Basic Concepts and Taxonomy of Dependable and Secure Computing

Algirdas Avizienis, Fellow, IEEE, Jean-Claude Laprie, Brian Randell, and Carl Landwehr, Senior Member, IEEE

Min Yang Jung
8/31/11
About the Paper

• This paper gives main definitions relating to **dependability**, a generic concept including such as reliability, availability, safety, integrity, maintainability, etc.

• Effort of this paper: 1980~ (book, workshop, conferences, TC on Fault-Tolerant Computing of IEEE CS, ...)

• Cited ~ 1590 times since 2004
Overview

1. System Function, Behavior, Structure, and Service
2. The Threats to Dependability and Security: Failures, Errors, Faults
3. Dependability, Security, and Their Attributes
4. The Means to Attain Dependability and Security
5. The Dependability and Security Tree
Overview

Dependability and Security

Attributes
- Availability
- Reliability
- Safety
- Confidentiality
- Integrity
- Maintainability

Threats
- Faults
- Errors
- Failures

Means
- Fault Prevention
- Fault Tolerance
- Fault Removal
- Fault Forecasting
Elementary Fault Classes

- Phase of creation or occurrence
  - Development faults
    - [occur during (a) system development, (b) maintenance during the use phase, and (c) generation of procedures to operate or to maintain the system]
  - Operational faults
    - [occur during service delivery of the use phase]
  - Internal faults
    - [originate inside the system boundary]
  - External faults
    - [originate outside the system boundary and propagate errors into the system by interaction or interference]
  - Natural faults
    - [caused by natural phenomena without human participation]

- System boundaries
  - Human-Made faults
    - [result from human actions]
  - Hardware faults
    - [originate in, or affect, hardware]
  - Software faults
    - [affect software, i.e., programs or data]
  - Malicious faults
    - [introduced by a human with the malicious objective of causing harm to the system]
  - Non-Malicious faults
    - [introduced without a malicious objective]
  - Deliberate faults
    - [result of a harmful decision]
  - Non-Deliberate faults
    - [introduced without awareness]
  - Accidental faults
    - [introduced inadvertently]

- Phenomenological cause
  - Incompetence faults
    - [result from lack of professional competence by the authorized human(s), or from inadequacy of the development organization]
  - Permanent faults
    - [presence is assumed to be continuous in time]
  - Transient faults
    - [presence is bounded in time]

- Dimension
  - Malicious faults
  - Non-Malicious faults
  - Deliberate faults
  - Non-Deliberate faults

- Objective
  - Development faults
  - Operational faults
  - Internal faults
  - External faults
  - Natural faults

- Intent
  - Development faults
  - Operational faults
  - Internal faults
  - External faults
  - Natural faults

- Capability
  - Development faults
  - Operational faults
  - Internal faults
  - External faults
  - Natural faults

- Persistence
  - Development faults
  - Operational faults
  - Internal faults
  - External faults
  - Natural faults
Error Propagation in System
Fault Tolerance Techniques

Fault Tolerance

Error Detection
[identifies the presence of an error]

Concurrent Detection
[takes place during normal service delivery]

Preemptive Detection
[takes place while normal service delivery is suspended; checks the system for latent errors and dormant faults]

Rollback
[brings the system back to a saved state that existed prior to error occurrence; saved state: checkpoint]

Rollforward
/state without detected errors is a new state]

Compensation
[the erroneous state contains enough redundancy to enable error to be masked]

Diagnosis
[identifies and records the cause(s) of error(s), in terms of both location and type]

Isolation
[performs physical or logical exclusion of the faulty components from further participation in service delivery, i.e., makes the fault dormant]

Reconfiguration
[either switches in spare components or reassigns tasks among non-failed components]

Reinitialization
[checks, updates and records the new configuration and updates system tables and records]
Means for Dependability and Security