항공우주산업기술동향 5권1호 (2007) pp. 15~24
기술동향
www.kari.re.kr
/lib/index.html
에서 보실 수 있습니다.

항공용 S/W 개발 및 인증 기술동향

글 / 박 무 혁 mhpark@kari.re.kr
한국항공우주연구원 항공사업단 KHP개발실 세부계통팀

초 록

항공용 소프트웨어의 개발 및 인증은 현재까지 국내에서는 거의 경험이 없는 분야이다. 물론 각종 무인기 등의 개발사업을 통해 항공용 소프트웨어를 개발하고 시험한 사례는 다수 있으나, 체계적으로 개발 및 시험된 경우는 흔치 않다. 특히 유인기 분야에서는 거의 전무하다고 할 수 있다. KFP, KT-1, T-50 등의 군 사업을 통하여, 국외에서 개발된 소프트웨어에 대한 유지보수 경험 및 인력과, 이를 위한 체계가 구축되어 있는 정도라 할 수 있다. 이러한 상황에서, 이제는 항공용 소프트웨어를 국내에서 개발하고 시험, 인증할 수 있는 능력의 확보가 요구되고 있으며, 이는 국내 항공산업이 항공기 독자개발 능력 확보를 위해서는 필수적인 핵심기술이다. 이러한 기술력 확보를 위하여, 현재 항공용 소프트웨어 개발과 관련한 세계적인 흐름 및 최신의 기술동향을 파악하는 것이 무엇보다 필요하다. 항공선진국에서 이미 적용하지 않는 규격, 기술, 개발방식을 그대로 따라하는 과정을 거친다면, 경쟁력 확보는 요원한 일이기 때문이다.

따라서 본 논문에서는 항공용 소프트웨어 인증을 위한 규격의 역사 및 종류와, 현재 주로 적용되고 있는 DO-178B에 대한 주요 내용 및 현안에 대하여 살펴보고, 소프트웨어 개발과 관련한 소프트웨어 툴, 모델기반 개발 방식 등 해외 선진업체 및 기관들의 최신 기술동향을 정리하였다.

주제어 : 소프트웨어 개발 및 인증

1. 서 론

항공산업에서 인증이라 함은, 요구되는 각종 규격 및 절차를 만족하였고, 요구되는 안전성을 확보하였음을 확인 받는 절차라 할 수 있다. 군용인 경우, 소요군이 요구하는 운용요구성능 및 각종 군사규격 등을 군이 요구하는 절차 및 규격에 따라 입증하여야 하며, 민간용인 경우, FAR 또는 JAR 등 해당 정부에서 법률화한 요구조건을 만족하기 위하여, 수용 가능한 방법(Acceptable means of compliance) 에 따라 요구조건을 만족하였음을 입증하여야 한다. 국내에는 아직까지 민항기에 대한 인증체계가 수립되지 않았으나, 군용으로는 T-50 등 군 개발사업을 통하여, 군 인증을 획득한 사례가 다수 있다.

항공용 소프트웨어의 개발 및 인증은 현재까지 국내에서는 거의 경험이 없는 분야이다. 물론 각종 무인기 등의 개발사업을 통해 항공용 소프트웨어를 개발하고 시험한 사례는 다수 있으나, 체계적으로 개발 및 인증된 경우는 흔치 않다. 특히 유인기 분야에서는 거의 전무하다고 할 수 있다. KFP, KT-1, T-50 등의 군 사업을 통하여, 국외에서 개발된 소프트웨어에 대한 유지보수 경험 및 인력과, 이를 위한 체계가 구축

되어 있는 정도라 할 수 있다. 이러한 상황에서, 이제는 항공용 소프트웨어를 국내에서 개발하고 시험, 인증할 수 있는 능력의 확보가 요구되고 있으며, 이는 국내 항공산업이 항공기 독자개발 능력 확보를 위해서는 필수적인 핵심기술이다. 이러한 기술력 확보를 위하여, 현재 항공용 소프트웨어 개발과 관련한 세계적인 흐름 및 최신의 기술동향을 파악하는 것이 무엇보다 필요하다. 항공선진국에서 이미 적용하지 않는 규격, 기술, 개발방식을 그대로 따라하는 과정을 거친다면, 경쟁력 확보는 요원한 일이기 때문이다.

따라서 본 논문에서는 항공용 소프트웨어 인증을 위한 규격의 역사 및 종류와, 현재 FAA가 S/W인증을 위하여 요구하고 있는 DO-178B에 대한 주요 내용 및 현안에 대하여 살펴보고, 소프트웨어 개발과 관련한 소프트웨어 툴, 모델기반개발 방식 등 해외 선진업체 및 기관들의 최신 기술동향을 정리하였다.

2. 항공용 S/W 인증 규격 동향

2.1 인증규격의 종류

항공용 고신뢰성 소프트웨어의 인증을 위하여, 다양한 소프트웨어 규격이 만들어 졌으며, 적용되어 왔다. 이러한 규격들은 군용 및 민간용, 미국, 유럽의 규격이 있으며, 시대에 따라 적용되었고 취소되기도 하였다. 이러한 규격들은 크게 3가지 유형으로 분류가 가능하며, 다음과 같다.

표 1. 인증규격의 종류 및 특징

종류	특징	관련규격
Assessment Standards	S/W개발자의 능력 및 성숙도에 대한 질 및 적절성 평가	CMM ISO-9000-3
Development Standards	S/W개발 프로세스에 대한 반복 가능한 지침 제공	MIL-STD 2167A/2168/498 IEC 12207 (FAA-STD-026) DEF-STD 055/056
Assurance Standards	S/W개발 프로젝트에 있어서 특정 속성을 달성하기 위한 방법 제공	DO-178B DO-278 IEC 61508

평가규격(Assessment Standards)은 소프트웨어를 개발하는 기관의 소프트웨어 개발 능력 및 품질의 적절성을 평가하기 위한 규격으로서, Capability Maturity Model (CMM), ISO 9000-3 등이 여기에 속한다.

개발규격(Development Standards)은 순차적이고 반복 가능한 소프트웨어 개발 프로세스에 대한 지침을 제공하기 위한 규격으로서, MIL-STD-2167/ 2167A /2168/498, DEF-STD 055/056등의 군용 규격과, IEC 12207(FAA-STD-026)이 민간용 규격으로서 여기에 속한다. 개발규격은 개발프로세스 동안 생성하여야 할 문서 및 자료들을 정의하며, 소프트웨어 유지보수에 유용하다. 다음 그림은 개발규격이 MIL-STD- 2167A로 시작해서, IEC 12207이 제정된 과정을 보여준다.

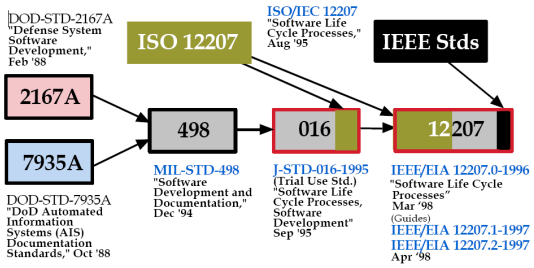

그림 1. IOC/IEC 12207

보증규격(Assurance Standards)은 소프트웨어 개발 프로젝트에 있어서, 특정한 속성(Attributes)을 달성하기 위한 방법을 제공하는 규격으로서, 어떻게(HOW) 보다는 무엇을(What) 수행하여야 할 것인가를 정의한다. DO-178B, DO-278, IEC 61508등이 여기에 속한다. 보증규격은 안전성 및 법규(regulation)를 만족할 수 있는 방법을 제공하며, 측정 기준을 제시한다.

이와 같은 규격의 3가지 종류에 대하여 시대적으로 나열해 보면 다음과 같다.

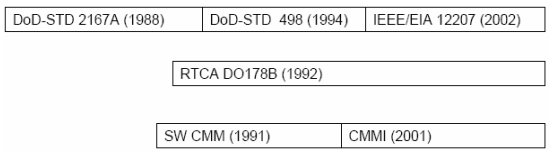

그림 2. S/W 인증규격 역사

이상과 같은 유형들의 규격들은 각 특성에 따라 장단점이 있다. 현재 항공용 고신뢰성 소프트웨어 개발에 적용되는 이러한 규격들에 대하여 간단히 살펴보면 다음과 같다.

CMM(Capability Maturity Model)

개발성숙도 및 능력을 결정하기 위한 프로세스와 개발 효율, 소프트웨어 질(quality)을 개선하기 위한 수단을 제공한다. 다섯 단계의 성숙도(maturity) 수준이 있으며, 핵심 프로세스 분야에 대하여 독립적으로 평가한다. 다음 그림은 5단계의 CMM level을 보여준다.

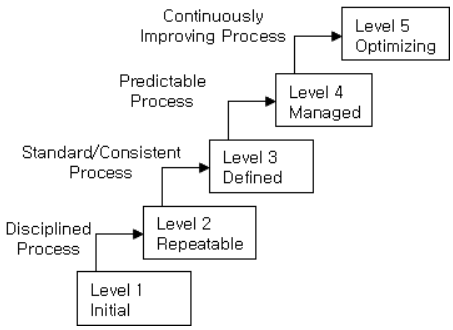

그림 3. CMM 5단계 Level

Level 1은 개인의 개발능력에 따라 소프트웨어의 질이 결정되는 단계로 핵심프로세스 분야 자체가 없다. 여기서 지침화 된 절차에 따라 개발하는 단계가 되면 Level 2가 되며, 사업관리의 측면에 초점이 맞춰진 경우다. Level 3는 규정화된 일관성 있는 프로세스가 정립된 경우에 해당한다. 엔지니어링 프로세스에 초점을 두며, Level 4는 산출물 및 프로세스의 품질에 대하여 평가가 이루어지며 정량적인 관리가 이루어진다. Level 5가 되면, 지속적인 개선을 통하여, 프로세스를 변경 관리하며, 기술적인 혁신과 결함 방지를 추구할 수 있는 단계이다.

MIL-STD-498, IEEE/EIA 12207

MIL-STD-498은 미 군사규격으로서, 소프트웨어 개발 및 문서화에 대한 단일화된 요구조건을 정립하는 목적으로 제정되었다. 1994년 11월에 공표되었으며, DOD-STD-2167A, -7935A 등을 대체(replace)하였다. 이 규격은 당초부터 상용규격이 제정되기까지 약 2년 동안만 적용할 예정이었으며, 1998년 5월 J-STD-016과 IEEE 12207로 대체되면서 취소되었다. 하지만 이 규격은 표준화된 문서가 무료로 공개되어 있어 미군 이외의 분야에서 수행하는 사업에는 그 후에도 지속적으로 사용되었다. MIL-STD-498에서는 22개의 산출물을 요구하고 있으며, 각 산출물들의 표준양식 및 포함되어야 할 내용들을 Data Item Description이라는 문서에 정의하였으며, 이것이 이 규격의 핵심이라고 할 수 있다.

IEEE/EIA 12207(Standard for Information Technology-Software Life Cycle Processes)은 소프트웨어 생명주기 프로세스의 일반적인 프레임워크(framework)를 규정하는 규격으로서 1998년 8월에 공표되었다.

DO-178B/DO-278

RTCA의 문서인 DO-178B는 FAA 및 국제인증기구에 의해 인증규정 만족을 위한 수단으로 채택되었으며, 안전필수시스템의 소프트웨어에 대하여 최소한의 규정으로 간주된다. DO-278은 DO-178B에 매우 유사하며, 단지 지상시스템에 적용되는 것이 다르다. DO-178B에 대한 자세한 내용은 2.2절에 정리하였다.

인증규격간의 관계

이상에서 살펴 본 바와 같이 다양한 규격들이 존재하며, 현재 FAA에서 요구하고 있는 DO-178B와 타 규격들 간의 관계를 개략적으로 살펴보면 다음 그림과 같다.

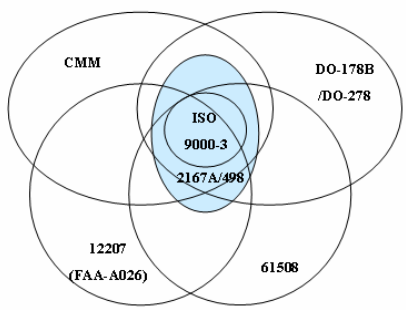

그림 4. 인증규격간의 관계

보는 바와 같이 각 인증규격별로 공통된 부분도 있으나, 차이점도 많이 있다. 따라서, 특정 인증규격으로 인증된 소프트웨어를 다른 인증규격으로 인증 받고자 하는 경우는 이러한 차이점에 대한 차이분석(Gap Analysis)을 수행하고, 차이에 대한 인증절차를 수행하여야 한다.

2.2 DO-178B

DO-178B의 역사

RTCA/DO-178B "Software Considerations in Airborne Systems and Equipment Certification"은 항공기 탑재 소프트웨어에 대한 FAA 인증 획득을 위해서 준수하여야 할 지침으로서, 1992년 12월 제정되었다. 이 문서는 RTCA와 EUROCAE의 합의하에 국제적 적용을 위하여 개발되었으며, 미국 캐나다, 유럽의 항공업계에서 주로 참여하였다. 이 규격은 1993년 1월 FAA문서인 AC 20-115B에서 FAR에 부합하기 위한 지침으로 채택되었으며, 대부분의 항공업계에서 채택되어 사용되고 있다. DO-178B의 제정 과정을 보면, 다음과 같다.

표 2. DO-178B 제정 과정

규격	주요내용	년도
DO-178	기본적인 절차	1980
DO-178A	소프트웨어 엔지니어링 관련 원칙 강화. Verification 및 Validation 개념적용	1985
DO-178B	"어떻게" 보다는 "무엇을"에 중점, Validation 개념은 제외	1992
DO-248	DO-178B 관련 FAQs 및 명확화	2001
DO-278	지상용 CNS/ATM 소프트웨어에 대한 DO-178B 적용 관련	2002

DO-178B는 소프트웨어 기술이 급격히 발전하고 있고, 그 규모 및 복잡성이 증가하고 있으며, 더욱 더 많은 비행안전과 관련된 분야에서 사용되고 있는 현실에서 그 중요성이 부각되고 있다.

DO-178B 소프트웨어 생명 주기 프로세스(Life Cycle Processes)

DO-178B에서 요구하는 소프트웨어의 생명 주기 프로세스는 개발프로세스와 통합프로세스(Integral Process)로 구성되며, 다음 그림과 같다.

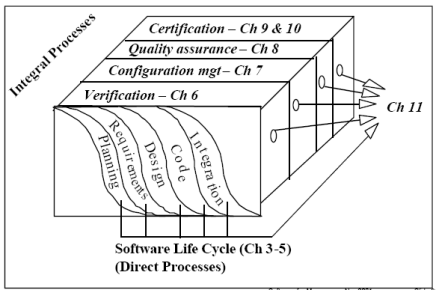

그림 5. DO-178B S/W 생명주기프로세스

개발 프로세스는 소프트웨어 계획 단계, 요구조건 단계, 설계 단계, 코딩 단계 및 통합/시험단계로 구성되며 이와 병행하여 통합 프로세스가 진행된다. 통합 프로세스는 그림에서 보는 바와 같이 검증(Verification),형상관리(Configuration Management), 품질보증(Quality Assurance) 및 인증(Certification) 활동이 포함된다. 개발 프로세스와 통합 프로세스가 진행되면서 생성된 문서들은 소프트웨어 생명주기 산출물로서 11장에 정의되어 있다.

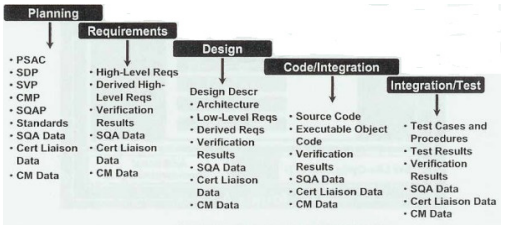

그림 6. DO-178B S/W 생명주기 프로세스별 산출물

DO-178B 소프트웨어 Level 및 신뢰성

DO-178B에서는 소프트웨어를 5개의 Level로 분류한다. 이러한 분류는 소프트웨어 탑재장비의 안전성 및 신뢰성 카테고리에 따라 결정되며, 이는 항공기 개발 프로세스 중 시스템 안전성 평가(System Safety Assessment) 프로세스에 의하여 결정된다.

DO-178B는 소프트웨어의 신뢰성을 확인하기 위한

설계보증(design assurance) 규격이므로, 소프트웨어의 신뢰성 Level은 해당 탑재장비의 신뢰성 Level을 따른다. 다음은 ARP 4761과 AC 25.1309에서 정의하는 H/W 카테고리와 그에 대응하는 DO-178B 소프트웨어 Level이다.

표 3. DO-178B S/W Level

ARP4761 Category	ARP4761 안전/신뢰성	DO-178B S/W Level	# of DO-178B Objective
Catastrophic	10^{-9}	A	66
Hazardous	10^{-7}	B	65
Major	10^{-5}	C	57
Minor	10^{-3}	D	28
No Effect	don't care	E	0

ARP 4761과 AC 25.1309에서 정의하는 H/W 카테고리는 FAR 25.1309에서 요구하는 항공기 시스템 또는 그 구성품에 대한 설계보증(design insurance)를 위한 분류로서, H/W에 적용되는 분류이다. 이러한 분류는 해당 H/W에 탑재되는 S/W의 분류와 동일하여야 하며, 따라서, DO-178B에서는 S/W의 Level을 이에 따라 분류하였다.

DO-178B Objectives

DO-178B는 보증규격(Assurance Standard)에 해당한다. 따라서 달성하여야 하는 속성들을 정의하고 있으며, 이는 objective 들로 이루어진다. 이러한 objective들은 개발 대상 소프트웨어의 Level에 따라 그 적용 objective가 달라진다.(표 3 참고) DO-178B의 objective들은 DO-178B Annex A에 프로세스별로 10개의 Table로 정리되어 있으며, Level 별 만족하여야 할 objective들과, 산출물, 형상통제 카테고리 등이 요약되어 있다. 다음 표는 각 Table을 보여준다.

표 4. DO-178B Annex A Tables

Table	제 목
A-1	Software Planning Process
A-2	Software Development Process
A-3	Verification of Requirements Process
A-4	Verification of Design Process
A-5	Verification of Coding/Integration Process
A-6	Testing of Integration Process
A-7	Verification of Verification Process Results
A-8	Software Configuration Management Process
A-9	Software Quality Assurance Process
A-10	Certification Liaison Process

DO-178B Level 별 주용 objective들을 살펴보면 다음과 같다.

표 5. DO-178B Objectives & Assurance

Level	주요 objectives & assurance
Level A (66)	Additional Independence Modified Condition/Decision Coverage Source to object code traceability
Level B (65)	Compatibility with target computer Source code verifiability Decision Coverage Evaluate transition criteria
Level C (57)	Development standards Verify requirement and design Test low-level requirements Ensure correctness of test cases & results Coordinate plans & include transition criteria Statement Coverage Data & control coupling analysis Develop transition criteria
Level D (28)	Planning Configuration Management & Quality Assurance High-level req. coverage & robustness Target compatibility testing Tool qualification

DO-278

DO-278은 “Guidelines for CNS/ATM Systems Software Integrity Assurance”로서, 2002년 3월에 제정되었다. CAN/ATM 시스템 중 지상장비 운용 소프트웨어의 개발에 적용을 목적으로 하며, DO-178B를 기초로 제정하였다. DO-278은 적용 데이터(Adaptation Data)와 COTS 소프트웨어에 대한 내용을 추가적으로 포함하였으며, DO-178B에 비하여 하나의 소프트웨어 레벨이 더 있다. DO-178B objective 중 일부를 수정하였으며, 일부 objective들에 대하여 독립성을 추가로 요구하였고, 지상용임을 고려하여 이에 적합하도록 용어(Terminology)를 수정하였다.

다음 그림은 DO-178B와 DO-278의 소프트웨어 Level 비교를 보여준다. DO-278에서는 보증레벨(Assurance Level)이라는 용어를 사용한다.

표 6. DO-278 vs DO-178B Level

DO-278	DO-178B
AL1	Level A
AL2	Level B
AL3	Level C
AL4	No Equivalent Level
AL5	Level D
AL6	Level E

2.3 DO-178C

2005년 봄 RTCA Special Committee #205 (SC-205)가 만들어졌다. 이 위원회는 EUROCAE Working Group #71(WG-71)과 통합(Joint) 운영되며, 그 목적은 다음과 같다.

- 항공 소프트웨어의 안전 구현 증진
- 시스템 개발 프로세스와 안전 프로세스간의 명확하고 일관된 연계 방안 제공
- 새로운 소프트웨어 동향 및 기술에 대한 접근
- 기술발전 및 변화를 따라갈 수 있는 접근방법 구현

이 위원회에서는 현재 산업계가 직면하고 있는 새로운 소프트웨어 기술 관련 이슈들을 다룰 예정이며, 주요 이슈들은 다음과 같다.

- 객체지향(Object Oriented) 기술
- 외주(Outsourcing) 및 Off-Shore 개발
- 모델기반 개발(Model-Based Development)
- 증가하는 소프트웨어 툴 사용
- RTOS 및 다른 COTS 구성품들의 사용

이러한 이슈들에 대한 연구를 통하여, 기술에 독립적인 핵심 Objectives와 이에 대한 지침(description)을 가능한 한 DO-178B의 Objectives와 가깝게 유지하면서, RTCA/ EUROCAE의 DO-178C/ED-12C와, DO-248C/ ED-94C로 제정하고, 특정 기술에 종속되는 부분에 대해서는 관련 지침을 Objectives와 함께 Supplements 형태로 제시할 계획이다. 이는 2008년 12월 1일을 목표로 추진 진행되고 있다.

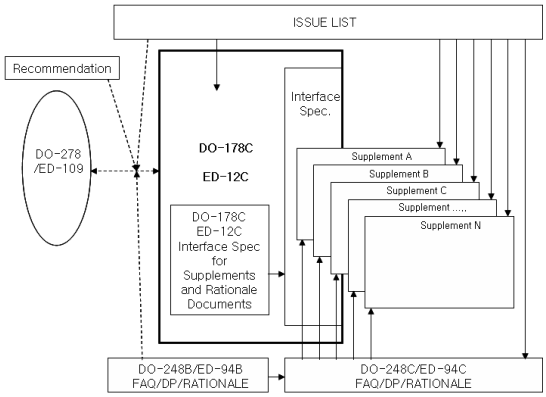

그림 7. DO-178C 제정 방안

3. S/W 개발 관련 기술 동향

3.1 소프트웨어 툴

DO-178B에서 정의하고 있는 소프트웨어 툴은 다른 소프트웨어 프로그램 또는 해당 문서를 개발, 시험, 분석, 산출 또는 수정할 때 사용되는 컴퓨터 프로그램으로 정의한다. 툴은 개발 또는 검증(verification) 프로세스 상의 일부 업무를 제거하거나, 줄이거나, 자동화하는 목적으로 사용된다. DO-178B는 다음과 같은 두 종류의 소프트웨어 툴을 정의한다.

1) 소프트웨어 개발 툴
   ; 툴의 결과물이 항공탑재용 소프트웨어의 일부분으로서, 에러를 유발할 수 있는 툴
2) 소프트웨어 검증 툴
   ; 에러를 유발할 수는 없으나, 에러를 찾는데 실패할 수 있는 툴

현재 소프트웨어 툴과 관련하여 다양한 새로운 움직임이 있으며, 이로 인하여 많은 이슈들이 제기되고 있다. 기술이 발전함에 따라 더욱 많은 툴들이 사용되기 시작하였다. 툴을 이용하여 개발함으로써, DO-178B에서 요구하는 개발 방식을 벗어나거나, DO-178B에 정의되지 않은 다른 범주에 속하는 툴(안전성 평가, 형상관리, 통합, 데이터베이스 등)의 사용이

빈번하게 발생하였다. 또한 다양한 툴들이 장비 개발 업체가 아닌 제3의 공급업체/제작사에 의해 개발되고 있으며, 이러한 툴 공급업체들은 복수개의 소프트웨어 개발 프로그램에 적용할 수 있도록 툴 자체에 대한 인증을 요구하고 있다. 이러한 소프트웨어 툴은 소프트웨어 개발과정에서 사람의 개입을 최소화하는 방향(시험까지 자동화하는 방향으로)으로 진행되고 있다. 현재 세계적으로 많이 사용되고 있는 소프트웨어 툴들은 다음과 같다.

표 7. 주요 소프트웨어 툴

툴 이름	개발자	용도
DOORS	Telelogic	요구도관리
Synergy	Telelogic	형상관리
ClearCase	IBM	
SCADE	Esterel Tech	모델기반개발
Beacon	ADI	
MATRIXx	NI	
Simulink	Mathworks	
Rhapsody	Telelogic	
LDRA Tool Suite	LDRA	Code Coverage

이러한 툴들의 사용으로 인하여 DO-178B에서 제시하는 인증 기준에 대하여 수정의 필요성이 제기되고 있다.

2004년 5월 Embry-Riddle Aeronautical University (ERAU)에서 소프트웨어 툴 포럼이 개최되었다. 이 포럼은 ERAU와 FAA의 공동 후원으로 개최되었는데, 항공용 소프트웨어 개발에 사용되는 소프트웨어 툴과, 향후 적용이 예상되는 새로운 툴들의 증가로 인하여 발생한 이슈들이 개최 동기가 되었다. 여기에는 미국, 유럽, 캐나다의 인증기관을 비롯하여, 툴 공급업체, 항공전자 및 항공기 개발업체 등에서 약 150여명의 참가자들이 참가하였다. 툴과 관련된 이슈들에 대한 Brainstorm을 통하여, 52개의 주요 이슈들이 도출되었으며, 크게 다음과 같은 6개 분야로 분류되어 우선순위가 결정되었다.

1) DO-178B 상의 개발 툴에 대한 인증 (Qualification) 기준 수정 필요성
2) Model-Based Development에 대한 기준 제정 필요성
3) 특정 프로그램에서 인증(Qualification)된 툴의 다른 프로그램 적용을 위한 인증 기준 필요성
4) Autocode generator의 사용 및 인증 방식에 대한 다른 접근방식 문서화 필요성
5) 통합 툴(Integration Tool)관련 이슈
6) 기타 툴 관련 이슈

이 포럼의 결과로 FAA는 우선순위 1~ 5까지에 대하여, 현실적으로 가능한 범위 내에서 최대한 빨리, 정책(policy) 및 지침(guidance)에서 다루기로 하였으며, 우선순위 6에 대해서는 긴급한 사항이 아니므로, 필요시 추가적인 연구를 통하여 미래에 고려하겠다는 입장을 표명하였다. 이 포럼에서 결정된 사항들이 항공용 소프트웨어 분야의 공통된 의견이라 할 수 는 없지만, FAA가 툴과 관련하여 향후 추진할 업무에 충분히 중요한 정보를 제공하였다고 할 수 있다. FAA가 추진할 수 있는 다음 스텝은 DO-178B/ED-12B 를 수정(update)하거나, 소프트웨어 툴과 관련한 새로운 전용 지침을 제정하거나, 특정 툴 이슈들 관련한 연구업무를 정의하는 3가지 중의 하나일 가능성이 매우 높은 것으로 이 포럼에서는 예측하였으며, FAA는 현재 소프트웨어 개발 툴 및 검증 툴에 대한 연구를 후원하고 있으며, 새로운 RTCA 위원회(SC-205/WG-71)는 툴에 대한 지침 제정을 계획하고 있다.

3.2 모델기반개발 방식 (Model Based Development)

DO-178B의 개발 프로세스에 따라 상위요구도를 정의하고, 이에 대하여 하위요구도를 작성하며, 코딩 및 시험을 수행하는 전통적인 소프트웨어 개발 방식은 근래에 들어, 다양한 소프트웨어 개발 툴을 적용함에 따라 크게 변화되고 있다.

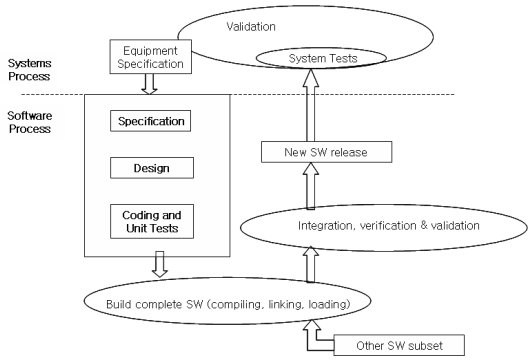

그림 8. 전통적 소프트웨어 개발 방식

이러한 변화의 대표적인 예가 모델 기반 개발(Model-Based Development : MBD) 방식이다.

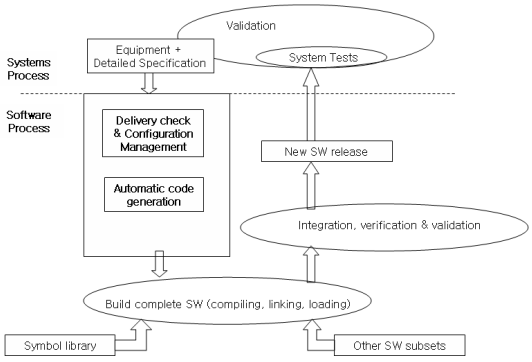

그림 9. 모델기반 소프트웨어 개발 방식

그림에서 보는 바와 같이 모델기반개발 방식과 기존 개발 방식의 가장 큰 차이점은 소프트웨어 규격 작성, 설계/ 코딩 과정을 툴을 이용하여 자동화 하는 것이라 할 수 있다. 모델기반개발 툴은 하드웨어 규격으로부터 직접 특정 모델을 기반으로 설계를 수행하고, 이 모델들로부터 코드를 자동 생성한다. 전통적인 방식에서의 소프트웨어 단위시험은 작성된 코드에 대해서 수행하는데, 모델기반개발 방식에서는 이 시험을 수행하지 않는다. 시험은 모델 자체에서 수행하며, 시험결과는 즉시 반영함으로써, 개발기간을 단축할 수 있다. 또한 자동코드생성기를 사용함으로써, 코딩 단계에서 발생 가능한 개발자 실수에 의한 오류를 방지할 수 있다.

소프트웨어 개발 시, 소프트웨어 구조(Architecture)를 먼저 정의하여야 한다. 전체 소프트웨어를 기능별 프로세스로 나누어 이를 소프트웨어 단위(unit)로 할당하고, 이들 간의 데이터 흐름 및 제어 흐름을 표시함으로써, 소프트웨어 구조를 정의할 수 있는데, 이를 위한 방법론은 Yourdan-DeMacro, Hatley-Pirbhai, Object Modeling Technique 등 여러 가지가 있다. 이러한 방법론들은 각각 특정 모델을 이용하는데, 어떤 모델은 요구조건을 위주로 하는가 하면 어떤 모델들은 요구조건 보다는 설계에 더 치중하는 등 모델에 따라 그 특성이 다르다. 다음은 모델들의 예이다.

- Structured
- Context Diagram
- Data Flow
- Control Flow
- State Diagram

다음 그림은 Data Flow Diagram과 Data Context Diagram의 예를 보여준다.

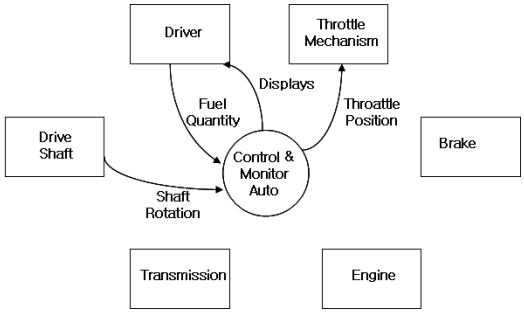

그림 10. Data Flow Diagram

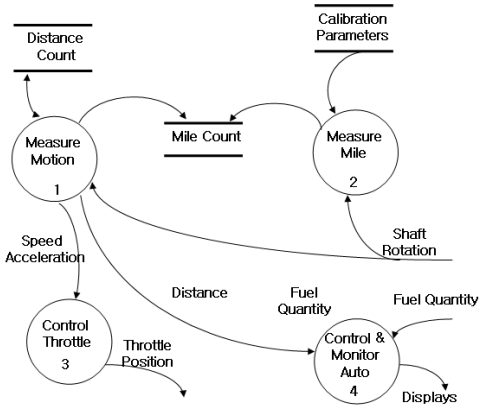

그림 11. Data Context Diagram

모델기반개발 툴은 이러한 모델을 이용하여 직접 설계/시험할 수 있는 편리한 기능을 제공한다.

SCADE Suite는 DO-178B Level A 소프트웨어 개발에 성공적으로 적용되었던 MBD 툴로서, Esterel Technologies사 제품이며, 현재 상용화되어 판매되고 있다. Esterel Technologies사는 1999년 11월에 설립된 회사로서, SCADE의 개발로 세계 항공용 소프트웨어 개발 툴 시장에서 주도적인 위치를 차지하고 있다. 또한 SCADE suite를 simulink, Altia 설계 툴, 주요 형상관리툴, DOORS 등 각 분야별로 시장을 주도하고 있는 다른 툴들과 쉽게 통합이 가능하도록 설계함으로써, 그 지위를 확고히 하고 있다. 다음 그림은 SCADE Suite를 사용하여 소프트웨어 개발 시 적용 과정을 보여준다.

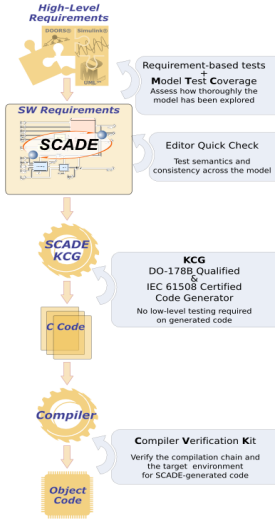

그림 12. SCADE를 이용한 모델기반방식 S/W 개발

그림에서 보는 바와 같이 SCADE는 소프트웨어 상위 요구조건으로부터 직접 모델기반으로 설계를 수행한다.

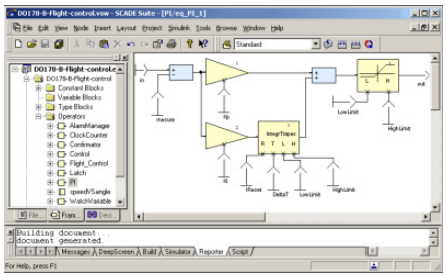

그림 13. Data Flow Editor

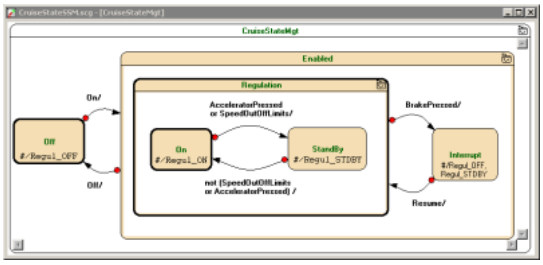

그림 14. State-transition diagram editor

DO-178B에서는 상위요구조건 정의, 하위요구조건 정의, 코딩, 시험의 순으로 각 단계에 해당하는 문서를 작성하고, 추적성을 확보 관리하며, 시험결과 반영하여 코딩 및 시험을 반복한다. 이때, 수행하여야 할 시험에는 Requirement based tests와, Structural Code coverage test를 수행하여야 하는데, 여기에는 매우 많은 시간이 소요된다. 그러나, SCADE에서는 상위요구조건으로부터 작성된 모델에 대하여, 바로 Requirement based test와, Model coverage test를 수행한다.

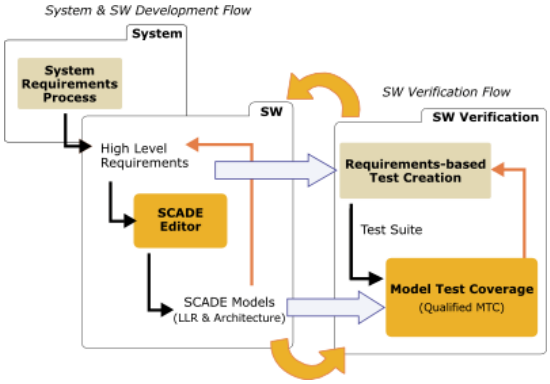

그림 15. SCADE Model Test Coverage

모델에 대한 시험이 완료되면, 자동코드생성기를 이용하여, 코드를 생성하며, 이 코드에 대해서는 시험을 수행할 필요가 없다. 코드를 컴파일하여 Object 코드를 생성하며, 이때 컴파일러 검증 키트을 사용하여 검증함으로써 개발을 완료한다. 이러한 모델기반개발 개념은 Mathworks사의 Simulink에서도 거의 동일한 방식으로 적용되었다.

다음은 모델기반개발방식을 적용하여 개발한 사례 및 성과이다.

표 8. 모델기반개발 사례 및 결과

회사	Product	Tools	Autocoded	Tool
Airbus	A340	SCADE with Code generator	- 70% FBW controls - 70% AFC - 50% Display computer - 40% Warning & Maintenance Computer	20x 에러줄임 개발기간 단축
Euro copter	EC-155 /135 Autopilot	SCADE with Code generator	-90% Autopilot	50% 개발기간 단축
GE & Lock -heed	FADEC Engine Controls	ADI Beacon	-Not Stated	에러 줄임 50% 개발기간단축 비용절감
Honey well	Primus Epic FCS	MATLAB Simulink	-60% AFC	5x생산성 증가 코딩에러 0 FAA 인증획득

AFC : Automatic Flight Controls,
FCS : Flight Control System

위의 표에서 보는 바와 같이 Airbus, Eurocopter, GE, Lockheed 등 주요 해외 선진업체들이 모델기반 개발 방식을 적용하고 있으며, 이를 통하여, 비용절감 및 개발기간을 단축하고 있다. 이러한 장점들로 인하여, 모델기반개발 방식은 시대적인 흐름이 되어가고 있다. 이에 따라, 이 방식으로 개발하는 소프트웨어에 대한 인증 기준의 제정 필요성이 제기되고 있으며, 해당 소프트웨어 툴에 대한 DO-178B 인증 기준도 이슈화 되고 있다. 현재 툴 개발업체들은 자사의 툴이 DO-178B 인증을 획득한 것처럼 발표하고 있으나, 이는 특정 개발사업에서 이 툴을 적용하여 개발된 소프트웨어가 인증을 획득하였음을 의미하는 것이며, 모든 사업에 일반적으로 적용 가능한 툴 자체에 대한 인증은 기준도 정의되지 않은 상태이다.

4. 결 론

이상에서 살펴본 바와 같이 항공용 소프트웨어의 개발 및 인증은 지금 변화기에 접어들었다고 할 수 있다. 1992년 DO-178B가 제정된 이 후, 15년이 지났고, 이미 그 실효성을 상실해가고 있으며, 새로운 소프트웨어 관련 기술 및 툴의 등장으로, 기업들의 개발 방식이 변화되고 있다. 또한 이러한 시대의 흐름에 따라가기 위해 신기술을 이용한 개발방식에 대한 인증을 위하여, 새로운 인증 기준의 제정이 요구되고 있으며, 이 작업이 구체적으로 진행되고 있다. DO-178C의 제정 및 적용이 시작되는 2009년부터 이러한 흐름은 더욱 가속화될 것으로 예상된다. 해외 선진업체 및 관련 기관들의 이러한 움직임에 국내 항공업계 소프트웨어 개발 분야에서는 주목할 필요성이 있으며, 그 흐름에 뒤처지지 않도록 최신 기술적용을 적극적으로 고려하여야 한다. 국내 관련분야에서는 이제 겨우 DO-178B에 대한 관심을 갖기 시작하는 단계이며, 아직까지 이의 적용을 주저하는 현실을 감안하면, 해외선진업체에 비해 최소 15년 이상 뒤처져 있다고 할 수 있다. 물론 항공용 소프트웨어 개발 및 국제적 인증 획득 경험이 많지 않은 국내에서 단숨에 선진국 수준을 따라간다는 것은 쉽지 않을 것이다. 그러나, 선진업체들이 기존의 DO-178B의 개발방식 보다는 현재까지 인증기준이 제대로 정립되지 않은 신기술을 적용하여 개발하는 이유가 개발기간 단축 및 비용 절감 등의 장점이 있기 때문임을 생각하면, 국내에서도 이러한 개발방식을 적극 고려하여야 경쟁력을 확보할 수 있을 것으로 판단된다. 본 논문의 내용이 국내 관련분야에서 세계적인 흐름을 인식하고, 그 추세에 따라감으로써, 최단기간 내에 경쟁력을 확보하는데 도움이 되기를 바란다.

참고문헌

1. Dr. Steven P.Miller, “Proving the Shalls : Requirements, Proofs, and Model-Based Development”, Rockwell Collins, spmiller@rockellcollins.com
2. Mike DeWalt, “Model-Based Development(MBD) Coming soon to a theater near you- Resolving MBD against DO-178B), Certification Services Inc., Mike. DeWalt@certification.com
3. 박무혁, “고신뢰도 소프트웨어 인증규격 및 시험기술 연구 (KARI-CAG-TM-2006-014)”, 한국항공우주연구원, 2006
4. Esterel Technologies사 Newsletter Q2-2004 (http://www.esterel-technologies.com/files/Newsletter-Q2-2004.pdf)