

Risk Assessment

Introduction

- Risk assessment includes incident identification and consequence analysis
- Incident identification analysis of the probabilities
- Consequence analysis describes the expected damage
- The Dow F&EI includes a calculation of the maximum probable property damage (MPPD) and the maximum probable days outage (MPDO)
- Hazard and operability (HAZOP) studies provide information on how a particular accident occurs
- No probabilities or numbers are used with the typical HAZOP study
- Experience of the review committee is used to decide on an appropriate course of action.

Introduction...

In this chapter we will

- Review probability mathematics, including the mathematics of equipment failure
- Show how the failure probabilities of individual hardware components contribute to the failure of a process
- Describe two probabilistic methods (**Event trees and Fault trees**),
- Describe the concepts of layer of protection analysis (LOPA)
- Describe the relationship between quantitative risk analysis (QRA) and LOPA.

Event Trees

- Event trees begin with an **initiating event** and work toward a final result
- This is used effectively to determine the probability of a certain sequence of events and to decide what improvements are required
- When an accident occurs in a plant, various safety systems come into play to prevent the accident from propagating
- These safety systems either fail or succeed
- The typical steps in an event tree analysis are
 1. Identify an initiating event of interest,
 2. Identify the safety functions designed to deal with the initiating event,
 3. Construct the event tree
 4. Describe the resulting accident event sequences

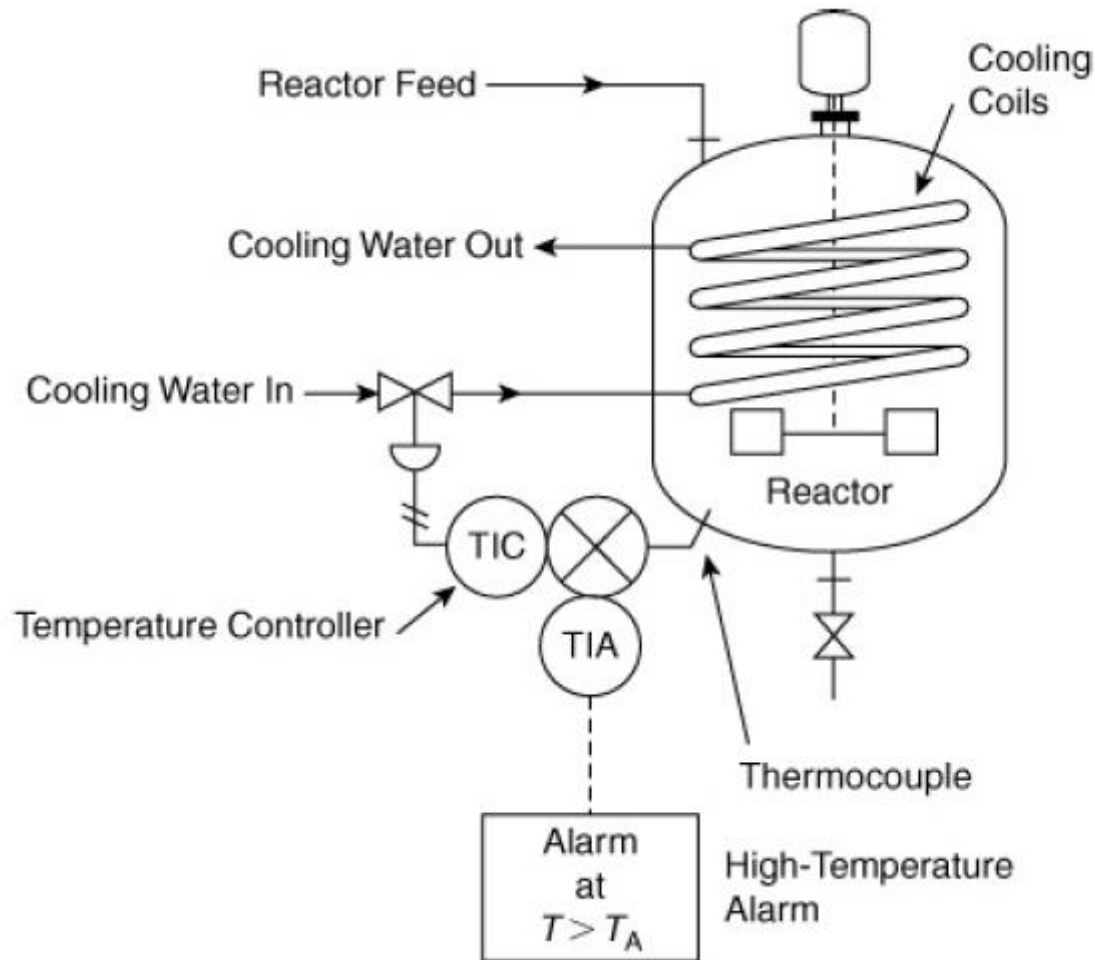
Event Trees

Diagrammatical representation

- The event tree is written from left to right.
- The initiating event is written first in the centre of the page on the left.
- A line is drawn from the initiating event to the first safety function.
- At this point the safety function can either succeed or fail.
- By convention, a successful operation is drawn by a straight line upward and a failure is drawn downward.
- Horizontal lines are drawn from these two states to the next safety function.
- If a safety function does not apply, the horizontal line is continued through the safety function without branching.

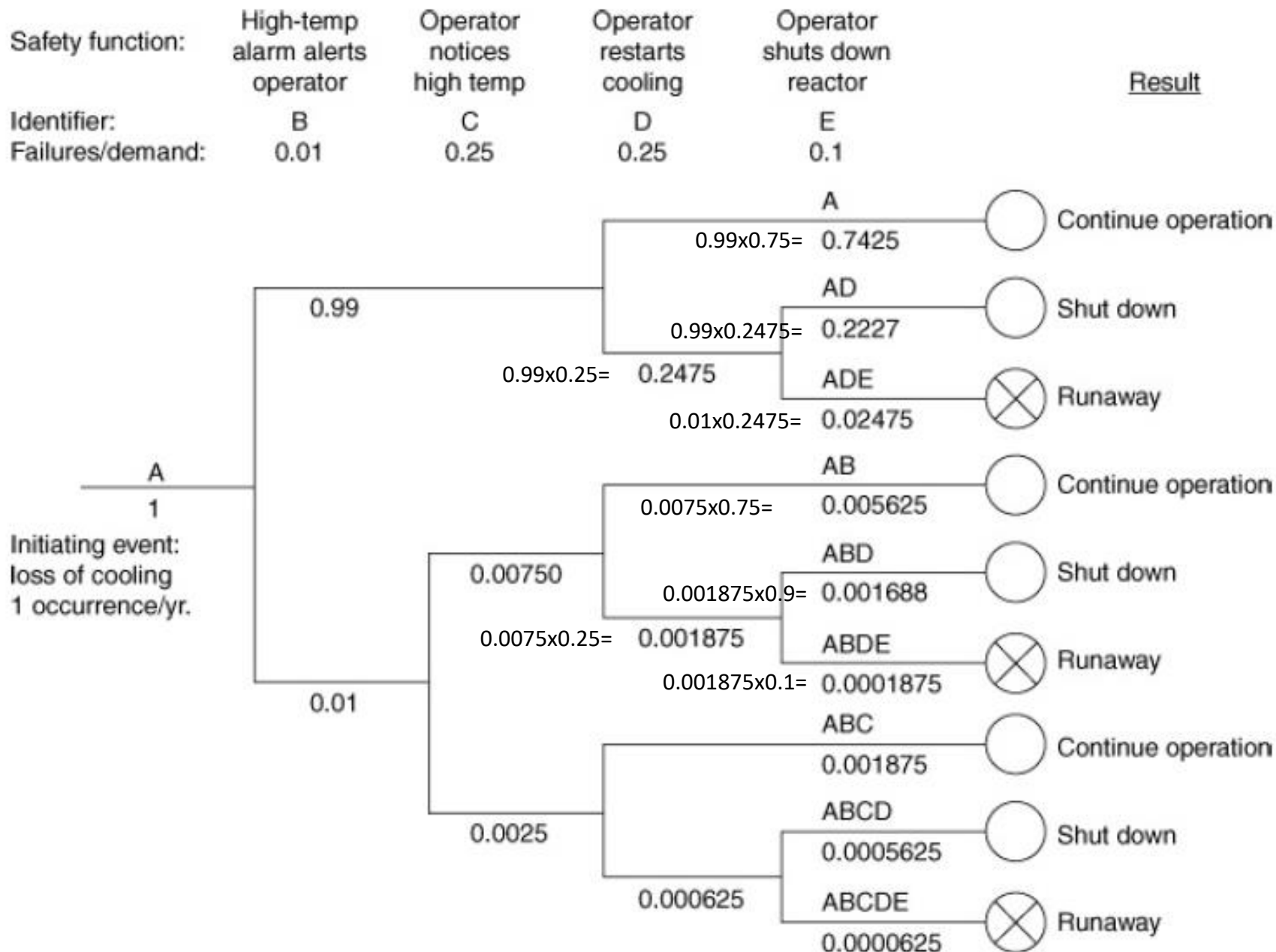
Event Trees (case study)

loss-of-coolant accident for the reactor



Event Trees (case study)

- A high-temperature alarm has been installed to warn the operator of a high temperature within the reactor.
- Four safety functions are identified.
- The first safety function is the high-temperature alarm.
- The second safety function is the operator noticing the high reactor temperature during normal inspection.
- The third safety function is the operator re-establishing the coolant flow by correcting the problem in time.
- The final safety function is invoked by the operator performing an emergency shutdown of the reactor.
- The letters indicate the sequence of failures of the safety systems.
- ADE represents initiating event A followed by failure of safety functions D and E.



Shutdown = $0.2227 + 0.001688 + 0.0005625 = 0.2250$ occurrences/yr.
 Runaway = $0.02475 + 0.0001875 + 0.0000625 = 0.02500$ occurrences/yr.

Event Trees

- The event tree is useful for providing scenarios of possible failure modes.
- If quantitative data are available, an estimate can be made of the failure frequency
- This is used most successfully to modify the design to improve the safety.
- The difficulty is that for most real processes the method can be extremely detailed, resulting in a huge event tree.
- If a probabilistic computation is attempted, data must be available for every safety function in the event tree.
- An event tree begins with a specified failure and terminates with a number of resulting consequences.

Major disadvantage of event trees.

- If an engineer is concerned about a particular consequence, there is no certainty that the consequence of interest will actually result from the selected failure.

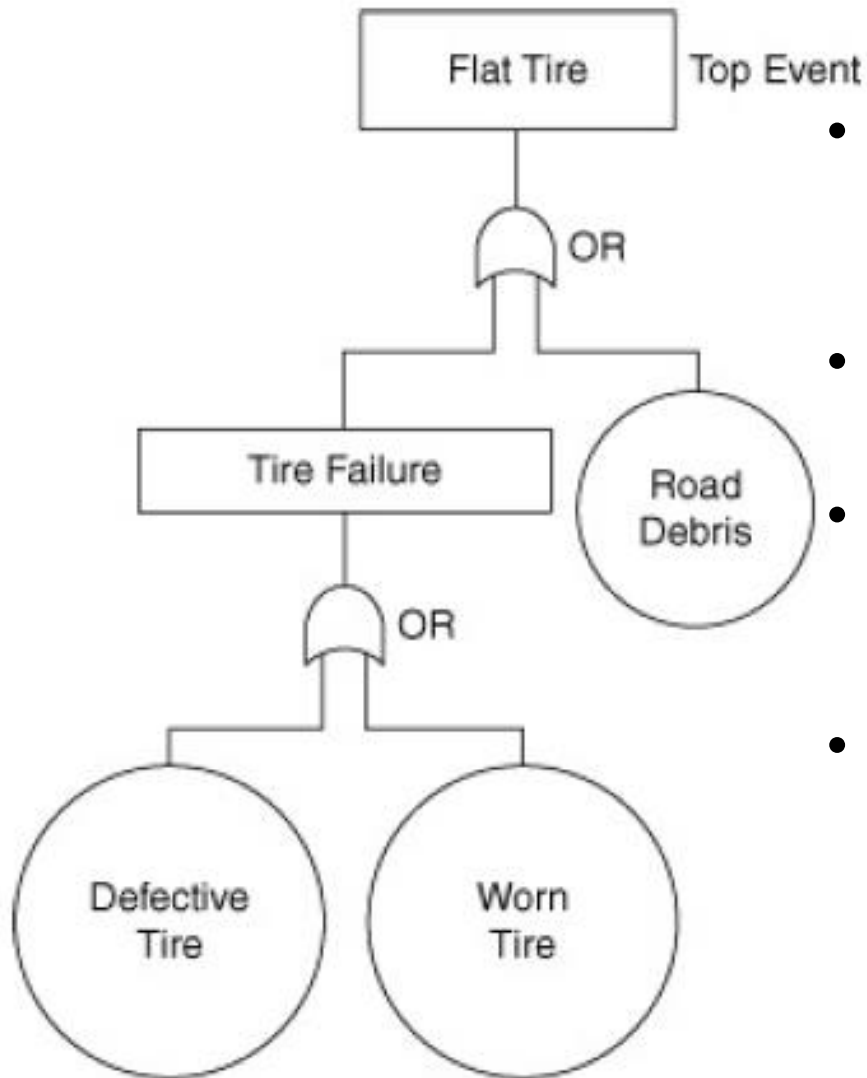
Fault Trees

- Fault trees are a deductive method for identifying ways in which hazards can lead to accidents.
- The approach starts with a well-defined accident, or top event, and works backward toward the various scenarios that can cause the accident.
- For instance, a flat tire on an automobile is caused by two possible events.
- In one case the flat is due to driving over debris on the road, such as a nail.
- The other possible cause is tire failure.
- The flat tire is identified as the top event.
- The two contributing causes are **either Basic or Intermediate** events.

Fault Trees

- A fault tree for anything but the simplest of plants can be large, involving thousands of process events.
- The basic events are events that cannot be defined further.
- Intermediate events are events that can.
- For this example, driving over the road debris is a basic event because no further definition is possible.
- The tire failure is an intermediate event because it results from either a defective tire or a worn tire
- Events in a fault tree are not restricted to hardware failures. They can also include software, human, and environmental factors.
- The flat tire example is pictured using a fault tree logic diagram

A fault tree describing the various events contributing to a flat tire



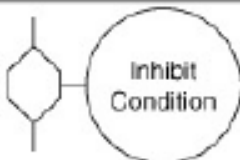




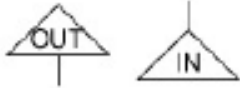


- The circles denote basic events and the rectangles denote intermediate events.
- The fishlike symbol represents the OR logic function.
- It means that either of the input events will cause the output state to occur.
- Flat tire is caused by either debris on the road or tire failure. Similarly, the tire failure is caused by either a defective tire or a worn tire.

Fault Trees

- For reasonably complex chemical processes a number of additional logic functions are needed to construct a fault tree.
- the purpose of the fault tree is to determine the individual event steps that must occur to produce the top event
- The AND logic function is important for describing processes that interact in parallel.
- Output state of the AND logic function is active only when both of the input states are active.
- The INHIBIT function is useful for events that lead to a failure only part of the time.
- For instance, driving over debris in the road does not always lead to a flat tire.
- The INHIBIT gate could be used in the fault tree of to represent this situation.

The logic transfer components used in a fault tree

	AND Gate:	The resulting output event requires the simultaneous occurrence of all input events.
	OR Gate:	The resulting output event requires the occurrence of any individual input event.
	INHIBIT Event:	The output event will occur if the input occurs and the inhibit event occurs.
	BASIC Event:	A fault event that needs no further definition.
	INTERMEDIATE Event:	An event that results from the interaction of a number of other events.
	UNDEVELOPED Event:	An event that cannot be developed further due to lack of suitable information.
	EXTERNAL Event:	An event that is a boundary condition to the fault tree.
	TRANSFER Symbols:	Used to transfer the fault tree into and out of a sheet of paper.

Preliminary steps must be taken

- Define precisely the top event. Events such as “high reactor temperature” or “liquid level too high” are precise and appropriate.
- Events such as “explosion of reactor” or “fire in process” are too vague, whereas an event such as “leak in valve” is too specific.
- Define the existing event. What conditions are sure to be present when the top event occurs?
- Define the unallowed events. These are events that are unlikely or are not under consideration at the present. This could include wiring failures, lightning, tornadoes and hurricanes.

Preliminary steps must be taken

- Define the physical bounds of the process. What components are to be considered in the fault tree?
- Define the equipment configuration. What valves are open or closed?
- What are the liquid levels? Is this a normal operation state?
- Define the level of resolution. Will the analysis consider just a valve, or will it be necessary to consider the valve components?
- Purpose of the fault tree is to determine the individual event steps that must occur to produce the top event.

Draw a fault tree

Consider again the alarm indicator and emergency shutdown system for this system.

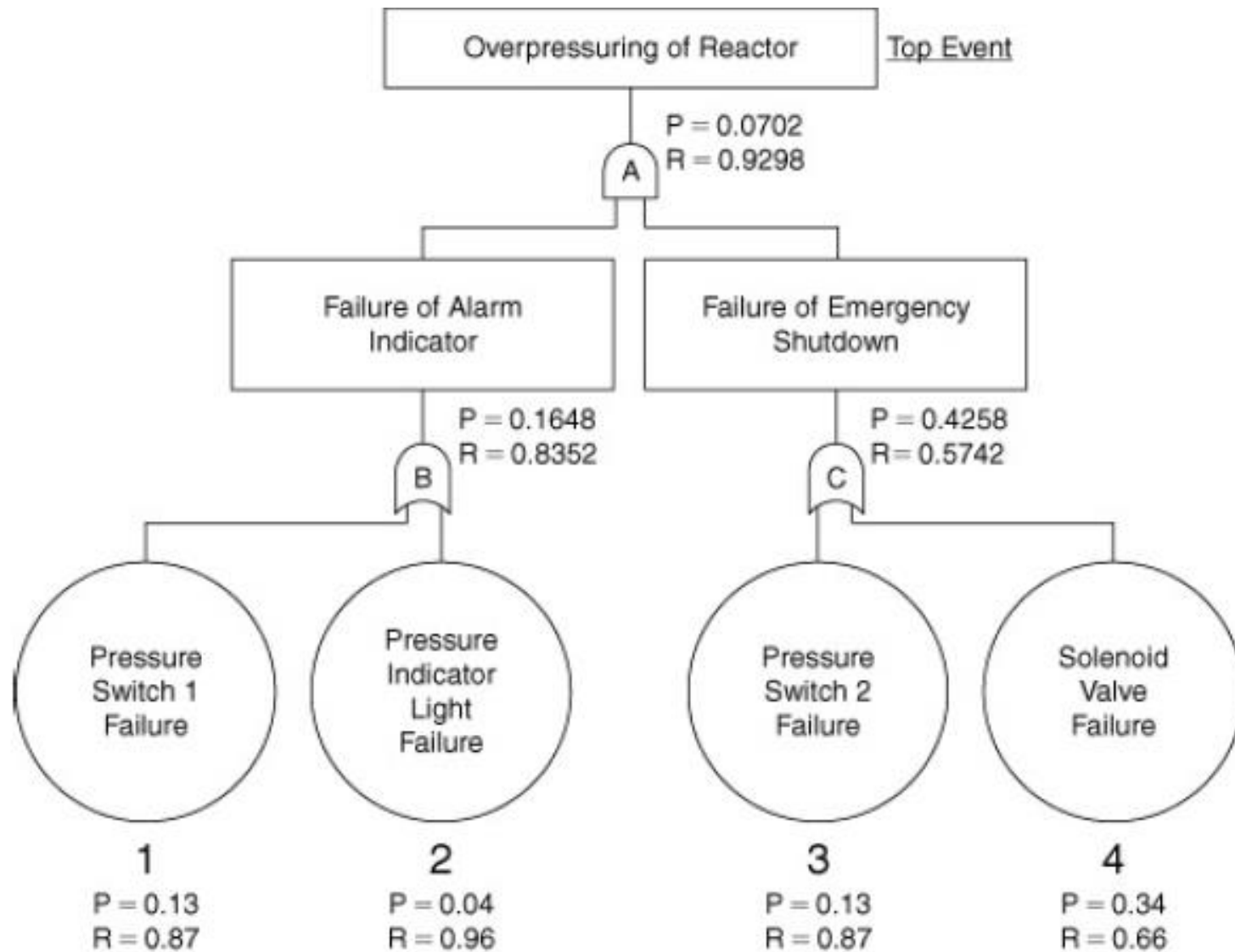
Solution

The first step is to define the problem.

1. Top event: Damage to reactor as a result of over pressuring.
2. Existing event: High process pressure.
3. Unallowed events: Failure of mixer, electrical failures, wiring failures, tornadoes, hurricanes, electrical storms.
4. Physical bounds:
5. Equipment configuration: Solenoid valve open, reactor feed flowing.
6. Level of resolution: Equipment as shown

The symbol P represents the probability and R represents the reliability

Draw a fault tree



Draw a fault tree

- First, draw the top event at the top of the page
- Second, determine the major events that contribute to the top event.
- Write these down as intermediate, basic, undeveloped, or external events on the sheet.
- If these events are related in **parallel** (all events must occur in order for the top event to occur), they must be connected to the top event by an **AND gate**.
- If these events are related in **series** (any event can occur in order for the top event to occur), they must be connected by an **OR gate**.

Determining the Minimal Cut Sets

- The minimal cut sets are the various sets of events that could lead to the top event.
- Top event could occur through a variety of different combinations of events.
- The **different unique** sets of events leading to the top event are the **minimal cut sets**.
- the minimal cut sets are ordered with respect to failure probability.
- The higher probability sets are examined carefully to determine whether additional safety systems are required.
- The probabilities from the cut sets are added together.
- The minimal cut sets represent the various failure modes. For events 1, 3 or 2, 3 or 1, 4 or 2, 4 could cause the top event

Quantitative Calculations Using the Fault Tree

$$P(1 \text{ AND } 3) = (0.13)(0.13) = 0.0169$$

$$P(2 \text{ AND } 3) = (0.04)(0.13) = 0.0052$$

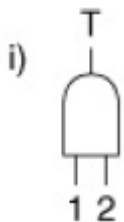
$$P(1 \text{ AND } 4) = (0.13)(0.34) = 0.0442$$

$$P(2 \text{ AND } 4) = (0.04)(0.34) = \underline{0.0136}$$

$$\text{Total } 0.0799$$

For this case This compares to the exact result of 0.0702 obtained using the actual fault tree

Given the fault tree gates shown in Figure and the following set of failure probabilities:



$$a) P(T) = P(1) P(2)$$

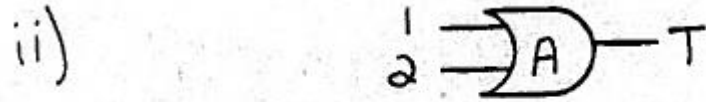
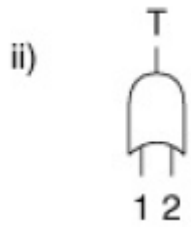
b) Minimum cut sets: $\bar{1} \quad 2$

$$P(T) = P(1) P(2)$$

SAME AS ABOVE

$$c) P(T) = P(1) P(2)$$

$$= (.1) (.2) = \underline{0.02}$$



a) $P(T) = P(1) + P(2) - P(1)P(2)$

b) Minimum cut sets: ~~A~~ 1

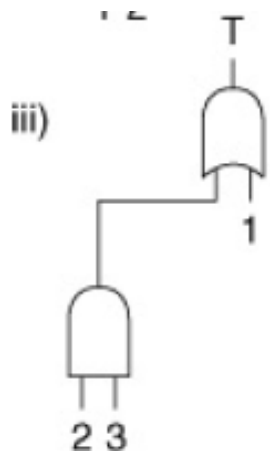
2

$$P(T) = P(1) + P(2) - P(1)P(2)$$

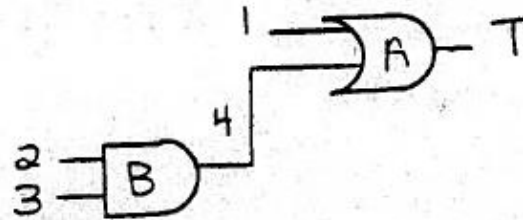
SAME AS ABOVE

c) $P(T) = P(1) + P(2) - P(1)P(2)$

$$= (.1) + (.2) - (.1)(.2) = \underline{0.28}$$



iii)



a) $P(T) = P(1+4) = P(1) + P(4) - P(4)P(1)$

$$= P(1) + P(2)P(3) - P(2)P(3)P(1)$$

$$P(1) + P(2)P(3) - P(2)P(3)P(1) = (0.1) + (0.2)(0.3) - (.2)(.1)(.3)$$

$$= .16 - .06 = \underline{\underline{.154}}$$

Relationship between Fault Trees and Event Trees

Both are used together to produce a complete picture of an incident, from its initiating causes all the way to its final outcome.

Disadvantages of Fault Trees

- Reasonably complicated process the fault tree will be enormous.
- Fault trees involving thousands of gates and intermediate events are not unusual. Fault trees of this size require a considerable amount of time, measured in years, to complete.
- never be certain that all the failure modes have been considered.
- Assume that failures are “hard,” that a particular item of hardware does not fail partially.
- Developed by different individuals are usually different in structure
-

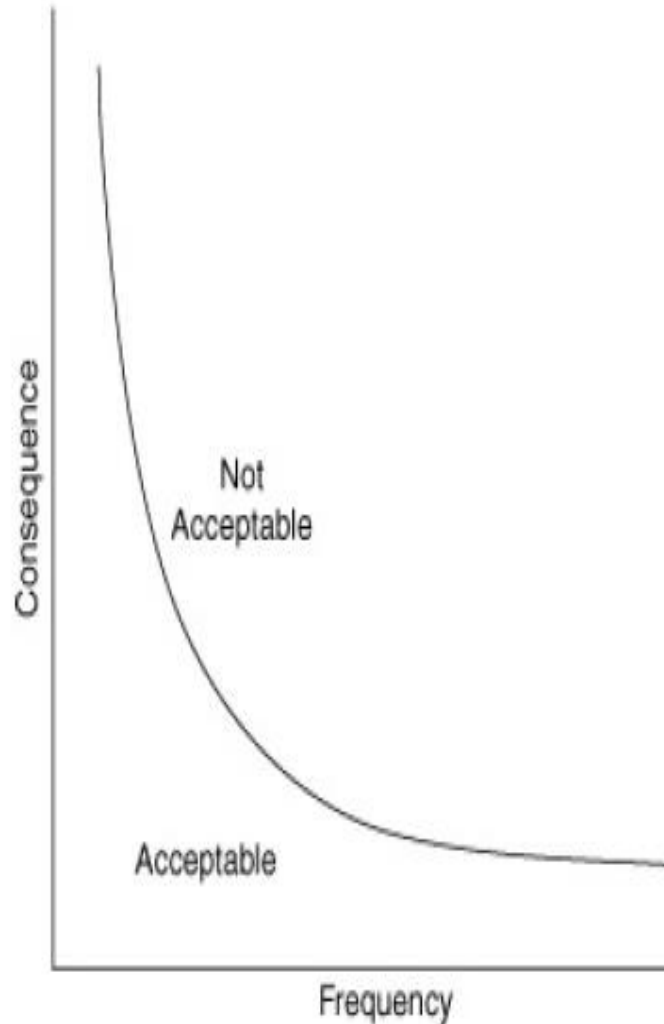
Advantages of Fault Trees

- It begins with a top event. This top event is selected by the user to be specific to the failure of interest.
- This is opposed to the event tree approach, where the events resulting from a single failure might not be the events of specific interest to the user.
- Software is available for graphically constructing fault trees, determining the minimal cut sets, and calculating failure probabilities.

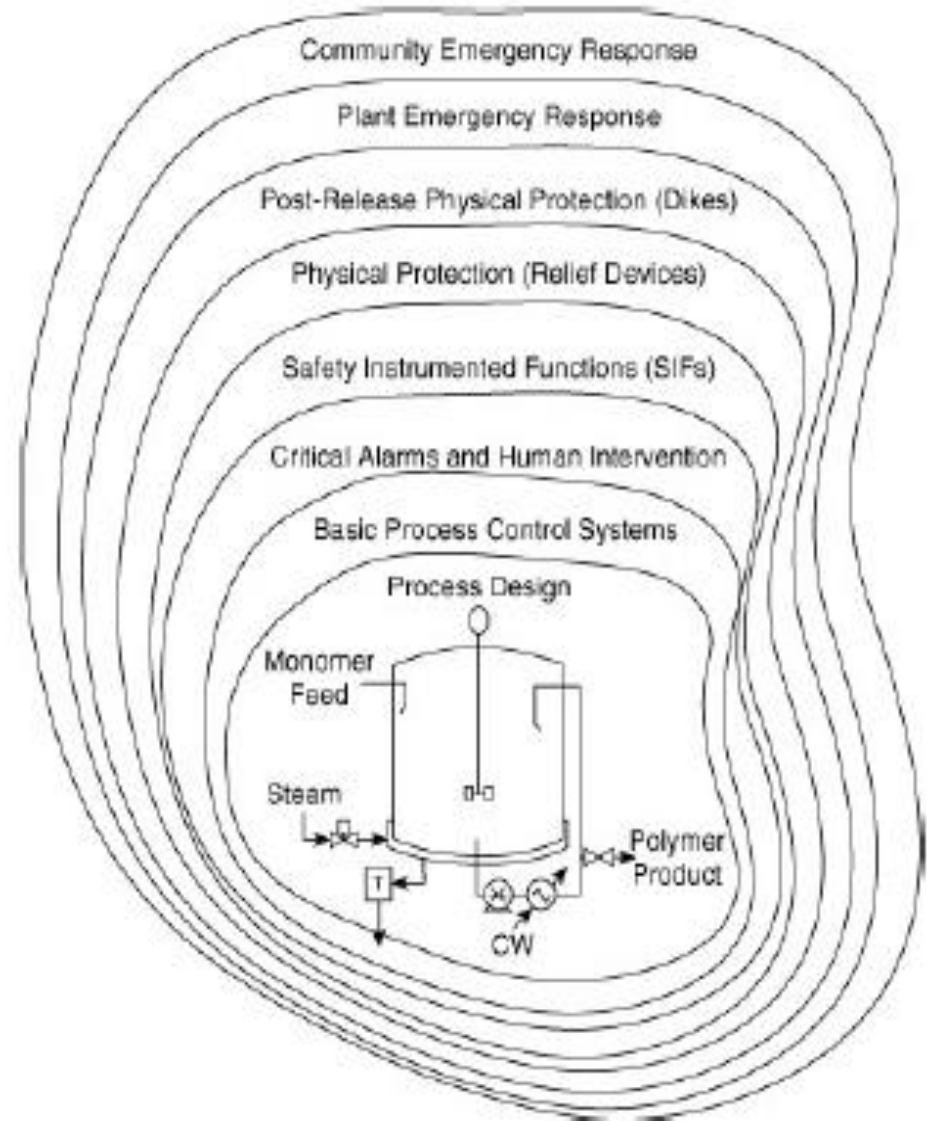
QRA and LOPA

- Risk is the product of the probability of a release, the probability of exposure, and the consequences of the exposure.
- The actual risk of a process or plant is usually determined using quantitative risk analysis (QRA) or a layer of protection analysis (LOPA).
- In both methods the frequency of the release is determined using a combination of event trees, fault trees, or an appropriate adaptation.

General description of risk



Layers of protection to lower the frequency of a specific accident scenario



Quantitative Risk Analysis

- QRAs are used to evaluate potential risks when qualitative methods cannot provide an adequate understanding of the risks.
- QRA is especially effective for evaluating alternative risk reduction strategies.

In general,

QRA is a relatively complex procedure that requires expertise and a substantial commitment of resources and time.

In some instances this complexity may not be warranted; then the application of LOPA methods may be more appropriate.

Layer of Protection Analysis

- LOPA is a semi-quantitative tool for analysing and assessing risk.
- The combined effects of the protection layers and the consequences are then compared against some risk tolerance criteria.
- In LOPA the consequences and effects are approximated by categories
- Thus the results of a LOPA should always be more conservative than those from a QRA.
- If the LOPA results are unsatisfactory or if there is any uncertainty in the results, then a full QRA may be justified.

THANKS