DO-278A 표준 기반 A-SMGCS(항공기 지상이동유도 및 통제시스템) 개발방법에 관한 연구

강호영*, 이석찬*, 김태원*, 신용학*
*LS산전 안양연구소 시스템S/W연구단
e-mail: hykang@lsis.com

A Study on Method for Developing DO-278A Compliant A-SMGCS Software

Ho-Young Kang*, Seok-Chan Lee*, Tae-Weon Kim*, Yong-Hark Shin*
*System Software R&D Center, LSIS Co., Ltd.

요 약

RTCA DO-278A는 통신, 항법, 감시 및 항공 교통 관리(CNS/ATM) 시스템과 장비에 대한 비항공용(지상 및 우주) 소프트웨어의 무결성을 보장하기 위한 개발 지침을 제공한다. 안전하고 효율적인 공항운영을 위한 차세대 지상이동 관제시스템인 A-SMGCS는 DO-278A의 무결성 보장 고려사항을 준수하여 개발되어야 한다. 본 논문에서는 소프트웨어 개발 수명 주기 전체에 걸쳐 DO-278A의 소프트웨어 무결성 보장 고려사항을 반영한 A-SMGCS 개발 방법을 제안한다.

1. 서론

국제민간항공기구(ICAO)에서는 항공기 지상이동유도 및 통제시스템(이하 A-SMGCS)을 저시정 상태 등의 시정 등급과 상관없이 안전 수준을 유지하며 공항 이동 구역에서의 항공기와 차량 등을 유도하기 위한 감시, 경로, 안내, 통제 기능 을 가진 시스템으로 정의하고 있다.[1]

RTCA DO-278A[2]는 통신, 항법, 감시 및 항공 교통 관리(CNS/ATM) 시스템과 장비에 대한 비항공용(지상 및 우주) 소프트웨어의 무결성을 보장하기 위한 개발 지침 및 안전성 확신 레벨에 적합한 소프트웨어 개발 권고를 포함하고 있으므로 국제민간항공기구(ICAO)에서 2004년에 발간한 ICAO Doc 9830(ICAO A-SMGCS Manual)[1]에서 정의하는 A-SMGCS 구현 레벨 IV급의 A-SMGCS 소프트웨어를 개발할 때, 개발 수명 주기 프로세스(개발계획, 요구분석, 설계, 구현, 검증 및 확인, 형상관리, 품질보증 등)에서 DO-278A의 소프트웨어 무결성 보장 고려사항을 포함한 개발 방법을 제안하고자 한다.

2. 관련 연구

A-SMGCS 시스템 개발과 관련된 연구 및 DO-278A에 대한 연구를 살펴본다.

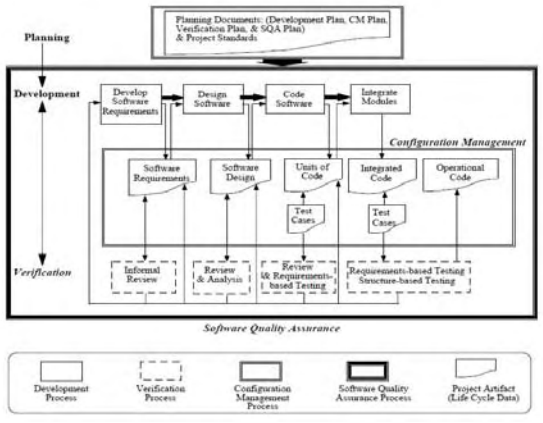
유럽지역에서는 2000년대 초반부터 A-SMGCS 프로젝트를 진행하고 있으며 특히, Eurocontrol의 EMMA2[3] 프로젝트는 총 4단계로 구분하여 2015년까지 레벨 IV급 A-SMGCS 개발을 목표로 하고 있고 미국에서는 NextGen이 ATM 부분에서 지상이동체의 효율적인 관리를 위한 연구를 진행 중이다.

항공분야 소프트웨어 안전성 인증 기준에는 실질적인 국제 표준으로 인정받고 있는 DO-178B가 있으며 이와 함께 지상용 소프트웨어 인증 기준으로는 DO-278A가 있다. DO-278A는 지상용임을 고려하여 이에 적합하도록 DO-178B를 수정하였으며 보증 레벨(Assurance Level) 개념을 도입하여 각 소프트웨어 레벨에서 획득해야 할 Objective를 기술하고 있다.

3. A-SMGCS 소프트웨어 개발 수명 주기

3.1 소프트웨어 수명 주기

DO-278A를 적용하여 개발하기 위한 소프트웨어 개발 수명 주기 참조모델은 그림 1과 같으며 A-SMGCS 개발을 위한 소프트웨어 개발 수명 주기는 DO-278A에서 정의하는 모든 소프트웨어 개발 수명 주기 프로세스를 포함



<그림 1> 소프트웨어 개발 수명 주기 참조모델

해야 하고 개발 단계별로 각 프로세스의 활동을 선택하고, 활동의 순서를 지정하고, 활동의 책임을 할당하여 정의해야 한다.

3.2 소프트웨어 개발 수명 주기 프로세스

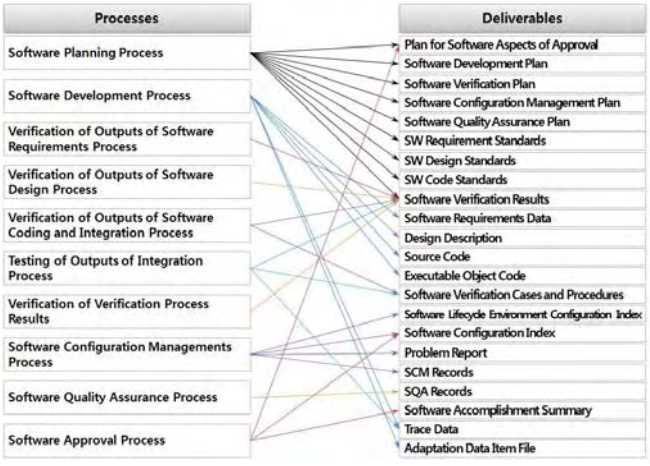
DO-278A에서 정의하는 소프트웨어 개발 수명 주기 프로세스는 표 1과 같다. 각 프로세스에 대한 프로세스 정의서에는 달성되어야 할 목표, 진입조건(Entry Criteria), 탈출조건(Exit Criteria), 입력물(Inputs), 출력물(Outputs), 활동(Activities)이 명시되어야 한다.

<표 1> 소프트웨어 개발 수명 주기 프로세스

	Process
A-1	Software Planning Process
A-2	Software Development Process
A-3	Verification of Outputs of Software Requirements Process
A-4	Verification of Outputs of Software Design Process
A-5	Verification of Outputs of Software Coding and Integration Process
A-6	Testing of Outputs of Integration Process
A-7	Verification of Verification Process Results
A-8	Software Configuration Managements Process
A-9	Software Quality Assurance Process
A-10	Software Approval Process

3.3 소프트웨어 개발 수명 주기 산출물

소프트웨어 개발 수명 주기 상의 모든 프로세스는 달성되어야 할 목표와 산출물을 명시해야 한다. 그림 2는 각 프로세스에서 획득되어야 할 산출물을 보여준다.



<그림 2> 소프트웨어 개발 수명 주기 프로세스 산출물

3.4 A-SMGCS 소프트웨어 개발 수명 주기

DO-278A의 무결성을 보장하기 위한 개발 지침을 적용하여 테일러링(Tailoring)한 A-SMGCS 소프트웨어 개발 생명 주기는 그림 3과 같다. 개발 단계는 모듈규격서작성/기본설계, 상세설계/기초구현, 연동시험/상세구현/통합시험, 시제품제작, 종합검증시험, 1차실증, 2차실증, 3차실

그림 3 A-SMGCS 소프트웨어 개발 수명 주기

증으로 구성하고 각 개발 단계의 특정 시점에 마일스톤을 두어 해당 시점에서 나와야 하는 산출물을 검토하도록 한다. 모듈규격서 및 기본설계가 완료되는 시점에서는 ORR(Operation Requirements Review)을 통해 소트트웨어 개발계획 프로세스의 산출물인 PSAA, SDP, SVP, SCMP, SQAP, SR표준, SD표준, Code표준, SVR-계획검토를 리뷰한다. SRR(System Requirements Review)에서는 소프트웨어 요구사항 프로세스의 산출물(SRD와 Trace Data), 소프트웨어 설계 프로세스의 산출물(DD-개념설계서, Trace Data), 소프트웨어 검증 및 확인 프로세스의 산출물(SVR-요구사항검토, SVR-개념설계검토, Trace Data), 소프트웨어 형상관리 프로세스 산출물(SCI, SLECI, SCMR, Problem Report), 소프트웨어 품질보증 프로세스 산출물(SQAR)을 검토한다. SFR(System Functions Review)에서는 소프트웨어 설계 프로세스 산출물(DD-상세설계서, Trace Data), 소프트웨어 구현 프로세스 산출물(Source Code, Trace Data), 소프트웨어 검증 및 확인 프로세스 산출물(SVR-상세설계검토, SVR-소스코드검토, SVCP-단위시험사양서, SVCP-연동시험사양서, Trace Data), 소프트웨어 형상관리 프로세스 산출물(SLECI, SCMR, Problem Report), 소프트웨어 품질보증 프로세스 산출물(SQAR)을 리뷰한다. PDR(Preliminary Design Review)에서는 소프트웨어 구현 프로세스 산출물(Source Code, Trace Data), 소프트웨어 검증 및 확인 프로세스 산출물(SVR-소스코드검토, SVCP-통합시험사양서, SVR-연동시험결과검토, Trace Data), 소프트웨어 형상관리 프로세스 산출물(SLECI, PCMR, Problem Report), 소프트웨어 품질보증 프로세스 산출물(SQAR)을 리뷰한다. CDR(Critical Design Review)에서는 소프트웨어 검증 및 확인 프로세스 산출물(SVCP-확인시험사양서, SVR-단위시험결과검토, SVR-통합시험결과검토, Trace Data), 소프트웨어 형상관리 프로세스 산출물(SLECI, SCMR, Problem Report), 소프트웨어 품질보증 프로세스 산출물(SQAR)을 리뷰한다. TRR(Test Readiness Review)에서는 소프트웨어 검증 및 확인 프로세스 산출물(SVR-확인시험결과검토, Trace Data), 소프트웨어 형상관리 프로세스 산출물(SLECI, SCMR, Problem Report), 소프트웨어

품질보증 프로세스 산출물(SQAR)을 리뷰한다. 다음 마일스톤은 DO-278A에서 규정하는 소프트웨어 개발 수명 주기의 적용 대상이 아니므로 생략한다.

4. A-SMGCS 소프트웨어 개발 방법

4.1 개발 조직의 구성

A-SMGCS 소프트웨어 개발 조직을 구성할 때, 표2와 같이 개발관리자, 개발담당자, 형상관리담당자, 형상통제위원회, 요구사항검토자, 설계검토자, 코드검토자, 테스터, 품질보증관리자 역할을 정의하고 해당 역할에 대해 사람을 할당하고 책임과 권한을 부여한다. DO-278A는 각 소프트웨어 개발 수명 주기 프로세스에서 보장 레벨별 독립적으로 만족해야 하는 목적을 규정하고 있기 때문에 DO-278A의 해당 지침을 만족시키기 위해 요구사항검토자, 설계검토자, 코드검토자, 테스터, 품질보증관리자는 독립적인 조직으로 구성해야 한다.

<표 2> A-SMGCS 소프트웨어 개발 조직의 구성

역할	책임/권한	독립 유무
개발관리자	· 제품의 수명 주기 동안 전반적인 소프트웨어 개발 관리 · 형상관리: 형상항목 식별, 베이스라인 형상감사	×
개발담당자	· 소프트웨어의 요구분석, 설계, 구현, 단위시험, 연동시험, 결함 해결 · 형상관리: 변경 요청 및 확인, 형상항목 변경 업무 수행, 형상감사 시정조치 수행	×
형상관리담당자	· 형상관리 시스템 구축 및 관리, 베이스라인 관리 수행 · 형상통제위원회 회의록 작성	-
형상통제위원회	· 형상통제위원회 구성: 개발조직 + 독립조직 · 변경요청에 대한 심의, 베이스라인 수립 승인	○
요구사항검토자	· 상위 요구사항에 대해 시스템 요구사항 준수 여부 검토 · 상위 요구사항의 정확성, 일관성, 검증가능성, 표준 준수 여부 검토 · 알고리즘의 정확성 검토	○
설계검토자	· 하위 요구사항에 대해 상위 요구사항 준수 여부 검토 · 하위 요구사항의 정확성, 일관성, 검증가능성, 추적가능성, 표준 준수 여부 검토 · 알고리즘의 정확성 검토 · 소프트웨어 아키텍처의 상위 요구사항 호환성 검토 · 소프트웨어 아키텍처의 일관성, 검증 가능성 등 검토	○
코드검토자	· 소스코드에 대해 하위 요구사항 및 소프트웨어 아키텍처 준수 여부 검토 · 소스코드의 검증 가능성, 표준 준수, 추적가능성, 정확성, 일관성 검토 · 소프트웨어 통합 결과의 완전성, 정확성 검토 · 설정 데이터 항목 파일의 정확성, 완전성 검토 · 설정 데이터 항목 파일의 검증 달성 유무 검토	○
테스터	· 실행 목적 코드의 상위 요구사항 준수 여부 검토 · 실행 목적 코드의 하위 요구사항 준수 여부 검토 · 시험 절차의 정확성, 시험 결과의 정확성 검토 · 상위 요구사항의 시험 적용 범위 달성 여부 검토 · 하위 요구사항의 시험 적용 범위 달성 여부 검토 · 소프트웨어 구조의 시험 적용 범위 달성 여부 검토	○
품질보증관리자	· 소프트웨어 수명 주기 전체에 걸친 품질보증 담당 · 형상관리: 형상감사 계획 수립, 형상 감사 수행, 형상감사 보고서 작성	○

4.2 무결성 보장을 위한 주요 활동

소프트웨어 검증 및 확인 프로세스의 활동은 크게 인스펙션, 추적성 검증, 시험으로 구분된다. 인스펙션은 요구사양 인스펙션, 개념설계 인스펙션, 상세설계 인스펙션, 소스코드 인스펙션으로 나눌 수 있다. 요구사양 인스펙션은 SRD(소프트웨어 요구사항 명세서)와 Trace Data를 요구사항 검토자가 문서 리뷰하고 SVR(소프트웨어 검증 결과)에 기록하는 활동이고, 개념/상세설계 인스펙션은 DD(소프트웨어 설계 사양서)와 Trace Data를 설계 검토자가 문서 리뷰하고 SVR(소프트웨어 검증 결과)에 기록하는 활동이고, 소스코드 인스펙션은 소스코드와 Trace Data를 코드 리뷰하고 SVR(소프트웨어 검증 결과)에 기록하는 활동이다.

추적성 검증 활동은 요구사양, 개념설계, 상세설계, 소스코드, 단위시험, 연동시험, 통합시험, 확인시험 간에 추적 데이터가 일관되게 기록되어 추적이 가능한지를 검증하는 활동이다.

시험 활동은 단위시험, 연동시험, 통합시험, 확인시험으로 구분되며, 각 시험에 대한 소프트웨어 검증 케이스 및 절차(단위시험사양서, 연동시험사양서, 통합시험사양서, 확인시험사양서)가 준비되고 이를 바탕으로 시험을 실시하고 그 검증 결과를 SVR(소프트웨어 검증 결과)에 기록하는 활동이다. 특히 단위시험은 개발자에 의한 수행되며 자동화 툴(xUnit Framework 등)을 사용하여 테스트 결과를 자동으로 생성하고 자동 생성된 문서에는 MC/DC 테스트 커버리지가 포함되어야 한다. 연동시험, 통합시험, 확인시험은 테스터에 의해 매뉴얼로 진행되고 해당 결과는 SVR(소프트웨어 검증 결과)에 기록된다.

5. 결론

항공기 지상이동유도 및 통제시스템(A-SMGCS)이 원래 의도한 기능을 수행하는 동시에 수용할 만한 수준의 안전성을 제공하려면 이러한 시스템의 소프트웨어에 대한 무결성 보장을 제공하는 일관되거나 동등한 수단을 정의하고 이에 따라 소프트웨어를 개발해야 한다. 개발 참조표준인 DO-278A는 A-SMGCS 시스템이 요구하는 각종 규격 및 절차를 만족하고 요구되는 안전성을 확보하였음을 확인받은 절차라 할 수 있다. 본 연구를 통해 DO-278A의 개발 지침을 준수하는 A-SMGCS 소프트웨어 개발 수명 주기, 프로세스, 산출물, 개발조직, 주요 활동을 정의하였다. 향후 후속 연구에서는 제안한 A-SMGCS 소프트웨어 개발 방법의 적용 결과에 대한 분석을 통해 효율적이고 효과적으로 세부 활동을 구체화 할 계획이다.

후기

본 연구는 국토교통부 및 국토교통과학기술진흥원의 항공기술연구사업의 일환으로 수행하였음.[13ATRP-C069188-01, 항공기 지상이동유도 및 통제시스템 개발]

참고문헌

[1] ICAO, 2004, Advanced Surface Movement Guidance

and Control Systems(A-SMGCS) Manual, Doc 9830 AN/452, ICAO, Canada.
[2] RTCA SC-205, EUROCAE WG-71, 2011, DO-278A Software Integrity Assurance Considerations for Communication, Navigation, Surveillance and Air Traffic Management (CNS/ATM) System, DO-278A, RTCA, USA.
[3] Joern Jakobi, 2008, A-SMGCS Services, Procedures, and Operational Requirements (SPOR), 2-D1.1.1, EMMA2, Germany.