대한조선학회논문집 Research Paper
Journal of the Society of Naval Architects of Korea
eISSN:2287-7355, Vol. 62, No. 1, pp. 25-37, February 2025
https://doi.org/10.3744/SNAK.2025.62.1.25

해사 사이버 보안 규제 프레임워크 방향성 연구

박제영 · 박치병† · 박한선
한국해양수산개발원 물류 · 해사산업연구본부 해사산업 · 안전연구실

Research for Direction of Maritime Cybersecurity Regulatory Framework

Jeyeong Park · Chybyung Park† · Han-Seon Park
Korea Maritime Institute

Autonomous ships are gaining continuous attention due to their superiority in terms of efficiency, cost-effectiveness, and safety from human error. However, as autonomous navigation systems are controlled in a cyber environment, the security and accuracy of information and data are critical factors. Therefore, establishing structural safeguards that can eliminate threats such as data breaches, tampering, and forgery, which may lead to financial, social, or terror-related risks to ships and human lives, is a prerequisite for the introduction of autonomous navigation systems in the maritime industry. This study focuses on reviewing existing cybersecurity rules and regulations in the maritime sector and identifying shortcomings compared to other industries. As a result, unlike other industries with highly standardized and detailed regulations, the security maturity of shipping against cyber threats was found to be based on a fragmented regulatory framework and inadequate response procedures. In addition, the lack of uniform global regulations and the lack of cybersecurity threat information and case-sharing mechanisms were identified as problems. In this paper, a framework is developed and proposed to address these problems and strengthen cybersecurity. Through this, the study aims to contribute to the secure adoption of autonomous systems in the maritime industry by ensuring more stringent cybersecurity measures. In addition, it is expected that sustainability can be improved by regularly and continuously performing prevention and response support for cybersecurity in the shipping industry.

Keywords : Autonomous ship(자율운항선박), Cybersecurity(사이버 보안), Regulatory framework(규제 프레임워크)

1. 서 론

1.1 배경

해운 산업은 세계 무역에 필수적이며, 전체 운송의 80% 이상을 차지한다 (UN trade and development, 2022). 최근에는 디지털 기술과 스마트 시스템의 통합을 특징으로 하는 새로운 해운 운영인 Shipping 4.0이라는 개념이 점점 더 받아들여지고 있다 (Kavallieratos et al., 2020). 이러한 추세는 점점 더 복잡하고 경쟁이 치열해지는 산업에서 더 큰 효율성, 비용 절감 및 향상된 안전성에 대한 필요성에 의해 주도된다. Shipping 4.0은 사물 인터넷(IoT, Internet of Things), 빅 데이터 분석, 인공 지능(AI, Artificial Intelligence), 자동화와 같은 첨단 기술을 활용하여 해운 운영을 최적화하여 실시간 모니터링, 예측 유지 관리 및 보다 정보에 입각한 의사 결정을 가능하게 한다 (Aiello et al., 2020).

Shipping 4.0은 컴퓨팅, 네트워킹 및 물리적 프로세스를 통합하는 시스템인 사이버 물리적 시스템(CPS, Cyber Physical System)의 채택 및 사용 증가와 밀접한 관련이 있으며 (Fjørtoft and Berge, 2019), 해상 운영의 맥락에서 CPS는 선박 및 항만 인프라와 같은 물리적 해상 자산과 이러한 자산을 관리 및 제어하는 디지털 시스템 간의 원활한 상호 작용을 가능하게 한다. 이러한 통합을 통해 실시간 데이터와 자동화된 의사 결정 프로세스를 기반으로 물리적 운영이 지속적으로 최적화되는 보다 반응성 있고 적응력 있는 해상 환경이 가능해진다 (Kavallieratos et al., 2020). 그러나 CPS에 대한 의존도가 높아지면서 이러한 상호 연결된 시스템이 사이버 공격의 잠재적인 대상이 되면서 새로운 사이버 보안 문제가 발생한다.

사이버 보안은 시스템, 네트워크, 장치 및 데이터를 디지털 공격, 무단 액세스, 손상 또는 도난으로부터 보호하는 것을 일컫는다 (Craigen et al., 2014). 여기에는 멀웨어, 피싱, 랜섬웨어 및 기타 사이버 위협과 같은 위협으로부터 정보 및 기술 자산을 보

Received : 2 October 2024 | Revised : 31 October 2024 | Accepted : 20 November 2024
† Corresponding author : Chybyung Park, cbpark@kmi.re.kr
It is noted that this paper is a revised edition based on the proceedings of SNAK 2024 in Changwon

호하기 위한 조치를 구현하는 것이 포함된다. 선박, 항구 및 해양 인프라에 대한 사이버 공격은 운영을 방해하고 재정적 손실을 초래하며 국가 안보 위험을 초래할 수 있으므로 Shipping 4.0 시대의 사이버 보안은 매우 중요하다고 할 수 있다.

실제 대표적인 해사 사이버 공격으로 2017년 6월에 덴마크 글로벌 해운사인 머스크(Maersk)의 사례가 있다. 유형은 랜섬웨어를 이용한 낫페트야 공격(NotPetya Attack)으로 중요 시스템이 차단되어 2주 동안 운영이 중단되었으며 약 3억 달러의 손실이 발생한 것으로 추산되었다 (Los Angeles Times, 2017). 이런 사이버 위협의 발생에 따라 규제 기관은 산업을 보호하기 위한 프레임워크를 개발하기 시작했다 (Al Ali et al., 2021). 이 논문은 해운 산업의 사이버 보안 규정의 현재 상태에 대한 포괄적인 개요를 제공하고, 다른 운송 수단과 비교하며, 해운 사이버 보안을 강화하기 위한 프레임워크를 제안한다.

1.2 도로 교통 분야의 사이버 보안

도로 교통 분야는 커넥티드 및 자율 주행 차량의 증가로 인해 사이버 보안 규정이 상당히 발전했다 (Schmittner and Macher, 2019). 이 분야의 최신 규정은 표준, 지침 및 법적 프레임워크를 확립하기 위한 국제적, 지역적 및 산업적 노력의 조합을 포함한다. 국제 표준 및 지침 측면에서, 유엔 유럽 경제 위원회(the United Nations Economic Commission for Europe, UNECE)의 차량 규정 조화를 위한 세계 포럼 WP.29는 2021년에 채택되었다(Costantino et al., 2022). UNECE WP.29 규정은 자동차 제조업체에 대한 사이버 보안 관리 시스템을 의무화하고 제조업체의 차량 사후 생산 및 사고 대응 기능을 포함하여 수명 주기 전반에 걸쳐 사이버 보안 표준을 충족한다는 것을 입증하도록 요구한다.

유럽 연합에서 UNECE WP.29 규정은 2024년 7월부터 모든 신차에 의무화되었다 (Brandt and Tamisier, 2021). 이 규정은 EU의 보다 광범위한 일반 안전 규정의 일부로, 차량의 안전과 보안을 강화하는 것을 목표로 한다. 또한 일본에서는 UNECE WP.29 규정이 채택되었으며, 국토교통성(MLIT, Ministry of Land, Infrastructure, Transport and Tourism)이 일본 자동차 시장에서 이러한 규정의 시행을 감독하여 차량 사이버 보안 표준을 발전시키고 있다 (Roberts et al., 2023). 미국에서는 국가 고속도로 교통 안전청(NHTSA, National Highway Traffic Safety Administration) 지침이 2016년에 "현대 차량의 안전을 위한 사이버 보안 모범 사례"를 발표하여 차량의 사이버 보안에 대한 지침을 제공했다 (Das et al., 2019). 이 지침은 위험 평가, 사고 대응 및 정보 공유를 강조한다.

산업 이니셔티브 측면에서는 자동차 정보 공유 및 분석 센터(Auto-ISAC, The Automotive Information Sharing and Analysis Center)가 설립되었다. 이는 자동차 제조업체, 공급업체, 상용차 회사를 포함한 회원 간의 협업과 정보 공유를 촉진하여 자동차 부문의 사이버 보안 태세를 강화하는 글로벌 산업 주도 이니셔티브다 (Lee et al., 2020). 이 센터는 위협 인텔리전스, 취약성 정보 및 모범 사례를 공유할 수 있는 플랫폼을 제공하여 회사가 새로운 사이버 보안 위협보다 앞서 나갈 수 있도록 한다.

1.3 철도 운송 분야의 사이버 보안

철도 운송의 사이버 보안은 열차 제어, 통신, 신호 및 운영을 위한 디지털 시스템에 대한 의존도가 높아짐에 따라 중요한 문제가 되었다 (Kour et al. 2023). 이러한 과제를 인식하고 철도 운송 시스템의 회복성을 강화하기 위한 다양한 사이버 보안 규정 및 표준이 개발되었다. 국제 규정 측면에서 국제 전기 기술 위원회(IEC, International Electrotechnical Commission)는 산업 및 운송 시스템을 위한 표준을 개발했다. 특히 기존에 산업 시스템을 위해 설계되었지만, 신호 및 제어 시스템에서 철도 시스템을 포함하도록 조정된 IEC 62443은 산업 자동화 및 제어 시스템(IACS, Industrial Automation and Control Systems)의 사이버 보안을 위한 포괄적인 표준을 보여준다 (Copeland, 2020). 국제 표준화 기구(ISO)는 정보 보안 관리 및 위험 관리에 중점을 두고 철도 운송의 사이버 보안과 관련된 여러 표준을 제공하고 있다. 구체적으로 ISO/IEC 27001 표준은 정보 보안 관리 시스템(ISMS, Information Security Management System)을 수립, 구현, 유지 관리하고 지속적으로 개선하기 위한 요구사항을 지정하였다 (Tomić Rotim, 2020). ISO/IEC 27032 표준은 사이버 보안 위험의 식별 및 관리를 포함하여 사이버 공간에서의 정보 보호를 포괄하는 사이버 보안 상태를 개선하기 위한 지침을 제공한다 (Tomić Rotim, 2020).

EU는 철도 운송을 위한 포괄적인 사이버 보안 규정 개발 분야에서도 앞장서 왔다. 네트워크 및 정보 보안(NIS2) 지침은 철도 운송을 포함한 필수 서비스 운영자에게 엄격한 요구 사항을 설정하여 EU 전역의 사이버 보안을 강화하는 것을 목표로 한다 (Vandezande, 2024). EU 사이버 보안법은 유럽 연합 사이버 보안 기관(ENISA, European Union Agency for Network and Information and Security)의 역할을 강화하고 철도 시스템과 관련된 사이버 보안을 위한 EU 전역 인증 프레임워크를 수립하였다(Markopoulou et al. 2019). 또한, 기술 사양(TS) 50701은 철도 부문의 사이버 보안에 대한 지침을 제공하고 있다(Prochazka et al. 2022). 이러한 지침들을 통해 사고 보고, 위험 평가 및 보안 조치의 구현이 의무화되고 있다는 것을 식별할 수 있다. 일본에서는 일본의 사이버 보안 기본법 프레임워크에서 철도를 포함한 중요 인프라 부문이 강력한 사이버 보안 조치를 채택하도록 의무화하고 있다 (Kawaguchi. 2023). 호주에서는 Australasian Railway Association에서 개발한 Australian Rail Cybersecurity Guidelines에서 철도 운영자가 사이버 위험을 관리할 수 있는 프레임워크를 제공한다 (Kennedy et al. 2020).

산업 이니셔티브 측면에서 철도 운송의 글로벌 협회인 국제철도연합(UIC, Union International des Chemins de fer)은 사이버 보안을 위한 여러 지침과 모범 사례를 개발했다 (Soderi, Masti et al. 2023). 특히 UIC 사이버 보안 권장 사항은 신호 및 제어 시스

템 보호에 중점을 두고 다양한 수준의 철도 시스템에서 사이버 보안 조치를 구현하는 방법에 대한 지침을 제공한다. 철도 산업 표준(RIS)은 영국의 철도 안전 및 표준 위원회(RSSB)에서 개발한 RIS-3703-TOM을 제안했으며, 이는 철도 운영에서 사이버 보안 위험을 관리하는 것이 중요하며, 이를 위한 요구사항들을 식별하고 제공한다 (RSSB 2021).

1.4 항공 수송 분야의 사이버 보안

항공 산업은 통신, 항법 및 제어를 위한 복잡한 디지털 시스템에 의존하기 때문에 오랫동안 사이버 위협의 표적이 되어 왔다 (Kagalwalla and Churi 2019). 국제 민간 항공 기구(ICAO, International Civil Aviation Organization)는 사이버 보안을 포함하여 항공 안전 및 보안에 대한 표준과 규정을 수립하는 주요 글로벌 기관으로서 역할을 하고 있으며(Elmarady 및 Rahouma 2021), 특히 회원국이 공항 및 항공사를 포함한 항공 인프라 전반에 사이버 보안 조치를 구현하도록 의무화하는 사이버 보안 프레임워크를 개발하였다. 항공 시스템, 네트워크 및 데이터를 보호하기 위한 모범 사례를 설명하는 Doc 9985는 민간 항공에서 사이버 보안 위험을 관리하기 위한 포괄적인 프레임워크를 제공한다(Limnaios 2022). 마지막으로, 글로벌 항공 보안 계획(GASeP)은 글로벌 항공 보안을 강화하기 위한 로드맵의 핵심 요소로 사이버 보안을 포함하고 있으며, 국가가 ICAO 지침에 따라 사이버 보안 조치를 채택하도록 장려하고 있다 (Sena et al., 2021).

유럽 민간 항공에서 최고 수준의 안전과 환경 보호를 보장할 책임이 있는 유럽 연합 항공 안전 기관(EASA, European Union Aviation Safety Agency)은 위험 관리, 사고 대응 및 지속적인 모니터링에 대한 지침이 포함된 항공 안전 및 보안에 대한 현재 및 새로운 위협을 해결하기 위한 포괄적인 사이버 보안 전략을 개발하고 제공하고 있다. 또한, 미국에서 연방 항공청(FAA, Federal Aviation Administration)은 항공 산업의 사이버 보안 표준을 설정하는 데 중요한 역할을 하고 있으며 (De Cerchio and Riley 2011), 여기에는 운영자, 제조업체 및 서비스 제공자가 사이버 보안 제어를 구현하기 위한 지침이 포함된다. 중국에서는 민간 항공 사이버 보안 지침이 민간 항공의 사이버 보안에 대한 구체적인 지침을 도입하여 항공기 시스템, 항공 교통 관리 및 승객 데이터 보호에 중점을 두고 있다 (ICAO 2016). 산업 이니셔티브 측면에서 국제항공운송협회(IATA, International Air Transport Association)는 항공사 간 사이버 보안 인식과 모범 사례를 촉진하는 데 중추적인 역할을 한다 (Ukwandu et al., 2022). 특히 IATA 사이버 보안 툴킷은 항공사에 위험 평가 도구, 사고 대응 프로토콜 및 교육 프로그램이 포함된 효과적인 사이버 보안 조치를 구현하기 위한 리소스와 지침을 제공하고 있다.

1.5 해운 운송 분야의 사이버 보안

최근 IMO는 해운 산업을 보호하기 위해 글로벌 사이버 보안 표준을 수립하는 데 중심적인 역할을 하며 사이버 보안 프레임워크를 개발하기 시작했다 (Karim, 2022). 특히, IMO는 2017년에 "해운 사이버 위험 관리 지침"(MSC-FAL.1/Circ.3)을 채택했는데, 이는 해운 부문의 사이버 위험을 해결하기 위한 비강제적 프레임워크 역할을 한다 (Mraković and Vojinović, 2019). 이 가이드라인은 사이버 위험 관리가 기존 안전 관리 시스템의 일부가 되어야 하며, 해운 조직은 사이버 위협으로부터 보호하기 위한 조치를 구현하도록 권장하고 있다. 또한, 모든 선박과 회사가 2021년 1월 1일 이후 준수 문서의 첫 번째 연례 검증을 통해 사이버 보안을 안전 관리 시스템(SMS, Safety Management System)의 일부로 포함하도록 규정하며, 사이버 위협으로부터 운송 작업을 보호하기 위한 위험 관리 접근 방식을 채택하도록 권장한다. SOLAS 협약의 일부인 국제 선박 및 항만 시설 보안(ISPS, International Ship and Port Facility Security) 규정에서는 선박 및 항만 시설에 대한 보안 조치를 의무화하고 있다 (Melnyk et al., 2022). 주로 물리적 보안에 초점을 맞추고 있지만 최근 논의에서는 사이버 위협에 대한 고려가 진행되며 항구와 선박이 사이버 보안을 보안 평가 및 프로토콜에 통합하도록 촉구하였다.

EU에서 지침(EU) 2016/1148(NIS 지침)은 해상 운송을 포함한 중요 부문 전반의 네트워크 및 정보 시스템 보안에 중점을 두고 있으며 (Androjna, 2020), 회원국이 사이버 보안 조치를 구현하고 필수 서비스 제공에 상당한 영향을 미칠 수 있는 사고를 보고하도록 요구한다. 유럽 해사 안전 기관(EMSA, European Maritime Safety Agency) 사이버 보안 지침은 EU 회원국과 해사 이해 관계자가 효과적인 사이버 보안 조치를 구현하도록 지원하고 있다 (Androjna et al. 2022). 이러한 지침은 IMO의 프레임워크와 일치하지만 지역적 맥락에 대한 추가적인 구체성을 제공한다. 미국에서는 미국 표준 기술 연구소(NIST, National Institute of Standards and Technology) 사이버 보안 프레임워크가 해사를 포함한 미국 산업 전반에 널리 사용되어 강력한 사이버 보안 관행을 수립하고 있으며 (Erich, 2021), 물리적 보안에 초점을 맞춘 2002년 해상 운송 보안법(MTSA, Maritime Transport Security Act)은 사이버 보안 고려 사항을 포함하도록 업데이트되었다 (Finley, 2017). 싱가포르에서는 싱가포르 해사 및 항만청(MPA, Maritime and Port Authority of Singapore)이 해상 사이버 보안 지침과 사이버 사고 의무 보고(Neo, 2021)를 포함하여 해상 부문의 사이버 보안 회복력을 강화하기 위한 이니셔티브를 도입했다.

산업 이니셔티브 측면에서 가장 큰 국제 해운 협회인 BIMCO는 위험 평가, 보호 조치, 탐지, 대응 및 복구를 포함한 사이버 보안의 다양한 측면을 다루는 선박 내 사이버 위험을 관리하기 위한 사이버 보안 지침을 개발했다 (Daum, 2019). 이 외에도, Oil Companies International Marine Forum(OCIMF)에서 개발한 Tanker Management and Self-Assessment(TMSA) 프레임워크에는 사이버 보안을 다루는 특정 요소가 포함되어 있다 (Lagouvardou, 2018). 이 프레임워크에서는 탱커 운영자는 온보드 시스템과 데이터를 보호하고 탱커 함대의 안전한 운영을 보장하기 위해 사이버 보안 제어를 구현하도록 권장한다.

1.6 해운 분야의 사이버 보안 규정 평가 및 권장 사항

해운 산업 보호를 위한 규제 강화 노력에도 불구하고, 해운의 사이버 위협에 대한 보안 성숙도는 도로, 철도, 항공과 같은 다른 운송 부문에 비해 아직 미흡한 단계에 있다. 구체적으로, 도로 운송 부문에서는 사이버 위험을 완화하기 위한 선제적 조치와 수명 주기 관리에 중점을 두고 강력한 규제를 수립하고 시행하고 있다. 이와 달리 현재 해운에서는 고도로 표준화되고 세부적인 규정이 있는 도로, 항공 및 철도와 달리 단편화된 규제 프레임워크로 안전한 사이버 분야의 적용 및 활용에 어려움을 겪고 있다. 특히, IMO와 같은 국제 지침은 광범위한 반면 지역 및 국가 규정은 각 국가의 상황을 반영하여 상이하거나 미비하다. 또한 해상 운영에 맞게 특별히 설정된 표준화된 사이버 보안 조치가 없기 때문에 모범 사례가 종종 균일하게 적용되지 않아 일부 선박과 항구가 사이버 위협에 취약해질 수 있다. 더욱이 현재 규정은 종종 IT 시스템에 중점을 두고 해상 환경에서 사용되는 OT 시스템이 제기하는 구체적인 문제를 반영하지 못하여 위험을 증가시키기도 한다. 또 다른 중요한 문제는 해양 이해 관계자 간에 사이버 보안 위협 정보와 모범 사례를 공유하기 위한 공식적인 메커니즘이 부족하여 협업과 정보 공유가 부족하다는 점이다. 마지막으로, 제한된 사고 대응 및 복구 지침과 부적절한 교육으로 인해 효과적인 대응 및 복구가 방해를 받아 사고의 영향이 악화될 수 있는 문제점도 존재한다.

논문을 통해 식별된 이와 같은 문제점들을 해결하기 위해 다음과 같은 사항을 도출하고 이 논문을 통해 해결 방안을 제시하고자 한다. 첫째, 국제적, 지역적 및 국가적 규정을 조화시키는 해운 산업을 위한 통합적이고 포괄적인 사이버 보안 프레임워크를 개발하는 것이 중요하다. 이 프레임워크는 IMO와 같은 국제 기관과의 협력을 통해 다양한 관할권에서 표준화되어야 하며, 모든 이해 관계자가 따를 수 있는 다양한 사이버 보안 프로토콜과 모범 사례에서 일관성과 효과성을 보장해야 한다. 또한, 항해 시스템에서 엔진 제어에 이르기까지 모든 것을 포괄하는 해상 작업 중에 사용되는 OT 시스템의 사이버 보안에 특별히 맞춰진 규정과 지침을 제정하여 제공할 필요가 있으며, 이를 위해서는 업계 전문가가 참여하여 해양 환경에서 OT 시스템의 고유한 요구 사항과 과제에 맞는 사이버 보안 표준을 개발하고 구현해야 한다.

둘째, 선박 운영자, 항만 당국, 사이버 보안 전문가를 포함한 해양 이해 관계자 간의 협업과 정보 공유를 촉진하기 위한 공식적인 메커니즘을 개발해야 한다. 예를 들어, 실시간 위협 인텔리전스 공유를 용이하게 하는 업계 전체 포럼이나 컨소시엄을 구성하면 해양 사이버 보안 정보 공유 센터를 설립하고 글로벌 및 지역 위협 인텔리전스 네트워크 참여를 장려할 수 있다.

마지막으로, 승무원과 항만 직원을 포함한 모든 해양 인력을 대상으로 포괄적인 사이버 보안 교육 및 인식 프로그램을 표준화하고 구현하는 것이 가장 중요하다. 여기에는 피해 완화, 이해관계자와의 소통, 업계 조직 및 사이버 보안 교육 프로그램과 인증 과정을 제공하는 교육 기관과의 협력을 통한 운영 복구를 위한 명확한 단계가 포함되어야 한다.

2. 자율 선박의 사이버 보안에 대한 규칙 및 규정

2.1 IMO

IMO는 사이버 위험 취약성에 대한 상황을 인지하고 제98차 해사안전위원회(MSC, Maritime Safety Committee) 및 제41차 간소화위원회(FAL, Facilitation Committee)에서 '해상 사이버 위험관리 지침(Guidelines on maritime cyber risk management)'을 승인하였다 (IMO, 2021). '해상 사이버 위험관리 지침'의 부속서 -10은 '안전관리시스템 해상 사이버 위험관리(Maritime cyber risk management in safety management systems)'에 대한 결의안으로 2017년 6월에 채택되었고 이후 결의안 따라 IMO는 기국으로 하여금 2021년 1월 이후 시작되는 첫 번째 연차검사에서 사이버 위험에 대한 관리가 안전관리시스템에서 수행되고 있음을 나타내는 적합증서(DoC, Document of Compliance)를 비치하도록 권고하였다. IMO의 '해상 사이버 위험관리 지침'은 사이버 위협으로부터 효과적인 사이버 위험관리를 지원하기 위한 상위 수준의 기능적 요소를 포함하고 있고 선박 시스템에서 사이버 위험에 노출될 수 있는 취약 시스템은 선교 시스템, 화물 처리 및 관리 시스템, 추진 및 파워 컨트롤 시스템, 접근 제어 시스템, 여객 서비스 및 관리 시스템, 여객 접속 공용 네트워크, 선원 지원 시스템, 통신 시스템이 포함된다. IMO MSC 101차 회의에서는 자율운항선박 관련 시스템 및 기반시설의 시운전이 환경보호와 관련하여 안전하게 수행될 수 있도록 관련 당국과 이해당자사를 지원하기 위한 '자율운항선박 임시 시운전 지침(Draft integrim guidelines for MASS trials)'을 승인하였다. 이후 MSC 106차 MASS 작업반을 통해 MASS Code 개발 로드맵과(MSC 106/WP.8, Annex 5), MASS Code 구성 초안(MSC 106/WP.8, Annex 1)이 도출되었고 MASS Correspondence Group 작업으로 인해 MASS 기능에 대한 요건(MASS Code, Part.3)(안)이 도출되었으며 MASS Code는 GBS(Goal-Based Standard)체계로 개발되고 있는 중이다. 이는 자율운항선박 운용에 대한 경험이 없으며, 기술적으로도 명확하지 않은 부분이 다수 존재하여 규범적 요건을 제시하기가 어렵기 때문으로 판단된다.

나아가, 현재 선박에 집중된 사이버 보안 규정이 선박뿐만 아니라 항만과 통합적으로 이루어져야 한다는 공감대가 형성되고, 대한민국과 미국 대표단이 공동으로 IMO에 의제문서를 제출하고 규정에 반영하기 위하여 노력하고 있다.

2.2 국제항로표지협회(IALA)

IALA 이네비위원회(ENAV, ENAVigation Committee) 제24차 회의에는 IEC 62443 및 IEC 61162-460 표준에 기초한 해상 ICT 장비에 적용되는 사이버 보안 형식승인 사례와 적용 사례를 소개한 의제문서(Introduction of cyber security type approval applicable case based on IEC 62443 and IEC 61162-460

standards)가 제출었다. 이후 제27차 회의에는 '자율운항선박 개발 가이드라인(IALA guideline on developments in Maritime Autonomous Surface Ships)' 초안이 제출되었으며, MASS 환경을 지원하기 위한 가이던스 개발 우선순위 항목을 식별하였다.

제28차 회의에는 '국제표준 기반 선박 e-Navigation 서비스 표시장치에 적용 가능한 사이버보안 요구사항(The analysis of general cybersecurity requirements applicable to ship's e-Nav service display device based on international standards)' 의제 문서가 제출되었으며, 선박의 e-Navigation 서비스 장치에 사이버 보안 요구사항을 도출하기 위해 수행된 정보가 포함되어 있다. IALA는 사이버 보안 워크숍을 개최하고 주요 결론을 바탕으로 IALA 자체의 사이버 보안 가이드라인을 개발 중이며 사이버 보안과 관련한 기존 표준이나 모범사례에서 다뤄지지 않은 IALA 관련 주체에 대한 사이버 보안 가이드라인을 제시하고 있다.

2.3 ISO

국제표준화기구(ISO, International Organization for Standardization) 및 국제전기기술위원회(IEC, International Electrotechnical Commission)의 ISO/IEC 27001은 정보보안 관리 체계에 대한 국제표준으로 2005년 ISO와 IEC에 의해 공동 발행되었으며, IMO의 '해상 사이버 위험관리 지침'에 모범사례로 포함되어 있다. 또한 ISO/IEC 27001 표준은 정보기술 – 보안기술 – 정보보안 관리시스템 – 요구사항에 대한 내용을 포함하고 있다. 해당 표준은 조직의 상황(조직에 대한 이해, 이해관계자의 기대 및 요구사항 이해, 정보보안 관리시스템의 범위), 지도부(지도부의 책무, 정책, 역할 및 책임), 책임(위험조치 – 정보보안 위험 평가/ 정보보안 위험 취급, 정보보안대상 및 계획), 정보보안 관리체계 지원 및 운영, 성능 평가, 개선 등의 내용으로 구성된다. 해당 표준의 부속서에는 정보보안 위험 취급을 위한 위험관리 통제 대상 및 통제 항목을 제시하고 있으며, 통제 대상에는 정보보안 정책, 정보보안 조직, 인적 보안, 자산 관리, 접근 통제, 암호화 정책, 물리적·환경적 보안, 운영 보안, 통신 보안, 시스템 획득과 개발 및 유지관리, 공급자 관계, 정보보안 사고 관리, 비즈니스 연속성 관리의 정보보안 측면, 준수와 같은 사항이 포함되어 있다 (Malatji, 2023).

2.4 국제선급협회(IACS)

국제선급협회는 2022년 4월 선박의 사이버 복원력을 위한 공통 규칙을 발표하였는데, 선박에서 발생하는 사이버 사고가 인명과 재산 및 환경에 직접적인 악영향을 미칠 수 있음을 인식하고 선박 Onboard 컴퓨터 기반 시스템의 기능적 효율성과 신뢰성에 대해 꾸준히 주목 및 사이버 시스템 공동작업그룹을 소집하여 접근방식 등을 식별하였다. 공통규칙 발표는 연결성이 가속화되는 디지털 해양 세계에 대한 국제선급협회의 중요한 이정표로 의미가 있다. 신규 건조선박에 대한 사이버 복원력 공통 규칙(IACS UR E26) – Cyber resiliecne of ship은 선박의 설계, 건조, 시운전 그리고 운항까지 선박의 운용 주기 동안 운영기술(OT) 및 정보기술(IT) 장비를 안전하게 선박 네트워크에 통합하는 것을 목표로 설정하고 선박 대상 및 사이버 복원력을 위해 장비 식별, 보호, 공격 탐지, 대응 및 복구의 5가지 주요 측면을 다루고 있다 (IACS 2023). 선박 온보드 시스템 및 장비의 사이버 복원력 공통규칙(IACS UR E27) – Cyber resilience of on-board system and equipment은 제조사 및 기자재 시스템 요구사항으로 시스템 무결성이 제조사에 의해 보호되고 강화 될 것을 목표로 하고 온보드 시스템과 장비의 사이버 복원력에 대한 요구사항을 제공하며 사용자와 온보드 컴퓨터 기반 시스템 간의 인터페이스와 관련된 추가 요구사항을 제공한다 (IACS, 2024). 이는 2024년 1월 1일 이후 건조계약을 체결한 신규 선박에 적용된다.

2.5 국내 해사 사이버 보안 규정

정부는 '23.4월 교통분야에서 최초로 정부·민간 역할을 규정하는 「해사 사이버안전 관리지침」을 제정하고 시행하였다. 이 지침에서는 선박을 대상으로 벌어질 수 있는 사이버 공격·위협으로부터의 안전을 확보하고 해운선사를 지원하기 위한 정부의 역할 및 해운선사가 사이버안전 관리체계를 구축할 때 고려해야 하는 사항을 권고 성격으로 규정하였다 (Ministry of Oceans and Fisheries, 2023). 또한, 사이버 공격·위협으로 선박 운항장애 등 해양사고가 발생하거나 발생할 우려가 있는 경우 해운선사는 그 사실을 바로 해양수산부에 통보하도록 하며, 해양수산부는 관련 부서·기관에 이를 전파하고 사고대응, 복구 지원 및 사고원인 조사를 실시하도록 명시하였다 (Ministry of Oceans and Fisheries, 2023).

정부는 「해사 사이버안전 관리지침」의 별표에 위험성 평가절차를 제시했는데 평가절차는 사전평가활동, 선박평가, 보고 및 취약성 검토, 제조업체 보고로 구성되어 있다. 사전 평가 활동은 운항시스템에 대한 자료를 검토하고 기밀성·무결성·가용성 등을 고려하여 잠재적인 영향 수준을 평가하며 선박 평가는 모든 선박의 선원이 참여하며, 이를 통해 선박 운항시스템의 구현과 이와 관련된 설계자료의 차이를 파악할 수 있다. 또한, 위험성 평가에는 평가된 선박 결과, 권장사항 및 전체 보안개요, 발견된 취약성 분석, 우선순위 목록, 보충자료, 위험성 평가팀이 수행한 활동기록과 사용도구 등이 포함되어야 한다. 더불어, 선박소유자가 조사결과를 검토, 논의 및 평가하는 경우에는 조사결과에 따라 영향을 받는 시스템의 제조업체에 조사결과를 보낼 수 있다.

선박소유자, 운항자, 안전관리책임자·대행자 등은 해사 사이버 공격 및 위협으로 인해 해양사고가 발생하거나 발생할 우려가 있는 경우에 해양수산부 장관에게 통보해야하며, 상황 통보 시 개요, 피해사항, 선박의 상세제원, 조치사항 등을 포함하고 상황변동 및 추가사항 발생 시 지체 없이 통보해야한다 (Ministry of Oceans and Fisheries, 2023).

2.6 해사 분야 사이버 보안 규정 간의 차이점 및 시사점 도출

국제사회에서는 2005년에 ISO와 IEC의 ISO/IEC 27001 공동

발행에 따라 정보 보안 관리 체계에 대한 국제표준이 정해지며 사이버 보안에 대한 인식을 가지게 하였다. 이를 모범사례로 여겨 해사분야에서는 IMO를 시작으로 사이버 보안 가이드라인이 제시되고 있으며 IALA, IACS 등에서는 각자 자체의 규정을 개발 중이다. 또한 각 기관에서는 기존의 표준 및 사례에서 다뤄지지 않은 가이드라인을 제시하기 위해 노력 중이다.

반면 국내의 경우 다소 늦은 시점인 2023년에 「해사 사이버안전 관리지침」을 제정하여 시행함에 따라 사이버 공격·위협에 대한 정부의 역할을 규정했으나 권고성 지침이라는 한계점이 있다.

앞서 설명한 IALA, IACS 등에서 각자 자체 규정을 개발하고 적용하는 것에 비해 우리나라는 현재 국내 산업계의 의견을 반영한 독자적인 지침을 개발하기보다는 국제 지침을 따라가고 수용하는 입장에 있다. 또한 사이버 공격·위협의 발생 현황 및 보안에 대한 국내의 자체 실태 파악이 미흡하고 정기적인 조사와 모니터링이 이루어지지 않고 있다. 사이버 공격·위협이 발생 또는 우려되는 경우에 해운선사의 통보에 따라 사고대응, 복구 지원 및 사고원인 조사가 이뤄지고 있으나 예방 및 대응지원의 경우 정기적이지 않고 지속적으로 수행되고 있지 않아 지속 가능성 측면에서 미흡하다.

3. 자율주행 자동차 산업에서 사이버 보안 동향

3.1 UNR NO.155

유럽경제위원회(UNECE)의 산하기구인 WP.29는 자동화 및 자율 연결 자동차의 보안 수준을 높이기 위해 UN Regulation No.155를 발표하였다(UN 2021). UNR 155은 '사이버 보안 및 사이버 보안 관리 시스템(CSMS)에 관한 차량 승인'으로 새로운 보안요구사항을 포함하고 있으며, 차량 종류(자동차, 버스, 트레일러 등) 및 CSMS의 준수 여부를 바탕으로 차량 판매 승인 여부를 결정하고 사이버 보안 요건을 정의하고 있다. 사이버 보안에 관한 법률을 채택함에 따라, CSMS 인증을 획득하지 못한 신형 차종은 2022년 7월부터, 기존차량은 2024년 7월부터 UNECE 대상국 및 협약국에 차량을 판매할 수 없다.

여기서 CSMS란, 차량의 전기/전자 부품에 대한 보안뿐만 아니라, 사이버 보안을 위해 조직 프로세스, 책임, 관리, 리스트 평가 방법 등이 반영된 거시적인 규제를 말한다. CSMS 인증을 위한 평가가 정상적으로 완료되고 인증업체로부터 사이버 보안 구현 확인을 위한 'Model of Manufacturer's Declaration of Compliance for CSMS'를 받으면 CSMS 준수 인증서가 제조업체에 부여되게 된다 (AEM, 2022).

제조사가 UNR 155가 적용된 자동차를 생산하기 위해서는 다음의 변경사항을 적용해야한다.

- CSMS에 대한 완전한 적용 인증
- 규제가 적용되는 차량의 요구사항과 관련 서류가 충분히 고려되었는지 점검
- 철저한 위험 평가 및 위험을 평가/관리하는 데에 적절한 방식과 과정이 사용되었는지 여부
- 차량 제조업체가 사이버 공격과 취약점을 모니터링하고 탐지하며 대응하기 위해 사용된 과정과 도구 및 방식
- 해당 분야의 차량 제조사가 적절한 시간 이내에 공격에 반응할 수 있는 계획이 있는 지 여부

UNR No. 155의 구성은 아래 Table 1과 같다.

Table 1 UNR No. 155 (UN, 2021)

Type approval	Self-certification
UN cyber security standard	Domestic introduction targets
Scope	○
Definitions	○
Application for approval markings	△ (About Type Approval)
Approval Certificate of compliance for cyber security management system	△
Specifications – Requirement of cyber security management system – Requirement of vehicle type – Reporting provisions	○
Modification and extension of the vehicle type Conformity of production Penalties for non-conformity of production Production definitively discontinued Names and addresses of Technical Services responsible for conducting approval test, and of type approval authorities	△ (About type approval)
Annexes	Domestic introduction targets
Information document	○
2. Communication 3. Arrangement of approval mark 4. Model of certificate of compliance for CSMS	About type approval
5. List of threats and corresponding mitigations	○

3.2 국내 자율주행 자동차 사이버 보안 가이드라인

국내에서 자동차 제작사가 현재 UNR No.155를 바탕으로 제정될 국내 기준에 대비가 가능하도록 제작사 권고사항 및 승인/시험기관의 역할 등을 제시하였는데 권고안은 자동차의 사이버 보안을 확보하기 위하여 자동차 제작사 및 자동차 보안 전담 기관 등에게 권고되는 사항을 규정함을 목적으로 한다. 또한 자동차의 라이프사이클 동안 참여하는 자동차 부품사, 서비스 제공업체, 협력업체 등도 권고안을 참고할 수 있다. 사이버 보안 가이드라인에서 제시한 용어는 아래 Table 2와 같다.

Table 2 List of service requirements

	Terms	Details
1	Threats	Potential cause of an accident that could cause harm to a system/vehicle, organization, or person
2	Vulnerability	Weaknesses in assets or security measures that could be exploited by threats
3	Risk	The potential for a threat to cause harm to an organization or person through a vulnerability
4	Risk Assessment	An overall process for assessing risk, including the following procedures – Risk identification: Discovery, recognition, and description of risks – Risk analysis: Understanding risk characteristics and determining risk level (judgment) – Risk assessment: Determine whether the risk level is acceptable based on the results of the risk analysis
5	Risk Management	Integrated activities to supervise and control the organization in order to respond to risks
6	Cyber security	A state that cars and their features are protected from cyber threats
7	CSMS	The following management system established by an organization to respond to risks to vehicles (risk-based approach) – Processes of organization for responding to risks – Distribution of responsibilities, authority, etc. related to risk response
8	Mitigation	Technical measures to eliminate or reduce risks
9	Vehicle Type	A series of vehicle types that have the same characteristics as the following – Shape, specifications and performance of the structure and devices of automobiles – Cybersecurity-related electrical and electronic structures and external connection devices, etc.
10	Lifecycle	The entire period from the initial development stage of the automobile type to the disposal of the type is divided as follows – Development stage – Production stage – Post-production stage
11	Aftermarket	The secondary market of the automobile industry formed after the manufacturer sells automobiles in relation to the use or operation of automobiles (Example) Manufacturing, re-production, distribution, sales and installation of automobile parts, software, services, chemical products, equipment and accessories, etc

또한 전기/전자적 설계요소가 존재하는 모든 자동차는 사이버 공격 대상이 될 수 있으므로 보안에 유의 해야하며 자율차 및 통신연결 기능이 있는 차량은 보안 확보가 필수이다.

자동차제작사는 사이버 보안 관리체계(CSMS)를 갖출 것이 권고되는데 CSMS를 구축하는 주체는 자동차 제작사로, 공급업체나 협력업체 등의 공급망에 있어서도 CSMS 관리체계에서 자동차제작사가 관리할 필요가 있다. 또한 사이버 보안 관리체계는 조직의 품질관리시스템(QMS)의 일부이거나 독립적일 수 있으며, 조직의 품질관리시스템의 일부일 경우에도 명확하게 구분 가능하여야 한다. 사이버 보안 관리체계는 차량의 라이프사이클 전반에 적합하도록 구축되고 적용될 수 있어야하며 제작사는 차량의 라이프

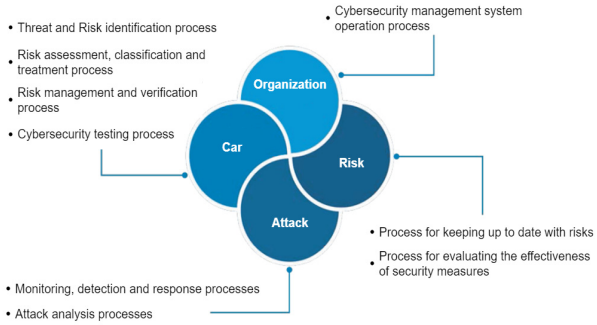

Fig. 1 Process of cybersecurity management system in the autonomous car industry

사이클(개발단계, 생산단계, 생산후단계) 전반에 걸쳐 사이버 보안 관리체계(CSMS)의 위험을 관리하기 위해 적절한 절차를 따르고 보안 조치를 마련해야 한다.

사이버 보안 관리체계의 구성요소로는 아래의 Fig. 1과 같이 프로세스가 요구된다.

3.2.1 사이버 보안 관리체계

사이버 보안 관리체계의 구축 및 관리체계 자체의 적정성 유

지·관리를 위한 활동과 매뉴얼 등을 포괄하는 체계로 사이버 보안 관련 구조화, 사이버 보안 관리에 있어 역할·책임 등의 규정 및 권한 배분 그리고 자동차 형식 라이프사이클(개발/생산/생산 후 단계) 에 따른 사이버 보안 관리활동 매뉴얼 등을 포함한다 (Boannews, 2022). 자동차에 대한 위험을 발견·인지할 수 있도록 하는 프로세스에는 최소한 사이버 보안에 대한 시스템의 연관성 식별 활동, 각 시스템/기능 정의 및 다른 시스템과의 상호작용· 제약 등을 고려한 전체 시스템을 기술/묘사하는 활동 그리고 자동차의 안전한 운행과 관련하여 보안의 대상이 되는 자산(중요요소) 식별 활동 그리고 사이버 위협 및 취약점 식별 활동을 포함한다 (Boannews, 2022).

식별된 위험을 적절히 관리하기 위하여 시행되는 프로세스로는 위험 분석 및 산정을 위한 식별된 위험에 대한 영향평가 및 잠재적 공격 경로 분석, 예상이 가능한 모든 공격경로에 대한 실행 가능성 판단과 위험 분류 및 처리를 위한 산정 결과에 따라 위험을 분류하고, 보안조치를 통해 위험수준을 크게 감소시키는 등 적절하게 처리하는 절차를 포함한다.

보안조치 등의 처리과정을 거쳐 잔존한 위험이 추후 자동차에 대한 실제 위험으로 이어지지 않도록 잔존한 위험의 수준 등을 검증하는 프로세스로는 잔존한 위험의 수준을 제작사가 명시한 위험허용범위 이내로 유지할 것을 고려한다.

자동차에 대한 사이버 위협은 다음과 같다.

- 실도로 차량과 관련된 백엔드 서버에 대한 위협
- 통신 채널을 이용한 차량 위협
- 자동차 업데이트 절차 관련 위협
- 의도하지 않은 인간 행동으로 인한 위협
- 차량의 외부 연결과 접속에 대한 위협
- 자동차 데이터/코드에 대한 위협
- 보고하 미흡하거나 강회되지 않으면 악용될 수 있는 잠재적인 취약성

3.2.2 자동차 사이버 보안 확보를 위한 제작자 권고사항

사이버 보안 관리체계에 따른 제작사 조치 권고사항으로는 위험평가, 보안조치, 보안시험, 모니터링 및 대응, 보안기록관리, 정보공유와 상호협력의 조치들을 시행함과 보안 모니터링 중 신규위협이 발견되면, 위험평가를 다시 실시하고 보안시험을 통해 보안조치를 수행함이 있다. 사이버 보안 관리체계 활동을 아래 Fig. 2로 정리하였다.

위험평가로 제작사는 사이버 보안 관련 위험요소를 식별, 평가하고 식별된 위험을 적절히 처리하고 관리해야 하는데 다음 사항의 고려가 필요하다.

- 총체적 관점에서 위험평가 및 위험관리 실시 필요(자동차 내·외부 시스템들 간의 상호작용, 잠재적인 위협 식별 뿐만아니라 공급망에 존재하는 위협 등도 고려 요함)
- 수용/허용 가능한 위험 수준 및 위험 심각도를 정의하여 위험 관리 필요(위험 평가를 통해 산정된 위험과 완화 조치 후에도 잔존한 위험에 대해 별도의 보안 조치 필요 여부 판단 기준 설정 요함)
- 자동차의 사이버 보안에 영향을 미치는 위협이 발생하면 즉각 위험도 평가를 수행

조치 및 모니터링으로 제작사는 사이버 보안 공격위협, 취약점 등에 대해 탐지 및 예방, 모니터링 및 원인분석 등의 보안조치를 취할 수 있어야한다. 보안 시험으로 자동차제작사는 보안조치가 적절한 수준으로 설계되고 구현되었는지를 확인하기 위해 객관적이고 충분한 시험평가 수행이 필요한데 시험 대상 및 근거, 평가 방법론과 근거, 시험 수행 주체와 근거, 합격/불합격 기준 및 시험 결과를 포함해야 한다.

기록 관리로 제작사는 자동차의 사이버 보안과 관련한 자료를 기록·보전하고 변경이력을 관리할 필요가 있으며 정보 공유로는 자동차 보안전담기관에게 사이버 보안 관련 정보를 공유할 수 있어야한다.

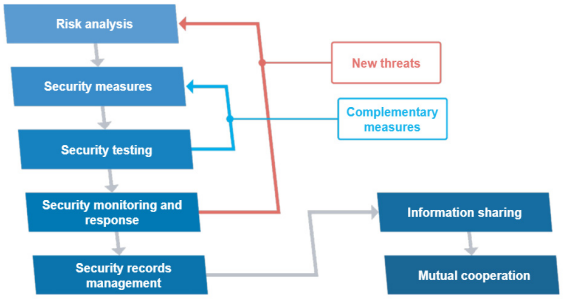

Fig. 2 Cybersecurity management system activities in the car industry

마지막으로 상호 협력으로 자동차제작사는 부품제작사, 자동차 사이버 보안 관련 사항 등을 시험·인증하는 자동차보안전담기관, 기타 관련자들과 상호 협력할 수 있어야하며 또한 위험이 발견되면 즉시 보안대책을 마련할 수 있도록 긴밀한 협력이 필요하다.

4. 국내 해사 사이버 보안 법/규제 프레임워크 방향성 제안

4.1 해사 사이버 보안 확보를 위한 법/규제 방향성

국제사회에서는 선박 내 장비의 디지털화 등으로 사이버 보안 위협 사고가 증대할 것으로 전망하고 있으며 해사 사이버 보안을 확보할 체계 마련을 권고하고 있다. 국내 또한 해사 분야의 특성을 반영하고 해사 안전 관련 의무사항 등을 전문적으로 규정하는 사이버 보안 관련 법령 제·개정이 필요하며, 사이버 보안의 기술적 특성 및 현행 국제기준의 제도 기반을 고려하여 인증 및 승인 방식을 제정하고 안내해야 한다.

해사 사이버 보안은 특수한 상황과 국가 간의 수송으로 인한 선박이 타국의 항구에 입항과 출항을 하는 등의 국제성을 고려할 때 국내적 체계만으로는 다소 한계가 있다. 따라서 국제사회에서

국가 간의 사이버 공격·위협에 관한 효과적인 대응을 위해 국제 협력을 통한 거버넌스 구축과 이를 뒷받침 할 수 있는 법적 근거가 필요하다.

사이버 보안 관리는 국제적인 동향을 바탕으로 안전 관리요소를 분석하는 것을 기반으로 하며, 예상되거나 잠재적인 위협을 연속적으로 식별하고 이에 대응 및 모니터링을 통해 이뤄진다. 이때 안전을 위협하는 위험요소를 결정하는 것이 첫 단계이며, 공격 경로를 분석하고, 위험도를 결정 및 이를 기반으로 보안 조치를 수행하고 대응하는 과정에 대한 확립이 필요하다.

이 외에도, 선박뿐만 아니라 항만 시설 포괄적으로 포함하는 견고한 사이버 보안 체계를 개발할 필요가 있으며, 서로 다른 관할 지역에서 일관되지 않은 사이버 보안 규정의 문제에 대한 검토 및 해운 산업 내 모든 이해관계자를 위한 사이버 보안에 대한 맞춤형 교육 및 인식 제고 프로그램 개발도 검토가 필요하다.

4.2 해사 사이버 보안 위협 식별

타 산업군의 사이버 보안 위협을 검토하고 해운의 특성을 고려하여, Table 3과 같이 자율운항선박 도입 시 예상되는 사이버 보안 위협을 식별하고 제시한다.

Table 3 Autonomous ship cybersecurity threats

Mid-classification	Expected threat cases	
1. Remote Operation Center (ROC) Attack	1.1	Insider attack
	1.2	Unauthorized internet access
	1.3	Unauthorized connection to remote operation center server
2. Remote Operation Center (ROC) service interruption	2.1	Autonomous vessel communication interruption due to service outage, unable to provide requested services
3. Remote Operation Center (ROC) Data breach and corruption	3.1	Insider attack
	3.2	Data loss due to service provider incident
	3.3	Unauthorized Internet connection to the server
	3.4	Unauthorized physical connection to the server (USB, etc.)
	3.5	Information breach due to unintended data sharing
4. Spoofing of messages or data received by autonomous ships	4.1	Message spoofing using a spoof attack
	4.2	Sybil Attack via virtual ship creation
5. Unauthorized manipulation of data/code on board autonomous ships, etc.	5.1	Injecting malicious code into a communication channel
	5.2	Change of data/code onboard the vessel through communication channels
	5.3	Overwrite data/code onboard the ship via communication channels
	5.4	Deletion of data/code onboard the vessel via communication channels
	5.5	Allows embedding of data/code into ships through communication channels
6. The communication channel allows untrusted messages or session hijacking/replay attacks	6.1	Accepting information from unreliable sources
	6.2	Interception attack/session hijacking
	6.3	Replay attack
7. Information disclosure	7.1	Information interception/jamming/communication monitoring (eavesdropping)
	7.2	Obtaining unauthorized access to files or data
8. Interference with autonomous ship functions using communication channels	8.1	Transmitting a large amount of data may cause normal service disruption
	8.2	Inter-ship communication disruption
9. Access rights management vulnerability in autonomous ship systems	9.1	Deodorization of access to autonomous ship systems by unauthorized user
10. Infection of autonomous ship systems through viruses embedded in communication media	10.1	Infection of ship systems through viruses embedded in communication media
11. Messages containing malicious content received from ships	11.1	Malicious internal message
	11.2	Malicious diagnostic message
	11.3	Malicious unique message (normally sent by the supplier)
12. Misuse or corruption of the update procedure	12.1	Corruption of the over-the-air software update(OTA) procedure
	12.2	Corruption of local/physical software update procedures
	12.3	The update process is not corrupted, but the software was already manipulated and corrupted before the process

Mid-classification	Expected threat cases	
	12.4	Allowing invalid updates due to compromised software vendor encryption key
13. Normal update rejection	13.1	Denial of service attacks on update servers or networks to prevent important updates
14. Actions that facilitate cyber attacks	14.1	Allowing unintended execution of malware or attacks by legitimate actors(ship owners, ship operators or maintenance engineers)
	14.2	Failure to follow defined security procedures
15. Extract ship data/code	15.1	Extraction of copyrighted or proprietary software from autonomous ship systems(product piracy)
	15.2	Unauthorized access to owner's personal information
	15.3	Extract the encryption key
16. Manipulation of ship data/code	16.1	Identity manipulation
	16.2	Bypass monitoring system
	16.3	Data manipulation for tampering with ship operation data (route planning)
	16.4	Unauthorized alteration of system diagnostic data
17. Delete data/code	17.1	Unauthorized deletion/manipulation of system event logs
18. Install malware	18.1	Malicious software or malicious software activity
19. Install new software or overwrite existing software	19.1	Software falsification of autonomous ship control systems or information systems
20. Interruption of system operation	20.1	Denial of service
21. Autonomous ship parameter manipulation	21.1	Modification of configuration parameters of key functions of autonomous ships through unauthorized access

4.3 해사 사이버 보안 강화를 위한 프레임워크

해사 사이버 보안 강화를 위해서 Fig. 3과 같은 프레임워크를 제안한다. 이 프레임워크는 발생할 수 있는 위험에 대한 시나리오를 식별하고, 식별된 위험에 대해 공격 경로를 분석 및 위험 영향 등급에 따라서 차별화된 조치를 수행하도록 설계되었다. 또한 수행된 보안 조치에 대해 보안 시험을 통해 보완 사항을 식별하고 개선된 조치를 가능하게 하며, 최종적으로 보안 모니터링 및 대응을 통해 사이버 보안 강화를 달성할 수 있도록 한다. 이 과정에서 공격 가능성 등급과 위험도가 결정되는데, 이 때 낮은 등급에 대해서는 누락된 위험 시나리오가 없었는지 재검토 과정을 수행하도록하며, 최종 모니터링 및 대응 과정에서 추가적으로 식별된 위험에 대해 시나리오 식별을 수행할 수 있도록 설계되었다.

이러한 수행 결과는 기록 및 관리가 매우 중요하기에 관리 기준 및 기한에 대한 검토가 필요하며, 식별된 보안 위협 및 대응 방안에 대한 정보를 다른 사용자들과 공유하고 상호 협력을 통해 공동으로 대응 할 수 있는 방안 마련이 필요하다. 이 과정에서 미처 파악하지 못한 위험이 식별될 수 있으며, 이 또한 시나리오 식별 과정을 통해 적절히 관리 될 수 있도록 프레임워크가 구성되었다.

5. 논 의

이 논문은 지속적으로 발전하고 있는 자율운항선박 기술에 비해 해사 사이버 보안에 대한 현재 규정이 매우 미비함을 식별하고, 현재 사이버 보안 관련 규정과 시스템이 잘 갖추어져있는 타 산업의 규제와의 비교, 분석을 통해 해운 분야의 사이버 보안 강화를 위한 프레임워크를 제시하였다는 점에서 의미가 있다.

4.2절 '해사 사이버 보안 위협 식별'의 Table 3에서 제시하고 있는 원격운항센터에 대한 공격, 운영 중단, 데이터 유출 및 자율운항선박의 통신 기능 방해 등 자율운항선박에 대해 중대한 위험이 될 수 있는 사이버 보안 위협을 타 산업군의 자율운항시스템을 검토하고 해운 실정을 고려하여 식별하였으며 자율운항선박에 적용할 수 있도록 제공하였다. 더 나아가, 해사분야에서 이러한 위협이 지속적으로 관리되고 저감될 수 있도록 사이버 보안 강화 프레임워크를 고안하였다. 이를 통해 철저한 사이버 보안을 확립을 이루고 해운 분야에 자율운항시스템이 안전하게 도입되는데 기여할 수 있을 것으로 기대된다.

이렇게 식별된 사이버 보안 위협은 단순히 사이버 보안 강화를 위한 프레임워크를 따르고, 보안을 위한 규정과 규제를 제정하고 시행하는 것만으로는 달성하기 어려운 실정이다. 이 논문의 한계점은 단순히 이러한 위험요소들을 식별하고 프레임워크를 제안하는 것에 그친다는 것이다. 이렇게 식별되고 제안된 사항들이 적절히 산업에 반영되고 강화된 사이버 보안을 달성하기 위해서는 산업계의 목소리를 반영하고, 학계와 규제/규정 제정자, 정책 입안자들이 함께 모여 제시된 프레임워크를 검토하고 식별된 위험요소들에 대한 저감 방안을 논의할 필요가 있다. 이러한 과정을 통해 더욱 견고하고 철저한 사이버 보안 강화 프레임워크 제정이 필요하다.

6. 결 론

자율운항시스템은 효율성, 경제성 및 인간의 실수를 줄이는 측면에서의 향상된 안전성을 달성할 수 있다는 사실에 의해 지속적으로 주목되고 있습니다. 사물 인터넷(IoT), 빅 데이터 분석, 인공지능(AI), 자동화와 같은 첨단 기술을 활용하는 이러한 시스템은

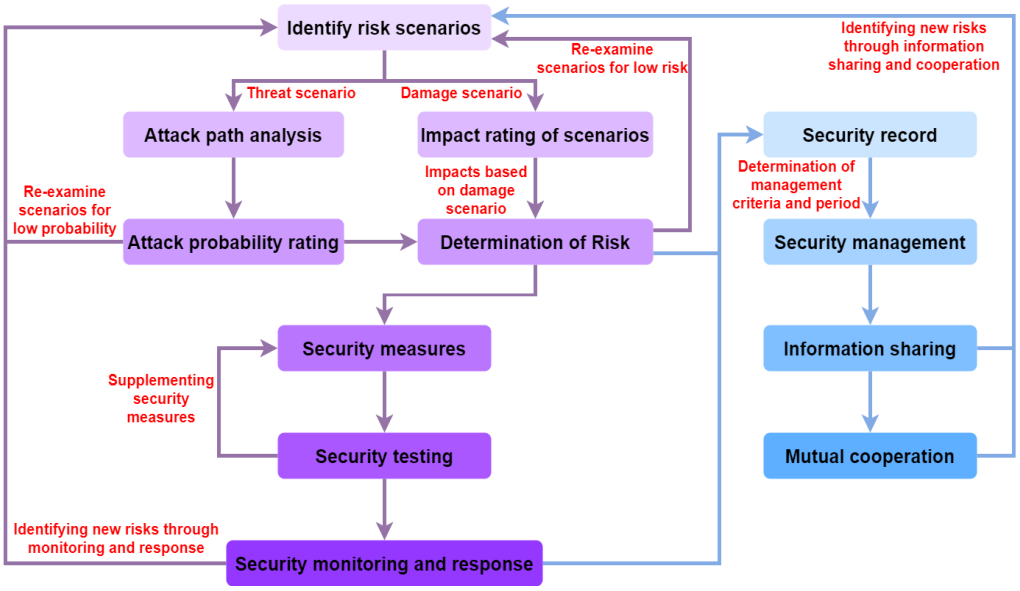

Fig. 3 Framework for strengthening maritime cybersecurity

다양한 정보를 기반으로 최적화된 선박의 운영을 가능하게 한다.

하지만 이러한 과정은 정보의 송수신이 안전하고 정확하게 이루어질때 가능하며, 다양한 정보가 지속적으로 전송되기에 정보의 탈취, 변조, 위조 등의 다양한 위협이 존재한다. 뿐만아니라 선박을 통한 중대한 금전적, 사회적 위협을 가능하게 할 수도 있다.

이러한 위협으로부터 보호를 위해 자율운항시스템의 사이버 보안은 그 중요성이 지속적으로 커지고 있다. IMO, 국제항로표지협회(IALA), ISO, 국제선급협회(IACS) 등에서 관련 규정을 제정하였거나 개발하고 있으며, 대한민국 정부 또한 해사 사이버 보안 규정을 제정하여 시행하고 사이버 공격이나 위협으로 부터 보호를 강화하고 있다. 하지만 자율운항시스템이 먼저 도입된 자동차 등의 산업군과 비교했을 때 해운분야의 자율운항시스템 관련 사이버 보안 규정 및 지침은 미비하다는 것이 이번 연구를 통해 식별되었다. 이러한 한계점을 극복하고자 해운 특성을 고려하여 21가지 중분류의 자율운항선박 사이버 보안 위협을 식별하고 제시하였으며, 해운분야에서 자율운항시스템이 적절히 활용될 수 있도록 사이버 보안 강화를 위한 프레임워크를 제안하였다.

이 논문에서 식별하고 제안한 결과물을 통해 해운분야의 사이버 보안을 위한 예방 및 대응지원이 정기적이고 지속적으로 수행됨으로써 지속 가능성을 향상시킬 수 있도록 기여할 수 있으며, 자체 실태 파악이 미흡하고 국제 지침을 수용하는 입장의 국내 해사 사이버 보안 규정이 국내 산업계의 의견을 반영한 독자적인 지침을 개발하도록 방향성을 제시한다.

후 기

본 논문은 2024년도 해양수산부 및 해양수산과학기술진흥원, 자율운항선박 기술개발(20200615)의 지원으로 수행된 연구임

References

AEM, 2022. *Cybersecurity management system security coding response plan* [Online] Available at: https://www.autoelectronics.co.kr/article/articleView.asp?idx=4542 [Accessed 08 October 2024].

Aiello, G., Giallanza, A. and Mascarella, G., 2020. *Towards shipping 4.0. a preliminary gap analysis. Procedia Manufacturing,* 42, pp.24-29.

Al Ali, N.A.R., Chebotareva, A.A. and Chebotarev, V.E., 2021. Cyber security in marine transport: opportunities and legal challenges. *Pomorstvo,* 35(2), pp.248-255.

Androjna., 2020. *Cyber threats to maritime critical infrastructure* [Online] Available at: https://www.researchgate.net/profile/Andrej-Androjna-3/publication/349502224_CYBER_THREATS_TO_MARITIME_CRITICAL_INFRASTRUCTURE/links/6033c2f592851c4ed58ce729/CYBER-THREATS-TO-MARITIME-CRITICAL-INFRASTRUCTURE.pdf [Accessed 15 October 2024].

Androjna, A., Perkovič, M. and Pavić, I., 2022. *Cyber security challenges for safe navigation at sea.* Technologies, Techniques and Applications Across PNT, 47.

Boannews, 2022. *[Future car cybersecurity-2] 9-step Automotiveecurity guidelines and management system process* [Online] Available at: https://m.boannews.com/html/detail.html?idx=109426 [Accessed 14 October 2024].

Brandt, T. and T. Tamisier., 2021. The future connected car – safely developed thanks to UNECE WP. 29? 21. *Internationales Stuttgarter Symposium: Automobil-und Motorentechnik,* Springer.

Copeland, G., 2020. Practical cyber security for digital trains.

Cyber security practitioner's guide. World Scientific, pp.81-107.

Costantino, G., De Vincenzi, M. and Matteucci, I., 2022. A comparative analysis of unece wp. *29 r155 and ISO/SAE 21434. 2022 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, IEEE.

Craigen, D., Diakun-Thibault, N. and Purse, R., 2014. Defining cybersecurity. *Technology innovation management review,* 4(10).

Das, S., Geedipally, S.R., Dixon, K., Sun, X. and Ma, C., 2019. M*easuring the effectiveness of vehicle inspection regulations in different states of the US*. Transportation research record 2673(5), pp.208-219.

Daum, O., 2019. Cyber security in the maritime sector. *Journal of Maritime Law and Commerce,* 50, pp.1.

De Cerchio, R. and C. Riley., 2011. Aircraft systems cyber security. *IEEE/AIAA 30th digital avionics systems conference,* IEEE.

Elmarady, A.A. and K. Rahouma., 2021. Studying cybersecurity in civil aviation, including developing and applying aviation cybersecurity risk assessment. *IEEE Access,* 9, pp.143997-144016.

Erich, S., 2021. *Cyber security framework for napa onboard products*. Metropolia University of Applied Sciences.

Finley, I. B., 2017. *An evaluation of national cybersecurity policies for the maritime transportation system*, Northcentral University.

Fjørtoft, K. and S.P. Berge., 2019. *ICT for sustainable shipping*. Sustainable shipping: a cross-disciplinary view, pp.137-166.

IACS, 2023. *UR E26, Cyber resilience of ships*

IACS, 2024. *UR E27, Cyber resilience of on-board systems and equipment*

IALA, 2019. *ENAV24-6.1.14, Introduction of cyber security type approval applicable case based on IEC 62443 and IEC 61162-460 standards.*

IALA, 2021. *ENAV27-12.2.2, IALA guideline on developments in maritime autonomous surface ships.*

IALA, 2021. *ENAV28-5.1.1.4, The analysis of general cybersecurity requirements applicable to ship's e-Nav service display device based on international standards.*

ICAO, 2016. *Implementation of effective cyber security measures to achieve - a safe, secured and efficient air traffic control system in Hong Kong, China* [Online] Available at: https://www.icao.int/APAC/Meetings/2016%20APANPIRG27/WP%2019,%20AI%203.6%20-%20ATS%20Cyber%20Security__HK_China.pdf [Accessed 10 October 2024].

IEC, 2018. *61162-460, Maritime navigation and radiocommunication equipment and systems - Digital interfaces.*

IEC, 2019. *62443, Security for industrial automation and control systems.*

IMO, 1989. *A.647(16), ISM Code, International Safety Management Code.*

IMO, 2017. *MSC.428(98), Maritime cyber risk management in safety management systems.*

IMO, 2017. *MSC-FAL.1/Circ.3, Guidelines on maritime cyber risk management.*

IMO, 2019. *MSC 101/5/5, Draft interim guidelines for MASS trial.*

IMO, 2021. *MSC-FAL.1/Circ.3/Rev.2, Guidelines on maritime cyber risk management.*

ISO/IEC, 2013. *ISO/IEC 27001, standard on Information technology - Security techniques - Information security management systems - Requirements*

Kagalwalla, N. and P.P. Churi., 2019. Cybersecurity in aviation: An intrinsic review. *5th international conference on computing, communication, control and automation (ICCUBEA),* IEEE.

Karim, M.S., 2022. Maritime cybersecurity and the IMO legal instruments: Sluggish response to an escalating threat? *Marine Policy,* 143, pp.105138.

Kavallieratos, G., Diamantopoulou, V. and Katsikas, S.K., 2020. Shipping 4.0: Security requirements for the cyber-enabled ship. *IEEE transactions on industrial informatics,* 16(10), pp.6617-6625.

Kavallieratos, G., Katsikas, S. and Gkioulos, V., 2020. Modelling shipping 4.0: A reference architecture for the cyber-enabled ship. *Asian conference on intelligent information and database systems,* Springer.

Kawaguchi, T., 2023. Two approaches to responding to destructive cyberattacks on critical infrastructure in Japan: Addressing cyber crises as service failures or armed attacks. *Civil defense in Japan,* Routledge, pp.180-195.

Kennedy, G.A., Scott, W.R., Shirvani, F. and Campbell, A.P., 2020. Modeling the evolution of organizational systems for the digital transformation of heavy rail. *A framework of human systems engineering: Applications and case studies,* pp.63-96.

Kour, R., Patwardhan, A., Thaduri, A. and Karim, R., 2023. A review on cybersecurity in railways. Proceedings of the institution of mechanical engineers, Part F, *Journal of Rail and Rapid Transit,* 237(1), pp.3-20.

Lagouvardou, S., 2018. *Maritime cyber security: concepts, problems and models.* Kongens Lyngby, Copenhagen.

Lee, Y., Woo, S., Song, Y., Lee, J. and Lee, D.H., Practical vulnerability-information-sharing architecture for automotive security-risk analysis. *IEEE Access,* 8, pp.120009-120018.

Limnaios, G., 2022. *Cybersecurity considerations for aerial*

networks. International Hellenic University.

Los Angeles Time*Cyberattack cost Maersk as much as $300 million and disrupted operations for 2 weeks* [Online] Available at: https://www.latimes.com/business/la-fi-maersk-cyberattack-20170817-story.html [Accessed 16 September 2024].

Malatji, M., 2023. Management of enterprise cyber security: A review of ISO/IEC 27001: 2022. *2023 International conference on cyber management and engineering (CyMaEn).*

Markopoulou, D., Papakonstantinou, V. and de Hert, P., 2019. The new EU cybersecurity framework: The NIS Directive, ENISA's role and the general data protection regulation. *Computer law & security review,* 35(6), pp.105336.

Melnyk, O., Onyshchenko, S., Pavlova, N., Kravchenko, O. and Borovyk, S., 2022. Integrated ship cybersecurity management as a part of maritime safety and security system. *International Journal of Computer Science and Network Security,* 22(03), pp.135-140.

Ministry of OcFisheries, 2023. *Establishment of management guidelines to enhance ship cybersecurity* [Online] Available at: https://www.mof.go.kr/doc/ko/selectDoc.do?docSeq=50842&menuSeq=971&bbsSeq=10 [Accessed 27 September 2024].

Mraković, I. and R. Vojinović., 2019. *Maritime cyber security analysis-how to reduce threats?* Transactions on maritime science 8(01), pp.132-139.

Neo, M., 2021. The rising threat of maritime cyber-attacks: Level of maritime cyber-security preparedness along the straits of Malacca and Singapore. *Royal Australian Navy Sea Power,* 42, pp.38.

Prochazka, J., Novobilsky, P., Prochazkova, D. and Valousek, S., 2022. Cybersecurity design for railway products. *Understanding and Managing Risk and Reliability for a Sustainable Future*, pp.304-311.

Roberts, A., Marksteiner, S., Soyturk, M., Yaman, B. and Yang, Y., 2023. A global survey of standardization and industry practices of automotive cybersecurity validation and verification testing processes and tools. *SAE International Journal of Connected and Automated Vehicles*, 12-07-02-0013.

RSSB, 2021. *RIS-3703-TOM Iss 4.1 passenger train dispatch and platform safety measures* [Online] Available at: https://www.rssb.co.uk/standards-catalogue/Catalogueltem/ris-3703-tom-iss-4-1 [Accessed 30 September 2024].

Schmittner, C. and G. Macher., 2019. Automotive cybersecurity standards-relation and overview. *Computer safety, reliability, and security: SAFECOMP 2019 Workshops,* ASSURE, DECSoS, SASSUR, STRIVE, and WAISE, Turku, Finland, September 10, 2019, Proceedings 38, Springer.

Sena, A., Hariri, A., Prasojo, G. L. and Iswahyudi, P., 2021. Diplomacy review of delegation of Republic of Indonesia to the International Civil Aviation Organization in Montreal Canada. *SKYHAWK: Journal Aviasi Indonesia,* 1(1), pp.52-66.

Soderi, S., Masti, D. and Lun, Y.Z., 2023. Railway cyber-security in the era of interconnected systems: a survey. *IEEE Transactions on Intelligent Transportation Systems,* 24(7), pp.6764-6779.

Tomić Rotim, S., 2020. Implementing cybersecurity measures in Transport Organisation. *Annals of Disaster Risk Sciences: ADRS,* 3(1).

Ukwandu, E., Ben-Farah, M.A., Hindy, H., Bures, M., Atkinson, R., Tachtatzis, C., Andonovic, I. and Bellekens, X., 2022. Cyber-security challenges in aviation industry: A review of current and future trends. *Information,* 13(3), pp.146.

UN, 2021. *UN regulation No. 155, Uniform provisions concerning the approval of vehicles with regards to cyber security and cyber security management system.*

UN trade & development, 2022. *Review of maritime transport 2022*, New York: UNCTAD.

Vandezande, N., 2024. Cybersecurity in the EU: How the NIS2-directive stacks up against its predecessor. *Computer Law & Security Review,* 52, pp.105890.


박 제 영


박 치 병


박 한 선