Dependability: basic concepts and terminology

Supporting reading

A. Avizienis, J.C. Laprie, B. Randell, C. Landwehr
Basic Concepts and Taxonomy of Dependable and Secure Computing
IEEE Transactions on Dependable and Secure Computing, Vol. 1, N. 1, 2004

Dependable Systems

System dependability is the ability of the system to deliver the expected functionality during its operational life.

Faults are unexpected events that may compromise the system functionality

Faults in computer systems:

- hardware faults
- software faults

General questions:
how to build dependable computer-based systems ?
can we justifiably trust the dependability of such systems?

What is a system?

System: entity that interacts with other entities (systems), including

- hardware,
- networks,
- operating systems software,
- application software,
- humans, and
- the physical world with its natural phenomena.

These other systems are the environment of the given system.

Hw and sw systems relaying on hidden components

a system is as strong as its weakest component

Computer failures differ from failures of other equipment

➡ small hidden faults may have large effects (digital machine)

Dependability: a definition

Dependability is "that property of a computer system such that reliance can justifiably be placed on the service it delivers"

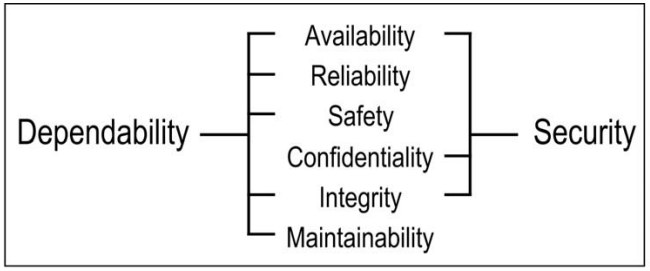
If the system stops delivering the intended service, we call this a failure.

Trust in a computer controlled system could be justified through numbers that show the quality level of the system. Such numbers are obtained using probabilities and statistical methods

In the field of safety critical systems, for example in the avionic field, a **rate of occurrence of failures** of 10^{-9} was set as a design target

Dependability attributes

Dependability is a concept that encompasses multiple properties



- **Availability**
  readiness for correct service
- **Reliability**
  continuity of correct service
- **Safety**
  absence of catastrophic consequences on the user(s) and the environment
- **Confidentiality**
  the absence of unauthorized disclosure of information
- **Integrity**
  absence of improper system alterations
- **Maintainability**
  ability to undergo modifications and repairs

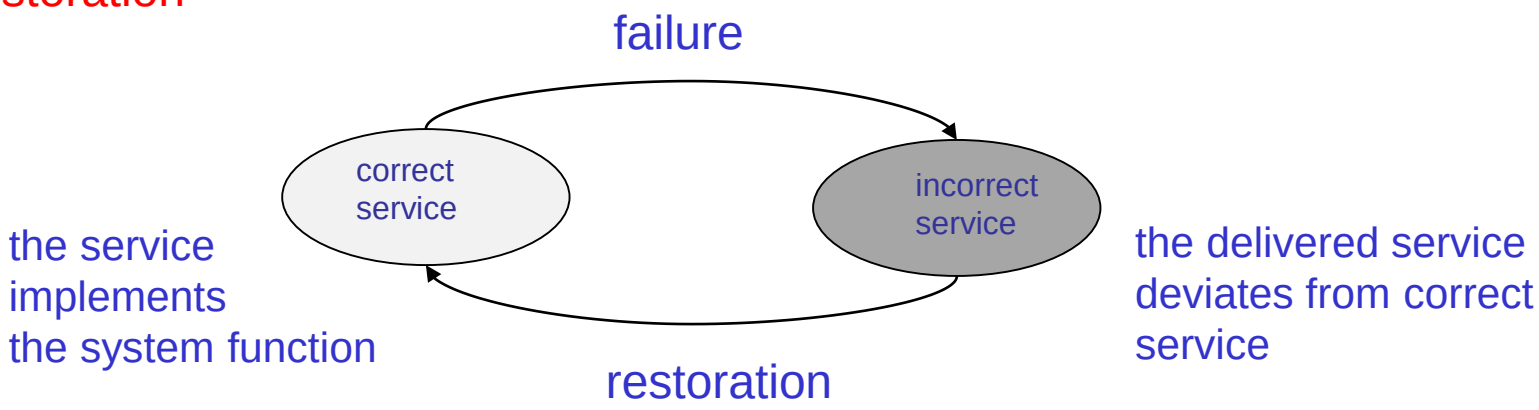
System

Function of a system:
what the system is intended to do and is described by the functional specification

Behavior of a system:
what the system does to implement its function and is described by a sequence of states.

Service delivered by a system (in its role as a provider):
its behavior as it is perceived by its user(s)

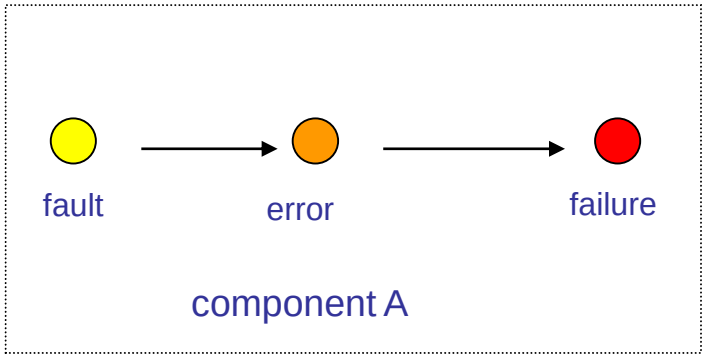
Failure
Restoration



the service implements the system function

the delivered service deviates from correct service

Threats to Dependability: Failures, Errors and Faults



A fault causes an error in the internal state of the system. The error causes the system to fail

Partial failure: Services implementing the functions may leave the system in a degraded mode that still offers a subset of needed services to the user. The specification may identify several such modes, e.g., slow service, limited service, emergency service, etc. Here, we say that the system has suffered a partial failure of its functionality or performance.

Means for achieving dependability

- A combined use of methods can be applied as means for achieving dependability. These means can be classified into:

1. **Fault Prevention techniques**

   to prevent the occurrence and introduction of faults

   – design review, component screening, testing, quality control methods, ...

   – formal methods

2. **Fault Tolerance techniques**

   to provide a service complying with the specification in spite of faults

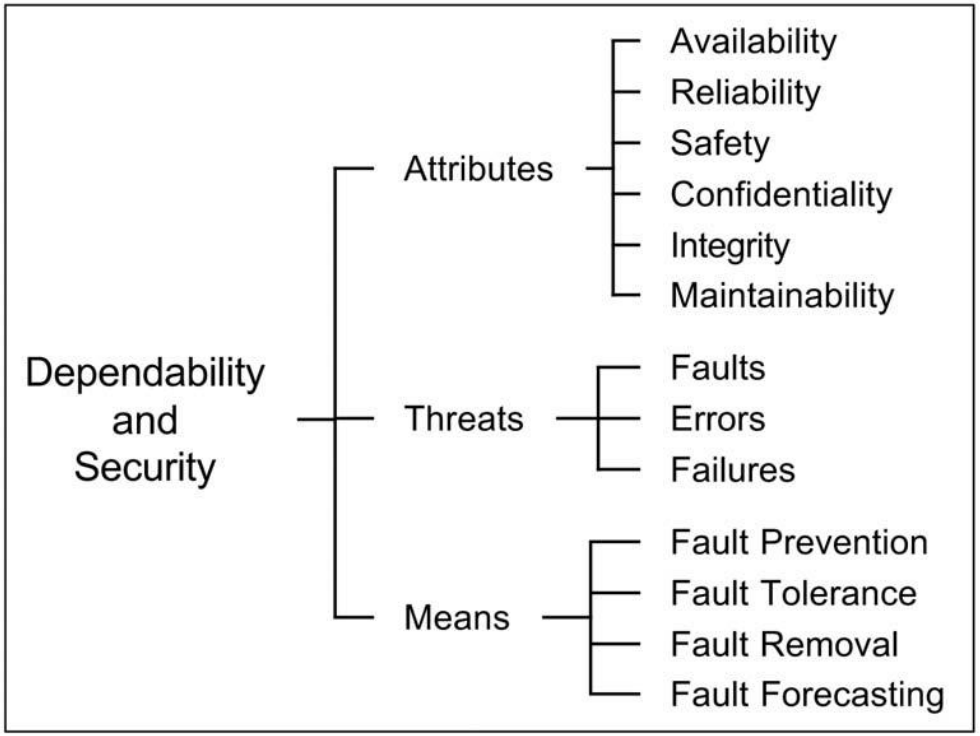
3. **Fault Removal techniques**

   to reduce the presence of faults (number,seriouness, ...)

4. **Fault Forecasting techniques**

   to estimate the present number, the future incidence, and the consequences of faults

Dependability tree



From A. Avizienis, J.C. Laprie, B. Randell, C. Landwehr. Basic Concepts and Taxonomy of Dependable and Secure Computing, IEEE Transactions on Dependable and Secure Computing, Vol. 1, N. 1, 2004

(*) Security: Availability, Confidentiality, Integrity