PRA: A Historical Perspective

George E. Apostolakis
Massachusetts Institute of Technology

Course 22.38

November 21, 2005

Overview

- Traditional Regulations
- Farmer's Paper (1967)
- Reactor Safety Study (1975)
- Zion and Indian Point PRAs (1981)
- NUREG - 1150 (1989)
- Individual Plant Examinations (GL:1988)
- PRA Policy Statement (1995)
- Risk-Informed, Performance-Based Regulation (1997)
- Reactor Oversight Process
- Current Activities

The Pre-PRA Era

- **Management of (unquantified at the time) uncertainty was always a concern.**
- **Defense-in-depth and safety margins became embedded in the regulations.**
- **"Defense-in-Depth is an element of the NRC's 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." [Commission's White Paper, February, 1999]**
- ***Design Basis Accidents* are postulated accidents that a nuclear facility must be designed and built to withstand without loss to the systems, structures, and components necessary to assure public health and safety.**

Defense-in-Depth Elements

- Prevention of Core Damage
- Containment
- Accident Management
- Emergency Plans

General Design Criteria (February, 1971; 10 CFR 50, Appendix A)

- **Necessary design, fabrication, construction, testing, and performance requirements for structures, systems, and components <u>important to safety</u>, i.e., those that provide <u>reasonable assurance</u> that the facility can be operated <u>without undue risk</u> to the health and safety of the public.**

- **Six major categories:**
  - **Overall requirements**
  - **Protection by multiple fission product barriers**
  - **Protection and reactivity control systems**
  - **Fluid systems**
  - **Reactor containment**
  - **Fuel and reactivity control**

The Single-Failure Criterion

- "Fluid and electric systems are considered to be designed against an assumed single failure if neither (1) a single failure of any active component (assuming passive components function properly) nor (2) a single failure of a passive component (assuming active components function properly), results in a loss of the capability of the system to perform its safety functions."
- The intent is to achieve high reliability (probability of success) without quantifying it.
- Looking for the worst possible single failure leads to better system understanding.

Emergency Core Cooling System (ECCS) (January 1974, 10 CFR 50.46)

- **Postulate several LOCAs of different sizes and locations to provide assurance that the most severe LOCAs are considered.**

- **Postulate concurrent loss of offsite or onsite power and the most damaging single failure of ECCS equipment (GDC 35).**

- **Acceptance Criteria**
  - **Peak cladding temperature cannot exceed 2200 ºF (1204 ºC)**
  - **Oxidation cannot exceed 17% of cladding thickness**
  - **Hydrogen generation from hot cladding-steam interaction cannot exceed 1% of its potential**
  - **Core geometry must be coolable**
  - **Long-term cooling must be provided**

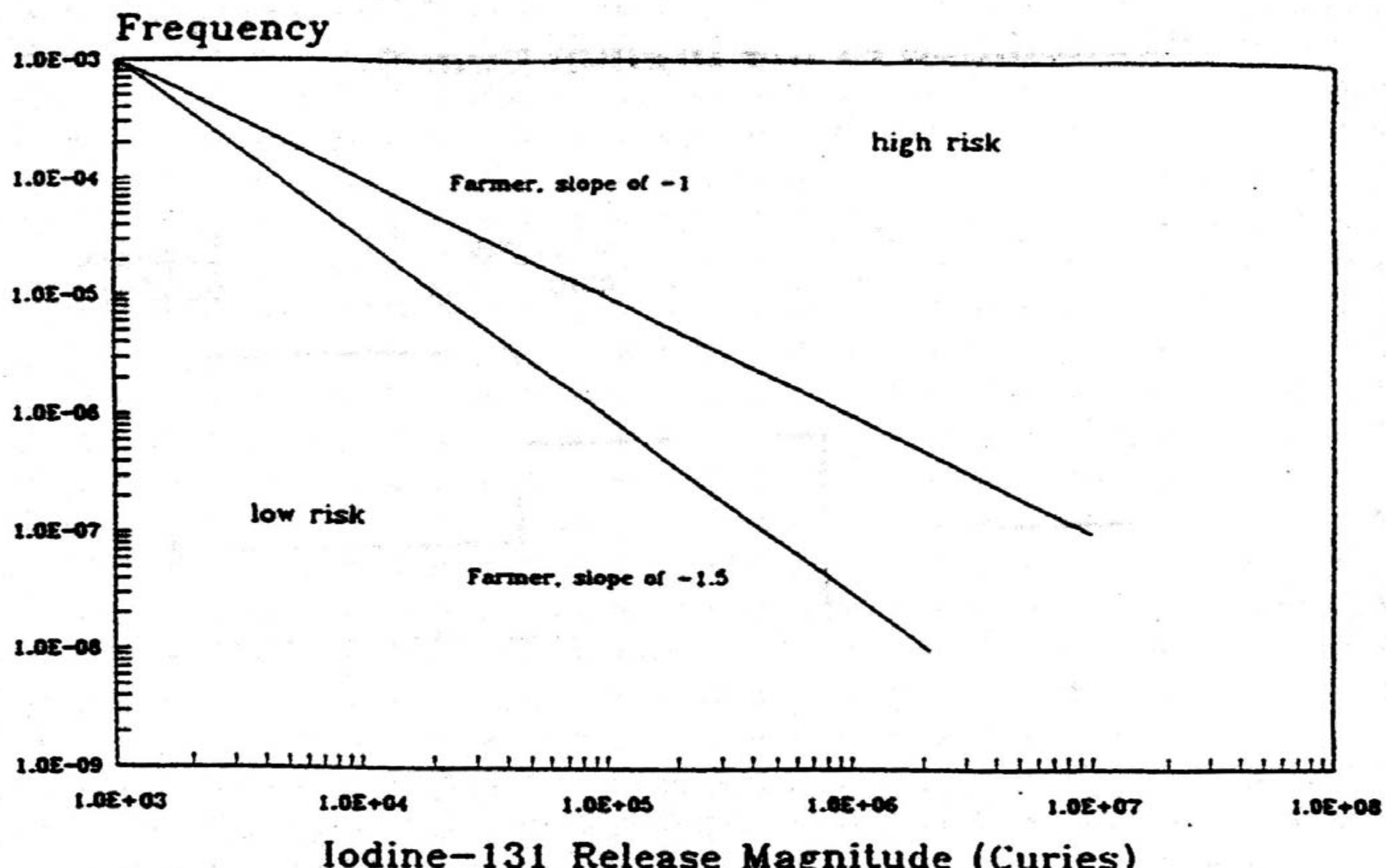
ECCS Evaluation Models

- **Conservative models**
- **"Best estimate" models with uncertainty evaluation (September, 1988)**

Farmer's Paper (1967)

- Iodine-131 is a major threat to health in a nuclear plant accident.
- Attempting to differentiate between credible and incredible accidents is not logical.
- If one considers a fault, such as a loss-of-coolant accident (LOCA), one can determine various outcomes, from safe shutdown and cooldown, to consideration of delays and partial failures of shutdown or shutdown cooling with potential consequences of radioactivity release.

THE FARMER LINE



Courtesy of U.S. NRC.

Reactor Safety Study (WASH-1400; 1975)

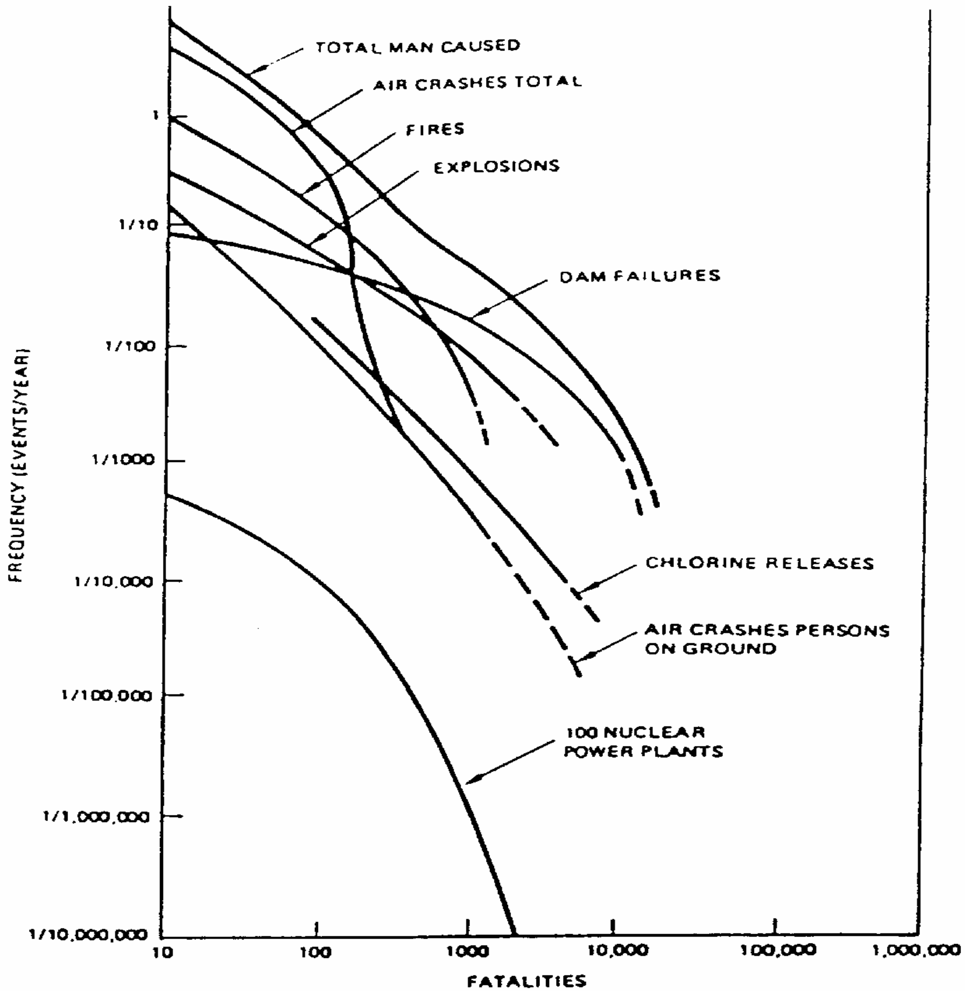
Prior Beliefs:

1. Protect against large LOCA.
2. CDF is low (about once every 100 million years, 10^{-8} per reactor year) .
3. Consequences of accidents would be disastrous.

Major Findings

1. Dominant contributors: Small LOCAs and Transients.
2. CDF higher than earlier believed (best estimate: 5×10^{-5}, once every 20,000 years; upper bound: 3×10^{-4} per reactor year, once every 3,333 years).
3. Consequences significantly smaller.
4. Support systems and operator actions very important.

Risk Curves



Frequency of Fatalities Due to Man-Caused Events (RSS)

Courtesy of U.S. NRC.

Risk Assessment Review Group

- "We are unable to define whether the overall probability of a core melt given in WASH-1400 is high or low, but we are certain that the error bands are understated."
- WASH-1400 is "inscrutable."
- "…the fault -tree/event-tree methodology is sound, and both can and should be more widely used by NRC."
- "PSA methods should be used to deal with generic safety issues, to formulate new regulatory requirements, to assess and revalidate existing regulatory requirements, and to evaluate new designs."

Commission Actions (Jan. 18, 1979)

- **"…the Commission has reexamined its views regarding the Study in light of the Review Group's critique."**
- **"The Commission withdraws any explicit or implicit past endorsement of the Executive Summary."**
- **"…the Commission does not regard as reliable the Reactor Safety Study's numerical estimate of the overall risk of reactor accidents."**

Zion and Indian Point PRAs (1981)

- First PRAs sponsored by the industry.
- Comprehensive analysis of uncertainties (Bayesian methods).
- Detailed containment analysis (not all accidents lead to containment failure).
- "External" events (earthquakes, fires) may be significant contributors to risk.

RISK RESULTS

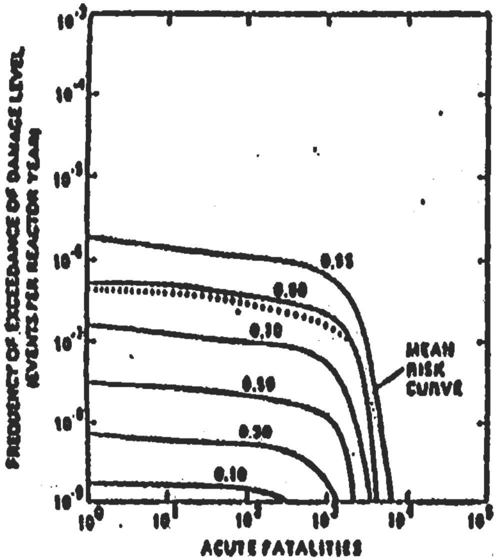


FIGURE 1-1a. RISK OF EARLY FATALITIES

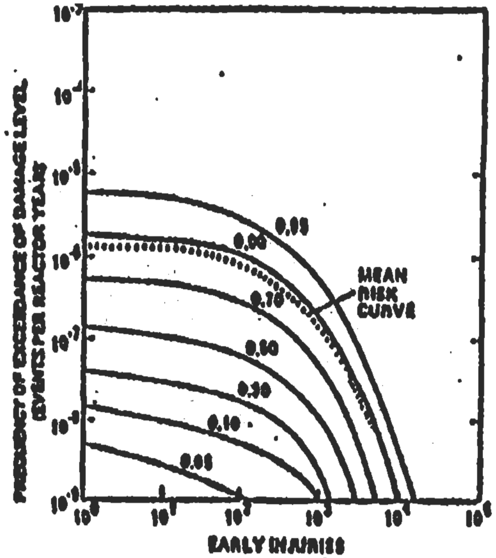


FIGURE 1-1b. RISK OF INJURIES

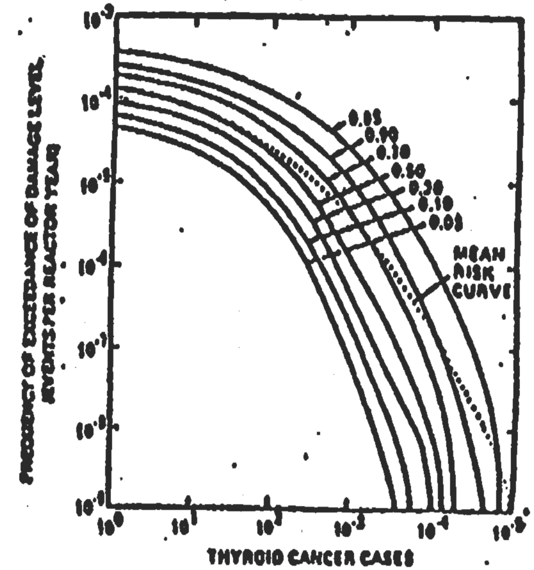


FIGURE 1-1c. RISK OF THYROID CANCER CASES

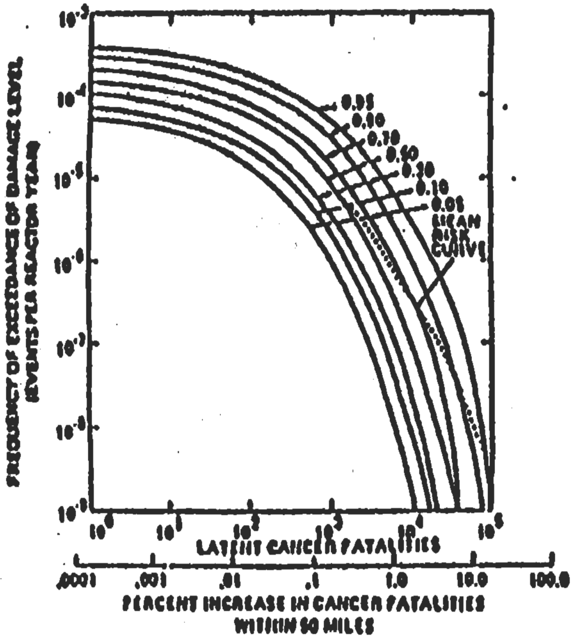


FIGURE 1-1d. RISK OF LATENT CANCER FATALITIES (OTHER THAN FATAL THYROID CANCERS)

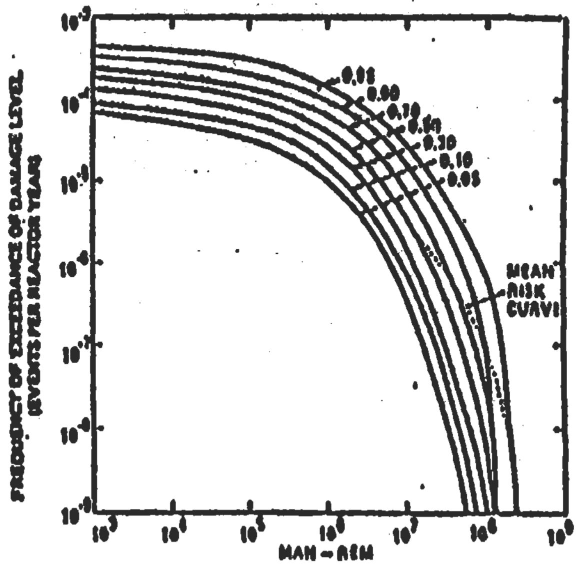


FIGURE 1-1e. RISK OF MAN-REM

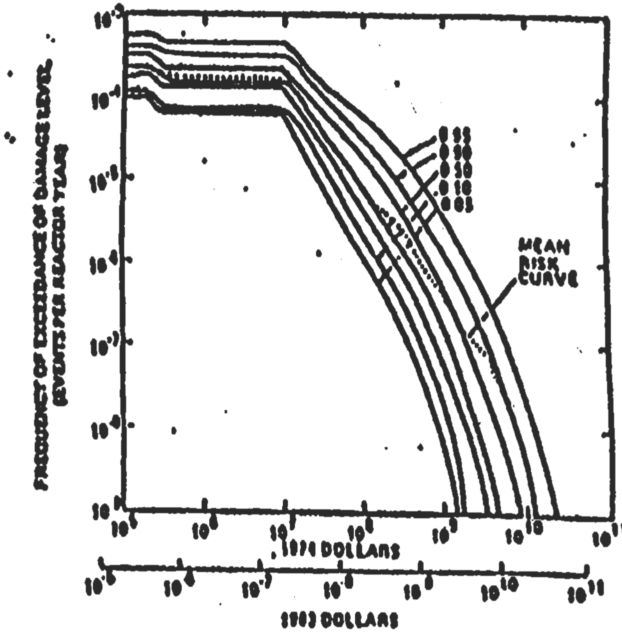


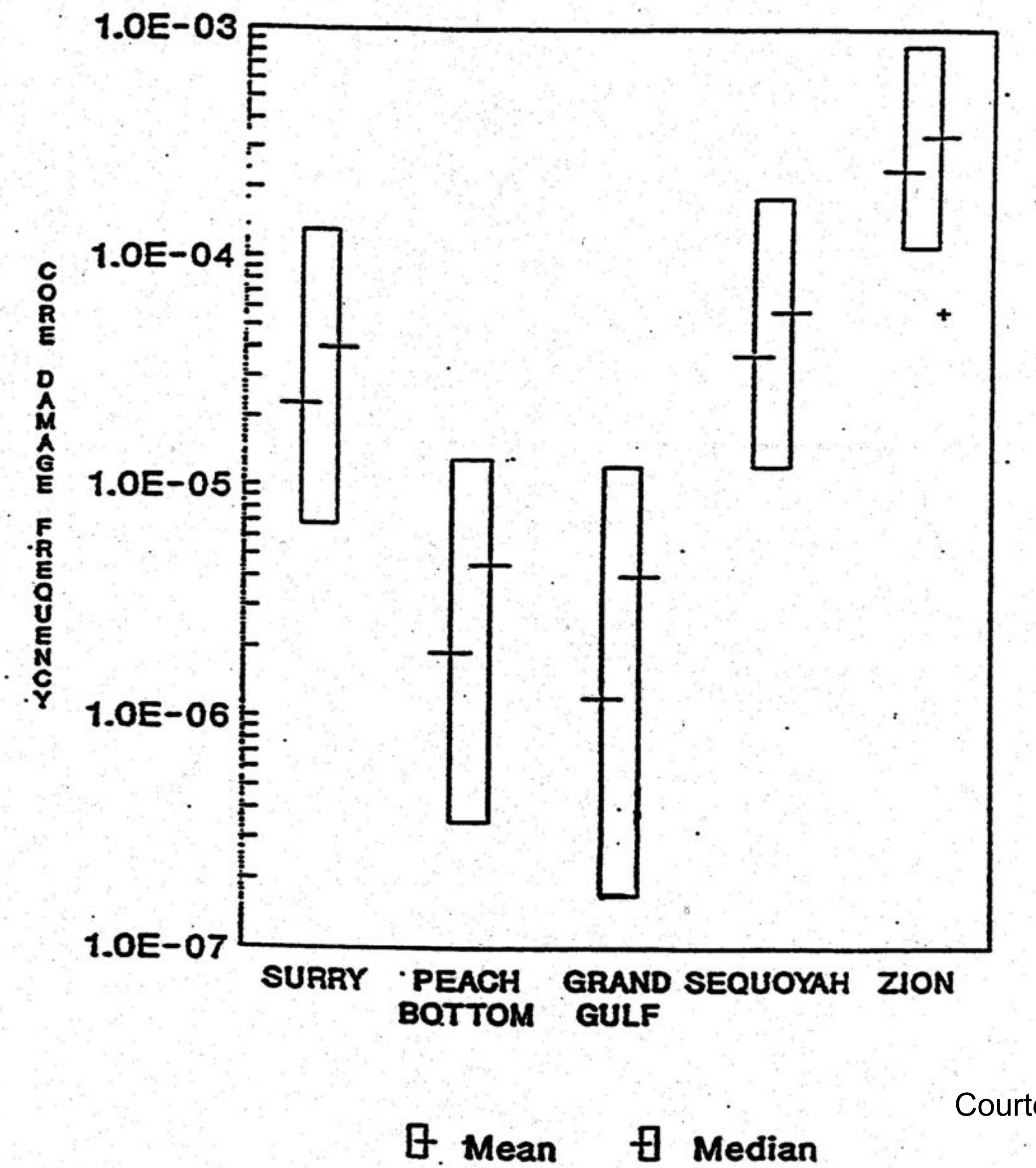
FIGURE 1-1f. RISK OF PROPERTY DAMAGE AND EVACUATION COSTS

SUMMARY OF ACCIDENT SEQUENCES WITH SIGNIFICANT RISK AND CORE MELT FREQUENCY CONTRIBUTIONS

Initiating Event	Additional System Failures/ Human Actions	Resulting Dependent Failures	Sequence Frequency (per reactor year)	Sequence Ranking: Core Melt	Sequence Ranking: Latent Health Risk	Sequence Ranking: Early Health Risk
Loss of Offsite Power	Onsite AC Power, No Recovery of AC Power Before Core Damage	Component cooling, high pressure makeup (ECCS), reactor coolant pump seal LOCA, containment filtration and heat removal.	3.3-5	1	1	*
Loss of Offsite Power	Service Water, No Recovery of Offsite Power	Onsite AC power, component cooling, high and low pressure makeup (ECCS), reactor coolant pump seal LOCA, containment filtration and heat removal.	9.2-6	2	2	*
Small LOCA	Residual Heat Removal	None.	8.9-6	3	*	*
Control Room Fire	None	Component cooling, high and low pressure makeup (ECCS), reactor coolant pump seal LOCA, containment filtration and heat removal.	8.7-6	4	3	*
Loss of Main Feedwater	Solid State Protection System	Reactor trip, emergency feedwater, high and low pressure makeup (ECCS), containment filtration and heat removal.	8.3-6	5	4	*
Steam Line Break Inside Containment Heat Removal	Operator Failure to Establish Long Term		5.6-6	6	*	*
Reactor trip	Component Cooling	High and low pressure makeup (ECCS), reactor coolant pump seal LOCA, containment filtration and heat removal.	4.6-6	7	5	*
Loss of Offsite Power	Train A Onsite Power, Train B Service Water, No Recovery of AC Power Before Core Damage	Train B onsite power, component cooling, high and low pressure makeup (ECCS), reactor coolant pump seal LOCA, containment filtration and heat removal.	4.4-6	8	6	*
Loss of Offsite Power	Train B Onsite Power, Train A Service Water, No Recovery of AC Power Before Core Damage	Train A onsite power, component cooling, high and low pressure makeup (ECCS), reactor coolant pump seal LOCA, containment filtration and heat removal.	4.4-6	9	7	*
PCC Area Fire	None	Component cooling, high and low pressure makeup (ECCS), reactor coolant pump seal LOCA, containment filtration, and heat removal.	4.1-6	10	8	*

*Negligible contribution to risk.

NOTE: Exp tial notation is indicated in abbreviated form; i.e., 3.3-5 = 3.3 0^{-5}.

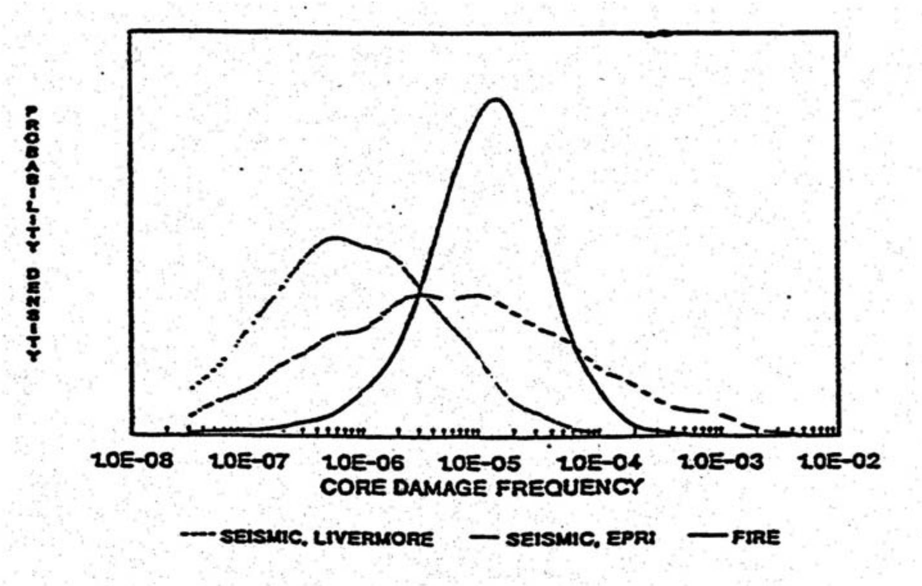


Courtesy of U.S. NRC.

"+" indicates recalculated Zion mean core damage frequency based on recent plant modifications.

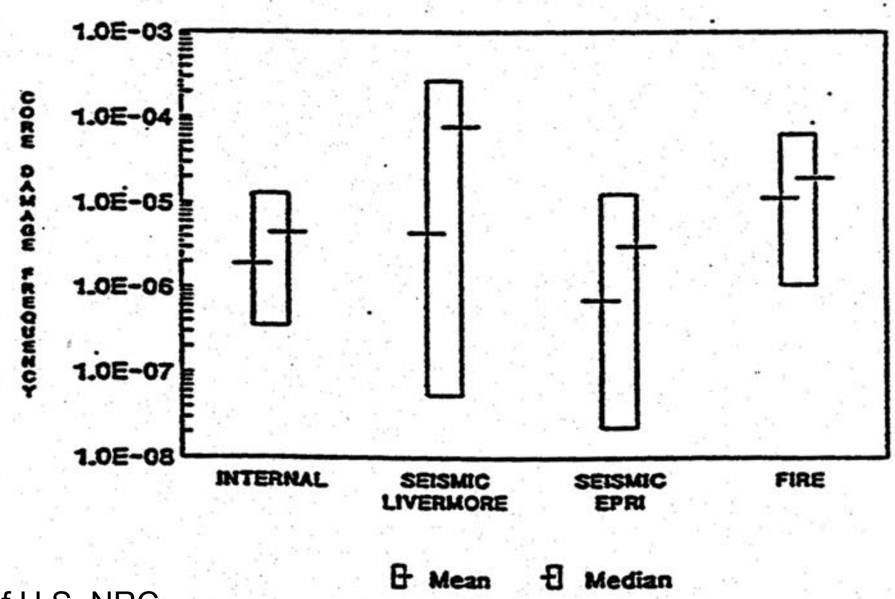
NUREG-1150 Internal Core Damage Frequency Ranges (5th to 9th percentiles).

NUREG-1150: Peach Bottom external-event core damage frequency distributions.



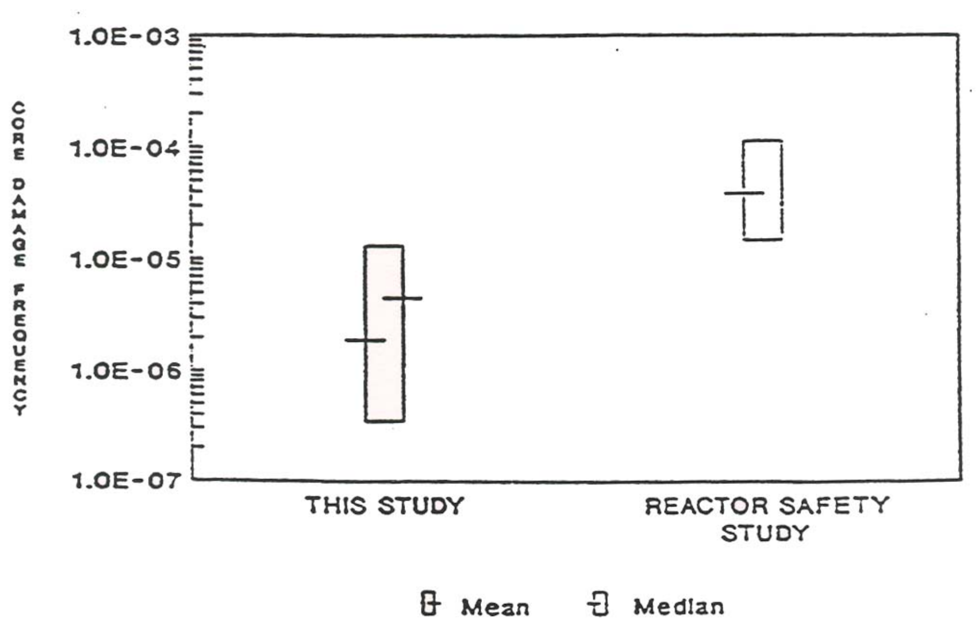
Courtesy of U.S. NRC.

NUREG-1150: Peach Bottom internal and external event core damage frequency ranges.



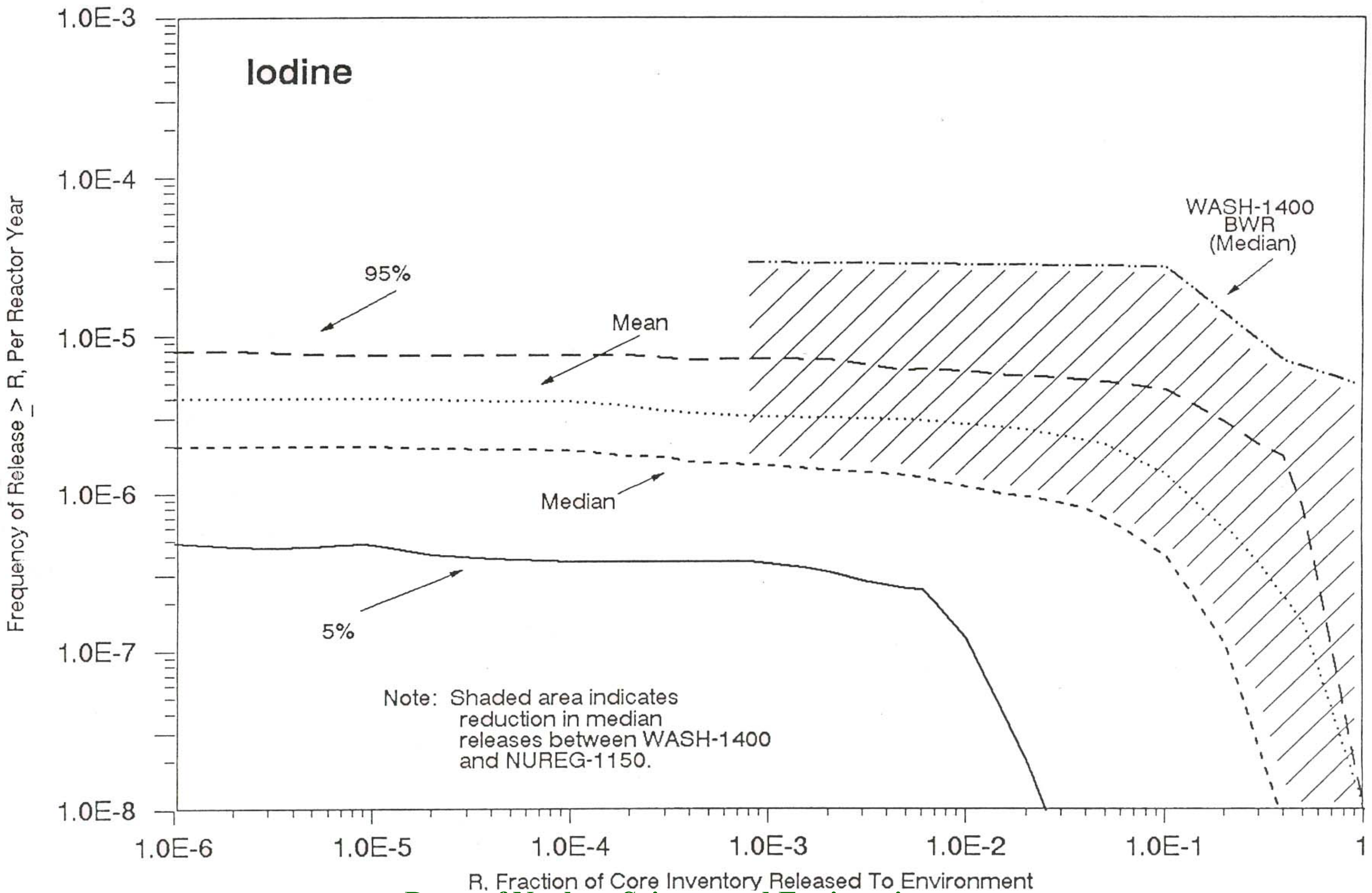
Courtesy of U.S. NRC.

NUREG-1150 and RSS CDF for Peach Bottom

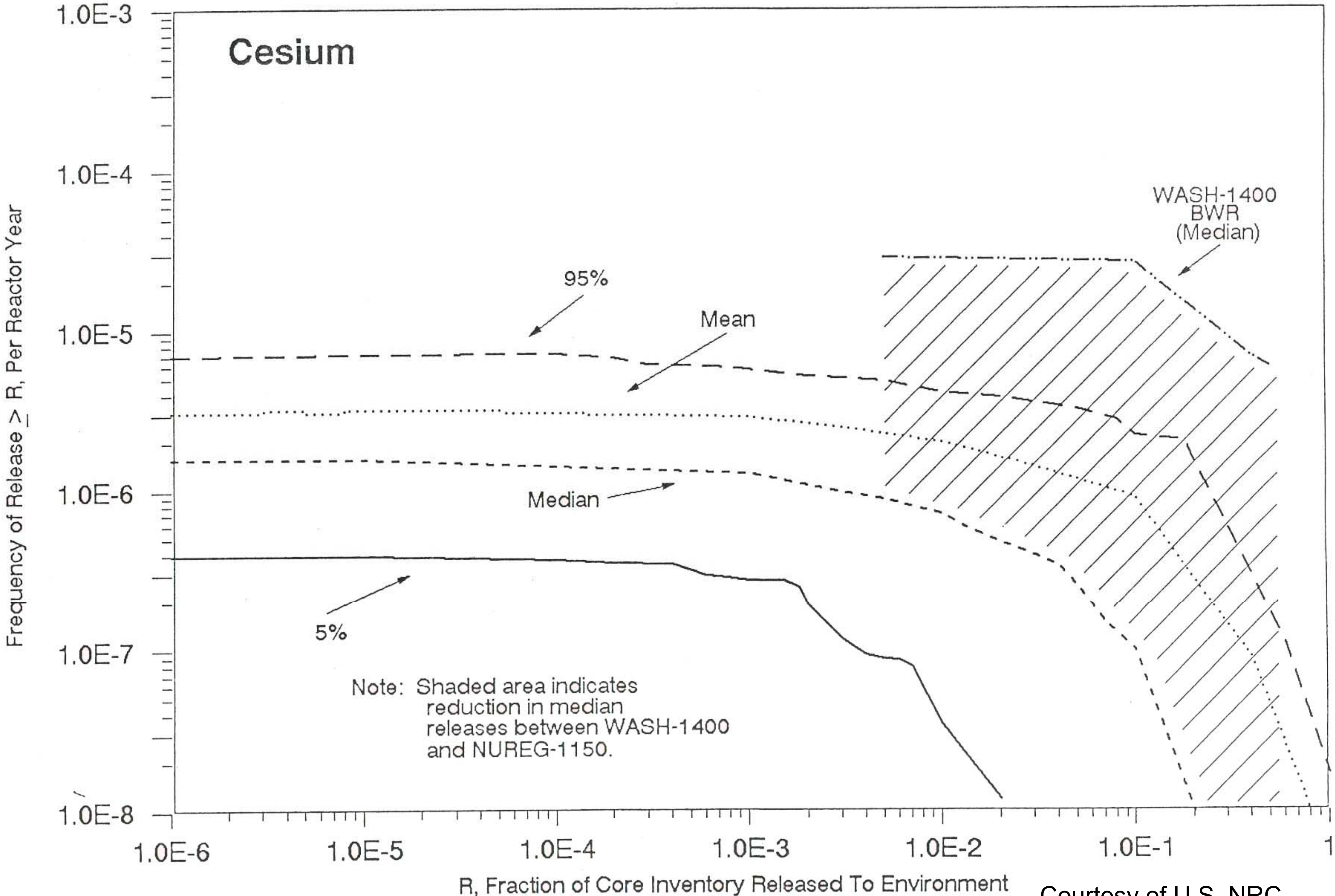


Courtesy of U.S. NRC.

Comparison of Iodine Releases (Peach Bottom)



Comparison of Cesium Releases (Peach Bottom)



Courtesy of U.S. NRC.

Observations on IPEs (GL: 1988)

- Quality of the IPEs varies from licensee to licensee
- Level I PRA methods generally sound
- Some concerns relative to
  - human reliability analysis
  - common cause failures
  - data analysis
- Containment performance analysis less thorough.

Quantitative Safety Goals of the US Nuclear Regulatory Commission (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.**

Subsidiary Goals

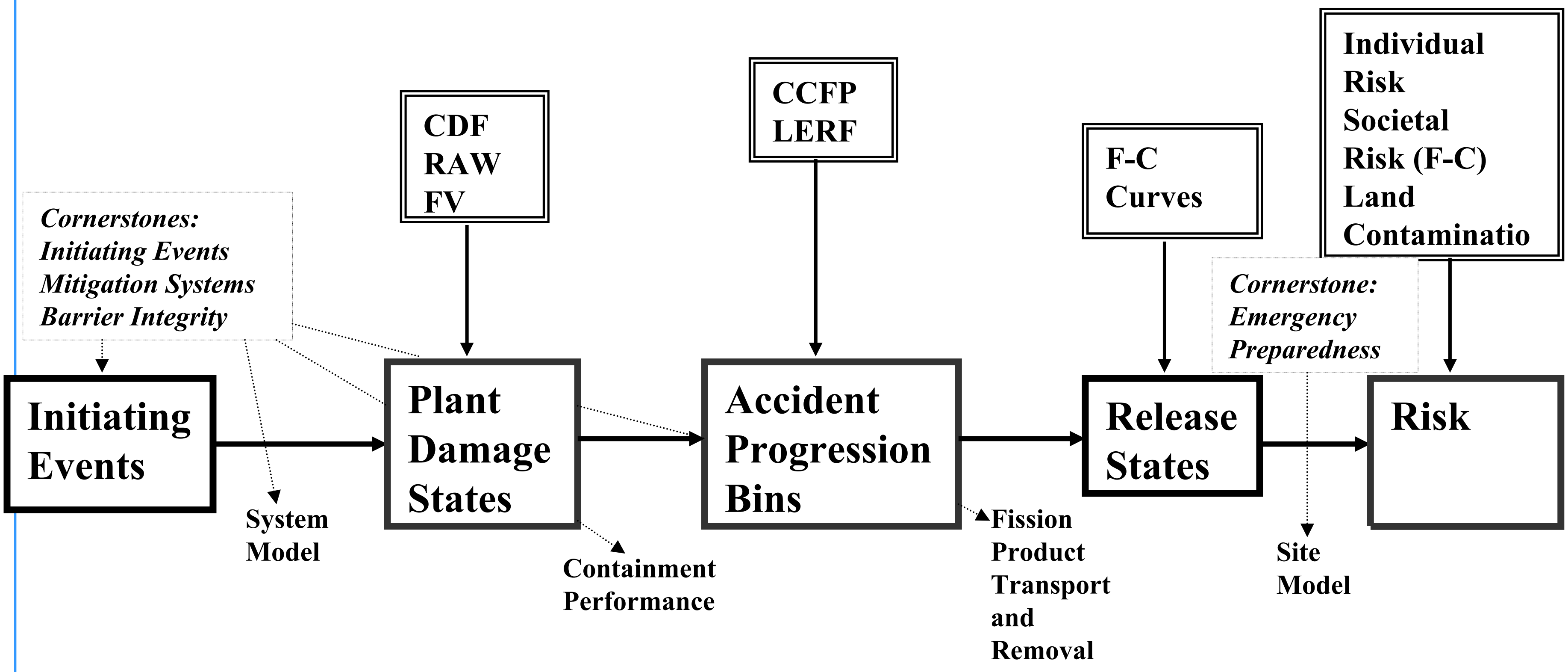
- The average core damage frequency (CDF) should be less than 10^{-4}/ry (once every 10,000 reactor years)

- The large early release frequency (LERF) should be less than 10^{-5}/ry (once every 100,000 reactor years)

Large Early Release Frequency

- LERF is being used as a surrogate for the early fatality QHO.
- It is defined as the frequency of those accidents leading to significant, unmitigated releases from containment in a time frame prior to effective evacuation of the close-in population such that there is a potential for early health effects.
- Such accidents generally include unscrubbed releases associated with early containment failure at or shortly after vessel breach, containment bypass events, and loss of containment isolation.

Subsidiary Objectives: A PRA Perspective



PRA Policy Statement (1995)

- 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.

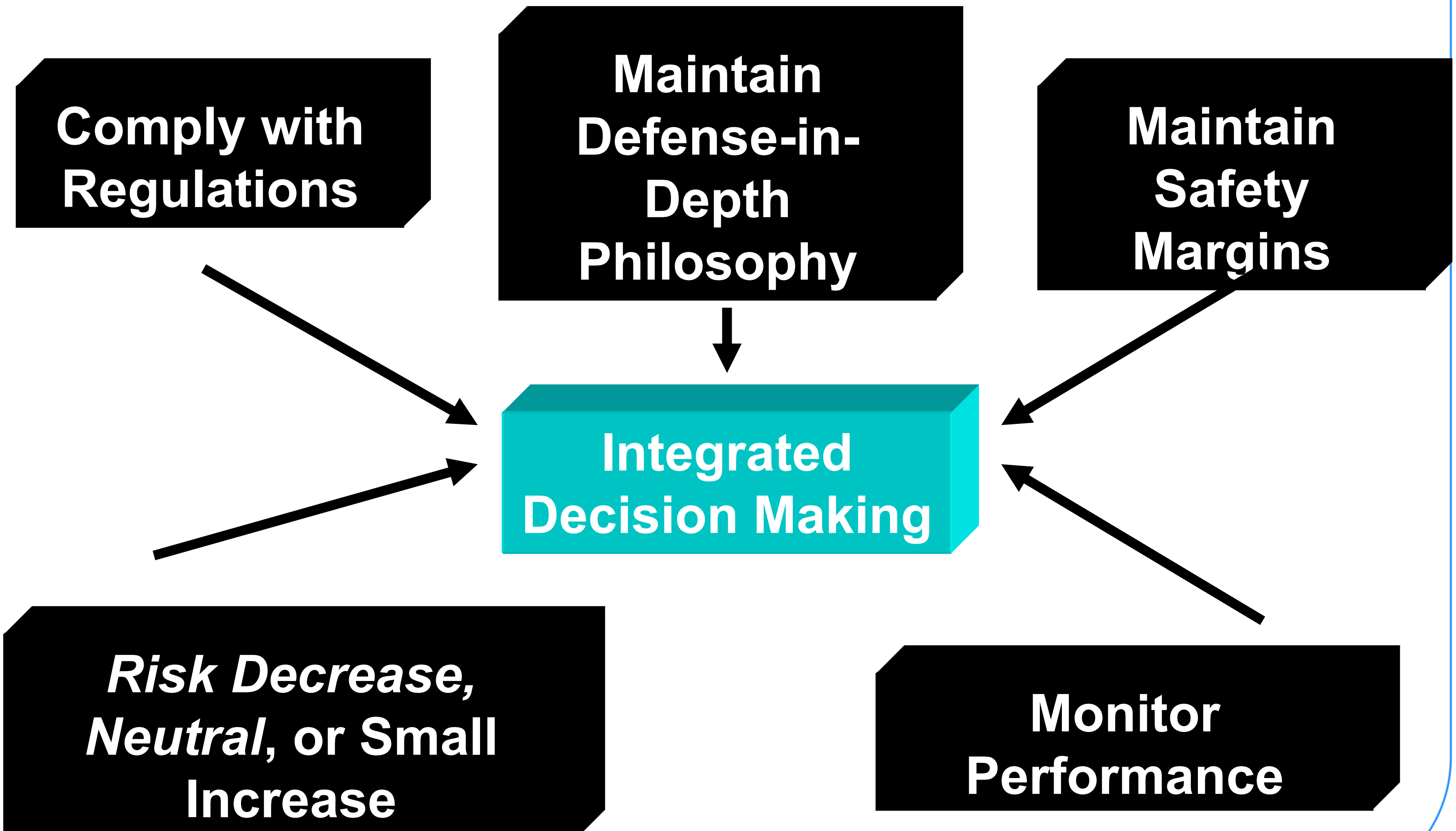
Risk-Informed Regulation

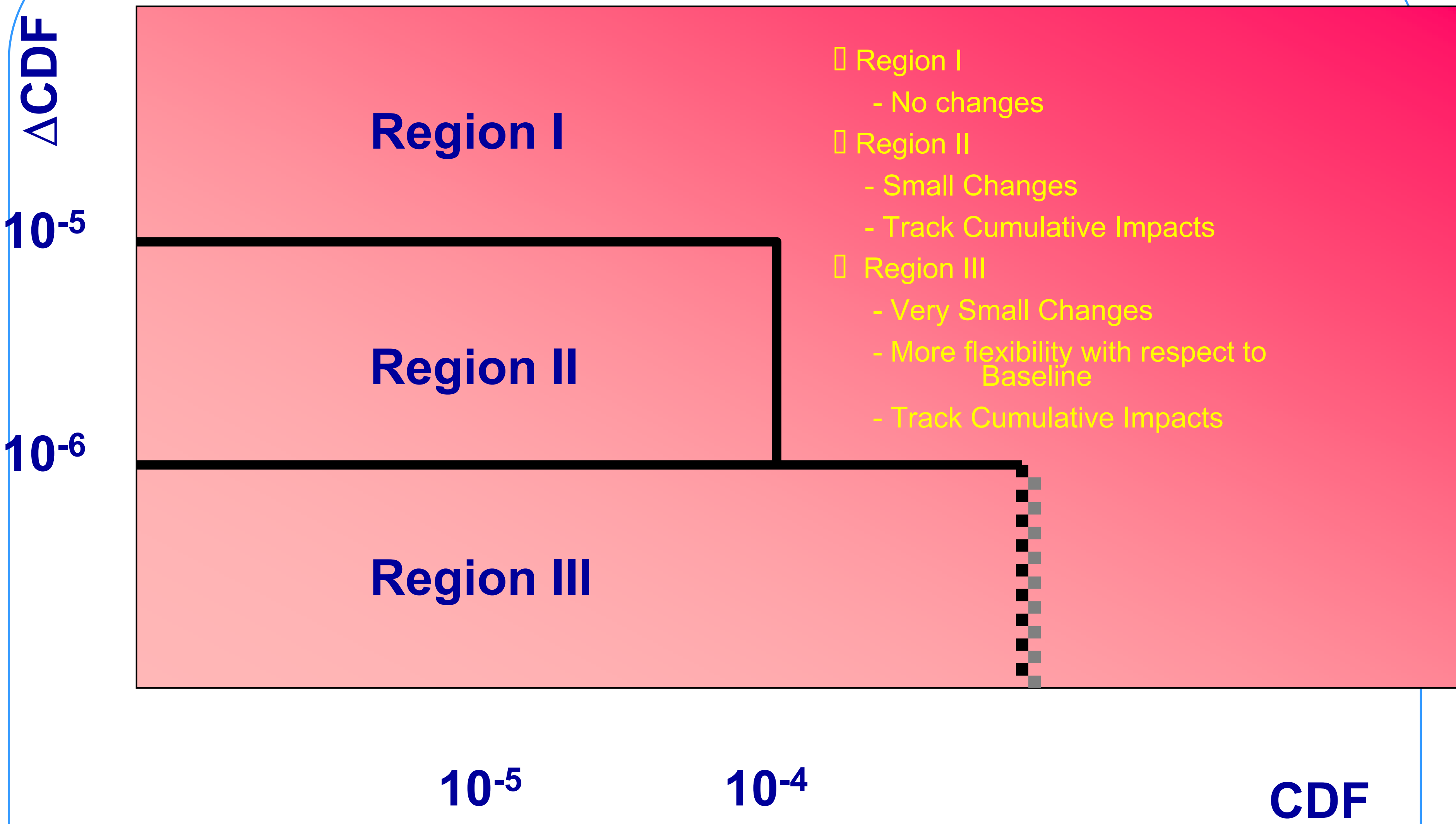
- Insights derived from PRAs are used in combination with deterministic system analysis to focus licensee and regulatory attention on issues commensurate with their importance to safety.

Performance-Based Regulation

- Measurable parameters to monitor plant and licensee performance.
- Objective criteria to assess performance based on a combination of risk insights, deterministic analysis, and performance history.
- Licensee flexibility to determine how to meet established performance criteria.
- Failure to meet a performance criterion must not result in unacceptable consequences.

Risk-Informed Decision Making (RG 1.174; 1998)





Acceptance Guidelines for Core Damage Frequency

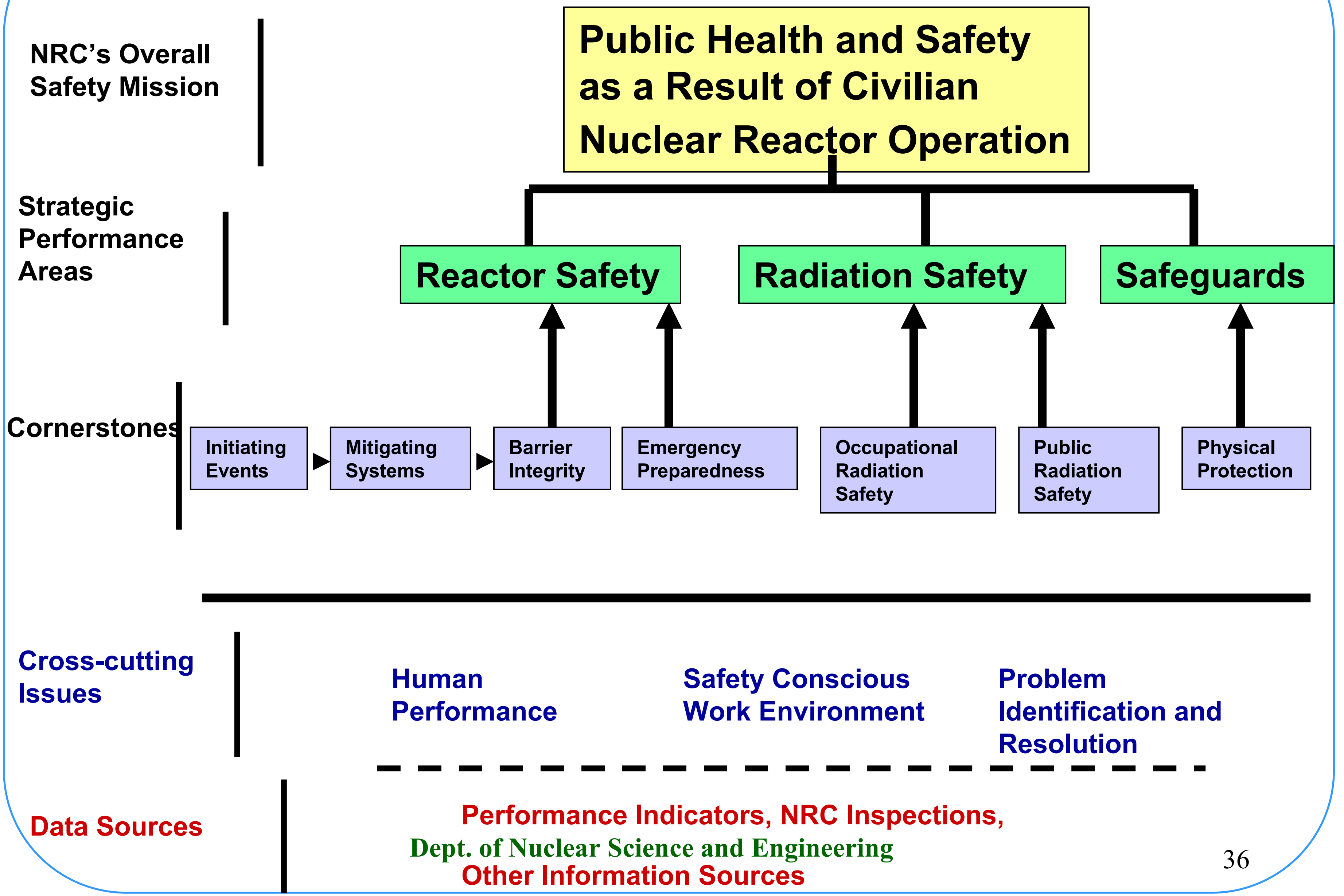
Regulatory Guides

- General Guidance (RG 1.174)
- In-Service Testing (RG 1.175)
- Graded Quality Assurance (RG 1.176)
- Technical Specifications (RG 1.177)
- In-Service Inspection (RG 1.178)

South Texas Project Experience with Allowed Outage Times

- **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.**

Reactor Oversight Process

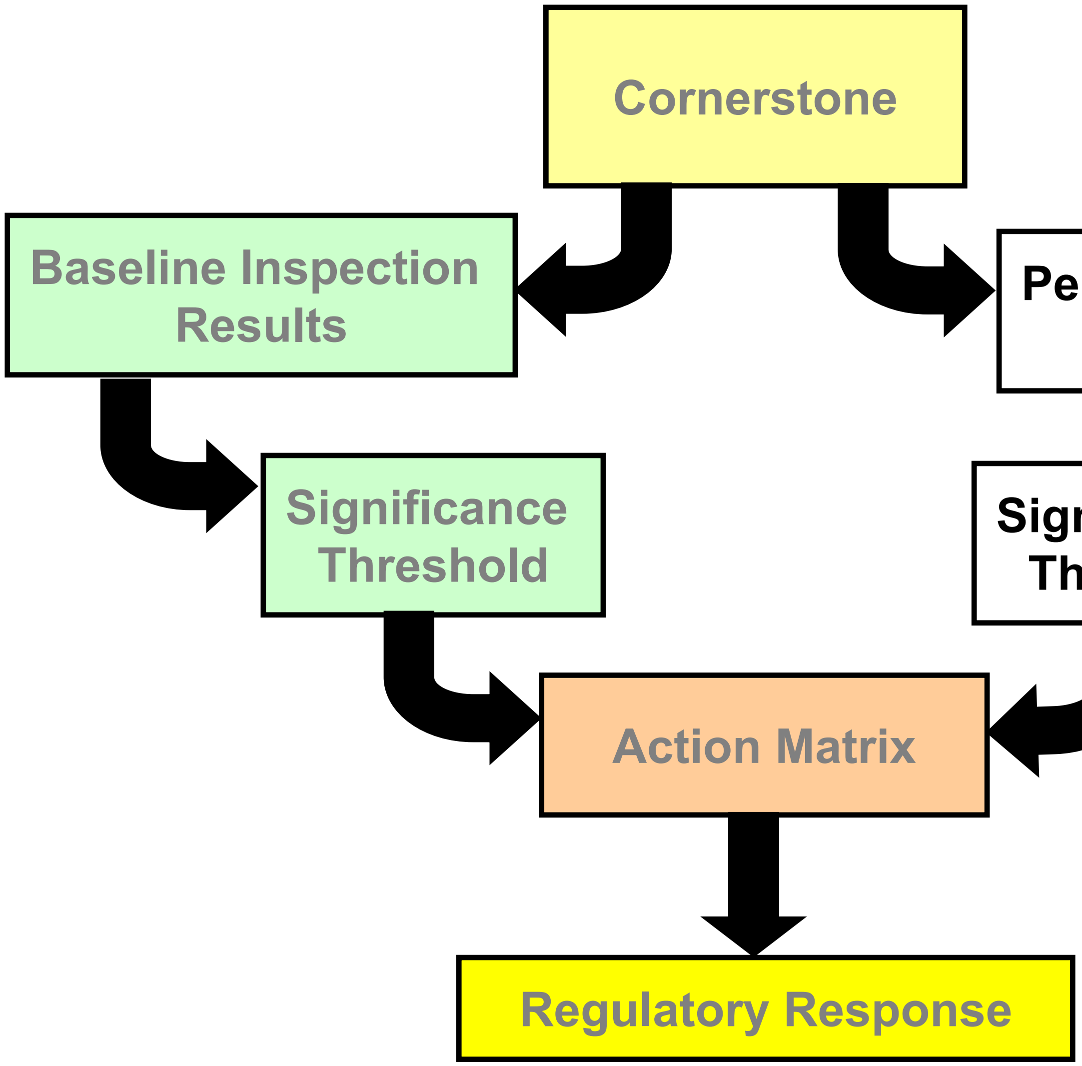


Dept. of Nuclear Science and Engineering

Levels of Significance Associated with Performance Indicators and Inspection Findings

- **Green - very low risk significance (for PIs: Within peer performance)**
- **White - low to moderate risk significance**
- **Yellow - substantive risk significance**
- **Red - high risk significance**

$\Delta CDF < 1E\text{-}6$
$1E\text{-}6 < \Delta CDF < 1E\text{-}5$
$1E\text{-}5 < \Delta CDF < 1E\text{-}4$
$\Delta CDF > 1E\text{-}4$


Cornerstone
Baseline Inspection Results
Performance Indicator Results
Significance Threshold
Significance Threshold
Action Matrix
Regulatory Response

Examples of Performance Indicators

- Initiating Events
  - Unplanned Scrams
  - Scrams with Loss of Normal Heat Removal
  - Unplanned Power Changes
- Mitigating Systems
  - Safety System Unavailability
  - Safety System Functional Failures
- Barriers
  - Fuel Cladding (Reactor Coolant System)
  - Reactor Coolant System (Leak Rate)

		Licensee Response Column	Regulatory Response Column	Degraded Cornerstone Column	Multiple Repetitive Degraded Cornerstone Column	Unacceptable Performance Column
Results		All assessment inputs (performance Indicators (PI) and inspection findings) Green; cornerstone objectives fully met	One or two White inputs (in different cornerstones) in a strategic performance area; Cornerstone objectives fully met	One degraded cornerstone (2 White inputs or 1 Yellow input) or any 3 White inputs in a strategic performance area; cornerstone objectives met with minimal reduction in safety margin	Repetitive degraded cornerstone, multiple degraded cornerstones, multiple Yellow inputs, or 1 Red input[1] ; cornerstone objectives met with longstanding issues or significant reduction in safety margin	Overall unacceptable performance; plants not permitted to operate within this band, unacceptable margin to safety
Response	Regulatory Conference	Routine Senior Resident Inspector (SRI) interaction	Branch Chief (BC) or Division Director (DD) meet with Licensee	DD or Regional Administrator (RA) meet with Licensee	EDO (or Commission) meet with Senior Licensee Management	Commission meeting with Senior Licensee Management
Response	Licensee Action	Licensee Corrective Action	Licensee corrective action with NRC oversight	Licensee self assessment with NRC oversight	Licensee performance improvement plan with NRC oversight	
Response	NRC Inspection	Risk-informed baseline inspection program	Baseline and supplemental inspection **95001**	Baseline and supplemental inspection **95002**	Baseline and supplemental inspection **95003**	
Response	Regulatory Actions	None	Document response to degrading area in assessment letter	Document response to degrading condition in assessment letter	10 CFR 2.204 DFI 10 CFR 50.54(f) letter CAL/Order	Order to modify, suspend, or revoke licensed activities
Communications	Assessment Report	BC or DD review / sign assessment report (w/ inspection plan)	DD review / sign assessment report (w/ inspection plan)	RA review / sign assessment report (w/ inspection plan)	RA review / sign assessment report (w/ inspection plan) Commission informed	
Communications	Public Assessment Meeting	SRI or BC meet with Licensee	BC or DD meet with Licensee	RA discuss performance with Licensee	EDO (or Commission) discuss performance with Senior Licensee Management	Commission meeting with Senior Licensee Management
	Increasing Safety Significance →					

[1] It is expected in a few limited situations that an inspection finding of this significance will be identified that is not indicative of overall licensee performance. The staff will consider treating these inspection findings as exceptions for the purpose of determining appropriate actions.

PRA Quality

- **PRA is ambitious. It models the whole system including hardware failures, human performance, and relevant physical phenomena.**

- **Defining a "good-enough" PRA for a specific application *a priori* is a highly subjective and very difficult task, given the varied nature of potential risk-informed decisions.**

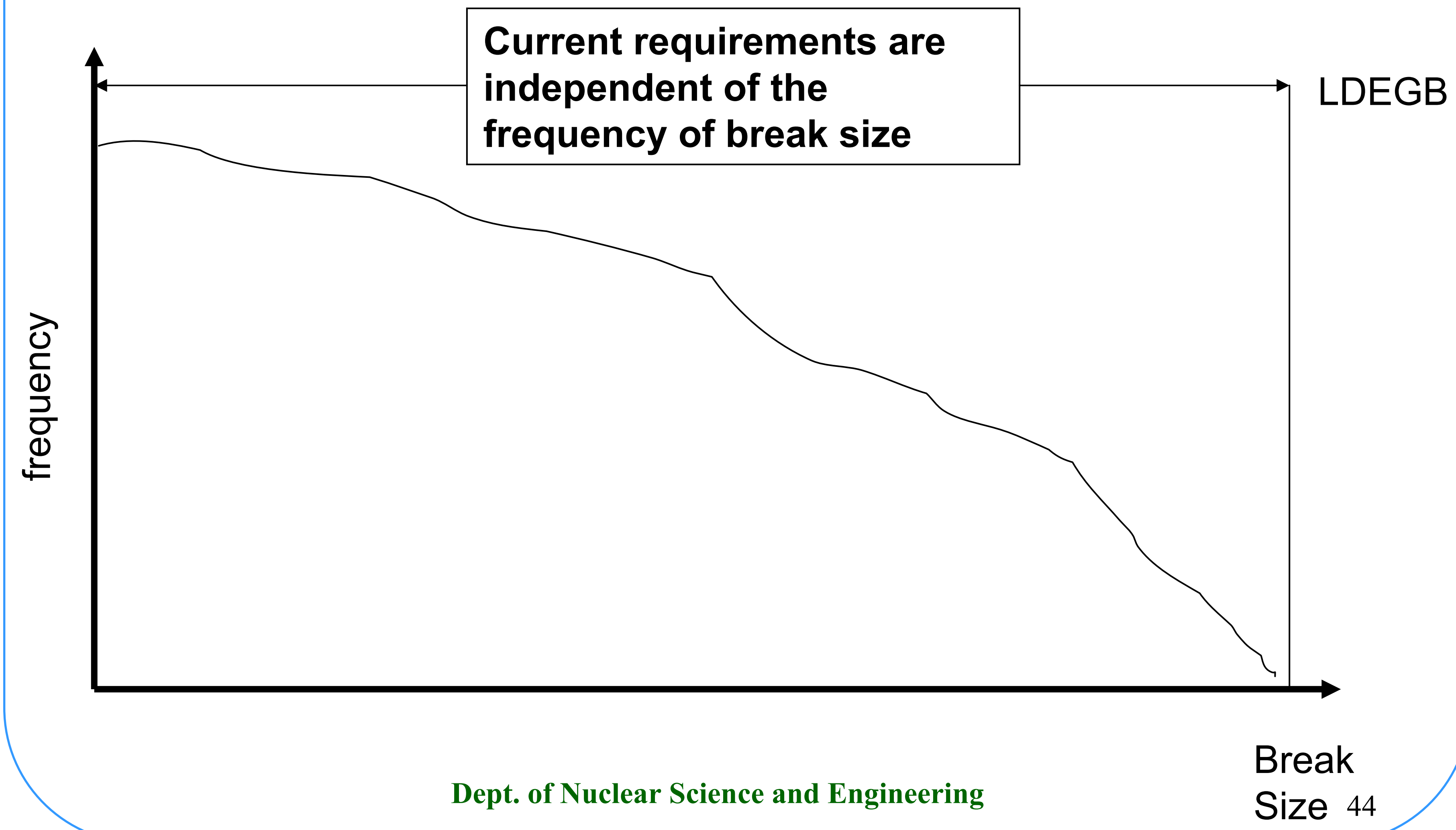
PRA Standards

- **Cannot be traditional, “design-to” standards.**
- **Purpose: To facilitate reviews.**
- **Reviews will still be required.**

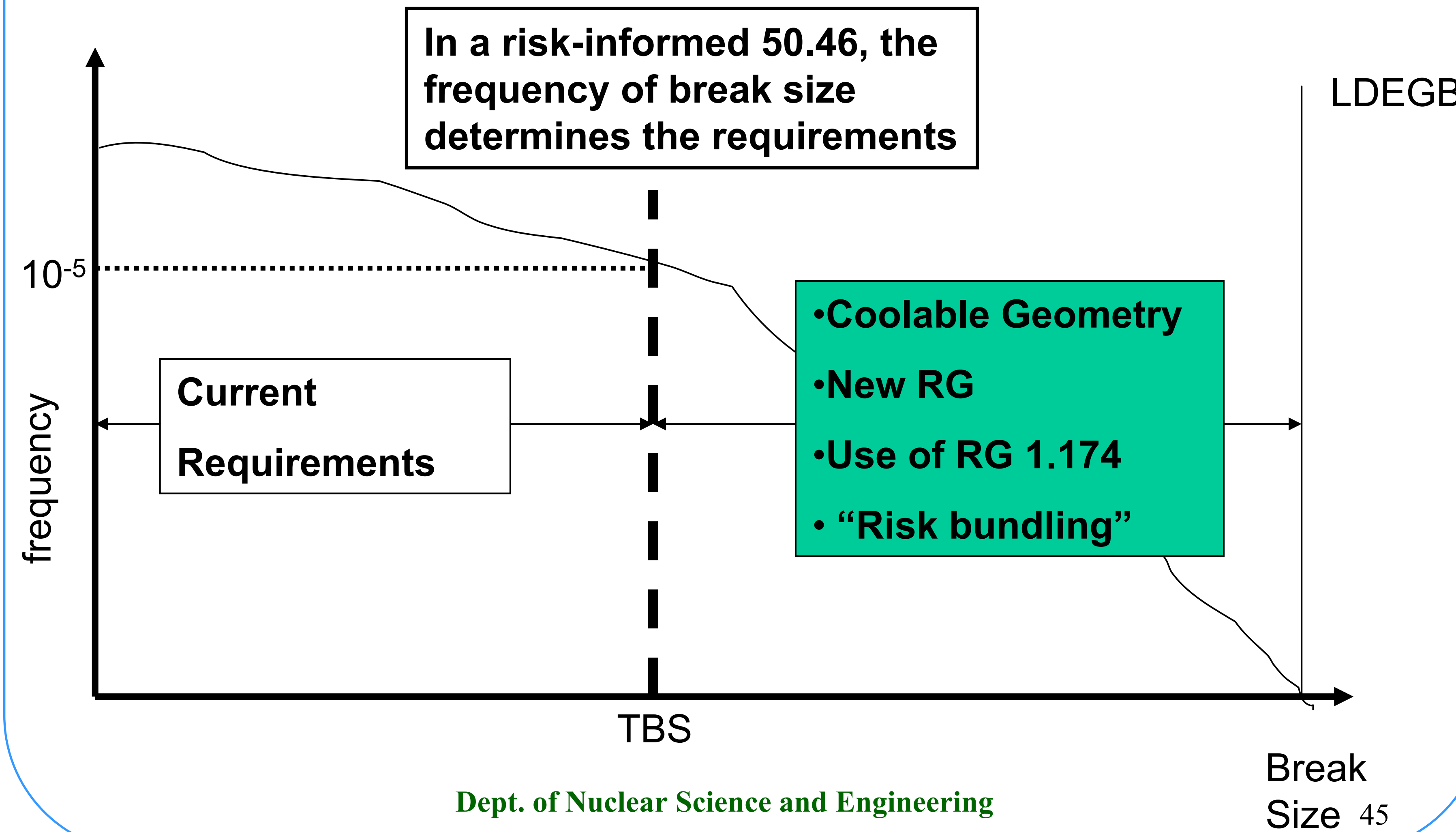
Phased Approach to PRA Quality

- **In the 12/18/03 Staff Requirements Memorandum, the Commission approved the implementation of a phased approach to PRA quality.**
- **The phases are differentiated by the availability of standards.**
- **Phase 3 should be achieved by December 31, 2008. Guidance documents will be available to support all anticipated applications.**

Risk-Informing 10 CFR 50.46 (1)



Risk-Informing 10 CFR 50.46 (2)



Risk-Informing 10 CFR 50.46 (3)

Uncertainties in expert opinions create uncertainty in TBS determination