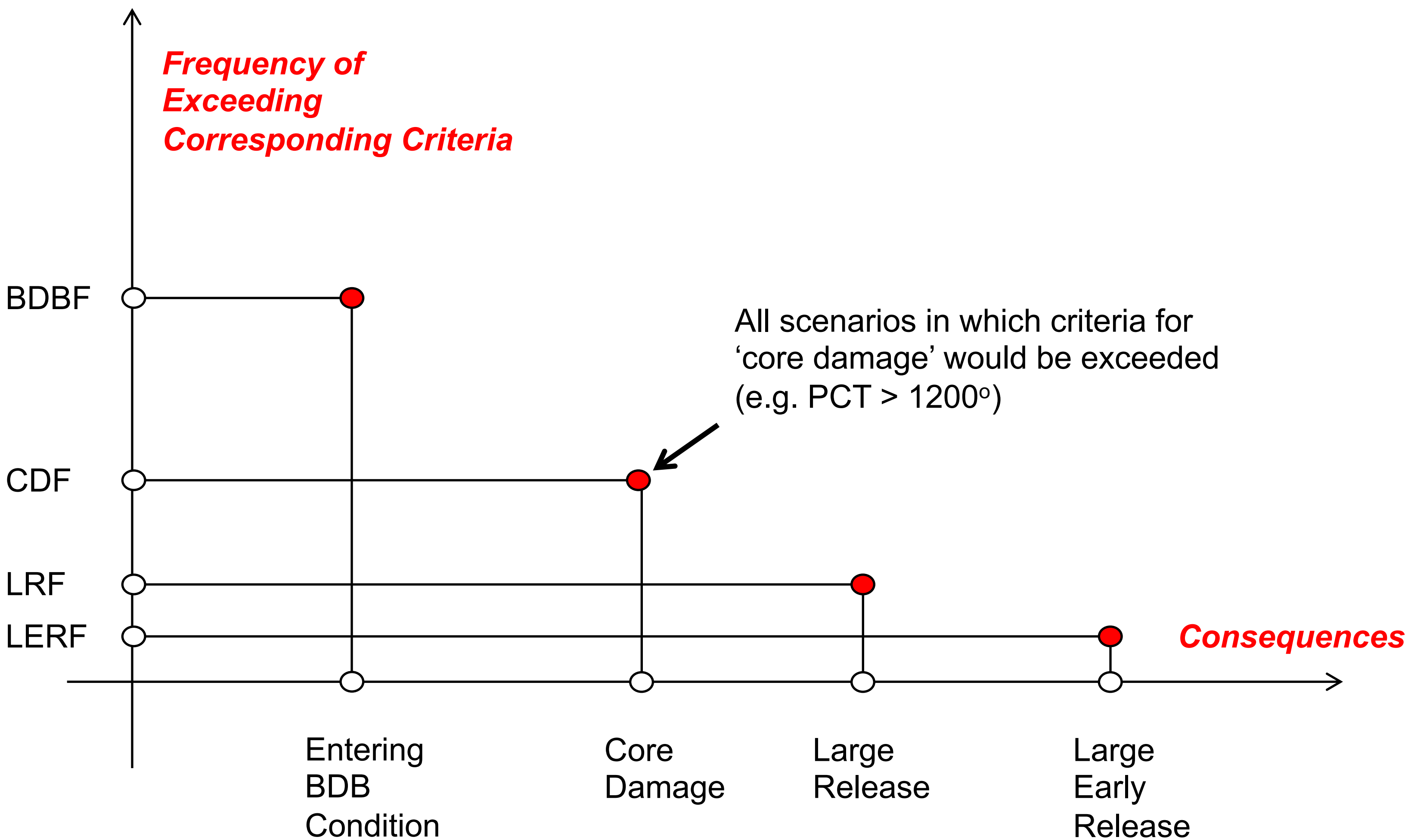
Example: Consideration of Risk in NPP Safety Applications

- Frequencies or probabilities of predefined consequence classes
  - **Quantitative risk metrics**
- Examples of most frequently used:
  - Core Damage Frequency (CDF);
  - Large Release Frequency (LRF);
  - Large Early Release Frequency (LERF);
- Examples of others, also in use:
  - Frequency of entering BDB condition;
  - RC boiling frequency (shutdown modes);
  - SFP boiling frequency;
  - SFP fuel uncovering frequency
  - ...

Example: Consideration of Risk in NPP Safety Applications

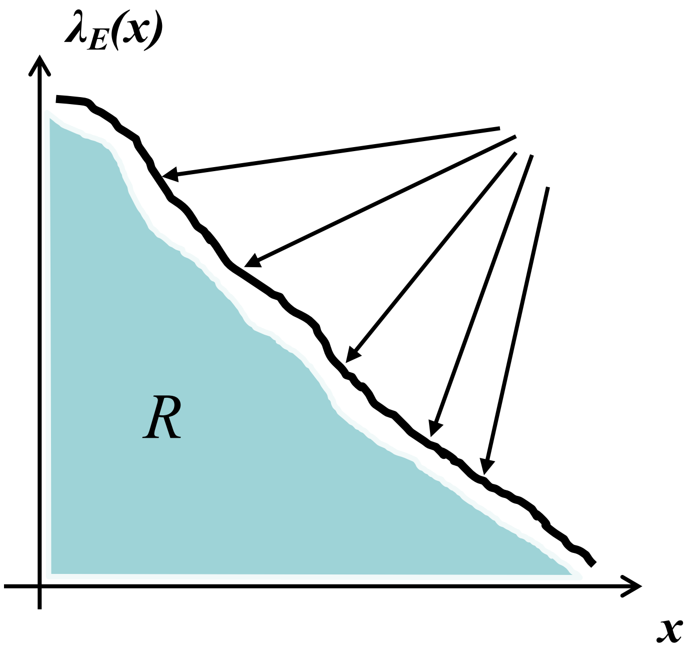
- Consider:
  - '**Entering BDB Condition**' as a consequence
    - Effectively lower than 'core damage' as consequence, because:
      - Only some of 'BDB condition' scenarios would result with 'core damage'
        - » Example: PWR Rx trip with loss of all MFW and EFW
        - » Initiate Primary Feed and Bleed
    - Hence: BDB Frequency bounds CDF (**BDBF > CDF**)
  - '**Core Damage**' as a consequence
    - Effectively lower than 'large release' as consequence, because:
      - Only some of 'core damage' scenarios would lead to 'large release'
    - Hence: CDF bounds LRF (**CDF > LRF**)
  - '**Large Release**' as a consequence
    - Effectively lower than 'large early release' consequence, because:
      - Only some of 'large release' scenarios would be 'large early release'
    - Hence: LRF bounds LERF (**LRF > LERF**)

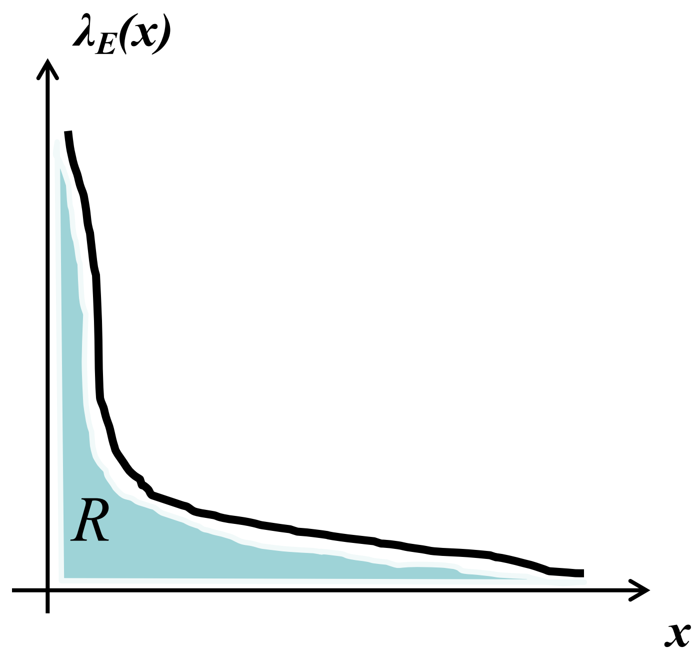
Consideration of Risk in NPP Safety Applications



Risk Control (Risk Management)

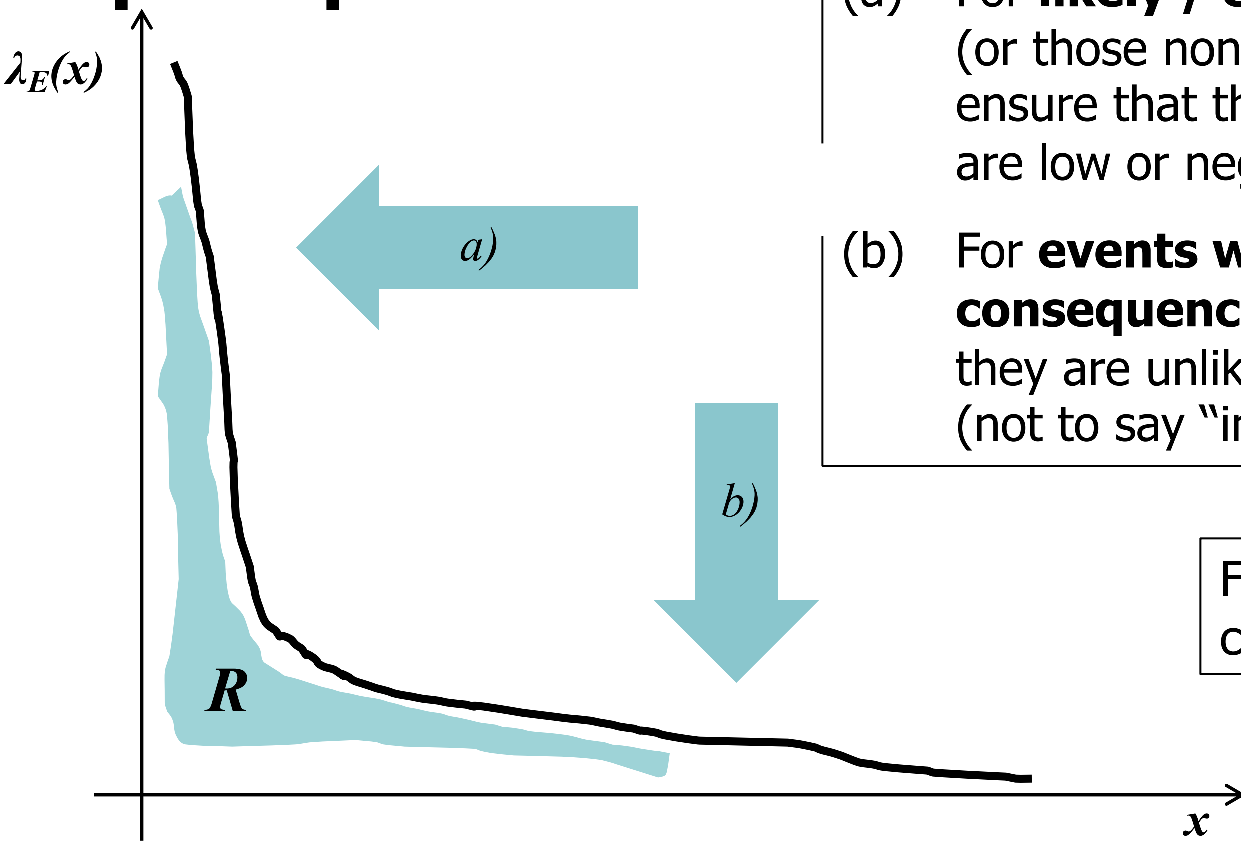
- Control over risk (risk management):
  - To conduct processes and projects, make decisions and expose to conditions in a manner that ***R*** is as small as possible





Risk Control

- Risk control (management) based on **two main principles**:



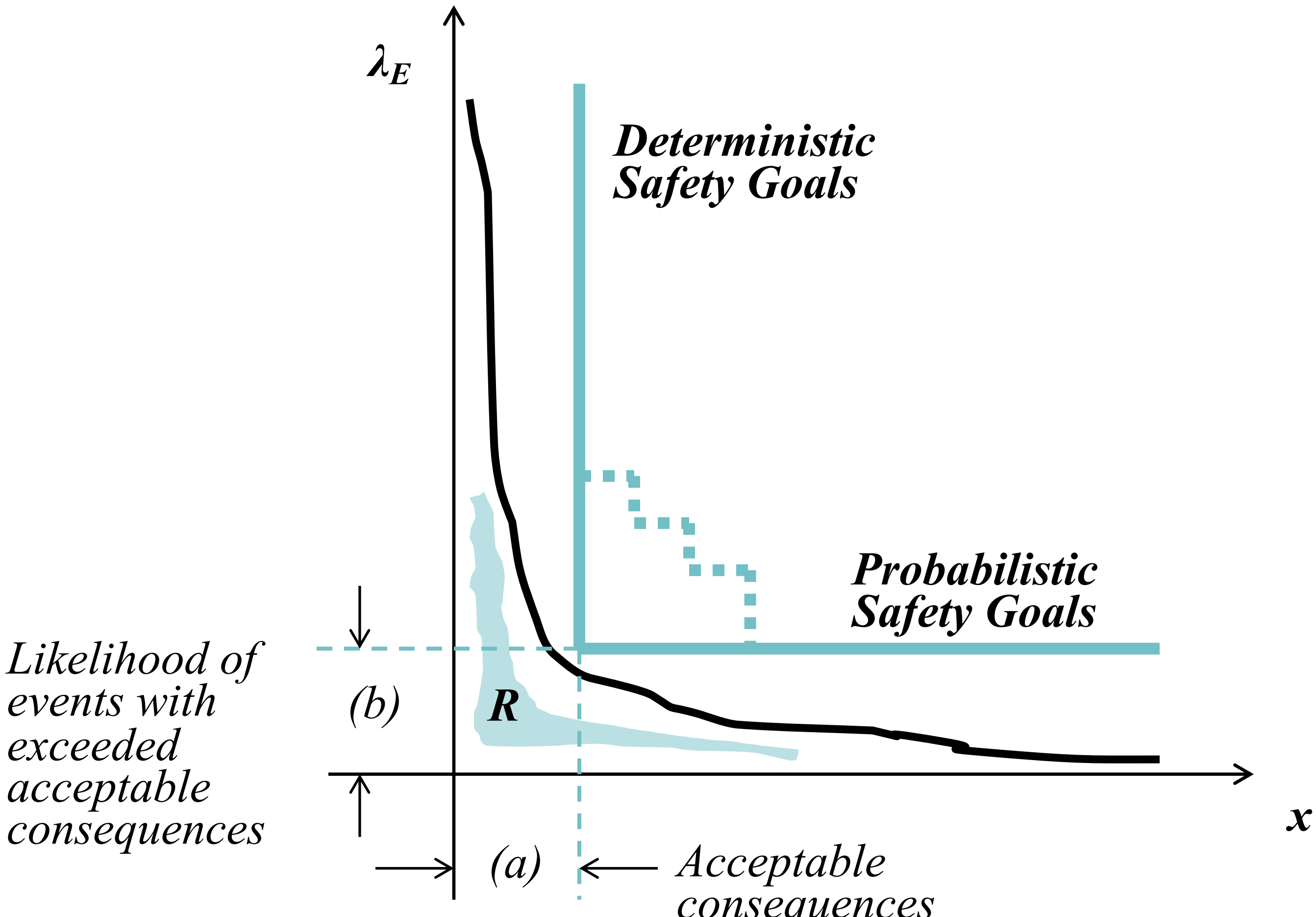
(a) For **likely / expected events** (or those non-avoidable) ensure that their consequences are low or negligible

(b) For **events with large consequences** ensure that they are unlikely or improbable (not to say "impossible")

For "others", use combined approach

Risk Control

- Two types of acceptance criteria (goals, targets)



Risk Model

- Risk from a consequence of class x:

Logical model	Quantitative model
$R = H\,V\,C_x$	$R = \lambda_{OH}\,Q\,x$

H	Hazard;
V	Vulnerability of system;
C_x	Consequence of class x

λ_{OH}	Hazard frequency;
Q	Probability of inducing damage which leads to consequence C_x;
x	Measure of consequence C_x (e.g. financial loss)

Risk Model

- For risk to "materialise":
  1. There must be a hazard, **and**
  2. System / process must be vulnerable to a hazard, **and**
  3. Vulnerability must produce undesired consequences.
- These are **three elements of risk**.
  - In order to remove risk, it is "sufficient" to remove any of them.
- There is no risk if:
  1. There is no hazard, **or**
  2. System is not vulnerable, **or**
  3. No consequences can be produced.

Risk Model for Substituted Consequence (PSA)

- With specifically defined **representative** or **substitute** for consequence
  - E.g. 'core damage' or 'large early release'
- Risk equation

Risk = Frequency x Consequence

- Reduces, even further, to

Risk = Frequency (of relevant scenarios)

- Which **scenarios**?
  - Those leading to specified consequence
  - (Those where corresponding **criteria** would be **exceeded**).

Risk Model for Substituted Consequence (PSA)

- ‘Risk model’
  - **Logical and quantitative** model for occurrence of any scenario which can lead to specified consequence
  - **NPPs: PSA Level 1**: Risk model for ‘core damage’
  - **NPPs: PSA Level 2**: Risk model for ‘radioactivity release’ (including ‘large early release’)
- Two elements (factors in equation):
  - **Hazard** or initiator; and
  - **Vulnerability** of system (facility) to hazard / initiator
    - Such that it can result in exceeding the criteria and leadin to specified consequence

Risk Model for Substituted Consequence (PSA)

- Risk model (PSA model) has **two main layers**:

Logical model	Quantitative model
$$R = H\,V$$	$$r = \lambda\, q$$

H	Hazard;
V	Vulnerability of system

λ	Hazard frequency;
Q	Probability of inducing damage which leads to specified consequence

- **Third layer**:
  - Characterization of **uncertainty**

Analitical Tools (Disciplines) for Risk Modeling in PSA

- First layer: Logical modeling
  - Event trees and fault trees
  - Supporting deterministic analyses
  - Boolean Algebra
- Second layer: Quantification:
  - Probability theory
  - Reliability theory
- Third layer: Characterization of uncertainty
  - Identification of uncertainty
  - Quantification of uncertainty
    - Random variables and distributions

Main Technical Elements of PSA

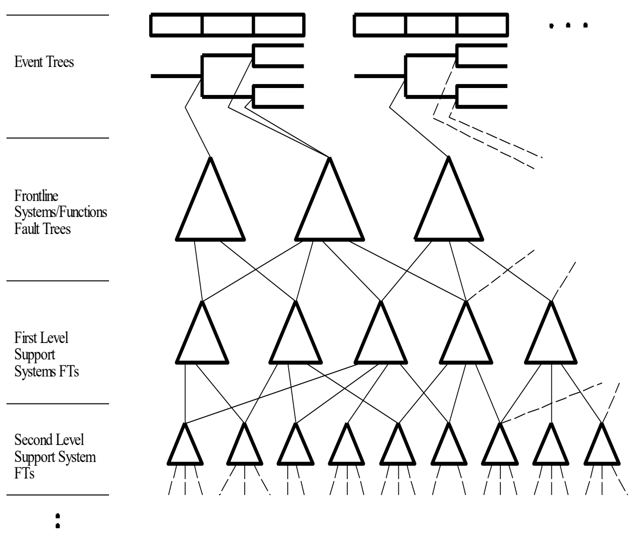
- Some internationally recognized standards for PSA:
  - "Development and Application of Level 1 Probabilistic Safety Assessment for Nuclear Power Plants", Specific Safety Guide No. SSG-3, International Atomic Energy Agency, Vienna, 2010
  - "Development and Application of Level 2 Probabilistic Safety Assessment for Nuclear Power Plants", Specific Safety Guide No. SSG-4, International Atomic Energy Agency, Vienna, 2010
  - ASME/ANS RA-Sa–2009. 2009, Addenda to ASME/ANS RA-S–2008, "Standard for Level 1/Large Early Release Frequency Probabilistic Risk Assessment for Nuclear Power Plant Applications", An American National Standard, The American Society of Mechanical Engineers, New York, 2009
  - ASME/ANS RA-S-1.2-2014, "Severe Accident Progression and Radiological Release (Level 2) PRA Standard for Nuclear Power Plant Applications for Light Water Reactors (LWRs), American Society of Mechanical Engineers - American Nuclear Society, January 2015
  - U.S. NRC Regulatory Guide 1.174, "An Approach for Using Probabilistic Risk Assessment in Risk-Informed Decisions on Plant-specific Changes to the Licensing Basis", Revision 2, U.S. Nuclear Regulatory Commission, May 2011
  - U.S. NRC Regulatory Guide 1.200, An Approach for Determining the Technical Adequacy of Probabilistic Risk Assessment Results for Risk-Informed Activities, Revision 2, U.S. NRC, 2009

Main Technical Elements of PSA

- For internal IEs at power:
  - Initiating Events Analysis;
  - Accident Sequence and Success Criteria Analyses;
  - Systems Analysis;
  - Human Reliability Analysis;
  - Data Analysis;
  - Dependent Failures Analysis;
  - Model Integration and Quantification; and
  - Results Interpretation.
- Additionally, specific technical elements for:
  - Other initiating event categories (e.g. external hazards), other modes of operation (e.g. shutdown modes) and other risk measures (e.g. risk from radioactivity releases).

Main Technical Elements of PSA

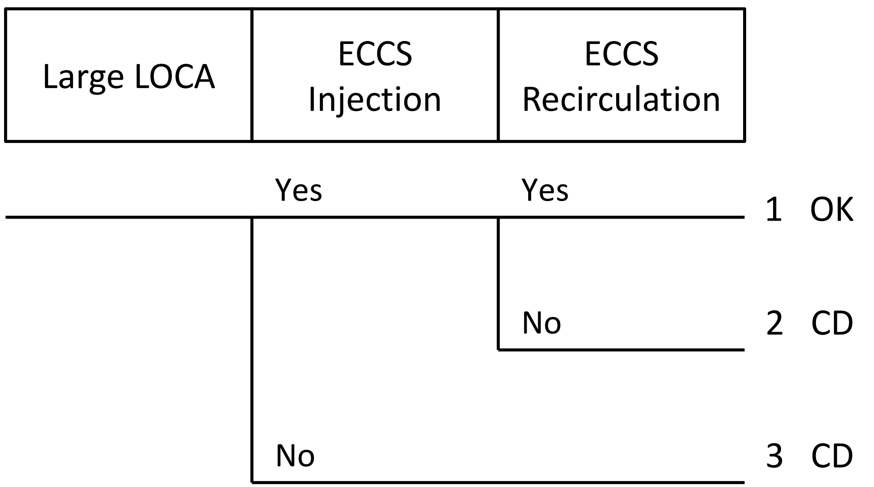
- "PSA model"
  - Large logic equation in which a top event (e.g. reactor core damage) is expressed in terms of initiators / hazards, equipment failures and human errors.
  - Usually built by means event trees (ET) and fault trees (FT)



Main Technical Elements of PSA

- Initiators, failures and errors in PSA model:
  - Represented by "basic events"
  - Top event (e.g. core damage) is, thus, expressed as logic function of "basic events".
- Key term in top event analysis / quantification:
  - "**Minimal cutset**" (MCS): Minimal combination of basic events leading to the top event
- Top event analysis / quantification usually done in two major steps:
  - <u>Identification of MCSs</u>: Logic function (ETs / FTs) by the rules of Boolean algebra resolved into the form of logic sum of MCSs;
    - List of MCSs generated;
  - <u>Quantification of top event</u>: logic sum of MCSs is used as a basis for calculating the top event probability or frequency (e.g. CDF).
- Quantified list of MCSs: basis for risk profiling and risk-importance evaluation

A Word on Combined Use of DSA and PSA in Safety Design Verification



Design basis sequence: At least 1 (out of 2) ECCS train successful in injection and recirculation.

- Not quantified by PSA. Covered by DBA.

Beyond design basis sequence: Both ECCS trains fail injection or/and recirculation.

- Quantified by PSA to demonstrate acceptably low risk. (Risk Assessment)

A Word on Combined Use of DSA and PSA in Safety Design Verification

- DB sequences: “success” sequences in PSA ETs
  - Covered by DB analyses in FSAR, with demonstration of adequate safety margins
  - Not quantified by PSA
- PSA quantifies risk from BDB sequences
  - Calculate probability (frequency) of BDB sequences to demonstrate acceptably low risk from getting out of DB envelope
  - Remark:
    - Not every BDB sequence is in PSA necessarily “failed” sequence
    - Example: successful feed and bleed sequence

The End

- Thank You for You attention!