Reliability of Technical Systems

- **Goal:** To learn how the system reliability can be estimated and improved.
- **Learning:** Interactive
- **Tutorial:** CAB G 52, 12-13 h (Tuesday)
- **Exam:** Oral, 4 CP
- **Lecturer:** Prof. Dr. Wolfgang Kröger
  Laboratory for Safety Analysis
  Room ML J 13.1, +41 44 632 64 18,
  kroeger@mavt.ethz.ch
- **Assistant :** Cen Nan cnan@mavt.ethz.ch

Main Topics

1. Short Introduction, Reliability Parameters: Failure Rate, Failure Probability, etc.
2. Some Important Reliability Distributions
3. Component Reliability
4. Introduction, Key Terms, Framing the Problem
5. System Reability I: Reliability Block Diagram, Structure Analysis (Fault Trees)
6. System Reability II: State Analysis (Markovian chains)
7. System Reability III: Dependent Failure Analysis
8. Static and Dynamic Redundancy
9. Advanced Methods for Systems Modeling and Simulation (Petri Nets, network theory, object-oriented modeling)
10. Software Reliability, Fault Tolerance
11. Human Reliability Analysis
12. Case study: Building a Reliable System

Bibliography

Zio, Enrico. (2007) *An Introduction To the Basics of Reliability and Risk Analysis*. World scientific Publishing Co.

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

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).

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

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

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.

Main Topics

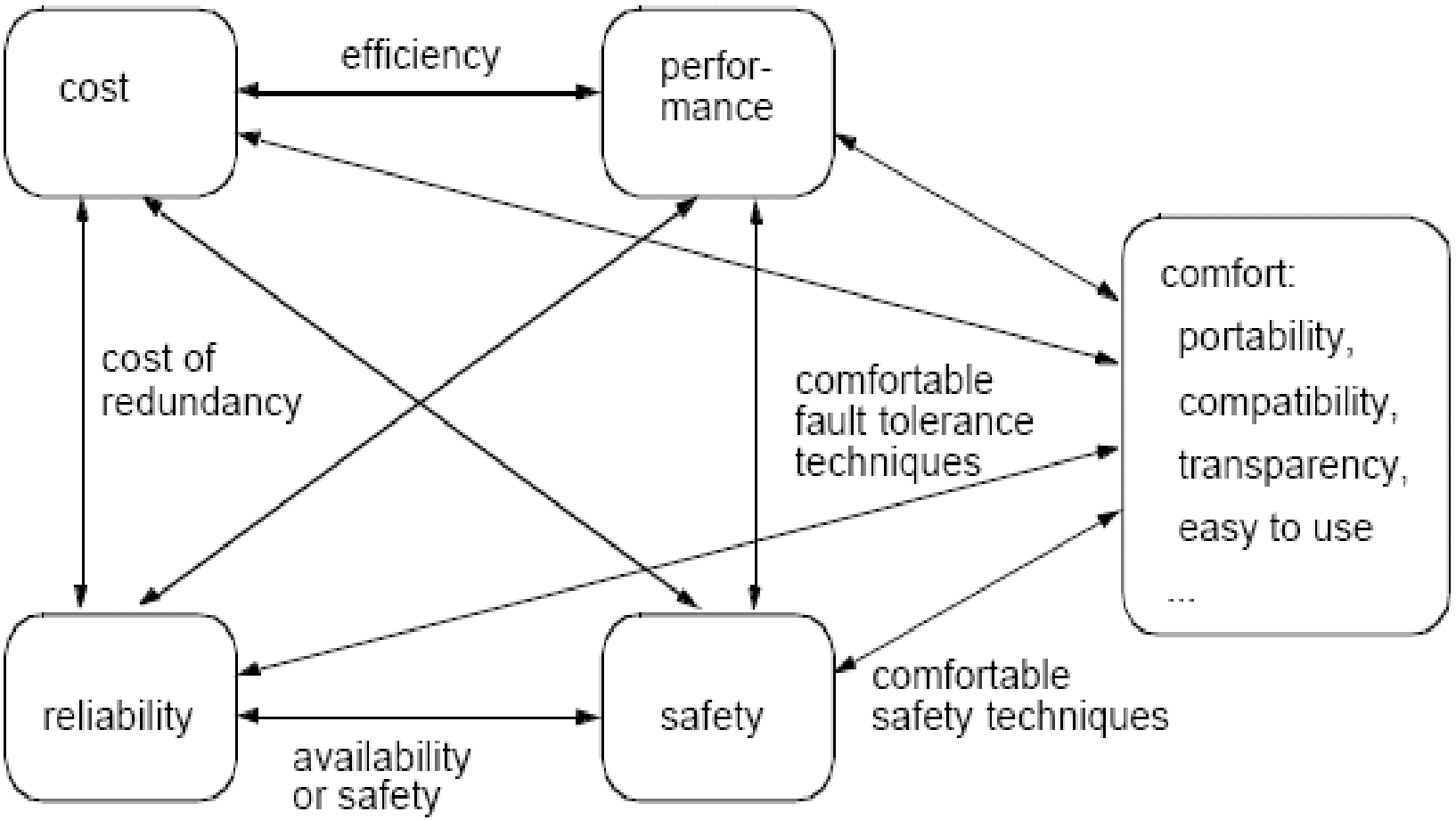
1. Short Introduction, Reliability Parameters: Failure Rate, Failure Probability, etc.
2. Some Important Reliability Distributions
3. Component Reliability
4. Introduction, Key Terms, Framing the Problem
5. System Reability I: Reliability Block Diagram, Structure Analysis (Fault Trees)
6. System Reability II: State Analysis (Markovian chains)
7. System Reability III: Dependent Failure Analysis
8. Static and Dynamic Redundancy
9. Advanced Methods for Systems Modeling and Simulation (Petri Nets, network theory, object-oriented modeling)
10. Software Reliability, Fault Tolerance
11. Human Reliability Analysis
12. Case study: Building a Reliable System

Motivation

Today (complex) devices and systems should:

- ✓ Be free of defects and systematic failures for a certain time after being implemented (i.e. from the time t = 0 onwards).
- ✓ Exhibit a fail-safe-behaviour in case of a critical or catastrophic breakdown.

General Objectives of System Design



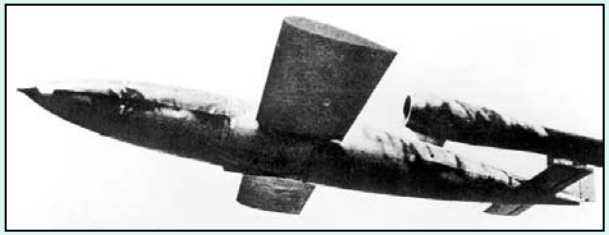
Quality: Property of an unit regarding its suitability to fulfil presumed or fixed standards.

Differences in quality emerge due to:

- Differences in materials
- Manufacturing techniques
- Carefulness during manufacture, etc.

Quality connotation is not sufficient for complex systems!

Historical Retrospective: Development of the Fi 103 („V1“) During WW2



Problem: rate of success ≤ 20%
- Despite quality control (QC) and
- after eliminating frequently occurring failures,

no pattern of weaknesses was observed (no systematic failure).

R. Lusser, project management, technical solutions:

- **More test flights for the survey and isolation of seldom events.**
- **But: Otherwise over-dimensioning of components not possible.**

Consequence: Solution unsuccessful!

E. Pieruschka, project mathematician:

- **Most of all organized structures tend to break down.**
- **Also a very small tendency occurs as soon as many elements operate for a long time.**
- **Measured variable: Failure rate λ.**
- **Survival probability of the system $R_s(t)$, if all components have to function, i.e.**

$$R_s = \prod_{i=1}^{N} R_i = \exp\left[-\sum_{i=1}^{N} \lambda_i t \right]$$

with $N \approx 10^5$, $\lambda \approx 10^{-5}$ [1/h], $t = 1.5$ [h] delivers $R_s \approx 22\%$.

- **Effect: From the model to sufficient $R_s(t)$.**

Supposing a system consists of components which will not fail with a probability of 99% (p=0,99) and which are connected in series. Then the probability that the entire system will not fail changes with the number of components as follows:

10 components lead to a survival probability of 90.40%,

20 components lead to a survival probability of 81,71 %,

30 components lead to a survival probability of 73,86 %,

40 components lead to a survival probability of 66,76 %,

50 components lead to a survival probability of 60,35 %,

100 components lead to a survival probability of 36,40 %.

What will happen if a system consists of **thousands** of components?

The difficulties depended to a lesser extent on the systematic failure (bad quality), but rather on the **multitude of failure possibilities** due to the **interaction** of the numerous units/components.

Quality: Property of a unit regarding its suitability to fulfil presumed or fixed standards.

Reliability: Property of a unit regarding its suitability to fulfil reliability standards during a given time period under presumed operational conditions.

Trust in Toyota Motor Company (1/2)

As recent as 2007, Toyota was seen as one of the most trusted and successful corporations. Toyota used “lean manufacturing”, defined as reliance on common parts across product lines and a smaller number of suppliers, thereby allowing greater economies of scale, quality control, and cost reduction. Toyota was also seen as a pioneer of green technologies. In 2009, Toyota became Japan’s largest company, with $230 billion in global sales.

In March 2007, Toyota began receiving reports that pedals in the Tundra pick-up truck were slow to return to idle after the driver removed pressure from the pedal. In late 2008, complaints about sticky gas pedals were received in Europe from owners of the small cars Aygo and Yaris (despite the fact that these models were equipped with a new friction lever that is supposed to address the problem experienced in the Tundra). In the fall of 2009, more complaints about Toyota vehicles were voiced in Canada and the US and, in model year 2008, Toyota vehicles accounted for 41% of the sudden acceleration complains in the entire US car industry [Greimel, 2010].

Trust in Toyota Motor Company (2/2)

Critics argue that Toyota did not communicate openly or honestly about the potential problems, even offering dubious explanations at various points in the time line (e.g., the suggestion that after-market carpets were causing the pedals to stick) rather than acknowledging that they did not know the causes of the reported problems.

After months of criticism in the US media, Toyota effectively capitulated. They recalled 9.5 million vehicles between late 2009 and February 1, 2010. They suspended sales of eight new models in the US, including their best sellers, until they could address the complaints about their products. In the midst of these actions, the CEO of Toyota Motors was effectively compelled testify at congressional hearings [Maynard, 2010].

The consequences of Toyota's communication failures have already been financially significant: billions of dollars in lawsuits against Toyota have been filed in US courts. Toyota's market share of new vehicle sales is rapidly falling in the US; and the resale value of used Toyota products in the US has fallen noticeably.

- **Reliability:** The ability of an item to perform a required function under stated conditions for a specified period of time

- **Safety:** Non existence of a danger (as possibility of a damage)

- **Fault Tolerance:** The capability of a system to satisfy its specification even in the presence of a limited number of faults.

Reliability, Fault Tolerance and Safety
can be influenced by failures.

Failure (Fault):

Wrong or "missing" function of a component.

Failure causes:

- Design failure
- Manufacture failure
- Operation failures
  - ✓ Failures due to disturbances
  - ✓ Wearing failures
  - ✓ Random physical failures
  - ✓ Handling failures
  - ✓ Maintenance failures

Further Key Terms

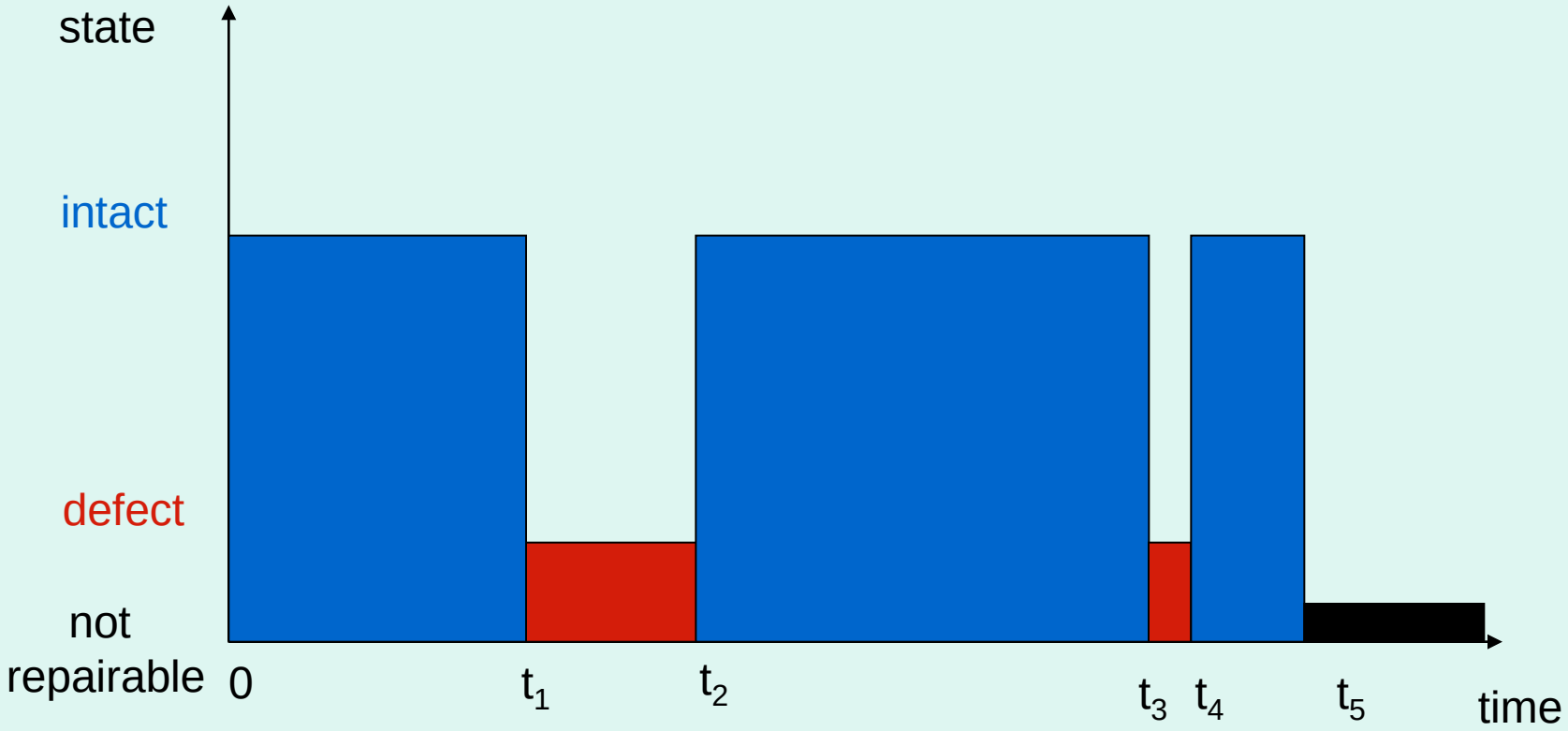
Availability is the probability that a system is intact at any point in time.

Redundancy: The presence of additional technical means.

MTTF: Mean Time To Failure

MTTR: Mean Time To Repair

System State as a Function of Time



Relation: Safety - Reliability

M: Set of all failure states of a system resp. the set of human errors with the subsets.

- M_g: Failure states / human errors with dangerous consequences.
- M_u: Failure states / human errors with no hazardous consequences.

For the safety only M_g is relevant. However, for the reliability $M = M_g + M_u$ has to be considered!

Conclusion:

- $M_g = 0$: System with absolute safety (without dangerous failure states).

But: Reliability R can still be very bad (usually for $M_g << M_u$).

- M = small: System with high reliability R.

But: In comparison with other systems with the same reliability, a lower safety is possible ($M_1 = M_2$ and $M_{g1} > M_{g2}$).

Relation: Reliability - Fault Tolerance (I)

Redundancy and Fault Tolerance Techniques

- in many physical systems, reliability improvement is solely based on an increased number of components (replicated components), e.g.
  - additional aircraft engines
  - additional wheels on a vehicle
  - spare wheels
  - etc.

- in computing systems, a fault tolerance technique is required in addition to guarantee that
  - a consistent state is preserved and
  - fault diagnosis and error processing is performed automatically.

Relation: Reliability - Fault Tolerance (II)

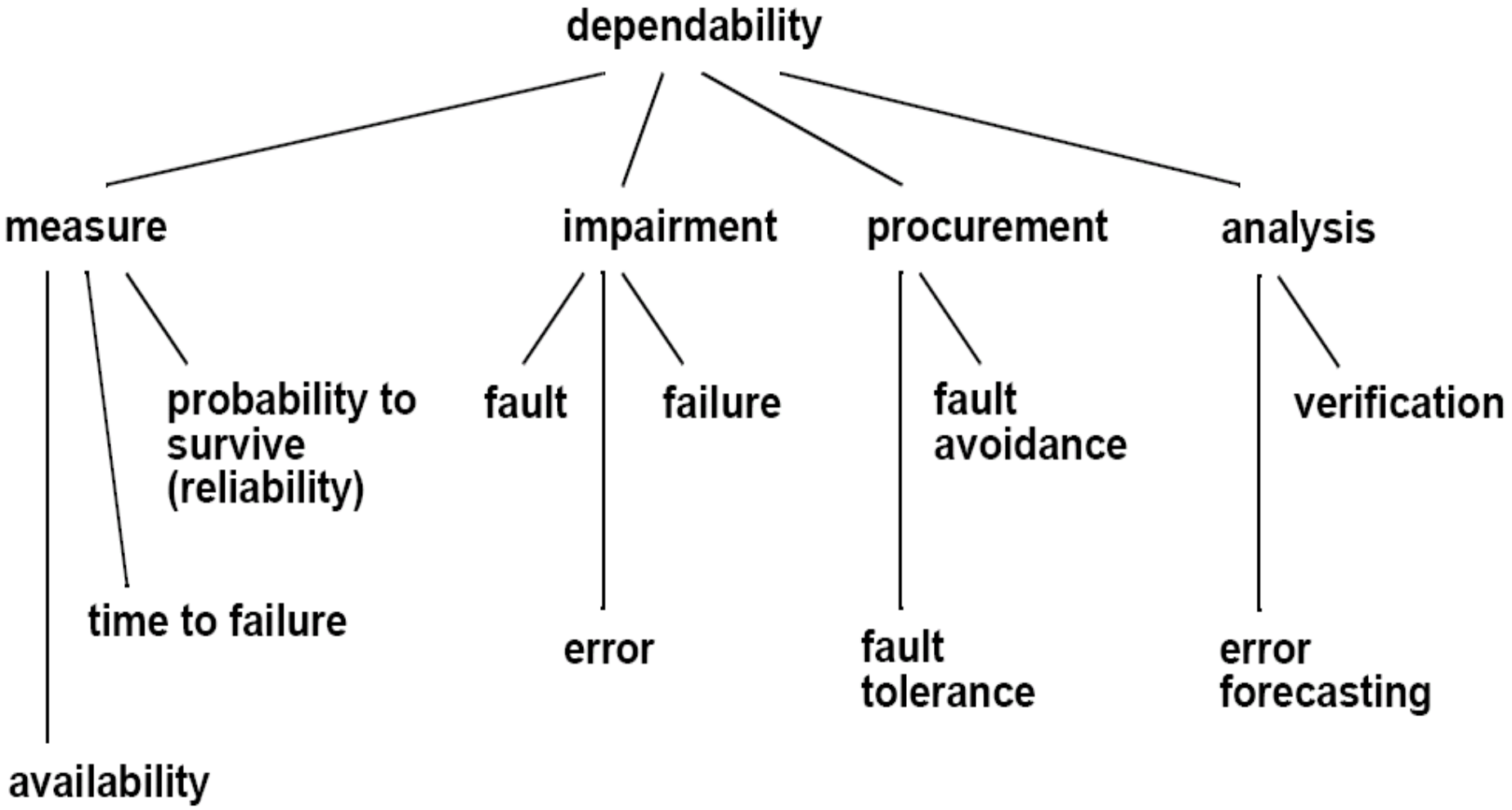
Reliability Metrics are widly used and well known, e.g.

- Failure rate
- MTTF, MTTR
- etc.

Quantitative measures of Fault Tolerance are not obvious, e.g.

- Number of tolerated faults
- Reconfiguration time
- etc.

Reliability Terminology

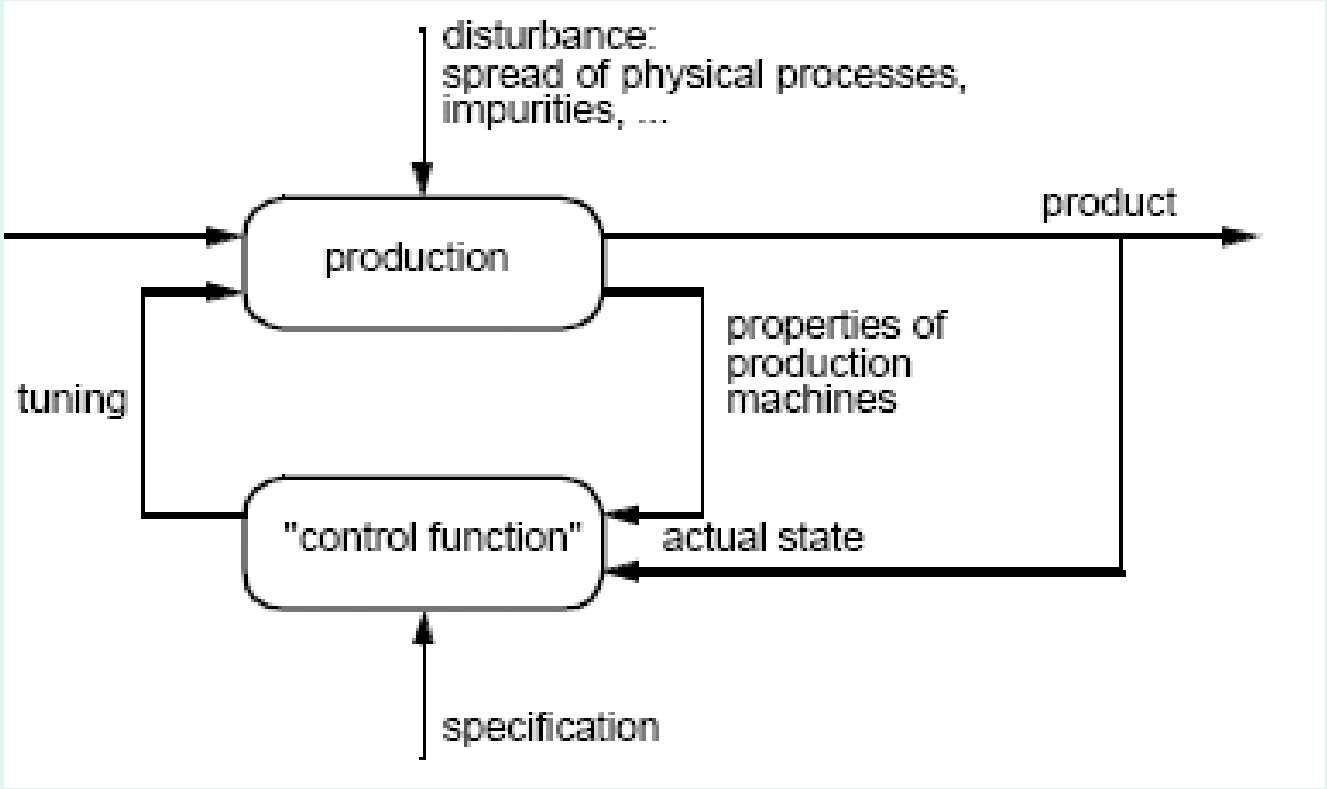


Assessment of the Obtained Reliability

Objectives:

- Proof of meeting the reliability requirements
- Forecasting reliability
- Comparison of different design alternatives
- Identification of weaknesses (“reliability bottlenecks”)
- Control of the production

Control of production / Fault Avoidance by Manufacturing

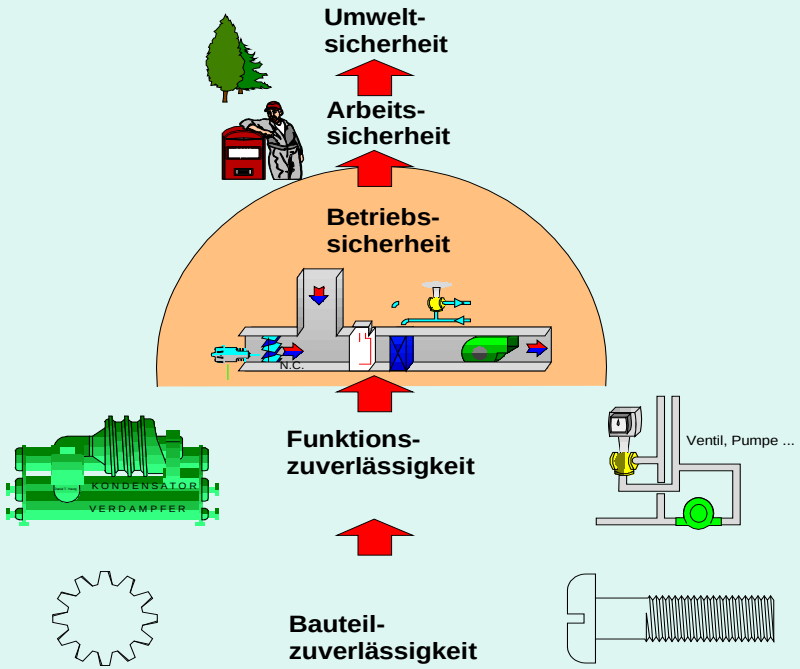


Reliability Evaluation

Procedure:

1. Analysis of occurring failure types
2. Analysis of the environment and operation stress
3. Analysis of failure effects and subsequent failure
4. Modelling the complete system
5. Deriving the system reliability from the components reliability
6. Validating the model based on failure statistics
7. Application of the reliability models for the mentioned above objectives

Component- and Function Reliability as Basis for Operation-, Working- and Environment Safety



Without the requirement of component and function reliability being fulfilled, operation-, working- and environment safety will not be achievable!