JANT 한국항행학회논문지
Journal of Advanced Navigation Technology

항공 우주 해상

J. Adv. Navig. Technol. 22(3): 179-188, Jun. 2018

Relex를 이용한 항공기 시스템 안전성 평가 절차 사례분석

A Case Study on Safety Analysis Procedure of Aircraft System using the Relex

이 동 우[1] · 김 입 수[2] · 나 종 화[1*]
[1]한국항공대학교 항공전자연구소
[2]방위사업청 헬기사업팀

Dong-Woo Lee[1] · Ip-Su Kim[2] · Jong-Whoa Na[1*]

[1]Avionics Research Institute, Korea Aerospace University, Gyeonggi-do, 10540, Korea

[2]Helicopter Project Team, Defense Acquisition Program Administration, Gyeonggi-do, 13809, Korea

[요 약]

항공전자 시스템의 개발할 때 항공 사고를 예방하기 위해서 SAE ARP4761 (민간 항공 시스템 및 장비 안전성 평가 프로세스 수행 방법 및 지침) 규격에 명시된 안전성 분석 및 평가를 수행한다. 안전성 분석은 시스템의 정상상태가 아닌 비정상상태에 대한 지식과 다른 규격들 간의 상호 연관성에 대한 지식이 요구된다. 때문에, 안전인증규격의 준수를 입증하는 자료를 자동으로 출력하는 도구가 필요하다. 본 연구는 규격의 안전성 분석 절차를 도식화하고, 안전 분석 CAD 도구들을 개별 절차에 적용하는 방법을 연구하였다. 예시 연구로서, ARP4761 부록의 여객기용 휠 제동 시스템 (WBS; wheel brake system)을 대상으로 ARP4761분석을 수행하였다.

[Abstract]

In developing avionics systems, safety analysis and evaluation specified in SAE ARP4761 (Methods and Guidelines for Civil Aviation System and Equipment Safety Assessment Process) are carried out to prevent air accidents. Safety analysis requires knowledge of the abnormal state of the system, not its normal state, and its interrelationships with other standards. Therefore, a tool that automatically outputs data which proves compliance with safety certification standards is required. In this study,In this study, Schematized the safety analysis procedure of the specification and studied the method of applying the safety analysis CAD tools to individual procedure. As an example study, ARP4761 analysis was performed on the wheel brake system (WBS) of the ARP4761 appendix.

Key word : Avionic, Safety analysis, Reliability block diagram, Fault tree analysis, Failure mode and effect analysis.

https://doi.org/10.12673/jant.2018.22.3.179

Received 8 May 2018; **Revised** 4 June 2018
Accepted (Publication) 22 June 2018 (30 June 2018)

***Corresponding Author; Jong-Whoa Na**

Tel: +82-2-300-0410
E-mail: jwna21@gmail.com

Ⅰ. 서 론

항공전자 시스템의 개발에서는 항공 사고를 예방하기 위해서 국제기능안전규격에 명시된 안전성평가를 수행한다[1]. 항공전자시스템 설계를 위한 민간부문의 국제기능안전규격은 SAE ARP4754 (항공기 시스템 인증 지침), SAE ARP4761 (민간 항공 시스템 및 장비 안전성 평가 프로세스 수행 방법 및 지침), RTCA DO-178C/254 (항공기 시스템 및 장비 소프트웨어/하드웨어 인증 가이드라인)이 있다. 이제는 항공전자시스템을 생산하려면 위의 규격들의 준수 및 이의 입증이 필수적이다.

안전성 분석은 시스템의 정상상태가 아닌 비정상상태에 대한 지식이 필요한 점과 다른 규격들 간의 상호 연관성 때문에 여러 규격에 대한 지식이 필요한 점 때문에 어렵다 [2]. 그러나 최근 항공기 부문에서도 저가격화 및 개발기간단축이 요구되고 있으며, 국내 안전설계경험이 부족하여 문제가 더 어려워지고 있다. 이 규격들 중에서도 ARP4761은 시스템의 비정상상태의 결함 및 고장을 분석하는 규격이므로 이 규격의 국내산업 적용이 어려운 상황이다. KF-X 및 드론 산업이 시작되는 시점에서 ARP4761 규격의 이해, 추진 절차의 보편화 및 산업체 보급이 시급한 상황이다.

문제의 해결방법은ARP4761규격의 입증자료를 자동으로 출력하는 도구이지만, 주제가 광범위하므로 이 연구에서는 첫 단계로서 그 규격의 안전성 분석 절차를 도식화하고, CAD 도구들을 적용하는 방법을 연구하였다. 연구내용은 두 단계로 수행되었다. 먼저 첫 단계에서는 항공기 시스템의 안전성 평가를 지원하기 위하여 ARP4761 규격에 명시된 안전성분석 절차를 단계화 하였고, 각 단계의 수행 내역 및 입·출력 자료를 식별하였다. 두 번째 단계에서는 안전성 분석 단계별 수행 내역을 효율적으로 처리하기 위해 안전 분석 CAD 도구들 중에서 RBD (reliability block diagram), FMEA (failure mode and effect analysis), FTA (fault tree analysis), 고장률 예측 등을 안전 분석에 적용하는 방법을 연구하였다.

예시 연구로서, ARP4761 부록의 여객기용 휠 제동 시스템 (WBS; wheel break system)을 대상으로 ARP4761 분석을 수행하면서 안전성 분석 CAD도구의 하나인 RELEX를 이용하여 RBD, FMEA, FTA를 수행하였다. 연구에서 제시된 절차를 이용하여 기본형 (baseline) WBS 설계가 설계 안전 목표에 미달하는 문제점과 취약점을 확인하였다. 식별된 안전성 문제를 해결하기 위하여 고장감내형 (fault tolerant) WBS를 개발하고 안전 분석을 다시 시행하여 최종적으로 최초에 제시된 안전 목표를 달성하는 것을 확인하였다.

본 논문의 구성은 다음과 같다. 2장은 항공 시스템의 국제안전규격을 적용사례 및 안전성평가 지원 소프트웨어를 소개한다. 3장은 ARP4761 안전성평가절차의 자료들과 그들 간의 연관성을 설명한다. 4장은 ARP4761의 WBS 안전성을 RELEX를 사용하여 수행한 결과와 안전 요구사항 충족 방법을 설명하고, 5장에서 결론을 맺고 향후 연구방향을 제시한다.

표 1. ARP4761 적용 연구
Table 1. Research using the ARP4761.

Case Study	HW/SW	Guidelines	Safety assessment Process	Result
Civil aircraft[3]	HW	ARP4761	FHA, PSSA (FMEA, FTA)	Safety design of wheel brake system
KC-100[4]	HW, SW	ARP4761	FHA, PSSA SSA, CCA	Certification, Failure rate
KASS[5]	HW, SW	ARP4754 ARP4761	FHA	Allocation of Design Assurance Level for KASS

Ⅱ. 연구 동향

항공전자 시스템은 항공사고 회피를 위하여 안전성을 분석하고 취약점이 발견되면 결함 감내 기능을 탑재한다. 항공 시스템 개발의 안전성 평가는 ARP4761을 적용한다[2]. 국내에서도 ARP4761를 기반으로 시스템의 안전성을 확보하는 연구가 다수 수행되었다. 대표적으로 (1) 소형제트기의 전방 휠 조향 장치 설계, (2) KC-100감항 인증을 위한 안전성 평가 등 항공기 시스템, (3) 위성보강항법시스템의 안전성 평가, (4) 철도 안전성 평가를 위한 운용 아키텍처 개발 방안 연구 등이 수행되었으며, 표1에서 확인 할 수 있다 [3]-[5].

항공전자 시스템 개발은 기능 및 안전성에 대한 요구사항이 복잡하고, 고장의 치명도(severity)가 높기 때문에, 안전성 평가에 많은 비용, 기간 및 인력이 투입된다. 안전성 분석은 시스템의 복잡도와 분석과 검토의 반복성의 문제를 해결하기 위해서, 안전성 분석용 CAD 도구 사용이 필요하다. 대표적인 안전성 분석 상용 소프트웨어로 Isograph, Item, Relex, Reliasoft 등이 사용되고 있다[4].

Relex는 ARP4761에서 요구하는 (1) 고장모드 영향분석 (FMEA), (2) 고장계통도분석(FTA), (3) 신뢰도 예측 기능을 지원, (4) EPRD/NPRD 신뢰성 라이브러리를 제공하므로, 항공전자 시스템의 안전성 분석에 적합하다. Relex를 활용하여 FTA와 FMEA를 수행하고, 수명주기를 예측하는 다양한 연구가 진행되었으며, 표2에서 확인 할 수 있다. 기존 연구에서는 Relex를 활용하여 개별적으로 타겟 또는 항목의 FTA, FMEA, MTBF를 계산하였다.

표 2. Relex 관련 연구
Table 2. Research using the Relex..

Case study	HW/SW	Procedure	Excution	Result
Braking system[6]	HW	Failure rate estimation	Identify the cause of failure	Safety design using RPN
Self-propelled Gun engine [7]	HW	Reliability Assessment	MTBF Prediction	Optimization of life cycle maintenance
The door system for railway vehicles [8]	HW	Reliability Assessment	MTBF Prediction	Optimization of life cycle maintenance

안전성 분석 평가 자동화를 위하여 여러 절차들과 CAD 도구들을 복합적으로 연동하는 문제는 시도되지 않았다. 항공기시스템의 안전성 분석 평가 자동화는 국제안전성평가 규격들과 다양한 도구들을 동시에 이해해야 한다. 따라서 항공분야 안전성 평가 규격인 ARP4761의 개별 절차에 Relex도구를 적용하여 안전 분석을 수행하는 방법을 WBS에 적용하여 설명한다.

Ⅲ. ARP 4761 기반 안전성 평가

3-1 ARP4761 수행절차

ARP4761의 안전성평가절차는 시스템 개발 주기는 기능위험성평가(FHA), 예비시스템안전성평가(PSSA), 시스템안전성평가(SSA)에 따라 진행되며, 각 단계별 안전성 평가절차의 관계를 그림1, 수행단계별 입출력 내역은 표3으로 설명한다.

첫 번째로 수행되는 FHA는 설계하려는 대상 즉 타겟 시스템의 기능을 정의하고, 기능별 고장과 심각도를 분류, 시스템이 요구하는 최상위 안전요구사항을 정의한다. FHA의 수행목표는 (1) 항공기 기능과 관련된 고장조건을 항공기와 시스템 수준에서 식별 및 분류 (2) 각 고장조건의 설계 제약, 경보와 같은 안전 요구사항을 수립 (3) 안전 목표 달성의 입증방법 설계이다. FHA는 최초 항공기 수준에서 기능과 고장 조건을 식별한 후, 시스템 수준으로 세분화 하는 top-down 방식을 따른다.

F1. 항공기(시스템) 수준의 기능을 비행단계별로 식별
F2. 식별된 기능의 고장조건을 비행단계(운용환경)별로 식별
F3. 고장조건에 의한 항공기(시스템)의 영향 판단
F4. 고장조건 영향에 의한 항공기 및 승무원의 심각도 분류
F5. 고장조건을 위한 하위수준(subsystem) 안전요구사항 할당
F6. 안전요구사항을 만족하기 위한 방법 식별

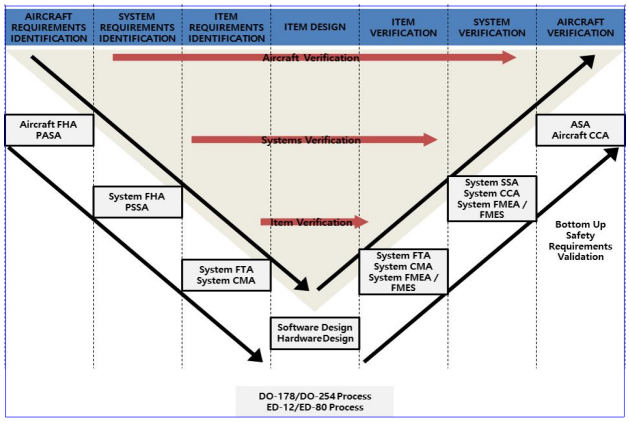


그림 1. ARP4754 시스템 개발절차와 ARP 4761 안전성 평가절차 간의 관계
Fig. 1. Relationship of the ARP4754 and the ARP4761.

표 3. ARP4761 수행 단계별 입출력 자료
Table 3. Inputs and outputs of the ARP4761 phase.

Phase	Inputs	Outputs
Aircraft Level AFHA	- The list of the top-level aircraft functions. - The aircraft objectives and customer requirements. - Initial design decisions	- FHA input function list - Environmental and Emergency Configuration list - Derived safety requirements for the design at each level
System Level SFHA	- The list of the main functions to consider - A functional diagram showing external interfaces - The list of functions created in the higher design level FHAs - The list of the failure conditions identified in the higher design level FHAs - The requirements defined in design requirements and objectives documents - The design options chosen at the upper level and their rationale	- FHA Report which contains the following (1) Function Description (2) Failure Conditions (3) Phase of Operations (4) Effect of the Failure Condition on the Aircraft, Crew and Occupants (5) Classification of the Failure Condition (6) Reference to Supporting Material (7) Verification Method (for the design solution chosen to meet the safety objective)
PSSA	- Failure conditions and requirements identified in the aircraft and/or system level FHA - The system architecture description and the rationale for this choice - The list and functions of system equipment - The system interfaces and relations with other systems - Preliminary Common Cause Analyses	- Planned compliance method with FHA requirements - Updated FHA - Material supporting the classification list - A failure condition list - Lower level safety requirements (Including Development Assurance Levels) - Qualitative FTAs - Preliminary CCAs - Operational requirements (flight and maintenance
SSA	- System architecture description and the associated design rationale - Systems interfaces and their interactions with the items of the adjacents systems - Requirements and failure conditions identified in the System Level FHA / PSSA - List of functions and the associated rationale from the System Level FHA - Common Cause Analyses results - Results of all the supporting materials and lower level studies required in the FHA/PSSA	- The updated failure condition list or FHA which includes the rationale showing compliance with safety requirements - Documentation showing how requirements for the design of the system items' installation have been incorporated - The materials used to validate the failure condition classification - The safety maintenance tasks and associated "Not to Exceed Time" - Documentation showing how the system and items have been developed in accordance with assigned development assurance levels

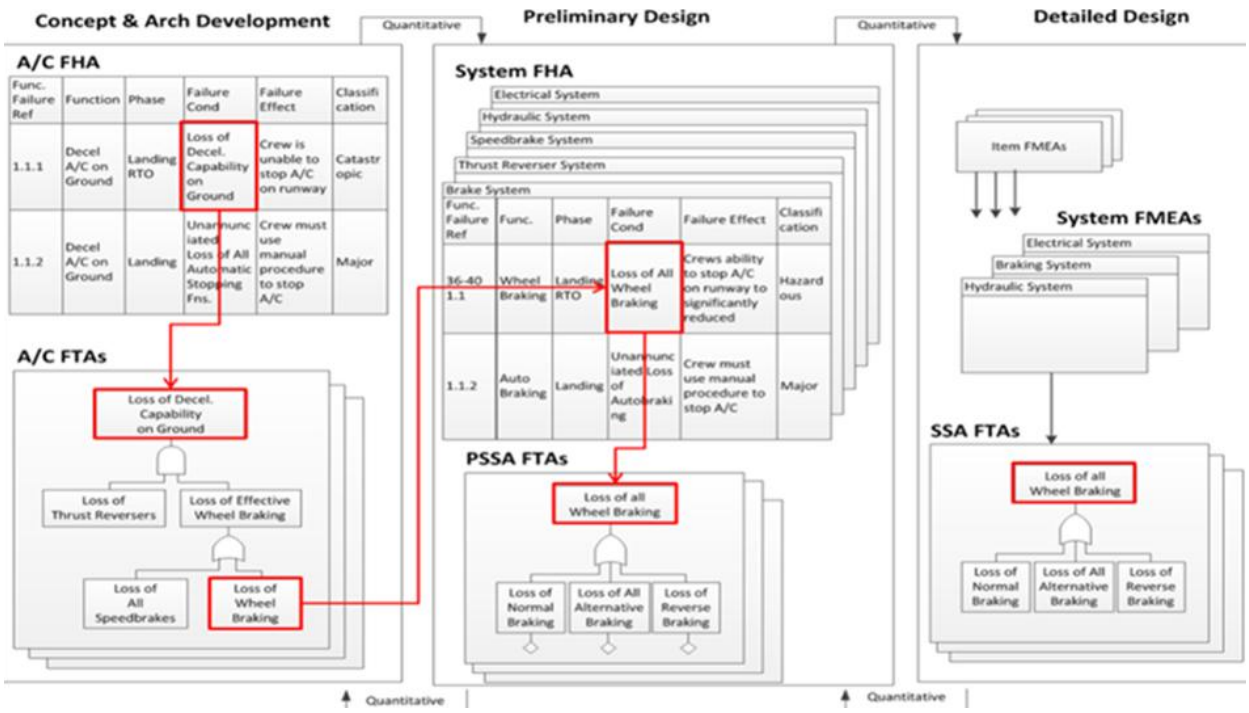


그림 2. SAE ARP4761에서 FHA, FTA, FMEA 분석 관계
Fig. 2. A relationship of the FHA, the FTA, the FMEA in SAE ARP4761.

항공기 수준 FHA (AFHA) 이후 항공기의 기능을 수행하는 (항공기 하위 수준인) 시스템에 대해 다시 F1 ~ F6을 적용하여 시스템 수준 FHA (SFHA)를 수행한다. FHA의 수행 결과물인 시스템 수준 안전 요구사항, 검증계획은 이후에 수행되는 PSSA의 입력 자료로 활용된다.

두 번째로 PSSA는 시스템 구성요소에 대한 고장조건들과, 이에 대응하는 안전요구사항을 정의하고, 안전 목표를 달성하기 기능적/구조적 대응방안을 수립한다. 안전 목표를 달성하기 위한 구체적인 방안으로 파티셔닝, 자기진단, 모니터링, 유지보수 절차 등을 포함한다. PSSA는 FHA에서 식별한 고장조건의 초래하는 위협요소를 시스템 수준에서 부품수준까지 추적한다. 또한 FHA에서 정의한 안전요구사항이 충족되었는지를 분석한다. PSSA의 수행절차는 다음과 같다.

P1. 항공기/시스템 수준 안전요구사항 식별
P2. 제안된 개념설계내역이 목표로 하는 안전요구사항 만족 여부 확인
P3. 하위수준의 아이템 설계, 설치 및 운용에 대한 안전요구사항 할당
P4. PSSA, FTA에서 확인된 고장모드 및 목표 신뢰성을 하위수준 설계 요구사항으로 할당

PSSA를 수행하면 항공기 및 시스템 FHA 결과로 산출된 초기안전요구사항이 시스템 수준의 안전요구사항으로 확정된다. PSSA 결과로 생성된 시스템수준 안전요구사항, 정성적 고장계통도 분석, 운영 요구사항 등은 SSA 분석 자료로 활용된다.

마지막으로 SSA는 시스템 구현·통합하는 단계에서 설계 시스템과 구현 시스템이 정의된 안전 요구사항과의 충족여부를 검증한다. SSA는 PSSA와 유사하지만 그 범위가 다르며, 하위수준에서 시스템 수준까지 상향식으로 진행된다. PSSA는 시스템의 설계내역을 평가하고, 시스템/부품 안전요구사항들을 도출하는 방법인 반면에 SSA는 구현된 시스템이 정의된 안전요구사항들을 충족하는지 정성적·정량적으로 입증한다. SSA의 수행절차는 다음과 같다.

S1. FHA/PSSA에서 설정 된 항공기 수준 영향 분류에 대한 타당성 확인
S2. 항공기 설계 요구사항으로부터 파생된 안전 요구사항이 충족되었는지 검증
S3. CCA에서 식별된 설계 요구사항이 충족되었는지 검증
S4. 시스템 수준 FHA에서 설정된 설계 요구사항이 충족되는지 검증
S5. 시스템 수준 SSA와 항공기 수준 FHA의 연결

3-2 시스템 개발단계와 안전성 평가단계의 관계

항공기 수준 기능 및 위험분석 고장조건이 시스템 수준 고장조건으로 세분화 되고 상세설계단계에서 FMEA, FTA 분석방법으로 설계의 안전성을 확인한다. 안전성 평가는 시스템의 기능에 대하여 발생 가능한 모든 고장조건에 대하여 분석을 수행한다. 시스템 개발 단계별 안전성평가 절차와 자료의 활용 순서는 그림 2 으로 확인 할 수 있다.

항공기 및 시스템 수준 기능 분석의 항공기 수준 기능에는 항공기의 추력 제어, 조종면 제어, 위치 및 방위각 판단과 같은 기본 기능이 있다. 항공기 시스템의 기능 분석 결과는 그림 3으

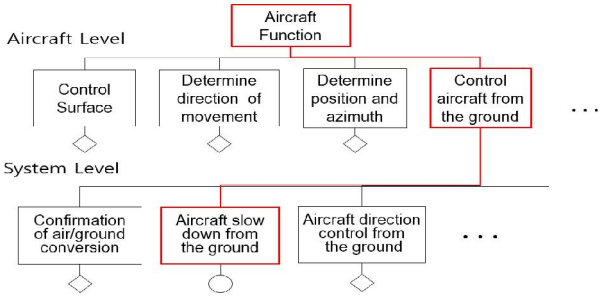


그림 3. 항공기 및 시스템 수준 기능분석
Fig. 3. The functional analysis of aircraft and system level.

로 확인 할 수 있다. 그러나 본 연구에서는 항공기 수준의 기능 "지상에서 항공기 제어"와 시스템 수준의 기능 "지상에서 항공기 감속"에 해당되는 WBS의 안전성 평가만을 다룬다. 분석의 대상은 그림 3의 붉은색 선 흐름을 따라 "지상에서 항공기 제어", "지상에서 항공기 감속" 기능에 관련된 고장 조건의 하나인 "loss of deceleration capability on ground: 지상에서 항공기 감속 기능 상실"의 분석 절차를 설명한다.

① 항공기 수준 FHA를 수행하면서 "loss of deceleration capability on ground: 지상에서 항공기 감속 기능 상실" 항공기수준의 고장조건 영향과 심각도 식별

② FTA를 이용하여 항공기 기능 "decelerate the wheels on ground: 지상에서 항공기 감속"에 영향을 미치는 고장 요인을 분석(표4)

③ 그 중 "loss of all wheel braking: 모든 휠 제동의 상실" 시스템수준의 고장조건에 대해서 분석한다. 시스템수준 FHA를 수행하여 고장조건과 영향, 설계 요구사항, 안전 요구사항을 표 또는 보고서 형식으로 정리

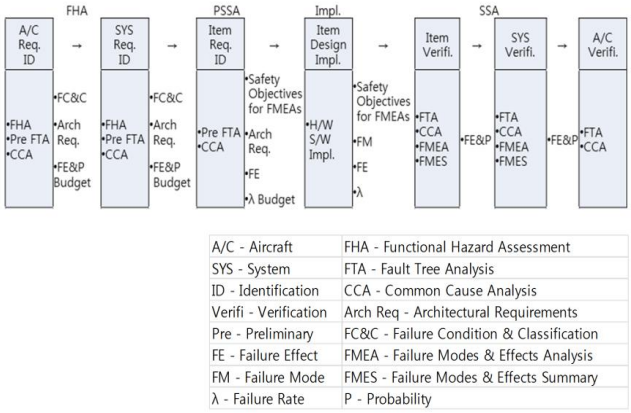
④ PSSA 수행: 여러 결함감내 기법들 중의 하나인 FTA를 사용하여 "loss of all wheel braking: 모든 휠 제동의 상실" 고장조건의 안전 목표 수립을 포함하는 안전 요구사항 개발

⑤ 안전 요구사항을 이용하여 시스템 상세설계 수행 후, 설계 결과물이 안전요구사항 및 안전 목표를 충족하는지 확인. 확인 절차는 상향식으로 아이템 수준부터 시작하여 시스템 수준까지 단계별로 수행

시스템 개발주기에 따라 안전성 평가 활동 내용은 그림4로 확인 할 수 있다. 음영 처리된 부분은 시스템 개발주기의 각 단

표 4. 지상에서 항공기 감속 기능의 고장조건 식별
Table 4. Identification of failure condition of aircraft deceleration function on the ground.

System function	Failure condition
Decelerate the wheels on ground	- Loss of all wheel braking
	- Reduced deceleration capability
	- Loss of all auto stopping features
	- Inadvertent deceleration



A/C - Aircraft	FHA - Functional Hazard Assessment
SYS - System	FTA - Fault Tree Analysis
ID - Identification	CCA - Common Cause Analysis
Verifi - Verification	Arch Req - Architectural Requirements
Pre - Preliminary	FC&C - Failure Condition & Classification
FE - Failure Effect	FMEA - Failure Modes & Effects Analysis
FM - Failure Mode	FMES - Failure Modes & Effects Summary
λ - Failure Rate	P - Probability

그림 4. 안전성 평가절차 별 산출물
Fig. 4. Output of each safety evaluation procedure.

계와 수행해야 할 안전성평가 방법을 나타낸다. 개발주기의 각 단계 사이에는 안전성평가에 사용될 수 있는 입·출력물이 있다. 모든 절차가 필요하지는 않지만 분석자는 위 사항을 고려해 적용여부를 결정해야 한다.

3-3 ARP4761의 안전성평가 기법

ARP4761은 고장 계통도 분석, 마르코프 분석, 신뢰성 블록도 또는 이와 합당하다고 인정되는 안전성평가 분석기법을 사용할 것을 권고한다[3]. 첫 번째로 고장계통도 분석은 논리연산 게이트를 이용하여 고장모드에서의 고장의 영향 간 관계를 보여준다. 가장 일반적인 논리 게이트는 AND와 OR이다. AND 게이트는 모든 입력조건이 공존할 때 상위수준 사건의 출력을 만든다. OR 게이트는 하나 혹은 다수의 입력조건하에서 상위수준 사건의 출력을 만들어 낸다.

두 번째로 마르코프 분석은 다양하게 존재할 수 있는 시스템의 상태 확률을 시간 함수로 계산한다. 마르코프 분석모델에서의 상태는 고장과 시스템 중복여유의 동작에 따른 전체 시스템의 상태를 나타낸다. 상태간의 변화가 일어날 때 고장률 또는 중복여유와 같은 변수가 주어지고 각각의 상태로의 변화는 무작위로 일어난다고 본다. 정의된 마지막 상태에 도달할 확률은 그 상태에 도달하기 위한 조합으로 계산될 수 있다.

세 번째로 신뢰성 블록도는 고장 계통도 분석의 논리 게이트를 고장의 관계 경로로 대체하여 시스템을 분석한다. 각 고장이 직렬로 연결된 형태는 OR 게이트, 병렬로 연결된 형태는 AND 게이트로 표현가능 하다. 신뢰성 블록도는 구조 그림을 이용해서 개발자 간의 의사소통을 원활하게 하고 여러 가지 대안 설계방법들을 비교할 수 있는 장점이 있다.

항공기 시스템의 안전성 분석은 분석의 대상이 되는 시스템의 복잡도가 높으며 부품 별로 운영데이터가 요구되어 CAD 도구의 지원이 필요하다. 신뢰성 분석에 많이 사용되는 도구는 Item, Isograph, Windchill (Relex), Reliasoft 등에서 공급한다[11,12,13,14]. 본 연구는 Relex CAD 도구와 EPRD, NPRD 고장률 데이터 라이브러리를 이용하여 안전을 분석하였다[13].

Ⅳ. 안전성 평가 사례연구

ARP4761는 시스템 개발 단계별 안전성 평가절차와 각 단계별 분석 내용을 제시한다. 신뢰성 평가도구를 활용하여 안전성 평가절차와 분석 방법을 설명하기 위해, ARP4761 에서 제시하는 WBS의 “지상에서 항공기 감속”에 대한 고장 분석을 수행한다. 항공기 수준에서 시스템 수준까지 “지상에서 항공기 감속”에 대한 기능 위험평가 (FHA)와 예비 시스템 안전성평가 (PSSA), 시스템 안전성 평가(SSA)를 수행한다. 안전성 평가 입증자료는 신뢰성 분석 도구인 Relex를 활용하여 생산한다. 본 장에서는 WBS의 “지상에서 항공기 감속” 기능의 안전성 평가를 위해, 4.1에서 WBS의 구성과 기능을 설명하고, 4.2에서 안전성 평가 사례를 제시한다.

4-1 WBS의 구성 및 기능

WBS는 green 및 blue 유압서브시스템, BSCU(brake steering control unit), 메인 기어 휠 조립체로 구성된다. WBS 시스템 구성은 그림 5로 확인 할 수 있다. Green 및 blue 유압서브시스템은 이중화 된 유압펌프에서 압력을 공급받고, 메인 기어 휠 조립체의 서보 밸브로 제동한다. 각 유압 라인은 차단 밸브와 미터링 밸브를 가지고 있으며, blue 유압서브시스템에는 비상모드 제동과 계류를 위한 축압기가 있다. BSCU는 페달 위치를 전기적으로 입력 받고, 제어신호를 브레이크로 전송한다. 또한 BSCU는 항공기와 제동시스템 상태를 모니터하고, 비행제어 컴퓨터에 경고, 표시, 유지보수 등의 정보를 전송한다.

항공기 착륙동작은 정상, 대체, 비상의 세 가지 모드로 구성된다. (1) 정상모드는 green 유압서브시스템으로부터 브레이크 어셈블리의 서보밸브로 제동과 미끄럼방지 기능을 수행한다.

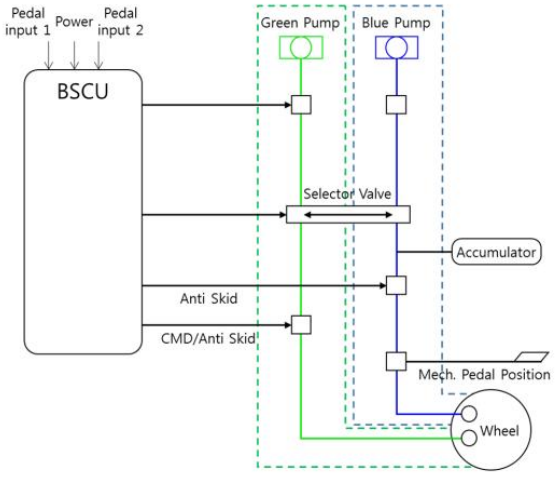


그림 5. WBS 구성
Fig. 5. Configuration of WBS.

(2) 대체모드는 green 유압서브시스템 고장으로 정상모드가 동작 할 수 없는 경우 발동한다. 대체모드가 발동되면 glue 유압서브시스템으로 자동으로 전환되어 네 개의 서보밸브 만으로 항공기 제동과 미끄럼방지 기능을 수행한다. (3) 비상모드는 정상모드와 대체모드 동시에 발동할 수 없는 상황에서, blue 유압서브시스템에 연결된 축압기의 압력으로 제한된 제동을 수행한다.

4-2 WBS 안전성 평가 사례

WBS 개발절차에 관련된 안전성 평가는 세 단계로 수행한다. 첫 번째 FHA 단계에서는 항공기와 시스템 수준에서 WBS의 기능과 위협요소를 분석하여 안전 목표를 설정한다. 두 번째 PSSA 단계에서는 WBS의 시스템 및 아이템에 안전요구사항을 할당한다. 세 번째 SSA 단계에서는 개발된 설계와 구현 시스템이 이전에 설정된 안전요구사항과 안전 목표를 충족하는지 확인한다. WBS 안전성 평가 사례를 Relex도구의 FTA, FMEA, RBD를 사용하여 분석한다.

1) 항공기 수준 FHA

분석 자료는 ARP4761의 부록에서 이해를 돕기 위해 제공하는 가상 항공기에 대한 FHA이다. FHA는 항공기 수준 FHA 수행 후에 시스템 수준 분석을 진행한다. 항공기 수준의 FHA 분석 내용은 다음과 같다

F1: 최초 설계 요구사항으로부터 추력 제어기능, 조종면 제어기능, 위치 및 방위각 판단 기능과 같은 항공기의 기본기능을 식별한다. 사례연구는 “지상에서의 항공기 감속 기능”을 대상으로 한다.

F2 “지상에서의 항공기 감속 기능”에 관련된 고장조건을 판단하기 위해 항공기 운용단계와 운용 환경 및 발생 가능한 비상상황에 대한 분류를 수행한다. 항공기 운용단계에는 “지상 활주, 이륙, 착륙, 이륙 포기 상황(RTO)” 등이 있고, 운용 환경 및 발생 가능한 비상상황에는 “활주로 노면상태, 활주로 길이, 배풍/측풍, 엔진 정지, 유압시스템 고장, 전기 계통 고장” 등이 있다. 항공기 운용단계와 운용환경을 고려해서 고장조건을 식별한다.

F3 F2에서 식별한 각 고장조건 별로 항공기와 승무원 및 승객에 미치는 영향을 판단한다. 여기에서는 “지상에서의 항공기 감속 기능 상실로 인해 승무원이 활주로 내에서 항공기를 정지시키지 못하는 상황”을 고려하였다.

F4 F2에서 식별한 각 고장조건으로 인한 영향의 심각도를 분류한다. 심각도는 ARP4761의 고장 발생 확률과 고장조건의 영향에 따른 심각도를 참조하여 분류된다.

F5 안전 목표를 달성하기 위해 시스템 수준의 각 부품이 충족해야 하는 고장률을 하위 수준 시스템에 할당한다.

F6 항공기 수준 FHA 과정 검토를 통해 구성품 변경, 중복여유설계의 추가 등 설계의 변경이 발생할 수 있다.

표 5. 고장발생 확률과 고장 조건의 영향에 따른 심각도 구분
Table 5. Severity classification based on the probability of failure and effect of failure condition.

Probability (Quantitative)	Probability (Descriptive)	Failure Condition Severity	Failure Condition effect
1.0	Frequent	Minor	-Slight reduction in safety margins -Slight increase in crew workload -Some inconvenience to occupants
1.0x10-5	Remote	Major	-Significant reduction in safety margins or functional capabilities -Significant increase in crew workload or in conditions impairing crew efficiency -Some discomfort to occupants
1.0x10-7	Extremely Remote	Hazardous	-Large reduction in safety margins or functional capabilities -Higher workload or physical distress such that the crew could not be relied upon to perform tasks accurately or completely -Adverse effects upon occupants
1.0x10-9	Extremely Improbable	Catastrophic	-All failure conditions which prevent continued safe flight and landing

2) 시스템 수준 FHA

시스템 수준의 FHA 분석 내용은 다음과 같다.

F1 시스템 수준 FHA는 WBS의 기능을 식별한다. WBS의 기능에는 승무원에 의한 휠 제동 기능, 자동 제동 기능, 미끄러짐 방지기능 등이 있다.

F2 항공기 수준 FHA와 같이 "승무원에 의한 휠 제동 기능"에 관련된 고장조건을 판단하기 위해 항공기 운용단계와 운용 환경 및 발생 가능한 비상상황에 대한 분류를 수행한다. "모든 휠 제동기능의 상실", "모든 휠의 제동기능 일부 상실", "휠 제동의 비대칭적 상실", "의도치 않은 휠 제동의 적용" 고장조건을 식별하였다.

F3 "모든 휠 제동기능의 상실" 고장조건은 활주로에서 항공기를 멈추게 할 수 없게 되는 영향이 발생한다.

F4 활주로에서 항공기를 멈추게 할 수 없게 되는 상황은 고장 발생확률과 고장조건의 영향에 따른 심각도(표5)에 의해 위험한 상황으로 분류한다.

F5 항공기 수준 FHA와 시스템 수준 FHA 결과 "모든 휠 제동능력을 상실" 고장모드에 대해서 발생 가능성은 비행당 5×10^{-7}이하가 되도록 결정한다.

F6 시스템 수준 FHA 결과를 반영해 구성품 변경, 중복여유 설계의 추가 등 설계의 변경이 발생할 수 있다.

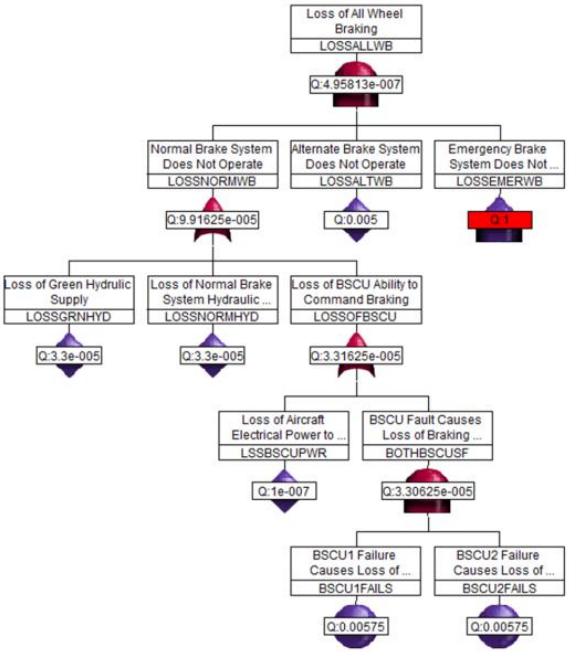


그림 6. 모든 휠 제동의 상실 고장수목분석
Fig. 6. Fault tree anlaysis of loss of all wheel braking.

3) 휠 제동 시스템 PSSA

PSSA 단계는 WBS의 개념설계 및 예비설계 단계에서 수행된다. PSSA 단계에서는 안전 요구사항 및 목표를 충족하는 설계가 완성된 이후라도 설계변경으로 인하여 안전성/신뢰성 평가 재수행이 빈번하게 발생한다. 따라서 CAD를 이용한 평가하면 시간과 비용을 절약할 수 있다. RELEX 도구의 FTA 기능을 사용하여 예상되는 고장률을 도출한다.

P1 항공기 및 시스템 FHA를 통해 결정된 안전 요구사항 목록을 작성하고, 이를 충족시키기 위한 설계를 결정한다.

P2 P1절차를 통해 결정된 설계 변경 사항이 안전 요구사항을 충족시키는지를 평가한다. 평가에는 FTA가 사용될 수 있다. 휠 제동시스템의 안전 요구사항 목록 및 설계 결정의 "1. 착륙 또는 이륙 단념 간 휠 제동의 상실은 비행당 5×10^{-7}보다 작아야 한다."는 휠 제동시스템의 안전 요구사항이 있다. 그러나 하나의 BSCU와 유압서브시스템으로 구성된 Baseline WBS에 의한 고장발생확률은 5.75×10^{-3} 만족해야 하므로 유압서브시스템에 대해서 하나 이상의 유압서브시스템을 설치하는 결함감내 설계를 도입해야 한다.

P3 P2의 방법으로 얻어진 시스템 아키텍처에 대해서 각 노드에 허용 가능한 고장발생확률을 할당한다. 그림 6은 "모든 휠 제동능력을 상실"을 최상위 사상(top event)으로 하는 RELEX FTA분석이다. 정상 제동 시스템의 고장발생확률은 해당 기능의 중요도를 고려해 가장 엄격하게 1×10^{-4}으로 할당되었다.

P2-1 WBS의 PSSA FTA에서 주요 기능을 수행하는 서브시

FMEA Worksheet

	Function Name (Mo...	Failure Mode (Mo...	Failure Rate (M...	Mission Phase (M...	Failure Effect (Mo...	DetectionMethod (Mode)	Comments (Mode)
1	+5 Volt	+5V out of spec.	0.214300	All Phases	Possible P/S shutdown	Power Supply Monitor tri... shuts down supply and passes "invalid power supply(P/S)" to other BSCU system	BSCU channel fails
2		+5V short to ground	0.285700	All Phases	P/S shutdown	Power supply monitor passes invalid P/S to other BSCU system	BSCU channel fails
3		Loss of / reduced filtering	0.357100	All Phases	Increase Ripple	May pass out of spec voltage to rest of BSCU if ripple is such that it is not detected by the P/S monitor	May cause spurious P/S monitor trip
4		+5V open	0.571400	All Phases	P/S shutdown	Power supply monitor passes invalid P/S to other BSCU system	BSCU channel fails
5		No Effect	0.142900	All Phases	No Effect	None/No Effect	No Effect
6	Total Failure Rate of +5V Supply		#.#				

그림 7. BSCU의 FMEA 분석[SAE ARP 4761]
Fig. 7. FMEA analysis of BSCU[SAE ARP 4761].

스템인 BSCU를 세부적으로 분석하였다. 휠 제동시스템의 안전 요구사항 목록 및 설계 결정의 "1. 착륙 또는 이륙 단념 간 휠 제동의 상실은 비행당 5×10^{-7}보다 작아야 한다." 는 휠 제동시스템의 안전 요구사항이 있었다. 그러나 단일 모듈의 BSCU를 가진 Dual-Hydraulic WBS는 2.91×10^{-5} 의 고장발생확률을 가진다. 안전요구사항 충족을 위해 고장감내 기법이 결정되어야 한다.

P3-1 고장감내 기법을 도입하여 WBS의 PSSA에서 BSCU의 "BSCU고장으로 인한 제동명령의 상실"의 전체 안전요구사항을 완성한다.

4) 휠 제동 시스템 SSA

SSA단계는 개발된 시스템이 FHA와 PSSA의 안전요구사항 및 목표 충족 여부를 확인한다. SSA분석 절차는 다음과 같다.

S1 시스템을 설계한 후 통합하는 단계에서는 이전에 할당된 고장률을 만족하는지 부품수준에서 시스템 수준까지 상향식으로 확인하고 안전 목표를 달성하는지 검증하는 절차를 수행한다. FTA의 기본사상 고장률은 상용제품의 공개된 신뢰성 정보, 운용을 통한 경험적 자료, 유사제품의 신뢰성 정보는 FMEA로 분석한다. 그림 7은 BSCU의 +5Volt 전원공급장치의 FMEA예이다.

S2 "BSCU고장으로 인한 제동명령의 상실"을 정상사상으로 하는 FTA분석한다. SSA단계의 FTA는 기본적으로 PSSA단계의 FTA와 동일하다.

S3 설정된 안전 요구사항에 대한 검증은 SSA를 통해서 이루어진다. SSA는 최하위 노드에서부터 시스템 수준까지 상향식으로 이루어진다.

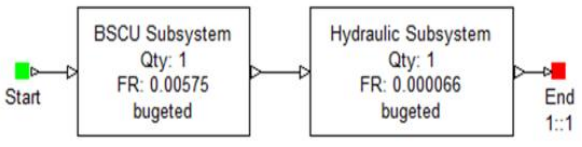


그림 8. FHA 단계에서 baseline WBS의 RBD
Fig. 8. Reliability block diagram of baseline WBS at FHA.

4-3 RBD(reliability block diagram)를 이용한 설계 검토

RBD는 시스템의 안전요구사항을 충족시키기 위한 설계 변경을 고려할 때 유용하다. RELEX도구를 이용해서 실제 시스템을 구현하기 전에 고장전파 관계를 분석하고 구성요소들을 재배치하여 시스템 전체의 신뢰도를 미리 예측할 수 있다.

1) FHA 단계의 항공기 수준 설계

안전설계 초기 FHA의 항공기 수준의 안전 목표를 설정하기 위하여 시스템 요구사항 및 유사 시스템 설계를 분석하여 WBS를 비행 당 5×10^{-7}이하의 고장발생률을 가지도록 안전 목표를 설정하였다[3]. 일반적으로 고 신뢰성 시스템은 결함감내 장치를 탑재하기 때문에 시스템 가격상승의 문제가 발생한다. 따라서 저비용으로 설정된 안전목표를 만족하는 WBS를 개발하기 위하여 단일체계로 구성되는 baseline WBS와 함께, 다양한 고장 감내 설계안을 분석 할 수 있다.

A. Baseline Wheel Brake System

항공기 제동을 위한 WBS에는 BSCU와 유압작동부가 필요하다. 유사시스템의 운용기록을 통해 경험적으로 얻어진 BSCU모듈과 유압서브시스템의 비행당 고장발생가능성은 5.75×10^{-3}과 6.6×10^{-5}이다. Baseline WBS를 RDB로 설계한 결과는 그림8로 확인 할 수 있으며, 시험한 결과 전체 고장발생률은 약 5.82×10^{-3}이다. WBS의 고장률은 WBS 안전요구사항을 만족시키지 못하므로 결함 감내 설계가 요구된다.

2) SSA 단계의 시스템 신뢰도 검증

"모든 휠 제동 기능의 상실" 고장에 대한 RBD 분석을 수행하였다. 그림 9는 RBD를 통해 결정된 최종 WBS의 시스템 구성이다. 전체 시스템은 BSCU파트와 기계적 작동파트가 직렬구조로 구성되어 있다. BSCU는 primary unit과 secondary unit이 병렬로, 버퍼와 스위치가 직렬로 구성되어 있고, 기계적 작동파트는 green 및 blue 유압서브시스템이 병렬로 구성되어 있고 각 유압서브시스템은 펌프와 수개의 밸브가 직렬구조로 되어있다. WBS의 신뢰도를 확인하기 위해서 정상, 대체, 비상모드 전체의 고장과 연관된 부품을 식별해서 사용된 각 부품의 신뢰도 데이터를 수집하였다. Green과 blue 유압서브시스템 및 BSCU의 system1 과 system2는 상시 대기상태이다.

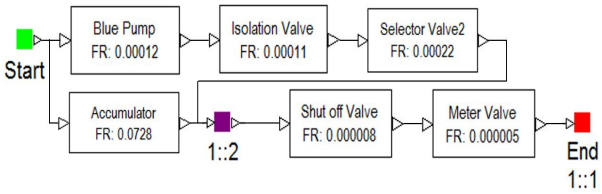


그림 9. SSA 단계에서 baseline WBS의 RBD
Fig. 9. Reliability block diagram of baseline WBS at SSA.

Ⅴ. 결론 및 향후 과제

ARP4761 안전성평가절차는 그 난이도와 복잡성 때문에 전문 분석도구 소프트웨어의 지원이 필요하다. 따라서 본 연구에서는 ARP4761 안전성평가절차를 해석하여 각 단계별 입·출력물을 정리하였다. 이렇게 구조화된 각 단계별 입·출력물에 전문 분석도구를 이용하는 방법을 보여주었다. SAE ARP4761에서 제공하는 가상의 항공기를 활용하여 분석하였다. SAE ARP4761는 자료의 일부만을 제공하므로 나머지 안전성평가에 필요한 데이터는 수용 가능한 수준에서 추정하여 사용하였다. 항공기 수준 FHA, PSSA, SSA에 이르는 전반적인 안전성 평가 절차를 따라 기술하였으며 CCA는 생략되었다. 안전성 평가는 항공 시스템 개발에 반드시 적용해야 하는 사항이기 때문에 국제기구의 국제기능안전규격의 획득이 품질 측면 및 사업 측면에서 중요하다. 본 연구는 CAD 도구 활용하여 안전성 분석 자료를 생산하였다. 향후 연구에서는 복합 시스템의 안전 분석 및 국제기능안전 인증업무를 자동화 할 수 있는 CAD 도구 개발을 수행할 수 있다.

Acknowledgement

본 연구는 산업통산자원부 항공우주부품기술개발사업의 연구비 지원(10067079:초음속 항공기 장착용 원뿔형 다기능 통합 대기자료 시스템 개발)에 의해 수행되었습니다.

References

[1] A. Boydston and W. Lewis, “Qualification and reliability of complex electronic rotocraft systems,” in *Proceeding of AHS Specialists' Meeting on Systems Engineering*, Hartford: CT, pp. 2-17, 2009.

[2] J. Wang, Y. Pu, and G. Li, “Fault model libraries for safety analysis and their ontology-based reuse,” in *Proceeding of the Conference on Computational Intelligence and Security*, Guangzhou: China, pp. 1-4, 2012.

[3] Guidelines and methods for conducting the safety assessment process on civil airborne systems ans equipment, Society of Automotive Engineers Inc, USA, ARP4761, 1996

[4] S. H. Hong, J. Y. Lee, J. Y. Kim, and Y. Park, “Study on safety assessment and certification of part 23 avionics system”, in *Proceeding of the Conference on the Korean Society for Aeronautical and Space*, Jungsun: Korea, pp. 391-394, 2013.

[5] D. H. Bae, “Allocation of design assurance level for KASS based on international standards,” *The Journal of Advanced Navigation Technology*, Vol. 20, No. 5, pp. 1-7, June 2016.

[6] T. Ting, Y. Lu, T. T. Zhou, H. L. Jing, H. Sun, “FTA and FMEA of braking system based on relex 2009,” in *Proceeding of the Conference on Information Systems for Crisis Response and Management*, Harbin: China, pp. 106-112, 2011.

[7] G. W. Jeon, D. Y. Ju, “Determination of the maintenance period for self-propelled artillery engine by using RELEX,” in *Proceeding of Conference of Korean Institute of Industrial Engineers*, Seoul: Korea, pp. 301-308, 2004.

[8] C. S. Kim, H. S. Lee, “A study on the reliability analysis methodology of passenger door system of electrical type,” *The Journal of the Korea Society of Systems Engineering*, Vol. 10, No. 1, pp. 43-48, June 2014.

[9] Item. How to use item [Internet]. Available: http://www.itemsoft.com/item_toolkit.html

[10] Reliasoft. How to use ReliaSoft [Internet]. Available: https://www.reliasoft.com/products

[11] Relex. How to use Relex [Internet]. Available: https://www.ptc.com/en/products/plm/capabilities/quality

[12] Isograph. How to use reliability workbench [Internet]. Available: https://www.isograph.com/software/reliability-workbench/

이 동 우 (Dong-Woo Lee)
2014년 8월 : 한국항공대학교 항공전자공학과 (공학박사)
2014년 ~ 현재: 한국대학교 항공전자연구소 연구원
※관심분야: 고신뢰성 시스템, 영상처리, 항공전자, 안전설계 및 검증

김 입 수 (Ip-su, Kim)
2018년 2월 : 한국항공대학교 항공전자공학과 (공학석사)
2018년 ~ 현재: 방위사업청 사업관리담당
※관심분야: 고신뢰성 시스템, 항공전자, 안전설계 및 검증

나 종 화 (Jong-Whoa Na)
1995년 2월 : 아리조나대학교(미) 컴퓨터공학과 (공학박사)
2005년 ~ 현재: 한국항공대학교 항공전자 및 정보통신공학부 교수
※관심분야: 컴퓨터 시스템, 고신뢰성 시스템