신뢰성응용연구
제7권, 제2호. pp.89-100, 2007

항공기 시스템의 안전성 평가에 관한 연구

이경철 · 이종희 · 이백준 · 유승우

한국항공우주연구원

A Study on the System Safety Assessment of Aircraft

Kyung-chol Lee · Jong-hee Lee · Baeck-Jun Yi · Seung-Woo Yoo

Korea Aerospace Research Institute*

Abstract

For the certification of aircraft and part, it must be show the compliance with applicable requirements through system safety assessment. The safety assessment process should be planned and managed to provide the necessary assurance that all relevant failure conditions have been identified and that all significant combinations of failures which could cause those failure conditions have been considered. Complex systems, especially aircraft, should take into account any additional complexities and interdependencies which arise due to integration. In all cases involving integrated systems, the safety assessment process is of fundamental importance in establishing appropriate safety objectives for the system and determining that the implementation satisfies these objectives.

This study review the safety assessment for the certification process of the aircraft engine system and analyze turbo-fan engine by fault analysis method for compliance with airworthiness requirement of aircraft engine system.

1. 서 론

항공기는 3차원 공간을 운행하는 비행체로서 고속 운송수단으로 사용되므로, 사고가 발생하게 되면 수많은 인명피해와 재산손실을 초래하게 된다. 이에 따라 항공기 또는 관련 부품의 개발 및 운용과정에서는 높은 수준의 신뢰성 및 안전성이 요구되고 있다.

항공기의 안전성(safety)이라 함은 항공기의 작동에 중요한 역할을 하는 각 시스템이 위험에 이르지 않는 상태 또는 정도를 의미하며 항공기 시스템에 대한 안전성 평가는 설계(design), 생산(production), 그리고 인증(certification)이 통합된 것으로서 과거의 운용 경험을 바탕으로 항공기 안전성 평가 요건은 세분화 된다.

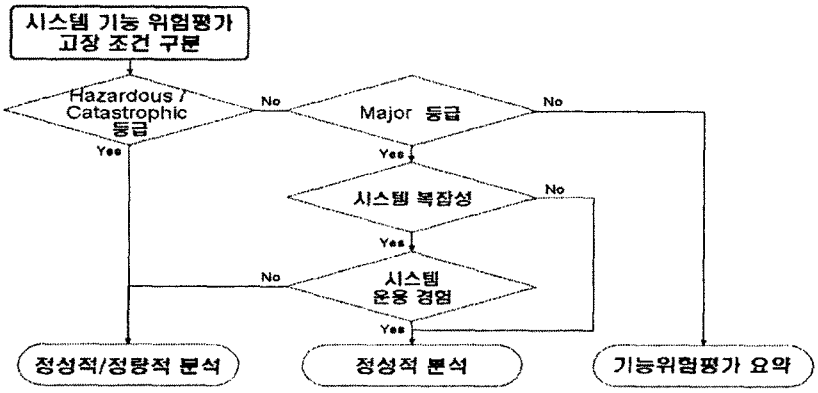
민간 항공기 및 부품에 대한 안전성 평가와 입증에 대한 법적 요구조건은 다음과 같은 목표 설정에 대한 활동으로부터 시작된다. 첫째는 발생할 수 있는 위험요소 자체를 제거하는 것이고, 둘째는 제거가 불가능한 위험요소의 경우 잔존하는 위험수준을 허용수준 이하로 낮추는 것이다. 이 두 가지 모두 시스템의 안전성을 확보하기 위하여 여러 가지 공학적 기법 또는 기술을 응용하게 되며 그 중 하나가 안전성 평가(safety assessment)이다. 항공기 시스템 안전성 평가에서는 고장이나 재해의 발생확률에 대한 평가 방법을 이용하여 종합적이고 균형적인 안전성을 확보하기 위한 분석을 전 수명 주기에 대하여 실시하여야 하고 필요시 적절한 조치를 취하여야 한다.

본 논문에서는 항공 선진국의 항공기 및 엔진 제작회사에서 개발한 각 시스템에 대하여 감항당국의 감항기술기준에 상응하는 최소한의 안전성 요구조건에 적합함을 입증하기 위하여 수행하고 있는 안전성 평가방법의 사례에 대하여 살펴보고 안전성 평가 수행 방안을 고찰하고자 한다.

2. 본 론

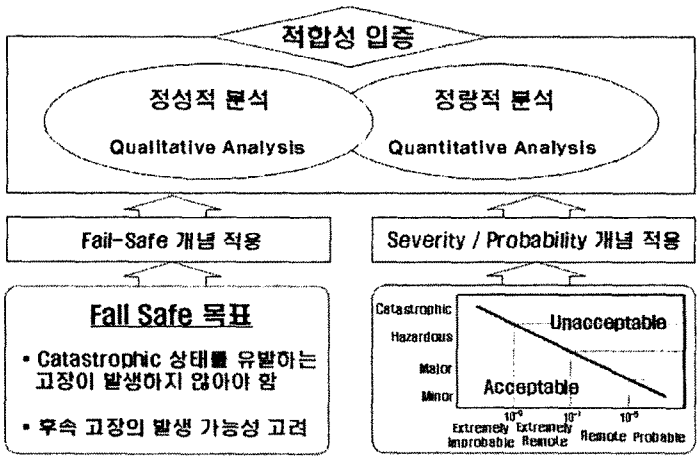
2.1 안전성 평가 세부기법

직접적인 방법으로 설계가 가능할 정도로 간단한 시스템의 경우에는 몇 가지 기본적인 안전성 평가 기법을 적용하는 것만으로도 안전성을 입증할 수 있지만, 복잡한 시스템의 경우에는 개별 구성품의 고장 확률을 적용하여 전체 시스템에 대한 고장 및 안전성 분석을 수행할 필요가 있다. 특히 항공기 인증을 위해서 적용되는 안전성 평가 및 분석 수준을 설정하기 위해서는 개별 고장 조건에 대하여 항공기 및 시스템을 안전성 목표에 부합시키기 위한 방안이 사전에 결정되어야 한다. 다음의 <그림 1>에 제시된 업무 흐름도는 대상 시스템의 고장 조건에 따라 이를 분석 및 입증하기 위한 지침을 제공한다. 안전성 분석 수준 결정이 가장 까다로운 등급은 major 등급으로서, 시스템의 복잡성 및 시스템 운용경험 등을 검토하여 분석 방법을 결정하게 된다.



<그림 1> 안전성 분석기법 결정 프로세스

이와 같이 대상 시스템의 복잡도, 시스템의 운용경험 및 고장 조건 등에 따라 안전성 평가를 위한 분석방법은 정성적 분석과 정량적 분석으로 구분하는데, 이는 서로 완전히 독립된 방법으로 취급할 수는 없으며 중첩되는 영역이 존재한다. 이러한 사항은 다음 <그림 2>와 같이 나타낼 수 있으며, 두 가지 분석 방법은 상호 보완적인 관계로 적용하여야 한다.



<그림 2> 정성적 분석과 정량적 분석 비교

2.2 정성적 분석

정성적 분석은 고장, 잠재 고장 및 기능 손상과 이로 인한 영향을 다루고 fail-safe 설계 개념이 도입된다. 여기서 fail-safe 설계는 치명적인 상태를 유발하는 단일 고장의 발생을 방지할 수 있는 설계로 정의하며, 고장 발생으로 인하여 안전한 비행 및 착륙을 방해하거나 항공기의 성능 또는 승무원의 능력 저하를 유발하는 단일 고장이 발생하지 않도록 모든 시스템 및 부품을 설계하여야 한다는 것이다. 항공기 안전성 평가에 적용할 수 있는 정성적 분석법의 종류는 다음과 같다.

- 설계 평가/검토 (design appraisal/review)
- 장착성 평가 (installation appraisal)
- 고장모드 및 영향분석 (failure modes and effects analysis)
- 위험 지수법 (hazard indices)
- 리스크 평가 코드법 (risk assessment codes)
- 예비 위험 분석 (preliminary hazard analysis)
- 결함 위험 분석 (fault hazard analysis)
- 시스템 리스크 분석 (system hazard analysis)
- 운용 위험 분석 (operating hazard analysis)
- 중복고장 행렬법 (double failure matrix method)
- 관리감독 및 리스크 트리 분석 (management oversight and risk tree)
- 미주회로 분석 (sneak analysis)
- What if 분석 ("what-if" analysis)
- 위험 및 운용성 연구 (hazard and operability study)
- 시나리오 분석법 (scenario analysis)

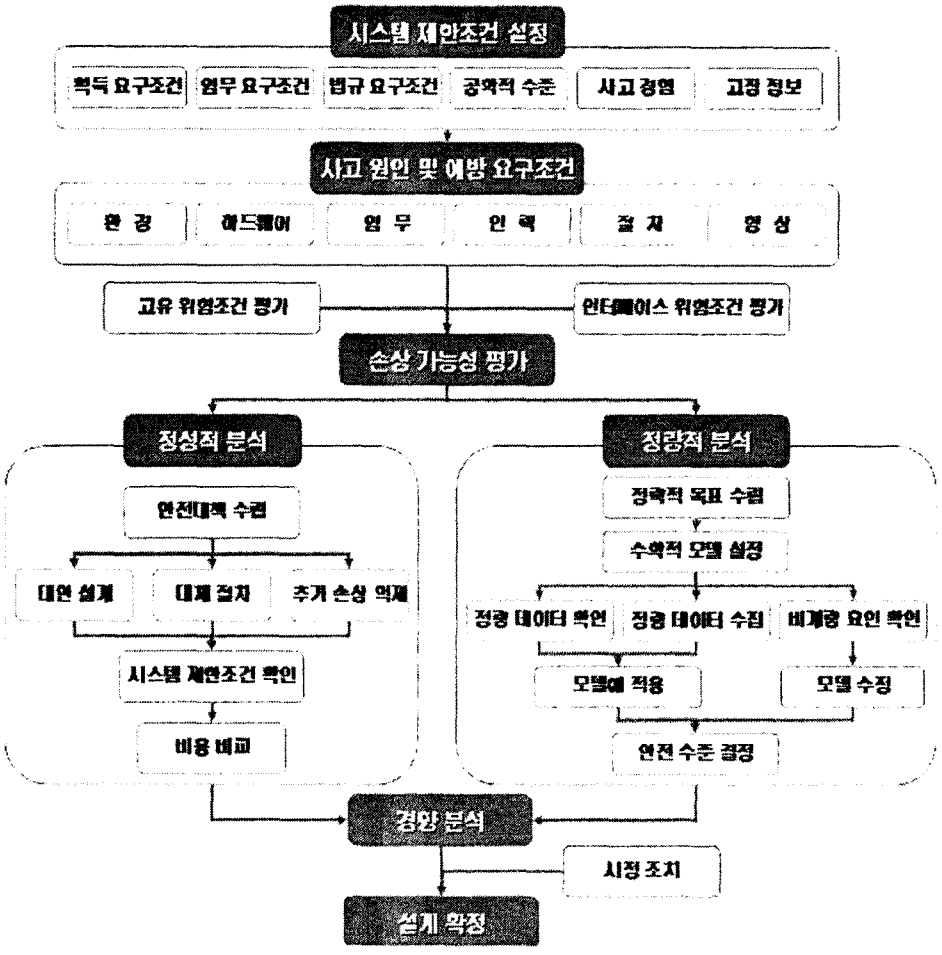
2.3 정량적 분석

정량적 분석은 고장 및 기능 손실로 인한 영향의 심각도와 발생 가능성을 척도로 시스템의 안전성을 분석하는 것으로서, 정확한 분석을 위해서는 부품 및 서브시스템의 고장 확률 정보가 필요하다. 이러한 고장 확률 정보는 보통 기존 항공기에 장착되어 사용된 경험 또는 유사한 설계의 부품에 대한 정보를 바탕으로 확보하지만, 새로운 설계에 의해 개발된 경우에는 이러한 방법이 불가능하므로 고장 확률에 대한 분석 및 예측을 통해 계산하여 적용한다. 이와 같은 부품 및 서브시스템의 고장 확률을 통합하여 항공기 또는 시스템에 대한 정량적 분석을 수행하게 되는데, 이 때 적용하는 정량적 분석 기법의 종류는 다음과 같다.

- 경로 추적법 (path tracing method)
- 치명도 분석 (criticality analysis)
- 신뢰성 블록다이어그램 분석(reliability block diagram analysis)
- 종속 다이어그램 (dependency diagram)
- 사상 트리 분석 (event tree analysis)
- 결함 트리 분석 (fault tree analysis)
- 인적 신뢰성 분석 (human reliability analysis)
- 공통 모드 고장 분석 (common mode failure analysis)

- 시뮬레이션 (simulation)
- 마르코브 분석 (markov analysis)

정량적 분석을 위해서는 부품 및 서브시스템에 대한 데이터 외에도 항공기 또는 시스템에 대한 정량적 안전성 목표 및 요구조건이 먼저 설정되어야 객관적인 평가가 가능한데, 이는 부품 또는 서브시스템의 고장이 항상 항공기, 승무원, 승객에게 치명적인 영향을 주는 것은 아니기 때문이다. 따라서 안전성 기준 또는 목표치는 항공기 수준에서 정의하여야 하고, 통상적으로 항공기 및 시스템의 안전성 분석을 통해 설계를 확정하는 프로세스는 <그림 3>과 같다.



<그림 3> 설계 프로세스에서 수행되는 안전성 분석

앞에서 언급한 바와 같이 항공기 안전성 평가 프로세스에서 결함트리분석, 종속 다이어그램, 마르코브 분석은 동등한 수준의 분석기법으로서 모두 하향식(top-down) 분석기법이다. 이러한 분석은 연속적으로 보다 상세한 설계 수준인 하향식으로 수행한다.

기능 위험 평가단계에서 고장조건을 설정한 이후, 결함트리분석, 종속 다이어그램, 마르코브

등을 실시하며, 이는 개별 고장을 유발할 수도 있는 하위 수준에서 단일 결함 또는 조합된 결함이 발생할 수 있는지를 판단하기 위하여 시스템 안전성 예비 평가의 일환으로 적용된다. 고장 모드 및 영향 분석(FMEA) 또는 고장 모드 및 영향 요약(FMES)이 수행되면 기본 사상과 같이 결함트리분석/종속 다이어그램/마르코브 분석에서 식별된 모든 중요한 영향을 보장할 수 있도록 비교가 수반되어야 한다.

결함트리분석은 고장 유형과 고장 영향의 관계를 나타내기 위하여 boolean 논리 게이트를 이용하며, 가장 일반적인 논리 게이트는 AND-게이트와 OR-게이트이다. AND-게이트는 상위 수준의 사상을 나타내는 출력을 산출하기 위해서 모든 입력의 공존 조건이 필요하다는 것을 나타낸다. OR-게이트는 상위 수준의 사상을 나타내는 하나의 출력을 산출하기 위하여 하나 또는 그 이상의 입력 조건을 나타낸다.

결함트리분석은 중대한 고장을 유발시키는 사건(top event)에 대해서 발생 원인을 하부 수준의 사건(lower event)에서 어떻게 시작되었는지를 추적해 가는 연역적인 분석 기법이다. 이러한 결함트리분석 방법은 1960년대 초에 미국 bell laboratory의 H.A.Watson이 고안하고, 1965년 Boeing 항공회사의 D.F.Haall에 의해 보완됨으로써 실용화되기 시작한 시스템 고장 해석방법으로 대륙간탄도미사일(ICBM)개발 계획의 안전성 분석에 처음으로 사용된 이후 기계 장치가 규칙적으로 작동되고 있는 가운데 어느 정도의 고장이 일어날 것인가를 규명하는데 사용되었으며, 최근에는 시스템의 안전성 및 신뢰성 분석에 널리 이용된다.

결함트리분석은 시스템 고장을 발생시키는 사상(event)과 그의 원인과의 인과관계를 논리기호(AND와 OR)를 사용하여 나뭇가지 모양의 그림으로 나타낸 결함트리를 만들고, 이에 따라 시스템의 고장확률을 구함으로써 문제가 되는 부분을 찾아내어 시스템의 신뢰성을 개선하는 정량적 고장해석 및 신뢰성 평가방법이다. 즉, 결함트리분석은 연역적(추론적) 방식의 분석기법으로 원하지 않는 사건의 발생을 유발하거나 그 발생에 기여하며, 시스템의 성능, 안전, 경제성이나 기타 지정된 특성에 큰 영향을 미치는 요인과 조건을 파악하고 분석한다.

보통 정상사상은 시스템의 고장, 오동작, 화재, 탈선 등과 같이 상당한 위험이나 많은 비용 또는 오랜 고장시간을 야기하는 고장요인으로서 정상사상 아래 OR 게이트나 AND 게이트를 통해서 다음에 원인이 되는 사상들과의 인과관계를 나열하게 된다. 이렇게 표시된 각 고장원인의 발생 확률로부터 시스템의 고장확률을 구함으로써 시스템의 고장을 발생시키는 영향이 가장 큰 원인을 찾아내고, 이에 대한 시정조치를 수행함으로써 신뢰성 및 안전성을 개선시키고자 하는 고장해석 및 안전성 평가를 실시하게 된다. 다시 말해서 상위의 사상에 대한 원인이 되는 하부수준의 사건들이 각각 어느 정도의 확률로 발생하는지 추정하고 결함트리의 논리적 관계에 따라 정상사상의 발생 확률을 계산할 수 있다.

2.4 항공기 안전성 평가 사례

본 연구에서는 항공기 터보팬 엔진 FADEC(full authority digital engine control) 시스템이 감항기술기준의 요구항목에 적합함을 입증하기 위하여 수행한 안전성 평가 사례를 바탕으로 분석하였다. 터보팬 엔진의 시스템 안전성 평가(system safety assessment) 측면에서 결함트리 분석(FTA, fault tree analysis) 기법을 적용하여 다음과 같이 분석하였다.

결함트리분석 기법은 잠복고장이나 인간의 실수 등과 같은 복잡한 시스템 논리에 의해 발생하는 복수고장에 대해서 사용할 수 있기 때문에 시스템의 안전성 분석에 매우 유용한 방법이다. 특히 비행관제 시스템이나 화학 처리공장 혹은 원자력 발전소와 같은 대규모 시스템에 대

한 안전성 분석에 흔히 사용되나 결함트리는 매우 복잡하고, 수작업이 불가능하기 때문에 대규모 시스템에서는 결함트리분석을 위한 컴퓨터 프로그램들이 개발되어 사용되고 있다. 이러한 결함트리분석은 전체 시스템을 관심의 대상으로 하여 시스템의 결함을 가정하고 세부 절차에 따라 가능한 모든 원인들을 확인하게 된다.

결함트리분석의 특징은 다음과 같이 정리할 수 있다.

① 결함트리분석의 장점

- 특정 효과로부터 근본 원인까지 논리적 고장 경로를 체계적으로 파악하고 기록할 수 있다.
- 병렬, 중복 또는 선택적인 고장 경로를 다룰 수 있다.
- 대부분의 조합사건(combinatorial events)과 종속성(dependencies)을 다룰 수 있다.
- 몇 개의 하부시스템들이 교차 연결된(cross linked) 시스템을 다룰 수 있다.
- boolean 대수 등을 활용하여 비교적 쉽게 최소 논리 모델을 만들 수 있다.
- 논리 모델을 확률 척도로 쉽게 변환할 수 있다.
- 고장 모드의 원인과 정상 사상에 미치는 주요 효과를 파악한다.
- 미리 예상하기 어려운 최종 결과(영향)의 잠재적 원인을 찾을 수 있다.
- 1~2개의 정상사상에서 출발하는 전반적이고 체계적인 고장 분석에 적합하다.

② 결함트리분석의 단점

- 분석을 과도하게 하는 경우 규모가 방대해진다.
- Fault tree의 서로 다른 부분에 동일한 사상이 나타남으로써 혼동을 야기할 수 있다.
- 어느 한 사상의 상태 사이의 전이 경로를 나타내지 못한다.
- 각 정상 사상들에 대해 별도의 fault tree 작성이 필요하다.
- 특정 정상사상을 유발하는 주요 원인이 다른 사상에 미치는 영향은 분석되지 않는다.
- 수리/정비 정책이나 가용성 분석에는 유용하지 않다.
- 공통원인고장(common cause failure) 및 귀결고장이 누락되는 경우가 많다.

③ 결함트리분석의 용도

- Single points of failure의 확인
- 정상사상에 대한 동시발생 non-critical events의 결합 효과 조사
- 잠재적 설계결함 및 위험조건 (hazard)의 확인
- 안전성 향상
- 유효한 시정조치의 평가
- 정비(maintenance)와 고장점검(trouble-shooting)의 단순화

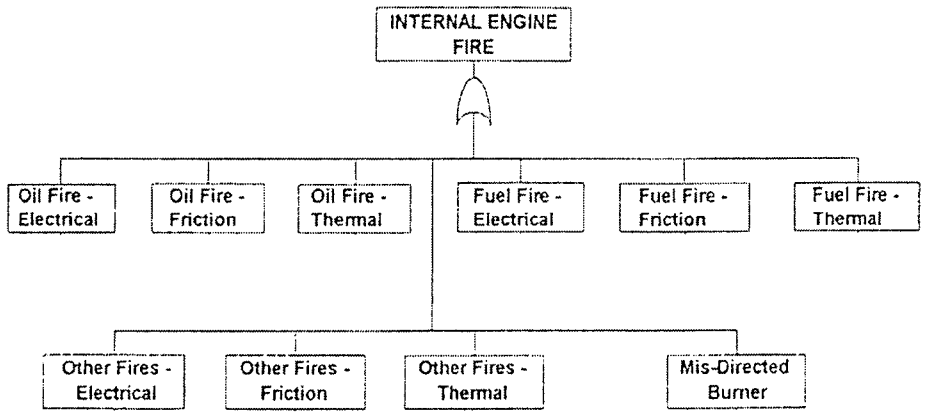
- Human interface/software interface 평가

항공기 엔진의 화재 및 제반 안전성이 감항기술기준 요건에 적합함을 입증하기 위하여 터보팬 엔진 시스템에서 유발 가능한 경우를 모두 고려한 결함트리(fault tree)를 구성하고, 각각의 요소 결함에 대한 분석을 바탕으로 다음과 같이 제시할 수 있다.

(1) 화재에 대한 안전성 분석

엔진 내부에서 화재가 발생할 수 있는 요인은 전기, 마찰 또는 열이며, 이러한 원인에 의해 오일이나 연료가 발화될 수 있다. 또한 같은 요인으로 기타부분에 대한 화재도 발생할 수 있으며, 연소실의 부적절한 화염전파도 고려할 수 있다. 이와 같은 엔진 내부 화재 가능성에 대한 결함트리를 <그림 4>와 같이 작성하고, 각각에 대한 가능성을 설계 측면에서 검토하여야 한다.

전기 계통은 스파크를 발생하는 부분품을 포함하지 않도록 설계하고 마찰에 의한 인화는 베어링의 결함 등으로 인한 과도한 마찰력이 발생한다면 가능하지만, 설계에서 해당 사항이 충분히 고려되었으며, 운용 경험에 의하면 마찰력에 의한 화재는 발생한 적이 없어야 한다.



<그림 4> 엔진 내부 화재 발생 가능성에 대한 결함 트리

고열에 의한 화재 발생 가능성이 있는 곳은 bearing compartment이며, 누설되는 오일을 외부로 배출하기 위한 통로를 별도로 마련하고, 이제까지의 경험에 근거하면 화재 발생 가능성이 없어야 한다.

시동실패(hung start)로 인하여 연소실에 잔류되는 연료는, 재시동 할 때 화재로 진전되지 않아야 한다.

(2) 외부라인, 피팅, 기타 구성품의 내화성 분석

적용된 모든 구성품은 내화성이 있으며, 피팅이나 비금속성인 호스류는 TSO C-75의 기준품질에 적합하며, 작동 압력에 대한 시험을 수행하고, 결함이 발생하는 경우에도 화재 발생가

능성이 최소화되는 위치에 호스류를 배치하는 것이 설계에서 고려되어야 한다.

(3) 기어박스, 오일탱크에 대한 내화성 분석

오일박스는 내화성 자재로 덮고, 화재 가능성이 희박한 팬 케이스 쪽으로 위치를 이동하고, 기어박스에 대하여 내화 특성을 분석으로 입증하고, 해당 내용을 적용하여야 한다.

(4) 인화성 연료 또는 증기의 배출에 대한 분석

의도하지 않은 인화성 연료나 증기의 누적이 발생하지 않도록 설계시 고려하여, 배출될 수 있는 인화성 액체를 한 곳으로 모을 수 있도록 공간을 구비해야하고, 이동 구간에 적용된 배관은 모두 내화성 자재를 사용해야 한다.

(5) 점화에 대한 안전성 분석

화재구역은 엔진 하부의 부품 설치공간과 압축기, 연소실, 터빈이며, 이 구역에는 내화성 자재를 사용하여 점화 가능성이 없어야 한다.

(6) 엔진결함 파편에 의한 케이스 관통이나 파손에 대한 분석

케이스 관통이나 파손에 대한 결함 트리를 <그림 5> 및 <그림 6>과 같이 작성하고, 각각에 대한 가능성을 설계 측면에서 검토하여야 한다.

10조 시간 이상인 동일 계열 엔진의 운용 경험 자료와 비교 분석하여, 디스크의 경우 과온이나 저주기피로(LCF)로 인한 문제점이 발생하지 않아야 한다.

추력 증가로 인한 온도상승을 고려하여, 자재 선정 및 최신 설계기술의 활용 등을 통하여 예방을 위한 최대의 조치를 강구하여야 한다.

블레이드의 이탈에 대비한 운동에너지 계산이 케이스 설계에서 고려되어야 한다.

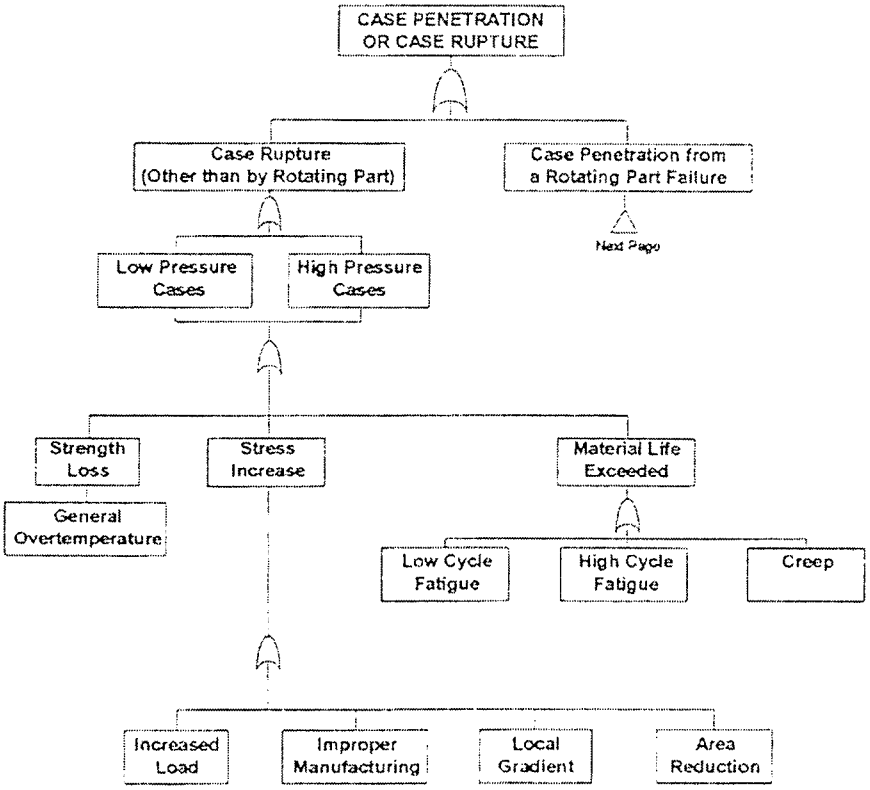
- ECC(electronic engine control) software에는 압축기 출구에서 과도한 압력이 발생하지 않도록 조절하는 기능이 포함되어 있어야 한다
- 회전체의 과속은 여유한계를 20%까지 설정하여 설계되어야한다.

(7) 엔진 장착부 구조에 대한 분석

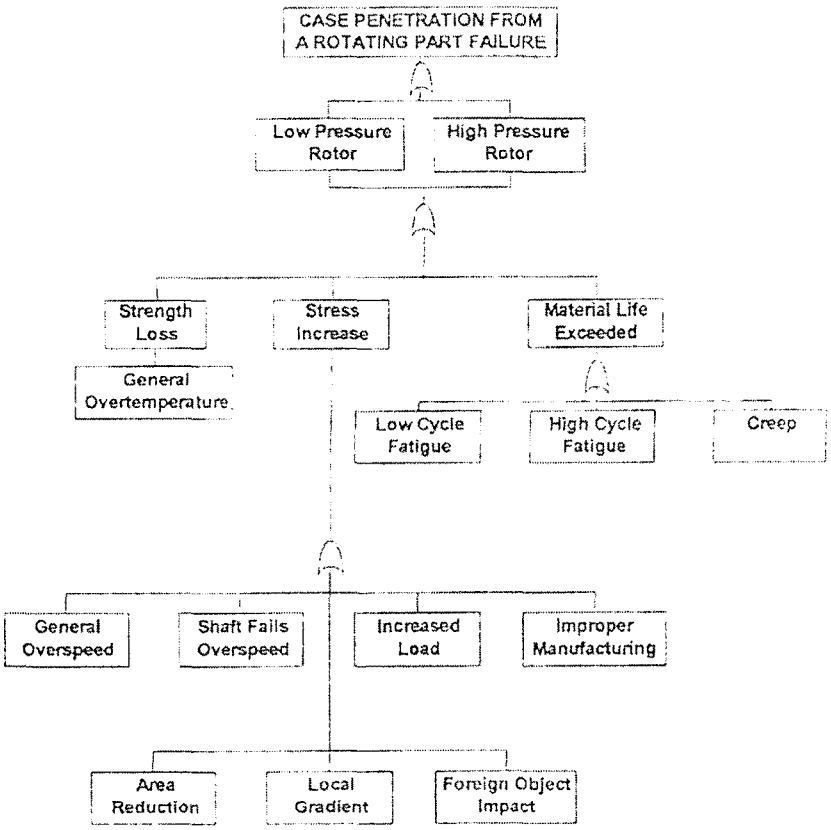
기존의 엔진과 동일한 개념의 장착부를 유지하되, 추력증가로 인한 하중분배를 고려한 설계이며, 다음과 같은 극한하중을 고려하여야 한다.

- 충돌하중 : 9 g
- 회전부 급격 정지 하중
- 팬 블레이드 손실로 인한 하중

최대 기동하중의 1.5배



<그림 5> 케이스 파손/관통에 대한 결함트리



<그림 6> 케이스 파손/관통에 대한 결함트리(회전부 파손의 경우)

(8) 엔진 시동 및 정지 능력에 대한 분석

어떠한 상황에서도 엔진의 시동을 정지시킬 수 있어야한다.

이와 같이 항공기 엔진의 안전성평가를 위해서는 감항기술기준 요건에 화재안전성, 발화, 폭발 및 제반 안전성 등의 요건에 적합함이 입증되어야 하며, 터보팬 엔진에 대한 결함트리 분석 기법 연구를 통해 추가적으로 고려해야 하는 사항을 도출하였다.

3. 결 론

항공기 및 부품의 인증을 위해서는 해당 시스템의 안전성 평가를 통하여 세부 요구조건에 대한 적합성을 입증하여야 한다. 이를 위해서 안전성 평가를 위한 모든 고장상태를 설정하고, 이러한 고장상태를 유발할 수 있는 원인 중 중요사항이 모두 고려되었다는 것을 보장할 수 있

어야 한다. 특히, 항공기와 같은 복합시스템의 경우에는 시스템 및 부품의 통합으로 인해 야기되는 복잡성 및 상호 의존성을 고려하여야 하며, 통합 시스템을 포함한 모든 경우에 대하여 시스템의 적절한 안전성 목표를 수립하고, 이 목표의 만족 여부를 판단하기 위한 안전성 평가를 전체 항공기의 관점에서 수행하여야 한다.

또한, 운용 중 변경사항이 발생할 경우에는 이로 인하여 시스템의 안전성에 미치는 영향을 다시 평가하여야 하며, 시스템의 안전성을 수치적 확률 분석만으로 입증하여서는 안되고, 시스템 안전성 평가를 위한 공학적 판단이 중심이 되어야 한다. 이를 위해서는 안전성 평가를 위한 지속적인 연구 및 개선활동이 진행되어야 하며, 대상 품목에 따라 세부적으로 적용해야 할 기법의 개발이 필요하다.

본 논문에서는 현재 항공선진국의 항공기 엔진 시스템에 대한 안전성 평가를 인증 측면에서 수행하는 절차와 평가 기법의 사례를 고찰하였으며, 항공기 엔진 시스템의 안전성이 감항기술기준 요건에 적합함을 입증하기 위하여 터보팬 엔진에 대한 결함 분석 기법을 분석하였으며, 제시한 분석 방법은 향후 우리나라에서 제작하게 될 항공기 엔진 시스템의 설계에 대한 안전성 평가시에 긴요하게 활용될 것으로 판단된다.

참 고 문 헌

[1] 항공안전본부 고시 제2007-13호, "항공기 기술기준"

[2] SAE, Certification Considerations for Highly-integrated or Complex Aircraft Systems, ARP 4754

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

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

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

[6] FAA System Safety Handbook, Practices and Guidelines for Conducting System Safety Engineering and Management