

# 듀플렉스 시스템의 구조에 따른 신뢰성 평가에 관한 연구

## A study on the Dependability Evaluation according to the structure of Duplex system

김현기\*, 강민수\*, 신덕호\*\*, 권용훈\*\*, 이기서\*\*\*

Kim Hyun Ki, Kang Min Soo, Shin Duck Ho, Kwon Yong Hoon, Lee Key Seo

### ABSTRACT

This paper shows two models of the duplex system having a fault tolerant system characteristic used in airplane and railway system. The architecture of these systems is based on MC68000, and we designed the single system, single duplex system, dual system and dual duplex system to evaluate the system characteristic. We calculate the failure rate of components using MIL-SPEC-217F and evaluate the reliability, availability, safety and MTTF(Mean Time To Failure) of the designed systems by Markov model. We choose our system depending on the developing system characteristic.

### 1. 서론

오늘날 우리는 눈부신 과학발전을 이루는 산업 사회에서 살고 있다. 이러한 산업사회에서 인간이 할 수 있는 일을 전자 시스템이 대신하는 부분이 더욱더 증가하고 있다. 이러한 시스템은 또한 점점 더 복잡해지고 다양한 기능을 갖도록 시스템이 개발되고 있다. 시스템이 복잡하고 많은 기능을 갖도록 발전함으로써 고장에 대한 연구가 필요하게 되었고, 결함(fault), 오류(error), 고장(failure) 사이에 상관 관계가 있음을 알게 되었으며, 지금은 고장 발생 단계 중에서도 처음 단계인 결함을 연구하여 시스템의 신뢰도(reliability)를 향상시키는 방법이 연구되고 있다.

시스템의 신뢰도를 향상시키기 위한 방법으로는 전자 부품의 질을 향상시키고 많은 테스트를 거쳐서 완벽한 시스템을 만드는 결함 회피(fault avoidance) 방법과 결함 허용(fault tolerance) 방법이 사용되고 있다. 하지만, 전자 부품의 수명시간이 경과함에 따라 결함이 발생하게 되므로 완벽한 결함 회피는 이룰 수 없다. 그러므로, 결함이 발생하여도 정상 동작을 계속 수행하도록 하는 결함 허용 방법에 관한 많은 연구가 진행되고 있다. 결함 허용 방법은 본래의 시스템 외에 따로 여분(redundancy)을 두어 결함의 발생을 허용하는 방법으로 하드웨어 여분, 소프트웨어 여분, 시간 여분, 정보 여분 구조가 있다. 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. 이 능동적인 하드웨어 여분을 두는 방법은 시스템의 동작 상태에 따라 콜드 스탠바이(cold standby), 핫 스탠바이(hot standby), 워밍 스탠바이(warm standby)로 나누어진다.

\* 광운대학교 제어계측공학과 박사과정

\*\* 광운대학교 제어계측공학과 석사과정

\*\*\* 광운대학교 제어계측공학과 교수

본 논문에서 연구될 듀플렉스 시스템(duplex system)은 현재 동작을 하는 시스템과 한개의 대기 상태의 시스템을 합쳐서 구성되는 시스템으로, MC68000을 기반으로 하여 VME 버스상에서 동작할 수 있는 단일 듀플렉스 시스템(single duplex system), 듀얼 듀플렉스 시스템(dual-duplex system)의 모델을 제시하고, MIL-SPEC-217F를 이용하여 설계될 각각의 전자 소자의 고장율을 계산하고, 마코브 모델을 이용하여 시스템의 신뢰도(reliability), 가용도(availability), 안전도(safety)와 MTTF를 구하여 각각의 시스템에 대한 비교를 한다. 이렇게 평가된 시스템은 특성에 따라서 항공기나 철도 시스템에 적용될 수 있다.

## 2. 전자소자의 고장율 및 평가 함수

### 2.1. 고장율 계산

고장율(Failure rate)은 모든 하드웨어 시스템 평가, 즉 구성될 시스템의 신뢰도, 안전도, 가용도와 MTTF를 평가를 하는데 가장 중요한 요소로서 전자소자 또는 시스템이 동작한 시간의 역수로서 식(1)과 같이 나타낼 수 있다.

$$\lambda = \frac{1}{\text{Operating Time}} \quad (\lambda: \text{고장율}) \quad (1)$$

설계된 소자의 고장율은 MIL-HDBK-217F를 이용하여 표1과 같이 계산하였다.

표1. 설계된 시스템에 사용된 전자소자 고장율

부품	고장율	부품	고장율
MC68000	4.9200	ROM(27C010)	0.6700
RAM(681000)	2.2700	SIO(8530)	1.8240
RTC(DS1284)	1.0240	74LS244	0.0260
74LS245	0.0260	OSCILLATOR	0.0180
PIO(8255)	0.0620	EPM7128LC84	0.0012
TLP621_4	4.8672	TLP523_4	4.8672

(단위: failure/million hours)

### 2.2. 평가 함수

#### 2.2.1. 신뢰도(reliability)

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

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

#### 2.2.2. 안전도(safety)

안전도는 시스템이 동작하는 데 있어서 시스템이 동작하는 관점에서 볼 때 3가지의 경우를 가질 수 있다. 즉, 시스템이 정상적으로 동작하는 경우, 고장이 발생했을 때 안전측으로 동작하는 경우와 고장이 발생했을 때 불안전하게 동작하는 경우로 나눌 수 있다. 여기서의 안전도의 의미는 시스템이 정상적으로 동작을 하는 경우와 안전하게 고장이 발생한 경우의 확률적인 값으로 표현

될 수 있는 것이다. 안전도를 평가할 때는 시스템의 결함 수용능력(fault coverage)가 중요시된다. 본 논문에서는 결함 수용능력을 단일 듀플렉스 구조에서 사용하였다. 소프트웨어를 이용한 결함 검지 기법이기 때문에 완벽한 결함 검지기능을 갖지 못한다는 단점이 있다. 반면 듀얼 듀플렉스 구조는 하드웨어 결함검지(fault detection) 구조로서 결함 수용능력은 소프트웨어 검지 기법보다 높은 수용능력을 가질 수 있다.

### 2.2.3. 가용도(availability)

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

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

### 2.2.3. MTTF(Mean Time To Failure)

MTTF(Mean Time To Failure)는 시스템이 동작을 시작해서 시스템이 멈추는 시간적인 확률값을 나타낸다. MTTF는 식(4)과 같이 신뢰도 함수를 이용해서 구할 수 있다.

$$MTTF = \int_0^{\infty} tf(t)dt = \int_0^{\infty} R(t)dt \quad (4)$$

## 3. 설계된 시스템 구조

여기서는 단일 시스템(single system), 단일 듀플렉스 시스템(single duplex system), 듀얼 시스템(dual system), 듀얼 듀플렉스 시스템(dual duplex system)을 MC68000을 기반으로 한 시스템을 설계하여, 각 시스템에 따른 신뢰도, 가용도, 안전도와 MTTF를 구하여 각각의 시스템의 특성을 비교한다.

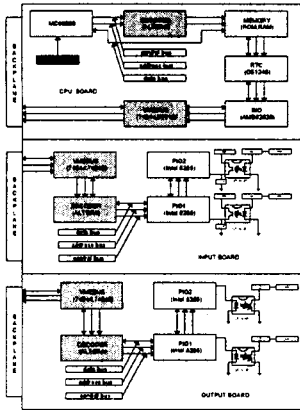


그림 1. 단일 시스템 구조



$P_0$ : 시스템이 동작하는 상태

$P_f$ : 시스템이 고장이 발생하였을 상태

그림 2. 단일 시스템 상태도

### 3.1. 단일 시스템

단일 시스템은 가장 기본적인 구조로 그림1과 같이 설계될 수 있다. 즉, 기본적인 동작을 할 수 있도록 설계된 구조이다. VME 버스에서 작동되도록 하며, MC68000을 기본으로 하여, 메모리, RTC(Real Time Clock), 입/출력 포트, 포토 커플러를 사용한 구조이다. 표2는 단일 시스템을 설계할 때 사용되는 소자의 개수를 나타내고 있다.

표2. 단일 시스템에 사용된 전자소자 갯수

부품	갯수	부품	갯수
MC68000	1	ROM(27C010)	2
RAM(681000)	2	SIO(8530)	1
RTC(DS1284)	1	74LS244	6
74LS245	4	OSCILLATOR	1
PIO(8255)	5	EPM7128LC84	3
TLP621_4	6	TLP523_4	6

그림 2는 시스템의 마코브 모델을 구성하고 있다.  $\lambda$ 는 전체 시스템의 고장율이고,  $\mu$ 는 시스템의 수리율이다. 시스템의 여러 평가함수는 이 요소에 따라 신뢰도에 큰 영향을 미치게 된다. 이 시스템에 대한 상태 방정식을 이끌어 보면, 식(5)과 같이 된다.

$$\begin{bmatrix} P_O(t+\lambda\Delta t) \\ P_F(t+\Delta t) \end{bmatrix} = \begin{bmatrix} 1-\lambda\Delta t & \mu\Delta t \\ \lambda\Delta t & 1-\mu\Delta t \end{bmatrix} \begin{bmatrix} P_O(t) \\ P_F(t) \end{bmatrix} \quad (5)$$

### 3.2. 단일 듀플렉스 시스템

이 시스템은 우리가 일반적으로 알고 있는 하드웨어 대기 여분구조이다. 즉, 그림 3과 같이 단일 시스템이 A(마스터), B(슬레이브)로 구성된다. 그러나, 이 시스템은 두 개의 보드가 통신으로 슬레이브가, 마스터가 결함이 발생하였는지를 감시하는 구조이기 때문에 실질적으로 하드웨어 기술이 아닌 소프트웨어 기법으로 결함을 검지하는 구조를 가지게 된다. 그러므로, 결함 검출 소프트웨어의 완전성을 증명하는 어려움이 있고, 어떤 시스템이 정말 고장인지를 검지하기 어려울 때가 발생할 수 있다. 그러므로, 결함이 발견되지 않을 때도 있다.

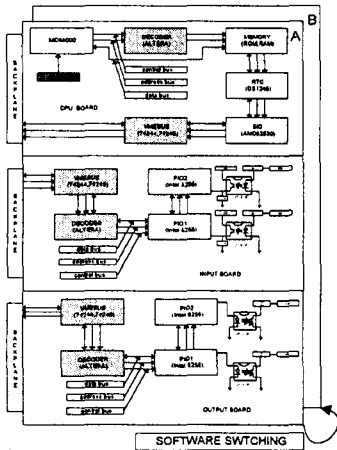
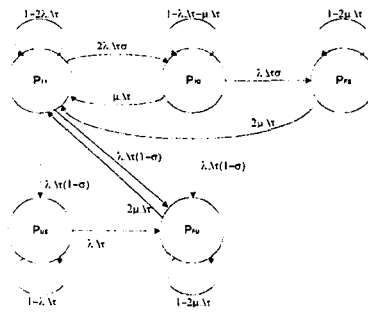


그림 3. 대기 이중계 시스템



- $P_{11}$ : 두 개의 모듈이 정상동작을 하는 상태.
- $P_{10}$ : 마스터가 결함이 발생하여 대기 여분으로 전환된 상태
- $P_{12}$ : 대기여분에서 고장이 검지되지 않은 상태.
- $P_{13}$ : 시스템이 안전측으로 고장이 난 상태
- $P_{14}$ : 시스템이 안전하지 않은 고장 상태

그림4. 단일 대기 이중계의 상태도

즉, 결함을 검지하는 로직이 완전성을 가지기가 어렵다는 것이다. 그러므로, 이 시스템은 결함 수용능력에 따라 시스템의 신뢰도가 달라질 있다. 이 시스템의 마코브 모델은 그림 4와 같이 나타낼 수 있다. 만약 시스템이 완전한 결함 수용능력을 가지게 되면 이 시스템은  $P_{US}$ 와  $P_{FU}$ 의 상태는 고려되지 않지만 소프트웨어적인 결함 검출 시스템에서는 결함 수용능력을 완전화할 수 없는 단점이 있다. 결국 시스템의 상태도는 결함을 어느 정도까지 검출할 수 있는가에 따라 시스템의 신뢰도가 결정된다는 것을 알 수 있다. 결국, 결함 수용능력인  $o$ 의 값에 따라 시스템의 신뢰도 및 안

전도에 영향을 미칠 수 있고, 여기에 사용된 부품은 결국 단일 시스템의 두배와 같게 된다. 그러므로, 시스템의 상태 방정식은 그림 4에서 보는 바와 같이 식(6)로 표현될 수 있다.

$$\begin{bmatrix} P_{11}(t+\Delta t) \\ P_{10}(t+\Delta t) \\ P_{US}(t+\Delta t) \\ P_{FU}(t+\Delta t) \\ P_{FS}(t+\Delta t) \end{bmatrix} = \begin{bmatrix} 1-2\lambda\Delta t & \mu\Delta t & 0 & 2\mu\Delta t & 2\mu\Delta t \\ 2\lambda\Delta t\sigma & 1-\lambda\Delta t-\mu\Delta t & 0 & 0 & 0 \\ \lambda\Delta t(1-\sigma) & 0 & 1-\lambda\Delta t & 0 & 0 \\ \lambda\Delta t(1-\sigma) & \lambda\Delta t(1-\sigma) & \lambda\Delta t & 1-2\mu\Delta t & 0 \\ 0 & \lambda\Delta t\sigma & 0 & 0 & 1-2\mu\Delta t \end{bmatrix} \begin{bmatrix} P_{11}(t) \\ P_{10}(t) \\ P_{US}(t) \\ P_{FU}(t) \\ P_{FS}(t) \end{bmatrix} \quad (6)$$

### 3.3. 듀얼 시스템

이 시스템은 그림5에 나타난 것과 같이 CPU나 모든 전자소자가 각각의 데이터가 입/출력이 될 때, 어드레스 버스, 데이터버스가 하드웨어를 사용한 데이터의 비교에 의해서 결함을 검지하는 기법을 가진 구조를 가지게 된다.

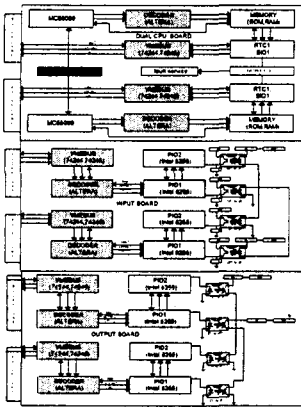
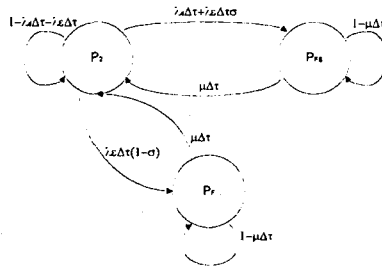


그림 5. 듀얼 시스템의 구조



- $P_1$ : 시스템이 고장없이 동작하는 상태
- $P_{FS}$ : 시스템이 안전측으로 동작하는 상태
- $P_F$ : 시스템이 고장이 발생하는 상태

그림 6. 듀얼 시스템의 상태도

이 시스템은 하드웨어로 결함을 검출하는 구조이다. 그러므로, 결함 검출 회로가 보드내의 데이터 버스, 어드레스 버스, 제어버스 상에서 두 개의 시스템의 동기 동작에 의해서 동작하므로, 결함검출 회로가 고장이 나지 않는 경우 시스템은 안전측으로 동작한다. 그림 6은 시스템의 상태도인데,  $\lambda_a$ 는 시스템의 고장율,  $\lambda_e$ 는 결함 검출 소자(ALTERA)의 고장율,  $\mu$ 는 수리율이고,  $\sigma$ 는 결함 수용 범위율(fault coverage)이다. 즉, 결함 검출기가 결함을 검지할 수 있는 범위를 나타낸다. 그러므로, 결함 검출 로직이 고장이 발생하지 않는다면 항상 고장 안전 모드로 전환이 된다. 이 시스템에 사용된 소자의 개수는 표3과 같다.

표3. 듀얼 시스템에 사용된 전자소자 개수

부품	갯수	부품	갯수
MC68000	2	ROM(27C010)	4
RAM(681000)	4	SIO(8530)	2
RTC(DS1284)	2	74LS244	12
74LS245	8	OSCILLATOR	2
PIO(8255)	10	EPM7128LC84	5
TLP621_4	12	TLP523_4	12

그림 6의 상태에 대한 방정식을 이끌어보면 식(7)와 같다.

$$\begin{bmatrix} P_2(t+\Delta t) \\ P_{FS}(t+\Delta t) \\ P_F(t+\Delta t) \end{bmatrix} = \begin{bmatrix} 1-\lambda_a\Delta t-\lambda_e\Delta t & \mu\Delta t & \mu\Delta t \\ \lambda_a\Delta t+\lambda_e\Delta t\sigma & 1-\mu\Delta t & 0 \\ \lambda_e\Delta t(1-\sigma) & 0 & 1-\mu\Delta t \end{bmatrix} \begin{bmatrix} P_2(t) \\ P_{FS}(t) \\ P_F(t) \end{bmatrix} \quad (7)$$

### 3.4. 듀얼 듀플렉스 시스템

이 시스템은 듀얼 시스템이 대기 이중계 구조로 설정된 시스템으로 그림 7에 나타나 있다. 하드웨어로서 결함을 검지하는 구조를 가지기 때문에 완전한 결함 검지기능을 가질 수 있게 된다. 그러므로, 단일 이중계 시스템이 가지는 단점을 하드웨어 결함 검지회로를 첨가해서 구성될 수 있다. 이 시스템도 마찬가지로 결함 검출 로직이 고장이 나지 않는다면 고장 안전 모드로 전환된다. 즉, A에서 결함이 검지되면, B로 전환을 하게 된다. 여기서  $\lambda_{da}$ 는 듀얼 듀플렉스 한 개의 시스템의 고장율이고,  $\lambda_{ea}$ 는 결함검출 회로와 B보드로 전환스위치 회로(ALTERA, 8255)의 고장율이다.  $\sigma$ 는 시스템이 결함검출을 할 수 있는 결함 수용범위율로서 단일 듀플렉스 시스템보다는 완벽한 값을 가질 수 있는 특징을 가진다. 그러므로, 이러한 결함검출 회로의 개발이 많은 관건이 되고 있다.

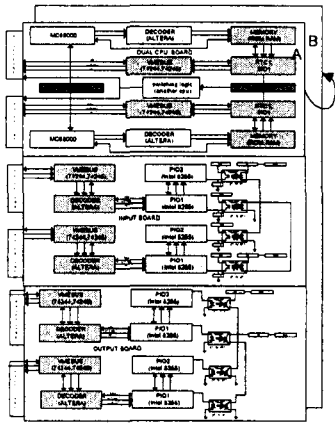
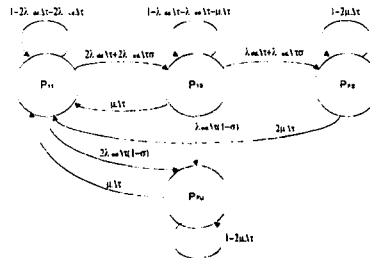


그림 7. 듀얼 듀플렉스 시스템 구조



- $P_{11}$ : 두개의 듀얼 시스템이 고장이 없는 상태
- $P_{10}$ : 한개의 시스템이 동작하는 상태
- $P_{FS}$ : 안전한 고장이 발생한 상태
- $P_{US}$ : 불안정한 고장이 발생한 상태

그림 8. 듀얼 듀플렉스 시스템의 상태도

이 시스템의 상태도는 그림 8과 같고, 이 시스템의 방정식을 유도하면 식(8)과 같다.

$$\begin{bmatrix} P_{11}(t+\Delta t) \\ P_{10}(t+\Delta t) \\ P_{FS}(t+\Delta t) \\ P_{FU}(t+\Delta t) \end{bmatrix} = \begin{bmatrix} 1-2\lambda_{da}\Delta t-2\lambda_{ea}\Delta t & \mu\Delta t & 2\mu\Delta t & \mu\Delta t \\ 2\lambda_{da}\Delta t+2\lambda_{ea}\Delta t\sigma & 1-\lambda_{da}\Delta t-\mu\Delta t-\lambda_{ea}\Delta t & 0 & 0 \\ 0 & \lambda_{da}\Delta t+\lambda_{ea}\Delta t\sigma & 1-2\mu\Delta t & 0 \\ 2\lambda_{ea}\Delta t(1-\sigma) & \lambda_{ea}\Delta t(1-\sigma) & 0 & 1-\mu\Delta t \end{bmatrix} \begin{bmatrix} P_{11}(t) \\ P_{10}(t) \\ P_{FS}(t) \\ P_{FU}(t) \end{bmatrix} \quad (8)$$

### 4. 시뮬레이션 및 고찰

각 시스템 시스템에 대한 신뢰도는 식(5),(6),(7),(8)의 미분 방정식을 풀면 구할 수 있다. 이 때 시스템의 신뢰도, 안전도와 MTTF는 시스템이 갖는 고유의 특성이 되므로, 수리율  $\mu=0$ 로 놓고 구해야 한다. 표4는 각 시스템의 신뢰도, 안전도와 MTTF를 나타낸다.

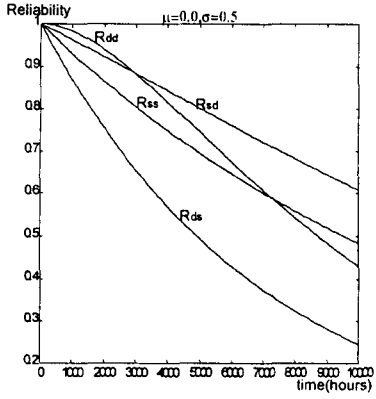


그림 9. 각 시스템의 신뢰도 I

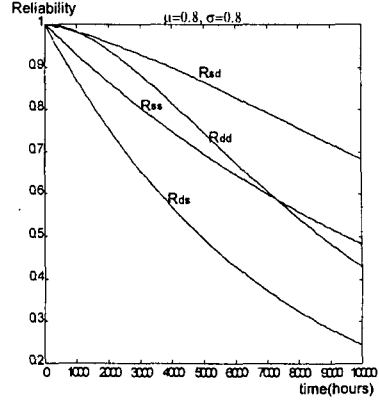


그림 10. 각 시스템의 신뢰도 II

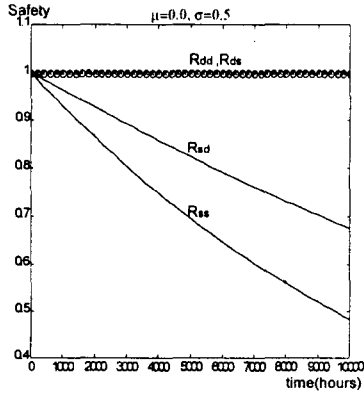


그림 11. 각 시스템의 안전도 I

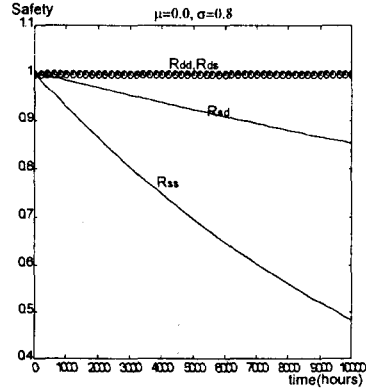


그림 12. 각 시스템의 안전도 II

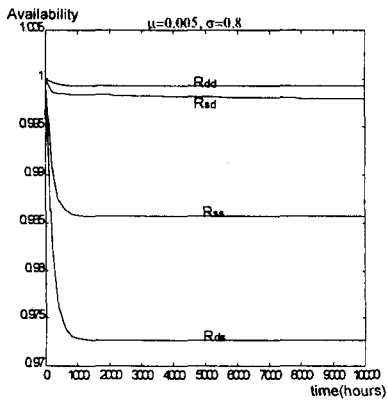


그림 13. 각 시스템의 가용도 I

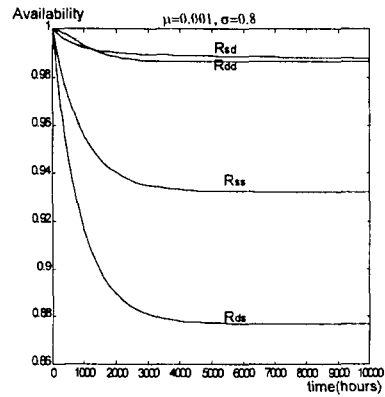


그림 14. 각 시스템의 가용도 II

표4. 각 시스템의 신뢰도, 안전도 와 MTTF( $\mu=0.0, \sigma=0.8$ )

	신뢰도( $R(t)$ )	안전도( $S(t)$ )	MTTF(hours)	고장율
단일 시스템(ss)	$P_o$	$P_o$	13788.9	$\lambda = 72.522e-6$ $\lambda_d = 140.4836e-6$ $\lambda_{dd} = 140.4216e-6$ $\lambda_e = 0.0012e-6$ $\lambda_{ed} = 0.0632e-6$
단일 듀플렉스(sd)	$P_{11} + P_{10} + P_{US}$	$P_{11} + P_{10} + P_{US} + P_{FS}$	19304.5	
듀얼 시스템(ds)	$P_2$	$P_2 + P_{FS}$	7118.21	
듀얼 듀플렉스(dd)	$P_{11} + P_{10}$	$P_{11} + P_{10} + P_{FS}$	10677.3	

신뢰도에 대한 시스템의 특성곡선은 그림 9와 10에 나타나 있다. 그림 9와 10의 차이는 각각 시스템은 결합 수용범위  $\sigma$ 의 값에 따라 신뢰도 곡선의 특성이 다르게 나타난다는 것을 알 수 있다. 그러므로, 시스템을 설계할 때,  $\sigma$ 의 값에 대한 시스템의 설계에 따라 시스템의 특성이 다르게 나타나는 것을 알 수 있다. 그림 9에서는 3000시간까지는 듀얼 듀플렉스 시스템이 가장 높은 신뢰도를 가지고, 그 이후부터는 단일 듀플렉스 시스템이 가장 높은 신뢰도를 가진다. 그림 10에서도 1500시간까지는 가장 높은 신뢰도를 가지고, 나머지는 단일 듀플렉스 시스템이 가장 높은 신뢰도를 가진다. 그러므로, 결합 수용능력( $\sigma$ )이 시스템의 신뢰도, 가용도에 지대한 영향을 끼친다는 것을 알 수 있다. 그림 11은 표4의 안전도에 대한 방정식의 시뮬레이션이다. 여기서 듀얼 시스템이나, 듀얼 듀플렉스 시스템은 안전도가 거의 1로 나타난다. 그 이유는 시스템의 결합 검출을 하드웨어로 이용하기 때문에 즉, 안전도에 미치는 고장율이 작기 때문에 두 개의 시스템의 안전도가 높다는 것을 알 수 있다. 결국은 시스템의 안전도에 대한 전이 고장율은 결합 검지 소자의 고장율이 된다. 그렇기 때문에 시스템의 안전도는 결합 검출기의 고장율에 따라 다르게 나타날 수 있다. 그리고, 그림 12에서 보면 결합 수용율이 달라져도 듀얼 시스템에 대한 안전도는 변함이 없고, 단일 듀플렉스 시스템은 안전도가 다르게 나타나는 것을 알 수 있다. 즉, 높은 결합 수용범위를 갖는 시스템이 더욱더 안전도가 높다는 것을 알 수 있다.

그림 13와 14는 각 시스템의 가용도를 나타낸다. 일종의 신뢰도로 볼 수 있지만 가용도는 수리율에 따라 시스템의 특성이 다르게 나타난다. 가용도는 수리율을 포함하는 시스템의 특성을 나타내기 때문에 수리율  $\mu=0.005, \mu=0.001$ 로 가정하고, 계산한 시스템의 가용도 곡선이 그림 13와 14에 나타나 있다. 그림 13에서는 가용도가 듀얼 듀플렉스 시스템이 가장 높고, 그 다음이 단일 듀플렉스, 단일 시스템, 듀얼 시스템 순으로 나타나고, 그림 14에서는 수리율에 따라 시스템의 가용도의 특성이 다르게 나타난다는 것을 볼 수 있다. 그러므로, 시스템의 특성을 결정짓는 요소로서 수리율, 결합 수용능력, 고장율에 따라서 설계된 시스템의 신뢰도, 안전도, 가용도가 다르게 나타나는 것을 알 수 있다. 그리고, 각각의 시스템의  $\sigma=0.8$ 일 경우 각 시스템의 MTTF는 표1에 나타나 있다. 가장 높은 MTTF를 가진 시스템은 단일 듀플렉스 시스템에서 가장 높게 나오고, 그다음은 단일 시스템, 듀얼 듀플렉스 시스템, 듀얼 시스템의 순으로 나타난다. 마찬가지로 MTTF도 시스템의 결합 수용능력에 따라 다르게 나타난다.

### 5. 결론

본 논문에서는 단일 시스템, 단일 듀플렉스 시스템, 듀얼 시스템, 듀얼 듀플렉스 시스템의 구조에 대해서 MC68000을 기반으로 한 시스템의 구조를 설계를 하였으며, 각각의 시스템에 대한 신뢰도, 안전도, MTTF와 가용도의 특성이 어떠한지를 알아보았다.

●시스템의 신뢰도는 결합 수용능력의 값에 따라 시스템의 특성이 결정된다. 설정된 결합 수용능력에 따라 다른 신뢰도의 값을 나타내는 것을 알 수 있었다. 처음 일정한 시간동안 시스템의 신뢰도는 듀얼 듀플렉스 시스템이 가장 높고, 다음은 단일 듀플렉스 시스템이 가장 높은 신뢰도를 가지



는 것을 알 수 있었다.

●시스템의 안전도는 결함 수용능력(fault coverage)에 따라 단일 듀플렉스 시스템의 특성이 다르게 나타난다는 것을 알 수 있었고, 결국은 하드웨어 결함 검출기를 이용한 듀얼 시스템, 듀얼 듀플렉스 시스템의 구조가 결함 수용 능력에 상관없이 높은 안전도를 나타낸다는 것을 알 수 있다. 이 이유는 제안된 시스템에서 사용된 결함 검출소자의 낮은 고장율로 인한 전체 시스템의 안전도가 높아짐을 나타낸다. 즉, 비교기의 고장율과 결함 수용능력이 시스템의 안전도를 결정한다.

●가용도는 각각의 시스템의 수리율과 결함 수용능력에 따라 다르게 나타난다는 것을 알 수 있었다. 결국 시스템을 얼마나 빨리 복구를 하느냐에 따라 단일 듀플렉스와 듀얼 듀플렉스 시스템에서 가용도의 우위가 결정된다는 것을 알 수 있었다.

결국 듀플렉스 시스템의 설계에 있어서 시스템의 결함 수용능력이 중요한 요소로서 두 개의 듀플렉스 시스템의 신뢰성에 영향을 미치는 것을 보았고, 안전도가 요구되는 시스템일 경우에는 확실히 듀얼 듀플렉스 시스템 구조가 더 우수하다는 것을 볼 수 있다. 그러므로, 안전도가 중시되지 않는, 교환기같은 시스템은 전체적인 시스템 특성을 볼때는 단일 듀플렉스 시스템의 구조가 적당하다고 볼 수 있고, 고속철도나 항공기와 같이 인간의 생명이 중시되는 시스템에서는 높은 안전도를 확보하기 위해서는 듀얼 듀플렉스 시스템 구조로 가는 것이 바람직하다고 볼 수 있다. 그러므로, 앞으로의 당면과제는 완벽한 결함을 검지할 수 있는 결함 수용능력을 높이는 시스템의 설계라고 할 수 있다.

## 참고 문헌

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