Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.31, NO.4, Aug. 2021 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2021.31.4.817

무기체계 개발을 위한 RMF A&A의 실증에 관한 연구*

조 광 수,[1†] 김 승 주[2‡]
[1,2]고려대학교 정보보호대학원 (대학원생, 교수)

A Study on Proving RMF A&A in Real World for Weapon System Development*

Kwangsoo Cho,[1†] Seungjoo Kim[2‡]
[1,2]ICSP(Institute of Cyber Security & Privacy), School of Cybersecurity, Korea University (Graduate student, Professor)

요 약

소프트웨어를 안전하게 관리하기 위해 군은 RMF A&A(Risk Management Framework Assessment & Authorization) 표준에 따라 제품을 구매하고 관리한다. 해당 표준은 무기체계를 비롯한 군 IT 제품의 획득 체계에 관한 표준으로 제품에 대한 요구사항, 평가를 통한 구매, 유지보수를 다룬다. 해당 표준에 따르면 제품 개발활동에는 군에서 제시한 임무의 위험도가 반영되어야 한다. 즉, 개발사는 보안 내재화 및 공급망 보안을 통해 제시된 위험도를 완화하였고, RMF A&A의 보안 요구사항을 제대로 준수하였음을 입증하는 자료를 제출해야하고, 군에서는 개발사로부터 제출된 증거자료에 대한 평가를 통해 최종 획득 여부를 결정한다. 기존에 RMF A&A 실증 연구가 수행된 사례가 있다. 하지만, 해당 연구는 RMF A&A의 전체 단계가 아닌 일부분에 대해서만 다루고 있고, 해당 연구의 실증 사례가 대외비인 관계로 상세한 정보가 공개되지 않아 실제 산업 환경에 적용하는데 어려움이 있다. 이에 본 논문에서는 군의 위험도 측정 및 RMF A&A 관련 표준들을 분석하고, 이를 바탕으로 군 RMF A&A의 요구사항을 만족시킬 수 있는 증거자료 작성방안에 대해 제시한다. 또한, 제시한 방안을 실제 드론 시스템에 적용하여 작성된 평가 제출물이 RMF A&A의 요구사항에 부합한지 검증을 수행한다.

ABSTRACT

To manage software safely, the military acquires and manages products in accordance with the RMF A&A. RMF A&A is standard for acquiring IT products used in the military. And it covers the requirements, acquisition through evaluation and maintenance of products. According to the RMF A&A, product development activities should reflect the risks of the military. In other words, developers have mitigated the risks through security by design and supply chain security. And they submit evidence proving that they have properly comply with RMF A&A's security requirements, and the military will evaluate the evidence to determine whether to acquire IT product. Previously, case study of RMF A&A have been already conducted. But it is difficult to apply in real-world, because it only address part of RMF A&A and detailed information is confidential. In this paper, we propose the evidence fulfilling method that can satisfy the requirements of the RMF A&A. Furthermore, we apply the proposed method to real-world drone system for verifying our method meets the RMF A&A.

Keywords: Risk Management, Risk Assessment, RMF A&A, Security by Design, Supply Chain Security

Received(05. 18. 2021), Modified(06. 29. 2021), Accepted(07. 19. 2021)

* 이 논문은 2021년도 정부(과학기술정보통신부)의 재원으로 정보통신기술평가원의 지원을 받아 수행된 연구임 (No.2018-0-00532, 고등급(EAL6 이상) 보안 마이크로커널 개발)

† 주저자, cks4386@korea.ac.kr
‡ 교신저자, skim71@korea.ac.kr(Corresponding author)

I. 서 론

소프트웨어와 하드웨어를 포함하는 IT 제품의 복잡성이 증가함에 따라 IT 제품 내 결함 및 취약점이 증가하여 이로 인한 사이버 보안 위협 또한 증가하고 있다. 군에선 이러한 사이버 보안 위협으로부터 군에서 사용되는 무기체계를 비롯하여 다양한 IT 제품을 보호하기 위해 노력한다[1]. 이러한 노력의 일환으로 미국의 군 조직은 무기체계에 대해 지속적으로 위험을 관리하기 위해 RMF A&A 표준을 따른다. 기존 2000년도 초반까지는 미군에서만 RMF A&A 표준을 준수하였지만 2019년에 F-35 전투기를 운용하는 동맹국들에게도 미군과 같은 수준의 RMF A&A를 준수할 것을 요구하였다. 이에 따라 미국의 동맹국인 대한민국의 국군(이하 군 또는 군 조직)의 경우에도 RMF A&A 표준에 따라 IT 제품을 평가하고 획득해야한다. RMF A&A는 군에서 사용되는 IT 제품 및 통신 기능이 포함된 무기체계에 탑재되는 시스템 획득에 관한 표준이다. 해당 표준에는 제품에 대한 요구사항 도출 방법, 요구사항에 대한 평가, 유지보수에 대한 활동이 정의되어 있다. 이에 따라 군에 제품을 판매하고자 하는 개발 업체는 RMF A&A의 평가 요구사항을 모두 만족해야한다. 이를 위해 개발 업체는 평가 제출물을 작성하고 제출해야하며, 각 평가 제출물의 내용이 실제 개발된 IT 제품에 온전히 반영되어있음을 입증하는 증거자료도 함께 군에 제출해야한다. 하지만, RMF A&A 표준에는 평가자의 입장에서 평가 활동, 평가 요구사항 등이 설명되어 있으며 실제 개발을 수행하고 평가를 받아야하는 개발 업체가 각 평가 제출물 템플릿의 세부 항목을 어떻게 작성해야 하는지에 대해선 설명되어 있지 않다. 따라서 개발 업체가 RMF A&A 평가를 받기에 적합한 평가 제출물 및 증거자료를 작성하기 위한 각 평가 제출물 템플릿의 세부 항목 작성 방안에 대한 연구가 필요하다.

기존에 수행된 군의 RMF A&A에 관련한 연구는 요구사항 도출 단계와 같은 일부분에 대해서만 다루거나[2], 평가자의 관점에서 RMF A&A의 평가 활동을 다루었다[3]. 이에 개발 업체가 군 제품을 개발 및 판매하고자 할 때 RMF A&A의 요구사항을 모두 만족하기 위해 참고할 수 있는 연구가 부족하다. 이러한 이유로 인해 기존 연구들을 활용하여 군 제품을 개발하고자 할 경우 기존 연구에서 제시한 평가 제출물 및 증거자료 이외에 추가적인 문서들을 작성해야 RMF A&A의 요구사항을 모두 만족할 수 있다. 본 논문에서는 RMF A&A의 요구사항을 모두 만족할 수 있는 평가 제출물 및 증거자료의 상세한 작성방안에 대해서 제시하고자 한다. 만약 개발 업체가 본 논문에 제안된 작성방안에 따라 평가 제출물 및 증거자료를 작성할 경우 군의 획득 평가 기준을 만족시킬 수 있을 것으로 기대된다. 다음 Fig. 1은 본 논문의 주요 연구 범위를 보여준다.

본 논문에서 제안하는 RMF A&A 평가 제출물 및 증거자료 작성방안을 활용할 경우 다음과 같은 이점을 얻을 수 있다. 첫 번째로, 개발 업체의 입장에서 활용할 수 있는 평가 제출물 및 증거자료의 상세한 작성 방안을 제시한다. RMF A&A 획득 프로세스에서 개발 업체가 제출하도록 요구되는 평가 제출물의 목록을 식별한 후 각 평가 제출물의 템플릿을 수집한다. 이때 평가 제출물 템플릿을 상세한 목차 단위로 파악한 후 기존의 소프트웨어 개발 생명주기 동안 도출되는 개발 산출물 중 평가 제출물 작성에 활용할 수 있는 부분과 기존 개발 산출물로 작성되기에 부족한 평가 제출물 내 세부항목을 구분한다. 이후 부족한 부분을 채우기 위해 어떠한 타 인증 및 평가 표준을 활용할 수 있는지 분석하는 것으로 전체 평가 제출물을 작성할 수 있는 작성 방안을 제시한다. 두 번째로, 실증을 통해 제시된 평가 제출물 및 증거자료 작성방안의 유효성을 검증한다. 본 논문에서 수집한 평가 제출물 및 증거자료 템플릿과 도출한 평가 제출물 작성 방안을 고신뢰 수준의 드론 시스템 개발에 적용한다. 이처럼 직접 해당 평가 제출물 및 증거자료를 직접 작성해보는 과정을 통해 개발자 입장에서 제안된 평가 제출물 및 증거자료 작성방안을 용이하게 활용할 수 있는지 그리고 제안된 작성방안이 RMF A&A 평가 요구사항을 모두 만족하는지 실증한다. 위와 같은 연구들을 수행하는 것으로 본 연구에서는 개발 업체가 용이하게 평가 제출물 및 증거자료를 작성하고 RMF A&A를 만족할 수 있도록 각 평가 제출물 및 증거자료 템플릿 내 항목을 작성할 때 참조할 수 있는 문서 목록을 제시한다.

본 논문은 다음과 같이 구성되어있다. 먼저 본 1장에선 논문의 개요 및 주요 아이디어와 기여에 대해 설명한다. 2장에선 본 연구를 위해 조사한 관련연구들을 설명한다. 이후 3장에선 RMF A&A에 따라 수집한 평가 제출물 및 증거자료의 목록과 각 문서의 템플릿 대해 설명한다. 4장에선 3장에서 수집한 템플릿을 바탕으로 실제 드론용 보안마이크로커널에 대

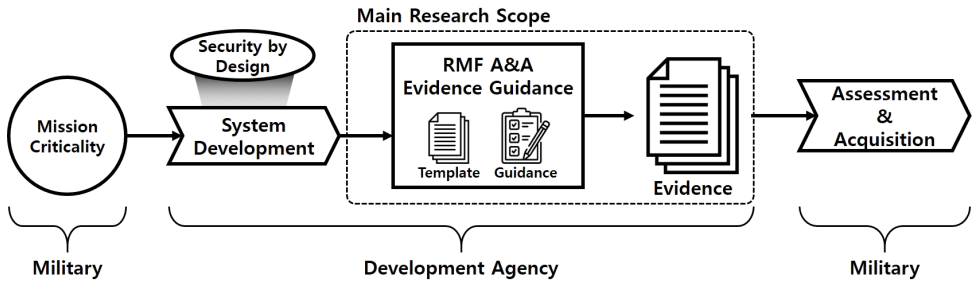

Fig. 1. Main Research Scope

한 RMF A&A의 평가 제출물 및 증거자료를 작성하고, 각 템플릿을 작성하는데 활용될 수 있는 상세한 작성지침을 제시한다. 또한, 제안된 작성방안을 RMF A&A의 요구사항과 비교하여 제안한 방법론의 타당성을 검증한다. 이때, 3장과 4장에서 실제 작성된 문서의 예시 및 상세 설명은 공간상 제약으로 생략하였다. 이에 본 내용에 대한 상세 설명 및 예시는 다음 홈페이지*를 참조하길 바란다. 마지막 5장에선 본 논문의 결론을 짓는다.

II. 관련 연구

2장에서는 본 연구를 진행하는 과정 중 분석한 표준, 논문, 특허에 대해서 설명한다. 앞서 언급한 바와 같이 안전하게 시스템을 개발하고 획득하기 위해 RMF A&A의 중요성은 계속해서 증가하고 있다. 하지만 국내의 경우 이러한 RMF A&A 평가를 받기위해 실제로 평가 제출물을 작성하기 위한 기술에 대한 연구가 많이 부족하게 수행되었다. 본 연구에선 개발 업체가 RMF A&A 평가 제출물을 실제로 작성하는데 어려움이 없도록 기존 RMF A&A 관련 연구의 문제점을 파악하고 RMF A&A 평가 요구사항을 모두 만족할 수 있는 평가 제출물 및 증거자료 작성방안에 대해 제안하고자 한다.

2.1 관련 표준

개발사는 RMF A&A에 따라 구매자에게 제품을 판매하고자 할 경우, 개발된 제품이 RMF A&A의 요구사항을 잘 만족하고 있음을 판매자가 구매자에게 납득시켜야한다. 즉, 제품을 판매하고자 하는 개발업체는 구축된 소프트웨어 개발 프로세스가 임무 위험도를 충분히 완화하고 있음을 증명하는 증거자료를 제출해야한다. 이에 본 절에서는 군의 RMF A&A 표준과 위험도 측정 기준을 다루는 표준들에 대해 분석한다. 먼저 분석할 표준은 미국의 Department of Defense(이하 DoD)에서 따르는 RMF A&A 표준이다. 2013년 미국의 DoD는 IT 제품의 획득 프로세스인 RMF A&A가 제안되었고, 이를 2014년부터 실질적으로 무기체계 획득 프로세스에 적용하기 시작하였다. 이러한 RMF A&A의 가장 큰 특징은 위험도를 기반으로 제품을 획득하기 위한 요구사항을 도출한다는 점이다. 이전에 DoD가 따르던 인증·인가 프로세스인 DIACAP(DoD Information Assurance Certification & Accreditation Process)[4]에서 현재의 RMF A&A로의 전환에 따라 발생된 가장 큰 변화는 군 무기체계에 대해 기존의 정보보증(Information Assurance)에서 더 나아가 사이버보안을 요구하는 점, System Development Life Cycle(이하 SDLC) 프로세스와 Risk Management Framework(이하 RMF) 프로세스를 서로 강하게 결합하여 개발활동과 보안활동이 상호 보완되면서 병행되기를 요구한다는 점이다. 이러한 변화에 맞춰 자연스럽게 시험평가획득 프로세스 및 SDLC 프로세스의 모든 활동들이 RMF 프로세스의 가장 처음단계인 위험도 분석을 시작으로 수행된다. 이러한 RMF A&A 표준에 따르면 제품 개발을 위한 SDLC에 ▲위험도 분석, ▲보안통제항목 선정, ▲보안통제항목 구현, ▲구현된 보안통제항목 평가, ▲시스템 인가, ▲모니터링에 6가지 보안활동이 포함되어야 한다. 하지만 해당 RMF A&A 표준의 경우 개발 업체의 입장에서 평가 제출물의 각 세부항목을 작성하기 위해 필요한 가이드라인을 제공

* https://library.korea.ac.kr에서 "무기체계 개발을 위한 RMF A&A의 실증에 관한 연구"를 검색하여 열람할 수 있음

하지 않는다. 이에 개발 업체가 RMF A&A 평가 제출물을 작성하고자 할 때 어떠한 내용을 작성해야 하는지 명확히 알 수 없는 문제점이 존재한다.

이러한 RMF 프로세스의 6가지 주요 보안활동에 맞춰 시험평가획득 프로세스의 활동들이 조정되며, 관련 산출물 및 증거자료들이 도출된다. RMF A&A는 이러한 산출물 및 증거자료를 통해 개발 업체가 RMF 프로세스에 맞게 IT 제품을 개발하였고, 제품의 위험도를 허용 가능한 수준까지 완화시켰음을 평가한 후 획득한다.

다음으로 분석할 표준은 위험도 측정 관련 표준이다. RMF A&A 표준 DoDI 8510.01(RMF for DoD IT)이 따르고 있는 위험 평가 표준인 NIST SP 800-30을 시작으로 MAGERIT, TARA(Threat Assessment and Remediation Analysis) 등과 같은 다양한 위험측정 방법론 표준에 대해서 분석하여 본 연구에서 고려하려한다.

NIST(National Institute for Standards and Technology)는 2004년에 정보 시스템 또는 정보에 대한 보안 카테고리 표준인 FIPS(Federal Information Processing Standards)-199를 제정하였다[5]. 이는 정보 시스템 또는 정보가 공격당했을 경우 기밀성, 무결성, 가용성 세 가지의 보안적인 측면에서 발생하는 피해 수준을 측정하기 위한 표준이다. 이후 위험 측정 가이드라인인 NIST SP(Special Publication) 800-30 표준을 제정하였다[6]. 이는 공격이 발생할 확률과 해당 공격이 악영향을 미칠 확률을 합쳐 종합 위협 발생 가능성을 도출하고, FIPS-199에 따라 측정한 공격 영향력과 종합하여 해당 정보 시스템의 최종 위험도를 측정하기 위한 가이드라인이다. 해당 표준을 기반으로 다양한 조직들에서 위험 평가 가이드라인들을 개발하였다.

스페인 정부는 분석가의 역량에 따라 위험 분석 수행 결과가 상이하게 도출되는 것을 완화시키기 위해 MAGERIT이라는 정형화된 위험 분석 방법론을 표준으로 제정하였다[7]. 조직의 보안팀은 MAGERIT을 이용하여 정보 시스템에 대한 잠재적인 위협을 모두 도출하고 현재 시스템에 구현되어 있는 완화방안에 따라 이미 완화된 잠재적 위협들을 필터링하여 실제 위협을 도출할 수 있다. 또한 MAGERIT은 각 위협에 대한 위험도를 평가하는 기준을 상세히 제공하여 분석가의 역량에 따른 분석 결과의 간극을 감소시켰다.

미국의 비영리단체 MITRE에서는 위협 분석 및 위험 측정 표준으로 TARA(Threat Assessment and Remediation Analysis)를 제정하였다[8]. TARA는 사이버시스템의 취약점 식별 및 위험도 측정과 이에 대한 효과적인 완화방안을 선택하기 위한 공학 기법이다. TARA의 경우 고신뢰가 요구되는 시스템 중 하나인 차량에 대한 위협 및 위험도 분석 시 활용되는 방법론이다. 이는 위험도 분석에 있어서 시스템 사용자의 능력에 해당되는 제어능력(Controllability)을 고려한다. 자동차를 개발하는 업체에선 먼저 HARA(Hazard Analysis and Risk Assessment)방법론을 통해 의도치 않은 결함에 대한 위험도를 분석한다. 이후 TARA 방법론을 통해 악의적 공격자에 의한 의도적 결함에 대해 분석한다. 자동차에서 위험은 궁극적으로 탑승자의 생명을 위협할 수 있는 자동차의 잘못된 제어로 이어지기에 이렇게 자동차가 잘못 운행될 수 있는 결함에 대해서 HARA를 통해 식별한 후 TARA를 통해 HARA에서 식별된 결함을 공격자가 임의로 일으킬 수 있는 시나리오를 도출하는 것이다. 이에 따라 분석된 악성 시나리오는 모두 HARA에서 분석된 의도치 않은 결함과 매핑되어야한다. 이러한 TARA 위협 분석 방법론은 시스템에 대한 위협을 도출하고 각 위협에 대해 영향력, 난이도 등의 12개의 기준을 통해 위험도 점수를 산정한다.

위에서 설명한 표준 이외에도 Microsoft의 DREAD(Damage, Reproducibility, Exploitability, Affected users, Discoverability)와 같이 산업에서 널리 사용되는 위험도 측정 방법론들이 존재한다. 위에서 언급한 바와 같이 현재 발표된 RMF A&A 표준의 경우 개발 업체가 평가 제출물을 작성하기 위해 필요한 세부 작성 지침을 제공하지 않는다. 본 논문에서는 이러한 문제를 해결하기 위해 위험도 및 보안성 관련 표준 및 방법론을 분석하고, 이를 바탕으로 RMF A&A 평가 제출물 작성방안을 도출하고자 한다.

2.2 관련 논문

본 절에서는 안전한 소프트웨어 개발 방법론에 대해 연구한 기존 논문들을 분석하고, RMF A&A 평가 요구사항을 만족하기에 부족한 점을 언급한다. 관련 논문 분석의 경우 본 논문의 핵심 키워드인 “RMF A&A”, “Risk Management”, “Security

by Design" 중 하나를 포함하고, 오래되어 더 이상 현재의 시스템에 적용하기 어려운 연구를 제외하기 위해 최근 5년 내에 수행된 논문을 중심적으로 조사하였다. 이때 대상 저널의 경우 IT와 관련하여 대표적으로 알려진 IEEE, Elsevier, Springer, ACM을 중점적으로 조사하였다. 조사 결과 중복되는 논문, 관련성이 떨어지는 연구 제거 등의 필터링 과정을 거쳐 최종적으로 60건의 논문을 선정하였고 개요, 서론을 분석하여 해당 논문들이 어떠한 안전한 소프트웨어 개발 방안을 제안하고 있는지 파악하였다. 분석 결과 전체 60건의 논문은 안전한 소프트웨어 개발을 중심으로 다음 Fig. 2와 같이 ▲국내 무기체계에 RMF A&A를 적용시키고자 하는 논문[2,3], ▲SDLC의 효율을 향상시키고자 하는 논문[9-16], ▲소프트웨어의 보안 수준을 평가하고자 하는 논문[17-32], ▲SDLC 각 단계에 대한 보안성을 향상시키고자 하는 논문[33-56], ▲SDLC의 각 단계별 지원도구를 개발한 논문[57-69]의 총 5가지로 분류된다.

이렇게 나눠진 5가지의 분류 중 본 논문과 가장 관련성이 깊은 분류는 "국내 무기체계에 대한 RMF A&A의 적용"이다. 해당 분류에 속하는 2건의 논문을 상세히 분석한 결과 첫 번째 [3]논문은 국군의 무기체계 획득 프로세스와 미국 DoD의 RMF A&A 시험평가체계를 비교분석하여 RMF A&A에 비해 부족한 평가활동을 보완하는 논문이었다. 두 번째 [2]논문은 실제로 RMF A&A의 시험평가를 통과하기 위해 개발사가 수행해야하는 활동 및 산출물에 대한 실 적용사례를 연구하였으나, 전체 산출물이 아닌 요구사항 분석, 설계단계에 해당하는 산출물에 대해서만 연구되었다. 이에 개발 업체가 RMF A&A 시험 평가를 완전히 통과할 수 있는 산출물을 모두 다루고 있는 연구는 기존에 수행되지 않았음을 알 수 있다.

본 논문과 직접적인 관련은 없지만 RMF A&A의 궁극적인 목적은 소프트웨어를 안전하게 개발하고 획득하는 것이므로 안전한 소프트웨어 개발 방안에 관련한 연구도 분석을 수행하였다. 이에 관해 CC(Common Criteria)[70], ISMS(Information Security Management System), 등의 표준에 기반하여 요구사항 단계부터 보안측면을 고려하는 SDLC인 Secure SDLC를 자동으로 구축해주는 프레임워크에 대한 연구가 수행되었다[61]. 해당 연구의 프레임워크는 업체가 개발하고자 하는 소프트웨어의 보안보증수준을 정량적으로 제시하면 이를 만족할 수 있는 요구사항들과 보안활동, 산출물 템플릿을 도출해준다. 하지만, 해당 연구에서 도출된 산출물 템플릿에 따라 개발 산출물을 작성하고 군에 제출할 경우 RMF A&A의 요구사항을 충분히 만족하지 못하기에 시험평가를 통과하지 못한다. 예를 들어 RMF A&A의 Security Plan(이하 SP) 산출물에서는 군에서 제시한 임무의 위험도, 위험도에 기반한 최소 보안통제항목 목록 등이 포함될 것을 요구한다. 하지만 CC의 증거 제출물 중 해당 문서와 가장 유사한 Security Target(이하 ST) 문서에는 임무 위험도 평가, 최소 보안통제항목 목록과 같은 항목들이 포함되지 않기에 RMF A&A의 평가자가 해당 문서를 전달받는다 하여도 올바른 평가를 수행할 수 없다.

Fig. 2. Categorization of Related Work

이러한 관련 연구들에 대한 분석 결과로 미루어 볼 때 RMF A&A의 모든 평가 요구사항을 모두 만족할 수 있는 산출물 작성방안에 관한 연구는 수행되지 않았다. 이에 기존 연구를 활용하여 RMF A&A 평가를 받고자 할 경우 개발 업체는 충분한 정보를 제공받지 못한다는 단점이 있다. 하지만, 본 논문에서는 기존의 연구들과 다르게 RMF A&A의 평가 요구사항을 모두 만족할 수 있는 평가 제출물 작성방안을 제시한다. 이에 RMF A&A 평가를 받고자 하는 개발 업체가 본 논문을 참고할 경우 충분한 정보를 제공받아 적절한 평가 제출물을 작성할 수 있다는 장점이 있다.

III. 개발 업체와 관련된 RMF A&A 평가 제출물

본 장에선 군의 RMF A&A에서 개발 업체에게 작성 및 보조하도록 요구되는 평가 제출물을 식별한다. 앞서 언급한 바와 같이 기존의 안전한 소프트웨어 개발 방안 및 RMF A&A 실증에 대한 연구들은 RMF A&A의 평가 요구사항을 모두 만족하지 못한

다. 또한, 앞서 설명한 바와 같이 RMF A&A 표준에는 개발 업체가 평가 제출물을 준비하는데 필요한 상세 정보가 제공되지 않는다. AcqNotes와 같은 RMF A&A 관련 사이트에선 각 평가 제출물 문서에 대한 개요와 대략적인 목차는 제공하지만 세부 목차를 작성하기 위해 활용될 수 있는 충분한 정보를 제공하고 있지 않다. 이에 본 장에서는 실질적인 평가 제출물 작성방안을 제안하기 이전에 필요한 평가 제출물의 목록과 각 문서의 템플릿을 수집한 내용에 대해 설명한다. 이때, 먼저 AcqNotes와 같은 RMF A&A관련 사이트에서 템플릿을 수집하고, 충분한 정보가 제공되지 않는 문서 템플릿의 경우 공개된 DoD 공식 문서를 우선적으로 수집하여 각 문서의 세부목차에 대한 상세 설명을 작성하였다. DoD 공식 문서에서 다루어지지 않거나 공개된 문서가 없는 경우 타 기관들(FedRAMP, NIST, Homeland Security 등)에서 공개된 문헌들을 통해 상세 설명을 작성하였다. 이러한 과정을 통해 식별한 RMF A&A의 획득평가 프로세스에서 생성되는 전체 평가 제출물 문서는 ATO, CDD, CMS, CSS, DT&E Report, ICD, LCSP, POA&M, PPP, RAR, SAP, SAR, SP, TEMP, RFP에 총 15건이 존재한다.

이 중 RMF A&A 표준에 따르면 개발 업체가 직접 작성하거나 타 기관이 작성하는데 보조해야하는

Table 1. Description of each Potential Impact Level

Impact Level	Description
High (H)	The loss of confidentiality, integrity or availability could be expected to have a **severe or catastrophic adverse effect** on organizational operations, assets, or individuals
Moderate (M)	The loss of confidentiality, integrity or availability could be expected to have a **serious adverse effect** on organizational operations, assets, or individuals
Low (L)	The loss of confidentiality, integrity or availability could be expected to have a **limited adverse effect** on organizational operations, assets, or individuals

평가 제출물 및 증거자료는 총 8건이다. 첫 번째 문서는 SP이다. 해당 문서는 개발 프로젝트의 착수 및 계획 단계에서 처음 생성되어 개발 진행 중에 지속적으로 업데이트되어야 하는 문서이다. 해당 문서에서 주요하게 식별되고 작성되어야 하는 부분은 임무 위험도가 반영된 시스템 위험도 측정과 최소 보안 요구사항인 최소 보안통제항목의 식별이다. 이 중 시스템 위험도 측정(System Categorization)의 경우 CNSSI 1253 표준[71] 및 NIST SP 800-60 표준[72]을 참조하여 수행할 수 있다. 시스템의 위험도는 3가지의 보안 목적(Confidentiality, Integrity, Availability)에 대해 각각 High, Moderate, Low 3가지 수준 중 하나로 평가되도록 요구된다. 시스템 내에서 처리, 저장, 송수신되는 데이터 각각에 대해 위험도 평가가 수행되어야 하며 전체 평가결과를 하나로 종합하여 최종적인 시스템 위험도가 도출된다. 각 위험도 수준에 대한 판단 근거는 NIST SP 800-60에 다음 Table 1과 같이 정의되어 있다.

다음으로 SP 문서에서 중요한 항목인 최소 보안통제항목의 경우 먼저 시스템 위험도가 도출되면 DoDI-8510.01 표준 문서에서 제시되고 있는 위험도별 보안통제항목을 기입하면 된다. 이러한 RMF A&A 표준의 보안통제항목은 연방정부의 CNSSI 1253, NIST SP 800-53[73]을 기반으로 도출되어있다. 하지만, 연방정부 표준에서 설명되고 있는 보안통제항목 이외에 군에서 추가로 도출한 보안통제항목의 경우 외부에 공개되지 않기에 본 연구에서 다루지 못하였다. 이처럼 RMF A&A의 보안통제항목이 연방정부 표준을 기반으로 도출된 이유는 DIACAP에서 RMF A&A로 대체됨에 따라 타 정부 기관과의 통일성과 원활한 의사소통, 타 기관에서 평가받은 제품에 대한 평가결과의 재사용 등을 위해 통일시켰기 때문이다.

DoDI 8510.01에서 제시하는 전체 보안통제항목 목록은 총 617건의 항목으로 구성되어있다. 하지만 이를 모두 필수로 적용해야 하는 것은 아니며 위험도 수준에 따라 필수적으로 적용되어야 하는 최소 보안통제항목이 지정되어있다. 전체를 종합해본 결과 L(Low) 위험도를 갖는 시스템은 총 96건, M(Moderate) 위험도를 가질 경우 총 152건, H(High) 위험도를 가질 경우 총 157건의 최소 보안통제항목을 필수적으로 구현해야 한다. 이외의 보안통제항목에 대해선 선택적으로 구현 가능하다.

Table 2. Contents of SP

Chapter	Title
1	Information System Name
2	Information System Categorization
3	Information System Owner
4	Authorizing Official
5	Other Designated Contacts
6	Assigned of Security Responsibility
7	Information System Operation Status
8	Information System Type
9	General System Description
10	System Environment
11	System Interconnections
12	Related Laws/Regulations/Policies
13	Minimum Security Controls
14	Information System Security Plan Completion Date
15	Information System Security Plan Approval Date

위험도 평가와 최소 보안통제항목 이외의 부분에 대해선 일반적으로 시스템 개발 프로젝트 계획 수립 시 결정될 수 있는 사항으로 자연스럽게 채워질 수 있는 항목들로 구성되어있다. 이러한 SP 문서의 전체 목차는 다음 Table 2와 같다.

개발 업체가 필수적으로 작성해야 하는 두 번째 문서는 SAP 문서이다. 해당 문서의 경우 개발된 제품에 대해 보안 취약점을 테스트하기 위한 계획을 담은 문서로 테스트 일정, 테스트에 활용할 도구, 테스트 프로세스, 가정사항, 제약사항 등에 대해 기술한다. 해당 문서의 경우 개발 업체가 일반적으로 구축 및 준수해야 하는 SDLC에서도 작성된다. 이에 기존의 문서를 동일하게 작성하여 제출하면 된다. SAP 문서에 이어서 취약점 평가 결과에 대해 작성하는 SAR 문서도 개발 업체가 작성해야 한다. 해당 문서는 실제 테스트 기간, 테스트에 사용된 도구, 계획대비 변경된 사항, 취약점 테스트에서 활용된 시스템 내 공격표면, 발견된 취약점 등에 대해서 기술한다. 해당 SAR 문서 또한 SAP 문서와 동일하게 일반적인 SDLC에서도 작성되는 문서이기에 자연스럽게 RMF A&A 제출물로 활용이 가능하다. 다음 Table 3, Table 4는 SAP, SAR 문서에 대한 목차를 보여준다.

다음으로 개발 업체가 도출해야하는 문서는 Security Requirements and Design Specification(이하 SRDS) 문서이다. SRDS 문서의 경우 시스템 내 구현된 인터페이스, 서브 시스템, 모듈, 시스템 내 구성요소와 보안 요구사항의 매핑 등에 대해 기술한다. 개발 업체는 해당 문서를 통해 SP 문서에 기재된 보안통제항목이 모두 보안 요구사항으로 변환이 되었고, 시스템 설계에 해당 보안

Table 3. Contents of SAP

Chapter		Title
1		Introduction
	1.1	Scope
	1.2	Assumption/Limitation
2		Assessment Tools
3		Scanning Authorization
4		Team Composition
5		Schedule
6		Security Assessment Procedures
	6.1	Process Overview
	6.2	Test Procedures
	6.3	Component Identification
	6.4	Automated Scans
	6.5	Requirements Traceability Matrix
	6.6	Results Documentation
7		Acronyms

Table 4. Contents of SAR

Chapter		Title
1		Introduction and Purpose
	1.1	Applicable Laws and Regulations
	1.2	Applicable Standards and Guidance
	1.3	Purpose
	1.4	Scope
2		System Overview
	2.1	Security Categorization
	2.2	System Description
	2.3	Purpose of System
3		Scanning Authorization
	3.1	Perform Tests
	3.2	Identification of Vulnerabilities
	3.3	Consideration of Threats
	3.4	Perform Risk Analysis
	3.5	Recommend Corrective Actions
	3.6	Document Results
4		Risk Exposure Table
	4.1	Security Assessment Summary
5		Non-Conforming Controls
	5.1	Risks Corrected During Testing
	5.2	Risks with Mitigating Factors
	5.3	Risks Remaining Due to Operational Requirements
6		Risks Known for Interconnected Systems
7		Authorization Recommendation

요구사항이 반영되었음을 보여야한다. SRDS 문서에서 가장 주요하게 작성되어야 하는 부분은 시스템 구성요소와 보안 요구사항의 매핑 내용이다. 해당 내용을 통해 SP의 보안통제항목이 모두 시스템 설계에 반영되어 구축되었음을 보이고 평가되어야한다. 다음 Table 5는 SRDS 문서의 목차에 대해 보여준다.

Table 5. Contents of SRDS

Chapter	Title
1	Introduction
1.1	Purpose
1.2	Scope
1.3	Definitions and Acronyms
2	Sub-systems
2.x	Sub-system A
2.x.x	Crypto Module
2.x	Mapping of Sub-systems and Security Objectives
3	Interfaces
3.x	Sub-system A
3.x.x	CLI:Sys_login
3.x.x	CLI:Sys_set_crypto_mode
3.x	Sub-system B
3.x.x	CLI:Interface B
3.x	Mapping of Sub-system and Security Functional Requirements
3.x	Mapping of Sub-system and Interface

마지막으로 개발 업체가 작성하여 제출해야 하는 문서는 POA&M 문서이다. POA&M 문서의 경우 개발 과정 중 또는 개발된 제품에 대한 취약점 평가 과정 중 추가적으로 식별된 취약점 또는 결함에 대한 수정 계획을 기술한 문서이다. 해당 문서는 각 수정 계획의 식별자, 해당 취약점의 대상 자산, 수정 계획의 상세한 일자, 결함 수정 시 참고할 수 있는 외부 문서, 결함 수정 이전에 평가된 시스템 위험도와 결함 수정 이후 재평가된 시스템 위험도, 각 수정 계획에 대한 책임자에 대한 연락처 등에 대해 기술한다. POA&M 문서는 기존 Secure SDLC의 산출물 중 결함수정 계획 또는 유지보수 계획 문서와 유사한 부분이 존재하나 시스템 위험도 측정의 경우 CNSSI 1253, NIST SP 800-60에 기반한 평가를 수행한 후 그 결과를 작성해야한다. 다음 Table 6은 POA&M 문서의 목차를 보여준다.

이러한 문서 이외에 개발업체는 RFP, PPP, System Engineering Plan(이하 SEP)문서 작성에 관여해야한다. RFP 문서의 경우 시스템에 대한 설명, 최소 요구사항과 같은 내용에 대해 군에 자문을 주어야 한다. 하지만 RFP 문서 작성 시기에는 계약된 개발 업체가 없기에 전체 개발 업체에게 자문을 요청해 특정 업체만 기회를 얻을 수 없도록 유의해야한다. 다음으로 PPP 문서의 경우 군에서 개발된 시스템을 올바르게 운영할 수 있도록 관리자를 위한 운영 가이드라인, 운영 환경에서 발생할 수 있는 취약점, 취약점에 대한 공격이 발생할 시 시스템 운영자가 취해야 할 행동(완화방안) 등에 대해 지속적으로 군에게 전달해야 한다. 마지막으로 SEP 문서의 경우 개발 업체가 개발하고자 하는 소프트웨어의 구성요소를 식별하여 전달해야한다. 또한 해당 문서가 개발된 이후 개발 업체는 자신이 작성한 SP, SAP 문서와 상이하게 작성된 부분이 없는지 모니터링해야 하며, 만약 상이한 부분이 발견될 경우 군 또는 관련 이해관계자와 커뮤니케이션을 통해 동기화해야한다. 또한, 개발 업체는 지정된 문서 이외에 필요시 증거자료로 System Requirements Specification(이하 SRS), System Design Specification(이하 SDS), Source Code 등과 같은 자료를 함께 제출해야한다.

Table 6. Contents of POA&M

Chapter	Title
A	POA&M ID
B	Security Control IDs
C~F	Weakness Information
G	Asset ID
H	Point of Contact
I	Overall Remediation Plan
J	Original Detection Date
K	Scheduled Completion Date
L	Planned Milestones
M	Milestone Changes
N	Status Date
O	Vendor Dependency
P	Last Vendor Check-in Date
Q	Vendor Dependent Product Name
R	Original Risk Rating
S	Adjusted Risk Rating
T	Risk Adjustment
U	False Positive
V	Operational Requirement
W	Devation Rationale
X	Supporting Documents
Y	Comments
Z	Auto-Approve

본 3장에서는 RMF A&A에서 개발 업체에게 작성하거나 타 기관이 작성하는데 보조할 수 있도록 요구하는 평가 제출물을 식별하고 각 문서에 대한 템플릿을 수집하였다. 본 장에서 수집한 템플릿에 따라 평가 제출물을 작성할 경우 군이 제품 평가를 수행하는데 필요한 정보를 충분히 제공할 수 있을 것으로 사료된다. 이후 4장에서는 실제로 각 평가 제출물을 템플릿에 따라 작성해보면서 개발 업체가 평가 제출물을 작성하기 위한 작성방안을 제안하고자 한다. 또한, 제안된 작성방안이 RMF A&A의 평가 요구사항을 모두 만족하고 있는지 검증하여 타당성을 입증하고자 한다.

IV. ChibiOS를 대상으로 한 RMF A&A 제출물 및 증거물 작성 실증

본 장에서는 앞서 제안한 제출물 및 증거자료 템플릿에 따라 실제 드론에 탑재되는 커널에 대한 평가 제출물을 작성한다. 이후 작성과정에서 참조한 표준과 각 문서의 세부항목을 매핑하여 개발 업체를 위한 상세한 작성방안을 보여주고, 최종적으로 실제로 작성한 평가 제출물이 RMF A&A의 평가 요구사항을 모두 만족한다는 실증 결과를 보여준다. 실증 대상은 드론 시스템에 탑재되는 마이크로커널인 ChibiOS이다. 기존에 보안 기능이 탑재되어있지 않은 일반 마이크로커널을 기반으로 CC 고등급(EAL 6, 7)의 고신뢰 보안 마이크로커널을 개발하고자한다. 본 연구에서는 이러한 고신뢰 보안마이크로커널의 개발 과정에서 작성된 CC 평가 제출물과 기타 개발 산출물, 증거자료를 기반으로 평가 제출물 및 증거자료 작성 방안을 실증한다.

3장에서 설명한 바와 같이 개발 업체는 총 8건의 문서에 대해 직접 작성 또는 타 참여자가 올바르게 작성할 수 있도록 보조해야한다. 본 논문의 저자는 평가 제출물을 직접 작성하며 기존 개발 산출물로 대체 가능한 부분과 타 표준 문서들을 참고하여 새롭게 작성해야 하는 부분을 식별하였다. 최종적으로, 평가 제출물의 각 항목들과 참고 될 수 있는 자료의 항목을 매핑하여 개발 업체가 문서를 용이하게 작성할 수 있게 제시한다. 이렇게 제시된 매핑 결과를 참조하여 평가 제출물 및 증거자료를 작성하는 것으로 개발 업체는 RMF A&A 평가 요구사항을 모두 만족할 수 있다. 이후 부분에서는 본 저자가 RMF A&A 평가 제출물의 목록에 따라 각 문서의 템플릿을 작성한 결과 도출한 상세 작성 방안을 설명한다.

4.1 평가 제출물 작성

RMF A&A에서 평가 제출물 작성 시 가장 주요하게 고려되어야 하는 사항 중 하나는 개발될 IT 제품 또는 무기체계의 위험도이다. 본 연구에선 이러한 중요성을 충족시키기 위해 연방정부의 FIPS 199, NIST SP 800-64 표준과 DoD의 PM's Guidebook을 참고하여 위험도를 측정한다. 해당 표준 및 지침에 따르면 위험도는 해당 시스템이 투입될 임무의 위험도, 시스템 내 데이터의 중요도에 2가지 관점에서 평가되어야한다. 실증 대상인 드론 시스템은 정찰 임무를 목적으로 설계되었으며, 실제 목표 타격 임무 및 적을 사살하는 킬체인(Kill Chain)임무는 수행되지 않는다. 이에 따라 시스템 내 처리되는 데이터는 센서 데이터, 위치 데이터, 자세제어 데이터에 3가지로 식별하였다. 이처럼 드론 시스템 내부에서 처리되는 데이터와 시스템이 투입될 임무의 위험도를 고려하여 드론 시스템의 종합 위험도는 다음 수식과 같이 도출되었다.

$$SC_{Drone.m} = (C\colon High, I\colon High, A\colon Moderate) = High$$

위험도 측정 이후 해당 위험도를 기반으로 SP를 비롯하여 개발사가 작성해야 하는 문서들을 직접 작성하였다. 먼저 SP 문서의 경우 개발업체는 군으로부터 제시받은 임무위험도와 개발하고자 하는 시스템에서 저장, 처리, 송수신되는 데이터를 고려하여 종합 위험도를 도출해야 한다. 위험도 도출의 경우 본 장의 앞부분에서 설명한 바와 같이 수행되었고, 도출된 위험도를 바탕으로 SP에 기재되어야 하는 가장 중요한 항목 중 하나인 최소 보안통제항목 목록을 도출하였다. 이때 이전에 언급한 바와 같이 NIST SP 800-53 문서에서 제공되는 위험도별 최소 보안통제 항목 목록을 활용하여 작성하였다. 해당 부분 이외에 SP 문서에 기재될 항목들은 시스템 사양, 보안 책임자의 인적사항, 보안 계획의 승인 및 완료 일정과 같은 항목들이 존재한다. 해당 항목들은 개발 업체가 일반적으로 작성하는 시스템 개발 계획 문서 또는 CC 평가의 ST 문서 내용 중 TOE(Target of Evaluation) 설명 내용을 참고하여 작성될 수 있다.

다음으로 개발업체가 작성해야 할 SAP 문서의 경우 정보 시스템에 대한 취약점 분석 시 제약/가정

사항, 사용하고자 하는 도구, 분석 프로세스 등에 대해 기술하는 문서이다. 해당 문서의 경우 개발 업체가 RMF A&A 평가를 받기위해 일반적인 개발 프로세스의 “평가 단계” 또는 “테스트 단계”에서 작성되는 테스트 계획 문서를 참고하여 작성할 수 있다. 해당 문서에서 가장 주요하게 작성되어야 하는 항목은 제약/가정사항 항목과 평가 프로세스 항목이다. 먼저 제약/가정사항 항목의 경우 취약점 분석 시 필히 고려되어야 하는 시스템 접근에 대한 제약사항과 공격자의 능력과 같은 가정사항을 설명하는 부분으로 CC의 ST에 기재된 가정사항 항목을 참고하여 작성될 수 있다. 다음으로 평가 프로세스 항목의 경우 보안팀이 수행할 취약점 분석 활동의 상세한 과정에 대해서 기술하는 항목이다. 개발 업체는 해당 항목에 대해 다양한 취약점 분석 방법론들인 위협 모델링, 침투 테스트 등을 참고하여 작성하면 된다.

다음으로 개발업체가 작성해야 할 SAR 문서의 경우 수행된 취약점 분석 결과에 대해 기술하는 문서이다. 해당 문서에는 SAP에서 계획한 사항들이 모두 수행되었는지, 계획에서 변경된 사항이 있는지, 취약점 분석 수행 결과 어떠한 취약점들이 시스템 내에서 식별되었는지, 식별된 취약점에 대해 권장되는 완화방안에는 어떠한 것들이 있는지 등을 기재해야 한다. SAR 문서 또한 SAP 문서와 동일하게 일반적인 소프트웨어 개발 과정의 “평가 단계” 또는 “테스트 단계”에서 도출되는 테스트 결과 문서를 참고하여 작성될 수 있다. 해당 문서에서 가장 주요하게 작성되어야 하는 항목은 식별된 취약점 정보 항목과 위험도 재평가 항목이다. 먼저 식별된 취약점 정보의 경우 취약점 분석 과정 중 확인된 취약점의 소스코드 상 발생 위치, 취약점의 상세 설명, 관련 취약점 데이터베이스 정보에 대해 기술해야 한다. 해당 항목은 위협 모델링, 침투 테스트를 통해 식별된 취약점에 대해 MITRE의 CVE(Common Vulnerabilities and Exposures), CWE(Common Weakness Enumeration) 목록과 NIST에서 제공되는 NVD(National Vulnerability Database)를 참고하여 작성될 수 있다. 취약점 정보와 더불어 SAR 문서에는 SAP 문서 대비 변경된 부분에 대해 상세히 작성되어야 한다.

마지막으로 개발업체가 직접 작성해야 할 문서는 POA&M 문서이다. 해당 문서는 취약점 분석 및 인수 테스트 등의 평가활동들을 포함한 개발 과정 중 또는 시스템 운영 중 발견된 결함, 취약점에 대해 개발 업체의 수정 계획에 대해 기술하는 문서이다. 이러한 POA&M 문서에는 항목은 결함의 식별자(ID), 해당 결함과 관련된 보안통제항목, 결함의 이름 및 요약 설명, 영향 받을 수 있는 자산 등의 정보들이 기재된다. 개발 업체는 각 결함, 취약점에 대한 요약과 관련 보안통제항목을 이전에 작성된 SAR 문서를 참고하여 작성할 수 있고, 수정 계획 일정의 경우 업체 내부의 개발팀과 지속적인 커뮤니케이션을 통해 수립해야한다. 또한, 수정 계획 일정에 변동이 있을 경우 개발 업체는 변동된 일자와 변동 사유에 대해서 상세히 기록해야한다.

위에서 언급된 4종의 문서는 개발 업체가 직접 작성하거나 군에서 작성된 초안을 기반으로 개발업체가 직접 갱신 해주어야한다. 해당 문서들 이외에 개발업체가 다른 RMF A&A 획득 프로세스 참여 역할이 작성하는데 도움을 주어야하는 문서는 총 3종 존재하며 각각 다음에 설명될 증거자료 내 항목들에 대해 관여해야한다.

먼저 개발 업체가 직접 작성에 관여하지 않지만 군에서 IT 제품을 획득하는데 자문을 주어야 하는 문서는 RFP이다. 해당 문서는 군이 직접 작성하는 문서로 잠재적 계약자인 개발 업체가 군의 요구사항 중 기능적으로 실현 가능한 부분과 운영환경에서 만족되어야 할 부분을 구분해주거나 하나의 개발 업체가 완전한 시스템을 온전히 개발하지 못할 경우 여러 개발 업체가 참여할 수 있도록 전체 시스템을 서브시스템 단위로 분할하는 부분에 대해 군에게 자문을 주어야 한다. 해당 문서의 경우 개발 업체가 문서 작성에 직접적인 관여를 하게 되면 계약에 대한 청렴도 등과 같은 문제가 발생될 수 있기에 직접적으로 관여하지 않고 군이 획득하고자 하는 IT 제품에 대해 적절한 계획을 세울 수 있도록 도움을 주어야한다. 또한 군은 아직 계약이 이루어진 개발업체가 존재하지 않은 만큼 특정 업체에게 편향되는 계약 조건 및 계획을 수립하지 않도록 유의해야한다. 즉, 실제 RFP 작성이 시작되기 전에 시스템 획득 계획 단계에서 자문을 얻을 수 있도록 해야 한다. 실제 RFP 문서의 작성 이전에 군은 시스템에 어떠한 서브 시스템들이 필요한지 분석하고 식별하는 Material Solution Analysis 활동을 수행한다. 이때 군이 전체 시스템을 분석한 결과 식별한 필요 서브 시스템, 모듈, 세부기능의 목록이 적합한지 개발 업체가 검토 후 자문을 주어야 한다. 이렇게 개발업체에게 자문을 받아 최종적으로 식별한 서브시스템, 모듈, 세부기능들을

실제로 개발하기 위해 군은 RFP 문서를 작성하고 개발 업체와 계약을 맺게 된다.

다음으로 개발 업체가 작성에 도움을 주어야 하는 문서는 SEP, PPP이다. 개발 업체는 두 문서에 대하여 직접 작성한 문서 중 하나인 SAP문서와 일치되도록 갱신해야한다. 먼저 SEP, PPP문서 내 위험 평가와 관련된 활동 내역과 설명, 일정 작성에 대해 SAP 문서와 일치될 수 있도록 도움을 주어야한다. 즉, 개발 업체는 SAP 문서에 기재된 취약점 분석 일정과 SEP 문서에 기록된 취약점 관리 일정, PPP 문서에 기록된 위험 관리 일정이 일치 할 수 있도록 군 또는 SEP, PPP 문서 작성 주체와 의사소통이 되어야한다. 또한, 취약점 관리 일정동안 개발 업체가 활용할 도구, 취약점 분석 프로세스를 포함하는 주기적 위험 관리 활동이 SEP, PPP 문서에 올바르게 기재될 수 있도록 관여해야한다.

지금까지 언급된 7종의 문서에 기재된 내용들이 실제로 개발된 시스템에 반영되었다는 사실을 증명하기 위해 개발 업체는 개발 과정 중 도출된 산출물을 추가로 군에 제출해야한다. 이 중 가장 주요하게 제출되어야 하는 문서는 SRDS로 해당 문서에 기재된 보안 요구사항과 시스템 내부 구성요소에 대한 사항을 필수 증거자료로 제출해야한다. 이러한 SRDS 문서는 시스템을 구성하는 인터페이스, 모듈에 대한 설명을 시작으로 각 구성요소와 보안 요구사항의 매핑에 대해서 기술한다. 이 중 가장 마지막에 기술되

Table 7. Mapping between RMF A&A Evaluation Documents and Other Related Standards or Development Documents

RMF A&A Evaluation Document		Other Related Standards or Documents		
Title	**Contents**	**Category**	**Title**	**Contents**
Security Plan	Minimum Security Controls	NIST	NIST SP 800-53	The Controls
		CNSSI	CNSSI 1253	Control Selection within the RMF
	Information System Categorization	FIPS	FIPS 199	Categorization of Information and Information Systems
		NIST	NIST SP 800-60	Security Categorization of Information and Information Systems
		CNSSI	CNSSI 1253	Categorizing NSI and NSS
	System Environment	CC	Security Target	Product Overview
				TOE Overview - TOE usage
				TOE Overview - Non TOE H/W and S/W
	System Interconnections / Information Sharing	Threat Modeling	Date Flow Diagram	External Objects
				Data Flow
		Software Engineering	Software Design Specification	Interaction Systems

Request For Proposal	Description / Specifications / Statement of Work	CC	Security Target	Product Overview
				TOE Overview
				TOE Description
				Security Functional Requirements
System Engineering Plan	Technical Performance Measures and Metrics	CC	TSF_INT	Minimal Complexity of TSF
	Technical Schedule and Schedule Risk Analysis	RMF A&A	Security Assessment Plan	Security Assessment Schedule
	Technical Activities and Products	NIST	NIST SP 800-53	The Controls
		CNSSI	CNSSI 1253	Control Selection within the RMF
		Software Engineering	Security Requirements and Design Specification	Sub Systems and Requirements Traceability Matrix
				Interfaces and Requirements Traceability Matrix
Program Protection Plan	Program Protection Summary	RMF A&A	Security Assessment Plan	Security Assessment Schedule
	Processes for Management and Implementation of PPP		Security Assessment Report	Security Assessment Process
	Program Protection Costs	RMF A&A	Request for Proposal	Supplies and Services and Prices/Costs
	Threat, Vulnerabilities, and Countermeasures	CC	ST	Threats
				Security Objectives
				Security Functional Requirements
				Security Assurance Requirements
		Threat Modeling	Threat Modeling Report	Threats
Security Requirements and Design Specification	Sub System and Requirements Traceability Matrix	CC	Security Target	Security Functional Requirements

				Rationale
				Security Assurance Requirements Rationale
Security Assessment Plan	All	Software Engineering	Test plan	All
		CC	AVA_VAN	Attack Scenario
Security Assessment Report	All	Software Engineering	Test Report	All
		Security Assessment	Vulnerability Analysis Report	All
		CC	AVA_VAN	Attack Scenario
Plan Of Action & Milestone	All	ENISA-Risk Management	Incident Response Plan	All
		NIST	NIST SP 800-53	The Controls
		RMF A&A	Security Plan	Minimum Security Controls
				Assignment of Security Responsibility
		CC	Security Target	Security Problem Definition - TOE Assets

는 시스템 내 각 구성요소와 보안 요구사항의 매핑 항목에서 개발 업체는 군으로부터 제시받은 위험도가 요구사항 도출, 설계 단계부터 올바르게 반영되었고 구현되었음을 증명하게 된다. 해당 항목의 경우 CC의 ST문서에 기재되어있는 보안목적에 대한 이론적 근거, 보안기능요구사항에 대한 이론적 근거 항목을 참고하여 기입할 수 있다.

SRDS 문서 이외에 상세한 설계 내용, 구현 내용을 군이 필요로 할 시 추가적으로 시스템 요구사항 문서(SRS), 설계 문서(SDS) 더 나아가서는 실제 구현된 소스 코드까지 제출할 수 있다. 해당 문서들에 대해선 일반적인 소프트웨어 공학에서 다루어지는 산출물이기에 별도로 추가 작성을 수행하지 않고 개발 업체는 군 또는 해당 문서를 필요로 하는 RMF A&A 획득 프로세스의 참여 역할에게 제출할 수 있다.

이처럼 본 장에서는 3장에서 제안된 RMF A&A 평가 제출물 및 증거자료 템플릿을 실제 드론 시스템 개발 프로젝트에 적용하여 개발 업체가 꼭 작성해야 하는 부분, 도움을 줄 수 있는 부분을 구분하였다. 또한 각 평가 제출물 및 증거자료 문서 템플릿의 세부항목을 작성하기 위해 어떠한 타 문서들을 참조할 수 있는지 상세한 작성지침을 설명하였다. 최종적으로 본 장에서 주요하게 설명하는 각 평가 제출물 별 참고할 수 있는 타 인증 제도의 제출물 및 표준을 Table 7에서 종합하여 보여준다.

4.2 RMF A&A의 평가 요구사항 분석

이처럼 이전 4.1절에서 다양한 표준과 개발 산출물을 참고하여 개발 업체가 작성해야하는 평가 제출물과 증거자료를 작성하였다. 본 절에서는 작성방안에 따라 작성한 평가 제출물과 증거자료가 타당함을 입증하기 위해 RMF A&A의 평가 요구사항을 모두 만족하고 있음을 보이고자한다. RMF A&A 표준에서는 획득하고자 하는 제품에 대한 평가자의 평가활동과 각 평가활동에 대한 평가 요구사항, 평가활동 결과가 적용되어야 하는 산출물에 대해서 설명하고 있다. 이에 개발 업체가 제품을 개발하고 RMF A&A에 따라 획득을 진행하는 군에 이를 납품하고자 할 경우 당연히 RMF A&A의 평가 요구사항에 맞추어 증거자료를 제출하여야 한다. 따라서 본 절에서는 RMF A&A 표준에서 개발 업체에게 요구하는

평가 요구사항들을 모두 식별한다. 그리고 4.1절에서 실증한 작성 방안이 RMF A&A의 평가 요구사항을 만족하는지 입증한다.

DoD에선 DoDI-8510.01외에 RMF에 따라 무기체계를 획득할 수 있도록 "DoD Program Manager's Guidebook for Integrating the Cybersecurity Risk Management Framework into the System Acquisition Lifecycle"(이하 DoD PM's Guidebook)[74]을 제공한다. 해당 문서를 통해 개발 업체를 비롯한 기관은 수행되어야 하는 평가활동 및 제출물에 대해 어떠한 책임 역할을 부여받는지 알 수 있다.

RMF A&A 표준을 통해 평가획득 프로세스 내 식별된 이해관계자는 총 17종이다. RMF A&A 표준을 분석한 결과 전체 이해관계자 중 개발 업체인 D/SI(Developer/System Integrator)와 관련된 평가 요구사항은 총 24건으로 추려진다. 24건의 평가 요구사항 중 가장 중대한 책임이 요구되는 Responsible에 개발 업체가 할당된 것은 4건이며 나머지 20건은 Accountable, Supportive, Consulted, Informed의 보조적인 역할을 수행하도록 할당되어 있다. 다음 Table 9는 평가자를 위한 평가 요구사항의 일부분을 보여준다. 이때 전체 평가 요구사항을 보여주기에 공간이 부족한 관계로 각 이해관계자를 기호로 표기하고, 각 기호가 어떠한 이해관계자를 가리키는지 Table 8에서 보여준다.

최종적으로 위에서 설명한 바와 같이 분석된 각 평가 요구사항들과 제안된 평가 제출물 작성방안의 세부항목을 매핑하여 작성방안이 타당함을 보이고자 한다. 24건의 전체 평가 요구사항은 각각 이전에 작성된 평가 제출물 및 증거자료 8건에 대해서 작성될 것을 요구하고 있다. 이에 다음과 같이 각 문서에 대한 요구사항을 만족하였다.

Table 8. Abbreviations Key in RASCI

Sym.	Role
①	Program Manager
②	Information Owner
③	Security Control Assessor
④	Chief Engineer
⑤	Authorizing Official
⑥	Information System Security Manager
⑦	User Representative
⑧	Developer/System Integrator
⑨	Chief Developmental Tester
⑩	Operational Test Agency
⑪	Defense Intelligency Agency
⑫	Req./Func. Sponsor
⑬	Joint Req. Oversight Council
⑭	Milestone Decision Authority
⑮	DoD(or Component) CIO
⑯	Systems Security Engineering
⑰	Joint Staff

SP 문서의 경우 보안통제항목 식별, 시스템 위험도 측정, 개발 대상 시스템과 연관된 주변의 타 시스템 식별과 같은 항목에 대해 주요하게 기술되어야 한다. 본 연구에선 NIST SP 800-53, CNSSI 1253, FIPS 199 등의 문서를 참조하여 위험도 측정 결과를 도출하고, 보안통제항목을 식별하여 작성하였고, CC의 Security Target, 위협 모델링의 Data Flow Diagram과 같은 문서를 통해서 주변 시스템을 식별하는 것으로 SP 문서에 대한 요구사항을 타당하게 만족한 것으로 사료된다.

다음으로, SAP 문서의 경우 보안 활동일정 및 수행될 보안 테스트 활동의 목록이 명확하게 식별되고 SP, SEP, PPP와 같은 다른 계획 문서들과 보안 테스트 일정이 일치해야 한다. 본 연구에선 CC의

Table 9. Assessment Requirements and Responsibility

Requirement	①	②	③	④	⑤	⑥	⑦	⑧	⑨	⑩	⑪	⑫	⑬	⑭	⑮	⑯	⑰
…																	
Characterize the attack surfaces and initiate cybersecurity assessment in planning and conduct component and system integration testing	A			R		C		R	R	C						C	
The detailed system design is completed and ensure that all cybersecurity requirements are included				C				R								C	
…																	

Security Target, 소프트웨어 공학의 테스트 계획 문서 등을 통해 보안 평가 계획일정과 수행될 테스트 활동의 종류(사용될 도구, 테스트 프로세스 등)를 SAP에 작성하고, SEP, PPP 문서에 해당 내용이 올바르게 기입되었는지 검토하는 것으로 SAP 문서에 대한 요구사항을 타당하게 만족한 것으로 사료된다.

SAR 문서의 경우 보안 테스트 결과를 작성하는 만큼 SAP 문서대비 변경된 점, 주요하게 다뤄져야 하는 수정사항과 같은 항목들이 상세히 기술될 것이 요구되었다. 본 연구에선 소프트웨어 공학의 기능 테스트 결과, CC의 AVA_VAN 컴포넌트와 관련된 보안 테스트 결과 문서 등을 참조하여 SAP 문서 대비 변경된 테스트 일정, 테스트를 위한 공격 시나리오 등을 참조하여 SAR 문서를 작성하는 것으로 SAR 문서 관련 요구사항을 타당하게 만족한 것으로 사료된다.

POA&M 문서는 결함 수정 일정과 해당 수정사항을 책임질 책임자가 명확히 식별되어야 한다. 또한, 지속적인 모니터링이 이루어져야 하므로 POA&M 문서가 동시에 지속적으로 갱신되고 있음을 감시해야한다. 본 연구에선 ENISA의 사고 대응 계획 문서, NIST의 800-53, 이전에 작성된 SP 문서, CC의 Security Target 문서 등을 참고하여 발견된 결함에 대한 수정 일정이 최종 배포 일정을 초과하지 않고 보안 책임자가 명확히 매핑될 수 있도록 작성하는 것으로 POA&M 문서에 대한 요구사항을 만족하였다. 또한, 최근 보안 테스트가 수행된 일자에 맞춰 POA&M 문서를 갱신하여 지속적인 업데이트 관련 요구사항도 만족한 것으로 사료된다.

RFP 문서의 경우 이전에 설명한 바와 같이 군이 전체 시스템을 구현하는데 필요한 서브 시스템, 모듈, 세부기능을 올바르게 식별할 수 있도록 도움을 주어야한다. 본 연구에선 CC의 ST 문서를 참조하여 전체 드론 시스템을 안전하게 구축하는데 필요한 구성요소를 식별하였다. 이를 통해 실제로 군이 필요하다고 판단한 서브 시스템, 모듈, 세부기능이 올바른지 검토할 수 있다.

이외에도 PPP, SEP 문서에 대해서도 타 기관이 해당 문서를 작성할 때 개발 업체의 개발 일정과 타 기관의 시스템 공학 일정, 프로그램 보호 일정이 어긋나지 않도록 검토해야한다. 또한, 개발 업체는 SEP, PPP 문서에 기술된 보호 감시 대상 시스템의 위협, 취약점, 대응방안 목록과 수행될 개발 및 보안 활동 목록이 잘못되지 않았는지 검토해야한다. 본 연구에선 이전에 SAP 문서를 작성하면서 보안 테스트 일정이 올바른지 검토하였다. 또한, SAP 문서에 작성된 보안 테스트 활동의 종류를 PPP 문서에 동일하게 기입하고, CC의 TSF 내부 기능 문서에서 설계 및 구현된 각 기능의 복잡도 측정 기준과 측정 결과를 SEP 문서에 작성하였다. 위협, 취약점, 대응방안 목록은 위협 모델링 결과와 CC의 ST 문서를 참고하여 PPP문서에 기입하였다. SEP, PPP 문서와 관련하여 도출된 위협이 모두 완화될 수 있도록 보안 요구사항을 도출하였고 각 보안 요구사항이 설계에 모두 반영되었음에 대한 증거자료로 시스템 설계(구성된 서브 시스템 및 인터페이스)와 보안 요구사항의 추적성이 포함되어 있는 SRDS 문서를 채택하는 것으로 SEP, PPP 관련 요구사항을 모두 타당하게 만족한 것으로 사료된다. 다음 Table 10은 RMF A&A의 요구사항을 어떠한 평가 제출물의 어떠한 항목으로 만족시켰는지 매핑한 결과를 보여준다.

V. 결론 및 향후 연구

최근 소프트웨어 제품의 복잡도가 높아짐에 따라 버그, 취약점 등으로 인한 사이버 보안 위협도 같이 증가하고 있다. 이러한 추세에 따라 증가하는 사이버 보안 위협을 완화시키기 위해 군은 RMF A&A를 통해 제품을 평가하고 획득한다. 일반적으로 상용제품을 개발하고 판매하는 업체들의 경우 보안내재화 철학이 반영된 소프트웨어 개발 방법론에 따라 제품을 개발한다[75]. 기존의 안전한 소프트웨어 개발 방법론에 보안내재화 철학이 반영된 점은 RMF A&A와 유사하다. 하지만, 기존의 안전한 소프트웨어 개발 방법론에 따라 제품을 개발하여도 RMF A&A에서 요구하는 평가 제출물을 도출할 수 없다. 또한, 개발 업체가 기존의 RMF A&A 관련 연구를 참고하고자 할 경우 1) 평가자의 행동에 대한 요구사항만 제시하거나, 2) 개발 프로세스의 전체 단계가 아닌 일부 단계에 대해서만 연구가 수행되었기에 RMF A&A의 평가 요구사항을 만족할 수 있는 전체 평가 제출물 및 증거자료를 작성하기 어렵다.

본 논문에서는 기존의 관련 연구들이 RMF A&A의 요구사항을 만족하지 못하는 문제점에 대해 분석하고 해당 문제점을 해결할 수 있도록 증거자료 작성방안을 제시하였다. RMF A&A 표준 분석을 통해 개발 업체가 작성하거나 타 기관이 작성하는데

Table 10. Rationale of Satisfying RMF A&A Requirements

RMF A&A Requirements	Rationale
Baseline of security control should be identified Input to: Security Plan	Satisfied by identifying baseline of security controls Doc: 〔SP〕Minimum Security Plan
The cybersecurity capability requirements of the system should satisfy planned security controls	Satisfied by documenting traceability between cybersecurity requirements and security controls Doc: 〔SAP〕Requirements Traceability Matrix
To prepare for the System Requirements Review, detail and refine cybersecurity requirements that derived from Program Protection Plan, cybersecurity strategy, Security Plan, technical solution specification	Satisfied by refining minimum security controls through threat, vulnerability, countermeasure list in PPP Doc: 〔SP〕Minimum Security Controls, 〔PPP〕Threat, Vulnerabilities, and Countermeasures
Update about these activity results should focus on system-level functions: Critical Analysis, Threat Assessment, Vulnerability Assessment, Trusted Systems and Networks Analysis include risk assessment and mitigation identify Input to: Security Plan	Satisfied by documenting risk assessment process and result in security plan Doc: 〔SP〕Information System Categorization
Refine system specification by translating system's cybersecurity function requirements to cybersecurity specification Input to: Request For Proposal	Satisfied by describing system cybersecurity functional requirements Doc: 〔RFP〕Description / Specifications / Statement of Work
Evaluate that the system functional baseline satisfies the draft CDD's cybersecurity requirements and that functional requirements and verification methods support the initial Request for Proposal development Input to: Request For Proposal	Satisfied by identifying security functional requirements in CC's Security Target Doc: 〔RFP〕Description / Specifications / Statement of Work
Update the System Engineering Plan and Program Protection Plan align with the Test and Evaluation Master Plan, Security Assessment Plan, and Acquisition Strategy Input to: System Engineering Plan, Program Protection Plan	Satisfied by reviewing that schedule and security test process(activity) in SEP and PPP is equal with SAP Doc: 〔SEP〕Technical Performance Measure and Metrics, 〔SEP〕Technical Schedule and Schedule Risk Analysis, 〔PPP〕Processes for Management and Implementation of PPP, 〔PPP〕Program Protection Costs
Baseline of cybersecurity requirement should be defined Input to: Security Plan, Security Requirements and Design Specification, Preliminary Design Review(Activity)	Satisfied by identifying baseline of security controls and requirements Doc: 〔SP〕Minimum Security Controls, 〔SP〕System Environment, 〔SP〕System Interconnections / Information Sharing
Map and allocate cybersecurity requirements to the hardware and software design	Satisfied by mapping sub system and interfaces in system with cybersecurity requirements listed in SP Doc: 〔SRDS〕Sub System and Requirements Traceability Matrix
Characterize the attack surfaces and initiate cybersecurity assessment in planning and conduct component and system integration testing	Satisfied by describing security test process(activity) in SAR Doc: 〔SAR〕Conduct Vulnerability Analysis
The detailed system design is completed and ensure that all cybersecurity requirements are included	Satisfied by describing system design and mapping each component with cybersecurity requirements Doc: 〔SRDS〕Sub System and Requirements

	Traceability Matrix
Conduct systems engineering, including technical planning as defined in the SEP(System Engineering Plan), and check the functional and security control baselines are properly complied	Satisfied by describing development process and mapping security requirements with design components Doc: 〔SEP〕Technical Activities and Products, 〔SRDS〕Sub System and Requirements Traceability Matrix
Ensure that cybersecurity requirements are mapped and allocated to hardware and software design	Satisfied by mapping hardware and software design components and cybersecurity requirements Doc: 〔SRDS〕Sub System and Requirements Traceability Matrix
Ensure that Critical Design Review initiating criteria for cybersecurity baseline design are met and that all cybersecurity requirements are reflected in the product baseline, which includes the design Input to: Security Requirements and Design Specification, Critical Design Review (Activity)	Satisfied by mapping design components and cybersecurity requirements Doc: 〔SRDS〕Sub System and Requirements Traceability Matrix
Develop Security Assessment Plan and provide it to the Authorizing Official in support of the Interim Authorization To Test activity Input to: Security Assessment Plan	Satisfied by creating SAP Doc: 〔SAP〕All
Submit draft Security Authorization Package at IATT(Interim Authorization To Test) in order to conduct system testing activities	Satisfied by creating Security Assessment Package(SP, SAP, SAR, POA&M) Doc: 〔SP〕All, 〔SAP〕All, 〔SAR〕All, 〔POA&M〕All
Conduct Developmental Test and Evaluation activity to demonstrate system maturity and readiness to begin production, preparedness for Operational Test and Evaluation, deployment and sustainment activities	Satisfied by describing security assessment result which include how much risk is reduced Doc: 〔SAR〕All
Prepare Developmental Test and Evaluation assessment as input to Milestone C Decision Input to: Security Assessment Plan, Developmental Test & Evaluation Assessment (Activity)	Satisfied by creating SAR and explaining that risk is reduced to acceptable level Doc: 〔SAR〕All
Submit complete Security Authorization Package to obtain ATO(Authorization To Operate) decision	Satisfied by creating Security Assessment Package(SP, SAP, SAR, POA&M) Doc: 〔SP〕All, 〔SAP〕All, 〔SAR〕All, 〔POA&M〕All
Update cybersecurity risk assessment for deficiencies/weaknesses Input to: Security Plan	Satisfied by updating risk assessment result in SP during the development process Doc: 〔SP〕Information System Categorization
Based on results of the cybersecurity risk assessment, document corrective tasks in the Plan of Action and Milestones Input to: Plan Of Action & Milestone	Satisfied by describing defects information(include defects ID) and corrective tasks in POA&M Doc: 〔POA&M〕All
Must address discovered defects before making Full-Rate Production or Full Deployment decision Input to: Program Protection Plan	Satisfied by describing program protection activity summary and complete schedule in PPP and checking every task in POA&M is completed before protection complete date of PPP Doc: 〔PPP〕Program Protection Summary, 〔POA&M〕All
Update cybersecurity risk assessment result	Satisfied by updating risk assessment result in SP

Input to: Security Plan	align with SAR's vulnerability analysis Doc: 〔SP〕Information System Categorization, 〔SAR〕Conduct Vulnerability Analysis
After sustainment phase, implement disposal phase. A risk assessment for decommissioned systems should be conducted and the appropriate steps taken to ensure that residual classified, sensitive, or privacy information is not exposed.	Satisfied by identifying security controls relate with disposal phase Doc: 〔SP〕 Minimum Security Controls

보조해야하는 평가 제출물과 증거자료의 종류를 식별하고, 각 문서의 템플릿을 수집하였다. 이후 각 문서들을 직접 작성하는 과정을 거쳐 각 템플릿 내 항목을 수월하게 작성할 수 있도록 참고할 수 있는 내용을 도출하였다. 이때 템플릿 내 각 항목별로 작성 시 참고할 수 있는 기존 개발 산출물 및 타 보안성 표준의 내용을 매핑하여 상세한 작성지침을 제시한다. 마지막으로 실증 결과 RMF A&A의 요구사항을 모두 만족할 수 있음을 보였다. 이에 개발 업체가 무기체계를 비롯한 군 IT 제품을 개발하는데 본 연구가 활용할 수 있을 것으로 기대된다.

본 연구에서 제시하고 있는 평가 제출물 작성 방안의 경우 RMF A&A라는 평가 표준에 국한된 내용을 제시하고 있다. 하지만 RMF A&A 이외에도 CC, CMVP(Cryptographic Module Verification Program), ISMS 등과 같은 다양한 IT 제품에 대한 보안성 평가 및 인증 제도가 존재한다. 과거부터 이러한 평가 및 인증의 단점은 평가를 받기 위한 문서작업의 오버헤드가 크다는 점이 존재하였다. 이에 향후에는 다양한 평가 및 인증 제도의 평가 제출물 간 관련성을 분석하여 재사용 될 수 있는 부분과 새롭게 작성되어야 하는 내용을 식별하는 것으로 보안성 평가 및 인증을 받는데 필요한 문서작업을 효율적으로 줄이는 방안에 대해 연구할 것이다.

References

〔1〕 DoD, "Risk Management Framework (RMF) for DoD Information Technology (IT)", DoDI 8510.01, 2014.

〔2〕 Hyunsuk Cho, Sungyong Cha and Seungjoo Kim, "A Case Study on the Application of RMF to Domestic Weapon System", Journal of The Korea Institute of Information Security & Cryptology, 29(6), pp. 1463-1475, Dec. 2019.

〔3〕 Jiseop Lee, et al, "Research for construction Cybersecurity Test and Evaluation of Weapon System", Journal of The Korea Institute of Information Security & Cryptology, 28(3), pp. 765-774, Jun. 2018.

〔4〕 M. Bendel, "An Introduction to Department of Defense IA Certification and Accreditation Process(DIACAP)", 2006.

〔5〕 NIST, "Standards for Security Categorization of Federal Information and Information Systems", FIPS 199, 2004.

〔6〕 NIST, "Guide for Conducting Risk Assessments", NIST SP 800-30, 2012.

〔7〕 M. A. Amutio, J. Candau, and J. A. Manas, "MAGERIT-version 3.0 Methodology for Information Systems Risk Analysis and Management, Ministry of Finance and Public Administration", Jul. 2014.

〔8〕 J. Wynn, et al, "Threat Assessment & Remediation Analysis (TARA)", MITRE, Oct. 2011.

〔9〕 B. Naqvi and A. Seffah, "A methodology for aligning usability and security in systems and services", 2018 3rd International Conference on Information Systems Engineering (ICISE), pp. 61-66, May 2018.

〔10〕 A. Sanchez-Gomez, J. Diaz and D. Arroyo, "Combining usability and privacy protection in free-access public cloud storage servers: review

of the main threats and challenges", arXiv preprint arXiv:1610.08727, 2016.
[11] V. K. Mishra, "Blockchain for Cybersecurity-Standards & Implications", Cybernomics, vol.1, no.5, pp. 11-15, Dec. 2019.
[12] E. Venson, et al, "Costing secure software development: A systematic mapping study", Proceedings of the 14th International Conference on Availability, Reliability and Security, pp. 1-11, Aug. 2019.
[13] J. Jaskolka, "Recommendations for Effective Security Assurance of Software-Dependent Systems", Science and Information Conference, pp. 511-531, Jul. 2020.
[14] J. Nguyen and M. Dupuis, "Closing the Feedback Loop Between UX Design, Software Development, Security Engineering, and Operations", Proceedings of the 20th Annual SIG Conference on Information Technology Education, pp. 93-98, Sep. 2019.
[15] E. Venson, et al, "The Impact of Software Security Practices on Development Effort: An Initial Survey", 2019 ACM/IEEE International Symposium on Empirical Software Engineering and Measurement (ESEM), pp. 1-12, Sep. 2019.
[16] E. Venson, "The effects of required security on software development effort", Proceedings of the ACM/IEEE 42nd International Conference on Software Engineering: Companion Proceedings, pp. 166-169, Jun. 2020.
[17] S. Harrison, et al, "A security evaluation framework for UK e-goverment services agile software development", arXiv preprint arXiv:1604.02368, Apr. 2016.
[18] R. Kumar and R. Goyal, "Assurance of data security and privacy in the cloud: A three-dimensional perspective", Software Quality Professional, vol. 21, no.2, pp. 7-26, Mar. 2019.
[19] A. Jurcut, et al, "Security Considerations for Internet of Things: A Survey", SN Computer Science, vol.1, no.193, pp. 1-19, Jun. 2020.
[20] M. Zarour, M. Alenezi and K. Alsarayrah, "Software Security Specifications and Design: How Software Engineers and Practitioners Are Mixing Things up", Proceedings of the Evaluation and Assessment in Software Engineering, pp. 451-456, Apr. 2020.
[21] S. Evangelou and C. Akasiadis, "Security Assessment in IoT Ecosystems", 2020.
[22] S. A. Ehikioya, E. Guillemot, "A critical assessment of the design issues in e commerce systems development", Engineering Reports, vol.2, no.4, Mar. 2020.
[23] A. Kott, J. Ludwig and M. Lange, "Assessing mission impact of cyberattacks: toward a model-driven paradigm", IEEE Security & Privacy, vol.15, no.5, pp. 65-74, Oct. 2017.
[24] M. M. Jakeri and M. F. Hassan, "A Review of Factors Influencing the Implementation of Secure Framework for in-House Web Application Development in Malaysian Public Sector", 2018 IEEE Conference on Application, Information and Network Security (AINS), pp. 99-104, Nov. 2018.
[25] H. F. Atlam, et al, "Internet of Things Forensics: A Review", Internet of Things, vol.11, May 2020.
[26] J. Heilmann, "Application Security

Review Criteria for DevSecOps Processes", MS Thesis, Lulea University of Technology, Jun. 2020.
[27] E. A. Wanniarachchi, "Program security evaluation using dynamic disassembly of machine instructions in virtualized environments", PhD Thesis, 2016.
[28] Sungyong Cha, et al, "Security evaluation framework for military iot devices", Security and Communication Networks, vol. 2018, pp. 1-12, May 2018.
[29] R. Egan, et al, "Cyber operational risk scenarios for insurance companies", British Actuarial Journal, vol. 24, Feb. 2019.
[30] M. Kern, et al, "A Cybersecurity Risk Assessment Process for Model-Based Industry 4.0 Development", 23th World Multi-Conferebce on Systemics, Cybernetics and Informatics (WMSCI), 2019.
[31] M. W. Meersman, "Developing a Cloud Computing Risk Assessment Instrument for Small to Medium Sized Enterprises: A Qualitative Case Study Using a Delphi Technique", PhD Thesis, Northcentral University, May 2019.
[32] T. Pavleska, et al, "Cybersecurity Evaluation of Enterprise Architectures: The e-SENS Case", IFIP Working Conference on The Practice of Enterprise Modeling, pp. 226-241, Nov. 2019.
[33] A. Hudic, et al. "Towards a unified secure cloud service development and deployment life-cycle", 2016 11th International Conference on Availability, Reliability and Security (ARES), pp. 428-436, Aug. 2016.
[34] C. J. D'Orazio, et al, "A Markov adversary model to detect vulnerable iOS devices and vulnerabilities in iOS apps", Applied Mathematics and Computation, vol. 293, pp. 523-544, Jan. 2017.
[35] H. Rygge and A. Josang, "Threat poker: solving security and privacy threats in agile software development", Nordic Conference on Secure IT Systems, pp. 468-483, Nov. 2018.
[36] L. Sion, et al, "Solution-aware data flow diagrams for security threat modeling", Proceedings of the 33rd Annual ACM Symposium on Applied Computing. pp. 1425-1432, Apr. 2018.
[37] P. Frijns, R. Bierwolf and T. Zijderhand, "Reframing security in contemporary software development life cycle", 2018 IEEE International Conference on Technology Management, Operations and Decisions (ICTMOD), pp. 230-236, Nov. 2018.
[38] H. Aranha, et al, "Securing Mobile e-Health Environments by Design: A Holistic Architectural Approach", 2019 International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), pp. 1-6, Oct. 2019.
[39] K. M. Kaariainen, "Improving security in software development process: Case Tieto AS", MS Thesis, South-Eastern Finland University of Applied Sciences, May 2019.
[40] M. T. Baldassarre, et al, "Privacy oriented software development", International Conference on the Quality of Information and Communications Technology, pp. 18-32, Aug. 2019.
[41] P. Siddhanti, P. M. Asprion and B. Schneider, "Cybersecurity by Design for Smart Home Environments",

Proceedings of the 21st International Conference on Enterprise Information Systems (ICEIS), pp. 587-595, 2019.
[42] P. De Cremer, et al, "Sensei: Enforcing secure coding guidelines in the integrated development environment", Software: Practice and Experience, vol.50, no.9, pp. 1682-1718, Jun. 2020.
[43] S. Ramalingan, et al, "A Holistic Systems Security Approach Featuring Thin Secure Elements for Resilient IoT Deployments", Sensors, vol.20, no.18, pp. 5252, Sep. 2020.
[44] S. Evangelou, "Auditing and extending security features of IoT platforms", Diploma Thesis, University of Thessaly, Jul. 2020.
[45] M. Howard and S. Lipner, "The Security Development Lifecycle - SDL: A Process for Developing Demonstrably More Secure Software", Microsoft Press, May 2006.
[46] T. M. MIR, et al, "Threat analysis and modeling during a software development lifecycle of a software application", U.S. Patent No 8,091,065, 2012.
[47] E. Chen, et al, "Designing security into software during the development lifecycle", U.S. Patent Application No 13/619,581, 2013.
[48] W. Douglas and R. Simon. "Applying Secure Software Engineering (SSE) Practices to Critical Space System Infrastructure Development", In: 14th International Conference on Space Operations, pp. 2392, 2016.
[49] B. J. Greer, "Cybersecurity For Healthcare Medical Devices", PhD Thesis, Utica College, May 2018.
[50] A. Sanchez-Gomez, et al, "Review of the main security threats and challenges in free-access public cloud storage servers", Computer and Network Security Essentials. Springer, pp. 263-281, Aug. 2018.
[51] N. Alhirabi, O. Rana and C. Perera, "Designing Security and Privacy Requirements in Internet of Things: A Survey", arXiv preprint arXiv:1910.09911, Oct. 2019.
[52] K. Chermana, H. Pemmaiah, "Cleansing Legacy Data for GDPR Compliance: A Case Study", PhD Thesis, Auckland University of Technology, 2019.
[53] W. Hassan, et al, "Latest trends, challenges and solutions in security in the era of cloud computing and software defined networks", Int J Inf & Commun Technol ISSN, vol.2252, no.8776, 2019.
[54] Jin-Keun Hong, "Component Analysis of DevOps and DevSecOps", Journal of the Korea Convergence Society, 10(9), pp. 47-53, Sep. 2019.
[55] J. Geismann and E. Bodden, "A systematic literature review of model-driven security engineering for cyber-physical systems", Journal of Systems and Software, vol. 169, Nov. 2020.
[56] M. Alenezi and S. Almuairfi, "Essential activities for Secure Software Development", International Journal of Software Engineering & Applications (IJSEA), vol. 11, no. 2, Mar 2020.
[57] F. Y. Akeel, "Secure data integration systems", PhD Thesis, University of Southampton, Oct. 2017.
[58] S. Lipke, "Building a secure software supply chain using docker", MS Thesis, Hochschule der Medien, 2017.
[59] A. Schaad and T. Reski, "Open Weakness and Vulnerability Modeler(OVVL) - An Updated

Approach to Threat Modeling", Proceedings of the 16th International Joint Conference on e-Business and Telecommunications, pp. 417-424, Jan. 2019.
[60] F. Nabi, J. Yong and X. TAO, "Classification of logical vulnerability based on group attacking method", Journal of Ubiquitous Systems & Pervasive Networks, vol.14, no.1, pp. 19-26, 2021.
[61] Sooyoung Kang and Seungjoo Kim, "CIA-Level Driven Secure SDLC Framework for Integrating Security into SDLC Process", Journal of The Korea Institute of Information Security & Cryptology, 30(5), pp. 909-928, Aug. 2020.
[62] Sungyong Cha, Seungsoo Baek and Seungjoo Kim, "Blockchain Based Sensitive Data Management by Using Key Escrow Encryption System From the Perspective of Supply Chain", IEEE Access, vol.8, pp. 154269-154280, Aug. 2020.
[63] T. Pavleska, et al, "Drafting a Cybersecurity Framework Profile for Smart Grids in EU: A Goal-Based Methodology", European Dependable Computing Conference, pp. 143-155, Aug. 2020.
[64] V. Casola, et al, "A novel Security-by-Design methodology: Modeling and assessing security by SLAs with a quantitative approach", Journal of Systems and Software, vol.163, May 2020.
[65] L. David, "DREADful", Microsoft, Aug. 2007.
[66] E. Zheng, J. Kao and B. He, "Automated secure software development management, risk assessment, and risk remediation", U.S. Patent No 10,740,469, 2020.
[67] A. Van den Berghe, et al, "Design notations for secure software: a systematic literature review", Software & Systems Modeling, vol.16, no.3, pp. 809-831, Aug. 2017.
[68] R. Buijtenen and T. Rangnau, "Continuous Security Testing: A Case Study on the Challenges of Integrating Dynamic Security Testing Tools in CI/CD", 17th SC@ RUG, 2019.
[69] A. Johannsen, D. Kant and R. Creutzburg, "Measuring IT security, compliance and data governance within small and medium-sized IT enterprises", Electronic Imaging, vol. 252, pp. 1-11, 2020.
[70] ISO, "Evaluation criteria for IT security(CC)", ISO/IEC 15408, 2009.
[71] CNSS, "Security Categorization and Control Selection for National Security Systems", CNSSI 1253, 2009.
[72] NIST, "Volume I: Guide for Mapping Types of Information and Information Systems to Security Categories", NIST SP 800-60, 2008.
[73] NIST, "Security and Privacy Controls for Information Systems and Organizations", NIST SP 800-53, 2020.
[74] DoD, "DoD Program Manager's Guidebook for Integrating the Cyb-ersecurity Risk Management Framework into the System Acquisition Lifecycle", 2015.
[75] Microsoft, "Security Development Lifecycle - SDL Process Guidance Version 5.2", 2012.
[76] V. John and M. Gary, "Building Secure Software: How to Avoid Security Problems the Right Way", Addison-Wesley, Aug. 2001.
[77] NIST, "Risk Management Framework for Information Systems and Organizations: A System Life Cycle

Approach for Security and Privacy", NIST SP 800-37, 2018.
〔78〕 NIST, "Security Considerations in the System Development Life Cycle", NIST SP 800-64 Revision 2, 2019.
〔79〕 L. J. Moukahal, M. A. Elsayed and M. Zulkernine, "Vehicle Software Engineering (VSE): Research and Practice," IEEE Internet of Things Journal, vol. 7, no. 10, pp. 10137-10149, Jun. 2020.

〈저자소개〉

조 광 수 (Kwangsoo Cho) 정회원
2019년 2월: 호서대학교 컴퓨터공학과 졸업
2019년 3월~현재: 고려대학교 정보보호대학원 석사과정
〈관심분야〉 보안공학, RMF A&A, 시큐어 코딩, 소프트웨어 개발

김 승 주 (Seungjoo Kim) 종신회원
1994년~1999년: 성균관대학교 정보공학과(학사, 석사, 박사)
1998년~2004년: 한국인터넷진흥원(KISA) 팀장
2004년~2011년: 성균관대학교 정보통신공학부 부교수
2004년~현재: 한국정보보호학회 이사
2011년~현재: 고려대학교 정보보호대학원 정교수
2014년~2015년: 육군사관학교 초빙교수
2014년~2016년: 다음카카오 프라이버시 정책 자문위원
2016년~2018년: 개인정보분쟁조정위원회 위원
2016년~현재: 산업통상자원부 전략물자기술 자문위원
2016년~현재: 한국카카오뱅크 정보보호부문 자문교수
2017년~현재: 고려대학교 국방RMF연구센터(AR2C) 센터장
2018년~2020년: 대통령직속 4차산업혁명위원회 위원
2018년~현재: 고려대학교 고신뢰 보안운영체제 연구센터(CHAOS) 센터장
2019년~현재: 중소벤처기업부 규제특례 심의위원
2020년: 합동참모본부 정책자문위원회 자문위원
2020년~현재: 해군발전자문위원회 자문위원
2020년~현재: 서울특별시 스마트도시위원회 위원
2021년~현재: 사이버작전사령부 자문위원
〈관심분야〉 보안공학 및 보안내재화 방법론, 자동차 및 무인이동체 보안성 평가 인증, RMF A&A, 암호학 및 블록체인