

# SKF4163: Safety in Process Plant Design

## Risk Assessment

Mohammad Fadil Abdul Wahab

*Faculty of Petroleum and Renewable Energy Engineering*



# Risk

- Risk is a product of
  - The probability of failures (e.g. related to frequency of release of toxic chemical, explosion, fire etc.)
  - and
  - The consequence of failures (e.g. death, injury, illness, damage to equipment/environment etc.)
- Risk can be evaluated/measured
  - Using Risk Rating (such as in CHRA)
  - In Term of Number of Potential Fatalities
  - Individual risk
  - In term of amount of release/damage using category (See LOPA)

# Risk Calculation Method in Term of Fatalities

- Risk can be measured using the expected number of fatalities per year,
- The expected annual number of fatalities is calculated from combination of all possible release events as described by the following equation :

- $Risk = E (F) = \sum [P_i \cdot E_i (F)]$       Expected number of fatalities per year

$$P_i = 1 - e^{-\mu t}$$

Probability of occurrence of release event  $i$

Where,

$\mu$  = failure rate or frequency of failure of event  $i$  per year.

$E_i(F)$  = Expected number of fatalities due to release event  $i$   
 = Consequences or Severity of event  $i$

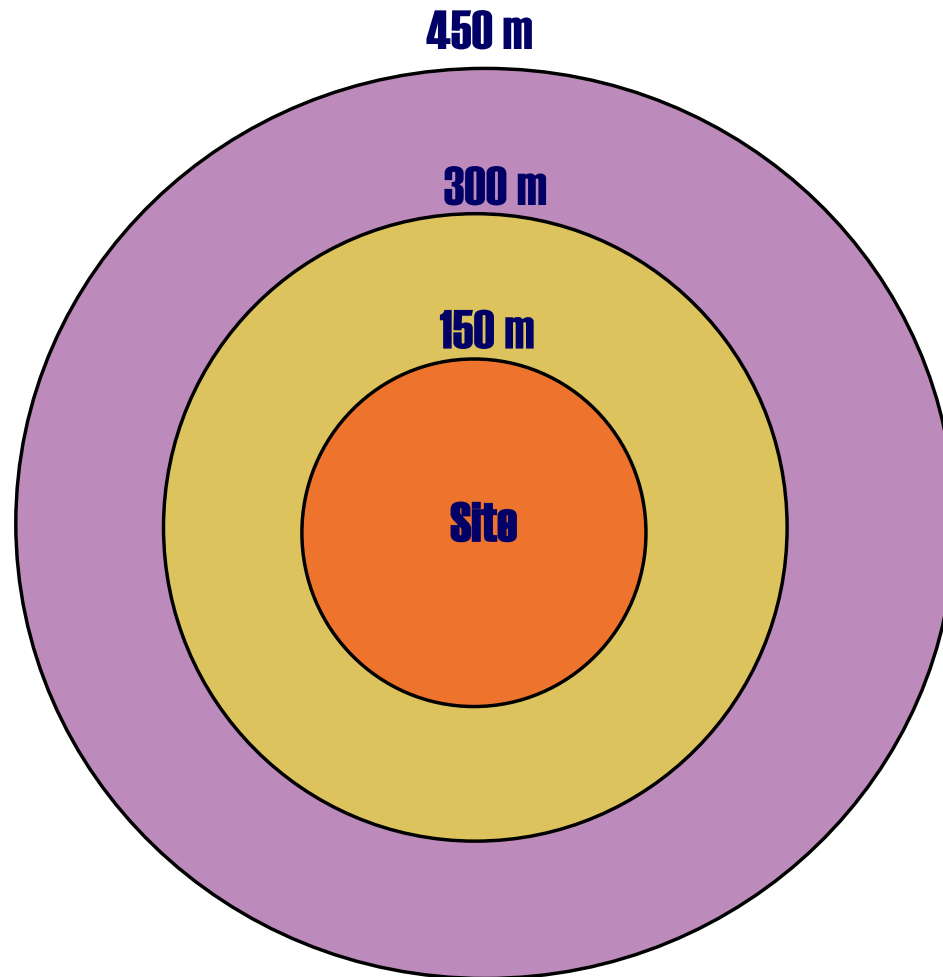
# Individual Risk Calculation Method

- Individual risk ( $R_I$ ) is measured by the average annual risk level of the population potentially exposed to the accident.

$$R_I = E(F_a) / N_t$$

- $N_t$  is the total number of population exposed within a hazard zone.
- Unit: Death per person per year

# Example Risk Contour



## LEGEND Individual Risk Contour



$2.45 \times 10^{-4}$  death per  
person per year



$3.06 \times 10^{-5}$  death per  
person per year



$2.55 \times 10^{-5}$  death per  
person per year

# Voluntary & Involuntary Risk

Voluntary risk are exposure to activities such as

Smoking, football, rock climbing, flying in the commercial or private aircraft, driving or riding in an automobile, and working in an industrial facility.

Involuntary risk are

Secondary smoker, lightning strike, disease, typhoons, and population in residential or recreational areas near the industrial facilities.

## Acceptable Risk?

Risk associated with the chemical plants includes industrial site and surrounding residential area.

Industrial workers are classified as voluntary risk recipients.

Persons living in surrounding area are classified as involuntary risk recipients.

According to Starr (1969,1977), society acceptance of voluntary risk is approximately the same as its acceptance of death by disease.

Each company decides its level of acceptable and unacceptable risk (due to its operation).

# Risk assessment covers,

- Incident identification
  - How it occurs<sup>1</sup>
  - Probability of occurrences
- Consequence analysis
  - Include the qualitative or quantitative assessment of expected fatalities/damage.
    - Loss of life
    - Damage to environment
    - Damage to capital equipment or properties<sup>2</sup>
    - Days outage<sup>2</sup>
- Complexity of assessment depends on the assessment method and process.

Note: 1. HAZOP  
2. DOW FE&I, MPPD and MPDO are simple versions



# Quantitative Risk Analysis (QRA)

- Risk assessment of a process plant is usually called Quantitative Risk Analysis (QRA) and it can be quite comprehensive and complex for a chemical plant.
- In general, QRA is relatively complex procedure that requires expertise (knowledge & experience), commitment, resources and time.
- An example of a simplified QRA is Layer of Protection Analysis (LOPA)

# Purpose of QRA

- To identify where operations, engineering, or management system can be modified to **reduce** risk
- A tool for managers to evaluate the overall risk of a process.
- QRA could be used at the conceptual review and design phase and maintained throughout the life of the plant.

# Scope of QRA

- QRA includes
  - Defining the potential event sequences and potential incidents
  - Evaluating the incident consequences (e.g. using dispersion modeling and fire & explosion modeling)
  - Estimate the potential incident frequencies using event trees or faults trees methods
  - Estimate the incident impacts (consequences) on people, environment, and property
  - Estimate the risk level by combining the incident impacts (consequences) and frequencies (use graph similar to Figure 11-15)

# Estimate The Potential Incident Frequency

- Probabilistic Methods,
  - Event Trees Method
  - Fault Trees Method
- For this, we need to understand a little bit about probability of failure

## EQUIPMENT FAILURES

### Reliability ( $R$ )

Reliability is a probability of a component or system of an equipment WILL NOT fail, and is given by Poisson distribution,

$$\underline{R(t) = e^{-\mu t}}$$

$t$  is time

$\mu$  is average failure rate in faults/time

The value of  $R$  is between 0 and 1 per unit time.

$$\text{As } t \implies 0, \quad R \implies 1$$

$$\text{As } t \implies \infty, \quad R \implies 0$$

The larger the value of  $\mu$ , the faster  $R \implies 0$

Note:  $\mu$  is also known as frequency of failure of a component or a system.

For a component (e.g. pump)  $\mu$  is determined from actual failure rate data of that component.

Here we assume the value of  $\mu$  is constant.

Also lets define,

**Mean Time Between Failures (MTBF)**

$$\text{MTBF} = 1/\mu$$

Unit: time such as year

This is the average expected time for the component or system to fail.

# Failure Probability

Failure Probability (P) or Unreliability is,

$$\underline{P(t)} = 1 - R(t) = 1 - e^{-\mu t}$$

$$\text{As } t \implies \infty, \quad P \implies 1$$

$$\text{As } t \implies 0, \quad P \implies 0$$

The value of P is between 0 and 1 per unit time.

The larger the value of  $\mu$ , the faster  $P \rightarrow 1$

# Components' Failure Interaction

Plant accidents result from interaction of a number of process components,

Two types of components' failure interaction,

- a. Parallel interaction
- b. Series interaction



## a. Parallel interaction

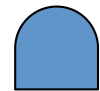
For process/system failure resulting from parallel interaction (simultaneous failures) of a number of components, failure probability is

$$P = \prod_{i=1}^n P_i = P_1 P_2 P_3 \dots P_n$$

or

$$R = 1 - \prod_{i=1}^n (1 - R_i)$$

*Represented as AND gate in fault trees logic diagram*



The failure of the system requires the failure of all components simultaneously

## b. Series interaction

For process failure resulting from failure of a component in series,

$$R = \prod_{i=1}^n R_i$$

or

$$P = 1 - \prod_{i=1}^n (1 - P_i)$$

*Represented as OR gate in fault trees logic diagram*



i.e. The failure of one component leads to the total system failure

# Event Trees

- To estimate the potential incident frequencies in QRA.
- Start with initiating event (e.g. loss of cooling) and work towards final consequences
- Useful for providing scenarios of possible failure modes
- Can estimate failure frequency if data available (failure rate etc.) for every safety function
- Could be extremely detailed with huge event tree.

## Steps in Event Trees

- Identify an initiating event (A)
- Identify the **safety functions** designed to deal with the initiating event.
- Write the safety functions across the top page in the order they logically occur and
- Give lettering notations (identifiers) for the safety functions (e.g. B,C,D,E)

- Write the failure rates of each safety function

For example,

High temp alarm has a failure rate of 1% upon Demand

i.e. 0.01 failures/demand



Operator fail to notice high temperature at 25% of the time

i.e. 0.25 failures/demand

Note: these data might not be available, this is where experience and good judgment required

- Construct the event tree,
  - Start from left to right
  - The initiating event written first, give a letter notation (e.g. A), and write its occurrence frequency below the line.
  - From this draw line to the first safety function
  - Branch UPWARDS and to the right to the next safety function if successful safety operation
  - Branch DOWNWARDS and to the right to the next safety function if safety operation fails
  - No branching if safety function does not apply.

- Compute frequency of failure (lower branch)  
Occurrence frequency  $\times$  (failures/demand)
- Compute frequency of success (upper branch)  
Occurrence frequency  $\times$  (1 - failures/demand)
- with the new values of occurrence frequency written below the lines.

- Describe the resulting accident event sequences on the extreme right-hand side of the event tree (under Result).
- The line end with either open circle (safe condition)  or circle with cross (unsafe condition)  .
- The net failure frequency is the sum of the frequency of the unsafe conditions.

Possible improvement,

Install a high temperature reactor shutdown system that has a failure rate of 10%.


note: The shutdown temperature is higher than the alarm temperature






# Fault Trees

Deductive method.

Start from top events and work backwards (or downwards) to identify various input events (basic or intermediate) that cause the failures (hardware/software failures, human errors)

Basic events are the causes that could not be defined further, denoted by circles 

Intermediate events are the causes that can be defined further, denoted by rectangles. 

The input events passes through logic gate (OR or AND) that identify whether the events interact in series or parallel  



Once the fault tree completed, the probability of top event can be calculated.



# Before Drawing a Fault Tree

- 1. Define precisely the top events such as ‘Damage due to over pressure’  
Note: Avoid event that vague such as ‘explosion of reactor’
- 2. Define the existing event. What conditions are sure to be present when top event occurs? E.g. ‘high pressure process’ .
- 3. Define unallowed events that are unlikely or are not under consideration at the present such as wiring failures, lightning strike, tornadoes, hurricanes etc.
- 4. Define the physical bounds of the process. What components are to be considered in the fault tree.
- 5. Define equipment configuration. What valves are open or closed? What are the liquid level? Is this normal operation state?
- 6. Define the level of resolution. Will the analysis consider just a valve or will it be necessary to consider the valve components?

# Drawing a Fault Tree

- 1. Place top event at the top of the page (in a rectangle box and label it as top event)
- 2. Determine the events that contribute to the top event.
- 3. Determine whether these events are intermediate or basic.
- 4. If these events are related in parallel, they must be connected by an AND gate. 
- 5. If these events are related in series, they must be connected by an OR gate. 

- 6. Focus to one of the immediate events
- 7. Determine the events that contribute to this immediate event.
- 8. Repeat 3 - 6 for all the intermediate events.
- 9. Continue developing the fault tree to expand any intermediate events until all branches have been terminated by basic, undeveloped, or external events.

# Quantitative Calculations for Fault Tree

Perform the calculation on the fault tree diagram itself.

- The data of failure probabilities for basic, external, undeveloped event has to be obtained or calculated.
- Parallel interaction (AND gate):  $P = \prod P_i$
- Series interaction (OR gate):  $R = \prod R_i$
- Calculate gate by gate until you reach the top gate.

# Minimal Cut Sets

- Give the various sets of events that could lead to the top event.
- Useful for determining the various failure modes in which a top event could occur.
- The failure probabilities are likely to be different among the minimal cut sets.
- The higher failure probability sets are examined carefully to determine for requirement for additional safety systems.
- The minimal cut sets are determined using procedure by Fussell and Vesely (see next example) or Boolean Rules

# Boolean Algebra and Minimal Cut Set

## Boolean Rules

Idempotent Law

$$A+A=A$$

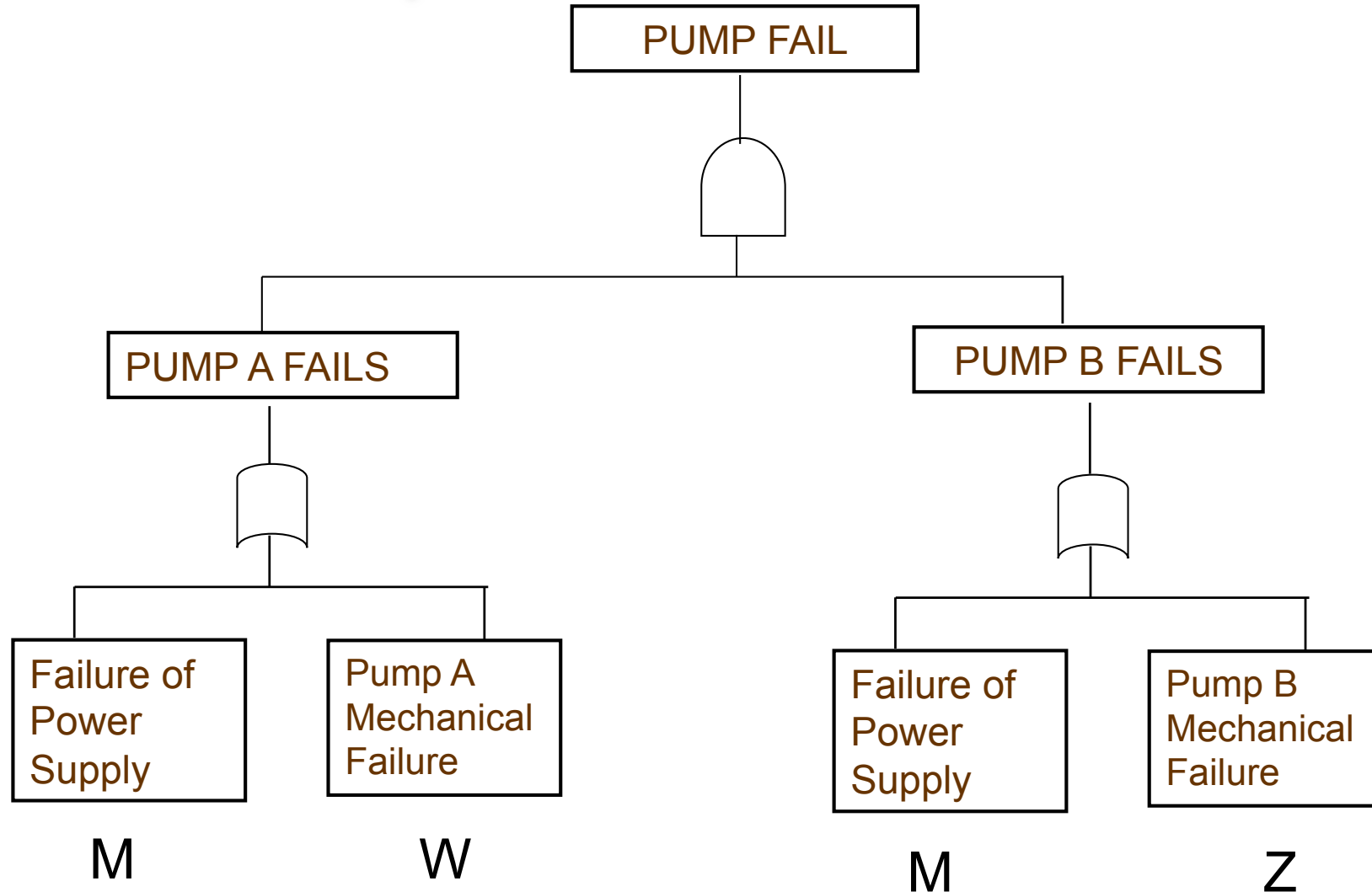
$$A.A=A$$

Absorption Law

$$A+A.B=A$$

$$A.(A+B)=A$$

# Example - Minimal Cut Set





# Boolean Algebra and Minimal Cut Set

Boolean Algebra,  
 $(M+W) \cdot (M+Z)$   
 $= M.M + M.Z + W.M + W.Z$

Apply Idempotent and  
 Absorption Laws

$$= M + M.Z + W.M + W.Z$$

$$= (M + M.Z + M.W) + W.Z$$

$$= (M + M.W) + W.Z$$

$$= M + W.Z$$

**A CUT SET** = combination of  
 basic events which will produce  
 TOP EVENT

In the example :

M, M.Z, W.M, W.Z are all cut sets

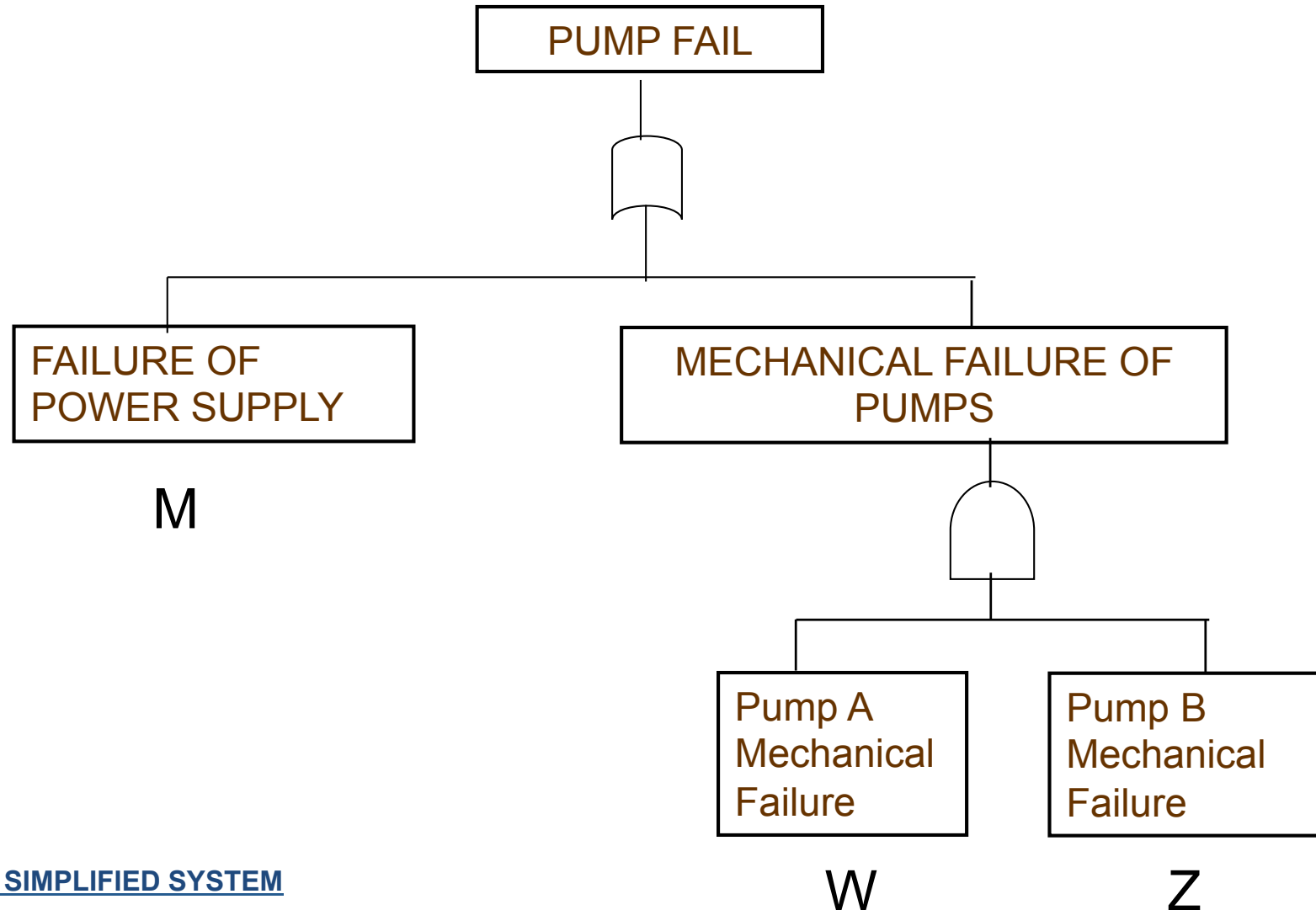
But

Minimal CUT SET is M and W.Z

.....can redraw the FAULT  
 TREE.....

Note: OR gate is addition  
 AND gate is multiplication

## Redraw using M+WZ



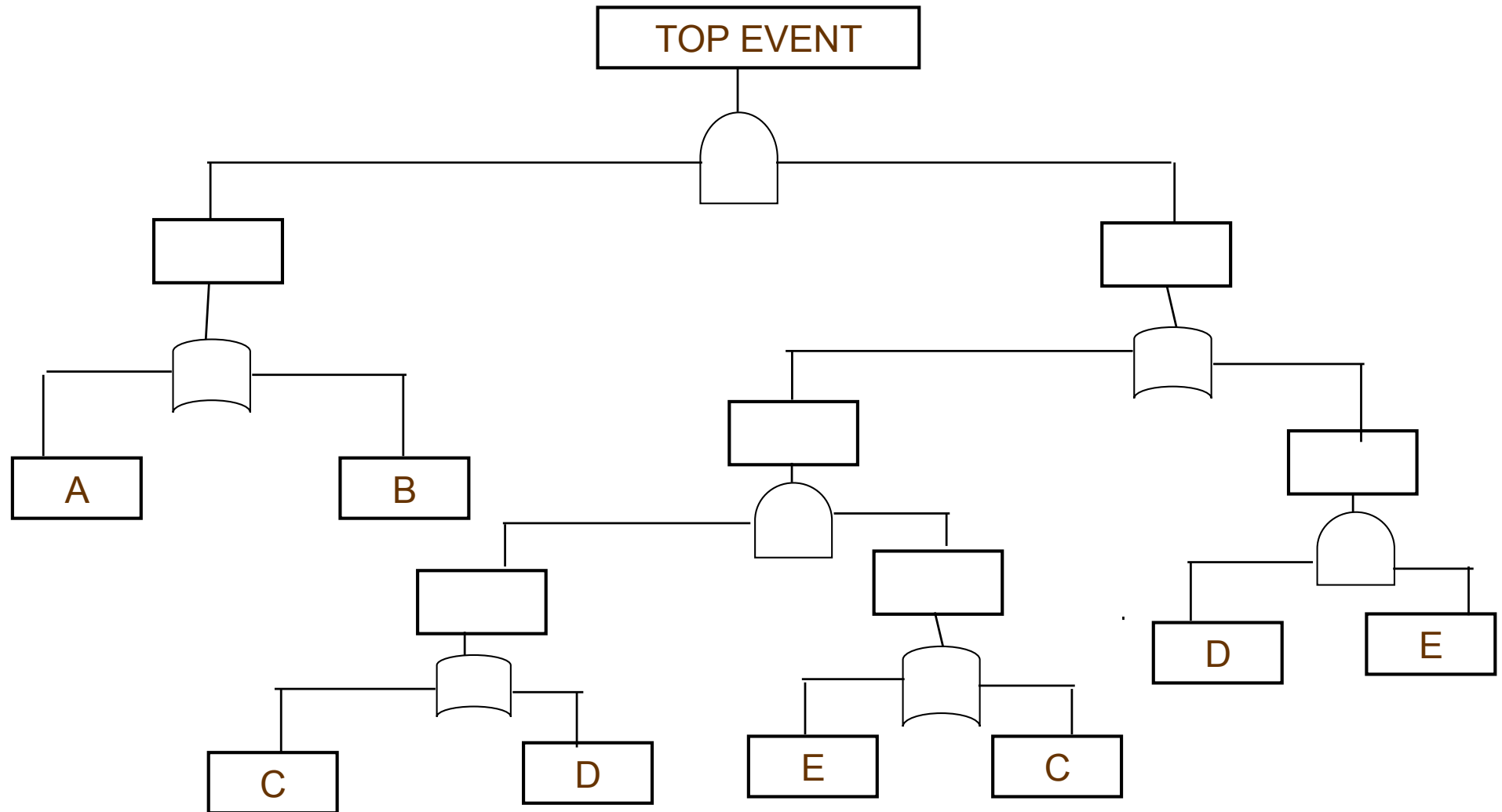
Apply to Example

$$(1+2).(3+4) = 1.3 + 1.4 + 2.3 + 2.4$$

In this case Idempotent and Absorption laws are not needed.

So all the cut sets are minimal cut sets and they are 1.3,1.4, 2.3 and 2.4

# Example

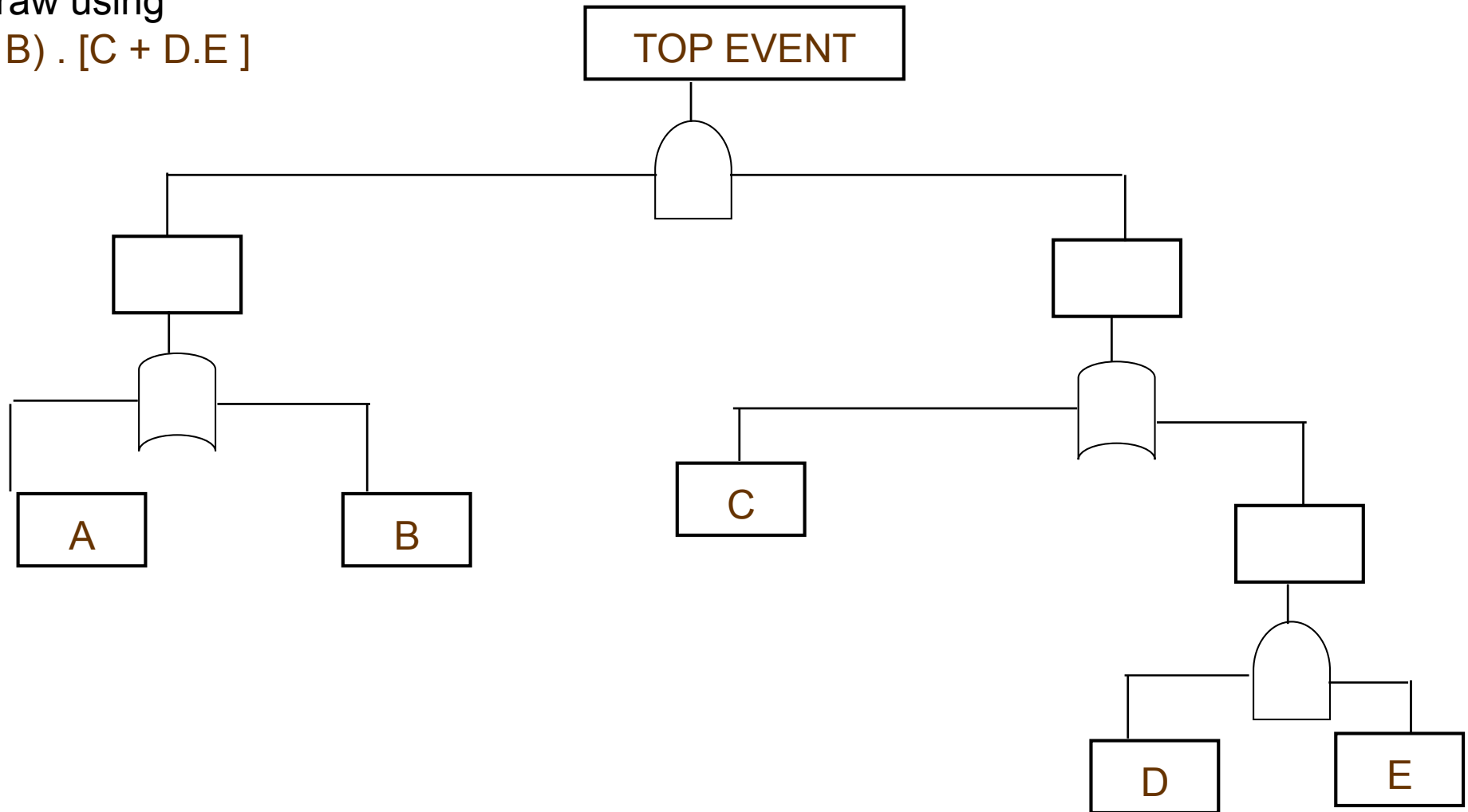


$$\begin{aligned} & (A + B) \cdot [(C + D) \cdot (E + C) + (D \cdot E)] \\ &= (A + B) \cdot [C \cdot E + D \cdot E + C \cdot C + D \cdot C + D \cdot E] \\ &= (A + B) \cdot [C \cdot E + D \cdot E + C + D \cdot C + D \cdot E] \\ &= (A + B) \cdot [C + C \cdot E + D \cdot E + D \cdot C + D \cdot E] \\ &= (A + B) \cdot [C + C \cdot D + C \cdot E + D \cdot E + D \cdot E] \\ &= (A + B) \cdot [C + C \cdot D + C \cdot E + D \cdot E] \\ &= (A + B) \cdot [C + C \cdot E + D \cdot E] \\ &= (A + B) \cdot [C + D \cdot E] \\ &= AC + ADE + BC + BDE \end{aligned}$$

So AC, ADE, BC, BDE are minimal cut sets (4 sets)

# Boolean Algebra - Minimal Cut Set

Redraw using  
 $(A + B) \cdot [C + D \cdot E]$



# Quantitative Calculations for Fault Tree

Perform the calculation using the minimal cut sets

Example ,

Minimal cut sets are (1,3), (2,3),(1,4),(2,4)

The probability of top event can be estimated using special equation of 11.9 (valid for small values of failure probabilities)

$$P = \sum P_i$$

$$P = P(1 \text{ AND } 3) + P(2 \text{ AND } 3) + P(1 \text{ AND } 4) + P(2 \text{ AND } 4)$$

$$= (0.13)(0.13) + (0.04)(0.13) + (0.13)(0.34) + (0.04)(0.34)$$

$$= 0.0169 + 0.0052 + 0.0442 + 0.0136$$

$$= 0.0799$$

Compare to actual fault tree of 0.0702.

# Advantage of Fault Tree

- User could select the top event to be specific to the failure of interest.
- The minimal cut sets provide enormous insight into the various failure modes for top event to occur.
- Minimal cut sets with a product of 4 or more independent failure will increase the reliability of the system.
- Provide a qualitative and quantitative reliability analysis.
- Softwares are available to construct fault tree, to determine cut sets and to calculate the failure probabilities.



# Disadvantage of Fault Tree

- Can be enormous (thousands gate and intermediate events)
- Not necessarily all of failure modes are considered.
- Need experienced engineers
- Assume hardware not to fail partially (such the possibility of valve leak is not considered)
- Assume failure of one component does not put stress on the other components (that could change component failure probabilities).
- External events not correctly treated

# Recommended Use of Fault Tree Analysis

- Suitable for well-defined system
- Normally used to study high-risk scenario
- Essential in Quantitative Risk Assessment (QRA)

# Reference

- Crowl, Daniels A. and Louvar, Joseph F.,  
Chemical Process Safety: Fundamentals with  
Applications, Prentice Hall, 1990, New Jersey,  
USA.