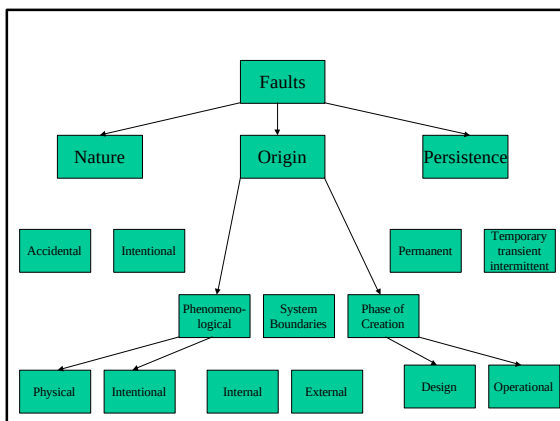


Dependability

Basic Concepts
From IFIP WG 10.4
Dependable Computing and Fault-Tolerant Systems, Vol. 5, Springer Verlag

Dependability

- Trustworthiness of a computer system such that reliance can justifiably be placed on the delivered service.
- Viewpoints
 - readiness for usage: available
 - continuity of service: reliable
 - secure, safe



Failures

- Failure domain
 - value failures
 - service does not comply with specification
 - timing failures
 - timing: too late (or too soon)

Fault pathology

- The result of a programmer's error is a dormant fault in the written software.
- When program runs, fault may become active.
- If the delivered service is affected (value and/or timing), a failure occurs.

The Means for Dependability

- Validation
 - Fault removal
 - Fault forecasting
- Building the system right (verification)
- Building the right system (validation)
- For how long will it be right (fault forecasting)

Signaling of component failures

- Error recovery
 - backward (go back to previous recovery point)
 - forward (go forward to a new state, frequently a degraded mode)
- Exception handling convenient for implementing error recovery, especially forward recovery.

Verification Techniques

- Static
 - compiler checks, proofs of correctness, inspections and walk-throughs
- Dynamic
 - run program

Criteria

- Purpose
 - conformance (satisfies specification)
 - fault-finding (revealing faults)
- System model
 - depending on whether the system model relates to the function or structure: functional testing (black box) and structural testing (white box, glass box)

Criteria

- Existence of fault model
 - aimed at finding specific classes of faults
 - stuck-at faults
 - design faults in software
