JANT 한국항행학회논문지
Journal of Advanced Navigation Technology

항공 우주 해상

J. Adv. Navig. Technol. 28(1): 27-36, Feb. 2024

국제선급협회 공통 규칙 – 선박의 사이버 복원력에 대한 기술적 분석

IACS UR E26 - Analysis of the Cyber Resilience of Ships

강 남 선[1*] · 손 금 준[2] · 박 래 천[1] · 이 창 식[1] · 유 성 상[3]
[1]이글루코퍼레이션 전략사업팀
[2]한국선급 사이버인증팀
[3]중소조선연구원 특수선박지원센터

Nam-seon Kang[1*] · Gum-jun Son[2] · Rae-Chon Park[1] · Chang-sik Lee[1] · Seong-sang Yu[3]

[1]Strategic Business Division, IGLOO Corp., Seoul 05836, Korea
[2]Cyber Certification Team, Korean Register, busan 46762, Korea
[3]Research Institude of Medium & Small Shipbuilding, Busan 46757, Korea

[요 약]

본 논문에서는 2024년 7월 1일 협약 이행을 앞둔 국제선급협회의 공통규칙 – 선박의 사이버 복원력을 분석하여 5가지 요구조건과 17개의 세부사항, 선박 사이버 복원력에 따라 제출되거나 유지관리되어야 하는 문서들을 기준으로 선박 전주기 동안의 선박 사이버 복원력 대응을 위한 기술로 선급 인증 문서·설계서 등의 문서관리, 보안이 강화된 네트워크 구성, 사고 대응을 위한 프로세스 정립과 소프트웨어 도구를 이용한 형상관리, 네트워크 통합관리, 멀웨어 보호, 보안 관리 솔루션으로 선박 네트워크 보안 위협 탐지와 실시간 대응이 가능한 기술을 제안하였다.

[Abstract]

In this paper, we analyze the unified requirements of international association of classification societies - cyber resilience of ships, ahead of implementation of the agreement on July 1, 2024, and respond to ship cyber security and resilience programs based on 5 requirements, 17 details, and documents that must be submitted or maintained according to the ship's cyber resilience,. Measures include document management such as classification certification documents and design documents, configuration of a network with enhanced security, establishment of processes for accident response, configuration management using software tools, integrated network management, malware protection, and detection of ship network security threats with security management solutions. proposed a technology capable of real-time response.

Key word : Cyber resilience of ships, Cyber Security on board ship, Cyber security framework, Operational technology on ships, International association of classification societies.

http://dx.doi.org/10.12673/jant.2024.28.1.27

Received 19 January 2024; **Revised** 27 February 2024
Accepted (Publication) 28 February 2024 (29 February 2024)

***Corresponding Author; Nam-seon Kang**

Tel: +82-2-3452-8814
E-mail: namseon.kang@igloo.co.kr

Ⅰ. 서 론

스마트 선박, 자율운항선박의 출현과 해사 분야의 디지털 기술의 확대로 인해 해상에서의 사이버 사고가 증가함에 따라 발틱 국제해사협의회 (BIMCO; the Baltic and International Maritime Conference)에서는 2016년 선박 사이버보안 가이드라인을 발간하고 국제정유사해운포럼 (OCIMF; the Oil Company International Marine Forum)는 2017년 탱커관리와 자체평가 (TMSA; tanker management and self assessment) 3에 사이버보안 관련 위험 식별을 포함하는 절차 및 요건을 포함하였으며 2018년 SIRE (ship inspection report programme) VIQ (vessel inspection questionnaire) 7에 사이버보안 요건을 추가하는 등 국제기구를 중심으로 선박 사이버보안에 대한 대책을 마련하였다[1]-[4].

국제해사기구(IMO; International Maritime Organization)는 사이버 위협 및 취약성으로부터 운송을 보호하기 위하여 2017년 해상 사이버 리스크 관리지침 (MSC-FAL.1/Circ.3/ Rev.2 – guideline on maritime cyber risk management)을 승인하고, 2021년까지 선주와 선박 관리사들에게 사이버 리스크의 국제안전관리코드 내 안전관리체계 (SMS; safety management system) 통합을 권고하는 결의서인 안전관리시스템에서의 해상 사이버 위험 관리(Resolution MSC 428(98) - maritime cyber risk management system)를 채택하였다[5],[6].

또한 국제선급협회 (IACS; International Association of Classification Societies)는 회원 선급들이 규정 및 지침서에 포함하여 이행해야 하는 최소한의 기술적인 요구사항 (UR; unified requirements)인 E26 - 선박의 사이버 복원력 (cyber resilience of ships)과 E27 - 선박 기자재 사이버 복원력 (cyber resilience of on-board systems and equipment)을 발행하였다[7].

IACS UR E26은 선박을 UR E27은 선박에 탑재되는 온보드 시스템과 장비를 대상으로 최소 요구사항을 명시함으로써 선박에 최소한의 사이버보안을 보장할 수 있도록 2024년 7월 1일부터 건조 계약되는 선박의 기술적 필수 요구사항으로 적용을 목표하고 있다. UR E26은 선박 건조뿐 아니라 선박 운영 등 선박 전주기의 사이버 복원력 확보를 규정하고 있어 선박 건조 시 UR E27을 만족하는 선박 기자재를 탑재함으로써 UR E26을 만족할 수 없으며 반드시 선박 운영 기간의 사이버 복원력 대응 방안이 필요하다.

따라서 본 논문에서는 IACS의 UR E26 – 선박의 사이버 복원력의 요구사항을 분석하여 UR E26 규제와 선박의 사이버 위협에 대응 가능한 기술을 검토하고자 하며, 구성은 다음과 같다. 2장에서는 IACS UR E26을 분석하고 3장에서 분석결과를 기반으로 한 선박 사이버보안 대응 기술의 요구조건을 도출하며 4장에서 결론을 제시한다.

Ⅱ. 선박의 사이버 복원력

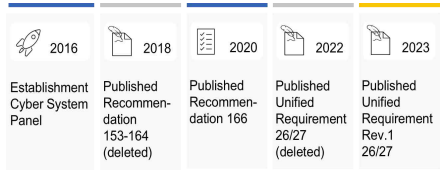

그림 1. 국제선급협회의 사이버보안 활동
Fig. 1. The history of IACS cyber panel.

IACS는 그림 1과 같이 2016년 사이버 보안 패널을 신설하고 선박에 사용되는 컴퓨터 기반 시스템 (CBS; computer based system)의 소프트웨어 유지보수 절차, 네트워크 아키텍처, 데이터 검증, 물리적/네트워크 보안, 자산목록, 원격 업데이트 등에 관한 권고서 Recommendation 153-164를 발행하였으며, Rec. 153-164를 포함하여 사이버 복원력 권고서 Rec. 166 – Recommendation on cyber resilience를 2020년 4월에 발행하였다[7]. 2022년 4월에는 UR E26과 UR E27을 발행하였으며, 2023년 11월 UR E26, UR E27의 개정판 Rev.1을 발행하였다[8],[9].

IACS UR E26 선박의 사이버 복원력은 사이버 복원력에 대한 집합체로서 선박을 목표로 선박의 사이버 복원력에 대한 최소 요구사항을 정의하며, 선내 시스템, 장비 및 구성품들의 사이버 복원력을 다루는 산업 표준 및 다른 UR의 상호보완적 적용을 위해 제정되었다.

UR E26은 2024년 7월 1일 이후 건조 계약되는 선박에 대해 IACS 선급들에의해 국제항해에 종사하는 선급 등록 선박에 일관되게 적용되며, 선박 내 운영기술 (OT; operational technology)에 사용되는 CBS, 특히 선박 기능 및 시스템의 작동에 이용되는 경우와 협약 규정에서 요구되는 항해시스템, 선급 규칙 및 협약 규정에서 요구되는 내부 및 외부 통신 시스템에 적용된다[8].

해사 분야의 대표적 사이버보안 지침인 IMO MSC 428(98), BIMCO 선박 사이버보안 가이드라인 등 많은 해사 사이버보안 지침은 미국 국립표준기술원(NIST; National Institute of Standards and Technology)의 사이버보안 프레임워크 (CSF; cyber security framework)을 기반으로 한다. CSF는 가장 많은 도메인에서 채택하는 보안 프레임워크 중 하나로 사이버보안 위협을 보다 효과적으로 관리하는데 필요한 표준, 지침, 기술 사양으로 구성된 리스크 기반의 프레임워크이며, 그림 3과 같이 식별, 보호, 탐지, 대응, 복구의 다섯 가지 핵심 기술로 구성된다[10].

IACS는 선박의 안전한 운항을 위해 사용되는 운영기술(OT)의 중단 또는 손상으로 인한 사고 발생을 줄이고, 영향을 완화하기 위한 기능으로서 선박 사이버 복원력에 대한 최소 요구사항을 정의하며 그림 4와 같이 NIST CSF를 적용하여 UR E26의 프레임워크를 정의하고 식별, 보호, 탐지, 대응, 복구에 대한 요구사항과 이에 대한 17개의 세부사항을 정의하였다.

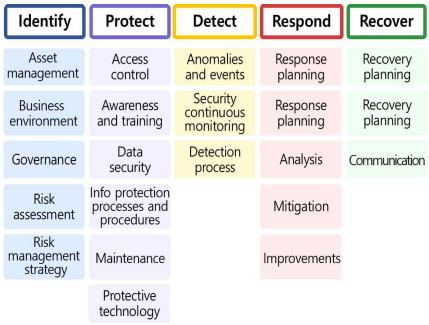

그림 2. 미국표준기술연구소의 사이버보안 프레임워크
Fig. 2. NIST cyber security framework.

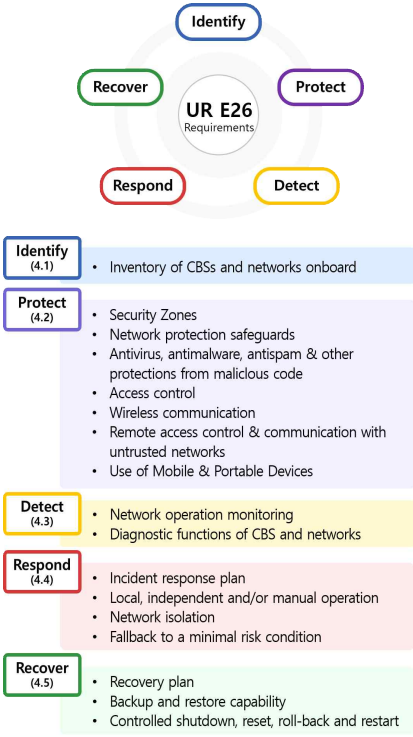

그림 3. 선박 사이버 복원력의 프레임워크 및 요구사항
Fig. 3. Frameworks and requirements for IACS UR E26.

2-1 식별

식별 기능은 선박에 설치된 CBS와 네트워크 구성 등 선박의 사이버보안을 위해 관리되어야 할 자산을 식별하고 이를 목록화하는 것을 목표한다.

OT 시스템에 사용되는 선내 CBS와 소프트웨어가 관리되지 않을 경우 사이버 범죄에 악용될 수 있으며, 네트워크를 기반하는 CBS가 사이버 공격의 잠재적 취약 포인트가 될 수 있어 선내 CBS의 하드웨어와 소프트웨어, CBS의 선내 또는 선육간 네트워크 목록을 식별하고 선박의 전주기 동안 최신으로 유지해야한다.

하드웨어 목록에는 제조업체, 모델, 주요 기술 데이터 등이 포함되어야 하며, CBS 간, CBS와 외부장치, 네트워크 사이의 논리적·물리적 연결 등 CBS가 포함된 네트워크 토폴로지, 네트워크 내 사용되는 프로토콜에 대한 주소/식별자 등이 기술되어야 한다. 소프트웨어는 제조업체, 모델, 주요 기술 데이터와 함께 버전 정보, 초기 설치일과 만료일이 포함된 라이선스 정보, 업데이트 로그와 유지보수 정책 등이 기술되어야 한다.

2-2 보호

보호 기능은 잠재적 사고의 영향을 제한하거나 억제할 수 있는 보호장치 마련을 목표한다.

보호 기능 요소는 보안 구역 설정과 네트워크 구성, 네트워크 보호 안전장치 설치, 안티바이러스 등 악성코드로부터 보호, 접근 통제, 무선통신, 원격 접근제어 및 모바일 장치에 대한 보호를 정의한다.

보안 구역과 네트워크 구성은 사이버 공격의 위험과 범위를 줄이고 네트워크 성능을 향상시킬 수 있도록, 보안 정책 및 보안 기능이 있는 구역을 보안 구역으로 그룹화하여 관리하며, 다른 보안 구역 또는 네트워크 연결 시에는 데이터 통제 수단을 통해 연결하는 등 허용된 트래픽만 보안 구역 경계를 통과할 수 있어야 한다.

네트워크 보호는 네트워크의 무결성, 기밀성 및 가용성을 보호할 수 있도록 방화벽 등과 같은 수단을 통해 과도한 데이터 흐름 및 네트워크 리소스의 서비스 품질을 손상시킬 수 있는 위험으로부터 보호하기 위한 수단을 포함하여야 한다.

또한, 바이러스, 웜, 트로이 목마, 스파이웨어 등과 같은 악성코드로부터 CBS를 보호하기 위하여 멀웨어 소프트웨어를 설치하고 주기적으로 업데이트 해야한다.

접근 통제는 무단접근의 예방을 위한 선원 및 방문자 등의 물리적 접근 통제, 네트워크 엑세스 포인트의 물리적 접근 통제, 허가·검증된 이동식 매체의 이용, 사용자 권한과 암호키 및 다중요소 인증 등을 통해 자격증명을 관리해야 한다.

무선 통신 네트워크는 유선 네트워크보다 높은 사이버보안 리스크를 가지기 때문에 무선 네트워크 장치 및 통신 장치의 식별과 인증 기능, 데이터 무결성과 기밀성 확보를 위한 암호화 등의 장치가 설계, 구현 및 유지하여야 한다.

원격접근 통제는 신뢰할 수 없는 네트워크로부터 승인되지 않은 접근과 사이버 위협으로부터 보호를 위해 선내 IT 및 OT 시스템에 대한 원격접근 권한과 원격 유지보수에 원격접근이 이용되는 경우의 요구사항을 정의하였다.

CBS는 일반적으로 모바일 또는 휴대용 장치로 인한 악성코드 감염 가능성이 높은 것으로 알려져 모바일 및 휴대용 장치는 선박의 운항 또는 유지보수를 위한 연결을 제외하고 물리적·논리적으로 차단하도록 명시하였다.

2-3 탐지

탐지 기능은 정교해지는 사이버 공격과 알려지지 않은 취약성을 표적으로 하는 사이버 공격의 대응 방안으로 선내 CBS 및 네트워크를 실시간 모니터링하여 사이버 사고를 식별하고 이상 발생 시 경보 발생을 위한 방안 마련을 목표한다.

네트워크 모니터링은 과도한 트래픽에 대한 모니터링 및 보호, 네트워크 연결 모니터링, 기기 관리 활동 모니터링 및 기록, 미승인된 장치의 연결에 대한 모니터링 또는 보호 기능이 포함되어야 하며, 네트워크 모니터링 수단에 침입 탐지 시스템(IDS; intrusion detection system) 기능이 포함되는 경우 CBS 성능에 영향을 미치지 않도록 보호 기능이 제한된 수동형 IDS를 관련 지식을 보유한 직원이 운용할 수 있도록 하여야 한다.

또한, UR에서 요구하는 보안 기능의 성능과 기능성을 확인할 수 있도록 CBS와 네트워크 진단기능을 제공해야 하며, 네트워크 진단기능은 선박의 시험 및 유지보수 단계에서 모든 보안 기능이 정상적으로 동작하는지 확인할 수 있는 수단으로 사용할 수 있어야 한다.

2-4 대응

대응 기능은 사이버 사고의 영향을 최소화하기 위한 방안 구현을 목표로 하며, 사고 대응계획, 로컬 제어 및 모니터링, 네트워크 격리, 최소 위험 조건으로의 대비책을 요구한다.

사고 대응계획은 사이버보안 사고 대응 방안을 상세화하여 선주에 의해 개발되어야 하며, UR 적용 범위에 있는 CBS에 대한 사이버 사고의 탐지, 대응 및 영향을 제한하기 위한 지침 및 절차 문서 등이 포함되어야 한다.

사이버 사고가 발생 되면 보안 구역의 네트워크 기반 통신을 종료할 수 있어야 하며, UR의 적용 범위에 있는 CBS 또는 네트워크 기능을 손상시키는 사이버 사고가 발생될 때 영향을 받는 시스템 또는 네트워크를 최소 위험 상태로 되돌릴 수 있는 최소 위험 조건으로의 대비책이 공급업체와 조선소·선박 설계자·시스템 통합자가 설계 단계부터 고려되어야 한다.

2-5 복구

복구 기능은 사이버 사고의 영향을 받은 선내 CBS 및 네트워크를 복원하는 기능 지원을 목표하며 이를 위해 복구, 백업 및 복구 기능의 요구사항, 제어된 종료, 리셋, 롤백 및 재시작에 대한 요구사항을 정의하였다.

복구 계획은 사이버 사고목록, 표시 및 경보, 영향, 사고 대응, 복구정책, 자동 및 수동 복구 절차 등이 선주에 의해 작성되어야 한다. 데이터 손실을 방지하고 손실 발생 시 데이터베이스를 재구성할 수 있도록 백업 및 복구 기능이 제공되어야 하며, 사이버 사고로 인한 손상으로부터 복구가 가능하도록 제어되는 종료, 리셋, 롤백 또는 전원이 꺼진 상태에서 재시작할 수 있어야 하며, 이에 대한 기능을 선원이 이용할 수 있도록 문서가 제공되어야 한다.

UR E26의 식별, 보호, 탐지, 대응, 복구의 다섯 가지 요구사항의 만족 여부는 IACS 선급 검사원을 통해 성능평가 또는 성능시험으로 판단하며, 시험 대상자에 의해 작성된 시험계획서를 기반으로 선박의 설계·건조 단계, 시운전 단계, 선박의 운항 단계 등 선박의 전주기에 이행된다.

선박의 설계·건조 단계에서는 UR E27 인증절차를 만족하는 장비의 승인 문서와 보안 구역과 네트워크 구성도, 사이버보안 설계 문서(CSDD; cyber security design description), 선박 자산 목록, UR E26 적용을 받지 않는 CBS에 대한 위험 평가(risk assessment) 결과를 시스템 통합 업체를 통해 제출하여야 한다.

시운전 단계에서는 선박의 최종 시운전 전에 설계·건조 단계에서 제출된 문서의 최종본과 시험 및 평가 방법이 기술된 사이버 복원력 시험절차를 시스템 통합 업체를 통해 제출하고 선급의 입회하에 시험절차에 따라 수행한다. 선박 사이버 복원력 시험절차는 시험 조건을 재현하여 결과를 검증하고 얻어진 결과를 비교할 수 있도록 시험 장비, 초기 조건, 시험 방법론, 상세시험단계, 예상결과와 허용 기준이 명시되어야 하며, 각 CBS가 UR E27을 만족하는 경우 시운전 단계에서 각 CBS의 사이버 복원력 시험은 생략될 수 있다.

선박의 운항 단계에서는 선주가 UR E26에서 요구하는 프로세스를 수립하고 이행하기 위한 기술적, 조직적 보안대책의 주체로서 UR E26의 요구사항인 식별, 보호, 탐지, 대응, 복구와 이에 대한 17개의 세부사항의 관리와 이에 대한 사이버 복원력 테스트 절차의 업데이트 뿐 아니라, CBS와 선내 네트워크에서 발생한 변경사항, 새로운 사이버 위협과 취약성 및 선박의 운항 환경에 대한 변화를 반영하여 선박 사이버 복원력 테스트 절차를 업데이트 해야한다.

선주는 선박의 최초 연차 검사 시 CBS의 사이버보안 및 사이버 복원력 관리를 문서화 한 사이버보안 및 사이버 복원력 프로그램을 제출해야 하며 프로세스의 구현 기록 또는 증빙자료를 최초 검사 및 연차 검사 시 입증하여야 한다. 또한, 선주가 선박 관리 회사를 변경하는 경우에는 선박 사이버보안 및 사이버 복원력 프로그램에 대한 새로운 검증을 받아야한다.

Ⅲ. 선박 사이버 복원력 대응 기술의 요구조건

IACS UR E26 - 선박 사이버 복원력에 따라 제출되거나 유

지·관리되어야 하는 문서는 표 1과 같다[8]. 표 1과 같이 선박의 건조·시운전 단계에서는 시스템 통합 업체가 선박에 탑재되는 시스템과 장비의 UR E27 승인 문서를 제출하고, 네트워크 토폴로지, 보안 구역 정보, 네트워크 간의 보안 구성 정보 등이 담긴 구성도와 보안 구역 및 네트워크 세분화, 보안 요구사항별 설계 및 구현, 사이버사고 대응 및 복구 계획, CBS 적용제외 사이버 리스크 평가가 담긴 사이버보안 설계서(CSDD), 하드웨어·소프트웨어 정보, 네트워크 장치와 보안장치 정보가 명시된 선박 자산명세, CBS 제외에 대한 위험 평가 결과서, 보안대책과 선박 시험 절차서를 제출·관리한다.

시운전이 완료되면 선박 인도와 함께 선박 사이버 복원력 관련 문서는 선주에게 인도되어 변경관리절차(MoC; management of change)에 따라 선주에 의해 유지·관리되어야 할 뿐 아니라 표 1의 사이버보안 및 복원력 프로그램의 운영 주체로서 선박 사이버보안 및 복원력 프로그램을 개발하고 운항 종료 시까지 운영·관리하여야 한다.

IACS UR E26 대응과 IMO 및 국제기구의 선박 사이버보안 규제에 대응하기 위해서 조선소를 중심으로 조선·해양 및 산업 플랜트 분야에서 일반적으로 적용되지 않았던, 최초로 또는 새롭게 개발되는 부품, 재료, 기자재 및 시스템 등의 개념설계에 대한 승인인 기본 인증(AiP, approval in principle)을 받고있다. 또한 선박에 탑재되는 온보드 시스템과 장비에 대한 UR E27 이행에 대비하여 조선·해양 기자재 기업들은 제품의 설계도면을 검토·승인하고, 제조된 제품이 승인된 도면과 일치 여부와 사양의 적합성을 검사하고 성능을 증명하는 기자재 형식승인을 준비하고 있다.

하지만 선박의 전주기 동안의 선박 사이버 복원력을 확보하기 위한 UR E26에 대한 대응, 특히 선박의 운영관점에서의 사이버보안 및 복원력 프로그램에 대한 준비는 미미한 상황이다.

이에 본 논문에서는 2장에서 분석한 IACS UR E26의 5가지 요구조건과 17개의 세부사항, 표 1의 주요 제출문서를 기준으로 선박 전주기 동안의 선박 사이버 복원력 대응을 위한 기술을 그림 5와 같이 제안한다.

제안기술은 물리적 방법과 소프트웨어 도구를 이용한 방법으로 구분되며, 물리적 방법은 선급 인증문서·설계서 등 문서관리, 보안이 강화된 네트워크 구성, 사고 대응을 위한 프로세스 정립이 있으며, 소프트웨어 도구를 이용한 방법으로는 형상관리, 네트워크 통합관리, 멀웨어 보호, 보안 관리솔루션으로 구성하였다.

3-1 문서관리

표 1. 국제선급협회 선박 사이버 복원력의 주요 제출문서
Table 1. Summary of actions and documents.

Document	System integrator			Shipowner			
	Design	Construction	Commissioning	operation	1st AS	AS	SS
Approved supplier documentation [5]		maintain	maintain	maintain			
Zone and conduit diagram [5.1.1]	submit	maintain	maintain	maintain			
Cyber security design description [5.1.2]	submit	maintain	maintain	maintain			
Vessel asset inventory [5.1.3]	submit	maintain	maintain	maintain			
Risk assessment for the exclusion of CBSs [5.1.4] NOTE 1	submit	maintain	maintain	maintain			
Description of compensating countermeasures [5.1.5] NOTE 1	submit	maintain	maintain	maintain			
Ship cyber resilience test procedure [5.2.1]		submit	demonstrate	maintain			demonstrate
Ship cyber security and resilience program [5.3.1] - Management of change(MoC) [4.1.1.4.4] - Management of software updates [4.1.1.4.4] - Management of firewalls [4.2.1.4.4] - Management of malware protection [4.2.3.4.4] - Management of access control [4.2.4.4.4] - Management of confidential information [4.2.4.4.4] - Management of remote access [4.2.6.4.4] - Management of mobile and portable devices [4.2.7.4.4] - Detection of security anomalies [4.3.1.4.4] - Verification of security functions [4.3.2.4.4] - Incident response plans [4.4.1.4.4] - Recovery plans [4.5.1.4.4]				maintain	submit	demonstrate	

NOTE 1 : If applicable
Submit : The stakeholder shall submit the document to the Class society for verification and approval of compliance with requirements in this UR
Maintain : The stakeholder shall the document updated in accordance with procedure for management of change(MoC), Updated document and change management records shall be submitted to the Class society as per UR E22.
Demonstrate : The stakeholder shall demonstrate compliance to the Class society in accordance with the approved document.

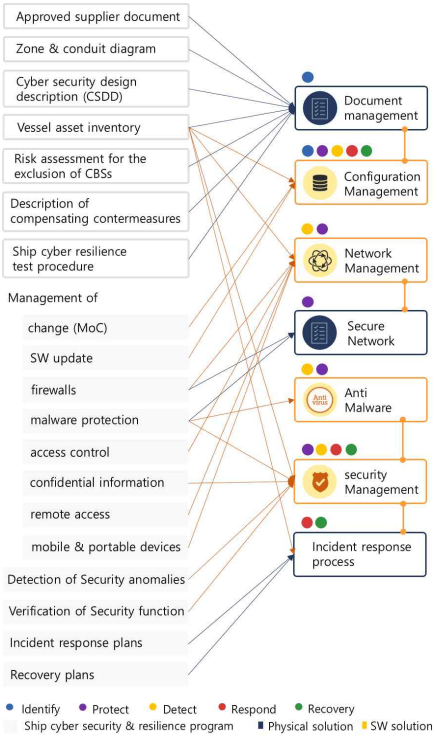

그림 4. 선박 사이버 복원력 대응을 위한 기술 제안
Fig. 4. Technical proposal for ship cyber resilience.

선박에서는 UR E27 승인 문서, CSDD, 선박 자산목록, CBS 제외에 대한 평가결과서, 보안대책과 선박 시험 절차서를 건조·시운전·운영 단계에서 최신의 상태를 유지해야 하며, 변경 이력과 세부 내용을 확인할 수 있도록 변경사항을 관리해야 한다. 문서는 책임자에 의해 증빙서류로 관리할 수 있으나 형상관리 프로그램을 통해 문서의 버전과 변경 이력 및 세부사항을 관리하여 업무 및 선급의 연차 검사 대응의 효율성을 높일 수 있다.

특히 선박 자산목록은 선박의 사이버보안관점에서의 기밀성(confidentiality), 무결성(integrity), 가용성(availability)을 위하여 관리 항목을 식별하고 식별된 항목의 우선순위를 정하여 보안 관리의 기준을 세우기 위함으로 문서의 변경 이력과 최신 정보가 시스템에 반영될 수 있도록 형상관리 프로그램으로 관리되어야 한다.

3-2 보안이 강화된 네트워크 구성

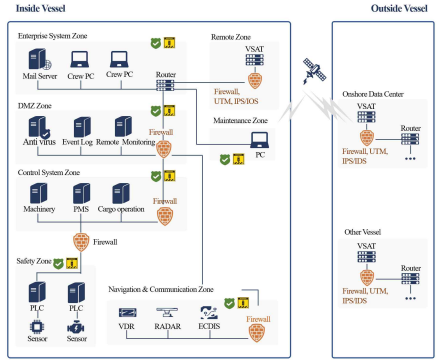

그림 5. 보안이 강화된 네트워크 예
Fig. 5. Example of a security-enhanced network.

선내 네트워크는 선박의 건조 단계부터 그림 6과 같이 운영 목적에 따라 물리적 또는 논리적으로 네트워크 구역을 구분하고 구역과 구역 사이에는 방화벽, 스위치와 같은 보안장치를 설치하여 보안사고 확산을 예방하여야 한다.

그림 6과 같이 위성 포트를 모니터링하거나 침입 탐지 시스템(IDS; intrusion detect system)등을 통하여 선육간 통신 구간의 육상에서 선박으로 인가되지 않은 연결, 비정상적인 통신 패턴, 권한 밖의 사용자 또는 시스템을 실시간으로 확인하여 선육간 통신 구간에서의 사이버 공격/위협을 감지할 수 있다.

선내는 각 구역의 방화벽, 스위치를 연동하여 외부 침입, 내부 위협 감지 등을 확인할 수 있으며, 사이버 사고 발생 시 해당 구역에 설치된 방화벽, 스위치 등을 제어하여 다른 구역으로의 사고 확산을 방지할 수 있다.

또한 선내 장치에 비인가 장치 또는 데이터를 사용하여 발생되는 사고를 예방하기 위해 선박에 설치된 모든 CBS에 멀웨어 보호장치를 설치하고 Port locker 등을 설치하여 비인가 장치를 차단하여야 한다.

3-3 사고 대응 프로세스

사이버 사고는 네트워크를 기반으로 급속히 피해가 확산되기 때문에 사고 발생 초기 탐지·대응이 필수적이나 선박은 운항 특성상 고립된 환경에서 제한된 인력이 근무하고 있으며, 네트워크·IT 전문인력이 부재하기 때문에 전문지식이 부족한 선내 인원이 사이버 사고에 신속히 대응할 수 있도록 사고 대응 프로세스가 정립되어야 한다.

사고 대응 프로세스는 선박 사이버 사고로 발생될 수 있는 비상 상황 즉, 사이버 사고목록을 작성하고 선박에 설치된 CBS에 사이버 위협이 탐지되면 신속하게 대응할 수 있도록 그림 7 한국인터넷진흥원의 사이버 침해 대응 7단계를 기반으로 선박에서의 사고 대응 프로세스를 정립할 수 있다[11].

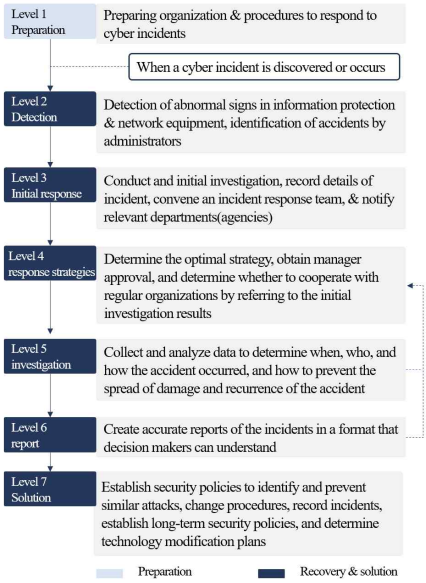

그림 6. 사이버 침해 대응 7단계 - 한국인터넷진흥원
Fig. 6. 7 steps to respond to cyber breaches.

해사 사이버 사고에 대한 신속한 대응을 위하여 사고 대응에 대한 프로세스를 사전에 정립하고 네트워크 통합관리, 보안 솔루션을 통해 선박 CBS의 네트워크 상태를 실시간 모니터링하여 사이버 침해를 탐지하고 사고 대응 프로세스에 따라 초기 대응, 최적의 전략을 결정하고 사고 조사, 의사결정자 결정을 위한 보고서 작성, 문제 해결을 위한 상세 계획을 수립한다.

사고 대응 프로세스도 문서로 관리·운영될 수 있으나 문서를 기반으로 선원이 직접 관리할 경우 선박에 설치된 수많은 CBS의 실시간 사이버 위협 탐지, 사고 대응 전략 및 원인 분석이 불가능하기 때문에 보안 솔루션을 통해 사이버 침해 사고 대응이 이루어져야 한다.

3-4 네트워크 통합관리

UR E26에 따라 선박에 설치된 모든 CBS의 상태를 모니터링 해야하나 선박 CBS의 연동 표준이 정립되어있지 않기 때문에 선내 CBS의 상태 모니터링 시 시스템 로그(syslog) 또는 SNMP (simple network management system)를 이용하고 있다. 그러나 이러한 방법은 개별 CBS의 상태를 모니터링하거나 네트워크 상태 또는 CBS 이상 시 해당 CBS의 On/Off를 제어할 수 있을 뿐 사이버 위협에 대한 분석, 검색, 위험 경보 생성 등의 관리가 불가능하다.

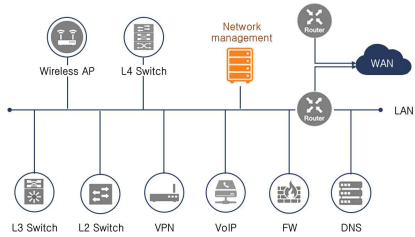

그림 7. 선내 네트워크 통합관리
Fig. 7. Integrated network management onboard ship.

그림 8. 네트워크 토폴로지기반 네트워크 모니터링
Fig. 8. Network topology-based network monitoring.

따라서 선박 네트워크 통합관리 솔루션은 그림 8과 같이 선박에 설치된 다양한 CBS에 API, 시스템 로그, 데이터베이스 등을 연동하여 데이터를 수집·정규화하여 사이버 위협의 정도와 대응 방안을 사고 절차에 따라 판단할 수 있어야 한다. 수집된 정보를 바탕으로 사고의 경중을 판단하여 사용자에게 종합된 정보를 제공하고 위험구역의 스위치/VPN/방화벽 등을 제어하여 사고의 확산을 방지해야 한다.

네트워크 통합관리 솔루션을 형상관리 프로그램과 연계하면 네트워크 토폴로지, 선박 자산목록을 기준으로 선내 네트워크에 연결된 모든 CBS를 확인하고 비인가 장치의 연결과 장비 사용 상태를 모니터링할 수 있다.

네트워크 토폴로지와 선박 자산목록을 기준으로 네트워크를 모니터링하면 그림 9와 같이 이상 징후가 탐지된 CBS의 상태와 위치 정보, 사고 대응을 위한 세부 정보를 선원이 쉽게 확인할 수 있어 사이버 위협에 신속하게 대응할 수 있다. 또한 선급 검사 시 각 CBS의 권한에 따른 접근, 승인된 장치의 연결, 서비스 거부 이벤트로부터 보호, 보안 감시 기록의 점검 등의 검사 항목을 네트워크 통합관리 솔루션을 통해 대응할 수 있다.

3-5 소프트웨어 기반 형상관리

선박의 모든 CBS는 사이버보안관점의 잠재적 취약점이 될 수 있으므로 선박 자산목록의 변경과 자산목록에 등재된 하드

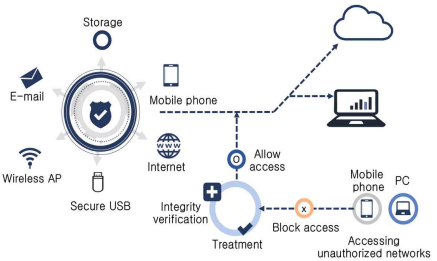

그림 9. 멀웨어 보호 솔루션
Fig. 9. Malware protection.

웨어·소프트웨어의 변경내역, 이력 그리고 변경됨으로써 고유의 기능 또는 다른 CBS에 미치는 영향을 검토할 수 있도록 소프트웨어 기반 형상관리 시스템을 통해 관리되어야 한다.

3-6 멀웨어 보호

안티바이러스와 같은 멀웨어 보호 솔루션은 그림 10과 같이 보안 솔루션과 연계하여 바이러스 위협 정보를 식별하여 사이버 위협에 대한 탐지 범위를 확장할 수 있으며, 비인가 장치접속 또는 멀웨어 솔루션을 통해 감지된 CBS의 식별과 세부사항, 이력을 관리할 수 있다.

멀웨어 보호 솔루션은 변화되는 사이버 공격에 대응할 수 있도록 네트워크 통합관리 장치를 통해 업데이트 패치를 배포하여 모든 CBS에 동일한 버전으로 설치·관리하여야 하며 형상관리 프로그램으로 업데이트 이력을 관리하여야 한다.

3-7 보안 관리

선내 CBS와 네트워크의 이상 징후를 탐지하기 위해서는 비정형 데이터와 보안 로그에서 침입자의 공격을 바르게 분석하고 예측해야 한다.

그림 11과 같이 데이터가 수집되지 않으면 분석할 수 없고, 분석하지 못하면 악성 여부를 판단할 수 없으며, 악성코드를 확인하지 못하면 사고 대응을 할 수 없다. 또한 분석 결과를 패턴화하지 못하면 동일한 위협을 자동으로 탐지할 수 없고, 패턴화 작성을 자동화할 수 없다면 알려지지 않은 새로운 위협에 대한 실시간 대응이 불가능하다[12].

따라서 그림 12와 같이 선박에 설치된 방화벽, 멀웨어 솔루션, 서버, 네트워크 장비 등의 다양한 로그와 보안 이벤트 정보를 수집하고 수집된 데이터를 식별·분석·관리할 수 있도록 정규화하여 해사 사이버 위협에 대한 지표와 분류기준을 개발하며 해상 고위험도 위협에 대한 분석과 학습을 통해 해사 이상위협 탐지 패턴을 개발함으로써 새로운 해사 위협에 대한 실시간 대응이 가능한 기술이 필요하다.

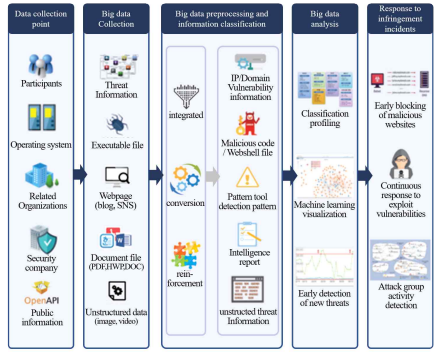

그림 10. 인터넷진흥원 사이버보안 빅데이터 센터
Fig. 10. Korea internet & security agency cyber security big data center.

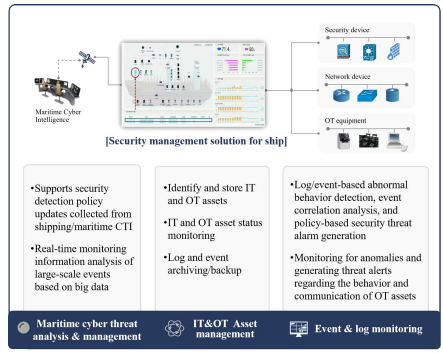

그림 11. 선박용 보안 관리 솔루션
Fig. 11. Cyber security management solution for ships.

선교에는 각종 항해장비로부터 나오는 많은 알람이 발생되어 항해사에게 위험 상황을 정확하게 전달하지 못하고 있으며 이를 개선하기 위한 선교경보관리시스템 (BAM; bridge alert management) 등이 도입되는 실정이다.

따라서 사이버 위협 이벤트 발생 시 바로 알람을 발생하는 것이 아니라 발생되는 이벤트를 누적으로 처리하고 다양한 조건으로 알람을 생성하여 선원이 직관적인 위협을 인지할 수 있도록 선별된 위협경보 전달이 필요하다. 또한 선박에는 IT 전문 인력이 부재하므로 선별된 위협정보와 이에 대한 가이드라인을 그림 9와 같이 선원에게 최적화된 대시보드를 통해 전달할 수 있는 신속한 침해사고 대응지원이 이루어져야 한다.

Ⅳ. 결 론

본 연구에서는 2024년 7월 1일 협약 이행을 앞둔 IACS UR E26을 분석하고 UR E26의 5가지 요구조건과 17개의 세부사항, 주요 제출문서를 기준으로 선박 전주기 특히, 운항 중 선박 사이버 복원력 대응을 위한 기술을 선급 인증문서 설계서 등의 문서관리, 보안이 강화된 네트워크 구성, 사고 대응을 위한 프로세스 정립, 소프트웨어 도구를 이용한 형상관리, 네트워크 통합관리, 멀웨어 보호, 보안 관리 솔루션으로 제안하였다.

선내 수많은 CBS 장비의 사이버보안을 장비 개별로 관리하거나 혹은 문서형태로 관리할 경우 선원 업무가 가중될 뿐 아니라 선급검사 시 증빙서류 검토 및 기능검증에 시수가 증가되어 비용과 운항에 영향을 줄 수 있다. 또한 스마트선박과 디지털화된 선박 특히 자율운항선박의 등장으로 증가 되는 해사 사이버 위협에 대한 실시간 대응과 제한된 인력 혹은 무인 환경에서도 침해사고 대응이 가능한 자동화된 기술이 필요하다.

이처럼 선박의 사이버보안 및 복원력 프로그램은 소프트웨어 기반으로 한정되지 않으나 선박의 환경과 고도화되는 해사 사이버 위협 대응을 위해서는 선내 사이버 위협을 탐지하고 자동 대응 및 선내·원격지 지원이 가능한 소프트웨어 기반의 선박용 보안 관리 솔루션이 필요하다.

Acknowledgments

본 연구는 2023년도 산업통상자원부 조선해양산업핵심기술개발사업(20026436)의 지원에 의하여 이루어진 연구로서, 관계부처에 감사드립니다.

References

[1] ITTP, Weekly ICT Trends, Vol.2105, pp.2-14, 2023

[2] TTA, ICT Standardization strategy map, Ver. 2023, pp.11-37, 2023.

[3] OCIMF, SIRE-overview-factsheet, pp.1-2, 2022.

[4] BIMCO, The guideline on cyber security onboard ship, Edition 4, pp. 1-39, 2023.

[5] IMO, Maritime cyber risk management in safety management systems, resolution MSV.428(98), pp.1, 2017.

[6] IMO, Guidelines on maritime cyber risk management, MSC-FAL/Circ.3/Rev.2, pp.1-6, 2022.

[7] International association of classification societies, Resolutions 153-164 [Internet]. Available https://iacs.org.uk/resolutions/recommendations/141-160.

[8] International association of classification societies, unified-requirements E26 Cyber resilience of ships – Rev.1, Nov, 2023 [Internet]. Available : https://iacs.s3.af-south-1.amazonaws.com/wp-content/uploads/2022/02/04140503/UR-E26-Rev.1-Nov-2023-CR.pdf.

[9] International association of classification societies, unified-requirements E27 cyber resilience of on-board systems and equipment-Rev.1, Sep, 2023 [Internet]. Available :https://iacs.s3.af-south-1.amazonaws.com/wp-content/uploads/2022/05/29103853/UR-E27-Rev.1-Sep-2023-CLN.pdf.

[10] National institute of standards and technology, Framework for improving critical insrastructure cybersecurity, Version 1.1, pp. 1-12, Aprol 2018 [Internet]. Available : https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.

[11] KISA, Infringement incident analysis procedure guide, Jen 2010 [Internet]. Available : https://www.kisa.or.kr/2060204/form?postSeq=11&page=1#fnPostAttachDownload.

[12] KISA, Korea internet & security agency cyber security big data center[Internet]. Available: https://sift.ssu.ac.kr/intro/orga/members/.

강 남 선 (Nam-seon Kang)

2005년 2월 : 목포해양대학교 기관시스템공학과 (공학석사),
2007년 12월 ~ 2008년 12월 : 대한조선 조선기본성능연구소,
2016년 9월 ~ 2022년10월 : 마린웍스 책임연구원,
※관심분야 : 해사위성통신, 선박자동화, e-Navigation, 해사 사이버보안
2005년 6월 ~ 2007년 11월 : 한국해양과학기술원 연구원
2005년 3월 ~ 2016년 8월 : 증소조선연구원 선임연구원
2023년 6월 ~ 현재 : 이글루코퍼레이션 수석연구원

손 금 준 (Gum-jun SON)

2006년 2월 : 목포해양대학교 기관시스템공학과
2011년 3월 ~ 2013년 2월 : 인하대학교 조선해양공학과(공학석사)
2013년 9월 ~ 현재 : 한국선급 책임연구원
※관심분야 : 해사위성통신, 선박자동화, e-Navigation, 선박 사이버보안
2006년 3월 ~ 2013년 2월 : STX 팬오션 1등기관사
2013년 2월 ~ 2013년 9월 : 한국해양과학기술원 연구원

박 래 천 (Rae-cheon Park)
2006년 2월 : 광주대학교 컴퓨터전자정보통신공학부 (공학학사)
2003년 3월 ~ 2004년 12월 : 동강대학교 전자계산소
2004년 12월 ~ 2009년 3월 : 연합뉴스 정보통신
2013년 7월 ~ 현재 : 이글루코퍼레이션 전략사업팀장
※관심분야 : 클라우드, 선박자동화, e-Navigation, 해사 사이버보안

이 창 식 (Chang-sik Lee)
2008년 2월 ~ 현재 : 이글루코퍼레이션 부장
※관심분야 : 정보보안, 보안컨설팅, OT보안, 해사 사이버보안

유 성 상 (Seong-sang Yu)
2017년 2월 : 인하대학교 조선해양공학과 (공학석사)
2017년 2월 ~ 2021년 1월 : 한국선급 사이버인증팀
2021년 10월 ~ 현재 : 중소조선연구원 특수선박지원센터
※관심분야 : 선박항해통신, e-Navigation, 해사 사이버보안, 스마트·자율운항선박