Fault Tolerance

define error, fault and failure and types of faults and failure and recovery mechanisms

Tuesday, January 10, 2023 7:12 AM

- Reliability (Robust)
  - Define:
    - Fault: Causes a failure
      - Component
      - Design
    - Error: May lead to a failure
      - Recoverable or Not Recoverable
      - Severity
    - Failure: Deviation from specification
      - RTO → uptime / downtime — 9 9s
      - RPO — txns / ops — "lost data"

* Faults:
  - Transient
  - Intermittent
  - Persist

* Concerns
  - Availability
  - Reliability
  - Safety
  - Maintainability

* Caveats

Fault → Error → Failure does not always happen!

↳ Behavior outside of specification is not always a Failure!

- Failure Modes
  - Crash: Complete Failure / Inactive state
  - Omissions: I/O, Failure to send/receive comms
  - Timing: Response / Processing outside of time thresholds (timeout)
  - Response: Incorrect output / result
  - Arbitrary: Catch-All (inconsistent / unknown results or behavior)

- Recovery Mechanisms (Compensation) *SLA
  - Monitoring / Alerting: Manual Intervention
  - Redundant / Backup components: Degraded Functionality
  - Checkpoint / Logs: Recovering state / Restarting