Aalto University
School of Engineering

MEC-E2009 Marine Risks and Safety

L2
Introduction to reliability theory, classic accident modeling theories

Ahmad BahooToroody, Ph.D.

Aalto University, Marine and Arctic Technology

L2: Intended Learning Outcome (ILO)

By this course You will be able to;

- Learn about different types of Uncertainty
- Understand the Basic Concepts in Reliability Engineering
- Find your track for developing your knowledge for advanced Reliability Assessment of Complex Systems or Structures
- Understand the foundations and goal/objectives of classic accident modeling techniques

Aalto University
School of Engineering

Reliability engineering

Definitions

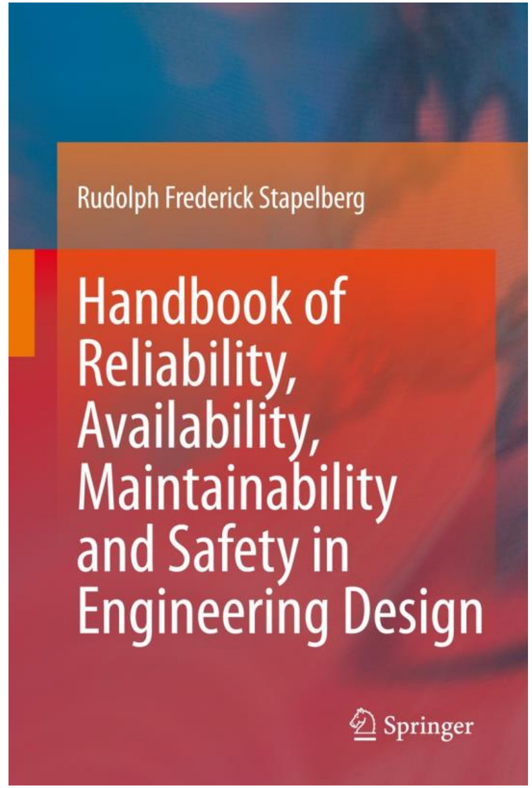
How would you define safety?

Safety:

- Safety is the state of being "safe", the condition of being protected from harm or other danger.
- Safety can also refer to the control of recognized hazards in order to achieve an acceptable level of risk.

Safety in engineering is about understanding hazards and risks, managing risks by providing the appropriate layers of protection to reduce the frequency and severity of incidents, and learning from incidents when they happen

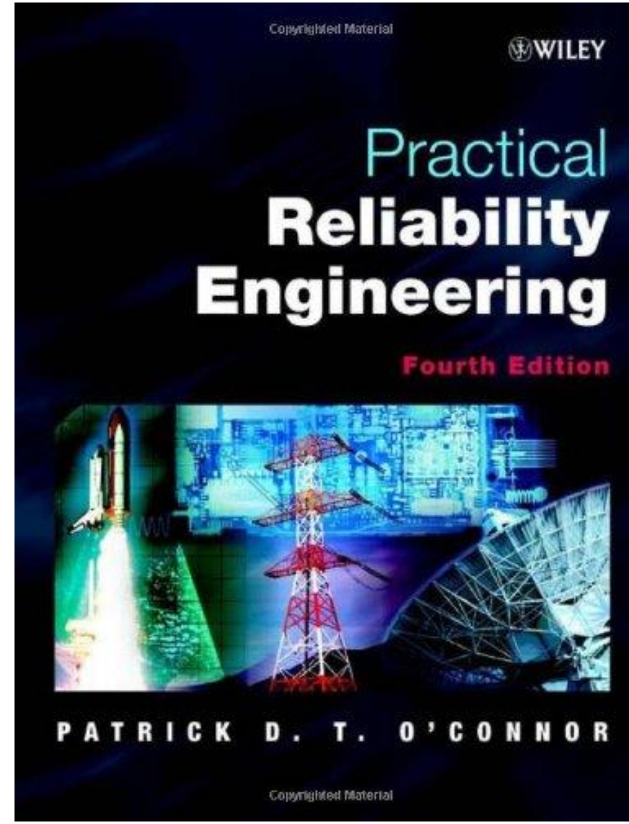
(Stapelberg, 2009) ”



Definitions

Reliability:

“Reliability is defined as the probability that a product, system, or service will perform its intended function adequately for a specified period of time, or will operate in a defined environment without failure (O'Connor, 2012)”



Why Reliability is important?

1. To estimate remaining useful lifetime of an asset
2. To optimize the maintenance plan
3. To reduce costs of failure caused by system downtime
4. To increase the availability of asset
5. To optimize the asset value by increasing asset lifespan

How to define Reliability?

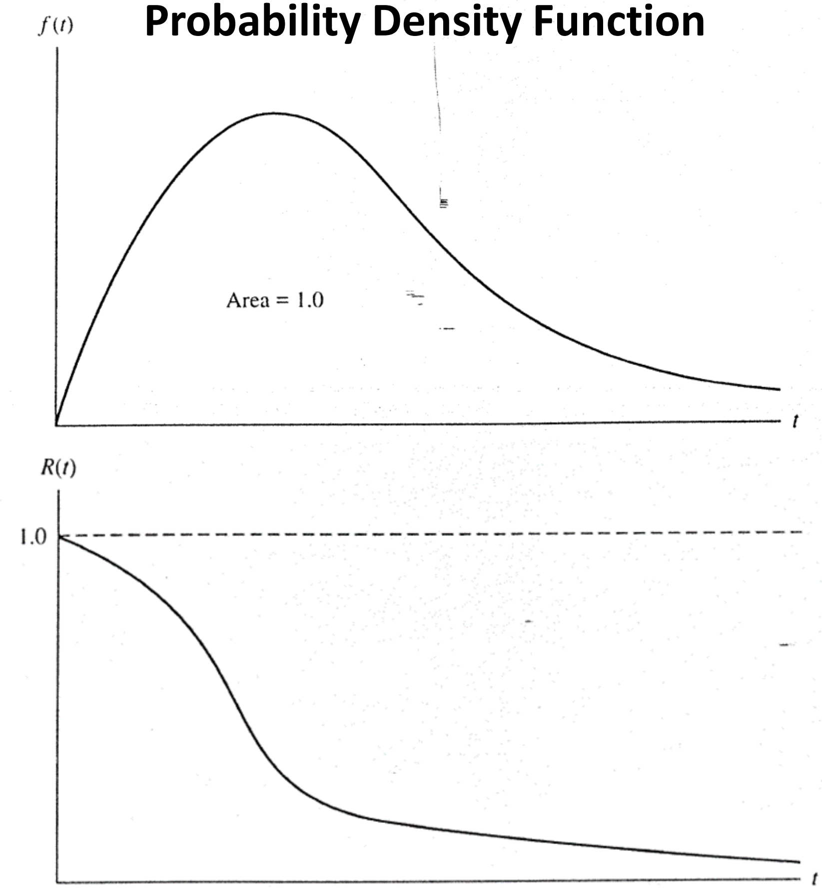
Reliability is defined as a probability that a system (structure) will function over some time period t

$$R(t) = Pr\{T > t\} = \int_t^{\infty} f(x)\,dx$$

where *f(x)* is the failure probability density function and t is the length of the period of time (which is assumed to start from time zero).

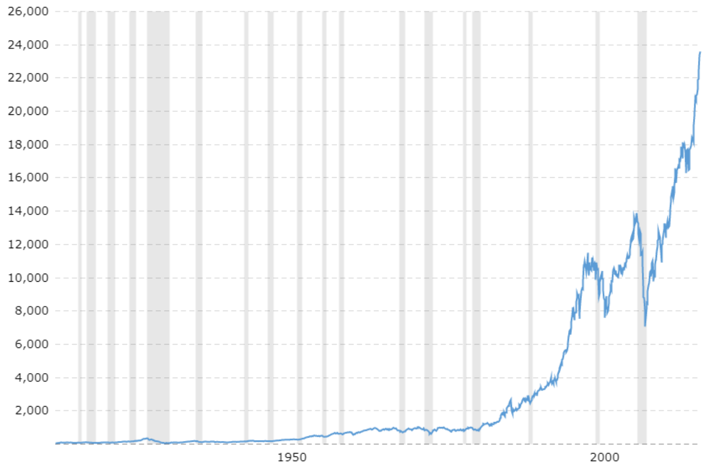
f(x) is probability of failure at time t

Probability Density Function



How to define Reliability?

Historical Data of a system (structure) function over some time period t



Accelerated Life Testing (ALT) to induce field failure in the laboratory at a much faster rate by providing a harsher, but nonetheless representative, environment.

Probability Density Function

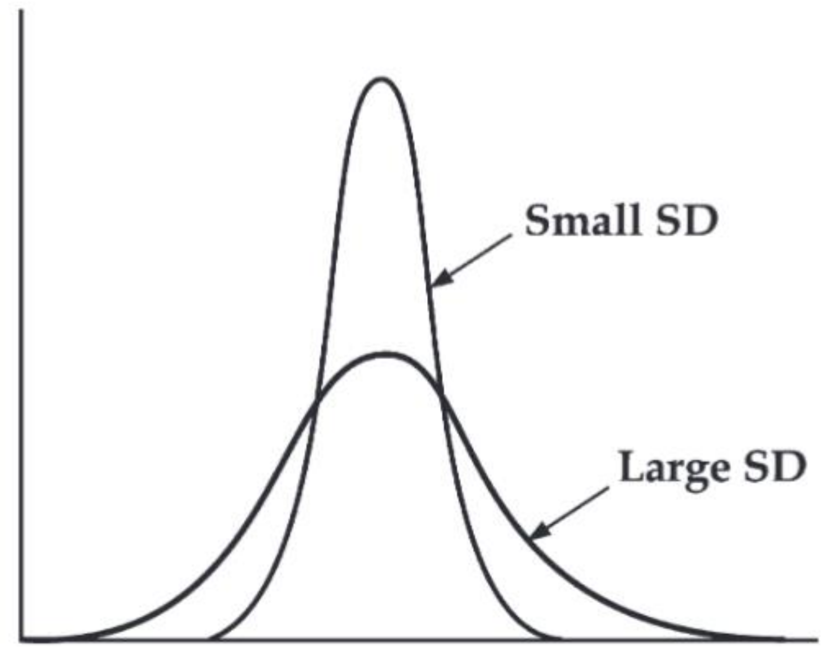
Different PDF can represent the failure trend over the operational time. What are the most common options for that?

1. Normal distribution

normal distribution is a probability distribution that associates the normal random variable around central value, called the mean.

$$f(x) = \frac{e^{-(x-\mu)^2/(2\sigma^2)}}{\sigma\sqrt{2\pi}}$$

Not frequently used



Bathtub Hazard Rate Curve

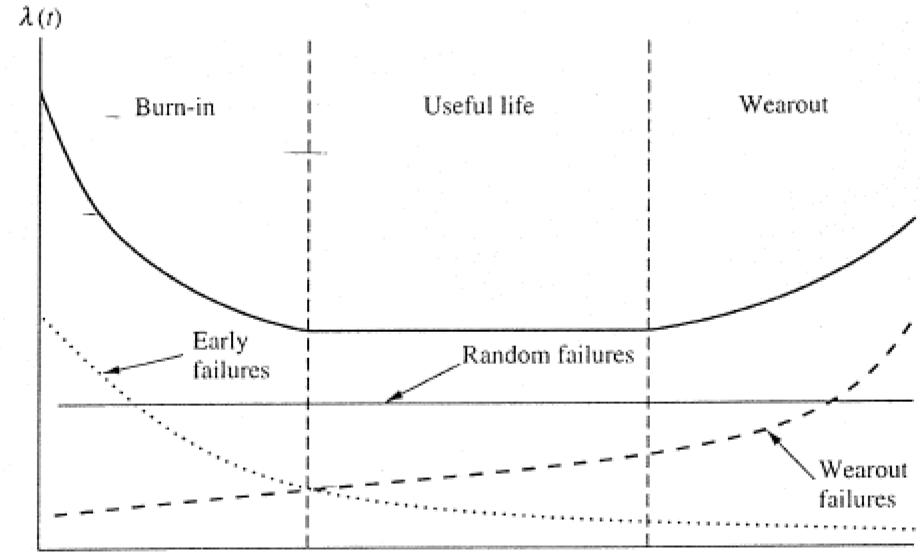
Failure Rate:

gives an instantaneous rate of failure in time

$$\lambda(t) = \lim_{\Delta t \to 0} \frac{-[R(t+\Delta t) - R(t)]}{\Delta t} \cdot \frac{1}{R(t)}$$

$$= \frac{-dR(t)}{dt} \cdot \frac{1}{R(t)} = \frac{f(t)}{R(t)}$$

$$= \frac{Number\ of\ failures}{Period\ of\ Time} = n / T$$

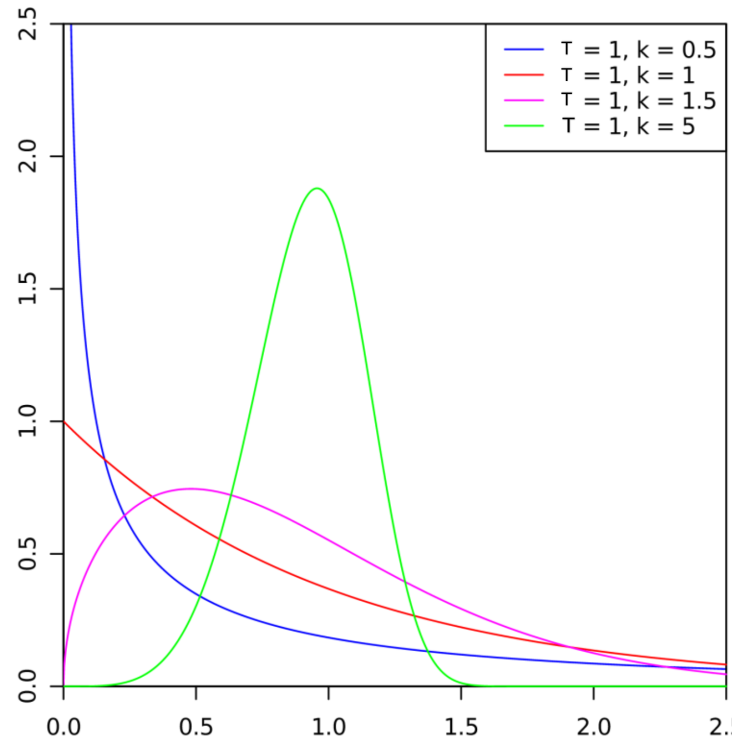


Probability Density Function

2. Weibull distribution

where *k* > 0 is the *shape parameter* and T > 0 is the *scale parameter* of the distribution.

$$f(x;\mathrm{T},k) = \begin{cases} \frac{k}{\mathrm{T}}\left(\frac{x}{\mathrm{T}}\right)^{k-1} e^{-(x/\mathrm{T})^k} & x \geq 0, \\ 0 & x < 0, \end{cases}$$



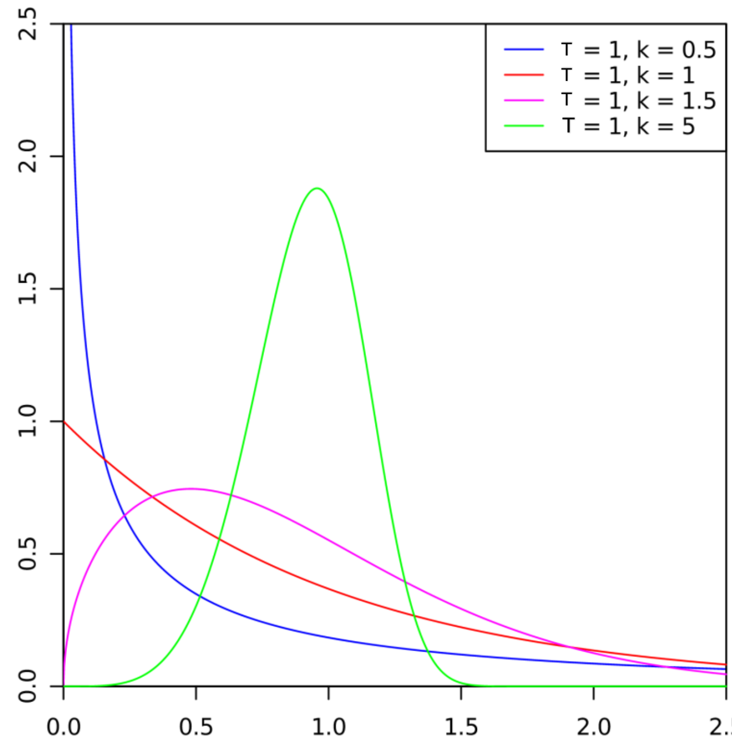
Probability Density Function

2. Weibull distribution

A value k<1 indicates that the failure rate decreases over time

A value of k=1 indicates that the failure rate is constant over time.

A value of k>1 indicates that the failure rate increases with time.



Probability Density Function

3. Exponential distribution

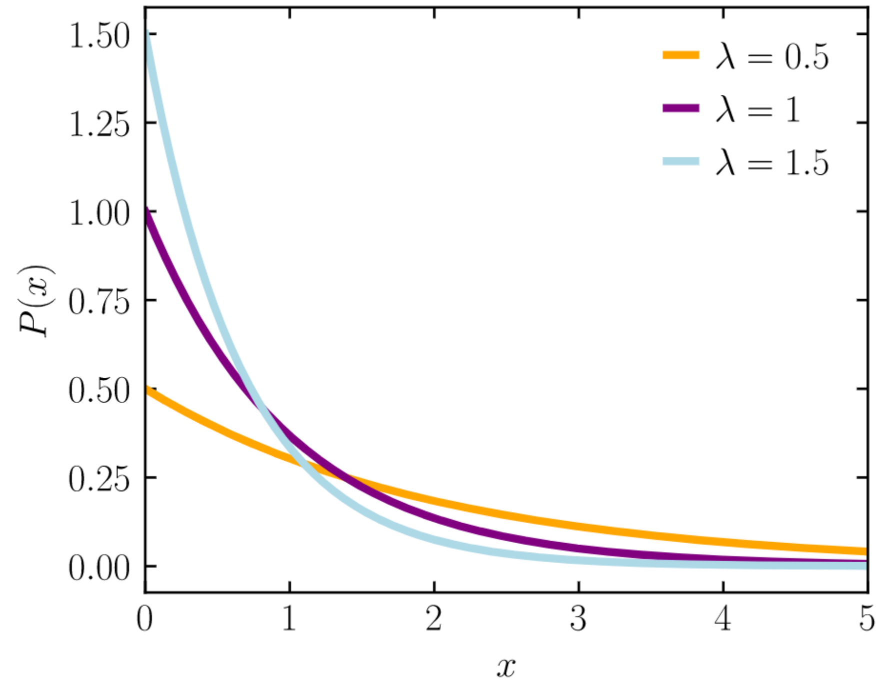
Here λ > 0 is the parameter of the distribution, often called the failure rate parameter.

k=1

λ=1/T

$$f(x; \mathrm{T}, k) = \begin{cases} \frac{k}{\mathrm{T}}\left(\frac{x}{\mathrm{T}}\right)^{k-1} e^{-(x/\mathrm{T})^k} & x \geq 0, \\ 0 & x < 0, \end{cases}$$

$$f(x; \lambda) = \begin{cases} \lambda e^{-\lambda x} & x \geq 0, \\ 0 & x < 0. \end{cases}$$



Type of Weibull

Probability Density Function

4. Lognormal – aging components, but highly skewed
5. Gamma – sum of exponential random variables, with multiple failure modes
6. Poisson – rare events or failures in a large population (close to exponential)
7. Pareto – high uncertainty in the data, extreme events

What is Uncertainty?

The Engineering Problems involves in two Type of Uncertainties

1. Epistemic uncertainty: reducible uncertainty

An epistemic uncertainty refers to the deficiencies by a lack of knowledge or information.

Sources: (1) the statistical uncertainty due to the use of limited samples. For example, the mean value of wave load based on two or three measurements;

(2) the model uncertainty associated with the idealization and assumptions of model, for example, an assumption of a constant coefficient in a PDE.

What is uncertainty?

Measures of epistemic uncertainty

Table 1
Uncertainty rating classification scheme, based on Flage and Aven (2009).

Rating	Conditions
Low uncertainty	All of the following conditions are met: – The assumptions made are seen as very reasonable – Much reliable data are available – There is broad agreement/consensus among experts – The phenomena involved are well understood; models used are known to give predictions with the required accuracy
High uncertainty	One or more of the following conditions are met: – The assumptions made represent strong simplifications – Data are not available, or are unreliable – There is lack of agreement/consensus among experts – The phenomena involved are not well understood; models are non-existent or known/believed to give poor predictions
Medium uncertainty	Conditions between those characterizing low and high uncertainty

Goerlandt and Reniers, 2016, On the assessment of uncertainty in risk diagrams

What is uncertainty?

Measures of epistemic uncertainty

IMO Circ. 1455 - Guidelines For The Approval Of Alternatives And Equivalents As Provided For In Various IMO Instruments

Table 1: Categorization of new technology

		Technology status		
		Proven	Limited field history	New or unproven
Application Area		1	2	3
Known	0	1	2	3
New	1	2	3	4

What is Uncertainty?

The Engineering Problems involves in two Type of Uncertainties

2. Aleatoric uncertainty: uncertainties due to intrinsic variability in the system

Intrinsic variability may be attributed to a property of the system based on repeated measurements of the property or may be associated with variability in time or space; differ each time we run the same experiment

Aleatoric is derived from the Latin *alea* or *dice*, referring to a game of chance

Expressed with probability distribution

What is Uncertainty practically?

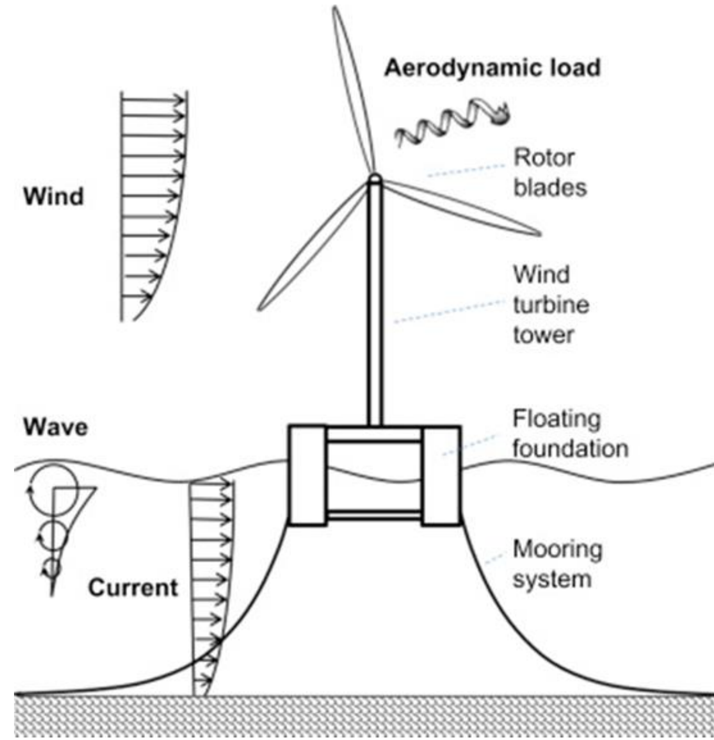
- How will System/Component/Structure fail?
- It is Epistemic Uncertainty: Since we need to model the process either with Physics or Experiments
- What is variation in environmental condition? Such as Wave load, Humanity, vibration in system, and etc.
- It is mostly Epistemic Uncertainty.
- When a light bulb will break after you conduct experiments with many other types of light bulbs?
- It is mostly Aleatory uncertainty.

First Discussion

Please define Aleatoric and Epistemic Uncertainty in this example? How can we model it?

Uncertainty associated with performance:

Uncertainty associated with Operational Condition:



Aalto University
School of Engineering

Approaches for reliability assessment

Reliability assessment

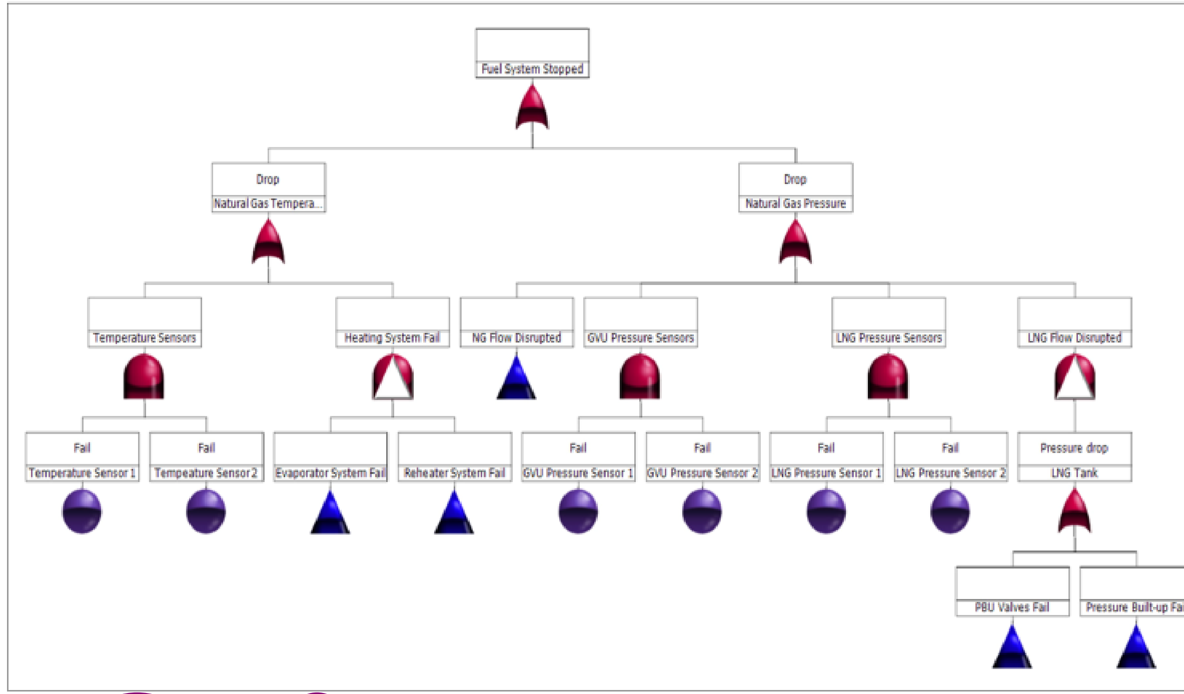
Traditional Approach:

FMEA (Qualitative-Qualitative Approach)

Fault Tree Analysis (FTA) (Quantitative Approach based on Constant Failure Rate)

FTA example

An example of ship propulsion system failure progress using the application of (D)FTA



More in the second half of the lecture

Milioulis, K.; Bolbot, V.; Theotokatos, G. Model-Based Safety Analysis and Design Enhancement of a Marine LNG Fuel Feeding System. J. Mar. Sci. Eng. 2021, 9, 69. https://doi.org/10.3390/jmse9010069

FMEA example

An example of LNG fuel feed system failure using FMEA

Table 7. FMECA table as generated from MADe indicating the Risk Priority Number (RPN) of each system component failure mode (O: Occurrence; S: Severity; D: Detectability).

No	Component	Function	Failure Mode	Causes of Failure			Failure End Effect	Detection Method	Criticality			
			Functional Failure	Fault	Mechanism	Cause			O	S	D	RPN
1	LNG tank	Stores the LNG	Overpressure	High boil-off gas evaporation rate	-	Heat penetration into the fuel tank	To vent the excessive boil-off gas	LNG pressure sensor	3	4	1	12
2	Pressure build-up unit	Maintains the pressure inside the LNG tank	Disrupted natural gas supply to the LNG tank	Fractured Ice outgrowths Shrunk Corroded Surface cracks	Brittle fracture Ice formation Thermal contraction Corrosive fatigue Corrosive fatigue	Low temperature Low temperature Low temperature Temperature fluctuations Temperature fluctuations	To stop the entire system	LNG pressure sensor	4	8	4	128
3	Evaporator	Converts LNG to natural gas at the desired temperature	Low natural gas temperature	Fractured Ice outgrowths Shrunk Corroded Surface cracks	Brittle fracture Ice formation Thermal contraction Corrosive fatigue Corrosive fatigue	Low temperature Low temperature Low temperature Temperature fluctuations Temperature fluctuations	To stop the entire system	Temperature sensor	4	8	4	128
4	Glycol-water heat exchanger	Increases the temperature of the natural gas	Low natural gas temperature & pressure	Fractured Corroded Perforated Shrunk Expanded	Thermal fatigue Corrosive attack Corrosive attack Thermal contraction Thermal expansion	Temperature fluctuations Corrosive contaminant Corrosive contaminant Low temperature Temperature difference	To stop the entire system	Temperature & Pressure sensors	3	8	3	72

Milioulis, K.; Bolbot, V.; Theotokatos, G. Model-Based Safety Analysis and Design Enhancement of a Marine LNG Fuel Feeding System. J. Mar. Sci. Eng. 2021, 9, 69. https://doi.org/10.3390/jmse9010069

More in the second half of the lecture

FMEA vs FTA

	FTA	FMEA
Purpose	Identify causes of top event (Why?)	Identify components failure modes and effects What (?)
Output	Tree structure	Tabular structure
Analysis approach	Top bottom	Bottom up
Strength and focus	Captures combinations of component failures	Captures various failure modes of components

Reliability assessment

Novel and new approaches:

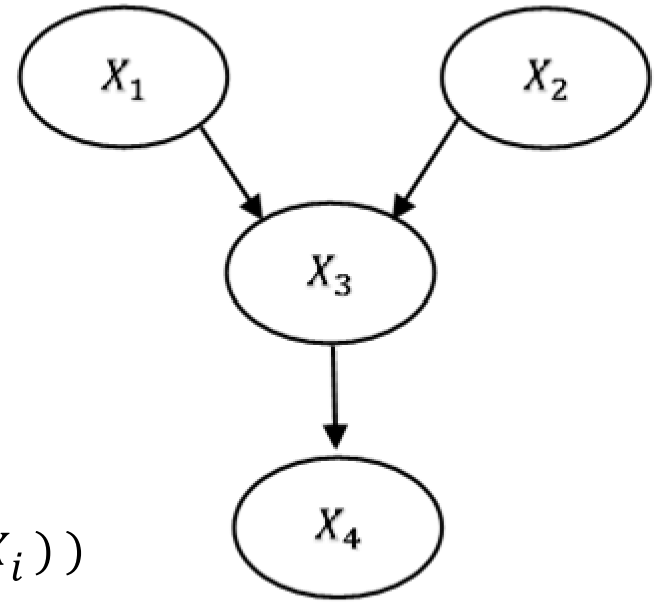
Bayesian Network

Machine Learning

- Supervised Learning
- Unsupervised learning
- Reinforcement learning

Deep Learning

Bayesian Network



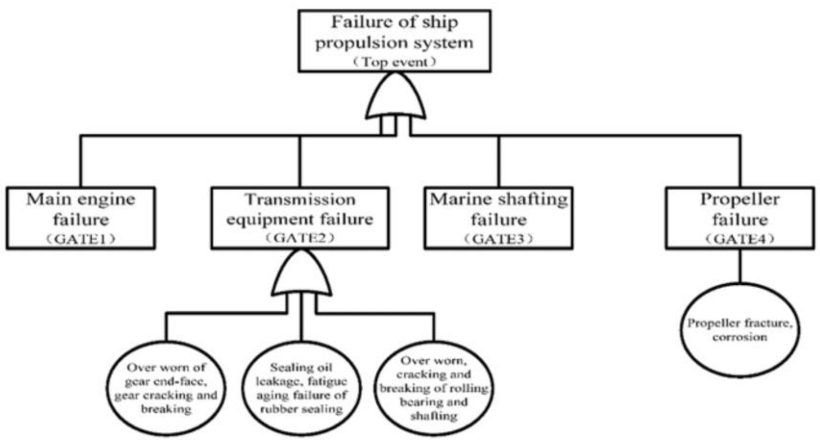
- Directed Acyclic Graph (DAG); (no directed cycles)
- Nodes represent variables
- Arcs represent conditional dependencies

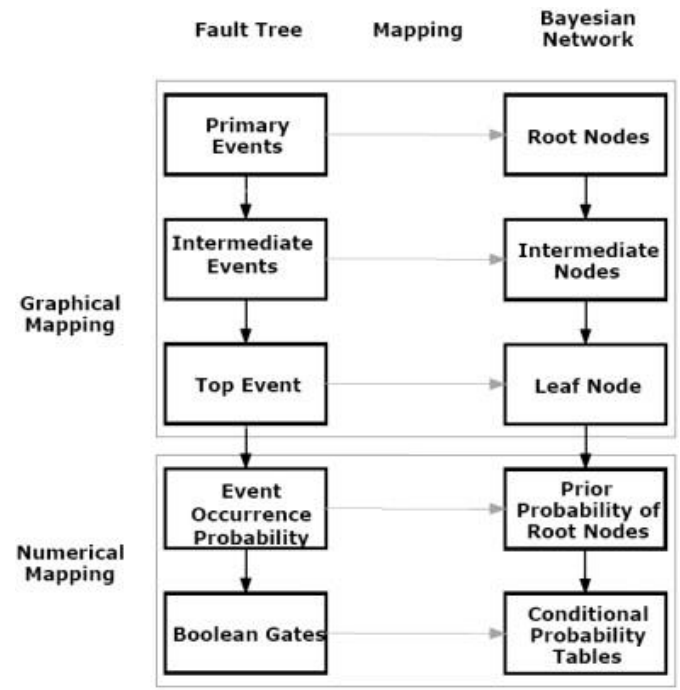
$$P(X_1, X_2, \ldots . X_N) = \prod_i P(X_i \mid parents(X_i))$$

$$P(X_1, X_2, X_3, X_4) = P(X_1)\, P(X_2)\, P(X_3|X_1, X_2)\, P(X_4|X_3)$$

BN example

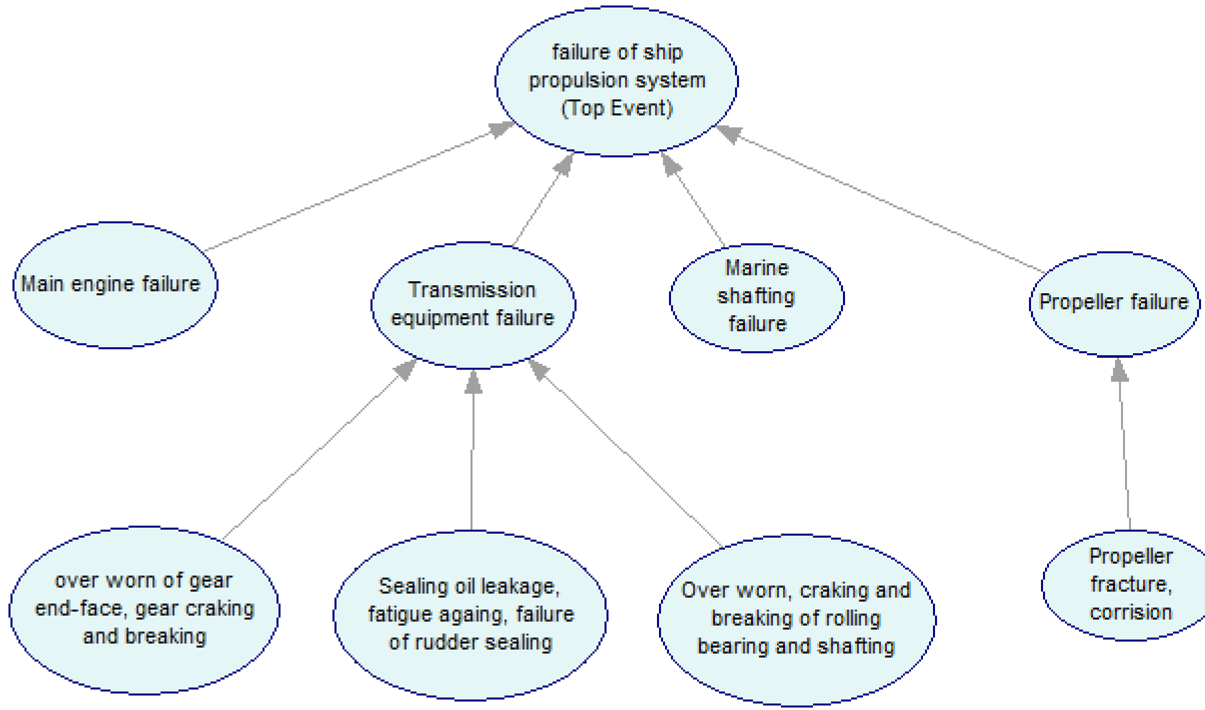
Mapping FTA into BN





BN example

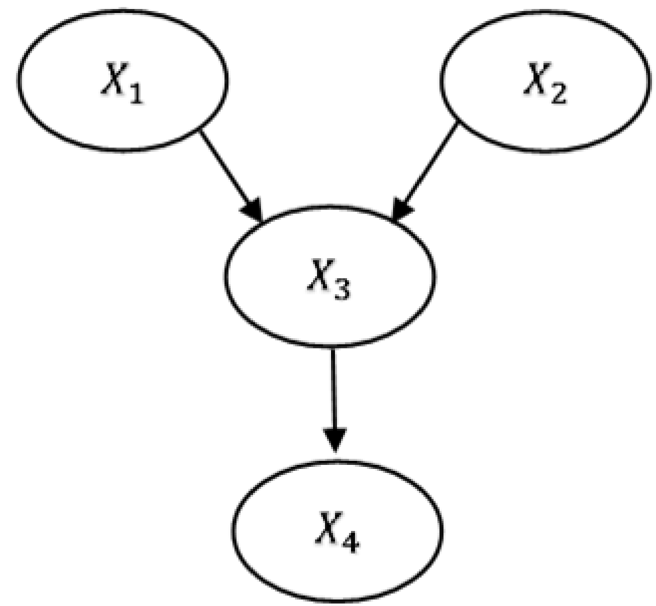
An example of ship propulsion system failure progress using the application of BN



Comparison of FTA and BN

Updating capability; By propagation of new observations through the network, BN updates the prior probabilities, yielding posterior probabilities. Not the case in FTA

When new information about the state/value of any of the node in the network is acquired, BN estimates the updated joint probability distribution based on Bayes' Theorem. Given the evidence that X_3 is in a state/value *"e"* the joint probability distribution is updated using



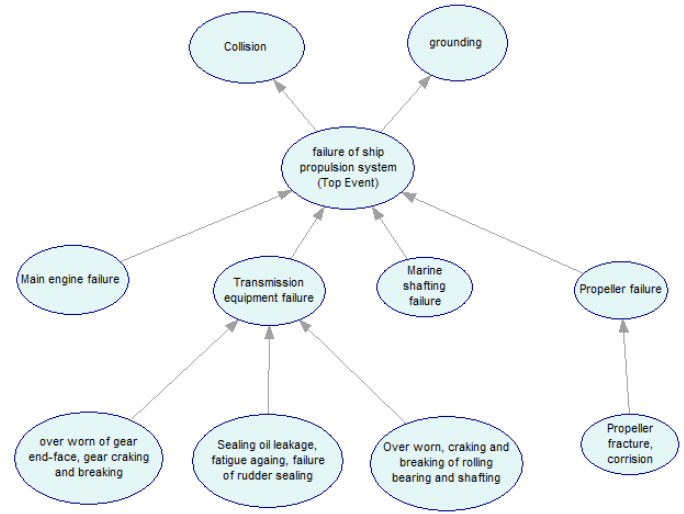
$$P(X_1, X_2, X_4|e) = \frac{P(X_1, X_2, X_4, e)}{\sum_{X_1, X_2, X_4} P(X_1, X_2, X_4, e)}$$

Comparison of FTA and BN

Both cause and consequence of an accident can be modeled by BN

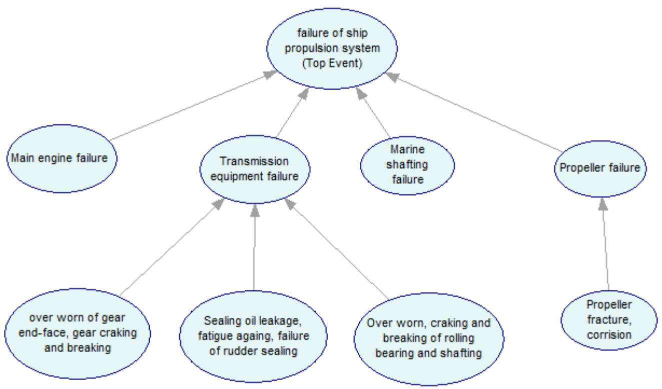
Reasoning under uncertainty;

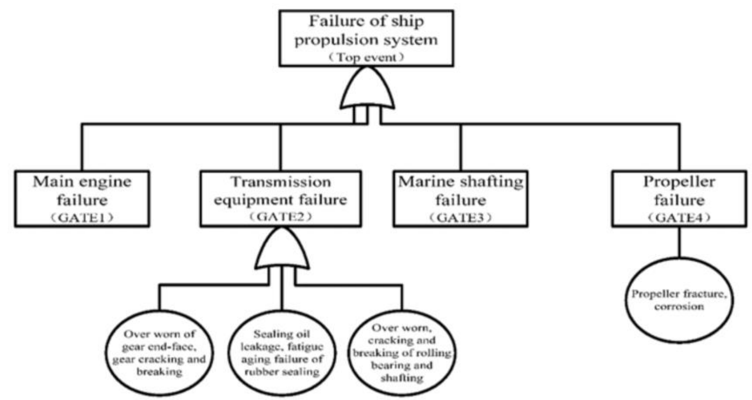
- Through the arcs you can explain the relationship between the variables and reduce the uncertainty. (what type of Uncertainty?)



Second Discussion

Does a BN necessarily have an equivalent FT? (Yes, How?/ No, Why?)





Aalto University
School of Engineering

Structural reliability theory

Structural Reliability

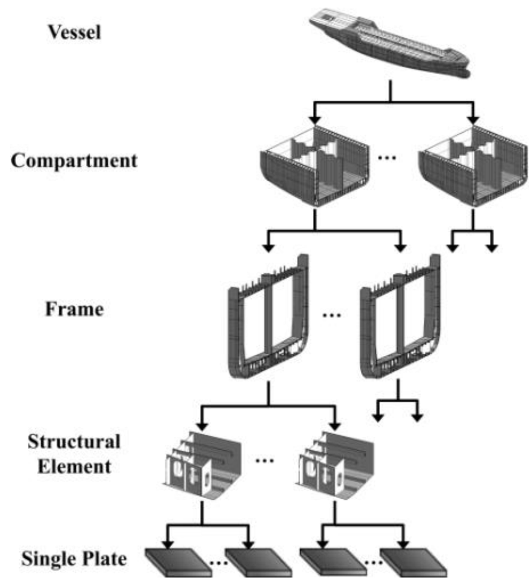
Structural reliability is the ability of a structure or structural element to fulfill the specified performance requirements under the prescribed conditions during the prescribed time.

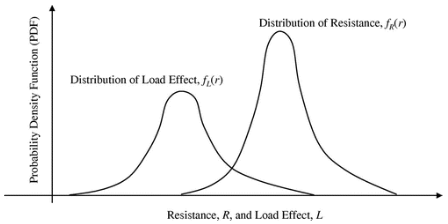
Prescribed Time

Refers to the design working life; The assumed period for which a structure or structural elements is to be used for its intended purpose without a major repair being necessary.

Structural Reliability Engineering

- Structural failure are very rare, and typically occur due to the occurrence of a rare event
- Structural components and systems are unique, due to choices in materials and geometry, and/or due to operational differences in loading and exposure
- *Hence, no experience-based failure probabilities can be obtained*





Whole Story about Structural Reliability Engineering (SRE)

Performance of a structure must **Resist (R)** extreme environmental **Load (L)**

SRE define simply as **Limit State Function** or **Failure Function** g(x):

g(x) = Resistant– Load

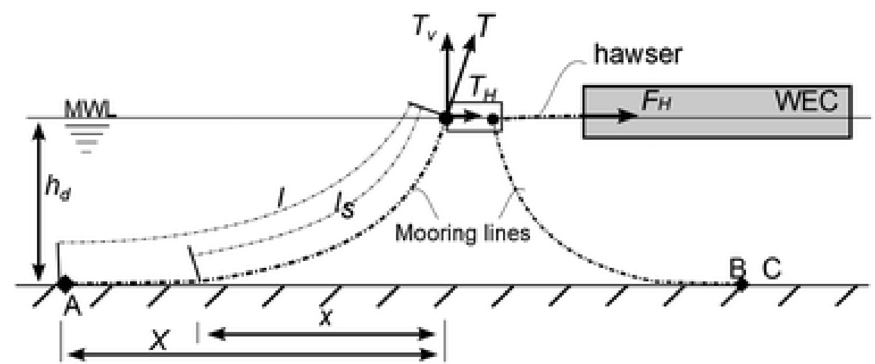
$$g(x) > 0 \quad Safe$$
$$g(x) < 0 \quad fail$$

Structural Reliability Engineering (SRE) e.g., mooring failure

We want a mooring line that resist 200 KN. The wave load is random which can lead to stochastic response in mooring. For example, for a significant wave height of 2 m, the mooring might observe response of 150, 100, 110, 240.

Resistant is equal to 200 KN.

Load are [150, 100,110,240]



$$g(x)\begin{cases} 200 - 150 = 50 > 0 \\ 200 - 100 = 100 > 0 \\ 200 - 110 = 90 > 0 \\ 200 - 240 = -40 < 0 \end{cases}$$

Then, Probability of Failure is equal to 1/4

Structural reliability theory
Defining R and L

- The structural resistance is calculated based on theories of structural elements, if necessary using Monte Carlo techniques

- The load is often represented by extreme value distributions, e.g., Pareto/Weibull distirbution (Why?)

Aalto University
School of Engineering

Conclusion of reliability engineering

Conclusions about reliability engineering

- Two types of uncertainties; Epistemic and Aleatoric
- Reliability engineering is a very useful tool to understand the failures on physical measurable phenomena (e.g. structural reliability).
- Probabilistic models for estimation of the statistical characteristics of component failure are highly used* and are common input for risk analysis and assessment.
- Component failure probabilities can be estimated based on failure frequencies from operational experience and material tests.

Aalto University
School of Engineering

Classic accident modelling theories and hazard analysis methods

Hazard, risk and safety

Hazard

Any source of potential damage, harm or adverse health effects on something or someone (2)

Risk

The chance that a person will be harmed or experience an adverse health effect if exposed to a **hazard** (3)

Safety

The condition of being protected from or unlikely to cause danger, **risk**, or injury (4).

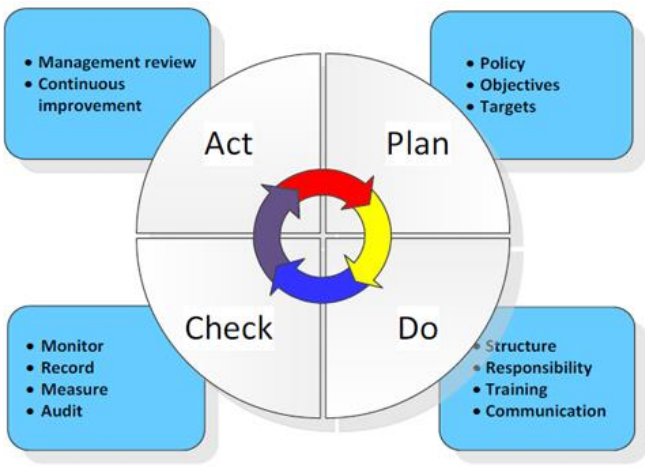
Risk and safety management

Risk Management

The identification, evaluation, and prioritization of risks followed by coordinated and economical application of resources to minimize, monitor, and control the impact of unfortunate events (5).

Safety Management

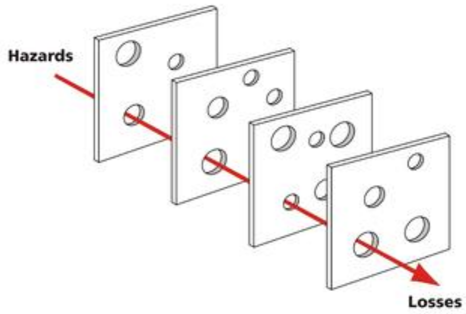
Includes the arrangements made by the organization to establish and promote a strong safety culture while achieving and controlling a determined safety performance (6).



Modellling accident causation as event changes

Accidents are caused by chain of directly related events. We can understand accidents by looking at the chain of events leading to loss

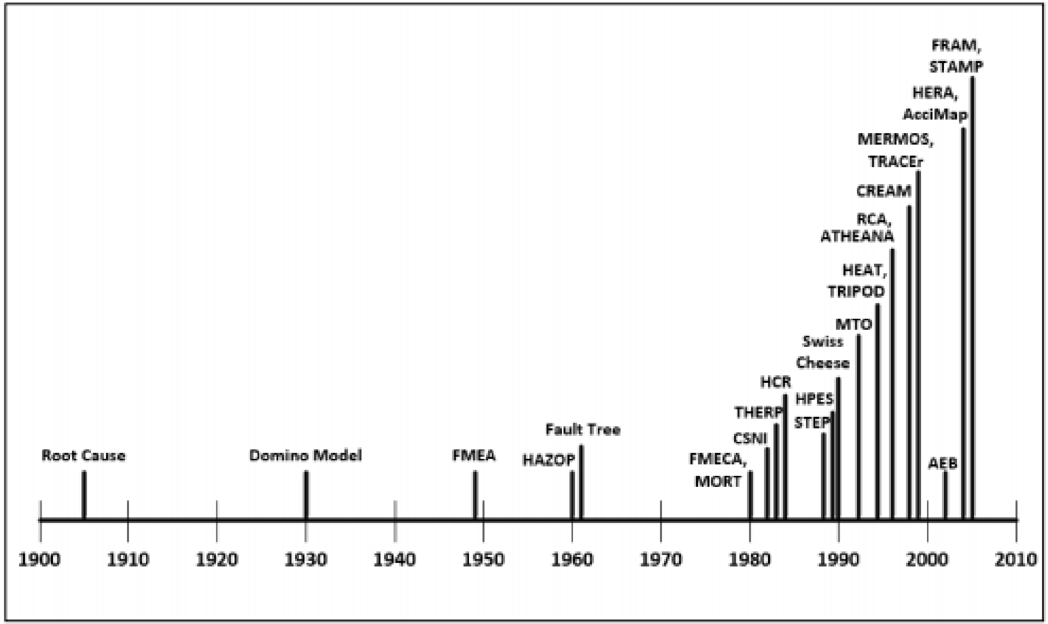
Subjectivity in selecting the events to include, subjectivity in identifying changing conditions, and exclusion of systemic factors.



Swiss cheese model by Reason (1990)

Hazard analysis

- For identifying the hazards and analysing the potential causes and effects of hazards, several methods are available.
- Failure Modes and Effect Analysis (FMEA), Hazard and Operability Study (HAZOP), Fault Tree Analysis (FTA) are some of the widely used methods in maritime domain.



Failure Modes and Effect Analysis (FMEA)

- FMEA is an analysis technique for evaluating the effects of potential failure modes of system components or functions.

- A failure mode is a manner by which a component fails to perform its intended function or the way in which the failure of an item occurs.

- The FMEA worksheet should contain the following information:
  - Component or function of the system
  - Failure mode
  - Effects of failure mode
  - Causes of failure mode
  - Risk of each failure mode
  - Recommendations or safety controls

FMEA procedure

Step1: Define system under assessment.

Define scope and boundary of the system. Identify the system operation, components and functions. Gather all information about system components and its functions.

Step 2: Identify potential failure modes.

For each of the components or functions, identify the potential failure modes.

Step 3: Identify the potential effects.

Identify how the failure mode can affect the component or overall system. In detailed FMEA analysis, the severity level of the failure mode is also defined.

FMEA procedure

Step 4: Identify the potential causes.

Using the system information and brainstorming, identify the potential causes (component failures, human errors, software issues etc) of each failure mode. In detailed FMEA analysis, the probability of occurrence (possibility of occuring) for each failure mode is also defined.

Step 5: Calculate the risk of each failure mode.

Using the severity and probability of occurrence (also detection level if available), calculate the risk of each failure mode.

RisK = Severity x Occurrence (x Detection)

Step 6: Define safety controls for each failure mode.

For each failure mode, define the preventive measures to mitigate it's causes or effects.

Example FMEA worksheet

Failure Mode Effects Analysis

System Description: Landing Gear

Operation Mode: Flight - Level 2

Item Number	Item Description	Function	FM. Id.	Failure Mode	Local Effect	Next Higher Effects	End Effects	Sev.	Detection Method	Compensating Provisions	Remarks
1.1.1	Main Pump	Provides pressure when requested by Pilot Command	1	Fails to operate	No effect during this phase	No effect during this phase	No effect	IV	Indication to pilot	None	
			2	Untimely operation	Untimely hydraulic pressure in Main Hydraulic Generation Assembly	Untimely hydraulic pressure from Main Hydraulic Generation Assembly to Actuator Assembly	Untimely extension of Landing Gear	I	Indication to pilot	None	
1.1.2	Check Valve (Main)	Prevents reverse flow	1	Stucked closed	Loss of fluid flow through the Main Generation Assembly check valve	No effect during this phase	No effect	IV	Indication to pilot	None	
			2	Stucked open	Permits fluid flow through the main assy check valve when not required	No effect during this phase	No effect	IV	Undetected	None	

Hazard and Operability study (HAZOP)

- HAZOP, is a technique to identify and prevent the unwanted deviations of system functions.
- The system deviations are identified by combining functional parameters (such as flow, pressure, etc.) of components with predefined guidewords.
- Common guidewords used in HAZOP are:

  No – Not provided at all

  More – Provided more than design intent

  Less – Provided less than design intent

  As well as – Provided together with another parameter

  Part of – Provided partly

  Reverse – Provided opposite or another than intended

  Other than – Substituted completely by another parameter

HAZOP procedure

Step1: Define system under assessment.

Define scope and boundary of the system. Identify the system operation, components and functions. Gather all information about system components and its functions.

Step 2: Identify functional parameter or design intentions.

For each of the components or functions, identify the functional parameters with which the component was designed for. For example, a pump can include parameters such as flow rate, pressure and start-up/shut-down.

Step 3: Identify the system deviations using guidewords.

By combining the functional parameter and the guidewords, identify the system deviations.

HAZOP procedure

Step 4: Identify the potential effects.

Identify how the system deviation can affect the component or overall system. In detailed HAZOP analysis, the severity level of the failure mode is also defined.

Step 5: Identify the potential causes.

Using the system information and brainstorming, identify the potential causes (component failures, human errors, software issues etc) of each potential deviation. In detailed HAZOP analysis, the probability of occurrence (possibility of occuring) for each failure mode is also defined.

HAZOP procedure

Step 6: Calculate the risk of each system deviation.

Using the severity and probability of occurrence (also detection level if available), calculate the risk of each system deviation.

RisK = Severity x Occurrence (x Detection)

Step 7: Define safety controls for each system deviation.

For each system deviation, define the preventive measures to mitigate it's causes and effects.

Example HAZOP worksheet

STUDY TITLE: AUTOMATIC TRAIN PROTECTION SYSTEM								**SHEET:** 1 of 2		
REFERENCE DRAWING No.: ATP BLOCK DIAGRAM					**REVISION No.:** 1			**DATE:**		
TEAM COMPOSITION: DJ, JB, BA								**MEETING DATE:**		
PART CONSIDERED:				INPUT FROM TRACKSIDE EQUIPMENT						
DESIGN INTENT:				TO PROVIDE SIGNAL TO PES VIA ANTENNAE GIVING INFORMATION ON SAFE SPEEDS AND STOPPING POINTS						
No.	**Element**	**Characteristic**	**Guide word**	**Deviation**	**Possible causes**	**Consequences**	**Safeguards**	**Comments**	**Actions required**	**Action allocated to**
1	Input signal	Amplitude	NO	No signal detected	Transmitter failure	Considered in separate study of trackside equipment			Review output from trackside equipment study	DJ
2	Input signal	Amplitude	MORE	Greater than design amplitude	Transmitter mounted too close to rail	May damage equipment	Checks to be carried out during installation		Add check to installation procedure	DJ
3	Input signal	Amplitude	LESS	Smaller than design amplitude	Transmitter mounted too far from rail	Signal may be missed	As above		Add check to installation procedure	DJ
4	Input signal	Frequency	OTHER THAN	Different frequency detected	Pick up of a signal from adjacent track	Incorrect value passed to processor	Currently none		Check if action is needed to protect against this	DJ
5	Antennae	Position	OTHER THAN	Antennae is in other than the correct location	Failure of mountings	Could hit track and be destroyed	Cable should provide secondary support		Ensure that cable will keep antennae clear of track	JB
6	Antennae	Voltage	MORE	Greater voltage than expected	Antennae short to live rail	Antennae and other equipment become electrically live			Check if there is any protection against this occurring	DJ

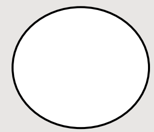
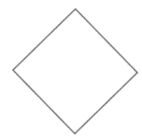
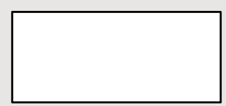
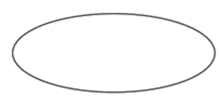
Fault trees analysis (FTA)

- An FT is a logical diagram constructed by deductively developing a specific system failure, through branching intermediate fault events until a primary event is reached.

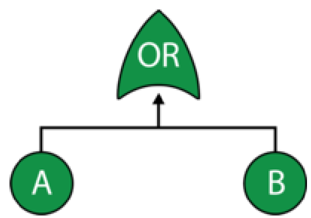
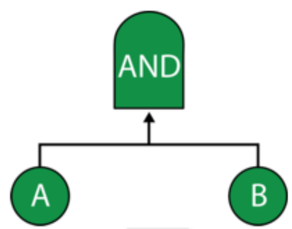
- A fault tree diagram construction consists of two categories of graphical symbols:

1. Event symbols
2. Logic symbols

FTA common events and symbols

Symbol name	Symbol	Description
Basic event		A basic initiating fault or failure event.
Undeveloped event		An event that could have been expanded further into fault tree but was not for the analysis.
Output event		An event that is dependent on the logic of the input events
Conditioning event		A specific condition that can apply to a gate. (only if this condition is met, the output occurs)

FTA common gates and symbols

Symbol name	Symbol	Description
OR gate		OR gate indicates that the output occurs only if one of the input events occur. Either A or B
AND gate		AND gate indicates that the output occurs only if all of the input events occur. Both A and B

FTA process:

Step1: Define system under assessment.

Define scope and boundary of the system. Identify the system operation, components and functions. Gather all information about system components and its functions.

Step 2: Define the top-level fault to analyse.

Define the top-level fault in system for which the fault tree is to be developed.

Step 3: Identify the combination of events that can lead to the top-level fault .

Identify the causes that can lead to the top-level fault. This should be done by using the symbols of events and gates.

FTA process:

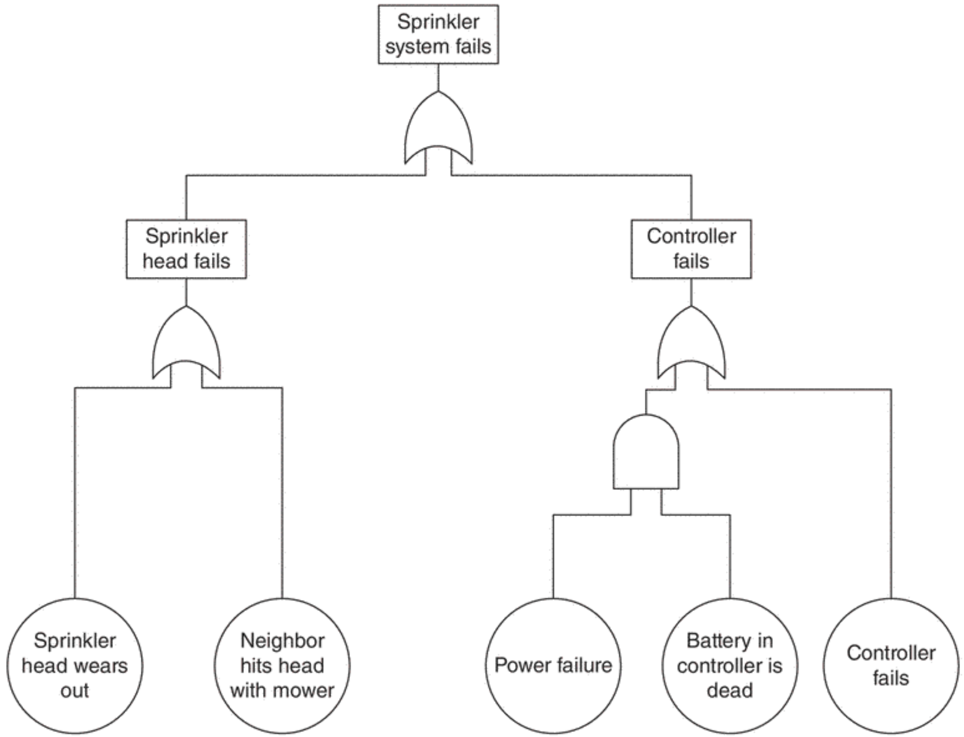
Step 4: Develop the tree further.

Develop the tree further until the root causes are identified or until the desired details are acheived.

Step 5: Define safety controls for the basic events.

For each of the identified basic events, define the preventive measures to mitigate it's causes and effects.

Example FTA diagram



Hazard analysis conclusions

- Several methods for analyzing hazards in system exists.

- The main principle of these methods is to identify the hazards, its effects and its causes.

- In detailed hazard analysis, the risk of each hazards are also calculated, which is determined by defining the severity and probabbility of occurrence.

- The end goal is to define the safety controls to mitigate the effects and causes.

Aalto University
School of Engineering

CA, LL, and FQuiz

Course assignment

Introduction to the course assignment …..

Learning logs

Please return the second learning log by Sunday 17.09 at 23:59

Aalto University
School of Engineering

Thank you

Next lecture more about system safety engineering tools