Reactor Safety: The Emergence of Probabilistic Risk Assessment

22.39 Elements of Reactor Design, Operations, and Safety

Lecture 7

Fall 2006

George E. Apostolakis
Massachusetts Institute of Technology

The Pre-PRA Era (prior to 1975)

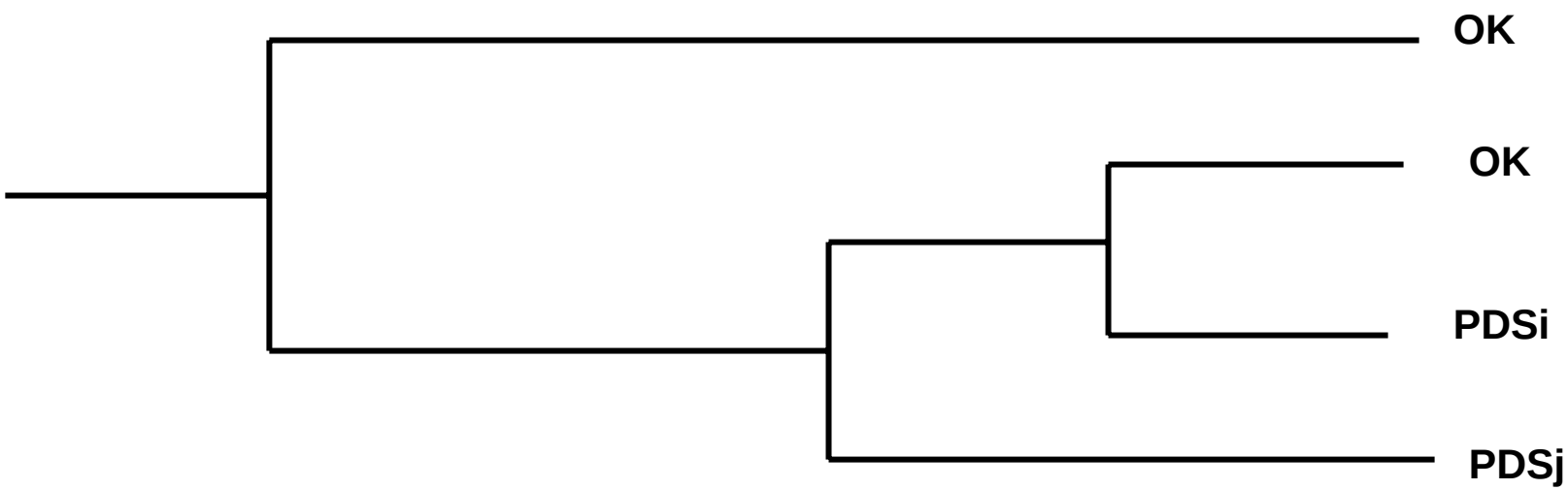
- **Management of (unquantified at the time) uncertainty was always a concern.**
- **Defense-in-depth and safety margins became embedded in the regulations.**
- **"Defense-in-Depth is an element of the NRC's safety philosophy that employs successive compensatory measures to prevent accidents or mitigate 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.**

Farmer's Paper (1967)

- **Iodine-131 is a major threat to health in a nuclear plant accident.**
- **Attempting to differentiate between credible (DBAs) and incredible accidents (Class 9; multiple protective system failures) 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.**

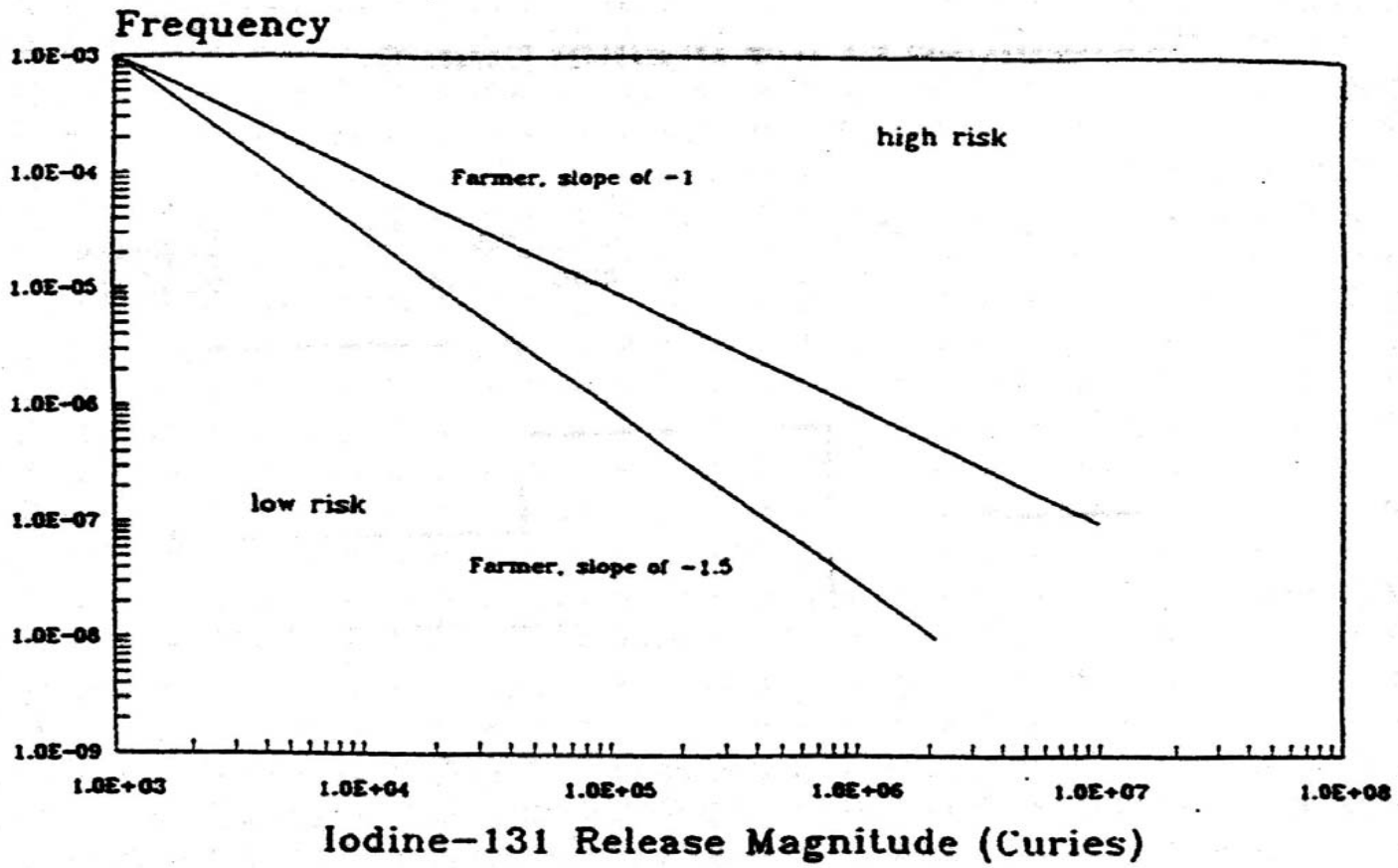
Loss-of-offsite-power event tree

LOOP	Secondary Heat Removal	Bleed & Feed	Recirc.	Core



THE FARMER LINE

Source: Oak Ridge National Laboratory



Technological Risk Assessment

- **Study the system as an integrated *socio-technical* system.**

Probabilistic Risk Assessment (PRA) supports Risk Management by answering the questions:

- **What can go wrong? (accident sequences or scenarios)**
- **How likely are these scenarios?**
- **What are their consequences?**

The Kaplan & Garrick Definition of Risk

(*Risk Analysis*, 1 (1981) 11-28)

$$R = \{< s_i, \pi_i(\varphi_i), c_i >\}$$

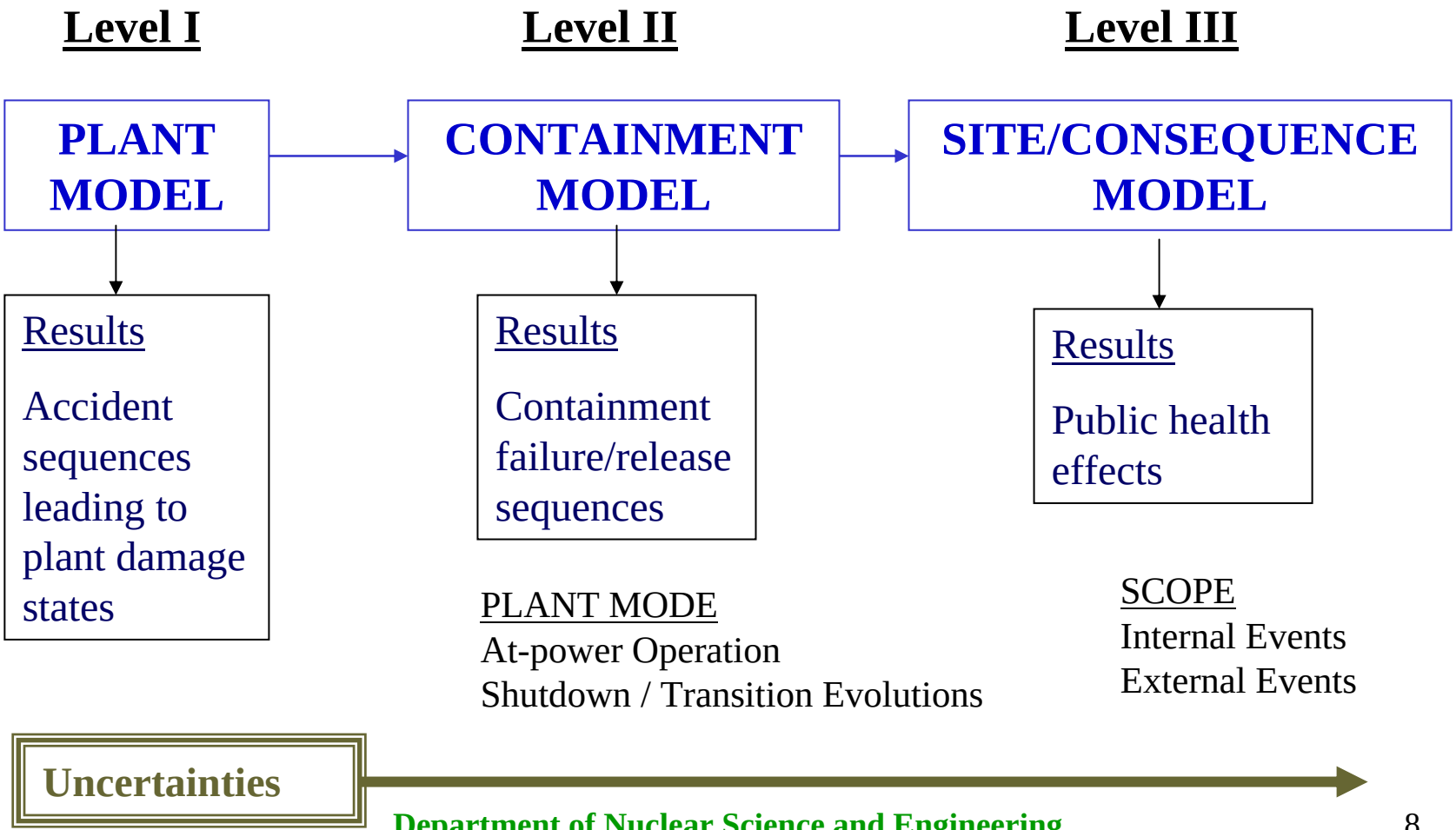
s_i: scenario i, $i = 1,\ldots,N$

φ_i: frequency of s_i (aleatory uncertainty)

$\pi_i(\varphi_i)$: pdf of φ_i (epistemic uncertainty)

c_i : consequence i

PRA Model Overview



At Power Level I Results

CDF = 4.5×10^{-5} / yr (Modes 1, 2, 3)

Initiator Contribution to CDF Total:

- **Internal Events……..56%**
- **External Events ……44%**
  - ***Seismic Events*** ***24%***
  - ***Fires*** ***18%***
  - ***Other*** ***2%***

From: K. Kiper, MIT Lecture, 2006

Level I Results

- **Functional Sequences**

Contribution	CDF
– Transients - Station Blackout/Seal LOCA	45%
– Transients - Loss of Support Systems/Seal LOCA	29%
– Transients - Loss of Feedwater/Feed & Bleed	12%
– LOCA - Injection/Recirculation Failure	7%
– ATWS - No Long Term Reactivity Control	6%
– ATWS - Reactor Vessel Overpressurization	2%

From: K. Kiper, MIT Lecture, 2006

At Power Level II Results

Release Categories	Conditional Probability
– *Large-Early*	*0.002*
– *Small-Early*	*0.090*
– *Large-Late*	*0.249*
– *Intact*	*0.659*

Large-Early Release Freq (LERF) = 7×10^{-8} / yr

Large-Early Failure Mode	Percent Contribution
– *Containment Bypass*	*82%*
– *Containment Isolation Failure*	*18%*
– *Gross Containment Failure*	*0.1%*

From: K. Kiper, MIT Lecture, 2006

SHUTDOWN

Shutdown, Full Scope, Level 3 PSA (1988)

Results: **Mean $CDF_{shutdown}$ ~ Mean CDF_{power}**

- **Dominant CD sequence:**
  ***Loss of RHR at reduced inventory*.**
- **Risk dominated by operator actions - causing and mitigating events.**
- **Significant risk reductions with low-cost modifications and controls.**
  - ***Midloop level monitor, alarm***
  - ***Procedures, training***
  - ***Administrative controls on outage planning***

From: K. Kiper, MIT Lecture, 2006

Shutdown PRA Issues

- **Risk is dominated by operator actions - importance of HRA.**
- **Generic studies give useful insights, but risk-controlling factors are plant-specific.**
- **Shutdown risk is dynamic - average risk is generally low (relative to full power risk), but is subject to risk "spikes."**
- **Shutdown risk is more amenable to "management." At-power risk is designed in.**

From: K. Kiper, MIT Lecture, 2006

Integrated Risk (All Modes) – 2002 Update

Mode	Description	CDF	Percent of Total
Mode 1	Full-power (>70% pwr)	4.28 E-5	63%
Mode 2	Low-power (<70% pwr)	0.15 E-5	2%
Mode 3	Hot Standby	0.08 E-5	1%
Mode 4	Hot Shutdown	0.05 E-5	1%
Mode 5	Cold Shutdown	0.91 E-5	13%
Mode 6	Refueling	1.38 E-5	20%
Total Core Damage Frequency		6.86E-5	100%

From: K. Kiper, MIT Lecture, 2006

Reactor Safety Study (WASH-1400; 1975)

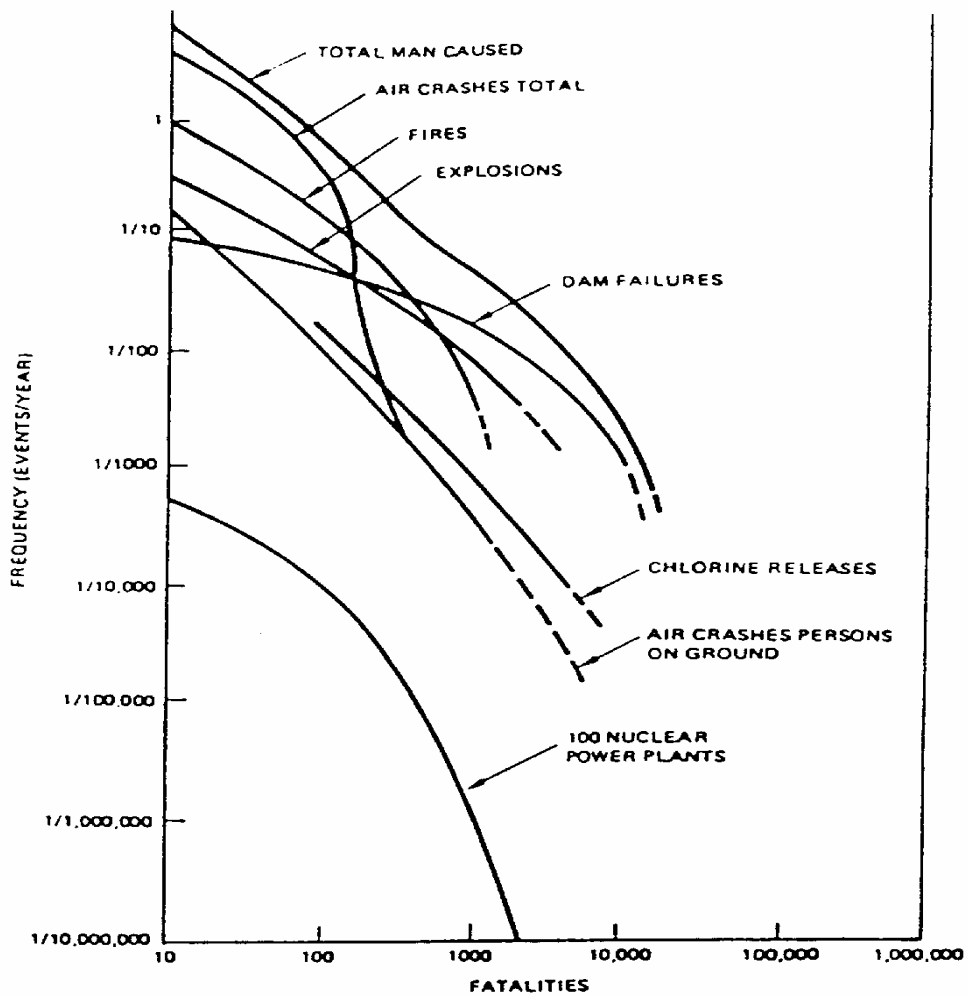
Prior Beliefs:

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



Source: WASH-1400, U.S. AEC.

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

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.**

Example PRA Results

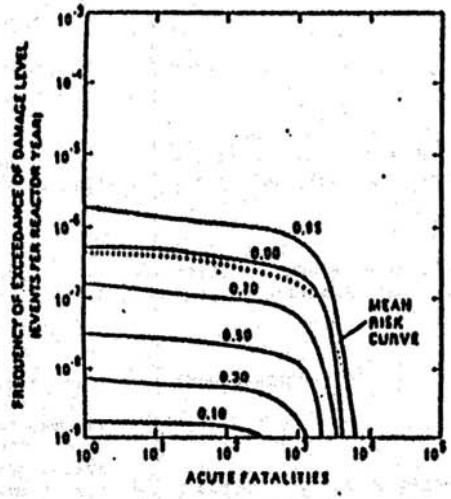


FIGURE 1-1a. RISK OF EARLY FATALITIES

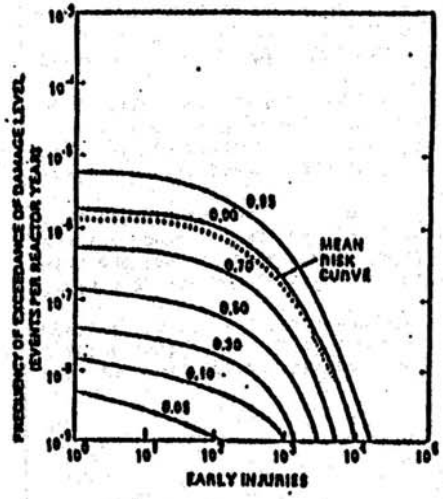


FIGURE 1-1b. RISK OF INJURIES

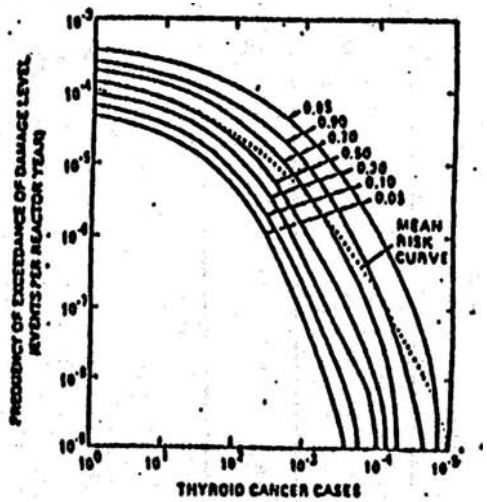


FIGURE 1-1c. RISK OF THYROID CANCER CASES

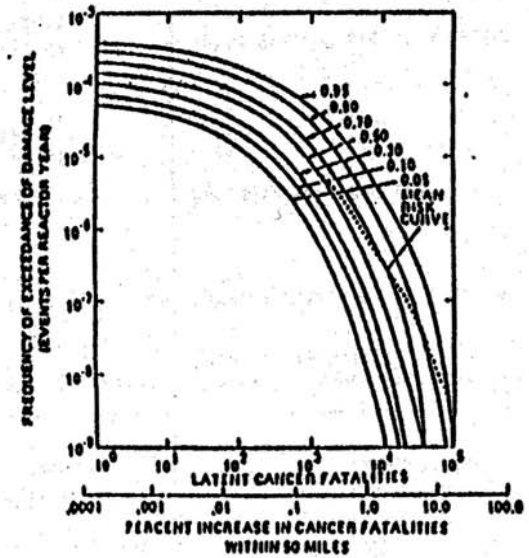


FIGURE 1-1d. RISK OF LATENT CANCER FATALITIES (OTHER THAN FATAL THYROID CANCERS)

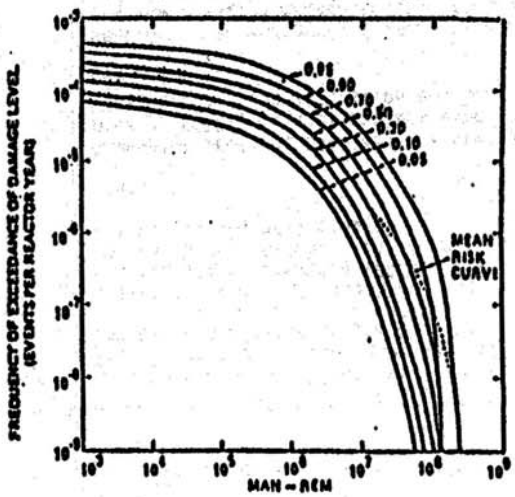


FIGURE 1-1e. RISK OF MAN-REM

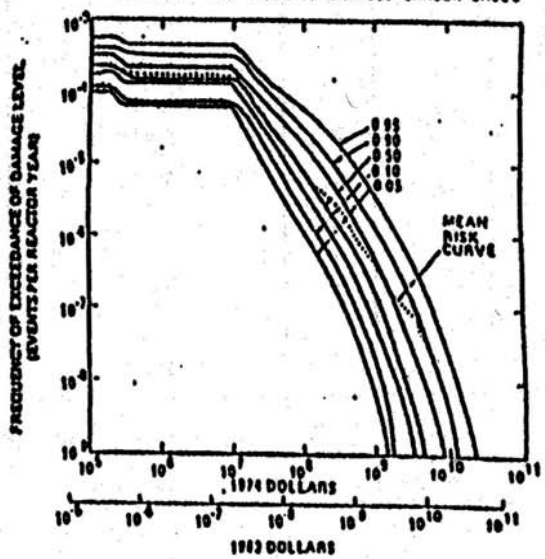


FIGURE 1-1f. RISK OF PROPERTY DAMAGE AND EVACUATION COSTS

Courtesy of K. Kiper. Used with permission.

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

Sheet 1 of 2

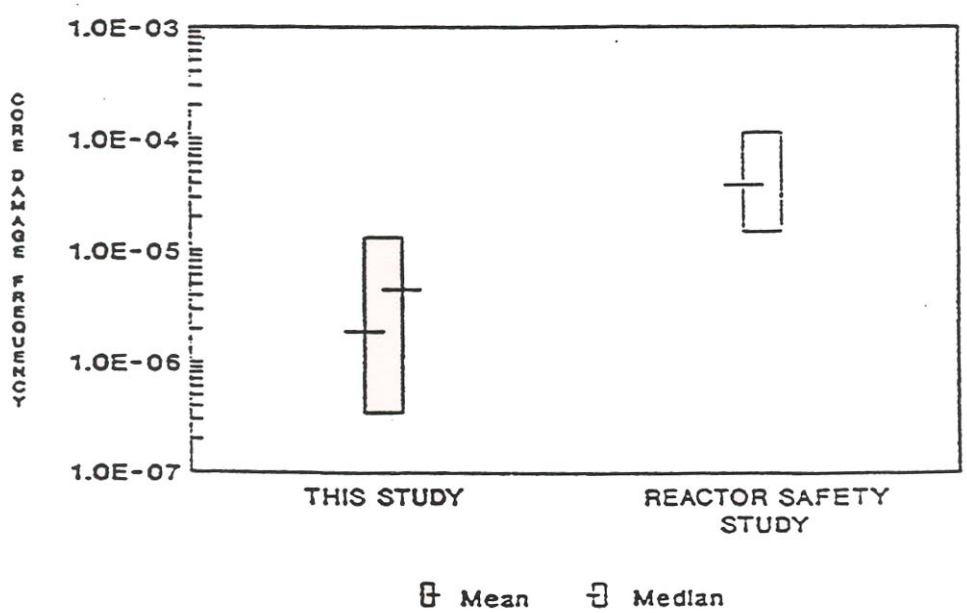
Initiating Event	Additional System Failures/ Human Actions	Resulting Dependent Failures	Sequence Frequency (per reactor year)	Sequence Ranking		
				Core Melt	Latent Health Risk	Early Health Risk
Loss of Offsite Power	Onsite AC Power, No Recovery of AC Power Before Core Damage	Component cooling, high 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.

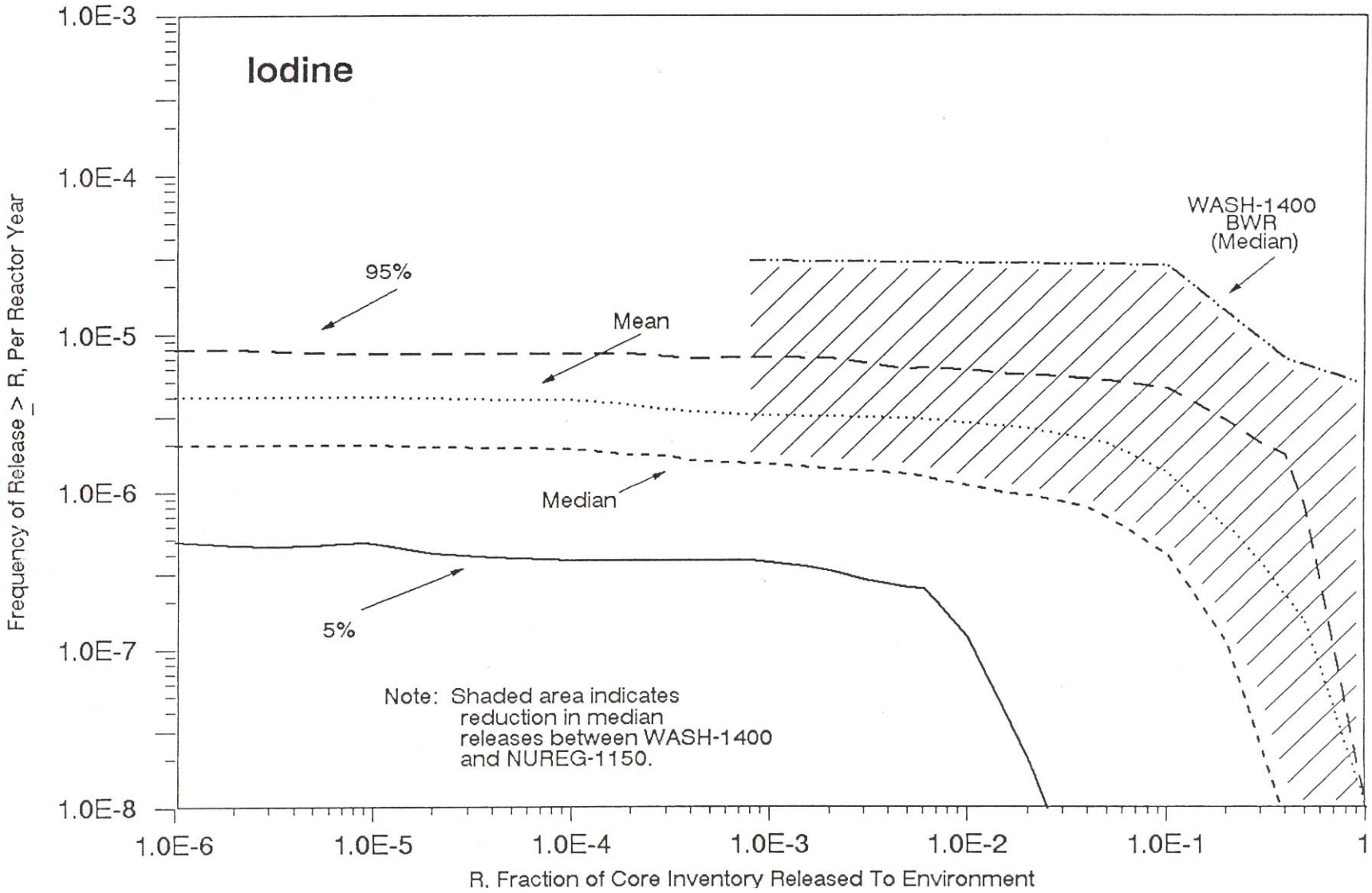
NOTE: Exponential notation is indicated in abbreviated form; i.e., 3.3-5 = 3.3×10^{-5}.

Courtesy of K. Kiper. Used with permission.

NUREG-1150 and RSS CDF for Peach Bottom



Comparison of Iodine Releases (Peach Bottom)



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.**

Societal Risks

- ***Annual Individual Occupational Risks***
  - **All industries 7×10^{-5}**
  - **Coal Mining: 24×10^{-5}**
  - **Fire Fighting: 40×10^{-5}**
  - **Police: 32×10^{-5}**
  - **US President $1{,}900 \times 10^{-5}$ (!)**
- ***Annual Public Risks***
  - **Total 870×10^{-5}**
  - **Heart Disease 271×10^{-5}**
  - **All cancers 200×10^{-5}**
  - **Motor vehicles: 15×10^{-5}**

From: Wilson & Crouch, *Risk/Benefit Analysis*, Harvard University Press, 2001.

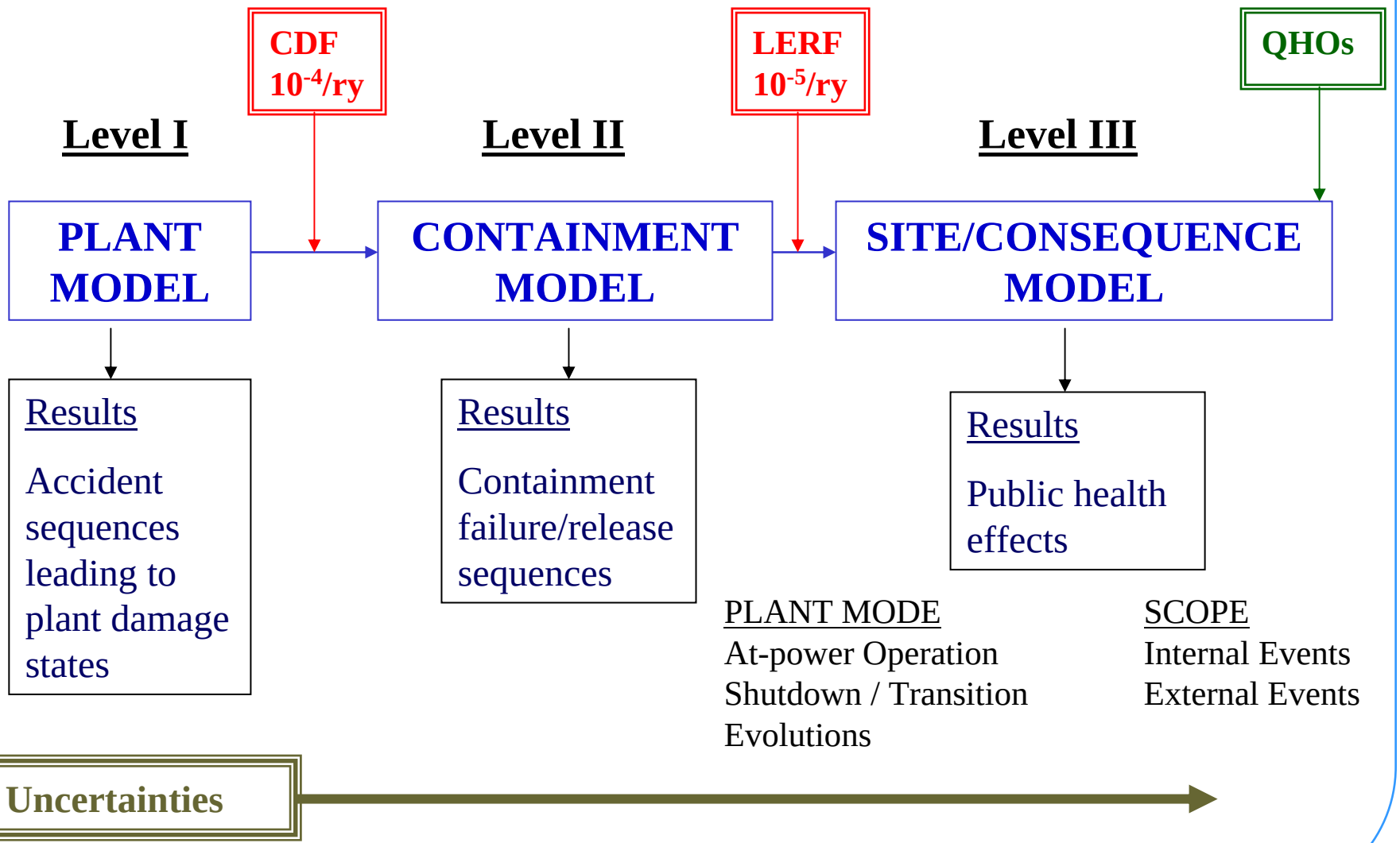
Subsidiary Goals

- **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)**

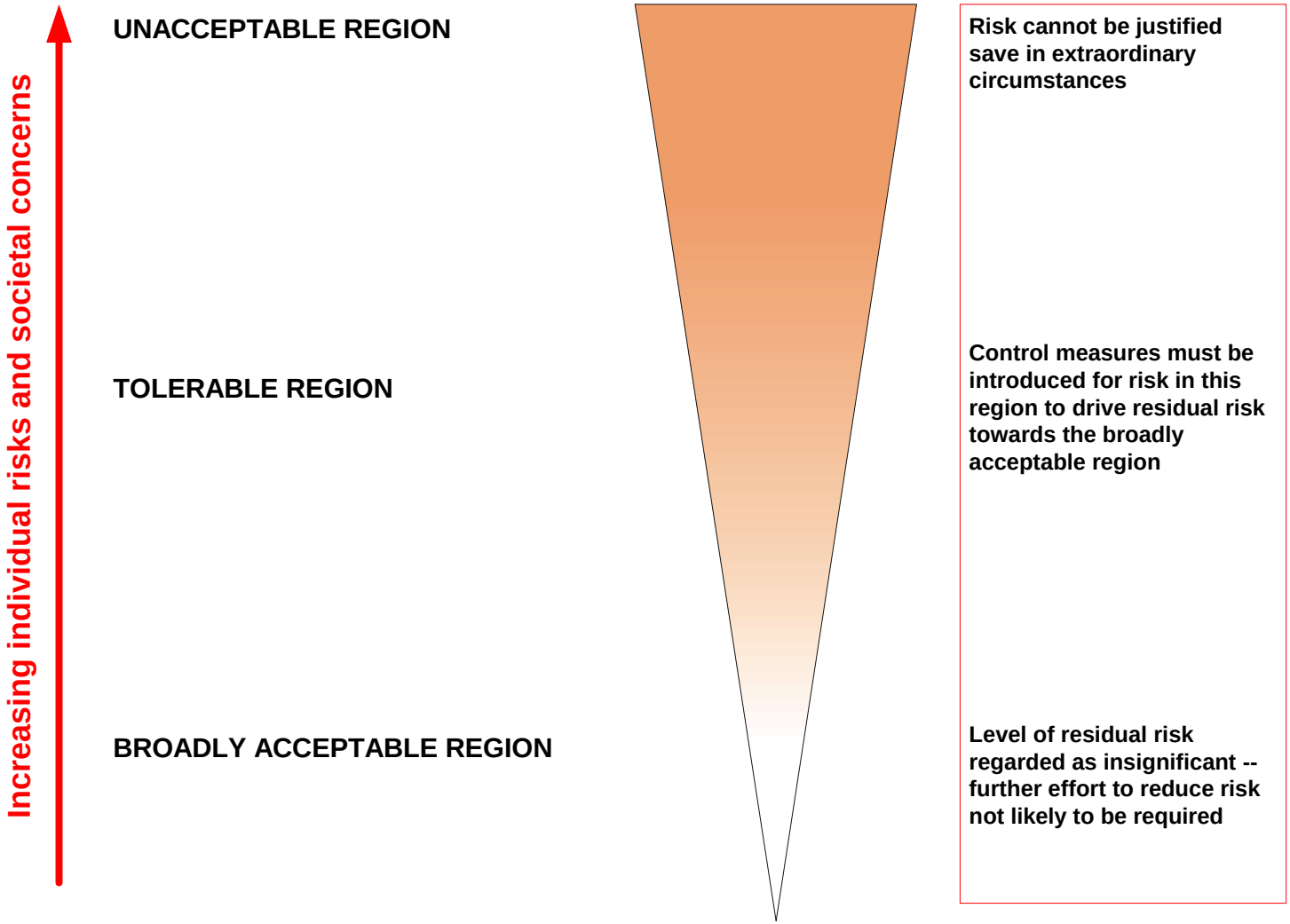
Large Early Release Frequency

- **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.**

PRA Model Overview and Subsidiary Objectives



“Acceptable” vs. “Tolerable” Risks (UKHSE)

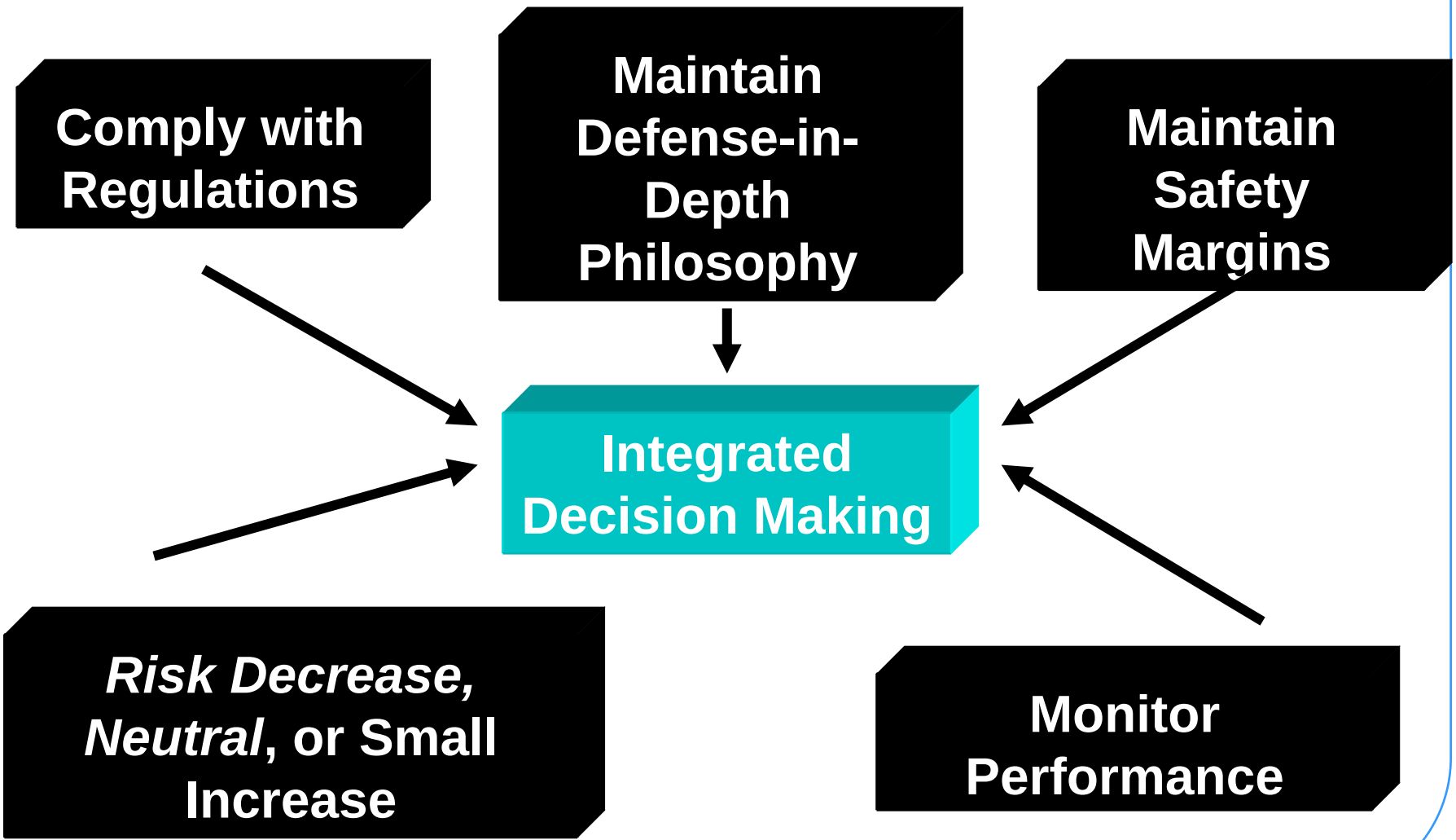


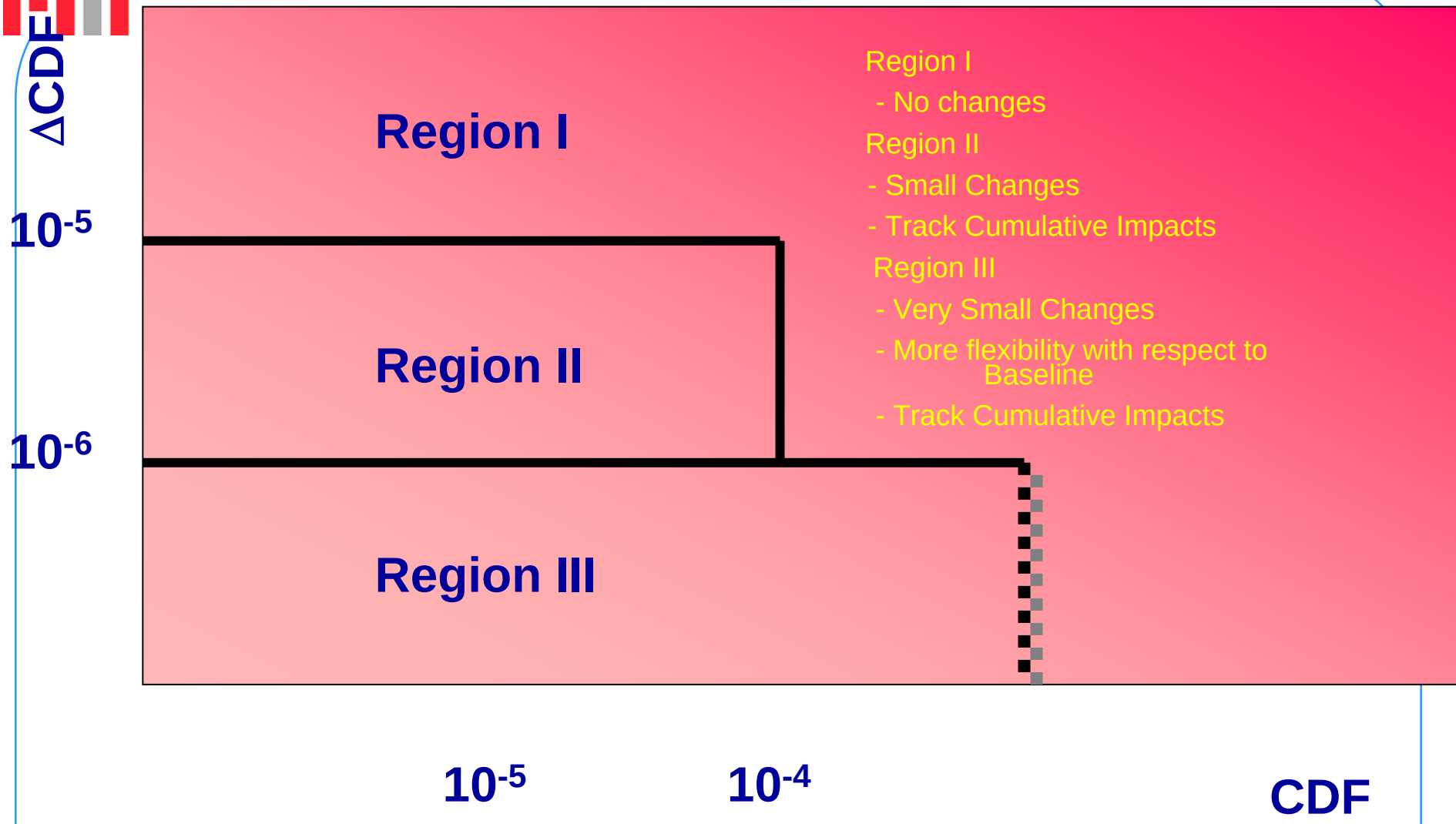
PRA Policy Statement (1995)

- **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 Decision Making for Licensing Basis Changes (RG 1.174, 1998)





Acceptance Guidelines for Core Damage Frequency

Risk-Informed Framework

Traditional "Deterministic" Approaches

- **Unquantified Probabilities**
- **Design-Basis Accidents**
- **Structuralist Defense in Depth**
- **Can impose heavy regulatory burden**
- **Incomplete**

Risk-Informed Approach

- **Combination of traditional and risk-based approaches**

Risk-Based Approach

- **Quantified Probabilities**
- **Scenario Based**
- **Realistic**
- **Rationalist Defense in Depth**
- **Incomplete**
- **Quality is an issue**