論文

국내 개발 무기체계의 체계안전에 관한 연구

강자영*, 이상철**, 고상호**

System Safety of Domestically Developed Weapon Systems

Ja-Young Kang*, Sangchul Lee** and Sangho Ko**

ABSTRACT

The problem of establishing weapon system safety especially during the development process has been one of the very important fields related with public safety in advanced countries such as USA, UK and so on. These countries have launched strong policies on system safety to reduce the chance of accidents. However, the Republic of Korea (ROK) has limited experiences and application of the system safety on domestically produced weapon systems. Therefore, it is imperative that the government starts a comprehensive and systematic policy on system safety to reduce the occurrence of potential accidents during the development of weapon systems. In this paper, we analyze system-level activities needed through the life-cycle of the weapon systems and provide a suggestion for application of the system safety.

Key Words : 체계안전(System Safety), 무기체계(Weapon System), 체계공학(System Engineering), 획득 프로세스(Acquisition Process)

1. 서 론

연구개발 무기의 체계안전에 대한 문제는 미국, 영국 등 여러 선진국에서 오래 전부터 관심을 갖고 연구하는 공공의 안전에 관련된 중요한 분야이다. 각 정부는 무기체계의 사고로 인한 사망, 부상으로부터 개인 및 공중을 보호하고, 사고로 인한 파괴나 손상으로부터 무기체계, 장비, 재료 및 시설을 보호하기 위하여 노력을 기울이고 있다. 미 국방부는 군 내부 발생 사고를 조사하고 분석한 결과 항공기, 함정, 미사일 등과 같은 주요 무기체계 획득과정에서의 안전사고와 운영 중인 체계의 안전사고가 대부분 체계가 불안전함에 따라 발생하고 있다는 사실을 확인하였다[1]. 미국의 조사 결과를 고려할 때 연구개발 무기체계는 체계 불안전으로 인하여 사고가 발생할 확률이 매우 높다할 수 있겠다. 미국은 이러한 안전사고 발생확률을 줄이기 위해 강화된 체계안전 정책을 추진하는 것으로 보인다.

미국의 무기체계에 대한 안전성과 관련된 표준 및 지침으로 사용되는 문서인 MIL-STD-882D에 의하면 체계안전이란 “체계 수명주기의 모든 단계에 걸쳐 운용효과 및 적합성, 시간, 비용의 제한 범위 안에서 사고 위험성을 허용 가능한 수준으로 달성하기 위한 공학과 관리 원칙, 조건 및 기법의 적용”이라고 정의되며[2], 오늘날에는 체계안전은 군사표준에서 정의된 제약을 벗어나 더욱 확장되고 있는 실정이다.

현재까지 국내에서 무기 체계의 안전성과 관련된 적용사례는 1990년 대 이후 진행되고 있는 KT-1 기본 훈련기, T-50 고등 훈련기 및 기술 시범기 등과 같은 군용기 외에는 전무하며, 우리나라의 무기 체계 안전성에 관련 규격이나 지침은 아직 없는 상황이다[3].

2009년 6월 12일 접수 ~ 2009년 6월 24일 심사완료
* 한국항공대학교 항공운항학과
** 한국항공대학교 공과대학 항공우주 및 기계공학부
연락저자, E-mail : sanghoko@kau.ac.kr
경기도 고양시 덕양구 화전동 200-1

따라서 국내에서도 무기체계 연구 개발 시 안전사고 발생확률을 줄이기 위해 정부차원의 종합적이고 체계적인 체계안전 정책을 추진하는 것이 바람직하다. 이를 위해 본 연구에서는 앞으로 국내에서 개발될 군용항공기와 같은 무기체계의 체계 안전성을 위한 체계 안전 제도와 기준 그리고 체계안전 업무 절차의 국내 적용방안을 제시한다.

이를 위해 본 논문의 2장에서는 무기체계의 획득 프로세스와 체계공학에서의 주요한 활동사항에 대해 간략히 검토하고, 3장에서는 무기 체계의 각 수명주기 상에서의 단계별 안전 활동의 종류에 대해 분석한다. 4장에서는 추후 한국에서의 무기체계 안전성과 관련된 발전방향에 대해 기술한 후, 5장에서 결론을 맺는다.

2. 무기체계 획득 프로세스와 체계 공학 활동

2.1 무기체계 획득 프로세스

체계안전은 체계공학의 필수적인 하나의 프로세스이기 때문에 체계안전 활동 역시 체계공학의 단계별 활동과 보조를 맞춰 수행되어야 한다. 따라서 체계안전은 획득 프로그램의 여러 단계, 즉 탐색개발 단계, 체계개발단계, 생산 및 배치단계, 운용단계에 걸쳐 체계공학의 활동과 함께 추진되어야 한다.

각 국가 또는 기관마다 획득 프로그램의 전체 수명주기에 대한 단계구분과 이와 관련된 활동은 다소 차이는 있지만 근본적으로 유사하다. Fig. 1은 미국의 주요 국방체계에 대한 개정된 획득 프로세스를 보여주고 있다. DoD 5000 계열 문서는 프로세스를 좀 더 유연하게 하여 전투 수행자들에게 좀 더 신속하고 보유 비용이 저렴한 첨단 기술을 공급하기 위해 2000년도에 개정되었다.

프로세스 그 자체는 4개의 개발단계 즉, 개념 및 기술개발 단계, 체계개발 및 시연 단계, 생산 및 배치 단계, 유지 및 폐기 단계로 구성된다.

이러한 새로운 프로세스는 관련된 기본 기술의 성숙도에 따라 다수의 진입시점과 체계를 정의하고 개발하기 위한 진화적 방법의 사용을 권장한다. 이는 근본적 획득 및 공학관리에 맞춤식 접근법을 허용하면서도 체계공학 프로세스의 기본 로직을 변경하지는 않는다.

Fig.1 에서 진입 시점은 이정표(Milestone) A, B, C가 될 수 있다. 이정표 A는 개념 및 기술 개발단계의 시작점이고, 이정표 B는 체계 개발 및 시연단계의 시작점이고, 이정표 C는 생산 및 배치단계의 시작점을 의미한다.

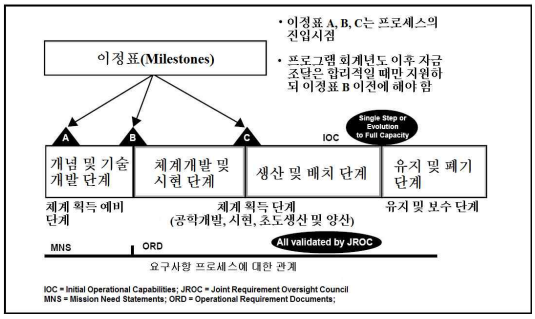

Fig. 1 개정된 DoD 5000 획득 프로세스

프로세스는 기술이 정의되어 실현 가능한 개념으로 성숙되고, 그 다음에 개발/생산되며, 생산된 체계가 현장에 배치되어 지원되는 일련의 단계들로 정의된다. 프로세스는 주어진 체계가 모든 개발단계의 과정에 진입하는 것을 허용한다. 예를 들어 증명되지 않은 기술을 사용하는 체계는 초기 단계의 프로세스에서 진입하여 장기간의 기술성숙을 통하여 진행될 것이고, 성숙되고 증명된 기술에 기초를 둔 체계는 직접 기술개발 및 생산단계로 진입할 수 있다.

본 연구에서는 탐색개발을 미 국방성에서 정의하고 있는 개념상세화단계와 기술개발단계로 세분하고, 체계개발단계에는 체계시연 부분을 추가하여 체계개발 및 시연 단계로 재정의하고, 운용단계 역시 지원 부분을 추가하여 체계 운용 및 지원단계로 재정의하여 각 단계별로 요구되는 체계안전의 필수요소 및 활동 등을 상세하게 분석하여 획득프로그램의 전 수명 주기에 걸친 체계안전의 문제를 파악하고자 한다. 마지막 항목인 운용 및 지원의 단계에 지원이 추가된 이유는 체계안전 활동이 수요자 관점의 체계운용과 관련된 부분과 개발자 또는 제작사 관점에서의 체계지원과 관련된 부분이 존재하기 때문이다.

2.2 체계공학 활동

체계는 명백히 규정된 필요 또는 목적을 충족시키기 위한 능력을 제공하는 인력, 제품 및 프로세스의 종합된 합성체로 정의될 수 있으며, 체계공학이란 “고객의 필요를 충족시키는 체계 솔루션들의 통합되고 수명주기에 걸쳐 균형된 집합을 진화시키고 검증하는 학제 간 공학적 관리 프로세스”라고 요약될 수 있다.

미 국방성의 DoD 5000.2-R[4]이 요구하는 체계공학의 프로세스는 다음과 같다.

- 운용상의 필요와 요구사항을 모든 수명주기상의

필요(즉, 개발, 제작, 시험평가, 검증, 전개, 운용, 지원 훈련 및 폐기)에 대해 일관된 고려를 통하여 통합된 체계 설계 솔루션으로 변환시켜야 한다.

- 모든 기능적 물리적 인터페이스의 적합성, 상호운용 및 통합을 확인하고, 체계 정의 및 설계가 모든 요소, 즉 S/W, H/W, 시설, 인력 및 자료들에 대한 요구사항을 반영하고 있는지를 확인해야 하며
- 기술적 위험성을 규명하고 관리해야 한다.
- 보안 취약성을 식별하고 관련된 정보 보증 및 군사력 보안 위험성을 최소화하기 위해 과학적, 공학적 원리들을 적용해야 한다.

이러한 목표들은 관리 개념 및 기술을 통하여 성취되어야 하며, 체계공학 관리는 획득 단계와 일치되어 적용되어야 한다. 이정표상의 결정을 지원하기 위하여 중요한 기술검토 활동이 체계 설계의 성숙도를 평가하기 위해서 수행되어야 한다.

이를 위하여 미 국방성은 다음과 같은 10개의 일반화된 기술검토 활동을 제시하고 있다. 그렇지만 모든 프로그램에서 반드시 모든 검토를 수행할 필요는 없다[5].

대안체계검토(Alternative Systems Review; ASR): 획득프로세스의 개념 및 기술개발단계의 개념탐색 동안에 수행되는 활동으로서 선호되는 체계 개념이 식별된 요구에 대한 비용 대 효과, 운용상 효과적이고 적합한 솔루션을 제공하는지 그리고 수용 가능한 위험성의 수준에서 솔루션을 적기에 제공하는지를 검토한다.

체계요구사항검토(System Requirement Review): 체계가 Fig. 1 의 이정표 B를 지나서 체계개발 및 시연 단계로 진행될 때 수행하는 것이 적합하며, 이 검토는 사용자 요구사항이 체계의 특정 기술요구사항으로 변환되고, 임계 기술이 식별되며, 요구된 기술시연이 계획되고, 위험성이 충분히 숙지되어서 완화계획이 준비되었는지를 확인한다.

체계기능검토(System Functional Review): 체계 기술설명서(기능적 베이스라인)에 의해 표현되는 체계의 기능적 요구조건들을 평가하고, 모든 요구된 체계 성능이 충분히 분류되어 기능 베이스라인에 충분히 정의되었는지를 확인하는 검토이다.

소프트웨어규격검토(Software Specification Review): 체계수준의 예비설계검토(PDR)를 준비하는 경우에, 할당된 베이스라인을 확립하기에 앞서 소프트웨어 품목의 설계와 개발을 안내하기 위한 기능, 성능, 인터페이스 및 기타 정보를 기술하는 소프트웨어 규격서를 검토한다.

예비설계검토(Preliminary Design Review): 이 검토는 체계의 각 품목 성능 규격서에 상응하도록 체계예비설계가 수행되었는지 평가하고, 기능 베이스라인의 각 기능이 하나 또는 그 이상의 체계 형상 품목 그룹에 할당되었는지 확인하며, 체계 개발 및 시연 단계에서 수행된다.

상세설계검토(Critical Design Review): 생산라인 구축에 앞서 생산될 품목의 세부사항에 대한 상호이해를 확인하고 공식화하며, 체계설계문서가 초도제작을 착수하기에 만족스러운지를 결정하기 위한 생산 베이스라인 초안을 평가한다.

시험준비검토(Test Readiness Review): 체계개발 및 시연 단계 동안에 수행되며, 시험 목적, 절차 및 자원들의 시험 협조를 평가한다. TRR이 완료되면 공식적인 형상품목의 시험이 개시된다.

생산준비검토(Production Readiness Review): 체계개발 및 시연 단계와 생산 및 배치 단계의 생산준비 동안 체계, 부체계 및 형상품목에 대한 생산준비가 완료되고, 포괄적이며, 조정되었는지를 결정하기 위해 개최된다.

기능적형상감사/체계검증검토(Functional Configuration Audit/System Verification Review): SVR을 통해 고객의 요구조건과 체계 및 부체계 기술성능설명서에 대한 관계를 재검사하고 검증하며, 생산된 체계가 규격서 시험계획서 등에 확립된 기술성능요구사항을 충족시킬 수 있는지를 결정한다. FCA는 규격서, 관련 시험계획서 및 기타 문서에 설정된 모든 요구사항들이 시험되었는지, 그리고 품목이 시험을 통과했고, 수정 조치가 취해졌는지를 검증한다.

물리적형상감사(Physical Configuration Audit): 규격서 및 기술자료 패키지(TDP)를 포함한 제품 베이스라인을 공식화함으로써 향후 변경사항이 전체 형상관리 절차를 통해서 이행될 수 있도록 해주며, 제품이 제품 베이스라인을 기술하고 있는 TDP와 일치하는지를 검증한다.

3. 체계 수명주기상의 단계별 안전 활동 분석

3.1 개념 상세화 단계

이 단계에서의 체계공학 소단계에 따른 체계안전 활동을 설명하면 다음과 같다.

① 사용자 요구사항을 숙지하고, 운용능력 및 환경 제약조건을 분석한다. 이 때 체계안전활동은 체계위협평가서를 검토해야 하고, 적용 가능한 체계안전 ESOH[1] 기준을 식별해야 한다.

② 개념성능 및 제약조건을 정의하고 검증 목표를

정한다. 이때 체계안전 활동은 식별된 체계 안전 기준에 대한 각 체계 개념을 평가해야 한다.

③ 개념성능을 기능적 정의 및 검증 목표로 분해한다. 이때 체계안전 활동은 개념 수준의 체계 안전 기준을 기능적 요구사항으로 전환해야 하며, 적용 가능한 검증 목표를 식별해야 한다.

④ 개념의 기능적 정의를 개념 컴포넌트와 평가 목표로 분해한다. 이때 체계 안전 활동은 예비위험목록(PHL[2]) 작성을 개시해야 하며, 역사적 자료(예: 성공, 위험, 교훈 등)를 검토해야 한다.

⑤ 컴포넌트 개념, 즉 능력실현/임계 기술(enabling[3] /critical technologies[4]), 제약조건 및 비용/위험성 견인 인자를 찾아낸다. 이때 체계안전 활동은 PHL을 갱신해야 하고, 컴포넌트 제약조건의 식별작업을 시작하며 계획된 체계 감소율로 입력을 권고한다.

⑥ 능력실현/임계 컴포넌트 대 능력을 분석하고 평가한다. 이때 체계안전 활동은 임계 컴포넌트 능력에 대한 체계 요구사항을 식별해야 하고, 식별된 체계 제약조건에 대한 컴포넌트 시험결과를 평가해야 한다.

⑦ 체계개념 대 기능적 능력을 분석하고 평가한다. 이때 필요한 체계안전 활동은 컴포넌트 시험 결과에 근거하여 체계개념에 대한 체계안전 기능 요구사항을 평가해야 한다.

⑧ 개념을 평가/분석하고, 체계개념의 성능을 검증한다. 이때 필요한 체계안전 활동은 식별된 안전 제약조건 내에서 성능능력 요구사항을 충족시키기 위한 체계개념의 능력을 평가해야 한다.

⑨ 개념 대 정의된 사용자 요구 및 특정 환경제약조건을 분석하고 평가한다. 이때 필요한 체계안전 활동은 각 체계 개념에 대한 PHL을 마무리해야 하고, 체계개념에 대한 선호하는 접근 방법을 추천해야 한다.

3.2 기술개발 단계

이 단계에서의 체계공학 소단계 및 이에 대응하는 체계안전 활동을 설명하면 다음과 같다.

① 사용자 요구사항을 파악하고, 운용능력 및 환경제약조건을 분석한다. 이때 필요한 체계안전 활동은
- 체계안전 제약조건의 식별을 갱신해야 한다.
- 안전기준을 개발해야 한다.
- ESOH가 중요한 기술의 필요성을 식별해야 한다.

② 체계성능 규격과 능력실현/임계 기술 및 검증계획을 개발한다. 이때 필요한 체계안전 활동은
- 체계안전기준을 갱신해야 한다.
- 검증계획에 체계안전이 중요한 규격을 포함시켜야 한다.

③ 능력실현/임계 기술 및 관련 검증 계획에 대한 기능적 정의를 개발한다. 이때 필요한 체계안전 활동은
- 체계안전기준을 갱신해야 한다.
- 위험성완화관리를 검증하기 위한 요구사항을 개발해야 한다.

④ 기능적 정의를 임계 컴포넌트 정의 및 기술 검증계획으로 분해한다. 이때 필요한 체계안전 활동은
- 체계안전 기준을 최신화해야 한다.
- 컴포넌트 위험성 완화 관리의 검증을 위한 요구사항을 개발해야 한다.

⑤ 체계개념, 즉 능력실현/임계 기술을 개발하고, 제약조건 및 비용/위험성 유발 요인을 갱신한다. 이때 필요한 체계안전 활동은
- PHL을 최신화해야 한다.
- 제약조건을 최신화해야 한다.
- 잠재적 운용/유지보수 훈련 및 요원 요구사항들을 식별해야 한다.
- 체계 감소율에 대한 입력을 상세화해야 한다.

⑥ 능력실현/임계 기술 컴포넌트 대 계획을 시연한다. 이때 필요한 체계안전 활동은
- 체계안전의 관점에서 능력실현/임계 기술을 평가해야 한다.
- 새로운 기술 컴포넌트 위험에 대한 시연 결과를 검토해야 한다.

⑦ 체계 기능 대 계획을 시연한다. 이때 필요한 체계안전 활동은
- 체계안전관점에서 능력실현/임계 기술을 평가해야 한다.
- 새로운 위험에 대한 시연결과를 검토해야 한다.

⑧ 통합체계 대 성능규격을 시연하고 모델링 한다. 이때 필요한 체계안전 활동은

---

1) Environmental Safety and Occupational Health(환경안전 및 직무 보건)

2) Preliminary Hazard List

3) 능력실현기술(Enabling Technology): 다른 공학설계가 경제적으로 실용적이거나 가능하게 하는 일련의 기술

4) 군사적임계기술(Militarily Critical Technology): 미국방성이 미군의 우월한 능력을 유지하는데 결정적인 것으로 평가하는 기술. 이 기술들의 일부를 잠재적 대항자가 획득하게 되면 대항국의 군수산업 능력은 심각하게 증대되나 상대적으로 아국의 안보관계는 저하됨(예: 화생방 무기 및 유도발사시스템의 확산과 관련된 기술 등이 이에 속함)

- 체계안전의 관점으로부터 능력실현/임계 기술을 평가해야 한다.
- 새로운 위험에 대한 시연/모델 결과를 검토해야 한다.

⑨ 체계개념 및 기술 성숙도 대 정의된 사용자 요구를 시연하고 검증한다. 이때 필요한 체계안전 활동은
- 체계안전의 관점에서 능력실현/임계 기술을 평가해야 한다.
- 새로운 위험에 대해 시연결과를 검토하고, 모델결과를 검증해야 한다.

3.3 체계개발 및 시연 단계

이 단계에서의 체계공학 소단계 및 이에 대응하는 체계안전 활동을 설명하면 다음과 같다.

① 사용자의 요구를 해석하고, 체계성능규격 및 환경제약조건을 상세화 한다.
- 체계안전은 수명주기 환경 프로파일과 체계의 경계를 개발해야 한다.
- 좀 더 상세한 체계안전 기준을 개발해야 한다.
- 비군사화/폐기계획에 대한 입력을 제공해야 한다.
- 체계 안전이 중요한 요구사항들을 식별하고 개발해야 한다(예: 안전요구사항/기준요구사항 분석서[SRCA[5]]를 갱신해야 한다.)
- 체계안전이 중요한 요구사항들이 요구사항 추적 체계에 포함되었는지 검증해야 한다.

② 체계기능규격 및 체계검증계획을 개발한다.
- 체계안전은 예비위험분석서(PHA[6]) 개발에 착수해야 한다.
- 위협위험평가(THA[7])를 시작해야 한다.
- 체계안전기준을 갱신해야 한다.
- 비군사화/폐기계획을 위한 갱신된 입력을 제공해야 한다.
- SRCA에 기능규격을 포함시킨다.
- 체계안전이 중대한 기능규격들이 요구사항추적체계에 포함되었는지 검증해야 한다.
- 체계검증계획서에 체계안전이 중대한 규격을 포함시켜야 한다.

③ 기능적 성능규격을 형상항목(CI[8]) 기능적 규격 및 CI 검증계획으로 발전시킨다.
- 체계안전은 예비위험분석(PHA)을 마무리하고, 적정한 부체계 위험분석(SSHAs[9])의 개발에 착수해야 한다.
- 위협위험분석(THA)을 마무리 한다.
- 체계안전기준에 시험 요구사항(컴포넌트, 부체계)을 포함시켜야 한다.
- 비군사화/폐기계획을 위한 갱신된 입력을 제공해야 한다.
- SRCA를 확장하고 갱신해야 한다.
- 체계안전이 중요한 설계규격서가 요구사항추적체계 및 상세설계규격에 포함되었는지를 확인해야 한다.
- 체계안전이 중요한 규격을 CI 검증계획에 포함시켜야 한다.

④ CI기능규격을 제품생산문서(Product Build to Documentation) 및 검사계획서로 발전시킨다.
- 체계안전은 SSHAs를 마무리한다.
- 체계위험분석(SHA) 및 운용지원위험분석서(O&SHA[10]) 개발에 착수한다.
- 체계안전기준이 시험검사요구사항들(컴포넌트, 부체계, 체계)을 포함하도록 갱신해야 한다.
- 비군사화/폐기계획을 위한 갱신된 입력을 제공해야 한다.
- 제품생산문서를 위한 체계안전이 중요한 프로세스를 식별해야 한다(예: 안전이 중요한 항목 목록).
- 체계안전이 중요한 프로세스 및 컴포넌트들을 검사계획서(예: 컴포넌트 선정 및 시험)에 포함시켜야 한다.
- 체계안전분석을 이용하는 컴포넌트 설계 선정에 참여해야 한다.
- 필요에 따라 SRCA를 확장하고 갱신해야 한다.
- 체계안전이 중요한 설계규격이 요구사항추적체계 및 상세설계규격에 포함되었는지를 확인해야한다.

⑤ 제작문서에 따라 제작, 조립, 코딩한다.
- 체계안전은 필요에 따라 프로세스 및 설계변경을 평가해야 한다.
- 체계안전분석에 기초하여 시험평가종합기본계획(TEMP)에 대한 갱신내용을 검토하고 추천해야 한다.
- CI검증 개발시험평가(DT&E[11]) 절차들이 안전요구사항 및 검증시험을 포함하고 있는지를 보장해야 한다.

5) Safety Requirements Criteria Analysis
6) Preliminary Hazard Analysis
7) Threat Hazard Assessment
8) Configuration Item
9) Subsystem Hazard Analysis
10) Operating and Support Hazard Analysis
11) Development Test and Evaluation

- 안전해제문서의 작성을 시작해야 한다.

⑥ 개별 CI검증 개발 시험평가(DT&E): 이때 체계안전은 다음과 같은 활동을 해야 한다.
- 안전시험이 수행되었는지 확인하고, 위험통제 효과에 대한 시험결과를 검토해야 한다.
- 위험의 상태를 갱신한다.
- 종합개발시험평가, 실사격 시험평가(LFT&E[12]) 및 조기운용평가(EOA[13]) 절차들이 체계안전분석을 통하여 유도된 적절한 시험을 포함하는지를 검증해야 한다.
- 개발시험평가 시험결과를 적정한 것으로 추천해야 한다.
- 안전해제문서를 적정한 것으로 제공해야 한다.

⑦ 종합 개발시험평가(DT&E), 실사격 시험평가(LFT&E) 및 조기운용평가(EOAs)는 규격서에 성능준수를 검증한다. 이 때 체계안전은 다음과 같은 활동을 해야 한다.
- 안전시험들이 수행되었는지를 확인하고, 위험통제효과에 대한 시험결과를 검토한다.
- 위험상태를 갱신한다.
- 형상변경에 기초하여 위험분석을 갱신한다.
- 필요에 따라 시험에 대한 형상변경을 평가하고, 결과(예: 안전평가)를 문서화 한다.
- 비군사화/폐기계획을 위한 갱신된 입력을 제공한다.
- 체계 DT&E, LFT&E 및 EOA 절차들이 체계안전분석을 통하여 도출된 적절한 시험을 포함하고 있는지를 검증한다.
- 시험결과에 기초한 위험종료를 추천한다.
- 다가오는 시험활동에 대한 안전면제를 적당하게 제공한다.

⑧ 체계개발시험평가, 실사격 시험평가 및 운용평가는 규격에 대한 체계 기능 및 제약조건 준수를 검증한다. 이때 체계안전은 다음과 같은 체계안전 활동을 해야 한다.
- 체계시험들이 수행되었음을 확인하고, 위험통제효과를 위한 시험결과를 검토한다.
- 위험상태를 갱신한다.
- 형상변경에 기초한 위험분석을 갱신한다.
- 필요에 따라 시험을 위한 형상변경을 평가하고, 결과(예: 안전평가)를 문서화한다.
- 결합된 DT&E/OA/LFT&E 절차들이 체계안전분석을 통하여 유도된 적절한 시험을 포함하는지를 검증한다.
- 적정하게 시험결과에 기초하여 위험종료를 추천한다.
- 적정하게 다가오는 시험활동에 대한 안전해제를 제공한다.

⑨ 결합된 개발시험평가, 운용시험평가, 실사격 시험평가는 특정 사용자 요구 및 환경 제약조건에 대한 체계를 시연한다. 이때 체계안전은 다음과 같은 활동을 해야 한다.
- 체계시험들이 수행되었는지 확인하고, 위험통제효과에 대한 시험결과를 검토한다.
- 위험상태를 갱신한다.
- 형상변경에 기초한 위험분석을 갱신한다.
- 적정하게 시험결과에 기초한 위험종료를 추천한다.

3.4 생산 및 배치 단계

생산 및 배치단계에서의 체계활동의 소단계 및 이에 대응하는 체계 안전 활동을 설명하면 다음과 같다.

① 수정 활동을 결정하기 위해 결점을 분석한다. 체계안전은 다음과 같은 활동을 해야 한다.
- 체계안전 연계에 대한 결점보고서를 검토하고, 수정 활동의 개발에 참여한다.
- 기술 변경 제안서(ECPs[14])를 검토하기 위한 형상변경위원회에 참여한다.

② 결점을 수정하기 위한 형상(HW/SW/규격)을 수정한다. 체계안전은 다음과 같은 활동을 해야 한다.
- 체계안전이 중요한 항목 및 검사 요구사항을 식별한다.
- 체계안전분석에 기초하여 시험평가종합계획에 대한 갱신내용을 검토하고 추천한다.
- 적정하게 안전해제문서를 제공한다.

③ 생산 형상을 검증한다(V&V). 이때 체계안전은 다음과 같은 활동을 해야 한다.
- 체계안전이 중요한 항목형상을 검증한다.
- 적정하게 시험활동에 참여한다.

④ 운용시험준비 검토회의(OTRR[15]): 체계활동은 안전해제를 제공하기 위한 사업책임자(PM)의 요구사항을 지원하기 위해 안전평가보고서(SAR)를 갱신해야 한다.

⑤ 물리적 형상감사(PCA): 체계안전은 잠재적 체계안전 연계를 식별하기 위한 PCA를 검토해야 한다.

12) Live Fire Test and Evaluation
13) Early Operational Assessment
14) Engineering Change Proposal
15) Operational Test Readiness Review

3.5 운용 및 지원 단계

운용 및 지원 단계의 체계활동의 소단계 및 이에 대응하는 체계 안전 활동을 설명하면 다음과 같다.

① 모든 서비스 이용 데이터를 감시하고 수집한다. 이때 체계안전은 다음과 같은 활동을 해야 한다.
- 기술 및 병참 인력에게 체계안전 검토 기준을 제공한다.
- 체계안전 연계에 대한 데이터(예: 경향분석)를 검토한다.
- (신규 또는 노후 기술)의 위험성을 줄이기 위한 기술적용의 기회를 확인한다.

② 근본 원인을 결정하기 위한 데이터를 분석한다. 이때 체계안전은 다음과 같은 활동을 해야 한다.
- 근본원인(예: 실패모드, 효과 및 치명성 분석[FMECA[16)]], 고장계보분석[FTA[17)]])을 결정하기 위한 적정한 체계안전분석기술을 적용한다.
- 체계안전연계를 위한 데이터를 평가한다.
- 위험분석/데이터베이스를 적정하게 갱신한다.

③ 체계위험성/위험심각도를 결정한다. 이때 체계안전은 다음과 같은 활동을 해야 한다.
- 위험성 완화를 위한 위험의 우선순위를 정한다.
- 위험성 분석/데이터베이스를 적정하게 갱신한다.

④ 수정 활동을 개발한다. 이때 체계안전은 다음과 같은 활동을 해야 한다.
- 수정 활동에 대해 선행체계안전훈령을 적용한다.
- 위험분석/데이터베이스를 적정하게 갱신한다.
- 갱신된 체계안전분석에 기초하여 위험성 완화 방법을 위한 요구사항을 식별한다.

⑤ 수정 활동을 종합하고 시험한다. 이때 체계안전은 다음과 같은 활동을 해야 한다.
- 위험성 완화효과에 대한 시험결과를 평가한다.
- 위험성 분석/데이터베이스를 적정하게 갱신한다.

⑥ 개선된 체계의 위험성을 평가한다. 이때 체계안전은 다음과 같은 활동을 해야 한다.
- 위험성 분석/데이터베이스를 적정하게 갱신한다.
- 해당 위험성 승인 당국에 위험 종료를 권고한다.

⑦ 이행 및 처리: 체계안전은 체계보건, 사고, 위험, 종료행위, 완화방법효과 및 잔존 위험성을 계속 추적해야 한다.

⑧ 현장검토: 이때 체계안전은 다음과 같은 활동을 해야 한다.
- 사고에 대한 현장 검토에 입력을 제공한다.
- 위험성 평가, 선택된 완화 방법, 완화 통제의 검증, 잔존 위험성의 승인 새로이 식별된 위험에 관한 현장 검토에 입력을 제공한다.

⑨ 절충연구: 이 단계를 통하여, 체계안전은 수립된 체계안전기준에 대한 선택사항을 평가하기 위한 절충연구에 참여해야 한다.

16) Failure Mode, Effects, and Criticality Analysis
17) Fault Tree Analysis

4. 체계안전 및 업무절차의 적용 방향

미국의 경우와 같이 방위사업법 시행령 및 시행규칙 하에서 방위사업청 훈령(방위사업 관리규정)을 통하여 체계안전 제도를 구축하는 방안과 영국의 경우와 유사하게 산업안전보건법을 통하여 체계안전제도를 정립하는 방안이 있다. 어느 경우든 공히 법적 근거에 따른 훈령 및 규정을 통하여 체계안전에 대한 제도를 구축하는 것이 필요하다.

체계안전 기준은 미국의 MIL-STD-882(체계안전을 위한 표준 실행)를 준용하여 체계안전을 위하여 해야 할 사항(what)을 우선 규정하도록 하고 어떻게(how)수행하느냐 하는 문제는 단계적으로 발전시키도록 하는 것이 바람직하다. 앞에서 언급한 바와 같이 체계안전은 체계공학 업무에 반드시 포함되어야 한다.

새롭고 복잡한 무기체계의 출현으로 경험하지 못한 잔존 위험성은 증대되고 있는 추세이며, 미국의 경우 2003년 5월 DoD에서 사고 예방을 위한 방위체계 안전 감독위원회(Defense Safety Oversight Council)가 구성되어 관련 업무를 추진하고 있다. 향후 환경문제와 직무보건 문제의 중요성이 강조될 것을 고려하여 환경, 안전, 직무관련 보건(ESOH) 등을 종합적으로 평가할 수 있는 정책 및 지침을 마련하여 방위 획득체계에 반영하는 것이 필요하다.

체계안전을 위해서는 개개의 개발사업을 체계안전의 기준에 따라 수행하는 것도 중요하지만 전체 개발사업의 체계안전 계획, 체계안전 평가 리포트 등의 자료를 잘 관리하여 국가적 차원에서 데이터베이스를 구축하는 것이 반드시 필요하다 하겠다. 체계 공학 프로세스와 대응된 각 단계별 체계 안전 업무활동은 2절 및 3절에 설명된 내용을 기준으로 각각의 무기 체계 개발 사업에 맞도록 수정하여 적용하는 것이 타당할 것으로 사료된다.

5. 결 론

본 논문에서는 국내에서 연구개발한 무기 체계에 대한 체계 안전 문제를 체계 공학적 측면에서 검토해 보았다. 체계공학 그 자체가 체계의 신뢰성과 안전성을 보장하는 수단으로 어느 정도 활용되고 있기는 하지만 현재까지 무기체계에 대한 체계공학은 체계의 안전문제 보다는 체계의 설계, 제작 및 시험 등 기술개발에 초점이 맞추어져 있었다. 그리고 안전은 개발이 종료되어 현장에 배치된 후 운용 측면에서 다시 강조되고 있는 실정이다.

서론에서 언급했듯이 국내에서 무기 체계의 안전성과 관련된 적용사례는 1990년대 이후 진행되고 있는 KT-1, T-50 및 기술 시범기 등에서 찾아볼 수 있으나 아직도 전체 무기 체계에 대한 체계안전 규격이나 지침들이 폭넓게 개발되어 있지 않다. 무기 체계 개발 시 체계의 전체 수명주기 상에서 조우될 수 있는 안전 문제를 심도 있게 분석 예측하지 못하면 개발시험, 현장배치 및 운용 폐기에 이르기까지 관련된 환경, 안전 및 직무보건의 문제가 소홀해 질 수 있다.

특히 요즘에는 체계의 폐기에 이르기 까지 충분한 운용경험이 없는 새로운 무기 체계들을 개발하여 운용하는 경우가 많아서 이들 중에 운용 시 발생할 수 있는 잠재적 위험 요소가 내재되어 있을 수가 있다. 또한 최근 들어 무기체계는 하드웨어에 비해 소프트웨어의 비중이 점점 커지고 있는데, 이들은 복잡할 뿐만 아니라 정확하게 구현되지 않을 경우 운용 중에 치명적 결과를 초래할 수 있다. 소프트웨어 체계의 안전문제는 설계단계에서부터 미리 충분히 분석하고 또한 운용 중에도 계속 검토함으로써 내재해 있는 위험 요소들을 식별하고 위험성을 수용할 수 있는 수준으로 통제할 수 있다.

따라서 국내개발 무기체계의 안전 문제는 앞에서도 언급한 바와 같이 개념 상세화 단계에서부터 운용, 폐기 단계에 이르기까지 체계의 전 수명주기에 걸쳐 체계 공학적 접근이 필요하다. 즉 지금까지 체계의 기능 및 성능에 중점을 둔 체계공학에 안전의 문제를 포함시켜야 할 것이다. 이를 위하여 앞에서 예로 제시한 체계의 수명주기 단계별 안전 활동은 물론 시스템 요구사항에 환경, 안전, 직무건강(ESOH)에 대한 요구사항을 충분히 분석하여 포함시켜야 하며, 이 요구사항들에 대한 준수 방법(Compliance Methods) 및 평가 방법 등도 개발되어야 할 것이다.

참고문헌

1) Joseph J. Angello, Jr. "Secretary Rumsfeld's Mishap Reduction Initiative,"

2) MIL-STD-882D, Standard Practice for System Safety, USA Department of Defense

3) 정나현, 임상수, 주현준, "체계 안전성 국내 적용 사례 및 발전 방향," 2008 항공우주무기체계 발전세미나

4) DOD 5000.2-R, Mandatory Procedures for Major Defense Acquisition Programs (MDAPS) and Major Automated Information System (MAIS) Acquisition Programs, April 5, 2002.

5) System Engineering Fundamentals, Defense Acquisition University Press, 2001.