Hong Kong Industrial Safety Association
Safety Seminar

Risk Management & Decision Analysis in Safety

23 April 2006

Vincent Ho

The presentation material will be posted at
www.hkarms.org

Under HKARMS Web Resources

Two Key Questions from Stakeholders

- How safe is safe?
- How much can you afford safety?

How Safe is Safe?

- How much budget is available?
- Afford unlimited spending is impractical
- No such thing as zero accident, zero risk
- Unknown victim versus someone you know – the "young girl accident"
- Need rational decision – costs of safety improvement should take account of potential life saved
- As Low As Reasonably Practical (ALARP)?

What Doesn't Get Measured Doesn't Get Managed

…but how do you measure safety?

Instead of measuring how safe you are, it is often easier to assess how "unsafe" you are – risks

Manage safety by managing risks!

Measuring Safety

- Safety is difficult to measure directly
- One way to measure safety is to measure
  - The accident rate and/or
  - Degree of unsafe: risk
- Accident rate reflects the “realized risks” – something that has already occurred
- Risk profile predicted by system safety or risk models reflects the total risk (including both ***realized risks*** and ***unrealized risks***)

Accident Rate

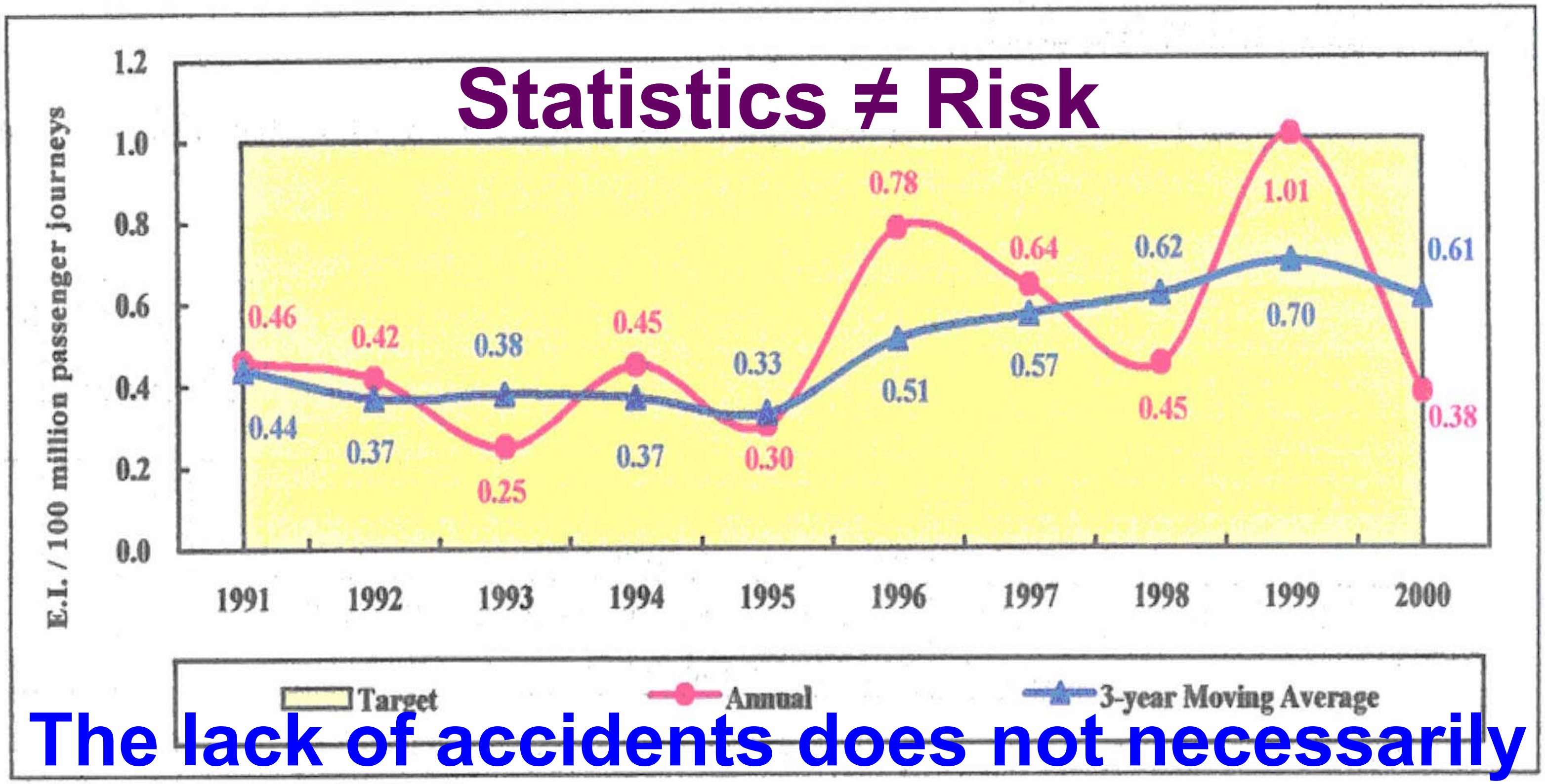
- Type unit for measure safety in accident rate is x/y where x can be
  - Number of fatalities
  - Number of “serious” accidents
  - Number of “reportable” accidents
- The basis, y, can be
  - Per year
  - Per train-miles or kilometers
  - Per passenger-journey
  - Per population

Measuring Safety by Accident Rate

- Easy to benchmark safety performance and set objective
- Benchmarking requires a common definition on accident – many benchmarking groups adopt fatality per year for simplicity
- Difficult to apply in risk management
  - Does not consider unrealized risks; i.e., accidents not yet occurred
  - Depends on the reporting culture
  - Difficult to compare accidents with different severity

What's Wrong with This Picture?

Graph 18 -Annual Safety Performance - Individual Passenger Risk



Statistics ≠ Risk

The lack of accidents does not necessarily indicate the presence of safety

Measuring Safety by Risks

- Require a system safety model or risk model
- Accident statistics complement risk models for rare accidents
- Require a different set of expertise
  - Consider both *realized* and *unrealized risks*
  - Require objective and subjective input
  - Depends on the accuracy and sophistication of the risk model
- Establishing acceptance criteria relies on the risk acceptance principle adopted

Evolution of Risk Management in Safety

- **Key players:**
  - 1960's: Aerospace industry
  - 1970's: Nuclear power industry
  - 1980's: Petro-Chemical industry
  - 1990's: Railway industry

- **Typical applications:**
  - Adequacy of Engineering Safeguards and safety barriers
  - Risk induced by external events (fires, earthquakes, flooding, etc.)
  - Risk exposure to operator, public, environment, etc.

Making Decision Based on Risk Information

- To carry out a more detailed analysis to obtain further information to allow a decision to be made
- Not to continue with the activity
- To accept the risk without any further treatment
- To control risks

Topics to Discuss

- Concept of Risk
- Risk Management Principles
- Fault Tree and Event Tree
- Decision Analysis

Concepts of Risk

First Application of Risk Management?

孫子兵法

作戰篇

故不盡知用兵之害者，
則不能盡知用兵之利也。

是故智者之慮，必雜于利害，
雜于利而務可信也，
雜于害而患可解也。

What is “RISK”?

- What can go wrong?
- How likely is it?
- What is the consequence?
- What are the uncertainties?

Characterisation of Risk

- Qualitative terms are frequently used to indicate the risk level of the hazards
  - Yes/No
  - acceptable/Unacceptable
  - High, Medium, Low
  - Risk classes; e.g., A, B,C, D
- Numbers are preferred in a quantitative risk assessment; e.g., 4.3 x 10^{-6} death/yr

Do not trust the absolute value of the numbers, they are for comparison only

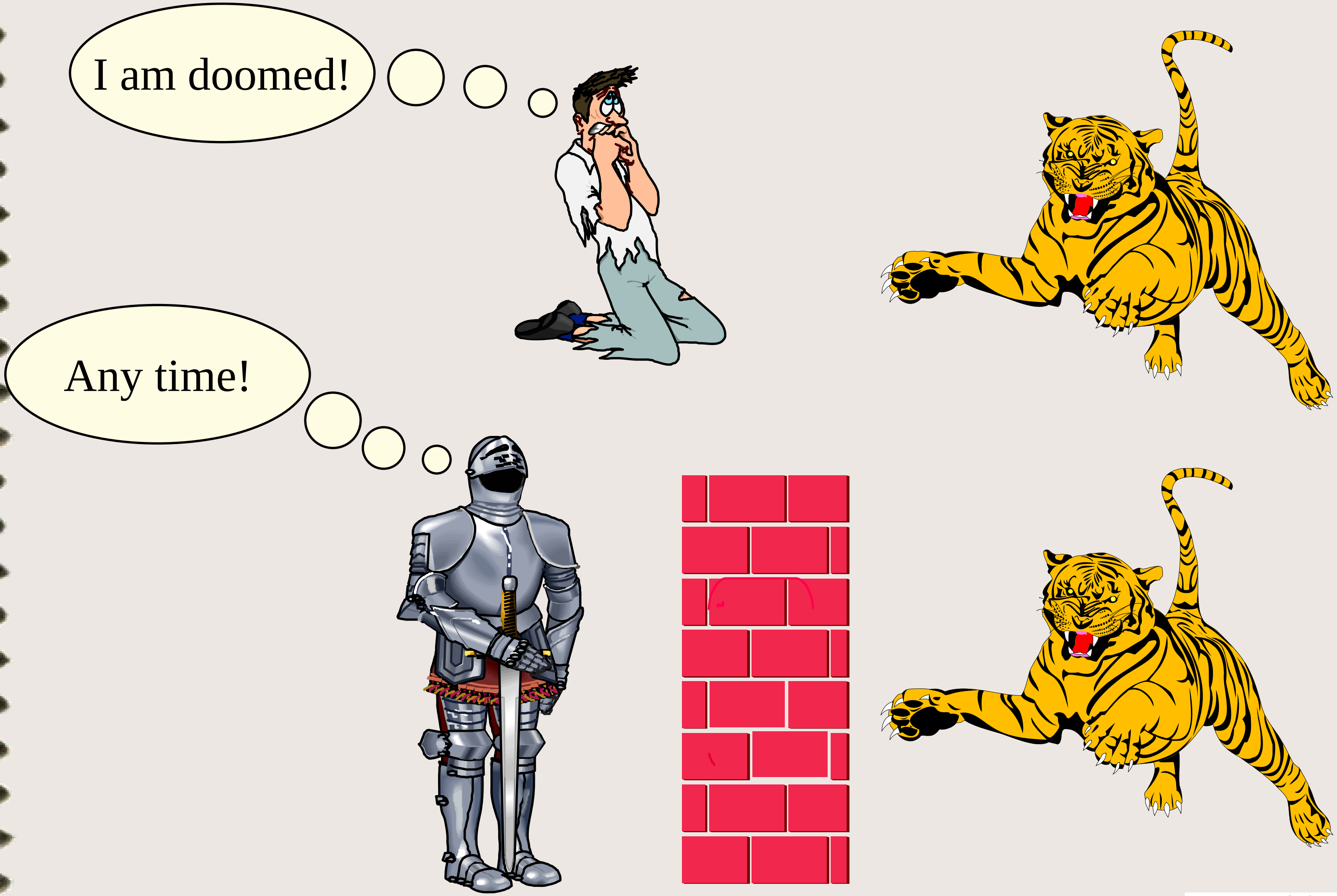
The Amount of Hazard Does Not Necessarily Indicate The Risk Level

Higher Amount of Fire Hazard

The Totality of a Situation is a Better Indicator of the Risk Level

Higher Fire Risk

Same Hazard May Impose Different Risks Due to Different Safeguards



Hazard vs Risk

- Risk has been defined in various ways in different industries, and is often misunderstood and misapplied
- To characterise risk, we must have:
  - A hazard -- source of danger
  - An initiating event that activates the danger
  - A target (risk receptor)
  - A transfer mechanism to expose the target to the dangerous situation

Hazard, you measure.
Risk you assess.

Hazard vs Risk

- Hazard is a source of danger, or the presence of a condition or a situation, that has the potential of resulting in undesirable consequences
- Hazard can be measured by absolute terms; e.g., weight, volume
- A Hazard must be "activated" by a Triggering Event to result in the prescribed consequence before its risk impact can be assessed
- The progression of an accident can be described by its associated Hazard Scenario

Hazard Description + **Triggering Event** → **Consequence**

Hazard vs Hazard Scenario

- The terms, Hazard and Hazard Scenario, although not the same, are frequently used interchangeably
- A Hazard can be measured by its physical properties: dimensions, mass, location, temperature, frequency of occurrence, etc.
- You can assess the risk of a Hazard Scenario but not a hazard

Qualitative Definitions of Risk

$$\text{Risk} = \frac{\text{Hazard}}{\text{Safeguards}}$$

- Risk is never zero by increasing level of safeguards, as long as hazard is present

$$\text{Risk} = \text{Likelihood} \times \text{Consequence}$$

- Classical, but most misleading. More useful in hazard analyses

$$\text{Risk} = \text{Uncertainty} \times \text{Damage}$$

- Without uncertainty or damage, there is no risk

Quantitative Definition of Risk

- **In general, risk is used to answer the questions:**
  - **What can go wrong?**
  - **How likely is it that this will happen?**
  - **If it happens, what are the consequences?**
  - **What are the uncertainties?**
- **Thus, risk can be thought to be consisting of four elements:**
  - **Scenarios**
  - **Likelihood**
  - **Consequence**
  - **Uncertainties**

Quantitative Definition of Risk

Scenario	Likelihood	Consequence
s_1	L_1	C_1
s_2	L_2	C_2
s_3	L_3	C_3
•	•	•
•	•	•
•	•	•
•	•	•
•	•	•
s_N	L_N	C_N

- **Risk = $\{\langle s_i, L_i, C_i \rangle\}$**
- **For each s_i, Risk = $L_I \times C_i$**
- **L_I and C_i can be represented by probability distributions to indicate the uncertainties in these parameters**

Uncertainties

- Uncertainties are measured by level of belief; i.e., probability
- In general, there are three types of uncertainties associated with a risk assessment:
  - Stochastic uncertainties
  - Modelling uncertainties
  - Parameter uncertainties
- The final results of a risk assessment for complex engineering systems are seldom expressed by one number but by distributions to express the level of uncertainties associated with the result

Most Risk Assessments do not address uncertainties

Uncertainty

- Dealing with uncertainty is an unavoidable problem in reality
- To make decision with uncertainty, we need
  - Probability theory
  - Utility theory
  - Decision theory

Sources of uncertainty

- No access to the whole truth
- No categorical answer
- Incompleteness
  - The qualification problem - impossible to explicitly enumerate all conditions
- Incorrectness of information about conditions
- The rational decision depends on both the relative importance of various goals and the likelihood of its being achieved.

Uncertainties

- Uncertainties are measured by level of belief; i.e., probability
- In general, there are three types of uncertainties associated with a risk model:
  - Stochastic uncertainties
  - Modelling uncertainties
  - Parameter uncertainties
- Strictly speaking, $A+A \neq 2 \times A$
- It is this explicit consideration of uncertainties distinguishes a risk assessment from a hazard analysis

Probability of Frequency

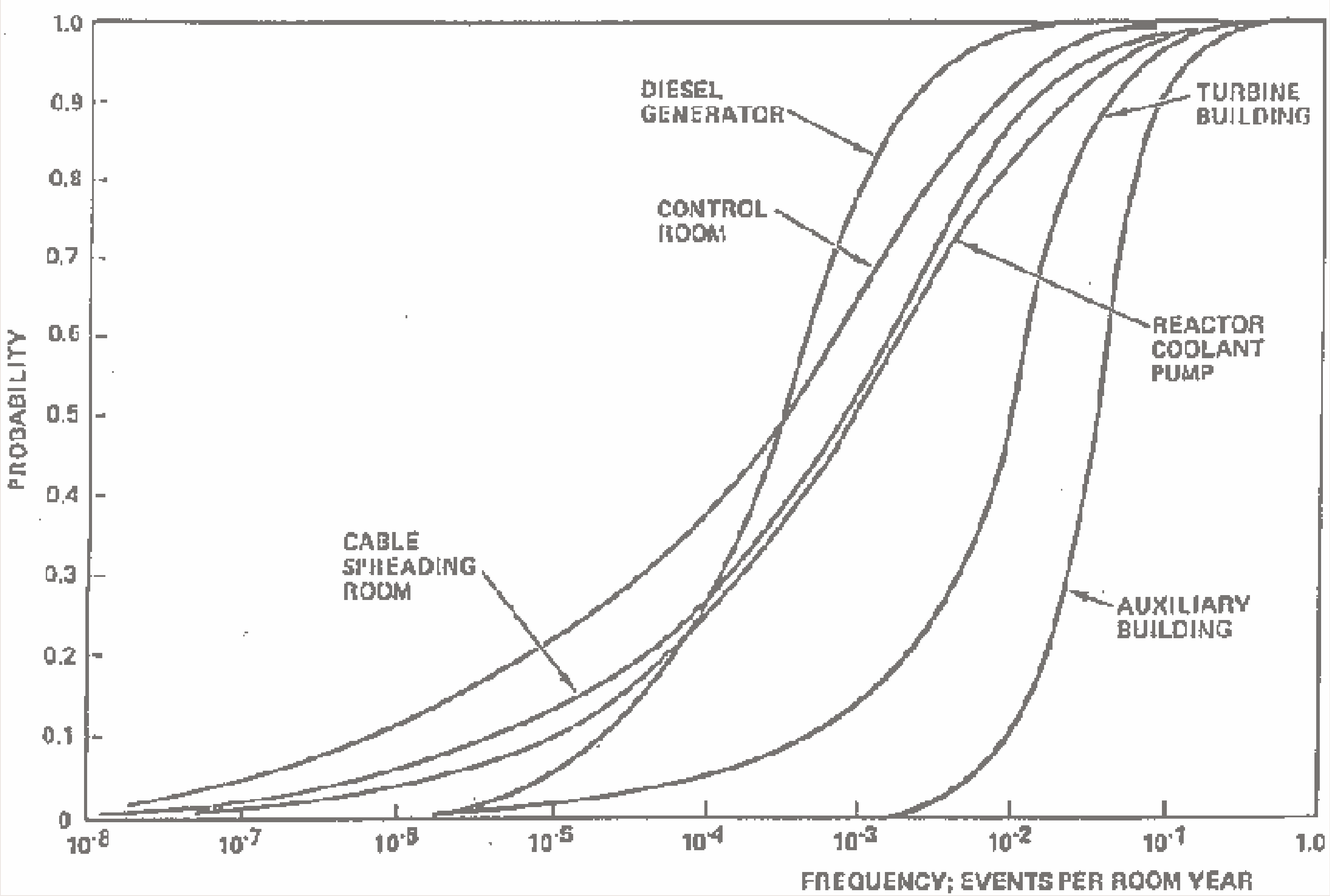
- Frequency is a measure of the rate of occurrence. E.g., failure rate of a pump is 6.2×10^{-3}/hr
- Probability is a measure of the level of belief, a fraction, or failure per demand. It is dimensionless. E.g., the failure rate of the pump is

Frequency	Probability
1.0×10^{-4}/hr	0.2
2.0×10^{-3}/hr	0.5
3.2×10^{-3}/hr	0.2
4.5×10^{-2}/hr	0.1

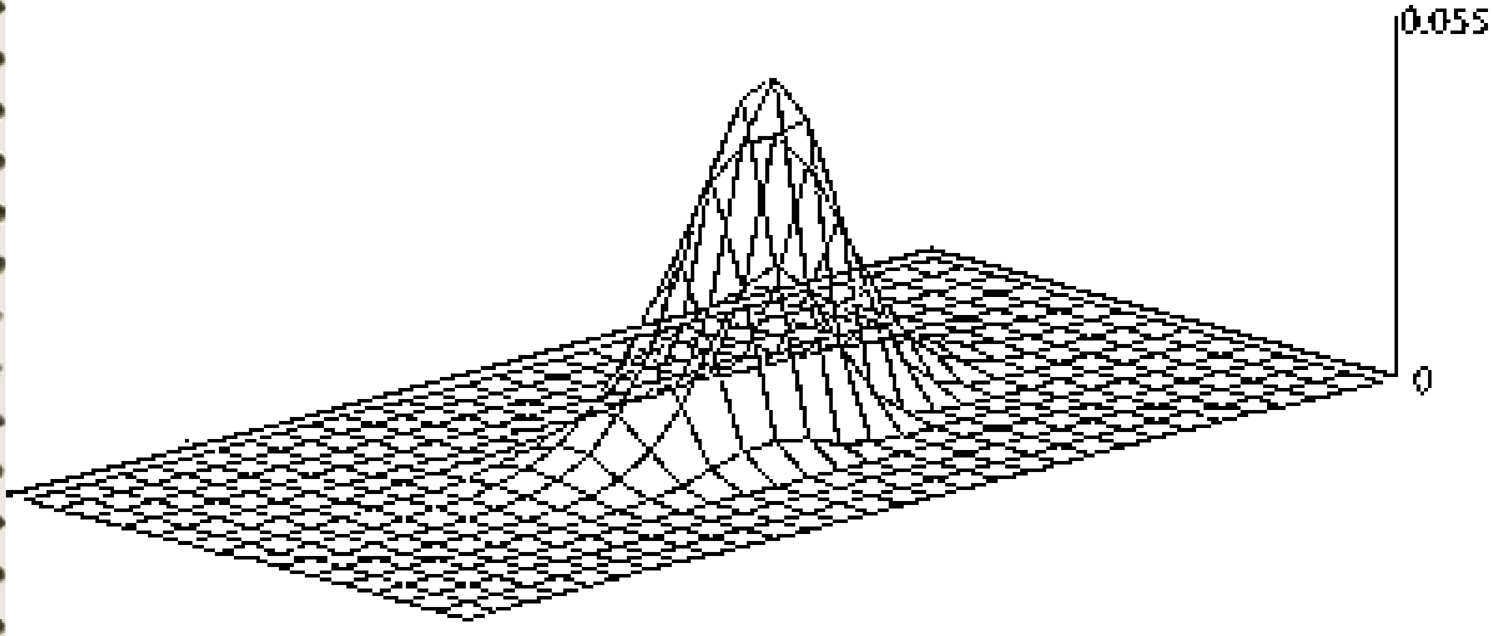
with a mean of 6.2×10^{-3}/hr

- Strictly speaking, $A+A \neq 2 \times A$

PROBABILITY CURVES FOR FREQUENCY



A PROBABILITY CURVE CAN BE RATHER SCARY



Types of Risk

- Individual Risk
- Societal Risk
- Collective Risk

- Background Risk
- Voluntary Risk
- Involuntary Risk

- Non-realized Risk
- Realized Risk

Individual Risk

- Risk to an (often hypothetical) individual
- Usually expressed in frequency of death (per year)
- Tolerable level highly dependent on whether risk is voluntary or not

Common UK Individual Risks (/year)

Rock climbing	1 in 10
Entire population	1 in 100
Deep sea fisherman Minimum tolerability	1 in 1,000
Road user	1 in 10,000
General employment	1 in 100,000
Tolerable	1 in 1,000,000
Lightning	1 in 10,000,000

Railtrack (UK) Targets for 2009

Accident	Target (per passenger journey)
Passenger Fatalities	1 in 133 million
Passenger Major Injuries	1 in 7.5 million

1 fatality = x injuries?

Equivalent Injuries

- Equivalent Injury (or Equivalent Fatality) provides a common measurement for different severity of injuries
- EI= No. fatalities + 1/a * (no. of Serious Injuries) + 1/b * (no. of minor injuries)
- A, b various between countries

Organisation	Country	a Major (Serious)[1] injuries equivalent to one fatality	b Minor injuries equivalent to one fatality
Railway Group	UK	10	200
IE	Ireland	10	200
KCRC	Hong Kong	(14.3)[1]	200
London Underground	UK	10	100
MTRC	Hong Kong	10	100
Land Transport Authority	Singapore	9.1	100

Analysis of Survey Results

Equivalent Injuries

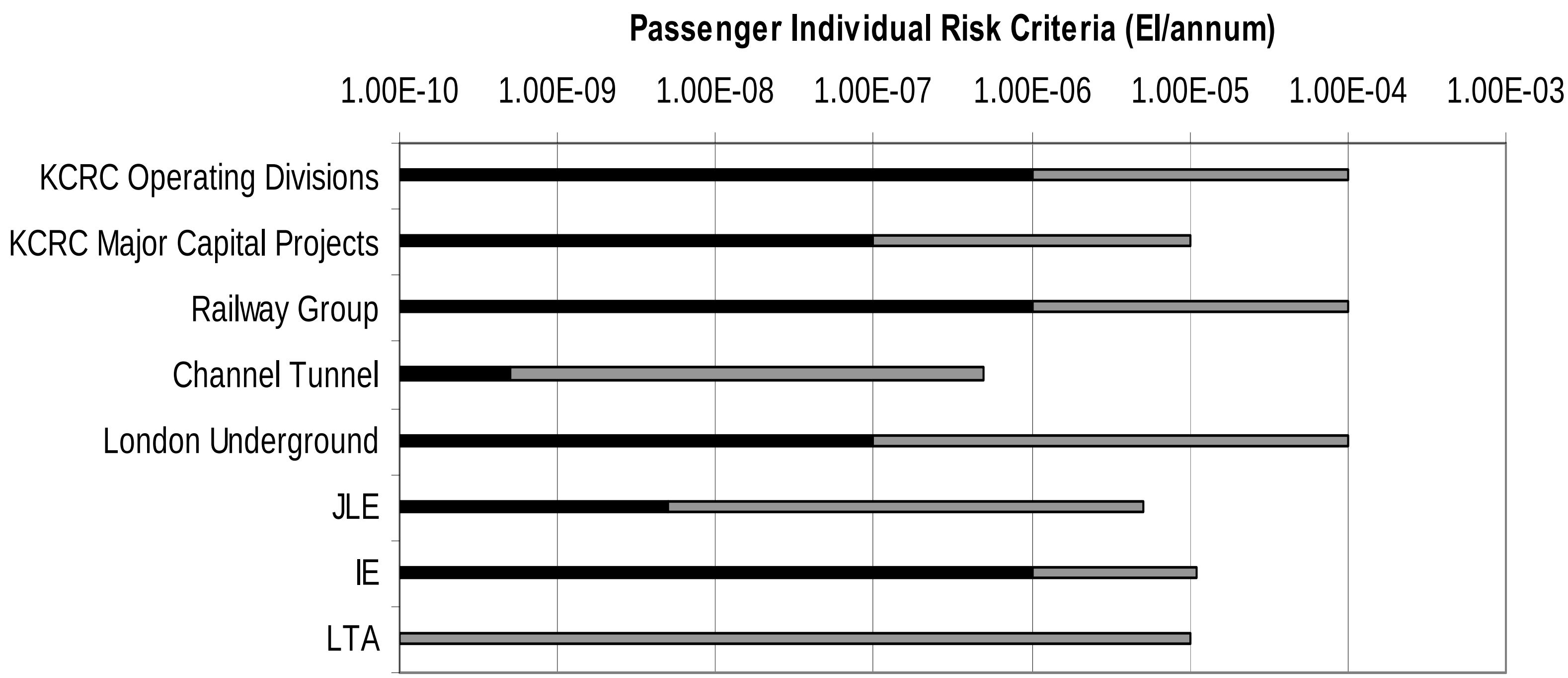
- A factor of a=10 is commonly adopted for 'Serious Injury' but is arbitrary
- One organisation selected a=14.3 which is considered to be acceptable as a geometric mean of 1 and b=1/200 for minor injury
- Should also consider the number and type of historical minor accident cases before adopting 1:10:100 or 1:14.3:200

Individual Risks
For Railway

- Passengers
  - Per year
  - Per train miles
  - Per passenger journey
- Staff
- The Public

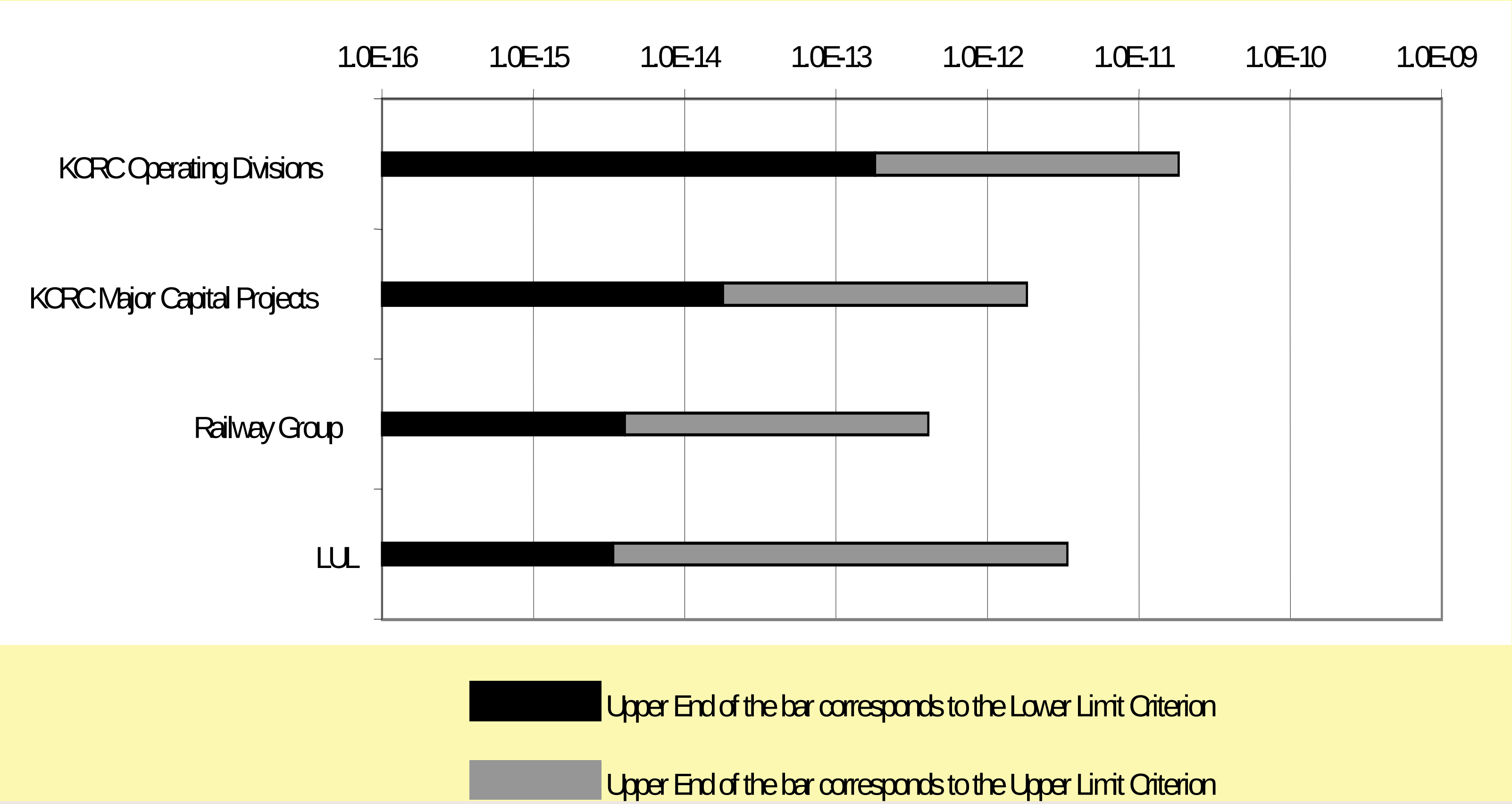
Passenger Individual Risk

(EI/annum)



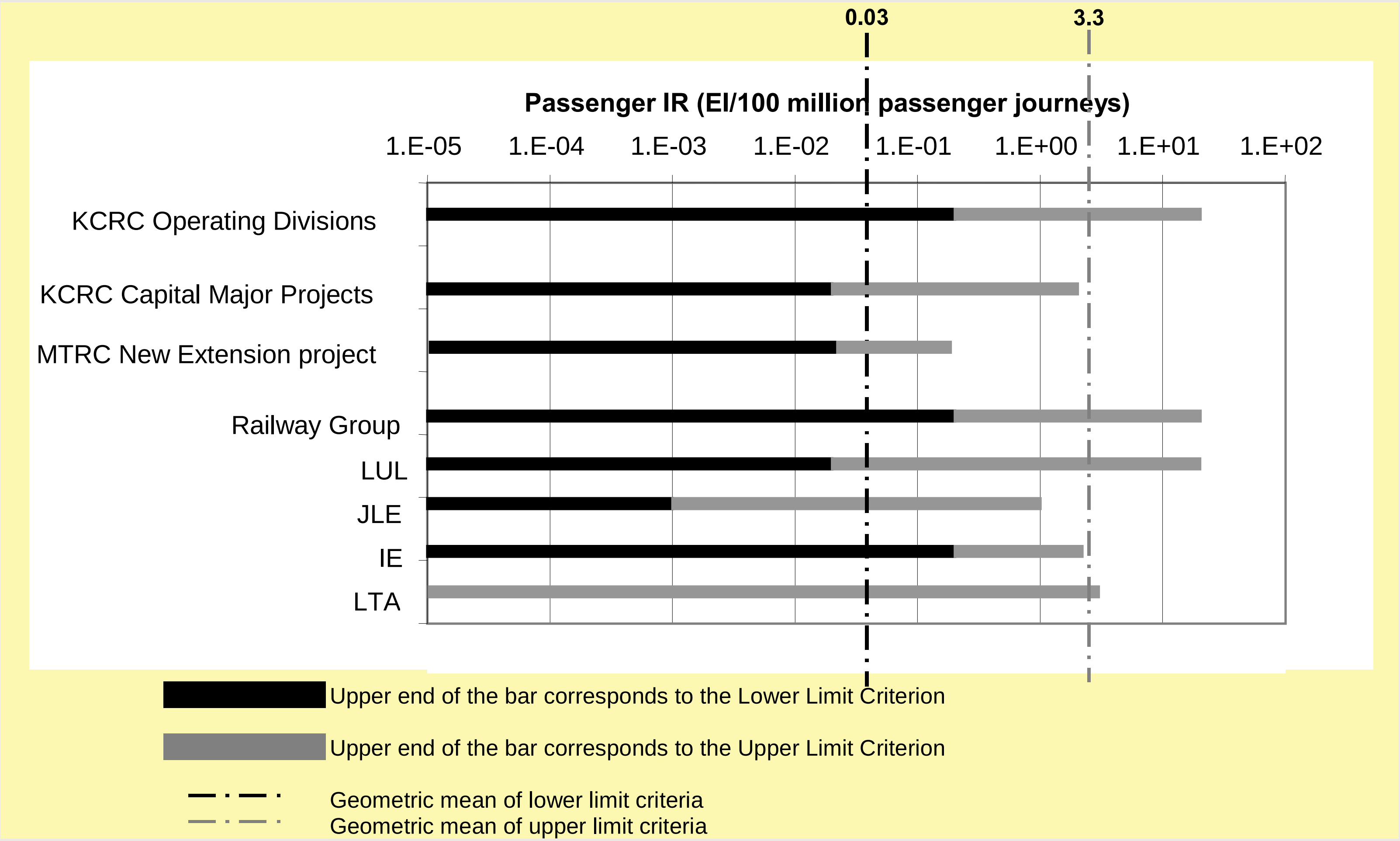
Passenger Individual Risk

(EI/train miles)



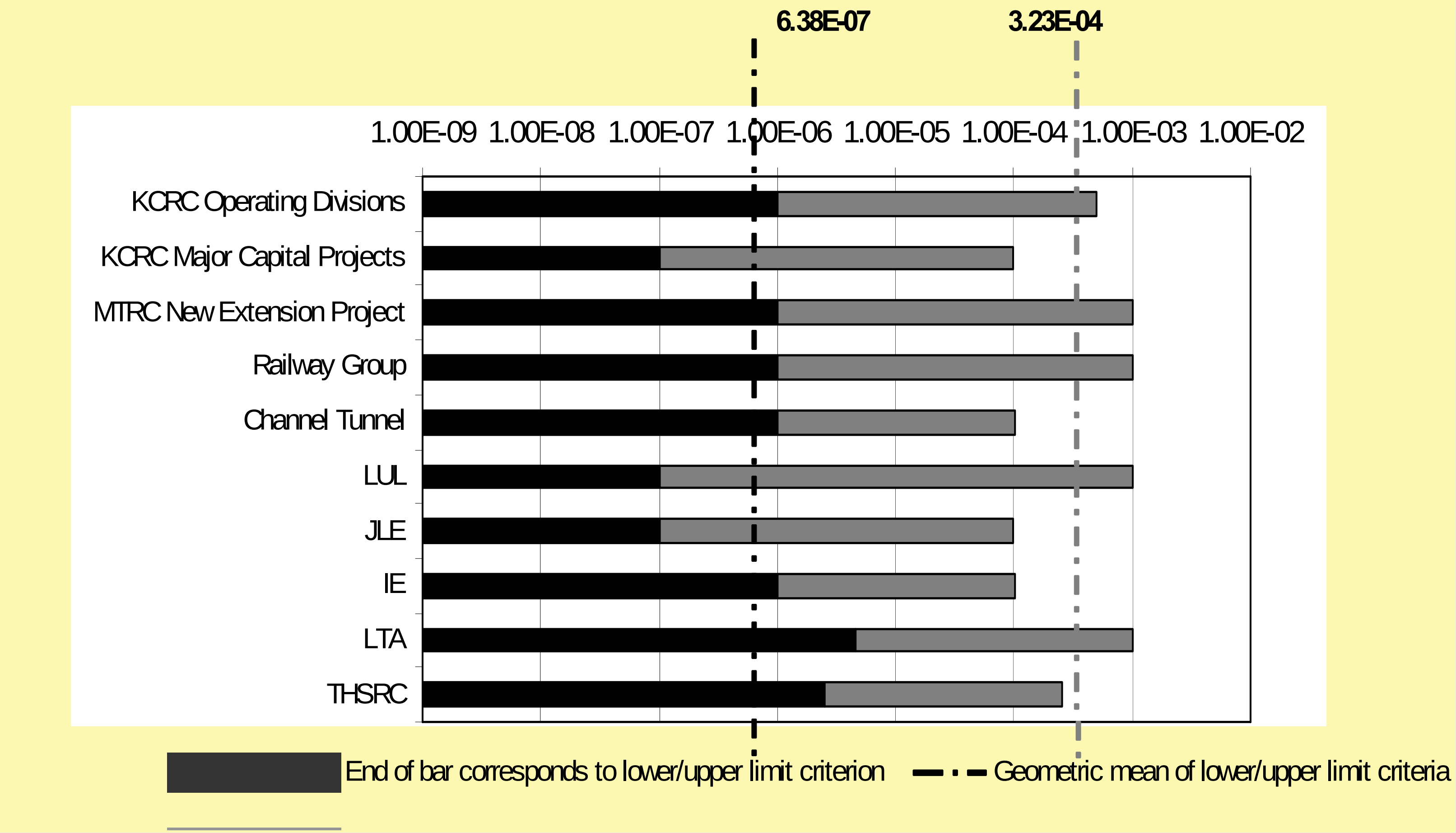
Passenger Individual Risk

(EI/100 million passenger journeys)



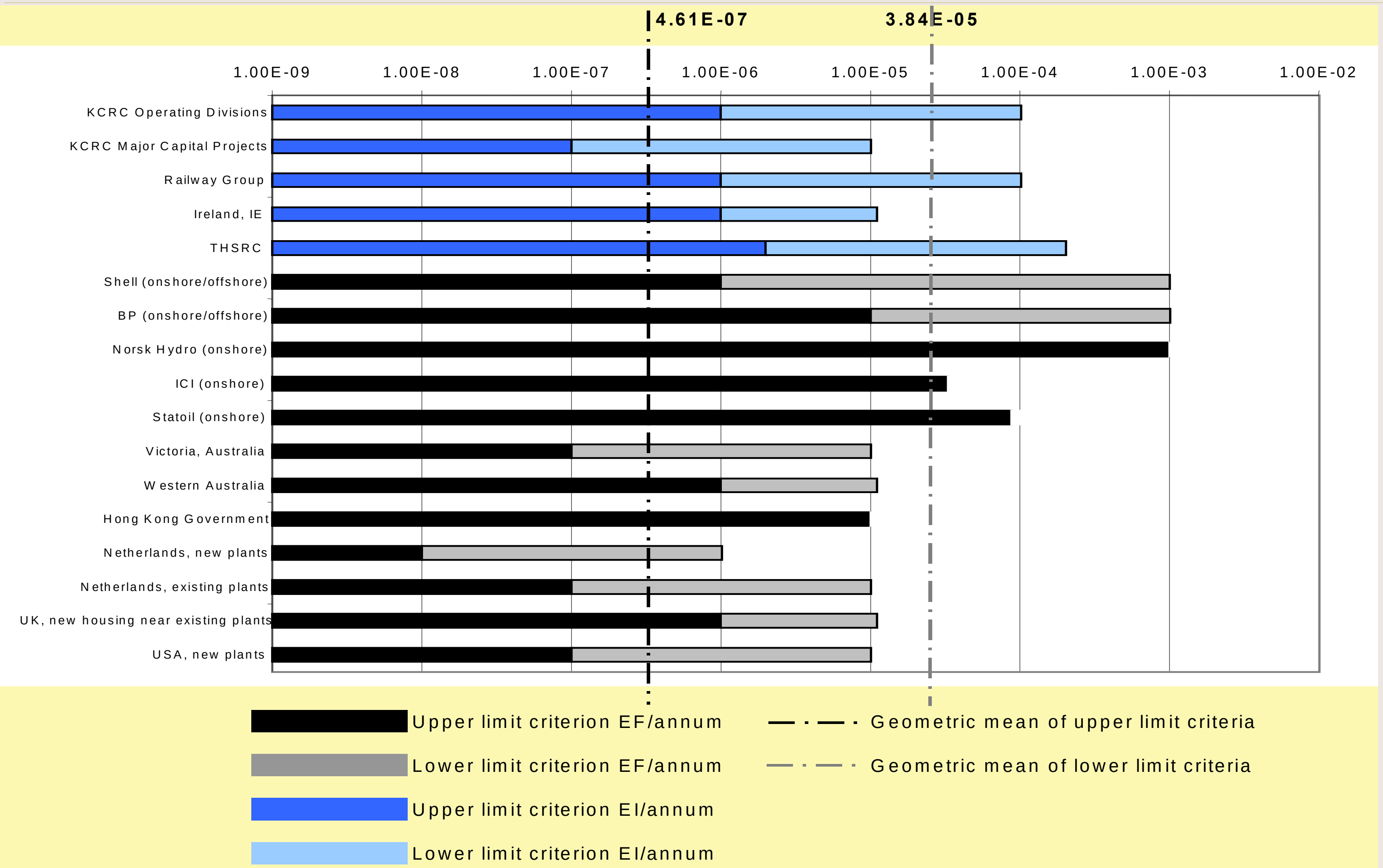
Staff Individual Risk

(EI/annum)



Public Individual Risk

(EI/annum)



Individual Risk – Pros and Cons

Pros

- Simple concept
- Public association with betting odds
- Easy to benchmark with everyday events
- Ability to differentiate between voluntary and involuntary

Cons

- Difficult to grasp national picture
- Concept of non-zero risk is difficult to perceive
- ‘It can happen tomorrow’ dilutes arguments

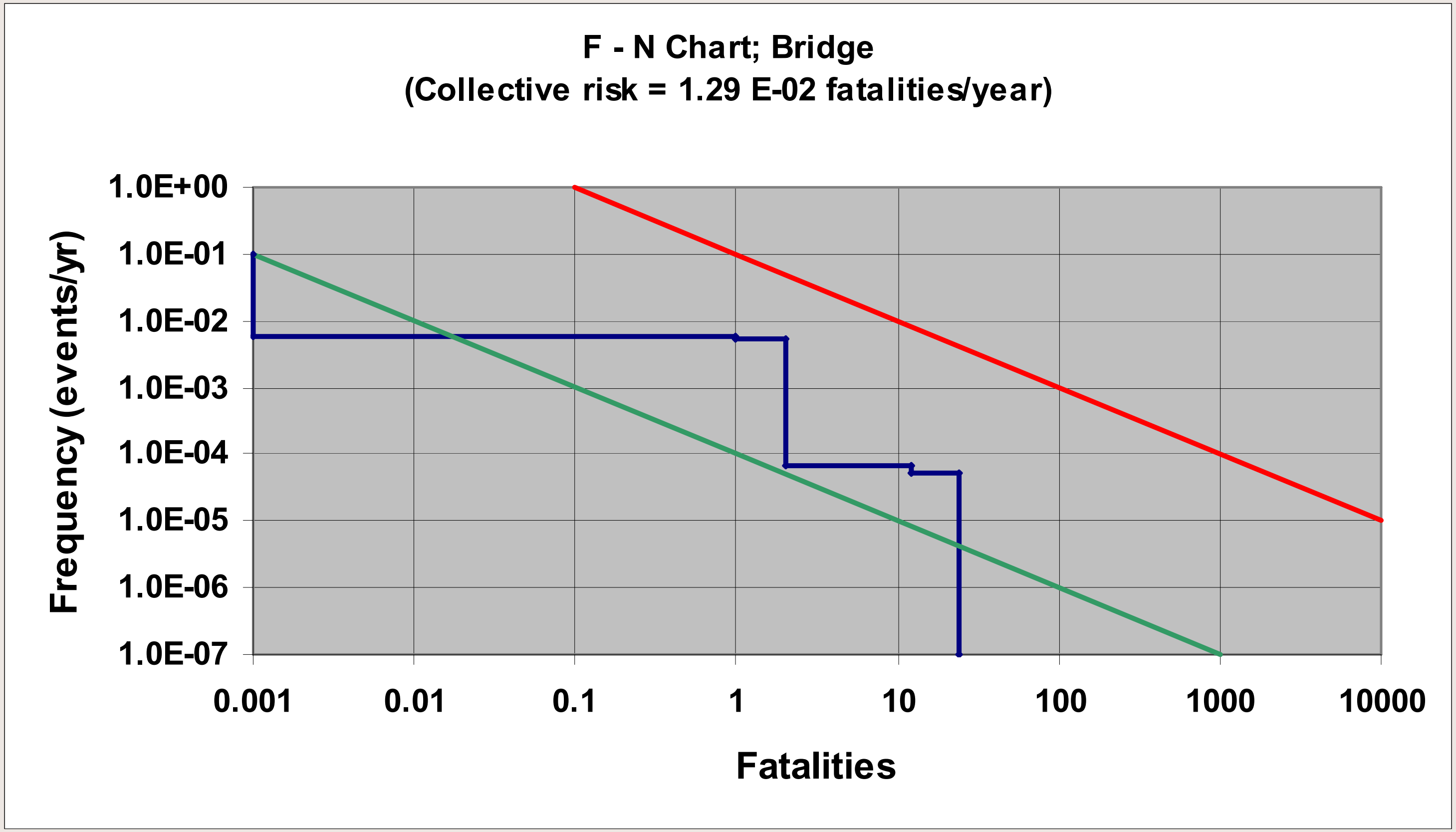
Societal Risk

- Considers risk to a community or defined population
- Takes account of accidents involving multiple fatalities

Typical Societal Risk Criteria

HKARMS 香港風險管理與安全協會 Hong Kong Association of Risk Management and Safety

Societal Risk Example



F/N Curves, Points to Note

- **Scientific notation -??**
- **Gradient of –1 implies risk neutral**
- **Concept of ALARP is difficult**
- **Breadth of ALARP zone is even more difficult**
- **Cumulative curves are foreign to most**
- **Area under curve gives *collective risk***

Collective Risk

- Risks sum form all concerned individuals
- Area under F/N curve
- No national criteria
- Useful for Cost Benefit Analysis to test ALARP

Concepts of Risks
Conclusions

- Individual risk criteria are useful and comprehensible to many people
- They are inadequate to expressive collective risk
- Societal risk criteria are arcane but necessary to consider collective risk and carry out ARARP
- Several organisations are shying away from societal risk
- Need to develop methodologies to take account of economic esthetical and social issues

Risk Management Principles

Two Key Questions

- **How safe is safe?**
- **How much can you afford safety?**

Typical Acceptable Risk

LAND USE	FATALITIES/YEAR
Hospitals, Schools, Child Care facilities	0.5×10^{-6} per year
Residential developments and places of continuous occupancy. (e.g.; hotels)	1×10^{-6} per year
Commercial developments, offices, warehouses etc	5×10^{-6} per year
Sporting complexes	10×10^{-6} per year
Industrial sites	50×10^{-6} per year

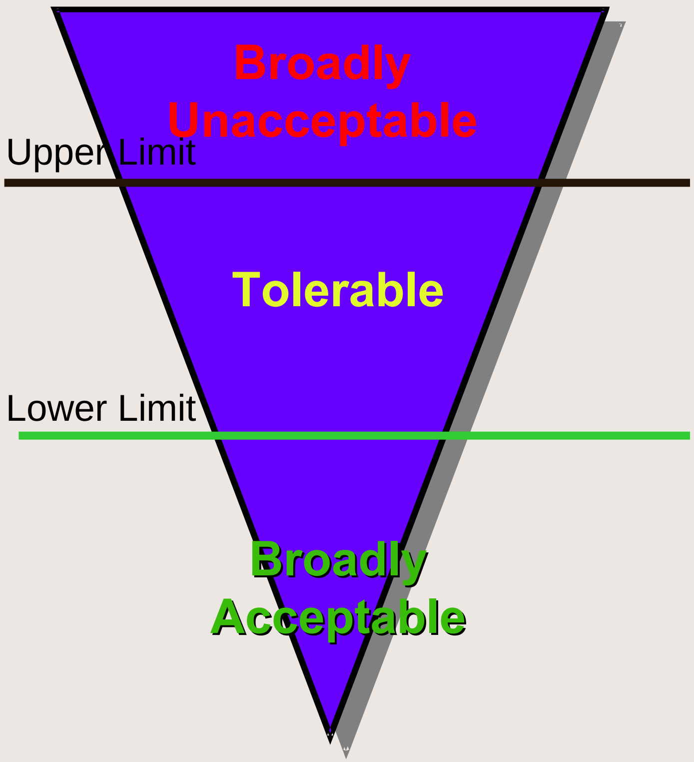
Some Criteria Can be Very Detailed

- "Toxic concentrations in residential areas should not exceed a level which would be seriously injurious to sensitive members of the community following a relatively short period of exposure at a maximum frequency of 10 in a million per year
- Toxic concentrations in residential areas should not cause irritation to eyes or throat, or coughing or other acute physiological responses in sensitive members of the community over a maximum frequency of 50 in a million per year

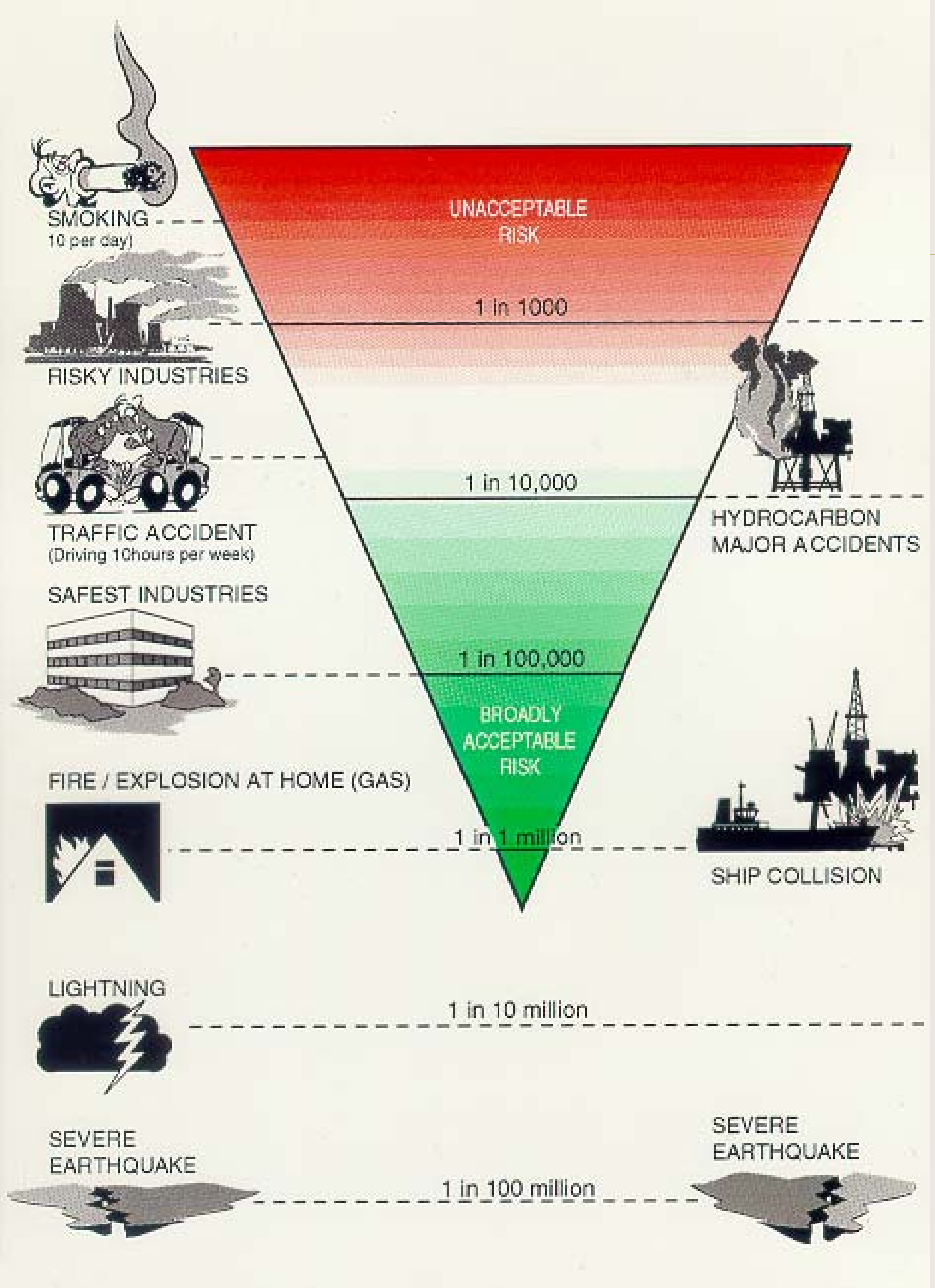
Common Principles in Risk Acceptance

- As low as reasonably practicable (ALARP)
- Globally at least as good –Globalement Au Moins Aussi Bon (GAMAB)
- Minimum Endogenous Mortality (MEM)

ALARP: As Low As Reasonably Practicable



- Commonly adopted in UK and related systems
- Broadly distinguish risks into 3 regions
- If risk falls into Tolerable (ALARP) region, risk reduction is introduced unless the cost is grossly disproportional to the improvement gained
- Many gray areas


SMOKING
10 per day)
UNACCEPTABLE
RISK
1 in 1000
RISKY INDUSTRIES
TRAFFIC ACCIDENT
(Driving 10hours per week)
1 in 10,000
HYDROCARBON
MAJOR ACCIDENTS
SAFEST INDUSTRIES
1 in 100,000
BROADLY
ACCEPTABLE
RISK
FIRE / EXPLOSION AT HOME (GAS)
1 in 1 million
SHIP COLLISION
LIGHTNING
1 in 10 million
SEVERE
EARTHQUAKE
1 in 100 million
SEVERE
EARTHQUAKE

GAMAB: Globally At Least As Good

- Any system change shall keep the total risk at the same level or lower
- Consider all aspects of the system; "total risk"gives room for trade off
- Assume existing risk is tolerable; focus on "delta" risk
- Avoid black and white risk acceptance

MEM: Minimum Endogenous Mortality

- Use the mortality rate of a specific population or social group as an indicator – the background risk
- Any technological system change shall not significantly increase the mortality rate
- Allow acceptance criteria that are based on the social setting and culture; e.g., the lower limit is 0.1% of background risk

Risk Acceptance Criteria Observations

- Assume one "knows" a level of risk that is acceptable to all stake-holders
- Assume a black and white world, either acceptable or not acceptable. Skillful analyst can direct the result as he sees fit

- Some systems set an upper limit on consequence, regardless what the probability is
- GAMAB and MEM do not depend on costs

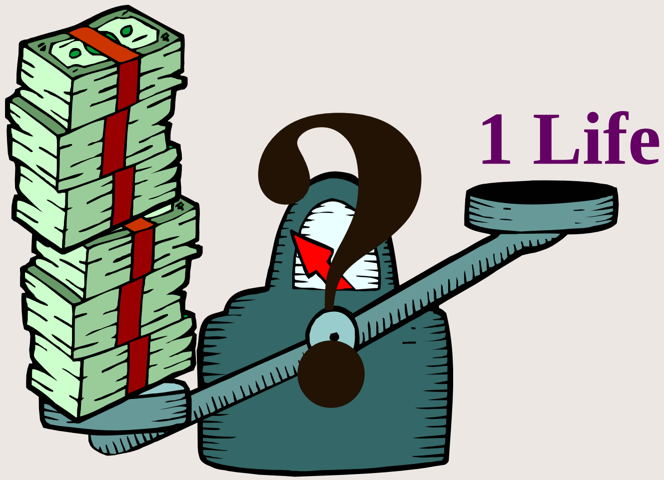
Two Key Questions

- How safe is safe?
- **How much can you afford safety?**

Expected the unexpected – always think outside the box

What is The Cost of Safety?

- Safety improvement alternatives must be balanced against the improvement in safety or reduction in risk
- The cost of safety measures must be balanced against failure costs



Failure Costs

- Loss in human life, quality of life, level of comfort
- Increased insurance premiums
- Lost time
- Loss in morale
- Production
- Equipment and materials damage
- Rework

Cost to Save a Statistical Life

Regulation	mortality/10^6 exposed	cost/life saved ($million)
Unvented space heater ban	1890	0.1
Seat belts	6370	0.1
Aircraft seat cushion flammability	11	0.4
Crane suspended platform standard	81,000	0.7
Children's sleepwear flammability	29	0.8
Standards for radionucleides in uranium mines	6300	3.4
Occupational exposure limit for asbestos	3015	8.3
Asbestos ban		110.7
Hazardous waste wood preservatives	<1	5,700,000

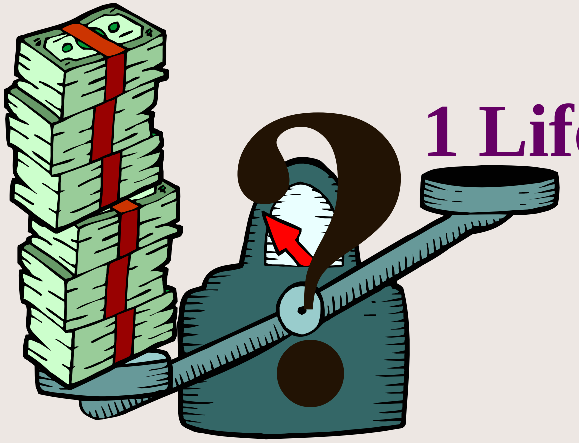
Decisions are often irrational and are with special interest

Value of Life

- Need a unit to measure cost of life
- Equate death or level of injuries to a dollar value
  - A fatality can be assumed to be equal to X number of major injuries and Y number of minor injuries
  - Value of life would then be a function of death, major and minor injuries
- Typical values of life
  - US$2.7m/life for US transportation industry
  - A$900k/life for Australian mining and A$3m/life to $10m/life for Chemical Plants

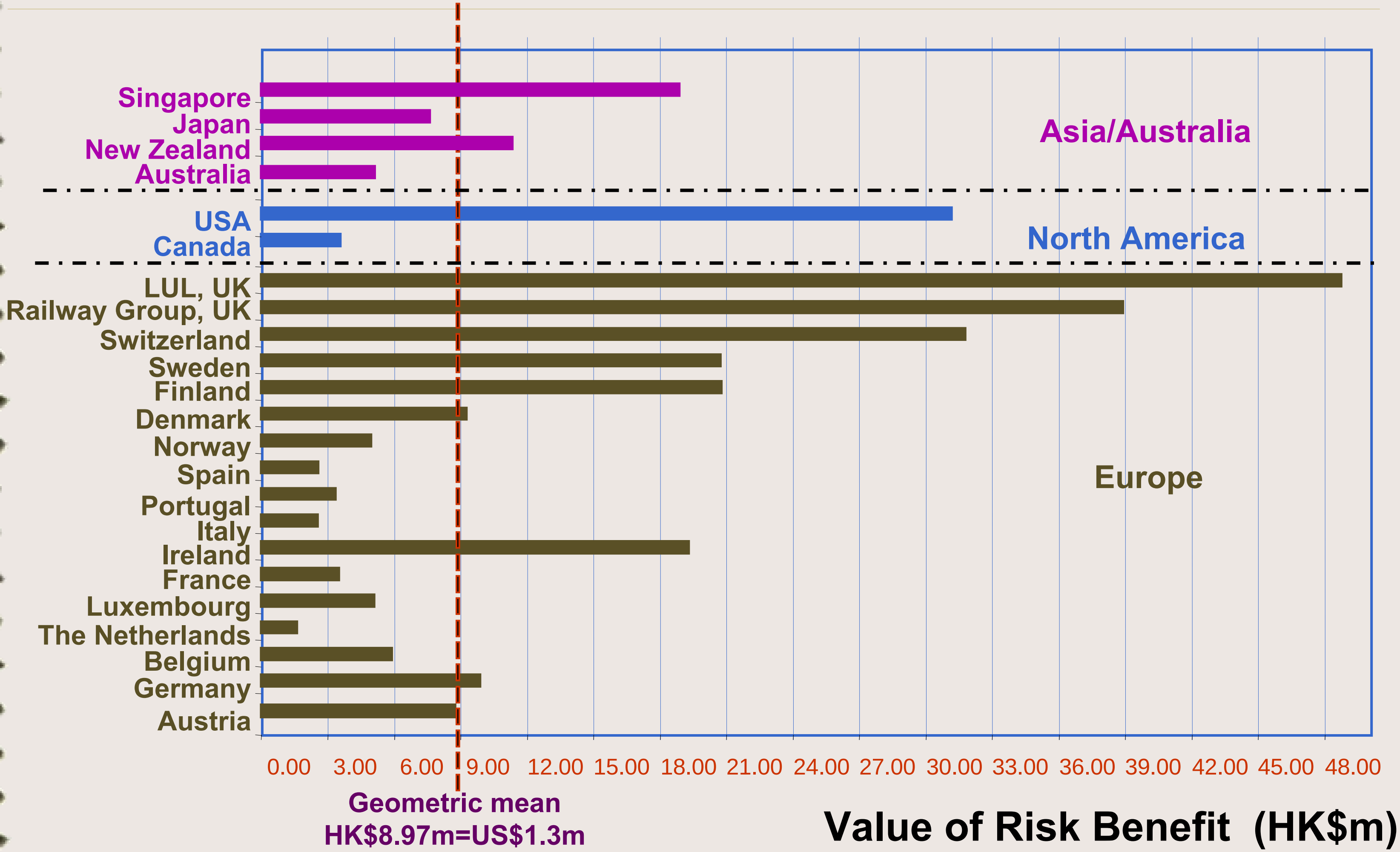
Value of Risk Benefit

- To determine whether a risk mitigation measure is cost-effective
- Equate consequences (death or level of injuries) to a dollar value
- Other terms:
  - value of life
  - willingness to pay
  - value to prevent fatality
  - value to avoid death
- Not politically correct: value of “whose” life?
- Controversial but unavoidable topic



HKARMS 香港風險管理與安全協會 Hong Kong Association of Risk Management and Safety

Survey of Value of Risk Benefit Used



HKARMS 香港風險管理與安全協會 Hong Kong Association of Risk Management and Safety

Cost/Risk-Benefit Analysis

- Commonly used in evaluating the cost-effectiveness of safety measures

$$B/C = \frac{Risk_{Existing} - Risk_{Residual}}{Cost}$$

- Risk-benefit may include passenger risk, property damage, risk perception, etc.
- Risk-benefit is converting to $: Value of risk benefit, value of preventing fatality, willingness to pay, value of life saved, etc.
- May include risk aversion factors for multiple deaths

Cost/Risk-Benefit Analysis

$$B/C = \frac{Risk_{Existing} - Risk_{Residual}}{Cost}$$

- **While costs are calculated by standard financial equations, benefits are assessed by risk analyses**
- **If *B/C* >1, an alternative is generally considered cost-effective; however, there are exceptions**

Example

- Subject: Reduce the risk of falling objects
- Option A: buy a better ladder
  - Cost: $2000
  - Risk benefit: 1 injury reduction per year
  - Each injury costs, on the average, $10,000
  - B/C ratio = ($10,000 x 1)/$2000 = 5
- Option B: Wear safety helmet
  - Cost: $100
  - Risk benefit: 0.5 injury reduction per year
  - Each injury costs, on the average, $10,000
  - B/C ratio = ($10,000 x 0.5)/$100 = 50
- Garbage-in, garbage-out. Are the inputting data realistic?

Cost/Risk-Benefit Analysis

- Example
  - Safety Project A can reduce the risk by 5 fatality per year and a life costs HK$15M. The risk benefit of Project A is 5x$15M=$75M
  - Total cost of Project A is $25M
  - B/C is $75M/$25M=3 > 1; it is an viable option
  - If the project cost is $150M, B/C = 0.5<1; it is not a cost-effective option
- The B/C ratio can be used to rank order the cost-effectiveness of different options

Cost/Risk-Benefit Analysis

- Perhaps, the most important use of risk information in safety management
- risk acceptance criteria, and value of risk benefit are used to compare with the costs of options
- Often used as a tool to justify not to do anything
- Must consider cost of money

Purpose of Risk Management

- To please your boss?
- To optimise resources ($) by balancing cost, risk and benefit: cost/risk-benefit analysis
- To rank options (including do nothing)
- To address liability issues - Have you done enough to avoid the accident?

Can risk be “managed”, “treated” or “controlled”?

Principles of Risk Control

- Risk Elimination/Avoidance
- Risk Transfer
- Risk Reduction
- Risk Absorption

Chance only favors the prepared mind.

Louis Pasteur

Risk Management

- Risk Management is a term given to a set of practices that lead to minimizing possible harm to individuals

- While it may not be possible to totally protect individuals, a risk management system seeks to identify factors that may increase those risks and actively promote practices that will keep risk as low as reasonably practicable

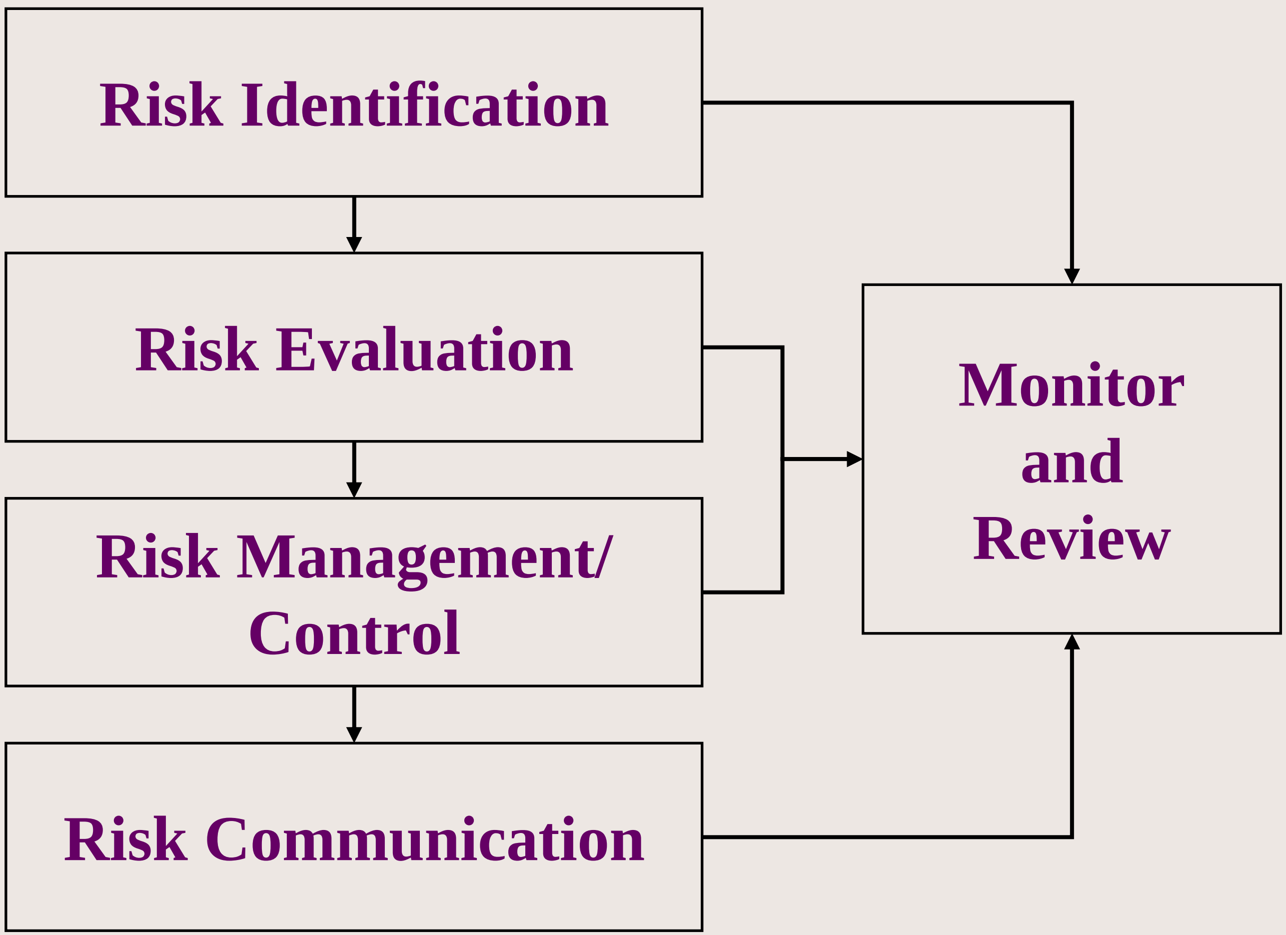
Risk Management Principles

- Prevention of serious incidents is the highest priority
- Safe and accessible environments are everyone’s responsibility
- Continuous communication, accurate reporting, consistent analysis of information, and development of sound, person-centered strategies are essential to prevent serious incidents

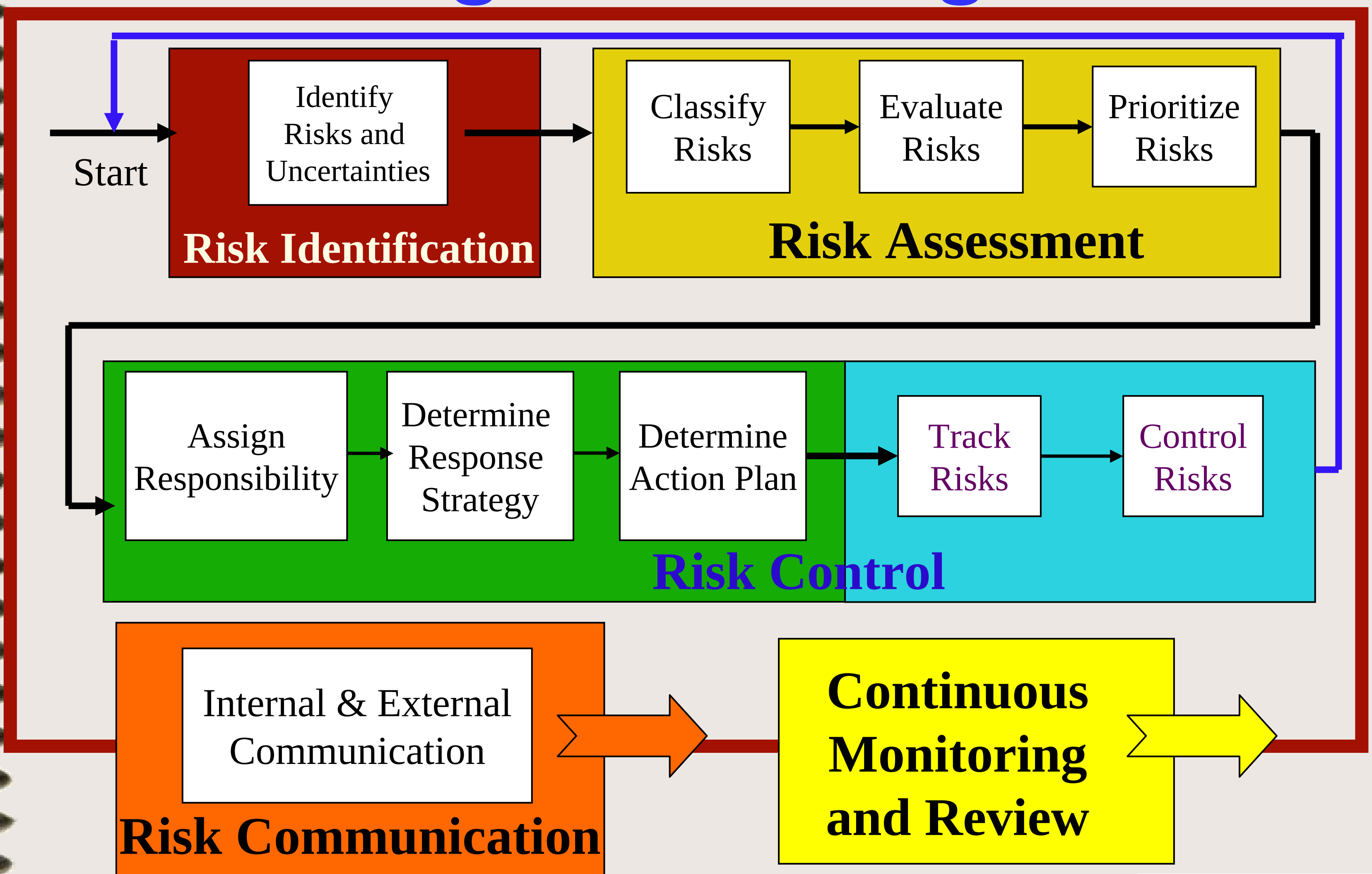
Risk Management Principles

- Staff are competent to respond to, report and document incidents in a timely and accurate manner
- Individuals have the right to a quality of life that is free of abuse, neglect, and exploitation
- Risk management systems should emphasize staff involvement as integral to providing safe environments
- Quality of life starts with those who work most closely with persons receiving services and supports

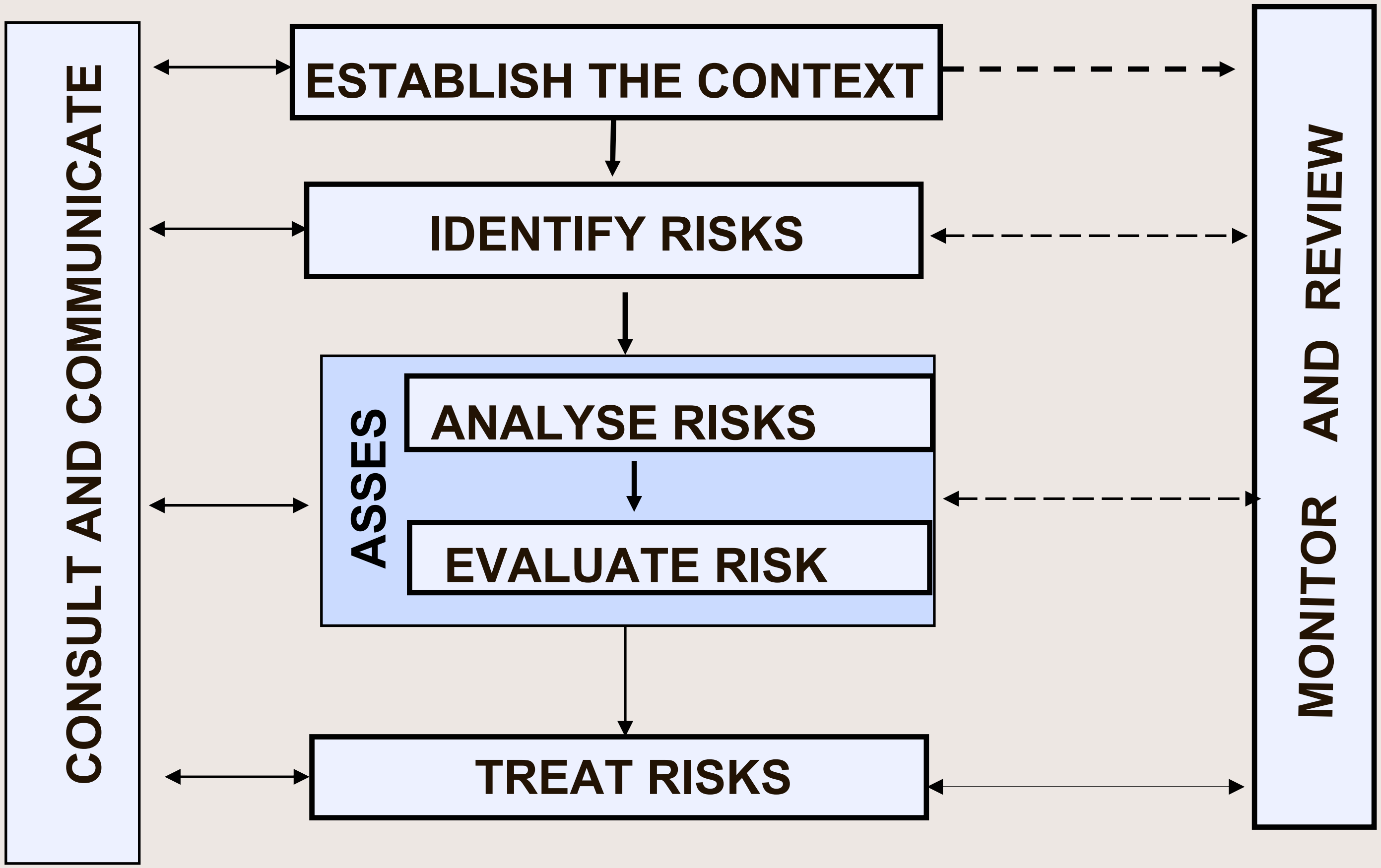
Key Steps in a Risk Management Program



Key Steps in a Risk Management Program



Risk Management AS/NZS 4360



Elements of Effective Risk Management

- Training of all involved in supporting individuals with developmental disabilities in the risk management process
- Individual risk assessment, evaluation, and planning
- A well-defined process for reporting incidents that is timely, complete, and accurate
- Immediate follow up and intervention to ensure health and safety and to mitigate future risk

Elements of Effective Risk Management

- Regular review and analysis of incidents by a risk management, assessment and planning committee
- Trending of data to detect patterns and facilitate development of risk mitigation strategies
- Proactive measures to prevent or minimize the likelihood of further incidents


crashtst.mpeg

Risk Management Principles

Conclusions

- Address “How safe is safety “ by designing risk acceptance criteria
- Apply value of risk-benefit in cost/risk-benefit analysis to address “How much can you afford safety?”

Fault Tree Basics

Typical Tools to Perform Risk Management

- Hazard Log
- Preliminary Hazard Analysis (PHA)
- Hazard & Operability Analysis (HAZOP)
- Failure Mode, Effects, and Criticality Analysis (FMECA)
- Fault Tree Analysis (FTA)
- Event Tree Analysis (ETA)
- Subsystem Hazard Analysis (SSHA)
- System Hazard Analysis (SHA)
- Interface Hazard Analysis (IHA)
- Operating & Support Hazard Analysis (O&SHA)
- System Assurance (SA) Modelling
- Design Safety Review (DSR)
- Safety Audits

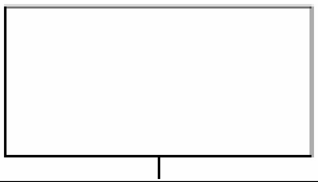
Fault Trees Analysis

- Start with Top Event and follow through scenario
- Use deductive logic to systematically identify event initiators
- Separate tree into functional level, system level, subsystem level, component level, fault level, etc.
- Bottom of the tree are basic events or developed events
- Can be qualitative or quantitative

Fault Tree Symbols

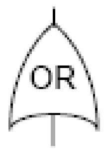
- Two kinds of symbols are used in a fault tree:
  - Logic symbols
  - Event symbols
- Many symbols and styles, we stay with the simple ones here

Fault Tree Symbols – Logic Symbols

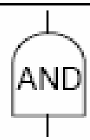


TOP Event – forseeable, undesirable event, toward which all fault tree logic paths flow,or **Intermediate event** – describing a system state produced by antecedent events.

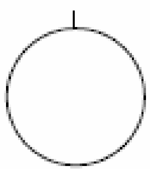
Most Fault Tree Analyses can be carried out using only these four symbols.



"Or" Gate – produces output if any input exists. Any input, individual, must be (1) necessary and (2) sufficient to cause the output event.



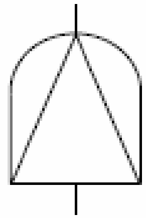
"And" Gate – produces output if all inputs co-exist. All inputs, individually must be (1) necessary and (2) sufficient to cause the output event



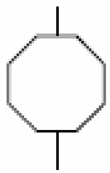
Basic Event – Initiating fault/failure, not developed further. (Called "Leaf," "Initiator," or "Basic.") The Basic Event marks the limit of resolution of the analysis.

Events and **Gates** are **not** component parts of the system being analyzed. They are symbols representing the logic of the analysis. They are bi-modal. They function flawlessly.

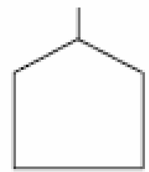
Fault Tree Symbols – More Symbols…



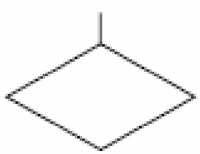
Priority AND Gate
$P_T = P_1 \times P_2$
Opens when input events occur in predetermined sequence.



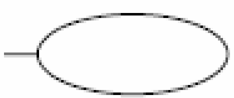
Inhibit Gate
Opens when (single) input event occurs in presence of enabling condition.



External Event
An event normally expected to occur.

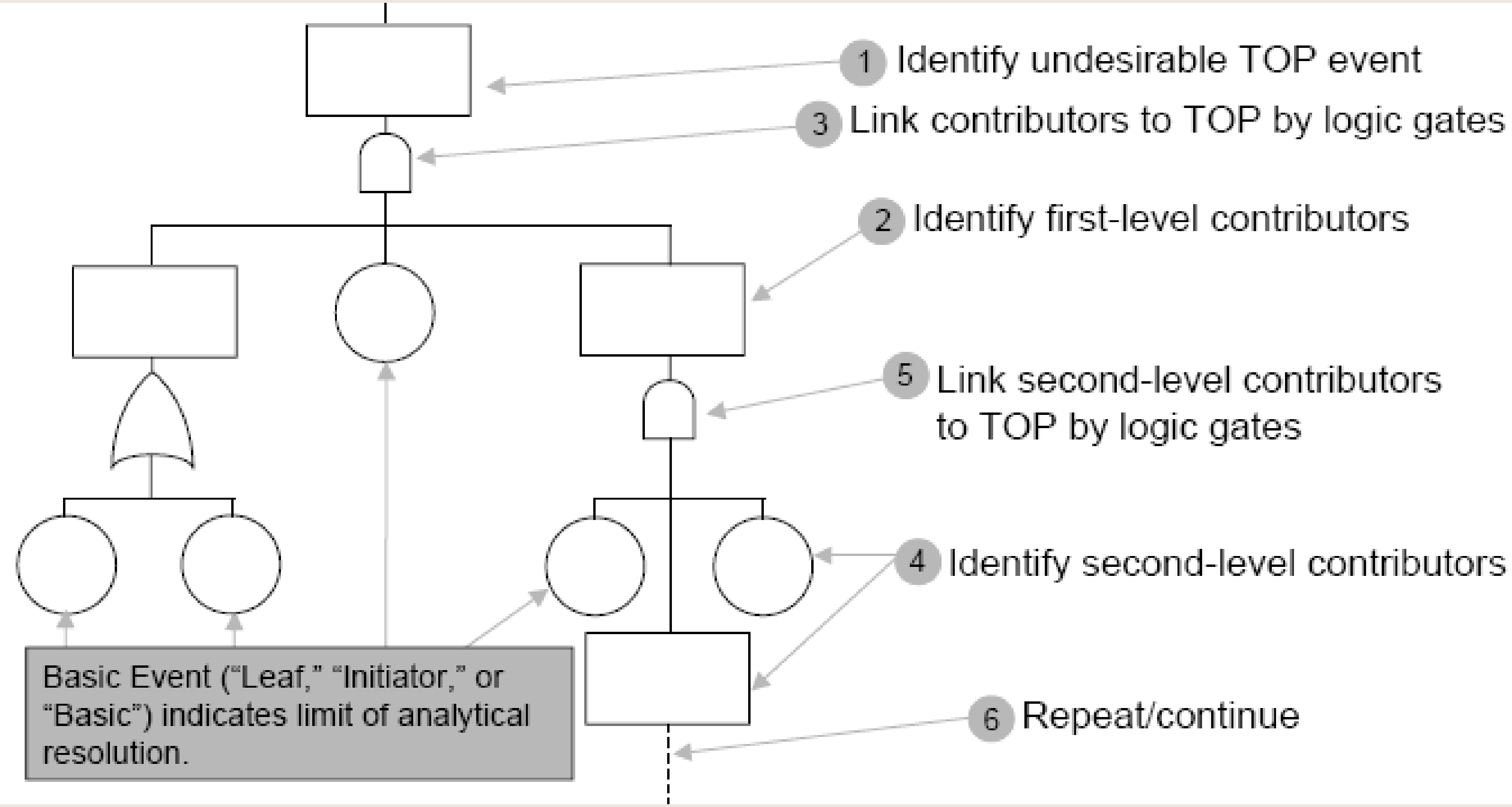


Undeveloped Event
An event not further developed.

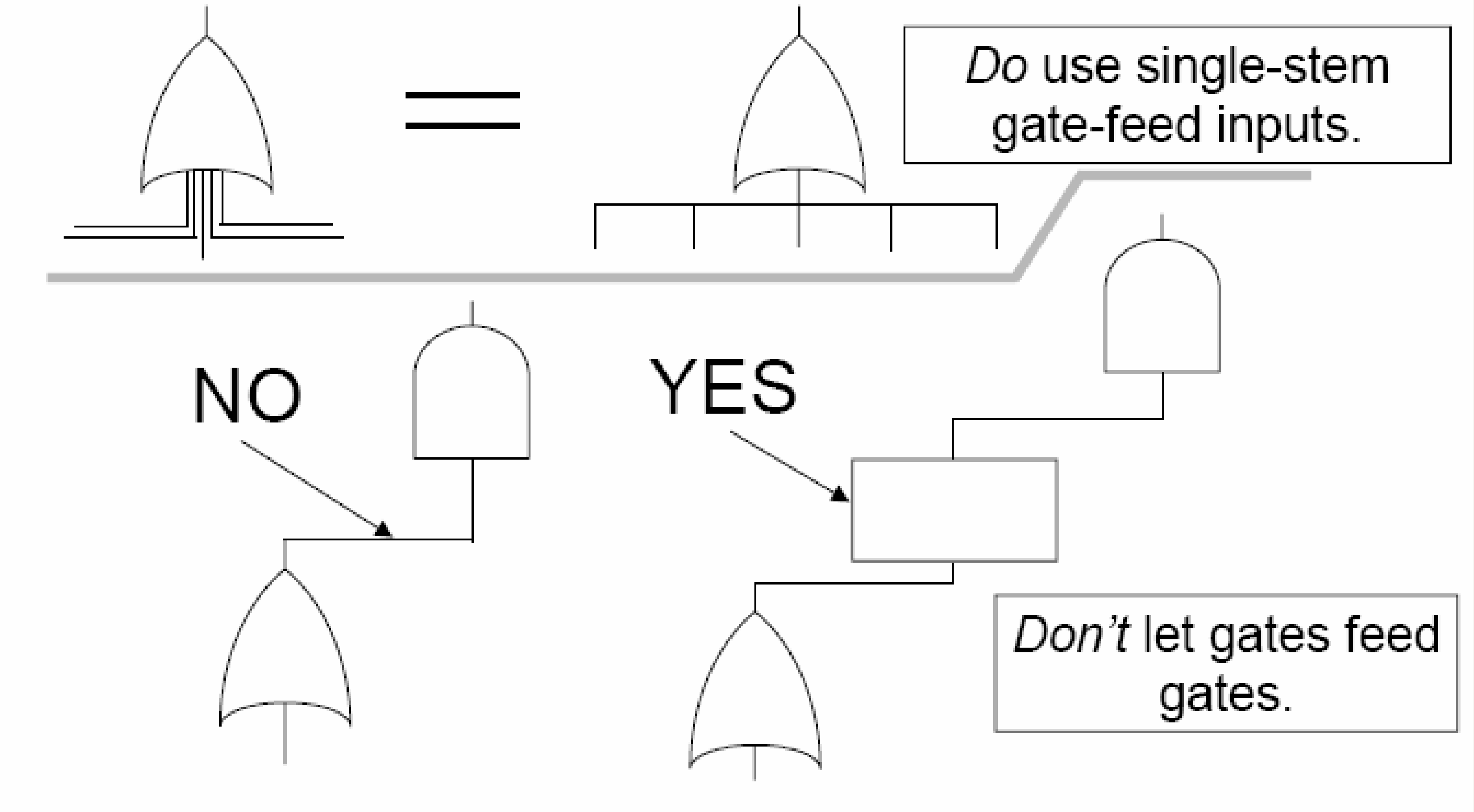


Conditioning Event
Applies conditions or restrictions to other symbols.

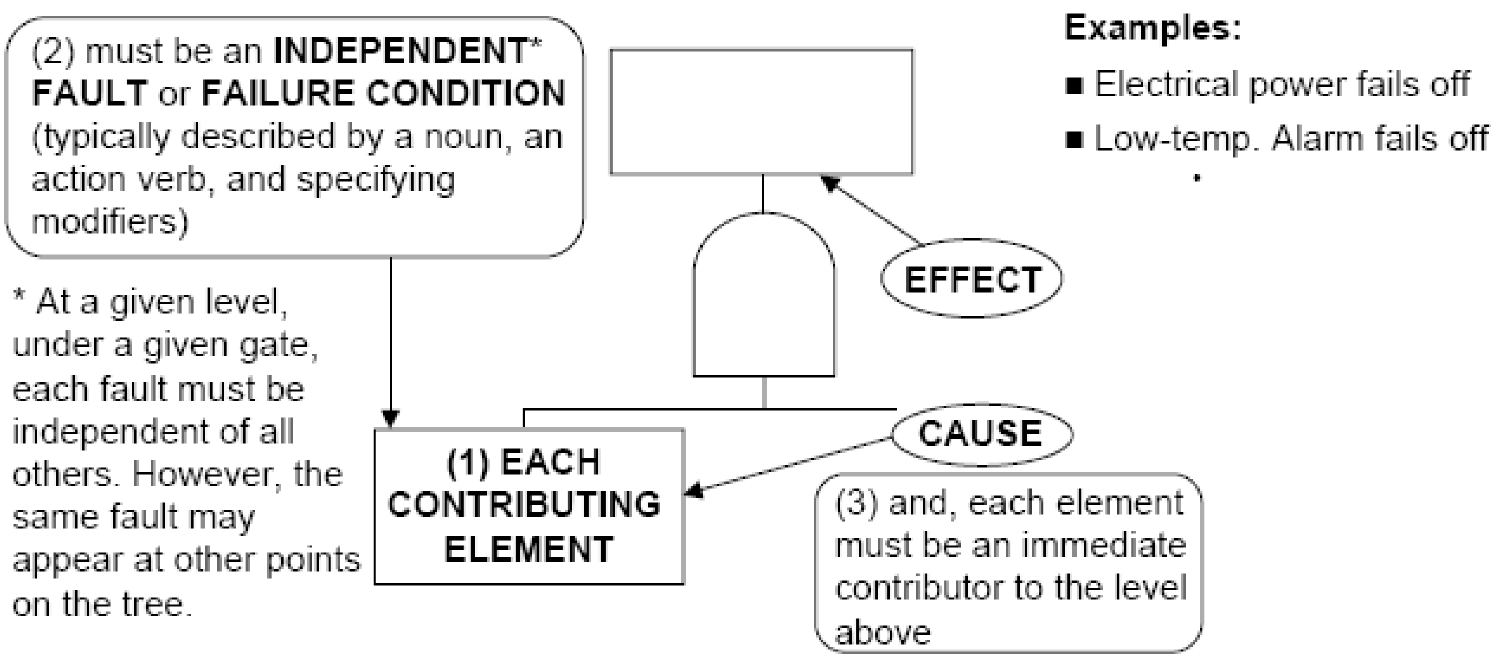
Fault Tree Symbols – Event Symbols



Fault Tree Symbols – Event Symbols



Fault Tree Symbols – Event Symbols

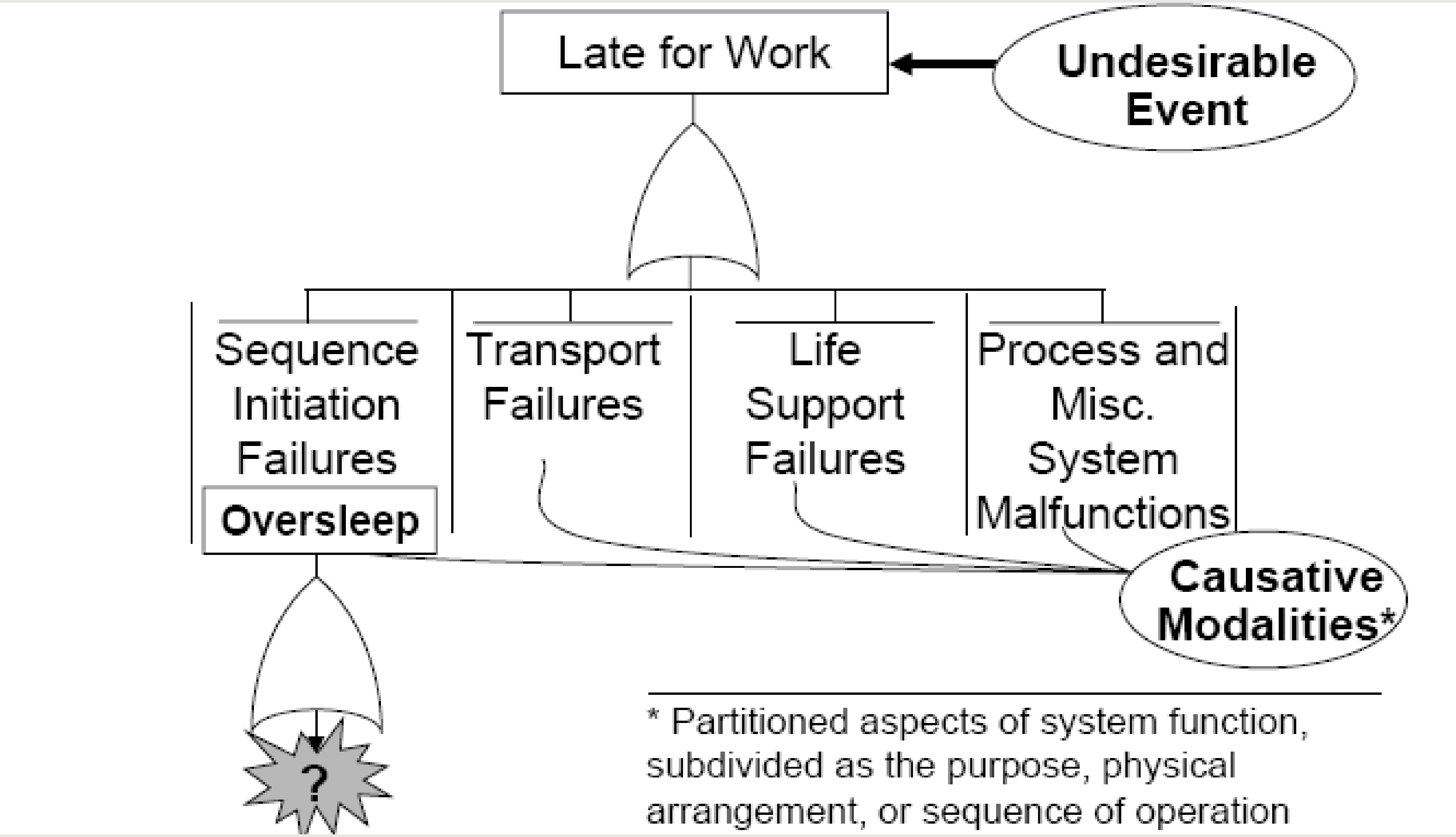


NOTE: As a **group** under an AND gate, and **individually** under an OR gate, contributing elements must be both **necessary** and **sufficient** to serve as **immediate** cause for the output event.

Fault Tree Construction

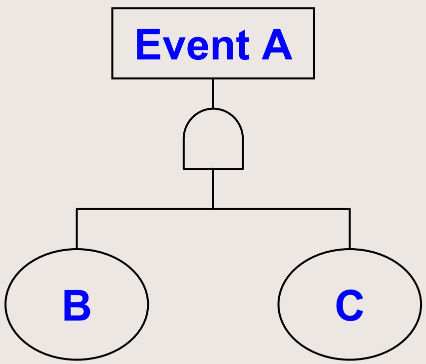
- Identify the Undesired Top Event. A different tree is required for each unique Top Event
- Constructing the logic
- Identify and sketch the Intermediate Events to develop logical branches
- Spotting/correcting some common errors
- Adding quantitative data

Fault Tree Example

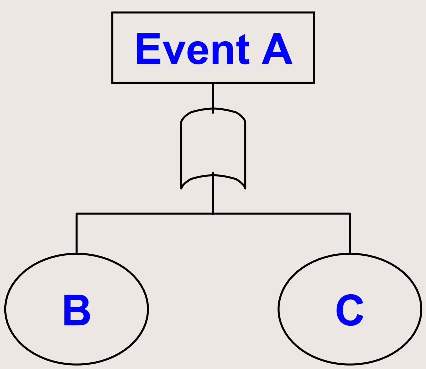


Fault Tree Structure

- Event A occurs because of Event B and Event C occur

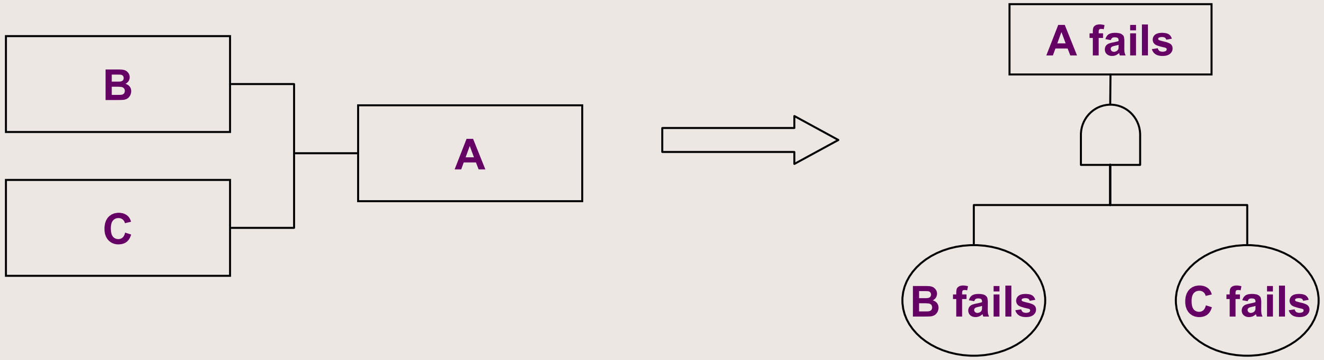


- Event A occurs because of Event B or Event C occur

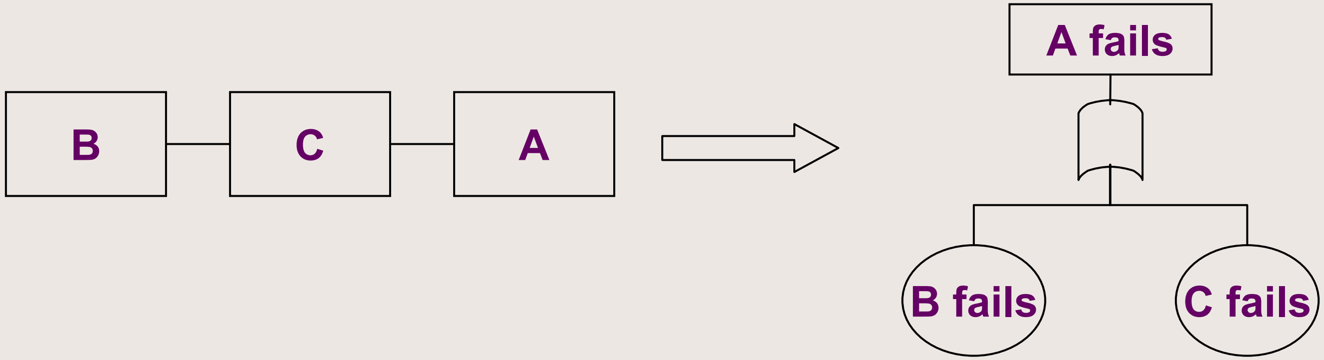


Fault Tree Structure

A parallel system (system works if either component works

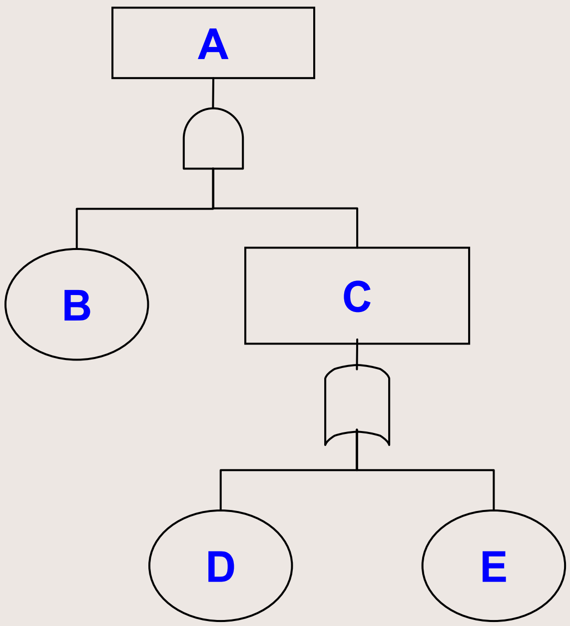


A series system (system works when all components work

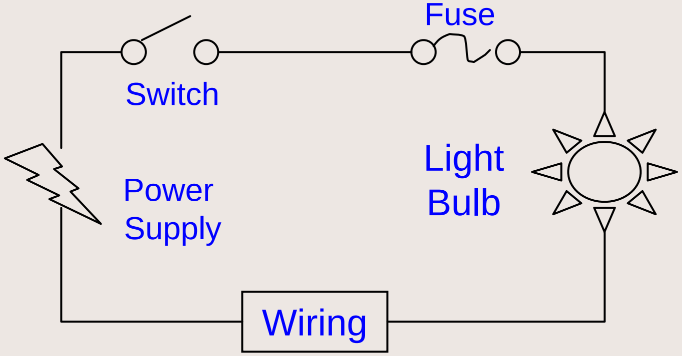


Fault Tree Structure

- Event A occurs because of Event B and Event C occur
- Event C occurs because of Event D or Event E occur

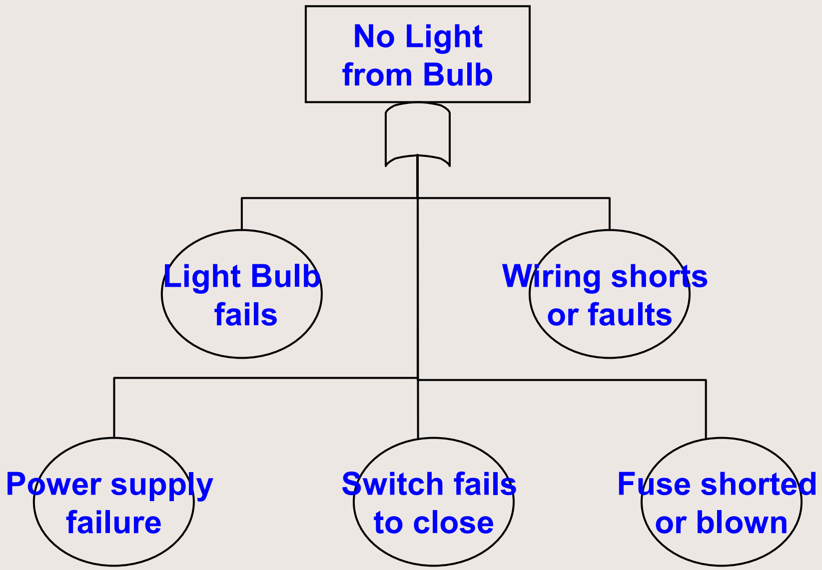


Fault Tree Structure, Example

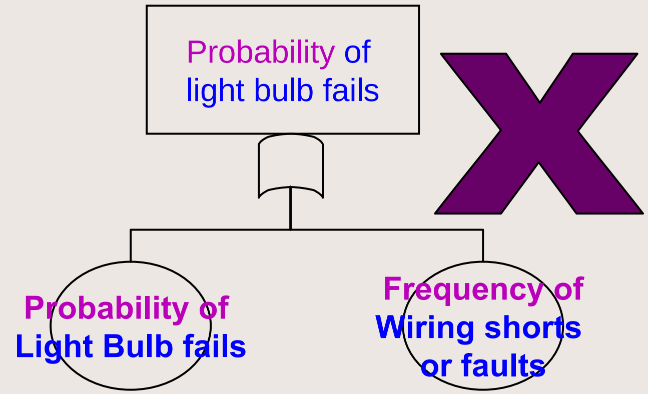


Develop fault event with top event: No light from bulb

Initial conditions: Switch closed
Not-considering events: failure external to system

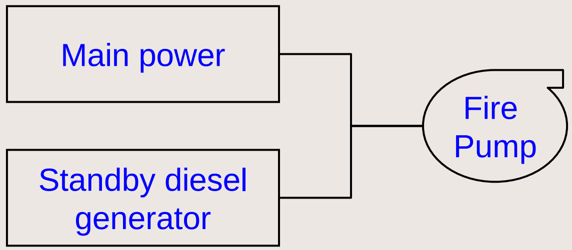


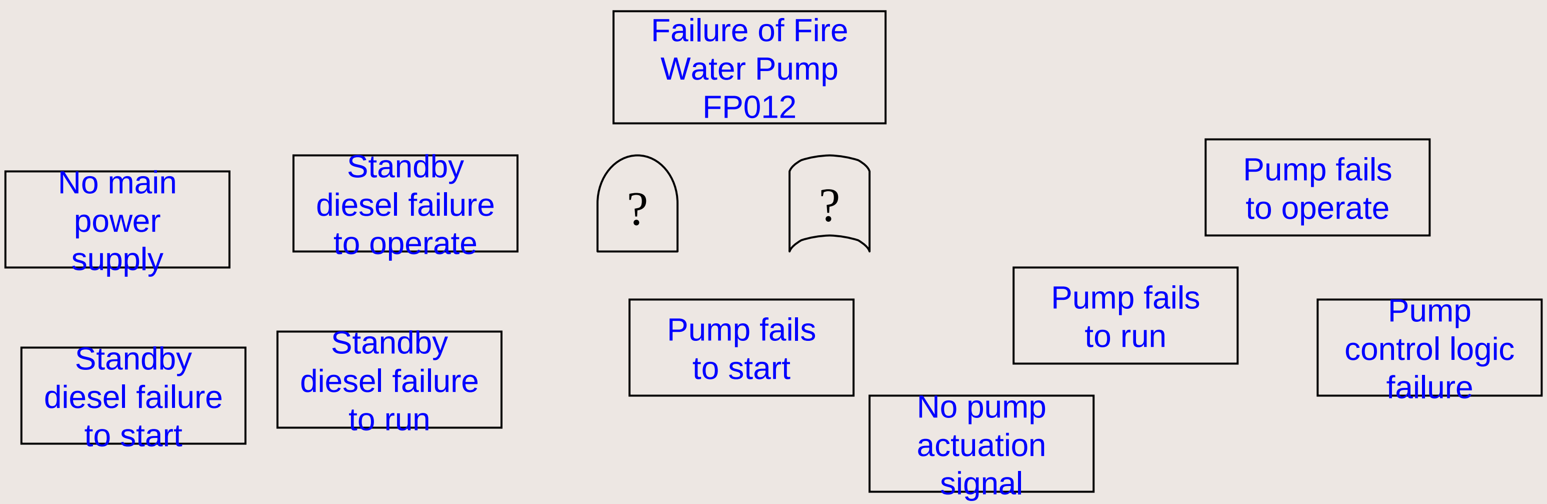
Do not put down:



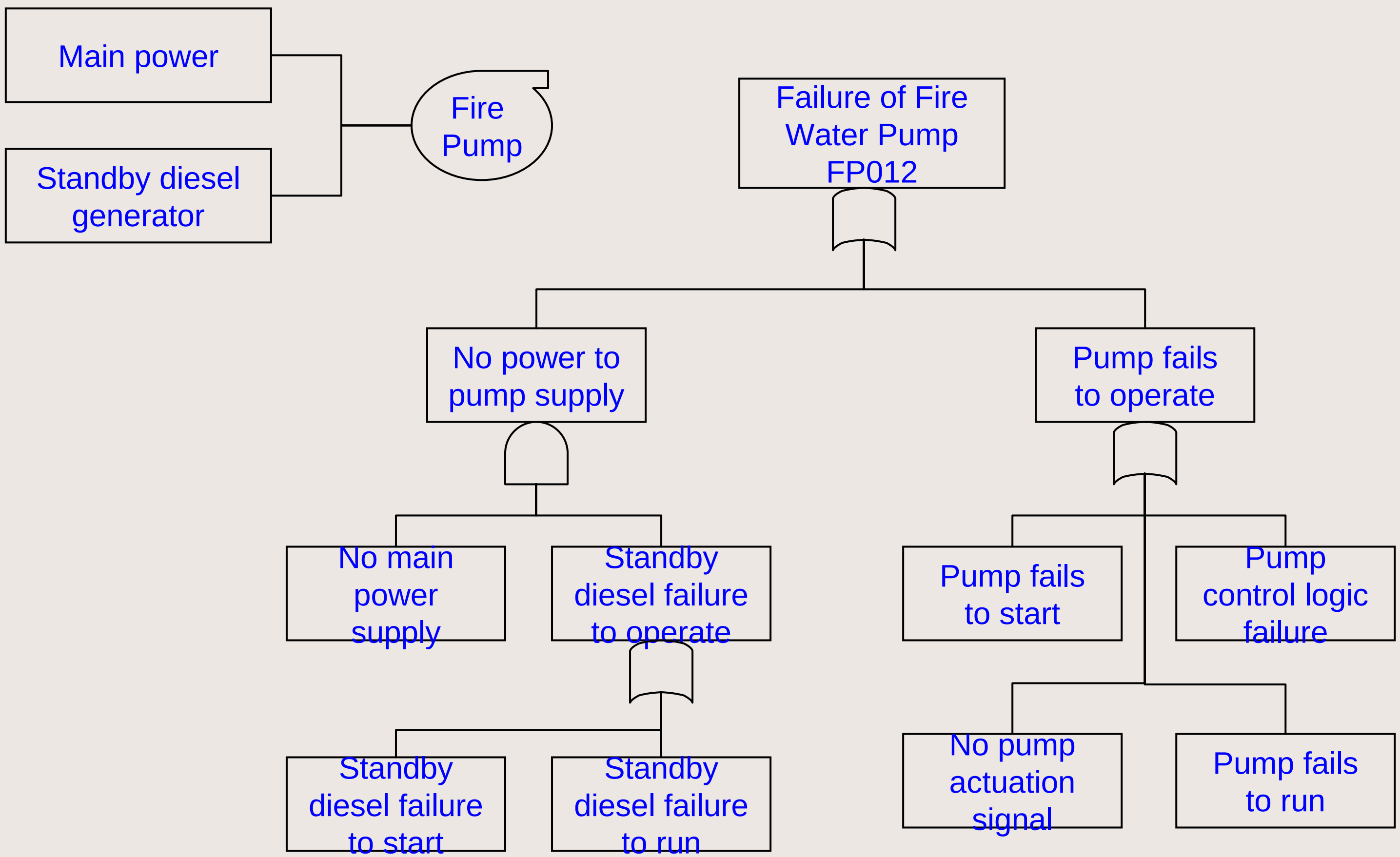
Fault Tree Structure,Example

- **Example**

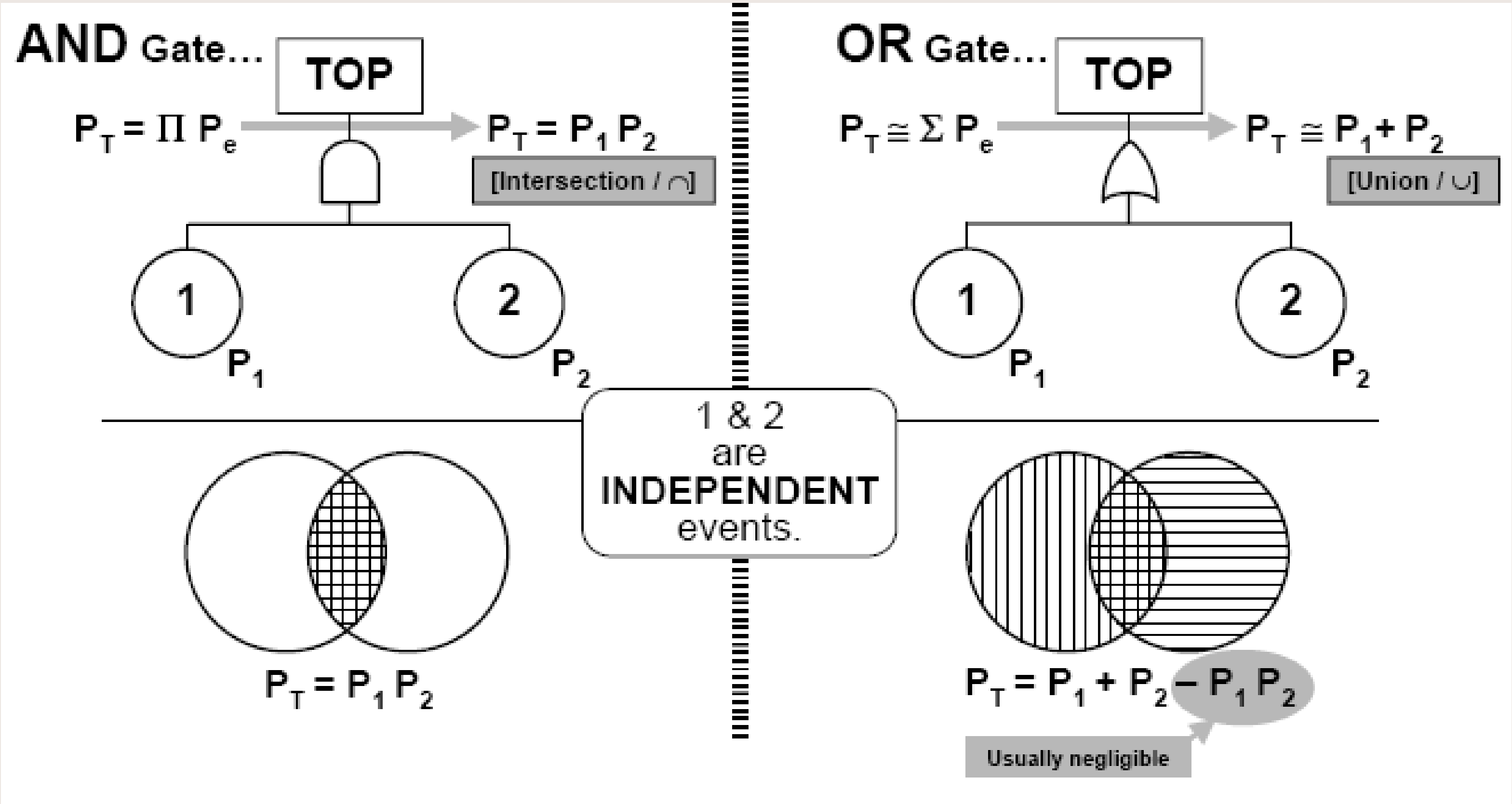




Fault Tree Structure, Example

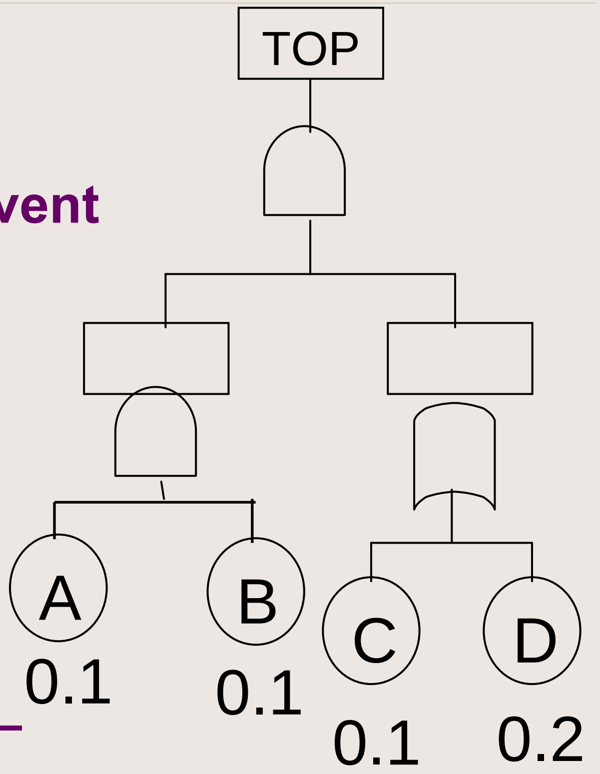


Fault Tree Calculations



Fault Tree Analysis

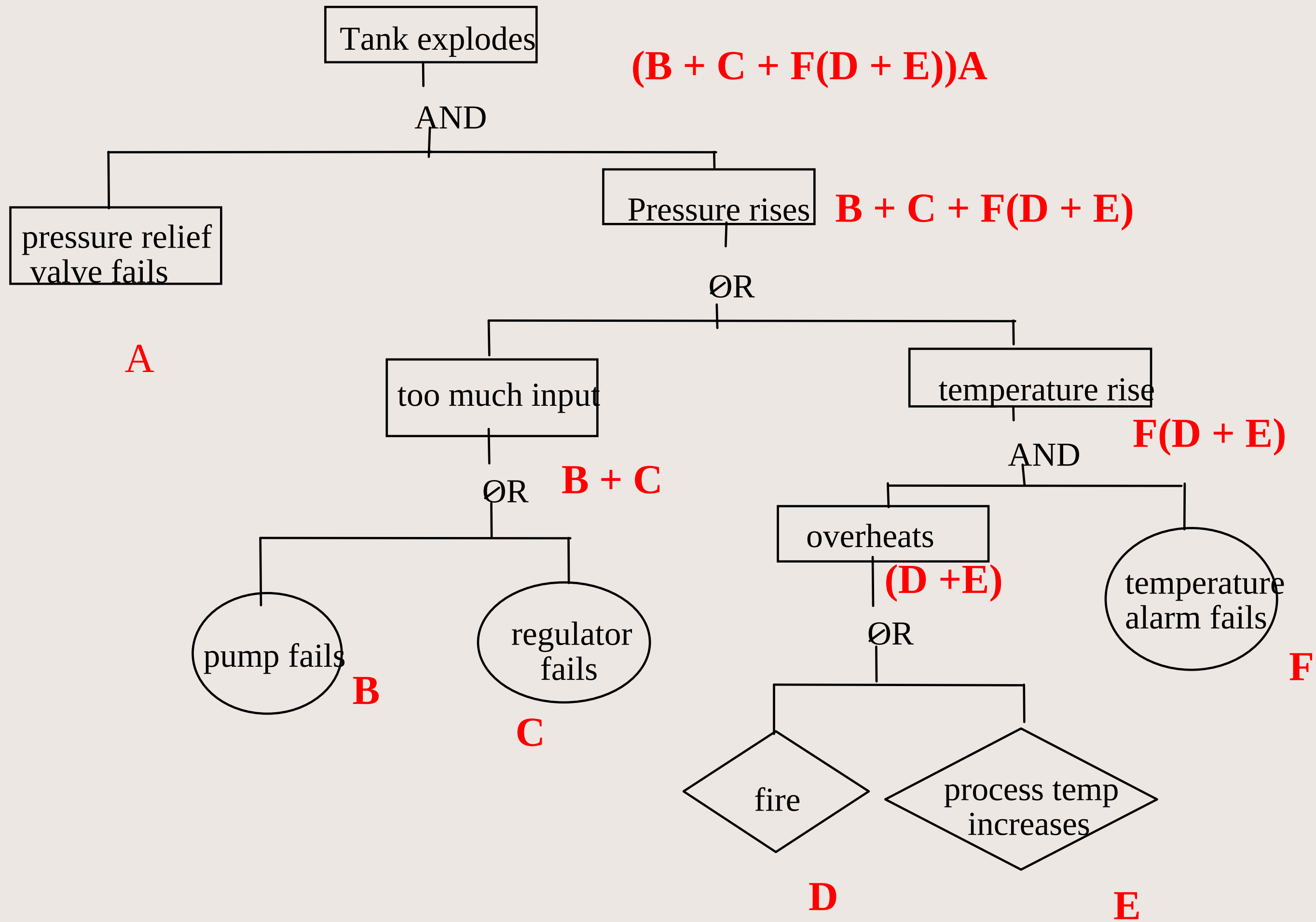
- **Fault trees use deductive logic to identify fault or failure precursors postulate and to quantify the top event probability**
- **Fault tree is based on probability theory in solving Boolean algebra**
- **Approximation:**
  - **P(Top) ≈ P(A) x P(B) x [P(C) + P(D)]**
  - **P(Top) ≈ 0.1x0.1x(0.1+0.2) = 0.003**
- **Exact:**
  - **P(Top) = P(A) x P(B) x [P(C) + P(D) – P(C)xP(D)]**
  - **P(Top) ≈ 0.1x0.1x(0.1+0.2 – 0.1x0.2) = 0.0028**



Typical Faults in Fault Tree Analysis

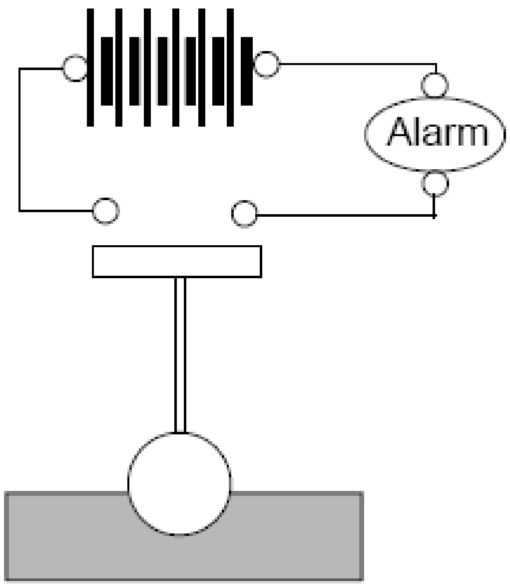
- Fault trees propagate probability or unavailability, NOT frequency
- Approximation led people to think they can add events together for “OR” gate regardless of contents
- Should not use fault tree simply to add events, A+B is not necessary A or B ;
  A or B = A + B – A*B

Fault Tree Example



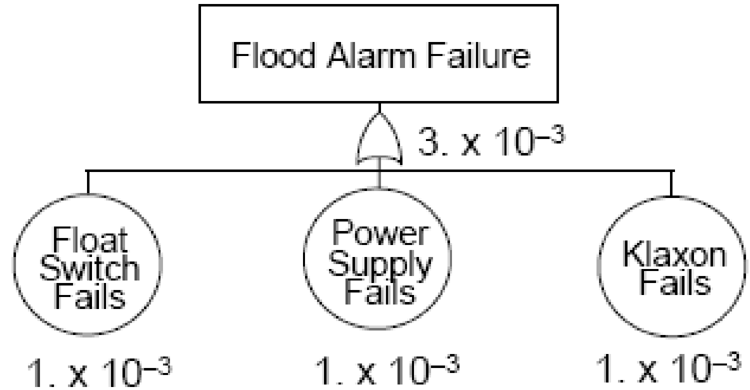
TOP= AB + AC + AFD + AFE

A Flood Alarm System



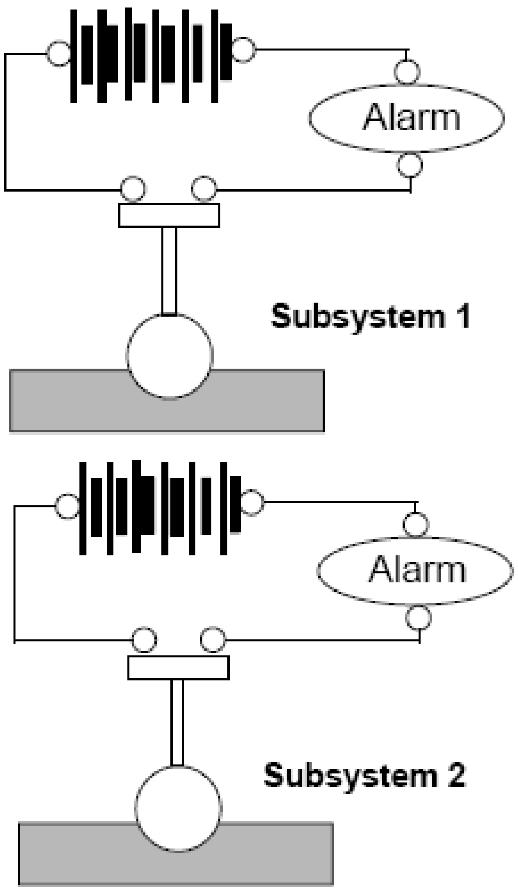
A system design goal is $P_F < 5 \times 10^{-6}$, per flood.

A subgrade compartment is protected against flooding by a simple alarm system. Each of the three components shown has a failure probability of 10^{-3} per demand. What is the probability of failure to alarm upon flooding?

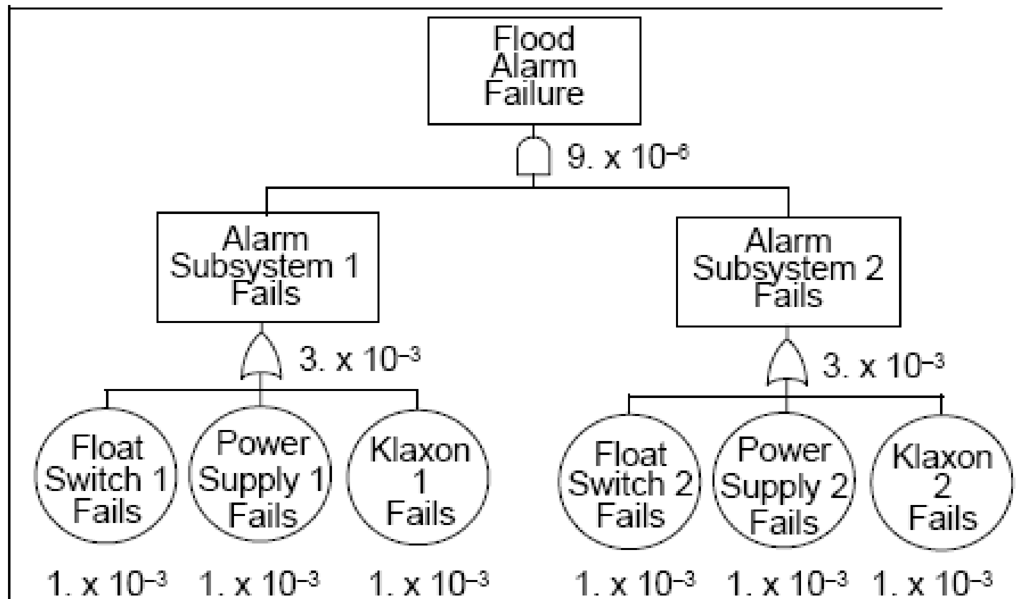


The system will fail three times in 1,000 demands, long-term average.
TOO MUCH RISK! So – go redundant.

A Flood Alarm System
Two System Redundancy

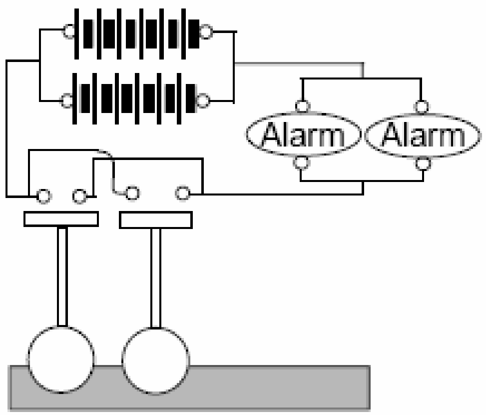


Two subsystems identical to the first system are now used. Ignoring common-cause effects, what now is the probability of failure to alarm upon flooding?

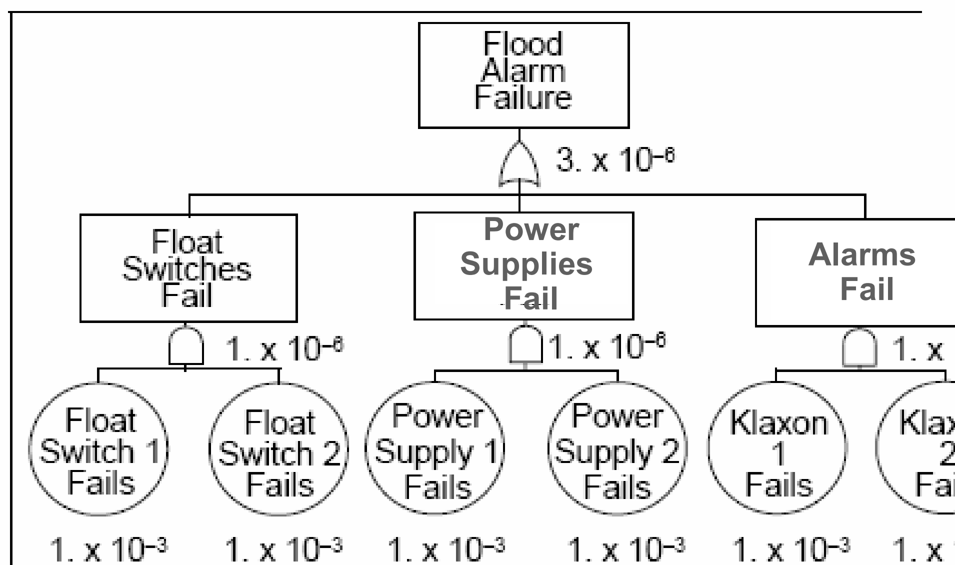


The system will fail 9 times in 10^6 demands…
STILL TOO HIGH! Can it be further reduced, perhaps using the same components?

A Flood Alarm System
Component Level Redundancy



Components themselves are made redundant, rather than the whole system. What **NOW** is the probability of alarm failure upon flooding?



The system now fails 3 times in 10^6 demands – lower by a factor of three than for the previous case.

Failure Rates

- Typically use generic frequency or rates
- Should use specific data (past failure records) with consideration of generic data
- Can use expert judgment for rare events – must handle degree of belief; i.e., uncertainties
- Can be a discrete value (like those in a risk matrix) or a continuous function

Frequency

- Frequency is a measure of the rate of occurrence. E.g., failure rate of a pump is 6.2x10-3/hr
- Frequency data are based on statistics with consideration of uncertainties (probability); e.g., the failure rate of a pump is 6.2x10-3/hr. But it could be

Frequency	Fraction	Product
1.0x10-4/hr	0.2	2.0x10-5/hr
2.0x10-3/hr	0.5	1.0x10-3/hr
3.2x10-3/hr	0.2	6.4x10-4/hr
4.5x10-2/hr	0.1	4.5x10-3/hr
	Sum:	6.2x10-3/hr

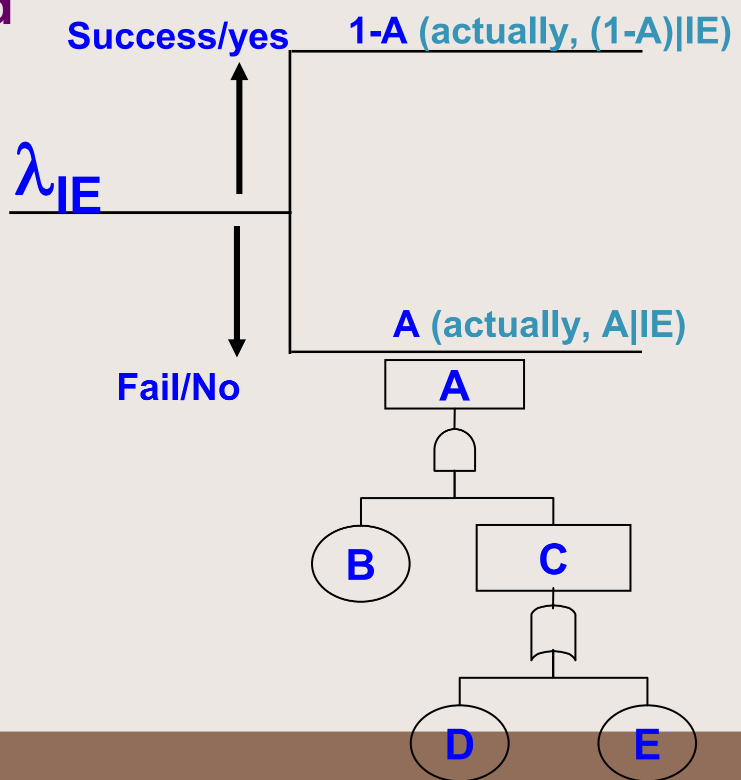
Event Tree Methodology

Event Trees

- Use inductive logic to postulate and quantify accident scenarios or accident sequences
- Start with initiating event and follow through scenario to identify possible scenarios which need to be managed
- Event trees should be used to display the progression of an accident
- A typical event tree in a nuclear power plant risk analysis may generate millions of accident sequences

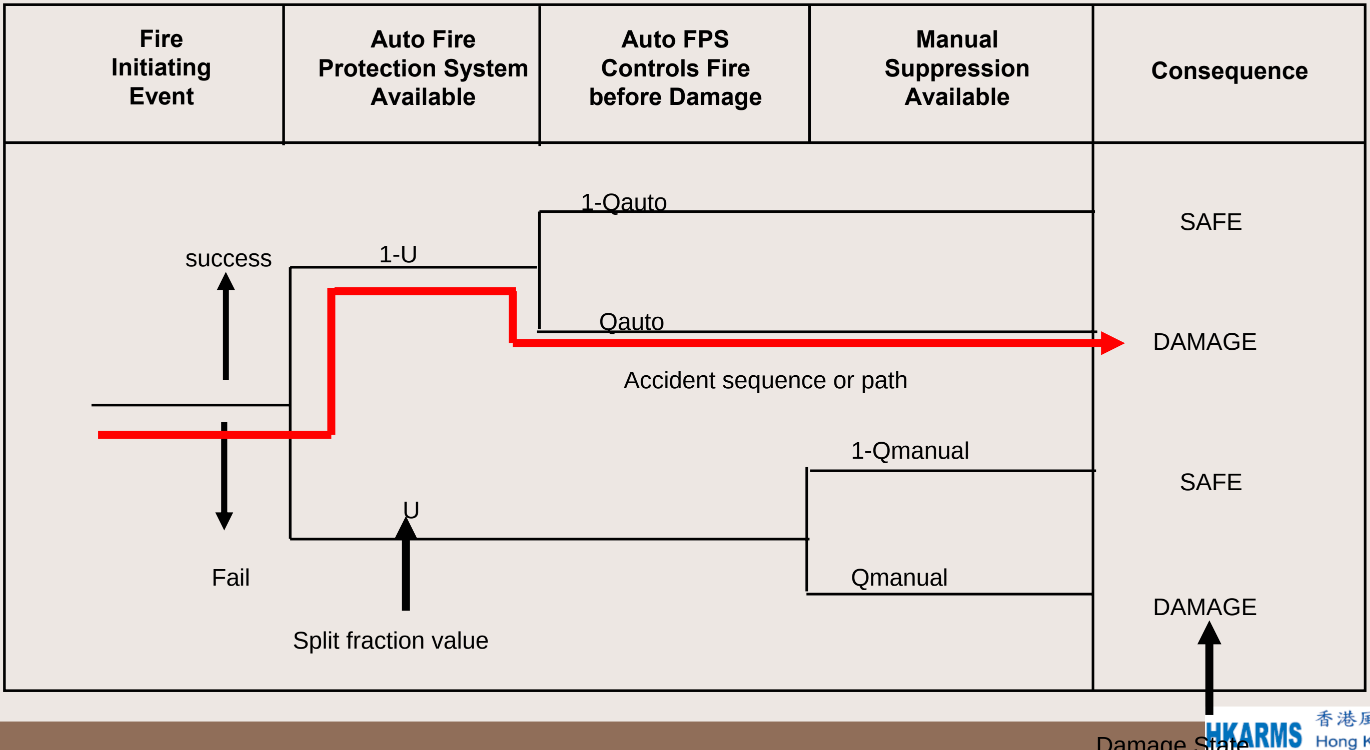
Event Tree Analysis

- Use inductive logic to postulate and quantify accident scenarios or accident sequences
- Start with initiating event and follow through scenario to identify possible scenarios which need to be managed



Event Tree Analysis

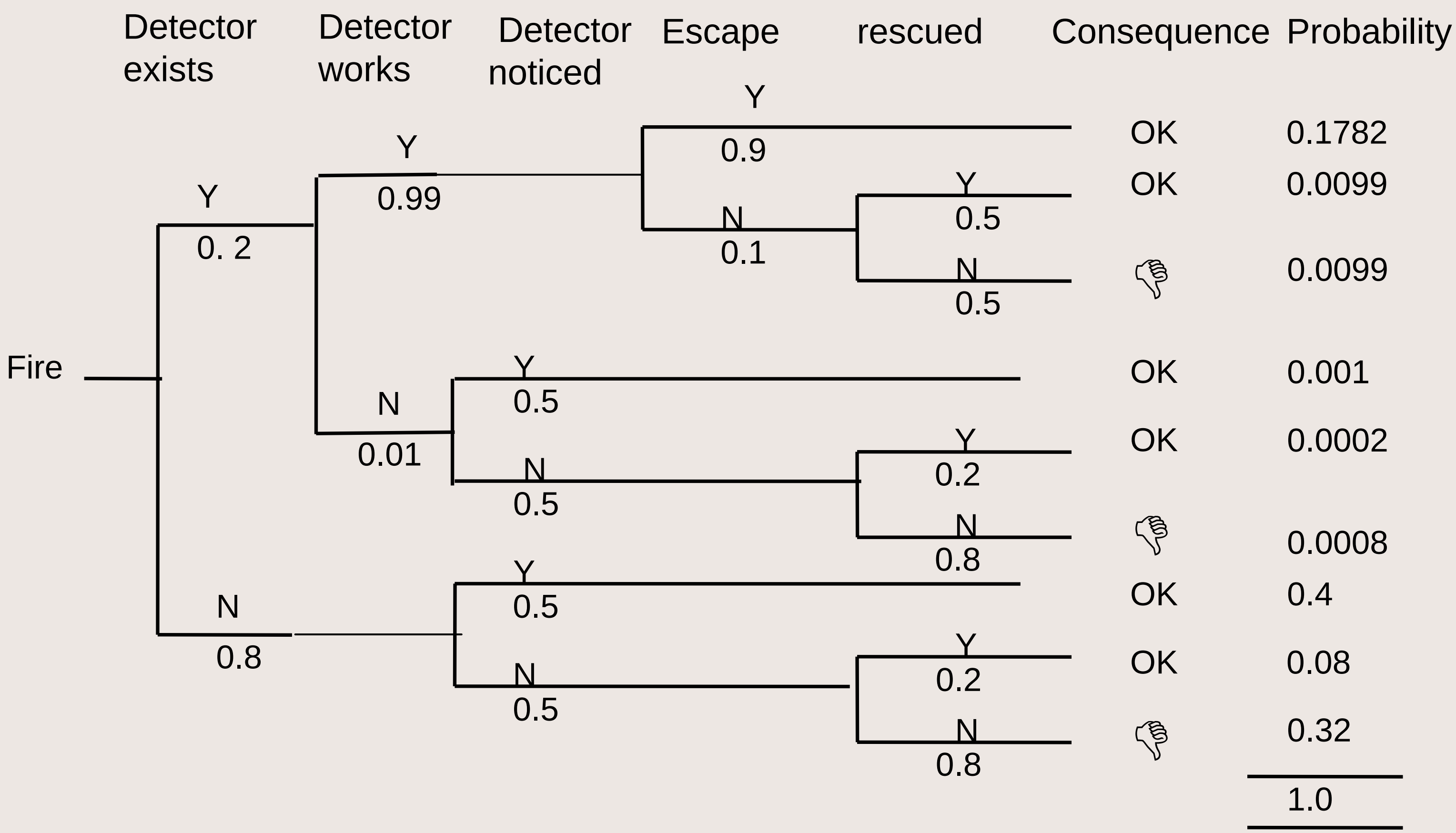
- Each event tree heading may have more than 2 branches, although binary tree is most common
- Event trees should start with an initiating event, not a damage state. Most people confuse event tree with decision tree



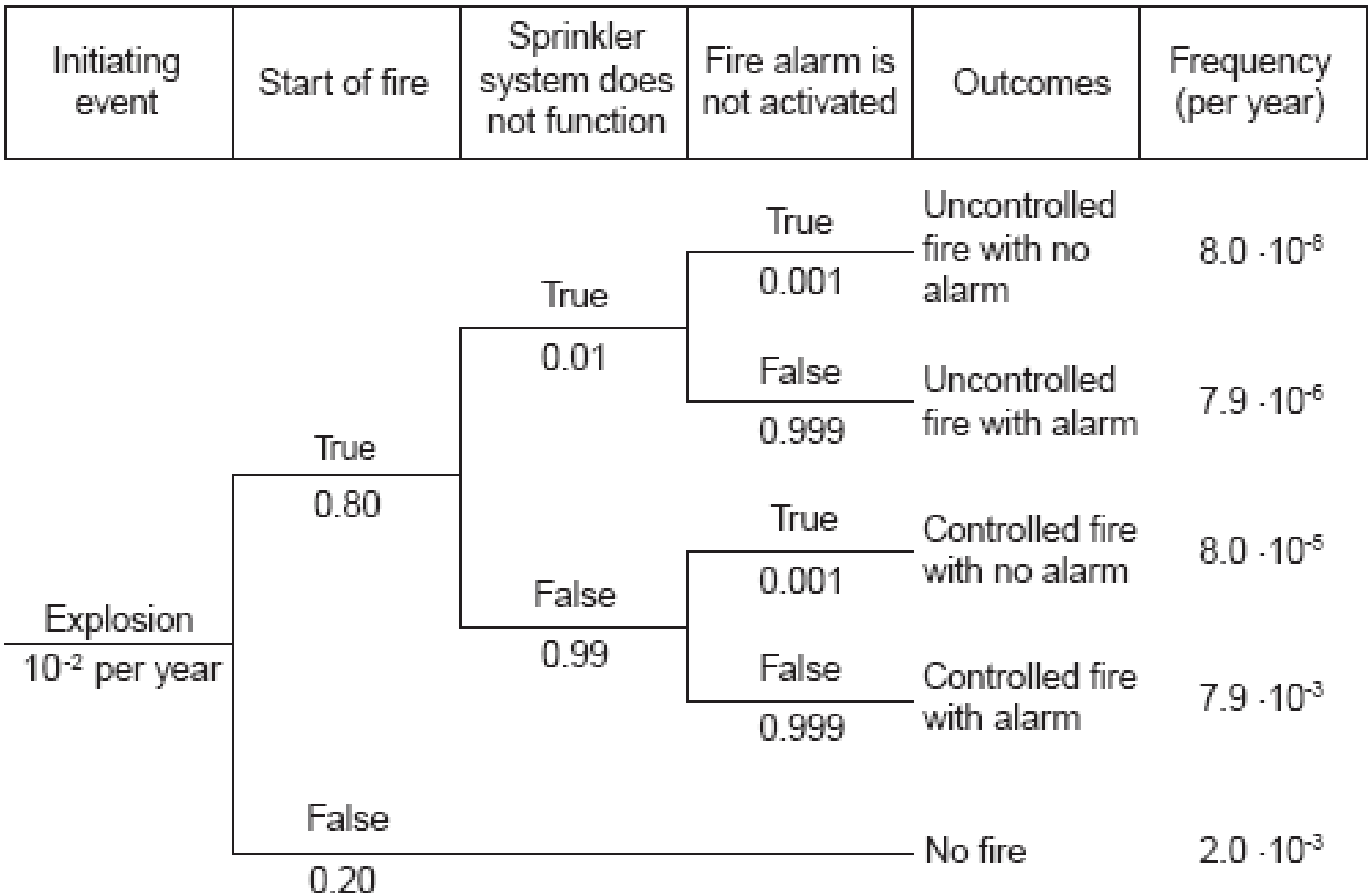
Event Tree

- Event headings are usually state o system, function of safety barriers, actions or events that can alter the course of the accident scenario
- Easier if you put key actions first
- Event tree and fault tree are inter-changeable in most cases

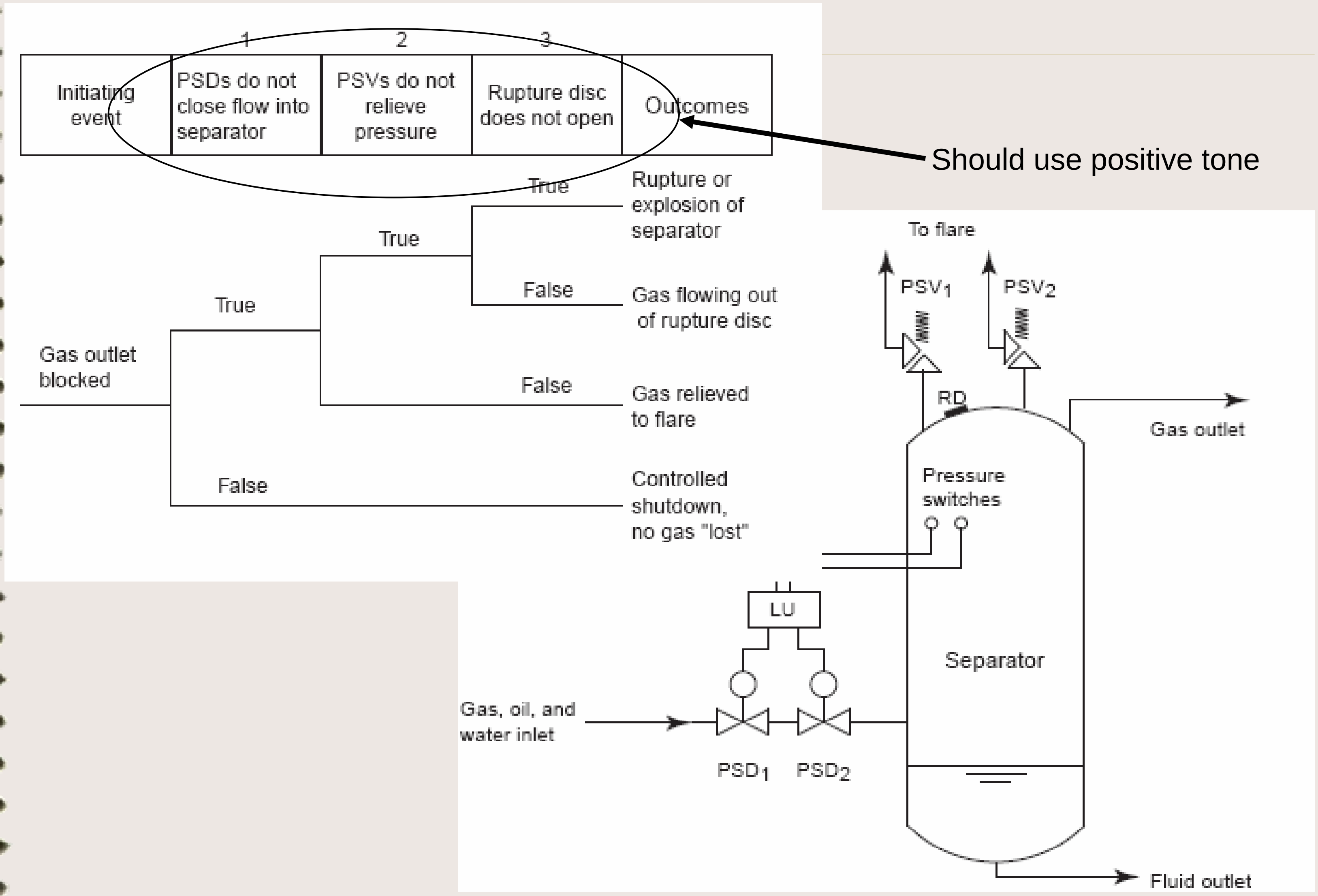
Example – Building with Fire Detector



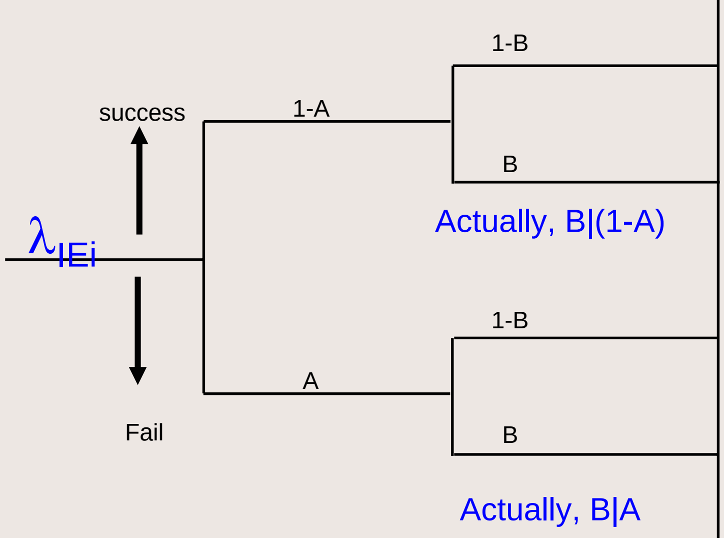
Another example



Pressure Tank



Event Tree Analysis



Initiating Event	Safety System A Available	Safety System B Available	Consequence	Path Conditional Probability	Path Frequency	Path Risk
			q_1	$p_1=(1-A)(1-B)$	$\lambda_1= \lambda_{IE}p_1$	$R_1= \lambda_1 q_1$
			q_2	$p_2=(1-A)B$	$\lambda_2= \lambda_{IE}p_2$	$R_2= \lambda_2 q_2$
			q_3	$p_3=A(1-B)$	$\lambda_3= \lambda_{IE}p_3$	$R_3= \lambda_3 q_3$
			q_4	$p_4=AB$ $\Sigma=1$	$\lambda_4= \lambda_{IE}p_4$	$R_4= \lambda_4 q_4$

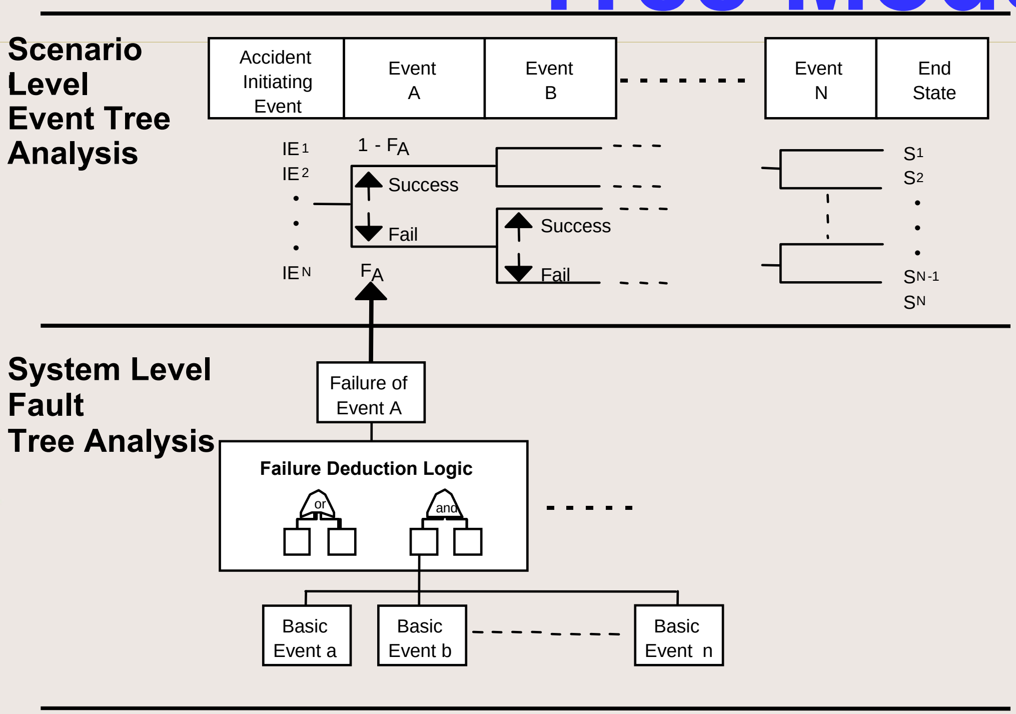
Given: λ_{IEi} = 2.3/yr; A=0.4, B=0.1, q_4= 24 fatalities

P_4= 0.4*0.1 = 0.04; $\lambda_4= \lambda_{IE} P_4$ = 2.3*0.04/yr = 0.092/yr;

R_4=0.092*24 = 2.2 fatalities/yr

Total Risk (given IE_i) = $\lambda_{IEi} \Sigma R_{i|IEi}$; **Total System Risk = $\Sigma_j (\lambda_{IEj} \Sigma_i R_i)$**

Integrated Event Tree/Fault Tree Model



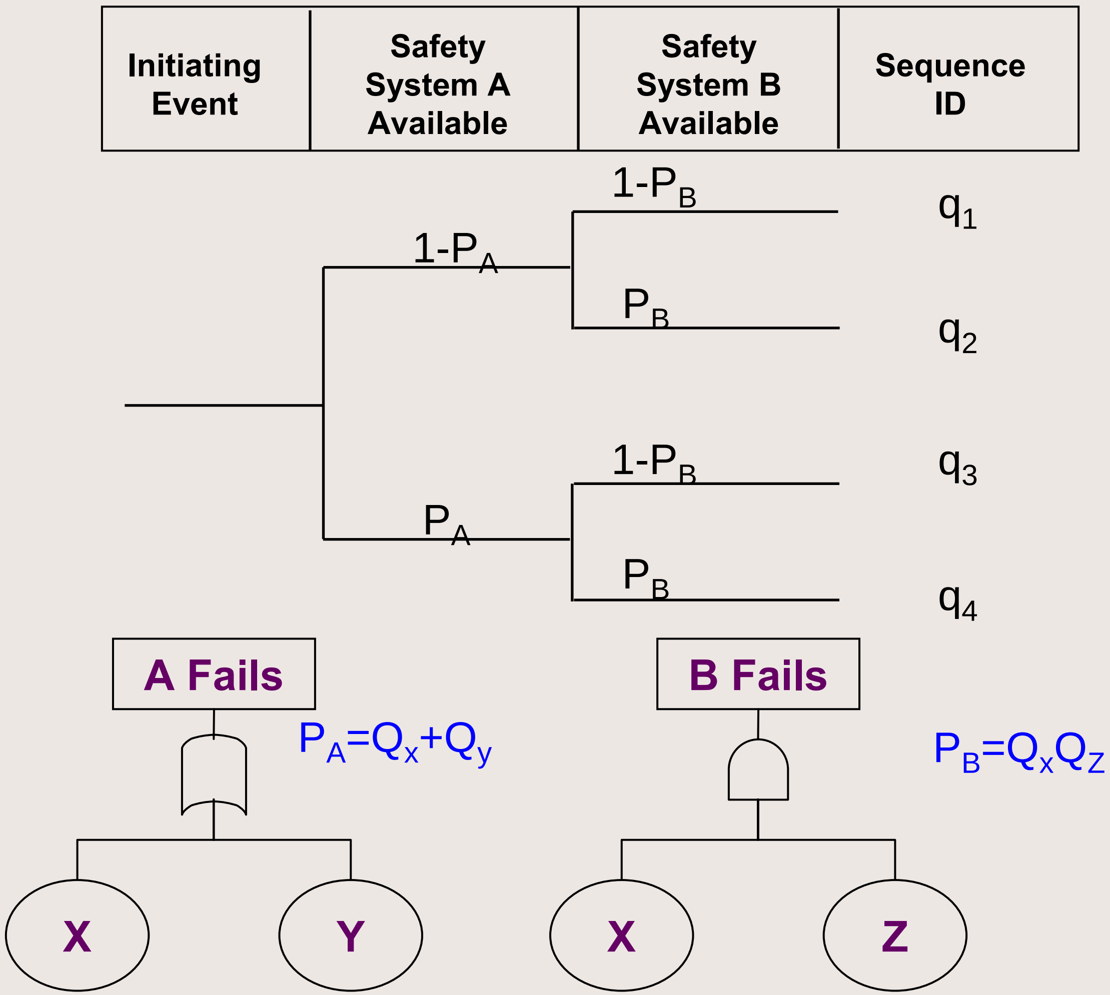
- **Event Trees were used to postulate accident sequences and quantify the Frequency of each sequence**
- **$F_{S|IEi}$ are conditional probabilities quantified by fault tree analysis or engineering calculations**

- **The likelihood of an accident sequence, *Freq(S_i)*, with a defined End State S_i, is**

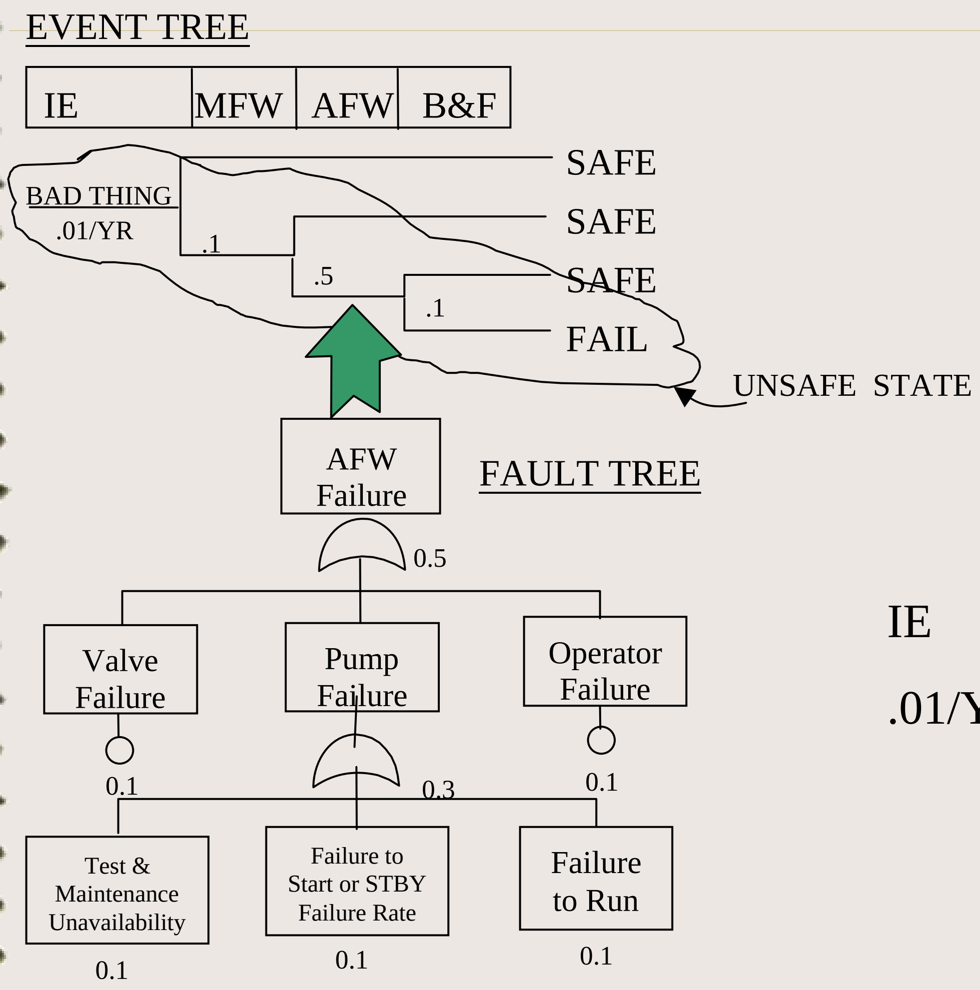
$$Freq(S_i) = \lambda_{IEi} \prod F_{S|IEi} Q_i$$

- **The Consequence is assessed by the consideration of the failure scenario. May not be as simple as Safe/Unsafe. Can be many states of failure**

Event Tree Analysis



Example



Fail Path Frequency

IE MFW AFW B&F

.01/YR X .1 X .5 X .1 = $5X10^{-5}$/YR

Decision Analysis

Decision Alternatives

- **Options to choose based on chosen decision criteria**
- **Alternatives can be either independent or mutually exclusive**
- **In addition to list of generated alternatives, there is the** do nothing **alternative (status quo)**

Economic Issues to be Answered before Deciding on an Alternative

- How much does the option cost
- How much will the option save
- How do we get the money to pay for it
- What are the tax effects
- What is the criteria to be used to decide on the option
- What are the assumptions used in the estimates
- How dependent is a decision on the assumptions-sensitivity analysis

Different Decision Alternatives Incur Different Costs

- First Cost (Initial outlay, capital costs)
  - capital costs
  - construction costs
- Interest Rate
- Tax Effects
- Loss of revenue
- life cycle costs
  - Estimated Useful Life
  - Estimated Annual Income or Revenue
  - Estimated Annual Expenses or Costs
  - Salvage Value

Decision-Making Strategies : An Optimization Process

- Select the alternative that gives the best overall value
- Identify criteria (decision attributes) to judge alternatives
- Difficult to solve when model involves qualitative criteria tie with emotion and perception
- Can be expressed in mathematical terms and implemented using computer programs

Decision-Making Strategies

- Visit temple, pray for god
- Muscling, louder voice wins
- Roll dice, flip coin
- Qualitative approach
- Quantitative approach

Decision-Making Strategies: Qualitative Approach

- Satisficing
- Elimination-by-aspects
- Incrementalism
- Mixed scanning
- Political approach
- Others

Decision-Making Strategies: Quantitative Approach

- **Voting, scoring**
- **Multi-Attribute Utility Theory (MAU)**
- **Analytical Hierarchical Process (AHP)**

Qualitative Approach: Satisficing

- Select the first alternative that is good enough with respect to some minimal criteria
- Cutoff level of constraints governs decision
- Apply to time-constrained situations

Qualitative Approach: Elimination-by-Aspects

- Alternatives are examined by a series of aspects (attributes/criteria)
- An aspect is like a constraint involving one or more criteria
- An alternative is eliminated if it cannot meet the requirement of an aspect
- Make judgment by elimination
- Order of aspects can strongly influence results
- An alternative that superior in many aspects may be eliminated

Qualitative Approach: Incrementalism

- Compare alternative courses of action to the current course of action
- Look for alternatives that can overcome shortcomings of the current course of action
- A decision that results in incremental improvement

Qualitative Approach: Mixed Scanning

- Scanning: Collection, processing, evaluating and weighing of information
- Importance of decision determines the degree of scanning and choice
- Each alternative is briefly considered
- Reject alternatives for which strong objections are detected

Qualitative Approach: Political Approaches

- Actions and decisions result from bargaining among players
- To predict decision, find out:
  - who the players are
  - what are the players' interests or stands?
  - what are the players' relative influence?
  - How does the combined dynamics of the above affect the decisions

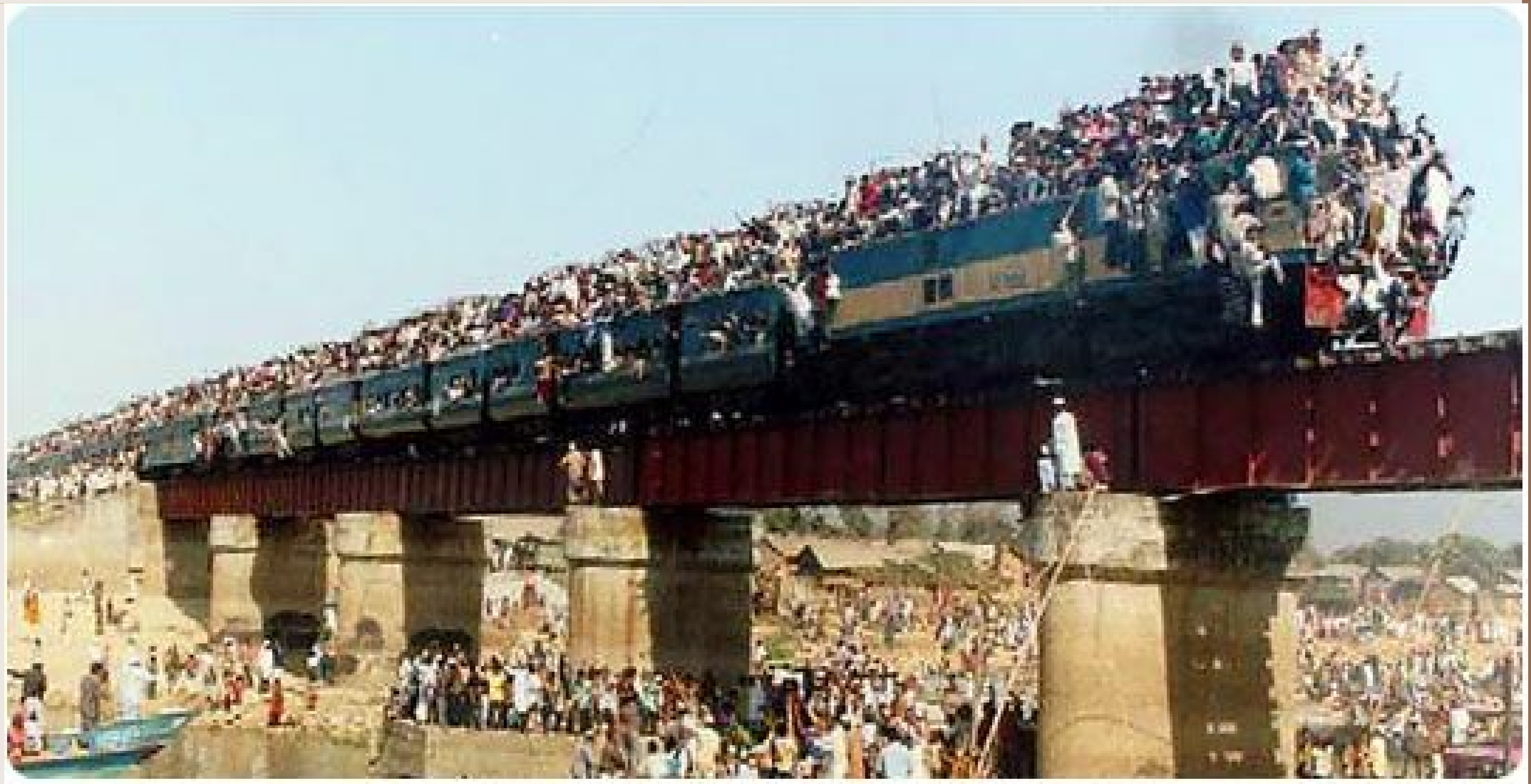
Quantitative Approach: Multiattribute Utility (MAU) Theory

- Assumes a decision alternative can be characterized by a set of independent attributes
- Attribute scales are measured using utility
- Relative values of decision alternatives are measured by aggregating the attribute utilities
- Benefits of decision alternatives are measured by improvement of relative values attributable to their implementation.

Quantitative Approach: Analytic Hierarchy Process

- Decomposes the overall decision objective into a hierarchic structure of criteria, sub-criteria, and alternatives
- Pair-wise comparison matrix for criteria, sub-criteria and alternatives
- Matrices are mathematically processed to calculate relative weights of criteria and sub criteria
- Relative weights are used to arrive at a score for each alternative

If there is no risk…



there is no opportunity.

The presentation material will be posted on www.hkarms.org

Under HKARMS Web Resources

END

For enquires, please contact Vincent Ho

vsho@hkarms.org