2nd International Week on Risk Analysis
as Applied to Dam Safety and Dam Security
Theoretical-Practical Course
Universidad Politecnica de Valencia
Valencia, Spain
27 & 28 February 2008

RAC
Engineers & Economists

Utah State University
IDSRM

Risk Analysis as Applied to Dam Safety Fundamentals:

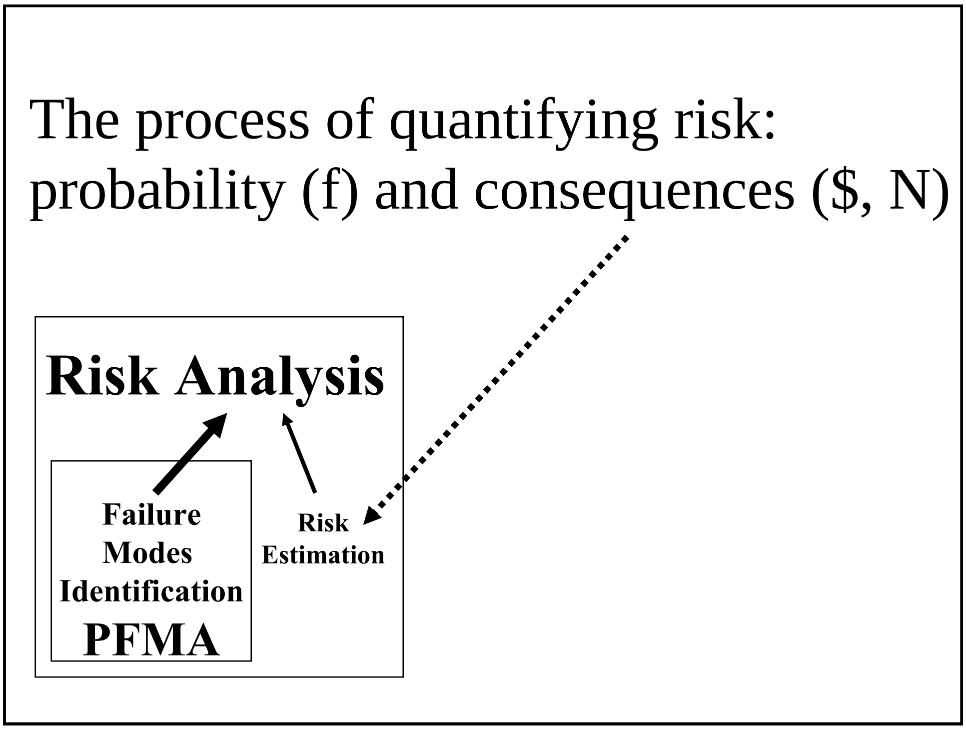
L.3 - Risk Model for an Existing Dam

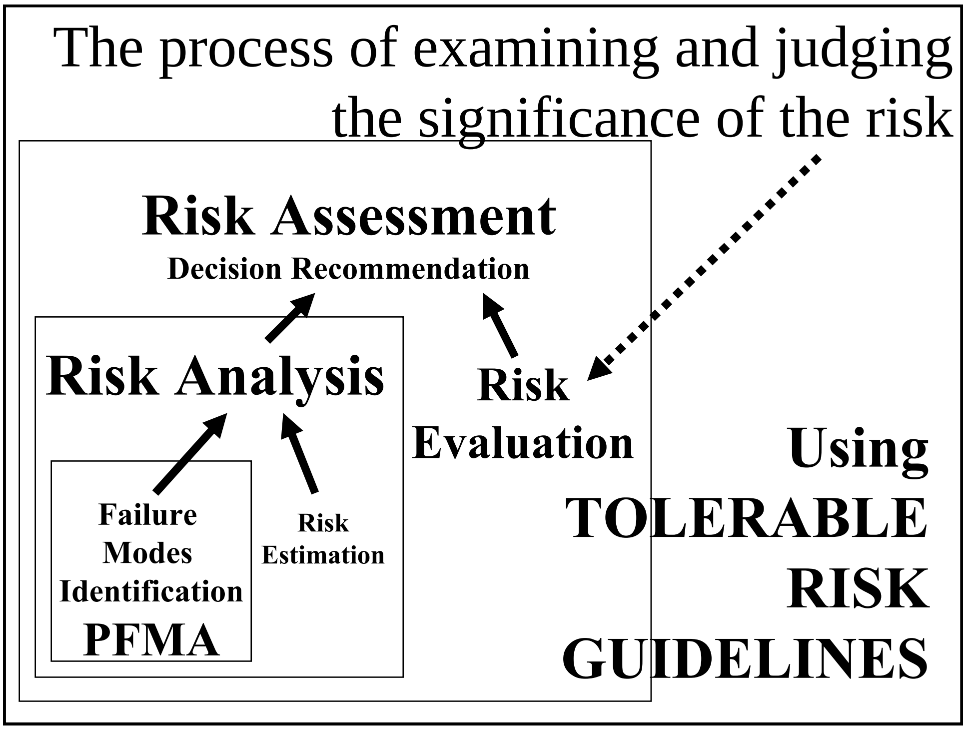
David S. Bowles
Institute for Dam Safety Risk Management - Utah State University
and RAC Engineers & Economists

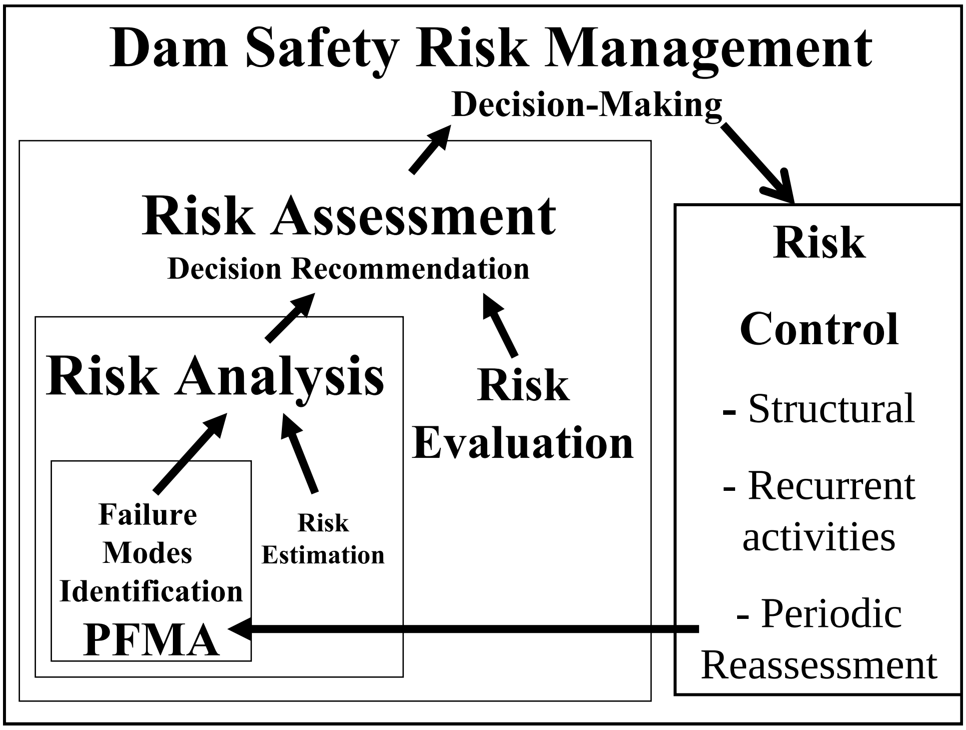
The process of determining a) what can go wrong, why and how, *and b) its consequences*

FOUNDATION for RA

Failure Modes Identification
PFMA


The process of quantifying risk:
probability (f) and consequences ($, N)
Risk Analysis
Failure
Modes
Identification
PFMA
Risk
Estimation


The process of examining and judging
the significance of the risk
Risk Assessment
Decision Recommendation
Risk Analysis
Failure
Modes
Identification
PFMA
Risk
Estimation
Risk
Evaluation
Using
TOLERABLE
RISK
GUIDELINES

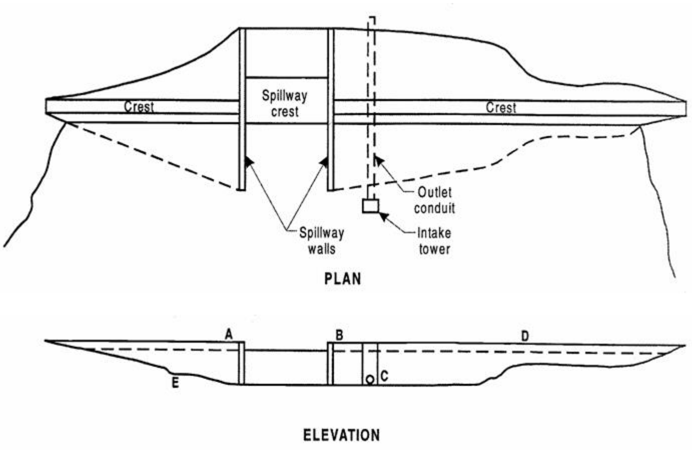


Risk Assessment Framework

	INITIATING EVENT	SYSTEM RESPONSE	OUTCOME (BREACH/ NO BREACH)	EXPOSURE	CONSEQUENCE
RISK IDENTIFICATION	External Earthquake Upstream Dam Failure Internal Piping	Overtopping Deformation Slope Instability	Breach No Breach	Time of Day Season Warning Time	Economic Damage Loss of Life Environmental Social

FERC now requires Potential Failure Modes Analysis

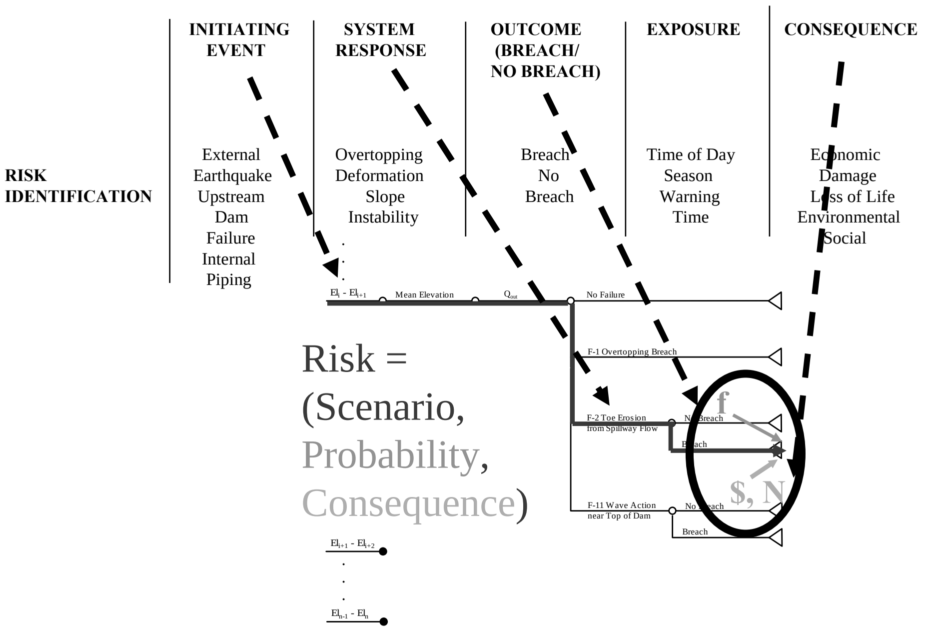
Typical Embankment Dam Showing Potential Piping Failure Paths



LEGEND:

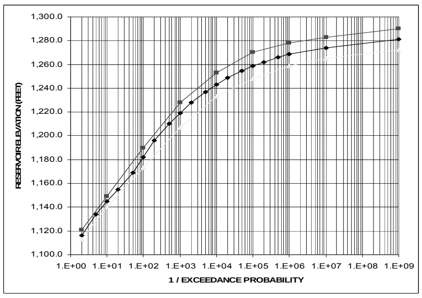
- A, B Adjacent spillway walls.
- C Adjacent outlet conduit.
- D,E Related to irregularities in the foundation profile.
- F In the foundation
- G From embankment to foundation

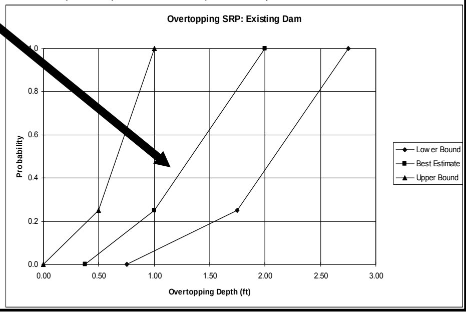
Risk Assessment Framework



Risk Assessment Framework

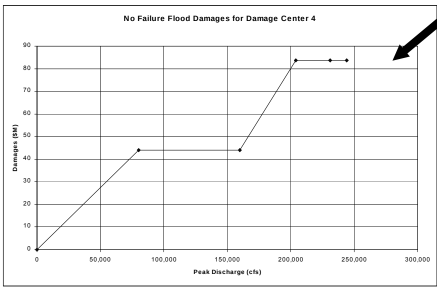
	INITIATING EVENT	SYSTEM RESPONSE	OUTCOME (BREACH/ NO BREACH)	EXPOSURE	CONSEQUENCE
RISK IDENTIFICATION	External: Earthquake Upstream Dam Failure Internal: Piping	Overtopping Deformation Slope Instability	Breach No Breach	Time of Day Season Warning Time	Economic Damage Loss of Life Environmental Social
RISK ESTIMATION	Loading Prob (E) →	Response Prob (R/E) →	Outcome Prob (O,E,R) →	Exposure Prob (L/E,R,O) →	Losses



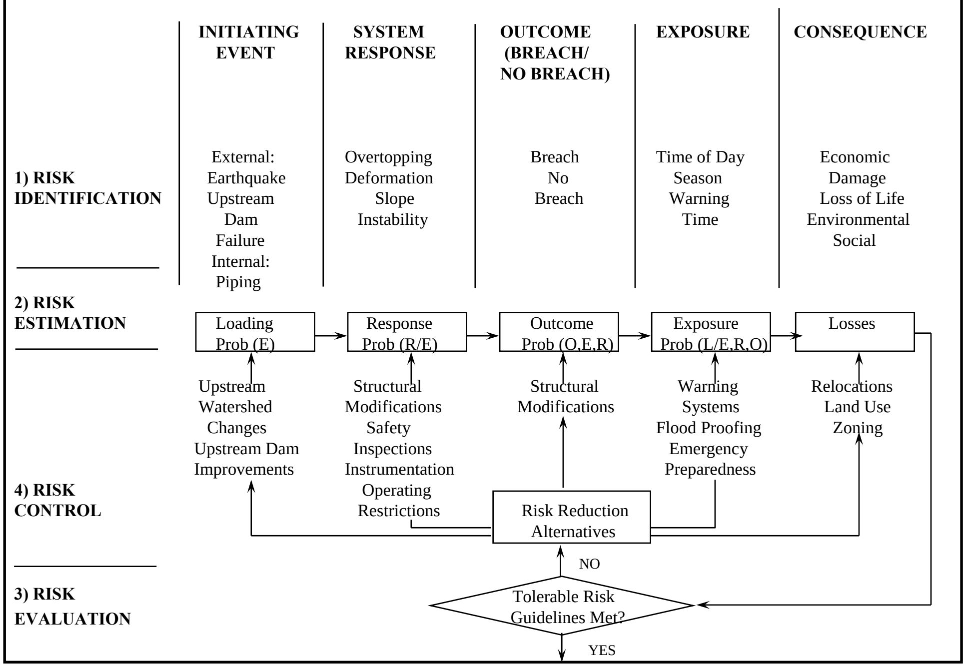


Risk Assessment Framework

	INITIATING EVENT	SYSTEM RESPONSE	OUTCOME (BREACH/ NO BREACH)	EXPOSURE	CONSEQUENCE
RISK IDENTIFICATION	External: Earthquake Upstream Dam Failure Internal: Piping	Overtopping Deformation Slope Instability	Breach No Breach	Time of Day Season Warning Time	Economic Damage Loss of Life Environmental Social
RISK ESTIMATION	Loading Prob (E) →	Response Prob (R/E) →	Outcome Prob (O,E,R) →	Exposure Prob (L/E,R,O) →	Losses



Risk Assessment Framework

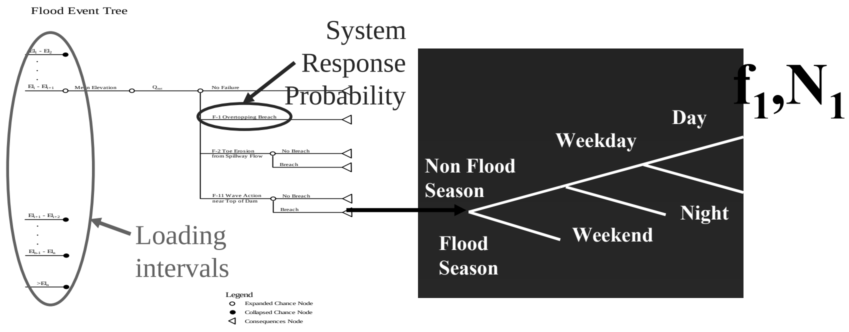


Outline

1) General Principles of Event Trees
2) Pathway Probability
3) Total Probability of Failure
4) Probability of Consequences
5) Probability-Consequence pairs
6) Annualized Consequences
7) Common Cause Failure Modes

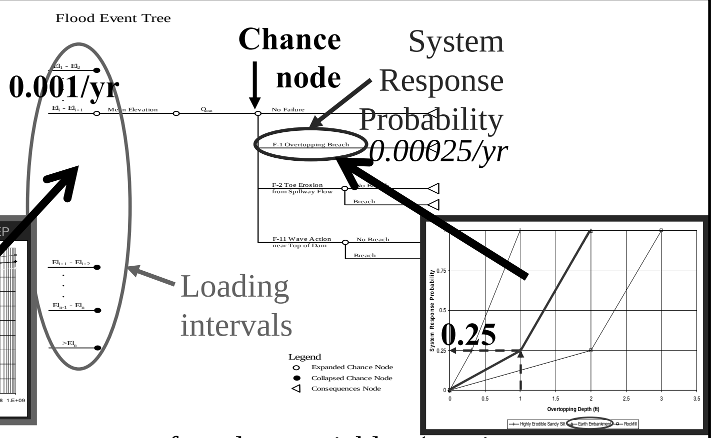
1) General Principles of Event Trees

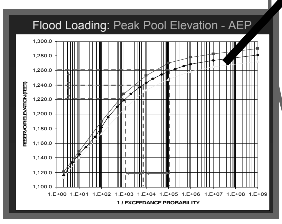
Event Tree Components



- Tree structure
- Begins with a single branch on the left side
  - initiating event
- Branches at various nodes
- Terminal branches on the far right side
  - Consequences are associated with terminal nodes

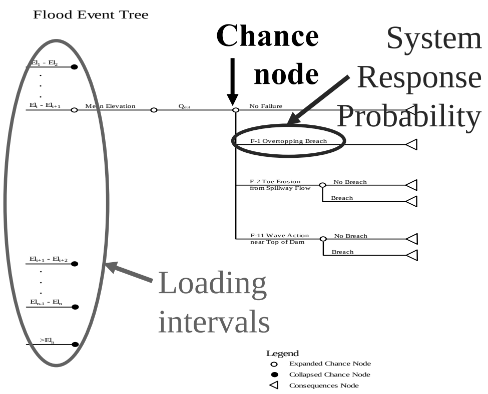
Definitions





- **Event tree** - a sequence of random variables (continuous or discrete) or event sets that can be associated with random variables
- **Chance node** - a branching point at which a new (random) variable is introduced in the tree
- **Branch probability** - probability of the event (branch) conditioned on occurrence of those events that precede it (to left) in the tree

Branches & Nodes



- Each branch represents an event (state of nature)
- At each (chance) node
  - number of branches represents all possible results from the precursor event sequence (collectively exhaustive)
  - the likelihood that any one of the succeeding events will occur, is governed by chance, and is conditioned on branches to the left
- Often a chronological sequence, but NOT essential
- IS essential that occurrence of any event (branch) is conditioned ONLY on events to the left

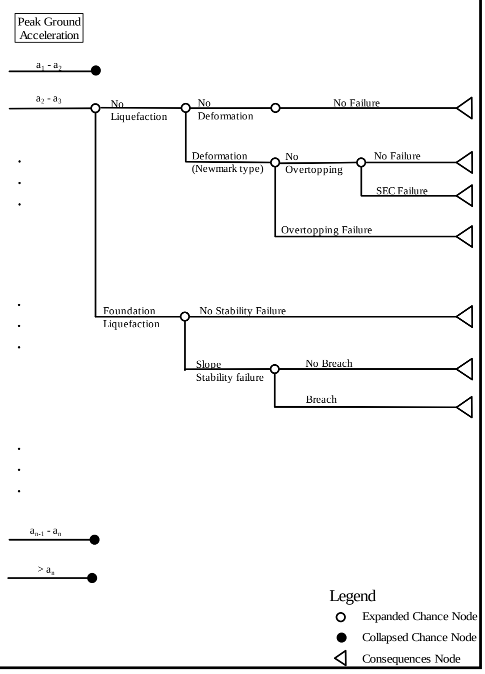
Application of Event Trees

- Separate trees for each type of initiating event:
  - e.g. Floods & Earthquakes
  - Independent & additive ($f_{Total} = f_{Flood} + f_{Earthquake}$)
- Branches at chance nodes can represent
  - System responses of the dam system to event sequences
  - Human actions and interventions - timeliness and effectiveness
  - Emergency response and factors affecting survival in flooding
  - Continuously operating or standby systems

Earthquake Event Tree

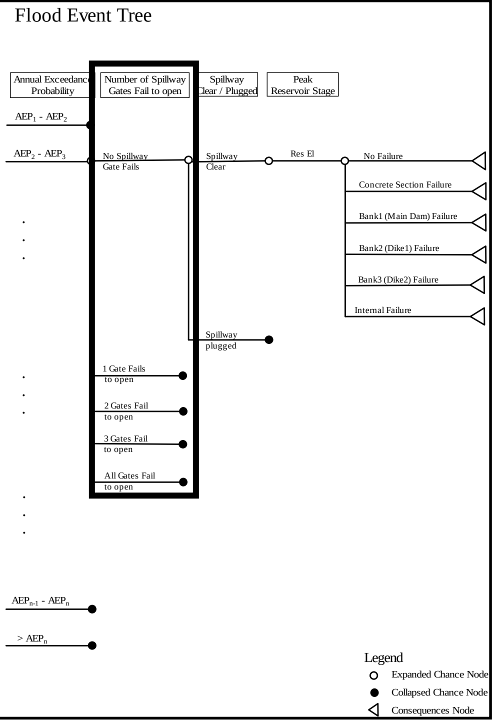
- Excessive "Newmark type" deformation
  - Sudden overtopping failure
  - Delayed seepage through cracks (SEC) failure
- Liquefaction induced instability

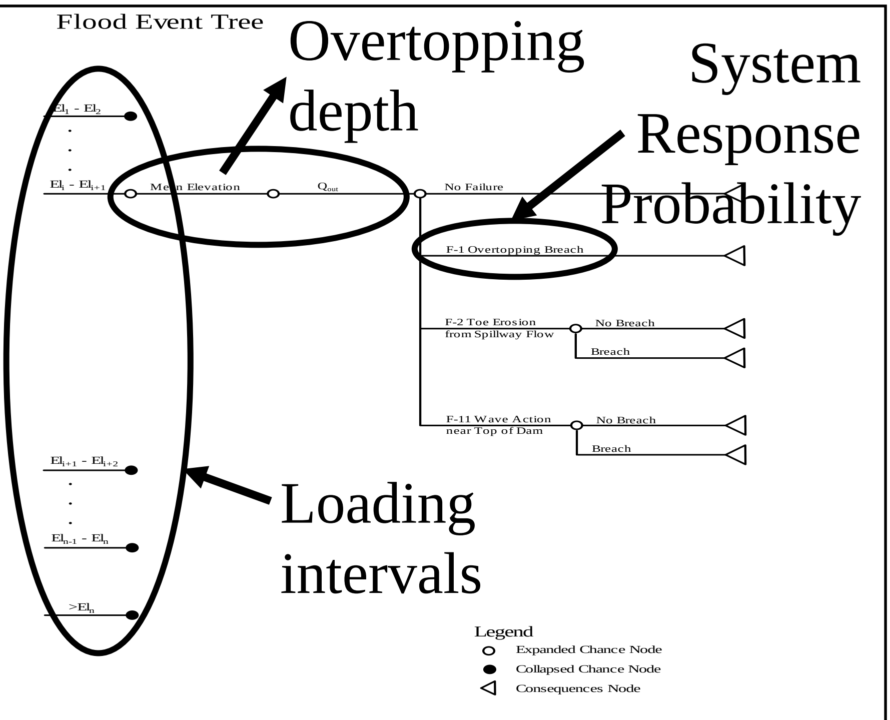
Earthquake Event Tree

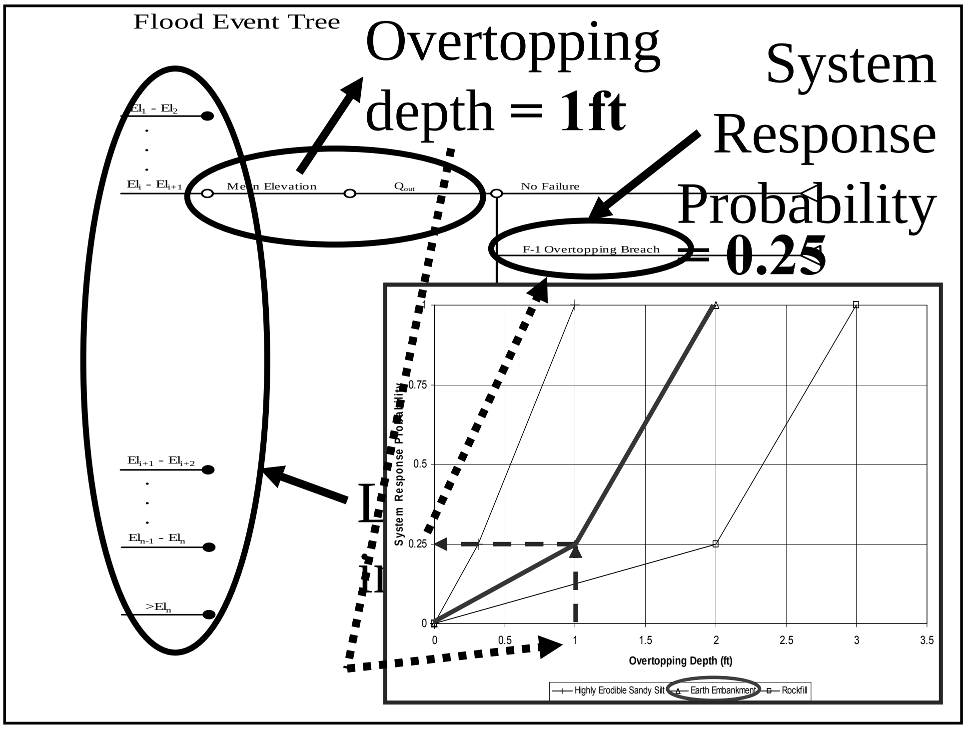


Flood Event Tree

- Embankment Failure Modes
  - Overtopping – main dam or dikes
  - Piping
  - Slope stability
- Concrete Section Failure Modes
  - Foundation scour
  - Overstress
  - Instability
- Gate failure cases
  - Combinations of individual gates
  - Common cause failure of all gates
- Spillway plugging by debris
- Consequences
  - Life loss
  - Economic damages



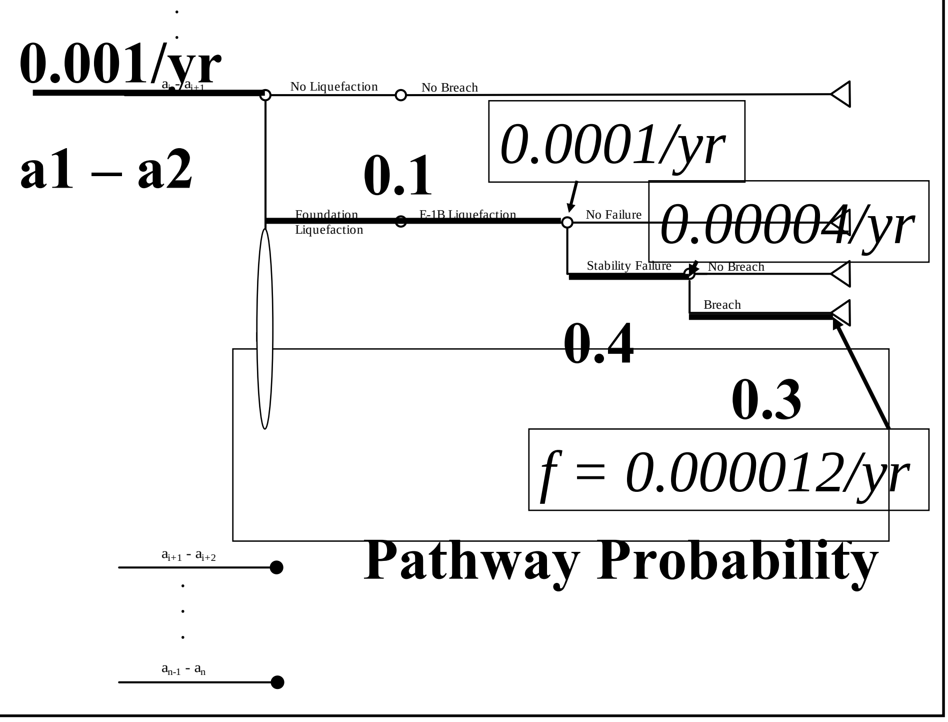




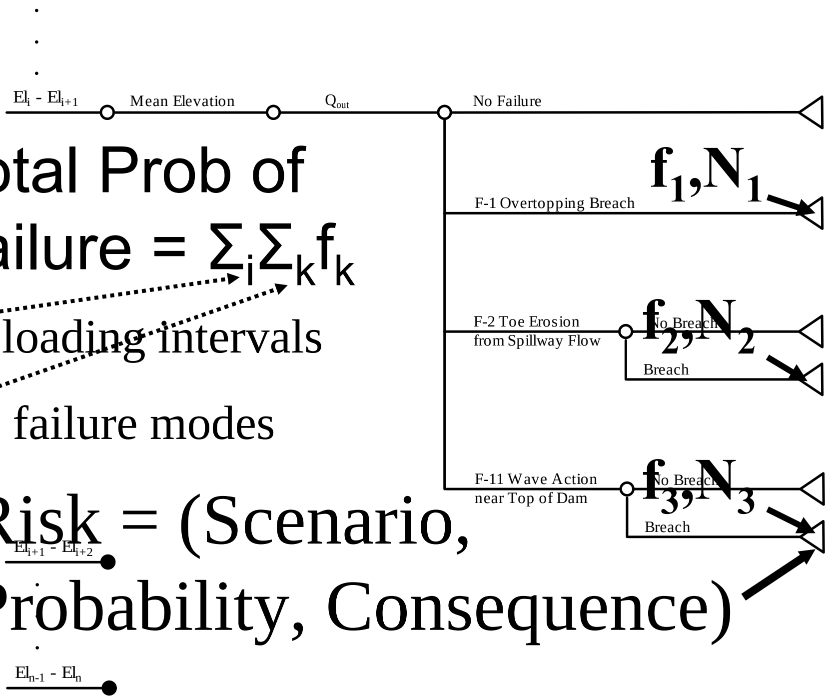
Event Tree Calculations – Loading Interval Size

- Adjust to control numerical errors
- Event tree for representative interval
  - Protocols to assign probabilities and consequences
- Risk reduction alternatives
  - Same step size as for existing dam

2) Pathway Probability



3) Total Probability of Failure



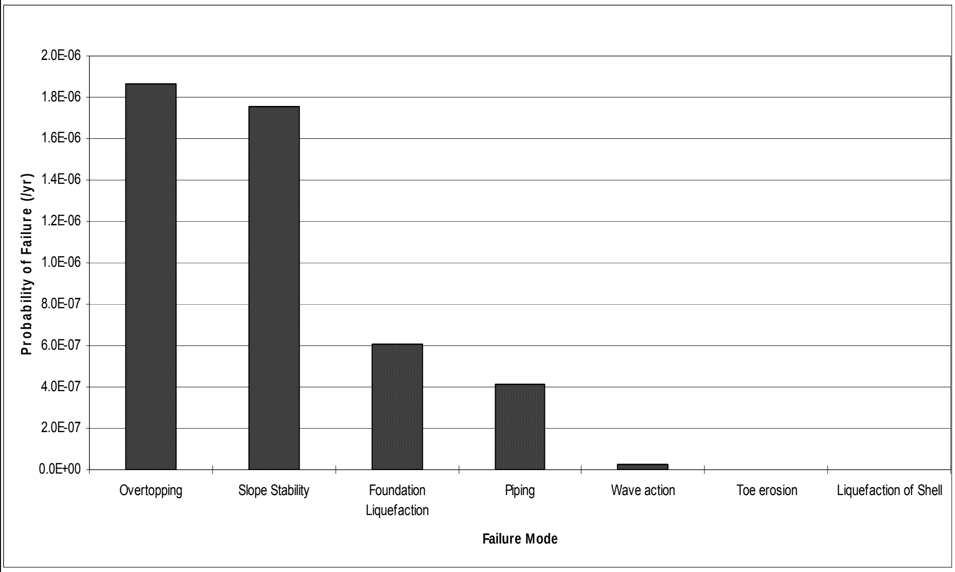
Total Prob of Failure = $\Sigma_i \Sigma_k f_k$

i = loading intervals

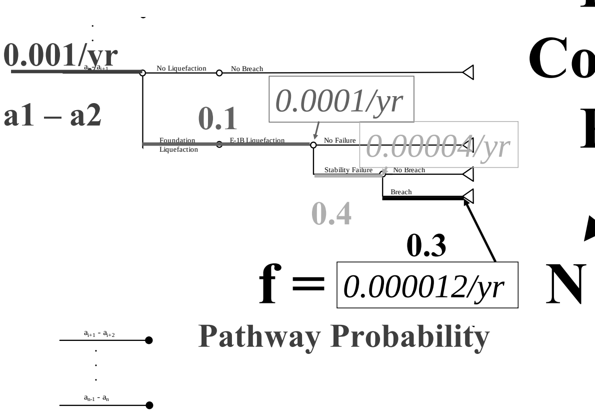
k = failure modes

Risk = (Scenario, Probability, Consequence)

Failure Probability vs. Failure Mode



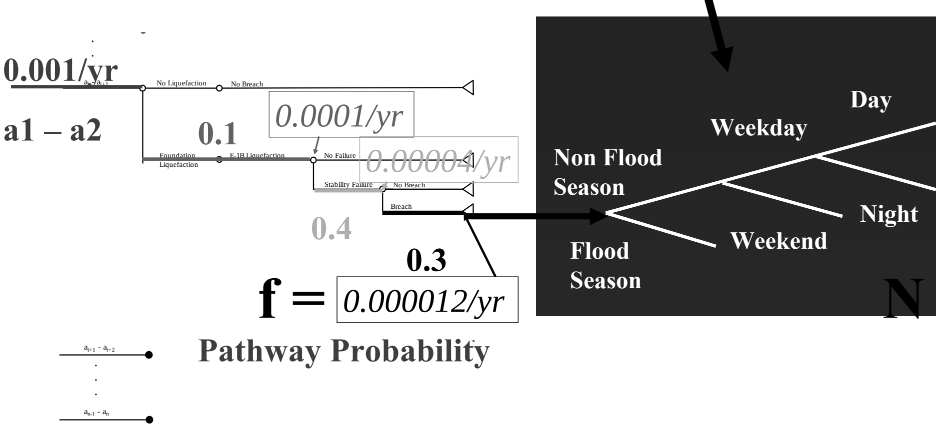
3) Probability of Consequences



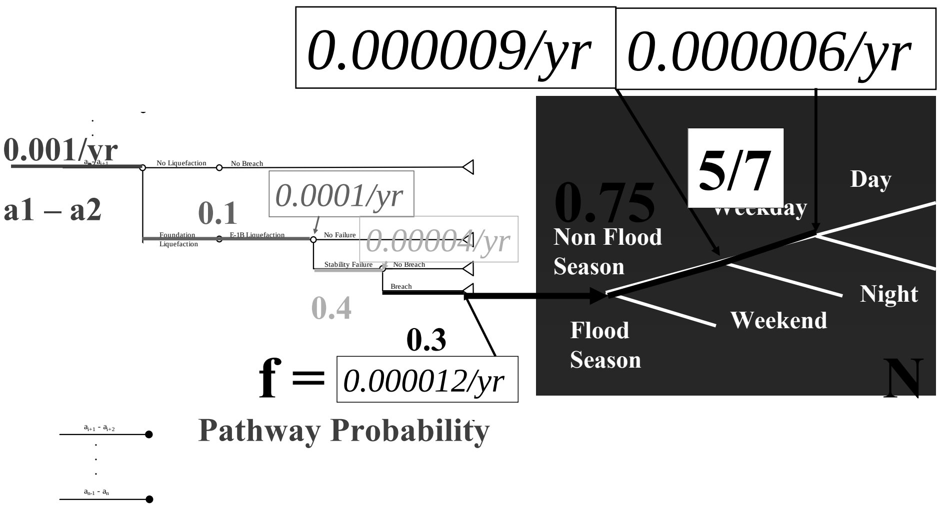
Probability of Consequences ≠ Probability of Failure

Exposure Sub Tree

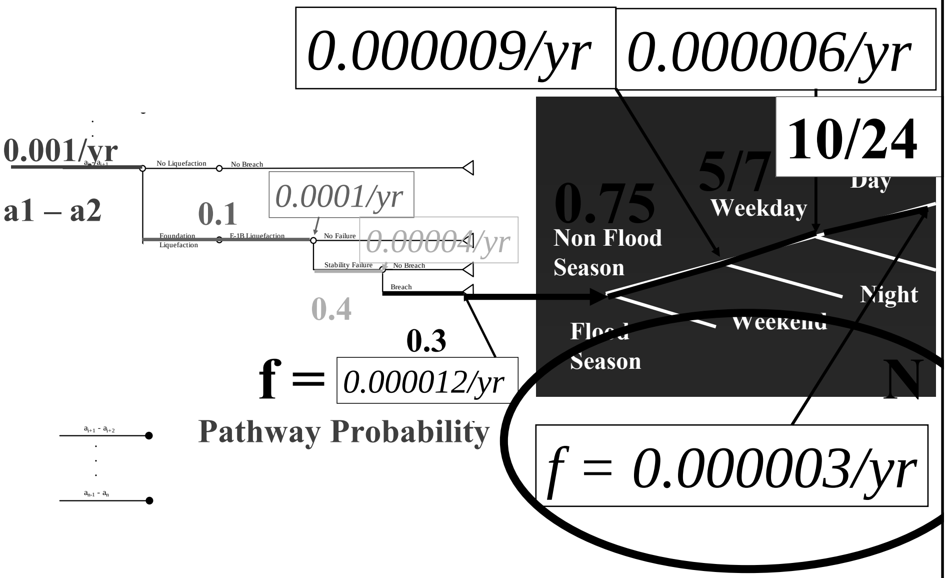
– Appended to Engineering Event Tree



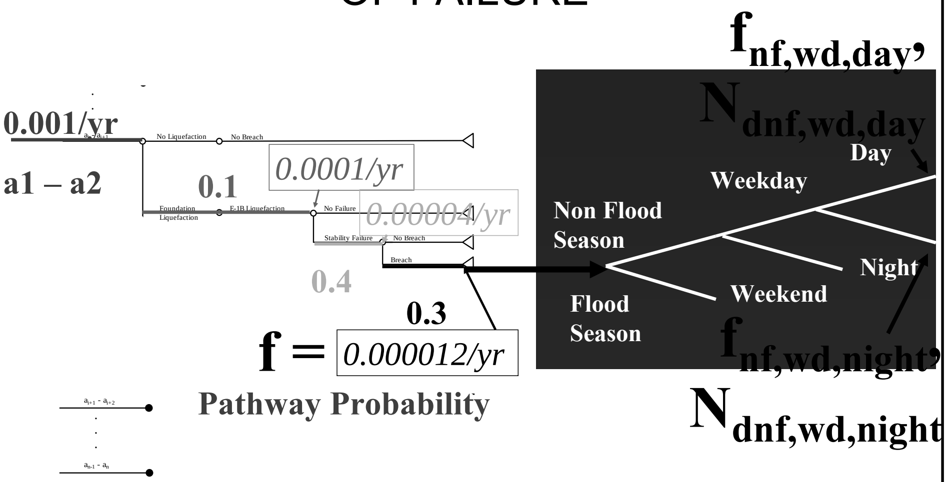
Probability of Consequences



Probability of Consequences

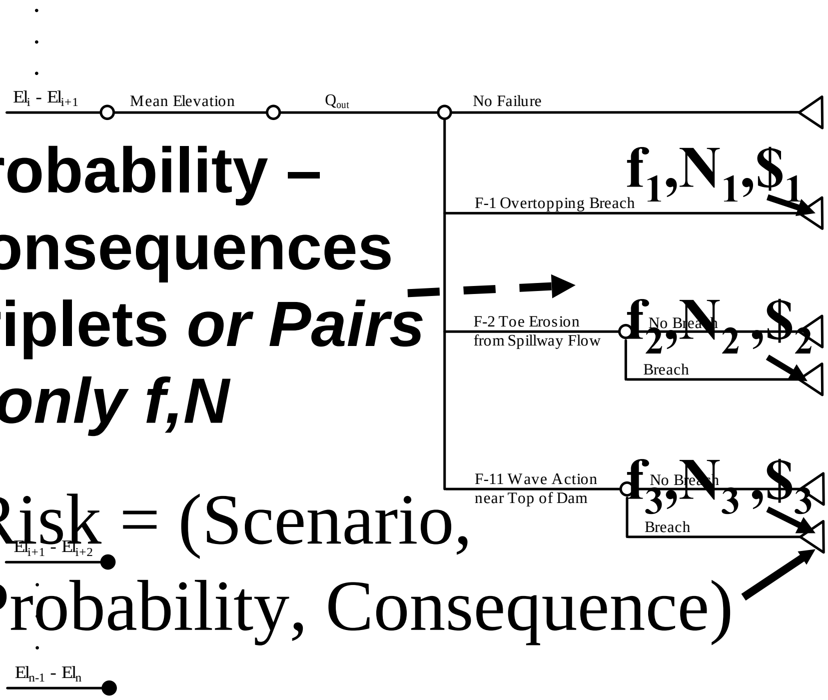


Probability of Consequences
NOT THE SAME AS PROBABILITY OF FAILURE



5) Probability- Consequences Pairs

Probability – Consequences Triplets *or Pairs if only f,N*



Risk = (Scenario, Probability, Consequence)

5) Annualized Consequences

“Risk = Probability * Consequences”

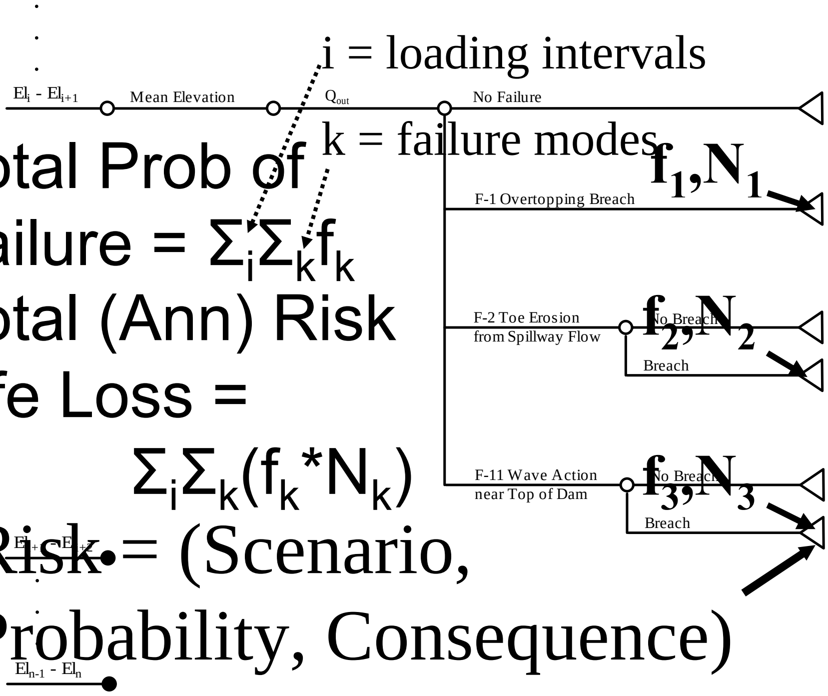
$$= \Sigma f * N$$

Special Case

– Annual Average or Annualized Consequences

Risk Cost, $/year

Lives/year



i = loading intervals

k = failure modes

Total Prob of Failure = $\Sigma_i \Sigma_k f_k$

Total (Ann) Risk Life Loss = $\Sigma_i \Sigma_k (f_k * N_k)$

Risk = (Scenario, Probability, Consequence)

Annualized Life Loss

ANNUALIZED LIFE LOSS	=	LIFE LOSS PER *FAILURE* EVENT	X	PATHWAY PROBABILITY

<u>UNITS</u>

$\frac{\text{LIVES}}{\text{YEAR}}$	=	$\frac{\text{LIVES}}{\text{EVENT}}$	X	$\frac{\text{EVENTS}}{\text{YEAR}}$

<u>EXAMPLE</u>

10^{-2} LIVES/yr	=	10 LIVES	X	10^{-3}/yr

Risk Cost

$$\text{RISK COST} = \begin{matrix}\text{DAMAGE PER} \\ \textbf{FAILURE}\text{ EVENT}\end{matrix} \times \begin{matrix}\text{PATHWAY} \\ \text{PROBABILITY}\end{matrix}$$

UNITS

$$\frac{\$}{\text{YEAR}} = \frac{\$}{\text{EVENT}} \times \frac{\text{EVENTS}}{\text{YEAR}}$$

EXAMPLE

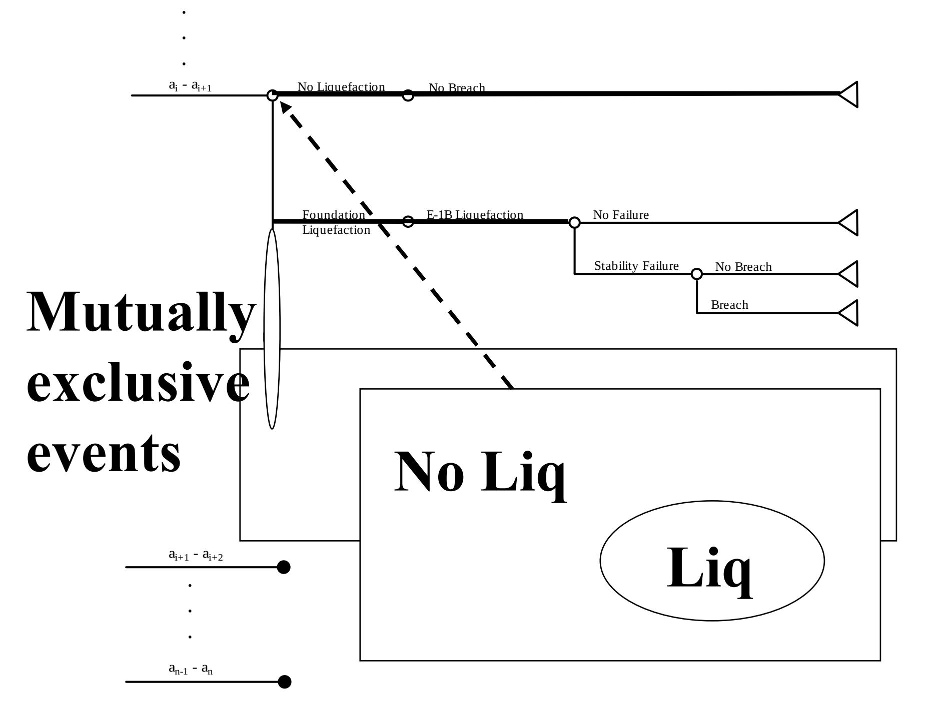
$$\$1{,}000/\text{yr} = \$1{,}000{,}000 \times 10^{-3}/\text{yr}$$

7) Common Cause Failure Modes

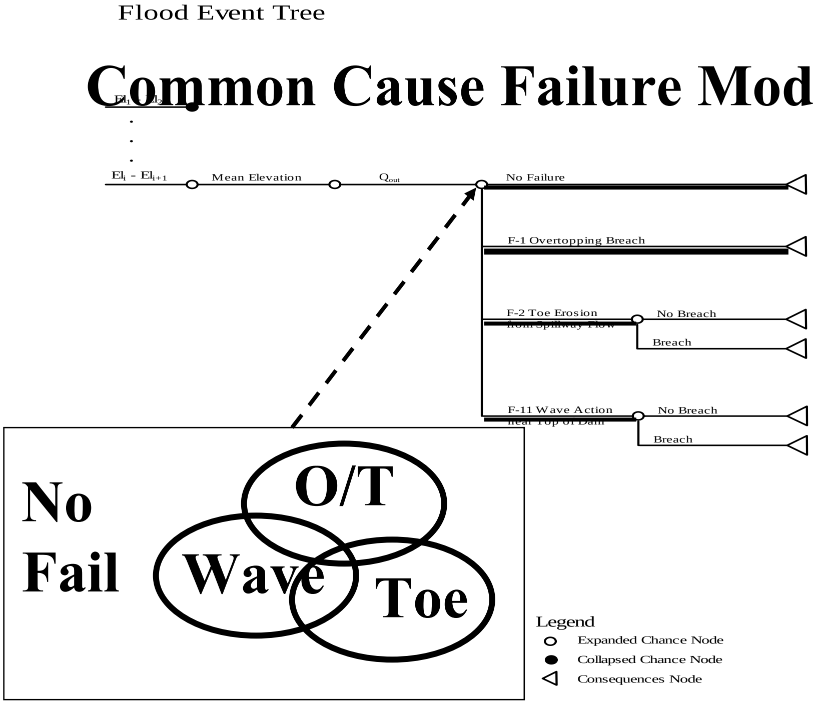
Common Cause Events

Events *emanating from a node*:

- MUST be **collectively exhaustive** (i.e. must cover all possible events)
- PREFERABLY **mutually exclusive** (i.e. only one of the outcomes can happen - sum of conditional probabilities = 1.0)
- Example exceptions:
  - Multiple failure modes at a single dam section
  - Failure modes at multiple dam sections
- If not mutually exclusive - COMMON-CAUSE EVENTS



Common Cause Failure Modes



Common cause adjustments

- Uni-modal bounds theorem
- Physical dominance

Common Cause Failure Modes
Uni-modal Bounds Theorem
(Ang and Tang 1984)

For k positively correlated failure modes, with branch failure probabilities (SRPs), p_i, the system (total) branch failure probability, p_f , lies between the following upper (u) and lower (l) bounds:

$$p_f^l \leq p_f \leq p_f^u$$

$$\max_i [p_i] \leq p_f \leq 1 - \Pi_{i=1}^{k} (1 - p_i)$$

Common Cause Failure Modes
Uni-modal Bounds Theorem

$$p_i^u = p_i (p_f^u / p_f)$$

- Upper (u) bound used to adjust the each branch probability for flood and flood-internal failure modes
- Freeze adjustment at value for smallest loading interval for which one of the branch failure probabilities equals or exceeds 1.0 for flood
- Not necessary for earthquake loading it does not progressively increase like floods
- Lower (l) bound: set all branch failure probabilities to zero, except for the maximum one which should retain its value without adjustment for floods
- Freeze as for upper bound

E-mail:
David.Bowles@usu.edu

Home Page
(including links to selected papers):
http://www.engineering.usu.edu/uwrl/www/faculty/bowles.html