技術論文 DOI:10.5139/JKSAS.2010.38.8.813

KUH 임무탑재시스템의 안전성설계 및 검증

김유경*, 김명진**, 김태현***, 임종봉*

Safety Design and Validation of Mission Equipment Package for Korean Utility Helicopter

Yoo-Kyung Kim*, Myung-Chin Kim**, Tae-Hyun Kim*** and Jong-Bong Yim*

ABSTRACT

Integrated data processing for display of flight critical data and mission critical data was conducted without additional display instruments using glass cockpit design. Based on a pre-designed flight critical system and a mission critical system, this paper shows an optimal design of subsystem integration. The design satisfies safety requirements of flight control systems(FCS) and requires minimized modification of pre-designed systems. By conducting integration test using System Integration laboratory(SIL), it is confirmed that the introduced design approach meets the safety requirements of the MEP system.

초 록

안전성 요구수준이 서로 다른 비행필수 데이터(Flight Critical Data)와 임무필수 데이터(Mission Critical Data)의 시현을 처리하기 위해 별도의 독립된 계기를 사용하지 않고 Glass Cockpit 설계를 적용하여 데이터를 통합처리하였다. 본 논문에서는 독립적으로 설계 진행되어온 비행조종계통과 임무탑재시스템의 통합설계를 위해 설계변경을 최소화하면서 비행조종계통에서 요구되는 비행필수 데이터처리의 안전성 요구수준을 만족시키는 최적화 설계를 제안하였다. 비행필수 데이터의 시현을 처리하기 위해 KUH 임무탑재시스템의 핵심구성품인 임무컴퓨터(Mission Computer)의 하드웨어 및 소프트웨어 설계변경을 최소화하였다. 임무탑재시스템의 안전성 요구도(Safety Requirement)를 검증하기 위한 시험절차를 개발하여 임무탑재시스템 통합시험장비(SIL)를 이용한 시험 수행 결과 안전성 요구도가 만족됨을 확인하였다.

Key Words : Mission Computer(임무 컴퓨터), Mission Equipment Package(임무탑재장비), Safety Design(안전성 설계), Flight Critical Data(비행 필수 데이터)

Ⅰ. 서 론

항공기상에서 요구되는 다양하고 복잡한 임무를 성공적으로 수행하기 위해 다기능, 고신뢰도의 임무 탑재 시스템설계가 필수적이다. 고성능 전자부품의 급속한 발전으로 인하여 전자장비의 소형화, 경량화 및 고성능화가 가능하게 되어 현대전에서 요구되는 다양한 기능을 충족시킬 수 있게 되었다. 또한, Glass Cockpit 설계가 적용되어 아날로그 다이얼 및 계기를 대체한 다기능 시현기(Multi-Function Display, MFD)를 이용하여 조종사가 연동조작 항법, 통신, 항공기 상태 모니터링, 비행제어 기능등을 효율적으로 조작하도록 최적화 설계가 진행되어 왔다. 효율적인 시스템

† 2010년 5월 6일 접수 ~ 2010년 7월12일 심사완료
* 정회원, 국방과학연구소
교신저자, E-mail: yoo1029@add.re.kr
대전시 유성우체국 사서함 35-7호
** 정회원, 국방과학연구소
*** 정회원, 한국항공우주산업(주)

Fig. 1. Glass Cockpit Display of KUH (Surion)

시험방안을 연구하여 개발기간 단축 및 저비용 항공전자 시스템 개발 시도가 계속되어오고 있다.

항공기에서 처리하게 되는 데이터는 계기 비행에 요구되는 비행필수데이터와 임무를 수행하기 위한 임무필수데이터에 따라 요구되는 신뢰성 및 안전성이 각각 차별화 된다. 장비간 통신을 제어하고, 조종사의 명령을 수행하는 임무컴퓨터는 항공기의 임무탑재시스템에서 핵심 구성품으로서 현대전에서 요구되는 많은 기능을 수행하기 위해 고성능으로 개발하여야 한다. KUH 임무탑재시스템에서는 비행필수데이터처리를 위해 별도의 추가 장비없이 임무컴퓨터에 동시 설계하여 단순화된 Glass Cockpit(Fig. 1) 설계가 가능했으며 비용절감 및 경량화된 임무탑재시스템을 구현하였다.

본 논문에서는 안전성 요구도 수준이 다른 비행필수데이터 및 임무필수데이터 처리를 한 대의 임무컴퓨터에서 서로 분리하여 제어하였다. 임무컴퓨터의 구조를 소형화, 경량화하고 효율적으로 관리하기 위한 설계내용이 기술되었으며 KUH 임무탑재시스템개발에 적용된 새로운 설계기법 및 시험방안을 제시하였다.

II. 비행필수데이터처리를 위한 설계

2.1 비행필수데이터

본 논문에서 정의하는 비행필수데이터는 MIL-STD-882 [1]에 정의된 Safety Critical Item을 의미한다. 해당 규격에 따르면, 비행필수데이터는 항공기의 비행을 제어 및 유지하기 위해 필수적으로 인지, 제어, 실행 또는 유지되어야 하는 정보로서 잘못된 정보가 인지될 경우 항공기 및 승무원의 치명적 손상을 유발시키는 항공기 체계 및 비행관련 정보이다[1].

해당 정보는 Fig. 2의 Secured Core 구현에 필요한 정보로 관련 기능의 신뢰도가 적어도 10^{-7}이 되도록 설계하는 것이 일반적이다. 실제로, 해당 신뢰도를 만족하기 위해서, 대부분의 항공기는 비행필수데이터가 일반 임무정보(Mission Information)와는 분리(Segregation)되어 처리하

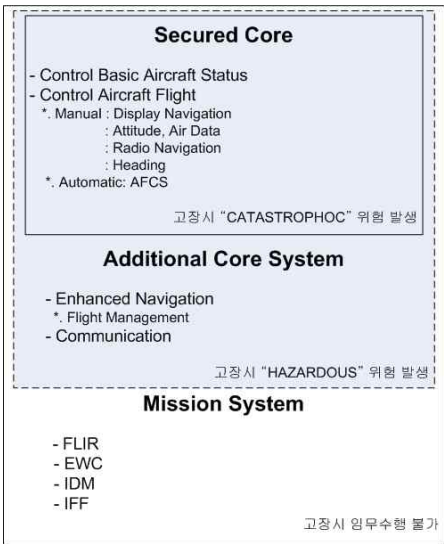


Fig. 2. Safety Requirements for Subsystems

도록 하거나, 관련 데이터 및 부체계(Functional Subsystem)에 대해서 다중화(Redundancy), 백업(Backup) 설계하는 기법을 적용하고 있다.

2.2 타 무기체계 사례 조사

비행필수데이터의 처리 및 시현과 관련되어서 타 무기체계에서 적용된 사례는 다음과 같다.

2.2.1 타기동형 회전익기 사례 1 [2]

비행필수데이터에 대한 처리는 별도의 VMS(Vehicle Management System)에서 이루어진다. 항공기체계 차원에서는 VMS를 중심으로 하드웨어 및 소프트웨어 측면에서 비행필수정보는 100% 분리 및 보호되는 구조 (Fully Secured Scheme)에서 처리되도록 설계되어 있다.

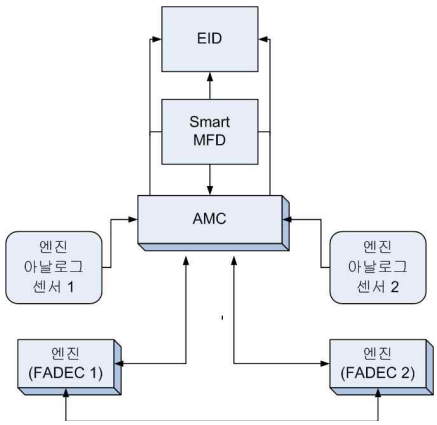


Fig. 3. Block Diagram of VMS

적용된 VMS는 비행필수데이터를 별도 처리하는 AMC (Aircraft Management Computer), 엔진 관련 정보를 시현하는 EID(Engine Instrument Display) 및 기구적인 Board Rack으로 구성이 되어 있다. Fig. 3에 나타난 것처럼, AMC(Aircraft Management Computer)에서 처리된 비행필수데이터는 VMS의 EID(Engine Instrument Display) 및 Smart MFD를 통하여 시현된다. 또한, 동일 엔진으로부터 오는 복수의 정보값이 상이할 경우에는 별도 아날로그 센서로부터 오는 정보를 이용하도록 하여 체계안전성을 높였다.

2.2.2 기동형 회전익기 사례 2

비행필수데이터 처리를 위하여 부분적으로 비행필수데이터를 보호 및 분리처리하는 개념(Partially secured scheme)이 적용된 임무컴퓨터를 개발하였다. Fig. 4와 같이 비행필수데이터는 음영으로 표시된 경로를 통해서만 전달 및 처리될 수 있도록 하였다. 비행필수데이터는 범용 Input/Output(I/O) 카드(Fig. 4 상의 I/O로 명기된 보드)가 아닌 전용 입출력 카드(Fig. 4 상의 EICAS 보드)를 이용하여 수신하며, 임무컴퓨터 내부에서도 별도의 VME 버스만을 이용해서 프로세서 (Fig. 4 상의 MGP-2에 해당)에 전달이 될 수 있도록 하였다.

시스템 차원에서는 비행필수 데이터의 데이터에 대해서는 임무컴퓨터간 데이터 실시간 상호 비교 (Cross-Check) 및 임무컴퓨터간의 데이터 불일치가 발생할 경우를 대비하여 비행필수 데이터를 주기적으로 상대 임무컴퓨터에 전송하도록 설계하여 시스템 안전성을 높였다.

2.3. 제안된 시스템 설계 방안

2.3.1 시스템 설계

2.2장의 사례분석을 통하여 비행필수데이터의 처리 및 시현과 관련되어서는 3가지 공통된 설계 원칙을 다음과 같이 도출할 수 있다.

1) 비행필수데이터는 일반정보와 분리되어 처리
2) 비행필수데이터에 대한 프로세서간 상호점검을 실시
3) 정보의 신뢰성에 문제가 발생할 경우에는 별도의 센서를 참고하며 이를 시현체계에 반영

2.1 및 2.2 장에서 소개된 비행필수정보에 대한 일반적인 정의 및 시스템 안전성 분석 결과 등을 종합한 결과, KUH에서의 비행필수정보는 Table 1과 같이 비행조종관련 정보, 항공기의 상태 정보 및 추진계통의 현황(Engine Status) 세 가지로 분류하여 정의하였다.

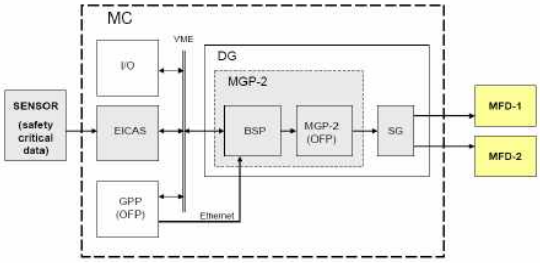


Fig. 4. Example of Mission Computer Block Diagram

정의된 비행필수데이터 중, 비행조종계통에서 획득되는 정보는 부분적으로 분리처리(Partially Secured Scheme)되도록 설계된 임무컴퓨터를 통해서 정보가 처리 및 시현되도록 하였으며, 예비 및 전용계기를 통하여 시스템 안전성을 높였다. 또한, 엔진, 연료 및 항공기의 정보 시현은 독립된 전용계기를 적용하여 시현하며 임무컴퓨터를 통하여 다기능 시현기에도 관련 정보가 시현되도록 정의하였다.

Table 1. Identified Flight Critical Information

비행 조종	Airspeed Vertical Speed Attitude Radar Altitude Heading (Magnetic/True) Automatic FCS Mode VOR/ILS Navigation Data
항공기 상태 정보	Engine Oil Temperature/Pressure MGB Temperature/Pressure Hydraulic Pressure Fuel Temperature/Pressure Transmission/Hydraulic Cautions Air Data Parameters Fuel Flow Rotor Speed Failure Message
추진계 통현황	Engine Speed Gas Turbine Temperature Torque 1/2/1+2 Outside Air Temperature Engine Auxiliary Data System Message Engine Caution

2.3.2 상세 설계

2.3.2.1 임무컴퓨터 하드웨어 설계

임무컴퓨터 하드웨어에 대해서는 비행필수 데이터 처리를 위해 임무컴퓨터 내부에 미들웨어(Middleware) 수준의 분리된 이더넷(Ethernet) 통신 채널을 추가하였다.

이더넷 통신은 고신뢰도가 요구되는 최신 민항기인 Airbus 380 기종과 Boeing 787기종의 비행제어계통에도 적용이 된 인터페이스이다[3]. 한편, 비행필수데이터의 획득을 위해 임무컴퓨터와 외부적으로 연동되는 인터페이스는 타 항공기사례에서 비행필수 데이터의 처리에 있어서 대부분 ARINC-429 인터페이스를 이용한다는 점과 MIL-STD-1553B에 비해서 Single Point Failure의 가능성이 적은 점을 고려하여, ARINC-429 인터페이스를 적용하였다. 또한, 비행필수 입출력 데이터처리를 위해 분리된 비행필수데이터 입출력 모듈 (Flight Input Output Module, FIOM)을 추가하였다.

2.3.2.2 임무컴퓨터 소프트웨어 설계

MFD상에 비행필수데이터를 시현하는 CSCI (Computer Software Configuration Item)는 기타 임무정보를 시현하는 CSCI와는 별도로 운용하도록 Fig. 5와 같이 설계하였다. 또한, ARINC-429 인터페이스를 이용하여 데이터가 전달되는 비행조종 데이터에 대해서 상호 검증 로직과 두 대의 임무컴퓨터가 동시에 정상 작동되는 MC 운용로직을 구현하였다. 또한, 비행계기시현기능인 주계기시현(PFD, Primary Flight Display) CSCI에 대해서는 DO-178B[4]의 level A에서 요구되는 각종 시험 (MC/DC 시험 등)을 실시하여 시스템의 안전성을 확인하였다. MC/DC 시험은 커버리지 목표값을 85%로 설정하였으며 시험자동화도구(LDRA)를 사용하여 시험 수행결과 조건식이 포함된 함수에 대해 87~100 % 결과를 얻었다.

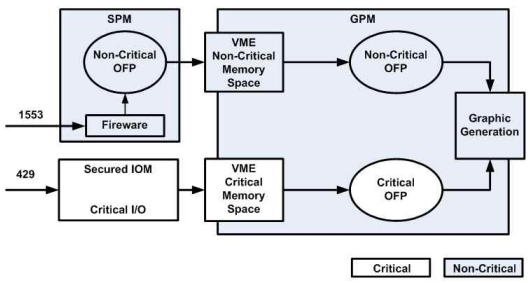


Fig. 5. Segregation of Flight Critical Data within Mission Computer

2.3.2.3 데이터별 흐름

Fig. 6은 임무컴퓨터의 비행필수정보와 임무정보가 전달 및 처리되는 흐름을 도식화하였다. 그래픽 생성 모듈(GPM; Graphic Processor Module)은 MFD 버튼 입력 값 및 시스템 서브시스템 데이터를 수신하여 영상 신호를 생성하여 MFD에 전시한다. 또한, 시스템 처리 모듈(SPM; System Processor Module)은 MIL-STD-1553B 통신의 BC (Bus Controller)로 전체 임무탑재체계 통신 제어 및 내부의 데이터관리제어를 담당한다.

비행필수정보는 임무컴퓨터 내부의 FIOM (Flight Input Output Module)만을 통해서 임무컴퓨터로부터 입/출력이 되도록 한다. 즉, "비행필수정보→ FIOM → GPM" 의 경로를 형성한다. 이에 반하여, 임무정보는 "임무정보→SPM→GPM"의 경로를 따라 연산 및 처리된다.

2.3.2.4 상호점검 (Cross Check)

원자력 발전, 자동차의 엔진제어장치 등과 같이 데이터의 획득 및 처리 과정에서 높은 신뢰도가 요구되는 경우에 프로세서를 다중으로 두어 프로세서간의 상호 점검을 통하여 중요 데이터가 무결(Fault Free)함을 확인하는 것이 일반적이다[5]. 비행필수데이터의 신뢰도는 항공기 체계 자체의 안전성과 직결되는 중요한 요소로, 해당 데이터의 신뢰성을 증대하기 위해서 비행필수데이터와 관련된 센서를 다중으로 두는 것이 일반적이다. 본 논문에서도 이중센서를 통해서 공급되는 각종 데이터의 비교 분석 기능을 구현하였다.

임무컴퓨터는 이중 센서 데이터 비교를 위해 이중으로 설치된 센서의 데이터를 모두 수신한다. 상호 점검은 지정된 이더넷 인터페이스를 이용하여 주 임무 컴퓨터(Primary Computer)와 부 임무 컴퓨터(Secondary Computer) 사이에서 수행된다. 상호 점검 과정에서 두 컴퓨터간의 차이가 문턱치(Threshold Value) 이상일 경우에는 조종사에게 이를 알리는 경고를 시현하여 조종사가 아날로그 계기값을 바탕으로 판단을 하도록 하였다.

한 대의 임무컴퓨터가 고장 또는 전원이 인가되지 않은 경우에는, 한 대의 임무컴퓨터로만 운용되며 센서에 대한 상호 점검은 수행하지 않도록 하였다. 설사, 상호 점검이 수행되지 않더라도 관련된 전용계기를 별도로 조종석에 설치하였기 때문에, 비행안전성에 큰 영향이 없도록 하였다. 실제 설계된 이중센서의 상호점검 방식이 Fig. 7에 나타나 있다. 또한, 이중센서가 항공기에 장착

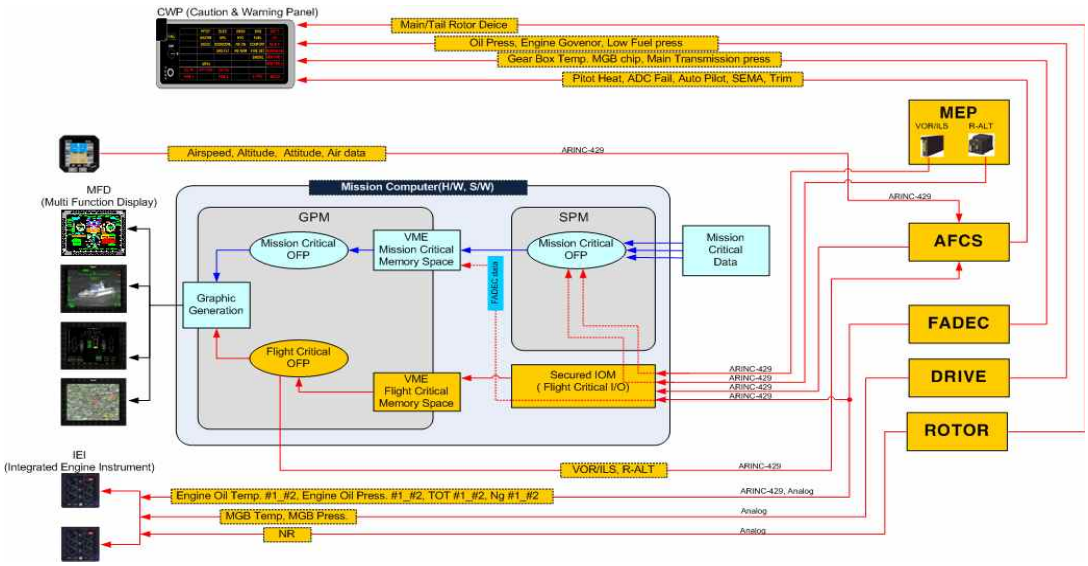


Fig. 6. Data flow of flight critical information

되지는 않지만 비행필수데이터로 정의된 정보(지면으로부터의 고도, 주요 항법원)를 제공하는 전파고도계(Radar Altimeter)와 VOR/ILS로부터 획득되는 정보에 대해서도 양쪽 임무컴퓨터에 모두 정보를 제공하고, 해당 정보에 대해서 임무컴퓨터간 상호점검기능을 Fig. 8과 같이 구현하였다.

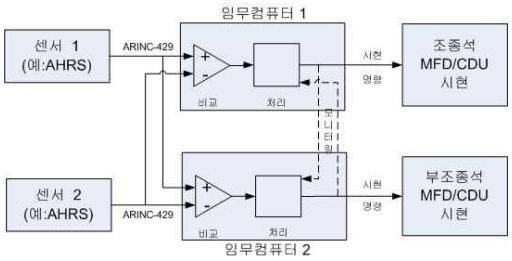


Fig. 7. Cross -Check Logic for Dual sensor data

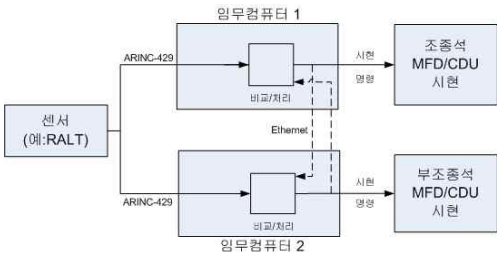


Fig. 8. Cross-Check Logic for single sensor data

2.4. 체계 안전성 분석

앞 장에서 적용된 설계 개념을 바탕으로 비행필수데이터의 시현 및 운용등과 관련된 체계 차원의 안전성 분석(System Safety Analysis)을 실시하여 안전성 요구도의 만족여부를 해석적으로 확인하였다.

2.4.1 안전성 목표

한국형 헬기 임무탑재체계에 적용된 안전성 평가 기준은 군용기에 적용되는 MIL-STD-882를 따르고 있으며 민간항공기에 적용되는 FAR 규정과의 차이는 다음과 같다[3].

- MIL-STD-882 : 설계허용 안전 수준을 사업별 특성에 부합되게 설정할 수 있도록 허용하고, 기준을 예(Example) 로서만 제시
- FAR AC 29-1309: 심각도별 설계 허용 발생빈도 수준이 정량적으로 명시되고 MIL-STD 제시보다 엄격함.

기본적으로, MEP체계와 장비들은 단일고장이 항공기 수준에서 Catastrophic 이나 Critical 수준의 사건을 야기하지 않도록 설계되는 것을 목표로 하였다. Catastrophic 이나 Critical 수준의 위험요소에 대한 고장율은 2시간 비행동안 10^{-8}고장 이하이어야 하며, Critical 수준의 위험요소에 대해서는 10^{-7}고장 이하이어야 한다. Marginal 수준의 위험요소에 대한 고장율은 2시간 비행동안 10^{-5}고장 이하이어야 한다[6].

총 160건의 결함조건(Failure Condition)이 식별되었으며, Catastrophic 수준의 사건을 야기하

지 않도록 설계되어야 하는 결함조건이 9건, Critical 수준에 해당 하는 조건이 17건, Marginal 수준에 해당하는 조건이 62건 및 Negligible 수준에 해당하는 조건이 71건으로 분류되었다. 특히, 본 논문에서 관심을 두는 비행필수정보의 시현과 관련된 위험 요소는 대부분 Catastrophic 수준에 해당하는 위험요소이며 다음과 같다.

*. MEP1.3.c: Undetected erroneous display of attitude information on both sides(in IFR condition)

*. MEP1.4.c: Undetected erroneous display of barometric altitude information on both sides (in IFR condition)

*. MEP1.6.a: Loss of DH(Decision Height) on both sides and loss of the associated audio alarm(in IFR condition)

*. MEP2.2.d: Complete loss of navigation and communication means(in IFR condition)

*. MEP7.2.c: Non restorable loss of external communication combined with non restorable loss of radio navigation information

*. MEP11.2.a: Loss of VOR, ILS course setting capability on displays(in IFR condition)

*. MEP11.2.b: Unintended change in VOR/ILS course setting simultaneously on all displays(in IFR condition)

*. MEP11.5.a: Complete loss of ADC (Air Data Computer) baro-correction setting capability

*. MEP11.5.b: Undetected change or erroneous baro-correction setting simultaneously from both sides

2.4.2 분석 결과

총 160건의 결함조건에 대해서 FTA(Fault-Tree Analysis)를 실시한 결과, 모두 할당된 요구도를 만족하는 것으로 분석되었다. 비행필수데이터와 관련된 결함조건이 속해 있는 항목의 대부분이 Catastrophic인 것을 감안하여 본 논문에서는 해당 위험요소에 대한 분석 결과를 Table 2에 제시하였다. 분석은 Relex Software사에서 제공하는 Relex Reliability Studio 2007을 이용하여 수행하였다. Table 2에서 알 수 있듯이 모든 요소에 대해서 분석 결과가 목표치를 만족함을 알 수 있다.

III. MEP 체계 안전성 시험

비행필수기능과 연관된 MEP 주요시스템 기능에 대해 기본적인 시스템 안전성 및 적합성을 확인하는 시험으로 본 논문에서는 일반적인 시스템

Table 2. Safety Analysis results for CAT degree event

결함 ID	목표	분석결과
MEP1.3.c	10^{-8}	1.52 X 10^{-14}
MEP1.4.c		3.58 X 10^{-14}
MEP1.6.a		4.76 X 10^{-16}
MEP2.2.d		1.44 X 10^{-35}
MEP7.2.c		1.14 X 10^{-48}
MEP11.2.a		1.36 X 10^{-11}
MEP11.2.b		1.36 X 10^{-11}
MEP11.5.a		3.68 X 10^{-10}
MEP11.5.b		8.99 X 10^{-18}

안전성 가이드[7~9]를 참고하여 결함주입시험(Failure Mode Effect Test, FMET), Coverage Test, Trajectory Test, Operational Load Test, Operator in the Loop Test, Sensor Orientation Test로 6개 항목으로 선택하였다.

3.1 결함주입시험

결함주입시험은 비행필수 센서기능에 결함을 주입하여 시스템이 결함감지, 격리, 보고능력에 대한 요구사항 충족여부를 검증하는 시험으로 센서결함모사, 장비간 통신결함 모사, 비디오 신호 결함모사, 이중 임무컴퓨터 제어신호 결함모사시험 등으로 구성된다. Fig. 9는 SIL(System Integration Laboratory)에서 LOC/GS (Localizer/Glide Slope) 신호 인가시 시스템의 운용을 확인하기 위한 시험환경이다. LOC 센서 신호의 결함을 모사하기 위해 센서모의 시험장비인 Ramp 시험기와 VOR/ILS 장비간 연결을 분리하고 GS 신호를 인가했을 경우 Fig. 10 (a)와

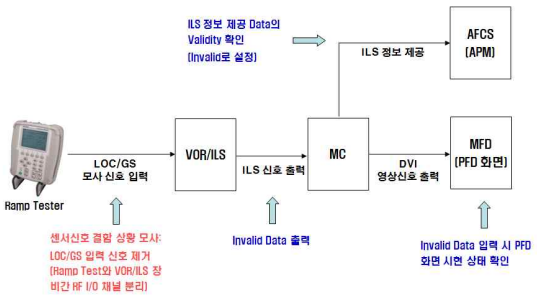


Fig. 9. Sensor safety test using LOC/GS simulator

(a) GS input (b) LOC input

Fig. 10. Display of ADI

ARINC 429 on Device: 1, Module: 2	Label: 174 Ch: 2	sdi	ssm
		10	1
ARINC 429 on Device: 1, Module: 2	Label: 173 Ch: 3	sdi	ssm
		10	11

(a) LOC SSM validity

ARINC 429 on Device: 1, Module: 2	Label: 174 Ch: 2	sdi	ssm
		10	11
ARINC 429 on Device: 1, Module: 2	Label: 173 Ch: 3	sdi	ssm
		10	1

(b) GS SSM validity

Fig. 11. ARINC-429 SSM validity of the LOC/GS

같이 LOC가 시현되고 있는 상황에서 Fig. 10 (b)와 같이 수평노란색 바 형태의 GS 신호가 시현된다. Fig. 11 (a)은 LOC 신호 인가시 LOC(ARINC 429 신호 라벨 173) 신호의 SSM(Sign/Status Matrix)이 '11'로 정상상태를 나타내며, Fig. 11 (b)은 GS 신호 인가시 ARINC 429 신호 라벨 174의 SSM이 No Computed data를 나타내는 '01'에서 '11'로 변경되고 LOC는 '01'로 전환된다.

3.2. Coverage Test

비행필수 시현변수들에 대한 유효 범위값 작동시험으로 정적 커버리지 시험(static coverage test)과 동적 커버리지 시험(dynamic coverage test)을 수행하였다. Fig. 12는 0~2,000 feet 유효범위를 가진 고도지시계의 정적 및 동적 커버리지 시험개념도를 나타낸다. 모델을 이용 가상입력을 연속적으로 입력시키면서 설계에 따른 고도계 시현값을 확인 하며, Fig. 13은 정적 커버리지 시험환경하에서 각 고도계 시현 상태를 나타낸다.

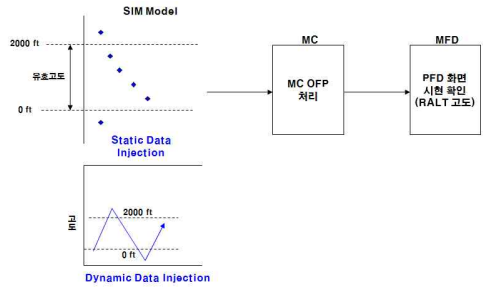


Fig. 12. Static and dynamic coverage test block diagram

(a) < 0 (b) 0 (c) 0~2,000 (d) 2,000 (e) > 2,000

Fig. 13. Display of Radar Altimeter for each data input

3.3. Trajectory Test

실제와 유사한 동적환경에서의 시스템 동작 및 시현을 확인하는 시험으로 변수 입력값뿐 아니라 이와 연계한 시스템 및 서브시스템 상태 및 모드를 포함한 동적환경에서 시험을 수행하며, 실제 환경과 유사한 환경에서 기록된 데이터를 이용하여 Fig. 14와 같이 trajectory test를 수행하였다. 조종사가 계획된 시나리오에 따라 비행조종을 조작시 임무컴퓨터로 가는 출력값을 테이프에 녹화하고 이를 임무컴퓨터에 입력하여 재현시 PFD에 비행필수 변수가 설계요구도에 따라 정상시현되는지를 확인하는 시험이다. Fig. 15는 비행조종컴퓨터의 작동상태가 비정상일때 C, YR, P 신호가 점멸되는 상태로써 임무컴퓨터를 통해 다기능시현기에 나타난다.

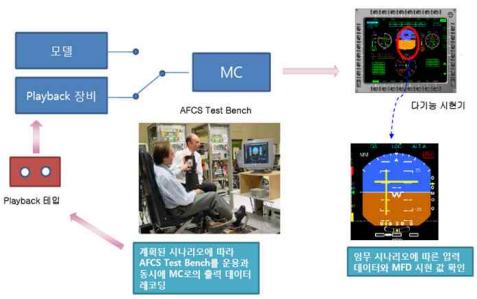


Fig. 14. Trajectory test using Playback equipment

(a) Normal Status

(b) Abnormal Status

C: Collective, YR: Yaw/Roll, P: Pitch
Fig. 15. Function Status of the AFCS

3.4. Operational Load Test

본시험은 최대 운용부하 상태에서에서의 화면 시현 및 시스템 동작확인을 하는 시험과 최대 운용시간중 시스템 동작확인시험으로 구성하였다. 최대 운용부하 상태시험은 MFD 4대에 Worst Case Display Format(모든 센서 가동하)인 PFD 화면 (Fig. 16)을 시현시키면서 30분간 시스템 동작을 확인하였다. 최대 운용시간중 시스템 동작

Fig. 16. PFD Dispaly

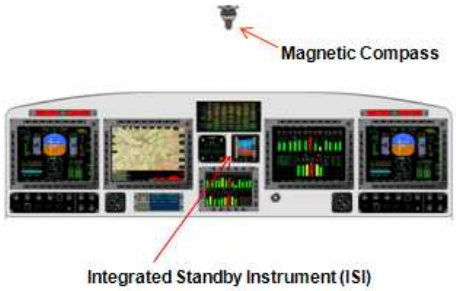
Fig. 17. DMAP Display

확인시험은 2대 MFD는 PFD, 다른 2대 MFD는 전자지도(Digital map, DMAP) 화면(Fig. 17)을 시현시키면서 일반 운용 상태에서 최대운용시간인 4시간 동안 정상작동함을 확인하였다.

3.5. Pilot in the Loop Test

시스템의 결함상태 및 결함보고에 따른 운용자의 조치상황을 고려한 종합적인 시스템 대처 능력을 확인하는 시험이다. 본 시험은 가상의 결함발생 시나리오를 구성하여 해당 결함 발생시 운용자가 시스템의 결함 또는 동작 상태를 식별하여 적절한 대처 조치를 하도록 시스템이 구성되어 있는지를 확인하는 시험으로써 이중 센서 불일치 및 이중 임무컴퓨터 간 제어 신호 고장시에 대해 본 기법을 적용하였다. Fig. 18은 AHRS1과 AHRS2 간 기수정보가 7도 이상 차이의 이중 센서 불일치 발생시(a) 제 3의 센서인 ISI (Integrated Standby Instrument)와 비교하여 고장센서를 식별하며(b), 운용자는 결함 식별 후 항공기 센서 및 시스템 동작상태를 종합적으로 판단하여 RCU (Reconfiguration Control Unit)에서 AHRS1 과 AHRS2 중 어느 센서 정보를 사용할지(c) 최종 결정하게 되는 과정을 보여준다(d).

(a) Warning display of Heading Discrepancy



(b) Decision of aircraft sensor and system operation

(c) Selection of AHRS sensors

(d) Display of normal operation

Fig. 18. Display of Heading information

3.6. Orientation Test

방향성이 있는 센서 데이터에 대한 방향설정이 정확한지 확인하는 시험으로 다음 3항목으로 구성된다.

1) VOR/ILS Orientation
- VOR 정보의 Radiation/Bearing 설정 확인
- LOC 정보 +/- 설정에 따른 Deviation Bar 시현 방향 확인 (Left/Right)
- GS 정보 +/- 설정에 따른 Deviation Bar 시현 방향 확인 (Up/Down)

2) INS Orientation
- 좌표계 Orientation 확인 (X/Y/Z축)
- INS Tilt에 따른 Pitch Angle 방향
- INS Roll에 따른 Roll Angle 방향
- INS Azimuth에 따른 Heading 방향

3) AHRS Orientation
- Pitch Angle 방향
- Roll Angle 방향

Fig. 19는 INS Orientation의 예로써 INS와 Frame간 Bonding Strap 설치 후 INS 장비를 X/Y/Z 각 축 방향으로 움직임에 따라서 해당 좌표의 속도 값 변화량을 확인하며, INS를 + X

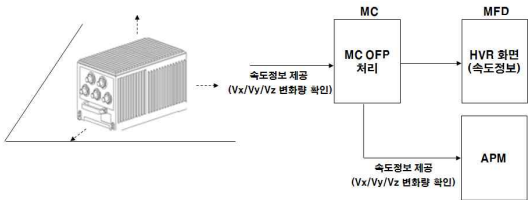


Fig. 19. INS orientation test block diagram

Name	Value / Discrete	Units	Time Tag
GPS_INS_VX	0.0625	m/sec	00:03:36.137749
GPS_INS_VY	0	m/sec	00:03:36.137749

Fig. 20. Display of GPS/INS velocity data

축 방향으로 이동시켰을 경우 Fig. 20에서와 같이 Vx 값이 + 값을 나타내므로 정의된 방향과 일치함을 알 수 있다.

Ⅳ. 결 론

종래의 군용 항공기는 민간항공기와는 달리 그 목적상 시스템의 안전성이나 효율성 보다는 임무수행이 가장 큰 평가의 기준이 되어 왔다. 하지만, 최근에는 임무가 더욱 복잡하고 다양할 뿐만 아니라 고가의 장비들이 사용됨에 따라 과거보다 높은 수준의 시스템 신뢰성이 요구되며 조종사 및 승무원의 안전성 확보가 최우선 고려요소가 됨에 따라 군용기에 있어서도 민항기 수준의 안전성을 요구하는 추세이다.

본 논문에서는 이러한 추세에 따라 KUH 임무탑재장비에 적용된 안전성 설계 및 검증 방법을 고찰하였다. 안전성 설계나 검증 기법이 보편화된 해외 항공선진국에 비해 상대적으로 뒤떨어진 국내 항공개발 분야의 안전성 설계에 있어 새로운 설계기법 및 시험방안을 제시한 것은 큰 성과라 할 수 있겠다.

본 연구를 통하여 제시된 설계 및 검증기법들을 더욱 발전시켜 향후 예상 되는 유사 항공기개발에서는 한 단계 더 진보된 항공기 신뢰성 설계에 도움이 되기를 기대한다.

참고문헌

1) MIL-STD-882D, "Standard Practice for System Safety", JAN 1993.

2) KUH System Design Review Meeting, DEC 2002.

3) Y.H. Lee, P.A. Scandura and E. Rachlin,

"Safety and Certification Approaches for Ethernet based Aviation Dtabuses", FAA/NASA Software Conference, JUL 2005.

4) DO-178B, "Software Considerations in Airborne Systems and Equipment Certification", DEC 1992.

5) W.R. Dun, "Practical Design of safety-critical computer systmes", Reliability Press, 2002.

6) KUH MEP 체계 안전성 분석 보고서, JAN 2010.

7) Joint Software System Committee, "Software System Safety Handbook", A Technical & Managerial Team Approach, DEC 1999.

8) Patrick R. H. Place and Kyo C. Kang, "Safety-Critical Software: Status Report and Automated Bioliography", JUL 1993.

9) IPL Information Processing Ltd, "An Introduction to Safety Critical Systems", MAR 1997.