

# 리스크 기반 신조선 사이버 설계보안 접근 방식

박 개 명\*, 임 정 규\*

## 요 약

국제해사기구(IMO)는 2017년 해사안전위원회(Maritime Safety Committee, MSC)에서 안전관리시스템으로의 해상 사이버 리스크 관리 결의하였다. 또한 국제선급협회(IACS)는 선박 사이버 사고가 인명, 재산 및 환경에 심각한 영향을 미칠 수 있음을 인식하여, 사이버 이슈를 체계적으로 논의하기 위한 사이버시스템 패넬을 2016년 신설하였다. IACS 는 2022년 4월, 신조선 사이버보안 통합 요구사항(UR E26) 및 기자재 시스템 사이버보안 통합 요구사항(UR E27)을 배포하였다. 이 규정은 2024년 건조 계약을 체결한 신조선에 강제 적용될 예정이다. 본 논문에서는 신조선에 대한 리스크 기반 사이버 설계보안 접근 방식을 제안한다.

## I. 서 론

국제해사기구(IMO)는 2017년 해사안전위원회(Maritime Safety Committee, MSC)에서 안전관리시스템으로의 해상 사이버 리스크 관리(Resolution MSC.428(98))를 결의하였다. 각 기국은 2021년 1월 1일 이후 도래하는 첫 번째 회사의 안전관리적합증서(Document of Compliance)에 대한 심사를 수검하기 전까지 안전관리시스템(Safety Management System, SMS)에 사이버 리스크 관리를 적절하게 통합하고 구현된 것을 주관청이 확인하도록 권고하였다. 이에 미국, 독일, 마셜 아일랜드, 싱가포르, 그리스 등 22개국은 강제사항으로 적용중이며, 특히 미국 USCG의 경우 선박 사이버리스크 관리에 대한 업무지침(CVC-WI-027)을 배포하고 검사를 시행하고 있다. 개정으로 2018.1.1.부터 탱커선 (O/C, Oil, Shuttle, Gas)을 보유하고 있는 선사는 사이버보안 관리능력이 요구되며 사이버보안 정책서·절차서 이행, 리스크평가 수행, 임직원 인식제고 교육 등을 포함한 17개 항목을 점검하고 있다.

선주, 선박 운항사 및 관련 이해관계자를 대표하는 비영리 단체인 발트국제해사협의회(Baltic and International Maritime Council: BIMCO)는 2017년 해운업계가 선박 사이버 사고로 인해 발생할 수 있는 주요 안전, 환경 및 상업적 문제를 예방할 수 있도록 “선박 사이버보안 지침”을 발표하였으며 매년 개정판

을 배포하고 있다. 최신 버전(2020년)에서 사이버 위협관리 접근방식을 제안하고 있다.

IACS 는 2022년 4월, 신조선 사이버보안 통합 요구사항(UR E26)을 배포하였으며 리스크 평가 문서 제출을 요구하고 있다. 이러한 맥락에서 우리는 신조선에 적용 가능한 리스크 기반 사이버 설계보안 접근방식을 제안한다.

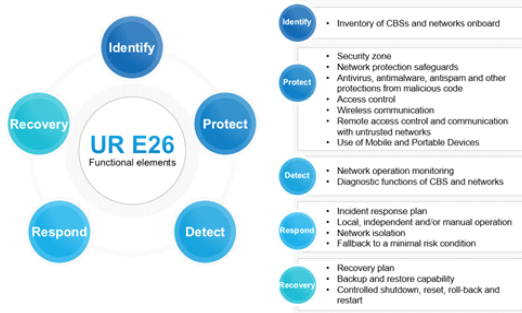
## II. 사이버보안 참조 표준

이 장에서는 본 논문에서 참조하는 표준인 IACS (International Association of Classification Societies) UR E26 및 IEC 62443 표준에 대해 설명한다.

### 2.1. IACS UR E26 : “Cyber resilience of ships”

통합요구사항(Unified Requirement: UR) E26은 선박 요구사항으로써 설계, 건조, 시운전 및 운영 등 선박 생애주기 전반에 걸쳐 OT 및 IT 시스템 사이버 복원성을 목표로 한다. 효과적인 사이버 리스크 관리를 위해 그림 1과 같이 5가지 기능요소와 세부 요구사항을 명시하며, 각 요구사항은 선박의 설계, 건조 및 운영에 관련된 이해 관계자의 책임 하에 선박에서 구현 및 검증되어야 한다.

\* 한국선급 (수석연구원, kaemyoung@krs.co.kr, 책임연구원, jklim@krs.co.kr)



(그림 1) 선박 사이버리스크 관리를 위한 요구사항

(표 1) 선박 사이버리스크 관리를 위한 5가지 기능요소

기능요소	요구사항
식별	선박 시스템, 사람, 자산, 데이터 및 기능 사이버 리스크를 관리하기 위한 조직적 이해를 개발
보호	사이버 사고로부터 선박을 보호하고 운송 연속성을 극대화하기 위한 적절한 보호장치 개발 및 구현
탐지	선상에서 사이버 사고의 발생을 탐지하고 식별하기 위한 적절한 조치를 개발하고 구현
대응	선내에서 탐지된 사이버 사고에 대해 조치를 취하기 위한 적절한 조치 및 활동을 개발 및 구현
복구	사이버 사고로 인해 손상된 운송에 필요한 모든 기능 또는 서비스를 복구하기 위한 적절한 조치 및 활동을 개발하고 구현

## 2.2. IACS UR E26 : “Cyber resilience of ships”

IEC 62443 표준은 OT 시스템의 현재 및 미래 취약성을 해결하고 체계적이고 방어 가능한 방식으로 필요한 완화를 적용하는 유연한 프레임워크를 제공한다[3]. 이 표준에서는 7가지 기본 요구 사항(Foundational Requirement: FR)을 시스템 요구사항(System Requirement: SR)으로 확장한다. 각 SR에는 보안을

(표 2) 기본 요구사항에 따른 시스템 SL 요구사항 수

기본요구사항	SL1	SL2	SL3	SL4
FR1. 식별 및 인증(IAC)	11	5	6	2
FR2. 사용제어(UC)	8	4	9	3
FR3. 시스템 무결성(SI)	6	4	6	3
FR4. 데이터 기밀성(DC)	2	2	1	1
FR5. 제한된 데이터 흐름(RDF)	4	2	4	1
FR6. 사고 적시 대응(TRE)	1	1	1	0
FR7. 자원 가용성(RA)	7	3	3	0

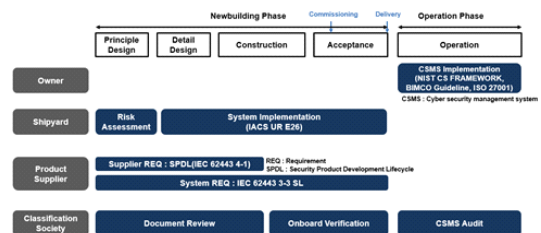
강화하기 위한 기본 요구사항 및 향상된 요구사항 (Requirement Enhancement: RE)으로 구성되어 있다. 7개의 FR에는 모두 4개의 SL(보안 수준)이 정의되어 있으며, 표 2는 각 시스템이 준수해야 하는 SL 요구사항의 수를 나타낸다.

## 2.3. IEC 62443 4-1 : “Security product development lifecycle requirements”

이 표준은 제품 공급자가 준수해야 하는 프로세스 요구 사항을 지정하고 안전한 제품을 개발하고 유지하기 위한 SDL(Secure Development Life-Cycle)을 정의한다[4]. 보안 관리(SM), 보안 업데이트 관리(SUM), 보안 요구사항 사양(SR), 보안 설계(SD), 보안 구현(SI), 보안 검증 및 검증 테스트(SVV), 보안 관련 문제 관리(DM), 보안 지침(SG) 등 8가지 범주가 포함된다.

## III. 표준리스크 기반 사이버 설계보안 접근 방식

선박 생애주기에 따른 각 이해 관계자의 사이버보안 활동사항은 그림 2와 같다. 신조선의 경우 조선소는 IACS UR E26 및 IEC 62443 3-3 표준을 준수해야 하며, 제품 공급자는 IEC 62443 3-3, 4-1 표준을 준수해야 한다. 선주는 선박 인도 후 IMO 결의안 MSC.428(98)에 따라 사이버보안 관리 시스템(Cyber Security Management System: CSMS)을 운영해야 한다. 선급협회는 검증자로서 모든 단계에 참여하여 문서검사, 현장검사, 현장심사를 수행한다. 이 논문에서는 신조선으로 다루는 범위를 한정한다.



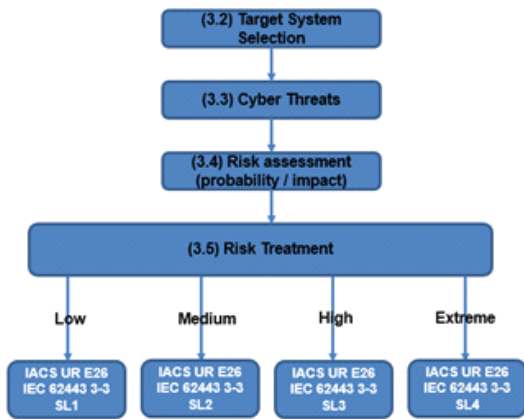
(그림 2) 각 이해관계자 사이버보안 활동사항

## 3.1. 방법론

여기서는 소단원을 작성할 때 내용을 설명하고자 한다.

통합요구사항(Unified Requirement: UR) E26은 선박 요구사항으로써 설계, 건조, 시운전 및 운영 등 선박 생애주기 전반에 걸쳐 OT 및 IT 시스템 사이버 복원성을 목표로 한다. 효과적인 사이버 리스크 관리를 위해 그림 1과 같이 5가지 기능요소와 세부 요구사항을 명시하며, 각 요구사항은 선박의 설계, 건조 및 운영에 관련된 이해 관계자의 책임 하에 선박에서 구현 및 검증되어야 한다.

사이버 리스크평가 전체 프로세스는 그림 3과 같다. 이 방법의 주요 목적은 적절한 요구사항을 적용하기 위해 각 시스템의 보안수준을 확인하는 것이다. 각 시스템은 리스크 수준에 따라 IACS UR E26, IEC 62443 SL 요구사항을 구현함으로써 사이버 설계보안을 달성할 수 있다.



(그림 3) 사이버리스크평가 방법론

### 3.2. 대상 시스템 선정

본 방법론은 선박에 설치된 IT 및 OT 시스템에 적용되며, 다음 조건을 만족하는 경우 사이버리스크 수준이 매우 낮다고 판단되므로 적용 대상 시스템에서 제외한다.

- i) 시스템에 다른 시스템에 대한 IP 기반 네트워크 연결이 없음
- ii) 시스템은 다른 시스템에 의한 사이버사고 영향을 받지 않음
- iii) 시스템은 제한 구역에 위치함
- iv) 시스템에는 USB(범용 직렬 버스)와 같은 물리적 인터페이스가 없음

### 3.3. 사이버 위협

본 논문에서 고려하는 사이버 위협은 다음과 같으나 이에 국한되지 않는다[5].

- i) 악의적 행위: 무차별 대입, 서비스 거부, 멀웨어, 사회 공학, 데이터 조작, 피싱, 스푸핑, APT (Advanced Persistent Threat), 중간자 공격 등
- ii) 물리적 공격: 사보타주, 무단 물리적 접근 등
- iii) 의도하지 않은 손상: IT 시스템의 데이터 탐지/변경, 제3자 보안 장애 등
- iv) 오작동 : 시스템의 장애 또는 오작동, 시스템의 취약점 등

### 3.4. 리스크 평가

사이버리스크는 위협(공격이 발생할 확률), 취약성(공격이 발생했을 때 공격이 성공할 확률), 영향(공격이 발생하고 성공했을 때 예상되는 영향의 정도)의 조합으로 정의한다. 각 시스템에 대해 사이버 위협과 관련된 사이버 공격 시나리오가 식별되면 다음 공식을 사용하여 사이리스크를 산정한다.

$$\text{사이버리스크(Cyber Risk)} = \text{가능성 요인(위협(Threat)} \times \text{취약성(Vulnerability)} \times \text{영향(Impact)}$$

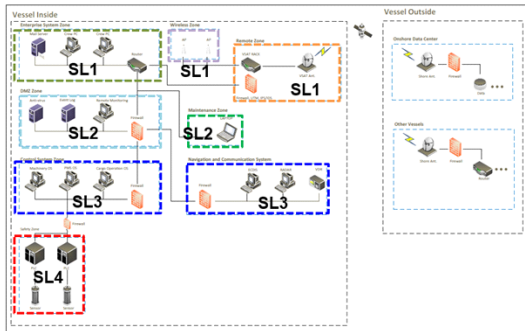
		1 Low	2 Low	3 Low	4 Medium	5 High	
Impact	5	1 Low	10 Medium	15 High	20 Extreme	25 Extreme	
	4	4 Low	8 Medium	12 High	16 High	20 Extreme	
	3	3 Low	6 Medium	9 Medium	12 High	15 High	
	2	2 Low	4 Low	6 Medium	8 Medium	12 High	
	1	1 Low	2 Low	3 Low	4 Low	5 Low	
		1	2	3	4	5	
		Probability (Threat, Vulnerability)					

(그림 4) 사이버리스크평가 매트릭스

### 3.5. 리스크 평가

시스템 사이버리스크가 산정되면 다음 기준에 따라 각 시스템의 SL을 결정한다. IACS UR E26 요구사항은 (3.2)에서 검증된 모든 대상 시스템에 적용한다.

- i)  $RL < 6$ : 낮은 리스크 수준, 시스템의 리스크 처리는 "IEC 62443 SL1"으로 간주함
- ii)  $6 \leq RL \leq 10$ : 중간 리스크 수준, 시스템의 리스크 처리는 "IEC 62443 SL2"로 간주함
- iii)  $11 \leq RL \leq 19$ : 높은 리스크 수준, 시스템의 리스크 처리는 "IEC 62443 SL3"으로 간주함



(그림 5) 제안 방법론을 적용한 선박 시스템 보안 수준

- iv)  $RL \geq 20$  : 극도의 리스크 수준, 시스템의 리스크 처리는 "IEC 62443 SL4"로 간주함

#### IV. 결 론

현존선의 경우 선박 네트워크 구성 변경 및 사이버 보안 기능 구현이 매우 어렵다. 따라서 신조선 건조단계에서부터 선박 네트워크 구성을 고려한 설계보안이 필요하다. 본 논문에서는 IACS UR E26 및 IEC 62443 표준 요구 사항을 기반으로 신조선의 사이버 복원력을 달성하기 위해 리스크 기반 사이버 설계보안 접근방식을 제안하였다.

#### 참 고 문 헌

- [1] DNV, "A proposed approach applied to modern cruise ship newbuilding", August, 2018
- [2] IACS, "UR E26 : Cyber resilience of ships", April.2022
- [3] IEC, "IEC 62443 3-3, Industrial communication networks - Network and system security Part 3-3: System security requirements and security levels", 2013
- [4] IEC, "IEC 62443 4-1, Security for industrial automation and control systems - Part 4-1: Secure product development lifecycle requirements", 2018
- [5] IACS, "Rec.171 : Recommendation on incorporating cyber risk management into Safety Management Systems", June.2022

#### <저자 소개>



##### 박 개 명 (Park Kaemyoung)

1996년 8월: 카이스트 전산공학과 졸업  
 2001년 5월~2008년 7월: (주)대한항공 항공기술연구원  
 2009년 1월~현재: 한국선급 <관심분야> 정보보호, 사이버 인텔리전스, 선박/해양플랜트 CPS 보안



##### 임 정 규 (Lim JeoungKyu)

2009년 2월: 경북대학교 전기컴퓨터공학부 졸업  
 2011년 2월: 서울대학교 전기공학부 졸업  
 2011년 1월~2017년 8월: (주)HD현대중공업  
 2017년 9월~현재: 한국선급 <관심분야> 정보보호, 사이버 리스크 평가, 사이버 인텔리전스, 선박/해양플랜트 CPS 보안