The Concept of Risk and Reactor Safety

Dr. George Apostolakis
Head, Nuclear Risk Research Center
apostola@mit.edu

NRRC Symposium, Tokyo
February 8, 2018

Overview

- The concepts of risk and residual risk
- Traditional ("deterministic") approach to safety
    - Defense in Depth
- Probabilistic Risk Assessment (PRA)
    - Frequency of core damage
    - Frequency of radioactive releases
- Risk Management

Risks in Society

- **Hazard: A source of danger**
  - Ø **Industrial facilities**
  - Ø **Activities, e.g., driving a car**
- **Risk: The possibility that something bad or unpleasant (such as an injury or a loss) will happen**
- ***Uncertainty* is an integral part of risk**
- **Risk: Probability and adverse consequences**

Safety vs. Residual Risk

- **Safety is a continuum**
  - Ø It is meaningless to call something safe or unsafe without further explanation
  - Ø Claim: A plant is "safe" if it meets the regulations
  - Ø A very obscure statement
- **The proper way is to speak of the *residual risk*.**
  - Ø Example: In Japan, 5 people die in transportation accidents for every 100,000 residents every year
  - Ø Therefore, the residual risk (frequency per year) is

    $\frac{5}{100{,}000} = 0.00005$ a very small frequency
- **This residual risk is "accepted" or "tolerated" by Japanese society**

Why do we tolerate Residual Risks?

- **Because each facility or activity provides benefits**
- **For individual voluntary activities in which a person feels in control the residual risk may be relatively high (the risk in general aviation is about 1,000 times greater than that in commercial aviation)**
- **For industrial facilities, it is society through its representatives, government and regulatory agencies, that decides**
- **Risk-Benefit tradeoffs are rarely quantitative; benefit is much harder to quantify than risk**

Nuclear Power Plants

- Undesirable potential consequences
  - Ø Health effects
  - Ø Evacuation
  - Ø Land contamination
- Commonly used potential consequences
  - Ø Damage to the reactor core
  - Ø Release of various amounts of radioactivity
- Accidents are very rare
  - Ø The uncertainties are large
- Management of uncertainties has always been a concern of the industry and regulators

Managing Uncertainty in Nuclear Safety (1)

- **Traditional "conservative" approach**
  - **A bottom-up approach**
  - **A limited number of potential accidents is considered**
  - **Uncertainty is not quantified**
  - **Unquantified uncertainty is managed by conservatism via defense in depth and safety margins**

- ***Defense-in-Depth* is a safety philosophy that employs successive compensatory measures to prevent accidents or mitigate damage if a malfunction, accident, or naturally caused event occurs at a nuclear facility.**

- ***Safety Margin*: The imposed stress on a component or structure is maintained well below the onset of damage.**

Defense in Depth

- A philosophy for managing risk
- It ensures that safety will not be wholly dependent on any single element of the design, construction, maintenance, or operation of a nuclear facility.
- The net effect of incorporating defense-in-depth into design, construction, maintenance, and operation is that the facility or system in question is more tolerant of failures and external challenges.

Major Elements of Defense in Depth

Accident Prevention

↓

Safety Systems

↓

Containment

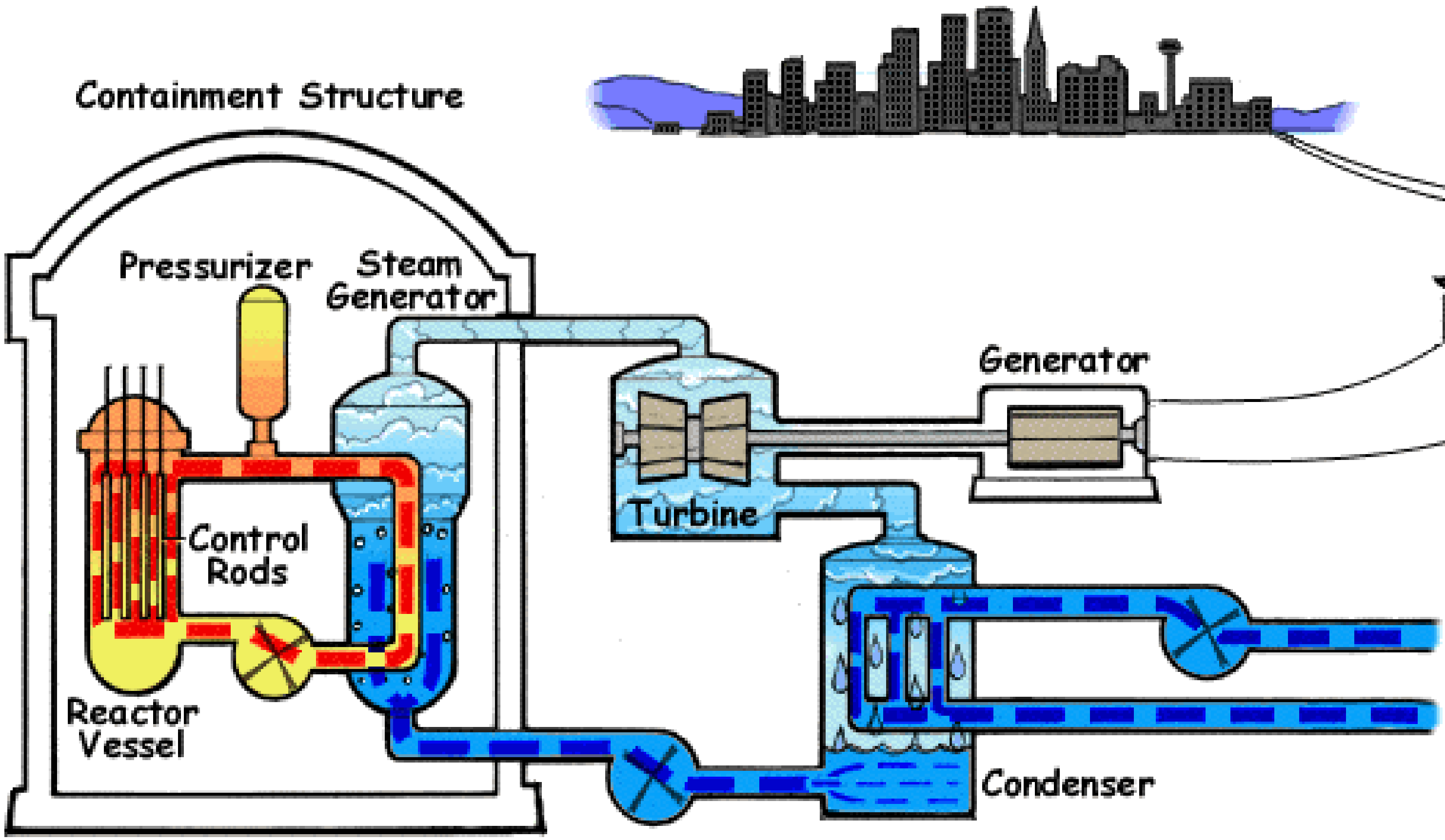
↓

Accident Management

↓

Emergency Plans

Pressurized Water Reactor



U.S. NRC website

Managing Uncertainty in Nuclear Safety (2)

- **Probabilistic Risk Assessment (PRA)**
  - Ø **A top-down approach**
  - Ø **Thousands of potential accident sequences are investigated**
  - Ø **Uncertainty is quantified and managed**
  - Ø **More realistic depiction of what can go wrong**

- **Probabilistic Risk Assessment (PRA) supports Risk Management by answering the questions:**
  - Ø **What can go wrong? (thousands of accident sequences or scenarios)**
  - Ø **How likely are these scenarios?**
  - Ø **What are their consequences?**

PRA Model Overview

CDF
10^{-4}/ry

LERF
10^{-5}/ry

Level I

PLANT MODEL

Level II

CONTAINMENT MODEL

Results

Accident sequences leading to core damage

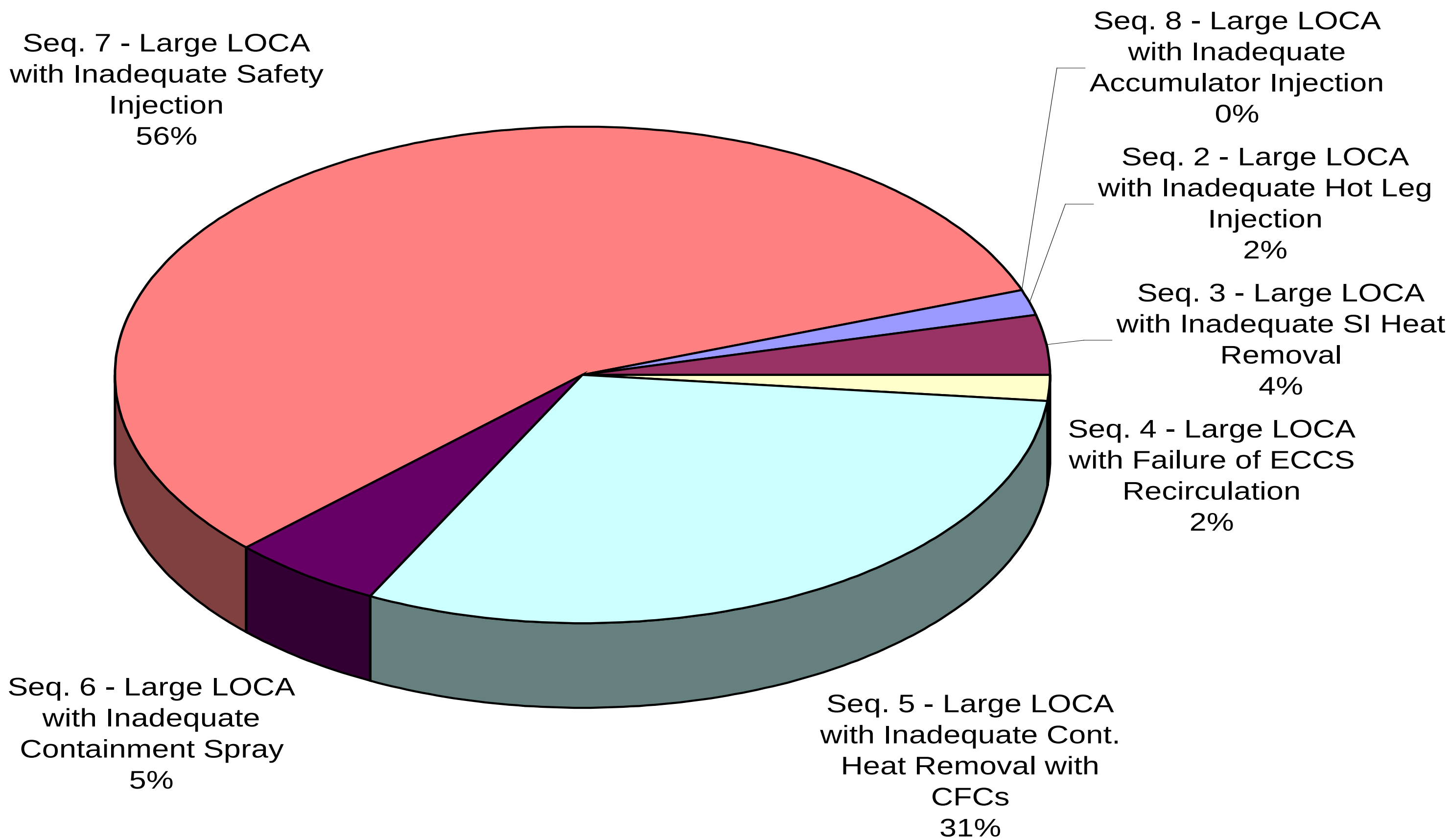
Results

Containment failure

Release of radioactive material

Recently proposed goal: **The frequency of accidents leading to long-term evacuation should be less than once in a million years.**

Contributions to Core Damage Frequency (CDF) for a Current U.S. Plant



CDF = 1.46×10^{-5}/yr (once every 68 thousand years)

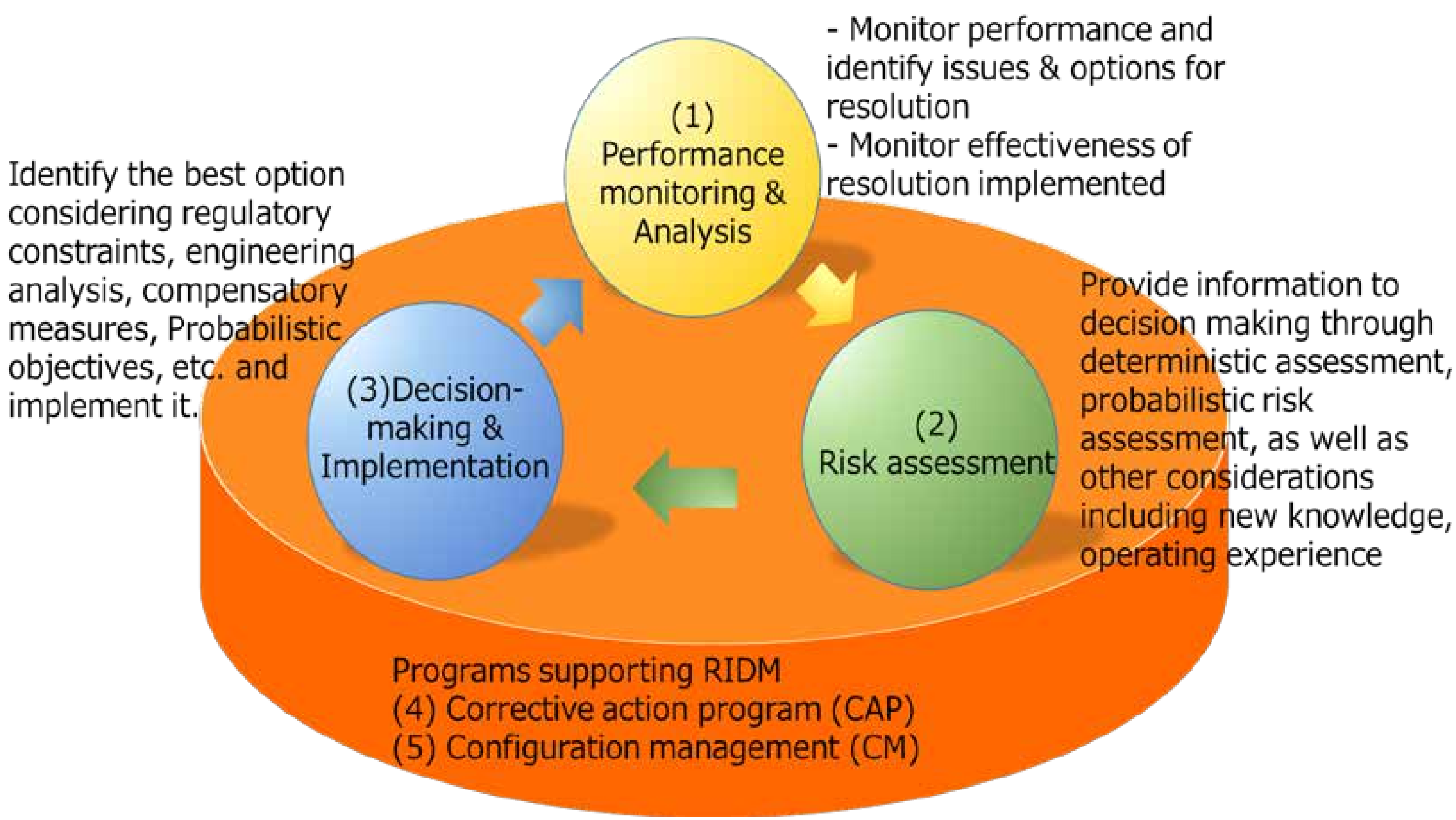
D. True, Presentation at MIT, 2010

Can we benefit from both the Traditional and the Probabilistic Approaches?

"A risk-informed approach to regulatory decision-making represents a philosophy whereby risk insights are considered together with other factors to establish requirements that better focus licensee and regulatory attention on design and operational issues commensurate with their importance to public health and safety."

[Commission's White Paper, U.S. NRC, 1999]

Comprehensive Risk Management



Strategic Plan of the Japanese Nuclear Industry

Concluding Remarks

- The question of what is acceptable or tolerable risk cannot be avoided.
- The residual risk metrics are a more rational way to communicate the degree of plant safety to the technical community and the public.
- Decision making regarding reactor safety issues must be based on the totality of available information, i.e., from both traditional and probabilistic analyses.