Research Paper
Journal of Aerospace System Engineering
Vol.15, No.5, pp.24-32 (2021)
EISSN 2508-7150
http://dx.doi.org/10.20910/JASE.2021.15.5.24

모델기반 항공기 안전성평가에 관한 연구

김주영[1,†]· 이동민[2]· 이병길[3]· 길기남[1]· 김경남[1]· 나종화[2]
[1]대한항공 항공기술연구원
[2]한국항공대학교
[3]현대자동차

A Study of Model-Based Aircraft Safety Assessment

Ju-young Kim[1,†], Dong-Min Lee[2], Byoung-Gil Lee[3], Gi-Nam Gil[1], Kyung-Nam Kim[1] and Jong-Whoa Na[2]
[1]Koreanair R&D Center
[2]Korea Aerospace University
[3]Hyundai Motor Co.,Ltd

Abstract

Personal Air Vehicle (PAV), Cargo UAS (Cargo UAS), and existing manned and unmanned aircraft are key vehicles for urban air mobility (UAM), and should demonstrate compatibility for the design of aircraft systems. The safety assessment required by for certification to ensure safety and reliability should be systematically performed throughout the entire cycle from the beginning of the aircraft development process. However, with the increasing complexity of safety critical aviation systems and the application of state-of-the-art systems, conventional experience-based and procedural-based safety evaluation methods make ir difficult to objectively assess safety requirements and system safety. Therefore, Model-Based Safety Assessment (MBSA) using modeling and simulation techniques is actively being studied at domestic and foreign countries to address these problems. In this paper, we propose a Model-Based Safety Evaluation framework utilizing modeling and simulation-based integrated flight simulators. Our case studies on the Traffic Collision Availability System (TCAS) and Wheel Brake System (WBS) confirmed that they are practical for future safety assessments.

초 록

도심 항공 모빌리티(Urban Air Mobility, UAM)의 핵심 이동수단인 개인 항공기(PAV) 및 화물 운송용 무인항공기(Cargo UAS)는 항공기 시스템의 설계 적합성과 안전성을 동시에 확보해야 한다. 이를 입증하여 형식 증명(인증)을 받으려면 안전성 분석 및 평가를 항공기 개발과정 초기부터 전체 주기에 걸쳐서 체계적으로 수행해야한다. 그러나 안전 필수 항공시스템의 복잡도가 증가하고 최첨단 시스템이 적용됨에 따라 기존의 경험기반, 절차기반의 안전성평가만으로는 항공기 시스템의 안전성을 객관적으로 평하기 어려워졌다. 이러한 문제를 해결하기 위해 국내외적으로 모델링 및 시뮬레이션 기술을 이용한 모델기반 안전성평가(Model-based Safety Assessment, MBSA)가 활발히 연구되고 있다. 본 논문에서는 비행 시뮬레이터와 타겟의 시뮬레이션 모델을 연동한 통합 비행 시뮬레이터를 활용한 모델기반 안전성평가 프레임워크를 제안하였다. 공중충돌방지시스템(Traffic Collision Avoidance System, TCAS) 과 휠 제동 시스템 (Wheel Brake System, WBS) 사례연구를 통해 제안된 프레임워크를 UAM 안전성평가에 적용 가능함을 확인하였다.

Key Words : Model-Based Safety Assessment(모델기반 항공기 안전성평가), Type Certification(형식 증명), UAM (도심항공모빌리티), PAV(개인용 항공기), Integrated Flight Simulator(통합 비행 시뮬레이터)

1. 서 론

도심 항공 모빌리티(Urban Air Mobility, UAM)의 핵

Received: Jan. 22, 2021 Revised: Apr. 12, 2021 Accepted: Apr. 13, 2021
† Corresponding Author
E-mail:juyoung.kim@koreanair.com

심 이동수단인 개인항공기(PAV) 및 화물 운송용 무인 항공기(Cargo UAS)는 첨단기술이 접목된 복잡한 시스템으로 구성되어 있기 때문에 안전한 비행 및 성공적인 임무 수행을 위해서는 제품의 성능만 아니라 시스템에 대한 고도의 안전성 및 신뢰성이 확보되어야 한다[1]. 이에 따라 항공기 시스템의 설계 적합성을 입증하기 위해 필수적으로 형식 증명(인증)에서 요구하는 안전성평가가 항공기 개발과정 초기부터 전체 주기에 걸쳐서 체계적으로 수행되어야 한다[2].

민·군용 항공기 개발에는 항공기 시스템 안전성평가 절차 수행 지침서로 SAE ARP4761과 MIL-STD-882를 활용하고 있다 [3]. 이 지침서들을 이용하여 안전성을 평가하면 항공기 시스템 개발과정에서 잠재적 위험요소를 조기에 식별하여 고장이 발생하지 않도록 항공기를 설계하거나 운용 한계를 설정할 수 있다. 또한 시스템의 잔존하는 리스크를 허용 수준 이하로 낮춰 고장 발생 확률을 감소시키거나 결함 감내 메커니즘을 도입하여 고장 영향을 최소화할 수 있다[4].

하지만 이 지침서들은 절차 기반, 경험기반으로 안전성평가를 수행하기 때문에 신규 기능이 탑재된 첨단 항공기를 개발할 때에는 안전 엔지니어의 주관적 평가가 개입될 수 있어 객관적으로 안전성을 평가하기 어렵다는 단점을 가지고 있다. 또한 잘못된 안전 요구사항이 초기에 발견되지 않고 시험평가 단계에서 발견되면 재설계 및 검증을 위한 개발 기간과 비용이 증가되기 때문에 설계 초기에 정확한 안전 요구사항을 개발하는 것이 중요하다[5].

이러한 문제를 해결하기 위해 국내외적으로 모델링 및 시뮬레이션 기술을 이용한 모델기반 안전성평가(Model-based Safety Assessment, MBSA)가 활발히 연구되고 있다[6,7]. 모델기반 안전성평가를 시스템 개발에 활용하면 시스템 안전성평가에 필요한 검증된 데이터를 확보할 수 있어 안전 엔지니어는 경험만 아니라 새로운 시스템에 대한 정확한 안전성을 평가할 수 있다.

본 논문에서는 모델기반 안전성평가의 심화 연구로 비행 시뮬레이터인 X-Plane, Simulink로 설계한 Avionics model, 결함주입환경이 연동된 통합 비행 시뮬레이터를 활용한 모델기반 안전성평가 프레임워크를 제안하고자 한다.

제안하는 모델기반 안전성평가 프레임워크는 예비시스템 안전성평가에서 도출된 아이템 수준 요구사항으로부터 모델을 구현하고, 결함 모델을 이용한 결함주입 시험을 수행하여 시스템 및 항공기 수준의 고장영향을 확인한다. 또한, 획득한 데이터로부터 심각도 등급을 정량적인 분석 지표로 산출하여, 객관화된 안전 지표를 제공함으로써, 기존의 경험적 안전성 평가를 보완한다.

사례연구로 공중충돌방지시스템(Traffic Collision Avoidance System, TCAS)과 휠 제동 시스템 (Wheel Brake System, WBS)을 Simulink 모델로 구현하고 X-Plane Simulator와 연동하여 통합 시뮬레이션 모델을 제작하여 요구 기능을 검증하였다[8-10]. 공중충돌방지시스템과 휠 제동 시스템에서 발생할 수 있는 결함을 식별하고, 잠재된 위험요소를 기반으로 결함 주입 시험을 수행하여 고장영향을 확인 및 결함에 대한 심각도 등급을 산출하였다. 사례연구에서 모델기반 안전평가기술의 중요성을 확인하였다.

2. 항공기 안전성평가

항공기 안전성 평가는 잠재적 위험요소를 제거하여 고장이 발생하지 않도록 항공기를 설계하거나 운용 한계를 설정하는 활동으로 Fig. 1과 같이 항공기 개발 전 단계에서 수행한다[3]. 항공기 안전성 평가는 현실적으로 모든 위험요소를 제거하는 것이 불가능하기 때문에, 잔존하는 리스크를 식별하고 허용 수준 이하로 낮추는 것을 목표로 한다. 이러한 목표를 달성하기 위하여 항공기 시스템 안전성평가 지침서인 SAE ARP4761을 이용한다. SAE ARP4761의 안전성 평가는 세 가지 프로세스로 구성된다. 먼저 아이템 (HW 및 SW)개발 전 단계에서는 항공기 및 시스템의 기능위험평가(Functional Hazard Assessment, FHA)과 예비시스템안전성평가(Preliminary System Safety Assessment, PSSA)를 수행한다. 아이템이 개발된 이후에는 시스템안전성평가(System Safety Assessment, SSA)를 수행하여 안전성을 검증한다.

2.1 기능위험평가

기능위험평가(Functional Hazard Assessment, FHA)는 시스템 설계 초기에 정의된 기능과 관련된 잠재적 위험요소(Hazard)를 식별하고, 식별된 고장 조건(Failure condition)에 따른 고장영향(Failure effects)를 분석 및 고장영향의 심각성을 분류(Classification)하는 평가이다[3].

2.2 예비시스템안전성평가

예비시스템안전성평가(Preliminary System Safety Assessment, PSSA)는 항공기와 시스템의 안전성요구조건을 확정하고, 구현된 설계를 통해 해당 고장영향 등급에 해당하는 요구조건을 충족할 수 있는지 평가하는 과정이다[3]. 이 절차를 통해서 항공기 및 시스템 기능위험평가 수행 결과 생성된 초기 안전 요구사항이 시스템에 대해 완전한 안전 요구사항이 된다.

2.3 시스템안전성평가

시스템안전성평가(System Safety Assessment, SSA)는 구현된 시스템 설계를 통해 기능위험평가나 예비시스템안전성평가에서 설정한 안전성 요구조건을 충족하는지 검증 및 확인하기 위한 종합적인 평가 프로세스이다[3]. 예비시스템안전성평가는 제안된 설계를 평가하고, 시스템/부품 안전요구사항들을 도출하는 방법인 반면에 시스템안전성평가는 구현된 설계가 안전 요구사항들을 충족하는지 정성적·정량적으로 입증한다.

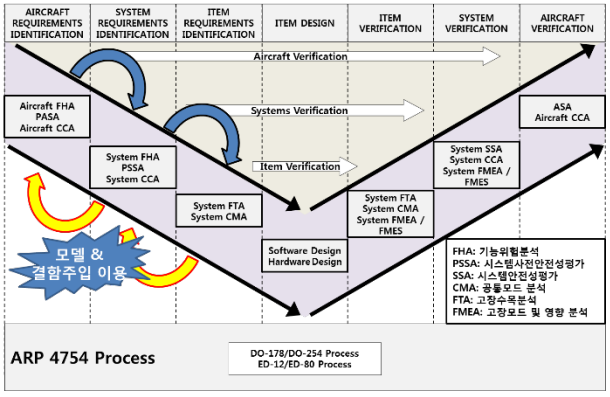

Fig. 1 Interaction Between Safety and Development Processes using Model and Fault Injection [2]

3. 모델기반 항공기 안전성평가

국내외적으로 시스템 엔지니어들은 시스템이 복잡해짐에 따라 모델링 및 시뮬레이션을 활용한 모델기반으로 요구사항 관리부터 시스템 설계 및 검증에 이르는 개발절차를 수행하고 있다. 항공기 시스템의 인증과 개발 절차에 대한 가이드라인 지침서인 SAE ARP4754A는 Table 2와 같이 요구사항 식별 및 요구사항 검증과 관련된 개발보증수준(Development Assurance Level, DAL) A, B, C에 모델링 및 시뮬레이션 기법을 사용할 것을 권장한다[11]. 소프트웨어의 개발보증수준(DAL)은 안전 평가 프로세스, 위험도 분석으로부터 결정된 레벨로서 Table 1과 같다.

또한 RTCA에서 제정한 항공전자 소프트웨어 고려사항 지침서인 DO-178C와 항공전자 하드웨어 설계 보증 지침서인 DO-254 역시 개발 규격 인증을 위해 모델기반 개발 및 검증을 요구한다[12].

항공기 설계 및 검증에 모델링 및 시뮬레이션을 활용하는 것처럼 모델기반의 장점을 안전성 평가에 이용하려는 연구가 2000년대 후반부터 에어버스를 비롯한 유럽연합 산학연구단체와 미항공우주국 NASA를 중심으로 주도적으로 연구되었다[7]. NASA에서 모델기반의 체계안전 프로세스 V-모델을 Fig. 2와 같이 제안하였고 모델기반으로 구현한 Braking System Control Unit을 제시하였다[7]. 또한 미육군의 군용항공기 및 무인항공기 안전성 평가를 위한 방법으로 시뮬레이션 모델을 이용한 새로운 안전성평가 방법의 필요성이 제기되면서 모델기반 안전성평가연구가 활발히 진행되고 있다[6].

Table 1 Failure Condition of DAL level [13]

DAL Level	Failure Condition	Description
A	Catastrophic	Failure may cause deaths, usually with loss of the airplane
B	Hazardous	Failure has a large negative impact on safety or performance
C	Major	Failure significantly reduces the safety margin or significantly increases crew workload
D	Minor	Failure slightly reduces the safety margin or slightly increases crew workload
E	No Effect	Failure has no impact

Table 2 Requirements Validation Methods and Data [11]

Methods &Data	DAL-A, B	DAL-C	DAL-D	DAL-E
PSSA	R*	R	A**	N***
Validation Plan	R	R	A	N
Validation Matrix	R	R	A	N
Validation Summary	R	R	A	N
Requirement Traceability	R	R	A	N
Requirement Rationale	R	R	A	N
Analysis, Modeling, or Test	R	One recommended	A	N
Similarity (Service Experience)	A		A	N
Engineering Review	R		A	N

*Recommended for certification, ** As negotiated for certification, ***Not required for certification

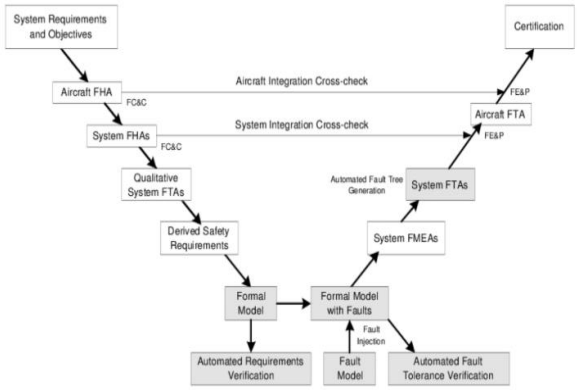

Fig. 2 Modified "V" Safety Assessment Process [7]

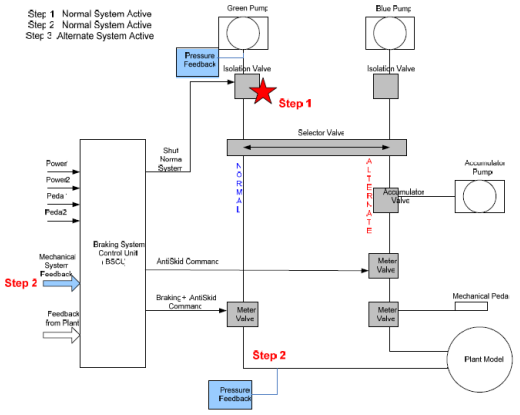

Fig. 3 Example for Braking System Control Unit Model [7]

4. 통합 모델기반 항공기 안전성평가

모델기반 안전성평가는 시스템 간의 긴밀한 통합 및 안전 분석을 가능하게 한다. 또한 개발 프로세스 초기에 시스템 아키텍처의 동작을 분석함으로써 잠재적 위험요소를 식별할 수 있고 안전설계(Fail-safe) 검증도 가능하다.

본 연구에서는 비행 시뮬레이터인 X-Plane, Simulink로 설계한 Avionics model, 결함주입환경으로 구성된 통합 비행 시뮬레이터를 활용한 모델기반 안전성평가(Model-Based Safety Assessment, MBSA) 프레임워크를 제안한다. 4.1절에서 제시하는 모델기반 안전성평가 프레임워크는 Fig. 1과 같이 예비시스템안전성평가에서 수행되어 나온 아이템 수준의 안전 요구사항으로부터 시스템 수준의 모델을 개발하고 결함 주입 시험을 수행하여 시스템 수준 위험 분석과 항공기 수준 기능 위험 분석을 재 검증하고 데이터를 기반으로 객관적 안전성 평가를 수행할 수 있다. 또한 Simulink LRU 모델, X-Plane, 결함주입 환경으로 구성된 통합 비행 시뮬레이터를 항공기 안전성평가 프레임워크에 활용함으로써 설계 초기에 기능 검증과 시스템 안전을 향상시킬 수 있도록 결함에 의한 영향을 정량적인 분석 지표로 나타내어 심각도 등급을 산출하는 방법을 제안한다.

본 연구에서는 Avionics model로 공중충돌방지시스템 모델과 휠 제동 시스템 모델을 구현하여 사례연구에 활용하였다.

4.1 모델기반 항공기 안전성평가 프레임워크

ARP4761 안전성 평가는 2장에서 설명한 것과 같이 항공기 수준 기능위험평가(Aircraft FHA), 시스템 수준 기능위험평가(System FHA), 예비시스템안전성평가(PSSA), 시스템안전성평가(SSA) 단계로 수행한다.

SAE ARP4761 안전성평가는 항공기에서 시스템을 거쳐 아이템까지 아래로 내려가는 하향식(Top-down) 방식이다. 이러한 방식은 인력이 많으면, 빠르고 효율적으로 수행할 수 있는 장점을 가지나, 중간에 구조를 변경해야 하거나 계획 자체를 변경이 필요할 경우 다시 재 수행해야 되기 때문에 이로 인한 시간과 자원이 낭비된다.

특히, 예비시스템안전성평가에서 시스템안전성평가 단계로 넘어올 경우, 각 아이템에 대한 안전 요구사항이 할당되어 개발이 진행되기 때문에 시스템 안전성평가에서의 변경은 매우 치명적이다. 또한, 시스템안전성평가 이전 단계까지의 항공기 안전성 평가는 초기 설계 단계에서 병행되어 수행되기 때문에, 전문가의 경험 및 지식에 의존하는 주관적인 안전성 평가로 수행된다.

Figure 4와 같이 제안하는 모델기반 안전성평가 프레임워크는 예비시스템 안전성평가에서 도출된 아이템 수준 요구사항으로부터 모델을 구현하고, 결함 모델을 이용한 결함 주입 시험을 수행하여 시스템 및 항공기 수준의 고장영향을 확인한다. 또한 획득한 데이터로부터 심각도 등급을 정량적인 분석지표로 산출하여, 객관화된 안전 지표를 제공함으로써, 기존의 경험적 안전성 평가를 보완해준다.

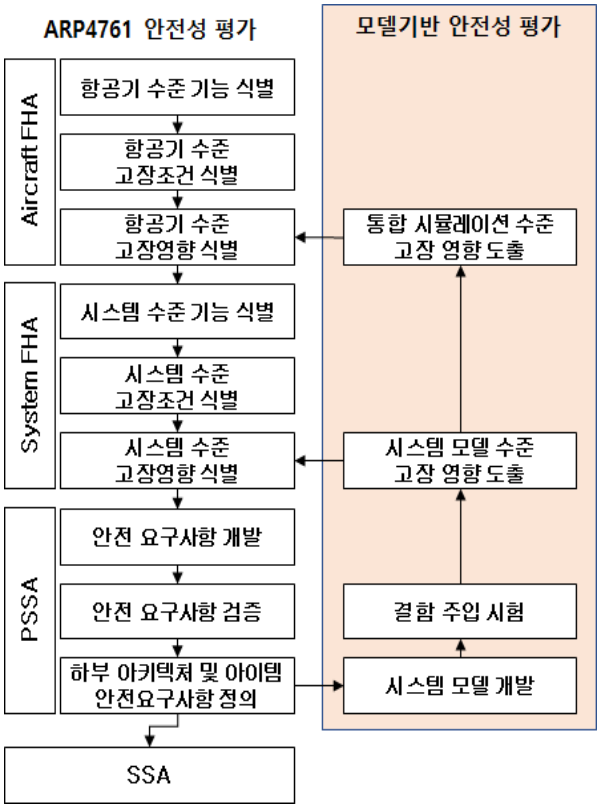

Fig. 4 MBSA Framework

4.2 통합 비행 시뮬레이터

모델기반 항공기 안전평가를 수행하기 위해 Fig. 5와 같이 통합 비행 시뮬레이터를 구축하였다. 통합 비행 시뮬레이터는 Avionics model, X-Plane Control Interface(XCI), Flight simulator로 구성된다.

Avionics Model은 설계 수준에서 객관적인 안전성 평가를 수행하기 위한 기능 수준의 모델이다. 시스템이 동작하기 위해 필요한 입출력 데이터를 Flight simulator와 연동하여, 모델 검증 및 안전성 평가를 수행하게 된다. 본 논문에서는 공중충돌방지시스템과 휠 제동 시스템에 대한 안전성 평가를 위해 Avionics model로 구현했다.

XCI는 Simulink 환경으로 개발된 Avionics model과 Flight simulator 간 통신을 연결해주고, 중간에 데이터 저장 및 결함 주입 시험 설정을 해주기 위해 C# 기반으로 개발한 프로그램이다. Flight simulator는 Laminar Research 사에서 개발한 X-Plane 10 비행 시뮬레이터를 이용하였다.

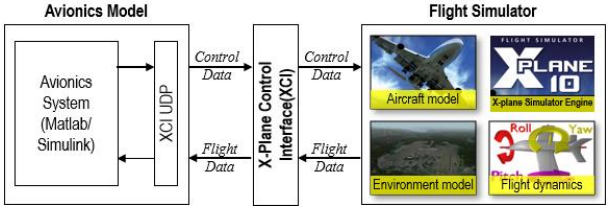

Fig. 5 Integrated Flight Simulator

4.3 공중충돌방지시스템 모델

공중충돌방지시스템(Traffic Collision Avoidance System, TCAS)은 항공기 간 공중충돌을 방지하기 위해 설계된 시스템이다. 공중충돌방지시스템은 감시 영역에 진입한 Intruder에 대해 거리 테스트와 고도 테스트를 수행한 후 충돌 위험 여부를 판정하고 회피지시를 수행한다. Intruder 항공기가 계속 접근하여 노란색으로 표시된 TA(Traffic Advisory) 영역에 도달하면 고도 테스트 및 거리테스트의 결과에 따라 항공기의 TCAS는 TA를 발행한다. 마찬가지로 항공기가 빨간색으로 표시된 RA(Resolution Advisory) 영역으로 들어오면 RA를 발행하고 이 항공기에 대한 회피 방향을 지시한다.

통합 비행 시뮬레이터의 TCAS 모델은 TCAS-II에 대한 Minimum Operational Performance Standards (MOPS) 문서인 DO-185에 정의된 충돌회피 알고리즘에 따라 Simulink/Stateflow를 이용하여 단일 모델과 Fail-safe기능이 포함된 이중화 모델을 구현하였다. 단일 모델은 Fig. 7과 같이 센서데이터를 전달해주고 TCAS의 상태를 확인해주는 컨트롤 프로세스와 TCAS 상태 정보와 회피 신호를 송신하는 TCAS 프로세스로 구현하였다. 이중화 모델은 Primary 모델과 Secondary 모델로 구성 되어있고 Primary 와 Secondary 모델 모두 Fig. 8과 같이 단일모델에 Heartbeat 프로세스를 추가하여 구현하였다.

단일 및 이중화 모델은 결함을 주입할 수 있도록 프로세스내부에 변수를 포함하여 구성하였다.

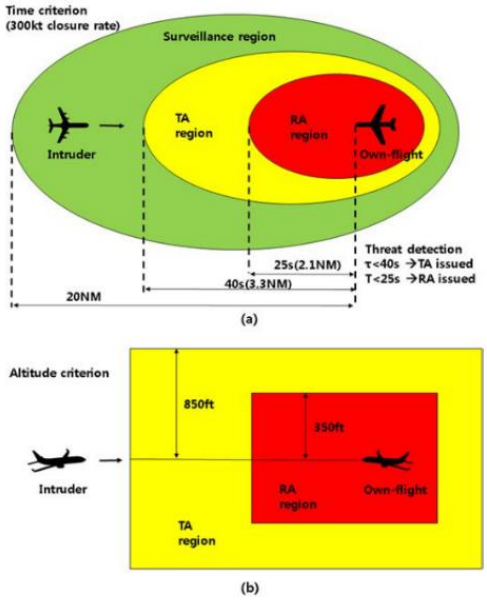

Fig. 6 (a) Range test at SL 5 (b) Altitude test at SL 5

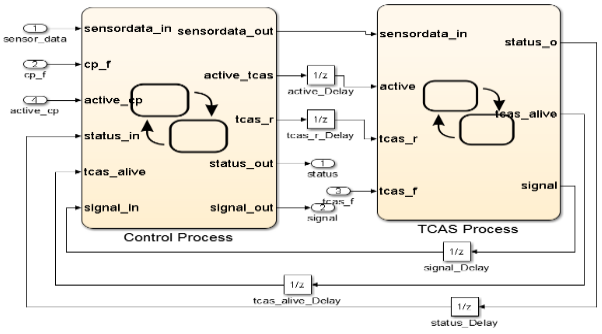

Fig. 7 Single TCAS Model

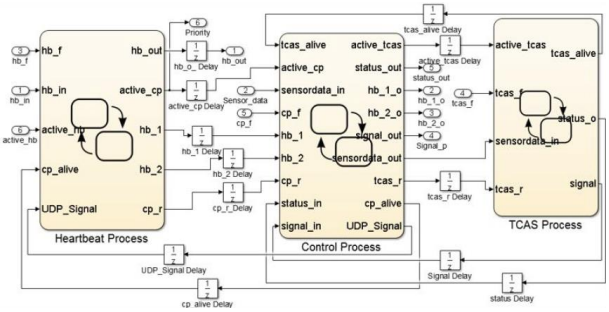

Fig. 8 Dual TCAS Model

4.4 휠 제동 시스템 모델

휠 제동 시스템(Wheel Brake System, WBS)은 항공기가 지상에서 항공기를 정지시키거나 정지한 항공기를 유지시켜주는 시스템이다. 휠 제동 시스템은 브레이크 시스템 제어 장치(Brake System Control Unit BSCU)와 유압 작동 시스템(Hydraulic Operating System)으로 구성된다.

브레이크 시스템 제어 장치는 조종사가 조종한 페달의 위치를 전기적인 데이터로 입력 받아 적절한 브레이크 제어 신호를 생성하는 시스템이다. 유압 작동 시스템은 유압펌프로부터 압력을 공급받아 브레이크 신호에 맞게 항공기 휠 조립체를 제어하는 시스템이다.

Fig. 9에서 구현한 휠 제동 시스템 모델은 시뮬레이터 조종기의 제어 정보를 입력 받아 BSCU와 HOS 모델을 거쳐 0과 1사이의 Brake 신호를 출력한다.

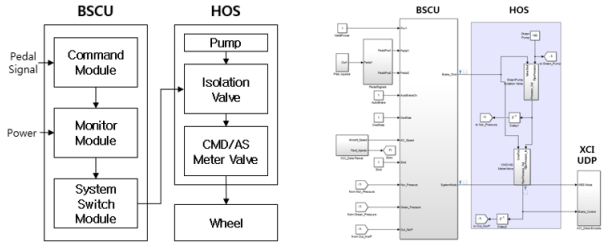

Fig. 9 WBS Architecture & Simulink Model

4.5 Fault Injection Test

객관적인 항공기 안전성 평가를 위해 구현한 Avionics model에 대해 결함 주입 시험을 수행했다. 결함 주입 시험은 예비시스템안전성평가 단계에서 도출한 아이템 요구사항으로부터 구현한 Avionics model에 결함을 주입하여 나온 결과로부터 시스템 및 항공기 수준의 고장영향을 확인할 수 있다. 이를 통해 예비시스템안전성평가 단계까지의 경험 기반의 주관적 안전성 평가로부터 데이터 기반의 객관적 안전성 평가로 확장할 수 있다. 또한 전문가가 놓칠 수 있는 잠재적인 위험요소와 고장영향을 발견할 수 있다.

4.5.1절에서는 TCAS 입력 센서 결함을 구현하기 위한 결함 주입 환경을 설명하고 있으며, 4.5.2절에서는 WBS의 유압 제어 출력 시스템에 결함을 구현하기 위한 결함 주입 환경에 대해 설명한다.

4.5.1 TCAS Fault Injection 환경

TCAS모델에 대한 결함 주입 시 영향을 확인하기위해 통합 비행 시뮬레이터는 Simulink를 이용한 시뮬레이션 기반 결함 주입 환경을 구성하였다.

결함주입 환경은 Fig. 10과 같이 Fault Injection Manager(FIM)와 Fault Injection Interface(FII)로 구성되어있다. FIM에서 UDP(User Datagram Protocol)를 통해 결함 Parameter를 FII에 보내면 Fig. 11과 같은 Simulink 결함모델로 구성된 FII는 결함 Parameter를 받아 해당되는 결함 모델을 선택하고 결함 값을 TCAS모델에 전달한다.

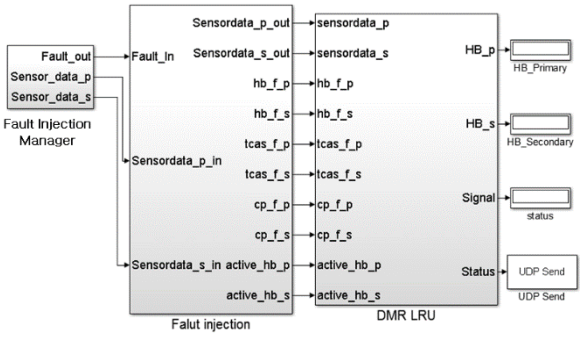

Fig. 10 TCAS Fault Injection Model

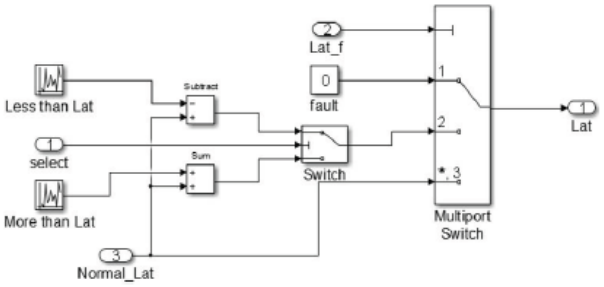

Fig. 11 Relationship of Fault, Error, Failure Latitude Simulink Fault Model

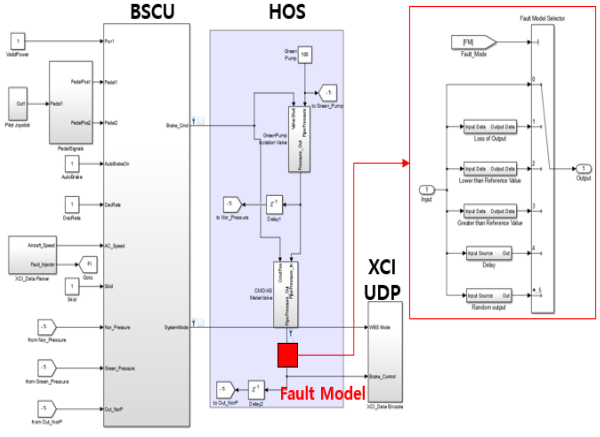

Fig. 12 WBS Fault Injection Model

4.5.2 WBS Fault Injection 환경

WBS 결함 주입 시험을 수행하기 위해 SAE ARP4761에서 제시하고 있는 특정 고장모드 5가지 (Loss of Output, Lower than Reference Value, Greater than Reference Value, Delay on Output,

Noise on Output)를 발생시킬 수 있는 Mutation Model을 Fig. 12와 같이 개발하였다. Avionics Model에 분석하고 싶은 시스템 노드에 Mutation Model을 결합한 후, 테스트를 수행하여 시스템의 고장영향을 검증할 수 있다.

4.6 정량적인 지표를 이용한 심각도 판정 방법

4.6.1 충돌 확률 기반 심각도 등급 산출

통합 비행 시뮬레이터에서는 TCAS모델에 결함이 주입되면 결함에 따른 영향을 엔지니어가 시각적으로 볼 수 있을 뿐 아니라 결함에 대한 충돌 확률을 측정한다. 여기서 말하는 충돌 확률이란 최근 접점에서 두 항공기의 상대 거리(rf)가 기준 값 이하가 되는 확률이다. 기준 값을 R이라고 정의하면 식(1)와 같은 조건을 만족할 때 두 항공기는 충돌 확률이 높다고 할 수 있다. 식 (2), (3)으로부터 충돌 확률(PC)은 Fig. 13과 같이 PC를 -R부터 R까지 적분하여 구할 수 있다. 기준 값 R은 NASA ERAST에서 제시한 See and Avoid를 위한 최소 거리를 근거로 500 feet로 설정하였다[14].

통합 비행 시뮬레이터에서 측정한 충돌 확률을 Fig. 14와 같이 기존 심각도 등급 분류 기준들과 함께 고려하여 정량적인 지표 기반의 심각도 등급을 산출하였다.

$$r_f \leq \mathrm{R} \tag{1}$$

$$P_C = \int_{-R}^{R} P(r_{|f})dr_f = \frac{1}{\sqrt{2\pi\sigma_{r_f}}}\int_{-R}^{R} \exp\left(-\left(\frac{r_f-\overline{r_f}}{\sqrt{2}\sigma_{r_f}}\right)^2\right)dr_f \tag{2}$$

$$P_C = \frac{1}{2}\mathrm{erf}\left(\frac{R+\overline{r_f}}{\sqrt{2}\sigma_{r_f}}\right)+\frac{1}{2}\mathrm{erf}\left(\frac{R-\overline{r_f}}{\sqrt{2}\sigma_{r_f}}\right) \tag{3}$$

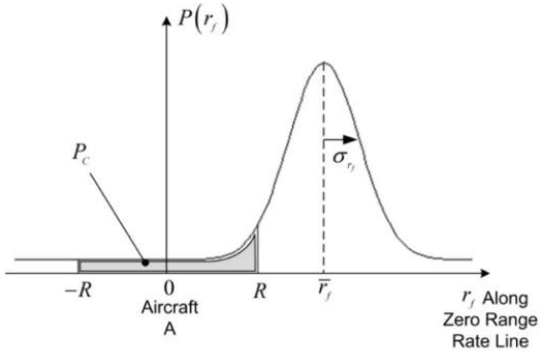

Fig. 13 Passive Attitude Control Using Permanent Magnet Stabilization Probability Density Function of r_f

[기존]

Criteria: Severity of the Effect		Severity
정성적 요소	정량적 요소	
사망 영구적인 전신불구, 회복불가능한 환경 손상 초래,	1000만 달러 초과손실	Catastrophic
영구적인 부분불구, 최소 한 세명 이상이 입원해야하는 상해	100만 달러 이상 1000 달러 이상 손실	Critical/ Hazardous
하루 이상의 업무 불가 상해	10만 ~ 1백만 달러 손실	Marginal/ Major
하루 미만의 업무 불가 상해 또는 직업병	10만 달러 미만의 손실	Negligible/ Minor
-	-	No Safety Effect

추가

[분석지표 기반 평가]

충돌 확률	Severity
P_c : 80 – 100 %	Catastrophic
P_c : 60 – 80 %	Critical/ Hazardous
P_c : 40 – 60 %	Marginal/ Major
P_c : 20 – 40 %	Negligible/ Minor
P_c : 0 – 20 %	No Safety Effect

Fig. 14 Collision Probability based Severity Rank

4.6.2 착륙거리 도표기반 심각도 등급 산출

휠 제동 시스템 심각도의 정량적인 판정을 위해, Fig. 15와 같이 항공기 매뉴얼의 총 중량/활주로 고도에 따른 착륙거리 도표를 이용하여 심각도를 정의하였다.

본 사례연구에 사용한 항공기 기체는 B747-400이며, 공항은 KSFO(San Francisco International Airport) 공항 28L로 설정하였다. KSFO 28L 활주로 길이는 총 3231 m이고, 표면고도는 3.96 m, Dry Runway, Flap 25조건에서 287톤 항공기 기체의 정상 착륙거리는 2,366 m이며, 최대 착륙 활주거리는 같은 환경 조건에서 최대치인 2,460 m로 제한하고 있다. 이를 이용하여 제동거리에 따른 심각도는 Fig. 16과 같다.

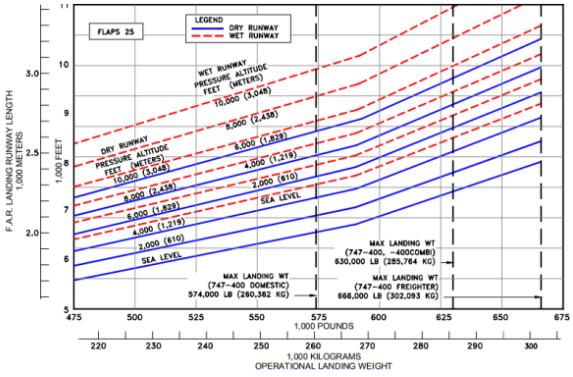

Fig. 15 Landing distance chart according to gross weight/runway altitude

[기존]

Criteria: Severity of the Effect		Severity
정성적 요소	정량적 요소	
사망 영구적인 전신불구, 회복불가능한 환경 손상 초래,	1000만 달러 초과손실	Catastrophic
영구적인 부분불구, 최소 한 세명 이상이 입원해야하는 상해	100만 달러 이상 1000 달러 이상 손실	Critical/
하루 이상의 업무 불가 상해	10만 ~ 1백만 달러 손실	Major
하루 미만의 업무 불가 상해 또는 직업병	10만 달러 미만의 손실	Minor
-	-	No Safety Effect

추가

[분석지표 기반 평가]

Braking Distance(m)	Severity
0~2366	No Safety Effect/Minor
2366~2460	Major
2460~3231	Hazardous
More than 3231	Catastrophic

Fig. 16 Braking Distance based Severity Rank

4.7 시험 결과 및 분석

4.7.1 TCAS Test Case

FAA William J. Hughes Technical Center에서 생성한 Encounter 시나리오를 사용하여 TCAS의 기능을 확인하였고 TCAS 모델에 다양한 결함을 주입시켜 충돌 확률과 심각도 등급을 확인하였다. Fig. 17는 시나리오를 사용해서 Intruder TCAS모델에 고도 결함을 주입한 비행 경로로 Intruder가 비정상 확인할 수 있다. 또한 Fig. 18과 같이 고도 결함으로 인해 Own-flight과 Intruder 간에 거리가 500 feet 이하인 Near Mid Air Collision 상황이 발생한 것을 시각적으로 표현하고 있다. 이 시험에서 두 항공기간의 거리는 Fig. 19와 같이 50 m, 충돌 확률은 89%로 계산되었고 심각도 등급은 가장 높은 단계인 Catastrophic으로 측정되었다.

4.7.2 WBS Test Case

휠 제동 시스템의 정량적 지표를 이용한 시스템 안전성 평가를 수행하기 위해 임무 시나리오에 따른 결함 주입 시험을 수행하였다. SAE ARP4761 부록에서 제시하고 있는 휠 제동 시스템 기능 상실에 대한 고장모드 중 5개를 선정하고, Fig. 20과 같이 착륙중인 항공기 시나리오에서 해당 고장모드를 재현하는 결함 주입 시험을 수행하였다. 결함 주입 시험에 의해 휠 제동 시스템 기능이 오동작이 진행되며, 이에 따른 고장영향으로 항공기의 제동거리에 영향을 주는 것을 Fig. 21에서 확인할 수 있다. 이를 통해, Fig. 16에서 정의한 심각도 지표를 기반으로 Table 3와 같이 항공기 수준 위험 평가 표를 도출할 수 있다.

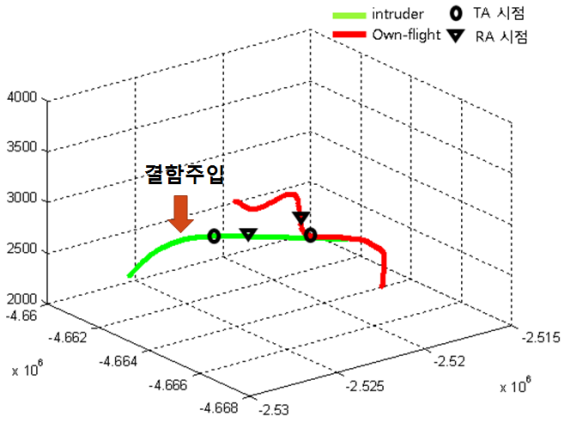

Fig. 17 Aircraft Route

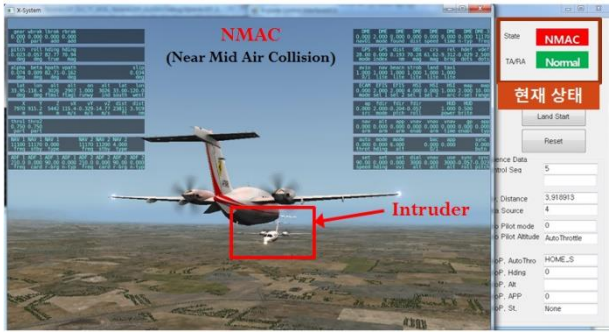

Fig. 18 NMAC status Simulation

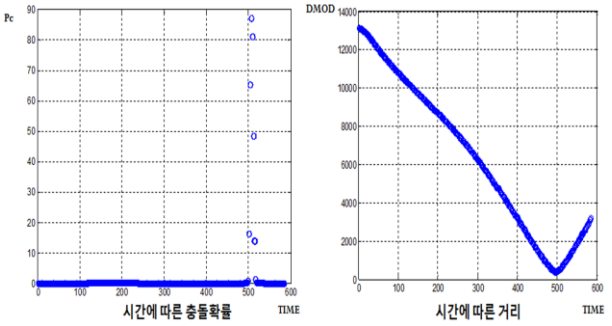

Fig. 19 Result of Fault Injection Simulation

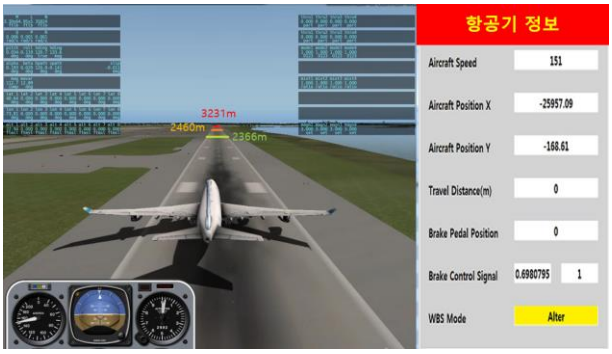

Fig. 20 WBS Simulation

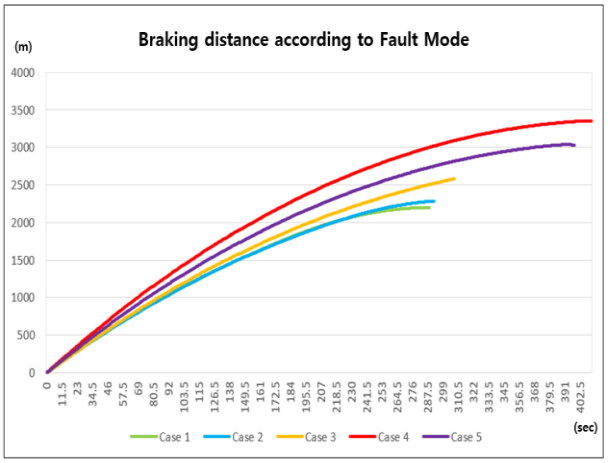

Fig. 21 Braking distance according to Fault Mode

Table 3 Model Based Functional Hazard Analysis

Case	Failure Mode	Fault Mode (Fault Location)	Braking Distance (Severity)
1	Normal Brake System Does Not Operate	Loss of Output (Brake Valve)	2200 m (No Effect /Minor)
2	BSCU Fault Causes Loss of Braking Commands	Delay on Output (BSCU Brake Signal)	2285 m (No Effect /Minor)
3	BSCU Validity Monitor Incorrectly Report Failure Causing switch to Alternate	Noise on Output (BSCU Monitor)	2581 m (Major)
4	BSCU Power Supply Failure	Greater than Reference Value (BSCU Power)	3342 m (Catastrophic)
5	Pump Valve Leak	Lower than Reference Value (Pipe Pressure Line)	3030 m (Hazardous)

5. 결 론

본 논문은 사례연구인 공중충돌방지시스템(TCAS)과 휠 제동 시스템(WBS) 모델을 활용한 검증을 바탕으로 모델기반 안전성평가 프레임워크를 제안하였다. 제안한 모델기반 안전성평가 프레임워크는 예비시스템안전성평가에서 도출된 아이템 수준 요구사항으로부터 모델을 구현하고, 결함 주입 시험을 수행하여 시스템 및 항공기 수준의 고장 영향을 확인하였다. 또한, 획득한 데이터로부터 심각도 등급을 정량적인 분석 지표로 산출하여 객관화된 안전 지표를 제공함으로써, 기존의 경험적 안전성평가를 보완하였다.

향후 통합 비행 시뮬레이터의 Flight simulator인 X-Plane을 대신하여 FAA 14 CFR Part 60에 규정하는 정규 비행훈련 시뮬레이터 엔진을 적용하면 본 논문에서 제안하는 모델기반 안전성평가 프레임워크 데이터 신뢰의 타당성을 높일 수 있을 것으로 기대된다.

기존의 안전성 평가는 예비시스템안전성평가 단계까지의 구체적인 설계 아이템이 없기 때문에 전문가의 경험에 의존할 수밖에 없었다. 그러나 항공전자 기술의 발전으로 신기술이 도입되고 시스템의 복잡성이 증가하여 경험 기반 안전성평가가 어려워지고 있다.

따라서 본 연구에서 제시한 모델기반 안전성평가 프레임워크를 UAM의 핵심 이동수단인 PAV 및 Cargo UAS 등 최첨단 항공기 설계 시 기존 안전성 평가 절차와 병행하여 적용한다면 형식 증명(인증) 안전성 분야의 확인 및 검증을 합리적으로 수행할 수 있을 뿐 아니라 설계초기단계에 잠재 위험요소를 효율적으로 줄여 개발비용 절감 및 기간 단축을 기대할 수 있다.

References

[1] Seung Woo Yoo and Jin Young Kwon, "System safety evaluation for aircraft certification," *Journal of Aviation Development of Korea*, no. 2, pp. 191-210, Jun 2006.

[2] SAE, "Guidelines for Development of Civil Aircraft and Systems," ARP4754A, 2010.

[3] SAE, "Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment," ARP4761, 1996.

[4] R. Douglas, David D. et al. "4.4. 2 incose systems engineering handbook v3. 2: Improving the process for se practitioners," *INCOSE International Symposium*. vol. 20, no. 1, 2010.

[5] Seung Woo Yoo and In Gul Kim, "A Study on the Implementation of Aircraft System Safety Assessment using Probabilistic Analysis of Failure Data," *Journal of Aerospace System Engineering*, vol. 14, no. 0, pp. 31-38, March 2020.

[6] Peng Wang, "Formal Model Based Safety Analysis Methods and the Application," Civil Aircraft Electrical Power System Safety Assessment, pp. 259-287, 2017.

[7] A. Joshi, and M. Heimdahl, "Model-Based Safety Analysis Final Report," *NASA Techreport*, 2006.

[8] Ju-young Kim, "Developing an Integrated Simulator for Verifying Sense and Avoid Equipment for UAVs," *Master's Thesis*, Korea Aerospace University, Goyang, Korea, 2016.

[9] Gyeong Min Baek, "Avionics development environment using hardware-in-the-loop simulation," *Master's Thesis*, Korea Aerospace University, Goyang, Korea, 2016.

[10] Dong-woo Lee, Ip-su Kim and Jong-whoa Na, "A Case Study on Safety Analysis Procedure of Aircraft System using the Relex," *The Journal of Korea Navigation Institute*, vol. 22, no. 3, pp. 179-188, Jun 2018.

[11] R. Leanna, Developing Safety-Critical Software, *CRC Press*, Boca Raton, Florida, 2013.

[12] Hochstrasser, Markus, et al. "Aspects of a consistent modeling environment for DO-331 design model development of flight control algorithms," *Advances in Aerospace Guidance, Navigation and Control*, pp. 69-86, 2018.

[13] RTCA, "Software Considerations in Airborne Systems and Equipment Certification," DO-178C, 2011.

[14] FAA, "Introduction to TCAS II Version 7.1," Feb 28, 2011.