Reliability of Technical Systems

Main Topics

1. Introduction, Key Terms, Framing the Problem
2. **→ Reliability Parameters: Failure Rate, Failure Probability, Availability, etc.**
3. Some Important Reliability Distributions
4. Component Reliability
5. Software Reliability
6. System Reliability: Structure and State Modelling
7. Dependent Failures
8. Human Reliability
9. Static and Dynamic Redundancy
10. Fault Tolerance
11. Advanced Methods for System Modelling and Simulation
12. Dependability

Qualitative: Reliability is the ability of a component/system to perform a required function under stated conditions for a specified period of time.

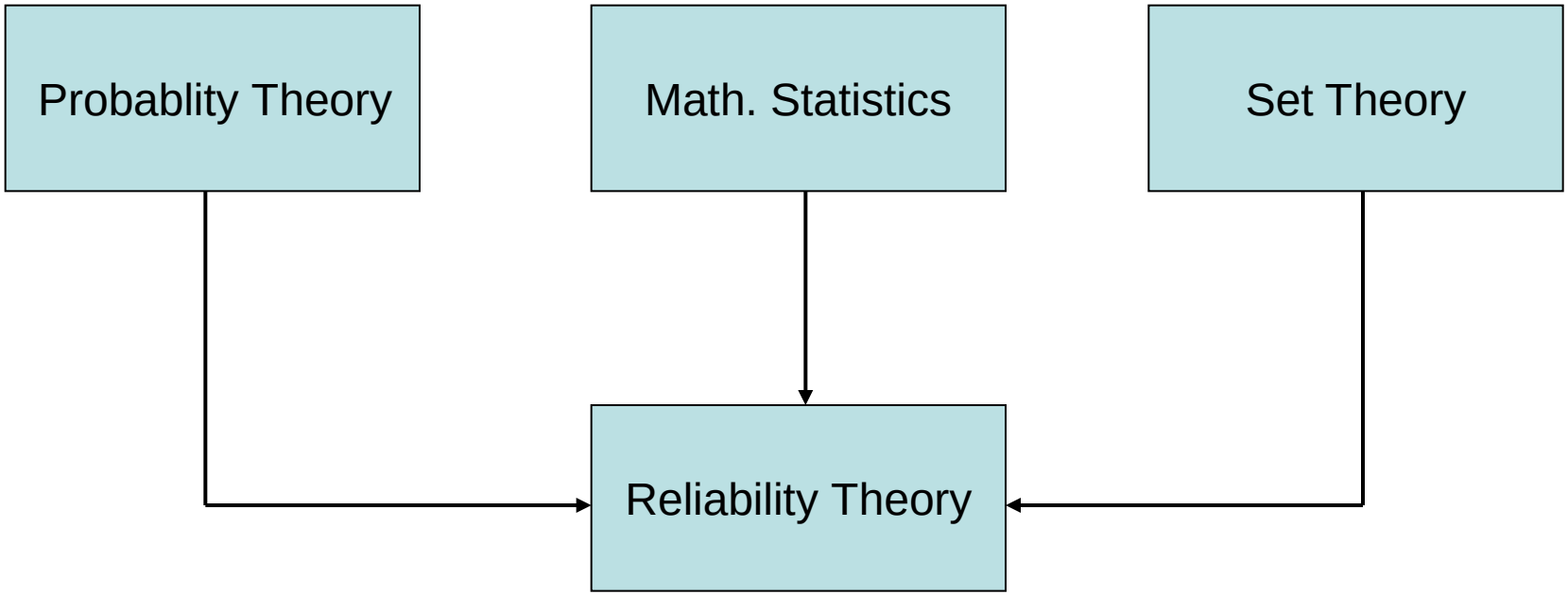
How can we estimate reliability?

How to evaluate e.g. how likely a system failure is within a certain period of time?

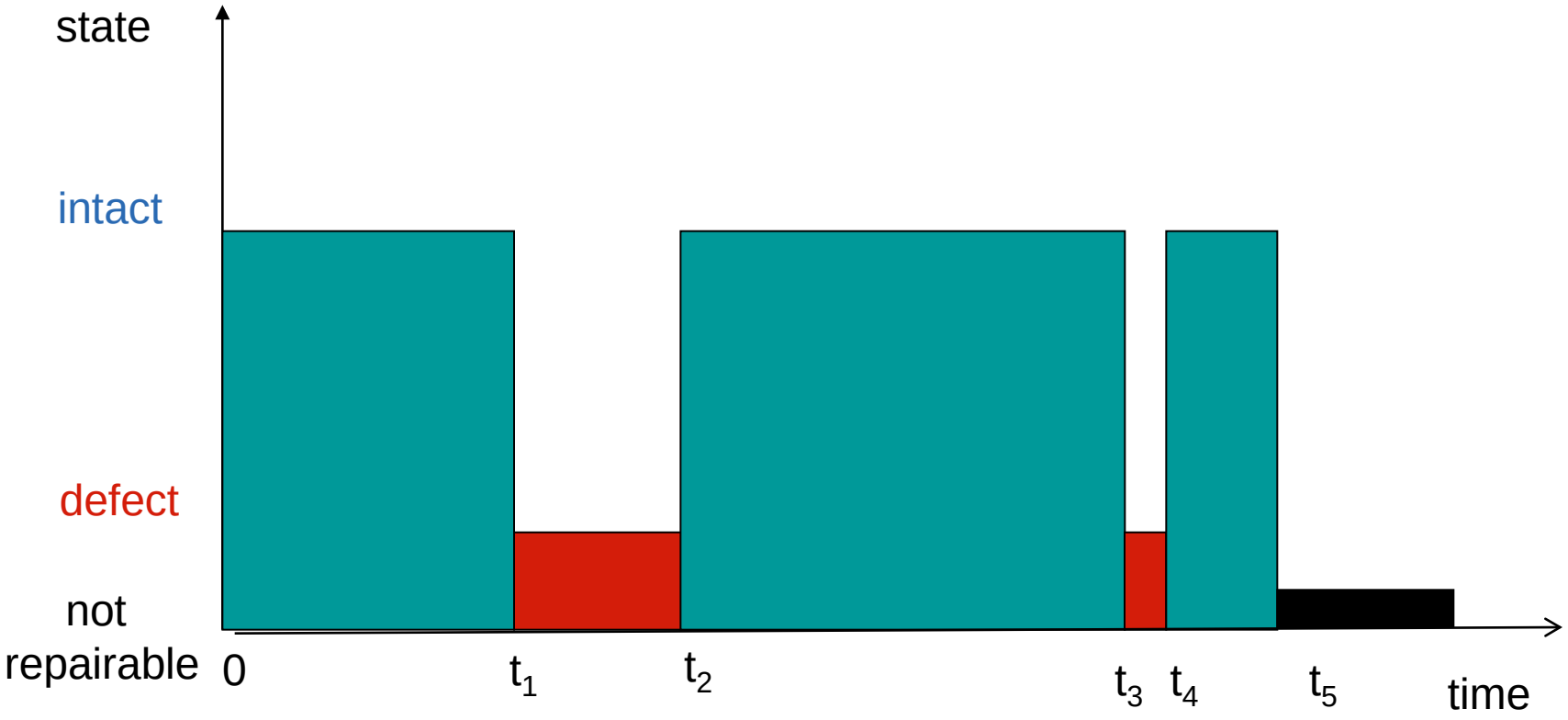
With particular probability:

Distribution Function

Subareas of the Mathematics as a Basis for the Reliability Theory



System State as a Function of Time



Essential Terminology

Probability	Occurrence	Frequency	Rate
Dimensionless parameter **between 1 and 0**. Fixed by the Kolmogorov axioms.	Occurrence bases on data and therefore belongs to a random test.	Occurrence over time.	Rate measures the current change of one parameter of units depending on the change of another one (usually time).
Classical: P. are usually taken and interpreted as *relative occurrence*.	*Absolute:* Number of events that occurred.		A rate can often be *empirically* estimated by taking of the average (relative occurrence) over a longer time interval.
Subjective: Degree of the expectation of an individual that a possible event occurs.	*Relative:* Regarding an event: Number of occurrences divided by the whole number of cases. Regarding time: See *rate, frequency.*		

Kolmogorov axioms (Andrey Nikolayevich; [1903-1987])

Given: set of events Ω,

σ-Algebra with the partial events A_i

The number Pr(A) is the probability of the event A, if, and only if,

1. Non negativity axiom: $0 \le Pr(A) \le 1 \quad \forall \quad A \in \alpha$

Pr(A) is a distinct determined, real positive number for all events A in α

2. Norming axiom: $Pr(\Omega) = 1$

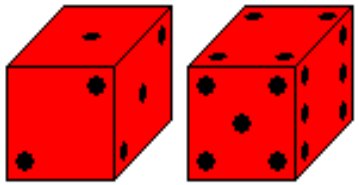
The sure event has the probability 1, also $\sum_{\text{alle } i} Pr(A_i) = 1$

3. Additive axiom: $Pr(A_1 \cup A_2 \cup \ldots) = Pr(A_1) + Pr(A_2) + \ldots.$

$A_1, A_2, \ldots. \in \alpha \qquad A_i \cap A_j = \varnothing \; \forall \; i \neq j \; (i, j = 0, 1, 2, \ldots)$:

Probabilities of contradicting, i.e. each other excluding, different events can be represented as a sum of single probabilities. Contradicting means that the connection of the different events leads to an impossible event Pr(A) = 0.

Random event* **(is an event chosen at random from a finite family of events):**



Appearing a number on top of the dice

The dice is used in many board games. The numbers 1 to 6 appear on the six sides of a cube. You throw the dice and let it roll to a standstill.

It is by chance which number appears on top!

This is the attraction of throwing the dice. It gives the game unexpected turns and adds excitement to it.

We can also do it for a statistical experiment. In this case a real number is assigned to an elementary event of a statistical experiment (throwing the dice).

* Failure occurrence is a randon event.

Random Variable

A function that assigns the elements of the result or event set of an experiment (random tests) to real numbers is called Random Variable.

Random Variables are denoted with **capital letters**, while *small letters* denote the possible *values* or realisations of the Random Variable.

$$X := \{X \mid x_1, x_2, \ldots, x_n\}$$

Every Random Variable X is a mapping from the random test into the real numbers. If X is only expressed by whole numbers, it is called *discrete*, otherwise *continuous.*

A Random Variable is called *discrete* if it can take on at most a countable number of values x_i with single probabilities $Pr(X = x_i)$, whose sum is equal to one.

X is called Random Variable if for each real number x the probability $Pr(X \leq x_i)$, exists.

For a single roll of an *s*-sided dice, the probability of rolling each value is exactly 1/*s*. This is an example of a discrete uniform distribution. For s = 6:

$$P(X = x) = \begin{cases} 1/6 & (x = 1,2,\ldots 6) \\ 0 & otherwise \end{cases}$$

Suppose we repeat the dice throwing experiment asking what the probability that the dice will land on a number that is at most equal to 4 is.

Solution: There are 6 possible outcomes represented by S = { 1, 2, 3, 4, 5, 6 }. Each possible outcome is equally likely to occur (uniform distribution). This problem involves a cumulative probability. The probability that the dice will land on a number x ∈ { 1, 2, 3, 4} is equal to:

P(X ≤ 4) = P(X = 1) + P(X = 2) + P(X = 3) + P(X = 4) = 1/6 + 1/6 + 1/6 + 1/6 = 2/3

The so called distribution function is defined as

F(x) = P(X ≤ x)

the probability that the random variable X takes on a value which is less than or equal to x.

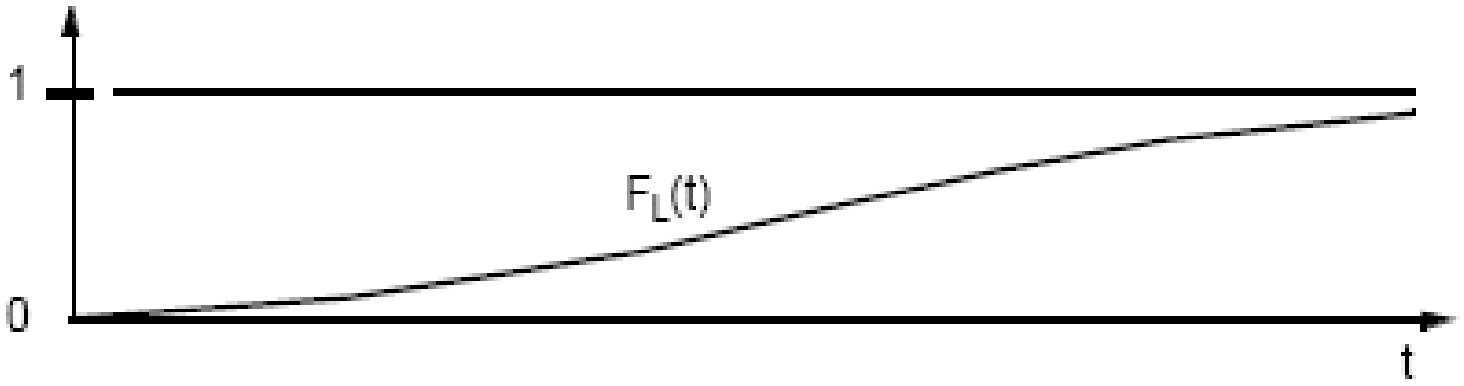
In order to transfer the just now explained terms into the scope of reliability, we just need to change the random variable X to the time T, which passes until components fail or get defect.

The function

$$\mathbf{F(t) = P(T \leq t)},$$

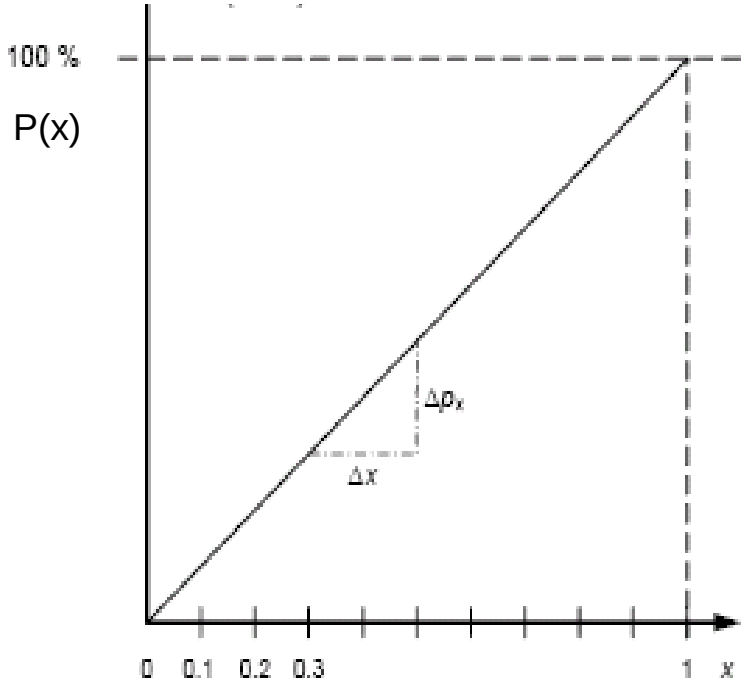
which gives the probability of operating time until failure, not longer than a given time period t, is therefore logically called failure distribution function.

The failure probability is 0 for $t \leq 0$, since a negative time to failure is impossible. For increasing times $t > 0$, the fault probability increases monotonically. It approaches 1 for $t \rightarrow \infty$.



Probability Density

How to estimate probability Pr($x \leq X \leq x+\Delta x$)?



New parameter: The gradient m of a straight (or function) is not equal to zero.

difference quotient: $m = \frac{\Delta p_x}{\Delta x}$ or as

differential quotient: $m = f(x) = \frac{dp_x}{dx}$

and therefore

- $dp_x = f(x) \cdot dx$
- $p_x = Pr(x_1 \leq X \leq x_2) = \int_{x_1}^{x_2} f(x) \cdot dx$

p_x is the probability that values in the interval $[x_1, x_2]$ are realised.
f(x) is the *Density Function*.

Probabilities in the Reliability Theory are often related to the operational time t.

Therefore $p_t = \Pr(t_1 \leq T \leq t_2) = \int_{t_1}^{t_2} f(t) \cdot dt$,

the density f(t) is the gradient of the distribution function F(t) at t (time).

Consequently:

$$f(t) = \frac{dF(t)}{dt} \qquad F(t) = \int_{-\infty}^{t} f(x)dx$$

F(t) can be defined in terms of the probability density function *f* as well.

The failure distribution function F(t) has the **complement**:

Reliability (in the sense: probability to survive)

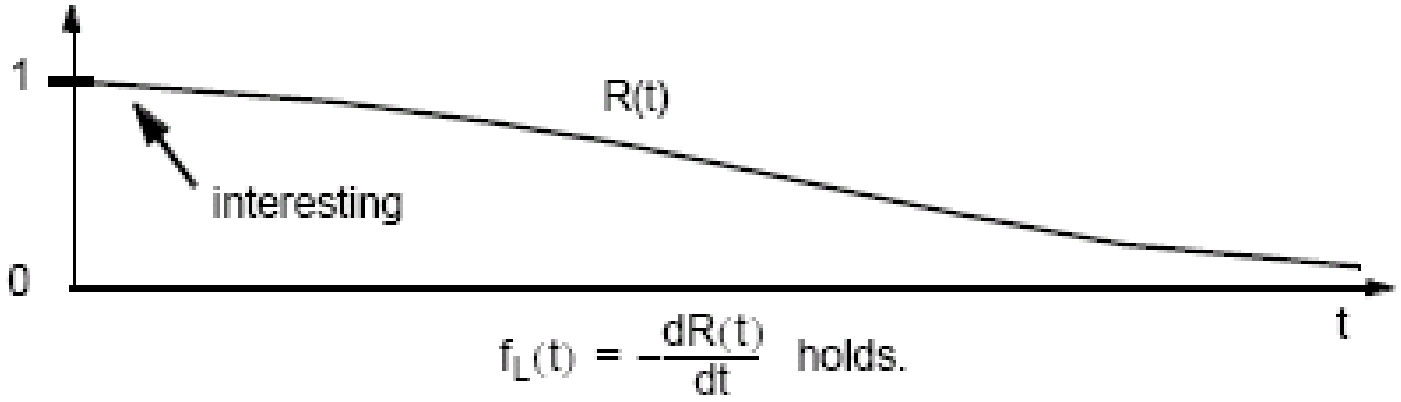
$R(t) = 1 - F(t)$

Quantitative:

The **reliability** R(t) expresses the probability of surviving the operation duration [0, t] without an interruption by failure occurrence.

Reliability

R(0) = 1. For an increasing time t > 0 the reliabilty decreases monotonically and approaches 0 for $t \to \infty$.



In practice, reliabilities close to 1 (and corresponding small times) are most relevant.

Reliability Parameters (I)

Referring to the distribution function:

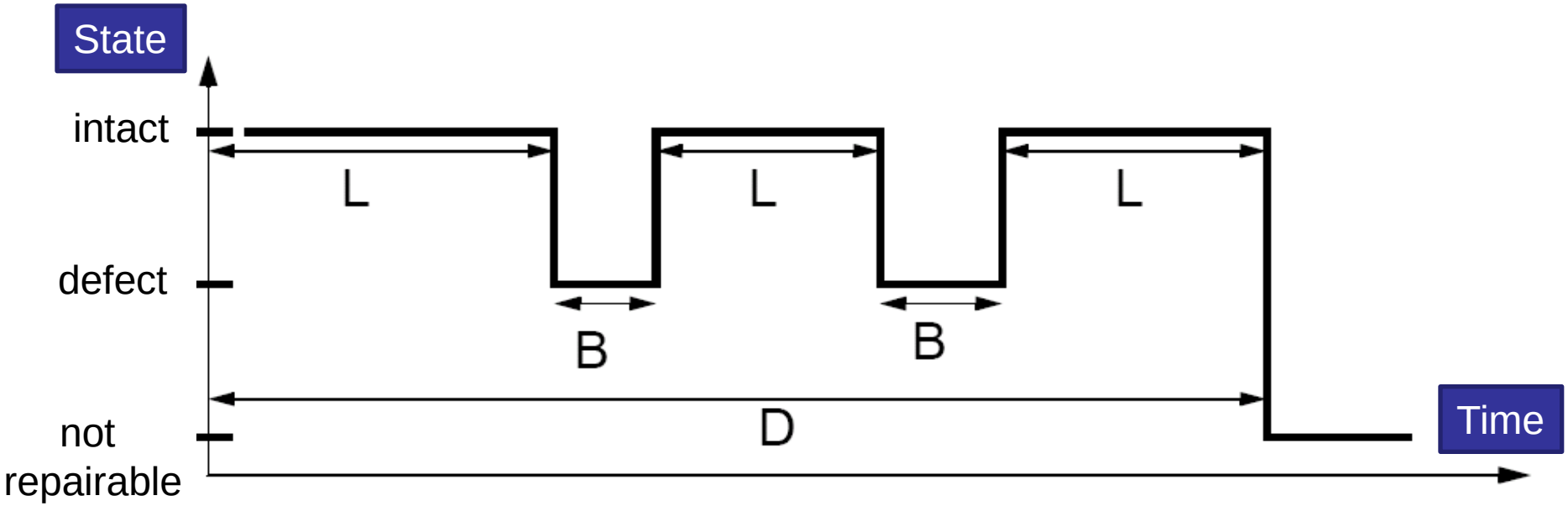
- (Total) failure probability $F_L(t)$ or $F(t)$ regarding L
- First failure probability $F_A(t)$ regarding A
- In-between failure probability $F_B(t)$ regarding B

Referring to the complement of the distribution function:

- (Total) survival probability $R_L(t)$ or $R(t)$ regarding L
- First survival probability $R_A(t)$ regarding A
- In-between survival probability $R_B(t)$ regarding B

The Random Variables

L (t) – time to failure B (t) – repair time D (t) – whole live time



"Time to fault" and "time to failure" have the same meaning. The difference only arise from the layer from which the system is considered.

The time to fault/failure L is the time difference between the begin of operation (assumed to be faultless) and fault/failure occurrence.

The time to repair B denotes the duration of a manually or automatically executed repair to reach a faultless state. Fault tolerance techniques can be considered as a means for automatic repair.

Reliability Parameters (II)

- Mean time to failure (MTTF) E_L or E (L)
- Mean time to the first failure (MTTFF) E_A
- Mean time to repair (MTTR) E_R or E (B)

$$E(L) = \int_0^\infty (t \cdot f_L(t))dt = \int_0^\infty R(t)dt$$

$$E(B) = \int_0^\infty (t \cdot f_B(t))dt$$

Only for repairable systems the stationary availability (steady-state availability) V is defined by

$$V = \frac{E_L}{E_L + E_R} = \frac{MTTF}{MTTF + MTTR}$$

The availability V denotes the probability that a system is properly functioning at any point in time. The general (time dependent) availability V(t) can only be calculated after the introduction of a state model.

Random Variables

The failure rate is a random variable.

the **failure rate** $z(t) = \frac{f_L(t)}{R(t)}$.

The failure rate is appropriate to express the reliability of **components** (and systems).

By analogy we define the **repair rate**: $r(t) = \frac{f_B(t)}{1 - F_B(t)}$

If the failure rate or the repair rate does not depend on the time, we write the constants λ instead of $z(t)$ or the constant μ instead of $r(t)$, respectively.

Reliability parameters (III)

Referring to the rate:

• (Total) failure rate	λ_L or λ	$z_L(t)$
• First failure rate	λ_A	$z_A(t)$
• In-between failure rate	λ_B	$z_B(t, \tau)$
• Repair rate	μ	$z_S(t, \tau)$

The signs in the left column are used when the rate is constant over time.

Reliability Formulary

$$\int_0^\infty f(\tau)d\tau = 1, \qquad F(\tau) = \int_0^\tau f(\tau)d\tau, \qquad E = \int_0^\infty \tau \cdot f(\tau)d\tau,$$

$$\frac{dF}{d\tau} = f(\tau), \qquad R(\tau) = \frac{1}{e^{\int_0^\tau z(x)dx}}, \qquad E = \int_0^\infty R(\tau)d\tau$$

- $f(\tau)$ density function
- $F(\tau)$ failure probability
- $R(\tau)$ survival probability
- E mean time to failure (mean lifetime)

The Conditional Probability of Survival $R(\tau | t_1)$ is the probability that a system which has survived a point of time t_1, will also survive time $t > t_1$.

Simple example:

Two engineers, Engelbert and Engeline forecast the MTTF for a new server. Engeline assumes 30 months, while Engelbert believes in 12 months. Since both engineers have the same experience (the probability for a correct assumption is 50% for each), an average value results:

$$\mathrm{MTTF} = \frac{30 + 12}{2} = 21$$

The installed server does not fail once during a test time of 6 months.

Due to this new experience

(a) how should one re-weight the experience of the two engineers?

(b) what should the new adjusted MTTF value look like?

Solution:

Let $\Pr(t_1) = \Pr(t_2) = 0.5$ be a priori probabilities for a correct assumption of the engineers.

If these are correct, then the probability of operating for six months without failure is:

$$R(\tau \mid t_i) = \exp\left[-\frac{t}{\mathrm{MTTF}_i}\right]$$

(assumed a failure rate is constant, exponential distribution).

Therefore the survival probability yields:

Engeline: $\Pr(\tau \mid t_1) = \exp\left[-\frac{6}{30}\right] = 0.819$

Engelbert: $\Pr(\tau \mid t_2) = \exp\left[-\frac{6}{12}\right] = 0.607$

New evaluation of the probability (a posteriori) that their forecast is correct:

$$\Pr(\tau_1) = \frac{0.819 \cdot 0.5}{0.819 \cdot 0.5 + 0.607 \cdot 0.5} = 0.574,$$

$$\Pr(\tau_2) = \frac{0.607 \cdot 0.5}{0.819 \cdot 0.5 + 0.607 \cdot 0.5} = 0.426.$$

MTTF = 0.574 * 30 months + 0.426 * 12 months = 22.3 months

Exercise example:

For a larger number of simultaneously implemented identical devises, it was discovered after one year that 5% of the devices failed, and were not repaired.

1. What is the mean lifetime E of the devices if an exponential distribution with parameter λ is assumed?

2. What is the mean lifetime E of the devices if an uniform distribution with the parameters a and b is assumed and a = 0?

Most Relevant Distributions in Reliability Theory

Continuous ones

1. **Exponetial**
2. **Weibull**
3. **Normal**
4. **Log Normal**
5. **Uniform (Rectangular)**

Discrete ones

6. **Poisson**
7. **Binomial (Bernoulli)**

To present (10-15 min):

- Description
- Reliability parameters
- Illustration (in function of time/event)
- Application in Reliability Theory

Deadline: October 5th, 14:00
Eusgeld@mavt.ethz.ch

Bibliography

Birolini, A. (2004) *Reliability Engineering: Theory and Practice*. 4th ed. Berlin, Heidelberg: Springer-Verlag.

P. Lee and T. Anderson (1990) *Fault tolerance – principles and practice; Dependable computing and fault-tolerant systems*. vol. 3. Springer-Verlag.

Boris Wl. Gnedenko, Igor V. Pavlov and Igor A. Ushakov (1999) *Statistical Reliability Engineering.* Wiley & Sons. ISBN-10: 0471123560.

Frank, M.V. *(2002) Probabilistic Risk Assessment in Aerospace: Evolution from the Nuclear Industry (Presentation)*. in *PSAM6 - Probabilistic Safety Assessment and Management (June 22-28, 2002)*. San Juan, Puerto Rico (USA).

DIN-40041 (1990) *Zuverlässigkeit: Begriffe*. Berlin: Beuth Verlag GmbH. p. 19.

Meyna, A. (1985) *Grundlagen von Sicherheitsanalyseverfahren*, in *Handbuch der Sicherheitstechnik*, Peters O. H. and Meyna A., Editors. München: Carl Hanser Verlag. p. 627f.

Pahl, G. (1985) *Sicherheit maschineller Einrichtungen*, in *Handbuch der Sicherheitstechnik*, Peters O. H. and Meyna A., Editors. München: Carl Hanser Verlag. p. 30f.

VDI-4002-Blatt1 (1986) *Erläuterungen zum Problem der Zuverlässigkeit technischer Erzeugnisse und/oder Systeme*. Düsseldorf: VDI-Verlag GmbH.

Number	Name	Distribution
1		Binomial
2		Exponential
3		Log Normal
4		Normal
5		Poisson
6		Uniform
7		Weibull

Example: Exponential Distribution

The exponential distribution is the only continuous memoryless random distribution.

The exponential distribution is the most common and simplest distribution function to model the reliability of components.

The failure rate and the time to failure are reciprocal.

Application: To estimate the reliability of componets or systems with constant failure rate.

Exponentially Distributed Time to Failure

If the time to failure is exponential distributed with parameter λ, we obtain:

Density: $f_L(t) = \lambda \cdot e^{-(\lambda \cdot t)}$

Failure prob.: $F(t) = \int_0^t (\lambda \cdot e^{-(\lambda \cdot x)})dx = -(e^{-(\lambda \cdot x)})\Big|_0^t = 1 - e^{-(\lambda \cdot t)}$

Reliability: $R(t) = e^{-(\lambda \cdot t)}$

Mean time to f.: $E(L) = \int_0^\infty (e^{-(\lambda \cdot t)})dx = -\left(\frac{1}{\lambda} \cdot e^{-(\lambda \cdot t)}\right)\Big|_0^\infty = \frac{1}{\lambda}$

Failure rate: $z(t) = \frac{f_L(t)}{R(t)} = \lambda$ **constant**

Illustration of the Exponentially Distributed Time to Failure