System*:** Technical and organizational means for the autonomous fulfillment of a task. Consist of h/w, s/w, ppl (service and maintenance personnel) & logistic assistance. Ex. A complete Aviation system includes aircraft, launch site, aviation s/w, and ground crew. ***Technical System: System where influences by people and logistics are ignored. ***Quality:*** Degree in which the inherent attributes of an entity fulfill quality requirements .***Quality Req*:** Expectation or demand defined (by a customer) that is generally assumed or mandatory. ***Quality Characteristic:*** Property of an entity on the basis of which its quality is described and estimated, but which makes no statement about the degree of fulfillment of the characteristic. **Quality Measure:** Measure which allows to draw conclusions on the fulfillment of specific quality characteristics. For instance, MTTF (Mean Time To Failure) is a quality measure of the quality characteristic Reliability. **Safety.** State where the danger of a personal or property damage is reduced to an acceptable value. **Technical Safety:** Measure for the ability of a failure afflicted item to endanger neither persons, property nor the environment. **Correctness:** An artifact is correct if it is consistent to its specification. **Completeness:** A system is functional complete, if all functions required in the specification are implemented. This concerns the treatment of normal cases as well as the interception of failure situations. **Robustness:** Property to deliver an acceptable behavior also in exceptional situations (e.g. ability of a software to detect hardware failures) .property of the specification than of the implementation .gradual character. **Reliability:** Measure for the ability of an item to remain functional, expressed by the probability that the required function is executed failure-free under given working conditions during a given time period **Availability:** Measure for the ability of an item to be functional at a given time. **A=MTBF/(MTBF+MTTR)**. **Failure**: Inconsistent behavior w.r.t. specified behavior while running a system (happens dynamically during the execution) => Each failure has a time-stamp. **Fault, defect:** Statically existent cause of a failure, i.e. a „bug"(usually the consequence of an error made by the programmer) .**Error:** Basic cause for the fault (e.g., misunderstanding of a particular statement of the programming language). **Accident** is an undesired event that causes death or injury of persons or harm to goods or to the environment. **Hazard** is a state of a system and its environment where the occurrence of an accident depends only on influences that are not controllable by the system. **Risk** is the combination of hazard probability and severity of the resulting accident. **Acceptable Risk** is a level of risk that authorities or other bodies have defined as acceptable according to acceptance criteria. | ***Risk*: R = H * S; H:** expected frequency of the occurrence of an event that leads to a particular harm **S:** expected severity of the harm. **H** determined by **FTA.** Severity of a harm quantified on subjective basis .Financial loss, injuries, or death. **Aim of risk acceptance** is to bring about a decision in a systematic and founded fashion whether the risk under consideration can be accepted or not. **Costs for risk reduction** do not increase linearly with reducing residual risks. Merely, they are disproportionately high, there exists an economically optimal trade-off between the costs of a system and its residual risks. This trade- off could be acceptable, but it can also be the case that the residual risks are still too high and further risk reduction is demanded.

Risk Accpt. Influencing factors •Degree of benefit? Great distances in aviation: Is the exposure to this particular risk related to travel distance or time spent in the aircraft? •Who is at risk? Astronauts, sick persons, railway travelers, service personnel, uninvolved public•Degree of self-determination? – Driving a car vs. taking an elevator•How many people are at risk? – Car vs. nuclear power plant •Severity?Death or injuries?**MEM-Minimal Endogenous Mortality:** Method is based upon the fact that there exist different mortality rates in society, depending on age and gender. These deaths are partly caused by technical systems. MEM now compares the risks due to a new system with already existing risks caused by „natural "mortality. MEM demands that the new system does not significantly contribute to the existing mortality caused by technical systems. Adv. Can be used for a novel system, where comparison with pre-existing systems is not feasible. Disadv: - Underlying referenced time basis left unclear. - Not clear if exposure to a certain hazard is for particular individual or public – Questionable whether focusing on single system is sufficient as in numerous systems whose individual risks might accumulate.

Collective Risk Fatality:

$$RF_{total} = \sum_{All\ hazards\ i} A_i \cdot F_i \cdot \frac{N_{endangered\ i}}{N_{all}} \cdot HR_i$$

HRi [1/t]:Rate, with which hazard i occurs. S=Ai Fi [1] Extent of damage (Cost of hazard). Ai [1] Probability that hazard i will result in an accident (typically from event trees, fault trees).Fi [Persons] Measure of death or injury persons caused by accident. Nendangered [Persons] Number of the actually endangered persons in danger area of hazard I. Nall [Persons] Total number of system users.

Individual Risk Fatality:

$$IRF_i = \sum_{hazard\ j} NP_i \cdot \left[HR_j \cdot (D_j + E_{ij}) \cdot \sum_{Accidents\ A_k} C_{k,j} \cdot F_{k,j} \right]$$

NPi [1/t] Usage profile (number of usages per time)
HRj [1/t] Rate, with which hazard j occurs
Dj [t] Duration of hazard j
Eij [t] Time during which individual i is exposed to hazard j
Ck,j [1] Probability that hazard j leads to accident k
Fk,j [Persons] Probability that death or injury is caused by accident k.

GAMAB – Globalement Au Moins Aussi Bon:-Requires the existence of a reference system with accepted residual risks •Word globalement (overall) plays an important role. What counts for at the end is the sum of the residual risks of the overall system. • GAMAB requires the determination of the residual risks of the system under consideration and their comparisons with the residual risks of the reference system. This can be achieved by e.g. an explicit risk analysis. The system is acceptable if, all in all, it is not worse than the reference system.

ALARP – As Low as Reasonably Practicable.

•ALARP aims to minimize risks under consideration of economic and social aspects. ALARP tries to assess what is technically feasible within the context of financial feasibility and acceptance in society •The overall risk can fall into one of three possible ranges

1.The risk is negligible and can be accepted without further measures
2.The risk is higher than commonly accepted but falls below the upper limit of tolerability
3. The risk is unacceptably high, measures to reduce the risk must be taken.

•Correct categorization requires an assessment of the residual risks and a comparison with corresponding acceptance values. •These acceptance values are specific to each sector and group of people. •E.g. in the sector railway systems, higher residual risks are accepted for an employee than for the ordinary passenger.

•ALARP requires that the residual risk of a new system falls below it.

Safety Integrity."probability of an E/E/PE* safety-related system satisfactorily performing the required safety functions under all the stated conditions within a stated period of time".**Safety Integrity Level (SIL):** "discrete level (one out of a possible four) corresponding to a range of safety integrity values where safety integrity level 4 has the highest level of safety integrity and safety integrity level 1 has the lowest"

Risk parameter Classification: C1: Minor injury. **C2**: Serious permanent injury to one or more persons; death of one person. **C3**: Death of several people. **C4**: Great many people killed

F1: Rare to more often exposure to the hazardous zone. **F2**: Frequent to permanent exposure to the hazardous zone. **P1**: Possible under certain conditions. **P2**: Almost impossible

W1: A very slight probability that the unwanted occurrences will happen and only a few unwanted occurrences are likely **W2**: A slight probability that the unwanted occurrences will happen and few unwanted occurrences are likely. **W3**: A relatively high probability that the unwanted occurrences will happen and frequent unwanted occurrences are likely.

The Failure Mode, Effects and Criticality Analysis (FMECA) is a preventive method for the identification of problems, their risks and effects

FMECA goals . • Detection of hazards and problems • Identification of potential risk
• Quantification of risks • Determination of corrective measures
Performed as component FMECA (e.g. for a subsystem), as system FMECA (a complete system) or as process FMECA (e.g. for a development process) .

FMECA steps :

• Fault analysis: Collection of possible faults including available information about the type, causes and consequences • Risk evaluation with the aid of the risk priority number
RPN = occurrence probability * severity of consequences * probability of non-detection .
• Formulate proposed actions • Decide for actions • Analyze residual risk (recalculate RPN)
• Conduct cost-benefit analysis • Comparison of RPN before and after the improvement
• Relate obtained improvement to invested effort

FTA Procedure:1. Identify the objective 2. Get familiar with operation and success criteria of the system 3. Define the top-event 4. Define the scope 5. Define resolution 6. Define ground rules 7. Construct the FT. 8. Evaluate the FT . 9. Interpret and present the results .

$P_{out} = \prod_{i=1}^{n} P_i$	$P_{out} = 1 - \prod_{i=1}^{n} (1 - P_i)$
AND Gate	OR Gate

RBD: Interconnection of all components of a system which are involved in performing the required function; represented as a flow chart. RBDs distinguish only two states (intact/failed). R(t)=1-F(t) is the probability that at time t no failure has occurred yet.

Serial Connection

$$R_S(t) = R_{K_1}(t)\ R_{K_2}(t)\ R_{K_3}(t)\ \ldots\ R_{K_n}(t) = \prod_{i=1}^{n} R_{K_i}(t)$$

Parallel Connection

$$R_S(t) = 1 - F_S(t) = 1 - \prod_{i=1}^{n} F_{K_i}(t) = 1 - \prod_{i=1}^{n} (1 - R_{K_i}(t))$$

Markov Models

• Based on a description of the system behavior with state machines.
• Common assumption - The probability of the next state depends on the current state; it is independent from previous states, i.e. Markov models do not take into account the history

Model types, e.g.:

• Discrete time models (Markov chain)
Markov chains assume that state changes occur at discrete points in time. e.g. Throwing a coin.

$$\frac{dP_A(t)}{dt} = -\lambda P_A(t) + \mu P_B(t)$$

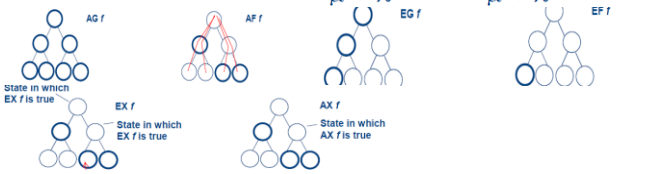
$$\frac{dP_B(t)}{dt} = \lambda P_A(t) - \mu P_B(t) = -\frac{dP_A(t)}{dt}$$

$$P_A(t) + P_B(t) = 1$$

• Continuous time models; also called Markov processes. Are continuous time models.

$$P_A(t) = \frac{\mu}{\mu + \lambda} + \left(c - \frac{\mu}{\mu + \lambda}\right) e^{-(\mu + \lambda)t}$$

$$P_B(t) = 1 - P_A(t) = 1 - \left[\frac{\mu}{\mu + \lambda} + \left(c - \frac{\mu}{\mu + \lambda}\right) e^{-(\mu + \lambda)t}\right]$$



A **Petri Net** N contains at least places (P), transitions (T) and a flow relation (F) as well as an initial marking (M0): N = (P, T, F, M0):

C/E Net	P/T Nets *(P/T Net, Place/Transition Net)*	Pr/T Nets (Predicate/Transition Net)	Timed Petri Net
Objects, respectively tokens, are of **Boolean** data type	Places can obtain **more than one** token. (in C/E nets only one token)	Tokens are **colored**: They can be individualized, they do have a description (unlike other tokens)	Similar as in C/E net
Transitions are interpreted as **Events**	Transitions must release or add as many tokens when firing as the **weights** that are given on the arcs.	Transitions have a **firing condition** and a **firing effect**.	There is a ***firing delay*** *associated* with each **transition**. This delay specifies the time that the transition has to be *enabled*, before it can actually fire:
Places are denoted as **Conditions. Binary Condition**: Each place is allowed to receive exactly one or no token.	Places have a **capacity** (maximum number of tokens that may lie in one place): If it is to be bigger than 1, this will be denoted as **»K = ...«** at the place.	Places contain a number of tokens that can be Integers or variables.	Similar as in C/E net

SPN (Stochastic Petri Net) If the delay is a random distribution function (exponential distribution), the resulting net class is called stochastic Petri net.
• Delay is exponentially distributed
• Can be transformed into an equivalent Markov Process
GSPN (Generalized SPN) SPN plus immediate transitions (no delay) and inhibit edges. (To convert markov to GSPN, make μ to 1/μ and so on with λ)
DSPN (Deterministic SPN) GSPN plus deterministic transitions (delay is fixed). • Exponentially distributed delay + immediate transitions (no delay) + deterministic transitions (delay is fixed) and inhibit arcs
Fault Tree Analysis: Analysis method for the qualitative and quantitative evaluation of a specific failure of a system. • Goal of the **qualitative analysis** is the systematic identification of all possible failure combinations which lead to a predetermined undesired event. Find Minimal Cutsets, path-sets.
• Goal of the quantitative analysis is the determination of reliability parameters, e.g. failure rates w.r.t. the undesired event or unavailability of the system. disadv: no seq AND, inhibit - only basic boolean
Event: anything that happens with a certain probability.
Reliability Function R(t):
• F(t) gives the probability that at time t the (non-repairable) system has failed
• Thus R(t) = 1 - F(t) is the probability that at time t no failure has occurred yet
Probability Density f(t):

• The probability density f(t) describes the modification of the probability that a system fails over time:	$f(t) = \frac{d\,F(t)}{dt}$

Failure Rate: The failure rate is the relative boundary value of failed entities at time t in a time interval that approximates zero, referring to the entities still functional at the beginning of the time interval:

$$\lambda(t) = \frac{f(t)}{R(t)} = \frac{dF(t)\,/\,dt}{R(t)} = \frac{-\,dR(t)\,/\,dt}{R(t)}$$

• A **Cut Set** is a set of basic events, which in conjunction cause the top event
• A **(MCS)** is a cut set that no longer is a cut set if any of its basic events is removed• A **Path Set** is a set of basic events that, if they are false, inhibit the top event from occurring• A **(MPS)** is a path set that no longer is a path set if any of its basic events is removed.

$$P_{top} = \sum_{all\ MCS} P_{MCS_i} \qquad P_{MCS} = \prod_{all\ events\in MCS} P_i$$

•**Correctness has a binary character**, an item is either correct or incorrect
•A fault-free realization is correct •An artifact is correct if it is consistent to its specification •If no specification exists for an artifact, correctness is not defined. A system is functional **complete**, if all functions required in the specification are implemented. A correct system can have a low robustness.
•Accordingly, robustness is rather a property of the specification than of the implementation •A robust program is the result of the correct implementation of a good and complete specification •**Robustness has a gradual character**
Fussel Vasili: abs or relative % contribtn to the top event probability
Risk Reduction worth: decrease in top event prob, if a given event is assured not to occur

For each OR gate, generate as many entries as there are inputs...

$$\{(F_{sys})\} \xrightarrow{or} \{(F_{12}),(F_{13}),(F_{23})\}$$

For each AND gate, generate one entry containing all inputs...

$$\{(F_{sys})\} \xrightarrow{and} \{(F_1,F_2),(F_1,F_3),(F_2,F_3)\}$$

$$\Rightarrow P(F_{sys}) = P_{MCS,1} + P_{MCS,2} + P_{MCS,3} = P(F_1)\cdot P(F_2) + P(F_1)\cdot P(F_3) + P(\dots$$
$$\Rightarrow P(F_{sys}) = 3\cdot(0.03)^2$$
$$\Rightarrow P(F_{sys}) = 0.0027$$

MTBF, MTTF .measure for reliability , defines the mean value of the lifetime resp. the mean value for the time interval between two successive failures	$\overline{T} = E(T) = \int_0^\infty t\, f(t)\, dt$
The conditional probability that a system that operated failure free until t also survives the period delta t is (dice eg)	$\frac{R(t+\Delta t)}{R(t)}$

$$1 - \frac{R(t+\Delta t)}{R(t)} = 1 - \frac{1-F(t+\Delta t)}{1-F(t)} = \frac{1-F(t)-(1-F(t+\Delta t))}{1-F(t)} = \frac{F(t+\Delta t)-F(t)}{1-F(t)}$$

Thus, the probability that the **product fails within Δ t** is .
As the given probability for short time intervals Δt is proportional to Δt, we divide the term by Δt and determine the boundary value when Δt approximates 0

$$\lim_{\Delta t\to 0} \frac{1}{\Delta t}\,\frac{F(t+\Delta t)-F(t)}{1-F(t)} = \frac{1}{R(t)} \lim_{\Delta t\to 0} \frac{F(t+\Delta t)-F(t)}{\Delta t} = \frac{f(t)}{R(t)} = \lambda(t)$$

Thus the probability that a system, that is operational at time t fails within the (Short) time interval Δt, is approximately Δt λ(t) .
Example of Distribution Function.
• The failure rate λ is constant over time

$$\lambda(t) = \frac{f(t)}{R(t)} = \frac{dF(t)\,/\,dt}{R(t)} = \frac{-\,dR(t)\,/\,dt}{R(t)} = \frac{\lambda\, e^{-\lambda t}}{e^{-\lambda t}} = \lambda$$

• A constant failure rate causes an exponential distribution of the lifetime.
• Determination of the MTTF

$$\overline{T} = E(T) = \int_0^\infty t\, f(t)\, dt = \int_0^\infty t\,\lambda\, e^{-\lambda t}\, dt = \lambda \int_0^\infty t\, e^{-\lambda t}\, dt = \lambda \left[\frac{\lambda\, e^{-\lambda t}}{\lambda^2}(-\lambda t - 1)\right]_0^\infty = \frac{1}{\lambda}$$

If lifetime is exponentially distributed, the MTTF is the reciprocal of the failure rate and thus constant.

	Exponential Distribution. & Poisson	**Weibull Distribution.**
Life Distribution.	$F(t) = 1 - e^{-\lambda t}$	$F(t) = 1 - e^{-(\lambda t)^\beta}$; λ, β > 0
Density func..	$f(t) = \lambda e^{-\lambda t}$	$f(t) = \frac{dF(t)}{dt} = \lambda\,\beta\,(\lambda\, t)^{\beta-1}\, e^{-(\lambda t)^\beta}$
Reliability func..	$R(t) = 1-F(t) = e^{-\lambda t}$	$R(t) = e^{(-\lambda t)^\beta}$
Failure-rate.	λ(t)= λ	$\lambda(t) = \frac{f(t)}{R(t)} = \lambda\,\beta\,(\lambda\, t)^{\beta-1}$
MTTF	T= 1/ λ	

As the value of ß increases the failure rate increases.
Poisson Distribution

$$P_x(t) = \frac{(\lambda t)^x e^{-\lambda t}}{x!}$$

Musa Execution time Model: A software system fails due to errors in the software randomly at t1, t2, ... (t here refers to execution time, i. e. CPU-seconds)
• It is assumed that the number of failures observed in □t is linearly proportional to the number of faults contained in the software at this time
• μ(t) is the total number of failures for times t >= 0
• μ(t) is a limited function of t
• The number of failures is a monotonic increasing function of t
• At t=0 no failures have been observed yet: □(0)=0
• After very long execution time (t →∞) the value of μ(t) is equal to a. a is the total number of failures in infinite time. (There are also models where infinite numbers of failures are assumed to happen)
Model development :
• The number of failures observed in a time interval □t is proportional to □t and to the number of errors not yet detected .

$$\mu(t+\Delta t) - \mu(t) = b[a-\mu(t)]\Delta t \Rightarrow \frac{\mu(t+\Delta t)-\mu(t)}{\Delta t} = ba - b\mu(t)$$

With Δt→0 we get:	$\frac{d\mu(t)}{dt} = ba - b\mu(t) = \mu'(t)$
With μ(0)=0 and μ(∞)=a we get:	$\mu(t) = a\left(1-e^{-bt}\right)$
The failure rate is:	$\lambda(t) = \mu'(t) = abe^{-bt}$

The initial failure rate is proportional to the expected number of failures a, with the constant of proportionality b .

$$\mu(t) = a\left(1-e^{-bt}\right) = a\left(1-e^{-\frac{\lambda_0 t}{a}}\right) \qquad \lambda(t) = abe^{-bt} = \lambda_0 e^{-\frac{\lambda_0 t}{a}}$$

$$\mu(t) = a\left(1-\frac{\lambda(t)}{ab}\right) \Rightarrow \lambda(\mu) = b(a-\mu) = ab\left(1-\frac{\mu}{a}\right) = \lambda_0\left(1-\frac{\mu}{a}\right)$$

If λ is the present failure rate and a target λz is defined, Δ μ additional failures till occur until this target is reached .

$$\Delta\mu = \mu_z - \mu = a\left(1-\frac{\lambda_z}{\lambda_0}\right) - a\left(1-\frac{\lambda}{\lambda_0}\right) = a\left(\frac{\lambda-\lambda_z}{\lambda_0}\right)$$

The additional time Δt until this target is reached is .

$$\Delta t = t_z - t = -\frac{a}{\lambda_0}\left[\ln\left(\frac{\lambda_z}{\lambda_0}\right) - \ln\left(\frac{\lambda}{\lambda_0}\right)\right] = \frac{a}{\lambda_0}\left[\ln\left(\frac{\lambda}{\lambda_0}\right) - \ln\left(\frac{\lambda_z}{\lambda_0}\right)\right] = \frac{a}{\lambda_0}\ln\left(\frac{\lambda}{\lambda_z}\right)$$

$$P_0(t+\Delta t) = P_0(t)(1-\lambda\,\Delta t) \Leftrightarrow \frac{P_0(t+\Delta t)-P_0(t)}{\Delta t} = -\lambda\, P_0(t)$$

$$\lim_{\Delta t\to 0}\frac{P_0(t+\Delta t)-P_0(t)}{\Delta t} = \frac{d\,P_0(t)}{dt} = -\lambda\, P_0(t) \qquad R(t) = P_0(t) = e^{-\lambda t}$$

$P_x(t+\Delta t) = P_0(t)$ [P(x failures between t and t+Δt)]

$$= P_{x-1}(t)(\lambda\ \Delta t) + P_x(t)(1-\lambda\ \Delta t) \qquad P_x(t) = \frac{(\lambda t)^x e^{-\lambda t}}{x!}$$

$$\frac{P_x(t+\Delta t)-P_x(t)}{\Delta t} = -\lambda\left[P_x(t) - P_{x-1}(t)\right]$$

$$\mu(t) = \int_0^t \lambda(\tau)\, d\tau \quad \text{and} \quad P_x(t) = \frac{\mu(t)^x e^{-\mu(t)}}{x!}$$

This is called a non-homogeneous Poisson Process (NHPP)

Reliability-availability: For the majority of items, which are repairable.
Reliability is different from availability.Availability tells information the time an item is able to operate as a ratio to the time in service. It is driven by time lost.Reliability is the ability that an item can work failurefree under a given time period and given working conditions. It is driven by number of failures.However, for the items which cannot be repaired,such like light bulbs, ball bearings and smoke detectors. People just replace them with a new one when a failure takes place. In this case, reliability equals to availability.