Federation University | School of Engineering, IT and Physical Sciences

MREGC5007

RISK ENGINEERING

2023
Study Guide

Prepared by
Dr. Kyoumars Bahrami,
Sessional Academic

Federation University

School of Engineering, IT and Physical Sciences

Prepared by:
Dr Kyoumars Bahrami for the School of Engineering, IT and Physical Sciences, Federation University, in conjunction with the Off-Campus Learning Centre, Federation University, k.bahrami@federation.edu.au.

Produced and Published by:
Off-Campus Learning Centre,
Federation University,
Churchill, Victoria, Australia, 3842

Revised July 2023

This off-campus learning material is for a study course that is part of one or more of the Fed Uni postgraduate programs in Maintenance and Reliability Engineering. These comprise the Graduate Certificate in Maintenance Management, Graduate Certificate in Reliability Engineering, Graduate Diploma of Engineering Maintenance Management, and the Master of Maintenance and Reliability Engineering.

It has evolved over some years of offering these courses. The material is reviewed each year and updated. Some Reader resource items are retained despite their age because they are considered to be of ongoing value to students.

If you are not a student, you are invited to consider enrolling in one of our programs. Studies run full year, starting in late February, and each course has an associated website. You can see the latest details on the School website. For further information, contact the Coordinator of the programs: Dr. Gopinath Chattopadhyay – g.chattopadhyay@federation.edu.au (or phone +61351228629; +61402467737)).

Contents

Introduction to MREGC5007

Welcome to the course MREGC5007: *Risk Engineering*

The risk management process is the systematic identification, analysis, assessment, treatment, monitoring and communication of risks. The application of engineering principles and methods as part of the risk management process is termed **risk engineering**.

Risk engineering utilises the logical/methodical approach to identify hazards, and attempts to resolve the root cause so that some degree of control measure (mitigation) can be applied to reduce the risks to acceptable levels. There are many techniques that can be used for risk engineering including:

a. Fault Trees Analysis (**FTA**).
b. Event Trees Analysis (**ETA**).
c. Failure Modes and Effects Analysis (**FMEA**).
d. Failure Modes, Effects and Criticality Analysis (**FMECA**).
e. HAZard and OPerability study (**HAZOP**).
f. Reliability Block diagram (**RBD**).

The Course includes:

- This Course Guide

- A **Course Book** designed to bring the student up to date with the state of knowledge and practice in the subject of Risk Engineering. Sections in the Course Book that indicates how the student can extend his/her knowledge and skills by further study and reading on the subject. Exercises that give the student an opportunity to apply the techniques described to his/her own work. These exercises are designed to reinforce the student's learning of the course material, and to verify that this learning process has been effective.

- A **Reader** that contains selected articles and book sections/chapters that provides a range of views and materials on the subject.

As I could not choose one single book (as the textbook) that covers all the relevant Risk Engineering topics and techniques, I decided to put together the course **Reader**.

You are not expected to read & understand all the **Reader** contents though!

The **Reader** contains a lot of risk engineering related materials from different sources that can be used as a reference and additional source of readings. I have also placed additional relevant materials on the course **Moodle** – for those of you who enjoy reading!

Context of this course

Most of you will study this course as part of the Federation University postgraduate programs in Maintenance and Reliability Engineering. If you are studying this course on its own, then I suggest that it would be worthwhile for you to have a look at books on reliability engineering and maintenance management in general, to see where the topics here fit into context.

Introducing your Course Adviser

Dr Kyoumars Bahrami is currently working as Safety & Reliability SME in the rail industry.

His career has included over twenty-five years of experience in Process & Systems Safety and Reliability Engineering areas in a wide range of safety critical industries (Railways and Oil & Gas).

Kyoumars holds a PhD qualification degree from Monash University, Australia; an MSc degree in Mechanical Engineering from the University of Oklahoma, USA; and a BSc degree in Engineering from Shiraz University, Iran.

His major achievements are:

* Contribution to the “Handbook of RAMS in Railway Systems: Theory and Practice”, March 2018 (CRC Press).

* Member of the RISSB Standards and Guideline Development Groups (e.g., Systems Safety Assurance, RAM for Railways, Condition Monitoring,

* Fellow of the Institution of Engineers Australia (**FIEAust**),

* Engineers Australia Chartered Professional Engineer (**CPEng**)

* Exida Certified Functional Safety Expert (**CFSE**),

* TUV certified Functional Safety Engineer (**FSE**),

* Member of the UK based IET Independent Safety Assurance (ISA) Working Group.

* Approved Assessor for Major Hazard Facilities – Australian Government (Comcare)

* Review board for Asset Management Council “AMPEAK Asset Management Conference”.

* Review board for the Australian System Safety Conferences.

* Contribution to the development of ‘National Safety and Health Risk Assessment Guideline - Minerals Council of Australia.

* Member of Australian Safety Critical Systems Association (ASCSA);

* Member of Asset Management (Reliability & Maintenance Engineering) Society of Australia

How to contact your Course Adviser

Do not hesitate to contact Kyoumars if you have any questions, are getting into difficulties with your studies, or simply want to share some information and experience you’ve gained in your workplace in the areas of risk engineering.

The best and easiest way to contact me is by email: **k.bahrami@federation.edu.au**

Course aims and objectives

Objectives

The objective of the Risk Engineering course is to provide practising engineers with a ready means of enhancing and updating their professional knowledge and skills. To this end, the course is designed to actively involve the student in the learning process.

The course addresses the need of industry to improve the management of resources associated with short- and long-term risk to people, assets, production and the environment. The course provides further studies for graduates from all branches of Engineering, Applied Sciences and Business who wish to gain more specialist knowledge in Risk Engineering and Management.

Among objectives of this course are also to:

- disseminate knowledge about risk engineering techniques and methodologies;
- develop a basic understanding of selected engineering management techniques as applied to risk analysis;
- help students in learning to provide expert risk engineering advice to industry, government and the community as required;
- develop the ability to be pro-active in the management of risk in your organisation, and to be a leader rather than a follower.

Aims

When you have successfully completed this course, you should have developed the ability to:

- identify engineering hazards;
- quantify the probabilities and consequences of identified hazards;
- establish priorities for the control of identified hazards;
- control and/or reduce the consequences of engineering hazards;
- select and apply the most appropriate risk engineering techniques; and
- manage risk in a pro-active way.

Course overview

Study Guide 1

In your Course Book, Study Guides, the following topics are covered:

1. Introduction to Risk Engineering

Human Perception of Risk, Risk Terminology. Some of the International Disasters.

2. Engineering Risk Management

3. Risk and Reliability Mathematics and Modelling

Probability/Derivation of Probabilities, Rules for Combining Probabilities, Probability Distributions. The Reliability of a Product, Reliability of Systems/Reliability Block Diagrams (RBD), An Introduction to Monte-Carlo Simulation, Simulating Time in Monte-Carlo Modelling.

4. Hazard Identification

Introduction to Hazard Identification, Hazards in the Process Industries, Hazard Identification Techniques, Preliminary Hazard Analysis (PHA), Hazard and Operability Study (HAZOP), Failure Mode, Effect and Criticality Analysis (FMECA).

5. Modelling of Accidents & Risk Assessment

Introduction to Modelling of Accidents, Event Tree Analysis (ETA), Fault Tree Analysis (FTA), Cause-Consequence Diagrams (CCD), Probabilistic Risk Assessment.

6. Human Element in Risk Assessment

An Overview - Human Reliability Analysis (HRA), Maintenance Errors, The Probability of Human Error.

7. Industrial Hazard and Risk Assessment Case Studies

Hazardous Waste Disposal Facilities, The Channel Tunnel, A Fire Protection System, A Blowout Preventer, Hydraulic Control System, The Ventilation Recirculation System in an Undersea Mine.

8. Emergency Planning, Documentation and Management

General Preparation - Planning, Documentation of the Emergency Plan, Management of the Plan.

9. Recent Issues in Risk Engineering

Offshore QRA, Transport Risks, Safety Management Systems, Chemical Warehouse Storage, The Environmental Effects of Accidents, Safety-Critical Computing Systems.

10. Engineering Risk Management Report Writing

Preparation for Report Writing, Format of the Report, Writing the Report, Oral Presentation.

Study materials

The course study materials are all available online.

They are as below:

- **this COURSE Guide,**
- **the COURSE BOOK,**
- **the COURSE READER (sections of relevant papers and articles).**

As I seek to continuously improve the study material, I would very much appreciate any comments or suggestions for improvements from you at any time, during the year or later.

Textbook

There is no prescribed text for this course – see the Reader.

Study program

I suggest that you draw up a study program to fit with other courses you are studying, considering your work and personal life.

Assessment

Course assessment will be by "*three* assignments" and "*one* final exam". **Assignments and the Exam are compulsory.**

Assignments: 60% of the total Mark,
Examination: Final Exam: 40% of the total mark.

Students are required to achieve at least 45% in the total continuous assessment assignments component, and at least 45% in the final examination component, and an overall mark of 50% or more to achieve a pass grade in the course.

This mean that, to pass the Course, you need to pass **both the "continuous assessment assignments**" and the **"final examination" separately**.

Assignments due dates to through Moodle are:

Assignment No 1	**CoB Friday August 4th**
Assignment No 2A	**CoB Friday September 1st**
Assignment No 2B	**CoB Friday September 29th**

Please check that for the assignments you cover all parts (you don't get marks for what you don't provide and you also don't get marks for what you provide but was not asked for!).

Your assignments will be assessed according to:

- familiarity with the topic being presented;
- application of information which has been supplied during the course;
- evidence of individual research and literature surveys;
- application of original ideas to problems; and
- standard of technical communication, which includes presentation (layout), spelling and grammar.

It goes without saying that you are expected to provide original work and copying from others is not countenanced. You are not to use work documents unless in a minor way to illustrate your views, and this is to be clearly acknowledged.

HD	High Distinction	Outstanding level of achievement	80-100%
D	Distinction	High level of achievement	70%-79%
C	Credit	Satisfactory, sound work	60% - 69%
P	Pass	Just OK – more effort desirable	50% - 59%
N	Fail	Not good enough – more effort is required to pass	Below 50%

Note:

Both the "Mark for Assignments" and the "Mark for the Final Exam" may be subject to normalization adjustments across all students, depending on the class performance.

Submission of assignments

Please submit ONLY one file (preferably in MS Word) for each assignment.

If the work requires an EXCEL spreadsheet, copy and paste the outcomes in MS Word.

Declaration:

Assignments submitted are required to have the following Declaration on the Cover page:

Declaration

- To the best of my belief, no part of this assignment has been copied from any other student's work or from any other source except where due acknowledgement is made in the text.
- No part of this assignment has been written for me by any other person, except where such collaboration has been authorised by the *Course Coordinator* concerned.

Signatures:
Date:

Assignments are submitted in Moodle. This helps for all assignments in Moodle and checking submission dates.

Students still can send an assignment by email only if necessary – with prior approvals.

Write your assignment as a MS WORD document and number the pages.

Use the following as the file name:

- Your complete name (first_second).
- The course code (e.g. MREGC5007).
- Assignment number.

Example: "John_Student_MREGC5007_Ass_1"

Policy on late submission of assignments

Extensions to the due date will be granted for good reasons (e.g. illness or extraordinary work requirements) *if the request is received by me (email), at least* ***a week BEFORE the due date.***
PLEASE READ THAT LAST SENTENCE AGAIN!

Assignments received after the due date (without an approval for extension) will be subject to the following penalties:

(a) One grade per week or part thereof up to two (2) weeks late.
(b) No assessment of the assignment if received later than two (2) weeks after the due date.

Examination

The date of your examination will be notified to you by the university admin nearer the time and will be available via your university Internet portal. It is of three hours and is open book (this means that you can take any paper book or note into the exam **except a computer**).

When you check the portal for your examination information, you will find the details of your venue by clicking on the link in the table that appears. If any problems (e.g. if you have moved away from near the examination location that you notified to us on your initial application form), contact the examinations people (university admin) promptly.

Recommended readings.

A. Books that can be viewed through University Library Internet site

There are many excellent books in the areas of Risk Engineering that can be viewed through University Library website for free!!

Follow the following links:

First go to the library site:

Then Select:	Databases
Then select letter 'k' and look for:	Knovel
Select:	Safety, Health & Hygiene
and then:	Industrial Safety

Now have fun!!

B. Books available at University libraries

These books are available from the University libraries. I ask you to borrow and retain them for as short a time as you need, and return promptly so that they are available to others. You can check to see what is held or available at any time, via the University Library Home Page.

1. *Allianz Handbook of Loss Prevention* (1978). Berlin: Allianz Versicherungs AG (1978 issue in library).
2. Bahr, Nicholas J. *System safety engineering and risk assessment: a practical approach*.
3. Cote, A.E. (2003). *Fire Protection Handbook, National Fire Protection Association*. Quincy.
4. CoVan, James. *Safety engineering*.
5. Covello, V.T. (Ed.) (1986). *Risk Evaluation & Management*. New York: Plenum Press.
6. Haimes, Yacov Y. (1998). *Risk modelling, assessment, and management*, Yacov Y. Haimes (Ed.). New York: Wiley.
7. Hertz, David Bendel (1984). *Practical risk analysis: an approach through case histories*, David Hertz and Howard Thomas (Eds). New York: Chichester, Wiley.
8. Jones, Richard B. (1947). *Risk-based management: a reliability centered approach*.
9. King, R., Magid, J. (1979). *Industrial Hazard and Safety Handbook*. Newnes Butterworth.
10. Kletz, Trevor. *Hazop and hazan: identifying and assessing process industry hazards*.

11. Lees, Frank P. *Loss Prevention in the Process Industries*.

12. Mooney, G.H. (1977). *The valuation of Human Life*. London: Macmillan Press.

13. Pitblado, R. and Turney, R. (Eds). *Risk assessment in the process industries*.

14. Ridley, J. (1986). *Safety at Work*. London: Butterworths.

15. Rowe, W.D. (1985). *An Anatomy of Risk*. Krieger.

16. Sadgrove, Kit. *The complete guide to business risk management*.

17. Samson, D. (Ed.) (1995). *Management for Engineers*. Melbourne: Longman Cheshire (e-book and paper).

18. Viner, Derek (Ed.) (1987). *Risk engineering for public, product and employee safety*. Melbourne: Institution of Engineers, Australia, Victoria Division, Risk Engineering Branch and the National Panel on Risk Engineering.

19. Viner, D. (1994). *Accident Analysis and Risk Control.* Melbourne: VJR Delphi.

C. General references (not available at the University libraries)

1. Baird, B.F. (1989). *Managerial Decisions under Uncertainty: An Introduction to the Analysis of Decision Making*. New York: John Wiley & Sons.

2. Fischoff, et al. (1984). *Acceptable Risk.* Cambridge University Press.

3. Hamer, W. (1989). *Occupational Safety Management & Engineering*. Englewood Cliffs, New Jersey: Prentice-Hall.

4. Merrit, A. (1985). *Guidebook to Australian Occupational Health and Safety Laws*. Sydney: CCH.

5. Rescher, N.A. (1983). *Philosophical Introduction to the Theory of Risk Evaluation & Management*. University Press of America.

6. Schwing, R.C., Albers, W.A. (Jr) (Ed.) (1980). *Societal Risk Assessment, How Safe is Safe.* New York: Plenum Press.

D. Industry standards and guidelines

AS 61508 - Australian Functional safety of electrical/electronic/programmable electronic safety-related systems

AS 61511 - Australian Functional safety of electrical/electronic/programmable electronic safety-related systems for the Process Industry Sector

E. Internet sites

The following are some useful Internet sites related to this course:

1. Risk Engineering Society of Australia
2. Society of Risk Analysis
3. Risk World
4. The American Society of Safety Engineers
5. Risk Analysis and Assessment Research Guide
6. Engineering Disasters: Learning from Failure.
7. IEC Organisation (IEC61508, IEC61511)
8. CENELEC Rail Safety Standards (EN50126, EN50128, EN50129)

ASSIGNMENTS

Always use a **cover sheet** for your assignments. Include your complete name, student ID, and email address.

Assignment 1: 20% of the total course mark

Assignment 1

Note: Please submit your assignment only as "ONE MS Word" document. Please copy and paste any Excel or other format materials into your Word document.

Introduction:

Give a brief description of yourself (qualifications, awards, experience, etc.), the workplace that you are currently / were previously working in. Also identify the main tasks/roles that you are / were normally involved with.

Assignment 1 (a) - 4 Marks

1. Identify at least 10 types of hazards that are to be found in your workplace/industry.

   Hazard: potential source of harm .. a state or set of conditions of a system ... that, together with other conditions in the environment of the system ..., will lead inevitably to an accident (incident)

   Accident: an undesired and unplanned (but not necessarily unexpected) event that results in (at least) a specified level of loss .. ~ the loss event

2. Describe the way in which the hazard manifests itself (e.g., failure mode / types of machinery, equipment or activity in which it is to be found).

3. Identify engineering and other control measures for the hazards (describe prevention / control / mitigation measures).

Hint: See Table 4 given in 'Efficiently Managing Risk', Chapter 2 - Reader Book 2.1 'Occupational Health and Safety', Derek Viner (1988).

1. Hazard	2. Manifestation of the Accident (incident)	3. Control Measures (Engineering and others)

Assignment 1(b) - 4 Marks

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:

What Can Go Wrong?	Likelihood "Frequency of the event happening"	The Potential Effect	Financial Consequence "$ Per Incident"
EGU generates too little power	1 time/year	Does not satisfy customer requirements	$5,000
EGU generates too much power to be controlled by ECU	0.005 times/year	System damage caused by explosion due to accumulated energy	$1,000,000
ECU fails to control power output accurately	2 times/year	Does not satisfy customer requirements	$5,000
ECU completely loses control	0.001 times/year	System damage and possible casualties (Catastrophic failure)	$10,000,000
ETU fails to transport energy to the network – (pollution released to environment instead)	0.02 times/year	Environmental impact	$500,000
Complete loss of ETU	0.005 times/year	System damage caused by explosion due to accumulated energy	$1,000,000

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 only.

3. Determine a quantitative measure of the potential financial risk (in $/year) associated with operating this **Energy System**.

Assignment 1(c): 4 Marks

Discuss the following three items (two page each - supported by a short **literature review):**

1. In your opinion, what degree of **safety risk** is acceptable and why?

2. Give your understanding and opinion on the validity of the idea of keeping risk ALARP?

3. What is your understanding of the *SFAIRP* principle? Is there any difference between ALARP and SFAIRP?

Assignment 1(d): 4 Marks

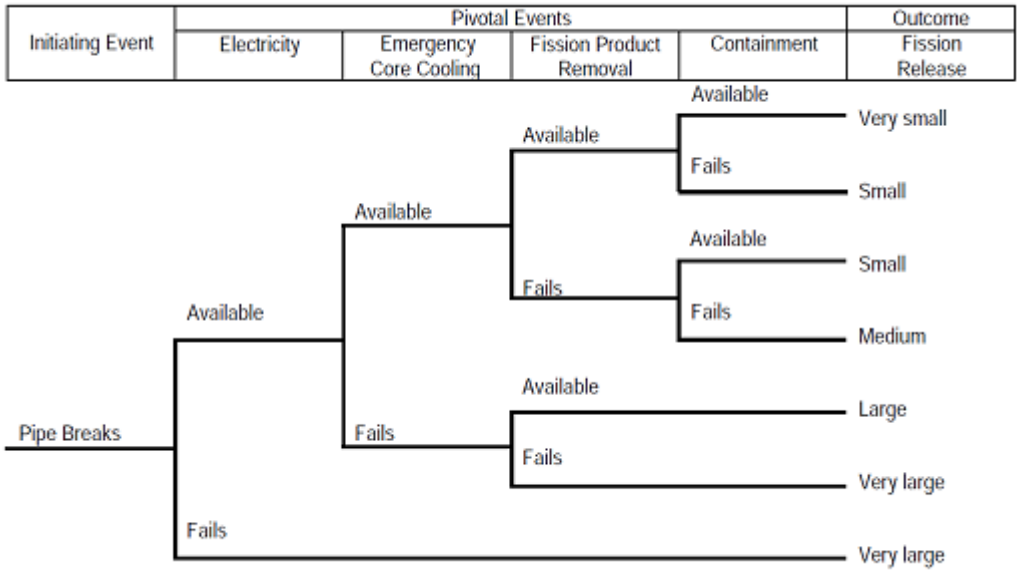
The following scenario is for a nuclear power plant system. The Initiating Event (IE) for the Event Tree is “a pipe break in the cooling sub-system” that begins the scenario, with a frequency of once every thousand years.

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”



Assignment 1(e): 4 Marks

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”.

Assignment 2A: 20% of the total mark

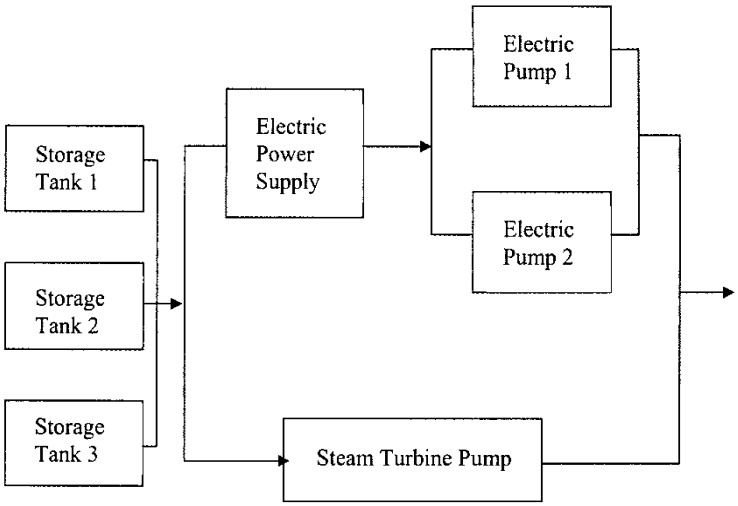
Assignment 2

Note: Please submit your assignment only as "ONE MS Word" document. Please copy and paste any Excel or other format materials into your Word document.

Assignment 2(a): 4 Marks

In the event of loss of the main feed water in a Pressurised Water Reactor the reactor system turns to the backup system, the Auxiliary Feed Water (**AFW**) supply system, to provide water to the steam generator.

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:

Event	Description	Probability	Frequency of Occurrence
IE	Loss of main feed water	P(IE)	0.2/year
E1	No water supply from three storage tanks	P(E1)	0.00001/year
E2	Failure of both electric pumps, including failure caused by malfunction of the electric power supply	P(E2)	0.002/year
E3	Failure of turbine pump	P(E3)	0.01/year

(IE = Initiating Event; E1 = First Event; E2 = Second Event; E3 - Third Event)

2(a).1: Construct a Fault Tree diagram for the loss of AFW supply system.
2(a).2: Construct an event tree for loss of main feed water as an initiating event.
2(a).3: From the Event Tree, calculate the likelihood of the loss of the main feed water and AFW supply system failure.

Assignment 2(b): 4 Marks

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.

2(b).1: Draw a fault tree, which summarises the failure logic analysis given below.
2(b).2: Calculate the likelihood of the runaway reaction.
2(b).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 dump valve 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.

Failure	Failure Rate
Pump failure Line blocked Supply tank empty	0.2/year 0.01/year 0.1/year

Failure Mode	Probability of Failure (on demand)
Dump valve fails shut Low flow trip failure High temperature trip failure	0.001 0.01 0.01

Assignment 2(c): 4 Marks

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 per year.
    - Primary Wiring Failure – Shorted: Rate = once every hundred years
    - Primary Power Failure – Surge: Rate = once in ten years

Assignment 2(d): 4 Marks

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.

Assignment 2(e): 4 Marks

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.

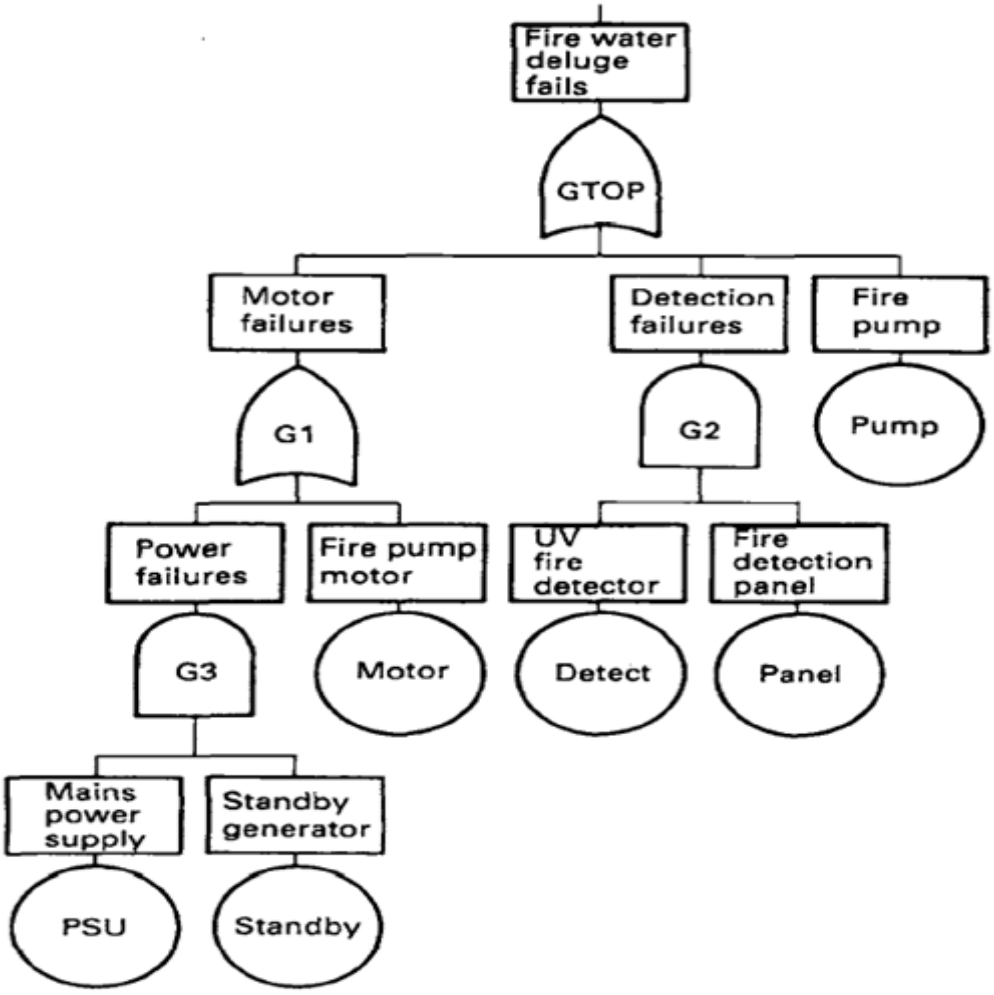
Evaluate the frequency of the top event (lambda / failure rate) and MDT for the failure logic modelled.

You are required to show all the working outs (calculations).

Assume the following basic event data:

	Failure rate, (10^6 hours)	MDT (hours)
Main Power Supply (PSU)	100	24
Standby Generator	500	168
Fire Pump Motor	50	168
UV Fire Detector	5	168
Fire Detection Panel	10	24
Fire Pump	60	24

MDT = Mean Down Time,



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.]

Assignment 2B: 20% of the total mark

Assignment 3

Note: Please submit your assignment only as "ONE MS Word" document. Please copy and paste any Excel or other format materials into your Word document.

Assignment 3(a): 4 Marks

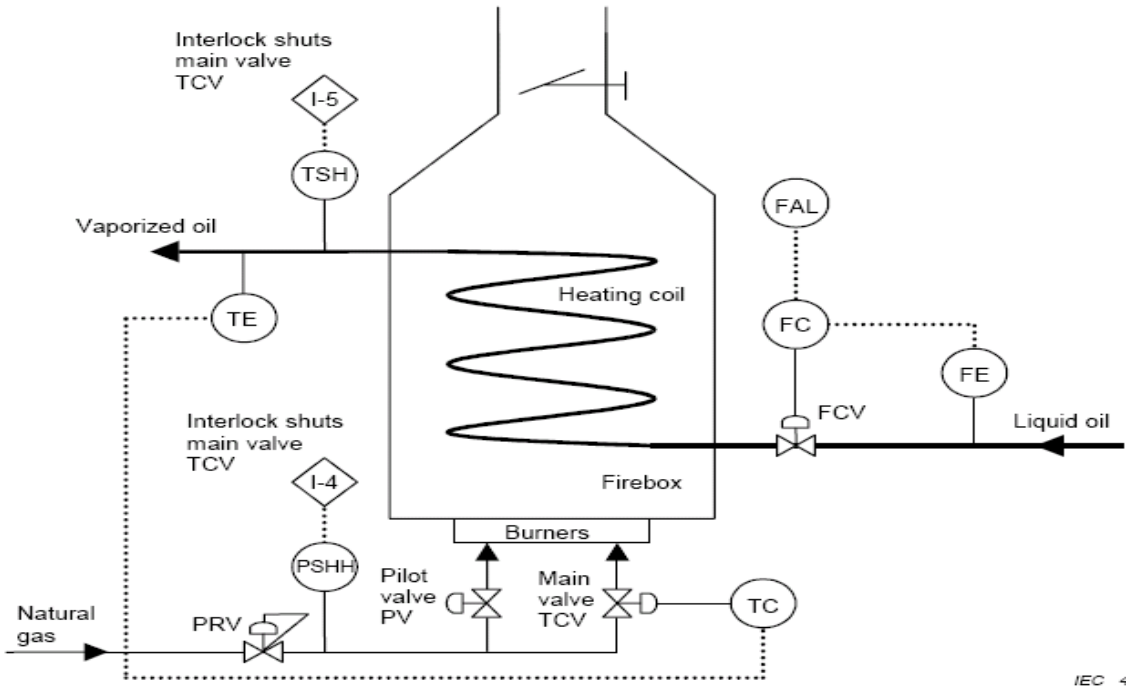
Conduct a complete **FMEA** for the following case:

An aluminium beverage can, which all of us have used, may be described as a pressure vessel when it contains a carbonated beverage, especially under accident conditions when it has been dropped or shaken. The can must be designed as carefully against accidental failure by explosion as does a steam boiler or nuclear reactor vessel, which has strict safety design codes. The successful design of a beverage can depend on avoiding the possibility that it will fail.

Divide the can into four (4) parts, i.e. side, top, bottom and rivet in the pop-top.

Assignment 3(b): 5 Marks

HAZOP: Consider an oil vaporiser that consists of a furnace containing a heating coil and burners, which are fired by natural gas. The oil enters the heating coil as a liquid, is evaporated, and leaves the coil as a superheated vapour. The natural gas entering the burners combines with external air and burns in a hot flame. The combustion gases leave through the stack.



The oil flow is controlled by a flow control set which includes:

- a flow control valve (FCV);
- a flow element (FE), that measures the oil flow;
- a flow controller (FC); and
- a low flow alarm (FAL), which alarms if the oil flow reduces below a set point.

The natural gas flow passes through a self-actuating pressure-reducing valve (PRV) to the main burner control valve (TCV), and a pilot valve (PV). The main burner control valve is actuated by the temperature controller (TC) which receives the signal from the temperature element (TE), which measures the oil vapour discharge temperature.

The high/high pressure switch (PSHH) on the natural gas line is interlocked, via 1-4 to close the main burner control valve (TCV), if the gas pressure is too high. There is also a high temperature switch (TSH) on the vaporised oil outlet to close the main burner control valve (TCV), if the oil is superheated above a maximum temperature. Finally, there is a flame detector device (not shown) which will close both gas valves should the flame go out.

Select ONLY the vaporiser coil from the oil inlet (before flow measurement), to vapour exit to process (after temperature control) for examination. The design intent for this part is “Oil flow from the feed line, heat from the furnace, vaporise, superheat and transfer oil vapour to the process”.

Apply at least five (5) guide words and examine ten (10) deviations (from the design intent) in order to construct a possible HAZOP output for the ‘material’ and ‘activity’ elements.

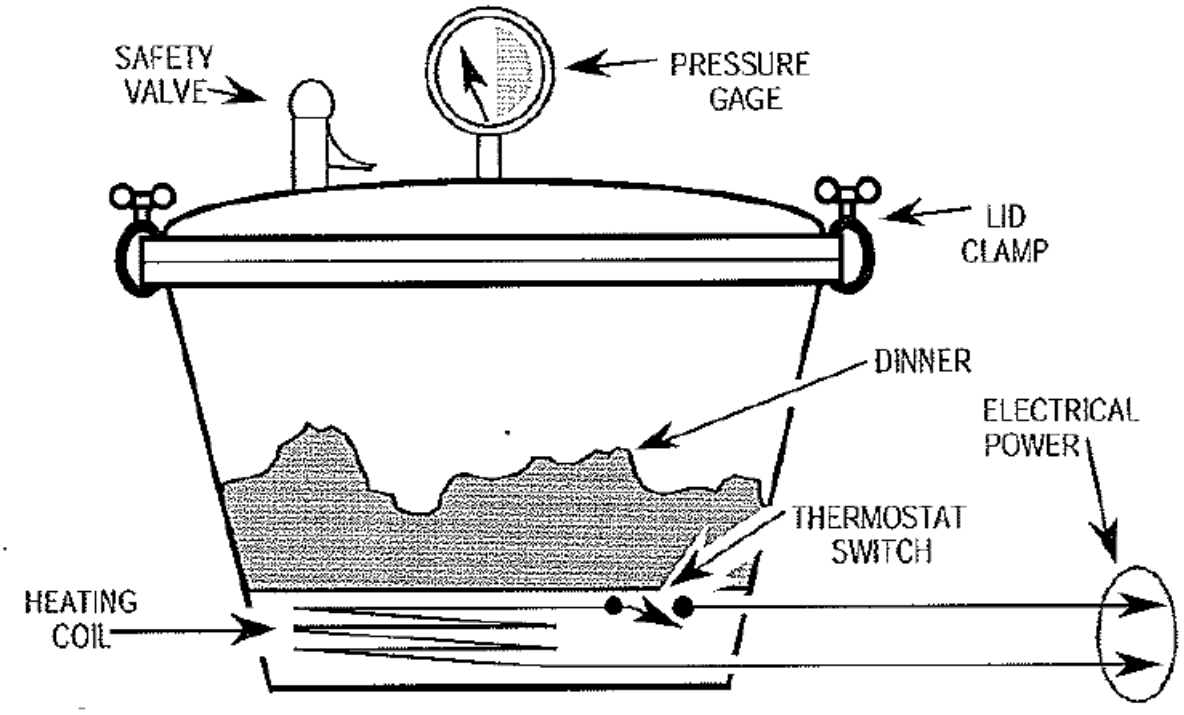
Assignment 3(c): 4 Marks

Prepare a **FMEA** at component level for an Electric coil heat pressure cooker.

Operational phase(s): Cooking (after load/close/sealing)

Components:

- Safety Valve (spring-loaded): opens on overpressure.
- Thermostat Switch: controls temperature, where Switch opens >120° C.
- Pressure Gage: dark zone indicates overpressure.
- Lid Clamps: keeps lid sealed and closed
- Heating coil: heats up the food to cook



Operator's Tasks: (1) loads cooker, (2) closes/seals lid, (3) connects power, (4) observes pressure, (5) times cooking at prescribed pressure, (6) offloads cooked food.

Assignment 3(d): 4 Marks

The following scenario is for an automobile system where the car battery has failed.

The Initiating Event (IE) for the Event Tree is "Dead Battery" that begins the scenario, with a frequency of once every ten years.

The barriers that are relevant (in the sequence they will be activated) are as below:

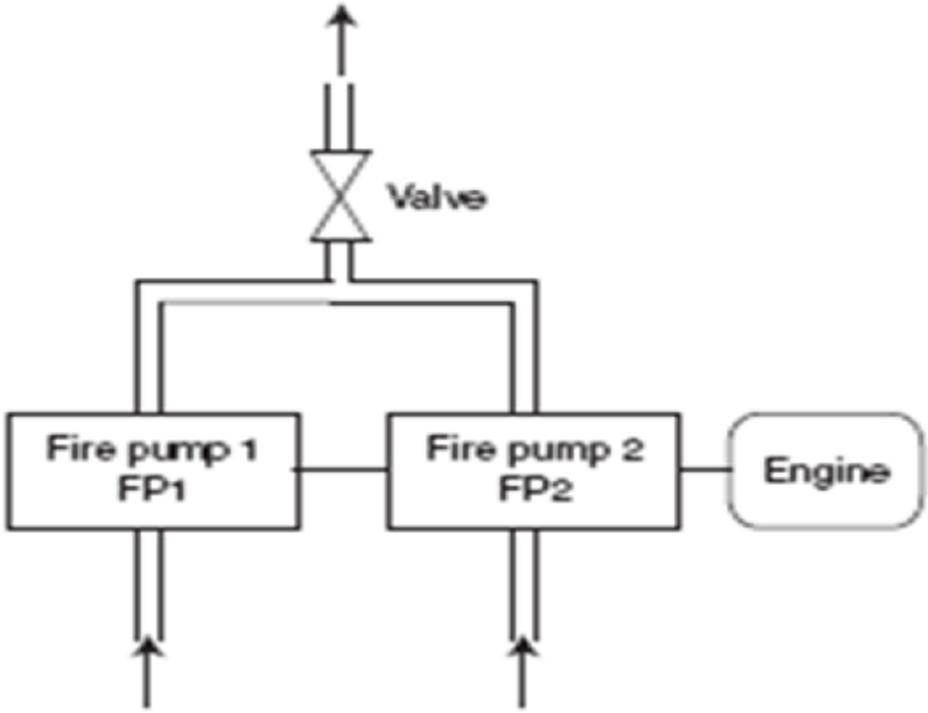
1. **Jumper Cables**: The probability of jumper cables is available is 75 out of hundred times.
2. **Donor Battery**: The likelihood of a Donor Battery is available is 0.5.
3. **Cables set**: The chance of Cables set is connected properly is 90% of the times.
4. **Donor Battery**: The probability of the Donor Battery starts the Car is 5 out of hundred times.

You are required to:

- Draw an **Event Tree** Diagram to demonstrate the above scenario.
- Calculate **the probability** for "Car not started",
- Calculate **the probability** for Car Started.
- Draw a **Fault Tree** Diagram for the 'Car not Started" to demonstrate potential causes.

Assignment 3(e): 4 Marks

For the Redundant Fire Pumps shown below:



Top Event: No Water from fire water system

Causes for the Top Event:

VF:	Valve Failure	= 1.00E-02/hr
FP1:	Failure of Fire Pump 1	= 1.00E-04/hr
FP2:	Failure of Fire Pump 2	= 1.00E-04/hr
EF:	Failure of Engine	= 1.00E-03/hr

1. **Draw a Fault Tree Diagram for the "Top Event"**
2. **Calculate the Likelihood of the Top Event happening.**