AVTMR 과 듀얼 듀플렉스 시스템 비교에 관한 연구

정회원 김 현 기*, 신 석 균*, 이 기 서*

A study on the comparision of AVTMR(All Voting Triple Modular Redundancy) and Dual-Duplex system

Hyun Ki Kim*, Suk Kuin Shin*, Key Seo Lee* *Regular Members*

요 약

본 논문에서는 결함의 영향을 받지 않고 동작할 수 있는 AVTMR(All Voting Triple Modular Redundancy) 시스템과 듀얼 듀플렉스(Dual-duplex) 시스템을 설계하고, 각 시스템의 평가를 통하여 RAMS(Reliability, Avaliability, Maintainability, Safety)를 비교하였다. AVTMR 시스템은 3중화된 보터(voter)를 사용하여 설계를 하였으며, 듀얼 듀플렉스 시스템은 비교기(comparator)를 이용하여 시스템을 설계하였다. 각 시스템은 버스 레벨로 데이터를 비교하도록 설계하였으며, 시스템 평가를 위해서 소자의 고장율은 MILSPEC-217F에 기반을 두고 RELEX6.0을 이용하였고, 마코브 모델(Markov model)을 이용하여 시스템의 RAMS를 평가하였다. 본 논문에서는 각 시스템을 MC68000을 기반으로 설계하여, 각각 시스템에 사용되는 비용 및 시스템이 어느 부분에서 선호될 수 있는 가를 RAMS 및 MTTF(Mean Time To Failure)를 통하여 선택할 수 있는 기반을 제시하도록 나타내고 있다.

이러한 AVTMR 이나 듀얼 듀플렉스 시스템(dual-duplex system)은 결함 허용 시스템(fault tolerant system)으로 인간의 생명과 직접적인 관련이 있는 고속철도 시스템이나 항공기 시스템에 적용될 수 있다.

ABSTRACT

In this paper, AVTMR(All Voting Triple Modular Redundancy) and dual-duplex system which are operated correctly in case of faults are compared through system design and evaluation.

AVTMR system is designed in triplicated voting technique, and dual-duplex is designed in comparator. The technique of bus level voting and comparator is applied to AVTMR and dual-duplex system. The failure rate of electronic components is calculated as MILSPEC-217F, and RAMS(Reliability, Avaliability, Maintainability) is evaluated by Markov model. In this paper, AVTMR and dual-duplex system is based on MC68000, and the preference of each system is proposed as RAMS and MTTF(Mean Time To Failure). AVTMR and dual-duplex system are fault-tolerant system, and so they can be applied to life critical systems - airplane and high speed railway system.

I. 서 론

산업사회의 발전에 따라 인간의 생명과 밀접한 시스템에서 높은 신뢰도(reliability)와 안전도(safety)를 요구하고, 결함(fault)을 허용(folerance)할 수 있는 시스템이 요구되어 왔다.

이러한 문제를 해결하기위해 다수결 보터(majority voter)를 이용하는 최초의 결함허용 시스템(fault tolerant system)이 아폴로의 유도 시스템에 적용이 되었으며, 대기 여분의 특성을 갖는 스탠바이 시스템(standby system)이 인간의 생명과 직접적으로 관련된 시스템인 항공기, 철도 시스템 등에 사용되어 왔다.

이러한 결함 허용 시스템(fault tolerant system)은

* 광운대학교 제어계측공학과
논문번호 : 00274-0720, 접수일자 : 2000년 7월 20일

발생하는 결함(fault)에 대해 영향을 받지 않고, 동작을 할 수 있는 특성을 가져하므로 고장(failure)에 대한 연구가 필요하게 되었으며, 결국 결함(fault), 오류(error), 고장(failure)의 관계가 시스템에서 밀접한 관계가 있다는 것을 알게 되었다. 즉, 결함(fault)이 오류(error)를 발생시키고, 오류(error)가 시스템의 고장(failure)을 발생시킨다는 것이다. 즉, 결함 허용 시스템(fault tolerant system)이란, 결함(fault)이 발생했을 때, 시스템이 오류(error)나 고장(failure)으로 전이되는 것을 방지하는 시스템이라 볼 수 있다.

결함(fault)을 방지하는 기법으로는 결함 회피(fault avoidance)와 결함 허용(fault tolerance)이 있다. 결함 회피(fault avoidance)는 전자소자의 질을 향상시켜서 고장율(failure rate)을 작게 하고, 시스템에 대한 완전한 테스트를 통한 시스템을 구성하는 방법으로, 실질적으로 구현하기 어려운 시스템이다. 왜냐하면, 시간이 지나감에 따라 전자소자는 질은 떨어지고, 예상치 못한 경우에 대해서 완벽한 테스트를 한다는 것은 어려운 일이기 때문이다. 결함 허용 시스템(fault tolerant system)은 시스템에서 결함(fault)이 발생하더라도 정상적인 동작이 계속 유지되는 시스템이다. 그래서 결함 허용 시스템(fault tolerant system)은 결함 회피 시스템(fault avoidance system)보다 비용이나 시스템을 개발하는데 있어서 많은 장점을 가지게 된다. 일반적으로 결함 허용 시스템(fault tolerant system)은 여분(redundancy)을 가지고 있는 구조로 되어있고, 결함이 발생을 하여도 정상적인 동작을 멈추지 않고 동작을 하는 특성을 가지게 된다. 이러한 기법으로는 하드웨어 여분(hardware redundancy), 소프트웨어 여분(software redundancy), 시간여분(time redundancy), 정보여분(information redundancy)의 구조가 있다. 하드웨어 결함허용 기법은 소프트웨어 결함 허용 시스템보다 시간이 중요시되는 시스템에 적용된다. 하드웨어 결함 허용 시스템은 버스 레벨(bus level)로 데이터를 비교하고, 보팅(voting)을 하는 특성을 가지는 반면, 소프트웨어 기법은 시스템 레벨에서 데이터를 처리하는 구조를 가지게 된다.

미국의 NASA에서는 상용항공기에 적용하기 위해 하드웨어를 이용한 결함허용 시스템인 FTMP (Fault Tolerant Multi-processor) 와 소프트웨어를 이용한 결함허용 시스템인 SIFT(Software Implemented Fault Tolerant)를 개발하였다.

하드웨어 기법으로 수동하드웨어 여분(passive hardware redundancy), 능동하드웨어 여분(active hardware redundancy), 하이브리드 하드웨어 여분(hybrid hardware redundancy) 구조가 있다. 수동 하드웨어 여분(passive hardware redundancy)은 결함을 검지하지 않고, 결함이 발생하였을 때 정상적인 동작을 하면서 결함 마스킹(fault masking)을 하는 특성을 가지며, 능동하드웨어 여분(active hardware redundancy)은 대기여분(standby sparing) 시스템의 동작 상태에 따라 콜드 스탠바이(cold standby), 핫 스탠바이(hot standby), 웜 스탠바이(warm standby)이 있고, 결함 검지(fault detection), 결함 한정(fault location), 결함 복구(fault recovery)의 특성을 가지게 된다. 하이브리드 여분(hybrid redundancy) 구조는 능동과 수동 구조를 다 가지고 있는 구조이다.

AVTMR 시스템은 3중화된 보터(voter)를 적용한 수동하드웨어 여분(passive hardware redundancy)의 구조를 가지고 있고, 결함이 발생했을 때는 결함 검지(fault detection)를 하는 특성을 가지고 있다. 하지만, 결함을 마스킹(masking)하는 시스템으로 설계되어서 결함에 따른 시스템의 동작의 변화는 없는 구조로 설계되어 있다.

듀얼 듀플렉스 시스템(dual-duplex system)은 능동하드웨어 여분(active hardware redundancy) 구조로 두 개의 CPU가 한 보드에서 동기 클럭으로 동작을 하면서 비교기에 의한 데이터를 비교하는 특성을 가지며, 결함 발생시 결함을 복구하는 시간이 가장 짧은 핫 스탠바이(hot standby) 특성을 가지고 있다.

이렇게 개발된 시스템의 비교평가를 위해서 각 시스템에 사용된 전자소자의 고장율(failure rate)을 MILSPEC-217F에 근거하여 RELEX 6.0을 이용하여 구하였고, 마코브 모델(Markov model)을 이용하여 개발된 AVTMR 과 듀얼 듀플렉스(dual-duplex) 시스템의 RAMS(Reliability, Avaliability, Maintainability and Safety)와 MTTF(Mean Time To Failure)을 평가, 분석하였다. 이러한 방법으로 개발된 결함허용 시스템은 높은 신뢰성과 안전성이 요구되는 항공기나 고속철도 시스템에 적용될 수 있다.

Ⅱ. AVTMR 시스템 설계

하드웨어 결함허용 기법에는 수동 하드웨어 여분(Passive Hardware Redundancy), 능동 하드웨어 여분(active hardware redundancy), 하이브리드 하드웨

어 여분(hybrid hardware redundancy)이 있다. 본 논문에서는 3중화된 보터를 이용한 수동하드웨어 여분을 이용한 시스템을 개발하였다. 수동하드웨어 여분 구조는 오류를 일으키는 결함을 없애거나 결함의 발생을 은폐하기 위한 결함 방지(fault masking)의 개념을 사용한다. 이 하드웨어의 구조는 보터(voter)를 이용해서 결함 발생 시에 오류가 발생하는 시스템의 부분에 대해서 어떠한 복구 없이 결함 허용을 구성하는 것이다.

보터(voter)는 입력되는 데이터 중 2개 이상의 같은 값을 가지는 데이타를 출력하게 된다. 그러므로, 한 개의 결함을 가지는 입력에 대해서 이 다수결 보터를 통해서 결함이 마스킹(masking)되는 구조를 가지고 있다. 본 논문에서는 이러한 다수결 보터를 CPU 보드에서 3중화하여 한 개의 보터가 고장이 발생을 해도 시스템은 정상적인 동작을 할 수 있는 AVTMR 시스템을 설계하였다. 설계방식은 3개의 MC68000 CPU를 기반으로 하여 설계하였으며, 모든 CPU의 버스는 보터를 통하여 입/출력되는 구조를 가지고 있다. 양방향버스의 설계 시에는 74244를 이용한 리드와 라이트시의 방향성 보터를 설계하였다. 이렇게 구성된 AVTMR시스템은 한 개의 클락을 이용해서 동기를 맞추어 동작을 하도록 구현하였으며, 보팅 시간을 결정짓는 동기화 요소는 MC68000의 제어신호인 /DTACK 신호를 이용하여 보팅을 하는 시간의 시점을 결정지었다.

설계된 AVTMR 시스템은 MC68000을 기반으로 설계되었으며, 보터의 설계는 EPLD인 ALTERA사의 EPM7128LC84를 사용하여 설계하였다. 개발된 CPU 보드의 사진이 그림 1에 나타나 있다. 그림 1의 CPU 보드가 그림 2과 같은 구조로 동작을 한다.

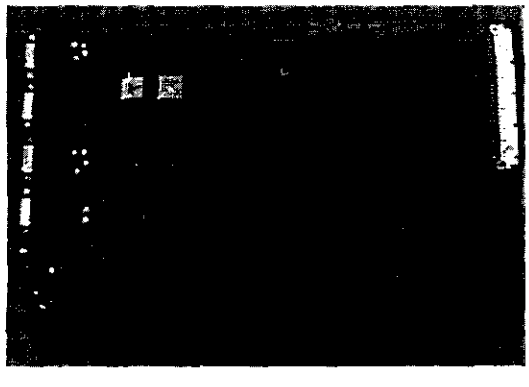


그림 1. 개발된 CPU 보드

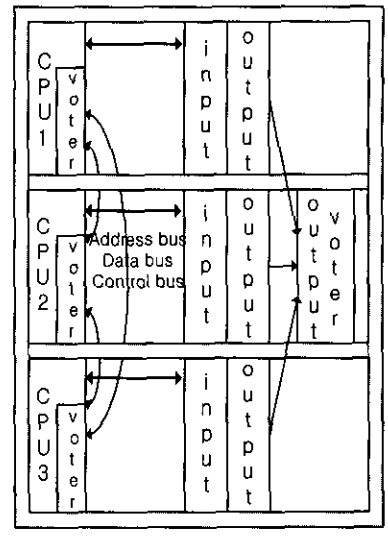


그림 2. AVTMR 시스템 구성도

이 3개의 CPU 보드는 공통 클락으로 동작을 하고, 각각의 보드는 두 개의 다른 CPU 보드로부터 어드레스 버스, 데이터 버스, 제어 버스를 받아서 보팅이 되도록 구성이 되었다. 보팅이 되는 제어신호는 /DTACK 신호를 CPU의 데이터가 가장 안정한 시점에서 입/출력의 데이터가 비교되도록 설계를 하였다. 이 보드의 리셋 회로는 TL7705를 이용하여 일정 시간동안 초기화를 시켜주는 회로를 구성하였다. 독립적인 입/출력 보드와의 연계를 위해서 VME버스 구조를 가지는 인터페이스 로직을 설계하였다.

입력보드(Input board)의 경우에는 동기 클락으로 동작하는 3개의 CPU가 동시에 같은 입력을 외부에서 받도록 구성된다. 즉, 같은 데이터 입력이 3개의 입력 보드의 같은 포트에 연결이 되어 있다. 이 입력보드에서는 VME버스를 이용한 구조를 채택하였으며, 8255와 ALTERA, 74244,74245를 이용한 입력 회로를 구성하였다. 출력 보드도 마찬가지로 입력 보드와 같은 소자를 사용하였고, 각각의 CPU가 3개의 보드로 출력을 하도록 설계가 되어 있으므로, 최종출력에는 마찬가지로 보터를 이용하여 한 개로 출력이 되도록 설계하였다.

Ⅲ. Dual-duplex 시스템 설계

설계된 듀얼 듀플렉스 시스템(dual-duplex system)은 능동 하드웨어 구조로서 결함이 있는 하드웨어를 검출하여 대기 여분 시스템으로 전환하는 방법

이다. 이러한 구조로 두개의 모듈이 같은 동작을 하여 두개의 출력을 비교하여 데이타가 같을 경우 다음 동작을 하고 틀릴 경우에는 비교기(comparator)의 결함 검지(fault detection)회로에 의해서 시스템을 정지시키거나 다른 대기여분(standby sparing) 하드웨어로 전환을 한다. 즉, 이 시스템은 모든 모듈이 함께 동작을 하는 시스템이다. 따라서, 모든 모듈이 전력을 소비하는 단점을 갖고 있으나, 시스템에 결함이 발생했을 때 시스템을 재구성하는데 시간이 적게 소비되는 장점을 갖는다. 우리가 구성하는 듀얼 듀플렉스 시스템(dual duplex system)은 시간이 중요시 되는 시스템에 적용되기 위해서 고장이 발생했을 때 대기 여분이 곧바로 사용될 수 있는 구조를 채택했다. 즉, 두개의 듀얼 보드(dual board)중 한개의 보드에 입력되는 데이타에 따라 데이타를 처리하고, 다른 대기 여분 구조는 입력되는 데이타를 가지고 동작을 하면서 시스템의 결함 검지(fault detection) 회로의 입력을 기다리는 구조로 구성된다. 설계된 시스템은 두개의 CPU가 한 보드에서 동기 클락(Synchronous clock)으로 동작을 하고, 버스 레벨로 어드레스 버스(address bus), 데이터 버스(data bus), 제어 버스(ontrol bus)를 비교하면서, 데이타가 틀릴 경우 대기하고 있던 다른 보드로 전환을 한다. 우선 설계된 듀얼 CPU보드의 사진은 그림3과 같다. 그림 3에서 보면, 두개의 MC68000을 리셋 안정화 소자인 TL7705를 이용하여 동기 리셋 회로를 구성하였고, 클락 회로는 오실레이터를 이용하여 동기 클락으로 동작을 하고, 비교기에서는 제어 신호(control bus)와 데이타 버스(data bus), 어드레스 버스(address bus)가 데이타가 가장 안정한 시점인 DTACK 신호가 끝나는 시점에서 비교를 하도록 회로를 구성하였다. 비교기는 ALTERA를 이용하여 XOR 로직을 이용하여 설계하였다.

그러므로, 각각의 비교기에서 데이타에 이상이 발생할 경우에는 스위칭 로직(Switching logic)에 의해서 대기 여분(Standby sparing)으로 스위칭하는 특성을 가지고 있다. CPU보드의 확장성을 위해 VME 버스에서도 동작을 할 수 있도록 하드웨어를 구성하였다. 이러한 듀얼 구조의 입/출력 보드도 또한 듀얼 구조를 가지게 된다. 이 입/출력 구조는 그림 4에 나타나 있다. 입/출력은 전부 노이즈에 강한 광소자를 사용하여 설계가 되었다. 입력의 경우는 듀얼 보드의 각 CPU가 같은 데이터가 입력이 되어야 하므로, 입력의 결선이 각각의 듀얼 입력 보드에 연결이 된다. 입력과 마찬가지로 출력도 광소자를 이용하였으며, 결함이 발생하지 않았을 때, 광소자에 전원을 공급해 주고, 두 개의 출력이 한 개의 출력이 되도록 결선을 하여 회로를 구성하였다. 만약, 결함이 발생하였을 경우에는 광소자의 전원 공급이 계전기에 의해서 차단된다.

즉, 두 개의 데이터가 일치하지 않을 경우에는 1이 출력되도록 구성되어 있다. 일시적인 결함에 대해서 동작의 안정성을 확보하기 위해 카운터를 이용하여 결함이 3번이상 발생을 하였을 경우에 결함이 검출되는 래치카운터(latch counter) 회로가 구성되었다.

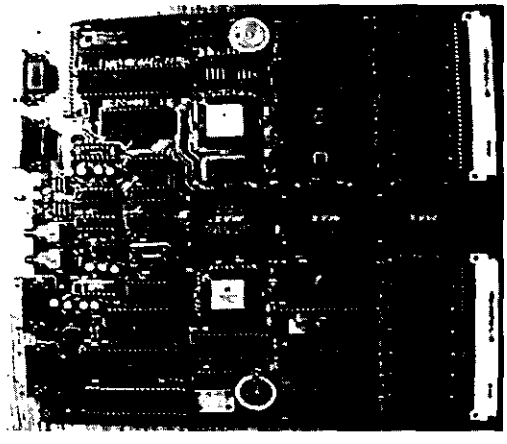


그림 3. 듀얼 듀플렉스 CPU 보드

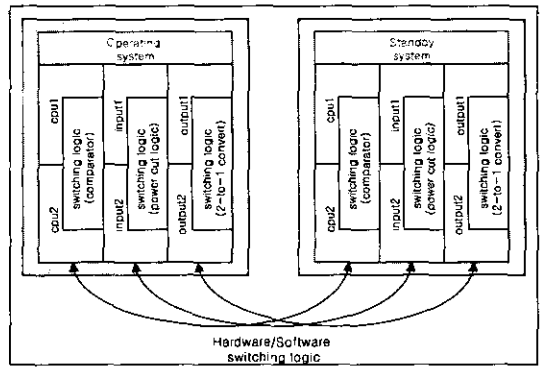


그림 4. 듀얼 듀플렉스 시스템 구성도

이 카운터의 출력에 의해서 계전기에 의해 출력되는 광소자의 전원을 차단하고, 대기 중인 시스템에 사용 권한을 넘기는 구조로 구성되어 있다.

대기 중인 시스템은 8255로 주기적으로 전환 입력을 검사하여 고장이 발생하였을 경우에 시스템의

동작 권한을 가지게 된다. 즉, 대기 중인 시스템은 항상 입력 데이타를 받고, 처리하면서 전환을 기다리게 된다.

Ⅳ. RAMS 평가

1. 고장률 계산

고장률(Failure rate)은 모든 하드웨어 시스템 평가, 즉 구성될 시스템의 신뢰도(Reliability), 가용도(Avaliability)와 MTTF(Mean Time to Failure)를 평가하는데 가장 중요한 요소로서 전자소자 또는 시스템이 동작한 시간의 역수로서 식(1)과 같이 나타낼 수 있다.

$$\lambda = \frac{1}{Operating Time} \quad (\lambda: 고장률) \tag{1}$$

본 논문에서 설계된 시스템의 소자의 고장율은 표1과 같이 구해진다. 표 1에서는 전자소자의 종류에 따라서 고장율1은 일반적인 상업용 전자소자의 고장율이고, 고장율 2는 MILSPEC 중 가장 작은 고장율을 가지는 전자소자의 고장율을 나타낸다. 이러한 전자소자의 고장율은 MIL-HDBK-217F에 근거하여 계산되었다. 고장율은 RELEX 6.0을 이용하여 계산하였다. 표 1에 나타난 전자소자의 개수는

표 1. 각 전자소자의 고장율 및 사용된 소자수

사용된 소자	고장율1 (10^{-6}h)	고장율2 (10^{-6}h)	SS (개수)	AVTMR (개수)	DS (개수)
MC68000	1.329899	0.033247	1	3	2
27C010	0.086332	0.002158	2	6	4
681000	0.139243	0.003481	4	12	8
Z8530	0.242960	0.006074	1	3	2
EPM7128LC84	0.219911	0.005498	4	22	5
74LS244	0.058272	0.001457	12	40	24
74LS245	0.058272	0.001457	6	18	12
74LS04	0.044916	0.001123	1	3	2
74LS05	0.044916	0.001123	1	3	6
74LS07	0.047508	0.001188	1	3	6
TL7705	1.095121	0.027378	1	3	1
8255	0.126798	0.003170	2	6	6
oscillator	0.021441	0.000536	2	2	2
저 항	0.002945	0.000029	164	340	328
콘덴서	0.005131	0.000051	84	204	172
스위치	0.200783	0.100391	2	6	2
max232	0.033405	0.000835	1	3	2
optoisolator	0.016047	0.072946	24	72	48
다이오드	0.010425	0.001327	26	103	50
계전기	0.141030	0.072946	N/A	N/A	2

(SS : Single System, AVTMR : All Voting Triple Modular Redundancy, DS:Dual System)

CPU보드와 입/출력 보드에 사용된 총 소자의 개수를 나타내고 있다. 표 1에서 나타내듯이 AVTMR 시스템이 SS 보다 3배 정도의 소자가 더 사용되고, 듀얼 듀플렉스 시스템은 듀얼 시스템(Dual system)이 두 개 필요하므로 대략 4배 정도의 소자가 더 필요하다는 것을 알 수 있다. 표1의 전자소자의 개수는 CPU 보드 및 입/출력 보드에 사용되는 전자소자의 개수를 나타내고 있다. AVTMR 시스템의 고장율은 지상 시스템으로 설정하여 계산하였다.

2. 평가 함수

2.1.신뢰도(reliability)

시스템과 전자 소자의 신뢰도는 시간 t_0에서 올바르게 동작하고 있을 때, 시간 간격 $[t_0, t]$에서 올바르게 동작을 하는 조건적인 확률이다. 그러면, N 개의 똑같은 요소를 시간 t_0에서 시작하여 N 개의 시스템을 검사한다고 가정할 때, $N_f(t)$는 시간 t에서 고장나는 시스템 개수이고, $N_o(t)$는 시간 t 에서 올바르게 동작하고 있는 시스템의 개수이다. 시스템의 신뢰도는 식(2)와 같다.

$$R(t) = \frac{N_o(t)}{N_o(t) + N_f(t)} = e^{-\lambda t} \quad (\lambda: 고장율) \tag{2}$$

2.2. 가용도(Availability)

시스템의 가용도 $A(t)$는 시스템이 시간 t의 순간에 어떠한 태스크를 수행할 수 있는 확률로서 정의된다. 즉, 가용도는 시스템이 바르게 동작되는 시간의 비율로 볼 수 있다. 그러므로, 식(3)와 같이 시스템이 동작하는 시간과 수리하는 시간의 비율로서 표현될 수 있다.

$$A(t_{current}) = \frac{t_{op}}{t_{op} + t_{repair}} \tag{3}$$

2.3.유지보수도(Maintainability)

유지 보수도는 고장난 시스템이 확정된 시간내에 회복될 수 있는 확률을 말한다. 유지 보수율 $M(t)$는 시스템이 시간 t 이하의 시간에 수리될 확률을 이야기한다. 이 유지 보수율은 수리율을 이용해서 구할 수 있다.

$$M(t) = 1 - e^{-\mu t} \quad (\mu: 수리율) \tag{4}$$

2.4.안전도(safety)

본 논문에서는 시스템의 안전도를 평가하기 위해서 마코브 모델을 이용해서 시스템의 상태를 3가지로 즉, 시스템이 정상적으로 동작하는 경우, 고장이 발생했을 때 안전측으로 동작하는 경우와 고장이 발생했을 때 불안전하게 동작하는 경우로 나누었다. 여기서 안전도의 의미는 시스템이 정상적으로 동작을 하는 경우와 안전하게 고장이 발생한 경우의 확률적인 값으로 나타낸다.[8] 안전도(safety)는 시스템의 응용분야에 따라 평가되는 것이지만 다중화된 시스템의 감지되지 못한 고장이나 오류가 제어대상을 불안전한 모드로 유도할 수 있다고 가정할 때 결함이 정확한 것이며 결함 검지, 회복 등 일련의 결함 수용능력이 안전도 제고의 중요한 요소로 사용될 수 있다. 본 논문에서는 안전도를 평가하기 위해서 결함 수용 능력을 계산하였다. 실질적으로 결함을 입력하여, 즉, 영구결함(permanent fault)과 일시적인 결함(transient fault)을 주입(fault injection)하여 결함 검출 수용능력(fault detection coverage)을 계산하였다.

2.5. MTTF(Mean Time To Failure)

MTTF는 시스템의 수명을 나타내는 요소로 고장이 나는 시간 간격을 나타낸다. 이 MTTF는 시스템의 확률적인 고장율로 시스템의 질을 평가하는데 중요한 계수로 사용된다. 시스템이 시간 $t=0$ 에서 동작을 시작해서 시스템의 고장이 나기 전까지의 시간을 말한다. 이 MTTF는 고장 시간의 기대값으로 표현되는데, 확률적으로 불규칙한 X에 대한 기대값의 식은 결국 신뢰도의 함수를 시간에 대한 무한대의 적분으로 표현될 수 있다.

$$MTTF = \int_0^\infty R(t)dt \tag{5}$$

2.6. MTTR(Mean Time To Repair)

MTTR은 시스템을 수리하기 위해 요구된 평균시간 이다. 즉, N 개의 고장을 수리하기 위해 t_i의 시간이 필요하다면, MTTR은 다음과 같이 나타낸다.

$$MTTR = \frac{\sum_{i=0}^{N} t_i}{N} \tag{6}$$

V. 시스템 모델링

본 논문에서는 시스템을 평가하는 데 있어서 마코브 모델링(Markov modeling) 기법을 이용한다. 마코브 모델(Markov model)은 시스템이 가질 수 있는 상태에 따라 표현될 수 있는 확률적인 시스템 평가 모델을 제공한다. 즉, 설계된 시스템의 신뢰도 표현을 위해 각각의 상태는 동작이 가능한 모듈과 고장 모듈로 표현된다. 시스템에서 각 모듈은 동작 상태와 결함 상태의 한 조건이 된다. 이러한 상태의 변화를 상태 전이(State transition)라고 한다. 이러한 상태 전이에 따라 이산 시간모델로 되는 전이율로 시스템 고장율에 따른 확률을 할당하여 시간의 변화에 따른 식을 유도하여 시스템을 모델링한다. 이렇게 모델링된 시스템은 각각 전자소자의 고장율에 따른 시스템의 RAMS(Reliability, Avaliability, Maintainability and Safety)가 구해진다.

1. 단일 시스템 모델링

단일 시스템은 가장 기본적인 구조로 그림5와 같이 설계될 수 있다. CPU 보드, 입/출력 보드로 구성되어 있다. 그림 6는 시스템의 마코브 모델을 구성하고 있다. λ는 전체 시스템의 고장율이고, μ는 시스템의 수리율이다. 이 시스템에 대한 상태 방정식을 이끌어 보면, 식(7)과 같이 된다.

그림 5. 단일 시스템 구조

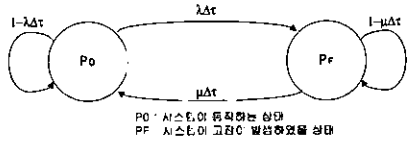


그림 6. 단일 시스템의 마코브 모델

$$\begin{bmatrix} P_O(t+1) \\ P_F(t+1) \end{bmatrix} = \begin{bmatrix} -\lambda & \mu \\ \lambda & -\mu \end{bmatrix} \begin{bmatrix} P_O(t) \\ P_F(t) \end{bmatrix} \tag{7}$$

2.AVTMR 시스템 모델링

제안된 AVTMR 시스템의 구조가 그림 6에 나타나 있다. 3개의 CPU 보드 B1, B2, B3가 데이터 버스, 어드레스 버스, 제어 버스를 받아서 보팅을 하는 구조를 가지고 있다. CPU보드의 보터는 3중화 되어있기 때문에 한 개의 보터가 고장이 발생을 하여도 정상적인 동작을 하는 구조를 가지고 있다. AVTMR 시스템의 RAMS를 평가하기 위하여 그림

6의 시스템에 대한 마코브 모델을 그림7과 같이 구성하였다.

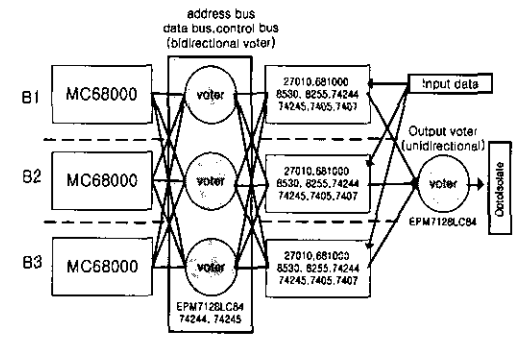


그림 7. AVTMR 시스템의 블럭도

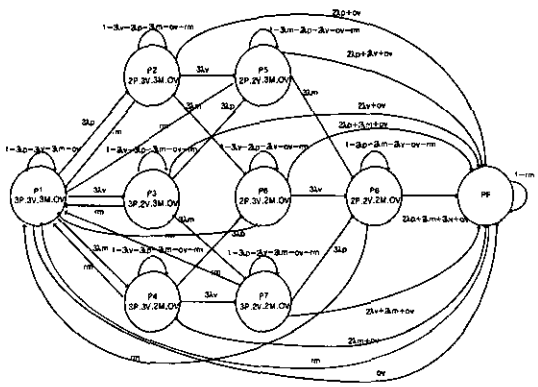


그림 8. AVTMR 시스템의 마코브 모델

그림 8에서 첨자 P는 프로세서를 의미하며, 3P는 3개의 CPU가 정상적인 동작을 하는 것을 나타내고, 상태 변화에 의해서 2P가 되는 경우는 프로세서 1개가 고장이 나는 경우를 나타낸다. 3V는 3중화 보터를 의미하고, 2V는 3중화 보터 중 한 개가 고장이 나는 경우를 나타낸다. 3M은 나머지 소자의 정상적인 상태를 의미하고, 2M은 한 개의 고장난 상태를 가지는 경우를 나타낸다. Ov는 출력 보터와 공통클럭으로 구성된다. 그리고, 각 상태에서 시스템이 고장이 발생을 하였을 때는 같은 수리율을 가지것으로 시스템의 마코브 모델을 구성하였다.

즉, 그림에서는 각상태에서 3개의 시스템이 정상동작하는 상태로의 같은 수리율이 전이가 된다. 그림의 복잡성 때문에 Pf의 상태에서의 수리율의 전이만 나타내고, 나머지 7개의 상태에서 각각 Po 의 상태로 수리율의 전이가 방정식으로 표현된다는 것을 그림 8에서 알 수가 있다. 이 마코브 모델의 방정식은 식(11) 같다.

$$\begin{bmatrix} p_1(t+1) \\ p_2(t+1) \\ \cdot \\ \cdot \\ p_8(t+1) \\ p_F(t+1) \end{bmatrix} = \begin{bmatrix} s_{11} & r_m & r_m & . & . & r_m & r_m \\ s_{21} & s_{22} & 0 & . & . & 0 & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & 0 & . & . & s_{88} & s_{89} \\ s_{91} & s_{92} & s_{93} & . & . & s_{98} & s_{93} \end{bmatrix} \begin{bmatrix} p_1(t) \\ p_2(t) \\ \cdot \\ \cdot \\ p_8(t) \\ p_F(t) \end{bmatrix} \quad (11)$$

3. 듀얼 듀플렉스 시스템 모델링

구현된 듀얼 듀플렉스(dual-duplex) 시스템 구조는 그림 9와 같다. 이 구조는 두 개의 듀얼 CPU보드를 핫 스탠바이(hot standby)로 구성한 것이다. 즉, 동작하고 있는 시스템에서 결함이 검출되면, 계전기를 다운 시켜서 출력을 차단하고, 대기 중인 시스템으로 전환하는 특성을 가지도록 설계되어 있다. 이 시스템의 마코브 모델은 그림 10에 나타나 있다. 한 개의 대기 여분 구조가 있으므로, 대기 전환 상태가 존재하게 된다.

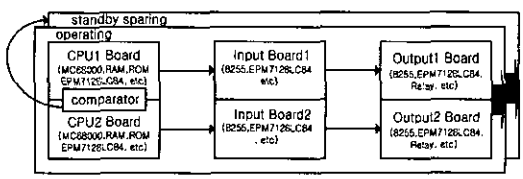


그림 9. 듀얼 듀플렉스 시스템 구성도

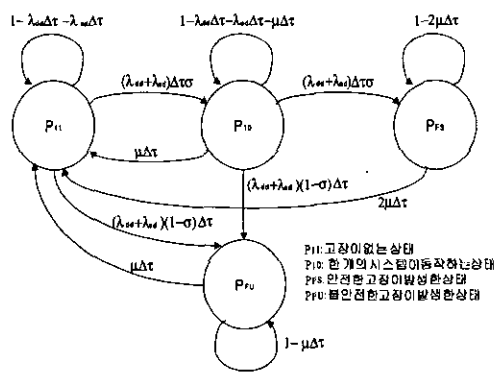


그림 10. 듀얼 듀플렉스 시스템 마코브 모델

이 시스템의 방정식은 식(9)와 같다. 여기서, λ_{dd}는 듀얼 시스템의 고장율, λ_{cd}는 결함 검출로직의 고장율, μ는 수리율이고, σ는 결함 수용능력이다. 듀얼 시스템과 마찬가지방법으로 결함 수용능력을 계산하였다. 영구결함은 100%의 확률을 가졌고, 일시적인 결함은 64개중 61개의 검출을 하는 특성을

나타내었다. 여기서 사용된 결함 수용능력은 3번을 테스트하여, 3개의 값을 평균한 데이터로 결함 수용능력을 나타내었다. 그러므로, 결함 수용능력은 0.9765625을 가진다.

$$\begin{bmatrix} P_{11}(t+1) \\ P_{10}(t+1) \\ P_{FS}(t+1) \\ P_{FU}(t+1) \end{bmatrix} =$$

$$\begin{bmatrix} -\lambda_{dd}-\lambda_{ed} & \mu & 2\mu & \mu \\ (\lambda_{dd}+\lambda_{ed})\sigma & -\lambda_{dd}-\lambda_{ed}-\mu & 0 & 0 \\ 0 & (\lambda_{dd}+\lambda_{ed})\sigma & -2\mu & 0 \\ (\lambda_{dd}+\lambda_{ed})(1-\sigma) & (\lambda_{dd}+\lambda_{ed})(1-\sigma) & 0 & -\mu \end{bmatrix}$$

$$\times \begin{bmatrix} P_{11}(t) \\ P_{10}(t) \\ P_{FS}(t) \\ P_{FU}(t) \end{bmatrix} \quad (9)$$

Ⅵ. 시뮬레이션

6.1. 신뢰도(Reliability)

그림 11과 그림 12는 단일 시스템(SS), AVTMR 시스템, 듀얼 듀플렉스 시스템(DD)의 신뢰도를 나타내고 있다. m(military component)은 군사용 소자를 , c(Commercial component)는 상업용 소자를 의미한다. 그림11, 12에 나타나 있는 바와 같이 상업용 소자를 사용한 경우보다는 군사용 소자를 사용한 경우가 더 좋은 신뢰도를 나타내고 있는 것을 알 수 있다. 우선, 그림 11은 듀얼듀플렉스 시스템이 결함 수용율(fault coverage)가 0 인 경우에 대해서 시뮬레이션 한 경우이다. 이때는 듀얼 듀플렉스 시스템이 단일 시스템이나 AVTMR 시스템보다 상당한 시간동안 좋지 않은 신뢰도를 가진다는 것을 알수 있다. 그리고, AVTMR_c 시스템은 120000시간까지 단일 시스템보다 좋은 신뢰도를 나타내고, AVTMR_m 시스템은 600000시간까지 단일 시스템 보다 좋은 신뢰도를 가진다는 것을 알 수 있다.

그림 12는 랜덤한 결함을 듀얼 듀플렉스 시스템에 주입하여 구한 결함 수용율(fault coverage)인 0.96875인 시스템의 신뢰도를 나타내고 있다. 이 것은 그림 12와는 다르게 듀얼 듀플렉스 시스템이 상당한 시간동안 즉, DD_c는 300000시간까지, DD_m은 1000000시간 이상 가장 좋은 신뢰도를 갖는 다는 것을 알 수 있다. 즉, 시스템의 결함 수용율(fault coverage)이 높을수록 시스템의 신뢰도에 우수하다는 것을 알 수 있다.

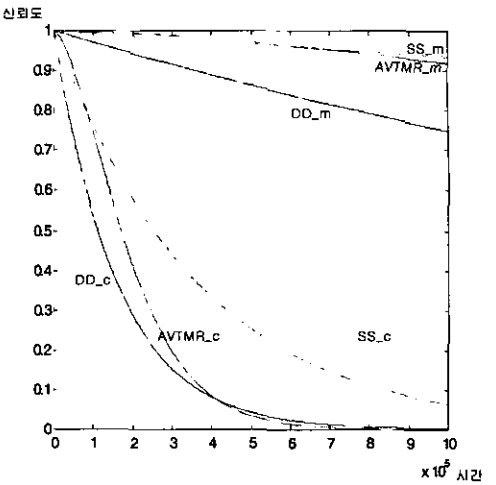


그림 11. 각 시스템의 신뢰도 1

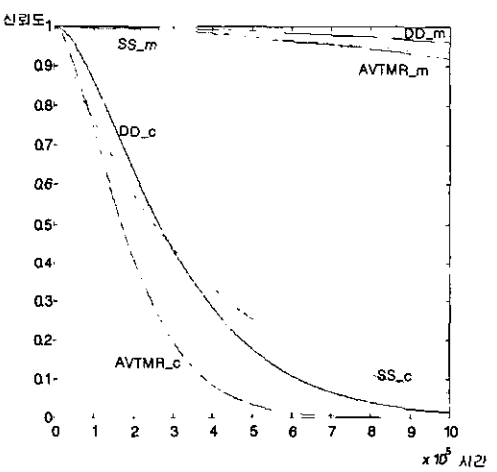


그림 12. 각 시스템의 신뢰도 2

6.2. 가용도(Availability)

그림 13과 그림 14는 각 시스템의 가용도를 나타내고 있다. 가용도도 마찬가지로 결함 수용율에 따라 다른 결과를 나타낸다는 것을 알 수 있다. 결함 수용율이 작으면 설계된 시스템 구조에서는 듀얼 듀플렉스 시스템이 가장 좋지 않은 시스템 시스템의 가용도를 가지게 되고, 단일 시스템, AVTMR 시스템의 순으로 나타나게 된다. 그러나, 설계된 듀얼 듀플렉스 시스템의 결함 수용율 0.96875를 적용하였을 경우에는 듀얼 듀플렉스 시스템이 가장 좋은 가용도를 나타내고, AVTMR 시스템, 단일 시스템의 순으로 나타난다는 것을 알 수 있다. 하여튼, 결함 허용 특성을 갖도록 시스템이 단일 시스템보다 더 좋은 가용도를 가진다는 것을 알 수 있다.

즉, 결함 허용 시스템의 설계목적과 일치하는 것을 시뮬레이션을 통하여 알 수 있다.

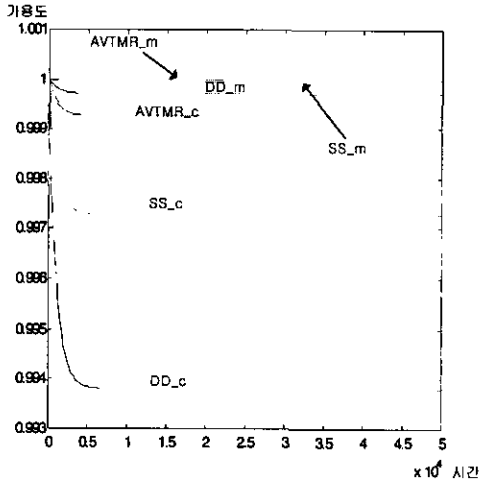


그림 13. 각 시스템의 가용도 1

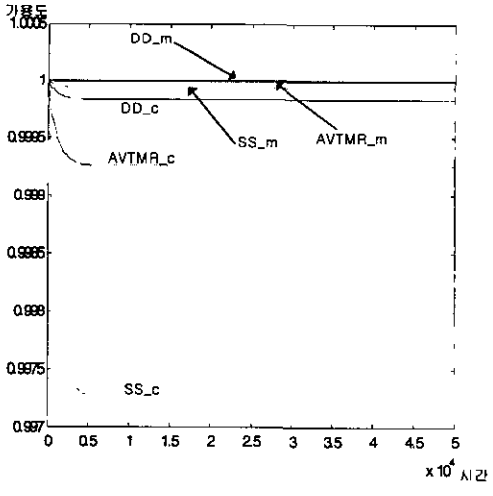


그림 14. 각 시스템의 가용도 2

6.3. 유지보수도(Maintainability)

그림 15는 시스템의 유지 보수도를 나타내고 있다. 유지 보수도는 각 시스템의 수리율에 따라 결정된다는 것을 알 수 있다. 즉, 수리율 m이 작으면, 좋지 않은 유지 보수도를 가진다는 것을 알 수 있다. 즉, 시스템의 가용도를 높이기 위해서는 유지 보수도가 높아야 한다는 것을 그림 16으로부터 알 수 있다.

6.4. 안전도(Safety)

그림 16과 17은 시스템의 안전도를 나타내고 있

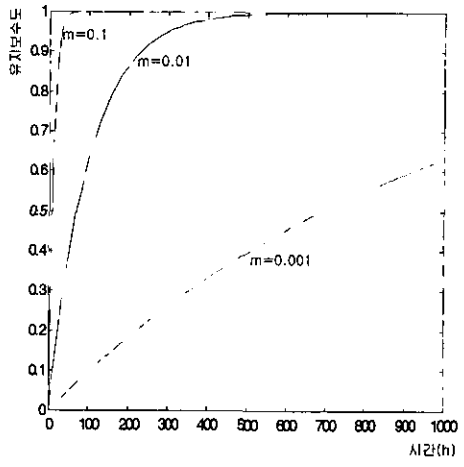


그림 15. 시스템의 유지 보수율

다. 마찬가지로 듀얼 듀플렉스 시스템의 결함 수용율에 따라서 다른 시스템의 안전도를 나타내고 있다는 것을 알 수 있다. 그림 17은 결함 수용율이 0인경우의 안전도를 나타내고 있다. 단일 시스템과 AVTMR시스템은 결함 수용율이 없으므로, 마코브 모델에서 신뢰도와 안전도가 같은 값으로 표현이 된다. 그러나, 듀얼 듀플렉스 시스템은 결함 검지 및 시스템 전환이라는 특성을 가지기 때문에 고장 안전상태가 더 존재하게 된다. 하지만, 결함 수용율이 0일 경우에는 고장 안전상태가 의미가 없어진다. 이때 시스템의 안전도는 상당한 시간동안 가장 좋지 않은 안전도를 가지게 된다. 처음에는 AVTMR이 가장 좋은 안전도를 가지다가 일정시간후에 단일 시스템이 가장 좋은 안전도를 가진다는 것을 알 수 있다.

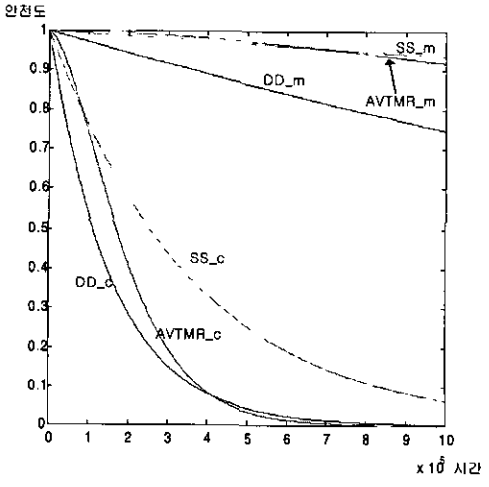


그림 16. 각 시스템의 안전도 1

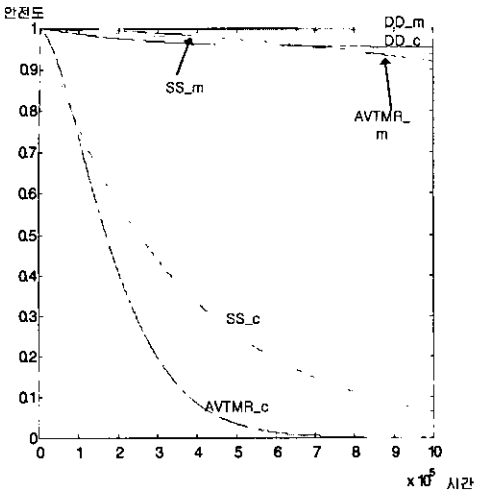


그림 17. 각 시스템의 안전도 2

결함 수용율이 적용된 그림 17의 경우는 듀얼 듀플렉스 시스템이 가장 우수한 안전도를 가진다는 것을 알 수 있다. 이것은 듀얼 듀플렉스 시스템을 설계하는 목적에 해당한다. 시뮬레이션에 나와 있는 것 처럼 AVTMR, 단일 시스템보다 월등한 안전도를 가진다는 것을 알 수 있다.

Ⅶ. 결 론

본 논문에서는 개발된 단일 시스템, AVTMR 시스템, 듀얼 듀플렉스 시스템의 RAMS를 분석 및 비교하였다. 적용되는 환경에 따른 적당한 적용을 하기 위하여 비교 분석하였다. 전체적으로 볼 때 듀얼 듀플렉스 시스템이 우수한 것으로 나타난다. 하지만, 듀얼 듀플렉스 시스템은 상당한 비용, 시간이 드는 단점이 존재한다. 즉, 설계된 시스템에서 AVTMR 시스템보다 25%이상의 소자가 더 사용되기 때문이다. 또한, 스위칭 특성을 갖는 알고리즘이 등이 고려되어야 하기 때문에 더욱더 많은 개발 시간이 존재할 수 있다. 결국은 적용되는 시스템이 일정한 시간동안 어느 정도의 신뢰도, 가용도, 안전도, 유지 보수도를 요구하는 가에 따라 시스템이 선택될 수 있다. 또한, 결함 수용율이 시스템의 RAMS에 상당한 영향을 미친다는 것을 알 수 있었다. 듀얼 듀플렉스 시스템이 낮은 결함 수용을 가진다면 오히려, 설계된 AVTMR 시스템 및 단일 시스템 보다 더욱 좋지않은 특성을 가지는 시스템이 될 수 있다는 것이다. 그러므로, 대기 여분 시스템의 설계시 결함을 얼마나 수용할 수 있게 설계하는 것이 또한 시스템의 성능에 지대한 영향을 끼친다는 것을 알 수 있었다. 표 2는 각 시스템의 MTTF를 나타내고 있다.

표 2. 각 시스템의 MTTF

MTTF			
SS_c	337585	SS_m	13993500
AVTMR_c	211028	AVTMR_m	4359940
DD_c	315495	DD_m	6796810

각 시스템의 MTTF는 신뢰도의 무한적분으로 표현된다. 그러므로, 가장 넓은 분포를 가지는 단일 시스템이 가장 크고, 듀얼 듀플렉스, 단일 시스템의 순으로 나타난다. 마찬가지로, MTTF도 적용되는 시스템의 환경에 따라서 RAMS와 함께 고려하여, 적절한 시스템을 선택하는 값으로 볼 수 있다.

추후 연구과제로는 듀얼 듀플렉스, TMR 시스템에 동시에 적용이 될 수 있는 유동성이 있는 CPU 보드의 개발이 되어야 할 것이다.

참 고 문 헌

[1] Barry W.Johnson, "Design and Analysis of Fault-Tolerant Digital Systems", Addison Wesley Publishing Company, 1989.

[2] Dhiraj K. Pradhan, "Fault-Tolerant Computer System Design", Prentice Hall,1996.

[3] 김 현기, "결함 허용 실시간 시스템 개발에 관한 연구", 광운대 석사학위 논문, 1995.

[4] Terje Aven, "Avaliability Formulae for Standby Systems of Similar Units that are Preventively Maintained.", IEEE Trans. on Reliability, Vol.39, No.5, 1990 December.

[5] Charles Y.Choi, Barry W.Johnson and Joseph A. Profeta Ⅲ, "Safety Issues in the Comparative Analysis of Dependable Architectures", IEEE Tran. on Reliability, Vol. 46, NO.3, 1997 September.

[6] David G.Robinson and Marcel F. Neuts, "An Algorithm Approach to Increased Reliability Through Standby Redundancy", IEEE Tran. on Reliability, Vol.38, NO.4, 1989 October

[7] Robert D.Yearout, Prabhaker Reddy and Doris

Lloyd Grosh, "Standby Redundancy in Reliability-A Review", IEEE Tran. on Reliability, Vol.R-35, NO.3, 1986 August.

[8] Daniel P. Siewiorek and Robert S. Swarz "Reliable Computer System" Second Ed, Digital Press,1992

[9] "MC68000 Data Book", MOTOROLA.

[10] Jeffrey A. Clark and Dhiraj K.Pradhan, "Reliability Analysis of Unidirectional Voting TMR systems through Simulated Fault-Injection" IEEE Tran. on Reliability, Vol.38, NO.7, 1992 July

[11] Albert L, Hopkins, Basil Smith, "FTMP-A Highly Reliable Fault-Tolerant Multiprocessor for Aircraft", Proceedings of IEEE. Volume 66, No10, October 1978.

[12] John H, Wensley , et al., "SIFT:Design and Analysis of a Fault Tolerant Computer for Aircraft Control", Proc. IEEE, Vol 66., No 10, Oct. 1978, pp.1240-1255

[13] JOHN F. WAKERLY, "Microcomputer Reliability Improvement Using Triple Modular Redundancy", PROCEEDING OF THE IEEE, VOL.64,No.6,JUNE 1976

[14] "MC68000 Data Book", MOTOROLA.

[15] 김현기외 2인, "보터의 구조에 따른 TMR 시스템의 신뢰도 평가에 관한 연구", 전기학회 춘계학술 대회, 1998

[16] 김현기외 4인, "듀플렉스 시스템의 구조에 따른 시스템의 신뢰성 평가에 관한 연구", 대한 철도학회 춘계학술대회, 1998

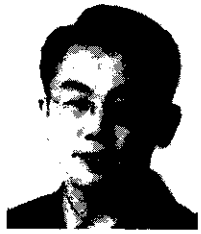
[17] 김현기, 이기서, "AVTMR 시스템 설계 및 RAM 평가", 제 12호, vol25,한국 통신학회 2000.

[18] 김현기, 이기서, "듀얼 듀플렉스 시스템 설계 및 평가에 관한 연구", 제50A권, 4호, 대한 전기학회 논문지, 2001.

[19] "MILITARY HANDBOOK 217F", Department of defense, U.S.A

[20] "RELEX 6.0 User Guide", RELEX

김 현 기(Hyun Ki Kim)



1993년 2월 : 광운대학교 제어계측공학과 졸업(학사)

1995년 2월 : 광운대학교 대학원 제어계측공학과 졸업(석사)

2000년 2월 : 광운대학교 대학원 제어계측공학과 박사수료

1999년 6월~현재 : 모토로라 코리아 테크너러지 센타 근무

<주관심 분야> 결함허용 시스템, 이동 통신, 영상처리

신 석 균(Suk Kuin Shin)

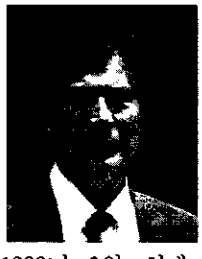
1996년 2월 : 광운대학교 제어계측공학과 졸업

1999년 2월 : 광운대학교 제어계측공학과 대학원 졸업

현재 : 광운대학교 제어계측공학과 박사과정 재학중

<주관심 분야> 철도신호,컴퓨터 제어, 결함 허용시스템 설계

이 기 서(Key Seo Lee)



1977년 2월 : 연세대학교 공과대학 전기공학과

1979년 2월 : 연세대학교 대학원 전기공학과 석사과정

1986년 8월 : 연세대학교 대학원 전기공학과 박사

1989년 3월~현재 : 광운대학교 공과대학 정보제어공학과 교수

<주관심 분야> 철도신호, 컴퓨터 제어, 결함 허용시스템 설계, 적응제어