방산안보연구
Journal of Defense Industrial Security

방산안보연구, 1권 2호, 2025년 9월, 65-79면.
Journal of Defense Industrial Security, Volume 1, Issue 2, September 2025, Pages 65-79.
https://doi.org/10.64227/jdis.2025.1.2.4

Print ISSN 3091-5546
Online ISSN 3091-5554

원저

무기체계 개발을 위한 RMF-AT 통합 보안 프레임워크 연구 : 사이버보안과 기술보호의 효과적 융합 방안

이규호

LIG넥스원 수석연구원

교신저자: 이규호 (kyuho.lee@lignex1.com)

요약

현대 무기체계는 고도화된 소프트웨어와 네트워크 기술의 집약체로 진화하면서, 사이버 위협과 기술 유출이라는 이중적 보안 과제에 직면하고 있다. 대한민국 국방 분야에서는 K-RMF(위험관리 프레임워크)와 Anti-Tamper 기술이 각각 도입되어 운영되고 있으나, 이들의 분리된 적용은 개발 현장에서 프로세스 중복, 요구사항 상충, 보안 공백 등의 문제를 야기하고 있다. 본 연구는 시스템 엔지니어링(SE) 사상에 기반하여 위험관리 프레임워크(RMF)와 안티탬퍼(Anti-Tamper)를 유기적으로 융합하는 통합 보안 프레임워크를 제안한다. 연구 방법으로는 문헌 연구와 비교 분석을 통해 두 체계의 특성을 파악하고, 시뮬레이션을 통해 제안된 프레임워크의 효과성을 검증하였다. 우리는 통합된 프레임워크에 단일화된 위험 관리, 통합된 요구사항 추적, 전 수명주기 보안 내재화를 핵심 원칙으로 적용했다. 또한 MITRE ATT&CK 기반의 통합 위협 모델링과 DevSecOps 파이프라인 연계를 통해 실용성을 확보했다. 검증 결과, 통합 프레임워크는 기존 방식 대비 개발 효율성과 보안성을 동시에 향상시킬 수 있음을 확인하였다.

핵심어

무기체계 보안, 위험관리 프레임워크(Risk Management Framework), 안티탬퍼(Anti-Tamper), 통합 보안 프레임워크, 시스템 엔지니어링

차례

Open Access

접수일: 2025년 8월 06일
수정일: 2025년 9월 07일
게재승인일: 2025년 9월 16일
출판일: 2025년 9월 30일

Copyright: © 2025 Author(s)

This is an Open Access article distributed under the terms of the Creative Commons CC BY 4.0 license (https://creativecommons.org/licenses/by/4.0/) which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Original Article

Research on an Integrated RMF-AT Security Framework for Weapon Systems Development: Effective Integration Strategies of Cybersecurity and Technology Protection

Kyuho Lee

Chief Research Engineer, LIG Nex1, Republic of Korea

Corresponding Author: Kyuho Lee (kyuho.lee@lignex1.com)

ABSTRACT

Modern weapon systems have evolved into complex systems with advanced software and network technologies, facing dual security challenges of cyber threats and technology leakage. In the Republic of Korea's defense sector, K-RMF (Risk Management Framework) and Anti-Tamper technologies have been separately implemented, but this segregated application causes process redundancy, requirement conflicts, and security gaps in the development field. This research proposes an integrated security framework that organically combines as research methods, we identified the characteristics of both systems through literature review and comparative analysis, and validated the effectiveness of the proposed framework through simulation. We applied core principles to the integrated framework including unified risk management, integrated requirements traceability, and security embedded throughout the entire lifecycle. We also ensured practicality through MITRE ATT&CK-based integrated threat modeling and DevSecOps pipeline integration. Through validation, the integrated framework demonstrated simultaneous improvements in development efficiency and security compared to existing approaches.

KEYWORDS

Weapon System Security, Risk Management Framework, Anti-Tamper, Integrated Security Framework, System Engineering

1. 서론

1.1. 연구 배경 및 필요성

21세기 전장 환경의 급속한 변화는 무기체계 개발 패러다임에 근본적인 전환을 요구하고 있다. 현대 무기체계는 단순한 기계적 플랫폼을 넘어서 이제는 인공지능, 빅데이터, 사물인터넷 등 첨단 ICT 기술이 융합된 복합 시스템으로 진화하고 있다[1]. F-35 전투기의 경우 소프트웨어 의존성이 90%에 육박하며, 이는 무기체계의 공격 표면(Attack Surface)이 물리적 경계를 넘어 사이버 공간으로 확장되었음을 의미한다[2].

이러한 기술적 고도화에 따라 위협 환경 또한 전례 없이 복잡하고 다층적으로 변모했다. 과거 정부 기관이나 군 지휘부를 대상으로 하던 사이버 공격은 이제 방위산업체, 중소 협력업체, 연구기관 등 무기체계 개발 및 공급망 전체로 확대되고 있다[5]. 또한, 무기체계에 대한 수출이 증가하고, 무인화되면서 분실 및 탈취에 따른 비인가자에 의한 핵심 기술이 유출될 가능성이 높아지고 있는 현실이다[8,21].

대한민국 국방 분야에서는 이러한 안보 환경 변화에 대응하기 위해 두 가지 중요한 정책적 흐름이 형성되었다. 첫째, K-방산의 위상 제고와 수출 확대에 따라 핵심 기술의 불법적 분석이나 복제를 방지하기 위한 '기술보호(Technology Protection)'의 중요성이 대두되었으며, 이에 대한 공학적 해법으로 Anti-Tamper(이하 'AT' 또는 '안티탬퍼') 기술의 적용이 강조되고 있다[4,8]. 둘째, 고도화되는 사이버 위협으로부터 무기체계의 안정적 운용을 보장하기 위해 미국 국방부의 Risk Management Framework(이하 'RMF' 또는 '위험관리 프레임워크')를 벤치마킹한 한국형 위험관리 프레임워크(K-RMF)가 도입되어 2024년부터 시행되고 있다[3,7].

1.2. 연구 목적 및 범위

현재 RMF와 AT는 서로 다른 정책적 기반과 절차에 따라 개별적으로 관리되고 있어, 개발 현장에서 심각한 비효율과 혼란을 야기하고 있다. 본 연구는 이러한 분절된 접근법의 한계를 극복하고, 개발자 관점에서 두 보안 요구사항을 효과적으로 융합할 수 있는 통합 프레임워크를 개발하는 것을 목적으로 한다.

연구 방법으로는 첫째, 문헌 연구를 통해 RMF와 AT의 이론적 배경과 특성을 고찰하고, 둘째, 비교 분석 방법을 활용하여 두 체계의 목적, 범위, 프로세스, 평가 방식 등을 다각도로 비교한다. 셋째, 시스템 엔지니어링(System Engineering, SE) 방법론을 적용하여 통합 프레임워크를 설계하고, 넷째, 시뮬레이션 연구를 통해 제안된 프레임워크의 효과성을 검증한다.

연구의 공간적 범위는 대한민국 국방 무기체계 연구개발 환경을 주된 분석 대상으로 하되, 이론적 기반과 선진 사례 분석을 위해 미국 국방부의 RMF 및 AT 정책을 참조한다. 내용적 범위는 RMF와 AT의 이론적 고찰, 비교 분석, 통합 프레임워크 설계, 수명주기 적용 방안, 통합 방법론 제시, 검증 및 정책 제언을 포괄한다.

본 논문은 총 5개의 장으로 구성된다. 제1장 서론에서는 연구의 배경과 필요성, 목적과 범위, 그리고 연구 방법 및 구성을 기술한다. 제2장 이론적 배경 및 현행 체계의 문제점 분석에서는 무기체계 보안의 개념을 시작으로, RMF와 AT의 개념과 특성을 상세히 고찰하고 RMF와 AT의 두 보안 체계를 다각적으로 비교하고, 현행 적용상의 문제점과 한계를 심층적으로 분석한다. 제3장 무기체계 개발자 관점의 통합 보안 프레임워크에서는 본 연구의 핵심으로, 시스템 엔지니어링 기반의 RMF-AT 통합 프레임워크를 제안하고, 개발 생명주기 단계별 적용 방안과 통합 요구사항 관리 및 평가 방법론을 상세히 제시한다. 제4장 사례 연구 및 검증에서는 데이터 시뮬레이션을 통해 제안

된 통합 프레임워크의 효과성을 분석하고, 실제 다양한 무기체계 적용 시의 시사점을 도출한다. 제5장 결론 및 제언에서는 연구 결과를 종합적으로 요약하고, 도출된 결론을 바탕으로 국방 정책 및 제도 개선을 위한 구체적인 제언을 제시하며, 연구의 한계와 향후 연구 방향을 논한다.

2. 이론적 배경 및 현행 체계의 문제점 분석

2.1. 무기체계 보안의 개념 및 중요성

무기체계 보안은 일반적인 상용 정보 시스템 보안과 근본적으로 다른 차원의 개념과 중요성을 갖는다. 정보 시스템 보안의 전통적 목표가 기밀성(Confidentiality), 무결성(Integrity), 가용성(Availability)이라는 'CIA Triad'를 보호하는 데 있다면, 무기체계 보안은 이를 포함하면서도 '임무 보증(Mission Assurance)'과 '안전성(Safety)'을 최우선 가치로 고려해야 한다[1].

현대 무기체계의 복잡성과 네트워크 의존성 증가는 보안의 중요성을 더욱 증폭시키고 있다. 과거의 독립형 시스템과 달리, 현대 무기체계는 지휘통제체계(C4I), 데이터 링크, 위성 통신망 등과 유기적으로 연결된 '시스템의 시스템(System of Systems)'으로 작동한다. 이러한 초연결성은 작전 효율성을 극대화하지만, 동시에 하나의 취약점이 전체 시스템 붕괴로 이어질 수 있는 연쇄적 위험을 내포한다.

2.2. RMF와 Anti-Tamper의 개념 및 특성

위험관리 프레임워크(RMF)는 조직이 운영하는 정보 시스템과 그 안에 포함된 정보 자산에 대한 보안 위험을 식별, 평가, 관리하고, 그 결과를 바탕으로 시스템 운영을 공식적으로 승인하는 체계적이고 구조화된 프로세스를 의미한다[6]. RMF의 근본적 목적은 '위험 기반의 의사결정'을 통해 조직이 수용 가능한 수준으로 보안 위험을 관리하는 데 있다[2].

NIST SP 800-37에서 정의한 RMF는 7단계 프로세스로 구성된다: ①준비(Prepare), ②분류(Categorize), ③선정(Select), ④구현(Implement), ⑤평가(Assess), ⑥인가(Authorize), ⑦모니터링(Monitor). 각 단계는 순차적이면서도 반복적으로 수행되며, 시스템의 전 수명주기에 걸쳐 보안 활동을 체계적으로 안내한다[6,9].

K-RMF는 NIST RMF의 프로세스를 기본 골격으로 하되, 국내 국방 환경에 맞게 특화된 특성을 가진다[10]. 가장 큰 특징은 대한민국의 국방획득체계가 획득(방위사업청 주관)과 운용(각 군 주관)으로 이원화된 구조를 고려하여, 각 단계별 보안 활동의 주체를 명확히 정의했다는 점이다[10].

안티탬퍼(Anti-Tamper, AT)는 무기체계에 적용된 핵심 기술, 소프트웨어 알고리즘, 중요 데이터 등의 '중요 프로그램 정보(Critical Program Information, CPI)'가 적에게 탈취, 노획, 또는 분실되었을 경우, 비인가된 사용자가 역공학, 분석, 변조, 복제 등을 시도하는 것을 방지하거나 현저히 지연시키기 위해 적용되는 모든 시스템 공학적 조치를 총칭한다[8,26].

AT 기술은 방어 행위를 기준으로 억제(Deterrence), 방지(Prevention), 감지(Detection), 대응(Response)의 4단계로 분류되며, 적용 계층에 따라 하드웨어 기반과 소프트웨어 기반으로 나뉜다. 하드웨어 기반 AT는 TPM(Trusted Platform Module), 보호 메시(Mesh), 코팅(Potting) 등을 통해 강력한 물리적 보호를 제공하며, 소프트웨어 기반 AT는 코드 난독화, 안티-디버깅, 패킹 등을 통해 분석을 어렵게 만든다[12,21].

국내 AT 정책은 방위사업청을 중심으로 K-방산 수출 확대와 맞물려 점차 강화되는 추세에 있다. 수출용 무기체계에 대한 AT 기술 탑재가 의무화되고 있으며, AT 관련 연구개발 투자도 확대되

고 있다[5].

2.3. RMF와 Anti-Tamper의 비교 분석 및 현행 적용 한계

목적 및 범위 비교: RMF와 AT는 '보안'이라는 공통 목표를 추구하지만, 그 구체적 목적과 보호 대상의 범위에서 명확한 차이를 보인다. RMF의 주 목적은 '사이버보안 위험의 체계적 관리'에 있으며, 무기체계라는 하나의 '시스템'이 직면할 수 있는 모든 종류의 사이버 위협을 포괄적으로 다룬다[24]. 보호 대상은 시스템을 구성하는 하드웨어, 소프트웨어, 네트워크, 데이터 등 모든 자산이며, 보호의 목표는 이들 자산의 기밀성, 무결성, 가용성을 보장하는 것이다. 반면 AT의 주 목적은 '핵심 기술 및 중요 정보의 보호'에 있다[8]. 이는 무기체계가 적에게 노획되었을 때 발생할 수 있는 역공학, 불법 복제, 기술 분석과 같은 특정 위협 시나리오에 집중한다. 보호 대상은 무기체계의 모든 구성요소가 아니라, 사전에 식별된 CPI로 한정된다.

프로세스 및 방법론 비교: RMF는 NIST SP 800-37에 의해 표준화, 정형화된 프로세스를 따르며, 이 프로세스의 핵심은 '위험평가'에 기반한 합리적 의사결정이다[6,10]. Top-down 방식으로 전체적인 위험관리 전략 하에 개별 보안 요구사항을 도출하는 구조이다. AT는 RMF와 같이 국제적으로 표준화된 단일 프레임워크가 존재하지 않는다. 일반적으로 'CPI 식별 → 위협 분석 → AT 기법 선정 → 구현 → 검증'이라는 비정형적 절차를 따르며, 보호해야 할 핵심 기술에서 출발하여 필요한 보호 수단을 찾아가는 Bottom-up 방식의 성격이 강하다[13].

현행 적용상의 문제점 및 한계: RMF와 AT의 분리된 접근 방식은 여러 가지 구조적 문제점을 야기한다. 첫째, 프로세스 단절 및 중복으로 인한 비효율이다. 본질적으로 유사한 활동들이 중복적으로 수행되며, 개발자는 두 프로세스를 위해 별도의 위협 분석을 수행하고 서로 다른 문서를 작성해야 하는 비효율에 직면한다[11]. 둘째, 개발자 부담 가중 및 혼란 야기이다. 개발자 입장에서 RMF와 AT는 두 개의 상이한 '규제'로 인식되며, 이 두 요구사항 체계 간의 명확한 연관관계나 통합 가이드라인이 부재하여 개발 현장에서 큰 혼란이 발생한다[11]. 셋째, 보안 공백 발생 가능성이다. 두 체계의 분리는 각자의 사각지대를 만들어 보안 공백을 유발할 수 있으며, 진정한 의미의 보안은 이 두 관점이 유기적으로 결합될 때 완성될 수 있다. 다음 표는 RMF와 AT의 핵심 특징을 비교하고, 통합 시 고려해야 할 사항들을 정리한 것이다.

표 1. RMF와 Anti-Tamper 핵심 특징 비교

구분	RMF	Anti-Tamper	통합 시 고려사항
주목적	사이버보안 위험 관리 (시스템의 안전한 운용)	핵심기술 보호 (CPI의 안전한 보호)	시스템 운용성과 기술보호라는 두 목표의 균형점을 찾는 단일화된 보안 목표 설정 필요
보호 대상	시스템 전체 자산 (HW, SW, NW, 데이터 등)	중요 프로그램 정보 (CPI)	CPI를 시스템의 가장 중요한 자산으로 식별하고, RMF의 자산 분류 및 등급화 프로세스에 통합
접근 방식	Top-down (위험관리 전략 → 개별 통제)	bottom-up (보호대상 기술 → 보호기법)	두 접근법을 융합하여, 전체 시스템 관점에서 CPI 보호 전략을 수립하는 하이브리드 접근법 모색
주요 방법론	정형화된 6/7 단계 위험관리 프로세스	비정형적 기술 적용 (억제, 방지, 감지, 대응)	AT의 4단계 방어 행위를 RMF의 '보안통제항목'으로 정의하고, AT 적용 절차를 RMF 프로세스에 편입
적용 시점	전 수명주기 (기획 ~ 폐기)	주로 개발 단계 (설계, 구현)	AT 관련 활동을 RMF의 전 수명주기 단계(특히 기획, 모니터링)로 확장하여 연계 관리

핵심 주체	다수의 이해관계자 (정책, 인가, 사업, 개발, 평가, 운용 기관)	개발 주관기관 (방산업체, ADD)	RMF의 다중 이해관계자 거버넌스 내에서 AT 관련 역할과 책임을 명확히 정의
평가/ 검증	프로세스 준수 및 위협 수용 가능성 평가 (인가 획득)	기술적 방어 능력 및 유효성 검증	RMF의 '평가' 단계에서 AT 기법의 유효성 검증을 포함하는 '통합 시험평가' 방법론 개발

2.4. 선행 연구 검토 및 연구의 학술적 공백

RMF와 AT의 통합적 적용에 관한 연구는 국내외에서 아직 초기 단계에 머물러 있다. 미국 국방부에서는 'Technology and Protection Plan(TPP)'이라는 체계를 통해 사이버보안과 기술보호를 통합적으로 관리하려는 시도가 있었으나, 이는 정책적 수준의 통합에 그치고 있으며 개발 현장에서의 구체적인 방법론으로 발전되지는 못했다[25].

국내에서는 송경호 등(2021)이 '무기체계 안티탬퍼링을 위한 기술 식별 및 위험평가 방안'에서 위험관리 관점에서 AT를 적용하는 방안을 제시했으나, RMF와의 통합적 접근까지는 다루지 않았다[27]. 또한 이승목(2021)은 '국내 무기체계의 RMF 적용방안 연구: 무기체계 & 보안시스템 통합'에서 RMF의 무기체계 적용 방안을 연구했으나, AT와의 통합은 향후 연구 과제로 남겨두었다[11].

이처럼 RMF와 AT를 통합적으로 접근한 선행 연구는 매우 제한적이며, 특히 개발자 관점에서 두 체계를 효과적으로 융합하는 구체적인 방법론에 관한 연구는 찾아보기 어렵다. 이러한 연구 공백은 본 연구의 필요성과 학술적 기여도를 뒷받침한다.

3. 무기체계 개발자 관점의 통합 보안 프레임워크 제안

3.1. 통합 프레임워크의 개념 및 구성

제안하는 'RMF-AT 통합 보안 프레임워크'는 시스템 엔지니어링(SE) 사상을 기반으로 한다. SE는 복잡한 시스템을 구성하는 다양한 하위 시스템과 이질적인 요구사항들을 상호 연관된 전체의 관점에서 바라보고 최적의 균형점을 찾는 공학적 방법론이다[14]. 이러한 SE의 특성은 RMF라는 '프로세스 중심의 사이버보안 요구사항'과 AT라는 '기술 중심의 기술보호 요구사항'을 통합하는 데 최적의 철학적 토대를 제공한다.

아래 그림과 같이 통합 프레임워크는 현행 K-RMF의 6단계 프로세스라는 큰 틀을 유지하여 정책적 수용성을 높이되, 각 단계의 활동과 산출물에 AT 고유의 요구사항을 유기적으로 통합하는 형태로 구성된다. 이는 개발자에게 완전히 새로운 프로세스를 강요하는 것이 아니라, 기존의 익숙한 RMF 절차 내에서 AT를 자연스럽게 고려하도록 유도하기 위함이다.

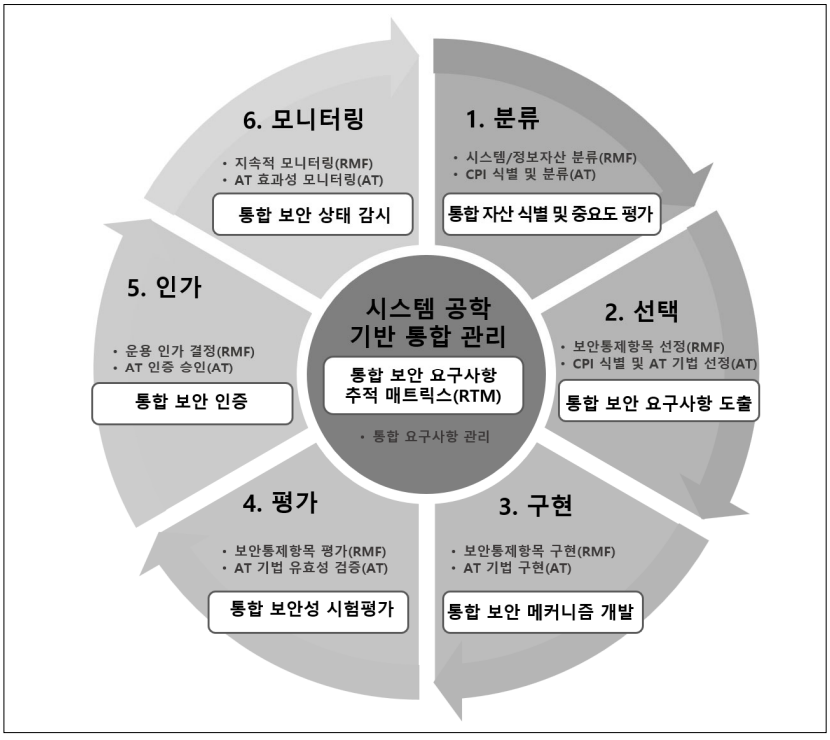

그림 1. RMF-AT 통합 보안 프레임워크 구성도

프레임워크는 다음 네 가지 핵심 원칙에 기반한다: ①단일화된 위험 관리, ②통합된 요구사항, ③수명주기 연계, ④개발자 중심. 이러한 원칙들을 통해 사이버 공격 위협과 기술 유출 위협을 단일화된 위험 관리 프로세스 내에서 통합적으로 분석하고, 모든 보안 요구사항을 '통합 요구사항 추적 매트릭스(Requirement Traceability Matrix, RTM)'라는 단일 창구를 통해 일관되게 관리한다.

3.2. 개발 생명주기 단계별 통합 적용 방안

3.2.1. 기획/요구사항 분석 단계

이 단계는 보안의 성패를 좌우하는 가장 중요한 시점으로, 'Shift Left' 원칙에 따라 개발 초기부터 RMF와 AT를 통합적으로 고려한다. 핵심 통합 활동으로는 통합 자산 식별 및 분류, 통합 위협 모델링, 통합 보안 요구사항 도출 및 테일러링이 있다.

통합 자산 식별 과정에서는 시스템의 정보 자산을 식별하고 CIA 등급을 분류하는 RMF 1단계 활동 시, 보호해야 할 CPI를 가장 핵심적인 정보 자산으로 식별한다. 통합 위협 모델링에서는 일반적인 사이버 공격 시나리오와 기술 유출 시나리오를 동시에 식별하며, 이를 위해 MITRE ATT&CK for Enterprise와 for ICS 프레임워크를 함께 활용한다[22].

주요 산출물로는 '통합 보안 계획서(Integrated Security Plan, ISP)' 초안과 '통합 요구사항 추적 매트릭스(RTM)' 초안이 있다.

3.2.2. 설계 및 구현 단계

설계 단계에서는 통합 보안 요구사항을 시스템의 아키텍처와 상세 설계에 구체적으로 반영한다.

보안 아키텍처 통합 설계와 인터페이스 보안 설계가 핵심 활동이며, RMF 통제를 위한 보안 기능과 AT 기법을 위한 보호 메커니즘을 연계하여 설계한다.

구현 단계에서는 시큐어 코딩 및 AT 기법 동시 구현과 보안 형상관리가 주요 활동이다. 개발자는 방위사업청의 시큐어 코딩 가이드라인을 준수하여 일반적인 코딩 취약점을 제거하는 동시에, 설계된 AT 기법을 소스코드에 직접 구현한다[16].

3.2.3. 시험/평가 단계

이 단계에서는 개발된 시스템이 통합 보안 요구사항을 만족하는지 종합적으로 검증한다. 통합 정적/동적 분석과 통합 모의 침투 테스트가 핵심 활동이며, 소스코드 정적 분석과 AT 기법 적용 여부를 동시에 점검한다.

레드팀이 수행하는 모의 침투 테스트 시나리오는 RMF와 AT 관점을 통합하여 구성되며, End-to-End 통합 시나리오를 통해 전체 방어 체계의 유기적 연동과 심층 방어 능력을 종합적으로 평가한다[23].

3.2.4. 운용/유지보수 단계

이 단계에서는 시스템이 전력화되어 실제 운용되는 단계로, 지속적인 보안 관리가 핵심이다. 통합 시험평가 결과 보고서를 바탕으로 평가 및 인가를 획득하며, 시스템을 운용하면서 새로운 사이버 위협과 새로운 AT 우회 기술 동향을 지속적으로 모니터링한다.

시스템의 패치, 설정 변경, 성능 개량 등이 발생할 경우, 이것이 기존의 RMF 통제와 AT 기능에 미치는 영향을 평가하고, 필요시 위험 재평가 및 보안 업데이트를 수행한다.

다음 표는 제안된 통합 프레임워크의 생명주기 단계별 활동을 요약하여 보여준다.

표 2. RMF-AT 통합 생명주기 활동 매트릭스

개발 생명주기	통합 RMF-AT 단계	핵심 통합 활동	주요 산출물
기획/ 요구사항	RMF 1, 2단계 통합	• CPI를 포함한 통합 자산 식별 및 분류 • 사이버/기술유출 위협 통합 모델링 • RMF 통제/AT 기법 통합 요구사항 도출 및 테일러링	• 통합 보안 계획서(ISP) 초안 • 통합 요구사항 추적 매트릭스(RTM) 초안
설계	RMF 3단계(설계)	• 보안 아키텍처 통합 설계 • RMF 통제와 AT 기법 연계 설계 • 인터페이스 보안 통합 설계	• 통합 보안 요구사항이 반영된 설계명세서 • 보안 요구사항이 명시된 ICD • 업데이트된 통합 RTM
구현	RMF 3단계(구현)	• 시큐어 코딩 및 AT 기법 동시 구현 • 보안 관련 형상항목의 통합 관리	• 보안 기능이 구현된 소스코드 및 실행 파일 • 업데이트된 통합 RTM
시험평가	RMF 4단계(평가)	• 통합 정적/동적 분석(SAST/DAST) • End-to-End 시나리오 기반 통합 모의침투 테스트	• 통합 시험평가 계획서 및 결과 보고서 • 최종 통합 RTM
운용/ 유지보수	RMF 5, 6단계 통합	• 통합 평가 결과 기반 시스템 운용 인가 • 신규 사이버 위협 및 AT 우회 기술 지속적 모니터링 • 변경 발생 시 통합 영향 분석 및 위협 재평가	• 지속적 모니터링 보고서 • 변경 영향 분석 보고서 • 재인가 평가 자료

3.3. 통합 보안 요구사항 도출 및 관리 방법

3.3.1. 위협 모델링(MITRE ATT&CK 등) 활용

위협 모델링은 시스템에 가해질 수 있는 잠재적 위협을 체계적으로 식별, 분석, 평가하는 구조화된 활동으로, MITRE ATT&CK 프레임워크가 강력한 도구 역할을 한다[22]. ATT&CK는 실제 관측된 공격 사례들을 기반으로 공격자들이 사용하는 전술, 기술, 절차를 방대하게 정리한 지식 베이스이다. 무기체계는 기업 IT 환경과 산업 제어 시스템의 특성을 모두 가지므로, ATT&CK for Enterprise와 ATT&CK for ICS를 함께 참조하여 통합적인 공격 시나리오를 구성할 수 있다[17]. 이를 통해 하나의 공격 흐름 속에서 필요한 RMF 통제와 AT 기법을 자연스럽게 연계하여 식별할 수 있다.

3.3.2. 통합 요구사항 추적 매트릭스(RTM) 구축

RTM(Requirement Traceability Matrix)은 요구사항과 그와 관련된 설계 문서, 소스코드, 테스트 케이스 등 모든 개발 산출물 간의 관계를 양방향으로 연결하여 보여주는 핵심적인 시스템 엔지니어링 도구이다[19]. 통합 RTM은 식별된 위협에서부터 시작하여 최종 검증 결과까지 모든 과정을 추적한다. 통합 RTM의 구성요소는 위협 정보, 요구사항 정보, 설계/구현 정보, 검증 정보를 포함하며, 영향 분석, 커버리지 분석, 보안 공백 식별 등의 강력한 이점을 제공한다.

3.4. 통합 평가 및 검증 방안

통합 평가 및 검증의 핵심은 RMF의 보안통제항목 준수 여부를 확인하는 '컴플라이언스 관점'의 평가와, AT 기법의 방어 능력을 확인하는 '유효성 관점'의 검증을 분리하지 않고 동시에 수행하는 것이다[18]. 이는 하나의 시험 시나리오 내에서 두 가지 측면을 모두 확인하는 '통합 보안성 시험평가' 개념을 도입하는 것을 의미한다.

실제 공격자의 관점에서 시스템의 취약점을 찾는 레드팀 활동을 적극 활용하며, 레드팀의 공격 시나리오는 RMF와 AT의 관점을 통합한 End-to-End 형태로 구성된다. 이러한 통합 시나리오 기반의 검증을 통해 개별 보안 기능의 성능을 넘어, 각기 다른 보안 메커니즘들이 상호작용하며 만들어내는 전체 시스템의 방어 능력을 종합적으로 평가할 수 있다.

4. 사례 연구 및 검증

4.1. 데이터 시뮬레이션을 통한 정량적 효과 분석

무기체계 개발 프로젝트의 민감성으로 인해 실제 데이터를 확보하는 데 현실적 제약이 따르므로, 본 연구는 방위산업 및 보안 전문가 자문을 통해 도출된 경험적 가정치와 논리적 추론에 기반한 시뮬레이션 모델을 구축하였다. 이 모델은 제안 프레임워크가 복잡도에 따라 어떤 성능적 우위를 가지는지를 논리적으로 입증하는 데 목적을 둔다. 향후 시범사업을 통해 본 모델의 타당성을 검증하고 실제 데이터를 확보하는 것을 연구 과제로 제안한다.

아래 그림은 프로젝트 복잡도(50 가정)에 대한 개발 효율성, 보안성, 적용 용이성 지표를 중심으로 기존 분리 방식과 제안된 통합 방식을 비교 분석한 결과이다. 시뮬레이션 모델에서 사용된 변수와 기본 수치, 그리고 기존 방식과 제안 방식의 측정값 계산식을 함께 제시하였다.

시뮬레이션 결과, 제안된 통합 프레임워크는 프로젝트 복잡도 전반에 걸쳐 기존 방식 대비 월등

한 성능 우위를 보이는 것으로 나타났다.

첫째, 개발 효율성 측면에서 통합 프레임워크는 기존 방식과 비교해 평균 20% 이상의 향상을 보였다. 이는 프로세스 중복 제거와 요구사항 상충 해소를 통해 낭비되는 자원을 최소화한 결과로 해석할 수 있다. 둘째, 보안성 지표는 통합 프레임워크가 기존 방식 대비 평균 30% 이상의 높은 성능을 유지하는 것으로 나타났다. 이는 사이버 위협과 기술 유출 위협을 통합된 관점에서 관리함으로써, 분리된 체계에서는 놓칠 수 있는 복합적 보안 공백을 효과적으로 메웠음을 시사한다. 셋째, 프로젝트 복잡도가 증가할수록 제안 프레임워크의 성능적 우위는 더욱 두드러진다. 특히, 복잡도가 80을 초과하는 고난도 프로젝트에서는 기존 방식의 효율성 및 보안성이 급격히 저하되는 반면, 통합 프레임워크는 상대적으로 안정적인 성능을 유지하며 통합의 시너지를 입증하였다. 이는 복잡한 현대 무기체계 개발 환경에 제안 프레임워크가 최적화되어 있음을 보여준다.

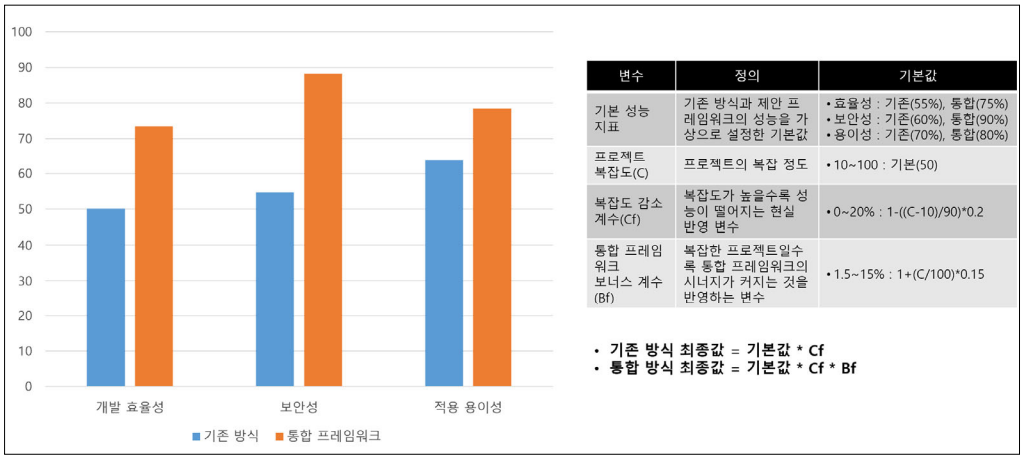

그림 2. 기존 방식 대비 성능 시뮬레이션 비교

4.2. 효과성 분석 및 평가

다음 표는 보안 전문가와 무기체계 개발자의 인터뷰를 통해 기존 방식과 통합 프레임워크의 효과성을 정성적 측면에서 항목별로 비교 분석한 결과이다. 이는 정량적 지표와 함께 논리적 분석을 결합하여 프레임워크의 총체적 우수성을 입증하기 위함이다. 기대 효과는 실제 무기체계에 제안된 통합 프레임워크를 사용됨으로써 얻는 실질적인 효과의 타당성을 입증하였다.

표 3. 접근 방식별 효과성 비교 분석

평가 항목	기존 방식(분리 접근법)	통합 프레임워크(제안 방식)	기대 효과
요구사항 관리	• RMF/AT 요구사항 별도 관리 • 요구사항 간 연관성/상충 파악 어려움	• 통합 RTM을 통한 단일 관리 • 양방향 추적성 확보로 연관성/상충 조기 식별	• 요구사항 누락 및 왜곡 방지 • 변경 관리 효율성 증대
위협 분석	• 사이버 위협, 기술 유출 위협 별도 분석 • 중복 활동 발생, 분석 범위 제한적	• 통합 위협 모델링(MITRE ATT&CK 활용) • 복합적/연계 위협 시나리오 식별	• 분석 비용/시간 절감 • 보안 사각지대 최소화

개발/보안 연계	• 개발 후반부 보안 검증 집중 (Bolt-on) • 개발자와 보안팀 간의 단절	• 개발 초기부터 보안 내재화 (Security by Design) • DevSecOps 연계로 지속적 자동 검증[20]	• 보안 품질 향상 • 개발-보안-운영 협업 강화
시험/평가 (T&E)	• 기능별/단편적 테스트 • RMF 평가, AT 검증 분리 수행	• End-to-End 시나리오 기반 통합 테스트 • RMF/AT 유효성 동시 검증	• 재작업 및 추가 개발 공수 감소 • 인가 획득 기간 단축
총 개발 비용/기간	• 중복 활동, 재작업으로 인한 비용/기간 증가	• 프로세스 효율화로 비용/기간 절감	• 획득 예산 효율적 사용 • 적기 전력화 기여
총체적 보안 수준	• 개별 보안 기능의 합 • 보안 공백 발생 가능성 존재	• 기능 간 시너지를 통한 총체적 보안 • 심층 방어 (Defense-in-Depth) 강화	• 무기체계 생존성 및 임무 보증 능력 극대화

4.3. 다양한 플랫폼 적용 가이드라인

본 연구의 제안 프레임워크는 가상의 무기체계를 중심으로 설계되었으나, 그 근간이 되는 시스템 엔지니어링 및 통합 보안 개념은 다양한 무기체계 플랫폼에도 적용될 수 있다. 따라서 유도무기, 함정, 항공기, 전차 등 대표적인 플랫폼별 특성을 고려한 적용 가이드라인을 제시함으로써 프레임워크의 범용성과 확장성을 입증한다.

각 플랫폼은 운영 환경, 위협 모델, 핵심 기능에서 상이한 특징을 갖는다. 따라서 통합 프레임워크를 적용할 때에는 각 플랫폼의 고유한 특성을 반영한 맞춤형 전략이 필수적이다. 아래 표는 주요 무기체계 플랫폼별 핵심 보안 요구사항과 RMF-AT 통합을 통해 얻을 수 있는 시너지를 정리한 것이다. 각 플랫폼의 고유한 보안 요구사항을 RMF와 AT의 통합된 관점에서 분석하고 대응하면, 기존의 분리된 접근법으로는 해결하기 어려웠던 복합적 위협에 효과적으로 대응할 수 있다. 예를 들어, 함정의 전투체계 네트워크에 대한 위협은 RMF의 네트워크 보안 통제와 AT의 핵심 데이터 암호화 기술을 통합함으로써 더욱 견고하게 방어할 수 있다. 이처럼, 본 프레임워크는 특정 무기체계 국한되지 않고, 각 플랫폼의 특성을 고려한 맞춤형 적용 전략을 통해 광범위한 국방 무기체계 개발 분야에 적용될 수 있는 높은 범용성을 지닌다.

표 4. 주요 무기체계 플랫폼 별 적용 가이드라인

플랫폼	핵심 보안 요구사항	통합 시너지
유도무기	• 실시간성, 정밀타격, 데이터링크 보안	• 표적정보 암호화 및 무결성 강화 • 비행 중 재밍(Jamming) 공격 및 탈취 시도에 효과적 대응
함정	• 전투체계 네트워크, 위성 통신 보안	• 망분리 아키텍처 강화 및 주요 장비에 대한 접근통제 연계 • 복잡한 네트워크 환경에서 보안 취약점 노출 최소화
항공기	• 항공전자 시스템, 임무 데이터 보호	• 핵심 소프트웨어 역공학 방지 및 무결성 보장 • 비행 제어 및 임무 컴퓨터의 논리적/물리적 무결성 확보
전차	• 사격통제장치, 피아식별장비 보안	• 하드웨어 기반 암호화 및 무효화 기술 연계 • 주요 전자 장비에 대한 물리적 탈취 및 분석 시도에 대비

5. 결론 및 제언

5.1. 연구 결과 요약

본 연구는 현재 무기체계 보안이 사이버보안(K-RMF)과 기술보호(Anti-Tamper)라는 두 개의 상이한 정책 및 기술 체계로 이원화되어 관리되고 있음을 확인하였다. 이러한 분리된 접근 방식은 개발 현장에서 프로세스 중복, 요구사항 상충, 개발자 혼란 가중, 잠재적 보안 공백 발생 등 다양한 문제점을 야기하고 있다.

이러한 문제점을 근본적으로 해결하기 위해, 본 연구는 시스템 엔지니어링 사상을 기반으로 RMF와 AT를 유기적으로 융합하는 'RMF-AT 통합 보안 프레임워크'를 제안하였다. 제안된 프레임워크는 단일화된 관리 체계, 전 수명주기 보안 내재화, 실용적인 통합 방법론 제시라는 핵심 특징을 가진다.

정량적, 정성적 비교 평가를 통해, 제안된 통합 프레임워크가 기존의 분리된 접근 방식에 비해 개발 효율성, 보안성, 적용 용이성 측면에서 명백한 우위를 가짐을 검증하였다.

5.2. 정책적 제언

본 연구에서 제안한 'RMF-AT 통합 보안 프레임워크'가 대한민국 국방 환경에 성공적으로 안착하기 위해서는 이를 뒷받침하는 정책적·제도적 개선이 필수적이다.

1) 「국방 사이버보안 위험관리 지시(K-RMF)」의 개정 및 고도화: 현행 K-RMF 지침 내에 '기술보호'를 RMF가 포괄해야 할 주요 보안 영역으로 명시적으로 추가하고, RMF 프로세스의 일부로서 AT 활동이 공식적으로 수행되도록 제도화해야 한다[10]. 이를 통해 개발자는 두 개의 별도 지침이 아닌 단일화된 규정을 따르게 되어 업무 혼란이 크게 줄어들 것이다.

2) 「무기체계 소프트웨어 개발 및 관리 매뉴얼」 개정: '통합 보안 계획서(ISP)'와 '통합 요구사항 추적 매트릭스(RTM)'를 무기체계 개발 시 필수 제출 산출물로 지정해야 한다[15]. 특히, RTM을 필수 산출물로 지정하면 요구사항 누락 및 왜곡을 방지하고, 변경 관리의 효율성을 증대시킬 수 있다. 이는 실제 개발 과정에서 발생할 수 있는 비효율을 근본적으로 줄이는 효과적인 방안이다.

3) 통합 가이드라인 개발 및 전문 교육 프로그램 신설: 개발자들이 제안된 프레임워크를 쉽게 이해하고 실제 프로젝트에 적용할 수 있도록 상세한 'RMF-AT 통합 적용 가이드라인'을 개발하여 보급해야 한다. 또한, 방위사업청, 국방부 등 관련 기관이 협력하여 역할 기반의 전문 교육 과정을 운영함으로써, 실무 담당자의 역량을 강화하고 프레임워크의 성공적인 정착을 지원해야 한다.

4) 시범사업 추진을 통한 실증적 효과 검증: 본 연구에서 제시한 프레임워크의 효과성을 정량적으로 입증하기 위해 국방부 또는 방위사업청 주관의 시범사업을 추진해야 한다. 시범사업을 통해 개발 공수, 결함 발견율, 재작업률 등의 실증 데이터를 수집하고, 이를 바탕으로 프레임워크의 경제적 타당성(비용-효과 분석)을 객관적으로 입증할 수 있다. 이는 정책 결정자들이 통합 프레임워크 도입을 결정하는 데 필수적인 근거가 될 것이다.

5.3. 연구의 한계 및 향후 연구 방향

본 연구는 다음과 같은 한계를 가진다. 첫째, 실증 데이터의 부재이다. 제안된 프레임워크를 실제 무기체계 개발 프로젝트에 적용하여 개발 효율성 향상도나 보안성 강화 수준을 정량적으로 측정한 실증적 데이터를 확보하지 못했다. 둘째, 조직 문화 및 거버넌스 측면의 도전과제 분석이 부족하다. 제안된 프레임워크의 성공적 적용을 위해서는 기술적 측면뿐만 아니라 조직 문화, 인력 역

량, 거버넌스 체계 등의 변화가 필요하나, 이에 대한 심층적 분석이 이루어지지 못했다. 셋째, 비용-효과 분석의 한계가 있다. 통합 프레임워크 도입에 따른 초기 투자 비용과 장기적 효과에 대한 경제성 분석이 수행되지 않아, 정책 결정자들의 의사결정을 지원하기에는 한계가 있다.

향후 연구 방향으로는 실증적 적용 및 효과성 검증 연구, 통합 프레임워크 지원 자동화 도구 개발, 미래 신기술 대응을 위한 프레임워크 확장 연구가 필요하다. 특히 국방부 또는 방위사업청 주관의 시범사업을 통해 실제 무기체계 개발 프로젝트에 통합 프레임워크를 적용하고, 이를 통해 개발 공수, 결함 발견율, 재작업률 등의 데이터를 수집하여 프레임워크의 효과성을 정량적으로 측정하는 후속 연구가 시급하다.

무기체계 보안에 대한 패러다임을 '분리'에서 '통합'으로 전환하고, 개발 효율성과 보안성이라는 두 마리 토끼를 동시에 잡을 수 있는 실질적 대안을 제시한 본 연구가 향후 대한민국 국방 무기체계의 보안 수준을 한 단계 끌어올리는 데 중요한 이론적, 실무적 기반이 되기를 기대한다.

참고문헌

[1] 정성욱. 무기체계 사이버 보안 강화를 위한 보안정책 및 정보보호 관리체계. 제주대학교 대학원, 박사학위논문. 2022.

[2] 김재우, 정석재. 한국형 위험관리체계(KRMF)의 성공을 위한 첫걸음: 시스템 분류 방향 연구. 선진국방연구, 제5권 제2호, pp. 73-106. 2022.

[3] 보안뉴스. [한국의 사이버 안보전략 토론문-1] 국방사이버안보전략의 현황과 과제. https://www.boannews.com/media/view.asp?idx=134060 (검색일 2025. 6. 21).

[4] 방위사업청. 2024 방위사업청 주요 정책 추진계획 : K-방산을 안보의 기반과 신성장 동력으로 육성한다!. 2024.

[5] 방위사업청. 2022~2026 방위산업기술보호 종합계획. 2021.

[6] NIST. Risk Management Framework for Information Systems and Organizations. NIST SP 800-37 Rev 2. 2018.

[7] 국방부. 국방 사이버보안 위험관리 지시. 2024. 4. 12 시행.

[8] 김민욱. 안티탬퍼링의 동향 및 발전 방향 연구. 한국산학기술학회논문지, 제24권 제9호, pp. 82-88. 2023.

[9] 황재윤, 권혁진. 국방 사이버보안을 위한 RMF-CMMC 공통규정준수 메타모델 개발방안 연구. 인터넷정보학회논문지, 제25권 제1호, pp. 123-136. 2024.

[10] 양우성 등. 국방획득체계 적용 한국형 보안위험관리 프레임워크. 정보보호학회논문지, 제32권 제6호, pp. 1183-1192. 2022.

[11] 이승목. 국내 무기체계의 RMF 적용방안 연구: 무기체계 & 보안시스템 통합. 선진국방연구, 제4권 제3호, pp. 191-208. 2021.

[12] 이재호 등. TPM 기반 안티탬퍼링 솔루션을 통한 무기체계 기술 보호. 전자통신동향분석, 제39권 제5호, pp. 49-60. 2024.

[13] 이민우, 이재천. 무기 시스템 개발에서 기술보호를 위한 위험관리 기반의 Anti-Tampering 적용 기법. 한국산학기술학회논문지, 제19권 제12호, pp. 99-109. 2018.

[14] 방위사업청. 연구개발사업의 체계공학(SE) 기반 기술관리업무 실무지침서. 2012.

[15] 류지선, 양재형. ISO/IEC 25023을 활용한 무기체계 소프트웨어 보안성 확보 방안. 한국산학기술학회논문지, 제22권 제12호, pp. 89-94. 2021.

[16] 방위사업청. 무기체계 소프트웨어 개발 및 관리 매뉴얼. 방위사업청 매뉴얼 제2022-6호 (개정 : 2022.12.2.).

[17] 최승오, 김형천. MITRE ATT&CK 프레임워크 기반 에너지분야 기반시설 보안 모니터링 방안. 정보보호학회지, 제30권 제5호, pp. 13-23. 2020.

[18] USD R&E. Test and Evaluation Enterprise Guidebook. Defense Business System Acquisition Pathway. 2022.

[19] Altium. 요구 사항 추적성 행렬이란 무엇인가?. https://resources.altium.com/kr/p/requirements-t

raceability-matrix (검색일 2025. 6. 21).

[20] 이글루코퍼레이션. 개발의 전주기에 보안을 고려한 DevSecOps의 이해와 구현방법. https://www.igloo.co.kr/security-information/%EA%B0%9C%EB%B0%9C%EC%9D%98-%EC%A0%84%EC%A3%BC%EA%B8%B0%EC%97%90-%EB%B3%B4%EC%95%88%EC%9D%84-%EA%B3%A0%EB%A0%A4%ED%95%9C-devsecops%EC%9D%98-%EC%9D%B4%ED%95%B4%EC%99%80-%EA%B5%AC%ED%98%84%EB%B0%A9/ (검색일 2025. 6. 21).

[21] 국방기술진흥연구소. 무기체계 기술 보호를 위한 안티탬퍼링 적용 방안 제언. 2023.

[22] 서석호 등. MITRE 프레임워크 기반 무기체계 사이버 능력 확보 방안 연구. 한국산학기술학회논문지, 제25권 제6호, pp. 230-238. 2024.

[23] QINETIQ. Modernising Test & Evaluation for Weapons and Munitions. https://www.qinetiq.com/-/media/0493beec834446b7af7a6c297ee3d73b.ashx (검색일 2025. 6. 21).

[24] GAO, Weapon Systems Cybersecurity: DOD Just Beginning to Grapple with Scale of Vulnerabilities. 2018.

[25] DoD. Technology and Program Protection Guidebook. 2022.

[26] DoDD. Anti-Tamper (AT). 5200.47E. 2022.

[27] 송경호 등. 무기체계 안티탬퍼링을 위한 기술 식별 및 위험평가 방안. 한국방위산업학회지, 제28권 제2호, pp. 41-49. 2021.