항공전자시스템 하드웨어/소프트웨어 개발 및 인증 접근 방식에 대한 10가지 제안사항 - 2. 개발 및 인증 전과정 안전성 평가 수행

정수영[1]*
수담연구소[1]

10 Suggestions for Avionics System Hardware and Software Development and Certification Approach - 2. Safety Assessment for whole Development and Certification Process

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 두 번째 제안인 '개발 및 인증 전과정 안전성 평가 수행'에 대해서 좀 더 상세하게 논하고자 한다.

본 론

1. 항공업계의 안전성 평가 접근법

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.

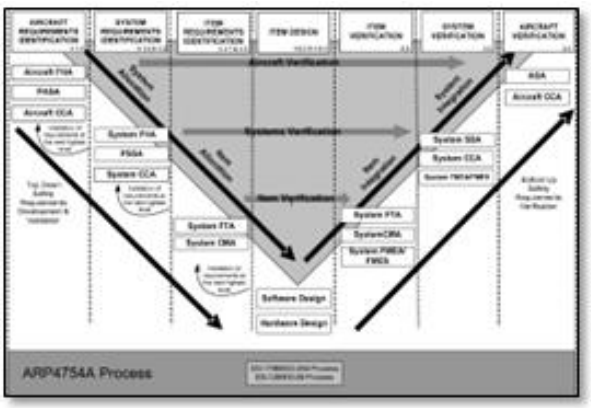

Fig. 1. Safety Assessment & Development

참고로 Figure 1의 그림에서 안전성 평가 항목 자체는 그림 최상단 및 최하단의 박스들을 제외하고 V모델 전체에 걸쳐서 표시되어 있는 작은 네모 박스들이라고 할 수 있다. 결국 위의 그림을 통해서도 항공업계의 안전성 평가는 개발 전 과정에서 이루어진다는 것을 확인할 수 있는 것이다.

비록 Figure 1이 상당히 단순화된 그림이기는 하지만 이를 통해서 항공기/시스템/HW/SW 개발 및 인증 과정이 안전성 평가에 상당히 큰 영향을 받는다는 것을 짐작할 수 있다. 실제적으로도 항공기/시스템/HW/SW 각 레벨별로 개별적인 안전성 평가가 수행되며 여기서 나온 결과는 해당 레벨의 설계 및 요구사항을 결정할 뿐만 아니라 상위 레벨의 결정 사항에 대한 근거가 되며 하위 레벨의 결정 사항에 대한 입력이 될 수 있다.

항공업계의 안전성 평가에 대한 접근법은 바로 이런 형태로 볼 수 있으며 특히 이런 과정 전체가 명시적으로 추적성을 유지하고 관리되며 전체적인 일관성을 유지한다는 점에서 특히 다른 업계와 상당한 차이를 보이는 부분이라고 할 수 있다.

다음 절에서는 항공업계와 유사하다고 볼 수 있을 정도로 엄격한 안전성 평가가 이루어지는 자동차 분야(Automotive)와의 비교를 통해서 항공전자시스템/HW/SW 개발 및 인증 접근법에서 우리가 주목해야 할 안전성 평가에 대한 특징을 확인해 보자.

2. 안전성 평가 - Automotive vs Aviation

결론부터 정리하자면 자동차업계에서 이루어지고 있는 안전성 평가와 항공업계에서 이루어지고 있는 안전성 평가는 '사실상' 유사한 방식이라고 볼 수 있다. 그런 가운데에도 유의할 만한 차이점이 존재하는데 여기에는 세부적인 방법론이나 과정의 차이도 있지만 가장 큰 차이점은 무엇보다도 각 레벨끼리 연결되는 명시적인 추적성이라고 할 수 있다.

여기서 우선 자동차와 항공기에서 수행되는 안전성 평가에 대한 비교부터 정리해 보자.

Table 1. Automotive vs Aviation

안전성 평가 - Automotive (ISO 26262)	안전성 평가 - Aviation (ARP4754A, ARP4761)
▪ Item Definition ▪ Hazard Analysis and Risk Assessment(HARA) ▪ Safety Goals ▪ ASIL ▪ Safety Requirements ▪ System Design - Hardware, Software ▪ Safety Analysis - FMEA, FTA, DC ...	▪ Function Design ▪ Functional Hazard Assessment(FHA) - Aircraft/System FHA ▪ Safety Requirements ▪ FDAL/IDAL ▪ System Design - Architecture, HW, SW ▪ Safety Analysis - FMEA, FMES, FTA, CCA

참고로 Table 1은 안전성 평가에 많이 사용되는 도구인 Ansys medini analyze의 사용자 매뉴얼[5]에서 제시하는 각 분야의 안전성 평가와 관련된 주요 항목들을 정리한 것으로 실제 현장에서 사용되는 도구를 참고함으로써 이론적인 관점만이 아닌 실무적인 관점에서의 결과를 보여주는 것이라고 할 수 있다.

사실 Table 1을 통해서 자동차와 항공기에 적용되는 안전성 평가의 유사성을 확인할 수 있는 것은 사실이지만 단순히 위의 표 하나만으로 자동차와 항공기에 적용되는 안전성 평가의 유사점 및 차이점을 완전히 파악할 수 있는 것은 아니다.

하지만 Table 1의 근거가 되는 해당 매뉴얼뿐만 아니라 업계의 지침서, 관련 자료 등을 통해서 확인한 바로는 Table 1에서 보여주는 유사성만큼이나 실제 수행되는 과정, 결과 등에서도 상당한 유사성을 확인할 수 있었으며 활용된 방법(methods) 및 결과물 자체를 통해서도 그 유사성을 확인할 수 있었다. 즉, 자동차에서 적용되는 안전성 평가 방법(methods)이 항공기에도 거의 동일하게 적용될 수 있음을 확인할 수 있었다.

3. 항공인증을 위한 안전성 평가 적용

자동차와 항공기에 적용되는 안전성 평가가 아무리 유사하다고 하더라도 결국 중요한 것은 항공전자시스템/HW/SW 개발 및 인증을 위해서 안전성 평가를 수행하는 방법이 앞서 살펴본 배경을 기준으로 실무에서 실제 어떻게 적용되느냐이다. 이에 대해서는 앞서 Figure 1을 통해서 개발 과정 전체에서 각 레벨별로 모두 안전성 평가를 수행해야함을 언급한 바가 있다.

이를 조금 더 구체화하자면 바로 항공전자시스템 개발 지침서인 ARP4754A에서 제시하는 Figure 2[3]로 표현할 수 있다.

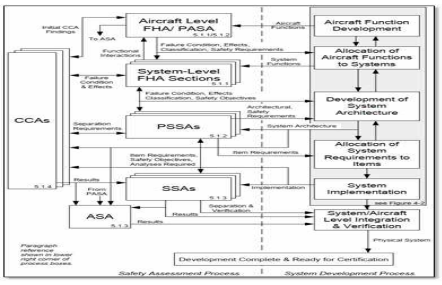

Fig. 2. Safety Assessment Process Model

Figure 2는 가장 최상위의 항공기 레벨에서부터 가장 하위 레벨이라고 할 수 있는 하드웨어/소프트웨어 레벨까지의 각각의 진행 과정에서 실제 수행되어야 할 각각의 안전성 평가 방법(methods)과 연결을 세부적으로 보여주고 있다.

물론 모든 과정이 이처럼 선형적이고 고정된 형태인 것은 아니지만 적어도 이런 흐름과 연결성이 명시적으로 이루어져야 하며 각각의 결과물이 확보되고 궁극적으로는 인증당국에 제공되어 확인될 수 있어야 한다는 점을 명심해야 한다.

현실적으로 항공기를 제외한 다른 업계의 일반적인 개발 현장에서는 안전성 평가가 Figure 2와 같은 방식으로 수행되는 경우는 거의 없는 것이 사실이다. 다만 자동차 업계에서는 이와 유사한 활동을 구체적으로 수행하고 있으며 관련된 산출물을 생성하고 활용하는 경험과 노하우를 보유하고 있기 때문에 항공업계의 이러한 접근에 있어서 상당히 많은 부분을 참고할 수 있을 것으로 예상된다.

결 론

지금까지 본 논문을 통해서 항공전자시스템/HW/SW 개발 및 인증 과정에 적용하는 안전성 평가에 대한 접근법, 방법, 과정, 전략 등을 개략적으로 제시하였다. 하지만 결국 가장 중요한 것은 이러한 안전성 평가 활동을 개발 현장에 직접 반영해서 구체적인 수행 방법과 과정을 실제로 경험하는 것이다.

항공전자시스템/HW/SW가 점점 더 복잡해지고 그에 따라서 개발 과정 역시 점점 더 복잡해지고 있음을 고려한다면 특히 지금까지 한 번도 안전성 평가라는 부분을 접해보지 못한 조직인 경우 기존 개발 과정에 안전성 평가를 추가하는 것은 기존 실무자들에게는 감당하기 어려운 상당한 부담이 가중될 수 있다는 점을 명확하게 이해하고 그것을 극복하기 위해 적극적으로 대응해 나갈 것을 제안하는 바이다.

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) Ansys, “Ansys medini™ analyze User Guide“, 2023, pp. 263~274.