항공전자시스템 하드웨어/소프트웨어 개발 및 인증 접근 방식에 대한 10가지 제안사항 - 3. 항공기/시스템/HW/SW 개발의 동기화

정수영[1]*
수담연구소[1]

10 Suggestions for Avionics System Hardware and Software Development and Certification Approach - 3. Aircraft/Systems/HW/SW Development Synchronization

Suyoung Jeong[1]*

Key Words : Aircraft/System Development(항공기/시스템 개발), Avionics System Certification (항공전자시스템 인증), Safety Assessment(안전성 평가)

서 론

국내에서 수행 중인 항공전자시스템(3)/HW(4)/SW에 대한 개발 및 인증에 대해서 AAM/UAM 산업을 효과적으로 대응하고 이를 기반으로 향후 세계 시장까지 고려하는 '글로벌 스탠다드'를 기준으로 한 접근법에 대해서 지난 논문(1)에서 10가지 접근법을 제안한 바가 있다.

본 논문에서는 그 중 세 번째 제안인 '항공기/시스템/HW/SW 개발의 동기화'에 대해서 좀 더 상세하게 논하고자 한다.

본 론

1. 항공기/시스템/HW/SW 개발 동기화의 의미

지난 논문(1)에서 항공전자시스템에 대한 개발 지침서인 ARP4754A(3)와 ARP4761(2)을 기준으로 항공기/시스템/HW/SW의 개발 및 인증 과정 전체에서 수행되는 안전성 평가(Safety Assessment)의 개요를 보여주는 예시를 Figure 1과 같이 제시한 바가 있다.

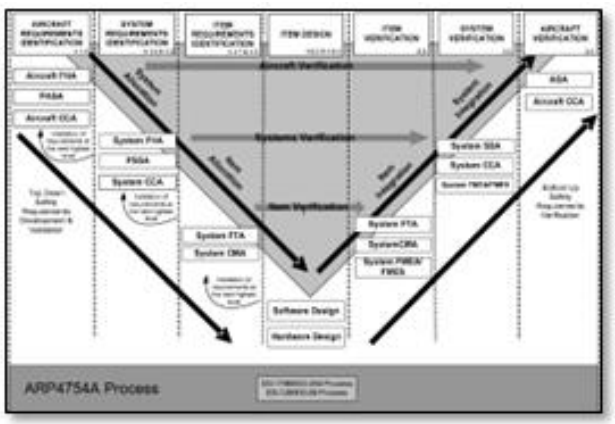

Fig. 1. Safety Assessment & Development

사실 Figure 1의 그림만 보자면 항공이 아닌 다른 업계에서도 일반적으로 제시되는 V모델과 다를바가 없다는 것을 알 수 있다. 다만 그림 최상단 및 최하단의 박스들을 제외하고 V모델 전체에 걸쳐서 표시되어 있는 작은 네모 박스들을 통해서 안전성 평가가 개발 과정의 모든 레벨에서 수행되고 있음을 확인할 수 있다.

사실 Figure 1의 그림은 단순히 일반적인 개발 흐름을 보여주는 것이 아니라 항공기 개발의 '실제'를 보여주는 것이다. 특히 항공기 개발에서 가장 중요한 안전성 평가의 단계별 수행 항목들과 시점, 그리고 연결지점을 제시하고 있다는 점에서 항공기/시스템/HW/SW 개발의 동기화를 잘 설명하고 있다고도 볼 수 있다.

이를 바탕으로 최대한 단순화시켜서 설명하자면 항공기/시스템/HW/SW 개발 동기화의 의미는 Figure 1의 그림 그대로 실제 개발 과정에 반영되고 실현된다는 것을 의미하며 이는 달리 말하면 그림과 같은 진행이 되지 못할 경우 항공기/시스템/HW/SW 개발의 동기화가 '이루어질 수 없다', 혹은 '이루어지지 않았다'를 말하는 것이라고 할 수 있다.

2. 항공기/시스템/HW/SW 개발 동기화 방법

그렇다면 Figure 1과 같이 항공기/시스템/HW/SW 개발의 동기화를 이룰 수 있는 구체적인 방법은 무엇일까?

사실 개발 과정에 대한 구체적인 방법 하나하나를 본 논문을 통해서 세세하게 제시하는 것은 현실적으로는 불가능하다고 할 수 있다. 그럼에도 이를 언급하는 것은 적어도 그러한 각각의 방법론에 담길 수 있는 원칙적인 부분을 찾을 수 있다고 보기 때문이다.

2.1 완전한(complete) 추적성

항공기/시스템/HW/SW 개발의 동기화를 위한 방법론에서의 첫 번째 원칙은 '완전한(complete) 추적성'을 달성하는 것이다. 추적성이라고 하면 일반적인 개발에서는 주로 '요구사항'이 초점인 경우가 많다. 사실 이는 항공기 개발에 있어서도 마찬가지며 요구사항 관점의 추적성에 대한 이해와 활용은 항공에서도 거의

유사한 모습을 확인할 수 있다. 하지만 항공인증 관점에서 추적성이 적용되는 범위는 그보다 훨씬 더 광범위한 영역이라고 할 수 있다.

본 논문에서 제시하는 확장된 추적성의 개념을 보여주는 것이 바로 Figure 2[(5)]이다.

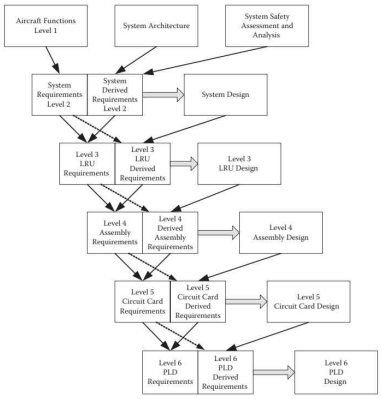

Fig. 2. Function/Requirement/Design/Safety

Figure 2는 최상위 레벨인 항공기의 기능/아키텍처/안전성 평가로부터 시작해서 중간 레벨의 요구사항/설계 그리고 가장 하위 레벨인 HW, 그 중에서도 PLD 레벨의 요구사항/설계에까지 연결되는 추적성을 화살표로 표시하고 있다. 여기서 중요한 점은 항공인증 관점에서는 Figure 2에서 표시된 화살표는 반드시 그림과 같은 형태로 '명시적'으로 연결되어야 하며, 만약 그림처럼 연결할 수 없는 항목이 존재한다면 그 자체는 '잘못된' 상태를 보여주는 것이라고 할 수 있다.

항공기/시스템/HW/SW 레벨의 동기화는 바로 이러한 연결성, 추적성을 말하는 것이며 이에 대한 완전성(completeness)을 요구하는 것이다.

2.2 근거 혹은 타당성(rationale)의 확보

항공기/시스템/HW/SW 개발의 동기화를 위한 방법론에서의 두 번째 원칙은 바로 '근거 혹은 타당성(rationale)의 확보'이다.

본 절에서 제안하는 '근거 혹은 '타당성(rationale)의 확보'는 사실 2.1에서 제시한 '완전한(complete) 추적성'과 유사한 개념이라고 할 수 있다. 즉 추적성이 연결된 상태라면 그렇게 연결된 추적성 자체가 본 절에서 말하는 '근거' 혹은 '타당성'이 되는 것이다.

다만 추적성은 그 속성상 요구사항 추적성과 같이 추적성 자체로 체계적인 관리 및 확인이 가능한 별도의 프로세스, 도구, 방법론이 주로 활용된다는 점에서 본 절에서 언급하는 '근거' 혹은 '타당성'과는 차이점이 있다. 참고로 '근거' 혹은 '타당성'에 대해서는 일반적으로 이슈 관리(Issue Management) 및 형상 관리(Configuration Management) 시스템이 주로 활용되는 것으로 볼 수 있다.

본 논문에서는 '완전한(complete) 추적성'과 더불어 항공기/시스템/HW/SW 개발의 동기화를 이룰 수 있는 구체적인 방법에 대한 원칙에 대해서 바로 이와 같은 '근거' 혹은 '타당성'의 확보를 제안한다.

이때 '근거' 혹은 '타당성'의 확보는 항공업계에서 많이 사용하는 다른 단어로 바꾸어서 표현하자면 '증빙(evidence)' 혹은 '산출물(artifacts)' 확보로 표현할 수 있다. 이는 결국 항공기/시스템/HW/SW 개발 및 인증 과정에서 수행되는 모든 활동에 대해서는 그 '근거' 혹은 '타당성'이 있어야 하며 그러한 활동의 결과를 증명할 수 있는 '증빙' 혹은 '산출물'을 제시할 수 있어야 함을 의미한다.

한편 이는 달리 말하면 '근거' 혹은 '타당성'이 없는 그 어떤 활동도 '수행되어서는 안된다'는 것을 의미하며 '증빙' 혹은 '산출물'이 없는 활동은 항공인증 관점에서는 사실상 어떤 활동도 '수행되지 않았다'는 의미가 될 수 있다. 그런 의미에서 항공기/시스템/HW/SW 개발의 동기화를 위한 '증빙' 혹은 '산출물'에 대해서는 이슈 관리 및 형상 관리가 철저하게 이루어져야 한다는 점도 유의할 필요가 있다.

결 론

지금까지 본 논문을 통해서 항공전자시스템/HW/SW 개발 및 인증 과정에 적용할 수 있는 개발의 동기화에 대한 의미, 그리고 구체적인 방법과 관련된 원칙적인 부분을 제안하였다.

한편 그러한 원칙적인 부분을 요구사항, 증빙, 산출물 등과 같은 실제 개발 현장에서 연결될 수 있는 대상으로 특정해서 접근함으로써 실무적인 관점에서 고려할 수 있을만한 구체적인 방법에 대해서도 참고가 될 수 있었다고 판단된다.

하지만 그럼에도 현장에서 실제로 선택할 수 있는 구체적인 방법은 프로그램, 조직, 환경 등에 따라서 다양할 수 있다는 점 역시 이해할 필요가 있다.

참고로 본 논문에서 제안하는 방식은 대부분의 항공인증 지침서에서 채택하고 있는 방식이므로 만약 기존 지침서를 기반으로 한 지식과 통찰력을 가지고 있는 상태라면 본 논문에서 제안하는 부분 역시 유사한 관점에서 이해하고 참고할 수 있을 것이다.

참고문헌

1) Suyoung Jeong, "10 Suggestions for Avionics System Hardware and Software Development and Certification Approach", ASSK, 2024.

2) SAE ARP4761, "GUIDELINES AND METHODS FOR CONDUCTING THE SAFETY ASSESSMENT PROCESS ON CIVIL AIRBORNE SYSTEMS AND EQUIPMENT", SAE Aerospace, 1996.

3) SAE ARP4754A, "Guidance for Development of Civil Aircraft and Systems", SAE Aerospace, 2010.

4) RTCA/DO-254, "Design Assurance Guidance For Airborne Electronic Hardware", April 19, 2000.

5) Randall Fulton, Roy Vandermolen, "Hardware Design Assurance - A Practitioner's Guide to RTCA/DO-254", CRC PRESS, 2015, pp. 74.