Reliability Engineering

Notes 11

Risk

- A risk is an uncertain event which may occur in the future.
- A risk may prevent or delay the achievement of an organization’s or units objectives or goals
- A risk is not certain – Its likelihood can only be estimated.
- Not all risk is bad, some level of risk must be taken in order to progress.

Risk

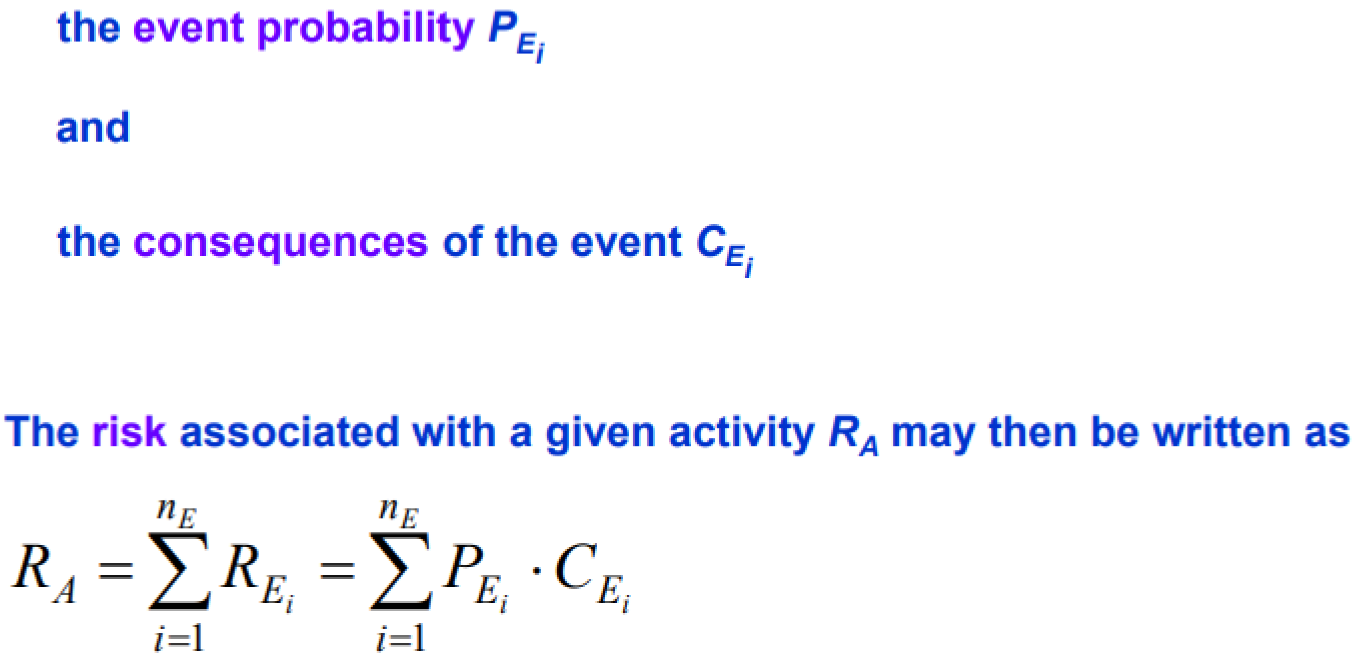
- Uncertain event or condition with an effect
- It can affect the fulfillment of a goal negatively (threat)
- • It can affect the fulfillment of a goal positively (opportunity)
- Risk is the uncertainty associated with the outcome of a future event
- and has a number of attributes:
- – Uncertainty (probability)
- – Time (future event)
- – Potential for loss (or gain)

Risk

- Risk is mathematically defined as a combination of probability and severity of an adverse event.
- Risk can be conceptually defined in the most general sense as any adverse factor that causes or can cause organizations to fail to achieve their strategic, financial, or operational objectives.

Risk

- The risk of an event can be described with



the event probability P_{E_i}

and

the consequences of the event C_{E_i}

The risk associated with a given activity R_A may then be written as

$$R_A = \sum_{i=1}^{n_E} R_{E_i} = \sum_{i=1}^{n_E} P_{E_i} \cdot C_{E_i}$$

Risk Categories

- There are different categories of risks
- **Technology**, quality and execution risks – e.g.: untested technology, unrealistic goals, change of technological platform , failure of an IT system
- **Project management risks** – e.g.: poor allocation of time and resources, poor quality of planning, poor leading of project group
- **Organizational risks** – e.g.: lack of prioritization, unclear financing, employee loss, resource conflicts with other projects (e.g., people working on several projects simultaneously)
- **External risks** – e.g.: changed laws and regulations, work conflicts, change of owners, weather

- **Financial risks -** Reduction in funding, poor cash flow management, poor budgeting
- **Operational risks -**Poor quality of services delivered , lack of succession planning ,health & safety risks , staff skill levels
- **Reputational risks-** Organization engages in activities that could threaten it’s good name, staff / members acting in an unethical way, poor stakeholder relations

Risk Management

- Risk management starts with three basic questions
  1. What can go wrong?
- 2. What will be done to prevent risk?
- 3. What will be done in the event that risk occurs?

Risk Management

- Risk Management is the process of measuring or assessing the actual or potential adverse implications of a business operation.
- Risk management is an inherent part of everyday life both for businesses and individuals.
- It is a systematic way of thinking about all possible risks before they occur.
- It helps an organisation to set up strategies to deal with potential risks.

Risk Management

- Risk is a reality in life.
- Risk management is a proactive process/method to identify and handle inner and outer threats to project success.
- Risk management is a process of thinking systematically about all possible risks, problems or disasters before they happen and setting up procedures that will avoid the risk, or minimise its impact, or cope with its impact. It is basically setting up a process where you can identify the risk and set up a strategy to control or deal with it.

Analyze the risk

- Once risks are identified we determine the likelihood and consequence of each risk. We develop an understanding of the nature of the risk and its potential to affect project goals and objectives.
- Assuming the working group has done its job, you will have generated a long list of risks.
- The task now is to assess those risks according to how likely they are to occur, and how severe the consequences would be if they did occur.

Risk Management

- Identify all relevant risks
- Analyze the risk
- Evaluate or Rank the Risk
- Treat the Risk
- Monitor and Review the risk

Identify Risks

- Risks come in two kinds; risks that apply to every workplace or organisation, and risks that come from doing the particular work you do.
- The purpose is to identify specific risks that can threaten the project success.

- Risk has two main components:
- • Probability / likelihood
- • Consequence / impact

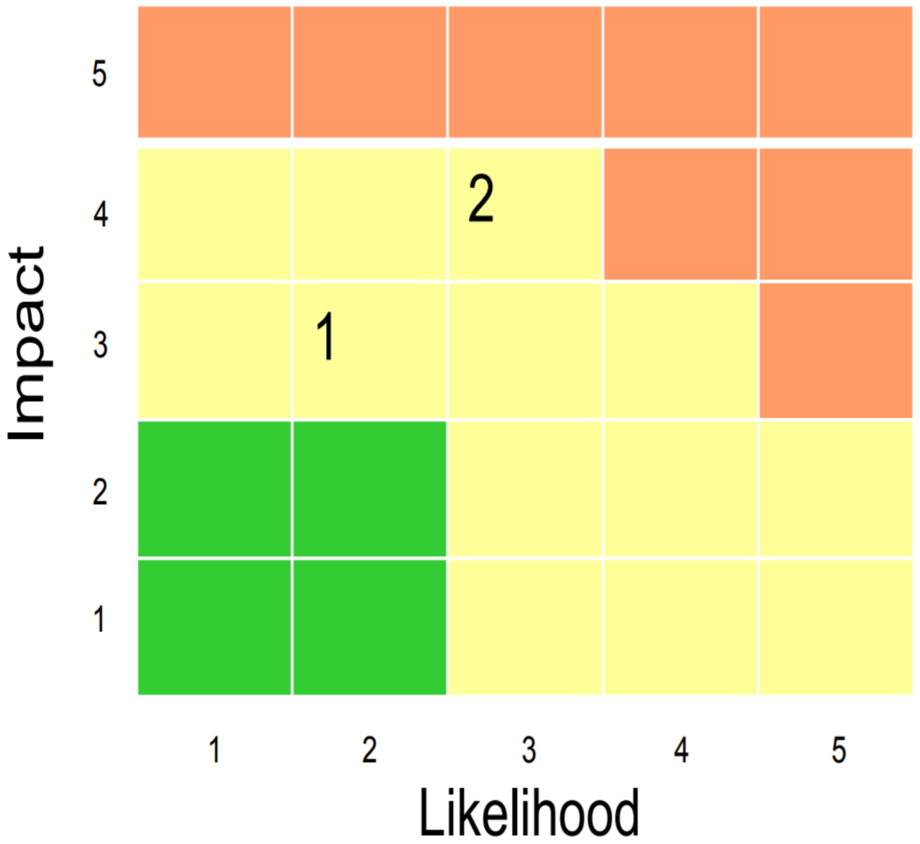
- There are different methods for risk analysis and evaluation:
- • Qualitative
- • Quantitative

- The four categories of severity are:
- • Disastrous risks
- • Very serious risks
- • Serious risks
- • Minor risks
- The four categories of likelihood are:
- • Almost certain
- • Very likely
- • Likely
- • Unlikely

Evaluate or Rank the Risk

- You evaluate or rank the risk by determining the risk magnitude, which is the combination of likelihood and consequence.
- You make decisions about whether the risk is acceptable or whether it is serious enough to warrant treatment.

Risk Matrix



Treat the Risk

- During this step you assess your highest ranked risks and set out a plan to treat or modify these risks to achieve acceptable risk levels. How can you minimize the probability of the negative risks as well as enhancing the opportunities? You create risk mitigation strategies, preventive plans and contingency plans in this step.
- This step is to develop a response for each of the risks you have identified.

- When faced with risk, an organisation may do one of the following;
  1. Avoid the risk
- 2. Treat or control or minimize the risk
- 3. Transfer the risk to another party
- 4. Accept the risk

- **Avoid the risk**
- One way is to stop doing whatever it is that creates the risk.
- Eliminate it (not always possible)

- **Transfer the risk**
- Risk transfer occurs when you get someone else to bear the risk for a particular activity. For example using insurance.

- **Minimize the risk**
- Decrease the likelihood or impact

- **Accept and observe**
- If you can’t effectively treat the risk

Monitor and Review the risk.

- This is the step where you monitor, track and review risks.
- Over time, circumstances change and your risk management plan may become inappropriate.
- The risks you identified in your risk management plan, and your assessment of them, were probably fairly accurate at the time you did the plan.

- There are two ways that you can ensure that your risk management plan is up to date.
- Firstly, it should be reviewed on a regular basis. The more volatile and changeable your organisation and its environment, and the higher the level of risk you face, the greater the need to keep your risk management plan up to date. At a minimum, your risk management plan should be reviewed at least once a year.
- Secondly, you should evaluate changes within your organisation, or within your organisation's environment, in terms of their implications for risk within your organisation. New legislation relevant to your organisation, taking on new roles, acquisition of new equipment, or creation of new positions should all be considered for their implications for risk management.

- Risk analysis techniques are divided into two categories:
- Proactive techniques
- Reactive techniques.
- Proactive techniques describe the precautions that should be taken before a defined risk arises
- Reactive techniques are the techniques used to investigate the factors that cause a risk or a precaution after the risk occurred.

FMEA

- Failure mode and effects analysis (FMEA) is a tool for evaluating the effect(s) of potential failure modes of subsystems, assemblies, components, or functions. It is primarily a reliability tool to identify failure modes that would adversely affect overall system reliability. FMEA has the capability to include failure rates for each failure mode in order to achieve a quantitative probabilistic analysis.
- Additionally, the FMEA can be extended to evaluate failure modes that may result in an undesired system state, such as a system hazard, and thereby also be used for hazard analysis.

History

- The FMEA was developed for the U.S. military as a formal analysis technique in 1949. It was used as a reliability evaluation technique to determine the effect of system and equipment failures.

FMEA

- A Failure Mode and Effects Analysis is often the first step in a systems reliability study. It involves reviewing as many components, assemblies and subsystems as possible to identify possible failure modes and the causes and effects of such failures.

FMEA

- The FMEA is applicable to any system or equipment, at any desired level of
- design detail—subsystem, assembly, unit, or component. FMEA is generally performed
- at the assembly or unit level because failure rates are more readily available for the individual embedded components. The FMEA can provide a quantitative reliability prediction for the assembly or unit that can be used in a quantitative safety analysis

FMEA

- The technique is thorough for evaluating potential individual failure modes and providing reliability information. However, for safety purposes, an FMEA is limited because it considers only single item failures and not the combination of items failing together.
- The FMEA technique is a valuable reliability tool for analyzing potential failure modes and calculating subsystem, assembly, or unit failure rates. Severity and probability evaluation of failure modes provides a prioritized list for corrective actions.

FMEA

- FAILURE: The inability of a system, subsystem, or component to perform its required function. The inability of an item to perform within previously prescribed limits.
- FAULT: – Inability to function in a desired manner, or operation in an undesired manner, regardless of cause.
- FAILURE EFFECT: – The consequence(s) of a failure mode on an operation, function, status of a system/process/activity/environment. The undesirable outcome of a fault of a system element in a particular mode.
- Risk priority number (RPN): Risk ranking index for reliability.
- RPN = (probability of occurrence) x (severity ranking) x (detection ranking).

FMEA

- FAILURE MODE: – The way in which the component, subassembly, product, input, or process could fail to perform its intended function. Failure modes may be the result of upstream operations or may cause downstream operations to fail. The manner in which a fault occurs, i.e., the way in which the element faults.
- Failure Mode Examples
- switch: open, partially open, closed, partially closed
- cable: stretch, break, kink, fray

FMEA

- A structured approach to:
  - Identifying the ways in which a product or process can fail
  - Estimating risk associated with specific causes
  - Prioritizing the actions that should be taken to reduce risk
  - Evaluating design validation plan (design FMEA) or current control plan (process FMEA)

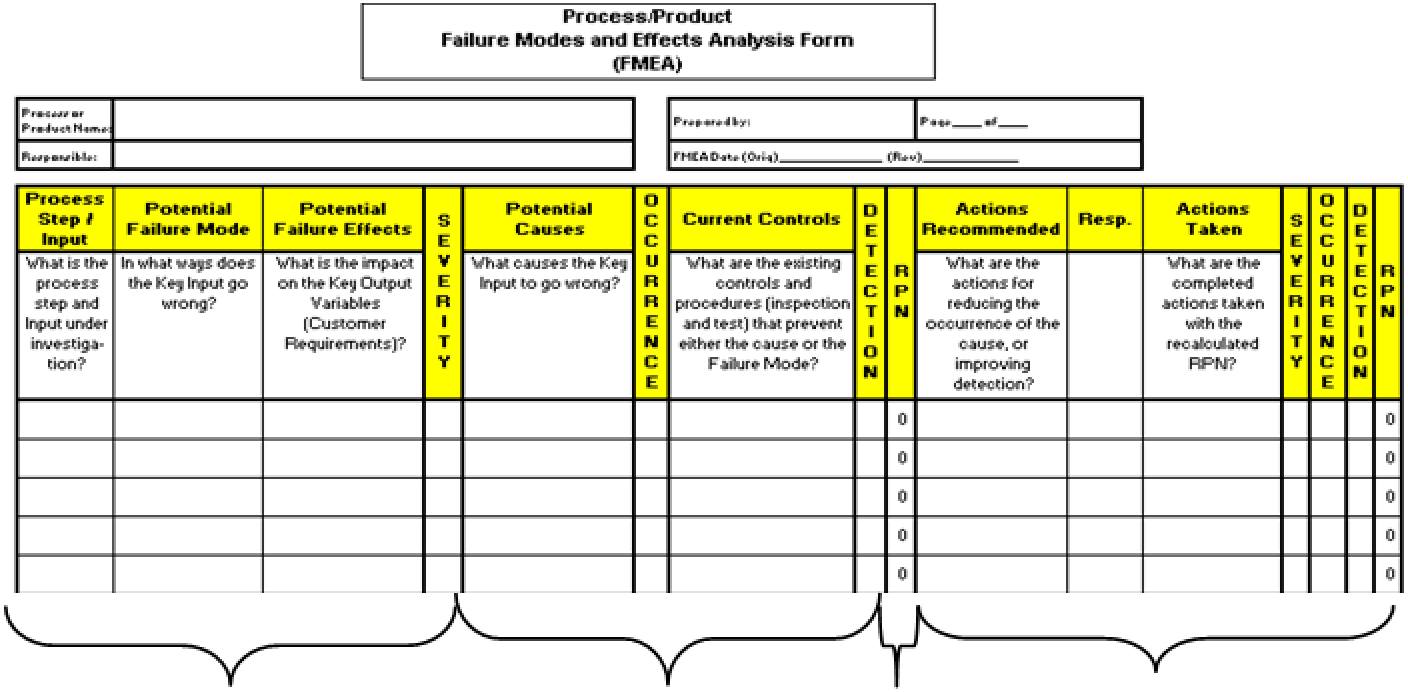
- The FMEA technique is a qualitative and quantitative analysis method used for the evaluation of potential failure modes. The FMEA is a technique that answers a series of questions:
- . What can fail?
- . How does it fail?
- . How frequently will it fail?
- . What are the effects of the failure?
- . What is the reliability/safety consequence of the failure?

Benefits

- Allows to identify areas of our process that most impact the customers
- Helps to identify how our process is most likely to fail
- Points to process failures that are most difficult to detect
- Improves the quality, reliability, and safety of products / services / machinery and processes
- Improves company image and competitiveness
- Increases customer satisfaction
- Reduces product development timing and cost / support integrated product development
- Documents and tracks action taken to reduce risk
- Integrates with Design for Manufacturing & Assembly techniques

Limitations

- The technique examines individual faults of system elements taken singly, the combined effects of coexisting failures are not considered. ⍰
- If the system is at all complex and if the analysis extends to the assembly level or lower, the process can be extraordinarily tedious and time consuming. ⍰
- Failure probabilities can be hard to obtain; obtaining, interpreting, and applying those data to unique or high-stress systems introduces uncertainty which itself may be hard to evaluate.
- It is too easy to forget human errors in the analysis



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 investigation?	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

Prioritize

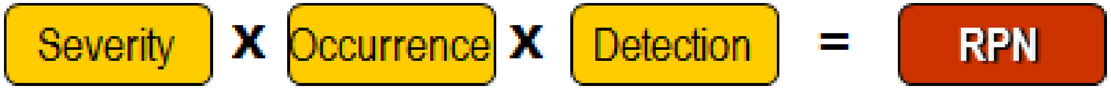
Determine and assess actions

Steps

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
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

- Severity
  - Importance of the effect on customer requirements
- Occurrence
  - Frequency with which a given cause occurs and creates failure modes (obtain from past data if possible)
- Detection
  - The ability of the current control scheme to detect (then prevent) a given cause (may be difficult to estimate early in process operations).
  - the likelihood the failure will be detected before the system reaches the end-user/customer

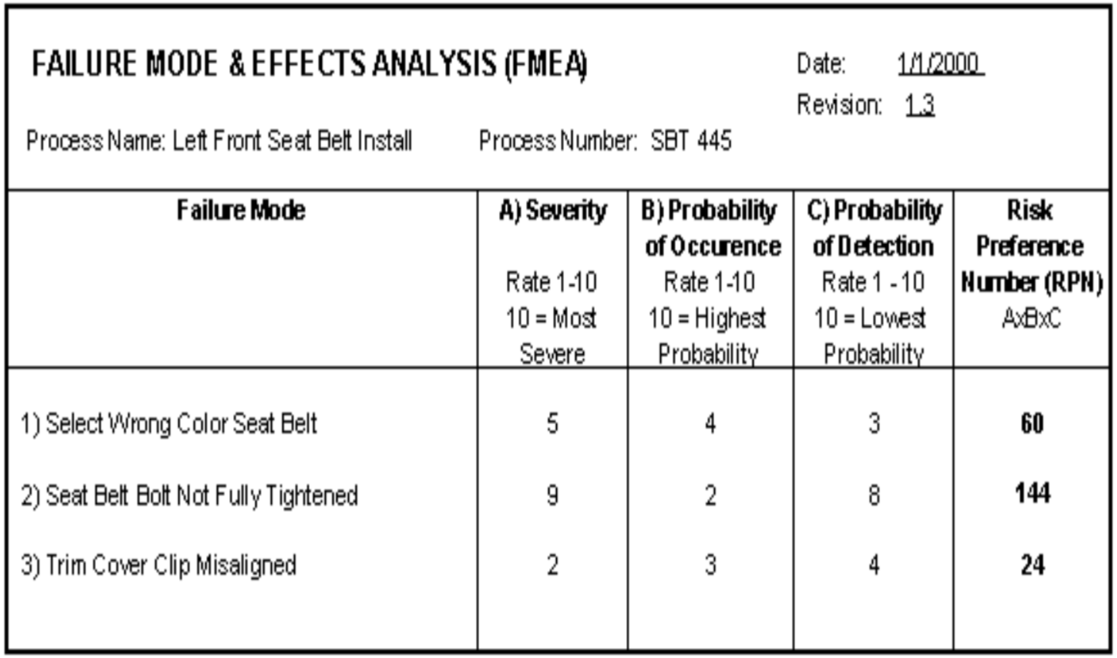
- RPN is the product of the severity, occurrence, and detection scores.



Severity X Occurrence X Detection = RPN

- It is common to use a scale from 1 to 10
- The smaller the RPN the better – and – the larger the worse

Here is an example of a simplified FMEA for a seat belt installation process at an automobile assembly plant.



FAILURE MODE & EFFECTS ANALYSIS (FMEA)

Date: 1/1/2000

Revision: 1.3

Process Name: Left Front Seat Belt Install

Process Number: SBT 445

Failure Mode	A) Severity Rate 1-10 10 = Most Severe	B) Probability of Occurence Rate 1-10 10 = Highest Probability	C) Probability of Detection Rate 1 - 10 10 = Lowest Probability	Risk Preference Number (RPN) AxBxC
1) Select Wrong Color Seat Belt	5	4	3	**60**
2) Seat Belt Bolt Not Fully Tightened	9	2	8	**144**
3) Trim Cover Clip Misaligned	2	3	4	**24**

Actions

- The risk may be reduced by introducing:
- Design changes
- Engineered safety features
- Safety devices
- Warning devices
- Procedures/training

Resources

- Introduction to Risk Management (Theory & Practice) DCU Risk & Compliance Officer November 2015
- https://www.dcu.ie/sites/default/files/ocoo/pdfs/Risk%20Mgt%20Training%20Slides.pdf
- Risk and Safety Risk and Safety in Engineering, Prof. Dr. Michael Havbro Faber Swiss Federal Institute of Technology ETH Zurich, Switzerland, http://webarchiv.ethz.ch/ibk/emeritus/fa/education/ws_safety/Safety09/Web_Lecture_1.pdf
- Lecture Notes: Risk Management, https://slideplayer.com/slide/15167799/

Resources

- http://ocw.jhsph.edu/courses/EnvironmentalHealth/PDFs/Lecture9.pdf
- https://people.eecs.ku.edu/~hossein/Teaching/Sp08/816/Lec/software-risk
- Karasan, A., Ilbahar, E., Cebi, S., & Kahraman, C. (2018). *A new risk assessment approach: Safety and Critical Effect Analysis (SCEA) and its extension with Pythagorean fuzzy sets. Safety Science, 108, 173–187.* doi:10.1016/j.ssci.2018.04.031
- https://www.dcu.ie/sites/default/files/ocoo/pdfs/Risk%20Mgt%20Training%20Slides.pdf
- https://continuingprofessionaldevelopment.org/risk-management-steps-in-risk-management-process/
- https://www.ukessays.com/essays/statistics/risk-analysis-methods.php
- Chang W.L., Tay K.M., Lim C.P. (2014) A New Application of an Evolving Tree to Failure Mode and Effect Analysis Methodology. In: Loo C.K., Yap K.S., Wong K.W., Beng Jin A.T., Huang K. (eds) Neural Information Processing. ICONIP 2014. Lecture Notes in Computer Science, vol 8836. Springer, Cham

Resources

- Chapter 3 - Qualitative System Analysis, TPK4120 - Lecture summary, Jørn Vatn
- Failure Modes and Effects Analysis R.R. Mohr February 2002 8th Edition, Jacobs Sverdrup, https://userweb.icecube.wisc.edu/~kitamura/NK/Flasher_Board/Useful/FMEA.pdf
- Hazard Analysis Techniques for System Safety, Clifton A. Ericson, II , 2005, JOHN WILEY & SONS, INC., PUBLICATION
- Failure Modes Effect Analysis (FMEA), Tom Kuczek, Statistical Quality Control Lecture Notes
- slideplayer.com/slide/5921308/
- Chapter 3 FMECA, Marvin Rausand , RAMS Group Department of Production and Quality Engineering, NTNU, Slides related to System Reliability Theory Models, Statistical Methods, and Applications Wiley, 2004