

## Reliability of Multi-component Systems

- Software system: number of modules.
- Individual modules developed and tested differently: different defect densities and failure rates.
  - **Sequential execution**
  - **Concurrent execution**
  - **N-version systems**

## Sequential execution

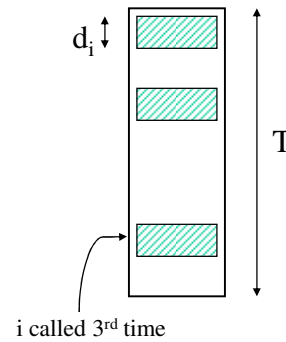
- Assume one module executed at a time.
- $f_i$ : fraction of time module  $i$  under execution;  $\lambda_i$  its failure rate
- Mean system failure rate:

$$\lambda_{sys} = \sum_{i=1}^n f_i \lambda_i$$

## Sequential Execution (cont.)

- $T$ : mean duration of a single transaction
- module  $i$  is called  $e_i$  times during  $T$ , each time executed for duration  $d_i$

$$f_i = \frac{e_i d_i}{T}$$



## Sequential Execution (cont.)

- System reliability  $R_{sys} = \exp(-\lambda_{sys} T)$

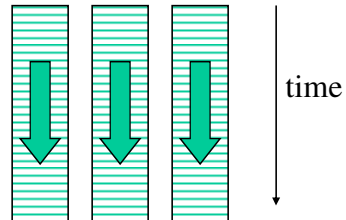
$$R_{sys} = \exp\left(-\sum_{i=1}^n e_i d_i \lambda_i\right)$$

- Since  $\exp(-d_i \lambda_i)$  is  $R_i$ ,

$$R_{sys} = \prod_{i=1}^n (R_i)^{e_i}$$

## Concurrent execution

- Concurrently executing modules: all run without failures for system to run
- $j$  concurrently executing modules

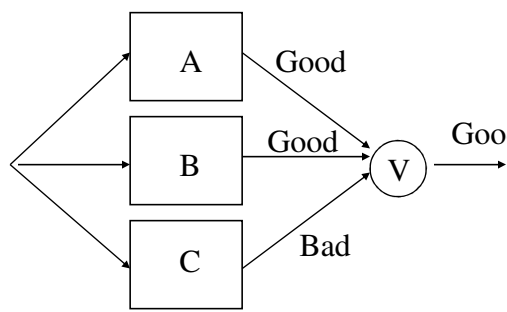


$$\lambda_{sys} = \sum_{j=1}^m \lambda_j$$

## N-version systems

- Critical applications, like defense or avionics
- Each version is implemented and tested independently
- Common implementation uses triplication and voting on the result

## N-version Systems (Cont.)



$$R_{\text{sys}} = 1 - (1-R)^3 - 3R(1-R)^2$$

$$R=0.9 \Rightarrow R_{\text{sys}}=.972$$

$$\bar{R}=0.1 \Rightarrow \bar{R}_{\text{sys}}=.028$$

## N-version systems: Correlation

- Correlation significantly degrades fault tolerance
- Significant correlation common in N-version (Knight-Leveson)
- Is it cost effective?

## N-version systems: Correlation

- 3-version system
- $q_3$ : probability of all three versions failing for the same input.
- $q_2$ : probability that any two versions will fail together.
- Probability  $P_{sys}$  of the system failing

$$P_{sys} = q_3 + 3q_2$$

## N-version systems: Correlation

- Example: *data collected by Knight-Leveson; computations by Hatton*
- *3-version system, probability of a version failing for a transaction 0.0004*
- *in the absence of any correlated failures*

$$\begin{aligned} P_{sys} &= (0.0004)^3 + 3(1 - 0.0004)(0.0004)^2 \\ &= 4.8 \times 10^{-7} \end{aligned}$$

## N-version systems: Correlation

- Uncorrelated improvement factor of  $0.0004/4.8 \times 10^{-7} = 833.3$
- Correlated:  $q_3 = 2.5 \times 10^{-7}$  and  $q_2 = 2.5 \times 10^{-6}$
- $P_{\text{sys}} = 2.5 \times 10^{-7} + 3.25 \times 10^{-6} = 7.75 \times 10^{-6}$
- improvement factor:  $0.0004/7.75 \times 10^{-6} =$   
**51.6**
- state-of-the-art techniques can reduce defect density only by a factor of **10!**