J. Korea Saf. Manag. Sci. Vol. 17 No. 1 March 2015
http://dx.doi.org/10.12812/ksms.2015.17.1.75

ISSN 1229-6783(Print)
ISSN 2288-1484(Online)

무기체계 실사격 시험의 안전성 강화를 위한 다중 사건나무분석 기반의 시험구조에 관한 연구

예 성 혁* · 이 재 천**
*국방과학연구소 제8기술연구본부 · **아주대학교 시스템공학과

On Multiple ETA-based Test Framework to Enhance Safety Maturity of Live Fire Tests for Weapon Systems

Sung Hyuck Ye* · Jae-Chon Lee**
*Defense Systems Test Center, Agency for Defense Development
**Dept. of Systems Engineering, Ajou University

Abstract

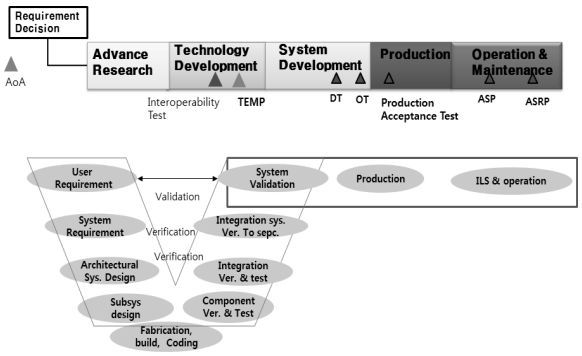
Successful development of weapon systems requires a stringent verification and validation (V&V) process due to the nature of the weapons in which continual increase of operational capability makes the system requirements more complicated to meet. Thus, test and evaluation (T&E) of weapon systems is becoming more difficult. In such a situation, live fire tests appear to be effective and useful methods in not only carrying out V&V of the weapon systems under development, but also increasing the maturity of the end users operability of the system. However, during the process for live fire tests, a variety of accidents or mishaps can happen due to explosion, pyro, separation, and so on. As such, appropriate means to mitigate mishap possibilities should be provided and applied during the live fire tests. To study a way of how to accomplish it is the objective of this paper. To do so, top-level sources of hazard are first identified. A framework for T&E is also described. Then, to enhance the test range safety, it is discussed how test scenarios can be generated. The proposed method is based on the use of the anticipatory failure determination (AFD) and multiple event tree analysis (ETA) in analyzing range safety. It is intended to identify unexpected hazard components even in the environment with constraints. It is therefore expected to reduce accident possibilities as an alternative to the traditional root-cause analysis.
Keywords : Range Safety, Test Scenario, Live-fire Test, ETA, AFD

1. 서 론

무기체계 연구개발은 국가 전략에 따라서 수행되는 정부 주도의 대형 프로젝트로서 천문학적인 비용이 투입되고, 장기간의 개발 기간과 개발 후 수십 년의 수명주기를 가짐으로서 신뢰성이 확보되고 이해당사자들의 의사결정과정에서 생성된 다양한 요구사항이 충족되어야 하는 복잡하고 대형화된 시스템 개발 과정을 가지고 있다.

†이 논문은 2014년도 정부(미래창조과학부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업임(No. NRF-2012R1A1A2009193)
†Corresponding author: Prof. Jae-Chon Lee, Dept. of Systems Engineering, Ajou University, Wonchon-dong, Youngtong-gu, Suwon, 443-749.
Tel: 031-219-3941, E-mail: jaelee@ajou.ac.kr
Received January 20, 2015; Revision Received March 15, 2015; Accepted March 16, 2015.

개발과정 초기의 최종 사용자인 소요군(軍)을 중심으로 도출된 사용자의 개념적 요구사항을 상세 요구사항으로 개발하는 개념설계부터 최종적 전력화 여부를 판단하기 위한 성능검증 단계에 이르기까지 사용자 요구조건 만족을 위한 성능 검증방안이 수립되어야만 하며, 검증방안은 시험 요구조건과 연계된다. 대형화되고 고도화된 무기체계는 국내외 연구개발 사례에서 군 전력화를 위한 양산 과정에서 지연요소가 식별되어 적기 전력화가 문제가 발생하고 있다. 이러한 주변 환경 변화는 초기 개념 설계시 도출된 사용자 요구사항의 만족여부를 판별하기 위한 시험평가의 중요성이 한층 더 부각되고 있다. 운용환경을 고려한 전투 성능평가에 적용하는 실사격 시험(Live-Fire Test)은 무기체계 특성상 폭발, 발사, 분리, 기계적 거동 등 많은 위해 요소를 포함하고 있다. 무기체계 수명주기 측면에서 개발기간 이외에 운용 단계에서도 성능검증 및 훈련을 위한 시험과 양산품의 성능 보증, 장기 저장품의 신뢰도 확인 목적으로도 지속적으로 실사격 시험이 수행되며, 소수이기는 하지만 외국에서 도입한 무기체계에 대한 성능시험도 수행되어야 한다. [Figure 1]은 한국의 무기체계 획득 수명주기와 시스템 공학 기반의 V-model에 대한 주요 실사격 시험 수행 단계를 나타낸 것이다.



[Figure 1] A comparative view of the two life-cycle models for weapon systems development: the defense aquisition model in Korea and the popular V-model.

무기체계 시험평가는 실사격 시험이 가진 잠재된 위험성을 수용하고 공신력과 신뢰성 있는 자료 제공을 위하여 전 세계적으로 국가 소유 또는 국가 공인시험장에서 수행하고 있으며, 최근에는 무기체계의 첨단화, 전략 · 비닉성 증가로 따라서 과거에 재래식 무기체계 운용 환경에 비하여 시험체계 구성이 복잡화되고 대형화되고 있다. 시험 비용의 증가와 준비 기간등을 고려할 때 효율적이고 효과적인 연구개발 사업 수행을 위하여 무기체계 연구개발과 함께 시험평가 분야에서도 시스템 공학 요소를 결합하여 체계적인 시험 수행을 위하여 노력 중에 있다[1,2]. 실사격 시험은 시험 수행 중에 오작동 및 예기치 않는 현상으로 인하여 시험을 수행하는 시험장 내부 인력과 시설 및 인근 거주민들까지 시설에 대한 손상 뿐 아니라 인명 손상과 같은 치명적인 위해가 발생할 수 있으므로 시험 수행 체계는 안전을 최우선으로 고려한 안전중시 시스템으로 구성되어야 하며, 안전 제약사항과 시험 요구사항을 기반으로 시험 수행체계를 설계하고 구성해야만 한다.

예측할 수 있는 위험 요소를 관리를 위한 안전적 측면과 시험 요구에 따른 기능적인 요소의 검증이 제대로 이루질 수 있도록 체계적인 관리와 추적성을 확보한 시스템 공학적인 방법을 사용한 시험 아키텍처 설계가 전제되어야만 예측되는 사고의 저감과 사고 발생시 대처할 수 있는 사고 시나리오 구성시 무결성을 확보할 수 있을 것이다.

사고는 발생 단계, 사고 원인, 조치 대응 시간에 따라서 사후 결과가 전혀 다른 방향을 발생할 수 있음으로 시험 수행시의 대처 방안을 제시하는 사고 시나리오 구성에 따라서 결과의 파급효과는 전혀 다른 방향으로 전개될 수 있다. 모든 경우의 수에 대하여 사고 시나리오를 구성하여 검토하는 것은 비효율적일 뿐 아니라 설계과정이 길어짐에 따라서 효율적인 설계를 통한 시험 수행 주기 단축과 비용 절감과는 다른 결과를 도출할 수 있음으로 사고 시나리오 구성에도 경험을 바탕으로 한 정성적인 접근과 다른 정량적인 예측이 가능한 체계적인 접근이 필요하다.

본 논문에서는 주요 사고원인들을 시스템을 구성하는 자원 중심으로 식별하기 위하여 근본원인분석(Root Cause Analysis)인 FMEA(Failure Mode and Effect Analysis)나 HAZOP(Hazard and operability) 등 전통적인 위험 예측방식을 대신하여 AFD(Anticipatory Failure Determination) 개념을 이용, 사고 위험을 투입 자원 중심으로 고려하여 사고 시나리오를 구성하고, 사고 위험의 정량적 판단을 위해 다중 사건나무기법(Event Tree Analysis)을 적용, 사고 시나리오의 정량적 위험치를 제시하여 기존 경험 중심의 정성적인 사고 시나리오 구성을 개선, 정량적인 예측값을 제시할 수 있는 개선된 시나리오 구성방안을 제시하고자 한다.

논문의 구성은 다음과 같다. 서론에서는 연구 배경에 대하여 기술하였으며, 2장에서는 무기체계 연구개발 시험평가의 위험도 분석과 관련된 선행연구 분석과 문제정의 및 연구목표를 기술하고, 3장에서는 시험 시나리오 구성을 위한 위험도 분석과 연구 방안, 적용 사례 등 정량적인 시험 방안을 4장에서는 도출된 사고 시나리오의 논리적 검증을 위한 전산 도구를 위한 시나리

ISSN 1229-6783(Print)
ISSN 2288-1484(Online)

오 구성을 마지막 5장에서는 본 논문의 결과를 정리 요약하였다.

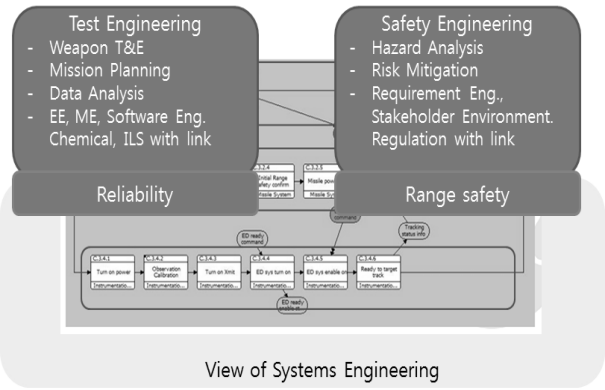
2. 문제 정의

2.1 안전중시 시스템

안전중시 시스템이란 인명손상이나 환경에 대한 치명적인 영향을 미칠 수 있는 시스템으로서 의료기기, 비행 통제, 무기체계, 핵발전소 등을 그 예로 들 수 있다 [3,4]. 광역 범위로 고려할 때, 119 서비스, 수도/전기 공급망 등 인프라 구축 시설도 그 피해 정도를 고려할 때, 안전중시 시스템으로 간주할 수 있다.

안전중시 시스템으로서 무기체계 시험장에서의 시험 절차를 수립하기 위해서는 시험 설계시 안전요소가 반영되어야 하며, 효과적인 시스템 구축을 위한 시스템 공학 기반의 프레임워크를 구성해야만 한다[5,6].

[Figure 2]는 시스템 공학 기반의 안전 중시 시스템으로서 전통적인 공학기반 중심의 시험공학과 안전공학과 같이 서로 다른 분야의 연계성을 고려하여 무기체계 시험의 시스템 아키텍처 개념을 제시한 것이다.



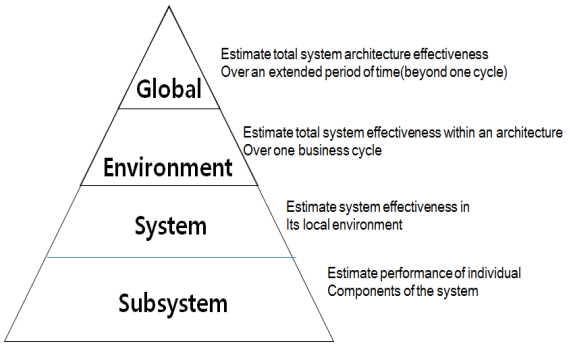
[Figure 2] A view on systems engineering in connection with interaction of test and safety engineering.

무기체계 실사격 시험을 수행하는 시험장(Test Range)에서는 발생할 수 있는 사고 방지를 위하여 위험 식별 및 위험 완화 조치를 수행하고 있다 [7,8,9]. 미국 등 선진국에서도 신개념 무기체계나 새로운 무기체계에 대한 위험 식별과 위험 완화방안에 대한 연구가 수행되고 있으며, 무기체계 운용 환경을 고려하여 시험평가계획서 작성 지침에 새로운 무기체계 또는 우주 발사체 등과 같이 고가의 시험비용을 수반하는 시험 설계시 고려사항을 제시하고 있다 [7].

시험장의 안전지침은 인명 피해의 최소화가 아닌 인명 피해의 가능성을 원천적으로 차단하는데 있다. 요구 시험에 대한 시험수행 가능여부는 시험에 잠재된 위험에 대한 통제 가능여부에 따라서 결정된다. 실사격 시험시 요구되는 안전 반경이란 비정상 상태 또는 기상 등 외적인 현상에 따라서 시험이 강제적으로 종료될 때, 최소한의 피해 반경을 의미하는 것으로서 무기체계의 개발시 요구성능 검증 방안에 따라서 변화될 수 있음으로 시험 의뢰자가 시험 요구 또는 시험 설계 협의시 안전반경에 대한 정보를 같이 제공해야만 한다. 이와 함께 시험 의뢰자는 시험에 위험성을 높이는 각종 위험 잠재 요인들도 제공해야만 한다.

2.2 연구개발 단계의 시나리오

무기체계 연구 개발에서 시나리오(scenario)는 다양한 의미로 사용될 수 있다. 개념 설계 단계에서 사용자 요구(user needs)를 기능적 또는 성능 요구조건을 도출하고 전장에서의 운용 개념을 고려하여 생성하는 시나리오는 운영 시나리오라고 정의한다. 운용 환경이 보다 상세화되고 이에 따른 시험 검증을 위하여 시나리오는 변화되는 데 이와 같이 개발 시스템의 시험 범위에 따라서 시나리오의 정의 분류를 [Figure 3]에 제시하였다. 본 연구에서는 개발 검증단계에서의 체계 효과도 분석과 부품의 성능해석을 위한 무기체계 개발시험 및 운용시험에서 사용하는 실사격 시험 시나리오 중심으로 기술하고자 한다.

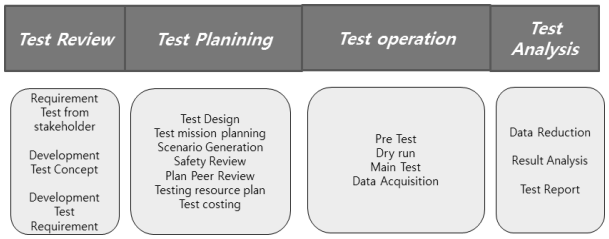


[Figure 3] Hierarchy of a test scenario [10].

2.2 시험시나리오 구성

참고문헌[2]에서 제시한 바와 같이 무기체계 시험은 시험 검토(Test review), 시험 준비(Test Planning), 시험 수행(Test Operation) 그리고 산출물 제시 전 검토를 위한 시험결과 분석(Test Analysis)의 단계

등 총 4단계로 구성된다. [Figure 4]는 이를 제시한 것이다.



[Figure 4] Live fire test procedure for weapon systems development V&V.

시나리오 작성은 시험검토 및 시험 준비단계에서 수행되는데, 일반적인 시험 시나리오는 아래와 같은 항목을 포함하고 있다.

- 투입 인원 및 장비 점검
- 시험 전 준비 통신 상태 확인
- 시험 진행 상태 안내
- 안전 통제 점검
- 시험 준비 시각 안내
- 중요 단계 안내
- 시험 종료 선언

시험 시나리오에서 비정상 상태에 따른 사고 시나리오는 주로 지상에서 시험 시작 전 대상 장비 상태에 따른 위험 완화 조치를 중심으로 기술되는데, 대부분의 경우 위해요소 식별과 이에 따른 완화조치들은 시험 대상체인 무기체계 중심으로 구성되어 있으며, 시험 수행체계에 대한 오류에 대해서는 고려되는 부분이 일부분에 불과하다.

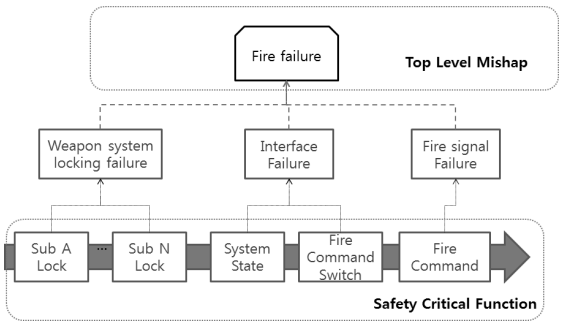
2.3 무기체계 시험 위해요소 식별

무기체계의 시험의 상위단계사고(Top Level Mishap)분류는 무기체계의 이상, 오작동에 발사 정지 등 불능상태에서의 완화조치가 주를 이루고 있다. 안전한 시험 절차를 구성하기 위하여 시험수행을 위한 설계 단계에서 시험 시나리오 구성과 함께 안전요소 분석이 수행되는데, 참고 문헌[9]에서 제시한 바와 같이 초기에 식별된 위해 요소(PHL: Preliminary Hazard List)들이 이 시스템 위험분석(SHA: System Hazard Analysis)단계에서 기능적 오류에 대한 조치 사항으로 변환되어 TLM을 생성한다. 식별 내용은 안전협의를 통하여 시험 설계에 반영하고 있는데, TLM과 안전 핵심 기능(SCF: Safety Critical Function)은 시험 안전 설계의 필수 요소로서 [Table 1]에서 두 기능간의 상관관계를 제시하였다[9].

[Figure 5]는 TLM과 SCF와의 관계를 무기체계 발사 절차사례를 중심으로 제시한 것이다. 발사 절차인 SCF 과정에서 문제가 발생하였을 때, 최종적으로 발생되는 TLM과의 관계를 나타낸 것으로서 시험설계에 반영할 시험 안전 요구조건 및 기능적 안전 조치를 식별할 수 있다[9].

<Table 1> Relationship between TLM and SCFs [9].

TLM No	Top-Level Mishap	SCFs
1	Inadvertent W/H initiation	Warhead initiation sequence
2	Inadvertent missile launch	Missile launch sequence
3	Inadvertent missile destruct	Destruct initiation sequence
4	Incorrect target	
5	Missile fire	
6	Missile destruct fails	Destruct initiation sequence
7	Personnel injury	
8	Unknown missile state	
9	Inadvertent explosive denotation	
10	Range Instrumentation fails	Flight Testing sequence



[Figure 5] SCF thread composed of a top level mishap.

2.4 연구 목표

무기체계 시험평가는 안전준수와 효율이라는 두 가지 요소를 모두 포함하며, 두 가지 관점에서 성공적인 시험 수행을 위해서는 시험 설계 및 결과 제공까지 시험 프로세스와 수행 시스템의 성숙도를 높여야만 한다.

성숙도란 정성적인 분석이나 경험적인 판단에 의존

ISSN 1229-6783(Print)
ISSN 2288-1484(Online)

하지 않고, 모델링, 정량적인 수치 계산이나 통계적 접근을 통하여 위험 분석을 통하여 예측까지 가능하여 밀 위험을 완화시킬 수 있는 단계까지의 대상 조직 또는 체계의 수준을 의미한다. 본 연구에서는 시험 설계의 산출물인 사고 시나리오 구성시, 시험 자원 중심의 사고위험 도출 개념을 이용하여 사고 시나리오에서 영향을 줄 수 있는 시험 자원을 식별하고 자원에 대한 사고 시나리오에서 정량적인 신뢰성 제고와 이에 따른 시험 비용적인 영향을 제시하고 안전성과 함께 효율적인 시험 수행을 위한 시험 체계 구성 방안 수립을 제안하여 시험 수행 체계의 성숙도를 높이고자 한다.

3. 시험 시나리오 구성

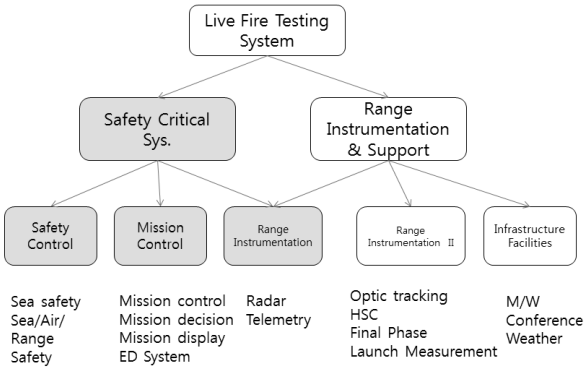
사고 시나리오의 정량적 위험 해석을 위해 기본 운영 시나리오의 시험 프레임워크 구성, 적용 이론 검토, 시나리오 구성, 투입자원에 대한 신뢰성 검토, 사고 시나리오 구성 순으로 제시하였다.

3.1 시험 수행 프레임워크

시험 아키텍처를 구성하기 위하여 시험 요구조건을 반영하여 투입 자원을 식별해야 한다. 안전 중시 시스템으로 시험 수행 요소에 안전 관련 참여 요소를 식별해야 한다. 안전 중시 시스템으로 물리적인 아키텍처를 구성해야만 하므로 시험 대상물인 유도무기 또는 총포탄약 시험체를 제외하고, 시험 수행 체계를 안전 업무를 수행하는 장비나 시설 등을 포함하는 안전 통제(safety control), 시험의 전체적인 수행 및 상태를 판단하는 시험 통제(mission control), 시험 수행을 위하여 필수적으로 필요한 기반시설인 통신, 전기, 수송등의 시험 지원(test facility) 그리고 시험 요구조건의 자료를 제시할 수 있는 시험 계측(instrumentation)으로 구분 할 수 있으며, 시험 계측 분야는 실시간 자료 획득에 따른 시험 중 안전 판단 기능 여부에 따라서 안전요소와 순수계측요소로 구분할 수 있다. [Figure 6]은 시험 안전에 직접적으로 연관되는 부분과 계측 및 지원 체계로 구분하여 이중 중요 안전 자원과 일반 시험 자원을 구분하여 식별 하였다.

시험 자원의 중요도는 안전 영향 여부, 중요 시험 요구조건 충족 여부 등 상세 시험 요구조건을 기반으로 결정할 수 있다.

시험 시나리오 구성시 시험 수행 신뢰도와 관련된 항목은 좌측의 안전중시 기능을 포함한 자원에 대해서 신뢰도를 분석한다.



[Figure 6] Resource breakdown structure for weapon systems live fire test.

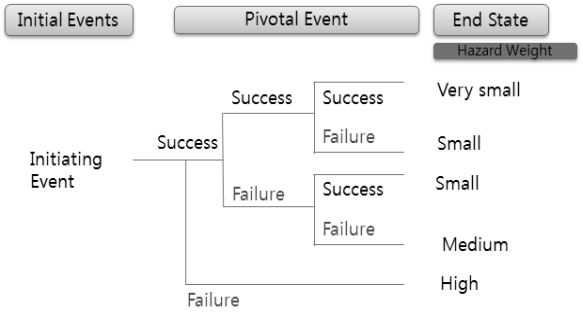
3.2 FTA

결함나무 분석(Fault Tree Analysis)은 위험 및 신뢰도 추정을 위하여 널리 사용 중인 기법으로서 시스템 내에서 발생할 수 있는 환경조건, 조작오류 등 원인 간의 상호관계를 AND, OR 논리게이트를 사용하여 논리정연하게 오류 원인을 추정할 수 있으며, 최종 오류 원인의 빈도나 확률에 대하여 정량적 정보를 제공, 시스템의 잠재적 고장에 대한 정성적 분석이 가능하게 한다. FTA시 내부 고장 발생확률은 통상 경험적 또는 실험적으로 구해지나 이러한 고장확률이 정적인 상태에서의 문제점인 경우가 많고, 불완전한 정보 하에도 오류 상태를 구현할 수 있다. FTA는 가시적으로 오류 원인을 확인할 수 있고, 오류원 식별에 유리하나 시간적인 변화에 대한 표현이 어려우며, 복잡한 시스템에 대해서는 구현이 어렵다는 단점이 있다.

3.3 ETA

사건나무분석(Event Tree Analysis)은 초기 이벤트(Intial Event)에 따라서 잠재적인 사고 시나리오를 식별하여 해석하는 방식으로서 단계 별로 발생확률을 계산하고, 중간 상태의 변화에 따라서 생성된 여러 최종 상태의 사고 심각도를 예측할 수 있다. [Figure 7]은 사건 나무 분석과 마지막 종결단계에서 위험 가중치에 대하여 제시한 것이다.

귀납적 방식이지만 정량적인 해석방법으로서 간과되기 쉬운 위해 요인의 분석에 적합하여 안전 경로, 위험 증가 방식, 위험 운영 등을 제시하고 문제점을 식별하여 대안을 파악할 수 있다.



[Figure 7] ETA-based accident scenario concept.

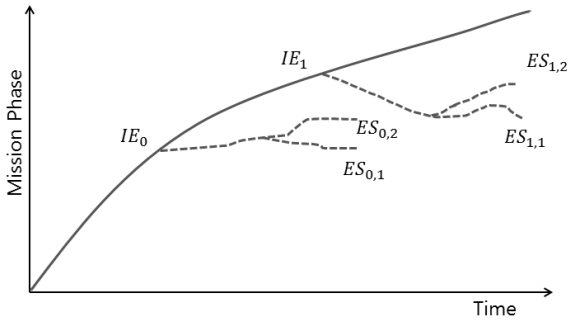
사건나무분석은 초기이벤트(IE)와 사고 전환단계(Pivotal Events) 그리고 최종 상태(End State)로 구성된다. 사건나무분석에서 전체 오류발생 확률은 초기부터 전환단계까지의 발생 확률의 합으로 구성되며, 초기 단계의 발생확률을 P_A, 전환단계의 발생확률을 $P_{B1}, P_{B2} \cdots P_{Bn}$ 이라고 하면, 3단계가지를 고려시, 사고 발생 확률은 (식 1)로 제시할 수 있다.

$$P_{case1} = P_{A1} \cdot P_{B1} \cdot P_{B2} \cdot P_{B3} \quad \text{(식 1)}$$
$$P_{case2} = P_{A1} \cdot P_{B1} \cdot P_{B2'} \cdot P_{B3'}$$
$$\vdots$$
$$P_{caseN} = P_{An} \cdot P_{Bn1} \cdot P_{Bn2} \cdot P_{Bn3}$$

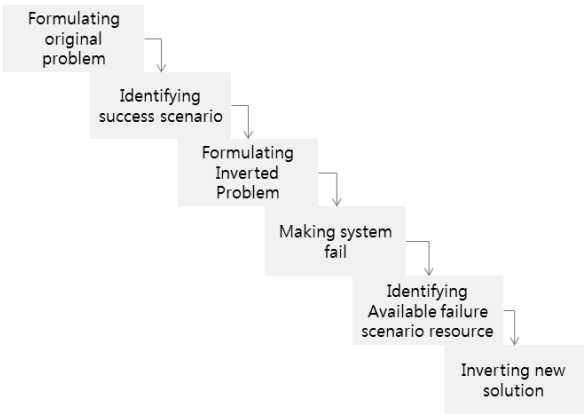
다양한 단계와 경우의 수를 모두 포함하기에는 계산과정이 복잡하고 해석과정이 길어지므로, 시스템 수행정도에 따른 위험도를 고려하여 임계점을 가지는 것이 중요하다.

3.4 AFD

AFD는 결합 발생 사건을 사전에 시스템적으로 식별하는 절차로서 트리즈(Triz) 이론에서 발전하였다. 기존의 고장 예측이 자기중심적이고, 기본적으로 안전을 준수하였다고 간주하여 부정적인 영향을 최소화 하여 도출된 위험을 축소화하는 치명적인 오류를 수반할 수 있다.
기존 위험 해석 방식이 특정 오류에 대한 완화조치 등 대안을 도출하는 것으로 무엇이 잘못될 수 있는가라는 위해 요소의 가능성 해결을 중심으로 한다면 AFD는 어떤 위해요소를 생성할 수 있는가하는 역발상에서 시작된다. 사고 원인을 도출하기 위하여 정상적 운영 또는 시험 시나리오와 발생할 수 있는 사고 발생 경위를 정리해야 한다. 정상 시나리오(S_0)에 대하여 사고 확률에 의한 시나리오들을 구성할 수 있는데 i개의 시나리오 구성시 S_i 로 정의할 수 있다. 초기 사고 원인(Initial Event, IE_0)에 근거하여 여러 개의 사고 초기 원인이 존재할 수 있으며, 이에 따른 좀 더 다양한 사고결과(Ending State, ES)를 도출할 수 있다.
사고결과는 치명적 오류, 임무 실패, 임무 종료 등 위험도가 각기 다른 결과를 가지게 될 것 이며, 전체 시나리오 구성을 [Figure 8]과 같이 구현하여 실사격 시험 진행에서 사고 발생경로를 직관적으로 인지할 수 있도록 구성할 수 있다.



[Figure 8] System scenario with accident status [12].



[Figure 9] AFD-based scenario concept [12].

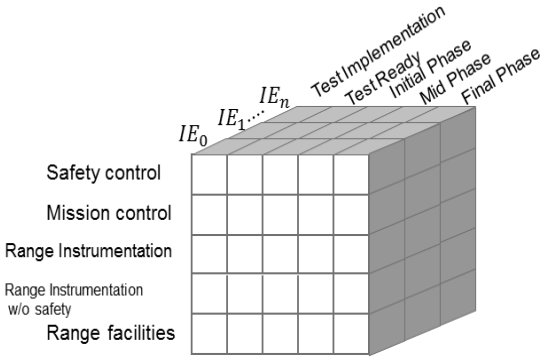
AFD의 사고 예측을 위한 절차를 [Figure 9]에서 제시하였다. 먼저 외부 영향이나, 시스템 내부의 오류 발생 가능성을 문제점을 도출한 뒤, 이를 고려하여 성공적으로 수행 할 수 있는 시나리오를 구성한다. 처음 도출한 문제를 이용하여 시스템에 관련된 모든 사고원인을 도출한다. 도출된 원인을 중심으로 사고 시나리오를 구성하고, 관련되는 자원을 식별하여 해결책을 모색하는 방안이다.

3.5 시험 시나리오 구성 방안

본 연구에서는 AFD의 위험예측 방식을 적용, 시험체계와 관련된 사고 시나리오를 구성하여 시험 무기체

계의 신뢰도에 대한 확률은 P' (T)로 정의하고, 시험 체계와 관련된 사고 시나리오를 작성하여 사건나무분석을 실시하였다. 시험 수행 시스템에서 식별된 중요 안전 자원을 중심으로 문제 발생 원인을 도출하고, 발생할 수 있는 시나리오 상황($IE_0 - IE_n$)별 사고 발생 확률을 사건나무분석을 사용하여 계산 한다. 이에 따라서 시험 투입자원과 시험 단계 그리고 구성된 사고 시나리오 상황이라는 3개의 변수에 대하여 사고시나리오는 3차원 매트릭스로 [Figure 10]과 같이 제시할 수 있다.

본 연구에서는 시험투입 자원만을 고려함으로 시험 대상체인 무기체계가 가지고 있는 결함이나 사고 확률을 고려에서 제외하였다. 시험 수행단계는 발사전, 초기/중기/종말 단계로 가정하였다.



[Figure 10] Flight test accident scenario configuration for weapon systems development.

3.6 투입 장비별 신뢰도

무기체계 시험 특성상 시험 자원이 직렬구조로 구조화되는 경우는 거의 없으며, 안전중시 시스템의 특성상 n개의 동일목적 장비의 병렬 구조로서 1대만 정상적으로 동작해도 정상상태를 가지도록 구성된다.

식별된 자원들 중 N개의 동일한 장비 중 m개가 활동되는 경우와 병렬 구조로서 1대만 정상적인 동작일 경우를 들 수 있는데, 병렬 구조에 대한 신뢰도 함수($R_s(t)$)는 (식 2)로 정의할 수 있다.

$$R_s(t) = 1 - \prod_{i=1}^{n}(1 - R_i(t)) \qquad \text{(식 2)}$$

여기서 i번째 시스템의 신뢰도($R_i(t)$)가 동일하다고 가정하면, (식 3)으로 나타낼 수 있다.

$$R_s(t) = 1 - (1 - R_i(t))^n \qquad \text{(식 3)}$$

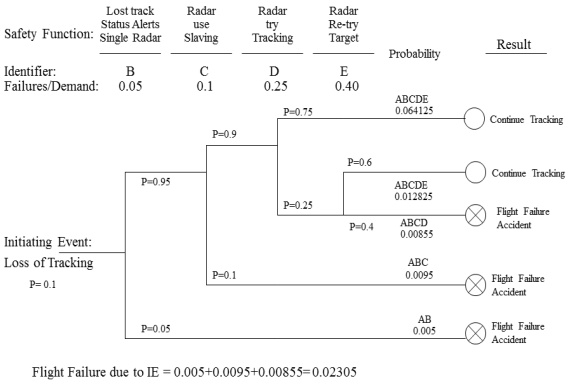
만약 동일한 신뢰도인 0.9를 갖는 장비가 병렬 구조를 갖도록 두 대의 장비가 동일한 목적으로 투입된다면 (식3)에서 0.99의 신뢰도를 얻음을 알 수 있다. 얻어진 신뢰도는 FTA를 통하여 중요 이벤트에 대한 실패 확률에 다른 조건으로 정의할 수 있다. n중 k 시스템의 신뢰도 함수는 (식 4)으로 정의할 수 있다.

$$R_s(t) = \sum_{x=k}^{n}\binom{n}{x}e^{-\lambda t\, x}(1 - e^{-\lambda t})^{n-x} \qquad \text{(식 4)}$$

위식에서 λ는 상수 고장률을 표시하고 있다. 경우에 따라서 n대의 장비를 투입하여 최소 k대가 정상적으로 동작해야 된다는 가정이 있을 경우에 적용한다.

3.7 사고 시나리오 구현

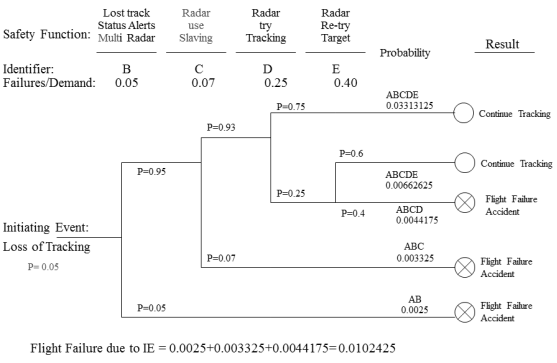
구성된 사고 시나리오에서 시험 자원에 대한 사건나무 분석을 수행할 수 있는데, 시험 중 시험 장비 오류나 운용상 문제가 발생하는 경우 조치 사항을 고려하여 [Figure 11]과 같이 사건나무구조로 사고 확률을 구할 수 있다. 여기서 제시한 사례는 무기체계 시험 중에서 레이더가 추적을 수행하지 못하여 시험에 정상적으로 이루어지지 못하는 경우를 가정하여 계산한 것으로서 최종적으로 시험 실패까지 가는 동안의 각종 경우에 대하여 고려한 것이다. 이러한 경우 레이더라고 가정한 시험자원의 오류에 따른 시험의 실패 사고 확률($P_1(t)$)은 0.02305이라 가정할 수 있다.



[Figure 11] Flight test accident scenario – ETA case.

무기체계 시험에 안전을 위하여 적용되는 시험 자원의 [Figure 11]과 같이 얻어진다면, 자원의 신뢰도를 높이기 위하여 병렬로서 자원을 투입할 수 있다. 사건나무 해석값은 자체 기능의 신뢰도와 함께 연관된 안

전 기능(safety function)에도 영향을 미쳐 전체 사고 발생확률을 저감할 수 있다. [Figure 12]에서는 시험 임무계획의 변경에 따라서 개선된 사고 확률 사례를 나타낸 것이다. 동일한 경우에 복수의 장비를 사용하여 투입 자원으로 가정한 경우에 사고 시나리오 중 두 건의 pivotal event에 영향이 발생하여 시험 실패 확률 ($P_1(t)$)은 0.0102425로 얻어진다. 시험 자원의 증가는 시험 신뢰도 증가 뿐만 아니라 사고 위험성을 감소시킬 수 있지만, 시험 비용에도 영향을 미칠 수 있다. 두 사례 비교에 따라서 시험 사고 확률은 $P_{IE0} = 0.02305$에서 $P_{IE0'} = 0.0102425$로 발생 확률이 44% 감소하였음을 알 수 있다. 그러나 시험 비용의 증가 측면에서도 이를 고려해야만 한다.



[Figure 12] Flight test accident scenario with resource allocation modified – ETA case.

3.8 시험 비용과의 연관성

위험성 감소를 위하여 투입 장비의 증가는 시험 비용 증가에 직접적 영향을 미칠 수 있다. 시험 수행시 자원에 따른 단위당 비용 및 투입 자원을 가정하여 제시하였다. 레이더는 C_{radar}, 원격측정장비는 C_{TLM}, 광학장비는 C_{opt}, 비상종단 장치는 C_{ED}, 안전통제 선박은 C_{ss}, 임무제어는 C_{MC}라고 정리하면, 표 2와 같이 투입 자원의 물량과 투입 단계를 정의하였다.

<Table 2> Map of available test resource.

System	cost	Qty	Phase
Radar	C_{radar}	1~3	1-2-3
Telemetry	C_{TLM}	1~4	1-2-3
Optics	C_{opt}	1~5	2-3
ED	C_{ED}	1~3	1-2-3
Safety_ship	C_{ss}	1~3	3
Mission_control	C_{MC}	1~3	1-2-3

(식 5)는 i번째 단계에서 투입되는 투입 장비 자원에 따른 시험 단계 비용을 수식으로 나타낸 것이다. 여기서 x는 가중치, 투입 자원 댓수를 정의한 것이다.

$$C_{i,test} = x_{i,\alpha}C_{radar} + x_{i,\beta}C_{TLM} + x_{i,\gamma}C_{opt} + x_{i,\theta}C_{ED} + x_{i,\sigma}C_{SS} + x_{i,\omega}C_{MC} \quad \text{(식 5)}$$

(식 5)에서 레이더를 제외한 나머지 부분을 (식 6)으로 정의하면, (식 5)는 (식 7)과 같이 나타낼 수 있다.

$$x_{i,rest} = x_{\beta}E_{TLM} + x_{\gamma}E_{opt} + x_{\theta}E_{ED} + x_{\sigma}E_{SS} + x_{\omega}E_{MC} \quad \text{(식 6)}$$

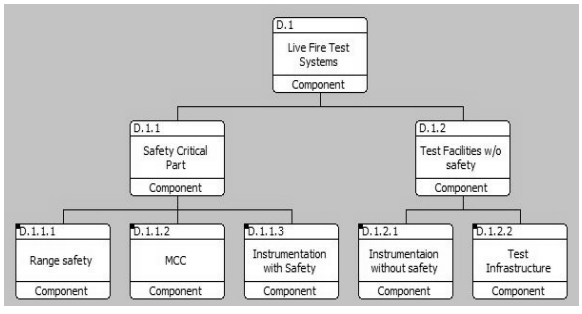
$$e_{i,test} = x_{i,\alpha}E_{radar} + x_{i,rest} \quad \text{(식 7)}$$

여기서 3대의 레이더를 투입한다고 가정하면, $x_{i,\alpha}$는 최소 5에서 9까지 변화할 수 있으며, 이는 동일한 신뢰도에 대하여 최대 2배까지 자원 가용도를 조정할 수 있다. 이는 시험계획 수립의 조정에 따라서 투입자원 감소에 따라서 비용절감과 같은 효율적인 시험 수행을 도모 할 수 있음을 의미한다.

4. 사고 시나리오 검증

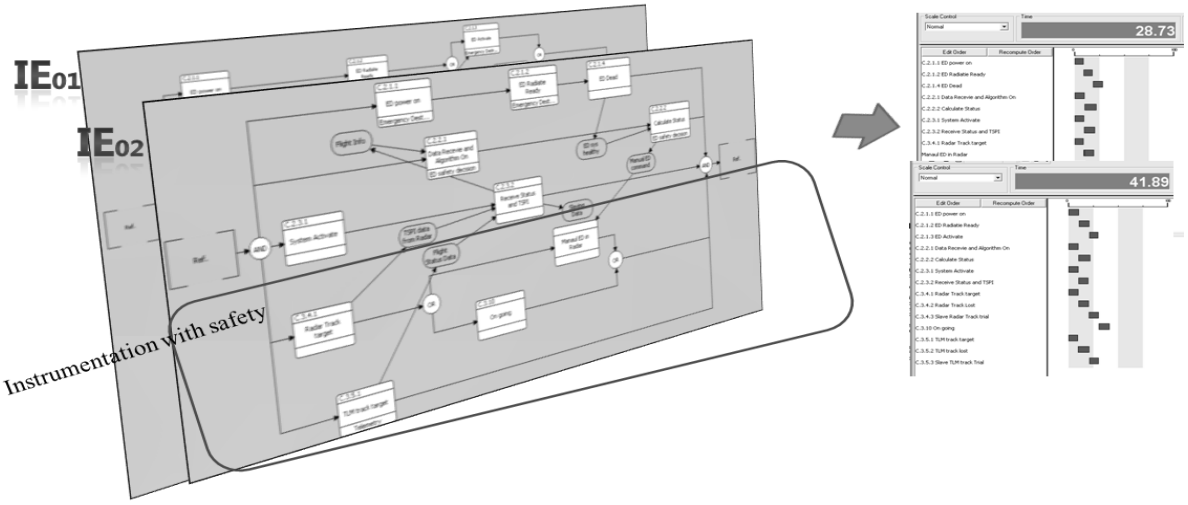
4.1 사고 시나리오 구성

기본적으로 구성될 시험 시나리오와 사고 시나리오간의 논리적 전개와 연계성을 확인하기 위하여 시나리오를 시스템 공학 전산 도구인 Vitech사의 Core을 이용하여 아키텍처를 [Figure 13]과 같이 구성하였다. 앞에서와 같이 시험 자원은 안전 중시 시스템으로서 사고 시나리오에 직접적으로 연관이 있는 시험 자원과 일반적인 시험 수행을 위한 시험 자원으로 구분하였다.



[Figure 13] A physical hierarchy model for the test range system in weapon systems development.

ISSN 1229-6783(Print)
ISSN 2288-1484(Online)



[Figure 14] A functional hierarchy model of the accident scenarios for live fire test.

시험 시나리오와 사고 시나리오는 [Figure 11]와 [Figure 12]에서 제시한 사고 시나리오에 대하여 [Figure 14]에서와 같이 두 가지 사례에 대한 정상 동작 여부를 인지하기 위하여 구현하였다. 앞서 사례에서는 단일 장비에 대한 위험 확률을 제시하고 이에 따른 사고 원인을 제시하였지만, 전산 도구를 사용한 논리적 검증을 위하여 n개의 사고 사례(IE_n)에 대하여 여러 시험 자원 정상적 동작 여부를 확인하기 위하여 기능적 블럭 다이어그램을 EFFBD(Enhanced Functional Flow Block diagram)로 구성하였다. 본 결과를 통하여 시험 시나리오 구성시 사고 시나리오의 자원 투입 계획 및 시간별 동작 여부에 대한 논리적 구성의 적합성을 확인할 수 있으며, 시나리오의 절차상 오류를 방지할 수 있다.

5. 결 론

무기체계 연구개발에서 실사격 시험을 수행하는 시험수행체계는 안전중시 시스템으로서 시험 안전을 최우선으로 하고 있다. 시험 설계의 산출물인 시험 시나리오는 시험 대상인 무기체계 중심으로 사고를 기술하고 시험 투입자원에 대해서는 고려하지 않았다. 새로운 무기체계 개발에 따른 고난이도 시험 요구사항에 따른 시험 위험도 증가와 시험평가 비용의 급격한 증가에 따른 최소한의 시험횟수로 요구 성능 확인 요구는 과거보다 높은 시험수행 체계의 신뢰도를 가져야하며, 위험에 대한 대책이 요구된다.

본 연구에서는 기존에 무기체계 중심의 시험 시나리오에서 식별하지 못한 시험 자원 중심의 오류 도출 방안 등 체계적인 시험 시나리오 구성방안을 연구하였다. 시험 자원과 시험 단계 그리고 사례별 사고 시나리오 구성은 시각적으로 어디서, 언제, 어떤 방식으로 사고가 발생함을 직관적으로 확인할 수 있으며, 다중사건나무구조를 가지게 됨으로서 사건나무구조의 정량적인 오류 확률 판단이 가능케 하였다.

시험 자원에 투입에 따른 정량적인 신뢰도 분석과 시험 비용의 연관성을 제시하여, 무조건 적인 시험자원의 투입량 증가가 신뢰도의 정량적인 증가가 아니므로 효과적이고 효율적인 시험 설계를 통하여 시험 비용 저감을 위한 근거를 제시하였다.

향후 연구에서는 투입 자원에 따른 안전도와 시험비용의 상관관계 분석을 전체 시험자원과 시험 설계에 확대 적용, 시험 비용 산출과 시험 수행의 안전 신뢰도를 함께 제시할 수 있는 실사격 시험 수행 체계 프레임워크 구현 방안 연구가 이루어져야 할 것이다.

6. References

[1] W. D. Bell (2010), “Systems Engineering Test and Evaluation - The Integration Process,” ITEA Journal, 31:56-62

[2] B. J. Yoo et al. (2012), “Systems Engineering based Live Fire Test of Weapon systems,” KIMST, 5:28-35

[3] Sunghyuck Ye, Jae-chon Lee (2014), "Model-Based Architecture Design of the Range safety process for live fire test with enhanced safety, " Korea Safety Management & Science, 14:43-52

[4] M. Bouissou (1999), "Assessment of a

safety- critical system including software: a bayesian belief network for evidence source," IEEE RAMS, pp. 142-150
[5] J. C. Knight (2002), "Safety Critical Systems: Challenges and Directions," ICSE '02. May. 2002
[6] Sung Hyuck Ye (2012), "On the development of IT-based test information system to share test infrastructure and advanced test requirement process for industry in Korea," ITEA Annual symposium
[7] "Preparation guide for the joint services weapon safety review safety data package," 1st Ed Jun. 2014 DoD
[8] R. C. Terry (2005), "System safety in systems engineering process," NDIA 8th Annual systems engineering conference
[9] C. A. Ericson, II (2005), "Hazard Analysis Techniques for system safety," John Wiley & Sons, Inc.
[10] A. Kossiakoff et al. (2011), "Systems Engineering Principles and Practices," 2nd Ed, Wiely : 170-179
[11] NASA "Fault Tree Handbook with aerospace application," NASA
[12] S. Kaplan et al. (2005) "New tools for failure and risk analysis," IDEATION
[13] A. Angel (2010), "Verification, Validation, and Testing of Engineering Systems," John Wiley & Sons, Inc.

저 자 소 개

예 성 혁

현 국방과학연구소 책임연구원, 아주대학교 시스템공학과 박사과정. 관심분야는 시험평가 관련 시스템공학 및 안전설계, 모델기반 시스템공학 등

주소 : 충청남도 태안군 태안우체국 사서함 1호 국방과학연구소 제8기술연구본부

이 재 천

현 아주대학교 시스템공학과 정교수. 서울대학교 전자공학과에서 공학사, KAIST 전기 및 전자공학과에서 공학석사 및 박사학위를 취득. 미국 MIT에서 Post-Doc을 수행하였으며, Univ. of California (Santa Barbara)에서 초빙연구원, 캐나다 Univ. of Victoria (BC)에서 방문교수, 미국 Stanford Univ. 방문교수 역임. 현재 연구 및 교육 관심분야는 시스템공학(SE), 모델기반 시스템공학(MBSE), 시스템 안전(Systems Safety), 시스템 시험평가(Systems T&E) 및 다양한 산업 및 공공 분야에서의 SE 응용 등.

주소 : 경기도 수원시 영통구 원천동 산5번지 아주대학교 서관 309호