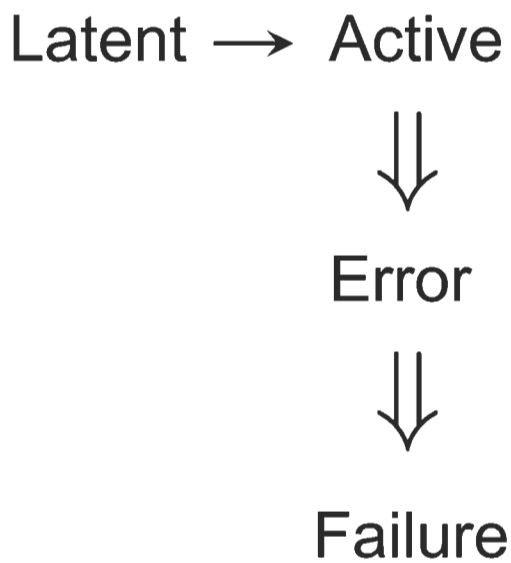
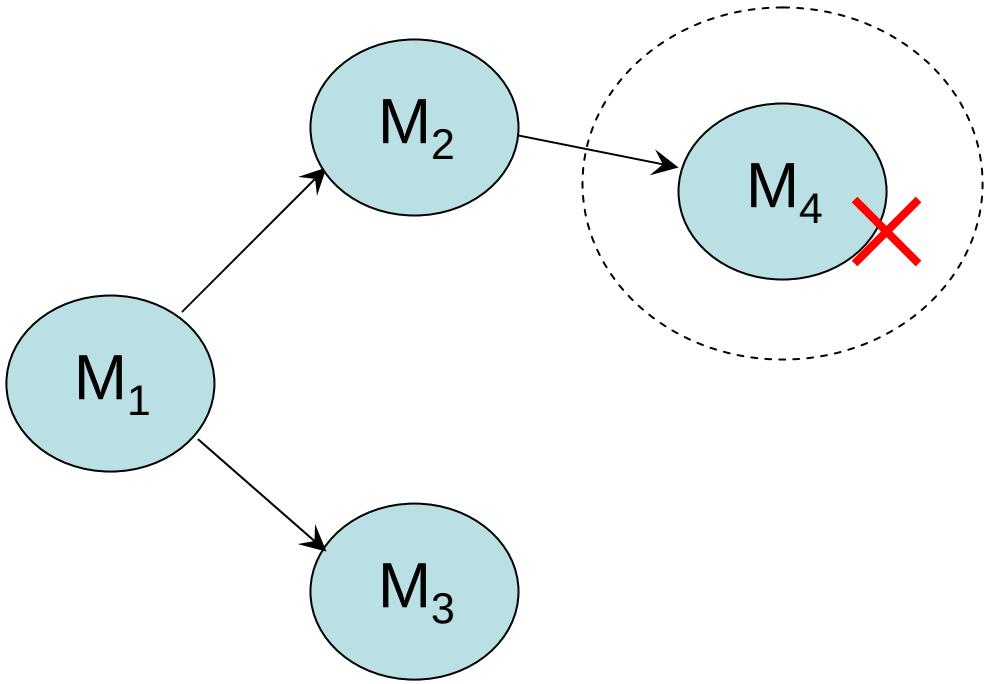
Fault-tolerance

Faults:

- Software
- Hardware
- Design
- Operational



- Unreliable components (modules).



Examples

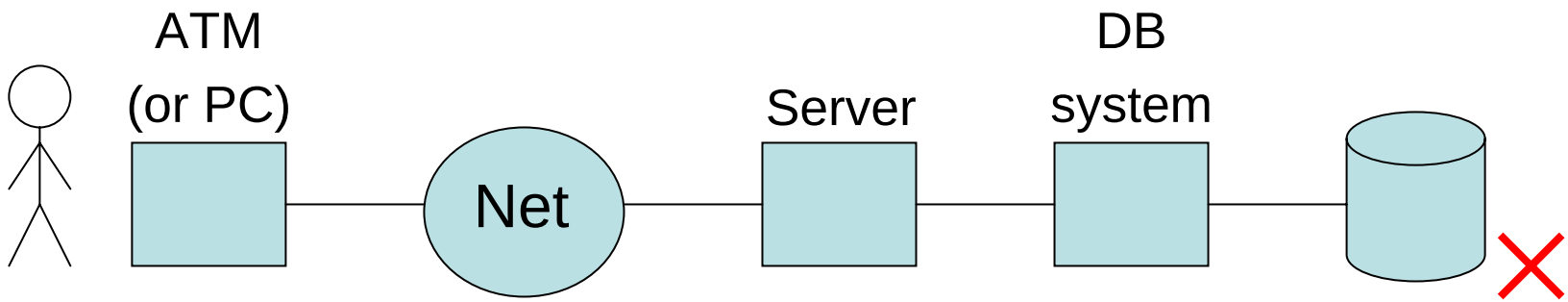
- Bad locking
- Routing
- Packet loss
- Congestion collapse
- DNS

Systematic Approach

1) Modularize
2) Detect errors
3) Mask errors

→ Conform to spec

Redundancy



XFER (from, to, $)

- Fail-stop
- Fail-fast
- Fail-soft
- Fail-safe

Models

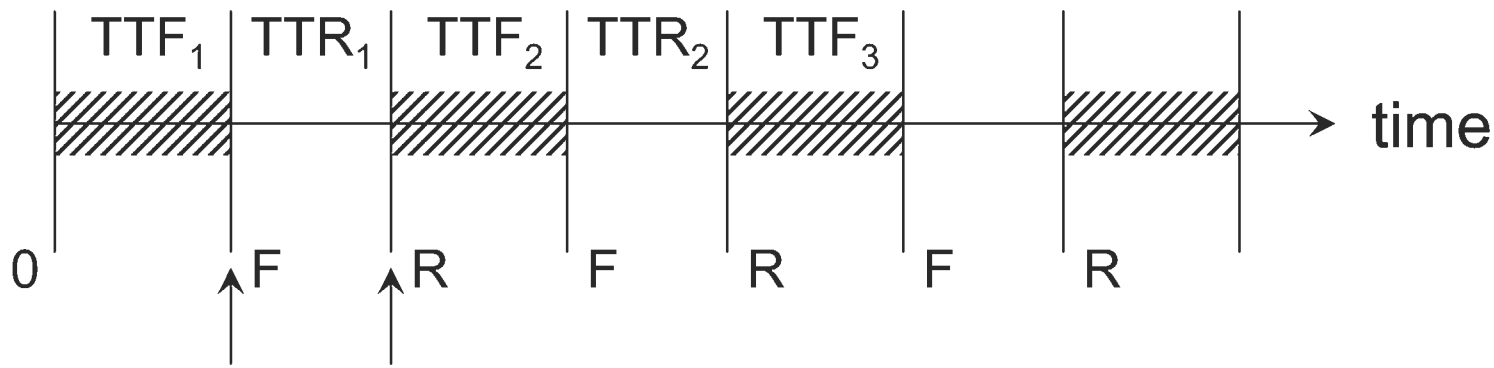
1) # tolerated failures

2) Mean Time To Failure (MTTF)

Availability

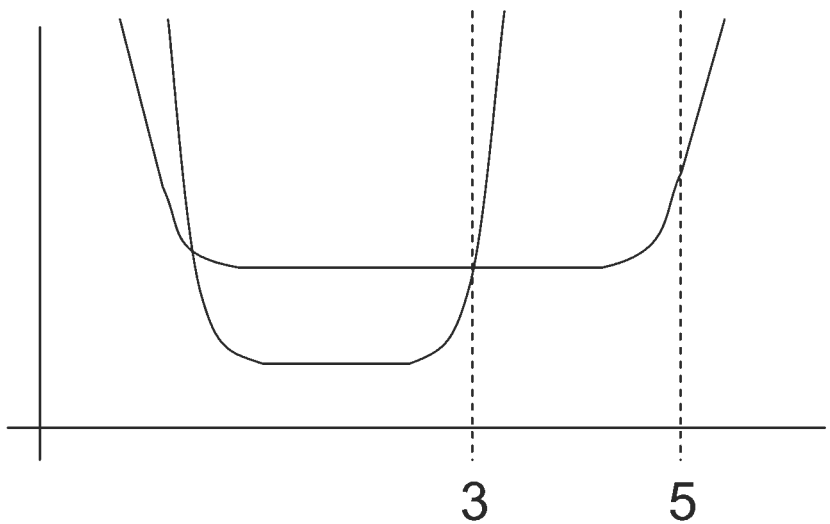
$$= \frac{\sum TTF_i}{\sum TTF_i + \sum TTR_i}$$

$$= \frac{MTTF}{MTTF + MTTR}$$



Failure Rate:

$$h(t) = P(\text{failure in } t, t + dt \mid \text{OK @ } t)$$



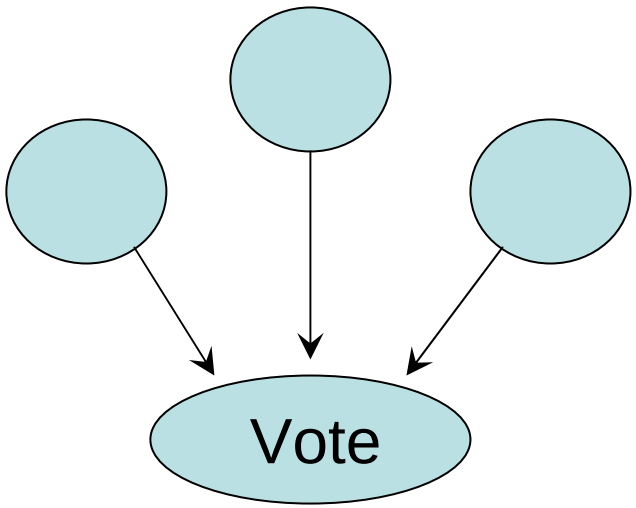
Reliability: $R(t) = P(\text{OK @ time } t)$

$$e^{-(t/MTTF)}$$

Example:

1) Spatial: coding, logs, copy + voting
2) Temporal: retry / undo

Voting



$$R_{3V} = R^3 + 3R^2(1- R) > R$$

when R in (½, 1)