PROBABILISTIC RISK ANALYSIS
INTRODUCTION OF THE BASIC ELEMENTS OF PROBABILISTIC RISK (PRA) ANALYSES

- Fault Trees
- Risk
- Data
- Uncertainties
- Nuclear Power Plant PRA Structure
- Typical Results
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.
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?

\[
\text{Risk} = \text{Expected consequences} = \sum_{\text{Sequences,i}} \text{Prob}_i \ast \text{Consequence}_i
\]
DEFINITION OF RISK

Event Risk $≡$ Vector (Set) of Expected Consequences From an Event
For an Event of Type $i$, the Associated Risk Vector, $\vec{R}_i$

$$\vec{R}_i = \langle \vec{C}_i \rangle = (\text{Probability of Event, } i) \times (\text{Set of Consequences of Event, } i)$$
$$= [(\text{Frequency of Event, } i) \times (\text{Time Interval of Interest})] \times (\text{Set of Consequences of Event, } i)$$

CORE DAMAGE RISK DUE TO $N$ DIFFERENT CORE DAMAGE EVENTS

$$\vec{R}_{total} = \sum_{i=1}^{N} \vec{R}_i = \sum_{i=1}^{N} p_i \begin{bmatrix} \text{Consequence}_{1, i} \\ \downarrow \\ \text{Consequence}_{M, i} \end{bmatrix}$$

Total Risk is the Sum Over All Possible Events of the Risks Associated with Each Event, Respectively
RISK CALCULATION

\[
\vec{\text{Risk}} = \sum_{i, \text{All Event Sequences}} \overline{C}_i p_i = \langle \overline{C} \rangle = \begin{bmatrix} \langle C_a \rangle \\ \langle C_b \rangle \\ \vdots \\ \langle C_n \rangle \end{bmatrix}
\]

\[\overline{C}_i = \text{Vector of consequences associated with the } i^{th} \text{ event sequence}\]
\[p_i = \text{Probability of the } i^{th} \text{ event sequence}\]
\[\langle \overline{C} \rangle = \text{Mean, or expected, consequence vector}\]
\[\langle C_a \rangle = \text{Mean, or expected, consequence of type a, summed over all event sequences}\]

EXAMPLE

\[\overline{C}_i = \begin{bmatrix} \text{Offsite acute fatalities due to event } i \\ \text{Offsite latent fatalities due to event } i \\ \text{Onsite acture fatalities due to event } i \\ \text{Onsite latent fatalities due to event } i \\ \text{Offsite property loss due to event } i \\ \text{Onsite property loss due to event } i \\ \text{Costs to other NPPs due to event } i \end{bmatrix}\]
# THE HAZARD
(some fission-product isotopes)

<table>
<thead>
<tr>
<th>Isotope</th>
<th>Half-Life</th>
<th>Volatility</th>
<th>Health Hazard</th>
</tr>
</thead>
<tbody>
<tr>
<td>$^{131}$I</td>
<td>8 d</td>
<td>Gaseous</td>
<td>External whole-body radiation; internal irradiation of thyroid; high toxicity</td>
</tr>
<tr>
<td>$^{89}$Sr</td>
<td>54 y</td>
<td>Moderately volatile</td>
<td>Bones and lungs</td>
</tr>
<tr>
<td>$^{106}$Ru</td>
<td>1 y</td>
<td>Highly volatile</td>
<td>Kidneys</td>
</tr>
<tr>
<td>$^{137}$Cs</td>
<td>33 y</td>
<td>Highly volatile</td>
<td>Internal hazard to whole body</td>
</tr>
</tbody>
</table>
DECAY HEAT

Image by MIT OpenCourseWare. Adapted from Todreas & Kazimi, *Nuclear Systems Volume I: Thermal Hydraulic Fundamentals*. 
THE FARMER LINE

[Graph showing frequency on a logarithmic scale against iodine-131 release magnitude (Curies).]

- **High risk** line with a slope of -1.
- **Low risk** line with a slope of -1.5.

Image by MIT OpenCourseWare.
KEEP FISSION PRODUCTS WITHIN THE FUEL

- Control Reactor Power
  - Control reactivity additions
  - Shutdown reliably
- Cool the Reactor and Spent Fuel
  - Maintain coolant inventory
  - Maintain coolant flow
  - Maintain coolant heat sinks

KEEP RADIOACTIVE MATERIAL OUT OF THE BIOSPHERE

- Maintain Containment Integrity
  - Prevent over-pressurization
  - Prevent over-heating
  - Prevent containment bypass
- Capture Material Within Containment
  - Scrubbing
  - Deposition
  - Chemical capture

SHIELD PERSONNEL FROM RADIATION
EMERGENCY SAFETY FUNCTIONS

PARR:
Removal of radioactivity from containment atmosphere.

CI:
Prevention of dispersal of radioactivity to environment.

RT:
Rapid shutdown of reactor to limit core heat production.

PAHR:
Removal of heat from containment to prevent overpressurization.

Sprays or filters collect radioactivity from containment atmosphere.
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 \times 10^{-5}, once every 20,000 years; upper bound: 3 \times 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)

• “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.”
NPP: END STATES

- Various states of degradation of the reactor core.
- Release of radioactivity from the containment.
- Individual risk.
- Numbers of early and latent deaths.
- Number of injuries.
- Land contamination.
NPP: INITIATING EVENTS

- Transients
  - Loss of offsite power
  - Turbine trip
  - Others
- Loss-of-Coolant Accidents (LOCAs)
  - Small LOCA
  - Medium LOCA
  - Large LOCA
LOSS-OF-OFFSITE-POWER
EVENT TREE

- LOOP
- Secondary Heat Removal
- Bleed & Feed
- Recirc.
- Core

- OK
- OK
- PDSi
- PDSj
<table>
<thead>
<tr>
<th>LOSP</th>
<th>DGs</th>
<th>LOCA</th>
<th>EFW</th>
<th>EP Rec.</th>
<th>Cont.</th>
<th>END STATE</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.07 per yr</td>
<td>0.993</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>success</td>
</tr>
<tr>
<td></td>
<td>0.007</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
<td>success</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>success</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>core melt</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>core melt</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>core melt w/ release</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>success</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>core melt</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>core melt</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>core melt w/ release</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>success</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>core melt</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>core melt</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>core melt w/ release</td>
</tr>
</tbody>
</table>

From: K. Kiper, MIT Lecture, 2006

Courtesy of K. Kiper. Used with permission.
PRA MODEL OVERVIEW AND SUBSIDIARY OBJECTIVES

Level I
PLANT MODEL
Results
Accident sequences leading to plant damage states

Level II
CONTAINMENT MODEL
Results
Containment failure/release sequences

Level III
SITE/CONSEQUENCE MODEL
Results
Public health effects

PLANT MODE
At-power Operation
Shutdown / Transition Evolutions

SCOPE
Internal Events
External Events

Uncertainties
Epistemic Uncertainties

- 5th: $0.005/yr$ (200 yr)
- Median: $0.040/yr$ (25 yr)
- Mean: $0.070/yr$ (14 yr)
- 95th: $0.200/yr$ (5 yr)

LOSP DISTRIBUTION

From: K. Kiper, MIT Lecture, 2006

Courtesy of K. Kiper. Used with permission.
OFFSITE POWER RECOVERY CURVES

From: K. Kiper, MIT Lecture, 2006

Courtesy of K. Kiper. Used with permission.
LOGIC SYMBOLS ("GATES")

Operation, OR

Meaning:
Event A occurs when either event B or C occurs

Operation, AND

Meaning:
Event A occurs when both events B and C occur

Venn Diagrams
CONSIDER SYSTEM MINIMAL CUT SETS A & B

\[
\text{Prob Failure} = \text{Prob}_A + \text{Prob}_B - [\text{Prob } (B/A) \text{ Prob}_A] \\
= \text{Prob}_A + \text{Prob}_B - (\text{Prob}_A \times \text{Prob}_B) \\
\text{if A & B are independent}
\]

For a Good System:
\[
\text{Prob}_A, \text{Prob}_B << 1 \text{ and } \text{Prob}_A \times \text{Prob}_B << \text{Prob}_A \text{ or } \text{Prob}_B, \text{ and} \\
\text{Prob Failure} \leq \text{Prob}_A + \text{Prob}_B \text{ (rare event approximation)}
\]
ILLUSTRATION OF ELEMENT OF FAULT TREE ELEMENTS

TOP EVENT

“OR” Gate

INTERMEDIA EVENT, A

“AND” Gate

A1
Basic Event A1

A2
Basic Event A2

INCOMPLETELY DEVELOPED EVENT, B

2
Transfer in from Sheet 2
AN EXAMPLE OF A PUMPING SYSTEM
FAULT TREE FOR THE FUEL PUMPING SYSTEM

FAILURE OF FUEL DELIVERY, T

LOSS OF TRAIN 1, F_1

LOSS OF TRAIN 2, F_2

MECHANICAL LOSS OF TRAIN 2, M_2

- Loss of Electricity, E_2
- Loss of Control, C_2
- Loss of Cooling, CO_2

MECHANICAL LOSS OF TRAIN 1, M_1

- Loss of Electricity, E_1
- Loss of Control, C_1
- Loss of Cooling, CO_1

T_1, P_1, V_1

T_2, P_2, V_2
FAULT TREE FOR THE FUEL PUMPING SYSTEM

FAILURE OF FUEL DELIVERY

E Fails

C Fails

CO Fails

Pumping Branches Fail Mechanically

Mechanical Loss of Train 1

T1 Fails to Supply Fuel

P1 Fails to Pump Fuel

V1 Fails Closed

Mechanical Loss of Train 2

T2 Fails to Supply Fuel

P2 Fails to Pump Fuel

V2 Fails Closed
CUT SET: A cut set is any set of failures of components and actions sufficient to cause system failure.

MINIMAL CUT SET: A minimal cut set is a set of failures necessary to cause system failure. A minimal cut set contains only a single cut set.
Any Binary Combination of an Element of

- \( T_1, \) Tank
- \( P_1, \) Pump
- \( V_1, \) Valve

Train 1

and of

- \( T_2, \) Tank
- \( P_2, \) Pump
- \( V_2, \) Valve

Train 2

C  Control System
E  Electric Power Source
CO  Cooling System

\{\text{Dependent Failure of Pumping Train 1 and 2}\}

Failure of Any Minimal Cut Set Will Result in System Failure
VENN DIAGRAM FOR FUEL SYSTEM SUPPLY FAILURE

E

C

CO

Train 1

Train 2

Trains 1 & 2
ILLUSTRATION OF DE-COMPOSITION OF TOP EVENT INTO A COMBINATION OF MINIMAL CUT SETS

\[ T = E_1 \diamond E_2 \]  (1)

\[ E_1 = E_1 + C_1 + CO_1 + M_1 \]  (2)

\[ E_2 = E_2 + C_2 + CO_2 + M_2 \]  (3)

\[ M_1 = T_1 + P_1 + V_1 \]  (4)

\[ M_2 = T_2 + P_2 + V_2 \]  (5)

\[ E_1 = E_1 + C_1 + CO_1 + (T_1 + P_1 + V_1) \]  (6)

\[ E_2 = E_2 + C_2 + CO_2 + (T_2 + P_2 + V_1) \]  (7)

NOTE:  \( E = E_1 = E_2, \ C = C_1 = C_2, \ CO = CO_1 = CO_2 \)
\[ T = [(E + C + CO) + (T_1 + P_1 + V_1)] \times [(E + C + CO) + (T_2 + P_2 + V_2)] \]
\[ = (E_1 + C_1 + CO_1) \times (E_2 + C_2 + CO_2) + (E_2 + C_2 + CO_2) \times [(T_1 + P_1 + V_1) + (T_2 + P_2 + V_2)] \]
\[ T = (E + C + CO) \{ 1 + [(T_1 + P_1 + V_1) + (T_2 + P_2 + V_2)] \} \]
\[ + (T_1 + P_1 + V_1) + (T_2 + P_2 + V_2) \]
\[ = \bigg( [T_1 \cdot T_2 + T_1 \cdot P_2 + T_1 \cdot V_2] \bigg) \]
\[ \bigg[ + P_1 \cdot T_2 + P_1 \cdot P_2 + P_1 \cdot V_2 \bigg] \]
\[ \bigg[ + V_1 \cdot T_2 + V_1 \cdot P_2 + V_1 \cdot V_2 \bigg] \]
\[ T = (E + C + CO) + \sum_{i=1}^{N} (MCS_i) \]
DATA SOURCES

- Generic Data Bases (those available are strongly safety-oriented; e.g., NPRDS/EPIX, NRC, GADS, . . .)

- Plant-Specific Data

- New Tests

- Subjective Judgment and Modeling
Consider a Set of $N$ Identical Components, Which are Tested Repeatedly Until Failure

\[ \text{Area} = \frac{N}{2} \]

\[ \langle T \rangle = \int_0^\infty T f(T) \, dT : \text{Mean} \]
UNCERTAINTY

• FACTORS OF UNCERTAINTY
  - Randomness
  - Phenomenological Ignorance
  - Systematic Ignorance (complexity, Sensitivity)
  - Data Ignorance

• IMPORTANT UNCERTAIN PHENOMENA
  - Common Cause Failures
    - Internal
    - External
  - Rare Events (e.g., Reactor Core Melt Progression)

• TREATMENT OF UNCERTAINTY
  - Statistical (via Standard Deviation)
  - Sensitivity Analyses
  - Subjective Probability Elicitation
  - Research and Data Collection
  - Assignment of Bias
# TYPES OF COMMON CAUSE FAILURES AND THEIR ASPECTS

<table>
<thead>
<tr>
<th>Description of Failure Cause</th>
<th>DEPENDENT</th>
<th>STRUCTURAL*</th>
<th>ENVIRONMENTAL</th>
<th>EXTERNAL*</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Hardware Examples</strong></td>
<td>Failure of an interfacing system, action or component</td>
<td>A common material or design flaw which simultaneously affects all components population</td>
<td>A change in the operational environment which affects all members of a component population simultaneously</td>
<td>An event originating outside the system which affects all members of a component population simultaneously</td>
</tr>
<tr>
<td><strong>Human Examples</strong></td>
<td>Following a mistaken leader</td>
<td>Incorrect training</td>
<td>Common cause psf's</td>
<td>Explosion</td>
</tr>
<tr>
<td></td>
<td>An erroneous maintenance procedure is repeated for all components of a given class</td>
<td>Poor management</td>
<td>New disease</td>
<td>Toxic substance</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Poor motivation</td>
<td>Hunger</td>
<td>Weather</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Low pay</td>
<td>Fear</td>
<td>Earthquake</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Noise</td>
<td>\</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Radiation in control room</td>
<td>Concern for families</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Easy to Anticipate?</th>
<th>Component failure</th>
<th>Human error</th>
<th>Component failure</th>
<th>Human error</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>High</td>
<td>Medium</td>
<td>Very Low</td>
<td>Medium</td>
</tr>
<tr>
<td></td>
<td>Medium</td>
<td>Medium</td>
<td>Medium</td>
<td>Medium</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Easy to Mitigate?</th>
<th>Component failure</th>
<th>Human error</th>
<th>Component failure</th>
<th>Human error</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>High, if system designed for mitigation</td>
<td>High, if feedback provided to identify the error promptly</td>
<td>Very Low, hard to design for mitigation</td>
<td>Very Low, the factors making CCF likely also discourage being prepared for correction</td>
</tr>
<tr>
<td></td>
<td>Very Low</td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
</tr>
</tbody>
</table>

* Usually there are no precursors
PRA MODEL OVERVIEW AND SUBSIDIARY OBJECTIVES

Level I

PLANT MODEL

Results
Accident sequences leading to plant damage states

Level II

CONTAINMENT MODEL

Results
Containment failure/release sequences

CDF 10^{-4}/ry
LERF 10^{-5}/ry

Level III

SITE/CONSEQUENCE MODEL

Results
Public health effects

PLANT MODE
At-power Operation
Shutdown / Transition Evolutions

SCOPE
Internal Events
External Events

QHOs

Uncertainties
RISK MODEL OVERVIEW

RISK MODEL

PLANT MODEL

SECTION 3

CONTAINMENT MODEL

SECTION 4

SITE MODEL

(Not Included)

LEVEL I
RESULTS
Core Melt Sequences
Section 3.4.1.1

LEVEL II
RESULTS
Containment Failure/
Release Sequences
Section 3.4.1.2

LEVEL III
RESULTS
Public Health Effects
(Not Included)
INTEGRATED LEVEL 3 PRA FRAMEWORK

FRONT-END ANALYSIS

LEVEL 1

INTERNAL EVENTS
CORE DAMAGE
FREQUENCY
ANALYSIS

• EVENT TREES
• FAULT TREES
• FAILURE DATA
• FREQUENCIES

EXTERNAL EVENT
CORE DAMAGE
FREQUENCY
ANALYSIS

• RESOLUTION OF CORE VULNERABLE
SEQUENCES
• PLANT DAMAGE STATE DEFINITION

BACK-END ANALYSIS

LEVEL 2

ACCIDENT
PROGRESSION
EVENT TREE
ANALYSIS

• PLANT
DAMAGE
STATE
FREQUENCIES
• FRONT-END
UNCERTAINTY
ISSUES

SOURCE
TEHM
ANALYSIS

• ACCIDENT
PROGRESSION
BIN
FREQUENCIES
• CONTAINMENT
UNCERTAINTY
ISSUES

CONSEQUENCE
ANALYSIS

• SOURCE
TERM
GROUPS
• SOURCE
TERM
ISSUES

LEVEL 3

EXTERNAL EVENT
CORE DAMAGE
FREQUENCY
ANALYSIS

HISK

• SOURCE
TERM
GROUP
DEFINITION

• FREQUENCY
OF HEALTH &
ECONOMIC
CONSEQUENCES
Contributions to Core Damage Frequency
Accidents Grouped by Initiating Event

- Transients: 83%
  - Loss of Support Systems: 39%
  - General Transient: 19%
  - LOCA: 8%
  - ATWS: 9%
  - LOCX: 25%
CONTRIBUTIONS TO CORE DAMAGE FREQUENCY
Accidents Grouped by Internal and External Initiating Event

INTERNAL EVENTS
55%

EXTERNAL EVENTS
45%

- Fire: 24%
- Seismic: 13%
- Flood: 5%
- Other: 3%
CONTAINMENT PERFORMANCE RESULTS
(Conditional Failure Probability Given Core Damage)

- Late Containment Failure ** 65.4%
- Early, Large Containment Failure/Bypass* 0.2%
- Early, Small Containment Failure/Bypass 14.2%
- Intact Containment 20.2%

* Equivalent to "unusually poor" containment performance, as defined in GL 88-20

**The containment failure probability of late containment failure is believed to be overestimated relative to containment intact. No credit has been taken for post-core melt recovery actions.
CONTAINMENT FAILURE MODE CONTRIBUTIONS TO EARLY, LARGE CONTAINMENT FAILURES/BYPASS ("Unusually Poor" Containment Performance)

- Containment Isolation Failure: 58.7%
- Direct Containment Heating: 26.8%
- Induced Steam Generator Tube Rupture: 11.1%
- Other: 1.3%
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 $5 \times 10^{-7}$/year for early death and $2 \times 10^{-6}$/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: 7x10^-5
  - Coal Mining: 24x10^-5
  - Fire Fighting: 40x10^-5
  - Police: 32x10^-5
  - US President: 1,900x10^{-5} (!)

• Annual Public Risks
  - Total: 870x10^{-5}
  - Heart Disease: 271x10^{-5}
  - All cancers: 200x10^{-5}
  - Motor vehicles: 15x10^{-5}

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)
“ACCEPTABLE” VS. “TOLERABLE” RISKS (UKHSE)

Risk cannot be justified save in extraordinary circumstances

Control measures must be introduced for risk in this region to drive residual risk towards the broadly acceptable region

Level of residual risk regarded as insignificant -- further effort to reduce risk not likely to be required

“ACCEPTABLE” VS. “TOLERABLE” RISKS (UKHSE)

Adapted from "The tolerability of risk from nuclear power stations", Health Safety Executive.
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)

Comply with Regulations

Maintain Defense-in-Depth Philosophy

Maintain Safety Margins

Integrated Decision Making

Risk Decrease, Neutral, or Small Increase

Monitor Performance
ACCEPTANCE GUIDELINES FOR CORE DAMAGE FREQUENCY

- Region I
  - No changes
- Region II
  - Small Changes
  - Track Cumulative Impacts
- Region III
  - Very Small Changes
  - More flexibility with respect to Baseline
  - Track Cumulative Impacts
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
- Rationalist Defense in Depth
- Incomplete
- Quality is an issue
RISK IMPORTANCE MEASURES

Risk = R(q_1, q_2, \ldots, q_n),

where

\[ r_i = \text{reliability of the } i^{th} \text{ plant component, action, or cut set} \]

\[ q_i = \text{unreliability of the } i^{th} \text{ component} = 1 - r_i \]

\[ I_{Fussell-Vesely_i} = \text{the fraction of total risk involving failure of element, } i \]

\[ I_{Fussell-Vesely_i} = \frac{R(q_i)}{R_{Nom}} = \frac{R(mcs_{i_1} + mcs_{i_2} + \cdots + mcs_{i_m})}{R(mcs_1 + \cdots + mcs_n)} \]

where

\[ R(q_i) = \text{risk arising from event sequences involving failure of component, action or cut set, } i \]

\[ R_{Nom} = \text{nominal plant risk} \]

\[ m = \text{number of minimal cut sets involving element (basic event) } i \]

\[ n = \text{total number of minimal cut sets} \]
Risk Achievement Worth (RAW$_i$) Maximum relative possible increase in total risk due to failure of element, i; the element is assumed always to fail.

\[
\text{RAW}_i = \frac{R(q_i = 1)}{R_{\text{Nom}}}
\]

where

RAW$_i$ = the risk achievement worth of the i$^{th}$ component, action or cut set
COMPONENT RISK IMPORTANCE

(Average of NUREG-1150 Surry and Sequoyah results)

Number of components

Increase in core damage frequency if component always failed

Image by MIT OpenCourseWare. Adapted from F. Gillespie, MIT Reactor Safety Course, 1993.
Risk Reduction Worth (RRW_i) = Maximum possible relative reduction in risk due to perfection of event i reliability; the component is assumed always to succeed every time.

\[
RRW_i = \frac{R_{\text{Nom}}}{R(q_i = 0)},
\]

where

RRW_i = the relative risk decrease importance of the i^{th} component, action or cut set
CORE DAMAGE FREQUENCY
PERCENT INCREASE PER SYSTEM 1

CDF Breakdown by Doubling System Unavailability
(Including contributions from maintenance)

Risk Increase [% CDF (Per Year)]

- ESW
- 12AVDC
- SRV
- EDG
- RHR/LPCI/ESF
- VENTING
- HPCI
- 115KV
- RCIC
- 600VAC
- RPS

Image by MIT OpenCourseWare.
USES OF RISK IMPORTANCE MEASURES

• Fussell-Vesely
  ■ Measure a Component’s or System’s Participation in Risks
  ■ Can Be Used to Identify Which Components or Systems Contribute to Current Risks

• Risk Achievement Worth
  ■ Identifies Which Components or Systems Must Be Kept Reliable

• Risk Reduction Worth
  ■ Identifies Which Components or Systems Are Most Valuable for Improvement
  ■ Note

\[ I_{\text{Fussell-Vesely}_i} = 1 - \frac{1}{\text{RRW}_i} \]
## SYSTEM COMPONENT COST AND RELIABILITY DATA

<table>
<thead>
<tr>
<th>Component</th>
<th>Component Failure Probability</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tank, T-1 or T-2</td>
<td>3.00E-5</td>
</tr>
<tr>
<td>Valve, V-1 or V-2</td>
<td>1.20E-4</td>
</tr>
<tr>
<td>Pump, P-1 or P-2</td>
<td>9.00E-5</td>
</tr>
<tr>
<td>Electric Power, E</td>
<td>1.50E-4</td>
</tr>
<tr>
<td>Control System, C</td>
<td>3.00E-4</td>
</tr>
<tr>
<td>Cooling System, CO</td>
<td>1.00E-4</td>
</tr>
</tbody>
</table>
## SUMMARY OF IMPORTANCE RANKINGS

<table>
<thead>
<tr>
<th>Component / or System</th>
<th>Control System, C</th>
<th>Electric Power System, E</th>
<th>Valve, V-1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Importance Measures</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fussell-Vesely</td>
<td>0.54</td>
<td>0.27</td>
<td>5x10^{-5}</td>
</tr>
<tr>
<td>Risk Reduction Worth</td>
<td>2.18</td>
<td>1.37</td>
<td>1.00005</td>
</tr>
<tr>
<td>Risk Achievement Worth</td>
<td>1819</td>
<td>1819</td>
<td>1.44</td>
</tr>
</tbody>
</table>
TIMELINE FOR NUCLEAR WASTE DISPOSAL

- **1957**: National Academy of Sciences (NAS) supported deep geologic disposal
- **1982**: Congress passes Nuclear Waste Policy Act
- **1987**: Congress limited characterization to Yucca Mountain
- **1992**: Energy Policy Act sets Environmental Protection Agency (EPA) standard process
- **2002**: President recommended and Congress approved Yucca Mountain
- **2008**: DOE scheduled to submit License Application
- **2017**: DOE scheduled to begin receipt of spent nuclear fuel and high-level radioactive waste

Image by MIT OpenCourseWare.
* Counties designated as affected units of local government

- 100 miles northwest of Las Vegas in Nye County
- Located on Western boundary of the Nevada Test Site, a U.S. Department of Energy (DOE) facility

Image by MIT OpenCourseWare.
YUCCA MOUNTAIN
SUBSURFACE OVERVIEW

South Portal
North Portal
Repository Level
Surface
Water Table
1,000 Feet

Transporting Containers by Rail
Remote Control Locomotive
Access Tunnel
Permanent Waste Packages
Mechanical Support Inner Barrier
Protective Outer Barrier
Various Permanent Waste Packages

HYPOTHETICAL SCENARIOS

- Volcanism
- Seismic

- Nominal
- Early defects

YUCCA MOUNTAIN: PREDICTED AVERAGE ANNUAL DOSE FOR 10,000 YEARS

Fig. F-17 in Draft Supplemental Environmental Impact Statement for a Geologic Repository at Yucca Mountain. U.S. Department of Energy, October 2007, DOE/EIS-0250F-S1D.
Fig. F-17 in Draft Supplemental Environmental Impact Statement for a Geologic Repository at Yucca Mountain. U.S. Department of Energy, October 2007, DOE/EIS-0250F-S1D.