선박 및 시스템의 사이버복원력 지침

(개발검토 : 외부의견조회용)

2024. 2.

기 관 규 칙 개 발 팀

2024

선박 및 시스템의 사이버복원력 지침

한 국 선 급

2024

선박 및 시스템의 사이버복원력 지침

GC-43-K

한 국 선 급

“선박 및 시스템의 사이버복원력 지침”의 적용

1. 이 지침은 별도로 명시하는 것을 제외하고 2024년 7월 1일 이후 건조계약 되는 선박 및 선내 시스템에 적용한다.

차 례

제 1 장 일반사항

제 1 절 일반사항

101. 목표와 목적

1. 이 지침은 사이버 복원력을 갖춘 선박에 관한 기술적 수단을 제공할 목적으로 이해관계자에게 선박의 사이버 복원력에 대한 최소 요구사항을 제공하기 위한 것이다.
2. 이 지침은 사이버 복원력에 대한 집합체로서 선박을 목표로 하며, 선내 시스템, 장비 및 구성요소의 사이버 복원력을 다루는 산업 표준과 상호보완적 적용을 위한 기반으로 의도된다.
3. 선내 시스템 및 장비의 사이버 복원력에 대한 최소 요구사항은 **3장**에 기술되어 있다.

102. 적용

1. 이 지침의 요건은 **선급 및 강선규칙 1편**에 따라 우리 선급에 등록하고 유지하는 선박에 적용한다.
2. 이 지침 **2장**의 사이버복원력에 대한 최소 요건은 제조중 등록검사를 받는 선박에 적용한다.
3. 이 지침 **3장**은 사이버복원력에 대한 최소 요건은 2장을 적용하는 선박의 선내 시스템 및 장비에 적용한다.
4. 이 지침 **4장**의 추가 요건은 선주의 요청 시 선박의 사이버보안관리체계에 대하여 추가로 적용한다.
5. 이 지침의 요건에 추가하여 **선급 및 강선규칙 6편 2장**의 관련 규정 요건도 만족해야 한다.
6. 이 지침에서 고려되는 사이버 사고는 적용 범위에 있는 선내 운영 기술(OT) 시스템을 대상으로 하는 모든 공격 행위로 인해 발생하는 사건을 의미한다.
7. 이 지침에서 별도로 규정하고 있지 않은 사항에 대해서는 **선급 및 강선규칙**의 관련 규정을 따른다.

103. 적용 범위

1. 적용 선박

(1) 국제항해에 종사하는 여객선 (고속여객선 포함)
(2) 국제항해에 종사하는 500GT 이상의 화물선
(3) 국제항해에 종사하는 500GT 이상의 고속선
(4) 500GT 이상의 이동식 해양 시추선
(5) 건설에 종사하는 자체 추진 이동식 해양 구조물(예: 풍력 터빈 설치, 유지 보수 및 수리, 크레인 유닛, 시추부속선(tender), 숙박 시설 등)

(비고) 이 지침은 다음의 선박에 대하여 비강제적인 지침으로 사용할 수 있다.

1) 군함, 군수송선 및 함정
2) 총톤수 500톤 미만의 화물선
3) 기계적 수단으로 추진되지 않는 선박
4) 원시적 구조의 목선
5) 여객용 요트(12인 이하 승객)
6) 무역에 종사하지 않는 유람선
7) 어선
8) 고정식(Site specific) 해양 구조물(예: FPSO, FSU 등)

2. 적용 시스템

(1) 선박 내 운영 기술(OT) 시스템, 즉 물리적 프로세스를 제어 또는 감시하기 위해 사이버 공격에 취약할 수 있는 데이터를 사용하고, 만약 손상될 경우, 인명의 안전, 선박의 안전 및/또는 환경 위협에 대한 위험한 상황을 초래할 수 있는 검퓨터기반시스템(이하: CBS)

특히, 다음의 선박 기능 및 시스템의 작동에 이용되는 CBS가 본선에 있는 경우 고려되어야 한다.

(가) 추진
(나) 조타
(다) 앵커링 및 무어링

(라) 발전 및 배전
(마) 화재 탐지 및 소화 시스템
(바) 빌지 및 평형수 시스템, 로딩 컴퓨터
(사) 수밀 무결성 및 침수 탐지
(아) 조명 (예: 비상 조명, 저위치 조명, 항해등 등)
(자) 중단 또는 기능 손상이 선박 운항에 위험을 초래할 수 있는 어떠한 규정상 요구되는 안전 시스템
(예: 비상정지 시스템, 화물 안전 시스템, 압력 선박 안전시스템, 가스 탐지 시스템 등)

(2) 항해 및 통신 시스템
(가) 협약 규정에서 요구되는 항해시스템
(나) 선급 규칙 및 협약 규정에서 요구되는 내부 및 외부 통신 시스템

(3) 지침의 적용 범위에 속하는 CBS로부터 다른 시스템으로의 IP 기반 통신 인터페이스.
(비고) 상기 다른 시스템의 예는 다음과 같으며 이에 국한되지 않는다.
1) 여객 또는 방문객 서비스 및 관리 시스템
2) 여객 대상 네트워크
3) 관리 네트워크
4) 선원 복지 시스템
5) 영구 또는 일시적으로(예: 유지보수 중) OT 시스템에 연결되는 다른 기타의 시스템

3. 시스템의 적용 제외

CBS가 **3절**에 따라 위험도 평가를 수행하고, 우리 선급으로부터 **304.**의 허용 기준을 만족하는 것으로 확인되는 경우 이 지침의 적용 범위에서 제외할 수 있다.

104. 선급부호

이 지침의 요건에 적합한 선박은 다음의 선급부호를 부여할 수 있다.

1. **Cyber Resilience**: 이 지침 **2장**의 관련 요건에 따라 선박의 수명주기 동안 사이버복원력을 가진 선박
2. **Cyber Resilience(Managed)**: 이 지침 **2장**의 요건에 추가하여 **4장**의 추가 요건에 따라 선박의 운항 단계에서 사이버위험관리 프로세스 기반의 사이버보안관리시스템을 이행하는 선박

105. 시스템 카테고리

시스템 카테고리는 인명의 안전, 선박의 안전 및/또는 환경 위협에 대한 시스템 고장의 영향을 기반으로 **선급 및 강선 규칙 6편 2장 4절**에 정의되어 있다.

106. 동등 효력

항해 및 무선통신 시스템에 대해서는 **2장**의 관련 요건을 만족하는 조건으로 **3장 4절**에서 요구되는 보안 기능들을 대신하여 IEC 61162-460 또는 다른 동등한 표준의 적용이 우리 선급에 허용될 수 있다.

107. 참조 문서

검퓨터기반시스템 및 사이버복원력에 대하여 다음의 IACS 문서 및 국제표준을 추가로 참조한다.

1. **IACS UR E22 Rev.3**: 컴퓨터기반시스템
2. **IACS UR E26 Rev.1**: 선박의 사이버복원력
3. **IACS UR E27 Rev.1**: 선내 시스템 및 장비의 사이버복원력
4. **IACS Rec.166**: 사이버복원력에 대한 권고사항
5. **IEC 62443-3-3 (2013)**: 산업 통신 네트워크 - 네트워크 및 시스템 보안 Part 3-3: 시스템 보안 요구사항 및 보안 수준
6. **IEC 62443-4-1 (2018)**: 산업 자동화 및 제어 시스템 보안 Part 4-1: 보안 제품 개발 수명주기 요구사항

제 2 절 정의

201. 용어 정의

1. **연차검사**: **선급 및 강선규칙 1편 2장 2절** 참조
2. **공격 표면(attack surface)**: 권한이 없는 사용자가 시스템에 접근하여 영향을 미치거나 데이터를 추출할 수 있는 모든 가능한 지점의 집합. 공격 표면은 디지털 및 물리적 두 가지 범주로 구성된다. 디지털 공격 표면은 조직의 네트워크에 연결하는 모든 하드웨어와 소프트웨어를 포함한다. 여기에는 애플리케이션, 코드, 포트, 서버 및 웹사이트를 포함한다. 물리적 공격 표면은 공격자가 물리적으로 접근할 수 있는 모든 종단 장치(예: 데스크톱 컴퓨터, 하드 드라이브, 노트북, 휴대폰, 이동식 드라이브 및 부주의하게 폐기된 하드웨어)로 구성된다.
3. **인증(authentication)**: 주장된 신원의 특성이 올바르다는 보증을 제공한다.
4. **가용성(availability)**: 시스템 정보 및 기능에 대한 적시의 신뢰성 있는 접근 및 사용을 보장하는 속성을 말한다.
5. **보상 대책(compensating countermeasure)**: 하나 이상의 보안 요구사항을 충족하기 위해 고유 보안 기능을 대신하거나 추가로 적용된 추가하여 도입된 대책을 말한다.
6. **컴퓨터기반시스템(CBS: Computer Based System)**: 정보의 수집, 처리, 유지, 사용, 공유, 보급 또는 처리와 같은 하나 이상의 특정 목적을 달성하기 위해 구성된 프로그래밍 가능한 전자 장치 또는 상호 운용 가능한 프로그래밍 가능한 전자 장치의 집합. 선내 CBS에는 IT 및 OT 시스템을 포함한다. 선내 CBS는 네트워크를 통해 연결된 하부 시스템의 조합일 수 있다. 선내 CBS는 직접 또는 공용 통신 수단(예: 인터넷)을 통해 육상의 CBS, 다른 선박의 CBS 및/또는 기타 설비에 연결될 수 있다.
7. **전송로(conduit)**: 공통 보안 요구사항을 공유하는 두 개 이상의 구역을 연결하는 통신 채널의 논리적 그룹화를 말한다.
8. **컴퓨터 네트워크(computer network)**: 합의된 통신 프로토콜 수단으로 전자적으로 데이터를 통신하기 위한 목적을 위한 두 대 이상의 컴퓨터 간의 연결을 말한다.
9. **기밀성(confidentiality)**: 정보 접근 및 공개에 대한 공인된 제한을 보존하는 속성을 말한다.
10. **통제(control)**: 정책, 절차, 지침, 실무서(practice) 또는 조직도를 포함하여 위험을 관리하는 수단으로서 행정, 기술적, 관리, 또는 법적 성격을 가질 수 있다.
11. **사이버 사고(cyber incident)**: 의도적 또는 비의도적으로 하나 이상의 선내 CBS를 대상으로 하거나 영향을 미치는 공격으로 인해 발생하며, 실제로 또는 잠재적으로 선내 시스템, 네트워크 및 컴퓨터 또는 이들이 처리, 저장 또는 전송하는 정보에 부정적인 영향을 초래할 수 있으며, 영향를 완화하기 위해 대응 조치가 필요할 수 있는 사건. 사이버 사고에는 선내 CBS에서 생성, 보관 또는 사용되거나 이러한 시스템들을 연결하는 네트워크에서 전송되는 정보의 무단 접근, 오용, 변경, 파괴 또는 부적절한 공개를 포함한다. 사이버 사고에는 시스템 고장을 포함하지 않는다.
12. **사이버복원력(cyber resilience)**: 잠재적으로 인명의 안전, 선박의 안전 및/또는 환경 위협에 대하여 위험한 상황으로 이어질 수 있으며, 선박의 안전한 운항을 위해 이용되는 운영 기술(OT)의 중단 또는 손상으로 인해 발생하는 사이버 사고의 발생을 줄이고 영향을 완화하는 능력을 말한다.
13. **심층 방어(Defence in Depth)**: 조직의 여러 계층과 임무에 걸쳐 다양한 장벽을 세우기 위한 사람, 기술 및 운영 능력을 통합하는 정보 보안 전략을 말한다.
14. **중요용도(essential System)**: 선박의 추진, 조타 및 안전에 필수적인 서비스 제공에 기여하는 검퓨터기반시스템. 필수 서비스는 “일차 중요용도” 및 “이차 중요용도”로 구성된다. 일차 중요용도는 추진 및 조타를 유지하기 위해 연속적으로 운영이 필요한 용도이다. 이차 중요용도는 추진 및 조타를 유지하기 위해 반드시 연속적으로 운영될 필요는 없지만, 선박의 안전을 유지하기 위해 필요한 용도이다.
15. **방화벽(firewall)**: 사전 정의된 규칙을 통해 통제되는 들어오고 나가는 네트워크 트래픽을 감시하고 제어하는 논리적 또는 물리적 장벽을 말한다.
16. **펌웨어(firmware)**: 엔지니어링 제품 및 시스템의 제어, 감시 및 데이터 처리를 제공하는 전자 장치에 내장된 소프트웨어. 이러한 기능은 일반적으로 자체에 내장되어 있어 사용자 조작에 접근할 수 없다.
17. **하드닝(hardening)**: 강화는 공격 표면을 줄임으로써 시스템의 취약성을 줄이는 관행이다.
18. **정보기술(IT: Information Technology)**: 운영 기술(OT)과 반대로 데이터를 정보로 사용하는 데 중점을 둔 장치, 소프트웨어 및 관련 네트워크를 말한다.
19. **통합 시스템(integrated system)**: 하나 이상의 지정된 목적을 달성하기 위해 구성된 다수의 상호 작용하는 부시스템 및/또는 장비를 결합하는 시스템을 말한다.
20. **무결성(integrity)**: 자산의 정확성과 완전성을 보호하는 속성을 말한다.

21. **논리적 네트워크 세그먼트(logical network segment)**: “네트워크 세그먼트”와 동일하나 둘 이상의 논리적 네트워크 세그먼트가 동일한 물리적 구성요소를 공유한다.
22. **네트워크(network)**: 합의된 통신 프로토콜의 수단에 의해 데이터를 전자적으로 통신할 목적을 위한 둘 또는 이상의 컴퓨터들 사이의 연결을 말한다.
23. **네트워크 세그먼트(network segment)**: 이 지침의 관점에서, 네트워크 세그먼트는 OSI 2계층 이더넷 세그먼트(방송 도메인)이다.
    (비고) TCP/IP : 네트워크 주소 계획에는 해당 IP 주소와 네트워크 마스크가 헤더에 붙는다. 네트워크 세그먼트 간의 통신은 네트워크 계층(OSI 3계층)에서 라우팅 서비스를 사용해야만 가능하다.
24. **네트워크 스위치(switch)**: 데이터를 수신, 처리 및 목적지 장치로 전송하기 위해 패킷 교환을 사용하여 컴퓨터 네트워크상에서 장치들을 서로 연결하는 장치를 말한다.
25. **공격적 사이버 행동(offensive cyber manoeuvre)**: OT 또는 IT 시스템의 거부, 성능 저하, 중단, 파괴 또는 조작을 초래하는 행동을 말한다.
26. **운영 기술(OT: Operational Technology)**: 선내 시스템을 감시 및 제어하는 장치, 센서, 소프트웨어 및 관련 네트워킹. 운영 기술 시스템은 물리적 프로세스를 제어하거나 감시하기 위한 데이터 사용에 중점을 둔 것으로 생각될 수 있다.
27. **운영 시스템(OT system)**: 제어, 경보, 감시, 안전 또는 내부 통신 기능을 제공하는 컴퓨터기반시스템을 말한다.
28. **패치(patches)**: 보안 취약성 및 기타 버그를 해결하거나 운영 체제 또는 응용 프로그램을 개선하기 위해 설치된 소프트웨어 또는 지원 데이터를 업데이트하도록 설계된 소프트웨어를 말한다.
29. **물리적 네트워크 세그먼트(physical network segment)**: "네트워크 세그먼트"와 동일하나, 물리적 구성요소는 다른 네트워크 세그먼트와 공유하지 않는다.
30. **프로토콜(protocol)**: 네트워크상 컴퓨터가 통신하는 데 사용하는 공통 규칙 및 신호 집합. 프로토콜은 데이터 통신, 네트워크 관리 및 보안을 수행하는 것을 허용한다. 선내 네트워크는 일반적으로 TCP/IP 스택 또는 다양한 필드버스를 기반으로 하는 프로토콜을 구현한다.
31. **복구(recovery)**: 복원력 계획을 유지하고 사이버보안 이벤트로 인해 손상된 기능이나 서비스를 복원하기 위한 적절한 활동을 개발 및 구현한다. 복구 기능은 사이버보안 이벤트의 영향을 줄이기 위해 적시에 정상 작동으로 복귀하도록 지원한다.
32. **보안구역(security zone)**: 지침의 적용 범위에 있는 동일한 접근 통제 정책이 필요한 CBS의 모음. 각 구역은 접근 통제 정책이 적용되는 단일 인터페이스 또는 인터페이스 그룹으로 구성한다.
33. **선주/회사(shipowner/company)**: 선주 또는 선주로부터 선박 운항에 대한 책임을 지고 모든 부수적 의무와 책임을 인수하기로 동의한 관리자, 대리인(agent) 또는 나용선 용선자(bareboat charterer)와 같은 어떤 다른 기관 또는 개인. 초기 건조 중에 선주는 조선소 또는 시스템 통합자일 수 있다. 선박 인도 후, 선주는 선박 관리회사에 일부 책임을 위임할 수 있다.
34. **정기검사(Special Survey)**: **선급 및 강선규칙 1편 2장 4절** 참조
35. **공급자(supplier)**: 시스템 또는 부시스템과 함께 작동하며 응용 프로그램, 임베디드 장치, 네트워크 장치, 호스트 장치를 구성하는 하드웨어 및/또는 소프트웨어 제품, 시스템 구성품 또는 장비(하드웨어 또는 소프트웨어)의 제조사 또는 제공업체. 공급자는 프로그램 가능 장치, 부시스템 또는 시스템을 시스템 통합자에게 제공할 책임이 있다.
36. **시스템(system)**: 하나 이상의 특정 목적을 달성하기 위해 조직된 상호작용하는 프로그램 가능한 장치 및/또는 부시스템들의 조합을 말한다.
37. **시스템 카테고리 (I, II, III)**: **선급 및 강선규칙 6편 2장 4절**에서 정의된 시스템 기능의 영향성에 기반한 시스템 카테고리를 말한다.
34. **시스템 통합자(system integrator)**: 공급자가 제공한 시스템 및 제품을 선박 사양서의 요구사항에 따라 적용된 시스템에 통합하고 통합 시스템을 제공할 책임이 있는 특정 개인 또는 조직. 시스템 통합자는 선박 내 시스템 통합의 책임을 담당할 수도 있다. 선박 인도 시까지, 이 역할은 대체 조직이 책임을 특별히 계약되어 할당되지 않는 한 조선소에서 수행해야 한다.
35. **비신뢰 네트워크(untrusted network)**: 지침의 적용 범위 밖에 있는 어떠한 네트워크를 말한다.

202. 약어

1. **AS**: Annual Survey
2. **ACL** : Access Control List

3. CBS: Computer Based System
4. COTS: Commercial-Off-The-Shelf
5. DoS: Denial of Service
6. HMI : Human-Machine Interface
7. IDS : Intrusion Detection System
8. IPS : Intrusion Prevention System
9. IT: Information Technology
10. MoC: Management of Change
11. OT: Operational Technology
12. TCP/IP: Transmission Control Protocol/Internet Protocol
13. SDLC: Secure Development Life-Cycle
14. SS: Special Survey

제 3 절 CBS의 적용 제외를 위한 위험도 평가

301. 요구사항

1. 이 지침의 적용 범위에 속하는 CBS가 관련 요구사항의 적용에서 제외하는 경우 위험도 평가를 수행해야 한다. 위험도 평가는 제외된 CBS와 관련된 허용 가능한 위험 수준의 증거자료를 제공해야 한다.

302. 근거

1. 관련 요구사항의 적용에서 이 지침의 적용 범위에 속하는 CBS를 제외하는 것은 적절한 절차에 따라 정당화하고, 문서화 해야 한다. 이러한 제외는 CBS 운영과 관련된 위험 수준이 특정 위험 평가 수단에 의해 허용이 가능한 한계점 미만이라는 증거자료가 제공된 경우에만 우리 선급에서 허용할 수 있다.
2. 위험도 평가는 CBS 카테고리, 선박과 CBS의 연결성과 기능 요구사항 및 사양을 고려하여 유사한 설계에 대한 이용 가능한 지식 및 경험을 바탕으로 해야 한다. 내부 및 외부 소스의 사이버 위협 정보는 사이버보안 사건의 가능성과 영향을 보다 더 잘 이해하는 데 활용될 수 있다.

303. 세부 요구사항

1. 위험도 평가서는 최초 설계의 변경 가능성과 처음부터 알려지지 않은 새롭게 발견된 위협 및/또는 취약점을 고려하여 설계 및 건조 단계 시 시스템 통합자에 의해 작성되고 최신 상태로 유지되어야 한다.
2. 선주는 선박의 운항 수명 동안 지속적인 개선 프로세스로서, 사이버 시나리오의 지속적인 변화와 선내 CBS에서 식별된 새로운 약점을 고려하여 위험도 평가서를 업데이트해야 한다. 새로운 위험이 식별될 경우, 선주는 기존 위험도 평가서를 업데이트하고, 새로운 위험 완화 조치를 구현해야 한다.
3. 사이버 시나리오의 변경이 검토 중인 CBS와 관련된 위험 수준을 허용이 가능한 위험 한계점 이상으로 높아지게 하는 경우, 우리 선급에 알리고 평가를 위해 업데이트된 위험도 평가서를 제출해야 한다.
4. 검토 중인 CBS에 대한 예상되는 운영 환경은 CBS의 카테고리를 고려하여 사이버 사고의 가능성과 인명의 안전, 선박 또는 해양 환경의 안전에 미칠 수 있는 영향을 식별하기 위해 위험도 평가에서 분석되어야 한다. 공격 표면은 CBS의 연결성, 휴대장치용 인터페이스, 논리적 접근 제한 등을 고려하여 분석되어야 한다.
5. 검토 중인 CBS의 특정 설정과 관련된 새로운 위험 또한 식별되어야 한다. 위험도 평가에서 다음 요소들을 고려해야 한다.
   (1) 자산 취약점
   (2) 내부 및 외부의 위협
   (3) 인명 안전, 선박 안전 및/또는 환경 위협 상 자산에 영향을 주는 사이버 사고의 잠재적 영향
   (4) 선내에 없는 시스템을 포함하여(예: 선내 시스템에 대한 원격 접근이 제공되는 경우) 시스템의 통합 또는 시스템 간의 인터페이스와 관련된 가능한 영향

304. 허용 기준

1. 지침의 적용 범위에 해당하는 CBS를 관련 요구사항의 적용으로부터 제외하는 것은 CBS의 운영이 사이버 위험에 대한 운항의 안전에 아무런 영향을 주지 않는다고 보장되는 경우에만 우리 선급에서 허용할 수 있다.
2. 언급된 제외는 아래 나열된 추가 기준을 완전히 만족하지 않는 CBS에 대해서도 허용될 수 있으나, 증거자료와 함께 합리적인 설명이 제공되어 우리 선급에 만족스러운지 확인되어야 한다. 우리 선급은 언급된 제외를 고려하기 위해 추가적인 문서들의 제출을 요구할 수 있다.
3. 본 지침의 적용 범위에서 제외하기 위해서는 다음의 기준들을 만족해야 한다.
   (1) CBS가 격리되어야 한다. (즉, 다른 시스템 또는 네트워크에 어떠한 IP-네트워크 연결이 없어야 함)
   (2) CBS는 접근이 가능한 물리적 인터페이스 포트를 가지지 않아야 한다. 미사용 인터페이스는 논리적으로 비활성 되어야 하고, 무허가 장치는 CBS에 연결할 수 없어야 한다.
   (3) CBS는 물리적 접근이 통제되는 구역 내에 위치해야 한다.
   (4) CBS는 지침의 적용 범위(103. 참조) 내 명시된 다중의 선박 기능을 제공하는 통합 제어 시스템이 아니어야 한다.
4. 다음의 추가 기준은 위험도 수준 허용 가능성의 평가를 위해 고려해야 한다.
   (1) CBS는 카테고리 III의 선박 기능을 제공하지 않아야 한다.
   (2) CBS에 영향을 주는 알려진 취약점, 위협, 사이버 사고로 파생하는 잠재적 영향이 위험도 평가에서 적절하게 고려

해야 한다.

(3) CBS에 대한 공격 표면은 무선 접근 지점을 포함하여 복잡성, 연결성, 물리적 및 논리적 접근 지점을 고려하여 최소화해야 한다. ⚓

제 2 장 선박의 사이버복원력

제 1 절 일반사항

101. 도입

1. 상용 기성품(COTS)의 선내 광범위한 사용과 함께 선박의 컴퓨터 시스템들의 상호 연결은 선원 데이터, 인명 안전, 선박 안전에 영향을 미치고 해양 환경을 위협하는 공격 가능성을 야기 할수 있다.
2. 공격자는 선내 시스템과 외부 세계 간의 네트워크 연결 또는 어떤 다른 인터페이스가 있는 곳 어디에서나 그들의 목표를 달성하기 위해 사람과 기술의 어떤 조합을 표적으로 삼을 수 있다. 현재 및 새로운 위협으로부터 선박과 일반적인 해운을 보호하기 위해서는 지속적으로 발전하는 다양한 조치들이 필요하다.
3. 실질적인 사이버복원력이 있다고 설명할 수 있는 선박을 인도하기 위해 공통의 최소 기능 및 성능 기준들을 수립해야 한다.
4. 사이버복원력을 가진 선박을 건조하고 운항하기 위해서는 목표 기반 접근 방식을 이용하여 전체 위협 표면에 일관되게 적용되는 최소 요구사항이 필요하다.

102. 적용

1. 이 장의 요건은 **1장 103.**의 1항에 따른 적용 대상 선박에 대하여 선박의 전체 수명주기 동안 적용한다.
2. 이 장의 적용 범위에 포함되는 선내 시스템 및 장비는 이 장에 추가하여 **3장**의 최소 요건을 만족해야 한다.
3. 별도로 명시하는 경우를 제외하고 이 장에서 언급되는 CBS와 네트워크는 **1장 103.**의 2항에 따른 지침의 적용 범위에 포함되는 CBS 및 네트워크를 의미한다.

제 2 절 선박 검사

201. 일반

선급 검사는 이 절에서 명시된 관련 단계에서 우리 선급의 문서 평가 및 검사를 통해 실시해야 한다.

1. 제출문서 및 자료

(1) 공급자가 제출하는 문서는 **3장**에 명시되어 있다. 이 문서의 승인 버전은 **3장 202.**의 3항에 명시된 바와 같이 공급자가 시스템 통합자에게 제공해야 한다. (**표 3.2.1** 참조)

(2) 시스템 통합자가 제출해야 하는 문서 목록은 **202.**의 1항 및 **202.**의 **2항**에 나열되어 있다. (**표 2.2.1** 참조)

(3) 선주가 제출해야 하는 문서 목록 **203.**의 1항에 나열되어 있다. (**표 2.2.1** 참조)

2. 선주 제공문서 및 자료

선박의 인도 시 시스템 통합자는 선주에게 다음 문서를 제공해야 한다.

(1) 공급자가 제공하는 승인 버전의 CBS 문서 (**3장 202.** 참조)

(2) 시스템 통합자가 생산한 문서 (**202.**의 1항, **202.**의 **2**항 및 **표 2.2.1** 참조)

표 2.2.1 문서 및 조치 요약

문서명	항목	시스템 통합자			선주			
		설계	건조	선내시험	운항	1st AS	AS	SS
승인된 공급자 문서	3장 201.		유지보수	유지보수	유지보수			
구역 및 전송로 다이어그램	202.의 1항 (1)호 (가)	승인	유지보수	유지보수	유지보수			
사이버보안 설계 기술서(CSDD)	202.의 1항 (1)호 (나)	승인	유지보수	유지보수	유지보수			
선박 자산 목록	202.의 1항 (1)호 (다)	승인	유지보수	유지보수	유지보수			
CBS 적용 제외 위험도 평가서 (1)	202.의 1항 (1)호 (라)	승인	유지보수	유지보수	유지보수			
보상 대책 기술서 (1)	202.의 1항 (1)호 (마)	승인	유지보수	유지보수	유지보수			
선박 시험절차서	202.의 2항 (2)호		승인	검사	유지보수			검사
선박 사이버보안 및 복원력 프로그램 - 변경 관리 (MoC) [401.의 1항 (5)호] - 소프트웨어 업데이트 관리 [401.의 1항 (5)호] - 방화벽 관리 [402.의 1항 (5)호] - 멀웨어 보호 관리 [402.의 3항 (5)호] - 접근 통제 관리 [402.의 4항 (5)호] - 기밀 정보 관리 [402.의 4항 (5)호] - 원격 접근 관리 [402.의 6항 (5)호] - 모바일 및 휴대용 장치 관리 [402.의 7항 (5)호] - 보안 이상징후 탐지 [403.의 1항 (5)호] - 보안 기능의 검증 [403.의 2항 (5)호] - 사고 대응 계획 [404.의 1항 (5)호] - 복구 계획 [405.의 1항 (5)호]	203.의 2항 (1)호				유지보수	승인 & 검사	검사	

1. (1) 적용되는 경우
2. **승인**: 이해관계자는 이 장의 요구사항을 준수의 검증 및 승인을 위해 우리 선급에 문서를 제출해야 함
3. **유지보수**: 이해관계자는 변경관리(MoC) 절차서에 따라 문서를 업데이트해야 한다. 업데이트된 문서 및 변경관리 기록은 **선급 및 강선규칙 6편 2장 4절**에 따라 우리 선급에 제공되어야 한다.
4. **검사**: 이해관계자는 승인된 문서에 따라 준수하고 있음을 우리 선급의 검사 시 입증해야 한다.

4. 선박 검사의 종류

선박 사이버복원력에 대한 검사의 종류는 다음과 같다.

(1) 제조중 등록을 위한 검사(이하, 등록검사)

등록검사는 제조중 등록 신청이 있을 경우 실시하며, 다음의 단계에서 문서 승인 및 검사를 포함한다.

(가) 설계 단계

(나) 건조 단계

(다) 선내시험 단계

(2) 등록을 유지하기 위한 검사(이하, 유지검사)

유지검사는 선박의 인도 후에 등록 유지를 위해 실시하며, 다음의 검사들을 포함한다.

(가) 연차검사(AS)

(a) 1번째 연차검사

1번째 연차검사는 **선급 및 강선규칙 1편 2장 2절**에서 규정하는 1번째 연차검사 시기에 실시한다.

(b) 후속 연차검사

후속 연차검사는 **선급 및 강선규칙 1편 2장 2절**에서 규정하는 2번째 연차검사부터 4번째 연차검사 시기에 실시한다.

(나) 정기검사(SS)

정기검사는 **선급 및 강선규칙 1편 2장 4절**에서 규정하는 시기에 시행한다.

(다) 임시검사(OS)

임시검사는 **선급 및 강선규칙 1편 2장 10절**에서 규정하는 시기에 시행한다.

202. 등록검사

1. 설계 및 건조 단계

(1) 승인문서 및 자료

(가) 구역 및 전송로 다이어그램(Zone and Conduit Diagram)

이 문서의 내용은 **402.**의 **1**항 (4)호 (가)에 명시되어 있다.

(나) 사이버보안 설계 기술서(CSDD: Cyber Security Design Description)

이 문서의 내용은 **4절**의 각 하부의 "설계 단계"에 명시되어 있다.

(다) 선박 자산 목록(Vessel Asset Inventory)

이 문서의 내용은 **401.**의 **1**항에 명시되어 있다.

(라) CBS 제외를 위한 위험도 평가

이 문서의 내용은 **1장 3절**에 명시되어 있다.

(마) 보상 대책의 기술

어떠한 CBS가 **3장**의 요구사항을 대신하여 보상 대책으로 승인된 경우, 이 문서는 해당 CBS와 부족한 보안 기능을 명시하고, 보상 대책에 대한 상세한 기술을 제공해야 한다. 공급자가 시스템 문서 내에 이러한 보상 대책을 기술하도록 요구하는 3장 **301.**의 **3**항을 참조한다.

(2) 공급자는 **3장 2절**에 명시된 인증 프로세스에 따라 우리 선급에 규정 준수를 입증해야 한다.

(3) 시스템 통합자는 평가를 위해 상기 (1)호의 승인용 문서들을 우리 선급에 제출하여 규정 준수를 입증해야 한다.

(4) 설계 및 건조 단계에서 설계 변경은 **선급 및 강선규칙 6편 2장 4절**의 변경 관리(MoC) 요구사항에 따라 실시되어야 한다.

2. 선내시험 단계

(1) 선박의 최종 선내시험 전에 시스템 통합자는 다음을 이행해야 한다.

(가) 업데이트된 설계 문서(**202.**의 **1**항 (1)호의 최신 버전을 우리 선급에 제출해야 한다.

(나) 시험 및/또는 분석적 평가를 통해 이 장의 규정 준수를 입증하는 방법을 기술하는 선박 사이버복원력 시험절차서를 우리 선급에 승인용으로 제출해야 한다.

(다) 우리 선급의 입회 하에 승인된 선박 사이버복원력 시험절차서에 따라 시험을 실시해야 한다.

(2) 선박 사이버복원력 시험절차서

(가) 이 문서의 내용은 이 장 **4절**의 각 하부 절 "선내시험 단계"에 명시되어 있다.

(나) CBS의 선내시험

(a) 각 CBS에 대하여 요구되는 고유의 보안 기능과 설정은 각 CBS의 인증 과정에서 시험하고 검증해야 한다. (**3장** 참조).

(b) 이러한 보안 기능에 대한 시험은 각 "선내시험 단계"에 명시되어 있는 경우, 이러한 보안 기능이 **3장**에 따른 CBS의 인증 과정 중에 성공적으로 시험이 실시되는 것을 조건으로 생략할 수 있다.

(c) 그럼에도 불구하고, 모든 시험은 선박 사이버복원력 시험절차서에 포함되어야 하며, 시험을 생략하는 결정은 우리 선급만이 할 수 있다.

(d) 인증 과정에서 선내시험 단계로 전달된 발견사항 또는 지적사항이 있거나, 각각의 요구사항이 보상 대책으로 만족될 수 있는 경우, 또는 인증 과정 이후 CBS의 변경과 같은 다른 사유로 인해 시험은 일반적으로 생략되지 않을 수 있다.

(다) 선박 사이버복원력 시험절차서는 **202.**의 **1**항 (1)호 (마)에 기술된 보상 대책을 시험하는 방법을 또한 명시해야 한다.

(라) 선박 사이버복원력 시험절차서에는 시험 중에 상태를 업데이트하고 결과를 기록하는 수단을 포함해야 하며, 다음의 정보를 명시해야 한다.

(a) 필요한 시험 설정 (즉, 동일한 예상 결과로 시험이 반복될 수 있도록 보장하기 위한 것)

(b) 시험 장비

(c) 초기 조건

(d) 시험 방법론, 상세한 시험 단계

(e) 예상되는 결과 및 허용 기준

(마) 선박 사이버복원력 시험절차서를 우리 선급에 제출하기 전에 시스템 통합자는 변경관리에 따라 정보가 업데이트되고 있는지를 검증해야 한다.

(a) CBS와 이러한 선내 시스템을 선내가 아닌(예: 육상) 다른 CBS와 서로 연결하는 네트워크의 최신 설정이 일치해야 한다.

(b) 문서상 시험 내용은 선내 CBS 및 네트워크의 최종 설정상에서 관련 요건을 만족하기 위해 채택한 조치들의 설치 및 작동을 검증할 수 있도록 충분히 상세해야 한다.

(바) 시스템 통합자는 완전히 통합된 선박 내에서 보안 통제 및 조치에 대한 검증 시험 또는 평가를 문서화해야 한다. 또한, 구성에 대한 변경 관리를 유지하고, 선박 사이버복원력 시험절차서에서 다루는 특정 상황이나 고장으로 인해 안전 상태가 영향을 받을 수 있는 경우에 대하여 문서화된 시험 결과에 기록되어야 한다.

(사) 시험은 CBS의 가능한 다른 선내시험이 완료된 후 승인된 선박 사이버복원력 시험절차서에 따라 선내에서 실시해야 한다.

(아) 우리 선급이 필요하다고 인정하는 경우 추가적인 시험을 요구할 수 있다.

203. 유지검사

1. 일반사항

(1) 선박이 선주에게 인도된 후, 선주는 이 장에서 명시한 바에 따라 프로세스를 수립하고 이행함으로써 기술적 및 조직적 보안 대책을 관리해야 한다.

(2) CBS에 대한 변경은 **선급 및 강선규칙 6편 2장 4절**의 변경관리(MoC) 요구사항에 따라 실시되어야 한다. 여기에는 CBS의 문서를 최신 상태로 유지하는 것을 포함한다.

(3) 선주는 공급자의 지원을 받아 선박 사이버복원력 시험절차서를 최신 상태로 유지하고, 선내 CBS 및 이러한 시스템들을 서로 연결하거나 선박 외부(예: 육상)의 다른 CBS에 연결하는 네트워크와 일치하도록 유지해야 한다. 선주는 선내 CBS와 네트워크상에서 발생한 변경과 이러한 변경과 관련하여 발생할 수 있는 새로운 위험, 새로운 위협과 취약성 그리고 선박 운영 환경의 다른 가능한 변화를 고려하여 선박 사이버복원력 시험절차서를 업데이트해야 한다.

(4) 선주는 운영 절차를 준비하여 이행하여야 하며 선내 선원 및 다른 관련 육상 직원들에 대하여 선박에 탑재된 CBS 및 이들 시스템을 서로 간에 및 선내가 아닌(예: 육상) 다른 CBS에 연결하는 네트워크에 익숙하게 하고 요구사항의 충족을 위해 채택된 조치들을 적절하게 관리할 수 있도록 주기적인 교육과 훈련을 실시해야 한다.

(5) 선주는 공급자의 지원을 받아 선박에 탑재된 CBS의 하드웨어 및 소프트웨어와 이러한 시스템을 연결하는 네트워크의 정기적인 유지보수와 같은 요구의 충족을 위해 채택된 조치들을 최신 상태로 유지해야 한다.

(6) 선주는 시험 실시 결과의 사본과 업데이트된 선박 사이버복원력 시험절차서를 선내에 보관해야 하며, 이를 우리 선급에서 이용할 수 있어야 한다.

2. 연차검사

(1) 1번째 연차검사

(가) 선박의 1번째 연차검사 이전 적절한 시기(최초 검사의 경우 가능한 6개월 전) 까지, 선주는 CBS의 사이버보안 및 사이버복원력의 관리에 대한 선박 사이버보안 및 복원력 프로그램을 우리 선급에 승인용으로 제출하여야 한다.

(나) 선박 사이버보안 및 복원력 프로그램은 **4절**의 각 하부의 “유지검사”에 명시된 프로세스/활동에 대한 정책, 절차, 계획 및 기타 정보를 포함해야 한다.

(다) 선박 사이버보안 및 복원력 프로그램이 승인된 이후, 선주는 1번째 연차검사에서 승인된 선박 사이버보안 및 복원력 프로그램에 기술된 프로세스의 이행에 대한 기록 또는 다른 문서로 된 증거자료를 제시하여 준수 여부를 입증해야 한다.

(라) 선박의 관리회사가 변경된 경우, 우리 선급이 필요하다고 인정하는 경우 선박 사이버보안 및 복원력 프로그램의 새로운 승인을 추가로 요구할 수 있다.

(2) 후속 연차검사

선박의 후속 연차검사 시 선주는 우리 선급의 요청이 있는 경우 선박 사이버보안 및 복원력 프로그램의 이행 여부를 입증해야 한다.

3. 정기검사

선박 선급 증서의 갱신 시, 선주는 우리 선급의 입회하에 선박 사이버복원력 시험절차서에 따라 시험을 실시해야 한다. 특정 보안 보안장치들은 정기검사에서 실시되어야 하며, 다른 것들에 대해서는 **4절**의 "유지검사"의 하부에 명시된 바에 따라 CBS의 변경을 기반으로 우리 선급의 요청이 있는 경우 실시해야 한다.

제 3 절 요구사항의 목표와 구성

301. 주요 목표

1. 주요 목표는 사이버 위험에 대하여 운영상 복원력 있는 안전한 해운을 지원하는 것이다.
2. 안전한 해운은 효과적인 사이버 위험 관리 시스템을 통해 달성될 수 있다. 사이버 위험에 대하여 복원력이 있는 안전하고 확실한 해운을 지원하기 위해서, 사이버 위험 관리를 위한 다음의 하위 목표는 아래 302.에 나열된 5가지 기능 요소에 정의되어 있다.

302. 기능 요소별 하위 목표

1. 다음의 하위 목표 및 관련 기능 요소는 동시에 이루어져야 하며 하나의 포괄적인 위험 관리 프레임워크의 일부로서 고려되어야 한다. (표 2.3.1 참조)

표 2.3.1 기능 요소별 하위 목표

순서	기능 요소	목표	내용
1	식별	'식별' 기능 요소에 대한 요구사항은 다음을 식별하는 것을 목표로 한다. 1) 선내 CBS, 이들의 상호의존성 및 관련 정보 흐름; 2) 관리, 운영 및 거버넌스, 역할 및 책임과 관련된 주요 자원	선내 시스템, 사람, 자산, 데이터 및 기능(capabilities)에 대한 사이버보안 위험을 관리하기 위한 조직적 이해를 개발
2	보호	'보호' 기능 요소에 대한 요구사항은 잠재적 사고의 영향을 제한하거나 억제하는 능력을 지원하는 적절한 보호 장치의 개발 및 구현을 목표로 한다.	사이버 사고로부터 선박을 보호하고 해운 운영의 연속성을 최대화하기 위한 적절한 보호 장치를 개발하고 이행
3	탐지	'탐지' 기능 요소에 대한 요구사항은 선내 CBS 및 네트워크에 대한 이상 활동을 나타내고 인식하며 사이버 사고를 식별하는 능력을 지원하는 적절한 수단의 개발 및 구현을 목표로 한다.	선내 사이버 사고의 발생을 탐지하고 식별하기 위한 적절한 조치를 개발하고 이행
4	대응	'대응' 기능 요소에 대한 요구사항은 선내 CBS 및 네트워크에서 가능한 손상 확대를 포함한 사이버 사고의 영향을 최소화할 수 있는 능력을 지원하는 적절한 수단의 개발 및 구현을 목표로 한다.	선내에서 탐지된 사이버 사고에 대한 조치를 취하기 위한 적절한 조치 및 활동을 개발하고 이행
5	복구	'복구' 기능 요소에 대한 요구사항은 사이버 사고의 영향을 받은 선내 CBS 및 네트워크를 복구하는 기능을 지원하는 적절한 수단의 개발 및 구현을 목표로 한다.	사이버 사고로 인해 손상된 선박 운항에 필요한 모든 기능 또는 서비스를 복구하기 위한 적절한 조치 및 활동을 개발하고 이행

303. 요건의 구성

1. 요건은 목표 기반 접근 방식에 따라 구성된다. 기능적/기술적 요구사항은 각 기능 요소의 특정 하위 목표 달성을 위해 제공된다. 요구사항은 OT 시스템의 운영상 위험 및 복잡성에 관계 없이 수용이 가능한 수준의 복원력을 가능하게 하고 모든 유형의 선박/장치에 적용이 가능한 방식으로 모든 유형의 선박에 일관된 구현을 가능하게 하고 적용할 수 있도록 하기 위함이다.
2. 각 요구사항에 대한 근거(rationale)가 제공되었다.
3. 선박 수명의 각 단계와 해당 단계에 참여하는 관련 이해관계자에 대해 수행해야 할 조치 및 사용 가능한 문서 요약

은 **표 2.2.1**에 제공되었다.

4. **4절**은 **302.**에서 식별된 5가지 기능 요소에 따라 구성된 **301.**에 정의된 기본 목표를 달성하기 위해 충족되어야 하는 요구사항들을 포함한다.

304. 이해관계자

1. 이 장의 요건은 선박의 설계, 건조 및 운항에 관련된 이해관계자의 책임하에 충족되어야 한다. 그들 중 다음 이해관계자들이 식별될 수 있다. (용어 정의는 **1장 2절** 참조)
   (1) 선주/회사
   (2) 시스템 통합자
   (3) 공급자
   (4) 우리 선급
2. 상기 요건은 이들 이해관계자에 의해 충족될 수 있지만, 이 장의 목적을 위해 이를 충족할 책임은 우리 선급과 계약한 이해관계자에게 있다.

제 4 절 선박의 사이버복원력 요구사항

401. 식별

1. 선박 자산 목록(Vessel asset inventory)

(1) 요구사항

CBS의 하드웨어 및 소프트웨어(응용 프로그램, 운영 체제, 만약 있다면 펌웨어 및 기타 소프트웨어 구성 요소를 포함)와 이러한 시스템들을 서로 간 및 선내 다른 CBS 또는 육상으로 연결하는 네트워크의 목록은 선박의 전체 수명 동안 제공되고 최신으로 유지되어야 한다.

(2) 세부 요구사항

(가) 선박 자산 목록은 선내에 존재하는 **1장 103.**의 2항에 나열된 CBS들을 최소한 포함해야 한다.

(나) 목록은 선박의 전체 수명 동안 업데이트를 유지해야 한다. 잠재적으로 새로운 취약성을 도입하거나 시스템 간의 기능 종속성 또는 연결을 변경하는 소프트웨어 및 하드웨어 변경 사항은 목록에 기록되어야 한다.

(다) 기밀 정보(예: IP 주소, 프로토콜, 포트 번호)가 목록에 포함되어 있는 경우, 이러한 정보에 대한 접근을 오직 허가된 사람으로 제한하기 위한 특별한 조치를 해야 한다.

(라) 하드웨어

모든 하드웨어 장치의 경우, 선박 자산 목록에는 최소한 **3장 301.**의 1항의 정보를 포함해야 한다. 또한, 선박 자산 목록은 CBS와 관련된 시스템 카테고리 및 보안 구역을 지정할 수 있다.

(마) 소프트웨어

(a) 모든 소프트웨어(예: 응용 프로그램, 운영 체제, 펌웨어)의 경우, 선박 자산 목록에는 최소한 **3장 301.**의 1항의 정보를 포함해야 한다.

(b) CBS의 소프트웨어는 선박 사이버보안 및 복원력 프로그램상 선주의 소프트웨어 유지보수 관리에 대한 프로세스 및 업데이트 정책에 따라 유지보수 및 업데이트되어야 한다. (**203.** 참조).

(3) 근거

OT 시스템에 사용되는 선내 CBS와 관련 소프트웨어 목록은 선박의 사이버복원력을 효과적으로 관리하는 데 필수적이며, 모든 CBS가 잠재적인 취약점이 되는 주요 원인이다. 사이버 범죄자들은 시스템을 해킹하기 위해 미확인된 오래된 하드웨어와 소프트웨어를 악용할 수 있다. 또한, CBS 자산을 관리함으로써 회사는 선박 안전 목표에 대한 각 시스템의 중요도(criticality)를 이해할 수 있다.

(4) 등록검사

(가) 설계 단계

(a) 시스템 통합자는 선박 자산 목록을 우리 선급에 제출해야 한다. (**202.**의 1항 (1)호 참조)

(b) 선박 자산 목록은 모든 개별 CBS의 자산 목록을 포함해야 한다. 시스템 통합자에 의해 제공되는 모든 장비는 선박 자산 목록에 포함되어야 한다.

(나) 건조 단계

시스템 통합자는 업데이트된 선박 자산 목록을 유지해야 한다

(다) 선내시험 단계

(a) 시스템 통합자는 선박 사이버복원력 시험절차서(**202.**의 2항 (2)호 참조)을 제출해야 하며, 다음 사항을 우리 선급에 입증해야 한다.

(i) 인도 시 선박 자산 목록에 대한 업데이트 및 완성도

(ii) CBS는 선박 자산 목록에 대한 표시의 정확성

(iii) CBS의 소프트웨어는 업데이트 상태, 예를 들어 취약성 스캐닝 또는 스위치를 켜는 동안 CBS의 소프트웨어 버전을 확인하여 입증

(5) 유지검사

(가) 일반사항

(a) 운항 단계에서 검사에 대한 일반 요구사항에 대해서는 **203.**을 참고한다.

(b) 선주는 선박 사이버보안 및 복원력 프로그램에서 CBS에 대한 이 장의 최소한 다음 요구사항들을 반영한 변경 관리(MoC) 프로세스를 기술해야 한다.

(i) 변경 관리(**203.**의 1항)

(ii) 하드웨어 및 소프트웨어 변경(**401.**의 1항 (2))

(c) 선주는 선박 사이버보안 및 복원력 프로그램에서 최소한 다음 요구사항들을 반영한 소프트웨어 업데이트 관

리를 기술해야 한다.

(i) 취약점 및 사이버 위험(401.의 1항 (2)호 및 (3)호)

(ii) 보안 패치(402.의 6항 (2)호 (마))

(나) 1번째 연차검사

선주는 우리 선급에 선박 사이버보안 및 복원력 프로그램을 이행하고 있음을 입증하는 기록 및 기타 문서로 된 아래의 증빙자료를 제출해야 한다.

(a) 승인된 변경 관리 프로세스가 준수되고 있다.

(b) CBS의 소프트웨어에 대한 알려진 취약점과 기능 종속성이 고려되고 있다.

(c) 선박 자산 목록은 업데이트가 유지되고 있다.

(다) 후속 연차검사

선주는 1번째 연차검사에서 명시된 바와 같이 선박 사이버보안 및 복원력 프로그램을 이행하고 있음을 기록 및 기타 문서로 된 증거자료를 제시함으로써 우리 선급에 입증해야 한다.

(라) 정기검사

선주는 선박 사이버복원력 시험절차서에 따라 401.1.(4).(다)의 활동을 우리 선급에 입증해야 한다.

402. 보호

1. 보안 구역 및 네트워크 분할 (Security Zones and Network Segmentation)

(1) 요구사항

(가) 모든 CBS는 잘 정의된 보안 정책 및 보안 기능을 가진 보안 구역으로 그룹화되어야 한다.

(나) 보안 구역은 격리(예: 에어 갭)되거나 구역 간 통신하는 데이터의 통제를 제공하는 수단(예: 방화벽/라우터, 단방향 시리얼 링크, TCP/IP 다이오드, 드라이 접점 등)에 의해 다른 보안 구역 또는 네트워크에 연결되어야 한다.

(다) 명시적으로 허용된 트래픽만 보안 구역 경계를 통과해야 한다.

(2) 세부 요구사항

(가) 보안 구역에는 다수의 CBS와 네트워크를 포함할 수 있으며, 이들 모두 이 장 및 3장에 있는 적용 가능한 보안 요구사항들을 만족해야 한다.

(나) 보안 구역의 네트워크는 논리적 또는 물리적으로 다른 구역 또는 네트워크와 분할해야 한다. (402.의 6항 (2)호 또한 참조)

(다) 규정에서 요구되는 안전 기능들을 제공하는 CBS는 별도의 보안 구역으로 그룹화되어야 하며 다른 보안 구역과 물리적으로 분할해야 한다.

(라) 항해 및 통신 시스템은 기관 또는 화물 시스템과 동일한 보안 구역 내에 있지 않아야 한다. 만약 항해 및/또는 무선통신 시스템이 다른 동등한 표준에 따라 승인된 경우(3장 102.의 2항 참조), 이러한 시스템은 전용의 보안 구역 내에 있어야 한다.

(마) 무선 장치는 전용의 보안 구역 내에 있어야 한다. (402.의 5항 또한 참조)

(바) 이 장의 적용 범위 밖에 있는 시스템, 네트워크 또는 CBS는 비신뢰 네트워크로 고려되어야 하며 이 장에서 요구되는 보안 구역들과 물리적으로 분할되어야 한다. 대안적으로 OT 시스템이 구역에서 요구하는 것과 동일한 요구사항을 만족하는 경우, 이러한 시스템은 보안 구역의 일부로서 허용한다.

(사) 구역 내 CBS의 주요 기능에 영향을 주지 않고 보안 구역을 격리하는 것이 가능해야 한다. (404.의 3항 참조)

(3) 근거

네트워크는 방화벽 경계로 보호되고 들어오는 트래픽을 감시하기 위해 침입 탐지 시스템(IDS) 또는 침입 방지 시스템(IPS)으로 보호될 수도 있지만, 경계를 위반하는 것은 항상 가능하다. 네트워크 분할은 공격자가 전체 네트워크를 통해 공격하여 침투하는 것을 더 어렵게 한다.

보안 구역 및 네트워크 분할의 주요 이점은 공격 표면의 범위를 줄이고 공격자가 시스템을 통한 측면 이동을 달성하는 것을 방지하며 네트워크 성능을 향상시키는 것이다. CBS를 보안 구역에 할당하는 개념은 위험 프로필에 따라서 CBS를 그룹화하는 것을 허용한다.

(4) 등록검사

(가) 설계 단계

(a) 시스템 통합자는 구역 및 전송로 다이어그램과 사이버보안 설계 기술서를 제출해야 한다. (202.의 1항 (1)호 참조)

(b) 구역 및 전송로 다이어그램은 CBS들을 어떻게 보안 구역으로 그룹화했는지에 대하여 보여야 하며, 다음의 정보를 포함해야 한다.

(i) 보안 구역의 명확한 표시

(ii) 각 CBS의 단순한 삽화(illustration), 그리고 CBS가 할당된 보안 구역 표시 및 CBS/장비의 물리적 위치 표시

(iii) 공급자가 제공한 CBS 시스템 토폴로지 다이어그램의 승인된 버전을 참조(**3장 301.**의 2항)

(iv) 보안 구역 내 시스템 간의 네트워크 통신의 삽화

(v) 서로 다른 보안 구역(전송로)에 있는 시스템 간의 어떠한 네트워크 통신의 삽화

(vi) 보안 구역 내 시스템 간 및 비신뢰 네트워크(전송로) 간의 어떠한 통신의 삽화

(c) 시스템 통합자는 사이버보안 설계 기술서 상에 다음의 정보를 포함해야 한다.

(i) 보안 구역에 할당된 CBS의 간략한 설명. 구역 및 전송로 다이어그램에서 각 CBS를 식별하는 것이 가능해야 한다.

(ii) 동일한 보안 구역 내 CBS들 간의 네트워크 통신. 기술서에는 통신의 목적과 특성(즉, 프로토콜 및 데이터 흐름)을 포함해야 한다.

(iii) 서로 다른 보안 구역 내 CBS들 간의 네트워크 통신. 기술서에는 통신의 목적과 특성(즉, 프로토콜 및 데이터 흐름)을 포함해야 한다. 기술서는 또한 구역 경계 장치를 포함하고, 구역 경계를 통과하는 것이 허용되는 트래픽(예: 방화벽 규칙)인지를 명시해야 한다.

(iv) 보안 구역에 있는 CBS와 비신뢰 네트워크 간의 어떠한 통신. 기술서는 이산 신호, 시리얼 통신, IP 기반 네트워크 통신의 목적과 특성(즉, 프로토콜 및 데이터 흐름)을 포함해야 한다. 또한, 기술서에는 구역 경계 장치를 포함해야 하며, 구역 경계를 통과하는 것이 허용되는 트래픽(예: 방화벽 규칙)을 명시해야 한다.

(나) 건조 단계

시스템 통합자는 구역 및 전송로 다이어그램을 최신으로 유지해야 한다.

(다) 선내시험 단계

시스템 통합자는 선박 사이버복원력 시험절차서(**202.**의 2항 (2)호 참조)를 제출하고 다음을 우리 선급에 입증해야 한다.

(a) 승인된 문서들(즉, 구역 및 전송로 다이어그램, 사이버보안 설계 기술서, 자산 목록 및 공급자가 제공한 관련 문서들)에 따라 선내 보안 구역이 구현되어 있다. 이것은 예를 들어 물리적 검사, 네트워크 스캐닝 및/또는 기타 방법 등을 통해 설치된 장비들이 승인된 설계에 따라 보안 구역으로 그룹화되어 있음을 검사원의 확인을 통하여 입증할 수 있다.

(b) 보안 구역 경계는 승인된 사이버보안 기술서에 문서화되어 있는 트래픽만을 허용한다. 이것은 예를 들어 방화벽 규칙의 평가 또는 포트 스캐닝을 통해 확인할 수 있다.

(5) 유지검사

(가) 일반사항

(a) 운항 단계에서 검사에 대한 일반 요구사항은 **203.**을 참고한다.

(b) 선주는 선박 사이버보안 및 복원력 프로그램에서 보안 구역 경계 장치(예: 방화벽)의 관리를 기술해야 하며, 이 장의 요구사항에 따라 최소한 다음을 다루어야 한다.

(i) 최소 기능의 원칙 (**402.**의 2항 (1)호)

(ii) 예외적으로 허용된 트래픽 (**402.**의 1항 (1)호)

(iii) 서비스 거부(DoS) 사건에 대한 보호 (**402.**의 2항 (1)호)

(iv) 보안 감사 기록의 검사 (**403.**의 1항 (2)호)

(나) 1번째 연차검사

선주는 구역 및 전송로 다이어그램이 최신 상태로 유지되고 있음을 우리 선급에 입증해야 하며, 선박 사이버보안 및 복원력 프로그램의 이행, 즉 보안 구역 경계는 상기 요건에 따라 관리되고 있음을 입증하는 기록 또는 문서로 된 증거자료를 제시해야 한다.

(다) 후속 연차검사

선주는 우리 선급의 요청 시 1번째 연차검사에 명시된 것와 같이 기록 또는 다른 문서로 된 증거자료를 제시함으로써 선박 사이버보안 및 복원력 프로그램의 이행을 입증해야 한다.

(라) 정기검사

선주는 선박 사이버복원력 시험절차서에 따른 **402.**의 1항 (4)호 (다)의 활동을 우리 선급에 입증해야 한다.

2. 네트워크 보호 안전장치(safeguard)

(1) 요구사항

(가) 보안 구역은 402.의 1항에서 명시된 것와 같이 방화벽 또는 동등한 수단으로 보호되어야 한다.

(나) 네트워크는 과도한 데이터 흐름 속도 및 네트워크 자원의 서비스 품질을 훼손할 수 있는 기타 사건의 발생으로부터 보호되어야 한다.

(다) CBS는 최소 기능의 원칙에 따라 구현되어야 한다. 즉, 필수 기능만 제공하고 비필수 기능의 사용은 금지하거나 제한하도록 구성되어야 하며, 불필요한 기능, 포트, 프로토콜 및 서비스는 비활성화되거나 그 외에는 금지되어야 한다.

(2) 세부 요구사항

(가) 네트워크 설계에는 네트워크를 통한 의도된 데이터 흐름을 충족하고 서비스 거부(DoS) 및 네트워크 스톰/높은 트래픽 속도의 위험을 최소화하기 위한 수단을 포함해야 한다.

(나) 데이터 흐름 속도의 추정은 네트워크 용량, 의도된 응용 소프트웨어 및 데이터 형식에 대한 데이터 속도 요구사항을 최소한 고려해야 한다.

(3) 근거

네트워크 보호는 컴퓨터 네트워크의 무결성, 기밀성 및 가용성을 보호하도록 설계된 다양한 기술, 규칙 및 설정을 포함한다. 위협 환경은 항상 변화하고 있으며 공격자는 항상 취약점을 찾아 악용하려고 시도한다.

네트워크 보호를 다룰 때는 고려해야 할 많은 계층이 존재한다. 공격은 네트워크 계층 모델의 모든 계층에서 발생할 수 있으므로, 네트워크 하드웨어, 소프트웨어 및 정책은 각 영역을 고려하도록 설계되어야 한다.

물리적 및 기술적 보안 통제는 권한이 없는 선원으로부터 네트워크 구성품에 물리적으로 접근하는 것을 방지하고 저장되거나 네트워크를 통해 전송 중에 있는 데이터를 보호하도록 설계되며, 절차적 보안 통제는 사용자 행동을 통제하는 보안 정책 및 프로세스로 구성된다.

(4) 등록검사

(가) 설계 단계

요구사항 없음

(나) 건조 단계

요구사항 없음

(다) 선내시험 단계

(a) 시스템 통합자는 선박 사이버복원력 시험절차서(202.의 2항 (2)호 참조)를 제출해야 하며, 우리 선급에 다음을 입증해야 한다.

(i) 적용이 가능한 경우, 구역 경계 보호 장치를 목표하는 서비스 거부(DoS) 공격 시험

(ii) 각 네트워크 세그먼트 내부로부터 발생하는 과도한 데이터 흐름 속도에 대한 보호를 보장하기 위한 서비스 거부를 시험. 이러한 서비스 거부(DoS) 시험은 네트워크의 한계 초과(즉, 네트워크 세그먼트 상의 가용 용량을 소비하는 시도) 및 응용 계층 공격(즉, 네트워크 내의 선택된 종단지점의 용량을 처리) 커버해야 한다.

(iii) 예를 들어, 분석적 평가 및 포트 스캐닝을 통해, CBS의 불필요한 기능, 포트, 프로토콜 및 서비스가 공급자가 제공한 강화 지침에 따라 제거되었거나 금지되었는지 시험 (3장 203.의 5항 (7)호 및 3장 502.의 7항 참조)

(b) 상기 (ii) 및 (iii)의 시험은 202.의 2항 (2)호에 따라 CBS의 인증 중에 실시된다면 생략될 수 있다.

(5) 유지검사

운영 단계에서 검사에 대한 일반 요구사항은 203.을 참조한다.

(가) 정기 검사

CBS에 변경이 있는 경우, 선주는 선박 사이버복원력 시험절차서에 따라 402.의 2항 (4)호 (다)의 활동을 우리 선급에 입증해야 한다.

3. 안티바이러스, 안티멀웨어, 안티스팸 및 악성코드로부터 기타 보호

(1) 요구사항

CBS는 바이러스, 웜, 트로이 목마, 스파이웨어 등과 같은 악성코드로부터 보호되어야 한다.

(2) 세부 요구사항

(가) 멀웨어 보호는 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 안티바

이러스 및/또는 안티멀웨어 소프트웨어가 설치되어, 유지 관리 및 정기적으로 업데이트되어야 한다.

(나) 안티바이러스 및 안티멀웨어 소프트웨어를 설치할 수 없는 CBS의 경우, 멀웨어 보호는 운영 절차, 물리적 보호 장치의 형태로 또는 공급자의 권장 사항에 따라 구현되어야 한다.

(3) 근거

사용자가 모르는 사이에 사용자의 시스템에 침입하는 바이러스 또는 사용자 동의 없이 설치된 프로그램은 자가 복제 및 확산될 수 있으며 시스템 성능, 사용자의 데이터/파일에 영향을 미치거나 데이터 보안 조치를 우회하는 원치 않는 악의적인 작업을 수행할 수 있다.

안티바이러스, 안티멀웨어, 안티스팸 소프트웨어는 예방 기능을 수행하는 악의적인 침입 바이러스를 방어하는 경비원이 있는 닫힌문과 같은 역할을 한다. 잠재적인 바이러스를 감지한 다음 대부분 바이러스가 시스템에 피해를 주기 전에 제거한다.

악성코드가 CBS에 침입하는 일반적인 수단은 전자 메일, 전자 메일의 첨부 파일, 웹사이트, 이동식 미디어(예: 범용 직렬 버스(USB) 장치, 디스켓 또는 컴팩트 디스크), PDF 문서, 웹 서비스, 네트워크 연결 및 감염된 노트북이다.

(4) 등록검사

(가) 설계 단계

시스템 통합자는 사이버보안 설계 기술서 상에 다음의 정보를 포함해야 한다.

(a) 각 CBS에 대한 악성코드 및 무단 소프트웨어에 대한 보호를 위해 제공업체가 제공한 승인된 메커니즘의 요약

(b) 멀웨어 방지 소프트웨어를 가진 CBS에 대하여, 소프트웨어 업데이트를 유지하는 방법에 대한 정보

(c) 선주의 관리 시스템에서 이행되어야 할 어떠한 운영 조건 또는 필요한 물리적 보호조치

(나) 건조 단계

시스템 통합자는 건조 단계에서 멀웨어 보호가 업데이트 상태로 유지되도록 보장해야 한다.

(다) 선내시험 단계

(a) 시스템 통합자는 선박 사이버복원력 시험절차서(202.의 2항 (2)호 참조)를 제출하고 우리 선급에 다음을 입증해야 한다.

(i) 승인된 멀웨어 방지 소프트웨어 또는 다른 보상 대책이 유효함 (예: 신뢰할 수 있는 멀웨어 방지 시험 파일로 시험)

(b) 상기 시험은 202.의 2항 (2)호에 따른 CBS의 인증 중에 실시될 경우 생략할 수 있다.

(5) 유지검사

(가) 일반사항

(a) 운항 단계에서 검사에 대한 일반 요구사항은 203.을 참조한다.

(b) 선주는 선박 사이버보안 및 복원력 프로그램에서 이 장의 최소한 다음의 요구사항들을 다루는 멀웨어 방지의 관리를 기술해야 한다.

(i) 유지보수/업데이트 (402.의 3항 (2)호)

(ii) 운영 절차, 물리적 보호조치(402.의 3항 (2)호)

(iii) 모바일, 휴대용, 이동식 매체의 사용 (402.의 4항 (2)호 (라) 및 402.의 7항 (2)호)

(iv) 접근 통제 (402.의 4항)

(나) 1번째 연차검사

선주는 선박 사이버보안 및 복원력 프로그램의 이행을 입증하는 기록 또는 다른 문서로 된 증거자료를 우리 선급에 제시해야 하며, 즉 다음을 확인한다.

(a) 멀웨어 방지 소프트웨어가 유지보수되고 업데이트되고 있음.

(b) 모바일, 휴대용 또는 이동식 매체에 대한 절차를 따르고 있음.

(c) 접근 통제에 대한 정책과 절차를 따르고 있음.

(d) 물리적 보호조치가 유지되고 있음.

(다) 후속 연차검사

선주는 선급의 요청 시 1번째 연차검사에서 명시된 것과 같이 기록 및 문서로 된 증거자료를 제시하여 선박 사이버보안 및 복원력 프로그램의 이행을 입증해야 한다.

(라) 정기검사

선주는 선박 사이버복원력 시험절차서에 따라 402.의 3항 (4)호 (다)의 활동을 우리 선급에 입증해야 한다.

4. 접근 통제(Access control)

(1) 요구사항

(가) CBS 및 네트워크는 시스템 자체와 통신하거나 상호 작용하기 위해, 정보 처리를 위해 시스템 자원을 사용하기 위해, 시스템이 포함하는 정보의 지식을 얻거나 시스템 구성요소와 기능을 제어하기 위한 능력과 수단을 선택적으로 제한하는 물리적 및/또는 논리적/디지털 조치를 제공해야 한다.

(나) 이러한 조치는 최소 특권 원칙에 따라 접근 수준에 대해 인가된 선원이 CBS에 접근하는 능력을 방해하지 않는 방식이어야 한다.

(2) 세부 요구사항

CBS와 네트워크 및 이러한 시스템에 저장된 모든 정보에 대한 접근은 이들의 직무 또는 의도된 기능의 일부로서 정보 접근의 필요성을 바탕으로 인가된 선원에게만 허용되어야 한다.

(가) 물리적 접근 통제

카테고리 II 및 카테고리 III의 CBS는 무단 접근을 방지하기 위해 일상적으로 잠겨진 방 내 또는 통제 공간 내에 일반적으로 위치하거나, 잠금 케비닛 또는 콘솔 내에 설치되어야 한다. 이러한 위치 또는 잠금 캐비닛/콘솔은 그러나 설치, 통합, 운영, 유지보수, 수리, 교체, 폐기 등을 위해 CBS에 접근할 필요가 있는 선원 및 여러 이해관계자들이 선박의 효과적이고 효율적인 운항을 방해하지 않고 쉽게 접근할 수 있어야 한다.

(나) 방문객에 대한 물리적 접근 통제

정부관계자, 기술자, 대리인, 항만 및 터미널 공무원 및 선주 대표자와 같은 방문객은 예를 들어 선내 감독 하에 접근을 허용하는 경우를 제외하고 선내에서 CBS에 대한 접근이 제한되어야 한다.

(다) 네트워크 접근 지점의 물리적 접근 통제

(a) 카테고리 II 또는 카테고리 III의 CBS를 연결하는 선내 네트워크에 대한 접근 지점은 문서로 된 절차(예: 유지보수)에 따라 감독 하에 연결하는 경우를 제외하고 물리적 및/또는 논리적으로 차단되어야 한다.

(b) 모든 선내 네트워크, 또는 전용의 게스트 접근 네트워크 또는 여객 오락 활동 전용 네트워크와 같은 다른 네트워크로부터 격리되는 독립된 컴퓨터가 방문객에 의한 간헐적인 연결 요청(예: 문서 인쇄용)이 있는 경우 사용되어야 한다.

(라) 이동식 매체 통제 (Removable media controls)

이동식 매체 장치의 사용에 대한 정책이 선박 시스템에 파일을 업로드하거나 선박에서 데이터를 다운로드하는 것을 허용하기 이전에 전자서명과 워터마크 및 스캔을 통해 이동식 매체를 멀웨어에 대해 점검 및/또는 합법적인 소프트웨어를 검증하기 위한 절차와 함께 수립되어야 한다. (**402.**의 **7**항 참조)

(마) 자격증명 관리 (Management of credentials)

(a) CBS 및 관련 정보는 파일 시스템, 네트워크, 애플리케이션 또는 데이터베이스 특정 접근 통제 목록(ACL)으로 보호되어야 한다. 선내 및 육상 직원에 대한 계정은 계정 소유자의 역할과 책임에 따라 제한된 기간 동안만 활성 상태로 유지되어야 하며 더 이상 필요하지 않은 경우 삭제되어야 한다.

(비고) CBS는 **3장 표 3.4.1**의 1번 항목에 따른 인간 사용자를 식별 및 인증해야 한다. 달리 말하면, 모든 인간 사용자들을 유일하게 식별하고 인증하는 것은 불필요하다.

(b) 선내 CBS에는 이들의 보안 구역 정책에 적합하면서 주요 목적에 부정적인 영향을 미치지 않는 적절한 접근 통제가 제공되어야 한다. 강력한 접근 통제가 필요한 CBS는 강력한 암호키 또는 다중요소 인증을 사용하여 보호해야 한다.

(c) 관리자 권한은 접근 통제 정책에 따라 관리되어야 하며, 오직 인가된 적절한 교육을 받은 선원만 CBS에 대한 전체 접근을 허용해야 하며, 회사 내 또는 선상에서 이들 역할의 일부로서 이러한 권한을 사용하여 시스템에 로그인할 필요가 있다.

(바) 최소 권한 원칙 (Least privilege principle)

(a) CBS 및 네트워크에 접근이 허용되는 어떤 인간 사용자는 그 기능을 수행하는데 필요한 최소 권한만 가져야 한다.

(b) 모든 새 계정 권한에 대한 기본 설정은 가능한 한 낮게 설정되어야 한다. 가능한 한 상향된 권한은 예를 들어 만료되는 권한과 1회용 자격증명만 사용하여 필요한 순간만으로 한정되어야 한다. 시간상 권한 축적은 예를 들어 사용자 계정의 정기적인 감사를 통해 피해야 한다.

(3) 근거

공격자는 선박 내, 회사 내 또는 인터넷 연결을 통해 원격으로 선박의 시스템 및 데이터에 접근을 시도할 수 있다. 사이버 자산, 네트워크 등에 대한 물리적 및 논리적 접근 통제는 선박과 화물의 안전을 보장하기 위해 구현되어야 한다.

또한 물리적 위협 및 관련 대응책은 ISPS 코드에서도 고려된다. 이와 유사하게 ISM 코드는 선박의 안전한 운항과

환경 보호를 위한 지침이 포함되어 있다. ISPS 코드 및 ISM 코드의 구현은 선박 보안 계획서(SSP: Ship Security Plan) 및 선박 안전 경영 시스템(SMS: Safety Management System)에 안전 중요 자산에 대한 접근 통제를 위한 설명과 절차를 포함하는 것을 의미할 수 있다.

(4) 등록검사

(가) 설계 단계

시스템 통합자는 사이버보안 설계 기술서에 다음 정보를 포함해야 한다.

(a) CBS에 대한 위치 및 물리적 접근 통제. 즉각적인 접근을 필요로 하는 운영자를 위한 휴먼머신인터페이스(HMI)를 제공하는 장치는 이들이 물리적 접근 통제 장소 내에 설치되는 경우 사용자 식별 및 인증을 시행할 필요가 없다. 이러한 장치는 명시되어야 한다.

(나) 건조 단계

시스템 통합자는 건조 단계에서 CBS에 대한 무단 접근을 방지해야 한다.

(다) 선내시험 단계

시스템 통합자는 선박 사이버복원력 시험절차서(202.의 2항 (2)호 참조)를 제출하고 다음을 우리 선급에 입증해야 한다.

(a) CBS의 구성 요소는 물리적 접근이 인가된 선원으로 통제될 수 있는 장소 또는 외함 내에 위치한다.

(b) 사용자 권한은 직무 분리 및 최소 권한의 원칙에 따라 설정되며, 임시 계정은 삭제되어야 한다. (202.의 2항 (2)호에 따라 CBS의 인증을 기초로 생략될 수 있음)

(5) 유지검사

(가) 일반사항

(a) 운항 단계에서 검사에 대한 일반 요구사항은 203.을 참조한다.

(b) 선주는 선박 사이버보안 및 복원력 프로그램에서 논리적 및 물리적 접근 관리를 기술해야 하며, 이 장의 최소한 다음의 요구사항들을 다루어야 한다.

(i) 물리적 접근 통제 (402.의 4항 (2)호 (가))

(ii) 방문객에 대한 물리적 접근 통제 (402.의 4항 (2)호 (나))

(iii) 네트워크 접근 지점의 물리적 접근 통제 (402.의 4항 (2)호 (다))

(iv) 자격 증명 관리 (402.의 4항 (2)호 (마))

(v) 최소 권한 정책 (402.의 4항 (2)호 (바))

(c) 선주는 선박 사이버보안 및 복원력 프로그램에서 기밀 정보 관리를 기술해야 하며, 이 장의 최소한 다음의 요구사항을 다루어야 한다.

(i) 기밀 정보 (401.의 1항 (2)호)

(ii) 인가된 선원에 허용되는 정보 (402.의 4항 (2)호)

(iii) 무선 네트워크상 전송되는 정보 (402.의 5항 (2)호)

(나) 1번째 연차검사

선주는 선박 사이버보안 및 복원력 프로그램의 이행을 입증하는 기록 또는 다른 문서로 된 증거자료를 우리 선급에 제출해야 하며, 즉 다음을 확인한다.

(a) 선원은 그들의 책무에 따라 CBS에 접근하는 것이 허가된다.

(b) 허가된 장치만 CBS에 연결한다.

(c) 방문객은 관련 정책 및 절차에 따라 CBS에 대한 접근이 주어진다.

(d) 물리적 접근 통제가 유지되고 적용된다.

(e) 자격증명, 키, 비밀, 인증서, 관련 CBS 문서들 및 다른 민감한 정보는 관련 정책 및 절차에 따라 기밀로 관리되고 유지된다.

(다) 후속 연차검사

선주는 선급의 요청 시 1번째 연차검사에서 명시된 것과 같이 기록 또는 문서로 된 증거자료를 제시하여 선박 사이버보안 및 복원력 프로그램의 이행을 입증해야 한다.

5. 무선통신

(1) 요구사항

이 장의 적용 범위 내에 있는 무선통신 네트워크는 다음을 보장하도록 설계, 구현 및 유지 관리되어야 한다.

(가) 사이버 사고는 다른 제어 시스템으로 전파되지 않는다.

(나) 허가된 인간 사용자만 무선 네트워크에 접근할 수 있다.

(다) 허가된 프로세스 및 장치만 무선 네트워크에서 통신을 허용한다.
(라) 무선 네트워크에서 전송 중인 정보는 조작되거나 공개할 수 없다.

(2) 세부 요구사항

(가) 무선 네트워크에서 전송되는 정보의 무결성과 기밀성을 보장하기 위해 산업계 표준 및 모범 사례에 따라 암호화 알고리즘 및 키 길이와 같은 암호화 메커니즘을 적용해야 한다.
(나) 무선 네트워크의 장치는 무선 네트워크상에서만 통신해야 한다. (즉, “dual-homed”가 아니어야 함).
(다) 무선 네트워크는 402.의 1항에 따라 별도의 구역(segment)으로 설계되어야 하고 402.의 2항에 따라 보호되어야 한다.
(라) 네트워크에 있는 무선 접근 지점 및 기타 장치는 네트워크에 대한 접근이 통제될 수 있도록 설치 및 구성되어야 한다.
(마) 무선통신을 활용하는 네트워크 장치 또는 시스템은 통신에 참여하는 모든 사용자(사람, 소프트웨어 프로세스 또는 장치)를 식별하고 인증하는 기능을 제공해야 한다.

(3) 근거

무선 네트워크는 유선 네트워크보다 추가의 또는 다른 사이버보안 위험을 야기한다. 이것은 주로 장치의 불충분한 물리적 보호와 무선 주파수 통신의 사용 때문이다.
부적절한 물리적 접근 통제는 미허가 선원이 물리적 장치에 접근을 획득하게 할 수 있으며, 이는 논리적 접근 제한을 우회하거나 네트워크에 악성 장치(rogue device)를 배치하는 것을 초래할 수 있다.
무선 주파수에서 신호 전송은 Piggybacking 또는 Evil Twin 공격을 제공하는 도청뿐만 아니라 재밍에 관계된 위험을 도입한다. (https://us-cert.cisa.gov/ncas/tips/ST05-003 참조).

(4) 등록검사

(가) 설계 단계

시스템 통합자는 사이버보안 설계 기술서에 다음의 정보를 포함해야 한다.
(a) 무선 네트워크와 이들이 별도의 보안 구역으로 구현되는 방법에 대한 기술. 기술서에는 구역 경계 장치를 포함하고, 구역 경계를 통과하도록 허용되는 트래픽(예: 방화벽 규칙)을 명시해야 한다.

(나) 건조 단계

시스템 통합자는 건조 단계에서 무선 네트워크에 대한 무단 접근를 방지해야 한다.

(다) 선내시험 단계

(a) 시스템 통합자는 선박 사이버복원력 시험절차서(202.의 2항 (2)호 참조)을 제출하고 다음을 우리 선급에 입증해야 한다.
(i) 오직 허가된 장치만 무선 네트워크에 접근할 수 있음.
(ii) 보안 무선통신 프로토콜이 각 제공업체의 승인된 문서에 따라 사용됨 (예를 들어 네트워크 프로토콜 분석 도구를 사용하여 입증)
(b) 상기 시험은 202.의 2항 (2)호에 따른 CBS의 인증 중에 실시될 경우 생략할 수 있다.

(5) 유지검사

운항 단계에서 검사에 대한 일반 요구사항은 203.을 참조한다.

(가) 정기 검사

무선 네트워크에 변경이 있는 경우, 선주는 선박 사이버복원력 시험절차서에 따라 402.의 5항 (4)호 (다)의 활동을 우리 선급에 입증해야 한다.

6. 원격 접근 통제 및 비신뢰 네트워크에서 통신

(1) 요구사항

CBS는 비신뢰 네트워크로부터 무단 접근 및 다른 사이버 위협으로부터 보호되어야 한다.

(2) 세부 요구사항

(가) 사용자 매뉴얼은 선내 IT 및 OT 시스템에 대한 원격 접근 통제를 위해 제공되어야 한다. 명확한 지침은 기능과 함께 역할과 허가를 식별해야 한다.
(나) CBS에 대하여, 어떠한 IP 주소도 비신뢰 네트워크상에 노출되지 않아야 한다.
(다) 비신뢰 네트워크와 또는 이를 경유한 통신에는 종단점 인증, 무결성 보호, 네트워크 또는 전송 계층에서의 인증 및 암호화를 통해 보안 연결(예: 터널링)을 요구한다. 읽기 권한이 필요한 정보에 대해서는 기밀성이 보장되어야 한다.
(라) 설계

CBS는 다음을 만족해야 한다.

(a) 선내 연결 종단점으로부터 연결을 종료할 수 있는 기능을 가져야 한다. 어떠한 원격 접근은 선내 책임자가 명시적으로 수락할 때까지 가능하지 않아야 한다.

(b) OT 시스템의 안전한 기능 또는 OT 시스템에서 사용하는 데이터의 무결성 및 가용성을 훼손하지 않도록 원격 세션 중에 중단을 관리할 수 있어야 한다.

(c) (예를 들어, 사이버 사고의 탐지 후에) 원격 연결의 오프라인 검토를 위해 모든 원격 접근 사건을 기록하고 충분한 기간 동안 유지하는 로깅 기능을 제공해야 한다.

(마) 원격 유지보수에 대한 추가 요구사항

원격 접근이 유지보수에 이용되는 경우, 402.의 6항 (2)호 (라)에 추가하여 다음의 요구사항을 만족해야 한다.

(a) 육상 쪽과 어떻게 연결되고 통합되는지를 보여주는 문서가 제공되어야 한다.

(b) 보안 패치 및 소프트웨어 업데이트는 설치 전에 유효하고 허용될 수 없는 부작용이나 사이버 사건을 일으키지 않는지를 확인하기 위해 설치되기 전에 시험 및 평가되어야 한다. 원격 업데이트를 수행하기 전에 소프트웨어 공급자로부터 이에 대한 확인 보고서를 득해야 한다.

(c) 공급자는 보안 업데이트 계획을 선주의 이용이 가능하도록 제공해야 한다. (3장 502.의 2항, 3장 502.의 3항 및 3장 502.의 4항 참조)

(d) 언제든지 원격 유지 관리 활동 중에 권한이 있는 선원은 활동을 중단하고 관련된 CBS 및 시스템을 이전의 안전한 구성으로 되돌릴 수 있어야 한다.

(e) 다중요소 인증은 비신뢰 네트워크로부터 CBS에 대한 인간 사용자의 어떠한 접근에 대하여 요구된다.

(f) 설정 가능한 횟수의 실패한 원격 접근 시도 후에는, 미리 설정한 시간 동안 다른 시도가 차단되어야 한다.

(g) 원격 유지보수 장소에 대한 연결이 어떠한 이유로 중단된 경우, 시스템 접근은 자동 로그아웃 기능에 의해 종료되어야 한다.

(3) 근거

선내 CBS는 매우 다양한 규정상 기능을 수행하기 위해 점점 더 디지털화되고 인터넷에 연결되고 있다. 선내 CBS를 감시하고 제어하기 위한 디지털 시스템의 사용은 이들을 사이버 사고에 취약하게 만든다. 공격자는 인터넷 연결을 통해 선내 CBS에 접근을 시도할 수 있으며, CBS의 작동에 영향을 주는 변경사항을 만들거나 심지어는 CBS의 완전한 제어를 달성할 수도 있으며, 또는 선박의 CBS로부터 정보를 다운로드하는 것을 시도할 수 있다. 또한, 더 이상 지원되지 않고 구식 운영 체제에 의존하는 IT 및 OT 시스템의 사용은 사이버복원력에 영향을 미치므로, 이러한 시스템에 원격으로 접근할 수 있는 경우 충분한 수준의 사이버복원력을 유지하는 것을 돕기 위해 선내의 관련 하드웨어 및 소프트웨어 설치에 특별한 주의를 기울여야 하며, 또한 모든 사이버 사고가 고의적인 공격의 결과인 것은 아니라는 점을 염두에 두어야 한다.

(4) 등록검사

(가) 설계 단계

시스템 통합자는 사이버보안 설계 기술서에 다음의 정보를 포함해야 한다.

(a) 원격으로 접근될 수 있거나 보안 구역 경계를 통해 비신뢰 네트워크와 통신하는 적용 범위 내 CBS의 식별

(b) 각 CBS에 대하여, 적용 가능한 402.의 6항 (2)호의 요구사항 준수의 기술

(나) 건조 단계

시스템 통합자는 비신뢰 네트워크와의 어떤 통신이 이 절의 요건에 따라 오직 일시적으로만 활성화되어 사용되도록 보장해야 한다.

(다) 선내시험 단계

시스템 통합자는 선박 사이버복원력 시험절차서(202.의 2항 (2)호 참조)을 제출하고 다음을 우리 선급에 입증해야 한다.

(a) 비신뢰 네트워크와의 통신은 3장 402.에 따라 보호되며 통신 프로토콜은 부족한 보안 버전으로 타협될 수 없다. (예를 들어 네트워크 프로토콜 분석도구를 사용하여 입증)

(b) 원격 접근은 원격 사용자에 다중요소 인증을 요구한다.

(c) 실패한 로그인 시도의 제한하고, 세션이 성립되기 전에 원격 사용자에게 알림 메시지를 제공한다.

(d) 원격 연결은 선내 책임자에 의해 명시적으로 수락되어야 한다.

(e) 원격 세션은 선내 선원에 의해 수동으로 종료되거나 미활동 기간 이후 세션이 자동으로 종료된다.

(f) 원격 세션은 로그가 기록된다. (3장 401.의 13번 항목 참조)

(g) 지침 또는 절차서가 관련 장비 공급자에 의해 제공된다. (3장 301.의 3항 참조)

(5) 유지검사

(가) 일반사항

(a) 운항 단계에서 검사에 대한 일반 요구사항은 **203.**을 참조한다.

(b) 선주는 선박 사이버보안 및 복원력 프로그램상에서 비신뢰 네트워크와의 원격 접근 및 통신의 관리를 기술해야 하며, 최소한 이 장의 다음의 요구사항을 다루어야 한다.

(i) 사용자 매뉴얼 (**402.**의 **6**항 (2)호)

(ii) 역할 및 허가 (**402.**의 **6**항 (2)호)

(iii) 패치 및 업데이트 (**402.**의 **6**항 (2)호 (마))

(iv) 원격 소프트웨어 업데이트 수행 전의 확인 (**402.**의 **6**항 (2)호 (마))

(v) 중단, 중지, 롤백 (**402.**의 **6**항 (2)호 (마))

(나) 1번째 연차검사

선주는 선박 사이버보안 및 복원력 프로그램의 이행을 입증하는 기록 및 문서로 된 증거자료를 제시해야 하며, 즉 다음을 입증한다.

(a) 원격 접근 세션은 기록되거나 로그를 생성하고 있으며 관련 정책 및 사용자 매뉴얼에 따라 시행되고 있다.

(b) 보안 패치 및 기타 소프트웨어 업데이트 설치는 변경 관리 절차에 따라 그리고 공급자와 협력하여 수행되고 있다.

(다) 후속 연차 검사

선주는 선급의 요청 시 1번째 연차검사에서 명시된 것과 같이 기록 및 다른 문서로 된 증거자료를 제시함으로써 선박 사이버보안 및 복원력 프로그램의 이행을 입증해야 한다.

(라) 정기 검사

선주는 선박 사이버복원력 시험절차서에 따라 **402.**의 **6**항 (4)호 (다)의 활동을 우리 선급에 입증해야 한다.

7. 모바일 및 휴대용 장치의 사용

(1) 요구사항

CBS 내 모바일 및 휴대용 장치의 사용은 필요한 활동만으로 제한되어야 하며 **3**장 **401.**의 10번 항목에 따라 통제되어야 한다. 이 요구사항들을 완전히 만족할 수 없는 어떠한 CBS의 경우 인터페이스 포트는 물리적으로 차단되어야 한다.

(2) 세부 요구사항

모바일 및 휴대용 장치는 허가된 선원만 사용해야 한다. 오직 허가된 장치만 CBS에 연결할 수 있다. 이러한 장치들의 모든 사용은 CBS 내 멀웨어 유입 위험을 고려하여 모바일 및 휴대용 장치 사용에 대한 선주의 정책을 따라야 한다.

(3) 근거

CBS는 모바일 또는 휴대용 장치를 통한 멀웨어 감염으로 인해 손상될 수 있다는 것은 일반적으로 알려져 있다. 따라서 모바일 및 휴대용 장치의 연결은 신중하게 고려해야 한다. 또한 선박의 운항 및 유지보수에 사용이 요구되는 모바일 장비는 선주의 통제 하에 있어야 한다.

(4) 등록검사

(가) 설계 단계

시스템 통합자는 사이버보안 설계 기술서에 다음의 정보를 포함해야 한다.

(a) **3**장 **401.**의 10번 항목 요구사항을 만족하지 못하는 적용 범위에 있는 어떠한 CBS, 즉, 포트 블록커와 같은 물리적 수단에 의해 인터페이스 포트의 보호 수단을 갖추어야 한다.

(나) 건조 단계

시스템 통합자는 CBS 내 물리적 인터페이스 포트의 사용이 **3**장 **401.**의 10번 항목에 따라 통제되며, 이러한 장치의 어떠한 사용은 CBS 내 멀웨어가 유입되는 것을 방지하기 위한 절차를 따르도록 보장해야 한다.

(다) 선내시험 단계

시스템 통합자는 선박 사이버복원력 시험절차서(**202.**의 **2**항 (2)호 참조)를 제출해야 하며, 모바일 및 휴대용 장치의 사용을 통제하는 기능들이 올바르게 구현되었는지를 우리 선급에 입증해야 한다. 관련하여 다음의 대응 조치들이 입증되어야 한다.

(a) 모바일 및 휴대용 기기의 사용은 허가된 사용자로 제한한다.

(b) 인터페이스 포트는 특정 장치 형식에서만 사용할 수 있다.

(c) 이러한 장치로부터 시스템으로 파일이 전송될 수 없다.

(d) 이러한 장치의 파일은 (자동실행 비활성화에 의해) 자동으로 실행되지 않는다.
(e) 네트워크 접근은 특정 MAC 또는 IP 주소로 제한한다.
(f) 미사용 인터페이스 포트는 비활성화된다.
(g) 미사용 인터페이스 포트는 물리적으로 차단한다.

(5) 유지검사

(가) 일반

(a) 운항 단계에서 검사에 대한 일반 요구사항은 **203.**을 참조한다.
(b) 선주는 선박 사이버보안 및 복원력 프로그램상 모바일 및 휴대용 장치의 관리를 기술해야 하며, 이 장의 최소한 다음의 요구사항을 다루어야 한다.
(i) 정책 및 절차서 (**402.**의 **4**항 (2)호 (라))
(ii) 인터페이스 포트의 물리적 차단 (**402.**의 **7**항 (1)호)
(iii) 허가된 ~~선원~~에 의한 사용 (**402.**의 **7**항 (2)호)
(iv) 허가된 장치에만 연결 (**402.**의 **7**항 (2)호)
(v) 멀웨어 유입의 위험을 고려 (**402.**의 **7**항 (2)호)

(나) 1번째 연차검사

선주는 선박 사이버보안 및 복원력 프로그램의 준수를 입증하는 기록 또는 다른 문서로 된 증거자료를 우리 선급에 제시해야 한다. 즉 다음을 입증한다.
(a) 모바일, 휴대식 또는 이동식 매체의 사용은 허가된 ~~선원~~으로 제한하고 관련 정책과 절차서를 따른다.
(b) 오직 허가된 장치만 CBS에 연결한다.
(c) 물리적 인터페이스 포트의 사용을 제한하는 수단이 승인된 설계 문서에 따라 구현한다.

(다) 후속 연차 검사

선주는 우리 선급의 요청 시 1번째 연차검사에서 명시된 것과 같이 기록 및 다른 문서로 된 증거자료를 제시함으로써 선박 사이버보안 및 복원력 프로그램의 이행을 입증해야 한다.

(라) 정기 검사

선주는 선박 사이버복원력 시험절차서에 따라 **402.**의 **7**항 (4)호 (다)의 활동을 우리 선급에 입증해야 한다.

403. 탐지

1. 네트워크 운영 감시

(1) 요구사항

이 장의 적용 범위에 있는 네트워크는 지속적으로 감시되어야 하며, 오작동 또는 용량 감소/저하가 발생하면 경보를 발해야 한다.

(2) 세부 요구사항

(가) 네트워크를 감시하기 위한 조치는 다음 기능들을 포함해야 한다.
(a) 과도한 트래픽에 대한 감시 및 보호
(b) 네트워크 연결 감시
(c) 기기 관리 활동 감시 및 기록
(d) 무단 장치의 연결에 대한 보호
(e) 네트워크 대역폭의 사용이 공급자에서 비정상인 것으로 지정한 한계점을 초과하는 경우 경보 발생 (**선급 및 강선규칙 6편 2장 407.** 참조)

(나) 다음에 적합한 경우, 침입 탐지 시스템(IDS)이 구현될 수 있다.
(a) IDS는 관련 CBS의 공급자에 의해 검증되어야 한다.
(b) IDS는 수동적이어야 하며 CBS의 성능에 영향을 줄 수 있는 보호 기능을 활성화하지 않아야 한다.
(c) 관련 선원은 IDS 사용에 대한 교육을 받고 자격을 갖추어야 한다.

(3) 근거

사이버 공격은 점점 더 정교해지고 있으며 건조 당시에 알려지지 않은 취약점을 표적으로 하는 공격은 선박이 위협에 대비하지 못한 경우 사고로 이어질 수 있다. 이러한 알려지지 않은 취약점을 표적으로 하는 공격에 조기 대응하기 위해서는 비정상적인 사건을 감지할 수 있는 기술이 필요하다. 네트워크 내 이상 징후를 탐지하고 사후 분석을 사용할 수 있는 감시 시스템은 사이버 사고에 적절하게 대응하고 추가로 복구하는 능력을 제공한다.

(4) 등록검사

(가) 설계 단계

요구사항 없음

(나) 건조 단계

요구사항 없음

(다) 선내시험 단계

(a) 시스템 통합자는 선박 사이버복원력 시험절차서에 명시해야 하며, CBS의 네트워크 감시 및 보호 메커니즘을 우리 선급에 입증해야 한다.

(i) 연결이 끊긴 네트워크 연결은 경보를 발하고 사건이 기록되는지를 시험한다.

(ii) 비정상적으로 높은 네트워크 트래픽이 탐지되면 경보 및 감사 기록이 생성되는지 시험한다. 이 시험은 **404.**의 4항 (2)호의 시험과 함께 수행할 수 있다.

(iii) CBS가 유니캐스트 및 브로드캐스트 메시지를 모두 고려하여, 네트워크 스톰(network storm) 시나리오에 안전한 방식으로 대응하는 지를 입증한다. (**402.**의 2항 (2)호 (다) 참조).

(iv) 감사 기록의 생성을 입증한다. (보안 관련 사건의 로깅)

(v) 침입 탐지 시스템이 구현된 경우, 이것이 수동적이며 CBS의 의도된 작동에 영향을 줄 수 있는 보호 기능을 활성화하지 않음을 입증한다.

(b) 상기 시험은 **202.**의 2항 (2)호에 따라 CBS의 인증 중에 실시된 경우 생략할 수 있다.

(c) 적용 범위에 있는 CBS에 구현되는 침입 탐지 시스템은 선급의 검증을 받아야 한다. 관련 문서가 승인용으로 제출되어야 하며, 검사/시험이 선내에서 실시되어야 한다.

(5) 유지검사

(가) 일반

(a) 운항 단계에서 검사에 대한 일반 요구사항은 **203.**을 참조한다.

(b) 선주는 선박 사이버보안 및 복원력 프로그램상에서 CBS와 네트워크의 이상징후를 탐지하기 위한 관리 활동을 기술해야 하며, 이 장의 최소한 다음의 요구사항을 다루어야 한다.

(i) 이상 활동을 표시와 인식 (**403.**)

(ii) 보안 감사 기록의 검사 (**403.**의 1항 (2)호)

(iii) 사고 탐지를 위한 지침과 절차 (**404.**의 1항 (1)호)

(c) 상기 활동은 **404.**의 1항의 사고 대응과 함께 다루어질 수 있다.

(나) 1번째 연차검사

선주는 선박 사이버보안 및 복원력 프로그램의 이행을 입증하는 기록 및 다른 문서로 된 증거를 우리 선급에 제시해야 한다. 즉 다음을 입증한다.

(a) CBS는 보안 감사 기록 점검과 CBS 경보를 조사함으로써 이상징후가 일상적으로 감시된다.

(다) 후속 연차검사

선주는 선급의 요청 시 1번째 연차검사에서 명시된 것과 같이 기록 및 다른 문서로 된 증거자료를 제시함으로써 선박 사이버보안 및 복원력 프로그램의 이행을 입증해야 한다.

(라) 정기 검사

CBS에 변경이 있는 경우, 선주는 선박 사이버복원력 시험절차서에 따라 **403.**의 1항 (4)호 (다)의 활동을 우리 선급에 입증해야 한다.

2. CBS 및 네트워크의 검증 및 진단 기능

(1) 요구사항

CBS와 네트워크는 이 장에서 요구되는 보안 기능의 성능과 기능성을 확인할 수 있어야 한다. 진단 기능은 의도된 사용자의 사용을 위한 CBS 무결성 및 상태에 대한 충분한 정보와 선박의 안전한 운항을 위해 이들의 기능성을 유지하기 위한 수단을 제공해야 한다.

(2) 세부 요구사항

CBS 및 네트워크의 진단 기능은 선박의 시험 및 유지보수 시 모든 요구되는 보안 기능의 의도된 작동을 검증하는 것이 가능해야 한다.

(3) 근거

보안 기능의 의도된 작동을 검증하는 능력은 선박의 수명 동안 사이버복원력 관리를 지원하는 데 중요하다. 진단 기능을 위한 도구는 각 장치의 자가 진단 기능과 같은 자동 또는 수동 기능 또는 (ping, traceroute, ipconfig, netstat, nslookup, wireshark, nmap 등과 같은) 네트워크 감시 도구로 구성될 수 있다. 그러나 진단 기능의 실

행은 때때로 CBS의 작동 성능에 영향을 줄 수 있다는 점에 유의해야 한다.

(4) 등록검사

(가) 설계 단계

요구사항 없음

(나) 건조 단계

요구사항 없음

(다) 선내시험 단계

(a) 시스템 통합자는 선박 사이버복원력 시험절차서(202.의 2항 (2)호 참조)를 제출하고, 제공업체가 제공하는 보안 기능의 검증을 위한 절차의 효과성을 우리 선급에 입증해야 한다.

(b) 상기 시험은 202.의 2항 (2)호에 따라 CBS의 인증 중에 실시된 경우 생략할 수 있다.

(5) 유지검사

(가) 일반

(a) 운항 단계에서 검사에 대한 일반 요구사항은 203.을 참조한다.

(b) 선주는 선박 사이버보안 및 복원력 프로그램상에서 CBS와 네트워크의 보안 기능의 올바른 작동을 검증하기 위한 관리 활동을 기술해야 하며, 이 장의 최소한 다음의 요구사항을 다루어야 한다.

(i) 시험 및 유지보수 기간 (403.의 2항 (2))

(ii) 주기적 유지보수 (203.의 3항)

(나) 1번째 연차검사

선주는 선박 사이버보안 및 복원력 프로그램의 준수를 입증하는 기록 또는 다른 문서로 된 증거자료를 우리 선급에 제시해야 한다. 즉 다음을 입증한다.

(a) CBS의 보안 기능은 주기적으로 시험되거나 검증된다.

(다) 후속 연차검사

선주는 선급의 요청 시 1번째 연차검사에서 명시된 것과 같이 기록 및 다른 문서로 된 증거자료를 제시함으로써 선박 사이버보안 및 복원력 프로그램의 이행을 입증해야 한다.

404. 대응

1. 사고 대응 계획 (Incident response plan)

(1) 요구사항

관련 비상상황을 커버하고 사이버보안 사고에 대응하는 방법을 명시한 사고 대응 계획이 선주에 의해 개발되어야 한다. 사고 대응 계획은 CBS에 대한 사고를 탐지, 대응 및 영향을 제한하기 위해 미리 지정된 지침 및 절차 문서들를 포함해야 한다.

(2) 세부 요구사항

(가) 선박의 설계 및 건조 단계에서 관계되는 다양한 이해관계자들은 1번째 연차검사에서 본선에 비치되는 사고 대응 계획을 준비하기 위해 선주에게 정보를 제공해야 한다. 사고 대응 계획은 선박의 운항 수명 동안 (예를 들어 유지보수 시) 최신으로 유지되어야 한다.

(나) 사고 대응 계획은 네트워크상 탐지된 사이버 사고에 대해 적절한 관할 당국에 통보하고 사고의 필요한 증거자료를 보고하며 시기적절한 시정조치를 취함으로써 대응하고, 사이버 사고 영향을 사고가 난 네트워크 세그먼트로 한정하기 위한 절차를 제공해야 한다.

(다) 사고 대응 계획에는 최소한 다음 정보를 포함해야 한다.

(a) 침해된 시스템의 격리를 위한 중단점(Breakpoint)

(b) 탐지된 진행 중인 사이버 사건을 알리는 경보 및 표시 또는 사이버 사건으로 야기된 이상 증상의 기술

(c) 사이버 사고와 관련된 예상되는 주요 결과의 기술

(d) 만약 있는 경우, 비상 정지, 독립 또는 로컬 제어에 의존하지 않는 우선적인 대응 옵션

(e) 적용이 가능한 경우, 사이버 사고로 인해 고장이 난 시스템으로부터 독립적으로 운전하기 위한 독립의 로컬 제어 정보

(라) 사고 대응 계획은 전자기기의 완전 상실 시에도 이용이 가능한 인쇄물로 비치되어야 한다.

(3) 근거

사고 대응 계획은 책임자가 사이버 사고에 대응할 수 있도록 돕기 위한 수단이다. 이러한 사고 대응 계획은 단순하여 효과적이고 신중하게 설계된다. 사고 대응 계획을 개발할 때 사이버 사고의 중대성을 이해하고 이에 따른 대응

행동의 우선순위를 지정하는 것이 중요하다.

선박의 안전 운항을 위한 기능성 및 서비스 수준을 가능한 한 유지하기 위한 수단(예를 들어 실행을 이중화 장치로 전환)이 표기되어야 한다. 육상 직원은 사이버 사고 발생 시 선박과 통합되어야 한다.

(4) 등록검사

(가) 설계 단계

시스템 통합자는 사이버보안 설계 기술서에 다음의 정보를 포함해야 한다.

(a) 사고 대응 계획을 수립하기 위해 선주에 의해 적용될 수 있는 공급자가 제공한 정보(**3장 301.**의 8항 참조)에 대한 참조.

(나) 건조 단계

요구사항 없음

(다) 선내시험 단계

요구사항 없음

(5) 유지검사

(가) 일반

(a) 운항 단계에서 검사에 대한 일반 요구사항은 **203.**을 참조한다.

(b) 선주는 선박 사이버보안 및 복원력 프로그램상에서 사고 대응 계획을 기술해야 한다. 계획은 CBS를 포함해야 하며 이 장의 최소 다음의 요구사항을 다루어야 한다.

(i) **404.**의 1항의 요구사항에 따른 사이버 사고에 누가, 언제 및 어떻게 대응할지에 대한 기술

(ii) **404.**의 2항의 요구사항에 따른 로컬/수동 제어에 대한 절차 또는 지침

(iii) **404.**의 3항의 요구사항에 따른 보안 구역의 격리를 위한 절차 또는 지침

(iv) **404.**의 4항의 요구사항에 따른 사이버 사고 시에 CBS의 예상 행동의 기술

(나) 1번째 연차검사

선주는 선박 사이버보안 및 복원력 프로그램의 이행을 입증하는 기록 및 다른 문서로 된 증거자료를 우리 선급에 제시해야 한다. 즉 다음을 입증해야 한다.

(a) 사고 대응 계획은 선내 책임자의 이용이 가능하다.

(b) 로컬/수동 제어를 위한 절차 또는 지침은 선내 책임자의 이용이 가능하다.

(c) 보안구역의 분리/격리를 위한 절차 또는 지침은 선내 책임자의 이용이 가능하다.

(d) 어떠한 사이버 사고는 사고 대응 계획에 따라 대응되고 있다.

(다) 후속 연차검사

선주는 선급의 요청 시 1번째 연차검사에서 명시된 것과 같이 기록 및 다른 문서로 된 증거자료를 제시하여 선박 사이버보안 및 복원력 프로그램의 이행을 입증해야 한다.

2. 로컬, 독립 및/또는 수동 운전

(1) 요구사항

선급 및 강선규칙 6편 2장 201.의 4항에서 요구하는 로컬 백업 제어에 필요한 어떤 CBS는 주제어 시스템과 독립되어야 한다. 이는 효과적인 로컬 작동을 위한 휴먼 머신 인터페이스(HMI)를 포함한다.

(2) 세부 요구사항

(가) 로컬 제어 및 감시를 위한 CBS는 독립적(self-contained)이여야 하며, 의도된 작동을 위해 다른 CBS와의 통신에 의존하지 않아야 한다.

(나) 원격 제어 시스템 또는 다른 CBS에 대한 통신이 네트워크에 의해 연결되는 경우, **402.**의 1항 및 **402.**의 2항에 기술된 것과 같이 분할 및 보호 안전장치가 구현되어야 한다. 이는 로컬 제어 및 감시 시스템이 별도의 보안 구역으로 간주되어야 함을 의미한다. 상기에도 불구하고 사례 별로 다른 개념을 가진 CBS에 특별한 고려가 필요할 수 있다.

(다) 로컬 제어 및 감시를 위한 CBS는 이 장의 요구사항을 준수해야 한다.

(3) 근거

안전한 운항을 유지하는 데 필요한 기관 및 장치의 독립적인 로컬 제어는 유인 선박에 대한 기본 원칙이다. 이 요구사항의 목적은 전통적으로 선원이 기관 근처에서 수동 운전을 실행함으로써 고장 및 다른 사고에 대처할 수 있도록 하는 것이다. 악의적인 사이버 사고 역시 고려되어야 하므로, 독립적 로컬 제어 원칙 또한 중요하다.

(4) 등록검사

(가) 설계 단계

시스템 통합자는 사이버보안 설계 기술서 상에 다음의 정보를 포함해야 한다.

(a) 연결된 원격 또는 자동 제어 시스템 내의 사이버 사고로부터 **선급 및 강선규칙 6편 2장 201.**의 4항에 명시된 로컬 제어가 보호되는 방법에 대한 기술.

(나) 건조 단계

요구사항 없음

(다) 선내시험 단계

(a) 시스템 통합자는 우리 선급에 선박 사이버복원력 시험절차서를 제출하고 선박의 안전에 필요하고 이 장의 적용 범위 내에서 요구하는 로컬 제어가 원격 또는 자동 제어 시스템으로부터 독립적으로 작동될 수 있음을 입증해야 한다.

(b) 시험은 로컬 제어시스템으로부터 다른 시스템/장치들에 대한 모든 네트워크의 연결을 해제하여 실시한다.

(c) 상기 시험은 **202.**의 2항 (2)호에 따른 CBS의 인증 중에 실시된다면 생략할 수 있다.

(5) 유지검사

운항 단계에서 검사에 대한 일반 요구사항은 **203.**을 참조한다.

(가) 정기검사

CBS에 변경이 있는 경우, 선주는 선박 사이버복원력 시험절차서에 따라 **404.**의 2항 (4)호 (다)의 활동을 우리 선급에 입증해야 한다.

3. 네트워크 격리 (Network isolation)

(1) 요구사항

보안구역과의 네트워크 기반 통신을 종료하는 것이 가능해야 한다.

(2) 세부 요구사항

(가) 사고 대응 계획에서 이행해야 할 조치로서 네트워크 격리를 가리키는 경우, (예를 들어, 네트워크 장치의 물리적 ON/OFF 스위치를 조작하거나 라우터/방화벽에 연결된 케이블을 분리하는 것과 같은 유사한 조치와 같이) 표시된 절차에 따라 보안 구역을 격리할 수 있어야 한다.

(나) 선원이 효과적인 방식으로 네트워크를 격리하는 것을 허용하도록 장치에 대한 이용 가능한 지침과 분명한 표시(marking)가 있어야 한다.

(다) 안전을 포함하여 기능 및 올바른 작동에 영향을 미칠 수 있는 개별 시스템의 데이터 의존성이 식별되어야 하며, 비상 상황 시 격리되는 경우 시스템이 데이터 또는 기능 입력에 대한 보상을 받아야 하는 위치를 명확하게 보여주어야 한다.

(3) 근거

보안 침해 사고가 발생하여 탐지된 경우 사고 대응 계획에 사고의 추가 전파 및 영향을 예방하기 위한 조치들이 포함될 수 있다. 이러한 조치들은 네트워크 세그먼트와 필수 기능을 지원하는 시스템을 격리하는 것일 수 있다.

(4) 등록검사

(가) 설계 단계

시스템 통합자는 사이버보안 설계 기술서에 다음의 정보를 포함해야 한다.

(a) 다른 구역 또는 네트워크로부터 각 보안 구역을 격리하는 방법의 설명서. 이러한 격리의 영향이 기술되어야 하며, 보안 구역 내 CBS가 다른 구역이나 네트워크로부터 IP 네트워크로 전송되는 데이터에 의존하지 않음을 입증해야 한다.

(나) 건조 단계

요구사항 없음

(다) 선내시험 단계

(a) 시스템 통합자는 선박 사이버복원력 시험절차서(**202.**의 2항 (2)호 참조)를 제출하고 보안 구역 경계를 횡단하는 모든 네트워크 연결을 끊음으로써 보안 구역 내 CBS가 다른 보안 구역 또는 네트워크와 네트워크 통신 없이도 충분한 운영상 기능성을 유지함을 우리 선급에 입증해야 한다.

(b) 상기 시험은 **202.**의 2항 (2)호에 따라 CBS의 인증 중에 실시되는 경우 생략할 수 있다.

(5) 유지검사

운항 단계에서 검사에 대한 일반 요구사항은 **203.**을 참조한다.

(가) 정기검사

CBS에 변경이 있는 경우, 선주는 선박 사이버복원력 시험절차서에 따라 **404.**의 3항 (4)호 (다)의 활동을 우리 선급에 입증해야 한다.

4. 최소 위험 상태로의 대비책(fallback)

(1) 요구사항

의도된 서비스를 제공하기 위해 CBS 또는 네트워크의 능력을 손상시키는 사이버 사고의 경우, 영향을 받는 시스템 또는 네트워크는 최소 위험 상태로 되돌릴 수 있어야 한다. (즉, 발생이 가능한 안전 문제의 위험을 줄이기 위해 안정되고 정지된 상태로 만드는 것)

(2) 세부 요구사항

(가) 요구되는 것과 같이 의도된 서비스를 제공하는 시스템의 능력을 손상시키며, CBS 또는 네트워크에 영향을 미치는 사이버 사고가 탐지되는 즉시, 시스템은 합리적으로 안전한 상태가 달성될 수 있는 상태로 되돌아 가야 한다. 대비책 조치는 다음을 포함할 수 있다.

(a) 시스템을 완전 정지 또는 다른 안전 상태로 이르게 함;

(b) 시스템 해제;

(c) 제어권을 다른 시스템 또는 인간 운전자에게 이전;

(d) 기타 보상 대책들.

(나) 최소 위험 상태로의 대비책은 선박을 안전한 상태로 유지하기 위해 충분한 기간(time frame) 내에 조치 되어야 한다.

(다) 최소 위험 상태로 되돌아갈 수 있는 시스템의 능력은 공급자와 시스템 통합자의 설계 단계부터 고려되어야 한다.

(3) 근거

예상치 못한 또는 관리할 수 없는 고장 또는 이벤트의 경우 도달할 하나 이상의 최소 위험 조건으로 되돌아가기 위한 CBS 및 통합 시스템의 능력은 시스템을 일관되고 알려진 안전한 상태로 유지하기 위한 안전 조치이다.

최소 위험 조건으로의 대비책은 일반적으로 현재의 작동을 중단하고 도움이 필요하다는 신호를 알리는 시스템의 능력을 의미하며, 환경 조건, 선박의 항해 단계(예: 항구 출발/도착 대 공해 통과) 및 발생된 사건에 따라 다를 수 있다.

(4) 등록검사

(가) 설계 단계

시스템 통합자는 사이버보안 설계 기술서 상에 다음의 정보를 포함해야 한다.

(a) CBS의 제어 기능에 대한 안전 상태 설명서

(나) 건조 단계

요구사항 없음

(다) 선내시험 단계

(a) 시스템 통합자는 선박 사이버복원력 시험절차서(**202.**의 **2**항 (2)호 참조)를 제출하고 예를 들어, 필수 서비스에 대한 출력을 유지하고 운전자가 대체 수단으로 제어 및 감시 기능을 수행하는 것이 가능하게하는 것과 같이 지침의 적용 범위에 있는 CBS가 사이버 사고에 (**404.**의 **4**항 (4)호 (가)에 따른) 안전한 방식으로 대응함을 우리 선급에 입증해야 한다.

(b) 시험은 최소한 서비스 거부(DoS) 공격을 포함해야 하며 **403.**의 **1**항 (4)호 (다)에 관련된 시험과 함께 실시할 수 있다.

(c) 상기 시험은 **202.**의 **2**항 (2)에 따른 CBS의 인증 중에 실시될 경우 생략할 수 있다.

(5) 유지검사

운항 단계에서 검사에 대한 일반 요구사항은 **203.**을 참조한다.

(가) 정기 검사

CBS에 변경이 있는 경우, 선주는 선박 사이버복원력 시험절차서에 따라 **404.**의 **4**항 (4)호 (다)의 활동을 우리 선급에 입증해야 한다.

405. 복구

1. 복구 계획

(1) 요구사항

사이버 사고로 인한 중단 또는 고장이 발생한 이후 CBS를 작동 상태로 복구하는 것을 지원하기 위한 복구 계획이 선주에 의해 수립되어야 한다. 어디에서 누구에게 지원을 받을 수 있는지에 대한 세부 내용이 복구 계획의 일부로서 포함되어야 한다.

(2) 세부 요구사항

(가) 선박의 설계 및 건조 단계에서 관련된 다양한 이해관계자는 1번째 연차검사에서 본선에 비치될 복구 계획의 준비를 위한 정보를 선주에게 제공해야 한다. 복구 계획은 선박의 운항 수명 동안 (예를 들어, 유지보수 시) 최신으로 유지되어야 한다.

(나) 복구 계획은 선원과 외부 직원이 쉽게 이해할 수 있으며, 실패한 시스템의 복구를 보장하기 위한 필수 지침과 절차, 그리고 육상 지원이 필요한 경우 외부 지원을 받는 방법을 포함해야 한다. 게다가, 선내에서 복구에 필수적인 소프트웨어 복구 매체 또는 도구를 이용할 수 있어야 한다.

(다) 복구 계획을 개발할 때 관련된 다양한 시스템과 부시스템들이 명시되어야 한다. 또한, 다음의 복구 목표가 명시되어야 한다.

(a) 시스템 복구: 통신 기능을 복구하는 방법 및 절차는 복구 시간 목표(RTO: Recovery Time Objective) 측면에서 명시되어야 한다. 이는 필요한 통신 링크 및 처리 기능을 복구하는 데 필요한 시간으로 정의된다.

(b) 데이터 복구: OT 시스템의 안전한 상태 및 안전한 선박 운항을 회복하기 위해 필요한 데이터 복구 방법 및 절차는 복구 시점 목표(RPO: Recovery Point Objective) 측면에서 명시되어야 한다. 이것은 데이터 부재를 용인할 수 있는 가장 긴 기간으로 정의된다.

(라) 일단 복구 목표가 정의되면, 잠재적인 사이버 사고 목록이 생성되고, 복구 절차를 개발되고 기술된다. 복구 계획은 다음 정보를 포함하거나 참조해야 한다.

(a) 이중화, 독립 또는 로컬 운전을 통해 운전의 중단 없이 실패한 시스템을 복원하기 위한 지침 및 절차

(b) 정보의 백업 및 안전한 저장을 위한 프로세스 및 절차

(c) 완전한 최신의 논리적 네트워크 다이어그램

(d) 실패한 시스템의 복구를 위한 담당 선원 목록

(e) 시스템 지원 업체, 네트워크 관리자 등을 포함하여 외부 기술 지원을 위해 연락하기 위한 통신 절차 및 직원 목록

(f) 모든 구성요소에 대한 현재의 구성 정보

(마) 선박의 운항 및 항해는 선내 선원의 안전을 보장하기 위해 계획 내에서 우선시되어야 한다.

(바) 선내 및 육상의 인쇄물로 된 복구 계획은 사이버보안 담당 선원과 사이버 사고 지원 임무를 맡은 직원이 이용할 수 있어야 한다.

(3) 근거

사고 대응 절차는 시스템 복구의 필수적인 부분이다. 담당 선원은 (드라이브 지우기와 같은) 복구 작업의 영향을 조심스럽게 고려하고 숙지하여 신중하게 실행해야 한다. 그러나, 일부 복구 작업은 사고 원인에 대한 귀중한 정보를 제공할 수도 있는 증거의 파괴를 야기할 수도 있음에 유의해야 한다.

적절한 경우, 운항 능력을 복구하면서 증거 보존을 지원하기 위해 외부의 사이버 사고 대응 지원을 받아야 한다.

(4) 등록검사

(가) 설계 단계

시스템 통합자는 사이버보안 설계 기술서 상에 다음의 정보를 포함해야 한다.

(a) 사이버 사고로부터 복구하기 위한 계획을 수립하기 위해 선주에 의해 적용될 수 있는 공급자가 제공한 정보 (3장 301.의 8항 참조)에 대한 참조.

(나) 건조 단계

요구사항 없음

(다) 선내시험 단계

(a) 시스템 통합자는 선박 사이버복원력 시험절차서(202.의 2항 (2)호 참조)를 제출하고 405.의 2항 및 405.의 3항에 명시된 것과 같이 사이버 사고에 대응하기 위해 공급자가 제공한 절차와 지침의 유효성을 우리 선급에 입증해야 한다.

(b) 상기 시험은 202.의 2항 (2)에 따라 CBS의 인증 중에 실시되는 경우 생략될 수 있다.

(5) 유지검사

(가) 일반

(a) 운항 단계에서 검사에 대한 일반 요구사항은 203.을 참조한다.

(b) 선주는 선박 사이버보안 및 복원력 프로그램에서 사고 복구 계획을 기술해야 한다. 계획은 지침의 적용 범위에 있는 CBS들을 포함해야 하며, 이 장 내 최소한 다음의 요구사항을 다루어야 한다.

(i) 405.의 1항의 요구사항에 따라 사이버 사고로부터 복원 및 복구를 누가, 언제 및 어떻게 하는지에 대한 기

술

(ii) 405.의 2항의 요건에 따라서 수용가능한 고장시간, 제어를 위한 대체 수단의 가용성, 공급자 지원 합의, CBS의 중요성를 고려한 백업의 빈도, 유지보수 및 시험을 다루는 백업 정책

(iii) 405.의 2항 및 405.의 3항의 요구사항에 따라 CBS의 백업, 종료, 재설정, 복원 및 재시작에 대한 사용자 매뉴얼 또는 절차에 대한 참조

(나) 1번째 연차검사

선주는 선박 사이버보안 및 복원력 프로그램의 이행을 입증하는 기록 또는 다른 문서로 된 증거자료를 우리 선급에 제시해야 한다.

(a) 사고 복구에 대한 지침 및/또는 절차는 선내에서 담당 선원의 이용이 가능해야 한다.

(b) 복구에 필요한 장비, 도구, 문서 및/또는 필요한 소프트웨어 및 데이터는 선내에서 담당 선원의 이용이 가능해야 한다.

(c) CBS의 백업은 정책 및 절차에 따라 진행되어야 한다.

(d) 종료, 재설정, 복원 및 재시작에 대한 매뉴얼 및 절차는 선내에서 담당 선원의 이용이 가능해야 한다.

(다) 후속 연차검사

선주는 우리 선급의 요청 시 1번째 연차검사에서 명시된 것과 같이 기록 및 문서로 된 증거자료를 제시하여 선박 사이버보안 및 복원력 프로그램의 이행을 입증해야 한다.

2. 백업 및 복구 기능

(1) 요구사항

CBS 및 네트워크는 시기적절하며 완전하고 안전한 방식으로 백업 및 복구를 지원하는 기능을 가져야 한다. 백업은 정기적으로 유지관리되고 시험해야 한다.

(2) 세부 요구사항

(가) 복구 기능

(a) CBS는 사이버 사고 후에 선박이 안전하게 항해 및 운항 상태를 회복할 수 있도록 백업 및 복구 기능을 가져야 한다.

(b) 데이터는 안전한 사본 또는 이미지로부터 복구할 수 있어야 한다.

(c) 정보 및 백업 설비는 사이버 사고로부터 복구하는데 충분해야 한다.

(나) 백업

(a) CBS 및 네트워크는 데이터 백업을 제공해야 한다. 오프라인 백업의 사용은 온라인 백업 기기에 영향을 주는 랜섬웨어 및 웜바이러스에 대한 내성을 개선하기 위해 고려되어야 한다.

(b) 백업 계획은 범위, 모드 및 빈도, 저장 매체 및 보존 기간을 포함하도록 개발되어야 한다.

(3) 근거

일반적으로 백업 및 복구 전략의 목적은 데이터 손실을 보호하고 데이터 손실 후 데이터베이스를 재구성해야 한다. 일반적으로, 백업 관리 작업에는 다음이 포함한다.

(가) 다양한 종류의 고장에 대한 대응 방안을 계획하고 시험

(나) 백업 및 복구를 위한 데이터베이스 환경 구성

(다) 백업 일정 설정

(라) 백업 및 복구 환경 감시

(마) 장기 저장을 위한 데이터베이스 복사본 생성

(바) 데이터베이스 또는 호스트에서 다른 곳으로 데이터 이동 등

(4) 등록검사

(가) 설계 단계

요구사항 없음

(나) 건조 단계

요구사항 없음

(다) 선내시험 단계

(a) 시스템 통합자는 선박 사이버복원력 시험절차서(202.의 2항 (2)호 참조)를 제출하고 CBS의 제공업체가 제공하는 백업 및 복구에 대한 절차 및 지침을 우리 선급에 입증해야 한다.

(b) 상기 시험은 202.의 2항 (2)호에 따라 CBS의 인증 중에 실시된 경우 생략할 수 있다.

(5) 유지검사

운항 단계에서 검사에 대한 일반 요구사항은 **203.**을 참조한다.

(가) 정기 검사

CBS에 변경이 있는 경우, 선주는 선박 사이버복원력 시험절차서에 따라 **405.**의 **2**항 (4)호 (다)의 활동을 우리 선급에 입증해야 한다.

3. 제어된 셧다운, 재설정, 롤백 및 재시작 (Controlled shutdown, reset, roll-back and restart)

(1) 요구사항

(가) CBS 및 네트워크는 사이버 사고로 인해 가능한 손상으로부터 신속하고 안전한 복구가 가능하도록 제어된 셧다운, 초기 상태로 재설정, 안전한 상태로 롤백 및 전원이 꺼진 상태에서 재시작할 수 있어야 한다.

(나) 상기 언급된 작업을 실행하는 방법에 대한 적절한 문서는 선내 선원이 이용할 수 있어야 한다.

(2) 세부 요구사항

(가) CBS 및 네트워크는 다음의 기능을 갖추어야 한다.

(a) 전체 통합 시스템을 안전하고 일관적이며 알려진 상태로 유지할 수 있도록 다른 연결된 시스템이 보류 중인 트랜잭션을 위임(commit)/롤백, 프로세스 종료, 연결 끊기 등을 허용하는 제어된 종료(Controlled shutdown)

(b) 시스템을 종료 프로세스를 거쳐 메모리를 지우고 장치를 초기화 상태로 재설정하도록 지시하는 자체 재설정

(c) 시스템 무결성 및 일관성을 회복하기 위해 이전 구성 및/또는 상태로 롤백

(d) 읽기 전용 소스로부터 (예를 들어, 롤백 작업 후) 모든 소프트웨어 및 데이터의 새로운 이미지를 재시작 및 다시 로드. 재시작 시간은 시스템의 의도된 서비스와 호환되어야 하며 다른 연결된 시스템 또는 이 시스템이 속한 통합 시스템을 일관성이 없거나 안전하지 않은 상태를 야기하지 않아야 한다.

(나) 사이버 사고의 영향을 받는 시스템의 경우 위에서 언급한 작업을 실행하는 방법에 대한 문서는 선원의 이용이 가능해야 한다.

(3) 근거

제어된 셧다운은 다른 연결된 시스템들이 전체 통합 시스템을 안전하고 알려진 상태로 유지하도록 보류 중인 트랜잭션을 커밋/롤백, 프로세스 종료, 연결 끊기 등을 허용하는 소프트웨어 기능에 의해 CBS 또는 네트워크를 끄는 것으로 구성된다. 제어된 셧다운은 예를 들어 전원 중단으로 인해 컴퓨터가 강제 종료되어 발생하는 하드 셧다운과는 반대되는 것이다.

일부 사이버 사고의 경우 하드 셧다운이 안전 예방 조치로 간주될 수 있지만 통합 시스템의 경우 예측 가능한 동작으로 일관되고 알려진 상태를 유지하기 위해 제어된 셧다운이 선호된다. 표준 셧다운 절차가 이행되지 않을 때, 데이터 또는 프로그램 및 운영 체제 파일 손상이 발생할 수 있다. OT 시스템의 경우, 손상의 결과로써 불안전, 부정확한 작동 또는 의도한 서비스 제공 실패가 발생할 수 있다.

재설정 작업은 전형적으로 소프트 부팅을 시작하여 시스템에 종료 프로세스 진행하도록 지시하고, 메모리를 지우고 장치를 초기화 상태로 재설정하도록 명령한다. 해당 시스템에 따라 재설정 작업은 다른 영향을 가질 수 있다.

롤백은 시스템을 이전 상태로 되돌리는 작업이다. 롤백은 잘못된 작업이 수행된 후에도 시스템 데이터와 프로그램을 깨끗한 사본으로 복원할 수 있음을 의미하기 때문에 데이터 및 시스템 무결성에 중요하다. 이것은 충돌 및 사이버 사고로부터 복구하고 시스템을 일관된 상태로 복원하는 데 중요하다.

시스템을 재시작하고 읽기 전용 소스로부터 (예를 들어 롤백 작업 후) 모든 소프트웨어 및 데이터의 새로운 이미지를 다시 로드하는 것은 예기치 않은 결점 또는 사이버 사고로부터 복구하는 효과적인 접근 방식이다. 그러나 재시작 작동은 단일 구성품의 예상치 못한 재시작이 불안정한 시스템 상태 또는 예측할 수 없는 동작을 초래할 수 있는 경우, 특히 통합시스템에 대해서 통제되어야 한다.

(4) 등록검사

(가) 설계 단계

시스템 통합자는 사이버보안 설계 기술서 상에 다음의 정보를 포함해야 한다.

(a) CBS를 안전하게 종료, 재설정, 복원 및 재시작하는 방법을 기술한 제품 매뉴얼 또는 절차서에 대한 참조

(나) 건조 단계

요구사항 없음

(다) 선내시험 단계

(a) 시스템 통합자는 선박 사이버복원력 시험절차서(**202.**의 **2**항 (2)호 참조)를 제출하고 CBS의 종료, 재설정 및 복원을 위해 매뉴얼 또는 절차서가 수립되어 있음을 우리 선급에 입증해야 한다. 이러한 매뉴얼/절차서는 선주에게 제공되어야 한다.

(b) 상기 시험은 **202.**의 **2항** (2)호에 다라 CBS의 인증 중에 실시된 경우 생략될 수 있다.

(5) 유지검사

운항 단계에서 검사에 대한 일반 요구사항은 **203.**을 참조한다.

(가) 정기검사

CBS의 변경이 있는 경우, 선주는 선박 사이버복원력 시험절차서에 따라 **405.**의 **3**항 (4)호 (다)의 활동을 우리 선급에 입증해야 한다. ⚓

제 3 장 선내 시스템 및 장비의 사이버복원력

제 1 절 일반사항

101. 도입

선박, 항만, 컨테이너 터미널 등의 기술 진화와 운영 기술(OT) 및 정보 기술(IT)에 대한 의존도의 증가는 비즈니스, 인적 데이터, 인명의 안전, 선박의 안전에 영향을 미치고 해양 환경을 위협할 수 있는 사이버 공격의 가능성 증가를 창출했다. 현재와 떠오르는 위협으로부터 해운을 보호하려면 설계 및 제조 단계에서 장비 및 시스템에 보안 기능을 통합하는 것을 요구하며 지속 발전하는 다양한 제어 기능들을 포함해야 한다. 따라서 사이버복원력으로 설명할 수 있는 시스템과 장비를 제공하기 위해 최소 공통 요구사항들을 수립할 필요가 있다.

102. 적용

1. 이 장의 요건은 **1장 103.**의 2항에 따른 지침의 적용 범위에 포함되는 CBS에 대하여 적용한다.
2. 항해 및 무선통신 시스템에 대해서는 **2장**의 관련 요건을 만족하는 조건으로 **4절**에서 요구되는 보안 기능들을 대신하여 IEC 61162-460 또는 다른 동등한 표준의 적용이 우리 선급에 의해 허용될 수 있다.
3. **4절**은 CBS에 대해 요구되는 보안 기능들을 명시한다.
4. **4절**의 요구사항은 IEC 62443-3-3 내에서 선택된 요구사항들을 기반으로 한다. 각 요구사항에 대한 전체 내용, 근거(rationale) 및 관련 지침을 결정하기 위해서 참조된 표준을 참고할 수 있다.

103. 제한 사항

1. 이 장은 시스템 하드웨어 및 소프트웨어 기능에 대한 환경 성능을 다루지 않는다. 이 장에 추가하여 다음의 규칙 및 지침이 적용되어야 한다.
   (1) 시스템 하드웨어에 대한 환경시험에 대한 **제조법 및 형식승인 등에 관한 지침 3장 23절** 요구사항
   (2) 소프트웨어 기능 관련 장비 안전에 대한 **선급 및 강선규칙 6편 2장 4절** 요구사항

104. 보안 원칙(Philosophy)

1. 시스템 및 장비

(1) 시스템은 안전하고 안심되며 신뢰할 수 있는 프로세스 운영을 가능하게 하는 하드웨어 및 소프트웨어 그룹으로 구성될 수 있다. 대표적인 예는 엔진 제어 시스템, DP 시스템 등이 있다.
(2) 장비는 다음 중 하나일 수 있다.
   (가) 네트워크 장치 (즉, 라우터, 관리되는 스위치)
   (나) 보안 장치 (즉, 방화벽, 침입탐지시스템)
   (다) 컴퓨터 (즉, 워크스테이션, 서버)
   (라) 자동화 장치 (즉: PLC)
   (마) 가상 머신 클라우드 호스팅

2. 사이버복원력

4절의 사이버복원력 요구사항은 해당되는 경우 **1장 103.**의 적용 범위 내의 모든 시스템에 적용한다. 비신뢰 네트워크와의 인터페이스와 관련된 추가 요구사항은 이러한 연결이 설계된 시스템에만 적용된다.

3. 중요용도 가용성

(1) 중요용도에 대한 보안 조치는 시스템의 가용성에 부정적인 영향을 주지 않아야 한다.
(2) 보안 조치의 구현은 안전 기능 상실, 제어 기능 상실, 감시 기능 상실 또는 건강, 안전 및 환경 영향을 초래할 수 있는 기타 기능의 상실을 야기하지 않아야 한다.
(3) 시스템은 선박, 시스템, 선원 및 화물의 안전에 필요한 데이터의 기밀성, 무결성 및 가용성을 보장하는 방식으로 선박이 임무 수행에 필수적인 운전을 계속할 수 있도록 적절하게 설계되어야 한다.

4. 보상 대책

(1) 보상 대책은 하나 이상의 보안 요구사항을 만족하기 위해 고유의 보안 기능을 대신하거나 추가로 적용될 수 있다.

(2) 보상 대책은 참조된 표준뿐만 아니라 각 요건과 표준의 관련 항목 간의 차이를 고려하여 원래의 언급된 요구사항의 의도와 엄격함을 만족해야 하며, 301.의 3항에 명시된 원칙을 따라야 한다.

제 2 절 시스템 및 장비의 검사

201. 일반사항

1. 적용 대상 결정

공급자는 시스템 통합자와 협력하여 CBS가 **3장**의 강제적용 대상인지를 결정해야 한다. (**그림 3.2.1** 참조)

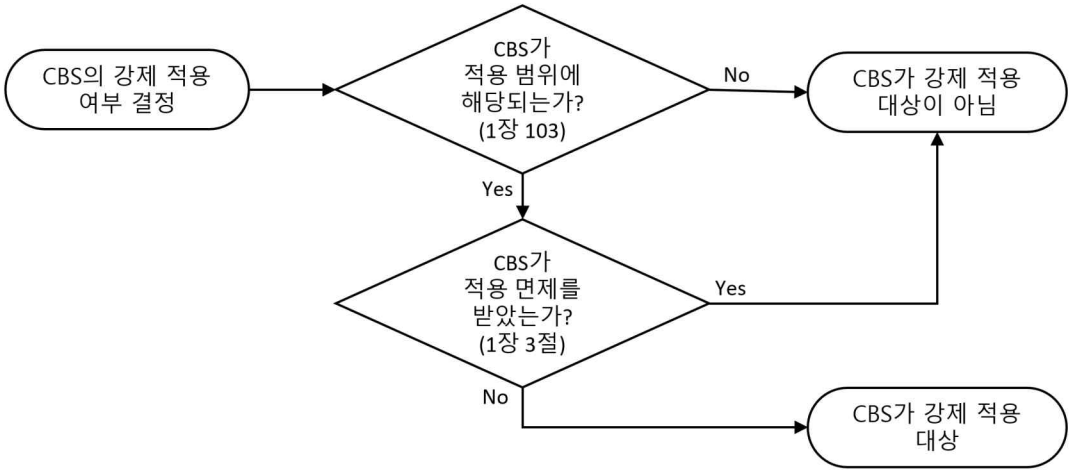

그림 3.2.1 CBS의 적용 대상 결정

2. 사이버복원력 형식승인(TA)

(1) 이 지침의 적용 범위에 포함되는 CBS는 기본적으로 이 장의 관련 요건에 따라 우리 선급으로부터 사이버복원력 형식승인을 받아야 한다.

(2) 사이버복원력 형식승인에 대한 승인 절차 및 제반 사항은 제조법 및 형식승인 등에 대한 지침에 따라야 한다.

3. 호선용 CBS의 도면승인 및 검사 절차

(1) 호선용 CBS의 검사 요건은 이장의 요건에 추가하여 **선급 및 강선규칙 6편 2장 4절**의 요건에도 적합해야 한다.

(2) 일반적인 호선용 CBS의 도면승인 및 검사 절차는 다음 **그림 3.2.2**을 따른다.

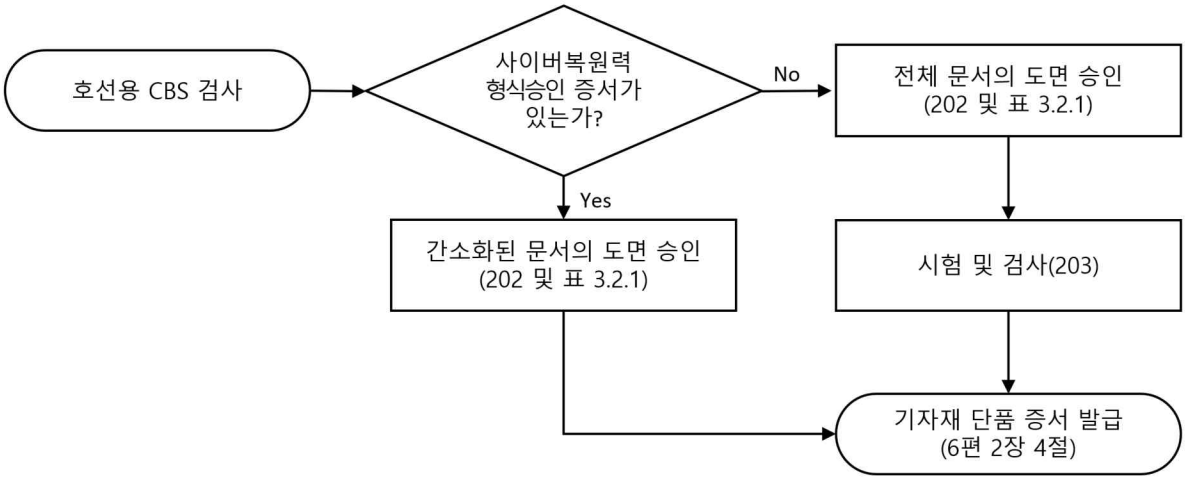

그림 3.2.2 호선용 CBS 도면승인 및 검사 절차

(3) CBS가 사이버복원력 형식승인을 받지 않은 경우, **표 3.2.1**에 따른 전체 문서의 도면승인을 포함한 **203.**에 따른 시험 및 검사를 받아야 한다. (**그림 3.2.2** 참조)

(4) 항해 및 무선통신 장비가 **102.**의 **2**항에 따라 다른 동등한 표준이 **4절**을 대신하여 적용되는 경우 다음에 적합해야 한다.

(가) 문서 승인 및 검사는 **그림 3.2.2**에 표시된 절차에 따라야 한다.

(나) 우리 선급의 별도로 필요하다고 인정하는 경우, **2장**의 요건을 만족하는지를 입증하기 위한 추가의 도면 승인 및 검사를 요구할 수 있다.

(5) **선급 및 강선규칙 6편 2장**에 따른 기자재 검사가 요구되지 않는 CBS가 사이버복원력 형식승인을 보유하고 있는 경우, **203.**에 따른 시험 및 검사와 기자재 단품 증서 발급은 요구되지 아니 한다.

202. 도면승인

1. 도면승인은 특정 선박용으로 의도된 CBS의 문서 평가이다. **3절**의 문서들은 공급자에 의한 제출이 요구된다. 문서는 우리 선급이 이 장의 요구사항을 준수하는지를 검증하는 것이 가능해야 한다.
2. CBS가 이 장의 요구사항을 커버하는 우리 선급에서 승인한 유효한 형식승인 증서를 보유하고 있는 경우, 공급자는 축소된 세트의 호선용 문서를 우리 선급에 제출할 수 있다. (**표 3.2.1** 참조)
3. 공급자는 승인된 버전의 문서들을 시스템 통합자에게 CBS의 인도 시 함께 제공해야 한다.

표 3.2.1 제출 문서 목록

번호	문서명	요구사항	TA	호선용 승인	
				TA 있음	TA 없음
1	CBS 자산 목록	선박 자산 인벤토리에 포함될 내용 (**2장 401.**의 1항)	승인	승인	승인
2	토폴로지 다이어그램	시스템 통합자가 보안구역 및 전송로 설계를 가능하게 해야 함 (**2장 402.**의 1항)	승인	승인	승인
3	보안 기능 기술서	요구되는 보안 기능들 (**401.**)	승인		승인
		만약 적용되는 경우, 추가의 보안 기능들 (**402.**)			
4	보안 기능 시험절차	요구되는 보안 기능들 (**401.**)	승인		승인
		만약 적용되는 경우, 추가의 보안 기능들 (**402.**)			
5	보안 설정 지침	네트워크 및 보안 설정 (**401.**/29번 항목)	참고		참고
6	SDLC 문서	SDLC 요구사항 (**5절**)	승인		승인
7	유지보수 및 검증 계획	보안 기능 검증 (**401.**/19번 항목)	참고		참고
8	사고 대응 및 복구 계획 지원 정보	감사 이벤트 (**401.**/13번 항목)	참고		참고
		결정론적 출력 (**401.**/20번 항목)	참고		참고
		시스템 백업 (**401.**/26번 항목)	참고		참고
		시스템 복구 및 재구성 (**401.**/27번 항목)	참고		참고
9	변경관리 계획	변경관리 프로세스 (**선급 및 강선규칙 6편 2장 4절**)	참고		참고
10	시험 보고서	보안 기능 설정 및 강화 (**301.**의 5항, **501.**의 7항)	참고	참고	참고

203. 시험 및 검사

1. 일반

(1) 시험 및 검사는 사이버복원력 형식승인 증서를 보유하지 않은 CBS에 요구되는 호선용 검증 활동이다.

(2) 시험 및 검사 목적은 CBS가 이 장의 관련 요건을 만족함을 시험 및/또는 분석적 평가를 통해 입증하기 위함이다.

시험 및 검사 공급자의 구내 또는 시험 및 검사를 위해 적절한 시설을 갖춘 다른 시험 장소에서 실시되어야 한다.

(3) 시험 및 검사가 완료된 이후 우리 선급은 기자재 단품 증서 증서를 공급자에 발급하며, 공급자는 시스템 통합자에게 인도 시 CBS와 함께 제공해야 한다.

(4) 시험 및 검사는 아래 2항 내지 5항에 명시된 요건을 따라야 한다.

2. 일반 검사 항목

(1) 공급자는 설계, 구성 및 내부 시험이 완료되었음을 입증해야 한다.

(2) 인도되는 시스템이 승인된 문서에서 올바르게 표시되어 있는지를 입증되어야 한다. 이는 시스템 검사와 구성 요소 및 배치/아키텍처를 자산 목록(301.의 1항) 및 토폴로지 다이어그램(301.의 2항)과 비교를 통해 수행되어야 한다.

3. 보안 기능 시험

(1) 공급자는 인도되는 시스템의 요구되는 보안 기능을 시험해야 한다. 시험은 301.의 4항의 승인된 시험절차서에 따라 실시되어야 하며 우리 검사원에 의해 입회하여 인정되어야 한다.

(2) 시험은 선급 검사원에게 모든 요구사항을 만족하는지에 대한 합리적인 보증을 제공해야 한다. 이는 동일한 구성품들의 시험은 일반적으로 요구되지 않음을 의미한다.

4. 보안 기능의 올바른 설정

(1) 공급자는 시스템 구성품의 보안 설정이 301.의 5항의 설정 지침에 따라 설정되었는지를 선급 검사원에게 시험 및 입증해야 한다. 이러한 입증은 보안 기능의 시험과 연계하여 실시될 수 있다.

(2) 보안 설정은 보고서 내에 문서화되어야 한다(예: 호선용 설정 지침).

5. 보안 개발 수명주기

공급자는 301.의 6항의 문서에 따라 5절의 보안 개발 수명주기 요구사항을 준수함을 입증해야 한다.

(1) 개인키 통제 (IEC 62443-4-1/SM-8)

(가) 이 요구사항은 시스템에 사용자가 진위 여부를 검증하는 것을 목적으로 디지털로 서명된 소프트웨어가 포함된 경우에 적용한다.

(나) 공급자는 무단 접근으로부터 코드 서명에 사용되는 개인키의 생성, 저장 및 사용을 보호하기 위한 정책, 절차 및 기술적 통제를 입증하는 관리 시스템 문서를 제시해야 한다.

(다) 정책과 절차는 역할, 책임 및 작업 프로세스를 다루어야 한다. 기술적 통제에는 예를 들어, 개인키의 저장매체에 대한 물리적 접근 제한과 암호화 하드웨어(예: 하드웨어 보안 모듈)를 포함해야 한다.

(2) 보안 업데이트 문서 (IEC 62443-4-1/SUM-2)

공급자는 보안 업데이트를 사용자에게 알리는 것을 보장하기 위한 조직 내 프로세스가 수립되어 있음을 입증하는 관리 체계 문서를 제시해야 한다. 사용자에 대한 정보에는 502.의 2항에 나열된 항목들을 포함해야 한다.

(3) 종속 구성요소 보안 업데이트 문서 (IEC 62443-4-1/SUM-3)

공급자는 시스템 내 획득한 소프트웨어의 업데이트 버전(운영 체제 또는 펌웨어의 새로운 버전/패치)이 시스템과 호환되는지를 사용자에게 알리는 것을 보장하는 프로세스가 조직 내에 수립되어 있음을 입증하는 관리 체계 문서를 제시해야 한다. 획득한 업데이트 소프트웨어를 적용하지 않는 것에 관련된 위험을 관리하는 방법에 대한 정보를 포함해야 한다.

(4) 보안 업데이트 제공 (IEC 62443-4-1/SUM-4)

공급자는 사용자가 시스템 보안 업데이트를 이용할 수 있도록 보장하고, 사용자가 업데이트 소프트웨어의 진위 여부를 확인하는 방법을 기술하는 프로세스가 조직 내에 수립되어 있음을 입증하는 관리 체계 문서를 제시해야 한다.

(5) 제품 심층 방어 (IEC 62443-4-1/SG-1)

(가) 공급자는 설치, 유지보수 및 운영 중에 CBS의 소프트웨어에 대한 보안 위협을 완화하기 위한 심층 방어 조치에 대한 전략을 문서화하기 위한 프로세스가 조직 내에 수립되었음을 입증하는 관리 체계 문서를 제시해야 한다.

(나) 위협에 예시로는 선박의 운항 단계에서 무단 소프트웨어의 설치, 패치 프로세스의 취약점, 소프트웨어 변조 등이 있다.

(6) 환경에서 예상되는 심층 방어 조치 (IEC 62443-4-1/SG-2)

공급자는 물리적 배치, 정책 및 절차 등 외부 환경에서 제공할 것으로 예상되는 심층적인 방어 조치를 문서화하기 위한 프로세스가 조직 내에 수립되어 있음을 입증하는 관리 체계 문서를 제시해야 한다.

(7) 보안 강화 지침 (IEC 62443-4-1/SG-3)

(가) 공급자는 502.의 7항에서 요구되는 바와 같이 시스템에 대한 강화 지침이 작성되는 것을 보장하기 위한 프로세스가 조직 내에 수립되어 있음을 입증하는 관리 체계 문서를 제시해야 한다.

(나) 지침은 불필요한 소프트웨어, 계정, 서비스 등을 제거하여 시스템의 취약점을 줄이는 방법을 명시해야 한다.

제 3 절 승인문서 및 자료

301. CBS의 승인문서 및 자료

이 장의 요구사항에 따라 검토 및 승인을 위해 다음 문서를 우리 선급에 제출해야 한다. (2절 참조)

1. CBS 자산 목록(CBS Asset Inventory)

CBS 자산 목록은 다음의 정보를 포함해야 한다.

(1) 하드웨어 구성품 목록 (예: 호스트 장치, 임베디드 장치, 네트워크 장치)
- (가) 명칭
- (나) 브랜드/제조사
- (다) 모델/형식
- (라) 기능/목적의 간략한 설명
- (마) 물리적 인터페이스 (예: 네트워크, 시리얼)
- (바) 시스템 소프트웨어의 명칭/형식 (예: 운영체제, 펌웨어)
- (사) 시스템 소프트웨어의 버전 및 패치 수준
- (아) 지원되는 통신 프로토콜

(2) 소프트웨어 구성품 목록 (예: 응용 소프트웨어, 유틸리티 소프트웨어)
- (가) 설치된 하드웨어 구성품
- (나) 브랜드/제조사
- (다) 모델/형식
- (라) 기능/목적의 간략한 설명
- (마) 소프트웨어 버전

2. 토폴로지 다이어그램 (Topology Diagram)

(1) 물리적 토폴로지 다이어그램은 시스템의 물리적 아키텍처를 보여야 한다. CBS 자산 목록 내 하드웨어 구성품을 식별할 수 있어야 한다. 다이어그램은 다음을 표시해야 한다.
- (가) 이중화 장치 식별을 포함한 모든 종단점(endpoints) 및 네트워크 장치
- (나) 입출력(I/O) 장치와 통신을 포함한 통신 케이블(네트워크, 시리얼 링크)
- (다) 다른 네트워크 또는 시스템에 대한 통신 케이블

(2) 논리적 토폴로지 다이어그램은 시스템의 구성요소 간의 데이터 흐름을 보여야 한다. 다이어그램은 다음을 표시해야 한다.
- (가) 통신 종단점 (예: 워크스테이션, 제어장치, 서버)
- (나) 네트워크 장치 (예: 스위치, 라우터, 방화벽)
- (다) 물리 및 가상의 컴퓨터
- (라) 물리 및 가상의 통신 경로
- (마) 통신 프로토콜

(3) 하나로 결합된 토폴로지 다이어그램이 모든 요청되는 정보가 분명하게 보인다면 허용될 수 있다.

3. 보안 기능 기술서 (Description of security capabilities)

(1) 이 문서는 하드웨어 및 소프트웨어 구성품을 가진 CBS가 어떻게 401.의 필수 보안 기능을 만족하는 지를 기술해야 한다.

(2) 2장의 적용 범위 내의 다른 CBS에 대한 모든 네트워크 인터페이스가 기술되어야 한다. 기술서는 목적지 CBS, 데이터 흐름 및 통신 프로토콜을 포함해야 한다. 만약 시스템 통합자가 목적지 CBS를 다른 보안구역에 할당한 경우, 보안구역 경계 보호(2장 402.의 2항 (1)호 참조)를 제공하는 구성품이 CBS의 일부로 제공된다면 자세히 기술되어야 한다.

(3) 2장의 적용 범위 밖의 다른 시스템 또는 네트워크(비신뢰 네트워크)에 대한 모든 네트워크 인터페이스가 기술되어야 한다. 기술서는 402.의 추가 보안 기능의 준수를 명시하고 선원을 위한 관련 절차 또는 설명을 포함해야 한다. 보안구역 경계 보호(2장 402.의 2항 (1)호 참조)를 제공하는 구성품이 CBS의 일부로 제공된다면 자세히 설명되어야 한다.

(4) 각 요구사항에 대한 별도의 장이 지정되어야 한다. 시스템 내 모든 하드웨어 및 소프트웨어 구성품은 관련된 기술서에서 다루어져야 한다.

(5) 만약 요구사항을 완전히 만족하지 못하는 경우, 기술서에 명시되고 보상 대책이 제안되어야 한다. 보안 대책은 다음을 만족해야 한다.

(가) 원래의 요구사항과 동일한 위협으로부터 보호해야 한다.
(나) 원래의 요구사항과 동등하게 수준의 보호를 제공해야 한다.
(다) 이 장의 다른 요구사항에서 요구되는 보안 통제가 아니어야 한다.
(라) 추가의 보안 위험을 도입하지 않아야 한다.

(6) 요구사항 준수를 검증하기 위해 필요한 모든 증빙 문서들(예: OEM 정보)이 기술서 내에 참조되고 제출되어야 한다.

4. 보안 기능 시험절차서

(1) 이 문서는 시스템이 어떠한 보상 대책을 포함하여 **401.** 및 **402.**의 요구사항을 만족하는지를 시험하여 증명하는 방법을 기술해야 한다. 분석적 평가에 의한 준수의 증명이 특별히 고려될 수 있다.

(2) 시험절차서는 각 적용 가능 요구사항에 대한 별도의 장으로 포함해야 하며, 다음을 기술해야 한다.
(가) 필요한 시험 설정 (즉, 동일한 예상 결과로 시험을 반복할 수 있는지 보장하기 위함)
(나) 시험 장비
(다) 초기 조건
(라) 시험 방법론, 상세한 시험 단계
(마) 예상되는 결과 및 합격 기준

(3) 시험절차서에는 시험 중에 시험 결과를 업데이트하고 결과를 기록하는 수단을 포함해야 한다.

5. 보안 설정(Security configuration) 지침

(1) 이 문서는 보안 기능의 권장되는 구성 설정을 기술하고, 초기값을 명시해야 한다. 지침의 목적은 보안 기능이 시스템 통합자에 의해 **2장** 및 사양서에 따라서 구현되는 것을 보장하기 위한 것이다. (예: 사용자 계정, 인증, 암호 정책, 기계의 안전 상태, 방화벽 규칙 등)

(2) 문서는 **401.**의 29번 항목의 검증을 위한 기초로서 제공되어야 한다.

6. 보안 개발 수명주기(SDLC: Secure Development Lifecy-Cycle) 문서

(1) 이 문서는 요청 시 우리 선급에 제출되어야 하며 **5절**의 보안 개발 수명주기에 대한 요구사항에 따라 공급자의 프로세스 및 통제 방안을 기술해야 한다.

(2) 소프트웨어 업데이트 및 패치 방법이 기술되어야 한다.

(3) 문서는 **203. 5.**에 따라 검사를 위해 우리 선급에 준비되어야 한다.

7. CBS의 유지보수 및 검증 계획

이 문서는 요청 시 우리 선급에 제출되어야 하며 시스템의 보안 관련 유지보수 및 시험을 위한 절차를 포함해야 한다. 문서에는 **401.**의 19번 항목에서 요구되는 시스템 보안 기능의 올바른 작동을 검증하는 방법에 대한 설명을 포함해야 한다.

8. 선주의 사고 대응 및 복구 계획 지원 정보

이 문서는 요청 시 우리 선급에 제출되어야 하며, 사용자가 다음을 달성할 수 있도록 허용하는 절차 또는 설명을 포함해야 한다.

(1) 로컬 독립 제어 (**2장 404.**의 **2**항 참조)
(2) 네트워크 격리 (**2장 404.**의 **3**항 참조)
(3) 감사 기록의 사용에 의한 포렌식 (**401.**의 13번 항목 참조)
(4) 결정론적 출력 (**401.**의 20번 항목 참조)
(5) 백업 (**401.**의 26번 항목 참조)
(6) 복구 (**401.**의 27번 항목 참조)
(7) 제어된 종료, 재설정, 롤백 및 재시작 (**2장 405.**의 **3**항 참조)

9. 변경관리 계획

이 문서는 요청 시 우리 선급에 제출되어야 한다. 이 절차서는 사이버보안에만 국한되지 않으며 **선급 및 강선규칙 6편 2장 4절**에 의해서도 요구된다.

10. 시험 보고서

이 장의 보안 기능을 커버하는 형식승인 증서를 가진 CBS는 선급 검사로부터 면제될 수 있다. 그러나, 공급자가 서명한 시험 보고서가 우리 선급에 제출되어, 공급자가 설계, 구축, 시험, 구성 및 강화(hardening)를 완료했음이 입증되어야 하며, 그렇지 않을 경우 검사를 통해 우리 선급에 검증되어야 한다. (**203.** 참조)

제 4 절 보안 기능 요구사항

401. 필수 보안 기능

1. 다음의 보안 기능은 **1장**에서 명시된 범위 내의 모든 CBS에 대해서 요구된다.

표 3.4.1 필수 보안 기능 요구사항

항목번호	목적	요구사항	참조 표준
○ 미인증된 개체로부터 우발적 또는 우연한 접근으로부터 보호			
1	인간 사용자 식별 및 인증	CBS는 시스템에 직접 또는 인터페이스를 통해 접근할 수 있는 모든 인간 사용자를 식별하고 인증해야 한다.	IEC62443-3-3/ SR1.1
2	계정 관리	CBS는 계정 추가, 활성화, 수정, 비활성화 및 제거를 포함하여 허가된 사용자의 모든 계정 관리를 지원하는 기능을 제공해야 한다.	IEC62443-3-3/ SR1.3
3	식별자 관리	CBS는 사용자, 그룹 및 역할별 식별자 관리를 지원하는 기능을 제공해야 한다.	IEC62443-3-3/ SR1.4
4	인증자 관리	CBS는 다음의 능력을 제공해야 한다. - 인증자 내용을 초기화 - 제어 시스템 설치 시 모든 기본 인증자를 변경 - 모든 인증자를 변경/새로고침 - 저장 및 전송 시 모든 인증자를 무단 공개 및 수정으로부터 보호	IEC62443-3-3/ SR1.5
5	무선 접근 관리	CBS는 무선통신에 관계되는 모든 사용자(인간, 소프트웨어 프로세스 또는 장치)를 식별하고 인증할 수 있는 기능을 제공해야 한다.	IEC62443-3-3/ SR1.6
6	패스워드 기반 인증 강도	CBS는 최소 길이와 다양한 문자 유형에 기반하여 설정 가능한 패스워드 강도를 시행하는 있는 기능을 제공해야 한다.	IEC62443-3-3/ SR1.7
7	인증자 피드백	CBS는 인증 과정 중에 피드백을 잘 보이지 않게 해야 한다.	IEC62443-3-3/ SR1.10
○ 우발적 또는 우연한 오용으로부터 보호			
8	권한부여 시행	모든 인터페이스에서 인간 사용자는 직무 분리와 최소 특권의 원칙에 따라서 권한이 할당되어야 한다.	IEC62443-3-3/ SR2.1
9	무선 사용 통제	CBS는 일반적으로 허용되는 보안 산업 관행에 따라 시스템에 대한 무선 연결에 대해 허가, 감시 및 사용 제한을 시행하는 기능을 제공해야 한다.	IEC62443-3-3/ SR2.2
10	휴대용 및 모바일 장치의 사용 통제	CBS가 휴대용 및 모바일 장치 사용을 지원하는 경우 시스템은 다음의 기능을 포함해야 한다. a) 휴대용 및 모바일 장치 사용은 설계상 허용된 대상으로만 제한 b) 휴대용 및 모바일 장치로의/로부터 코드 및 데이터 전송을 제한 (비고) 포트 제한/블록커 (및 실리콘)은 특정 시스템에 대하여 허용될 수 있다.	IEC62443-3-3/ SR2.3
11	모바일 코드	CBS는 자바스크립트, ActiveX 및 PDF와 같은 모바일 코드의 사용을 통제해야 한다.	IEC62443-3-3/ SR2.4
12	세션 잠금	CBS는 설정이 가능한 비활성 시간 이후 또는 수동 세션 잠금의 활성화에 따라 추가 접근을 방지할 수 있어야 한다.	IEC62443-3-3/ SR2.5

13	감사가능 사건	CBS는 최소한 다음의 사건에 대한 보안 관련 감사 기록을 생성해야 한다. 접근 통제, 운영 체제 사건, 백업 및 복구 사건, 설정 변경, 통신 상실	IEC62443-3-3/ SR2.8
14	감사 저장 용량	CBS는 일반적으로 인정되는 로그 관리 권고사항에 따라 감사 기록 저장 용량을 할당하는 기능을 제공해야 한다. 감사 메커니즘이 이러한 용량을 초과할 가능성을 줄이기 위해 구현해야 한다.	IEC62443-3-3/ SR2.9
15	감사 처리 실패 대응	CBS는 감사 처리 실패 시 중요서비스 및 기능의 손실을 방지하는 기능을 제공해야 한다.	IEC62443-3-3/ SR2.10
16	타임스탬프	CBS는 감사 기록에 타임스탬프를 포함해야 한다.	IEC62443-3-3/ SR2.11
○ 우발적 또는 우연한 조작으로부터 CBS 무결성 보호			
17	통신 무결성	CBS는 전송된 정보의 무결성을 보호해야 한다. (비고) 암호화 메커니즘이 무선 네트워크에 적용되어야 한다.	IEC62443-3-3/ SR3.1
18	악성코드 보호	CBS는 악성코드 또는 무단 소프트웨어로 인한 영향을 예방, 탐지 및 완화하기 위한 적절한 보호조치를 구현하는 기능을 제공해야 한다. 보호 메커니즘을 업데이트하는 기능이 있어야 한다.	IEC62443-3-3/ SR3.2
19	보안 기능 검증	CBS는 보안 기능의 의도된 작동의 검증을 지원하고 유지보수 중 이상이 발생 시 보고하는 기능을 제공해야 한다.	IEC62443-3-3/ SR3.3
20	결정론적 출력	CBS는 공격의 결과로 정상적인 작동을 유지할 수 없는 경우 미리 결정된 상태로 출력을 설정하는 기능을 제공해야 한다. 미리 결정된 상태의 예시는 다음과 같다. - 무전원 상태, - 마지막 알려진 값, 또는 - 고정값	IEC62443-3-3/ SR3.6
○ 도청 또는 우연한 노출을 통한 무단 정보 노출 방지			
21	정보 기밀성	CBS는 미사용 또는 전송 중인 명시적 읽기 권한이 지원되는 정보의 기밀성을 보호하는 기능을 제공해야 한다. (비고) 무선 네트워크의 경우 전송 중인 모든 정보의 기밀성을 보호하기 위해 암호화 메커니즘을 사용해야 한다.	IEC62443-3-3/ SR4.1
22	암호 사용	암호가 사용되는 경우, CBS는 일반적으로 허용되는 보안 산업 관행 및 권고에 따라서 암호 알고리즘, 키 길이 및 메커니즘을 사용해야 한다.	IEC62443-3-3/ SR4.3
○ CBS 작동 감시 및 사고 대응			
23	감사 로그 접근성	CBS는 허가된 사용자 및/또는 도구에 의해 읽기 전용 기반으로 감사 로그에 접근하는 능력을 제공해야 한다.	IEC62443-3-3/ SR6.1
○ 제어 시스템이 정상 생산 조건에서 안정적으로 작동하는지 확인			
24	서비스 거부 (DoS) 보호	CBS는 DoS 사건 중 중요 기능들을 유지하는 최소 능력을 제공해야 한다. (비고) DoS 사건 시 CBS가 성능 저하 모드에서 작동하는 것이 허용될 수 있지만, 위험한 상황을 초래할 수 있는 방식으로 실패하지 않아야 한다. 네트워크 용량이 초과되는 경우와 컴퓨터의 리소스가 소모되는 경우와 같이 과부하 기반 DoS 이벤트를 고려해야 한다.	IEC62443-3-3/ SR7.1

25	자원(resource) 관리	시스템은 자원 부족을 방지하기 위해 보안 기능의 자원 사용을 제한하는 능력을 제공해야 한다.	IEC62443-3-3/ SR7.2
26	시스템 백업	중요 파일의 식별자와 위치와 사용자 및 시스템 정보(시스템 상태 정보 포함)의 백업을 수행하는 능력은 정상 작동에 영향이 없도록 CBS에서 지원해야 한다.	IEC62443-3-3/ SR7.3
27	시스템 복구 및 재구성	CBS는 중단 또는 고장 후 알려진 보안 상태로 복구하거나 및 재구성할 수 있는 기능을 제공해야 한다.	IEC62443-3-3/ SR7.4
28	대체 전원	CBS는 기존 보안 상태 또는 문서로 된 성능 저하 모드에 영향을 주지 않고 대체 전원 공급으로/으로부터 전환할 수 있는 능력을 제공해야 한다.	IEC62443-3-3/ SR7.5
29	네트워크 및 보안 구성 설정	CBS는 공급자가 제공한 지침에 기술된 바와 같이 권장되는 네트워크 및 보안 구성에 따라 설정할 수 있는 능력을 제공해야 한다. CBS는 현재 배치된 네트워크 및 보안 구성 설정에 대한 인터페이스를 제공해야 한다.	IEC62443-3-3/ SR7.6
30	최소화 기능	다음에 대한 설치, 가용성 및 접근 권한은 CBS에서 제공하는 기능의 엄격한 필요성에 제한되어야 한다. - 운영 체제 소프트웨어 구성요소, 프로세스 및 서비스 - 네트워크 서비스, 포트, 프로토콜, 경로 및 호스트 접근 및 소프트웨어	IEC62443-3-3/ SR7.7

402. 추가 보안 기능

1. 다음의 추가 보안 기능은 비신뢰 네트워크(즉, **2장**의 적용 범위 밖에 있는 네트워크에 대한 인터페이스)에 네트워크 통신을 하는 CBS에 대하여 요구된다.
2. 또한, 보안구역 경계를 통과하여 통신하는 CBS는 **2장 402.**의 1항 및 **402.**의 2항의 네트워크 분할과 구역 경계 보호 요구사항을 만족해야 한다.

표 3.4.2 추가 보안 기능 요구사항

항목번호	목적	요구사항	참조 표준
31	인간 사용자에 대한 다중요소 인증	비신뢰 네트워크를 통해 CBS에 접근하는 경우 다중요소 인증이 인간 사용자에 대해 요구된다.	IEC62443-3-3/ SR1.1, RE2
32	소프트웨어 프로세스 및 장치 식별 및 인증	CBS는 소프트웨어 프로세스와 장치를 식별하고 인증해야 한다.	IEC62443-3-3/ SR1.2
33	실패한 로그인 시도	CBS는 지정된 시간 동안 비신뢰 네트워크로부터 연속적으로 무효한 로그인 시도 제한을 시행해야 한다.	IEC62443-3-3/ SR1.11
34	시스템 사용 알림	CBS는 인증 전에 시스템 사용 알림 메시지를 표시하는 능력을 제공해야 한다. 시스템 사용 알림 메시지는 허가된 선원에 의해서 설정될 수 있어야 한다.	IEC62443-3-3/ SR1.12
35	비신뢰 네트워크를 통한 접근	CBS는 비신뢰 네트워크를 통한 어떤 접근이 감시되고 통제되어야 한다.	IEC62443-3-3/ SR1.13
36	명시적 접근 요청 승인	CBS는 선내 허가된 선원이 명시적으로 승인하는 경우를 제외하고 비신뢰 네트워크를 통한 접근을 거부해야 한다.	IEC62443-3-3/ SR1.13, RE1
37	원격 세션 종료	CBS는 설정된 미사용 시간 이후 자동으로 또는 세션을 시작한 사용자가 수동으로 원격 세션을 종료하는 기능을 제공해야 한다.	IEC62443-3-3/ SR2.6
38	암호 무결성 보호	CBS는 비신뢰 네트워크를 통해 통신하는 동안 정보의 변경을 인식하기 위해 암호 메커니즘을 적용해야 한다.	IEC62443-3-3/ SR3.1, RE1
39	입력 검증	CBS는 프로세스 제어 입력 또는 CBS의 동작에 직접 영향을 주는 입력으로서 사용되는 비신뢰 네트워크를 통한 입력 데이터의 구문(syntax), 길이 및 내용을 입증해야 한다.	IEC62443-3-3/ SR3.5
40	세션 무결성	CBS는 세션의 무결성을 보호하는 기능을 제공해야 한다. 무효한 세션 ID는 거부되어야 한다.	IEC62443-3-3/ SR3.8
41	세션 종료 후 세션 ID 무효화	시스템은 사용자 로그아웃 또는 기타 세션 종료 시(브라우저 세션을 포함) 세션 ID를 무효화해야 한다.	IEC62443-3-3/ SR3.8, RE1

제 5 절 보안 개발 수명주기 요구사항

501. 일반

1. 시스템 또는 장비 개발에 대하여 다음 단계에서 광범위하게 보안 측면을 다루는 보안 개발 수명주기(SDLC)를 따라야 한다.
   (1) 요구사항 분석 단계
   (2) 설계 단계
   (3) 구현 단계
   (4) 검증 단계
   (5) 출시 단계
   (6) 유지보수 단계
   (7) 수명 종료 단계
2. 위의 단계들에서 보안 측면이 어떻게 반영되었는지를 기록한 문서를 생성하고 최소한 아래 502.의 1항에서 7항까지 규정된 바와 같이 최소한 통제된 프로세스를 통합해야 한다.
3. 해당 문서는 검토 및 승인을 위해 우리 선급에 제출해야 한다.

502. 요구사항

1. **개인키 통제** (IEC 62443-4-1/SM-8)
   공급자는 적용이 가능한 경우 코드 서명에 사용되는 개인키를 무단 접근 또는 수정으로부터 보호하기 위한 절차 및 기술적 통제를 마련해야 한다.
2. **보안 업데이트 문서** (IEC 62443-4-1/SUM-2)
   제품 보안 업데이트에 대한 문서는 사용자의 이용이 가능하도록 보장하는 프로세스(사용자가 접근할 수 있는 사이버 보안 연락처 또는 정기 간행물을 통해 이루어질 수 있음)가 채택되어야 하며, 문서는 다음을 모두 포함하지만 이에 국한하지 않는다.
   (1) 보안 패치가 적용되는 제품 버전 번호
   (2) 승인된 패치를 수동 및 자동 프로세스를 통해 적용하는 방법에 대한 설명
   (3) 재부팅을 포함하여 제품에 패치를 적용할 경우 미칠 수 있는 영향에 대한 기술
   (4) 승인된 패치가 적용되었는지를 검증하는 방법에 대한 설명
   (5) 자산 소유자가 승인하거나 및 적용 배치하지 않은 패치에 사용될 수 있는 패치 및 교정을 적용하지 않을 경우의 위험
3. **종속 구성요소나 운영체제 보안 업데이트 문서** (IEC 62443-4-1/SUM-3)
   종속 구성요소 또는 운영 체제 보안 업데이트에 대한 문서를 사용자가 이용할 수 있도록 보장하는 프로세스가 채택되어야 하며, 이는 다음을 포함하지만 이에 국한하지 않는다.
   (1) 제품이 종속 구성요소 또는 운영 체제 보안 업데이트와 호환되는지 여부를 명시
4. **보안 업데이트 제공** (IEC 62443-4-1/SUM-4)
   모든 지원되는 제품 및 제품 버전에 대한 보안 업데이트를 제품 사용자가 보안 패치가 정품임을 쉽게 검증할 수 있는 방식으로 이용할 수 있도록 보장하는 프로세스가 채택되어야 한다.
   (비고) 공급자는 출시 전에 업데이트를 시험하는 품질보증 프로세스를 갖추어야 한다.
5. **제품 심층 방어** (IEC 62443-4-1/SG-1)
   제품이 설치, 운영 및 유지보수를 지원하기 위한 보안 심층 방어 전략을 기술하는 제품 문서를 생성하기 위한 프로세스가 있어야 한다. 이는 다음을 모두 포함한다.
   (1) 제품에서 구현된 보안 기능과 심층 방어 전략에서의 역할
   (2) 심층 방어 전략에 의해 고려된 위협
   (3) 레거시 코드(legacy code)와 관련된 위험을 포함하여, 제품과 관련하여 알려진 보안 위험에 대한 제품의 사용자 완화 전략
6. **환경에서 예상되는 심층 방어 조치** (IEC 62443-4-1/SG-2)
   제품이 사용되는 외부 환경에서 제공할 것으로 예상되는 보안 심층 방어 조치를 설명하는 제품 사용자 문서를 작성하는 프로세스가 채택되어야 한다.
7. **보안 강화 지침** (IEC 62443-4-1/SG-3)

제품을 설치 및 유지보수 시 제품을 강화하기 위한 지침을 포함하는 제품 사용자 문서를 생성하는 프로세스가 채택되어야 한다. 지침에는 다음에 대한 설명, 근거 및 권고사항을 포함하지만 이에 국한하지 않는다.

(1) 제품 보안 관점에서 제 3자의 구성품을 포함하는 제품의 통합

(2) 제품의 응용 프로그래밍 인터페이스/프로토콜과 사용자 응용 소프트웨어의 통합

(3) 제품의 심층 방어 전략의 적용 및 유지보수

(4) 로컬 보안 정책을 지원하고 각 보안 옵션/능력에 대한 설정 및 사용, 그리고 각 보안 옵션/능력에 대한 다음의 내용을 포함:

(가) 제품의 심층 방어 전략에 대한 기여 부분

(나) 각각이 작업 관행에 미치는 잠재적 영향과 함께 어떻게 보안에 영향 주는지를 포함하는 설정 가능한 초기값의 기술, 그리고

(다) 값 설정/변경/삭제

(5) 제품 보안의 관리, 감시, 사고 처리 및 평가를 지원하는 모든 보안 관련 도구 및 유틸리티의 사용에 대한 지침 및 권장 사항

(6) 정기적인 보안 유지보수 활동에 대한 설명 및 권고

(7) 제품에 대한 보안 사고를 공급자에게 보고하는 것에 대한 설명

(8) 제품의 유지보수 및 관리를 위한 보안 모범 관행의 기술 ⚓

제 4 장 선박 사이버보안관리시스템 추가 요구사항

제 1 절 일반사항

101. 목표

1. 이 장의 추가 요건은 **2장**의 요건에 따라 건조된 사이버복원력 선박이 운항 단계에서 사이버위험관리 프로세스 기반의 적절한 사이버보안관리시스템의 이행을 지원하기 위함이다.
2. 2장의 요건에 따라 건조된 선박이 추가로 이장의 요건을 만족하는 사이버복원력 선박은 IMO 결의서 MSC.428(98)에 따른 선박 사이버위험관리 요건을 기본으로 충족하며, 또한, OCIMF 및 RightShip과 같은 화주들의 선박 사이버보안 대한 최소 검사 요건을 만족할 것이다.

102. 적용

1. 이 장의 요건은 **2장**의 요건에 따라 건조된 선박에 대하여 선주의 요청이 있는 경우 추가로 적용한다.
2. 이 장의 요건을 추가로 만족하는 선박에 대해서는 선급 부호 **"Cyber Resilience(Managed)"**를 부여한다.
3. 이 장의 요건은 별도로 명시하는 경우를 제외하고 **1장 103.**에 따른 적용 범위에 있는 CBS 및 네트워크를 대상으로 적용한다.

103. 제한 사항

1. 이 지침에서 명시되지 않는 국제협약, 기국법 및 기항지의 국내법 등에서 요구되는 사이버보안 관련 규정의 경우, 우리 선급의 검사 범위에 포함되지 않으며 이에 대한 규정 준수의 책임은 선주에게 있다.

104. 승인문서 및 자료

1. 선박 사이버보안 및 복원력 프로그램

선박 사이버보안 및 복원력 프로그램은 **201.1**항의 요건에 적합해야 한다.

2. 참고 자료

선주는 다음의 자료를 참고용으로 제출해야 한다.

(1) 선박 사이버 위험도 평가 보고서 및 위험 관리 계획

(2) 사이버보안관리 조직도 및 보안 인력 직무기술서

105. 선박 검사

1. 일반사항

(1) 이 장에 따른 검사의 종류 및 시기는 **2장 201.**의 **4**항에 따른다.

(2) 이 장에 따른 선박 검사 요건에 추가하여 **2장 203.**에도 적합해야 한다.

2. 연차 검사

(1) 선주는 이 장에 따른 검사를 최초로 실시하는 연차검사 예정 시기 전에 **104.**에서 명시된 문서 및 자료를 우리 선급에 제출하여 승인받아야 한다.

(2) 선주는 연차 검사 시 **2절** 요건의 이행을 입증하는 최소한 다음의 증적자료를 우리 선급에 제시해야 한다. 다만, 이에 국한하지 아니한다.

(a) 선박 사이버 위험 평가 보고서 및 위험 관리 결과

(b) 사이버보안 교육 계획 및 결과

(c) 사이버보안 사고 보고서 (만약 있는 경우)

(d) 내부심사 결과

제 2 절 추가 요구사항

201. 사이버보안 정책

1. 선박 사이버보안 및 복원력 프로그램
   선주는 **2장 203.**의 1항 (2)호에서 명시된 선박 사이버보안 및 복원력 프로그램에 다음의 정책들을 추가로 포함해야 한다.
   (1) 사이버 위험관리 정책(Policy for management of cyber risk)
   (2) 사이버보안관리 역할 및 책임
   (3) 선원 인식제고 및 교육 정책(Policy for Crew Awareness and Training)
   (4) 사이버보안 내부 심사 정책
2. 선주는 선박 사이버보안 및 복원력 프로그램을 선내에 비치하고 검토 및 관리하여야 한다.
3. 선주는 선박 사이버보안 및 복원력 프로그램의 운영 및 관리할 수 있는 역량을 갖춘 인력을 지정하고 책임과 권한을 부여하여야 한다.

202. 사이버위험관리 프로세스

1. 선주는 선박 내 CBS 및 네트워크에 대한 사이버 위험의 식별, 분석, 평가 및 처리를 포함한 사이버위험관리 프로세스를 수립해야 한다.
2. 선박 내 CBS 및 네트워크의 운영에 악영향을 줄 수 있는 내외부 사이버위협을 식별하고 목록화해야 한다.
3. 선박 내 CBS 및 네트워크에 대한 사이버위험 평가를 사이버 위협과 취약성을 고려하여 주기적으로 실시해야 한다.
4. 위험 평가 결과를 바탕으로 위험 수준별 우선순위를 선정하고, 필요한 경우 개선조치를 실시해야한다.

203. 인식제고 및 교육

1. 선내 보안활동 관련 직원을 대상으로 사이버보안 교육 계획을 수립하고 적절한 방법으로 주기적으로 보안교육을 실시해야 한다.
2. 선내에서 사이버보안에 대한 인식 제고를 위한 활동을 적절히 이행해야 한다.
   (비고) 다음은 이러한 인식 제고 활동의 예시이다.
   1) 외부 사이버 위협, 사고 사례 등 사이버보안 이슈 관련 정보의 선원 공유
   2) 사이버보안 인식 제고를 위한 홍보물 게시 (예: 안전한 모바일 기기 사용 수칙, 패스워드 보호 지침, 악성코드 예방 수칙 등)

204. 사고 대응 및 복구

1. 선박 내 시스템 운영 및 보안이슈에 즉각적으로 대응 및 복구 업무를 수행할 조직 또는 담당자를 구성하여 역할 및 책임을 정의해야 한다.
2. 내외부 관계자들과 신속한 연락이 가능하도록 비상연락망을 구축하고 최신화하여 관리해야 한다.
3. 선박 사이버 사고 발생 시 적절한 관할 당국에 통보하고 관련 책임자에게 보고하기 위한 절차를 수립하고 이행해야 한다.

205. 사이버보안 내부심사

1. 선박 사이버보안관리에 대한 내부심사 절차를 수립하고, 주기적으로 수행해야 한다. ⚓

부록 I - 선박 요구사항 및 문서 요약

선박 자산 목록 (2장 401.의 1항)		
CBS 보안 기능	제품 보안 업데이트 문서 제공 종속 구성요소 보안 업데이트 문서 제공 보안 업데이트 제공	3장 502.의 2항 3장 502.의 3항 3장 502.의 4항
CBS 문서	CBS 자산 목록 변경관리 계획	3장 301.의 1항 3장 301.의 9항
선박 설계 문서	선박 자산 목록	2장 401.의 1항 (4)호 (가)
선박 사이버보안 및 복원력 프로그램	변경 관리	2장 401.의 1항 (5)호
	소프트웨어 업데이트 관리	2장 401.의 1항 (5)호
보안 구역 및 네트워크 분할 (2장 402.의 1항)		
CBS 보안 기능		
CBS 문서	토폴로지 다이어그램	3장 301.의 2항
선박 설계 문서	구역 및 전송로 다이어그램 설계 기술서 선박 사이버복원력 시험절차서	2장 402.의 1항 (4)호 (가) 2장 402.의 1항 (4)호 (가) 2장 402.의 1항 (4)호 (다)
선박 사이버보안 및 복원력 프로그램	보안 구역 경계 장치의 관리 (예: 방화벽)	402.의 1항 (5)호
네트워크 보호 안전장치 (2장 402.의 2항)		
CBS 보안 기능	서비스거부(DoS) 보호 (#24) 결정론적 출력 (#20)	3장 401.
CBS 문서	보안 기능 기술서 보안 기능 시험절차서	3장 301.의 3항 3장 301.의 4항
선박 설계 문서	선박 사이버복원력 시험절차서	2장 402.의 2항 (4)호 (다)
선박 사이버보안 및 복원력 프로그램		
안티바이러스, 안티멀웨어, 안티스팸 및 악성코드로부터 기타 보호 (2장 402.의 3항)		
CBS 보안 기능	악성코드 보호(#18)	3장 401.
CBS 문서	보안 기능 기술서 보안 기능 시험절차서	3장 301.의 3항 3장 301.의 4항
선박 설계 문서	설계 기술서 선박 사이버복원력 시험절차서	2장 402.의 3항 (4)호 (가) 2장 402.의 3항 (4)호 (다)
선박 사이버보안 및 복원력 프로그램	멀웨어 보호 관리	2장 402.의 3항 (5)호
접근 통제 (2장 402.의 4항)		
CBS 보안 기능	인간 사용자 식별 및 인증 (#1) 계정 관리 (#2) 식별자 관리 (#3) 인증자 관리 (#4) 권한부여 시행 (#8)	3장 401.
CBS 문서	보안 기능 기술서 보안 기능 시험절차서	3장 301.의 3항 3장 301.의 4항
선박 설계 문서	설계 기술서 선박 사이버복원력 시험절차서	2장 402.의 4항 (4)호 (가) 2장 402.의 4항 (4)호 (다)
선박 사이버보안 및 복원력 프로그램	기밀 정보의 관리 논리적 및 물리적 접근의 관리	2장 402.의 4항 (5)호
무선 통신 (2장 402.의 5항)		

CBS 보안 기능	무선 접근 관리 (#5) 무선 사용 통제 (#9)	3장 401.
CBS 문서	보안 기능 기술서 보안 기능 시험절차서	3장 301.의 3항 3장 301.의 4항
선박 설계 문서	설계 기술서 선박 사이버복원력 시험절차서	2장 402.의 5항 (4)호 (가) 2장 402.의 5항 (4)호 (다)
선박 사이버보안 및 복원력 프로그램		
원격 접근 통제 및 비신뢰 네트워크에서 통신 (2장 402.의 6항)		
CBS 보안 기능	다중요소 인증 (#31) 소프트웨어 프로세스 및 장치 식별 및 인증 (#32) 실패한 로그인 시도 (#33) 시스템 사용 알림 (#34) 비신뢰 네트워크를 통한 접근 (#35) 명시적 접근 요청 승인 (#36) 원격 세션 종료 (#37) 암호 무결성 보호 (#38) 입력 검증 (#39) 세션 무결성 (#40) 세션 ID 무효화 (#41)	3장 402.
CBS 문서	보안 기능 기술서 보안 기능 시험절차서	3장 301.의 3항 3장 301.의 4항
선박 설계 문서	설계 기술서 선박 사이버복원력 시험절차서	2장 402.의 6항 (4)호 (가) 2장 402.의 6항 (4)호 (다)
선박 사이버보안 및 복원력 프로그램	비신뢰 네트워크를 통한 원격 접근 및 통신의 관리	2장 402.의 6항 (5)호
모바일 및 휴대용 장치의 사용 (2장 402.의 7항)		
CBS 보안 기능	휴대용 장치의 사용 통제 (#10)	3장 401.
CBS 문서	보안 기능 기술서 보안 기능 시험절차서	3장 301.의 3항 3장 301.의 4항
선박 설계 문서	설계 기술서 선박 사이버복원력 시험절차서	2장 402.의 7항 (4)호 (가) 2장 402.의 7항 (4)호 (다)
선박 사이버보안 및 복원력 프로그램	모바일 및 휴대용 장치의 관리	2장 402.의 7항 (5)호
네트워크 운영 감시 (2장 403.의 1항)		
CBS 보안 기능	휴대용 장치의 사용 통제 (#10) 감사가능 사건 (#13) 서비스 거부(DoS) 보호 (#24) 과도한 대역폭 사용 경고 (6편 2장 4절)	3장 401.
CBS 문서	보안 기능 기술서 보안 기능 시험절차서	3장 301.의 3항 3장 301.의 4항
선박 설계 문서	선박 사이버복원력 시험절차서	2장 403.의 1항 (4)호 (다)
선박 사이버보안 및 복원력 프로그램	사고 대응 계획	2장 403.의 1항 (5)호
CBS 및 네트워크의 검증 및 진단 기능 (2장 403.의 2항)		
CBS 보안 기능	보안 기능성 검증 (#19)	3장 401.
CBS 문서	보안 기능 기술서 보안 기능 시험절차서 유지보수 및 검증 계획	3장 301.의 3항 3장 301.의 4항 3장 301.의 7항
선박 설계 문서	선박 사이버복원력 시험절차서	2장 403.의 2항 (4)호 (다)
선박 사이버보안 및 복원력 프로그램	보안 기능 검증	2장 403.의 2항 (5)호

사고 대응 계획 (2장 404.의 1항)		
CBS 보안 기능		
CBS 문서	보안 기능 기술서 보안 기능 시험절차서 사고 대응 및 복구 계획 지원 정보	**3장** 301.의 3항 **3장** 301.의 4항 **3장** 301.의 8항
선박 설계 문서	설계 기술서 선박 사이버복원력 시험절차서	**2장** 404.의 1항 (4)호 (가)
선박 사이버보안 및 복원력 프로그램	사고 대응 계획	**2장** 404.의 1항 (5)
로컬, 독립 및/또는 수동 운전 (2장 404.의 2항)		
CBS 보안 기능		
CBS 문서	보안 기능 기술서 보안 기능 시험절차서 사고 대응 및 복구 계획 지원 정보	**3장** 301.의 3항 **3장** 301.의 4항 **3장** 301.의 8항
선박 설계 문서	설계 기술서 선박 사이버복원력 시험절차서	**2장** 404.의 2항 (4)호 (가) **2장** 404.의 2항 (4)호 (다)
선박 사이버보안 및 복원력 프로그램	사고 대응 계획	**2장** 404.의 2항 (5)
네트워크 격리 (2장 404.의 3항)		
CBS 보안 기능		
CBS 문서	보안 기능 기술서 보안 기능 시험절차서 사고 대응 및 복구 계획 지원 정보	**3장** 301.의 3항 **3장** 301.의 4항 **3장** 301.의 8항
선박 설계 문서	설계 기술서 선박 사이버복원력 시험절차서	**2장** 404.의 3항 (4)호 (가) **2장** 404.의 3항 (4)호 (다)
선박 사이버보안 및 복원력 프로그램	사고 대응 계획	**2장** 404.의 3항 (5)호
최소 위험 상태로의 대비책 (2장 404.의 4항)		
CBS 보안 기능	결정론적 출력 (#20)	**3장** 401.
CBS 문서	보안 기능 기술서 보안 기능 시험절차서 사고 대응 및 복구 계획 지원 정보	**3장** 301.의 3항 **3장** 301.의 4항 **3장** 301.의 8항
선박 설계 문서	설계 기술서 선박 사이버복원력 시험절차서	**2장** 404.의 4항 (4)호 (가) **2장** 404.의 4항 (4)호 (다)
선박 사이버보안 및 복원력 프로그램	사고 대응 계획	**2장** 404.의 4항 (5)호
복구 계획 (2장 405.의 1항)		
CBS 보안 기능		
CBS 문서	보안 기능 기술서 보안 기능 시험절차서 사고 대응 및 복구 계획 지원 정보	**3장** 301.의 3항 **3장** 301.의 4항 **3장** 301.의 8항
선박 설계 문서	설계 기술서 선박 사이버복원력 시험절차서	**2장** 405.의 1항 (4)호 (가) **2장** 405.의 1항 (4)호 (다)
선박 사이버보안 및 복원력 프로그램	복구 계획	**2장** 405.의 1항 (5)호
백업 및 복구 기능 (2장 405.의 2항)		
CBS 보안 기능	시스템 백업 (#26) 시스템 복구 및 복원 (#27)	**3장** 401.

CBS 문서	보안 기능 기술서 보안 기능 시험절차서 사고 대응 및 복구 계획 지원 정보	3장 301.의 3항 3장 301.의 4항 3장 301.의 8항
선박 설계 문서	선박 사이버복원력 시험절차서	2장 405.의 2항 (4)호 (다)
선박 사이버보안 및 복원력 프로그램	복구 계획	2장 405.의 2항 (5)호
제어된 셧다운, 재설정, 롤백 및 재시작 (2장 405.의 3항)		
CBS 보안 기능	시스템 복구 및 복원 (29번)	3장 401.
CBS 문서	보안 기능 기술서 보안 기능 시험절차서 사고 대응 및 복구 계획 지원 정보	3장 301.의 3항 3장 301.의 4항 3장 301.의 8항
선박 설계 문서	설계 기술서 선박 사이버복원력 시험절차서	2장 405.의 3항 (4)호 (가) 2장 405.의 3항 (4)호 (다)
선박 사이버보안 및 복원력 프로그램	복구 계획	2장 405.의 3항 (5)호
요건의 적용으로부터 CBS의 제외를 위한 위험도 평가 (1장 3절)		
CBS 보안 기능		
CBS 문서		
선박 설계 문서	CBS의 제외를 위한 위험도 평가	2장 202.의 1항 (1)호 (라)
선박 사이버보안 및 복원력 프로그램		

인 쇄 2024년 3월 1일
발 행 2024년 3월 1일

선박 및 시스템의 사이버복원력 지침

발행인 이 형 철
발행처 한 국 선 급
부산광역시 강서구 명지오션시티 9로 36
전화 : 070-8799-7114
FAX : 070-8799-8999
Website : http://www.krs.co.kr

신고번호 : 제 2014-000001호 (93. 12. 01)