# Question A

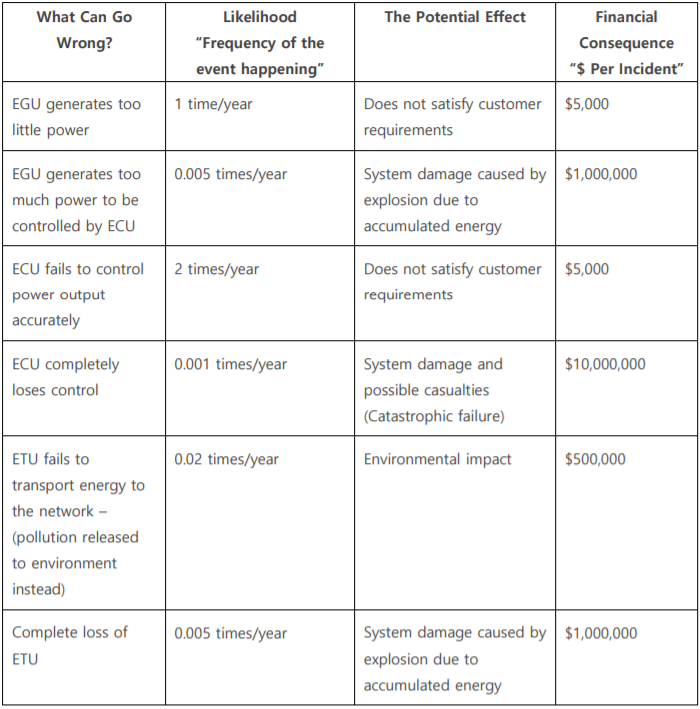
Consider an Energy System (ES) consisting of only the following three Units:

(i) Energy Generation Unit (EGU): Generates energy from fuel inside.

(ii) Energy Control Unit (ECU): Controls energy generation according to requirements.

(iii) Energy Transport Unit (ETU): Transports energy to distribution network

The system would fail if failure of any of the three units occurred. Each unit would fail due to any of its own failure modes or common modes. Other relevant data are as below:



1. Table the Energy System’s failure modes (“What Can Go Wrong”) and determine any potential cause(s) for each (make fair and sound engineering assumptions and write them down).

2. Draw a Fault Tree Diagram for the Energy System failure modes (loss of energy) based on the

“What Can Go Wrong” items given above.

3. Determine a quantitative measure of the potential financial risk (in $/year) associated with

operating this Energy System.

# Question B

The following scenario is for a nuclear power plant system. The Initiating Event (IE) for the Event Tree is “a pipe break in the cooling sub-system” that begins the scenario, with a frequency of once every thousand years. The barriers that are relevant (in the sequence they will be activated) are as below:

1. Electricity: The probability of Electricity being available is 99 out of hundred times.

2. Emergency Core Cooling: The likelihood of Emergency Core Cooling being available is 0.85.

3. Fission Product Removal: The chance of Fission Product Removal failure is 10% of the times.

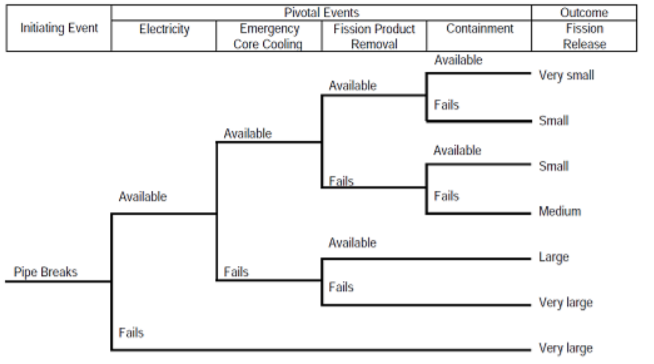
4. Containment: The probability of Containment fails is 1 out of ten times.

You are required to:

• Calculate the probability for a “Large & Very Large Fission Release”,

• Calculate the probability for a “Medium Fission Release”

• Calculate the probability for a “Small & Very Small Fission Release”



# Question C

The causes of a Vehicle headlamp to fail (No Light) are as below:

• Either there is “No Power”; or “Lamp Failure = 1.00E-04/hr”; or “Switch Failure = 1.00E-03/hr”.

• If either “Battery Fails = 1.00E-04/hr” or “Contact Fails = 1.00E-04/hr”, then there would be “No

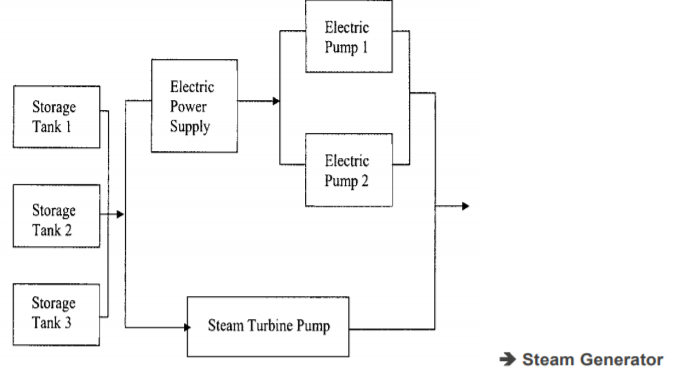
Power”

1. Draw A Fault Tree for the “No Light” as the “Top Event”.

2. Calculate the likelihood of the top even happening “per hour”.

**Question D**

In the event of loss of the main feed water in a Pressurised Water Reactor the reactor system turns tothe backup system, the Auxiliary Feed Water (AFW) supply system, to provide water to the steamgenerator. By neglecting other components such as piping, valves, control systems, etc, a simplified model of the AFW supply system is shown in the figure below:

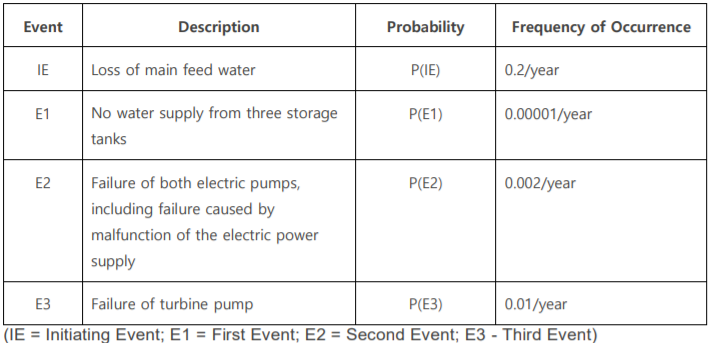


The success of the AFW system requires the following:

• At least one of three of the Storage Tanks

• At least one of the three pumps.

One of the pumps is steam-turbine driven, whereas the other two are electric pumps that depend on the functioning of electric power supply from diesel generators. Assume the following probability data for the initiating event and the system responses:



1: Construct a Fault Tree diagram for the loss of AFW supply system.

2: Construct an event tree for loss of main feed water as an initiating event.

3: From the Event Tree, calculate the likelihood of the loss of the main feed water and AFW supply system failure.

**Question E**

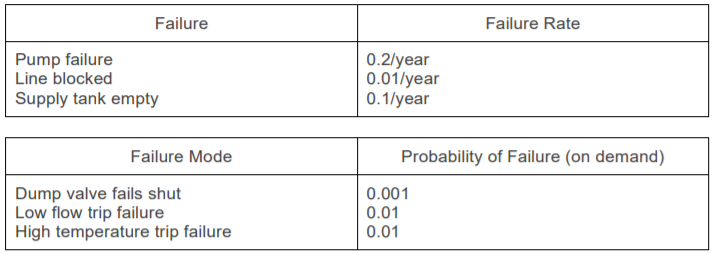
A reactor effecting an exothermic reaction is at risk of thermal runaway in the event of coolant failure. Its protective trip system is intended to open a dump valve, which empties the reactor if low coolant flow or high reaction temperature is detected.

1: Draw a fault tree, which summarises the failure logic analysis given below.

2: Calculate the likelihood of the runaway reaction.

3: Identify the primary failures that the system is most sensitive to (explain)?

Failure Logic Analysis:Runaway reaction occurs if cooling water failure occurs whilst the protective system is inoperative.Cooling water failure can occur because of pump failure, line blockage or an exhausted water supply.The protective system may be inoperative when either the shutdown system fails because the dumpvalve fails shut, or because the detection system fails; the detection system fails when both low coolant flow trip and high temperature trip fail.

Assume a low demand mode of operation for the safety instrumented functions. 

**Question F**

For an electric motor:

1. Draw a fault tree diagram for when the motor “Overheats”.

• The motor overheats either because of a “Primary Motor Failure – Over heated), or an “Excessive Current Thru Motor”.

• The “Excessive Current Thru Motor” happens when both the “Fuse fails to Open” and an “Excessive Current in Circuit”.

• The “Fuse fails to Open” due to the “Primary Fuse Failure – Closed”.

• The “Excessive Current in Circuit” is due to either “Primary Wiring Failure – Shorted” or “Primary Power Failure – Surge”.

2. What is the likelihood of a motor “Overheats” if knowing that:

• Primary Motor Failure – Over heated: Rate = once a year

• Primary Fuse Failure – Closed: Probability = 0.01

• Primary Wiring Failure – Shorted: Rate = once every hundred years

• Primary Power Failure – Surge: Rate = once in ten years

**Question G**

The following situation is an example for a fire detection and suppression system in an office building. The Initiating Event (IE) for the Event Tree is “fire starts”, with a frequency of once every hundred years. The barriers that are relevant (in the sequence they will be activated) are as below:

1. Fire flame/rise in temperature detection: The probability of fire flame/thermal (rise in

temperature) detection system to work is 95 out of hundred times.

2. Fire Alarm system: The likelihood of the Fire Alarm system to work is 0.8.

3. Fire Sprinkler System: The chance of Fire Sprinkler (protection) System to work is 85% of the

times. You are required to:

• Draw an Event Tree to demonstrate the above scenario.

• Calculate the probability for Death/Injury (extensive damage)

• Calculate the probability for limited damage.

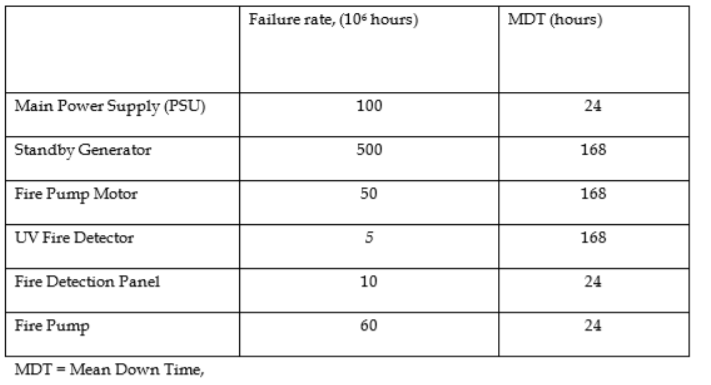
**Question H**

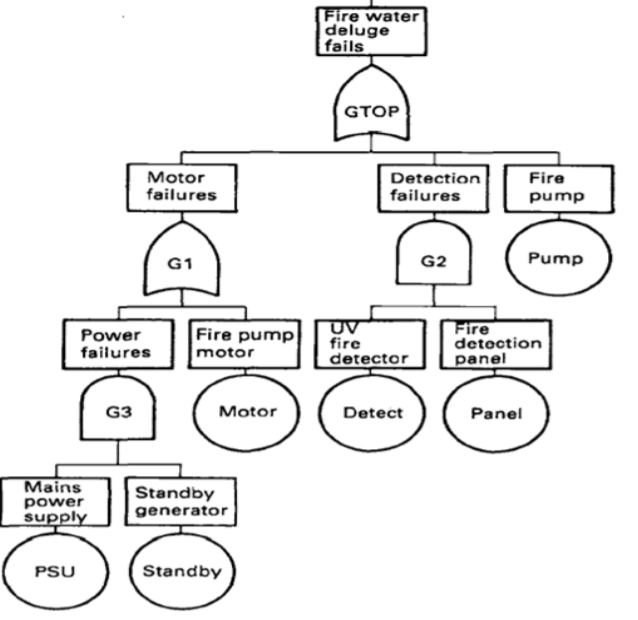
Figure below shows a typical fault tree modelling the loss of “Fire Water Deluge System”. The loss

arises from the failure of a pump, a motor, the combined detection system (UV fire detector / detection panel), and the combined failure of both power sources.

Evaluate the frequency of the top event (lambda / failure rate) and MDT for the failure logic modelled. You are required to show all the working outs (calculations).

Assume the following basic event data:





**Notes:** The failure rate “output” of an AND gate:

(failure rate\_1) x (failure rate\_2) x (MDT\_1+MDT\_2)

The MDT “output” of an OR gate is the weighted average of the two MDTs weighted by failure ate:

[(MDT\_1 X failure rate\_1) + ((MDT\_2 X failure rate\_2)]/[ (failure rate\_1) + (failure rate\_2)]

The MDT “output” of an AND gate is multiple of individual MDTs divided by their sum:

[(MDT\_1 X MDT\_2]/[MDT\_1 + MDT\_2)]

[If interested more, please refer to “Reliability, Maintainability and Risk” by Dr David J Smith.]