Dependability

AFFIDABILITÀ

- "The trustworthiness of a computing system which allows reliance to be justifiably placed on the service it delivers

  ATTENDIBILITÀ

  DIPENDENZA

Attributes

- Reliability: R(t) —> perform correctly in interval (t0, t)
- Availability: A(t), A —> prob is performing correctly at t Steady availability: A —> independent from t

  Costante
- Safety: S(t) —> prob perform correctly, or discontinue but safely; a measure of fail-safe cap of a sys (a sys have to be able to fail in a safe manner)
- Performability: P(L,t) —> prob performance at or above L at t (Fortes, 1984); measure of system ability to achieve a performance goal;
- Maintainability: M(t) —> prob that restoring require time <= t ; measure of speed of repair; correlated with availability —> if M(0) = 1.0, the system will be always available.
- Testability: how easy verify the attributes; related to maintainability —> the easiest the test, the fastest identify and repair
- Security: degree of protection; structures and processes must take into account the actions of hackers.

App with dependability reqs

- Long-life app: >= 10 yrs; >=0.95 prob of being operational at the end of 10 yrs.
- Critical-computational: can cause safety problem to people and business. (e.g.: aircraft, air traffic systems etc.) —> 0.99 prob of operational, no human maintenance during period.
- Hardly maintainable: maintainable costly or difficult (e.g.: remote systems)
- High availability: avail. Key parameter. high prob of operational (e.g. banking —> maint. Immed and easy.)

Impairments

- Failure: deviation from system function
- Error: part liable to lead to failure
- Fault: cause of error
- Photos from p.17
- Failure modes: taxonomy
- Fault classification
  - Phenomenological causes, nature, phase of reaction, system boundaries, temporal persistence
- Human-made faults
  - Non-malicious: design or interaction faults
  - Malicious: design faults, interaction faults (hacking)