대한조선학회논문집 Research Paper
Journal of the Society of Naval Architects of Korea
eISSN:2287-7355, Vol. 61, No. 6, pp. 427-436, December 2024
https://doi.org/10.3744/SNAK.2024.61.6.427

IACS UR E26을 고려한 선박 네트워크 토폴로지 설계

손금준[1] · 최상훈[1] · 강남선[2] · 김성록[3]
(사)한국선급[1]
이글루코퍼레이션[2]
현대LNG해운[3]

Design of Ship Network Topology Considering IACS UR E26

Gumjun Son[1] · Sanghun Choi[1] · Namseon Kang[2] · Sungrok Kim[3]
Korea Register[1]
Igloo Coperation[2]
Hyundai LNG Shipping[3]

With the advent of smart ships, cyber security threats to ship control system are increasing. In order to strengthen ship cyber security, the IACS issued UR E26 in April 2022 and declared it to be applied to ships contracted for construction on July 1, 2024. Therefore, in this paper, we conduct research on ship networks that can respond to cyber threats by considering the distinct characteristic of the ship network construction environment and the requirements of IACS UR E26. For this purpose, we analyzed the reference model of IEC 62443 along with the requirements of IACS UR E26. In addition, we identified the network structure and characteristics of the recently built smart ship. Based on this, we propose a ship network model that includes the configuration setting of the network and security device along with the deployment of the OT/IT device in the ship. Finally, we applied the proposed ship network security model to the network of recently built smart ships to verify its function and performance.

Keywords : Zone & conduit(구역 & 도관), Firewall(방화벽), TCP/IP diode(TCP/IP 다이오드), Dry contacts(무전압 접점 입력), Simplex serial link(단방향 직렬 통신)

1. 서 론

선박에서의 산업제어시스템(ICS, Industrial Control System)은 선박 항해를 위해 필요한 최소한의 기능을 제공하는 기반 장치로서 산업 제어망(Network)이라는 매개체를 통하여 시스템 운영을 위한 다양한 정보가 상호 간 공유 또는 배포되고 있다.

21세기 초기 이전에 건조된 선박은 RS232 등 시리얼 통신을 토대로 별도의 사설망(private network)으로 네트워크가 구성되어 타 시스템 또는 육상과의 연계가 거의 이루어지지 않았다. 그러나, 최근 들어 선박에 탑재되는 시스템도 점차 첨단화, 통합화되어 선원에게 지능화된 항해 및 제어 감시 기능이 제공됨에 따라 선박 제어망 내 운영 기술(OT, Operating Technology)을 위한 정보통신기술(IT, Information Technology)의 도입이 점차 확대되고, 이로 인해 선박 제어망에 대한 사이버 보안 위협이 증대되고 있다 (Choi, 2020).

산업제어시스템은 IT 시스템과 주요한 운영적 차이점이 존재한다. 이에 기존 IT 시스템에 적용하던 보안 제어 방법을 OT 환경에 적용하기 위해서는 이에 부합되도록 보안 제어 방법이 변경되어야 한다. 따라서 기존 보안 프로그램을 OT 기술과 환경 요구사항 및 특성에 맞도록 개발/재구성하고, 이러한 기술을 활용하여 네트워크 체계를 구성하는 것이 산업제어시스템에서 보안성 강화를 위한 필수 요소이다 (Jeon, 2009).

선박이라는 특수한 환경 속에 구성된 산업제어시스템의 사이버보안 강화를 위해 국제선급연합회 (IACS, International Association of Classification Societies)는 2022년 4월 UR(Unified Requirement) E26 (2022)을 발행하고, 2024년 7월 1일 건조 계약되는 선박에 적용할 것을 선언하였다.

IACS UR E26은 선박의 사이버 자산 관리, 선박 네트워크 설계 및 운영, 사이버 사고 대응 및 복구 등이 포함된 선박 건조 및 운영을 위한 최소한의 필수 요구사항으로, 국내 대형 조선소의 경우 개념 승인 획득 (The Korea Maritime News, 2023), 보안 전문 기관과의 파트너쉽 체결 (The Korea Economic Daily, 2024) 등 IACS UR E26 대응을 위한 다양한 활동이 이뤄지고 있

Received : 25 July 2024 | Revised : 26 August 2024 | Accepted : 12 September 2024
† Corresponding author : Gumjun Son, gjson@krs.co.kr

다. 다만, 중소형 조선소의 경우 대형 조선소와는 다르게, 대상 장비 식별부터 어려움을 겪고 있는 실정이다.

본 논문에서는 이러한 연구의 필요성에 부응하여, 스마트 선박의 네트워크 구조 설계 및 구현을 위해 관련 규제 및 규정을 분석/연구하여 IACS UR E26에 부합되는 선박 네트워크 토폴로지를 제안하였다.

본 논문의 구성은 다음과 같다. 2절에서는 선박 네트워크 구조 설계를 위한 관련 규정 및 지침을 분석하였고, 3장에서는 분석된 결과를 토대로 선박 네트워크 보안 모델을 제안하였다. 그리고 4장에서는 3장의 모델을 실제 건조 중인 선박에 적용하여 모델에 대한 실용성을 검증하고, 5장에서는 결론을 제시하였다.

2. 관련 연구

2.1 IACS UR E26(Cyber resilience of ships)

IACS UR E26은 IEC(International Electrotechnical Commission) 62443(산업제어시스템 보안) 3-3(시스템 보안 요구사항 및 보안 등급)을 토대로 선박에 특성에 맞게 재구성한 산업계 규정으로 선박 건조 및 운영과 관련된 사이버 복원력에 관한 필수 요구사항을 다루고 있다. 동 규정은 선박 네트워크 및 산업제어시스템의 관리적, 기술적, 물리적 통제 항목을 나열하고 통제 항목별 수명주기 관점에서 상세 요구사항을 포함하고 있다.

IACS UR E26에서 제시하는 산업제어시스템(ICS, Industrial Control System) 보안 구조는 OT 네트워크와 업무용(IT) 네트워크를 포함하는 IP 기반 통신 인터페이스를 범위로 한정하고, 업무 목적 및 영역별로 네트워크를 분리하는 것을 제안하고 있다. 특히 필수 안전기능을 제공하는 시스템, 항해 및 통신시스템, 기관 및 화물 제어시스템, 무선 통신시스템을 별도의 보안 구역으로 설정하기를 권고하고 그 연결은 방화벽(firewall) 등을 통하여 구성하도록 요구하고 있다. IACS UR E26에서 권장하는 네트워크는 다음의 요구사항을 포함하여 Fig. 1과 같이 구성되어야 한다.

- 보안 영역의 네트워크는 다른 영역의 네트워크와 물리적 또는 논리적으로 분리되어야 함
- 필수 안전기능을 제공하는 CBS(Computer-Based System)는 별도의 보안 구역으로 그룹화되어 물리적으로 분리되어야 함
- 항해/통신시스템은 기관 또는 화물시스템과 별도의 보안 구역으로 분리되어져야 함
- 항해/통신시스템이 61162-460에 의해 승인되어 졌을 경우 전용 보안 구역 내 설치되어야 함

이와 함께, IACS UR E26은 방화벽 등 보안 구역을 구성하기 위한 장벽 디바이스의 형상 설정 요건을 다음과 같이 제시하고,

- 불필요한 포트, 프로토콜, 서비스 비활성화
- 설정된 트래픽 허용 범위 내 트래픽의 안정적인 관리
- 서비스 거부 및 네트워크 과부하 제어

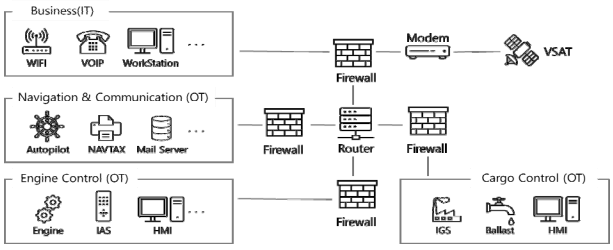

Fig. 1 UR E26 network requirements(segregation)

또한, OT 네트워크에 무선 통신이 활용될 경우, 접근 제어 관리와 함께 암호화 매커니즘을 통한 정보의 무결성, 기밀성 보장을 요구하고 있다.

2.2 IEC 62443(산업제어시스템 보안)

IEC 62443 (Security for Industrial Automation and Control Systems)은 미국 ISA(International Society of Automation)가 산업제어시스템(ICS)에 대한 보안 이슈를 다루기 위해 제정한 표준이다. ISO/IEC 62443 시리즈의 보안 요구사항 및 보안 대책은 산업제어시스템 환경에 적합하고, 특성화되도록 제정된 표준으로 일반, 정책 및 절차, 시스템, 컴포넌트의 4가지 범주로 분할 구성되어져 있다 (Kim et al., 2018).

IEC 62443 2-1 (2010)은 산업 자동화 및 제어 시스템 (IACS, Industrial Automation and Control System)을 위한 사이버보안 관리 시스템 (CSMS, CyberSecurity Management System)을 구축하는 데 필요한 요소를 정의하고 이를 위한 기준으로 Fig. 2와 같이 ICS 네트워크 참조 모델을 제시하고 있다. 동 참조 모델은 프로세스, 로컬 및 안전/보호, 감시 제어, 운영 관리, 엔터프라이즈 시스템 등 ICS를 구성하는 시스템별 역할을 기능으로 정의하고, 이를 다음과 같이 5가지 수준으로 분류하고 있다.

- Level 4 – 엔터프라이즈 시스템 : 생산 일정 계획, 운영 관리 및 유지보수 등과 관련된 인프라
- Level 3 – 운영관리 시스템 : 인사 및 교육, 엔지니어링에 필요한 데이터 수집 및 분석 등과 관련된 인프라
- Level 2 – 감시 제어 : 물리적 프로세스 모니터링 및 제어 (HMI) 등과 관련된 인프라
- Level 1 – 로컬 및 안전/보호 : 물리적 프로세스 감지 및 조작 (DLC, PLC, RTU 등) 등과 관련된 인프라
- Level 0 – 프로세스 : 장비에 직접 연결된 센서 및 액추에이터

또한, 방화벽 등 장벽 디바이스 배치를 통해 제어 영역, 비무장지대(DMZ, DeMilitarized Zone) 비즈니스 영역 등 3가지 보안 영역으로 세분화하고 있다.

- 제어 영역 : 산업제어시스템이 포함된 영역으로서, 기본적으로 모든 통신을 허용하지 않고, 간헐적인 대화식 통신만 허용, 외부로부터 접근 가능한 포트 및 서비스 차단

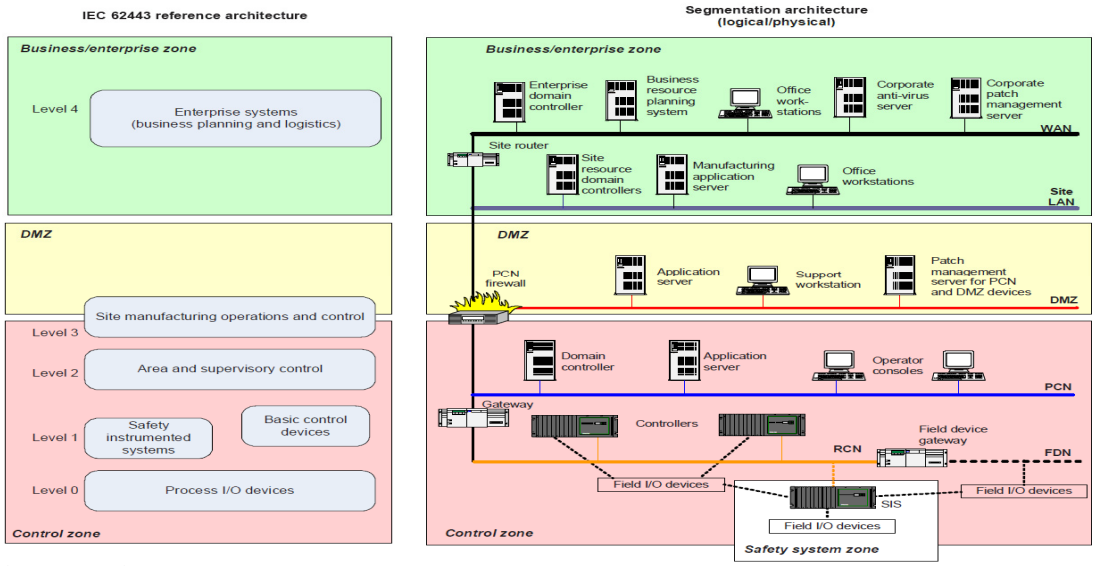

Fig. 2 IEC 62443 reference architecture

- 비무장지대 : 제어 영역과 비즈니스 영역 간 브릿지 또는 버퍼 역할 장치(RMS, Web Server 등) 등이 포함된 영역으로 서, 제어 영역 장치와 사용되는 포트 및 서비스와 비즈니스 영역 장치와 사용되는 포트 서비스를 다르게 설정
- 비즈니스 영역 : WAN을 통해 타 엔터프라이즈와 통신하거나 비즈니스 프로세스를 위한 IT 자산이 포함된 영역

2.3 현존선 네트워크 구성 현황

최근 국내 조선소에서 건조·인도된 스마트 선박의 네트워크 구조는 Fig. 3과 같이 통신 모뎀-L3스위치/L2스위치-OT/IT장치 순으로 배치되고 있다. 통상적으로 방화벽은 선주 공급품으로 선주의 요구에 따라 위성 통신 사업자에 의해 설치/관리되고 있으며, 대부분의 OT/IT 장치는 별도의 분리 없이 하나의 네트워크 장치(L3/L2 스위치)에 연결되어져 있다. 다만, 기관제어의 핵심 시스템인 IAS(Integrated Bridge System)의 경우 선내 네트워크와 별도의 사설 네트워크망으로 구성되어있다 (Son, 2024).

이러한 선박 네트워크는 사용 목적에 따라 Instrument 네트워크, Shipboard Control 네트워크, 4S(Ship-shore/shore-ship 통신) 네트워크 등 Table 1과 같이 분류된다 (Yoo, 2011).

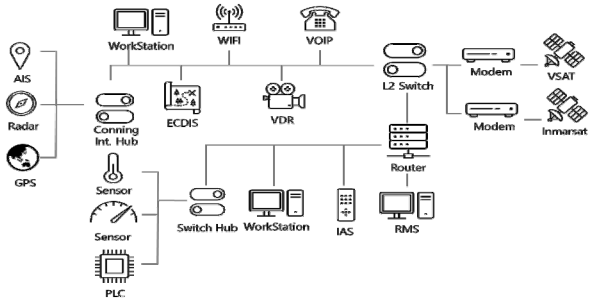

Fig. 3 Ship in service network topology

Table 1 Ship equipment list (Park et al., 2011)

Phase	System	Protocol
Instrument	GPS, Loran-C, Auto pilot, Anemometer, Gyro compass, Rudder, Speed Log, Radar, Echo Sounder, AIS, Rudder	IEC 61162-1/2 (NMEA0183)
	M/E control system, M/E oil system, M/E J.C.F.W., M/E air and exhaust gas system, M/E Misc, Generator engine, Boiler system, Purifier system, S/G system, Tank level gauge system, BWMS(Ballast Water Treatment System), Valve remote control system, Cargo pump system, Cargo valve system, Cargo tank system, System Error	TCP/IP
Instrument	ECDIS, VDR, BMS(Bridge Maneuvering System)	IEC 61162-1/2/450, TCP/IP
	PMS(Power Management System), CTMS(Custody Transfer Measurement System)	Modbus, CAN
	BHSMS(HullStress Monitoring System), Fire/Gas detection system	TCP/IP, IEC61162-1/2
Shipboard Control	IAS(Integrated Bridge System), BMWAS(Bridge Watch Monitoring System)	IEC 61162-1/2/450, TCP/IP
	ICMS(Integrated Control Monitoring System)	TCP/IP, CAN, IEC 61162-1/2
4S	VSAT System, Inmarsat system, Network system	TCP/IP

Instrument 네트워크는 IEC 61162(항해·통신 장비용 인터페이스) 프로토콜 등을 사용하는 항해 통신 장치 그리고 산업용 필드버스 분야에서 자주 사용되는 Modbus TCP, UDP 등을 사용하는 기관 및 화물 제어/모니터링 장치 등과 센서 간 실시간 정보 교환을 위한 네트워크이다.

Shipboard Control 네트워크는 시스템 통합 감시/제어를 목적으로 TCP/IP 프로토콜을 기반으로 Instrument 장치로부터 데이터를 수집하고, 제어 명령을 배포하기 위한 네트워크이다.

4S 네트워크는 VSAT 또는 Inmarsat 모뎀과 연결되어 e-Mail 서버, 선원 여가용 Wifi, 업무용 IT서비스 등 일반적인 IP 기반 프로토콜을 사용하는 네트워크이다.

2.4 네트워크 구역(Zone) & 도관(Conduit) 기술

네트워크는 요구사항을 공유하는 논리적 또는 물리적 자산 그룹인 구역(zone)과 통신을 목적으로 구역을 연결하는 케이블인 도관(conduit)으로 구성된다. IACS UR E26에서는 구역 & 도관을 구성하기 위한 장치로서 방화벽/라우터, TCP/IP diodes, Simplex Serial Links, dry contacts 등을 제시하고 있다.

2.4.1 방화벽/라우터

방화벽은 원치 않는 트래픽으로부터 네트워크를 보호하는 네트워크 보안 솔루션으로 사전에 프로그래밍된 일련의 규칙에 따라 악성코드를 차단하는 장치 또는 시스템이다. (FORTINET) 또한, 라우터는 네트워크를 상호 연결하고 데이터 패킷을 한 위치에서 다른 위치의 목적에 도착할 때까지 포워딩하는 장치로서, 네트워크 구역 및 도관 설정을 위한 가장 기본적인 장치이다. 방화벽 및 라우터는 Table 2와 같은 장·단점이 있다.

2.4.2 Simplex Serial Links

Serial 통신은 하나의 신호선을 이용하여 한번에 1 비트씩 전송하는 전기 통신 분야의 일반적인 직렬 데이터 통신 방법으로 송수신 장치의 역할이 정해져 한 방향으로만 전송이 가능한 단방향(Simplex), 송수신이 모두 가능 하지만 데이터를 전송한 후 수신이 가능한 Half Duplex, 데이터를 전송하는 동시에 수신이 가능한 Full Duplex 방식이 존재하며, Table 3과 같은 4가지 통신 프로토콜이 가장 널리 사용되고 있다.

Table 2 Firewall/Router pros and cons

Device	Functions	Advantage	Disadvantage
Fire wall	· Access control to services from in/outbound · Direction control of information about specific service · Service access control to users · Use means control for specific service	· Protect vulnerable services · Apply consistent security policies to all resources on the internal network · Host system access control · Maintain logs and statistics	· Vulnerable to viruses and new types of threats · Unable to respond to attacks by malicious internal users · Providing limited services · Unable to control bypass traffic
Router	· Setting the destination path of the packet · Change the IP address of packets sent to an external network · Prioritize network traffic based on data type · Direct access by external network remote users · Control the amount of data flowing through the network · Network traffic monitoring and fault diagnosis	· Enhanced security by acting as a network relayer · Improve Internet connectivity and information flow through network address translation · Improve traffic efficiency through dynamic routing · Traffic management through switching and filtering between packets	· Decreased network connection speed when a large number of traffic occurs · Additional costs due to installation difficulties · Quality problems due to time conversion issues

Table 3 Serial communication protocols

Property	RS232C	RS423	RS422	RS485
Operation	Single – Ended	Single– Ended	Differential	Differential
Maximum driver /receiver	1Driver 1Receiver	1Driver 10Receiver	1Driver 32Receiver	32Driver 32Receiver
Maximum distance range	15m	1.2Km	1.2Km	1.2Km
Maximum Transmission Speed	20Kb/s	100Kb/s	10Mb/s	10Mb/s
Transmission method	Full Duplex	Full Duplex	Full Duplex	Half Duplex

Simplex Serial 통신은 상기 언급된 바와 같이 데이터 전송이 한방향으로 만 이루어지는 통신으로 무전기, 라디오, 텔레비전 등 브로드캐스팅 통신에 널리 활용되고 있다. Simplex Serial 통신 예시로는 Fig 4와 같이 RS(Recommended Standard) 232C의 4개의 핀 중 2개의 핀을 결선하지 않는 것을 들 수 있다 (Byun, 2005).

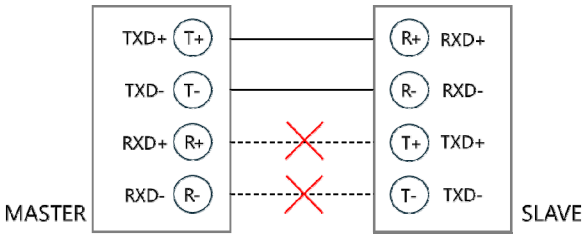

Fig. 4 RS232 based Simplex serial link example

2.4.3 TCP/IP diodes

데이터 다이오드(data diode)라고도 불리는 단방향 전송 기술 또는 시스템은 한 네트워크(A)에서 다른 네트워크(B)로 물리적인 단방향 연결을 제공하는 기술이다 (Kim and Min, 2016). 물리적으로 데이터를 단방향으로만 전송할 수 있기 때문에 데이터 다이오드는 두 지점 사이에 물리적 장벽 또는 “Air Gap”을 만든다. 이를 통해 데이터 유출을 방지하고, 악성코드로부터 위협을 방지하며, 데이터 다이오드의 네트워크 경로를 통해 외부 위협으로부터 송신 네트워크를 완벽하게 보호 할 수 있다. 데이터 다이오드는 보안관점에서 방화벽 및 라우터와 유사한 역할이 가능하지만 Fig. 4과 같은 차이점이 존재한다 (OWL Cyber Defense).

Table 4 Differences between diodes and firewall/router

Item	Firewall	Router (One-way gateway)
Difference	(Firewall) Software-based solution that requires patching and maintenance	(Router) Only handles a single protocol or data type per link
	(Diode) Hardware-based solution that cannot be modified or forced to operate after initial installation	(Diode) Transfer data to multiple servers or devices simultaneously without bottlenecks

2.4.4 Dry Contacts

Dry contact는 전원/전압이 스위치에 직접 제공되지 않고 스위치로 들어오는 신호/데이터를 활용하여 접점이 동작되는 릴레이/스위치로서, Dry contacts는 열림 또는 닫힘 두 가지 버전이 존재하며 Fig. 5와 같이 발전기, 알람 시스템, 에어컨 등 경보 등의 신호 조건에 Dry Contact가 주로 활용되고 있다 (Didactum Security, 2016).

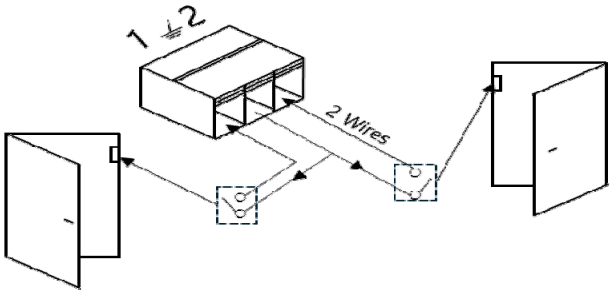

Fig. 5 Dry Contacts example

3. 선내 네트워크 보안 모델 제안

3.1 선내 네트워크 구역

네트워크 구역은 OT & IT 객체에 필요한 접근 허용 수준 및 방법을 공통적으로 적용하고, 관리할 수 있어야 한다. 이를 위해 본 논문에서는 IEC 62443의 참조 모델을 기반으로 2장의 선박 네트워크 정보를 활용하여 선박의 네트워크 구역을 Table 5와 같이 분류하였다.

Table 5 Ship network zone based on IEC 62443

Zone	Level	Description
Enterprise	Level 5	VSAT system, Inmarsat system, Mail server, Office PC, CCTV
DMZ	Level 4	ECDIS update server, PMS RMS, ICMS RMS, Smart platform
Control system	Level 3 (Central operation)	(NAV) IBS/INS, BMS, VDR
		(ENG) PMS, ICMS,
		(CARGO) BWMS
	Level 2 (Local operation)	(NAV)GPS, Loran-C, Auto pilot, Anemometer, Gyro compass, Rudder, Speed Log, RADAR, Echo sounder, AIS, BMWAS, ECIDS
		(ENG) M/E control system, M/E oil system, M/E J.C.F.W. system, M/E air and exhaust gas system, M/E misc system, generator engine, boiler system, purifier system, S/G system
		(CARGO) Water ballast, Water ballast valve, cargo pump, Cargo valve, Cargo tanks
	Level 1 (Safety)	Fire/Gas
	Level 0 (I/O device)	Sensor or Gauge (level, pressure, temperature), etc.

3.1.1 Enterprise zone

Enterprise zone은 선박 외부와 연결되는 관문이며, 선내 네트워크를 형성하는 구역으로 선내 IT 장치 및 어플리케이션 간의 연결을 제공하는데 사용하는 IT 인프라로 구성되어진다. 통상적으로 Enterprise zone에 설치되는 시스템은 2.3절에서 언급된 4S 네트워크 내 장치로서 선박-육상 간 통신을 위한 위성 통신 모뎀, 선박 네트워크 라우팅을 위한 라우터, 선원 복지를 위한 wifi 등 네트워크와 관련된 시스템, 그리고 업무용 VOIP 전화기, 선사 이메일 서버(ERP 등), 선내 설치된 사무용 PC 등을 포함하는 업무용 IT 시스템 등으로 구분 지을 수 있다.

3.1.2 DMZ zone

DMZ zone은 별도의 네트워크 구성 및 보안 정책을 갖는 구역으로써 Enterprise zone과 Control zone의 중간 지역에 구축되어 데이터 송·수신을 위한 가교 역할을 한다.

DMZ zone에 분류된 시스템은 Control zone으로부터 전달받은 데이터를 통해 육상에서 선박 내 대상 장치 상태를 모니터링하거나, 대상 장치에 제어 명령을 대신 전송하는 역할들로서, Integrated Automation System (IAS), EMS (Engine Monitoring System) 등에 원격 유지보수 또는 관제 서비스를 제공하기 위해 별도로 제공 되는 RMS (Remote Management Service), ECDIS의 해도 업데이트를 위해 설치된 업데이트 서버, 조선소 등에서 설치되는 스마트쉽 플랫폼 등이 이 계층에 위치된다.

3.1.3 Control System zone

Control zone은 선박 운항을 위하여 필요한 필수 OT 시스템이 위치되는 구역으로 상태 정보를 계측·수집하고 이러한 데이터를 통해 모니터링 또는 제어하는 역할을 수행하는 컴포넌트들로 구성된다.

Control zone은 IACS UR E26에 따라 항해/통신시스템, 기관제어시스템, 화물 제어시스템 등 목적에 따라 별도의 구역으로 설정되며. 각 구역은 2.2절에 정의된 3가지 수준(Lev. 0 ~ Lev. 3)으로 다음과 같이 재구성된다.

- Level 0 : 상태 데이터 계측·수집을 위한 센서(Input) 및 신호 처리를 위한 액추에이터(Output) 등 입출력 신호 처리를 위한 필드 디바이스
- Level 1 : 입출력 신호를 제어하기 위한 Programmable Logic Controller(PLC) 및 PC 등의 제어 디바이스로서, 선박 화재, 비상 제어와 관련된 시스템
- Level 2 : 입출력 신호를 제어하기 위한 Programmable Logic Controller(PLC) 및 PC 등의 제어 디바이스로서, 선박항해 및 기관 그리고 화물 제어와 관련된 시스템
- Level 3 : 컨트롤러, 센서, 액츄이이터 등을 연결하는 프로세스를 제어·감시하기 위한 통합된 시스템으로, IAS 및 Integrated Navigation System (INS), EMS 등이 포함됨

3.2 선내 네트워크 간의 도관

효율적인 선박 네트워크 구축을 위해서는 선내 네트워크를 구성하는 장치/시스템 및 프로토콜 등을 토대로 구역별 네트워크/보안 장치의 효율적 배치가 필요하다. 이에 본 절에서는 IACS UR E26에서 권고된 4가지 장치를 활용하여 각 구역별 연계 방안과 함께 설치된 네트워크/보안 장치의 형상을 제시하였다.

3.2.1 Enterprise zone

외부망과 선박 네트워크망 사이에 방화벽과 라우터를 병행 도입하여 공격자가 통과해야 할 두 개의 장벽을 세움으로서 심층 방어 체계의 초석을 다질 수 있다.

일반적으로는 패킷 필터링 서비스를 제공하는 라우터를 방화벽 앞단에 설치하여 대량의 입력 패킷으로부터 방화벽을 보호하도록 배치하고 있다. 다만, 선박의 경우 선박-육상 간 교환되는 트래픽 수준이 선내 트래픽 보다 높지 않고, 2Mbps ~ 4Mbps 수준의 낮은 통신 서비스를 활용하다는 점, 그리고 서비스 거부 공격(DDos, Distributed Denial of Service) 등 트래픽과 관련된 위협 보다는 포트 스캐닝 또는 랜섬웨어 등 방화벽으로 대응 가능한 위협이 보다 많이 발생되는 점을 고려하여 그림 6과 같이 통신 모뎀-방화벽-라우터(L3스위치) 순의 배치를 제안한다.

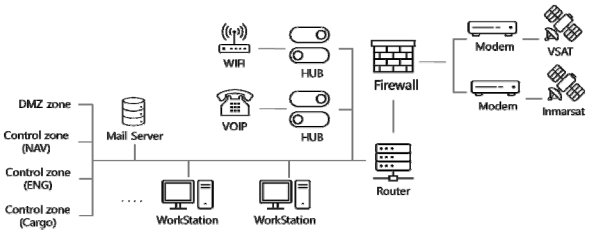

Fig. 6 Conduit for Enterprise

다만, 자율운항선박 또는 무인선이 도입되어 선박-육상 간 교환되는 트래픽이 증대되어 졌을 때는 통신 모뎀-라우터(L3스위치)-방화벽 배치를 고려해 볼 필요가 있다.

이와 함께 동 문서 2.1항에 언급된 네트워크/보안 장치의 형상 설정 요구사항을 만족시키기 위하여 다음과 같은 형상을 방화벽에 최소한 적용하여야 하며,

- (Access control) 패킷 필터링 또는 프록시 설정을 통한 허용된 서비스 및 메일 서버 등 특정 호스트를 제외한 접근 제한
- (Auditing / logging) 정책 및 권한 수정, 차단 등 이벤트 정보를 로그로 저장하고, 선내 보안 모니터링 시스템으로 전송

아래과 같은 형상을 라우터에 설정하여야 한다.

- (Network segregation) Wifi, 업무망 등을 Enterprise zone 내 논리적/물리적으로 분리
- (Privacy protection) Network Address Translation (NAT) 설정을 통해 내부 네트워크(LAN) 정보가 외부 네트워크로 유출되는 것을 차단
- (Auditing / logging) 정책 및 권한 수정, 차단 등 이벤트 정보를 로그로 저장하고, 선내 보안 모니터링 시스템으로 전송

3.2.2 DMZ zone

원격 유지보수 서비스 등 양방향 통신이 필요한 경우 방화벽을 적용하고, 상태 모니터링 등 정보 제공만 필요한 경우 TCP/IP diodes 설치를 통해 효율적으로 DMZ를 구성할 수 있다

방화벽을 통해 DMZ를 구성하는 경우, 데이터 서버 또는 제어망에 접근할 수 있는 PC, 원격 및 제3자 접근 시스템 등이 필요하며, Control zone에 의해 개시되는 연결에 대해서만 허용하는 방화벽 정책 등 Fig.7과 같이 삼각 방화벽 설정을 통해 DMZ를 형성하거나, Fig. 8과 같이 2개의 방화벽 중간에 DMZ를 구성하여 Enterprise 구역의 네트워킹이 Control system 구역으로 연결되는 것을 방지하도록 구성하여야 한다.

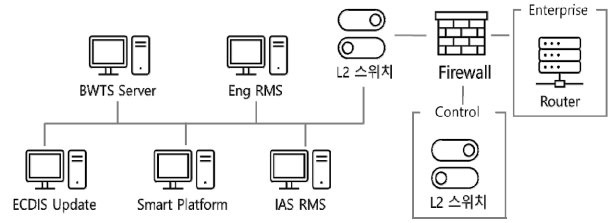

Fig. 7 Conduit for DMZ by one firewall

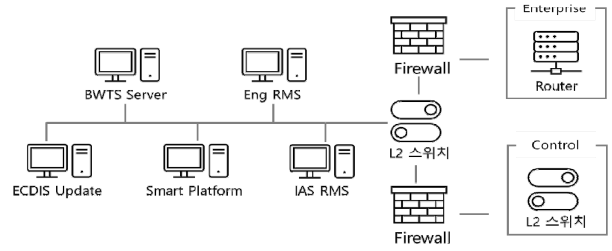

Fig. 8 Conduit for DMZ by two firewall

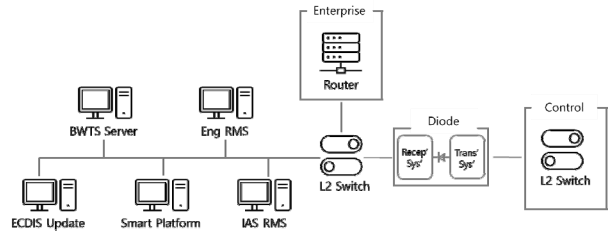

Fig. 9 Conduit for DMZ by Diode

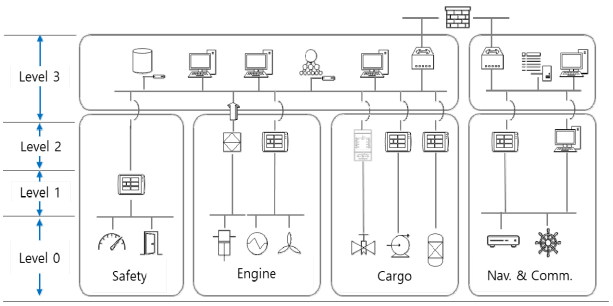

Fig. 10 Conduit for control system zone

Diode를 활용하여 DMZ 구성하는 경우, Fig. 9와 같이 Enterprise 구역에서 DMZ 구역으로 모든 연결을 차단하도록 구성/연결하여야 한다.

3.2.3 Control system zone

Control system zone은 IACS UR E26의 요구사항에 따라 Fig. 10과 같이 항해·통신시스템(NAV), 기관시스템(ENG), 화물시스템(CARG)으로 네트워크 망이 논리적 또는 물리적으로 분리되어야 한다.

Lev. 0~2 구간의 데이터 전송은 통상적으로 표준화 직렬 인터페이스인 hardwired I/O 방식의 연결이 가장 많이 사용됨에 보안을 위한 별도의 장치 배치는 불필요하다.

Lev.2~3 구간은 일반적으로 RS422 또는 RS485의 Multi-drop 방식 또는 Ethernet을 이용한 기기 간 연결이 이루어지고 있다. 이에 온도, 압력 센서 등 데이터 송신만 하는 기기의 경우 Simplex Serial Links, 액츄에이터 등 제어 기능이 포함된 경우 Dry Contacts 방식을 사용한 기기 간 연결을 통해 심층 방어 체계 구축이 가능하다.

4. 선내 네트워크 보안 모델 검증

4.1 실선 내 네트워크 보안 모델 적용

본 논문에서 제시한 선박 네트워크 보안 모델 검증을 위해 Fig. 10에서 건조 중인 선박에 본 논문에서 제시한 보안 모델을 적용하여 Fig. 11과 같이 네트워크를 재구성하였다.

Fig. 11 Target vessel (HLS)

L2 스위치 중심의 기존 선박의 네트워크 체계를 재구성하기 위하여 방화벽 및 L3 스위치 그리고 L2 스위치를 추가 공급하고, 그림 11과 같이 모뎀-방화벽-라우터-방화벽-L2스위치 순으로 네트워크 장치를 배치하였다. 그리고 각 구역의 물리적 분리를 위해 항해통신 OT 시스템, 기관 OT 시스템을 그룹핑하고 각 구역에 배치된 L2 스위치에 케이블 결선을 진행하였다.

선내 설치된 방화벽은 DMZ zone을 제외하고 각 구역의 특성에 따라 별도의 정책을 적용하였다. Enterprise zone의 방화벽은 선사에서 인가된 IP 및 도메인 정보를 기반으로 설정을 진행하였으며, Control zone의 방화벽은 내부 네트워크 간 필수 서비스를 제외하고 차단하도록 설정하였다. 다만, DMZ zone에 설치된 IAS, 스마트쉽 플랫폼의 경우 조선소 및 기자재업체의 보안상의 이유로 별도의 보안 정책 설정을 진행하지는 못하였다.

4.2 선박 네트워크 보안 모델 실증 결과

본 논문에서 제시한 모델이 IACS UR E26의 시험 요건을 충족하였는지 평가하기 위해 Table 6와 같이 IACS UR E26의 요건을 기준으로 시험 시나리오를 수립하였다.

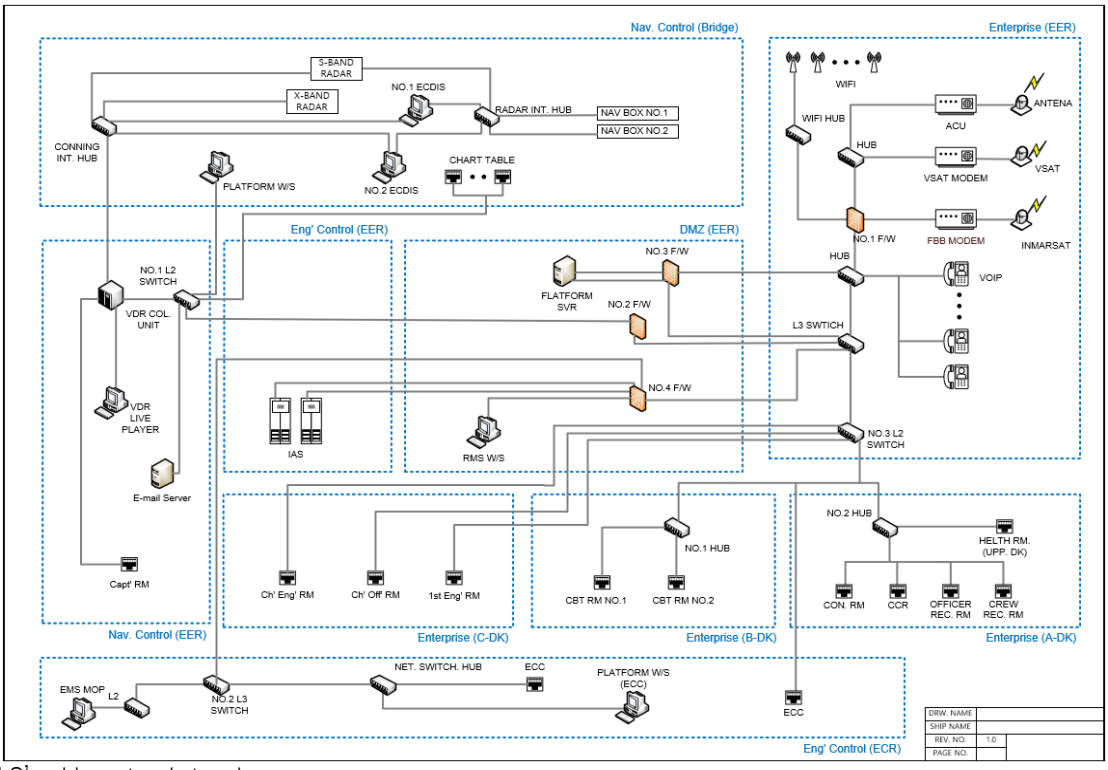

Fig. 12 HLS's ship network topology

Table 6 Cyber Threat scenario based on IACS UR E26

No.	UR E26 Requirement	Scenario
1	4.2.1 Security zones and network segmentation	Access attempt (Eng. → Nav. Control) · No.3 Firewall set to block web service (e-mail) port · Attempting to access a ERP installed on an email server after connecting a notebook to an ECC port · Checking inaccessible screen display
		Access attempt (Enterprise → Nav. Control) · Connect test laptop to L3 switch · Enter the ECDIS IP into the test notebook web browser(chrome) · "Site can't be reached" message in web browser
2	4.2.2 Network protection safeguards	Onboard network device denial of service attack · Connect test laptop to L3 switch · Transfer a large packet to a Capt. RM PC using a traffic generation solution (Hping) · Check the log of excess traffic event occurrences on the No.2 firewall
3	4.2.4 Access control	Access to Critical Assets by Unauthorized Persons · Add an L3 switch account and don't assign remote access rights to the account. · Attempt remote access using a new account ID using the head office PC (on shore) · "Site can't be reached" message in web browser
4	4.2.5 Wireless communication	Access attempt (Wifi → Nav.Control) · Connect to the ship's WIFI with the sailor's personal laptop · Enter the ship's e-mail IP into the sailor's personal laptop web browser(chrome) · "Site can't be reached" message in web browser
5	4.2.6 Remote access control and communication with untrusted network	Remote access failure · Attempt to access an unregistered ID on a VPN installed on board using a PC at the head office(on shore) · Trying to reconnect in the same way after checking for connection failure · Check the firewall for related events

이와 함께, 선박 내부, 선박-육상 간 발생 가능한 보안 위협을 임의로 생성하기 위하여 Fig. 12와 같이 모의 해킹 도구인 칼리 리눅스가 설치된 시험용 노트북을 선내 L3 스위치에 연결하고, 사용 가능한 IP를 할당하여 사이버 공격을 위한 환경을 구축하였다.

Fig. 13 Testing environment

시험용 노트북을 이용하여 Enterprise 구역 내 IT 장치, 항해 & 기관 OT 구역의 PC 등에 Ping Test(ICMP 기반 네트워크 장치 연결 여부 확인)를 실시하였다. 이를 통해 선내 네트워크의 기본 기능(네트워크 연결) 및 성능(모든 항목 3ms 이내 전송)을 검증하였다. 이와 함께, 상기 정의된 시나리오 기반 시험을 통해 ①불필요한 포트 및 프로토콜 그리고 서비스 비활성화 여부(시나리오 1) 검증, ②설정된 트래픽 허용 범위 내 트래픽의 안정적인 관리(시나리오 1, 3, 4, 5) 여부 확인, ③서비스 거부 및 네트워크 과부하 제어(시나리오 2) 등을 확인하였다.

5. 결 론

본 논문에서는 선박 건조 및 운영과 관련된 사이버 복원력에 관한 필수 요구사항인 IACS UR E26과 함께 산업제어시스템 보안 요구사항(IEC 62443)의 참조 모델을 분석하였다. 또한, 최신 건조/인양된 스마트 선박의 네트워크 구조 및 특성을 파악하고, IACS UR E26에 언급된 구역 및 도관을 형성하기 위한 장치로서 Firewall, Simplex Serial Links, TCP/IP diode, Dry Contacts 등의 특징을 살펴보았다.

본 논문에서는 상기 분석된 결과를 토대로 선박 네트워크 보안 모델을 제안하고 제안된 보안 모델을 구성하기 위한 방안을 제시하였다.

선박 네트워크 보안 모델은 IEC 62443 참조 모델과 마찬가지로 3가지(Control, DMZ, Enterprise) 구역 6가지 레벨로 네트워크를 구분 짓고 다시 제어망은 항해·통신, 화물 제어, 기관 제어 영역으로 정의하였다.

또한, 본 논문에서는 활용되는 프로토콜에 따라 네트워크 구역을 형성하기 위한 보안 장치를 다르게 권고하고 있다. IP 기반 통신 네트워크의 경우 기본적으로 방화벽에 정책을 적용하기를 권고하고 있으며, 전 수명주기 관점에서 탈거 등 변경이 될 가능성이 없거나, 강화된 보안이 필요할 경우 DMZ와 제어망 사이의 경계 보안 방안으로 TCP/IP Diode 활용을 제안하고 있다. 이와 함께 주로 Serial 통신을 사용하는 Lev.2 ~ Lev.3 네트워크는 통신 유형(단방향, 쌍방향)에 따라 Simplex Serial Links 또는 Dry Contacts를 배치하기를 권고하고 있다.

본 논문에서 제안된 선박 네트워크 보안 모델은 최근 건조된 스마트 선박의 네트워크에 적용하여 기능과 성능 등 실용성을 검증하였다.

본 연구를 통해 변화되는 국제 규제와 기술 수요에 대처하고 조선 산업의 경쟁력 및 부가가치 제고를 위한 주요한 기반을 구축 할 수 있으리라 사료되며, 향후 도래할 자율운항 또는 무인선 연구에 많은 도움이 되리라 본다.

후 기

본 논문은 2024년도 해양수산부 및 해양수산과학기술진흥원 연구비 지원으로 수행된 '자율운항선박 기술개발사업(20200615)'의 연구결과입니다.

본 연구는 2024년도 산업통상자원부 조선해양산업핵심기술 개발사업(20026436)의 지원에 의하여 이루어진 연구로서, 관계부처에 감사드립니다.

References

Byun, P.S., Kim, M.H., Kim, D.J., Park, S.H. and Park, Y.S. 2005, The implementation of home network using the RS422 Multi-drop mode serial communication, *Journal of the Korea Institute of Information and Communication Engineering*, 9(7), pp.1445-1451.

Choi, I.J., 2020, A empirical study on the patch impact assessment method for industrial control network security compliance, *Journal of The Korea Institute of Information Security & Cryptology,* 30(6), pp.1141-1149.

Didactum Security, 2016, Dry contact I/O monitoring, URL: https://www.didactum-security.com/en/blog/dry-contact-i/o-monitoring.html. [Accessed 19 May 2016]

FORTINET, 2020, What is a network firewall?, URL: https://www.fortinet.com/kr/resources/cyberglossary/firewall. [Accessed 19 September 2020]

IEC-62443-2-1, 2010, *Industrial communication networks - Network and system security Part 2-1 : Establishing and industrial automation and control system security program,* 2010.

International association of classification societies(IACS), 2022, unified- requirements E26 Cyber resilience of ships -

Rev.1, URL : https://iacs.s3.af-south-1.amazo naws.com /wp-content/uploads/2022/02/04140503/UR-E26-Rev.1-Nov-2023-CR.pdf. [Accessed 4 February 2022]

Jeon, Y.H., 2009, Network design and architecture for ICS security, *The Korea Institute of Information Security and Cryptology,* 19(5), pp.60-67.

Kim, D.W. and Min, B.G., 2016, Design of a reliable Dta diode system, *Journal of The Korea Institute of Information Security & Cryptology,* 26(6), pp.1571-1582.

Kim, I.Y. Lim, H.T. Ji, D.B. and Park, J.P., 2018, A efficient network security management model in industrial control system environments, *Journal of The Korea Academia-Industrial cooperation Society*, 19(4), pp.664-673.

OWL Cyber Defense, 2018, What is a Data Diode & How Do Data Diodes Work?, URL: https://owlcyberdefense.com/blog/what-is-data-diode-technology-how-does-it-work/. [Accessed 25 July 2018]

Park, J.W. Lim, Y. K. Yun, C. H. Lee, J. W. and Chung H. N., 2011, The Current situation of the digital interface international standards and an analysis of integration condition of ships, *Journal of the Society of Naval Architects of Korea*, 48(6), pp.490-500.

Son, G.J. Ahn, J.W. Lee, C.S. Kang, N.S. and Kim, S.R., 2024. Research on security detection policy model in the SIEM for ship. *Journal of the Society of Naval Architects of Korea,* 61(4), pp.278-288.

The Korea Maritime News, 2023, KR-HD Hyundai 'Cyber Resilience of Ships' Approval in Principal, URL: http://www.haesanews.com/news/articleView.html?idxno=109955 [Accessed 12 May 2023]

The Korea Economic Daily, 2024. HD Hyundai Marine Solution to enter ship cyber security, URL: https://www.kedglobal.com/shipping-shipbuilding/newsView/ked202401220008. [Accessed 22 January 2024]

Yoo, Y.H., 2011, Domestic technology trends in ship standard networks, *TTA Journal,* 133, pp.116-121.


손 금 준


최 상 훈


강 남 선


김 성 록