Research Paper

Journal of Aerospace System Engineering
Vol.14, No.특별호, pp.31-38 (2020)

EISSN 2508-7150
http://dx.doi.org/10.20910/JASE.2020.14.S.31

고장 데이터의 확률 분석을 적용한 항공기 시스템 안전성 평가 수행 방안 연구

유승우[1,†] · 김인걸[2]

[1]한국항공우주연구원 발사체보증팀
[2]충남대학교 항공우주공학과

A Study on the Implementation of Aircraft System Safety Assessment using Probabilistic Analysis of Failure Data

Seung-woo Yoo[1,†] and In-Gul Kim[2]

[1]Launcher Assurance Team, Korea Aerospace Research Institute
[2]Department of Aerospace Engineering, Chungnam National University

Abstract

The aircraft system safety assessment, which is emphasized in the development and certification of aircraft, is a systematic and comprehensive evaluation process to determine that all relevant failure conditions have been identified and that all significant combinations of failures cannot result in unacceptable hazards. As the aircraft systems become more complex and require integrated function and performance, proper safety objectives must be established and appropriate assessments are need to be accompanied. This paper has prepared to propose the efficient probabilistic analysis of failure data to evaluate the risk level over the entire aircraft lifecycle through the safety assessment and to review the considerations for aircraft certification and safety improvement.

초 록

항공기의 개발 및 인증 과정에서 중요성이 강조되고 있는 시스템 안전성 평가는 고장 또는 결함으로 인해 발생할 수 있는 위험을 사전에 식별하고, 이에 대한 영향성을 판단하여 요구되는 수준의 안전성을 확보하기 위해 적용하는 시스템 엔지니어링 기법이다. 항공기 시스템이 복잡해지고, 통합적인 기능 및 성능이 요구되면서 항공기 개발 초기부터 적절한 안전성 목표를 수립하고, 체계적인 평가를 통해 이에 대한 검증 및 후속 조치를 이행하여야 한다. 본 논문에서는 고장 데이터의 확률 분석을 수행하는 방안을 제시하여 항공기의 전체 수명주기에 걸쳐 리스크를 진단하고 효율적인 안전성 평가를 수행하기 위한 방법론을 제시하였고, 항공기 인증 및 안전성 확보를 위해 고려해야 할 사항을 제시하였다.

Key Words : System Safety Assessment(시스템 안전성 평가), Probabilistic Analysis(확률 분석), Hazard Analysis(위험 분석), Compliance(적합성), Development Assurance Level(개발보증수준)

1. 서 론

복합적인 기능을 하는 다양한 구성품이 통합된 시스템으로 구성되는 항공기는 개발 및 인증 단계에서 안전성(safety)을 확인하는 것은 물론 항공기를 운용하는 전체 수명주기에 걸쳐 안전한 상태가 유지되어야 한다. 여기서 안전한 상태는 위험 요인(hazard)을 완전히 제거하였거나, 발생 가능성이 있더라도 이에 대한 제어 및 억제를 통해 예상되는 피해나 영향을 수용할 수 있는 상태를 의미한다. 항공기 개발 과정에서부터 안전성을 확인하기 위한 시스템 안전성 평가 프로세스를 적용하며, 시스템의 고장(failure), 결함(defect) 및

Received: Mar. 08, 2020 Revised: Mar. 18, 2020 Accepted: Mar. 24, 2020
† Corresponding Author
Tel: +82-42-860-2534, E-mail: swyoo@kari.re.kr

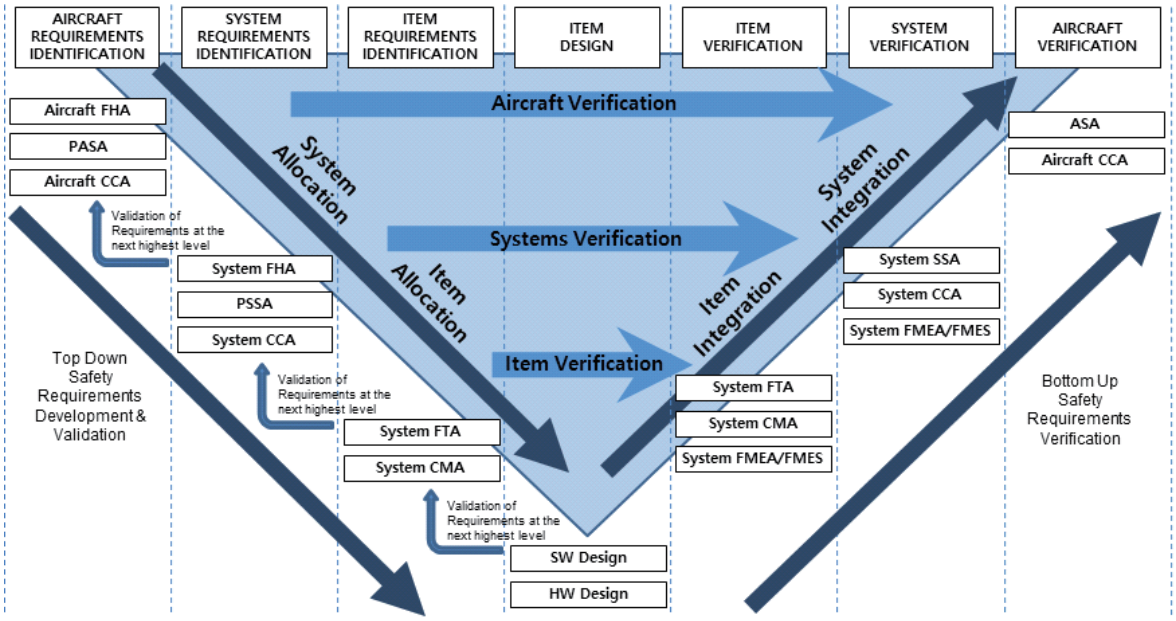

Fig. 1 Interaction between Safety and Development Processes

기능장애(malfunction)로 인하여 나타날 수 있는 위험요인을 사전에 식별하고, 이들 사이의 상호 연관성 또는 발생 메커니즘을 규명하여 이를 제거하거나 허용 가능한 안전수준(acceptable level of safety) 이하로 낮추기 위한 활동을 지속적으로 이행해야 한다[1].

본 논문에서는 항공기의 개발 및 인증 과정에서 중요성이 강조되고 있는 안전성 평가 프로세스에 대하여 살펴보고, 정량적인 안전성 목표에 대한 검증과 리스크를 진단하기 위한 확률 분석 기법을 수행하는 방안 및 항공기 개발 및 운용단계에서 안전성 확보를 위해 고려해야 할 사항을 제시하고자 한다.

2. 항공기 안전성 평가 프로세스

항공기 안전성 평가 프로세스는 목적에 따라 다음과 같은 2가지 영역으로 구분할 수 있다. 첫째는 잠재적 위험 요인을 제거하여 고장이 발생하지 않도록 항공기를 설계하거나 운용한계를 설정하기 위한 활동이고, 둘째는 위험 요인을 완전히 제거하는 것이 불가능하여 잔존하는 리스크를 허용 수준 이하로 낮추기 위한 활동으로 고장 발생 확률을 감소시키거나 고장으로 인한 영향을 최소화하는 것이다. Fig. 1은 항공기 개발 단계에 따라 진행되는 안전성 평가 프로세스를 나타낸 것이다[2].

2.1 기능위험평가

기능위험평가(FHA: Functional Hazard Assessment)는 항공기 및 시스템 수준의 기능을 구분하고, 예상되는 고장상태(failure condition)를 식별하여 이로 인한 영향의 심각도(severity)를 평가하는 방식으로 고장 영향 등급을 평가하는 프로세스이다. 일반적으로 항공기 기능위험평가와 시스템 기능위험평가를 구분하여 항공기 개념설계 단계에서부터 진행한다. 항공기에 요구되는 기능을 확인하고 해당 기능의 고장상태를 구분하여 상호간의 영향성을 논리적으로 판단하여 고장 영향 등급을 평가하는 것이 항공기 수준의 기능위험평가이며, 항공기의 기능을 시스템으로 배분한 이후에는 시스템을 대상으로 반복하여 기능위험평가를 수행한다.

2.2 안전성 예비평가

안전성 예비평가(PSA : Preliminary Safety Assessment)는 항공기와 시스템의 안전성 요구조건을 확정하고, 구현된 설계를 통해 해당 고장 영향 등급에 해당하는 요구조건을 충족할 수 있는지 평가하는 프로세스이다. 대상 시스템의 설계수준, 복잡도 및 고장 영향 등급에 따라 평가 수준을 달리 적용하는데, 단순하거나 기능이 독립된 시스템은 기존 유사 장치의 데이터와 해석 및 시험 결과를 활용하여 판단하지만, 설계가 복잡한 경우에는 결함수목분석(FTA: Fault Tree Analysis),

종속다이어그램 분석(dependence diagram analysis), Markov 분석 등의 기법을 이용하여 시스템의 기능과 구조를 하위수준으로 분해하여 평가를 진행한다.

2.3 시스템 안전성 평가

시스템 안전성 평가(SSA: System Safety Assessment)는 구현된 시스템 설계를 통해 기능위험평가나 안전성 예비평가에서 설정한 안전성 요구조건을 충족하는지 검증 및 확인하기 위한 종합적인 평가 프로세스이다. 이 단계에서는 확률 분석 기법을 통해 확인된 정량적 결과와 FMEA(Failure Modes and Effects Analysis)나 FMES(Failure Modes and Effects Summary) 등을 통해 도출한 정성적 결과를 함께 고려하여 종합적으로 판단해야 한다. 귀납적인 분석 기법인 FMEA와 연역적인 분석 기법인 FTA는 상호 보완적으로 이용할 수 있는데, FMEA를 통해 도출한 고장 영향이 FTA의 사상(event)으로 반영되었는지 확인하는 방식으로 적용하는 것이다. 이 과정에서 고려해야 할 점은 시스템이 복잡해질수록 고장의 원인을 특정한 원인으로 규명하기 어렵고, 원인으로 추정된 사상을 제거하더라도 시스템의 고장 또는 사고가 발생할 수도 있으며, 고장 사건들이 서로 독립적이지 않을 수도 있다는 것이다. 하위 시스템에서 고장이 발생하지 않더라도 상위 시스템은 안전하지 않은 상황에 도달할 수 있다는 점도 고려해야 한다.

시스템 안전성 평가의 정량적 분석은 확률 분석 기법과 고장 및 기능 손실로 인한 영향의 심각도를 종합적으로 고려하는 것으로서, 정확한 분석을 위해서는 부품과 서브시스템의 고장데이터가 확보되어야 한다. 기존 항공기에 장착되어 운용된 이력이 있거나 유사한 설계 제품의 데이터가 있는 경우에는 이를 이용하기도 하지만, 새로운 설계 개념을 도입한 시스템의 경우에는 확률 분석을 통해 동일 형식 항공기가 운용되는 전체 수명주기에서의 고장 발생 확률을 추정하여 적용해야 한다.

3. 안전성 요구조건

단순한 기능을 수행하는 시스템은 고장으로 인한 영향을 평가하여 이를 제거하거나 고장 발생 가능성을 감소시키기 위한 조치를 이행하고, 시험 또는 해석을 통해 감항기준을 비롯한 관련 요구조건에 대한 적합성을 입증할 수 있다. 복합시스템이나 전기전자 및 소프트웨어 기반 항공전자시스템은 개발이 완료된 이후 요구조건에 대한 충족 여부를 확인하는 것은 비효율적이며, 불가능할 수도 있기 때문에, 항공기 개발 초기부터 종합적인 안전성 평가 계획을 수립하여 적용해야 한다. 이 과정에서 도출되는 요구조건의 효율성과 적절성은 항공기 개발 및 인증 과정에서 요구되는 적합성 입증 프로세스, 비용, 일정 등에 큰 영향을 주기 때문에 개발 초기부터 최적화된 요구조건을 수립하는 것은 매우 중요하다. 또한, 일부 요구조건은 인증당국의 적합성 판정(compliance finding)이 필요하므로 인증 계획, 기준 및 방법에 대하여 인증기관과 사전에 협의하는 것이 효율적이다[3].

3.1 고장 확률 기준

기능위험평가를 통해 고장상태를 식별하고, 고장으로 인하여 항공기 시스템, 승객 및 비행승무원이 받는 영향의 수준에 따라 구분한 고장 영향 등급에 따라 고장 확률 목표를 설정하는데, 수송급 항공기에 적용되는 기준은 Table 1에서와 같이 4단계로 구분한다[4]. 여기에 제시된 수치적 확률 기준은 절대적인 요구조건이 아니라, 항공기 전체 수명주기에 걸쳐 확보되어야 하는 최소한의 확률 수준을 의미하는 것으로, 항공기 개발자는 가능한 많은 고장 데이터를 수집하고 통계적인 확률 분석 기법을 적용하여 정확한 리스크를 진단해야 하며, 여러 가지 불확실성을 감안하여 보수적인 방향으로 접근해야 한다.

(1) 극히 불가능(extremely improbable) : 동일한 형식의 항공기 기단(fleet)의 전체 운용주기 동안 발생 가능성이 거의 없는 수준으로, 수송급 항공기 기준 비행시간당 1×10^{-9}의 확률을 적용한다. 이는 개별 항공기가 연간 3,000시간 운용된다고 가정하였을 때, 동일 형식 항공기 100대 운용시 3,000년에 1회의 사고가 발생할 확률에 해당한다.

(2) 극히 희박(extremely remote) : 항공기 기단 전체 운용주기 동안 발생 가능성이 존재하는 수준으로, 수송급 항공기 기준 비행시간당 1×10^{-7}을 확률을 적용한다. 이는 개별 항공기를 연 3,000시간 운용시

Table 1 Failure Conditions related to Probability Objectives and Development Assurance Level (Transport)

Failure Conditions	Minor	Major	Hazardous	Catastrophic
Effect on Airplane	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	Physical discomfort for passengers	Physical distress to passengers, possibly including injuries	Serious or fatal injury to an occupant	Multiple fatalities
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
Probability Objectives	Probable ($< 10^{-3}$)	Remote ($< 10^{-5}$)	Extremely Remote ($< 10^{-7}$)	Extremely Improbable ($< 10^{-9}$)
SW & CEH DALs	D	C	B	A

100대의 기단이 30년간 운용될 경우 1회의 사고가 발생할 확률이다.

(3) 희박(remote) : 항공기 기단 전체 운용주기 동안 개별 항공기에서 수차례 발생할 수 있는 수준의 고장 확률로서, 수송급 항공기의 경우 비행시간당 1×10^{-5} 미만이어야 한다. 일반적인 항공기 설계 수명의 약 2배에 해당하는 10만 비행시간 운용시 1건의 고장이 발생하는 수준이다.

(4) 가능(probable) : 발생 확률이 비행시간당 1×10^{-5} 미만이며, 고장이 발생하더라도 안전 여유의 경미한 감소, 승무원 업무량의 증가, 조종사가 불편함을 느끼는 수준의 Minor 등급 고장인 경우에만 이를 허용할 수 있다.

3.2 개발보증수준

항공전자시스템에 소프트웨어 기반 기술과 복잡 전자하드웨어(CEH: Complex Electronic Hardware) 기술이 사용되면서, 복잡성으로 인해 식별 또는 제거하지 못하는 결함이나 다른 시스템과의 통합 과정에서 확인되지 않은 오류에 의한 고장 발생 가능성은 증가하게 되었다. 복합시스템은 해석 또는 시험을 통한 결정론적 방법(deterministic method)을 적용해서 기준에 대한 적합성을 입증하거나, 확률론적 리스크 분석을 통해 안전성을 확인할 수 없었기 때문에 새로운 기법과 절차의 필요성이 대두되었다. 이에 따라 미국과 유럽의 인증당국은 SAE(Society of Automotive Engineers), RTCA(Radio Technical Commission for Aeronautics), EUROCAE(European Organisation for Civil Aviation Equipment) 등의 기관에 의뢰하여 인증 신청자와 인증기관이 적합성 입증방법(MoC: Means of Compliance)으로 적용할 수 있는 방법론을 개발하였으며, 소프트웨어나 CEH의 중요도에 따라 개발보증수준(DAL: Development Assurance Level) 개념을 채택하였다. 이것은 대부분의 항공기 개발과정에서 표준 프로세스로 받아들여지고 있으며, 군수, 자동차, 우주, 철도, 원자력 등의 분야에서도 통용되고 있다. 항공기 개발과정에서 요구되는 시스템 안전성 평가 프로세스, 복합 전자하드웨어 및 소프트웨어의 개발보증을 위한 기준 및 라이프 사이클 지침, 그리고 항공기 운용과정에서 감항성 유지와 안전성 관리를 위한 지침서로 활용되고 있는 문서와 상호 연관성은

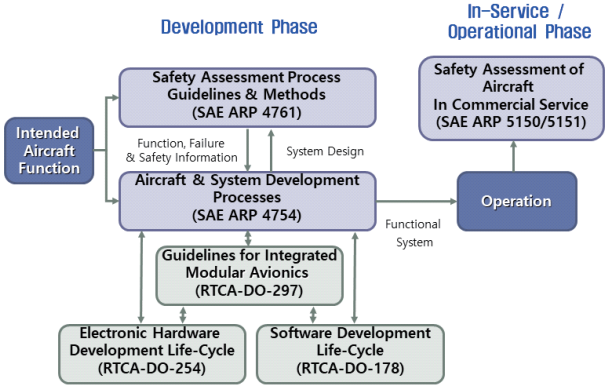

Fig. 2 Guidance Documents covering Development, In-service and Operational Phases

Fig. 2와 같다.

3.3 파생 요구조건

항공기 개발 과정에서는 시스템 설계에 대한 검증 및 확인 결과에 따라 후속 과정에서 다른 요구조건이 새롭게 생성되기도 한다. 이와 같은 파생 요구조건(derived requirements)은 상위 수준에서 할당되는 것이 아니라 개발 프로세스가 진행되면서 도출되므로 설계 초기부터 고려하기에는 어려움이 있다. 다음은 파생 요구조건이 도출되는 사례로서, 요구조건이 도출되는 시점부터 추적 관리가 이루어져야 한다.

(1) Catastrophic 등급에 해당하는 고장은 단일 고장 원인에 의해 발생하지 않도록 설계되어야 한다. 이를 위하여 수송급 항공기의 경우 Catastrophic 등급 시스템은 4중화, Hazardous 등급은 3중화 설계를 적용하는 것이 일반적이다.

(2) 시스템 설계를 다중화하는 경우에는 공통원인에 의한 고장을 방지하기 위하여, 서로 다른 서브시스템을 적용하여야 한다. 이는 화재, 유체 오염, 낙뢰, EMC(Electromagnetic Compatibility), HIRF(High Intensity Radiated Fields) 등의 특정 위험환경에 노출될 경우 백업시스템이 함께 영향을 받을 수 있기 때문이다.

(3) 특정한 안전 기능을 위한 장비에 대해서는 독립된 전력원에서 전원을 공급해야 하며, 이와 같은 전원 공급장치의 개발보증수준은 전원을 받는 시스템과 동등한 수준 이상이어야 한다.

(4) 설계 단계에서 확정된 시스템 구조에 따라 서로 다른 파생 요구조건이 도출되기도 한다. 예를 들어, 상위 시스템을 3중화 구조로 설계하는 경우에는 2중화 설계의 경우와 비교하여 개별 서브시스템에 요구되는 개발보증수준은 낮출 수도 있으며, 이에 따라 다른 파생 요구조건이 도출된다는 것이다. 이와 반대로, 채택하는 하위 구성품의 개발보증수준에 따라 상위 시스템의 구조를 변경할 수도 있다.

(5) 장비 장착 위치 선정시에는 고속 회전부품의 방출, 동체착륙, 고압 부품의 파열, 타이어 파열 등의 위험을 고려하여야 하고, 가연성 유체 또는 산소시스템에 의한 발화, 상호 접촉으로 인한 손상 등을 방지할 수 있도록 관련 배관 및 배선의 장착성을 검증하여야 한다. 이 경우에는 구역 안전성 분석(ZSA; Zonal Safety Analysis)이나 외부 위험에 대한 특정 리스크 분석(PSA: Particular Risk Analysis)을 추가 적용하게 된다.

(6) 위험 노출 시간(exposure time) 또는 정비주기 제한을 줄이기 위하여 자체점검(built-in test) 기능을 탑재한 경우에는 장비의 운용이 시작될 때마다 자체점검을 통해 고장상태를 파악할 수 있는지 검증하여야 한다.

4. 안전성 평가를 통한 조치사항

시스템 안전성 평가 결과에 따라 다음과 같은 설계 변경이나 후속조치를 적용할 수도 있으며, 대상 시스템의 고장으로 인한 영향, 발생확률 및 고장 영향 등급을 종합적으로 고려해야 한다.

4.1 안전장치 설치

완전히 제거할 수 없는 위험요소에 대해서는 잔존하는 리스크를 허용 가능한 수준 이하로 낮추거나, 고장에 노출될 가능성을 감소시키기 위하여 추가적인 안전장치를 설치하는 방법을 적용하기도 한다. 하지만 추가 장착된 안전장치로 인해 시스템의 고장 발생 확률은 증가할 수도 있으므로, 반드시 신뢰성이 확인된 장치를 선택하여야 한다.

4.2 경보장치 설치

리스크를 최소화하는 설계를 적용할 수 없는 경우에는 항공기의 상태를 감지하여 위험 발생 조건에 대하여 적절한 경보를 발생할 수 있는 경보장치를 설치하여 조종사의 추가적인 조치를 통해 안전성을 확보할 수도 있다. 이 경우 경보장치는 인적요소를 충분히 고려하여 설계에 반영하고, 운용과정에서 오작동과 부적절한 반응이 발생하지 않도록 설계하여야 한다.

4.3 절차 및 훈련과정 개발

설계 변경을 통해 위험 경감이 불가능한 경우에 비상절차를 마련하고, 이를 비행 매뉴얼에 포함시켜서 절차에 따라 조치를 이행하도록 할 수도 있다. 하지만 이 방법은 고장에 대한 근본 원인에 대한 조치가 아니

므로, Catastrophic 또는 Hazardous 고장 영향 등급에 대해서는 이 보완 조치만으로 안전성을 확보할 수는 없다. 또한, 조종사가 이 절차를 숙지하고 대응할 수 있도록 반복적으로 훈련하는 프로세스도 별도로 확인되어야 한다.

4.4 검사 및 정비주기 설정

운용수명의 제한이 있거나 노화로 인한 고장 발생 가능성이 있는 항공기 구조부재, 탑재장비 및 시스템은 교체, 점검 및 정비주기를 설정하여 관리하며, 항공기 운용과정에서 안전성을 유지 관리하기 위하여 지속적인 운용 안전성(operational safety) 평가도 이루어져야 한다. 이를 위해서 항공기 운용과정에서 발생하는 모든 고장, 기능불량, 결함 및 운용장애(Service Difficulties) 정보는 수집되어야 하며, 개별 항공기 뿐만 아니라 동일 형식의 항공기 기단의 비행시간에 따른 확률 분석을 통해 Fig. 3과 같이 나타내고, 리스크에 따라 필요한 조치사항을 결정하는 방식으로 항공기의 지속감항성을 관리해야 한다. 고위험(high risk) 수준에서는 비행을 중단하고 즉각 조치를 이행해야 하고, 과도한 위험(excessive risk) 수준의 경우에는 비행은 가능하지만 설정한 시점이 도래하기 전에 필요한 조치를 이행해야 한다.

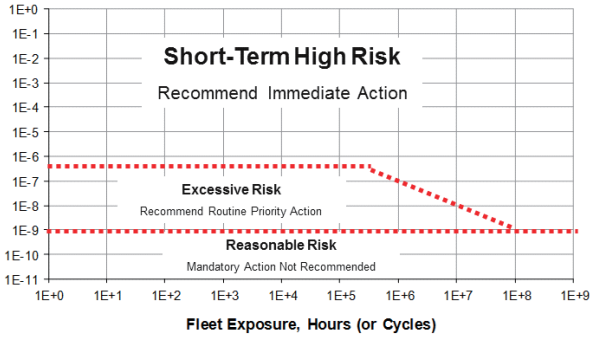

Fig. 3 Fleet Risk Analysis Visualization Chart

5. 확률 분석 기법

5.1 발생 확률 산출

시스템 안전성 평가에서 사용하는 사건 또는 고장의 발생 확률(probability of occurrence)은 발생횟수, 전체 항공기 운항시간, 장비 운용시간, 비행횟수, 동작횟수 등의 데이터를 이용하여 계산한다. 작동 신호에 대하여 단발적으로 응답하는 요구 기반형(demand based) 장비의 고장 확률은 고장횟수를 전체 작동횟수로 나누어 계산하고, 특정 비행시간 동안 운용하는 시간 기반형(time based) 장비의 고장 확률은 비행시간당 발생횟수를 이용하여 간단하게 산출할 수 있다. 이와 같이 계산한 고장 확률은 항공기의 기령, 운용환경, 비행 프로파일 등 실제 운용환경을 고려하지 않은 점추정치(point estimator)로서, 물리적, 모델링, 통계적 원인에 의한 불확실성이 내재되어 있다.

보다 정확한 고장 확률을 산출하기 위해서는 평균적인 비행 프로파일의 단계를 구분하여 비행시간의 비율을 산정하고, 단계별로 비행시간당 발생 확률을 산출해야 한다. 또한, 항공기 또는 장비품의 초기고장(infancy failure), 우발고장(random failure), 열화고장(wear-out failure) 등이 모두 고려되어야 하므로, 확률밀도함수(probability density function)를 적분하여 누적분포함수 형태로 도출하기도 한다.

5.2 발생 확률의 구간추정

시스템 안전성 평가 결과를 이용하여 후속 프로세스를 이행하는 과정에서는 보수적인 접근을 위해 다음과 같은 방법을 적용하기도 한다. 분석된 고장의 심각도를 상위 등급으로 변경하여 적용하거나, 고장 확률을 산출하는 과정에서 민감도 해석(sensitivity analysis)을 통해 불확실성이 있는 여러 매개변수 중에서 주요한 인자를 선별하고, 이를 이용하여 통계적인 상세 분석을 수행하기도 한다.

또한, 발생 확률에 대한 점추정 대신 구간추정을 통해 구한 신뢰구간의 상한을 채택하여 불확실성을 포함하는 보수적인 발생 확률을 적용할 수도 있다.

$$Probability \leq \chi^2_{\alpha,2(r+1)} / 2T \qquad (1)$$

Eq. 1은 사건 발생횟수가 서로 독립인 정상 포아송 과정에서 고장 확률을 산출하기 위한 수식으로, 자유도 $2(r+1)$인 Chi-square 분포의 $100(1-\alpha)\%$ 백분위수에 대한 단측 신뢰상한을 의미한다. T는 비행시간 또는 비행횟수, α는 유의수준(significance level), r은 관측된 고장횟수이다.

10만 시간의 운용시간 동안 고장이 발생하지 않은

Table 2 Comparison of Probability between Point Estimation and Interval Estimation

	zero failure	4 failures
Point Estimation	$P_f = 0/100{,}000 = 0.0$	$P_f \le \chi^2_{0.1,2(0+1)}/2T \le 2.3\times10^{-5}$
Interval Estimation	$P_f = 4/100{,}000 = 4.0\times10^{-5}$	$P_f \le \chi^2_{0.1,2(4+1)}/2T \le 7.99\times10^{-5}$

* Confidence level = 90% ($\alpha = 0.1$)

경우와 4회의 고장이 발생한 경우, 발생 확률에 대한 점추정 및 구간추정 결과를 비교하면 Table 2와 같다. 구간추정의 상한치는 발생 확률의 점추정치에 비해 크게 추정되며, 고장이 관측되지 않은 무고장의 경우에도 구간추정을 통해 발생 확률을 산출할 수 있으므로 보수적인 확률 분석을 적용할 수 있다.

고장 확률에 대한 구간추정 상한과 점추정치의 비율을 신뢰지수(confidence factor)라고 하며, 실제 관측된 고장 횟수에 신뢰지수를 곱한 값을 고장 확률로 적용할 수도 있다. 또한, Table 3과 같이 적용하는 신뢰수준에 따라 신뢰지수는 달라지며, 우주발사체의 경우에는 안전 필수장비, 중요도 또는 고장등급이 높은 시스템에 대한 확률 분석에서는 높은 신뢰수준을 적용하기도 한다[8].

Table 3 Confidence Factors to Adjust Observed Probability

	Confidence Level				
Failure	50%	60%	90%	95%	99%
1	1.678	2.022	3.890	4.744	6.638
2	1.337	1.553	2.661	3.148	4.203
3	1.224	1.392	2.227	2.585	3.348
4	1.168	1.309	1.998	2.288	2.901
5	1.134	1.258	1.855	2.103	2.622
6	1.112	1.224	1.755	1.974	2.428
7	1.096	1.199	1.682	1.878	2.286
8	1.084	1.179	1.624	1.804	2.175
9	1.074	1.164	1.578	1.745	2.087
10	1.067	1.152	1.541	1.696	2.014

5.3 수명 데이터의 반영

고장 확률을 산출하는 과정에서 개별 부품이나 구성품의 고장률이 일정한 우발고장 구간의 고장률을 이용하는 경우가 많은데, 전기전자부품을 제외한 대부분의 구성품이나 부품에 대한 고장확률분포는 지수분포로 나타나지 않는다. 금속 및 복합재료의 강도, 기계부품의 수명분포는 와이블 분포(Weibull distribution)를 사용하는 것이 적합하며, 고장 확률은 다음과 같이 나타낸다.

$$F(t) = 1 - e^{-(t/\eta)^{\beta}} \tag{2}$$

여기서 η는 와이블 특성수명(characteristic life), β는 형상모수(shape parameter)를 의미하며, 와이블 분포를 이용한 운용 수명은 다음과 같다.

$$t = \eta[-\ln(1-F(t))]^{1/\beta} \tag{3}$$

이와 같은 방법으로 부품의 수명한계를 산출할 수 있으며, 노화로 인한 고장모드를 배제하기 위하여 검사 또는 교체 주기를 설정하게 되면 해당 내용은 정비 매뉴얼에 반영해야 한다.

5.4 베이지안 기법 적용

항공기 설계 과정에서는 운용 데이터가 부족하고, 모든 고장 정보를 확보할 수 없기 때문에, 실제 제품이 아닌 유사 부품의 고장 정보 또는 다른 항공기에 사용되는 구성품의 데이터를 활용하기도 한다. 개발과정에서 수행된 시험이나 분석을 통해 고장 데이터가 추가되고, 항공기 운용 과정에서 지속적으로 고장 데이터가 확보되면 이를 활용하여 고장 확률을 다시 산출하고, 안전성 평가를 업데이트하는 방식을 적용한다면 보다 정확한 데이터에 기반한 안전성 관리가 가능하다. 이를 위해 제한된 데이터 외에 사전 지식이나 정보를 활용하는 베이지안 추론(Bayesian Estimation)을 적용하면, 추가된 정보를 활용하여 고장 확률 분석 결과를 통계적으로 업데이트할 수 있다.

$$\pi_1(\theta|x) = \pi(\theta)\frac{f(x|\theta)}{\int f(x|\theta)\,\pi(\theta)\,d\theta} \tag{4}$$

여기서 $\pi_1(\theta|x)$는 사후분포(posterior distribution),

$\pi(\theta)$는 사전분포(prior distribution), $f(x|\theta)$는 우도(likelihood) 함수를 의미한다.

베이지안 기법은 실제 관측된 객관적 데이터와 관련 지식이나 사전 정보를 함께 활용할 수 있다는 장점이 있지만, 처리해야 하는 데이터의 양이 많아지고 계산이 복잡해진다. 따라서 고장 확률에 영향을 많이 주는 확률변수를 선별하고, 계산 과정에서 적절한 가정을 적용하여 단순화하며 유효성을 검증 및 보정하기 위한 마르코프 연쇄 몬테카를로(MCMC)와 Gibbs 표본 추출 기법을 함께 적용하기도 한다[9].

6. 결 론

본 논문에서는 항공기의 개발 및 인증을 위해 통용되는 안전성 평가 프로세스, 여러 가지 요구조건에 대한 적합성 입증 방법, 안전성 평가 후속 조치사항을 살펴보았다. 이 모든 단계에서 확률 분석을 통해 대상 시스템의 안전 수준을 진단하고, 적절한 리스크 관리 절차가 진행되어야 한다. 시스템 안전성 평가는 항공기 인증과 요구조건에 대해 적합성 입증을 위한 수단으로만 적용할 것이 아니라, 항공기 개발자의 정책과 전략이 반영된 종합적인 안전성 관리 프로세스로 활용되어야 한다. 이를 위해 항공기 개발자는 설계 초기 단계에서부터 안전성 목표를 수립하고 이를 안전성 요구조건으로 설정하여야 하며, 형식증명 단계에서는 물론 항공기 운용단계까지 안전성에 대한 검증 및 개선 활동을 지속적으로 수행해야 한다.

궁극적인 항공기 안전성 관리의 목표는 항공기의 모든 수명주기에 걸쳐 확보된 안전성에 기반하여 감항성이 유지되도록 관리하여 사고를 예방하는 것이므로, 항공기 인증 과정에서 안전성 평가를 통해 확인된 안전성이 항공기의 전체 수명주기 동안 유지될 수 있도록 위험 요인을 모니터링하고, 지속적으로 개선하는 관리 프로세스가 이어져야 한다. 이를 위해 항공기 개발단계에서 시험과 분석을 통해 확인된 고장 데이터와 항공기 운용과정에서 지속적으로 수집하는 고장, 결함 및 오작동의 발생에 관한 데이터는 통계적인 기법을 이용해서 분석하여야 한다. 또한, 항공기 운용과정에서 적절한 검사, 정비 및 수리 작업을 실시하는 것 이외에도 항공 제품의 설계 결함, 제작 및 검사과정에서의 문제점, 항공기 수리 및 정비 상의 문제점, 안전관리 체계에 대한 개선점 등을 파악하고, 이를 개선하기 위한 활동으로 이어져야 한다.

References

[1] Society of Automotive Engineers, Inc., *"ARP 4761: Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment"*, Warrendale, U.S.A., Dec. 1996.

[2] Society of Automotive Engineers, Inc., *"ARP 4754A: Guidelines for Development of Civil Aircraft and Systems"*, Warrendale, U.S.A., Dec. 2010.

[3] S. W. Yoo, J. P. Jung, and B. J. Yi, "A Study on the Safety Requirements Establishment through System Safety Processes", *Journal of Aerospace System Engineering*, vol. 7, no. 2, pp. 14-19, Jun. 2013.

[4] S. W. Yoo and J. H. Lee, "A Study on Promoting the Efficiency of Aircraft System Safety Assessment", *Journal of Aerospace System Engineering*, vol. 6, no. 3, pp. 7-12, Dec. 2012.

[5] Society of Automotive Engineers, Inc., *"ARP 5150, Safety Assessment of Transport Airplanes in Commercial Service"*, Warrendale, U.S.A., Nov. 2003.

[6] Federal Aviation Administration, *"AC 23.1309-1E: System Safety Analysis and Assessment for Part 23 Airplanes"*, Washingtion D.C., U.S.A., Nov. 2011.

[7] Federal Aviation Administration, *"Flight Safety Analysis Handbook"*, Version 1.0, Washingtion D.C., U.S.A., Sept. 2011.

[8] Federal Aviation Administration, *"Guide to Reusable Launch and Reentry Vehicle Reliability Analysis"*, Version 1.0, Washingtion D.C., U.S.A., Apr. 2005.

[9] National Aeronautics and Space Administration, *"NASA/SP-2009-569: Bayesian Inference for NASA Probabilistic Risk and Reliability Analysis"*, Washingtion D.C., U.S.A., Jun. 2009.