항공기 인증 과정에서 소프트웨어의 승인 프로세스

한 상 호 *

디지털 하드웨어가 값이 싸다는 것과 그 외형적 크기도 작아지고 있으며 소모 전력도 적다는 경향 때문에 항공에서 디지털 시스템의 사용이 현저하게 증가하게 되었다. 일부에서는 디지털 실용화가 아날로그 기반의 설계를 대체하기까지 하고 있으며 전연 새로운 개념이 도입되고 있는 데 이는 모두 디지털 시스템 덕분이다. 대부분의 경우 항공에서 디지털 시스템은 안전에 치명적인 특성을 가지며 해당 소프트웨어의 오류로 항공기의 지속적인 비행과 착륙을 할 수 없는 고장을 유발할 수 있다. 이러한 이유로 항공기에 적용되는 소프트웨어의 인증이 대두되는 것이다. 이 글에서는 향후 우리나라에서도 전개될 소프트웨어의 인증에 대비하여 인증의 기준으로 적용되고 있는 RTCA DO-178B의 내용을 살펴보고 전형적인 항공기 또는 TSOA 인증과정에서의 소프트웨어의 승인 프로세스를 살펴보았다.

목차

* 한국항공우주연구원 항공우주안전인증센터 항공인증그룹(선임연구원)

I. 소프트웨어 인증의 대두

현대의 상용 항공기 기술은 상당수의 운용 및 서비스 분야에서 디지털 시스템을 채용하고 있다. 디지털 시스템의 운용 사례로서 대표적으로 자동조종, FADEC, EFIS등이 있다. 또한 이 디지털 시스템에 대한 의존도는 상당 부분 일반 항공에도 적용이 되고 있다. 대부분의 경우 항공에서 디지털 시스템은 안전에 치명적이다(safety critical). 여기서 안전에 치명적이라 함은 해당 소프트웨어의 오류로 항공기의 지속적인 비행과 착륙을 할 수 없는 고장을 유발할 수 있음을 말한다.

복잡한 디지털 시스템은 대개 소프트웨어 집약적이므로 많은 항공 시스템의 정확한 운용은 관련 소프트웨어의 정확한 작동에 달려 있다. 상용 수송항공기의 비행 치명 시스템의 신뢰도 요건은 항공기의 손실을 가져오는 고장이 비행시간당 1×10^{-9}이나 이것은 시스템 요건이지 소프트웨어의 요건은 아니며 소프트웨어의 요건은 하드웨어 구성부품이 완전하지 않으므로 이 요건을 훨씬 초과한 안전도를 가져야 한다. 또한 디지털 항공 시스템은 신뢰성 요건이 매우 높기 때문에 개발에 있어 많은 복합적인 기술적 문제가 도사리고 있다.

디지털 하드웨어가 값이 싸다는 것과 그 외형적 크기도 작아지고 있으며 소모 전력도 적다는 경향 때문에 항공에서 디지털 시스템의 사용이 현저하게 증가하게 되었다. 일부에서는 디지털 실용화가 아날로그 기반의 설계를 대체하기까지 하고 있으며 전연 새로운 개념이 도입되고 있는 데 이는 모두 디지털 시스템 덕분이다. 자동조종의 경우 종래에는 자동조종에 아날로그 시스템을 채용하였으나 지금은 디지털로 바뀌고 있으며 그 결과 더 많은 기능성과 유연성을 가지게 되었다. 전혀 새로운 개념의 도입 사례로서 전자동디지털식 엔진제어장치(FADEC : Full Authority Digital Engine Control, 페이덱이라고 읽음)가 있다. FADEC은 정교한 장치로 종래에는 할 수 없었던 것을 디지털 시스템을 채용함으로서 대형 항공기 엔진을 운영하고 성능을 감시할 수 있게 되었다. FADEC의 장점을 살펴보면 다음과 같다.

- 연료 효율의 향상(연료절감)
- 작동 한계값을 초과하지 않도록 엔진을 보호
- 다중 채널을 사용하는 대체경로 활용으로 고장에 대한 안전성 증대
- 목표하는 추력을 정확하게 낼 수 있으므로 추력 설정에 특별한 주의가 필요하지 않음
- FADEC 프로그램을 수정하는 것으로 하나의 엔진에 대하여 추력 범위를 다양하게 지정할 수 있음
- 엔진을 반자동으로 시동시킬 수 있음
- 항공기의 Fly-by-Wire 제어시스템과 통합이 용이함

- 엔진의 작동상태, 고장여부, 수명 등을 모니터링 할 수 있음 등

소프트웨어의 사용으로 기능이 보강된 사례는 조종실의 자동화에도 미치고 있으며 상당수의 비행 정보의 표시에 컴퓨터 시스템을 이용하므로 EFIS (Electronic Flight Information Systems)로 대표되는 유리조종석(glass cockpit)이란 용어가 나오게 되기에 이르렀다.

여기서 항공용 소프트웨어에 대한 종래의 인식을 살펴보면 항공 시스템에서 처리장치의 수, 정확한 의사소통 구조 그리고 소프트웨어의 사용분야를 확인해 내기가 쉽지 않으며 프로세서(processor)라 하는 것은 전문화된 전자장치를 사용함으로서 그 구성 내역을 규명해 내기는 용이하지 않다는 점, 소프트웨어는 소프트웨어라기보다는 ROM속에 있는 것으로 펌웨어로 잘못 알고 있다는 점, 디지털 시스템은 대개 비안전관련 기능에 사용되므로 중요하지 않다고 생각한다는 점 그리고 항공에 사용되는 디지털 시스템의 상당수 세부 사항은 특정회사가 독점적하고 있으며 만들기기 쉽지 않다고 하는 점 등을 들 수 있으며 이러한 이유로 소프트웨어의 인증에 다소 거부감이 있는 것은 사실이다.

하여튼 이러한 사유가 있음에도 불구하고 현재 소프트웨어를 이용한 안전-치명(safety-critical) 디지털 시스템이 항공에 상당수 적용되고 있으며 이러한 시스템은 대부분의 경우 아주 복잡하지만 이러한 이유로 항공기에 적용되는 소프트웨어의 인증이 대두되는 것이다.

II. 항공전자장비에 대한 인증의 형태

가. 증명 일반

항공전자장비에 대한 인증의 형태는 크게 네 종류로 구분할 수 있으며 증명의 내역별로 정리하면 표 1 과 같다.

위와 같은 각 증명의 형태별 인증의 내역은 감항기준에 대한 합치성과 설계적합성의 검증으로 이루어지는 데 공통적으로 다음과 같은 절차로 진행이 되고 있다.

- 감항기준 합치성 : 항공기 기술기준(Korean Airworthiness Standard, KAS)
- 설계 적합성 입증 : 분석, 시험, 유사성 비교 및 과거의 경험 자료 등
- 소프트웨어의 인증 : RTCA DO-178B의 요건에 입각한 증명
- 환경 적합성 인증 : RTCA DO-160E에 의거한 시험의 실시
- 안전성 평가(SSA, System Safety Assessment) : SAE ARP 4761 등에 의거한 안평평가 요구사항 이행

< 표 1> 항공전자장비에 대한 인증의 형태

증명의 구분	대상	평가 내역	승인 방식	비고
형식증명 (TC/STC)	신규 설계/개발 항공기, 엔진, 프로펠러에 장착되는 모든 장비품	해당 감항기술기준에 의거한 설계 적합성 평가	설계승인	항공전자장비에 대한 개별적인 인증서는 발급되지 않음
기술표준품 형식승인 (TSOA)	표준 장비품 및 부품으로 지정된 품목	품목별 최소성능표준 (MPS)에 의거한 설계 적합성 평가	설계승인 및 생산승인	항공전자 90종 (FAA TSO 총 126종)
부품제작자 증명 (PMA)	교체 또는 개조용으로 장착되는 부품 (TSO 이외의 항공전자부품)	해당 감항기술기준에 의거한 설계 적합성 및 동일성 (Identicality) 평가	설계승인 및 생산승인	상당수

- 비행시험 : 비행시험을 통해 입증이 되어야 하는 사항의 경우 비행 시험을 실시한다.

나. TSO

TSO란 폭증하는 부품생산에 대한 검사 누락을 방지하고 감항당국의 권한을 분권화하여 생산자에게 책임을 위임하여 스스로 품질을 보증하도록 하는 제도로서 부품에 대하여 최소한의 성능 표준 (MPS : minimum performance standard)을 정하여 운용하고 있다. TSOA 승인의 내역은 다음과 같다.

- 설계승인과 생산승인을 동시에 받음 (dual approval)
- 신청자는 제품에 대한 시장성과 인증성을 검토한 후 신청하게 됨
- 절차
  - 개발 제품에 대한 합치성인정서 (Statement of Conformance)
  - 관련 기술자료
  - 품질관리 시스템에 관한 자료
  - 기타 감항당국이 요구하는 자료
- 승인된 제품에 대해서는 TSO 번호 자체 각인 (예 : TSO-C129a)
- 기술기준 : RTCA, SAE 기술문서

다. PMA

형식증명 받은 항공기에 장착되는 교환용 부품 또는 수리개조 부품의 생산 승인제도로서 TSO가 아닌 장비를 대상으로 하고 있다. 예로서 GPS Receiver, Engine Tachometer 등이 있다. PMA 승인의 내역은 다음과 같다.

- 설계승인 및 생산승인 동시에 받음 (dual approval)
- 제외 사항
  - 생산증명 제품
  - BAA 또는 BASA가 체결된 외국에서 생산된 품목
  - 항공기 소유자가 자체 사용을 목적으로 제작한 제품
  - 표준부품(Standard Parts) : 이것은 국가 산업규격에 의거 생산해야 함
  - TSOA 지정품
  - 특수 공정 (표면처리, 용접 등)만 소요되는 품목
- 절차
  - 승인 받고자 하는 제품에 대한 기술자료 및 적합성 입증자료
  - 복제생산능력에 관한 자료
  - 제조검사 시스템(FIS : Fabrication Inspection System)에 관한 자료

III. 소프트웨어의 인증기준

가. 소프트웨어 증명 표준

현재까지 국제 사회에서 개발 통용되고 있는 소프트웨어 증명 표준은 아래 표 2 와 같이 평가 표준, 개발 표준, 보증 표준으로 3종류로 볼 수 있으며 크게 군사용 기술기준, 민간단체 기술기준, ISO 기술기준 그리고 항공전문용 기술기준으로 나눌 수 있다.

< 표 2> 세가지 형태의 소프트웨어 표준

구분	종류	내용	장점
평가 표준	· CMM(Capability Maturity Model, 능력성숙도 모델) · ISO 9000-3 · AS9006	· 조직이 소프트웨어를 생산하는 능력 및 성숙도와 적절성과 품질을 평가함	· 획득 프로세스에서 중요한 여과기능에 대한 접근방법을 제공 · 개발자가 좋고 나쁜 프로세스를 알도록 하여 획득 프로세스를 지원함
개발 표준	· MIL-STD-2167/ 2167A/ 2168/498 · IEC 12207(및 FAA-STD-026)	· 순서적이고 되풀이 되는 소프트웨어 개발 프로세스가 되도록 지침을 제공함	· 개발 프로세스 수행과정에서 생성되는 데이터를 정의 함 · 유자를 지원함
보증 표준	· DO-178B · DO-278 · IEC 61508	· 소프트웨어 개발 프로젝트에서 확실한 특성이 나타나도록 하는 수단을 제공함 · 방법 보다는 대상을 규정함	· 안전과 규정이 엮어지도록 함 · 측정 기준을 제공함 · 방법이아니라 대상을 정의함

나. DO-178B 개요

항공기 인증과 관련하여 항공전자장비를 비롯한 항공기 시스템에 활용되는 소프트웨어의 인증을 다루는 문서로는 RTCA에서 발행한 DO-178B(제목: Software Considerations in Airborne Systems and Equipment Certification, 항공 시스템 및 장비의 인증에서의 소프트웨어 고려사항)가 있으며 이는 FAA에서 합치성 증명의 승인할 수 있는 지침서로 통용되고 있다.

DO-178B는 항공 전자 개발자, 설치자 및 사용자가 항공 장비를 마이크로컴퓨터 기술을 이용하여 설계할 때 소프트웨어 고려사항을 설정하기 위해 항공전자 산업계에서 개발하였다. 이 문서는 마이크로컴퓨터 시스템에 사용될 확인, 검증, 문서화 및 소프트웨어 형상관리와 품질보증 원칙을 기술하고 있다. 특히, 이 문서는 소프트웨어 툴의 인증, 이전에 개발된 소프트웨어의 재이용, 사용자가 개조할 수 있는 소프트웨어, 항공기에서의 자료입력, 공식적인 방법, 다중 버전의 유사 소프트웨어 및 제품 서비스의 내력에 대한 지침을 제시한다. DO-178B는 중재의 시기에 이루어 졌던 디지털 프로세스의 적용에서 상당한 진보를 고려한 1985년 발행된 DO-178A의 개정판이다.

FAA 권고 회람 AC 20-115B는 DO-178B를 모든 새로운 항공 소프트웨어를 인증하는 인정된 방법으로 인정하고 있으며 DO-178B는 유럽에서도 EUROCAE에 ED-12B로 똑같이 활용되고 있다. ED-12B는 ED-12A의 개정판으로 1985년에 출판되었다. DO-178B의 수록 내역은 다음과 같다.

- 소프트웨어 개발 관련 시스템 사항(2)
- 소프트웨어 라이프 사이클(3)
- 소프트웨어 계획 프로세스(4)
- 소프트웨어 개발 프로세스(5)
- 소프트웨어 검증 프로세스(6)
- 소프트웨어 형상관리 프로세스(7)
- 소프트웨어 품질보증 프로세스(8)
- 인증협력 프로세스(9)
- 항공기 및 엔진 증명 개관(10)
- 소프트웨어 라이프 사이클 데이터(11)
- 추가 고려사항(12)
- 소프트웨어 수준별 프로세스 목표 및 출력물(부속서 A)

DO-178B 및 ED-12B는 전 세계의 산업계 대표자의 확대 위원회에서 개발되었는데 공식 작업 그룹은 RTCA SC-167 및 EUROCAE WG-12이고 그 구성원은 FAA, CAA, 보잉, Aerospatiale, Bendix/King, Veridatas, NASA, British Aerospace, 스

미스 산업계, Litton 항공, Rockwell Collins, 허니웰, Deutsche Airbus, ARINC, SNECMA, GE 항공기 엔진, Pratt & Whitney(Rolls-Royce)의 대표자등이 참여하였다.

DO-178B/ED-12B는 안전-중요한 항공전자 시스템에서 디자인하고, 규정하고, 개발하고, 테스트하고 소프트웨어를 전개하는 데 대한 지침을 제시하고 있다. 이것은 소프트웨어 라이프 사이클, 소프트웨어 계획 프로세스, 소프트웨어 개발 프로세스, 소프트웨어 검증 프로세스, 소프트웨어 형상관리 프로세스, 소프트웨어 품질 보증 프로세스 및 안전-중요한 환경을 위해 우량 소프트웨어를 만드는 데 관점을 두고 있다.

다. DO-178B 내용

기본적으로, DO-178B는 모든 코드 라인이 바로 요구조건과 시험 절차에 추적 가능하도록 하고 이 프로세스의 외부에서의 이질적인 코드는 제작과정에서 배제하도록 규정하고 있다. FAA(또는 다른 정부 기관) 검토에서 검사관은 소프트웨어 개발 소산물 검토 및 툴을 확인하면서 문서 패키지에 대한 시험에서 설계에서 코드화 까지 추적을 할 수 있다.

다른 치명도 환경을 적응시키기 위해, DO-178B는 소프트웨어가 시스템 안전 평가에서 확인된 안전관련 고장을 유발하는 가능성에 근거하여 5 가지의 소프트웨어 수준(A, B, C, D, E)을 만들었다. 그러므로 이 소프트웨어 수준은 DO-178B 증명 요구조건을 충족시키는 데 드는 노력의 수준에 직접 관계가 있다. 여기서 수준 A는 가장 치명적인 수준으로서 소프트웨어 신뢰성을 증명하는 데 가장 엄격한 노력을 요구한다. DO-178B는 다음과 같이 소프트웨어를 5가지 수준으로 분류하고 있다(표 3 참조).

DO-178B/ED-12B의 부속서 A는 각 특성 소프트웨어 수준이 충족하여야 하는 목표(objectives)를 제시하고 있다. 이 소프트웨어 수준은 소프트웨어 개발 및 검증 프로세스에서 바람직한 속성(desirable attributes)을 정의한다. 엄격함의 차이는 어떤 목표는 독립적으로 충족하여야 하는 것도 있지만 만족시켜야 하는 목표의 수와 개발 과정에서 생성되는 소프트웨어 자료의 형상 관리의 공식절차에 의해 결정된다. 예를 들면, 각 소프트웨어 수준별 목표의 수는 아래와 같다:

- 수준 A: 66 목표
- 수준 B: 65 목표
- 수준 C: 58 목표
- 수준 D: 28 목표
- 수준 E: 0 목표

DO-178B/ED-12B는 크게 개발 활동과 통합 프로세스로 구분된다. 개발 활동에는 계획, 요구조건, 설계, 코드 및 통합(planning, requirements, design, code, and integra-

< 표 3> 소프트웨어의 5 가지 수준 분류

SW 수준	고장 상태	고장상태의 분류
A	계속적인 안전 비행과 착륙을 막는 고장 상태	Catastrophic
B	아래와 같은 혹심한 운용 조건을 대처해 나가는 항공기 또는 승무원의 능력을 떨어뜨리는 고장 상태. (1) 안전여유 또는 기능적 성능의 상당한 감쇄 (2) 승무원이 임무를 정상적으로 완전하게 수행할 수 없는 물리적 재난이 있거나 과도한 조종 부하상태 (3) 소수의 승객에게 심각하거나 잠재적 치명 상해와 같은 혹심한 영향이 있는 상태	Hazardous
C	승무원의 조종부하의 상당한 증가, 승무원의 능률이 저하되는 상태 또는 승객에게 부상이 발생하는 불편함과 같은 안전여유 감소 또는 항공기의 성능저하와 같은 혹심한 운항조건에 대처해 나가는 항공기의 성능 또는 승무원의 능력을 감쇄시키는 고장 상태	Major
D	항공기의 안전을 현저하게 감쇄시키는 상태로서 승무원의 능력범위 안에서 수습이 가능한 고장상태	Minor
E	항공기의 운용 성능을 떨어뜨리지 않으며 조종 부하를 증가시키지 않는 고장 상태	No Effect

tion)이 있고 통합 프로세스에는 검증, 형상관리, 품질 보증 및 인증협력(verification, configuration management, quality assurance, and certification liaison) 이 있다. 그러나 이 두 개의 프로세스가 독립적으로 구분되는 것은 아니며 통합 프로세스는 각 개발 활동과 중첩되어 진행이 된다. 즉, 검증, 형상관리, 품질 보증 및 인증협력은 각 개발 활동에 적용된다.

DO-178B/ED-12B의 66가지 목표는 부속서 A에 표 1부터 표 10으로 제시되 있으며 전체 개발 활동과 전술한 바와 같이 통합 프로세스로 구성된다. 각 표의 제목은 다음과 같다

- 표 A-1: 소프트웨어 계획 프로세스(Software Planning Process)
- 표 A-2: 소프트웨어 개발 프로세스(Software Development Processes)
- 표 A-3: 소프트웨어 요구조건 프로세스 출력의 검증 (Verification of Outputs of Software Requirements Process)
- 표 A-4: 소프트웨어 설계 프로세스 출력의 검증(Verification of Outputs of Software Design Process)
- 표 A-5: 소프트웨어 부호화 및 통합 프로세스 출력의 검증(Verification of Outputs of Software Coding & Integration Processes)
- 표 A-6: 통합 프로세스 출력의 시험(Testing of Outputs of Integration Process)
- 표 A-7: 검증 프로세스 결과의 검증(Verification of Verification Process Results)
- 표 A-8: 소프트웨어 형상관리 프로세스(Software Configuration Management

< 그림 1> DO-178B 의 표 A-5, Verification of Output Software Coding and Integration Processes 의 첫줄

	Objective		Applicability by SW level				Output		Control category by SW level			
	Description	Ref.	A	B	C	D	Description	Ref.	A	B	C	D
1	Source Code complies with low-level requirements.	6.3.4a	●	●	○		Software Verification Results	11 14	②	②	②	

Process)

- 표 A-9: 소프트웨어 품질 보증 프로세스(Software Quality Assurance Process)
- 표 A-10: 인증 협력 프로세스(Certification Liaison Process)

부속서 A의 표 배치 및 구조를 설명하기 위해 그림 1에 표 A-5를 예로 들었다. 칼럼의 첫 번째 세트는 DO-178B/ED-12B 목표에 관한 정보를 나타내고 있다.

좌측부터 차례로 목표 번호, 설명 및 그 목표가 상술되는 DO-178B/ ED-12B의 참고 문헌을 나타낸다. A, B, C, D로 표시된 다음 칸은 이 소프트웨어 수준에 대한 특별 목표의 적용성(applicability by SW level)을 보여 준다. 예를 들면, 목표 1은 수준 A, B 및 C에 적용되며 소프트웨어 수준 D에 대해서는 만족시킬 필요가 없다. 적용성을 표시하고 있는 원이 채워진 경우, 그 목표는 독립적으로 충족하여야 한다. 다음 칸은 목표가 충족되었다는 증거로서 산출된 출력물(output)을 나타낸다. 설명(description) 칼럼은 자료의 출처를 나타낸다. Ref. 칼럼은 그 소프트웨어 자료의 특성을 상술하는 DO-178B/ED-12B의 장·절을 나타내며 여기서는 11.14가 해당됨을 나타낸다. 마지막 네 번째 칼럼은 관련 소프트웨어 해당 소프트웨어 수준에 대한 특정 출력의 형상관리의 엄격성을 나타낸다. 통제 분류(Control category) 1(CC1)은 통제 분류 2(CC2)보다 많은 형상관리 활동을 필요로 한다. 예를 들면, 통제 분류 1은 문제 보고 및 변경 관리를 필요로 하는 반면 통제 분류 2는 단지 변경관리만을 요구한다.

DO-178B/ED-12B의 평가는 FAA 인원, 관선기술대리인(DER) 또는 소프트웨어 개발자의 팀 멤버가 현장 검토(on-site reviews) 또는 데스크톱 컴퓨터(desktop review)에서 자료검토로 수행된다. 이 평가는 DO-178B/ED-12B의 부속서 A에서 기재된 목표가 충족되었는지를 결정하는 자료에 대한 평가이다. 1998년 6월 FAA는 "소프트웨어 인증을 위한 증명전 소프트웨어 검토 (Conducting Software Review Prior to Certification)"란 제목의 job aid를 발행하였다. 이 job aid는 DO-178B/ED-12B의 목표에 대한 합치성을 보증하는 프로세스에 대해 기술하고 있다. 특정 시

스템에 대한 인증 수준은 장비 제조업자와 FAA 또는 JAA 와 같은 인증 당국의 고장 분석 및 입력 프로세스로 결정되며 최종 결정은 인증 당국이 하게 된다.

다른 소프트웨어 구성 요소는 특별히 각 지정 수준으로 인증 받을 필요는 없다. 임의의 수준에서의 증명은 lower-level 요구조건을 자동적으로 다룬다. 그러나 분명하게, 역은 그러하지 아니하다. 수준 A로 인증받는 소프트웨어는 어떠한 항공전자 적용에 사용될 수 있다. 다음 표 4는 DO-178B 증명에 대해 제공할 필요가 있는 문서 및 기록 목록을 보여준다. 이 표에서 제출문서라 표기된 사항은 감항당국에 필히 제출되어야 하는 문서임을 나타낸다.

< 표 4> Software Life Cycle Data DO-178B 작성물 목록 (Deliverables List)

Acronym	Document Title		Type	Section
PSAC	Plan for Software Aspects of Certification	소프트웨어 인증계획서	제출문서	11.1
SDP	Software Development Plan	소프트웨어 개발계획서	Document	11.2
SVP	Software Verification Plan	소프트웨어 검증계획서	Document	11.3
SCMP	Software Configuration Management Plan	소프트웨어 형상관리계획서	제출문서	11.4
SQAP	Software Quality Assurance Plan	소프트웨어 품질보증계획서	Document	11.5
SRS	Software Requirements Standards	소프트웨어 요구규격서	Document	11.6
SDS	Software Design Standards	소프트웨어 설계표준서	Document	11.7
SCS	Software Code Standards	소프트웨어 코드 기준서	Document	11.8
SRD	Software Requirements Data	소프트웨어 요건기술서	Document	11.9
SDD	Software Design Description	소프트웨어 설계기술서	Document	11.10
	Source Code	소스 코드	Software	11.11
	Executable Object Code	실행 목적 코드	Software	11.12
SVCP	Software Verification Cases and Procedures	소프트웨어 검증 케이스 및 절차	Document	11.13
SVR	Software Verification Results	소프트웨어 검증 결과	Records	11.14
SECI	Software Life Cycle Environment Configuration Index Document	소프트웨어 라이프사이클 인덱스 문서	Document	11.15
SCI	Software Configuration Index	소프트웨어 형상 인덱스	Document	11.16
PRs	Problem Reports	문제점 보고서	Records	
	Software Configuration Management Records	소프트웨어 형상관리 기록서	Records	
	Software Quality Assurance Records	소프트웨어 품질보증 기록서	Records	
SAS	Software Accomplishment Summary	소프트웨어 성취 보고서	제출문서	

라. DO-178B 소프트웨어 검증

대부분의 DO-178B projects 관련 구조 시험에는 다음 세 가지 주요 커버리지가 있다. 커버리지라 함은 검증행위의 범위를 나타내는 것으로서 반복적인 검증행위의 종결기준을 제공하며 커버리지 분석은 이러한 검증행위의 범위를 확인하는 것이다.

- SC: Statement Coverage(구문 커버리지)

프로그램의 모든 구문이 최소한 일회 실행 또는 사용됨을 의미한다. 이것은 용어 "code coverage"의 가장 일반적인 활용이다.

- DC: Decision Coverage(결정 커버리지)

프로그램의 입구 및 출구의 모든 점이 최소한 일회 실행되고 프로그램의 각 결정이 최소한 일회 모든 가능한 결과에 대해 실행됨을 의미. 본질적으로, 이것은 모든 불리안(Boolean) 문이 둘 다 TRUE 및 FALSE로 평가됨을 의미한다.

- MCDC: Modified Condition Decision Coverage(수정 조건 결정 커버리지)

프로그램의 입구 및 출구의 모든 점이 최소한 일회 실행되고 프로그램의 모든 결정이 최소한 일회 모든 가능한 결과를 취하고 결정에서의 각 조건이 결정 결과에 독립적으로 영향을 미치는 것으로 나타남을 의미. 복합 부울 대수는 TRUE 및 FALSE가 가변적인(내부의 불리안 연산식) 세트로 개발되는 진리 표가 있을 필요가 있다.

다음 표는 각 DO-178B 수준을 위해 코드 커버리지 요구조건을 상술한다.

Level	Coverage	Coverage Requirements
Level A	MCDC	Level B + 100% Modified Condition Decision Coverage
Level B	DC	Level C + 100% Decision Coverage
Level C	SC	Level D + 100% Statement (or Line) Coverage
Level D	-	100% Requirements Coverage Requirements
Level E	-	No Coverage Requirements

이 코드 커버리지 연습을 수동으로 수행하는 것이 가능하나 이 프로세스는 상용의 코드 커버리지 툴을 이용한 실행이 지금 가능하다. 다수의 코드 커버리지 툴 판매자가 DO-178B를 증명하고 및 합치성을 충족시키기 위해 적절한 시험 출력을 내는 시험 툴을 공급하고 있다.

DO-178B/ED-12B는 충족시켜야 하는 특별 검증 목표 (specific verification objectives)를 제시하고 있는 데 다음과 같은 것이 있다.

1. 소프트웨어 개발 프로세스의 검증
2. 소프트웨어 개발 라이프 사이클 생성물의 검토

3. 소프트웨어의 기능적인 확인
   a. 요구조건에 기반을 둔 시험 및 분석
   b. 건강성 시험
4. 구조상의 커버리지 분석

구조상의 커버리지 분석은 일반적으로 엄격한 코드 개발 및 시험에 익숙해 있지 않은 사람들이 떠맡는 아주 어려운 과업으로 인정되고 있다. 게다가, 하드웨어, 캐시, 인터럽트, 메모리 관리 및 프로세스/과업 관리와 밀접하게 통합된 운영체제를 인증하는 것은 구조상의 시험을 훨씬 더 어렵게 할 수 있다. 이 저 수준(low-level)의 관점은 확인 프로세스에 대한 중요한 도전이 되고 있다. 예를 들면 Level A 인증 신청은 다음을 언급해야 한다.

1. 구문 커버리지(Statement Coverage)
2. 결정 커버리지(Decision Coverage)
3. 수정 조건/결정 커버리지 (MCDC, Modified Condition Decision Coverage)
4. 죽거나 또는 비활성화된 코드의 표식
5. 원천부터 오브젝트 코드까지의 추적성

IV. 항공기 등의 증명업무에 대한 개관

그림 2는 전형적인 형식증명의 과정을 보여준다. 여기서는 증명 프로그램을 15가지의 과업으로 나누었으며 소프트웨어 집약형의 과업 8종은 이탤릭체로 표시 하였다. 이 과업은 연속적이지 않을 수 있으며 다소 중복이 있을 수 있다.

V. 항공기 인증과정에서의 소프트웨어 인증 프로세스

이 절에서는 간단히 과업의 일반적인 사항을 기술하고 총체적인 증명 프로젝트에서 8개의 소프트웨어-특성 과업(즉, 과업 #1, 4, 5, 6, 7, 8, 11 및 12)의 내용을 설명하기로 한다.

가. 친숙화 회의(Familiarization Meeting)

친숙화 회의는 FAA 및 신청자가 잠재적인 프로그램 계획에서 예상되는 문제

< 그림 2> 전형적인 형식증명 프로그램에서 소프트웨어 관련 과업

점에 대해 논의하는 대화의 장이다. 이 회의는 소프트웨어 개발시 FAA와 신청자 각자가 자원 활용을 계획하도록 가능한 한 빨리하는 것이 좋다. 최초의 회의에 뒤이어, 추가 소프트웨어-특성 회의를 할 수 있다. 소프트웨어 계획 문제, 접근방법, 수준 및 잠재 위험은 이 회의에서 또는 후속 소프트웨어-특성 회의에서 논의하여야 한다. 이 친숙화 회의 및 후속 소프트웨어-특성 회의에서 FAA의 역할과 책임은 다음과 같다.

- 회의 전 안건을 작성하기 위해 신청자와 협조한다.
- 모든 필요한 주제가 다루어 지도록 안건을 마련한다.
- FAA 증명 팀을 소개한다.
- 열린 대화로 협력의 분위기를 촉진한다.
- 대화와 협의를 통해 알게 된 모든 기업의 정보는 비밀이 보장됨을 알린다.
- 열린 논의를 허용하여 회의가 유연하게 진행되도록 한다.
- 신청자의 신청내역을 듣고 및 이해한다.
- 증명 기초(certification basis)와 인용규격, 정책, 지침 및 규칙에 대해 협의한다.
- 증명 프로세스 및 예측 사항을 논의한다.
- 이용 가능한 훈련 방안을 논의한다.
- 안전 평가 프로세스와 소프트웨어 수준 설정 등 소프트웨어 연결점을 논의한다.
- 적절한 문서 즉 RTCA DO-178B SAE ARP 4754 및 4761, AC 25-1309 또는

AC 23-1309 및 항공기기술기준(KAS)의 적용 가능한 코드를 확인한다.
- 일정 및 예상되는 사항을 논의한다.
- 임의의 잠재적인 문제에 관해 언급한다.
- 소프트웨어 승인 프로세스 문서화의 목록을 제공한다.(예를 들면, DO- 178B, 권고 문헌, Notices, Orders, 규칙 및 job aids).
- 전형적인 소프트웨어 승인 프로세스 및 이용 가능한 문서화를 기술한다. Software Review Job Aid(증명전 소프트웨어 검토) µi健 ÀÖヴ.
- 소프트웨어에 연결되는 구조 및 시스템을 논의한다.
- 판매인(vendor) 감독을 위해 여러 가지 소프트웨어 프로젝트, 개발자, 사이트 및 계획을 논의한다.
- 위임자(designee) 관리 및 참가 계획을 논의한다.
- 증명 계획의 소프트웨어-특성 관점을 논의한다.
- 업무 분담을 명백히 한다.
- 회의 후 회의 결과, 행위 및 협약서등 문서에 필요시 합의 서명한다.

신청자는 친숙화 회의에서 다음 역할/책임 과업을 가진다.
- 프로젝트 라이프 사이클에서 가능한 한 이른 시기에 회의가 진행되도록 계획한다.
- 회의에 앞서 안건을 개발하는 데 감항당국의 입력 사항을 발굴한다.
- 회의에 앞서, 회의에서 제공하는 관심의 질문 및 영역을 준비한다.
- 회의에 앞서 감항당국 문서, 요구조건 및 웹 사이트를 조사한다.
- 현재의 계속적인 소프트웨어 정책 및 지침 활동에 대해 잘 알아야 한다. 예를 들면, RTCA 활동 및 감항당국 웹 사이트 등.
- 프로젝트 팀 멤버, 증명 협력 연락 인원, 관선기술대리인(DERs)및 다른 출석자를 소개한다.
- 시스템 해설 및 취지들을 제시한다.
- 안전 프로그램 및 소프트웨어 수준을 논의한다.
- 새로운 특징, 새로운 접근방법 및 기존의 증명 정책에서 편차를 확인하여 issue papers, 특수 조건 또는 정책이 조기에 발행되도록 한다.
- 일정 목적을 확인한다. 또는 그렇게 하기 위해 취한다.
- 특별한 소프트웨어 고려를 확인한다. 예를 들면, 서비스 이력, 특별한 설계 접근방법 및 소프트웨어 툴 등.
- FAA와의 빈번한 의사소통을 위한 계획을 개발한다.
- 이것에는 분기별 프로그램 상태 회의, 정기적인 전문가 회의 또는 매월 일정 제출 회의가 있다.
- 예비적인 일정 및 문서화 결과 제출 요구조건을 확인한다.
- 계획된 프로세스 및 팀을 확인한다.

- 회의 후 향후 FAA에 질문할 내용을 상세하게 기록한다.
- 회의 후 회의록, 회의 결과 요약서, 실행 사항 및 합의서 등을 준비한다.
- 회의 후 회의록에 공동 서명함으로서 회의 결과에 대한 FAA 간의 서면 협약서를 작성 보관한다.
- 후속 소프트웨어-특성 회의에서 이전의 회의에서 문제와 실행 사항을 확인한다.

나. 공식 증명 신청서 제출 (Formal Application)

신청자가 FAA에 TC 신청서를 공식으로 제출할 때 공식 신청 행위가 발생한다. 이 때 이 형식증명 프로젝트에 감항당국의 프로젝트 번호가 할당 된다.

다. 예비형식증명위원회 (Preliminary TC Board Meeting)

예비형식증명위원회에는 감항당국 및 신청자가 함께 참석한다. 예비형식증명위원회는 신청자의 의도와 감항당국의 입장을 공식적으로 전달하는 통로이다. 논의 사항은 증명 기초(certification basis), 감항당국 요구사항 및 증명 일정 등과 같은 주제를 포함한다.

라. 소프트웨어 계획단계(Software Planning Stage)

소프트웨어 계획단계는 모든 소프트웨어 개발 문서의 개발, 검토 및 승인을 포함한다. 이 과업의 산출물에는 증명에서의 소프트웨어 입장에 대한 계획(PSAC, Plan for Software Aspects of Certification), Software 개발 계획(SDP, Software Development Plan), 소프트웨어 품질 보증 계획(SQAP, Software Quality Assurance Plan), 소프트웨어 형상 관리 계획(SCMP, Software Configuration Management Plan), 소프트웨어 확인 계획(SVP, Software Verification Plan), 소프트웨어 개발 표준 및 기타 필요한 계획 문서 등이 있다. PSAC은 프로그램의 이 단계에서의 특히 중요한 문서다. PSAC은 신청자의 프로그램의 계획을 상세하게 기록한다. 예를 들면, 소프트웨어 수준, 유일한 소프트웨어 문제 및 소프트웨어 개발 일정 그리고 감항당국과 신청자간의 합의서 역할을 하게 된다. 계획 단계는 소프트웨어 개발을 시작에 앞서 완료되어야 하고 및 감항당국과 협의하여 승인 받는다. 즉, 소프트웨어 계획은 소프트웨어 개발에 앞서 FAA 승인을 받는 것이 좋다. 이 과업에서 감항당국의 역할/책임은 다음과 같다.

- PSAC(피쌕이라고 읽음)을 가능한 빨리 검토하고 서면으로 피드백 한다.
- FAA 증명 팀(즉, 프로그램 담당자, 비행시험, 시스템, 추진 및 기체구조 담당자 등)과 PSAC에서 제시한 소프트웨어 수준의 적절성에 대해 협의한다.
- 소프트웨어 개발 프로젝트(예를 들면, 검토자의 수, 위임 사항 및 필요한 문

서화의 내역 등)에서 감항당국의 요원의 참여 정도를 결정하고 문서화 한다.
- 감항당국 프로그램 관리자 및 신청자의 팀에 관련 참여자수 및 위임 사항을 요약한 문서를 제출한다.
- 신청자에 어느 소프트웨어 계획이 감항당국에 제출되어야만 하는지 지정한다.
- 새로운 정책 또는 issue papers를 필요로 하는 잠재적 문제를 확인하고 그 문제에 관해 다루기 시작한다.
- 잠재적인 프로그램 충격성이 있는 issue papers에 신속한 응답을 제공한다.
- 신청자의 위임 계획에 피드백 및 협약서를 제공한다.
- 가능한 신속하게 PSAC의 서면 승인을 제공한다.
- 문서 제출 후 제출 계획을 DO-178B의 목표에 따라 이행한다는 것을 보증하기 위해 SDP, SQAP, SVP를 검토한다.
- 신청자와 함께 관심 사항을 조정한다.
- 필요시 계획 단계에 대해 현장에서 또는 데스크톱 컴퓨터로 검토 한다.(소프트웨어 재검토 Job Aid를 필요에 따라 사용한다.)
- 신청자와 함께 시기적절한 방법으로 모든 관심 사항을 전달한다.
- 신청자와 함께 협약서를 문서화 한다.
- 필요시 국가의 자원 전문가(NRS, National Resource Specialists), 기술적 전문가(TS, Technical Specialist), 본부 인원 및 이사회 인원과 조정한다.
- 향후 활동 사항을 계획한다.

소프트웨어 계획 단계에서의 신청자의 역할/책임은 다음과 같다.
- 프로세스의 초기에 위임자를 참여시킨다.
- PSAC은 구속력이 있는 협약서를 설정하도록 충분히 상세하게 작성한다.
- 신청자의 증명팀 및 소프트웨어 승인에 대해 책임이 있는 감항당국 엔지니어와 PSAC 초안과 제안 소프트웨어 수준을 조정한다.
- 감항당국과 협약서를 체결하도록 가능한 한 초기에 PSAC을 제출한다.
- 감항당국 피드백에 대응하여 PSAC을 재제출하고 필요시 팔로우업한다.
- 이전에 합의한 계획서에 대한 중요한 변경사항은 감항당국에 통보한다.
- 잠재적 프로그램 충격을 가지고 있는 issue papers에 신속히 응답한다.
- 위임 계획서를 제출한다.(즉, 제안 대리인과 그들의 활동 계획 및 승인 계획을 확인한다.)
- 감항당국에 문서에 우선 목록을 제출한다.(즉, 자료 검토에 대한 중요하고 즉각적인 요구 사항을 감항당국과 의사소통한다.)
- 안전 평가 프로세스 상태/갱신(개발 라이프 사이클 전체에 지속적으로 수행한다.)을 협의한다.
- PSAC의 갱신 사항은 승인 또는 서면 협약서를 감항당국으로 부터 받는다.
- SDP, SQAP, SCMP, SVP 및 개발 표준(development standards)을 작성한다.
- 위임자와 계획을 협의한다.

· 감항당국 요구 시 소프트웨어 계획서를 제출한다.
· 개발 활동에 앞서 모든 것 소프트웨어 계획의 승인을 조화시킨다.

마. 증명 프로그램 계획서(CPP, Certification Program Plan)

증명 프로그램 계획서(CPP) 또는 이와 동등한 문서에는 요구되는 제출 문서, 예상되는 위임 계획, 중요한 프로그램 상의 문제, 일정 계획 및 기타 중요한 프로그램 상의 문제들에 대해 프로그램의 소프트웨어 관점에서 감항당국의 의도된 참여를 기록한다. CPP는 이전의 과업에서 신청자가 제출한 사항에 근거하여 감항당국이 작성하며 PSAC의 승인 후 가능한 빨리 완료되어야 한다. CPP는 주로 감항당국 내부 조정을 위해 사용된다. 그러나 신청자에 프로그램 동안 내내 감항당국의 기대를 명쾌하게 하기 위해 제공되어야 한다.

이 과업에서 감항당국의 소프트웨어-특성 역할/책임은 다음과 같다:

· 소프트웨어 프로그램에서 감항당국의 예상 참여 수준을 확인한다.
· 신청자의 계획서에 있는 위임자의 업무 담당 범위를 검토한다.
· 관련 참여 계획(예를 들면, 소프트웨어 검토의 수, 필요 제출 자료 및 위임에 대한 협약서)을 문서화 하고 CPP에 포함시킨다.
· 프로그램의 잠재 위험을 문서화한다.
· 감항당국 증명 팀과 함께 CPP을 조정한다.
· 신청자와 CPP를 조정한다.
· CPP 과업을 위한 신청자의 역할/책임은 CPP을 재검토하고 및 시기적절한 방법으로는 피드백을 감항당국에 제공하는 것이다.

바. 소프트웨어 개발단계(Software Development Stage)

소프트웨어 개발단계는 신청자가 승인된 계획에 따라 소프트웨어를 개발하는 단계이다. 신청자는 요구조건, 설계, 코드 및 다른 개발 자료를 개발한다. 이 때 감항당국은 승인 계획의 이행과 DO-178B의 목표에 대한 감독을 수행한다. 계획으로부터 다소 벗어난 사항은 감항당국 및 신청자 사이에서 조정하여야 하고 및 가능한 한 신속하게 해결하여야 한다. 소프트웨어 개발 단계 동안의 감항당국의 역할/책임은 다음과 같다.

· 필요시 엔지니어/감사인 팀을 통하여 신청자의 문서를 검토한다.
· 모든 관심 사항을 신청자에게 알린다.
· 기대 사항을 확실히 말한다.
· 다른 감항당국 증명 팀 구성원과 협의한다.
· 필요시 현장 및 데스크톱 컴퓨터 재검토에 소프트웨어 재검토 Job Aid를 따른다.

· 프로그램 동안 내내 관심 사항과 문제를 문서화 한다.
· 이 과업에서 신청자는 다음 역할/책임을 수행한다.:
· 승인된 계획 및 전환 기준을 지킨다.
· PSAC 또는 문서를 통하여 프로세스에 임의의 변경 사항을 감항당국과 조정한다.
· 감항당국과의 열린 통신을 유지한다.
· 요구조건, 설계, 인정 요건 등을 명확히 개선하고 증명 상의 위험을 완화하기 위해 감항당국과 증명 신청팀 간에 개념을 공유한다.
· 프로세스 합치성의 증거를 문서화한다.
· 소프트웨어 재검토 Job Aid를 활용하여 내부 소프트웨어 검토를 수행한다.
· 감항당국 또는 위임자가 도착하기 전에 소프트웨어 재검토를 작성하고 조정한다.
· 대리인은 지속적으로 참여하도록 한다.

사. 소프트웨어 확인/시험단계(Software Verification/Test Stage)

소프트웨어 확인/시험단계는 프로젝트가 끝날 때까지 개발 프로세스 및 소프트웨어 시험 동안 내내 단계별로 확인을 수행한다. 확인은 개발 계획 동안 내내 필요 불가결하다. 그러나 시험 단계에서 많은 개발 활동이 있게 된다. 이 과업 동안 신청자는 확인 및 시험 활동을 수행한다. 이 때 감항당국은 모든 활동을 감시한다.

소프트웨어 확인/시험 단계 동안의 감항당국의 역할/책임은 다음과 같다.

· 필요시 현장에서 또는 데스크톱 컴퓨터 재검토(엔지니어/감사인 팀을 활용하여)를 통하여 신청자의 문서, 확인 프로세스 및 결과를 그리고 프로그램 테스트를 검토한다.
· 소프트웨어 상의 문제에 관해 이해하고 및 언급하기 위해 위임자와 의사소통한다.
· 위임자 활동을 감독한다.
· 현장에서의 또는 데스크톱 컴퓨터 재검토에서 필요한 경우 소프트웨어 재검토 Job Aid를 따른다.
· 신청자에게 요구사항을 분명히 설명한다.
· 모든 관심 사항을 신청자에게 알린다.
· 다른 감항당국 증명 팀 멤버와 의사소통한다.
· 이 과업에서 신청자의 역할/책임은 다음과 같다.
· 일정 압력에도 불구하고 초점을 유지한다.
· 전환 기준 및 승인 계획을 준수한다.
· 감항당국과 함께 열린 의사소통을 유지한다.

- 문제가 발생될 때 감항당국과 함께 문제 및 관심 사항을 논의한다.
- 요구조건, 설계, 인정 요건 등을 명확히 개선하고 증명상의 위험(risk)을 완화하기 위해 감항당국과 증명 신청팀 간에 개념을 공유한다.
- 피어검토(peer review) 및 내부 검토를 실행한다.
- 문제를 포함하여 확인 및 시험 결과를 문서화한다.
- 프로세스 합치성(예를 들면, 문제 추적, 형상 관리 및 품질 보증)의 증거를 문서화한다.
- 내부 재검토, 워크 스로우 및 검사를 조정하고 및 준비한다.
- 지속적인 위임자 참가를 유지한다.
- 감항당국 또는 위임자 검토를 위해 지침서로서 소프트웨어 재검토 Job Aid를 사용한다.

아. 소프트웨어 회의 및 검토(Software Meetings and Reviews)

소프트웨어 회의 및 검토는 소프트웨어 개발 및 승인 프로세스 전체 과정에서 문제에 관해 언급하기 위해 수행한다. 이 회의는 감항당국 및 신청자의 소프트웨어 전문가를 수반하며 규칙적으로 연다. 다중의 소프트웨어 구성 요소가 있는 적극적인 TC 프로그램에서 이 회의가 규칙적으로 개최되어야 한다. 성공적인 프로그램을 위해 감항당국, 신청자 및 소프트웨어 개발자 사이의 명백한 및 일관된 의사소통 경로는 필수다.

소프트웨어의 치명도, 위임자 지원의 분량 및 신청자 또는 소프트웨어 개발자의 경험에 따라, 감항당국 또는 위임자는 현장에서의 또는 데스크톱 컴퓨터 소프트웨어 재검토를 수행한다. 소프트웨어 재검토 프로세스에 관한 추가 정보를 위해 참고 문헌 소프트웨어 재검토 과업 목적. 이 과업 동안의 감항당국의 활동은 다음과 같다.

- 문제의 조기 해결을 위해 노력한다.
- 회의의 안건을 조정한다.
- 회의(즉, 필요에 따라 NRS, TS, 본부 또는 이사회의 권고를 따른다.)에서 정확한 사람들이 참가하도록 조정한다.
- 회의를 준비한다. (예를 들면, 이전의 회의의 재검토 및 이전의 회의로부터의 제시된 실행사항의 이행 등)
- 필요시 증명 팀을 포함시키도록 한다.
- 책임을 유지한다.
- 시간의 틀 및 예상에 관해 합의한다.
- 소프트웨어 재검토를 수행할 때 소프트웨어 재검토 Job Aid를 사용한다.
- 문제의 조기 해결을 위해 노력한다.
- 업무 분담을 명백히 한다.

· 시기적절하게 회의/재검토 합의 사항 및 필요한 실행 사항을 문서화한다.
이 과업 동안의 신청자의 활동은 다음과 같다.:
· 이전 회의에서 제시된 실행 사항과 협의 사항을 검토한다.
· 마스터 실행 사항 목록을 유지한다.
· 감항당국과 함께 자주 열린 의사소통을 가진다.
· 감항당국과 함께 소프트웨어 검토를 조정한다.
· 감항당국 소프트웨어 재검토 Job Aid를 감항당국 또는 위임자 재검토에 대비하기 위해 사용한다.
· 프로젝트 동안 내내 및 감항당국과의 모든 것 회담에 위임자를 수반한다.

자. 비행전 형식증명위원회(Pre-flight TC Board Meeting)

비행전 형식증명위원회는 증명 비행 시험 프로그램에 앞서 수행하고 증명 비행 시험에 앞서 언급된 문제 사항을 해결하기 위해 수행한다.

차. 형식 검사 승인(TIA, Type Inspection Authorization)

형식 검사 승인(TIA)은 증명 프로그램에서 시험 사항과 합치성을 기록하는 문서다. TIA는 증명 전문가로부터의 입력을 모으고 및 증명 비행 시험에 앞서 종결되어야 한다. TIA는 전형적으로 새로운 시험 계획 및 항공기 형상을 고려하여 TC 계획 동안 내내 여러 차례 개최한다.

카. 적합성 검사 및 증명 비행시험 (Conformity Inspection and Certification Flight Testing)

적합성 검사 및 증명 비행시험은 항공기를 형상화하는 프로세스이며 항공기를 비행시험 하는 프로세스이다. 항공기는 증명 시험에 앞서 뚜렷하게 정의되고 문서화된 형상이어야 한다. 적합성 검사는 시험 형상이 인증하고 있는 형상이라는 것을 보증하는 것이다. 증명 비행 시험은 전형적으로 소프트웨어에 영향을 미치는 시스템 요구조건에 변경을 가져온다. 감항당국 및 신청자는 적기에 비행 시험 프로그램에서 발생하는 문제를 다루는 프로세스가 있어야 한다. 감항당국의 역할/책임은 다음과 같다.
· 증명 엔지니어, 검사원 및 신청자 사이에서 합치성 예상을 조정한다.
· 조정이 발생하면 지침에서 변경에 관해 언급한다.
· 비행 문제/관심의 안전 사항에 대해서 비행 시험 및 증명 팀과 함께 조정한다.
· 이 과업 동안의 신청자의 역할/책임은 다음과 같다:
· 종업원 및 협력업체/공급자에게 합치성에 대한 훈련을 제공한다.

- 감항당국에 첨단 설계 및 로직을 확실히 설명한다.
- 이전의 협약서에 변경을 최소로 한다.
- 조기에 그리고 항공기에 장착하기 전에 벤치 시험을 수행한다.

타. 최종 소프트웨어 합치성 단계(Final Software Compliance Stage)

최종 소프트웨어 합치성 단계는 문제 보고서 및 비행 시험에서 확인한 소프트웨어의 해결, 소프트웨어 성취 요약서, 형상 인덱스 및 기타 감항당국이 요구하는 문서 등이 있다. 신청자 및 감항당국 소프트웨어 전문가 사이의 소프트웨어 회의 또는 검토 결과는 모든 소프트웨어 문제를 해결하고 소프트웨어 승인을 내주는데 필요 하다. 최종 소프트웨어 합치성 단계에서 감항당국의 역할/책임은 다음과 같다:

- 이전의 회의, 재검토 또는 논의에서 임의의 미해결 사항에 관해 언급한다.
- 위임자와 함께 최종 합치성 예상(예를 들면 내부 검토 또는 위임 목적 등)을 조정한다.
- 최종판 합치성 단계 동안 소프트웨어 재검토 Job Aid를 따fms다.
- 신청자와 함께 모든 문제를 논의하고, 문서화하고 및 추적한다.
- 증명 팀과 의사소통하고 필요시 모든 미해결 사항을 해결하기 위해 국가 자원 전문가(NRS)를 활용한다.
- 모든 확인 가능한 결함이 해결되었을 때 가능하면 수령 즉시 필요한 문서를 승인한다.

이 과업 동안의 신청자의 역할/책임은 다음과 같다.:

- 내부 검토를 실시하고 위임자를 수반한다.
- 소프트웨어 문제 해결서를 검토하고 및 문서화하고 안전 관련 문제를 스크린한다.
- 시스템, 안전 또는 비행 시험에 관한 문제를 증명 팀과 함께 조정한다.
- 최종 형상 관리 lockdown을 수행하고 형상 인덱스를 작성한다.
- 감사 수행 및 문제점 시정에 소프트웨어 검토 Job Aid를 활용한다.
- 소프트웨어 합치성 검토를 실시한다.
- 소프트웨어 성취 요약을 작성한다.
- 모든 필수 자료 및 요구 자료를 작성하여 제출한다.
- 필요시 감항당국에 검토 준비가 되었음을 알린다.
- 필요시 실행 사항을 검토하고 목록을 작성한다.
- 필요시 시정조치를 취하고 그 결과를 문서로 제출한다.

파. 항공기 평가 그룹(AEG, Aircraft Evaluation Group)의 최종 결정

항공기 평가 그룹(AEG) 결정은 전형적으로 증명 비행 시험의 과정이나 후에 완료된다. AEG 결정은 감항당국의 제품의 운용 평가 및 감항성 관점의 평가를 포함한다.

하. 최종 형식증명위원회(Final TC Board Meeting)

최종 형식증명위원회는 증명 프로그램의 끝단계에서 감항당국과 신청자간에 이루어진다. 때로 증명서는 이 회의에서 실지 발행된다. 그러하지 않은 경우 미해결 증명 문제는 확실히 의사소통하고 및 문서화한다.

거. 형식증명서의 발행(Issuance of TC)

형식증명서의 발행은 증명 프로세스의 최종 단계 과업이다. 대형 형식증명 프로그램의 경우 이것은 대개 media coverage와 신청자의 고위 경영층 발언을 수반한다. 총체적인 프로그램은 TC의 발행으로 끝나는 경우는 많지 않다. 대개 많은 후속발생 문제들이 남아 있기 마련이다. 감항당국 및 신청자 사이의 후속 계획 및 협약서는 TC의 교부에 앞서 확실히 문서화되어야 한다.

VI. 증명 과정에서 DER 의 역할

가. DER 제도의 목적

DER 즉 Designated Engineering Representatives는 관선기술대리인으로 번역되며 미국 연방 항공법에 의거 항공기 증명서의 발행과정에서 연방항공국 직원을 대신해서 필요한 조사, 시험, 검사 또는 승인의 업무를 할 수 있도록 일정 부분 적정한 능력이 있는 개인에게 업무를 위임하도록 하여 원활한 증명 수행업무를 도모하고자 하는 제도이다. 항공기의 설계가 여러 가지 다양한 기술이 복합된 고도의 공학 기술을 바탕으로 하고 있기 때문에 설계 내용이 감항 기준에 합치하며 안전하다는 것을 확인하는 데도 역시 고도의 전문 기술이 필요하다. 검증 수행을 위해 감항당국이 이러한 전문 기술을 일거에 전문 분야별로 습득할 수는 없는 실정이며 이러한 인증과정에서의 기술해석상의 문제를 중간자의 입장에서 해석 및 판단하는 역할자가 필요하게 되는 데 이러한 역할을 DER이 담당하게 된다. 이 DER에는 개인적으로 활동할 수 있는 상담역 DER(Consultant DER)과 회사에

소속되어 회사직원의 신분으로 업무를 수행하는 회사 DER(Company DER)이 있다.

이 DER 제도는 감항당국의 입장에서는 직원의 업무 영역을 확대할 수 있다는 장점이 있으며 기업의 입장에서는 증명 업무를 용이하게 해준다는 이점이 있다. 현재 미국에는 약 500여명의 증명관련 직원이 있고 약 3500여명의 DER이 있다.

나. DER의 업무

DER의 주업무는 증명 신청자의 자료의 승인과 합치성 증명서에 대한 동의 서명 등의 업무가 있고 기타 증명업무에 대한 제반 관심 사안에 대한 지도, 증명관련 문서작성 지원 그리고 ACO와 협력적 관계 유지하면서 ACO의 질문에 답을 제공하는 일 등이 있다. DER의 업무 자세로서는 우선 증명 요건에 대해 잘 알아야 하며 소관 업무에 대한 완전성과 신뢰성 유지할 수 있어야 한다.

다. DER 자격

DER의 자격은 FAA Order 8100.8 paragraph 201.c에 규정이 있으며 다음과 같은 네 가지 관점에서 업무 경험을 심사하여 인정하고 있다.

- 항공관련 법·규정에 대한 지식
- 소관 업무 분야에 대한 기술적 지식
- 원만한 대인 관계
- 해당 기술 표준에 대한 지식
- DER에 지원하기 위해서는 다음과 같은 조건을 갖추어야 한다.
- 신청 분야에 대한 FAA와의 직접업무 경험이 있을 것
- 감항당국 입장에서의 업무 수행 능력에 근거한 조언 능력이 있을 것

라. DER 지정분야

DER 지정분야는 14 CFR part 183.29에 다음과 같이 9 분야로 지정하고 있다. 한번 DER로 지정 받으면 매년 재심을 받아야 한다.

- Structural
- Powerplants
- Systems and Equipment
- Radio
- Engine
- Propeller
- Flight Analyst

· Flight Test Pilot
· Acoustical

마. DER의 권한과 책임

DER은 아래 사항과 같은 기술자료에 대한 승인의 업무와, 각종 시험의 입회 및 시험자료의 승인 그리고 기타 감항당국이 특별히 지정하는 업무 등이 있다.
· 도면, 보고서, 프로세스 규격서, 분석문서, 시험결과 등
· 회사 DER(Company DER) 소속회사의 자료만을 승인함
· 상담역 DER(Consultant DER) 은 어떤 자료도 승인함.
DER로서의 업무를 수행할 때는 감항당국(FAA) 요원과 동일하며 업무 수행에 있어서는 심사숙고한 판단을 하여야 하고 다른 기술분야의 업무를 존중하며 업무 일정보다 합치성 확인에 우선하고 자료 승인시의 부당한 압력은 감항당국에 보고하여야 한다.

바. 소프트웨어의 인증에서 DER의 역할

대부분의 고객 및 FAA는 DO-178B 제출 문서에 대해 품질 및 완전성을 보증받고 싶어 하며 DER이 이것을 제공한다. 모든 증명 프로젝트에는 감항당국 대표자가 배정되며 DER이 모든 제출물들을 검토하게 된다. DER은 감항당국의 대변자로서 프로젝트 문서에 서명하는 전권을 가지고 있다. 그러나 DERs이 모든 항공 전자/항공기 인증에 인증하는 것은 아니며 소프트웨어 DER은 해당 소프트웨어 활동을 승인하는 데만 국한된다.

DER의 활동은 대개 감항 당국에 문서를 제출하기 전에 문서를 검토하는 것이다. 감항당국에 서명을 하여 제출하는 문서는 FAA 양식 8110이다. DER의 서명은 근본적으로 감항당국의 인증이 되었다는 것을 의미한다. 그러나 소프트웨어가 최신의 것으로 바뀌지는 경우 또 다른 증명 시험이 필요하다. DER이 결국 문서를 조사하기 때문에, 다음과 같은 두 가지 이유로 DER을 소프트웨어 개발의 초기 단계부터 포함시키는 것이 좋다. 첫 번째 DER는 소프트웨어 시험의 일부로서 문서에 대한 확인을 담당한다. 두 번째 DER은 당신의 문서 또는 프로세스가 맘에 들지 않기 때문에 종결 서명하기 전에 변경을 주장할 수 있다. 이 변경은 프로젝트 완성시점보다는 설계 및 개발 시점에 하기가 훨씬 쉽다. 공식 가이드라인에 따라 개발하지 아니한 기존 소프트웨어를 인증 받으려 하는 경우 증명의 과정에서 불필요하게 자원이 소모되지 않도록 DER과 협의하는 것이 좋다.

VII. 결 론

항공기 형식증명의 과정에서 수행될 수 있는 소프트웨어-특성 과업은 약술하였다. 비록 감항당국 및 신청자의 역할 및 책임이 별도로 논의되었지만, 그것은 전 증명 프로세스 전체에 과업에서 양쪽 모두에 있어서 함께 중요하다. 증명 프로그램을 통한 조기의 합의 및 지속적인 의사소통은 성공에 있어 필수다. 감항당국 및 신청자는 증명 프로세스의 동반자 관계(partners)이지 적대관계가 아니다. 이 둘은 이해관계자이면서 소관 증명이 성공적으로 종료되기를 바라고 있다.

이 논문은 증명 당국과 신청자가 소프트웨어의 인증관련 활동 및 관련 필요성을 간단히 알도록 한 것이다. 바라건대 이 정보는 협력관계 프로세스를 고무하도록 하였으며 모든 관련자가 계획을 잘 수립하도록 하고 성공적인 소프트웨어 승인을 얻도록 하였다.

제시된 프로세스는 증명 프로그램의 소프트웨어 관점에 집중했다. 증명 프로그램에는 많은 안전 관련 및 비 안전관련 사항들이 발생된다. 마찬가지로 미국 내에서의 형식증명 프로세스에 중점을 두었으나 제시된 프로세스는 비 형식증명 관련 사항 국제적인 프로젝트에 적용 가능함을 첨언한다.

[참고문헌]

1. 한상호(2004), "항공전자부품의 감항성 인증", 『항공산업연구소』, 제67집, 세종대학교 항공산업연구소
2. ARINC(1993), ARINC Report 652, *Guidance for Avionics Software Management*, ARINC
3. FAA(2003), FAA Order 8110.49, *Software Approval Guidelines*
4. Leanna K. Rierson(1998), *Partnering to Improve the Software Approval Process for Aircraft Certification*
5. RTCA(1992) RTCA DO-178B, *Software Considerations in Airborne Systems and Equipment Certification*
6. Software Review Job Aid - Conducting Software Reviews prior to certification (2004) Rev 1, FAA Aircraft Certification Service(AIR)
7. FAA(2001), *The FAA and Industry Guide to Avionics Guide*