Technical Paper

Journal of Aerospace System Engineering
Vol.15, No.3, pp.71-78 (2021)

EISSN 2508-7150
http://dx.doi.org/10.20910/JASE.2021.15.3.71

MIL-HDBK-516C 기반의 군용항공기 탑재 소프트웨어 개발 프로세스

허진구[1] · 문용호[2,†]

[1]국방기술품질원 / 경상국립대학교 기계항공공학부
[2]경상국립대학교 항공우주 및 소프트웨어공학과

Software Development Process of Military Aircraft based on MIL-HDBK-516C

Jin-Gu Heo[1] and Yong-Ho Moon[2,†]

[1]Defense Agency for Technology and Quality / Aerospace Engineering, Gyeongsang National University
[2]School of Aerospace and Software Engineering, Gyeongsang National University

Abstract

Since most functions of modern aircraft are controlled by software, software errors are directly related to aircraft safety. The criterion in Chapter 15 of the MIL-HDBK-516C addresses safe development and verification of military aircraft software. As the U.S. Air Force repeatedly experienced non-compliance with Chapter 15 criterion of the MIL-HDBK-516C, it published an Airworthiness Circular (AC-17-01) as a guide to meeting the criterion. In this paper, Chapter 15 of MIL-HDBK-516C, AC-17-01 and the SW Qualification Guideline (DO-178C) as applied by the Federal Aviation Administration are compared and analyzed. For the analysis, a matching ratio formula between the MIL-HDBK-516C criteria specified in AC-17-01 and the DO-178C specified in MIL-HDBK-516C criteria is defined. The sections that satisfy MIL-HDBK-516C criterion are derived when AC-17-01 or DO-178C matches. Based on the analysis results, the aircraft software development process is established and examples of application of Chapter 15 of MIL-HDBK-516C are addressed.

초 록

현대 항공기에서 대부분의 기능은 소프트웨어에 의해 통제되고 있으므로 소프트웨어 오류는 항공기 안전과 직결된다. MIL-HDBK-516C 15장은 군용항공기 탑재 소프트웨어의 안전한 개발과 검증을 위해서 적용되는 기준이다. 미 공군은 이 기준이 반복적인 미충족을 경험함에 따라 기준 충족을 위한 지침으로 감항성 회람(AC-17-01)을 발간하였다. 본 논문에서는 MIL-HDBK-516C 15장, AC-17-01, 그리고 미 연방항공청에서 적용하고 있는 SW 인증 지침(DO-178C)을 비교 분석하였다. 먼저 AC-17-01 단계와 각 단계에서 명시된 MIL-HDBK-516C 15장 기준 그리고 MIL-HDBK-516C 기준에서 DO-178C를 명시한 기준간 정합 비율 식을 정의하였다. 그리고 비율 분석을 통하여 AC-17-01과 DO-178C를 달성하는 경우 MIL-HDBK-516C 충족 가능한 기준을 도출하였다. 분석결과를 바탕으로 항공 소프트웨어 개발 프로세스를 수립하고 MIL-HDBK-516C 15장 적용 사례를 제시하였다.

Key Words : Airworthiness(감항), Certification(인증), DO-178C, Military Aircraft(군용항공기), MIL-HDBK-516C, Safety Critical(안전 필수), Software(소프트웨어)

1. 서 론

현대 대부분의 항공무기체계 관련 주요기능은 소프트웨어로 통제되고 있으며, 소프트웨어의 통제 범위는 비행 및 엔진 제어에서 항법, 통신, 센서까지 광범위하다. 따라서 소프트웨어의 기능 결함 또는 오작동은 항공기의 안전과 직접적으로 연관될 수밖에 없는 상황이다.

항공 선진국에서는 민간항공기 및 군용항공기에 탑

Received: Sep. 27, 2020 Revised: Nov. 22, 2020 Accepted: Nov. 28, 2020
† Corresponding Author
Tel: +82-55-772-1374, E-mail: yhmoon5@gnu.ac.kr

재되는 소프트웨어에 대한 비행 안전성 확보를 위하여 국제적인 기준들을 제정하였다. 민간항공기의 경우 미 연방항공청에서 적용하고 있는 DO-178C 그리고 군용항공기의 경우 미군에서 적용하고 있는 MIL-HDBK-516 15장이 대표적이다.

국내의 경우 2009년 군용항공기 비행안전성(감항) 인증에 관한 법률이 제정됨에 따라 2009년 이후 군용항공기 연구개발, 구매, 개조·개량 그리고 부품·구성품 및 무기·장비 등을 제작·개조 또는 개량하여 군용항공기에 장착하는 일련의 사업들은 감항인증의 대상이 되고 있다[1]. 하지만 군용항공기 탑재 소프트웨어의 경우, 사업 범위 내에서 감항인증을 수행하였거나, 또는 감항인증기준을 고려하지 않고 소프트웨어 개발 및 산출물을 작성하는 사례가 많이 발생하였다.

본 논문에서는 군용항공기 탑재 소프트웨어의 감항인증기준인 MIL-HDBK-516C 15장과 MIL-HDBK-516C 15장에 대한 세부지침으로 미 공군에서 발행한 감항성 회람(AC-17-01) 그리고 민간항공기에서 적용 중인 소프트웨어 인증 지침(DO-178C)에 각 장절 및 상호관계를 분석한다. 그리고 분석 결과를 바탕으로 AC-17-01 또는 DO-178C을 적용하여 요구된 목표를 달성한 경우 MIL-HDBK-516C 15장 기준 충족 여부 및 비행 안전을 고려한 소프트웨어 개발 프로세스를 세계 최초로 제안한다.

2. 본 론

2.1 항공 소프트웨어 감항인증기준 분석

2.1.1 MIL-HDBK-516C

MIL-HDBK-516C는 미군에서 채택하고 있는 감항인증기준이다. 국내에서는 「군용항공기 비행안전성 인증에 관한 법률」제3조에 따라 방위사업청에 의해 MIL-HDBK-516C를 기반으로 한 표준감항인증기준 Part 1이 고시되었다[2].

MIL-HDBK-516은 미 국방성에서 2002년 제정하였으며 3차례의 개정이 이루어졌다. 특히 소프트웨어 분야(15장)의 경우 MIL-HDBK-516B에서 C로 개정될 때 15장 분야명칭이 컴퓨터자원에서 컴퓨터시스템 및 소프트웨어로 변경되었으며 기준 수는 27개에서 42개로 증가하였다.

MIL-HDBK-516C 15장은 Table 1과 같이 6개 세부절과 42개의 기준으로 구성되어 있음을 알 수 있다. 컴퓨터시스템과 관련된 기준은 15.1절(12개 기준)과 15.2절(8개 기준), 하드웨어와 관련된 기준은 15.3절(4개 기준), 소프트웨어와 관련된 기준은 15.4절(3개 기준), 15.5절(10개 기준), 15.6절(5개 기준)에서 다루고 있다[3].

Table 1 Criterion In MIL-HDBK-516C Section 15

Section	Name	Criterion #
15.1	SPA(System processing architecture)	12
15.2	Design and functional integration of SPA elements	8
15.3	Processing hardware/electronics	4
15.4	Software development processes	3
15.5	Software architecture and design	10
15.6	Software qualification and installation	5

2.1.2 AC-17-01

미 공군은 감항인증 심사 활동 중 MIL-HDBK-516C 15장(컴퓨터시스템 및 소프트웨어) 감항인증기준이 반복적으로 미충족하는 것을 경험하였으며 이러한 기준 미 충족을 방지하고 개발 단계에서 비행안전성(감항) 관점에서 수행하여야 되는 활동에 대한 지침을 제공하기 위하여 2017년 3월 감항성 회람 AC-17-01을 발간하였다[4].

AC-17-01에서는 컴퓨터시스템 및 소프트웨어 개발 프로세스를 안전필수기능 식별, 안전필수기능 스레드 분석, 컴퓨터시스템 무결성 수준 할당, 소프트웨어 식별 및 안전지원요소의 개발 프로세스 목표/산출물이라는 5단계로 분류하고 있다.

1) 안전필수기능 (SCF; Safety Critical Function) 식별

SCF는 기능의 작동 결함 및 잘못된 작동으로 재난적 또는 치명적 심각도를 직접적으로 초래할 수 있는 기능으로 정의된다. 개발 기관에서는 직접적으로 초래할 수 있는 이라는 문구에 대하여 다양한 해석을 가지고 있었다. 이 문구에 대한 해석을 명확히 하기 위하여 AC-17-01 문서에는 SCF 식별 시 기능의 손실 또는 오작동 되었을 때의 확률을 고려하지 않아야하며 특정 조건하에서 작동 할 경우(비상조건, 특정 결함조건)를 고려되어야 한다고 명시되어 있다. 또한 SCF를

비행필수, 운용필수, 지시필수, 회피필수, 비상필수로 구분하여 구체화하였다.

2) SCF 스레드 분석 (SCFTA; Safety Critical Function Thread Analysis)

SCFTA 단계에서는 SCF 작동에 필요한 시스템 내 요소들의 조합과 요구되는 인터페이스를 식별하고 상호 관계가 분석된다. SCFTA는 분해, 분류 및 검증&확인 커버리지 분석 단계로 세분화된다.

분해 단계에는 SCF를 분해하여 데이터 출처/목적지 식별 및 데이터가 통과하는 기능적 경로를 분석하여 안전지원요소가 식별된다. 안전지원요소는 안전지원 소프트웨어요소와 안전지원 하드웨어요소로 세부적으로 분류된다. 스레드(기능적 경로) 다이아그램을 통하여 아키텍처 중복 설계 여부 및 인터페이스가 식별되며 모든 안전지원요소가 식별될 때까지 안전필수기능을 분해하고 식별된 모든 요소 및 인터페이스가 문서화된다.

분류 단계에는 식별된 안전지원요소에 대하여 수준(등급)을 할당하고 안전필수기능을 지원하는 인터페이스가 식별된다.

검증&확인 커버리지 분석 단계에는 SCF의 끝단간 검증&확인 커버리지 달성여부를 확인하기 위하여 기능 및 고장모드 영향성 시험 여부가 분석된다. 분석 내용에는 SCF 결함 및 오작동 시 영향 있는 요소가 식별되어 영향 요소들 간의 추적성이 제공되어야 한다.

3) 컴퓨터시스템 무결성 수준 (CSIL; Computer System Integrity Level) 할당

CSIL은 하드웨어 및 소프트웨어에 할당되는 설계보증 수준(DAL; Design Assurance Level)과 동일한 의미이며 일반적으로 수준(A가 최상위 수준)이 높을수록 요구도 또는 달성 목표가 많다. 이러한 수준 또는 등급(CSIL 또는 DAL)이 할당되면 이에 상응하는 개발 프로세스를 정의하고 적용하여야 한다.

4) 소프트웨어 식별

소프트웨어 식별 단계는 소프트웨어 형상항목 단위로 소프트웨어를 개발 및 비개발로 구분한다. 개발 소프트웨어는 자체 개발(개조) 또는 공급업체에 의해 개발(개조)되는 소프트웨어이며 비개발 소프트웨어는 수정되지 않은 상용제품 또는 재사용 소프트웨어이다.

5) 안전지원요소(SSE; Safety Support Element)의 개발 프로세스 목표/산출물

SSE의 개발 프로세스 목표달성/산출물 단계는 형식인증(항공기 설계가 해당 기종의 감항인증기준을 충족하여 비행안전에 적합하다는 정부의 인증)을 받으려는 컴퓨터시스템/소프트웨어 개발 및 검증&확인에서 요구되는 프로세스 및 산출물 작성을 위한 목표를 정의하고 있다. SSE 프로세스 및 산출물 작성을 위한 목표는 안전지원 소프트웨어 요소(SSSE; Safety Support Software Element) 프로세스와 시스템 처리 아키텍처(SPA; System Processing Architecture) 프로세스로 Table 2와 같이 구분된다.

SSSE 프로세스는 146개 달성 목표를 SPA 프로세스는 41개의 달성 목표를 제시하여 감항인증 심사 시 점검표로 활용 가능하도록 세부적인 내용을 포함하고 있다. 예들 들면 시스템 요구도-소프트웨어 요구도-설계-소스코드-시험 케이스에 대한 양방향 추적성, 형상관리, 소프트웨어 구조적 커버리지 확보, 고장모드 영향성 및 치명성 분석(FMECA; Failure Modes Effects Criticality Analysis) 및 고장모드 영향성 시험(FMET; Failure Modes & Effects Test) 포함여부 등을 포함한다.

Table 2 SSE Development Process/Product Attribute

SSSE(Safety Support Software Element) Process		
#	Group	Check #
1	Development Foundation	11
2	Basic Development	40
3	Interface Control	3
4	Avoiding Unsafe Attributes	12
5	Failure Detection & Accommodation	9
6	Configuration Management	15
7	Traceability	11
8	Software V&V	14
9	System V&V	10
10	Building & Loading	21
SPA(System Processing Architecture) Process		
1	SPA Level Development Foundation	6
2	SPA Level Basic Development	13
3	SPA Level Interface Control	7
4	SPA Level Failure Detection & Accommodation	2
5	SPA Level System V&V	9
6	System Flight Clearance	4

2.1.3 DO-178C

DO-178C는 미 연방항공청에서 채택한 민간항공기에 사용되는 시스템/장비의 소프트웨어 개발을 위한 인증 관점에서의 지침 문서이다.

이 문서는 미 항공통신 기술위원회에 의하여 1980년 제정되었고, 최신 개발기술 등을 반영하기 위하여 3차례의 개정이 있었다[5-6].

DO-178C에서는 Table 3과 같이 결함 수준(또는 심각도)에 따라 소프트웨어를 5개 수준(A~E)으로 분류하고, 수준에 따라 소프트웨어 수명주기 프로세스에서 달성되어야 하는 목표를 제시하고 있다.

Table 3 DO-178C Software Level

SW Level	Failure Level (Severity)	DO-178C Objective # (satisfied with independence)
A	Catastrophic	71(30)
B	Hazardous	69(18)
C	Major	62(5)
D	Minor	26(2)
E	No Effect	0(0)

DO-178C 부록A는 개발하는 소프트웨어 수준에 따른 목표와 객관적 검토를 위하여 3자 검증(독립적 검토)이 필요한 목표를 제시하고 있다. 예를 들면 DO-178C 수준(등급) A에 해당하는 소프트웨어의 경우 71개 목표를 달성하여야 하며 71개 목표 중 30개 목표는 3자 검증(독립적 검토)을 통하여 목표를 달성하여야 한다. DO-178C 12장(기타 고려사항)은 비개발 소프트웨어(상용구매, 기 개발)에 대한 입증 방법을 설명하고 있다.

DO-178C 준수 여부는 미 연방항공청에서 발간한 지시서(ORDER 8110.49/Software Approval Guidelines, ORDER 8110.37E/Designated Engineering Representative Handbook)에 따라 미 연방항공청으로부터 자격을 부여받은 위임된 기술 전문가가 주요 개발 프로세스에 참여 및 검토를 통하여 판단한다[7-8].

2.2 항공 소프트웨어 감항인증기준 상호관계 분석

2.2.1 MIL-HDBK-516C 15장과 AC-17-01 관계분석

AC-17-01에 의하면 컴퓨터시스템 및 소프트웨어 개발 프로세스는 5단계로 분류되며 각 단계에서 관련되는 MIL-HDBK-516C 15장 기준을 명시하고 있다.

AC-17-01 각 단계와 각 단계에서 명시된 MIL-HDBK-516C 15장 기준을 비교하면 AC-17-01의 특정 단계를 만족할 경우 MIL-HDBK-516C 15장에서 충족 가능한 기준을 식별할 수 있다. 본 논문에서는 AC-17-01 단계와 각 단계에서 명시된 MIL-HDBK-516C 15장 기준간 정합 비율(MR; Matching Ratio)을 식(1)과 같이 정의한다. N_{516C}는 MIL-HDBK-516C 15장 절 전체 기준 수, N_{Ref}는 AC-17-01에서 명시된 MIL-HDBK-516C 15장 기준 수를 나타낸다.

$$M_R(\%) = (\frac{\sum N_{Ref}}{\sum N_{516C}}) \times 100 \qquad (1)$$

Table 4는 AC-17-01의 컴퓨터시스템 및 소프트웨어 개발 프로세스 5단계 중 2개 단계(SCF 식별, SSE의 개발 프로세스 목표/산출물)에서 MIL-HDBK-516C 15장 기준을 명시한 비율(M_R)을 분석한 결과를 나타낸다.

Table 4 Comparison Between AC-17-01 & MIL-STD-516C

AC-17-01 Section	Refer to MIL-HDBK-516C		Results of Comparison
	Section	Criteria	
Safety Critical Function(SCF) Identification	15.1 SPA(System processing architecture)	15.1.1, 15.1.3~11	N_{REF} = 10 N_{516C} = 12 M_R = 83%
	15.2 Design and functional integration of SPA elements.	15.2.1~3, 15.2.5~8,	N_{REF} = 7 N_{516C} = 8 M_R = 88%
	15.3 Processing hardware/electronics	15.3.1~3	N_{REF} = 3 N_{516C} = 4 M_R = 75%
	15.4 Software development processes	15.4.1~3	N_{REF} = 3 N_{516C} = 3 M_R = 100%
	15.5 Software architecture and design	15.5.2~4, 15.5.6~8, 15.5.10	N_{REF} = 7 N_{516C} = 10 M_R = 70%
	15.6 Software qualification and installation	15.6.1~3	N_{REF} = 3 N_{516C} = 5 M_R = 60%
Computer System & SW Development Process and Product Attribute	15.1 SPA(System processing architecture)	15.1.1, 15.1.4, 15.1.7~8	N_{REF} = 4 N_{516C}= 12 M_R = 33%
	15.2 Design and functional integration of SPA elements.	15.2.3~5	N_{REF} = 3 N_{516C}= 8 M_R = 38%
	15.4 Software development processes	15.4.1~3	N_{REF} = 3 N_{516C} = 3 M_R = 100%
	15.5 Software architecture and design	15.5.4, 15.5.8, 15.5.10	N_{REF} = 3 N_{516C} = 10 M_R = 30%
	15.6 Software qualification and installation	15.6.1~5	N_{REF} = 5 N_{516C} = 5 M_R = 100%

Table 4에 따르면 AC-17-01의 SCF 식별 단계에서 MIL-HDBK-516C 15장 기준을 명시한 비율이 15.1절 83%, 15.2절 88%, 15.3절 75%, 15.4절 100%, 15.5절 70% 및 15.6절 60%이다. 이는 MIL-HDBK-516C 15장 대부분의 기준이 SCF를 기반으로 설정되어 있음을 알 수 있다. AC-17-01의

SSE의 개발 프로세스 목표 달성/산출물 단계에서 MIL-HDBK-516C 15장 기준을 명시한 비율이 15.1절 33%, 15.2절 38%, 15.3절 0%, 15.4절 100%, 15.5절 30% 및 15.6절 100%이다. 이는 MIL-HDBK-516C 15장 중 소프트웨어 관련 기준(15.4절~15.6절)과 연관됨을 알 수 있으며 15.5절 중 AC-17-01에서 명시되지 않은 기준은 소프트웨어 아키텍처(15.5.1, 15.5.2, 15.5.3), 결함 관리 설계(15.5.5, 15.5.6, 15.5.7) 및 자원 용량(15.5.9)이다. 이는 AC-17-01에서 직접 언급하고 있지는 않지만 소프트웨어 요구도 또는 설계에 반영되어야 할 사항이다.

AC-17-01에서 명시된 MIL-STD-516C 15장 기준을 분석한 결과 SCF를 식별하고 SSE의 개발 프로세스 목표/산출물을 달성하는 경우 소프트웨어 수준에서 요구하는 기준이 대부분 충족 가능한 것을 알 수 있다.

2.2.2 MIL-HDBK-516C 15장과 DO-178C 관계분석

MIL-HDBK-516C 15장은 항공기(체계)에 대한 인증기준이며, DO-178C는 항공 시스템/장비 소프트웨어 인증 지침으로 그 목적과 범위가 달라서 비교 분석이 쉽지가 않다. 미군은 MIL-HDBK-516C 15장 기준 개발 시 모든 사항을 기준에 포함할 수 없어 세부적인 사항은 참조문서로 명시하고 있으며 DO-178C를 참조문서로 명시된 기준이 존재한다. MIL-HDBK-516C 15장에서 DO-178C를 명시한 기준을 식별하고 그 비율을 비교하면, DO-178C를 만족할 경우 MIL-HDBK-516C 15장에서 충족 가능한 기준을 식별할 수 있다.

Table 5는 식(1)에 따라 N_{516C}는 MIL-HDBK-516C 15장 절 전체 기준 수, N_{Ref}는 MIL-HDBK-516C 15장절에 있는 기준 중에서 참조문서로 DO-178C를 명시하고 있는 기준을 M_R로 환산한 결과를 정리한 것이다.

MIL-HDBK-516C 15장에서 DO-178C를 참조문서로 명시하고 있는 비율은 15.1절 33%, 15.2절 50%, 15.3절 0%, 15.4절 100%, 15.5절 70%, 15.6절 100%이다. 이는 DO-178C가 MIL-HDBK-516C 15장 중 소프트웨어 관련 기준(15.4~15.6)과 연관됨을 알 수 있다.

MIL-HDBK-516C 15.5절 중 DO-178C를 참조문서로 명시하지 않는 15.5.4, 15.5.5 및 15.5.7 기준은 DO-178C를 직접 명시하고 있지는 않지만 소프트웨어 설계에 반영하여야 되는 고장탐지, 고장관리 및 재시작/리셋 등을 포함한다. 따라서 DO-178C을 적용할 경우 15.4절~15.6절 기준이 충족 가능하다[9].

Table 5 Comparison Between MIL-STD-516C & DO-178C

MIL-HDBK-516C		DO-178C Corresponding Section	Results of Comparison
Section	Criteria (Ref. DO-178C)		
15.1 SPA(System processing architecture)	15.1.2, 15.1.4 15.1.7, 15.1.8	2.1; 2.3; 2.3.2; 2.3.3; 2.3.4; 2.4.1; 2.5.5.b; 11.1.b	N_{REF} = 4 N_{516C}= 12 M_R = 33%
15.2 Design and functional integration of SPA elements.	15.2.1, 15.2.4 15.2.5, 15.2.7	2.2.2.d; 4.5 Note 2; 6.3.4.d; 6.4.4.d; 6.4.4.2.c; 7.1.c; 7.2.3; 8.3.d; 11.1; 11.8; 11.14; 11.17; 11.20.k; 12.1.1.c; 12.2	N_{REF} = 4 N_{516C}= 8 M_R = 50%
15.3 Processing hardware/ electronics	N/A	N/A	N_{REF} = 0 N_{516C}= 4 M_R = 0%
15.4 Software development processes	15.4.1, 15.4.2 15.4.3	All Section	N_{REF} = 3 N_{516C}= 3 M_R = 100%
15.5 Software architecture and design	15.5.1, 15.5.2 15.5.3, 15.5.6 15.5.8, 15.5.9 15.5.10		N_{REF} = 7 N_{516C}= 10 M_R = 70%
15.6 Software qualification and installation	15.6.1, 15.6.2 15.6.3, 15.6.4 15.6.5		N_{REF} = 5 N_{516C}= 5 M_R = 100%

2.3 제안하는 소프트웨어 개발 프로세스

기존의 군용항공기 소프트웨어 개발 프로세스는 비행안전을 고려하지 않고 방위사업청에서 발간한 무기체계 소프트웨어 개발 및 관리 매뉴얼에 따라 개발하여 항공 안전을 고려한 S/W 개발 프로세스가 없었다[10].

군용항공기 탑재 소프트웨어를 개발하는 기관이 기존의 소프트웨어 개발 프로세스를 적용할 경우, 해당 소프트웨어가 SCF와 관련 여부에 상관없이 동일한 소프트웨어 개발 프로세스를 적용하여야 한다. 제안하는 소프트웨어 개발 프로세스를 적용할 경우 SCF 수행여부 및 식별된 소프트웨어 수준(등급)에 따라 소프트웨어 개발 목표를 다르게 수립하여 개발 일정 및 비용을 절약하면서 비행 안전을 확보할 수 있다.

제안하는 소프트웨어 개발 프로세스는 본 논문 2.1 및 2.2에서 분석된 바와 같이 MIL-HDBK-516C 15장을 토대로 AC-17-01 및 DO-178C 상호관계 분석 결과를 바탕으로 새로운 프로세스를 제안한다.

새로운 소프트웨어 개발 프로세스 제안에 앞서 MIL-HDBK-516C 15장 42개 기준을 단순하게 표현하고 기준 간 관계 정의를 위하여 기준을 그룹화하고 기준 간 절차 정의가 필요하다. 본 논문 2.1.1절에 따라 MIL-HDBK-516C 15장을 컴퓨터시스템(15.1절~15.2절),

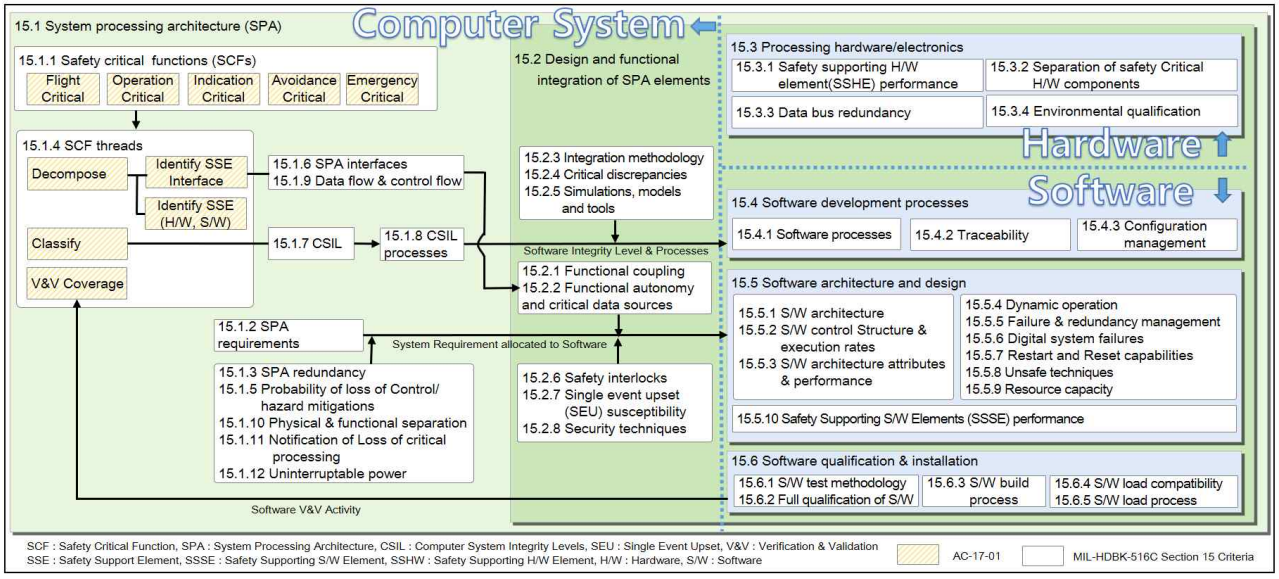

Fig. 1 MIL-HDBK-516C Section 15 Criteria(Included In AC-17-01) Diagram

하드웨어(15.3절) 그리고 소프트웨어(15.4절~15.6절)로 구분하였으며 본 논문 2.1.2절에 따라 MIL-HDBK-516C 기준에 포함되지 않은 AC-17-01 내용을 추가하여 Fig. 1과 같이 도식화하였다.

Table 6 SCF Category

Category	SCF Example
Flight Critical	· Flight Control(Level III Flying Qualities, Air Data Sensing, Pitot Heating Autopilot) · Supply and Control of Critical Utilities (Electrical, Hydraulic, Thermal Management) · Automated Landing/Takeoff/Terrain Following · Thrust/Propulsion Control · In-flight Restart/Reset · Ground Steering · Landing Gear Extension/Control
Operation Critical	· Ground Deceleration(Differential Braking Arresting Hook, Thrust Reversing) · Navigational Control/Auto-Pilot Operation · Fuel Tank Pressurization, Temp. Control · Fuel Feed to Propulsion System · Mid-Air Refueling/Boom Control · Anti-Icing(Control surfaces, Engine/Inlet) · Communication Link Control [UAS] · Crew Visibility/Canopy Defog · Life Support (Crew O_2 Supply/Pressurization) · Pilot Altitude and G protection · Operation for Armament/Counter Measures
Indication Critical	· Primary Flight References(Altitude, Airspeed, Attitude), Heading · Fuel Quantity · Engine Health Monitoring · Caution & Warnings · Manual Terrain Following · Communication Link Status [UAS]
Avoidance Critical	· Bleed Air Leak Detection · Ice Detection · Ground/Air Collision Avoidance System · Emissions Control(Toxins, Lasers, RF Energy) · Bird Strike/Lightning Protections · Turbulence Detection [UAS]
Emergency Critical	· Fire Detection · Crew Ejection · Fire/Explosion Suppression · Fuel Shutoff · Flight Termination [UAS]

SCF 기준(15.1.1)은 본 논문 2.1.2절에 따라 SCF를 비행필수, 운용필수, 지시필수, 회피필수, 비상필수로 구분하였으며 SCF 예는 Table 6과 같다. SCFTA 기준(15.1.4)은 15.1.1 기준에서 식별된 SCF를 기반으로 본 논문 2.1.2절에 따라 SCFTA 단계를 분해, 분류, 검증&확인 커버리지로 구분하였다. 분해 단계에서 식별된 SCF 관련 인터페이스는 15.1.6, 15.1.9, 15.2.1, 15.2.2 기준과 연계하여 기능적 및 물리적 흐름을 명확히 정의하고 소프트웨어 아키텍처 및 설계에 반영되어야 한다. 분류 단계에서 식별된 소프트웨어 수준(CSIL 또는 DAL) 및 프로세스(15.1.7~8)는 소프트웨어 개발 프로세스(15.4)로 연계된다. 검증&확인 커버리지 단계는 소프트웨어 인증/설치(15.6) 과정에서 수행된 소프트웨어 검증&확인 활동으로 검증&확인 커버리지 만족 여부 판단한다. 그리고 시스템 수준의 요구도(15.1.2, 15.1.3, 15.1.5, 15.1.10~12, 15.2.6~8)는 소프트웨어 아키텍처 및 설계에 반영된다.

제안하는 소프트웨어 개발 프로세스는 Fig. 2와 같이 MIL-HDBK-516C 15장 장절의 수준별 구분(컴퓨터시스템, 하드웨어, 소프트웨어)에 따라 시스템 개발(수명주기) 프로세스와 소프트웨어 개발(수명주기) 프로세스로 구분한다. 그리고 시스템 개발(수명주기) 프로세스에서는 Fig. 1에서 컴퓨터시스템 수준에서 그룹화한 것과 같이 SCF 식별 후 SCFTA를 통하여 SSE 여부

및 소프트웨어 수준(CSIL 또는 DAL)을 할당한다. 소프트웨어 개발(수명주기) 프로세스에서는 소프트웨어를 개발(신규, 개조) 또는 비-개발(상용구매, 재사용)로 분류하여 전체 소프트웨어를 식별한다. 식별된 소프트웨어의 경우 시스템에서 할당된 소프트웨어 요구도 및 수준(CSIL 또는 DAL)에 따른 소프트웨어 개발 프로세스 목표와 산출물 작성방안을 선정되어야 한다.

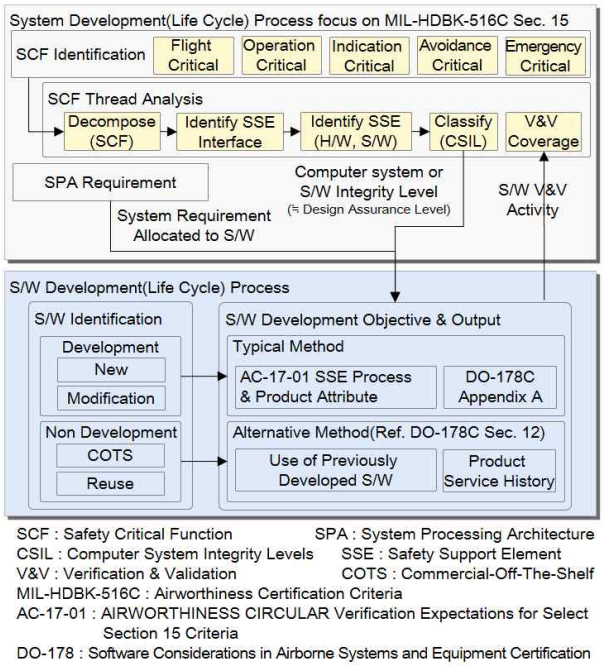

Fig. 2 The Proposed S/W Development Process Based On MIL-HDBK-516C Section 15 criteria

MIL-HDBK-516C 15장, AC-17-01 및 DO-178C 관계분석 결과(본 논문 2.2절)에 따라 소프트웨어 개발 프로세스 목표와 산출물은 AC-17-01의 SSE의 프로세스 목표/산출물(Table 2) 또는 DO-178C 부록A를 따르는 경우 소프트웨어와 관련된 MIL-HDBK-516C 15장 기준(15.4절~15.6절)이 충족 가능하다.

비 개발(상용구매 및 재사용) 소프트웨어를 사용하는 경우, 소프트웨어 개발 목표와 산출물은 DO-178C 12장을 적용하여 해당 소프트웨어에 대한 평가 및 서비스 이력 등을 통하여 비 개발 소프트웨어에 대한 적용 가능 여부에 대한 검토가 요구된다.

2.4 제안하는 S/W 개발 프로세스 적용 사례

'19년도에 수행된 항공기(체계) 연구개발사업의 소프트웨어 감항인증기준은 MIL-HDBK-516C 15장이 적용되었으며 제안된 소프트웨어 개발 프로세스에 기반하여 시범적용을 하였다.

SCF는 시스템 안전 표준서(MIL-STD-882E)를 기반으로 항공기 기능 중 재난적 및 치명적 심각도에 해당하는 58종이 식별되었다. 식별된 SCF를 기반으로 SCFTA가 수행되었으며 기능적 경로에 포함되는 소프트웨어는 SSE로 식별되었다. SSE는 Table 8과 같이 SCF 식별 근거인 기능적 위험도 분석보고서(FHA), 시스템-세부시스템-소프트웨어 요구도, 소스 코드, 인터페이스 및 시험 결과에 대한 장절을 명시하여 안전필수기능, 요구도, 시험결과 간의 추적성이 확인되었다.

Table 8 SCF Traceability Example

SCF		Requirement			Code	ICD	Test				
SCF ID	FHA	PIDS	ORS/ FRS	SRS			STR	IT	AT	GT	FT
SCF_X	X.X.X	X.X.X	X.X.X	X.X.X	X.c	X.X	X.X	X.X	X.X	X.X	X.X

SCF ID : Safety Critical Function Identification Number
FHA : Functional Hazard Analysis
PIDS : Prime Item Development Specification
ORS : Operational Requirement Specification for OO System
FRS : Functional Requirement Specification for OO System
SRS : Software Requirement Specification, Code : Software Source Code
ICD : Interface Control Document, STR: Software Test Report
IT: Integration Test (LAB), AT: Acceptance Test (LAB)
GT: Ground Test (Aircraft Level) FT: Flight Test (Aircraft Level)

또한 SCF를 지원하는 소프트웨어에 대한 개발/검증 프로세스 목표 달성 여부를 확인하기 위하여 현장 방문 심사를 수행하였다. 현장 방문 심사 전 심사팀이 AC-17-01을 기반으로 SSE의 개발 프로세스 목표/산출물에 대한 187개 점검표(Table 2 참조)를 작성하여 항공기 제작사에 제공하였으며, 이 점검표를 통해 소프트웨어 개발기관 및 항공기 제작사에서 자체점검을 할 수 있도록 하였다.

현장 방문 심사 시 DO-178C를 적용한 소프트웨어가 확인되어 DO-178C 산출물을 인정하였으며 심사 과정 중 확인된 주요 보완사항은 다음과 같다.

소프트웨어 개발계획서(SDP)에 안전필수기능을 수행하는 소프트웨어 여부(수준 포함) 명시, 도구 식별(개발도구 또는 검증도구) 및 도구 분류(개발, 상용)가 필요하였다. 소프트웨어 요구도 명세서(SRS)/소프트웨어 설계 기술서(SDD)에 자체진단시험(BIT)에 대한 수

행시간, 전원 상태/프레임 오버런에 대한 모니터링 요구도 및 설계 반영이 필요하였다. 그리고 장비 간 통신 인터페이스 결함에 따른 고장모드 영향성 시험(FMET) 수행 및 소프트웨어시험결과서(STR)에 시험 형상 정의가 필요한 것으로 확인되었다. 이 보완 요구사항은 기존 소프트웨어 개발 프로세스(방위사업청 무기체계 소프트웨어 개발 및 관리 매뉴얼)에서는 검토 항목으로 포함되지 않은 사항으로 제안된 S/W 개발 시범적용을 통하여 최초 확인하였다.

또한 제안된 소프트웨어 개발 프로세스를 안전과 관련되지 않은 소프트웨어에 적용 할 경우, 개발업체는 방위사업청 무기체계 소프트웨어 개발 및 관리 매뉴얼 산출물 외에 추가적인 산출물을 작성하여야 됨에 따라 개발 비용/일정에 영향이 있을 수 있음을 알 수 있었다. 이러한 미비한 사항을 보완하기 위해서는 안전지원 소프트웨어와 비-안전지원 소프트웨어에 대한 개발 프로세스를 이원화하여 수립 할 필요성을 확인하였다.

3. 결 론

본 논문에서는 군용 항공기 소프트웨어 비행안전성 확보를 위하여 국내 및 선진국에서 적용하고 있는 감항인증기준인 MIL-HDBK-516C 15장, AC-17-01 및 DO-178C를 비교분석하여 소프트웨어 개발 방안을 제시하였으며 이를 통해 도출한 사항은 아래와 같다.

MIL-HDBK-516C 15장과 AC-17-01을 분석한 결과 SCF 식별 및 SCFTA를 통하여 SCF를 수행하는 소프트웨어(SSE)에 대한 개발 프로세스 목표/산출물을 달성하는 경우 MIL-HDBK-516C 15장 중 소프트웨어 수준에 해당하는 15.4절~6절 기준이 충족 가능함이 확인되었다.

MIL-HDBK-516C 15장과 DO-178C를 분석한 결과 DO-178C를 따르는 경우 MIL-HDBK-516C 15장 중 소프트웨어 수준에 해당하는 15.4절~6절 기준이 충족 가능함이 확인되었다.

따라서, SSE로 식별된 소프트웨어에 적용되는 개발 프로세스 목표/산출물은 AC-17-01 SSE 개발 프로세스 목표/산출물 또는 DO-178C 부록A에 따라야함을 알 수 있다.

개조/상용구매/재사용 소프트웨어의 경우, DO-178C 12장에 따른 서비스 이력 및 이전 개발 소프트웨어 재사용 방안이 적용 가능하다.

제안된 방안에 대한 시범 적용결과 일부 보완사항이 식별되었지만 식별된 미비한 사항은 지속적인 보완활동과 미비점 분석을 수행할 예정이며, 정부 차원에서 항공기 탑재 소프트웨어 개발 및 감항인증 방안을 규정하고 이후 항공기 연구 개발 사업에 적용할 경우 항공기 수출 경쟁력 확보에 도움이 될 것으로 판단된다.

References

[1] DAPA, “Military Aircraft Flight Safety Certification Regulation”, DAPA Instruction, Number 561, Nov. 2019.

[2] DAPA, “Military Aircraft Standard Airworthiness Certification Criteria”, DAPA Notice, 2020-3, Apr. 2020.

[3] US Department of Defense, “AIRWORTHINESS CERTIFICATION CRITERIA", *MIL-HDBK-516C*, Dec. 2014.

[4] US Air Force, “AIRWORTHINESS CIRCULAR : Verification Expectations for Section 15 Criteria", *AC-17-01*, Mar. 2017.

[5] RTCA, “Software Consideration in Airborne Systems and Equipment Certification”, *RTCA DO-178C*, Nov. 2011.

[6] Youn Won-Keun, Yi Baeck-Jun, "Development Tread of Software Certification Technology for the Safety of Avionic system", *Aerospace Industry Technology Trend*, pp 189-196, Nov. 2013.

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

[8] FAA, "Designated Engineering Representative[DER] Handbook", *FAA ORDER, 8110.37E*, Mar. 2011.

[9] Jin Gu Heo, Min Sung Kim, Man Tae Kim, Yong Ho Moon, “The Study on Airworthiness Certification Process on Military Airborne Safety Critical Software based on DO-178”, J*ournal of Aerospace System Engineering*, Vol.13, No.1, pp. 62-68, Feb. 2019

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