CSED601
Dependable Computing
Lecture 4

Jong Kim

Dept. of CSE

POSTECH

Review of Previous Lecture

- Fault / Error /Failure
- Fault
  - Cause of faults
  - Fault classification
  - Fault modeling
  - Fault avoidance
- Error
  - Error model
  - Fault masking

Fault Tolerance

- Informal definition
  - The ability of a system to continue to perform its tasks after the occurrence of faults.
  - Consists of a series of actions
    - Fault-detection
    - Fault-location
    - Fault containment
    - Damage assessment
    - Reconfiguration
    - Recovery

Fault-Tolerance Idea

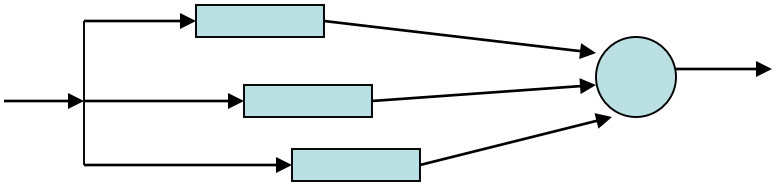
- Protective redundancy
  - Provide redundancy to protect resources
- Types of redundancy
  - Hardware
  - Software
  - Information
  - Time

Hardware redundancy

- Original concept of redundancy
- Three forms of H/W redundancy
  - Passive : no action
    - fault-masking : prevent the faults from resulting in errors
  - Active : dynamic method
    - fault-detection, fault-location, reconfiguration, recovery
  - Hybrid : combining the above two
    - combines the attractive features of both the passive and active approaches (eg. replacing the faulty module with spares)

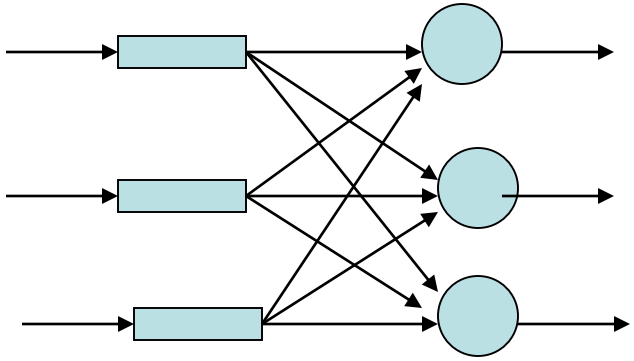
Passive H/W redundancy

- Relies on voting mechanism to mask the occurrence of faults
- Triple Modular Redundancy (TMR)
  - triplicate the hardware and perform a majority vote to determine the output of a system
  - can also be applied to software
  - problem voter < not larger than that of a voter (single-point-of-failure : SPF)

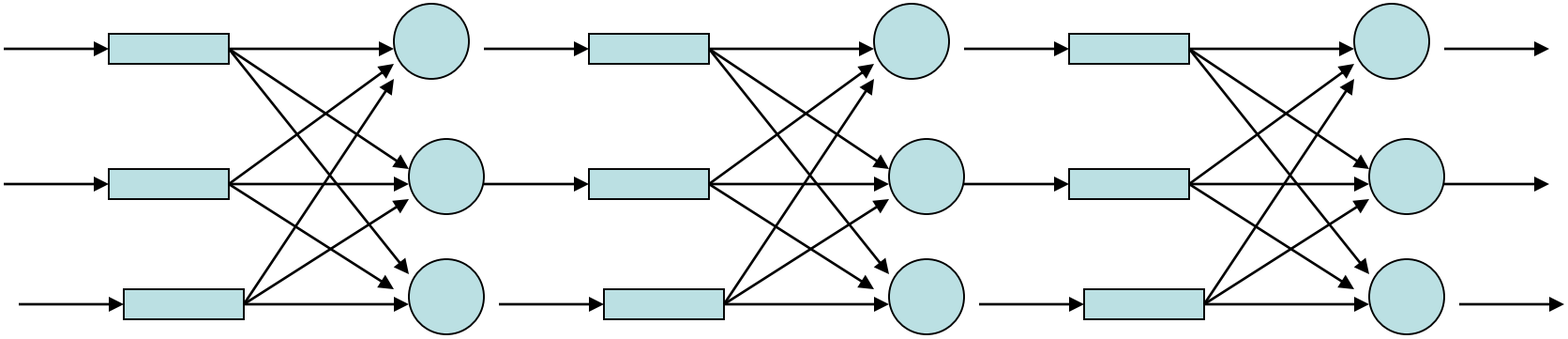


Enhancement of TMR

- Problem of TMR : SPF in voter
- Enhancement



- Restoring organ



Generalization of TMR

- N-Modular-Redundancy (NMR)
  - The same principle
  - Can tolerate more modular faults
    - Up to floor(N/2), N should be odd number

Voter

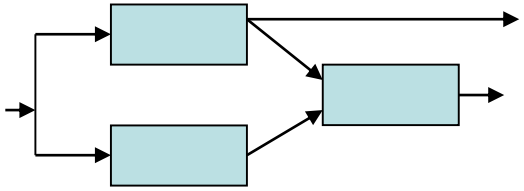
- Voter types
  - H/W (majority logic), S/W
  - H/W is fast; S/W is easier to implement and flexible
- Timing problem
  - H/W : Use flip/flop, two phase clock
  - S/W : No imminent problem
- Data imprecision problem
  - Three inputs have different values (sensor input)
  - Have a snowball effect
  - Solution
    - Mid-value select
    - Ignore LSB bits

Active H/W redundancy

- Attempt to achieve fault-tolerance by a series of actions such as fault-detection, fault-location, and fault-recovery
- Most common in applications
- Do not have the property of fault-masking
- Methods
  - Duplication with comparison
  - Stand-by sparing
  - Pair and a spare
  - Watchdog timer

Duplication with comparison

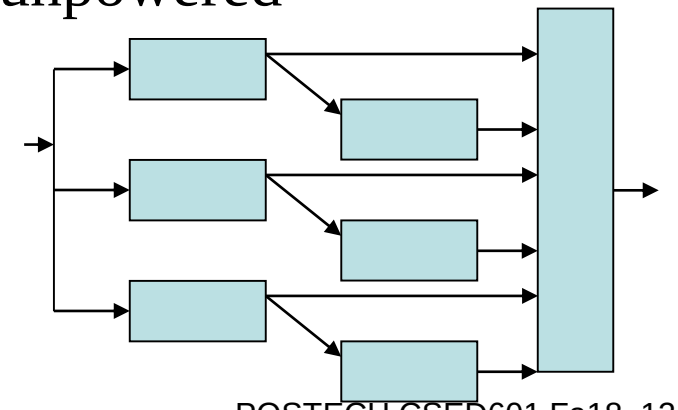
- Structure
  - Two identical pieces of hardware with comparator



- Operation
  - Perform the same computations in parallel
  - Compare the results of those computations
- Result
  - Can only detect a fault : cannot decide which one is faulty
- Problem
  - Cannot detect input errors
  - Comparator may not be able to perform an exact comparison
  - An error in the comparator
  - Imprecise results (Use only MSB)

Stand-by sparing

- Structure
  - One module operational
  - One or more modules serve as standbys or spares
  - Use various fault-detection or error detection schemes (to decide when an where) : key component
- Types
  - Hot-standby sparing : standby operates in synchrony
  - Cold-standby sparing : standby is unpowered
- Advantages of standby sparing
  - Low overhead



Pair and a spare technique

- Idea
  - Combines the features present in both stand-by sparing and duplication with comparison
- Method
  - Approach 1: select 2 outputs / compare /detect / use spare
  - Approach 2: use pair as a set / discard a pair / use a pair

Watchdog timer

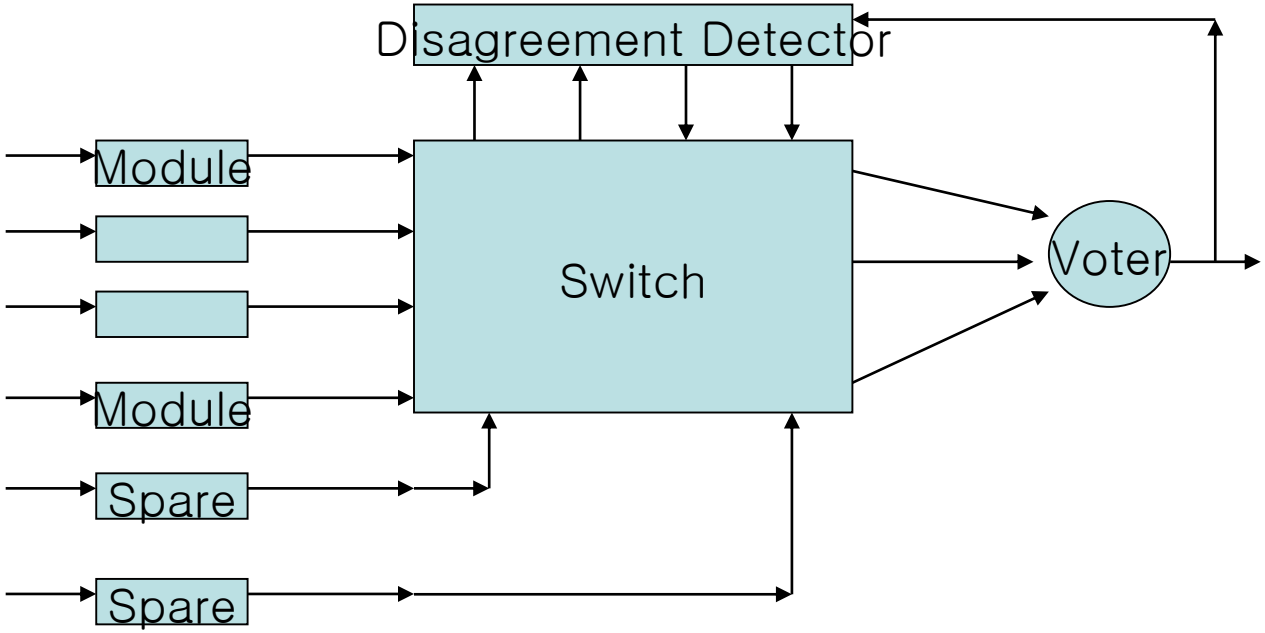
- Properties
  - Used for detecting a fault
  - Some action is required on the part of the system to indicate a fault-free status
  - System is fault-free if it possesses the capability to repetitively perform a function such as setting a tier
  - The frequency at which the timer must be reset is a function of the system
  - Watchdog timers are particularly useful for detecting a lack of response
  - Can be implemented by software

Hybrid H/W redundancy

- Idea
  - Combines the attractive features of both the active and the passive approaches
  - Most often used in applications that require extremely high integrity of computations
- Method
  - NMR with sparing
  - Self-purging redundancy
  - Sift-out modular redundancy
  - Triple-duplex architecture

NMR with spares

- Idea
  - Spares are provided to replace failed units in the NMR core
- Structure

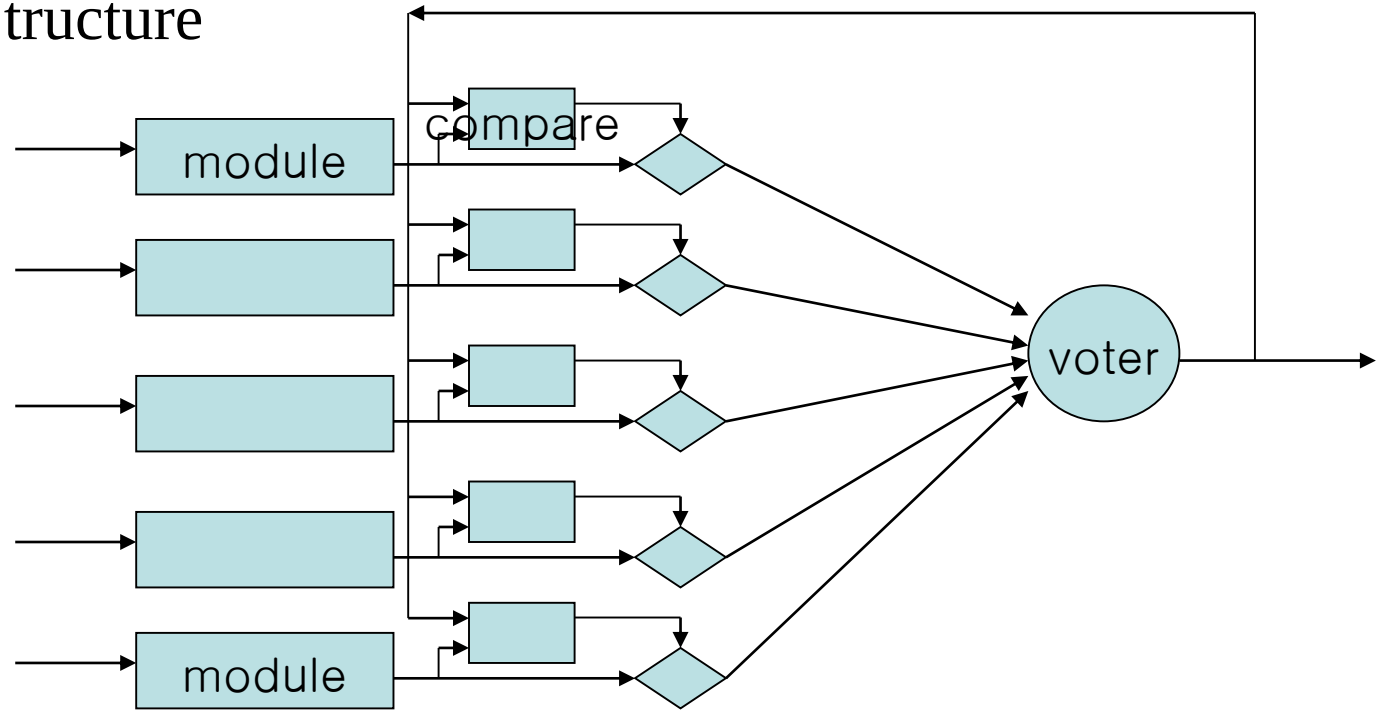


NMR with spares

- Characteristics
  - Only NMR approach : fault-masking
  - NMR with spares : fault-detection, location, and reconfiguration
  - How to detect/locate : compare individual output with voter output

Self purging redundancy

- Idea
  - Similar to NMR with spares
  - Difference : All units are actively participating in the system
- Structure

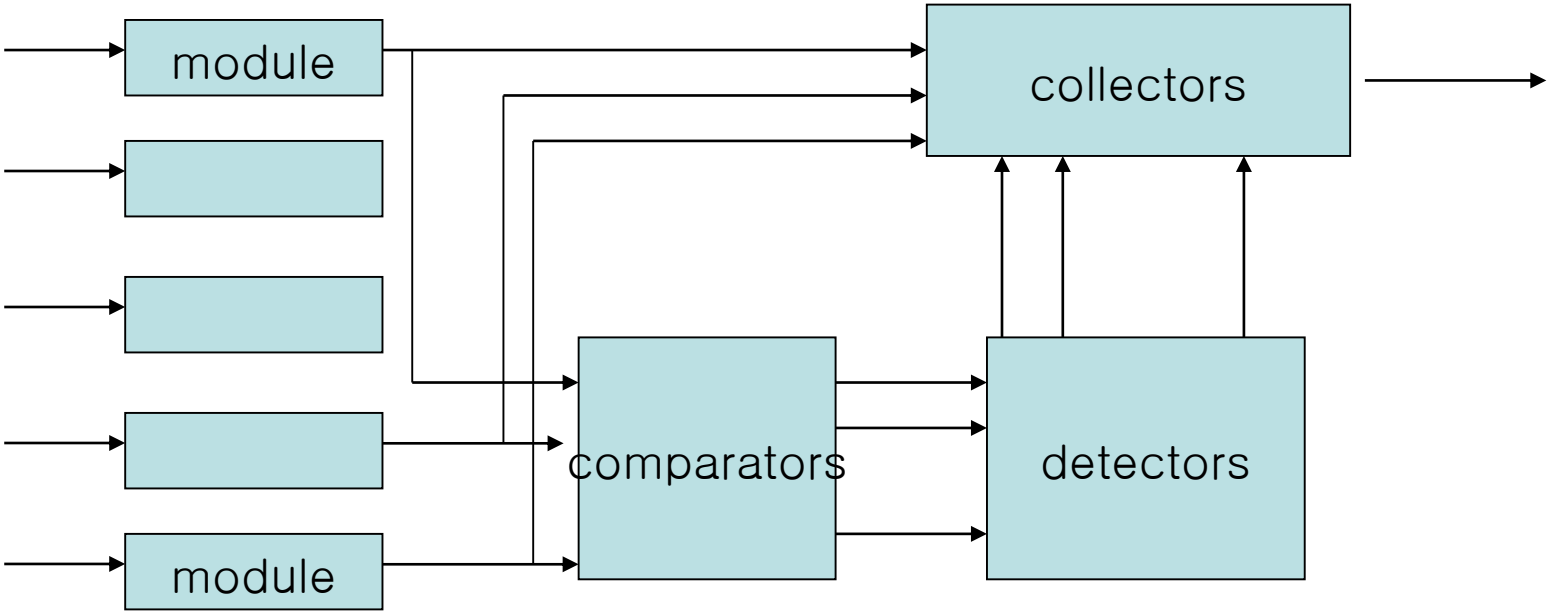


Self-purging redundancy

- Characteristics
  - Each module is designed with the capability to remove itself from the system in the event that its output disagrees with the voted output of the system
  - How to adjust a voter to reduced inputs : a threshold voter
    - A threshold voter is like a neuron in neural network
    - Adjust the threshold value according to the input

Sift-out modular redundancy

- Structure
  - Use N elements, comparators, detectors, collectors

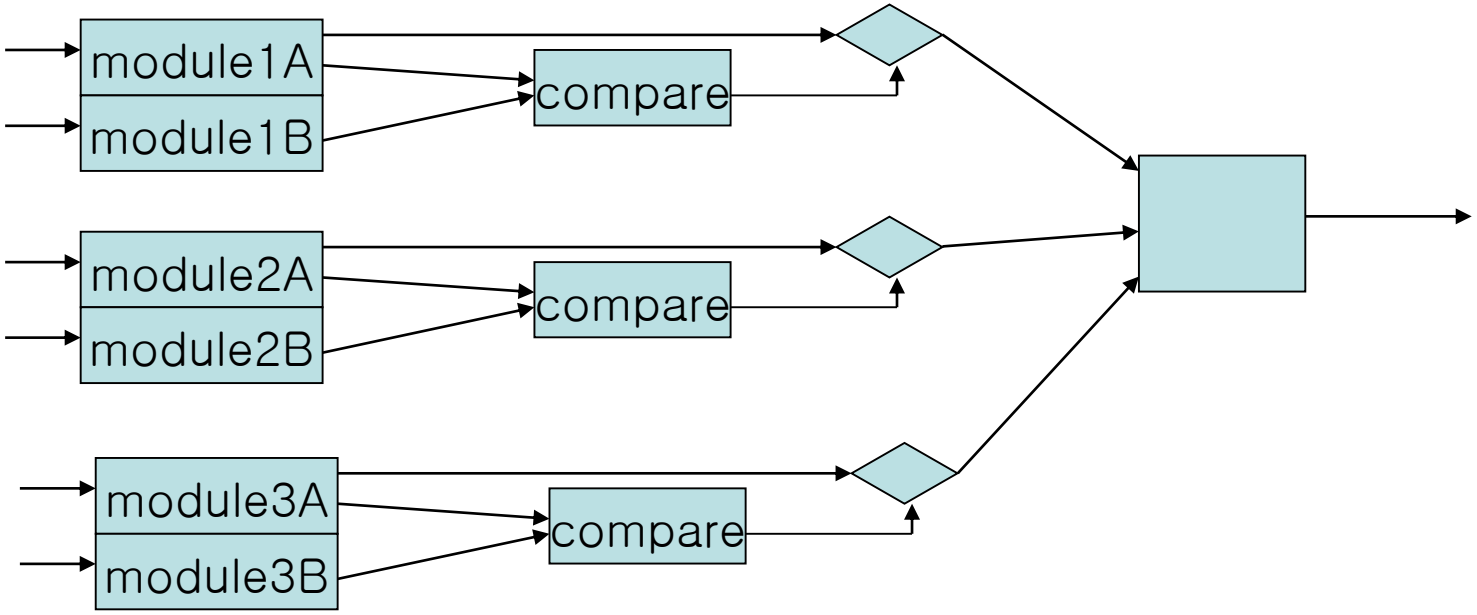


Sift-out modular redundancy

- Role of each component
  - Comparators
    - Compare each module's output with the remaining modules' output: N(N-1) comparisons
  - Detector
    - Determine which disagreements are reported by the comparator and to disable a unit that disagrees with a majority of the remaining modules
  - Collector
    - To produce the system's output, given the outputs of the individual modules and the signals from the detector that indicate which module is faulty

Triple-duplex architecture

- Structure
  - Combines duplication with comparison and TMR
  - Use duplication for error-detection
  - Use TMR for fault-masking



Summary of H/W redundancy

- Critical computation applications
  - Mandate passive or hybrid redundancy
- The highest reliability
  - Can be achieved by hybrid
- Long life and high availability
  - Active approaches are used
  - It is acceptable to have a temporary, erroneous outputs
- Hardware cost
  - Active / Passive / Hybrid