CLIENTS | PEOPLE | PERFORMANCE

# Risk Assessment for Dams

**Malcolm Barker**

**(Principal Engineer Dams)**

# Purpose of the Presentation

- Introduce Risk Assessment
- Describe the ANCOLD Risk Assessment Process
- Introduce analysis methods and areas of concern in Risk Assessment
- Discuss Human Factors in Risk Assessments

# Winston Churchill

True Genius resides in the capacity for the evaluation of

uncertain,

hazardous and

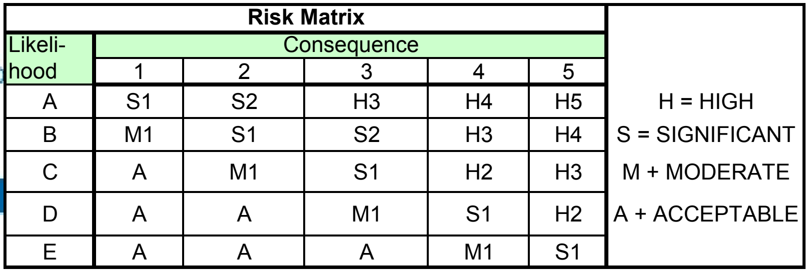
conflicting

Information”

# What is Risk

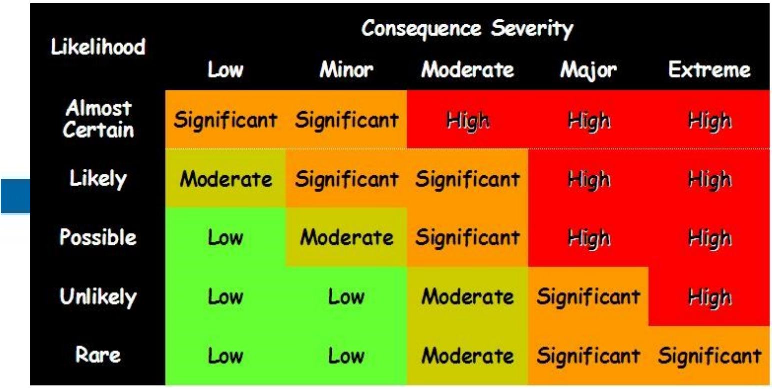
- ANCOLD 2003 – Measure of the Probability and Severity of an adverse effect to life, health, property or the environment
- Risks (Fatality rate/yr) (Department of Planning, Sydney 1990)

| | |
|---|---|
| Travelling by car 1.5E-4 | (1 in 6666) |
| Accidents at home 1.1E-4 | (1 in 9090) |
| Floods 2E-7 | (1 in 5,000,000) |
| Fires 1E-5 | (1 in 100,000) |
| Lightning Strikes 1E-7 | (1 in 10,000,000) |
| Meteor Strike 1E-9 | (1 in 1,000,000,000) |



Risk Matrix

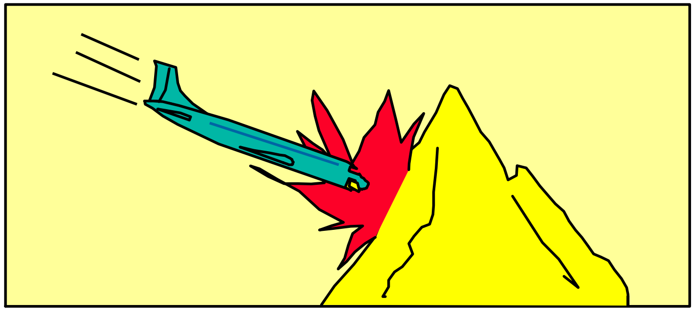
| Likeli-hood | Consequence | | | | | |
|---|---|---|---|---|---|---|
| | 1 | 2 | 3 | 4 | 5 | |
| A | S1 | S2 | H3 | H4 | H5 | H = HIGH |
| B | M1 | S1 | S2 | H3 | H4 | S = SIGNIFICANT |
| C | A | M1 | S1 | H2 | H3 | M + MODERATE |
| D | A | A | M1 | S1 | H2 | A + ACCEPTABLE |
| E | A | A | A | M1 | S1 | |

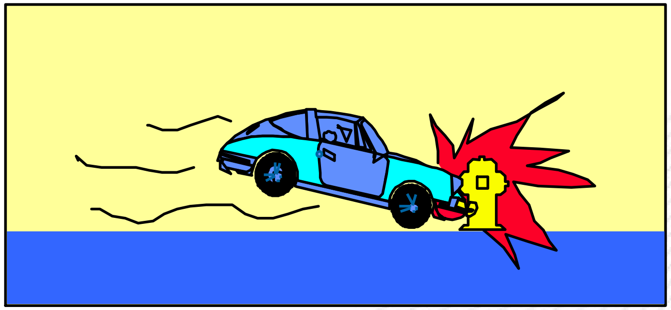


| Likelihood | Consequence Severity | | | | |
|---|---|---|---|---|---|
| | Low | Minor | Moderate | Major | Extreme |
| Almost Certain | Significant | Significant | High | High | High |
| Likely | Moderate | Significant | Significant | High | High |
| Possible | Low | Moderate | Significant | High | High |
| Unlikely | Low | Low | Moderate | Significant | High |
| Rare | Low | Low | Moderate | Significant | Significant |

# Probability & Consequence

- Which illustration depicts the higher risk?



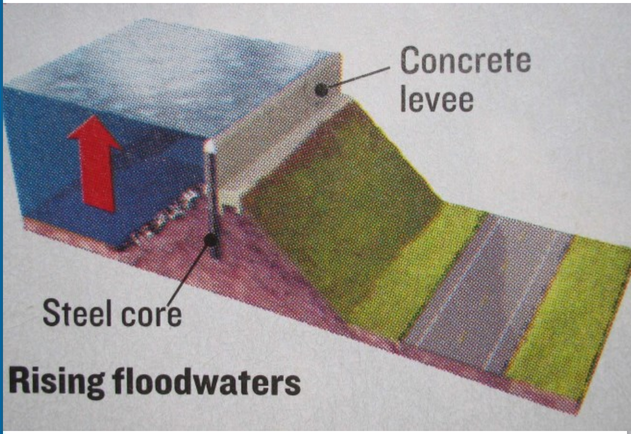


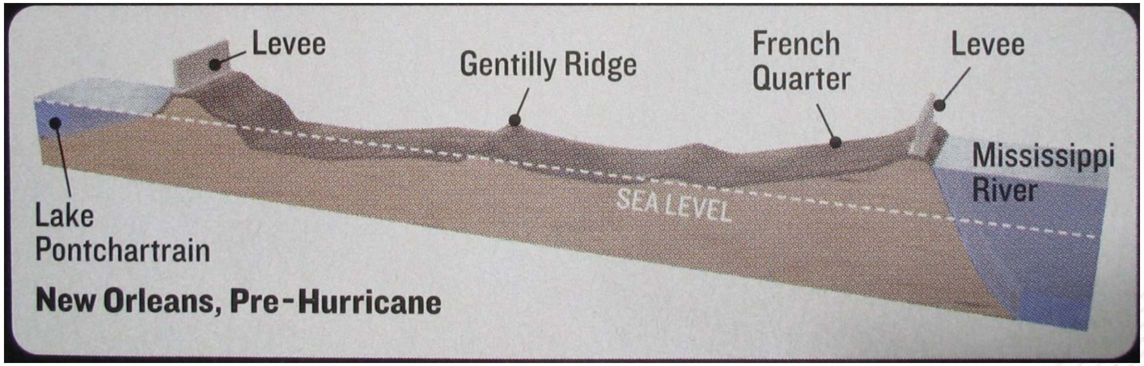
Consequence = Extreme 5
Probability = Unlikely D
Risk = High 2

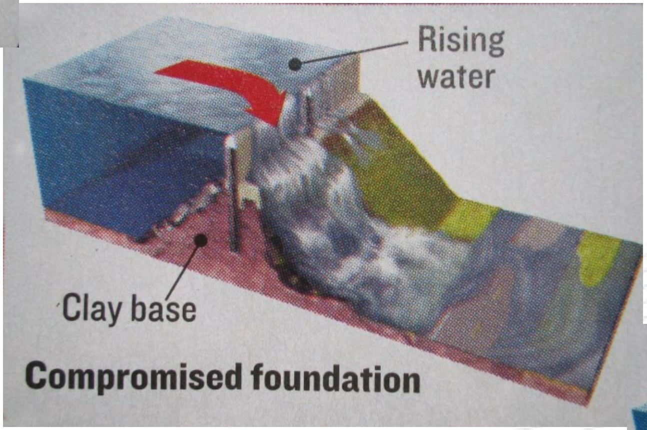
Consequence = Major 4
Probability = Possible C
Risk = High 2

- Probability or consequence of a risk condition is not, by itself, a good measure of risk

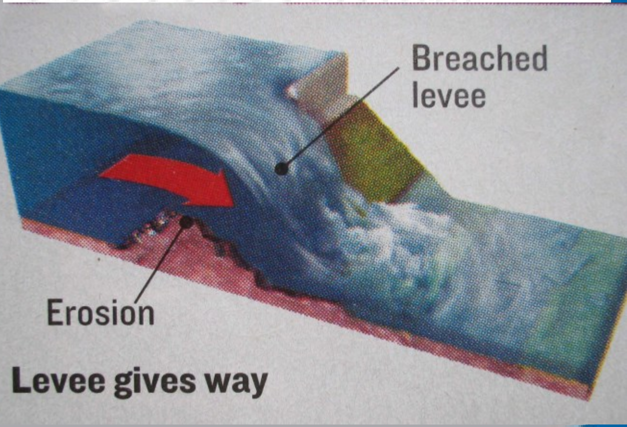
# Understanding Risk







Source : Newsweek September 2005



**Understanding :**

- the loads (mag & frequency)
- the capacity
- the consequences
- the failure process (pathway)
- the politics of taking action

**Remember** : There but for the Grace of God go I

# Measures of Risk

- Expected Value
  - Risk = Σ [Probability x Consequence]
- Non-Product Form
  - Risk = Σ [Scenario/ Probability/ Consequence]
  - Suited to zero/infinity risks (very low probability but very large consequences)

# Why Bother with Risk Assessments

- Objective Assessment - Are probabilities objective or Subjective? - Degree of belief
- Transparency in decision making process, defensible
- Structured Framework for evaluating risks, their relative importance and options for risk reduction
- Can be staged to provide the required degree of improvement

# Risk Assessment and Dam Safety Management

- Dam safety management requires decision-making under uncertainty
- Risk Assessment is a Decision Process to decide
  - Are existing risks tolerable; and
  - Are risk control measures adequate;
  - If not, are alternative risk control measures required
- The AIM of risk assessment is NOT to have less safe dams than traditional approach
- RA "provides a systematic structuring of uncertainty, and this structuring allows us better to understand how uncertainty arises and how information may lessen it." (Baecher, 2001).
- Risk Assessment does not replace the traditional approach but aids Dam Safety Management.

# Benefits of risk Assessment

- ✓ Improved understanding of the dam.
- ✓ Due diligence;
- ✓ Rational, systematic process;
- ✓ Consider all loading and operating conditions;
- ✓ Treatment of uncertainty;
- ✓ Quantitative comparison of risks for remedial works prioritisation;
- ✓ Understand potential liabilities of dam ownership;

# Limitations of risk Assessment

- Difficulty of estimating uncertainties and the probabilities of failure;
- Difficulty of estimating loss of life;
- Setting tolerable life safety criteria
- Cost of detailed studies
- Difficulty of dealing with only one hazard
- Few persons with experience

# Uncertainty

Uncertainty is not created by Risk Analysis but is inherent in dam safety

## Aleatory Uncertainty

- Arises from the ***inherent random variability in nature***
- Considered “objective” – it exists in the real world
- Measured by probability as frequency
- Examples are exceedance probabilities of floods and earthquakes

# Uncertainty

## Epistemic Uncertainty

- Arises from our ***incomplete or lack of knowledge***
- Considered “subjective” – it exists in the minds of humans, but not in the real world – not a property of the dam
- Measured by probability as the degree of confidence in an outcome, based on the evidence
- The probability can be expected to change as our knowledge about the factors influencing the outcome changes
- Example is the probability that a concrete gravity dam would fail, given a specified reservoir water level not previously experienced

# Dealing with Uncertainty

- Precautionary Approach
  - More weight attached to consequences than likelihoods
  - Safety factors built-in in the assessment process where appropriate
  - Credible scenarios established for the purpose of assessing risks
- Risk Assessment
  - Uncertainties for loads and responses
  - Recognition of uncertainties in the analyses and probability estimates

# Questions to be Answered by Risk Analysis Team

| | |
|---|---|
| • what are the hazards? | Earthquake, flood, ice, wind, groundwater, sabotage etc |
| • what can go wrong? | Failure modes |
| • what is the likelihood that it will go wrong ? | Probability/Annual Frequency |
| • what are the consequences? | Life loss, business, financial, social, environmental? |
| • what are the risks? | Likelihood x Consequences |

# Questions to be Answered Risk Analysis Team and Owner

- Is the dam safe enough? Acceptance Criteria
- If not, how can the risks be reduced? – Structural and non structural measures
- Are residual risks after remedial works tolerable?
- How are risks to be managed in the long term?

# Roles of Risk Assessment

**Three roles for Risk Assessment and dam safety:**

a) **Enhancement to the traditional approach**

b) **Alternative to the traditional approach**

c) **Sole basis for decision making**

**Traditional Safety Factors do not always ensure "Safe" dams as safety factors cannot consider all failure modes**

**ANCOLD supports the first of the three roles - (a)**

**Recognition is being given to the use of Risk Assessment for decision making eg Queensland's Dam Safety Regulator "Guidelines on Acceptable Flood Capacity for Dams"**

CLIENTS | PEOPLE | PERFORMANCE

# Types of Risk Assessment

- *Qualitative analysis or Semi quantitative*
  - *Risk Index Systems*
  - *Hazard Identification*
  - *Failure Modes Analysis*
  - *Matrix Schemes*
  - *Hazard Failure Mode Control Schemes*
- *Quantitative*

***All Types can be used for Individual or Portfolio of Dams but Qualitative are difficult to apply to a portfolio of dams***

# Levels of Risk Assessment

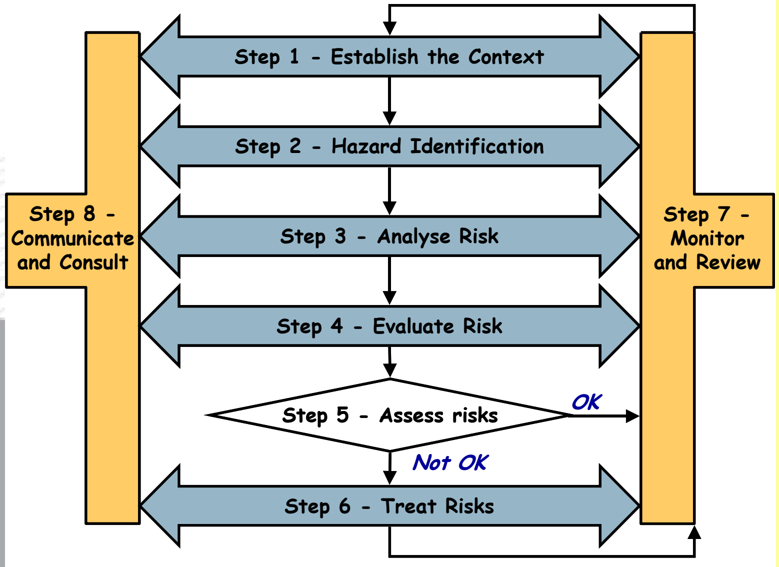
- Four Levels of Risk Assessment
  - Screening
  - Preliminary
  - Detailed
  - Very Detailed

# Levels and Study Inputs

| Level | Type | Engineering Inputs | Estimation of Probabilities of Failure | Estimation of Consequences | Risk Evaluation Method |
|---|---|---|---|---|---|
| Screening | Qualitative or Quantitative | Basic | Screening to preliminary | Basic to moderate | Basic |
| Preliminary | Quantitative | Moderate to basic | Preliminary | Moderate | Moderate to Basic |
| Detailed | Quantitative | Advanced to moderate | Detailed | Advanced to moderate | Detailed to moderate |
| Very detailed | Quantitative | Advanced to very advanced | Very detailed | Advanced to very advanced | Detailed or very detailed |

# ANCOLD Typical Risk Assessment Process for Dams

## AS/NZS 4360 Risk Management Steps



Step 1 - Establish the Context

Step 2 - Hazard Identification

Step 3 - Analyse Risk

Step 4 - Evaluate Risk

Step 5 - Assess risks

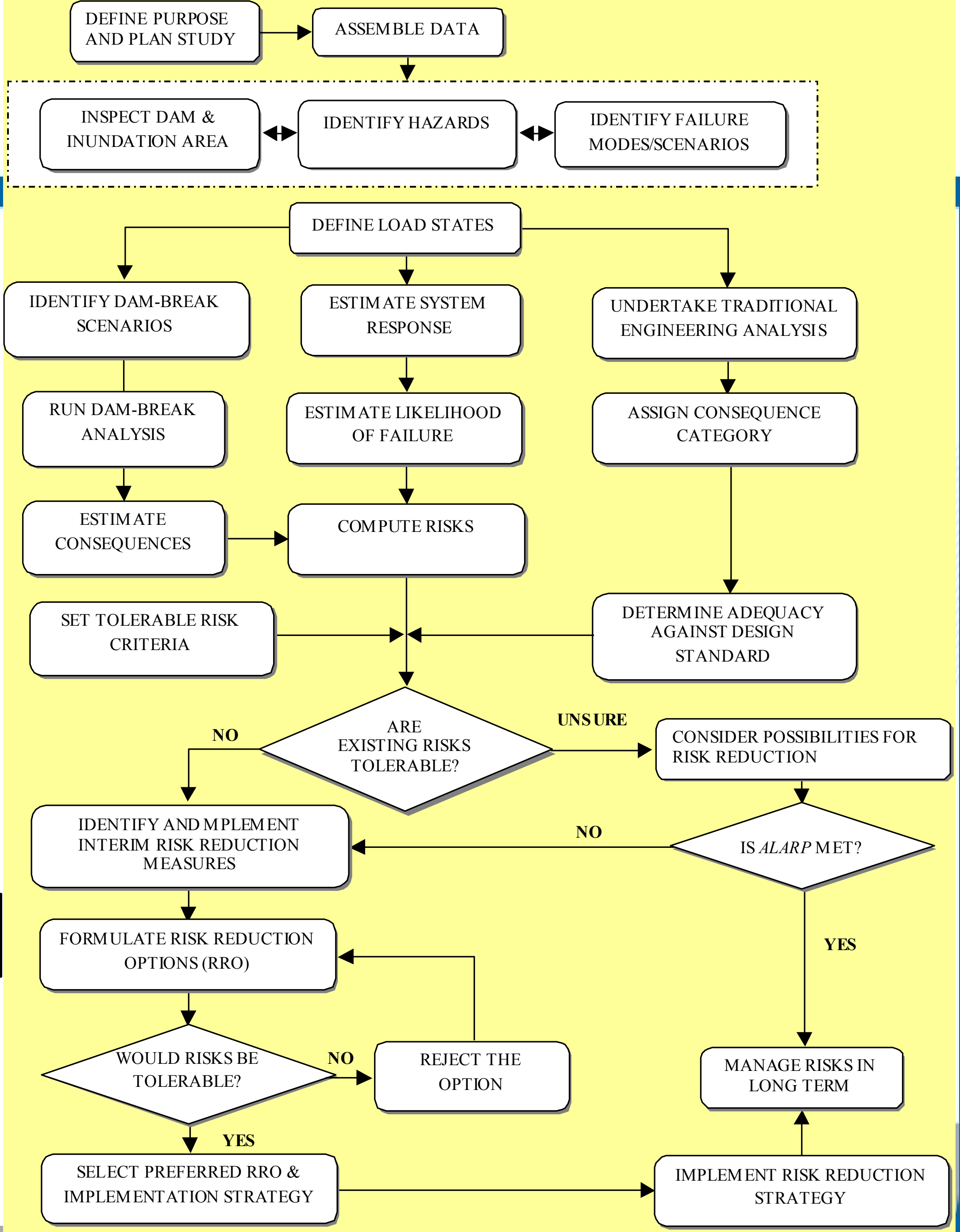
OK

Not OK

Step 6 - Treat Risks

Step 7 - Monitor and Review

Step 8 - Communicate and Consult



DEFINE PURPOSE AND PLAN STUDY

ASSEMBLE DATA

INSPECT DAM & INUNDATION AREA

IDENTIFY HAZARDS

IDENTIFY FAILURE MODES/SCENARIOS

DEFINE LOAD STATES

IDENTIFY DAM-BREAK SCENARIOS

ESTIMATE SYSTEM RESPONSE

UNDERTAKE TRADITIONAL ENGINEERING ANALYSIS

RUN DAM-BREAK ANALYSIS

ESTIMATE LIKELIHOOD OF FAILURE

ASSIGN CONSEQUENCE CATEGORY

ESTIMATE CONSEQUENCES

COMPUTE RISKS

SET TOLERABLE RISK CRITERIA

DETERMINE ADEQUACY AGAINST DESIGN STANDARD

ARE EXISTING RISKS TOLERABLE?

NO

UNSURE

CONSIDER POSSIBILITIES FOR RISK REDUCTION

IDENTIFY AND MPLEMENT INTERIM RISK REDUCTION MEASURES

NO

IS *ALARP* MET?

YES

FORMULATE RISK REDUCTION OPTIONS (RRO)

WOULD RISKS BE TOLERABLE?

NO

REJECT THE OPTION

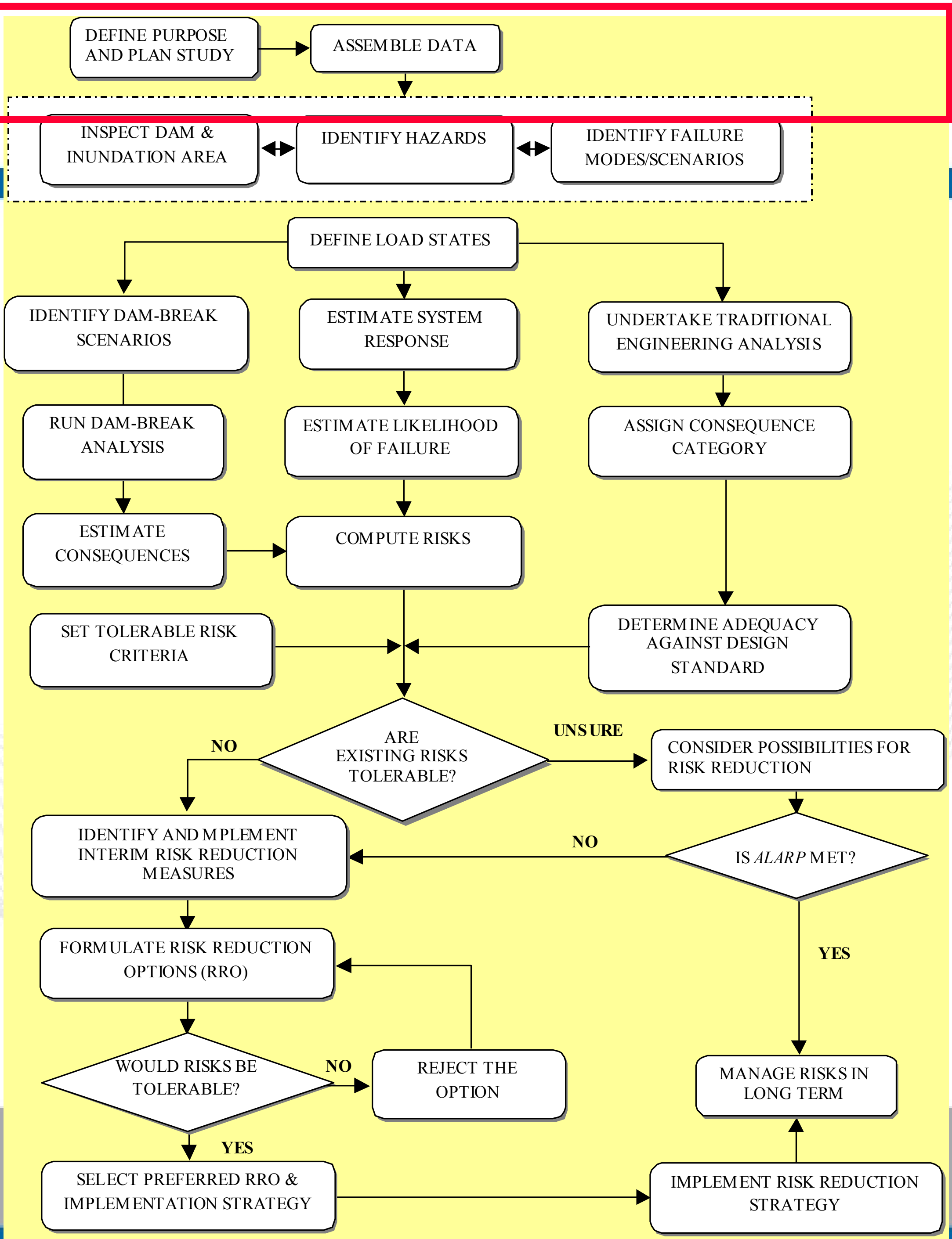
MANAGE RISKS IN LONG TERM

YES

SELECT PREFERRED RRO & IMPLEMENTATION STRATEGY

IMPLEMENT RISK REDUCTION STRATEGY

# Planning



DEFINE PURPOSE AND PLAN STUDY

ASSEMBLE DATA

INSPECT DAM & INUNDATION AREA

IDENTIFY HAZARDS

IDENTIFY FAILURE MODES/SCENARIOS

DEFINE LOAD STATES

IDENTIFY DAM-BREAK SCENARIOS

ESTIMATE SYSTEM RESPONSE

UNDERTAKE TRADITIONAL ENGINEERING ANALYSIS

RUN DAM-BREAK ANALYSIS

ESTIMATE LIKELIHOOD OF FAILURE

ASSIGN CONSEQUENCE CATEGORY

ESTIMATE CONSEQUENCES

COMPUTE RISKS

SET TOLERABLE RISK CRITERIA

DETERMINE ADEQUACY AGAINST DESIGN STANDARD

ARE EXISTING RISKS TOLERABLE?

NO

UNSURE

CONSIDER POSSIBILITIES FOR RISK REDUCTION

IDENTIFY AND MPLEMENT INTERIM RISK REDUCTION MEASURES

NO

IS *ALARP* MET?

YES

FORMULATE RISK REDUCTION OPTIONS (RRO)

WOULD RISKS BE TOLERABLE?

NO

REJECT THE OPTION

MANAGE RISKS IN LONG TERM

YES

SELECT PREFERRED RRO & IMPLEMENTATION STRATEGY

IMPLEMENT RISK REDUCTION STRATEGY

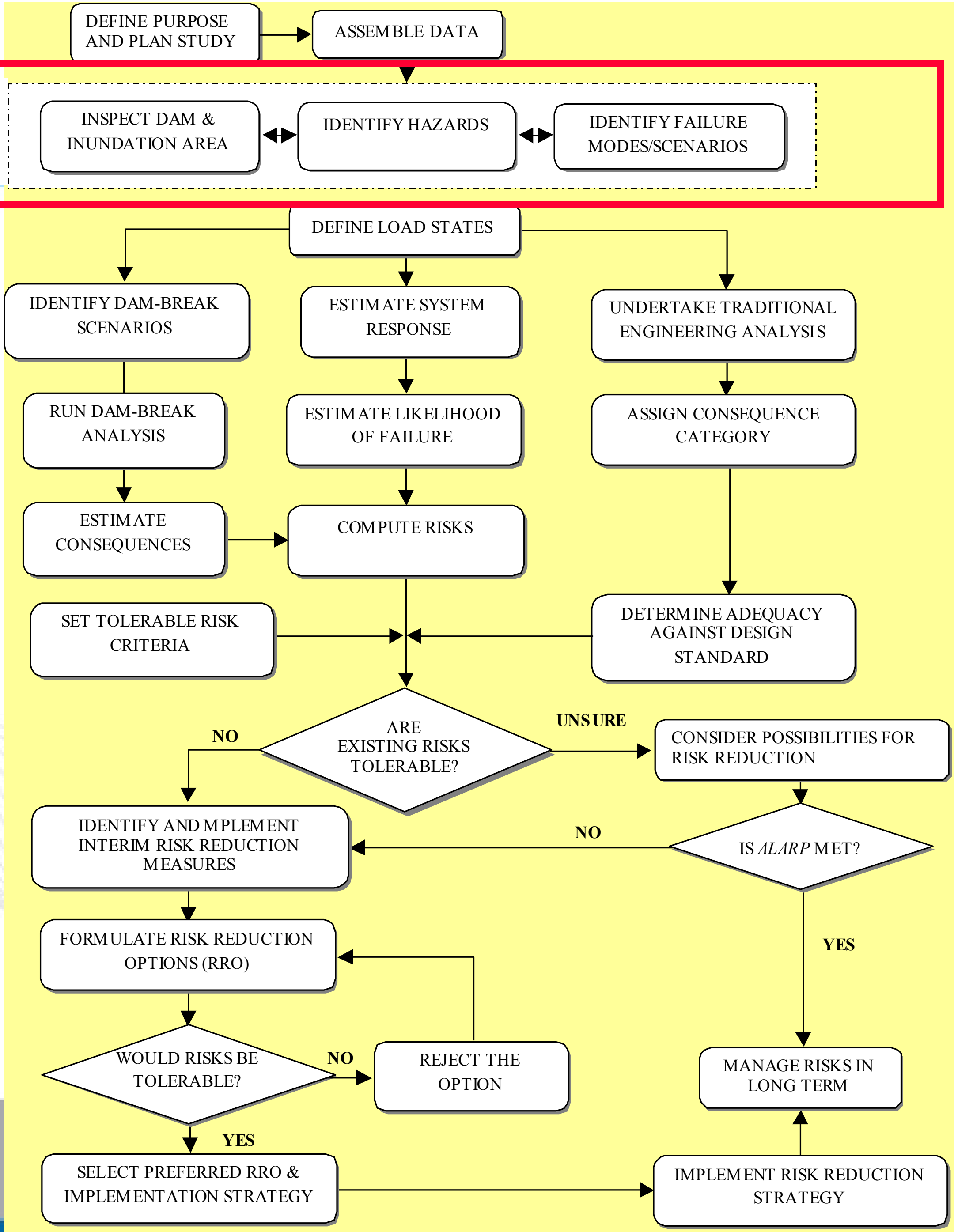
# Planning a Risk Assessment

- Purpose and Decision context
  - What is to be decided
  - How is the decision to be made for further action
- Determine Type, Level and Rigour of the RA
- Identify the legal and regulatory context
- Design the study as a systematic process (ANCOLD Fig 7.1 and 7.2)
- Consider staged approach:
  - Early recognition of high risk failure modes
  - More focused detail evaluation after screening
  - Early low cost assessment for justification or not of further work

# Planning a Risk Assessment Contd.

- Identify key participants and their roles
  - Owner
  - Decision maker
  - Analysis Team
  - **Reviewers**
  - **Regulator**
  - Other owner members
- Implement comprehensive documentation
- Follow recognised QA Procedures
- Assemble Data
  - Assemble all available records for the dam/s
  - Catalogue and list sources of data in the report
  - Review the documentation (allow for this in the budget)
  - Define the system to be analysed

# First Phase



DEFINE PURPOSE AND PLAN STUDY

ASSEMBLE DATA

INSPECT DAM & INUNDATION AREA

IDENTIFY HAZARDS

IDENTIFY FAILURE MODES/SCENARIOS

DEFINE LOAD STATES

IDENTIFY DAM-BREAK SCENARIOS

ESTIMATE SYSTEM RESPONSE

UNDERTAKE TRADITIONAL ENGINEERING ANALYSIS

RUN DAM-BREAK ANALYSIS

ESTIMATE LIKELIHOOD OF FAILURE

ASSIGN CONSEQUENCE CATEGORY

ESTIMATE CONSEQUENCES

COMPUTE RISKS

SET TOLERABLE RISK CRITERIA

DETERMINE ADEQUACY AGAINST DESIGN STANDARD

ARE EXISTING RISKS TOLERABLE?

NO

UNSURE

CONSIDER POSSIBILITIES FOR RISK REDUCTION

IDENTIFY AND MPLEMENT INTERIM RISK REDUCTION MEASURES

NO

IS *ALARP* MET?

YES

FORMULATE RISK REDUCTION OPTIONS (RRO)

WOULD RISKS BE TOLERABLE?

NO

REJECT THE OPTION

MANAGE RISKS IN LONG TERM

YES

SELECT PREFERRED RRO & IMPLEMENTATION STRATEGY

IMPLEMENT RISK REDUCTION STRATEGY

# Site Inspection

- Very Important part of Risk Analysis
- Include key personnel from analysis team
  - Independent reviewers
  - Operating personnel
  - Surveillance personnel
  - Owner or representative
- Review data
- Prepare checklists for inspection
- Assemble equipment needed for inspection
- Make initial list of Hazards and Failure Modes
- Make on site record of observations include downstream inundation area
- Prepare Inspection report

# Hazard Analysis

- List all hazards that could conceivably occur
- Identify Hazards that are negligible giving reason for exclusion
- List remaining hazards for analysis

# Hazard Identification

| Item | Failure Initiating Events | Screening Criteria | Comments | Subsequent Events for Failure Pathways Analysis |
|---|---|---|---|---|
| 1 | Aircraft Impact | 5 | No major flight paths directly over Dam? | |
| 2 | Avalanche | 3 | None in area | |
| 3 | Chemical Reaction | 5 | Dissolution of the rock in foundation unlikely | |
| 4 | Earthquake | | High embankment phreatic surface prior to earthquake may increase failure potential | Embankment settlement, embankment slope failure, cracking leading to piping, foundation joints opening |
| | | 1 | Approx. 1 m thick of gravelly clay, sandy clay under the highest part of the embankment. Materials not likely to be liquefiable. (residual soil material) based on site investigaton report | |
| | | 5 | Weak foundation soils removed | |
| | | 1 | | |
| 5 | Fire | 5 | No affect on the dam, gravity inflow, complete failure of control system flow will be passed through the spillway | |
| 6 | Hail | 5 | No affect on the dam | |
| 7 | Human Error | | Human error in surveillance | |
| 8 | Hydrological / Flood (operational level rising) | | Upgrade works designed for upper bound PMF. | High reservoir level, spillway blockage, wind seiche, waves, slope failure, overtopping |
| | | | Upper part of embankment not protected by downstream filter | Piping through embankment , piping through upper part of embankment, piping through geotextile, pipng through sand, piping through foundation, piping through outlet work, piping through inlet work, piping through unknown pipe |
| 9 | Ice | 5 | No ice at this location | |
| 10 | Lightning | 5 | Affects valve power supply, but no affect on dam (gravity inflow, complete failure of control system flow will be passed through the spillway) | |
| 11 | Temperature | 5 | No affect on the dam | |
| 12 | Meteor Strike | 2 | | |
| 13 | Pore pressures | | Drainage system failure | Slope stability, piping, embankment overtopping (incorporated with hydrological flood) |
| 14 | Reservoir Level Fluctuations | | Site specific, requires study | Embankment slope failures, piping |
| 15 | Reservoir Rim Slope Failure | 1 | Significant freeboard. Gentle slopes along reservoir rim and no identified slope failures. | |
| 16 | Pipe burst | | Likely leak in the inlet pipe | Piping, overtopping |
| | | | Leak in the outlet pipe | Piping, overtopping |
| 17 | Terrorism | 5 | | High energy impact of the dams or spillway (explosives) |
| 18 | Toxic Gas | 3 | Chorination house near dam. Approx. 3 tonnes storage. No effect on dam | |
| 19 | Transportation Accident | 5 | Not a public road | |
| 20 | Vandalism | 5 | | Failure of outlet works or valves, spillway damage |
| 21 | Volcanic Activity | 3 | None in area | |
| 22 | Wind | 1 | Small fetch distance | |

**Screening Criteria**

**1** The event is of equal or lesser damage potential that the events for which the dam is designed. Design Significantly exceeds requirement.

**2** The event has a significantly lower mean frequency of occurrence than other events with similar uncertainties and could not result in worse consequences than those events

**3** The event cannot occur close enough to the dam to affect it.

**4** The event is included in the definition of other event(s)

**5** The event is judged to have an insignificant effect on the dam

**6** Not an initiator

# Failure Mode Analysis

## What is a Failure Mode

- **ANCOLD 2003**

  ***A way that failure can occur, described by the means by which element or component failures must occur to cause loss of the sub-system or system function.***

- **IEC 1985**

  ***A failure mode is the effect by which a failure is observed in a system component***

# Failure Incidents

ABSTRACT FROM UNICIV REPORT ON ANALYSIS OF EMBANKMENT DAM FAILURE INCIDENTS

Overall statistics of failure occurring before and after 1950, large embankment dams

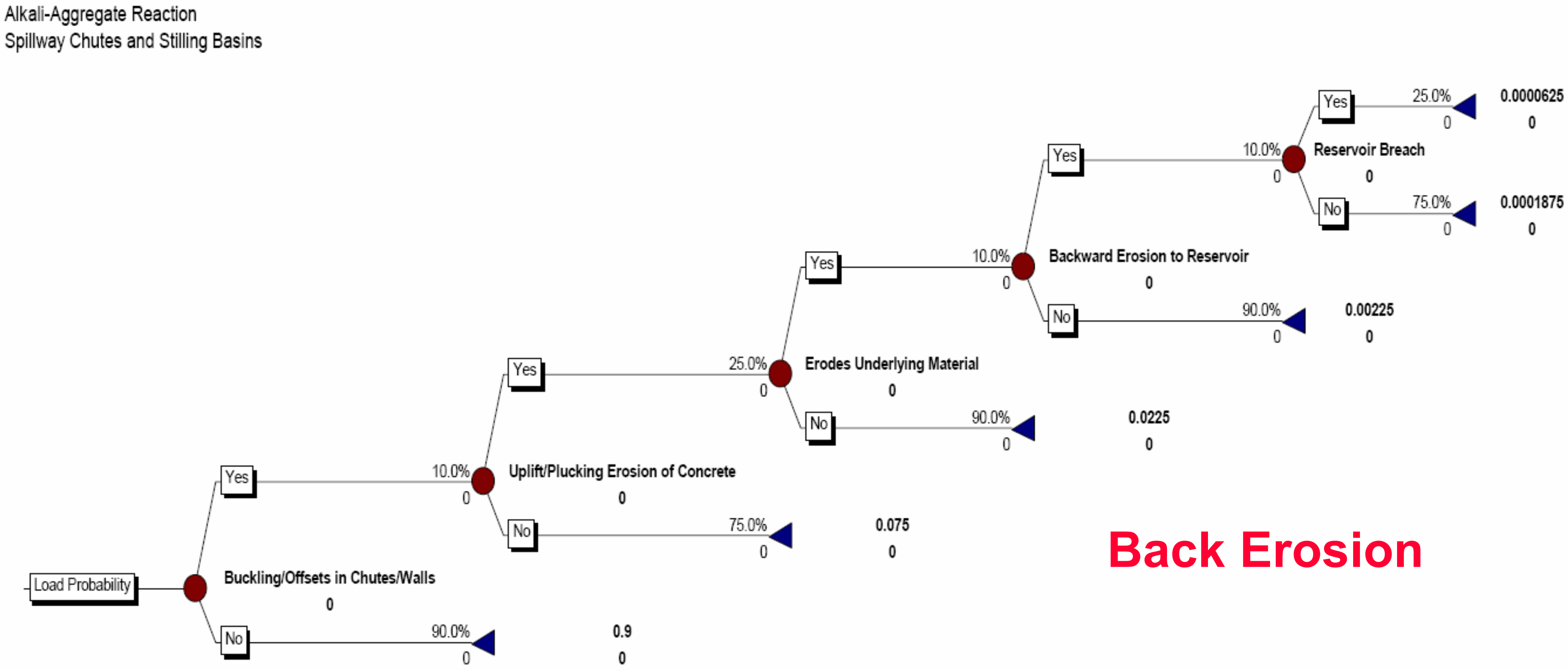
| **Mode of Failure** | **% Total Failures (where mode of failure known)** | **% Failures pre 1950** | **% Failures post 1950** |
|---|---|---|---|
| Overtopping | 34.2 % | 36.2 % | 32.2 % |
| Spillway/gate (appurtenant works) | 12.8 % | 17.2 % | 8.5 % |
| Piping through embankment | 32.5 % | 29.3 % | 35.5 % |
| Piping from embankment into foundation | 1.7 % | 0 % | 3.4 % |
| Piping through foundation | 15.4 % | 15.5 % | 15.3 % |
| Downstream slide | 3.4 % | 6.9 % | 0 % |
| Upstream slide | 0.9 % | 0 % | 1.7 % |
| Earthquake | 1.7 % | 0 % | 3.4 % |
| Totals (3) | 102.6 % | 105.1 % | 100 % |
| Total overtopping and appurtenant works | 48.4 % | 53.4 % | 40.7 % |
| Total piping | 46.9 % | 43.1 % | 54.2 % |
| Total slides | 5.5 % | 6.9 % | 1.6 % |
| Total no. of embankment dam failures (exc. During construction) | 124 | 61 | 63 |
| Total embankment dam years operation (up to 1986) | 300,400 | 71,000 | 229,400 |
| Annual probability of failure | 4.1 x $10^{-4}$ | 8.6 x $10^{-4}$ | 2.7 x $10^{-4}$ |

***Notes:***

1. *Percentages based on the % of cases where the mode of failure is known.*
2. *Percentages are for failures of embankment dams in operation only, i.e. excluding failures during construction.*
3. *Percentages do not necessarily sum to 100% as some dams were classified as multiple modes of failure.*

# Example of Failure Pathways for a Failure Mode

## Effects of Concrete Deterioration on Safety of Dams
## DSO-03-05 Dec 2003


Alkali-Aggregate Reaction
Spillway Chutes and Stilling Basins
Load Probability
Buckling/Offsets in Chutes/Walls
0
Yes
10.0%
0
No
90.0%
0
0.9
0
Uplift/Plucking Erosion of Concrete
0
Yes
25.0%
0
No
75.0%
0
0.075
0
Erodes Underlying Material
0
Yes
10.0%
0
No
90.0%
0
0.0225
0
Backward Erosion to Reservoir
0
Yes
10.0%
0
No
90.0%
0
0.00225
0
Reservoir Breach
0
Yes
25.0%
0
0.0000625
0
No
75.0%
0
0.0001875
0

Back Erosion

# FMEA Process

- Agree on the Criticality system to be used (if Criticality Analysis is being done);
- Define the system and components for analysis which do not overlap in function eg spillway, embankment dam;
- Give each component to be analysed an Identification Number
- Determine primary and other functions

**Table 1: Risk Matrix**

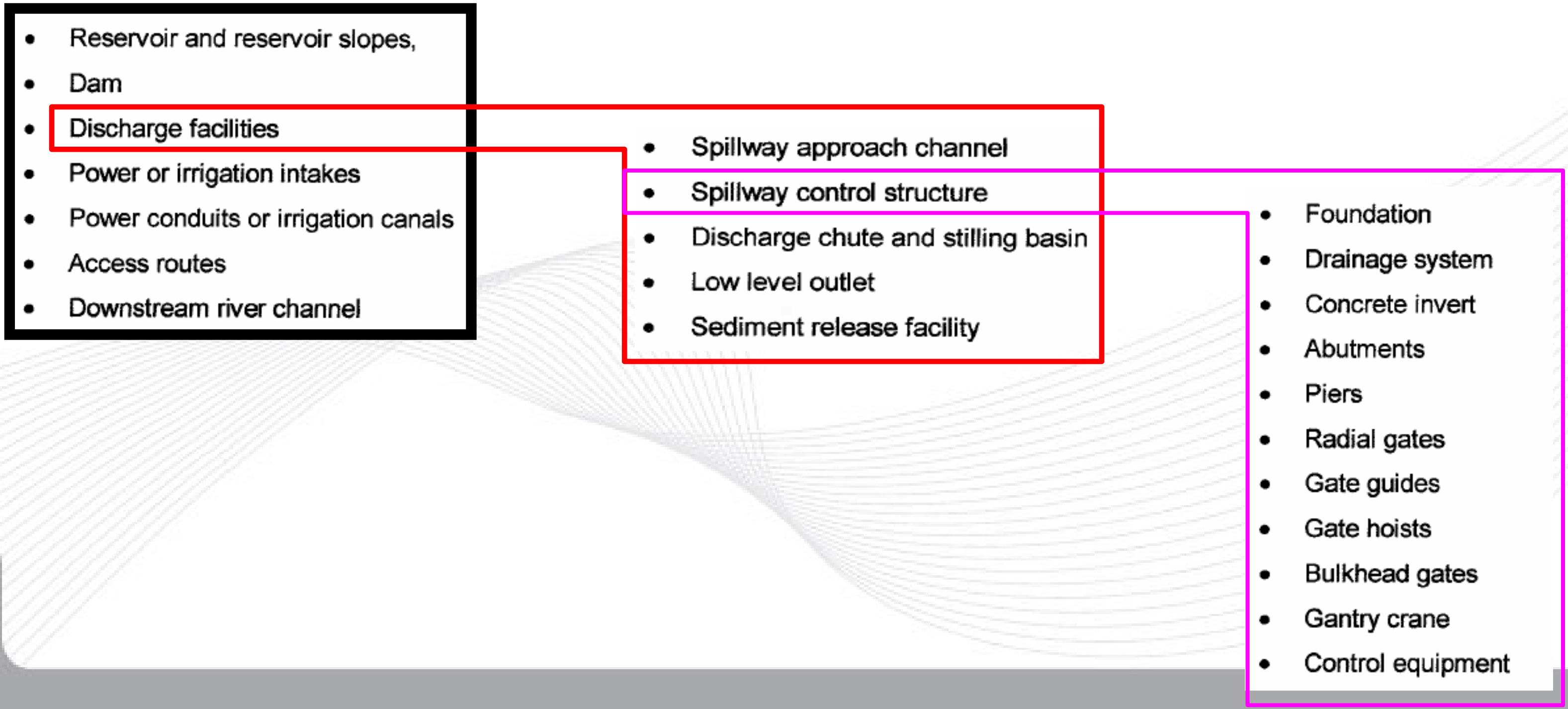
| | | Consequence / Severity | | | | |
|---|---|---|---|---|---|---|
| | | Low | Minor | Moderate | Major | Critical |
| Likelihood | Almost Certain | High (15) | High (10) | Extreme (6) | Extreme (3) | Extreme (1) |
| | Likely | Moderate (19) | High (14) | High (9) | Extreme (5) | Extreme (2) |
| | Possible | Low (22) | Moderate (18) | High (13) | Extreme (8) | Extreme (4) |
| | Unlikely | Low (24) | Low (21) | Moderate (17) | High (12) | Extreme (7) |
| | Rare | Low (25) | Low (23) | Moderate (20) | High (16) | High (11) |

**Table 2: Likelihood Table**

| Likelihood | Description in terms of full operating life of the site | Description in terms of frequency |
|---|---|---|
| Almost Certain | Consequences expected to occur in most circumstances | Daily or continuous |
| Likely | Consequences will probably occur in most circumstances | Weekly or monthly |
| Possible | Consequences could occur at some time | Annually |
| Unlikely | Consequences may occur in specific circumstances | Within the life of the operation |
| Rare | Consequences may occur in exceptional circumstances | > 100 years |

# Component Definition Example

- Primary Sub-systems
  - Discharge Facilities Sub-systems
    - Spillway Control Structure



- Reservoir and reservoir slopes,
- Dam
- Discharge facilities
- Power or irrigation intakes
- Power conduits or irrigation canals
- Access routes
- Downstream river channel

- Spillway approach channel
- Spillway control structure
- Discharge chute and stilling basin
- Low level outlet
- Sediment release facility

- Foundation
- Drainage system
- Concrete invert
- Abutments
- Piers
- Radial gates
- Gate guides
- Gate hoists
- Bulkhead gates
- Gantry crane
- Control equipment

# FMEA Process

- Identify failure modes and causes
- Evaluate the effect of the failure (local and end)
- Evaluate detection methods
- Evaluate mitigating action
- Estimate consequences/severity classification (minor to catastrophic)

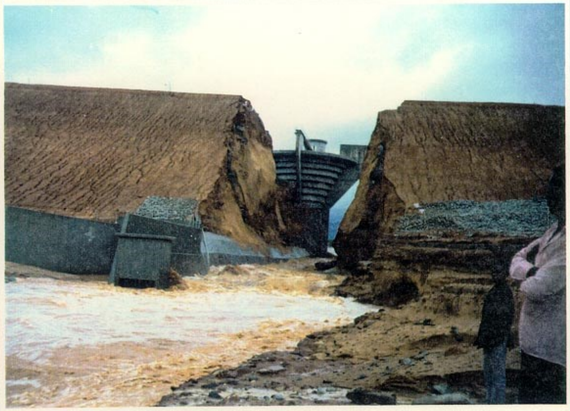


Plate 1. Breached dam with conduit still standing.

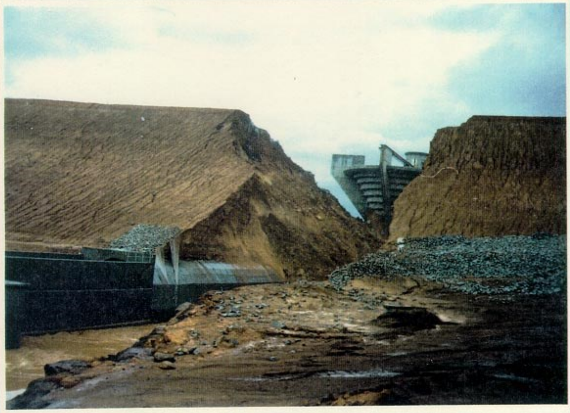


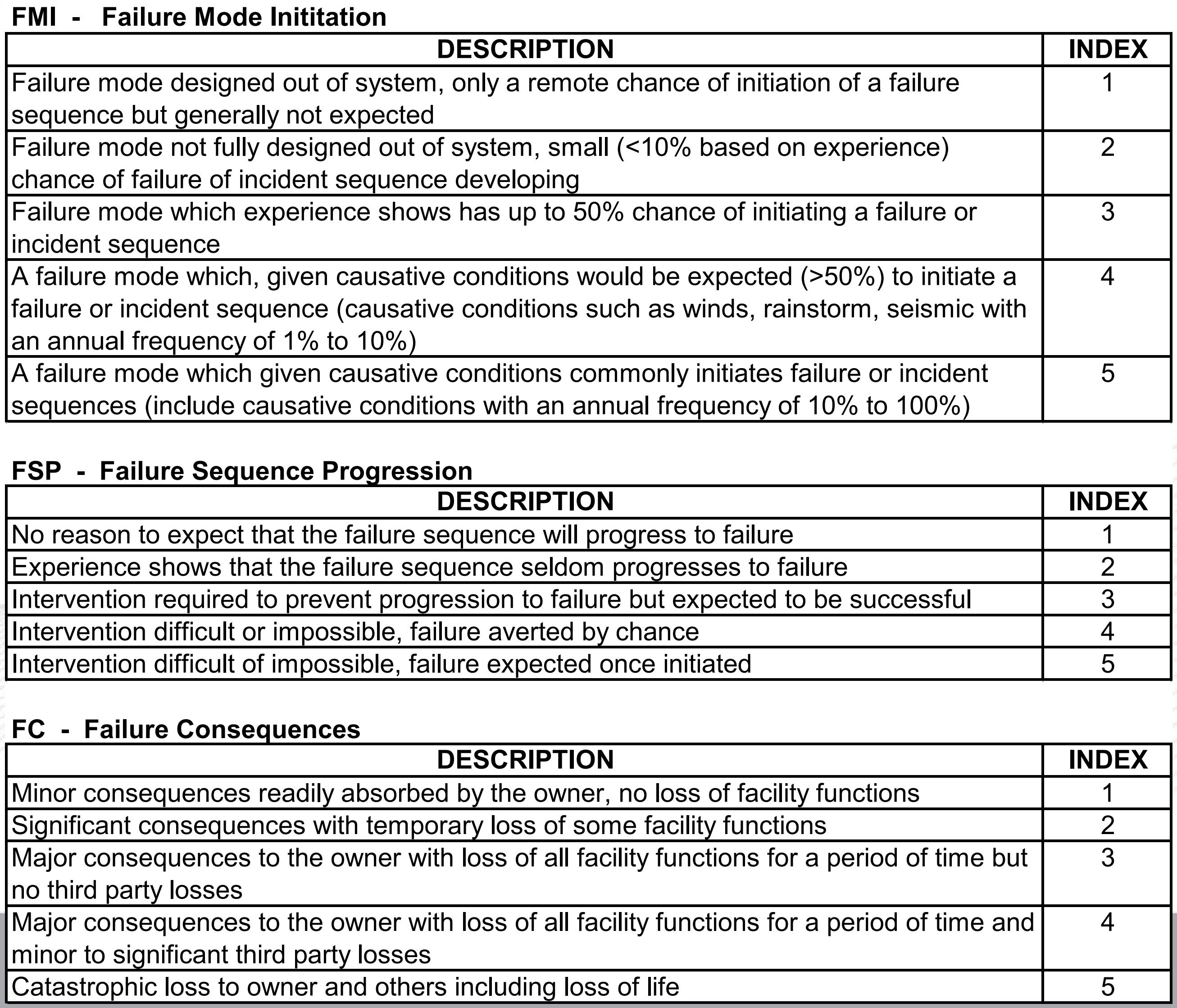
Plate 2. Breached dam with collapsed conduit.

# Additional Steps for Criticality Calculation

- System 1
  - Probability Index Rating (PI) – Likelihood of the failure mode occurring
  - Severity Index Rating (SI)  - Consequences
  - Criticality Index calculated as either the sum or product of the SI and PI
- System 2
  - Failure mode initiation likelihood (FMI)
  - Failure Sequence Progression (FSP)
  - Failure Consequences/Severity Index (FC)
  - Criticality Index calculated as either the sum or product of the FMI, FSP and FC

Do NOT use a zero index rating because difficult to prove a FM will not occur

# FMECA Data Input Examples



**FMI - Failure Mode Inititation**

| DESCRIPTION | INDEX |
|---|---|
| Failure mode designed out of system, only a remote chance of initiation of a failure sequence but generally not expected | 1 |
| Failure mode not fully designed out of system, small (<10% based on experience) chance of failure of incident sequence developing | 2 |
| Failure mode which experience shows has up to 50% chance of initiating a failure or incident sequence | 3 |
| A failure mode which, given causative conditions would be expected (>50%) to initiate a failure or incident sequence (causative conditions such as winds, rainstorm, seismic with an annual frequency of 1% to 10%) | 4 |
| A failure mode which given causative conditions commonly initiates failure or incident sequences (include causative conditions with an annual frequency of 10% to 100%) | 5 |

**FSP - Failure Sequence Progression**

| DESCRIPTION | INDEX |
|---|---|
| No reason to expect that the failure sequence will progress to failure | 1 |
| Experience shows that the failure sequence seldom progresses to failure | 2 |
| Intervention required to prevent progression to failure but expected to be successful | 3 |
| Intervention difficult or impossible, failure averted by chance | 4 |
| Intervention difficult of impossible, failure expected once initiated | 5 |

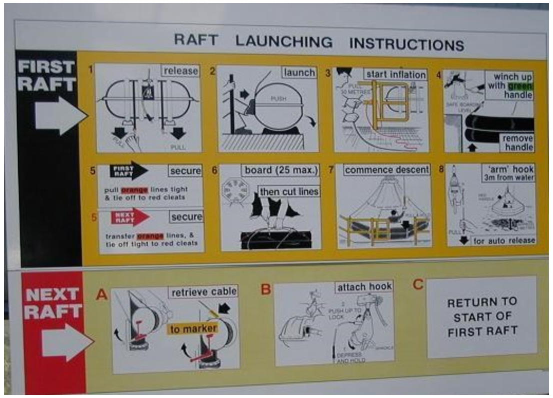
**FC - Failure Consequences**

| DESCRIPTION | INDEX |
|---|---|
| Minor consequences readily absorbed by the owner, no loss of facility functions | 1 |
| Significant consequences with temporary loss of some facility functions | 2 |
| Major consequences to the owner with loss of all facility functions for a period of time but no third party losses | 3 |
| Major consequences to the owner with loss of all facility functions for a period of time and minor to significant third party losses | 4 |
| Catastrophic loss to owner and others including loss of life | 5 |

# Prompts for Failure Modes

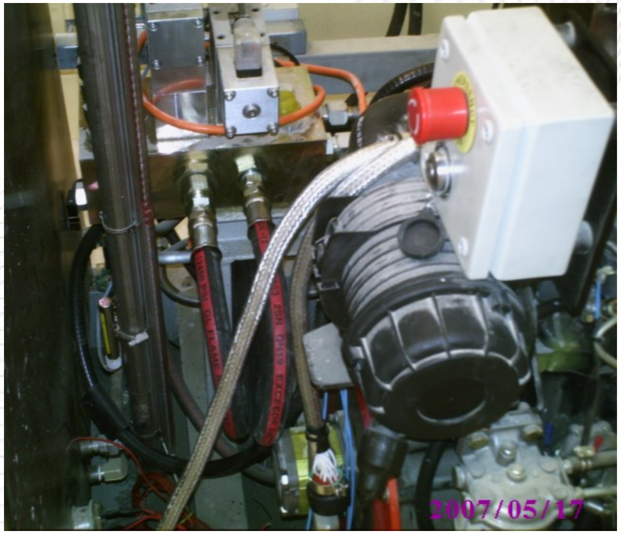
Procedural Failure Mode prompts:

- Fail to follow procedure
- Unable to follow procedure
- Fail to perform checks
- Fail to respond to errors…


RAFT LAUNCHING INSTRUCTIONS
FIRST RAFT
1 release
PULL
2 launch
PUSH
3 start inflation
4 winch up with green handle
remove handle
5 FIRST RAFT secure
pull orange lines tight & tie off to red cleats
5 NEXT RAFT secure
transfer orange lines, & tie off tight to red cleats
6 board (25 max.)
then cut lines
7 commence descent
8 'arm' hook 3m from water
for auto release
NEXT RAFT
A retrieve cable
to marker
B attach hook
PUSH UP TO LOCK
DEPRESS AND HOLD
C RETURN TO START OF FIRST RAFT

Mechanical/Electrical Failure Mode prompts:

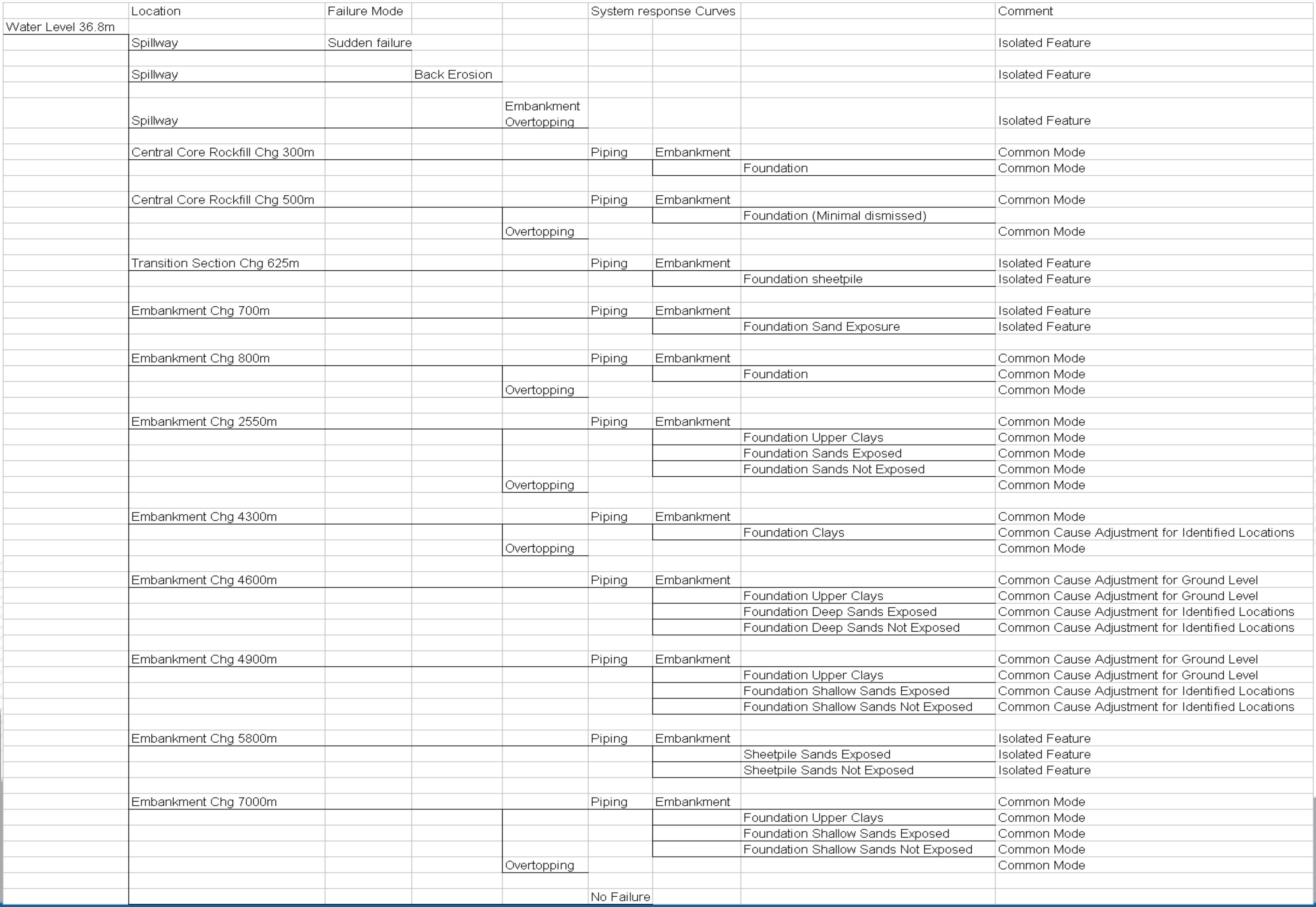
- Equipment failure
- Undetected (existing) equipment failure
- Maintenance failure (fail to restore)
- External effects (e.g. weather)



# FMEA Table Example

| Component | ID Number | Primary Function | Auxiliary Functions | Failure Modes | FM No | Causes | Failure Effect | | Failure Detection | Mitigating Action | Severity |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | Local Effect | End Effect | | | |
| | | | | | | | | | | | |
| | | | | | | | | | | | |
| | | | | | | | | | | | |

# Failure Modes and Combination Methods

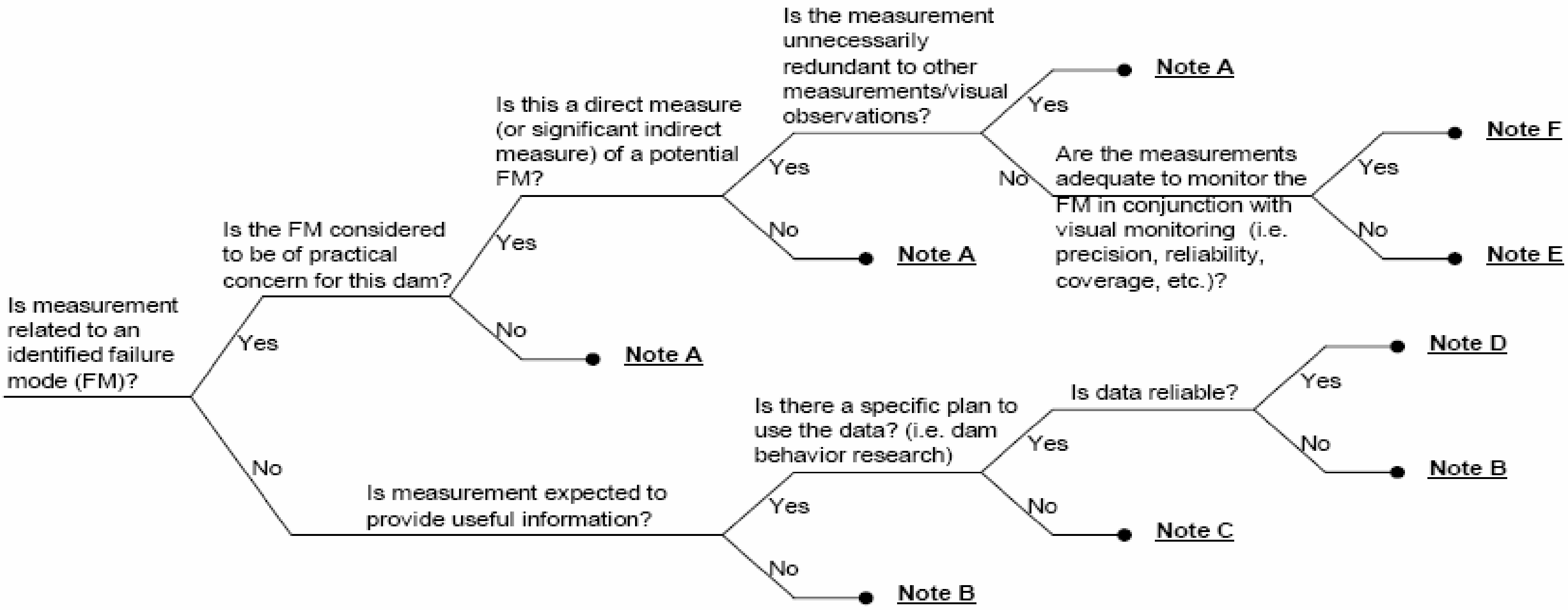


| | Location | Failure Mode | | | System response Curves | | | Comment |
|---|---|---|---|---|---|---|---|---|
| Water Level 36.8m | | | | | | | | |
| | Spillway | Sudden failure | | | | | | Isolated Feature |
| | Spillway | | Back Erosion | | | | | Isolated Feature |
| | Spillway | | | Embankment Overtopping | | | | Isolated Feature |
| | Central Core Rockfill Chg 300m | | | | Piping | Embankment | | Common Mode |
| | | | | | | | Foundation | Common Mode |
| | Central Core Rockfill Chg 500m | | | | Piping | Embankment | | Common Mode |
| | | | | | | | Foundation (Minimal dismissed) | |
| | | | | Overtopping | | | | Common Mode |
| | Transition Section Chg 625m | | | | Piping | Embankment | | Isolated Feature |
| | | | | | | | Foundation sheetpile | Isolated Feature |
| | Embankment Chg 700m | | | | Piping | Embankment | | Isolated Feature |
| | | | | | | | Foundation Sand Exposure | Isolated Feature |
| | Embankment Chg 800m | | | | Piping | Embankment | | Common Mode |
| | | | | | | | Foundation | Common Mode |
| | | | | Overtopping | | | | Common Mode |
| | Embankment Chg 2550m | | | | Piping | Embankment | | Common Mode |
| | | | | | | | Foundation Upper Clays | Common Mode |
| | | | | | | | Foundation Sands Exposed | Common Mode |
| | | | | | | | Foundation Sands Not Exposed | Common Mode |
| | | | | Overtopping | | | | Common Mode |
| | Embankment Chg 4300m | | | | Piping | Embankment | | Common Mode |
| | | | | | | | Foundation Clays | Common Cause Adjustment for Identified Locations |
| | | | | Overtopping | | | | Common Mode |
| | Embankment Chg 4600m | | | | Piping | Embankment | | Common Cause Adjustment for Ground Level |
| | | | | | | | Foundation Upper Clays | Common Cause Adjustment for Ground Level |
| | | | | | | | Foundation Deep Sands Exposed | Common Cause Adjustment for Identified Locations |
| | | | | | | | Foundation Deep Sands Not Exposed | Common Cause Adjustment for Identified Locations |
| | Embankment Chg 4900m | | | | Piping | Embankment | | Common Cause Adjustment for Ground Level |
| | | | | | | | Foundation Upper Clays | Common Cause Adjustment for Ground Level |
| | | | | | | | Foundation Shallow Sands Exposed | Common Cause Adjustment for Identified Locations |
| | | | | | | | Foundation Shallow Sands Not Exposed | Common Cause Adjustment for Identified Locations |
| | Embankment Chg 5800m | | | | Piping | Embankment | | Isolated Feature |
| | | | | | | | Sheetpile Sands Exposed | Isolated Feature |
| | | | | | | | Sheetpile Sands Not Exposed | Isolated Feature |
| | Embankment Chg 7000m | | | | Piping | Embankment | | Common Mode |
| | | | | | | | Foundation Upper Clays | Common Mode |
| | | | | | | | Foundation Shallow Sands Exposed | Common Mode |
| | | | | | | | Foundation Shallow Sands Not Exposed | Common Mode |
| | | | | Overtopping | | | | Common Mode |
| | | | | | No Failure | | | |

# Use of FMA for Monitoring Equipment installation USBR

## Instrumentation Review Decision Tree

(for each measurement – current or proposed (including surveys)



Is measurement related to an identified failure mode (FM)?

Yes

Is the FM considered to be of practical concern for this dam?

Yes

Is this a direct measure (or significant indirect measure) of a potential FM?

Yes

Is the measurement unnecessarily redundant to other measurements/visual observations?

Yes

Note A

No

Are the measurements adequate to monitor the FM in conjunction with visual monitoring (i.e. precision, reliability, coverage, etc.)?

Yes

Note F

No

Note E

No

Note A

No

Note A

No

Is measurement expected to provide useful information?

Yes

Is there a specific plan to use the data? (i.e. dam behavior research)

Yes

Is data reliable?

Yes

Note D

No

Note B

No

Note C

No

Note B

**Note A** – Read on the minimum frequency necessary to confirm proper functioning of the instrument<br>
**Note B** – Decommission and/or abandon the instrument

**Note C** – Stop measuring, and either place the instrument on standby or decommission/abandon the instrument

**Note D** – Read at the frequency justified by the planned use of the data consistent with the resources dedicated to the planned research

**Note E** – Identify additional visual monitoring and/or measurement consistent with the need for analyzing or reducing risk

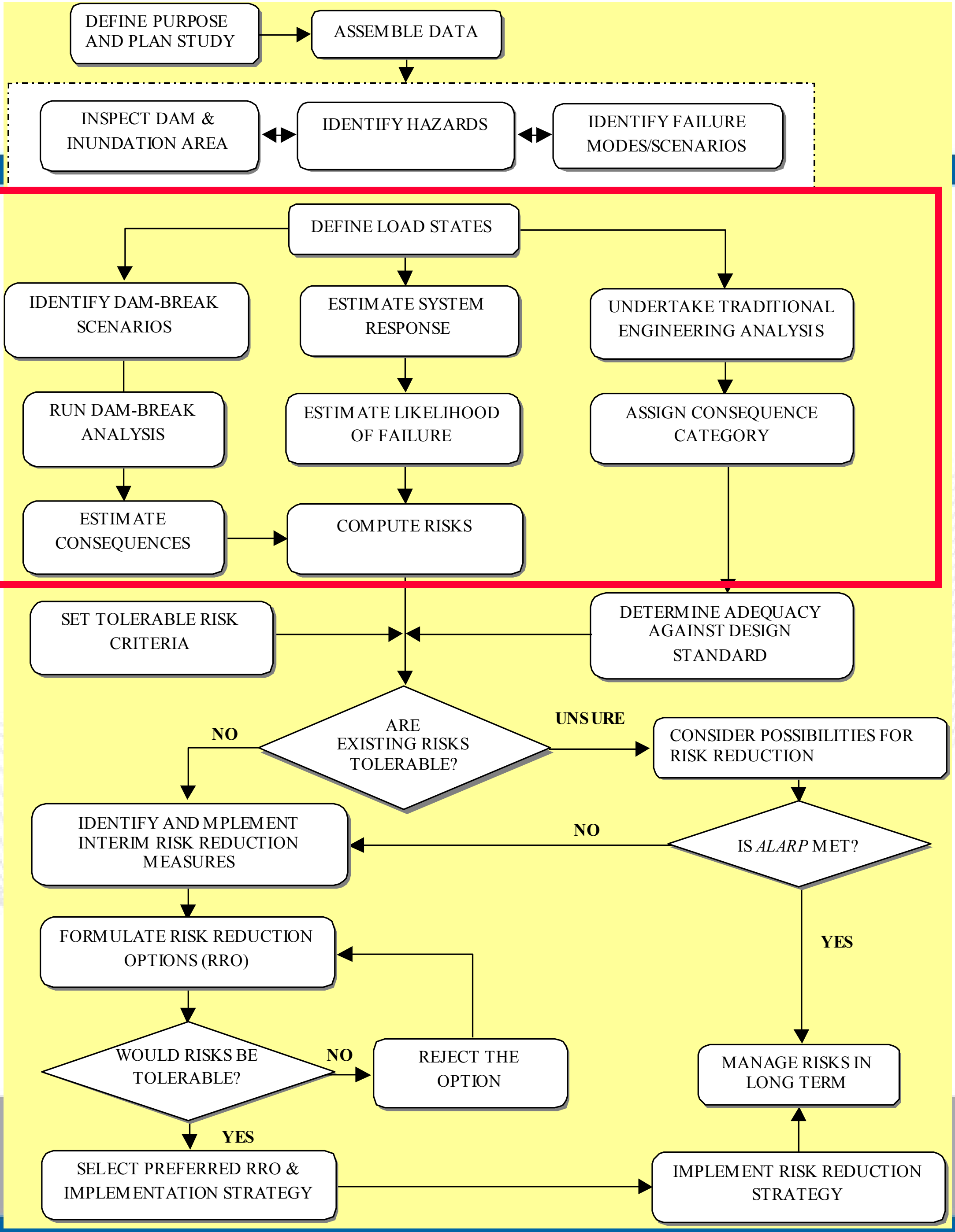
**Note F** – Read on a frequency consistent with use of the measurement in analyzing or reducing risk

# Standards Assessment as part of the RA

- Assessed for the dam or components as appropriate using Safety Factors, Guidelines Standards etc for loading conditions and dam components eg seismic, normal, flood loading.
- Can include:
  - Percentage of Compliance
  - Compliance method
  - Confidence in Assessment

| **Compliance categories for Standards Based Assessment of Dam Safety** | | Sufficient Information is available to make a definitive assessment | |
|---|---|---|---|
| | | Yes | No |
| The dam is assessed to conform with current practice with respect to the particular loading condition | Yes | Pass (P) | Apparent Pass (AP) |
| | No | No pass (NP) | Apparent No Pass (ANP) |

# Risk Analysis Phase



DEFINE PURPOSE AND PLAN STUDY

ASSEMBLE DATA

INSPECT DAM & INUNDATION AREA

IDENTIFY HAZARDS

IDENTIFY FAILURE MODES/SCENARIOS

DEFINE LOAD STATES

IDENTIFY DAM-BREAK SCENARIOS

ESTIMATE SYSTEM RESPONSE

UNDERTAKE TRADITIONAL ENGINEERING ANALYSIS

RUN DAM-BREAK ANALYSIS

ESTIMATE LIKELIHOOD OF FAILURE

ASSIGN CONSEQUENCE CATEGORY

ESTIMATE CONSEQUENCES

COMPUTE RISKS

SET TOLERABLE RISK CRITERIA

DETERMINE ADEQUACY AGAINST DESIGN STANDARD

ARE EXISTING RISKS TOLERABLE?

NO

UNSURE

CONSIDER POSSIBILITIES FOR RISK REDUCTION

IDENTIFY AND MPLEMENT INTERIM RISK REDUCTION MEASURES

NO

IS *ALARP* MET?

YES

FORMULATE RISK REDUCTION OPTIONS (RRO)

WOULD RISKS BE TOLERABLE?

NO

REJECT THE OPTION

MANAGE RISKS IN LONG TERM

YES

SELECT PREFERRED RRO & IMPLEMENTATION STRATEGY

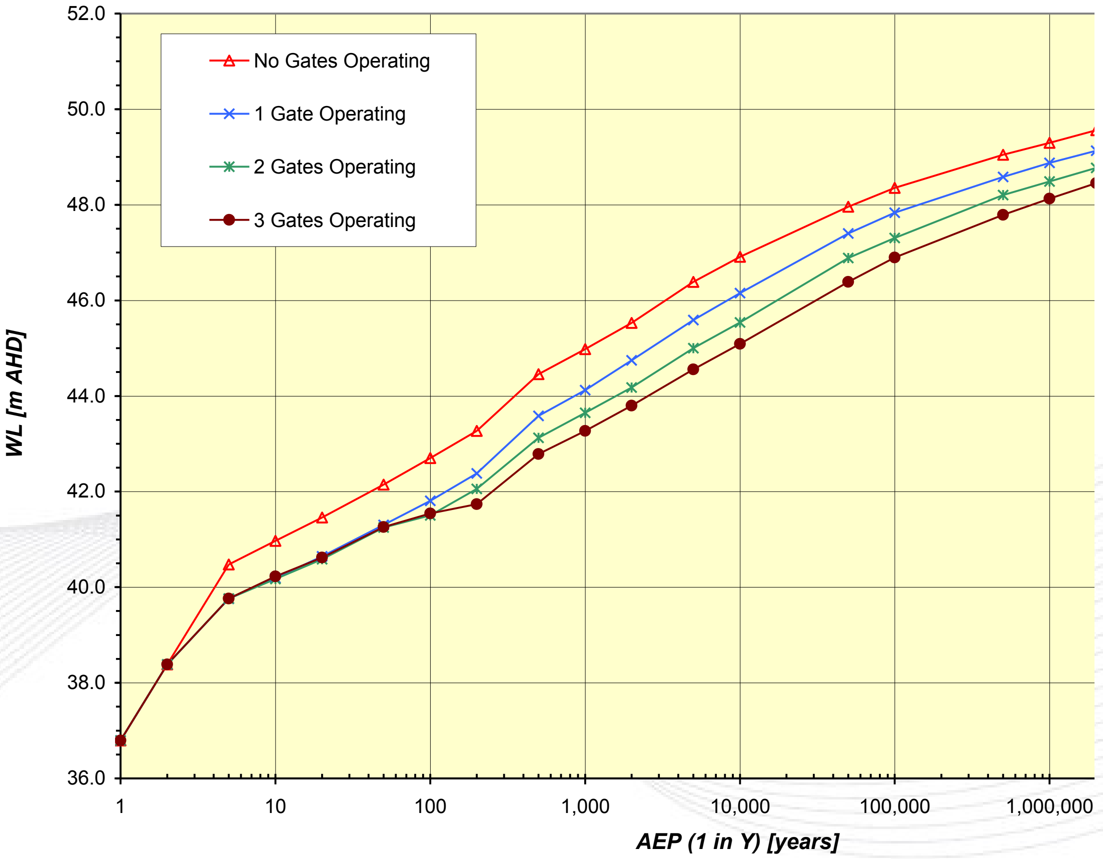
IMPLEMENT RISK REDUCTION STRATEGY

# Define Load States and Scenarios for Analysis

- **Event magnitude versus frequency data for each hazard**
  - ✓ **flood**
  - ✓ **earthquake**
  - ✓ **reservoir level**
  - ✓ **wind**
  - ✓ **etc**

- **Divide the load domain into load states to be used for the analysis – consider the critical events found from the failure modes analysis**

# Spillway Gates and Flood Hydrology



# Quantitative Failure Calculation Methods

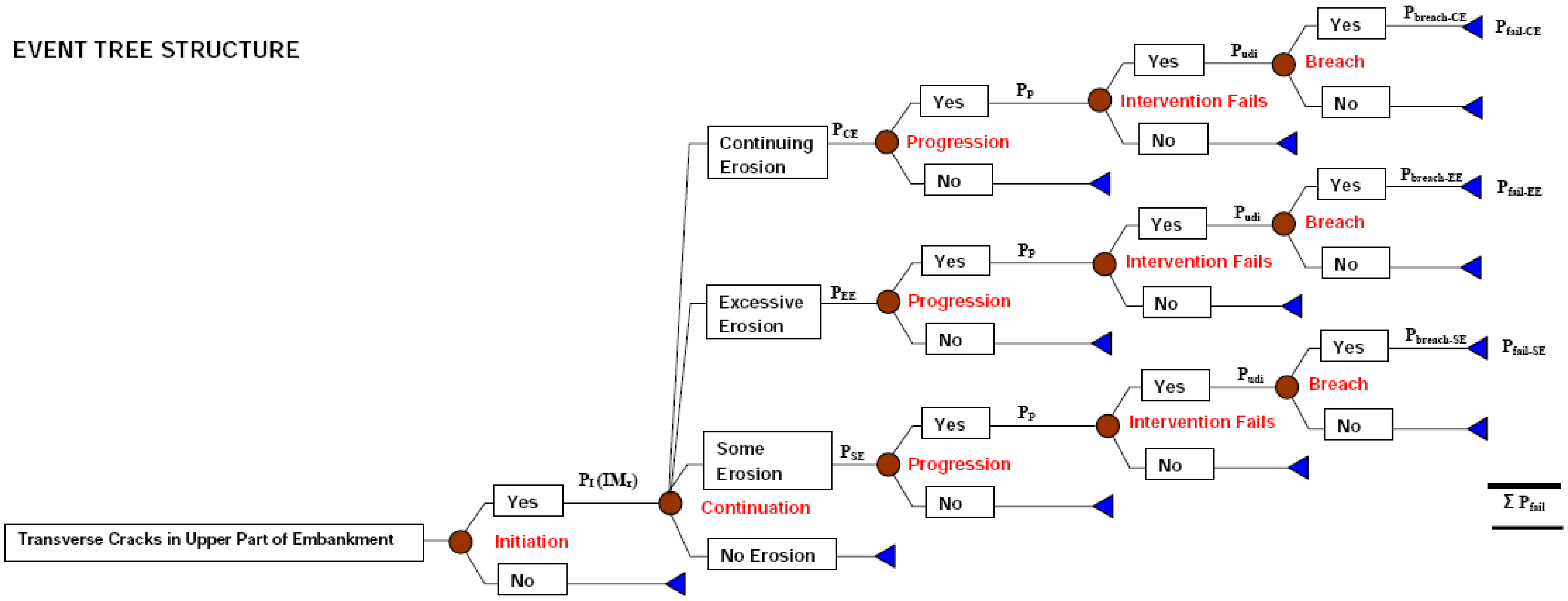
- Structural reliability analysis
  - First order Second Moment (FOSM)
  - Point Estimate Method
  - Monte Carlo
- Historical Failure rates
  - Bayes Theorem
  - Adjustments based on Judgement (UNSW Methods)
- Subjective engineering judgement and Experts (Use more than 1 person with  reasons for assigned numbers which are challenged to reach final numbers)
- Event Trees or Fault Trees - decompose failure mechanisms
- Mapping schemes  - numeric value of probability versus descriptions

Need Sound Logic and accepted scientific knowledge

# Definitions

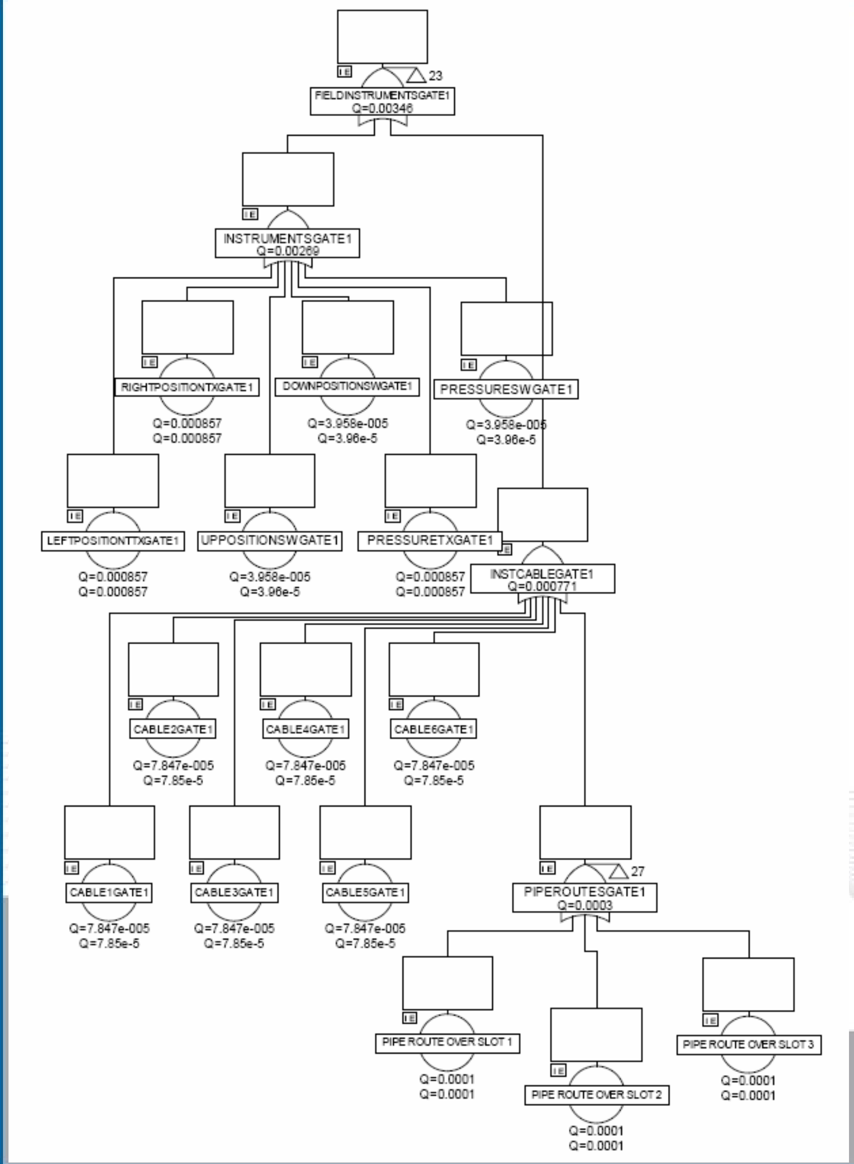
- Mutually Exclusive – When the occurrence of one event precludes the occurrence of another event
  - Flood and drought of a river at the same time
  - Failure and survival of a dam as a result of an earthquake
- Independent Events – If the certain knowledge of the outcome of one would not alter the assessed probability of the other
- Conditional Probability p(B/A) is the probability of B given the certain knowledge that A has occurred
- Positively Correlated – If one failure mode were triggered, would the occurrence of any other failure mode be more likely – if so, these failure modes are positively correlated – Use De Morgan's unimodal bounds theorem for combination.

# Event (Logic) Tree Example



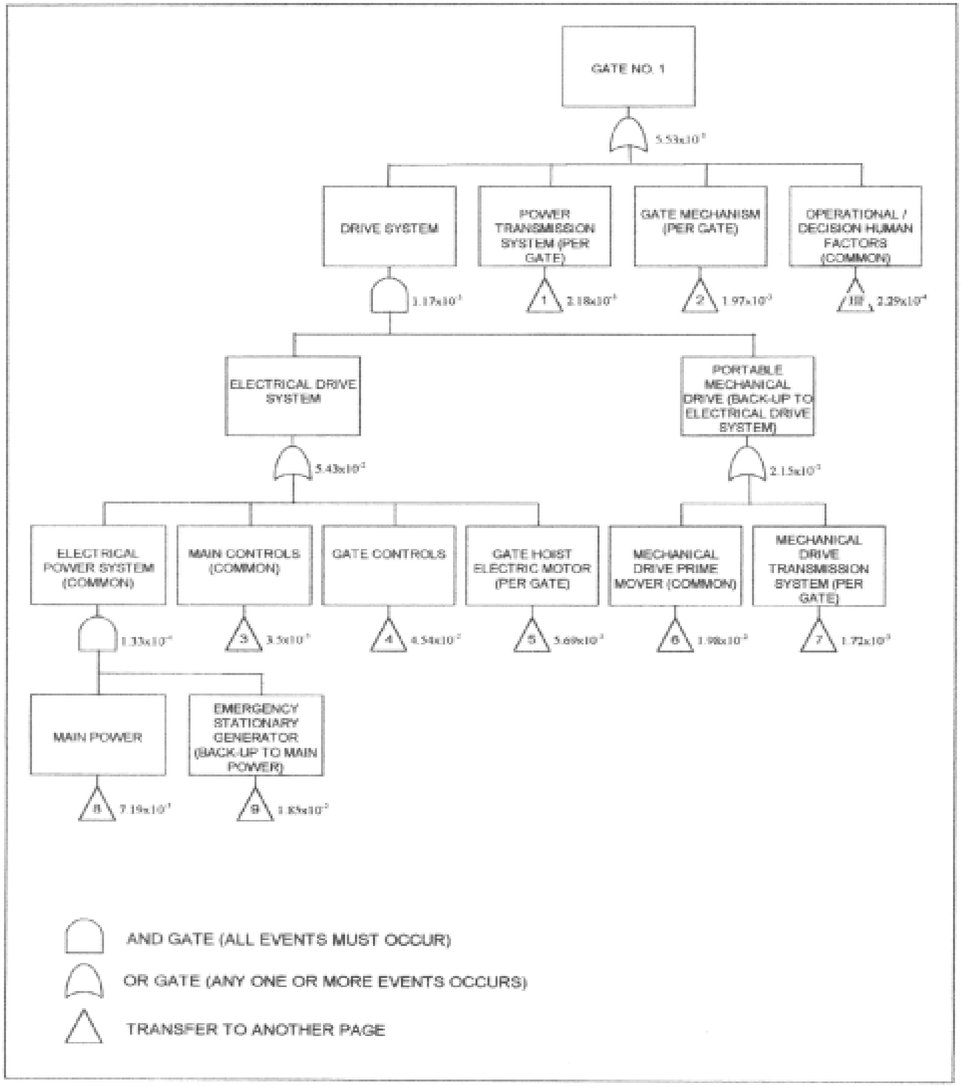
CLIENTS | PEOPLE | PERFORMANCE

# Fault Tree Examples



DAM SPILLWAY RELIABILITY ASSESSMENT

Single Isolated Gate Failure
0Hour

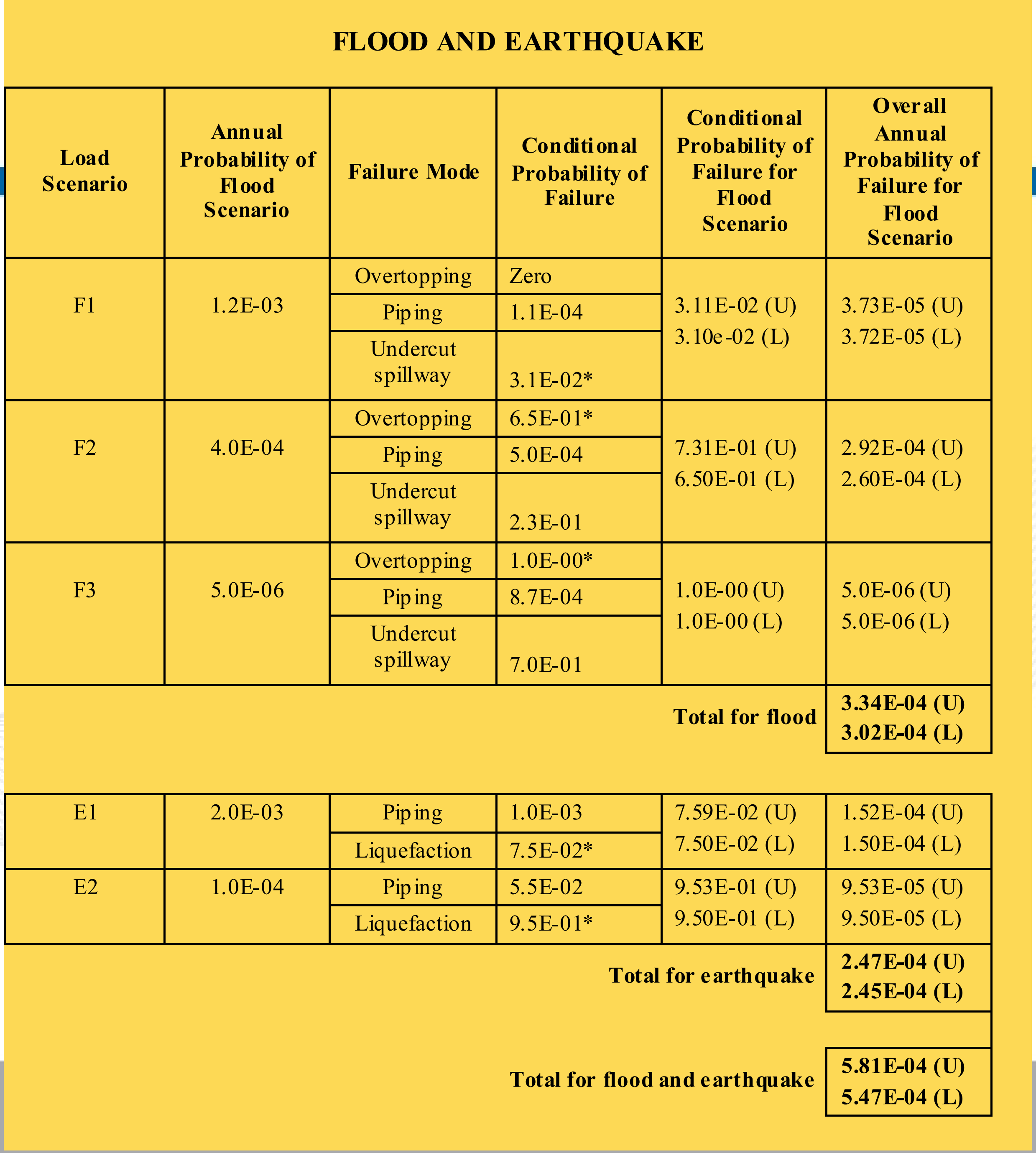

GATE NO. 1
5.53x10^-3
DRIVE SYSTEM
1.17x10^-3
POWER TRANSMISSION SYSTEM (PER GATE)
1
2.18x10^-3
GATE MECHANISM (PER GATE)
2
1.97x10^-3
OPERATIONAL / DECISION HUMAN FACTORS (COMMON)
HF
2.29x10^-4
ELECTRICAL DRIVE SYSTEM
5.43x10^-2
PORTABLE MECHANICAL DRIVE (BACK-UP TO ELECTRICAL DRIVE SYSTEM)
2.15x10^-2
ELECTRICAL POWER SYSTEM (COMMON)
1.33x10^-4
MAIN CONTROLS (COMMON)
3
3.5x10^-3
GATE CONTROLS
4
4.54x10^-2
GATE HOIST ELECTRIC MOTOR (PER GATE)
5
5.69x10^-3
MECHANICAL DRIVE PRIME MOVER (COMMON)
6
1.98x10^-2
MECHANICAL DRIVE TRANSMISSION SYSTEM (PER GATE)
7
1.72x10^-3
MAIN POWER
8
7.19x10^-3
EMERGENCY STATIONARY GENERATOR (BACK-UP TO MAIN POWER)
9
1.85x10^-2

AND GATE (ALL EVENTS MUST OCCUR)

OR GATE (ANY ONE OR MORE EVENTS OCCURS)

TRANSFER TO ANOTHER PAGE

# Example Probability calculation



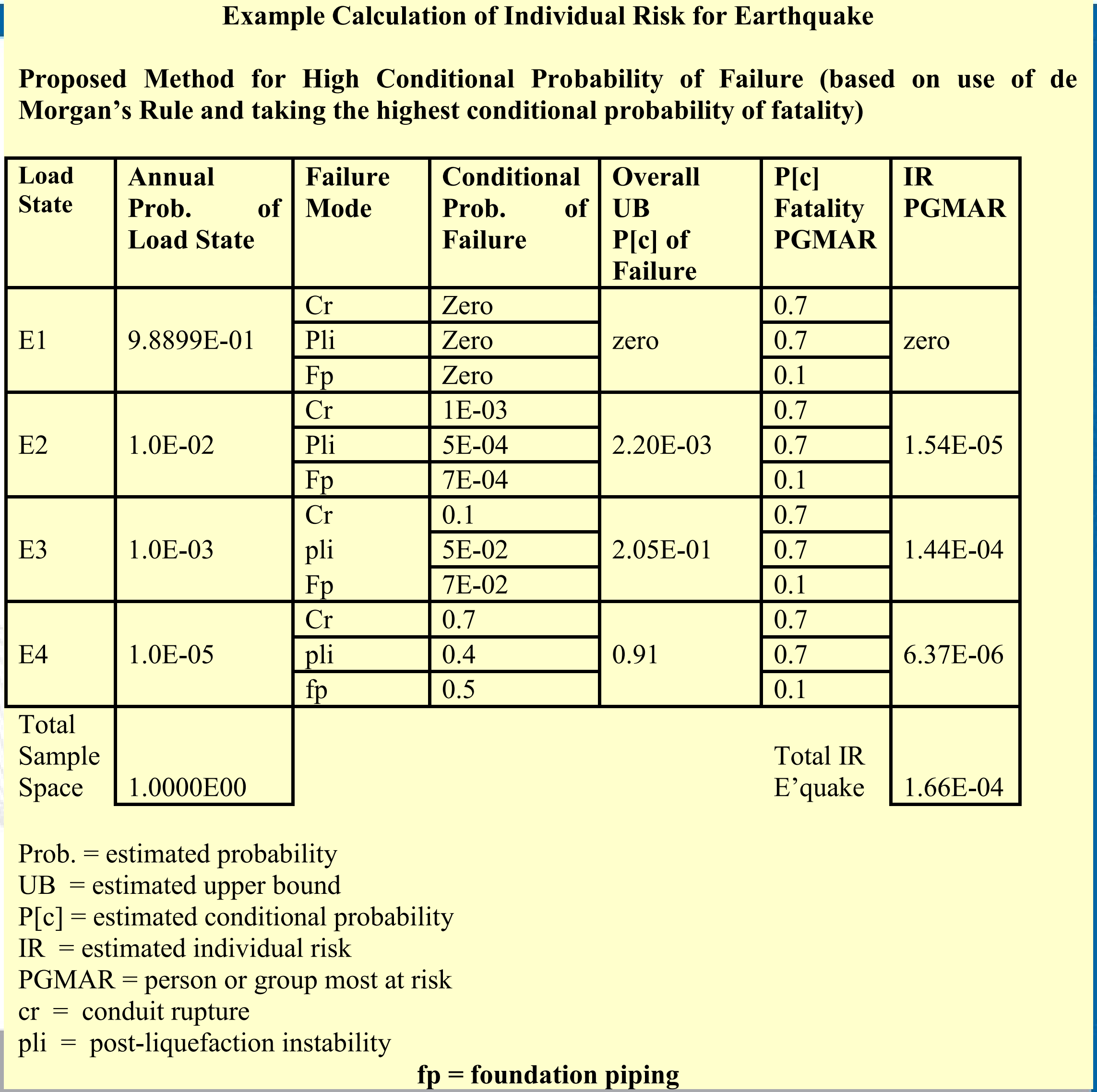
## FLOOD AND EARTHQUAKE

| Load Scenario | Annual Probability of Flood Scenario | Failure Mode | Conditional Probability of Failure | Conditional Probability of Failure for Flood Scenario | Overall Annual Probability of Failure for Flood Scenario |
|---|---|---|---|---|---|
| F1 | 1.2E-03 | Overtopping | Zero | 3.11E-02 (U)<br>3.10e-02 (L) | 3.73E-05 (U)<br>3.72E-05 (L) |
| | | Piping | 1.1E-04 | | |
| | | Undercut spillway | 3.1E-02* | | |
| F2 | 4.0E-04 | Overtopping | 6.5E-01* | 7.31E-01 (U)<br>6.50E-01 (L) | 2.92E-04 (U)<br>2.60E-04 (L) |
| | | Piping | 5.0E-04 | | |
| | | Undercut spillway | 2.3E-01 | | |
| F3 | 5.0E-06 | Overtopping | 1.0E-00* | 1.0E-00 (U)<br>1.0E-00 (L) | 5.0E-06 (U)<br>5.0E-06 (L) |
| | | Piping | 8.7E-04 | | |
| | | Undercut spillway | 7.0E-01 | | |
| | | | | **Total for flood** | **3.34E-04 (U)**<br>**3.02E-04 (L)** |
| E1 | 2.0E-03 | Piping | 1.0E-03 | 7.59E-02 (U)<br>7.50E-02 (L) | 1.52E-04 (U)<br>1.50E-04 (L) |
| | | Liquefaction | 7.5E-02* | | |
| E2 | 1.0E-04 | Piping | 5.5E-02 | 9.53E-01 (U)<br>9.50E-01 (L) | 9.53E-05 (U)<br>9.50E-05 (L) |
| | | Liquefaction | 9.5E-01* | | |
| | | | | **Total for earthquake** | **2.47E-04 (U)**<br>**2.45E-04 (L)** |
| | | | | **Total for flood and earthquake** | **5.81E-04 (U)**<br>**5.47E-04 (L)** |

# Individual Risk

Existing Dams 10 $^{-4}$ per annum

New Dams 10 $^{-5}$ per annum



**Example Calculation of Individual Risk for Earthquake**

**Proposed Method for High Conditional Probability of Failure (based on use of de Morgan's Rule and taking the highest conditional probability of fatality)**

| Load State | Annual Prob. of Load State | Failure Mode | Conditional Prob. of Failure | Overall UB P[c] of Failure | P[c] Fatality PGMAR | IR PGMAR |
|---|---|---|---|---|---|---|
| E1 | 9.8899E-01 | Cr | Zero | zero | 0.7 | zero |
| | | Pli | Zero | | 0.7 | |
| | | Fp | Zero | | 0.1 | |
| E2 | 1.0E-02 | Cr | 1E-03 | 2.20E-03 | 0.7 | 1.54E-05 |
| | | Pli | 5E-04 | | 0.7 | |
| | | Fp | 7E-04 | | 0.1 | |
| E3 | 1.0E-03 | Cr | 0.1 | 2.05E-01 | 0.7 | 1.44E-04 |
| | | pli | 5E-02 | | 0.7 | |
| | | Fp | 7E-02 | | 0.1 | |
| E4 | 1.0E-05 | Cr | 0.7 | 0.91 | 0.7 | 6.37E-06 |
| | | pli | 0.4 | | 0.7 | |
| | | fp | 0.5 | | 0.1 | |
| Total Sample Space | 1.0000E00 | | | | Total IR E'quake | 1.66E-04 |

Prob. = estimated probability
UB = estimated upper bound
P[c] = estimated conditional probability
IR = estimated individual risk
PGMAR = person or group most at risk
cr = conduit rupture
pli = post-liquefaction instability

**fp = foundation piping**

# Calculate Overall Probabilities

- Combine the estimated annual probabilities of load states/scenarios or failure initiation with the conditional probabilities of failure to obtain the estimate of overall annual probability of failure.
- Mutually exclusive failure modes or independent events - additive
- Not mutually exclusive failure modes – De Morgans Theorem before multiplying by annual likelihood of being in load state
- Check logic of the event tree to ensure dimensions are correct for the failure calculations

# Always Keep in mind

- The buzzwords and know how to deal with them
  - Mutually exclusive failure modes
  - Common cause of failure
  - Common mode of failure
- Length effects for n sections using Unimodal Bounds theory of de Morgan $P_{failure} = 1-(1-p)^n$;
- Event tree probabilities are conditional on the preceding events;
- Fault tree analysis – rules for development;
- All probabilities must be consistent;
- Conditional probabilities must be combined and adjusted before calculation of annual failure probability.

# Risk Integration

- Common cause Adjustment

  Failure Modes Not Mutually Exclusive
  Unimodal Bounds theorem

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

or

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

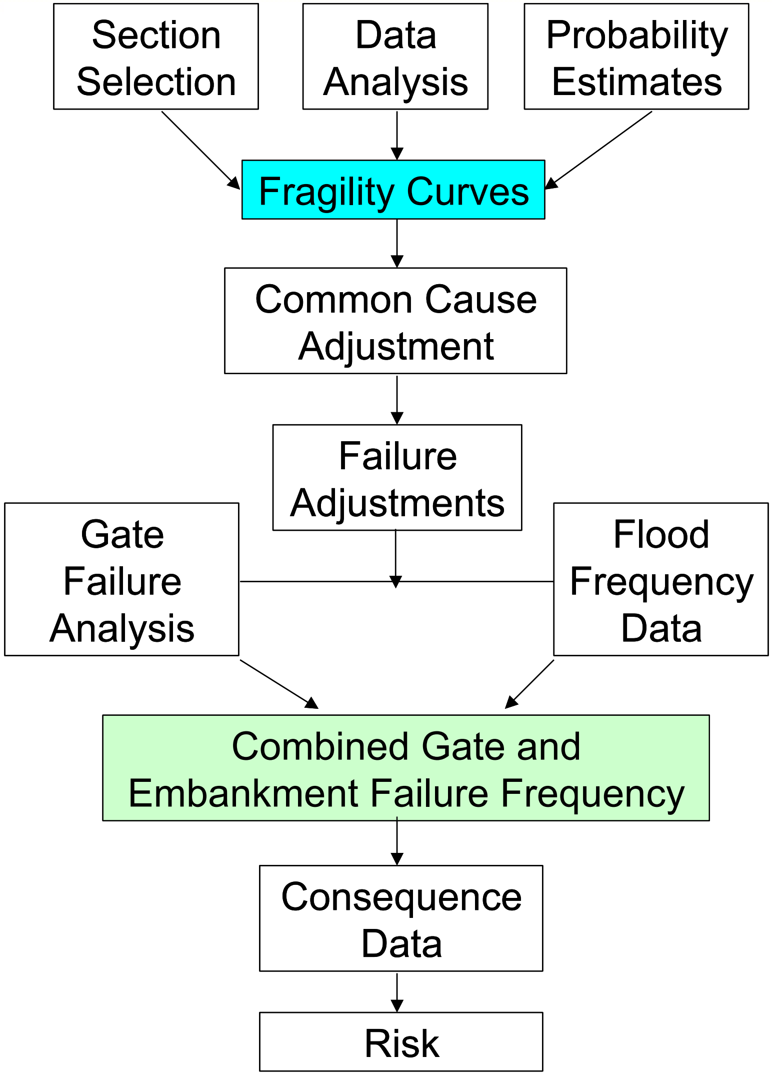
- Adjustment of all probabilities

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

Where:

$p_i$ = branch failure probability

$p_f$ = total probability of failure



# Example of Combining Probabilities

| Water Level | Minimum Probability | Min (Max Mode) | Total Sum | Common Cause | Adjustment |
|---|---|---|---|---|---|
| **34.40** | 1.24E-07 | Found - Chg700m Fnd Sand Exp - Trench | 1.3165E-07 | 1.3165E-07 | 1.0000 |
| **38.55** | 1.73E-07 | Found - Chg700m Fnd Sand Exp - Trench | 2.8664E-07 | 2.8664E-07 | 1.0000 |
| **41.20** | 1.11E-06 | Found - Chg700m Fnd Sand Exp - Trench | 2.1312E-06 | 2.1312E-06 | 1.0000 |
| **43.20** | 7.70E-06 | Spill - Spillway Emb Ers & Ovtp | 3.7173E-05 | 3.7172E-05 | 1.0000 |
| **45.20** | 7.70E-05 | Spill - Spillway Emb Ers & Ovtp | 2.2537E-04 | 2.2535E-04 | 0.9999 |
| **47.50** | 4.30E-02 | O'Top - Chg 2550m | 1.9586E-01 | 1.8095E-01 | 0.9239 |
| **49.00** | 1.00E+00 | O'Top - Chg 7000m | 5.0059E+00 | 1.0000E+00 | 0.1998 |

$$\max_i [p_i]$$

$$Total\,p_f = \sum p_i$$

$$p_f = 1 - \prod_{i=1}^{k} (1 - p_i)$$

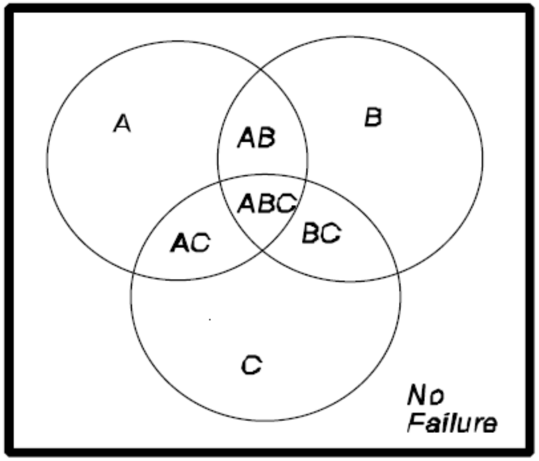
$$p_i^u = p_i (p_f^u / p_f)$$

GHD CLIENTS | PEOPLE | PERFORMANCE

# Combining Failure Probabilities

- The following outcomes are not mutually exclusive since any one or a combination could occur. If summed, they add to more than 1.0. Adjustment can be done as follows:

| Outcome | Failure Probability |
|---|---|
| A) Structural Failure of the Arch Dam | 0.7 |
| B) Failure of a Foundation Block on the Abutment | 0.5 |
| C) Failure of the Thrust Block | 0.5 |



Step 1: Compute the probability of no failure occuring

P[No Failure] (probability of no failure) = (1 - P[A]) x (1 - P[B]) x (1 - P[C])

= (1 - .7) x (1 - .5) x (1 - .5)

= (.3 x .5 x .5) = 0.075

Step 2. - Allocate a failure probability of (1- .075) = .925 among the failure modes.

P[A] = (.925/1.7) * .7 = 0.381
P[B] = (.925/1.7) * .5 = 0.272
P[C] = (.925/1.7) * .5 = 0.272

# Probability in Context

- Probability is the analyst's or analysis team's degree of confidence in an outcome;
- that the degree of confidence is based on evidence; that is, the knowledge and data available at the time;
- probability may change as knowledge and information changes.

***Probability has no objective reality but is rather a reflection of the of the state of mind of the analysts or team, given the available knowledge and data concerning the question at issue***

- Subjective probability has a place using a transparent process to derive probabilities

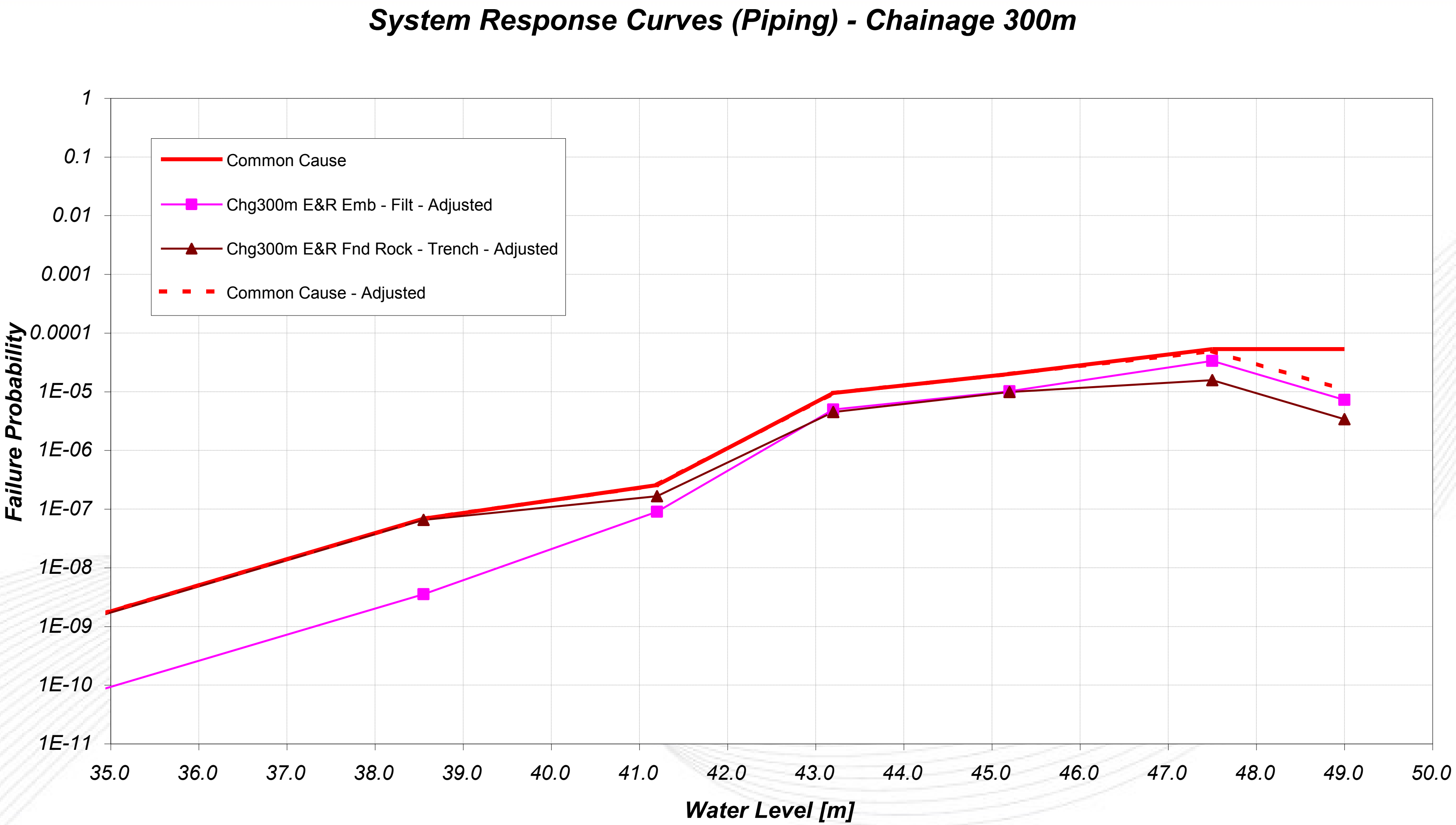
CLIENTS | PEOPLE | PERFORMANCE

# Mapping Scheme for Probability (Barneich et al 1996)

| Description of Condition or Event | Order of Magnitude of Probability Assigned |
|---|---|
| Occurrence is virtually certain | 1 |
| Occurrence of the condition or event are observed in the available database | $10^{-1}$ |
| The occurrence of the condition or event is not observed, or is observed in one isolated instance, in the available database; several potential failure scenarios can be identified. | $10^{-2}$ |
| The occurrence of the condition or event is not observed in the available database. It is difficult to think about any plausible failure scenario; however, a single scenario could be identified after considerable effort. | $10^{-3}$ |
| The condition or event has not been observed, and no plausible scenario could be identified, even after considerable effort. | $10^{-4}$ |

GHD CLIENTS | PEOPLE | PERFORMANCE

# System Response Curves



# Recent Developments in Analysis

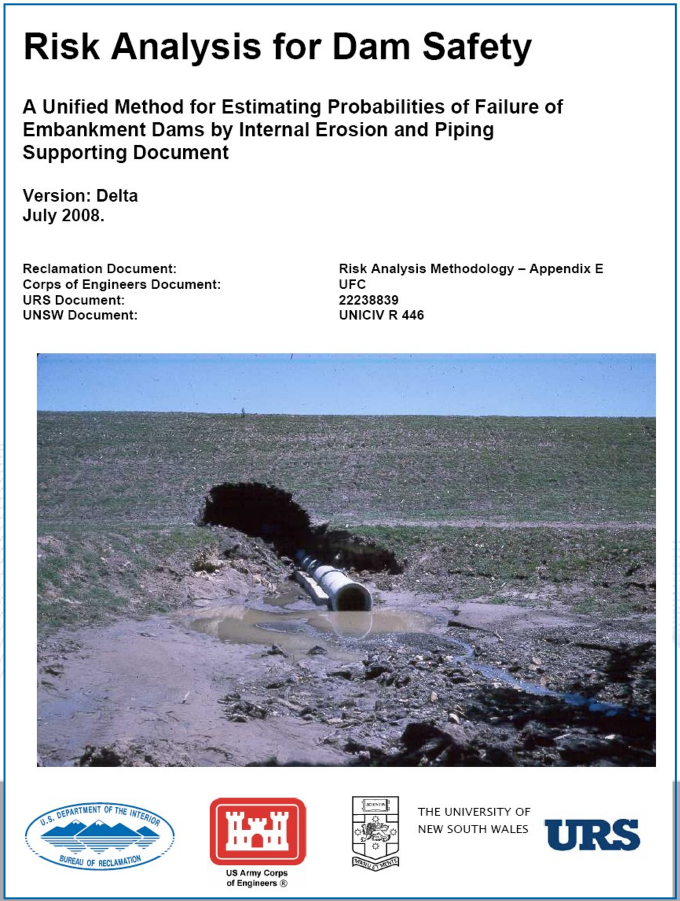
- Internal Erosion and Piping
- Life Loss Models

Tunbridge dam

Zoeknog dam

# Internal Erosion and Piping

- Collaborative effort by Reclamation, USACE, UNSW & URS



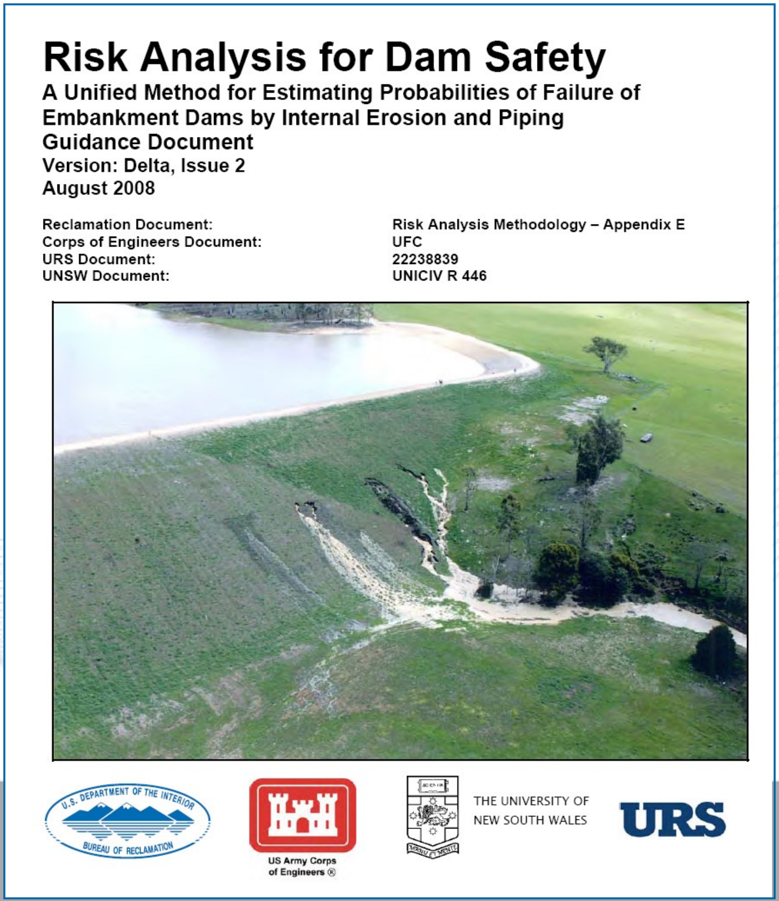
## Risk Analysis for Dam Safety

A Unified Method for Estimating Probabilities of Failure of Embankment Dams by Internal Erosion and Piping
Supporting Document

Version: Delta
July 2008.

| | |
|---|---|
| Reclamation Document: | Risk Analysis Methodology – Appendix E |
| Corps of Engineers Document: | UFC |
| URS Document: | 22238839 |
| UNSW Document: | UNICIV R 446 |

U.S. DEPARTMENT OF THE INTERIOR BUREAU OF RECLAMATION
US Army Corps of Engineers ®
THE UNIVERSITY OF NEW SOUTH WALES
URS



## Risk Analysis for Dam Safety

A Unified Method for Estimating Probabilities of Failure of Embankment Dams by Internal Erosion and Piping
Guidance Document
Version: Delta, Issue 2
August 2008

| | |
|---|---|
| Reclamation Document: | Risk Analysis Methodology – Appendix E |
| Corps of Engineers Document: | UFC |
| URS Document: | 22238839 |
| UNSW Document: | UNICIV R 446 |

U.S. DEPARTMENT OF THE INTERIOR BUREAU OF RECLAMATION
US Army Corps of Engineers ®
THE UNIVERSITY OF NEW SOUTH WALES
URS

# Internal Erosion Framework

- Reservoir Rises
  - Initiation – Flaw exists[1]
    - Initiation – Erosion starts
      - Continuation– Unfiltered exit exists (consider: no erosion/some erosion/excessive erosion/continuing erosion)
        - Progression – Roof forms to support a pipe
          - Progression – Upstream zone fails to fill crack
            - Progression – Upstream zone fails to limit flows
              - Intervention fails
                - Dam breaches (consider all likely breach mechanisms)
                  - Consequences occur

[1] For Backward Erosion Piping failure modes, no flaw is required. In the case of BEP, initiation assesses the soil type, gradient and heave potential.

# Consequences

Three elements:

- Dambreak
- Floodrouting
- Consequence Evaluation

# Risk Calculation

- Societal Risk (f~N and FN Curves)
- Individual Risk (Most exposed group and conditional probability of dam failure and loss of life)
- Financial Risk (f~$ and F$)
- Other Risks

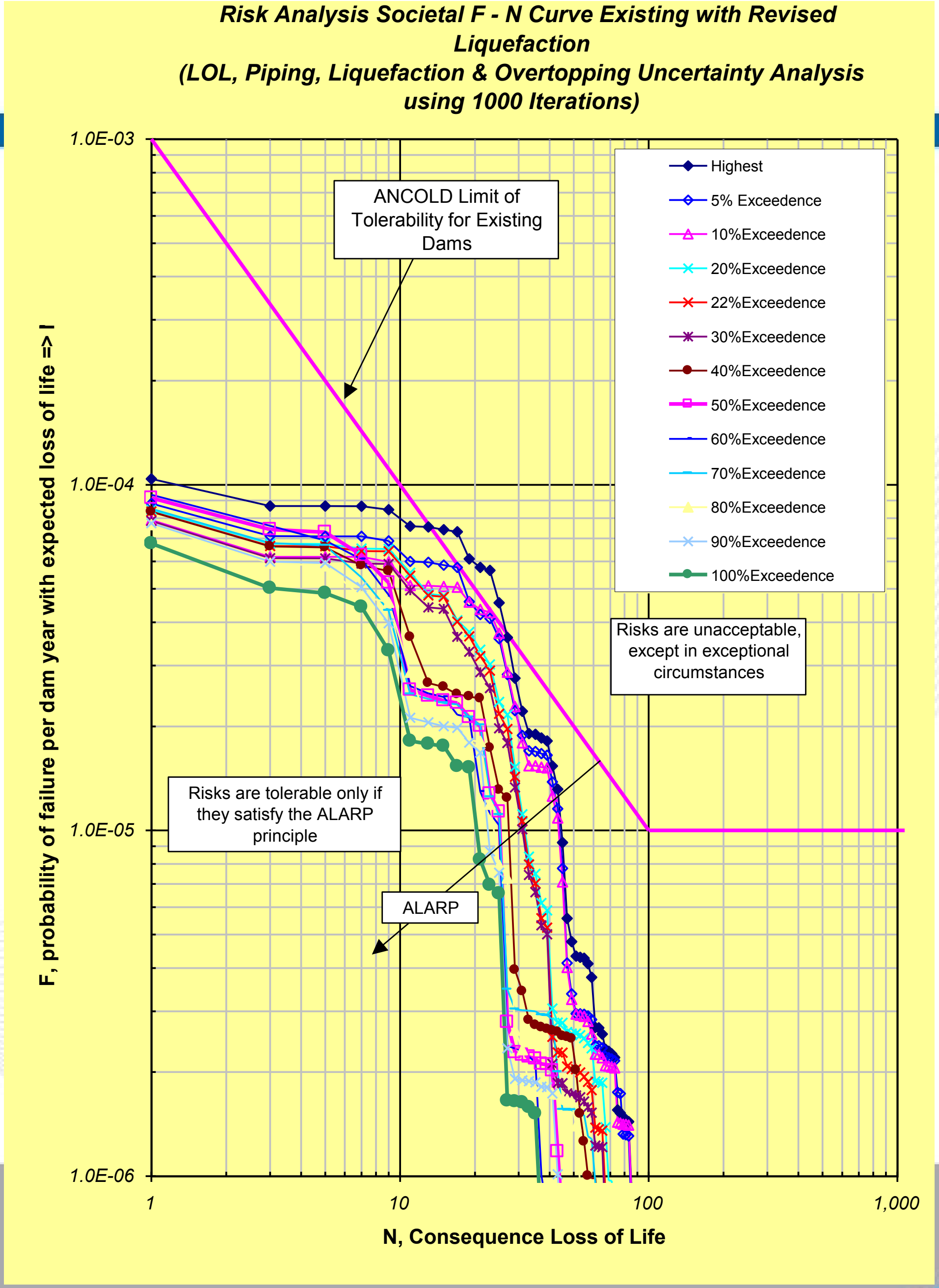
# Uncertainty

- Model or data uncertainty due to randomness in nature
- This is a key area for the development of improved procedures.
- Carry uncertainty through the analysis
- Sensitivity testing

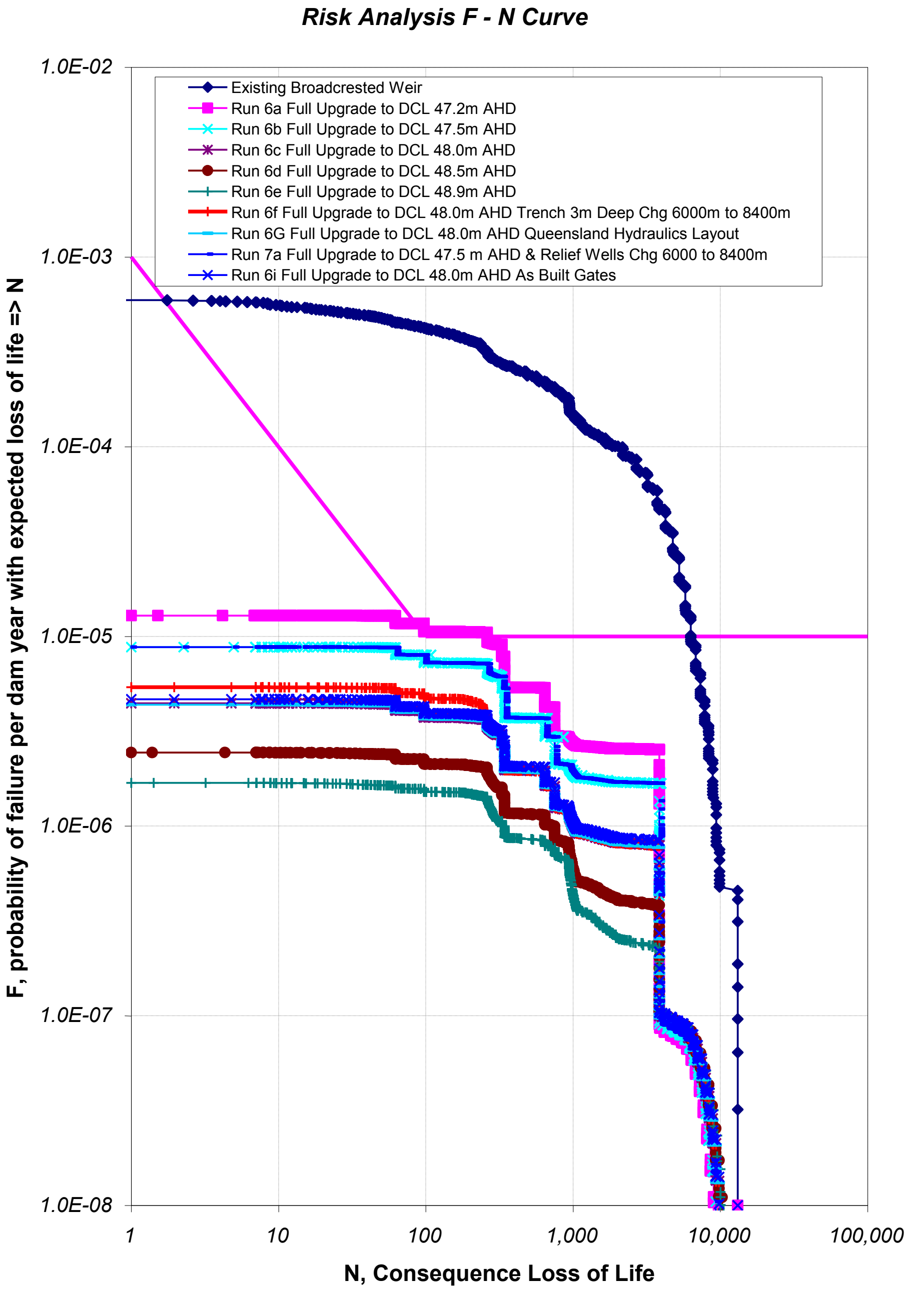
**In general, we identify key variables affecting uncertainty and estimate their impact on the results**

CLIENTS | PEOPLE | PERFORMANCE

# Societal Risk Uncertainty Analysis Results



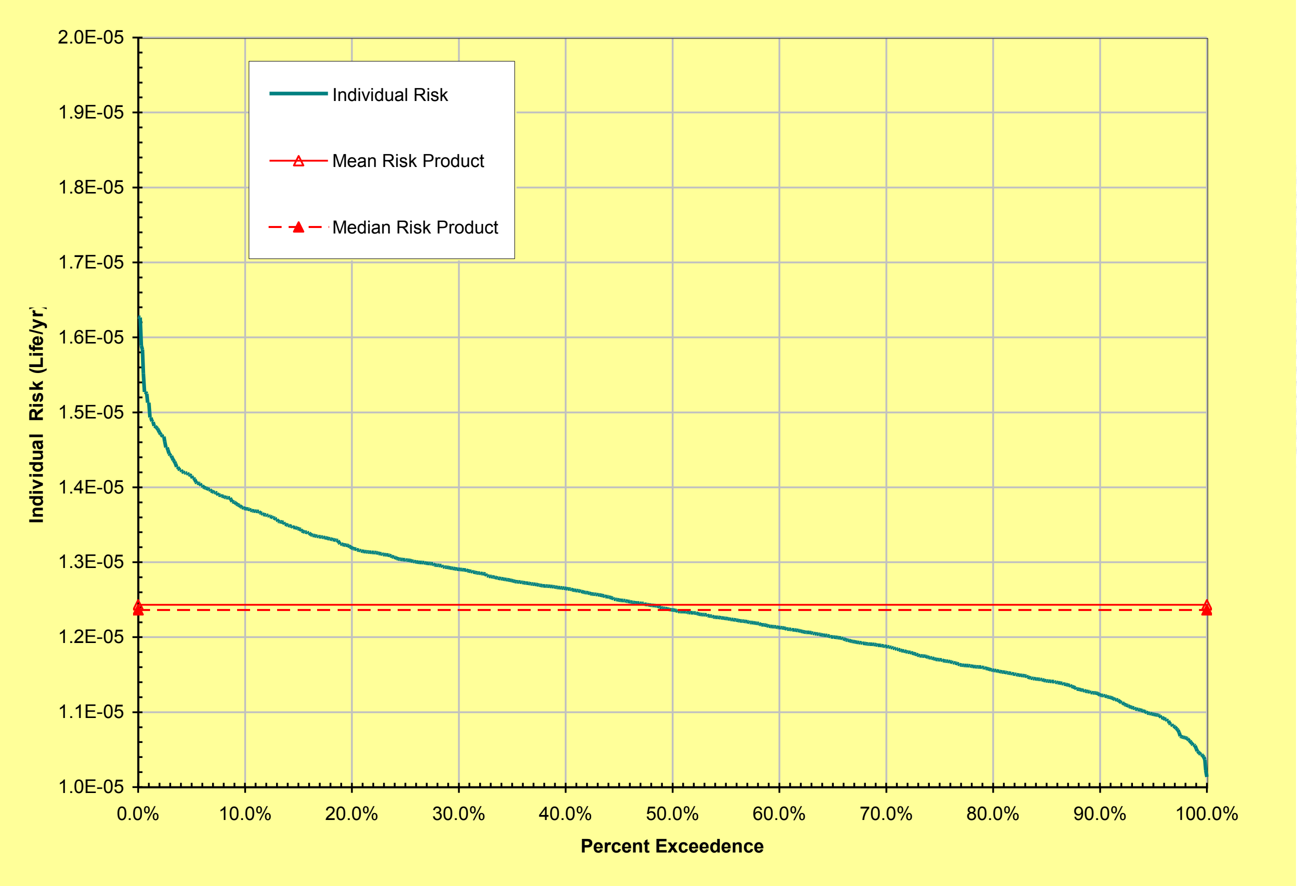
# Risk Analysis Output example for Societal Risk with Upgrade Options



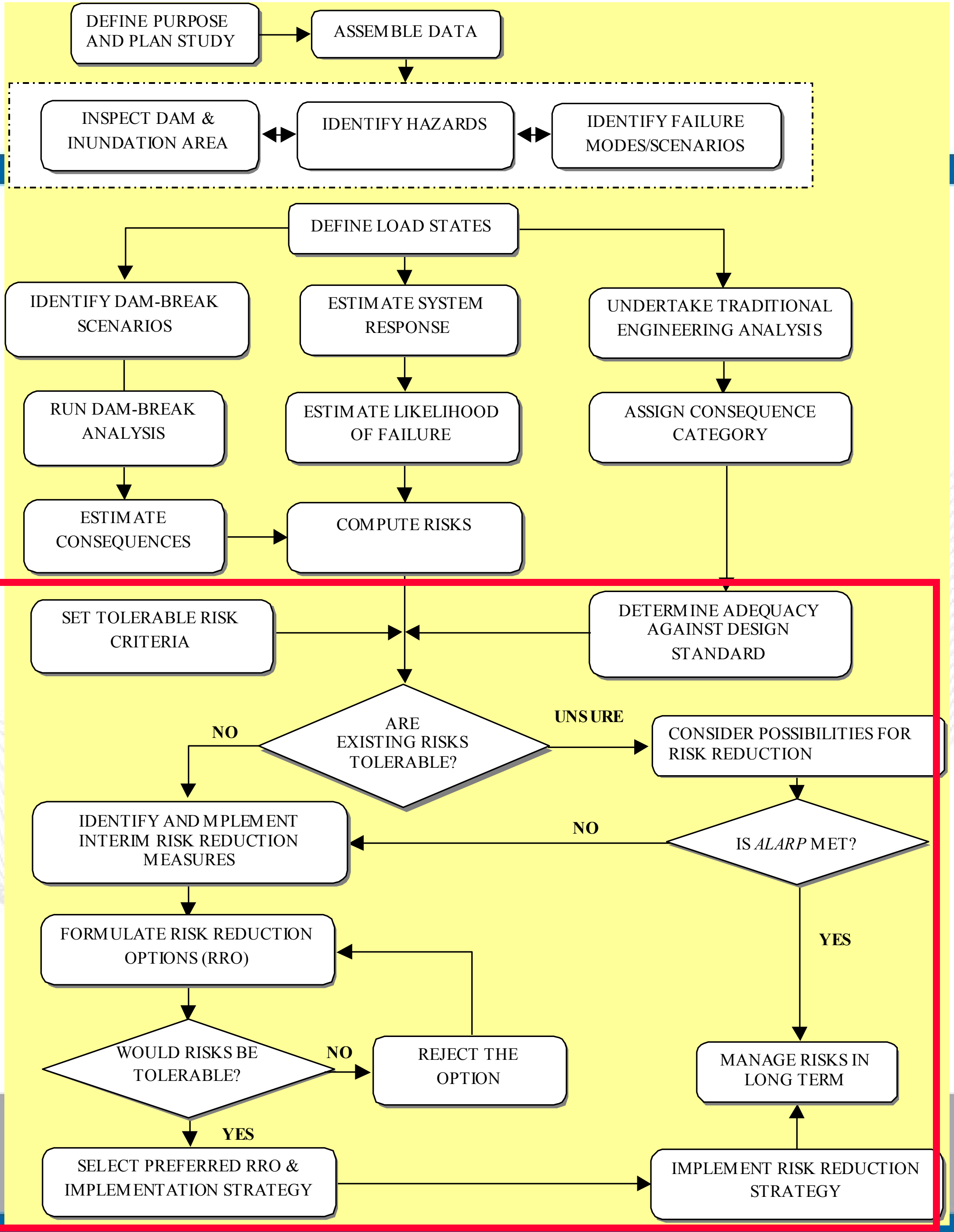
# Individual Risk Output with Uncertainty

Existing Dams $10^{-4}$ per annum

New Dams $10^{-5}$ per annum



# Risk Evaluation Phase



DEFINE PURPOSE AND PLAN STUDY

ASSEMBLE DATA

INSPECT DAM & INUNDATION AREA

IDENTIFY HAZARDS

IDENTIFY FAILURE MODES/SCENARIOS

DEFINE LOAD STATES

IDENTIFY DAM-BREAK SCENARIOS

ESTIMATE SYSTEM RESPONSE

UNDERTAKE TRADITIONAL ENGINEERING ANALYSIS

RUN DAM-BREAK ANALYSIS

ESTIMATE LIKELIHOOD OF FAILURE

ASSIGN CONSEQUENCE CATEGORY

ESTIMATE CONSEQUENCES

COMPUTE RISKS

SET TOLERABLE RISK CRITERIA

DETERMINE ADEQUACY AGAINST DESIGN STANDARD

ARE EXISTING RISKS TOLERABLE?

NO

UNSURE

CONSIDER POSSIBILITIES FOR RISK REDUCTION

IDENTIFY AND MPLEMENT INTERIM RISK REDUCTION MEASURES

NO

IS *ALARP* MET?

FORMULATE RISK REDUCTION OPTIONS (RRO)

YES

WOULD RISKS BE TOLERABLE?

NO

REJECT THE OPTION

MANAGE RISKS IN LONG TERM

YES

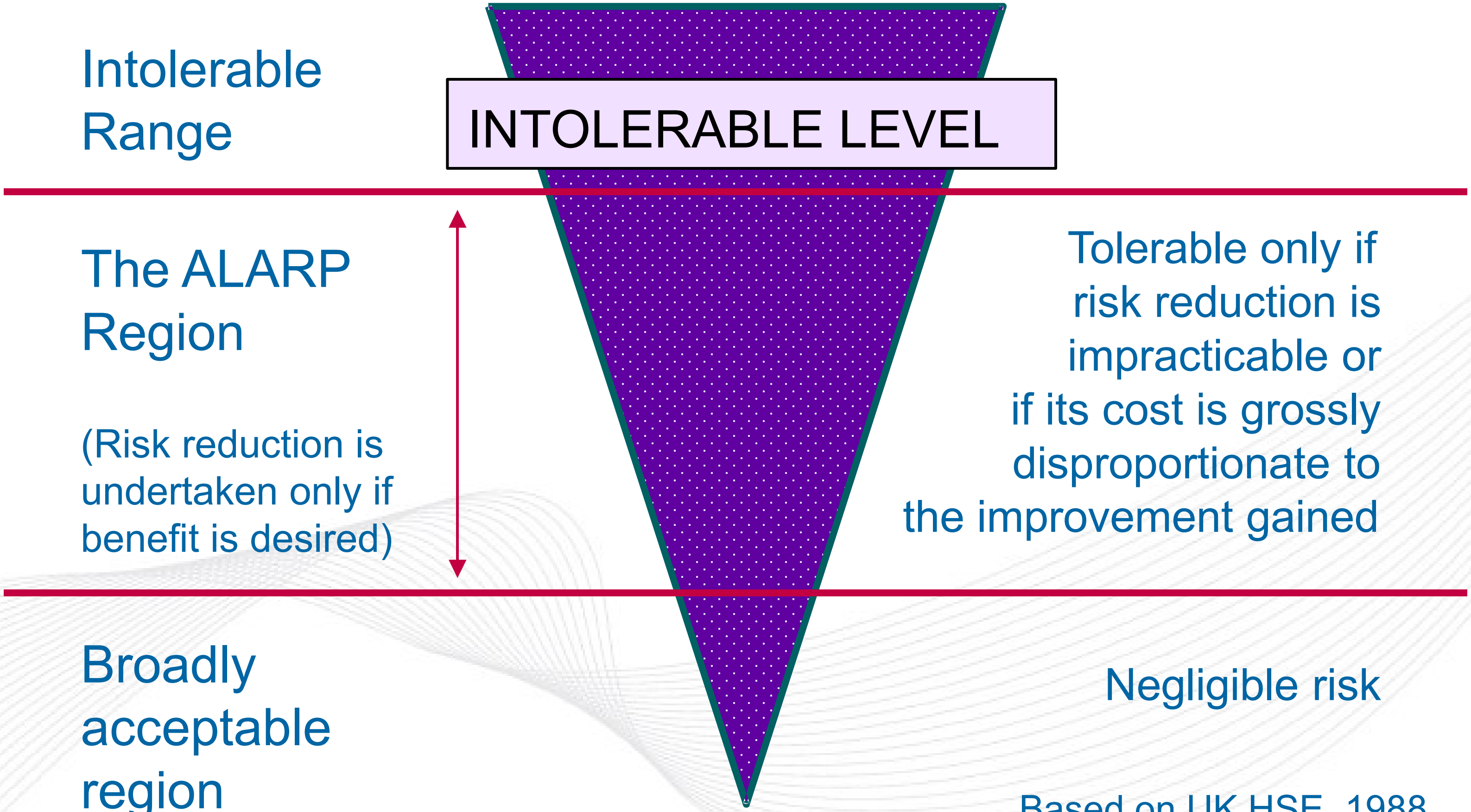
SELECT PREFERRED RRO & IMPLEMENTATION STRATEGY

IMPLEMENT RISK REDUCTION STRATEGY

# Criteria to Evaluate Risk

- Societal
- Individual Risk
- Financial
- Environmental
- ALARP (As Low As Reasonably Practicable)
  - cost-to-save-a-statistical-life (CSSL);
  - whether good practice is met;
  - the level of the existing risk;
  - societal concerns;
  - affordability is not a consideration.

# Levels of Risk & ALARP



Intolerable Range

INTOLERABLE LEVEL

The ALARP Region

(Risk reduction is undertaken only if benefit is desired)

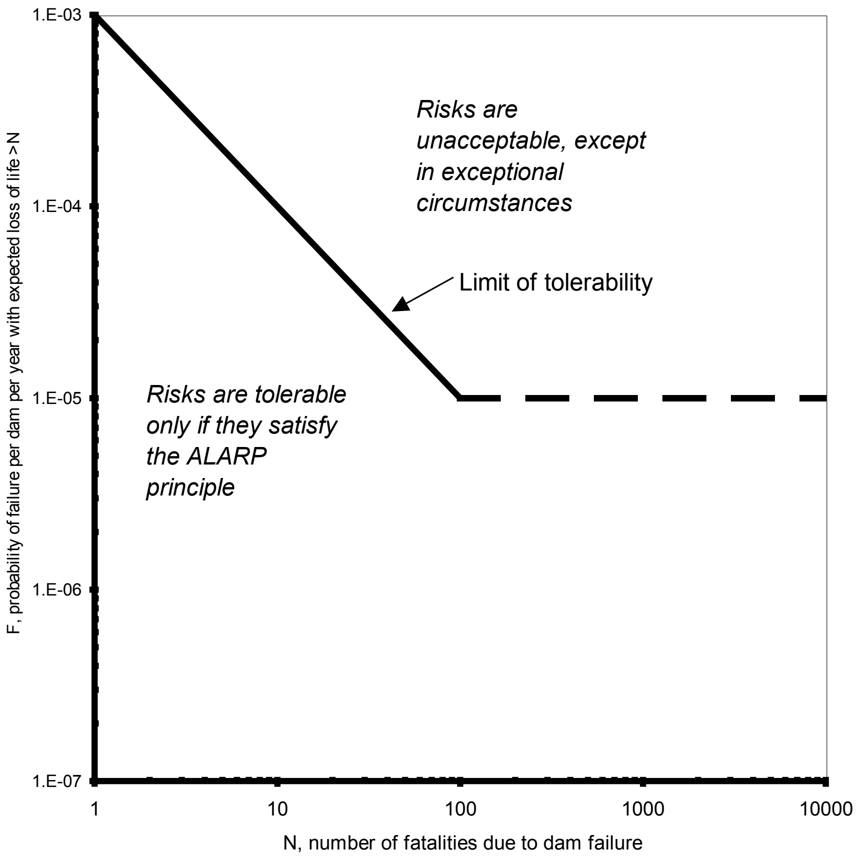
Tolerable only if risk reduction is impracticable or if its cost is grossly disproportionate to the improvement gained

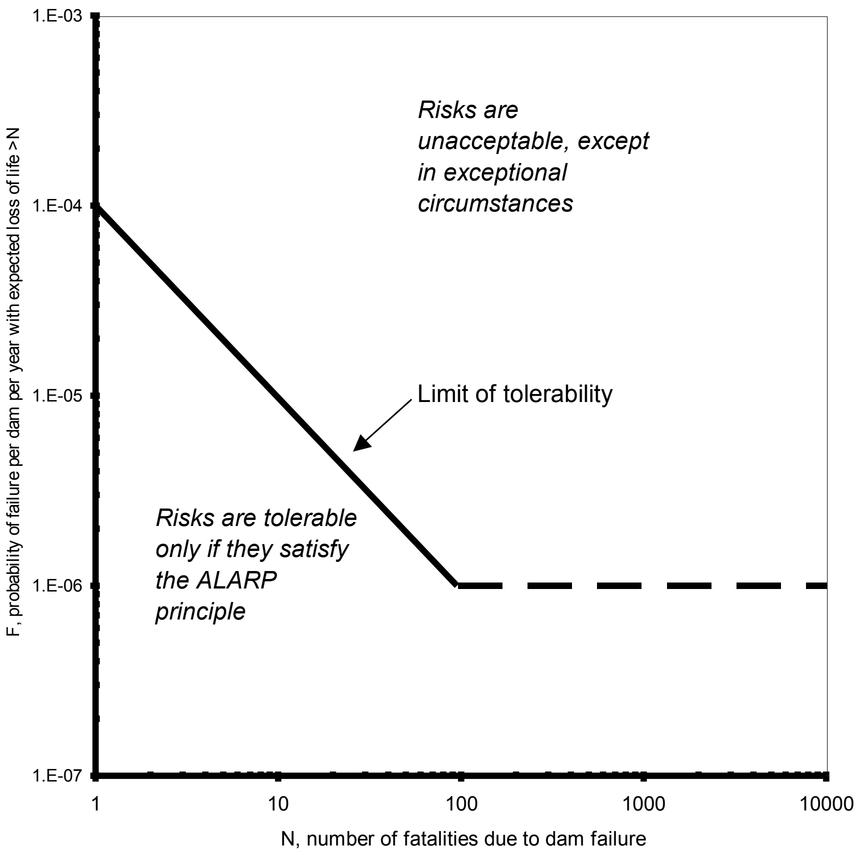
Broadly acceptable region

Negligible risk

Based on UK HSE, 1988

# ANCOLD Societal Risk Acceptance Criteria



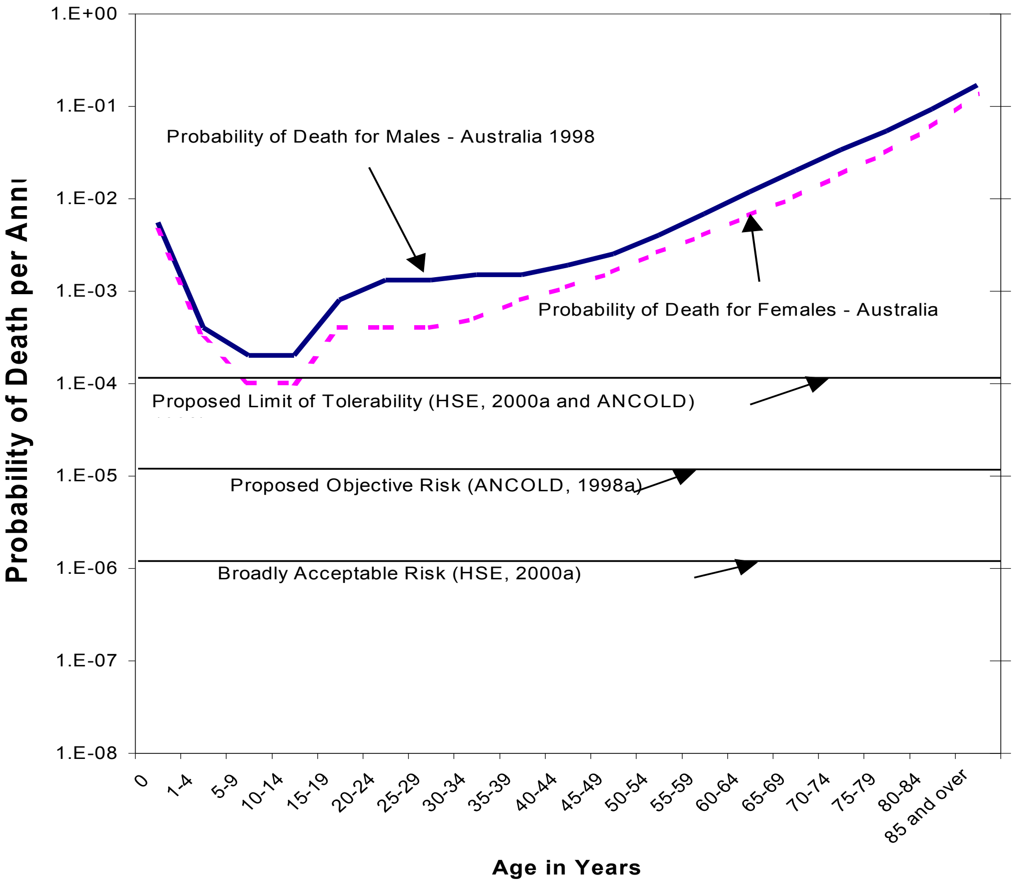


# Individual Risk Criteria

- Average Background Risk = $1 \times 10^{-4}$
- Existing dams $1 \times 10^{-4}$

  (1 in 10,000)
- New dams $1 \times 10^{-5}$

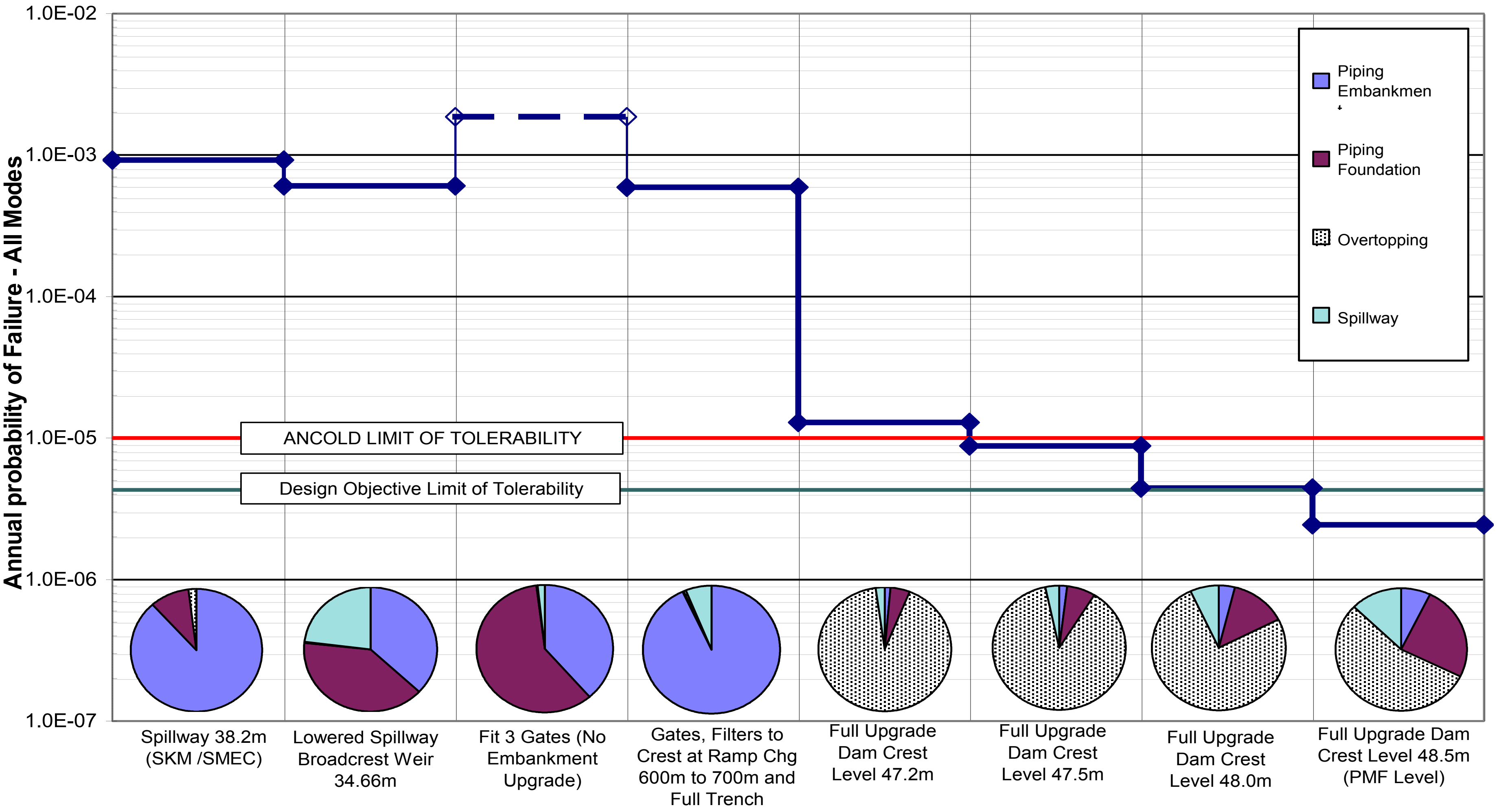
  (1 in 100,000)



# Risk Reduction

- Identify and evaluate structural and non-structural risk reduction options
- Compare all options against the “Do nothing” option
- Determine whether “residual” risk after implementation would be acceptable
- Select the preferred option and develop a Strategy for implementation. Consider:
  - ✓ the level of residual risk
  - ✓ the time scale in which the measures can be practically implemented
  - ✓ economic efficiency and effectiveness
  - ✓ other considerations, taken into account by the decision-maker

# Risk reduction Strategy



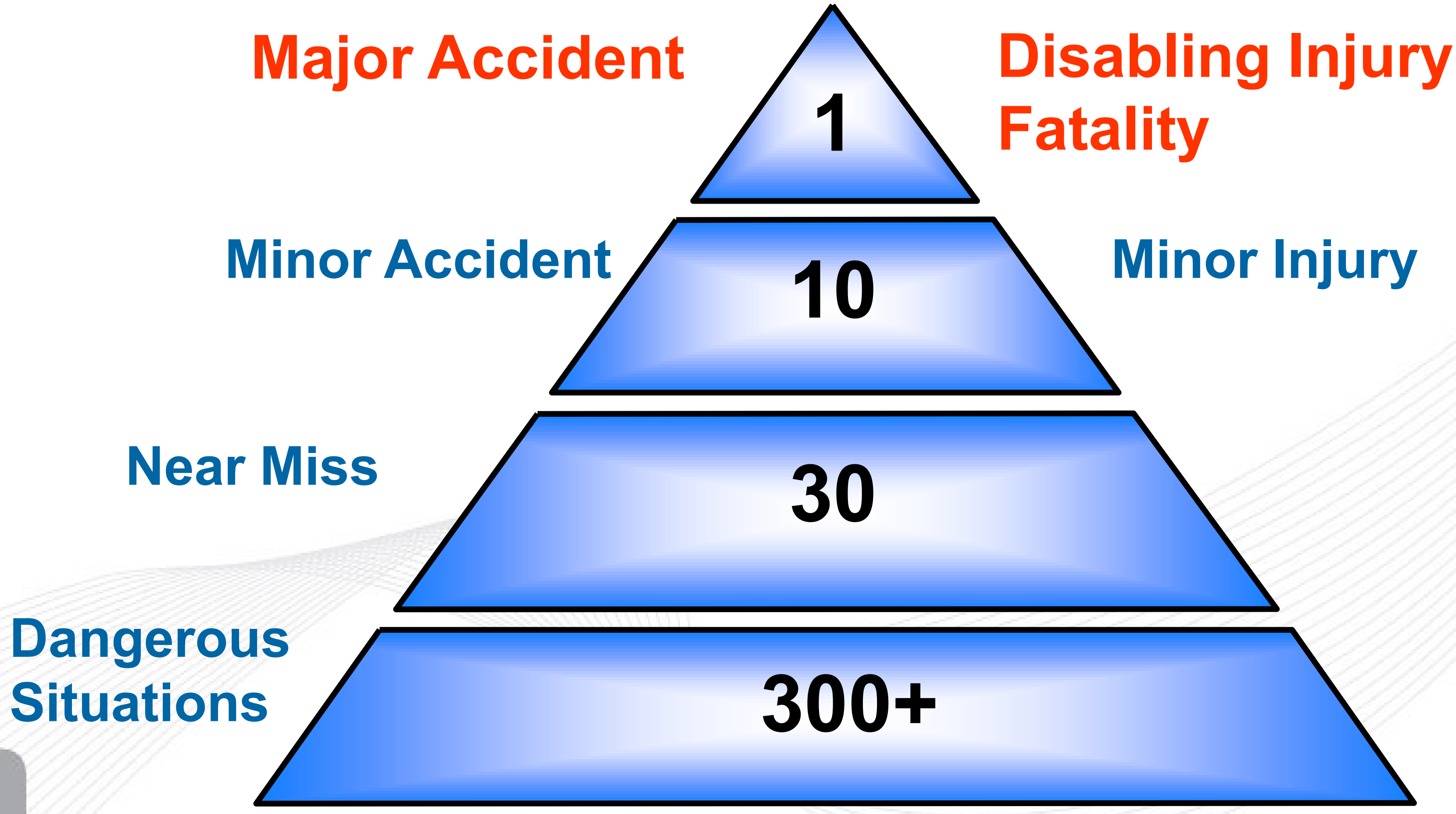
# Strategy and Implementation

Applicable to a portfolio of dams, components of dams or failure modes

- Priority – Highest Risks and life safety risks first
- Urgency – To the extent that risks exceed the tolerable limits
- Progressive improvement – where works can be completed in stages and achieve the best outcomes in reducing risk with the available resources
- Consider Interim Measures – for short term protection while planning for long term reduction
- Long term management – Use guidelines for dam safety management

# HUMAN ERROR

# Pyramid of events



# THE HUMAN ERROR “PROBLEM”

“Fumbling with his recline button, Ted unwittingly instigates a disaster.”

Larson
VOL
CHANNEL
WINGS STAY ON
WINGS FALL OFF

70 - 80% accidents

*Hollnagel 1993*

# The “Human” Factor

- Managers
- System designers
- Trainers
- Maintainers
- Operators

*Error occurs at all levels*

*Initiate*

*Design*

*Implement*

*Operate*

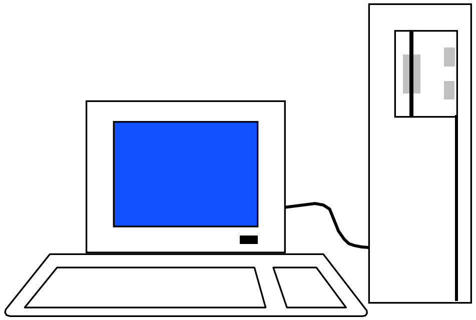
*Maintain*

*Decommission*

Individual error - Unsafe acts

Organisational - Latent failures

# THE COMPUTER vs THE HUMAN



## COMPUTER

large memory stores
several tasks at same time
acts in standard way

**Inflexible: no initiative**

## HUMAN

limited memory stores
do one thing at a time
vulnerable to biases

**Flexible: use initiative**

# INDIVIDUAL - UNSAFE ACTS

# Human Failures ANCOLD Table C2

| | | | | | |
|---|---|---|---|---|---|
| Human Failures | Errors | **Skill**-based errors | Slips & Lapses | **Increasing chance of failure per action** ↓ | **Increasing chance of recovery** ↑ |
| | | Mistakes | **Rule**-based mistakes | | |
| | | | **Knowledge**-based mistakes | | |
| | Violations | | Routine | | |
| | | | Situational | | |
| | | | Exceptional | | |

# SKILLS-RULES-KNOWLEDGE FRAMEWORK

*Rasmussen & Jensen (1974)*

## Skill-based level:

- Human performance is governed by stored patterns of pre-programmed instructions.
- Errors occur when monitoring of the task fails
- Slips of action
- Lapse of memory
- The planning is adequate but the actions fail

# SKILLS-RULES-KNOWLEDGE FRAMEWORK

- Rule-based level
  - Tackles familiar problems in which solutions are governed by stored rules of the type:
    - if (state) then (diagnosis) ; or
    - if (state) then (remedial action)
  - Actions may conform to the plan but the plan is wrong
  - Errors
    - associated with the misclassification of situations
    - lead to the application of the wrong rules or with the incorrect recall of procedures

# SKILLS-RULES-KNOWLEDGE FRAMEWORK

- Knowledge-based level:
  - Problem solving skills (Likelihood of error is high)
  - Novel situations for which actions must be planned on-line, using conscious analytical processes and stored knowledge
  - Errors arise from resource limitations and incomplete or incorrect knowledge

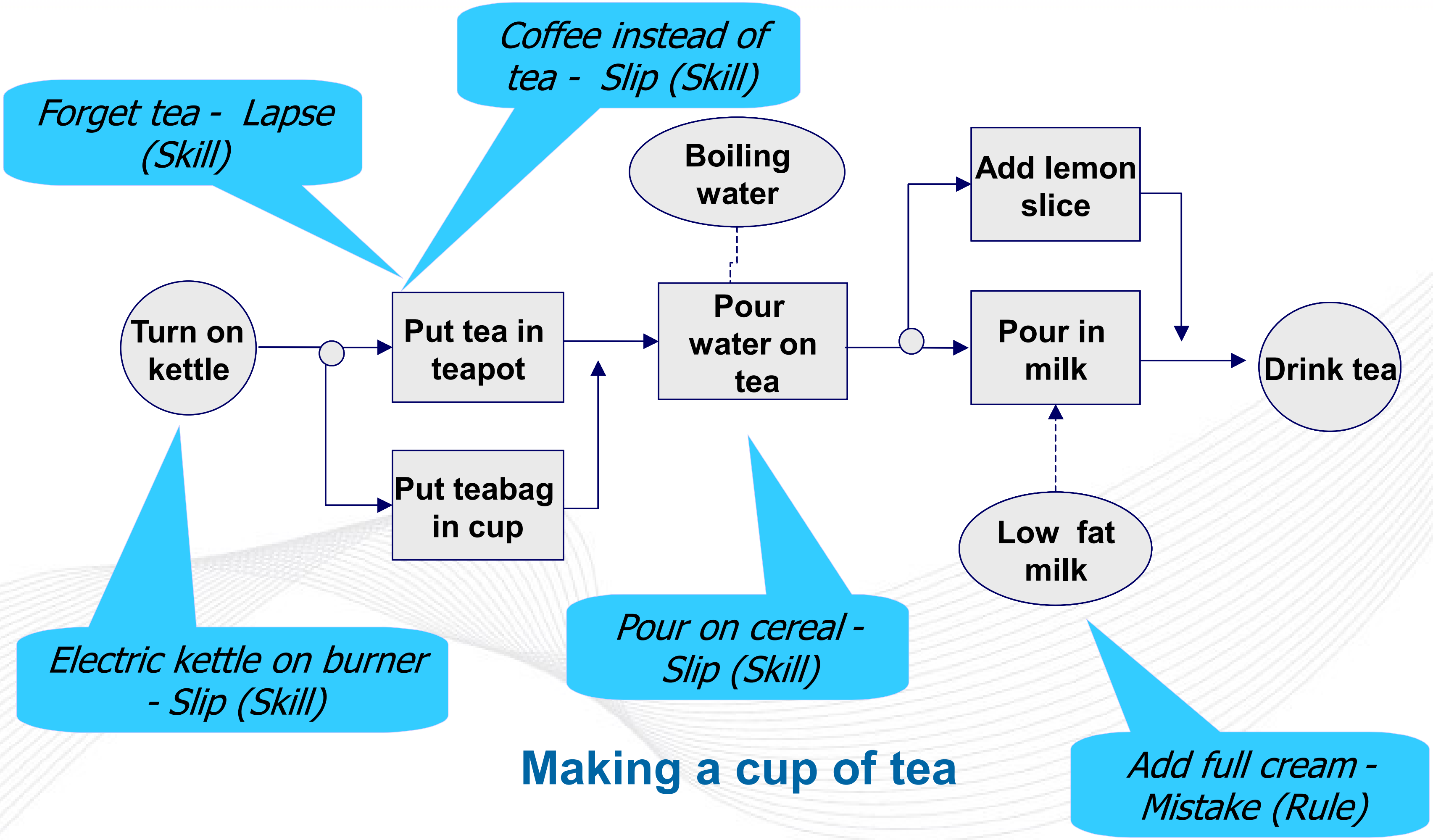
# Violations

## Deliberately failing to apply the rule

- In many industries violations (procedure workarounds) are more common than expected
- Not good enough to say “people should just follow the procedures”
  - Find out *what* violations are actually occurring and *why* they are occurring
  - Enforce or assist compliance with good procedures, change bad procedures

CLIENTS | PEOPLE | PERFORMANCE

# NORMAL ERRORS



Turn on kettle

Put tea in teapot

Put teabag in cup

Boiling water

Pour water on tea

Add lemon slice

Pour in milk

Low fat milk

Drink tea

*Forget tea - Lapse (Skill)*

*Coffee instead of tea - Slip (Skill)*

*Electric kettle on burner - Slip (Skill)*

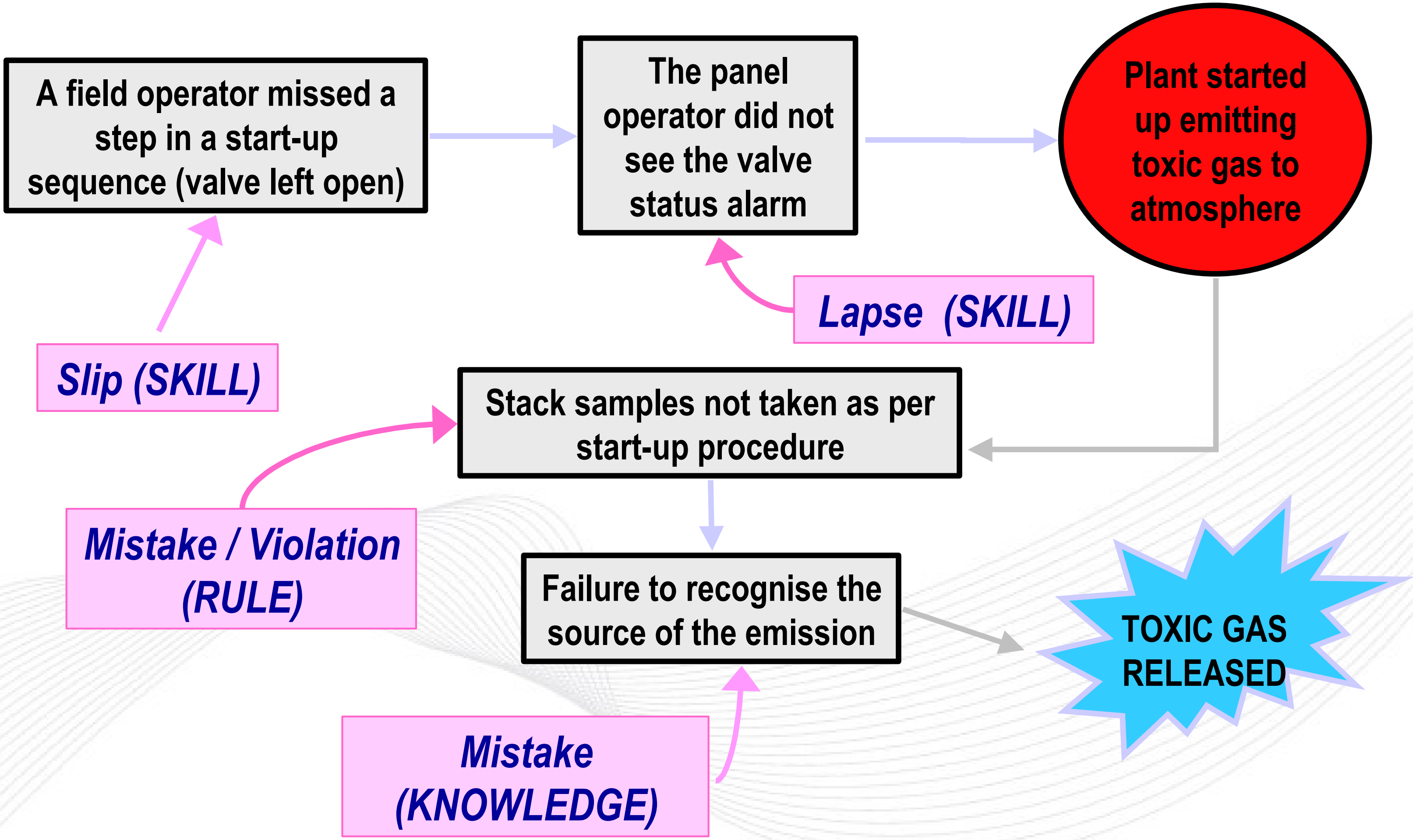
*Pour on cereal - Slip (Skill)*

*Add full cream - Mistake (Rule)*

**Making a cup of tea**

GHD CLIENTS | PEOPLE | PERFORMANCE

# THIS REALLY HAPPENED!



A field operator missed a step in a start-up sequence (valve left open)

The panel operator did not see the valve status alarm

Plant started up emitting toxic gas to atmosphere

Slip (SKILL)

Lapse (SKILL)

Stack samples not taken as per start-up procedure

Mistake / Violation (RULE)

Failure to recognise the source of the emission

TOXIC GAS RELEASED

Mistake (KNOWLEDGE)

# ROUTINE VS. NON-ROUTINE OPERATIONS

ROUTINE OPERATIONS:

- Automatic behaviour, everyday tasks
- Skill / rule based errors more common

NON-ROUTINE OPERATIONS:

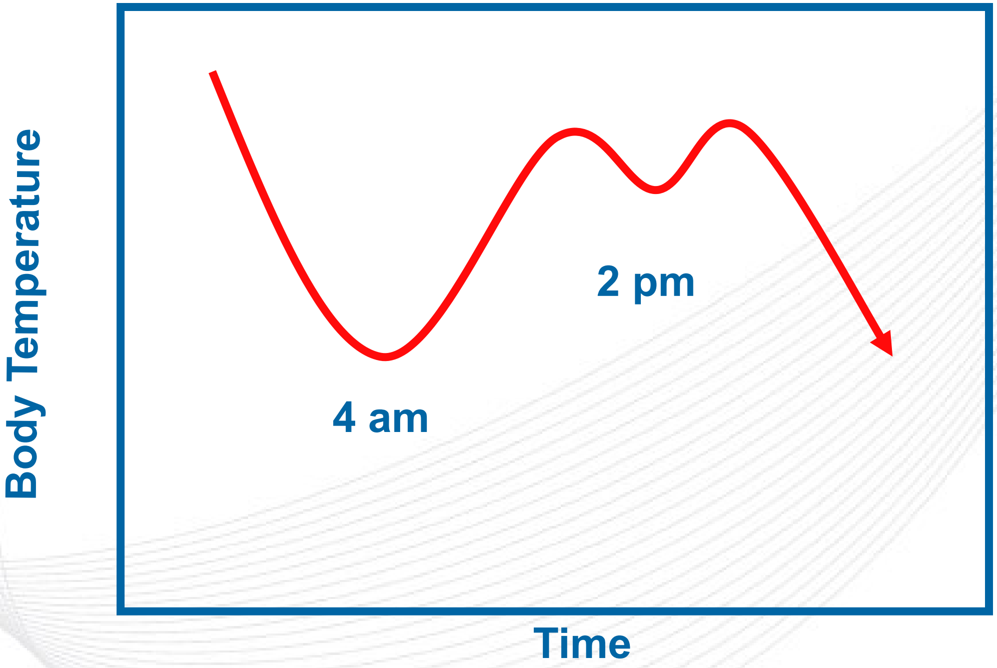
- Analytical thought, often situations never encountered before
- Require a deviation from usual operations
- Knowledge based errors more common

# VIGILANCE ERRORS IN ROUTINE OPERATIONS

Difficult to maintain vigilance on routine tasks

Alertness affected by the time of the day:

- Post Lunch Dip
- Zombie Zone



# DISTRACTION ERRORS IN ROUTINE OPERATIONS

- Operators are easily distracted when carrying out routine tasks

Sources of distraction:

– phone
– alarm
– colleague
– daydreaming
– personal problems

# SUMMARY

Design:

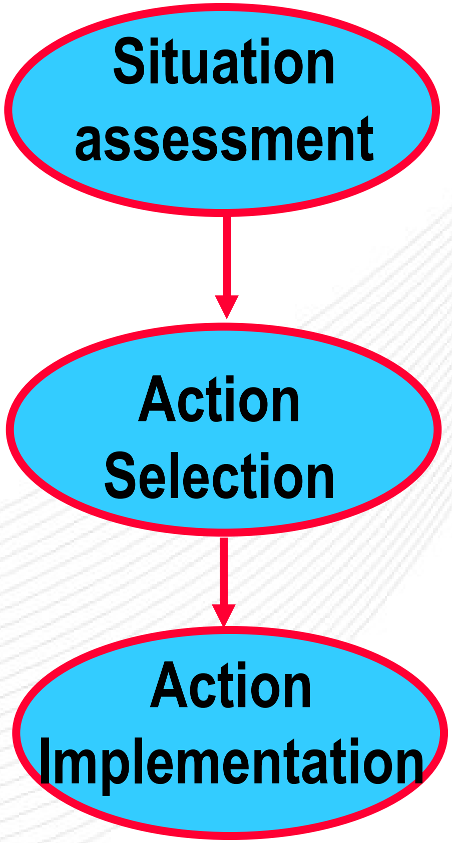
- Remember human vulnerability under routine - boring - conditions!
- Difficulty maintaining vigilance
- Vulnerability to distraction and forgetting
- Don’t rely on human vigilance and memory
- Design for defences in depth

Chairing a Workshop:

- Remember that participants can and DO get bored

# NON-ROUTINE OPERATIONS

- Require analytical thought processes
- Knowledge-Based Errors more common (Mistakes)


Situation assessment

Action Selection

Action Implementation

# FOUR COMMON ERROR TYPES IN NON-ROUTINE OPERATIONS

1. Filtering bias
2. Easy-option bias
3. Group-Think bias
4. Single fault bias

# 1. FILTERING BIAS

- Information is filtered:
  - not possible to pay attention to everything
- More likely to attend to:
  - salient information
  - important information
  - familiar information
- Danger of ignoring important information
- High workload exacerbates this bias

# 2. EASY OPTION BIAS

- Humans generally lazy. Prefer to operate in automatic mode (auto-pilot) than analytic mode
- Danger of:
  - explaining away mismatches
  - rejecting contradictory data

# 3. GROUP THINK BIAS

- The Group-Think bias is the tendency to agree with another persons' analysis of the situation

- This agreement strengthens the original person's viewpoint: they become more certain that their view is correct

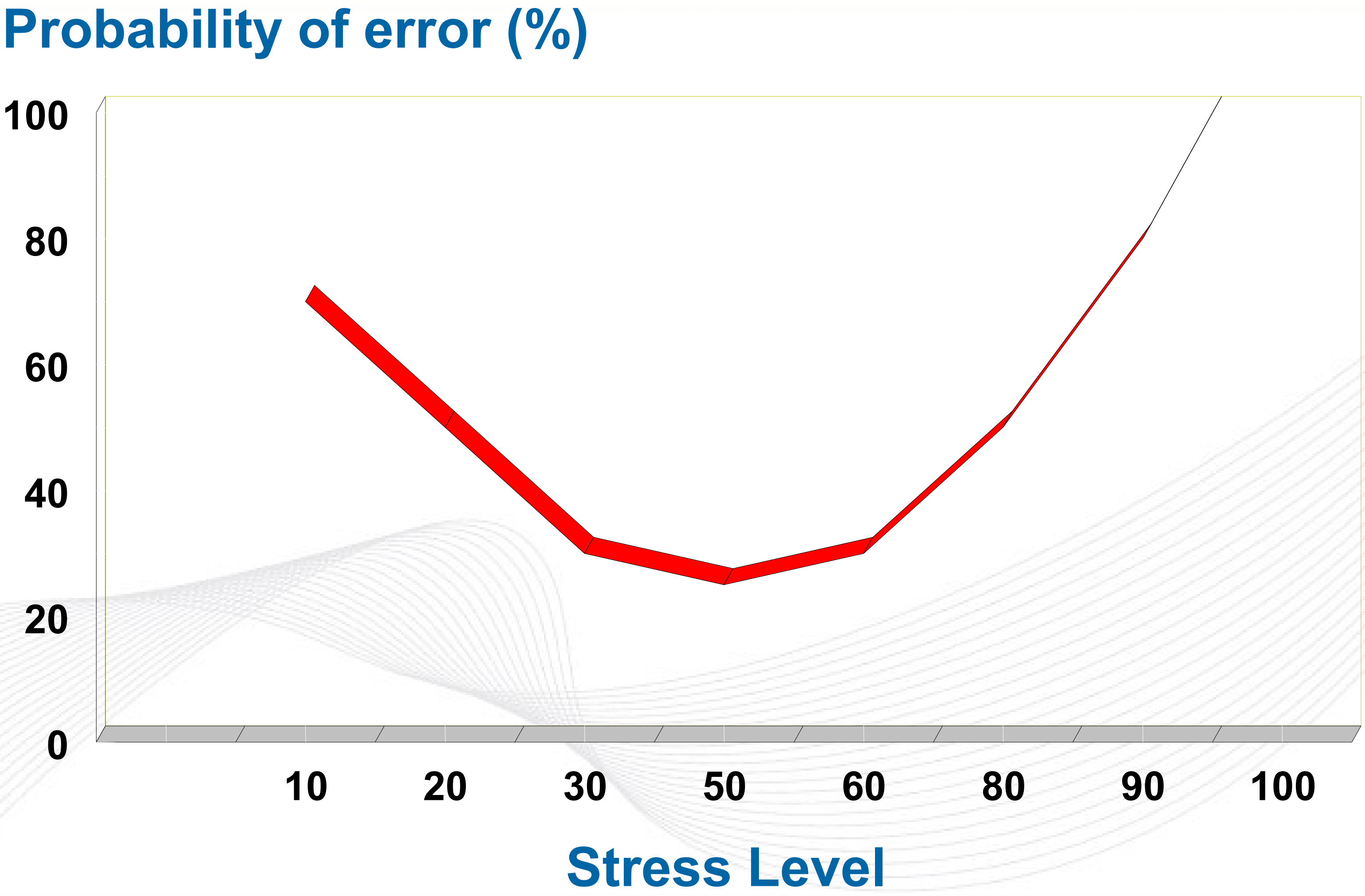
# Dangers of the Group-Think bias

- Failure to examine other alternatives
- Not being critical of each other's ideas
- Not seeking expert opinion
- Limits or stops further information gathering
- Original understanding of the situation may be wrong and false confirmation leads to wrong decisions and incorrect action

# 4. SINGLE FAULT BIAS

- Humans prefer to devise a simple explanation for an abnormal event
- Single-fault rather than multiple fault explanation
- Dangers:
  - could “explain away” conflicting information

# STRESS


Probability of error (%)
100
80
60
40
20
0
10
20
30
50
60
80
90
100
Stress Level

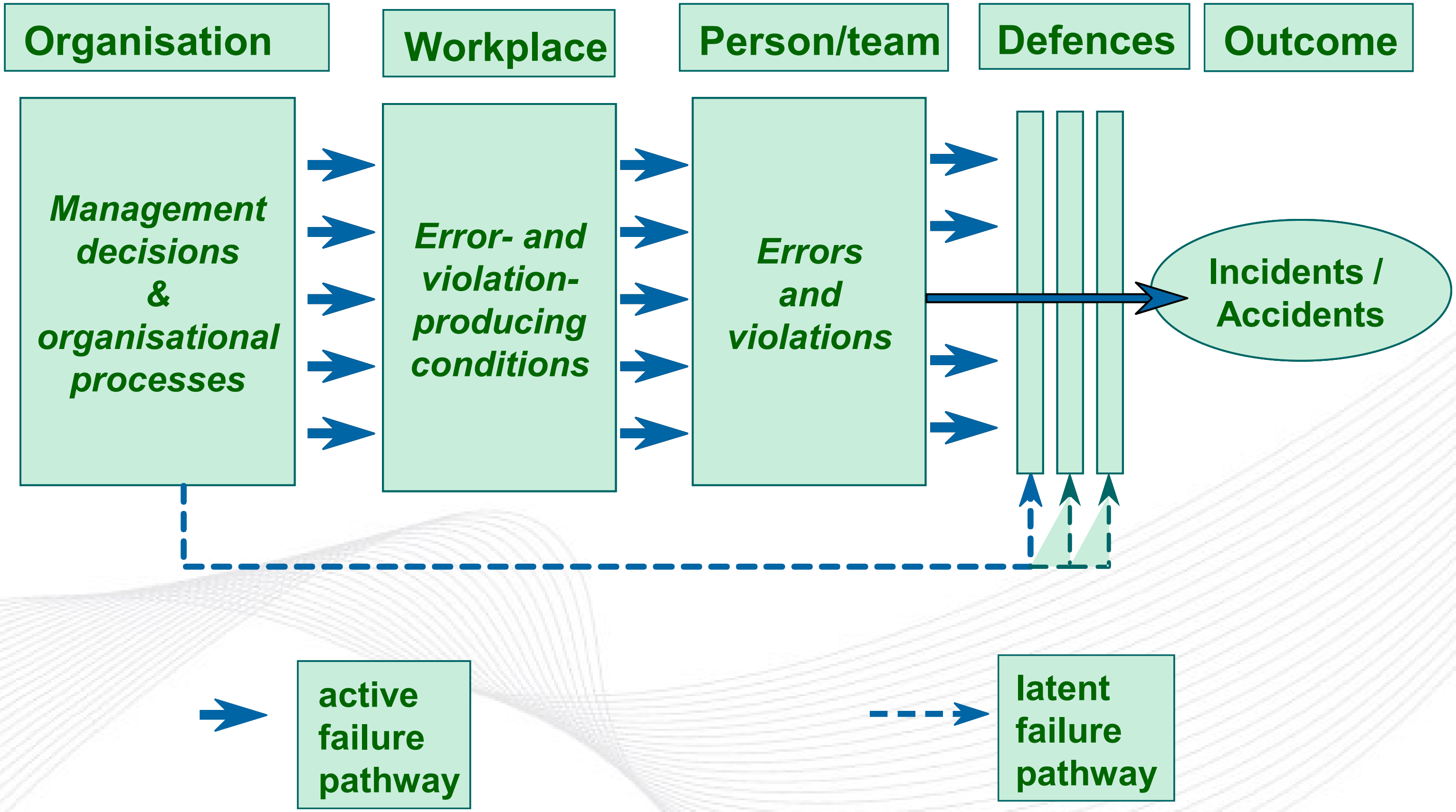
# Generic Tasks And Associated Error Probabilities (Ref: Williams)

| *Generic task description* | *Nominal error probabilities*<br>*(5th – 95th percentile bounds)* |
|---|---|
| 1. Totally unfamiliar, performed at speed with no idea of likely consequences | 0.55<br>(0.35 – 0.97) |
| 2. Shift or restore system to a new or original state on a single attempt without supervision or procedures | 0.26<br>(0.14 – 0.42 ) |
| 3. Complex task requiring high level of comprehension and skill | 0.16<br>(0.12 – 0.28) |
| 4. Fairly simple task performed rapidly or given scant attention | 0.09<br>(0.06 – 0.13) |
| 5. Routine, highly practised, rapid task involving relatively low level of skill | 0.02<br>(0.007 – 0.045) |
| 6. Restore or shift system to original or new state following procedures, with some checking | 0.003<br>(0.0008 – 0.007) |
| 7. Completely familiar, well designated, highly practised routine task, oft-repeated and performed by well motivated, highly trained individual with time to correct failures but without significant job aids | 0.0004<br>(0.00008 – 0.009) |
| 8. Respond correctly to system event even when there is an augmented or automated supervisory system providing accurate interpretation of system state | 0.00002<br>(0.000006 – 0.00009) |
| 9. Miscellaneous task for which no description can be found | 0.03<br>(0.008 – 0.11) |

CLIENTS | PEOPLE | PERFORMANCE

# ORGANISATION ERROR

# ORGANISATION ERROR



Organisation

Workplace

Person/team

Defences

Outcome

*Management decisions & organisational processes*

*Error- and violation-producing conditions*

*Errors and violations*

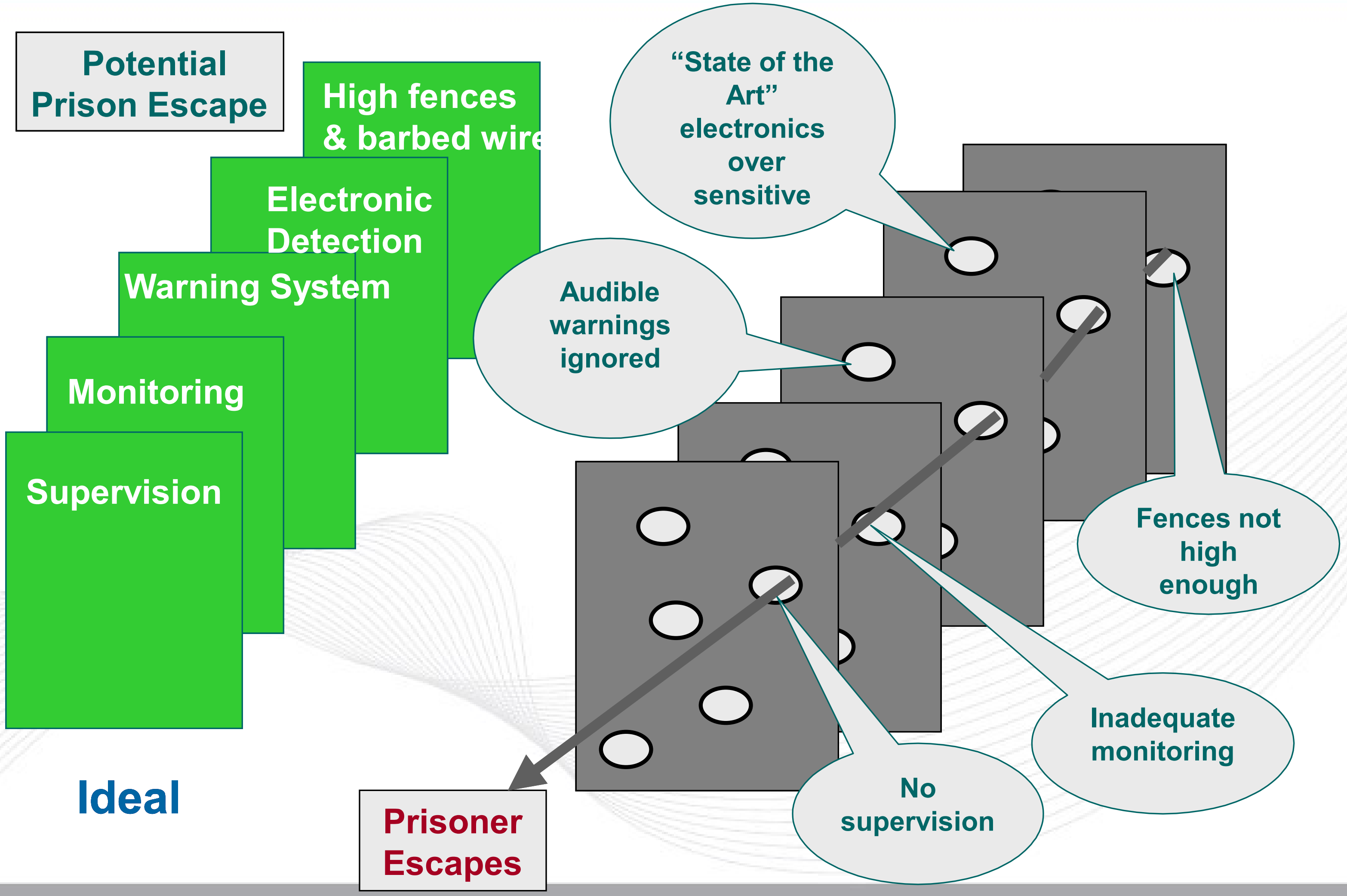
Incidents / Accidents

active failure pathway

latent failure pathway

***Reason, 1997***

# SWISS CHEESE – DEFENCE FAILURES

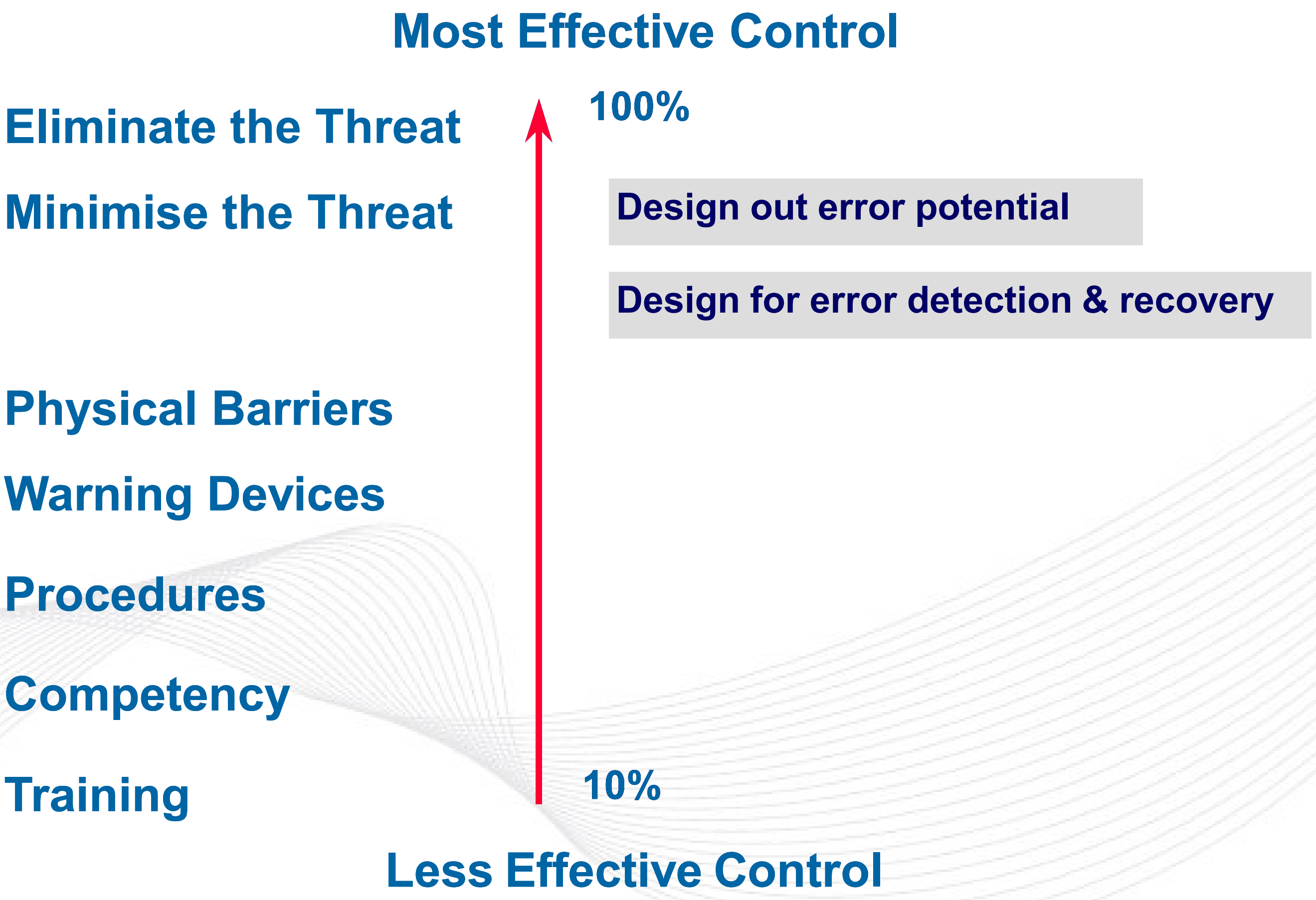


# MANAGING HUMAN ERROR

# MANAGING THE RISK OF HUMAN ERROR

- Human error reduction
- Defences-in depth:
  - Acknowledge that human error is inevitable
  - “Resilience” - create a system that is better able to tolerate and recover from the occurrence of errors

# A Human Factors Hierarchy of Controls



**Most Effective Control**

**100%**

**Eliminate the Threat**

**Minimise the Threat**

**Design out error potential**

**Design for error detection & recovery**

**Physical Barriers**

**Warning Devices**

**Procedures**

**Competency**

**Training**

**10%**

**Less Effective Control**

# Thank You