Risk-Informed Decision Making at Nuclear Power Plants

George Apostolakis

Head, Nuclear Risk Research Center

apostola@mit.edu

Presented at

Tohoku University

November 3, 2018

Outline

- Hazards, risks and benefits
- Uncertainties in nuclear safety
  - Traditional regulations
  - Risk-informed regulations
- U.S. NRC Safety Goals (1986)
- U.S. NRC Policy Statement on PRA (1995)
- Examples of RIDM applications
  - Extension of AOT
  - ROP
  - Piping inspections
- Challenges for Japan
- NRRC activities
- Concluding remarks

Risks in Society

- **Hazard: A source of danger**
  - **Industrial facilities**
  - **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 (not times) adverse consequences**

Safety vs. Residual Risk

- **Residual risk**
  - **Example: In Japan, 5 people die in transportation accidents for every 100,000 residents every year**
  - **Therefore, the individual residual risk of death is**

$$\frac{5}{100{,}000} = 0.00005 \text{ per year, a very small frequency}$$

- **This residual risk is "accepted" or "tolerated" by Japanese society**

- **Safety is a continuum**
  - **It is meaningless to call something safe or unsafe**
  - **Claim: A plant is "safe" if it meets the regulations**
  - **We should not "continuously improve safety." We should continuously manage the residual risk.**

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 that decides; public input is important
- Risk-Benefit tradeoffs are rarely quantitative; benefit is much harder to quantify than risk

Managing Uncertainty in Nuclear Safety (1)

- **Traditional "conservative" approach**
  - ➢ **A bottom-up approach**
  - ➢ **A limited number of potential design-basis 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.**

- **It is a protection against the unknown unknowns.**

Major Elements of Defense in Depth

Accident Prevention

↓

Safety Systems

↓

Containment

↓

Accident Management

↓

Emergency Plans

Incompleteness of Traditional Regulations

- Small (not large) LOCAs and transients dominate risk (NRC's Reactor Safety Study).
- The significance of support systems and human performance had not been appreciated (NRC's Reactor Safety Study).
- Station Blackout could be a significant risk contributor (before the rule).
- Earthquakes and fires usually dominate risk (industry-sponsored Zion and Indian Point PRAs).
- PRAs should be plant specific.
- Plants licensed under the same rules have different core damage frequencies.

External Influence for Change

- **Regulatory agencies are, by their nature, conservative.**
- **Major changes usually require an external intervention.**
  - **Senator Pastore's letter to the U.S. Atomic Energy Commission (1971)**
    - ***"The members suggested that a comprehensive assessment of the safety aspects of nuclear reactors be made with the intent of setting down for the industry and public a clear-cut summary of what the facts are in this matter."***
    - ***Outcome: The Reactor Safety Study (1974)***

3

Managing Uncertainty in Nuclear Safety (2)

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

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

Additional Problems with the Traditional Approach

- There is no guidance as to how much defense in depth is sufficient
- Qualitative approaches are used to ensure system reliability (the single-failure criterion) when more modern quantitative approaches exist
- Human performance is stylized (e.g., operators are assumed to take no action within, for example, 30 minutes of an accident’s initiation)
- Difficult to reflect operating experience and modern understanding
- Industry-sponsored PRAs showed a variability in risk of plants that were licensed under the same regulations.

PRA Model Overview

Level I	Level II	Level III
PLANT MODEL	**CONTAINMENT MODEL**	**SITE/CONSEQUENCE MODEL**
Results: Accident sequences leading to plant damage states	Results: Containment failure/release sequences	Results: Public health effects

PLANT MODE
At-power Operation
Shutdown / Transition
Evolutions

SCOPE
Internal Events
External Events

Uncertainties

Contributions to Core Damage Frequency for a U.S. BWR (NUREG-1150, 1990)

- **Total** — 9.7×10^{-5} per year
- **Internal Events** — 4.5×10^{-6} per year
  - Station Blackout — 2.2×10^{-6} per year
  - ATWS — 1.9×10^{-6} per year
- **External Events**
  - Seismic (LLNL*) — 7.7×10^{-5} per year
  - Fires — 2.0×10^{-5} per year
- Note: Deemed to be conservative today.

Quantitative Health Objectives (QHOs) (USNRC, August, 1986)

- **Early and latent cancer mortality risks to an individual living near the plant should not exceed 0.1 percent of the background accident or cancer mortality risk, approximately**

5×10^{-7}/year for early death and

2×10^{-6}/year for death from cancer.

- ❖ **The prompt fatality goal applies to an average individual living in the region between the site boundary and 1 mile beyond this boundary.**
- ❖ **The latent cancer fatality goal applies to an average individual living in the region between the site boundary and 10 miles beyond this boundary.**

PRA Model Overview and Subsidiary Objectives

CDF
10^{-4}/ry

LERF
10^{-5}/ry

QHOs

Level I

PLANT MODEL

Results

Accident sequences leading to plant damage states

Level II

CONTAINMENT MODEL

Results

Containment failure/release sequences

PLANT MODE
At-power Operation
Shutdown / Transition Evolutions

Level III

SITE/CONSEQUENCE MODEL

Results

Public health effects

SCOPE
Internal Events
External Events

Uncertainties

PRA Policy Statement (USNRC1995)

- The use of PRA should be increased to the extent supported by the state of the art and data and in a manner that complements the defense-in-depth philosophy

- PRA should be used to reduce unnecessary conservatisms associated with current regulatory requirements

Risk-informed Regulation

"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."

[USNRC Commission's White Paper, USNRC, 1999]

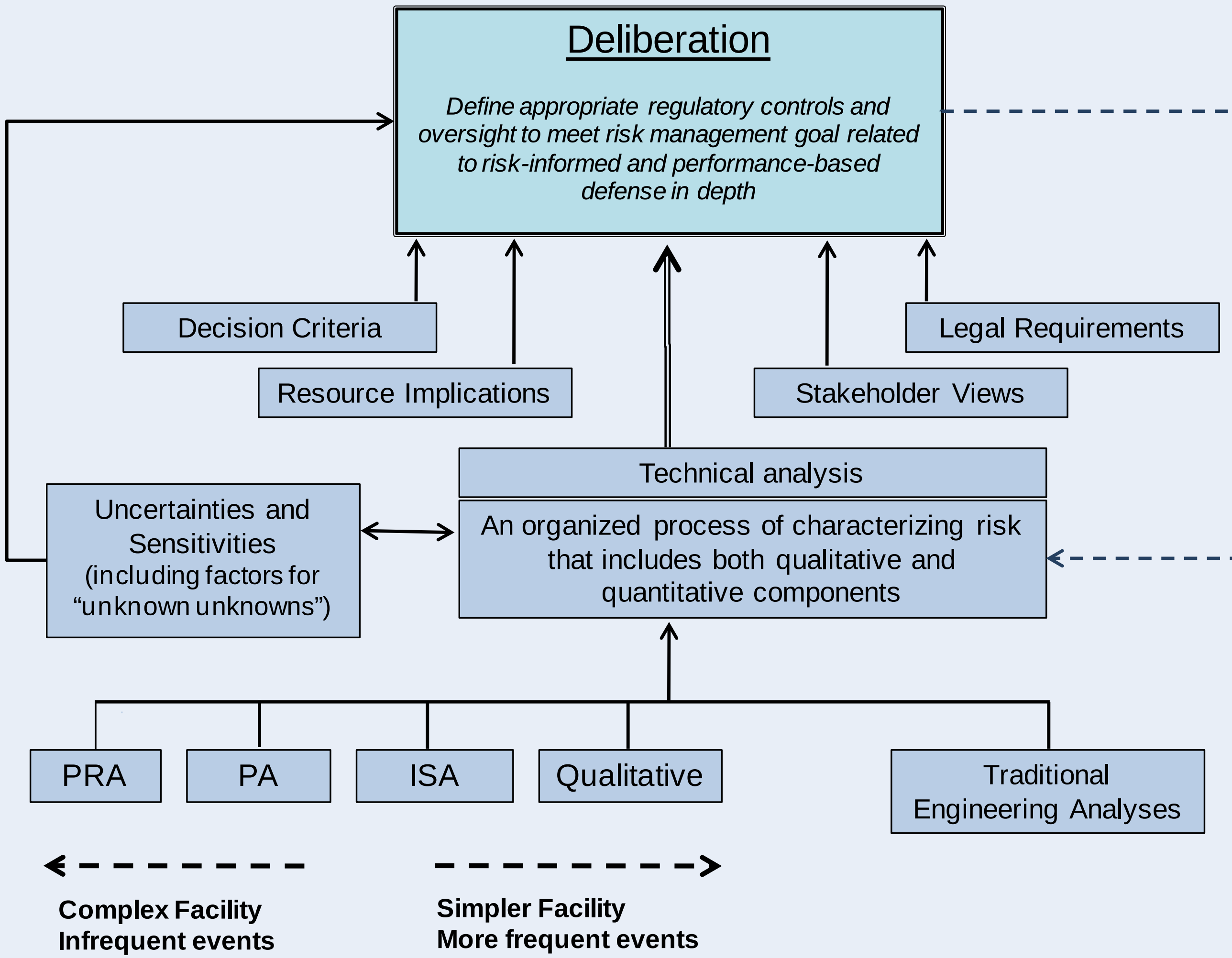


Figure B-4 Technical Analysis Techniques & Deliberation

NUREG-2150, *A Proposed Risk Management Regulatory Framework*

Risk-Informed Framework

Traditional "Deterministic" Approach

- Unquantified probabilities
- Design-basis accidents
- Defense in depth and safety margins
- Can impose unnecessary regulatory burden
- Incomplete

Risk-Informed Approach

- Combination of traditional and risk-based approaches through a deliberative process

Risk-Based Approach

- Quantified probabilities
- Thousands of accident sequences
- Realistic
- Incomplete

Risk-Informed Changes to the Licensing Basis (RG 1.174; 1998)

Comply with Regulations

Maintain Defense-in-Depth Philosophy

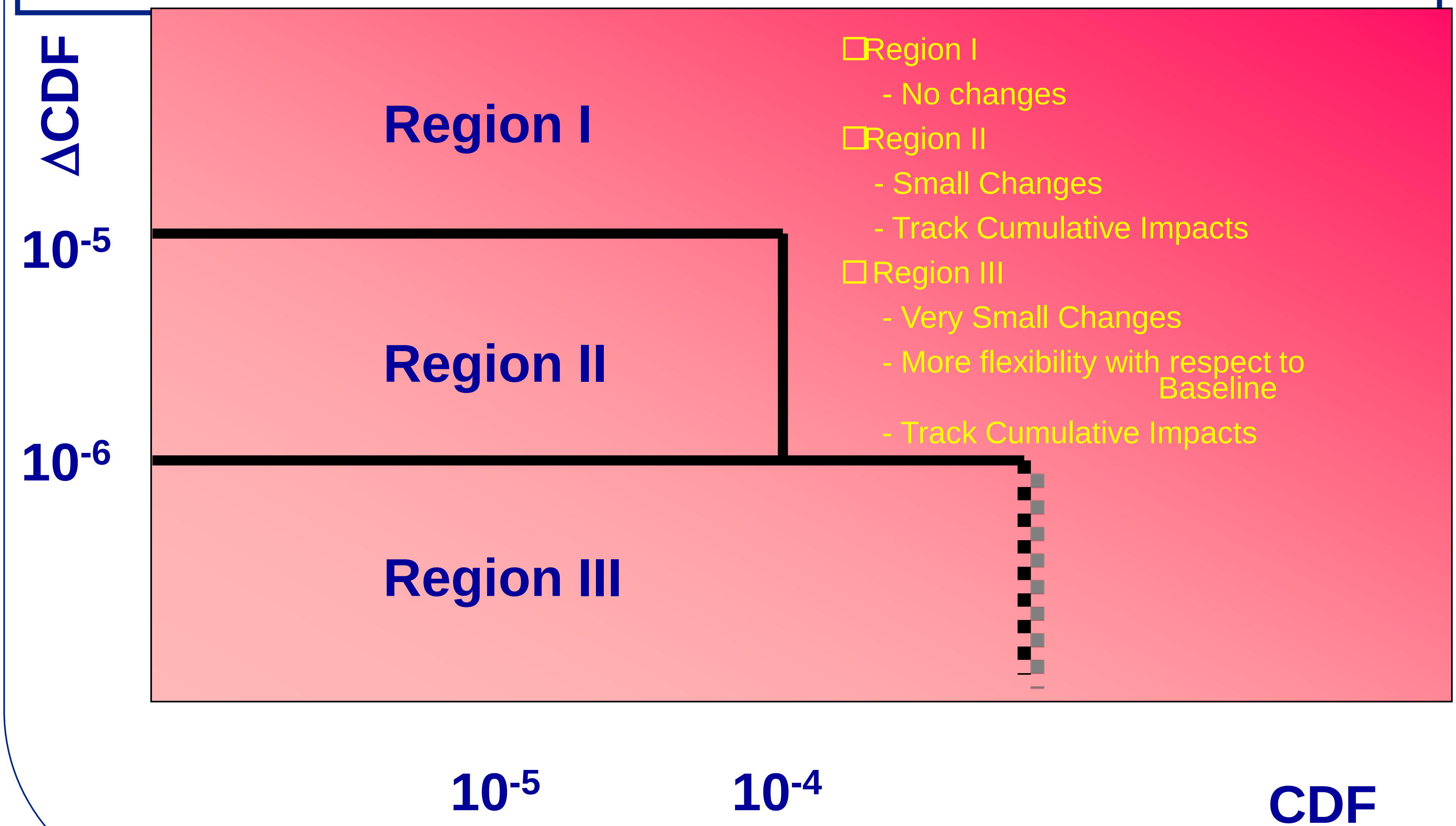
Maintain Safety Margins

Integrated Decision Making

Risk Decrease, Neutral, or Small Increase

Monitor Performance

Risk-Informed Changes to the Licensing Basis (RG 1.174)



Acceptance Guidelines for Core Damage Frequency

Important Note

"The analysis will be subject to increased technical review and management attention as indicated by the darkness of the shading of the figure. In the context of the integrated decision-making, the boundaries between regions should not be interpreted as being definitive; the numerical values associated with defining the regions in the figure are to be interpreted as indicative values only."

Regulatory Guide 1.174

Example: 1-out-of-2 System

$$Q = \frac{1}{3}\lambda^2 T^2 + \lambda\tau + \frac{1}{2}\lambda_{CCF} T + \gamma_0 \gamma_1$$

λ	standby failure rate
T	Surveillance Test Interval
τ	Allowed Outage Time
λ_{CCF}	common-cause failure rate
γ_0	unconditional human error rate
γ_1	conditional human error rate

ΔCDF and Δ LERF can be calculated from the PRA.

South Texas Project Experience

- AOTs extended from 3 days to 14 days for emergency AC power and 7 days for Essential Cooling Water and Essential Chilled Water systems.
- Actual experience: Less than 5 days.
- Confidence building.

A Success: Reactor Oversight Process

- **Motivation**
  - **The previous inspection, assessment and enforcement processes**
    a. **Were not clearly focused on the most safety important issues**
    b. **Consisted of redundant actions and outputs**
    c. **Were overly subjective with NRC action taken in a manner that was at times neither scrutable nor predictable.**
  - **Commission's motivation**
    a. **Improve the objectivity of the oversight processes so that subjective decisions and judgment were not central process features**
    b. **Improve the scrutability of these processes so that NRC actions have a clear tie to licensee performance**
    c. **Risk-inform the processes so that NRC and licensee resources are focused on those aspects of performance having the greatest impact on safe plant operation.**

ROP: Challenges and Context

- **Challenges**
  - The large size of the program, in terms of both the number of USNRC staff (e.g., hundreds of affected staff) and the number of licensed facilities affected (i.e., all licensed power reactors).
  - The development of performance indicators using plant data (e.g., results of equipment tests translated into quantitative estimates of system reliability) required the development of methods to collect the data, techniques for consistently and clearly displaying the results, and determining action “thresholds” (e.g., what action should be taken in response to decreasing performance).
  - The quality of the licensee PRAs varied considerably across the set of plants
  - This variability presented a significant challenge to USNRC as it attempted to develop realistic and objective assessment tools that were not sensitive to this variability.

ROP: Outcomes

- Very successful
- Improves the consistency and objectivity of the previous process by using more objective measures of plant performance
- Focuses NRC and licensee resources on those aspects of performance that have the greatest impact on safe plant operation
- Provides explicit guidance on the regulatory response to inspection findings
- Full implementation required considerable resources, including data collection and evaluation, training, and agency risk expertise and models
- The benefits of the program, including the objectivity and public availability of plant evaluations, justified the costs incurred.

ROP: Take-Away

- **Implementation of a risk-informed reactor oversight process requires considerable development, testing, and communication among stakeholders early in the process, and an extensive infrastructure during use. The objectivity and clarity of outcomes more than justifies the investment.**

- **Implementation of RIDM requires "Good" plant-specific PRAs.**

- **The NRRC is aiding Japanese utilities in developing "Good" PRAs.**

ASME Boiler and Pressure Vessel Code (BPVC) Section XI

- Class 1 components include piping and components whose failure would prevent orderly reactor shutdown and cause a loss of coolant in excess of normal makeup capability.
- Class 2 components include safety system components of the following: residual heat removal system, reactor containment heat removal systems, emergency core cooling system including injection and recirculation portions, air cleanup systems used to reduce radioactivity within the reactor containment, containment hydrogen control system and portions of the steam and feedwater systems.
- Class 3 components include portions of the reactor auxiliary systems that provide boric acid, emergency feedwater system, portions of components and process cooling systems (electrical and/or compressed air) that cool other safety systems including the spent pool cooling system, on-site emergency power supply and auxiliary systems.

ASME BPVC Section XI Requirements

- Class 1 piping systems: 25% welds examined every 10-year interval
- Class 2 piping systems: 7.5% welds examined every 10-year interval
- Class 3 piping systems: Only pressure test for leakage every 10-year interval

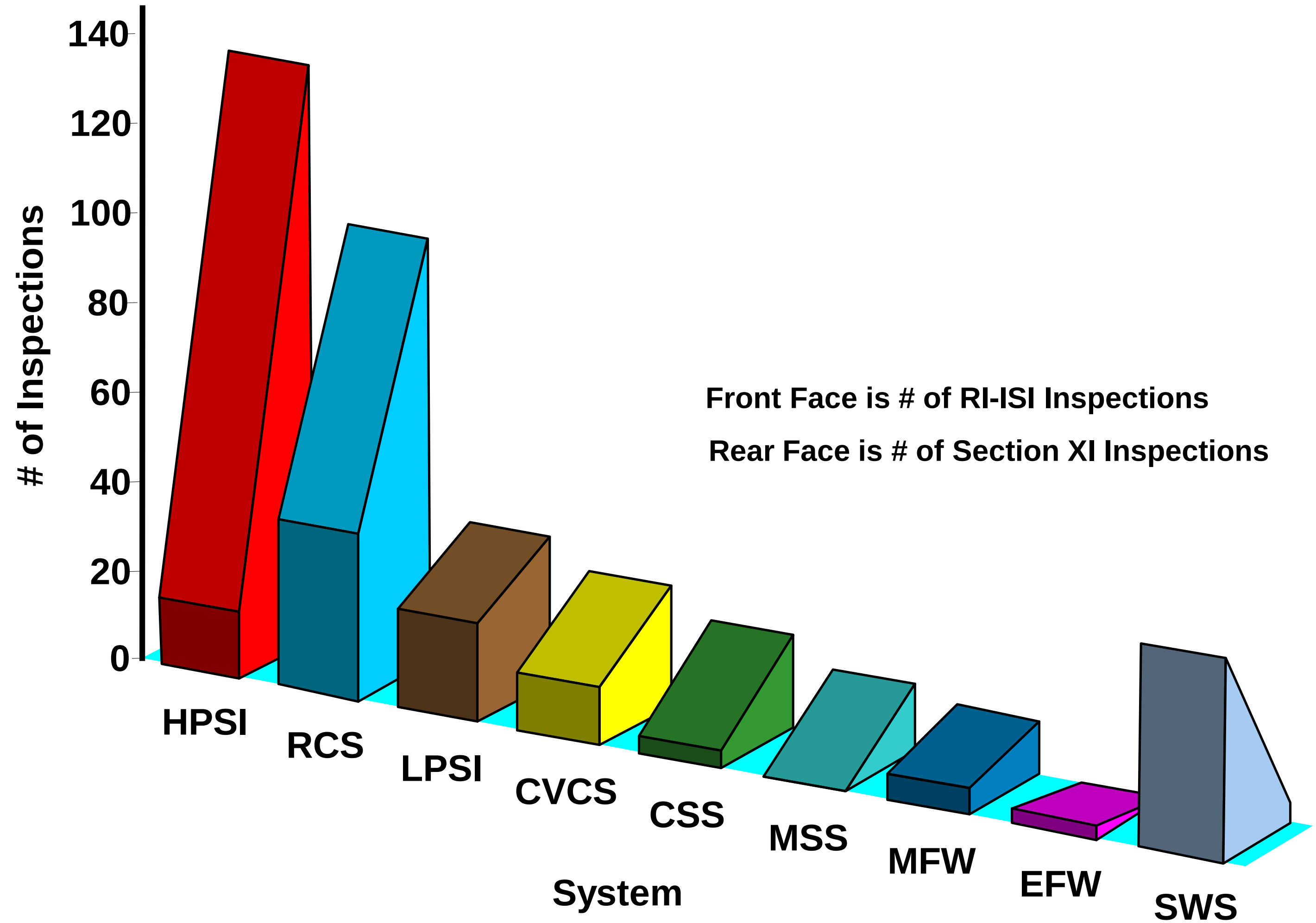
- The selection of inspections is primarily based on "high (design) stress/high (design) fatigue" weld locations.

Risk Evaluation Matrix

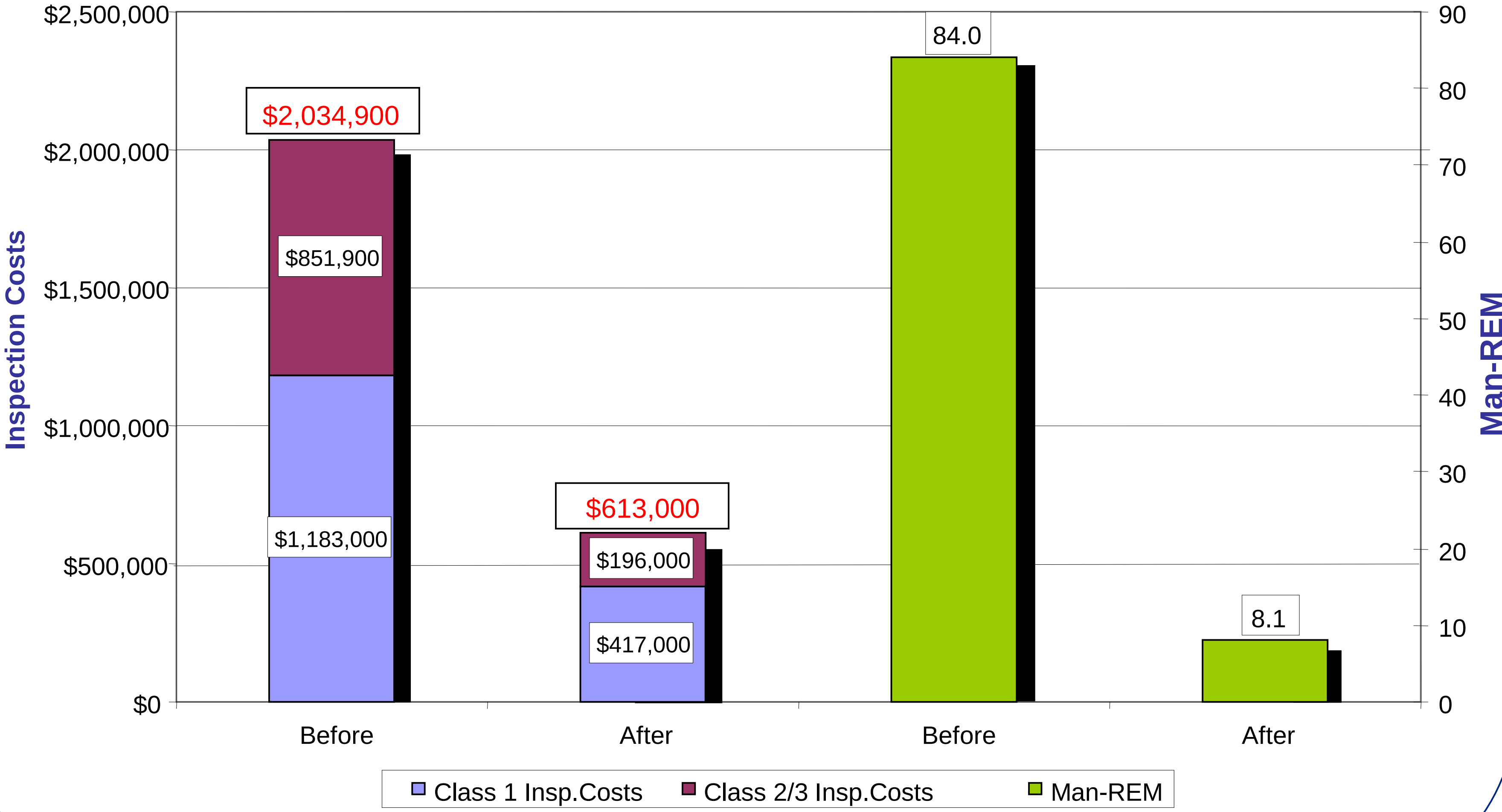
(Conditional) CONSEQUENCE CATEGORY
(Safety Significance)

DEGRADATION CATEGORY (Pipe Rupture Potential)	NONE	LOW	MEDIUM	HIGH
HIGH	LOW (Cat. 7)	MEDIUM (Cat. 5)	HIGH (Cat. 3)	HIGH (Cat. 1)
MEDIUM	LOW (Cat. 7)	LOW (Cat. 6)	MEDIUM (Cat. 5)	HIGH (Cat. 2)
LOW	LOW (Cat. 7)	LOW (Cat. 7)	LOW (Cat. 6)	MEDIUM (Cat. 4)

Benefits of RI ISI: Number of Inspections Before and After for Plant X



Benefits of RI ISI: Cost and Man-Rem Savings



CRIEPI Central Research Institute of Electric Power Industry

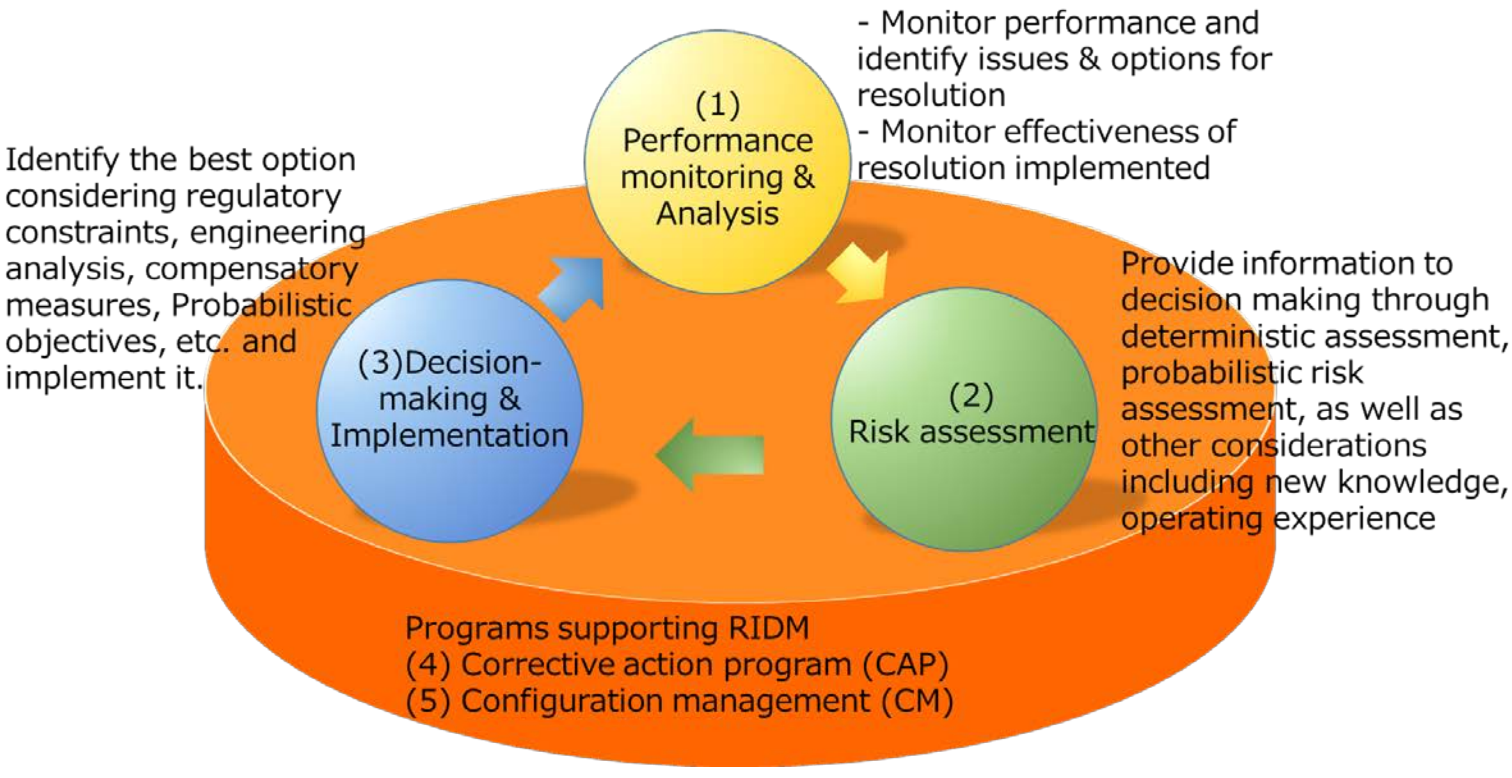
Challenges in Japan

- An increased understanding of the value and use of risk concepts and risk management language
- Development of a cadre of risk analysts, both in the industry and the regulator
- Need to focus on effective means of risk communication to the public
- Need to develop quantitative safety goals
- A long-term commitment from both the regulator and industry would be required for implementation

NRRC Mission Statement

To assist nuclear operators and nuclear industry to continually improve the safety of nuclear facilities by developing and employing modern methods of Probabilistic Risk Assessment(PRA), risk-informed decision making and risk communication.

Risk-Informed Decision-Making



From: Strategic and Action Plans for the Implementation of Risk Information Utilization at Nuclear Power Plants, February 8, 2018.

PRA Quality

- A plant-specific PRA is the essential element for RIDM and the ROP.
- Such a PRA is a complex combination of logic models, experimental and statistical evidence, and judgment.
- The uncertainties for some initiators may be very large (however, they are not quantified in the "deterministic" system).
- An exhaustive review was performed for the industry-sponsored Zion/Indian Point PRAs by Sandia National Laboratories on behalf of the NRC.
- This review was unique and very resource intensive.
- A practical solution was needed.

Assuring PRA Quality in the U.S.

- U.S. scientific societies (ASME and ANS) issued standards.
- The NRC issued reports and regulatory guides endorsing the standards (with exceptions, as appropriate).
- NEI issued guidance on peer reviews.
- NRC and ACRS staff observed several peer reviews.
- NRC approved the NEI peer review process.
- Compliance with these documents has eased the NRC's burden regarding PRA reviews.
- The NRC receives a PRA summary but staff may review as much of the industry's PRA as they wish.

Japanese Industry's Efforts on PRA Quality

- **Improving the infrastructure (NRRC)**
  - Guides on HRA, Fire PRA, Data Collection
  - Models for external events, including the SSHAC process
  - Multi-unit PRA
- **NRRC's Technical Advisory Committee (TAC) high-level review of Ikata 3 PRA**
  - Expanding the list of Initiating Events, e.g., adding loss of instrument air system
  - Improving plant-specific data collection
- **International expert reviews following the ASME/ANS standards and the NEI process**
  - Ikata 3: Torri, Lin, Fleming (U.S.), Boneham (U.K.)
  - KK 7: Chapman, Wachowiak (U.S.), Nusbaumer (Switzerland)
- **NRA staff are welcome to observe these meetings, the resulting actions, and relevant documents**

NRRC Training Courses

1. **PRA and risk information utilization course**
   - For beginners
   - Preparing for implementation in FY2018

2. **Risk professional course (supported by EPRI)**
   - Mainly L1 internal events PRA
   - For utility's PRA practitioners and regulatory staff
   - Started in FY2018

3. **Risk information utilization course**
   - For decision makers (NPP managers)
   - Preparing for a trial offering in FY2018.

Final Remarks

- **RIDM is the rational way to proceed both for the industry and regulators**
- **PRAs should be plant-specific**
- **We need to move from a regulatory-compliance culture to a risk-informed culture**
- **The ROP and the industry's strategic and action plans are significant steps forward**
- **PRA quality is improved by issuing standards, regulatory guidance, and implementing peer reviews**
- **RIDM is an inherently subjective process requiring substantial training**
- **The deliberative process for establishing safety goals should start soon**