Journal of the Korea Academia-Industrial cooperation Society
Vol. 25, No. 8 pp. 587-595, 2024

https://doi.org/10.5762/KAIS.2024.25.8.587
ISSN 1975-4701 / eISSN 2288-4688

국방분야 AI 적용 무기체계 도입을 위한 전순기 품질확보방안 연구

강지훈*, 정민경, 이영민, 박주영
국방기술품질원

Research on Ensuring Quality Assurance for the Introduction of AI-Enabled Weapon Systems during the Total Life Cycle

Ji Hoon Kang*, Min-Kyung Jeong, Yeong-Min Lee, Joo-Young Park
Defense Agency for Technology and Quality

요 약 미래전장에서 AI 기술의 도입은 국방력 향상에 필수 요건이다. 미국·중국 등 선진국들도 미래군사전략의 일환으로 AI 기술에 집중투자하고 있으며, 국내에서도 국방부, 방사청 등을 중심으로 AI 적용 무기체계 도입을 위한 중·장기 전략을 제시하고 있다. 본 연구는 소요군의 AI 적용 무기체계 수요 증가를 고려하여 전투원이 믿고 사용할 수 있는 AI 실현의 요소인 품질확보 수단으로 성능평가 방안을 연구하는 데 목적이 있다. 연구는 국내·외 AI 기술 동향 및 성능평가 관련 이슈를 분석함으로써 AI 연구의 필요성을 고찰하고 AI 적용 무기체계의 품질확보를 위한 성능평가 방안에 대한 방향을 제시하는 것으로 수행하였다. 품질확보를 위한 성능평가 방안은 크게 연구개발 단계, 양산 단계, 운영·유지 단계로 구분하였고 단계별로 AI 구현 성숙도 평가, AI 성능점검 및 모니터링 업무수행을 위한 세부 방안을 제시하였다. 본 연구 결과를 바탕으로 AI 적용 무기체계 도입을 위한 시험평가와 전투원이 믿고 사용할 수 있는 AI 실현에 이바지할 수 있기를 희망하며 AI 과학기술 강군 육성의 조기 달성을 이룩할 수 있길 바란다.

Abstract In a future battlefield, AI technology will be an essential requirement for enhancing the national defense capabilities. Advanced countries, such as the United States and China, invest heavily in AI technology as future military strategies. Domestically, the South Korean government, focusing on the Ministry of National Defense and the Defense Acquisition Program Administration, is presenting medium to long-term strategies for introducing AI-applied weapon systems. This research aims to study methods for evaluating AI performance to secure quality in realizing AI that warfighters can trust and use, considering the increasing demand for AI-applied weapon systems in the military. This study analyzed the domestic and international trends in AI technology and performance evaluation-related issues to examine the necessity of AI research and propose directions for performance evaluation methods to ensure the quality of AI-applied weapon systems. The quality was ensured by dividing the performance evaluation methods into three stages: research and development, production, and operational maintenance. Detailed approaches for assessing the AI implementation maturity, conducting AI performance checks, and monitoring tasks were provided for each stage. Based on the results of this study, testing and evaluation for the introduction of AI-applied weapon systems can be facilitated, contributing to the realization of AI that warfighters can trust and use. Furthermore, the early achievement of AI technological prowess can be attained, fostering a strong AI scientific and technological power.

Keywords : Artificial Intelligence, Quality, Total Life Cycle, Weapon system

*Corresponding Author : Ji-Hoon Kang(Defense Agency for Technology and Quality)
email: jh1989@dtaq.re.kr
Received May 31, 2024 Revised July 2, 2024
Accepted August 2, 2024 Published August 31, 2024

1. 서론

최근 선진국을 중심으로 전투원의 생존성 향상, 전투 효율성 극대화, 군사적 우위 달성 등의 목적하에 국방 분야에 AI 적용 무기체계 도입을 위한 노력을 기울이고 있다[1]. 특히, 미국, 중국 등은 군사전략의 일환으로 인공지능(Artificial Intelligence, 이하 “AI”) 기술에 대한 집중투자를 추진하고 있다. 우리나라도 제2 창군 수준의 「국방혁신 4.0」추진으로 AI 과학기술 강군 육성이라는 국정과제를 선정하고 국방부를 중심으로 국방AI센터 설립, 방위사업청(이하 “방사청”) AI 기반 무기체계 획득제도 개선, 한국국방연구원 국방데이터연구단 출범 등 기관별 AI 도입 관련 미래 비전과 추진방안을 제시하고 있다. 하지만 앞서 언급한 기관별 미래 비전과 추진방안은 대부분 AI 거버넌스 조성, 소요·기획, 기술개발 등 중·장기적 관점 중심의 논의들이기 때문에 AI 적용 무기체계 도입과 관련하여 현재 당면한 문제점을 해소하기에는 한계점이 있다. 여러 당면한 문제 중 시급히 풀어야 할 사안으로 요구사항 달성 여부 확인, 성능평가 방안 수립, 데이터 품질 평가 등이 있으며, 이는 결국 객관적 기준과 방법으로 성능평가를 수행하는 것과 직결된다. 또한, AI 기술의 특성에 따라 AI의 성능은 반복적인 학습을 통해 확보되고 지속적으로 최신화되어야 하므로 이에 대한 관리방안이 마련되어야 한다.

본 논문에서는 AI 적용 무기체계 전순기 품질확보방안 도출을 위하여 2절에서 AI 기술 도입을 위한 대내·외 동향을 조사하였으며, 3절에서 2절의 조사내용을 기반으로 AI 적용 무기체계 성능평가 방안을 연구개발 단계, 양산 단계, 운영유지 단계 등으로 구분하여 제안하였다. 최종적으로 결론에서 이를 바탕으로 AI 적용 무기체계의 신뢰성과 품질을 확보함으로써 전투원이 신뢰를 기반으로 믿고 사용할 수 있는 AI 기술 도입을 달성을 위한 성능평가의 필요성과 향후 연구 방향에 대하여 제언하였다.

2. AI 기술 도입을 위한 대내·외 동향

우리나라를 포함한 미국, 중국 등 선진국을 중심으로 국방분야에 AI 기술 도입을 위하여 다양한 정책 및 전략이 제시되고 있으며, 민간의 급속한 기술발전을 토대로 AI 기술 관련 민간기업과의 협력도 다각적으로 추진되고 있다. 본 절에서는 미국과 우리나라를 중심으로 AI 기술 도입 관련 국방분야 추진 동향과 AI 성능평가 관점의 이슈 사항에 대하여 논의하고자 한다.

2.1 미국 AI 기술 도입 관련 동향

미 국방부는 2014년 첨단기술을 활용하여 중국과 러시아의 기술발전을 상쇄하는 것을 목표로 제3차 상쇄전략을 발표하였으며, 여기서 언급된 첨단기술의 한 분야로 AI에 대한 도입이 고려되었다. 이후, 미 국방부는 2017년 Project Maven을 통해 무인 항공 시스템에서 확보한 비디오 영상을 분석하는데 AI 기술을 시범 적용하였으며, 기대보다 큰 성공을 거둠으로써 AI에 대한 도입을 가속화하여 2018년 DARPA 주관으로 20억 달러의 예산을 투입한 ‘AI Next Campaign' 추진을 이끌었다[2]. 이와 동시에 국방 분야 AI 도입을 위한 정책이 빠르게 연구되었다. 이에 관한 결과로 2018년 6월 「국방 AI 전략」을 발간함으로 AI는 미 국방 및 국가안보 전략의 핵심축이 되었으며, 2020년 AI 윤리원칙 채택, 국가 AI 이니셔티브법 제정을 통한 법적 기반 마련을 하였다[3].

이후, 2022년 6월 AI의 국방 분야 도입을 위한 신뢰 확보방안으로 책임 있는 AI 전략 및 구현경로를 제정함으로써 거버넌스 확보, 전투원 신뢰 보장, 수명주기 관리, 요구사항 검증, AI 생태계 구축과 전문인력 양성 등 6대 원칙 방향을 제시하였다[4]. 이에 따라 AI 적용 무기체계 획득을 위한 전략적 접근 및 중점분야 수행과업이 추진되고 있으며, 이를 효율적으로 조정·통제하기 위한 조직으로 합동AI센터(Joint Artificial Intelligence Center, 이하 “JAIC”)를 설립하였다. 현재는 JAIC는 차관 직속 최고 디지털 및 AI 책임관(Chief Digital and Artificial intelligence Office, 이하 “CDAO”) 기구로 통합, 확대되어 AI와 데이터에 대한 업무 강화를 선도하고 있다. 이러한 상황을 바탕으로 미국은 AI 기술을 활용하여 모든 군사분야에 혁신적인 발전을 이루고 국제사회에서 주도권을 지속하기 위해 AI 기술 개발과 활용을 꾸준히 증가시키고 있으며, 22년에만 총 55.4억 달러를 AI 적용 무기체계 획득에 투자하는 등 예산을 지속적으로 늘여가고 있다.

이러한 AI 도입과 관련된 정책, 조직, 예산적 측면과 함께 평가와 관리 측면의 검토도 지속적으로 수행되고 있다. CDAO에서는 AI 평가와 보증은 기존 시험평가와 책임 있는 AI의 조합이라 설명하고 있으며, 시험평가 프로세스를 AI 알고리즘 시험, 시스템 통합 시험, 인간-시스템 통합 시험, 운영 시험 4가지 영역으로 구분하고 있다. 여기서 AI 알고리즘 시험 영역으로 모델의 무결성, 신뢰성, 견고성, 복원력 등을 확인하며, 이 중 무결성, 신

뢰성의 시험평가 방법으로서 혼용 매트릭스를 통한 성능 평가와 강건성 측면의 평가가 포함된다.

이와 별도로 미 회계감사원에서는 2021년 정부기관 등이 AI 관련 많은 과제를 관리함에 있어 예산 집행의 투명성 확보를 위해 제3자 검증 프레임으로써 “연방기관 및 기타기관에 대한 AI 책임 프레임워크”를 배포하였다. 해당 프레임워크의 주요 내용은 거버넌스, 데이터, 성능, 모니터링 4개 핵심 영역에 대한 감사절차, 감사자 및 평가자가 고려해야 할 사항에 대하여 제시하고 실시를 요구하고 있다[5]. 또한, 미국표준기술연구소에서 2023년 1월 AI 시스템 설계, 개발, 배포 및 사용하는 조직을 위하여 AI 기술 사용 에 대한 이익 극대화 및 개인, 조직 및 사회에 부정적 영향을 줄일 수 있도록 위험관리 요소들을 선정 및 관리하기 위한 “AI 위험관리 프레임워크”를 제시하였다. 해당 프레임워크의 주요 내용은 거버넌스, 매핑, 측정, 관리 4가지 영역으로 구분하여 안정성, 책임성, 투명성, 신뢰 가능성 등의 AI 시스템 7가지 특성에 대한 위험요인을 선정 및 관리하는 방안이며, AI 시스템의 설계, 개발, 테스트, 배포 등 생애 전 단계에 걸쳐 평가가 수행되어야 하는 것이다[6].

2.2 국내 AI 기술 도입 관련 동향

국방부는 2017년 미래지향적 국방 역량 강화의 일환으로 AI 등 첨단기술의 국방 분야 융합 및 선진국의 국방혁신 사례 적용 등을 제시하는 것을 시작으로, 2020년 국방 AI 추진전략을 통해 국방 분야 AI 도입과 관련한 추진방향을 제시한 바가 있다. 이후, 2022년 신정부 들어서며 “제2창군 수준의「국방혁신 4.0」추진으로 AI 과학기술 강군 육성”이 국정과제로 선정됨으로써 국방 분야 AI 기술 도입이 본격적으로 추진되고 있다. 이에 따라 국방부는 과학기술 강군 육성 중 AI 관련 사항에 대한 추진계획으로 국방 AI 추진전략 2.0을 제시하였다. 또한, 2023년 국방혁신 4.0 기본계획에 따라 AI 기반 핵심 첨단전력 확보를 위한 유·무인 복합전투체계 구축이 수행되고 있으며, AI 기반 유 · 무인복합전투체계 구축 추진을 통해 전투 수행 개념, 네트워크 환경, 데이터 확보 · 관리와 운용 · 관리체계의 발전 등을 목표로 하고 있다. 이에 2023년 6월 국방과학기술조정협의회에서 유·무인복합전투체계 구축 추진계획과 관련된 사항이 논의되었으며, 해당 사항에는 AI 무인체계 신뢰성 확보에 대한 사항이 포함되어 있다.

방사청의 경우 AI 적용 무기체계 획득에 필요한 독자적 생태계 구축과 특화 획득절차/사업관리 방안 확보를 목적으로 획득제도 개선과 AI 거버넌스 구축을 추진하고 있다. 이와 관련하여 현재 국방 파운데이션 모델이라는 거대 AI 모델 개발 환경을 조성하고, AI 개발관리 절차 마련과 관련된 내용으로 정책적 방향 제시를 준비하고 있다. 또한, 방위사업법 개정을 통해 무기체계 신속획득(Fast- Track) 제도를 입법화하는 등 AI, 드론, 로봇 등이 중요 역할을 하게 될 미래전에 대응하기 위해 제도적 기반도 강화하고 있을 뿐만 아니라 AI, 무인화 기술이 급속도로 발전함에 따라 복잡성이 증대될 수 있어, 안전관리 측면에서의 연구도 추진하고 있다.

위에서 언급한 내용을 바탕으로 국내 AI 도입 관련 동향의 시사점은 우리나라도 국방분야에 AI 기술 도입을 위한 많은 노력을 기울이고 있으며, AI 거버넌스 조성, 소요·기획, 기술개발 부분은 일부 가시적인 추진 방향이 세워지고 있다는 것이다. 하지만, 아직 AI 적용 무기체계 도입을 위한 별도의 시험평가, 품질 측면의 연구가 활발히 수행되지 않고 있는 한계점이 있으므로 향후 해당 분야에 대한 관심이 필요할 것이라 생각된다.

2.3 AI 기술 성능평가 분야 이슈

앞서 국내 · 외 AI 기술 도입 관련 동향 파악을 통해 현재 AI 기술을 국방 분야에 도입하기 위한 많은 노력을 기울이고 있는 것을 확인하였으며, 실제 전장에서 AI 적용 무기체계를 운용하기 위해서는 AI 기술에 대한 성능을 확인하는 것이 필요하다는 것을 확인하였다. 본 절에서는 이러한 AI 기술 적용을 위한 성능평가 단계에서 발생하고 있는 이슈들에 대해 살펴보고자 한다. 성능평가와 관련된 이슈는 크게 두 가지를 언급할 수 있다.

첫째, AI 적용 무기체계의 성능평가를 수행하기 위한 성능지표와 기준이 운영목적과 요구성능에 대하여 명확히 고려되어 설정되고 있지 않은 경우이다. AI 기술이 무기체계에 활용되는 분야는 매우 다양하고, 실제 적용되는 환경, 운영목적 등이 상이하다. 그러나 현재 AI 성능평가에 사용되는 척도들은 앞서 언급한 사항에 대한 모든 조건을 시나리오로 만들고 이에 대한 성능지표와 기준이 적합한지, 해당 성능지표를 사용하였을 때 발생할 수 있는 제한사항 등이 발생할 수 있는지 확인하는 단계는 제도, 예산, 전문인력 등 여러 가지 이유로 인하여 미흡한 실정이다. 이와 관련된 예로 A 사업의 경우 AI 기술을 활용한 분류모델과 관련한 요구성능에 대하여 F1-Score를 성능평가 지표로 사용하였는데, 일반적으로 민간분야의 많은 연구에 따르면 분류모델의 학습능력 성능평가 지표는 ROC Curve를 이용하는 것이 더 적절하다고 제

시되었다. 이는 시험평가 간 AI 성능에 대한 평가가 원활하게 수행되어도 무기체계가 전력화된 후 실 운영 시 기대에 미치지 못하는 성능을 도출할 수 있는 문제를 일으킬 수 있다.

둘째, AI 적용 무기체계의 학습이 제한적으로 수행된 후 시험평가 단계에 진입하는 경우이다. 현재 개발되는 AI 적용 무기체계의 경우 국방분야 데이터 특수성(원천 데이터 부족, 보안 이슈 등)으로 인해 모델이 제한적으로 학습된 상태에서 실물에 의한 시험평가가 수행되는 경우가 발생할 수 있다. 즉, 제한적 환경에서 일부 시나리오를 통한 시험평가를 수행하고 있는데 이러한 방식으로 AI 적용 무기체계를 도입한다면 모델 학습 시 고려하지 못한 상황 또는 예기치 못한 상황이 발생했을 경우 요구 성능 발휘를 보장하기 어려울 수 있다. 따라서, 이러한 성능평가 과정에서 발생하고 있는 이슈들을 해결하고 AI 적용 무기체계의 품질을 확보하는 방안 모색이 필요하다.

3. AI 적용 무기체계 성능평가 방안

미 국방부의 “AI 윤리원칙” 및 “책임 있는 AI 전략 및 구현경로”, 미 회계감사원의 “AI 책임 프레임워크”, 미국 표준기술연구소의 “AI 위험관리 프레임워크” 등에서 AI 도입을 위해 공통적으로 언급되는 사항이 “적절한 성능평가”와 “수명주기 간 지속관리”이다. 여기서, “성능확인”과 “지속성 보장”은 전통적인 품질의 영역이며, 결론적으로 AI 적용 무기체계의 품질확보는 "성능평가"와 "성능 최신화(모니터링)" 두 가지 업무가 중요할 것으로 판단하였다.

본 논문에서는 AI 적용 무기체계 품질확보를 위한 “성능평가” 및 “모니터링” 관점에서 연구개발 단계, 양산 단계, 운영·유지 단계로 구분하여 업무수행 방안을 제시하였다.

3.1 AI 성능평가 개념

단계별 성능평가 수행방안 제시에 앞서 본 논문에서 언급하고 있는 성능평가의 개념에 대하여 살펴볼 필요가 있다. 성능평가의 개념은 AI 기능시험과 AI 시스템 시험으로 구분하여 Fig. 1에 정의하였다.

AI 기능시험은 AI 관련 요구사항에 따른 기능적 정합성을 만족하는지 확인하는 시험으로, 기존 민간분야에서 사용되는 혼동 매트릭스를 기반으로 한 성능지표달성 여부를 판단하는 것을 의미한다[7]. 예를 들어 탐지/추적, 감시/정찰 분야에 도입되고 있는 AI 적용 무기체계의 Accuracy, F_β-Score, mAP 등의 특정 성능지표를 데이터 기반의 시험을 통해 정량적인 수치 달성 정도를 확인하는 것이다. 해당 기능시험의 중점 연구사항은 데이터 및 시험계획/절차이다. AI 기능시험을 수행하기 위해서는 데이터의 확보와 데이터 품질에 대한 선제적 준비가

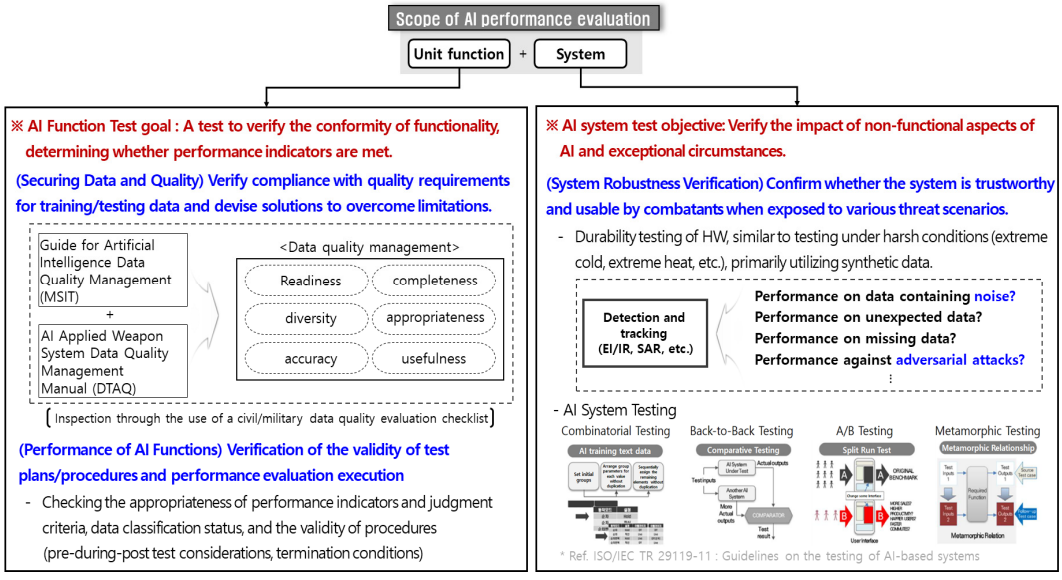

Fig. 1. Definition and scope of AI performance evaluation

필요다. 이에, 국방기술품질원(이하 “기품원”)에서는 시험용 데이터의 품질 요건이 충족되는지를 확인하기 위한 「국방 데이터 품질관리 가이드라인」을 제정하였으며, 현재 가이드라인에 대한 실효성과 적용 가능성에 대한 연구과제를 수행하고 있다. 또한, 추가적으로 성능평가를 수행함에 있어 데이터 부족 또는 확보가 어려운 데이터에 대해서는 합성데이터를 활용하는 방안에 관한 연구를 진행 중이며, 해당 연구에서는 합성데이터 사용 시 데이터에 대한 품질 검증 방안에 대한 사항을 포함하고 있다. 다음으로 데이터에 대한 준비가 완료되면 시험계획/절차의 타당성 확인 단계가 필요하다. 성능평가 지표와 기준이 적절한지, 시험 전·중·후 확인사항 및 시험조건 등이 제대로 설계되어 있는지 등을 중점적으로 점검해야 한다. 성능평가 지표·기준 및 평가절차는 민간에서 여러 연구를 통해 도출된 자료를 기반으로 국방분야 특수성을 고려할 수 있도록 선정하고, 반복적 성능평가가 이루어질 수 있도록 하는 것을 목표로 연구를 진행하고 있다.

다음으로 AI 시스템 시험은 AI 기능 외적 요소에 대한 영향성을 확인하는 것이라 할 수 있으며, 외적 요소에 대한 중점은 시스템의 강건성 확인이다. 여기에서 강건성 확인 방법으로는 ISO/IEC에서 배포한 “ISO/IEC TR 29119 AI 기반 시스템 테스트에 대한 지침”에서 언급되고 있는 블랙박스 테스팅 기법인 조합 테스팅, 백투백 테스팅, A/B 테스팅, 변성 테스팅 4가지 중 변성 테스팅을 적용하는 것을 고려하고 있다[8].

변성 테스팅 기법을 적용한 AI 시스템 시험은 다양한 외부 요인으로 인한 위협 상황에서도 신뢰할 수 있는 시스템인지 확인하는 것을 목적으로 하며, 외부 요인의 예는 날씨, 운용조건 등 환경적 요인, 학습 시 예상하지 못한 상황, 적대적 공격 등을 대표적으로 들 수 있다. 해당 시스템 시험에는 학습 시 사용된 데이터를 기반으로 외부 요인을 반영한 데이터를 평가 데이터로 사용하여야 하므로 주로 합성데이터가 활용될 필요성이 있으며, 이는 위에서 언급한 데이터 확보와도 연계성이 있다.

3.2 연구개발단계 AI 구현 성숙도 평가

AI 구현 성숙도 평가(AI Implementation Readiness Assessment, 이하 “AIRA”)는 연구개발단계 진행 간 개발시험평가(Development Test and Evaluation, 이하 “DT&E”) 진입 이전까지 기품원 주관으로 요구사항, 데이터, AI 성능과 관련하여 성숙도를 평가하는 것으로, 요구사항, 데이터 및 AI 모델의 보완점을 식별하고 연구개발주관기관에 조치를 권고하는 위험관리 업무이다. 무기체계 연구개발의 경우 개발수명 주기 관점에서 최종 도달해야 할 연구개발 목표(최종 성숙 단계)를 정의하고, 개발이 진행됨에 따라 주요 개발단계(SRR~규격화)에서의 완료 상태를 평가하고 향후 추진사항에 대한 개선점을 보완하는 방식을 고려하여 AI 구현 성숙도 평가방안을 Fig. 2와 같이 구체화하였다.

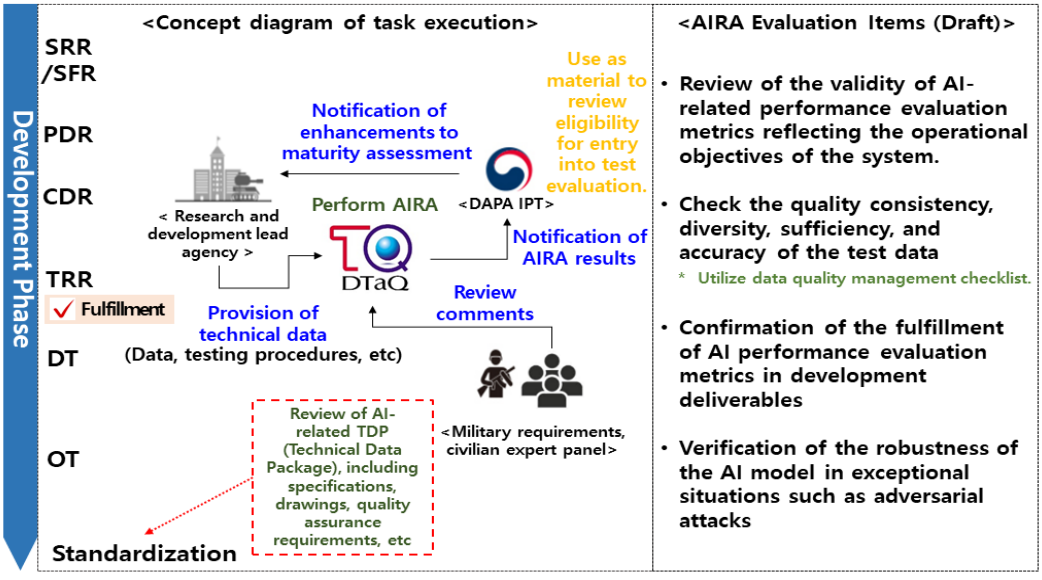

Fig. 2. Conceptual diagram of AIRA execution in the research and development stage

성숙도 평가사항으로는 3.1절에서 언급한 AI 성능평가 개념을 바탕으로 데이터 준비성, 일관성, 다양성, 충분성, 정확성 등을 포함한 데이터 품질 관련 사항과 AI 기능에 대한 단위기능, 시스템 시험 수행을 위한 제반 요소(시험장비, 도구, 절차 등) 및 시험 수행에 따른 결과 등에 대한 검토 사항을 포함하여 포괄적으로 고려하고 있다.

AIRA 결과는 방사청 IPT에 시험평가 가능 여부 판단을 위한 자료로 사용할 수 있을 것으로 판단되며, 기대효과로써 시험평가 관련 사업 지연을 예방할 수 있으며 실패 가능성 또한 사전에 확인할 수 있을 것으로 판단된다.

3.3 양산 단계 AI 성능점검

연구개발 단계에서 AIRA, 규격화 등의 업무를 통해 AI 적용 무기체계를 개발한 이후 전력화를 위하여 양산 단계에 진입하게 된다. 이때, AI 적용 무기체계는 양산 단계에서 일반적인 무기체계와는 달리 AI 성능점검이라는 추가적인 업무절차가 필요할 것으로 판단된다. AI 성능점검 업무를 간략하게 정의하면 연구개발 단계에서 사용된 성능확인 방식으로 무기체계 양산 단계에서 재확인하는 것이라고 할 수 있다. 다만, 모든 AI 적용 무기체계에 대해 성능점검을 수행하는 것은 아니고, AI 모델의 변경 또는 AI 모델의 입력값에 변화를 일으킬 수 있는 요인의 변경이 있는 경우 양산 단계에서의 성능 재확인이 필요하다고 할 수 있다.

양산 단계 AI 성능점검 절차는 Fig. 3과 같이 최초양산 단계에서 개발주관기관으로부터 데이터, 기술자료, (Technical Data Package, 이하 “TDP”), 시험 절차 등을 제공받아 기품원이 주관하여 성능을 재확인하며, 소요군이 시험 요구사항을 확인하기 위해서 성능점검 시 입회를 할 수 있다. 세부적으로 AI 모델의 변경이 있는 경우는 성능 재확인이 필요한데, 성능 재확인 시 개발 중 사용된 성능평가 방법을 사용해야 하며 개발주관기관은 성능지표, 시험절차, 시험방법, 데이터 등을 제공해야 한다.

단, 개발자가 시험의 동일성을 보장하는 경우 다른 방법으로 수행할 수 있다. AI 모델의 변경은 없더라도 입력값에 영향을 주는 요인(HW, SW)이 변경된 경우에도 성능 재확인 단계가 필요하다. 대표적인 요인 변경의 예로 센서 기종, 카메라 해상도, 영상처리 알고리즘 변경 등이 있을 수 있다. 만약 이러한 입력값에 영향을 주는 요인의 변경이 없는 경우 체크섬, 버전 확인 등 기존의 SW 품질 보증 방법을 적용하게 된다. 이러한 AI 성능점검 절차를 최초양산, 주요 형상변경 시점에서 수행할 수 있으며, 향후 명확한 절차 및 제도가 정립된다면 AI 모델 적용 제품 계약 시 양산 품질보증을 위한 성능 재확인 요구조건, 방법과 절차 등을 명시할 필요가 있다.

3.4 운영·유지 단계 모니터링

AI 기술이 적용되지 않은 일반적인 무기체계의 경우 기존의 획득절차에 따라 연구개발 단계 간 시험평가와 규격화, 양산 간 품질보증 등을 거쳐 군에 전력화가 된다면 요구성능이 보장되어있다고 할 수 있다. 하지만 최근

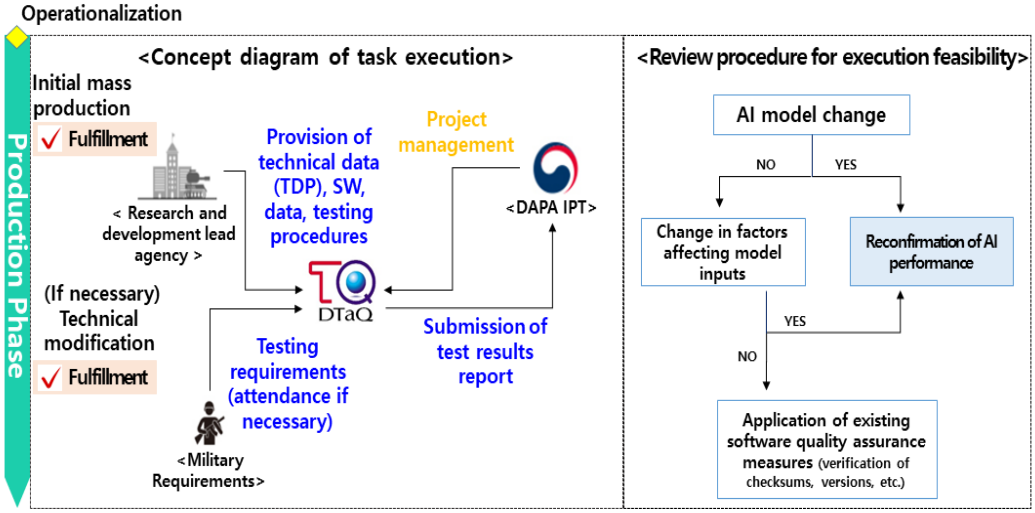

Fig. 3. Definition and scope of AI performance evaluation

시범적으로 도입된 일부 AI 기술이 적용된 무기체계의 경우 실 환경 적용 시 기대에 미치지 못하는 성능이 발생하고 있고, 이에 대한 성능개선 필요성이 요구되고 있다. 이는 개발 시 전력화될 체계가 모든 운용환경을 고려하기에는 한계가 있을 뿐만 아니라, 계속적으로 환경이 변화할 수 있다는 점 때문에 발생하는 문제라 생각된다. 따라서 AI 구현 성숙도 평가 단계 및 AI 성능점검 단계에서 AI 기능시험과 시스템 시험을 수행하였더라도, 전력화

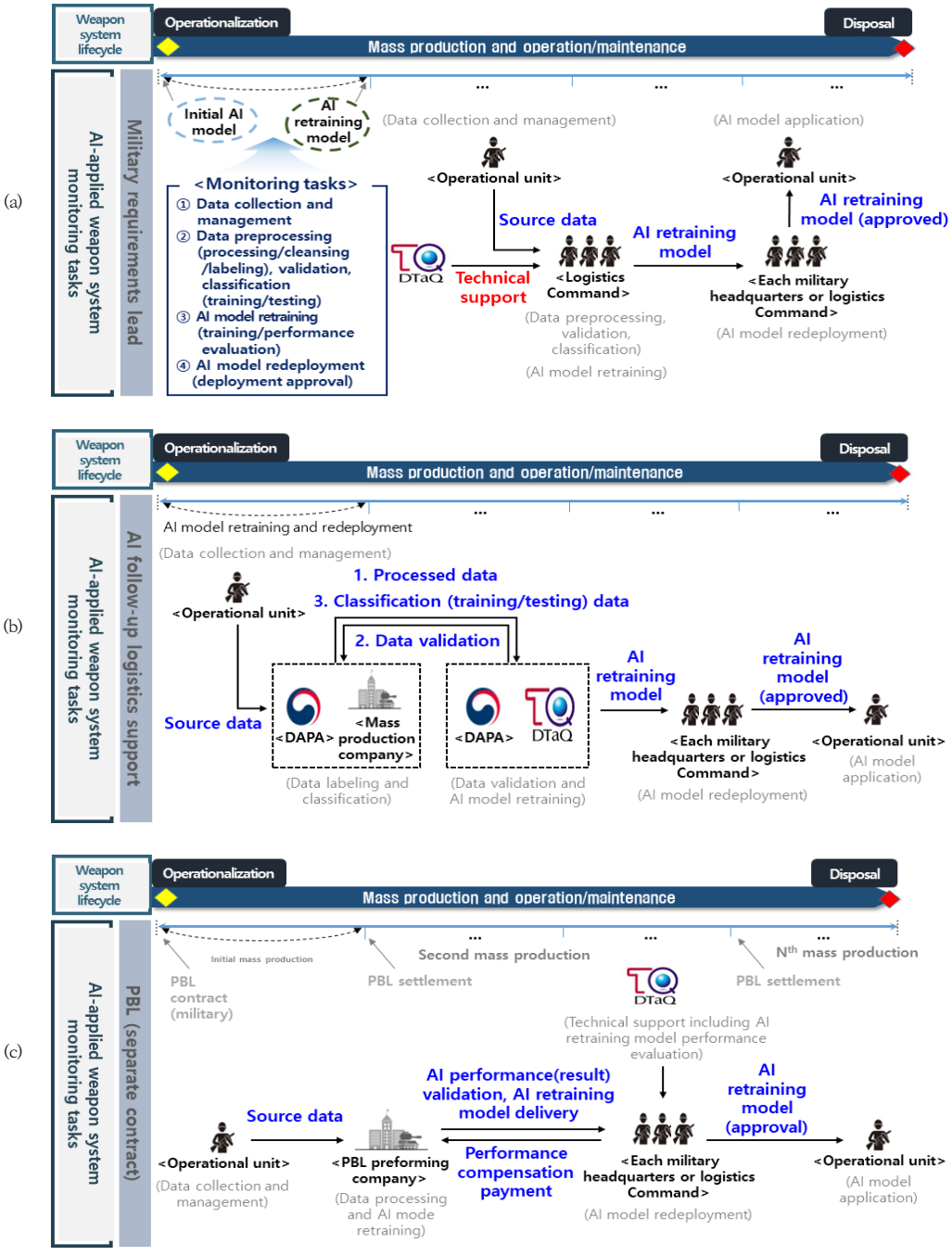

Fig. 4. Conceptual diagram of monitoring in the operation and maintenance stage

이후 실제 배치된 운용환경과의 적합성, 지속적인 모델 최신화 등의 수행이 필요하다. 기품원은 이러한 필요성을 기반으로 운영·유지단계에서의 품질관리 활동으로 모니터링 업무를 수행하고자 한다. 모니터링 업무의 목적은 실 운영단계에서 확보되는 자료를 활용한 재학습과 최신화 수행이며, 주요 과업으로서 데이터의 수집과 관리, 데이터의 가공, 검증 및 분류, 모델 재학습, AI 모델의 재배포 4가지로 구분하고 있다. 해당 과업에 대한 업무추진 관점은 3가지로 제시하였다. 첫 번째 업무추진 관점은 소요군 주관으로 수행할 경우 Fig. 4(a)이며, 두 번째 업무추진 관점은 후속 군수지원 활용하는 경우 Fig. 4(b)이다. 마지막 업무추진 관점은 기존의 성과 기반 군수(Performance Based Logistics, 이하 “PBL”) 개념을 활용하는 경우 Fig. 4(c) 이다. 3가지 업무추진 관점의 적용은 무기체계에 적용되는 AI 기술의 역할에 따라 보조기능일 경우 소요군 주관 활동으로 수행하고, 중요기능으로 판단될 경우 후속 군수지원, PBL 등을 적용하는 것을 고려하고 있다.

앞서 언급한 업무 추진관점에서 기품원의 역할은 데이터 검증 및 분류와 AI 모델 재학습 및 성능평가 관점의 기술지원이며, 이는 앞으로 관련 부서들과의 업무협조와 공감대 형성이 필요할 것으로 생각된다. 또한, 해당 과업 수행을 위해서는 향후 AI 성능평가 관련 제도개선과 병행되어야 하며, 앞서 언급하였듯이 전력화 이후 PBL 등과 연계하여 성능 보완 및 최신화를 수행하는 등 여러 가지 관점으로 검토되어야 할 필요성이 있다. 또한, 모니터링 수행과 관련하여 대상 선정, 계획 수립, 분석 주기 등에 관한 지속적인 연구를 통해 업무를 발전시켜야 한다고 판단된다.

4. 결론

본 논문에서는 국방분야 AI 적용 무기체계 도입과 관련하여 국내·외 AI 기술 도입 동향 및 성능평가 관련 이슈에 대하여 조사하였으며, 이에 대한 시사점으로 2가지를 들 수 있다. 첫째, 현재 국방분야에서도 선진국을 중심으로 첨단기술 패권경쟁에서의 우위 달성과 전투의 효율적 수행을 위하여 AI 기술에 관한 연구는 지속적으로 수행될 예정이며, 우리나라도 이에 따른 대응으로 AI 과학기술 강군 육성을 목표로 국방부, 방사청을 중심으로 AI 기술 관련 지속적인 관심과 연구가 필요하다는 점이다. 둘째, 최근 국방부, 방사청에서 제시되고 있는 정책 방향은 중·장기적인 측면에서 AI 거버넌스 조성, 소요·기획, 기술개발 등을 중심으로 추진되다 보니, 선진국에서 AI 기술 도입 시 고려하고 있는 중요 요소 중 하나인 “신뢰할 수 있는 AI”에 대해 고려가 미흡함으로 향후 해당 분야에 관한 연구가 필요하다는 점이다.

이에 본 연구를 통해 전투원이 믿고 사용할 수 있는 AI 실현의 요소인 품질확보는 AI 성능평가와 모니터링으로 확보될 수 있다는 관점하에 연구개발 단계, 양산 단계, 운영·유지 단계를 구분하여 AI 구현 성숙도 평가, AI 성능점검, 모니터링 방안과 해당 업무를 고도화하기 위한 향후 연구 방향에 대하여 일부 제시하였다. 아직 해당 업무를 수행하기 위해서는 유관기관들 간의 공감대 형성, 업무를 위한 제도개선 및 업무협조체계 구축 등 풀어야 할 문제가 많지만, AI 과학기술 강군 육성이라는 목표하에 믿고 사용할 수 있는 AI 적용 무기체계 도입을 위한 지속적인 관심과 연구를 수행이 필요할 것으로 생각된다.

References

[1] J. H. Kang, M. K. Jeong, J. Y. Park, W. Y. Lee, E. J. Choi, "A Study on the Policies, Application cases and Limitations for the Introduction of Artificial Intelligence(AI) Technology," *J. of the Korea Academia-Ind. cooperation Soc.*, vol. 24, no. 9, pp. 341-349, Sep. 2023.
DOI: https://doi.org/10.5762/KAIS.2023.24.9.341

[2] J. H. Yoon, Major Issues in the Introduction of AI Technology in the Defense Field and Plans to Improve Utilization, Technical Report, Science&Technology Poicy Institute, Korea, 2021.

[3] K. H. Choi, J. J. Oh, Y. G. Kim, "The Implications to ROK Armed Forces from the Artificial Intelligence Strategy of U.S. Department of Defense and Army", *Journal of The Korea Association of Defense Industry Studies*, Vol.27, No.1, pp.41-52, 2020.
DOI: http://doi.org/10.52798/KADIS.2020.27.1.4

[4] DoD(U.S. Department of Defense), “Responsible Artificial Intelligence Strategy and Implementation Pathway,” Policy Report, the U.S. Department of Defense(DoD), United States of America, Jun. 2022.

[5] GAO(the U.S. Government Accountability Office), “Artificial Intelligence: An Accountability Framework for Federal Agencies and Other Entities,” Policy Report, the U.S. Government Accountability Office(GAO), United States of America, Jun. 2021.

[6] NIST(National Institute of Standards and Technology), “Artificial Intelligence Risk Management Framework (AI RMF 1.0)”, Policy Report, National Institute of Standards and Technology(NIST), United States of

America, Jan. 2023.

[7] Y. M. Lee, "A Study on the Performance Enhancement of AI-Applied Weapon Systems at Operation and Sustainment Stage," Pro. of Korea Institute of Military Science and Technology Conf., pp.811-812, Nov. 2023.

[8] ISO/IEC, "ISO/IEC TR 29119-11 Software and systems engineering — Software testing — Part 11:Guidelines on the testing of AI-based systems," Technical Report, ISO/IEC, Nov. 2020.

강 지 훈(Ji Hoon Kang) [정회원]

- 2013년 2월 : 경상대학교 전자공학과 (공학사)
- 2015년 8월 : 경상대학교 전자공학과 (공학석사)
- 2016년 8월 ~ 2019년 7월 : 한국산업기술시험원(KTL) 연구원
- 2019년 8월 ~ 현재 : 국방기술품질원(DTaQ) 연구원

〈관심분야〉
국방, 전자공학, 인공지능, 시험평가

정 민 경(Min-Kyung Jeong) [정회원]

- 2020년 2월 : 부산대학교 나노메카트로닉스공학과 (공학사)
- 2019년 12월 ~ 현재 : 국방기술품질원(DTaQ) 연구원

〈관심분야〉
국방, 인공지능, 전자회로, 반도체 공정기술

이 영 민(Yeong-Min Lee) [정회원]

- 2016년 8월 : 금오공과대학교 전자공학부 (공학사)
- 2020년 8월 : 금오공과대학교 전자공학과 (공학석사)
- 2021년 7월 ~ 현재 : 국방기술품질원(DTaQ) 연구원

〈관심분야〉
인공지능, RF 회로 설계, 안테나 설계 및 해석

박 주 영(Joo-Young Park) [정회원]

- 2015년 2월 : 숭실대학교 전기공학과(공학사)
- 2019년 1월 ~ 현재 : 국방기술품질원(DTaQ) 연구원

〈관심분야〉
국방, 전기, 전자, 인공지능, 사이버보안