Hazard Identification

Most important stage of Risk Assessment Process

35+ Techniques

Quantitative / Qualitative

- **Failure Modes and Effects Analysis FMEA**
- **Energy Analysis**
- **Hazard and Operability Studies HAZOP**
- **Fault Tree Analysis FTA**
- **Event Tree Analysis ETA**

All based around Systems – Collection of inter-related elements

Elements include;
- **People**
- **Machines**
- **Tasks**
- **Environment**

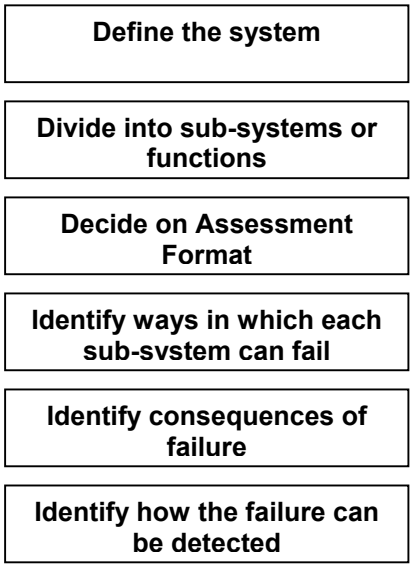
Systems – Sub-systems

Failure Modes and Effects Analysis FMEA

Systematic study of causes of failure and effects on the system

Mainly used for technical systems

Qualitative – identifies design areas needing improvement



Assessment Format – Usually Tabular

- **Identification of component and parent system**
- **Failure mode and cause of failure**
- **Effect of the failure on the subsystem or system**
- **Method of detection and diagnostic aids available**

Typical Format

Component	Function	Failure Mode	Failure Rate	Failure Effect	Criticality	Detection Method	Preventative Measures

Identify every way in which each sub system can fail

Typical failure modes include

- **Failure to open/close**
- **Failure to stop/start**
- **Failure to continue operation**
- **Degradation**
- **Scheduled service**
- **Scheduled replacement**

***Failure rates often included* – quantitative or qualitative (e.g. probable, frequent)**

***Identify consequences of failure* – include effects on other components**

Identify how failures can be detected

- **Alarms**
- **Sensors**
- **Inspection**
- **Maintenance**

Record preventative measures

- **Correct the failure**
- **Reduce failure rate**
- **Provide adequate detection**

Failure Modes, Effects and Criticality Analysis FMECA

Includes ranking failure and effects by severity

Produce a Critical Items List (CIL)

Modify system to address CIL

Advantages

- **Simple to carry out**
- **No mathematics**
- **Easy to interpret**

Disadvantages

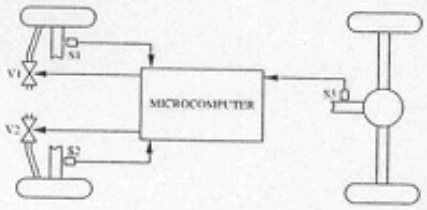
- **Only assess one failure at a time**
- **Fails to address complex interactions**
- **Can be time consuming**

ABS – Anti-lock Braking System

System objectives – prevent locking of front wheels under heavy braking for rear-wheel drive car.

System

- **Sensors S1, S2 measure speed of two front wheels**
- **Sensor S3 measures speed of drive shaft (rear wheels)**
- **Signals sent to microcomputer MC**
- **MC actuates valves V1 and/or V2 if speed of wheel(s) drops below speed of rear wheels**

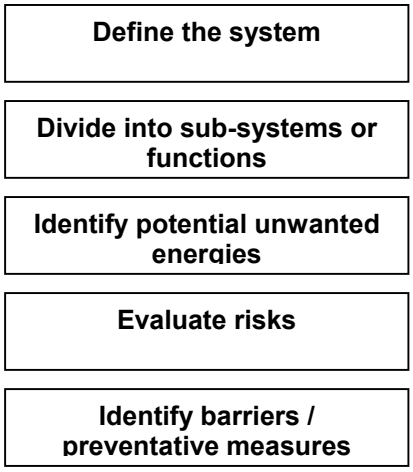


Passenger car anti-skid braking system FMEA

Component	Failure mode	Failure effect(s)	Comment
Front wheel sensor, S1 or S2	No output signal	Micro-computer will assume one wheel has stopped, and send a signal to open the relief valve on that wheel. Partial loss of front wheel braking.	Uneven braking on front wheels. Alarm system required — switch off micro-computer?
Front wheel valve, V1 or V2	Fail to open	One front wheel could lock on heavy braking	Unrevealed failure mode. Test facility required?
	Fail to close	Partial loss of front wheel braking	Uneven braking on front wheels. Isolation/stop valve required?
Rear wheel sensor, S3	No output signal	Micro-computer will have no reference speed from rear wheels, and hence will not attempt to open V1 and/or V2. Both front wheels could lock on heavy braking.	Alarm system required
Micro-computer, MC	No output signals to either front wheel valve	Both front wheels could lock on heavy braking	Alarm system required?
	No output signal to one front wheel valve	One front wheel could lock on heavy braking	Alarm system required?
	Spurious output to both front wheel valves	Total loss of front wheel braking	Alarm system required — switch off micro-computer?
	Spurious output to one front wheel valve	Partial loss of front wheel braking	Alarm system required — switch off micro-computer?

Energy Analysis (Energy Barrier Analysis)

Based on view that accidents are caused by abnormal or unexpected transfer of energy.



Define the system
What is to be assessed, what limits and what assumptions

***Define the sub-systems* – analyse one at a time**

Identify potential unwanted energies (PUE)
- **Electrical**
- **Kinetic (linear/rotational)**
- **Potential**
- **Explosive**
- **Chemical**
- **Stored pressure**
- **Thermal**
- **Radiation**

Typically use a checklist

Potential Energy	*Kinetic Energy – Linear*	*Kinetic Energy - Rotational*
Falls – same level	Human: strike against, lifting, handling	Machine components
Falls – different level	Vehicles	Nipping, crushing
	Projectiles, moving parts	Cutting, tearing

Evaluate risks
Probability and consequences

Identify barriers and preventative measures

- **Eliminate the energy**
- **Control or reduce the energy**
- **Separate the human from the flow of energy**

Advantages

- **In simple systems energy sources and barriers are easy to identify**

Disadvantages

- **Complex systems are difficult to analyse**

Hazard & Operability Studies (HAZOP)

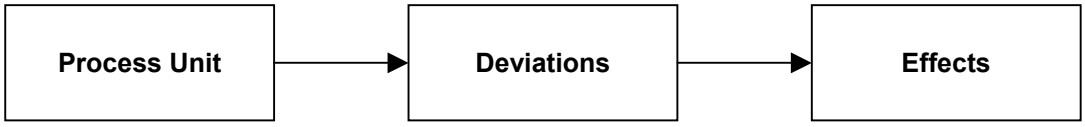
Introduced by ICI for review of chemical process design – extended into other processes

Assumes system is safe when all operating parameters are at acceptable levels.

Systematically search for hazards – deviations from norm with dangerous consequences.

Typical parameters studied include
- **Temperature**
- **Pressure**
- **Flow**

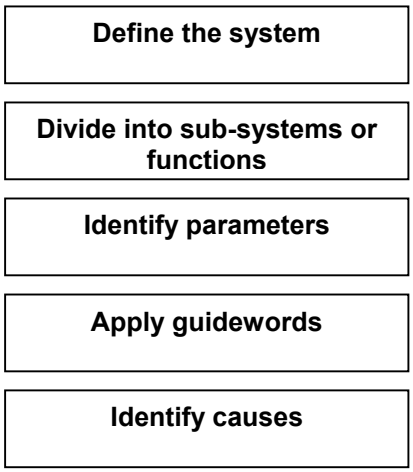
What are possible deviations? **What are the effects? Which effects are hazardous?**



Which contributors lead to deviations? **Which contributors are necessary For hazardous effects?**

HAZOP is a team approach – varied backgrounds

Produces extensive documentation



Define the system
What is to be assessed, what limits and what assumptions

***Define the sub-systems* – analyse one at a time - e.g.**
- **Tanks**
- **Pumps**
- **Connecting pipes**

Identify parameters
For each sub-system each parameter (e.g. flow, temp, pressure, viscosity) that has an influence is noted.

Apply Guidewords
- **To each parameter in each sub-system**
- **Common language – simplifies discussion within the team**
- **Helps to identify consequences**

Examples

Guideword	*Definitions*
NO or NOT	**No part of the design intent occurs, such as no flow in a pipeline due to blockage**
MORE or LESS	**A quantitative increase or decrease of some parameter such as flow or temperature**
PART OF	**Only part of the design intention is fulfilled**
REVERSE	**The logical opposite of the design intention occurs**
OTHER THAN	**Something completely different than intended occurs**

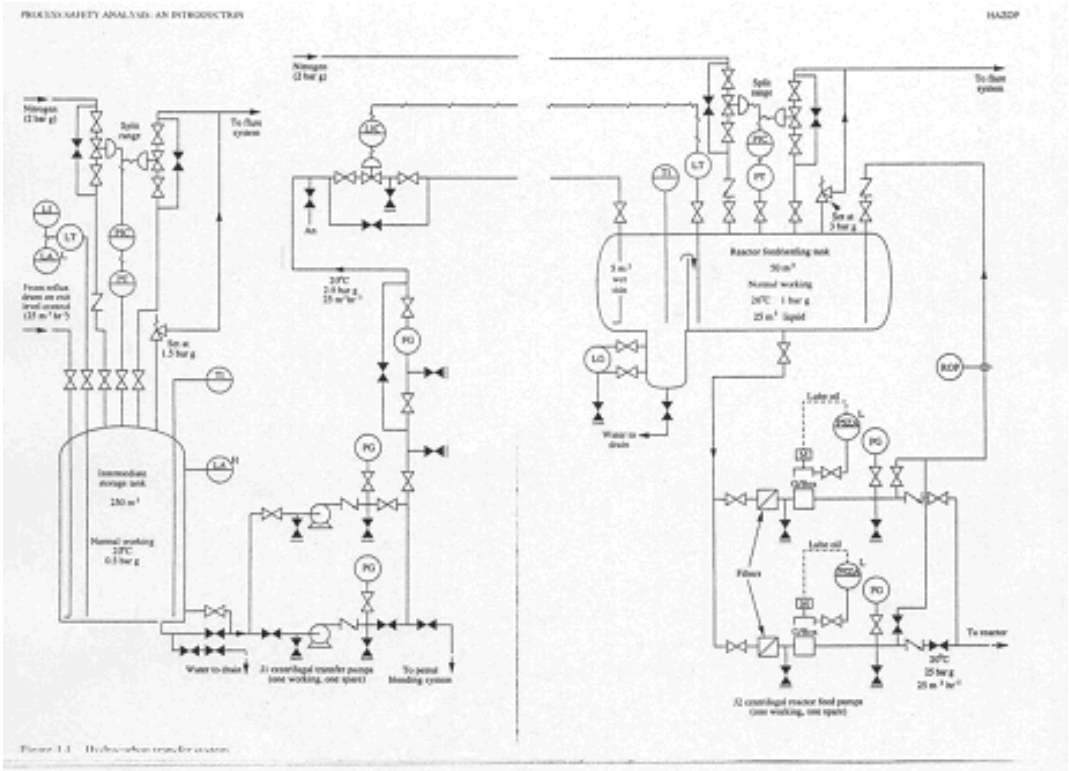
Identify causes
For each significant deviation, possible causes are identified e.g.
- **Human error**
- **Component failure**
- **External influences**

Advantages

- **Uses a team approach – pooled expertise**
- **Applicable to major hazards in process industries**
- **Systematic**

Disadvantages

- **Time and resource consuming**



HAZARD AND OPERABILITY STUDY OF PROPOSED HYDROCARBON TRANSFER SYSTEM:
Results of line section from intermediate storage to buffer/settling tank

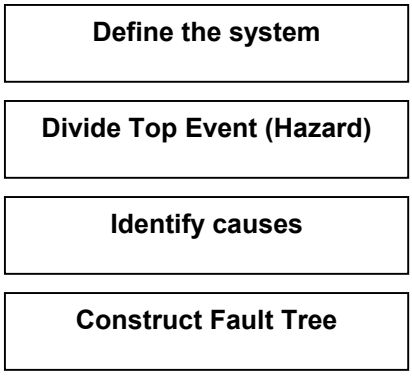
Guide word	Deviation	Possible causes		Consequences	Action required
NONE	NO FLOW	(1) No hydrocarbon available at intermediate storage		Loss of feed to reaction section and reduced output. Polymer formed in heat exchanger under no flow conditions. Buffer tank level falls.	(a) Ensure good communications with intermediate storage operator (b) Install low level alarm on settling tank LIC
		(2) J1 pump fails (motor fault, loss of drive, impeller corroded, etc), power failure		As for (1)	Covered by (b) Add pump running indicator lights (also in control room)
		(3) Line blockage, LCV fails shut		As for (1) J1 pump overheats Rising level in storage tank?	Covered by (b) (c) Install kickback on J1 pumps
		(4) Line fracture		As for (1) Hydrocarbon discharged into area adjacent to public highway	Covered by (b). Consider adding second FQ at buffer tank inlet. (d) Institute regular patrolling and inspection of transfer line.
		(5) Valve closure in error		As for (1)	(e) Review operator reliability and provision for J2 pump protection
REVERSE	REVERSE FLOW	(6) Failure of PIC and higher-than-normal N_2 pressure		N_2 gas breakthrough	(f) Add anti-siphon provision in buffer tank dip-pipe
		(7) Failure or leakage of NRV		N_2 passed to intermediate storage	(g) Check capacity of intermediate storage relief system. Review maintenance programme.
		(8) Backflow through standby pump of standby pump		Reduced delivery to buffer tank	(h) Check operating instructions for isolation
MORE OF	MORE FLOW	(9) LCV fails open or LCV bypass open in error or both pumps operating		Settling tank overfills Incomplete separation of water phase in tank leading to routine problems	(i) Install high level alarm on LIC and check sizing of relief opposite liquid overfilling. Consider high-high level trip with auto re-set. (k) Institute locking-off procedure for LCV bypass when not in use (l) Extend J2 pump suction line to 300 mm above tank base

Fault Tree Analysis FTA

Break down an accident hazard into contributing factors

Investigate combinations of events and conditions that lead to the hazard

Used extensively in nuclear, chemical process and offshore industries



Define the system
What is to be assessed, what limits and what assumptions

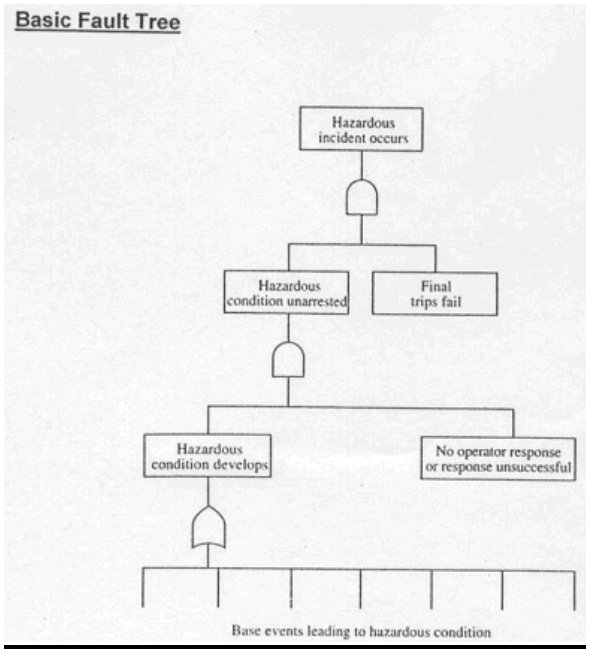
Define Top Event (Hazard)
Well defined and not too broad

Identify Causes
- **Structure tree with hazard at the top and work downwards**
- **Identify causes**
- **Break each cause down into sub-causes or events**
- **Repeat until the basic or 'root' causes are identified**

Construct Tree
- **Use standard symbols**
- **Completed tree shows potential sequences or events that lead to the top event.**

Advantages
- **Simple and logical overview of causes and initiating events**
- **Graphical – easy to follow**
- **Useful in identifying control measures**
- **Concentrates on multiple causes**
- **Easily extendible into QRA**

Disadvantages
- **Trees can grow rapidly**
- **Can be time consuming**
- **Needs experience**



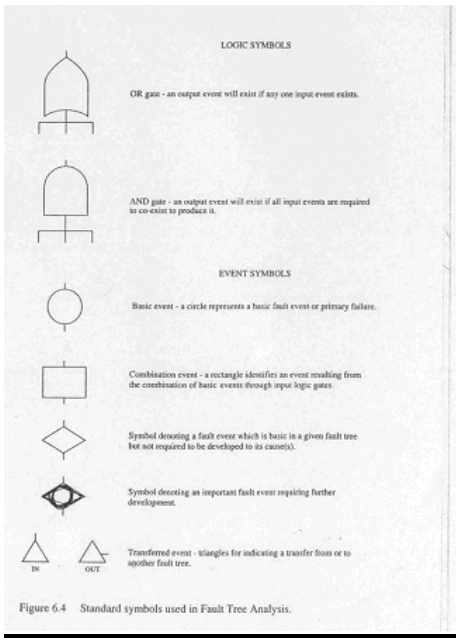


Figure 6.4 Standard symbols used in Fault Tree Analysis.

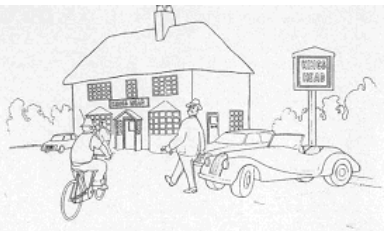


Figure 6.6 Exterior of public house. © AEA Technology plc 1996

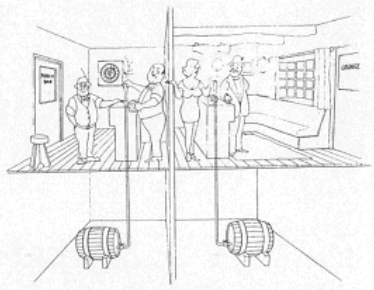
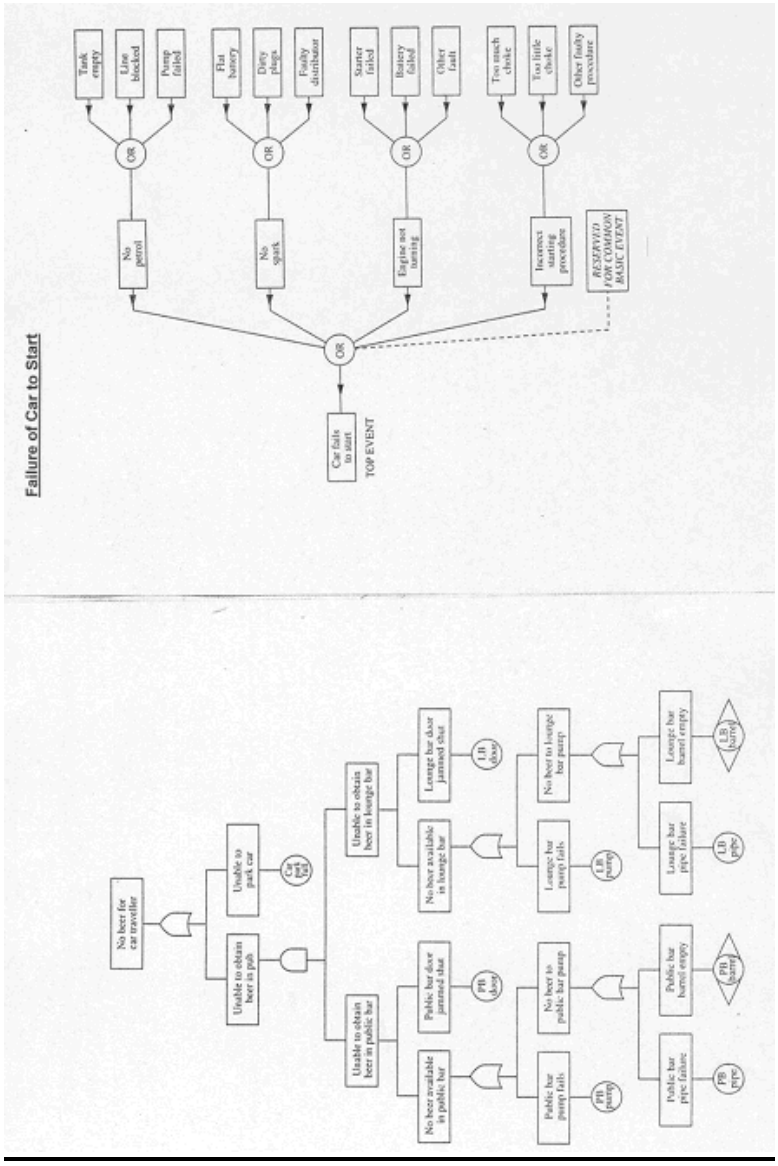


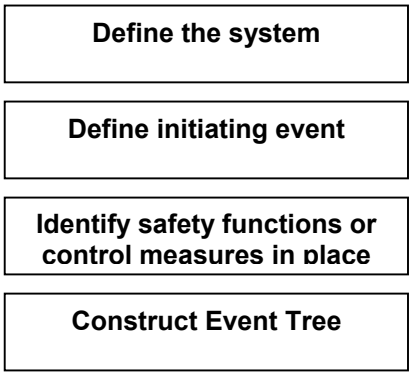
Figure 6.7 Interior of public house. © AEA Technology plc 1996


Failure of Car to Start
Car fails to start
TOP EVENT
OR
No petrol
Tank empty
Line blocked
Pump failed
No spark
Flat battery
Dirty plugs
Faulty distributor
Engine not turning
Starter failed
Battery failed
Other fault
Incorrect starting procedure
Too much choke
Too little choke
Other faulty procedure
RESERVED FOR COMMON BASIC EVENT
No beer for car traveller
Unable to obtain beer in pub
Unable to park car
Car fail
Unable to obtain beer in public bar
Unable to obtain beer in lounge bar
No beer available in public bar
Public bar door jammed shut
PB door
Public bar pump fails
PB pump
Public bar pipe failure
PB pipe
No beer available in lounge bar
Lounge bar door jammed shut
LB door
Lounge bar pump fails
LB pump
Lounge bar pipe failure
LB pipe
No beer to public bar group
Public bar barrel empty
PB barrel
No beer to lounge bar group
Lounge bar barrel empty
LB barrel

Event Tree Analysis ETA

Show how initiating events lead to accidents

Considers safety systems in place



Define the system
What is to be assessed, what limits and what assumptions

Define Initiating Event e.g.
- **Equipment failure**
- **Human error**
- **Process disturbance**

Identify Safety Functions (Control Measures) in Place e.g.
- **Automatic safety systems that respond to the initiating event**
- **Alarms**
- **Procedures and emergency responses that react to alarms etc.**
- **Barriers or containment measures**

Construct Event Tree
- **Initiating event is on the left**
- **Control measures are structured as headings – in sequential order across the top**
- **Failure or success states are defined for each control measure**
- **Work from left to right – examining sequence of events**
- **Rank the sequences in order of danger - Typically the most dangerous sequences are along the top of the tree**

Advantages
- **Forward thinking process – identifies development of accidents**
- **Useful in identifying control measures**
- **Useful in situations with varied outcomes**
- **Can be extended into QRA if data is available**

Disadvantages
- **Trees can grow quickly**
- **Can miss possible branches in the tree**

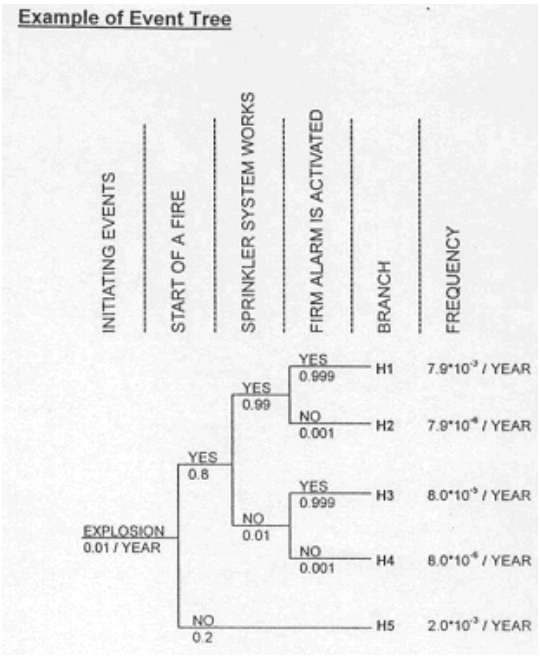


Table 3.9: Comparison of Hazard Identification Methods

IN THE WORK-PLACE CAN BE USED TO ASSESS:	METHOD	DESCRIPTION	IDENTIFIES MAJOR HAZARDS IN RELATION TO:	Special Training Req.	Identifies Hazards	Identifies Causes	Risk Measure
Machines	Failure Modes & Effects Analysis	Identifies failure of components which can lead to hazards.	Technical components or modules.	✓	✓	✓	SUB
Machines, Activities, Part of the workplace	Energy Analysis	Identifies hazardous forms of energy.	Components such as work areas or activities		✓	✓	SUB
N/A	HAZOP	Analysis of deviations in chemical processing plants.	Physical properties	✓	✓	✓	SUB
Specific type of work; Organisational routines.	Deviation Analysis/ Proc. HAZOP	Analysis of deviations in the functioning of equipment, humans & organisations.	Work Activities	✓	✓	✓	SUB
Any Work Hazard	Fault Tree Analysis	Logical representation of the consequences of a specific event.	Relation to top event	✓		✓	QRA
Effectiveness of control measures.	Event Tree Analysis	Logical representation of the consequences of a specific event.	Relation to initial event	✓			QRA
Specific types of work; Organisational routines	Human Reliability Analysis	Identifies possible causes brought about by human error		✓		✓	QRA

Risk Analysis

Numerous ways to express risk

e.g. Level of risk of death in any one year due to a particular activity.

Smoking 30 cigarettes per day	**1 in 200**
Man aged 35-44	**1 in 600**
Motor vehicle accident	**1 in 10,000**
Accident at home	**1 in 12,000**
Accident at work	**1 in 30,000**
Rail accident	**1 in 420,000**
Terrorist bomb (London)	**1 in 5,000,000**
Lightening	**1 in 10,000,000**
Animal venom (mostly wasps)	**1 in 20,000,000**

More useful is Fatal Accident Rate (FAR)

- **Risk of death per unit of activity**
- **Number of deaths in a workforce of 1000 during a working lifetime of 100,000 hours**
- **Death rate per 10^8 hours**

FAR for Industry

Chemical industry	**2**
UK industry (factory work)	**4**
Coal mining	**8**
Deep sea fishing	**40**
Offshore oil and gas	**62**
Steel erectors	**70**

FAR for Other Activities

Terrorist bomb in London area	**0.01**
Staying at home	**4**
Rail travel	**5**
Car travel	**30**
Air travel	**40**
Smoking (average)	**40**
Pedal cycling	**96**
Helicopter travel	**500**
Motor cycling	**660**
Rock climbing	**4000**

Risk v Benefit (ALARP)

Risk should be As Low As Reasonably Practicable

High benefits -> Higher acceptable risks
Low benefits -> Lower acceptable risks

The higher the risk the greater the spending justified to reduce it

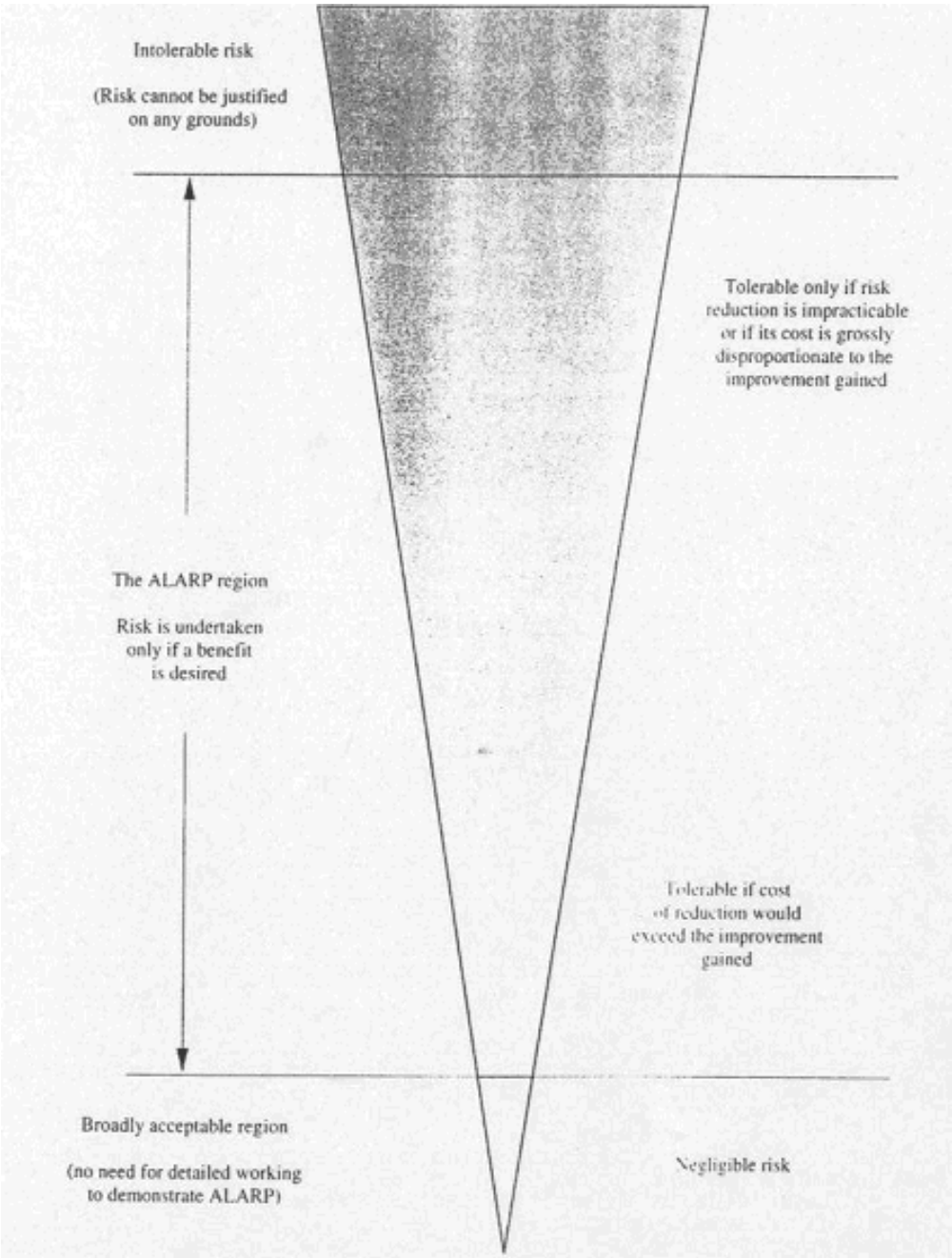
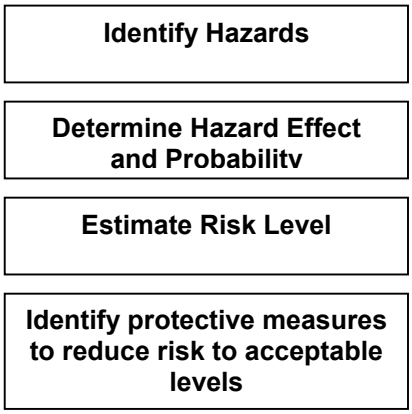


Figure 2.2 ALARP diagram. (Source: Health and Safety Executive, 1992, *The Tolerability of Risk from Nuclear Power Stations*. Crown copyright is reproduced with the permission of the Controller of HMSO.)

Qualitative Risk Assessment

Sometimes termed 'Practical' Risk Assessment



Identify Hazards

- **Using techniques identified previously**

Determine Hazard Effect and Probability

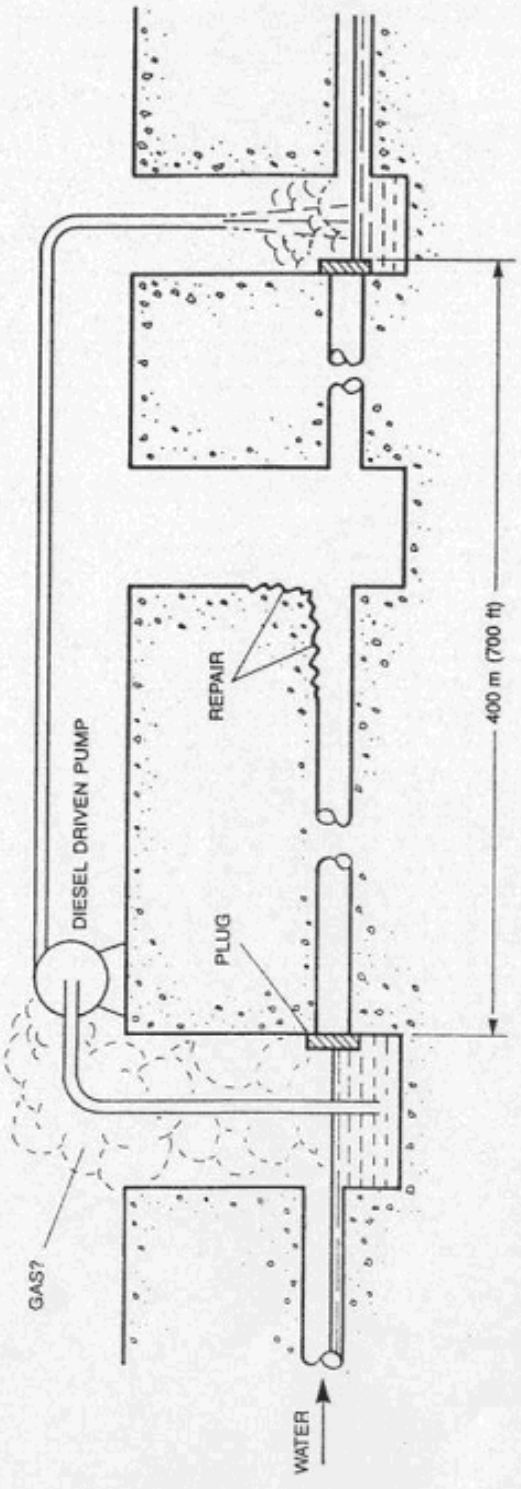
- **Hazard effects = types of injuries**
- **Classify effect into Low, Medium, High**
- **Classify probability into Low, Medium, High**

Estimate Risk Level

Risk = Hazard Effect x Probability

Prob. / H. Effect	Low	Medium	High
Low	*Low*	*Medium*	*Medium*
Medium	*Medium*	*Medium*	*High*
High	*Medium*	*High*	*High*

PROBLEM: Corrosion of the concrete of a 1.5m (5ft) diameter plant sewer has caused a partial collapse. Entry is necessary for inspection and repairs lasting three months during which the sewer must not shut down. It is proposed to pump the sewer water overland then isolate the damaged section. Repair and reline using glass reinforced resin. You are responsible for the job. Do you consider it can be done safely?



Quantitative Risk Assessment QRA

Usually based around some form of logic tree analysis

Probability

Dimensionless number between 0 and 1

Probability of particular outcome occurring = P

Probability combinations ->

Given two entirely separate events which can lead to outcomes A and B respectively which are entirely independent of each other P_A and P_B

- **Probability of outcome A AND outcome B occurring = $P_A P_B$**
- **Probability of outcome A OR outcome B occurring = $P_A + P_B - P_A P_B$**

Component Failure Rate

Failure or hazard rate λ = number of times a particular event occurs per unit time.

Probability of failure in time t is given by $P(t) = 1 - e^{-\lambda t}$

Example of Failure Rate Combinations

Two components A and B have mean failure rates of 50 per 10^6 hours and 100 per 10^6 hours respectively.

If either components fail then a hazard condition occurs.

What is the chance of the hazard condition occurring during a 1000 hour period?

λ_A **= 50 x 10^{-6}**
t = 1000
$\lambda_A t$ **= 50 x 10^{-3}**
P_A **= 0.049**

λ_B **= 100 x 10^{-6}**
t = 1000
$\lambda_B t$ **= 100 x 10^{-3}**
P_B **= 0.095**

P_A **OR** P_B **= 0.049 + 0.095 - (0.049 x 0.095)**

= 0.139

If the system is redesigned such that a hazard condition only occurs when both components fail at the same time, what is the chance now of the hazard condition occurring over the same period?

P_A **AND** P_B **= 0.049 x 0.095**

= 0.005 (c 28 times safer)