Risk Analysis and Management

Risk = Severity x Likelihood

- Extent of Damage
- Fatality
- Injuries
- Losses

- Analysis based on design and modeling equations

- Likelihood of event
- Based of failure frequency of process components

- Analysis based on manufacturer's and historical data

Risk – The probability that a hazard will result in a specified level of loss

LIKELIHOOD

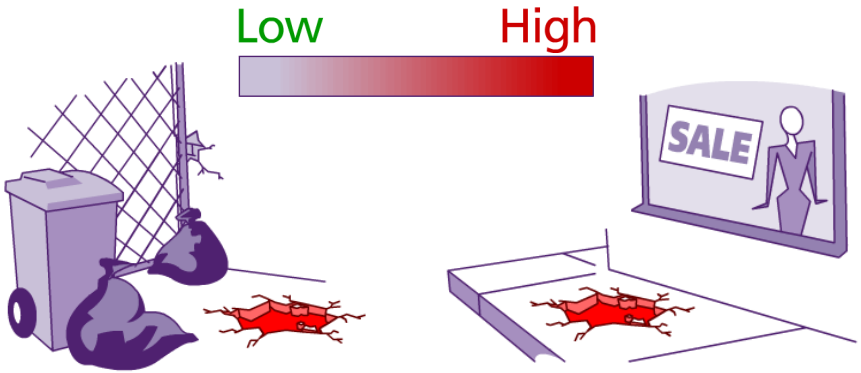
The likelihood is the chance that the hazardous event will occur

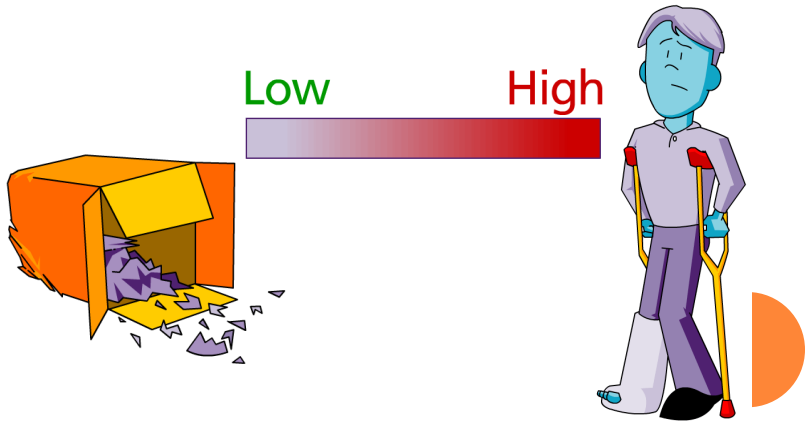
CONSEQUENCE

Consequence is the outcome of the hazardous event

RISK MEASUTREMENT

Risk = Likelihood x Consequence





Risk Management- The systematic application of management policies, procedures, and practices to the tasks of analyzing, assessing, and controlling risk in order to protect employees, the general public, and the environment, as well as company assets, while avoiding business interruptions.

Acceptable Risk: Risk that has been reduced to a level that can be tolerated by the organization having regard to its legal obligations and its own HSE policy.

Risk analysis is the estimation of the risk associated with the identified hazards, linking the likelihood of occurrence and severity of harms.

Risk evaluation compares the identified and analyzed risk against given risk criteria.

Risk communication is the sharing of information about risk and risk management between the decision makers and others. Communications might include those among interested parties (e.g., regulators and industry; industry and the patient; within a company, industry, or regulatory authority).

Risk control includes decision making to reduce and/or accept risks. The purpose of risk control is to reduce the risk to an acceptable level.

Risk assessment consists of the identification of hazards and the analysis and evaluation of risks associated with exposure to those hazards

Safety Audit:. "A safety audit subjects every area of organization's activity to a systematic Critical examination to reveal the strengths and weaknesses and the areas of vulnerability". One of the first systematic methods of hazard identification used in the chemical industry was the safety audit

Safety Survey: It is a detailed examination a narrow field such as specific procedures or a particular plant.

Safety inspection: Which is a scheduled inspection of a unit carried out by the units own personnel. Eg. Crane inspection

Safety Tour: It is unscheduled tour carried out by an outsider such as works manager or a safety representative.

5 steps of Risk assessment

Step 1: Identify the hazards

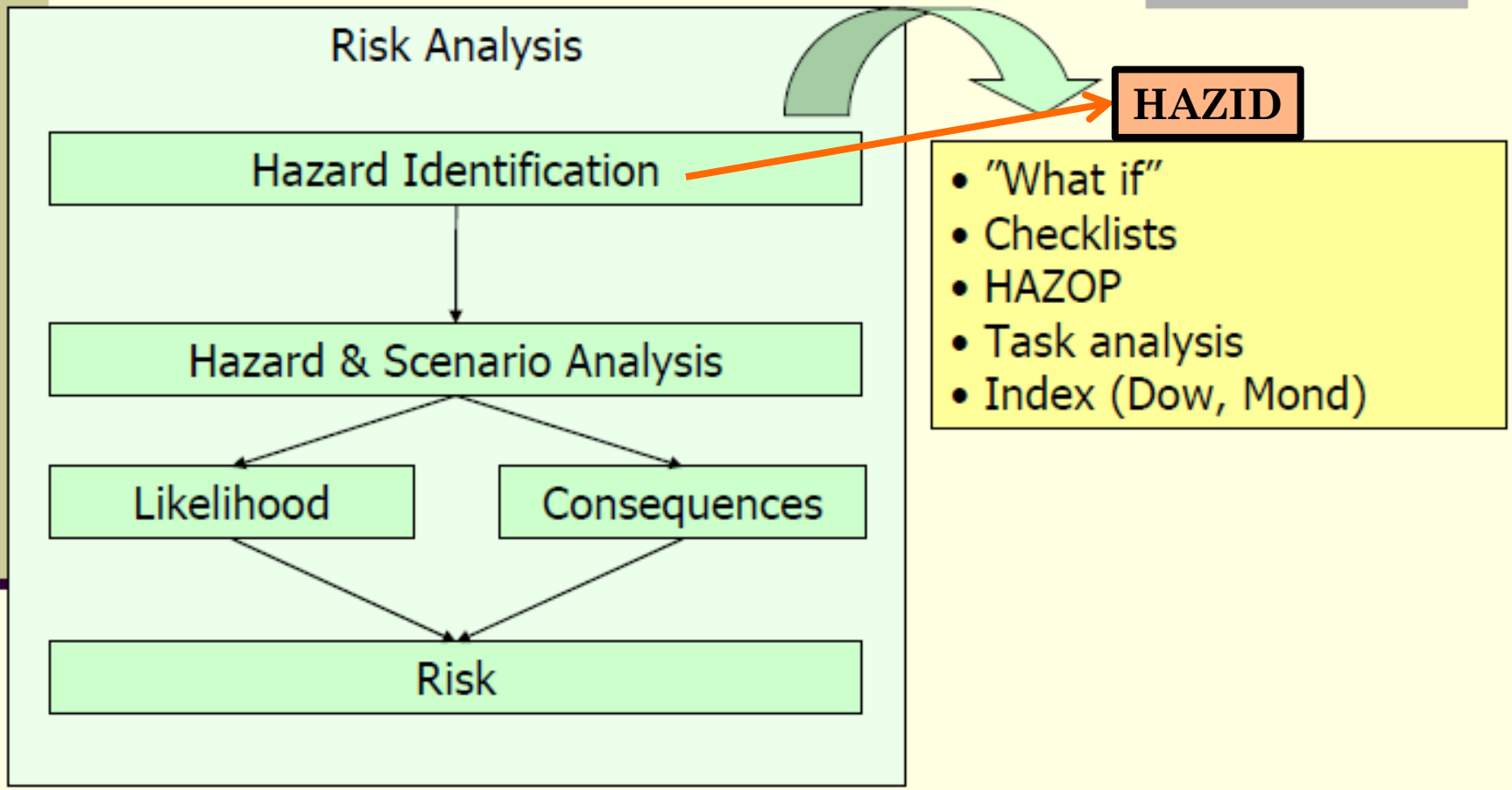
Step 2: Decide who might be harmed and how

Step 3: Evaluate the risks and decide on precautions

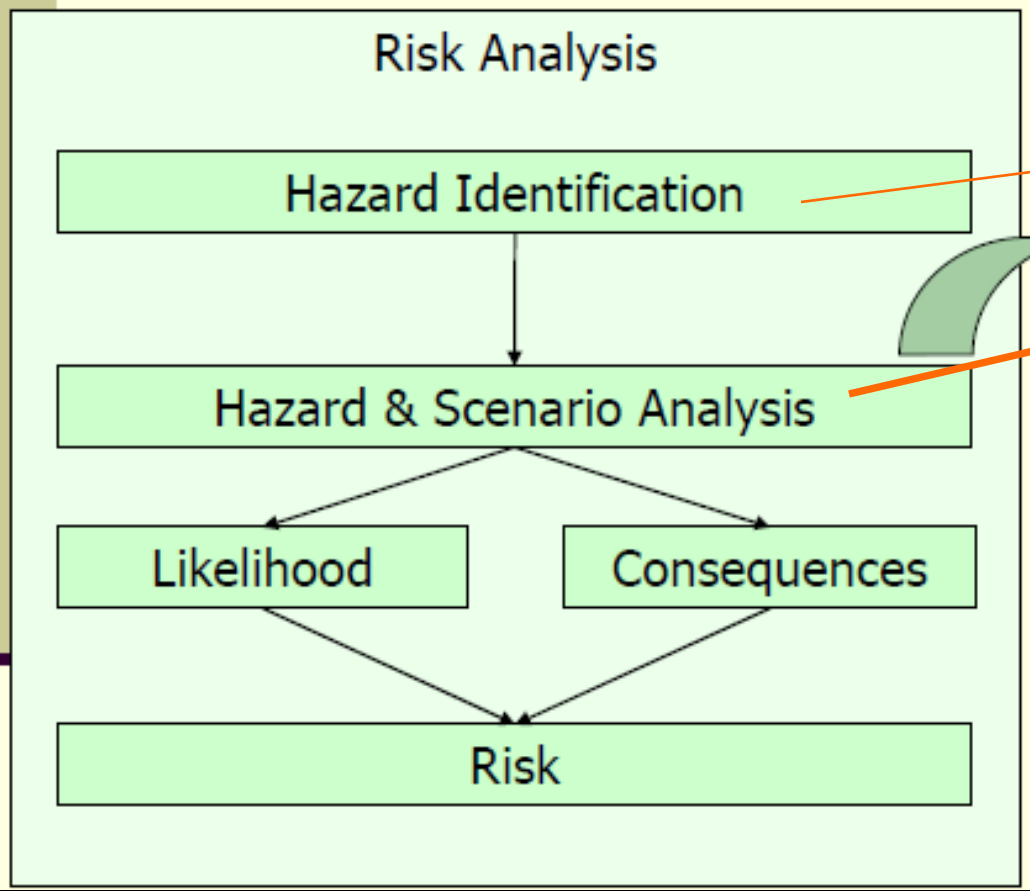
Step 4: Record your findings and implement them

Step 5: Review your risk assessment and update if necessary

Risk Analysis – Main Steps



Risk Analysis – Main Steps



HAZID

HAZAN

- Fault tree analysis
- Event tree analysis
- Bowties
- Barrier diagrams
- Reliability data
- Human reliability
- Consequence models

HAZID- Hazard Identification

Hazid is a high level hazard identification technique which is commonly applied on an area by area basis to hazardous installations. Hazid study is the systematic method of identifying hazards to prevent and reduce any adverse impact that could cause injury to personnel, damage or loss of property, environment and production, or become a liability. It is a component of the risk assessment and risk management..

HAZAN- Hazard Analysis

Hazan is the identification of undesired events that lead to the materialization of a hazard, the analysis of the mechanisms by which these undesired events could occur, and, usually, the estimation of the consequences

- It is good practice to review your risk assessment on a regular basis to be sure that nothing has changed and that your control methods are effective. Triggers for a review can also include:
- The start of a new project.
- A change in the work process or flow.
- A change or addition to tools, equipment, machinery (including locations or the way they are used).
- New employees.
- Moving to a new building or work area.
- Introduction of new chemicals or substances.
- When new information becomes available about a current product.

The following methods is generally used for the hazard identification

- What If Analysis
- Checklist Analysis
- Hazard and Operability Study (HAZOP)
- Failure Modes and Effects Analysis (FMEA)
- Job Safety analysis
- Human error analysis
- Safety Review
- Past accident report/ Near miss report

All these tools has their unique methodology and these are to be used as per the requirements. Finally all these methodologies are aim to minimise the Risk and suggest mitigation control measures to reach to the acceptable risk, if not possible to totally eliminate the Risk

Hazard Identification Techniques Reactive approach

- Accident Investigation
- Plant Inspection
- Incident Recall Technique

Proactive approach

- Safety Analysis (JSA)
- HIRA/HARC/HIRAC
- Failure Mode and Effect Analysis (FMEA)
- Hazard and Operability Study (HAZOP)
- Fault Tree and Event Tree Analysis (FTA & ETA)
- Fire Explosion and Toxicity Index (FETI)
- Material / Chemical Reactive Analysis
- Consequence analysis (Dispersion Modelling)

Incident recall technique

- Incident recall is to help people remember events that could have led to undesired consequences. These incidents help to learn from accidents / incidents.
- The interviewing could be done by a supervisor / manager or by a staff person
- It could be done on a one-on-one basis or as a group exercise.

Suitability of techniques to phase of project

	Concept	Process	Design	Commissioning	Operation	Modification	Decommissioning
HAZOP							
What if							
Checklist							
FMEA							
FTA							

Job Hazard Analysis

WHAT IS JOB HAZARD ANALYSIS (JHA)?

- A method of studying a job in order to:
  - **(a)** Identify hazards or potential incidents associated with each step or task and
  - **(b)** Develop solutions that will eliminate, nullify, or prevent such hazards or incident potential

When is a JHA required?

- If an existing JHA is **not** available
- Not adequately updated or suited to the job
- A **JHA** is a mandatory requirement for all tasks that require a Permit to Work to be issued.

JHA Team Selection

A team of skilled professionals should be used when developing a JHA, known as the **JHA Team**:

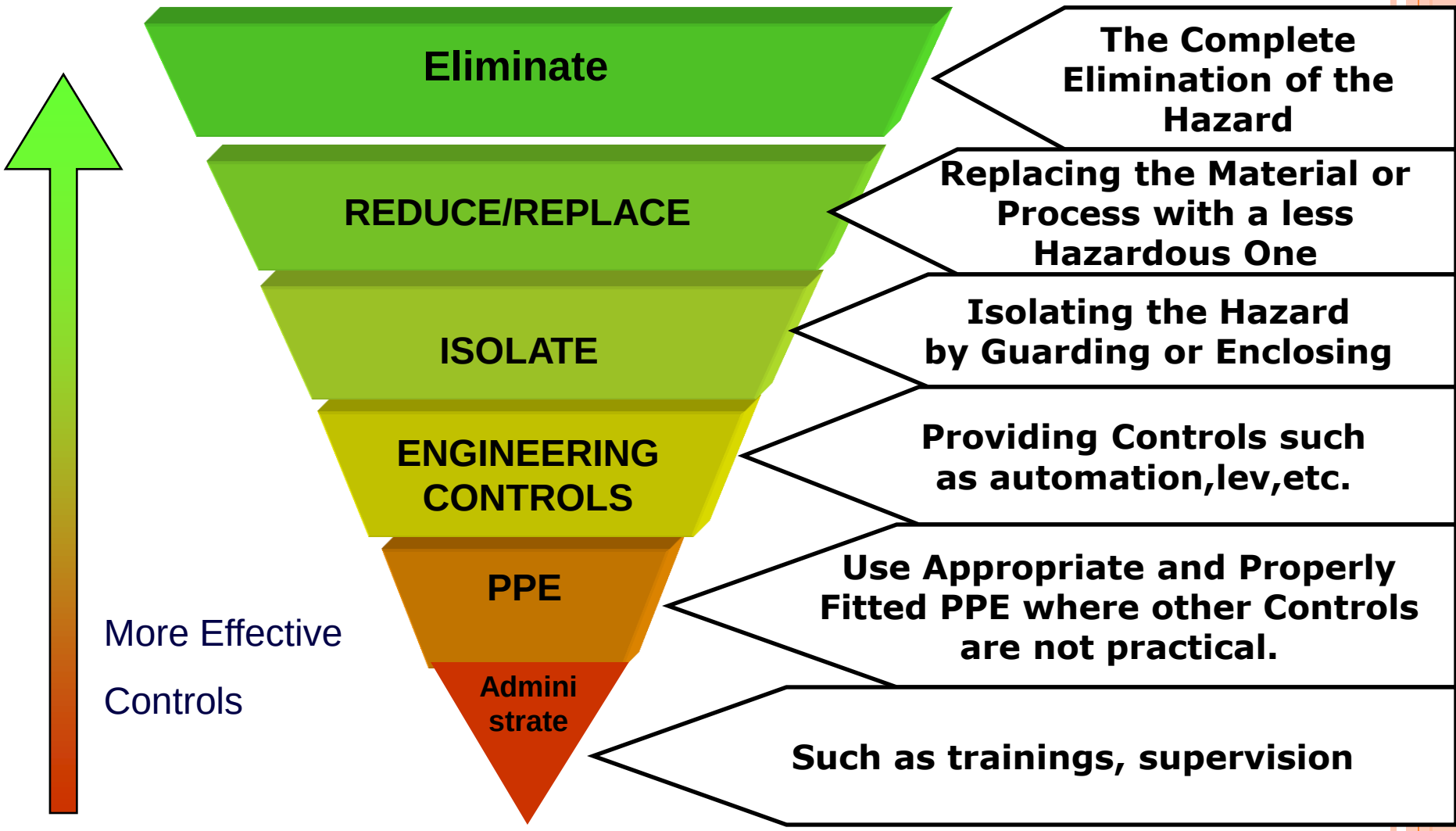
- Line Management (Supervisors)
- Employee who has experience with job
- Group Involvement - those that do the job (Performing party)
- Use safety professionals or practitioners as guidance & resource
- Emergency management team
- Communications

JHA Development

Five stages of JHA development

- Inspect the work site
- Breakdown the job into different Tasks
- Identify the Hazards for each Task
- Assess the Risk for Each Task
- Determine the Risk Control Measures and Action Plan

Determine the Risk Control Measures and Action Plan



JHA SIGN OFF AND RECORD

- Sign off of the JHA must occur by the involved parties for the JHA to be considered an accepted document.
- Records has to be updated and reviewed.

JHA Review

A **JHA** must be reviewed the following:

- The scope of work changes
- Significant change to the work environment
- There is an Incident or Near Miss
- At least once every two years to remain valid

HIRAC- Hazard Identification risk assessment and control

HIRAC (Hazard Identification risk assessment and control)

To develop a method for Identification of Occupational Health and Safety (OHS) hazards, assessment of risks and determination of necessary control measures to reduce the risks of injury and ill health

Example- Applied widely in construction industry

To what activity can the HIRAC be applied?

1. Only for Routine Activity
2. Only for Non Routine Activity
3. **Both**

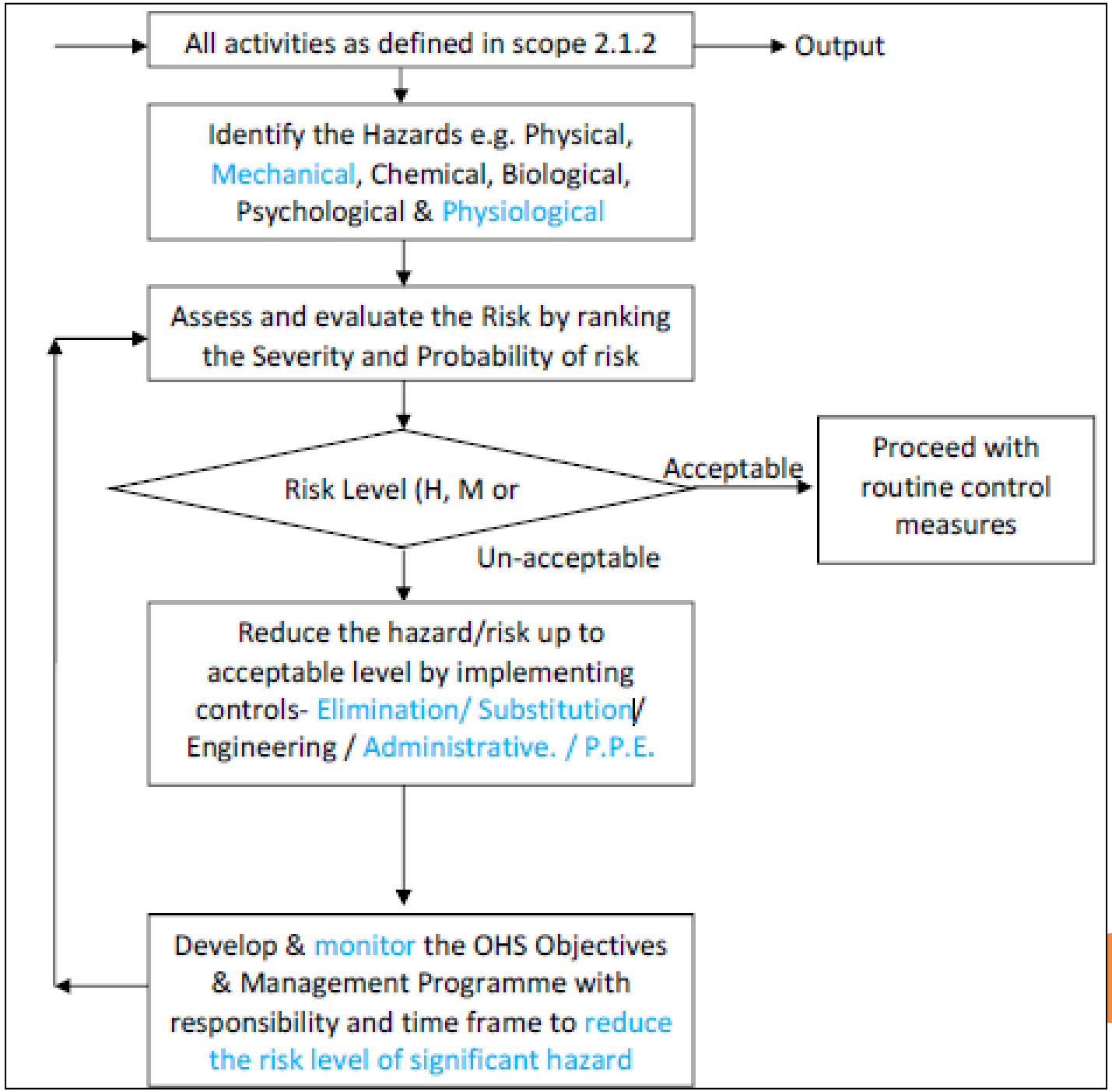
Non Routine Activity : An activity which can be carried out only a small period of time.

Example ; Blasting of rock occurs only for few days during construction

HIRAC (Hazard Identification risk assessment and control)

People who should participate in HIRAC Process

- Project Managers
- Functional and departmental Heads
- Workmen
- Supervisors,
- HSE Engineers


All activities as defined in scope 2.1.2
Output
Identify the Hazards e.g. Physical, Mechanical, Chemical, Biological, Psychological & Physiological
Assess and evaluate the Risk by ranking the Severity and Probability of risk
Risk Level (H, M or
Acceptable
Proceed with routine control measures
Un-acceptable
Reduce the hazard/risk up to acceptable level by implementing controls- Elimination/ Substitution/ Engineering / Administrative. / P.P.E.
Develop & monitor the OHS Objectives & Management Programme with responsibility and time frame to reduce the risk level of significant hazard

SEVERITY FACTOR

S	Severity	Impact
1	Negligible	Slight injury or health effects (including first aid and medical treatment cases) not affecting work performance or causing disability.
2	Marginal	Minor injury or health effects-affecting work performance e.g. restriction to activities or need a time off to recover (Lost time accident) reversible health effects, e.g. skin irritation, food poisoning.
3	Critical	Major injury or health effects (including permanent disability) – affecting work performance in longer term, e.g. irreversible health damage without loss of life (Noise induced hearing loss, chronic back injuries)
4	Severe	Single fatality or permanent total disability or major occupational illness.
5	Catastrophic	Multiple fatalities from an incident or Occupational chronic illness leading to death/fatality (poisoning, cancer).

PROBABILITY FACTOR

P	Probability	Frequency	Ratio
1	Remote	1 in every 10 year of operation.	1:1000
2	Unlikely	1 in every year of operation.	1:100
3	Occasional	1 in every month of operation.	1:10
4	Likely	1 in every week of operation.	1:4
5	Frequent	1 in every day of operation.	1:2

5*5 Risk Matrix

PROBABILITY						
	5	5	10	15	20	25
	4	4	8	12	16	20
	3	3	6	9	12	15
	2	2	4	6	8	10
	1	1	2	3	4	5
		1	2	3	4	5
		SEVERITY				

Risk Slab	Risk Level	Colour code
From 1 - 6	Low Risk (L)	
Between 8 - 12	Medium Risk (M)	
More than 15 - 25	High Risk (H)	

Determine Risk Level by using S & P factors using the formula given below:
Risk Level = Severity (S) X Probability (P)

PRELIMNARY HAZARD ANALYSIS

Preliminary Hazard Analysis

PHA [Preliminary Hazard Analysis] is carried out to **identify** and describe **Hazards & Threats** at **earliest stage** of the Project design development.

Example

Consider a design concept that feeds H_2S (Hydrogen sulphide)from a pressurized storage cylinder to a process unit. at this stage of the design , the analyst knows only that this material will be used in the process , nothing more . The analyst recognizes that h2s has toxic and flammable properties, and the analyst identifies the potential release of h2s as a hazardous situation.

The analyst lists the following causes for such a release….

- The pressurized storage cylinder leaks or ruptures
- The process does not consume all of the h2s
- The h2s process supply lines leak/rupture
- A leak occurs during connection of a cylinder to the process

The analyst then determines the effects of these causes. in this case , fatalities could result from large releases. The next task is to provide guidance and design criteria by describing corrective/preventive measures for each possible release.

The analyst suggests that the designer:….

- Consider a process that stores alternative, less toxic materials that can generate h2s as needed
- Consider developing a system to collect and destroy excess h2s from the process
- Provide a plant warning system for h2s releases
- Minimize on-site storage of h2s, without requiring excessive delivery/handling
- Develop a procedure using human factors engineering expertise for storage cylinder connection
- Consider a cylinder enclosure with a water deluge system that is triggered by h2s leak detection
- Locate the storage cylinder for easy delivery access, but away from other plant traffic.

HAZOP (Hazard Operability Study)

HAZOP

- HAZOP is a hazard analysis technique that systematically divides a system, equipment, or process into a series of nodes to identify possible deviations from normal operations and ensure that appropriate safeguards are in place to help prevent accidents.
- Before the HAZOP study is started, detailed information on the process must be available.
- This includes up-to-date process flow diagrams (PFDs), process and instrumentation diagrams (P&IDs), detailed equipment specifications, materials of construction, and mass and energy balances.
- The full HAZOP study requires a committee composed of a cross-section of experienced plant, laboratory, technical, and safety professionals. One individual must be a trained HAZOP leader and serves as the committee chair

Terminology used in HAZOP Study

a. STUDY NODES - The locations (on piping and instrumentation drawings and procedures) at which the process parameters are investigated for deviations.

b. INTENTION - The intention defines how the plant is expected to operate in the absence of deviations at the study nodes. This can take a number of forms and can either be descriptive or diagrammatic; e.g., flow sheets, line diagrams, P&IDS.

c. DEVIATIONS - These are departures from the intention which are discovered by systematically applying the guide words (e.g., "more pressure").

Guide word + Parameter → Deviation

d. CAUSES - These are the reasons why deviations might occur. Once a deviation has been shown to have a credible cause, it can be treated as a meaningful deviation. These causes can be hardware failures, human errors, an unanticipated process state (e.g., change of composition), external disruptions (e.g., loss of power), etc.

e. CONSEQUENCES - These are the results of the deviations should they occur (e.g., release of toxic materials). Trivial consequences, relative to the study objective, are dropped.

f. GUIDE WORDS - These are simple words which are used to qualify or quantify the intention in order to guide and stimulate the brainstorming process and so discover deviations.

Guide words	Meaning	Comments
NO, NOT, NONE	The complete negation of the intention	No part of the design intention is achieved, but nothing else happens.
MORE, HIGHER, GREATER	Quantitative increase	Applies to quantities such as flow rate and temperature and to activities such as heating and reaction.
LESS, LOWER	Quantitative decrease	Applies to quantities such as flow rate and temperature and to activities such as heating and reaction.
AS WELL AS	Qualitative increase	All the design and operating intentions are achieved along with some additional activity, such as contamination of process streams.
PART OF	Qualitative decrease	Only some of the design intentions are achieved, some are not.
REVERSE	The logical opposite of	Most applicable to activities such as flow or chemical reaction. Also applicable to substances, for example, poison instead of antidote.
OTHER THAN	Complete substitution	No part of the original intention is achieved – the original intention is replaced by something else.
SOONER THAN	Too early or in the wrong order	Applies to process steps or actions.
LATER THAN	Too late or in the wrong order	Applies to process steps or actions.
WHERE ELSE	In additional locations	Applies to process locations, or locations in operating procedures.

Example of HAZOP Matrix

Guide word / Process-variable	No	Low	High	Part of	Also	Other than	Reverse
Flow	No flow	Low flow	High flow	Missing ingredients	Impurities	Wrong material	Reverse flow
Level	Empty	Low level	High level	Low interface	High interface	-	-
Pressure	Open to atmosphere	Low pressure	High pressure	-	-	-	Vacuum
Temperature	Freezing	Low temp.	High temp.	-	-	-	Auto refrigeration
Agitation	No agitation	Poor mixing	Excessive mixing	Irregular-mixing	Foaming	-	Phase separation
Reaction	No reaction	Slow reaction	"Runaway reaction"	Partial reaction	Side reaction	Wrong reaction	Decom-position
Other	Utility failure	External leak	External rupture	-	-	Start-up Shutdown Maintenance	-

Parameters

Application of parameters will depend on the type of process being considered, the equipment in the process and the process intent.

- Pressure
- Temperature
- Flow
- Voltage
- Ph
- Velocity
- Viscosity
- Corrosion

Process parameters	No, not, none	More, higher, greater	Less, lower	As well as	Part of	Reverse	Other than	Sooner, faster	Later, slower	W
Flow	x	x	x	x	x	x	x	x	x	
Temperature		x	x					x	x	
Pressure		x	x	x				x	x	
Concentration	x	x	x	x	x		x	x	x	
pH		x	x					x	x	
Viscosity		x	x					x	x	
Level	x	x	x	x	x		x	x	x	
Temperature		x	x					x	x	
Pressure		x	x	x				x	x	
Concentration	x	x	x	x	x		x	x	x	
pH		x	x					x	x	
Viscosity		x	x					x	x	
Agitation	x	x	x		x	x		x	x	
Volume	x	x	x	x	x			x	x	
Reaction	x	x	x				x	x	x	
State				x			x	x	x	
Sample	x			x	x		x	x	x	

Deviation

- High temperature
- Low temperature
- High viscosity
- Low flow
- High flow
- Reverse flow

3 CAUSES OF DEVIATION

1. **Human Error** - acts of omission or commission by an operator, designer, constructor or other person creating a hazard that could possibly result in a release of hazardous or flammable material. Example- Operator failed to close the value on time
2. **Equipment failure** in which a mechanical, structural or operating failure results in the release of hazardous or flammable material. Example- Failure of a pump
3. **External Events** in which items outside the unit being reviewed affect the operation of the unit to the extent that the release of hazardous or flammable material is possible. Example- Explosion

- Safeguards should be included whenever the team determines that a combination of cause and consequence presents a credible process hazard

1. Those systems, engineered designs and written procedures that are designed to prevent a catastrophic release of hazardous or flammable material.
   Example- Pressure Relief Value
2. Those systems that are designed to detect and give early warning following the initiating cause of a release of hazardous or flammable material.
   Example- Pressure level Indicator
3. Those systems or written procedures that mitigate the consequences of a release of hazardous or flammable material. Example- Deliberate Ignition

Recommendations

Recommendations are made when the safeguards for a given hazard scenario, as judged by an assessment of the risk of the scenario, are inadequate to protect against the hazard.

1. High priority action items should be resolved within 4 months.
2. Medium priority action items should be resolved within 4-6 months.
3. Lower priority action items should be resolved following medium priority items.

Prerequisites

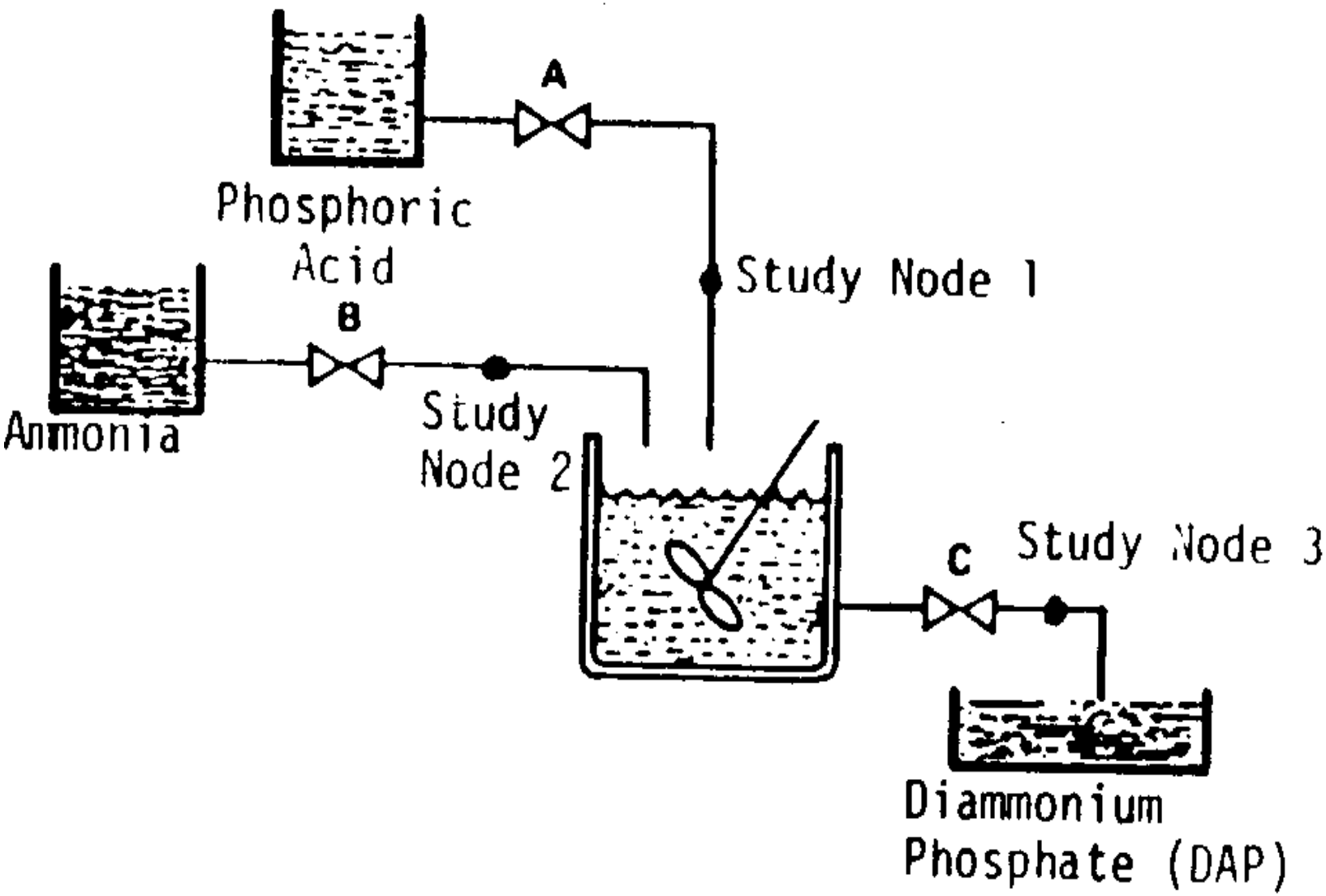
As a basis for the HAZOP study the following information should be available:

- **Process flow diagrams (PFD)**
- **Piping and instrumentation diagrams (P&IDs)**
- **Layout diagrams**
- **Material safety data sheets**
- **Provisional operating instructions**
- **Heat and material balances**
- **Equipment data sheets Start-up and emergency shut-down procedures**

HAZOP PROCEDURE

1. Divide the system into sections (i.e., reactor, storage)
2. Choose a study node (i.e., line, vessel, pump, operating instruction)
3. Describe the design intent
4. Select a process parameter
5. Apply a guide-word
6. Determine cause(s)
7. Evaluate consequences/problems
8. Recommend action: What? When? Who?
9. Record information
10. Repeat procedure (from step 2)

- Consider, as a simple example, the continuous process shown in Figure. In this process, the phosphoric acid and ammonia are mixed, and a non-hazardous product, diammonium phosphate (DAP), results if the reaction of ammonia is complete. If too little phosphoric acid is added, the reaction is incomplete, and ammonia is produced. Too little ammonia available to the reactor results in a safe but undesirable product. The Hazop team is assigned to investigate "Personnel Hazards from the Reaction".



CONTINUOUS PROCESS EXAMPLE FOR HAZOP TECHNIQUE

Node:1 **Process parameter: flow**

Intention:-Phosphoric acid feed solution to the reactor at a rate of 1000 lpm and 3 bar Pressure

Guide Word	Deviation	Causes	Consequences	Action Required
NO	No Flow	Empty Tank A Rupture of Value Blockage in wall		
Less	Less flow			

Node:1 **Process parameter: flow**

Intention:-Phosphoric acid feed solution to the reactor at a rate of X gpm and Y psig

Guide Word	Deviation	Causes	Consequences	Action Required
No	No Flow At Study Node 1	Valve A Falls Closed Phosphoric Acid Supply Exhausted Plug In Pipe, Pipe Ruptures	Excess Ammonia In Reactor And Release To Work Area	Automatic Closure Of Valve B On Loss Of Flow From Phosphoric Acid Supply.
More	Increased Flow At Study Node 1	----	Excess Phosphoric Acid Degrades Product But Presents No Hazard To Workplace.	-----
Less	Reduced Flow At Source Formatting	Valve A Partially Closed	Excess Ammonia In Reactor And Release To Work Area	Automatic Closure Of Valve B Based

Guide Word	Deviation	Causes	Consequences	Action Required
Part Of	Decreased Concentration Of Phosphoric Acid At Study Node 1	Vendor Delivers Wrong Material Or Concentration Error In Charging Phosphoric Acid Supply Tank	Excess Ammonia In Reactor And Release To Work Area. Amount Released Is Related To Quantitative Reduction In Supply. Team Member Assigned To Calculate Toxicity Level Versus Flow Reduction	Add Check Of Phosphoric Acid Supply Tank Concentration After Charging Procedures
Reverse	Reverse Flow At Study Node 1	No Reasonable Mechanism For Reverse Flow.	-----	-----
Other Than	Material Other Than Phosphoric Acid In Line A	Wrong Delivery From Vendor Wrong Material Chosen From Plant Warehouse	Depends On Substitution; Team Member Assigned To Test Potential Substitutions Based On Availability Of Other Materials At Site And Similarity In Appearance	Plant Procedures To Provide Check On Material Chosen Before Charging Phosphoric Acid Supply Tank.

Node:2 **Process parameter: flow**

Intention:-Deliver 20% ammonia solution to the reactor at Y gpm and Z psig

Guide word	Deviation	Causes	Consequences	Action required
High	High flow at study node 2	Ammonia feed line control valve B fails to open. Operator sets ammonia flow rate too high.	Untreated ammonia solution carry over to the DAP storage tank and release to the work area.	Consider adding an alarm/shutdown of the system for high ammonia solution flow to the reactor. Ensure periodic maintenance and inspection for valve B is adequate.
No flow	Leakage at ammonia tank	Corrosion erosion external impacts Gasket and packing failures Maintenance errors	Small, continuous leak of ammonia to the enclosed work area	Ensure adequate ventilation exists for enclosed work area.

Node:3 **Process parameter: flow**

Intention:-Deliver product flow to the storage tank at X gpm and Y psig.

Guide word	Deviation	Causes	Consequences	Action required
Reverse	reverse flow at study node 1	no reasonable mechanism for reverse flow.	-----	-----

Advantages

- **Systematic examination**
- **Multidisciplinary study**
- **Utilizes operational experience**
- **Covers safety as well as operational aspects**
- **Solutions to the problems identified may be indicated**
- **Considers operational procedures**
- **Covers human errors**
- **Study led by independent person**

Disadvantages

- Can be time-consuming
- Relies on having right people in the room

Finally…,

HAZOP is an essential tool for hazard identification and have been used successfully to improve the safety and operability of both new and existing chemical plant. The technique is not confined to the chemical and pharmaceutical industries and has also been used successfully in a number of other industries, including the off-shore oil and food industries.

WHAT IF ANALYSIS

What-If Analysis

- A What-If is a **brainstorming approach** in which a group of people familiar with the process ask questions about possible deviations or failures and what things can go wrong
- Each question represents a potential failure in the facility or mis-operation of the facility.
- Lead by an energetic and focused facilitator, each member of the review team participates in assessing what can go wrong based on their past experiences and knowledge of similar situations
- At each step in the procedure or process, What-If questions are asked and answers generated.

What-If Analysis – Steps

1. Divide the system up into smaller, logical subsystems
2. Identify a list of questions for a subsystem
3. Select a question
4. Identify hazards, consequences, severity, likelihood, and recommendations
5. Repeat Step 2 through 4 until complete

- What-If analysis are intended to identify hazards, hazardous situations, or accident scenarios.
- For a small or simple system a What-If analysis will take 4 to 8 hours to prepare, 1 to 3 days to evaluate the process, and 1 to 2 days to document the results.
- For larger or more complex processes, it will take 1 to 3 days to prepare, 4 to 7 days to evaluate, and 4 to 7 days to document.

What-If Question Example

- Equipment failures What if … a valve leaks?.
- Human error What if … operator fails to restart pump?
- External events What if … a very hard freeze persists?

Team members usually include

- Operators
- Maintenance personnel,
- Design engineers, chemist, structural engineer, radiation expert,

A safety representative will lead the team. Their knowledge of design standards, regulatory codes, past and potential operational errors as well as maintenance difficulties brings a practical reality to the review

WHAT if. . .	RISK	METHOD TO REDUCE RISK	ACTION REQUIRED
		The placing head is adequately covered by enclosure, in order to prevent finger trapping, shearing and drawing-in.	
. . . an N2 Overpressure occurs?	Equipment Damage	Pressure regulator limited to 30 psi. IR Specification for set point of the pressure regulator. Burst pressure of regulator and IR pressure rating of components set.	No further action
. . . vacuum pressure is high (near atmospheric)	Process error resulting in wafer damage	Vacuum presence monitored and system inhibits operation at high vacuum conditions	No further action
. . . vacuum pressure is low	Process error resulting in wafer damage	Vacuum presence monitored and system inhibits operation at low vacuum conditions	No further action
. . . no vacuum pressure	Process error resulting in wafer damage	Vacuum presence monitored and system inhibits operation at low vacuum conditions	No further action
. . . blockage of air between the pressure switch and heater assembly?	Burn-out the heater and smoke, potential evacuation	Add airflow switch	Action required – airflow switch must be installed
. . . voltage is too high?	Dielectric breakdown, overvoltage supplied to components and power supply failure	Test for dielectric withstand; DC power supplies incorporate internal voltage compensations by design	No further action
. . . shutter is activated and spring fails?	Potential for personnel to be exposed to Laser	Shutter is not NRTL approved. Information on laser shutter (i.e., spring failure, internal tests) required	Actions Required -- Info on Laser Shutter needed and Evaluation to be

Advantages of ‘What if?’ analysis

- Easy to apply.

Disadvantages of ‘What if?’ analysis

- Experienced assessors are required . Their thoroughness and accuracy are dependent upon the composition and expertise of the team performing the analysis.
- Hazards can be missed
- Time consuming for complex processes.
- ‘What If’ hazard analyses stops at a single point of failure and does not investigate the system further. (i.e., This method would not evaluate a series of failures and the potential consequence of this series.)

CHECKLIST ANALYSIS

Checklist

- Consists of using a detailed list of prepared questions about the design and operation of the facility
- Questions are usually answered “Yes” or “No”
- Used to identify common hazards through compliance with established practices and standards.
- Checklist analysis involve assessment using predefined checklists. They are used in various stages of the project life cycle like risk identification.
- A checklist intended for use during the initial design of the process will be considerably different from a checklist used for a process change

Checklist – Summary

- The simplest of hazard analyses
- Easy-to-use
- Provides quick results; communicates information well
- Effective way to account for ‘lessons learned’
- **Not** helpful in identifying new or unrecognized hazards.
- Checklist should be prepared by experienced engineers
- Its application requires knowledge of the system/facility and its standard operating procedures
- Checklist Should be audited and updated regularly

Checklist Question Categories

- Causes of accidents
  - Process equipment
  - Human error
  - External events
- Facility Functions
  - Alarms, construction materials, control systems, documentation and training, instrumentation, piping, pumps, vessels, etc.

Checklist task

Your University has many fire extinguisher materials AND Fire alarms inside the campus. Create a checklist for the inspection, maintenance and use of fire Extinguisher and Fire alarm.

SAFETY REVIEW

Safety Reviews

Method that is commonly used to identify safety problems in laboratory and process areas and to develop solutions is the safety review.

There are two types of safety reviews

- Informal and
- Formal.

Informal Safety Review

- The *informal safety review* is used for **small changes to existing processes**. The reviewers simply meet in an **informal fashion to examine the process equipment and operating procedures and to offer suggestions on how the safety of the process might be improved.**
- Significant improvements should be summarized in a memo for others to reference in the future. The improvements must be implemented before the process is operated.
- The informal safety review procedure usually involves just **two or three people**. It includes the individual responsible for the process and one or two others not directly associated with the process but experienced with proper safety procedures.
- The idea is to provide a lively dialogue where ideas can be exchanged and safety improvements can be developed.

Formal safety review

The *formal safety review* is used for

- New processes,
- Substantial changes in existing processes,
- Processes that need an updated review.

The formal safety review is a three-step process.

1. Preparing a detailed formal safety review report,

2.Committee reviews the report and inspect the process, and

3. Implementing the recommendations.

Event tree Analysis

- **Event tree analysis** is based on binary logic, in which an event either has or has not happened or a component has or has not failed. It is valuable in analyzing the consequences arising from a failure or undesired event.It is a forward bottomup approach.

- An event tree begins with an initiating event, such as a **Loss of Containment, Loss increase in temperature/pressure, Fire, Explosion or a release of a hazardous substance**. The consequences of the event are followed through a series of possible paths.

Why event tree analysis is required

When an accident or process deviation (i.e. an "event") occurs in a plant, various safety systems (both mechanical and human) come into play to prevent the accident from propagating. These safety systems either fail or succeed.

Definition

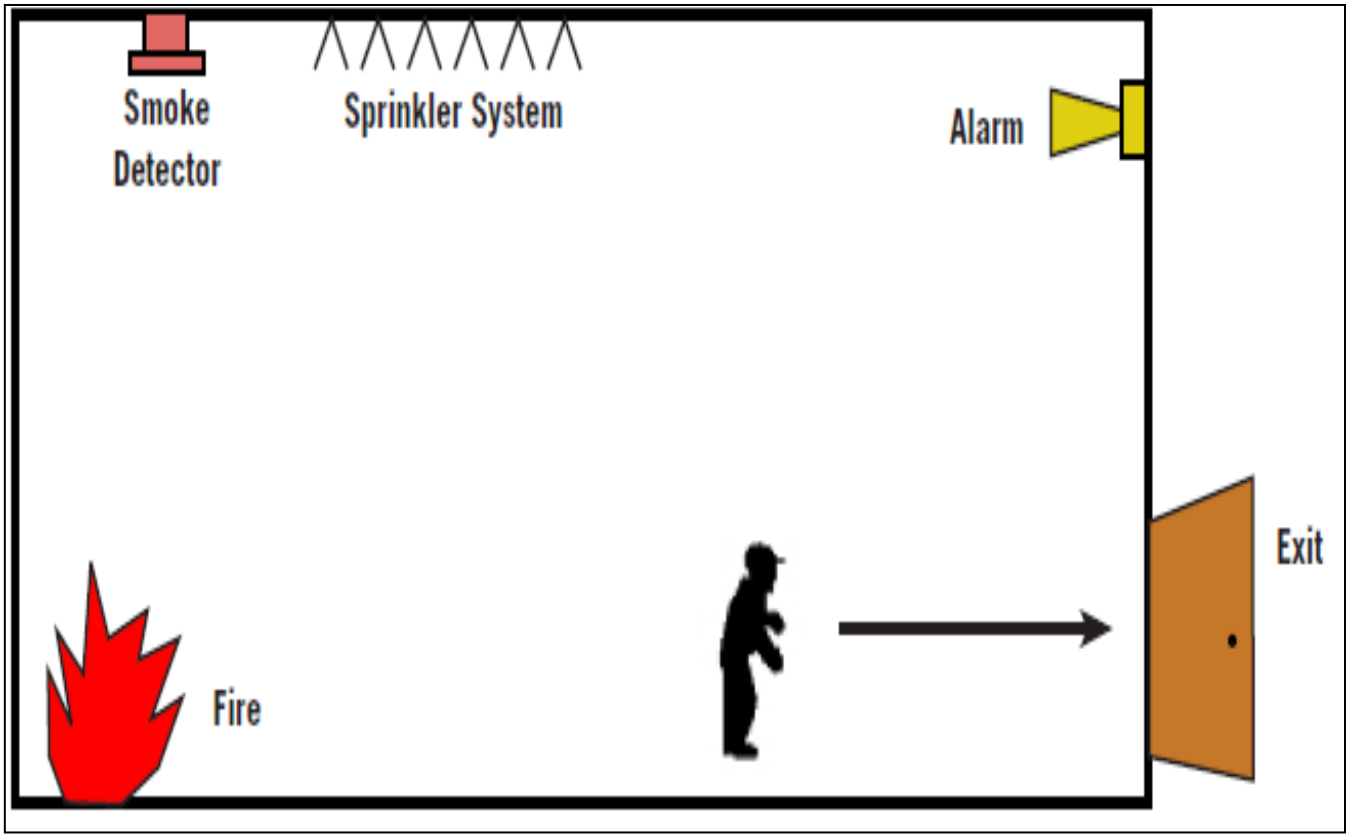
Initiating event - Failure or undesired event that initiates the start of an accident sequence.

Example- Fire, Explosion or a release of a hazardous substance

Pivotal events- Intermediary events between the IE and the final mishap. These are the failure/success events of the design safety methods established to prevent the Initiating Event from resulting in a mishap.

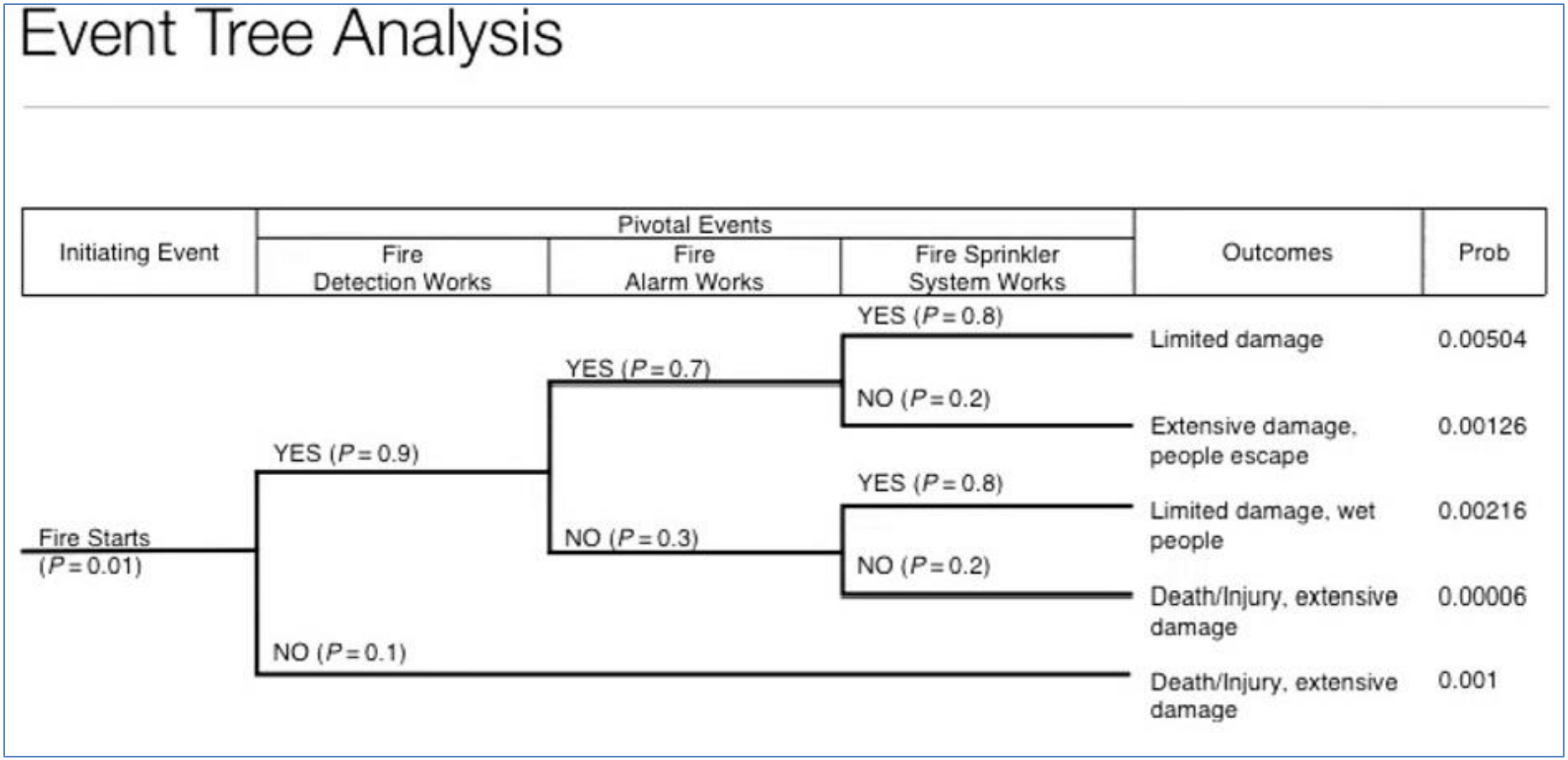
Example- Fire alarm works, Sprinkler system, Fire detection system

Accident scenario - Series of events that ultimately result in an accident. The sequence of events begins with an initiating event and is (usually) followed by one or more pivotal events that lead to the undesired end state.



The diagram shows an initiating event (e.g. fire) and the subsequent operation or failure of three systems (Fire Detection, Alarm system and sprinkler system) which would normally operate when the fire occur. The initiating event is typically specified as an expected annual frequency (e.g. 2 times per year) and the success/failure for each system as a probability.

Event tree Analysis- Fire in a room



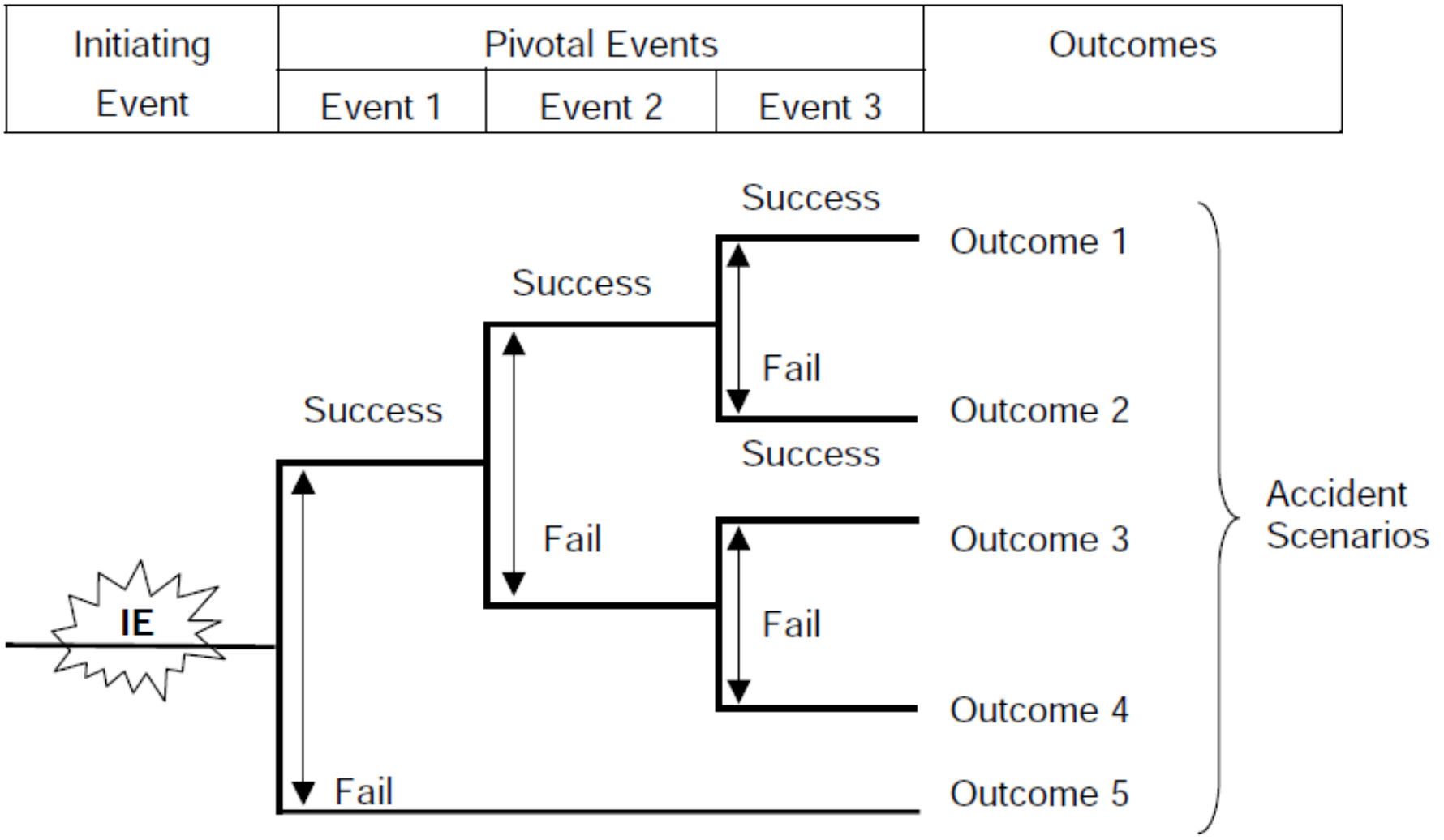


Figure 12.2 *Event tree concept.*

Event tree – PLG Leak from storage tank

VCE: Vapour Cloud Explosion

Jet fire: fire of a gas leak /pressurised liquid

Flash fire: deflagration without explosive effects

Steps in Event tree construction

1. Identify the Initiating event
2. Identify the controls that are assigned to deal with the primary event such as automatic safety systems, alarms on operator actions.
3. Construct the event tree beginning with the initiating event and proceeding through failures of the safety functions.
4. Establish the resulting accident sequences.
5. Identify the critical failures that need to be addressed

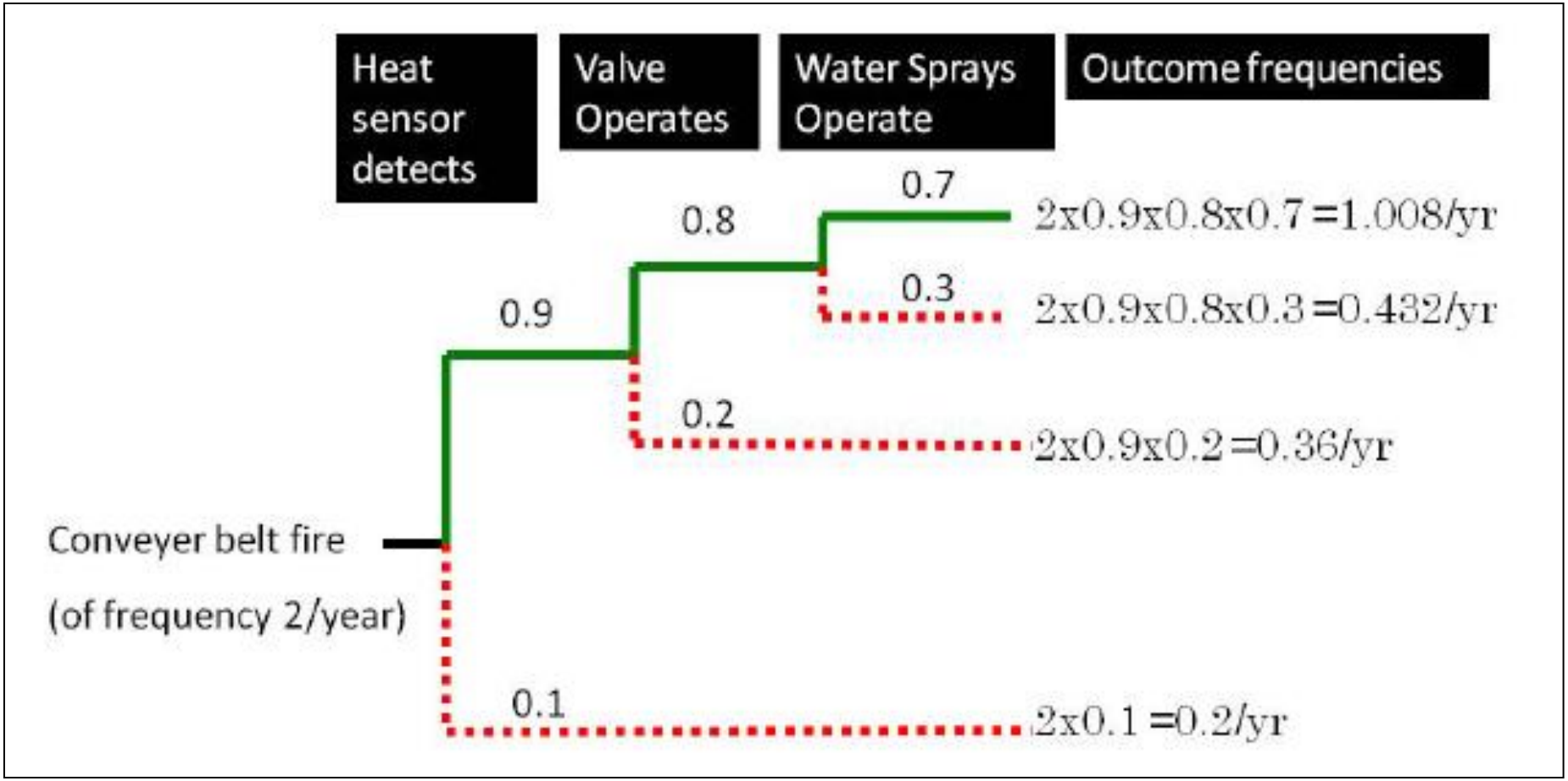
Advantages

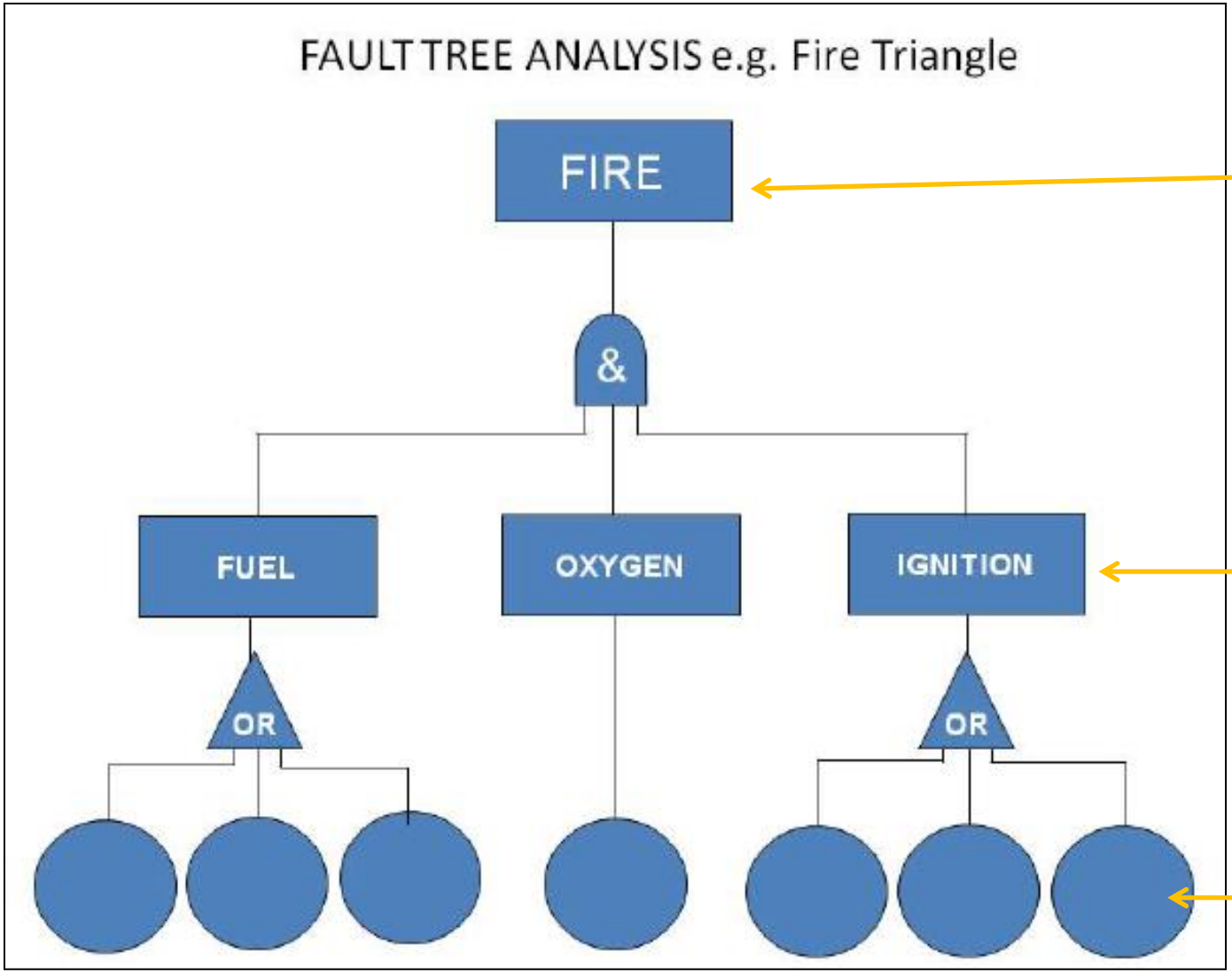
- Combines hardware, software, environment, and human interaction.
- Permits probability assessment.
- Commercial software is available.

Disadvantages

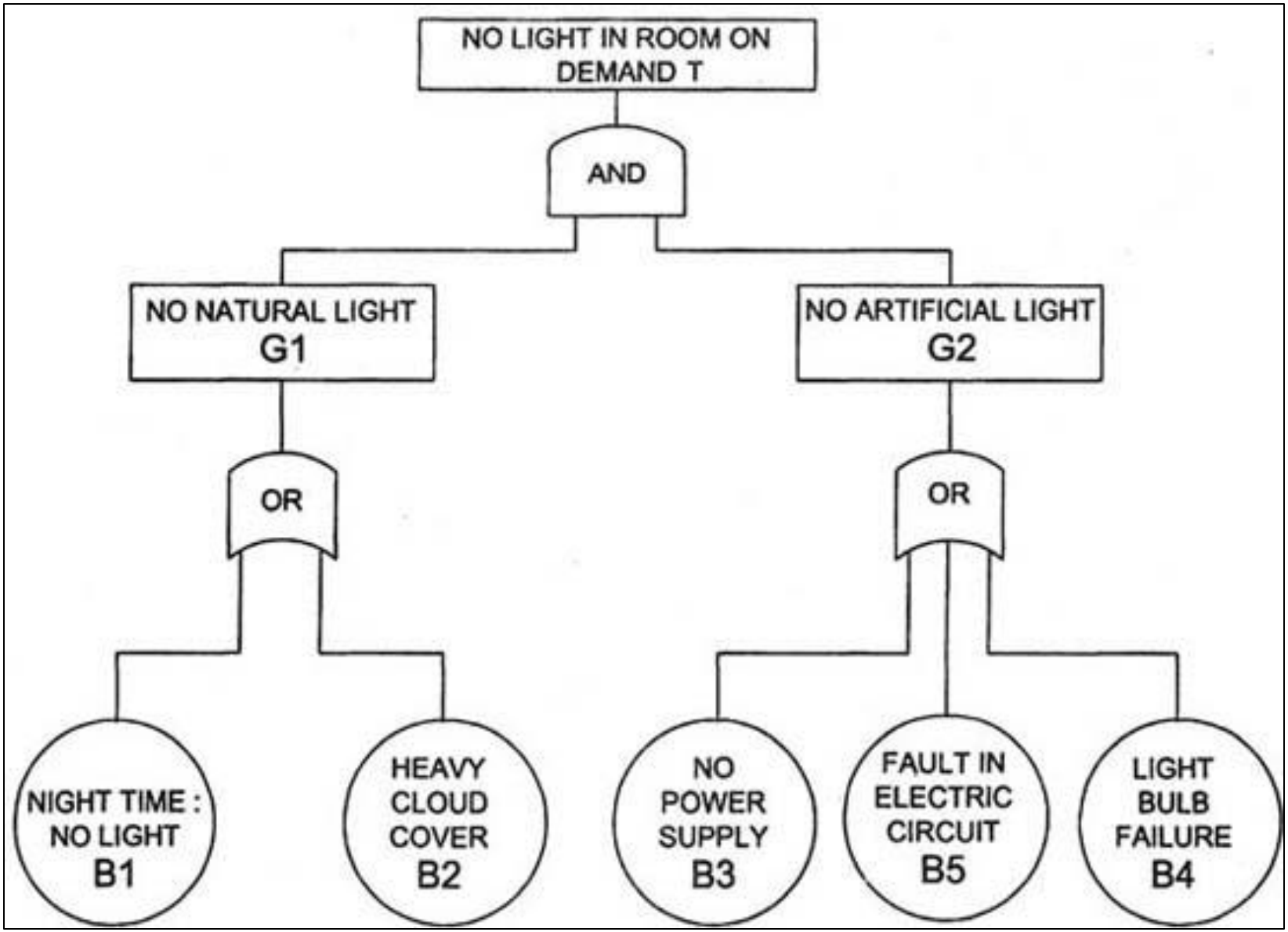
- An ETA can only have one initiating event, therefore multiple ETAs will be required to evaluate the consequence of multiple initiating events.
- Requires an analyst with some training and practical experience.

Event tree – Fire in a conveyor system

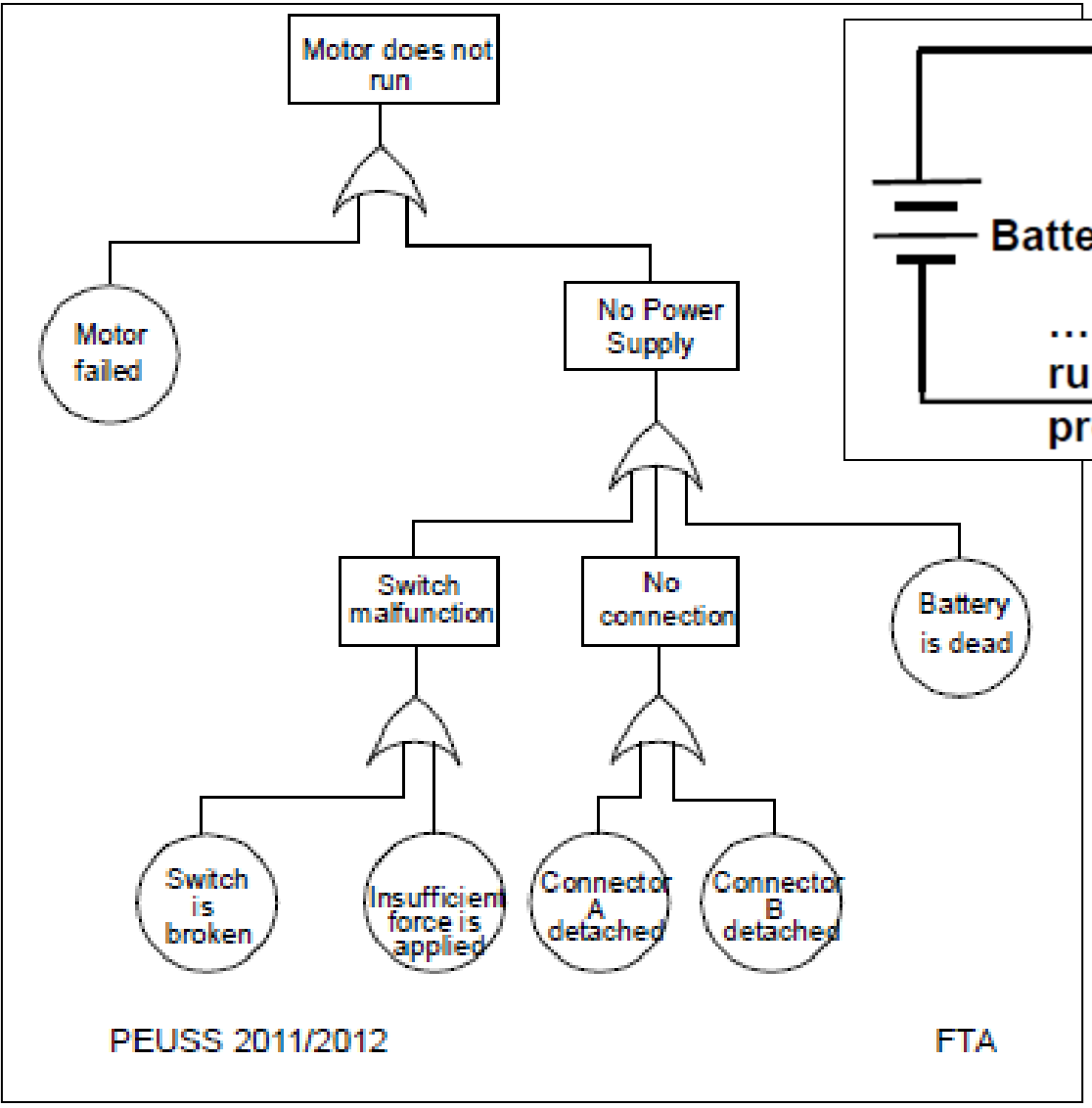


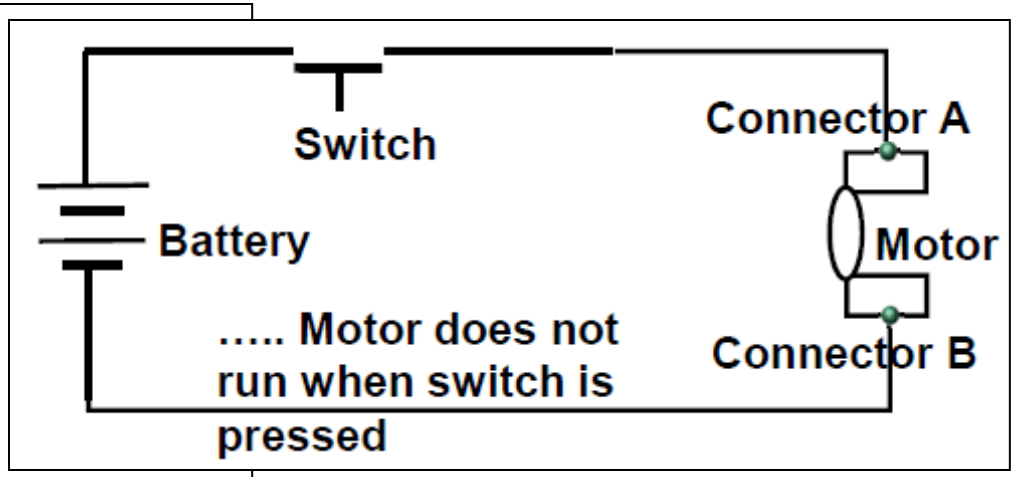

FAULT TREE ANALYSIS e.g. Fire Triangle
FIRE
&
FUEL
OXYGEN
IGNITION
OR
OR
Top Event
Intermediate Event
Basic Event

Fault tree Analysis



Motor does not run when switch is pressed





Fault Tree Analysis

- Fault tree analysis (FTA) is a **top-down** approach to failure analysis, starting with a potential undesirable event (accident) called a TOP event, and then determining all the ways it can happen.

- The analysis proceeds by determining how the Top event can be caused by individual or combined lower level failures or events.

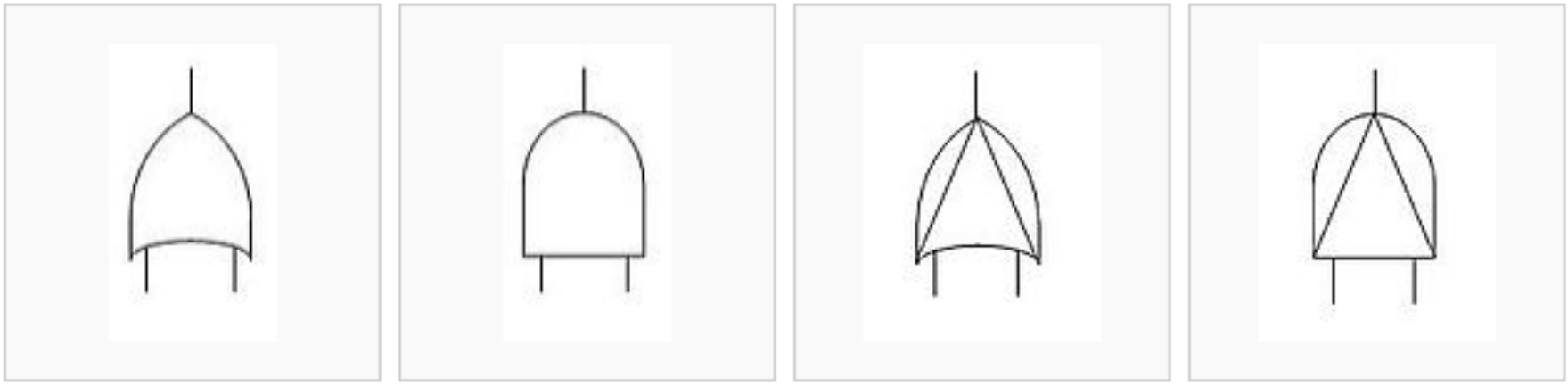
- The causes of the TOP event are “connected” through logic gates

Fault tree analysis

1. **An *undesired event* is defined**
2. **The event is resolved into its *immediate causes***
3. **This resolution of events continues until *basic causes* are identified**
4. **A logical diagram called a *fault tree* is constructed showing the logical event relationships**

- Fault trees originated in the aerospace industry and have been used extensively by the nuclear power industry to qualify and quantify the hazards and risks associated with nuclear power plants.

Gate Symbols



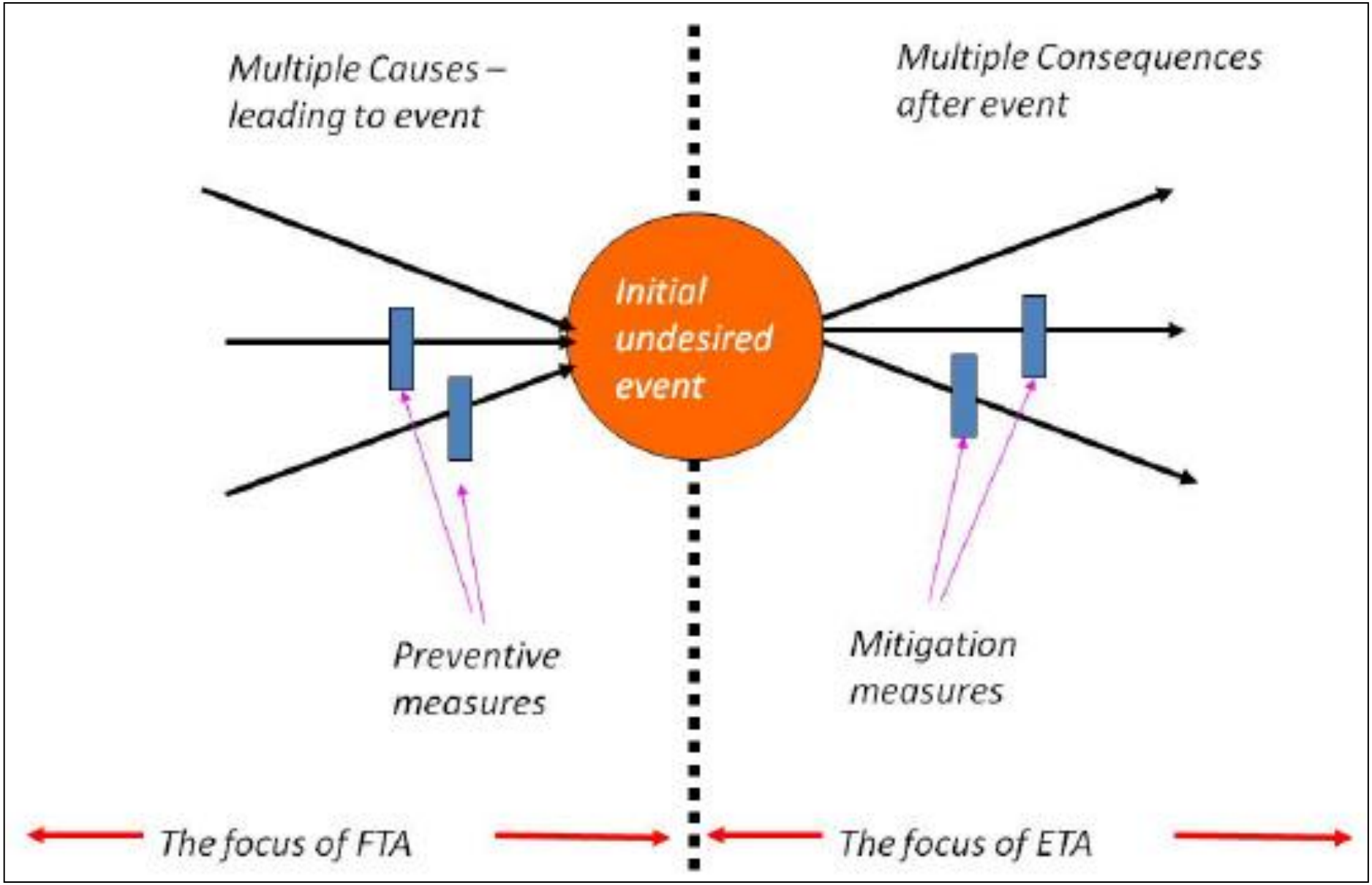
OR gate - the output occurs if any input occurs
AND gate - the output occurs only if all inputs occur (inputs are independent)
Exclusive OR gate - the output occurs if exactly one input occurs
Priority AND gate - the output occurs if the inputs occur in a specific sequence specified by a conditioning event

Add the probabilities which sit below an OR gate

Multiply the probabilities which sit below an AND gate

So, in this example, combining probabilities upwards to the next level gives:

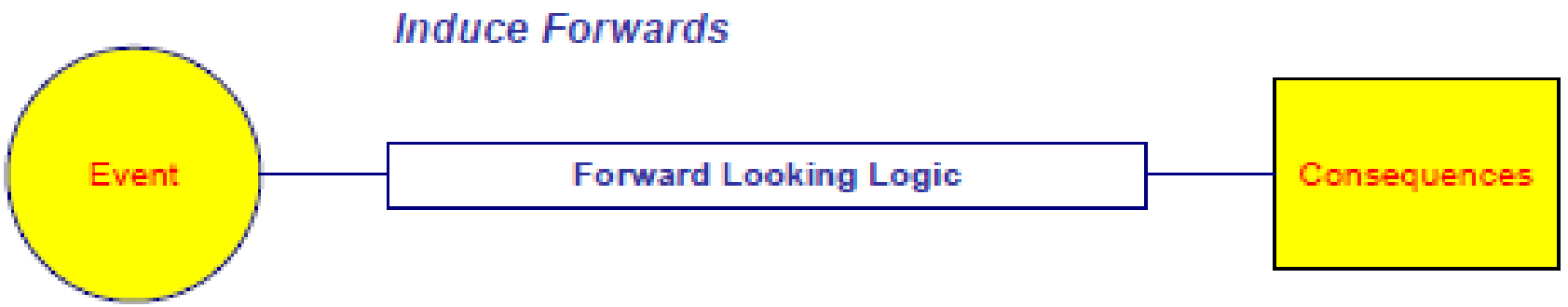
- Probability of FUEL being present = 0.1 + 0.02 + 0.09 = 0.21
- Probability of OXYGEN being present = 1
- Probability of IGNITION being present = 0.2 + 0.05 + 0.1 = 0.35


Multiple Causes – leading to event
Multiple Consequences after event
Initial undesired event
Preventive measures
Mitigation measures
The focus of FTA
The focus of ETA

Relationship between Fault Trees and Event Trees

- Event trees begin with an initiating event and work toward the top event (induction).
- Fault trees begin with a top event and work backward toward the initiating events (deduction).

Inductive models forwardly _induce_ the consequences of an event.



Deductive models backwardly _deduce_ the causes of an event.

FMEA (Failure mode Effect Analysis)

History of FMEA

- First used in the 1960's in the Aerospace industry during the Apollo missions
- In the late 1970's, the automotive industry was driven by liability costs to use FMEA
- Later, the automotive industry saw the advantages of using this tool to reduce risks related to poor quality

FMEA TERMS

- Failure mode - the way in which something might fail

- Effects analysis – studying the consequences of the various failure modes to determine their severity to the customer.

What is FMEA?

- **Failure modes and effects analysis (FMEA) is a step-by-step approach for identifying all possible failures in a design, a manufacturing or assembly process, or a product or service.**

OR

- **Failure Modes and Effects Analysis (FMEA) is a qualitative, systematic and highly structured technique that is used to investigate how a system or system components can result in performance problems.**

FMEA Procedure

1. For each process input (start with high value inputs), determine the ways in which the input can go wrong (failure mode)
2. For each failure mode, determine effects
   - Select a severity level for each effect
3. Identify potential causes of each failure mode
   - Select an occurrence level for each cause
4. List current controls for each cause
   - Select a detection level for each cause

FMEA Procedure (Cont.)

5. Calculate the Risk Priority Number (RPN)
6. Develop recommended actions, assign responsible persons, and take actions
   - Give priority to high RPNs
   - MUST look at severities rated a 10
7. Assign the predicted severity, occurrence, and detection levels and compare RPNs

FMEA Form (Template)

Process/Product
Failure Modes and Effects Analysis Form
(FMEA)

Process or Product Name:	
Responsible:	

Prepared by:	Page ___ of ___
FMEA Date (Orig) _____ (Rev) _____	

Process Step / Input	Potential Failure Mode	Potential Failure Effects	SEVERITY	Potential Causes	OCCURRENCE	Current Controls	DETECTION	RPN	Actions Recommended	Resp.	Actions Taken	SEVERITY	OCCURRENCE	DETECTION	RPN
What is the process step and Input under investiga-tion?	In what ways does the Key Input go wrong?	What is the impact on the Key Output Variables (Customer Requirements)?		What causes the Key Input to go wrong?		What are the existing controls and procedures (inspection and test) that prevent either the cause or the Failure Mode?			What are the actions for reducing the occurrence of the cause, or improving detection?		What are the completed actions taken with the recalculated RPN?				
								0							0
								0							0
								0							0
								0							0
								0							0

Identify failure modes and their effects

Identify causes of the failure modes and controls

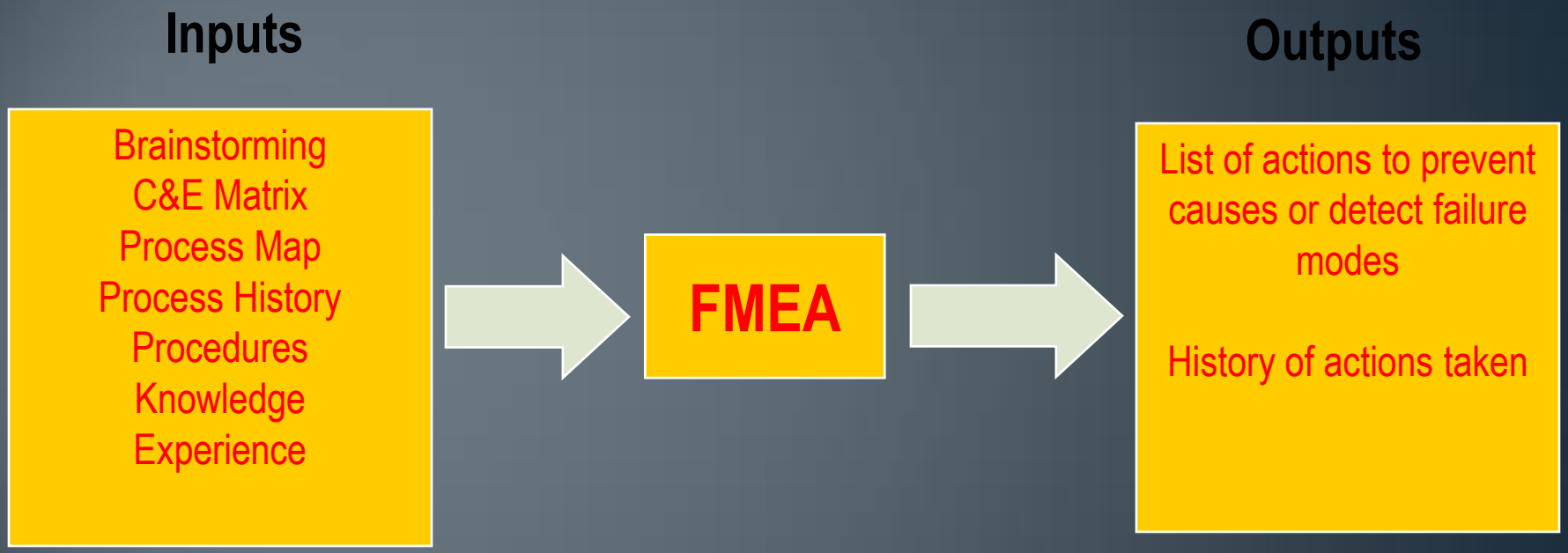
Prioritize

Determine and assess actions

Failure Mode	Specific Cause	Effect of Failure	Likeliness of Failure	Detectability of Failure	Severity of Failure	Risk Priority
Gas will not shut off	Spring broke preventing valve from closing	Explosion resulting in property damage and/or serious injury	3	5	10	150

- Likeliness of Failure: *1-10 with 10 representing most likely*
- Detectability of Failure: *1-10 with 10 representing most difficult*
- Severity of Failure: *1-10 with 10 representing most severe*
- Risk Priority = *(Likeliness of Failure) X (Detectability of Failure) X (Severity of Failure)*

FMEA INPUTS AND OUTPUTS



Likelihood of Occurrence Rank List

Rank of Likelihood of Occurrence	Description
1	*Never Happened*
2-3	*1 in 365 days*
4-5	*1 in 220 days*
6-7	*1 in 180 days*
8-9	*1 in 100 days*
10	*<30 days*

Severity Rank List (Failures)

Rank of Severity	Description
1	*Failure would not be noticed*
2-3	*Failure causes in nuisances but no performance losses*
4-5	*System under minor performance losses*
6-7	*System Inoperable or Unserviceable*
8-9	*Partial Breakdown of the system. System can be repaired*
10	*Complete Breakdown of the system*

Detection Rank List

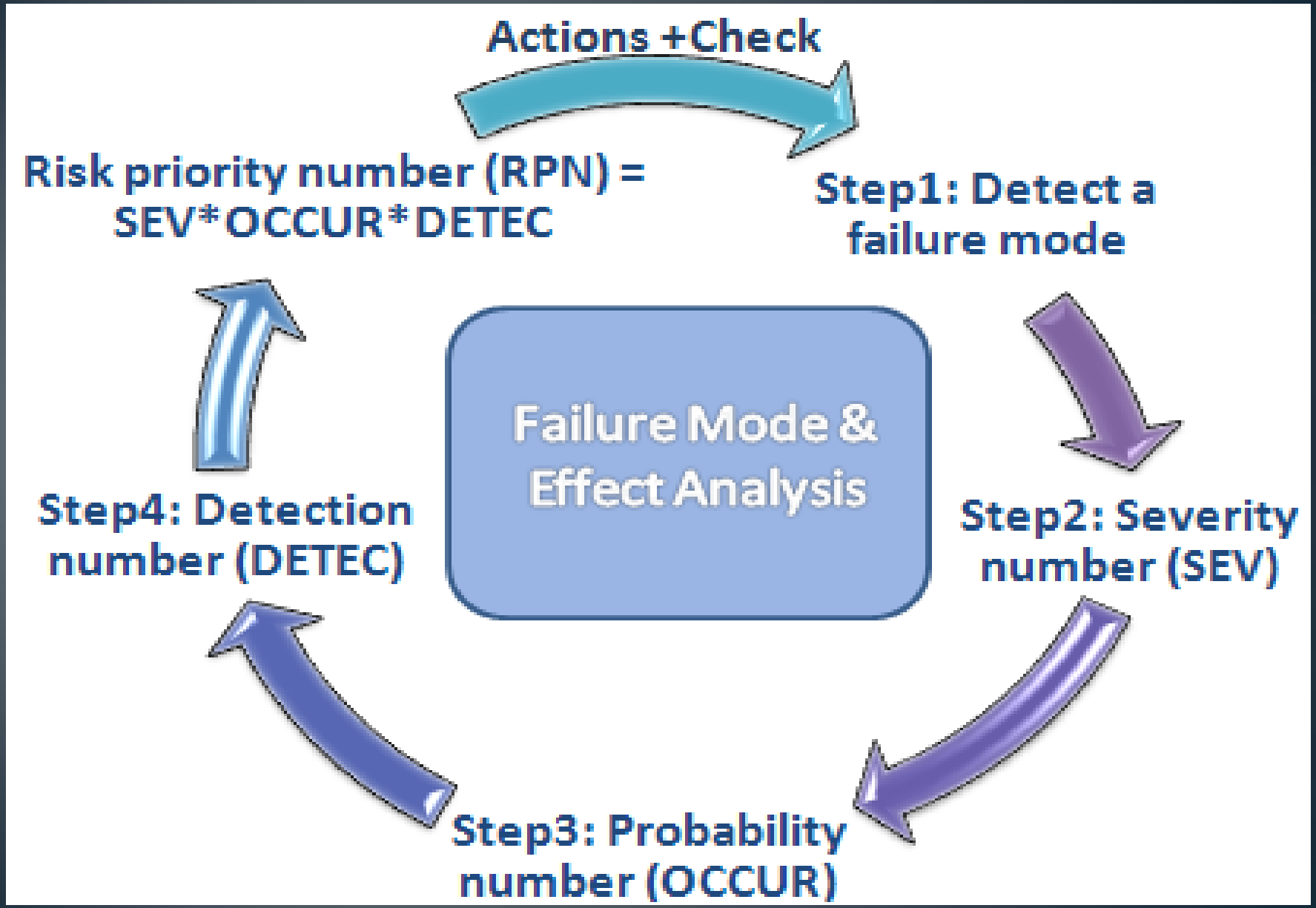
Rank of Detection	Description
1	*Online Detection & Automatic Response System*
2-4	*Online Detection & Manual Response System*
5-6	*Periodic Physical/ Manual Detection & Manual Response System*
7-8	*Random Physical/ Manual Detection & Manual Response System*
9-10	*No Detection & Manual System*

Risk Priority Number (RPN)

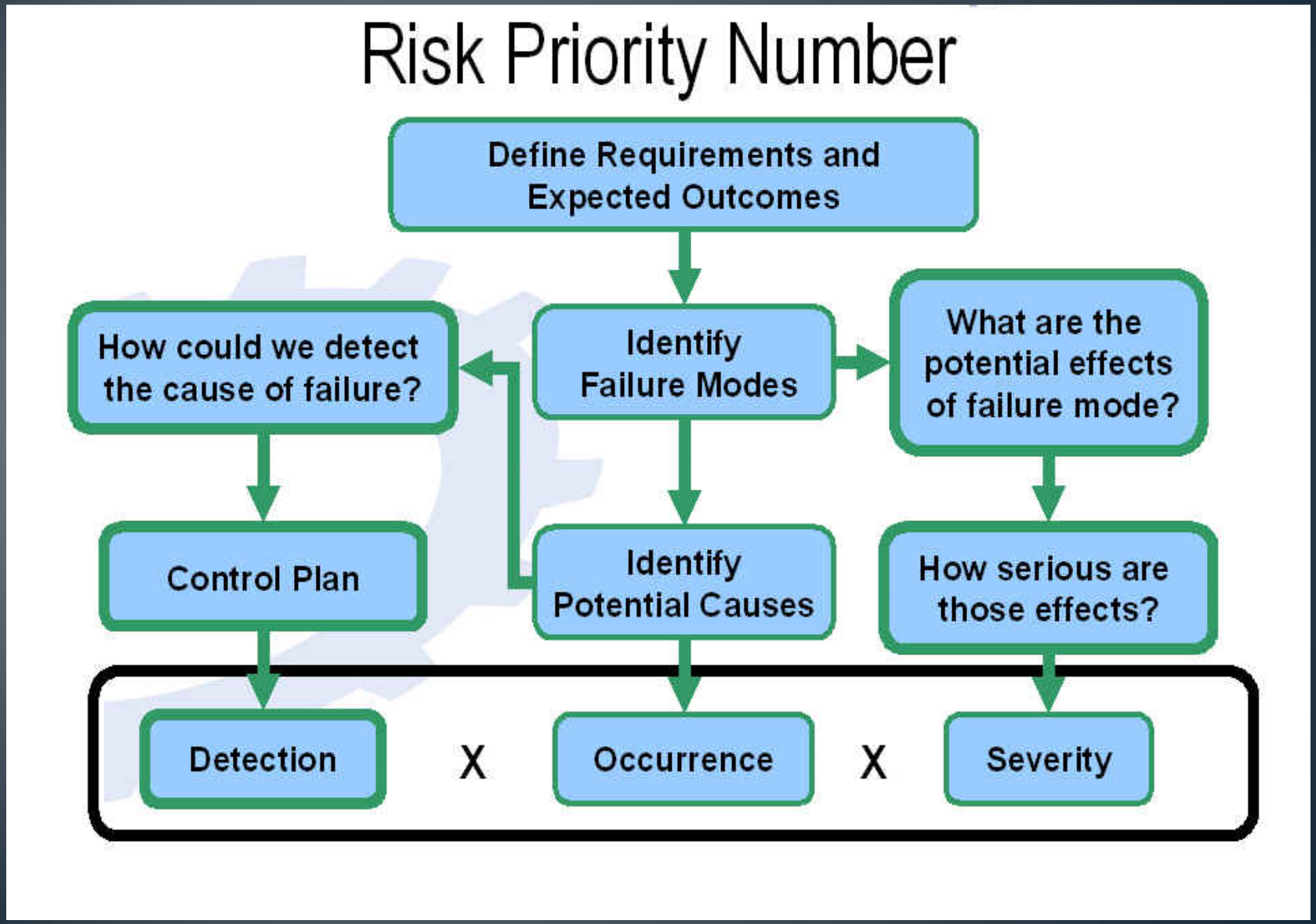
Risk Priority Number (RPN): The failure mode's risk is found by the formula RPN = S x O x D.

RPN = Severity x Probability of Occurrence x Probability of Detection.

RPN will be a number between 1 (virtually no risk) and 1000 (extreme risk).


Actions +Check
Risk priority number (RPN) = SEV*OCCUR*DETEC
Step1: Detect a failure mode
Failure Mode & Effect Analysis
Step4: Detection number (DETEC)
Step2: Severity number (SEV)
Step3: Probability number (OCCUR)

RISK PRIORITY NUMBER



TYPES of FMEAs

- Design
  - Analyzes product design before release to production, with a focus on product function.
  - Analyzes systems and subsystems in early concept and design stages.
- Process
  - Used to analyze manufacturing and assembly processes after they are implemented.
  - It is used either in the assembly or manufacturing or both.

WHEN TO DO FMEA?

- New process being designed.
- New equipment developed or purchased.
- Existing process being designed or redesigned.
- To monitor and track improvement over time.

BENEFITS OF FMEA

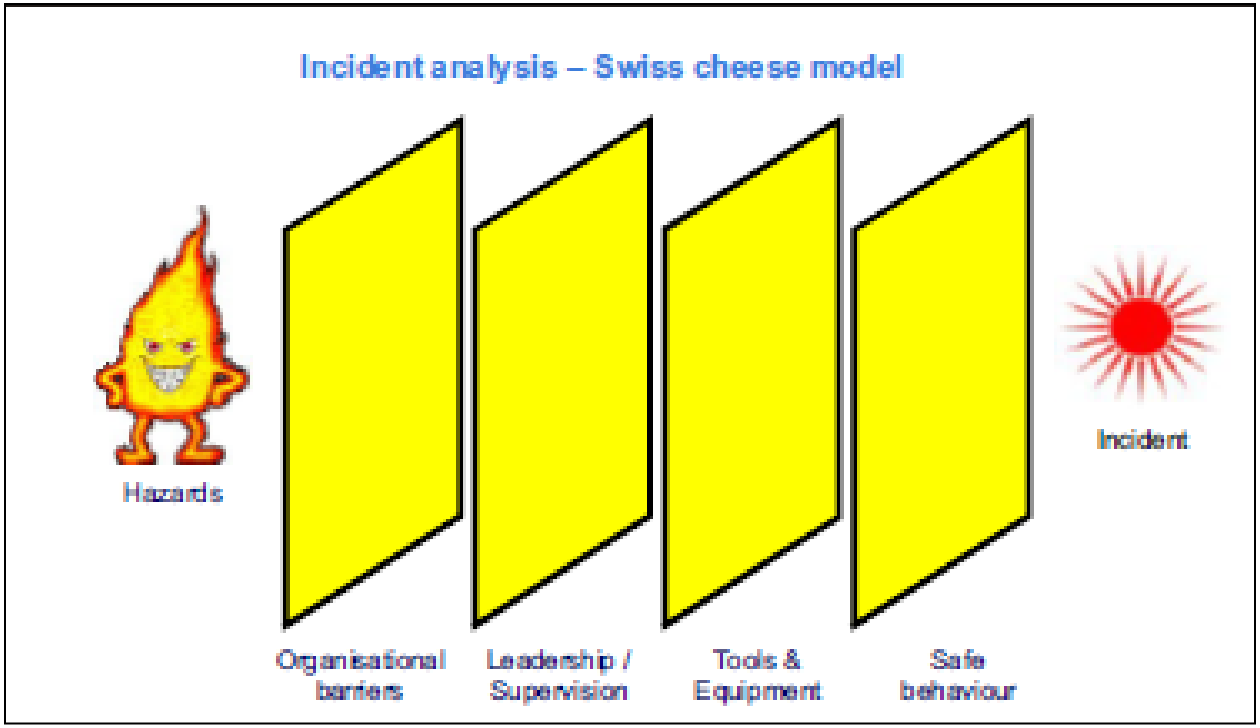
- Improve the quality, reliability and safety of a product/process.
- Improve company image and competitiveness.
- Increase user satisfaction.
- Reduce system development timing and cost.
- Collect information to reduce future failures, capture engineering knowledge.
- Reduce the potential for warranty concerns.
- Early identification and elimination of potential failure modes
- Emphasize problem prevention.
- Minimize late changes and associated cost.
- Catalyst for teamwork and idea exchange between functions.
- Reduce the possibility of same kind of failure in future.
- Reduce impact of profit margin company.
- Reduce possible scrap in production.

LIMITATIONS OF FMEA

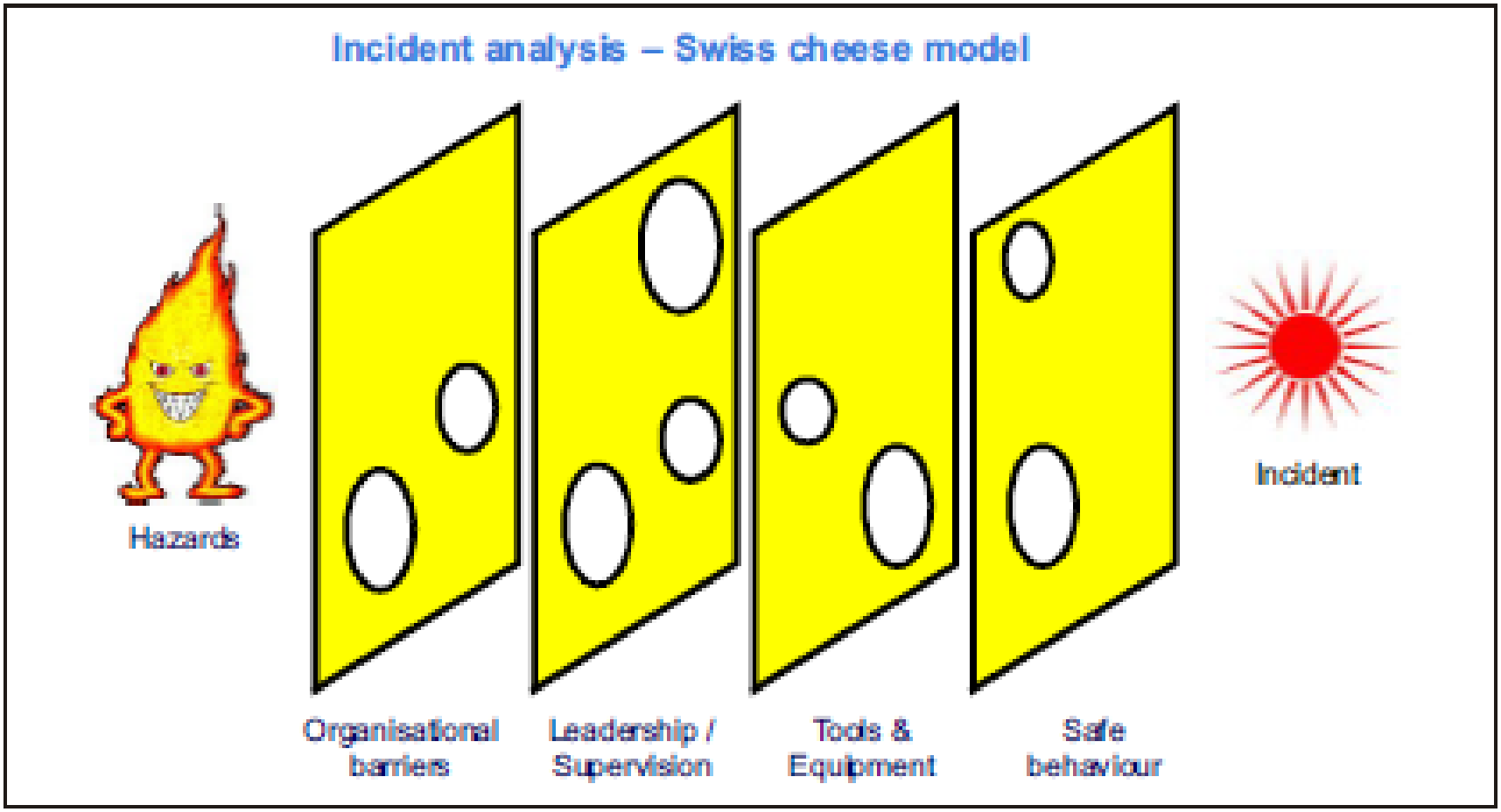
- Employee training requirements
- Initial impact on product and manufacturing schedules.
- Financial impact required to upgrade design, manufacturing, and process equipment and tools.

BOW TIE ANALYSIS

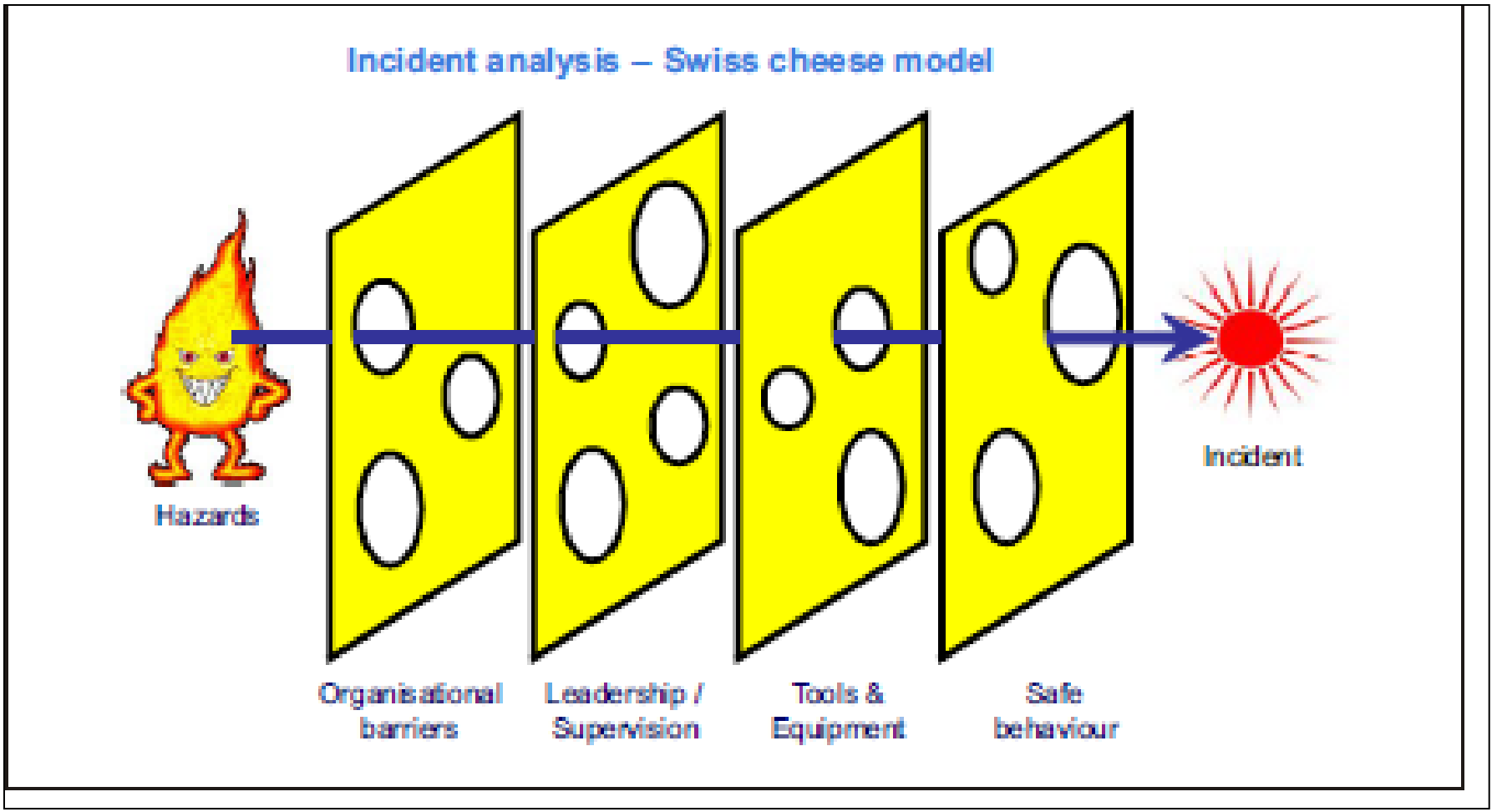
By linking ‘Hazards’ & ‘Consequences’ to an ‘Event’ it is possible to develop the relationship to include the causes, or ‘Threats’, and the ‘Prevention’ & ‘Recovery Measures



There is only an event when humans come into contact with a hazard. But there are many ways this contact can be prevented. Organisational barriers such as permits and Safe working procedures and standards. Leaders and supervisors who provide guidance and ensure procedures are followed



The problem is that none of these barriers is 100 percent safe, all of them have holes – big or small



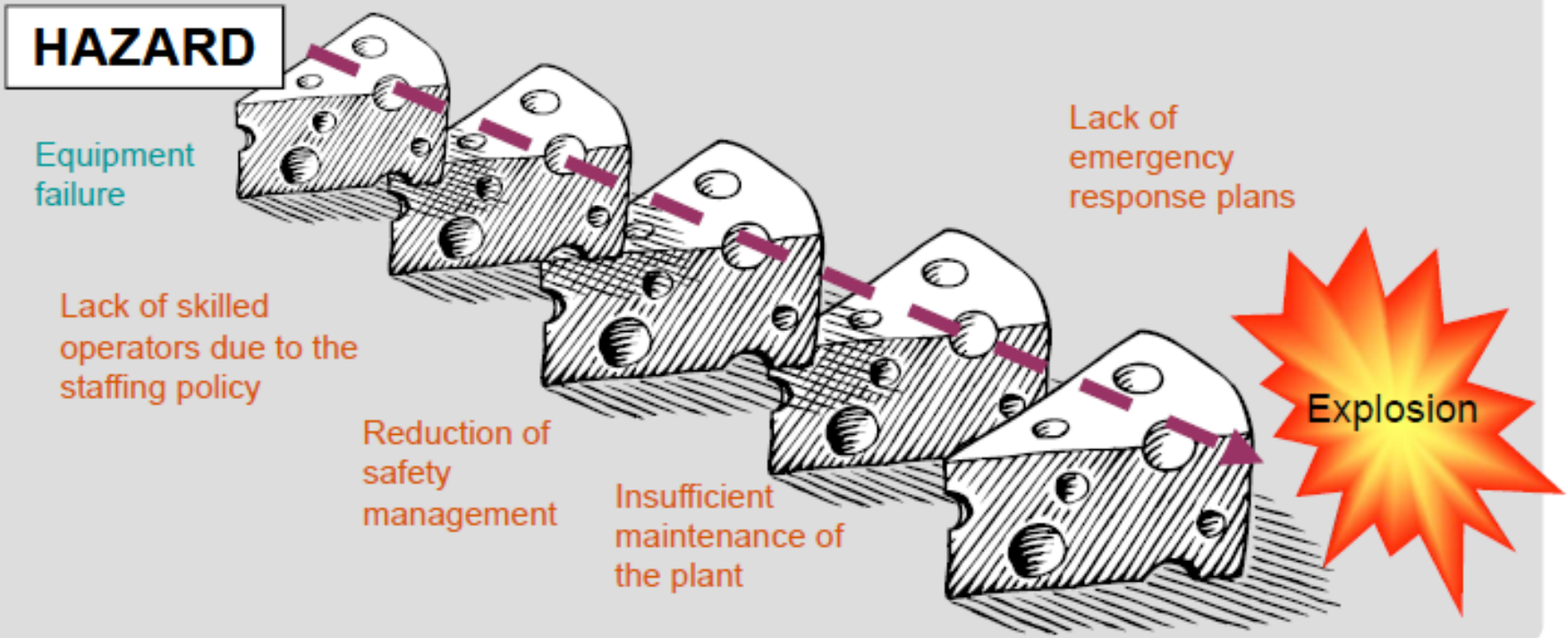
The holes all line up and at this point there is an event sometimes causing an injury.

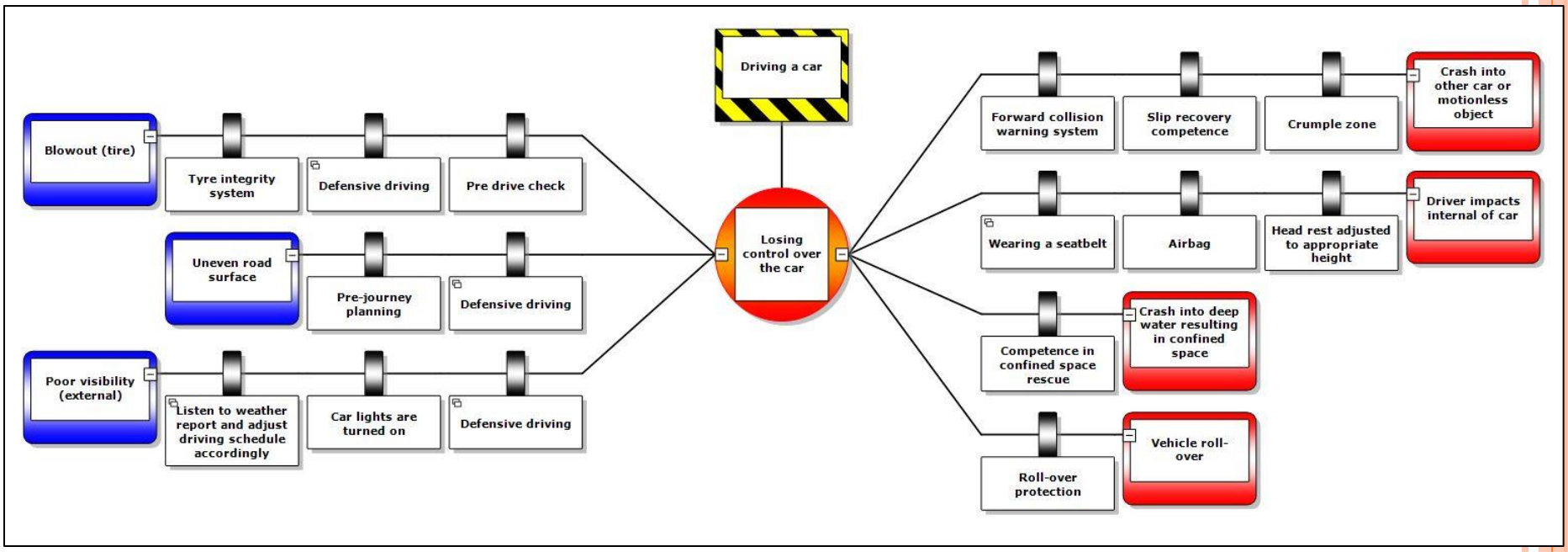
However as long as one barrier is working effectively, even when the others fail an individual will be protected (it will be a near miss)

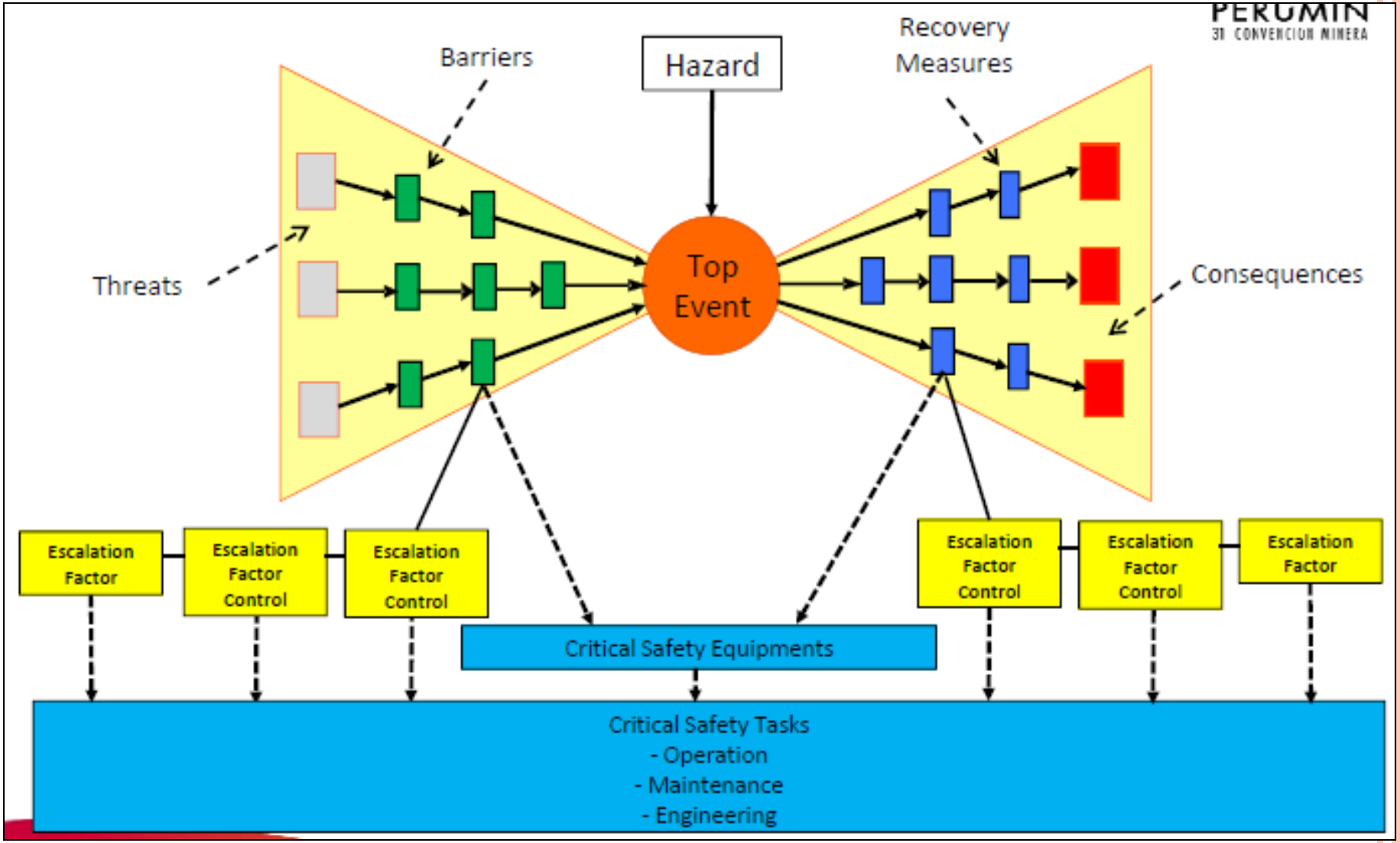
Swiss chesse Model

Case Study – Bhopal Disaster in India

- Equipment failure happened just before the incident was not the only cause of the incident



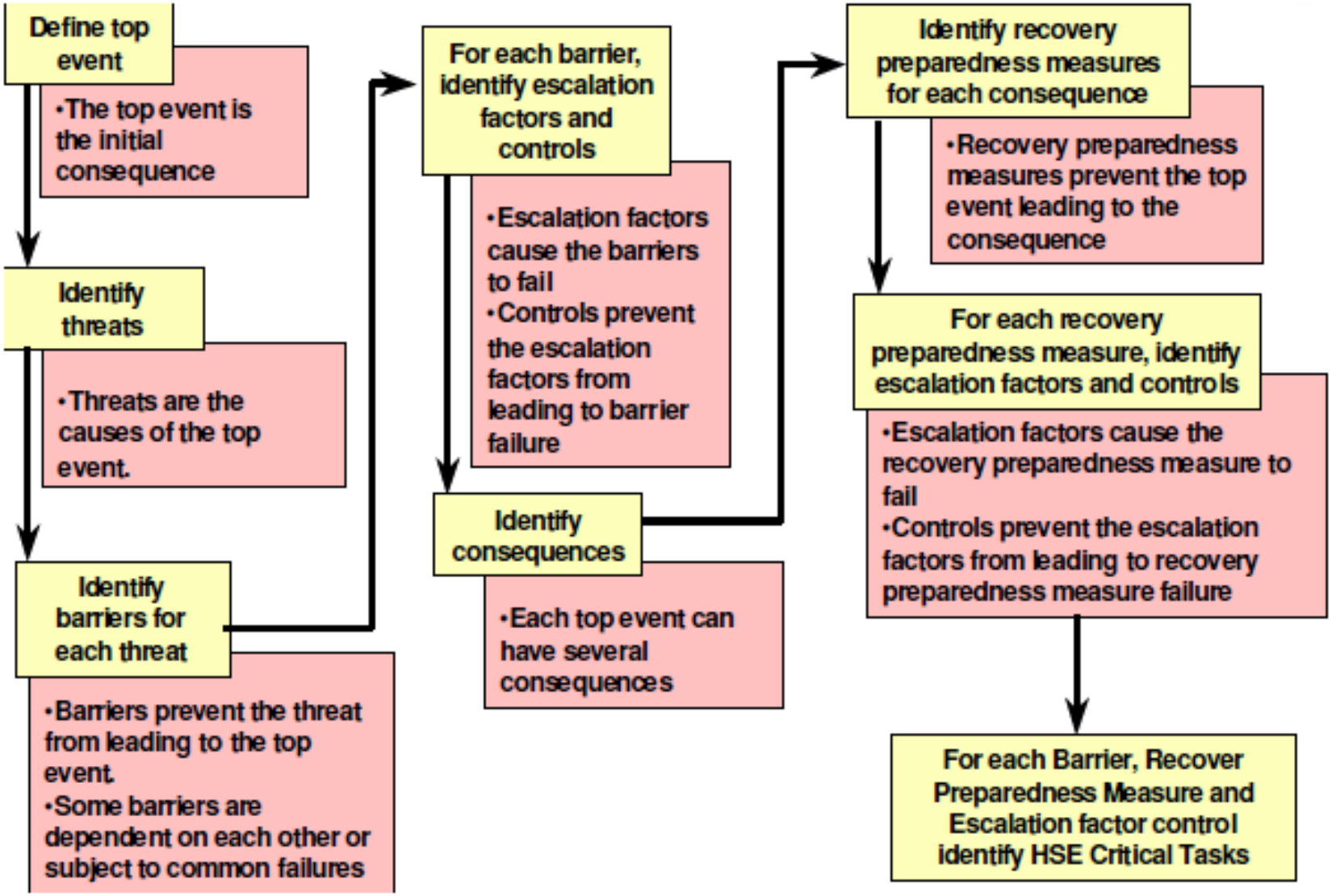

Driving a car
Losing control over the car
Blowout (tire)
Tyre integrity system
Defensive driving
Pre drive check
Uneven road surface
Pre-journey planning
Defensive driving
Poor visibility (external)
Listen to weather report and adjust driving schedule accordingly
Car lights are turned on
Defensive driving
Forward collision warning system
Slip recovery competence
Crumple zone
Crash into other car or motionless object
Wearing a seatbelt
Airbag
Head rest adjusted to appropriate height
Driver impacts internal of car
Competence in confined space rescue
Crash into deep water resulting in confined space
Roll-over protection
Vehicle roll-over


PERUMIN
31 CONVENCION MINERA
Barriers
Hazard
Recovery Measures
Threats
Top Event
Consequences
Escalation Factor
Escalation Factor Control
Escalation Factor Control
Escalation Factor Control
Escalation Factor Control
Escalation Factor
Critical Safety Equipments
Critical Safety Tasks
- Operation
- Maintenance
- Engineering

Bow Tie Terminology Definitions

- **Hazard** - Potential source of harm to people, assets, the environment and company reputation
- **Top Event** - The incident that occurs when a hazard is realized
- **Threats** - What could cause the top event to occur?
- **Consequences** - What could happen if the top event occurs?
- **Barrier** - What directly prevents or reduces the likelihood of a threat?
- **Recovery Measure** - What prevents, minimizes or helps recovery from the consequence?
- **Escalation Factor** - What could prevent the barrier or recovery measure from working as intended?
- **Escalation Factor Control** - What prevents or minimizes the chance of barriers or recovery measures becoming Ineffective?

Bow Tie Analysis Steps



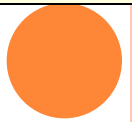
Typical Major Hazard Barriers

- Structures (jackets/decks) – preventive barriers
- Hydrocarbon containment - preventive barriers
- Chemical injection systems - preventive barriers
- Relief systems - preventive barriers
- Fire, gas & smoke detectors – recovery barriers
- Ignition control – recovery barriers
- Shutdown systems – preventive/ recovery barriers
- Active & passive fire protection systems – recovery barriers
- Firewater pumps & ringmain – recovery barriers
- Emergency response equipment – recovery barriers
- Emergency communication & power – recovery barriers
- Escape, evacuation & rescue provisions – recovery barriers
- Life/survival equipment – recovery barriers

Quantitative vs. qualitative risk analysis

- Identify all hazards
- Select a large set of scenarios
- Determine the expected frequency (likelihood) of all these scenarios
- Determine the consequences of all these scenarios
- Combine all these results (using wind direction statistics, etc) and calculate Individual Risk around the plant
- Draw Individual Risk on map and compare with acceptance criteria

- Identify all hazards
- Select a small set of scenarios with the largest consequences
- Obtain some "feel" for the likelihood of these scenarios
- Determine the consequences of these scenarios
- Draw safety distances on a map



Qualitative=Consequence-based: advantages and disadvantages

- Analysis is (relatively) easy and fast
- Decision process is simple (either “safe” or “unsafe”)
- Results are easy to communicate (based on easy-to-understand accident scenarios)
- Selection of scenarios and assessment of ”improbable = (?) impossible” accidents is often tacit or implicit.
- Can give a wrong impression of precision and safety
- Use of “worst case” scenarios leads to conservative results (expensive for society) (Results are determined by the worst-case – but unlikely accidents)
- Tendency to “forget” less severe scenarios in risk control and safety management

QRA=risk based: advantages and disadvantages

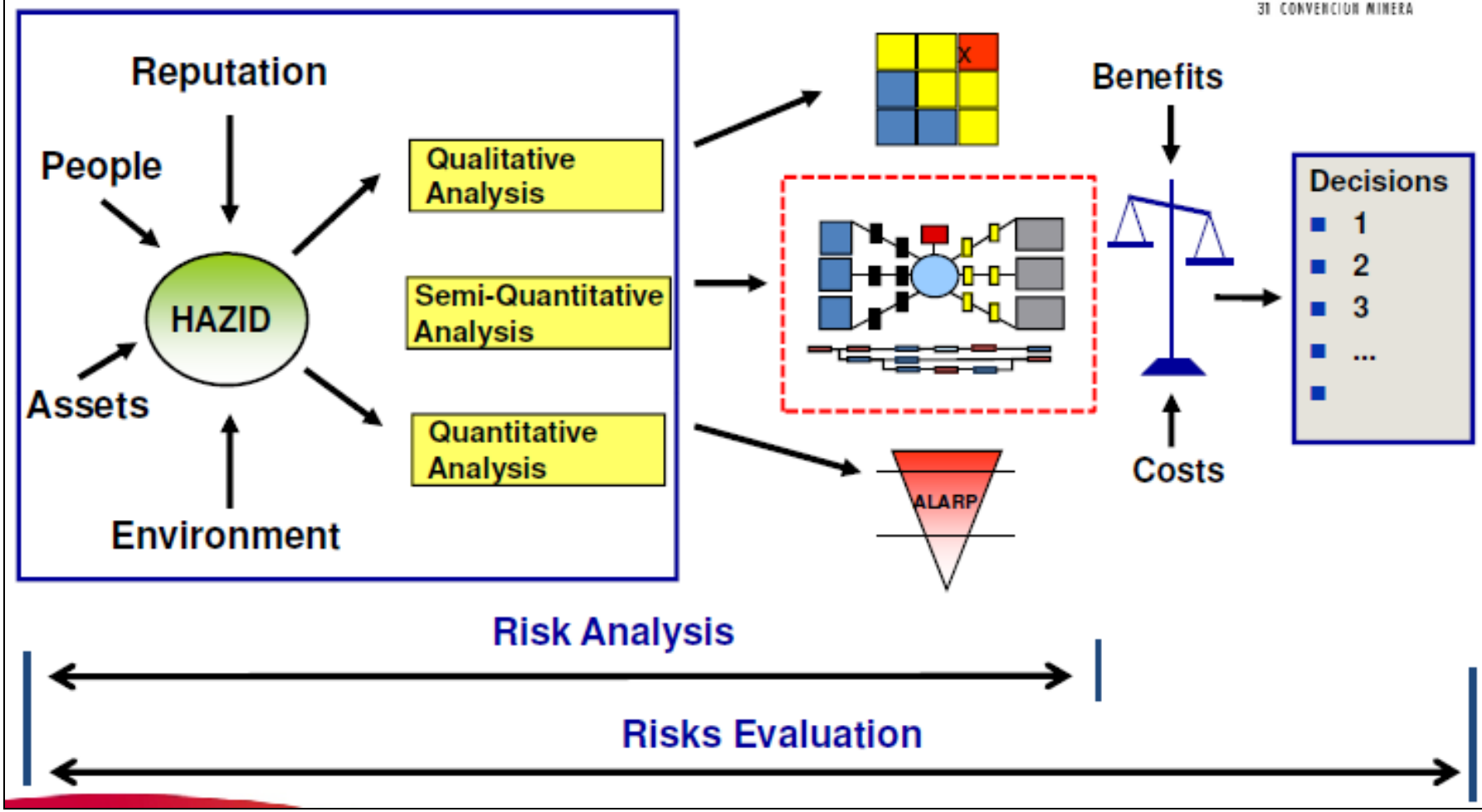
- Complete analysis, opportunity for setting priorities, focus on most “risky” items.
- Transparent (for experts?), both probabilities and consequences are included explicitly
- Results can be compared with criteria for risk acceptance
- Results for different types of facilities can easily be compared
- Not dominated by a single accident scenario – not sensitive for selection of scenarios

- Expensive and cumbersome analysis, which requires expert knowledge
- The ”probabilistic” element in the result is hard to communicate
- Result suggests large accuracy, but it includes large uncertainty
- The presence of accept criteria (hard political decision) is necessary beforehand

INSTITUTO DE INGENIEROS DE MINAS DEL PERÚ

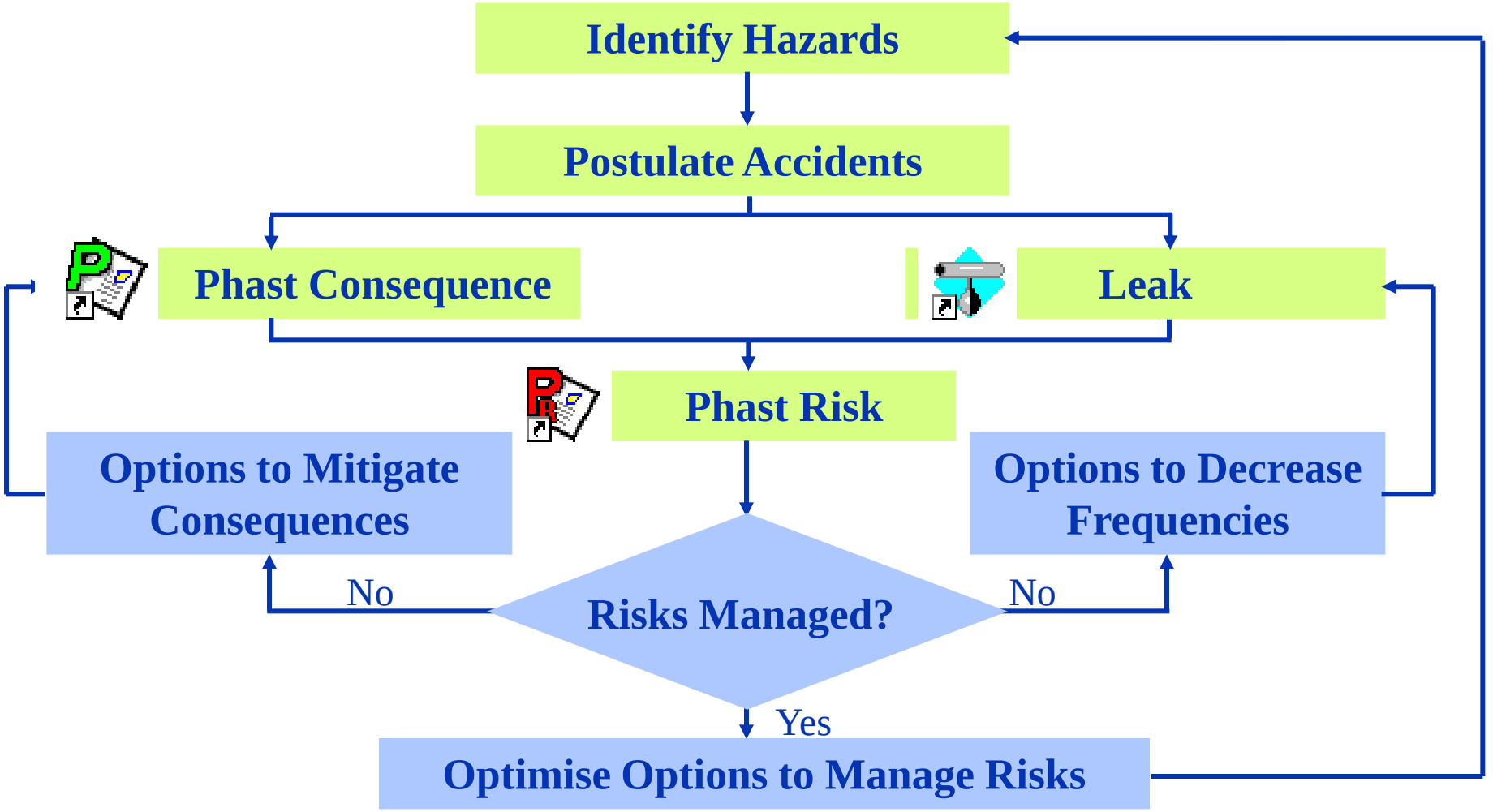
Risk Analysis and Assessment

PERUMIN 31 CONVENCION MINERA

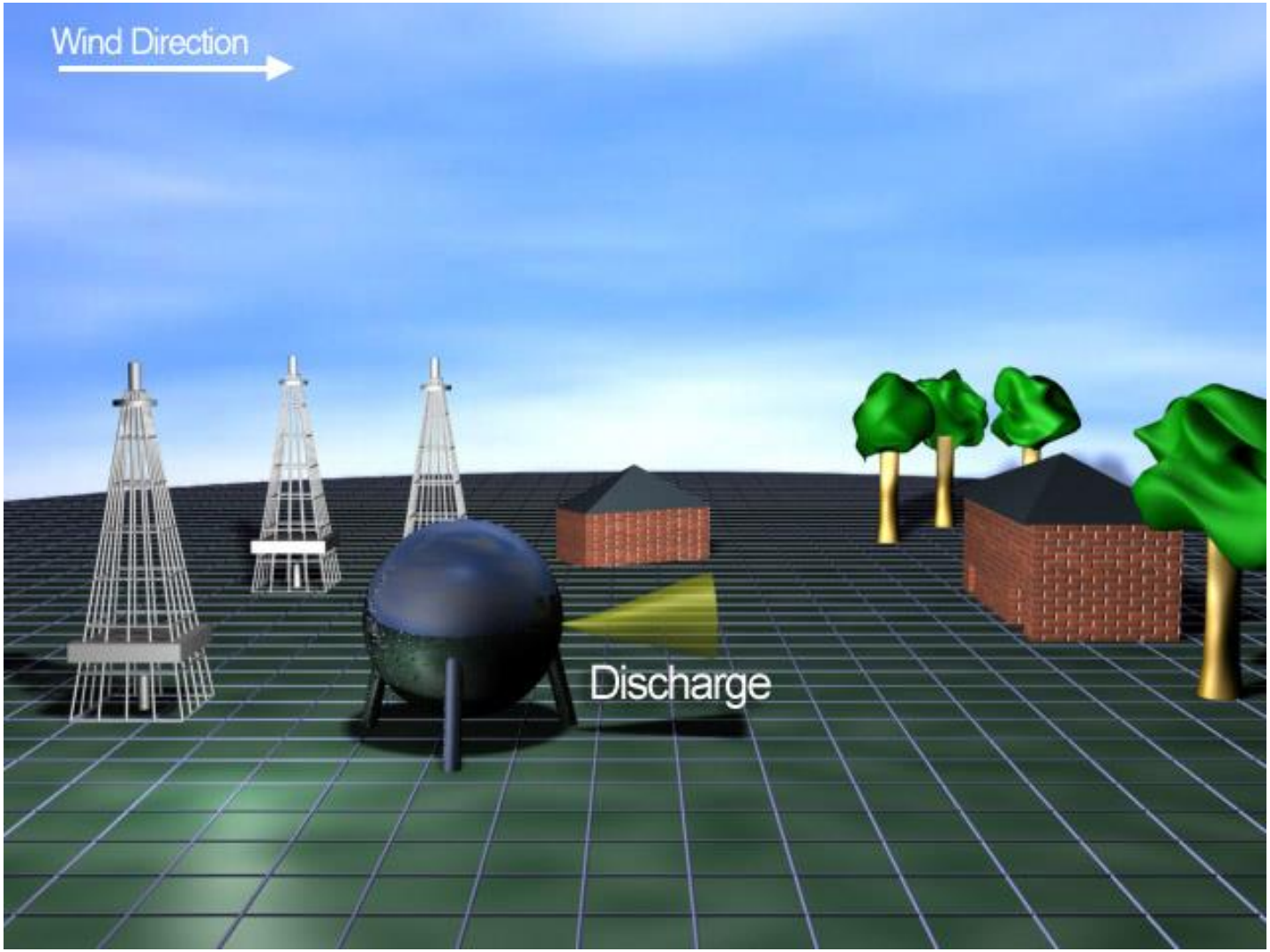


PHAST Software

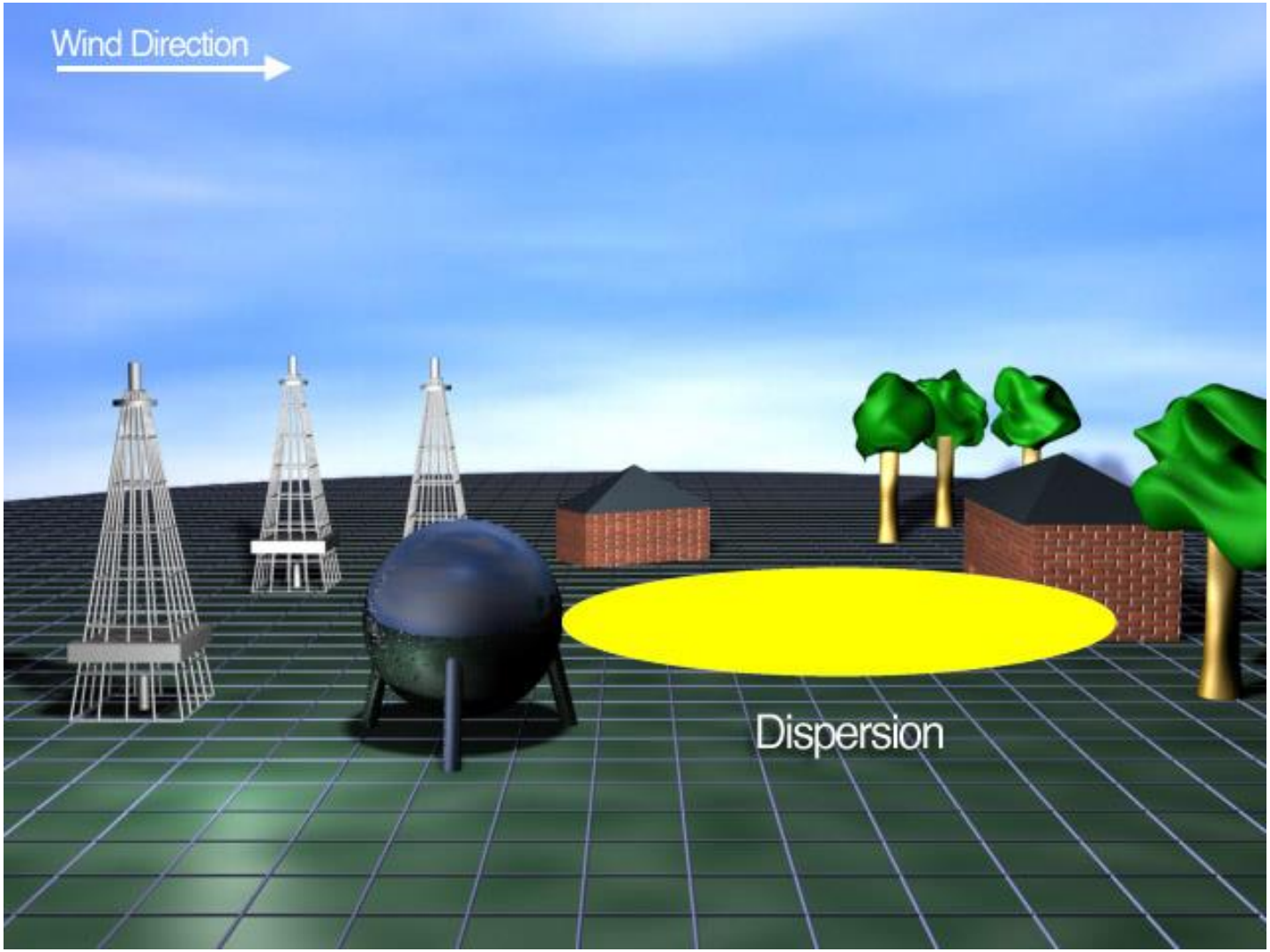
Safeti Risk Management Tools



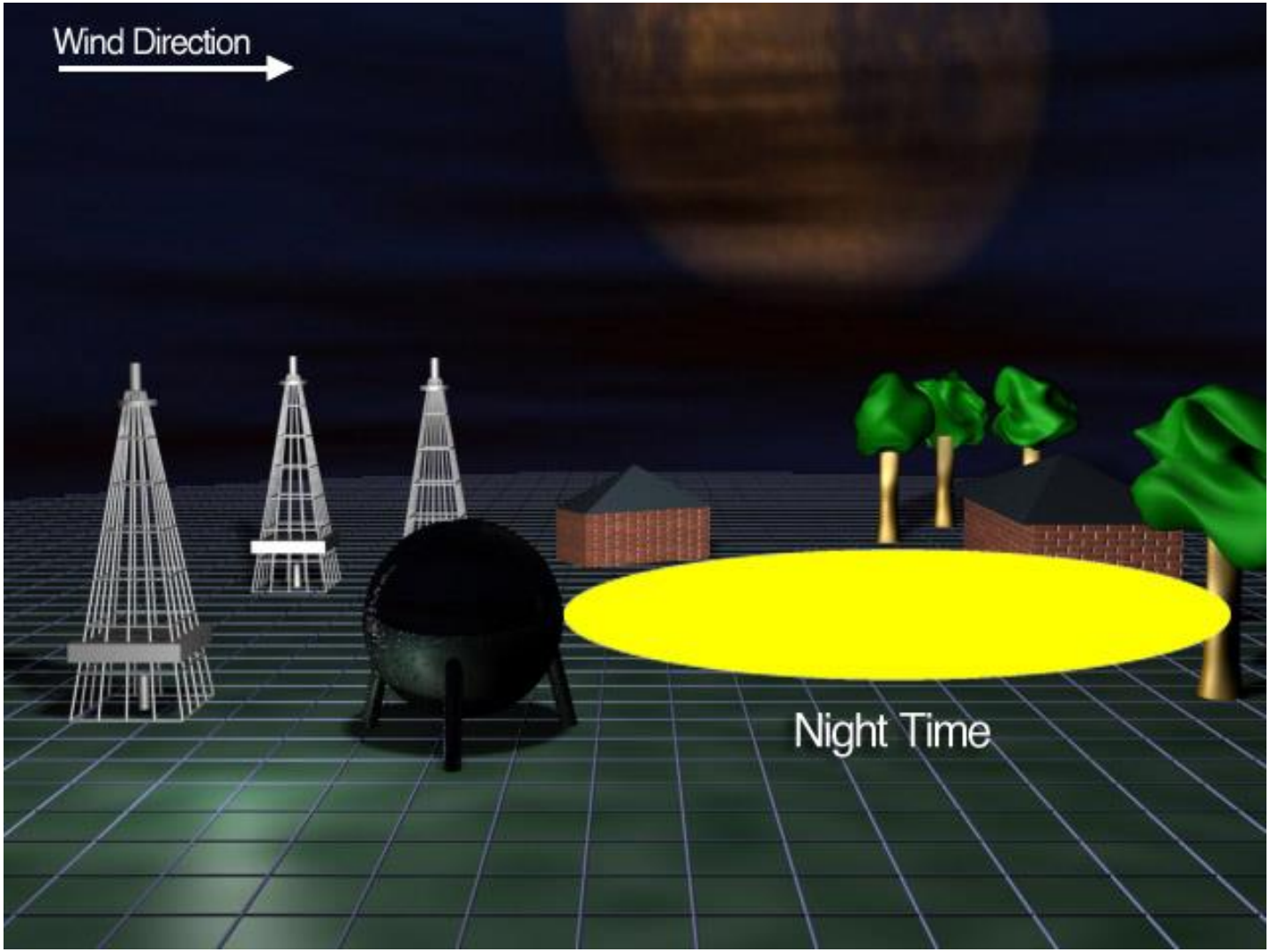
Consequence Calculations - Discharge



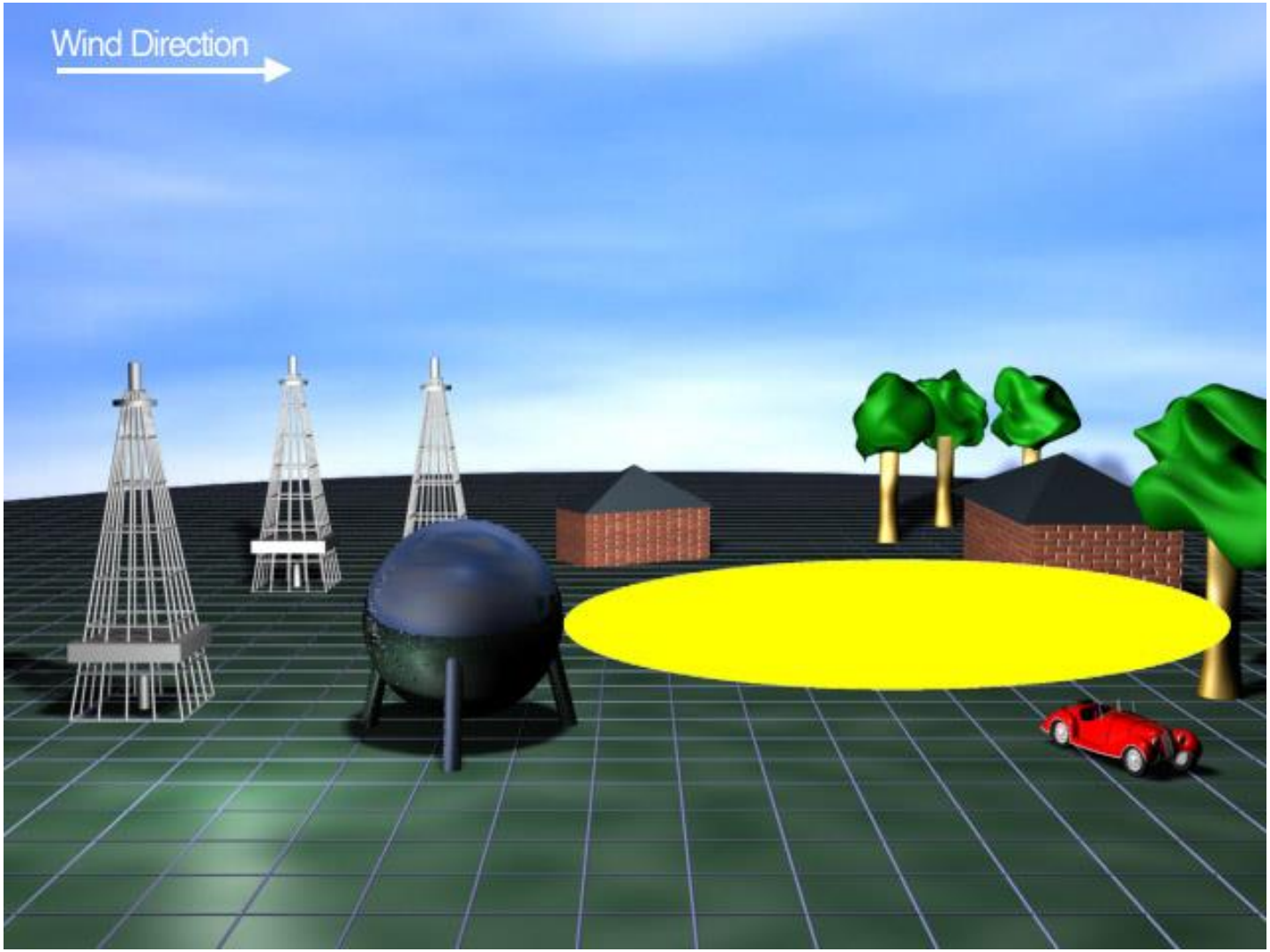
Consequence Calculations - Dispersion



Consequence Calculations - Dispersion

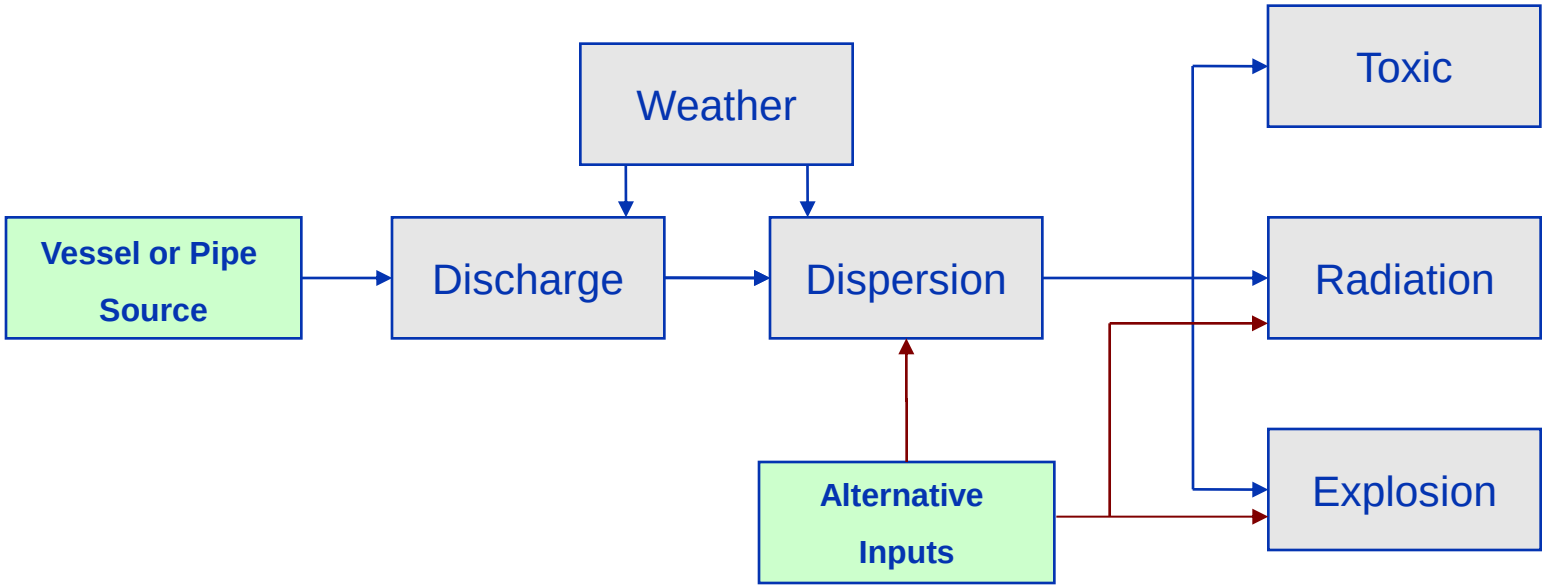


Consequence Calculations - Impact

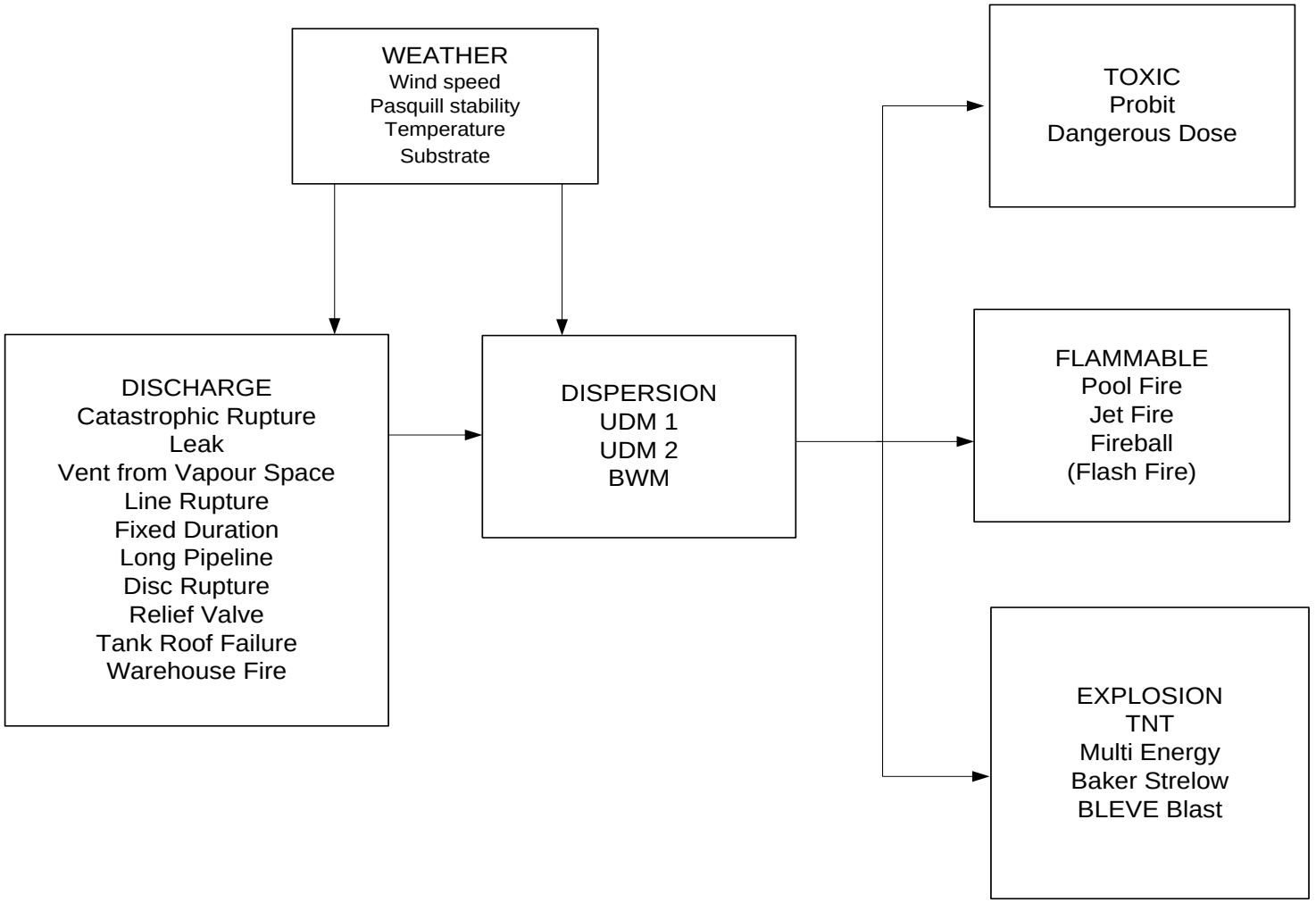


Phast Overview

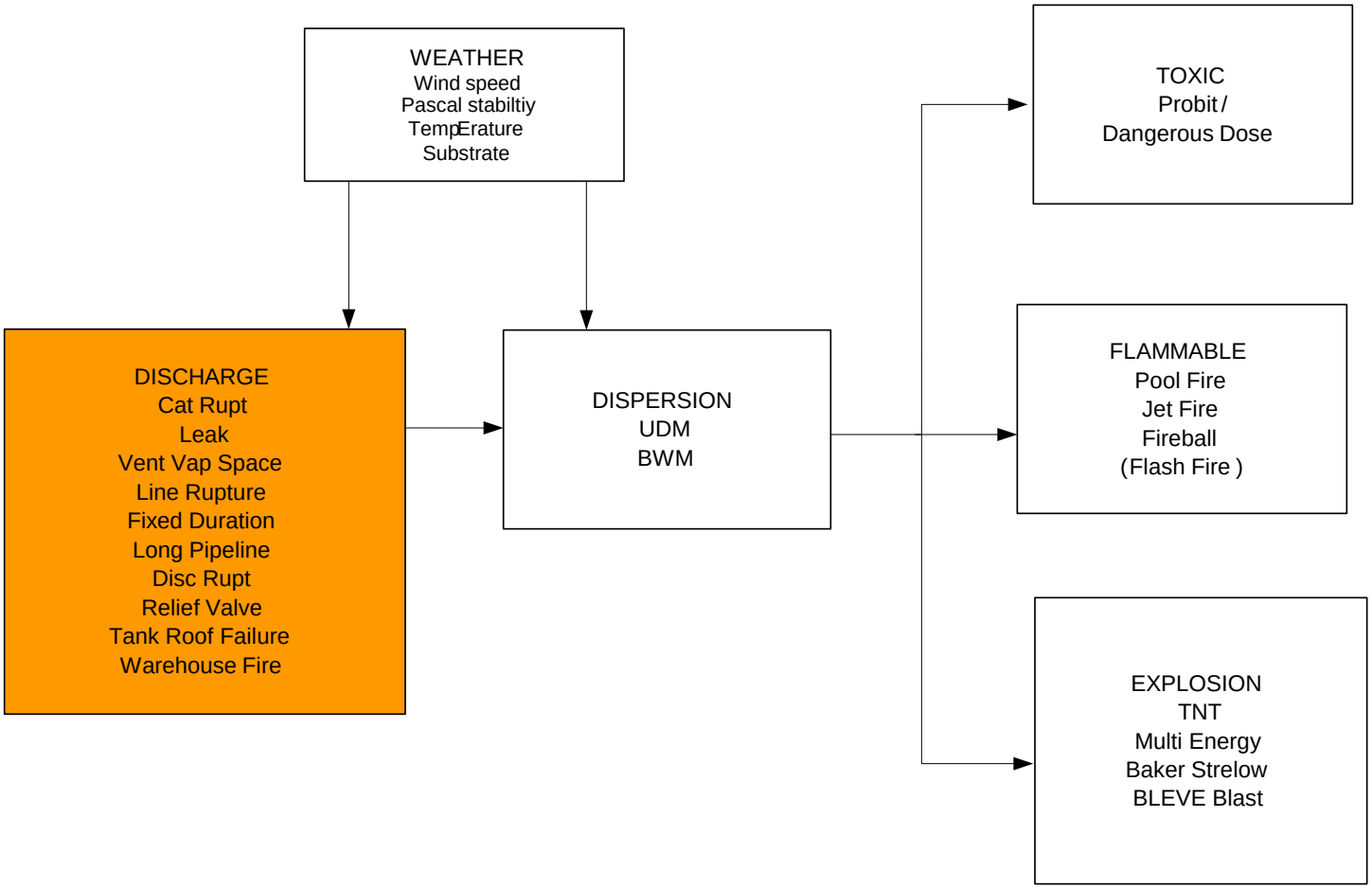
- This is the overall model path through Phast Consequence



Overview of models

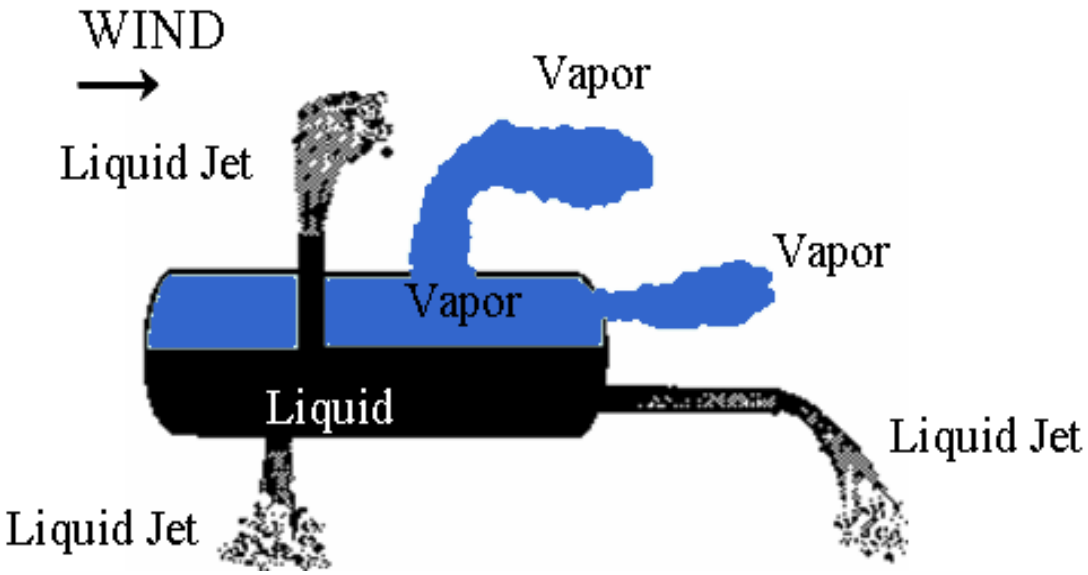


Discharge Models



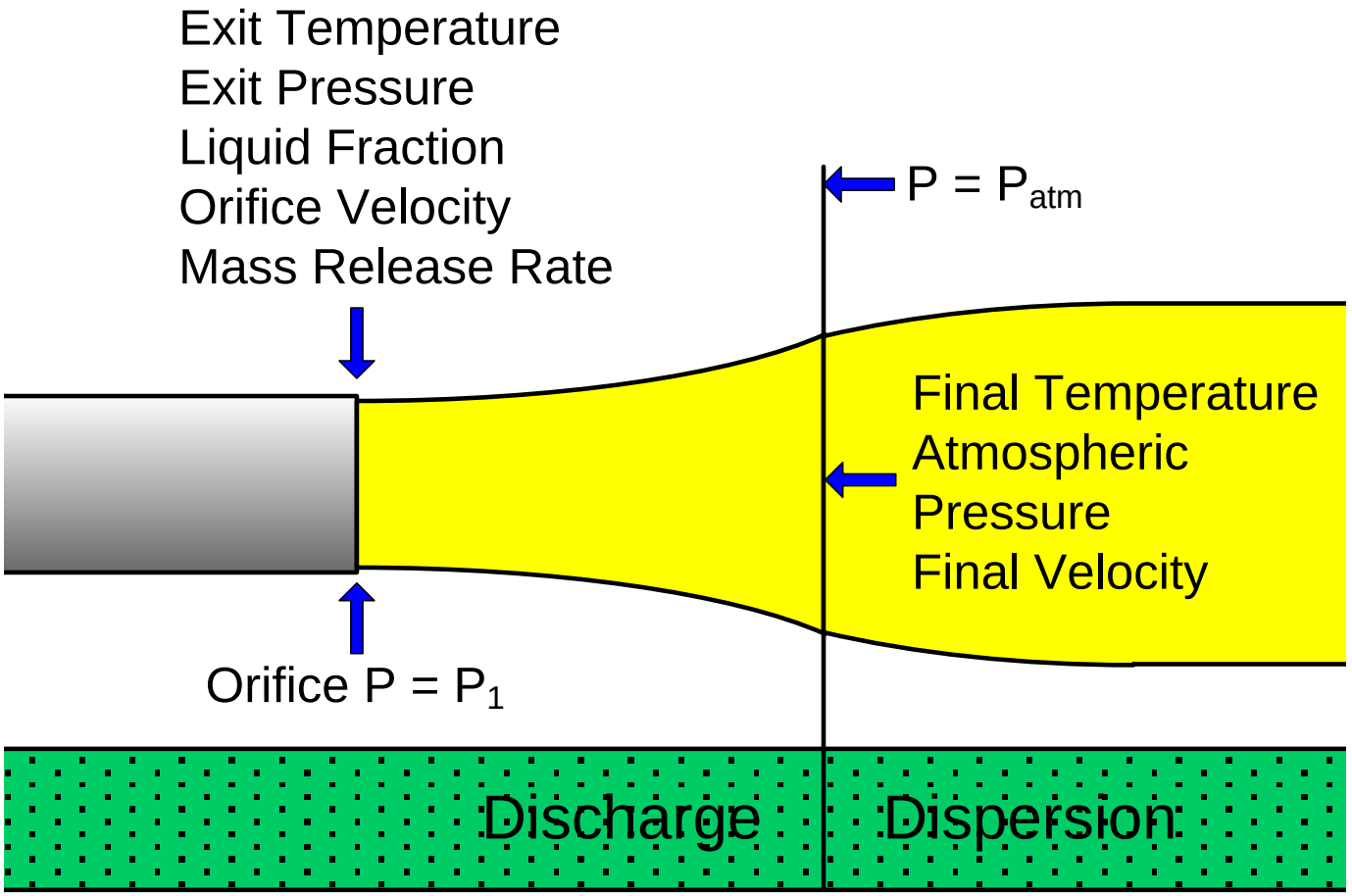
Direction and Phase

- Depending on the release material and physical conditions, Phast offers release phase options:
  - Liquid
  - Vapor
  - Two-phase
- Phast offers directional options:
  - Horizontal
  - Angled from Horizontal
  - Horizontal Impingement
  - Angled from Horizontal Impingement
  - Vertical
  - Downward Impinging on Ground



Definition of Discharge

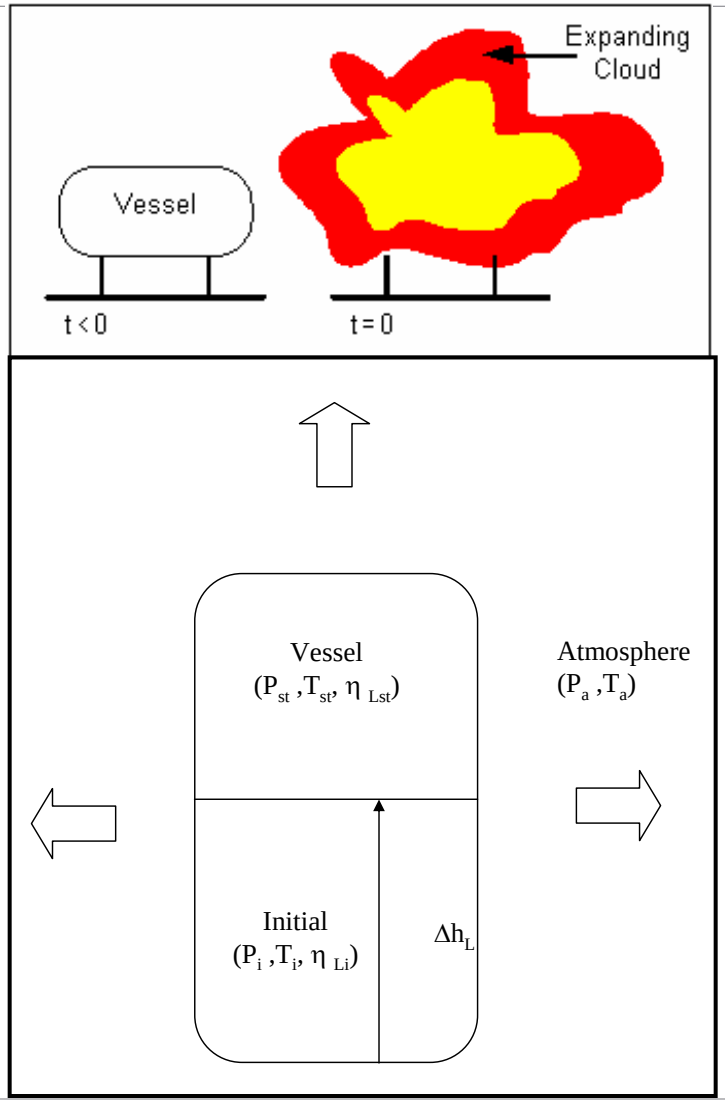
- Discharge is the time and distance it takes the material to go from the storage pressure to atmospheric pressure.



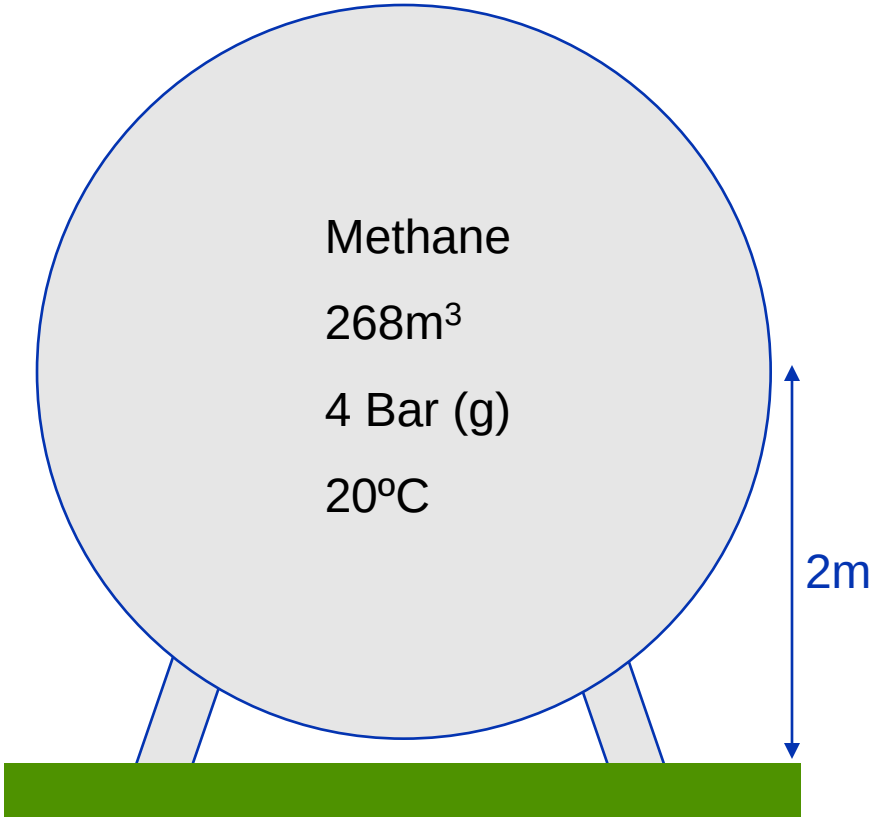
discharge scenarios

1.1 Catastrophic Rupture

- Designed to model an incident in which the vessel is destroyed by an impact, a crack, or some other failure which propagates very quickly
- Entire inventory is released
- No release direction, material is released in every direction
- Expands to atmospheric pressure
- Discharge is instantaneous

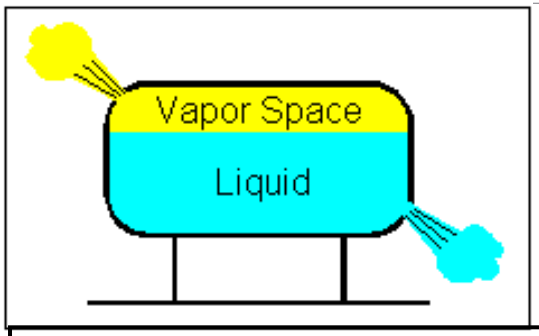


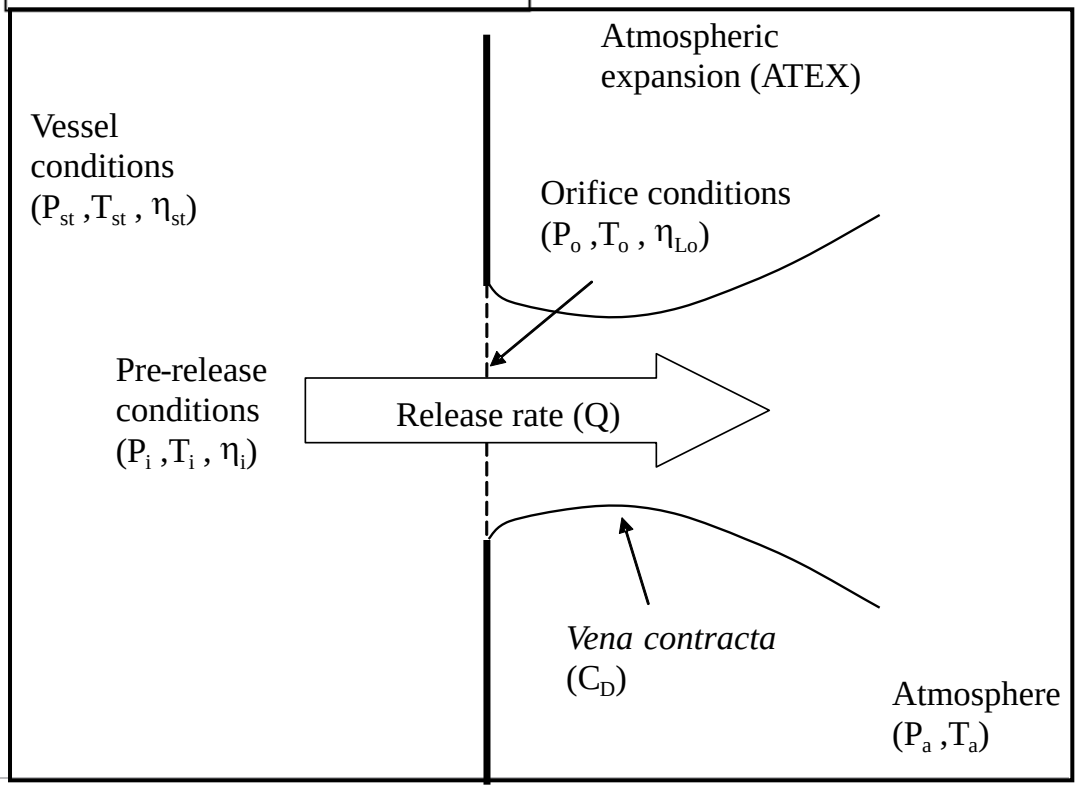
1.1 Catastrophic Rupture



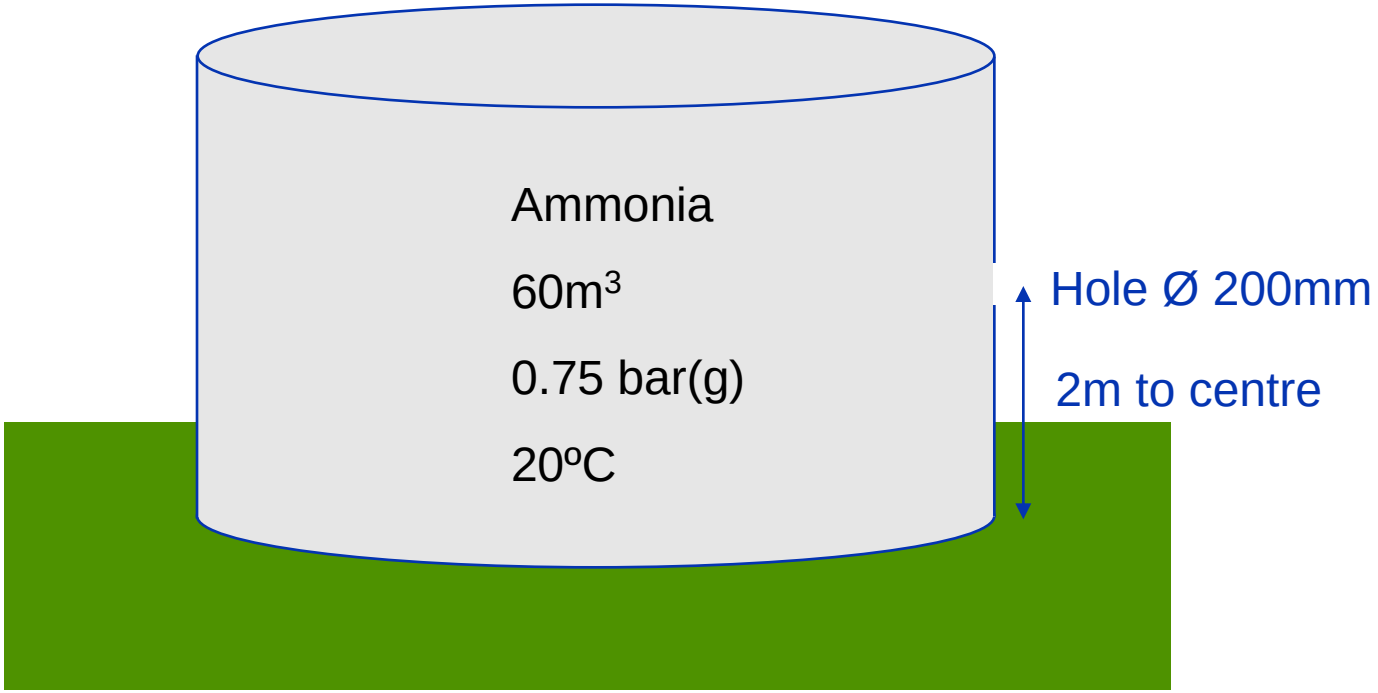
1.2 Leak

- Designed to model a hole in the body of a vessel, or a small hole in a large pipe
- Discharge has a duration
- Release has a direction
- No frictional losses as the fluid flows through the vessel or pipe towards the hole
- Tank and Pump Head can be specified
- For 2-phase storage, the material can be released from the vessel as either liquid (hole below the liquid level) or vapour (hole above liquid level)



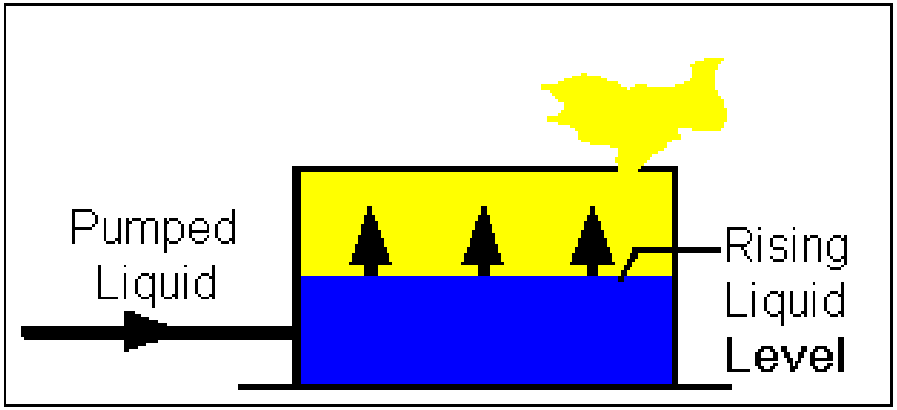


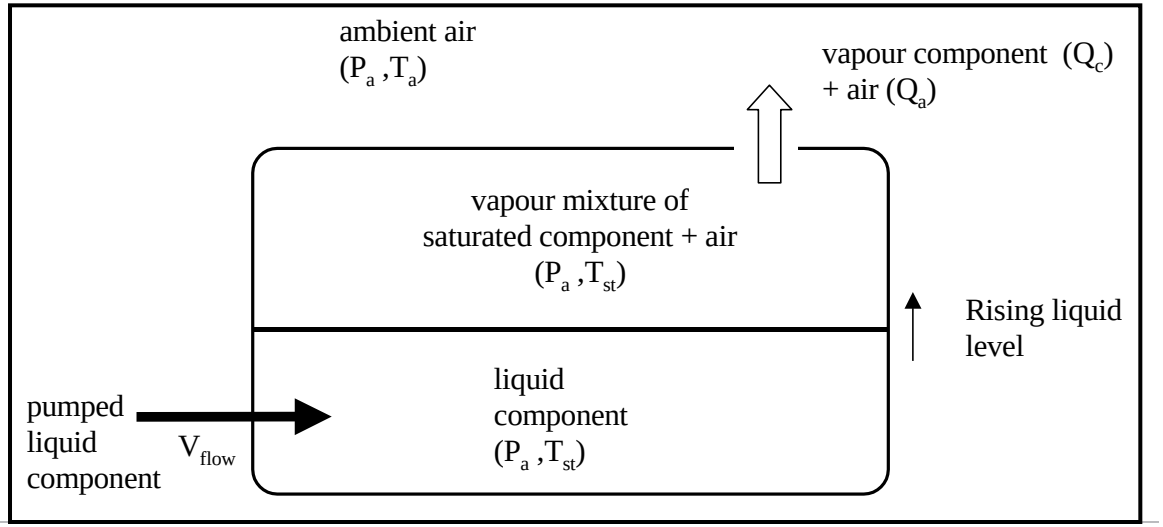
1.2 Leak



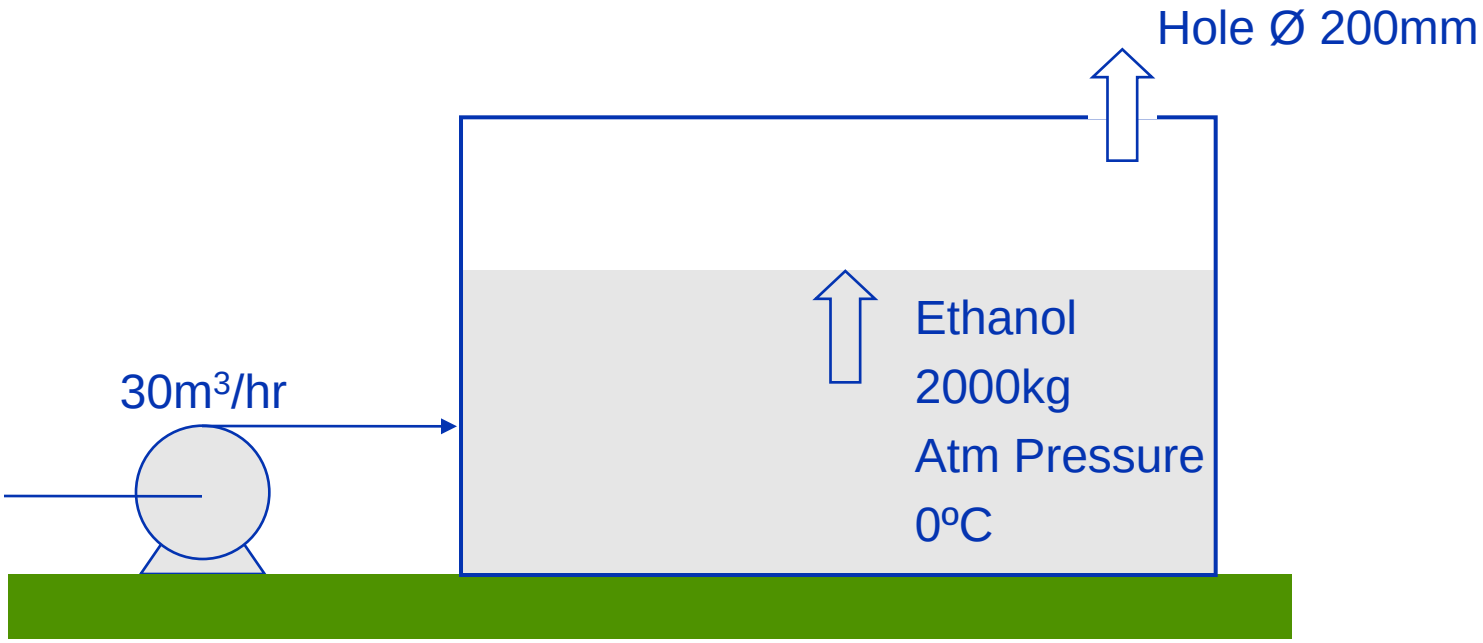
1.3 Vent from Vapour Space

- Designed for the venting of material from the vapour space of an unpressurized vessel
- The vapour volume flow out is equal to the liquid volume flow in
- The outgoing vapour is a mixture of air and the saturated vapour component



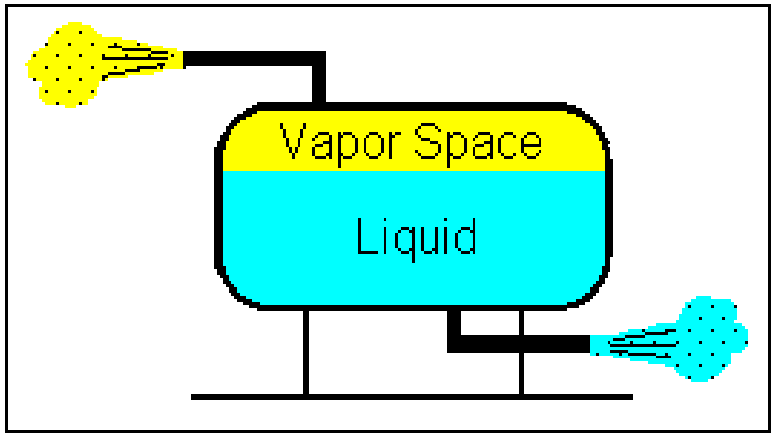


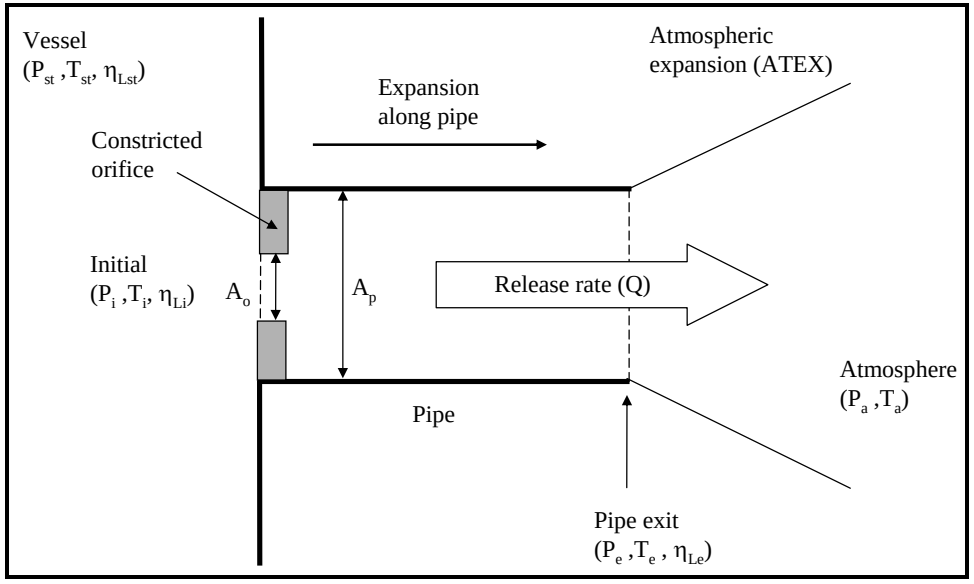
1.3 Vent from Vapour Space



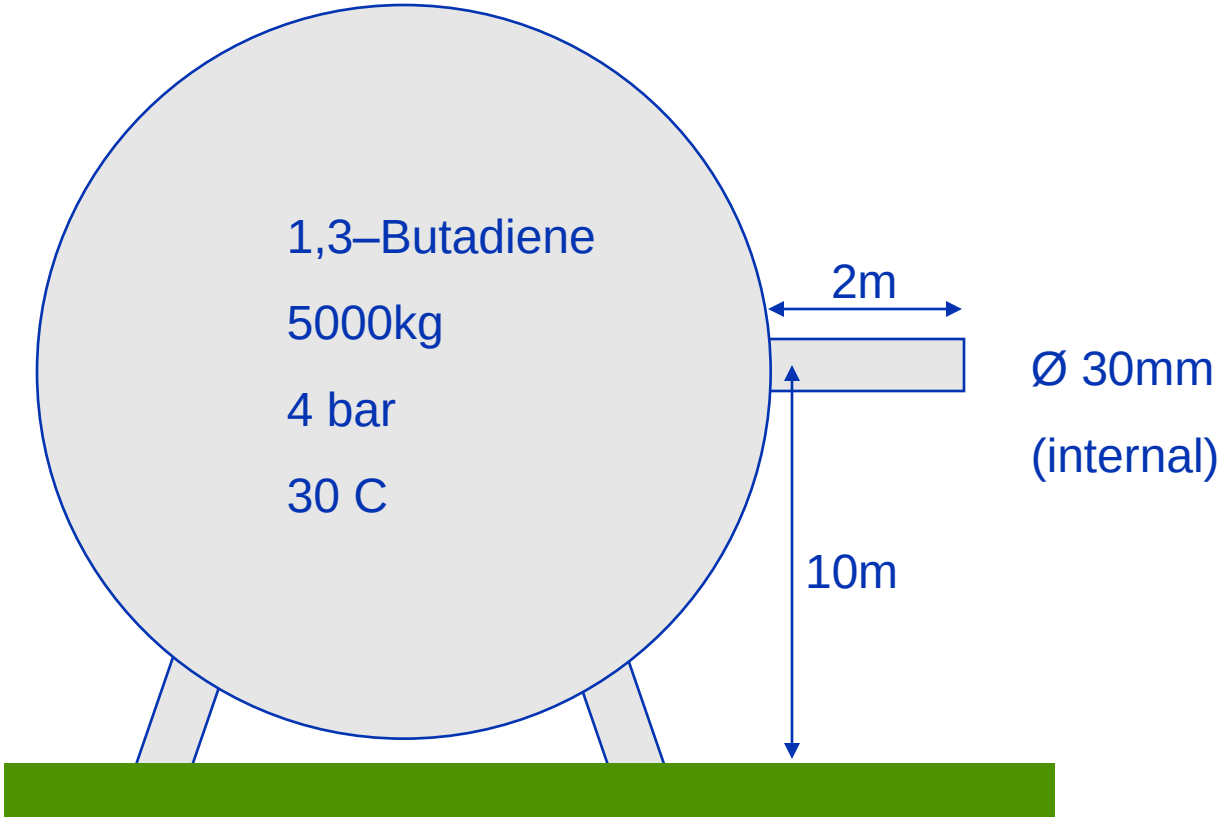
1.4 Line Rupture

- Designed for a full-bore rupture of a short length of pipework attached to a vessel
- Discharge has a duration and a direction
- Takes into account frictional losses along the pipe
- For 2-phase storage, the material can be released from the vessel as either liquid (pipe entrance below the liquid level) or vapour (pipe entrance above liquid level)
- The orifice at the entrance to the pipe is assumed to be the diameter of the pipe ($A_o = A_p$) for line ruptures
- Tank and Pump Head can be specified



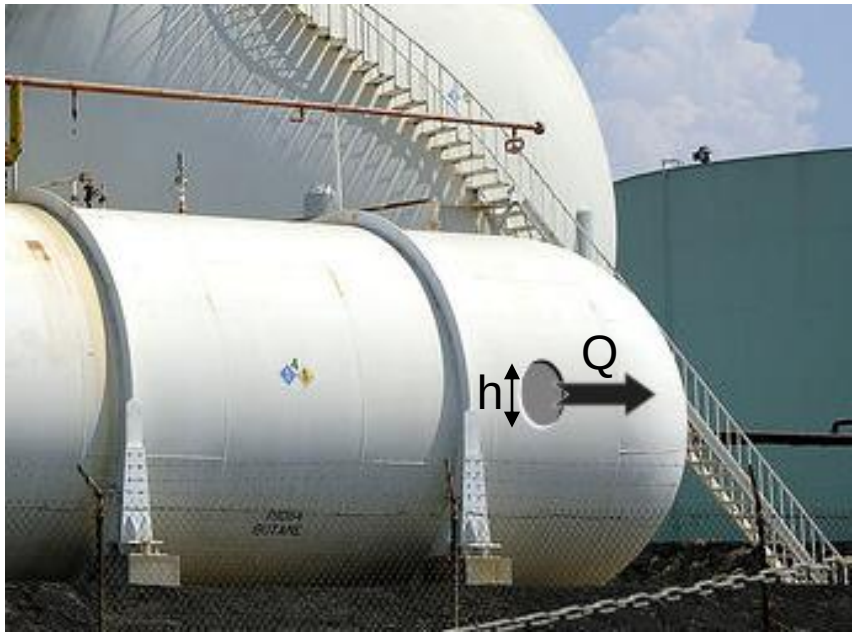


1.4 - Line Rupture



1.5 Fixed Duration

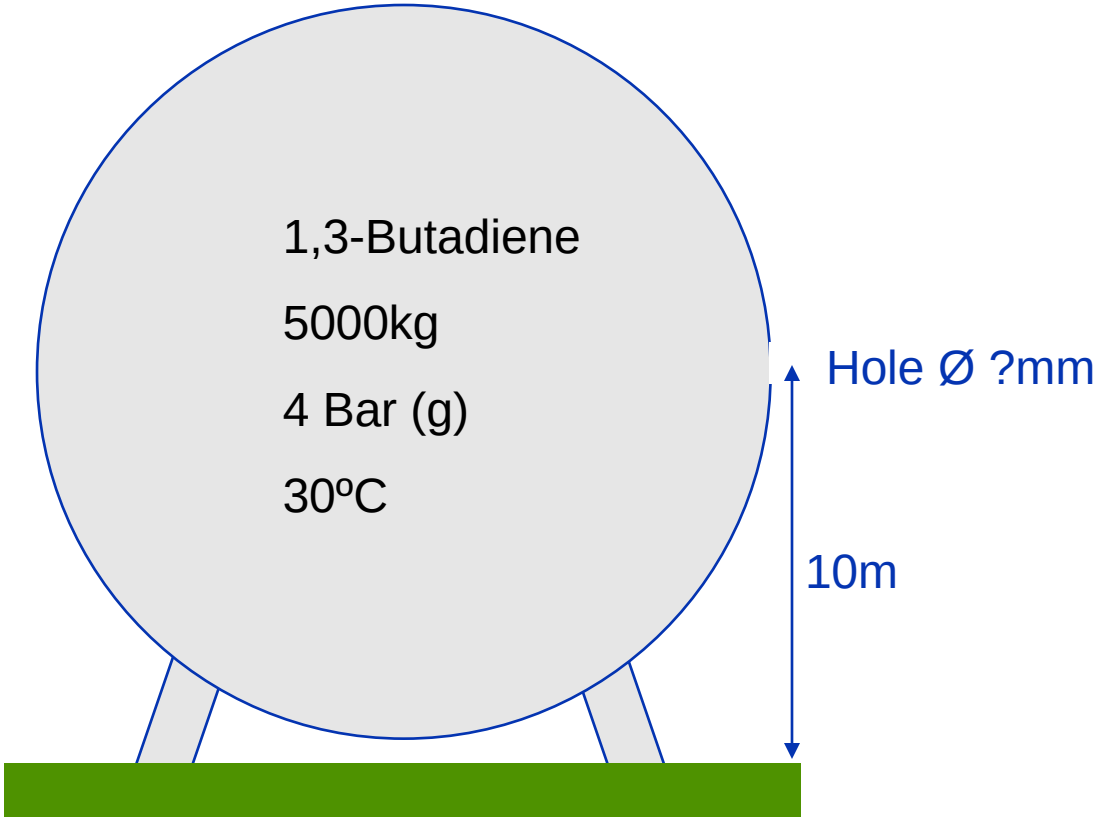
- The Orifice model, as used in the previously discussed Leak scenario calculates the mass flow rate and discharge duration from the provided release hole size and material storage conditions.
- When using the Fixed Duration scenario Phast will instead determine a hole size that corresponds to a flow rate that will expel the full inventory in the given time



- For a *Leak* the hole size *h* is specified and flow rate *Q* is calculated
- For a *Fixed Duration* the duration is specified and Phast uses a flow rate *Q* that empties the inventory in that duration and derives the corresponding hole size *h*

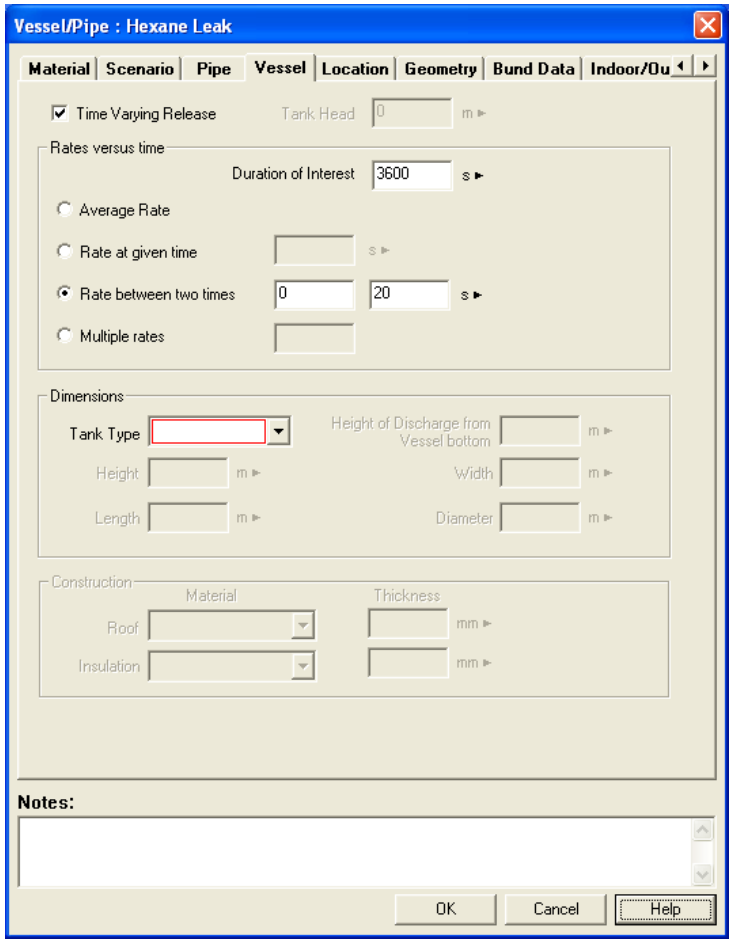
1.5 Fixed Duration

Fixed Release Duration: 600 seconds



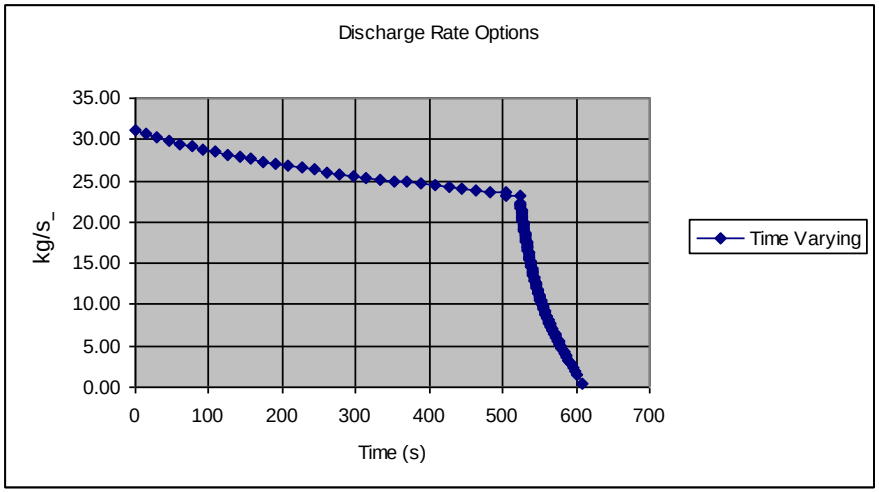
Time Varying Discharge

- The default release type in Phast is single segment, continuous release-rate at initial conditions

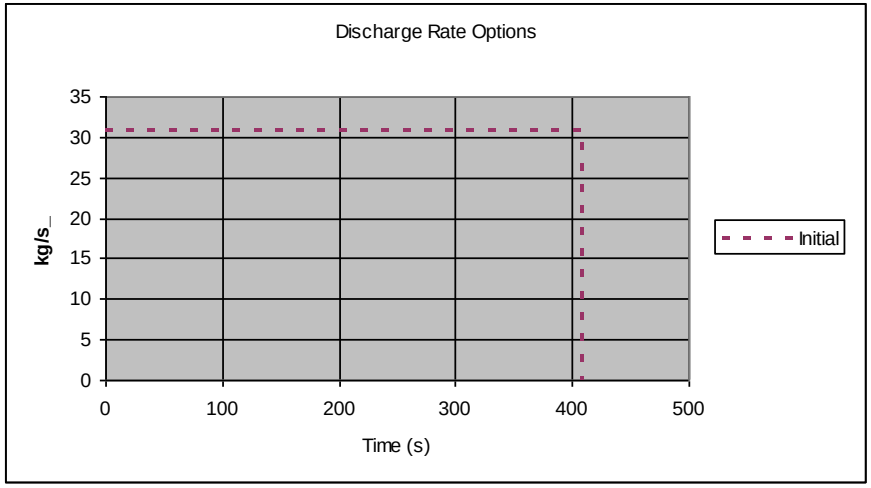


- Phast can calculate a varied release rate, but for calculation efficiency continuous rates are generated and passed to the dispersion calculations
- The initial release rate is the default value as it is conservative
- Phast offers 4 other options for calculation of a time varying release rate, though all options use steady state discharge segments
- Phast also produces a report of the actual time varying, non-segmented release rate if the Time Varying Release option is selected
- The discharge parameters allow control of a vacuum relief valve (operating by default) which stops “gulping” of air through the release orifice

Initial Rate and Time Varying



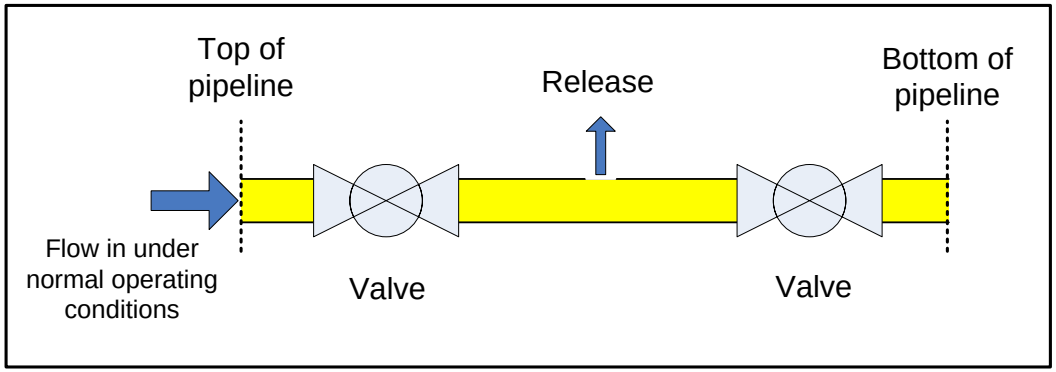
- With Time Varying activated, Phast will produce a TVDI report, containing the continuously varying discharge rate versus time
- Example profile from a 50mm cyclo-hexane leak. Liquid followed by vapour



- By default Phast will use a non-time-varying method and will use a continuous initial release rate until all inventory is released

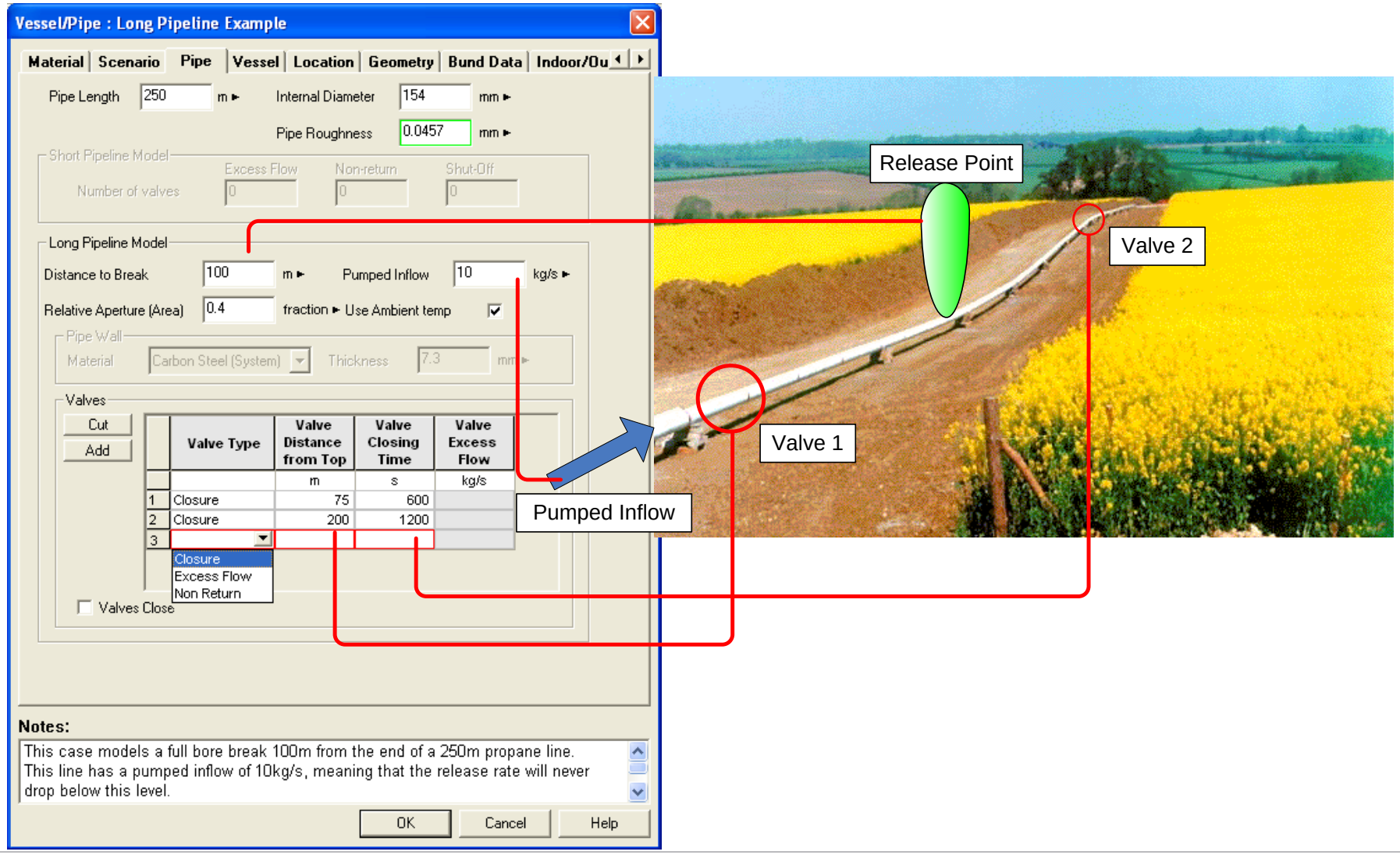
1.6 and 1.7 Long Pipeline

- Phast supports the following arrangement:



  - Pumped inflow
  - Valve with distances and closure times, excess flow rates, or non-return flow limit (of interest in downstream section)
  - User defined distance to break
  - User defined release aperture
- Always Time Varying (default: rate between 0 -20s)
- Applicable when Pipe Length >> 300D (for commercial steel pipes)
- Vapour or Superheated liquids
  - No Model for Sub-cooled liquids
- Non-Ideal gas behaviour

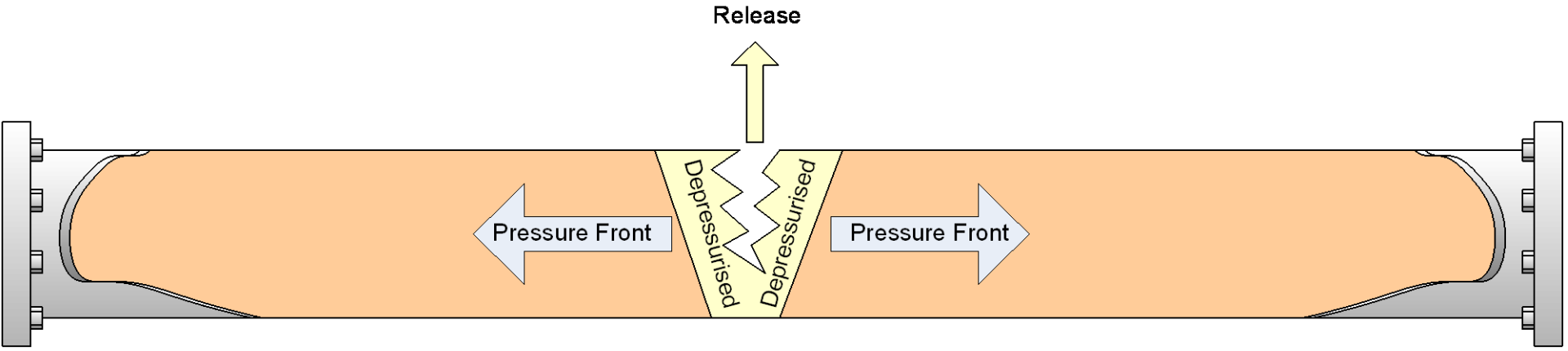
1.6 Long Pipeline



Long Pipeline Capabilities

Models releases where:

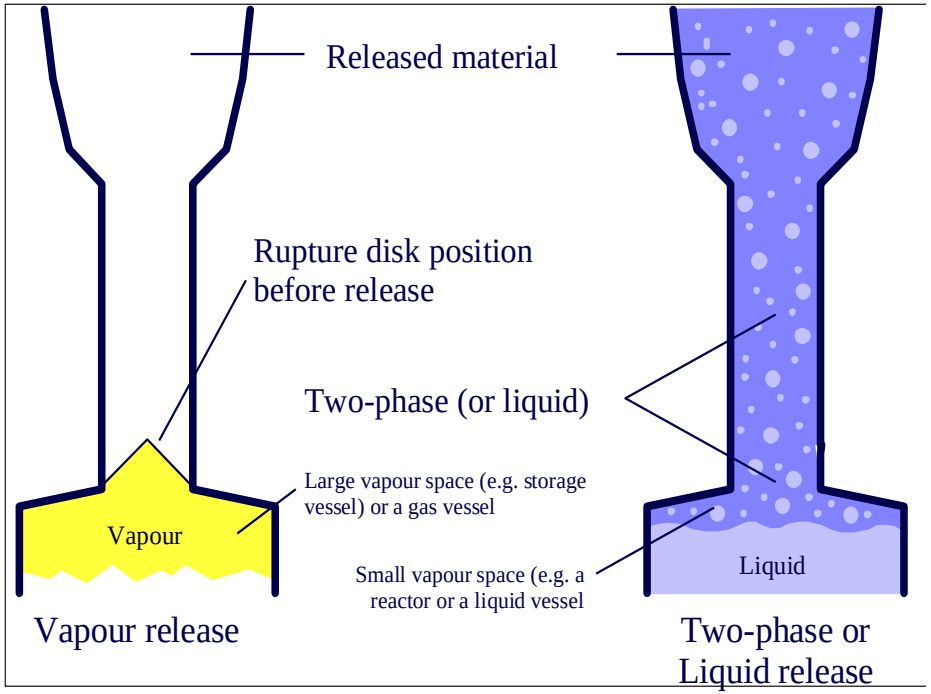
- conditions inside the pipe are changing as the material is released
- the material nearest to the release point will flash and depressurise first
- the material near the ends of the pipe will still be at the storage conditions
- the flash front will move further away from the release point so that eventually the entire contents of the pipe have depressurized to atmospheric conditions



1.8 Disc Rupture

- For overpressuring of a large vapour space vessel (storage disk rupture) or liquid swelling or over-filling of a small vapour space vessel (reactor disk rupture).

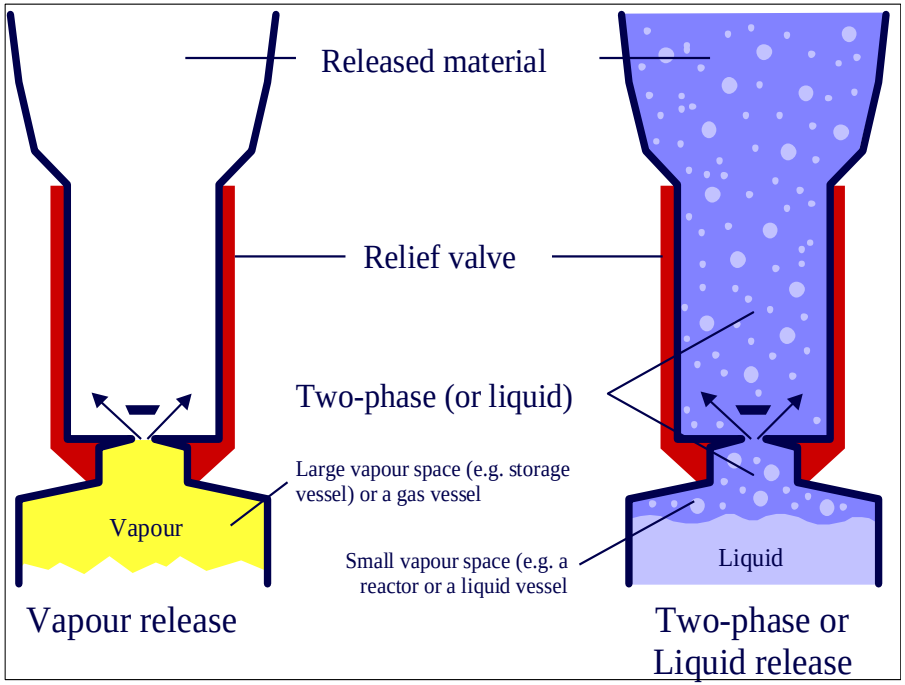
- Release through a burst rupture disk and along a short tailpipe.
- Discharge occurs through the disk seat (assumed not to be constricting).
- For 2-phase storage, the material can be released from the vessel as vapour (overpressuring of a large vapour space vessel) or as a homogeneous 2-phase.
- Pressurised liquid vessels cannot use this scenario.



1.9 Relief Valve

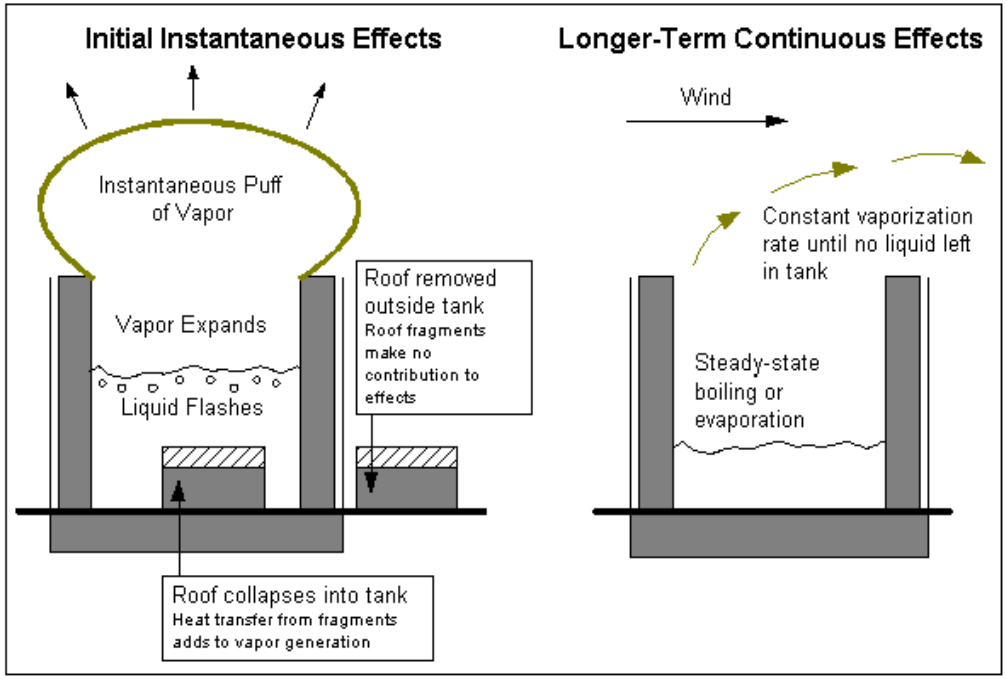
- Releases due to overpressuring of a large vapour-space vessel, or liquid swelling of a small vapour-space vessel.

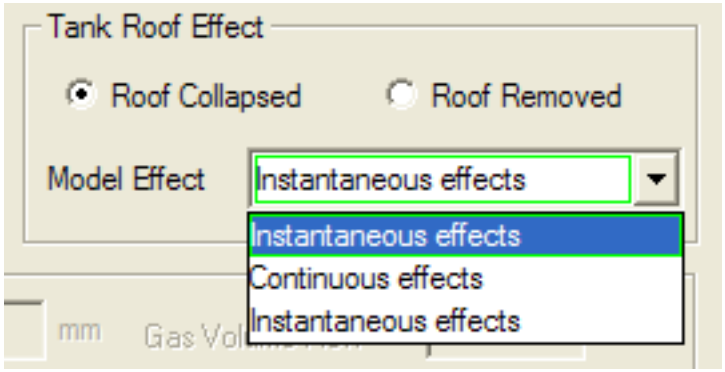
- The discharge occurs through the constricting relief valve at the entrance to the pipe and then along the length of a short tailpipe.
- For 2-phase storage, the material can be released from the vessel as either vapour (overpressuring of a large vapour space vessel) or as a homogeneous 2-phase .
- Pressurised liquid vessels cannot use this scenario.



1.10 Tank Roof Failure

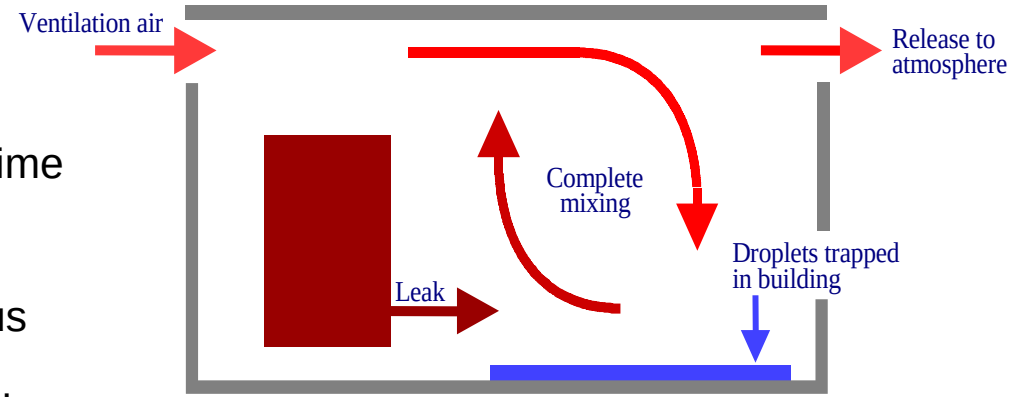
- Designed for the release of vapor from a refrigerated, insulated tank under saturated conditions, in the event that the roof fails
- Two types of failure
  - Roof removed
  - Roof collapsed
- Two types of dispersion
  - Initial instantaneous puff
  - Continuous evaporation





Inbuilding Release

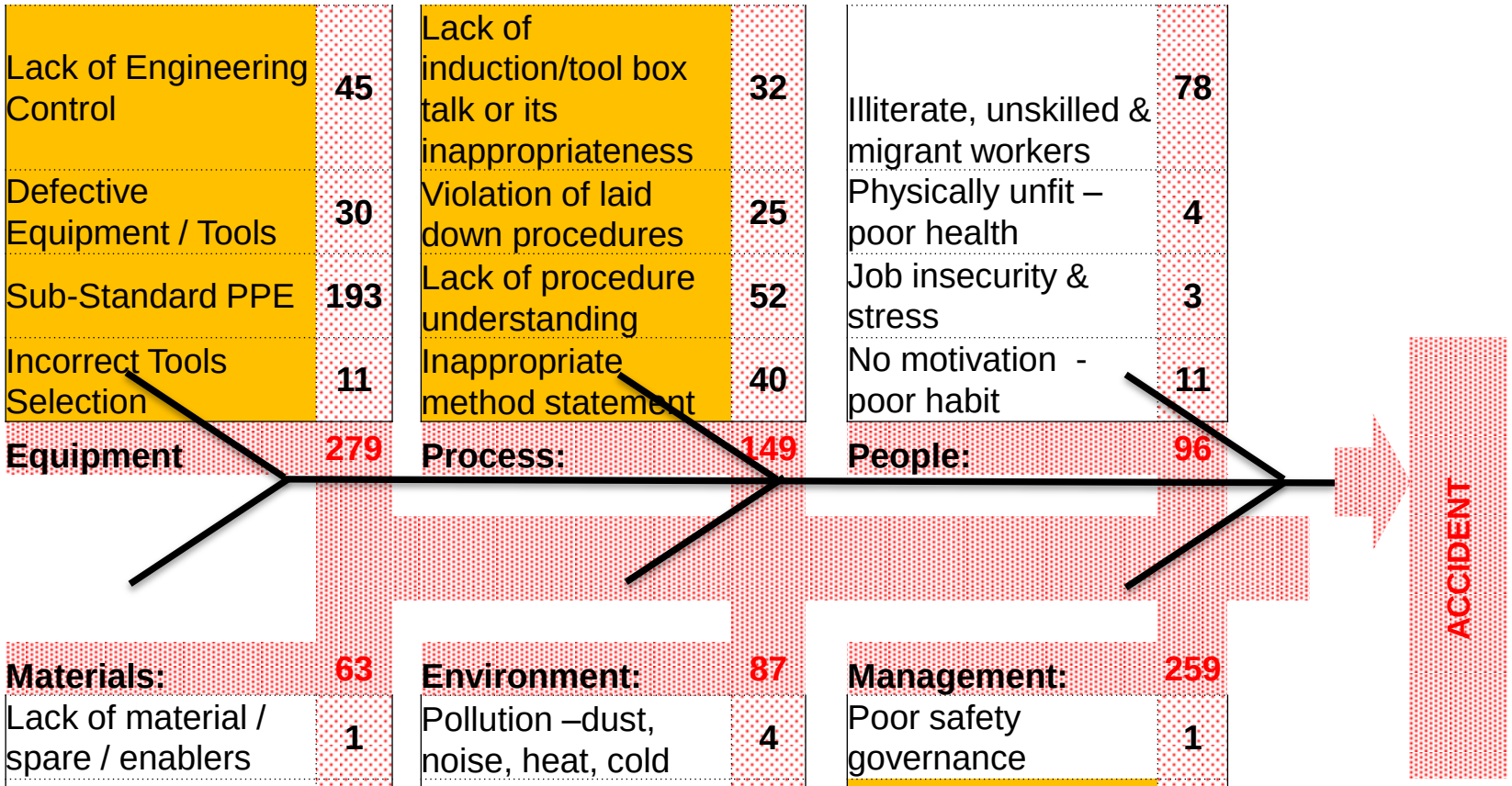
- Mixing of air with the release material within the building
- Concentration build-up and decay with time
- Liquid droplets can be trapped
- Constant mass release rate of hazardous material from the leak, a constant vent volume flow rate and ideal mixing conditions



- Calculates leak volume flow rate from the mass release rate, the release temperature and atmospheric pressure and assumes this leak volume flow rate to be constant until the release stops
- Volume flow rate of the release of hazardous material from the building is conservatively assumed to be the leak volume flow rate
- Concentration build-up and decay calculations apply ideal gas assumptions

CAUSE AND EFFECT ANALYSIS- FISHBORN ANALYSIS

Root cause analysis of First Aid Injury

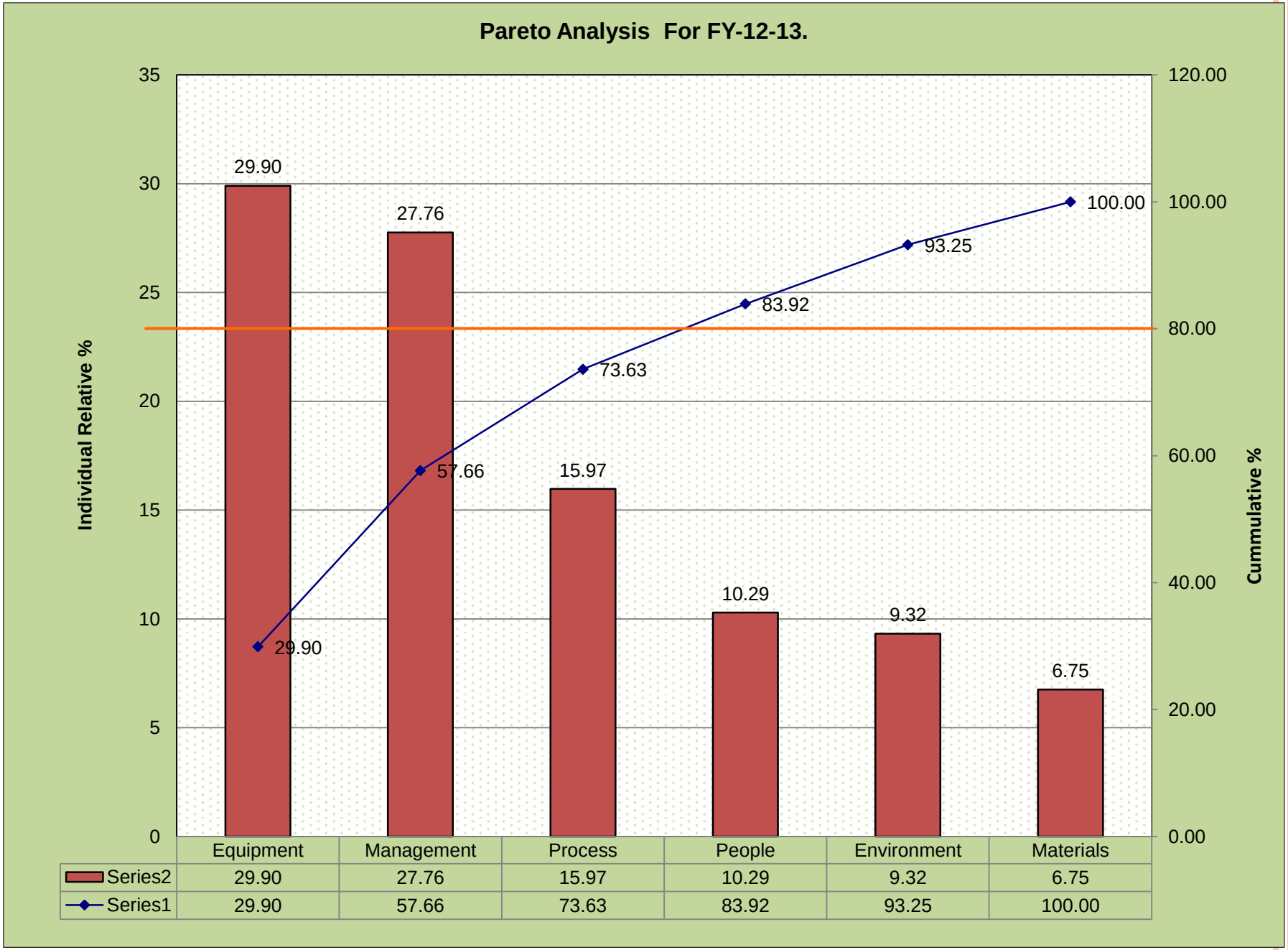


Causes are usually grouped into major categories to identify these sources of variation

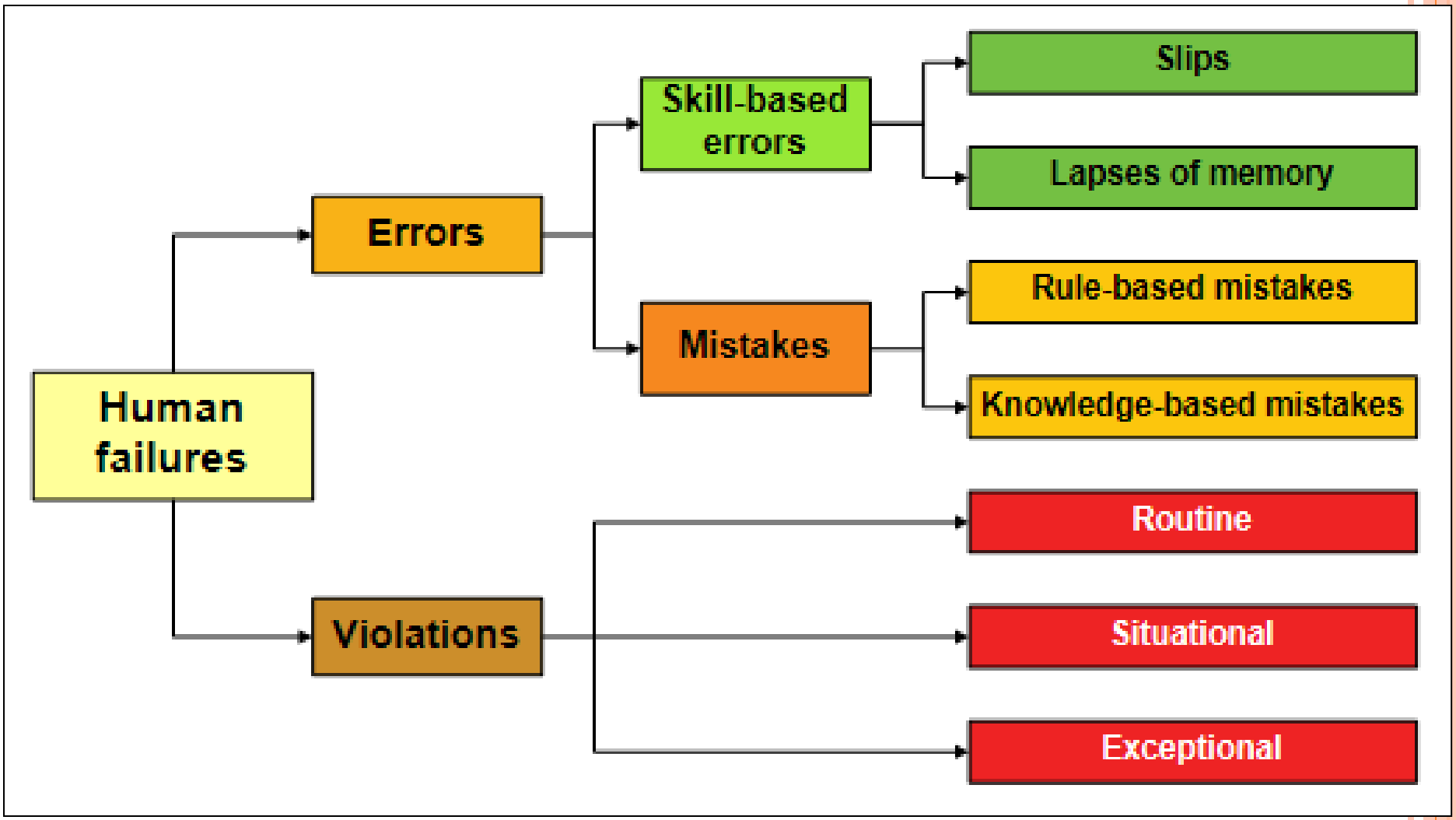
- People: Anyone involved with the process
- Methods: How the process is performed and the specific requirements for doing it, such as policies, procedures, rules, regulations and laws
- Machines: Any equipment, computers, tools, etc. required to accomplish the job
- Materials: Raw materials, parts, pens, paper, etc. used to produce the final product
- Measurements: Data generated from the process that are used to evaluate its quality
- Environment: The conditions, such as location, time, temperature, and culture in which the process operates

Pareto analysis

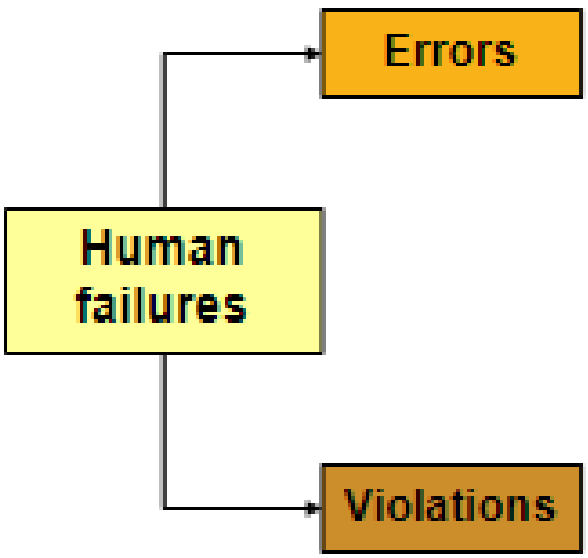
- This technique helps to identify the top portion of causes that need to be addressed to resolve the majority of problems. Once the predominant causes are identified, then tools like the Ishikawa diagram or Fish-bone Analysis can be used to identify the root causes of the problems. While it is common to refer to pareto as "80/20" rule, under the assumption that, in all situations, **20% of causes determine 80% of problems**, this ratio is merely a convenient rule of thumb and is not nor should it be considered immutable law of nature.
- The application of the Pareto analysis in risk management allows management to focus on those risks that have the most impact on the project.


Pareto Analysis For FY-12-13.
Individual Relative %
Cummulative %
35
30
25
20
15
10
5
0
120.00
100.00
80.00
60.00
40.00
20.00
0.00
29.90
27.76
15.97
10.29
9.32
6.75
29.90
57.66
73.63
83.92
93.25
100.00
Equipment
Management
Process
People
Environment
Materials
Series2 29.90 27.76 15.97 10.29 9.32 6.75
Series1 29.90 57.66 73.63 83.92 93.25 100.00

HUMAN FAILURES


Human failures
Errors
Skill-based errors
Slips
Lapses of memory
Mistakes
Rule-based mistakes
Knowledge-based mistakes
Violations
Routine
Situational
Exceptional

Human failures

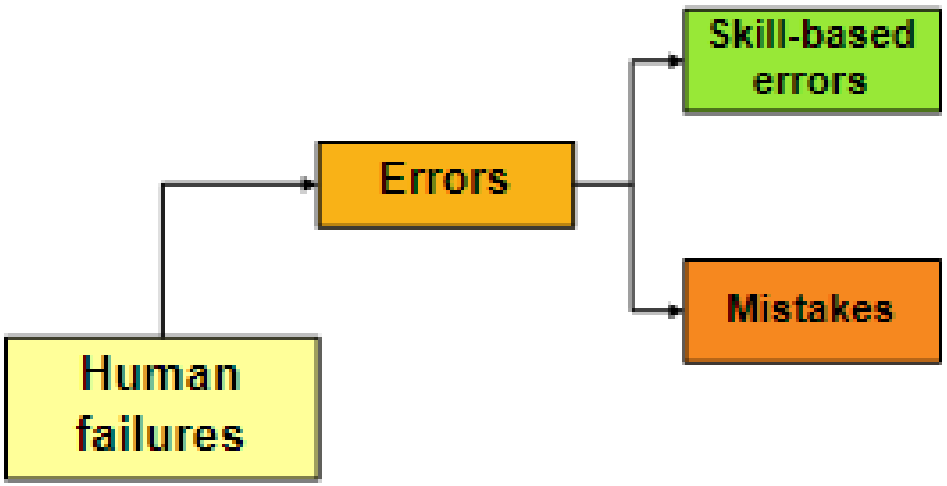


Human failure - main classification

A human error is an action which was **not intended**, which involved a deviation from a accepted standard, and which led to an undesirable outcome.

A violation is a **deliberate** deviation from a rule or procedure

Human failures



Let's have a look at the errors first:

Skill-based errors (or slips and lapses) occur in very familiar tasks which we can carry out without much need for conscious attention.
Driving a car is a typical skill-based activity for many of us. Slips and lapses are the errors which are made by even the most experienced, well-trained and highly-motivated people.

Mistakes are a more complex type of human error where we do the wrong thing believing it to be right.
The failure involves our mental processes which control how we plan, assess information, make intentions and judge consequences.

Slips are failures in carrying out the actions of a task. They are described as 'action-not-as-planned'. Examples would be: picking up the wrong component from a mixed box, operating the wrong switch, transposing digits when copying out numbers and misordering steps in a procedure. Typical slips might include:

- performing an action too soon in a procedure or leaving it too late;

Lapses cause us to forget to carry out an action, to lose our place in a task or even to forget what we had intended to do. They can be reduced by minimising distractions and interruptions to tasks and by providing effective reminders especially for tasks which take some time to complete or involve periods of waiting.

A useful reminder could be as simple as a partially completed checklist placed in a clearly visible location for the person doing the task.

We may be able to eliminate some of these lapses through better design of equipment or tasks.

Rule-based mistakes occur when our behaviour is based on remembered rules or familiar procedures. We have a strong tendency to use familiar rules or solutions even when these are not the most convenient or efficient.

The following is an example of a rule-based mistake causing an accident:

An operator was very familiar with the task of filling a tank. He expected the filling procedure to take about 30 minutes. However, on this occasion the diameter of the pipe entering the tank was filling much more rapidly than he anticipated. He ignored the high level alarms on the grounds that the tank could not be full so quickly. The tank overflowed.

Improved communications would have alerted the operator to the changes that had been made to the pipe.

In unfamiliar circumstances we have to revert to consciously making goals, developing plans and procedures. Planning or problem solving needs us to reason from first principles or use analogies. Misdiagnosis and miscalculations can result when we use this knowledge-based reasoning.

The following is an example of knowledge-based reasoning causing an accident:

The investigation following a major collapse of a tunnel showed that the organisation had relied on the experience of one person as a control measure. However, the nature of the method of working meant that this person had no reliable instrumentation for detecting when the tunnel was becoming unstable. Relying on 'experience' was actually relying on knowledge-based reasoning of the 'expert' and was not an effective control method to prevent a serious collapse given the unpredictable nature of the event. The expert needed more reliable instruments to carry out this work.

With a routine violation, breaking the rule or procedure has become a normal way of working within the work group. This can be due to:

- the desire to cut corners to save time and energy;
- the perception that the rules are too restrictive;
- the belief that the rules no longer apply;
- lack of enforcement of the rule; and
- new workers starting a job where routine violations are the norm and not realising that this is not the correct way of working.

In the case of situational violations breaking the rule is due to pressures from the job such as being under time pressure, insufficient staff for the workload, the right equipment not being available, or even extreme weather conditions. It may be very difficult to comply with the rule in a particular situation or staff may think that the rule is unsafe under the circumstances.
Risk assessments may help to identify the potential for such violations.
Encouraging reporting of job pressures through open communication will also be helpful.

Exceptional violations rarely happen and only then when something has gone wrong.
To solve a new problem you feel you need to break a rule even though you are aware that you will be 'taking a risk'. You believe, falsely, that the benefits outweigh the risks.

For example:
Before the accident at Chernobyl nuclear power plant a series of tests were being undertaken. When a failure led to dangerously low power levels the test should have been abandoned. Operators and engineers continued to improvise in an unfamiliar and increasingly unstable regime to protect the test plan.