Journal of the Korea Academia-Industrial cooperation Society
Vol. 22, No. 7 pp. 376-385, 2021

https://doi.org/10.5762/KAIS.2021.22.7.376
ISSN 1975-4701 / eISSN 2288-4688

유도탄의 안전도 설계 적용 방안

서양우*, 김희욱, 이승상, 김정태
LIG넥스원 PGM IPS연구소

A Study on Application of Safety Design for Guided Missile

Yang-Woo Seo*, Hee-Wook Kim, Seung-Sang Lee, Jung-Tae Kim
PGM IPS R&D Lab, LIG Nex1

요 약 안전은 시스템의 목표와 요구사항을 수행하는 동안 시스템의 매우 중요한 목표이지만, 무기체계에 보편적으로 적용되고 있지 않다. 무기체계의 안전에 대한 중요성이 증대되고 있으며, 실질적인 대응책이 필요하다. 이에 따라, 무기체계에 대한 안전도 설계 구현시 누락된 안전 요구사항에 대한 위험요인 분석을 완벽히 수행할 수 있는 프로세스를 구축할 필요가 있다. 본 논문은 유도탄 체계의 안전도 설계 적용 방안을 제시한다. 유도탄에 대한 안전도 설계 프로세스를 제시한 후, OOO 유도탄의 사례 분석을 수행하였다. 유도탄 안전 관련 설계 체크리스트를 적용한 예비 위험 요인을 식별한 후, 시스템 설계를 수행하도록 하였다. FMEA 기법을 적용한 위험요인 분석을 수행하여 리스크 평가를 수행하였다. 리스크 수용여부를 결정하기 위하여 리스크 평가 매트릭스를 활용하였다. 그 결과, 탄두 안전 유지, 탄 구속 및 해제, 부스터 연소, 사용자 운용, 점검 및 훈련에 대한 리스크 감소 대책을 수립하였다. 위험요인 감소를 위한 설계 및 안전장치 추가, 매뉴얼 경고 문구 및 교육 수행의 권고사항을 도출하였다. 추가로 주요 기능에 대한 운용유지 측면에서 고장 탐지 방안까지 도출하였다. 본 연구의 결과인 유도탄의 안전도 설계 적용 방안은 어떤 유도탄이든 설계 전에 유용하게 활용될 수 있다.

Abstract Safety is an important objective of a system when performing its objectives and requirements, but it is not applied universally to weapon systems. The importance of safety for weapon systems is increasing, and practical countermeasures are needed. Therefore, it is necessary to establish a process to perfectly perform a hazard analysis of missing safety requirements in implementing safety design for weapon systems. This paper presents an application of safety design for guided missiles. After presenting the safety design process for guided missiles, case analysis of the OOO missile was performed. First, after identifying the preliminary hazard applied to the design checklist related to guided-missile safety, the system design was carried out. A risk assessment was performed by hazard analysis applying FMEA techniques. The risk assessment matrix was used to determine the acceptance of risk. As a result, risk reduction measures were established for warhead safekeeping, missile restraint and release, booster combustion, user operations, checking, and missile training. The recommendations for adding design and safety devices, warning statements of manual and training are derived to reduce the hazard. In addition, failure detection methods were derived in terms of sustaining major functions. The safety design applications resulting from this study can be useful for the design of any guided missiles.

Keywords : Safety, Safety Design, Hazard Analysis, Design Checklist, Risk Assessment, Guided Missile

*Corresponding Author : Yang-Woo Seo(LIG Nex1)
email: yangwoo.seo2@lignex1.com
Received April 12, 2021 Revised May 3, 2021
Accepted July 2, 2021 Published July 31, 2021

1. 서론

안전도는 사망, 상해, 직업병, 장비의 손상이나 손실 또는 환경 파괴를 유발할 수 있는 조건이 없는 상태를 의미한다[1]. 시스템 안전은 복잡한 시스템의 위험과 사고를 방지하기 위해 수행되는 엔지니어링 분야이다. 시스템을 이해하여 시스템이 설계된 대로 작동하는지 최악의 경우에 시스템이 어떻게 작동되는지 검증해야 한다.

안전은 시스템의 요구사항을 수행하는 동안 시스템의 매우 중요한 목표이다. 안전은 수명주기 동안 위험요인 식별, 위험요인 분석 및 위험요인 제거 및 감소를 요구한다. 하지만, 설계변경에 따른 시스템 안전을 계속 간과하고 있기에 반드시 안전이 개입되어야 한다. 안전의 궁극적인 목표는 결함 수준을 0으로 줄이는 것이다. 설계자는 안전 관련 설계의 수정조치활동으로 발생가능한 사고에 대한 비용을 절대적으로 줄일 수 있음을 인지할 필요가 있다. 따라서, 설계주기의 중요한 시점에서 안전 변경을 위한 설계를 권장하고 설계의 사고방식을 이해하도록 유도해야 한다.

기존 연구사례를 살펴보면, 전세진 외[2]는 파형강판 구조물의 특성을 고려하여 기존의 내하력 평가법을 개선한 안전도 평가 절차를 제안하였고, 최순호 외[3]는 제주 전력계통 운영에 있어서 안정적으로 운영할 수 있도록 안전도평가를 제안하였고, 이민구 외[4]는 안전도 평가를 위해 BLE센서를 이용한 퍼지 포괄 평가 방식을 제안하였다. 한편, 이명철[5]은 전자연동장치의 기능 안전도 분석을 수행하였고, 정현승 외[6]는 도시철도 충돌안전도 향상을 위한 개선방안을 제안하였고, 이한상[7]은 전압원 컨버터 기반의 다수 분산형 전원의 접속에 대한 배전선로 안전도 확보방안을 제시하였다.

Table 1은 선행연구분석을 요약한 것으로 연구사례를 크게 안전도 평가 방법 및 안전도 분석으로 구분할 수 있다. 특히, 민수 분야에서만 활발하게 연구되고 있으며, 방산 분야에서는 업무 특성상 보안이라는 제한사항으로 인해 연구사례가 없는 실정이다. 하지만, 방산 분야의 무기체계 운용 중 폭발로 인한 인명 피해가 있을 수 있기 때문에 안전도 평가를 반드시 수행해야 할 필요가 있다. 안타깝게도 장비 성능 위주의 설계에 치중되고 안전 설계를 간과하고 있다고 볼 수 있다. 안전 설계를 제대로 수행하지 못하는 사유는 무기체계 요구사항에 부정적인 요구사항이 잘 언급되어 있지 않기 때문이다. 즉, 안전에 관련된 '~ 되어서는 안 된다.' 라는 요구사항이 제대로 설정되어 있지 않는 게 현실이다. 따라서, 무기체계의 안전에 대한 중요성을 인식해야 하며, 이에 대한 실질적인 대응책을 강구해야 한다. 특히, 누락된 부정적인 안전 요구사항에 대한 위험요인 분석을 완벽히 수행할 수 있는 프로세스를 구축할 필요가 있다.

Table 1. Summary table of prior Research and Analysis

Referen-ces Number	Classification	Subject	Applications
2	Safety Assessment	Safety Assessment Procedure	Corrugated steel plate structures
3		Safety Assessment	Renewables Interconnected Power System
4		Safety Assessment	A gas explosion or fire
5	Safety Analysis	Functional Safety Analysis	Electronic Interlocking Unit
6		Improvement of Safety	Metro Train
7		Optimal Supply Reliability and Safety	Distributed Power Lines

이러한 사항을 고려하여 본 논문에서는 방산 분야에서 안전이 가장 중요하다고 판단되는 유도탄 체계 분야의 안전도 평가 방법론을 연구 및 적용하고자 한다.

본 논문은 유도탄 체계의 안전도 설계 적용 방안을 제시한다. 유도탄에 대한 안전도 설계 절차를 제시한 후, 각각의 활동에 대한 세부 내용을 기술한다.

2. 본론

2.1 연구절차 개념도

본 논문에서의 주요 연구절차는 Fig. 1과 같이 수행하였다. 서론에서 선행연구분석을 수행한 결과를 활용하여 본론에서는 현 안전도 절차 현황 분석을 통한 시스템 안전도 설계 프로세스를 제안하였다. 제안한 안전도 설계

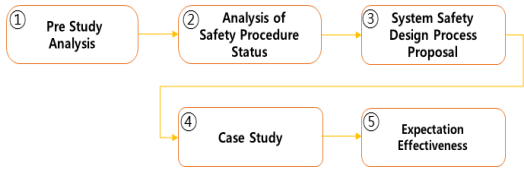

Fig. 1. The Main Research Procedure for this Paper

프로세스에 대한 사례분석을 수행한 후 기대효과를 기술하였다.

2.2 안전도 개념

예전에는 시스템 안전이 존재하지 않았으며, 사고가 발생하면 무엇이 잘못되었는지 조사한 후 시스템에 수정조치를 시행하였다. 이것이 'fly-fix-fly'접근법으로 시행착오의 접근방식이다. 시스템 안전은 2차 세계대전 이후 항공기 안전에 대한 군의 우려로 안전의 진화가 시작된 'fly-fix-fly'접근 방식에 대한 불만에서 비롯되었다. 설계상의 결함을 발견하기 위해 사고가 일어나기를 기다리는 것은 무책임했다. 'fly-fix-fly'철학은 위험요인을 식별하고 통제하는 허용할 수 없는 방법이 되었다. 1966년 미국방부가 초기 공군 버전에서 채택한 후에야 시스템 안전성에 대한 첫 공식 정의가 나타났다. 1969년 미국방부는 MIL-S-38310A 규격에 기반한 MIL-STD-882의 최초 버전을 발표하였다. 1977년 MIL-STD-882A에는 위험요인 식별 및 리스크 관리가 추가되었다. 1984년 MIL-STD-882B는 시스템 안전을 '상태'가 아닌 '활동'으로 만들었다. 1993년 MIL-STD-882C는 정의에 '안전의 모든 측면'을 포함한 미미한 변경을 하였다. 2000년 MIL-STD-882D는 시스템 안전의 정의에서 '안전을 최적화하기 위해'라는 단어가 '허용가능한 사고 리스크를 달성하기 위해'로 대체되었다. 2012년 MIL-STD-882E는 '허용가능한 사고 리스크를 달성하기 위해'를 '허용가능한 리스크를 달성하기 위해'로 대체함으로써 위험이 강조되었으며, '시스템 수명주기 모든 단계에서 운용 효과, 적합성, 시간 및 비용의 제약내에서 허용가능한 리스크를 달성하기 위한 엔지니어링 및 관리 원칙, 기준 및 기술의 적용'으로 정의되었다.

2.3 안전도 요구사항

대부분 사고 또는 시스템 고장은 규격의 잘못된 요구사항에서 비롯된다. 사업 일정이 지연되면, 새로운 기능을 구현할 강력한 설계변경이 이루어지지 않는다.

설계자는 이의 제기 없이 요구사항을 받아들이며, 누락되고 모호한 요구사항에 관심을 기울이지 않는다. 즉, 부적절한 요구사항이 설계에 반영됨으로써 시스템 위험요인으로부터 시스템 고장 및 사고가 발생한다. 또한, 시스템 성능, 비용 및 일정에 부정적인 영향을 미친다. 따라서, 규격에 누락된 기능이 있는지에 대해서 철저하게 요구사항 분석을 수행하는 것이 필연적이다. 알려진 문제에 대해서 아무 조치도 하지 않는 것을 용납해서는 안 된다.

Table 2. At least Perspectives of System Concept[8]

Number	Viewpoint of system concept
1	Functions of the product
2	What undesired functions the product should never do
3	Range of applications
4	Range of environments
5	Active safety
6	Duty cycles during life
7	Reliability for lifetime
8	Robustness for user/servicing mistakes
9	Logistics requirements to avoid adverse events
10	Manufacturability requirements for defect free production
11	Internal/External interface requirements
12	Installation requirements to assure safe functioning
13	Shipping/handling capabilities to keep the device safe
14	Serviceability/diagnostics capabilities
15	PHM to warn users in case of an anomaly
16	Interoperability with other products
17	Sustainability
18	Potential accidents and abuses
19	Human factors

정확하고 포괄적인 성능 규격을 작성하는 것은 안전한 설계를 위한 전제조건이다. 설계변경 비용이 미미한 개념단계에서 모든 안전 변경을 조기에 수행해야 한다. 시스템의 개념은 Table 2에서 제시한 관점으로부터 설계가 진행되어져야 한다[8].

위험을 완화하기 위한 우선순위는 다음과 같이 진행한다.

1) 위험요인을 방지하기 위한 요구사항 변경
2) 고장 허용 오차 도입
3) 임무를 안전하게 완수할 수 있도록 설계
4) 조기 진단 경고 제공

2.4 안전도 평가

안전한 시스템을 개발하려면 시스템 안전 분석이 필수로 수행되어져야 한다. 안전도 분석은 시스템의 잠재적 위험요인을 식별하고, 이러한 위험요인의 리스크를 평가하여 리스크를 제거하거나 허용가능한 수준으로 제어하는 것이다. 고장 유형 및 영향 분석(FMEA: Failure Modes and Effects Analysis, 이하 FMEA)은 고장 조건에 따른 고장 메커니즘의 위험요인 리스크 평가 및 설계 개선을 위한 수정조치를 통해서 고장 메커니즘 영향을 완화시키기 위한 구조화된 방법론이다.

Table 3은 주어진 리스크에 대하여 적합한 확률 수준을 정하기 위한 사고 발생도를 구분한다[1,8].

Table 3. Probability Levels[1,8]

Description	Level	Hazard Probability
Frequent	A	Probability of occurrence greater than 0.1 (continuously experienced)
Probable	B	Probability of occurrence less than 0.1 but greater than 0.01 (will occur frequently)
Occasional	C	Probability of occurrence less than 0.01 but greater than 0.001 (will occur several times)
Remote	D	Probability of occurrence less than 0.001 but greater than 0.000001 (unlikely, but can reasonably be expected to occur)
Improbable	E	Probability of occurrence less than 0.000001 (unlikely to occur, but possible)
Eliminated	F	Incapable of occurrence within the life an item

Table 4는 주어진 리스크에 대하여 적합한 심각도 범주를 정하기 위한 사망이나 상해, 환경 영향 또는 금전적 손실 가능성을 파악하여 심각도를 구분한다[1].

Table 4. Severity Categories[1]

Description	Severity Category	Mishap Result Criteria
Catastrophic	1	Could result in one or more of the following: death, permanent total disability, irreversible significant environmental impact or monetary loss equal to or exceeding $10M
Critical	2	Could result in one or more of the following: permanent partial disability, injuries or occupational illness that may result in hospitalization of at least three personnel, reversible significant environmental impact or monetary loss equal to or exceeding $1M but less than $10M
Marginal	3	Could result in one or more of the following: injury or occupational illness resulting in one or more lost work day(s), reversible moderate environmental impact or monetary loss equal to or exceeding $100K but less than $1M
Negligible	4	Could result in one or more of the following: injury or occupational illness not resulting in a lost work day, minimal environmental impact or monetary loss less than $100K

Table 5는 리스크 평가 매트릭스로 심각도 및 발생도의 조합으로 리스크를 평가한다[1,8].

Table 5. Risk Assessment Matrix[1,8]

Severity / Probability	Catastrophic (1)	Critical (2)	Marginal (3)	Negligible (4)
Frequent (A)	High	High	Serious	Medium
Probable (B)	High	High	Serious	Medium
Occasional (C)	High	Serious	Medium	Low
Remote (D)	Serious	Medium	Medium	Low
Improbable (E)	Medium	Medium	Medium	Low
Eliminated (F)	Eliminated			

2.5 안전도 절차 현황 분석

Fig. 2는 MIL-STD-882E에서 제시하고 있는 시스템 안전도 프로세스이다. 이 방법론을 시스템 엔지니어링 프로세스에 통합하여 진행해야 한다. DoDI 5000.02에서는 MIL-STD-882E의 방법론을 활용하여 위험의 상태를 평가하고, 설계검토회의를 통해 수용여부를 결정하도록 하고 있다[9]. 또한, 미국방부의 시스템 엔지니어링 관리계획서에 'Safety' 항이 별도로 구성되어 작성하도록 되어 있다[10].

따라서, 'Safety'는 시스템 엔지니어링 프로세스의 일부로 위험요인의 식별, 분류 및 완화를 위한 시스템 안전 방법을 문서화해야 한다. 시스템 안전 프로그램 계획은 위험요인 분석, 리스크 평가 및 리스크 관리의 체계적인 접근 방식을 구현하기 위해 필요한 상세한 업무 및 활동이 필요하다. 이에 따라, 시스템 안전 관리 활동이 시스템 엔지니어링 프로세스에 통합되는 방법을 정의한다. 특히, 시스템 안전 프로그램 계획에서 시스템 안전의 중요한 부분은 리스크를 처리하는 것으로 설계가 진행됨에 따라 위험요인을 식별하고 추적한다. 제품 개발 주기 동안 위험요인을 식별, 관련된 리스크를 평가, 위험요인을 완화 및 위험요인을 완전히 제거하기 위해서 다양한 유형의 위험요인 분석을 수행한다.

Fig. 2. Process of System Safety[1]

2.6 시스템 안전도 설계 프로세스 제안

시스템 설계는 시스템 요구사항분석 기반으로 안전도 분석을 포함하여 수행해야 한다. 요구사항 대비 안전도 요구사항을 추가적으로 명확히 식별할 필요가 있다. 이를 위해서는 안전설계가 포함된 설계체크리스트를 활용하여 식별할 수 있다. 이 후 사용자 요구사항을 시스템 사양으로 바꾸어야 한다. 이러한 사항을 반영하여 본 논문에서는 안전도 설계 프로세스를 Fig. 3과 같이 제시하였다. 불명확한 안전 관련 요구사항을 추가 식별하여 수용가능한 부분까지 설계에 반영하도록 하는 것이 이 프로세스의 목적이다. 위험요인 분석 수행시 FMEA 기법을 적용하여 위험요인 항목을 도출하고 확률을 평가한다. 리스크 수용여부에 따른 리스크 관리 및 추가 조치활동을 수행하는 프로세스이다.

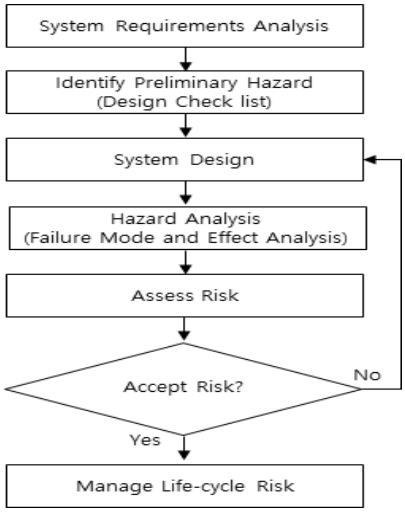

Fig. 3. Proposed for System Safety Design Process

제시한 프로세스의 각 활동에 대한 내용은 다음과 같다.

단계 1: 시스템 요구사항을 분석한다.

단계 2: 안전 관련 설계 체크리스트를 적용한 예비 위험 요인을 식별한다.

단계 3: 시스템 설계를 수행한다.

단계 4: FMEA 기법을 적용한 위험요인 분석을 수행한다.

단계 5: 리스크를 평가한다.

단계 6: 리스크 수용여부를 결정한다.

6-1) 리스크를 수용하면, 수명주기간 리스크 관리를 수행한다.

6-2) 리스크를 미수용하면, 추가 조치활동을 수행한다.

2.7 사례 연구

Fig. 3에서 제시한 프로세스에 따른 OOO 유도탄에 대해서 안전도 분석을 수행하였다.

1) 시스템 요구사항을 분석한다.

충분하고 효과적인 시스템 안전 요구사항은 향후 사고 발생을 예방하기 위한 수단이 된다.

Table 6. Requirements of OOO Missile

Number	Requirements
1	Seeker target capture distance shall be at least ○○ km when engaged in ○ dB status
2	Ability to cope with electromagnetic interference shall be capable of detecting/tracking targets in an electromagnetic interference environment
3	Guided control algorithm calculation shall receive target and flight information, calculate a guide command and transmit it to the driving device
4	Power supply should provide the power required to operate the main components
5	Safety and detonator shall be capable of maintaining the safety and armament
6	Antenna communication distance should be up to ○○ Km communication distance
7	Even if the guided missile fires accidentally, it should be in the launch tube stably
8	Booster insensitivity characteristics shall have combustion reaction class characteristics that do not affect operation

9	Angular velocity of the drive shall have a maximum angular velocity of at least ○ deg/sec
10	Thermal battery operating time shall be maintained for at least ○ seconds at the prescribed voltage
11	Missile shall be protected from salt or moisture that may be exposed
12	When an emergency shutdown order is received, the warhead shall detonate
⋮	⋮

OOO 유도탄의 업무기술서(SOW: Statement of Work)의 요구사항을 분석하였다. 단, Table 6은 보안상 OOO 유도탄 업무기술서의 요구사항 전체를 기술하지는 않았다.

2) 안전 관련 설계 체크리스트를 적용한 예비 위험 요인을 식별한다.

Table 7은 유도탄 설계 관련한 안전 체크리스트이다[11-16]. 안전 요구사항, 안전 기능 요구사항 및 특정 하드웨어, 소프트웨어 기능 요구사항을 고려하였다. 설계 체크리스트 적용 결과 10, 11, 15번 항목은 OOO 유도탄 업무기술서의 요구사항에 확인이 되지 않은 사항으로 추가로 도출되었다. 실 유도탄을 운용, 점검 및 훈련시 안전 설계 요구사항이 중요하기 때문에 사전에 안전 설계를 반영하는 것이 본 논문에서 제시한 프로세스에서 가장 중요하고 선제적인 활동이다. 따라서, 요구사항에 없다 하더라도 설계가 진입하기 전에 안전 위험요인을 설계에 반영하도록 하였다.

Table 7. Design Checklist related to Missile Safety

Number	Safety Design Checklist	Verify
1	Explosive train interruption(Fuze)	✓
2	Fail-safe	✓
3	Safety device	✓
4	Safety and arm device	✓
5	Safety Pin	✓
6	Safe indication	✓
7	Safety redundancy	✓
8	Design simplicity	✓
9	Design ruggedness	✓
10	Operated safety	-
11	Operational status indicator	-
12	Ignition system	✓
13	Explosive sensitivity	✓
14	Operator proficiency	✓
15	Fire enable provided incorrectly	-
⋮	⋮	⋮

3) 시스템 설계를 수행한다.

2)항에서 식별된 항목을 시스템 규격에 반영하여 시스템 설계를 수행하였다.

4) FMEA 기법을 적용한 위험요인 분석을 수행한다.

Table 8은 1) 시스템 요구사항 및 2) 안전 설계 체크리스트에서 식별된 기능을 나열하였다. 나열된 기능 기준으로 위험요인, 원인, 영향을 분석하였다. 각 위험요인에 대한 심각도 및 발생도를 산출하였다. 안전 측면에서 위험요인 우선순위를 권고 조치하였고, 유지측면에서는 고장탐지방안을 제시하였다.

5) 리스크를 평가한다.

위험요인에 의해 제시된 리스크를 결정하는데 활용하며, 위험요인의 우선순위를 정하는 방법을 제공한다. 사고의 리스크를 제거하거나, 완화하기 위한 설계 옵션을 결정하는데 사용한다. 심각도를 평가하여 위험요인 우선순위를 객관적으로 평가하여 설계 안전 리스크를 제거하거나 안전 위험요인 가능성을 최소화하기 위한 개선으로 이어진다. 따라서, 추가 조치활동 또는 리스크 허용 가능 여부를 결정하였다. 리스크를 정량화하는 일반적인 방법은 특정 결과와 그 결과의 발생 확률의 결과이다.

심각도(C: consequence severity) 및 발생도(P: probability of occurrence)를 곱하여 Eq. (1)과 같이 결과(R: Result)를 산출하였다.

$$R = C \times P \tag{1}$$

6) 리스크 수용여부를 결정한다.

6-1) 리스크를 수용하면, 수명주기간 리스크 관리를 수행한다.

리스크 평가가 Meduim이하이면, 위험 관리 검토회의를 통해 리스크를 수용한 후, 이 후 수명주기동안 지속적인 리스크 관리를 수행하였다.

6-2) 리스크를 미수용하면, 추가 조치활동을 수행한다.

Table 5의 리스크 평가 매트릭스를 활용하여 1A~3B에 해당하는 High, Serious 리스크에 대하여 Medium 리스크로 저감시키는 대책을 강구하였다. 이에 따라, 안전 측면에서 탄두 안전 유지, 탄 구속 및 해제, 부스터 연소, 사용자 운용, 점검 및 훈련에 대한 리스크 감소 대책을 Table 8에서 제시하였다. 따라서, 위험요인을 방지하고 위험요인 발생 가능성을 최소화할 수 있도록 심각도를 줄이는 설계변경을 구현하였다.

Table 8. Hazard Analysis applied to FMEA of OOO Missile

FMEA								
Function	Hazard	Cause	Effect	Risk			Recommended Action	
				C	P	R	Safety - Hazard reduction precedence	Sustainment - Failure detection method
1. Seeker target capture distance	Unable to capture target	Seeker target device fault	Missile function disabled	2	E	2E		BIT check
2. Ability to cope with electromagnetic interference	Unable to detect target	Seeker target device fault	Missile function disabled	2	E	2E		BIT check
3. Guided control algorithm calculation	Unable to guided control	Guided control device fault	Missile function disabled	2	D	2D		BIT check
4. Power supply	Unable to power supply	Power supply fault	Missile function disabled	2	D	2D		BIT check
5. Warhead safekeeping	Unable to keep safety status in case of sustaining of missile safe state	Detonation device fault	Unable to maintain safe state	1	D	1D	1. Reflecting the design of safety and arm device	
6. Antenna communication distance	Unable to communicate of command transmitter	Antenna fault	Missile function disabled	2	E	2E		BIT check
7. Missile restraint and release	Unable to keep safety status in case of accidental ignition of missile	Missile restraint device fault	Unable to maintain safe state	1	D	1D	1. Reflecting the design of missile restraint device and squib	
8. Booster insensitivity characteristics	Unable to insensitive booster	Booster fault	Unable to maintain safe state	1	D	1D	1. Reflecting the design of ignition safety device	
9. Angular velocity of the drive	Unable to operate of driving device	Driving device fault	Missile function disabled	2	E	2E		BIT check
10. Thermal battery operating time	Unable to operate of thermal battery	Thermal battery fault	Missile function disabled	2	E	2E		BIT check
11. Missile protection	Unable to protect of missile	Launch tube fault	Missile function disabled	3	E	3E		Visual check
12. Emergency detonation	Unable to operate command receiver when an emergency shutdown order is received	Command receiver fault	Unable to maintain emergency status	1	E	1E		BIT check
13. Users operations	Unable to control of missile launch	User operation error	Missile function disabled	1	D	1D	1. Reflecting the design of launch key (safety/arm) on the console 2. Reflecting the design of safety/arm switching assembly on the launch tube 3. Conduct training	
14. Check of missile	Launch signal transmitted to missile when checking missile	User check error	Unable to maintain safe state	1	C	1C	1. Reflecting the design of missile simulator 2. Add as warning phrase to technical manual 3. Conduct training	
15. Training of missile	Launch signal transmitted to missile when training missile	User training error	Unable to maintain safe state	1	C	1C	1. Reflecting the design of missile simulator 2. Add as warning phrase to technical manual 3. Conduct training	

Table 9. Risk Scoring of OOO Missile

Risk Scoring									
Function Number	Risk			Initial Risk			Residual Risk		
	C	P	R	C	P	R	C	P	R
1	2	E	2E	2	0.000001	0.000002	2	0.000001	0.000002
2	2	E	2E	2	0.000001	0.000002	2	0.000001	0.000002
3	2	D	2D	2	0.001	0.002	2	0.001	0.002
4	2	D	2D	2	0.001	0.002	2	0.001	0.002
5	1	D	1D	1	0.001	0.001	2	0.001	0.002
6	2	E	2E	2	0.000001	0.000002	2	0.000001	0.000002
7	1	D	1D	1	0.001	0.001	2	0.001	0.002
8	1	D	1D	1	0.001	0.001	2	0.001	0.002
9	2	E	2E	2	0.000001	0.000002	2	0.000001	0.000002
10	2	E	2E	2	0.000001	0.000002	2	0.000001	0.000002
11	3	E	3E	3	0.000001	0.000003	3	0.000001	0.000003
12	1	E	1E	1	0.000001	0.000001	2	0.000001	0.000002
13	1	D	1D	1	0.001	0.001	2	0.001	0.002
14	1	C	1C	1	0.01	0.01	3	0.01	0.03
15	1	C	1C	1	0.01	0.01	3	0.01	0.03
⋮									
Sub total						0.028014			0.072015
Risk Index	RI = Residual Risk/Initial Risk = 0.072015/0.028014 = 2.570679								

위험요인 저감 권고조치사항을 정리하면 다음과 같다. 탄두안전유지는 안전 및 기폭장치의 안전/무장상태를 유지 가능할 수 있도록 안전장전장치를 설계에 반영하였다. 탄구속 및 해제는 유도탄이 우발적으로 점화되어도 안정적으로 발사관 안에 위치할 수 있도록 탄구속장치 및 스퀴브를 설계 반영하였다. 부스터 연소는 유도탄 운용에 영향을 주지 않도록 점화안전장치를 설계에 반영하였다.

사용자 운용에서는 정상 및 비정상 발사절차 수행시 안전을 위한 콘솔에 발사키 및 캐니스터에 안전/무장스위치조립체를 설계반영하였고, 교육 내용을 추가하였다.

사용자 점검에서는 유도탄 점검시 발사신호가 유도탄에 송신이 되지 않도록 유도탄 시뮬레이터의 소프트웨어 설계에 반영하였고, 기술교범에 경고문구 처리 및 교육 수행을 추가하였다.

사용자 훈련에서는 유도탄 훈련시 발사신호 처리를 물리적으로 차단할 수 있도록 유도탄 시뮬레이터의 소프트웨어 설계에 반영하였고, 기술교범에 경고문구 처리 및 교육 수행을 추가하였다.

또한, 주요 기능에 대한 운용유지 측면에서 고장 탐지 방안을 추가하였다. 결론적으로 리스크 평가를 통해서 리스크 저감 대책의 우선순위를 결정하였다.

2.8 기대 효과

안전도 설계를 통해서 사망률 감소, 유지보수 비용 절감, 사고 비용 절감, 환경 피해 비용 및 기타 간접비용을 대폭 절감시키는 효과를 볼 수 있다. 설계 프로세스 초기에 위험요인을 식별함으로써 재설계와 관련된 비용도 피할 수 있다. 또한, 안전도 설계 프로세스 참여로 고객 만족도를 향상시킬 수 있다.

Table 9는 OOO 유도탄의 초기 리스크 대비 잔존 리스크를 정량적으로 평가하였다. 리스크 지수는 초기 리스크 대비 약 2.5배 개선됨을 볼 수 있었다. 따라서, 안전요구사항에 대한 리스크 관리 전략을 적용함으로써 시스템 안전 구현이 가능하다.

3. 결론

시스템 안전의 목적은 사고를 방지하여 인명을 구하고 부상을 예방하는 것이다. 사고를 예방하게 되면 장비, 시스템, 시설, 환경 등의 피해도 방지된다. 사고 예방에서 사고와 관련된 비용도 피할 수 있다. 시스템 안전은 설계의 중요한 측면이며, 어떤 프로그램에서든 시스템 안전의 구현으로 결과적으로 더 나은 제품을 개발하게 된다. 안전한 시스템을 개발하려면, 시스템 안전 분석이 필수로 수행되어져야 한다.

본 논문은 유도탄의 안전도 설계 적용 방안을 제시하였다. 유도탄의 안전도분석 프로세스를 제시한 후, OOO 유도탄에 대하여 사례분석을 수행하였다. 유도탄 안전 관

련 설계 체크리스트를 적용한 예비 위험 요인을 식별한 후, 시스템 설계를 수행하도록 하였다. FMEA 기법을 적용한 위험요인 분석을 수행하여 리스크 평가를 수행하였다. 리스크 수용여부를 결정하기 위하여 리스크 평가 매트릭스를 활용하였고, 탄두 안전 유지, 탄 구속 및 해제, 부스터 연소, 사용자 운용, 점검 및 훈련에 대한 리스크 감소 대책을 수립하였다. 위험요인 감소를 위한 설계 및 안전장치 추가, 매뉴얼 경고 문구 및 교육 수행의 권고사항을 도출하였다. 추가로 주요 기능에 대한 운용유지 측면에서 고장 탐지 방안까지 도출하였다.

OOO 유도탄의 초기 리스크 대비 잔존 리스크를 정량적으로 평가한 결과, 리스크 지수는 초기 대비 약 2.5배 개선되었다. 따라서, 본 논문에서 제시한 유도탄의 안전도 설계 적용 방안을 적용함으로써 시스템 안전을 구현하였다.

본 연구 결과인 유도탄의 안전도 설계 적용 방안은 어떤 유도탄이든 설계 전에 유용하게 활용될 수 있다. 안전 측면에서의 설계가 진행될 수 있도록 향후 사고 발생을 예방하기 위한 수단으로 활용할 필요가 있다.

References

[1] MIL STD 882E, System Safety, Department of Defense Standard Practice, pp.7-12, 2012.

[2] S. J. Jeon, B. J. Lee, "A Proposal for Improved Safety Assessment Procedure of Corrugated Steel Plate Structures Using Measured Displacements", *Journal of the Korean Society of Civil Engineers*, Vol.40, No.1, pp.13-24, 2020.
DOI: https://doi.org/10.12652/Ksce.2020.40.1.0013

[3] S. H. Choi, S. H. Park, J. H. Baek, Y. S. Cho, "Security Assessment of Renewables Interconnected Power System in Jeju", *The Korean Institute of Electrical Engineers Symposium*, pp.513-514, 2020.

[4] M. G. Lee, Y. K. Park, Y. J. Kim, K. K. Jung, "Design of Safety Evaluation System using BLE Sensors", *Information and Control Symposium*, pp.169-171, 2017.

[5] M. C. Lee, "A Study on the Functional Safety Analysis of PES-based Electronic Interlocking Unit according to IEC 61508", *The Transactions of the Korean Institute of Electrical Engineers*, Vol.63, No.11, pp.1526-1532, 2014.
DOI: https://doi.org/10.5370/KIEE.2014.63.11.1526

[6] H. S. Jung, S. W. Son, T. S. Kwon, J. S. Kim, "Study on Computational Simulation of a Collision Accident and Improvement of Passive Safety", *Transactions of the Korean Society of Mechanical Engineers*, Vol.39, No.9, pp.885-892, 2015.
DOI: https://doi.org/10.3795/KSME-A.2015.39.9.885

[7] H. S. Lee, "Optimal Supply Reliability and Safety of Multiple Distributed Power Lines based on Voltage Source Converter", *The Korean Institute of Electrical Engineers Symposium*, pp.270-273, 2019.

[8] L. J. Gullo, J. Dixon, Design for Safety, John Wiley & Sons, pp.7-8,130-132, 2018.

[9] Operation of the Defense Acquisition System, Department of Defense Instruction, Number 5000.02, p.90, 2019.

[10] F. Kockler, T. Withers, J. Poodiack, M. Gierman, Systems Engineering Management Guide, AD-A223 168, Defense Systems Management College, Chapter 3. Systems Engineering Management Plan, p.4, 1990.

[11] Missile Defence Agency Assurance Provisions, Department of Defense, MDA-QS-001-MAP-Rev A, p.138, 2006.

[12] MIL STD 1316F, Fuze Design Safety Criteria for, Department of Defense, pp.6-22, 2017.

[13] MIL HDBK 1512, Electroexplosive Subsystems, Electrically Initiated, Design Requirements and Test Methods, Department of Defense, pp.14-15, 1997.

[14] MIL STD 1911A, Hand emplaced Ordnance Design Safety Criteria for, Department of Defense, pp.8-9, 1993.

[15] MIL STD 1901A, Munition Rocket and Missile Motor Ignition System Design Safety Criteria for, Department of Defense, pp.9-14, 2002.

[16] S. J. Pereira, G. Lee, J. Howard, A System Theoretic Hazard Analysis Methodology for a Non-advocate Safety Assessment of the Ballistic Missile, Missile Defense Agency Washington DC, pp.6-8, 2006.

서 양 우(Yang-Woo Seo) [정회원]

- 1998년 2월 : 홍익대학교 전기공학과 (공학학사)
- 2014년 8월 : 아주대학교 IT융합공학과 (공학석사)
- 2019년 2월 : 아주대학교 시스템공학과 (공학박사)
- 1998년 7월 ~ 현재 : LIG넥스원 수석연구원

〈관심분야〉
RAMS, 시스템 엔지니어링, 데이터 분석

김 희 욱(Hee-Wook Kim) [정회원]

- 2010년 2월 : 부산대학교 산업공학과 (공학석사)
- 2010년 9월 ~ 2012년 12월 : 한국철도기술연구원
- 2013년 1월 ~ 2018년 8월 : LIG넥스원 선임연구원
- 2018년 8월 ~ 2019년 10월 : 네모시스(주) 책임연구원
- 2019년 10월 ~ 현재 : LIG넥스원 선임연구원

〈관심분야〉
RAMS, 모델링&시뮬레이션

이 승 상(Seung-Sang Lee) [정회원]

- 2008년 8월 : 한양대학교 정보경영공학과 (공학학사)
- 2020년 3월 ~ 현재 : 고려대학교 빅데이터융합학과 (석사과정)
- 2009년 1월 ~ 현재 : LIG넥스원 선임연구원

〈관심분야〉
신뢰성, 데이터 분석

김 정 태(Jung-Tae Kim) [정회원]

- 2020년 2월 : 한국항공대학교 항공기시스템공학과 (공학학사)
- 2020년 1월 ~ 현재 : LIG넥스원 연구원

〈관심분야〉
PHM, 기계학습