T-50 항공기 체계안전성 프로그램

T-50 Aircraft System Safety Program

김대식*, 오세창, 장재상, 이정욱(한국항공우주산업), 정창래(국방과학연구소)

1. 서 론

다양한 무기체계의 개발에 있어서 신뢰성(Reliability)은 이미 중요한 키워드로 인식되고 있다. 그런데 특별히 항공기체계의 개발에 있어서 신뢰성 못지않게 중요성이 높은 것이 바로 안전성(Safety)이다. 항공기 체계안전성(System Safety)은 항공기시스템의 손상 및 운용요원에게 위해를 유발하는 잠재적 위험요소(Hazard)를 설계단계에서 확인(Identification) 및 평가(Evaluation)하고 이를 제거(Elimination) 또는 허용수준으로 완화(Control)하는 것으로, 좁은 의미에서 설계안전(Design Safety) 라고도 한다. 설계결함에 의한 항공기 사고(Mishap)는 그 자체로 엄청난 손실이며 이후 사고예방을 위한 시스템 재설계 및 재시험 등의 비용지출을 야기하므로, 비용대비 효과측면에서도 항공기 체계안전성 프로그램의 중요성은 쉽게 인식된다.

과거 항공기에서의 안전프로그램은 사고발생 이후에 재발방지를 위해 단편적으로 적용되었다. 즉, 우선 만들어서 비행하고 문제가 있으면 고쳐서 다시 비행하는 개념으로, "Fly-Fix-Fly" 라고하며 Fig. 1과 같다. 또한 이런 접근법은 저성능 항공기에서 분명히 효과적인 것이었다.

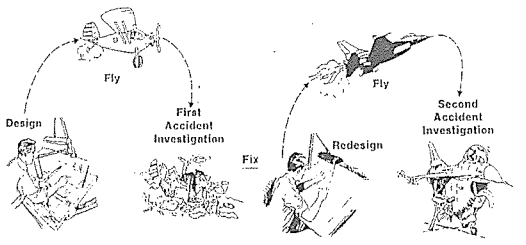

Fig. 1. The "Fly-Fix-Fly" Approach - Minimal Safety Program in the Past

그러나 점차 항공기가 고성능화 되면서 사고발생 결과가 더욱 심각해짐에 따라 기존의 단편적인 안전프로그램 적용이 더 이상 적합하지 않게 되자, 처음부터 안전을 확보할 수 있는 보다 강력한 안전프로그램의 적용이 필요로 되었다. 그 결과, 최근 항공기에서의 안전프로그램은 개발단계에서부터 계획하고 규정되어 조직화된 절차에 따라 적용하고 있다. 이런 방법은 "Identify-Analyze-Control"로 특징지어 지며 Fig. 2와 같다.

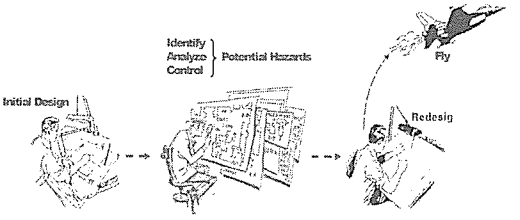

Fig. 2. The "Identify-Analyze-Control" Approach - Strong Safety Program Recently

최근 T-50 항공기 체계개발 단계에서도 체계적인 안전성 프로그램을 적용하여 요구되는 항공기의 정량적 및 정성적 안전성 수준을 만족시키기 위한 노력이 경주되었다. 다음은 T-50 항공기 개발에서의 안전성 프로그램 적용사례와 대표적인 안전성분석(Safety Analysis) 및 위험도평가(Risk Assessment)를 소개한다.

2. 체계안전성 개발계획

항공기 개발단계의 체계안전성 업무는 체계안전성 개발계획(System Safety Program Plan, SSPP)을 수립하고 소요군의 관련부서와 협의하여 확정하고 이를 수행하는 것이다. T-50 SSPP는 체계안전성 업무에 대한 일반적인 작성기준을 제시하고 있는 MIL-STD-882 'Standard Safety Program Requirement'을 기준으로 작성되었으며, T-50 사업의 규모, 예산, 예상 위험도수준(Level of Risk)을 고려하여 비용대비 효과적이며 달성 가능한 수준으로 수립하였다.

T-50 SSPP는 체계안전성 업무목표, 수행조직, 일정, 수행기준, 안전성 분석, 안전성 활동, 그리고 안전성 검증 등의 주요내용으로 구성되었으며, 특히 수행기준에는 확인된 잠재적 위험요소(Hazard)의 위험도평가(Risk Assessment)를 위한 T-50 시스템의 허용안전수준(Acceptable Safety Level)이 포함되었다. T-50 체계안전성 주요업무 흐름은 Fig. 3과 같다.

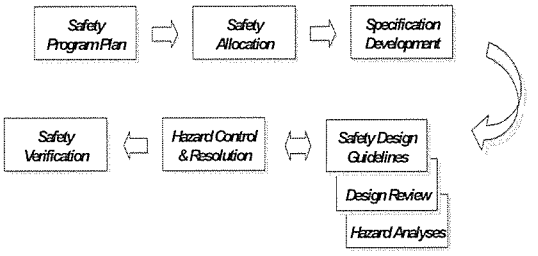

Fig. 3 T-50 System Safety Process

체계개발 초기 T-50 SSPP를 수립/확정한 이후에 항공기 수준의 정량적 안전성 요구도인 중사고율(Class A Mishap Rate)을 주요 시스템 수준으로 할당(Allocation)하고, 시스템사양서(Specification) 및 부품개발사양서에는 안전성 관련 요구도를 반영하였다. 또한 설계초기부터 설계자가 설계안전 개념을 이해하고 설계에 적용토록 안전성 설계지침(Design Guideline)을 제공하고, 설계가 진척됨에 따라 가용한 자료를 이용한 안전성 분석을 수행하였다. 체계개발 초기에는 정성적 안전성 분석을 수행하고, 후기에는 상세설계 자료가 가용해짐에 따라 정량적 안전성 분석과 위험도평가를 수행하였다.

3. 체계안전성 분석

3.1 위험요소 감소절차

체계안전성분석(System Safety Analysis)은 설계의 진척 단계별로 가용한 설계자료를 이용하여 잠재적 위험요소를 확인하고 이를 SSPP에서 설정한 허용안전수준 기준으로 평가하고, 위험도(Risk)가 높은 항목에 대해서는 위험요소 감소절차(Hazard reduction Procedure)를 적용하여 위험요소 제거 또는 완화 설계를 반영한다. Fig. 4는 위험요소 감소절차이다.

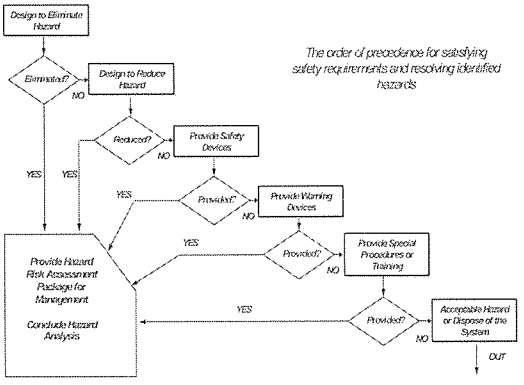

Fig. 4 Hazard Reduction Procedure

확인된 위험요소가 허용안전수준을 넘어서는 경우는 설계변경으로 위험요소 제거 혹은 위험도 감소를 우선 고려하고, 설계변경이 곤란한 경우는 안전장치 추가 혹은 경고장치 제공으로 위험상황 노출을 지연 하거나 조종사에게 위험을 인지시킨다. 마지막으로 위험상황에 빠지지 않도록 운용절차 혹은 점검주기를 보완한다. 도출된 위험요소 감소방안은 해당 설계자에게 통보되고 설계자는 이를 검토하여 위험요소 감소방안을 반영하게 되는데, 이 과정은 공식적인 절차로 처리되며 T-50에서는 체계안전 설계항목(System Safety Design Item) 관리절차를 적용하여 종결에 이를 때까지 최초로 해당 위험요소를 도출한 안전성 분석과 더불어 관리하였다.

T-50 체계안전성 분석은 크게 정성적(Qualitative) 분석과 정량적(Quantitative) 분석으로 나눈다. 정성적 분석은 예비위험요소분석(Preliminary Hazard Analysis, PHA), 계통위험요소분석(Subsystem Hazard Analysis, SSHA), 그리고 운용 및 지원위험요소분석(Operating and Support Hazard Analysis, O&SHA)이 있으며, 정량적 분석에는 고장계통도분석(Fault Tree Analysis, FTA)이 있다. Fig. 5는 설계단계별 안전성 분석 수행시기를 도표화 한 것이다.

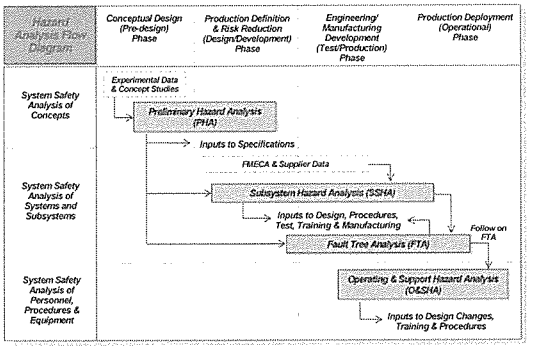

Fig. 5 Comparison of measured roughness data

3.2 정성적 체계안전성 분석

예비위험요소분석(PHA)은 개념설계부터 예비설계검토(PDR)까지 수행된 귀납적이며 정성적인 분석으로, 유사 항공기의 안전설계 및 사고사례를 고려하여 거시적 차원의 잠재적인 위험요소를 확인/평가하고 위험요소를 제거 또는 완화하는 설계를 반영하기 위한 위험요소 분석이다.

일단 위험요소가 확인되면 영향성을 고려하여 위험도를 정성적으로 평가하고, 앞서 소개된 위험요소 감소절차에 따라서 위험요소를 제거 또는 위험도를 낮추기 위한 설계방안을 제시하게 된다. 이후 변경되는 설계를 기준으로 안전성 평가를 다시 실시하고, 재평가된 안전성 수준이 SSPP에서 설정한 허용안전수준을 만족하는 것으로 평가되면 설계자에게 확인된 위험요소를 인지시키고 해당 위험요소가 적절히 조치될 때까지 추적/관리하게 된다. Fig. 6은 PHA 분석의 일부이다.

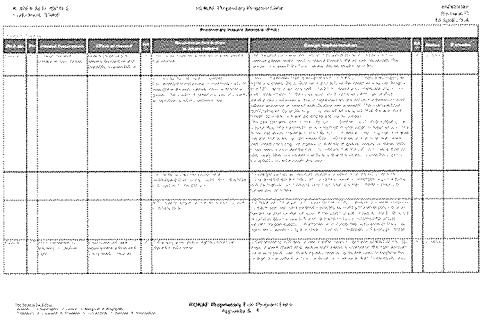

Fig. 6 PHA worksheet - Sample

계통위험요소분석(SSHA)은 예비설계검토(PDR) 이후 상세설계 시작과 더불어 수행하는 귀납적이며 정성적인 분석으로, 상세설계단계에서 시스템을 구성하는 주요 구성품의 성능저하 또는 고장이 항공기 안전에 미치는 영향을 확인/평가하고 위험요소를 제거 또는 완화하는 설계를 반영하기 위한 위험요소 분석이다.

확인된 위험요소 평가 및 조치는 PHA와 동일하며, 주요 설계변경 혹은 안전성 분석이 필요한 관심사항 발생시 추가분석을 수행하고, 해당 위험요소가 적절히 조치될 때까지 추적/관리하게 된다. Fig. 7은 SSHA 분석의 일부이다.

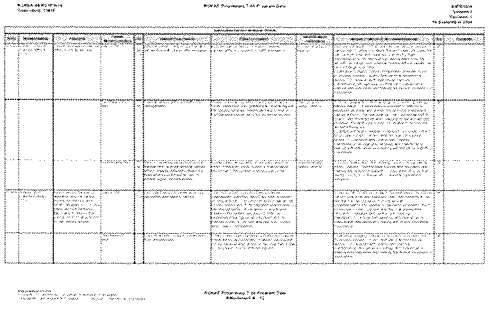

Fig. 7 SSSA worksheet - Sample

운용 및 지원 위험요소분석(O&SHA)은 상세설계검토(CDR) 이후 항공기 운용 및 지원절차서 작성시 수행하는 귀납적이며 정성적인 분석으로, 항공기 운용 및 지원절차에 존재하는 위험요소를 인적인 안전관점에서 확인하고 조치하는 것이다. 확인된 위험요소는 절차수정 혹은 경고/주의/주기 문구를 추가하여 작업자의 안전을 환기시킨다. Fig. 8은 O&SHA 분석의 일부이다.

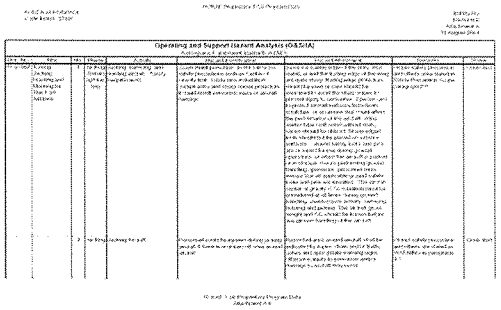

Fig. 8 O&SHA worksheet - Sample

3.3 정량적 안전성 분석

고장계통도분석(FTA)은 상세설계가 진행되고 어느 정도 가용한 분석자료 확보와 더불어 수행하는 연역적이며 정량적인 분석으로, 개발단계에서 중사고율(Class A Mishap Rate)을 예측하고 요구도 만족여부의 검증을 위해 수행하였다.

FTA는 최상위사상(Top Event)을 T-50 중사고(Class A Mishap)로 설정하고, 이를 유발하는 고장들의 인과관계를 조합하여 고장경로(Fault Path)를 구성하였다. 이때 T-50 항공기시스템 및 운용요원의 안전에 심각한 결과를 초래하는 거시적 고장은 앞서 분석된 PHA와 유사항공기 운용사례에서 도출하고, 부품단위의 상세한 고장유형(Failure Mode)과 영향성은 SSHA로 확인하여 최하위사상(Basic Event)을 구성하였다.

구성된 Fault Tree에는 정량적 분석을 위한 고장률(Failure Rate), 고장노출시간(Failure Exposure Time) 및 조건부확률값(Conditional Probability)을 입력하게 된다. 고장률은 고장유형 영향 및 치명도 분석(Failure Modes Effects and Criticality Analysis, FMECA) 자료에서 확인/입력하고, 고장노출시간은 항공기 임무계획, 주기검사, 평균임무시간, 지상운영시간 및 비행교범 등의 항공기 운용자료에 기초하여 산출/입력하며, 조건부확률값은 유사항공기 운용자료에 T-50 운영환경을 고려하여 적용하였다. FTA결과 산출에는 전용 컴퓨터프로그램이 사용되었다. Fig. 9는 FTA 분석의 일부이다.

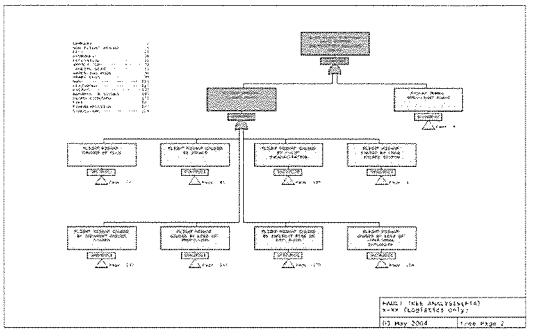

Fig. 9 FTA Tree - Sample

4. 위험도 평가

위험도평가(Risk Assesment)는 정성적 체계안전성 분석, 설계검토 혹은 비행시험에서 확인된 잠재적 위험요소를 심각성(Severity) 및 발생확률(Probability) 측면에서 위험도 수준을 평가하는 것이다.

심각성은 위험요소 발생시 항공기시스템, 운용요원 및 환경에 미치는 영향성의 심각한 정도에 따라서 정성적으로 Catastrophic, Critical, Marginal 및 Negligible의 4 단계로 분류하였다. 발행확률은 일정규모에서 항공기를 운용시 위험요소가 발생되는 빈도를 정성적으로 Frequent, Probable, Occasional, Remote 및 Improbable의 5 단계로 분류하고, 각 단계는 다시 정량적으로 그 범위를 정의하였다. 이때 정량적 기준은 T-50 항공기에 요구된 안전성 수준에 의해 고유하게 결정되었으며, 특히 발생확률의 정량적 분석에는 앞서 소개된 FTA 기법을 이용하였다. Table 1은 위험도 판정기준의 일부이다.

Mishap Severity Categories

Category	Description	Fleet or Inventory
1	Catastrophic	Death, system loss, or severe environmental damage
2	Critical	Severe injury, severe occupational illness, major system or environmental damage
3	Marginal	Moderate injury, moderate occupational illness, or minor system or environmental damage
4	Negligible	Minor injury, occupational illness, or less than minor system or environmental damage

Mishap Probability Levels

Level	Description	Fleet or Inventory	Probability of Failure
A	Frequent	Continuously experienced	More Than x.0E-0x
B	Probable	Will occur frequently	x.0E-0x ~ x.0E-0x
C	Occasional	Will occur several times	x.0E-0x ~ x.0E-0x
D	Remote	Unlikely but can reasonably be expected to occur	x.0E-0x ~ x.0E-0x
E	Improbable	Unlikely to occur, but possible	Less Than x.0E-0x

Table 1 Mishap Severity and Probability Levels

위험요소의 심각성과 발생확률이 판정되면 Table 2의 T-50 SSPP에서 설정한 위험도 평가표에서 위험도 수준을 평가한다. 이때 위험도 수준은 위험요소의 심각성과 발생확률의 정도에

Probability \ Severity		Catastrophic 1	Critical 2	Marginal 3	Negligible 4
Frequent	A	1A	2A	3A	4A
Probable	B	1B	2B	3B	4B
Occasional	C	1C	2C	3C	4C
Remote	D	1D	2D	3D	4D
Improbable	E	1E	2E	3E	4E

- Unacceptable - Immediate corrective action required
- Undesirable - Appropriate management decision required
- Acceptable with appropriate management review
- Acceptable - Be considered as adequately controlled and acceptable

Table 2 Risk Assesment Matrix

따라 Acceptable, Acceptable with appropriate management review, Undesirable , 그리고 Unacceptable 영역으로 구분하였다.

이러한 위험도평가는 항공기 개발과정에서 시기적절하게 위험요소를 확인 및 평가하여 조치함에 있어서 위험요소가 허용안전수준으로 완화되었는지를 판정하는 체계안전성 업무의 기준으로서 뿐만 아니라, 개발항공기의 전반적 안전성 수준을 결정짓는 중요한 요소이다.

5. 결론

본 논문에서는 T-50 항공기의 정성적 및 정량적 체계안전성 요구도를 만족시키기 위해서 적용된 T-50 항공기 체계안전성 프로그램과 사용된 대표적인 안전성분석 및 위험도평가 기법을 소개하였다.

T-50 체계개발 프로그램을 통하여 경험한 체계안전성 개발계획과 정량적 및 정성적 안전성분석 및 위험도평가 기법은 향후 진행되는 항공기 개발프로그램에 적용됨은 물론이고, 고위험성이 따르고 고개발비용이 소요되는 타 분야의 개발프로그램에서도 선택적으로 적용이 가능하기 때문에 T-50 체계안전성 프로그램 적용사례를 소개하는 본 논문의 의의가 있다고 하겠다.