Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.32, NO.2, Apr. 2022 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2022.32.2.279

개발 전주기 사이버보안 관점에서의 해상 사이버보안 형식승인과 RMF 비교 연구

이 수 원,[1†‡] 황 세 영,[2] 홍 진 아,[3] 김 병 진[2]
[1,2,3]한화시스템 (수석연구원, 전문연구원, 선임연구원)

A Comparative Study on Type Approval of Maritime Cyber Security and RMF in the View of System Development Lifecycle

Suwon Lee,[1†‡] Seyoung Hwang,[2] Jina Hong,[3] Byeong-jin Kim[2]
[1,2,3]Hanwha System (Chief Engineer, Senior Engineer, Junior Engineer)

요 약

최근 사이버 위협이 고도화되고 해킹기술이 발달함에 따라 자동차, 선박 등 다양한 분야에서 사이버보안이 강조되고 있다. 이러한 추세에 따라 여러 산업 분야에서 기자재 및 시스템에 대한 사이버보안을 요구하고 있으며, 이에 관련된 인증 및 제도가 구체화 되고 있다. 본 논문에서는 산업 분야의 사이버보안 형식승인이 RMF와 같이 명시적으로 개발 단계별로 구분하지는 않으나, 시스템 개발 전주기에 사이버보안 요소가 반영되어야 한다는 공통요소가 있다는 전제하에 RMF와 비교하였다. 비교 대상으로 해상 사이버보안 형식승인을 선정하였으며, 이는 공식적인 사이버보안 형식승인의 예로 국내 유일의 국제 선박검사 기관인 한국선급의 형식승인을 예로 비교한 것이지 산업 분야의 사이버보안 형식승인을 대표한다는 의미는 아니다. 비교 결과 해상 사이버보안 형식승인 획득 절차는 RMF와 같이 개발 단계별로 구분하지 않지만, RMF와 같이 개발 전단계에 대해 사이버보안 요소 적용해야 하는 절차상의 공통점과 단계별 결과물에 대한 유사성을 확인하였다. 이에 따라 해상 사이버보안 형식승인 획득과정을 통해 개발된 시스템은 개발 전주기에 사이버보안 요소가 적용되었다고 판단할 수 있는 가능성을 확인하였다.

ABSTRACT

With the advancement of cyber threats and the development of hacking technologies, cyber security is being emphasized in various fields such as automobiles and ships. According to this trend, various industrial fields are demanding cybersecurity, and related certifications. In this paper, cybersecurity type approval is compared with the RMF stage under the premise that there are common elements with RMF in that cybersecurity elements must be reflected in the entire system development cycle. For comparison, type approval of maritime cyber security of the Korean Register of Shipping was selected. In conclusion, although type approval of maritime cyber security acquisition procedure is not divided by development stage like the RMF, there are the commonalities in the procedure to apply the cybersecurity element to the System development lifecycle like the RMF. Accordingly, the possibility of determining that the cybersecurity element was applied to the entire development cycle was confirmed.

Keywords: RMF(Risk Management Framework), Cyber Risk, SDL(Security Development Lifecycle)

Received(12. 07. 2021), Modified(02. 03. 2022), Accepted(03. 15. 2022)

† 주저자, suwon.lee@hanwha.com
‡ 교신저자, suwon.lee@hanwha.com(Corresponding author)

I. 서 론

최근 해킹기술의 발달 및 고도화됨에 따라 폐쇄망 및 비개방형 환경이란 이유로 사이버 위협으로부터 안전하다고 인식되었던 방산, 선박, 자동차 등의 여러 분야에서의 해킹 가능성이 급속도로 증가되고 있다. 또한 초연결 및 초지능형 기술 적용에 따라 시스템 내 네트워크 연동이 많아지면서 사이버 위협에 대한 노출이 많아지고 있다. 이러한 추세로 인해 여러 산업 분야에서 사이버보안을 요구하고 있으며, 사이버보안에 관련한 인증 및 제도가 구체화 되고 있다. 방산 분야인 경우, 미국은 사이버무기에 대한 고등급(Common Criteria 표준을 기준으로 했을 때 EAL5 등급 이상) 보안성 시험·평가 기술 개발 및 관련 전문인력 양성에 막대한 예산을 투입해 오고 있으며, 특히 2015년에는 '사이버공격에 대응할 수 있는 무기체계 획득을 위한 사이버보안 시험·평가 가이드라인'을 발표하였다[1]. 미 국방부는 국방부(DoD, Department of Defense Instruction)지침 8510.01 "Risk Management Framework (RMF) for DoD Information Technology (IT)"에 의해 RMF (Risk Management Framework)를 준수하도록 규정하고 있다. 선박 분야에서는 국제해사기구인 IMO(International Maritime Organization)는 ISM (International Safety Management) 코드에 사이버 위험관리를 반영하지 않은 선박은 억류 조치할 수 있는 조항을 포함하였다[2]. 또한 IMO는 해상 사이버 위험관리 지침(MSC-FAL.1/Circ.3)을 승인함으로써 해상 사이버 위험관리는 디지털화, ICT 융합, 자동화 및 네트워크 기반 시스템의 의존도의 증가로 인한 해사산업(해운업, 항만업, 물류업 등)의 주요한 관리 항목임을 강조하고 있다. 자동차 분야에서, 국제 자동차기준 조화 회의체(UNECE WP.29)는 차량 제작사들이 차량 사이버보안 관리를 위한 사이버보안관리체계(Cyber Security Management System)를 갖추고, 차량 형식에 대한 위험평가·관리를 수행하여야 한다는 내용으로 자동차 사이버보안에 관한 최초의 국제기준을 채택하였다[3]. 자동차 사이버보안의 국제기준에는 제작사가 자동차 사이버보안에 필요한 각종 프로세스 등의 관리체계를 적절히 갖추었음을 입증해야 하며, 차량에 대한 위험평가·관리, 보안 조치 및 충분한 검증시험 등을 수행해야 하는 내용을 포함하고 있다. 본 논문에서는 여러 산업분야에서 요구되는 사이버보안이 시스템 개발 전주기에 걸쳐 관리되고 적용되어야 한다는 전제하에 해상 사이버보안 형식승인을 RMF에서 명시하는 개발 전주기 단계별로 유사성을 분석하였다. 이유는 각 산업 분야별로 요구되는 사이버보안 항목이 다를 수 있지만, 개발 전주기에 사이버보안 요구 항목을 반영해야한다는 공통점과 유사성을 도출함으로써, 추후 다른 산업분야 간의 활용되거나 참고할 수 가능성을 확인하기 위해서이다. 본 논문의 구성은 다음과 같다. 서론에 이어, 2장에서는 관련 연구로 미국의 RMF와 한국선급의 해상 사이버보안 형식승인에 대해 설명하고, 해상 사이버 형식승인 과정에서 필요로 하는 사이버보안 요소에 대해 구체적인 실례로 설명하기 위한 SecuAider에 대해 간단히 설명한다. 자동차에 대한 사이버보안 형식승인에 대해서도 비교 분석하고자 하였으나, 현재 국내 자동차의 사이버보안 형식승인을 인증하는 기관은 없기 때문에, 사이버보안의 형식승인이 발급 가능한 한국선급의 해상 사이버보안 형식승인이 인증과정을 통해 비교분석하였다. 3장에서는 해상 사이버보안 형식승인도 개발 전주기에 사이버보안 요소를 반영해야 한다는 관점에서 RMF 단계별로 해상 사이버보안 형식승인과 RMF와 공통점을 언급하고 실례로서 어떠한 내용이 반영되는지 SecuAider에서 적용한 내용을 예를 들어 설명하였다. 이후 4장에서는 결론 및 향후 연구 방향에 대해 설명하는 순서로 논문을 구성하였다.

II. 관련 연구

2.1 미국의 RMF

미국은 정보보호 시스템의 성능과 신뢰도를 평가하기 위해 수명주기 매 단계에서 정보보호 활동이 일관성 있게 수립·시행되도록 노력해왔다. 미 국방부는 인증 및 인가(C&A, Certification and Accreditation) 를 의무화하여 모든 시스템에 적용하고 있다. C&A의 시작은 1983년 오렌지 북으로 불리는 평가기준 TCSEC(Trusted Computer System Evaluation Critiera)를 발표하면서 시작되었고, 1985년 미 국방성의 표준(DoD STD 5200.28)으로 채택하였다. 이후 1997년 DITSCAP (DoD Information Technology Security Certification and Accereditation Process)로, 2007년에는 DITSCAP의 단점을 보완하여 DIACAP (Defense Information Assurance Certifica-

tion and Accreditation Process)로 업데이트 되었으며, 현재는 미국표준기술연구소(NIST, National Institute of Standard and Technology)에서 DIACAP의 정보보증 개념을 발전시켜 RMF를 도입하였다. RMF는 제품 개발부터 평가 및 유지관리에 이르기까지 제품 라이프사이클 전반에 걸쳐 보안 보증 활동을 고려한 모델이다[4]. RMF는 7단계로 구성되며 각 단계의 세부 내용은 NIST에서 배포하는 특별 간행물(Special Publication)에 설명되어 있다.

2.2 한국선급의 해상 사이버보안 형식승인

해상 사이버보안 형식승인 발행 기관으로 한국선급이 있다. 한국선급은 해상에서의 인명과 재상의 안전을 도모하고 조선 해운 및 해양에 관한 기술을 진흥시키기 위하여 설립된 대한민국 유일의 국제 선박검사기관이다[5]. 한국선급은 ISO 27001, ISO 27002, IEC 62443 등의 사이버보안에 대해 국제표준을 근거로 하는 해상 사이버보안 시스템 지침[6], 해상 사이버보안 형식승인 지침[7]을 제정하여 선박 및 기자재에 대한 사이버보안 인증을 수행하고 있다.

2.3 SecuAider

SecuAider는 해상 사이버보안 형식승인을 RMF와 비교할 때 구체적인 예를 들기 위해 언급한 상용 솔루션이다. SecuAider는 한국선급의 해상 사이버보안 형식승인을 획득하였으며, 주요 기능은 Fig 1.과 같이 선박 내 사이버 자산 관리, 네트워크 토폴로지 시각화 기능, 리스크 관리 및 모니터링 기능을 제공한다.

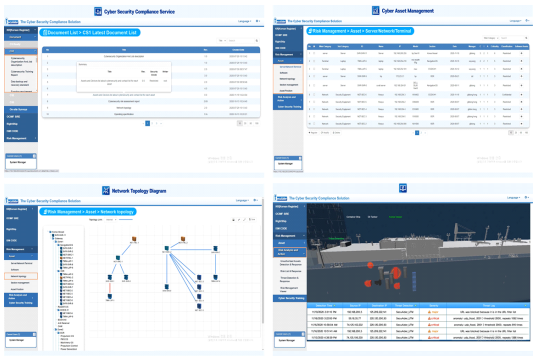


Fig. 1. SecuAider Key Features

III. RMF 단계별 사이버보안 적용 연구

본 장에서는 해상 사이버보안 형식승인 과정과 RMF 각 단계별로 유사성을 분석하고 실제 사이버보안 형식승인 과정에서 적용한 내용을 예를 들어 기술하였다. 개발 전단계의 사이버보안 적용 내용을 비교하기 위해 RMF 단계를 기준으로 사이버보안 형식승인 과정을 비교하였다. RMF 단계는 준비(Prepare), 분류(Categorize), 선택(Select), 구현(Implement), 평가(Assess), 승인(Authorize), 모니터(Monitor)의 7단계로 구성되며 각 단계에서의 RMF의 한국선급 해상 사이버보안 형식승인의 정의 및 요구사항에 대하여 기술하여 비교 분석을 수행하였다.

3.1 준비(Prepare) 단계

3.1.1 RMF에서의 준비 단계

RMF의 준비단계는 모든 단계 수행 전 보안 및 리스크를 관리하기 위해 필수적으로 수행해야 하는 단계로 조직과 시스템 레벨로 분류하여 수행된다. 리스크 관리 역할을 식별하고, 전략 수립, 조직 전반의 리스크 평가, 전략, 공통의 통제 항목 식별 등의 결과가 도출되는 단계이다.

3.1.2 해상 사이버보안 형식승인에서의 준비 단계

해상 사이버보안 형식승인에서는 RMF와 같이 준비단계로 명시하지 않았으나, 사이버보안 형식승인을 준비하는 과정과 유사하다고 볼 수 있다. 사이버보안 형식승인을 인증받으려는 대상을 선정하고 사이버인증을 받기위한 각 단계별 산출물 조사, 사이버인증을 받기위한 사내 조직 구성 및 역할에 대해 조사하는 과정이 RMF와 준비단계와 유사하다. 실제 적용 예로 SecuAider의 개발에 참여하는 부서 식별 및 역할을 정의하였고 형식승인에 필요한 개발요구서, 설계서, 사용자 매뉴얼 등 산출물을 식별하고 인증 단계별 수행 내용 분석하여 문서화 하였다.

3.2 분류(Categorize) 단계

3.2.1 RMF에서의 분류 단계

RMF의 분류단계는 3가지 분류기준(기밀성

(Confidentiality), 무결성(Integrity), 가용성(Availability))에 대하여 보안 영향성(Low, moderate, high)을 판단하여 시스템 분류의 영향성을 선정하는 단계이다. 시스템 특성을 문서화하고, 시스템과 정보의 보안 분류 및 분류의 보안 영향성을 확정하는 등의 결과가 도출되는 단계이다. table 1. 과 table 2.는 보안 분류를 결정하는데 기반이 되는 보안 목적 및 영향성 레벨을 정의하는 내용이다.

Table 1. Security Objective Definitions〔44 U.S.C., SEC. 3542〕

security objective	definition
confidentiality	Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.
Integrity	Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.
Availability	Ensuring timely and reliable access to and use of information.

Table 2. Potential Impact Definitions

level	definition
low	if the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation.
moderate	if the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation.
high	if the loss confidentiality, integrity, or availability could be expected to have a catastrophic adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation.

3.2.2 해상 사이버보안 형식승인에서의 분류 단계

한국선급의 해상 사이버보안 형식승인 절차에서도 리스크 평가를 위해 시스템 사이버자산의 가치 중요도를 산정하도록 규정하고 있다. 사이버자산의 중요도평가 기준은 자산의 가치 및 중요도에 따른 보호수준을 분류하여 자산을 효율적으로 관리하도록 하는데에 목적이 있으며, 가치 평가는 정보보호의 특성인 기밀성, 무결성, 가용성의 요구 정도를 평가하여 중요도를 산정하고 중요도 등급에 따라 사이버자산 가치 측정을 수행한다.

사이버 자산 중요도 등급(3~9)
= 기밀성(1~3) + 무결성(1~3) + 가용성(1~3)

Table 3. Asset Materiality Rating Criteria

rank	value	range	Description
1	3	8~9	Damage to the property may result in a very high level of loss, failure of the service, or loss of economic status.
2	2	5~7	Serious loss in case of damage to the property or negative impact on the service
3	1	3~4	Even if the property is damaged, there is little or no service impact.

구체적인 실례로서 SecuAider의 사이버자산 6종에 대하여 기밀성, 무결성, 가용성의 요구 정도를 산정하고, 결과를 합하여 사이버자산 중요도 등급을 도출하였다. 사이버자산의 가치 평가는 정보보호의 특성인 기밀성(Confidential), 무결성(Integrity), 가용성(Availability)의 요구 정도를 평가하여 중요도를 산정하고 중요도 등급에 따라 사이버자산 가치 측정한다. 사이버자산의 가치 중요도는 사이버자산에 산정된 결과를 합하여 사이버자산의 중요도 지수(total range)를 도출하였다. 사이버자산은 중요도 지수에 따라 자산의 등급(class)이 결정되고 등급에 따라 자산별로 정해진 가치(value)보안통제항목에 위협 취약성 평가, 리스트 평가의 가중치에 반영된

다. Fig. 2.는 산정 기준으로 개발한 시스템을 평가한 결과의 예이다. 평가는 시스템 개발자, 정보보호 관련 전문가, 과제 책임자 등으로 평가팀을 구성하여 도출된 점수의 평균값으로 산출하였다. 구성품은 보안장비, 주요서버, 네트워크 장비 등으로 구성된다.

위와 같이 자산에 대해 가치평가 결과는 사이버보안에 대한 리스크 평가에 영향을 미치며 자산의 주요도가 높을수록 보안대책을 강화하는 것이 일반적이다.

ANNEX 1. Asset value evaluation result

No	Asset No.	Assets	Asset Value					Criticality Index
			C	I	A	total	class	
1	SC-UTM-01	UTM	2	2	2	6	2	2
2	NW-SWT-01	switch	1	1	2	4	3	1
3	SVR-UBU-01	server	2	3	2	7	2	2
4	DB-MAR-01	data DB	2	2	2	6	2	2
5	DB-MON-01	log DB	2	2	2	6	2	2
6	PC-WIN-01	node	2	2	2	6	2	2

Fig. 2. Asset value evaluation result

3.3 선택(Select)

3.3.1 RMF에서의 선택 단계

RMF의 선택 단계는 리스크 평가에 기반하여 시스템을 보호하기 위해 NIST SP 800-53 문서에서 그룹핑하여 분류된 보안통제항목을 선택하는 단계이다. RMF에서 보안과 프라이버시 통제는 table 4.와 같이 20개의 패밀리군으로 구성되어 있다.

보안통제 항목은 기본통제 및 추가통제 항목으로 이루어지며, 추가통제는 기본통제에 특정 기능 또는 특수성을 추가하여 기본통제의 보안성 강도를 높인다. 추가통제는 항상 기본통제 상황에서 사용해야하며, 더 큰 보호가 필요하거나 조직에서 리스크 평가에 기반하여 통제 또는 보장에 대해 추가적으로 요구되어지는 경우 사용한다. 보안통제 항목은 RMF에 명시하는 모든 항목을 만족해야하는 것은 아니며 시스템 특성에 따라 적용되어야 하는 항목이 다르게 적용된다.

Table 4. RMF's family of security and privacy controls

family	definition
AC	Access Control
AT	Awareness And Training
AU	Audit And Accountability
CA	Assessment, Authorization, and Monitoring
CM	Configuration Management
CP	Contingency Planning
IA	Identification And Authentication
IR	Incident Response
MA	Maintenance
MP	Media Protection
PE	Physical and Environmental Protection
PL	Planning
PM	Program Management
PS	Personal Security
PT	Personally Identifiable Information Processing and Transparency
RA	Risk Assessment
SA	System and Service Acquisition
SC	System and Communications Protection
SI	System and Information Integrity
SR	Supply Chain Risk Management

3.3.2 해상 사이버보안 형식승인에서의 보안통제항목

사이버보안 형식승인에서 유사한 단계로 각 자산 및 시스템별로 적용해야 할 사이버리스크 항목을 선정하는 단계에 해당한다. 해상 사이버보안 형식승인에서는 table 5.와 같이 7개의 세션으로 구분하고 각 세션 별로 요구되는 사이버보안 요소를 명시하고 있다.

이는 사이버보안의 국제표준을 근거로 한국선급이 분류한 것으로 RMF 보안통제 항목과은 약간의 차이는 있으나 큰 범주안에서는 요구되는 내용을 비슷하였다. 해상 사이버보안 형식승인과 RMF의 보안통제 항목에 대한 비교 분석 내용에 대한 구체적인 내용은 논문 범위를 벗어나는 내용으로 자세한 내용은 생략한다. 이 단계에서 사이버보안 형식승인의 보안 요구사항 항목을 반영하기 위해서는 구체적으로 통제항목을 세분화하여야 한다. 왜냐하면 지침은 적용해야 하는 구체적인 방법까지 명시하지 않기 때문이다. RMF 또한 구체적인 방법에 대해 명시하지

Table 5. Cyber security requirements in accordance

section	number of requirements
Identification and authentication control	12
Use control	11
System integrity	8
Data confidentiality	3
Restricted data flow	2
Timely response to event	2
Resource availability	7

않으며 구현 방법에 대해서는 NIST의 기관에서 발간하는 별도의 문서에 정의되어 있다. 사이버보안 형식승인에 적용한 실제적인 예를 위해 SecuAider에서 설정한 보안통제항목을 설명하면, 기술적 취약점 분석, 평가방법 상세가이드, 한국선급의 형식승인 지침, STIG(Securiy Technical Implementation Guide) 항목 근거로 보안장비, 네트워크 장비, 서버, DB 영역을 분류하여 205항목을 선정하였다. 선정된 205개 항목은 RMF에서의 접근통제(AC), 보안평가 및 인가(CA), 식별 및 인증(IA) 등의 세부 내용과 유사하였다. 이 단계에서 SecuAider의 보안통제 항목 선정 절차는 한국선급이 검토하여 승인하는 절차로 수행되었다.

3.4 구현(Implement) 단계

3.4.1 RMF에서의 구현 단계

RMF의 구현 단계는 획득 단계 또는 구현 단계 동안 통제 항목이 구현되는 것을 의미한다. 조직에 의해 구현되어지는 일부 기본 통제 항목은 보유하고 있을 수도 있으며, 시스템에 종속되어진 통제 항목은 시스템 소유자가 보안과 프라이버시 요구사항, 시스템 분류, 시스템 리스크 평가 등에 기반하여 어떻게 구현할지 결정되어야 하는 단계이다.

3.4.2 해상 사이버보안 형식승인에서의 구현 단계

한국선급의 구현 단계는 한국선급의 형식승인을 위한 산출물인 기능사양 명세서, 소프트웨어 절차서 등에 각항목이 반영되도록 요구되고 있다. 시스템 개발에 있어서 위의 산출물을 제출해야 하며 한국선급은 이를 검토하여 승인을 한다. 실제 시스템을 구현할 때는 위의 산출물을 근거로 사이버보안 요소를 구현 단계에서 개발하여야 하며, 예를 들기 위해 언급된 SecuAider 또한 3.3.2에서 선정한 통제항목에 대해 항목별로 설계방안을 수립하고 사이버보안 기능을 개발 적용하였다.

3.5 평가(Assess) 단계

3.5.1 RMF에서의 평가 단계

RMF의 평가 단계는 통제항목이 구현되었는지, 의도한 대로 동작하는지, 요구한 결과물이 생산되었는지 등 보안과 프라이버시 요구항목을 만족하는지 판단하는 단계이다. 평가팀을 선정하여 평가 계획을 세우고 이를 리뷰하여 승인한다. 선정된 평가 계획에 따라 보안과 프라이버시를 평가하여 기록하고 보완이 필요한 항목은 보완하여 업데이트 하는 단계이다.

3.5.2 해상 사이버보안 형식승인에서의 평가 단계

RMF의 평가 단계는 한국선급의 사이버보안 형식승인 절차에서의 리스크 평가와 유사하다. 사이버보안 형식 승인의 리스크평가는 한국선급이 사이버보안 형식승인을 인증하기 위한 시험 단계로 소프트웨어 시험절차서, 리스크 평가 보고서 등의 문서를 근거로 리스크 평가를 한다. 평가 단계의 실례를 들어 설명하면, SecuAider에서의 리스크 평가는 취약점을 시험하는 자동화 도구, 자체 점검 툴 개발, 수동 방식 등으로 수행하였다. Fig. 3.은 SecuAider에서의 리스크 조치 이행 전후 결과를 나타낸 그림으로 y축은 통제 항목에 대한 수를 나타내며, x축은 리스크의 점수를 나타낸다. 리스크의 점수는 자산의 중요도, 위협 취약성, 발생 가능성을 산술적으로 계산한 값으로 한국선급에서는 리스크 점수가 9 이상이면 조치가 필요한 항목으로 식별하며, 이에 대해 이행조

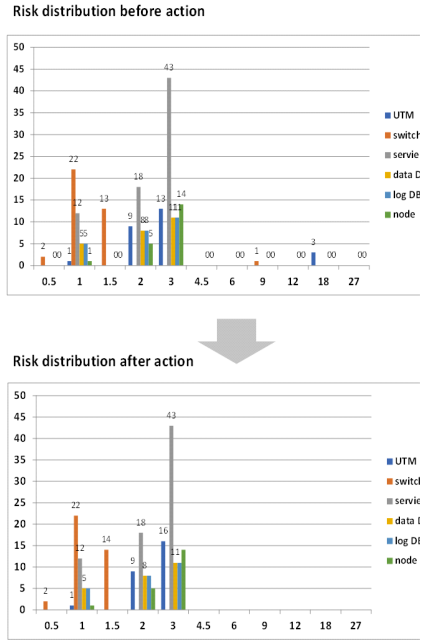


Fig. 3. Risk distribution before and after action

치 계획서를 작성하고 조치를 통해 리스크 점수가 4.5 이하가 되도록 조치하는 것을 권고하고 있다.

3.6 승인(Authorize) 단계

3.6.1 RMF에서의 승인 단계

RMF의 승인 단계는 보안, 프라이버시 리스크가 기본통제의 사용 또는 시스템의 동작에 기반하여 받아들일 수 있는지를 결정하여 승인을 하는 단계이다.

3.6.2 해상 사이버보안 형식승인에서의 승인 단계

한국선급에서는 요구되는 산출물을 심사하고 실제 구현된 시스템을 시험평가하여 형식승인을 인증한다. 각 단계에서 요구되는 산출물은 구성품 간 인증 매커니즘, 시스템 도면, 시스템 토폴로지, 자산목록, 기능사양 명세서, 사용자 매뉴얼, 소프트웨어 절차서, 리스크 평가 보고서 등이 있다. 본 논문에서 언급하는 SecuAider는 이러한 사이버보안에 대해 개발 전단계의 검증을 통해 사이버보안 형식승인을 획득하였다.

Fig. 4.는 SecuAider에 대한 한국선급의 사이버보안 형식승인 인증서이며, 인증서는 2년마다 갱신을 해야한다.


CYBER SECURITY TYPE APPROVAL CERTIFICATE

Certificate No. : CCTCS-0002-20 Initial Approval : 4th Nov. 2020

Product : SecuAider (Cyber Security Compliance Solution)

Applicant : Hanwha Systems Co., Ltd
111, Pangyoyeok-Ro, Bundang-Gu, Seongnam-Si, Gyeonggi-Do, 13524, Korea

Product Description : Cyber Security Compliance Solution
Type : SecuAider
• Manufacturing Plant
246, Igongjeom-ro, Gumi-si, Gyeongsangbuk-do, 39078, Korea
• See Appendix 1 *

Approval Condition : * See Appendix 1 *

THIS IS TO CERTIFY that the above-mentioned product has been approved in accordance with the relevant requirement of this Society's Rules and / or of the recognized standards as follows and entered in the "List of Approved Manufacturers and Cyber Security Type Approved Equipment".
Guidance for Type Approval of Maritime Cyber Security.

This Certificate is valid until 3rd Nov. 2023
Issued at Busan, Korea on 4th Nov. 2020

KOREAN REGISTER OF SHIPPING
General Manager of Cyber Certification Team

Fig. 4. SecuAider Type Approval Certificate

3.7 모니터(Monitor) 단계

3.7.1 RMF에서의 모니터 단계

RMF에서의 모니터 단계는 시스템과 조직의 보안과 프라이버시 통제항목에 대해 진행되고 있는 상황을 인식을 모니터링하는 단계이다. 모니터링 전략에 따라 동작 환경, 통제항목 평가, 프로세스 모니터링 등 실시간 리스크 관리가 수행되어지는 단계이다.

3.7.2 해상 사이버보안 형식승인에서의 모니터 단계

한국선급의 모니터 단계로는 사이버 형식승인의 위해서 주기적인 평가를 통해 인증서를 갱신하는 단계가 유사하다고 볼 수 있다. 또한 시스템 개발이 완료되고 최종 사이버보안 형식승인을 획득하였더라도 시스템의 구성요소 변경, 소프트웨어의 업데이트가 되면 사이버보안 형식승인을 다시 받아야 한다. 이러한 맥락에서 RMF의 모니터링 단계와 비슷하다고 볼 수 있다. 이와는 별개로 한국 선급은 제조사에게 새로운 사이버 위협에 대해 주기적인 취약점을 점검할 것을 권고하고 있다. 사이버보안 형식승인을 획득하였다고 하더라도 사이버보안 사고 발생 시에는 제조사의 책임이기 때문이다. 사이버보안 형식승인은 요구되는 사이버보안에 맞게 개발된 것을 인증하는 것이지 인증 제품이 사이버위협에 안전하다는 것을 보증하는 것은 아니기 때문이다. 이러한 권고사항에 맞게 주기적인 사이버 취약점을 점검하기 위한 실제 예를 설명하면 SecuAider에서는 주기적인 사이버 취약점 점검 방식은 다음과 같다.

1) 취약점 점검 자동화 도구

취약점 진단을 위한 취약점 분석 자동화 도구 중 OS 취약점 분석을 위해 Paws Studio[8]와 네트워크 장비의 보안 취약점을 위해 Nipper Studio[8]를 사용하였다. Paws Studio와 Nipper Studio는 사이버보안의 주요기관인 CIS, NIST, SANS, NSA, NERC 등의 정책을 지원하는 도구이다.

Fig. 5.는 취약점 점검자동화 도구인 Nipper Studio를 이용하여 SecuAier의 구성품인 UTM을 점검한 결과이다. 미국 국방성의 DISA(Defense Information Systems Agency)에서 작성한 구성 표준인 STIG(Security Technical Implementation Guide) 항목을 점검한 것으로 상당 수가 수동 점검 항목으로 나타나 있다. 이러한 항목은 사용하지 않는 포트 차단과 같이 보안 정책 여부를 자동화 점검도구가 판단할 수 없는 항목이며, 실패인 항목은 자동화 도구가 지원하지 않는 UTM 모델인 경우 UTM 설정 정보를 정확히 수집을 못한 경우이다.

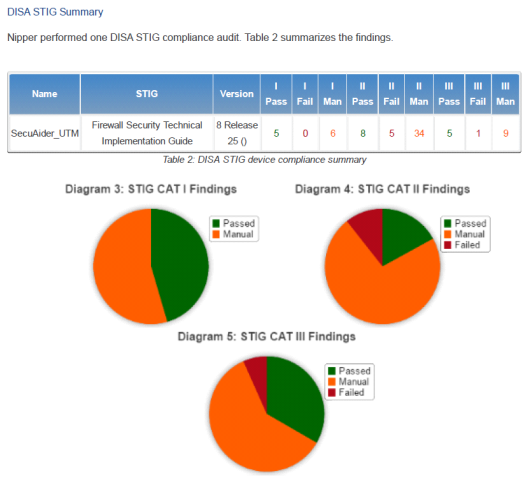


Fig. 5. Vulnerability check result using Nipper

2) 취약점 점검 자체 개발

상용 자동화 도구는 지원되는 OS 버전이나 해당하는 장비 이외는 정확한 점검결과 나오지 않기 때문에 본 논문에서 적용하는 시스템인 Ubuntu 18.04의 취약점 점검 툴을 개발[9]하여 적용하였다. 개발한 취약점 점검 프로그램은 정책 간의 공통점을 파악하여 해당 기능을 재사용하는 점검도구를 구현하였으며, 이를 통하여 변하는 기술에 발맞추어 점검도구 역시 변경 가능한 장점이 있다.

3) 수동 점검

취약점 자동화 도구을 이용한 점검 결과는 CIS, NIST 등의 주요기관 보안 정책 항목에 대해 통과(pass) 또는 실패(fail)로 결과가 나오는 경우도 있지만 수동점검(manual) 항목으로 결과가 나오는 항목이 있다. 이러한 경우는 실제적으로 운용환경 및 내부적 정책에 맞게 수동으로 점검해야 한다. 예를 들면 네트워크 분리, 불필요한 서비스 제거, 계정 정책에 대한 평가 항목 등이다. 취약점에 점검에 관련된 내용은 위와 같은 방식으로 취약점 점검으로 수행되었음을 예로서 설명하는 것이지 어떤 방식을 점검을 할 것인지는 제조사가 결정하여야 한다.

IV. 결 론

본 논문에서는 해상 사이버 형식승인에 대한 인증과정과 미국의 RMF 단계를 비교함으로써 시스템 개발 전주기에 사이버보안 요소가 어떻게 반영되는지와 어떠한 유사성이 있는지에 대해 연구하였다. 또한 시스템 개발 전주기에 사이버보안 요소를 고려한 하나의 예로서 SecuAider 개발 시 해상 사이버 형식승인 획득 과정에 필요하였던 절차 및 내용을 구체적인 예로 설명하였다. 본 논문은 여러 분야에서 요구하는 사이버보안은 시스템 개발 전주기에 관리되어야 한다는 관점에서 절차상의 유사성 및 단계별 사이버보안 결과에 대한 유사성을 분석한 것이지, 각 분야에서 요구하는 구체적인 사이버보안 요구항목에 대한 유사성을 비교 분석한 것은 아니다. 결론적으로 과거에는 기능 및 성능 위주 방식으로 시스템이 개발되었다면, 최근에는 사이버보안 요소가 시스템 개발에 필수적인 요소가 되었으며, 사이버보안은 시스템의 요구사항 분석 단계부터 설계, 개발, 시험, 운용 및 폐기에 이르는 전단계에 사이버보안 요소가 적용되어야 한다는 것이다. 이러한 점에서 사이버보안 형식승인은 RMF와 같이 개발 전단계별로 구분하여 수행해야 하는 절차를 명시하고 있지 않지만 개발 전단계에 대해 사이버보안 요소 적용하는 관점에서 유사성이 있음을 확인하였다. 또한 본 논문에서는 하나의 시스템이 해상 사이버 형식승인을 획득하는 과정에서 필요한 사이버보안 요소에 대해 구체적인 예를 들어 설명함으로써 유사성 내용에 대한 이해를 돕고자 하였다. 추후 연구로서는 산업 분야별 보호 통제 항목의 구체적인 요구사항을 비교하여 각 산업 분야간 상호 인정할 수 있는 사이버보안 요구사항을 도출하고자 한다.

References

[1] Seungmok Lee, "A study on the application of RMF for weapon systems in Korea: weapons and security system integration," Institute of Defense Acquisition program, Jornal of Advances in Military Studies, Vol. 4, No. 3, pp.191-208, Dec. 2021

[2] "IMO International Maritime Organization Policy Trends", Korea Maritime Institute. Aug. 2018. vol 7.

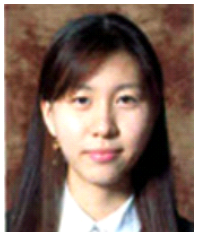
[3] "Automotive Cyber Security Guidelines," Ministry of Land, Infrastructure and Transport and Korea Transportation Safety Authority, Dec. 2020

[4] Cho Hyun Suk, "A Case Study on the Application of RMF to Domestic Weapon System," master's

thesis, Korea University, Feb. 2020
〔5〕 wikipedia, "Korean Register", https://ko.wikipedia.org/wiki/%ED%95%9C%EA%B5%AD%EC%84%A0%EA%B8%89, Nov. 2021
〔6〕 "Maritime Cybersecurity Systems Guidelines," Korean Register, Apr. 2019
〔7〕 "Maritime Cybersecurity Type Approval Guidelines," Korea Register, Apr. 2019
〔8〕 TITANIA, "Nipper, Paws" https://www.titania.com, Nov. 2021
〔9〕 Jina Hong, Seyong Hwang, Suwon Lee and Jaeyeon Lee, "Implementation of Reusable Technical Risk Assessment Tool to Reinforce Cybersecurity", 2020 KIMST, P 2-16, Nov. 2020
〔10〕 "Detailed guide to analysis and evaluation of technical vulnerabilities of major information and communication infrastructure," Korea Internet & Security Agency, Jun. 2018

〈저 자 소 개〉

이 수 원 (Suwon Lee) 정회원
2005년 8월: 충남대학교 컴퓨터공학과 졸업
2007년 8월: 충남대학교 컴퓨터공학과 석사
2007년 12월~현재: 한화시스템 수석연구원
〈관심분야〉 정보보호정책, 사이버리스크 평가, 사이버 능동방어



황 세 영 (Seyoung Hwang) 정회원
2007년 2월: 성균관대학교 전자전기공학과 졸업
2006년 12월~현재: 한화시스템 전문연구원
〈관심분야〉 정보보호, 해상 사이버보안, 사이버 능동방어

홍 진 아 (Jina Hong) 정회원
2015년 2월: 충남대학교 컴퓨터공학 학사
2017년 2월: 한국과학기술원 정보보호대학원 석사
2019년~현재: 한화시스템 선임연구원
〈관심분야〉 정보보호, 컴퓨터공학

김 병 진 (Byeong-jin Kim) 정회원
2008년 2월: 경희대학교 컴퓨터공학 졸업
2007년 12월~현재: 한화시스템 전문연구원
〈관심분야〉 정보보호, 컴퓨터공학