Introduction

What is a risk?

- Something undesired that can happen
- The probability of an harm
- ***The set of accident scenarios, their consequences and probabilities***

What is a hazard?

- An event that can happen
- ***The potential for harm or an adverse effect***
- A risk to people, objects and enviroment

What is resilience?

- The ability of the system to recover its functionality after an accident
- The ability of the system to prevent and mitigate from the occurrence of hazards
- The ability of the system to keeping its functionality for a given mission time
- ***The ability of the system to prevent the occurrence of hazards, absorb their impact in case of occurrence and recover from them***

What is reliability?

- The characteristic of a system to function with a certain degree or belief
- ***The ability to perform an assigned task for a given time***
- The ability of the system to function safely during its mission time

What is a barrier against the failure of a system?

- The set of physical boundaries that protects the system from external events
- A characteristic of the system that prevents the occurrence of hazards
- ***A procedure or physical boundary that prevents and/or mitigates the occurrence and impact of hazards***

A probabilistic risk assessment:

- Estimates the probabilities of hazardous events to the system and guides the design of the protective barriers
- ***Based on the available knowledge, identifies the accident sequences of the system, and quantifies their probabilities and consequences, to inform the decision makers***
- Quantifies every risk to the system in order to guaranteee the continuation of its functionality in safe condition

In a probabilistic risk assessment:

- ***All the risks are identified and accounted for***
- A multidisciplinary and multidimensional approach is needed in order to account as much as possible for the unknown unknowns
- Most of the attention should be put on those events that have the worst consequences on the system

Reliability of simple systems (1)

Given event A and its indicator variable XA, event B and its indicator variable XB, then X_(AuB)=

- XA + XB
- XAXB
- ***XA + XB - XAXB***

Event A is statistically independent from event B, when:

- P(AuB) = P(A) + P(B)
- ***P(A|B) = P(A)***
- P(A|B,C) = P(A|C)
- P(A,B) = P(A) P(B)

Given a union of non-mutually exclusive events: U_(i=1,..,n) E_i, the upper bound of P(E_U) =

- sum_(j=1)^n of (P(E_j) – sum_(i=1)^(n-1) of (sum_(j=i+1)^n of(E_i *intersecato* E_j)))
- ***sum_(j=1)^n of (P(E_j))***
- sum_(j=1)^n of (P(E_j) + sum_(i=1)^(n-1) of (sum_(j=i+1)^n of (E_i *intersecato* E_j)))

What is the mathematical definition of the reliability of a component?

- The distribution of the time t to failure of a component
- Probability that the component fails before time t
- ***Probability that the component survives up to time t***

The second period indicated by the hazard function of a component represents.. and the time-dependent characteristic of its failure rate is..

- ***useful life; constant***
- infant mortality; decreasing
- ageing; increasing

Failure time of a component is a random variable t. It's known that failure rate of the component is a constant lambda: then, the mean time to failure of the..

- ***1/lambda***
- t/lambda
- lambda*t

For a Poisson distribution, if its mean value (expectation) equals 1, the probability P(k=1) is?

- ***1/e***
- e
- e/2

Reliability of simple systems (2)

What is reliability?

- ***The ability of a system to perform a required function, under stated conditions and for a defined period of time***
- The ability of a system to function safely for a mission time T
- A quantity that defines the ability of the system to fulfill its assigned mission at any time t of his lifetime

What kind of failures are difficult to be prevented by improvement in design, manufacturing, maintenance?

- Early failures
- ***Random failures***
- Wear-out failures

When the age of a component is considered to influence its failure process so that the hazard rate does not remain constant throughout the lifetime, what distribution best describes the time to failure of the component?

- Exponential distribution
- ***Weibull distribution***
- Poisson distribution

For a system composed of 2 identical components in series with hazard rate of each component of 0.5 per hour, what is the mean time to failure of the system?

- 0.5 h
- ***1 h***
- 2 h

For a system composed of 2 identical components in series with mean time to failure of each component of 2 h, the hazard rate of the system equals?

- ***1 per hour***
- 1/2 per hour
- 2 per hour

Consider a system composed of 2 identical components in parallel with failure rate of 0.5 per hour. What is the mean time to failure of the system?

- 1 h
- 2 h
- ***3 h***

Consider a 2 out of 3 system with failure rate of each component of 0.5 per hour. What is the mean time to failure of the system?

- 1 h
- 1.5 h
- ***1.67 h***

Availability of systems

For the systems which must perform their function within an assigned period of time, which among these quantifies the ability to achieve the desired objective without failures?

- ***Reliability***
- Availability
- Resilience

[We defined reliability as the probability that no failures occure until the time of interest, i.e. the probability of survivng/functioning without failures until the time of interest. It's the probability that the time to failure is larger than the assigned period of time.]

Which among these quantifies the ability of a system to perform its assigned function at any specific moment in its life time?

- Reliability
- ***Availability***
- Resilience

[We defined availability as the probability of finding a system functioning at a given (specific) time.]

Limiting/asymptotic availability is a concept that applies to situations in which:

- the failure occured just now
- the maintenance is undergoing
- ***the failures are repaired***

[The limiting availability is the long time value of the availability of a component which undergoes failures with a given distribution and as soon as the component fails, it starts the repair. We look at the limiting availability as a single value to represent the ability of the component to be available in situations where the component can fail and upon failures repairs occur.]

Consider a component under periodic inspection. Which among these best allows evaluating its perfomance and why?

- The repair time, because if we minimize it the component can recover its functionality faster and is able to perform its function for more time in tis lifetime.
- ***The average unavailability, because it considers the average downtime of the component relative to the period of time T in which the component is performing its function.***
- The average availability, because if we maximize it the component can be found working more on average.

For a system composed of 2 identical components in series, the mean time between failures MTBF=10 years, the mean down time MDF=4 hours, the unavailability of the system is:

- ***10-4***
- 10-5
- 10-6

[Series system → total unavailability = sum of the unavailabilities of the components. For each component the availability is given by MDT/(MTBF + MDT).]

For a system composed of 2 identical components in parallel, the mean time between failures MTBF=5 years, the mean down time MDT=5 hours, the unavailability of the system is:

- 1.3 * 10-6
- ***1.3 * 10-8***
- 1.3 * 10-10

[Parallel system → total unavailability = multiplication of the unavailabilities of the components.]

Fault tree analysis

The intersection of events (AND Gate) is true if:

- ***All events are true***
- At least one event is false
- At least one event is true

The union of events (OR Gate) is false if:

- At least one event is false
- At most one event is true
- ***All events are false***

Which of the following statements is wrong

- Coherent structure functions can be expressed in reduced expressions in terms of minimal path sets
- ***A cut set is a set of components whose functioning ensures the failure of the system***
- Those components appearing in low order minimal cut sets (mcs) or in many mcs are most critical

Which component is shared among all the minimal cut sets that can be found from the following structure function:
$T = 1 - (1-L)\,[1 - (1-(1-A)(1-C))\,(1-(1-B)(1-D))\,]$?

- A
- B
- C
- D
- ***L***
- L and A

In fault-tree failure analysis, a primary event is:

- dependent on events that are higher in the hierarchy of the tree
- the top event of the tree
- ***considered independent and not further broken down***
- the output of a logic gate

Event tree analysis

The probability of the top event FIRE in the given fault tree example (Fig. 1) is:

- ***0.0735***
- 1
- 0.0465
- 0.5

Event trees are _____ logic methods

- deductive
- ***inductive***
- abductive

[Instead, fault trees are deductive (since they start from the starting event and they deduce the logic).]

An event tree is developed from a given:

- initial time
- key component
- mission time
- ***accident initiator***
- basic event

Event tree analysis aims at

- ***computing the probability of the accident sequence***
- estimating the reliability of the system
- characterizing the threats to the system

For defining a system ET, after selecting the accident initiator, we need to first:

- specify failure/success states for all components
- ***identify safety/protection systems demanded by the occurrence of the accident initiator***
- generate the accident sequences that can lead to failure

How many initiating events can be investigated in an event tree?

- ***1***
- maximum 3
- no theoretical limitation

When building an event tree, we need to consider:

- the time order of the events
- the logic order of the events
- ***both the above***

To compute the probability of an accident sequence in a system event tree one must:

- multiply the probabilities of failure of the systems along the sequence
- sum the conditional probabilities of the events along the sequence
- multiply the probabilities of the system events along the sequence
- ***multiply the conditional probabilities of the events along the sequence***
- sum the probabilities of the system events along the sequence

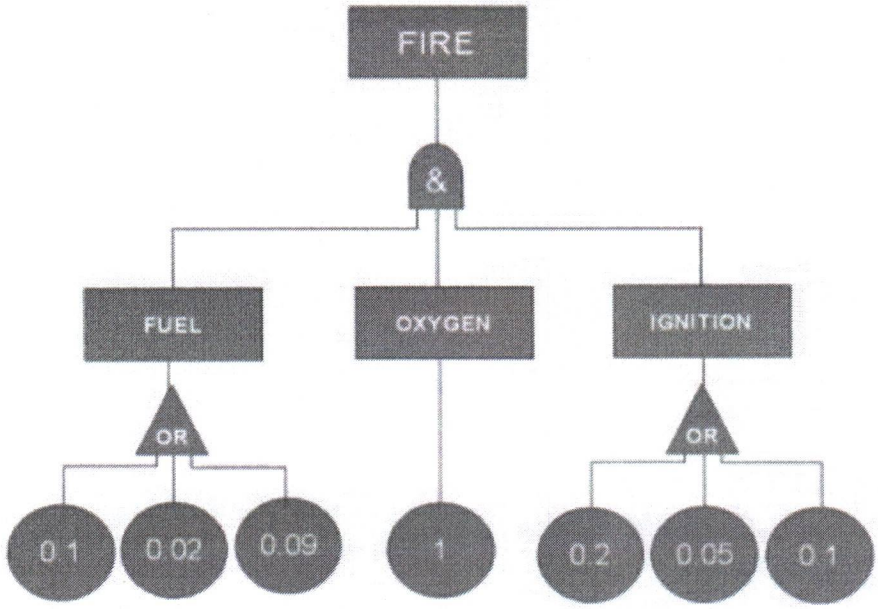

Fig. 1

Markov

Markov analysis is a technique that deals with the probabilities of future states occupancies by …

- using Bayes' theorem.
- ***considering known state transition probabilities***
- time series forecasting
- none of the above

Markov analysis might be effectively used for …

- technology transfer studies
- university retention analysis
- machine breakdowns
- accounts receivable analysis
- ***all of the above***

In Markov analysis, the probability that a system will change state from one time step to the next is given by the

- identity matrix
- matrix of state probabilities
- ***matrix of transition probabilities***

The system states of Markov Processes must satisfy one of the following conditions…

- infinite number
- mutually exclusive or exhaustive
- ***mutually exclusive and exhaustive***

Which of the following hypothesis is correct for a Discrete-Time Finite-State Markov Chain…

- ***the time interval Δt is small such that only one event (i.e., stochastic transition) can occur within it***
- the state space can be uncountable
- the probability of a future state depends on its entire life history

Given the initial state vector (1, 0) and the transition matrix (0.13 0.87; 0.91 0.09), find the state vector corresponding to two steps later (n = 2).

- (0.2002, 0.7998)
- (0.8086, 0.7998)
- ***(0.8086, 0.1914)***
- (0.7998, 0.2002)

Monte Carlo

Monte Carlo simulation:

- is a computational technique to account for risk in systems
- is based on sampling of random numbers and serves only to model random processes
- ***simulates a stochastic process by sampling realizations of possible outcomes from probability distributions of the stochastic variables***

When defining a Monte Carlo simulation for system reliability, the sources of uncertainty to consider are:

- ***the states of the components of the system and the time at which the components transit to a new state***
- the states of the components that the system is composed of and their transition rates
- the number of components to consider and the number of their states

When performing a Monte Carlo simulation for the calculation of system reliability, a large set of system random walks is simulated and, then:

- the reliability of the system corresponds to the reliability associated to the random walk with the earliest failure of the system among all random walks
- ***the reliability of the system is computed at each time step as the number of times the system did not fail averaged over all random walks***
- the reliability of the system is the reliability associated to the random walk with the earliest failure of a component

In the indirect Monte Carlo simulation:

- ***at each time step, the equivalent system transition rate is computed as the sum of the transition rates of the components out of their current states***
- the next system transition time is computed after sampling the component undergoing a transition to the next state
- the system transition rate is computed as the average of the transition rates of the components and, then, it is used to sample the next system transition time

In the direct Monte Carlo simulation:

- the transition time to the failed state for each component is sampled and, then, the system transition time is defined as the average among these
- ***each component transition time is directly sampled and, then, the next system transition time is defined as the first occurring component transition time***
- the system transition rate is computed as the average of the transition rates of the components and, then, it is used to sample the next system transition time

Dependent failures

Implicit methods for dependent failure analysis:

- Involve the identification and treatment of the specific root causes that induce a common cause failure
- ***Model the multiple failure events based on parameters***
- Involve only the analysis of complex system interdependencies, for which a direct identification and treatment is not doable

In the method "event trees with boundary conditions" for a system composed of 2 subsystems S1 and S2, with shared components C1 and C2, the event tree ET = {IE, S1, S2}:

- is modified as ET' = {IE, C1, S1, C2, S2} and the minimal cut sets for each possible sequence of events are found
- ***is modified as ET' = {IE, C1, C2, S1, S2} and the minimal cut sets for each possible sequence of events are found***
- is modified as ET' = {IE, C1, C2, S1, S2} and the minimal cut sets are found by merging the FT of S1 and S2 and developing the structure function

What is the difference between the method M1="event trees with boundary conditions" and M2="fault tree links"?

- In M1 the event trees consider all the possible sequences of the events, whereas M2 considers the event trees separately for each subsystem with common cause failure
- Both M1 and M2 merge the event trees for the subsystems with common cause failure and FT for the identification of the MCS
- ***M1 requires a priori knowledge of the shared equipment dependence, whereas M2 accounts for it automatically in the minimal cut sets***

Consider a parallel system of N exponential compontents with failure rate L. To consider the common cause failure (CCF) with the beta-factor model:

- The CCF is considered as component in series with reliability exp(-(1-beta)*L*t) whereas the reliability of the component is modified into exp(-beta*L*t)
- The CCF is considered as component in parallel with reliability exp(-(1-beta)*L*t) whereas the reliability of the components is modified into exp(-beta*L*t)
- ***The CCF is considered as component in series with reliability exp(-beta*L*t) whereas the reliability of the components is modified into exp(-(1-beta)*L*t)***

Consider a parallel system of N exponential components with failure rate L, subject to a common cause failure (CCF) with occurrence rate mu. Which among the following is true?

- ***The binomial failure rate model considers that, upon the occurrence of the CCF, each component has a failure probability p, binomially distributed***
- The binomial failure rate model considers the CCF as a component with failure rate mu in series with the system and the failure rate of the components is modified into L plus a quantity proportional to the failure probability of the components
- The binomial failure rate model is always more conservative than the beta factor model, provided that the parameters are estimated using the same experimental data