技術論文

3중 비행제어시스템의 다중화 기법 설계

박성한*, 김재용*, 조인제*, 황병문*

Redundancy Management Design for Triplex Flight Control System

Sung-Han Park*, Jae-Yong Kim*, In-Je Cho* and Byung-Moon Hwang*

ABSTRACT

Satisfying the same probability of loss of control and essentially two fail operative performance with a triplex computer architecture requires a lot of modification of the conventional redundancy management design techniques, previously employed in quadruplex digital flight control computer. T-50 FCS for triplex redundancy management design applied an advanced digital flight control architecture with an I/O controller which is functionally independent of the digital computer to achieve the same reliability and special failure analysis and isolation schemes for fail operational goals with a triplex configuration. The analysis results indicated that the triplex flight control system is to satisfy the safety requirement utilizing the advanced flight control techniques and the system performance of the implemented flight control system was verified by failure mode effect test.

초 록

3중 비행제어시스템이 종래의 4중 비행제어시스템과 유사한 수준의 시스템 신뢰성과 이중 결함시의 안전한 운용성능을 제공하기 위해서는 기존의 고전적인 다중화 설계기법에 많은 변경과 수정이 필요하다. 이에 따라 국내에서 개발된 고등훈련기급의 3중 비행제어시스템 다중화 설계기법은 4중 시스템과 동일한 수준의 생존성을 확보하기 위해서 3중 시스템의 핵심인 비행제어컴퓨터의 입출력 프로세서와 메인 프로세서를 기능적으로 분리시켜 상호 고장에 대한 영향성을 최소화키고, 시스템의 치명적인 결함을 검출하기 위해서 특별한 고장 분석 기법과 격리 알고리즘을 적용하여 비행제어시스템의 안정성과 신뢰도가 보장되도록 설계하였다. 본 논문은 이러한 다중 시스템 구조와 고장관리 설계기법을 소개하고 설계된 3중 비행제어시스템의 손실율 분석을 통해서 기존 신뢰성 요구도가 만족됨을 해석적으로 입증하였으며, 또한 3중 비행제어시스템의 각종 고장모드에 대한 시스템 영향성 및 안정성 시험을 통해서 그 성능을 검증하였다.

Key Words : Triplex Flight Control System(3중 비행제어시스템), Redundancy Management (다중관리)

Ⅰ. 서 론

비행제어시스템의 기능 손상은 항공기 안전에 치명적인 영향을 미치는 만큼 최대한의 신뢰성을 보장하도록 설계되어져야 한다. 따라서 비행제어시스템은 이러한 신뢰성 증대를 위해서 적절한

† 2009년 9월 24일 접수 ~ 2010년 1월 29일 심사완료
* 정회원, 한국항공우주산업(주)
교신저자, E-mail : shpark73@koreaaero.com
경남 사천시 사남면 유천리 802번지

다중화 설계가 필수적이며 이를 위해서 3중 혹은 4중의 시스템을 구성하는 것이 일반적이다. 또한 비행제어시스템 신뢰성을 충족시키는 범위 내에서 가급적 가볍고 부피가 작으며, 기술적으로 도달 가능한 시스템을 설계하는 것이 비행제어시스템 설계의 궁극적인 목적이 된다.

일반적인 3중 비행제어시스템에서 2중의 손상을 입었을 때에 별도의 백업 시스템에 의존하지 않고 정상적인 운용을 하기 위해서는 기존 F-16 혹은 F-18과 같은 4중 시스템에 적용하던 다중화 설계 기법들은 더 이상 효력을 발휘하지 못하게 된다. 따라서 전통적인 비행제어시스템에서 통용되고 있는 신뢰성 요구도를 충족시키기 위해서는 3중의 비행제어시스템에 새로운 방식의 다중화 설계 기법을 요구하게 된다.

본 논문에서 제시하고 있는 3중 비행제어시스템의 다중화 설계기법은 미공군 및 해군과 NASA가 당시 General Dynamics사(현 Lockeed Martin사)와 공동으로 연구한 AFTI/F-16 개발 프로그램을 통해 확보된 비행제어시스템 설계기법을 바탕으로 두고 있다. 특히 NASA Dryden 연구소는 1970년대 초반에 이미 Apollo 11호에 탑재된 비행제어컴퓨터를 F-8C에 장착하여 최초의 DFBW(Digital Fly-by-wire)를 개발하였으며, 그 이후에 비행제어시스템의 3중화를 통해서 해당 기술의 개발 경험을 가지고 있었다. 이러한 개발 경험이 AFTI/F-16 개발 프로그램에서 NASA와 General Dynamics의 공동개발을 통해 실증적 기술의 토대를 마련하게 된다. 또한 이 기술은 향후 Lockheed Martin사에서 개발하는 모든 DFBW 항공기 설계의 기본이 되었고 국내 고등훈련기 개발을 위한 비행제어시스템 설계기술의 근간을 이루게 되었다.

본 설계개념의 기본목적은 하드웨어 자체의 신뢰성 증가를 크게 요구하지 않은 채로 3중 디지털 시스템을 개발하여 이의 신뢰성이 기존 4중 시스템과 유사한 수준을 유지할 수 있는 방안을 고려하는 것이다. 따라서 새로운 3중 비행제어시스템의 다중화 설계 기법은 기존 4중 시스템과 동일한 수준의 생존성을 확보하기 위하여 비행제어

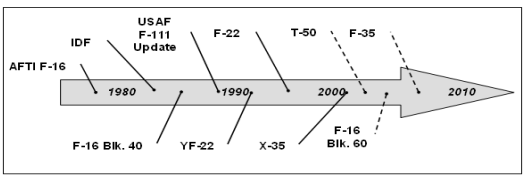

Fig. 1. Triplex FCS Development History

컴퓨터의 입/출력 프로세서(IOP : Input/Output Processor)와 메인 프로세서를 기능적으로 분리시켜 각각 독립적인 구조로 설계하고, 입력단과 출력단의 치명적인 결함으로 인해 발생 가능한 항공기의 안전성을 확보하기 위해 제어법칙의 재형상 모드를 부가적으로 설계하였다. 또한 결함의 정도를 치명적인 것과 정상 비행에 영향이 없는 사소한 것으로 구분하기 위하여, 개발된 3중 비행제어시스템에는 보편적인 아날로그 설계 기술에 의하여 손상을 감지하고 디지털 적인 방법에 의하여 손상 부위를 차단하는 손상 진단 및 관리절차를 단계적으로 수행하는 방안을 고려하여 설계하였다. 이 기술은 기존 프로그램에서 광범위한 실험을 통하여 그 효과가 입증된 바 있으며 하드웨어나 소프트웨어의 독립적인 손상 이외에도 하나의 손상 발생이 상호 간 영향을 미치는 경우 등을 시험하기 위해서 HWIL(Hardware-in-the-Loop) 시험환경에서 고장모드 시험을 통해서 그 성능이 입증되었다.

II. 본 론

2.1 비행제어시스템의 손실율(PLOC)

일반적으로 특정시간 동안의 하드웨어 신뢰도와 고장율은 아래와 같이 표현된다.

고장에 대한 누적분포함수(CDF, Cumulative Distribution Function)인 F(t)는 특정시간 동안 고장이 일어날 수 있는 확률을 말하며, 신뢰도(Reliability) R(t)는 특정시간 동안 고장 없이 시스템을 운용할 수 있는 확률을 말한다.

$$F(t) = P(\underline{t} \leq t),\ R(t) = P(\underline{t} > t) \quad (1)$$

where : t = Time to system failure
$\underline{t}$ = Some specified period of time

신뢰도는 0과 1사의의 정량적인 값으로 표현되며, F(t)는 신뢰도와 반대되는 개념으로 t 시간 동안 고장이 발생할 확률이기 때문에 R(t)와 F(t)의 합은 항상 1이다.

$$R(t) = 1 - F(t) \quad (2)$$

만약 운용시스템의 고장분포가 지수분포 형태를 따르고, 단위시간에 발생하는 고장회수인 고장률(λ, Failure Rate)로 신뢰도를 표현하면 아래와 같다.

$$R(t) = e^{-\lambda t}, \qquad F(t) = 1 - e^{-\lambda t} \quad (3)$$

이를 테일러 시리즈로 전개하면 다음과 같다.

$$F(t) = \lambda t - \lambda^2 t^2/2! \ldots\ldots (-1)^{n-1} (\lambda^n t^n/n!) \quad (4)$$

여기서 MTBF = 1/λ 이기 때문에

$$F(t) = t/MTBF - t^2/2(MTBF)^2 + \ldots\ldots \quad (5)$$

또한 MTBF가 ≫ 1 이면 F(t)는 첫 번째항에 의해 거의 결정되어지기 때문에 아래와 같이 정의할 수가 있게 된다.

$$F(t) = t/MTBF \quad (6)$$

3중 시스템의 경우 시스템의 채널별 고장확률을 p라고 가정하면 채널별 가동확률은 (1-p)가 되며, 모든 채널이 정상동작 하는 경우로부터 전 채널이 손상되는 경우의 수는 아래와 같이 된다.

Table 1. Number of Case in Failure

no failure	1 failure	2 failure	3 failure
$S_1S_2S_3$	$F_1S_2S_3$	$F_1F_2S_3$	$F_1F_2F_3$
	$S_1F_2S_3$	$F_1S_2F_3$	
	$S_1S_2F_3$	$S_1F_2F_3$	

Note : S = Success branch, F = Failure branch

따라서 최소한 n개의 채널이 정상 동작하기 위한 성공률의 계산은 아래와 같다.

Table 2. Probability of Failed Case

No. of Failure	No. of Ways	Probability
r = 0	1	$1p^0(1-p)^3$
r = 1	3	$3p^1(1-p)^2$
r = 2	3	$3p^2(1-p)^1$
r = 3	1	$1p^3(1-p)^0$

$$P_{[\text{exactly r failures in n trials}]} = nCr \times p^r(1-p)^{(n-r)} \quad (7)$$

3중 시스템에서 2중의 손상상태에서도 별도의 백업 시스템 없이 운용을 가능케 하여, 기존의 4중 시스템과 동일한 손실율을 보장하기 위해서는 새로운 개념의 다중화 설계기법이 필요하다. 기존의 시스템 구조는 시스템 손상이 발생되었을 때, 그 손상정도가 항공기 비행안전에 미치는 영향에 치명적인 고장인지 아니면 허용 가능한 고장인지를 구분하지 못했다. 그러나 만약 손상의 치명성 여부를 판단할 수 있다면 치명적인 결함을 시스템 내에서 제거함으로서 항공기의 생존성을 높이고 셀프테스트(Self Test) 요구도를 낮출 수가 있게 된다. 따라서 치명적인 결함에 의한 시스템의 손실율(PLOC, Probability of Loss of Control)을 정의하기 위해서는 3중 시스템의 2중 고장 조건에서 고장 난 채널을 선택하는 것과 같이 치명적인 결함만이 고려될 것이다. 이를 위해 주어진 식 (6)의 고장확률들 중에서 시스템 운용에 치명적인 고장(Critical Failure)과 그렇지 않은 고장(Non-critical Failure)을 구분하기 위하여 시스템 운용상에 치명적인 고장확률을 다음과 같이 정의한다.

$$F_{cr}(t) = t/MTBCF \quad (8)$$

3중 시스템의 손실율을 계산하기 위에서 식(7)에 고장확률 $F_{cr}(t)$를 대입하면 다음과 같은 계산식을 얻을 수 있다.

$$PLOC=[T^2 \times {}_3C_2 \times (1-ST)]/MTBCF^2, \quad MTBCF \gg 1 \quad (9)$$

where : PLOC = Probability Loss-Of Control
T = Time (1 flight hour for this study)
ST = Self Test coverage (% of critical faults that can be detected and isolated)
MTBCF = Mean Time Between Critical Failures
= MTBF / (% of faults that cause loss of function)

어떤 다중시스템에서 고장으로 고려될 수 있는 경우는 두 가지이다. 만약 시스템의 모든 채널이 고장이라면 해당 시스템이 더 이상 운용할 수 없다는 것이 분명하다. 그러나 이러한 경우는 극히 드물기 때문에 우리는 또 다른 경우를 고려해야만 한다. 만약 3중 시스템에서의 한 채널이 고장이라면 그것은 나머지 두개의 정상적인 채널에 의해서 쉽게 검출이 가능하다. 그러나 이러한 첫 번째 고장 이후에 또 다른 고장이 추가적으로 발생한다면, 다중 관리 소프트웨어는 남은 두개의 채널 중에서 하나를 선택해야만 한다. 이러한 경우에 만약 셀프테스트 기능이 없다면 고장이 없는 정상 채널을 선택할 가능성은 단지 50%이다. 그러나 이러한 경우를 위해서 셀프테스트 기능이 설계되어져 있다면, 정상적인 채널을 선택할 가능성이 50% 이상으로 증가하게 된다.

2.2 비행제어시스템의 손실율 요구도

국내 고등훈련기 개발 초기에 설정된 비행제어시스템 손실율 요구도는 기존 항공기의 Class A Mishap Rate(백만 비행시간동안 항공기 손실율) 분석을 통해서 통상적으로 달성 가능한 수치를 제시하게 된다. 이때 조사된 Mechanical 타입의 F-15 항공기의 비행조종계통에 의한 손실율은 백만 비행시간동안 2.2대의 손실이 발생하였으며, FBW 비행제어시스템을 채택한 F-16과 T-38은 백만 비행시간동안 0.91대와 1.7대의 손실이 각각 발생한 것으로 조사되었다.

이러한 항공기의 Class A Mishap Rate 분석을 통해서 고등훈련기에 적용될 비행제어시스템의 손실율을 2.5×10^{-6} (Accident/Flight Hours)으로 설정을 하였는데, 이는 전투기와 공격기에 통

상적으로 적용되는 수치이다. 또한 이 요구도는 이론적으로 항공기의 총운용 기간 동안 6대의 손실을 넘지 않는다는 설계의 요구도로서, 실제 비행제어시스템의 손실율 분석이 상당히 보수적으로 수행되어지기 때문에 실제 운용간 비행제어시스템으로 인한 항공기의 손실율은 예측치보다 상당히 낮출 수 있다는 판단에서이다.

2.3 비행제어시스템의 손실율 분석

비행제어시스템의 다중화 수준(Redundancy Level)의 선택은 하드웨어 생산업체의 기술수준을 사전 조사하여 이를 토대로 다중시스템을 설계하고 설계된 비행제어시스템이 항공기의 안전성 요구도에 충족하는지를 분석하여 최적의 시스템을 선택하게 된다.

신뢰도 분석을 위한 입력 값인 비행제어시스템 각 구성품의 신뢰도 요구조건은 하드웨어 업체의 자료를 참고하여 개발 경험치와 일반적으로 산업계에서 통용될 수 있는 범위 내에서 설정된다. 이렇게 선정된 개발품목과 신뢰성 자료는 비행제어시스템 전체의 신뢰도 예측의 구성요소로 포함된다. 여기서 고려된 주요 신뢰성 입력 값은 비행제어컴퓨터가 채널당 3,000 시간이며 각 조종면의 구동기(Surface Actuator)는 6,000시간 이었는데 이는 하드웨어 업체로부터 공급받은 자료에 개발 경험치가 고려된 것이다. 이와 같이 설정된 각 구성품의 신뢰도 수치를 위에서 제시한 식 (9)에 대입하면 Fig. 2와 같은 결과를 도출할 수 있다. 고등훈련기용 비행제어시스템 설계 초기에는 셀프테스트를 고려하지 않았기 때문에 손실율 분석을 위해서 보수적으로 50%의 셀프테스트 커버리지를 적용하였으며, 'Loss-of-Function (LOF)'은 가장 보수적으로 100%를 적용하였다.

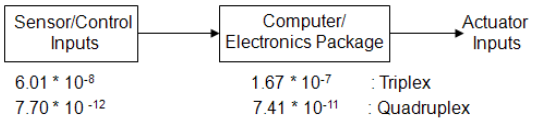

Fig. 2. LOC Calculations For FLCC and Sensors

또한 초기 개념설계 단계에서의 구동기에 대한 MTBF와 LOF 데이터는 여러 종류의 구동기에 적용 가능하도록 상당히 보수적으로 선정하였으며, 구동기의 ST는 조종면당 하나의 구동기를 사용하기 때문에 0%를 적용하였다.

첫 번째 구동기의 LOC 계산을 위해서는 구동기에 'Damped-by-pass' 모드를 고려하여 고장상태에서 Failed Surface로 인해 항공기 손실을 초래하는 것으로 가정하였다(즉, LOC = LOF). 이 경우 구동기의 LOC Rate은 4.17 x 10^{-5}로서 시스템의 다중화에 상관없이 동일하다.

두 번째 LOC 계산에서는 구동기의 재형상 모드를 고려하여 첫 번째 구동기의 고장은 이 모드를 활용하여 95%까지 항공기의 안전성을 보장하도록 하였다(즉, LOC = 5% of LOF). 따라서 이러한 구동기의 재형상 모드를 고려할 경우 구동기의 LOC Rate은 2.09 x 10^{-6}이다.

이와 같이 주어진 하드웨어의 신뢰성에 관련한 입력값을 이용하여 비행제어시스템 전체의 손실율을 분석해 보면 구동기 재형상 모드를 장착한 3중 시스템에서는 2.32×10^{-6}이며, 이는 200대의 항공기를 30년간 운용하는 것으로 가정할 경우 비행조종계통 손상으로 인한 항공기 사고가 5.57대 라는 결론이 나온다. 이는 4중 시스템일 경우 2.09×10^{-6}으로 동일한 조건의 항공기 운영시 5.02대 손상이라는 결론이 나오는데 이는 비행조종계통 손상 발생 빈도 중에서 구동기가 차지하는 부분이 매우크기 때문이다. 그러나 3중 혹은 4중 시스템 모두 비행제어시스템이 요구하는 PLOC를 만족하는 것으로 조사되었으며, 부가적으로 3중 시스템은 4중 시스템에 비해 한 채널이 하드웨어적으로 감소함에 따라서 무게는 17% 감소하고, 부피와 Recurring Cost는 각각 20%, 30%씩 감소하는 것으로 조사되었다. 또한 개발초기에 비행제어시스템에 백업 시스템의 적용 여부를 고려하였으나, 비행제어컴퓨터의 손상이 전체 시스템에서 차지하는 부분이 7.2%로서 백업 시스템을 적용하더라도 항공기 운용 수명 동안 비행제어시스템으로 인한 항공기 손실율은 5.57대에서 5.18대로서 전체 시스템의 신뢰성 향상에 크게 기여를 하지 못했다. 또한 백업 시스템의 적용은 추가적인 비용 상승과 설계의 복잡성을 수반하게 된다.

따라서 이와 같은 조사결과를 토대로 비행제어 시스템의 최종 형상은 백업 시스템이 없는 3중 시스템을 선택하게 된다.

2.4 다중시스템의 구조설계

2.4.1 Output Monitoring 시스템 구조

Fig. 3은 기존 3중 시스템의 기본적인 구조에서 출력단에 모니터/실렉터를 설계한 방식이다. 이러한 시스템 구조는 주로 전통적인 3중 혹은 4중 시스템에서 통용되던 방식이며, 또한 이 시스템에서는 출력 값의 선택 알고리즘으로 MLV (Mid-Level Voter)가 주로 채용되었으나 이를 구현하기 위해서는 부가적인 하드웨어 서킷의 설계가 요구되어졌다.

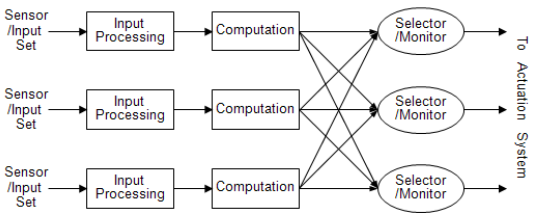

Fig. 3. Output Monitoring Triplex System

이러한 다중 시스템 구조의 PLOC는 앞에서 기술된 식(9)로 부터 다음과 같이 주어진다.

$$PLOC = 3T^2 (1\text{-}ST)/MTBCFb^2 \quad (10)$$

where : MTBCFb= Mean Time Between Critical Failures of Total Branch

비행제어시스템 전체의 손실율을 만족시키기 위해서 요구되는 비행제어컴퓨터의 PLOC는 1.67×10^{-7} 이며, 주어진 MTBCF는 채널당 3,000 시간 이상이 요구되어진다.

여기서 만약 Fig. 3에서와 같이 비행제어 컴퓨터가 물리적으로 메인 프로세서(Computational Elem ents)와 입력 프로세서(Input Processing Devices) 두개의 주요 부분으로 구성되는 경우에는 다음과 같이 MTBF를 근사화 시킬 수 있다.

$$MTBFb^{-1} = MTBFc^{-1} + MTBFi^{-1} \quad (11)$$

where : MTBFb = Mean Time Between Failure of Total Branch
MTBFi = Mean Time Between Failure of Input Processing Devices
MTBFc = Mean Time Between Failure of Computational Elements

따라서 만약 비행제어 컴퓨터(MTBFb)가 메인 프로세서(MTBFc)와 입력 프로세서(MTBFi)로 분리되어진다면 해당 PLOC는 식(10)으로부터 다음과 같은 근사식으로 표현될 수 있다.

$$PLOC = 3T^2(1\text{-}ST)(1/MTBCFc^2 + 2/MTBCFc\times MTBCFi + MTBCFi^2) \quad (12)$$

앞에서 기술하였듯이 초기의 비행제어시스템은 셀프테스트 기능을 고려하지 않았기 때문에 계산식에서의 셀프테스트 커버리지는 50%로 가정한다. 따라서 비행제어 컴퓨터 PLOC 요구도인 1.67×10^{-7} 을 만족시키는 MTBCFc와 MTBCFi를 주어진 계산식으로부터 산출하면 아래 Table 3과 같다.

Table 3. MTBCFc and MTBCFi in single voter System

MTBCFi	3,000	3,500	4,000	4,500	5,000	5,500	6,000	6,500
MTBCFc	N/A	21,000	12,000	9,000	7,500	6,600	6,000	5,571

앞의 표에서와 같이 MTBCFc와 MTBCFi는 서로 반비례 관계로 주어진다. 만약 MTBCFc와 MTBCFi 가 동일한 것으로 가정한다면 대략 6,000시간이 요구되어진다. 이러한 수치는 'State of the Art Technology ' 수준의 요구도 제한치를 거의 만족시킬 수가 있다. 그러나 실제로는 입력 프로세서가 메인 프로세서 보다 더 높은 수준의 신뢰도를 제공하고 있다(이 경우 달성 가능한 하드웨어 요구도 수준이지만 상당히 높은 정도의 요구도이기 때문에 비용이나 개발 위험이 동반 될 수 있다.). 만약 이 경우의 하드웨어 요구도를 낮추기 위해서는 두 가지 방법이 있을 수 있다. 하나는 보다 더 높은 셀프테스트 커버리지를 제공하거나 다른 하나는 신뢰도를 향상시킬 수 있는 개선된 시스템 구조를 설계하는 것이다.

2.4.2 Multi Monitoring 시스템 구조

하드웨어 신뢰도 요구도를 줄이기 위해서, 앞에서 제시된 전통적인 시스템 구조가 변경될 필요가 있다. 새로운 시스템 설계의 주요 개념은 메인 프로세서와 입출력 프로세서의 하드웨어 부분을 독립적인 구조로 설계하고 입력 단에 입력 신호의 고장감지를 위한 모니터/실렉터를 설계하는 것이다. 이러한 개념의 설계 방식은 이미 최초의 Triplex Digital FBW의 개발 사례인 AFTI/F-16 개발 프로그램에서 개발되어졌으며, Lockheed Martin FCS에서 현재 적용중인 설계 개념이다. 이 시스템에서의 메인 프로세서와 입출력 프로세서의 하드웨어 회로는 파워 써플라이를 제외하고는 완전히 독립적이다.

따라서 만약 CPU가 고장이라고 하더라도 IOP는 이러한 고장 조건하에서도 여전히 동작이 가능하게 된다. 또한 Fig. 4에서와 같이 모든 채널은 서로 다른 채널과 물리적으로 연결되어져 있으며, 따라서 입출력 프로세서는 상호 채널간 데이터 통신을 통하여 서로 다른 채널의 입출력 값을 공유하게 된다.

이러한 입출력 프로세서의 데이터 프로세싱은 CPU의 지시에 따라서 매 프레임 마다 수행되며,

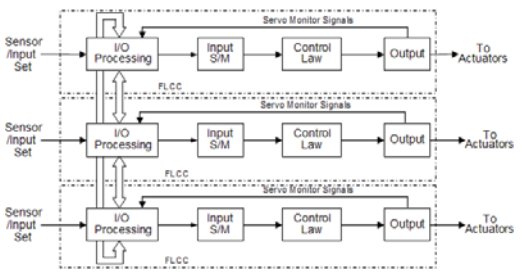

Fig. 4. Multi Monitoring System

만약 해당 채널에서 메인 프로세서단의 고장이 보고 되면 해당 채널의 입출력 프로세서는 프리런 모드(Free Run Mode)를 수행하게 된다.

비행제어컴퓨터 시스템의 이러한 구조적인 변경은 하드웨어의 독립성을 제공함에 따라 고장발생율을 다소 개선시키며, 특히 해당 시스템의 입력단에 모니터/실렉터 기능을 구현할 수 있는 구조적인 장점을 제공한다. 따라서 입력단에 구현된 이러한 모니터/실렉터는 메인 프로세서와 독립적으로 입력단의 고장을 검출할 수 있기 때문에 상기 식에서 2/MTBCFc×MTBCFi 항목을 제거시키는 효과를 얻을 수 있다. 따라서 해당 관계식은 아래와 같이 재정의 할 수 있다.

$$PLOC = 3(1\text{-}ST)(1/MTBCFc^2 + 1/MTBCFi^2) \quad (13)$$

이 식의 계산 결과는 아래 표와 같다. MTBCFc와 MTBCFi는 MTBCF가 4239 시간일 때에 동일한 값을 갖는다. 이러한 결과는 앞에서의 전통적인 시스템 구조 보다 거의 30%가 줄어든 값이다. 따라서 하드웨어 신뢰도 요구도가 그 만큼 줄어들게 된다.

Table 4. MTBCFc and MTBCFi in Multi Monitoring System

MTBCFi	3,500	4,000	4,239	4,500	5,000	5,500	6,000	6,500	7,000
MTBCFc	5,806	4,527	4,239	4,019	3,745	3,575	3,460	3,378	3,317

또한 입력에 대한 2중 고장 상태에서 한개의 유효한 입력을 정확히 분리해낼 수 있는 특별한 손상 진단 및 격리 알고리즘(In-Line Monitoring, Tie Break Monitoring 방식 등)을 설계하거나, 손상된 채널을 정확히 분리하기가 어려울 경우 손상된 입력 신호를 제거하고 안전하게 시스템을 구동시킬 수 있는 재형상 모드를 설계한다면 $MTBCFi^2$를 추가적으로 제거할 수 있다.

$$PLOC = 3T^2(1\text{-}ST)/MTBCFc^2 \quad (14)$$

이러한 결과는 MTBFCc가 3000시간일 때 (Comput- ational Part's ST = 50%) 신뢰도 요구도인 1.67×10^{-7}을 만족하기 때문에 전통적인 시스템 구조보다 50%가 줄어든 결과 값이며, 이 때문에 Computation 하드웨어 개발 요구도가 그만큼 줄어들게 된다. 따라서 메인 프로세서와 입출력 프로세서 부분을 물리적으로 분리시키고 입력단에 부가적인 고장진단 및 격리 알고리즘을 효과적으로 설계함으로서 FLCC의 모든 손상원인이 대부분 Computation 부분에 기인한다는 것을 유추할 수 있다. 또한 만약 이러한 가정들을 충족시키는 시스템설계가 보장된다면 다음과 같은 추가적인 시스템 성능 개선이 가능할 것이다.

고등훈련기의 6개 조종면을 구동하기 위한 각각의 TCO(Total Command Output) 단자에 모니터/실렉터를 추가적으로 삽입하는 것이다. 만약 여기서 어떠한 손상이 감지되었다면 이는 Computation 출력 패스 상의 손상일 수도 있고 6개 조종면 중에서 특정 조종면의 손상일 수도 있다. 따라서 각 조종면 출력에 대한 평균고장시간인 MTBFo가 동일하다고 가정하고 MTBFc = MTBFo× MTBFp/(MTBFo +MTBFp)로 가정한다면, 식(14)의 PLOC 공식을 다음과 같이 표현할 수 있다.

$$PLOC = 3T^2(1\text{-}ST)(1/MTBCFp^2 + 1/MTBCFp\times MTBCFo + 1/6\times MTBCFo^2) \quad (15)$$

where : MTBCFo = Mean Time Between Critical Failure of Output Processing Devices
MTBCFp = Mean Time Between Critical Failure of Computation Processing Devices

여기서 MTBCFp×MTBCFo 항은 식(13)과 달리 서로 종속적인 관계이기 때문에 소거가 될 수 없으나, Inter Channel 모니터에 의해서 특정 프로세스의 고장은 셀프테스트 없이도 다른 두 채널에 의해서 100% 제거가 가능하기 때문에 1/2 만큼 줄어든다(나머지는 출력단의 손상에 의한 TCO 고장을 나타냄). 그리고 식 (15)는 총 6개의 조종면 중에서 하나의 조종면 출력을 고려한 것으로서 $MTBCFo^2$는 1/6로 줄어들게 된다. 만약 프로세스와 출력단의 고장율이 유사하다고 한다면, 주어진 MTBCFc가 3000 시간이기 때문에 MTBCFp와 MTBCFo는 각각 6000 시간이 될 것이다. 또한 만약 하드웨어가 이러한 새로운 구조를 사용하게 된다면, 해당 시스템의 손실율(PLOC)은 9.03×10^{-8}(ST = 50%)으로 월등히 향상될 것이다.

따라서 이러한 구조의 시스템 출력 단에 2중 고장 상태에서 해당 결함 원인을 정확히 판별하여 고장을 적절히 격리시킬 수 있는 알고리즘을 설계할 수 있다면 부가적인 신뢰도 개선을 기대할 수 있을 것이다.

2.5 다중관리시스템의 설계기법

2.5.1 다중입출력신호의고장검출기법

앞에서 표현된 PLOC 계산식은 두 가지의 중요한 그라운드 룰이 만족되어질 때만 유효하다. 첫째는 고장 모드들이 독립적이라야만 된다. 즉, FLCC의 한 채널 혹은 센서 어셈블리의 자이로 등에서 발생된 단일 고장이 FLCC의 다른 채널 혹은 센서 어셈블리의 다른 자이로 등으로 해당 결함이 전파되지 않아야 한다. 이러한 비행제어 시스템 설계를 위해서는 센서 입력 단에서부터

조종면 구동기의 출력 단까지 전체 시스템을 구성하고 있는 각 잉여(Redundant) 채널 간에 고장의 독립성이 보장되어야 한다. 두 번째는 시스템의 전원이 인가된 후에는 해당 시스템에서 무결함 상태가 확보되어야만 한다. 이것은 비행 전에 시스템에 존재하는 잠재적 혹은 미 검출된 고장이 없어야 한다는 것을 나타낸다. 이러한 그라운드 룰은 다양한 Pre-flight Built-in-Test (BIT)의 구현을 통해서 만족시킬 수 있다. 따라서 이렇게 시스템간의 독립성을 만족시키고 시스템의 손실율을 충족시키는 비행제어시스템 설계를 위해서는 다중화 설계 기법의 적용이 반드시 필요하다.

여기서는 비행제어시스템의 특정 고장으로 인해 발생할 수 있는 항공기 과도현상이나 나쁜 조종 특성을 최대한 차단하고, 제어법칙에 사용될 가장 적절하고 유효한 정보들을 제공하기 위해서 입력신호에 대한 효율적인 모니터 기법과 새로운 실렉터 알고리즘을 적용한다.

2.5.2 입력 모니터/실렉터

아날로그 입력 모니터/실렉터는 두 단계의 소프트웨어 알고리즘으로 구성된다. 이 알고리즘은 FLCC로부터 활용되어지는 각각의 아날로그 입력 단에서 수행되어지며, 해당 알고리즘의 첫 단계는 Fig. 5와 같이 일반적으로 고장이 없는 정상운용(Normal Operation) 간에 수행되어진다. 이러한 운용 모드 동안에는 입력단의 고장이 사전에 검출되지 않은 상태로 각 채널은 자기 자신의 입력 값과 옆 채널의 값을 상호 비교하게 된다. 만약 세 개의 입력 값이 허용 가능한 트립 레벨을 벗어나지 않을 경우에는 모든 값들이 유효한 것으로 판단하여 제어법칙 혹은 다른 모듈의 입력 값으로 사용될 하나의 값을 선택하게 된다. 기존 선택 알고리즘 중에서 가장 많이 사용되고 있는 방식은 세 값들의 평균을 구하는 방법과 세 값들 중에서 중간 값을 선택하는 방법이 있다. 이러한 선택 알고리즘 중에서 어느 방식을 적용하는 가는 입력 신호의 특성에 따라서 결정되어진다.

이에 반해서, 세 개의 값들 중에서 임의의 하나가 다른 두 값들에 대해 트립 레벨을 벗어날 경우에는 해당 입력이 모니터에 의해 식별되고 고장이 검출된다. 이 경우 나머지 정상 입력들에 대한 선택 알고리즘은 남은 두개의 입력 값에 대한 평균을 취하게 된다. 또한 유효한 신호 범위를 벗어나는 이러한 경우가 주어진 한계시간(Persistence Limit) 이상동안 지속되면 해당 고장상태는 고장발생(Hard Failure)으로 최종 보고하게 된다.

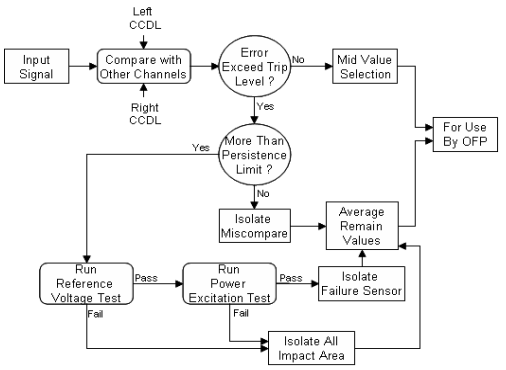

Fig. 5. Normal (No-Fail) operation algorithm

신호 모니터를 통해 고장을 보고 받은 고장관리 기능은 해당 고장을 격리시키기 위해서 상위 레벨 디바이스의 고장상태를 점검할 수 있는 기준전압 테스트(Reference Voltage Test) 혹은 전원 인가 테스트(Power Excitation Test)를 수행하여 그 결과에 따라서 해당 디바이스의 고장격리 절차를 수행하게 된다. 이러한 고장처리의 목적은 주로 고장을 격리하고 해당 시스템이 특정 고장 조건에 대해 사전에 정의된 고장처리 절차에 따라서 고장을 관리하는 것이다.

아날로그 모니터/실렉터 로직의 두 번째 단계는 Fig. 6과 같이 단일 고장 상태에서 운용되어진다. 특정입력 단의 단일 고장 상태는 세 채널의 입력 중에서 단 하나가 고장으로 선언된 것을 의미하며 이때는 고장판별을 위해서 단지 두 채널의 입력들만이 비교를 위한 값으로 사용된다. 만약 이 두 값의 차이가 트립 레벨을 벗어났지만 한계시간을 넘지 않은 경우에는 이전에 계산된값이 유지되며 더 이상의 모니터 프로세싱은 수

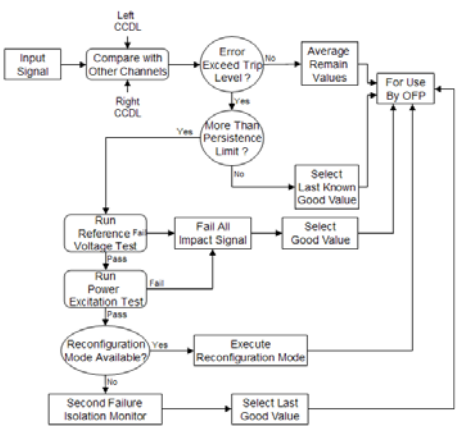

Fig. 6. Single-fail State Operation

행되지 않는다. 그러나 만약 해당 고장조건이 한 계시간까지 지속되면 그 시스템은 심각한 2중 고장 상태에 이르게 되고 이 시점에서는 두개의 입력 중에서 어떤 입력이 고장인지를 쉽게 판단하기가 어렵게 되기 때문에 고장관리 로직이 다시 작동하여 고장상태를 판단하게 된다.

고등훈련기용 비행제어시스템에서는 이러한 고장조건에서 상위레벨의 디바이스 점검 후에 해당 고장 상태가 발견되지 않을 경우에는 2차 고장 격리(Second Failure Isolation) 모니터에 의해서 인라인 모니터(ILM : In-line Monitor) 혹은 타이브레이크 모니터(Tie-Break Monitor)를 추가적으로 수행하여 결함이 발견된 입력을 최종적으로 격리 조치하게 된다. 그러나 만약 이러한 인라인 모니터 혹은 타이브레이크 모니터를 수행할 수 없는 입력신호에 대해서는 해당 입력에 대해서 재형상 모드로 시스템을 변경하게 된다.

디스크리트 입력 모니터/실렉터 로직은 아날로그 입력 처리 로직과 유사한 방식으로 작동한다. 단지 디스크리트 입력은 메모리상의 한 워드 중에서 bit 단위로 저장되어지기 때문에 불 대수(Boolean Algebra)를 이용하여 워드단위로 보팅과 모니터를 수행하게 된다. 디스크리트 입력의 선택 방식은 두개 혹은 세 개의 신호가 유효할 때에는 다수결 원칙(Majority Voting)을 이용하여 수행되고, 남은 두개의 디스크리트 신호가 서로 다를 때에는 고장이 선언되기 전까지 현재의 상태를 유지하게 된다. 만약 고장이 선언되면 재형상 모드(Reconfigured Mode)가 설정되어 일반적으로 비행 중 정상 상태의 값이나 디스크리트 오프 값으로 설정되며 스위치 기능은 효과적으로 차단(Disable)된다.

2.5.3 출력 모니터/실렉터

출력에 대한 모니터/실렉터 로직은 각 채널에 있는 컴퓨터 하드웨어(Computational Hardware)와 구동기 간의 인터페이스를 모니터 한다.

출력 모니터/실렉터는 아날로그 입력 모니터/실렉터의 한계시간 보다 일반적으로 짧은 소요시간(Time Frame)으로 설정되는 것을 제외하고는 동일하게 운용된다. 이는 출력단의 고장이 구동기를 통해 항공기의 거동에 직접적으로 영향을 미치기 때문에 보다 엄격한 소요시간으로 설계를 하는 것이다. 또한 고장의 발생으로 인해 과도한 반응 특성을 차단하기 위해서 어떤 고장은 즉각적으로 격리조치 되기도 한다. 반면에 입력단의 고장은 직접적으로 구동기에 전달되지 않고입력단의 보팅을 통해서 시스템 쪽으로 걸러지기 때문에 출력의 고장과는 영향성 측면에서 다르다. 이해를 돕기 위한 Fig. 7은 고등훈련기 FCS

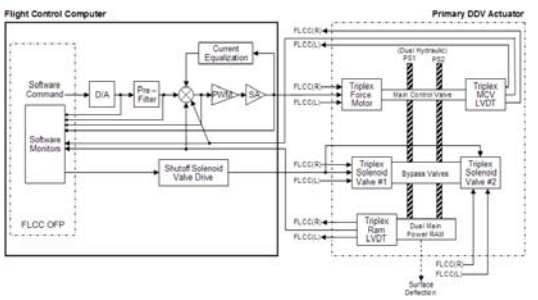

Fig. 7. Flight Control Surface Actuator Diagram

에서 적용된 조종면 구동기와 FLCC 사이의 하드웨어 구성과 신호흐름을 보여주고 있다.

여기서 FLCC 각 채널은 OFP의 일부인 제어법칙에서 계산된 구동기 명령값을 서보엠프 드라이브 일렉트로닉(Servoamp Drive Electronic)을 이용하여 전기적 전류로 변환시키며, 각 채널에서 생성된 이 전류는 MCV(Main Control Valve)에 연결된 3중의 포스 모터에서 전기적으로 합산된다. 이 MCV는 메인 파워 램(Main Power Ram)과 해당 조종면을 움직이도록 구동기실린더 내로 두개의 항공기 유압시스템으로부터 공급되는 유량을 조절하게 된다.

고등훈련기용 FLCC에 설계된 구동기 출력 단의 서보 일렉트로닉 모니터(Servo Electronic Monitor)는 서보 일렉트로닉 하드웨어상의 결함 감지를 위해서 신호 패스 상에서 랩 어라운드(Wrap-around)되어지는 3채널의 포스 모터 코일 전류(Force Motor Coil Current)와 PWM 컴맨드(Command), MCV 위치 피드백(Position Feedback) 값들을 상호 모니터하게 된다. 특히, 무 고장(No Fail) 모니터에서는 이러한 입력 신호들 중에서 어떠한 입력신호도 트립 레벨을 벗어나지 않았을 경우에는 정상 운용을 계속 수행하게 되지만, 트립레벨을 벗어날 경우에는 추가적으로 조종면 명령값을 서로 비교하여 만약 비교된 조종면 명령값들이 트립 레벨을 벗어난 경우 상위레벨 디바이스 점검을 통해 먼저 고장을 격리하게 된다. 그러나 해당 조종면 명령값들이 트립 레벨 내에 존재할 경우는 서보 일렉트로닉 상의 스팀 테스트(Stim Test) 및 -3 전압 테스트(Negative 3 Voltage Test)를 점차적으로 수행하여 신호 경로상의 결함을 감지하고 격리하게 된다. 일차 고장(Single Fail) 모니터에는 남은 2개의 유효 입력신호에 대해서 추가적인 모니터를 수행하게 되며, 만약 고장 감지 시에는 무 고장 모니터와 유사한 방식으로 처리하게 된다.

또한 MCV 모니터는 구동기 상에 스틱(Stuck)과 같은 기계적인 결함을 발견하기 위해서 MCV 피드백 값과 코일 전류 합계(Coil Current Sum)를 비교하여 모니터를 수행하게 된다. 만약 여기서 고장이 검출되면 해당 구동기는 페일-세이프 포지션(Fail-Safe Position)으로 위치하고 제어법칙은 재형상 모드를 통해 항공기를 제어한다.

전통적인 방식의 출력 실렉터/모니터 알고리즘은 비동기(Asynchronous) 시스템에서 채널간의 프로세싱 시간 차이(Time Gap)로 인해서 주기적으로 출력 신호에 대한 모니터와 실렉터를 수행하여 채널 간 출력신호의 차이를 최소화시키기 위해서 해당 로직이 설계되어졌다. 하지만 최근에 적용되고 있는 동기(Synchronous) 시스템은 채널 간 동기화를 수행하고 입력 보팅에 의한 동일 입력신호를 통해서 출력값이 계산되기 때문에 세 채널 출력 값들의 차이가 거의 무시할 정도로 미미하다(Fig. 10 참조). 이것은 기존의 각종 시험을 통해서 그 효율성이 입증되어 점차적으로 출력신호의 실렉터 알고리즘을 배제하는 방향으로 설계가 이루어지고 있다. 따라서 동기 시스템으로 설계된 고등훈련기용 비행제어컴퓨터는 출력 신호의 모니터는 수행하되 출력신호의 실렉터 로직은 초기화루틴을 제외한 정상 운용 간에는 적용하지 않는다.

2.5.4 고장관리(Failure Management) 기법

고장관리 기능은 3중으로 다중화된 컴퓨터 시스템에서 각 하드웨어의 고장진단 기능과 격리 및 관리기능을 구현하여 시스템의 안정된 성능을 보장하기 위한 것이다. 이러한 고장관리 기능은 특히 다음의 두 가지 이유로 인해 시스템의 안전성을 확보하는데 그 중요성이 높다.

첫째, 전기신호는 다양한 원인으로 고장이 발생될 수 있기 때문에 고장원인을 정확히 분석하여 결함이 발생한 디바이스를 적절히 격리시킬 필요가 있다. 예를 들면 결함이 없는(No-Fail) 하드웨어와 아날로그 입력 신호사이의 관계를 묘사

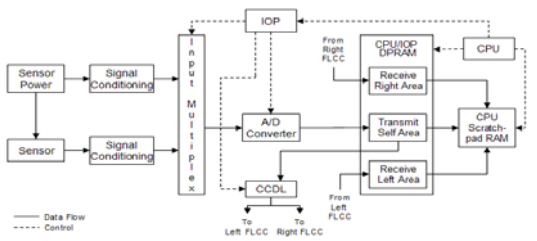

Fig. 8. The relationship between an analog input signal and the hardware

하고 있는 Fig. 8에서 해당 입력 신호가 피치 레이트 자이로(Pitch Rate Gyro)이고, 이 경우에 어떤 고장이 검출되었다고 가정한다면 해당 고장 조건은 자이로의 실제 결함이거나 자이로를 구동시키는 400Hz 전원 공급기의 결함 혹은 아날로그-디지털 변환기로 입력을 공급하는 Multiplex 칩의 결함 혹은 입력 값이 저장된 메모리 셀 등의 결함으로 그 고장 원인이 다양할 수가 있다.

만약 해당 고장이 센서에 제공되는 400Hz 전원 공급기의 결함에 의한 것이면 이 전원 공급기에 의해 구동되는 레이트 자이로들은 모두 해당 결함으로 인해 영향을 받기 때문에 시스템으로부터 고장으로 처리되어야만 한다. 왜냐하면 다른 자이로 입력들은 가로-방향 축(Lateral-Directional Axis) 방향의 항공기 운동이 적을 경우에는 롤 레이트(Roll Rate) 혹은 요우(Yaw Rate) 자이로 모니터로부터 고장 조건이 검출되지 않을 수 있기 때문에 모두 고장 처리되는 것이 타당하다.

만약 이러한 설계를 반영하지 않는다면 가로-방향 축 방향으로 항공기의 급격한 기동 시에 발생된 2중 고장조건에서 두개의 고장 난 신호에 편중되어 실제 유효한 신호를 결함으로 판단할 수도 있게 된다. 그러나 비행제어시스템에서는 이러한 요인으로 발생 가능한 잠재적인 고장원인을 허용해서는 안 된다. Table 5는 고등훈련기용 비행제어시스템에서 적용 중인 여러 가지 전원 소스를 타입별로 분류하고 있다.

Table 5. KTX-2의 Sensor Power Supply 분류

Sensors	Power Supply	비고
Accelerometer	±15Vdc	External Power
Rate Gyro	28Vdc	Buffered Power
Angle of Sideslip	7Vac 3200Hz Power	Buffered Power
Air Data	28Vdc	Buffered Power
Control Stick Transducer	7Vac 3200Hz Power	Main or Buffered Power
Rudder Pedal Transducer	7Vac 3200Hz Power	Main or Buffered Power
Throttle	7Vac 3200Hz Power	Buffered Power

둘째, 이중 고장(Dual Fail)과 같은 특정 고장 조건에서 수행하게 될 부가적인 고장 격리절차를 정의하여 발생가능한 모든 고장 상황에서 시스템을 안전하게 운용하는 것이다. 이차 유사고장(Second Like Failure)은 특정 모니터가 단일고장 상태에서 운용 간에 발생하는 또 다른 고장이 선언된 경우를 의미한다. 이때는 고장을 판단하기 위한 정보가 두개의 입력 신호뿐이기 때문에, 고장이 검출되더라도 정확히 고장을 격리시킬 수가 없게 된다. 이때 만약 추가적인 고장처리에 대한 계획이 없다면 제어법칙에 제공되는 Critical 입력에 대한 심각한 손실과 오류를 발생시킬 수가 있다. 따라서 고등훈련기의 3중 비행제어시스템

에서는 이차 유사고장을 처리하기 위해서 아래와 같은 방법들과 격리 절차가 구현되어졌다.

첫 번째 방법은 고장이 의문시 되는 입력에 의존하지 않고 만족스러운 성능을 달성하기 위해 시스템을 변경하거나 다른 센서들로부터 요구되는 정보를 계산하도록 시스템을 재 형상화시키는 것이다. 제어법칙 재형상화는 최근 항공기상에 항공기의 Loss-of-control을 방지하기 위해서 요구되어지는 것보다 많은 센서 입력을 활용할 수 있기 때문에 입력단의 재형상에 따른 시스템 변경이 가능한 것이다. 또한 항공기 운동방정식상의 입력 변수들을 상수 값으로 처리하도록 재형상 모드를 설정하기도 한다. 그러나 조종면의 재형상화는 항공기의 조종불능 상태(Departure)를 차단시켜 항공기의 안전성을 확보할 수 있으나 조종성(Handling Quality)의 저하를 초래할 수 있다. Table 9는 이전 개발 프로그램에서 적용한 제어법칙 재형상 모드와 현재 고등훈련기의 비행제어시스템에 설계된 재형상 모드를 보여주고 있다.

Table 9. Control Law Reconfiguration Mode

Failure Type	Reconfiguration Strategy	고등훈련기 FCS 적용여부
Discrete Input	Set to Normal Inflight or OFF Value Case by Case	Set to Normal Inflight or OFF Value Case by Case
Normal Accelerometer	Employ Pitch Rate Control System	Non*
Lateral Accelerometer	Set Feedback to Zero	Non*
Pitch Rate Gyro	Synthesize Pitch Rate from AOA and Elevator Position	Non*
Roll Rate Gyro	Set Feedback to Zero	Non*
Yaw Rate Gyro	Set Feedback to Zero	Non*
Angle of Sideslip	Set Feedback to Zero	Set Feedback to Zero
Air Data	Fixed Gain	Fixed Gain
Throttle Twist	Set Input to Zero	Non*
* : Embedded GPS/INS (EGI) data will be used to isolate a second like failure of rate and accelerometer sensor which of the remaining two branches of sensor data is valid and then the FCS will use the last remaining valid rate sensor.		

두 번째 방법은 이차 유사고장 조건에서 남은 두 입력 신호 중에서 유효한 값을 선택하기 위해서 부가적인 모니터링 기법을 설계하는 것이다. 이 방식은 'Coin-flip' 혹은 'Coin-toss'라고 불리는 방식에서 유효값 선택의 정확성을 향상시키기 위하여 기존 시스템에 적용 가능한 하드웨어와 소프트웨어를 추가적으로 설계하는 방식이다. 국내에서 개발된 고등훈련기에는 항공기의 각속도와 가속도 정보를 위해서 가속도계(Accelerometer) 및 레이트 자이로 센서를 기본적으로 장착하고 있으며 부가적으로 항공전자의 EGI 정보를 통해서 동일한 정보를 획득할 수가 있다. 따라서 가속도계 및 레이트 자이로 센서 입력단의 고장관리를 위해서 EGI 소스 데이터를 이용한 타이 브레이킹 모니터를 통해서 이차 유사고장 조건에서 고장이 발생한 입력을 정확히 격리할 수가 있게 된다. 또한 주 조종 입력(Primary Pilot Input : Side Stick, Rudder Pedal, Throttle) 신호에 대한 인라인 모니터(In-Line Monitor)는 이차 유사고장 조건에서 해당 조종 입력 장치에 대한 변위 측정 센서의 총 전압(Sum Voltage)을 점검하게 되는데, 측정된 총 전압이 기대값과 비교하여 허용범위를 벗어나게 되면 해당 입력 신호를 고장으로 판단하여 고장조치를 취하게 된다. 이러한 모니터 방식은 3중 비행제어컴퓨터의 다중화에 상관없이 해당 채널별로 독립적으로 수행이 가능하기 때문에 고장격리를 위해 유효한 기능을 제공하게 된다.

모니터에 의해서 보고된 고장은 고장조건에 따라서 고장 분석을 위한 추가적인 시험을 수행하고 이를 분석하여 고장의 원인을 하위레벨의 디바이스부터 상위레벨의 디바이스까지 계층적으로 점검하게 된다. 이러한 고장분석 절차는 Fig. 9에서 분류된 Failure Hierarchy에 따라서 진행된다.

여기서 상위 레벨의 고장 검출을 위해서는 신호 경로상의 기준 전압 테스트를 수행하거나 Power Excitation Test를 주로 수행하게 되며, 이를 통해서 상위 레벨의 고장(A/D, D/A Converter, Power Supply)을 격리하거나 경로상의 무결성을 검증하게 된다. 또한 CPU와 연관된 상위 레벨의 고장 검출(Channel Fail)은 최근 통용되고 있는 디지털 프로세서 셀프테스트 방식 중에서 Watchdog Timer 및 Parity Check, Illegal I/O Address Detection Test, Stack Overflow 및 Executive Call Trap Check등을 통해서 이루어진다.

끝으로 앞에서 기술한 3중의 다중화 설계기법을 근간으로 설계된 고등훈련기용 비행제어시스템은 HWIL 환경에서 모든 고장조건에 대한 시스템 영향성 및 시스템 성능 검증이 수행되었으며, Fig. 10은 특정 센서 입력단의 2중 고장조건에서 수행된 고장모드의 영향성을 분석한 사례를 보여주고 있다.

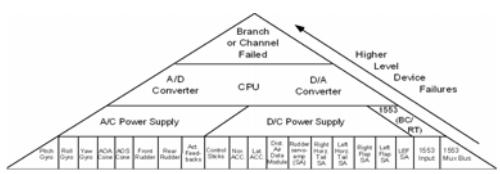

Fig. 9. Failure Hierarchy

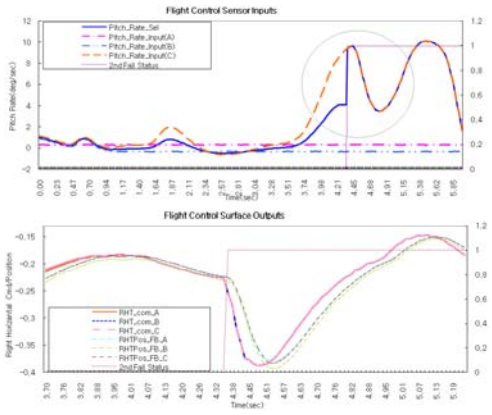

Fig. 10. Pitch Rate Sensor-Dual Failure Condition

HWIL 환경에서 수행된 피치 레이트 입력단의 이중고장 조건(고도 5,000ft, 마하 0.5)에 대한 고장 영향성 분석 결과에서 보듯이 피치 레이트의 일차고장(채널 A) 이후, 이차고장(채널 B)을 주입하더라도 조종사 입력이 인가되기 전까지는 고장이 보고 되지 않는다. 그러나 고장 인가 이후 약 3.3초 만에 조종사 피치 명령에 따라 두신호의 편차가 허용한도를 벗어나고 정상적으로 고장이 감지, 격리되는 것을 확인할 수가 있다. 이러한 고장 감지는 EGI의 피치 레이트 정보를 이용한 타이 브레이킹 모니터를 통해서 정상적인 센서 입력(채널 C) 단을 선택하여 제어법칙으로 제공함으로서 피치 축 조종면 구동이 안정적으로 제어되어 항공기의 안정성을 보장하게 된다.

III. 결 론

국내 고등훈련기 개발 초기의 PLOC 해석 결과는 백업시스템이 없는 3중 비행제어 시스템으로도 당시의 하드웨어 개발기술을 활용하여 제시된 시스템 안전성 요구도를 만족하는 것으로 조사되었다. 그러나 제시된 비행제어시스템 전체의 안정성 요구도를 충족시키기 위한 비행제어 컴퓨터 하드웨어의 개발 요구도를 낮추고 보다 신뢰성 있는 시스템을 보장하기 위하여 개선된 비 행제어 컴퓨터 시스템 구조를 개발하여 적용하였다. 이것은 동일한 비행제어컴퓨터라도 컴퓨터내의 입출력 프로세서와 메인 프로세서를 각각 독립적인 구조로 설계하고 채널 상호간의 인터페이스 방식을 변경함으로서 시스템 손실율을 효과적으로 줄일 수 있도록 설계되었다. 이러한 채널 상호간의 인터페이스 방식은 출력단의 모니터와 입력단의 모니터 및 보팅 설계를 포함한다.

또한 본 논문에서는 Multiple Voting Plane을 가진 다중구조시스템이 고장을 검출하기 위해서 어떻게 모니터를 수행하고 고장을 격리시키는 지를 기술하였다. 특히, 이차 유사고장 조건에서 추가적인 고장을 적절히 처리할 수 있도록 특별한 고장분석 기법과 격리 알고리즘을 설계함으로서 시스템의 안정성과 신뢰성을 현격히 증가시킬 수 있었다.

이러한 다중화 설계 기법들은 단일 입출력 신호와 같은 하위레벨의 고장과 A/D와 D/A 컨버터 혹은 CPU와 같은 상위레벨의 고장 디바이스를 처리하기 위해서 Failure Hierarchy를 활용하여 구현되었으며, 비행제어시스템 시험 단계에서는 각 고장모드에 대한 시스템 영향성 검증 및 시험을 통해서 설계된 고장 알고리즘이 충분히 효과적임을 입증하였다.

향후 이러한 개발기술을 근간으로 다중시스템의 신뢰성 및 안정성을 보다 향상시킬 수 있는 다양한 다중화 설계기법들이 국내에서 개발될 필요가 있을 것으로 판단된다.

참고문헌

1) W. J. Yousey, A. M. Arabian, T. T. Schindler, "AFTI/F-16 DFCS Development Summary - A Report to Industry Redundancy Management System Design", NACEON Conference, May 1983.

2) E. E. Lews, "Introduction to Reliability Engineering", John Wiley & Sons

3) C. L. Seacord, D. K. Vaugbn, "Preliminary Design Study for a Digital Fly-by-Wire Control System for a F-8C Aircraft", NASA Contractor Report, January 1976

4) 서준호 외 "기술시범기 비행제어시스템 고장모드 성능확인과 검증", 무기체계발전세미나, 2008.