Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.33, NO.5, Oct. 2023 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2023.33.5.827

무기체계 개발을 위한 한국형 국방 RMF 구축 방안 연구*

안 정 근,[1†] 조 광 수,[1] 정 한 진,[2] 정 지 훈,[2] 김 승 주[3‡]
[1,3]고려대학교 (대학원생, 교수), [2]한화시스템 (연구원)

A Study on Constructing a RMF Optimized for Korean National Defense for Weapon System Development*

Jung keun Ahn,[1†] Kwangsoo Cho,[1] Han-jin Jeong,[2] Ji-hun Jeong,[2] Seung-joo Kim[3‡]
[1,3]Korea University (Graduate student, Professor), [2]Hanwha System (Researcher)

요 약

외부와 연결되지 않고 독립적으로 운용되던 무기체계에 최근 네트워크 통신, 센서와 같은 다양한 정보기술이 접목되기 시작하였다. 이는 무기체계 운용자 및 지휘관의 신속하고 정확한 결심과 효과적인 무기체계 운용을 가능하게 한다. 하지만, 무기체계의 사이버 영역 활용이 증가함에 따라 사이버 공격에 의한 피해도 증가할 것으로 예상된다. 안전한 무기체계를 개발하기 위해서는 소프트웨어 개발 단계 중 요구사항 도출 단계에서부터 보안적 요소를 고려하는 보안 내재화를 구현하는 것이 필요하다. 미 DoD는 '사이버보안(cybersecurity)' 개념의 도입과 함께 무기체계 평가 및 획득 프로세스인 RMF A&A를 시행하고 있으며, 우리나라도 K-RMF 제도 시행을 위한 노력을 지속하고 있다. 하지만, 아직까지 개발 단계에서부터 K-RMF를 적용한 사례는 존재하지 않을뿐더러 미국의 국방 RMF 관련한 자료는 기밀 사항이기에 대부분 공개되지 않는다. 본 연구에서는 RMF와 관련하여 공개된 자료와 체계적인 위협 분석 방법을 바탕으로 우리나라의 국방용 RMF인 K-RMF를 예측하여 무기체계의 보안 통제항목을 구축하는 방안에 대해 제안하고, 함정 전투체계에 적용함으로써 그 효용성을 입증한다.

ABSTRACT

Recently, various information technologies such as network communication and sensors have begun to be integrated into weapon systems that were previously operated in stand-alone. This helps the operators of the weapon system to make quick and accurate decisions, thereby allowing for effective operation of the weapon system. However, as the involvement of the cyber domain in weapon systems increases, it is expected that the potential for damage from cyber attacks will also increase. To develop a secure weapon system, it is necessary to implement built-in security, which helps considering security from the requirement stage of the software development process. The U.S. Department of Defense is implementing the Risk Management Framework Assessment and Authorization (RMF A&A) process, along with the introduction of the concept of cybersecurity, for the evaluation and acquisition of weapon systems. Similarly, South Korea is also continuously making efforts to implement the Korea Risk Management Framework (K-RMF). However, so far, there are no cases where K-RMF has been applied from the development stage, and most of the data and documents related to the U.S. RMF A&A are not disclosed for confidentiality reasons. In this study, we propose the method for inferring the composition of the K-RMF based on systematic threat analysis method and the publicly released documents and data related to RMF. Furthermore, we demonstrate the effectiveness of our inferring method by applying it to the naval battleship system.

Keywords: Risk Management Framework, Threat Modeling, Weapon System, K-RMF, Security Control

Received(08. 16. 2023), Modified(09. 04. 2023), Accepted(09. 05. 2023)
* 본 연구는 2022년도 한화시스템㈜의 재원을 지원받아 수행되었습니다.
† 주저자, stable_root@korea.ac.kr
‡ 교신저자, skim71@korea.ac.kr(Corresponding author)

I. 서 론

소총, 기관총 등 전통적인 개인화기, 공용화기 뿐 아니라 전차 및 야포 등 근대 이후 등장한 무기체계의 경우에도 비교적 최근에 이르기까지 외부와 연결되지 않은 독립적인 시스템으로 구성되어 있었다. 현대에도 다수의 무기체계는 외부와 연결되지 않은 시스템으로 구성되어 있으나, 신속한 상황인식 및 결심 등 지휘통제 능력 강화와 여러 무기체계의 상호 간 정보 교류 등을 위해 네트워크로 연결되기 시작하였다. 외부와의 접촉 표면이 확대되고 다양한 정보기술이 적용됨에 따라 공격자가 무기체계에 침투할 수 있는 경로도 확대되었으며, 사이버 공격에 의한 정보 유출, 데이터 변조 등의 가능성도 증가하였다. 전시 적을 타격하고 정찰하는 등 주요 임무 수행에 필요한 무기체계는 위기 상황에서도 정상적인 임무를 수행할 수 있도록 보호되어야 하는 바, 무기체계에 대한 사이버보안의 중요성이 대두되고 있다[1]. 미 DoD(Department of Defense)는 사이버 위협으로부터 안전한 무기체계 및 정보체계를 획득하기 위한 평가 수단으로 1985년 TCSEC(Trusted Computer System Evaluation Criteria)으로부터 시작하여 현재의 국방용 RMF(Risk Management Framework)인 RMF A&A(RMF Assessment & Authorization)까지 이르는 다양한 제도를 발전시키며 사용하고 있다[2].

RMF 이전의 평가 수단은 특정 보안 등급을 달성하기 위해 그 등급에 요구되는 모든 평가 기준을 충족할 것을 일률적으로 요구하였다. 하지만, RMF는 기존의 평가 수단과는 달리 시스템에 대한 위험이 임무 수행에 미치는 영향의 정도에 초점을 맞추어 시스템이 정상적으로 임무를 수행할 수 있도록 위험을 제거하거나 완화하는 것을 목표로 한다[3].

RMF의 개념을 처음 창시한 미국의 경우, 국방 분야에선 DoD에서 관리하는 RMF A&A, 연방정부 분야에선 NIST(National Institute of Standards and Technology)에서 관리하는 연방정부용 RMF가 존재한다. 연방정부용 RMF는 2010년 발표된 NIST SP 800-37 Rev.1에서 미국 내 표준으로 지정되어 현재 미 연방정부 소속 기관에서 도입하는 모든 정보체계에 적용하고 있다. 해당 연방정부용 RMF는 관련 문서가 모두 민간 영역에 공개되어 있고, 특히 모든 보안 통제항목의 목록 및 세부내용 또한 NIST SP 800-53 Rev.5에 상세히 기술되어 있다. 하지만, 무기체계를 개발 및 획득하는데 적용해야 하는 것은 연방정부용 RMF가 아닌 DoD에서 관리하는 RMF A&A이다. DoD는 NIST와 달리 RMF A&A에 대한 문서 및 보안 통제항목 등을 민간 영역에 공개하지 않고 있다. DoD 산하기관인 DCSA(Defense Counterintelligence and Security Agency)에서 발행한 평가 및 인가 프로세스 메뉴얼(DAAPM, DCSA Assessment and Authorization Process Manual)[4]에 극히 일부의 보안 통제항목 baseline이 제시되어 있을 뿐이다.

2015년 DoD에서는 국방 사이버 전략을 발표하였으며, 국방 사이버 전략 내 목표 중 한 가지로 동맹국의 사이버보안 역량 강화를 포함하였다[5]. DoD에서는 전략 구현의 일환으로 우리나라를 포함한 동맹국들 중 미군의 무기체계와 직간접적으로 연동되는 무기체계 운용 국가에 대해 RMF 적용을 요구한 바 있다. 미국과 우리나라는 제도적 기반과 기존 구축된 보안 수준이 상이하기 때문에 미국의 RMF A&A를 그대로 도입할 수는 없다[6]. 이에 우리나라에서도 미국의 RMF를 벤치마킹하여, 무기체계에 적용 가능한 국방 사이버보안위험관리제도인 K-RMF(Korea-RMF)를 개발하고 있으나, 현재까지는 해당 제도와 관련하여 공개된 공식 문서가 존재하지 않는다.

본 연구에서는 향후 무기체계 개발 시 적용해야 할 K-RMF에 대비하기 위해 체계적인 위협 분석 방법과 연방정부용 RMF 및 극히 일부 공개된 DoD RMF A&A의 정보를 이용하여 무기체계를 위한 한국형 국방 RMF의 구축 방안을 제안한다. 또한, 본 연구에서 제안한 방법을 검증하기 위해 한 화시스템의 함정 전투체계를 대상으로 이를 모의 적용하였다.

본 논문의 이후 부분들은 다음과 같이 구성되어 있다. 2장에서는 RMF와 관련된 표준 및 규정, 민간 영역 및 국내에서의 위험관리 연구에 관한 동향을 설명한다. 3장에서는 RMF의 개념 및 수행 절차에 대한 개요를 설명한다. 4장에서는 본 논문의 주요 아이디어인 한국형 국방 RMF의 구축 방안을 설명하고, 5장에서는 이를 함정 전투체계에 적용하여 그 효과를 검증한다. 이후 6장에서는 결론 및 향후 연구되어야 할 내용을 제시하고 마무리한다.

II. 관련 연구

2.1 RMF와 관련된 표준

미국의 정보보호 인증 및 인가 제도는 1985년 TCSEC으로부터 시작하였다. 이후 TCSEC은 유럽의 ITSEC(Information Technology Security Evaluation Criteria)과 통합하여 국제 표준인 CC(Common Criteria)로 발전하였다. 그러나 CC는 실험실 수준의 평가란 한계가 존재하였다[7]. 이에 DoD는 이러한 한계를 극복하고, 더불어 무기체계의 전 개발 프로세스에 대한 보안성 평가를 통해 군에서 사용하는 체계를 안전하게 획득하고자 DITSCAP(DoD Information Technology Security Certification and Accreditation Process)을 제정하였다. 이후 DITSCAP은 DIACAP을 거쳐 현재에 이르러서 RMF로 발전되었다. 2014년 DoD는 훈령(DoDI) 8500.01과 8510.01을 발표하였다. DoDI 8500.01에서는 정보보증의 개념을 사이버보안(cybersecurity)으로 대체하고 위험 관리를 위해 NIST SP 800-37을 사용할 것을 명시하였으며, 8510.01에서는 NIST SP 800-37에 따른 RMF 적용 방법과 각 과업의 주 책임자를 명시하고 무기체계 획득 관리 시스템과 RMF를 통합하였다. 비록 RMF A&A와 연방정부 RMF의 관리 기관은 상이하나 동일한 원리와 절차를 통해 시스템의 보안성을 확보하고자 하기에 상호평가 결과를 재사용할 수 있는 상호호혜성의 원칙이 적용된다. 이는 RMF 이전 연방정부와 DoD에서 각각 사용하던 NIACAP과 DIACAP이 상호 평가 결과를 사용할 수 없던 문제를 해결하였다[2]. 한편, 미국에서는 한국, 일본 등 자국의 무기를 운용하거나 자국의 무기체계와 연동된 무기체계를 운용하고 있는 국가에 대해서도 RMF를 적용할 것을 요구하고 있으며, 특히 우리나라의 연합지휘통제체계에 대해서는 지휘통제 상호운용성위원회(CCIB, Command and Control Interoperability Board) 간 RMF를 이용하여 보안평가를 실시할 것을 요구하였다. 이를 토대로 2023년 6월에는 주한미군사와 한국합참 간 사이버보안 공동지침에 관한 합의각서를 교환하였으며, 양 기관은 한미간 지휘통제체계의 안정적 연동을 위해 상호 평가 결과를 신뢰 및 공유하는 것에 동의하였다[8].

2.2 RMF와 관련된 민간 영역 동향

미국을 비롯한 각국의 세계적인 주요 방위산업체 또한 방위사업 기술에 대한 사이버 공격에 대응하기 위해 RMF를 기반으로 하는 사이버보안 프레임워크를 독자적으로 개발하여 운영하고 있다.

미국의 대형 방위사업체인 Lockheed Martin은 2019년 무기체계의 사이버 복원력(cyber resilience) 성숙도 평가를 위한 프레임워크인 CRL(Cyber Resiliency Level)과 사이버 복원력 성숙도 평가 도구인 CRS(Cyber Resiliency Scoreboard)를 개발하였다. 사이버 복원력은 '효과적인 임무 수행 능력을 위해 필요한 기능을 유지하기 위해 환경 변화를 예측하고, 이를 견디고, 복구하고, 변화에 적응하는 능력'을 의미한다[9]. CRL은 ▲시스템의 현재 복원력 수준 식별, ▲사이버 위험 평가, ▲투자를 통해 증가하는 사이버 복원력 수준 평가, ▲투자안(案) 우선순위 결정의 순서로 수행된다. CRL을 사용함으로써 무기체계의 사이버 영역에 대한 투자의 비용-효과 분석을 통해 비용 대비 최대 효과를 얻을 수 있는 투자 영역을 선택할 수 있다.

미국의 또 다른 방위사업체인 Northrop Grumman은 사이버보안 아키텍처 평가 모델인 Fan과 사이버보안 역량 평가 프레임워크인 CyCape를 사용하고 있다. 이 도구들을 사용함으로써 시스템 내에서 정보의 흐름을 시각화할 수 있으며, 사이버보안 아키텍처를 분석하여 그 효과와 능력을 평가할 수 있다[10]. 이를 통해 시스템에 발생할 수 있는 사이버보안 위험을 체계적으로 분석하고 관리하여 안전한 시스템을 만들 수 있다.

영국의 방위사업체인 BAE Systems는 2018년 주요 문서를 포함한 데이터 관리 및 저장과 협업 기능을 제공하는 Epiphany를 도입하였다. 이는 NIST SP 등 여러 표준에 따른 문서를 자동으로 작성할 수 있게 하며, 무기체계 개발과 관련된 민감 정보를 안전하게 처리, 저장, 전송할 수 있는 보안기능을 제공한다[11].

Boeing은 SMIS(Security Monitoring Infrastructure System)라는 네트워크 보호 시스템을 운영하고 있다. SMIS는 NIST의 RMF 보안통제 항목을 모두 충족하도록 설계 및 구현되었으며, 침입탐지 시스템, 이벤트 관리 시스템, 트래픽 분석 도구 등이 통합된 시스템으로, 네트워크의 모든 트래픽을 실시간으로 감시 및 분석하며 경보를 제공하고 필요시 패킷

기록을 분석하는 등 포렌식 기능을 제공한다[12].

다수의 방위산업체에서 위험관리를 위한 도구와 프레임워크를 개발 및 사용 중이지만, 이는 상용 제품으로 관련 상세자료들이 공개되지 않는다. 또한, 공개된 자료만을 바탕으로 RMF를 준수하기에는 추상화된 정보만 제공되는 등의 어려움이 존재한다. 이러한 어려움을 해결하기 위해 공개된 자료 바탕의 RMF의 각 단계 수행 방안에 대한 상세 절차를 다루는 연구가 필요하다.

2.3 RMF와 관련된 국내 동향

한편, 국내에서도 무기체계에 대한 RMF 적용에 관한 연구가 수행되고 있다. 2016년 대한민국 합동참모본부에서는 첨단 무기체계에 대한 사이버보안의 중요성이 증가하고 있음을 인지하고 사이버보안에 관한 평가 능력을 갖춰야 할 필요성을 제기하였다. 이에 대해 김승주 등은 국방획득체계에 적용할 수 있는 사이버보안 시험평가 체계를 국내 최초로 제안하며 RMF 프로세스의 도입 필요성을 제기하였다[13]. 하지만, 해당 연구과제의 최종 보고서는 군 무기체계 시험평가 제도와 관련된 사안으로 대외에 공개되지 않았다. 이어 합동참모본부는 2017년 사이버보안 시험평가를 위한 국방획득체계 RMF 프로세스 구체화를 추진하였으며, 김승주 등은 이에 대해 미국의 RMF 프로세스 단계를 토대로 한국군에 적용해야 할 RMF 프로세스의 방향과 이에 따른 법령 개정 소요를 제안하였다[14]. [13]과 마찬가지로 해당 연구의 최종 보고서는 관련 법률에 의한 비공개 대상 정보로, 외부에 공개되지 않았다.

양우성 등[6]은 K-RMF의 개발 목적과 적용방안을 소개하고 K-RMF를 위한 핵심 요소를 제시하였다. 하지만 이는 K-RMF 제도를 개발하고 운영하는 정책적 부서 수준에 필요한 요소를 제안하여, K-RMF 제도에 따라 세부 활동을 수행해야 하는 무기체계 개발사가 활용하기에는 부적절하다.

이승목[15]은 무기체계에 대한 RMF 적용을 위해 무기체계와 보안시스템의 통합이 필요함을 제기하였다. 또한, 무기체계 획득 절차에 따라 RMF를 적용하며 보안 통제항목 식별 및 설계, 평가 및 시스템 인가 등이 순서대로 진행되어야 함을 단계별로 설명하였다. 하지만, 각 단계를 수행하는데 필요한 자료와 산출물이 제시되지 않아 무기체계 개발사가 실제 생산 과정에서 바로 활용하기에는 제한된다.

조현석 등[16]은 잠수함 무기체계를 대상으로 RMF의 일부 단계를 적용하였다. 그 결과 기존의 보안 요구사항에 포함되지 않았던 144개의 보안 통제항목을 추가로 발견하였다. 보안 통제항목들이 누락된 이유는 기존의 보안 요구사항은 잠수함 무기체계의 운용환경을 고려하지 않았기 때문이다. 하지만, 해당 연구는 연방정부용 RMF에 대한 수정 없이 그대로 적용한 연구로, 우리나라의 국방획득체계를 최소한으로 수정하며 연방정부용 RMF 관련 내용을 반영하는 방법을 제안하고 있다. 또한, 보안 통제항목 도출 이후 단계는 수행하지 않았기 때문에 이를 실제 구현하고 구현된 결과를 평가해야 하는 무기체계 획득 절차에 직접 적용할 수는 없다.

차성용 등[7]은 무기체계를 직접 개발하지 않는 경우, 즉 외국으로부터 무기체계를 구매하는 경우 보안 요구사항을 평가하기 위한 방법을 제안하였다. 이 방법은 무기체계 구매 절차에 RMF와 사이버보안 시험평가 방법론을 결합함으로써 구현되었다. 하지만 이는 RMF의 일부 단계만을 사용하여 구현되었기 때문에, 무기체계 획득절차에 RMF 전 단계를 온전히 이용하고자 하는 경우에 적용하기에는 적합하지 않다.

이처럼 RMF의 적용 방법과 그 효과에 관한 연구가 수행되었으나, 기존 연구들은 NIST의 연방정부용 RMF가 국방용 RMF와 다르지 않다는 사실을 전제로 수행되었다. 즉, 기존 연구들은 NIST에서 공개한 연방정부용 RMF와 같이 소요군에서 상세한 자료들을 공개하고 있는 경우 사용할 수 있다. 하지만, 우리나라의 경우 K-RMF 관련 자료가 충분히 공개되지 않았다. 본 연구에서는 이러한 제한적인 상황에서 실제 무기체계 개발에 활용할 수 있는 보안 통제항목을 체계적으로 도출하는 방법을 제시한다.

대한민국 국방부는 미국의 RMF 적용 요구에 대응하기 위해 2020년 한국형 사이버보안 위험관리 제도(K-RMF)를 개발하고, 2021년부터 일부 무기체계에 대해 시범적용 및 평가를 실시하고 있다. 하지만, K-RMF 개발 결과와 무기체계에 대한 시범적용 및 평가의 상세 결과는 공개되지 않아 민간영역에서 활용할 수 없다. 이외에도 2021년 발표된 대한민국 방위사업청의 방위산업기술보호 종합계획에 따르면, 미국의 사이버보안 인증제도 기반의 한국형 기술보호 인증제도를 국내에 도입하여 방위산업체의 자율적 기술보호체계를 구축하고 K-RMF 연계 여부를 검토할 수 있도록 명시하고 있다[17]. 이와 같이 국내에서도 무기체계에 RMF를 적용하기 위한 노력을 시

행하고 있으나, 앞서 반복하여 언급한 바와 같이 현재 공개된 K-RMF 관련 자료는 매우 부족하다. 이에 본 연구에서는 NIST, DoD 등 외국의 공개된 정보를 바탕으로 연구를 수행한다.

III. RMF의 개요

본 장에서는 본격적으로 제안하는 아이디어를 설명하기에 앞서 본 연구의 가장 큰 배경지식인 RMF의 개요에 대해 설명한다. 공개된 연방정부용 RMF 표준 문서 NIST SP 800-37에 따르면, RMF는 ▲준비(prepare), ▲시스템 보안 분류(categorize), ▲보안 통제항목 선정(select), ▲보안 통제항목 구현(implement), ▲보안 통제항목 평가(assess), ▲인가(authorize), ▲모니터링(monitor)의 총 7가지 단계로 구성되어 있다[18]. 다음 Fig. 1.은 RMF의 7단계 구성에 대해 간략히 보여준다.

RMF가 처음 제정되었을 당시에는 상기 7단계 중 준비 단계를 제외한 6단계로 구성되어 있었다. 하지만, 해당 6단계로 RMF를 수행할 경우 각 단계 수행에 필요한 자료가 수집되지 않거나 조직 내에서 RMF 적용에 대한 공감대가 형성되지 않는 등의 문제점이 발견되었다. 이러한 문제점을 해결하기 위해 개정된 RMF에는 나머지 6단계를 뒷받침할 수 있도록 준비 단계가 추가되었다. RMF의 단계별 수행 활동에 대한 설명은 다음과 같다.

- 준비 단계: RMF 전체 활동에 대한 조직 구성원의 책임과 이해관계를 정립하고, 보안 통제항목 baseline 및 RMF 관련 가이드라인, RMF 적용 대상 기관의 정보보호 정책, 조직구성 등 RMF 활동에 활용할 수 있는 자료를 확보하는 단계
- 보안 분류 선정 단계: 시스템이 처리하는 데이터의 3가지 보안 속성(기밀성, 무결성, 가용성)을 기준으로, 각 속성의 손상이 시스템의 임무 수행에 영향을 주는 정도를 고려하여 시스템의 보안 분류를 선정하는 단계
- 보안 통제항목 선정 단계: 선정된 시스템의 보안 분류에 따라 시스템 및 데이터를 보호하는데 필요한 보안 통제항목 baseline을 선정하고, 운영 환경 등 시스템과 데이터의 특성에 따라 필요한 추가 보안 통제항목을 선정한 후 가공하는 단계
- 보안 통제항목 구현 단계: 도출된 보안 통제항목을 실제 시스템과 조직에 기능적, 운영적, 정책적 방안으로 구현하고, 각 보안 통제항목을 구현하는 세부 절차에 대한 문서인 STIGs(Security Technical Implementation Guides)를 작성하는 단계
- 보안 통제항목 평가 단계: 구현하기로 선정된 보안 통제항목이 올바르게 구현되었는지, 의도한 대로 동작하는지, 보안 계획의 요구사항을 만족시키는데 필요한 결과를 도출해내는지 평가하고 부족한 부분을 보완한 후 인가 결정을 위한 문서를 생산하는 단계
- 인가 단계: 보안 통제항목 평가 결과를 바탕으로 잔여 위험도의 수용 가능 여부와 대응 방안을 판단하고, 이를 토대로 시스템 운용 가능 여부를 결정하는 단계
- 모니터링 단계: 시스템 운용 환경과 조직의 변화를 추적하고 이에 따른 보안 통제항목의 효과 변화를 평가하여 시스템의 지속 운용 여부와 폐기 전략에 대한 근거를 마련하는 단계

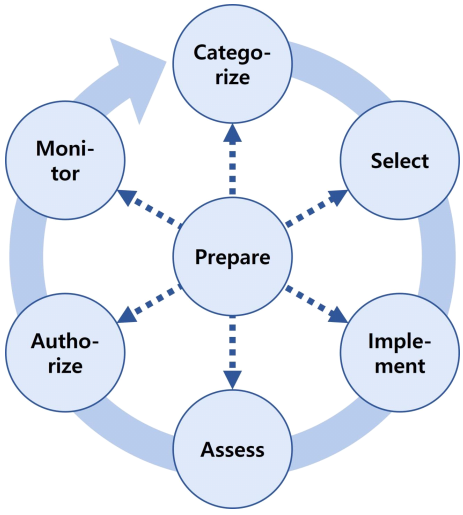

Fig. 1. Diagram of RMF process

미국의 RMF 표준에 따르면 무기체계에 대한 RMF는 어떠한 시스템을 개발한 후 실제로 사용하고자 하는 조직에서 수행하여야 한다[19]. 그리고, 이에 따라 각 단계와 단계 내 상세 활동별로 어떤 참여자(참여 기관)가 어떠한 종류의 책임소재를 지니게 되는지 분리되어 있다. 시스템 개발을 위탁받은 업체의 경우 수의계약, 부적절한 평가 등의 문제를 방지하기 위해 전체 RMF 단계 중 주로 구현 단계에 속한 활동에 주요한 책임소재를 지니게 되어있다.

이러한 RMF의 7개 단계 중 본 연구에서는 제안한 방안의 효과를 검증하기 위해 준비 단계부터 보안

통제항목 구현 단계까지 수행하였다. 이 중, 본 논문에서는 보안 통제항목 선정과 직접적으로 관련된 체계 보안 분류 선정 단계부터 구현 단계까지 총 3단계를 주요하게 다룬다. 본 논문의 목표는 무기체계 개발 시 사용할 수 있는 보안 통제항목 구축 방법을 제시하는 것이다. 그러므로 RMF를 수행하는데 있어서는 꼭 필요하지만 본 논문에서 주요하게 제안하는 방안과 직접적인 연관이 없는 준비 단계의 경우 본 논문에서 별도로 다루지 않는다.

IV. 국방용 RMF 구축 방안

RMF A&A 표준에 따르면 보안 통제항목은 군에서 제시한 보안 통제항목 baseline을 기반으로 시스템을 보호하는데 필요한 보안 통제항목을 추가하여 구현해야 한다. 하지만, 앞서 1장에서 설명하였듯이, DoD의 RMF A&A는 전체 baseline 중 극히 일부분에 대해서만 민간영역에 공개되어 있으며, 우리나라의 K-RMF는 현재 개발 중으로 이와 관련하여 민간영역에 공개된 자료는 존재하지 않는다. 즉, RMF 표준에 따라 무기체계를 개발하고자 하더라도 무기체계의 보안 분류 수준에 적합한 보안 통제항목 baseline을 선정할 수 없으며, 당연히 이를 구현하는 것도 불가능한 상황이다. 이에 본 장에서는 현재 공개된 RMF 관련 자료와 위협 모델링 방법론을 바탕으로 개발하고자 하는 무기체계에 대한 보안 통제항목을 구축하는 방법에 대해 제시한다. 다음 Fig. 2.는 본 연구에서 제안하는 위협 모델링 기반의 보안 통제항목 구축 방안에 대한 개요를 보여준다.

3장에서 설명한 RMF의 각 단계별 수행 활동의 내용을 고려할 때 7단계 절차 중 0~1단계(준비~보안 분류 선정 단계)와 4~6단계(보안 통제항목 평가~모니터링 단계)는 적용 대상 조직이나 체계가 상이하더라도 수행되는 활동은 큰 차이가 존재하지 않을 것임을 판단할 수 있다. 따라서, 연방정부용 RMF와 RMF A&A간 주된 차이가 존재하는 단계는 2~3단계에 해당하는 보안 통제항목 선정 단계, 보안 통제항목 구현 단계이다. 이에 본 연구에서는 해당 단계를 주 연구 대상으로 삼는다.

이후 4.1절에서는 위협 모델링 방법에 대해 간략히 설명하고, 4.2절에서는 국방용 RMF를 구축하기 위해 본 논문에서 제안하는 보안 통제항목 도출 방안 중 보안 통제항목 선정 단계에 해당하는 내용을 설명한다. 4.3절과 4.4절에서는 보안 통제항목 구현 단계에 해당하는 내용을 설명한다.

4.1 위협 모델링 개요

무기체계에 대한 사이버보안 위협은 곧바로 임무 실패에 직결될 수 있기에 무기체계에 잠재된 위협 중 수용할 수 없는 위험도를 가지는 위협을 식별하여 제거하는 것은 정상적인 임무 수행을 보장하기 위해 매우 중요하다. 본 연구팀은 이러한 목적을 달성하기 위해 체계적인 위협 분석 방법론인 위협 모델링(threat modeling)을 활용하였다.

위협 모델링은 ▲시스템 모델 작성 및 자산 식별, ▲공격 라이브러리 수집, ▲잠재 위협 분석, ▲공격

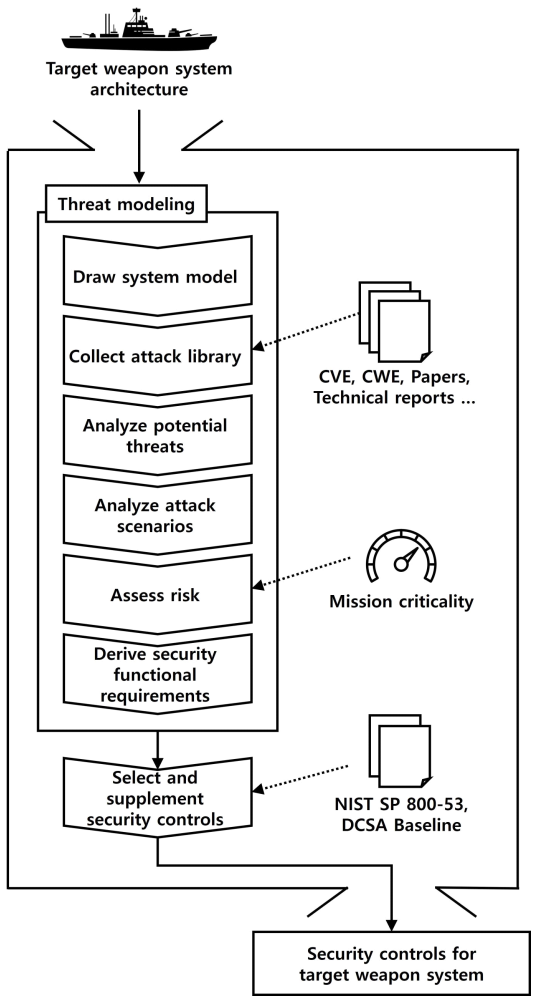

Fig. 2. Security controls inferring process for weapon system

시나리오 분석, ▲위험도 분석, ▲보안 요구사항 도출의 6개 단계로 구성된다. 다음 Table 1.은 위협 모델링의 각 단계에 대해 간략히 설명한다.

사이버보안과 관련된 국제 표준에서 언급되는 위협 모델링 방법으로는 STRIDE, LINDDUN 등이 존재한다. 조직은 분석하고자 하는 시스템의 특징, 위협의 종류 및 조직의 규모 등의 요인에 따라 어떠한 위협모델링 방법을 사용할 것인지 선택할 수 있다[20,21]. 예를 들어, 사용자의 개인정보를 다량 다루고, 이에 따라 개인정보보호와 관련된 위협을 주요하게 분석하고 싶을 경우에는 LINDDUN 위협 모델링 방법을 사용할 수 있다. 각 위협 모델링 방법을 구성하는 단계의 차이는 존재하나, 큰 흐름으로 봤을 때 Table 1.에서 설명하는 위협 모델링 단계를 벗어나지 않는다. 다음 Table 2.는 다양한 위협 모델링 방법에 대해 간략히 보여준다.

다양한 위협 모델링 방법 중 어떤 것을 선택할지 결정하기 위해서는 주로 분석하고자 하는 위협의 종류, 시스템의 특징, 조직 문화 및 위협 모델링 수행 인원의 전문성 수준 등 다양한 요인을 고려하여야 한다. 우리나라의 경우 외국에 비해 상대적으로 위협 모델링에 대한 연구가 활발히 수행되고 있지 않다. 또한, 위협 모델링에 대한 전문가도 외국에 비해 부족한 실정이다. 본 연구에서는 이러한 점을 고려하여 제안한 아이디어를 실증하기 위한 위협 모델링 방법으로 Microsoft에서 개발한 STRIDE 위협 모델링 방법을 사용하였다. STRIDE 위협 모델링 방법의 장점은 ▲참고할 수 있는 문헌이 많다는 점과 ▲타 위협모델링 방법에 비교적 적용하기 쉽다는 점, ▲가장 성숙한 위협모델링 방법이라는 점이 있다[22]. 무기체계의 경우 개인정보를 다루는 등의 특별한 특징을 가지지 않기 때문에, 본 연구에서는 가장 검증이 많이 되고 참고할 자료가 많은 STRIDE 위협 모델링 방법을 활용하였다. STRIDE 위협 모델링 방법은 시스템 내 존재하는 잠재적인 위협을 S, T, R, I, D, E의 6가지 범주로 나누어서 분석하는 것이다. 각 위협 범주의 의미와 상세한 STRIDE 위협 모델링 수행 과정은 4.2.1절에서 설명한다.

무기체계의 특성이나 식별하고자 하는 위협의 종류에 따라 STRIDE 이외에 다른 위협 모델링 방법이 더욱 적합할 수 있다. 본 연구에서는 STRIDE를 활용하였으나, STRIDE 위협 모델링이 무기체계 분야에 가장 적합한 방법이라는 것은 아니다. 본 연구에서 STRIDE 위협 모델링 방안을 활용한 이유는 상기에서 설명한 것처럼 참고할 수 있는 관련 자료가 많아 쉽게 접근할 수 있기 때문이다. STRIDE 위협

Table 1. Threat-modeling process

Steps	Description
Draw system model	Create system model to represent information needed for analyzation using formats such as DFD(Data Flow Diagram)
Collect attack library	Collect known vulnerabilities with respect to the system being analyzed
Analyze potential threats	Analyze potential threats based on attack libraries
Analyze attack scenarios	Analyze the scenarios through which an attacker could enter system and compromise assets based on the collected vulnerabilities
Assess risk	Assess the impact of risks on system to prioritize response
Derive security requirements	Identify mitigations to prevent identified attack scenarios from occurring

Table 2. Description of common threat modeling methodologies

Methodology	Description
STRIDE	Threat modeling methodology developed by Microsoft, used to discover threat in software, primarily from a developer's perspective
LINDDUN	Threat modeling methodology for system that mainly uses personal data
MORDA	Mission-oriented methodology developed by the NSA for use during system development life cycles
TARA	Threat modeling methodology for identifying and assessing cyber threats and selecting effective countermeasures to mitigate that threats
IDDIL/ATC	Threat-centric methodology based on a model of the relationships between threats, assets, controls

모델링 방법이 좋은 방법임에는 분명하지만 추후 군 무기체계에 가장 적합한 위협 모델링 방법을 별도로 연구할 필요가 있다.

위협 모델링 방법과 마찬가지로, 위험도 분석 단계에서 다양한 정량적, 정성적 분석 방법을 사용할 수 있다. 본 연구에서는 Microsoft의 DREAD를 위험도 분석 방법으로 사용하였지만 군 조직 그리고 무기체계에 가장 적합한 위험도 분석 방법 또한 추가로 연구될 필요가 있다. 본 연구에서 수행한 DREAD 위험도 분석과 관련하여 세부적인 내용은 4.2.1.5절에서 후술한다.

4.2 무기체계에 대한 보안 통제항목 도출 방법

4.1절에서 설명한 위협 모델링을 활용하면 시스템에 발생 될 수 있는 모든 잠재적 위협과 이를 이용한 공격 시나리오를 도출할 수 있게 된다. 도출된 잠재적 위협과 공격 시나리오를 바탕으로 시스템을 보호하는데 필요한 보안 요구사항을 선정할 수 있으며, 마찬가지로 보안 요구사항을 만족하기 위한 보안 통제항목을 선정할 수 있다. 이러한 과정을 통해 최종적으로 개발하고자 하는 무기체계를 보호하는데 필요한 보안 통제항목을 도출함으로써 최종적으로 해당 무기체계에 대한 하나의 RMF 프로젝트를 구축할 수 있다. 본 절에서는 이를 단계별로 설명한다.

4.2.1 위협 모델링 수행

본 절에서는 먼저 위협모델링 각 단계를 수행하는 방안에 대해 간략히 설명한다. 위협모델링 각 단계에 대한 상세 예시는 제안된 방안을 검증하기 위해 함정 전투체계에 대한 사례 연구를 진행하는 5장에서 설명한다.

4.2.1.1 시스템 모델링 및 자산 식별

위협 모델링의 첫 단계로, 분석 대상 무기체계의 아키텍처를 토대로 데이터 흐름도와 같은 형태를 이용하여 시스템을 모델링하고, 그 모델에서 보호하고자 하는 자산을 식별해야 한다. 데이터 흐름도는 분석 대상 시스템과 모델 사이의 차이가 최대한 발생하지 않도록 가능한 한 상세히 작성되어야 한다.

본 연구팀은 무기체계에 대한 시스템 모델링 방법으로 데이터 흐름도(data flow diagram)를 활용하였다. 데이터 흐름도를 이용하여 시스템 모델을 작성할 경우, 분석 대상 무기체계 내부의 데이터 흐름과, 분석 대상 무기체계와 외부 시스템 및 네트워크 간의 데이터 흐름을 시각적으로 파악할 수 있다. 또한, 시스템에 존재하는 보안상 취약점은 어떠한 데이터가 흘러가거나, 잘못된 데이터가 입력되는 등 데이터의 관점에서 분석하였을 때 직관적이고 쉽게 식별된다. 즉, 시스템에 취약점이 존재하는 경우 그 취약점을 유발하는 원인이 되는 데이터의 종류와 영향을 받는 시스템 구성요소를 파악하기에 용이하다[23]. 이러한 데이터 흐름도는 ▲프로세스, ▲외부 엔티티, ▲데이터 저장소, ▲데이터 흐름, ▲신뢰 경계의 5가지 구성요소로 작성된다.

4.2.1.2 공격 라이브러리 수집

공격 라이브러리는 위협 모델링 대상과 관련하여 현재까지 알려진 모든 취약점에 관한 정보를 수집하여 구축한 데이터베이스를 의미한다. 공격 라이브러리는 공개 취약점 데이터베이스인 CVE와 CWE, 각종 논문, 컨퍼런스 자료, 기술 문서 등 가능한 모든 수단을 이용하여 수집한다. 공격 라이브러리는 시스템의 명칭 및 그 구성요소의 이름 등 다양한 키워드를 조합하여 수집한다.

공격 라이브러리는 분석 당시 그 시스템에 대해 알려진 취약점만을 수집할 수 있으며, 기존에 알려지지 않은 새로운 취약점, 즉, 'zero-day' 취약점은 발견할 수 없다는 한계가 존재한다. 따라서, 공격 라이브러리 수집 활동은 시스템 수명주기 동안 최신 공격을 모두 고려할 수 있도록 반복하여 수행해야 한다.

4.2.1.3 잠재 위협 분석

잠재 위협 분석 단계에서는 수집된 공격 라이브러리와 적용하기로 한 위협 모델링 방법에서 제시하는 위협 분류를 토대로 시스템에 존재하는 잠재적 위협을 식별한다. 본 연구팀이 사용한 STRIDE 위협 모델링 방법은 S, T, R, I, D, E의 6가지 범주로 위협을 분류하여 시스템 내 구성요소에 각 위협을 대입해 보는 것이다. 6가지 위협 범주는 다음과 같다.

- 위장(S, Spoofing)
- 변조(T, Tampering)
- 부인(R, Repudiation)

- 정보 유출(I, Information disclosure)
- 서비스 거부(D, Denial of service)
- 권한 상승(E, Elevation of privilege)

예를 들어, 분석 대상 시스템에 웹 서버 프로그램이 구성요소 프로세스로 존재한다고 가정하였을 때 다음과 같은 "위장" 위협을 도출할 수 있다.

- 외부 사용자 A는 시스템 관리자 B로 **위장**하여 웹 서버 프로그램의 관리자 페이지에 접속할 수 있다.

이렇게 도출된 잠재적 위협은 발생 가능성을 검토할 수 있는 근거를 제시하기 위해 해당 위협과 긴밀한 연관을 가진 공격 라이브러리와 매핑된다. 이때, 도출된 잠재 위협은 분석 대상 시스템에 잠재적으로 발생할 수 있는 모든 위협을 의미하기 때문에 기술적 어려움, 높은 공격 비용에 비해 낮은 이익 등의 이유로 실제 공격에 활용될 가능성이 낮은 위협 또한 잠재 위협 분석 단계에서 도출될 수 있다.

4.2.1.4 공격 시나리오 분석

공격 시나리오 분석 단계는 식별된 잠재 위협이 어떻게 상호 연관되어 공격자의 최종 목표에 도달할 수 있는지 그 경로를 식별하는 단계이다. 이를 위해 우선 공격자의 최종 목표를 설정하여야 한다. 공격자의 최종 목표를 설정한 이후에는 각 목표를 달성하기 위해 공격자가 어떤 구성요소의 어떤 위협을 사용할 수 있을 것인지 그 경로를 식별한다. 공격 경로는 최종적으로 공격 트리라 불리는 그래프의 구조로 표현된다. 다음 Fig. 3.는 공격 트리의 예시를 나타낸다.

공격 트리에서 각 노드는 시스템 내 구성요소에 대한 공격자의 목표를 나타낸다. 간선은 보다 상위 목표로 진출하기 위해 달성되어야 하는 조건을 의미한다. 간선 사이에 호 형태의 곡선이 존재하면 AND의 의미로, 하위의 모든 공격 목표가 달성되어야 상위 공격 목표로 진출할 수 있음을 의미한다. 반대로, 곡선이 없으면 OR의 의미로, 하위 행동 중 하나만 달성되어도 상위 목표로 진출할 수 있다.

잠재 위협 분석 단계에서 시스템에 발생할 수 있는 모든 위협을 도출하였기 때문에, 공격 시나리오 분석 단계에서는 해당 위협들을 바탕으로 시스템에 발생 될 수 있는 모든 공격 시나리오가 도출된다.

4.2.1.5 위험도 분석 단계

위험도 분석은 앞서 식별한 공격 시나리오 중 어떤 것을 우선적으로 대응할지 순위를 결정하는 단계이다. 위험도 분석을 위한 대표적인 도구로는 Microsoft사의 DREAD가 있다[24]. DREAD는 다음 5가지의 항목에 각각 1점(낮음)-3점(높음)의 점수를 부여하여 공격의 위험을 평가한다. 즉, 이를 이용하면 각 공격을 5점에서부터 15점까지의 분포를 가지는 점수를 통해 순서를 매길 수 있다.

- Damage potential: 공격이 시스템에 미치는 영향
- Reproducibility: 공격을 반복 수행할 수 있는 정도
- Exploitability: 실제 공격을 수행하기 위한 난이도
- Affected users: 공격에 영향받는 사용자의 수
- Discoverability: 공격을 위한 취약점을 발견하기 용이한 정도

하지만, 모든 공격 시나리오에 대응하는 것은 막대한 비용과 시간을 소모한다. 따라서, 조직이 수용할 수 있는 위험도를 가지는 공격 시나리오의 경우 별도로 대응하지 않고 수용하는 전략을 선택할 수 있다. 이때, 수용할 수 있는 위험도의 기준을 선정하기 위해 RMF의 "체계 보안 분류 단계"에서 도출되는 체계 보안 분류를 활용할 수 있다.

RMF에서는 각 시스템이 기밀성, 무결성, 가용성의 손상으로부터 영향을 받는 정도를 선정하고, 각 수준을 높음(high), 보통(moderate), 낮음(low)의 3가지로 구분하여 총 27(=3^3)종의 시스템 보안

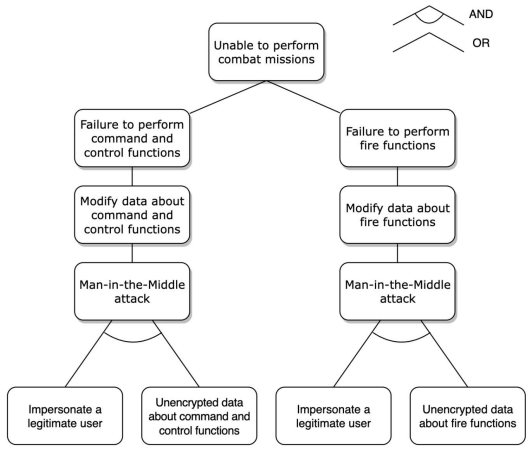

Fig. 3. Example of attack tree

수준 분류를 수행하여 구현해야 하는 대응의 정도를 결정한다. 이를 위해서는 시스템 내에서 저장, 처리, 송·수신되는 모든 정보 유형의 식별이 필요하다. 이후 식별된 정보 유형의 활용 목적과 무기체계의 임무 및 수행 환경을 분석하여 정보 유형과 무기체계에 대한 보안 분류의 판단 근거를 수립한다.

이어 정보 유형 식별을 통해 확보한 보안 분류 판단 근거를 토대로 정보 유형에 대한 임시 정보 영향 수준을 선정한다. 정보 영향 수준을 결정하는 기준은 다음 Table 3.에 제시되어 있다. 정보 유형별 정보 영향 수준이 확정되면, 무기체계 전체에 대한 보안 분류 수준을 도출한다. 이는 무기체계 내에서 저장, 처리, 송·수신되는 모든 정보 유형의 기밀성, 무결성, 가용성 수준 각각에 대하여 가장 높은 수준을 적용한다. 예를 들어, 무기체계 A에서 저장, 처리, 송·수신되는 데이터가 3가지가 존재하고, 각각의 기밀성, 무결성, 가용성 정보 영향 수준이 다음과 같다고 가정한다.

- 기밀성 = {**보통**, **보통**, 낮음}(M-M-L)
- 무결성 = {**높음**, 보통, 낮음}(H-M-L)
- 가용성 = {**낮음**, **낮음**, **낮음**}(L-L-L)

이때, 무기체계 A의 기밀성 보안 분류 수준은 {보통, 보통, 낮음} 중 가장 높은 수준인 보통이 된다. 마찬가지로, 무결성 및 가용성의 경우 각각 높음, 낮음으로 결정된다. 따라서, 무기체계 A의 보안 분류 수준은 {보통, 높음, 낮음}이 된다. 이를 수식화하면 다음 수식 (1)과 같다.

Table 3. Impact level determination criteria

Category	Impact of compromise
Low	The impact is so slight that the system will have no problem exe cuting its mission or is negligible
Moderate	The impact is non-negligible that allows the mission to proceed, b ut may require changes to the d etails
High	The impact is severe that the mi ssion would either fail immediate ly or require major changes to th e entire mission plan, making it completely impossible to proceed with the mission.

$$C = \max(c_n), I = \max(i_n), A = \max(a_n) \quad (1)$$

C, I, A는 각각 무기체계의 기밀성, 무결성, 가용성 보안 분류 수준을 의미하며, c_n, i_n, a_n은 각각 무기체계 내 처리, 저장, 송·수신되는 데이터의 기밀성, 무결성, 가용성 정보 영향 수준을 의미한다.

가장 높은 정도의 보호를 요구하는 높음-높음-높음 수준의 시스템은 기밀성, 무결성, 가용성의 손상이 임무수행에 직접적인 영향을 끼치기 때문에 도출된 모든 공격 시나리오에 대응하는 것이 타당할 것이다. 하지만, 가장 낮은 보호를 요구하는 낮음-낮음-낮음의 수준일 경우, 기밀성, 무결성, 가용성 모두 일정 손상이 발생하여도 이를 감내하고 임무 수행이 가능할 것이다. 따라서, 이 경우에는 대응하여야 할 공격 시나리오의 수가 가장 적게 식별될 것이다.

무기체계의 보안 분류 수준을 DREAD 등의 위험도 평가와 연관지으면, 위험도 점수라는 정량적인 기준으로 대응해야 할 공격 시나리오를 분류할 수 있다. 본 4.2.1.5절의 앞부분에서 설명한 것과 같이 DREAD 등의 위험도 평가를 수행하면 각 공격 시나리오에 대한 위험도가 정량적인 점수로 표현된다. 높은 위험도 점수를 받을수록 파급력이 크거나, 피해의 정도가 심하거나, 공격당하기 매우 쉬운 등의 사유로 인하여 해당 공격 시나리오가 위험하다는 것을 의미한다. 무기체계의 각 보안 분류가 몇 점의 위험도 점수까지 수용할 수 있는지를 의미하는 "수용 가능한 위험도 임계 점수"를 지정하여 대응해야 할 공격 시나리오를 정량적인 방식으로 식별할 수 있다. 예를 들어, 높음-높음-높음(H-H-H) 수준의 시스템은 모든 공격에 대응하여야 하므로, 수용 가능한 위험도 임계 점수를 DREAD에서 도출될 수 있는 가장 낮은 점수인 5점으로 선정해야 한다. 즉, DREAD 위험도 평가에서 어떠한 공격 시나리오라도 5점보다 낮은 점수를 획득할 수 없으므로 결국 모든 공격 시나리오가 완화 대상이 되는 것이다.

4.2.1.6 보안 요구사항 도출 단계

지금까지 시스템에 발생할 수 있는 모든 공격 경로를 식별하고, 시스템 보안 분류 수준 선정을 통해 대응해야 하는 공격 시나리오를 선정하였다. 위협 모델링 기반의 보안 요구사항 도출의 마지막 단계로, 대응하도록 선정된 공격 시나리오를 모두 차단하는데 필요한 보안 요구사항을 도출해야 한다.

보안 요구사항은 공격 트리의 최하위 노드에서 루트 노드인 최종 목표까지 이어지는 수많은 경로 중 비용 측면에서 가장 효과적인 경로를 차단할 수 있도록 도출된다. 이때, 가장 효과적인 차단 위치를 찾기 위해 공격 트리를 구성하는 AND와 OR 조건을 이용할 수 있다. AND 조건으로 연결된 간선일 경우, 그 하위 노드 중 한 가지라도 보안 요구사항을 통해 차단되면 더 이상 상위 노드로 진행될 수 없다. 반대로, OR 조건으로 연결되었을 경우 그 하위 노드 전체를 차단해야 더 이상 상위 노드로 진행될 수 없다. 따라서, 공격 트리 내 간선들을 차단하는데 필요한 비용을 계산하여 가장 효과적으로 각 공격 경로를 차단할 수 있는 지점들을 식별한다. 이후, 식별된 지점을 차단하는데 필요한 보안 요구사항을 도출한다. 다음 Table 4.는 Fig. 3.에 제시된 공격 트리에 대한 보안 요구사항의 예시를 나타낸다.

4.2.2 보안 통제항목 선정 및 보완 단계

보안 통제항목은 보안 요구사항을 실제로 시스템에 적용하기 위해 기능적, 운영적, 정책적 방법으로 구현해야 하는 항목이다. 보안 요구사항과 보안 통제항목은 유사한 의미에서 많이 혼용되지만, 보안 통제항목은 보안 요구사항을 실제로 시스템에 구현하는 관점에서 더욱 상세하게 기술한 것이다. 기본적으로 RMF A&A 표준을 따르면 무기체계에 대한 보안 통제항목의 경우, 우선 DoD에서 제시한 보안 통제항목 baseline 중 적절한 baseline을 선택한다. 다음으로, baseline에 포함된 보안 통제항목 외에 무기체계를 보호하는데 필요할 것으로 판단되는 보안 통제항목을 추가하여야 한다. 하지만, 앞서 설명하였듯 K-RMF와 관련하여서는 공개된 자료가 존재하지 않으며, 미국의 DCSA는 무기체계와 관련된 보안 통제항목 baseline을 단 2가지만 공개하고 있다. 이에 현재로선 어떠한 무기체계를 개발하고자 할 때에는 공개된 DCSA의 2가지 baseline과 NIST의 연방정부용 보안 통제항목 전체 목록을 참고하여 무기체계에 대한 보안 통제항목 전체를 도출해야 한다. 앞선 단계에서 위협 모델링을 수행하였고, 그 과정에서 시스템의 보안 분류 수준을 결정하였으며, 적용해야 할 보안 요구사항을 도출하였다. 보안 통제항목은 보안 요구사항을 실제 구현하기 위해 어떠한 상세 기능 또는 정책, 운영, 관리 항목이 필요한지 식별한 것으로, 보안 요구사항과 보안 통제항목은 서로 n:n의 관계로 직접 대응될 수 있다. 그러므로, 본 단계에서는 먼저 ▲공개된 RMF 관련 자료를 바탕으로 도출된 보안 요구사항에 대응되는 보안 통제항목을 식별하고, ▲만약 대응되는 보안 통제항목이 없다면 공개된 RMF 관련 자료의 보안 통제항목과 유사한 꼴의 추가 보안 통제항목을 작성하는 2가지 활동을 수행한다. 비록, 국방용 RMF인 RMF A&A의 보안 통제항목 및 baseline은 공개되어 있지 않으나, 이 두 가지 절차를 통해 개발하고자 하는 무기체계의 보안 통제항목을 도출할 수 있다.

Table 4. Examples of security requirement

Risk	Requirement name	Requirement text
Impersonate a legitimate user	Communicate on secure channel	The system should use a secure channel that logically separated from other channels
Unencrypted data	Encryption	The system should encrypt important data

4.3 보안 통제항목 가공(tailoring) 단계

보안 통제항목의 세부 내용 중 일부분은 조직 및 시스템의 특성에 맞게 작성하도록 빈칸 또는 선택지로 제시된다. RMF 표준에 따르면 선정된 보안 통제항목은 실제로 구현될 수 있도록 시스템에 알맞은 정보로 가공되어야 한다[25]. 예를 들어, 이전 단계에서 선택된 보안 통제항목은 "[할당: 시간] 동안 비활성화 된 세션은 강제 종료되어야 한다."와 같이 기술되어 있다. 업체는 보안 통제항목을 구현하는 단계에서 적절한 근거를 바탕으로 "[할당: 시간]"과 같은 빈칸을 채워야 한다. 이러한 가공의 근거를 찾기 위해 미군이 사용 중인 하드웨어 또는 소프트웨어의 보안 통제항목 상세 구현 방안을 기재한 STIGs를 참조할 수 있다[26]. STIGs에는 대상 시스템에 요구되는 보안 통제항목을 구현하고, 보안 통제항목이 올바르게 구현되었는지 점검하는 방법이 기록되어 있다. 즉, 보안 통제항목을 구현하고자 할 때 손쉽게 활용할 수 있도록 입력해야 할 명령어, 관련 문서, 담당 관계자 등이 상세히 기술되어 있다. STIGs 문서의 상세 내용에 대한 예시는 Table 5.와 Table 6.에서 보여준다.

이렇게 가공 과정까지 모두 마친 후 비로소 보안 통제항목을 실제 무기체계에 구현할 수 있다. 본 절에서 가공된 보안 통제항목은 추후 무기체계가 완성된 이후 보안 통제항목 평가 단계에서 평가의 기준으로도 활용된다.

4.4 보안 통제항목 구현 단계

보안 통제항목 가공 단계를 완료함으로써 무기체계에 발생할 수 있는 모든 위협을 완화하기 위해 필요한 보안 통제항목은 실제 구현할 수 있는 수준으로 구체화된다. 보안 통제항목 가공 단계를 수행하기 위해 사용한 STIGs는 미국의 DoD에서 획득하고 관리하는 제품들에 대한 구현 가이드 문서이다. 우리나라의 경우 아직 무기체계 개발 과정에서 K-RMF가 적용되지 않기 때문에, 국방부에서 관리하는 STIGs는 존재하지 않는다.

하지만, 국내에도 정보체계에 대한 보안 관련 기술적 가이드 문서가 지속적으로 개발 및 보완되고 적용되어 왔다. 만약, 현재 사용중인 보안 관련 기술적 가이드 문서의 내용이 K-RMF의 보안 통제항목과 중복되는 부분이 상당수 존재한다면, 이를 준수하고 있는 국내 방산업체는 현재의 개발 프로세스를 크게 수정해야 할 필요가 없기 때문에 K-RMF의 보안 통제항목을 구현하는데 기술적, 비용적으로 큰 이점을 얻을 수 있을 것이다. 대표적인 국내 보안 관련 기술적 가이드 문서로는 한국인터넷진흥원의 '소프트웨어 보안약점 진단 가이드'를 들 수 있다.

이에 대한 상세 내용은 5.4절에서 설명한다.

Table 5. Example of STIGs(technically implemented)

System	SUSE Linux Enterprise Server v11 for System z
Rule title	The system must not have accouts configured with blank or null passwords.
Check text	Verify the system will not log in accouts with blank passwords. # grep nullok /etc/pam.d/common-auth # grep nullok /etc/pam.d/common-account # grep nullok /etc/pam.d/common-password # grep nullok /etc/pam.d/common-session If an entry for nullok is found, this is a finding on Linux
Fix text	Edit /etc/pam.d/〈configuration file〉 and remove the "nullok" setting. OR Use 'pam-config' to configure the affected module if it is supported by pam-config
References	NIST SP 800-53 : CM-6b NIST SP 800-53A : CM-6.1(iv) NIST SP 800-53 Reveision 4 : CM-6 b

V. 국방용 RMF 구축 방안의 효과 검증

5장에서는 앞서 설명한 보안 통제항목 도출 방법의 효과를 검증하기 위해, 본 연구팀이 한화시스템과 산학과제를 통해 함정 전투체계에 직접 적용한 결과를 설명한다. RMF의 보안 분류 선정 단계부터 구현 단계까지 함정 전투체계를 대상으로 RMF를 적용하는 과정에서 본 연구팀이 제안한 방법을 활용한 결과를 설명한다. 본 연구에서 활용한 함정 전투체계

Table 6. Example of STIGs(policy implemented)

System	Traditional Security Checklist
Rule title	COMSEC Account Management - Appointment of Responsible Person
Check text	Check there is a current COMSEC Custodian appointment letter or verify there is a Hand Receipt Holder for COMSEC key material received from a supporting account. NOTE: Ensure that any COMSEC account, materials or equipment being inspected is used for encryption of DoDIN assets. COMSEC accounts or items not used with DoDIN assets should not be inspected.
Fix text	A person must be identified and appointed in writing to be either the COMSEC custodian or a COMSEC Hand Receipt Holder. Alternates must also be appointed in writing.
References	DoD Manual 5200.01 DoD 5200.22-M Section 4 NIST SP 800-53 : IA-1, PL-1, PS-1, PS-2, SC-1

관련 자료와 위협 모델링 결과, 보안 통제항목 가공에 대한 상세 내용은 대외 공개가 불가능하다. 이에, 공개가 가능한 범위 내 일부 자료만을 예시 형태로 제시한다.

5.1 함정 전투체계 아키텍처 대상 위협 모델링

5.1.1 시스템 모델 및 자산 식별

우선 시스템 모델 및 자산 식별 단계에서는 함정 전투체계 아키텍처를 토대로 데이터 흐름도를 작성하였다. 일반적으로 자산의 경우 해당 시스템을 소유하고 있는 조직에서 보호하고자 하는 구성요소를 선택해야 한다. 본 논문의 경우 함정 전투체계가 원활히 임무를 수행하도록 만들어야 하는 목표가 있다. 함정 전투체계의 구성요소 중 한 가지라도 제 기능을 하지 못할 경우 임무 수행에 영향을 미치기 때문에, 전체 구성요소를 보호해야 할 자산으로 가정한다. 다음 Fig. 4.는 본 연구팀이 작성한 데이터 흐름도 중 일부를 나타낸다.

5.1.2 공격 라이브러리 수집

공격 라이브러리를 수집하기 위해 5.1.1절에서 식별한 자산의 이름을 이용하여 CVE 및 CWE, 논문, 컨퍼런스 자료 및 기술문서 등 다양한 범주의 자료를 수집하고 분석하였다. 그 결과 CWE 20건, CVE 49건, 논문 18건, 컨퍼런스 자료 4건, 기술 문서 7건을 통해 98건의 공격 라이브러리를 수집하였다.

수집된 공격 라이브러리를 분석한 결과, 대표적인 취약점에는 버퍼 및 정수 오버플로우, 패킷 플러딩, 의도치 않은 권한 상승 등이 다수 발견되었다. 다음 Table 7.은 연구팀이 수집한 공격 라이브러리 중 일부를 보여준다.

5.1.3 잠재 위협 분석

앞서 4장에서 설명한 것과 같이, 잠재 위협 분석은 수집된 공격 라이브러리를 이용하여 시스템에 발생될 수 있는 위협을 식별하는 단계이다. 시스템 모델 및 자산 식별 단계에서 모델링한 함정 전투체계의 전체 구성요소에 대해 STRIDE 방법으로 잠재 위협을 식별한 결과, 총 904건의 잠재 위협을 발견할 수 있었다. 함정 전투체계는 GPS, 해군 지휘통제체계 등 외부와의

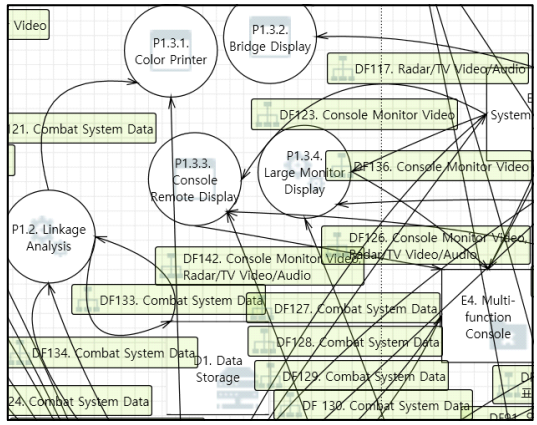

Fig. 4. Part of dataflow diagram

통신 접점이 존재하지만 모든 외부 통신은 군 통신망에 해당하였으며, 인터넷 등 민간영역 통신망과는 연결되지 않는다. 따라서, 네트워크 연동에 의한 위협보다는 내부 기능의 손상을 초래할 수 있는 버퍼 오버플로우 등의 위협이 다수 발견되었다. 다음 Table 8.은 본 연구팀이 분석한 잠재 위협의 예시를 보여준다.

5.1.4 공격 시나리오 분석

본 연구팀은 함정 전투체계에 대한 공격자의 최종 목표를 크게 2가지로 설정하였다. 첫 번째 공격 목표는 함정의 정상적인 전투 임무 수행을 방해하기 위해 임무 수행과 연관된 함정 내 기능을 마비시키는 것이며, 두 번째 목표는 함정의 전투 임무 수행과 관련된 정보를 유출하고자 하는 것으로 설정하였다. 이에 대한 예시는 앞선 Fig. 3.에 나타나 있다. 함정 전투체계에 대한 공격 시나리오를 분석한 결과, 임무 수행과 연관된 함정 내 기능을 마비시키기 위해서는 각 기능에 대해 공통적으로 데이터를 변조시키거나, 그 기능을 수행하는 시스템 구성요소에 서비스 거부(denial of service) 공격을 수행해야 함을 발견할 수 있었다. 또 다른 공격 목표인 함정 전투 임무 수행 관련 정보 유출을 위해서는 접근통제 우회, 중간자 공격 등의 위장 공격이 필요한 것으로 식별되었다.

5.1.5 위험도 분석

앞서 4장에서 기술한 것과 같이 모든 공격 시나리오에 대응하는 것은 비용적, 시간적 한계가 존재한다. 따라서 본 연구에서 대상으로 삼은 함정 전투체

계에서 대응해야 할 공격 시나리오를 선정하기 위해 함정 전투체계의 보안 수준 분류를 수행해야 한다.

함정 전투체계는 함정의 용도 및 규모, 운용 조직, 국가 등에 따라 구성요소와 데이터의 종류가 상이하다. 또한, 본 연구에서 대상으로 삼은 함정 전투체계의 경우 군용 무기체계의 특성상 민간에 공개된 정보가 한정적이어서, 모든 구성요소와 데이터를 정확히 식별하는 것은 제한된다. 따라서 보안 수준 분류 단계에서 데이터를 식별하고 임무 영향도를 분석하는 대상은 본 연구팀이 확보할 수 있었던 함정 전투체계 내 '탐색 레이더'로 한정한다. 앞서 설명한 것과 마찬가지로, 본 연구팀이 확보한 '탐색 레이더'에 관한 정보 역시 함정의 용도나 규모 등 여러 요인에 따라 상이하게 나타날 수 있다.

본 연구팀은 탐색 레이더에 대한 정보 영향 수준을 결정하기 위해 탐색 레이더가 처리하는 데이터의 보안 분류 수준을 검토하였다. 이때, 데이터의 기밀성, 무결성, 가용성 훼손이 함정 무기체계의 임무 수행에 미치는 영향을 수준 결정 기준으로 선정하였다.

함정 전투체계의 탐색 레이더는 함정 전투체계의 탐색범위 내에 존재하는 물체를 탐색하며, 탐색 레이더 연동단과 표적정보, 상태정보, 레이더 비디오, 연동관리 명령, 장비설정 명령 등 5가지 종류의 데이터를 송수신한다. 이 중 표적정보는 함정 전투체계 외부에 존재하는 표적과 함정간의 상대적 위치정보를 의미한다. 표적과 함정간의 상대적 위치정보가 외부에 유출될 경우, 표적과의 상대적 위치정보를 이용하여 함정의 위치를 계산할 수 있기 때문에 함정의 생존성 및 기동 범위에 영향을 미쳐 함정의 임무를 변경하게 만들 것이다. 따라서 표적정보는 높음 수준의 기밀성이 요구된다. 표적정보의 변조는 표적의 소실, 위치 식별 불가 등 함정의 정찰 및 타격 등 주요 임무에 직접적인 영향을 끼쳐 이를 수행할 수 없게 만든다. 따라서 표적정보는 높은 수준의 무결성이 요구된다. 마찬가지로, 표적정보를 사용하지 못하는 경우

Table 7. Examples of attack library

Type	Contents
CWE	CWE-200: Exposure of sensitive information to an unauthorized actor
CVE	CVE-2023-23559: In rndis_query_oid in drivers/net/wireless/rndis_wlan.c in the Linux kernel through 6.1.5, there is an integer overflow in an addition.
Paper	Threat assessment for GPS navigation: GPS signal can be jammed to make it impossible to determine current location
Conference	AIS exposed understanding vulnerabilities & attacks 2.0: AIS packets are being used without authentication or integrity verification, which could allow an attacker to use Software Defined Radio to cause false information to appear on radar.
Technical Paper	Hacking NAVTEX maritime warning messages: Fake warning messages can be generated on board the ship through modulation of the Navtex radio waves.

Table 8. Examples of potential threat

Target	Type	Description
Multi function console	S	The multi function console receives combat system data from the data process function. The multi function console can receive wrong data from adversary who disguises as a data process function.
Data process function	T	The data process function makes spooling before transmit print data. An adversary who connect to data process function could tamper print data via fake printer driver.
Connected analysis function	D	The connected analysis function processes data received from the data process function and the data storage. The connected analysis function may be halted its service when an adversary who connect to connected analysis function compromise the data.

에도 함정의 임무수행에 직접적인 영향을 끼치기 때문에 가용성 또한 높은 수준의 보호가 필요하다.

$$SC_{T.I.} = (Conf.: H, Int.: H, Avail.: H) \quad (2)$$

이와 마찬가지로 탐색 레이더가 처리하는 모든 종류의 데이터를 기밀성, 무결성, 가용성 측면에서 평가한 결과는 다음 Table 9.과 같다. TI, SI, RV, IM, CS는 각각 표적정보(Target Info), 상태정보(Status Info), 레이더 비디오(Radar Video), 연동관리 명령(Interoperation Management), 장비설정 명령(Component Setting)을 의미한다.

탐색 레이더가 처리하는 데이터의 위험도 분석 결과를 종합하여 탐색 레이더에 대해 요구되는 기밀성, 무결성, 가용성 수준, 즉 탐색 레이더의 임무 영향도를 평가할 수 있다. 임무 영향도는 {C: 위험도, I: 위험도, A: 위험도}의 형태로 표현하며, 높음, 보통, 낮음은 각각 H(High), M(Moderate), L(Low)로 표현한다. 탐색 레이더에 대해 요구되는 기밀성, 무결성, 가용성 수준은 각 데이터의 기밀성, 무결성, 가용성 평가 결과 중 가장 높은 수준과 동일하게 평가된다. 따라서 탐색 레이더는 기밀성 높음, 무결성 높음, 가용성 높음의 임무 영향도를 가지는 것으로 평가되며, {C: H, I: H, A: H} 또는 간략히 H-H-H로 표현할 수 있다.

Table 9. Evaluation result

Category		Low	Mode-rate	High
Confidentiality	TI			●
	SI	●	●	
	RV	●		
	IM		●	
	CS		●	
Integrity	TI			●
	SI			●
	RV			●
	IM			●
	CS			●
Availability	TI			●
	SI			●
	RV			●
	IM			●
	CS			●

DoD의 RMF 표준에 따르면 무기체계의 종합 임무 영향도는 무기체계 내 구성요소의 개별적인 임무 영향도 중 가장 높은 수준을 따르도록 되어 있다. 본 5.1.5절의 연구 결과에 따라 함정 전투체계의 경우 탐색레이더의 임무 영향도가 H-H-H 수준으로 도출되었기에 함정 전투체계의 종합적인 임무 영향도 또한 H-H-H로 결정된다.

5.1.6 보안 요구사항 도출

함정 전투체계의 보안 분류 수준은 H-H-H로 결정되었다. 임무 영향도가 가장 높은 수준인 H-H-H로 결정된 이상 함정 전투체계의 경우 가능한 공격 경로를 하나도 빠짐없이 모두 완화시켜야 함을 알 수 있다. 본 연구팀은 함정 전투체계에 대한 모든 공격 경로를 차단하기 위한 총 57개의 보안 요구사항을 도출하였다.

5.2 보안 통제항목 선정 및 보완

보안 요구사항을 도출한 이후에는 이를 함정 전투체계에 구현하기 위한 보안 통제항목을 선정하여야 한다. 일반적으로는 RMF 표준에 따라 공개된 보안 통제항목 baseline 중 무기체계의 보안 분류에 맞는 baseline을 선택하고, 추가적으로 필요한 보안 통제항목을 선택하면 된다. 하지만, 현재 H-H-H 보안 분류에 대한 baseline은 공개된 자료가 존재하지 않기에 위의 일반적인 방법을 따를 수 없다. 이에, 본 연구팀은 공개된 국방용 baseline 중 H-H-H에 가장 근접한 baseline을 고르고 우리가 도출한 보안기능 요구사항이 해당 baseline 내 보안 통제항목보다 더욱 엄격한 항목을 요구하고 있는지 검토하였다. 보안 통제항목 baseline은 자신보다 낮은 보안 분류에 대한 baseline을 기본적으로 포함하고, 추가적인 항목들을 더 요구하여 더욱 엄격하게 구성되기 때문이다.

본 연구팀이 선택한 DCSA의 보안 통제항목 baseline은 H-L-L 보안 분류에 대한 baseline이다. 해당 DCSA H-L-L baseline은 총 418개의 보안 통제항목으로 구성되어 있다. 418개의 보안 통제항목을 분석한 결과, 본 연구팀이 도출한 57개의 보안 요구사항 중 52개만을 다루고 있음을 확인하였

다. 이에 따라 본 연구팀은 보안 통제항목 baseline이 포함하지 못하는 5개의 보안 요구사항을 충족하기 위해 NIST SP 800-53의 전체 보안 통제항목 중에서 추가로 필요한 보안 통제항목을 총 3개 식별하였다. 이로써 보안 통제항목 baseline 418개에 추가 보안 통제항목 3개를 더해 총 421개의 보안 통제항목을 도출하였다. 이처럼 H-H-H에 해당하는 무기체계에 적용해야 할 보안 통제항목 baseline은 공개되어 있지 않았기에 본 연구팀이 제시한 방법을 통해 H-H-H 보안 분류를 가지는 함정 전투체계에 대한 보안 통제항목을 도출할 수 있었다.

5.3 보안 통제항목 가공

보안 통제항목을 가공할 때 각 가공 결과에 대한 적절한 근거를 제시하기 위해 본 연구팀은 함정 전투체계에서 사용되는 소프트웨어 및 하드웨어와 유사한 제품의 STIG를 벤치마킹하였다. 벤치마킹 대상으로 선정된 제품은 ▲Cisco IOS Switch L2S, ▲Cisco IOS Switch NDM, ▲Windows 10, ▲SUSE Linux Enterprise Server v11 for System z 등이다. 그 결과 보안 통제항목에서 조직 및 시스템의 특성에 맞게 작성하도록 주어진 모든 부분에 적절한 내용을 채워 넣을 수 있었다.

다음 Table 10.은 보안 통제항목 가공의 예시를 보여준다. 원래의 보안 통제항목은 '조직이 정의한 유형의 계정'의 동시 접속을 '조직이 정의한 수'로 제한하도록 하고 있다. 이와 관련한 기성 제품들의 STIGs를 분석한 결과, 'A10 networks ADC NDM'의 STIGs에서 관리자 계정의 동시 접속은 1개로 제한하도록 되어 있는 것을 발견할 수 있었다. 이와 같이 모든 보안 통제항목을 시스템의 특성에 맞도록 가공할 수 있다.

5.4 국내 가이드 문서와의 연관성 검토

4.4절에서 설명한 것과 같이 국내 방산업체에서는 다음과 같은 한국인터넷진흥원 발간 보안 관련 기술적 가이드 문서를 사용하고 있으며, 그 종류는 다음과 같다.

- 소프트웨어 개발보안 가이드[27]
- 소프트웨어 보안약점 진단 가이드[28]
- 주요정보통신기반시설 기술적 취약점 분석·평가 방법 상세 가이드[29]

Table 10. Example of security control tailoring

ID		Control text
AC-10	Before tailoring	Limit the number of concurrent sessions for each **[Assignment: organization-defined account and/or account type]** to **[Assignment: organization-defined number]**.
	+	
	STIGs	The A10 Networks ADC **must limit the number of concurrent sessions to one (1) for each administrator account and/or administrator account type**.
	=	
	After tailoring	Limit the number of concurrent sessions for each **administrator account and/or administrator account type** to **one(1)**.

이에 본 연구팀은 K-RMF 적용 이후 기존 가이드 문서의 지속 활용 가능성을 판단하기 위해 상기 문서들이 본 연구팀이 도출한 보안 통제항목을 얼마나 많이 포함하고 있는지 분석하였다. 상기 3종의 문서와 STIGs의 내용을 비교 검토한 결과, '주요정보통신기반시설 기술적 취약점 분석·평가 방법 상세 가이드'와 '소프트웨어 보안약점 진단 가이드'의 2가지 가이드 문서가 STIG에 준하는 수준으로 상세히 작성되었다고 판단하였다. 해당 2가지 문서와 본 연구팀이 도출한 함정 전투체계에 대한 전체 보안 통제항목 421개를 비교 검토하였을 때, 전체의 90.3%에 해당하는 380개의 보안 통제항목이 포함되어 있으며 9.7%인 41개의 보안 통제항목은 포함되지 않음이 확인되었다. 이처럼 국내 보안 관련 가이드만으로 RMF의 모든 보안 통제항목을 구현하는 것은 어려울 것으로 생각되며, 실제 시스템에 보안 통제항목을 구현할 때에는 해외의 각종 STIGs 문서를 참고해야 할 것으로 사료된다.

VI. 결 론

본 연구에서는 제한적으로 공개된 RMF 관련 자료를 바탕으로 K-RMF를 예측하여 무기체계에 대한 국방용 RMF를 구축하는 방법에 대해 제안하였다. 그리고, 실제 함정 전투체계 아키텍처에 이를 적용하고 공개된 하위 수준의 baseline보다 우리가 도출한 보안 요구사항이 더욱 엄격함을 보임으로써 그 효용성을 입증하였다. 이렇게 RMF 절차에 위협 모델링을 적용함으로써 공개되지 않은 국방용 RMF의 보안 통제항목 baseline을 직접 구축할 수 있다. 추후 K-RMF를 지속적으로 개발 및 보완하거나 다양한 방산업체에서 RMF를 준용하여 무기체계를 개발하고자 할 때, 또는 K-RMF에 대비하여 선행 사례 연구를 수행하고자 할 때, 본 논문에서 제시한 방안을 활용할 수 있을 것으로 기대된다.

본 연구에서는 STRIDE라는 한 가지의 위협 모델링 방법과 DREAD라는 위험도 분석 방법만을 소개하였다. STRIDE와 DREAD가 좋은 위협 모델링 방법임에는 분명하지만, 해당 방법들이 군 조직에 특화되고 가장 적합한 것은 아니다. 추후에는 차량과 같은 사이버보안 분야에서 가장 많이 사용되는 TARA, 개인정보보호 분야에서 가장 많이 사용되는 LINDDUN 등의 다양한 위협모델링 방법을 적용하거나, 무기체계에 적용할 수 있는 RMF에 적합한 위협 분석 및 위험도 평가 방법을 새롭게 개발하는 등의 연구가 수행될 필요가 있다.

이러한 점을 고려할 때, K-RMF를 실질적으로 구현하기 위해서는 먼저 다양한 무기체계 종류별 위협 분석 방안이나 주요 위협의 종류와 같은 관련 연구가 충분히 수행될 필요가 있다. 추가로, 해당 연구 내용을 토대로 실제 무기체계 개발 과정에 K-RMF를 적용할 수 있도록 방산업체의 사전 준비가 필요하다. 각 방산업체는 주력 사업 분야에 특화된 개발 프로세스와 노하우를 보유하고 있다. 추후 발표될 K-RMF 제도가 안정적으로 정착되기 위해 이러한 무기체계 종류별 특성에 관한 선행연구와 방산업체의 무기체계 개발에 대한 노하우가 잘 융합될 수 있도록 노력을 기울이는 것이 중요할 것으로 사료된다.

또한, 4장의 위험도 분석 단계에서 설명하였듯 무기체계의 보안 분류 수준에 따라 대응해야 하는 공격 경로와 대응하지 않고 수용할 공격 경로를 분류하기 위해서는 체계 보안 분류(임무 영향도)별 수용 가능한 위험도 기준이 수립되어야 한다. 해당 기준을 바탕으로 어떠한 보안 통제항목 baseline이 잘 도출되었는지, 업체가 구현한 보안 통제항목이 적합한지 평가할 수 있기 때문이다. 이에 추후에는 각 보안 분류 수준의 수용 가능한 위험도 기준을 선정할 수 있는 방법에 대한 연구가 필요하다.

References

[1] Ji-seop Lee, Sung-yong Cha, Seung-soo Baek and Seung-joo Kim, "Research for construction cybersecurity test and evaluation of weapon system," Journal of the korea institute of information security & cryptology, 28(3), pp.765-774, Jun. 2018

[2] Sung-yong Cha, "Study on methods to strengthen cybersecurity in the acquisition and operation of advanced weapon systems," Doctoral dissertation, Korea University, Jun. 2019

[3] Hyuk-Jin Kwon, Sung-Tae Kim and Ye-na Joo, "The direction of application of the RMF-based risk management system considering interoperability," Journal of korean society for Internet information, 22(6), pp.83-89, Nov. 2021

[4] DCSA, Defense counterintelligence and security agency assessment and authorization process manual, DCSA, Aug. 2020

[5] The DoD, "The DoD cyber strategy," The Department of Defense, Apr. 2015

[6] Woo-sung Yang, Sung-yong Cha, Jong-sung Yoon, Hyeok-joo Kwon and Jae-won Yoo, "Korean security risk management framework for the application of defense acquisition system," Journal of the korea institute of information security & cryptology, 32(6), pp.1183-1192, Dec. 2022

[7] Sung-yong Cha, Seungsoo Baek, Sooyoung Kang and Seungjoo Kim, "Security evaluation framework for

military IoT devices," Security and communication networks, vol. 2018, Jul. 2018
〔8〕 "ROK MND·JCS, Developing cybersecurity joint guidance with the USFK," Boan News, Jun. 3. 2023
〔9〕 Dawn Beyer, Michael Nance, Patrick Lardieri, Nelson Roberts, Rob Hale, Tom Plummer and John Johnson II, "Lockheed Martin Cyber Resiliency Level(CRL) Framework V3.0 for Weapon, Mission, and Training Systems," Lockheed Martin Corporation, 2020
〔10〕 Northrop Grumman, "Developing a framework to improve critical infrastructure cybersecurity," Northrop Grumman, Apr. 2013
〔11〕 BAE Systems, "Epiphany datasheet," BAE systems, Inc., Apr. 2019
〔12〕 The boeing company, "Security Monitoring Infrastructure System Product Card," The boeing company, 2023
〔13〕 MND, "Study on cybersecurity test and assessment methods," Policy research information service&management, Oct. 2016
〔14〕 MND, "Study on application of RMF process in national defense acquisition process for cybersecurity test and assessment," Policy research information service&management, Dec. 2017
〔15〕 Seungmok Lee, "A study on the application of RMF for weapon systems in Korea: weapons and security system integration," Journal of advances in military studies, 4(3), pp.191-208, Dec. 2021
〔16〕 Hyun-suk Cho, Sung-yong Cha and Seung-joo Kim, "A case study on the application of RMF to domestic weapon system," Journal of the korea institute of information security & cryptology, 29(6), pp.1463-1475, Dec. 2019
〔17〕 DAPA, "2022~2026 Defense industry technology protection masterplan," DAPA, Dec. 2021
〔18〕 NIST, "Risk Management Framework for Information Systems and Organizations," NIST SP 800-37 Rev.1, 2014
〔19〕 DoD, "DoD program manager's guidebook for integrating the cybersecurity management framework(RMF) into the system acquisition lifecycle," Department of Defense, pp 70-71, Sep. 2015
〔20〕 Jaewon Seo, Jiwon Kwak and Seungjoo Kim, "Formally Verified Software Update Management System in Automotive," VehicleSec 2023, Feb. 2023
〔21〕 Mina Deng, Kim Wuyts, Riccardo Scandariato, Bart Preneel and Wouter Joosen, "A privacy threat analysis framework: supporting the elicitation and fulfillment of privacy requirements," Requirements Engineering Journal, vol. 16, no. 1, pp 3-32, Mar. 2011
〔22〕 Nataliya Shevchenko, Timothy A. Chick, Paige O'Riordan, Thomas Patrick Scanlon and Carol Woody, "Threat modeling: a summary of available methods," Carnegie Mellon University Software Engineering Institute, Jul. 2018
〔23〕 Adam Shostack, Threat Modeling : Designing for Security, John Wiley & Sons, New Jersey, 624p, 2014
〔24〕 Adam Shostack, "Experiences Threat Modeling at Microsoft," MODSEC@ MoDELS 2008, 2008
〔25〕 NIST, "Risk Management Framework for Information Systems and Organizations," NIST SP 800-37 Rev.2, 2018
〔26〕 DoD Cyber Exchange Public, "DoD

STIGs," https://public.cyber.mil/stigs, Aug. 4. 2023
〔27〕 KISA, "Guide on software development security," KISA, Dec. 2021
〔28〕 KISA, "Guide on software vulnerability diagnosis," KISA, Nov. 2021
〔29〕 KISA, "Detailed guide on analysis and assessment of technical vulnerability of major information and communication infrastructure," KISA, Mar. 2021

〈저자소개〉

안 정 근 (Jung keun Ahn) 정회원
2014년 2월: 육군사관학교 지역연구학과 학사
2019년 8월~현재: 국군방첩사령부
2023년 3월~현재: 고려대학교 정보보호대학원 석사과정
〈관심분야〉 보안공학, 위험관리, 보안성 평가/인증

조 광 수 (Kwangsoo Cho) 정회원
2019년 2월: 호서대학교 컴퓨터공학과 학사
2019년 3월~2021년 8월: 고려대학교 정보보호대학원 석사
2021년 9월~현재: 고려대학교 정보보호대학원 박사과정
〈관심분야〉 보안공학, RMF A&A, 시큐어코딩, 소프트웨어 개발

정 한 진 (Han-jin Jeong) 정회원
2015년 2월: 한국해양대학교 컴퓨터정보공학과 졸업
2020년 1월~현재: 한화시스템 해양연구소 선임연구원
〈관심분야〉 RMF, 함정 전투체계

정 지 훈 (Ji-hun Jeong) 정회원
2006년 2월: 영남대학교 전자공학과 졸업
2005년 10월~2013년 6월: 삼성탈레스 선임연구원
2013년 7월~2016년 9월: 현대중공업 특수선 책임엔지니어
2016년 10월~현재: 한화시스템 해양연구소 수석연구원
2023년 2월~현재: 연세대학교 정보대학원 석사과정
〈관심분야〉 RMF, 함정 전투체계, 인공지능

김 승 주 (Seung-joo Kim) 종신회원
1994년~1999년: 성균관대학교 정보공학과(학사, 석사, 박사)
1998년~2004년: 한국인터넷진흥원(KISA) 팀장
2004년~2011년: 성균관대학교 정보통신공학부 부교수
2011년~현재: 고려대학교 사이버국방학과/정보보호대학원 정교수
2004년~현재: 한국정보보호학회 이사
2014년~2015년: 육군사관학교 초빙교수
2014년~2016년: 다음카카오 프라이버시 정책 자문위원
2016년~2018년: 개인정보분쟁조정위원회 위원
2016년~현재: 한국카카오뱅크 정보보호부문 자문교수
2017년~현재: 고려대학교 국방RMF연구센터(AR^{2}C) 센터장
2018년~현재: 원자력안전위원회 전문위원
2018년~현재: 국방부 정보화책임관(CIO) 자문위원
2018년~2020년: 대통령직속 4차산업혁명위원회 위원
2018년~현재: 고신뢰 보안운영체제 연구센터(CHAOS) 센터장
2020년~현재: 합동참모본부 정책자문위원회 자문위원
2023년~현재: 대통령직속 국방혁신위원회 위원
〈관심분야〉 보안공학, 위협모델링, 보안성 평가/인증, DevSecOps, 암호학, 블록체인