

## 항공기 시스템 안전성 평가 기술동향

글 유승우 swyoo@kari.re.kr, 이백준, 진영권  
한국항공우주연구원 항공우주안전·인증센터 제품보증그룹

### 1. 서론

항공기는 3차원 공간을 운항하는 비행체로서 초고속 운송수단으로 사용되는데, 사고가 발생하게 되면 수많은 인명피해와 재산손실을 초래하게 되므로 시스템 및 부품에 대하여 높은 수준의 신뢰성과 안전성이 요구된다. 또한 항공기의 안전한 운항을 위해서는 항공기 시스템은 물론이고, 항공교통관제 시스템, 공항시설, 항행안전시설 등에 대한 안전성 평가 및 안전관리가 필수적이다. 여기서 안전성(Safety)이란 시스템이 위험상태에 이르지 않는 상태 또는 정도를 의미하는 것으로서, 본 논문에서는 하드웨어와 소프트웨어를 포함한 항공기용 부품 및 시스템을 대상으로 고려하였다. 항공기용 부품 및 시스템에 대해서는 내구성, 내열성, 내식성과 같은 첨단재료기술과 임무수행을 위한 성능은 물론이고, 시스템에 대한 고도의 안전성 및 신뢰성이 요구된다. 따라서 대상제품의 설계 적합성을 입증하기 위한 안전성 평가가 수행되어야 하며, 이는 항공기 및 관련 부품의 인증을 위한 필수적인 요소기술이다. 즉 안전성 평가는 인증의 핵심사항으로 개념설계단계에서부터 착수하여 설계가 진행됨에 따라 세부적인 평가 및 분석이 수행되어야 하며, 설계변경이 발생하는 경우 변경된 설계에 대하여 재평가를 하여야 한다. 또한 항공기 운용과정에서 발생 가능한 각종 사고에 대한 사전 예방 및 정비를 위해서도 체계적인 안전성 평가가 필수적이다.

항공기용 부품 및 시스템의 안전성 평가에는 설계(Design), 개발(Development), 그리고 인증(Certification)

업무가 통합되어 적용되며, 과거의 사용 또는 경험에 따라 세분화된 안전성 평가 요구조건을 구분하여 적용한다. 특히 국제민간항공기구(ICAO, International Civil Aviation Organization)와 각국의 감항당국은 민간 항공기 또는 부품에 대한 법적 인증 제도를 자국의 실정에 맞추어 제도화하고 있으며, 항공기 및 부품을 개발, 생산, 운용함에 있어서 항공기 및 관련 부품에 대한 안전성 입증과 안전한 운항을 보장하기 위하여 국가 차원에서 이를 관리하고 있다. 이는 항공기의 개발, 제작 및 운용에 있어서 공공의 안전을 확보하기 위한 것으로서, 항공기 개발자는 해당 법규, 표준서 및 지침 등에 따라 최소한의 안전성을 입증하여야 한다.

한국항공우주연구원 항공우주안전·인증센터에서는 항공기 시스템에 대한 설계가 설정된 목표를 충족하고 있는지를 확인 평가하고, 설계, 개발, 인증사항을 고려하여 종합적인 안전성 평가기법을 적용할 수 있도록 안전성 평가에 관한 연구를 수행하고 있으며, 본 논문에서는 안전성평가에 대한 연구 동향에 대하여 소개하고자 한다.

### 2. 본론

항공기는 매우 복잡하고, 다양한 신기술의 첨단부품이 통합된 시스템으로서 개발비용이 매우 많이 소요되고, 사고가 발생하면 이의 파급효과가 매우 커서 고도의 신뢰성과 안전성을 확보하기 위한 활동이 필수적이며, 안전성을 입증하기 위해 체계적이고 매우 엄격한 인증이 수행되어야 한다. 또한 항공기 인증기술은 생산된 항공기 및 부품에 대하여 상품으로서의 가치를 부여하기 위하여 제품의 개발과 병행하여 확

보하여야 하는 기술의 한 분야로서, 경제성과 안전성의 확보를 목표로 개발되는 민간 항공기 및 관련 부품의 경우에는 필수적인 사항이다. 민간 항공기 인증

- ② 위험수준을 낮추기 위한 활동의 범위
- ③ 위험수준을 낮추기 위한 활동의 효율성
- ④ 해당 법규 및 기준의 만족 여부

표 1. 적용 분야 및 목표에 따른 안전성 평가의 구분

	민간 항공기 인증	시스템 획득 및 조달
목표	항공기/부품의 안전성 확보	해당 프로그램 또는 시스템의 위험조건을 확인, 평가하여 제거 또는 제어하는 것
적용 시점	항공기 및 부품 개발 단계 (인증 이전 단계)	항공교통관제 시스템 등의 획득/운용/관리 단계
안전성 평가 단계	① FHA (Functional Hazard Assessment) ② PSSA (Preliminary System Safety Assessment) ③ SSA (System Safety Assessment) ④ CCA (Common Cause Analysis) - PRA (Particular Risk Analysis) - ZSA (Zonal Safety Analysis) - CMA (Common Mode Analysis)	① OSA (Operational Safety Assessment) ② PHA (Preliminary Hazard Analysis) ③ SSAR (System Safety Assessment Report) - SSHA (Subsystem Hazard Analysis) ④ SHA (System Hazard Analysis)
관련 문서	- 감항기술기준, FAR, JAR - AC (Advisory Circular) - SAE ARP 4761/4754	- Order 8040.4 (Safety Risk Management) - SMS guidance - AMS(Acquisition Management System) policy

을 위하여 요구되는 안전성 평가는 운용기 또는 항공교통관제(ATC, Air Traffic Control) 시스템 등의 획득 및 조달에 적용되는 안전성 평가와는 다소 차이가 있으며, 용어 및 개념 등의 차이점은 표 1과 같다.

민간 항공기 및 부품에 대한 안전성 평가와 입증에 대한 법적 요구조건은 두 가지 목표에 따른 활동으로 구분된다. 첫째는 잠재적 위험요소 자체를 제거하는 것이고, 둘째는 제거가 불가능한 위험요소의 경우 잔존하는 위험수준을 허용할 수 있는 수준 이하로 낮추기 위한 활동이다. 두 가지 모두 시스템의 안전성을 확보하기 위하여 여러 가지의 기술과 공학적 기법을 응용하게 되며 이 중 하나가 안전성 평가(Safety Assessment)이다. 안전성 평가에서는 고장이나 재해의 발생확률을 평가하는 방법을 이용하며, 안전성을 확보하기 위한 종합적이고 균형적인 노력을 시스템의 전 수명주기에 걸쳐서 검토하고 적절한 조치를 취하여야 한다. 이 과정에서 제품 및 시스템 안전성을 입증하는 것은 개발자의 의무사항으로서, 다음과 같은 사항을 기본적으로 고려하여 적용하여야 한다.

- ① 허용할 수 있는 위험요소의 수준

## 2.1 해외 주요기관의 안전성 연구

1960년대에서부터 최근까지 전 세계적으로 발생한 항공기 사고율을 보면 1970년대 이전까지 높았던 사고율이 기술과 시스템의 발전으로 인하여 1970년대 들어 급격히 감소되었으나, 1970년대 중반 이후부터 항공기 사고율은 더 이상 낮아지지 않고 30여년 동안 정체상태에 머물러 있다. 그러나 항공 운송량은 해마다 증가하고 있어 전체 사고 발생 횟수는 오히려 늘어나고 있으며 이 같은 추세가 지속된다면 2010년에는 현재보다 2배 이상 증가할 것으로 예상된다. 이에 따라 세계 각 국의 감항당국을 비롯한 국제민간항공기구 등 항공안전과 관련된 조직은 다음과 같은 목표를 설정하고, 항공기 사고 예방을 위한 안전성 평가 기법 개발, 안전성 정보 공유, 안전성 평가를 위한 규정, 기준 또는 표준 제정, 항공기의 설계, 제작, 시험에 대한 체계적 인증과 운항, 정비 등에 대한 철저한 감독을 수행하기 위한 연구를 진행하고 있다.

국제민간항공기구에서는 다음과 같은 안전성 목표를 제시하고 있으며, 시카고 협약을 통해 항공기 인

증을 협약 체결국들의 의무사항으로 정하여 항공기 인증을 제도화하고 있다.

- ① 전세계 국제 민간 항공분야의 안전하고 체계적인 성장 보장
- ② 항공 사고율을 감소시키기 위한 국가와 항공 산업체간 협력 강화

미연방항공청(FAA)은 2007년까지 1994~1996년 당시 사고율의 80% 수준으로 낮추고, 이를 지속시키는 것을 목표로 안전성 확보를 위한 활동을 진행 중이다.

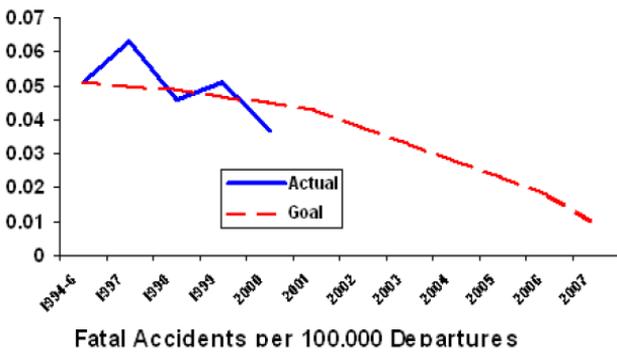


그림 1. 항공기 사고율 목표 및 변동추이 (FAA)

유럽연합은 항공안전 수준을 향상시키고, 유럽 각국에 동일한 체제를 유지하기 위하여 2002년에 유럽연합감항당국(EASA, European Aviation Safety Agency)을 구성하였으며, 민간 항공기에 대한 인증 업무를 비롯하여 안전성 확보를 위한 활동을 공동으로 수행중이다. 특히 유럽의 항공산업체간 과도한 경쟁으로 인한 손실을 방지하고, 공동 개발 및 연구를 통해 안전성 향상에 기여하기 위한 목표도 가지고 있으며, 최근에는 비유럽 국가의 감항당국과도 협력 체계를 확대해 나가고 있다.



그림 2. 항공기 안전성 평가 프로세스 모델 (ARP 4754)

또한 최근에는 항공 산업계에서 통용되고 있는 각종 지침서, 안내서, 표준서, 규격서 등의 활용도가 높아지고 있는데, 이는 감항당국이 감항기술기준을 통해 항공기 안전성 평가에 대하여 요구조건을 설정하고 있으나, 이것만으로는 충분한 지침을 제시할 수 없기 때문이다. 안전성 평가에 대한 권고 지침서로는 SAE(Society of Automotive Engineers)에서 제시하고 있는 ARP 4761과 ARP 4754가 대표적이다. 이는 항공기 개발자, 체계종합업체, 부품 제작자, 운항 및 정비 관련 조직, 감항당국을 비롯한 인증조직 등이 안전성 평가를 실제로 수행할 수 있도록 세부 기법, 절차, 판단기준, 정보 등을 제공하기 위한 것으로서, 항공기 안전성 평가 프로세스로서 권고하는 V-모델은 그림 2와 같다.

## 2.2 항공기 안전성 평가 적용 프로세스

민간 항공기 및 관련 부품에 대한 인증의 주요 목표는 항공기 및 부품이 해당 요구조건에 부합하는지 확인하고 최소한의 안전성을 보장하기 위한 것이다. 이러한 항공기 인증과정 중에서 시스템, 서브시스템, 부품의 인증을 안전성 평가의 개념이 적용되는 프로세스에는 감항성 승인, 규격 적합성 검증, 초도품 승인, 비행 안전 부품 승인 및 구조 견실성 검증 등이 있으며, 이와 같은 프로세스에는 예상 환경조건에서 인증 결과가 지속적으로 유지된다는 것을 입증하기 위한 시험 방법 및 적합성 입증에 위한 세부 기법들이 포함된다. 각 프로세스는 서로 다른 분야에 초점을 맞추어 진행되지만, 궁극적인 목표는 항공기의 인증을 위한 것으로서 이러한 프로세스들은 항공기 인증 프로그램 내에서 상관관계를 갖고 있으며 상호 중복되기도 한다.

시스템이 간단하여 직접적인 방법으로 설계가 가능한 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 분석을 수행하여야 한다. 또한, 시스템 안전성에 대한 목표를 수립하고, 시스템 설계가 설정된 목표를 충족하고 있는지를 평가하며, 항공기의 고장 또는 사고 발생을 방지하거나 고장이 발생하였을 때 이로 인한 영향

(손실)을 최소화하기 위한 노력이 체계적으로 이루어져야 한다. 이러한 프로세스의 최종 단계는 더 이상의 시험 또는 분석이 필요하지 않을 정도로 데이터 검토, 검사 또는 기타 조치 등을 수행하여 승인사항에 대하여 입증하기 위한 조사 및 관련 활동이 완결되는 시점이다.

### (1) 감항성 승인

감항성 승인에는 대상 제품(항공기 시스템, 서브시스템 또는 부품)의 감항성 확인을 위해 적용되는 분석, 설계, 시험 및 문서화 등의 프로세스가 포함되며, 주요 목표는 항공기가 설정된 범위에서 운용되는 경우, 요구되는 기능을 안전하게 수행할 수 있다는 것을 입증하기 위한 것이다. 또한, 시스템 또는 부품이 적절하게 통합될 수 있다는 것을 입증하기 위해서도 감항성 승인이 필요하며, 항공기 운용에 있어서의 모든 위험성이 최소화되었다는 것을 입증하기 위하여 수행된다. 즉, 감항성 승인은 시스템이 감항성 요구조건에 적합하다는 것을 보증하기 위해서, 부품, 서브시스템, 시스템 등 대상 수준에 대하여 수행되는 평가 프로세스이다. 예상 운용 범위 결정, 설정된 운용 범위 내에서의 시험 및 안전한 운용을 보증하기 위한 제한 작동사항 설정을 포함한 감항성 승인의 기초사항이 이 프로세스의 범위이며, 공학적 분석, 검사, 설계 검토, 안전성 평가, 공급업체 승인 및 시험 등이 이 프로세스에 포함된다. 감항성 승인 계획서 작성 단계에서 감항성 승인 요구조건이 개발되어야 한다. 공급업체에 대한 분석, 검토, 시험, 감사, 실증 등을 위해 공급업체가 수행해야 할 의무사항 및 감항성 승인 계획서의 내용을 수행하기 위한 세부 요구조건 등은 일반적으로 감항성 승인 규격에 포함된다.

### (2) 규격적합 검증

규격적합 검증은 대상 제품이 설정된 요구조건을 만족하는지 판단하기 위하여 적용되는 프로세스로서, 검사, 분석, 실증 및 시험을 통해 모든 계약 성능 규격 요구조건을 만족한다는 것을 입증하기 위한 것이다. 규격적합 검증은 계약업체가 계약 요구조건을 만족시켰는지를 확인하기 위하여 적용되는 프로세스이지만, 이 프로세스를 통해 도출된 대부분의 데이터는

시스템의 감항성 입증에 사용되기도 한다.

규격적합 검증은 시스템이 규격 요구조건에 적합하게 작동하는지 포괄적으로 평가하기 위한 프로세스로서, 주로 성능에 중점을 두고 진행되며, 시스템의 품질 보증 부분에 대한 규격에는 설정된 개별 규격 항목에 대하여 적합성을 입증하기 위한 적합성 매트릭스가 포함된다. 규격적합 검증의 범위는 이러한 규격 요구조건을 만족시키는 것으로서, 예를 들어 서브시스템 수준에 대한 규격적합 검증 프로세스에서는 서브시스템 수준에 대한 규격 요구조건을 규정하여야 한다.

### (3) 초도품 승인

초도품 승인은 개발자에 의해 생산된 초도품이 물리적 성능 요구조건에 적합한지 판단하기 위하여 사용되는 프로세스로 정의한다. 여기서 초도품(First Article)은 시제품(Prototype)과 구별해야 하는 개념으로서, 통상적으로 형식증명 단계에서는 개발, 설계 및 시제품을 대상으로 하는 반면, 제작증명 단계에서는 초도품 및 관련 품질시스템을 대상으로 하게 된다. 초도품 승인의 목표는 채택된 제작 공정을 통하여 이전에 승인된 특성을 보유한 제품을 생산할 수 있는지를 확인하기 위한 것이다. 초도품 승인 프로세스는 통상적으로 제품이 개발 생산단계에 착수한 이후에 적용된다. 이러한 초도품 승인은 제작 방법 및 프로세스가 승인된 시제품의 특성을 변경시키지 않는다는 것을 입증하기 위해서도 적용된다.

초도품 승인 프로세스는 대상 제품이 해당 프로세스 및 절차에 따라 제작되었는지 확인하고, 제작된 부품이 규정된 운용 조건에서 성능 요구조건에 부합하는지 확인하는 과정으로 구성된다. 이러한 초도품 승인 프로세스의 중요한 측면은 초도품 개발 및 승인 절차에서 검증된 수준과 동등한 성능이 나타나도록 제작 및 생산 절차와 공정을 설정하고 이를 확인하여야 한다는 것이다. 초도품 승인을 위한 검증 및 시험 범위는 성능 재확인을 위한 이전의 승인과정을 재수행하고 제작 공정에 대한 승인을 위한 추가 시험을 수행하는 것이다.

### (4) 비행안전부품 승인

비행안전부품 승인은 항공기를 운용하는 과정에서

안전성에 중요하다고 판단되는 부품을 지정하여, 이 부품에 대하여 집중적으로 분석, 시험, 제어 및 관리하는 프로세스로 정의하며, 다음과 같은 두 가지 목표에 따라 수행한다. 첫째는 항공기 인증 프로그램의 일환으로 비행안전부품이 적절하게 설계, 분석, 제조, 시험되었는지 확인하기 위한 것이고, 둘째는 비행안전부품의 중요한 특성을 사전에 파악하여, 제조 공정까지의 모든 과정에 대하여 관리해야 할 사항을 설정하고 이를 안정화시키기 위한 것이다.

이러한 비행안전부품 승인은 대상 부품에 대한 관리 수준과 기술적 세부 요건의 수준에 있어서, 기타 일반 부품에 대한 승인 프로세스와 차이가 있다. 비행안전부품 승인 프로세스에서 요구되는 검증 및 시험의 범위는 안전한 비행조건 유지를 위해 중요한 부품의 특성을 설정하고, 이러한 특성에 대한 시험 세부내용을 설정하는 것이다. 비행안전부품 승인 활동에는 비행안전부품의 설계, 부품의 비행 안전 특성에 대한 부품 수준에서의 시험, 그리고 검사활동 범위와 부품 추적 요구조건을 설정하는 활동이 포함된다.

**(5) 구조건실성검증**

구조건실성 검증이란 기체 강도, 경도, 손상 허용, 내구성 등과 같은 항공기의 구조적 건실성을 설정, 평가 및 실증하는 것으로 정의하며, 이러한 구조건실성 검증의 목표는 구조 설계 영역의 적합성을 보증하기 위한 것이다. 구조건실성 검증은 하중경로 및 응력이 예측한 결과와 일치하는지 확인하고, 정비 에

로사항을 경감시키거나 예방하기 위하여 취약한 세부 설계를 확인하기 위한 것이다.

구조건실성 검증 프로세스의 세부 활동에는 허용 가능한 구조 설계 영역 설정, 적절한 재료와 공정 및 조립 방법의 선정, 설계 분석, 하중 분석, 응력 분석, 손상 허용 분석, 진동 분석, 재료 시험, 전기체 정적 시험, 피로시험, 그리고 비행 및 지상 하중 검토 등이 포함된다.

**2.3 안전성 평가 결과의 설계반영**

항공기 및 부품에 대한 안전성 평가 결과는 지속적으로 설계에 반영되어야 하는데, 이러한 설계 변경은 고장 발생원인을 완전히 제거하는 것이 이상적이지만, 기술수준, 설계 제약조건, 비용 등의 문제로 인하여 불가능할 경우에는 평가 대상의 고장발생 확률 및 심각도 등급을 종합적으로 고려하여 다음과 같은 우선순위에 따라 적용하여야 한다.

**(1) 최소 위험성 설계**

제거가 불가능한 위험요소의 경우에는 잔존하는 위험성을 허용수준 이하로 낮추기 위한 설계변경이 이루어져야 한다. 여기서 허용 가능한 수준은 안전성 평가 대상에 따라 기술적, 공학적 판단을 바탕으로 설정되어야 하며, 발생확률을 낮추거나 고장으로 인한 영향을 최소화하는 방안이 이에 포함된다. 현재 감항기술기준 및 관련 문서에서 규정하고 있는 고장

표 2 고장 발생 가능성 및 심각도 구분

발생 가능성		고장 영향(심각도) 등급		항공기 및 탑승자의 영향	비행시간당 발생 확률
FAA	JAA	FAA	JAA		
Probable	Frequent	No Effect	No Effect	보통	1.0E-2
	Reasonably Probable	Minor	Minor	불편	1.0E-3
비상 절차에 따른 운용상의 제한 발생				1.0E-5	
Improbable	Remote	Major	Major	안전여유의 감소 (승무원 대처의 어려움, 승객 부상 등)	1.0E-7
	Extremely Remote	Severe Major	Hazardous	안전여유의 막대한 감소 (작업량 및 환경조건으로 인하여 승무원의 정상적인 대처 불가능, 소수의 탑승자 사상 등)	1.0E-9
Extremely Improbable	Extremely Improbable	Catastrophic	Catastrophic	다수의 탑승자 사망, 항공기 파손 등	

발생 가능성과 고장 영향 등급은 다음 표 2와 같다.

### (2) 안전장치의 추가 설치

위험성을 최소화하기 위한 설계가 불가능한 경우에는 안전 설계 특성을 반영하거나 자동으로 동작하는 고정식 안전장치를 추가적으로 설치하는 방안으로서, 설치된 안전장치에 대해서는 주기적인 기능 점검이 요구되며, 이를 해당 절차에 따라 문서화하여야 한다.

### (3) 경보장치 설치

위의 2가지 방안을 적용할 수 없는 경우에는 상태를 감지하여 위험 발생 조건에 대하여 적절한 경보 신호를 발생시킬 수 있는 경보장치를 설치한다. 이러한 경보신호 및 경보장치는 인적요소를 충분히 고려하여 설계에 반영하고, 운용상의 오작동 및 부적절한 반응이 발생하지 않도록 설치하여야 한다.

### (4) 절차 및 훈련과정 개발

위의 모든 대안이 실현 불가능한 경우에 비상절차를 개발하여 이를 숙지할 수 있도록 반복적으로 훈련하는 방안으로서, 심각도가 Hazardous 및 Catastrophic 등급인 경우 위험성을 감소시키기 위하여 절차 및 훈련과정을 개발하고자 하는 경우에는 감항당국의 승인을 받아야 한다.

## 3. 결론

항공기 및 관련 부품의 인증을 위해서는 안전성 평가를 수행하고, 대상품목의 세부 요구조건에 대한 적합성이 입증되어야 한다. 이를 위해서는 안전성 평가를 위한 모든 고장상태가 설정되고, 이러한 고장상태를 유발할 수 있는 원인 중 중요사항이 모두 고려되었다는 것을 보장할 수 있도록 계획 및 관리되어야 한다. 특히, 항공기와 같은 복합시스템의 경우에는 시스템 및 부품의 통합으로 인해 야기되는 추가적인 복잡성 및 상호의존성을 고려하여야 하며, 통합 시스템을 포함한 모든 경우에 대하여 시스템의 적절한 안전성 목표를 수립하고, 이 목표의 만족 여부를 판단하기 위한 안전성 평가를 전체 항공기의 관점에

서 수행하여야 한다. 그리고 운용 중 변동사항이 발생할 경우에는 이로 인하여 시스템의 안전성에 미치는 영향을 다시 평가하여야 하며, 시스템의 안전성을 수치적 확률분석만으로 입증하여서는 안 되고, 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.

## 참고문헌

1. SAE ARP 4754, "Certification Considerations for Highly-integrated or Complex Aircraft Systems"
2. SAE ARP 4761, "Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment"
3. FAA System Safety Handbook, "Practices and Guidelines for Conducting System Safety Engineering and Management"
4. Cranfield Univ., 2004, "Safety Assessment of Aircraft Systems"
5. ADS-51-HDBK Aeronautical Design Standard Handbook, 1996. "Rotorcraft and Aircraft Qualification(RAQ) Handbook"
6. Frank C. Fickeisen, SAE 2001-01-2664, "Improving the Effectiveness of Airplane Certification Analysis Processes"
7. 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"
8. J. Murdoch, J.A. McDermid, P.Wilkinson, International System Safety Conference, 2001. "Failure Modes and Effects Analysis (FMEA) and Systematic Design"
9. Safety & Security Measurement White Paper V 2.0, 2004. PSM Safety & Security TWG