CPE 633
Chapter 2 – Hardware Fault Tolerance

Dr. Rhonda Kay Gaede

UAH

Introduction

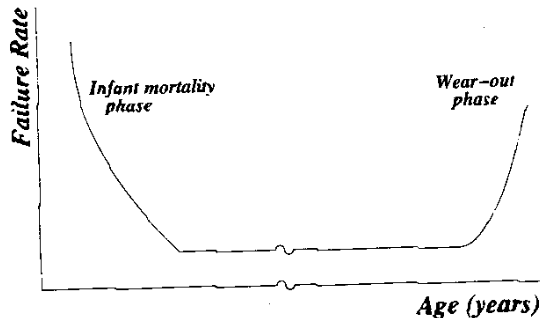
- Hardware fault tolerance is the most ________ of the fault-tolerance areas.
- Many techniques are extant.
- The main drawback has been ______.
- As transistors become free, ______ ________________________________ ________________________.
- ________ may be the new ______.

2.1 The Rate of Hardware Failures – Component Failure Rates

- Component failure rate
  - The ______________________________ that a currently _____________ component will suffer in a given _________________________

Depends on

1. ________
   ____
2. __________
   ____
   ____
3. __________
   ____
4. _________



2.1 The Rate of Hardware Failures – Factors Involved in Component Failure Rates

$$\lambda = \pi_L \pi_Q (C_1 \pi_T \pi_V + C_2 \pi_E)$$

λ Failure rate of component

π_L _____________ factor

π_Q ____________ factor

π_T ______________ factor

π_V ___________________ factor for CMOS

π_E __________________________ factor

C_1, C_2 ________________ factors

2.2 Failure Rate, Reliability and MTTF– Component Lifetimes

- Consider a component that is operational at time t = 0 and remains operational until it is hit by a failure (______________ and ___________________)
  - __ is the _____________ of the component
  - _____ is the ______________________, represents the _____________ probability of a failure at time t
  - ______ is the _______________________________, is the probability that the ___________ will __________ _______________, F(t) = Prob{T ≤ t}
  - ______ is the _____________ of a component, the probability that it will ____________________, R(t) = Prob{T > t} = 1 – F(t)
- Facts

$$f(t) = \frac{dF(t)}{dt} \quad F(t) = \int_0^t f(\tau)d\tau \quad \int_0^\infty f(t)dt = 1 \quad f(t) \geq 0 \; for \; t \geq 0$$

UAH Chapter 2 CPE 633

2.2 Failure Rate, Reliability and MTTF– Component Reliability

- F(t) represents the probability that a ______ component will fail ___________ in the future. A more meaningful quantity is the probability that a good component of ______________ will fail in the next ______________. This is a ________________ probability, since we know the component survived ______________________.

$$\lambda(t) = \frac{f(t)}{1 - F(t)}$$

- We can put this in terms of reliability

$$\frac{dR(t)}{dt} = \frac{d(1-F(t))}{dt} = \frac{-dF(t)}{dt} = -f(t)$$

- Solving for R (R(0) = 1)
  - R(t) =
- f(t) = F(t) =

2.2 Failure Rate, Reliability and MTTF– MTTF of a Component

- For an _______________ component, the _________ is equal to its ____________________, E[T]
  - MTTF = E[T] =
  - MTTF =

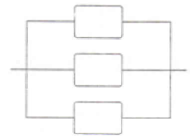
2.2 Failure Rate, Reliability and MTTF– Non-Constant Failure Rates

- Although a ________________ failure rate is used in most calculations of reliability, there are cases for which this simplifying assumption is _________________, especially during the ____________________ and ___________ phases of a component's life.
- In such cases, the ______________ distribution is often used, which has two parameters, ___ and ___, and has the following density function of the lifetime T of a component
  - f(t)
  - λ(t)
  - R(t)
  - MTTF =
  - Γ(x)

2.3.1 Series and Parallel Systems – Series System Reliability

- One of the most basic structures is the ________ system shown.
- A _________ system is defined as a set of N modules connected together so that the failure of ________________ causes the entire system to fail.
- If the failure of each module is _______________, the reliability of the system is
  - $R_s(t)$ =
- If module i has a constant failure rate, λ_I
  - $R_s(t)$ =
  - $MTTf_S$ =

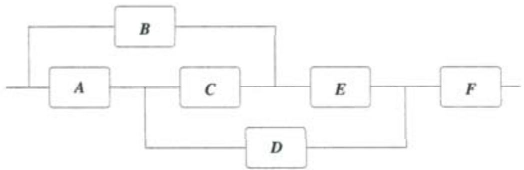
2.3.1 Series and Parallel Systems – Parallel System Reliability



- The other most basic structure is the __________ system shown.
- A _________ system is defined as a set of N modules connected together so that it requires the failure of _____________ for the system to fail.
- If the failure of each module is _______________, the reliability of the system is
  - $R_P(t)$ =
- For two modules
  - $R_P(t)$ =
  - $MTTF_p$ =

2.3.2 Non-Series/Parallel Systems – Hybrid System Reliability

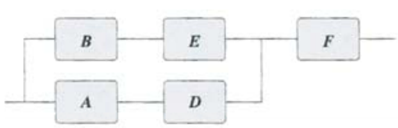
- Not all systems have a ______________________ with a _______________ structure.



- Each path represents a ____________________ that allows the system to operate _________________.
- For example, the path _________ means successful operation if ________________ are fault-free.
- A path in such reliability diagrams is valid only if all modules and edges are traversed from ________ _______________, for example, ___________ is an invalid path in the example shown.

2.3.2 Non-Series/Parallel Systems – Expansion Around C, C Not Working

- The diagram can be _____________ until we have the ______________ series or parallel forms. To do this, we rely on the ____________________________
  - $R_{system} = R_i$*Prob{system works|I is fault-free} + $(1-R_i)$*Prob{system works|I is faulty}
- We pick one module to ______________, in this case, module ___.



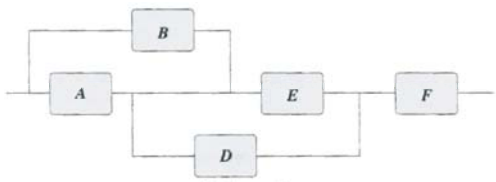
(a) C not working

For C not working, we have B and E in parallel with A and D, all in series with F.

Prob{system works|C faulty} =

2.3.2 Non-Series/Parallel Systems - Expansion Around C, C Working

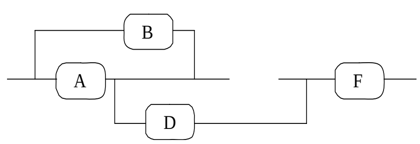
- For C working, we still _______________ simple parallel series combinations, so we must pick another module about which to _________. Let's try ___.



(b) C working

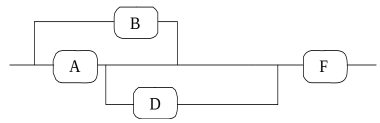
2.3.2 Non-Series/Parallel Systems - Expansion Around E, E Not Working

- The diagram for E not working is shown, it has a _________________ structure, the only path is _______.
  - $R_{E\ not\ working} = R_A*R_D*R_F$
  - $R_{system} = R_i$*Prob{system works|I is fault-free} + $(1-R_i)$*Prob{system works|I is faulty}



2.3.2 Non-Series/Parallel Systems - Expansion Around E, E Working

- The diagram for E working is shown. There are three paths, _____, ______ and _______. However, the ____ path __________ the _____ path (if ____ and ____ are both working, the system works whether ____ works or not.
  - Re working = R_F*(1-R_A)(1-R_B)



Putting it all together,
Rsystem =

2.3.2 Non-Series/Parallel Systems – Reliability Upper Bound

- If the structure is too complicated for repeated application of the _______________, it is possible to calculate upper and lower __________, rather than ________ values, for the reliabilities of the system.
- An upper ___________ is given by
  - Rsystem

    where R_{path} I is the reliability of the series connection of the modules along path I.
- This bound assumes that all the paths are ____________ and that they are _________________.
- Going back to our example, the paths are ______, _______, and ________.
  - Rsystem =
- The upper bound can be used to derive the ___________ reliability by replacing every occurrence of $(Ri)^k$ by R_i, since each module is used only once.

2.3.2 Non-Series/Parallel Systems – Reliability Lower Bound

- A lower bound can be calculated based on ___________ _________ of the system diagram, where a ____________ ______ is a minimal list of modules such that the removal of _____________ of the set will cause a ___________ system to ______.
- The lower bound is obtained by
  - R_{system} =
    where Q_{cuti} is the probability that _______________ is faulty.
  - Back to our example, where the __________________ are _____, ______, ______, _____, and _______.
  - R_{system} =
  - We'd rather use the ________ bound because we'd like to be _____________ about the reliability rather than _______________ and it's _________ to the exact value.

2.3.3 M-of-N Systems – Reliability

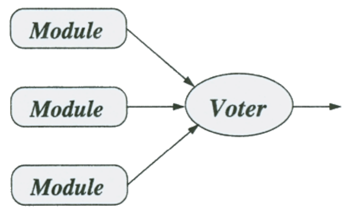
- An _________ system is a system that consists of ___ modules and needs at least ___ of them for proper operation, the system fails when ______________ modules are ______________.
- The best-known ________ is the ________, or _________, system, in which there are _________________ modules and a _________.
- Reliability of an ________ system
  - $R_{M\_of\_N}(t)$ =
- The assumption that failures are ______________ is _____ to the high reliability of ________ systems.

$R_{M\_of\_n\ cor}(t)$ =

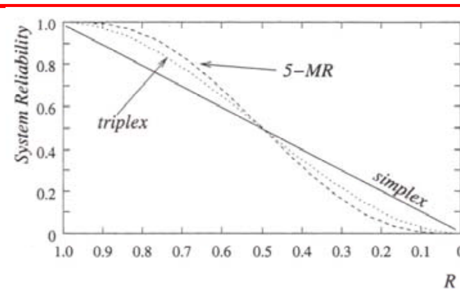
where is the probability that the entire system suffers a common failure.

2.3.3 M-of-N Systems – Triple Modular Redundant (TMR) Cluster

- If a ________ voter is used, that voter becomes a ________ point of failure and the reliability of the ___________ is
  - $R_{TMR}(t)$
- The general case of TMR is called ________________ redundancy (________) and is an M-of-N cluster with N odd and M = ⌈N/2⌉



2.3.3 M-of-N Systems – Comparing Reliabilities

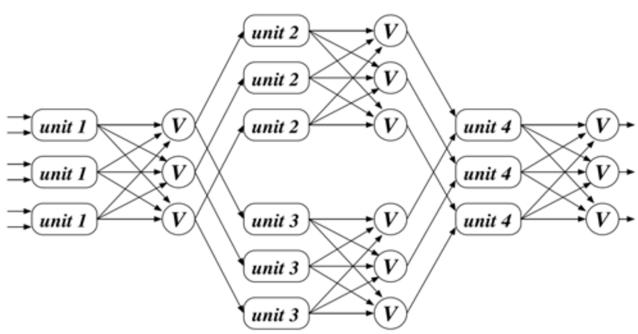


- For ______ values of R(t), the ___________ the redundancy, the ________ the system reliability. As R(t) ____________, the advantages of redundancy become __________; until for R(t) < _____, redundancy actually becomes a ___________, with the ________ being the most reliable.

2.3.4 Voters

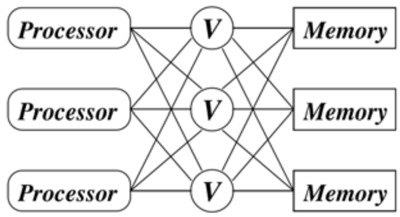
- A voter receives inputs $x_1, x_2, \ldots, x_N$ from an _______ _______ and generates a representative _______.
- The simplest voter is one that does a _________ comparison of the outputs and checks whether a __________ of the ____ inputs are ___________.
- This approach is valid when there is __________ ___________ between all modules.
- This __________ occurs when the modules are identical ___________, use identical _______ and identical __________ and have mutually ___________ clocks.
- We declare two outputs x and y as _____________ __________ if $|x - y| < \delta$ for some specified δ.
- There may also be __________ associated with each output.

2.3.5 Variations on NMR – Unit Level Redundancy



- The voters are no longer as critical as in ____.
- A single faulty voter will cause __________ than a single faulty unit, and the effect of either one will not propagate beyond the ________________.

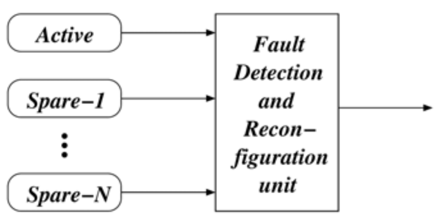
2.3.5 Variations on NMR – Triplicated Processor/Memory System



- Communication is ___________.
- All communications go through _______ voting.

UAH Chapter 2 CPE 633

2.3.5 Variations on NMR – Dynamic Redundancy

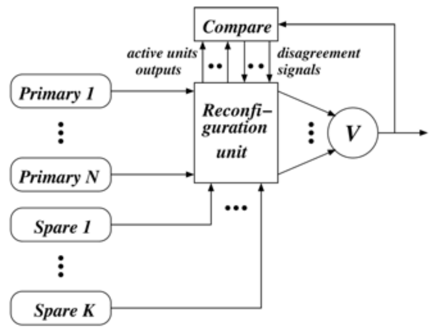


- Powered Spares
  - $R_{dynamic}(t)$ =
- Spares not Powered
  - $R_{dynamic}(t)$ =
  - c=
  - R_{dru} =

2.3.5 Variations on NMR – Hybrid Redundancy

Hybrid redundancy boosts _________ by adding _____ _______ that will be used to replace active modules once they become ______.

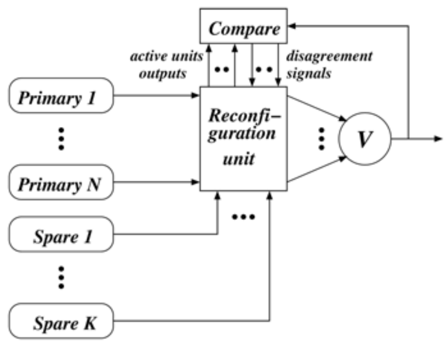
- The outputs of the active primary modules are compared to identify a faulty primary, which is disconnected and replaced by a spare.
- $R_{hybrid}(t)$
- m =
- $R_{voter}(t)$
- $R_{rec}(t)$



UAH Chapter 2 CPE 633

2.3.5 Variations on NMR – Hybrid Redundancy

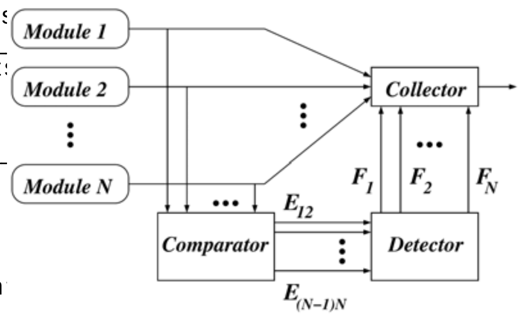
- Assumption was that any fault in the _____, ____________, or ______________________ will cause system failure.
- In practice, not all these faults are _____
- You'd have to know something about the various ______________



2.3.5 Variations on NMR – Sift-Out Modular Redundancy

As in _____, all N modules in the Sift-Out Modular Redundancy scheme are _______, and the system is operational as long as there are at least ______________ modules.

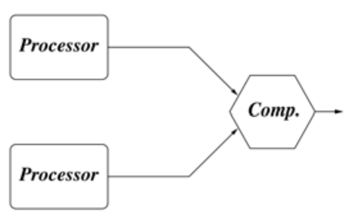
- Instead of a majority voter, this system uses ___________,___________ and __________ circuits
- Faulty outputs, as identified by the _________ and _______ are not used in the collector which _____ fault-free modules.
- Exclude ________ by requiring disagreement for _______________.



2.3.6 Duplex Systems – Basics

A duplex system, consisting of two processors and a comparator, is the simplest example of module redundancy.`

- Both processors execute ___________ ______.
- If the results are ___________, there is a ________, and ________ ______________ takes over.
- R_{duplex} =



$MTTF_{duplex}$ =

UAH Chapter 2 CPE 633

2.3.6 Duplex Systems – Faulty Processor Identification

- Acceptance Tests
  - Example, ___________, is the output in an expected _______
  - What should the _______ be?
    - If it's very _______, all bad will be identified as bad, but some good may also be identified as bad.
    - If it's very _______, all good will be identified as good, but some bad may also be identified as bad.
    - The ___________ is the conditional probability that the test ______________ given that the output is actually _____________.
    - The ______________ is the conditional probability that the output ____________ given that the test ______________________.
    - We want them both to be very _____.

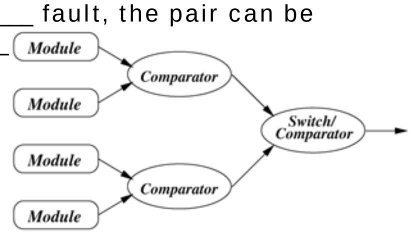
UAH Chapter 2 CPE 633

2.3.6 Duplex Systems – Faulty Processor Identification

- Hardware Testing
  - Subject both processors to some hardware/logic test routines.
  - This approach works well as long as the fault is _____________, though it can still have escapes.
- Forward Recovery
  - Use a third processor to repeat the computations. If only one of the three is faulty, then whichever processor the ______________ _______________ with is the faulty one.

2.3.6 Duplex Systems – More Complicated Resilient Structures

- Pair-and-Spare System
  - To avoid disruption of service, an ____________ is disconnected and the ________________ is transferred to a _____________.
  - The two members of the switched-out pair can now be tested offline to determine whether the fault was ___________ or __________.
  - In the case of a _________ fault, the pair can be marked as a __________



2.3.6 Duplex Systems – More Complicated Resilient Structures

- Triplex-Duplex System
  - Processors are tied together to form __________, and then, a _______ is formed out of these___________.
  - When the processors in a _________ disagree, both of them are _____________ of the system
  - This arrangement allows for the ___________ of voting combined with a simpler identification of ________ ____________.
  - Furthermore, the __________ can continue to function even if only _____________ is left functional, because the duplex arrangement allows the _______________ ___________.

2.4.1 Poisson Processes

- Consider _______________ events of some sort, occurring over time with the following ___________ behavior: For a time interval of very short length, Δt
  $P_1(\Delta t) =$
  $P_{>1}(\Delta t) =$
  $P_0(\Delta t) =$
- Let N(t) denote the _____________ occurring in an interval of length t, and let $P_k(t) = \text{Prob}\{N(t)=k\}$ be the probability of exactly _______ occurring during an interval of length t (k=0,1,2,...).
  $P_k(t + \Delta t)$
  $P_0(t + \Delta t)$

2.4.1 Poisson Processes

- These approximations become more accurate as $\Delta t \rightarrow 0$, and lead to the differential equations
- Using the initial condition $P_0(0) = 1$, the solution to this set of differential equations is

2.4.1 Poisson Processes

- N(t) is a Poisson process with rate λ.
  - The expected ______________ occurring in an interval of length t is λt.
  - The length of time between ___________events is an exponentially distributed random variable with parameter λ and mean value $1/\lambda$.
  - The number of events occurring in disjoint intervals of time are ______________ of one another.
  - The sum of two independent Poisson processes with rates $\lambda 1$ and $\lambda 2$ is itself a Poisson process with rate $\lambda 1 + \lambda 2$

2.4.1 Poisson Processes – Duplex System

- System consists of two _________ active processors with an unlimited number of _______ spares.
  - The two active processors are subject to failures occurring at a constant rate of λ per processor.
  - As before , the coverage factor c is the probability of successful detection and ________ – assume comparator failure rate is negligible and ________ is instantaneous.
  - N(t), the number of failures that occur in ____ ________, is a Poisson process with the rate λ.
  - M(t), the number of failures that occur in _________, is a Poisson process with the rate 2λ

Prob{k failures in duplex} = Prob{M(t)=k} =

2.4.1 Poisson Processes – Duplex System Reliability Calculation

- For the duplex system not to fail, each of these failures must be ________ and the processor __________ ________. The probability of one such success is c, and the probability that the system will survive k failures is c^k.

  $R_{duplex}(t) =$

  - The extension to the case with only a _______ set of spares requires capping the summation at the ______ ____________.

2.4.1 Poisson Processes – Duplex System Reliability Reasoning

- Individual processors fail at a rate λ, and so processor failures occur in the duplex at the rate 2λ.
- Each processor failure has a probability c of being successfully dealt with and a probability of (1 - c) of causing failure to the duplex.
- As a result, failures that crash the duplex occur with rate $2\lambda(1 - c)$
- The reliability of the system is thus $e^{-2\lambda(1-c)t}$

2.4.2 Markov Models

- Markov models provide a _______________ for the derivation of reliabilities of systems.
- A Markov chain is a special type of _________ _______, X(t) - infinite number of random variables, indexed by t with a special ___________ structure.
- For X(t) to be a Markov chain, is future state must depend only on the ___________ and not any _____ _____.
- If X(t) = i, the chain is in state i at time t.
- We deal only with Markov Chains with _________ time $(0 \le t \le \infty)$ and _______ state $(X(t)=0,1,2,\ldots)$

2.4.2 Markov Models – Probabilistic Behavior

- Once a Markov chain moves into some state i, it stays there for a length of time that has an __________ distribution with parameter, λ_i, implying a constant rate, λ_i, of leaving state i.
- p_{ij} is the probability that, when _______ state i, the chain will move to state j (with $j \neq i$)
- The ________ rate from state i to state j, λ_{ij}, is thus $\lambda_{ij} = p_{ij}\lambda_i$.
- $P_i(t)$ is the probability that the process will be in state i at time t.
- Either
  - It was in state i and ___________ during Δt
  - It was at some other state j and ______ during Δt

2.4.2 Markov Models – Probabilistic Behavior

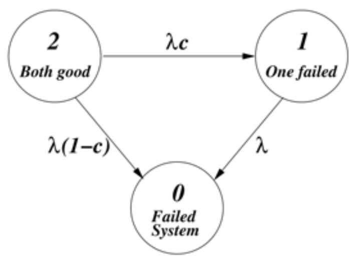
- We have
  - $P_i(t+\Delta t) \approx P_{i0}(\Delta t) + P_{j1}(\Delta t)$ from all other states
  - $P_{i0}(\Delta t) =$, $P_{j1}(\Delta t) =$
  - $P_i(t+\Delta t) \approx$

$$\frac{dP_i(t)}{dt} =$$

- Initial Conditions $P_{i0}(0) = 1$ and $P_j(0) = 0$ for $j \neq i_0$

2.4.2 Markov Models – Duplex System (Active + Standby Spare)

$$\frac{dP_2(t)}{dt} =$$



$$\frac{dP_1(t)}{dt} =$$

$$\frac{dP_0(t)}{dt} =$$

$P_2(t) = e^{-\lambda t}$, $P_1(t) = c\lambda t e^{-\lambda t}$, $P_0(t) = 1 - P_1(t) - P_2(t)$

$R_{system} =$

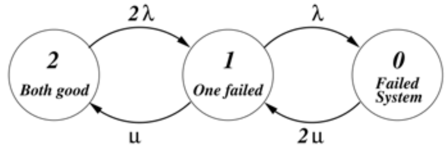
UAH Chapter 2 CPE 633

2.4.2 Markov Models – Duplex System (Both Active with Repair)

$$\frac{dP_2(t)}{dt} =$$

$$\frac{dP_1(t)}{dt} =$$

$$\frac{dP_0(t)}{dt} =$$



$P_2(t) =$

$P_1(t) =$

$P_0(t) = 1 - P_1(t) - P_2(t)$

$A(t) = P_1(t) + P_2(t)$, $A(\infty) = P_1(\infty) + P_2(\infty)$

Electrical and Computer Engineering Page 43

UAH Chapter 2 CPE 633

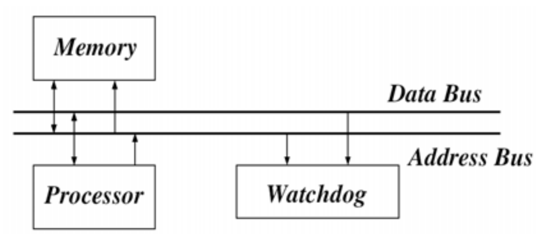
2.5 Fault-Tolerance Processor-Level Techniques

- ________ structures can be applied to a wide range of modules, from __________ to __________, to ______, etc.
- In many cases, the overhead is __________.
- Another approach is execute every program ______, using results only ____________. No hardware redundancy but severe time redundancy – _________________.
- We could apply this at the __________ level.
- Alternate scheme is ________ processor that monitors the behavior of the ______________.

Electrical and Computer Engineering Page 44

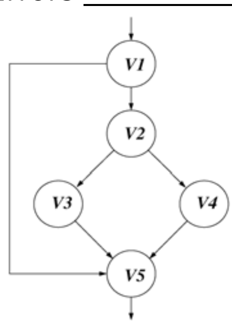
2.5.1 Watchdog Processor

- The watchdog processor monitors the ____________, looking mainly for proper program control.
- The _______ must know what to expect.
- This information is derived from the CFG, each node is a __________.



2.5.1 Watchdog Processor – Assigned Signatures

- Signatures correspond to _____ of the CFG, they can be ________ or _________.
- CFG and corresponding watchdog program with _______ signatures
- Errors ____________ are not detected.

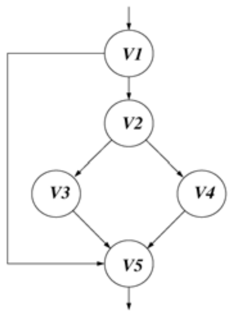



```
accept sig(V1);
either
    accept sig(V2);
    either
        accept sig(V3);
    or
        accept sig(V4);
    accept sig(V5);
or
    accept sig(V5);
```

UAH Chapter 2 CPE 633

2.5.1 Watchdog Processor – Calculated Signatures

- Signatures can be calculated, for example, by ______ ______________________________.
- Watchdog holds __________ calculated signatures
- Still won't detect data errors, could use __________ or supplement with other ______________ schemes.



accept & check sig(V1);
either
    accept & check sig(V2);
    either
        accept & check sig(V3);
    or
        accept & check sig(V4);
    accept & check sig(V5);
or
    accept & check sig(V5);

Electrical and Computer Engineering Page 47

UAH Chapter 2 CPE 633

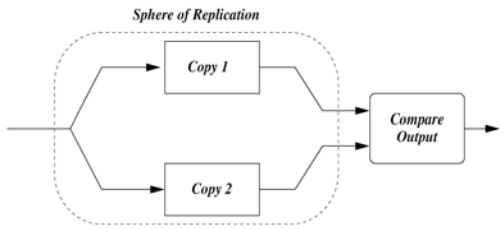
2.5.2 Simultaneous Multithreading for Fault Tolerance

- If data and control dependencies limit the amount of ___________ that can be extracted out of individual threads, allow the processor to execute _______ _______ simultaneously.
- __________________ for simultaneous execution is required.
- Each thread must have
  - ________________
  - ________________
- For fault detection purposes, two ___________ threads are created for each original thread.
- These threads execute the same code and receive the same inputs.
- If they produce the same results, __________, else ____________________ .

Electrical and Computer Engineering Page 48

2.5.2 Simultaneous Multithreading for Fault Tolerance

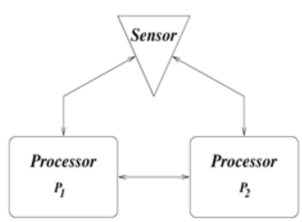
- To reduce the _________________ of re-execution, one thread trails the other and takes advantage of the __________________, for example, _______ _________ results.
- For the two threads to be ____________, they must execute on different sets of ______________.
- Items that are _________ for the two threads are said to be within the _________________, otherwise they are outside it.



2.6 Byzantine Failures

- Byzantine failures are ________ failures, failures that are not obvious faults but that produce ______________.
- If ______________ has such a failure in a TMR, the other two will just _______ it.
- However, when processors are __________ with no ___________ entity, problems can ensue.

•Consider a sensor providing information to two processors, it tells processor 1 25º and processor 2 45º. Each processor knows there is a problem but not which is right.



2.6 Byzantine Failures – Byzantine Generals (Interactive Consistency) Problem

- One sender ___________ an order to multiple receivers who can _______________________ about the value they received from the _______ ______.
- A functional unit will be _______ in all its messages.
- A faulty unit may behave ________.
- All communications have a _______ mechanism.
- Interactive Consistency Conditions
  - IC1. All _________ units must arrive at an ________ of the value that was transmitted by the ____________.
  - IC2. If the original source was ________, the value they agree upon must be the value that was transmitted by the original source.

2.6 Byzantine Failures – Interactive Consistency Algorithm

- Algorithm Byz(N, m).
  - N is the ___________ (_____ and N-1 _________)
  - m is the number of _____ units
  - Interactive consistency is possible if _________
- Pseudocode

```
Source disseminates the information to N-1 receivers.
If m > 0 then
    Each receiver runs Byz(N - 1, m - 1)
    Each unit takes a vote over all messages received
    If majority
        Use majority
    Else
        Use default
else
    each receiver uses value received from source
```

2.6 Byzantine Failures – IC Algorithm Notation & Degenerate Example

- If A and B are units, then _______ means that A sent B the message n.
- If *U* is a string of units A_1, A_2, ..., A_m, and B is a unit, then _______ means that B received the message n from A_m who claims to have received it from A_{m-1} and so on.
- A message that is not sent is denoted by φ. For example, A.B(φ) means that the message that A was supposed to send B was never sent.
- Example, degenerate case, m=0. The source sends to all receivers who use the value sent.

2.6 Byzantine Failures – IC Algorithm Example(m = 1)

- Example, m = 1, need at least 4 units, S, R_1, R_2, R_3
- S is faulty, default = 1, IC(R_2,R_1) is value of R_1 as reported by R_2
- Byz(4,1)

  S.R_1(1), S.R_2(1), S.R_3(0)

  Since m=1,

  R_1 runs(3,0) S.R_1R_2(1), S.R_1R_3(1),
  IC(R_2,R_1) = 1, IC(R_3, R_1) = 1

  R_2 runs(3,0) S.R_2R_1(1), S.R_2R_3(1),
  IC(R_1,R_2) = 1, IC(R_3, R_2) = 1

  R_3 runs(3,0) S.R_3R_1(0), S.R_3R_2(0),
  IC(R_1,R_3) = 0, IC(R_2, R_3) = 0

  ICV(R_1) = (1, 1, 0), ICV(R_2) = (1, 1, 0), ICV(R_3) = (1, 1, 0)

  R_1, R_2, and R_3 vote and get 1

  ICV(R_1) is (source, R_2 reported by R_1, R_3 reported by R_1)

2.6 Byzantine Failures – IC Algorithm Example(m = 2)

- Let N = 7, m = 2, S, R1, R2, R3, R4, R5, R6, R1 and R6 are faulty
- Byz(7,2)
  - $S.R_1(1)$, $S.R_2(1)$, $S.R_3(1)$, $S.R_4(1)$, $S.R_5(1)$, $S.R_6(1)$
  - R1 Byz(6,1)
    - $S.R_1.R_2(1)$, $S.R_1.R_3(2)$, $S.R_1.R_4(3)$, $S.R_1.R_5(4)$, $S.R_1.R_6(0)$
      - R2 Byz(5, 0)
        - $S.R_1.R_2.R_3(1)$, $S.R_1.R_2.R_4(1)$, $S.R_1.R_2.R_5(1)$, $S.R_1.R_2.R_6(1)$
      - R3 Byz(5, 0)
        - $S.R_1.R_3.R_2(2)$, $S.R_1.R_3.R_4(2)$, $S.R_1.R_3.R_5(2)$, $S.R_1.R_3.R_6(2)$
      - R4 Byz(5, 0)
        - $S.R_1.R_4.R_2(3)$, $S.R_1.R_4.R_3(3)$, $S.R_1.R_4.R_5(3)$, $S.R_1.R_4.R_6(3)$

2.6 Byzantine Failures – Another Algorithm Example

- R5 Byz(5, 0)
  - $S.R_1.R_5.R_3(4)$, $S.R_1.R_5.R_4(4)$, $S.R_1.R_5.R_5(4)$, $S.R_1.R_5.R_6(4)$
- R6 Byz(5, 0)
  - $S.R_1.R_6.R_2(1)$, $S.R_1.R_6.R_3(8)$, $S.R_1.R_6.R_4(0)$, $S.R_1.R_6.R_5(\varphi)$
- $ICV_{S.R1}(R_2)$ = (1, 2, 3, 4, 1) $S.R_1$ reported by $R_2 = 0$
- $ICV_{S.R1}(R_3)$ = (1, 2, 3, 4, 8) $S.R_1$ reported by $R_3 = 0$
  $ICV_{S.R1}(R_4)$ = (1, 2, 3, 4, 0) $S.R_1$ reported by $R_4 = 0$
- $ICV_{S.R1}(R_5)$ = (1, 2, 3, 4, 0) $S.R_1$ reported by $R_5 = 0$
  $ICV_{S.R1}(R_6)$ = (, , , ,) $S.R_1$ reported by $R_6 = 0$
- …

2.6.1 Byzantine Agreement with Message Authentication

- Algorithm ABYz(N, m).
  - Source ____________ with ψ and sends it out to each of the processors.
  - Each processor i that receives a ____________ ψ : A, where A is the set of __________ appended to the message , checks the _______ of signatures in A. If this number is less than _____, it sends out ψ : A ∪ {i} (what it received plus its own signature) to each of the processors __________. It also adds this message, ψ, to its list of _______ messages.
  - When a processor has seen the signatures of _____ ______ processor (or has timed out), it applies some _______________ to select from among the messages it has received.