초도비행 안전점검과 시스템 안전

조 건 현

System Safety Role on FFRR

Keun-Hyun Joe

● 조건현(국방과학연구소)
● 1949년생
● 기계공학(경영학)을 전공하였으며, 파괴역학 및 시스템 안전에 관심을 가지고 있다.

1. 개 요

지금으로부터 30여 년 전의 무기체계 설계에서는 과거의 경험에 의해 알려진 위험이나 명확히 밝혀진 위험을 제거하는 일 이외에는 시스템 안전분야가 거의 적용되지 못했었다. 그러나 오늘날과 같이 시스템의 복잡화에 따른 고가의 시스템 구입비, 크기 및 중량의 허용한계 등과 같은 여러 제한요인 때문에 고도의 신뢰성 있는 무기체계 개발을 위해서는 무기체계 개발과정의 전 순기 동안에 시스템 안전(system safety)분야의 적용이 불가피하게 되었다.

시스템 안전에 관한 연구는 매년 증가하는 사고로부터 발생하는 엄청난 손실을 줄여보자는 필요하에 1960년 경부터 미국의 군대에서 시작되었다. 1969년 7월 미국 군사표준서 MIL-STD-882(시스템 및 관련 부시스템에 대한 시스템 안전 프로그램 요구조건)가 제정된 이후 요즈음 미군의 방산물자 조달 및 획득시 시스템 안전분야 적용이 의무화되어 있다.[1]

시스템 안전분야는 개발중인 시스템의 설계, 개발, 운용과 관련된 여러 분야, 즉 품질보증, 인간공학, 시스템공학, 형상관리분야 등과 상호 밀접하게 연관되어 있으므로 이 분야에 대한 상호 이해와 끊임없는 정보교환이 요청되고 있다.

시스템 구성분야별, 무기체계 개발단계별로 조직적으로 분석된 시스템 안전결과를 토대로 프로젝트 관리자(PM)는 개발중인 무기체계 시스템에 내재된 시스템 위험을 어느 수준까지 수용할 수 있을 것인가에 대한 현명한 판단을 내릴 수가 있게 되는데 항공기 개발 프로그램의 경우 시스템 안전의 궁극적인 목표는 성공적인 초도비행이라고 할 수 있다.[2]

1.1 시스템 안전이란

시스템 안전은 시스템 관리자가 시스템 안전위험의 수용여부를 판단해야 할 때 체계적인 의사결정을 할 수 있도록 하는 유효한 수단 또는 과정이며, 또한 시스템 설계, 운용자, 운용환경 등이 서로 관련되어 있다.

시스템 안전은 전 순기비용, 시간 및 운용

효율성을 고려한 최적의 안전정도로서 정의될 수 있으며, 위험요소의 식별, 문서화, 통제, 제거에 공학적 원리, 기준, 기법을 사용한다. 또한, 시스템 안전개념을 시스템 개발 초기에 시스템에 통합시키고 위험을 감소시키며, 설계변경 및 수정사항을 최대한 줄여 개발비용을 절감하고 필요시 개량조치로 인하여 시스템 내의 고유의 안전이 저해되지 않는 것을 목표로 하는 하나의 분야라고도 할 수 있다.[3,4]

또 다른 정의로서 MIL-STD-882에서는 시스템 안전을 시스템의 설계, 운용, 폐기까지에 걸쳐 운용면의 유효성, 시간, 비용의 제약조건 내에서 안전을 최적화하기 위한 설계 및 관리원칙, 기준, 기법의 적용이라고 정의하고 있다.[5]

산업안전과 시스템 안전과는 책임 할당면에서 미소한 차이가 있다. 산업안전은 회사 종업원의 복리와 사고 및 장비, 재산손실 예방에 있으나, 시스템 안전은 업체 제품을 사용하는 고객에 대한 책임이 있는 점이 다른 점이다.

어떤 무기체계에 대한 개발이 진행되어 시스템 안전 프로그램 계획(SSPP)이 프로젝트 관리자(PM)에 의해 승인되면, 시스템 안전과 관련하여 보통 다음과 같은 6개의 기능이 무기체계 개발기간 동안에 수행된다.[6]

○안전 기준의 확립
○위험 평가
○과정의 보고
○잠재 위험의 확인(식별)
○수정 조치의 추천
○결과의 추적

이러한 단순한 6 단계의 순서는 안전공학이 프로그램 안전에 직접 영향을 미치는 사전(事前)의 방법(before-the-fact method)이라고 할 수 있다. 시스템 안전의 주요기능은 최종 설계결정에 이르기 전에 위험요소를 제거하거나 최소화하기 위해 수정조치/행동이 확인되고 취해지도록 위험요소를 조기에 식별하고, 위험등급(classification)을 매기는 것이라고 할 수 있다.

1.2 시스템 안전공학의 발생

지난 30년간 안전에 관한 새로운 2개의 유형 즉, 제품안전(항공기 및 기타제품 안전관련) 및 시스템 안전(사전(事前)의 예측적 안전관련)이 개발되었는데, 두 분야의 목적 역시 부상 또는 손상의 예방이라는 면에서 똑같다. 제품안전 및 시스템 안전은 매년 증가하는 사고로 인한 손실을 줄여보자는 의도로서 그 필요성이 제기되었으며 그중 시스템 안전은 미군사 기관으로부터 소요가 제기되어 개발되었다.

많은 안전문제가 적절한 설계에 의해 해결된다는 것은 자명한 사실이며, 시스템 안전 및 제품안전 개념은 이러한 원리에 기초를 두고 있다. 시스템 운용시 발생하는 사고를 예방하는 가장 효과적인 수단이란 설계 및 개발시 위험요소를 줄이거나 감소시키는 것이다. 과거의 시스템 개발시에는 시스템 구입 비용이 저렴하고 원자재가 풍부하였으며, 시스템 안전개념이 잘 적용되지 않았다.

즉, 과거의 경험에 의한 명백한 위험요소를 제거하는 것 이외에는 안전설계 개념이 시스템에 거의 적용되지 못하였으며, 일단 시스템이 운용되면 "비행(fly), 수리(fix), 비행(fly)"이라는 개념이 사용되었다. 어떤 확인된 위험요소는 수리를 통해 제거되거나 또는 수리를 할 필요가 없는 낮은 위험요소로 판단되었으며, 어느 경우든 중량 및 비용 등과 같은 제한요소를 수용할 수 있다고 판단하였다. 즉, 시스템 안전을 주요 설계요소로서 고려하기에는 비용대 효과면에서 적절하지 못하다고 판단되었던 것이다.

오늘날과 같이 시스템의 복잡성이 증가함에 따라 시스템 안전의 역할은 점차 오늘날의 시스템 안전개념으로 변모되었다. 즉, 시스템 구입 및 개발비용은 엄청나고, 제작은 쉽지 않으며, 설계변경 및 크기·중량 등과

같은 제한요인들이 지배하게 되었다. 다시 말해서 시스템 교체 및 수정비용이 천문학적으로 증가되었으므로 운용단계에서 나타나게 될 위험만을 대처할 수 없게 됨에 따라 안전개념을 시스템 개발초기부터 적용함으로써 전순기 비용을 줄이고 시스템의 신뢰성을 높여야 한다는 필요성은 더욱 증대되었다. 이전(以前)의 (일단 비행후 수리 및 재비행) 개념은 오늘날에는 안전요소의 "확인-분석-제거(identify-analyze-eliminate)"라는 시스템 개념으로서 사전(事前)의 과정으로 특정지워지게 되었다.[7]

시스템 안전을 강조하기 위한 초기의 노력은 미국의 각 군에 의해 여러 지시문서 및 훈령의 제정으로 나타나게 되었으며, 곧 이어 모든 군사기관 및 방산업체, 그리고 여러 개발계획에 적용 가능한 표준방안이 요구되어 MIL-STD-882(시스템 안전 프로그램 요구조건 ; 이전에는 MIL-S-38130 제정)에 이어서 수정판이 제정되었다.

이 표준서에서는 시스템 안전 프로그램의 시행을 하나의 요구조건으로서 규정했으며, 이 프로그램을 시행하는 정부 및 방산업체의 프로그램 관리자 및 관련요원들의 역할을 정의하고 있다.

1.3 시스템 안전 상호 관련분야

시스템 안전을 적용하기 위해서는 시스템 안전과 관련되는 여러 분야(품질보증, 인간공학요소, 신뢰성, 가용성, 정비성, 가치공학, 시험지원, 설계·생산공학, 산업안전, 훈련, 시스템 공학, 형상관리 등)로부터의 검토 결과에 대한 명확한 이해가 필요하며, 적절한 정보교환을 위해서는 상호협조가 이루어져야 한다.

시스템 안전은 산업안전 및 운용과 관련된 안전 분야에 대한 심층분석이 이루어져야 하며, 개발품 제작분야는 산업안전 및 시스템 안전 그룹과 상호 관련된다. 제작이 이루어짐에 따라 작업자에게 영향을 주는 안전 문제는 물론 설계에서의 문제점 검토시 제품이나 시스템 안전은 중요한 역할을 한다. 시스템 안전 및 이와 관계되는 분야의 상호작용 검토시에는 사상(事象) 및 그들의 발생확률에 대한 분석이 요구되며 시스템 안전은 개발중인 시스템의 설계, 개발, 운용과 관련된 모든 분야와 상호작용을 한다.[3]

2. 시스템 안전의 주요 목적

시스템 안전의 주요 목적은 사고를 줄일 수 있는 위험요소의 확인, 평가 및 제거이며, 이 목적은 무기체계를 개발하고, 획득하는 책임이 있는 정부와 방산업체에 의해 공동으로 수행되어야 한다. 시스템 안전 노력이 중복되지 않도록 하는 공식적인 토론형식의 모임이 시스템 안전 위원회(SSG)이다.

이 SSG는 무기체계의 획득과 관련된 정부와 방산업체를 대표하는 사람들로 구성된 정식으로 조직된 집단이며, 시스템 안전 목표를 달성하는데 있어서 정부 차원의 프로그램 관리자에 대한 조언의 역할을 한다. 이 위원회는 또한 방산업체로 하여금 방산물자 사용자에 의해 경험되는 안전관련 문제를 인지하고 있는지를 정부차원의 시스템 안전 담당자가 확인할 수 있는 역할을 한다.

3. 시스템 안전 목표

시스템 안전 프로그램은 다음과 같은 내용이 실행되도록 체계적인 분석방안을 제시해야 한다.

- ○임무 요구조건과 일치하는 안전이 적시에 그리고 비용과 효과면에서 유리하도록 시스템에 설계되어야 한다.
- ○각 시스템과 관련된 위험요소가 확인, 평가, 제거되며, 관련된 위험이 시스템의 전순기에 걸쳐 프로그램 관리자가 수용할 수 있는 수준으로 감소되어야 한다.
- ○다른 시스템으로부터의 경험에 의한 교

훈을 포함한 과거의 안전자료가 고려되어 사용되어야 한다.

○새로운 설계, 재질 및 제작, 시험기법을 수용하고 사용하는데 있어 위험요소가 최소화되어야 한다.

○위험요소를 제거하거나 위험을 감소시켜 프로그램 관리자가 수용할 수 있도록 취해진 조치가 문서화되어야 한다.

○프로그램 관리자가 수용할 수 있는 적절한 위험수준이 유지될 수 있는 범위내에서 설계 및 형상임무 조건의 변경이 이루어져야 한다.

○중요한 안전 데이터가 "경험에 의한 교훈(lessons learned)"으로서 문서화되어야 하며, 관련 핸드북이나 규격에 삽입되어야 한다.

○시스템 안전 위험분석을 위해 구성품(엔진, 탈출좌석, 착륙기어 등)의 구매시 제작사에 고장유형 및 영향 분석 관련자료(FMEA, FMECA, 시스템 안전 위험분석 보고서 등)를 반드시 요청해야 한다.

4. 시스템 안전 과정

시스템 안전과정이란 원하는 시스템 안전 목표를 얻기 위한 시스템 공학을 논리적으로 적용시키는 것이며 주요 요소는 다음과 같다.

○경험에 의한 교훈의 사용

○위험분석(예비위험분석(PHA), 시스템 위험분석(SHA), 운용 및 지원분야 위험분 석(O & SHA) 등) 실시

○위험요소 확인, 분류, 평가

○시스템 요소의 수정

○유효성 평가

5. MIL-STD-882의 전체 내용

MIL-STD-882는 어떤 무기체계 시스템에 대한 위험요소를 확인하고 무기체계 운용자가 수용할 수 있는 수준으로 위험을 감소시키거나 제거함으로써, 위험요소(mishap)를 방지하는 설계요구 조건과 관리통제 과정을 부여하여 광범위한 시스템 안전 프로그램 개발 및 실행에 있어서 일관성 있는 요구조건을 제시하고 있다. 이 시스템 안전계획 요구조건은 관리 및 설계 등 양 분야에 있어서 각 무기체계 개발계획의 특수 요구조건에 맞는 시스템 프로그램이 되도록 프로젝트 관리자에 의해 적절히 구성되어야 한다.

5.1 MIL-STD-882C와 관련된 무기체계 획득순기별 수행업무

MIL-STD-882C를 무기체계 획득순기와 관련시켜 각 개발단계별로 수행해야 할 시스템 안전활동 분야를 살펴보면 다음과 같다.

5.1.1 개념형성 단계

○시스템 안전 프로그램 계획(SSPP) 작성

○시스템 안전 설계기준(체크목록) 작성 ; AFSC DH 1-X 참고

○예비 위험분석(PHA)

○개념설계 검토(PDR-1)

5.1.2 타당성 검토 단계

○예비설계 검토(PDR-2)

○각종 위험분석(예비 위험분석(PHA), 시스템 위험분석(SSHA), 운용 및 지원분야 위험분석(O & SHA)) 실시

○위험평가 보고서(SAR) 초안 작성

○시스템 안전 실무위원회(SSWG) 구성

○기 발간 시스템 안전 관련자료 검토

○시험평가 계획 결정

5.1.3 전면 개발 단계

○각종 위험분석(예비 위험분석(PHA) 최신화, 시스템 위험분석(SSHA) 구체화, 운용 및 지원분야 위험분석(O & SHA) 구체화)

○시스템 안전계획 수립 및 시험

○세부설계 검토(CDR)

○시스템 안전 프로그램 계획(SSPP) 최신화

5.2 시스템 안전설계 및 평가관련 주요 수행업무

○Task 201(PHL) : 프로그램 관리자가 시스템 안전 프로그램을 보다 강조할 수 있도록 잠재위험 요소의 예비 목록을 기술

○Task 202(PHA) : 어떤 개념이나 시스템에 대한 초기위험 평가를 하기 위해 예비 위험분석을 수행하고 문서화하는 것

○Task 203(SSHA) : 각 부시스템(subassy)의 구성품 설계, 운용 및 고장유형과 관련된 각 부시스템 및 구성품에 대한 심층분석을 실시하며 분석시 FMEA (Failure Mode and Effect Analysis), FMECA(Failure Mode and Effect Criticality Analysis), FMET(Failure Mode and Effect Test), FHA(Fault Hazard Analysis), FTA(Fault Tree Analysis) 등이 사용된다.

○Task 204(SHA) : 시스템의 운용과 관련된 분석 또는 시스템 및 부시스템에서의 고장유형의 상호 연관관계를 검토하는 것으로 SSHA에서 실시되었던 것과 거의 같은 분석기법이 사용된다.

○Task 205(O & SHA) : 환경, 인간, 절차, 장비와 관련된 위험의 분석

○Task 209(Safety Assessment) : 방산업체에서의 시스템과 관련한 특별통제·절차 및 잔존 안전문제의 문서화

6. 시스템 위험평가

시스템 안전 프로그램을 효과적으로 수행하기 위해서는 식별된 위험과 관련하여 적절한 위험평가가 요구된다. 위험평가가 이루어지기 위해서는 잠재적인 위험요소와 그러한 위험요소를 줄이기 위한 비용이 적절히 등급이 매겨지고, 설계의 결정이 이루어질 수 있

		위험요소로 인한 피해강도 등급					
		Ⅰ (극히치명)	Ⅱ (치 명)	Ⅲ (보 통)	Ⅳ (무시가능)		
미 국방성 군사표준서 (MIL-STD-882B)		사망 또는 시스템 손실	중상, 심한 직업병, 주요시스템 손상	경상, 경미한 직업병 또는 경미한 시스템 손상	무시가능한 질병, 직업병, 시스템 손상	미 연방규격 FAR 25. 1309-1	
위험발생확률		1	3	7	13	1×10^{0} 가능 1×10^{-5}	위험발생확률
	자주일어남	2	5	9	16		
	가끔일어남	4	6	11	18	불가능 1×10	
	드묾	8	10	15	19		
	극히드묾	12	15	17	20	극히불가능 00	

그림 1 위험평가 지수 조합

상급위험 : 1~5(HRI), 중급위험 : 6~12(HRI), 저급위험 : 13~20(HRI)

도록 위험 요소들은 우선순위가 매겨져야 한다.

수정조치에 대한 우선순위를 매길 때에는 위험요소로 인한 피해 강도(Hazard Severity)와 위험요소 발생확률(Hazard Probability)이라는 2개의 요소를 고려하는 것이 필요하다. 위험요소가 미치는 피해 강도는 주로 인간의 안전에 대한 치명도, 크기 또는 성공적인 임무완수 등이 관련되며, 그 특성은 정성적이다. (등급 Ⅰ은 극히 치명, Ⅱ는 치명적, Ⅲ은 보통, Ⅳ는 무시 가능)

위험요소 발생확률은 어떤 사건이 일어날 확률의 척도이며, 보통 정량적이지만, 가끔 정성적(매우 빈번히 일어남, 번번히 일어남, 가끔 일어남, 드뭄, 극히 드뭄 등)으로 분류되기도 한다. 우선순위 할당이 주관적 평가이기는 하지만, 보통 정성적으로 우선순위 할당을 할 때 위험평가 지수(HRI)를 사용하는 것이 유리할 경우가 많다. 어떠한 위험요소를 그림 1의 가로와 세로의 조합(matrix)으로 나타낸 수치 즉 위험평가지수가 1~5는 매우 높은 위험등급이며, 지수가 6~12까지는 중간 정도의 위험등급으로 분류된다. 이러한 중급 이상의 위험등급을 갖는 해당 안전분석 항목들은 위험지수 13 이하인 낮은 위험등급으로 분류될 수 있도록 설계에 대한 수정조치가 이루어져야 하며, 또한 계속 추적되어야 한다.

7. 항공기 설계와 관련한 시스템 안전 분석

7.1 개발단계별 시스템 안전분석 업무

항공기 설계와 관련한 시스템 안전분석의 첫단계는 초도비행 전에 가장 낮은 위험요소만이 있도록 정식으로 시스템 안전프로그램을 기술하고 있는 시스템 안전 프로그램계획(SSPP)을 작성하는 것이다. 프로젝트 관리자의 검토 및 승인 후 사본이 개발담당 책임자급 및 무기체계 개발 담당 방산업체에 전달되는데, 이 단계는 시스템 개념형성 단계에서 이루어진다.

두번째는 시스템 안전설계 체크목록의 작성단계이다. 이는 항공기의 운용시 가장 낮은 위험요소에 대해 요구되는 최소기준으로서, 설계와 관련된 엔지니어로 하여금 시스템 안전사항을 설계에 고려하였는지의 여부를 체크하기 위해 사용되는데 여러 분야의 설계담당 엔지니어로부터의 검토내용을 토대로 위험요소가 확인되며 통제가 이루어지게 된다. 이 체크목록은 미공군 체계사령부(AFSC) 발간 설계 핸드북 1-X(설계기준 일반 체크목록)를 기준으로 작성되며, 일련의 주요 설계원리, 기준 등이 요약되어 있다. 참고로 미공군 체계사령부(현재 미공군 물가사령부(AFMC)로 개편되었음)가 항공기 설계에 시스템 안전을 적용하기 위해 개발한 설계 핸드북의 구성을 살펴보면 크게 4개분야(설계일반, 항공시스템, 우주 및 미사일 시스템, 전자 시스템)로 대별할 수 있으며, 미공군 체계사령부 발간 설계 핸드북 1-6에 시스템 안전에 관한 내용이 수록되어 있다. (표 1 참조)[8]

세번째 단계에서는 예비 위험분석(PHA)을 실시한다. 이는 주로 개념형성 및 시스템 확정단계에서 보통 작성되며, 예비설계 검토(PDR) 15~30일 전에 제출되어야 한다. 예비 위험분석 목적은 시스템이나 개념의 초기 위험 평가를 확립하는 것이며, 계속적으로 군사규격이나 군사 요구조건을 만족하면서 안전 위험을 줄이기 위한 대안을 검토해야 한다. 이 분석에서 각 검토항목은 위험을 완화(Mitigate)시키기 위한 수정조치 결과에 따라 계속 검토해야 할 항목(Open Item) 또는 조치완료 항목(Closed Item)으로 분류된다. 확인된 위험요소에 대해 수정조치가 취해지면 그 항목은 조치완료 항목으로 되나 수정조치가 취해지지 않으면 계속 검토항목으로 분류되어 다음 단계의 위험분석 단계로 옮겨지게 된다. 프로그램 관리자(PM)에 의

해 수용될 수 있는 위험(Acceptable Risk)으로 간주되면 이 항목은 조치완료 항목으로 분류된다.

네번째 단계에서는 부시스템 및 시스템 위험분석(SHA)을 수행하며, 시스템 확정 및 시스템 개발단계에서 이루어진다. 이 분석은

표 1 미 공군 체계사령부 발간 설계 핸드북(DH) 목록

DH	1-0	General
	1-1	General Index and Reference
	1-2	General Design Factors
	1-3	Human Factors Engineering
	1-4	EMC
	1-5	Environmental Engineering
	1-6	System Safety
	1-7	Aerospace Materials
	1-8	Microelectronics
	1-9	Maintainability
	1-10	Reliability
	1-11	Air Transportability
	1-X	Checklist of General Design Criteria
DH	2-0	Aeronautical System
	2-1	Airframe
	2-2	Crew Stations and Passenger Accommodations
	2-3	Propulsion and Power
	2-4	Electronic Warfare
	2-5	Armament
	2-6	Ground Equipment and Facilities
	2-7	System Survivability
	2-8	Life Support
	2-9	Communist Air Defense
	2-X	Checklist for Aeronautical System
DH	3-0	Space and Missile Systems
	3-1	Ballistic Missiles
	3-2	Space Vehicles
	3-3	Ground Equipment and Facilities
	3-4	System Survivability
	3-5	Fluid Components
	3-X	Checklist for Space and Missile Systems
DH	4-0	Electronics System
	4-1	Command & Control System
	4-2	Electronic Systems Test and Evaluation
	4-3	Electronic Systems Facilities
	4-4	System Survivability
	4-X	Checklist Electronic Systems

시스템의 운용에 있어 모든 시스템의 상호간섭 작용(Interface)을 검토하기 위해 수행되며, 고장유형(Failure Mode)이 어떻게 시스템의 전반적인 안전에 영향을 미치는지 등을 검토한다. 이 보고서는 세부 설계검토(CDR) 15~30일 전에 제출되어야 한다.

다음 단계는 운용 및 지원분야 위험분석(O & SHA)이다. 이 분석은 환경, 인원, 운용절차 및 장비와 관련한 위험의 분석과 관련된다. 이 O & SHA의 결과와 지금까지

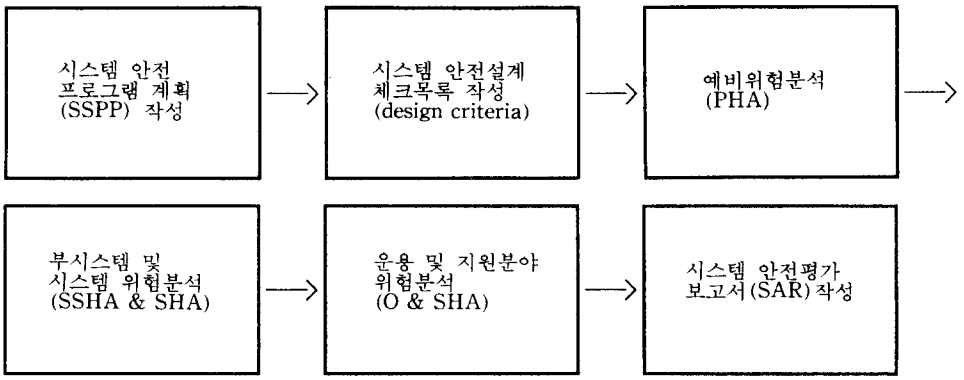

그림 2 항공기 설계시의 시스템 안전분석 활동

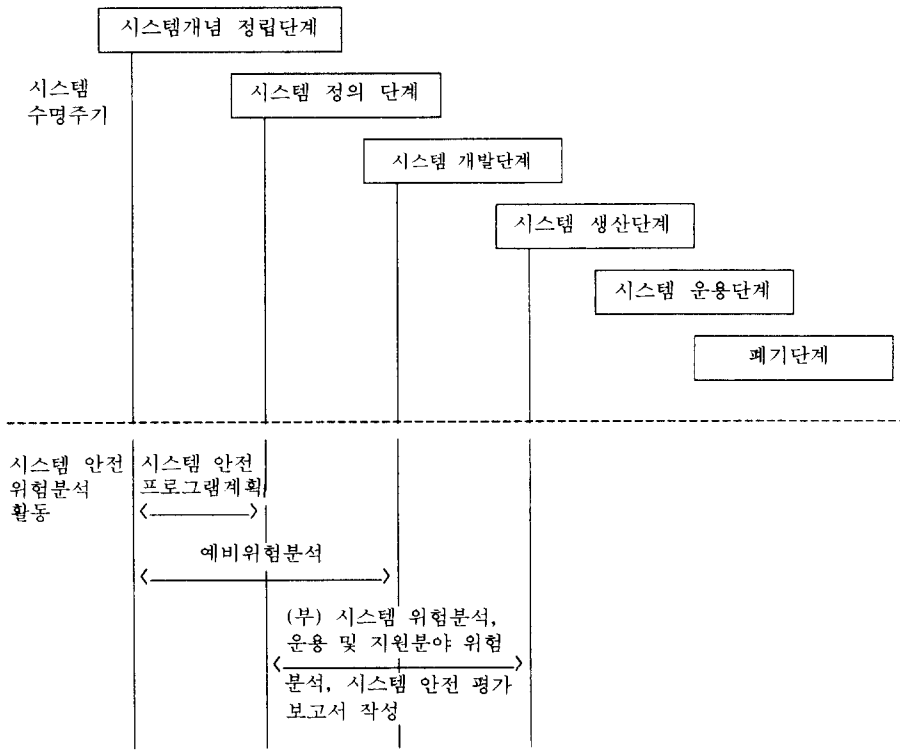

그림 3 시스템 안전프로그램 일정계획

수행된 위험분석으로부터의 계속 검토 요구된 위험항목 즉, Open Item에 대한 검토가 초도비행 안전점검팀(FFRRT)에서 이루어지는데, 운용 및 지원분야 위험분석결과 보고서는 보통 초도비행 30~60일 전에 제출되어야 한다.

마지막 단계에서는 시스템 안전 평가보고서(SAR)를 작성한다. 이 보고서는 초도비행 20~30일 전에 제출되며, 방산업체로 하여금 어떤 잠재 안전문제 및 시스템과 관련한 특별통제·절차를 문서화하는 업무가 수행되며, 초도비행 전에 프로그램 관리자에 의해 수용될 수 있는 최종 위험도 언급된다.

지금까지 언급된 항공기 설계시 수행되어야 하는 시스템 안전분석 활동의 순차적인 흐름을 요약하면 그림 2와 같으며 그림 3에서는 이러한 시스템 안전관련 활동을 무기체계개발 단계별로 연관시켜 제시하였다.

7.2 시스템 안전·책임·인원 구성

무기체계 개발과 관련된 모든 요원들은 시스템 안전분야에 대한 책임이 있으며, 프로젝트 관리자는 시스템 안전분야 전반에 관한 책임이 있다. 시스템 안전을 담당하는 부서를 가진 외국의 경우 어떤 무기체계 개발을 담당하는 정부 차원의 조직에서는 보통 3~6명의 요원이, 그리고 방위산업 관련 업체에서는 보통 6~10명이 담당하고 있다. 무기체계 개발에서 잠재적인 위험을 계속적으로 추적하고 효과적으로 대처하기 위한 시스템 안전 관련조직은 무기체계 개념형성 단계 및 전면 개발단계뿐만 아니라 무기체계에 대한 비행시험, 생산, 배치, 폐기단계에까지 계속 유지되어야 한다.

8. 초도비행 안전점검(FFRR)과 관련된 시스템 안전

새로 개발하거나 성능개량을 위한 항공기의 초도비행 인증을 위해 조직되는 전문분야별 검토팀(EIRT : Executive Independent Review Team)은 초도비행 준비태세를 점검하고 비행시험 및 평가업무를 수행한다. 이 EIRT는 새로운 항공기 개발시 시스템 안전분야에 대해 정부기관 또는 방산업체가 적절한 조치를 취했는지를 확인하는 임무를 수행하기 위해 구성된다. 이 팀은 항공기 개발부서와는 독립적인 검토팀으로서 개발 항공기가 성공적인 비행을 할 수 있고 또한 요구되는 모든 시스템이 수용될 수 있는 위험수준에서 운용될 수 있는가를 점검한다. 전문분야별 검토팀(EIRT)의 주요 관심사는 안전이므로 전체 시스템 관점에서 언급되어야 하며 아울러 초도비행과 관련된 위험요소 평가에 대해서도 언급되어야 한다.

이 EIRT는 대략 아래와 같은 분야에 대한 시스템 안전을 고려해야 한다.

- ○구 조
- ○비행기술
- ○추진기관
- ○비행장비
- ○조종실 및 비상 탈출시스템
- ○지원장비
- ○항공전자장비
- ○전력 발생 및 분배장치
- ○전자기 방해 및 적합성
- ○비행시험
- ○시스템 안전 고유업무 등

이상의 업무를 수행하는 EIRT로 이루어진 초도비행 안전 점검팀(FFRRT : First Flight Readiness Review Team) 제도는 미공군의 경우 항공무기 체계 개발시 채택되어 사용되고 있는데 국과연에서 개발하고 있는 훈련·지원기(KTX-1)의 초도비행 안전평가를 위해서는 미공군 물자사령부 산하요원, 미공군 비행시험센터 요원, 미 국립 비행시험학교 요원, 록히드 항공사 요원 등으로 구성된 초도비행 안전점검팀이 두 차례에 걸쳐 각각 한국을 방문하여 각 전문기술 분야에 대한 초도비행 준비상태를 점검한 결과 만족

할 만한 평가를 받아 성공적인 초도비행을 수행할 수 있었다.[9]

항공기 설계에 관련한 각 분야에 대해 FFRRT에서 검토한 비행안전요소 평가 등급은 다음과 같은 다섯 개의 범주로 구분된다.

○범주 A : 초도비행 이전에 반드시 해결되어야 할 사항
○범주 B : 가능한 한 초도비행전에 해결되어야 할 사항
○범주 C : 비행에 지장을 주지는 않으나 비행할 경우 제한이 가해지는 사항
○범주 D : 비행은 할 수 있으나 항공기 운용자가 문제점을 파악하고 있어야 할 사항
○범주 G : 일반적인 추천사항 등

FFRRT에서의 평가등급이 범주 A, B, C로 판정될 경우 특별한 사유가 없는 한 초도비행 전에 이러한 비행안전 저해요소는 반드시 해소(closed item)될 수 있도록 각별한 노력이 경주되어야 한다.

시스템 안전과 관련하여 초도비행 안전점검을 위해서는 크게 두 분야의 안전 즉, 시스템 안전 및 비행안전(flying safety) 등으로 구분되어 안전업무가 수행되어야 한다. 앞에서 언급된 바와 같이 시스템 안전은 항공기 개발 초기부터 전면개발, 생산, 운용, 폐기시까지의 장기간에 걸치는 활동인데에 반하여 비행안전은 개발 및 성능개량 항공기에 대한 비행시험 활동이 끝날 때까지에 한해서 전담인력으로서 구성되어야 하는 일종의 한시적인 조직이라고도 할 수 있다.

비행시험 프로그램을 담당하는 비행안전 관련요원은 안전과 관련하여 경험이 풍부한 조종경력이 있는 사람이어야 하며, 지상요원 및 시험비행 조종사가 언급하는 비행시험 관련내용을 조기에 파악할 수 있어야 한다.

비행안전요원의 역할을 열거하면 다음과 같다.

① 초도비행 안전 점검팀(FFRRT)의 일원으로서 참가
② 비행시험 계획 검토
③ 매일매일의 비행시험 카드에 서명 확인
④ 플러터 및 비행영역 확장 등을 포함한 모든 시험비행 관련사항의 확인 감독 및 조언
⑤ 비행전 및 비행후 브리핑에 참가
⑥ 비행 안전검토 위원회(SRB)에 참가 업무 등이다.

8.1 초도비행 안전점검(FFRR) 절차

초도비행 안전점검을 위해 EIRT로 구성된 FFRRT에서 수행하는 절차는 개략적으로 다음과 같이 기술할 수 있다.

① 비행교범에 수록된 정상절차 검토
② 비행교범에 수록된 비상절차 검토
③ 이륙직후 비상 착륙절차 검토
④ FMEA(Failure Mode and Effect Analysis) 실시
⑤ THA(Test Hazard Analysis) 감소방안 검토
⑥ 임무여부 결정 기준(GO/NO-GO 기준) 검토
⑦ GMC(General Minimizing Consideration) 검토
⑧ TPWG(Test Plan Working Group)에 의한 비행시험 계획검토를 기술검토 위원회(TRM)에서 실시
⑨ SRB(Safety Review Board) 개최 및 Action Item 검토 등이다.

9. 맺음말

시스템 안전분야는 어떤 무기체계의 획득과정에서 중요한 부분을 차지하고 있으며, 이러한 시스템 안전 프로그램 임무를 효과적으로 수행하는데 유용한 지침을 제공하는 MIL-STD-882C의 중요성을 무기체계 개발과 관련된 모든 요원들은 인식해야 한다.

정부차원의 시스템 안전 담당자의 중요한 역할이란 방산업체 시스템 안전 담당자에게 어떻게 위험이 수용될 수 있는 수준에서 분석되고 제거되며, 통제되어야 하는가에 대한 견해를 제시하는 "기술적인 조언자(Sparring Partner)"인 점이며, 이러한 상호교류를 통해서만이 시스템 안전 프로그램은 보다 효과적으로 수행될 수가 있는 것이다. 항공기 개발 프로그램에 한정할 경우 시스템 안전의 궁극적인 목표는 성공적인 초도비행이라고 할 수 있다.

시스템 안전 프로그램을 운용하는데 있어 가장 최선의 유일한 방법은 없다고 생각되며 우리나라에서는 다소 생소한 개념인 시스템 안전분야(System Safety Engineering)가 향후 우리나라의 항공기 관련 개발계획에 적절히 적용되고 지속적으로 수행된다면, 궁극적으로 시스템 안전분야에 대한 비용대 효과는 상당할 것으로 확신한다.

참고문헌

(1) MIL-STD-882C, 1984, "System Safety Program Requirements," pp. 202-1～205-2, A-1～A-18.

(2) US Air Force Systems Command Design Handbook 1-6, "System Safety," Chapt 1～3.

(3) US Aeronautical Systems Division Pamphlet 127-1, 1981, "System Safety Program," pp. 6-1～10-4.

(4) US Aeronautical Systems Division, Pamphlet 800-18, "First Flight Readiness Certification by EIRT," pp. 3～8.

(5) Roland & Moriarty 1983, "System Safety Engineering and Management," John Wiley & Sons, pp. 3～30.

(6) Sol, W. Malasky, 1982, "System Safety," Garland STPM Press, pp. 71～117.

(7) Nedresky, D. L., 1987, "Implementation of a Naval Aircraft System Safety Program," *8th International System Safety Conference.*

(8) KEUNHYUN JOE, 1990, "Implementation of KTX-1 System Safety Program," Lockheed Aeronautical Systems Company, Gerogia, U.S.A. pp. 1～38.

(9) 조건현, 1991, "시스템 안전의 항공기 설계에의 응용," 국방과 기술, pp. 55～63.