듀얼 듀플렉스 시스템 설계 및 평가에 관한 연구

論 文
50D-4-2

A Study on the Design and Evaluation of Dual-Duplex System

金 顯 起* · 申 德 浩** · 李 基 西***
(Hyun-Ki Kim · Duck-Ho Shin · Key-Seo Lee)

Abstract - In this paper, we develop a dual-duplex system which detects a fault by hardware comparator and switches to hot standby redundancy. This system is designed on the basis of MC68000 and can be used in VMEbus. To improve reliability, the dual-duplex system is designed in dual modular redundancy. The failure rate of electrical element is calculated in MILSPEC-217F, and the system RAMS(Reliability, Availiability, Maintainability and Safety) and MTTF(Mean Time to Failure) are evaluated by Markov modeling method. As the evaluation result shows improved reliability, it can be used as a component hardware for a highly reliable control system.

Key Words : dual-duplex, reliability, availability, maintainability, safety, fault-tolerant

1. 서 론

과학기술이 발전해 가면서 전자 산업분야에서 점점 더 복잡하고 다양한 기능을 갖는 시스템이 개발되었다. 결국, 시스템이 복잡하고 많은 기능을 갖도록 발전함으로써 고장(failure)에 대한 연구가 필요하게 되었고, 고장 발생 단계 중에서도 처음 단계인 결함(fault)을 연구하여 시스템의 신뢰도(reliability)를 향상시키는 방법이 연구되어 왔다.[1,10]
시스템의 신뢰도를 향상시키기 위한 방법에는 결함 회피(fault avoidance) 방법과 결함 허용(fault tolerance) 방법으로 나누어진다.
결함 회피에는 전자 부품의 질을 향상시키고 많은 테스트를 거쳐서 완벽한 시스템을 만드는 방법이다. 하지만, 전자 부품의 속성상 시간이 지남에 따라 결함이 생기게 된다. 그러므로, 결함이 발생하여도 정상 동작을 계속 수행하도록 하는 결함 허용(fault tolerance) 방법이 더욱 효과적이라 할 수 있다.
결함 허용 방법은 기본 시스템 외에 따로 여분을 두어 결함의 발생을 허용하는 것이다. 이러한 여분을 두는 방법으로 하드웨어 여분(hardware redundancy), 소프트웨어 여분(software redundancy), 시간 여분(time redundancy), 정보 여분(information redundancy)으로 나눌 수 있다.[1,6]
미국의 NASA에서는 상용항공기에 적용하기 위해 하드웨어를 이용한 결함허용 시스템인 FTMP(Fault Tolerant Multiprocessor)와 소프트웨어를 이용한 결함허용 시스템인 SIFT(Software Implemented Fault Tolerant)를 개발하였다.[3,4]
하드웨어 여분을 두는 방법에는 수동적인(passive) 방법과 능동적인(active) 방법, 하이브리드(hybrid) 방법이 있는데, 이 중에서 능동적인 방법은 결함 검출(fault detection), 결함 한정(fault location), 결함 복구(fault recovery)의 개념을 갖는다. 따라서, 결함 방지(fault masking) 개념을 갖는 수동적인 방법보다는 적극적으로 결함을 다루는 방법이다. 능동적인 하드웨어 여분을 두는 방법은 다시 대기여분(standby sparing) 시스템의 동작 상태에 따라 콜드 스탠바이(cold standby), 핫 스탠바이(hot standby), 웜 스탠바이(warm standby)로 나누어진다. 여기서, 핫 스탠바이 시스템은 결함이 발생했을 때 시스템을 재구성하는 시간이 가장 짧은 장점을 갖는다. 현재 동작을 하는 시스템과 대기 상태의 시스템이 합쳐서 구성될 때, 전체 시스템을 이중계 시스템(dual redundant system)이라 한다.[1,6,10]
본 논문에서는 MC68000을 기반으로 하여 VME버스 상에서 동작할 수 있는 핫 스탠바이 시스템(hot standby sparing)을 설계하였다. 특히, 각 CPU 보드는 두개의 CPU를 가지고 있으며, 버스 레벨에서 DTACK 신호를 이용해서 데이터를 비교하여 결함을 검출하는 특성을 가지고 있다. 결함 검출(fault detection)은 XOR와 8255로 구성된 하드웨어 결함 검지기(fault detector)를 이용해서 결함을 검출하고, 결함이 검출되었을 경우에는 계전기를 이용하여 출력전압을 차단하는 특성을 가지며, 대기하고 있는 2중화된 대기여분 구조로 전환할 수 있는 하드웨어를 구성하였으며, 단일 시스템(single system), 듀얼 시스템(dual system)과 듀얼 듀플렉스 시스템(dual duplex system)을 마코브 모델(Markov model)로 시스템의 신뢰도(reliability), 가용도(availability), 유지보수도

* 正 會 員 : 光云大 情報制御工學科 博士修了
** 正 會 員 : 光云大 情報制御工學科 博士課程
*** 正 會 員 : 光云大 情報制御工學科 教授
接受日字 : 2000年 6月 19日
最終完了 : 2001年 4月 3日

(maintainability), 안전도(safety)를 평가하였다.[5,7,8] 이렇게 개발된 듀얼 듀플렉스 시스템(dual duplex system)은 실제적으로 높은 신뢰도와 가용도가 중요시되는 임베디드 제어 시스템(embedded control system)에 적용될 수 있다.[9,10,11]

2. Dual-duplex 시스템 설계

본 논문에서 설계된 듀얼 듀플렉스 시스템은 능동 하드웨어 구조로 결함이 있는 하드웨어를 검출하여 대기 여분 시스템으로 전환하는 방법이다. 두개의 모듈이 동시에 동작하여 두개의 출력을 비교하여 데이타가 같을 경우 다음 동작을 하고 틀릴 경우에는 비교기(comparator)의 결함 검지회로에 의해서 시스템을 정지시키거나 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 재구성하는 시간이 적게 드는 장점을 갖는다. 우리가 구성하는 듀얼 듀플렉스 시스템은 시간이 중요시되는 시스템에 적용하기 위해서 고장이 발생했을 때 대기 여분이 곧바로 사용될 수 있는 구조를 채택했다. 즉, 두개의 듀얼 보드(dual board)중 한 개의 보드는 입력되는 데이터를 처리하고, 다른 대기 여분 구조는 입력되는 데이터를 가지고 동작을 하면서 시스템의 결함 검지 회로의 입력을 기다리는 구조로 되어있다. 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(control bus)를 비교하면서, 데이터가 틀릴 경우 대기하고 있던 다른 보드로 전환을 한다. 우선 설계된 듀얼 CPU보드의 블럭도는 그림 1과 같다. 그림 1에서 보면, 두개의 MC68000을 리셋 안정화 소자인 TL7705를 이용하여 동기 리셋 회로를 구성하였고, 클락 회로는 오실레이터를 이용하여 동기 클럭으로 동작을 하고, 비교기에서는 제어 신호(control bus)와 데이터 버스(data bus), 어드레스 버스(address bus) 데이터가 가장 안정한 시점인, DTACK 신호가 로우(low)에서 하이(high)로 변하는 에지(edge)에서 데이터를 비교하도록 설계되었다. 비교기는 ALTERA를 이용하여 XOR를 사용하여 설계하였다. 즉, 같은 데이터일 경우에는 출력이 0이고, 다른 데이터일 경우에는 1을 출력하는 특성을 갖도록 설계하였다. 그러므로, 각각의 비교기에서 비교 데이터에 결함이 발생할 경우에는 스위칭 로직(switching logic)에 의해서 대기 여분(standby sparing)으로 동작하고 있는 시스템으로 스위칭하는 특성을 가지고 있고, CPU보드의 확장성을 위해 VME 버스에서도 동작을 할 수 있도록 하드웨어를 구성하였다. 이러한 듀얼 구조의 입/출력 보드도 듀얼 구조를 가지게 된다. 입/출력 구조는 그림 2에 나타나 있다. 입/출력은 전부 노이즈에 강한 광소자를 사용하여 설계가 되었으며, 입력의 경우는 각 듀얼 보드 CPU에 같은 데이터가 입력되어야 하므로, 입력의 결선이 각각의 듀얼 입력 보드에 연결이 된다. 출력의 경우, 듀얼 보드에서는 두 개의 출력이 나오므로 한 개의 출력이 되도록 듀얼 스위치(dual switch)로 설계되었다.

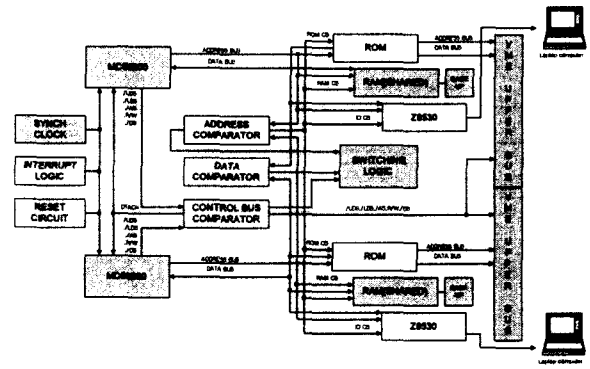

그림 1. 듀얼 듀플렉스 CPU보드의 구성도
Fig 1. The Block diagram of Dual-duplex CPU board

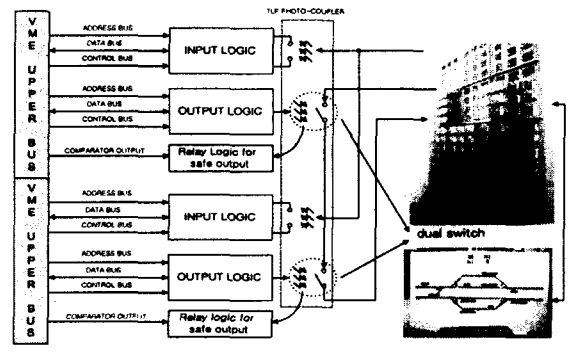

그림 2.듀얼 듀플렉스 입/출력 구조
Fig 2.The input/output structure of dual-duplex

입력과 마찬가지로 출력도 광소자를 이용하였으며, 결함이 발생하지 않은 경우에만, 광소자에 전원을 공급해 주고, 각각의 출력이 동시에 같은 값을 가질 때만 동작을 하는 듀얼 스위치(dual switch) 회로를 구성하였다. 만약, 결함이 발생하였을 경우에는 광소자의 전원 공급이 계전기에 의해서 차단된다.

그림 3은 결함 검출 및 스위칭 로직의 회로를 나타내고 있다. 우선 데이터 data0_0 와 data1_0 는 두 개 CPU의 데이터 버스이다. 이 신호는 XOR를 이용하여 두 개의 데이터가 두 개의 /DTACK 신호로 데이터가 가장 안정한 시점에서 비교를 하도록 구성되어 있으며, 두 개의 데이터가 일치하지 않을 경우에는 1을 출력시키도록 되어 있다. 결함 검출 시간 제어 로직은 이러한 비교 시간을 제어하는 로직이다. 카운터는 일시적인 결함에 의한 시스템 고장을 막기 위해서 최소 결함이 3번 이상 발생하였을 경우에 스위칭이 되도록 하는 래치 카운터(latch counter)로 구성된다. 카운터의 출력으로 계전기에 의해 공급되는 광소자의 전원을 차단하고, 대기 중인 시스템에 제어 권한을 넘기도록 설계되어 있다. 대기 중인 시스템은 8255로 주기적인 전환 입력을 검사하며, 고장이 발생하였을 경우, 시스템의 동작 권한을 갖게 된다. 대기중인 시스템의 스위칭 로직에 알고리즘은 그림 4와 같이 동작된다. 처음에 각 듀얼 듀플렉스 시스템이 초기화가 되고, 결함을 검지하는 8255는 입력모드로 초기화가 된다.
처음에 결함이 검지 되었는지 각 듀얼 시스템은 서로의 결함상태를 검사하게 된다.

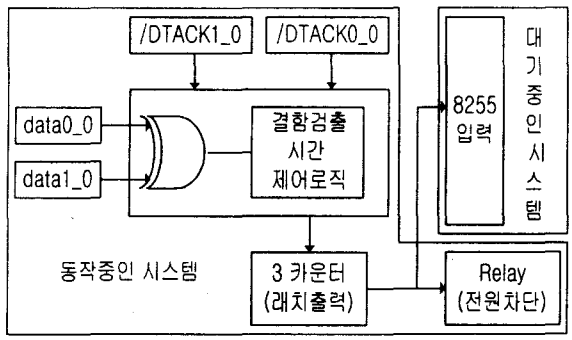

그림 3. 결함검출 및 스위칭 구조
Fig 3.The structure of fault detection and switching

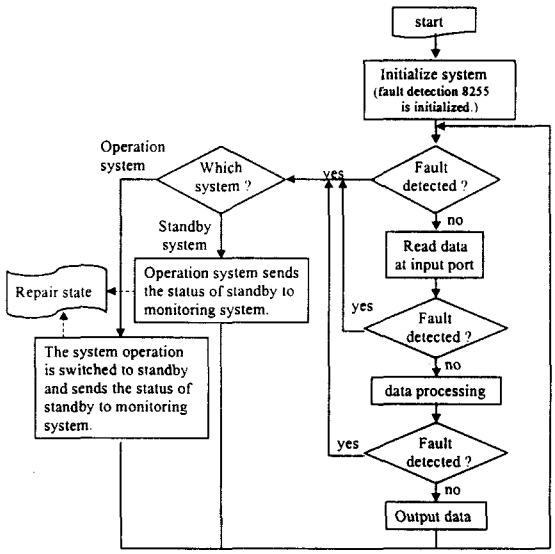

그림 4. 결함 검출 알고리즘의 플로우 차트
Fig 4. The flow chart of a fault detection algorithm

결함이 발생하지 않으면, 두 개의 듀얼 보드는 입력 데이터를 읽고, 다시 결함의 상태를 검사하고, 결함이 발생하지 않았으면, 데이터 처리를 하고, 다시 결함 검사를 하고, 이상이 없을 때는 동작하고 있는 시스템이 출력을 한다. 그리고, 다시 처음상태로 돌아가서 같은 일을 반복하게 된다. 만약, 각각의 단계에서 결함이 발생하였을 경우에는 어떤 시스템이 고장이 발생을 하였는가에 따라서 동작이 틀려지게 된다. 즉, 동작중인 시스템에서 결함이 발생하는 경우에는 대기중인 시스템이 동작을 하도록 구성이 되고, 대기중인 시스템에 결함이 발생하는 경우에는 액티브 시스템은 계속 동작을 수행하고, 결함의 상태를 모니터링 시스템으로 알려주게 된다. 본 논문에서 설계된 시스템은 철도 시스템중 전자 연동장치 시스템(electronic interlocking system)에 적용하기 위해 설계되었다. 이러한 하드웨어를 지원하기 위해서 운영체제는 VRTX를 사용하였으며, 위에 제시된 결함 검출 소프트웨어 알고리즘은 타이머를 이용하여 500ms에 한번씩 검사하도록 설계가 되어있다.[5,15]

표 1.전자소자의 고장율 및 사용개수

사용된 소자	고장율1 (10^{-6}h)	고장율2 (10^{-6}h)	SS (개수)	DS (개수)
MC68000	1.329899	0.033247	1	2
27C010	0.086332	0.002158	2	4
681000	0.139243	0.003481	4	8
Z8530	0.242960	0.006074	1	2
8253	0.125532	0.003138	1	2
EPM7128LC84	0.219911	0.005498	4	5
74LS244	0.058272	0.001457	12	24
74LS245	0.058272	0.001457	6	12
74LS04	0.044916	0.001123	1	2
74LS05	0.044916	0.001123	1	6
74LS07	0.047508	0.001188	1	6
TL7705	1.095121	0.027378	1	1
8255	0.126798	0.003170	2	6
oscillator	0.021441	0.000536	2	1
저 항	0.002945	0.000029	116	232
콘덴서	0.005131	0.000051	84	168
스위치	0.200783	0.100391	2	2
max232	0.033405	0.000835	1	2
optoisolator	0.016047	0.072946	48	96
다이오드	0.010425	0.001327	26	50
계전기	0.141030	0.072946	0	2

(고장율1:상업용 소자, 고장율2: MILSPEC 소자
SS: Single System, DS:Dual System)

3.시스템 평가

3.1. 정량화된 계산방법

3.1.1고장률 계산

고장률(failure rate)은 모든 하드웨어 시스템 평가, 즉 구성될 시스템의 신뢰도, 가용도와 MTTF(Mean Time to Failure)를 평가하는데 가장 중요한 요소이다. 고장율 λ는 전자소자 또는 시스템의 평균동작 시간의 역수로서 식(1)과 같이 나타낼 수 있다.

$$\lambda = \frac{1}{\text{평균동작시간}} \qquad (1)$$

본 논문에서 사용된 전자소자의 고장율은 표1과 같이 구해진다. 고장율 1은 일반적인 상업용 전자소자의 고장율이고, 고장율 2는 MILSPEC중 가장 작은 전자소자의 고장율을 나타낸다. 이러한 전자소자의 고장율은 MIL-HDBK-217F에 근거하여 계산되었다.[12] 고장율은 RELEX6.0을 이용하여 계산하였다.[13] 표 1에 전자소자의 개수는 CPU보드와 입/출력 보드에 사용된 총 소자의 개수를 나타내고 있다. 표 1에서 듀얼 시스템(DS)이 단일 시스템(SS) 보다 2배 정도의 소자가 더 사용된다는 것을 알 수 있다. 표1의 전자소자의 개수는 CPU 보드 및 입/출력 보드에 사용되는 전자소자의 개수를 나타내고 있다.

3.1.2. MTTF(Mean Time To Failure)

MTTF는 시스템의 수명을 나타내는 요소로 고장이 나는 시

간 간격을 나타낸다. 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 랜덤한 X에 대한 기대값의 식은 결국 신뢰도의 함수를 시간에 대한 무한대의 적분으로 표현될 수 있다.[1,6]

$$MTTF=\int_0^{\infty} R(t)dt \qquad (2)$$

3.1.3. MTTR(Mean Time To Repair)

MTTR은 시스템을 수리하기 위해 요구된 평균시간이다. 즉, N 개의 고장이 i번째 수리하기 위해 t_i의 시간이 필요하다면, MTTR은 식(3)과 같이 나타날 수 있다.

$$MTTR=\frac{\sum_{i=0}^{N} t_i}{N} \qquad (3)$$

3.2. RAMS 평가 방법

3.2.1.신뢰도(Reliability)

시스템과 전자 소자의 신뢰도는 시간 t_0에서 올바르게 동작하고 있을 때, 시간 간격 $[t_0, t]$에서 올바르게 동작하는 조건적인 확률이다. 그러면, N개의 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(4)와 같다.[1,6,9]

$$R(t)=\frac{N_o(t)}{N_o(t)+N_f(t)}=e^{-\lambda t} \qquad (4)$$

3.2.2 가용도(Availability)

시스템의 가용도 $A(t)$는 시스템이 시간 t의 순간에 어떠한 태스크를 수행할 수 있는 확률로서 정의된다. 즉, 가용도는 시스템이 올바르게 동작되는 시간의 비율로 볼 수 있다. 그러므로, 식(5)와 같이 시스템이 동작하는 시간과 수리하는 시간의 비율로서 표현될 수 있다.[1,6]

$$A(t_{current})=\frac{t_{op}}{t_{op}+t_{repair}} \qquad (5)$$

3.2.3.유지 보수율(Maintainability)

유지 보수율은 고장난 시스템이 확정된 시간 안에 회복될 수 있는 확률을 말한다. 유지 보수율 M(t)는 시스템이 t 이하의 시간에 수리될 확률을 이야기한다. 이 유지 보수율은 수리율 μ를 이용해서 구할 수 있다.[1,11]

$$M(t)=1-e^{-\mu t} \qquad (6)$$

3.2.4. 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.[11]

4. 시스템 모델링 및 시뮬레이션

마코브 모델링(Markov modeling method)을 이용하여 시스템을 평가하였다. 마코브 모델링은 시스템의 고장율에 따른 시스템의 상태 변환을 확률적인 시스템 모델로 표현한 기법이다. 마코브 모델링에서는 두 개의 결함이 동시에 발생하지 않는다는 조건에서 사용된다.

4.1.단일 시스템

기본적인 시스템으로 하드웨어 여분을 사용하지 않은 구조로 그림 5에 나타나 있다. 그림 6은 단일 시스템에 대한 마코브 모델을 나타내고 있다. 단일 시스템은 정상적인 상태와 고장이 난 상태로 나눌 수 있다.

그림 5 .단일 시스템 구조

Fig 5.The structure of Single System

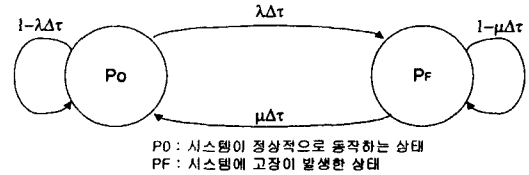

그림 6 . 단일 시스템의 마코브 모델

Fig 6. Markov model of Single System

이 단일 시스템의 마코브 모델 방정식은 식(7)과 같다. 식(7)에서의 μ는 시스템의 수리율이다.

$$\begin{bmatrix} P_O(\tau+\Delta\tau) \\ P_F(\tau+\Delta\tau) \end{bmatrix} = \begin{bmatrix} 1-\lambda\Delta\tau & \mu\Delta\tau \\ \lambda\Delta\tau & 1-\mu\Delta\tau \end{bmatrix} \begin{bmatrix} P_O(\tau) \\ P_F(\tau) \end{bmatrix} \quad (7)$$

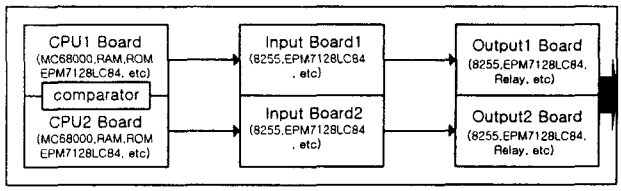

그림 7. 듀얼 시스템 구성도

Fig 7. The block diagram of dual system

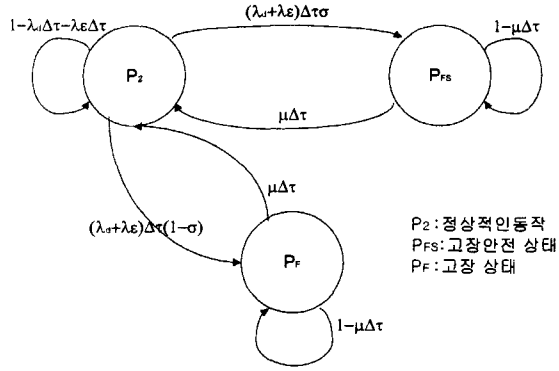

그림 8.듀얼 시스템의 마코브 모델

Fig 8. The markov model of dual system

4.2 듀얼 시스템

듀얼 시스템(dual system)의 구조는 그림 7에 나타나 있다. 단일 시스템의 구조를 두 개 붙여놓은 구조이다. 이 시스템은 두 개의 보드를 버스 레벨로 리드/라이트 시에 데이터를 비교하는 비교기 회로가 CPU 보드에 설계되어 있다. 이 로직은 ALTERA를 사용하여 설계가 되어있으며, 두 개의 CPU는 같은 클럭으로 동작을 하고, 두 개의 데이터가 가장 안정한 시점을 골라 XOR를 사용하여 비교하도록 MC68000의 제어신호인 /DTACK 과 /AS 신호를 이용하여 설계를 하였다.[14] 입력 보드는 두 개의 입력신호를 각각 동시에 받도록 설계되었고, 출력은 계전기를 이용하여 두 개의 출력이 한 개로 출력되도록 설계가 되었다. 즉, 결함이 발생하지 않을 경우에는 계전기를 계속 출력하는 상태로 유지하였고, 결함이 발생하였을 경우에는 계전기가 다운되어 출력이 차단되도록 설계가 되어있다. 림 8은 듀얼 시스템의 마코브 모델(Markov model)을 나타내고 있다. 즉, 결함이 발생되었을 경우, 결함 검지를 하여 안전한 상태로 전환된다.

식(8)은 듀얼 시스템의 방정식이다. 여기서 λ_d는 듀얼 시스템의 고장율이고, λ_ε는 결함을 검출하는 소자의 고장율이다. 이 고장율은 8255와 ALTERA를 사용하여 구성된다.

μ는 시스템의 수리율이고, σ는 듀얼 시스템의 결함 수용능력이 된다. 이 결함 수용능력은 영구결함 240가지의 경우에 대해 100%의 결함을 검출하였고, 일시적인 결함 주입시에는 120개중 109개의 검출 능력을 나타내었다. 그러므로, 결함을 검출 능력은 0.9750의 값을 가진다.

영구결함은 stuck-at-fault 0 와 stuck-at-fault 1을 강제로 입력하였고, 일시적인 결함은 글리치(glitch)를 임의 적으로 입력하여 결함 수용 능력을 구하였다. 듀얼 듀플렉스 시스템도 마찬가지의 방법으로 구하였다.

4.3. 듀얼 듀플렉스 시스템

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 다운시켜서 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.[14]

이 시스템의 방정식은 식(9)와 같다. 여기서 λ_{dd}는 듀얼 시스템의 고장율, λ_{ed}는 결함 검출로직의 고장율, μ는 수리율이고, σ는 결함 수용능력이다. 듀얼 시스템과 마찬가지 방법으로 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 0.9777을 가진다.

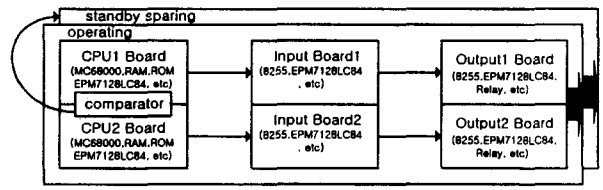

그림 9.듀얼 듀플렉스 시스템 구성도

Fig 9. The blockdiagram of dual-duplex system

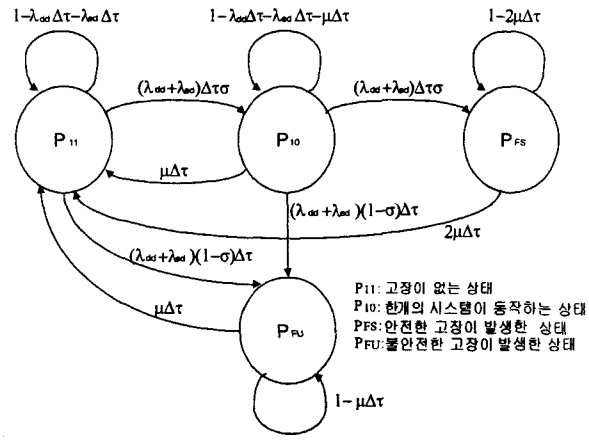

그림 10. 듀얼 듀플렉스 시스템의 마코브 모델

Fig 10. Markov model of dual-duplex system

$$\begin{bmatrix} P_2(\tau+\Delta\tau) \\ P_{FS}(\tau+\Delta\tau) \\ P_F(\tau+\Delta\tau) \end{bmatrix} = \begin{bmatrix} 1-(\lambda_d+\lambda_e)\Delta\tau & \mu\Delta\tau & \mu\Delta\tau \\ (\lambda_d+\lambda_e)\sigma & 1-\mu\Delta\tau & 0 \\ (\lambda_d+\lambda_e)(1-\sigma)\Delta\tau & 0 & 1-\mu\Delta\tau \end{bmatrix} \begin{bmatrix} P_2(\tau) \\ P_{FS}(\tau) \\ P_F(\tau) \end{bmatrix} \quad (8)$$

$$\begin{bmatrix} P_{11}(\tau+\Delta\tau) \\ P_{10}(\tau+\Delta\tau) \\ P_{FS}(\tau+\Delta\tau) \\ P_{FU}(\tau+\Delta\tau) \end{bmatrix} = \begin{bmatrix} 1-(\lambda_{dd}+\lambda_{ed})\Delta\tau & \mu\Delta\tau & 2\mu\Delta\tau & \mu\Delta\tau \\ (\lambda_{dd}+\lambda_{ed})\sigma\Delta\tau & 1-(\lambda_{dd}+\lambda_{ed}+\mu)\Delta\tau & 0 & 0 \\ 0 & (\lambda_{dd}+\lambda_{ed})\sigma\Delta\tau & 1-2\mu\Delta\tau & 0 \\ (\lambda_{dd}+\lambda_{ed})(1-\sigma)\Delta\tau & (\lambda_{dd}+\lambda_{ed})(1-\sigma)\Delta\tau & 0 & 1-\mu\Delta\tau \end{bmatrix} \begin{bmatrix} P_{11}(\tau) \\ P_{10}(\tau) \\ P_{FS}(\tau) \\ P_{FU}(\tau) \end{bmatrix} \quad (9)$$

4.4. 시뮬레이션

본 논문에서는 시뮬레이션을 하기 위하여, RELEX6.0을 이용하여 각 소자의 고장율을 구하였고, MATLAB을 이용하여 식(7),(8),(9)로 각 시스템의 RAMS(Reliability, Availability, Maintainability, Safety)를 평가하였다.[13] 그림 11은 각 시스템의 신뢰도(reliability)를 나타내고 있다. 즉, 상업용 소자를 이용하여 시스템을 구성한 것과 MILSPEC 소자중 가장 좋은 레벨의 소자를 사용한 경우를 비교하여 나타내고 있다. 초반에는 듀얼 듀플렉스 시스템이 가장 좋은 신뢰도를 가지고 있고, 다음은 단일 시스템, 듀얼 시스템의 순으로 나타난다는 것을 알 수 있다. 일정시간이 지나고, 단일 시스템, 듀얼 듀플렉스 시스템, 듀얼 시스템의 순으로 나타난다. 즉, 상업용 소자일 경우에는 470000(54년) 시간, MILSPEC 소자일 경우에는 2300000(263년) 시간정도가 단일 시스템과 듀얼 듀플렉스 시스템의 교차 시점이 된다. 신뢰도의 곡선이 교차하는 특성은 듀얼 듀플렉스 시스템이 단일 시스템보다 많은 양의 전자소자를 사용하기 때문에 시간이 흐르면서 구조적으로는 단일 시스템보다 우수한 신뢰도의 구조를 가지지만 소자의 특성으로 인하여 단일 시스템보다 신뢰도가 낮아지는 구조를 가지게 된다. 또한, 2300000의 시간일 때 교차하는 신뢰도의 값은 0.875이다. 즉, 단일 시스템의 신뢰도가 0.875보다 큰 값을 가질 땐 듀얼 듀플렉스 시스템 보다 고장이 날 확률이 많다고 볼 수 있다. 즉, 처음의 상당한 시간동안 듀얼 듀플렉스 시스템이 우수한 신뢰도(reliability)를 가진다는 것을 알 수 있다. 그림 12는 각 시스템의 가용도(availability)를 나타내고 있다. 가용도(avaliability)는 수리율을 0.001로 하여 계산하였다. 가용도는 상업용 소자나 MILSPEC 소자에 관계없이 듀얼 듀플렉스 시스템(dual-duplex system)이 가장 우수한 가용도를 가지고, 다음은 단일 시스템(single system), 듀얼 시스템(dual system)의 순으로 나타나는 것을 알 수 있다. 상업용 소자일 경우에 듀얼 듀플렉스 시스템은 0.99983, 단일 시스템은 0.99683, 듀얼 시스템은 0.99935을 갖는다. MILSPEC 소자일 경우에 듀얼 듀플렉스 시스템은 0.99999를 가지고, 단일 시스템 일 경우에는 0.99970, 듀얼 시스템일 경우에는 0.99997 의 가용도를 가지고 있다.

시스템의 유지 보수도(maintainability)는 각 시스템의 수리율(repair rate)에 따라 다르게 나타난다. 그림 13은 수리율이 0.1, 0.01, 0.001 일 때, 각 시스템의 유지 보수도(maintainability)를 나타내고 있다. 즉, 수리율이 좋을 수록 유지 보수도가 우수하게 되므로, 시스템의 가용도를 결정하는 중요한 요소가 된다.

그림 14는 상업용 소자의 안전도(safety)를 나타내고 있다. 처음에는 듀얼 듀플렉스 시스템의 안전도(safety)가 가장 우수하다가 200000 시간 정도에 듀얼 시스템이 더 좋은 안전도(safety)를 나타낸다는 것을 알 수 있다. 그림 15는 MILSPEC 소자를 사용한 경우를 나타내고 있다. 듀얼 듀플렉스 시스템(dual duplex system)이 가장 우수한 안전도(safety)를 가지고, 듀얼 시스템(dual system), 단일 시스템(single system)순으로 나타난다는 것을 알 수 있다.

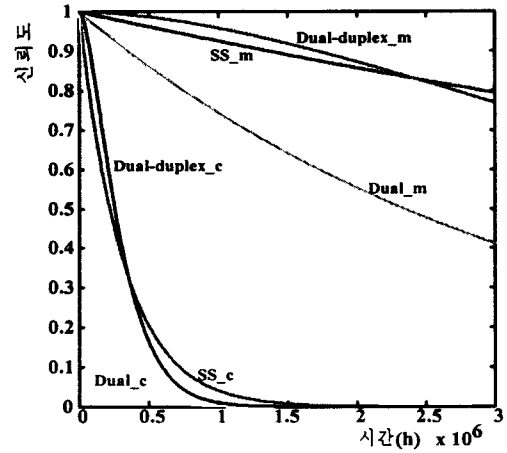

그림 11. 각 시스템의 신뢰도

Fig 11. The reliability of each system

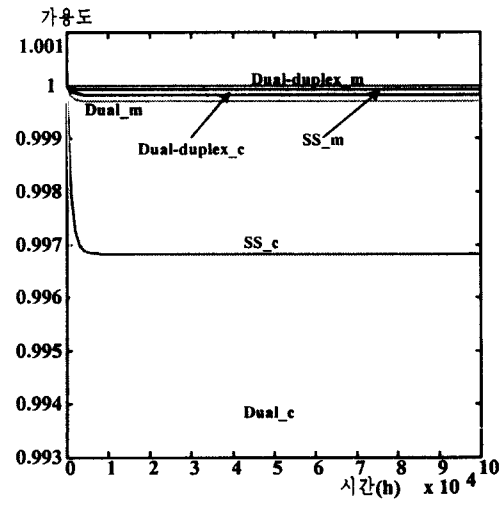

그림 12. 각 시스템의 가용도

Fig 12.The availability of each system

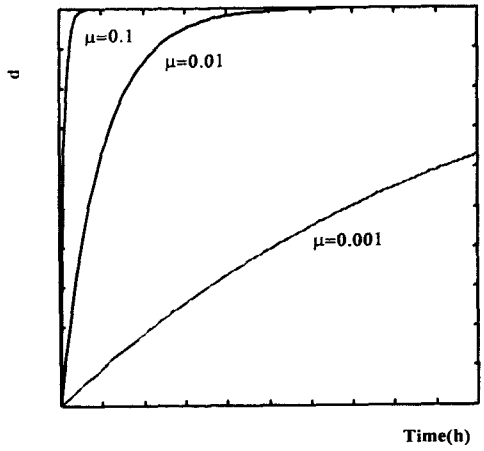

그림 13. 시스템의 유지보수도
Fig 13. The maintainability of system

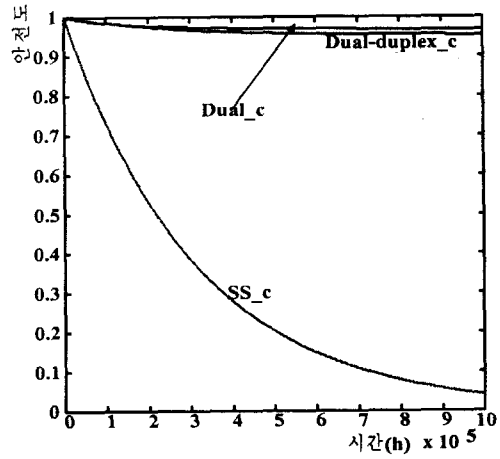

그림 14. 상업용 소자에 대한 시스템 안전도
Fig 14.The safety of commercial element

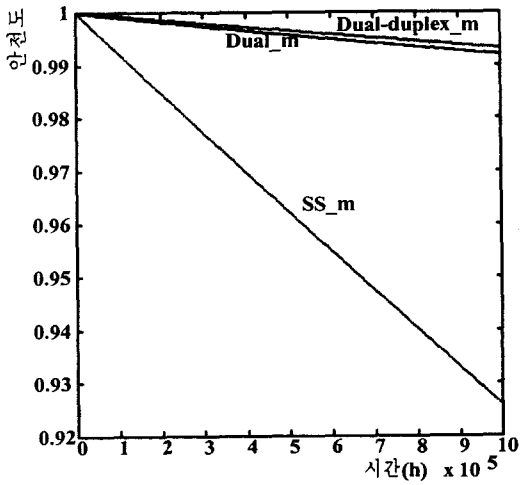

그림 15. MILSPEC 소자에 대한 시스템 안전도
Fig 15.The system safety of MILSPEC element

5. 실험 결과

그림 16은 개발된 듀얼 듀플렉스 시스템(dual duplex system)의 사진을 나타내고 있다. 듀얼 시스템(dual system)의 구조가 2중계로 구성된 것을 나타내고 있다. 한 개의 시스템이 동작중이고, 다른 한 개의 시스템은 대기중에 있는 구조를 나타내고 있다.
그림17은 정상적인 동작을 하고 있는 듀얼 듀플렉스 시스템의 타이밍도이다. 즉, 동작중인 시스템이 정상적인 동작을 할 경우에는 결함 검출 신호가 0으로 되어있는 것을 볼 수 있다. 그림18은 결함이 발생하였을 경우의 타이밍을 나타내고 있다. 즉, 데이터 data1_0이 0으로 되어 있을 때, data0_0와 비교하여, 3번의 사이클동안 결함이 발생되었을 경우에 결함 신호를 나타내는 것을 알 수 있다.

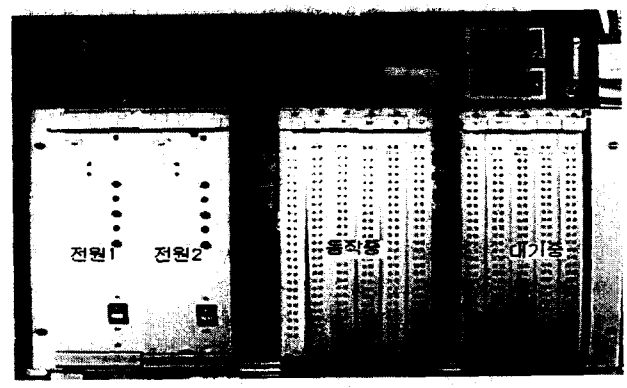

그림 16. 듀얼 듀플렉스 시스템 사진
Fig 16.The photograph of dual-duplex system

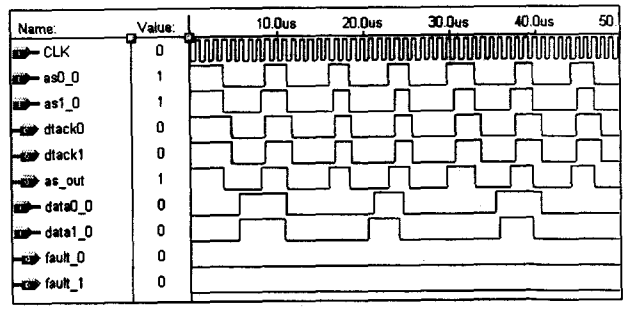

그림 17. 정상동작일 경우의 시스템 타이밍
Fig 17. The timing of stable operation

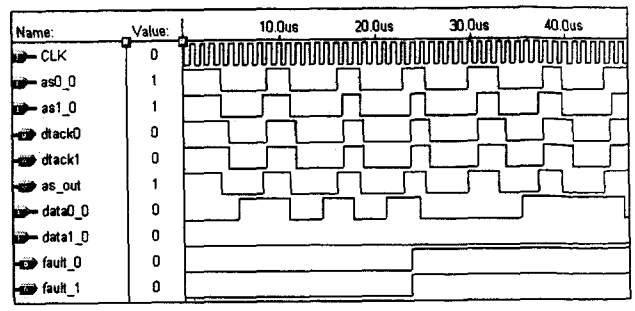

그림 18. 결함 검지시의 타이밍도
Fig 18. The timing of fault detection

어느 정도 일시적인 결함에 대해서 처리를 할 수 있는 특징을 가지고 있다는 것을 알 수 있다.

6. 결 론

본 논문에서는 듀얼 듀플렉스 CPU보드를 MC68000을 이용하여서 설계를 하였다. 또한, 단일 시스템(single system), 듀얼 시스템(dual system), 듀얼 듀플렉스 시스템(dual duplex system)을 평가하고 신뢰도(reliability), 가용도(avaliability), 안전도(safety)를 비교하였다. 설계된 듀얼 듀플렉스 시스템(dual duplex system)이 전체적으로 좋은 신뢰성을 가진다는 것을 알 수 있었다. 즉, 시스템의 동작은 영원히 요구되는 것이 아니라, 일정한 확률값까지 동작이 되도록 요구되기 때문에, 처음부터 일정한 확률의 값, 즉 일정 시간동안 듀얼 듀플렉스 시스템이 처음부터 가장 우수한 평가값을 가지기 때문에 전체적으로 우수하다고 볼 수 있다. 그리고, 상업용 소자보다는 고장율이 작은 MILSPEC 소자가 우수한 시스템 특성을 가진다는 것을 알 수 있었다. 시스템의 신뢰도(reliability)와 가용도(avaliability)는 듀얼 듀플렉스(dual duplex system), 단일 시스템(single system), 듀얼 시스템(dual system)의 순이 된다는 것을 알 수 있었고, 안전도(safety)는 듀얼 듀플렉스(dual duplex system), 듀얼 시스템(dual system), 단일 시스템(single system) 순이라는 것을 알 수 있었다. 안전도(safety)는 시스템의 결함 수용능력(fault coverage)에 따라 결정된다고 볼 수 있다. 시스템의 유지 보수도(maintainability)는 시스템의 수리율(repair rate)에 따라 결정된다는 것을 알 수 있었다. 즉, 수리 시간이 빠르면, 좋은 유지 보수도(maintainability)를 가진다는 것을 알 수 있었다. 그러므로, 시스템은 개발되는 환경에 따라서 중요시 되는 평가값과 비용에 따라 설계되어야 할 것이다.

표2.각 시스템의 MTTF

	상업용 소자(h)	MILSPEC(h)
단일 시스템	337585	13993500
듀얼 시스템	160251	3452350
듀얼 듀플렉스	315495	6796810

표2는 각 시스템의 MTTF(Mean Time To Failure)를 나타내고 있다. 시스템의 MTTF는 단일 시스템(single system), 듀얼 듀플렉스 시스템(dual duplex system), 듀얼 시스템(dual system)의 순이라는 것을 알 수 있다. 상업용 소자에 대한 물리적인 의미를 살펴보면, 단일 시스템의 경우는 337585개의 160251단일 시스템이 1시간동안 고장없이 동작할 수 있고, 듀얼 시스템, 듀얼 듀플렉스 시스템도 마찬가지로 개, 315495개가 1시간동안 고장없이 동작할 수 있다는 의미를 가진다. 마찬가지로, 100개가 1만 시간을 연속동작을 할 때 1개가 고장이 발생할 확률이 소수 4째 자리에서 반올림할 경우에 단일시스템은 0.338, 듀얼시스템은 0.160, 듀얼 듀플렉스 시스템은 0.315의 확률을 가지게 된다. MILSPEC의 소자로 구성된 시스템도 같은 물리적인 특성으로 해석될 수 있다. 물론, 단일 시스템이 가장 우수한 MTTF를 가지고 있지만, 시스템을 MTTF의 시간동안 사용하는 것이 아니라 시스템의 신뢰도, 가용도, 안전도, 유지보수도를 기준으로 특정 확률값의 시간까지 사용되기 때문에 단일 시스템에 가장 좋다고 말할 수는 없다. 처음의 상당한 시간동안 듀얼 듀플렉스 시스템이 RAMS를 비교해볼 때 가장 우수하다는 것을 알 수 있다.

이러한 시스템을 개발하는 데 있어서 앞으로 중요한 것은 높은 신뢰성를 얻기 위해 고장률이 작은 전자 소자를 만드는 것과 높은 수리율이 가장 중요하다고 볼 수 있고, 또한 시스템의 특성에 맞는 실시간 시스템(rela time system)에 적용하기 위해서 실시간 운영체제(RTOS)의 개발도 시스템의 성능을 향상시킬 수 있다고 생각한다.

참 고 문 헌

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

[2] K.G.Shin, C.M.Krishna, and Y.-H. Lee, " A unified method for evaluating real-time computer controllers and their application", IEEE Tans. Automat. Contr. Vol. AC-30, no.4, 1985.

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

[4] 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

[5] 김현기, 이기서, 임재식 "결함 허용 실시간 시스템 개발에 관한 연구", 대한 전기학회 전기철도 연구회 춘계학술발표 회, 1995.

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

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

[8] 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.

[9] 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

[10] 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.

[11] Ashok Kumar, M.G. Chopra and Vipin B.Kapoor,"A Computer Algorithm for Optimal Maintenance of

Standby Redundant System", IEEE Tran. on Reliability, Vol.R-30, NO.1.
[12] "MILITARY HANDBOOK 217F", Department of defense, U.S.A
[13] "RELEX 6.0 User Guide", RELEX Corporation, U.S.A 1999.
[14] 김현기외 4인, "듀플렉스 시스템의 구조에 따른 시스템의 신뢰성 평가에 관한 연구", 대한 철도학회 춘계학술대 회, 1998
[15] 김현기, 이기서, "AVTMR 시스템의 설계 및 RAM 평가", 제 25권,12호, 한국 통신학회, 2000

저 자 소 개

김 현 기 (金 顯 起)

1970년 10월 14일 생. 1993년 2월 광운대학교 공과대학 제어계측공학과 졸업. 1995년 2월 광운대 공과대학원 제어계측공학과 졸업(석사). 2000년 2월 광운대학교 대학원 제어계측공학과 박사수료. 1999년 6월 - 현재 모토로라 코리아 테크너러지 센타 근무. 주관심 분야: 결함허용 시스템, 이동 통신, 영상처리

Tel : 02-3440-7761, Fax: 02-3440-7859,
E-mail : Hyunki.Kim@motorola.com

신 덕 호 (申 德 浩)

1974년 4월 1일 생. 1998년 2월 광운대 공과대학 제어계측공학과 졸업. 2000년 2월 광운대 공과대학 제어계측공학과 졸업(석사). 2000년 3월~현 재: 광운대 공과대학 제어계측공학과 박사과정. 주관심 분야: 철도 신호, FT 내장형 시스템

Tel : 02-940-5154, Fax : 02-911-3930
E-mail : ducko@shinbiro.com

이 기 서 (李 基 西)

1951년 1월 18일 생. 1977년 2월 연대 공과대학 전기공학과 졸업. 1979년 2월 연대 대학원 전기공학과 졸업(석사). 1986년 8월 연대 대학원 전기공학과 졸업(공박). 1988년 1월 ~1989년 1월 YALE University Visiting Scholar. 1981년 3월 ~1989년 2월 광운대 공과대학 제어계측공학과. 1989년 3월 ~현재 광운대 공과대학 정보제어공학과 교수. 주관심분야: 철도신호, 결함허용 시스템, 컴퓨터제어

Tel : 940-5154, Fax : 02-911-3930
E-mail : kslee@daisy.kwangwoon.ac.kr