Technical Paper
Journal of Aerospace System Engineering
Vol.17, No.6, pp.108-117 (2023)
EISSN 2508-7150
http://dx.doi.org/10.20910/JASE.2023.17.6.108

KT-1 군항공기 소프트웨어 국제공동개발 사업의 미션 소프트웨어 신뢰성 시험방안에 관한 연구

배병덕[1,2] · 이선아[2,3,4]†

[1]한국항공우주산업㈜
[2]기술경영학과, 경상국립대학교
[3]항공우주및소프트웨어공학부, 경상국립대학교
[4]AI융합공학과, 경상국립대학교

A Study on Mission Software Reliability Test Methods of International Joint Development Project for KT-1 Military Aircraft Software

Byung Duck Bae[1, 2], Seonah Lee[2,34]†

[1]Korea Aerospace Industries, LTD.
[2]Department of Management of Technology, Gyeongsang National University
[3]Department of Aerospace and Software Engineering, Gyeongsang National University
[4]Department of AI Convergence Engineering, Gyeongsang National University

Abstract

Thus far, a mission software component of the KT-1 military fixed-wing aircraft for overseas export has been developed through international joint development with foreign companies. The reliability of the software component could be certified by complying with the development environment and procedures of foreign companies based on DO-178B. However, recently, DO-178C certification is required for overseas exports, and reliability tests to comply with the weapon system software development guidelines are required for domestic military forces. In this paper, we describe the problems in obtaining domestic airworthiness certification in the international joint development of a previously developed KT-1 export-typed aircraft system integration project. To this end, we find a solution to comply with both DO-178C and the Weapon System Software Development and Management Manual and provide the optimal software reliability test method.

초 록

지금까지 해외 수출용 KT-1 군용 고정익 항공기에 통합된 임무 소프트웨어는 해외업체와 국제 공동개발을 통하여 개발이 되었으며, 감항인증을 위해 DO-178B를 기반으로 하는 해외업체의 개발 환경과 절차를 준수함으로써 소프트웨어의 신뢰성을 인정받을 수 있었다. 하지만, 최근에는 해외 수출 시 DO-178C 인증을 요구하고 있으며, 국내 소요군에 납품 시 방사청 무기체계 소프트웨어 개발 및 관리 매뉴얼 준수를 위해 신뢰성 시험을 필수적으로 요구하고 있다. 본 논문은 기 개발된 KT-1 수출형 항공기 체계통합 사업의 국제 공동개발에 있어 국내 감항인증을 받기 위한 문제점을 기술하고 DO-178C와 무기체계 소프트웨어 개발 및 관리 매뉴얼을 모두 준수하기 위한 해결방안을 찾아서 최적의 소프트웨어 신뢰성 시험 방안을 제시한다.

Key Words : Mission Software(임무 소프트웨어), Software Reliability Test(소프트웨어 신뢰성 시험), DO-178C, Airworthiness(감항인증), International Joint Development(국제 공동 개발)

Received: Sep. 18, 2023 Revised: Nov. 24, 2023 Accepted: Nov. 27, 2023
† Corresponding Author
Tel: +82-55-772-1377, E-mail: saleese@gnu.ac.kr

1. 서 론

고부가 가치를 창출하는 항공 무기체계에서도 전자

전과 네트워크 중심의 전장에 대응하기 위하여 소프트웨어의 비중은 비약적으로 증가하고 있다. 미국 국방성(United Sates Department of Defense)자료에 의하면 Fig. 1과 같이 1960년대에 생산된 F-4전투기는 임무 기능 중 소프트웨어의 비율이 8%였으나 2007년 생산된 F-35 전투기의 경우 11배가량 증가한 90%에 달한다고 한다[1].

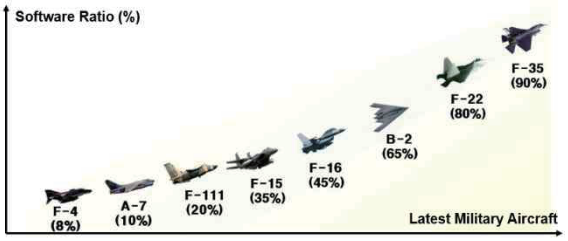

Fig. 1 Aircraft Mission System Software Ratio

항공기는 안전성을 검사하기 위한 감항인증을 받아야 하며, 이를 위해서는 MIL-HDBK-516C를 기반으로 한 표준 감항인증 기준을 따라야 한다. 이는 소프트웨어에서도 예외는 아니는데, 항공기 무기체계의 소프트웨어 인증을 위해서는 DO-178 및 미 국방성 문서 (Weapon Systems Software Management Guidebook 등)를 따라야 한다[2]. 즉, 항공 소프트웨어를 수출하기 위해서는 국제 표준인 DO-178 (Document-178)을 준수하여 감항인증을 받아야 한다.

본 논문에서 다루고자 하는 해외 수출용 군용 항공기 KT-1에 탑재되는 임무 컴퓨터는 해외 수출용으로 개발되었다. 임무 컴퓨터는 조종사 한 명이 다중 임무를 신속하고 정확하게 수행할 수 있도록 많은 양의 데이터를 제공하는 항공전자장비(센서)들의 정보를 실시간으로 처리하고 제어한다. 해당 임무 컴퓨터에 탑재되는 소프트웨어는 해외업체와 공동으로 개발되어 왔다. 또한, 해당 임무 소프트웨어는 개조 사업에서도 DO-178을 준수하여 감항인증을 받을 수 있었다.

이러한 해외 수출용 임무 소프트웨어를 국내용으로 활용하고자 하는 상황에서는 또 다른 표준을 준수해야 하는 상황이 발생하였다. 대한민국 방위사업청(방사청)에서는 무기체계 소프트웨어 개발 매뉴얼(무기체계 소프트웨어 개발 및 관리 매뉴얼)을 준수하도록 요구하고 있었다. 그런데, 일부 기능을 임무 소프트웨어에 추가하기 위해 개조 개발사업의 무기체계 소프트웨어 개발 매뉴얼을 준수하기 위해서는 아래와 같은 문제점에 직면하게 되었다.

첫째, 무기체계 소프트웨어 개발 매뉴얼의 요구 사항에 따라 임무 소프트웨어에 대한 신뢰성 시험을 수행해야 했다. 그러나, 이미 개발된 항공기에 탑재된 임무 소프트웨어는 개발 당시 DO-178B를 준수하여 감항인증을 받았고 수십 년간 운영이 되고 있어서 전체 소프트웨어를 무기체계 소프트웨어 개발 매뉴얼을 따라 신뢰성 시험을 하기에는 분량이 너무 많았다.

둘째, 기존의 임무 소프트웨어는 해외업체와 공동개발하여 하나의 CSCI(Computer Software Configuration Item)로 통합되어 있어 개조 시 해외업체가 개발한 소스 코드에 대해서도 신뢰성 시험을 수행해야 했다.

셋째, 기존의 임무 소프트웨어는 항법장비와 같은 안전에 관련된 정보를 처리하고 있어 신뢰성 시험 기준도 높은 수준의 신뢰성 시험을 수행해야 했다.

넷째,해외 수출도 지속해야 하기 때문에, 국내용으로 요구되는 무기체계 소프트웨어 개발 매뉴얼의 신뢰성 시험 준수와 DO-178C를 동시에 만족해야 했다. 그러나, 항공 탑재 소프트웨어를 무기체계 소프트웨어 개발 매뉴얼만 고려하여 개발할 경우 DO-178의 목표를 달성할 수 없을 뿐만 아니라 감항인증 기준을 충족할 수 없었다[3].

본 논문에서는 기존에 수출용으로 해외업체와 공동개발한 KT-1 항공기 임무 소프트웨어를 국내용으로도 사용하기 위해 해외와 국내의 소프트웨어 감항인증 표준을 동시에 만족시키기 위한 효과적인 방안을 제시한다. 해당 논문의 공헌은 다음과 같다.

첫째, 두 개의 수출용과 국내용 인증 체계를 준수하기 위해 파티셔닝 운영체제를 적용하여 소프트웨어 신뢰성 시험 범위를 줄이는 아이디어를 제시한다.

둘째, 구체적으로는 항공기에 탑재되는 임무 소프트웨어 중 한 개의 CSCI로 구성된 임무 소프트웨어를 기능별로 재 분류하여 안전등급별로 여러 개의 CSCI로 재구성한 후, 안전성 등급을 분류하여 등급별로 소프트웨어 신뢰성 시험을 수행한 방법을 제시한다.

셋째, 앞서 기술한 임무 소프트웨어의 일부를 개조하는 사업에서 제시한 아이디어를 적용한 성공적인 신뢰성 시험 방안에 대한 사례를 제시한다.

넷째, 항공기 임무 소프트웨어 신뢰성 시험에 적합한 시험 자동화 환경을 국내 업체인 슈어소프트사의 제품을 활용하는 자동화 환경을 설명한다.

본 논문에서 제시하는 시험 방안은 해외업체가 개발한 부분에 대해서는 해외 상용소프트웨어로 분류하여 DO-178C의 신뢰성 시험 결과만을 제출하고, 국내업체가 신규로 개발하는 부분에 대해서는 DO-178C와 무기체계 소프트웨어 개발 매뉴얼의 신뢰성 시험을 모두 수행함으로써 소프트웨어 신뢰성 시험에 대한 부하를 줄일 수 있다. 이후 국내업체가 신규 개발하는 부분에 대해서는 무기체계 소프트웨어 개발 매뉴얼의 신뢰성 시험과 DO-178C의 신뢰성 시험을 수행하고 기

존에 개발된 부분은 DO-178C를 준수하여 재개발할 수 있었다.

이를 통해 해외업체와 공동 개발된 무기체계 소프트웨어에 대하여 최적의 소프트웨어 신뢰성 시험 방안을 제시하고, 향후 국제공동개발사업에서도 참고 사례로 활용될 수 있도록 하자 한다.

2. 기존 신뢰성 시험절차 분석

2.1 DO-178C 신뢰성 시험절차 분석

DO-178C는 항공 시스템에 사용되는 소프트웨어의 개발 및 인증에 대한 지침을 제공하는 소프트웨어 표준이다[4]. RTCA(Radio Technical Commission for Aeronautics)가 EUROCAE(European Organization for Civil Aviation Equipment)와 협력하여 개발했으며 미국 FAA(Federal Aviation Administration)를 비롯한 항공우주 산업에서 널리 채택되고 있다.

DO-178C 소프트웨어 등급은 시스템 안전평가 프로세스 수행을 통하여 5개 등급(A~E)으로 분류된다. 소프트웨어의 에러로 인하여 결함이 발생될 경우, 항공기의 안전에 영향을 주는 실패조건에 따라 등급이 분류되고, 항공기가 추락하는 재난상황이 가장 높은 DAL(Design Assurance Level) A 등급이고, 영향이 작을수록 등급이 B, C, D, E로 낮아진다. 소프트웨어의 등급에 따라 충족해야 할 신뢰성 시험 커버리지가 다르며 등급이 높을 수록 시험을 충족시키기 위한 절차와 시간이 많이 투입되게 된다.

DO-178C에 따른 신뢰성 시험 충족 기준은 요구사항 기반으로 정상범위 시험과 강건성 시험을 수행하여 커버리지를 만족하여야 한다. 요구사항 기반으로 시험이 불가능한 부분은 구조적 분석을 통해 커버리지를 만족시켜야 한다. 이에 따른 DO-178C에서의 신뢰성 시험은 다음과 같이 두 가지로 나뉜다.

- 커버리지 분석: 커버리지 분석은 소프트웨어 테스트 노력의 적절성을 평가하는 시험이다. 이 시험은 요구 사항에 대한 소프트웨어 테스트 범위를 측정하고 테스트 노력의 차이를 식별하는 작업이 포함된다.
- 신뢰성 데모 테스트: 신뢰성 데모 테스트는 소프트웨어의 신뢰성을 입증하는 시험이다. 이 시험은 특정 기간 동안 소프트웨어 시스템의 예상 작동 조건을 시뮬레이션 하는 일련의 테스트에 소프트웨어 시스템을 적용하는 것과 관련된다. 이러한 시험 결과는 소프트웨어의 안정성을 입증하고 안정성 요구 사항을 충족하는 기능을 검증하는 데 사용된다.

2.2 무기체계 소프트웨어 개발 및 관리 매뉴얼 신뢰성 시험절차 분석

방사청 무기체계 소프트웨어 개발 매뉴얼(무기체계 소프트웨어 개발 및 관리 매뉴얼)의 신뢰성 시험절차는 무기체계 연구개발간 소프트웨어 신뢰성 시험을 정량적이고 객관적인 기준에 따라 체계적으로 실시하기 위하여 시험 절차, 기준 등 세부사항을 정의한다[5].

무기체계 소프트웨어 개발 매뉴얼에 따르면, 소프트웨어 신뢰성 시험은 소프트웨어가 동작할 수 있는 다양한 경우의 수를 확인함으로써 소프트웨어가 일으킬 수 있는 결함을 식별하는 시험이다. 신뢰성 시험은 다음과 같이 정적시험 및 동적시험으로 나눌 수 있다.

- 정적시험: 소프트웨어를 실행하지 않고 코딩 규칙 준수여부, 취약점, 소스 코드 메트릭 점검을 통해 실행시간 중에 발생할 수 있는 오류를 예방한다.
- 동적시험: 실제 하드웨어(Target)에 탑재한 상태에서 소프트웨어 통합시험절차서에 기술된 시험절차에 따라 요구사항 기반으로 소프트웨어 코드 실행률을 점검한다.

이중 동적시험은 신뢰성 시험에서 70% 이상의 많은 시간과 인력이 투입되는 시험으로, 신뢰성 시험 수행을 위해 자동화 도구 사용은 필수적이라고 할 수 있다. 또한 자동화 도구 사용시 한번 구축한 시험 케이스는 재 사용이 가능하다. 자동화 도구를 사용하기 위해서는 관련표준에서 인증된 제품을 사용하는 것으로 개발 계획 단계에서 고려되어야 한다.

최종적으로는 신뢰성 시험결과 미 충족 부분에 대해서는 건 별로 소명서를 작성하여 기술지원기관의 승인을 받아야만 한다.

2.3 파티셔닝 분석

RTOS에서 제공하는 파티셔닝은 Fig. 2와 같이 메모리, 처리 능력, 입력/출력 장치와 같은 시스템 리소스를 분할하여 소프트웨어 구성 요소 간에 격리를 제공한다. 이러한 파티셔닝은 결함을 격리시키고 결함 발생시에도 다른 파티셔닝에서 작동하는 소프트웨어 구성요소에 영향을 미치지 않도록 한다.

파티셔닝에 대한 국제표준으로는 ARINC 653 표준이 있다. ARINC 653은 소프트웨어를 파티션 레벨과 모듈 레벨로 이루어진 계층적 설계를 하도록 하고 있다. 모듈 레벨에서는 하드웨어의 자원을 제어하여 각 파티션에 시간과 공간을 분리하여 스케쥴링하는 역할을 주로 수행한다[6].

ARINC 653 표준의 파티션 레벨에서는 모듈 레이어별로 할당 받은 자원과 시간을 활용하여 OFP (Operational Flight Program)와 같은 어플리케이션을 수행한다. Figure 2의 ARINC 653 구조에서 하나의 파

티션은 다른 여러 파티션과 모듈 소프트웨어를 통해 내부적으로 하드웨어로 직접적으로 접근할 수 없다. 파티션은 모듈 소프트웨어를 통해서만 하드웨어로 접근이 가능하다[7]. 파티셔닝에서 시스템 리소스는 독립적인 파티션으로 나뉘며 우선순위 수준에 따라 특정 작업에 할당된다.

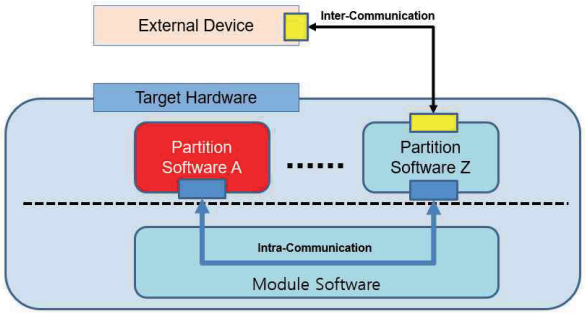

Fig. 2 ARINC 653 Structure

각 파티션은 다른 파티션과 분리되어 있어 한 파티션에서 실행 중인 작업이 다른 파티션에서 실행 중인 작업을 방해하지 않는다. 때문에 한 개의 파티션에서 작동중인 소프트웨어가 작동 불능상태에 빠져도 다른 파티션에서 구동중인 소프트웨어는 영향을 받지 않을 수 있다.

3. 임무 소프트웨어 개조개발 사업

기존 KT-1수출형 항공기의 임무 소프트웨어는 개발 당시 해외 선진업체와 공동 개발로 개발하였다. 이에 따라, 감항인증의 기준은 MIL-HDBK-516C에 따라 해당 기준으로 안전평가 프로세스를 수행하였다. 소프트웨어 개발 절차는 DO-178B를 준수하여 개발하였다. 임무 소프트웨어는 하나의 CSCI로 되어 있었다. 안전필수기능에 해당되는 PFD (Primary Flight Display) 정보도 시현을 하였으나, 계기 정보를 시현하는 H/W가 주 장비로 존재하고, 임무 소프트웨어는 보조 장비로 분류되어 DAL C에 준하여 개발하였다.

수출형 사업의 경우 새로운 해외 고객의 구매에 따른 항공기의 임무 소프트웨어 개조도 고객의 요구에 따라 변경된 부분에 대하여 기존의 DO-178을 준수하는 개발환경과 개발절차에 따라 개발하면, 개조된 부분과 영향성이 있는 부분만 검토를 받고 임무 소프트웨어에 대한 감항인증을 받을 수 있었다. 최초 개발 당시 무기체계 소프트웨어 개발 매뉴얼의 신뢰성 시험에 대한 규정도 없었기 때문에 신뢰성 시험은 수행하지 않았다.

국내 소요군을 위해 시행되는 통신 장비를 통합하는 임무 소프트웨어 개조개발에서 무기체계 소프트웨어 개발 매뉴얼을 충족하기 위해 도출된 문제점은 아래와 같다.

- 기존 임무 소프트웨어는 방사청 무기체계 소프트웨어 개발 매뉴얼 상의 신뢰성 시험을 실시하지 않았기 때문에 신규개발 소프트웨어에 해당하여 기존의 약 40만 라인의 모든 소스 코드에 대하여 신뢰성 시험을 수행해야 한다.
- 해외 공동개발 업체가 개발한 소스 코드도 경우에 따라 한국 방사청의 무기체계 소프트웨어 개발 매뉴얼의 기준에 따라 신뢰성 시험을 수행하고 시험 기준을 만족시켜야 할 수도 있다.
- 무기체계 소프트웨어 개발 매뉴얼 상의 신뢰성 시험 중 정적시험의 코딩규칙과 메트릭 등을 만족시키기 위해 기존의 소스 코드를 대부분 재개발해야 한다.

4. 임무 소프트웨어 신뢰성 시험 방안

우리는 DO-178C 적용과 무기체계 소프트웨어 개발 매뉴얼 적용을 동시에 수행하기 위한 효율적이고 효과적인 방안으로 Fig. 3과 같은 단계를 제안하며, 이러한 절차를 걸친 임무 소프트웨어 신뢰성 시험 방안을 고찰한다.

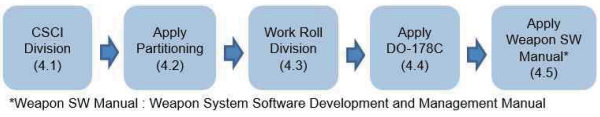

Fig. 3 Reliability Test Method Steps

4.1 임무 소프트웨어 기능별 CSCI 분리 및 등급 적용

기존의 임무 소프트웨어는 DO-178B 기준 DAL C의 등급을 준수하여 개발하였다. 항법 정보 등도 시현하기 때문에 무기체계 소프트웨어 개발 매뉴얼에 따라 결함 영향도, 결함발생 빈도 및 결함제어 가능성을 종합하여 평가하게 되면 가장 높은 등급인 DAL A 등급까지도 받을 수 있다.

우리는 임무 소프트웨어의 모든 기능들이 DAL A 등급의 신뢰성 시험을 해야 하는 비효율성을 해결하기 위해 Fig. 4처럼 기존에 공동 개발하였던 1개의 CSCI로 구성된 임무 소프트웨어를 기능별로 나누어 여러 개의 CSCI로 구성하고, 이러한 각 CSCI를 파티션으로 분할하는 것을 제안한다.

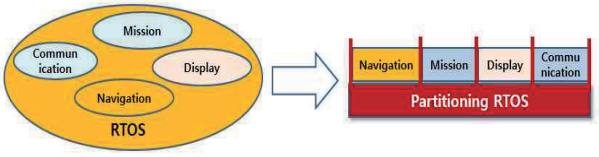

Fig. 4 CSCI Division

기존의 임무 소프트웨어는 기능별로 모듈화 되어 있지만, 하나의 CSCI로 구성되어 있기 때문에 DAL D 수준의 모듈을 추가 개발하더라도 모든 소프트웨어에 대하여 DAL A 수준의 신뢰성 시험을 수행해야 한다. 좀 더 효율적인 신뢰성 시험을 수행하기 위해 파티셔닝 RTOS를 기반으로 하여 기능들을 모듈화 하고 별도의 CSCI로 구성하였다. DAL A와 DAL B, DAL C, DAL D로 파티셔닝을 구성하면 파티셔닝 별 최고 높은 안전등급에 맞는 신뢰성 시험을 수행하면 된다. 한 개의 파티셔닝에 DAL D의 기능들만으로 구성을 할 경우 해당 파티셔닝은 DAL D에 해당하는 신뢰성 시험을 하면 된다.

주요 기능들에 대하여 시스템 안전평가 프로세스를 수행하여 DAL 등급을 받은 후 DAL 등급 별로 CICI로 구성하여 신뢰성 시험을 수행하는 것이 효율적인 것으로 판단하였다.

4.2 파티셔닝 적용

CSCI별로 등급에 맞춰 신뢰성 시험을 하기 위해서는 파티셔닝을 지원하는 RTOS를 사용해야 하며, 툴 검증을 대체하기 위해 툴 인증을 받은 RTOS를 사용하여야 한다.

본 사업에서는 ARINC 653 표준을 준수하고 DO-178C DAL A 인증을 받은 Green Hills Software사의 INTEGRITY-178 tuMP(Time-variant Unified Multi-Processing)를 RTOS로 사용한다.

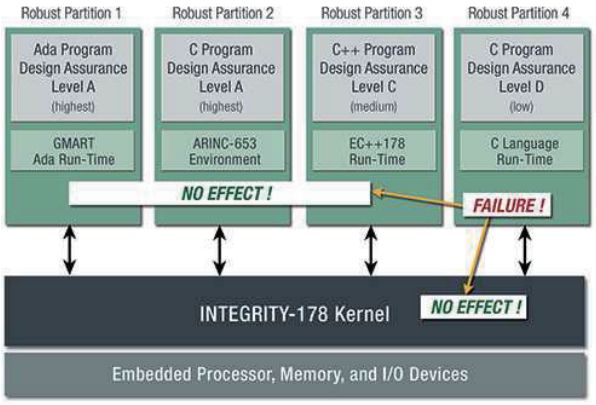

Fig. 5 INTEGRITY-178 RTOS Structure

INTEGRITY-178 tuMP는 다수의 항공기에서 인증을 받았고, 다양한 마이크로프로세서를 기반으로 시스템 안정성 관점에서 입증되었음을 확인하였다.

INTEGRITY-178 RTOS는 Fig. 5와 같이 강력한 파티셔닝 기능을 제공하며, 한 파티션의 결함으로 인한 오류가 다른 파티션 프로그램의 작동을 방해할 수 없음을 보장한다[8].

파티셔닝이 보장되고 검증된 RTOS를 기반으로 해외업체가 개발한 기능들과 국내업체가 개발해야 할 기능들을 별도의 CSCI로 구성하고, 해당 CSCI별 신뢰성 시험 기준과 DAL 레벨에 따른 신뢰성 시험을 수행하는 것으로 한다.

4.3 임무 소프트웨어 개발역할 분리

본 사업은 임무장비 체계통합 사업으로 기존은 임무 소프트웨어의 변경은 최소화하고, 일부 임무를 담당하는 Communication 부분을 개발하여 임무 소프트웨어에 통합하는 사업으로 진행한다.

이를 위해 이전에 해외업체가 개발한 임무 소프트웨어의 대부분은 큰 변경 사항 없이 새로운 임무 컴퓨터와 INTEGRITY-178 RTOS에서 작동할 수 있도록 해외업체가 DO-178C를 준수하여 개발하게 한다. 해외업체가 개발한 CSCI는 무기체계 소프트웨어 개발 매뉴얼에 따라 상용(COTS, Commercial-Off-the-Shelf) 소프트웨어에 해당되어 DO-178C 만 준수하고 신뢰성 시험 등 산출물과 DER (Designated Engineering Representative)의 공식 결과 보고서를 제출하면 감항인증을 받을 수 있다.

국내업체는 신규 개발 소프트웨어인 Communication CSCI를 소프트웨어 개발 매뉴얼과 DO-178C의 신뢰성 시험 기준을 모두 준수하여 개발하고 이를 임무 소프트웨어에 통합하여 감항인증을 받을 수 있도록 한다. 해외업체와 국내업체의 개발범위와 인증 방안은 Fig. 6과 같다.

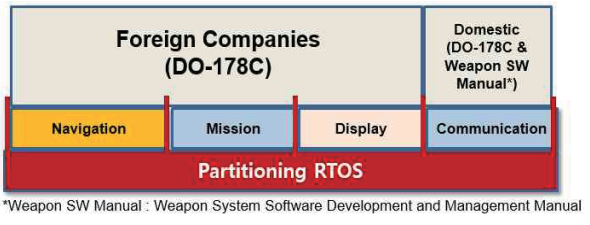

Fig. 6 Roll & Certification Standard

4.4 DO-178C 적용

DO-178C를 준수하는 신뢰성 시험을 인정받기 위해서는 DO-178C의 가이드에 따라 개발을 진행하고 시험 기준을 만족시키면 된다. DO-178에서의 검증절차

는 크게 검토, 분석 및 시험으로 진행한다. 요구도, 소스 코드, 추적성 등 문서나 데이터에 대하여 검토와 분석작업을 수행하고, 나머지는 시험을 통해 검증 기준을 만족하면 된다. 향후 수출기 사업에서도 활용을 위해 기존의 사업과 동일하게 DO-178C를 준수하는 영문 산출물들을 작성한다.

DO-178에 준하는 사내 개발 및 시험절차가 있고, DO-178을 준수하여 개발하였음을 입증하는 산출물들을 감항인증 단계에서 국내 감항당국에 제출하여 인증을 받았다. 본 사업에서는 해외업체의 신뢰성 시험 인증을 받기 위해 비용이 발생하더라도, 해외 DER을 고용하여 계획단계인 SOI(Stage of Involvement) 1단계부터 2단계 개발, 3단계 시험까지 공식적으로 DO-178C를 준수하였음을 인정받는 결과 보고서를 받을 수 있도록 한다. 해외업체도 별도로 고용된 DER의 참여와 검증을 통해 DO-178C를 준수하였음을 입증하는 결과 보고서를 받아서 임무 소프트웨어 전체에 대하여 시험단계인 SOI 3단계까지 DO-178C 준수를 공인 받기로 한다.

4.5 무기체계 소프트웨어 개발 매뉴얼 적용

무기체계 소프트웨어 개발 매뉴얼을 충족하는 신뢰성 시험을 인정받기 위해서는 국내 기술지원기관의 신뢰성 시험 참관과 검토 및 승인을 받아야 한다. 무기체계 소프트웨어 개발 매뉴얼의 산출물 양식은 한글로 되어 있어 기존 사업에서 DO-178을 준수하기 위하여 개발한 양식의 산출물로는 대체할 수 없다.

신뢰성 시험을 위해서는 정적시험과 동적시험을 위한 추가 개발환경 구축과 자동화된 시험환경을 구축하기로 한다. 기술지원기관의 참관 하에 시험기준을 만족하였음을 시연하고 소프트웨어 신뢰성 시험 확인서와 함께 소프트웨어 시험 결과서를 제출하기로 한다.

4.6 DO-178C와 무기체계 소프트웨어 개발 매뉴얼의 산출물 적용 비교

무기체계 소프트웨어 개발 매뉴얼에서 신뢰성 시험 관련 내용이 들어가는 산출물과 DO-178C 산출물의 비교는 Table 1과 같다. 무기체계 소프트웨어 개발 매뉴얼과 DO-178C에서 요구하는 공식 산출물들은 내용에 있어서도 유사한 부분이 있다. 또한, DO-178C의 경우 한글 양식의 산출물이라도 내용이 DO-178C에서 요구하는 요건만 충족하면 별도의 영문 양식의 산출물은 만들지 않아도 된다. 하지만, 무기체계 소프트웨어 매뉴얼의 산출물 양식은 한글로 되어 있으며 양식을 준수해야 하기 때문에 DO-178C의 문서로 대체하기 힘들다.

Table 1 Matrix Table of Development Outputs

Weapon System	DO-178C	Reference
-	PSAC	(For FAA Submission)
SDP	SDP	Requirements-based Test Plan on Target
STP	SVP	Inclusion of Static/Dynamic Reliability Test
STD	SVCP	Inclusion of Static/Dynamic Reliability Test
STR	SVR	Inclusion of Reliability Test Result
Software Reliability Test Confirm	Software Verification Review Report	Generation by Reliability Test Technical Support Division

본 사업에서는 DO-178을 준수하기 위한 영문 산출물과 무기체계 소프트웨어 개발 매뉴얼의 한글 양식의 산출물을 모두 개발하는 것으로 하였다.

5. 임무 소프트웨어 신뢰성 시험 방안 적용 사례

본 장에서는 기존의 KT-1 임무 소프트웨어에 통신 기능을 개발하여 통합하는 사업에서 소프트웨어 신뢰성 시험을 적용하는 방안을 적용한 사례를 설명한다. 이 중에서도 임무 소프트웨어 중 국내업체가 개발하는 Communication Software(가칭)의 신뢰성 시험 방안 적용 사례를 위주로 기술한다.

5.1 임무 소프트웨어 신뢰성 시험 승인 기준

임무 소프트웨어의 감항인증 기준은 MIL-HDBK-516C와 무기체계 소프트웨어 개발 매뉴얼이다.

MIL-HDBK-516C 국제 표준의 준수 입증 수단인 MOC(Means Of Compliance)로는 RTCA/DO-178C를 선택하여 준수해 오고 있었다. DER이 인증 심사에 사용하는 가이드라인으로는 FAA Order 8110.49A가 사용되어 MOC를 충족 시 신뢰성 시험결과가 포함된 SOI #3 인증서를 받도록 한다[9].

다음으로, 무기체계 소프트웨어 개발 매뉴얼의 신뢰성 시험을 충족하기 위해서는 기술지원기관의 승인을 받도록 한다.

본 과제에서 기존의 임무 소프트웨어의 대부분 기능은 해외업체가 DO-178C에 따라 동일한 기능을 개발하고 국내업체가 신규로 개발하는 통신기능을 담당하는 부분인 Communication Software는 기존의 DO-178C의 준수와 함께 무기체계의 신뢰성 시험을 준수

하여 개발하기로 한다.

5.2 신규개발 소프트웨어 별도 CSCI 분리 및 등급 적용

4.1절에서 설명한 바와 같이, 기존의 임무 소프트웨어를 시스템 기능 별로 재사용하는 부분과 신규 개발로 재 분류하여 CSCI로 구분한 뒤 인증 체계를 적용하였다. 이러한 각 소프트웨어 기능을 인증과 매칭하면 Table 2와 같이 분류할 수 있다.

임무 소프트웨어에 있어서 기존의 공대공(Air to Air), 공대지(Air to Ground) 임무를 담당하는 컴포넌트는 Mission Management로 기능을 통합하였다. EGI(Embedded GPS Inertial navigation systems), 통신, 네비게이션 등을 담당하는 컴포넌트는 Sensor Management로, 무장 투하 알고리즘과 무장 관리 컴포넌트는 Weapon Management 로 기능을 통합하였다. I/O Management는 원래 있던 기능이다.

Communication Software는 신규로 개발하는 통신 기능이다. 해당 기능은 Communication Management 기능으로 하여 임무 소프트웨어에 통합하였다.

Table 2 System Functional Description

Software	Primary Functions	Certification
Mission Computer Software	Mission Management	DO-178C
	Sensor Management	
	Weapon Management	
	I/O Management	
Communication Software	Communication Management	DO-178C + Weapon SW Manual*

*Weapon SW Manual: Weapon System Software Development and Management Manual

Mission Computer Software는 기존의 임무 소프트웨어의 기능 중 해외 협력업체에서 개발해야 할 부분을 COTS로 구매하는 부분이다. 따라서 해당 파트의 신뢰성 시험은 해외 협력업체 DER의 감독하에 DO-178C를 준수하여 개발한 소프트웨어 시험결과서와 SOI 3단계 인증서를 받는 것으로 대체할 수 있었다.

Communication Software는 국내에서 신규로 개발해야 하는 기능인 통신기능 통합 부분이다. 해당 부분을 CSCI로 하여 DO-178C를 준수하고, 무기체계 소프트웨어 개발 매뉴얼도 준수할 수 있도록 신뢰성 시험 계획을 세우고 진행하였다. 이 부분은 5.4장과 5.5장에서 추가로 설명한다.

5.3 CSCI에 따른 파티셔닝 구조와 역할 분리

기존의 임무 소프트웨어는 CSCI 1개로 되어 있지만, Fig. 7처럼 유지보수가 용이하도록 항법, 임무, HUD, MFD 등 주요 기능별로 분리가 가능하도록 모듈화 되어 개발되었기 때문에, 해당 기능들을 재 분류하여 별도의 CSCI로 통합하기가 용이하다.

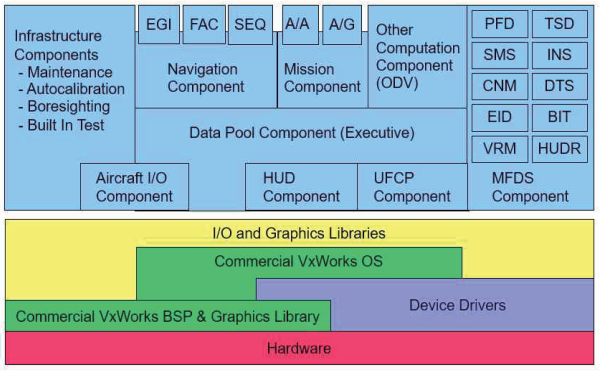

Fig. 7 Legacy Mission Software Structure

시스템 안전평가 프로세스를 통해 기능별 DAL등급을 도출하여 Mission Computer Software는 DAL B/C/D등급별로 재 분류한 후 3개의 CSCI로 통합하였다. Communication Software는 DAL C로 도출된 1개의 CSCI로 구성하였다. 총 4개의 CSCI를 4개의 파티션에서 독립적으로 구동 될 수 있도록 구성한 신규 임무 소프트웨어의 구조는 Fig. 8과 같다.

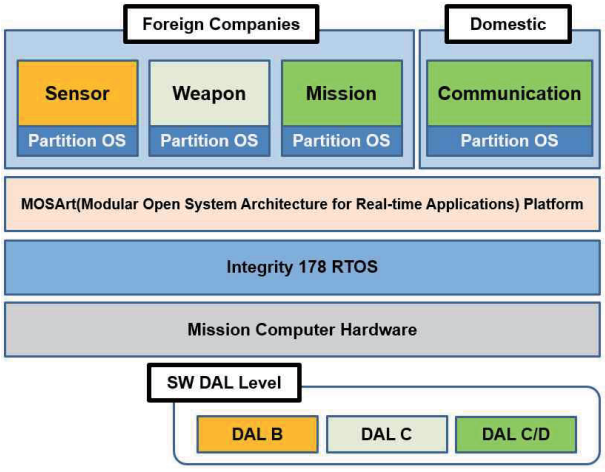

Fig. 8 New Mission System Software Structure

이렇게 분할된 CSCI에서 해외업체가 개발한 CSCI에 대해서는 해외에서 COTS로 구매하는 상용소프트웨어에 해당된다. DO-178C를 준수하여 개발한 산출물인 Software Test Report와 DER의 Audit 결과서 인 SOI 3단계 검토 리포트 문서를 제출하도록 한다. 문서 검토 후 승인을 받게 되면 본 사업의 임무 소프트웨어의 신뢰성 시험을 충족시킬 수 있도록 기술지원기관과 협의되었다.

5.4 임무 소프트웨어 신뢰성 시험 DO-178C 충족 기준

DO-178C의 표준에 따라 신규로 개발하는 Communication Software의 DAL을 결정하기 위해 MIL-HDBK-516C에 따라 Communication Software CSCI의 최악의 실패 상태를 도출하였다.

Communication Management 기능에 에러가 발생시 항공기의 안전에 영향을 주는 항목을 분석한 결과는 Table 3과 같이 정리하였다.

Table 3 Hardware Functions and Contribution to Potential Failures

Function	Example of Potential Failure
Provision of Communication Operation	Inability to Execute Communication Mission-related Tasks
Provision of Communication Message Information	Display and Operation of Incorrect or Inconsistent Mission Data
General Provision of Computing Capability	Total Loss of Mission Computer Platform

Table 3에서 첫 번째 기능은 Communication 네트워크 운용이며, 운용이 안될 경우 Communication 임무와 관련된 과업을 할 수 없게 된다. 두 번째 기능은 Communication 메시지 정보를 제공하는 것이며, 부정확하거나 일관성 없는 임무 데이터가 시현되거나 작동될 경우가 발생할 수 있다. 세 번째 기능은 컴퓨터의 계산 능력을 제공하는 것이며, 컴퓨터의 계산 능력을 초과하게 되는 경우를 가정할 수 있다. 이 때는 임무 컴퓨터의 기능을 잃게 된다.

그러나, 이러한 실패의 상황이 인명의 피해 등의 치명적인 실패는 아니다. 따라서, Communication Software CSCI의 기능에 대하여 수행한 시스템 안전 평가 프로세스 결과 세 번째 안전성 수준인 DAL C Level로 결정되었으며, 이에 따라 DAL C의 시험 목표를 충족하도록 한다.

DAL C를 만족하기 위한 목표는 아래와 같으며, Software Verification Results의 산출물 형태로 작성되어야 한다.

- 시험 절차들은 정확해야 한다.
- 시험 결과는 정확하고 불일치는 설명되어야 한다.
- 상위 요구도의 커버리지가 달성되어야 한다.
- 하위 요구도의 커버리지가 달성되어야 한다.
- 소프트웨어 구조(문장 커버리지) 커버리지가 달성되어야 한다.
- 소프트웨어 구조(데이터 커플링과 컨트롤 커플링) 커버리지가 달성되어야 한다.

DAL C 등급의 소프트웨어 시험은 요구도에 따라 시험절차서가 만들어져야 하며, 상위 요구도와 하위 요구도에 대한 시험이 이루어져야 한다. 추적성도 시스템 상위 요구도와 소프트웨어 상위 요구도, 소프트웨어 하위 요구도, 소스 코드까지 연결되어야 한다. 이를 위해서 상/하위 요구도와 시험 절차서 및 시험 수행결과까지 국내업체가 개발한 SILKROAD 개발형상 관리 프로그램을 통해 개발 산출물들을 관리하여 추적성 및 모든 요구도에 대한 커버리지가 누락되지 않도록 한다.

커버리지 분석은 문장에 대하여 100%를 달성해야 한다. 시험 커버리지 분석은 두 단계로 이루어 지며, 요구사항 기반 커버리지 분석은 소프트웨어 상위 요구도를 검증하는 기능시험과 소프트웨어 하위 요구도를 검증하는 Unit Test를 통해서 코드 실행률 100%를 달성하도록 한다.

강건성 시험을 위해 최대 최소값과 유효하지 않는 값을 입력하여 이상이 없는지를 확인하는 시험도 수행한다.

DO-178C에서는 DO-178B에 추가하여 Data Coupling과 Control Coupling을 만족할 것을 요구하고 있다. Data Coupling은 동적 데이터 흐름 분석을 통해 글로벌 변수와 매개 변수가 명확하게 사용되었는지를 확인하는 것이고 Control Coupling은 프로시저의 호출이 문제가 발생하지 않도록 명확히 사용되었는지를 분석하는 것이다. 이를 소프트웨어 개발 단계에서 동료평가를 통해 확인하도록 한다.

5.5 임무 소프트웨어 신뢰성 시험 무기체계 소프트웨어 개발 매뉴얼 충족 기준

무기체계 소프트웨어 개발 매뉴얼기준의 신뢰성 시험은 Fig. 9와 같이 정적시험과 동적시험으로 구분된다. 정적시험은 소프트웨어를 실행하지 않은 상태에서 잠재적인 결함을 검출하는 시험을 말한다. 동적 시험은 소프트웨어를 실행한 상태에서 잠재적인 결함을 검출하는 시험을 말한다.

Figure 9에서 보인 바와 같이 정적시험은 코딩 규칙 검증, 취약점 점검 및 소스 코드 메트릭 (Code Metrics) 점검으로 나뉘어진다. 이중, 코딩 규칙은 MISRA-C 총159개 규칙, MISRA C++ 총 288개 규칙을 적용하였다. 취약점 점검은 CWE(Common Weakness Enumeration)-658 총 84개 규칙과 CWE-659 총 88개 규칙을 적용하였다. 소스 코드 메트릭 점검은 6개의 점검 항목(Cyclomatic Complexity, Number of Call Levels, Number of Function Parameters, Number of Calling Functions, Number of Called Functions, Number of Executable Code Lines)

을 시험기준으로 적용하였다. 상용화된 정적시험도구는 시험도구에서 정적시험 적용 항목들과 제한 값을 선택하면 자동으로 시험 결과 위반 사항들을 정리해 준다.

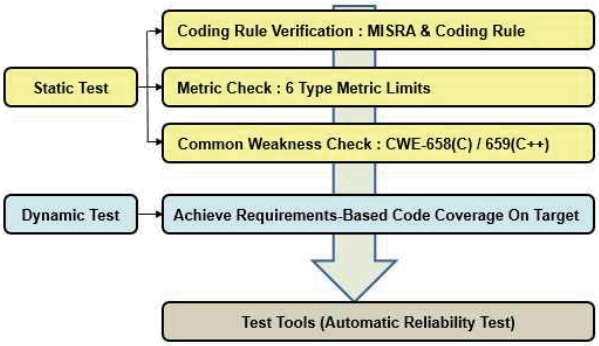

Fig. 9 Communication Software Reliability Test

이 때 정적시험을 제외할 수 있는 조건이 있는데, 상용소프트웨어(Hardware와 함께 제공되는 소프트웨어 포함)는 코딩 규칙 적용대상에서 제외한다. 또한 심볼 생성을 위한 Ansys사의 SCADE 프로그램과 같이 그래픽 디자인을 소스 코드로까지 자동 생성해주는 프로그램의 경우 코드 자동생성에 대한 개발 툴 인증을 받아서 정적시험 대상에서 제외할 수 있다. 이에 따라, 본 사업에서는 SCADE를 이용하여 개발한 프로그램 부분은 정적시험 대상에서 제외하였다.

동적시험은 소프트웨어를 실제 하드웨어(Target)에 탑재한 상태에서 소프트웨어 통합시험 절차서에 기술된 시험절차에 따라 요구사항기반으로 소프트웨어 코드 실행률을 점검하는 것을 말한다. 이러한 동적 시험을 위하여 6장에서 시험 자동화를 위한 도구를 선정한다. 동적시험 평가 기준으로는 임무 컴퓨터에 Communication Software를 로딩 하여 요구사항 기반의 시험을 수행하여 문장에 대한 코드 실행률을 100%를 달성하도록 한다.

6. 소프트웨어 신뢰성 시험 자동화를 위한 도구 선정

국내업체가 개발하는 Communication Software의 신뢰성 시험을 위해서 기존 DO-178을 만족하기 위해 사용했던 정적시험 도구와 문장 커버리지를 만족시키기 위한 유닛 테스트 도구로는 무기체계 소프트웨어 개발 매뉴얼의 신뢰성 시험을 충족시키기 어려웠다. 따라서, 정적시험과 동적시험 수행을 위한 도구를 추가로 선정하였다.

무기체계 소프트웨어 개발 매뉴얼의 정적시험에서 요구하는 코딩 규칙(Coding Rule)인 MISRA-C/C++ 지원하고, 취약점 점검을 위한 CWE-658/659 지원 및 소스 코드 메트릭 점검을 자동으로 수행할 수 있는 정적시험 도구로는 국산 슈어소프트사의 CODESCROLL STATIC을 선정하였다. CODESCROLL STATIC은 DO-178C에서 요구하는 코딩 스탠다드를 만족하는 시험을 할 수 있으며 DO-330 Tool Certification 인증을 획득한 제품이어서 DO-178C의 시험기준도 만족시킬 수 있다.

무기체계 소프트웨어 개발 매뉴얼의 동적시험에서 요구하는 타겟에서 요구도 기반 시험과 코드 실행률 달성 여부를 확인할 수 있는 동적시험 도구로서 슈어소프트사의 COVER와 Controller Tester를 선정하였다. COVER는 타겟인 임무컴퓨터에서 임무 소프트웨어를 로딩 하여 요구도 기반의 시험을 할 수 있고, 코드 실행률 달성 여부를 종합하여 시현할 수 있다. Controller Tester는 요구도 기반 시험에서 불가피하게 코드 실행률을 달성하지 못한 부분에 대하여 구조기반 단위 시험을 통하여 나머지 코드 실행률을 달성할 수 있도록 하는 제품이다. COVER, Controller Tester도 DO-330 Tool Certification 인증을 획득한 제품들로는 DO-178C에서 요구하는 문장에 대한 커버리지 달성 여부 시험을 만족할 수 있다.

우리는 Fig. 10과 같이 신뢰성 시험 자동화 환경을 구축하였다. 개발자들이 개발한 코드를 서버에 로딩하게 되면 하루 단위로 자동 컴파일 후 정적시험 도구와 동적시험 도구가 자동으로 시험하고 결과를 알려주어 개발자들이 코드를 수정할 수 있도록 하였다. 또한 임무 컴퓨터에서 수행한 동적시험 결과 및 코드 실행률 달성 결과를 시험도구에서 확인하고 문서화할 수 있도록 하였다.

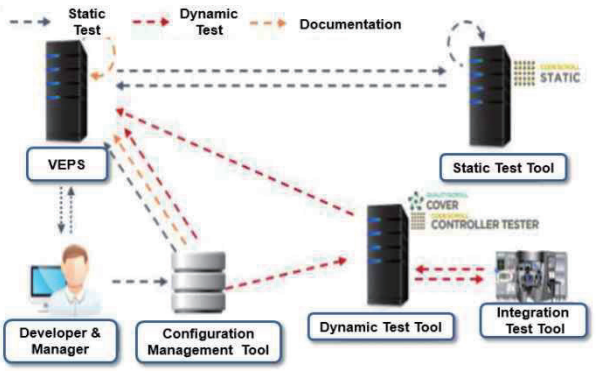

Fig. 10 Reliability Test Environment

이렇게 소프트웨어 신뢰성 시험 자동화를 위한 도구를 사용하게 되면 다음가 같은 장점이 있다. 첫째, 신뢰성 시험 정적 도구와 동적 시험 도구들이 도구 인증

을 통해 무기체계 소프트웨어 개발 매뉴얼에서 규정한 코딩규칙 등을 준수하였음을 보증하여 준다. 따라서 개발자들은 시험 도구가 알려주는 결과만을 보고 수정 작업을 통해 문제를 해결할 수 있다. 둘째, 개발자 각자가 소스 코드 수정 후 개별적으로 3~4시간이 소요되는 정적/동적 시험을 수행하고 문제점을 찾기 위해서는 많은 시간과 리소스가 필요하다. 신뢰성 시험 자동화를 구축하게 되면, 개발자는 별도로 신뢰성 시험을 수행하지 않고, 매일 저녁 서버에서 1개의 라이선스로 수행되는 신뢰성 시험 결과만을 보고 개발만 하면 된다. 마지막으로, 문제 해결에 있어서도 위반에 대한 다른 개발자의 수정 사항을 참고할 수 있어 빠른 문제해결과 전체 소프트웨어의 신뢰성을 높일 수 있다.

7. 결 론

본 연구는 해외 수출용으로 개발된 KT-1 임무 소프트웨어에 통신 장비를 통합하는 사업에서 국내용으로 활용하기 위하여 국내의 표준인 무기체계 소프트웨어 개발 및 관리 매뉴얼에서 규정한 소프트웨어 신뢰성 시험을 어떻게 수행할 수 있는가에 대한 문제를 풀어 내었다. 당시 해외업체와 공동 개발한 소스 코드를 국내업체가 보유하고 개조하여 수출기에 활용하였지만, 국내 납품을 위해 신뢰성 시험을 수행하지 않은 소스 코드 전체를 무기체계 소프트웨어 개발 매뉴얼의 보다 강화된 신뢰성 시험 절차를 준수하기에는 많은 시간과 자원의 투입이 필요한 상황이었다. 또한, 향후 지속적인 해외 수출과 국내 납품을 위해 무기체계 소프트웨어 개발 매뉴얼의 준수와 함께 수출을 위하여 DO-178C를 동시에 준수해야 했다.

본 논문은 이러한 상황, 즉 DO-178C는 준수하고 있었으나 무기체계 소프트웨어 개발 및 관리 매뉴얼을 준수하고 있지 않았던 기존 임무 소프트웨어의 개조 개발사업에 대하여 가장 효율적인 신뢰성 시험 방안을 적용할 수 있는지에 대하여 고찰하였다. 주요 아이디어는 기존에 안전평가 프로세스를 통해 한 개의 CSCI로 구성된 임무 소프트웨어를 기능에 따라 나누고, DAL 레벨 별로 분류하여 여러 개의 CSCI로 구성하는 것이었다. 기존의 기능에 변화가 없는 해외업체의 기능은 별도의 CSCI로 구성하여 해외 상용소프트웨어로 분류하고, 국내업체가 새롭게 개발하는 통신 기능에 대한 CSCI를 별도로 개발하여 별도의 파티셔닝에서 구동 될 수 있도록 한다면, 한정된 자원으로 높은 수준의 신뢰성을 확보하고 기존의 임무 소프트웨어에 대한 변경 영향성을 최소화할 수 있었다. 또한 DO-178C 준수를 위해 각 업체가 DER을 활용하여 개발하고 Audit 결과까지 받는 방안을 제시하였다.

또한 국내업체가 개발한 부분에 대하여 신뢰성 시험 자동화 환경을 구축하여 개발자들이 효율적으로 소프트웨어에 대한 신뢰성 시험을 수행할 수 있도록 하였다. 이를 통해 해외 수출을 위한 감항인증과 국내 무기체계 소프트웨어 개발 매뉴얼에서 규정한 소프트웨어 신뢰성 시험을 효과적으로 수행할 수 있다.

본 연구 결과는 해외업체와 공동 개발하여 수출되고 수십 년간 안정적으로 운용되고 있는 임무 소프트웨어를 이전에 많은 개발 예산을 투입하여 운용시험 및 평가 등을 통해 검증된 안전성을 해치지 않고 무기체계 소프트웨어 개발 매뉴얼 상의 신뢰성 시험을 적용하는 방안을 제시하였다. 본 연구 결과는, 향후 해외업체와 공동 개발된 KT-1 항공기 임무 소프트웨어의 재시험 및 재검증으로 과다하게 소요되는 비용 요소를 제거할 근거가 되어, 국내 무기체계 소프트웨어 획득 비용을 낮출 수 있을 것으로 전망한다.

후 기

본 논문은 산업통상자원부 융합기술사업화 확산형 전문인력 양성사업(2023년도)과 한국항공우주산업㈜의 지원을 받아 작성된 논문입니다.

References

[1] Firesmith, D.G., Capell, P., Falkenthal, D., Hammons, C.B., Latimer IV, D.T. and Merendino, T., *The method framework for engineering system architectures*. CRC Press, 2008.

[2] DAPA, "Military Aircraft Standard Airworthiness Certification Criteria", *DAPA Notice*, 2017-3, April 2017.

[3] Heo, J.G., Kim, M.S., Kim, M.T. and Moon, Y.H., "The Study on Airworthiness Certification Process on Military Airborne Safety Critical Software based on DO-178", *Journal of Aerospace System Engineering*, *13*(1), pp.62-68, 2019.

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

[5] DAPA, Weapon System S/W Development and Management Manual, *DAPA Notice 2020-1*, Feb. 2020.

[6] ARINC, "Avionics Application Software Standard Interface Part 1 - Required Services." *Specification 653P1-3*, 2010. http://www.arinc.com

[7] Lee, S.H., Yoon, K.B, Lee, J.M., Yoon, S.H., "A Study on ARINC 653 Partition Software Fault Injection Test", *KSAS*, pp.271-272, 2018.

[8] Green Hills Software, https://www.ghs.com.

[9] FAA, "Software Approval Guidelines", *FAA ORDER, 8110.49*, Sep. 2011.