Journal of the Korea Academia-Industrial cooperation Society
Vol. 25, No. 8 pp. 516-522, 2024

https://doi.org/10.5762/KAIS.2024.25.8.516
ISSN 1975-4701 / eISSN 2288-4688

무기체계 소프트웨어 공급망 관리를 위한 무기체계 SW 적용현황 조사 데이터필드 개선방안 연구

김종규*, 조한별, 채신영, 장지형, 임준영
국방기술품질원

Research on improvement measures for weapon system software status Datafield for weapon system software supply chain management

Jong-Kyu Kim*, Han-Byeol Cho, Shin-Yeong Chae, Ji-Hyung Chang, Jun-Yeong Lim
Defense Agency for Technology and Quality

요 약 오늘날 대부분의 산업에서 소프트웨어의 규모 및 비중이 급격하게 증대되면서, 더 이상 하나의 개발기관이 소프트웨어를 처음부터 끝까지 개발하는 것은 현실적으로 어려워졌다. 개발기관들은 효율적인 소프트웨어 개발을 위해 개발 간 상용, 공개 소프트웨어를 활용하고 있지만 외부에서 가져온 소프트웨어에 의한 보안사고도 빈번하게 발생하고 있는 상황이다. 2020년 솔라윈즈 해킹사건 등 소프트웨어 공급망을 이용한 공격이 지속적으로 발생하여 미국 정보통신청은 소프트웨어 구성 정보를 기재한 소프트웨어 자재명세서 개념 및 최소요소를 정의하였다. 소프트웨어 자재명세서는 소프트웨어 공급망 투명성을 확보·관리하여 공급망 공격에 대해 기민하게 대응할 수 있도록하여 공급망 보안 위협을 완화시켜준다. 오늘날 국방 분야에서도 무기체계 소프트웨어 공급망 관리를 위한 제도들이 있다. 하지만 현행 제도에는 소프트웨어 자재명세서 기준 일부 정보들에 대한 조사가 이루어지지 않아 소프트웨어 공급망 공격에 대해 원활하게 대응하기가 어려운 상황이다. 본 논문에서는 미국 정보통신청에서 제시한 소프트웨어 자재명세서를 기반으로 국방분야 현행 제도의 보완사항을 식별하고 보완을 위한 소프트웨어 적용현황 조사 양식을 제시한다. 이를 통해 무기체계 소프트웨어의 구성요소 파악이 수월해지고 효과적인 공급망 관리가 수행될 것을 기대한다.

Abstract With the rapid increase in the size and proportion of software in most industries today, it has become practically difficult for one development agency to develop software from start to finish. Development organizations use commercial and open software during development for efficient software development, but security incidents caused by software imported from outside often occur. Owing to attacks on the software supply chain, such as the 2020 SolarWinds incident, the U.S. Communications Administration defined the concept and minimum elements of a software bill of materials that describe software configuration information. This secures/manages software supply chain transparency, enables agile response to supply chain attacks, and mitigates supply chain security threats. Even in the defense field today, there are systems for weapons-system-software supply chain management. On the other hand, it is difficult to respond quickly to software supply chain attacks because the current system does not investigate some information based on a software bill of materials. This paper identifies supplements to the current system in the defense field and presents a software application status survey form for supplementation based on the software bill of materials presented by the U.S. Information and Communications Agency. The new system will make identifying the components of weapons system software easier and enable effective supply chain management.

Keywords : Software, Software Supply Chain, Software Bill of Material, Weapon System, Weapon System Software

*Corresponding Author : Jong-Kyu Kim(DTaQ)
email: rnseorka528@dtaq.re.kr
Received May 20, 2024 Revised June 17, 2024
Accepted August 2, 2024 Published August 31, 2024

1. 서론

무기체계는 전장에서 전투력을 발휘하기 위한 무기와 이를 운영하는데 필요한 장비, 부품, 시설, 소프트웨어 등 제반요소를 통합한 것으로써, 지휘통제통신, 감시정찰, 기동무기체계 등으로 구분되고, 연구개발을 통해 최종적으로 시험평가를 수행 후 규격화가 완료된다[1]. 국방종합표준정보체계(KDSIS : Korea Defense Standard Information System, 이하 KDSIS)에 따르면 무기체계 소프트웨어(Software, 이하 SW) 중 규격화가 이루어진 SW 기술자료의 총 개수는 3167건이며 연도별 제정 건수는 Fig. 1 및 Table 1과 같다. 무기체계의 SW는 최근 전장 환경이 변화함에 따라 비중이 꾸준하게 증가하고 있으며, 무기체계의 성능을 결정하는 요인이 되었다[2].

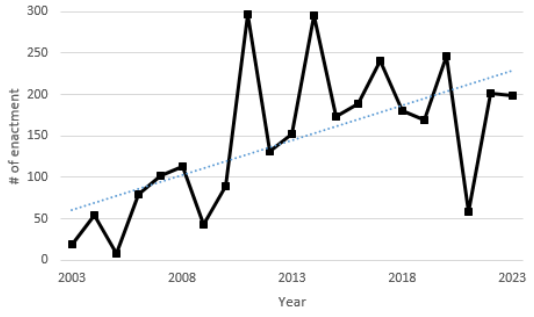

Fig. 1. Number of SW enactment for each year

Table 1. Number of SW enactmaent for each year

Year	Number of SW enactment	Year	Number of SW enactment
2003	20	2014	296
2004	54	2015	174
2005	8	2016	189
2006	79	2017	241
2007	102	2018	180
2008	113	2019	169
2009	43	2020	246
2010	89	2021	59
2011	297	2022	202
2012	132	2023	198
2013	152	others	124

무기체계에서 SW의 비중이 커짐에 따라 더 이상 한 개발주관기관에서 무기체계에 탑재되는 모든 SW를 개발하는 것은 사실상 불가능해졌다. 효율적인 무기체계 SW 개발을 위하여 개발주관기관은 기존에 만들어진 외부 라이브러리(상용SW, 공개SW)를 활용하여 무기체계 SW 개발을 수행한다. 하지만 외부 라이브러리들은 직접 개발한 것이 아니기에 해당 SW들의 확보 방법, 제작사 등 SW 공급망정보 관리가 엄격하게 필요한 상황이다.

방위사업청(이하 방사청)에서는 무기체계 SW 공급망 관리를 위해 SW 기술문서 관리 및 무기체계 SW 적용현황을 조사·관리하는 제도를 규정에 반영하여 시행하고 있으나 공개SW 정보, 개발SW의 재활용 관계 정보 등을 파악하기에는 조사하는 정보의 범위가 한정적이라는 한계점을 가지고 있다.

본 논문에서는 효율적인 무기체계 SW 공급망 관리를 위한 방안 중 하나인 소프트웨어 자재명세서(Software Bill Of Material, 이하 SBOM)에 대한 기존 연구내용을 기반으로 국방분야 제도 중 무기체계 SW 적용현황 조사 데이터필드의 한계점 분석 및 보완 필요사항을 식별한 뒤 개선된 데이터필드 항목 제안하여 효과적인 무기체계 SW 공급망 관리가 수행될 수 있도록 한다. 본 논문의 2장은 SW 공급망과 SBOM 대한 이론적 배경, 3장에서는 현 무기체계 SW의 공급망 관리를 위한 제도 중 분류체계식별자, 무기체계 SW 적용현황 조사의 한계점에 대해 살펴보며, 4장에서는 SBOM과 무기체계 SW 적용현황 조사에 대한 비교 및 개선방안에 대해 살펴본다. 마지막 5장에서는 결론에 대해 작성하였다.

2. 이론적 배경

2.1 SW 공급망

SW 공급망이란 SW 제품 및 서비스를 개발, 제공 및 유지 관리하는 프로세스인 개발생명주기에 관여되는 모든 자원, 기술 및 활동을 의미한다[3]. 2020년 전 세계적으로 사용되는 네트워크 관리 소프트웨어인 솔라윈즈(SolarWinds)의 업데이트 파일에 악성코드가 삽입되어 미국 재무부 등 주요 기관들이 해킹 공격을 받는 사례 등 SW 공급망을 이용한 공격사례가 발생하였으며 오늘날에도 SW 공급망을 통한 공격이 발생하고 있다[4].

2.2 SBOM (Software Bill Of Material)

SBOM은 SW제품을 이루는 SW 구성요소의 세부 정보와 의존관계를 기술하는 SW 구성명세서이다. 제품에 포함되어 있는 SW 구성요소의 구성요소명, 공급자명, 버전 등 관련 정보를 기술해 정확한 식별이 가능하게 한다[5].

2.3 CVE (Common Vulnerabilities and Exposure)

CVE(공통 취약점 및 노출)은 공개적으로 공개된 사이버 보안 취약점 식별, 정의, 분류 및 해당 취약점에 대해 어떻게 조치를 취해야 하는지에 대한 정보들을 의미한다. CVE는 전세계 보안관련 기관들이 식별된 상용SW, 공개SW에 대한 취약점 정보를 MITRE 기관을 통해 등록하여 공개된다[6].

2.4 SBOM 활용 방안

SBOM은 SW 공급망에 대한 공급자와 수요자의 이해도를 향상시켜 구성요소 수준에서 발생할 수 있는 위협에 대해 기민한 대응을 할 수 있게 한다[5]. Fig. 2에서 SBOM이 관리되지 않는 좌측 Tier3, Tier2 SW 컴포넌트의 경우 사이버공격에 노출되어도 사용자가 그 사실을 인지하지 못하는 반면 SBOM을 관리하는 Tier 1의 경우 사이버공격 노출시 공격에 대한 인지가 쉽게 가능하며 그에따른 후속조치를 수행할 수 있다. 제품에 사용된 SW 컴포넌트가 사이버공격 및 취약점에 노출된 것을 인지하는 방법은 CVE 목록에 등록된 SW명을 기반으로 SBOM에서 동일한 SW가 있는지 확인 가능하다.

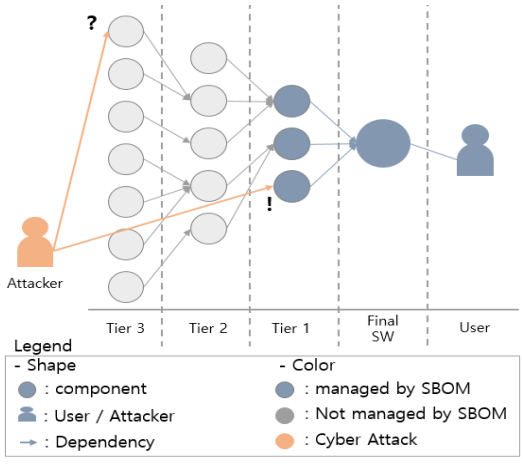

Fig. 2. Concept of SBOM and SW supply chain attack

2.5 SBOM 최소 구성요소 : 데이터 필드

미 행정명령(EO-14028)에 따라 미국 정보통신청(NTIA : National Telecommunications and Information Administration, 이하 NTIA)은 데이터필드, 자동화 지원, 실행 및 절차를 SBOM의 최소요소로 정의하였다. 이중 데이터 필드는 SW 공급망 전체에서 추적하고 유지관리해야 하는 각 데이터 구성요소에 대한 정보이다. 데이터 필드의 최소 요소 및 관련 설명은 Table 2와 같다[7].

Table 2. Minimum Datafield of SBOM

Data Field	Description
Supplier Name	The name of an entity that creates, defines, and identifies components.
Component Name	Designation assigned to a unit of software defined by the original supplier.
Version of the Component	Identifier used by the supplier to specify a change in software from a previously identified version.
Other Unique Identifiers	Other identifiers that are used to identify a component, or serve as a look-up key for relevant databases.
Dependency Relationship	Characterizing the relationship that an upstream component X is included in software Y.
Author of SBOM Data	The name of the entity that creates the SBOM data for this component.
Time stamp	Record of the date and time of the SBOM data assembly.

3. 무기체계 SW 공급망 관리 제도

3.1 분류체계 식별자

방사청은 무기체계 SW의 관리를 효율적으로 수행하기 위해 2007년 정책연구를 통해 미 공군의 무기체계 내장형 SW 식별방법을 기반으로 한국형 무기체계 내장형 SW 분류체계를 정립하였다. 분류체계 식별자는 무기체계 SW 개발 프로세스 중 소프트웨어 상세설계 단계의 산출물인 소프트웨어설계명세서(Software Design Description, 이하 SDD) 내 부록으로 작성된다. 분류체계 식별자는 소프트웨어 구성품(Computer Software Component, 이하 CSC) 단위로 부여되며 군급분류, 부품번호, 소프트웨어 형상항목(Computer Software Configuration Item, 이하 CSCI) 약어, SW 유형, SW버전 등 13가지 정보를 하나의 고유 식별자로 구성되어 관리된다[8].

3.2 분류체계 속성자료

분류체계 속성자료 목록은 SW 유지보수, 재활용 및 상용SW의 추적성관리 업무에 사용하기 위해 작성된다. 상세설계단계에서 식별된 분류체계 식별자를 기반 상세정보(무기체계분류, 개발언어, LOC, 분류체계 식별자 SW 탑재 디바이스 번호, 상용SW(OS/미들웨어/DBMS)

등)를 규격화 단계의 소프트웨어산출물명세서(Software Product Specification, 이하 SPS) 부록으로 정리해 놓은 목록이다[8].

3.3 무기체계 SW 적용현황 조사

무기체계 SW 규격화 이후 개발간 작성된 분류체계 식별자, 분류체계 속성자료 및 SW기술문서를 기반으로 무기체계에 탑재되는 개발SW(무기체계 개발기관에서 직접 개발한 SW), 상용SW(OS, 미들웨어, DBMS, 응용SW)를 디바이스 단위로 매년 조사하며 상용SW의 경우 제조사에 따른 국산·외산 현황을 같이 조사한다. 무기체계 SW 적용현황 데이터필드 중 SW 공급망 관리와 연관된 주요 속성들은 Table 3와 같다. 무기체계 SW 적용현황 조사를 통해 각 무기체계 디바이스별로 적용된 SW 목록을 한눈에 파악할 수 있으며 상용SW의 국산화율을 파악할 수 있는 이점이 있다.

Table 3. Datafield of SW Application status survey

Data Field	Detailed Data Field
Weapon System	Weapon system name, National defense standard number
CSCI Information	SW Technology data number, SW Specification name, CSCI name
SW equipped Device	SW equipped device drawing number, Device name, Develpoer of SW
Development SW	Development language, Line of code
Commercial SW	OS Sortation*, OS name, DBMS Sortaion, DBMS name, Middleware Sortation, Middleware name, Application SW Sortation, Application SW name * Sortation : Foreign / Domestic

3.4 무기체계 SW 적용현황 조사 한계점

무기체계 SW 적용현황 조사를 통해 무기체계에 탑재되는 SW를 디바이스 단위로 파악하여 SW 공급망 관리를 일부분 수행할 수 있으나, NTIA에서 제시하는 공급망 관리를 위한 데이터 최소요소들을 충족시키지는 못하는 상황이다.

상용SW 정보의 경우 각 SW명과 버전은 작성되어 있지만 SW 공급자 추적을 위한 정보가 누락되어 있으며, 개발간 사용된 공개SW의 경우는 목록부터 관리가 이루어지고 있지 않다.

개발SW의 경우 최근 성능개량 사업, 현존전력 극대화 사업과 같이 기존에 개발된 무기체계 SW를 수정하여 재활용하는 개발 사업이 증가하고 있음에도 개발언어, 라인수의 정보만 있어 재활용하는 SW의 출처가 무엇인지 파악에 어려움이 있다.

신규 개발SW에서 기개발SW 컴포넌트를 재활용하는 경우 SDD, SPS에 재활용 방안·대상을 작성하는 항목이 있어 근간이 되는 컴포넌트 추적이 가능하다. 하지만 재활용에 쓰이는 컴포넌트의 경우 이미 SW 기술문서가 규격화되었으며 SDD, SPS에 자신을 재활용하는 컴포넌트 목록을 작성하는 항목이 없어 자신이 재활용되어 사용되는 사실을 문서에 반영하기 어려운 상황이다.

4. 무기체계 SW 적용현황 조사 개선방안

4장에서는 3.4절에서 제시한 한계점을 보완하기위해 기존 수행하는 무기체계 SW 적용현황 조사에 SBOM의 개념 적용하는 방안을 데이터필드 관점에서 제시한다.

4.1 무기체계 SW 적용현황 조사 대상 SW 분류

데이터필드 개선 제안 이전에 먼저 조사대상 SW에 대한 분류를 정의하고자한다. 해당 내용은 Table 4와 같다.

개발SW는 개발기관에서 개발한 실행파일을 빌드하거나 실행하기 위해 개발기관에서 직접 개발한 소스코드, 라이브러리 등 모든 원천파일들을 의미하며, 상용SW와 공개SW는 운영체제, 응용SW와 같이 하나의 완제품SW와 개발SW 빌드/실행을 위한 라이브러리를 의미하도록 분류하였다.

Table 4. SW classification for SW application status survey

Classification	Detailed Classification
Development SW	Development Source
Commercial SW	OS, DBMS, Middleware, Application SW, etc.(bootloader)
	Commercial Library (Source Code, *.lib, *.dll, etc.) ※ Required for Development SW Build/Execution
Open Source SW	OS, DBMS, Middleware, Application SW, etc.(bootloader)
	Open Source Library (Source Code, *.lib, *.dll, etc.) ※ Required for Development SW Build/Execution

4.2 데이터필드 개선안

현재 무기체계 SW 적용현황 조사 데이터필드는 SBOM에서 제시하는 7가지 최소 구성요소 중 SW분류에 따라 많게는 3가지 항목 적게는 0개의 항목을 조사 수행 중 이다. 그렇기에 NTIA에서 제시하는 SBOM 데이터필드 최소 구성요소를 충족시키며 공급망을 통한 위협이 발생했을 경우 보다 기민한 대응을 할 수 있도록 새로운 SW 적용현황 조사 데이터필드를 제안한다. 새로운 데이터필드는 크게 4개의 레벨로 구성을 나누었으며 각 레벨별 포함하는 정보는 table 5와 같다.

Table 5. Proposed datafield of SW application status survey

Level	Data Field	Detailed Data Field
1	Weapon system	Weapon system name, National defense standard number
2	CSCI	CSCI name, SW Technology data number
3	SW equipped Device	Device ID (listed in SPS), Device name, Device drawing number, Device Produc ID (given by manufacturer)
4	Development SW	Dev SW ID, Version, SW Supplier, Reuse Dependency (from / to), SBOM creator, Created time
	Commercial SW	[Common] SW type(OS, DBMS, Middleware, Library, Application), COTS/OSS SW ID, SW name, Version, Dependency, SWSupplier, SBOM creator, Created time [Only OSS] License, Download Location
	Open Source SW	

Table 5를 살펴보면 조사의 단위는 기존과 동일하게 디바이스 단위로 설정하였다. Level 1/2/3 정보를 기반으로 특정 체계의 포함되는 디바이스를 특정 지을 수 있다. Level 4 정보는 Table 4의 SW분류별로 어떤 SW들이 탑재되는지 파악이 가능하다. Fig. 3과 같이 Level1/2/3 정보와 각 Level4의 정보를 결합하면 특정 디바이스에 어떤 SW들이 탑재되는지 파악이 가능하다.

Table 6은 기존 SW 적용현황 양식, 본 논문에서 제안된 SW 적용현황 양식, NTIA에서 제시하는 SBOM 최소 데이터필드를 비교한 표이다.

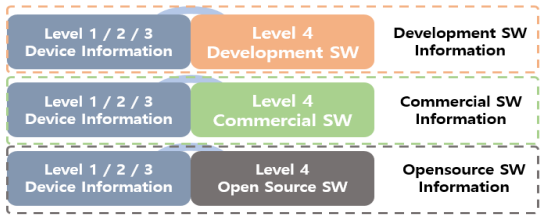

Fig. 3. Association betweern each levels

Table 6. SBoM Datafield Information

SBOM minimum Datafield	Present Form Datafield	Suggested Form Datafield
Supplier Name	-	SW Supplier
Component Name	CSCI number	Dev SW ID, SW name
Version of the Component	-	Version
Other Unique Identifiers	SW Technology data number	· Dev SW ID · COTS/OSS SW ID
Dependency Relationship	-	· Reuse Dependency (from / by) · Dependency
Author of SBOM Data	[Fixed by Regulation]	SBOM Creator
Time stamp	-	Created time

- : unidentifiable

4.3 개선사항 적용 기대효과

본 논문에서 제안한 무기체계 SW 적용현황 조사 양식을 기반으로 1) 개발SW는 “재활용 추적성(~부터/~의 한)” 항목을 통해 무기체계간 개발SW 재활용 추적성을 확보할 수 있으며, 2) 상용SW, 공개SW의 경우 해당 소프트웨어의 “공급자명”, “SW 컴포넌트명”, “버전”, “다운로드 위치” 항목들을 통해 어떤 서드파티의 특정 SW를 가져와 사용하는지 추적성을 확보할 수 있다.

확보한 추적성을 기반으로 1) 개발SW는 사용간 발견된 결함, 사용자 추가 요구사항 등 개정사항이 발생 하여 국방 프로세스에 따라 수정이 필요한 SW 컴포넌트 2) 상용SW, 공개SW는 MITRE에서 제공하는 CVE 목록에 등록된 SW와 SW명, 버전이 일치하여 조치가 필요한 SW 컴포넌트를 식별하고 해당 SW 컴포넌트들이 적용된 모든 무기체계를 빠르게 식별, 정보 환류, 보완조치가 가능하다.

이를 통해 본 논문에서 제안한 새로운 데이터필드를 기반으로 SW 공급망 관리 수행이 가능하며 좀 더 효과적으로 무기체계 SW 공급망 공격에 대응할 수 있을것으로 기대된다.

5. 결론

효과적인 무기체계 SW 공급망 관리를 위해 현재 시행되고 있는 제도 중 무기체계 SW 적용현황 조사를 수행하고 있으나 공개SW에 대한 현황은 관리되지 않아 무기체계 전체에 대한 SW 공급망 관리는 힘든 상황이다. 그렇기에 본 논문에서는 SW 적용현황 조사 대상에 공개SW를 포함시키며 추가적으로 NTIA에서 제시하고 있는 SBOM 최소 데이터필드 항목을 충족할 수 있도록 제안하였다. SBOM 기반의 SW 적용현황 조사 데이터에 CVE 취약점 정보를 접목시킨다면 보다 체계적인 무기체계 SW 공급망 관리가 가능해져 SW 공급망을 통한 공격에 더 기민하게 대응할 수 있을 것으로 기대된다. 하지만 현재 국방분야에서 작성되는 SW 기술문서에는 제안된 데이터필드를 위한 정보 전체가 기재되어 있지 않거나 그 내용들이 각기 다른 종류의 기술문서에 파편화되어 작성된다. 그렇기에 추후 관련 데이터 확보, 자동화에 대한 후속 연구가 수행되고 국방SW 개발 프로세스 및 산출물에 연구 내용을 적용한다면 국방분야 SW 공급망 관리가 보다 더 효과적으로 수행될 것으로 기대된다.

References

[1] Ministry of National Defense(MND) Instruction "National Defense Power Generation Service Instruction", MND, Korea, pp.163, 2023.

[2] Y. Jeong, "A Study about Development Methodology for Ensure the Software Security of Weapon System", Korea Software Congress, Korea Information Science Society, Korea, pp. 77-79, 2018. 6

[3] Joanna F. DeFranco, Nir Kshetri "Software Supply Chains", IEEExplore journals & magazines, Vol. 55, Issue: 10, pp. 16 - 17, Oct. 2022. DOI: https://doi.org/10.1109/MC.2022.3191405

[4] U.S. GAO(Government Accountability Office), "Federal Response to SolarWinds and Microsoft Exchange Incidents" Jan. 2022. (GAO-22-104746)

[5] W. O. Ryu, S. M. Park, S. Y. Lee "Software Supply Chain Management and SBOM Trends", ETRI electronic communication trend analysis, Vol. 38, No 4, pp. 81-94 Aug. 2023., DOI: https://doi.org/10.22648/ETRI.2023.J.380408

[6] The MITRE Coperation, Overview About the CVE, The MITRE Coperation, cited 1999, Available From : https://cve.org/About/Overview (accessed Jun. 12,2024)

[7] National Telecommunications and Information Administration (NTIA) Report "The Minimum Elements For a Software Bill of Materials (SBOM)", NTIA, U.S.A. Available From: https://www.ntia.gov/report/2021/minimum-elements-software-bill-materials-sbom (accessed April. 09, 2024)

[8] Defense Acquisition Program Administration(DAPA) Manual "Weapon System Software Development and Management Manual", DAPA, Korea, pp. Appendix 8-1 ~ Appendix 8-12, 2022.

김 종 규(Jong-Kyu Kim) [정회원]

- 2019년 8월 : 동국대학교 정보통신공학과(정보통신공학학사)
- 2019년 12월 ~ 현재 : 국방기술품질원 연구원

〈관심분야〉
국방, 무기체계 소프트웨어, 소프트웨어 공학

조 한 별(Han-Byeol Cho) [정회원]

- 2019년 2월 : 성신여자대학교 컴퓨터소프트웨어학(공학사)
- 2023년 12월 ~ 현재 : 국방기술품질원 연구원

〈관심분야〉
국방, 무기체계 소프트웨어, 소프트웨어공학

채 신 영(Shin-Yeong Chae) [정회원]

- 2023년 2월 : 강원대학교 컴퓨터학부(컴퓨터정보통신공학학사)
- 2023년 12월 ~ 현재 : 국방기술품질원 연구원

〈관심분야〉
국방, 무기체계 소프트웨어, 소프트웨어공학

장 지 형(Ji-Hyung Chang) [정회원]

- 1991년 2월 : 한국과학기술원 전기및전자공학과(공학사)
- 2003년 1월 : 국방대학교 무기체계학과(군사과학석사)
- 2023년 9월 ~ 현재 : 아주대학교 시스템공학과 박사과정
- 1995년 12월 ~ 현재 : 국방기술품질원 (SW/IT연구실장)

〈관심분야〉
무기체계 소프트웨어, 소프트웨어 품질보증, 시스템엔지니어링

임 준 영(Jun-Yeong Lim) [정회원]

- 2016년 8월 : 부산대학교 정보컴퓨터공학부 졸업 (학사)
- 2018년 8월 : 부산대학교 전기전자컴퓨터공학과 졸업 (석사)
- 2018년 9월 ~ 2019년 2월 : 부산대학교 산학협력단 연구원 (계약직)
- 2020년 1월 ~ 2023년 7월 : 부산은행 정보개발부 대리(정규직)
- 2023년 7월 ~ 현재 : 국방기술품질원 연구원 (정규직)

〈관심분야〉
국방무기체계, 국방무기SW, 인공지능, 빅데이터, 사물인터넷