Overview of IACS UR E26 - Cyber Resilience of Ship

2022. 07.

한국선급 사이버인증팀(cyber@krs.co.kr)

Overview of IACS UR E26

Cyber Resilience of Ship

2019 Maritime Authority 해사 사이버보안 유닛 설립

2017 U.K government 선박 사이버보안 행동 강령 발표

2016 BIMCO 선박 사이버보안 가이드라인 발간

2018, 2019 선박 사이버보안 가이드라인 개정 2판, 3판 발간

2020 선박 사이버보안 가이드라인 개정 4 발간

2019 DCSA 선박 사이버보안 이행 가이드 1판 발간

2017 IMO 해사 사이버 리스크 관리 가이드라인 승인

2017 IMO 2021년까지 선주와 선박 관리사들에게 사이버 리스크의 ISM 코드 내 안전관리체계(SMS) 통합을 권고하는 결의서 채택

2022 사이버보안 UR E26, E27 배포

2017 USCG 해양 운송 보안법 규제 시설에 대한 사이버 리스크 관리에 대한 가이드라인 초안 개발

2020 USCG 선박 사이버 리스크 관리 업무 지침 발표

2019 MPA 해상 사이버보안 운영센터 개설

주관청에서 IMO MSC.428(98)에 다라 선주와 선박 관리사들에게 2021년 이후 첫 DOC 심사에서 사이버 리스크가 안전관리체제(SMS)에서 적절히 다루어지고 있는지를 권고사항으로 확인 중.

USCG, Germany, Greece, Marshall Island, Singapore, Australia, Cyprus, Vanuatu 등 22개 기국 강제사항으로 적용

2017 TMSA 3에 사이버보안 관련 위협 식별 포함하는 절차 및 요건 포함

2018 SIRE VIQ 7 7.14에 사이버보안 요건 추가

2017 Rightship "건화물선에 대한 검사 및 평가 보고서"에 사이버보안 리스크 평가 및 비상대응계획 추가 요구

2021 RightShip 검사 선박 질문지(RISQ)에 사이버 리스크의 ISM 통합 등 사이버보안 요건 포함

Overview of IACS UR E26

Cyber Resilience of Ship

2016 — Establishment

2018 — Recommendation (Deleted)

2020 — Recommendation

2022 — Unified Req.

Cyber Systems Panel

- All 12 Class Societies
- Communicate with IMO & EU, Industry

- **선박의 사이버물리시스템**(CPS)
- **시스템 보증**
- **통합 문제**
- **소프트웨어 품질 관리**
- **데이터 전송, 무결성 및 보안 제어**

Rec. 153~164

- Recommended procedures for software maintenance of computer based systems on board
- Recommendation concerning manual / local control capabilities for software dependent machinery systems
- Contingency plan for onboard computer based systems
- Network Architecture
- Data assurance
- Physical security of onboard computer based system
- Network security of onboard computer based systems
- Vessel System Design
- Inventory List of computer based systems
- Integration
- Remote Update / Access
- Communication and Interface

Rec. 166

- Recommendation on **Cyber Resilience***

UR E26, E27

- **Cyber Resilience** of Ships (UR E26)
- **Cyber Resilience** of on-board system and equipment (UR E27)

*선박 복원력(Cyber Resilience) : 선박의 안전한 운항을 위해 사용되는 운영기술(OT)의 중단 또는 손상으로 인해 발생하는 사 발생을 줄이고 영향을 완화하는 기능을 의미한다

UR EXX
- Cyber Verification
(2022.05~2023.04)

Overview of IACS UR E26

Cyber Resilience of Ship

E26 (Apr 2022)

Cyber resilience of ships

1. Introduction

Interconnection of computer systems on ships, together with the widespread use onboard of commercial-off-the-shelf (COTS) products, open the possibility for attacks to affect personnel data, human safety, the safety of the ship, and threaten the marine environment.

Attackers may target any combination of people and technology to achieve their aim, wherever there is a network connection or any other interface between onboard systems and the external world. Safeguarding ships, and shipping in general, from current and emerging threats involves a range of measures that are continually evolving.

It is then necessary to establish a common set of minimum functional and performance criteria to deliver a ship that can indeed be described as cyber resilient.

IACS considers that minimum requirements applied consistently to the full threat surface using a goal-based approach is necessary to make cyber resilient ships.

1.1 Structure of this UR

Table 1: Structure of this UR

Introductory Part	1 Introduction
	2 Definitions
	3 Goals and Organization of Requirements
Main Part	4 Requirements 4.1 Identify 4.2 Protect 4.3 Detect 4.4 Respond 4.5 Recover
	5 Test plan for performance evaluation and testing 5.1 During design and construction phases 5.2 Upon ship commissioning 5.3 During the operational life of the ship
Supplementary Part	6. Risk assessment for exclusion of CBS from the application of requirements (required only when systems are excluded from application of this UR)
	Appendix: Summary of Actions and Documents

Note:

1. 이 UR은 **2024년 1월 1일 이후에 건조 계약된 선박**에 대해 IACS 선급협회에 의해 일관되게 적용되어야 하며 그 외 선박들에 대해서는 비강제 지침으로 사용될 수 있다. **이 UR의 비강제 시험 적용을 위한 충분한 시간을 허용하기 위해** 적용 일자는 2024년 1월 1일로 선택되었다.

2. "건조계약"일이란 선주와 조선소가 선박을 건조하기로 한 계약을 체결한 날을 의미한다. 건조계약 일자에 대한 자세한 사항은 IACS PR(절차 요구사항) No. 29를 참고한다.

1.2 목표 및 목적(Aim and Purpose)

이 UR의 목표는 이해 관계자에게 사이버 복원력을 가진 선박으로 이어지는 기술적 수단을 제공할 목적으로 **선박 *사이버 복원력(Cyber Resilience)에 대한 최소 세트의 요구사항을 제공**하는 것이다.

***선박의 안전한 운항을 위해 사용되는 운영기술(OT)의 중단 또는 손상으로 인해 발생하는 사 발생을 줄이고 영향을 완화하는 기능을 의미한다**

이 UR은 사이버 복원력에 대한 집합체로서 선박을 목표로 하며, 선내 시스템, 장비 및 구성품들의 사이버 복원력을 다루는 산업 표준 및 다른 UR의 상호보완적 적용을 위한 기반으로 의도된다.

선내 시스템 및 장비의 사이버 복원력에 대한 최소 요구사항은 IACS UR E27에 기술되어 있다.

선내 시스템 및 장비가 이 UR의 적용 범위에 속한 컴퓨터 기반 시스템의 일부이지만 개별 객체로 간주되지 않는 한, 이러한 시스템 및 장비에 대해서는 IACS UR E27에서 강제하는 것보다 더 엄격한 요구사항이 UR의 만족을 지원하기 위해 요구될 수 있다.

1.3 적용범위(Scope of applicability)

a) **선박 내 운영 기술**(OT) **시스템**, 즉 물리적 프로세스를 제어 또는 감시하기 위해 데이터를 사용하여, 사이버 공격에 취약할 수 있고, 만약 손상될 경우, 인명의 안전, 선박의 안전 및 또는 환경에 위협에 대한 위험한 상황을 초래할 수 있는 **컴퓨터 기반 시스템**(**이하** CBS)

- 추진
- 조타
- 앵커링 및 무어링
- 전기 발전 및 배전
- 화재 탐지 및 소화 시스템
- 화물 제어 시스템 (안전 관련 요소에 한함)
- 빌지 및 평형수 시스템, 적개/하역 시스템, 로딩 컴퓨터
- 보일러 제어 시스템
- 해양 오염 방지를 위한 선급 및 국제법을 준수하기 위해 필요한 스크러버 제어 지스템 및 기타 시스템
- 수밀 무결성 및 침수 탐지
- 조명 (예: 비상 조명, 저위치 조명, 항해등 등)
- 다른 기타 OT 시스템
- 중단 또는 기능 손상이 선박 운영에 위험을 초래할 수 있는 기타 모든 OT 시스템 (예: LNG 감시 및 제어시스템, 관련 가스 탐지 시스템 등)

1.3 적용범위(Scope of applicability)

추가로, 이 UR의 적용 범위에는 다음 시스템들을 포함한다.

- 협약 규정에서 요구되는 **항해 시스템**
- 선급 규칙 및 협약 규정에서 요구되는 **내부 / 외부 통신 시스템**

항해 및 무선 통신 시스템의 경우 IEC 61162-460 또는 IEC 63154 표준이 적용 될 수 있다.

Part	Title
IEC 61162-1(NMEA 0183)	Part 1: Single talker and multiple listener
IEC 61162-2(NMEA 0183)	Part 2: Single talker and multiple listener, high speed transmission
IEC 61162-3(NMEA 2000)	Part 3: Serial data instrument Network
IEC 61162-450	Part 450: Ethernet interconnection
IEC 61162-460	Part 460: Ethernet interconnection - safety a nd security
IEC 63154	Cybersecurity – General Requirements, methods of testing and required test results

1.3 적용범위(Scope of applicability)

b) 이 UR의 범위에 속하는 CBS로부터 다른 시스템으로의 IP **기반 통신 인터페이스**이러한 시스템의 예는 다음과 같으며 이에 국한되지 않는다.

- 여객 및 방문객 서비스 및 관리 시스템(passenger or visitor servicing and management systems)
- 여객 대상 네트워크(passenger-facing networks)
- 관리 네트워크(administrative networks)
- 선원 복지 시스템(crew welfare systems)
- 영구 또는 임시로(예: 유지보수 동안) OT 시스템에 연결되는 다른 시스템

컴퓨터 기반 시스템 및 사이버 복원력에 대한 추가 IACS **문서**는 다음과 같다.

1) IACS **UR E22** On Board Use and Application of Computer based systems

2) IACS **UR E27** Cyber resilience of on-board systems and equipment includes requirements for cyber resilience for on-board systems and equipment.

3) IACS Recommendation **166 Recommendation** on Cyber Resilience

6. 요구사항 적용 제외를 위한 CBS의 리스크 평가

이 UR의 적용 범위에 속하는 CBS가 관련 요구사항의 적용에서 제외하는 경우 리스크 평가를 수행해야 한다. 리스크 평가는 제외된 CBS와 관련된 허용 가능한 리스크 수준의 증거를 제공해야 한다. 관련 요구사항에서 제외된 애플리케이션의 간결한 목록은 선내 CBS 문서와 함께 생성되고 유지되어야 한다(예: 시험 계획 및 관련 업데이트된 시험 계획의 실행)

6.4 허용 기준(Acceptance Criteria)

a) CBS에 영향을 미치는 사이버 사고에서 파생되는 예측 가능한 취약성, 위협, 잠재적 영향이 리스크 평가에서 적절히 고려되었다.

b) CBS의 공격 표면은 복잡성, 연결성, 무선 AP를 포함하여 물리적 및 논리적 접근 지점을 고려하여 최소화 된다.

c) CBS가 속한 통합 시스템에서 기능과 역할을 고려하여, CBS는 다른 CBS 또는 네트워크 장치에 의해 매개되는 사이버 사건의 영향을 받을 수 없으며, 사이버 사고의 영향이 다른 CBS 또는 네트워크 장치로 전파할 수 없다.

d) CBS는 필수 서비스 또는 다중 선박 서비스를 제공하지 않아야 한다.

e) CBS는 접근이 통제된 구역에 위치해야 한다.

6. 요구사항 적용 제외를 위한 CBS의 리스크 평가

6.4 허용 기준(Acceptance Criteria)

f) 다른 CBS에 대한 CBS의 연결이 적절하게 조사, 이해 및 문서화 되어야 한다. 특히, CBS는 IP 기반 네트워크에 의해 다른 CBS 또는 장치에 연결되지 않아야 한다.

g) CBS에는 통제되지 않은/보안되지 않은 이동식 장치에서 사용할 수 있는 물리적 인터페이스가 없어야 한다.

h) CBS에 설치된 소프트웨어가 적절하게 식별되었으며 각 소프트웨어 애플리케이션, 운영 체제 및 펌웨어(해당되는 경우)의 목적, 이름, 버전, 제공업체 및 유지보수업체에 대한 증적이 제공된다.

i) CBS는 유지보수 정책의 적용을 받으며 정책에 신뢰할 수 없는 네트워크에 대한 영구적 또는 일시적 연결 또는 통제되지 않는/안전하지 않은 이동식 장치의 사용을 포함하지 않는다.

j) CBS는 하드웨어 및 소프트웨어 무결성 검사를 포함한 기능 무결성과 제공된 서비스 품질을 언제든지 검사할 수 있는 수단을 제공한다.

k) CBS는 인간 운영자가 로컬 수동 제어를 할 수 있는 적절한 인터페이스를 제공하며, 이러한 인터페이스는 공격 표면을 확장하지 않는다. (또한, b) 참조)

l) 사고 대응 계획 및 복구 계획에는 선박에서 사이버 사고가 발생한 경우 CBS를 처리하는 방법에 대한 표시를 포함한다.

3. 요구사항의 목표와 구성

5가지 기능 요소

4.1 **식별**(Identify) : 선내 시스템, 사람, 자산, 데이터 및 기능에 대한 사이버 보안 리스크를 관리하기 위한 조직적 이해를 개발한다.

4.2 **보호**(Protect): 사이버 사고로부터 선박을 보호하고 선박 운항의 연속성을 최대화하기 위한 적절한 보호 장치를 개발 및 구현한다.

4.3 **탐지**(Detect): 선내 사이버 사고의 발생을 탐지하고 식별하기 위한 적절한 조치를 개발하고 구현한다.

4.4 **대응**(Respond): 선내에서 탐지된 사이버 사고에 대한 조치를 취하기 위한 적절한 조치 및 활동을 개발 및 구현한다.

4.5 **복구**(Recover): 사이버 사고로 인해 손상된 선박 운항에 필요한 모든 기능 또는 서비스를 복구하기 위한 적절한 조치 및 활동을 개발하고 구현한다.
이러한 하위 목표와 관련 기능 요소는 동시에 이루어져야 하며 하나의 포괄적인 리스크 관리 프레임워크의 일부로 간주되어야 한다

Overview of IACS UR E26

Cyber Resilience of Ship

UR E26 프레임워크 및 요구사항(17개 항목)

Identify (4.1)

- 선내 CBS 및 네트워크 목록(Inventory)

Protect (4.2)

- 보안 구역 (Security Zones)
- 네트워크 보호 안전장치(Safeguard)
- 안티바이러스, 안티멀웨어, 안티스팸 및 악성코드로부터 보호
- 접근 통제(Access control)
- 무선 통신(Wireless Communication)
- 원격 접근 통제 및 신뢰할 수 없는 네트워크에서 통신
- 모바일 및 휴대용 장치의 사용

Detect (4.3)

- 네트워크 운영 모니터링
- CBS 및 네트워크의 진단 기능

Respond (4.4)

- 사고 대응 계획 (Incident response plan)
- 로컬, 독립 및/또는 수동 운전
- 네트워크 격리 (Network isolation)
- 최소 위험 조건으로의 대비책(Fallback to a minimal risk condition)

Recovery (4.5)

- 복구 계획
- 백업 및 복구 기능 (Backup and restore capability)
- 제어된 종료, 리셋, 롤백 및 재시작

성능 평가 및 시험(Performance Evaluation and Testing)

검사원 또는 다른 제3자가 의도한 시험 조건을 선내 재현하고, 시험을 실행하고, 시험 결과를 검증하며, 공급자(Supplier) 및/또는 **조선소(Shipyard)/ 시스템통합자(System Integrator)**에 의해 얻은 결과와 비교가 가능하도록 시험 절차를 기술하는 **시험계획을 제출**해야 한다.

시험 절차에는 기능 시험, 고장 시험, 정상 상태, 경고 및 경보를 알리는 데 사용되는 경보 및 기타 모니터링 수단에 대한 설명이 포함되어야 한다.

부록 : Summary of actions and documentation

Document	Reference Requirement	Phase	Supplier	Shipyard System Integrator	Shipowner Company	Class
Protect						
Documentation of the product, equipment or component supplied to construct network segregation, including a diagram of zones and conduits and the configuration of traffic filtering/shaping rules	Network segmentation / segregation	**Design**	Provide			Approve
		Construction		Maintain		Info
		Commissioning		Provide		Info
		Operation			Maintain	
		Survey			Make avail.	Check
Documentation on network protection measures including a test plan to verify the implemented control	Network protection sefaguards	**Design**	Provide			Info
		Construction		Maintain		Info
		Commissioning		Provide		Approve
		Operation			Maintain	
		Survey			Make avail.	Check
Antivirus, antimalware and antispam software installed or other security measures applied	Antivirus, antimalware, antispam and other protections from malicious code	**Design**	Provide			Approve
		Construction		Maintain		Info
		Commissioning		Provide		Info
		Operation			Maintain	
		Survey			Make avail.	Check
Installation locations, physical access restrictions, credential management policy, removable media access points	Physical and logical access control	**Design**	Provide			Info
		Construction		Maintain		Approve
		Commissioning		Provide		Info
		Operation			Maintain	
		Survey			Make avail.	Check

APPENDIX

기능	하위 항목	요구사항
식별 (Identity)	4.1.1 **선내 CBS 및 네트워크 목록**(Inventory)	이 UR의 적용 범위에 있는 CBS의 하드웨어 및 소프트웨어(응용 프로그램, 운영 체제, 펌웨어, 기타 소프트웨어 구성 요소를 포함)와 이러한 시스템을 서로 간 및 선내 다른 CBS 또는 육상에 연결하는 **네트워크의 목록은 선박의 전체 수명 동안 제공되고 최신으로 유지되어야 한다**.

하드웨어 목록에는 최소한 다음 정보가 포함되어야 한다.

1. 각 CBS에 대한 간략한 기능 설명 및 **기술적 특징(브랜드, 제조업체, 모델, 주요 기술 데이터)**과 함께 이것의 목적에 대한 간략한 설명
2. 선내 다양한 CBS 사이 및 CBS와 외부 장치 또는 네트워크 사이의 **논리적 및 물리적 연결을 식별하는 블록 다이어그램**, CBS를 연결하는 네트워크의 토폴로지 및 각 노드의 의도된 기능.
3. 스위치, 라우터, 허브, 게이트웨이 등과 같은 **네트워크 장치**의 경우, 연결된 서브 네트워크에 대한 설명, **IP 범위, 연결된 노드의 MAC 주소(또는 네트워크 내 사용되는 프로토콜에 특정한 주소/식별자)**
4. 모든 의도된 작동 모드에서 각 네트워크의 주요 특징**(예: 사용된 프로토콜)** 및 통신 데이터 흐름**(예: 데이터 흐름 다이어그램)**
5. CBS의 물리적 위치 및 네트워크 접근 포인트의 **물리적 위치를 포함**하여, 선내 CBS를 연결하는 각 디지털 네트워크의 물리적 레이아웃을 설명하는 지도.

APPENDIX

기능	하위 항목	요구사항
식별 (Identity)	4.1.1 **선내 CBS 및 네트워크 목록**(Inventory)	이 UR의 적용 범위에 있는 CBS의 하드웨어 및 소프트웨어(응용 프로그램, 운영 체제, 펌웨어, 기타 소프트웨어 구성 요소를 포함)와 이러한 시스템을 서로 간 및 선내 다른 CBS 또는 육상에 연결하는 **네트워크의 목록은 선박의 전체 수명 동안 제공되고 최신으로 유지되어야 한다.**

소프트웨어 목록은 각 소프트웨어 응용 프로그램, 운영 체제, 펌웨어 등에 대해 최소한 다음 정보가 포함되어야 한다.

1. 소프트웨어가 설치된 CBS와 목적의 짧은 설명, **기술적 특징(브랜드, 제조업체, 모델, 주요 기술 데이터)** 및 특정 기능의 간략한 설명
2. **버전 정보, 초기 설치 및 만료 일자가 포함된 라이선스 정보, 업데이트 로그**
3. **유지보수 정책(예: 현장 대 원격, 주기적 대 임시적 등) 및 책임자**
4. **역할 및 책임을 포함한 접근 통제 정책(예: 읽기, 쓰기 및 실행 권한 포함).**

APPENDIX

기능	하위 항목	요구사항
보호 (Protect)	4.2.1 **보안 구역** (Security Zones)	이 UR의 적용 범위에 있는 모든 CBS는 잘 정의된 보안 통제 정책 및 보안 기능이 있는 **보안 구역으로 그룹화**되어야 한다. 보안 구역은 격리(예: 에어 갭)되거나 구역 사이에 통신하는 데이터 통제를 제공하는 수단(예: 방화벽/라우터, 심플렉스 시리얼 링크, TCP/IP 다이오드, 드라이 접점 등)을 통해 다른 보안 구역 또는 네트워크에 연결되어야 한다. 오직 명시적으로 허용된 트래픽만 보안 구역 경계를 통과해야 한다.

보안 구역에는 여러 개의 CBS와 네트워크가 포함될 수 있으며, 이들 모두 본 UR 및 UR E27에 제공된 보안 요구사항을 만족해야 한다.

1. 보안 구역의 네트워크는 **논리적 또는 물리적으로 다른 구역 또는 네트워크와 분할**되어야 한다. (4.2.6.3 또한 참조)
2. 요구되는 **안전 시스템(Safety System)을 제공하는 CBS는 별도의 보안 구역으로 그룹화**되어야 하며 다른 보안 구역과 **물리적으로 분**할되어야 한다.
3. **항해 및 통신 시스템**은 **기관 또는 화물 시스템**과 동일한 보안 구역 내에 있지 않아야 한다.
4. **무선 장치**는 전용의 보안 구역에 있어야 한다. (4.2.5 또한 참조)
5. **이 UR의 적용 범위 밖에 있는 다른 OT 시스템 또는 CBS**는 이 UR에서 요구하는 보안 구역과 **물리적**으로 분할되어야 한다. 대안적으로 이러한 OT 시스템이 구역에서 요구하는 것과 동일한 요구사항을 만족하는 경우, 다른 OT 시스템이 보안 구역의 일부로 허용된다.
6. 구역 내 CBS의 주요 기능에 영향을 주지 않고 보안 구역을 수동으로 격리하는 것이 가능해야 한다.
7. 보안 통제 정책의 정의에서 네트워크 상 접근하거나 작동하도록 허용된 기능은 기술 절차 및 역할과 연관되어야 한다.

APPENDIX

기능	하위 항목	요구사항
보호 (Protect)	4.2.2 **네트워크 보호 안전 장치**(safeguard)	이 UR의 적용 범위에 있는 CBS를 연결하는 네트워크는 **방화벽 또는 4.2.1항에서 지정된 바와 같이 동등한 수단으로 보호되어야 한다.** 네트워크는 과도한 데이터 흐름 속도 및 네트워크 리소스의 서비스 품질을 손상시킬 수 있는 기타 사건의 발생으로부터 보호되어야 한다. 이 UR의 범위에 있는 CBS는 최소 기능의 원칙에 따라 구현되어야 한다. 즉, 필수 기능만 제공하고 비필수 기능의 사용은 금지하거나 제한하도록 구성되어야 하고, **불필요한 기능, 포트, 프로토콜 및 서비스는 비활성화되거나 금지되어야 한다.**

네트워크 설계에는 네트워크를 통한 의도된 데이터 흐름을 만족하고 **서비스 거부(DoS) 및 네트워크 스톰/높은 트래픽 속도의 리스크을 최소화하기 위해 데이터 흐름 속도를 제한하는 수단이 포함**되어야 한다. 데이터 흐름 속도의 추정은 최소한 네트워크 용량, 의도된 애플리케이션 및 데이터 포맷에 대한 데이터 속도 요구사항을 고려해야 한다.

APPENDIX

기능	하위 항목	요구사항
보호 (Protect)	4.2.3 **안티바이러스, 안티멀웨어, 안티스팸 및 악성코드로부터 기타 보호**	이 UR의 적용 범위에 있는 CBS는 바이러스, 웜, 트로이 목마, 스파이웨어 등과 같은 **악성 코드로부터 보호**되어야 한다.

멀웨어 보호는 이 UR의 적용 범위에 있는 CBS에 구현되어야 한다. 산업 표준 안티바이러스 및 안티멀웨어 소프트웨어를 사용할 수 있고 최신으로 유지 관리되는 운영 체제가 있는 CBS에는 이러한 소프트웨어 설치가 요구되는 서비스(예: 실시간 임무를 수행하는 카테고리 II 및 III CBS)의 기능과 수준을 제공하는 CBS의 능력을 손상시키지 않는다면 **안티바이러스 및 안티 멀웨어 소프트웨어가 설치되어, 유지관리 및 정기적으로 업데이트되어야 한다.**
안티 바이러스 및 안티 멀웨어 소프트웨어를 **설치할 수 없는 CBS의 경우**, 멀웨어 보호는 **운영 절차, 물리적 보호 장치의 형태로 또는 제조업체의 권장 사항에 따라 구현**되어야 한다.

APPENDIX

기능	하위 항목	요구사항
보호 (Protect)	4.2.4 **접근 통제** (Access control)	이 UR의 적용 범위에 있는 CBS 및 네트워크는 시스템 자체와 통신하거나 상호 작용하는, 정보를 처리하는 시스템 자원을 사용하는, 시스템이 포함하는 정보의 지식을 얻는 또는 시스템 구성품 및 기능을 제어하는 능력과 수단을 **선택적으로 제한하는 물리적 및/또는 논리적/디지털 조치를 제공**해야 한다. 이러한 조치는 최소 권한 원칙에 따라 접근 수준에 대해 허가된 직원이 CBS에 접근하는 능력을 방해하지 않아야 한다.

이 UR의 적용 범위 내에 있는 CBS와 네트워크 및 이러한 시스템에 저장된 모든 정보에 대한 접근은 이들의 책무 또는 의도된 기능의 일부로서 **정보 접근의 필요성을 바탕으로 권한을 부여받은 직원, 권한이 부여된 프로세스 및 장치에만 허용되어야 한다.**

4.2.4.3.1 물리적 접근 통제 : Cat.II 및 Cat.III
4.2.4.3.2 방문자에 대한 물리적 접근 통제
4.2.4.3.3 네트워크 억세스 포인트의 물리적 접근 통제 : Cat.II 및 Cat.III
4.2.4.3.4 이동식 매체 통제 (Removable media controls)
4.2.4.3.5 자격증명 관리 (Management of credentials)
4.2.4.3.6 최소 특권 정책 (Least privilege policy)

APPENDIX

기능	하위 항목	요구사항
보호 (Protect)	4.2.5 **무선 통신**	이 UR 범위 내에 있는 무선 통신 네트워크는 다음을 보장하도록 설계, 구현 및 유지 관리되어야 한다. - 사이버 사고는 다른 제어 시스템으로 전파되지 않는다. - 승인된 사용자만 무선 네트워크에 억세스할 수 있다. - 승인된 프로세스 및 장치만 무선 네트워크에서 통신이 허용된다. - 무선 네트워크에서 전송 중인 정보는 조작되거나 공개될 수 없다.

산업계 표준 및 모범 사례에 따른 **암호화 알고리즘 및 키 길이와 같은 암호화 메커니즘이 무선 네트워크에서 전송되는 정보의 무결성과 기밀성을 보장하기 위해 적용**되어야 한다.
- 무선 네트워크의 장치는 무선 네트워크에서만 통신해야 한다. (즉, dual-homed가 아니어야 함).
- 무선 네트워크는 4.2.1항에 따라 별도의 세그먼트로 설계되어야 하고 4.2.2항에 따라 보호되어야 한다.
- 네트워크에 있는 무선 AP(액세스 포인트) 및 기타 장치는 네트워크에 대한 접근이 통제될 수 있도록 설치 및 구성되어야 한다.
- 무선 통신을 활용하는 네트워크 장치 또는 시스템은 통신에 참여하는 모든 사용자(사람, 소프트웨어 프로세스 또는 장치)를 식별하고 인증하는 기능을 제공해야 한다.

APPENDIX

기능	하위 항목	요구사항
보호 (Protect)	4.2.6 **원격 접근 통제 및 신뢰할수 없는 네트워크에서 통신**	이 UR의 범위에 있는 CBS는 **신뢰할 수 없는 네트워크로부터 무단 접근 및 다른 사이버 위협으로부터 보호**되어야 한다.

사용자 매뉴얼은 선내 IT 및 OT 시스템에 대한 원격 접근 통제를 위해 제공되어야 한다. 명확한 지침은 기능과 함께 역할과 허가를 식별해야 한다.
이 UR의 적용 범위에 있는 CBS에 대하여, 어떠한 IP 주소도 신뢰할 수 없는 네트워크에 노출되지 않아야 한다. 신뢰할 수 없는 네트워크로부터 보안 구역으로 패킷을 직접 라우팅하는 것이 가능하지 않아야 한다. 신뢰할 수 없는 네트워크와의 또는 이를 통한 통신에는 종점 인증, 무결성 보호 및 네트워크 또는 전송 계층에서의 **인증 및 암호화를 통해 보안 연결(예: 터널링)을 요구**한다. 읽기 권한이 필요한 정보에 대해서는 기밀성이 보장되어야 한다.

<Design 요구사항>
이 UR의 적용 범위에 있는 CBS는 다음을 만족하여야 한다.
- 선내 연결 종점으로부터 연결을 종료할 수 있는 기능을 가져야 한다. 모든 원격 접근은 선내 책임 있는 역할에 의해 명시적으로 수락할 때까지 가능하지 않아야 한다.
- OT 시스템의 안전한 기능이나 이들 시스템에서 사용하는 데이터의 무결성 및 가용성을 훼손하지 않도록 원격 세션 동안 중단을 관리할 수 있어야 한다.
- (예를 들어, 사이버 사고의 탐지 후에) 원격 연결의 오프라인 검토를 위해 충분한 기간의 시간 동안 모든 원격 접근 이벤트를 기록하고 유지하는 로깅 기능을 제공해야 한다.

APPENDIX

기능	하위 항목	요구사항
보호 (Protect)	4.2.6 **원격 접근 통제 및 신뢰할수 없는 네트워크에서 통신**	이 UR의 범위에 있는 CBS는 **신뢰할 수 없는 네트워크로부터 무단 접근 및 다른 사이버 위협으로부터 보호**되어야 한다.

<원격 유지보수에 대한 추가 요구사항>

원격접근이 유지보수에 이용되는 경우, 4.2.6.3.1항의 요구사항에 추가하여 다음 요구사항을 준수해야 한다.

- **육상 쪽과 어떻게 연결되고 통합되는지를 보여주는 문서**가 제공되어야 한다.
- 패치 및 업데이트는 설치 전에 유효하고 허용할 수 없는 부작용이나 사이버 사건을 일으키지 않는지를 확인하기 위해 설치되기 전에 시험 및 평가되어야 한다. 원격 업데이트를 수행하기 전에 소프트웨어 공급업체로부터 이에 대한 확인 보고서를 득해야 한다.
- 지원 계획이 개발되어 모든 이해 관계자가 이용 가능하도록해야 한다.
- 원격 유지 관리 활동 중에 언제든지 권한이 있는 직원은 활동을 중단하고 관련된 CBS 및 시스템의 이전의 안전한 구성으로 롤백할 수 있어야 한다.
- 신뢰할 수 없는 네트워크로부터 범위 내의 CBS에 인간 사용자에 의한 어떠한 접근에 대해서는 **멀티팩터 인증이 요구**되어야 한다.
- 접속 시도가 실패 했을 경우에는 다음 시도는 미리 정해진 시간 동안 시작되지 않아야 한다. **접속 시도 실패 횟수가 미리 정해진 값에 도달할 경우에 인증 기능이 차단**되어야 한다.
- 원격 유지보수 장소에 대한 연결이 어떠한 이유로 중단된 경우, 시스템 접근은 **자동 로그아웃 기능**에 의해 종료되어야 한다.

APPENDIX

기능	하위 항목	요구사항
보호 (Protect)	4.2.7 **모바일 및 휴대용 장치의 사용**	이 UR의 적용 범위에 있는 CBS에 대한 모바일 및 휴대용 장치의 연결 및 이러한 시스템을 연결하는 네트워크의 연결은 **선박의 운항 또는 유지보수를 위해 연결할 때를 제외하고 물리적 또는 논리적으로 차단되어야 한다**. 무선으로 연결된 모바일 및 휴대용 장치는 4.2.5항의 요구사항을 준수해야 한다.

선박의 운영상 사용을 위한 이동식 및 휴대형 장치는 물품 목록(inventory list)에 기록되어야 한다.
유지 보수를 위해 모바일 및 휴대용 장치를 사용될 때에는 물품 목록에 유지보수 정보를 기입하는 것이 필요하다. CBS에 장착된 모바일 및 휴대용 장치의 연결 포트에 대한 정보는 유지 관리에 사용되는 연결 포트를 포함하여 물품 목록에 포함되어야 한다.
이동식 매체용 차단기(Blocker)는 4.2.4.3.3항에 언급된 독립된 컴퓨터 이외의 물리적으로 접근 가능한 컴퓨터 및 네트워크 포트 상에 사용되어야 한다.
선원의 선내 운영 또는 공급자의 유지보수를 위해 사용되는 모바일 및 휴대용 장치의 연결 포트에 대하여 미리 정해진 장비 이외의 연결을 방지하기 위한 조치를 취해야 한다. 연결 포트에 대한 정보는 물품 목록에 포함되어야 한다.
물리적 또는 논리적 블록이 적용된 포트는 명확하게 표시되어야 한다.

APPENDIX

기능	하위 항목	요구사항
탐지 (Detect)	**4.3.1 네트워크 운영 모니터링**	이 UR 범위의 네트워크는 지속적으로 감시되어야 하며, 오작동 또는 용량 감소/저하가 발생하면 경보가 발생되어야 한다.

이 UR의 적용 범위 내에 있는 **네트워크를 모니터링하기 위한 조치**는 다음 기능을 포함해야 한다.
- 과도한 트래픽에 대한 모니터링 및 보호
- 네트워크 연결 모니터링
- 기기 관리 활동 모니터링 및 기록
- 미승인된 장치의 연결에 대한 모니터링 또는 보호

다음을 만족하는 **침입 탐지 시스템(IDS)**이 구현될 수 있다.
- IDS는 해당 CBS의 공급업체에 의해 자격이 부여되어야 한다.
- IDS는 수동적(passive)이어야 하며 CBS의 성능에 영향을 미칠 수 있는 보호 기능을 활성화하지 않아야 한다.
- 관련 직원은 IDS 사용에 대한 교육을 받고 자격을 갖추어야 한다.

APPENDIX

기능	하위 항목	요구사항
탐지 (Detect)	**4.3.2 CBS 및 네트워크의 진단 기능 (Diagnostic functions)**	이 UR의 적용 범위에 있는 CBS와 네트워크는 이 UR에서 요구하는 **보안 기능의 성능과 기능성을 확인**할 수 있어야 한다. **진단 기능**은 의도된 사용자의 사용을 위한 CBS 무결성 및 상태에 대한 적절한 정보와 선박의 안전한 운항을 위한 기능성을 유지하기 위한 수단을 제공해야 한다.

CBS 및 네트워크의 진단 기능성은 **선박의 시험 및 유지보수 단계 동안 모든 보안 기능의 의도된 운전을 검증**하는 것이 가능해야 한다.
CBS 및 관련 네트워크의 정상 작동 동안 **네트워크 연결 및 장치의 상태 뿐만이 아니라 과도한 네트워크 트래픽을 지속적으로 모니터링하는 진단 기능이 구현**되어야 한다.
진단 기능은 이상 징후가 탐지되면 책임있는 선원에게 경고해야 한다.

APPENDIX

기능	하위 항목	요구사항
대응 (Respond)	**4.4.1 사고 대응 계획 (Incident response plan)**	관련 비상상황을 다루고 사이버 보안 사고에 대응하는 방법을 상세화한 **사고 대응 계획**을 개발해야 한다. 사고 대응 계획에는 이 UR의 적용 범위에 있는 CBS에 대한 **사고를 탐지, 대응 및 결과를 제한하기 위한 미리 지정된 지침 및 절차 문서들를 포함**해야 한다.

첫 번째 연차 검사에서 **본선에 배치될 사고 대응 계획을 준비하기 위하여 선박의 설계 및 건조 단계에서 관련된 다양한 이해 관계자는 정보를 선주에게 제공**해야 한다. 사고 대응 계획은 선박의 수명 동안 최신으로 유지되어야 한다(예: 유지보수 시).
사고 대응 계획은 적절한 당국에 통보하고, 사고의 필요한 증거를 보고하고, 시기적절한 시정조치를 취함으로써 네트워크에서 탐지된 사이버 사고에 대응하고 사이버 사고 영향을 관련 네트워크 세그먼트로 제한하기 위한 절차를 제공해야 한다.
사고 대응 계획에는 최소한 다음 정보가 포함되어야 한다.

- 손상된 시스템의 격리를 위한 중단점(Breakpoint)
- 탐지된 진행 중 사이버 이벤트 또는 사이버 이벤트로 야기된 이상 증상을 알리는 경보 및 표시들에 대한 설명
- 사이버 사고와 관련하여 예상되는 주요 결과에 대한 기술
- (만약 있는 경우) 비상 정지(shut down) 또는 독립 또는 로컬 제어에 의존하지 않는 우선순위화 된 대응 옵션들
- 사이버 사고로 인해 고장난 시스템으로부터 독립적으로 운영하기 위한 독립의 로컬 제어 정보
- 사고 대응 계획은 전자 기기의 완전히 상실 시에도 접근이 가능하도록 하드 카피로 보관되어야 한다.

APPENDIX

기능	하위 항목	요구사항
대응 (Respond)	4.4.2 로컬, 독립 및/또는 수동 운전	SOLAS 협약 II-1장 31규칙에서 요구하는 **로컬 백업 제어에 필요한 모든 CBS는 주제어 시스템과 독립**되어야 한다. 여기에는 효과적인 로컬 작동에 필요한 HMI(Human Machine Interface)도 포함된다.

로컬 제어 및 모니터링을 위한 CBS는 자체 포함되어야 하며 의도된 작동을 위해 다른 CBS와의 통신에 의존하지 않아야 한다.
원격 제어 시스템 또는 다른 CBS에 대한 통신이 네트워크에 의해 연결되는 경우 4.2.1항 및 4.2.2항에 기술된 **분할 및 보호 안전조치**가 구현되어야 한다. 이는 로컬 제어 및 모니터링 시스템이 별도의 보안 구역으로 간주되어야 함을 의미한다.
로컬 제어 및 모니터링을 위한 CBS는 이 UR의 요구사항을 준수해야 한다.

APPENDIX

기능	하위 항목	요구사항
대응 (Respond)	**4.4.3 네트워크 격리 (Network isolation)**	네트워크 세그먼트와의 **네트워크 기반 통신을 수동으로 또는 자동으로 종료하는 것이 가능**해야 한다.

사고 대응 계획이 수행해야 할 조치로 네트워크 격리를 기술한 경우, 예를 들어, **네트워크 장치의 물리적 ON/OFF 스위치를 조작하거나 라우터/방화벽에 연결된 케이블을 분리하는 것과 같은 유사한 조치와 같이 기술된 절차에 따라 물리적 네트워크 세그먼트를 격리**할 수 있어야 한다. 효과적인 방식으로 네트워크를 격리하는 것을 직원에게 허용하는 장치에 대한 이용 가능한 지침과 분명한 마킹이 있어야 한다.

APPENDIX

기능	하위 항목	요구사항
대응 (Respond)	**4.4.4 최소 위험 조건으로의 대비책(Fallback to a minimal risk condition)**	의도된 서비스를 제공하기 위해 이 UR의 적용 범위에 있는 CBS 또는 네트워크의 능력을 손상시키는 **사이버 사고의 경우, 영향을 받는 시스템 또는 네트워크는 최소한의 리스크 조건으로 되돌릴 수 있어야 한다. (즉, 가능한 안전 이슈의 위험을 줄이는 안정적인 정지된 상태로 되돌리는 것)**

요구되는 대로 의도된 서비스를 제공하는 시스템의 능력을 손상시키며, CBS 또는 네트워크에 영향을 미치는 사이버 사고가 탐지되는 즉시, 시스템은 합리적으로 안전한 상태를 달성할 수 있는 조건으로 되돌려야 한다. 대비책 조치는 다음을 포함할 수 있다.

- 시스템을 완전히 정지시키는 것;
- 시스템 해제;
- 제어권을 다른 시스템 또는 인간 운전자에게 이전;
- 기타 보상 조치

최소 위험 조건으로의 대비책은 선박을 안전한 상태로 유지하기에 적절한 시간 프레임 내에 발생해야 한다.

최소 위험 조건으로 되돌아갈 수 있는 시스템의 능력은 공급업체와 조선소/선박 설계자/시스템 통합자가 설계 단계부터 고려해야 한다.

APPENDIX

기능	하위 항목	요구사항
복구 (Recover)	4.5.1 복구 계획	사이버 사고로 인한 중단 또는 장애가 발생한 후 이 UR의 적용 범위에 있는 CBS를 작동 상태로 복구하는 것을 지원하기 위한 **복구 계획이 수립**되어야 한다. 어디에서 누구에의해 지원이 가능한지에 대한 상세 내용이 복구 계획의 일부로 포함되어야 한다.

선박의 설계 및 건조 단계에 관련된 **다양한 이해 관계자**는 **첫 번째 연차 검사**에서 **본선에 배치될 복구 계획을 준비하기 위한 관련 정보를 선주에게 제공**해야 한다. 복구 계획은 선박의 운항 수명 동안 (예: 유지보수 시) 최신 상태로 유지되어야 한다.

복구 계획은 선원과 외부 직원이 쉽게 이해가 가능해야 하며, 고장 시스템의 복구를 보장하기 위한 필수 지침과 절차, 그리고 육상 지원이 필요한 경우 외부 지원을 받는 방법을 포함해야 한다. 또한, 선내에서 복구에 필요한 소프트웨어 복구 매체 또는 도구를 이용할 수 있어야 한다.

복구 계획을 개발할 때 관련되는 다양한 시스템과 하위 시스템들이 명시되어야 한다. 다음의 복구 목표도 또한 지정되어야 한다.

(1) **시스템 복구**: 통신 기능을 복구하는 방법 및 절차는 복구 시간 목표(RTO) 측면에서 지정되어야 한다. 이는 필요한 통신 링크 및 처리 기능을 복구하는 데 필요한 시간으로 정의된다.

(2) **데이터 복구**: OT 시스템의 안전한 상태 및 안전한 선박 운항을 복구하는데 필요한 데이터 복구 방법 및 절차는 RPO(복구 시점 목표) 측면에서 지정되어야 한다. 이는 데이터 부재가 허용될 수 있는 가장 긴 기간으로 정의된다.

APPENDIX

기능	하위 항목	요구사항
복구 (Recover)	4.5.1 복구 계획	사이버 사고로 인한 중단 또는 장애가 발생한 후 이 UR의 적용 범위에 있는 CBS를 작동 상태로 복구하는 것을 지원하기 위한 **복구 계획이 수립**되어야 한다. 어디에서 누구에의해 지원이 가능한지에 대한 상세 내용이 복구 계획의 일부로 포함되어야 한다.

일단 복구 목표가 정의되면 잠재적인 사이버 사고 목록이 생성되고, 복구 절차를 개발 및 기술되어야 한다. **복구 계획은 다음 정보를 포함하거나 참조**해야 한다.
(1) 이중화, 독립 또는 로컬 운전을 통해 운전의 중단 없이 실패한 시스템을 복원하기 위한 지침 및 절차
(2) 정보의 백업 및 안전한 저장을 위한 프로세스 및 절차
(3) 완전한 최신의 논리 네트워크 다이어그램
(4) 고장 시스템 복구를 담당 직원 목록
(5) 시스템 지원 업체, 네트워크 관리자 등 외부 기술 지원을 위해 연락하기 위한 통신 절차 및 직원 목록
(6) 모든 구성품들 대한 현재 구성 정보
선내 직원의 안전을 보장하기 위한 선박의 운전 및 항해가 계획 내에서 우선시되어야 한다.
선내 및 육상의 복구 계획 하드카피는 사이버 보안을 책임자와 사이버 사고 지원 담당자가 이용할 수 있어야 한다.

APPENDIX

기능	하위 항목	요구사항
복구 (Recover)	**4.5.2 백업 및 복구 기능 (Backup and restore capability)**	이 UR의 적용 범위에 있는 CBS 및 네트워크는 **시기적절하고 완전하며 안전한 방식으로 백업 및 복원을 지원**할 수 있어야 한다. 백업은 정기적으로 유지 관리되고 시험하여야 한다.

4.5.2.3.1 복구 기능

이 UR의 적용 범위에 있는 CBS는 사이버 사고 후 선박이 빠르고 안전하게 항해 및 운영 상태를 회복할 수 있도록 **백업 및 복원 기능**을 가져야 한다.
- 데이터는 안전한 사본 또는 이미지로부터 복원할 수 있어야 한다.
- 정보 및 백업 설비는 사이버 사고로부터 복구하는데 충분해야 한다.

4.5.2.3.2 백업

이 UR의 적용 범위에 있는 CBS 및 네트워크는 **데이터 백업을 제공**해야 한다. 오프라인 백업의 사용은 온라인 백업 기기에 영향을 미치는 랜섬웨어 및 웜바이러스에 대한 내성을 향상시키기 위해 고려되어야 한다.
범위, 모드 및 빈도, 저장 매체 및 보존 기간을 포함한 백업 계획을 수립해야 한다.

APPENDIX

기능	하위 항목	요구사항
복구 (Recover)	**4.5.3 제어된 종료, 리셋, 롤백 및 재시작 (Controlled shutdown, reset, roll-back and restart)**	이 UR의 적용 범위에 있는 CBS 및 네트워크는 **사이버 사고로 인해 가능한 손상으로부터 신속하고 안전한 복구가 가능하도록 제어되는 종료, 초기 상태로 리셋, 안전한 상태로 롤백 및 전원이 꺼진 상태에서 재시작할 수 있어야 한다.** 상기 언급된 작업을 실행하는 방법에 대한 적절한 문서는 선내 직원이 이용할 수 있어야 한다.

이 UR의 적용 범위에 있는 CBS 및 네트워크는 다음의 역량을 갖추어야 한다.

- 전체 시스템을 안전하고 일관적이며 알려진 상태로 남을 수 있도록, 다른 연결된 시스템이 보류 중인 트랜잭션을 **롤백**, 프로세스 종료, 연결 끊기 등을 허용하 통제된 종료
- 시스템을 셧다운 프로세스를 거쳐 메모리를 지우고 장치를 초기화 상태로 재설정하도록 지시하는 자체 재설정
- 시스템 무결성 및 일관성을 복원하기 위해 이전 구성 및/또는 상태로 **롤백**
- 읽기 전용 소스에서 모든 소프트웨어 및 데이터의 프레쉬 이미지(예: 롤백 작업 후)를 재시작 및 다시 로드. 재시작 시간은 시스템의 의도된 서비스와 호환되어야 하며 다른 연결된 시스템 또는 이 시스템이 속한 통합 시스템을 일관성이 없거나 안전하지 않은 상태로 만들지 않아야 한다.

사이버 사고의 영향을 받는 시스템의 경우 위에서 언급한 작업을 실행하는 방법에 대한 문서가 선내 직원에게 제공되어야 한다.

Thank you for your attention!

Any Questions?

Providing the best service,
Creating a better world