DO-278A 절차를 활용한 A-SMGCS 소프트웨어 검증방안 연구

Verification of A-SMGCS Software utilize DO-278A Process

조상훈[1]*, 이홍석[2], 김자영[1], 이진근[1]
인천국제공항공사[1], 한국산업기술시험원[2]

초 록

DO-278A는 소프트웨어 인증 절차를 제공할 목적으로 만들어진 것은 아니지만, 소프트웨어 개발 절차를 설명하는 것으로 지상용 항공장비의 소프트웨어를 만드는데 적절한 역할을 수행할 수 있다. 대체적으로, 수명주기증거품(life cycle evidence)을 통해 프로세스가 정확하고 적합하게 이행되었다는 것을 증명할 수 있다면 소프트웨어는 적합성을 확인을 받을 수 있다. 본 논문에서는 국토부 R&D로 개발되고 있는 항공기 지상이동유도 및 통제시스템(Advanced-Surface Movement Guidance & Control System, A-SMGCS)의 소프트웨어 개발 및 검증에 DO-278A 절차를 적용한 방안을 제시하고자 한다.

1. 서 론

최근 통신, 항법, 감시 및 항공교통관리(CNS/ATM) 시스템의 발전으로 항공교통서비스(ATS)를 제공하는 시스템의 독립성이 증가하였다. CNS/ATM 시스템은 지상, 항공용 및 우주 기반 요소를 포함할 수 있다. 이러한 시스템이 원래 의도한 기능을 수행하는 동시에 수용할 만한 수준의 안전을 제공하려면 이러한 시스템의 소프트웨어에 대한 무결성 보장을 제공하는 일관되거나 동등한 수단을 정의할 필요가 있다.

DO-278A(Software integrity assurance considerations for communication, navigation, surveillance and air traffic management(CNS/ATM) system)는 승인 요구 사항을 준수하는 안전 신뢰 수준으로 원래 의도한 기능을 수행하는 CNS/ATM 시스템과 장비에 대한 비항공용 소프트웨어 제작을 위한 지침을 제공하기 위한 것으로 CNS/ATM 시스템용 소프트웨어 제작과 관련된 측면에 대해 논한다. 소프트웨어 개발 및 검증 프로세스에 대한 이해를 돕기 위해 시스템 수명 주기 및 소프트웨어 수명 주기와의 관계를 설명한다. DO-278A눈 승인 기관이 관여하는 수준을 정의하거나 암시하지 않는다. 승인 기관의 관여를 이해하려면 신청인이 적용 가능한 규정과 관련 승인 기관이 발행한 지침 자료를 참조해야 한다. 이 문서를 사용하여 시스템을 지정하거나 기능을 할당할 때 구현과 개발 보장의 효율적인 방법을 결정할 수 있다[1].

항공기 지상이동유도 및 통제시스템(Advanced Surface Movement Guidance & Control System, A-SMGCS)은 이동체 감시시스템, 운항정보시스템, 기상정보시스템, 항공등화시스템 등과 같은 여러 시스템들이 상호 협력적으로 참여하여 운영되는 포괄적 시스템으로 공항 이동지역 내 항공기와 차량 등 이동 물체에 대한 감시정보를 기반으로 이동물체의 목적지까지 경로를 지정(Routing)하고, 항공등화시설(시각지원 시설)의 점등을 통하여 안내(Guidance) 정보를 제공함은 물론 위험상황 발생 등에 대비하여 이동물체에 대한 통제(Control) 기능을 제공하는 시스템이다[2].

Eurocontrol 등 다수 기관들은 컨소시엄을 구성하여 1990년도 중반부터 A-SMGCS 관련 연구를 수행하고 있으며, 레벨 Ⅳ 이상의 시스템 개발을 목표로 연구를 진행하고 있다. 미국 역시 공항의 이동지역 내 이동체의 효율적 관리를 위한 연구가 지속적으로 수행하고 있다[3]. 국내에서는 2013년 말부터 국가 연구개발 사업으로 A-SMGCS 개발을 추진하고 있다.

A-SMGCS 개발품 대부분은 Software로 구성되어있기 때문에 DO-278A의 절차를 적용하여 소

프트웨어 요구사항에서부터 소프트웨어 설계 프로세스까지 해당 절차를 적용하고자 하였다. 따라서 본 논문에서는 DO-278A 기반 A-SMGCS 소프트웨어 개발 및 검증 지원 수행방안을 제시하였다.

2. 본 론

2.1 DO-278A기반 검증방안

DO-278A는 규정에 의해 적용을 의무화하지 않았다. 또한 CNS/ATM 소프트웨어용 개발 표준으로 FAA에서 인증이 가능하지 않으며 문서의 서문에서도 “가이드라인” 으로서의 성격을 가진다고 명시되어 있다[4]. 이러한 이유로 "shall"과 "must" 같은 의무를 의미하는 단어는 사용하지 않는다.

DO-278A에서의 소프트웨어 검증이란 소프트웨어에 대해 기능, 성능 상 시험을 통해 적절히 동작하는지를 확인하는 것이 아니라, DO-278A에 정의되어 있는 소프트웨어 수명주기에 따라 적합한 활동이 이루어져 있는지를 확인 및 검증하는 것을 의미한다. 소프트웨어 검증은 프로세스 검증 혹은 소프트웨어 자체에 대한 검증이 있을 수 있다. 보통 기능 안전(Functional Safety)과 관련된 표준인 DO-278A, DO-178C, IEC 61508, EN 50128, ISO 26262와 같은 표준은 소프트웨어 프로세스 검증과 소프트웨어 개발 산출물 검증을 포함한다.

A-SMGCS 개발에서 소프트웨어 검증을 수행하는 목적은 특정 프로젝트를 위해 개발된 소프트웨어가 A-SMGCS 시스템 및 설비 검증에 관한 소프트웨어 고려사항과 합치되는지를 점검하는 데 있다. DO-278A 부록 A(ANNEX A)는 10개의 표를 포함하고 있다. 이들 표는 개발자가 증명해야 할 목표 작업들이며 검증대상이다. 검증대상인 각 표의 제목은 아래와 같다.

A-1 : 소프트웨어 계획 프로세스
A-2 : 소프트웨어 개발 프로세스
A-3 : 소프트웨어 요구사항 프로세스
A-4 : 소프트웨어 설계 프로세스
A-5 : 소프트웨어 코딩 및 통합 프로세스
A-6 : 통합 프로세스
A-7 : 검증 프로세스
A-8 : 소프트웨어 형상관리 프로세스
A-9 : 소프트웨어 품질보증 프로세스
A-10 : 소프트웨어 승인 프로세스

A-SMGCS 소프트웨어 검증을 시행하는 의도는 DO-278A의 목적을 비롯하여 여타의 적용 가능한 소프트웨어 정책, 지도지침 및 이슈 문서들과의 합치성을 보장하기 위한 데 있다. 합치성의 검증을 위해서는 통상적으로 프로젝트의 소프트웨어 생명주기 전반에 걸쳐 네 개(계획, 개발, 확인, 최종)의 검증단계를 거친다.

먼저 계획 검증단계는 계획과 표준이 DO-278A의 목적에 부합하고 기타 적용 가능한 소프트웨어 정책, 지도지침, 이슈 문서들에 부응하도록 한다. 계획, 표준 및 제안된 적합성 방법론에 대해 검증팀 또는 검증자와 개발자 간 합의를 도출한다. 두 번째 개발 검증단계에서는 소프트웨어 요구조건, 설계, 코드에 관한 계획과 표준의 이행 및 관련 검증자료, 소프트웨어 품질보증, 소프트웨어 형상관리 데이터 평가 그리고 계획과 표준 변동사항에 대한 평가 및 동의를 점검한다. 신기술 및 방법론 이행 평가 및 계획, 표준, 동의와의 적합성 유지 여부를 점검하며 생명주기 데이터가 DO-278A의 목적과 기타 적용가능 소프트웨어 정책, 지도지침, 이슈 문서를 만족시킴을 재차 확인한다. 세 번째 확인 검증단계에서는 검증과 시험에 대한 계획과 절차 이행 여부 평가, 관련된 모든 소프트웨어 형상관리 및 소프트웨어 품질보증 임무의 완수 및 적합성 평가, 소프트웨어 요구조건 검증 사실 확인 및 강건성 시험의 계획 및 시행 사실 확인이 필요하다. 또한 DO-278A이 요구하는 (타이밍, 메모리, 커버리지 시험, 구조적 커버리지 및 데이터와 컨트롤 커플링을 포함하는)분석실험 시행 사실이 확인되어야 하고, 검증활동의 DO-278A 목적 만족 여부를 확인할 수 있어야 한다. 마지막으로 최종 검증단계에서는 최종 소프트웨어 상품이 DO-278A의 목적에 부합하며 평가 준비완료 되었음이 확인되어야 하고 평가 기간 동안의 모든 미검토 항목 언급 및 해결되어야 한다.

실제 검증단계는 개별 프로젝트의 요구에 따라 합동 혹은 승인된 피 지명인에 위임하는 방식으로 진행될 수도 있다. 프로젝트에 따라서는 4단계 이상의 평가가 인가될 수도 있다.

2.2 DO-278A기반 검증절차

A-SMGCS 소프트웨어 산출물에 대한 검증은 4단계에 걸쳐 진행되도록 계획하였다.

먼저 개발 업체는 단계별 검증관련 산출물을 작성하여 시험평가기관에 제출한다. 두 번째 단계에서 제출된 문서는 시험평가기관에 의해 DO-278A 검증용 체크리스트에 의거하여 산출물을 평가 및 검증한다. 검증 결과는 발견된 결함들을 포함하여 보고서로 기록한다. 세 번째 단계에서는 시험평가기관과 개발업체가 시험평가기관에서 수행한 검증 결과에 대해 합의하는 회의를 하여 합의안을 도출한다. 합의 내용에는 각각의 발견사항들에 대한 결함 판정과 각각의 결함에 대한 보완계획안이 포함된다. 그리고, 합의된 결함의 정도에 따라 추가 검증회의 개최 여부 결정한다. 마지막으로 각 개발 업체는 수정 조치 실행 및 증거문서를 시험평가기관에 제출한다. 최종 검증결과 보고서는 주관기관의 승인을 통해 최종 확정된다.

2.3 DO-278A기반 검증범위

소프트웨어의 검증범위 및 기준을 설정하는 것은 DO-278A 검증 업무를 수행하기 위해서 매우 중요한 일이다. DO-278A의 프로세스의 라이프사이클 모델은 아래 그림과 같다.

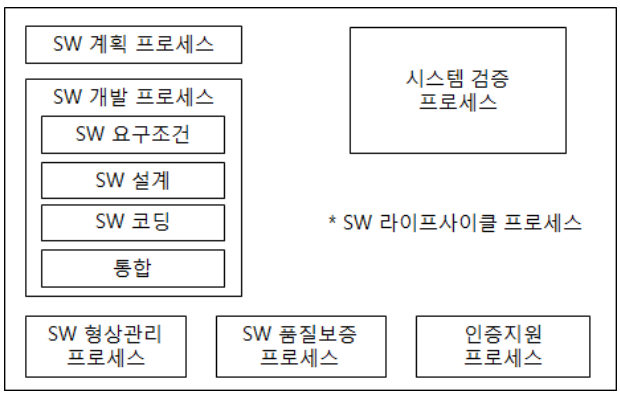

Fig 1. Software Life cycle Model

위의 그림에서 보듯이 소프트웨어 라이프 사이클 참조모델에는 계획 프로세스, 개발 프로세스(요구사항, 설계, 코딩, 통합), 검증 프로세스, 품질보증 프로세스, 형상관리 프로세스가 있다.

소프트웨어 계획 프로세스는 소프트웨어 개발 시작 단계에서 준비하는 활동으로 소프트웨어 개발 관련 계획 및 소프트웨어 개발과 관련된 표준을 수립한다. 개발 프로세스는 상위 요구사항이 소스 코드를 구현하는 데 사용할 수 있는 소프트웨어 아키텍처와 하위 요구사항을 개발하기 위해 소프트웨어 설계 프로세스에서 한 번 이상의 반복을 통해 재정의 된다. 소프트웨어 검증 프로세스에 대한 입력은 시스템 요구 사항, 소프트웨어 요구 사항, 소프트웨어 아키텍처, 추적 데이터, 소스 코드, 실행 목적 코드 및 소프트웨어 검증 계획을 포함한다. 품질 보증 프로세스는 목적이 달성되었고, 결함이 탐지, 평가, 추적 및 해결되었고, 소프트웨어 제품과 소프트웨어 수명 주기 데이터가 승인 요구 사항을 준수한다는 보장을 획득하기 위해 소프트웨어 수명 주기 프로세스와 그 출력사항을 점검한다. 형상관리 프로세스는 소프트웨어 코딩 프로세스에서 소스 코드가 소프트웨어 아키텍처와 하위 요구 사항으로부터 구현되었는지 확인하고 개발 단계 동한 형상관리 대상을 식별하고 유지 및 관리한다.

3. 결 론

본 논문에서는 소프트웨어 검증 과정에서 참고로 활용할 수 있는 DO-278A를 A-SGMCS 개발 소프트웨어 검증을 수행하기 위한 절차 및 방법론을 적용하였다. 하지만 본 연구개발에는 평가/승인 전 단계의 소프트웨어 평가만을 고려하여 적용하고 있다.

DO-278A는 지상기반의 CNS/ATM 소프트웨어 개발을 지원하기 위한 가이드라인이며, 소프트웨어 검증을 위한 가이드 문서이다. 하지만 제시하는 항목들이 프로젝트의 성격에 따라 소프트웨어 개발과 검증의 맥락에서 적절하지 않을 수도 있을 것이다. 개발자 및 검증자들은 각각의 소프트웨어 프로젝트들이 저마다 독특한 특징을 지니고 있음을 염두에 두고, 이 절차를 각각의 구체적 상황에서 최대한의 적합성을 발휘할 수 있도록

활용해야 할 것이다. 본 논문에서 A-SMGCS개발에 적용된 DO-278A의 세부 항목을 모두 제시하는 것은 어려운 부분이지만, 본 논문에 포함된 정보를 통해 항공용 소프트웨어의 개발 및 인증에 적용되는 사항을 이해하는데 도움이 되었으면 한다.

후 기

본 연구는 국토교통부 항공안전기술개발사업 연구비지원(15ATRP-C069188-03)에 의해 수행되었습니다.

참고문헌

[1] RTCA Inc., 2011, Do-278A, Software integrity assurance considerations for communication, Navigation, surveillance and air traffic management(CNS/ATM) systems, 2011.

[2] Sanghoon Jo, Jha-Young Kim, Jin-Geun Yi, 2015., Development of Advance-Surface Movement Guidance & Control System utilize System Engineering Process, 한국항행학회 2015 추계학술대회 논문집.

[3] Eun-suk Seol, Sang-hun Kim, Sung Kwan Ku, Jeong-hyum Cho, 2013, A Study on Systems Engineering Based Compliance Procedure for A-SMGCS, Journal of Advanced Navigation Technology, 17(5), 151-156.

[4] Hongseok Lee, Goohoon Kwon, Byeong gak Ko, 2015, A Study for Evaluation Method of Safety Critical Software in Avionics Industry, Journal of Advanced Navigation Technology, 19(2), 91-97.