SKM 4353 Safety in Petroleum Engineering
Chapter 4 – Risk Assessment

Name : Siti Norfaizah Razali, Mohd Zaidi Jaafar

Email: sfaizah@petroleum.utm.my, mzaidij@petroleum.utm.my

Overview

- Risk is defined as the likelihood of an adverse outcome.
- It is a combination of probability of occurrence and severity of the effect on events considered.
- These are then incorporated to formulate some index that will indicate the extent of risk involved.

Risk = Severity x Likelihood

Severity

- Severity is the extent of damage incurred following the accident.
- It can be in the form of fatality, injury, material loss or environmental degradation.
- To estimate the severity on an incident, detailed mathematical models are often used. Many softwares are available in the market to facilitate the effort.
- Severity is expressed as probability of fatality (0 to 1), or RM XXX Million of Losses incurred or some other measures depending on the nature of the assessment.

Likelihood

- Likelihood is the chance of an event to occur.
- It is estimated based on historical data on failure frequency of individual units or components. For example, there are failure data available for gasket failure, pipe rupture, pump switch failure etc. These data have been surveyed and collected over the years and published.
- Two methods are typically used to compute the overall likelihood of an event, these are:
    1. Fault-Tree Analysis (FTA)
    2. Event-Tree Analysis (ETA)
- Likelihood is expressed in terms of frequency of occurrence (per year)

Risk

- Risk is therefore expressed as Fatality per year, or RMXXX Million lost per year etc.

- There are several classes of risk assessments currently employed in the world.

- Some of them have been incorporated within safety legislation in Malaysia;
  1. Quantitative Risk Assessment (QRA)
  2. Chemical Health Risk Assessment (CHRA)
  3. Hazard Identification, Risk Assessment and Risk Control (HIRARC) .

Application of Risk assessment

- Prioritise safety action programme
- Rank and prioritise safety audit findings
- Evaluate benefit of accident prevention measures
- Prioritise expenditure
- Relative ranking of various types of risks

Types of Risk Assessment

Quantitative	Qualitative
Scientific studies and measurements	Semi-scientific or non-scientific
Comparison of results with limit values	Jugdement Decisions; • Proffesional and personal experiences/biases • Code of practices
Occupational hygiene, Noise, Structural design, Ergonomic etc.	

Methods of safety analysis

- Qualitative
  - Checklist
  - What if
  - HAZOP
  - Preliminary Hazard Analysis (PHA)

- Quantitative
  - Event Tree
  - Fault Tree
  - Failure Mode & Effects Analysis (FMEA)

Qualitative Risk Assessment (1)

- 'Decide' on risk level using judgement, experience and technical knowledge
  - Low or medium
  - High or very high
- Extremely subjective
- Personal and individual variations
- May not be 'bought in to' by any medium to large scale organisation

Qualitative Risk Assessment (2)

- Use numerical model to assess risk
- Probability and consequence models
- Judgement, technical knowledge and experience required
- Subjectivity remains
- A good model reduces personal and individual biases/variations
- Could be ‘bought in to’ by any medium to large scale company

Example - consequences

Four types of risk consequences generally used in the assessment;

1. Economic
2. Personnel
3. Public and Reaction
4. Environment

Risk consequences #1: Economic

- Category I: < 1k
- Category II: < 10k
- Category III: < 100k
- Category IV: < 1m
- Category V: > 1m
- Category VI: Total loss

Risk consequences #2: Personnel

- Category I: Insignificant
- Category II: Minor
- Category III: Major
- Category IV: Severe
- Category V: Fatality
- Category VI: Multiple fatalities

Effects on Personnel

- Insignificant: no human injury expected or < 3 days lost time
- Minor: Injury/illness, 3 – 28 or 56 days lost time, full recovery expected
- Major: Injury/illness, 28+ or 56+ days lost time, or permanent slight incapacity
- Severe: Permanent incapacitating injury/illness

Risk consequences #3: Public and Reaction

- Category I: Nuisance (Mild reaction)
- Category II: Complaints (Minor local outcry)
- Category III: GP attendances Complaints
- Category IV: Hospitalization and Local Media attention
- Category V: Serious injury or Local Media attention
- Category VI: Fatality or Government and Media attention

Risk consequences #4: Environment

- Category I: Insignificant
- Category II: Temporary short term damage
- Category III: Major Pollution
- Category IV: Severe Pollution
- Category V: Widespread damage
- Category VI: Catastrophic damage

Probability (Frequency) Ratings/Experiences

- 1 in 10 (Frequent)
- 1 in 100 (Probable)
- 1 in 1000 (Occasional)
- 1 in 10,000 (Remote)
- 1 in 100,000 (Improbable)
- 1 in 1,000,000 (Extremely Remote)

Probability (Frequency) Ratings/Experiences

- 1 in 10 (Frequent)
- 1 in 100 (Probable)
- 1 in 1000 (Occasional)
- 1 in 10,000 (Remote)
- 1 in 100,000 (Improbable)
- 1 in 1,000,000 (Extremely Remote)

Exposure to hazard

Estimated in time (% 24 hr day)

- < 1% (very rare)
- 1% (rare)
- 25%
- 50%
- 75%
- 100% (continuous)

What if analysis

- Communication and evaluation exercise
- The objective is the same as HAZOP; to assure that catastrophic incidents will be avoided during lifetime of the facility
- Usually combined with *Checklist* to provide a roadmap
- Brainstorm a safety review which ask “What-if” questions of the process

What-if limitations

- It is based on experience
  - cannot be relied upon for identifying unrecognized hazards
  - a review team may fail to delve deep enough if they became superficially familiar with the process
- It is not systematic
  - personnel familiar with the facility discuss aspects in random fashion

What-if advantages

- Can be accomplished with a relatively low skill level
- Fast to implement
- Can analyze a combination of failures
- Flexible

Comparison of HAZOP and What-if methods

	HAZOP	What-if
Experience Based	No	Yes
Systematic	Yes	partially
Skill	Moderate	Low
Speed	Slow	Fast
Cost	Moderate	Moderate – Low
Flexible	Yes	Yes

Suggested application

	Checklist	What-if	HAZOP
Wellhead	X		
Pipeline	X		
Production Test Facility		X	
Drilling operation		X	
Workover/wireline		X	
Water Injection Facility		X	
Toxic Vapor Treating Facility			X
Gas Injection Facility			X
LPG Processing Plant			X
LNG Processing Plant			X
Refinery Process Unit			X

Sample What-if/Checklist questions

- Piping
  - What if piping leaks?
  - What if piping fractured?
  - What if piping plugs?
  - What if piping corroded internally/externally?
  - What if high pressure flammable/toxic gas leaks into liquid pipeline?
  - What if piping supports fail?
  - What if pressure relief is not provided?

EVENT TREE ANALYSIS (ETA)

Event Tree Analysis (ETA)

- A bottom-up, deductive system safety analytical technique
- Applicable to:
  - physical systems, with or without human operators
  - decision-making/management systems
- Complementary to other techniques, e.g…
  - Fault Tree Analysis
  - Failure Modes and Effects Analysis

ETA approach

- Explores system RESPONSES to initiating "CHALLENGES"
- Enables PROBABILITY ASSESSMENT of SUCCESS/FAILURE

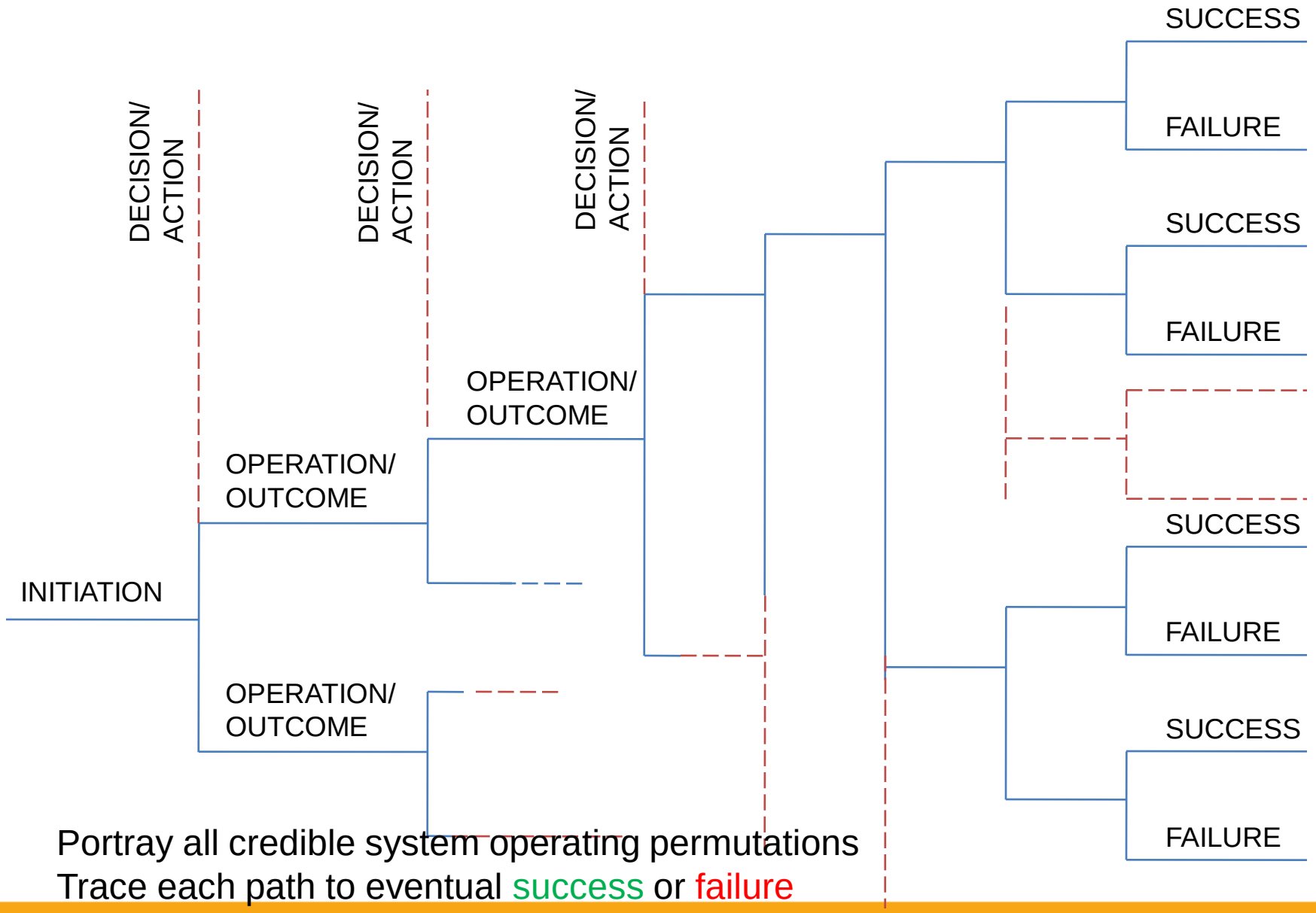
Examples of "CHALLENGES";

- Pipe or vessel Burst
- Ignition of Stored Combustibles
- Utility System Failure
- and…….

Approach

- Based on binary logic
- An event has happened/has not happened
- A component has failed/has not failed
- Begins with initiating event
- The consequences of the event are followed through a series of possible paths
- Each path is assigned a probability of occurrence

ETA (General Case)



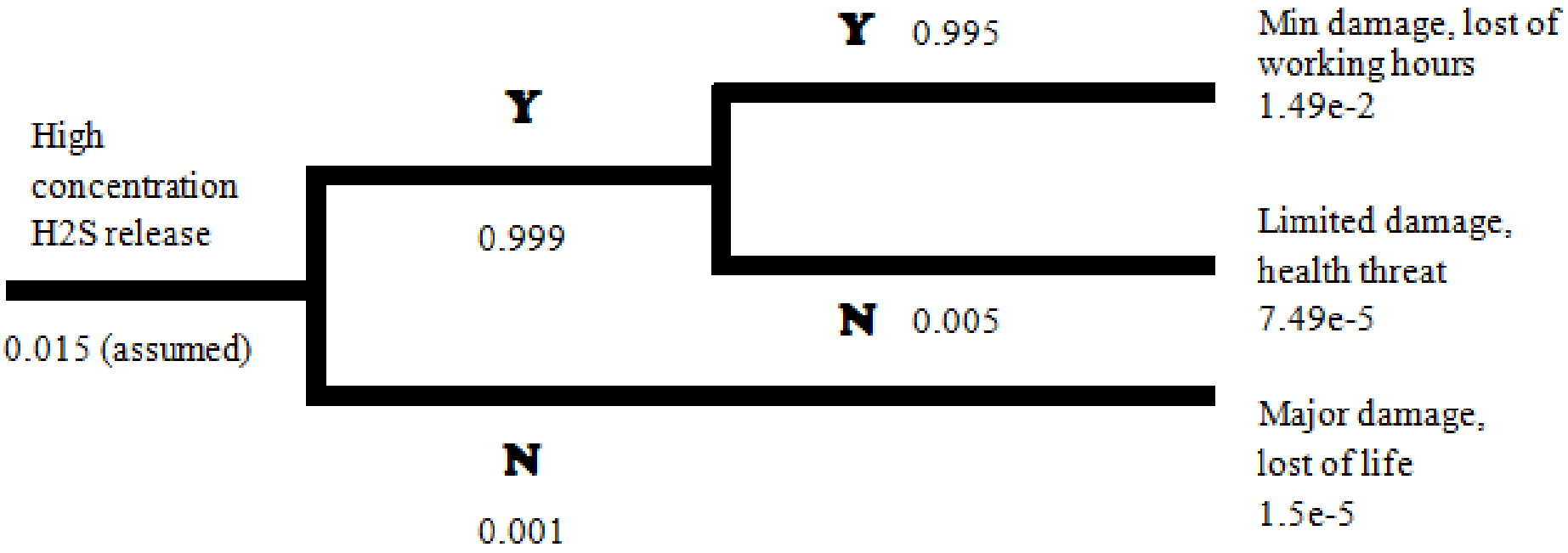
Portray all credible system operating permutations

Trace each path to eventual success or failure

ETA (Bernoulli Model)

- Reduce tree to simplified representation of system behavior.
- Use binary branching
- Lead unrecoverable failures and undefeatable successes directly to final outcomes
- A fault tree of other analysis may be necessary to determine probability of the initiating event or condition. (Unity probability may be assumed)

Initiating event	Alarm system works	Breathing Apparatus works	Consequences



Example of Event Tree Analysis

ASSESS RISK AND JUDGE TOLERABILITY…

- Failure statements express SEVERITY
- Event Tree Analysis explores OUTCOMES/ assesses PROBABILITY
- PROBABILITY and SEVERITY establish RISK

  IS THE RISK ACCEPTABLE?

  If not, develop intervenor(s)

  Select intervenor(s) on the basis of

  - EFFECTIVENESS
  - COST
  - FEASIBILITY (including schedule)

ETA ADVANTAGES

- End events need not be foreseen
- Multiple failures can be analyzed
- Potential Single-Point Failures can be identified
- System weaknesses can be identified
- Zero-payoff system elements/options can be discarded

ETA SHORTCOMINGS

- Operating pathways must be anticipated
- Partial successes/failure are not distinguishable
- Initiating events are treated singly (multiple trees are required for multiple events; co-existing initiating events are not considered)
- Sequence-dependent scenarios are not modeled well

FAULT TREE ANALYSIS (FTA)

Fault Tree Analysis (FTA)

- A graphic "model" of the **pathways** within a system that can lead to a **foreseeable, undesirable loss event**.
- The pathways interconnect contributory events and conditions, using **standard logic symbols**.
- Numerical probabilities of occurrence **can** be entered and propagated through the model to evaluate probability of the foreseeable, undesirable event

FTA Origins

- Was developed in 1962 for the US Air Force by Bell Telephone Laboratories
- Was later adopted and extensively applied by the Boeing Company
- Is one of many symbolic logic analytical techniques found in the operations research discipline

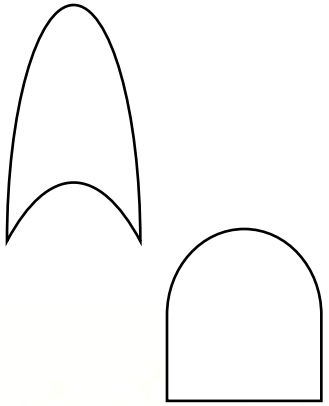
Applications

- Large, perceived threats of loss, i.e. high risk
- Numerous potential contributors to a mishap
- Complex or multi-element systems/processes
- Already-identified undesirable events
- Indiscernible mishap causes

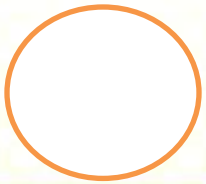
The logic Symbols

- **Top Event**
  - Forseeable, undesirable event toward which all fault tree logic paths flow

- **Intermediate event**
  - Describing a system state



- "**Or" Gate** - Produces output if any input exists
- "**And" Gate** – produces output if all input exist
- **Basic Event** – initiating fault/failure



Hazard Identification Risk Assessment & Risk Control (HIRARC)

Purpose of HIRARC

- to identify all the factors that may cause harm to employees and others (the hazards)
- to consider what the chances are of that harm actually be falling anyone in the circumstances of a particular case and the possible severity that could come from it (the risks)
- to enable employers to plan, introduce and monitor preventive measures to ensure that the risks are adequately controlled at all times

HIRARC should be conducted…

- where hazard appear to pose significant threat
- When uncertain whether existing controls are adequate
- before implementing corrective or preventive measures
- by organization intending to continuously improve OSH Management System

Process of HIRARC

In 4 simple steps;

i. classify work activities
ii. identify hazard
iii. conduct risk assessment (analyze and estimate risk from each hazard), by calculating or estimating
    a) likelihood of occurrence
    b) severity of hazard
iv. decide if risk is tolerable and apply control measures

Classify work activities

in accordance with their similarity;

- geographical or physical areas within/outside premises
- stages in production/service process
- not too big e.g. building a car
- not too small e.g. fixing a nut
- defined task e.g. loading, packing, mixing, fixing the door

Identify hazards

- Health hazards
- Safety hazards
- Environmental hazards

Likelihood

Likelihood (L)	Example	Rating
Most likely	The most likely result of the hazard / event being realized	5
Possible	Has a good chance of occurring and is not unusual	4
Conceivable	Might be occur at sometime in future	3
Remote	Has not been known to occur after many years	2
Inconceivable	Is practically impossible and has never occurred	1

Severity of hazards

Severity (S)	Example	Rating
Catastrophic	Numerous fatalities, irrecoverable property damage and productivity	5
Fatal	Approximately one single fatality major property damage if hazard is realized	4
Serious	Non-fatal injury, permanent disability	3
Minor	Disabling but not permanent injury	2
Negligible	Minor abrasions, bruises, cuts, first aid type injury	1

HIRARC Table

Hazard Identification					Risk Analysis			Risk Control
No	**Work Activity**	**Hazard**	**Cause/Effect**	**Existing Risk Control**	**Likelihood**	**Severity**	**Risk rating**	**Recommended control measures**
1								
2								
3								
4								

Example of Risk Matrix

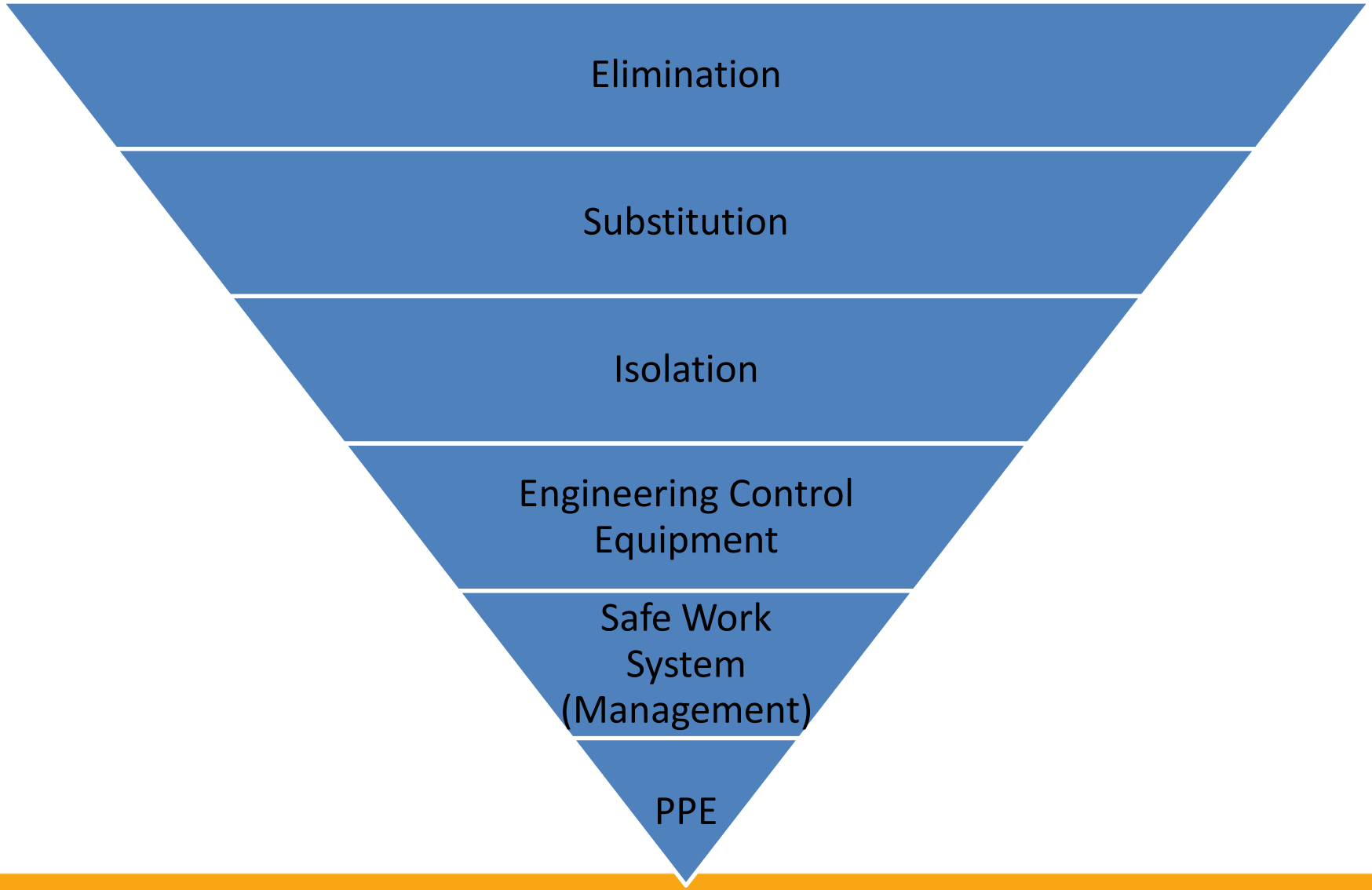
	Severity					
Likelihood		1	2	3	4	5
	1	1	2	3	4	5
	2	2	4	6	8	10
	3	3	6	9	12	15
	4	4	8	12	16	20
	5	5	10	15	20	25

Risk Matrix conclusion

RISK	DESCRIPTION	ACTION
15 - 25	HIGH	A HIGH risk requires **immediate** action to control the hazard as detailed in the hierarchy of control. Actions taken must be documented on the risk assessment form including date for completion.
5 - 12	MEDIUM	A MEDIUM risk requires a planned approach to controlling the hazard and applies temporary measure if required. Actions taken must be documented on the risk assessment form including date for completion.
1 - 4	LOW	A risk identified as LOW may be considered as acceptable and further reduction may not be necessary. However, if the risk can be resolved quickly and efficiently, control measures should be implemented and recorded.

Source: HIRARC Guidelines by DOSH Malaysia

Hierarchy of Risk Control



References

- Guidelines for Hazard Identification, Risk Assessment and Risk Control, DOSH Malaysia, 2008.
- P.L. Clemens and J. Sverdrup, *Event Tree Analysis*, 2nd Edition, June 1990.
- Siti Norfaizah Razali, UTM Final Year Examination Paper – SKM 4353, Skudai, 2012.
- Wikipedia – *Fault Tree Analysis and Event Tree Analysis*, retrieved in 2012.