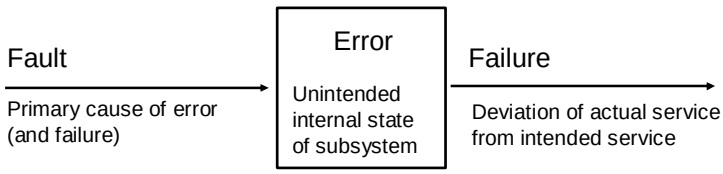
Embedded Systems

Bernd Finkbeiner
Calogero Zarba
Moritz Hahn

Sommersemester 2007

Fault Tolerance



Standardized terminology: J. C. Laprie (ed.) 1992,

„Dependability: Basic Concepts and Terminology“

Failures

- Nature
  - Value: incorrect value at system interface
  - Timing: value presented outside specified interval of real-time.
- Perception
  - Consistent: all users see the same (possibly wrong) result
  - Inconsistent (Byzantine): different users see different results
- Effect
  - Benign : failure costs in the same order of magnitude as utility
  - Malign: catastrophic costs
- Frequency
  - Permanent failure: remains until explicitly repaired
  - Transient : vanishes eventually

Errors

An error

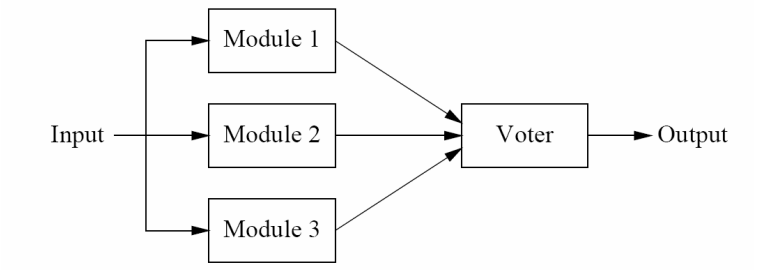
- is an *incorrect internal state* of a component
- may lead to a failure, but need not
  - design goal is to ensure the latter
- can be permanent or transient:
  - a faulty measurement entering a persistent database
  - a faulty measurement being overwritten by the next measurement

Faults

- Nature
  - Chance: random
  - Intentional: security break
- Perception
  - Physical: physical phenomenon
  - Design: error in design
- Boundaries
  - Internal: deficiency within the system
  - External: external disturbance
- Persistence
  - Transient
  - Permanent

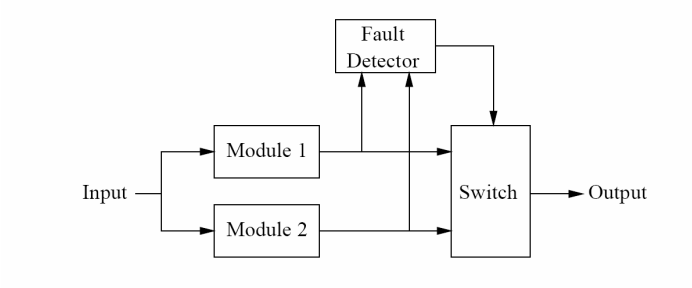
Hardware Fault Tolerance

- Static Redundancy
  E.g., Triple Modular Redundancy (TMR)



Hardware Fault Tolerance

- Dynamic Redundancy
  E.g., Standby-spare arrangement



Hybrid Redundancy