기능 안전 표준 기반의 무기체계 소프트웨어 개발 및 관리 매뉴얼 분석 및 개선 방안 연구†

(Analysis and improvement of weapon system software development and management manual based on functional safety standards)

김 태 현 ‡ 박 다 운 § 백 옥 현 ¶
(Taehyoun Kim) (Daun Bak) (Ockhyun Paek)

요 약 최근 기능 안전에 대한 관심이 높아짐에 따라 다양한 산업 분야에서 기능 안전 표준의 적용이 요구되고 있다. 기능 안전 표준은 시스템의 오작동을 방지하기 위해 필요한 기능 안전 관련 활동들을 정의한 문서이다. 이 표준에 정의된 모든 활동들은 시스템의 위험 분석 및 평가를 통해 산출된 등급 분류 결과에 따라 차등적으로 요구된다. 국내 무기체계 분야에는 방위사업청에서 발간한 무기체계 소프트웨어 개발 및 관리 매뉴얼이 존재한다. 이 매뉴얼은 기능 안전 관련 활동으로 소프트웨어 정적 및 동적 분석 활동을 요구한다. 하지만 해당 매뉴얼에는 선행 활동으로 요구되는 위험 분석 및 평가를 통한 등급 분류 활동 관련 내용이 구체적으로 언급되고 있지 않다. 따라서 본 연구에서는 대표적인 기능 안전 표준들을 기반으로 무기체계 소프트웨어 개발 및 관리 매뉴얼의 문제점을 분석하고 이에 대한 개선 방안을 제시하도록 한다.

키워드 : 무기체계 소프트웨어, 기능 안전, 소프트웨어 등급

Abstract As interest in functional safety has recently increased, application of functional safety standards has been required in various industrial fields. A functional safety standard is a document that defines functional safety-related activities required to prevent system malfunctions. All activities defined in this standard are required differentially according to the classification results calculated through the risk analysis and assessment of the system. In the field of domestic weapon systems, there is a manual for the development and management of weapon system software issued by the Defense Acquisition Program Administration (DAPA). This manual requires static and dynamic analysis of software for functional safety related activities. However, the manual does not specifically address the classification activity through risk analysis and assessment as required for the preceding activities. Therefore, in this study, we analyze the problems of the manual based on the representative functional safety standards, and propose improvement plans.

Key words : weapon system software, functional safety, software level

1. 서 론

국내 무기체계 분야 소프트웨어 개발 담당자들은 방위사업청에서 발간한 무기체계 소프트웨어 개발 및 관리 매뉴얼[1]에 따라 소프트웨어를 개발해야 한다. 이 매뉴얼에는 소프트웨어 개발, 관리, 지원 3가지 측면의 프로세스와 각각의 프로세스별 세부 활동들이 정의되어 있으며 이는 소프트웨어 생명 주기 관련 국제 표준인 ISO/IEC/IEEE 12207 Systems and software engineering -- Software life cycle processes (이하 'ISO/IEC/IEEE 12207')[2]를 기반으로 작성되었다.

최근에는 다양한 산업 분야에서 소프트웨어 생명 주기 관련 표준 외에도 기능 안전에 관한 표준의 적용이 요구되고 있다[3-5]. 기능 안전 표준은 시스템의 오작동을 방지하기 위해 필요한 기능 안전 관련 활동들을 정의한 문서이다. 이 표준에 정의된 모든 활동들은 시스템의 위험 분석 및 평가를 통해 산출된 등급 분류 결과에 따라 차등적으로 요구된다.

국내 무기체계 분야의 경우에는 기능 안전 관련 활동으로 소프트웨어의 정적 및 동적 분석 활동이 소프트웨어 개발 담당자들에게 요구된다[1]. 하지만 무기체계 소프트웨어 개발 및 관리 매뉴얼에는 앞서 언급한 기능 안전 활동들의 수행 수준 결정을 위한 내용이 구체적으로 언급되어 있지 않다. 따라서 본 연구에서는 대표적인 기

† 본 연구는 2020 한국 소프트웨어공학 학술대회에서 우수 산업체 논문으로 선정되어 소프트웨어공학 소사이어티 논문지로 추천을 받았습니다.
‡ 회 원 : 국방과학연구소 정보화기술실 SW기술팀
tae_hyoun@add.re.kr
§ 비 회 원 : 국방과학연구소 정보화기술실 SW기술팀
dwpark90@add.re.kr
¶ 비 회 원 : 국방과학연구소 정보화기술실 SW기술팀
ohpaek@add.re.kr
논문접수 : 2020년 02월 28일
심사완료 : 2020년 03월 01일

능 안전 표준들을 기반으로 등급 분류 관점에서 무기체계 소프트웨어 개발 및 관리 매뉴얼의 문제점을 분석하고 이에 대한 개선 방안을 제시하도록 한다.

본 논문의 장절 구성은 다음과 같다. 1장에서는 본 연구에 대한 개략적인 설명을 하였으며 2장에서는 본 연구의 배경 지식이 되는 기능 안전 표준 및 무기체계 소프트웨어 개발 및 관리 매뉴얼의 기능 안전 관련 내용을 간략히 이야기하도록 한다. 3장에서는 기능 안전 표준을 기반으로 분석한 무기체계 소프트웨어 개발 및 관리 매뉴얼의 문제점을 이야기하며 4장에서 이 문제점에 대한 개선 방안을 제시하도록 한다. 마지막으로 5장 결론을 통해 본 논문을 마치도록 한다.

2. 배경

기능 안전 표준은 시스템의 오작동을 방지하기 위해 필요한 기능 안전 관련 활동들을 정의한 문서이다. 이와 관련된 대표적인 표준으로는 전자, 전기 분야에 적용되는 IEC 61508 Functional safety of electrical/electronic/programmable electronic safety-related systems[3](이하 'IEC 61508')가 존재한다. IEC 61508을 기반으로 자동차, 철도 등 다양한 산업 분야에서 각 분야에 적합한 별도의 기능 안전 표준을 만들어 적용하고 있다[4,5].

기능 안전 표준에 정의된 모든 활동들은 시스템의 위험 분석 및 평가를 통해 산출된 등급 분류 결과에 따라 차등적으로 요구된다. 아래 표 1은 대표적인 기능 안전 표준인 IEC 61508[3]에 정의되어 있는 안전 무결성 등급(Safety Integrity Level, 이하 'SIL')에 대한 표이다. IEC 61508에서는 SIL에 따라 수행되어야 하는 활동의 수준을 달리한다.

Safety Integrity level (SIL)	Average probability of a dangerous failure on demand of the safety function	Average frequency of a dangerous failure of the safety function
4	≥10^-5 to < 10^-4	≥10^-9 to < 10^-8
3	≥10^-4 to < 10^-3	≥10^-8 to < 10^-7
2	≥10^-3 to < 10^-2	≥10^-7 to < 10^-6
1	≥10^-2 to < 10^-1	≥10^-6 to < 10^-5

표 2 IEC 61508[3]의 SIL 분류 기준

국내 무기체계 분야의 경우에는 기능 안전 관련 활동으로 개발자에게 소프트웨어의 정적 및 동적 분석 활동을 요구한다[1]. 무기체계 소프트웨어 개발 및 관리 매뉴얼에서는 정적 분석 활동으로 MISRA-C:2012[6] 등과 같은 코딩 규칙의 준수 및 CWE(Common Weakness Enumeration) 658, 659, 660[7]에 목록화 되어 있는 취약점 항목의 점검, 함수의 복잡도와 같은 소스코드 메트릭 분석 및 제한값 준수를 요구하고 있으며 동적 분석 활동으로는 요구사항 기반의 구조적 coverage 달성을 요구하고 있다.

무기체계 소프트웨어 개발 및 관리 매뉴얼에서는 동적 분석 활동에 한하여 별도의 등급 분류 기준을 제공한다. 아래 표 2와 3은 매뉴얼에 제시되어 있는 등급 분류 기준과 등급 별 요구되는 동적 분석 활동의 수준을 나타내는 표이다. 소프트웨어 개발 담당자는 아래 기준에 따라 등급 별 요구되는 구조적 coverage에 대한 분석을 수행해야 한다.

영향도 (Severity)	
수준	내용
S1	무시 가능
S2	사소함
S3	심각함
S4	치명적
발생 빈도 (Exposure)	
수준	내용
E1	매우 낮은 확률
E2	낮은 확률
E3	중간 확률
E4	높은 확률
제어 가능성 (Controllability)	
수준	내용
C1	간단히 제어가능
C2	보통의 경우 제어가능
C3	제어하기 어렵거나 불가능

표 3 무기체계 소프트웨어 개발 및 관리 매뉴얼의 등급 분류 기준

영향도 (Severity)	발생 빈도 (Exposure)	제어 가능성(Controllability)		
		C1	C2	C3
S1	E1	S	S	S
	E2	S	S	S
	E3	S	S	S
	E4	S	S	S
S2	E1	S	S	S
	E2	S	S	S
	E3	S	S	S
	E4	S	S	B
S3	E1	S	B	B
	E2	B	B	B
	E3	B	B	B
	E4	B	B	M
S4	E1	B	B	M
	E2	B	M	M
	E3	B	M	M
	E4	M	M	M
* S: Statement coverage, B: Branch coverage, M: MC/DC(Modified condition & decision coverage)				

표 4 무기체계 소프트웨어 개발 및 관리 매뉴얼의 등급 분류 기준 별 요구되는 동적 분석 활동 수준

3. 문제점

3.1 시스템 수준과 소프트웨어 수준의 기능 안전 관련 활동간 연계 미흡

국내 무기체계 분야에서는 방위사업관리규정[8]을 통해 사업 수행 시 시스템 수준의 위험 관리 활동 수행을 요구하고 있다. 이를 위해 방위사업청에서는 SE(System Engineering) 기반 위험관리 가이드북[9]을 발간하여 위험 관리 수행 방법과 절차 등을 제공하고 있다. 하지만 해당 가이드북은 시스템 및 소프트웨어의 기능 안전 관련 활동을 언급하고 있지 않으며 등급 분류에 관해서도 아래 표4와 같이 단순 예시만을 제공하고 있다.

구분		발생 가능성			
		낮음(1)	보통(2)	높음(3)	매우 높음(4)
영향성	낮음(1)	1	2	3	4
	보통(2)	2	4	6	8
	높음(3)	3	6	9	12
	매우 높음(4)	4	8	12	16
* 위험 수준에 따라 관리수준 설정: 실무자(1~4), 팀장(6~9), 부장(12), 본부장(16)					

표 5 SE 기반 위험관리 가이드북[9]의 매트릭스를 활용한 위험수준 관리 예시

아래 표 5는 무기체계 소프트웨어 개발 및 관리 매뉴얼에서 요구하는 정적 및 동적 분석 활동에 대한 등급 분류 기준 적용 여부를 분석한 표이다. 표 5에서 보는 바와 같이 정적 분석 활동의 경우에는 등급 분류 기준이 적용되고 있지 않으며 개발되는 모든 소프트웨어에 대해 동일한 수준의 활동이 요구되고 있다. 동적 분석 활동의 경우에는 표 2, 3과 같이 등급 분류 기준이 적용되고는 있으나 시스템 수준의 위험 관리 활동과 별개로 해당 활동이 요구되고 있다.

기능 안전 관련 활동 구분(대)	기능 안전 관련 활동 구분(중)	등급 분류 기준 적용 여부
정적 분석	코딩 규칙 준수	**등급 미분류** 및 모든 소프트웨어에 대해 동일한 기준의 활동 요구
	취약점 점검	
	소스코드 메트릭 제한값 준수	
동적 분석	요구사항 기반 구조적 coverage 분석	**시스템 수준과 별개로 등급 분류** 및 활동 수행

표 6 무기체계 소프트웨어 개발 및 관리 매뉴얼의 정적 및 동적 분석 활동 별 등급 분류 기준 적용 여부

3.2 등급 분류 활동을 위한 자원 부족

무기체계 분야는 다른 산업 분야와 비교했을 때 다양한 시스템이 개발된다는 특징이 존재한다. 따라서 위험 분석 및 평가를 통한 등급 분류 활동을 수행하기 위해서는 상당히 많은 비용과 시간이 필요하다. 또한 개발하는 시스템의 종류는 다양한 반면 각각의 시스템이 양산되는 수량은 타 산업 분야에 비해 현저히 적다는 특징이 있다. 이로 인해 등급 분류 활동을 위한 기반 데이터가 부족하다는 문제가 존재한다.

아래 표 6은 방위사업청에서 제공하는 무기체계 분류체계[10]의 대분류 항목을 나열한 표이다. 무기체계는 대분류 10종, 중분류 42종, 소분류 132종으로 분류된다. 타 산업 분야의 기능 안전 표준을 적용해보면 자동차 분야 기능 안전 표준 ISO 26262[4]는 기동 무기체계 분야의 일부에만 적용될 수 있으며 항공기 분야 기능 안전 표준 DO-178C[5]는 항공 무기체계의 일부에만 적용될 수 있다.

번호	대분류 항목	번호	대분류 항목
1	지휘통제 · 통신 무기체계	6	화력 무기체계
2	감시 · 정찰 무기체계	7	방호 무기체계
3	기동 무기체계	8	기타 무기체계
4	함정 무기체계	9	비무기체계
5	항공 무기체계	10	국방정보체계

표 7 무기체계 분류체계 - 대분류 항목

3.3 타 기능 안전 표준 대비 높은 수준의 동적 분석 활동 요구

2장에서 기술한 바와 같이 매뉴얼에서는 동적 분석 활동을 위해 별도의 등급 분류 기준을 제시하고 있다. 하지만 매뉴얼에서 요구하는 동적 분석 활동의 수준은 타 산업 분야의 기능 안전 표준[3,4,5]에서 요구하는 동적 분석 활동의 수준보다 상당히 높다. 아래 표 7, 8, 9는 대표적인 소프트웨어 기능 안전 표준인 ISO 26262-6[4]과 DO-178C[5]에서 요구되는 동적 분석 활동 수준을 무기체계 소프트웨어 개발 및 관리 매뉴얼의 등급 분류 기준에 대입한 결과를 나타내는 표이다. 표 7, 8, 9에서 보는 바와 같이 타 분야의 기능 안전 표준에서는 등급이 낮은 소프트웨어의 경우 동적 분석 활동을 요구하고 있지 않으나 방위사업청의 매뉴얼은 표3에서 보는 바와 같이 등급이 낮은 소프트웨어에 대해서도 최소 statement coverage 달성을 요구하고 있다.

영향도 (Severity)	발생 빈도 (Exposure)	제어 가능성(Controllability)		
		C1	C2	C3
S1	E1	-	-	-
	E2	-	-	-
	E3	-	-	-
	E4	-	-	-
S2	E1	-	-	-
	E2	-	-	-
	E3	-	-	S
	E4	-	S	B
S3	E1	-	-	-
	E2	-	-	S
	E3	-	S	B
	E4	S	B	B
S4	E1	-	-	S
	E2	-	S	B
	E3	S	B	B
	E4	B	B	M
* -: 활동 미요구 S: Statement coverage, B: Branch coverage, M: MC/DC(Modified condition & decision coverage)				

표 8 ISO 26262의 등급 분류 기준('++' Highly Recommendation 기준) 요구되는 동적 분석 활동을 무기체계 소프트웨어 개발 및 관리 매뉴얼의 등급 분류 기준에 대입한 결과

영향도 (Severity)	발생 빈도 (Exposure)	제어 가능성(Controllability)		
		C1	C2	C3
S1	E1	-	-	-
	E2	-	-	-
	E3	-	-	-
	E4	-	-	-
S2	E1	-	-	-
	E2	-	-	-
	E3	-	-	-
	E4	-	-	-
S3	E1	S	S	S
	E2	S	S	S
	E3	B	B	B
	E4	B	B	B
S4	E1	M	M	M
	E2	M	M	M
	E3	M	M	M
	E4	M	M	M
* -: 활동 미요구 S: Statement coverage, B: Branch coverage, M: MC/DC(Modified condition & decision coverage)				

표 10 DO-178C의 등급 분류 기준 요구되는 동적 분석 활동을 무기체계 소프트웨어 개발 및 관리 매뉴얼의 등급 분류 기준에 대입한 결과

영향도 (Severity)	발생 빈도 (Exposure)	제어 가능성(Controllability)		
		C1	C2	C3
S1	E1	-	-	-
	E2	-	-	-
	E3	-	-	-
	E4	-	-	-
S2	E1	-	-	-
	E2	-	-	-
	E3	-	-	M
	E4	-	M	M
S3	E1	-	-	-
	E2	-	-	M
	E3	-	M	M
	E4	M	M	M
S4	E1	-	-	M
	E2	-	M	B
	E3	M	M	M
	E4	M	M	M
* -: 활동 미요구 S: Statement coverage, B: Branch coverage, M: MC/DC(Modified condition & decision coverage)				

표 9 ISO 26262-6의 등급 분류 기준('+' Recommendation 기준) 요구되는 동적 분석 활동을 무기체계 소프트웨어 개발 및 관리 매뉴얼의 등급 분류 기준에 대입한 결과

4. 개선 방안

4.1 시스템과 소프트웨어 수준의 기능 안전 관련 활동 연계를 위한 제도 개선

3.1절에서 기술한 바와 같이 국내 무기체계 분야에서는 시스템 수준에서 수행되는 기능 안전 관련 활동이 소프트웨어 수준의 활동과 연계되지 않고 있다는 문제점이 있다. 이러한 문제를 해결하기 위해서는 먼저 시스템 수준의 관련 규정과 소프트웨어 개발 및 관리 매뉴얼 간의 연계성 확보를 위한 제도 개선이 필요하다. 정적 분석 활동의 경우 시스템 및 소프트웨어 수준의 등급 분류 기준에 따라 활동의 수준을 달리할 수 있도록 제도 개선이 필요하며 동적 분석 활동의 경우 시스템 수준의 등급 분류 기준과 소프트웨어 수준의 등급 분류 기준이 연계될 수 있도록 제도 개선이 되어야 한다.

본 연구에서는 이를 위해 MIL-STD-882E[11]의 시스템 및 소프트웨어 위험 등급 분류 방법을 국내 무기체계 분야에 적용하는 방안을 제시한다. MIL-STD-882E[11]는 미 국방부에서 발간한 시스템 안전 관련 문서이다. SE 기반 위험관리 가이드북에서 참고하고 있는 미 국방부 위험 관리 관련 문서[12]의 경우 시스템 안전과 관련된 내용에 대해서는 MIL-STD-882E를 참고하도록 하고 있으며 MIL-STD-882E에는 시스템 수준에서부터 소프트웨어 수준까지 연계되는 위험 분석 및 등급 분류 방법이 제시되어 있다. 아래 표 10은 MIL-STD-882E에서 제시하고 있는 시스템의 위험 평가 매트릭스이다. MIL-STD-882E는 시스템의 위험 분석 및 평가 활동과

연계하여 시스템의 위험에 소프트웨어가 미치는 영향의 등급을 결정하기 위한 별도의 기준을 제시하고 있으며 이에 대한 내용은 표 11과 12에서 보는 바와 같다.

Severity / Probability	Catastrophic (1)	Critical (2)	Marginal (3)	Negligible (4)
Frequent (A)	High	High	Serious	Medium
Probable (B)	High	High	Serious	Medium
Occasional (C)	High	Serious	Medium	Low
Remote (D)	Serious	Medium	Medium	Low
Improbable (E)	Medium	Medium	Medium	Low
Eliminated (F)	Eliminated			

표 11 MIL-STD-882E의 시스템 수준 Risk assessment matrix

Severity / SW Control	Catastrophic (1)	Critical (2)	Marginal (3)	Negligible (4)
Autonomous (AT)	SwCI 1	SwCI 1	SwCI 3	SwCI 4
Semi-Autonomous (SAT)	SwCI 1	SwCI 2	SwCI 3	SwCI 4
Redundant Fault Tolerant (RFT)	SwCI 2	SwCI 3	SwCI 4	SwCI 4
Influential	SwCI 3	SwCI 4	SwCI 4	SwCI 4
No Safety Impact (NSI)	SwCI 5	SwCI 5	SwCI 5	SwCI 5

* SwCI: Software Criticality Index

표 12 MIL-STD-882E의 Software safety criticality matrix

SwCI	Risk Level
SwCI 1	High
SwCI 1	Serious
SwCI 2	Medium
SwCI 3	Low
SwCI 5	Not Safety

표 13 MIL-STD-882E의 SwCI와 Risk Level 간의 관계

4.2 분류체계 기반 등급 사전 분류 및 정보 제공

3.2절에서 언급한 바와 같이 무기체계 분야는 다른 산업 분야와 비교했을 때 개발하는 시스템의 종류는 다양한 반면 각각의 시스템이 양산되는 수량은 적다는 특징이 존재한다. 이로 인해 위험 분석을 수행하기 위한 기반 데이터가 부족할 뿐만 아니라 상당히 많은 비용과 시간이 필요하다는 문제가 존재한다. 본 연구에서는 이를 해결하기 위해 방위사업청에서 제공하는 무기체계 분류체계[10] 및 국방과학기술 표준분류체계[10]를 기반으로 시스템 및 하위 구성품에 대한 등급을 사전에 분류하고 이에 대한 정보를 제공해주는 방안을 제안한다.

표 4에서 보는 바와 같이 무기체계 분류체계는 시스템 유형을 기준으로 무기체계를 분류하고 있다. 또한 표 10에서 보는 바와 같이 국방과학기술 표준분류체계는 시스템이 아닌 기술적인 측면에서 분류 기준을 제시하고 있다. 이 두 가지 분류체계 내 각각의 항목별로 대표적인 위험 요소를 사전에 분석하고 등급 분류 결과를 시스템 및 소프트웨어 개발 담당자들에게 제공한다면 기반 데이터 및 비용, 시간 부족으로 인한 담당자들의 어려움을 해소할 수 있을 뿐만 아니라 기능 안전과 관련된 시스템 수준 활동과 소프트웨어 수준 활동 간의 연계도 가능할 것으로 기대한다.

번호	대분류 항목	번호	대분류 항목
1	센서	5	추진
2	정보통신	6	화생방
3	제어전자	7	소재
4	탄약/에너지	8	플랫폼/구조

표 14 국방과학기술 표준분류체계 - 대분류 항목

4.3 타 기능 안전 표준과 유사한 수준의 동적 분석 활동 요구

3.3절에서 언급한 바와 같이 매뉴얼에 존재하는 동적 분석 활동의 수준은 다른 산업 분야의 기능 안전 표준[3-5]에서 요구하는 동적 분석 활동의 수준보다 상당히 높다. 만일 개발되는 모든 소프트웨어에 대해 요구사항 기반의 동적 분석 활동을 수행한다면 상당히 많은 시간과 비용이 요구될 것이다. 따라서 투입 노력 대비 효과를 고려하여 타 기능 안전 표준과 유사한 수준의 활동으로 수준을 조정할 필요성이 존재한다.

기능 안전 표준은 동적 분석 활동뿐만 아니라 소프트웨어 생명 주기 각 단계별로 기능 안전을 위한 다양한 활동들을 제시하고 있다. 그리고 이러한 활동들은 위험 분석 및 평가 활동을 통한 등급 분류를 기준으로 수준을 달리하도록 요구된다. 소프트웨어의 기능 안전을 고려한다면 단순히 높은 수준의 동적 분석 활동만을 수행하기보다는 생명 주기 별 여러 활동들을 등급에 따라 수준에 맞게 복합적으로 수행하는 것이 더욱 도움 될 것으로 판단한다.

5. 결론

본 연구에서는 기능 안전 표준을 기반으로 무기체계 소프트웨어 개발 및 관리 매뉴얼의 문제점을 분석하였으며 이에 대한 개선 방안을 제시하였다. 국내 무기체계 분야에서는 무기체계 소프트웨어 개발 및 관리 매뉴얼을 통해 기능 안전 관련 활동으로 소프트웨어 정적 및 동적 분석 활동을 요구하고 있다. 하지만 해당 매뉴얼에는 모든 기능 안전 관련 활동의 선행 활동으로 요구되는 위험 분석 및 평가를 통한 등급 분류 활동에 관한 내용이 구체적으로 나와 있지 않다. 본 연구에서는 등급 분류 관점에서 매뉴얼의 문제점을 3가지로 구분하여 분석하였으며 각각의 문제점에 대한 개선 방안을 제시하였다. 이를 통해 무기체계 소프트웨어 분야 개발 담당자들이 기능 안전 관련 활동을 더욱 원활하게 수행할 수 있기를 기대한다.

참 고 문 헌

[1] 방위사업청, “무기체계 소프트웨어 개발 및 관리 매뉴얼”, 2018.

[2] ISO/IEC/IEEE, ISO/IEC/IEEE 12207:2017 Systems and software engineering – Software life cycle processes, 2017.

[3] IEC, IEC 61508:2010 Functional safety of electrical/electronic/programmable electronic safety-related systems, 2010.

[4] ISO, ISO 26262 Road vehicles – Functional safety, 2012.

[5] RTCA, DO-178C Software Considerations in Airborne Systems and Equipment Certification, 2011.

[6] MISRA, MISRA-C:2012 Guidelines for the use of the C language in critical systems, 2013.

[7] MITRE, https://cwe.mitre.org/

[8] 방위사업청, “방위사업관리규정”, 2019.

[9] 방위사업청, “SE기반 위험관리 가이드북“, 2018.

[10] 방위사업청, 국방과학기술 정보관리 업무지침, 2018.

[11] DOD, MIL-STD-882E Standard practice for system safety, 2012.

[12] DOD, Risk, Issue, and Opportunity Management Guide for Defense Acquisition Programs, 2017.

김 태 현

2012년 아주대학교 정보 및 컴퓨터 공학부 졸업(학사). 2014년 한국과학기술원 전산학과 졸업(석사). 2014년~현재 국방과학연구소 연구원. 관심분야는 소프트웨어 공학, 소프트웨어 신뢰성 공학.

박 다 운

2013년 성균관대학교 시스템경영공학과 졸업(학사), 2015년 한국과학기술원 경영공학과 졸업(석사), 2015년~현재 국방과학연구소 연구원. 관심분야는 소프트웨어 신뢰성 공학.

백 옥 현

2000년 충북대학교 정치외교학과(학사). 2002년 충북대학교 전산학과(석사). 2002년~현재 국방과학연구소 연구원. 관심분야는 소프트웨어 아키텍처, 소프트웨어 테스팅.