J. Korean Soc. Aeronaut. Space Sci. 50(4), 259-267(2022)
DOI:https://doi.org/10.5139/JKSAS.2022.50.4.259
ISSN 1225-1348(print), 2287-6871(online)

항공기 시스템의 치명적인 공통 요인을 식별하기 위한 고장-안전 요구분석 절차 제안

임산하[1], 이선아[2], 전용기[3]

Proposal of a Fail-Safe Requirement Analysis Procedure to Identify Critical Common Causes an Aircraft System

San-Ha Lim[1], Seon-ah Lee[2] and Yong-Kee Jun[3]
Rotary-wing Division, Korea Aerospace Industries, Sacheon, Republic of Korea[1]
Department of Aerospace and Software Engineering, Department of AI Convergence Engineering, Gyeongsang National University, Jinju, Republic of Korea[2,3]

ABSTRACT

The existing method of deriving the fail-safe design requirements for the domestic developed rotary-wing aircraft system may miss the factors that cause critical system function failures, when being applied to the latest integrated avionics system. It is because the existing method analyzes the severity effect of the failures caused by a single item. To solve the issue, we present a systematic analysis procedure for deriving fail-safe design requirements of system architecture by utilizing functional hazard assessment and development assurance level analysis of SAE ARP4754A, international standard for complex system development. To demonstrate that our proposed procedure can be a solution for the aforementioned issue, we set up experimental environments that include common factors that can cause critical function failures of a system, and we conducted a cross-validation with the existing method. As a result, we showed that the proposed procedure can identify the potential critical common factors that the existing method have missed, and that the proposed procedure can derive fail-safe design requirements to control the common factors.

초 록

기존의 국내 개발 회전익 항공기 시스템의 고장-안전 설계 요구사항 도출 방법은 최신 통합형 항공전자 시스템에 적용 시 단일 항목의 고장으로 인하여 치명적인 시스템 기능 고장을 발생시키는 요인을 누락할 수 있다. 그 원인은 고장-안전 설계 대상을 선정함에 있어 단일 품목의 체계 기능 고장 영향성을 그 기준으로 함에 있다. 본 연구에서는 이를 해결하기 위하여 민수 항공기 개발 국제 표준인 SAE ARP4754A의 기능적 위험요소 평가 및 개발보증수준 할당 절차를 활용하여, 시스템 구조의 고장-안전 설계 요구사항을 도출하기 위한 체계적인 분석 절차를 제시한다. 또한 본 연구에서 제시한 절차가 앞서 제시한 문제점을 해결할 수 있는지를 확인하기 위하여 치명적인 기능 고장을 발생시킬 수 있는 단일 요인을 내포한 시스템 구조를 가정하여 교차 검증을 수행하였다. 그 결과 기존 연구 방법으로는 누락되었던 치명적인 공통 요인을 식별할 수 있었고 이를 통제하기 위한 고장-안전 설계 요구사항이 도출됨을 확인하였다.

† Received : December 4, 2021 Revised : February 22, 2022 Accepted : March 10, 2022
[1] Research Engineer, [2] Associate Professor, [3] Professor
[3] Corresponding author, E-mail : jun@gnu.ac.kr, ORCID 0000-0002-4753-3651

Key Words : Fail-Safe Design Requirement(고장-안전 설계 요구사항), Rotary-Wing Aircraft System(회전익 항공기 시스템), System Safety Analysis(체계안전성 분석)

Ⅰ. 서 론

품목 및 시스템의 개발 과실이 개발 및 검증 과정에서 식별되지 않고 운용 중인 항공기에서 발견될 경우 최대 1,000배에 달하는 비용이 발생할 수 있다[1]. 따라서 초기 개발 단계부터 이를 식별하여 추적관리하기 위한 안전 설계 요구사항을 분석하는 방법이 중요하며 다양한 분석 기법을 통해 이러한 설계 위험요인을 초기에 최대한 많이 발견하는 것이 필요하다. 특히 최신 통합형 항공전자 구조에서는 단일 품목의 고장뿐 아니라 품목 간의 영향으로 공통 요인 고장을 일으킬 수 있는 요인에 대한 분석이 기존 대비 상대적으로 중요하다. 기존 단순한 분산/독립형 항공전자 구조는 각 기능이 박스 형태의 Line Replaceable Unit(LRU)으로 명확히 구분된다. 따라서 기능 간 공유하는 영역이 작고 경계가 물리적으로 명확하여 공통 요인의 발생 가능성이 매우 적고 쉽게 탐지가 가능하다. 하지만 최근 항공전자 시스템은 서브시스템 간의 경계를 허물고 공통 여유 자원 풀을 공유하여 시스템의 가용도를 높이는 통합형 시스템으로 발전하고 있다[2]. 통합형 시스템은 시스템 자원을 공유함으로서 중량, 전력소모 등에서의 이득을 얻을 수 있으나 공유 자원이 공통 요인으로 작용하여 복수의 기능에 동시에 영향을 일으킬 수 있는 위험성이 상대적으로 높다[3]. 이때의 공통 요인이란 다중화 또는 독립성을 무시하거나 무효화하는 이벤트 또는 고장을 의미한다[4]. 따라서 다중화 설계 등과 같은 고장-안전 설계 개념에 공통 요인이 잠재할 경우 그 단일 고장으로 인하여 다중화 기능이 동시에 이상을 발생할 수 있다.

일반적으로 회전익 항공기 인증기준은 안전에 치명적인 기능의 고장 발생률을 최소화하기 위해 고장-안전 특성을 시스템 설계에 적용하도록 요구하고 있다[5]. 예를 들어 국내 개발 회전익 항공기인 수리온 및 그 파생형 항공기 또한 안전성 치명 항목(Safety Critical Item: SCI) 분석을 통해 다중화 설계 적용 요구사항과 같이 시스템의 고장-안전 상태를 이루기 위한 요구도 분석 절차를 수행하였다[6-9]. 하지만 기존의 분석 방식은 통합형 항공전자 시스템에 적용하기에는 경우에 따라 안전에 치명적일 수 있는 공통 요인에 대한 검토 절차를 누락 할 수 있다는 문제점이 있다. 문제의 원인은 고장-안전 설계 대상을 선정함에 있어 단일 품목의 체계 기능 고장 영향성을 기준으로 함에 있다.

본 논문에서는 치명적인 공통 요인의 점검 절차 누락을 방지하기 위하여 체계 기능적 위험요소의 평가 결과에 기반을 둔 시스템 고장-안전 요구도 도출 절차를 제시하고 이를 수리온 파생형 항공기에 적용한 결과를 보였다. 이를 위해 민수 항공기 개발 관련 표준서인 SAE ARP4574A의 기능적 위험요소 평가(Functional Hazard Assessment: FHA), 개발보증수준(Development Assurance Level: DAL) 및 ARP4764의 공통 모드 분석(Common Mode Analysis: CMA) 개념을 활용하였다. 먼저 FHA 및 DAL 분석의 중간 산출물인 기능 고장 세트(Functional Failure Set: FFS)를 활용하여 통해 분석 대상을 선정하였다. 이어서 ARP4761의 공통 모드 체크리스트 및 점검절차에 따라 안전에 치명적인 공통 요인을 제거하기 위한 고장-안전 설계 요구사항을 도출하도록 분석 절차를 수립하였다. 또한 치명적인 기능 고장을 일으킬 수 있는 공통 요인 1건을 내포한 시스템 구조를 가정하여 기존 분석 방식과 본 연구 결과와의 교차 검증을 수행하였다. 그 결과 기존 연구 결과에서는 누락되는 치명적인 공통 요인이 식별되었으며 이를 통제하기 위한 고장-안전 설계 요구사항이 도출됨을 확인하였다.

기존의 안전 치명 품목 분석은 기능 구현을 위한 시스템 구조가 구체화되는 상세설계 이후 단계에서 적용이 가능하다. 하지만 본 연구 결과는 기능 수준의 안전성 분석 활동인 FHA로부터 시작됨에 따라 시스템의 기능 목록이 구체화되는 이후, 개념 및 기본설계 단계와 같이 비교적 개발 초기부터 적용이 가능하다. 따라서 안전에 치명적인 공통 요인을 시스템의 구현 및 검증단계 이전에 식별할 수 있고 안전과 관련된 설계 변경의 발생을 최소화하여 시스템의 재검증 등으로 인한 비용 및 일정 증가의 영향성을 최소화 하는 데 공헌할 수 있다.

본 논문의 구성은 다음과 같다. 제1장에서는 연구의 배경, 목적, 방법 및 연구를 통해 제안하고자 하는 바에 대하여 다룬다. 제2장에서는 안전 설계 요구사항을 분석하기 위한 관련 연구들을 설명하고 이를 최신 항공전자 구조에 적용하기 위한 제한성에 대하여 살펴본다. 제3장에서는 본 연구에서 활용하는 FHA, DAL 및 CMA 분석에 대한 간략한 설명과 이를 활용한 고장-안전 요구도 분석 절차에 대하여 설계하고 이에 대한 구현 결과를 확인한다. 제4장에서는 치명적인 공통 요인을 내포한 시스템 구조를 가정하여 기존 연구 결과와의 교차 검증을 수행하였으며 이에 대한 실험 및 고찰 결과를 기술한다. 제5장에서는 연구결과의 요약과 연구의 의의 및 실제 항공기 시스템 설계 및 인증 적용 현황 그리고 연구의 한계 및 미래연구의 방향에 대하여 제시한다.

Ⅱ. 관련 연구

2.1 수리온 고장-안전 설계 적용

수리온 항전체계에서 기능 품목은 임무컴퓨터를 중심으로 연결된 LRU 단위로 구분된다. 수리온의 고장-안전 설계를 위해서 세계적으로 통용되는 민간 회전익항공기 기술기준인 Federal Aviation Regulations (FAR) Part 29를 기반으로 특성에 따라 일부 변경 적용한 773항목의 기준을 최종 적용하였다[10]. 품목들의 안전 수준을 FAR part 29의 개발보증수준 개념과 유사하게 아래 Table 1과 같이 A부터 D까지 총 4단계로 분류하였다. 이 중 Level A 및 일부 B 품목을 SCI로 선정하였다. 수리온은 SCI의 식별을 위하여 아래 Fig. 1과 같은 단계의 절차를 적용하였다. 먼저 안전에 치명적인 기능(Safety Critical Function: SCF)을 식별한다. 그리고 SCF를 구성하는 품목을 분석하고, 이 중 단일 품목의 고장으로 SCF의 고장상태를 일으키는 품목을 SCI로 선정한다. 또한 이러한 품목의 안전도를 높이기 위한 고장-안전 설계 또한 LRU 수준에서의 다중화를 수행하였다[7,8]. LRU 단위로 기능 품목이 구분되는 수리온 항전체계에서는 품목별 수행 기능과 고장 발생 시 체계에 미치는 영향성이 비교적 명확하다. 따라서 안전에 치명적인 영향을 미치는 품목이 명확하게 식별이 되며 이들을 물리적으로 구분된 LRU 단위로 고장-안전 설계를 적용함에 따라 대다수의 공통 요인에 대한 위험이 자연적으로 해소가 된다.

하지만 최근 항전체계의 발전 추세인 통합형 항공전자 체계에서는 기능 품목이 소프트웨어 단위로 구분되며 특정 품목이 여러 기능에 공유되어 품목 자체가 공통 요인으로서 작용할 수 있다. 이때 수리온의 SCI 분석 방식은 경우에 따라 공통 요인으로 인한 영향을 누락할 수 있는 위험이 있다.

Table 1. Hazard and item safety classification [5,6]

Severity Classification of the Hazard	Item Safety Classification	Remark
Catastrophic	Level A	SCI
Critical	Level B	Potential SCI
Marginal	Level C	
Negligible	Level D	

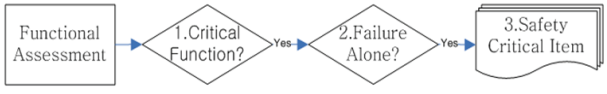

Fig. 1. Safety Critical Item Identification [7,8]

2.2 능동형 진동저감장치 고장-안전 설계 적용

능동형 진동제어장치(Active Vibration Control System: AVCS)는 헬기의 진동을 감지하여 이에 반대되는 제어 가능한 힘을 발생시켜 기체 진동을 제어하는 장치이다[11]. AVCS는 비행 조건의 변화에 따라 적극적으로 진동응답을 저감할 수 있으며, 수동형 저감 기법에 비해 동일한 중량 대비 진동 저감 성능이 우수하다는 이점이 있다[11]. 하지만 능동적으로 진동을 발생시키는 장비로서 기능의 오작동이 안전에 치명적인 영향을 발생시킬 수 있는 위험이 있다. 예를 들어 만약 AVCS의 오작동으로 인하여 발생한 비정상 하중 및 하중 주파수가 항공기의 공진 주파수에 가깝게 지속될 경우 이로 인하여 항공기의 조종력을 상실할 위험이 있다.

산업통상자원부의 소형무장헬기 연계 민수헬기 핵심기술개발사업에서는 이를 포함하여 안전성 관련 민간감항인증기준 규정을 준수하는 AVCS를 구현하기 위한 고장-안전 구조를 제시하는 연구를 수행하였다[12]. 해당 연구에서는 안전에 치명적인 고장 영향성을 제어하기 위한 설계 개념으로서 AVCS를 제어부분(Command Lane)과 감시 부분(Monitor Lane)으로 분리하는 고장-안전 개념을 제시하였다. 또한 향후 실 시스템의 상세 구현 시 명령부와 감시부의 독립성을 향상시키기 위하여 물리적으로 분리, 소프트웨어의 개발 툴 분리, 센서 종류의 분리 등의 독립성 개념을 제시하였다.

2.3 스마트다기능시현기 고장-안전 설계 적용

스마트 다기능시현기(Smart Multi Functional Display: SMFD)는 일반적으로 항공기 조종석에 탑재되어 조종사에게 항공기 운항에 필수적인 비행 정보 등을 제공하는 장비이다. 자세, 속도, 고도 등의 비행 필수 정보는 항공기의 안전한 운항에 반드시 필요한 정보로서 기능의 상실/오작동 등이 체계에 미치는 영향이 일반적으로 안전에 치명적인 수준의 심각도로 평가된다[13]. 이에 SMFD는 상대적으로 높은 안전성 수준이 요구되며 이를 충족하기 위해서는 고장-안전 등 안전성을 향상시키기 위한 설계 방안의 적용이 요구될 수 있다.

국내에서 설계된 SMFD 또한 안전 수준의 충족을 위하여 Prototype Model에 대한 안전성 분석과 고장-안전 설계 요구사항의 적용을 연구하였다[14]. 해당 연구에서는 SMFD가 개발규격에 명시된 정량적 안전성 요구사항을 충족하는지 확인하기 위해 고장유형 영향분석(Failure Mode Effect Analysis, FMEA)과 고장 트리 분석(Fault Tree Analysis, FTA)을 수행하였다. 분석 결과 제어 그래픽보드의 고장률을 정량적 안전성 요구도의 주요한 미 충족 원인으로 식별하였다. 이를 해결하기 위해 제어 그래픽보드를 이중화하

고 한쪽의 고장이 발생 시에도 기능이 정상적으로 수행되고 양쪽의 계산 결과 값을 상시 비교하도록 하는 다중화 설계 요구사항을 도출하였다.

하지만 해당 연구에서도 다중화된 보드의 공통 요인에 대한 점검을 고려하지 않았다. 예를 들어 다중화된 제어 그래픽보드가 공통 외부전원공급원 등의 공통 요인을 가진다면 관련된 소자 하나의 단일 고장이 다중화 보드의 전체적인 기능 상실을 야기할 수 있는 잠재적인 위험이 있다.

2.4 기존 고장-안전 설계 적용의 한계점

기존 분석 방식으로는 각 품목의 단일 고장 영향성은 상대적으로 낮으나, 시스템 구조상 품목이 공통 요인으로서 안전에 치명적인 기능 고장상태에 직간접적으로 관여할 경우를 누락할 수 있다. 이는 기존 분석 결과가 고장-안전 설계 대상을 선정함에 있어 단일 품목의 고장 영향성을 기준으로 분석하여 공통 요인에 의한 영향성을 체계적으로 고려하지 않기 때문이다. 그러나 최신 통합형 항공 전자 체계와 같은 구조에서는 품목이 다수의 기능에 공통요인으로서 작용하여 그 단일 고장의 발생 시 안전에 치명적인 고장상태를 일으킬 수 있다. 이때 이러한 공통 요인을 식별 및 분리하여 공유하지 않도록 처리하거나 개발 오류를 최소화하기 위해 개발보증절차 등을 적용하는 활동이 필요하다.

III. 요구사항 분석 절차 설계

고장-안전 설계 요구사항 분석 절차는 ARP4574A의 DAL 분석 절차에 대한 입력자료 및 중간 산출물을 활용하여 상세 고장-안전 설계 요구사항을 도출한다. Fig. 2는 본 연구에서 제시하는 분석 절차의 문맥적 흐름을 보여준다. 해당 분석 절차의 입력으로는 ARP-4754A DAL 분석의 중간 산출물인 기능적 개발보증수준(Functional Development Assurance Level: FDAL) FFS 분석결과와 Functional Architecture를 입력으로 받아 고장-안전 설계 요구사항을 도출한다.

분석 절차의 세부 스텝은 Fig. 2과 같이 1) 기능 분리 구현 요구도 할당, 2) 분리 대상 기능에 대한 공통 모드 점검, 3) 공통 모드 고장(Common Mode Error: CME)을 제거하기 위한 상세설계 요구사항 분석이 된다. 본 분석 절차를 통해 시스템의 초기 기능 설계 단계부터 항공기의 개발 수명주기 동안 지속적으로 적용되어 시스템의 안전도를 향상시키기 위한 설계 요구사항을 도출 및 점검한다.

3.1 기능 분리 요구도 할당

고장-안전 설계 요구사항 분석의 첫 번째 스텝인 기능 분리 요구도 할당에서는 분리 대상 기능의 식별을 수행한다. 분리 대상 기능은 항공기/시스템의 FHA로부터 식별된 안전에 치명적인 다중 기능 고장조건을 바탕으로 선정된다. 이는 다중 기능 고장을 구성하는 각 기능을 분리하여 구현하도록 요구함으로서 궁극적으로 치명적인 고장상태의 발생 확률을 최소화함이 그 목적이다.

ARP4754A의 DAL 분석 절차는 다중 기능 고장조건에 대한 FDAL 할당을 위해 FFS의 멤버 분석 결과를 중간 산출물로서 도출한다. 여기서 FDAL이란 FHA의 최상위 고장조건에서부터 기능 수준까지 할당되어 내려온 DAL이며 FFS는 최상위 고장조건을 일으킬 수 있는 멤버의 집합으로 정의된다[4]. FDAL 할당 과정에서의 FFS는 기능 수준으로 분리된 멤버로 구성되며 이를 바탕으로 시스템 구조에서 상호 독립적으로 설계 및 구현되어야 하는 기능 집합을 식별할 수 있다.

아래의 Table 2는 FDAL FFS 분석 결과를 바탕으로 기능 분리 요구도를 할당한 예시이다. ARP4754A의 정의에 따라 FDAL FFS 분석 결과로서 기능 수준 멤버는 '연료량 시현 기능'과 '저 연료 경고 기능'으로 구분된 FDAL FFS 멤버 기능을 명시할 수 있었다. 이후 본 연구에서 제안하는 세부 절차로서의 기능 분리 요구도 할당은 이들의 독립성을 확보하는 방향으로 수립되었다. 그 결과, '연료량 시현 기능 오

Table 2. Example of the first analysis procedure

FDAL FFS Member	Independent(Function) Requirement
Fuel Quantity Display	Fuel Quantity and Low Level Caution function shall be designed/worked independently
Low Level Caution Providing	

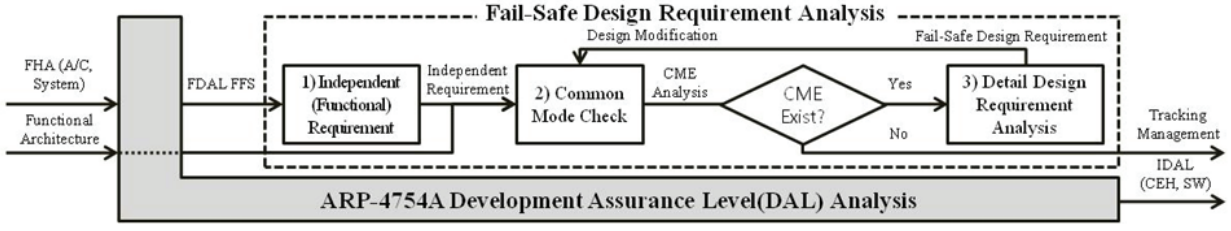

Fig. 2. Overview of Fail-Safe design requirement analysis

류 및 저 연료 경고 기능 상실'이라는 다중 기능 고장에 대한 요구도를 확보할 수 있었다.

Table 2의 예제와 같이 도출되어 할당된 요구사항은 관련 설계부서에 공유되어 개념 및 기본설계와 같은 개발 초기부터 안전성을 고려한 설계를 진행하도록 권고할 수 있다.

3.2 공통 모드 점검

고장-안전 설계 요구사항 분석의 두 번째 스텝인 공통 모드 점검은 이전 스텝을 통해 수립된 기능 분리 요구도를 시스템 상세설계를 위한 개발 요구도로 변환하기 위하여 수행된다. 본 스텝에서는 Fig. 2에서 보인 바와 같이 기능 분리 요구도와 현 설계 단계에서 제안된 Functional Architecture를 입력받는다. 출력으로는 시스템 구조에 잠재하는 CME의 식별 결과를 도출하여 다음 스텝으로 제공한다.

공통모드 점검 절차는 "ARP4761, Appendix K - Common Mode Analysis[15]"의 방법론을 활용하여 수행된다. Fig. 3은 공통모드 점검 절차의 흐름을 보여준다. 가장 먼저 점검 대상 공통모드 원인(Common Mode Source: CMS)을 선정한다. CMS 선정의 근간이 되는 CMA 점검표는 ARP4761의 예시를 바탕으로 개발 프로그램별로 수립될 수 있다. 다음으로 Functional Architecture 분석 결과에 따라 각 기능을 구성하는 품목 그룹을 식별하고 검토 대상으로 선정된 CMS에 대하여 공통 모드의 가능성을 식별한다. 마지막으로 공통 모드가 식별된 경우 공통 모드의 가능한 고장 시나리오를 분석하여 CME를 도출한다.

Table 3은 ARP4761의 일반적인 공통모드 원인 예시 중 'Component Type' 하나를 적용하여 공통모드 분석을 간략히 수행한 예시이다. Functional Architecture를 참조하여 저 연료 경고 기능의 경우 신호처리유닛(Signal Conditioning Unit: SCU), 데이터수집장치(Data Acquisition Unit: DAU) 및 스마트다기

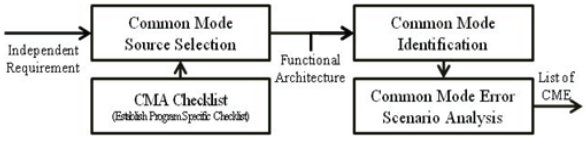

Fig. 3. Process of Common Mode Analysis

Table 3. Example of the second analysis procedure

CMS	Low Level Related Items	Fuel Qtt. Related Items	Common Mode
Component Type	SCU, DAU, SMFD	SCU, FI	Common Component (SCU) used

능 시현장치(Smart Multi Function Display: SMFD)로 구성한다. 연료량 시현 기능의 경우 SCU 및 연료량 지시기(Fuel Indicator: FI)로 구성됨을 가정한다. 이때 저 연료 경고 기능과 연료량 시현 기능 모두 기준으로 SCU라는 공통 모드(구성품)를 포함하는 것을 식별할 수 있다. 이에 따라 발생 가능한 고장 시나리오로서 '공통 구성품(SCU)의 고장으로 인한 저 연료 경고 및 연료량 시현 기능 동시 고장 발생 가능'이라는 CME를 식별할 수 있다.

Table 3은 CMS 예제 중 가장 일반적인 Component Type 한 사례를 바탕으로 수행하였으나 ARP4761은 장착, 조립, 검/교정, 시험, 운용, 환경 등 다양한 분야의 CMS 예시를 포함하고 있다. 이를 바탕으로 실제로 공통모드 점검 절차를 수행할 때는 개발 단계 및 환경을 고려하여 다양한 분야에 대한 공통모드 점검이 가능하다.

3.3 고장-안전 상세설계 요구도 분석

마지막으로 시스템 구조의 고장-안전 상세설계 요구도 도출 스텝은 이전 세부 절차의 결과로 식별된 CME를 해결하는 방향으로 수행한다. 이전 절차에서 CME가 식별되지 않으면 향후 설계변경사항의 발생에 대한 추적 관리를 수행하고 잠재적인 CME가 식별된 경우에는 이를 제거하기 위한 고장-안전 설계 요구사항을 수립하고 개선된 기능구조에 대한 재검토를 수행한다. 수립된 설계 요구사항은 시스템 개발 주기 동안 안전성 권고사항으로서 추적 관리가 필요하며 안전성 분석 담당자는 확정된 최종 시스템 구조에 대한 해당 요구사항의 입증 결과를 시스템의 안전성 평가 보고서에 기술한다.

아래의 Table 4는 식별된 CME를 제거하기 위해 수립된 고장-안전 상세설계 요구사항의 분석 결과이다. CME로서 공통 구성품(SCU)의 단일 고장으로 인

Table 4. Example of the last analysis procedure

Common Mode Source	Common Mode Error	Compensating Provision	Design Requirement
Component Type	Simultaneous failure of both function due to failure of common component(SCU)	Physical Separation of functional module Level	Fuel Q and Low Level caution function shall be implemented by physically separated module
		Independent Power Source Applying	Fuel Q and Low Level caution function module shall be powered by independent external source
		In/Out interface separation	SCU In/out port of Fuel Q and Low Level caution function shall be physically independent

한 다중 기능 고장 발생이 식별되었으며 이를 예방하기 위한 위험도 보상 방안을 구성품의 내부 및 외부 요소로 분리하여 각각 위험도 보상 방안을 수립하였다. 이에 따라 내부적으로는 저 연료 경고 기능과 연료량 시현 기능을 물리적으로 분리된 모듈에서 독립된 전원 공급원을 바탕으로 연산되도록 설계 요구사항을 수립하였다. 또한 외부적으로 각 신호의 입·출력 커넥터를 분리하여 단일 커넥터/와이어 손상으로 인한 동시 기능 상실을 예방토록 상세설계 요구사항이 수립되었다.

Table 4의 예제와 같이 최종적으로 도출된 고장-안전 설계 요구사항은 항공기 안전에 치명적인 공통 요인을 제거하도록 수립된다. 이러한 설계 요구사항은 개발 수명주기 동안 지속적으로 관리되며 그 입증결과를 시스템 안전성 평가 보고서에 기술한다.

Ⅳ. 실험 및 고찰

4.1 실험 설정

본 실험 결과에서는 제시한 방법의 적용으로 안전에 치명적인 공통 요인의 누락 발생 문제가 해결됨을 보이기 위해 아래 Table 5에 대한 예제에 대하여 비교 분석을 수행하였다. Table 5는 외부통신 기능, 항법정보 시현 기능의 단일 및 다중 상실 고장조건에 대한 기능적 위험요소 분석 예시이며 Federal Aviation Administration(FAA) AC 25-11B[13]의 비행 계기정보 기능 고장상태별 심각도 분류 사례를 적용하였다.

Table 5. Functional Hazard Assessment Sample[13]

Failure Condition	Aggravating Event	Severity	Failure Alone
Loss of COM	None	Major	Single
Loss of NAV	None	Major	Single
Loss of COM	Loss of NAV	Catastrophic	Multiple

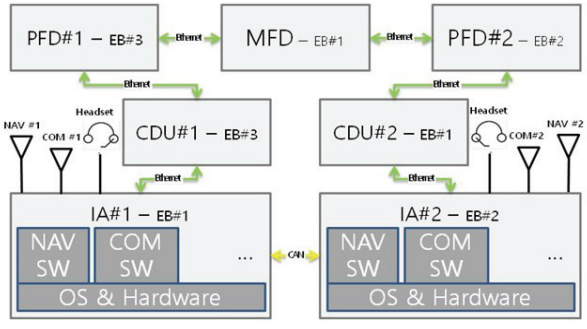

Fig. 4. Functional Architecture of COM/NAV

분석을 수행하기 위한 시스템 기능 구조는 Fig. 4와 같이 가정하였다. 항법(Navigation: NAV) 시현정보와 통신(Communication: COM) 음성정보기능은 이중화 적용된 통합 항전장비(Integrated Avionics: IA)에서 소프트웨어 항목으로 구현된다. NAV와 COM 애플리케이션은 동일한 개발 툴을 활용하여 개발될 예정이다. NAV 신호원 선택 및 COM 주파수 제어 등은 제어시현장치(Control Display Unit, CDU)가 담당하며 COM은 각 IA에 연결된 Headset으로, 그리고 NAV는 각 조종사측면의 주 비행계기 시현장치(Primary Flight Display; PFD)에 전달된다. 장비 간 정보 전달은 High-Speed Data Bus(HSDB) Packet을 주고받는 형식으로 이루어진다. 각 장비는 Electrical Bus(EB)#1 ~#3 중 하나에서 전원을 공급받도록 계획되었으며, 현재 장비별 공급원은 Fig. 4에 표기되었다. 해당 기능 구조는 아래의 잠재적인 공통 요인이 포함되도록 의도되었으며, 기존 분석방식과의 비교실험을 통해 요구사항 분석 절차를 통한 검출 가능 여부를 점검한다.

1) 모든 COM 및 NAV 기능은 동일한 하드웨어 환경(IA)에서 구동됨
2) 공통 전원: 모든 COM 및 NAV 기능경로 상에 동일한 전원 공급원(EB#1)이 존재함
3) NAV와 COM 소프트웨어는 동일한 개발 도구를 통해 구현됨

4.2 실험 결과

본 연구에서 제시하는 분석 방법은 FDAL FFS 분석 내용을 최초 입력 자료로써 활용한다. Table 5의 재난적 기능 고장조건은 2개 이상의 기능 고장이 조합된 다중 기능 고장 형태로서 ARP4754A의 멤버 정의에 따라 'NAV 시현'과 'COM 제공'의 기능 단위 멤버를 가지는 FFS로 분석될 수 있다.

4.2.1 기능 분리 요구도 할당 결과

Table 6은 Table 5에서의 FFS 분석 결과를 바탕으로 Fig. 2의 첫 번째 절차에 따라 기능 수준에서의 분리 요구도를 할당한 결과이다. Table 5의 재난적 위험요소에 대한 FFS 멤버는 기능 수준에서 COM과 NAV 제공기능으로 구분된다. 기능 분리 요구도는 두 멤버간의 독립성을 확보하기 위하여 상호 독립적으로 설계되어야 함을 기술한다.

Table 6. Allocation of Function Level Requirement

FDAL FFS Member	Functional Independent Requirement
Displaying NAV	NAV and COM function shall be designed/worked independently
Providing COM	

Table 7. Common Mode Analysis Result

CMS	COM(Function Path)	NAV(Function Path)	Common Mode	CME Scenario
	COM#1: IA#1↔CDU#1 COM#2: IA#2↔CDU#2:	NAV#1: IA#1↔CDU#1→PFD#1 NAV#2: IA#2↔CDU#2→PFD#2		
External Source	COM1: IA#1(EB#1)↔CDU#1(EB#3) COM2: IA#2(EB#2)↔CDU#2(EB#1) NAV1: IA#1(EB#1)↔CDU#1(EB#3)→PFD#1(EB#3) NAV2: IA#2(EB#2)↔CDU#2(EB#1)→PFD#2(EB#2)		Common EB#1 on both path	Loss of single source(EB#1) occurs loss of all functional path(COM1/2 and NAV 1/2)
Component Type	Both COM and NAV SW are implemented in the same hardware environment (IA1 and IA2)		Common IA used	Common development error of IA CEH cause simultaneous failure of all NAV/COM
Software	Both COM and NAV SW application are developed by the same tool		Common SW tool	Common development error of both NAV/COM SW causes simultaneous failure of all NAV/COM

4.2.2 공통 모드 분석 결과

두 번째 절차로 Table 6에서 수립된 기능 분리 요구도에 대한 CMA 분석을 수행한다. Fig. 2의 절차에 따라 기능구조 분석 결과가 추가적으로 요구되어 실험 설정 Fig. 4의 기능구조도를 입력 자료로 활용하였다. 4.1절 실험 설정에 따라 통신기능의 경로를 IA#1/#2↔CDU#1/#2, 항법정보 시현기능의 경로는 IA#1/#2↔CDU#1/#2→PFD#1/#2로 분석하였다. Table 7은 이를 바탕으로 두 번째 세부절차인 CMA 분석을 수행한 결과이다. CMA는 현재 시스템 구조의 설계 과정임을 감안하여 ARP4761에 정의된 대표적인 CMS 중 Concept and Design 타입의 항목에 대하여 수행하였다. 그 결과 External Source/Component Type/Software 3개 분야에서 시스템 구조에 잠재된 공통모드를 식별하였고 CME 발생 시의 시나리오를 분석하여 Table 5에 정의된 재난적 기능 고장상태가 발생 가능함을 확인하였다.

4.2.3 고장-안전 상세설계 요구도 분석 결과

마지막으로 Fig. 2의 세 번째 절차인 CME를 제거하기 위한 상세설계 요구사항 도출 절차를 진행하였다. 아래 Table 8의 설계 요구사항은 여러 가지 가용한 선택지 중 Table 7의 CME Scenario를 제거하면서도 변경범위와 영향을 최소화하는 방향으로 수립하였다.

공통 External Source의 경우 IA#1의 전원 공급원을 EB#1에서 EB#3으로 하나만 변경하도록 설계 요구사항을 수립하였다. 이 경우 EB#1의 상실 시에도 COM#1과 NAV#1의 기능경로가 유지되어 정상 작동함이 가능하며 단일 전원의 기능 상실로 인한 재난적 고장조건의 발생을 예방함으로써 시스템의 고장-안전 설계를 이룬다. 기능 경로의 유지 여부는 체계통합실험실 구축 시점에서 고장모드 영향성 시험(Failure Mode Effect Test: FMET)를 통해 인위적으로 고장상태를 재현하여 확인이 가능하다.

공통 Component Type의 경우 동일 장비로 다중화설계가 적용되어 있음을 감안하여 추가 다중화보다는 Complex Electronic Hardware(CEH)의 개발오류를 감소시키기 위한 방안으로 DO-254의 적용을 요구하고 DAL A 품목으로서 SCI 대상으로 지정하였다. 최고수준의 개발보증절차를 적용함으로서 공통 CEH의 개발오류로 인한 재난적 고장조건의 발생을 예방하고 이로써 시스템의 고장-안전 설계를 이룬다.

마지막으로 공통 Software의 경우 COM 및 NAV의 개발툴을 분리하여 동일한 개발 도구로 인하여 발생 가능한 공통 오류를 제거하도록 요구도를 수립하였다. 개발도구를 분리하여 NAV 및 COM Software에 잠재할 수 있는 공통적인 개발 오류의 가능성을 제거하고 이로 인한 재난적 고장조건의 발생을 방지함으로써 시스템의 고장-안전 설계 사항을 도출한다.

Table 8. Analysis of Fail-Safe Design Requirement

CMS	CME	Compensating Provision	Design Requirement
External Source	Failure of common power(EB#1)	Change power source to remain functional path, or apply duel power source	Req#1 - Change power source of IA#1 to EB#3 (tracking management of functional path is needed)
Component Type	Development error of common IA CEH	Applying highest DAL to IA CEH or consistency check generated by independent CEH	Req#2 - The CEH of IA shall be developed (or used) according to DO-254 Level A
Software	Development error generated by common tool	Uses different development tools for NAV and COM applications	Req#3 - NAV and COM software should apply different development tools.

4.3 고찰

기존 수리온에 적용된 고장-안전 설계 요구사항 분석 결과는 Fig. 1에 서술한 바와 같이 안전에 치명적인 기능 고장을 식별하는 단계부터 시작된다. 먼저 Table 5의 기능적 위험요소 분석 예시에서 안전에 치명적인 기능 고장상태(항법정보(NAV) 및 외부통신(COM) 기능 상실)가 있음을 확인할 수 있다. 두 번째로 해당 기능 고장상태가 단일 요인을 가지는지가 검토되어야 한다. Fig. 4의 기능 구조에 따르면 NAV와 COM 기능이 구현된 통합 항전장비(IA)가 이미 이중화 적용되어 있으며 각각 정/부 조종사 측으로 분리된 경로로 제공이 가능함으로 단일 요인이 없음으로 판단된다. 따라서 모든 항법/통신 기능 구성 품목이 SCI로 선정되지 않고 추가적인 고장-안전 설계 특성의 적용 확인 대상으로 식별되지 않는다.

반면 본 연구 결과에서 제시한 분석 절차에 따라 동일한 시스템을 분석하면 기존의 연구 결과와는 다른 결론을 도출할 수 있다. 고장-안전 설계 특성 검토 대상에서 제외되었던 기존 분석 결과와는 다르게 제안된 시스템 구조 내에 잠재된 안전에 치명적일 수 있는 3건의 공통 요인을 검출할 수 있다. 또한 공통 요인을 통제하기 위한 상세설계 요구사항을 수립하고 그 과정에서 SCI 관리대상 1건을 선정하였다(Table 9 참조). 수립된 고장-안전 상세설계 요구사항은 안전성 요구사항으로서 지속적으로 추적 관리되며 필요한 경우 시험평가 단계에서 FMET을 통해 공통 고장요인을 명시하고 관리할 수 있음을 이번 실험을 통해 보였다.

실제로 본 연구 결과는 최신 수리온 파생형 모델인 수출기본형 항공기(KUH-1E)의 체계안전성 분석/평가에 적용되었다[16-18]. KUH-1E는 본 연구 결과에 따라 분석된 결과를 포함하여 군용항공기 특별감항인증을 획득하였다. 먼저 KUH-1E 서브시스템 위험요소 분석(Subsystem Hazard Analysis: SSHA)[16]을 통해 체계의 위험요소 평가 결과와 연계하여 8건의 기능 분리 요구사항을 식별하였다. 다음으로 KUH-1E 시스템 위험요소 분석(System Hazard Analysis: SHA)[17]에서 기능 분리 요구사항에 대한 CMA 분석을 수행하여 22건의 잠재적인 CME 위험 시나리오를 도출하고 상세설계 요구사항을 도출하였다. 대표적인 사례로 항공전자 계통에서 Common External Source로 인한 CME가 식별되었다. 시나리오 분석 결과 특정 전원 버스의 단일 고장이 NAV/COM기능의 동시 상실을 야기할 수 있어 전원공급원 설계를 변경하였다. 마지막으로 KUH-1E 안전성 평가 보고서(Safety Assessment Report: SAR)[18]에 수립된 설계 요구사항의 반영 및 관련 시험 결과를 확인하고 시스템의 고장-안전 설계 평가에 대한 결과를 기술하여 특별감항인증을 획득을 위한 체계 안전성 평가 결과자료로서 제출하였다.

Table 9. Result of comparison review

	Potential Common Mode	Detected Common Mode	SCI
Existing Procedure	3	0	0
Proposed Procedure		3	1

V. 결 론

본 연구 결과에서는 시스템 구조의 치명적인 공통 고장요인을 통제하기 위한 안전성 설계 요구사항 분석 절차를 제시하였다. 기존의 분석 방식은 경우에 따라 안전에 치명적일 수 있는 공통 요인에 대한 검토 절차를 누락할 수 있다는 문제점이 있었다. 본 논문에서는 공통 요인에 대한 고장 요인을 검토하기 위한 방법으로 SAE ARP4754A의 DAL 분석 과정과 연계될 수 있는 시스템 구조의 고장-안전 설계 요구사항 분석 절차를 제시하였다. 또한 실험을 통하여 기존 분석 방식으로는 탐지되지 않는 잠재적인 치명적 공통 요인을 식별 및 통제 가능함을 확인하였다.

향후 과제로는 FHA의 완성도에 대한 종속성을 보완하는 연구가 필요하다. 본 연구 결과는 FHA를 통해 식별된 안전에 치명적인 다중 기능 고장조건을 대상으로 시작한다. 따라서 FHA가 체계에서 발생 가능한 모든 고장조건을 분석하였다면 본 연구 결과를 바탕으로 이를 통제하기 위한 모든 고장-안전 설계 요구사항을 검토할 수 있다. 이를 다르게 보면 요구사항 분석의 완성도가 체계 FHA의 성숙도에 크게 영향을 받는다는 구조적인 한계점을 가진다고 할 수 있다. 따라서 향후 연구에서는 이를 보완할 방법에 관한 연구를 진행할 필요가 있을 것이다.

후 기

이 성과는 정부(과학기술정보통신부, 교육부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구(No. NRF-2021R1A2C1014163 및 No. NRF-2021R1A2C1094167, 2021RIS-003)임.

약어정리

- AVCS: Active Vibration Control System, 능동형 진동 저감장치
- CDU: Control Display Unit, 통제 시현 장치
- CEH: Complex Electronic Hardware, 복합 전자 하드웨어
- CMA: Common Mode Analysis, 공통모드 분석
- CME: Common Mode Error, 공통모드 고장
- CMS: Common Mode Source, 공통모드 원인

• COM: Communication, 통신
• DAL: Development Assurance Level, 개발보증수준
• DAU: Data Acquisition Unit, 데이터 획득장치
• FAA: Federal Aviation Administration, 미연방 항공청
• FAR: Federal Aviation Regulation, 미연방 항공규정
• FDAL: Functional Development Assurance Level, 기능적 개발보증수준
• FFS: Functional Failure Set, 기능 고장 세트
• FHA: Functional Hazard Assessment, 기능적 위험요소 평가
• FI: Fuel Indicator, 연료량 지시기
• FMEA: Failure Mode Effect Analysis, 고장모드 영향성 분석
• FMET: Failure Mode Effect Test, 고장모드 영향성 시험
• FTA: Fault Tree Analysis, 고장트리분석
• HSDB: High Speed Data Bus, 고속 데이터 버스
• IA: Integrated Avionics, 통합형 항전장비
• LRU: Line Replaceable Unit, 부대정비 교환품목
• MFD: Multi Functional Display, 다기능 시현기
• NAV: Navigation, 항법
• PFD: Primary Flight Display, 주요 비행정보 시현기
• SAR: Safety Assessment Report, 안전성 평가 보고서
• SCF: Safety Critical Function, 안전 치명 기능
• SCI: Safety Critical Item, 안전 치명 항목
• SCU: Signal Conditioning Unit, 신호처리장치
• SHA: System Hazard Analysis, 시스템 위험요소 분석
• SMFD: Smart Multi Functional Display, 스마트 다기능 시현기
• SSHA: Subsystem Hazard Analysis, 서브시스템 위험요소 분석

References

1) Scott, F., “Avionics cost and complexity,” *Aviation Week & Space Technology*, February 2010.

2) Song, C. H., “Development trends in avionics technology,” *IT SOC magazine 34*, March 2009, pp. 24~31.

3) Fleming, C. H. and Leveson, N. G., “Improving Hazard Analysis and Certification of Integrated Modular Avionics,” *Journal of Aerospace Information Systems*. Vol. 11 No. 6, 2014, pp. 397~411.

4) SAE international, *ARP4754A: Guidance for Development of Civil Aircraft and Systems*, SAE international, 2010.

5) Federal Avionics Administration(FAA), *AC 29-2C: Certification of Transport Category Rotorcraft*, USA FAA, 2014.

6) Kim, D. S., Jeon, S. M., Jang, J. S., Choi, G. H. and Lee, S. H., “KUH System Safety Program,” *Proceeding of The Korean Society for Aeronautical and Space Sciences Fall Conference*, November 2014, pp. 693~697

7) Defense Acquisition Program Administration, *KUH-1 Safety Crtical Item*, Korea Aerospace Industries, 2012.

8) Korea Aerospace Industries(KAI), *KUH-1P Safety Critical Item,* KAI, 2015.

9) Department of Defence(DoD), *MIL-STD-882D: Standard Practice for System Safety*, USA DoD, 2000.

10) Yun, H. G., Kim, S. J., Kim, Y. T. and Lee, S. H., *Airworthiness Certification Practice Written By Experience in Aircraft Development,* G-World, 2014, pp. 217~227.

11) Lee, Y. L., Kim, D. Y., Kim, D. H., Hong, S. B. and Park. J. S., “Vibration Reduction Simulation of UH-60A Helicopter Airframe Using Active Vibration Control System,” *Journal of The Korean Society for Aeronautical and Space Sciences,* Vol. 48, No. 6, 2020, pp. 443~453.

12) Ahn, L. K., “Conceptual Design of AVCS Architecture Considering the System Safety,” *Proceeding of The Korean Society for Aeronautical and Space Sciences Spring Conference*, April 2016, pp. 628~629.

13) Federal Avionics Administration(FAA), *AC 25-11B: Electronic Flight Displays*, USA FAA, 2014.

14) Seo, J. H., “A Study on Reliability, Safety Analysis and Related Performance Improvement of Avionics Equipment,” *Journal of the Korea Institute of Information and Communication Engineering*, Vol. 22, No. 9, 2018, pp. 1220~1227.

15) SAE international, *ARP4761: Guidance and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment*, SAE International, 1996.

16) Korea Aerospace Industries(KAI), *KUH-1E Subsystem Hazard Analysis*, KAI, 2019.

17) Korea Aerospace Industries(KAI), *KUH-1E Preliminary System Safety Assessment*, KAI, 2019.

18) Korea Aerospace Industries(KAI) *KUH-1E Safety Assessment Report*, KAI, 2019.