Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.34, NO.5, Oct. 2024 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2024.34.5.1149

선박의 사이버 복원력 통합 요구사항(IACS UR E26)과 기존 사이버보안 및 사이버 복원력 프레임워크의 비교

김 진,[1†] 이 삼 열[2‡]
[1,2]연세대학교 (대학원생, 교수)

A Study on the Comparison of the United Requirement for Cyber Resilience of Ships (IACS UR E26) with Existing Cybersecurity and Cyber Resilience Frameworks

Jin Kim,[1†] Sam Youl Lee[2‡]
[1,2]Yonsei University (Graduate student, Professor)

요 약

스마트 선박 건조량의 급증과 함께 선박 IT 기자재의 비중이 증가하면서, 해양 사이버 사고의 빈도와 심각성 또한 크게 증가하고 있다. 국제선급협회(IACS)는 이러한 상황을 인식하여 최근 UR E26 규정을 발효하였다. 본 연구는 사이버 복원력의 정의와 기존 연구를 조사하고, AHP 기법을 이용하여 UR E26 규정에서 제시하는 선박 생애주기에 따라 요인 간 우선순위를 파악한다. 또한 UR E26 규정을 미국 표준기술연구소의 사이버보안 프레임워크 및 사이버 복원력 시스템과 비교 분석하였다. 이를 통해, 선박 사이버보안에 대해 익숙하지 않은 기업들이 UR E26 규정을 효과적으로 대응하도록 지원하고, 나아가 E26 규정의 개선 방향을 제언하였다.

ABSTRACT

With the rapid increase in the construction of smart ships and the growing proportion of IT equipment on vessels, the frequency and severity of maritime cyber incidents have significantly escalated. Recognizing this situation, the International Association of Classification Societies recently enacted the UR E26 regulation. This study investigates the definition of cyber resilience and reviews existing research, using the Analytic Hierarchy Process to determine the priority of factors across the ship lifecycle as presented in the E26 regulation. Additionally, the E26 regulation is compared and analyzed against Cybersecurity Framework and Cyber Resiliency System of the NIST. Through this analysis, the study aims to assist companies that are unfamiliar with maritime cybersecurity in effectively responding to the IACS UR E26 regulation and proposes recommendations for the improvement of the UR E26 regulation.

Keywords: Ship, Cyber Resilience, Cybersecurity, IACS UR E26, Framework

Received(08. 13. 2024), Modified(09. 03. 2024), Accepted(09. 03. 2024)

† 주저자, jin@cytur.net
‡ 교신저자, samyoul@yonsei.ac.kr(Corresponding author)

I. 서 론

최근 몇 년간 해양 산업은 정보통신기술(ICT)의 비약적인 발전과 함께 큰 변화를 맞이하고 있다. ICT 기반 선박, 즉 스마트 선박의 도입은 선박 운영의 효율성을 극대화하고, 실시간 데이터 모니터링 및 분석을 통해 항해 안전성을 크게 강화하고 있다. 최근 대한민국 중소기업부의 2024 미래형 선박 보고서에 따르면, 전 세계 스마트 선박 건조량이 2021년부터 $13.84B으로 매년 평균 4.57%의 성장률을 기록하고 있으며, 2027년에는 $18.1B 규모로 예상되었다. 이뿐 아니라, 선박 내에는 GPS, AIS(자동식별 시스템), ECDIS(전자 해도 정보 시스템) 등 다양한 첨단 기술을 활용한 선박 IT 기자재가 구성되는데, 선박 IT 기자재의 비중 또한 2017년 32.4%에서 2025년까지 36.5%로 증가할 것으로 예측되었다[1].

이와 같은 선박 IT 기술의 진보는 선박 공격 표면 증가로 이어지고, Fig.1과 같은 해양 산업에서 사이버 공격의 빈도와 심각성 증가에 큰 원인을 제공한다. 사이버 공격은 정보 유출 뿐 아니라 선박 운영에 직접적인 영향을 미치며, 경제적 손실, 화물 손실, 운영 중단 등을 초래하고 있다[2].

위 추세에 따라, 국내외 조선·해양 산업에서는 사이버보안의 중요성을 인식하고, 다양한 규제와 법안을 발표하였다. IEC/ISO는 2022년에 선박 항해·통신 시스템의 사이버보안을 포함한 표준을 제정하였고, 미국 해양경비대(USCG)는 2021년부터 해양 사이버보안 위협 인텔리전스 체계를 구축하였으며, 선박 사이버보안 조사 권한을 확대하고 강제화하였다. 또한 International Association of Classification Societies(IACS)는 선박 사이버 복원력에 관한 UR E26, E27을 발의하여 2024년 7월 이후 계약되는 선박에 대해 사이버 복원력을 필수적으로 갖추도록 강제화하였다.

따라서, 본 연구는 선박 사이버 복원력(IACS UR E26)의 구조와 특징을 분석하고, NIST 사이버보안 프레임워크의 통제 항목과 E26의 요구사항을 비교·분석한다. 아울러, NIST 사이버 복원력 프레임워크와의 비교를 통해 E26의 한계를 파악하고, 이에 대한 발전 방향을 제언한다.

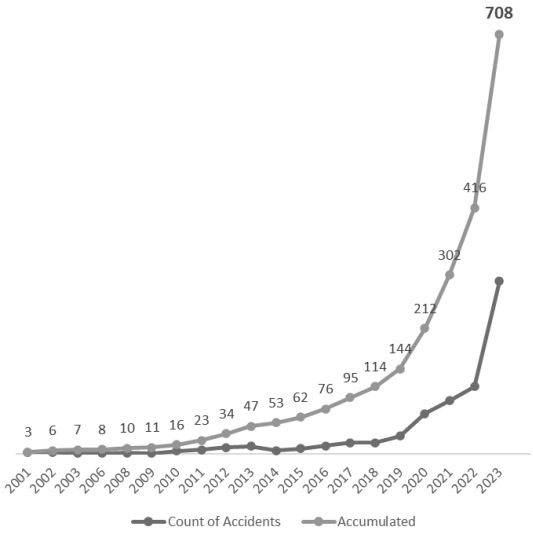

Fig. 1. Maritime Cyber Accidents Trends[2]

II. 이론적 배경 및 문헌 조사

2.1 사이버 복원력의 정의와 역량

우선 복원력이란 물질이 원래의 형태로 되돌아가거나 원래의 형태를 재개할 수 있는 능력을 의미한다. 그리고, 사람들이 어려움에서 다시 회복할 수 있는 능력을 의미하며, 더불어 어려운 상황에서도 계속 수행할 수 있는 능력을 의미한다[3]. 또한, Bjorck(2015)는 '복원력을 시스템이 충격을 받은 후 다시 회복되어 정상적인 가치 제공 수준으로 돌아갈 수 있는 기능'으로 정의했다[4].

Madni(2019)는 복원력의 4가지 역량에 대해 Fig.2과 같이 설명한다[5]. 첫째, Avoid는 시스템의 중단을 방지하기 위한 예측 기능으로, 사고를 피하고자 결과를 미리 예견하고 사전 조치를 취할 수

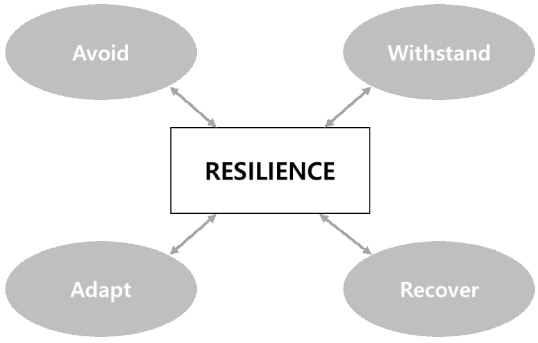

Fig. 2. Four Capabilities of Resilience[5]

있는 기능이다. 둘째, Withstand는 중단을 견디는 것으로, 시스템의 견고성 즉 시스템 중단에 대응하기 위해 시스템 스스로를 재구성할 필요 없이 스스로 중단을 견딜 수 있게 하는 것이다[6]. 셋째, Adapt는 예기치 않은 변화에 적응하기 위해 형태나 상황을 재구성하는 역량이다. 마지막으로, Recover는 중단으로부터 복구하는 것으로 시스템 중단 전 상태에 최대한 가깝게 복원할 수 있는 역량을 의미한다.

미국 국가 안보 연구 기관 MITRE는 사이버 복원력에 대해 기본적인 복원력의 개념을 기반으로, 사이버 위협을 해결하기 위한 사이버보안의 특징과 확실한 임무 완수의 특성을 결합하는 의미로 정의하고, 세 가지 영역의 각 고유한 특징을 융합하는 것으로 정의한다[8]. 즉, 사이버 상에 존재하고 있는 위협과 위험을 강조하고 이를 해결하기 위한 사이버보안과, 예측하고 견디며, 회복하고 적응하는 목표를 수립하는 복원력, 더불어 시스템의 운영 중에 조직의 미션 필수 기능을 수행하는 데 중요한 인력, 장비, 시설, 네트워크, 정보 및 정보 시스템, 인프라 및 공급망을 포함한 기능 및 자산의 지속적인 기능 및 복원력을 보호하고 보장하여 성공적인 임무 완수 기능을 모두 수행하는 것이 사이버 복원력의 핵심이라고 강조했다.

2.2 사이버보안에서 사이버 복원력으로 확장

일반적인 사이버보안의 목적은 '위험이나 위협으로부터 자유로운' 상태가 되는 것이다. 반면, 사이버 복원력 관리의 목적은 시스템 복구가 핵심이다. 이는 복원력 관리가 '위험 또는 위협으로부터 완벽하게 자유로운' 시스템 상태가 불가능하다는 것에 대한 반증을 의미한다[9]. Table 1은 사이버보안과 사이버 복원력의 특징을 비교하여 설명하였다[10].

Table 1. Characteristics of Cybersecurity vs. Cyber Resilience[10]

Aspect	Cybersecurity	Cyber Resilience
Objective	Protect IT systems	Ensure business delivery
Intention	Fail-safe	Safe-to-fail
Approach	Apply security from the outside	Build security from within
Architecture	Single layered protection	Multi layered protection
Scope	Atomistic, one organization	Holistic, network of organizations

사이버보안은 주로 IT 시스템을 외부로부터 지켜내고, 특정 조직이나 전문 인력들이 관리한다. 이에 반해, 사이버 복원력은 임무 완수를 목적으로 하여 시스템이 망가져도 안전하도록 조치하고 전 조직이 다양한 계층으로 입체적으로 관리하도록 권장한다.

2.3 프레임워크 소개

본 연구에서는 여러 산업에서 범용적으로 사용되는 NIST의 사이버보안 프레임워크와 NIST 사이버 복원력 프레임워크를 소개한다.

2.3.1 National Institute of Standards and Technology, Cybersecurity Framework

2014년 2월, 오바마 정부는 "행정명령(Executive Order 13636, 2013.02)"을 통해 국토안보부 주도로 국립표준기술연구소(National Institute of Standards and Technology, NIST)를 통해

Table 2. NIST Cybersecurity Framework[12]

Function	Category
Govern	Organizational Context
	Risk Management Strategy
	Roles, Responsibilities, and Authorities
	Policy
	Oversight
	Cybersecurity Supply Chain Risk Management
Identify	Asset Management
	Risk Assessment
	Improvement
Protect	Identity Management, Authentication, and Access Control
	Awareness and Training
	Data Security
	Platform Security
	Technology Infrastructure Resilience
Detect	Continuous Monitoring
	Adverse Event Analysis
Respond	Incident Management
	Incident Analysis
	Incident Response Reporting and Communication
	Incident Mitigation
Recover	Incident Recovery Plan Execution
	Incident Recovery Communication

Cybersecurity Framework(CSF)를 개발하여 발표하였다[11]. NIST CSF의 6가지 핵심 기능 요소는 Table 2와 같이 사이버보안 위험 관리에 대한 기본적이고 직관적인 전략적 관점을 제공한다[12]. 첫째, Govern은 조직의 사이버보안 위험 관리 전략 및 정책을 수립하고 소통하며 관리한다. 둘째, Identify는 조직의 자산, 데이터, 시스템, 네트워크를 이해하고 관리하여 사이버보안 위험을 관리하는 데 필요한 중요한 정보를 식별한다. 셋째, Protect는 사이버보안 사건이 발생하지 않도록 예방하기 위해 적절한 보호 조치를 수립하며, 이를 통해 주요 인프라와 데이터를 보호한다. 넷째, Detect는 사이버보안 위협을 신속하게 탐지하고 대응하기 위해 이상 징후 및 보안 사건을 감지하는 시스템과 프로세스를 구현한다. 다섯째, Respond는 탐지된 사이버보안 사건에 효과적으로 대응하기 위해 대응 계획을 수립하고 실행하며, 발생한 보안 사건의 영향을 최소화한다. 마지막으로, Recover는 사이버보안 사건으로부터 복구하고 정상 운영 상태로 복귀하기 위해 복구 계획을 마련하며, 이를 통해 조직의 복원력과 지속 가능성을 보장한다.

2.3.2 National Institute of Standards and Technology, Cyber-Resilient Systems

NIST는 2019년 11월, NIST SP 800-160 Vol. 2: Developing Cyber Resilient Systems: A Systems Security Engineering Approach을 발표하면서, 복원력 공학에 기반한 지속적인 생존성과 높은 신뢰성을 갖춘 사이버 복원력 시스템 개발의 필요성에 대해 강조하였다. NIST의 Cyber-Resilient Systems(CRS)는 기본적인 복원력의 핵심 요소 4가지를 Table 3과 같이 사이버 복원력의 핵심 목표로 정의하고, 시스템 수준, 임무 및 비즈니스 프로세스 수준, 조직 수준의 위험 관리 의사 결정 간 연계 기능을 제공한다[13].

NIST는 Cyber Resilient System을 구성하며, Madni의 모델을 인용했고, 사이버 측면에서 재해석했다. 첫째, Anticipate는 사이버 공격이나 기타 악의적인 활동을 사전에 인지하고 대비하기 위해 시스템 및 네트워크의 취약점을 식별하며, 잠재적인 위협을 예측하는 것이다. 둘째, Withstand는 사이버 공격이 발생했을 때 시스템이 해당 공격에 견디고 운영을 지속할 수 있도록 보장하는 것이다. 셋째,

Table 3. Cyber Resilience Goal[13]

Goal	Description
Anticipate	Maintain a state of informed preparedness for adversity.
Withstand	Continue essential mission or business functions despite adversity.
Recover	Restore mission or business functions during and after adversity.
Adapt	Modify mission or business functions and/or supporting capabilities in response to predicted changes in the technical, operational, or threat environments.

Recover는 사이버 공격이나 시스템 장애로부터 신속하게 복구하여 정상 운영 상태로 돌아갈 수 있도록 하는 것이다. 넷째, Evolve는 사이버 위협 환경의 변화에 따라 지속적으로 보안 전략과 시스템을 개선하고 발전시키는 것이다. 이 네 가지 목표는 조직이 사이버 위협에 대응하고, 공격을 견디며, 피해를 최소화하고, 빠르게 복구하는 능력을 강화하는 데 중점을 둔다. 나아가, 4개의 사이버 복원력 목표는 더욱 구체적인 8개의 Sub-objectives로 Fig. 3와 같이 연결되어, 대상 조직의 사이버 복원력 평가를 가능하게 한다. Table 4는 CRS의 Sub-objectives에 대해 설명한다.

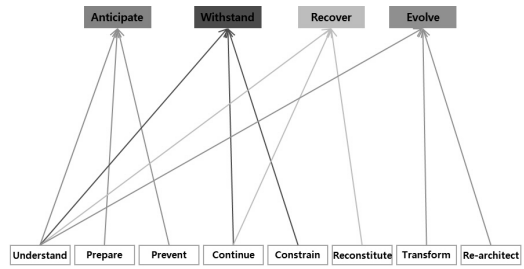

Fig. 3. Cyber Resiliency Goals and Objectives[13]

2.4 선박 사이버 복원력 규정

해양 산업의 사이버 사고 증가로 인해 해양 산업 관련 정책 전문가들은 사이버 위험 관리의 필요성을 인지하게 되었다. 즉 안전한 해양 산업의 운영을 위해 사이

Table 4. Cyber Resiliency Sub-objectives[13]

Sub-objectives	Description
Prevent or Avoid	Preclude the successful execution of an attack or the realization of adverse conditions.
Prepare	Maintain a set of realistic courses of action that address predicted or anticipated adversity.
Continue	Maximize the duration and viability of essential mission or business functions during adversity.
Constrain	Limit damage from adversity.
Reconstitute	Restore as much mission or business functionality as possible after adversity.
Understand	Maintain useful representations of mission and business dependencies and the status of resources with respect to possible adversity.
Transform	Modify mission or business functions and supporting processes to handle adversity and address environmental changes more effectively.
Re-architect	Modify architectures to handle adversity and address environmental changes more effectively.

버 위협에 적극 대응하는 사이버 복원력과 사이버보안을 보장하는 것이 얼마나 중요한지 확인하였다[14].

2016년 1월, Baltic and International Maritime Council(BIMCO)은 Guidelines on Cyber Security Onboard Ships을 발표하였다[15]. 이는 가장 빠른 해양산업의 사이버보안 가이드라인으로, IMO(국제해사기구)의 사이버 위험 관리 지침과 연계하였고, ISM Code(국제안전관리코드) 요구사항을 지원한다. 문서의 주된 목적은 사이버보안의 기술적 측면을 설명하기보다는 사이버보안에 대한 기본적인 이해와 인식을 높이기 위해 작성되었다. 2017년 6월, International Maritime Organization(IMO)의 Maritime Safety Committee(MSC)는 해양 산업 내 이해관계자들이 사이버 위험, 위협 및 취약성에 대한 인식을 높일 필요성을 인식하고 결의안 MSC.428(98)을 발표하였다[16]. 주요 요구사항에는 International Safety Management Code(ISM)에서 정의한 기능적 요구사항을 수행하는 것과 모든 선주들이 2021년 1월 이후부터 사이버 위험 관리 절차를 기존 SMS에 통합하는 것이 포함되었다. 2020년 4월, International Association of Classification Societies (IACS)는 Rec. 166 - Recommendation on Cyber Resilience를, 2년 후에는 UR E26 Cyber resilience of ships과 UR E27 Cyber resilience of on-board systems and equipment를 발표하면서, 선박의 사이버 복원력에 대해 거듭 강조하였다[17]. UR E26은 선박의 사이버 복원력 강화를 위해 온보드 시스템과 네트워크가 연결된 모든 목표 기반 접근 방식을 사용하여 전체 위협 표면을 관리하도록 권고하였다. UR E27은 선박 기자재 업체들을 위한 사이버 복원력 강화를 위한 시스템과 장비를 제공하는 데에 필요한 기본적인 요구사항들을 언급하였다.

III. 연구 설계

본 연구에서는 Analytic Hierarchy Process 기법을 이용하여 E26 규정이 제시하는 선박 생애주기에 따라 핵심 요인 간 우선순위를 파악한다. 또한 E26을 NIST의 사이버보안 프레임워크 및 사이버 복원력 시스템과 비교 분석한다.

3.1 IACS UR E26 분석

E26은 Identify, Protect, Detect, Respond, Recover 5개의 요소를 기준으로 요구사항이 구성되어 있으며, System Integrator와 Shipowner 역할과 Design - Construction - Commissioning - Operation에 이르는 선박의 생애주기로 구분되어 있다. IACS는 선박의 인증을 주관하는 선급에도 선박의 생애주기별 Phase에 따라 요구사항을 수행하고 해당 문서를 제출하도록 Table 5와 같이 안내한다. 이에 본 연구에서는 선박 사이버보안 전문가를 대상으로 하는 설문 조사를 수행한다. 이를 위해 Analytic Hierarchy Process(AHP) 기법을 활용하여, 선박 사이버 복원력에 필요한 평가 요인들의 선박 생애주기별 Phase에 따른 상대적 중요도를 도출하고 이를 바탕으로 요인 간의 우선순위를 확인한다.

AHP는 의사결정의 목표 또는 평가기준이 다수이며 복합적인 경우, 상호 배타적인 대안의 체계적인 평가를 위한 의사결정지원기법 중의 하나이다. AHP 기법은 의사결정 과정에서 인간의 뇌가 단계적으로 계층제적 분석과정을 이용한다는 점에 착안하여 개발

Table 5. UR E26 Requirements by Sub-goals[17]

Sub-goals	Requirements	Systems integrator			Shipowner			
		Design	Construction	Commissioning	Operation	First annual survey	Annual survey	Special survey
Identify	Vessel asset inventory	O	O	O	O	O	O	O
Protect	Security Zones and Network Segmentation	O	O	O	O	O	O	O
	Network protection safeguards			O	O			O
	Antivirus, antimalware, antispam and other protections from malicious code	O	O	O	O	O	O	O
	Access control	O	O	O	O	O	O	
	Wireless communication	O	O	O	O			O
	Remote access control and communication with untrusted networks	O	O	O	O	O	O	O
	Use of Mobile and Portable Devices	O	O	O	O	O	O	O
Detect	Network operation monitoring			O	O	O	O	O
	Verification and diagnostic functions of CBS and networks			O	O	O	O	
Respond	Incident response plan	O			O	O	O	
	Local, independent and/or manual operation	O		O	O			O
	Network isolation	O		O	O			O
	Fallback to a minimal risk condition	O		O	O			O
Recover	Recovery plan	O		O	O	O	O	
	Backup and restore capability			O	O			O
	Controlled shutdown, reset, roll-back and restart	O		O	O			

Table 6. Survey Participants

Category	Company	Experience
Shipyard	Company A	26 years
		16 years
		20 years
	Company B	22 years
Ship System Integrator	Company C	26 years
		17 years
	Company D	23 years
		9 years
Ship Equipment Company	Company E	18 years
	Company F	16 years
	Company G	20 years
	Company H	17 years
Ship Cybersecurity Expert Company	Company I	22 years
		18 years
		10 years
		5 years
	Company J	28 years
		12 years
Total	18 People	

되었으며, 모형을 이용하여 상대적 중요도 또는 선호도를 체계적으로 비율척도(Ratio scale)화하여 정량적인 결과를 얻을 수 있어 널리 사용되고 있다. 또한 간결한 적용 절차에도 불구하고 척도 선정, 가중치 선정 절차, 민감도 분석 등에 사용되는 기법이 실증분석과 엄밀한 수리적 검증 과정을 거쳐 채택된 방법을 활용한다는 점에서 이론적으로 높이 평가되고 있다[18].

본 설문 조사를 위해 총 18명의 전문가로 구성된 대상자를 선정하였다. 이들은 조선소, 선박 시스템 통합 업체, 선박 기자재 업체 그리고 선박 사이버보안 컨설팅을 수행하는 전문 업체 소속으로 Table 6과 같이 구성되었다.

3.2 프레임워크 비교 분석

UR E26의 기능별 요구사항을 기존의 사이버보안 평가 프레임워크인 NIST CSF 요구사항과 비교분석하여, UR E26이 기존의 사이버보안 개념을 어떻게 반영하고 있는지 개선점은 무엇인지에 관해 탐구한다. NIST CRS 평가 항목과의 비교를 통해 UR E26의 요구사항이 선박 사이버 복원력 확보에

필요한 요소들을 충분히 포함하고 있는지를 점검하고, 선박 산업에 특화된 사이버 위험 평가를 위한 요구사항 개발의 필요성에 대해 논의한다.

IV. 연구 결과

4.1 IACS UR E26 요소의 상대적 중요도 분석 결과

선박 사이버 복원력의 요소별 상대적 중요도 조사 결과는 Table 7과 같이 확인되었고, 선박 설계 단계는 Identify(0.585), Protect (0.190) 순으로 파악되었고, 선박 건조 단계는 Identify(0.538), Protect(0.246), 순으로 나타났다. 선박 시운전 단계에서는 Response(0.291), Recover(0.235) 순으로, 선박 운항 단계는 Recover(0.334), Detect(0.204) 순으로 나타났다.

조사에 참여한 조선소 관계자는 Design 단계가 자산 식별과 시스템 문서화를 위해 중요하고, Construction 단계에서는 앞서 계획한 사이버보안 조치들이 실제로 구현되었는지 확인하기 위해 Identify가 중요하다고 설명하였다. Commissioning 단계에서는 시스템의 실제 정상 작동 여부 검증을 하기 위해 Response와 Recover를 중요하게 인식하며, Operation 단계 또한 Response와 Recover를 가장 중요한 요소로 인식하여, 실제적인 사이버 복원력 대응 역량이 필요하다고 언급하였다.

따라서, 선박 사이버 복원력 향상을 위해서는, 선박 생애주기의 단계에 따라 상이한 환경과 목적을 이해하고, 이에 맞춘 구체적인 요구사항의 개발이 필요하다.

4.2 NIST CSF와 E26 비교

CSF는 2024년 2월에 Version 2.0을 발표하면서, 기존 5개 기능에 Govern을 추가하여, 6개로 구성하였다. UR E26의 통제 항목들은 CSF에 비해 구체적이지 않지만, 선박의 생애주기별로 요구사항을 구분하는 특징을 보여준다. 아래에는 CSF 기준에서 Function별로 구분하여 E26에서 언급하지 않은 부분과, CSF의 요청 내용을 비교하여 설명하였다.

CSF의 최근 버전에 추가된 Govern 기능은 E26에서는 언급되지 않지만, 조직의 사이버보안 리스크 관리 활동을 체계적으로 관리하고 통제하기 위한 전략적 방향을 설정하는 데 중점을 둔다. 또한 조직이 리스크 관리 목표와 전략을 명확히 하고 이를 지속적으로 검토하고 조정하는 과정을 강조하였다.

구체적으로 들여다보면, Identify 기능에 대해 E26은 자산 식별을 위한 기본적인 내용을 제시하고 있으나, CSF는 데이터에 대한 강조와, 사이버 위협 인텔리전스를 통한 식별, 취약성 파악 및 프로세스 준비를 비롯한 다양한 위험 평가 방법에 대해서도 제시하고 있고, 지속적인 개선 방법에 대해서도 강조하고 있다.

Protect 기능에 대해서는, E26은 보안 구역과 네트워크 구분, 접근 통제, 무선 통신, 원격 접근 등에 대해 구체적으로 제안하고 있으나, CSF는 데이터 관리 방법, 소프트웨어의 개발 수명 주기 관리, 기술적인 인프라를 통한 사이버 복원력 메커니즘에 대한 부분을 제시하여 보다 근본적인 사이버보안 전략 수립을 강조하고 있다.

Detect 기능에 대해 E26은 네트워크 운영 관리와 자산의 검증 및 분석에 대해 비교적 간단하게 제시하는 데에 반해, CSF는 다양한 방식의 이상 이벤트를 탐지하기 위한 모니터링을 강조하고 사이버 위협 인텔리전스 등의 상관관계 조사까지 요구한다.

Respond 기능에 대해 E26은 사고 대응 계획과 사고 복구에 대해 요구하나, CSF는 사고에 대응하기위한 보고서, 분석 수행에 대한 전략을 제시하고, 사고 완화 전략에 대해서도 제시한다.

Recover 기능에 대해 E26은 복원 계획, 백업 및 회복 역량, 복구 절차에 대해 제시하나, CSF는 우선순위, 무결성 등에 대한 자세한 복구 전략과, 사고 복원에 대한 내외부 커뮤니케이션을 포함하여 강조한다.

Table 7. AHP Survey Analysis Results

Phase	Identify	Protect	Detect	Response	Recover	Consistency Index
Design	0.585	0.190	0.094	0.063	0.068	0.078
Construction	0.538	0.246	0.097	0.060	0.059	0.010
Commissioning	0.099	0.291	0.204	0.171	0.235	0.039
Operation	0.081	0.180	0.204	0.201	0.334	0.005

Table 8. Matching rate with UR E26 in NIST CSF(Author's compilation)

Function	Count of Subcategory	Count of E26	Matching Rate
Govern	31	0	0.0%
Identify	21	2	9.5%
Protect	22	2	9.1%
Detect	11	1	9.1%
Respond	13	2	15.4%
Recover	8	2	25.0%
Total	106	9	8.5%

그 결과, CSF를 기준으로 E26의 요구사항과의 연결은, Recover 25%, Respond 15.4%로 나타나고, 전체 106개 중에 9개 항목, 즉 8.5%만 매칭되는 것으로 Table 8과 같이 확인할 수 있다. 이는 E26이 CSF와 동일한 Function을 이용해서 구성하기는 했지만, 사이버보안에 대한 구체적인 내용은 상당 부분 다르게 구성되었다는 의미이고, 선박 기업들이 해당 프레임워크를 기반으로 위험 평가를 진행하기에는 충분하지 않을 가능성이 높아 보인다.

4.3 NIST CRS와 E26 비교

NIST CRS는 4개의 목표와 하부 8개의 하위 목표로 구분되어 사이버 복원력 평가가 수행된다. Prevent에 대해 E26은 시스템을 식별하는 차원에서 방향은 동일하나, CRS는 시스템의 보호 조치 및 통제 방법, 자산의 변경에 따른 관리적 특성, 기만 시스템 사용, 위협 인텔리전스 등의 구체적인 방법들을 제안한다.

Prepare에 대해 E26에서는 사이버 대응에 대한 조치 방안를 수립하도록 권장하고, CRS는 테스트를 통한 검증을 강조한다.

Continue에 대해 E26은 사이버 사고에 대한 대응으로 위험 감소 방안에 대해 언급하고, CRS는 지속적 운영 방안에 대해 강조한다.

Constrain에 대해 E26은 사이버 사고로 인한 손상의 복원 방법에 대해 언급하고, CRS는 사이버 사고로 인한 손상에 대한 식별, 자원 격리 및 조정, 추가 손상 방지 전략에 대해 강조한다.

Reconstitute에 대해 E26은 사이버 사고로 인한 손상으로부터의 복원 방법에 대해 언급하고, CRS는 재구성 시 보호 기능 강화, 재구성된 자원의 신뢰도를 포함하여 강조한다.

Understand에 대해 E26은 사이버 대응 사고 계획을 요구하는데 반해, CRS는 기만 시스템을 통한 공격자에 대한 이해, 위협 이벤트와 연관된 자산 상태와 복원력의 효과까지 강조한다.

Transform과 Re-Architect에 대해 E26은 별도의 언급이 없으나, CRS는 운영을 위한 정책과 사업 운영 계획을 재정의하도록 강조하고, 위험을 감소하는 시스템의 재구성을 강조한다.

그 결과, CRS를 기준으로 E26은 Continue

Table 9. Matching rate with UR E26 in NIST CRS(Author's compilation)

Objective	Count of Object	Count of E26	Matching Rate
Prevent Or Avoid	4	3	75.0%
Prepare	3	1	66.7%
Continue	3	0	100.0%
Constrain	4	2	75.0%
Reconstitute	4	2	50.0%
Understand	4	2	25.0%
Transform	2	2	0.0%
Re-Architect	2	0	0.0%
Total	26	12	53.8%

100%, Prevent 75%, Constrain은 75% 매칭이 되고, 전체 26개 중 12개 항목, 즉 53.8% 매칭되는 것을 Table 9와 같이 확인할 수 있다. 이는 E26이 사이버 복원력의 관점에서 구성되어 있어, 다수의 항목들이 유사한 방향으로 연계된다는 것을 확인할 수 있다.

4.4 종합 분석

앞서, 선박 사이버 복원력의 요소별 상대적 중요도에 대한 조사를 통해 선박의 생애주기에 맞춘 역량 기반의 요구사항 개발이 필요함을 확인하였다. 이는 선박 사이버 복원력 평가의 시작점이 될 수 있다.

E26과 기존 프레임워크의 분석 결과, CSF와 E26의 매칭율은 8.5%로, 동일한 5가지 핵심 요소를 사용하지만, 세부 항목은 상당히 상이함을 확인할 수 있었다. E26은 기술적 조치의 이행 확인에 중점을 두었으며,
CSF와 같은 근본적인 사이버보안에 대한 질문들은 포함하지 않았다.

사이버 복원력 향상을 목표로 하는 CRS와의 비교에서는 53.8%의 매칭율을 보이며, 다수 동일한 방향을 지향하는 것으로 나타났다. 반면, E26은 CRS가 제시하는 구체적인 사이버 복원력 관련 지수 관리까지는 언급하지 않았고, 정책적인 대응 방안을 일부 제시하는 수준에 그쳤다.

또한, E26은 최근 CSF 2.0에 추가된 Govern 기능과의 연계점을 파악할 수 없었으며, 기존 CSF 1.1에 포함된 네트워크 보호 방안, 악성코드 보호 방안, 통신 체계 격리, 모바일 사용과 휴대용 기기에 대한 요구사항을 언급하고 있었다.

한편, E26은 독립적인 현장에 매뉴얼을 관리해야 한다는 요구사항을 포함하고 있는데, 이는 선박의 특수성을 고려한 요구사항이다. E26의 발전을 위해서는 조선·해양의 특수성을 고려한 더 많은 사이버보안 항목들이 개발되어야 한다. 기존 프레임워크들의 특장점을 선박 사이버보안에 적용하는 연구가 앞으로 지속적으로 이루어진다면, 추후 더욱 실효성 있는 규정으로 자리매김할 수 있을 것이고, 나아가 사이버 사고 방지에 기여할 수 있을 것이다.

4.5 IACS UR E26의 발전을 위한 제언

위 분석을 통해 본 연구는 IACS UR E26의 개선을 위한 내용을 제언한다.

Table 10. Suggestions for Improvement of IACS UR E26

No.	Suggestion
1	Lack of Consideration for Ship Lifecycle Characteristics: Specific requirements tailored to the phases of a ship's lifecycle are necessary for implementing cyber resilience elements, but these are insufficiently detailed in the current guidelines.
2	Insufficient Inclusion of Core Elements for Enhancing Cyber Resilience: Although there is some mention of Recovery Point Objective and Recovery Time Objective, the overall strategy and core elements for enhancing resilience are not comprehensively addressed.
3	Omission of Latest Cybersecurity Framework Elements: The guidelines reflect the content of NIST CSF 1.0, but they fail to incorporate the latest security requirements introduced in CSF 2.0.
4	Inadequate Consideration of Ship-Specific Environmental Factors: The unique aspects of ship environments, such as complex system structures and extended operational periods, are not adequately addressed in the current guidelines.

첫째, 선박 생애주기별 특성을 고려한 구체적인 요구사항이 미흡하다. 사이버 복원력 요소의 구현을 위해서는 선박 생애주기에 특화된 요구사항이 포함되어야 하지만, 현재는 이러한 세부적인 접근이 부족한 실정이다.

둘째, 사이버 복원력 강화를 위한 핵심 요소들이 충분히 반영되지 않았다. 예를 들어, 복구 시점 목표(RPO)와 복구 시간 목표(RTO)에 대한 일부 언급은 있으나, 전반적으로 복원력을 강화하기 위한 구체적인 전략과 요소들은 누락되어 있다.

셋째, 최신 사이버보안 프레임워크 요소가 반영되지 않았다. UR E26은 NIST CSF 1.0의 내용을 반영하고 있지만, 최신 CSF 2.0에 포함된 진보된 보안 요구사항들은 여전히 포함되지 않아 최신 기준을 충분히 충족하지 못하고 있다.

마지막으로, 선박의 특수한 환경을 고려한 요구사항이 충분히 반영되지 않았다. 선박의 크고 복잡한 시스템 구조와 긴 운영 기간, 인터넷 환경 등 선박 특유의 조건을 반영한 구체적인 요구사항이 미비하여, 이를 보완하기 위한 추가적인 연구와 개발이 필

요하다. 이를 간략히 Table 10에서 제시하였다.

V. 결 론

최근 스마트 선박 건조량이 급증하고 선박 IT 기자재의 비중이 증가함에 따라, 해양 사이버 사고의 빈도와 심각성 또한 증가하고 있다. 이에 따라 조선·해양 산업에서는 사이버보안의 중요성을 더욱 인식하게 되었고, IACS는 2024년 7월 1일에 UR E26을 발효하였다. 본 연구에서는 사이버 복원력의 정의와 기존 연구를 조사하고, AHP를 이용하여 E26 규정에서 제시하는 선박 생애주기에 따라 요인 간 우선순위를 파악하였다. 또한 E26과 기존 NIST CSF, NIST CRS와 비교 분석하였다. 본 연구 결과, 선박 사이버 복원력 향상을 위해 생애주기에 따른 구체적인 요구사항의 개발 필요성을 파악하였다. 더불어, E26이 기존 CSF의 핵심 키워드를 기반으로 구성되어 있으나, 사이버보안의 근본적인 문제와 구체적인 요구사항은 미흡한 것으로 나타났다. 나아가, CRS와 전체적인 방향성에서는 유사성을 보였으나, 사이버 복원력에 대한 구체적인 지수 관리 등 세부 사항에서 차이가 확인되었다. 이 분석을 토대로, E26의 발전 방향을 제언하였다.

본 연구는 사이버보안에 대해 생소한 선박 기업들이 IACS UR E26 수행을 위해 기존 프레임워크와의 연계성을 파악할 수 있도록 지원하였고, E26의 특징을 설명하고 개선 방향을 제시했다는 점에 그 의의가 있으며, 관련 생태계 내 이해관계자들의 목소리를 더 많이 포함하지 못했다는 부분에서는 아쉬움이 남는다. 이는 더 깊은 자료 조사를 통해 선박을 위한 새로운 프레임워크 개발 연구로 진행할 예정이다.

References

[1] SME Strategic Technology Roadmap 2024~2026 Futuristic Ship, Ministry of SMEs and Startups, 2024.

[2] CYTUR, "Maritime Cyber Attack MAP", https://mcti.cytur.net, Sep 2024

[3] Oxford University Press, "Oxford English Dictionary", https://www.oed.com/ dictionary/resilience_n?tab=factsheet#25634109, 2021.

[4] Björck, F., Henkel, M., Stirna, J., Zdravkovic, J. "Cyber Resilience - Fundamentals for a Definition.", Advances in Intelligent Systems and Computing, vol. 353. p311-316, Dec 2015.

[5] M. Omer, A. Mostashari, R. Nilchiani, and M. Mansouri, "A framework for assessing resiliency of maritime transportation systems", Maritime Policy Manage., vol. 39, no. 7, p685-703, Dec 2012.

[6] A. M. Madni and S. Jackson, "Towards a conceptual framework for resilience engineering," IEEE Systems Journal, vol. 3, no. 2, p181-191, 2009.

[7] A. M. Madni, "Agile Systems Architecting (ASA): Placing Agility Where it Counts", Proceedings of Conference on Systems Engineering Research, p1-7, Dec 2007.

[8] D. Bodeau, R. Graubart, J. Picciotto, and R. McQuaid, "Cyber resiliency engineering framework," MTR110237, MITRE Corporation, 2011.

[9] Twumasi-Boakye and J. O. Sobanjo, "Resilience of regional transportation networks subjected to hazard-induced bridge damages", J. Transp. Eng., Part A, Syst., vol. 144, no. 10, p. 04018062, Oct 2018.

[10] Y. Zhou, J. Wang, and H. Yang, "Resilience of transportation systems: concepts and comprehensive review", IEEE Trans. Intell. Transp. Syst., vol. 20, no. 12, p4262-4276, Jan 2019.

[11] E. Song and W. Kang, "U.S. Obama's Second-Term Cybersecurity Policy," Korea Internet & Security Agency, Sep. 2014.

[12] NIST, "The NIST Cybersecurity Framework 2.0," Feb 2023.

[13] NIST, "Developing Cyber-Resilient Systems: A Systems Security Engineering Approach", Dec. 2021.

〔14〕 Thetius - HFW - Cyberowl, "The Great Disconnect", https://cyberowl .io/wp-content/uploads/2022/04/CyberOwl-HFW-Thetius-Cyber-Security-Report-The-Great-Disconnect-.pdf, Apr 2022.
〔15〕 Baltic and International Maritime Council, "Guidelines on Cyber Security Onboard Ships", https://www.bimco.org/ about-us-and-our-members/publications/the-guidelines-on-cyber-security-onboard-ships, Dec 2016.
〔16〕 International Maritime Organization, "Resolution IMO MSC 428(98), Maritime Cyber Risk Management in Safety Management Systems", June 2017.
〔17〕 International Association of Classification Societies, "Unified Regulation E26 Cyber Resilience of Ships - New", https://iacs. org.uk/publications/unified-requirements/ur-e/?page=2, Apr 2022.
〔18〕 S. Choi, Y. Song, K. Lee, Y. S. Hoon, and Y. Choi, "Defects in Exposed Concrete Finishing Method Using AHP Techniques" *Korea Construction Management Association, vol. 20, no. 4, p46-55, Jan. 2019.

〈저자소개〉

김 진 (Jin Kim) 정회원
2003년 2월: 인하대학교 컴퓨터공학부 졸업
2020년 2월: 서울시립대학교 경영대학원 경영정보 전공 석사
2020년 8월~현재: 연세대학교 기술경영협동과정 박사과정
2008년~2012년: ㈜봄라이브러리 대표이사
2021년~현재: ㈜싸이터 부대표
〈관심분야〉 기술경영, 사이버보안, 정보화, 조선·해양, 창업

이 삼 열 (Sam Youl Lee) 정회원
1992년 2월: 연세대학교 행정학사 졸업
2004년 Carnegie Mellon University 정책학 박사
2004년 9월~2005년 8월: 정보통신정책연구원 책임연구원
2005년 9월~현재: 연세대학교 행정학과 교수
〈관심분야〉 과학기술정책, 정책분석 및 평가