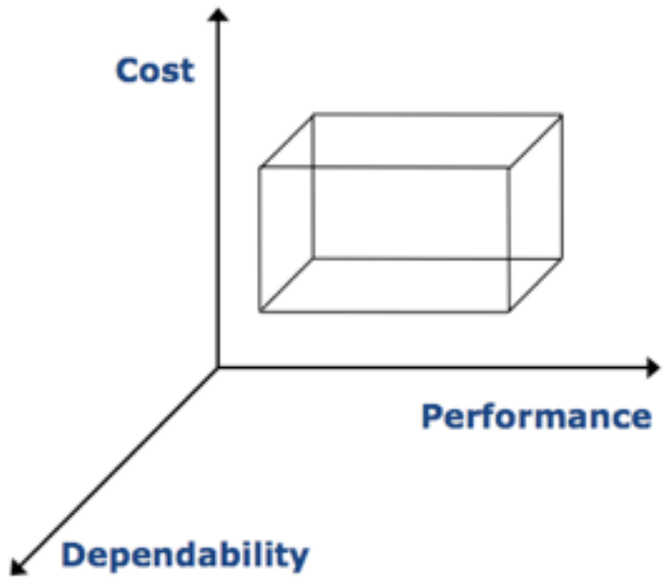
Dependable Systems

Definitions and Metrics (I)

Dr. Peter Tröger

Dependability

- **Umbrella term** for **operational** requirements on a system
  - IFIP WG 10.4: "*[..] the trustworthiness of a computing system which allows reliance to be justifiably placed on the service it delivers [..]*"
  - IEC IEV: "*dependability (is) the collective term used to describe the availability performance and its influencing factors : reliability performance, maintainability performance and maintenance support performance*"
  - Laprie: „ *Trustworthiness of a computer system such that reliance can be placed on the service it delivers to the user* “
- Adds a third dimension to system quality
- General question: How to deal with unexpected events ?
- In German: ‚Verlässlichkeit‘ vs. ‚Zuverlässigkeit‘



Dependability Examples

- A segmentation **fault** can lead to a system **failure.**
- A **faulty** controller in an RAID array lowers the **reliability** of the storage facility.
- The measurable **availability** of a web server depends on the **fault tolerance** capabilities in all its components.
- A database **fault** creates an **erroneous** state in the authentication component, which can lead to a system **failure** influencing the system **confidentiality.**
- The **integrity** of electronic voting systems depends on the complete absence of **failures** in the voting and the calculation procedures.
- **Fault forecasting** can support the **maintainability** of a system.
- Testing can only prove the presence of **faults**, not their absence.
- Our service level agreement guarantees an **availability** of 99.99%.

Observation: Dependable Systems Motivation

Money

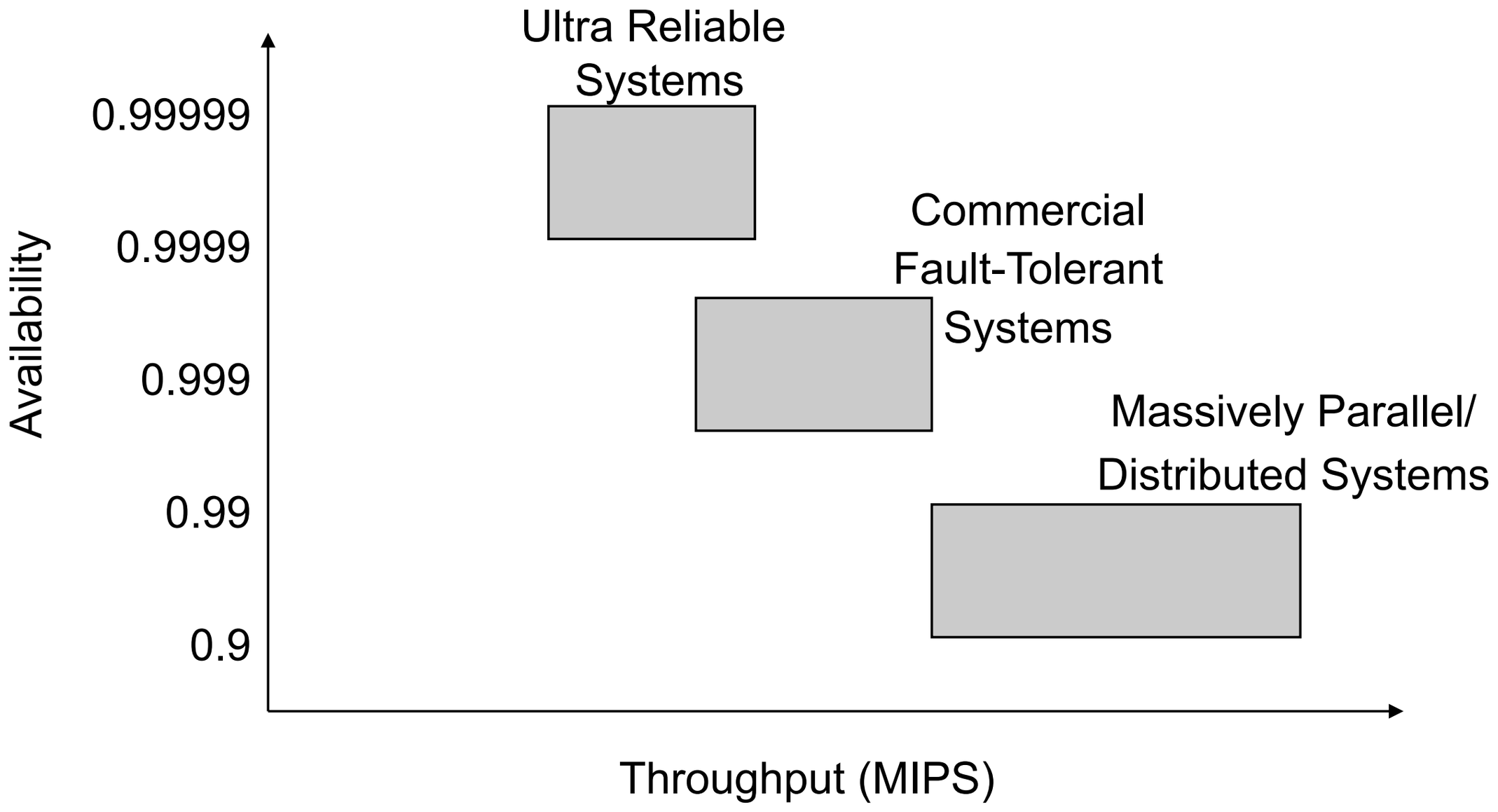
Life saving

Human users

Harsh environments

Complexity

Observation: Tradeoffs



Dependability Stakeholders

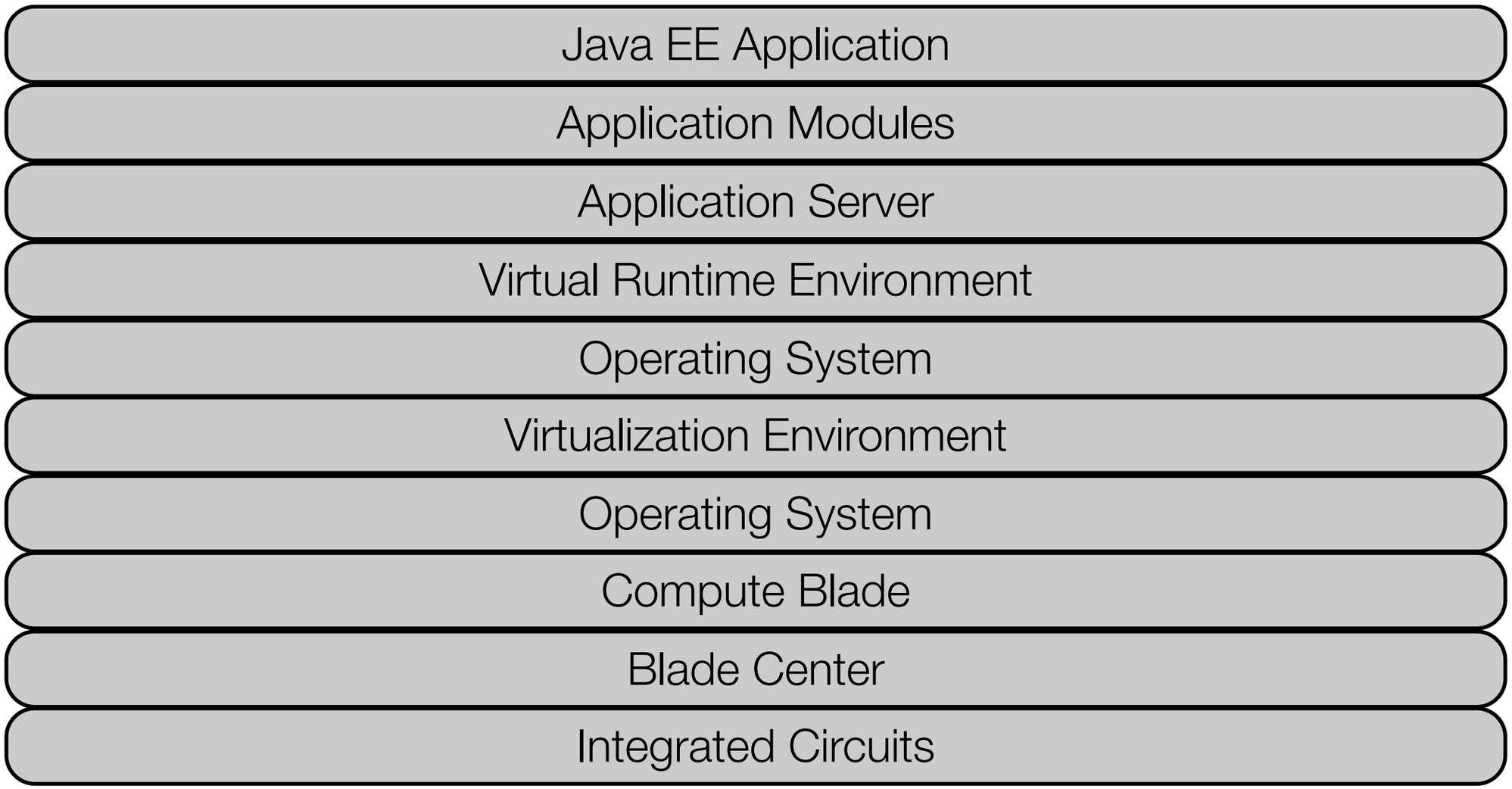
- **System** - Entity with function, behavior, and structure
  - A number of components or subsystems, which interact under the control of a design [Robinson]
- **Service** - System behavior abstraction, as perceived by the user
- **User** - Human or physical system that interacts with the systems service
- **Specification** - Definition of expected service and delivery conditions
  - On different levels, can lead to specification fault
- Reliance demands assessment of **non-functional dependability attributes**
- Provide ability for trustworthy service delivery by **dependability means**
- Undesired (maybe expected) circumstances form **dependability impairments / threats**

System Type Examples

- **Dependable (reliable) system**
  - Delivers a required service during its lifetime
- **Fault-tolerant computer system**
  - Continues correct service provisioning in the presence of faults
- **Real-time computer system**
  - Deliver a service within given time constraints (physical time, duration, ...)
- **Responsive computer system**
  - Fault-tolerant real-time system

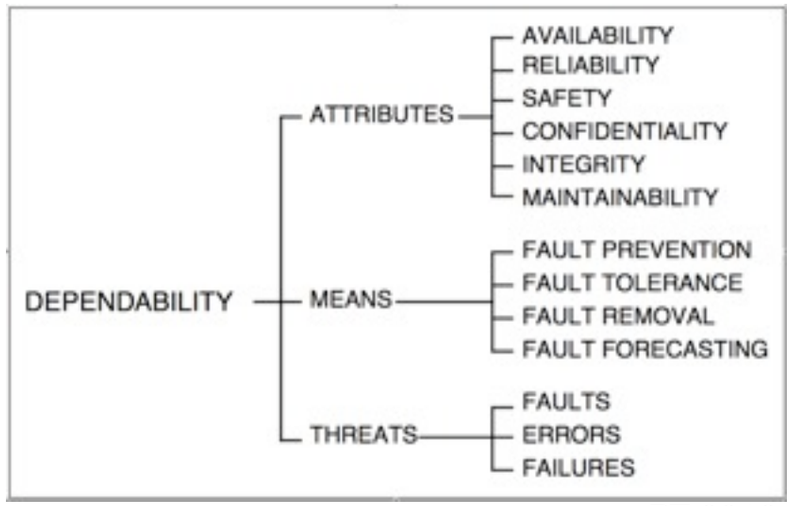
System Integration Levels

- Dependability has to be considered at every level
- Decomposition approach influences dependability success



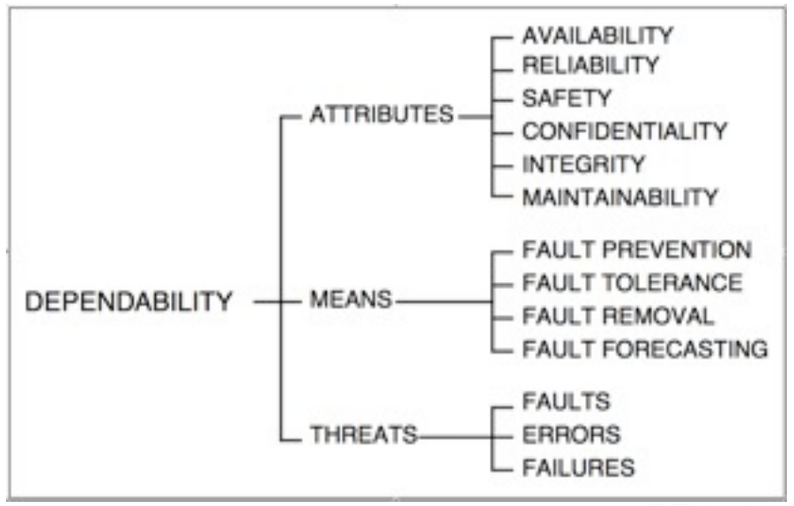
Attributes of Dependability

- Non-functional attributes such as reliability and maintainability
- Complementary dependability attributes resp. views
- In comparison to functional properties
  - ... hard to define
  - ... hard to abstract
  - ... ‚Divide and conquer‘ does not work as good
  - ... difficult interrelationships
  - ... often probabilistic dependencies



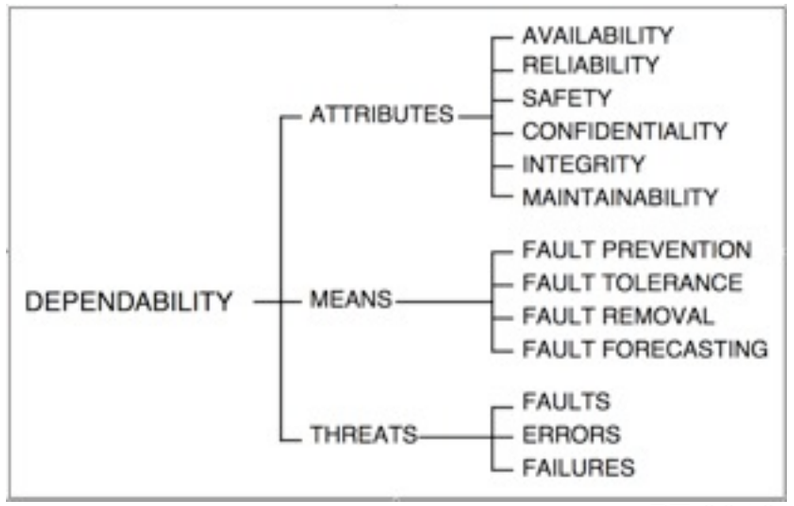
Attributes of Dependability

- **Reliability** - Continuity of service
  - Initial goal for computer system trustworthiness
  - *„Reliability is not doing the wrong thing.“* [Gray85]
  - Debated since the 60‘s, other disciplines have different understanding
    - IEEE: „*Reliability: Ability of a system or component to perform its required functions under stated conditions for a specified period of time*“
- **Availability** - Readiness for usage
  - Reliable computers are used and must be ready to serve
  - *„Availability is doing the right thing within the specified response time.“*



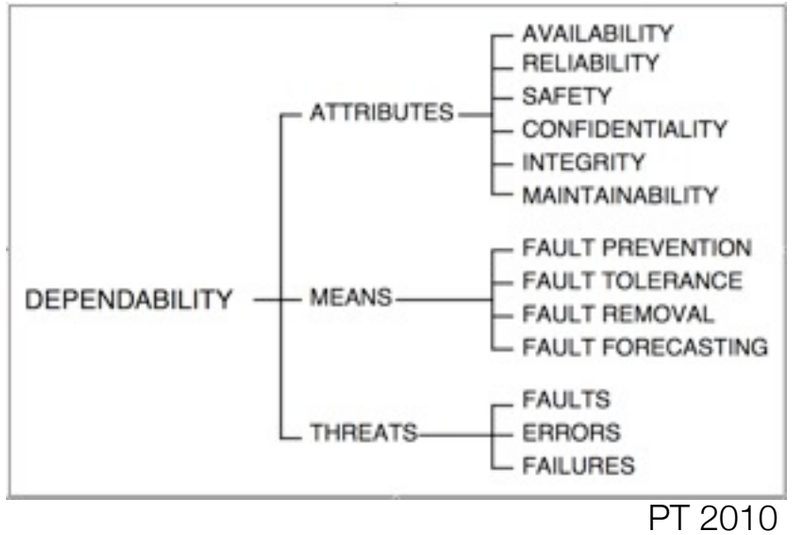
Attributes of Dependability

- **Safety** - Avoidance of catastrophic consequences on the environment
  - Critical applications
  - Specification needs to describe things that should not happen
- **Security** - Prevention of unauthorized access and / or information handling
  - Became relevant with distributed systems
- **Confidentiality** - Absence of unauthorized disclosure of information
- **Integrity** - Absence of improper system alteration
- **Maintainability** - Ability to undergo modifications and repairs



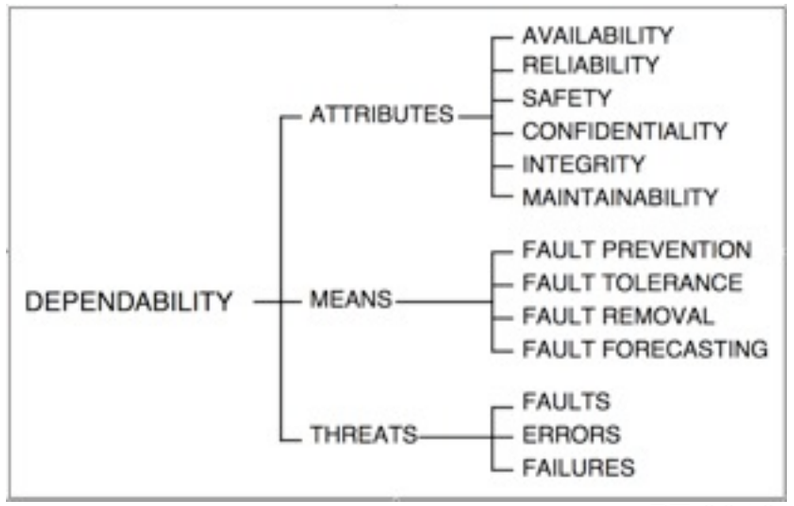
Impairments / Threats to Dependability

- System **failure - ‚Ausfall‘**
  - Event that occurs when the service no longer complies with the specification / deviates from the correct service.
- System **error - ‚Fehler(zustand)‘**
  - Part of system state that can lead to subsequent failure
- System **fault - ‚Fehler(ursache)‘**
  - Adjudged or hypothesized cause of an error
- Failure occurs when error state alters the service
- Systems are build from connected components, which are again systems
- Fault is the consequence of some other system failure

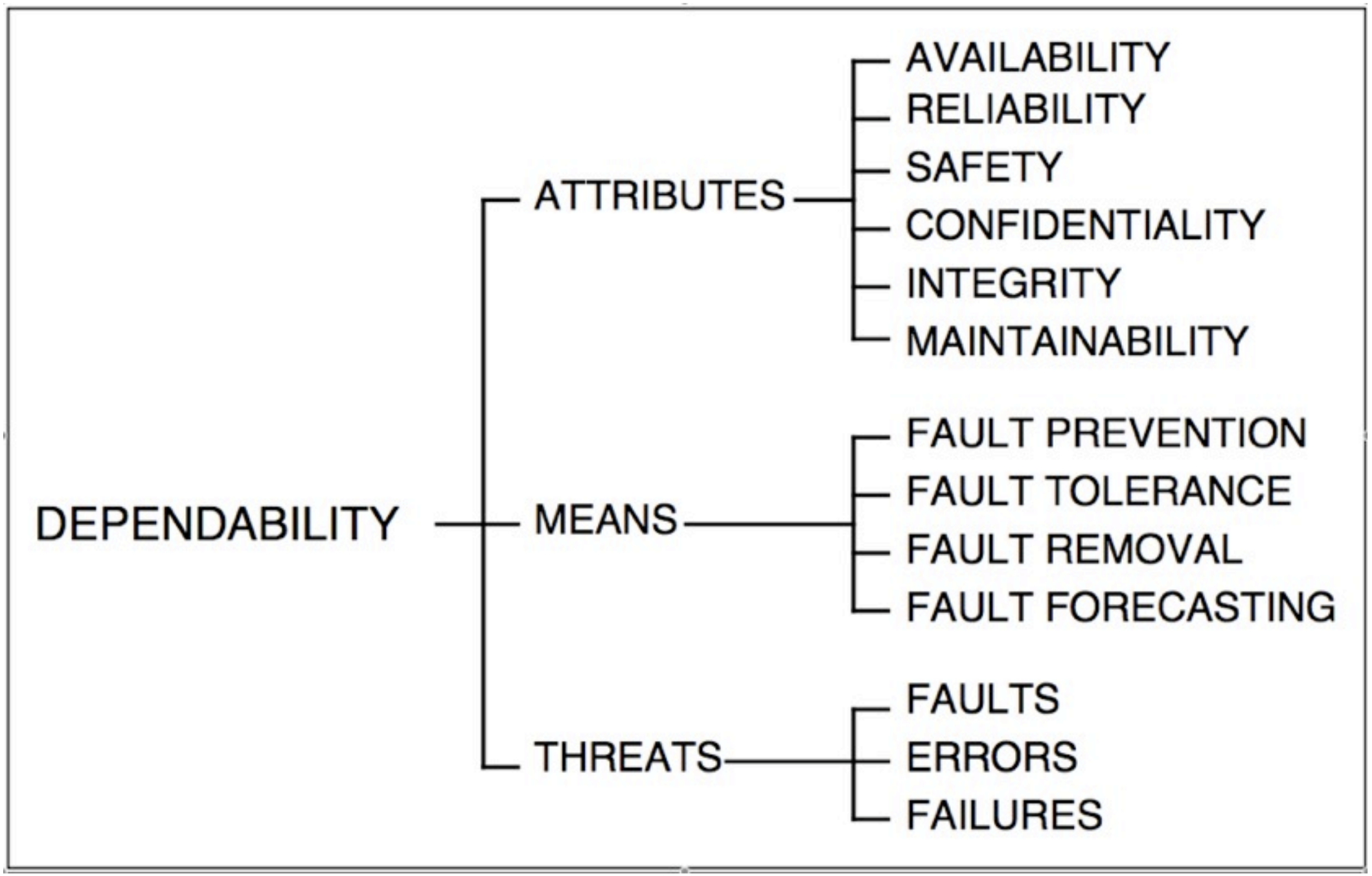


Means for Dependability

- Methods to achieve ability for dependable service delivery
  - **Fault prevention** - Prevent fault occurrence or introduction
  - **Fault tolerance** - Provide service complying with specification in spite of faults
- Methods to reach confidence in resp. validate dependability abilities
  - **Fault removal** - How to reduce the presence of faults
  - **Fault forecasting**- Estimate the present number, future incidence, and the consequences of faults
- Combined utilization



Dependability Tree (Laprie)



Dependability Tree (Laprie)