항공전자시스템 하드웨어/소프트웨어 개발 및 인증 접근 방식에 대한 10가지 제안사항 - 7. 증빙(evidence) 기반의 활동

정수영[1]*
수담연구소[1]

10 Suggestions for Avionics System Hardware and Software Development and Certification Approach - 7. Activities based on Evidence

Suyoung Jeong[1]*

Key Words : Aircraft/System Development(항공기/시스템 개발), Avionics System Certification (항공전자시스템 인증), Evidence(증빙), Outputs(출력), Artifacts(산출물)

서 론

국내에서 수행 중인 항공전자시스템[(2)]/HW[(3)]/SW[(4)]에 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 일곱 번째 제안인 '증빙(evidence) 기반의 활동'에 대해서 좀 더 상세하게 논하고자 한다.

본 론

1. 항공 인증에서 증빙(evidence)의 중요성

항공 인증과 관련해서 다음과 같은 표현이 있다. "Guilty until proven." 즉, 직관적으로 표현하자면 '증명하기 전까지는 유죄'라는 것이다.

흔히들 '무죄추정의 원칙'이라는 말을 많이 사용하는데 이런 우리말과 정반대의 관점이라고 볼 수 있는 이 표현은 주로 항공 인증의 감사(Audit)와 관련해서 일반적으로 인증 당국 혹은 DER(Designated Engineering Representative)이 가지는 관점이라고 볼 수 있다.

실질적으로 이러한 관점을 가진 인증 당국 혹은 DER을 '납득'시키기 위해 궁극적으로 제시해야 하는 것이 바로 '증빙(evidence)'인 것이다. 따라서 항공 인증 관점에서 증빙이라는 것은 공식적인 인증을 위한 결정적인 항목이라고 할 수 있다.

항공 인증 관점에서 항공전자시스템/HW/SW는 일반적으로 '복잡(complex)'하다고 표현한다. 여기서 complex라는 단어는 단순히 사전적인 의미뿐만 아니라 실질적으로는 항공 인증에서 요구하는 안전성(safety)을 증명하기가 상당히 어렵다는 것을 내포하고 있다. 즉, 정량적인 증거를 제시하는 것이 거의 불가능하다는 것이다.

이에 대해서 항공 업계는 개발 보증(Development Assurance)의 개념을 적용하고 있다. 참고로 이는 지침서에 따라서 품질 보증(Quality Assurance), 프로세스 보증(Process Assurance), 설계 보증(Design Assurance) 등의 용어로도 사용되고 있는데 결과적으로 모두 비슷한 의미로 사용된다고 할 수 있다.

결론적으로 항공 인증 관점에서는 이러한 개발 보증을 통해서 '복잡(complex)'한 항공전자시스템/HW/SW에 대한 안전성을 증명하게 되며 여기서 '증빙(evidence)'이 아주 중요한 역할을 수행하게 되는 것이다.

2. Evidence vs Outputs vs Artifacts

지침서를 비롯한 항공 인증과 관련된 다양한 자료들을 참고하다 보면 'Evidence'라는 단어와 함께 'Outputs', 'Artifacts'라는 단어들이 자주 사용되는 것을 볼 수 있다. 그런데 이 단어들이 실제 현장에서 뒤섞여 사용되다 보니 때로는 용어 자체로 인한 일부 혼선이 있는 것도 사실이다.

결론적으로 이 세 단어 모두 항공 인증 관점에서는 사실상 동일한 용도로 사용될 수 있다. 즉 이들 단어가 모두 항공 인증 관점에서 '증빙'의 의도로 사용될 수 있는 것이다. 물론 구체적인 사용처, 문맥 등에 따라서 미묘한 차이점이 있지만 실제 항공 인증 수행 과정에서는 굳이 엄격한 구분을 둘 필요는 없다는 점을 기억하자.

참고로 위의 단어 중 'Output'은 특히 ARP4754A, DO-254, DO-178C, DO-330, DO-331, DO-332, DO-333 등의 지침서에서 공식적으로 'Objective'라는 단어와 매칭되어 Figure 1[(2)], Figure 2[(4)]와 같은 형태로 사용되고 있다.(붉은색 박스)

Objective		Section	Applicability and Independence by Development Assurance Level (see 5.2.3)					Output	System Control Category by Level (see 5.6.2.6)					Comments
Objective No.	Objective Description		A	B	C	D	E		A	B	C	D	E	
2.0 Aircraft and System Development Process and Requirements Capture														
2.1	Aircraft-level functions, functional requirement, functional interfaces and assumptions are defined	4.1.4 4.2 5.3	R	R	R	R	N	List of Aircraft-level functions Aircraft-level Requirements	①	①	①	②		Note: Requirements capture process objectives presented in section 5.3 are included in this development process

Fig. 1. Objective & Outputs (ARP4754A)

	Objective		Activity	Applicability by Software Level				Output		Control Category by Software Level			
	Description	Ref	Ref	A	B	C	D	Data Item	Ref	A	B	C	D
1	High-level requirements are developed.	5.1.1.a	5.1.2.a 5.1.2.b 5.1.2.c 5.1.2.d 5.1.2.e 5.1.2.f 5.1.2.g 5.1.2.j 5.5.a	O	O	O	O	Software Requirements Data Trace Data	11.9 11.21	①	①	①	①

Fig. 2. Objective & Outputs (DO-178C)

3. 항공 인증을 위한 증빙 기반의 활동

2장에서 '증빙'과 관련된 여러 단어들을 제시하기는 했지만 결국 가장 중요한 것은 이러한 '증빙(evidence)'을 항공 인증에 실제로 어떻게 적용하느냐가 될 것이다.

앞서 Figure 1, 2를 통해서 각각의 지침서에서 제시하는 Objective, 그리고 그것과 매칭되는 Output을 살펴본 바가 있다. 기본적으로는 바로 이 Output을 '증빙(evidence)'으로 확보하는 것이 그 출발점이 될 것이다. 다만 여기서 유의할 점은 지침서에서 제시하는 Output을 '증빙(evidence)'의 유일한 대상으로 한정해서는 안된다는 점이다.

특히 항공전자시스템/HW/SW와 같은 '복잡(complex)'한 인증 대상인 경우에는 지침서에서 제시하는 Output만을 증빙으로 판단하는 경우 자칫 인증 준비 및 대응에 상당한 지장을 줄 수 있다. 즉, 내가 판단하는 인증 '증빙(evidence)'과 인증 당국이 판단하는 인증 '증빙(evidence)'이 서로 다를 수 있는 것이다. 이럴 경우 소위 지침서대로 잘 준비한 것 같은데도 그것만으로는 충분하지 않다는 것을 너무 늦게 깨닫게 될 수도 있다.

참고로 항공전자SW 인증에 대한 지침서인 DO-178C에는 Figure 3[4]과 같이 'SCM Records'를 Output으로 제시하는 경우가 있다.(붉은색 박스)

	Objective		Activity	Applicability by Software Level				Output	
	Description	Ref	Ref	A	B	C	D	Data Item	Ref
1	Configuration items are identified.	7.1.a	7.2.1	O	O	O	O	SCM Records	11.18
2	Baselines and traceability are established.	7.1.b	7.2.2	O	O	O	O	Software Configuration Index SCM Records	11.16 11.18

Fig. 3. Outputs - SCM Records (DO-178C)

앞서 언급한 것처럼 Figure 3에서 제시하고 있는 Output은 항공전자SW 인증을 위한 '증빙(evidence)'으로 사용될 수 있다. 그렇다면 여기서 SCM Records는 구체적으로 무엇일까?

일단 해당 표에 기술된 Objective를 기준으로 용어 자체만 보자면 '형상 관리 결과물'정도로 이해할 수 있을 것이다. 그렇다면 여기서 말하는 '형상 관리 결과물'은 구체적으로 무엇을 말하는 것일까?

참고로 DO-178C 지침서에서는 본문의 Section 11.18에서 SCM Records를 다음과 같이 조금 더 상세하게 설명하고 있다.

11.18 Software Configuration Management Records

The results of the SCM process activities are recorded in SCM Records. Examples include configuration identification lists, baseline or software library records, change history reports, archive records, and release records. These examples do not imply that records of these specific types need to be produced.

Note: Due to the integral nature of the SCM process, its outputs will often be included as parts of other software life cycle data.

Fig. 4. SCM Records (DO-178C)

그런데 과연 Figure 4[4]를 보고 우리는 '형상 관리 결과물'을 구체적인 '증빙(evidence)'으로 준비할 수 있을까?

우리가 항공 인증을 위한 '증빙(evidence)'을 확보하는 것은 결국 증빙 대상의 속성을 정확하게 파악하는 것에서 출발한다고 볼 수 있다. 물론 이는 지침서를 통해서 일차적으로 파악할 수 있지만 문제는 지침서의 내용이 모든 현장의 케이스들을 하나하나 상세하게 '지정'할 수는 없다는 점이다. 결국 인증 당국에서 요구하는 부분을 정확하게 파악하는 것이 관건이며 인증 당국이 '받아들일 수 있는 증빙(evidence)'을 제시하는 것이 중요하다.

본 논문에서 제안하는 '증빙(evidence) 기반의 활동'이라는 것은 결국 이런 관점을 담고 있는 것이다. 그리고 이는 지난 논문[1]에서 제안한 10가지 접근법 전체와 연계해서 이해하고 실천해야 하는 부분이라고 할 수 있다.

결 론

지금까지 본 논문을 통해서 '증빙(evidence) 기반의 활동'에 대한 의미와 중요성을 살펴보았다. 특히 지침서에서 제시하는 Output에 대한 실질적인 범위를 이해하고 인증 당국이 요구하는 '증빙(evidence)'을 어떻게 확보해서 제시할 것인가에 대해서도 살펴보았다.

항공 인증에 대한 적절한 대응을 위해 증빙과 관련된 이런 관점을 이해하고 지난 논문[1]의 다른 제안들과 연계한다면 항공 인증을 위한 증빙과 관련해서 현장에서 발생할 수 있는 다양한 변수들에 대한 대처에 상당한 도움이 될 수 있을 것이다.

참고문헌

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

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

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

4) RTCA/DO-178C, "Software Considerations in Airborne Systems and Equipment Certification", December 13, 2011.