

무기체계 획득에서 인공지능-시스템엔지니어링 융화를 위한 최상위 수준의 AI4SE, SE4AI 구현방안

이민우^{1)*}

1) 대한민국 방위사업청

Top-Level Implementation of AI4SE, SE4AI for the AI-SE convergence in the Defense Acquisition

Min Woo Lee^{1)*}

1) Defense Acquisition Program Administration (DAPA) of the Republic of Korea

Abstract : Artificial Intelligence (AI) is a prominent topic in almost every field. In Korea, Systems Engineering (SE) procedures are applied in Defense Acquisition, and it is anticipated that SE procedures will also be applied to systems incorporating AI capabilities. This study explores the applicability of the concepts “AI4SE (AI for SE)” and “SE4AI (SE for AI),” which have been proposed in the United States, to the Korean context. The research examines the feasibility of applying these concepts, identifies necessary tasks, and proposes implementation strategies. For the AI4SE, many attempts and studies applying AI to SE Processes both Requirements & Architectures Define, System implementation & V&V, and Sustainment. It needs Explainability and Security. For the SE4AI, the Functional AI implementation level, Quality & Security of the Data-set, AI Ethics, and Review policies are needed. Furthermore, it provides perspectives on how these two concepts should ultimately converge and suggests future directions for development.

Key Words : Artificial Intelligence, Systems Engineering, Defense Acquisition, Weapon Systems, Convergence

Received: November 20, 2023 / **Revised:** December 8, 2023 / **Accepted:** December 21, 2023

* Corresponding Author: Min Woo Lee / DAPA / fstblue@korea.kr

This is an Open-Access article distributed under the terms of the Creative Commons Attribution Non-Commercial License(<http://creativecommons.org/licenses/by-nc/3.0>) which permits unrestricted non-commercial use, distribution, and reproduction in any medium, provided the original work is properly cited

1. 서론

인공지능(Artificial Intelligence, 이하 AI)은 국방분야 뿐만 아니라 산업/문화/예술/체육/교육 등 거의 모든 분야에서 공통적으로 떠오르는 가장 중요한 이슈이다. 각종 서적이나 콘텐츠에는 기존 방법론에 “AI”, “챗GPT”라는 단어를 붙이는 방법으로 화제성을 강조하고 있으며, “AI 없는 세상”, “AI가 인류를 삼키는 세상”에 대한 불안감을 호소하고 대비를 외치는 사람들도 있다.

AI는 최근 갑자기 등장한 개념이 아니라 상당히 오래전에 등장한 개념이며, 빠른 컴퓨팅을 위한 장비, 부품 관련 기술의 비약적인 발전에 따라 이를 기반으로 더욱 혁신적인 AI 구현방안이 연구되어 지금의 붐이 일어난 것으로 판단된다. 다른 분야와 마찬가지로, 국방분야에서는 기술혁신의 구심점으로 AI를 내세우고 있는데, 선진국과 비선진국을 막론하고 무기체계 및 전력지원체계 모두에 AI 기능을 적용하고자 노력하고 있다.

한편, 우리나라는 방위사업청 훈령인 “방위사업관리규정”에서 무기체계 획득 시 시스템공학(Systems Engineering, 이하 SE) 절차를 의무적으로 적용하도록 규정하고 있는데, 이에 따라 효율적인 총수명주기관리가 가능하도록 단계별 기술검토와 다양한 과학적 사업관리 기법을 적용하고 있다. 다만, 적용 초기단계에서 많은 사람들이 SE의 적용원리보다는 다양한 기술검토회의와 산출물에 집중하여 사업을 관리해 온 탓에 일각에서는 “적용이 불필요한 방법론”, “신속한 획득을 방해하는 장애요소”로 취급하는 목소리도 나오고 있다.

그럼에도 SE는 복잡한 시스템을 구현하고 관리하기 위한 가장 효율적이고도 효과적인 개념이며, 이는 AI 기능이 포함된 시스템 구현에서도 같다. 군사분야의 가장 선도적인 입지를 갖춘 미국 역시 이러한 관점을 유지하고 있으며, “보다 효율적인 SE 활동을 위한 AI의 역할” 및 “AI 기능을 적용한 시스템 획득을 위한 SE의 역할”에 대한 다양한 연구가 이루어지고 있다.[1] 이를 “AI4SE(AI for SE) &

SE4AI(SE for AI)”라는 용어로 축약해서 표현하고 있는데, 국방혁신 4.0의 핵심 요소로서 AI의 적용을 추구하고 있는 우리나라 역시 AI4SE, SE4AI에 대해 본격적으로 연구해야 할 시점이라고 판단된다.

본고는 국방분야에서 AI4SE 및 SE4AI 이행 방안을 주로 정책적인 측면에서 제시하는 논문이다. 서론에 이어 제2장에서는 AI4SE, 제3장에서는 SE4AI 구현에 관련된 선행연구, 구현방안 및 선결과제를 각각 제시하였다. 마지막인 제4장은 결론으로서 두 가지 개념이 결국 어떻게 수렴할 것인지에 대한 견해와 함께 후속 연구방향을 제시하였다.

2. 보다 효율적인 시스템엔지니어링 활동을 위한 인공지능의 역할 - AI4SE

2.1 AI 적용이 가능한 SE 프로세스 검토

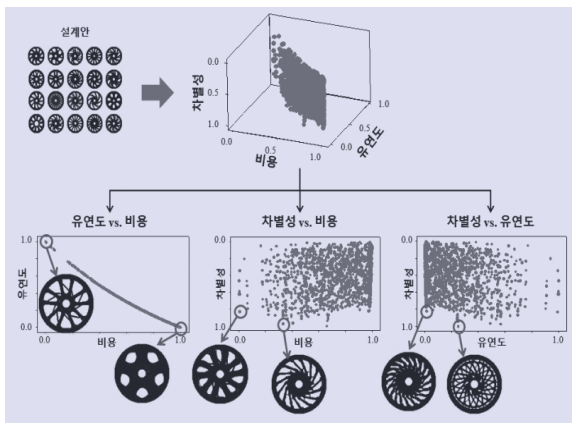
시스템엔지니어링 활동을 보다 효율적으로 수행하기 위해, 지금까지는 기존 문서기반 활동을 탈피하고 전산모델을 활용하여 SE 활동에 필요 일정과 비용을 단축하려는 모델기반 SE(Model-Based SE, MBSE) 개념이 제시되어 국내에서도 관련된 연구가 있었다.[2] 최근에는 AI 기법을 활용하여 더욱 효율적인 SE 활동을 수행하기 위한 연구들이 있는데, 이 연구들을 단순히 나열하기보다는 ISO/IEC/IEEE 15288:2015[3]의 기술 프로세스 활동을 기반으로 다음의 세 가지로 분류하여 제시한다. 첫째, 시스템 요구사항 및 아키텍처 정의 분야로, 김진일 등[4]이 분석하여 제시한 내용을 중심으로 소개할 것이다. 둘째는 시스템 통합 및 검증확인 분야이며, 셋째는 시스템 운영유지 분야에서도 AI를 적용하는 연구가 존재하였다.

2.1.1 요구사항 및 아키텍처 정의 분야

시스템 요구사항 정의 활동은 사용자의 정제되지 않은 요구, 즉 Needs를 시스템 개발에 활용 가능한 수준의 요구, 즉 Requirements로 변환하는 것이다. 개발자들은 프로젝트 초기에 막연한 Needs를 분석

하고 정제하여 시스템 개발 및 검증&확인에 필요한 요구사항을 도출하는데, 요구사항이 올바르게 도출되었는지 검증하는 것은 상당히 주관적인 영역이므로 어려움이 많다. 이에 Tetsuo 등[5]이나 IBM[6]은 자연어 처리 또는 머신러닝 기법을 적용하여 요구사항들의 무결성을 분석하는 등 품질 검토 방법론과 도구를 제시하였다.[4]

개발자들에 의해 도출된 요구사항이 승인되면, 이를 기반으로 여러 가지 시스템 아키텍처를 도출하여 일정/비용/성능을 고려한 최적의 대안과 구현 방법을 검토하는 과정이 필요하다. 오상은 등[7]은 그림 1과 같이 딥러닝 기반 생성모델을 통해 기본적인 파라미터를 기반으로 다양한 설계방안을 생성하여 이들을 평가하여 선호도에 따라 추천하는 딥 제너레이티브 디자인을 제시하였다.[4]



[Figure 1] Deep Generative Design's Design Validation example

또한, 김상국 등[8]은 가상 설계지원(Virtual Design Assistant, VDA) 플랫폼 기술을 발표하였는데, 이는 설계 전문가와 데이터로 학습된 AI 플랫폼이 상호작용하며 진화적인 개발을 추구하는 개념이다.[4]

2.1.2 시스템 통합 및 검증확인 분야

시스템 설계를 거쳐 구현된 시스템의 세부요소를 하나의 완성된 시스템으로 통합하는 과정은 매우 중요하다. 시스템에 적용된 소프트웨어의 무결성을 검

증하고, 식별된 결함을 하나하나 수정하는 것은 인간이 직접 수행할 수 있는 영역이 아니라고 판단된다. 이성복[9]은 소프트웨어 엔지니어링의 각각 단계에서 머신러닝 기술을 적용할 수 있음을 증명하였으며, 특히 구현 및 검증 단계에서는 데이터의 시각화와 설명가능한 AI(Explainable AI, XAI)의 적용이 필수적이라는 견해를 제시하였다.

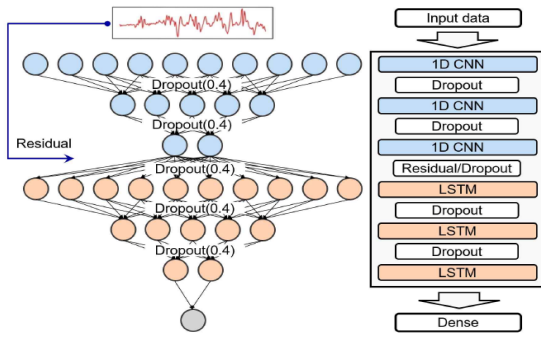
시스템 하드웨어의 체계통합과 양산 공정에 대한 점검과정 역시 지금까지는 인간에 의한 공정 확인 및 검수작업에 의존하였으나, 무인화 시스템의 경우 고정밀 구성품이 집적되므로 기존 방법론의 한계를 극복하기 위해 디지털 트윈 활용방안이 제시되고 있다. 정재성[10]은 공정과정에 디지털 트윈을 운영하기 위해 데이터 동기화, 계통 해석, 고장 진단 및 복구 등의 과정에서 강화학습이나 CNN, GAN 등의 딥러닝 모델을 활용할 수 있다고 제시하였다.

한편, 김각규 등[11]은 장차 AI 적용 무기체계가 군에 도입된 이후 전력화평가 및 야전운용시험 시 디지털 트윈을 활용하는 방안을 제안하였는데, 전술한 바와 같이 디지털 트윈 방법론은 AI 기술과 결합되어 시너지를 낼 수 있는바, 시스템 검증 및 확인 분야에서도 AI의 활용성이 제시된 것이라 하겠다.

2.1.3 시스템 운영유지 분야

시스템엔지니어링 관점에서는, 시스템 획득뿐만 아니라 장기간의 운영유지를 어떻게 효율적으로 수행할 수 있는지에 대해 깊은 고찰이 필요하다. 운영유지에는 시스템 획득보다 훨씬 많은 비용이 소요되기 때문에, 정비 및 수리를 위한 부속품의 적정 재고량을 산출하거나 잔여수명을 예측하여 이후의 정비전략을 재검토하는 과정이 매우 중요하다.

홍창우[12]는 예지정비 개념을 본격적으로 적용하기 위해 AI 및 빅데이터 기술을 활용해야 한다고 제시하면서, 잔여유효수명 예측과 부품의 이상 감지 결과에 그림 2의 심층신경망(DNN) 모델과 마할라노비스 거리 분석 등을 활용하여 유의미한 향상이 가능함을 증명하였다.



[Figure 2] Deep Neural Network Model for the Predictive maintenance

2.2 AI4SE 구현을 위한 선결과제

지금까지 다양한 SE 프로세스에 AI 기술 적용이 충분히 가능함을 살펴보았는데, 이를 각 단계에서 단편적으로 적용하는 것보다는 시스템 총수명주기 관리(TLCSM) 측면을 고려하여 통합적인 관리를 할 수 있는 지원 도구와 방법론 마련이 필요하다고 판단된다. 이러한 AI 기반 SE 지원 도구를 갖추기 위해서는 다음의 선결사항이 존재한다.

첫째, 설명가능한 AI(XAI)를 적용하여야 한다. 요구사항 및 아키텍처 정의, HW/SW 통합성 확인, 시스템 검증&확인 및 운영유지 활동에 사용된 AI 기능을 이해관계자가 100% 신뢰하고 활용하려면, 산출물을 제시하는 과정에서 AI가 얼마나 관여했고 판단과정과 추론 근거가 무엇인지에 대해 명확하고 구체적으로 설명할 수 있어야 한다. 단순한 자연어 처리과정에서는 이렇게 자세히 설명할 필요가 크지 않겠지만, 딥러닝이나 심층신경망 등을 적용할 경우 XAI 적용이 반드시 필요하다.[10],[12]

둘째, AI 기반 SE 지원 도구의 보안성을 충분히 확보하고, 지식재산권 보호 방안을 강구해야 한다. 국방분야는 군사보안 및 방산기술 보호 차원에서 주로 내부망 위주로 각종 자료를 운용하고 있으며, 외부망, 즉 인터넷과의 직접 연결을 지양하고 있다. 하지만 SE 지원 도구가 완전한 AI 기능을 구현하기 위해서는 필연적으로 외부망과 연결되어야 하므로, 지금까지 없었던 내부망-외부망 연결에 따라 보다 철저한 보안성을 갖추는 것이 최우선 과제가 될 것

으로 전망한다. 비단 외부망에 연결되지 않더라도, 최근 논의되고 있는 챗GPT에 국가운영 관련정보를 활용하지 않도록 하는 보안 가이드라인이 수립되고 있는 등 통제대상 정보를 활용한 AI 기능 사용에는 신중한 접근과 철저한 보안성 확보가 필요하다.

또한, 지원도구 운영은 국가기관이 주도하더라도 연구개발주관기관인 방산업체들 역시 도구를 활용하여 연구개발 활동에 참여해야 하므로, 각 업체는 자사 설계자료가 AI 기능을 통해 유사한 프로젝트에서 다른 업체에 의해 활용되는 상황을 경계하게 될 것이다. 이러한 우려를 해소하지 못한다면, 지원 도구 개발과 활용은 시작단계부터 난항을 겪을 수 있다. 따라서, 연구개발주관기관의 지식재산권 보호 방안을 강구하는 가운데 AI 기반 SE 지원 도구를 마련하기 위해 노력해야 할 것이다.

3. 인공지능 적용 무기체계의 TLCSM을 위한 시스템엔지니어링 역할 - SE4AI

다른 분야와 마찬가지로, 국방분야에서도 AI와 무인화 시스템의 도입 및 적용을 통해 기술추세와 사회환경에 부합하는 세상을 만들어가려는 다양한 시도가 이루어지고 있다. 이번 장에서는 인공지능 적용 시스템을 획득함에 있어 시스템엔지니어링이 왜 필요하며 구체적으로 어떠한 역할을 수행할 수 있는지, 그 선결조건은 무엇인지 살펴보도록 한다.

3.1 AI 적용 무기체계 획득에 SE 적용 필요성

국내에서, AI 기능이 적용된 시스템의 확보 관련 최근의 논의들이 가장 아쉬운 점은 시스템공학이 아니라 오직 소프트웨어공학 관점이 주를 이루고 있다는 점이라고 판단되며, 본격적인 논의에 앞서 왜 SE가 AI 적용 시스템 획득에 필수적인지를 짚어보고자 한다. AI 비전문가 관점에서, 다음의 막연한 기대를 할 수 있다.

- AI는 인간이 할 수 있는 모든 업무를 수행할 수 있다.

- AI는 스스로 우리가 필요한 것을 해 줄 것이다.
- AI를 적용하면 운용인력 절감에 도움이 될 것이다.
- AI를 적용한 시스템은 모든 면에서 우수하다.
- AI를 적용한 시스템은 획득하기만 하면 된다.

현재까지, AI는 전지전능한 해결책이라 하기는 어렵다. AI는 개발된 목적에 부합하도록 동작하여 한정된 기능과 역할을 하는 단일 또는 다수의 프로그램 집합체라고 할 수 있다. 여기서 중요한 것은, AI 기능의 구현 목적인 운영개념을 정립하고 이를 통해 구체적인 요구사항을 개발해야 한다는 것이다. 이는 비단 개발자만의 몫이 아니라 이해관계자들 모두가 힘을 합쳐야 한다.

AI를 적용하면 시스템 자체만으로는 언뜻 보아 운용인력이 절감되는 효과를 기대할 수도 있겠으나, 역설적으로 AI 기능의 기반이 되는 데이터셋 관리 및 학습, 유지보수를 위해 기존에는 필요하지 않던 많은 정비인력이 필요하다고 판단된다.

“우수하다”라는 표현의 기준에 따라 달리 볼 수 있겠으나, 이를 성능만으로 한정하지 않고 소요자원 대비 효과 관점에서 살펴보자면 AI를 적용한 시스템이 모든 면에서 우수하다고 단정할 수 없다. 확실히 성능 측면에서는 해당 시스템이 효과도가 더 높아질 가능성이 있겠지만, 전술한 바와 같이 많은 정비인력과 함께 높은 품질의 데이터셋을 확보 및 관리하고, 이를 지속적으로 학습시키면서 알고리즘 개선과 서버 능력 보강을 위한 다양한 인프라, 즉 Enabling systems를 동시에 획득하고 총수명주기 동안 운영유지해야 하므로, 비용대 효과가 언제나 높다고는 볼 수 없다고 판단함이 타당하다.

AI는 한번 학습한 것만으로 목표로 하는 최상의 성능을 발휘할 수 없을 가능성이 높다. 지속적으로 학습과 보안을 거쳐 발전해야만 비로소 그 목적에 부합하는 충분한 역할을 할 수 있는 것이다. 이와 같이 AI 적용 시스템은 획득만으로 문제를 해결할 수 없으며, 총수명주기관리 관점의 접근이 반드시 필요하다고 할 수 있다.

지금까지 나열한 막연한 기대에 대한 현실적인 한계와 필수적인 사항들의 핵심 키워드를 나열하면, ① 운영개념 정립, ② 요구사항 개발, ③ 성능-비용 절충, ④ 수명주기 지원체계(Enabling systems) 확보, ⑤ 총수명주기 관리(Total Life-Cycle Systems Management) 등 다섯 가지로 제시할 수 있겠다. 이 모든 것들을 중요하게 바라보고 시스템 획득 및 운영유지를 위해 활용할 수 있는 학문은 무엇인가? Kossiakoff 등[13]에 따르면, 이러한 모든 관점을 종합적으로 다루는 것이 바로 시스템공학이다. 결론적으로, AI 적용에 대한 요구를 모두 충족하는 가운데 시스템을 획득 및 운영유지하기 위해 반드시 시스템공학적 접근방법이 요구된다.

3.2 AI 적용 무기체계의 총수명주기관리를 위한 SE 프로세스

그렇다면, AI 적용 무기체계는 어떤 시스템공학 접근이 필요한가? 이번 장에서는 그림 3에서 보는 무기체계의 소요기획단계로부터 획득, 운영유지 및 폐기까지의 총수명주기 프로세스를 크게 세 가지로 분류하여 시스템공학 관점에서 제도적 발전 방향과 적절한 수행방안을 제시하였다.



[Figure 3] Defense Acquisition and O&S Process

3.2.1 소요기획 및 선행연구 단계의 SE4AI

무기체계 소요기획 활동은 주로 소요를 결정하는 합동참모본부와 운영자이자 소요제기 기관인 각군, 그리고 이를 지원하는 방위사업청과 연구기관들이 함께 모여 사업추진이 가능한 수준의 요구사항과 획득 목표 수량 및 시기 등을 결정하는 과정이다.

최근에는 소요기획 시 사전개념연구 체도를 통해 국방과학연구소의 기술지원을 거쳐 현재 또는 머지않은 미래에 구현 및 검증 가능한 요구성능을 도출하고자 노력하고 있다. 따라서 AI 기능 반영이 필요

한 대상체계 및 수준을 검토하고 이를 운용요구서 초안에 반영하도록 함이 타당하다. 현재까지는 사전 개념연구 수행조직에 AI 및 데이터과학 전문인력이 거의 없을 것으로 판단되나, 조속히 전문인력을 확보하고 조직의 역량을 갖추어 AI 적용 무기체계가 적절한 요구사항을 갖도록 해야 한다.[14]

이 단계에서 가장 중요하다고 제시하는 것은 두 가지이다. 첫째, 요구사항의 검증 가능성을 반드시 고려해야 한다. 과거 추종형 무기체계의 경우 해외 장비들의 발전추세를 고려하여 개발과정에서 목표 성능을 구체화하는 일이 잦았기에, “기술발전 추세를 고려하여 향후 결정”과 같은 성능 요구사항이 제시되더라도 크게 문제되지 않았다. 하지만 AI에 대한 요구사항들은 반드시 검증할 수 있어야 한다. AI 기능은 선진국의 기술발전 추세를 확인하기가 어렵고, 연구개발 과정에서 막연한 요구사항으로는 사업을 제대로 시작할 수도 없다고 판단된다.

둘째, AI 기능을 적용하는 이상 필연적으로 AI가 데이터를 학습하고 훈련을 통해 발전해야 하므로, 적어도 ① 학습 및 훈련 목적, ② 개발자가 시스템 학습 결과를 검증할 목적, ③ 운전자 또는 제3자가 객관적으로 기능을 평가할 목적 등 다양한 목적의 데이터 확보 방안에 대해서도 같이 검토해야 한다. [14] 만약, 제공 불가능한 데이터로 학습해야만 그 효과를 발휘하는 기능을 요구한다면 해당 무기체계 개발은 커녕 사업자 선정조차도 어려울 것이다.

3.2.2 획득단계(개발, 양산 및 전력화)의 SE4AI

무기체계 개발과정에서는, 특히 데이터셋을 통한 AI 기능 구현이 중요하다. 동시에, 데이터셋 확보와 반복적인 검증행위가 필수적이라 할 수 있다.

데이터셋은 아래의 표 1과 같이 다양성, 정확성, 유효성 측면에서 품질관리가 필요하다.[15]

개발과정에서 필요한 데이터셋은 최초 확보하는 시점에서 표 1의 다양성 및 정확성에 대한 검증을 수행해야 하고, 데이터셋을 목적별로 분류할 때는 유효성에 대해 검증해야 한다.[14] 또한, 평가용으

로 분류된 데이터셋의 경우 다양성/정확성/유효성 모두를 검증해야 확실한 시험평가가 가능하므로 보다 관심을 기울여야 한다.

<Table 1> Quality Verification context for Datasets

| 항 목 | 품질검증 내용 |
|-----|--|
| 다양성 | <ul style="list-style-type: none"> • 데이터가 편향되지 않도록, 주요 특성을 통계적 방법으로 분석(관심 객체, 카테고리, 수집환경 등) |
| 정확성 | <ul style="list-style-type: none"> • 구문 정확성 : 라벨이 정확하게 입력되어 있고, 필수항목 중 누락된 내용이 없는지 검사 • 의미 정확성 : 라벨이 의미적으로 참인지 검사하여 라벨의 정답 비율 확인 |
| 유효성 | <ul style="list-style-type: none"> • 인공지능 학습모델로 데이터 훈련 후, 목표 수준의 성능 달성이 가능한지 확인 • 훈련용(개발과정에서 인공지능 학습에 사용)/ 검증용(학습과정에 이상이 없는지 확인)/ 평가용(시스템 적합성 판정용)등으로 구분 |

감시·정찰 또는 정밀타격 분야에 사용되는 무기체계의 경우에는, AI 기능 구현에 필요한 데이터셋 확보 및 관리 과정에서 소요군과 개발기관 모두가 군사보안에 각별히 유념해야만 한다. 상당히 민감한 정보자산을 통해 확보된 데이터셋이 부적절한 관리로 인해 유출될 경우도 문제이지만, 악의적인 AI 공격용 데이터가 비의도적으로 수집될 경우에는 구현과 평가 모두 난항을 겪을 수 있으므로, 데이터셋의 검증과 관리 모두 중요하다고 판단된다.[14]

3.2.3 운영유지단계(전력화 초기부터)의 SE4AI

성공적으로 평가를 거쳐 개발이 완료되고 비로소 운용부대에 무기체계가 배치되면, 전력화 과정에서 AI 기능을 포함하여 전반적으로 그동안 식별되지 않았던 문제점들과 오류들이 식별될 수 있다. 이에 초도양산 후 전력화평가를 통해 식별된 문제점을 충분히 분석하여 필요시 기술변경 조치를 거친 뒤 후속양산에 이르러 완전성을 갖춘 무기체계가 모든 운

용부대에 공급된다.

AI 기능의 경우 문제점의 유형별로 조치방안이 각기 다를 것으로 판단된다. 예를 들면, 운용요구서(ORD)에 기술된 임무 시나리오에도 불구하고 초도 배치된 운용부대에서 부대 사정을 고려하여 다른 운용형태를 취함에 따라 기존 알고리즘의 수정이 필요할 수도 있고, 배치 이후 운용환경에서 학습한 데이터에 비정형성 오류가 존재하거나 적대적 예제 학습이 이루어져 기존 학습내용에 심각한 문제가 발생했을 가능성도 있다.

이러한 조치를 포함하여, 알고리즘과 데이터셋의 신뢰성을 지속적으로 유지하고 운용자가 무기체계 특성을 이해하는 과정에서 운용형태를 조금씩 개선하는 활동을 할 것이다. 이민우 등[14]은 운영유지 단계에서 이러한 소요를 충당하기 위해 기존 국방 M&S체계 운영유지단계에서 수행 중인 유지보수 및 성능개선 사업의 개념을 적용하여 착수에 장기간이 소요되는 신규 소요에 의한 성능개량보다는 훨씬 유연한 형상관리가 가능하도록 하는 방안을 제시한 바 있다. 구체적으로, 계약상대자로 하여금 AI 기능 유지보수 전문조직과 함께 운용자와 소통하며 운용개념을 발전시키고 AI 기능 교육훈련을 지원하는 전문분석관 조직을 구성 및 운용하도록 계약조건에 명

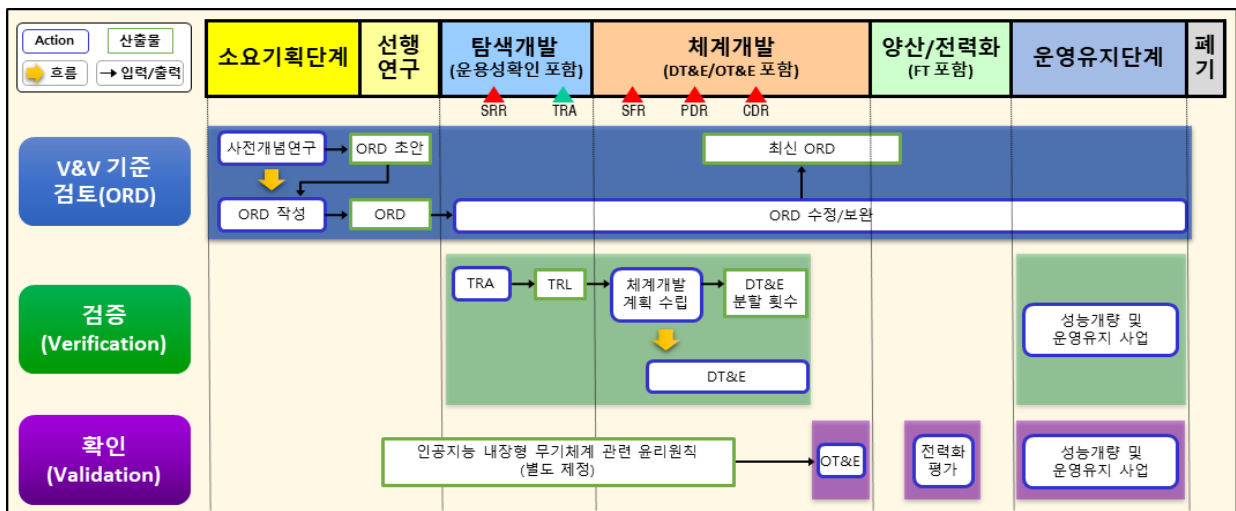
시하여 사업을 추진하는 것이다. 이를 통해 순환근무와 단기 근무가 이루어지는 부대원의 비전문성을 고려함과 동시에 전문인력에 의한 반복적인 알고리즘 수정 등의 형상관리를 수행하여 장기간의 운영유지에도 AI 기능이 잘 유지될 수 있을 것으로 기대한다. SE4AI의 핵심 요소는 이민우 등이 제시한 그림 4를 참조한다.[14]

3.3 SE4AI 구현을 위한 선결과제

지금까지 제시한 SE 프로세스가 잘 작동하려면, AI4SE와 마찬가지로 먼저 갖추어야 할 정책적인 숙제가 있다. 다음의 몇 가지 선결과제를 제시한다.

첫째, AI 기능의 수준은 한 가지로 정의할 수 없을 만큼 다양하다고 할 수 있으며, 이에 따라 사업 일정/비용이 각각 상이하고 경우에 따라 불필요한 고성능을 요구함에 따른 낭비요인도 발생할 것이다.

사업 초기단계에서 AI 기능 적용수준을 판단하고, 이에 부합하는 개발 및 검증 요구사항을 정립하는 활동이 필요하다고 판단되며, 이때 자율주행 수준, 유무인복합운용(MUM-T)에 필요한 상호운용성 수준 등 복합적인 고려가 필요하며, 민욱기 등[16]이 제시한 AI 기술 수준(AI Technical Level, ATL)을 유사한 사례로 제시한다.



[Figure 4] V&V Process for the TLCSM of AI-embedded Weapon Systems

<Table 2> AI Technical Level (ATL) 1.0

| | | | |
|-------|-----|---|---|
| Lv. 6 | ASI | 오픈 영역, 오픈 모달로 인간 개입 없이 지식이 성장하는 AI | AI가 스스로 미션을 만들고 수행할 수 있으며, 인간보다 빠르게 판단 |
| Lv. 5 | AGI | 인간의 4대 이상의 지능 통합 가능, 사람의 부분 개입으로 지식이 성장하고, 다른 분야로 확장 가능 | AI가 인간/상황/이력/지식을 종합 판단 가능, 인간과 상호 토론 및 목적에 따른 설득. 최종 판단은 사람 |
| Lv. 4 | | 인간의 2대 지능 이상을 통합적으로 추론 가능, 인간 개입으로 지식 성장 및 유사 분야로 확장 가능 | AI가 2~3개 입력 모달리티를 종합 판단하여 추천하고, 판단 근거까지 설명 제공. 시행 여부 사람 판단 |
| Lv. 3 | ANI | 단일 분야에서 전문가 수준으로 지식처리 가능, 동일 분야에서 지식 재사용 | AI가 현상 분석/추천 가능, AI끼리 협력하거나 사람과 협력하여 미션 수행 |
| Lv. 2 | | 사전 훈련된 영역에서만 대응이 가능한 고정적인 지식을 가진 AI | 동일한 형식(음성 또는 이미지 등)에 대한 인지와 사전 정의된 미션 수행 |
| Lv. 1 | | 정해진 규칙에 대한 반응으로 동작(예: 실내기온 28도 이상 시 에어컨 동작) | 사전에 정해진 순서나 기계적 수칙에 의존한 인지(예: 선박수 위험 경고등) |
| | | 똑똑한 AI(IQ) | 인간과 소통하는 AI(EQ) |

* ASI/AGI/ANI : Artificial Super/General/Narrow Intelligence

둘째, AI 적용 무기체계에 대한 국제사회 우려와 관련 검토 동향을 고려하여 국제인도법상 전쟁의 원칙을 준수하면서도 다양한 AI 관련 기준을 준수할 수 있는 윤리성 기준을 검토하고, 이를 국방부, 합참 및 소요군과 연구기관이 책임있게 준수하도록 제도적으로 반영해야 한다. 표 3에서는 국방분야 AI 윤리성 기준에 대한 연구들을 살펴볼 수 있는데, 이민우 등[14]은 미국 국방성의 5가지 AI 윤리성 원칙 및 특정재래식무기조약(The Convention on Certain Conventional Weapons, CCW)에서 논의된 지도적 원칙 중 6가지를 필수요소로 꼽았다. 조재규[17]는 기업, 대학, 미국 국방성, 한국 정부의 윤리기준을 고려하여 중요도가 높은 5가지를 제시하였다. 후속연구를 통해 국방분야에서 AI 윤리성 기준이 조속히 정립되기를 기대한다.

셋째, 전술한 AI 윤리성 기준이 잘 마련되더라도, 무기체계가 이를 준수할 수 있는지 검증&확인하는 과정이 없다면 충분한 신뢰성을 담보하기 어렵다. 제네바협약 제1추가의정서 제36조에서는 새로운 전투수단 획득 시 의정서 체결당사국에 적용되는 국

<Table 3> Studies for the Defense AI Ethics

| 연구자 | 국방분야 AI 윤리성 기준 연구내용 |
|------------|---|
| 이민우 등 [14] | <ul style="list-style-type: none"> 추적성 : 투명하고 감사 가능한 방법론, 데이터 소스, 설계 절차, 문서화를 포함하여 담당자가 AI기술, 개발 프로세스, 운영 방법에 대한 적절한 이해를 갖도록 AI기능을 개발하고 배포 신뢰성 : AI기능은 명확하게 정의되고 이러한 기능의 안전, 보안, 효과가 전체 수명주기에 걸쳐 정의된 용도 내에서 시험 및 보장 통제성: AI기능이 의도한 기능을 구현하도록 설계하고, '의도하지 않은 결과를 탐지하고 회피', '의도하지 않은 행위를 보이는 시스템을 분리 또는 비활성화' 가능한능력을 보유 무기체계 사용 관련 인간의 책임 유지 신기술에 기반한 새로운 무기의 개발 및 획득 시 적절한 안전조치 및 비확산조치 고려 신기술의 인격화(anthropomorphize) 금지 |
| 조재규 [17] | <ul style="list-style-type: none"> 인간 존엄성(human dignity) : 국방 인공지능의 개발 및 활용 등은 인간에게 이로우야 하며, 인간에 대한 안전이 우선 고려되어야 한다 통제성(governability) : 국방 인공지능의 활용에 있어 반드시 인간의 통제가 수반되어야 한다 안전성(safety) : 의도된 목적 및 결과에 충족되는 신뢰있는행동을 해야 하며, 목적에 어긋나거나 예상되는 결과를 벗어난다고 판단되면 그 행위를 거부하거나 중단시켜야 한다 책임성(responsibility) : 인공지능 운용에 따른 결과는 인간이 모든 책임을 져야 한다. (주체 명확) 설명 가능성(explainability) : 인공지능의 의사결정에 대한 인과관계를 분석해 결과를 인간이 이해할 수 있는 수준에서 설명할 수 있어야 한다 |

<Table 4> Weapons Review policies

| 구분 | 미국 | 영국 | 호주 |
|-------|---|--|---|
| 주관 | 각 군 산하 법무실 | 각 군 법무관으로 구성된 통합 조직에서 2인의 법무관이 수행 | |
| 시점 | <ul style="list-style-type: none"> 시제 개발 초도생산 | <ul style="list-style-type: none"> 예산투자 결정 도입 결정 운영단계 진입 | <ul style="list-style-type: none"> 운영개념 수립 요구사항 설정 운영단계 진입 |
| 검토 중점 | <ul style="list-style-type: none"> 과도한 상해, 불필요한 고통 초래 가능성 표적 분별 가능성 | | <ul style="list-style-type: none"> 비례의 원칙 준수 가능성 |
| | - | <ul style="list-style-type: none"> 자연환경에 대한 손상 가능성 국제인도법 추세 고려한 향후 영향성 | |
| 기타 | 예산 규모, 긴급성 무관 | 긴급 사업은 일부 절차 간소화 가능 | - |

제인도법상 금지 여부를 결정할 의무가 있음을 명시하였으며, [18] 이에 따라 일부 선진국은 표 4 [18]와 같이 “Weapons Review”를 수행하고 있다. 우리

나라도 이 제도를 도입하여 AI 적용 무기체계가 국제인도법상 금지되는 행위들은 수행하지 않음을 객관적으로 확인할 필요가 있다. 우리나라에서 이를 운영할 시, 자체적인 신뢰도 확보뿐만 아니라 AI 적용 무기체계를 수출할 때에도 상당한 도움이 될 것으로 기대한다.[18]

4. 결론

4.1 AI4SE와 SE4AI의 전망

제2장 및 제3장에서 살펴본 AI4SE 및 SE4AI의 구현방안 및 선결과제를 요약하면 표 5, 6과 같다.

요약한 바와 같이, 이미 SE 활동을 효율적으로 수행하기 위한 다양한 AI 적용 방법론이 단계별로 제시되어 있으며, 반대로 AI 기능을 적용한 시스템 획득에서 SE 활동 수행이 필요하다. 다만, 무기체계 획득에 적용하기 위해서는 여러 가지 선결과제를 해결하여 시행착오를 최소화하는 노력이 필요하다.

결국 그리 머지않은 미래에, 그 수준을 막론하고 대부분의 무기체계에 필연적으로 AI 기능이 적용될 것으로 전망할 수 있으며 SE 프로세스에 보다 다양한 형태로 AI가 활용되리라고 본다.

AI4SE의 관점에서, AI가 운영개념과 요구사항 도출에 직접적으로 기여하고 하드웨어 예지정비 및 소프트웨어 형상관리 활동을 지원하게 될 것이다. SE4AI 관점에서는 AI 기반의 SE 프로세스를 바탕

<Table 5> Summaries of AI4SE

| 구분 | 핵심 내용 |
|------------|--|
| 구현 방안 | <ul style="list-style-type: none"> 요구사항 및 아키텍처 정의 <ul style="list-style-type: none"> 요구사항 무결성 분석 : 자연어 처리, 머신러닝 파라미터 기반 설계방안 생성 및 추천 : 딥러닝 전문가와 AI 플랫폼 간 상호작용 |
| 구현 방안 (계속) | <ul style="list-style-type: none"> 시스템 통합 및 V&V <ul style="list-style-type: none"> SW 구현 및 검증 : 머신러닝 HW 체계통합 및 양산 : 디지털 트윈, 딥러닝 전력화평가, 야전운용시험 : 디지털 트윈 시스템 운영유지 <ul style="list-style-type: none"> 예지정비 : 심층신경망 모델 |
| 선결과제 | <ul style="list-style-type: none"> 설명가능한 AI(XAI) 적용 AI기반 SE 지원 도구의 보안성 확보 AI 적용에 따른 지체권 보호방안 마련 |

으로 하여 AI 적용 무기체계의 총수명주기 관리가 가능해 질 것이다. 결국, 이 두 가지 개념은 별도로 분리해서 연구하거나 발전해야 하는 것이 아니며 필연적으로 함께 발전해야 한다고 판단된다.

<Table 6> Summaries of SE4AI

| 구분 | 핵심 내용 |
|-------|---|
| 필요성 | <ul style="list-style-type: none"> AI 적용 시 시스템의 운영개념 정립, 요구사항 개발, 성능-비용 절충, 수명주기 지원체계 확보, 총수명주기 관리 등이 필요 시스템 획득 시 위의 모든 관점을 종합적으로 다루는 학문이 바로 시스템공학임 |
| 구현 방안 | <ul style="list-style-type: none"> 소요기획-선행연구 단계 <ul style="list-style-type: none"> 사전개념연구 시 AI 기능 적용대상 및 수준 검토 (전문인력 확충, 검증 가능한 요구사항 제시 필요) 데이터 확보 방안 검토(학습-훈련용, 훈련적도 검증용, 기능 평가용) 획득단계(개발 및 양산) <ul style="list-style-type: none"> 데이터셋 품질관리(다양성, 정확성, 유효성 고려) 데이터셋 보안관리(정보유출 / 악의적 공격 방지) 운영유지단계 <ul style="list-style-type: none"> 유지보수 + 성능개선 사업개념 적용 (SW 형상관리와 사용자 교육훈련 지원) |
| 선결과제 | <ul style="list-style-type: none"> 운용목적에 따라 AI 기능 적용 수준을 분류하고, 수준별 개발/검증 요구사항 정립 AI 윤리성 기준 마련 및 준수 윤리성 준수여부 검증&확인 제도 도입 |

4.2 향후 연구방향

서론에서 언급했던 바와 같이, 본 연구는 아직은 정책적인 수준에서 탐색적 분석과 발전방향을 제시하는 수준에 머물러 있다. 물론 현재까지 한국에서 SE와 AI를 함께 언급하는 연구가 드물기에 이러한 시도는 나름의 가치가 있다고 판단되지만, 실제 AI4SE와 SE4AI 구현을 위해서는 제도적인 뒷받침 뿐만 아니라 보다 현실적이고 구체적인 연구가 꼭 필요하다고 판단된다.

대표적으로, AI4SE 측면에서는 시스템 설계와 검증확인 분야에서 실질적인 AI의 역할을 기대하고 이를 적용하려는 시도로 이어질 수 있도록 연구가 필요하다. SE4AI 측면에서는, 국방부가 최근 국방 AI 센터 추진단을 창설하여 조직과 제도를 검토하고 있듯 AI 기능을 어떻게 시스템에 반영하고 운용 유지할 것인지에 대한 정책적 분야와 기술적 분야 모두 연구하여 충분한 인프라를 갖춘 상태에서 AI

시스템 획득이 요구되어야 할 것이다. 이때, 관련 기관별로 구체적인 역할과 책임을 정의하여 불필요한 노력의 낭비와 혼선이 없도록 해야 한다.

AI는 천천히 생각해 볼 만큼 멀리 있는 속제는 아니지만, 대충 풀어볼 만한 속제도 아니다. 면밀한 검토와 연구를 통해 보다 가치있는 방향으로 추진되기를 기대한다.

References

1. AI4SE & SE4AI Workshop 2023, <https://sercuarc.org/event/ai4se-se4ai-workshop-2023/#D2T1> (Available on 18 Nov 2023).
2. 권기한, 전기 자동차 개발에서의 MBSE (Model Based System Engineering) 활용, 기계저널, vol. 61, no. 10, pp. 44-47, 2021.
3. International Standard, ISO/IEC/IEEE 15288 (Systems and software engineering-System life cycle processes), 2015.
4. 김진일, 염충섭, 신중욱, 요구사항 분석 및 아키텍처 정의 분야의 인공지능 적용 현황 및 방향, Journal of KOSSE. Vol. 18, No. 2 pp. 50-57. 2022.
5. Tetsuo Tamai, Taichi Anzai, Quality Requirements Analysis with Machine Learning, 13th International Conference on Evaluation of Novel Approaches to Software Engineering, 2019, pp. 241-248.
6. Requirements Quality Assistant analysis workflow, <https://www.ibm.com/docs/en/erqa?topic=assistant-rqa-customer-managed-architecture> (Available on 19 Nov 2023).
7. Oh, S., Jung, Y., Kim, S., Lee, I., and Kang, N. Deep Generative Design: Integration of Topology Optimization and Generative Models. Journal of Mechanical Design, Vol. 141, No.11, 2019.
8. Sang-Gook Kim, Sang Min Yoon, Maria Yang, Jungwoo Choi, Haluk Akay, and Edward Burnell, AI for design: Virtual design assistant, CIRP Annals, Vol. 68(1), pp. 141-144, 2019.
9. 이성복, 소프트웨어 엔지니어링 단계별 머신러닝의 안전한 적용 방법론, 공학 석사학위 논문, 한양대학교 공학대학원, 2020.
10. 정재성, 전력계통 디지털 트윈 구현을 위한 인공지능 기술, 전기의 세계, Vol. 71, no. 3, pp. 37-41, 2022.
11. 김각규, 진강균, 조용주, 원경찬, 디지털트윈을 활용한 미래 무기체계 전력화평가 및 야전운용 시험 방안에 대한 연구, 선진국방연구, Vol. 5(3), pp. 1-22, 2022.
12. 홍창우, 인공지능과 빅데이터를 활용한 예지 정비 적용 방안에 관한 연구: NASA Data repository에 대한 적용을 중심으로, 국방정책연구, Vol. 136, pp. 197-228. 2022.
13. Kossiakoff, A., Biemer, S. M., Seymour, S. J., & Flanigan, D. A. Systems engineering principles and practice, John Wiley & Sons. 2020.
14. 이민우, 박승규, 인공지능 내장형 무기체계의 총수명주기관리(TLCSM)를 위한 V&V 프로세스, 2021년 KOSSE 추계학술대회, 2021년 12월.
15. 신준호, 인공지능 학습용 데이터 품질검증 방법, 전자공학회지, Vol. 48(7), pp. 28-34. 2021.
16. 민옥기 외, ATL 1.0: 인공지능 기술 수준 정의, ETRI 전자통신동향분석, Vol. 35(3), 2020.
17. 조재규, 국방 인공지능 윤리에 대한 연구, 국방정책연구, Vol. 139, pp. 213-240, 2023.
18. 이민우, 무기의 사용 및 이전에 관한 국제인도법상 규제동향을 고려한 무기체계 기능 검토 수행 방안, 국방정책연구, Vol. 130, pp. 147-179, 2021.