Yan Lin, Weekly report 07/05/05

General concept on fault tolerant computing

Measures of Fault-Tolerant Computing

i) Dependability: - a qualitative description that encompasses the terms above and reflects the overall quality of service.

ii) Reliability: R(t) -- the probability that a system will function properly over the time interval 0... t. (Typical spacecraft requirement R(10 years) = 0.95, aircraft requirement R(10 hours = .999999999)

iii) Availability: A(t) -- the probability that a system is operating correctly and able to perform its function at time t. (Sometimes expressed differently -- maximum downtime in an interval, e.g. telephone system < 10 minutes in 40 years.)

iv) Performability: P(L,t) the probability that a system will perform at or above some level L at time t. (Example a large network.)

v) Maintainability: M(t), the probability that a failed system can be restored to working condition within time t.

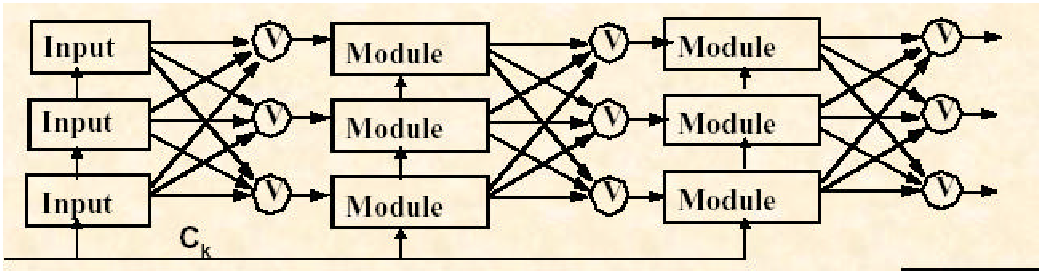
vi) Testability: – the ability to test a system; often measured in test coverage (the percentage of faults of a given class that can be uncovered by the test procedure).

vii) Safety: S(t) -- the probability that a system will either perform its functions correctly or fail in a benign way. (Example, a nuclear power plant).

Basic hardware redundancy techniques

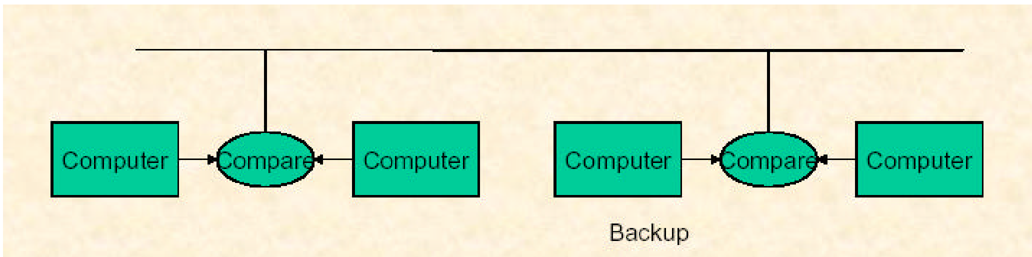
i) Replicate and Vote

Hardware -Implemented Triple Modular Redundancy (TMR)



ii) Duplicate and Compare

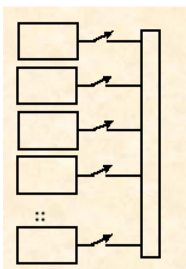
Duplex Self-Checking Approach (Stratus)



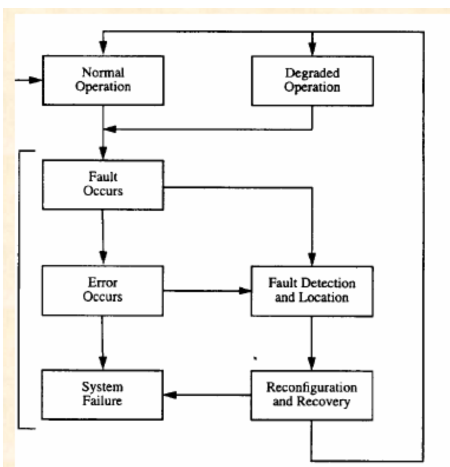
Computers run same programs in lockstep. If one pair internally disagrees, the other pair takes over immediately.

iii) Check and Replace (Standby Redundancy)

Active Hardware Redundancy – Detect error, remove fault, reconfigure, and recover state



basic operation of an active approach to fault tolerance



The Carter Self-checking Checker

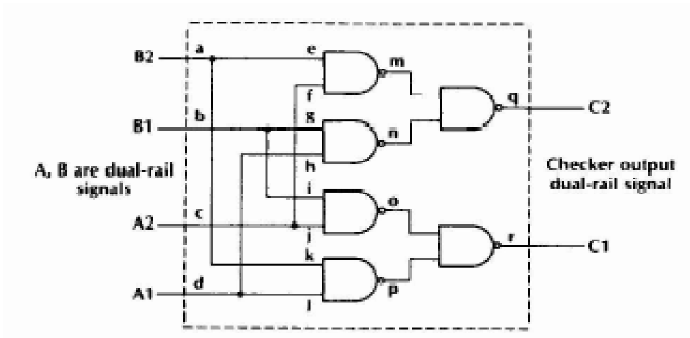
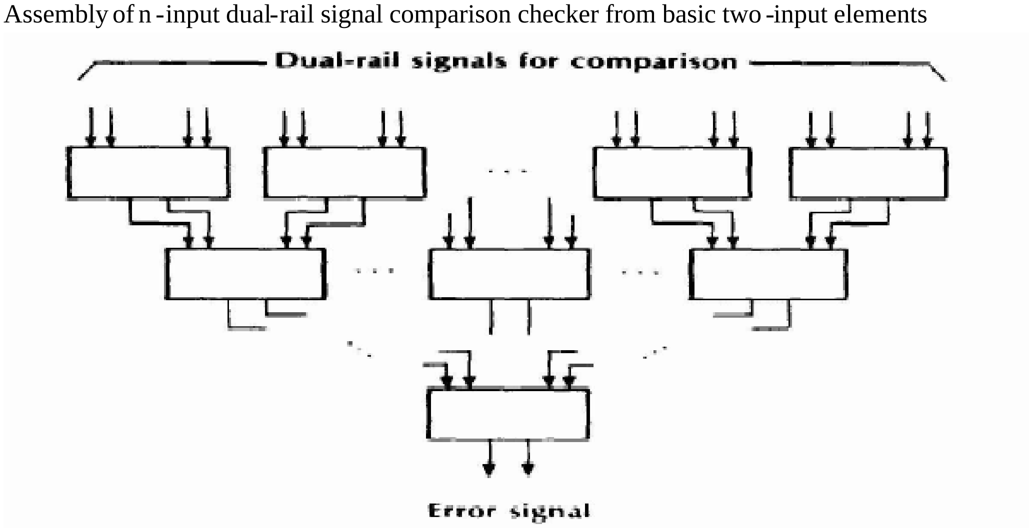


Table 3–12. TSC dual-rail comparator responses to stuck-at-faults.

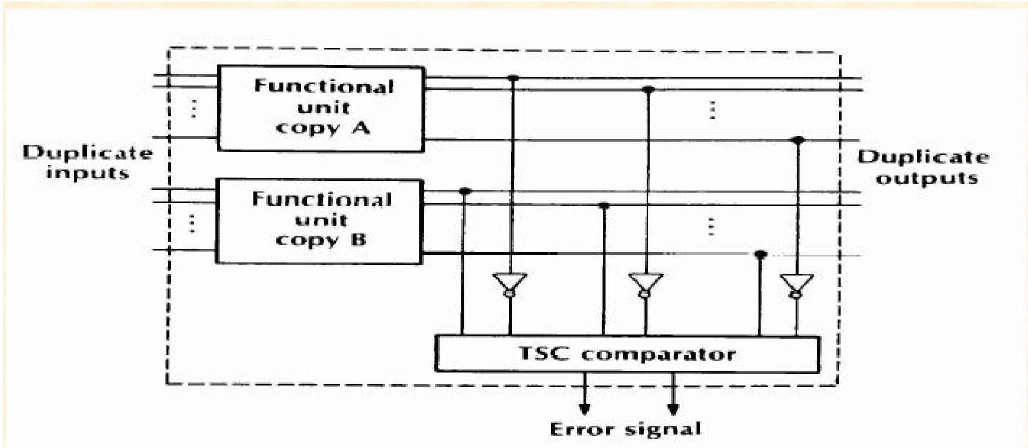
Inputs B2B1	Inputs A2A1	Normal Output	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r
			Outputs C2C1 Resulting from Single Stuck-at-1 Faults																	
01	01	10	11	10	11	10	10	10	10	10	10	11	11	10	10	00	10	10	10	11
01	10	01	11	01	01	11	11	01	01	11	01	01	01	01	01	01	00	01	11	01
10	01	01	01	11	11	01	01	11	11	01	01	01	01	01	01	01	01	00	11	01
10	10	10	10	11	10	11	10	10	10	10	11	10	10	11	00	10	10	10	10	11

Inputs B2B1	Inputs A2A1	Normal Output	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r
			Outputs C2C1 Resulting from Single Stuck-at-0 Faults																	
01	01	10	10	00	10	00	10	10	00	00	10	10	10	10	10	10	11	11	00	10
01	10	01	01	00	00	01	01	01	01	01	00	00	01	01	11	11	01	01	01	00
10	01	01	00	01	01	00	01	01	01	01	01	01	00	00	11	11	01	01	01	00
10	10	10	00	10	00	10	00	00	10	10	10	10	10	10	10	10	11	11	00	10

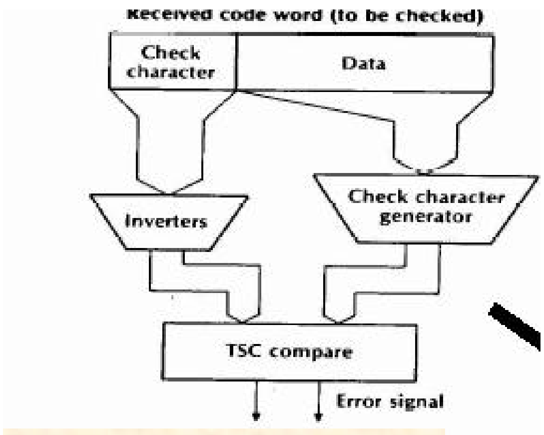
Assembly of n -input dual-rail signal comparison checker from basic two -input elements



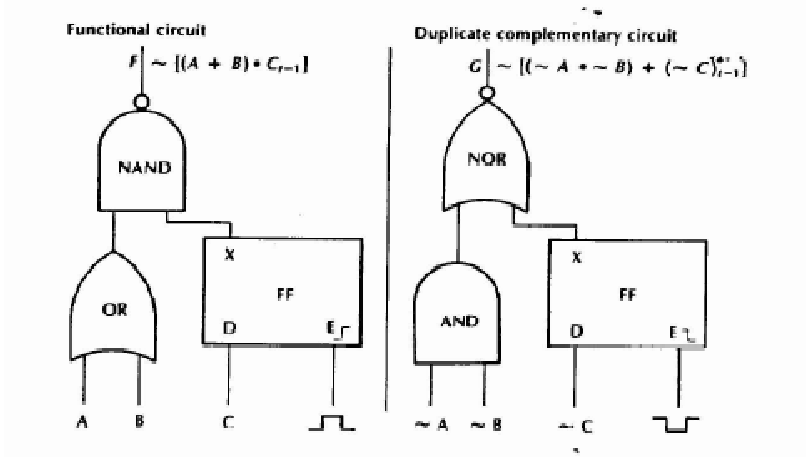
Self-checking circuit that duplicates and compares using a tree of Morphic And gates as below



Input protection



Using Complementary Logic to Detect Common Faults in a Duplicated System

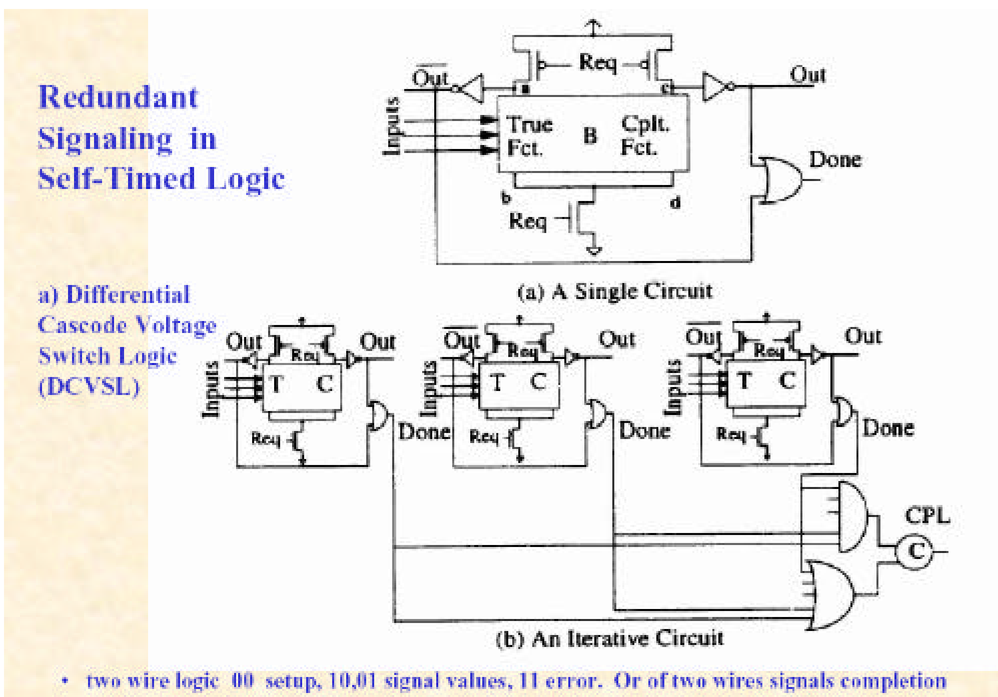


Truth Table

Inputs			Outputs	
A_t	B_t	C_t	F_t	G_t
L	L	L	H	L
L	L	H	H	L
L	H	L	H	L
L	H	H	L	H
H	L	L	H	L
H	L	H	L	H
H	H	L	H	L
H	H	H	L	H

Key

Symbol	Meaning
~	NOT
•	LOGICAL AND
+	LOGICAL INCLUSIVE OR
subscript t	Time period t
subscript $t-1$	Time period $t-1$
$E_{\_/}$	Enable on low to high transition of clock
$E_{\setminus\_}$	Enable on high to low transition of clock



Basic Modeling

R(t) = probability the system does not fail before time t, i.e., starting at t=0 the system provides acceptable service at least until time t.

If one was to create N identical systems, put them into service at t=0 and at time t group them into two subsets N_g (those still working) and N_f (those that have failed) then:

$N = N_g + N_f$, and in the limit as N goes to infinity

$$R(t) = \frac{N_g(t)}{N_g(t)+N_f(t)} = N_g(t)/N = 1 - N_f(t)/N$$ **and Unreliability** $Q(t) = 1 - R(t) = N_f(t)/N = 1 - N_g(t)/N$

$dR(t)/dt = d(1 - N_f(t)/N)dt = -(1/N)\, dN_f(t)/dt$ - this will decrease as a function of time because modules that hailed cannot fail again.

We define the hazard function, or hazard rate, or failure rate function as

$$z(t) = (1/N_0(t))\, dN_f(t)/dt = (1/N_0(t))\,(-N)\, dR(t)/dt = \frac{dR(t)/dt}{R(t)}$$ where $N_0(t)$ is the number of nodes remaining operational

This is the instantaneous rate (per module) that failures are occurring among the remaining working modules.

1

A non-redundant system with Constant Failure Rates

The Reliability function for Non-Redundant Systems

$dR(t)/dt = -z(t)\, R(t)$ if we assume that the failure rate is a constant λ then

$dR(t)/dt = -\lambda R(t)$ which has the solution

$$R(t) = e^{-\lambda t}$$

and if there are several independent components, all of which must work:

$R(t) = R1(t) * R2(t) * R3(3) .. * Rm(t)$ then $R(t) = e^{-\lambda 1 t} * e^{-\lambda 2 t} * e^{-\lambda 3 t} * .. * e^{-\lambda m t}$

or $R(t) = e^{-(\lambda 1 + \lambda 2 + \lambda 3 .. + \lambda m) t}$ You just add the failure rates of the internal components

The constant failure rate is commonly used for most reliability modeling.

It's a reasonable approximation to reality and it is mathematically tractable.

UCLA

Mean Time to Failure: MTTF

$$MTTF = \sum_{i=1}^{N} \frac{t_i}{N}$$

The *MTTF* can be calculated by finding the expected value of the time of failure. From probability theory, we know that the expected value of a random variable, *X*, is

$$E[X] = \int_{-\infty}^{\infty} x f(x)dx$$

where $f(x)$ is the probability density function. In reliability analysis we are interested in the expected value of the time of failure (MTTF), so

$$MTTF = \int_{-\infty}^{\infty} t f(t)dt$$

$$= -\int_0^{\infty} t \frac{dR(t)}{dt} dt = \left[-tR(t) + \int R(t)dt \right]_0^{\infty} = \int_0^{\infty} R(t)dt$$

MTBF is simply the integral of the reliability function from 0 to infinity, and for non-redundant systems:

$$\int_0^{\infty} e^{-\lambda t} = \frac{1}{\lambda}$$

1.1 Basic Concepts of Combinational Reliability Models

For statistically independent events P(A and B) = P(A) * P(B)

Given a system of n modules: M(1), M(2), M(3), ...M(n),

and a reliability for each module: R(1), R(2), R(3),...R(n)
where R(i) is the probability the ith module is OK

We perform an experiment to see which state the system is in.

There are 2^n possible outcomes:

W,W,W,......,W,W	P(S1)	=	R(1) * R(2) * ....* R(n-1) * R(n)
W,W,W,......,W,F	P(S2)	=	R(1) * R(2) * ....* R(n-1) * (1-R(n))
W,W,W,......,F ,W	P(S3)	=	R(1) * R(2) * ....* (1-R(n-1)) * R(n)
: : : : :	: : :		: : : : : :
F, F, F, ...,F, F	P(S2^n)	=	(1-R(1)) * (1-R(2))*,..*(1-R(n-1)) * (1-R(n))

To determine the reliability of a redundant system simply sum the probabilities of being in a working configuration.

If the system can tolerate two module failures, add the first three probabilities

P(S1-all work) + P(S2-all but one work) + P(S3-all but two work) etc.

The Concept of Coverage

Coverage "c" is defined as the conditional probability, given that a fault occurs, that the system will be able to recover from it.

It is a measure of the "goodness" of the fault-tolerance features of a system. We shall see that it is the most important (sensitive) parameter in determining the reliability of fault-tolerant systems.

Expanding the combinational models to include coverage:

Going back to the basic concept of listing outcomes and summing those that correspond to a working system:

W,W,W,.......,W,W $P(S1) = R(1) * R(2) * \ldots\ldots * R(n-1) * R(n)$
W,W,W,.......,W,F $P(S2) = R(1) * R(2) * \ldots\ldots * R(n-1) * (1-R(n))$
W,W,W,.......,F ,W $P(S3) = R(1) * R(2) * \ldots\ldots * (1-R(n-1)) * R(n)$
: : : : : : : : : : : : : :
F, F, F, ...,F, F $P(S2^n) = (1-R(1)) * (1-R(2))*,..*(1-R(n-1)) * (1-R(n))$

For all cases where an active computer fails there are now two cases -- one multiplied by c -- the probability of correct recovery and one multiplied by (1-c) the probability of incorrect recovery. Only the correctly recovered outcome can be counted.

This gets a bit complicated since failures of spares that are never called upon to replace active units have no coverage associated with their failure.

Consider a system with one active units and two spares: (The left unit starts as the active unit and spares are selected for replacement going from left to right.)

$R = p(WWW) + c*p(FWW) + p(WFW) + p(WWF) + p(WFF) + c*p(FWF) + c*c*p(FFW)]$

of course p(FFF) is excluded but what are the assumptions in including p(FFW)?

UCLA

MARKOV MODELS

CONSIDER OUR NON-REDUNDANT SYSTEM:

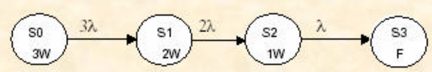
$R(t+dt) - R(t) = -R(t) * \lambda\, dt$

$\frac{dR(t)}{dt} = -\lambda * R(t) \Rightarrow R(t) = e^{-\lambda t}$

LET'S EXTEND THIS TO A SUBSYSTEM WITH 3 MODULES

S0: ALL THREE MODULES WORK
S1: ONE HAS FAILED, TWO WORK
S2: TWO HAVE FAILED, ONE WORKS
S3: ALL HAVE FAILED

Yields the following State Diagram



AND THE CORRESPONDING SET OF DIFFERENTIAL EQUATIONS

$$\begin{bmatrix} dP0 \\ dP1 \\ dP2 \\ dP3 \end{bmatrix} = \begin{bmatrix} -3\lambda & 0 & 0 & 0 \\ +3\lambda & -2\lambda & 0 & 0 \\ 0 & +2\lambda & -\lambda & 0 \\ 0 & 0 & +\lambda & 0 \end{bmatrix} \begin{bmatrix} P0 \\ P1 \\ P2 \\ P3 \end{bmatrix}$$

Start with P0,P1,P2,P3 =1,0,0,0