L15: Reliability (4/5/06)

Plan:
- Reliability
- Approach
- Metrics
- Ex: disk

Threats:
- Software fault
- Hardware failure (including consideration of hardware faults)
- Design
- Operation
- Environment

Approach:
1. Identify possible failures
2. Protect against failure
3. Options

Metrics:
- MTTF, MTTR

Fail-safe:
- Redundant in space
- Time

Fail-safe margin:
- Number of Q's

---

Examples:
- DNS: escape NS
- BGP: reason delete
- TCP: read pkt

---

Plan:
- Reliability
- Approach
- Metrics
- Ex: disk

Threats:
- Software fault
- Hardware failure

Design:
- Failure: protected code
- Operation:
  - fail-safe
  - fail-safe margin

Environment:
- fail-safe margin

(made connection to client/server interoperation hints)

Trust-Aware systems:
- Reliable systems from unreliable modules

Module doesn't meet spec.

MTTF:
- TTR + TTR
- MTTR + MTTF

MTTF:
- Number of Q's

---

(Show chart) Chart:
- Increased rate of failure
- MTTF: 1,000 disks
- 1,000 hours
- 500,000 hours
- 3,000 hours
- Redundant system

- Critical path
- Detal
- Cyclic path

202