시스템 안전성평가를 통한 효율적 요건 도출방안 연구

유승우* · 정진평* · 이백준*

A Study on the Safety Requirements Establishment through System Safety Processes

Seung-woo Yoo* · Jinpyong Jung* · Baeck-Jun Yi*

ABSTRACT

Safety requirements for aircraft and system functions include minimum performance constraints for both availability and integrity of the function. These safety requirements should be determined by conducting a safety assessment. The depths and contents of aircraft system safety assessment vary depending on factors such as the complexity of the system, how critical the system is to flight safety, what volume of experience is available on the type of system and the novelty and complexity of the technologies being used. Requirements that are defined to prevent failure conditions or to provide safety related functions should be uniquely identified and traceable through the levels of development. This will ensure visibility of the safety requirements at the software and electronic hardware design level.

This paper has prepared to study on promoting the efficiency of establishing hierarchical safety requirements from aircraft level function to item level through system safety processes.

Key Words: System Safety Assessment, Safety Requirements, Functional Hazard Assessment, Preliminary System Safety Assessment, Development Assurance, System Architecture

1. 서 론

항공기의 개발 및 인증 과정에서 중요성이 강조되고 있는 시스템 안전성의 개념은 고장 안전(Fail-Safe) 또는 시스템 백업이 포함된 다중설계에 대한 검증을 위해 도입되었으며, 항공기 시스템의 통합성 및 복잡성이 증가함에 따라 기존의 방식으로는 적절한 안전성평가가 불가능하기 때문에 항공기 안전성평가를 위한 기법, 기준 및 표준절차는 지속적인 연구가 이루어지고 있다. 여기서 안전성이라 함은 시스템이 위험상태에 이르지 않는 상태 또는 정도를 의미하며, 항공기 및 시스템의 결함 또는 고장으로 인하여 발생할 것으로 예상되는 위험을 사전에 식별하

†2008년 6월 25일 접수 ~ 2013년 6월 29일 심사완료
* 정회원, 한국항공우주연구원
연락저자, E-mail: swyoo@kari.re.kr

고, 이들 사이의 상호 연관성 또는 발생 메커니즘을 규명하여 설계단계에서부터 이를 제거하거나 허용안전수준(Acceptable Level of Safety) 이하로 낮추기 위한 종합 안전 관리대책을 적용하는 것이 시스템 안전성평가의 개념이다[1].

최근에는 항공기의 임무 및 성능에 대한 기대수준이 높아지고, 운용 환경의 변화에 따라 보다 다양한 전자기술이 적용되면서 항공전자시스템(Avionics)의 중요성이 날로 증대되고 있다. 전통적이고 복잡하지 않은 시스템은 개발 완료 이후의 시험 또는 분석을 통해 검증하는 것이 가능하였으나, 최신 전자기술 및 소프트웨어 기반 기술 등이 적용되어 복잡하고 통합적인 기능을 수행하는 복합 시스템의 경우에는 개발 완료 후의 검증만으로는 요건의 충족 여부 및 시스템 안전성을 평가할 수 없다는 것이 산업계의 중론이다. 이에 따라 복합 전자하드웨어(Complex Electronic Hardware, CEH) 기술 또는 소프트웨어 기반기술이 적용되는 최신 항공기 및 시스템에 대해 개발보증(Development Assurance)이라는 개념을 도입하여 항공기 고장상태(Failure Condition)의 원인이 되거나 영향을 줄 수 있는 오류의 가능성을 개발 초기 단계에서부터 제거하는 방식이 적용되고 있다. 이와 같은 복합 시스템의 경우에는 여러 프로세스 보증의 조합, 확인(Validation) 및 검증(Verification) 적용범위(Coverage) 기준, 항공기 및 통합 시스템 수준은 물론 시스템 인터페이스에 대하여 체계적인 분석 및 평가 기법을 적용하는 개발보증 기법을 적용하며, 이를 통해 요건 또는 설계상의 오류와 상호 영향성이 적절하게 식별되어 수정되었는지 확인할 수 있다[2, 3].

항공기 및 시스템 개발과정에서 요구되는 시스템 안전성평가 프로세스, 복합 전자하드웨어 및 소프트웨어의 개발보증을 위한 기준 및 라이프사이클 지침, 그리고 항공기 운용과정에서 감항성 유지 및 안전성 관리를 위한 지침서로 준용되고 있는 문서들은 다음 그림 1과 같으며, 본 논문에서는 항공기 개발 및 인증과정에서 요구되는 시스템 안전성평가에 대한 최신 연구동향과 함께 효율적인 안전성 요건을 도출하기 위하여 고려해야 하는 사항에 대하여 논하고자 한다.

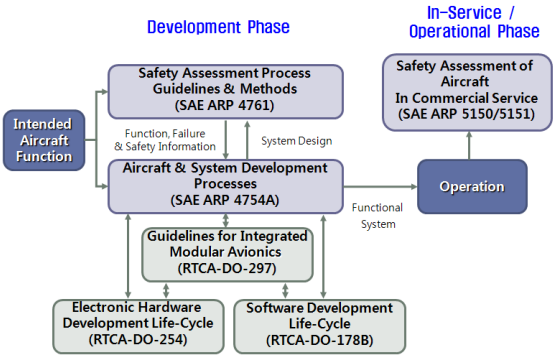

Fig. 1 항공용 시스템 안전성평가 관련 문서

2. 항공기 및 시스템 요건의 유형

항공기 및 시스템 개발과정에서 도출되는 요건의 효율성 및 적절성은 항공기 개발은 물론 인증 과정에서 요구되는 적합성 입증 활동, 비용, 일정 등에 막대한 영향을 주게 되므로 개발 초기부터 최적화된 요건을 수립하는 것은 매우 중요하다. 또한 인증 요건을 비롯한 일부 안전성 요건에 대해서는 적합성 입증이 요구되기 때문에 요건 도출을 위한 계획 및 기준을 수립하여 인증당국과 사전에 협의하는 것이 필요하다.

2.1 기능 요건 (Functional Requirements)

기능 요건은 항공기 시스템 요구 성능, 고객의 기대사항, 운용 제한사항, 각종 규정에 의한 제한사항 및 시스템 구현을 위한 현실 조건 등이 반영되어 도출된다. 항공기의 형식, 항속거리, 운용속도, 특정 기능, 운용 방식 및 정비 방식 등이 이에 해당된다. 요건의 출처가 기능 요건에 해당되더라도, 기능의 안전에 관계되는 사항은 안전성 요건과 동일하게 평가되어야 한다.

2.2 인증 요건 (Certification Requirements)

인증 요건은 우리나라의 항공기 기술기준(KAS, Korean Airworthiness Standard), 미국의 FAR(Federal Aviation Regulation) 또는 유럽연합의 CS(Certification Specifications) 등과 같이 각 국가별로 규정하고 있는 감항 기술기준(Airworthiness Standard)과 적합성 입증을 위해 기능, 특성 또는 시스템 구현 등의 측면에서 추가적으로 도출되는 요건이 이에 해당된다. 추가적인 적합성 입증 요건에는 설계에 대한 요건 외에도 제작, 분석, 검사 및 시험평가 등의 세부 절차 및 인증당국이 제시하는 지침서(국토교통부 고시, 미연방항공청(FAA)의 Advisory Circular 또는 유럽연합의 Acceptable Means of Compliance)의 내용이 이와 같은 유형의 요건에 해당한다.

2.3 안전성 요건 (Safety Requirements)

항공기 및 시스템 수준의 안전성평가 프로세스를 통해 도출되는 안전성 요건은 관련 기능의 고장상태를 식별하고 고장영향을 평가하여 결정된 고장영향등급에 따라 설정된다. 안전성 요건은 개별 고장상태를 논리적으로 식별하고, 이에 대한 영향을 평가하기 위하여 항공기 및 시스템 개발 초기에 수행되는 기능위험평가(FHA, Functional Hazard Assessment) 이후에 설정된다. 항공기 개념설계 단계에서 항공기에 요구되는 기능을 식별하고, 해당 기능의 고장상태에 대한 영향성을 판단하여 고장영향등급을 설정하는 것이 항공기 수준 기능위험평가이며, 항공기의 기능을 시스템으로 배분한 이후에는 개별 시스템에 대하여 시스템 기능위험평가를 수행하여야 한다.

Table 1. 고장상태 영향평가를 위한 기준 및 등급별 안전성 요건

Classification of Failure Conditions	No Safety Effect	Minor	Major	Hazardous	Catastrophic
Effect on Airplane	No effect on operational capabilities or safety	Slight reduction in functional capabilities or safety margins	Significant reduction in functional capabilities or safety margins	Large reduction in functional capabilities or safety margins	Normally with hull loss
Effect on Occupants	Inconvenience for passengers	Physical discomfort for passengers	Physical distress to passengers, possibly including injuries	Serious or fatal injury to an occupant	Multiple fatalities
Effect on Flight Crew	No effect on flight crew	Slight increase in workload or use of emergency procedures	Physical discomfort or a significant increase in workload	Physical distress or excessive workload impairs ability to perform tasks	Fatal Injury or incapacitation
Allowable Qualitative Probability	No Probability Requirement	Probable	Remote	Extremely Remote	Extremely Improbable
Allowable Quantitative Probability	No Probability Requirement	$<10^{-3}$	$<10^{-5}$	$<10^{-7}$	$<10^{-9}$
SW & Complex HW DALs	E	D	C	B	A

기능위험평가를 통해 설정된 고장영향등급에 따라 안전성이 확인되어야 하는 요건이 설정되며, 소프트웨어 및 복합 전자하드웨어의 개발보증수준이 결정되는데, 수송급 항공기 및 회전익 항공기에 요구되는 기준은 표 1과 같다.

안전성 요건에는 독립성, 정량적 확률 요건, 정성적 요건, 가용성, 통합성, 모니터링, 개발보증수준, 운용 요건 및 정비 요건 등이 있다.

2.4 파생 요건 (Derived Requirements)

항공기 개발 단계별로 특정 요건 또는 일련의 요건들을 어떻게 충족할 것인가에 대한 설계 측면에서의 의사결정이 이루어지게 되며, 이는 그 다음 개발 단계의 요건으로 설정된다. 이와 같은 파생 요건은 설계 프로세스의 결과에 의한 것으로서 상위 수준의 요건으로부터 할당되는 것이 아니라는 특징이 있으며, 파생 요건에 대해서는 해당 항공기 수준 기능의 고장영향등급이 적절하게 구분되었고, 해당 안전성 요건이 유효한지 확인하여야 한다. 파생 요건은 상위 수준 요건에 영향을 주지 않지만 일부의 경우에는 상위 수준과 관계가 있을 수도 있으므로, 하위수준에서부터 상향식으로 안전성평가 결과에 대한 영향이 없는지 확인하여야 한다. 이와 같은 파생 요건은 다음과 같은 사례와 같이 요건을 구체화하고 추적 관리해야 한다.

(1) 특정 기능을 위한 장비에 대해서는 독립된 전원이 공급되어야 한다는 요건이 설정될 수 있으며, 이와 같은 전원 공급 요건이 적용되는 기능의 결함 또는 고장으로 인한 고장상태에 대해서는 안전성 요건에 해당하는 개발보증수준이 추가적으로 요구된다.

(2) 파생 요건은 설계 단계에서 확정된 시스템 구조에 따라 도출될 수도 있다. 예를 들어, 고장영향등급이 높은 수준으로 구분되어 정량적인 안전성 요건이 높게 할당되며, 이를 충족하기 위해 3중 구조를 선택한 시스템 구조의 경우에는 동일한 확률목표 달성을 위해 2중 구조를 선정한 경우와는 다른 결과 및 다른 파생 요건이 도출된다는 것이다.

(3) 파생 요건은 낮은 고장영향등급에 해당하는 시스템의 고장이 발생하는 경우에 대비하기 위하여, 높은 고장영향등급에 해당하는 기능을 수행하는 시스템을 별도로 격리하여 장착하는 설계를 채택하는 경우에도 도출될 수 있다.

(4) 복합 전자하드웨어-소프트웨어 인터페이스에 대한 정의도 파생 요건에 포함될 수 있으며, 이러한 요건은 시스템 안전성예비평가를 통해 개발보증수준 형태의 안전성 요건으로 설정된다. 이와 같은 요건은 RTCA DO-178B (또는 EUROCAE ED-12B) 및 RTCA DO-254 (또는 EUROCAE ED-80)의 지침에 따라 개발보증 활동을 통해 확인되어야 한다.

3. 안전성평가를 통한 계층별 안전성 요건 도출

안전성 요건은 항공기, 시스템, 서브시스템, 유닛, 구성품 및 부품 등의 계층에서 각각 도출된다. 이와 같은 안전성 요건을 도출하는 과정 중 중요한 단계는 안전성 예비평가절차로서 SAE ARP 4754 개정본(Rev.A)에서는 항공기 안전성 예비평가(PASA, Preliminary Aircraft Safety Assessment)와 시스템 안전성 예비평가(PSSA, Preliminary System Safety Assessment)로 구분하여 수행하도록 권고하고 있다[4]. 항공기 수준의 기능을 대상으로 하는 항공기 기능위험평가를 통해서 도출되는 요건들은 항공기 수준의 요건으로 설정되고, 항공기 수준의 안전성 요건보다 세분화된 시스템 수준의 안전성 요건은 시스템 기능위험평가로부터 도출된다.

이와 같이 안전성 예비평가 프로세스를 2단계로 구분한 이유는 상위 수준에서부터 하향식으로 요건을 할당하는 과정뿐만 아니라, 하위 수준에서부터 설계의 실현 가능성, 개발과정에서 발생하는 고장모드, 그리고 초기 설계 및 기능위험평가 단계에서 적용한 가정(Assumption) 및 권고(Recommendation) 사항 등에 대한 타당성

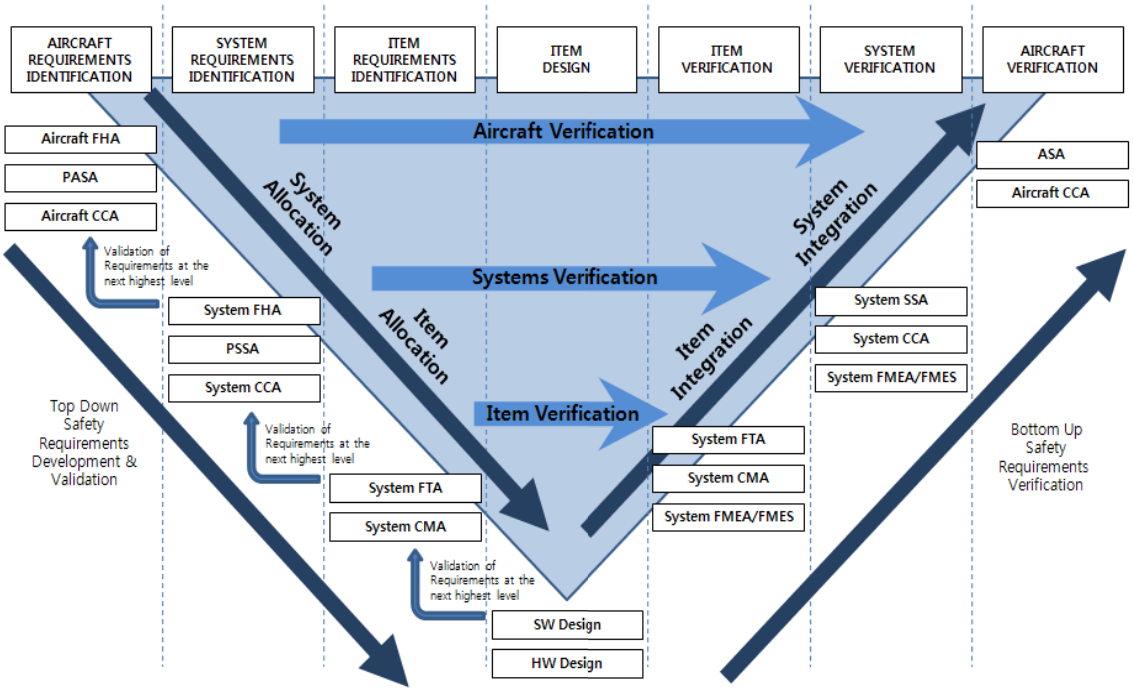

Fig. 2 시스템 안전성평가 및 항공기 개발 과정

확인(Validation) 과정이 매우 중요하고, 설계 진행에 따라 반복적으로 수행되므로 상당한 업무량 및 시간이 소요되기 때문이다. 다음 그림 2는 안전성 요건 설정 및 검증 절차를 통해 항공기 개발단계에서 도출되는 요건의 다양한 수준을 도식화한 것으로서, 일부 안전성 요건은 공통원인분석(CCA, Common Cause Analysis)을 통해서도 도출될 수도 있다.[5, 6]

3.1 항공기 수준 기능 설정 및 시스템 수준 요건 할당

이 단계에서는 항공기 수준의 성능 및 운용 관련 기본 요건을 설정하여 이로부터 항공기 수준의 기능 및 요건을 도출하고, 외부의 물리적 운용 환경과의 기능 인터페이스를 확정한다. 항공기 수준에서 기능을 설정하는 것은 상위 수준의 활동으로서 단순히 한 가지의 시스템 구현에만 관계되는 것이 아니므로, 하위 시스템의 설계 변경이 이루어질 경우 다시 반복하여야 한다. 시스템 설계가 확정되면 항공기 기능을 적절하게 그룹화하여 항공기 수준의 기능을 해당 시스템 수준 요건으로 할당하게 된다.[7]

3.2 시스템 구조 및 아이템 수준 요건 할당

시스템 구조를 구체화하는 단계로서, 모든 안전성 요건과 기술적 성능 요건을 충족하기 위하여 설계되는 시스템 내부 구조 및 경계를 결정하는 과정이다. 설계가 진행되면서 시스템 내부의 구조 및 아이템의 위치와 환경조건 등이 확정되고, 설계가 변경되는 경우 반복적으로 수행되어야 한다. 이와 같은 사이클이 반복됨에 따라 요건에 대한 식별 및 충실도는 증가하게 되며, 복합 전자하드웨어 또는 소프트웨어 수준으로 할당되는 시스템 수준의 요건은 더욱 명확해진다. 해당 기능에 대한 안전성 목표와 고장상태 위험에 대한 심각도에 따라 복합 전자하드웨어 또는 소프트웨어에 할당되는 요건과 개발보증수준, 기능 및 성능 요건 등과 같은 안전성 요건이 해당 수준별로 확정된다.[8]

3.3 시스템 구현 및 통합을 위한 요건 설정

항공기 및 시스템과 같은 상위수준에서부터 하향식으로 할당되는 요건과 달리 개발과정에 따라 시스템 구현 및 통합을 위한 요건이 설정되기도 한다. 특히 소프트웨어 및 복합 전자하드웨어에 대해서는 DO-178B/ED-12B 및 DO-254/ED-80의 지침을 준수할 필요가 있다. 이 문서들은 인증당국에서 발행한 기준서는 아니지만, 항공기 인증과정에서 소프트웨어 및 복합 전자하드웨어의 수명주기(life cycle) 지침서로서 준용되고 있다. 이 단계에서는 항공기 시스템을 개별적으로 또는 통합하여 검증하기 위한 요건도 설정되며, 복합 전자하드웨어-소프트웨어 통합 절차, 시스템 통합 절차, 하드웨어 도면, 관련 문서를 포함한 소프트웨어 소스 코드, 해당 개발보증 데이터, 브레드보드 또는 시제 하드웨어 및 실험실/비행시험체 등이 이에 해당된다.

4. 결 론

본 논문에서는 항공기의 개발 및 인증과정에서 필요한 시스템 안전성평가 과정에 대한 최신 동향과 효율적인 안전성 요건을 도출하기 위하여 고려해야 하는 사항에 대하여 살펴보았다. 안전성 요건은 주로 항공기 안전성 예비평가(PASA)와 시스템 안전성 예비평가(PSSA)를 통해 확정되며, 도출되는 안전성 요건은 반드시 문서화되어야 한다. 안전성 요건은 해당 내용에 따라 개발규격서, 업무절차서, 구매요구서, 설계지침서, 시험계획서 및 안전성평가보고서 등 항공기 개발을 위한 다양한 문서에 반영되는데, 설계변경의 빈도 및 범위에 따라 이 내용을 추적하여 개정하는 업무가 상당히 방대할 수도 있으므로, 체계적인 문서 체계 및 관리 절차가 확보되어야 한다.

그리고 시스템 개선을 위한 설계 변경은 상위수준에서부터 할당되어 내려오는 경우도 있지만, 하위수준 또는 실제 운용을 통한 피드백 과정을 통해 다시 항공기 수준에 영향을 주기도 하므로, 이와 같은 반복을 최소화하기 위해서는 설계 초기부터 운용과정 및 계속 감항성 유지 측면까지 고려하여야 한다. 특히, 항공기 시스템이 단순하지 않은 경우에는 관련 시스템 및 부품의 통합으로 인해 야기되는 추가적인 복잡성 및 상호의존성으로 인해 사전에 예상하지 못한 문제가 발생할 수가 있으므로, 요건 설정단계에서 적절한 여유(Margin)를 확보할 수 있도록 항공기 수준에서부터 통합 관리하여야 한다.

참 고 문 헌

[1] SAE ARP 4761, Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment

[2] 유승우, 이종희, “항공기 시스템 안전성평가 효율화 방안 연구”, 항공우주시스템공학회지, 제 6권, 제 3호, 2012, pp. 7-12.

[3] Frank C. Fickeisen, "Improving the Effectiveness of Airplane Certification Analysis Processes", SAE 2001-01-2664,

[4] SAE ARP 4754 Rev. A, Guidelines for Development of Civil Aircraft and Systems

[5] RTCA DO-178B, "Software considerations in airborne systems and equipment certification"

[6] RTCA DO-254, "Design Assurance Guidance for Airborne Electronic Hardware"

[7] Y. Papadopoulos and J.A.McDermid, "The Potential for a generic approach to certification of safety critical systems in the transportation sector", Reliability Engineering and Systems Safety 63, 1999, pp. 47~66

[8] J. Murdoch, J.A. McDermid, P.Wilkinson, International System Safety Conference, 2001. "Failure Modes and Effects Analysis (FMEA) and Systematic Design"