

http://dx.doi.org/10.17703/JCCT.2024.10.5.189

JCCT 2024–9–22

국방분야 보안 RTOS의 무기체계 적용 및 발전 방안

Application and Development Strategies of a Secure Real-Time Operating System in Weapon Systems within the Defense Sector

이상승*, 최근하**, 황승현***, 김현지****, 서경덕*****, 성화은*****

Sang-Seung Lee*, Keun-Ha Choi**, Seung-Hyeon Hwang***,
Hyun-Ji Kim****, Kyung-Deok Seo*****, Hwa-Eun Seong*****

요약 국방 분야에서 사이버 위협이 증대되면서 무기체계 소프트웨어의 보안이 중요해지고 있고, 현재 국내 무기체계 탑재 임베디드 소프트웨어의 대부분은 보안성이 없는 외산 실시간 운영체제(RTOS) 기반으로 동작하고 있다. 이에 따라 무기체계 임베디드 소프트웨어의 국산화와 보안 강화가 시급한 과제로 대두되고 있다. 본 연구에서는 보안 RTOS의 무기체계 적용 및 발전 방안을 제시하고자 한다. 이를 위해 국내외 RTOS 및 보안 RTOS 기술 동향을 살펴보고, 현 무기체계 임베디드 소프트웨어의 문제점을 분석하였다. 그 결과 국산화 저조, 사이버 공격 취약성, 유지보수 어려움, 비용 증가, 기술력 축적 기회 상실 등이 주요 문제점으로 도출되었다. 현존 무기체계에 적용된 임베디드 소프트웨어 현황을 조사한 결과, 기동, 화력, 방호, 지휘통제·통신, 함정, 항공 등의 분야에 임베디드 SW가 운용 중이며, 이 중 99% 이상이 VxWorks 등 외산 RTOS에 의존하고 있는 것으로 파악되었다. 보안 RTOS의 핵심 기능과 무기체계 적용 가능성을 검토한 결과, 현존 및 미래 무기체계의 사격통제, 항법장치, 비행제어 등 핵심 분야에서 실시간 성과 보안성이 요구되는 영역을 중심으로 적용이 가능할 것으로 전망된다. 다만 성능과 신뢰성 확보, 검증 및 호환성 확보, 정부의 체계적 지원 등이 선결 과제로 제기되었다.

주요어 : 무기체계 보안, 실시간 운영체제, 국산화, 사이버 방호, 임베디드 보안 RTOS

Abstract As cyber threats increase in the defense sector, the security of weapon system software is becoming increasingly important. Currently, most of the embedded software installed in domestic weapon systems operates based on foreign real-time operating systems(RTOS) that have no security. As a result, the localization and security enhancement of embedded software for weapon systems have emerged as urgent tasks. This study aims to propose the application and development strategies of secure RTOS for weapon systems. To this end, we examined the technological trends of domestic and foreign RTOS and secure RTOS, and analyzed the problems of current embedded software in weapon systems. The results revealed major issues such as low localization, vulnerability to cyber attacks, difficulty in maintenance, increased costs, and loss of opportunities for accumulating technological capabilities. An investigation of the current status of embedded software applied to existing weapon systems found that embedded SW are in operation across all fields, including maneuver, firepower, protection, command and control, communication, naval vessels, and aircraft. Among them, 99% rely on foreign RTOS such as VxWorks. A review of the core functions and applicability of secure RTOS to weapon systems suggests that it can be applied to key areas requiring real-time performance and security, such as fire control, navigation devices, and flight control in existing and future weapon systems. However, ensuring performance and reliability, securing verification and compatibility, and systematic government support were raised as prerequisites.

Key words : Weapon System Security, Real-Time Operating System (RTOS), Localization, Cyber Protection, Embedded Secure RTOS

*정회원, 한국과학기술원 책임연구원 (제1저자)

**정회원, 한국과학기술원 연구교수 (참여저자)

***정회원, 한화시스템 수석연구원 (참여저자)

****정회원, 한화시스템 수석연구원 (참여저자)

*****정회원, 한화시스템 수석연구원 (참여저자)

접수일: 2024년 6월 11일, 수정완료일: 2024년 7월 12일

게재확정일: 2024년 9월 5일

(본 연구는 (주)한화시스템에서 발주한 연구용역 중, 일부를 발췌

하여 수정 및 보완한 연구 논문임.)

Received: June 11, 2024 / Revised: July 12, 2024

Accepted: September 5, 2024

*Corresponding Author: lss4976@gmail.com

Eulji Research Center, Korea Advanced Institute of Science and Technology, Korea

I. 서 론

최근 사이버 위협이 증대되면서 국방 분야에서도 소프트웨어 보안의 중요성이 강조되고 있고, 현재 국내 무기체계 탑재 임베디드 소프트웨어의 대부분은 보안성이 없는 외산 실시간 운영체제(RTOS) 기반으로 동작하고 있다. 이에 따라 무기체계 내장형 소프트웨어의 국산화와 보안 강화가 시급한 과제로 대두되고 있다.

본 연구에서는 보안 실시간 소프트웨어 플랫폼(이하 보안 RTOS)의 무기체계 적용 및 발전 방안에 대해 연구하고자 한다. 이를 위해 먼저 국내의 RTOS 및 보안 RTOS 기술 동향을 살펴보고, 현 무기체계 임베디드 소프트웨어의 문제점을 분석한다. 이어서 현존 및 미래 무기체계에서의 임베디드 소프트웨어 적용 현황을 조사하고, 보안 RTOS의 기능을 고려하여 무기체계 적용 가능성을 검토한다. 마지막으로 보안 RTOS의 발전 방향과 무기체계 적용을 위한 정책적 제언을 제시하고자 한다. 따라서 본 연구를 통해 국산 보안 RTOS의 무기체계 적용 확대와 국방 소프트웨어 기술 자립에 기여할 수 있을 것으로 기대된다. 아울러 사이버 위협에 대응하는 무기체계 보안 역량 강화에도 도움이 될 것으로 전망된다.

II. 국내외 RTOS 및 보안 RTOS 기술 동향

실시간 운영체제(RTOS)는 자동차, 철도, 의료, 에너지 등 다양한 산업 분야에서 활용되고 있으며, 특히 국방 분야에서는 무인기 자동항법장치, 전투기 및 훈련기 장비, 유도탄 유도장치, 전자 화력통제시스템, 레이더, 센서 네트워크, 군용 통신장비 등 대부분의 무기체계에 사용되고 있다. 최근에는 무기체계의 보안성 유지를 위해 세계적으로 자국에서 개발된 RTOS를 사용하는 추세이다. 예를 들어, 미국 윈드리버사의 VxWorks MILS는 수출이 불가하며, 프랑스 탈레스사도 자국 업체를 인수하여 자체 개발한 OS를 사용하고 있다. 국방용 RTOS의 주요 요구사항으로는 RTOS 커널, RTOS 서비스시스템, 통신네트워크 지원, 통합개발환경, 안전성 보안, 하드웨어 지원 등 6가지가 제시되고 있다[1].

대표적인 상용 RTOS로는 윈드리버사의 VxWorks, 그린힐스사의 Integrity, 국내 MDS테크놀로지사의

표 1. 국방용 RTOS 중요 요구항목

Table 1. Key Requirements for Military-Grade RTOS

구분	요구사항
RTOS 커널	멀티태스킹, 선점형 스케줄링, IPC, 동기화 기능
RTOS 서비스	파일 시스템, 네트워크 프로토콜 스택, 디바이스 드라이버
통신네트워크 지원	다양한 통신 미들웨어 (CAN, TTCAN, TTP/C 등)
통합 개발환경	편집, 컴파일, 디버깅, 시뮬레이션, 테스트 기능
안전성 및 보안	메모리 보호, fault tolerance, 보안 통신
하드웨어 지원	프로세서, 메모리 보호 (MMU), 다중 프로세서

자료: 이서준(2011), “국방용 RTOS 기술동향”[1]을 바탕으로 저자가 수정·보완함

NEOS 등이 있다. VxWorks는 SMP와 AMP를 지원하며 국방, 항공 등 다양한 분야에 사용되고 있다. 특히 멀티코어 기술을 활용할 수 있고, 통합된 미들웨어를 제공하며, 개발환경 지원과 응용분야별 특화된 기능을 플랫폼에 제공한다.

Integrity는 분리형 커널 아키텍처를 기반으로 응용 프로그램을 격리하여 커널을 보호하고, 파티션 간 의도하지 않은 외부 데이터 접근을 차단한다. 국내 NEOS는 T-50 임무컴퓨터 국산화, GNSS 및 GPS 수신기 등에 적용되었으며, 타사 RTOS 응용프로그램과의 이식성과 재사용성을 지원하고, API 측면에서 VxWorks 등 타 RTOS와 기능상 호환이 가능하도록 설계되었다.

이처럼 RTOS 기술은 국방 분야에서 무기체계의 실시간 제어와 통신을 담당하는 핵심 소프트웨어로 자리 잡고 있다. 특히 사이버 위협이 고도화되면서 무기체계의 보안성 확보를 위해 자국 기술로 개발된 군사용 RTOS의 중요성이 커지고 있다. 향후 RTOS 기술은 멀티코어 활용, 고신뢰 미들웨어 통합, 개발 편의성 향상, 응용분야 특화 등을 통해 발전해 나갈 것으로 전망된다. 아울러 무기체계의 실시간 운용환경에 최적화된 보안 기능을 강화하고, 국제 표준과의 호환성을 유지하면서도 자주국방 역량을 확보하기 위한 국산 군사용 RTOS 기술 개발이 지속적으로 요구될 것이다.

III. 현 무기체계 임베디드 SW 문제점 분석

현 무기체계에 적용된 임베디드 SW의 문제점을 파악하기 위해 군 관계자 및 전문가 의견수렴과 문헌자료 분석을 실시하였다. 군 관계자 의견청취는 2023년 7월 25일에 육군 중령 3명을 대상으로 진행되었다. 또한, 군 전문가 의견수렴은 2024년 2월 2일에 육군, 해군, 공군 전문가 3명을 대상으로, 5월 23일 육군, 해군, 공군 전문가 5명을 대상으로 2회 실시하였다.

의견수렴 결과, 현 무기체계 임베디드 SW의 주요 문제점으로는 국산 SW에 대한 인식 부족, 국산화 저조, 사이버 공격에 취약, 유지보수의 어려움, 비용 증가, 국내 기술력 축적 기회 상실, 호환성 문제, 무기체계 소요제기 시 OS 성능 요구 제한 등이 도출되었다. 각 문제점에 대한 구체적인 내용은 다음과 같다.

첫째, 국산 SW에 대한 인식 부족이 문제점으로 지적되었다. 국방 SW는 부수적인 요소로 인식되고 있으며, 무기체계 개발 시 국내 기술에 대한 부정적 인식으로 인해 국산 SW를 신뢰하지 않는 경향이 있다. 국산 RTOS 적용을 위해서는 성능업증이 중요한 고려요소이나, 충분한 검증과 테스트를 위한 TEST-BED 제공이 쉽지 않은 실정이다.

둘째, 국산화가 저조한 것으로 나타났다. 실시간 운영체제(RTOS)의 경우 특정 회사에 의존도가 지나치게 높으며, 다양한 기능과 개발 편의성 등으로 인해 외산 제품을 선호하는 경향이 있다. 또한, 무기체계 SW는 하드웨어에 포함되어 함께 구매되므로 별도의 국산품 개발이나 구매가 이루어지지 않고 있다. 해외 선진국의 기술이전 제한 및 엄격한 통제로 인해 단기간 내 기술 확보가 어려운 점도 국산화를 저해하는 요인으로 작용하고 있다.

표 2. 무기체계 SW 국산화 저해요인
 Table 2. Factors Hindering the Localization of Weapon System Software

구분	내용
인식 부족	국방 SW를 부수적 요소로 인식, 국산 SW 신뢰도 부족
의존도	RTOS 특정 회사 의존도 높음, 외산 제품 선호
구매방식	SW 단독 구매 아닌 HW에 포함되어 구매
기술이전 제한	해외의 기술이전 제한 및 통제로 단기간 기술확보 어려움

셋째, 사이버 공격에 취약한 것으로 조사되었다. 사이버 공격의 75%는 SW의 보안 취약점을 이용하나, 임베디드 SW의 경우 PC와 같이 바이러스 백신, 방화벽, SW 패치 등으로 대응하기 곤란하다. 특히 상용 임베디드 체계는 군사용 무기체계와 달리 통신채널 암호화, HW 암호화 칩, 인증체계 등의 보호체계 적용이 제한적이다. 또한, 대부분의 임베디드 SW가 외산 OS를 사용함에 따라 알 수 없는 백도어 존재 우려, 취약점 보완과 성능개선의 즉각적 대응이 어렵다는 문제가 있다.

넷째, 유지보수의 어려움이 제기되었다. RTOS의 경우 응용SW와 달리 여러 무기체계에 재사용이 가능하나, 외산 RTOS 사용 시 유사시 빠른 수정 및 적용이 어렵다. 최근 침입 공격은 하드웨어와 연계한 운영체제 및 소프트웨어를 대상으로 하는 추세인데, 상용 RTOS는 다양한 인원이 운용 및 개발할 수 있어 취약점 공유 가능성이 높고 신속한 조치가 제한될 수 있다.

다섯째, 외산 SW 사용에 따른 비용 증가 문제가 있다. 양산단계에서 높은 로열티와 비싼 개발 라이선스 지급으로 기반구축에 고비용이 소요된다. 무기체계에서 임베디드 SW는 핵심기능을 담당하고 있어 전체 획득비용 중 SW 비중이 지속적으로 증가하는 추세이다.

여섯째, 외산 SW 운용으로 인해 국내 기술력 축적 기회를 상실하게 된다. 복잡한 시스템을 개발하고 유지할 수 있는 숙련된 인력이 부족하며, 장기간 사용되는 무기체계 특성상 기술발전에 따른 기존 시스템 유지보수에 어려움이 예상된다. 설계, 구현, 테스트 과정에서 의 어려움도 가중될 것으로 보인다.

일곱째, 호환성 문제가 대두되었다. 다양한 하드웨어와 소프트웨어가 통합되는 과정에서 호환성 문제로 인해 시스템 간 통신장애나 오작동이 발생할 수 있다.

여덟째, 무기체계 소요제기 시 OS에 특화된 성능요구가 제한적이라는 점이 지적되었다. 각 군에서는 무기체계의 성능에 대해 요구하도록 되어 있으나, 성능은 HW+OS+어플리케이션이 결합된 결과이기 때문에 OS에 특화된 성능을 요구하는 데에는 한계가 있다. 외산 OS 사용 시 군의 수정 요구 반영이 제한되고 추가 예산이 소요될 수 있는 문제점이 상존한다.

이상의 분석 결과를 종합해 볼 때, 현 무기체계 임베디드 SW는 외산 의존도가 높고 국산화가 저조한 가운데 사이버 위협에 노출되어 있으며, 유지보수와 호환성 측면에서 취약점을 안고 있는 것으로 파악된다. 이는

결과적으로 막대한 예산 소모와 국내 기술력 축적 기회 상실로 이어지고 있다. 향후 국산 보안 RTOS 적용 확대를 통해 이러한 문제점들을 해소하고, 자주국방 역량을 강화해 나가는 것이 시급한 과제라 할 수 있겠다.

IV. 현존/미래 무기체계 임베디드 SW 적용 현황

현존 및 미래 무기체계에 적용된 임베디드 SW의 현황을 파악하기 위해 공개된 자료를 수집하여 분석하였다. 2011년부터 2022년까지 발표된 연구보고서와 논문을 중심으로 조사하였으며, 그 결과는 다음과 같다.

먼저 안보경영연구원(2011)의 연구보고서에 따르면, 당시 육군 4종, 해군 6종, 공군 3종의 무기체계에 대한 임베디드 SW 적용 사례가 제시되었다[2]. 같은 해 다른 연구에서는 지상 7종, 해상 3종, 항공 1종 등 총 11종의 무기체계 SW 현황이 추가로 조사되었다[2].

안훈상 외(2015)의 연구에 의하면 육군이 운용 중인 무기체계 SW가 총 29종 235건이며[3], 이 중 임베디드 SW는 97건인 것으로 나타났다[3]. 방위사업청(2016)

연구에서는 ETRI의 조사 결과를 인용하여, 지상, 해상, 항공 무기체계 9종의 운영체계 중 86건이 외산인 것으로 파악되었다[4].

박규철(2021) 연구에 의하면 11종의 무기체계에 대해 SW 형상을 확인하였으나 세부 현황은 제시되지 않았다[5]. 한국방위산업진흥회(2022)의 시장조사 결과[6], 국내 무기체계 388개 중 RTOS 472개가 적용되어 있으며, 이 중 국산은 3개(0.6%)에 불과한 것으로 드러났다[6].

이상의 자료를 종합해 볼 때, 연구에서 조사된 현재 국내 무기체계의 임베디드 SW는 251개를 대상으로 하였다. 세부적으로는 VxWorks 175개(69.72%), Embedded Linux 70개(27.89%), NEOS 2개(0.80%), Windows Embedded 3개(1.20%), BIOS 1개(0.40%) 등이다.

무기체계별로는 기동 34개, 화력 40개, 방호 16개, 지휘통제·통신 85개, 함정 54개, 항공 22개 등 총 251개의 임베디드 SW가 운용되고 있다.

한편, 미래 무기체계의 경우 아직 구체적인 SW 현황 자료는 부족한 실정이다. 다만 현존 무기체계의 적용 사례와 기술 발전 추세를 고려할 때, 향후에도 실시간 운영체제의 중요성은 지속될 것으로 전망된다.

특히 자율·무인체계의 확대, 인공지능 기술의 도입, 사이버 위협의 증대 등으로 인해 고신뢰·고성능·고보안의 국산 RTOS 수요가 더욱 커질 것으로 예상된다. 전문가 의견 수렴 결과에서도 국산 보안 RTOS의 미래 무기체계 적용 가능성에 대해 긍정적인 평가가 우세하였다. 이처럼 국내 무기체계에 적용된 임베디드 SW는 대부분 외산에 의존하고 있는 상황이다. 자주국방 역량 강화와 사이버 방호 차원에서 핵심기술인 RTOS의 국산화가 시급한 과제로 대두되고 있다. 이를 위해서는 성능과 신뢰성을 확보한 국산 보안 RTOS의 개발과 함께, 제도적 지원 방안도 마련되어야 할 것이다.

V. 보안 RTOS의 무기체계 적용 방안

보안 RTOS의 핵심 기능으로는 실시간성, 보안성, 안전성 제공, 오픈 아키텍처 표준 API 확장 지원, VxWorks 기반 무기체계 응용 S/W 대상 핵심모듈 호환성 제공 등이 있다. 이러한 기능을 바탕으로 현존 및 미래 무기체계에 대한 적용 가능성을 분석하였다.

현존 무기체계의 경우, 기동, 화력, 방호, 지휘통제·통신, 함정, 항공 분야에서 사격통제, 항법장치, 운용통

표 3. 현 무기체계 임베디드 SW 적용 현황

Table 3. Current Status of Embedded Software Applications in Existing Weapon Systems

구분	장비 수	임베디드 SW 수	주요 OS
기동	6	34	VxWorks(00 Embedded Linux(00 NEOS(00
화력	11	40	VxWorks(00 Embedded Linux(00
방호	5	16	VxWorks(00, Embedded Linux(00 Windows Embedded(00
지휘 통제·통신	3	85	VxWorks(00 Embedded Linux(00
함정	3	54	VxWorks(00 BIOS(00
항공	4	22	VxWorks(00 Embedded Linux(00
합계	32	251	VxWorks(00), Embedded Linux(00), NEOS(00), Windows Embedded(00), BIOS(00)

자료: [2],[3],[4],[5],[6]를 바탕으로 저자가 요약·가공함

제, 차체(량)제어, 유도장치, 통신시스템 등 핵심 분야에 RTOS가 적용되고 있어 보안 RTOS의 적용이 가능할 것으로 예상된다. 특히 유사 무기체계에서는 RTOS SW가 공통적으로 적용되는 하부시스템이 식별되었으며, 이들의 성능 보장을 위해서는 실시간성, 보안성, 안전성이 요구된다.

표 4. 현존 무기체계 보안 실시간 SW 적용 가능성
 Table 4. Feasibility of Applying Secure Real-Time Software in Existing Weapon Systems

구분	적용 가능 분야
기동	사격통제, 운용통제, 차체(량)제어, 체계제어, 관성항법장치, 센서데이터 수집
화력	사격통제, 항법장치, 유도(제어)장치, 발사통제, 발사대 제어, 통신, 신호/데이터처리
방호	사격통제, 항법장치, 처리장치
지휘통제·통신	전화기, 중계기, 무선 송/수신기, 통신접속 처리장치, 위성통신 단말기, 관제소
함정	전투체계, 센서체계(레이더, 소나 등), 타격체계, 기관체계
항공	비행제어/통제, 데이터획득/처리, 항법장치, 구내통신

미래 무기체계는 현존 무기체계와의 유사성을 바탕으로 적용 가능성을 예측하였다. 예를 들어 현존 사단 정찰용 무인항공기의 비행제어, 항법장치 등에 적용된 사례를 통해 미래 다목적 무인항공기에도 적용 가능할 것으로 보인다. 전문가 의견에서도 국산 보안 RTOS의 미래 무기체계 적용에 대해 긍정적인 평가가 우세하였다.

다만 적용을 위해서는 성능과 신뢰성 확보, 다양한 테스트와 검증을 통한 호환성 확보, 정부의 지속적인 지원 등이 선결되어야 한다는 의견이 제시되었다. 또한 적용 우선순위로는 CAISR 시스템, 유도무기 시스템, 전차 및 장갑차 등 실시간성과 보안성이 중요시되는 분야, 위험부담이 적은 전력지원체계나 교육용 장비 등이 거론되었다.

이상의 분석 결과를 종합해 볼 때, 국산 보안 RTOS는 현존 및 미래 무기체계의 핵심 분야에 적용 가능성이 높은 것으로 판단된다. 특히 실시간 운용환경에 최적화된 보안 기능을 갖추고, 기존 체계와의 호환성을

확보한다면 외산 대체는 물론 수출 경쟁력 제고에도 기여할 수 있을 것이다.

이를 위해서는 성능 검증을 위한 테스트베드 구축, 관련 규정 및 제도 정비, 적용 사업에 대한 예산 지원 등 정부 차원의 체계적인 지원이 뒷받침되어야 할 것이다. 아울러 소요군과 방사청 등 유관기관의 적극적인 협력을 통해 국산 보안 RTOS의 조기 적용과 확산을 추진해 나가야 할 것이다.

References

- [1] Lee, Seo-Jun. "Trends in RTOS Technology for Defense Applications." Special Feature Article, Communications of the Korean Institute of Information Scientists and Engineers, 2011.
- [2] "Plan for Fostering Weapon System Software." Research Report, Institute for Security and Management, 2011.
- [3] Ahn, Hoon-Sang, et al. "Measures to Enhance the Safety of Embedded Software in Weapon Systems." Defense Technology, 2015.
- [4] Han, Jang-Geun, et al. "A Study on the Localization Strategy of Weapon System Software for Strengthening Self-Reliant Defense Capabilities." Special Feature Article, Communications of the Korean Institute of Information Scientists and Engineers.
- [5] Park, Gyu-Cheol. "Maintenance Plan for Embedded Software in Weapon Systems." Proceedings of the Fall Conference of the Korea Institute of Communications and Information Sciences, 2021.
- [6] "Survey on the Current Status of Weapon System Software." Korea Defense Industry Association, 2022.