Integrating Risk and Safety Margins

Mirela Gavrilas, Ph.D.

Office of Nuclear Regulatory Research

U.S. Nuclear Regulatory Commission

"The natural consequence of uncertainty is risk."

Bruce R. Ellingwood, NIST/Johns Hopkins University

…and our way of coping with uncertainty is operating with sufficient safety margins.

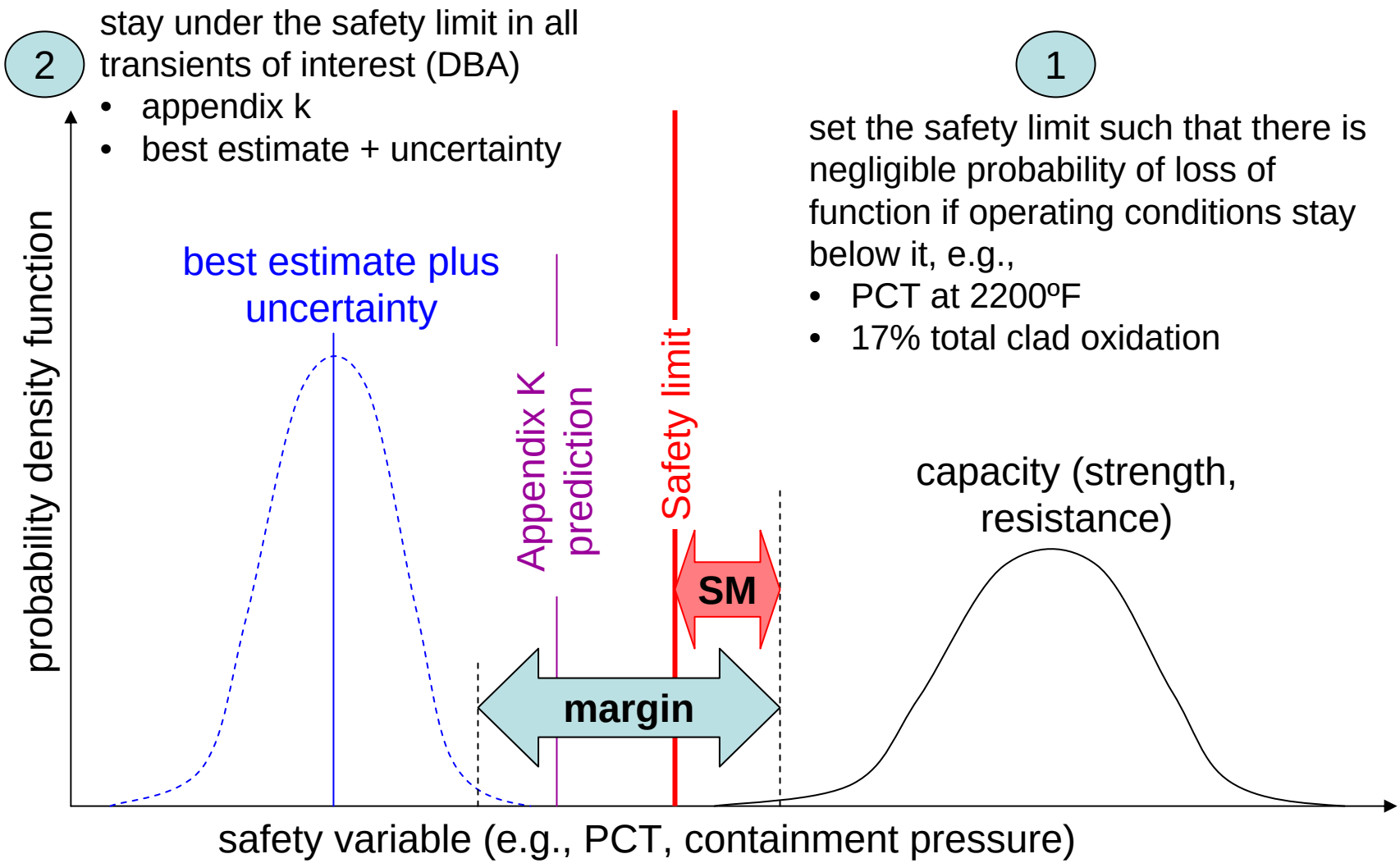
traditional “factor of safety”

the magnitude of the safety margin for a given safety variable is a function of

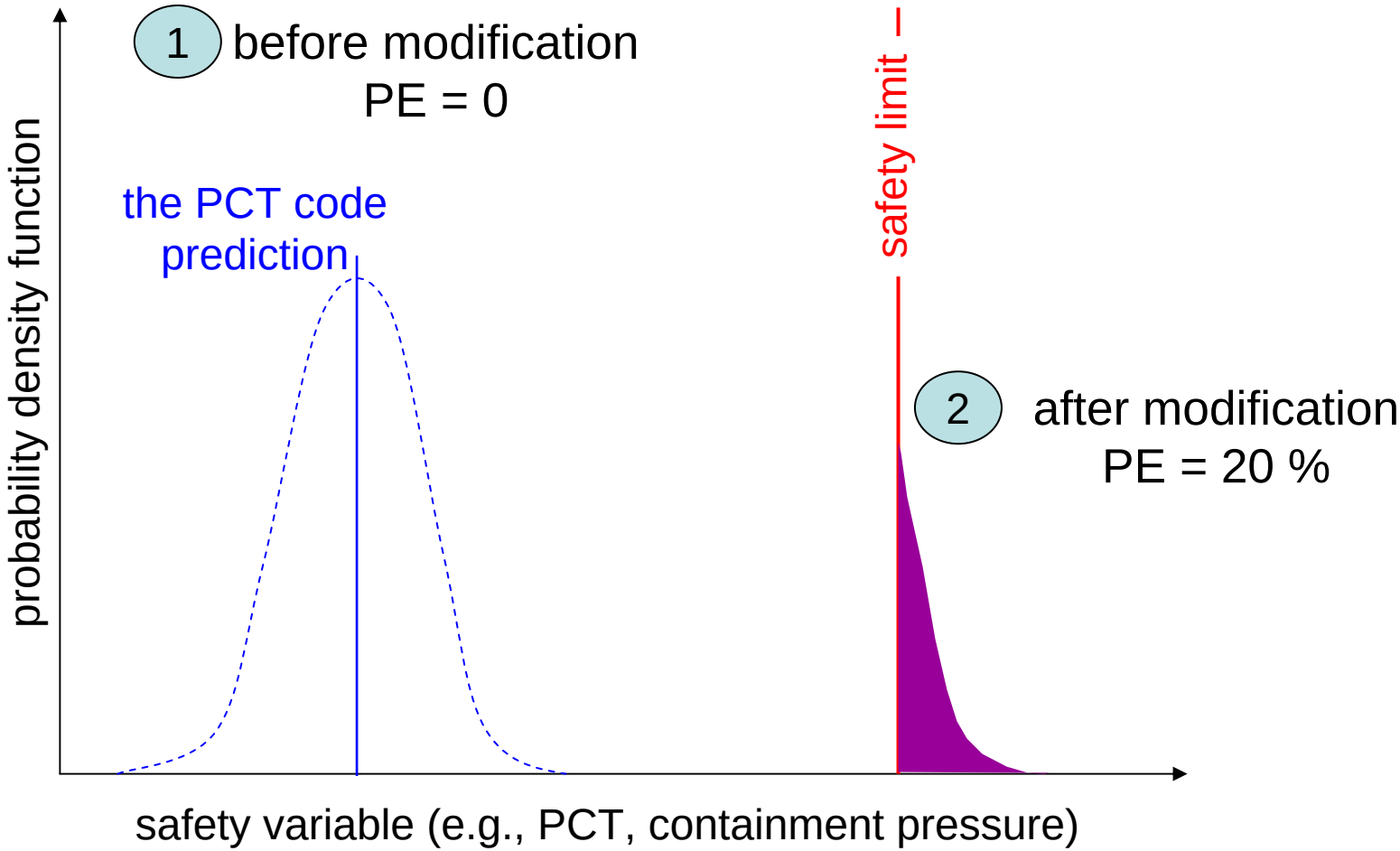
- accuracy/precision of load
- accuracy/precision of strength
- consequences of failure
- cost of over-engineering

additional protection against unknown-unknowns

safety margin for the nuclear authority



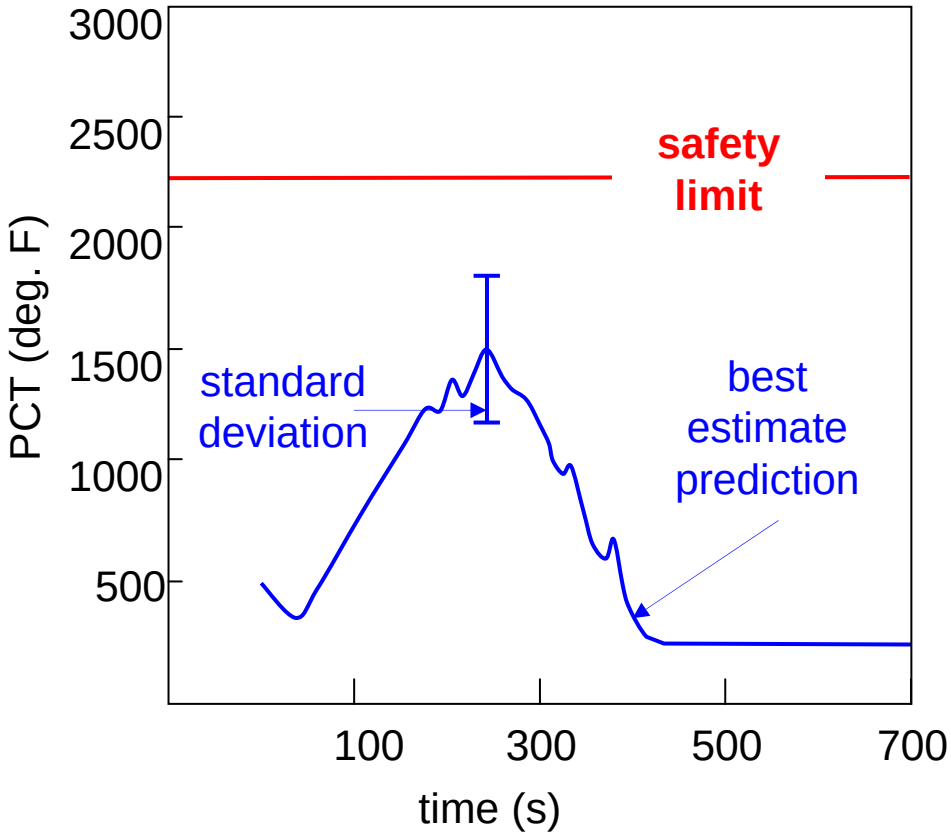
the amount by which the load exceeds the safety limit
probability of exceedance, PE



how can risk and safety margins be integrated?

any deterministic calculation
- assumes a specific series of events, e.g.,

a break of a specific size has occurred
- when a certain actuation signal is received, the injection system starts
- when a certain pressure is reached, the accumulators inject



⇒ ***the peak clad temperature computed deterministically is "conditioned" on the event sequence simulated.***

what is the probability of losing function in an event sequence?

probability that event sequence will occur

&

exceedance probability (assume the core will loose function)

from event tree frequency

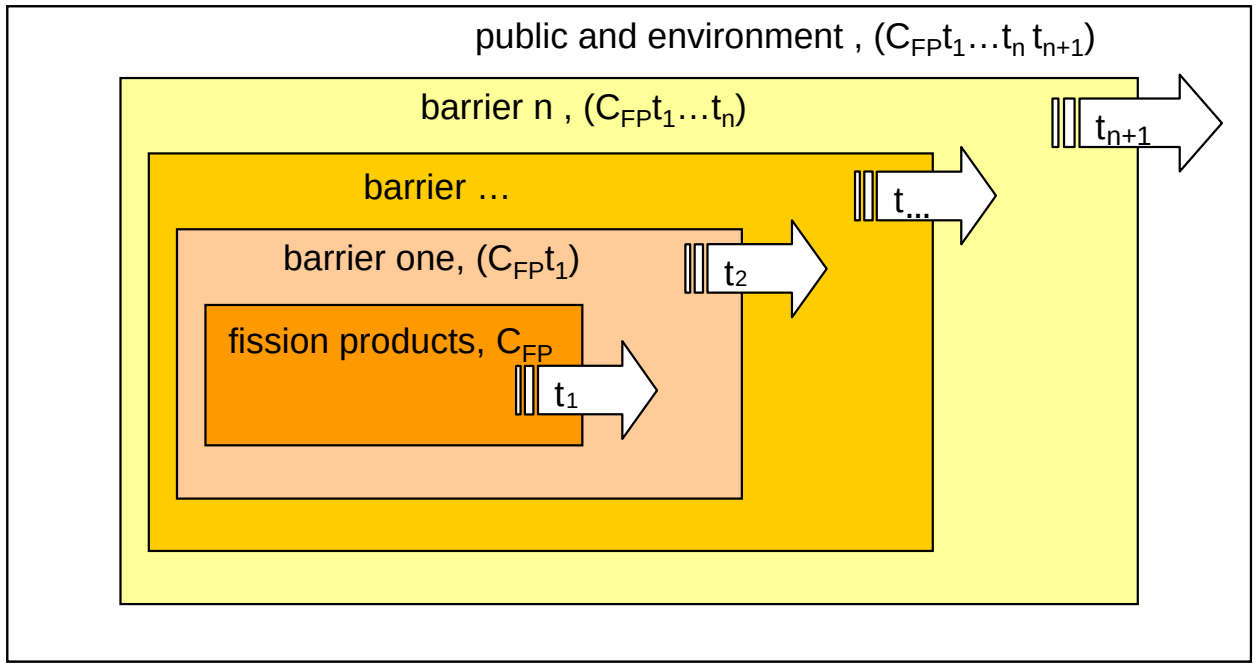
from engineering data, safety limits and deterministic calculations (the PE)

generalizing to multiple barriers: beyond CDF to QHO

premises:

- any existing or future nuclear power plant can be summarily described as a volume that contains the fuel and fission products surrounded by one or more physical barriers (this would include barriers electro-magnetic confinement or other radical departures from current designs)
- for any physical barrier, safety variables can be identified that demarcate the transition from intact to damaged, (e.g., PCT, enthalpy deposition rate, containment pressure)
- PRA tools exist to identify event scenarios that can lead to the loss of margin of any barrier

consequences of an event scenario in which barrier n is lost



($C_{FP}t…$)—concentration of fission products within the barrier

t_n—transmission factor from barrier n to barrier n+1 is a function of:

- volume confined by each barrier
- extent of damage to the barrier
- time between the breach of successive barriers
- pool scrubbing, …

risk from a single event sequence

probability

probability that event sequence will occur, p_{ES} & probability that barrier 1 will fail, PE_{B1} & … & probability that barrier n will fail , PE_{Bn}

from event tree analysis

from engineering data and deterministic calculations; this is a ***conditional probability***

consequences

$C_{FP}t_1 \ldots t_n$

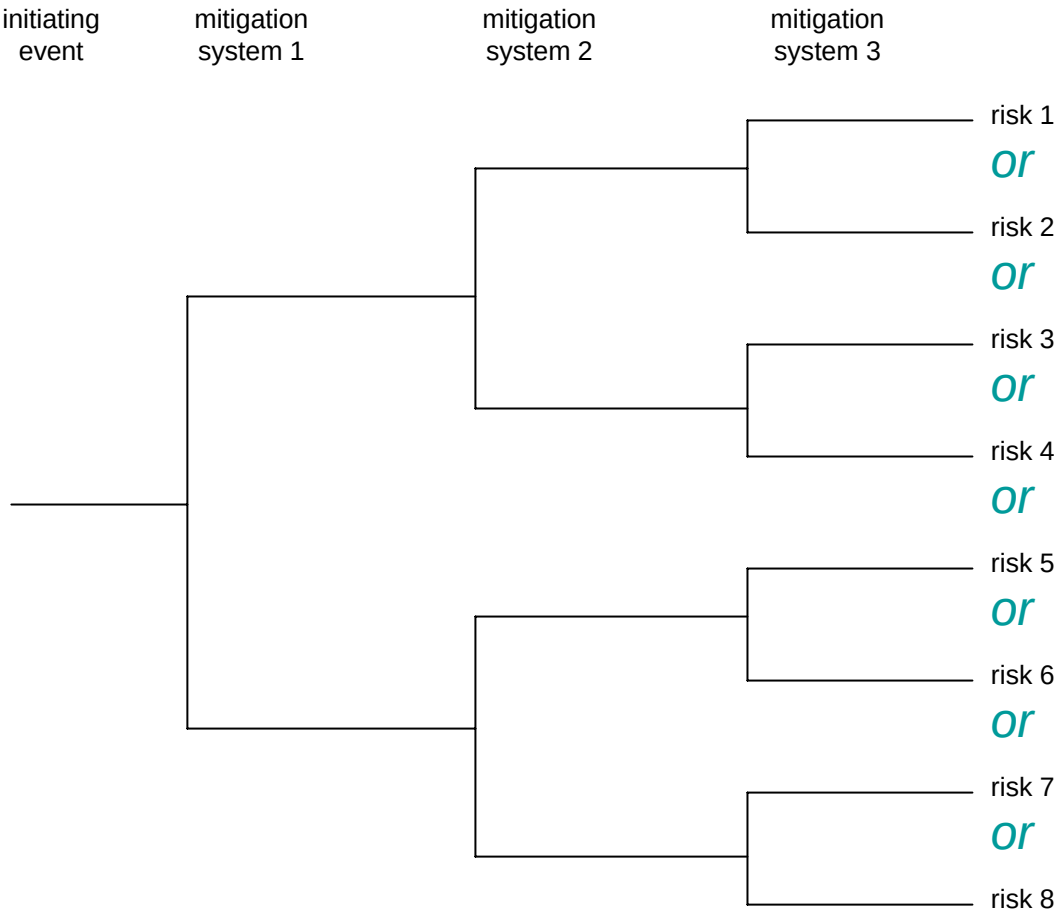
from deterministic calculations

risk for event sequence i

$$risk_i = p_{ES,i} \cdot PE_{B1,i} \cdot \ldots \cdot PE_{Bn,i} \cdot (C_{FP,i}\, t_{1,i} \ldots t_{n,i})$$

risk from all event sequences

assuming that only one event can occur at any given time:



$$\text{total risk} = \sum_i \text{risk}_i$$

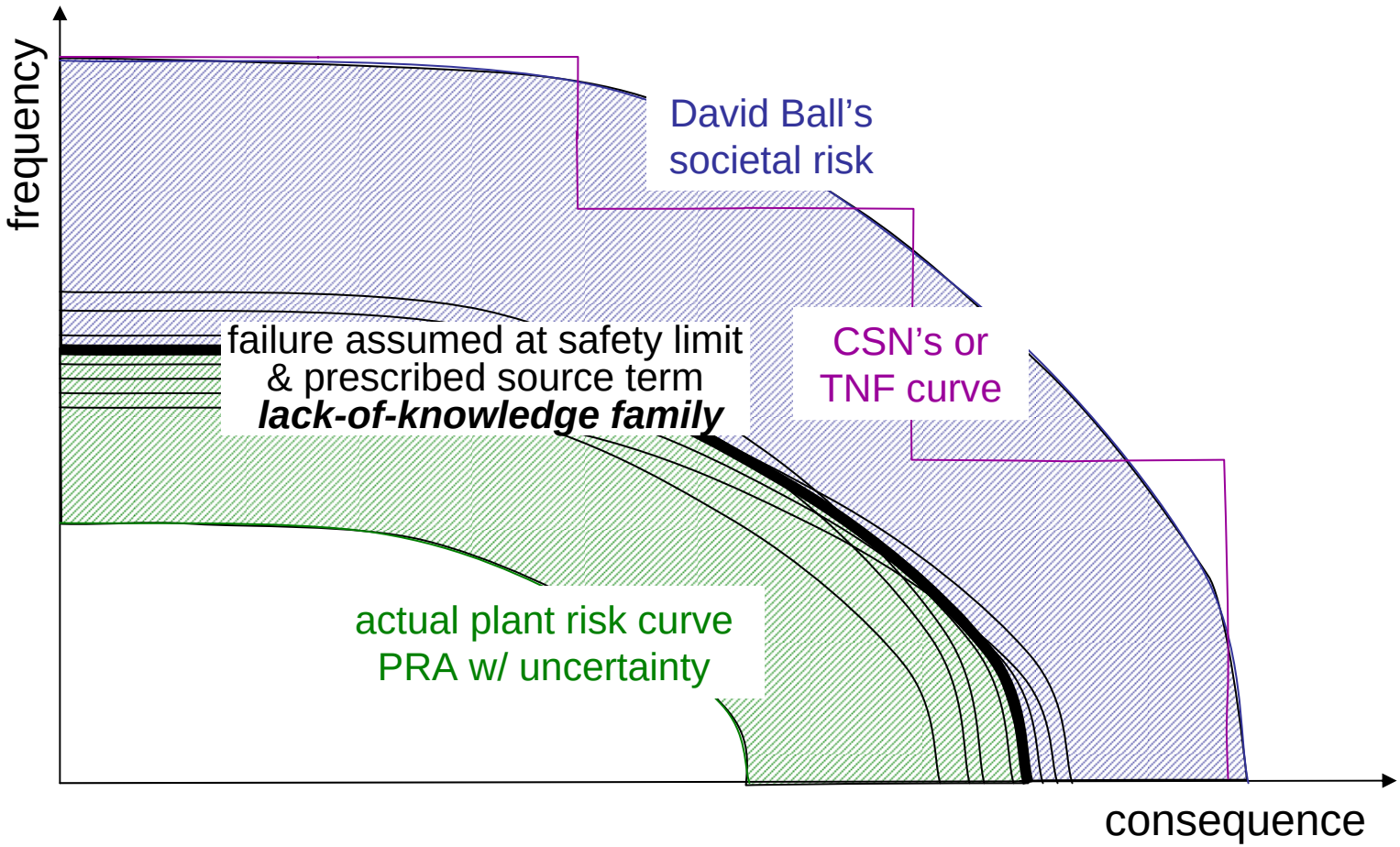
compare to Commission's safety goals or RG 1.174 thresholds and/or generate F-C curve

separating aleatory and epistemic uncertainty

- expand trees to capture aleatory (***natural randomness***) uncertainty
- propagate epistemic (***lack-of-knowledge***) uncertainty along each branch
  - there will be multiple values of risk at the end of each branch (all equally likely to occur)
- decide on how to integrate the risk from all event sequences in a tree (and subsequently in multiple trees)—traditional PRA techniques, evidence theory

relationship to F-C curve

10CFR Appendix A to Part 50--General Design Criteria for Nuclear Power Plants:
"sufficient margin for the **limited accuracy, quantity, and time in which the historical data have been accumulated**"—dictates blue area



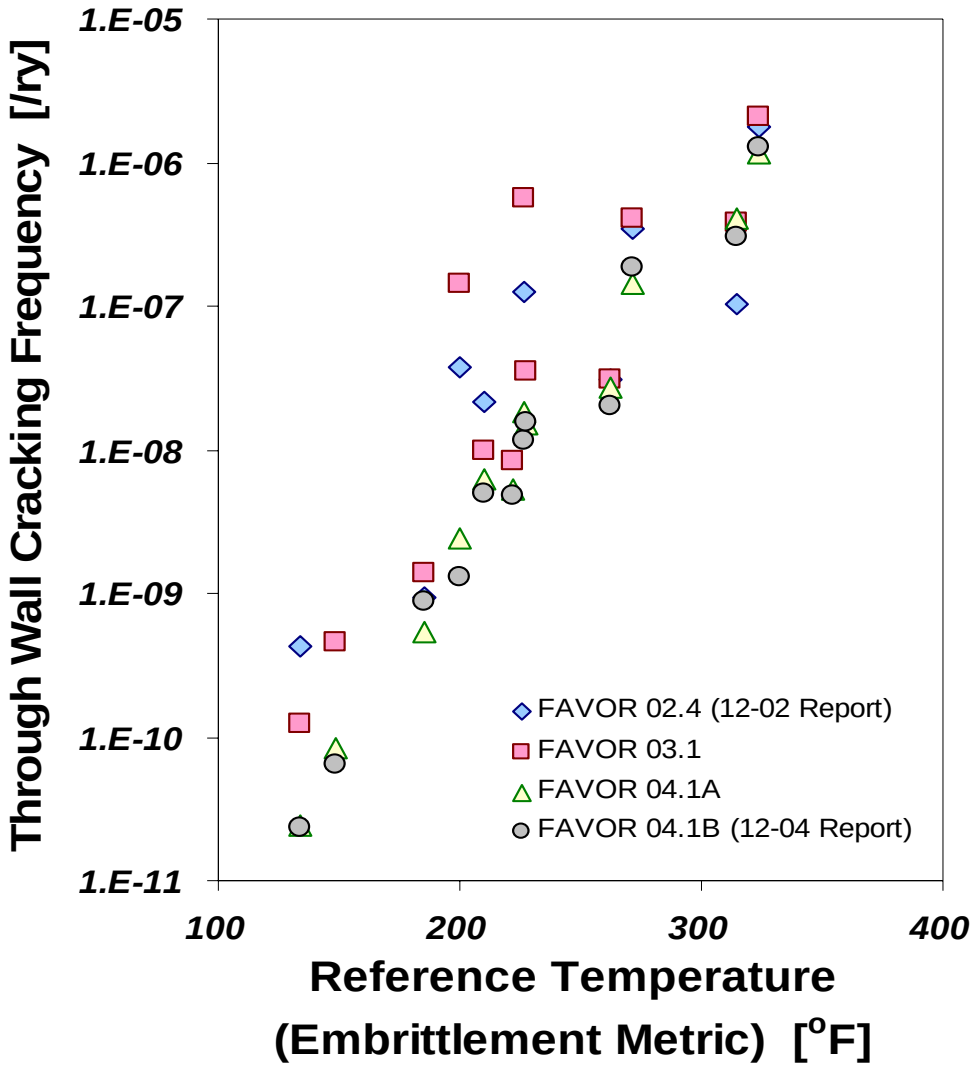
future work

- what is adequate safety margin
  - for a single accident sequence:
    - failure mechanism
    - barrier
    - consequences
  - for the whole risk space of a plant

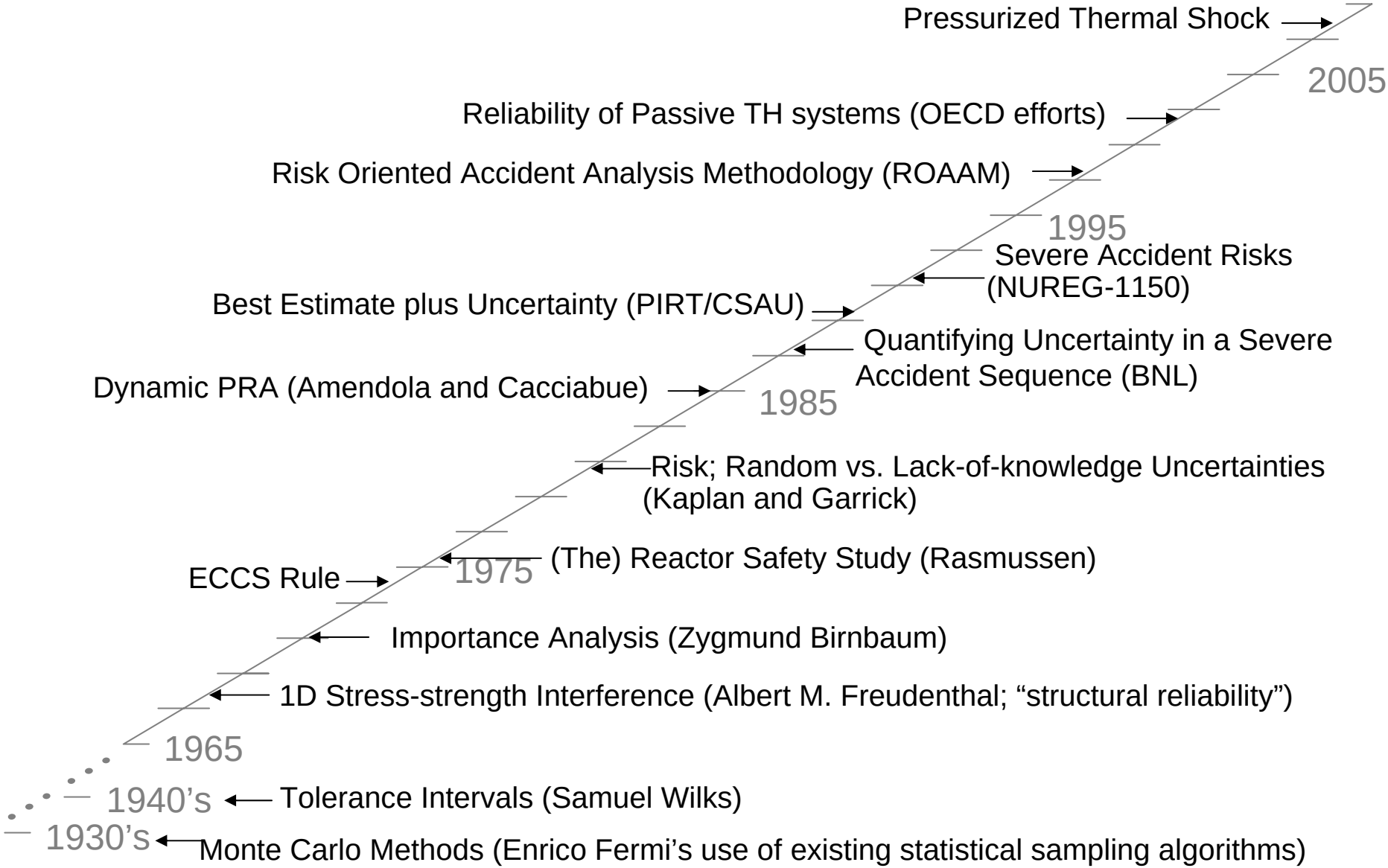
- what are the criteria and tools that can simplify the methodology to the point at which it becomes practically applicable
  - doing as much as necessary but no more given a particular safety question

back-up slides

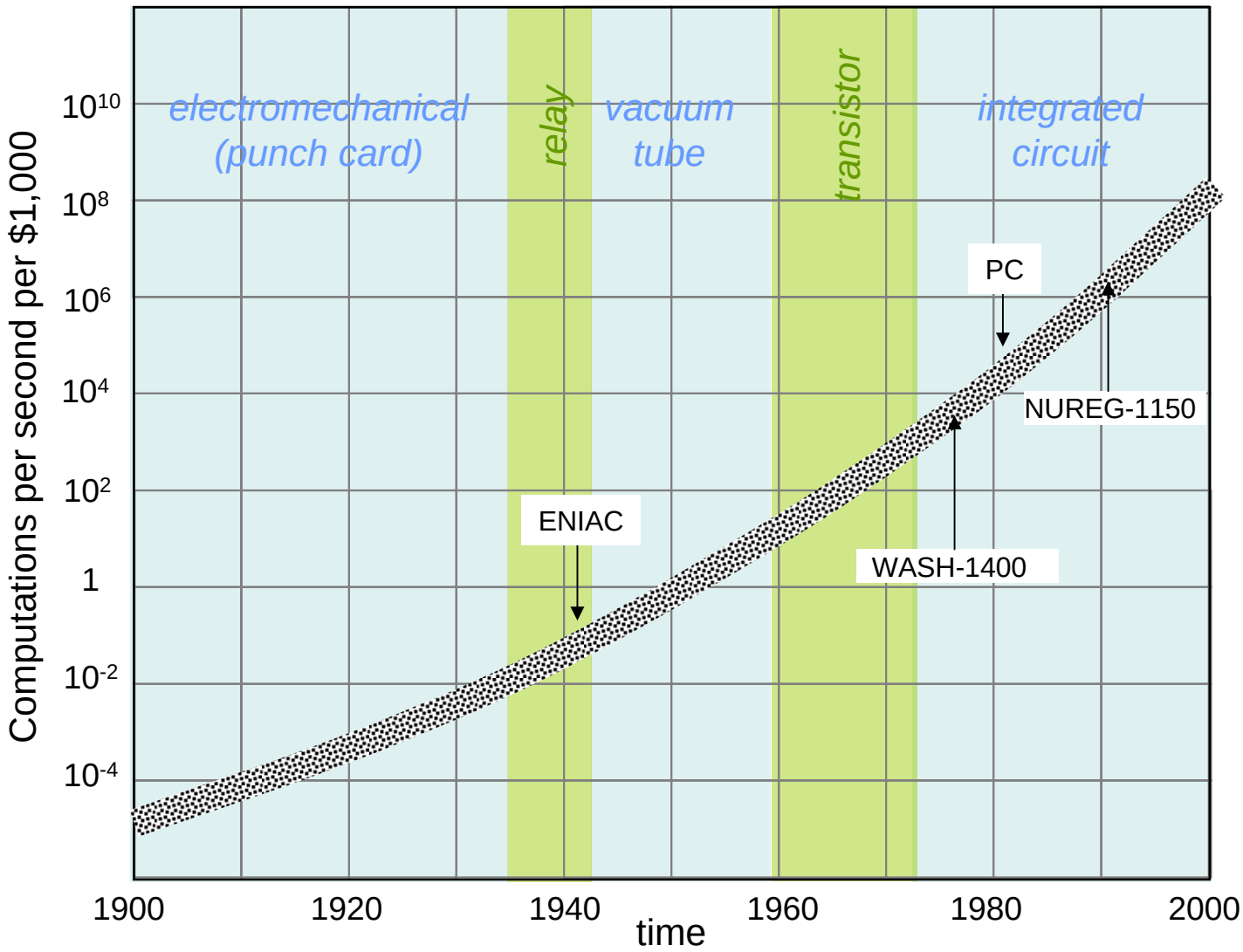
PTS: Accruing Knowledge
(graph courtesy of Mark Kirk, RES/DFERR)



historical milestones



increase in computational power over the last century
(adapted from Wikipedia)



procedure

steps (perform all before and after the modification):

- “draw” the event trees
- decide on uncertainties in the deterministic calculations for the particular safety margin
- complete best estimate plus uncertainty calculation
- multiply frequency with EP for each event
- add over all event sequences to get cumulative core damage frequency