Journal of the Korea Academia-Industrial cooperation Society
Vol. 22, No. 12 pp. 89-94, 2021

https://doi.org/10.5762/KAIS.2021.22.12.89
ISSN 1975-4701 / eISSN 2288-4688

ISO/IEC 25023을 활용한 무기체계 소프트웨어 보안성 확보 방안

류지선*, 윤재형
국방기술품질원

Improving Security for Software in Weapon Systems Using ISO/IEC 25023

Jiseon Yu*, Jae-Hyeong Yun
Defense Agency for Technology and Quality

요 약 무기체계 소프트웨어의 보안성은「무기체계 소프트웨어 개발 및 관리 매뉴얼」에 따라 전장관리정보체계만을 대상으로 하여 무기체계 소프트웨어의 보안성 확보는 미흡한 상황이다. 본 논문에서는 시스템 및 소프트웨어를 특성 및 부특성 관점에서 정량적으로 평가하기 위한 품질 측정 항목을 정의한 ISO/IEC 25023의 보안성 측정을 무기체계 소프트웨어 개발 프로세스에 적용하여 보안성을 확보할 수 있는 방안을 제안한다. 여기에 ISO/IEC 25023의 보안성에서 다루지 않는 '가용성'을 추가하여 무기체계 소프트웨어에서 보안의 3요소 모두를 확보할 수 있도록 한다. 제안하는 방안은 무기체계 소프트웨어 개발 산출물인 요구사항 명세서 작성 가이드에 적용하는데 이로써 무기체계 소프트웨어 개발 프로세스 내에서 추가 문서 작성 없이 항목 보완만으로도 보안성 확보가 가능하다. 결과적으로 본 논문에서는 무기체계 소프트웨어 보안성 확보를 위해 요구사항 명세서를 보완하고 시험단계에서 ISO/IEC 25023에 따른 보안성 측정 함수에 따라 보안성을 정량적으로 측정 방안을 제안한다. 그 결과로 개발 중인 무기체계 소프트웨어에 즉시 적용 가능한 요구사항 명세서 작성 가이드를 제안하고 시험 절차서에 적용하여 무기체계 소프트웨어가 요구하는 보안성의 목표값을 달성하여 무기체계 소프트웨어 개발 프로세스에서 보안성을 확보할 수 있는 방안을 제안한다.

Abstract Since security in「Weapon System Software Development and Management Manual」only covers the battle management system, it is necessary to improve security in weapon system software. To this end, we examine a method to improve the security of weapon system software by applying the security measures of the ISO/IEC 25023 standard. It provides measures including associated measurement functions for the quality characteristics in the product quality model. Here, we propose a method to supplement the software requirement specification and measure security quantitatively according to the security measures of the ISO/IEC 25023. Also, we add the 'availability,' one of the CIA triads, to acquire security-enhanced software in weapon systems. Finally, we propose a guide for writing software that applies the proposed method and apply it to the test phase of the weapon system development process. In conclusion, we contribute to improving security in the weapon system software development process by quantitatively measuring security and proposing a method that can manage this process from the requirements phase to the test phase.

Keywords : ISO/IEC 25023, Security, Weapon Systems, Software, Weapon System Software

*Corresponding Author : Jiseon Yu(DTaQ)
email: gsun2@dtaq.re.kr
Received August 6, 2021 Revised August 18, 2021
Accepted December 6, 2021 Published December 31, 2021

1. 서론

무기체계 소프트웨어의 획득 및 관리 원칙 중 하나는 '무기체계 품질 향상을 위하여 무기체계 소프트웨어 개발 및 관리 매뉴얼의 소프트웨어 개발 프로세스를 준수하고 소프트웨어 신뢰성 및 보안성 확보 활동을 추진하도록 관리한다' 이다[1]. 이와 같이 무기체계 소프트웨어 품질 향상에 중요 요소를 신뢰성과 보안성으로 보고 있지만 무기체계 소프트웨어에서 신뢰성 확보 활동이란 소프트웨어의 잠재적 결함을 최소화시키기 위한 제반활동(신뢰성 확보계획 수립, 검증 및 확인, 신뢰성 시험 등)으로 정의하며 일반적인 소프트웨어 분야에서 신뢰성을 명세된 조건과 지정된 시간 동안 명세된 기능을 수행하는 정도로 정의하는 것과 차이가 있다. 또한 무기체계 소프트웨어에서 보안성은 전장관리정보체계만을 대상으로 하고 있기 때문에 사실상 무기체계 소프트웨어에서는 소스코드가 일으킬 수 있는 결함을 사전에 식별하여 제거하는 코딩규칙 검증, 취약점 점검, 소스코드 메트릭 점검을 수행하는 정적 시험과 실제 하드웨어에 탑재한 상태에서 소프트웨어 통합시험 절차서에 기술된 시험 절차에 따라 요구사항기반으로 소프트웨어 코드 실행률을 점검하는 동적 시험이 소프트웨어의 품질을 확인하는 유일한 시험인 상황이다. 이에 따라 ISO/IEC 25023을 무기체계 소프트웨어 개발 프로세스 중 요구사항 단계에 적용하여 품질 특성을 정량적으로 측정함으로써 품질을 개선하는 연구[2]와 무기체계 소프트웨어 개발 프로세스에서 소프트웨어 품질 관점 보안성 확보의 한계점 분석과 이를 개선하기 위한 ISO/IEC 25023을 활용하여 무기체계 소프트웨어의 보안성을 정량적으로 측정하는 연구[3]가 진행되었다. 본 논문에서는 ISO/IEC 25023에서 정의한 주특성 중 보안성 확보가 필요함을 보이는 연구[3]를 발전시켜 실제 무기체계 소프트웨어 개발 산출물에 즉시 적용 가능한 작성 가이드를 보이고 ISO/IEC 25023 보안성 측정에서 정의하지 않는 가용성을 측정 요소로 추가하여 무기체계 소프트웨어 보안성 측정으로 소프트웨어 품질 관점 보안성 확보 방안을 제안한다.

ISO/IEC 25023에서 보안성의 부특성은 기밀성, 무결성, 부인방지성, 책임성, 인증성이 있다. 무기체계 소프트웨어는 하드웨어를 제어하는 내장형 소프트웨어이기 때문에 일부 부특성은 적용할 수 없거나 적용에 한계가 따른다. 예를 들어 부인방지성을 측정한다고 가정하면 부인방지가 요구되는 사건 중에서 전자 서명을 사용하여 처리되는 비율을 측정한다. 전자 서명이란 송신자가 보내는 원본 문서에 첨부된 전자 서명의 생성과 검증을 수행하며 일반적으로 공개키 알고리즘을 사용하여 구현하고 무결성과 인증성, 부인방지성을 확보하는 기술이다. 그러나 내장형 소프트웨어는 이런 고급 기술을 내포하거나 구현할 수 없기 때문에 사실상 부인방지성을 측정하는 데에는 분명한 한계가 존재한다[3]. 그러나 사이버 공간에서의 기술이 빠르게 발전하고 최신 기술을 우리 군의 무기체계에 탑재한다고 가정한다면 그 어떤 요소도 절대 측정할 수 없다거나 필요 없는 기능이라고 정의할 수는 없다. 따라서 ISO/IEC 25023에서 정의하는 보안성을 활용하여 무기체계 소프트웨어 개발 프로세스에서 보안 기능이 필요한 부분을 식별하고 요구사항부터 보안성을 관리하고 이를 활용해 시험 단계에서 보안성을 정량적으로 측정하는 소프트웨어 품질 관점의 보안성 확보가 필요하다.

본 논문에서는 2장 이론적 배경으로 ISO/IEC 25023 표준과 이 표준에서 정의하는 보안성의 부특성, 그리고 이를 적용할 무기체계 소프트웨어 개발 프로세스를 설명하며 3장에서는 현재 무기체계 소프트웨어 개발 프로세스 산출물을 활용하여 무기체계 소프트웨어의 보안성을 확보할 수 있는 방법을 제안한다. 끝으로 4장에서는 결론을 맺는다.

2. 이론적 배경

2.1 ISO/IEC 25023 시스템 및 소프트웨어 공학 – 시스템 및 소프트웨어 품질 요구사항 및 평가 (SQuaRE) – 시스템 및 소프트웨어 제품 품질 측정

ISO/IEC 25023에 명시된 적용 범위에 따르면 이 표준은 시스템 및 소프트웨어 제품 품질을 ISO/IEC 25010에서 정의된 특성 및 부특성 관점에서 정량적으로 평가하기 위한 품질 측정 항목을 정의한다. 정의된 품질 주특성에는 기능 적합성, 성능 효율성, 호환성, 사용성, 신뢰성, 보안성, 유지보수성, 이식성이 있고 위와 같은 특성과 각 특성을 세분화한 부특성에 대한 기본적인 품질 측정 항목과 소프트웨어 제품 및 시스템 품질 측정 적용 방법이 포함되어 있다. 이 표준에서 제안된 품질 측정은 주로 시스템 및 소프트웨어 제품의 개발 생명 주기 프로세스 동안 품질 보증 및 개선을 목적으로 사용된다[4].

위의 품질 주특성 중 보안성 확보 연구를 진행한 이유는 무기체계 소프트웨어 개발 및 관리 매뉴얼에서 보안

성 확보는 해킹 등 사이버 공격의 원인인 보안약점을 사전에 제거하기 위한 보안성 시험이 있지만 보안성 시험 대상은 전장관리정보체계로 한정하고, 이 시험의 기준인 행정안전부 「소프트웨어 개발보안 가이드」는 대부분 웹 취약점 방지가 목적이므로 내장형 소프트웨어가 대부분인 무기체계 소프트웨어에 적용에 한계가 따르기 때문이다[3]. 즉, 본 논문에서는 문서 산출물에 품질 목표값을 정량적인 값으로 설정하고 측정이 가능한 ISO/IEC 25023을 활용함으로써 현재 무기체계 소프트웨어 개발 프로세스의 기존 산출물을 활용해 무기체계의 소프트웨어 보안성을 확보하고자 한다.

Table 1. Quality Measure name and Description of subcharacteristics in security characteristic

Subcharacteristics	Quality measure name	Description
Confidentiality	Access controllability	What proportion of confidential data items are protected from unauthorized accesses?
	Data encryption correctness	How correctly is the encryption/decryption of data items implemented as stated in the requirement specification?
	Strength of cryptographic algorithms	What proportion of cryptographic algorithms has been well-vetted?
Integrity	Data integrity	To what extent is the data corruption or modification by unauthorized access prevented?
	Internal data corruption prevention	To what extent are the available prevention methods for data corruption implemented?
	Buffer overflow prevention	What portion of memory accesses with user input in software modules has been done bounds checking for prevention buffer overflow?
Non-repudiation	Digital signature usage	What proportion of events requiring non-repudiation is processed using digital signature?
Accountability	User audit trail completeness	How complete is the audit trail concerning the user access to the system or data?
	System log retention	For what percent of the required retention period is the system log retained in stable storage?
Authenticity	Authentication mechanism sufficiency	How well does the system authenticate the identity of a subject?
	Authentication rules conformity	What proportion of the required authentication rules is established?

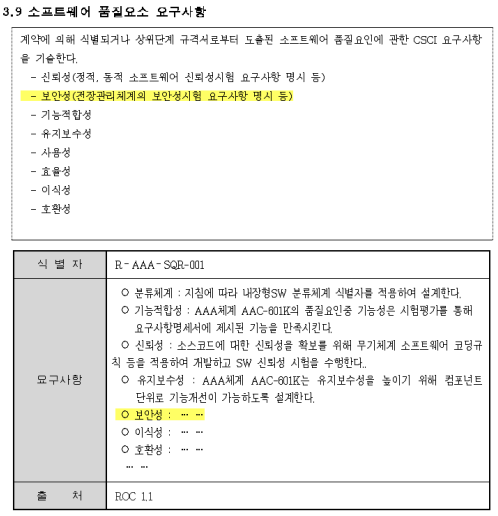
2.2 보안성 측정

ISO/IEC 25023에서 보안성 측정은 제품이나 시스템이 정보 및 데이터를 보호하여 사람이나 다른 제품 혹은 시스템이 그들의 유형과 권한 수준에 적합한 데이터 접근을 하도록 하는 정도를 평가하는 데 사용된다고 명시하고 있다[4]. 보안성의 부특성에는 기밀성, 무결성, 부인방지성, 책임성, 인증성이 있고 각 부특성(subcharacteristics)의 품질 측정 항목 이름(quality measure name)과 품질 측정으로 제공되는 정보(description)에 대한 설명은 Table 1과 같다. 대부분의 품질 측정 항목은 0.0에서 1.0사이로 정규화한 측정 함수를 사용하는데 측정 항목에서 측정하는 각 변수(Table 2 측정 함수의 A, B)를 품질 측정 요소(quality measure element)로 정의하고 이를 활용해 품질을 측정한다[4].

2.3 무기체계 소프트웨어 개발 프로세스

무기체계 소프트웨어는 「무기체계 소프트웨어 개발 및 관리 매뉴얼」에 따라 각 개발단계에 따라 소프트웨어 산출물을 작성한다. 소프트웨어 개발 단계를 〈요구사항 단계 - 설계 단계 - 구현 단계 - 시험 단계 - 배포 단계〉로 구분하면 이에 따른 무기체계 소프트웨어 기술자료 산출물은 〈소프트웨어 요구사항 명세서(SRS, Software Requirement Specification) - 소프트웨어 설계 기술서(SDD, Software Design Description) - 실행파일, 원시파일 - 소프트웨어 시험 절차서(STD, Software Test Description), 소프트웨어 시험 결과서(STR, Software Test Report) - 소프트웨어 산출물 명세서(SPS, Software Product Specification)〉로 나눌 수 있다. 본 논문에서 제안하는 품질 측정 요소를 요구사항 명세서에 작성하여 그 값을 측정하고자 하는 가장 큰 이유는 사용자 설명서가 개발단계 산출물에 포함되지 않기 때문에 기존 개발 프로세스 산출물의 큰 틀을 해치지 않고 품질 확보를 하는 최선의 방향이라고 생각했기 때문이다.

따라서 무기체계 소프트웨어 개발 프로세스의 요구사항 단계에 ISO/IEC 25023 적용을 위해 「무기체계 소프트웨어 개발 및 관리 매뉴얼」 소프트웨어 요구사항 명세서 작성 가이드를 살펴보면 소프트웨어 품질요소 요구사항에서 보안성은 특별한 예시가 작성되어 있지 않고, 계약에 의해 식별되거나 상위단계 규격서로부터 도출된 소프트웨어 품질요인에 관한 CSCI 요구사항을 기술하고


3.9 소프트웨어 품질요소 요구사항

계약에 의해 식별되거나 상위단계 규격서로부터 도출된 소프트웨어 품질요인에 관한 CSCI 요구사항을 기술한다.
- 신뢰성(정적, 동적 소프트웨어 신뢰성시험 요구사항 명시 등)
- 보안성(견장관리체계의 보안성시험 요구사항 명시 등)
- 기능적합성
- 유지보수성
- 사용성
- 효율성
- 이식성
- 호환성

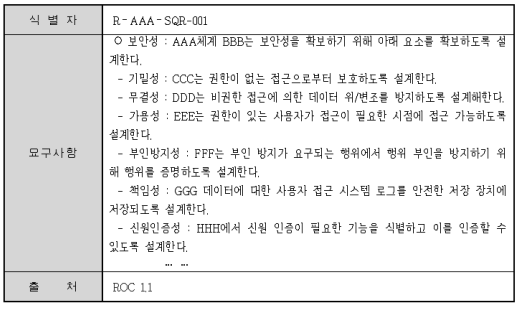
식 별 자	R-AAA-SQR-001
요구사항	○ 분류체계 : 지침에 따라 내장형SW 분류체계 식별자를 적용하여 설계한다. ○ 기능적합성 : AAA체계 AAC-601K의 품질요인중 기능성은 시험평가를 통해 요구사항명세서에 제시된 기능을 만족시킨다. ○ 신뢰성 : 소스코드에 대한 신뢰성을 확보를 위해 무기체계 소프트웨어 코딩규칙 등을 적용하여 개발하고 SW 신뢰성 시험을 수행한다. ○ 유지보수성 : AAA체계 AAC-601K는 유지보수성을 높이기 위해 컴포넌트 단위로 기능개선이 가능하도록 설계한다. ○ 보안성 : … … ○ 이식성 : … … ○ 호환성 : … … … …
출 처	ROC 1.1

Fig. 1. Software quality element requirements in SRS guide

그 중 보안성은 Fig. 1과 같이 전장관리정보체계의 보안성시험 요구사항 명시 등을 기재한다고 안내하고 있다. 본 논문에서는 이 소프트웨어 품질요소 요구사항 항목 보완으로써 무기체계 소프트웨어의 보안성을 확보하고자 한다.

3. 무기체계 소프트웨어 적용 방안

본 논문은 소프트웨어 품질은 최초의 소프트웨어 품질 요구사항 정의에 따라 결정되어 정량화 가능한 품질 요구사항의 확장을 제안한 [2]의 연구를 활용하여 무기체계 소프트웨어의 보안성 확보를 위해 보안성에 대한 요구사항을 산출물에 상세 기술이 필요함을 보이는 [3]의 연구를 본 연구에서 실제 산출물 적용 가이드를 보임으로써



식 별 자	R-AAA-SQR-001
요구사항	○ 보안성 : AAA체계 BBB는 보안성을 확보하기 위해 아래 요소를 확보하도록 설계한다. - 기밀성 : CCC는 권한이 없는 접근으로부터 보호하도록 설계한다. - 무결성 : DDD는 비권한 접근에 의한 데이터 위/변조를 방지하도록 설계해한다. - 가용성 : EEE는 권한이 있는 사용자가 접근이 필요한 시점에 접근 가능하도록 설계한다. - 부인방지성 : FFF는 부인 방지가 요구되는 행위에서 행위 부인을 방지하기 위해 행위를 증명하도록 설계한다. - 책임성 : GGG 데이터에 대한 사용자 접근 시스템 로그를 안전한 저장 장치에 저장되도록 설계한다. - 신원인증성 : HHH에서 신원 인증이 필요한 기능을 식별하고 이를 인증할 수 있도록 설계한다. … …
출 처	ROC 1.1

Fig. 2. The SRS writing guide including suggested security requirements

기존 연구를 개선하여 발전시켰음을 나타내고자 하였다. 대부분의 측정 항목은 요구사항 명세서나 설계 명세서 혹은 사용자 설명서 등에 명시한 목표값이 정규화 되어 있다[4]. 그러나 [2]의 연구에서 분석한 소프트웨어 품질 요구사항 사례를 보면 2020년 규격화된 무기체계 소프트웨어 282건 중 245건이 소프트웨어 품질 요구사항 식별자로 구분되어 요구사항으로 식별하였으나 「무기체계 소프트웨어 개발 및 관리 매뉴얼」에서 요구하는 신뢰성이 216건으로 88%를 차지하고 있지만 이외 품질 요소는 대부분 작성되지 않았다. 이와 같이 무기체계 소프트웨어의 품질은 무기체계 소프트웨어 개발 및 관리 매뉴얼에서 반드시 준수해야하는 신뢰성에 초점이 맞춰 있는 반면에 보안성은 실제 보안 기능이 구현되어 있더라도 품질 요소로 분리하여 그 요구사항까지 관리하고 품질을 평가하고 있지는 않은 것으로 보여 졌다. 이러한 현 상황을 개선하고자 본 논문에서는 ISO/IEC 25023에서 정의하는 보안성 측정 방법 적용에 무기체계 소프트웨어 개발 프로세스의 가장 적합한 개발 산출물을 요구사항 명세서로 식별하여 요구사항 단계부터 보안성을 확보할 수 있도록 소프트웨어 요구사항 명세서 내 품질요소 요구사항의 보안성관련 작성 가이드를 Fig. 2와 같이 제안한다. 이는 ISO/IEC 25023에서 정의한 보안성의 부특성 기준으로 작성되었고 정보보안의 주요소인 가용성을 추가로 작성하여 추후 소프트웨어 요구사항 명세서 작성 시 보안성 품질 확보 요소의 예시로 활용 될 수 있다. 여기서 ISO/IEC 25023 보안성의 부특성에 속하지 않는 가용성을 보안성 품질 요소의 측정 항목으로 작성 가이드에 함

Table 2. Measurement function and Expected result according to ISO/IEC 25023

Measurement function	Expected result
[Confidentiality] X = 1 - A/B A = Number of confidential data items that can be accessed without authorization B = Number of data items that require access control	1.0
[Integrity] X = 1 - A/B A = Number of data items which are actually corrupted by unauthorized access B = Number of data items for which data corruption or modification have to be prevented	1.0
[Availability] X = A/B A = System operation time actually provided B = System operation time specified in the operation schedule	1.0

께 작성한 이유는 ISO/IEC 25023에서 가용성은 신뢰성(reliability)의 부특성으로 분류하기 때문에 보안성에는 속하지 않지만 정보보안의 주요소로써 무기체계 소프트웨어에서는 보안성에서 다루어야 할 항목이라고 판단하였기 때문이다. 또한 가용성을 보안성에서 관리하여 현재 무기체계 소프트웨어에서 정의하는 신뢰성의 개념을 해치지 않음으로써 추후 보안성 외 ISO/IEC 25023의 다른 품질 특성 항목을 확대 적용하는데 혼선을 방지하고자 하였다.

앞서 Fig. 2로 제안한 소프트웨어 요구사항 명세서 내 보안성의 품질요소 요구사항 항목은 각 체계의 특성에 따라 구현되는 보안 기능은 차이가 있기 때문에 기밀성에서부터 신원인증성까지 모든 부특성을 이 항목에 작성하여 품질 요소로 관리가 필요한 것은 아니다. 다만 무기체계 소프트웨어인 만큼 비인가자의 데이터 접근과 데이터 위·변조는 해당 무기체계 뿐만 아니라 국가에 위협이 될 수 있는 중요한 사항이므로 최소 기밀성, 무결성, 가용성에 대해서는 이 항목에서 보안성의 주요 부특성으로 품질 요소 요구사항으로 작성함으로써 체계적인 관리가 필요하다. 이 항목에 작성된 보안성에 대한 요구사항은 설계단계를 거쳐 구현 후 시험 단계에서 ISO/IEC 25023에 따른 측정 함수를 활용하여 Table 2와 같이 보안성의 부특성에 따라 보안성을 정량적으로 측정할 수 있다. 0.0에서 1.0사이로 정규화한 측정 함수의 결과는 목표한 바와 같이 1.0이 되어야 하며 이러한 항목은 무기체계 소프트웨어 개발 산출물 중 요구사항에서 명세한 기능의 시험 절차를 작성한 소프트웨어 통합 시험 절차서 내 결과 평가를 위한 기준에 작성하여 시험 시 이를 기반으로 각 품질 요소를 정량적으로 측정하고 관리함으로써 무기체계 소프트웨어의 보안성을 확보할 수 있을 것이다. 이처럼 무기체계 소프트웨어의 보안성 확보를 목표로 각 부특성의 품질 측정 목표값(expected result)을 달성하기 위해서는 각 부특성의 구현이 필요한 데이터를 정확히 식별하는 것이 선제되어야 한다. 예를 들어 기밀성 측정 함수의 품질 측정 요소 B는 '접근 제어 기능이 요구되는 데이터 항목의 수'로 정의하고 있는데 측정 대상 소프트웨어를 제대로 이해하고 있지 않은 경우에는 어떤 데이터에 접근 제어 기능을 적용해야하는지 식별할 수 없기 때문에 측정에 필요한 품질 측정 요소는 측정 대상 소프트웨어 이해의 정도에 따라 결정될 수 있음에 유의해야 한다.

4. 결론

본 논문에서는 무기체계 소프트웨어 보안성 확보를 위해 무기체계 소프트웨어 개발 산출물인 소프트웨어 요구사항 명세서의 품질 요소 요구사항에 ISO/IEC 25023 표준에 따른 보안성 품질 요구 사항을 작성하고 목표값을 설정하여 시험단계에서 ISO/IEC 25023의 품질 측정 함수를 활용해 보안성을 정량적으로 측정하는 방법을 제안하였다. 이는 보안성 확보 활동을 전장관리정보체계만을 대상으로 하여 무기체계 소프트웨어의 보안성 확보에 미흡한 현 상황을 개선함으로써 무기체계 소프트웨어의 보안성 향상에 크게 기여할 수 있을 것으로 판단된다.

References

[1] Defense Acquisition Program Administration(DAPA), "Weapon System Software development and management manual", Notice, DAPA, Korea, 2020

[2] Yoon, Gyeonghwan, and Jiseon Yu. "Applying ISO/IEC 25023 to Software Engineering Process in Weapon System for Quality Improvement." Journal of the Korea Academia-Industrial cooperation Society 22.5, pp.387-393, 2021.
DOI: https://doi.org/10.5762/KAIS.2021.22.5.387

[3] Yu J, Yoon G, "Improving Security for Software in Weapon System", Proceedings of Conference on Information Security and Cryptography Summer, Seoul, Korea, pp.722-725, June 2021.

[4] ISO/IEC 25023 "Software engineering : Software product Quality Requirements and Evaluation(SQuaRE) - Measurement of system and software product quality", 2016.

류 지 선(Jiseon Yu) [정회원]

- 2018년 8월 : 고려대학교 정보보호대학원 정보보호학과 (정보보호학석사)
- 2018년 12월 ~ 현재 : 국방기술품질원 연구원

〈관심분야〉
무기체계 소프트웨어, 소프트웨어 보안

윤 재 형(Jae-Hyeong Yun) [정회원]

- 2017년 2월 : 건국대학교 전자공학부 (전자공학학사)
- 2017년 2월 ~ 현재 : 국방기술품질원 연구원

〈관심분야〉
국방, 무기체계 소프트웨어, 소프트웨어 품질