FAULT TOLERANT SYSTEMS

http://www.ecs.umass.edu/ece/koren/FaultTolerantSystems

Part 3 - Resilient Structures
Chapter 2 – HW Fault Tolerance

M-of-N Systems

- An M-of-N system consists of N identical modules
- Fails when fewer than M modules are functional
- Best-known example - The Triplex (TMR)
  - Three identical modules whose outputs are voted on
- This is a 2-of-3 system: as long as a majority of the processors produce correct results, the system will be functional

Reliability of M-of-N Systems

- **N** identical modules
- **R(t)** - reliability of an individual module
- The reliability of the system is the probability that **N-M** or fewer modules have failed by time **t** (or – at least **M** are functional)

$$R_{m-of-n}(t) = \sum_{i=0}^{N-M} \binom{N}{i} (1-R(t))^i R(t)^{N-i}$$
$$= \sum_{i=M}^{N} \binom{N}{i} R(t)^i (1-R(t))^{N-i}$$

where $$\binom{N}{i} = \frac{N!}{i!(N-i)!}$$

Correlated Failures in M-of-N Systems

- Key to the high reliability - statistical independence of failures in modules
- Correlated failure can greatly diminish reliability
- **Example**: q_{cor} - probability that the entire system suffers a global failure

$$R_{m-of-n-cor}(t) = (1-q_{cor}) \sum_{i=M}^{N} \binom{N}{i} R(t)^i (1-R(t))^{N-i}$$

M-of-N Systems - Modes of Correlation

- If system is not designed carefully, the correlated failure factor can dominate the overall failure probability
- Different modes of correlation among modules exist - not necessarily a global failure
- Correlated failure rates are extremely difficult to estimate
- From now on we will assume statistically independent failures in modules

Reliability of TMR - Triple Modular Redundant Cluster

- M-of-N system with M=2, N=3 - system good if at least two modules are operational
- A voter picks the majority output
- Voter can fail - reliability of voter $R_{vot}(t)$

$$R_{tmr}(t) = R_{vot}(t) \sum_{i=0}^{1} \binom{3}{i} (1 - R(t))^{i} R(t)^{3-i}$$

$$= R_{vot}(t) \sum_{i=2}^{3} \binom{3}{i} R(t)^{i} (1 - R(t))^{3-i}$$

$$= R_{vot}(t) \left(3R^2(t) - 2R^3(t) \right)$$

Reliability of TMR - Constant Failure Rates

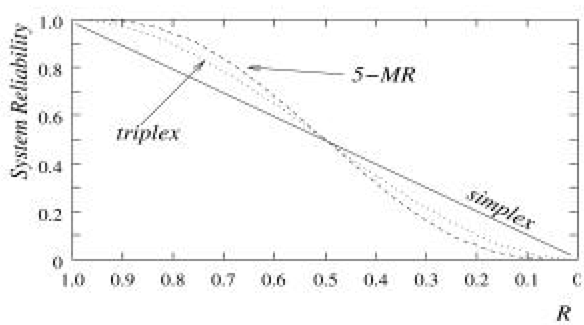
- $R(t) = e^{-lt}$
- **Assuming no voter failures -** **$R_{vot}(t)=1$**

$$R_{tmr}(t) = 3e^{-2lt} - 2e^{-3lt}$$

$$MTTF_{tmr} = \int_0^{\infty} R_{tmr}(t) \cdot dt = \frac{5}{6l} < \frac{1}{l} = MTTF_{simplex}$$

NMR - N-Modular Redundant Cluster

- **M-of-N cluster with N odd and M = (N+1)/2**
- **Assume voter failure rate negligible - $R_{vot}(t)=1$**



- **Below R=0.5 - redundancy becomes a disadvantage**
- **Usually R >> 0.5 - triplex offers significant reliability gains**

Compensating & Non-overalpping Faults

- **Conservative assumption** - every failure of voter leads to an erroneous output and any failure of two modules is fatal
- **Counter Example** - one module produces a permanent logical 1 and a second module has a permanent logical 0 - TMR will function properly
  - These are compensating faults
- A similar situation may arise regarding certain faults within the voter circuit
- **Another example** - non-overlapping faults - one module has a faulty adder and another module has a faulty multiplier
- If the circuits are disjoint, they are unlikely to generate wrong outputs simultaneously

Voters

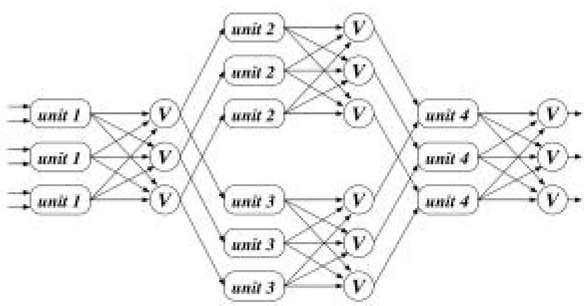
- A voter receives inputs $X_1, X_2, \ldots, X_N$ from an M-of-N cluster and generates a representative output
- **Simplest voter** - bit-by-bit comparison of the outputs producing the majority vote
- This only works when all functional processors generate outputs that match bit by bit
  - Processors must be identical, be synchronized and use the same software
- **Otherwise** - two correct outputs can diverge slightly, in the lower significant bits

Plurality Voting

- We declare two outputs X and Y as practically identical if |x-y| < d for some specified d
- A k-plurality voter looks for a set of at least k practically identical outputs, and picks any of them (or their median) as the representative
- Example - d = 0.1, five outputs
- 1.10, 1.11, 1.32, 1.49, 3.00
- The subset {1.10, 1.11} would be selected by a 2-plurality voter

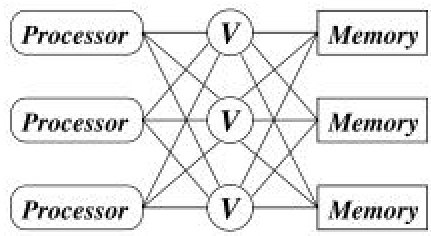
Variations on NMR

- Unit-level Modular Redundancy



- Voters no longer critical - a single faulty voter is no worse than a single faulty unit
- The level of replication and voting can be lowered using additional voters - increasing the size and delay of the system

Triplicated Processor/Memory System

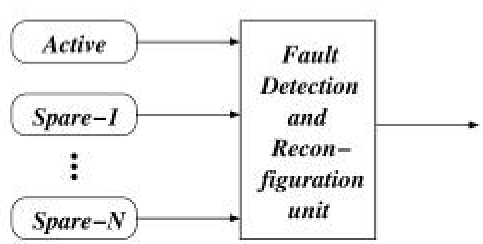


- All communications (in either direction) between triplicated processors and triplicated memories go through majority voting
- Higher reliability than a single majority voting of triplicated processor/memory structure

Active/Dynamic Redundancy

- In previous examples - considerable extra hardware used to instantaneously mask errors
- In many cases, temporary erroneous results may be acceptable if
  - * system can detect an error
  - * replace the faulty module by a fault-free spare
  - * reconfigure itself
- This is called dynamic (or active) redundancy

Example:



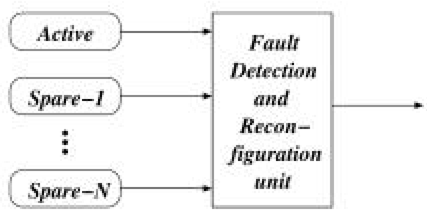
Reliability of Dynamic Redundancy - Powered Spares

- All **N** spare modules are active (powered) and have the same failure rate – resulting in a basic parallel system with **N+1** modules
- System reliability is

$$R_{dynamic}(t) = R_{dru}(t)[1-(1-R(t))^{N+!}]$$

R(t) - reliability of module

Rdru(t) - reliability of Detection & Reconfiguration unit



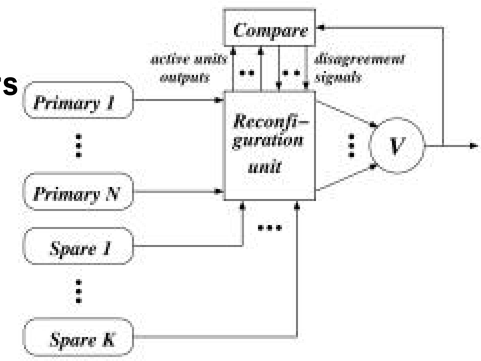
Dynamic Redundancy with Unpowered (Standby) Spares

- Spare modules are not powered (e.g., to conserve energy) and cannot fail until they become active
- **C** - **coverage factor** - probability that faulty active module is correctly diagnosed and disconnected, and good spare successfully connected
- Calculating exact reliability for the general case is complicated
- **Reliability for a special case**:
  - * Very large **N** ; constant failure rate l per active module
  - * Rate of nonrecoverable faults is **(1-C)**l
  - * Reliability at time **t** - probability of no nonrecoverable faults up to time **t**

$$R_{dynamic}(t) = R_{dru}(t)e^{-(1-c)\,l}$$

Hybrid Redundancy

- **NMR** masks permanent and intermittent failures but its reliability drops below that of a single module for very long mission times
- Hybrid redundancy overcomes this by adding spare modules to replace active modules once they become faulty
- A hybrid system consists of a core of **N** processors (**NMR**), and **K** spares



Hybrid Redundancy - Reliability

- Reliability of a hybrid system with a **TMR** core and **K** spares is

$$R_{hybrid}(t) = R_{vot}(t) R_{rec}(t)[1 - mR(t)(1-R(t))^{m-1} - (1-R(t))^m]$$

  - **m=K+3** - total number of modules
  - ***Rvot(t)*** and ***Rrec(t)*** - reliability of voter and comparison & reconfiguration circuitry
  - Assuming: any fault in voter or comparison & reconfiguration circuit will cause a system fault
- In practice, not all faults in these circuits will be fatal: the reliability will be higher

Sift-Out Modular Redundancy

- Like NMR all N modules are active but simpler than hybrid redundancy
- Comparing output of each module to outputs of other still operational modules
  - A module whose output disagrees with other is switched out
- Sift-out should not be too aggressive - most failures are transient
- Purge a module only if it produces incorrect outputs over a sustained period of time