JANT 한국항행학회논문지
Journal of Advanced Navigation Technology

항공 우주 해상

J. Adv. Navig. Technol. 19(2): 91-97, Apr. 2015

안전필수 항공 산업용 소프트웨어 평가 방법 연구

A Study for Evaluation Method of Safety Critical Software in Avionics Industry

이 홍 석 · 권 구 훈* · 고 병 각
한국산업기술시험원 IT안전기술센터

Hongseok Lee · Goohoon Kwon* · Byeonggak Ko
IT & Convergence Technology Center, Korea Testing Laboratory, Daejeon 305-500, Korea

[요 약]

이 논문은 항공 분야에서의 안전필수 소프트웨어를 평가하기 위한 고려사항을 기술한다. 항공 분야에서의 안전필수 소프트웨어의 평가를 수행하기 위해서는 해당 소프트웨어의 평가 수준에 대한 정보가 필요하다. 그 수준은 표준에 명시되어 있으나 소프트웨어 자체적으로 결정되는 요소가 아니며 시스템 안전 평가 결과 및 시스템 설계 결과에 의존적이다. 그러므로 소프트웨어 평가 수준을 결정하기 위해 시스템 개발 및 시스템 안전 평가 표준에서 필요로 하는 정보에 대해 설명한다. 그리고 소프트웨어를 평가하기 위한 기존의 방법론들을 조사하고 항공기 지상 유도 및 통제 시스템 소프트웨어의 평가에 적용할 방법을 제시한다.

[Abstract]

This paper specifies several considerations about assessing safety-critical software in the aerospace domain. In order to evaluate safety critical software in the aerospace industry, it is required to identify an information of evaluation criteria of software under evaluation. The information is specified in the standard, but determination of evaluation criteria cannot be decided by itself and depends on the results of safety assessment of a system and system design. Thus, this paper explains required information of system development standard and safety assessment standard to determine software evaluation criteria. It surveys existing methodologies about evaluating software, and suggests method which is adapted to evaluation of an advanced surface movement guidance and control system (A-SMGCS) software.

Key word : Advanced surface movement guidance and control system, DO-278A, Functional safety, Software assessment, Safety critical software.

http://dx.doi.org/10.12673/jant.2015.19.2.91

Received 15 January 2015; **Revised** 2 February 2015
Accepted (Publication) 23 April 2015 (30 April 2015)

***Corresponding Author; Goohoon Kwon**

Tel: +82-42-939-6012
E-mail: ghkwon@ktl.re.kr

Ⅰ. 서 론

항공기 지상 유도 및 통제 시스템(A-SMGCS) 은 안전과 관련이 있는 시스템으로 안전과 관련이 있는 속성을 가진 시스템이다. 이 시스템에 개발되는 소프트웨어 또한 안전과 관련이 있는 속성을 가진 소프트웨어이며, 해당 소프트웨어는 안전과 관련된 표준으로 개발되어야 할 필요가 있다.

항공분야 소프트웨어와 관련된 개발 표준으로는 DO-178C[2]와 DO-278A[1]가 있다. 지상용 항공장비에 탑재되는 소프트웨어를 위한 개발 표준은 DO-278A인 반면 항공기에 탑재되는 소프트웨어에 대한 개발 표준은 DO-178C이다. 안전과 관련된 항공기에 탑재되는 소프트웨어를 평가하기 위해서는 해당 소프트웨어를 평가하기 위한 개발 표준이 무엇인지, 해당 표준에서 여러 가지 등급으로 나누어서 평가를 수행하는 경우, 등급의 기준이 무엇인지, 그리고 평가를 어떠한 방식으로 수행할 것인지를 결정하는 것이 필요하다.

하지만, 국내 실정상 표준을 완벽하게 준수하여 개발하지 않고 일부 활동들이 누락된 채 개발을 수행하는 경우가 많다. 특히 항공 소프트웨어 개발을 하기위한 개발 기준에 대한 근거가 없는 경우에는 소프트웨어를 평가하기가 쉽지 않다.

본 논문에서는 이와 같이 항공기 소프트웨어를 평가하고자 할 때, 평가를 수행하기 위한 고려사항을 기술하고 평가 수행방법들을 설명하였다. 특히 항공기 지상 유도 및 통제 시스템에 탑재되는 소프트웨어를 평가하기 위해 소프트웨어 개발 표준인 DO-278A를 기반으로 평가하고자 할 때에 고려해야 하는 사항들을 서술하였다. 본 논문의 주요 공헌은 다음과 같다. 1) 항공 소프트웨어를 평가하기 위한 관련 사례를 조사하고 적용할 수 있는 적절한 방법을 제시한다. 2) 소프트웨어를 평가하기 위한 전제들을 제시한다.

본 논문의 구성은 다음과 같다. 2장에서는 항공 소프트웨어 개발 관련 표준들 및 표준 간의 관계에 대해서 설명하고 3장에서는 소프트웨어 평가 기준을 수립하기 위해 고려할 사항을 기술하고 한국형 A-SMGCS 평가에 적용하기 위한 방법을 설명한다. 4장에서는 유럽의 A-SMGCS와 관련된 연구들을 조사한 내용을 설명하였다. 5장에서는 DO-278A기반의 소프트웨어 평가 방법들을 설명하고 마지막으로 6장에서는 결론을 맺는다.

Ⅱ. 항공 분야 소프트웨어 개발과 관련된 표준

항공 소프트웨어 개발 표준은 DO-178C[2]와 DO-278A[1]이 있다. 이들 소프트웨어 개발 표준은 시스템 및 하드웨어 개발 표준과 연관이 있다. 그림 1은 항공 소프트웨어 개발 표준과 관련된 표준들 사이의 관계에 대해서 나타내고 있으며, 그림 2는 소프트웨어 표준과 시스템 및 하드웨어 개발 표준들 사이에서 정보의 흐름을 나타낸다. 시스템, 하드웨어, 소프트웨어는 개발 단계 중에 그림2와 같은 정보 전달을 통해 각각은 다른 개발 단계에게 영향을 미친다.

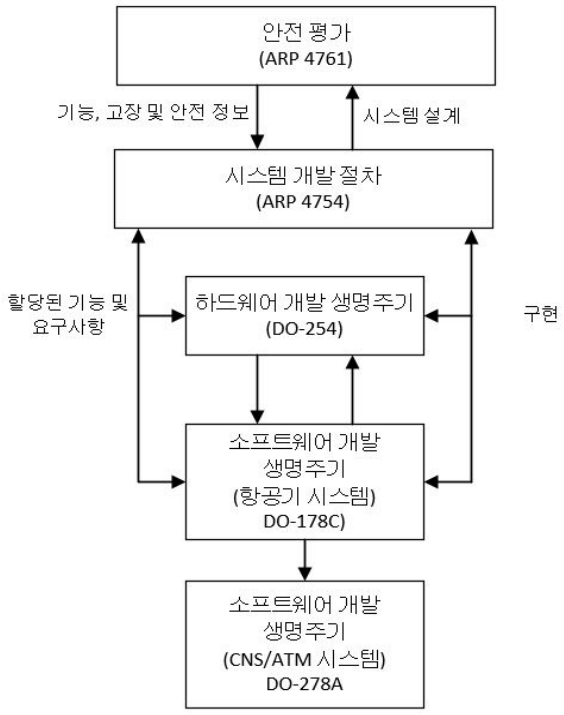

그림 1. 시스템 안전 평가, 시스템 개발, 하드웨어 및 소프트웨어 개발 관련 표준과 각 표준들 간의 관계

Fig. 1. System safety assessment, system development, hardware and software development standards and relationships between them.

그림 1에서 볼 수 있듯이, 항공기 관련 제품을 개발하기 위해서는 그 제품이 안전과 얼마나 관계가 있는지를 평가한다. 즉,

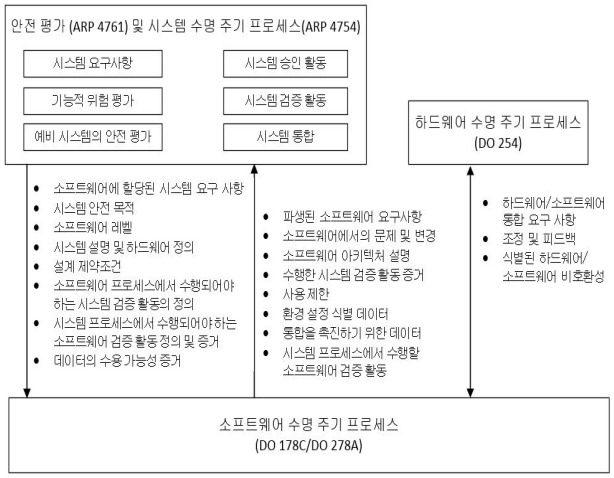

그림 2. 소프트웨어 표준과 다른 표준들(시스템 및 하드웨어) 사이에서의 관련된 정보의 흐름

Fig. 2. Related Information flow between software development standard and other standards (System and Hardware).

표 1. ARP4761의 개발 보장 등급별 고장조건의 심각도 및 발생 확률

Table 1. Criticality and frequency per development assurance Level(DAL) in ARP4761.

개발 보장 등급	고장 조건 심각도	발생확률(F) (per flight hour)
Level A	치명적인	F < 10-9
Level B	위험한	10-9 ≤ F < 10-7
Level C	중요한	10-7 ≤ F < 10-5
Level D	사소한	10-5 ≤ F
Level E	영향 없음	-

개발 대상이 구현해야 하는 기능의 오작동으로 인해 사람에게 미치는 위험을 5단계의 심각도로 나누어서 평가하고 심각도에 따라 제품이 만족해야 하는 고장 발생 확률을 정의한다. 이와 같은 제품의 안전 평가를 수행하는 표준이 ARP 4761[4]이다. 안전 평가는 제품 개발의 시작단계에서 수행되어야 하고 시스템, 하드웨어 및 소프트웨어 개발을 위한 기본 바탕이 된다.

표 1은 ARP 4761에서 정의한 개발 보장 등급별 고장조건 심각도와 고장의 발생확률을 나타낸 표이며, 표 2는 고장 조건 심각도의 분류기준을 정의한 표이다. ARP 4761에서는 제품의 안전과 관련된 심각도를 치명적인, 위험한, 중요한, 사소한, 영향 없음의 5가지 등급으로 나누었으며, 심각도에 따라 각각의 고장 발생 확률을 정의하였다. 표 1에서 개발 보장 등급이 Level A라는 말의 의미는 Level A등급에 해당되는 제품은 잘못된 기능으로 인해 사람에게 치명적인 위해를 가할 수 있으며, 그런 위험을 방지하기 위해서 고장의 발생확률을 10-9미만이 되도록 설계해야 함을 의미한다. ARP4761에서 안전과 관련된 등급은 Level A에서 Level D까지 이며, Level E등급은 안전과 관련이 없는 등급이다. 만약 어떤 제품의 안전 평가 결과 E등급이 나왔다면 해당 제품은 ARP 4754, DO 254, DO-178C 혹은 DO-278A와 같은 안전관련 개발 표준을 따를 필요가 없다.

표 2. 고장 조건 심각도의 분류

Table 2. Classification of failure condition.

고장 조건 심각도	설명
치명적인	대개 항공기의 상실로 인해 다중적 재해를 초래할 수 있는 고장 조건.
위험한	항공기 능력 또는 다음과 같은 범위까지의 부정적 작동 조건을 극복하는 비행 승무원의 능력을 감소시킬 수 있는 고장 조건: • 안전 여유 또는 기능상 능력의 대폭 감소; • 신체적 고통 또는 비행 승무원이 자신의 작업을 정확하게 또는 완전하게 수행하기 위해 의존할 수 없을 만큼 더 많은 업무량, 또는 • 비행 승무원을 제외한 비교적 소수의 탑승자에 대한 심각한 또는 치명적 부상.
중요한	항공기의 능력 또는 부정적 작동 조건을 극복하는 승무원의 능력. 예를 들어 안전 여유나 기능상 능력의 상당한 감소, 승무원 업무량이나 승무원 효율을 감소시키는 조건의 상당한 증가, 비행 승무원의 불편 또는 승객이나 객실 승무원의 신체적 고통(아마도 부상 포함)의 범위까지 감소시킬 수 있는 고장 조건.
사소한	항공기 안전을 크게 감소시키지 않고 승무원 능력 범위의 승무원 조치를 수반하는 고장 조건. 예를 들어 사소한 고장 조건은 안전 여유나 기능상 능력의 소폭 감소, 일상적 비행 계획 변경 등 승무원 업무량의 소폭 증가 또는 승객이나 객실 승무원의 약간의 신체적 고통을 포함할 수 있다.
영향없음	안전에 영향을 미치지 않는 고장 조건, 예를 들어 항공기의 운행 능력에 영향을 미치지 않거나 승무원 업무량을 증가시키지 않는 고장 조건.

안전 평가 수행 이후 시스템의 개발을 시작하게 되는데, 이와 관련된 표준은 ARP4754이다. 시스템 개발에서는 안전 평가에서 도출된 개발 보장 등급(Level A~Level D)을 만족시키기 위한 설계 및 구현을 수행해야 한다. 시스템을 개발하면서 하드웨어 및 소프트웨어의 개발에 착수하게 되며, 하드웨어 및 소프트웨어는 시스템에서 구현해야 하는 개발 보장 등급에 따라 하드웨어와 소프트웨어의 개발 수준도 결정된다. DO-278A는 소프트웨어의 개발 수준을 보장 수준(Assurance Level)이라는 표현으로 정의하였으며, 이를 6개의 등급으로 나누고 각 등급에 대한 고장 조건 심각도 수준을 정의하였다. 보장 수준은 AL1에서 AL6등급으로 나뉘어져 있으며 AL1이 가장 엄격한 등급

표 3. DO-278A의 보장 수준의 분류

Table 3. Classification of assurance level (AL) in DO-278A.

DO-278A의 보장 수준	설명
AL1	소프트웨어의 이상 행동이 CNS / ATM 시스템 기능의 고장을 야기하거나 기여할 수 있으며 항공기에 치명적(catastrophic) 고장 조건을 초래할 수 있는 소프트웨어
AL2	소프트웨어의 이상 행동이 CNS / ATM 시스템 기능의 고장을 야기하거나 기여할 수 있으며 항공기에 위험한(hazardous) 고장 조건을 초래할 수 있는 소프트웨어
AL3	소프트웨어의 이상 행동이 CNS / ATM 시스템 기능의 고장을 야기하거나 기여할 수 있으며 항공기에 중요(major) 고장 조건을 초래할 수 있는 소프트웨어
AL4	소프트웨어의 이상 행동이 CNS / ATM 시스템 기능의 고장을 야기하거나 기여할 수 있으며 항공기에 중요(major) 및 사소한(minor) 사이의 고장 조건을 초래할 수 있는 소프트웨어
AL5	소프트웨어의 이상 행동이 CNS / ATM 시스템 기능의 고장을 야기하거나 기여할 수 있으며 항공기에 사소한(minor) 고장 조건을 초래할 수 있는 소프트웨어
AL6	소프트웨어의 이상 행동이 항공기 운행 능력이나 조종사 업무량에 영향을 미치지 않고 CNS/ATM 시스템 기능의 고장을 야기하거나 기여할 수 있는 소프트웨어

표 4. 고장 조건 심각도의 분류
Table 4. Classification of failure criticality.

DO-278A 보증 레벨	DO-178C 보증 레벨	고장 상태 분류
AL1	A	치명적인
AL2	B	위험한
AL3	C	중요한
AL4	없음	없음
AL5	D	사소한
AL6	E	영향없음

이다.

DO-178C도 소프트웨어의 개발 등급을 A, B, C, D, E의 5단계로 정의하였으며, 각 등급에 대한 고장 상태 분류가 명시되어 있다. DO-178C에서 가장 엄격한 등급은 A등급이며, 가장 낮은 등급은 E이다. DO-278A와 DO-178C간의 고장 상태 분류 별 보증 레벨의 관계는 표 4와 같다.

시스템 수준에서는 고장 확률에 의해 개발 등급이 결정되므로 고장 확률이 중요하다. 그러나 소프트웨어 수준에서는 시스템 수준의 개발 등급을 따르며 고장 확률은 직접적인 관련이 없다. 그리고 소프트웨어의 평가 때에도 개발 등급에 따른 절차 및 기법을 적용했는지만을 평가하며 소프트웨어가 시스템 수준의 고장 확률을 만족하는지 여부에 대해서는 고려하지 않는다.

Ⅲ. 소프트웨어 평가 기준 수립

2장에서 소프트웨어 개발 표준 및 소프트웨어와 관련된 시스템 및 하드웨어 개발 표준에 대해서 설명하였으며, 각각의 표준이 다른 표준들에게 영향을 미친다고 서술하였다. 본래 제품을 개발하기 위해서는 안전 평가가 선행되어야 하고 시스템 개발 프로세스를 수행하면서 하드웨어 및 소프트웨어 개발 프로세스를 수행해야 한다. 하지만, 이와 같은 표준들 간의 관계를 미처 파악하지 못하고, 일부의 개발 프로세스만 수행하고 있는 것이 국내 실정이다. 특히 대부분의 경우 아직까지 안전 평가에 대한 개념이 미숙하고 적용하는 데에 어려움이 있어서 안전 평가 없이 개발되는 소프트웨어에 대해 이에 대한 평가기준을 수립하는 것이 평가자 입장에서는 문제가 된다.

이와 같은 문제를 해결하기 위해서 3가지 사항을 고려하였다. 첫째는 DO-278A의 보장 수준 결정과 관련된 요건을 면밀하게 검토하였다. DO-278A의 2.3.4 보장 수준 결정에 따르면 본래 소프트웨어에 할당된 보장 수준 보다 더 높은 수준으로 개발하는 것이 바람직하다고 명시하고 있다. 본래 안전 평가는 제품이 구현해야 하는 기능의 상실 및 기능의 오작동 모두에 대해 영향을 분석해야 하며, 부정적 환경 조건 및 아키텍처 전략 등과 같은 외부 요인을 검토해야 하는데, 시스템 및 소프트웨어 개발 도중 안전 평가 단계에서 미처 파악하지 못했던 사항들이 나중에 발견될 수 있기 때문에 소프트웨어 개발 시에 안전 평가 단계에서 도출된 보장 수준보다 좀 더 엄격하게 개발될 필요가 있다는 것을 의미하는 것이다. 그러므로 이런 결과로부터 소프트웨어의 개발 보장 수준은 보수적으로 결정해야 한다는 결론을 얻을 수 있다.

둘째로, A-SMGCS 표준 매뉴얼인 ICAO 9830[6]를 참고하였다. ICAO 9830에서는 A-SMGCS이 만족시켜야 하는 고장 확률을 $9 * 10^{-8}$로 정의하였는데, 이는 ARP 4761기준의 Level B에 해당하며, DO-278A기준으로는 AL2에 해당한다.

그리고 마지막으로 유럽의 항공기 지상 유도 및 통제 시스템 개발과 관련된 연구로는 EMMA[13], EMMA2[14]프로젝트를 조사하였다. EMMA프로젝트 결과 A-SMGCS의 안전 평가 결과는 고장 조건 심각도를 치명적인 사고로 판단하였으며 DO-278A기준으로는 AL1에 해당한다.

위의 3가지 고려사항으로부터 한국형 A-SMGCS제품에 대한 소프트웨어 보장 수준은 보수적으로 AL1으로 결정하는 것이 타당하며 합리적이라고 판단된다.

Ⅳ. 유럽의 항공기 지상 유도 및 통제 시스템 개발 사례 조사

유럽에서 항공기 지상 유도 및 통제 시스템 개발과 관련된 연구로는 EMMA[13], EMMA2[14]프로젝트가 있다. EMMA는 유럽 공항 이동 관리를 위한 항공기 지상 유도 및 통제 시스템의 약자(European airport Movement Management by A-SMGCS)로, 증가되는 항공 교통 수요에 대응하기 위해 2004년부터 2008년까지 진행된 프로젝트이다. EMMA2는 EMMA 프로젝트 이후 연속과제로서 진행되어온 프로젝트이다. 본 연구에서는 EMMA2에서 수행한 결과물 중에서 Milan Malpensa 공항의 항공기 지상 유도 및 통제 시스템에 대한 안전 평가 결과[8]를 참조하였다.

[8]의 안전 평가 연구에서 6가지의 안전과 관련 있는 위험한 시나리오가 도출되었다.

1. 지상에서 이동 중인 두 대의 항공기들의 충돌
2. 지상에서 이동 중인 항공기와 차량의 충돌
3. 지상에서 이동 중인 항공기와 이륙하려는 항공기의 충돌
4. 지상에서 이동 중인 항공기와 착륙하고 있는 항공기의 충돌
5. 다른 항공기의 제트 폭풍에 의해 영향 받는 이동 중인 항공기
6. 갑작스런 방향 전환 혹은 통과주행(overrun)에 의해 영향 받는 이동 중인 항공기

위의 시나리오에서 3, 4, 6번째 시나리오는 치명적이고 재난적인 결과가 야기되기 때문에 허용 가능한 발생 확률을 $8 * 10^{-9}$로 목표치를 설정하였으며, 1, 2, 5번째 시나리오는 치명적이지는 않으나 많은 피해를 야기하기 때문에 최대 허용 가능한 발생 확률을 $2 * 10^{-7}$로 목표치를 설정하였다. 3, 4, 6번째 시나리오에 의한 허용 가능한 발생 확률은 ICAO 9830[6]에서 정의한 전 세

계의 치명적 지상 이동 중의 사고 확률인 9 * 10^{-8}보다 엄격한 수준이며 미국 내의 치명적 사고 확률인 6.2 * 10^{-8}보다도 엄격한 수준임을 알 수 있다.

하지만, [8]의 연구결과는 어디까지나 참조를 위한 데이터일 뿐이며 본 연구의 한국형 A-SMGCS프로젝트에 직접적으로 영향을 미치는 데이터는 아닌데, 그 이유는 다음과 같다. 안전 평가는 기술 장비, 운영 절차, 그리고 사람들 간의 상호작용에 대한 고려가 필요한데, 국내와 외국의 기술 장비, 운영 절차, 사람들 간의 상호작용 모두가 동일하지 않기 때문이다. 다시 말하면, 기술 장비가 각기 다르다면 안전 평가 결과에 영향을 미칠 수 있다. 기술 장비는 시스템에서 수행하는 기능의 관점에서 봤을 때 기능상으로 차이가 발생할 수 있음을 의미하기도 한다. 그리고 운영절차도 각 공항마다 차이가 있을 수 있다. 즉 위험한 상황에 대해 공항마다 대처하기 위한 절차가 차이가 있음을 의미하며, 이 부분에서 역시 안전 평가 결과가 차이가 있을 수 있다. 하지만, 이와 같은 한계는 국내에서도 안전 평가 활동을 수행하지 않고서는 해결할 수 없는 문제이므로 본 연구의 범위를 벗어나는 문제이다.

그럼에도 불구하고 안전 평가의 위험 시나리오 관점에서 봤을 때 언급한 6가지의 시나리오가 국내에서도 충분히 발생 가능하며, 그 중에서 3, 4, 6번째 시나리오가 국내의 어떤 공항에서도 발생하는 경우 동일한 치명적인 결과를 초래할 것으로 판단되므로 안전평가가 수행되지 않는 국내 상황을 고려하기 위해 [8]의 결과물을 참고하여 국내에 적용하는 것은 의미가 있다고 판단된다.

Ⅴ. DO-278A 기반의 소프트웨어 평가 방법에 대한 연구

소프트웨어 평가에는 두 가지의 접근 방법이 있다. 하나는 제품개발 과정에 대해서 평가하는 방법이고, 다른 하나는 제품 자체에 대한 평가 과정이다. 일반적으로 소프트웨어의 인증이라고 하면 이 두 가지를 기반으로 한다. 그리고 이 때 소프트웨어의 인증은 그와 관련된 표준이 있으며 그 표준을 기반으로 한다.

항공 도메인의 소프트웨어는 그 자체가 인증 대상이 되는 경우가 일부 존재하기는 하지만, 일반적으로는 인증의 대상은 제품이며 소프트웨어는 제품의 일부로서 평가된다.

항공 도메인의 소프트웨어 관련 표준으로는 DO-178C[2]와 DO-278A[1]가 있는데, DO-178C가 항공기에 장착되는 소프트웨어용 개발 표준이고 DO-278A는 지상 항공 장비 소프트웨어용 개발 표준이라는 차이점 외에 DO-178C는 소프트웨어의 인증 적용 가능한 표준이고 DO-278A는 그렇지 않다는 차이점이 있다. 그래서 DO-178C에서는 소프트웨어 개발을 만족하기 위한 요구사항으로 '~을 해야 한다.'(shall)는 문구로 기술되어 있으나, DO-278A는 그와 같은 문구로 표현되어 있지 않다는 차이가 있다. DO-278A는 인증을 받기 위해 적용하는 표준이 아니며 가이드로서의 성격을 지닌다고 표준에 명시적으로 기술되어 있다.

DO-278A기반으로 소프트웨어를 평가를 수행하기 위해 1) 적합성(compliance) 기반 평가 접근법을 사용하거나 2) 개발 역량의 수준을 정량화한 프레임워크를 적용하여 평가하는 접근 방법을 사용할 수 있다. 두 가지 접근 방법을 평가 체계 구축의 용이성, 평가 체계에 대한 정당성, 평가 체계의 변경 용이성, 평가 체계의 형식성을 기준으로 비교하면 다음과 같다.

적합성 기반 평가 방법은 국제 평가체계에 따라 수행하는 것이 아니라 평가 기준 기반의 요구사항을 체크리스트로 만들어서 해당 체크리스트의 달성 여부를 평가하는 방법으로 평가 체계 구축하기는 쉽다. 하지만 체크리스트를 올바르게 만들었느냐에 대한 정당성을 확보하기는 쉽지 않으며 체크리스트 작성자의 역량에 따라 품질이 달라질 수 있다는 한계가 있다. 또한 하지만 표준화되지 않았기 때문에 체계적이지 않은 평가 방법으로 비춰질 우려가 있으며 동일 표준에 대한 여러 업체들의 평가 결과를 서로 비교할 수 없다는 문제점이 있다. 체크리스트 기반은 국제평가체계를 따르지 않으므로 변경하기 용이하며, 프레임워크 평가방식 대비 비형식적인 체계를 갖췄다.

한편, 프레임워크 평가 방법은 국제 평가체계에 따라 수행하기 때문에 평가체계를 구축하기 위해서는 사전 지식이 필요하며 새로운 평가 기준을 국제 평가 체계의 틀에 맞추는 작업이 필요하기 때문에 적합성 평가 구축의 노력보다는 더 많은 노력이 필요하다. 일반적으로 평가 프레임워크는 SPICE[11]나 CMMI[10]의 체계를 사용한다. 그리고 평가 프레임워크는 평가 체계가 표준화되어 있으며 그와 같은 평가 체계의 유용성을 널리 인정받은 방법이므로 적합성 기반 평가 방법보다는 보다 체계적이고 조직적이라고 볼 수 있다. 그러므로 평가 방법의 정당성을 부여받기는 훨씬 더 수월하다고 볼 수 있다. 그리고 프레임워크에 대한 기본적인 지식이 잘 알려져 있기 때문에 능력 있는 평가자를 양성하기가 보다 용이하다는 장점이 있다. 하지만 이 접근법은 기존의 프레임워크에 적용하고자 하는 표준을 맞춰야하기 때문에 기존의 프레임워크를 확장해서 개발해야 하는 어려움이 있다. 이런 작업은 평가 프레임워크 전문지식을 필요로 하고 기존의 평가 항목과의 융합을 필요로 하므로 적합성 평가 접근법과 비교했을 때 평가 구축을 하기 위해 보다 많은 노력이 필요하다. 그리고 변경 또한 상대적으로 어려우며, 평가가 비교적 형식적이다.

본 연구에서는 위에서 언급한 두 가지 접근 방법 중에서 표준 적합성 기반 평가 접근법을 선택하기로 하였는데, 그 이유는 다음과 같다.

1. 기존의 프레임워크를 기반으로 DO-278A 평가를 수행하기 위해서는 기존 프레임워크를 확장시켜야 하는데 이 작업을 수행하기 위해서는 상당한 수준의 작업이 필요하다.

2. 표준 대비 적합성을 평가하는 접근 방법은 표준을 분석하여 만족해야 하는 사항을 추출하여 체크리스트로 작성하여 평가하는 방식이므로 평가 항목을 작성하는 것이 비교적 쉽다.

3. FAA에서 인증 심사를 받고자 하는 업체를 위해 DO-178B 표준에 대한 인증 방법 및 평가 방법에 대한 자료[9]는 표준 적합성 접근 방법으로 평가를 수행하고 있으며 DO-178B/C의 문서구조가 DO-278A의 문서구조와 일치하고 대부분의 내용을 DO-278A에서 사용할 수 있기 때문에 평가 절차 및 방법과 평가항목을 정의하는데 유리한 점이 있다. 바로 이러한 장점이 앞에서 언급한 표준 적합성 접근법의 체계적이지 않은 평가 방법이라는 한계점을 보완할 수 있다는 점에서 유용한 접근 방법이라고 볼 수 있다.

Ⅵ. 결 론

항공기 지상 유도 및 통제 시스템에 탑재되는 소프트웨어 개발을 위해 DO-278A기반으로 개발을 수행하기 위해서는 소프트웨어에 영향을 끼치는 해당 시스템과 관련된 표준들을 이해해야 할 필요가 있다. 소프트웨어의 개발 기준은 시스템에 부과된 기능 혹은 요구사항에 대한 개발 보장 수준에 의존적일 수밖에 없으므로 소프트웨어 개발을 위해서는 관련된 정보들이 제공되어야 한다.

특히 소프트웨어 평가를 위해서는 평가 받는 팀이 개발하는 소프트웨어의 보장 수준을 파악해야 할 필요가 있는데 만약 직접적으로 자료를 제공받을 수 없다면 관련 연구나 유사 사례를 통해서 해당 기준의 근거를 확보하고 보수적으로 보장수준을 결정해야만 한다.

마지막으로 소프트웨어를 평가하기 위한 방법에는 적합성 접근법 및 평가 프레임워크를 활용한 방법이 있다. 각각의 방법이 모두 적용 가능하지만 관련 업계의 환경이나 실정에 맞는 방법을 택하여야 한다. 그런 점에서 본 논문에서의 적합성 평가 접근방법은 적절하다고 볼 수 있겠다.

감사의 글

본 연구는 국토교통부/국토교통과학기술진흥원의 지원으로 수행되었습니다(과제번호:15ATRP-C069188-03).

참고 문헌

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

[2] Software considerations in airborne systems and equipment certification, RTCA Inc, DO-178C, 2011

[3] Design assurance guidance for airborne electronic hardware, RTCA Inc, DO-254, 2000

[4] Guidelines and methods for conducting the safety assessment process on civil airborne systems and equipment, SAE, ARP 4761, 1996

[5] Aerospace recommended practice, SAE, ARP 4754, 1996

[6] Advanced surface movement guidance and control system(A-SMGCS) manual, ICAO, Doc 9830, 2004

[7] M. Johansson, “Additional requirements for process assessment in safety–critical software and systems domain,” *Journal of Software: Evolution and Process*, Vol 24, Issue 5, pp 501-510, 2012

[8] J. J. Scholte, Safety assessment of EMMA2 A-SMGCS operations on Milan Malpensa airport, Technical Report, 2010

[9] Conducting software reviews prior to certification, FAA, 2006

[10] CMMI for development, version 1.3, Technical Report, CMU/SEI, 2010

[11] Information technology − process assessment − part 5: an exemplar process assessment model, ISO, ISO/IEC 15504-5, 2006

[12] P. Johannessen, “Functional Safety Extensions to Automotive SPICE According to ISO 26262,” in *11th International Conference SPICE 2011*, Dublin: Ireland, Vol 155, pp 52-63, 2011

[13] EMMA, [Internet]. Available: http://www.dlr.de/emma/

[14] EMMA2, [Internet]. Available: http://www.dlr.de/emma2/

이 홍 석 (Hongseok Lee)
2011년 2월 : 아주대학교 전자공학과 (공학박사)
2010년 9월 ~ 현재 : 한국산업기술시험원 선임연구원
※ 관심분야 : 소프트웨어 평가, 기능 안전 소프트웨어, 프로세스 평가

권 구 훈 (Goohoon Kwon)
2012년 2월 : 충남대학교 전자전파정보통신공학과 (공학사)
2012년 6월 ~ 현재 : 한국산업기술시험원 연구원
※ 관심분야 : 기능 안전 소프트웨어, 프로세스 평가, 소프트웨어 정적 분석

고 병 각 (Byeonggak Ko)
2005년 11월 ~ 현재 : 한국산업기술시험원 선임연구원
※ 관심분야 : 기능안전 설계/검증, 소프트웨어 안전성/성숙도 평가