CIRCULAR

36 Myeongji ocean city 9-ro,
Gangseo-gu, Busan, 46762
Republic of Korea

Phone : +82-70-8799-8796
Fax : +82-70-8799-8419
E-mail: jmkim@krs.co.kr
Person in charge : KIM Jeongmin

No : 2023-14-E
Date : 2023.09.26

To : 전 검사원 및 관련업체

제 목 (Subject)	**9.183 선급기술규칙 제/개정사항 시행 알림** **- 사이버 복원력 지침**
적 용 (Application)	**1항 및 첨부의 각 적용일자 참조**

1. IACS Res. 및 선급기술규칙 제/개정 요청사항을 반영하여, 다음의 선급기술규칙을 첨부와 같이 제정하였음을 알려드리오니 해당 적용일자에 따라 관련 업무에 적용하시기 바랍니다.

개정된 선급기술규칙	적용일자	반영된 IACS Res.
사이버 복원력 지침	2024.1.1 (건조계약일 기준)	IACS UR E26, E27(New Apr 2022)

2. 아울러, 이 내용은 2024년 상반기 중 발행되는 2024년판 선급기술규칙에 반영될 예정임을 알려드립니다.

첨부: 선급기술규칙의 개정사항(국/영문)---------- 1부. (끝)

사이버 복원력 지침에 대한 제정(안)

2023. 9.

- 주 요 개 정 내 용 -

(1) IACS UR E26, E27 반영 <2024.01.01.일자 시행사항(건조계약일 기준)>

◉ UR E26 (New Apr 2022): 선박의 사이버 복원력

◉ UR E27 (New Apr 2022): 선내 시스템 및 장비의 사이버 복원력

2024.01.01.일자 시행사항

(건조계약일 기준)

2023

사이버 복원력 지침

한 국 선 급

2023

사이버 복원력 지침

GC-44-K

한 국 선 급

“사이버 복원력 지침”의 적용

1. 이 지침은 별도로 명시하는 것을 제외하고 2024년 1월 1일 이후 건조계약 또는 검사신청 되는 선박 및 기자재에 적용한다.

차 례

제 1 장 일반사항

제 1 절 일반사항

101. 도입

상용 제품(commercial-off-the-shelf)의 선내 광범위한 사용과 함께 선박 내 컴퓨터 시스템들의 상호 연결은 직원 데이터, 인명 안전, 선박 안전에 영향을 미치고 해양 환경을 위협하는 공격의 가능성을 열어준다. 공격자는 선내 시스템과 외부 세계 사이에 네트워크 연결 또는 기타 인터페이스가 있는 모든 곳에서 그들의 목표를 달성하기 위해 사람과 기술의 어떤 조합을 표적으로 삼을 수 있다. 현재 및 새로운 위협으로부터 선박과 일반적인 해운을 보호하려면 지속적으로 진화하는 다양한 조치가 필요하다. 실질적으로 사이버 복원력이 있다고 설명할 수 있는 선박을 제공하기 위해 공통의 최소 기능 및 성능 기준들을 수립해야 한다.

사이버 복원력을 가진 선박을 건조하고 운항하기 위해서 목표 기반 접근 방식을 이용하여 전체 위협 표면에 일관되게 적용되는 최소 요구사항이 필요하다.

102. 목적

1. 이 지침의 목표는 이해 관계자에게 사이버 복원력을 가진 선박으로 이어지는 기술적 수단을 제공할 목적으로 선박의 사이버 복원력에 대한 최소 세트의 요구사항을 제공하는 것이다.
2. 이 지침은 사이버 복원력에 대한 집합체로서 선박을 목표로 하며, 선내 시스템, 장비 및 구성품들의 사이버 복원력을 다루는 산업 표준과 상호보완적 적용을 위한 기반으로 의도된다.
3. 선내 시스템 및 장비의 사이버 복원력에 대한 최소 요구사항은 이 지침 3장에 에 기술되어 있다. 지침 3장의 요건을 충족하는 시스템 및 장비는 지침 2장을 만족하는 사이버복원력 선박을 만족하는 필요한 보안 역량을 가질 것이다.

103. 적용

1. 적용 일반

(1) 이 지침 요건은 선급 및 강선규칙 1편에 따라 우리 선급에 등록하고 유지하는 선박에 대하여 적용한다.

(2) 이 지침 3장의 요건은 2장의 적용 범위에 포함되는 선내 시스템 및 장비에 적용한다.

(3) 이 지침의 관련 요건에 추가하여 선급 및 강선규칙 6편 2장의 관련 규정을 만족해야 한다.

(4) 이 지침에서 별도로 규정하고 있는 사항 외에는 선급 및 강선규칙의 관련 규정을 따른다.

2. 이 지침은 다음에 적용한다.

(1) 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 컴퓨터기반시스템. 특히, 다음의 선박 기능 및 시스템의 작동에 이용되는 컴퓨터기반시스템이 본선에 존재하는 경우를 고려해야 한다.

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

(2) 추가로, 다음 시스템들이 이 지침의 적용 범위에는 포함되어야 한다:

(가) 협약에서 요구되는 항해시스템
(나) 선급 규칙 및 협약에서 요구되는 내외부 통신 시스템
항해 및 무선통신 시스템의 경우 IEC 61162-460 또는 IEC 63154와 같은 표준의 적용이 이 지침에 포함된 요구사항의 적용으로 얻게 되는 사이버 복원력과 동등 또는 이상을 제공하는 경우 이 지침의 대안으로 사용될 수 있다. 어떠한 경우에도 3장 4절의 요구사항을 준수해야 한다.

(3) 이 지침의 범위에 속하는 컴퓨터기반시스템으로부터 다른 시스템으로의 IP 기반 통신 인터페이스. 이러한 시스템의 예는 다음과 같으며 이에 국한되지 않는다.
(가) 여객 및 방문객 서비스 및 관리 시스템
(나) 여객 대상 네트워크
(다) 관리 네트워크
(라) 선원 복지 시스템
(마) 영구 또는 임시로(예: 유지보수 동안) OT 시스템에 연결되는 다른 시스템
이 지침에서 고려되는 사이버 사고는 105.에서 정의된 선내 OT 시스템을 대상으로 하는 모든 공격 움직임으로 인해 발생하는 사건이다.

104. 선급부호

이 지침이 요건에 적합한 선박은 다음의 선급부호를 부여할 수 있다.

1. Cyber Resilience : **2장**의 관련 요건에 따라 선박의 수명주기 동안 사이버복원력을 가진 선박

105. 용어의 정의

1. **공격 표면(Attack surface):** 권한이 없는 사용자가 시스템에 접근하여 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.
2. **가용성(Availability):** 자산이 적절한 시간에 인가된 당사자에게 접근 가능하여야 하는 것을 말한다.
3. **인증(Authentication):** 주장된 객체(entity)의 특성이 올바르다는 보증을 제공한다.
4. **보상 조치(Compensating countermeasure):** 하나 이상의 보안 요구사항을 만족하기 위한 고유 보안 기능을 대신하거나 추가하여 도입된 대책을 말한다.
5. **컴퓨터기반시스템(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 컴퓨터기반시스템에는 IT 및 OT 시스템을 포함한다. 선내 컴퓨터기반시스템에는 네트워크를 통해 연결된 하부 시스템의 조합일 수 있다. 선내 컴퓨터기반시스템에는 직접 또는 공용 통신 수단(예: 인터넷)을 통해 육상의 컴퓨터기반시스템, 다른 선박의 컴퓨터기반시스템 및/또는 기타 설비에 연결될 수 있다.
6. **컴퓨터 네트워크:** 합의된 통신 프로토콜 수단으로 전자적으로 데이터를 통신할 목적으로 두 대 이상의 컴퓨터 간의 연결을 말한다.
7. **기밀성(Confidentiality):** 자산이 인가된 당사자에 의해서만 접근하는 것을 보장하는 것을 말한다.
8. **통제(Control):** 정책, 절차, 지침서, 실무서(practice) 또는 조직도를 포함하여 리스크를 관리하는 수단으로서, 행정, 기술적, 관리, 또는 법적 성격을 가질 수 있다.
9. **사이버 공격(Cyber attack):** IT 및 OT 시스템, 컴퓨터 네트워크 및/또는 개인용 컴퓨터 장치를 표적으로 하고 회사 및 배송 시스템과 데이터를 손상, 파괴 또는 접근을 시도하는 모든 유형의 공격적 사이버 기동.
10. **사이버 사고(Cyber incident):** 선내 시스템, 네트워크 및 컴퓨터 또는 이들이 처리, 저장 또는 전송하는 정보에 실제로 또는 잠재적으로 부정적인 결과를 초래하고 결과를 완화하기 위해 대응 조치가 필요할 수 있는 하나 이상의 선내 컴퓨터기반시스템를 표적으로 삼거나 영향을 미치는 의도적이든 의도적이지 않든 모든 공격적 사이버 기동으로 인해 발생하는 사건을 말한다. 사이버 사고에는 선내 컴퓨터기반시스템에서 생성, 보관 또는 사용되거나 해당 시스템을 연결하는 네트워크에서 전송되는 정보의 무단 접근, 오용, 수정, 파괴 또는 부적절한 공개를 포함한다. 사이버 사고에는 시스템 장애는 포함하지 않는다.
11. **사이버 복원력(Cyber resilience):** 선박의 안전한 운항을 위해 사용되는 운영 기술(OT)의 중단 또는 손상으로 인해 발생하는 사이버 사고의 발생을 줄이고 그 영향을 완화하는 능력으로, 잠재적으로 인명 안전, 선박의 안전 및/또는 환

경에 대한 위협으로 이어질 수 있는 위험한 상황을 초래할 수 있는 사이버 사고의 발생을 줄이고 그 영향을 완화하는 능력을 말한다.

12. **심층 방어**(Defence in depth): 인적, 기술 및 운영 능력을 통합하여 조직의 여러 계층과 임무에 걸쳐 다양한 장벽을 세우기 위한 정보 보안 전략을 말한다.
13. **비무장 구역**(Demilitarized zon): 조직의 외부 대면 서비스를 외부 네트워크에 포함하고 노출하는 물리적 또는 논리적 경계 네트워크 세그먼트. 이것의 목적은 외부 정보 교환에 대한 내부 네트워크의 보안 정책을 시행하고 외부 공격으로부터 내부 네트워크를 보호하면서 외부의 신뢰할 수 없는 소스에 공개 가능한 정보에 대한 제한된 접근을 제공하기 위함이다.
14. **중요용도**(Essential System): 선박의 추진력, 조타 및 안전에 필수적인 서비스 제공에 기여하는 컴퓨터 기반 시스템. 중요 용도는 “일차 중요용도” 및 “이차 중요용도”로 구성된다. 일차 중요용도는 추진 및 조타를 유지하기 위해 연속적으로 운전이 필요한 용도를 말한다. 이차 중요용도는 추진 및 조타를 유지하기 위해 반드시 연속적으로 운전할 필요는 없지만, 선박의 안전을 유지하기 위해 필요한 서비스이다.
15. **방화벽**(Firewall): 사전에 정의된 규칙을 통해 제어되는 수신 및 발신 네트워크 트래픽을 감시하고 제어하는 논리적 또는 물리적 장벽을 말한다.
16. **펌웨어**(Firmware): 엔지니어링 제품 및 시스템의 제어, 감시 및 데이터 조작을 제공하는 전자 장치에 내장된 소프트웨어. 이러한 기능은 일반적으로 자체적으로 포함되므로 사용자가 조작할 수 없다.
17. **강화**(Hardening): 강화는 공격 표면을 줄임으로써 시스템의 취약성을 줄이는 방법이다.
18. **정보기술**(Information Technology): 운영 기술(OT)과는 달리 데이터를 정보로 사용하는 데 중점을 둔 장치, 소프트웨어 및 관련 네트워크를 말한다.
19. **초기 인증자 내용**(Initial Authenticator Content): 시스템의 초기 설치 및 구성을 위한 공장 기본 인증 자격증명(예: 초기 암호, 토큰 등)을 말한다.
20. **통합 시스템**(Integrated system): 하나 이상의 지정된 목적을 달성하기 위해 구성된 다수의 상호 작용하는 하위 시스템 및/또는 장비를 결합한 시스템을 말한다.
21. **무결성**(Integrity): 자산이 인가된 당사자에 의해서 인가된 방법으로만 변경 가능한 것을 말한다. 이는 자산의 완전성과 정확성을 보장하는 것을 의미한다.
22. **네트워크 스위치(이하 스위치)**: 패킷 교환을 사용하여 데이터를 수신, 처리 및 대상 장치로 전달함으로써 컴퓨터 네트워크에서 장치를 서로 연결하는 장치를 말한다.
23. **논리적 네트워크 세그먼트**(Logical network segment): “네트워크 세그먼트”와 동일하지만 두 개 이상의 논리적 네트워크 세그먼트가 동일한 물리적 구성 요소를 공유하는 것이다.
24. **네트워크 세그먼트**(Network segment): 동일한 네트워크 주소 계획을 공유하는 노드의 수집. 하나의 네트워크 세그먼트는 하나의 방송 도메인이다.
    (비고) TCP/IP: 네트워크 주소 계획에는 해당 IP 주소와 네트워크 마스크가 접두사로 붙는다. 네트워크 세그먼트 간의 통신은 네트워크 계층(OSI 3계층)에서 라우팅 서비스를 사용해야만 가능하다.
25. **공격적 사이버 기동**(Offensive Cyber manoeuvre): OT 또는 IT 시스템의 거부, 성능 저하, 중단, 파괴 또는 조작을 초래하는 작업을 말한다.
26. **운영 기술**(OT, Operational Technology): 선내 시스템을 감시하고 제어하는 장치, 센서, 소프트웨어 및 관련 네트워킹. 운영 기술 시스템은 물리적 프로세스를 제어하거나 감시하기 위한 데이터 사용에 중점을 둔 것으로 고려할 수 있다.
27. **패치**(Patches): 보안 취약성 및 기타 버그를 해결하거나 운영 체제 또는 응용 프로그램을 개선하기 위해 설치된 소프트웨어 또는 지원 데이터를 업데이트하도록 설계된 소프트웨어를 말한다.
28. **물리적 네트워크 세그먼트**(Physical network segment): "네트워크 세그먼트"와 동일. 물리적 구성품은 다른 네트워크 세그먼트와 공유하지 않는다.
    (비고) TCP/IP:분할(Segmentation)은 네트워크를 여러 물리적 세그먼트 또는 서브넷으로 나눈다. 들어오고 나가는 패킷이 제어되며, 연결 및 데이터 교환은 네트워크 계층(OSI 3계층)과 응용 프로그램 수준(OSI 7계층) 모두에서 허용되거나 차단된다. 트래픽 관리와 패킷 필터링은 모두 단일 소프트웨어 또는 하드웨어 장비로 관리될 수 있다.
29. **프로토콜**(Protocol): 네트워크 상의 컴퓨터가 통신하는 데 사용하는 공통 규칙 및 신호 집합. 프로토콜을 통해 데이터 통신, 네트워크 관리 및 보안을 수행하는 것을 허용한다. 선내 네트워크는 일반적으로 TCP/IP 스택 또는 다양한 필드버스를 기반으로 하는 프로토콜을 구현한다.

30. **복구(Recovery):** 복원력 계획을 유지하고 사이버 보안 사건으로 인해 손상된 기능이나 서비스를 복원하기 위한 적절한 활동을 개발하고 구현한다. 복구 기능은 사이버 보안 사건의 영향을 줄이기 위해 적시에 정상 작동으로 복귀하도록 지원한다.
31. **보안구역(Security zone): 2장**의 적용 범위에 있는 동일한 접근 통제 정책이 필요한 연결된 컴퓨터기반시스템 모음. 각 구역은 접근 통제 정책이 적용되는 단일 인터페이스 또는 인터페이스 그룹으로 구성된다.
32. **선박 설계자/조선소:** 개인 또는 조직으로 아래와 같이 정의한다.
(1) 개념, 계약 및 상세 설계 관리를 포함하여 선주가 제공한 선박 사양을 완전한 선박 프로젝트로 발전시키는 프로세스를 구현, 및/또는
(2) 선박 건조를 담당하고 선박 건조 중 해당 규칙 및 협약의 요구사항을 이행하고 선박 설계 사양을 구현하는 책임이 있음, 및/또는
(3) 공급자가 제공한 시스템 및 제품을 통합 시스템으로 통합하는 일을 담당.
33. **선주/회사:** 선박의 소유자 또는 관리자, 대리인 또는 나용선 용선자(bareboat charterer)와 같이 선주로부터 선박 운항에 대한 책임을 지고 모든 부수적 의무와 책임을 인수하기로 동의한 기타 조직 또는 개인. 초기 건조 중에는 선주는 조선소 또는 시스템 통합업체일 수 있으며, 선박 인도 후, 선주는 선박 관리 회사에 일부 책임을 위임할 수 있다.
34. **공급자:** 시스템 또는 하부시스템과 함께 작동하며 응용 프로그램, 임베디드 장치, 네트워크 장치, 호스트 장치 등으로 구성된 하드웨어 및/또는 소프트웨어 제품, 시스템 구성품 또는 장비(하드웨어 또는 소프트웨어)의 제조업체 또는 제공자. 공급자는 프로그램 가능한 장치, 하부 시스템 또는 시스템을 시스템 통합자에 제공할 책임이 있다.
35. **시스템:** 하나 이상의 특정 목적을 달성하기 위해 구성된 상호작용하는 프로그램밍 가능한 장치 및/또는 하부시스템의 조합을 말한다.
36. **시스템 카테고리(I, II, III): 선급 및 강선규칙 6편 2장 4절**에서 정의된 시스템 기능에 미치는 영향을 기반한 시스템 카테고리를 말한다.
37. **시스템 통합자(System Integrator):** 공급자가 제공한 시스템 및 제품을 선박 사양서의 요구사항에 따라 요구되는 시스템에 통합하고 통합 시스템을 제공하는 책임이 있는 특정 개인 또는 조직을 말하며, 시스템 통합자는 선박의 시스템 통합을 담당할 수도 있다. 이 역할은 대체 조직이 책임을 특별히 계약/위임받지 않는 한 조선소에서 수행한다.
38. **신뢰할 수 없는 네트워크(Untrusted network):** 이 지침의 적용 범위를 벗어난 모든 네트워크를 말한다.
39. **가상 사설 네트워크(VPN, Virtual Private Network):** 기존 물리적 네트워크 위에 구축한 가상 네트워크로서 전용 회선의 느낌을 주는 터널링, 보안 통제 및 종점 주소 변환을 활용하여 네트워크 또는 장치 사이에 전송되는 데이터에 대한 보안 통신 터널을 제공한다.

106. 약어

1. **IT:** Information Technology
2. **Switch:** Network Switch
3. **OT:** Operational Technology
4. **VPN:** Virtual Private Network

107. 참조문서

컴퓨터 기반 시스템 및 사이버 복원력에 대한 다음의 추가의 IACS 문서 및 국제표준을 참조한다.

1. IACS UR E22: 컴퓨터 기반 시스템의 선내 사용 및 적용
2. IACS UR E26: 선박의 사이버 복원력
3. IACS UR E27: 선내 시스템 및 장비의 사이버 복원력
4. IACS Rec.166: 사이버 복원력
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 장 선박의 사이버 복원력 요건

제 1 절 요구사항의 목표와 구성

101. 주요 목표

1. 주요 목표는 사이버 위험에 운영상 복원력 있는 안전하고 확실한(secure) 운항을 지원하는 것이다.
2. 효과적인 사이버 위험 관리 시스템을 통해 안전한 운항을 할 수 있다. 사이버 위험에 복원력이 있는 안전하고 확실한 운항을 지원하기 위해 사이버 위험 관리를 위한 다음의 하위 목표는 102.에 나열된 5가지 기능 요소에 정의되어 있다.

102. 기능 요소별 하위 목표

1. **식별:** 선내 시스템, 사람, 자산, 데이터 및 기능에 대한 사이버 보안 위험을 관리하기 위한 조직적 이해를 개발한다.
2. **보호:** 사이버 사고로부터 선박을 보호하고 선박 운항의 연속성을 최대화하기 위한 적절한 보호 장치를 개발 및 구현한다.
3. **탐지:** 선내 사이버 사고의 발생을 탐지하고 식별하기 위한 적절한 조치를 개발하고 구현한다.
4. **대응:** 선내에서 탐지된 사이버 사고에 대한 조치를 취하기 위한 적절한 조치 및 활동을 개발 및 구현한다.
5. **복구:** 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 위험 관리 프레임워크의 일부로 간주되어야 한다.

103. 요구사항의 구성

1. 요구사항은 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 수용 가능한 수준의 복원력을 가능하게 하고 모든 유형의 선박/장치에 적용 가능한 방식으로 모든 유형의 선박에 일관된 구현을 가능하게 하고 적용할 수 있도록 하기 위함이다.
2. 각 요구사항에 대한 이유가 제공되었다.
3. 선박 수명의 각 단계와 해당 단계에 참여하는 관련 이해관계자에 대해 수행해야 할 조치와 사용 가능한 문서 요약도 제공되었다.
4. 성능평가 및 시험을 위한 기준 또한 제공되었다.

제 2 절 요구사항

201. 일반사항

1. 이 절은 **102.**에서 식별된 5가지 기능 요소에 따라 구성된 **101.**에 정의된 주요 목표를 달성하기 위해 충족되어야 하는 요구사항들을 포함한다.
2. 요구사항은 선박의 설계, 건조 및 운영에 관련된 이해 관계자의 책임하에 충족되어야 한다. 그 중 다음 이해 관계자들이 식별될 수 있다.

(1) 선주/회사
(2) 선박 설계사/조선소
(3) 시스템 통합자
(4) 공급자
(5) 선급

202. 식별

'식별' 기능 요소에 대한 요구사항은 다음을 식별하는 것을 목표로 한다.: 한 편으로는 선내 컴퓨터기반시스템, 이들의 독립성 및 관련 정보 흐름; 다른 한편으로는 관리, 운영 및 거버넌스, 역할 및 책임과 관련된 핵심 자원

1. 선내 컴퓨터기반시스템 및 네트워크 목록(Inventory)

(1) 요구사항

2장의 적용 범위에 있는 컴퓨터기반시스템의 하드웨어 및 소프트웨어(응용 프로그램, 운영 체제, 만약 있다면, 펌웨어 및 기타 소프트웨어 구성 요소를 포함)과 이러한 시스템을 서로 간 및 선내 다른 컴퓨터기반시스템 또는 육상에 연결하는 네트워크의 목록은 선박의 전체 수명 동안 제공되고 최신으로 유지되어야 한다.

(2) 근거

OT 시스템에 사용되는 선내 컴퓨터기반시스템과 관련 소프트웨어 목록은 선박의 사이버 복원력을 효과적으로 관리하는 데 필수적이며, 모든 컴퓨터기반시스템이 잠재적인 취약 포인트가 되는 주요 원인이다. 사이버 범죄자들은 시스템을 해킹하기 위해 미확인된 오래된 하드웨어와 소프트웨어를 악용할 수 있다. 또한, 컴퓨터기반시스템 자산을 관리함으로써 회사는 선박 안전 목표에 대한 각 시스템의 중요성(criticality)을 이해할 수 있다.

(3) 세부 요구사항

(가) 선내 컴퓨터기반시스템 목록은 최소한 **1장 103.**의 **2항** (2)호 및 (3)호에 언급된 컴퓨터기반시스템들이 포함되어야 한다.

(나) 목록은 선박의 전체 수명 동안 업데이트가 유지되어야 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 허가된 사람만으로 제한하기 위한 특별한 조치를 취해야 한다.

(라) 하드웨어

하드웨어에 대한 선박 자산 목록에 최소한 다음 정보가 포함되어야 한다.

(a) 각 컴퓨터기반시스템에 대한 간략한 기능 설명 및 기술적 특징(브랜드, 제조업체, 모델, 주요 기술 데이터)과 함께 이것의 목적에 대한 간략한 설명

(b) 선내 다양한 컴퓨터기반시스템들 및 컴퓨터기반시스템의 외부 장치 또는 네트워크 사이의 논리적 및 물리적 연결을 식별하는 블록 다이어그램, 컴퓨터기반시스템을 연결하는 네트워크의 토폴로지 및 각 노드의 의도된 기능.

(c) 스위치, 라우터, 허브, 게이트웨이 등과 같은 네트워크 장치의 경우, 연결된 서브 네트워크에 대한 설명, IP 범위, 연결된 노드의 MAC 주소(또는 네트워크 내 사용되는 프로토콜에 특정한 주소/식별자)

(d) 모든 의도된 작동 모드에서 각 네트워크의 주요 특징(예: 사용된 프로토콜) 및 통신 데이터 흐름(예: 데이터 흐름 다이어그램)

(e) 컴퓨터기반시스템의 물리적 위치 및 네트워크 접근 포인트의 물리적 위치를 포함하여, 선내 컴퓨터기반시스템을 연결하는 각 디지털 네트워크의 물리적 레이아웃을 설명하는 지도.

상기 정보를 기반으로 시스템 분류 및 보안 구역이 컴퓨터기반시스템과 관련될 수 있고 목록에 기록될 수 있다.

(마) 소프트웨어

소프트웨어에 대한 선박 자산 목록은 각 소프트웨어 응용 프로그램, 운영 체제, 펌웨어 등에 대하여 최소한 다음의

정보들을 포함하여야 한다.

(a) 소프트웨어가 설치된 컴퓨터기반시스템 목적의 간략한 설명, 기술적 특징(브랜드, 제조업체, 모델, 주요 기술 데이터) 및 특정 기능의 간략한 설명

(b) 버전 정보, 초기 설치 및 만료 일자가 포함된 라이선스 정보, 업데이트 로그

(c) 유지보수 정책(예: 현장 대 원격, 주기적 대 임시적 등) 및 책임자

(d) 역할 및 책임을 포함한 접근 통제 정책(예: 읽기, 쓰기 및 실행 권한 포함).

203. 보호

보호 기능 요소에 대한 요구사항은 잠재적 사고의 영향을 제한하거나 억제하는 능력을 지원하는 적절한 보호 장치의 개발 및 구현을 목표로 한다.

1. 보안 구역 (Security Zones)

(1) 요구사항

(가) **2장**의 적용 범위에 있는 모든 컴퓨터기반시스템은 잘 정의된 보안 통제 정책 및 보안 기능이 있는 보안 구역으로 그룹화해야 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.

(나) 오직 명시적으로 허용된 트래픽만 보안 구역 경계를 통과해야 한다.

(2) 근거

(가) 네트워크는 방화벽 경계로 보호되고 들어오는 트래픽을 모니터링하기 위해 침입 탐지 시스템(IDS) 또는 침입 방지 시스템(IPS)을 포함할 수 있지만, 경계를 위반하는 것은 항상 가능하다. 네트워크 세분화는 공격자가 전체 네트워크를 통한 공격을 수행하는 것을 더 어렵게 만든다.

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

(3) 세부 요구사항

(가) 보안 구역에는 여러 개의 컴퓨터기반시스템과 네트워크가 포함될 수 있으며, 이들 모두 지침에 제공된 보안 요구사항을 만족해야 한다.

(나) 보안 구역의 네트워크는 논리적 또는 물리적으로 다른 구역 또는 네트워크와 분할되어야 한다. **4항** (3)호 또한 참조)

(다) 요구하는 안전 시스템을 제공하는 컴퓨터기반시스템은 별도의 보안 구역으로 그룹화되어야 하며 다른 보안 구역과 물리적으로 분할되어야 한다.

(라) 항해 및 통신 시스템은 기관 또는 화물 시스템과 동일한 보안 구역 내에 있지 않아야 한다.

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

(바) **2장**의 적용 범위 밖에 있는 다른 OT 시스템 또는 컴퓨터기반시스템은 **2장**에서 요구하는 보안 구역과 물리적으로 분할되어야 한다. 대안적으로 이러한 OT 시스템이 구역에서 요구하는 것과 동일한 요구사항을 만족하는 경우, 다른 OT 시스템이 보안 구역의 일부로 허용된다.

(사) 구역 내 컴퓨터기반시스템의 주요 기능에 영향을 주지 않고 보안 구역을 수동으로 격리하는 것이 가능해야 한다.

(아) 보안 통제 정책의 정의에서 네트워크 상 접근하거나 작동하도록 허용된 기능은 기술 절차 및 역할과 연관되어야 한다.

2. 네트워크 보호 안전장치(safeguard)

(1) 요구사항

(가) **2장**의 적용 범위에 있는 컴퓨터기반시스템을 연결하는 네트워크는 방화벽 또는 **1항**에서 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.

(나) **2장**의 범위에 있는 컴퓨터기반시스템는 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.

(2) 근거

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

(나) 네트워크 보호를 다룰 때 고려해야 할 많은 계층이 있다. 공격은 네트워크 계층 모델의 모든 계층에서 발생할 수 있으므로, 네트워크 하드웨어, 소프트웨어 및 정책은 각 영역을 고려하도록 설계되어야 한다.

(다) 물리적 및 기술적 보안 통제는 권한이 없는 직원으로부터 네트워크 구성 요소에 물리적으로 접근하는 것을 방지하고 저장되거나 네트워크를 통해 전송 중에 있는 데이터를 보호하도록 설계되며, 절차적 보안 통제는 사용자 행동을 통제하는 보안 정책 및 프로세스로 구성된다.

(3) 세부 요구사항

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 포함되어야 한다. 데이터 흐름 속도의 추정은 최소한 네트워크 용량, 의도된 애플리케이션 및 데이터 포맷에 대한 데이터 속도 요구사항을 고려해야 한다.

3. 안티바이러스, 안티멀웨어, 안티스팸 및 악성코드로부터 기타 보호

(1) 요구사항

2장의 적용 범위에 있는 컴퓨터기반시스템은 바이러스, 웜, 트로이 목마, 스파이웨어 등과 같은 악성 코드로부터 보호되어야 한다.

(2) 근거

(가) 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.

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

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

(3) 세부 요구사항

(가) 멀웨어 보호는 **2장**의 적용 범위에 있는 컴퓨터기반시스템에 구현해야 한다. 산업 표준 안티바이러스 및 안티멀웨어 소프트웨어를 사용할 수 있고 최신으로 유지 관리되는 운영 체제가 있는 컴퓨터기반시스템에는 이러한 소프트웨어 설치가 요구되는 서비스(예: 실시간 임무를 수행하는 카테고리 II 및 III 컴퓨터기반시스템)의 기능과 수준을 제공하는 컴퓨터기반시스템의 능력을 손상시키지 않는다면 안티바이러스 및 안티 멀웨어 소프트웨어가 설치되어, 유지관리 및 정기적으로 업데이트되어야 한다.

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

4. 접근 통제(Access control)

(1) 요구사항

2장의 적용 범위에 있는 컴퓨터기반시스템 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 제공해야 한다. 이러한 조치는 최소 권한 원칙에 따라 접근 수준에 대해 허가된 직원이 컴퓨터기반시스템에 접근하는 능력을 방해하지 않아야 한다.

(2) 근거

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

(나) 물리적 위협 및 관련 대응책은 ISPS 코드에서 또한 고려된다. 이와 마찬가지로 ISM 코드에는 선박의 안전한 운항과 환경 보호를 위한 지침이 포함되어 있다. ISPS 코드 및 ISM 코드의 구현은 선박 보안 계획(SSP) 및 선박 안전 관리 시스템(SMS)에 안전 중요 자산에 대한 접근 통제 지침 및 절차를 포함하는 것을 의미할 수 있다. 이 문서의 요구사항은 ISPS 및 ISM 코드의 적용에서 파생된 지침 및 절차에 대한 기술적 기반으로 간주될 수 있다.

(3) 세부 요구사항

2장의 적용 범위 내에 있는 컴퓨터기반시스템과 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.

(가) 물리적 접근 통제

카테고리II 및 카테고리III의 컴퓨터기반시스템에는 무단 접근을 예방하기 위해 일반적으로 잠겨진 방 또는 통제되는 공간 내에 위치하거나, 잠금가능 케니닛 또는 콘솔 내에 설치되어야 한다. 그러한 위치 또는 잠금가능 캐비닛/콘솔은 그러나 선박의 효과적이고 효율적인 운항을 방해하지 않도록 설치, 통합, 유지보수, 수리, 교체, 폐기 등을 위해 컴퓨터기반시스템에 접근해야 하는 선원 및 다양한 이해 관계자가 쉽게 접근할 수 있어야 한다.

(나) 방문자에 대한 물리적 접근 통제

정부관계자, 기술자, 대리인, 항만 및 터미널 공무원, 선주 대표자와 같은 방문자는 예를 들어 선내 감독하에 접근을 허용하는 경우를 제외하고 선내에서 컴퓨터기반시스템에 대한 접근에 대하여 제한되어야 한다.

(다) 네트워크 억세스 포인트의 물리적 접근 통제

(a) 카테고리II 또는 카테고리III의 컴퓨터기반시스템을 연결하는 선내 네트워크에 대한 접근 포인트는 문서화된 절차(예: 유지보수)에 따라 감독 하에 연결하는 경우를 제외하고 물리적 및/또는 논리적으로 차단되어야 한다.

(b) 모든 선내 네트워크로부터 격리된 독립의 컴퓨터, 또는 여객 오락 활동 전용 네트워크가 방문자에 의해 간헐적 연결 요청이 있는 경우(예: 문서 인쇄)에 사용되어야 한다.

(라) 이동식 매체 통제 (Removable media controls)

이동식 매체 장치의 사용에 대한 정책이 이동식 매체를 멀웨어에 대해 점검하고 디지털 서명 및 워터마크를 통해 합법적인 소프트웨어를 검증하고, 선박 시스템에 파일을 업로드하거나 선박에서 데이터를 다운로드하는 것을 허용하기 이전에 스캔하기 위한 절차와 함께 수립되어야 한다. (7항 또한 참조)

(마) 자격증명 관리 (Management of credentials)

(a) 컴퓨터기반시스템 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 더이상 필요하지 않은 경우 삭제되어야 한다.

(b) 선내 컴퓨터기반시스템에는 해당 보안 구역의 정책에 적합하지만 주요 목적에 부정적인 영향을 미치지 않는 적절한 접근 통제가 제공되어야 한다. 강력한 접근 통제가 필요한 컴퓨터기반시스템은 강력한 암호키 또는 다중요소 인증을 사용하여 보호해야 한다.

(c) 시스템 구성 설정 및 모든 데이터에 대한 전체 접근을 허용하는 관리자 권한은 회사 또는 선내에서 역할의 일부로서 이러한 특권을 사용하여 시스템에 로그온할 필요가 있는 적절하게 훈련된 직원에게만 부여되어야 한다. 관리 특권은 선내 관련자가 더 이상 승선하지 않으면 제거되어야 한다. 어떠한 경우에도 관리자 특권의 사용은 항상 이러한 접근을 요구하는 기능으로 한정되어야 한다.

(바) 최소 특권 정책 (Least privilege policy)

(a) 2장의 적용 범위 내에 있는 컴퓨터기반시스템 및 네트워크에 접근할 수 있는 모든 사용자, 프로그램 또는 프로세스는 해당 기능을 수행하는 데 필요한 최소한의 권한만 가져야 한다. 선내 시스템 및 네트워크에 접근할 수 있는 프로세스는 의도한 작업을 수행하는 데 필요한 것보다 높지 않은 권한 수준에서 작동해야 한다.

(b) 모든 새 계정 또는 프로세스 권한에 대한 기본 구성은 가능한 한 낮게 설정되어야 한다. 가능한 상향된 특권은 필요한 순간만으로 한정(예: 만료되는 권한과 1회용 자격증명만 사용)되어야 한다. 시간 경과에 따른 특권 축적은 예를 들어 사용자 및 프로세스 계정에 대한 정기적인 감사를 통해 회피해야 한다.

5. 무선 통신

(1) 요구사항

(가) **2장**의 범위 내에 있는 무선 통신 네트워크는 다음을 보장하도록 설계, 구현 및 유지 관리되어야 한다.

(a) 사이버 사고는 다른 제어 시스템으로 전파되지 않는다.

(b) 허가된 인간 사용자만 무선 네트워크에 접근할 수 있다.

(c) 허가된 프로세스 및 장치만 무선 네트워크에서 통신이 허용된다.

(d) 무선 네트워크에서 전송 중인 정보는 조작되거나 공개될 수 없다.

(2) 근거

(가) 무선 네트워크는 유선 네트워크보다 추가 또는 다른 사이버 보안 위험을 야기한다. 이것은 주로 장치의 더 적

은 물리적 보호와 무선 주파수 통신의 사용 때문이다.

(나) 부적절한 물리적 접근 통제는 미허가 직원이 물리적 장치에 접근을 획득하게 할 수 있으며, 이는 논리적 접근 제한을 우회하거나 네트워크에 악성 장치(rogue device)의 배치하는 것을 초래할 수 있다.

(다) 무선 주파수에 의한 신호 전송은 피기백(Piggybacking) 또는 이블트윈(Evil Twin) 공격을 제공하는 도청뿐만 아니라 재밍에 관계된 위험을 도입한다. (https://us-cert.cisa.gov/ncas/tips/ST05-003 참조).

(3) 세부 요구사항

(가) 산업계 표준 및 모범 사례에 따른 암호화 알고리즘 및 키 길이와 같은 암호화 메커니즘이 무선 네트워크에서 전송되는 정보의 무결성과 기밀성을 보장하기 위해 적용되어야 한다.

(나) 무선 네트워크의 장치는 오직 무선 네트워크에서만 통신해야 한다. (즉, dual-homed가 아니어야 함).

(다) 무선 네트워크는 **1항**에 따라 별도의 세그먼트로 설계되어야 하고 **2항**에 따라 보호되어야 한다.

(라) 네트워크에 있는 무선 AP(액세스 포인트) 및 기타 장치는 네트워크에 대한 접근이 통제될 수 있도록 설치 및 구성되어야 한다.

(마) 무선 통신을 활용하는 네트워크 장치 또는 시스템은 통신에 참여하는 모든 사용자(사람, 소프트웨어 프로세스 또는 장치)를 식별하고 인증하는 기능을 제공해야 한다.

6. 원격 접근 통제 및 비신뢰 네트워크에서 통신

(1) 요구사항

2장의 범위에 있는 컴퓨터기반시스템은 비신뢰 네트워크로부터 무단 접근 및 다른 사이버 위협으로부터 보호되어야 한다.

(2) 근거

선내 컴퓨터기반시스템은 점점 더 디지털화되고 인터넷에 연결되어 다양한 정당한 기능을 수행한다. 선내 컴퓨터기반시스템을 감시하고 제어하기 위한 디지털 시스템의 사용은 사이버 사고에 취약하게 만든다. 공격자는 인터넷 연결을 통해 선내 컴퓨터기반시스템에 접근을 시도할 수 있으며 컴퓨터기반시스템의 작동에 영향을 주는 변경을 수행하거나 또는 컴퓨터기반시스템의 완전히 제어를 달성하거나, 선박의 컴퓨터기반시스템으로부터 정보의 다운로드를 시도할 수 있다. 또한 더 이상 지원되지 않거나 구식 운영 체제에 의존하는 IT 및 OT 시스템의 사용은 사이버 복원력에 많은 영향을 미치므로, 이러한 시스템에 원격으로 접근할 수 있는 경우 충분한 수준의 사이버 복원력을 유지하는 데 도움이 되도록 선상에서 관련 하드웨어 및 소프트웨어 설치에 특별한 주의를 기울여야 하며 모든 사이버 사고가 고의적인 공격의 결과인 것만은 아니라는 점을 염두에 두어야 한다.

(3) 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) **2장**의 적용 범위에 있는 컴퓨터기반시스템에 대하여, 어떠한 IP 주소도 신뢰할 수 없는 네트워크에 노출되지 않아야 한다. 신뢰할 수 없는 네트워크로부터 보안 구역으로 패킷을 직접 라우팅하는 것이 가능하지 않아야 한다.

(다) 비신뢰 네트워크와의 또는 이를 통한 통신에는 종점 인증, 무결성 보호 및 네트워크 또는 전송 계층에서의 인증 및 암호화를 통해 보안 연결(예: 터널링)을 요구한다. 읽기 권한이 필요한 정보에 대해서는 기밀성이 보장되어야 한다.

(라) 설계

(a) **2장**의 적용 범위에 있는 컴퓨터기반시스템은 다음을 만족해야 한다.

(i) 선내 연결 종점으로부터 연결을 종료할 수 있는 기능을 가져야 한다. 모든 원격 접근은 선내 책임 있는 역할에 의해 명시적으로 수락할 때까지 가능하지 않아야 한다.

(ii) OT 시스템의 안전한 기능이나 이들 시스템에서 사용하는 데이터의 무결성 및 가용성을 훼손하지 않도록 원격 세션 동안 중단을 관리할 수 있어야 한다.

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

(마) 원격 유지보수에 대한 추가 요구사항

(a) 원격접근이 유지보수에 이용되는 경우, (라)의 요구사항에 추가하여 다음 요구사항을 준수해야 한다.

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

(ii) 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 공급업

체로부터 이에 관한 확인 보고서를 득해야 한다.

(iii) 지원 계획이 개발되어 모든 이해 관계자가 이용 가능하도록 해야 한다.

(iv) 원격 유지 관리 활동 중에 언제든지 권한이 있는 직원은 활동을 중단하고 관련된 컴퓨터기반시스템 및 시스템의 이전의 안전한 구성으로 롤백할 수 있어야 한다.

(v) 비신뢰 네트워크로부터 범위 내의 컴퓨터기반시스템에 인간 사용자에 의한 어떠한 접근에 대해서는 다중요소 인증이 요구되어야 한다.

(vi) 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 차단되어야 한다.

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

7. 모바일 및 휴대용 장치의 사용

(1) 요구사항

(가) **2장**의 적용 범위에 있는 컴퓨터기반시스템에 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.

(나) 무선으로 연결된 모바일 및 휴대용 장치는 **5항**의 요구사항을 준수해야 한다.

(2) 근거

컴퓨터기반시스템는 모바일 또는 휴대용 장치를 통한 악성코드 감염으로 인해 손상될 수 있는 것으로 일반적으로 알려져 있다. 따라서 모바일 장치와 휴대용 장치의 연결은 신중하게 고려해야 한다. 또한 선박의 운항 및 유지보수에 필요한 모바일 장비는 선주의 통제 하에 있어야 한다.

(3) 세부 요구사항

(가) 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. 컴퓨터기반시스템에 장착된 모바일 및 휴대용 장치의 연결 포트에 대한 정보는 유지 관리에 사용되는 연결 포트를 포함하여 물품 목록에 포함되어야 한다.

(나) 이동식 매체용 차단기(Blocker)는 **4항** (3)호 (다)에 언급된 독립된 컴퓨터 이외의 물리적으로 접근 가능한 컴퓨터 및 네트워크 포트 상에 사용되어야 한다.

(다) 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.

(라) 물리적 또는 논리적 블록이 적용된 포트는 명확하게 표시되어야 한다.

204. 탐지

탐지 기능 요소에 대한 요구사항은 선내 컴퓨터기반시스템 및 네트워크에 대한 이상 활동을 표시 및 인식하고 사이버 사고를 식별하는 기능을 지원하는 적절한 수단의 개발 및 구현을 목표로 한다.

1. 네트워크 운영 모니터링

(1) 요구사항

2장의 적용 범위 내에 있는 네트워크는 지속적으로 감시되어야 하며, 오작동 또는 용량 감소/저하가 발생하면 경보가 발생되어야 한다.

(2) 근거

사이버 공격은 점점 더 정교해지고 있으며 건조 당시 알려지지 않은 취약성을 표적으로 하는 공격으로 인해 선박이 위협에 대비하지 못한 사고가 발생할 수 있다. 이러한 알려지지 않은 취약점을 표적으로 하는 공격에 조기 대응하기 위해서는 비정상적인 이벤트를 감지할 수 있는 기술이 필요하다. 네트워크의 이상 징후를 감지하고 사후 분석을 사용할 수 있는 모니터링 시스템은 사이버 이벤트에 적절하게 대응하고 추가로 복구하는 기능을 제공한다.

(3) 세부 요구사항

(가) **2장**의 적용 범위 내에 있는 네트워크를 모니터링하기 위한 조치는 다음 기능을 포함해야 한다.

(a) 과도한 트래픽에 대한 모니터링 및 보호

(b) 네트워크 연결 모니터링

(c) 기기 관리 활동 모니터링 및 기록

(d) 미승인된 장치의 연결에 대한 모니터링 또는 보호

(나) 다음을 만족하는 경우, 침입 탐지 시스템(IDS)이 구현될 수 있다.

(a) IDS는 관련 컴퓨터기반시스템의 공급자에 의해 자격이 부여되어야 한다.

(b) IDS는 수동적이어야 하며 컴퓨터기반시스템의 성능에 영향을 미칠 수 있는 보호 기능을 활성화하지 않아야 한다.

(c) 관련 직원은 IDS 사용에 대한 교육을 받고 자격을 갖추어야 한다.

2. 컴퓨터기반시스템 및 네트워크의 진단 기능 (Diagnostic functions)

(1) 요구사항

2장의 적용 범위에 있는 컴퓨터기반시스템과 네트워크는 **2장**에서 요구하는 보안 기능의 성능과 기능성을 확인할 수 있어야 한다. 진단 기능은 의도된 사용자의 사용을 위한 컴퓨터기반시스템 무결성 및 상태에 대한 적절한 정보와 선박의 안전한 운항을 위한 기능성을 유지하기 위한 수단을 제공해야 한다.

(2) 근거

(가) 보안 기능의 의도된 작동을 검증하는 능력은 선박의 수명 동안 사이버 복원력 관리를 지원하는 데 중요하다. 진단 기능을 위한 도구는 각 장치의 자가 진단 기능과 같은 자동 또는 수동 기능 또는 네트워크 모니터링을 위한 도구(예: ping, traceroute, ipconfig, netstat, nslookup, Wireshark, nmap 등)로 구성될 수 있다.

(나) 그러나 진단 기능의 실행은 때때로 컴퓨터기반시스템의 운영 성능에 영향을 미칠 수 있다는 점에 유의해야 한다.

(3) 세부 요구사항

(가) 컴퓨터기반시스템 및 네트워크의 진단 기능성은 선박의 시험 및 유지보수 단계 동안 모든 보안 기능의 의도된 운전을 검증하는 것이 가능해야 한다.

(나) 컴퓨터기반시스템 및 관련 네트워크의 정상 작동 동안 네트워크 연결 및 장치의 상태 뿐만이 아니라 과도한 네트워크 트래픽을 지속적으로 모니터링하는 진단 기능이 구현되어야 한다. 진단 기능은 이상 징후가 탐지되면 책임있는 선원에게 경고해야 한다.

205. 대응

대응 기능 요소에 대한 요구사항은 컴퓨터기반시스템 및 선내 네트워크의 가능한 손상 확대를 포함한 사이버 사고의 영향을 최소화할 수 있는 능력을 지원하는 적절한 수단의 개발 및 구현을 목표로 한다.

1. 사고 대응 계획 (Incident response plan)

(1) 요구사항

관련 비상상황을 다루고 사이버 보안 사고에 대응하는 방법을 상세화한 사고 대응 계획을 개발해야 한다. 사고 대응 계획에는 **2장**의 적용 범위에 있는 컴퓨터기반시스템에 대한 사고를 탐지, 대응 및 결과를 제한하기 위한 미리 지정된 지침 및 절차 문서들를 포함해야 한다.

(2) 근거

(가) 사고 대응 계획은 책임자가 사이버 사고에 대응할 수 있도록 돕기 위한 수단이다. 이러한 사고 대응 계획은 단순하여 효과적이고 신중하게 설계 된다. 사고 대응 계획을 개발할 때 사이버 사고의 심각성을 이해하고 그에 따라 대응 조치의 우선순위를 지정하는 것이 중요하다.

(나) 선박의 안전한 운항을 위한 기능성과 서비스 수준을 가능한 많이 유지하기 위한 수단(예: 활성 중 실행을 이중화 장치로 전환)이 표시되어야 한다. 사이버 사고 발생 시에 육상에 지정된 인원이 선박과 통합되어야 한다.

(3) 세부 요구사항

(가) 최초 연차 검사에서 본선에 비치되는 사고 대응 계획을 준비하기 위하여 선박의 설계 및 건조 단계에서 다양한 이해 관계자는 관련 정보를 선주에게 제공해야 한다. 사고 대응 계획은 선박의 운항 수명 동안 (예를 들어 유지보수 시) 최신으로 유지되어야 한다.

(나) 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.

(다) 사고 대응 계획에는 최소한 다음 정보가 포함되어야 한다.

(a) 침해된 시스템의 격리를 위한 중단점(Breakpoint)

(b) 탐지된 진행 중인 사이버 사건 또는 사이버 사건으로 야기된 이상 증상을 알리는 경보 및 표시들에 대한 설명

(c) 사이버 사고와 관련하여 예상되는 주요 결과에 대한 기술
(d) 만약 있는 경우, 비상 정지 또는 독립 또는 로컬 제어에 의존하지 않는 우선순위화 된 대응 옵션들
(e) 사이버 사고로 인해 고장난 시스템으로부터 독립적으로 작동하기 위한 독립의 로컬 제어 정보

(마) 사고 대응 계획은 전자기기의 완전히 상실 시에도 접근이 가능하도록 하드 카피로 비치되어야 한다.

2. 로컬, 독립 및/또는 수동 운전

(1) 요구사항

SOLAS 협약 II-1장 31규칙에서 요구하는 로컬 백업 제어에 필요한 모든 컴퓨터기반시스템은 주제어 시스템과 독립되어야 한다. 여기에는 효과적인 로컬 작동에 필요한 인간 사용자 인터페이스(HMI: Human Machine Interface)를 포함한다.

(2) 근거

안전한 운항을 유지하는 데 필요한 기계 및 장비에 대한 독립적인 로컬 제어는 유인 선박의 기본 원칙이다. 이 요구사항의 목적은 전통적으로 직원이 기계 근처에서 수동 운전을 실행함으로써 고장 및 기타 사고에 대처할 수 있도록 하는 것이다. 악의적인 사이버 사고도 또한 고려되어야 하므로 독립적 로컬 제어 원칙은 적지 않게 중요하다.

(3) 세부 요구사항

(가) 로컬 제어 및 모니터링을 위한 컴퓨터기반시스템은 자체 포함되어야 하며 의도된 작동을 위해 다른 컴퓨터기반시스템과의 통신에 의존하지 않아야 한다.

(나) 원격 제어 시스템 또는 다른 컴퓨터기반시스템에 대한 통신이 네트워크에 의해 연결되는 경우 **1항** 및 **2항**에 기술된 분할 및 보호 안전조치가 구현해야 한다. 이는 로컬 제어 및 모니터링 시스템이 별도의 보안 구역으로 간주되어야 함을 의미한다.

(다) 로컬 제어 및 모니터링을 위한 컴퓨터기반시스템은 **2장**의 요구사항을 준수해야 한다.

3. 네트워크 격리 (Network isolation)

(1) 요구사항

네트워크 세그먼트와의 네트워크 기반 통신을 수동으로 또는 자동으로 종료하는 것이 가능해야 한다.

(2) 근거

(가) 보안 침해가 발생하여 탐지된 경우 사고 대응 계획에 사고의 추가 전파 및 영향을 예방하기 위한 조치가 포함될 수 있다.

(나) 이러한 조치는 네트워크 세그먼트를 격리하고 필수 기능을 지원하는 시스템을 제어하는 것일 수 있다.

(3) 세부 요구사항

(가) 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 격리할 수 있어야 한다. 효과적인 방식으로 네트워크를 격리하는 것을 직원에게 허용하는 장치에 대한 이용 가능한 지침과 분명한 마킹이 있어야 한다.

(나) 안전을 포함한 올바른 기능 및 동작에 영향을 미칠 수 있는 개별 시스템의 데이터 종속성을 식별하여 비상 상황 시 시스템이 고립된 경우 데이터 또는 기능 입력에 대한 보완이 필요한 부분을 명확하게 보여야 한다.

4. 최소 위험 상태으로의 대비책(fallback)

(1) 요구사항

의도된 서비스를 제공하기 위해 **2장**의 적용 범위에 있는 컴퓨터기반시스템 또는 네트워크의 능력을 손상시키는 사이버 사고의 경우, 영향을 받는 시스템 또는 네트워크는 최소 위험 상태로 되돌릴 수 있어야 한다. (즉, 가능한 안전 이슈의 위험을 줄이는 안정적인 정지된 상태로 되돌리는 것)

(2) 근거

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

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

(3) 세부 요구사항

(가) 요구되는 대로 의도된 서비스를 제공하는 시스템의 능력을 손상시키며, 컴퓨터기반시스템 또는 네트워크에 영향을 미치는 사이버 사고가 탐지되는 즉시, 시스템은 합리적으로 안전한 상태를 달성할 수 있는 조건으로 되돌려

야 한다. 대비책 조치는 다음을 포함할 수 있다.

(a) 시스템을 완전한 정지시키는 것

(b) 시스템 해제

(c) 제어권을 다른 시스템 또는 인간 운전자에게 이전

(d) 기타 보상 조치

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

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

206. 복구

복구 기능 요소에 대한 요구사항은 사이버 사고의 영향을 받은 선내 컴퓨터기반시스템 및 네트워크를 복원하는 기능을 지원하는 적절한 수단의 개발 및 구현을 목표로 한다.

1. 복구 계획

(1) 요구사항

사이버 사고로 인한 중단 또는 장애가 발생한 후 **2장**의 적용 범위에 있는 컴퓨터기반시스템을 작동 상태로 복구하는 것을 지원하기 위한 복구 계획이 수립되어야 한다. 어디에서 누구에의해 지원이 가능한지에 대한 상세 내용이 복구 계획의 일부로 포함되어야 한다.

(2) 근거

(가) 사고 대응 절차는 시스템 복구의 필수적인 부분이다. 책임있는 직원은 (드라이브 지우기와 같은) 복구 작업의 의미를 신중하게 고려하고 인식하고 실행해야 한다.

(나) 그러나 일부 복구 작업으로 인해 사고 원인에 대한 귀중한 정보를 제공할 수 있는 증거가 파괴될 수 있다는 점에 유의해야 한다.

(다) 적절한 경우, 운영 능력을 복구하면서 증거 보존을 지원하기 위해 전문적인 사이버 사고 대응 지원을 받아야 한다.

(3) 세부 요구사항

(가) 선박의 설계 및 건조 단계에 관련된 다양한 이해 관계자는 첫 번째 연차 검사에서 본선에 배치될 복구 계획을 준비하기 위한 관련 정보를 선주에게 제공해야 한다. 복구 계획은 선박의 운항 수명 동안 (예를 들어 유지보수 시) 최신 상태로 유지되어야 한다.

(나) 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.

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

(a) 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.

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

(라) 일단 복구 목표가 정의되면 잠재적인 사이버 사고 목록이 생성되고, 복구 절차를 개발 및 기술되어야 한다. 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 논리 네트워크 다이어그램

(d) 고장 시스템의 복구를 담당 직원 목록

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

(f) 모든 구성품들 대한 현재 구성 정보

(마) 선내 직원의 안전을 보장하기 위한 선박의 운전 및 항해가 계획 내에서 우선시되어야 한다.

(바) 선내 및 육상의 복구 계획은 출력본으로 사이버 보안 책임자와 사이버 사고 지원 담당자가 이용할 수 있어야

한다.

2. 백업 및 복구 기능

(1) 요구사항

2장의 적용 범위에 있는 컴퓨터기반시스템 및 네트워크는 시기적절하고 완전하며 안전한 방식으로 백업 및 복원을 지원할 수 있어야 한다. 백업은 정기적으로 유지 관리되고 시험하여야 한다.

(2) 근거

(가) 일반적으로 백업 및 복구 전략의 목적은 데이터 손실을 방지하고 데이터 손실 후 데이터베이스를 재구성하는 것이다. 일반적으로 백업 관리 작업에는 다음을 포함한다.

(a) 다양한 종류의 고장에 대한 대응 방안을 계획하고 시험

(b) 백업 및 복구를 위한 데이터베이스 환경 구성

(c) 백업 일정 설정

(d) 백업 및 복구 환경 모니터링

(e) 장기 저장을 위한 데이터베이스 복사본 생성

(f) 데이터베이스 또는 호스트에서 다른 호스트로 데이터 이동, 등

(3) 세부 요구사항

(가) 복구 기능

(a) **2장**의 적용 범위에 있는 컴퓨터기반시스템은 사이버 사고 후 선박이 빠르고 안전하게 항해 및 운영 상태를 회복할 수 있도록 백업 및 복원 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) **2장**의 적용 범위에 있는 컴퓨터기반시스템 및 네트워크는 데이터 백업을 제공해야 한다. 오프라인 백업의 사용은 온라인 백업 기기에 영향을 미치는 랜섬웨어 및 웜바이러스에 대한 내성을 향상시키기 위해 고려되어야 한다.

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

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

(1) 요구사항

(가) **2장**의 적용 범위에 있는 컴퓨터기반시스템 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.

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

(2) 근거

(가) 제어된 종료는 다른 연결된 시스템들이 전체 통합 시스템을 안전하고 알려진 상태로 남기면서 보류 중인 트랜잭션으로 롤백, 프로세스 종료, 연결 끊기 등을 허용하는 소프트웨어 기능에 의해 컴퓨터기반시스템 또는 네트워크를 끄는 것으로 구성된다. 제어된 정지는 (예를 들어 전원 중단으로 인해 컴퓨터가 강제로 종료되어 발생하는) 하드 종료(hard shutdown)와는 반대되는 것이다.

(나) 일부 사이버 사고의 경우 강제 종료가 안전 예방 조치로 간주될 수 있지만 통합 시스템의 경우 예측 가능한 동작으로 일관되고 알려진 상태를 유지하기 위해 제어된 종료가 선호된다. 표준 종료 절차가 이행되지 않을 때, 데이터 또는 프로그램 및 운영 체제 파일이 손상될 수 있다. OT 시스템의 경우 손상의 결과는 불안정, 오작동 또는 의도한 서비스 제공 실패가 될 수 있다.

(다) 리셋 작업은 전형적으로 소프트 부팅을 시작하여 시스템을 종료하고 메모리를 지우고 장치를 초기화 상태로 리셋하도록 명령한다. 고려하는 시스템에 따라 리셋 작업은 다른 효과를 가질 수 있다.

(라) 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. 충돌 및 사이버 사고로부터 복구하고 시스템을 일관된 상태로 복원하는 데 중요하다.

(마) 시스템을 재시작하고 읽기 전용 소스로부터 모든 소프트웨어 및 데이터의 새로운 이미지(예: 롤백 작업 후)를 다시 로드하는 것은 예기치 않은 오류 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.

(3) 세부 요구사항

(가) **2장**의 적용 범위에 있는 컴퓨터기반시스템 및 네트워크는 다음의 역량을 갖추어야 한다.

(a) 전체 시스템을 안전하고 일관적이며 알려진 상태로 남을 수 있도록, 다른 연결된 시스템이 보류 중인 트랜잭션을 롤백, 프로세스 종료, 연결 끊기 등을 허용하 통제된 종료

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

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

(d) 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.

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

제 3 절 성능 평가

301. 일반사항

1. 성능 평가 및 시험은 **2장**의 요구사항을 충족하기 위해 적용된 조치들의 효과적인 구현을 확인하는 것을 목표로 한다.
2. 성능 평가 및 시험은 주로 시험 계획의 설계, 개발, 유지보수 및 구현을 기반으로 하며, 지상 시험 및 검증 활동을 지원하기 위한 필수 도구이다. 이는 선박 수명의 여러 단계에서 진화하고 다양한 이해 관계자를 포함한다.
3. 시험 계획은 **2장**의 요구사항을 충족하기 위해 채택된 조치의 실제적이고 효과적인 구현을 검증하기 위한 도구 및 참조로서 사용되어야 한다. 추가 또는 대체 시험도 실행할 수 있다. 시뮬레이션된 사이버 사고는 시험 목적으로 의도적으로 유도될 수 있다.
4. 이 절은 필요한 모든 정보를 포함하기 위해 선박 수명의 여러 단계에서 테스트 계획을 설계, 구현 및 유지 관리하는 방법을 나타내다. 이러한 조치와 관련된 책임도 표시된다.
5. 이 절에는 검사를 실시하는 방법에 대한 요구사항을 포함하지 않는다. 검사 요구사항은 별도로 개발될 예정이다.
6. 다음의 정보는 시험 계획의 설계, 개발, 유지보수 및 구현을 위해 선박 수명의 여러 단계에서 생산되어야 한다.

302. 설계 및 건조 단계 중

1. 공급자는 **2장**의 적용 범위에 있는 컴퓨터기반시스템에 통합을 위해 조선소 또는 시스템 통합자에 제공되는 시스템 또는 장비, 그리고 이러한 시스템을 서로 및 선내 다른 컴퓨터기반시스템 또는 육상에 연결하는 네트워크에 대한 관련 요구사항들을 충족하기 위해 채택된 조치들의 성능을 검증하기 위해 적합한 시험절차를 설계하고 문서화(시험계획)해야 한다
2. 공급자는 관련 시험 절차를 따라 시험 계획 내 기술된 시험들의 실행 결과가 기록된 시험 보고서를 유지해야 하며, 시험결과가 기록된 경우 조선소에 제공해야 한다.
3. 조선소 또는 시스템 통합자는 공급업체에 의해 제공되는 문서를 **2장**의 적용 범위에 있는 컴퓨터기반시스템 및 그러한 시스템에 연결하는 네트워크에 대한 전반적인 시험 계획에 통합해야 한다.
4. 조선소 또는 시스템 통합자는 **2장**의 적용 범위에 있는 컴퓨터기반시스템에 통합을 위해 조선소 또는 시스템 통합자에 제공되는 시스템 또는 장비, 그리고 이러한 시스템에 연결하는 네트워크에 대한 관련 요구사항들을 충족하기 위해 채택된 조치들의 성능을 검증하기 위해 적합한 시험절차를 설계하고 문서화(시험계획)해야 한다. 시험 절차에는 기능 시험, 고장 시험, 정상 상태, 경보 및 경고를 알리는 데 사용되는 경보 및 모니터링 수단의 설명을 포함해야 한다.
5. 조선소 또는 시스템 통합자는 관련 시험 절차를 따라 시험 계획 내 기술된 시험들의 실행 결과가 기록된 시험 보고서를 유지해야 하며, 시험결과가 기록된 경우 선주 및 선급협회에 조선소에 제공해야 한다.
6. 시험 절차는 제 3자가 선박 시운전 및 운항 중에 의도된 시험 조건을 본선에 재현하고 시험을 실시하고 시험 결과를 검증하고 얻어진 결과를 공급 업자 또는 조선소/시스템 통합자가 제공한 결과와 비교가 가능하도록 하는 방식으로 시험계획에 기술되어야 한다.
7. 공급자와 조선소는 시험 계획을 최신 상태로 유지하고 선내 컴퓨터기반시스템의 실제 구현 및 설치에 맞춰 조정해야 한다.

303. 선박 시운전 중 (Upon ship commissioning)

1. 조선소와 선주는 시험 계획의 최종 버전에 포함된 정보가 업데이트되고 변경 관리되고 있는지 함께 확인해야 한다. 시험계획은 컴퓨터기반시스템 및 선내 네트워크의 최신 구성과 일치해야 한다. 시험 계획에 문서화된 시험들은 컴퓨터기반시스템 및 선내 네트워크의 최종 구성에 대한 관련 요구사항을 충족하기 위해 채택된 조치의 설치 및 운영을 검증할 수 있을 만큼 충분히 상세해야 한다.
2. 조선소는 완벽하게 통합된 선박의 보안 통제 및 조치에 대한 검증 시험 또는 평가를 문서화하고, 구성에 대한 변경 관리를 유지하며, 안전 조건이 시험 계획에서 언급된 특정 상황이나 고장에 의해 영향을 받는 경우 문서화된 시험 결과에 기록해야 한다.
3. 실제 컴퓨터기반시스템 구성 및 선내 구현에 따라 업데이트된 최종 시험 계획은 선급에서 이용 가능해야 한다. 선급은 추가 시험을 요구할 수 있다.

304. 선박의 운항 수명 중(During the operational life of the ship)

1. 선주는 시스템 통합자 및 공급업체의 지원을 받아 시험 계획을 최신 상태로 유지하고 선박에 탑재된 컴퓨터기반시스템 및 이러한 시스템을 서로 연결하고 외부 (예: 육상) 다른 컴퓨터기반시스템에 연결하는 네트워크와 일치시켜야 한다. 선주는 컴퓨터기반시스템 및 선내 네트워크에서 발생한 변경, 이러한 변경과 관련된 새로운 리스크 가능성, 새로운 위협, 새로운 취약성 및 선박 운영 환경의 기타 가능한 변경을 고려하여 시험 계획을 업데이트해야 한다.
2. 선주는 운영 절차를 준비 및 구현해야 하며, 정기적인 훈련을 제공하고 선내 직원 및 기타 육상 관계 직원이 선내 컴퓨터기반시스템 및 네트워크에 친숙해지고 요구사항 충족을 위해 채택된 조치들을 적절히 관리할 수 있도록 정기적인 교육과 훈련을 실시해야 한다.
3. 선주는 시스템 통합자 및 공급업체의 지원을 받아 요구사항 충족을 위해 채택된 조치를 최신 상태로 유지해야 한다. (예를 들어, 선내 컴퓨터기반시스템 및 이를 연결하는 네트워크의 하드웨어 소프트웨어의 정기적 유지보수)
4. 선주는 시험 결과 사본과 업데이트된 시험 계획을 본선에 보관하고 선급에 제공할 수 있어야 한다.

제 4 절 요구사항 적용 제외를 위한 컴퓨터기반시스템의 위험도 평가

401. 요구사항

2장의 적용 범위에 속하는 컴퓨터기반시스템을 관련 요구사항의 적용에서 제외하는 경우 리스크 평가를 수행해야 한다. 리스크 평가는 제외된 컴퓨터기반시스템과 관련된 허용 가능한 리스크 수준의 증거를 제공해야 한다. 관련 요구사항에서 제외된 애플리케이션의 간결한 목록은 선내 컴퓨터기반시스템 문서와 함께 생성되고 유지되어야 한다(예: 시험 계획 및 관련 업데이트된 시험 계획의 실행)

402. 근거

1. 관련 요구사항의 적용에서 **2장**의 적용 범위에 속하는 컴퓨터기반시스템을 제외하는 것은 적절하게 정당화되고 문서화해야 한다. 이러한 제외는 컴퓨터기반시스템의 운영과 관련된 위험 수준이 특정 위험 평가 수단에 의해 허용 가능한 임계값(threshold) 미만이라는 증거가 제공된 경우에만 우리 선급에서 수락할 수 있다.
2. 위험도 평가는 컴퓨터기반시스템 분류 및 연결 등급, 선박 및 컴퓨터기반시스템의 기능 요구사항 및 사양을 고려하여 유사한 설계에 대한 이용 가능한 지식 기반 및 경험을 기반으로 해야 한다. 내부 및 외부 소스의 사이버 위협 정보는 사이버 보안 이벤트의 가능성과 영향을 더 잘 이해하는 데 활용될 수 있다.

403. 세부 요구사항

1. 설계 및 건조 단계에서 조선소에서 리스크 평가를 수행하고 최신 상태로 유지해야 하며 원래 설계의 변경 가능성과 처음에 알려지지 않은 새로 발견된 위협 및/또는 취약성을 고려하여 최신 상태로 유지해야 한다.
2. 선박의 운항 수명 중에 선주는 지속적인 개선 프로세스 중에 사이버 시나리오의 지속적인 변화와 선내 컴퓨터기반시스템에서 식별된 새로운 약점을 고려하여 위험도 평가를 업데이트해야 한다. 새로운 위험이 식별되면 선주는 기존 위험을 업데이트하거나, 새로운 위험 완화 조치를 구현해야 한다.
3. 사이버 시나리오의 변경이 검토 중인 컴퓨터기반시스템과 관련된 위험 수준을 허용 가능한 위험 임계값 이상으로 높이는 것과 같은 경우, 선주는 선급협회에 알리고 업데이트된 위험도 평가서를 평가를 위해 제출해야 한다.
4. 관련 요구사항의 제외된 애플리케이션의 간결한 목록은 선내 컴퓨터기반시스템 문서와 함께 생성 및 유지되어야 한다(예: 시험 계획 및 관련 업데이트된 시험 계획 실행). 선급협회는 **2장**의 요구사항 적용에서 컴퓨터기반시스템의 제외를 수락하거나 거절할 수 있다.
5. 검토 중인 컴퓨터기반시스템에 대해 예상되는 운영 환경은 컴퓨터기반시스템의 분류를 고려하여 사이버 사고의 가능성과 이것이 인명의 안전, 선박의 안전 또는 해양 환경에 미칠 수 있는 영향을 식별하기 위해 리스크 평가에서 분석되어야 한다. 공격 표면은 컴퓨터기반시스템의 연결 등급, 휴대용 장치에 대해 가능한 인터페이스, 논리적 접근 제한 등을 고려하여 분석되어야 한다.
6. 검사 중인 컴퓨터기반시스템의 특정 구성과 관련된 새로운 위험도 식별해야 한다. 위험도 평가에서 다음 요소를 고려해야 한다.
   (1) 자산 취약성
   (2) 내부 및 외부의 위협
   (3) 자산에 영향을 주는 사이버 사고의 인적 안전, 선박 안전 및/또는 환경 위협에 대한 잠재적 영향
   (4) 시스템의 통합 또는 선내가 아닌 시스템을 포함하여 시스템 간의 인터페이스에 관련된 가능한 영향(예: 선내 시스템에 대한 원격 접근이 제공되는 경우)

404. 수용 기준

1. **2장**의 적용 범위에 해당하는 컴퓨터기반시스템의 관련 요구사항의 적용에서 제외하는 것은 컴퓨터기반시스템의 운영이 사이버 리스크과 관련된 운영의 안전에 영향을 미치지 않는다는 증적이 제공되는 경우에만 선급협회에서 수용될 수 있다. 이러한 제외는 다음 기준을 완전히 충족하지 않는 컴퓨터기반시스템에 대해 허용할 수 있다. **2항** 따른 기준을 모두 만족하지 못하는 컴퓨터기반시스템에 대해서는 그러나 증적과 함께 합리적인 설명이 제공되어 선급협회에 의해 만족하다고 인정되는 경우에 제외가 허용될 수 있다. 또한, 우리 선급에선 적용 제외를 고려하기 위해 추가의 문서 제출을 요구할 수 있다.
2. 다음의 기준이 위험도 수준 수용 평가를 위해 고려되어야 한다.
   (1) 컴퓨터기반시스템에 영향을 미치는 사이버 사고에서 파생되는 예측 가능한 취약성, 위협, 잠재적 영향이 리스크 평

가에서 적절히 고려되었다.

(2) 컴퓨터기반시스템의 공격 표면은 복잡성, 연결성, 무선 AP를 포함하여 물리적 및 논리적 접근 지점을 고려하여 최소화 된다.

(3) 컴퓨터기반시스템이 속한 통합 시스템에서 기능과 역할을 고려하여, 컴퓨터기반시스템은 다른 컴퓨터기반시스템 또는 네트워크 장치에 의해 매개되는 사이버 사건의 영향을 받을 수 없으며, 사이버 사고의 영향이 다른 컴퓨터기반시스템 또는 네트워크 장치로 전파할 수 없다.

(4) 컴퓨터기반시스템은 필수 서비스 또는 다중 선박 서비스를 제공하지 않아야 한다.

(5) 컴퓨터기반시스템은 접근이 통제된 구역에 위치해야 한다.

(6) 다른 컴퓨터기반시스템에 대한 컴퓨터기반시스템의 연결이 적절하게 조사, 이해 및 문서화 된다. 특히, 컴퓨터기반시스템은 IP 기반 네트워크에 의해 다른 컴퓨터기반시스템 또는 장치에 연결되지 않아야 한다.

(7) 컴퓨터기반시스템에는 통제되지 않은/보안되지 않은 이동식 장치에서 사용할 수 있는 물리적 인터페이스가 없어야 한다.

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

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

(10) 컴퓨터기반시스템은 하드웨어 및 소프트웨어 무결성 검사를 포함한 기능 무결성과 제공된 서비스 품질을 언제든지 검사할 수 있는 수단을 제공한다.

(11) 컴퓨터기반시스템은 인간 사용자가 로컬 수동 제어를 할 수 있는 적절한 인터페이스를 제공하며, 이러한 인터페이스는 공격 표면을 확장하지 않는다. (또한, (2)호 참조)

(12) 사고 대응 계획 및 복구 계획에는 선박에서 사이버 사고가 발생한 경우 컴퓨터기반시스템을 처리하는 방법에 대한 표시를 포함한다.

제 3 장 선내 시스템 및 장비의 사이버 복원력 요건

제 1 절 일반사항

101. 도입

1. 선박, 항만, 컨테이너 터미널 등의 기술 발전과 운영 기술(OT) 및 정보 기술(IT)에 대한 의존도 증가로 인해 비즈니스, 인적 데이터, 인명의 안전, 선박의 안전에 영향을 미치고 해양 환경을 위협할 수 있는 사이버 공격의 가능성이 증가했다. 현재 및 새로운 위협으로부터 해운을 보호하려면 설계 및 제조 단계에서 장비와 시스템에 보안 기능을 통합해야 하는 지속적으로 발전하는 다양한 제어 기능이 포함되어야 한다. 따라서 사이버 복원력으로 설명할 수 있는 시스템과 장비를 제공하기 위해 공통의 최소 요구사항 세트를 수립할 필요가 있다.
2. 이 문서는 선내 시스템과 장비의 사이버 복원력에 대한 통일 요구사항들을 명시한다.

102. 제한사항

1. **3장**은 시스템 하드웨어 및 소프트웨어 기능에 대한 환경 성능을 다루지 않는다. 이 장에 추가하여 다음의 규칙 및 지침이 적용되어야 한다.
   (1) **제조법 및 형식승인 등에 관한 지침 3장 23절** 자동화시스템
   (2) **선급 및 강선규칙 6편 2장 4절** 컴퓨터기반시스템

103. 범위

1. **3장**에 명시된 요건은 본 지침 **2장**의 적용 범위에 포함되는 컴퓨터기반시스템에 적용한다.
2. 항해 및 무선통신 시스템은 **3장**의 요구사항을 대신하여 IEC 61162-460을 따를 수 있다. (**1장 103.** 참조)

제 2 절 보안 원칙(Philosophy)

201. 시스템 및 장비

1. 시스템은 프로세스의 안전, 보안 및 안정적인 운영을 가능하게 하는 하드웨어와 소프트웨어 그룹으로 구성할 수 있다. 대표적인 예로 엔진 제어 시스템, DP 시스템 등이 있다.
2. 장비는 다음 중 하나일 수 있다.
   (1) 네트워크 장치(예: 라우터, 관리되는 스위치)
   (2) 보안 장치(예: 방화벽, IPS)
   (3) 컴퓨터(예: 워크스테이션, 서버)
   (4) 자동화 장치(예: PLC)
   (5) 가상 머신 클라우드 호스팅

202. 시스템 요구사항

4절의 시스템 요구사항은 해당되는 경우 **2장** 범위의 모든 시스템에 적용한다. 신뢰할 수 없는 네트워크와의 인터페이스와 관련된 추가 요구사항은 이러한 연결이 설계된 시스템에만 적용된다.

203. 보상 대책

1. 하나 이상의 보안 요구사항을 충족하기 위해 고유의 보안 기능 대신 또는 추가로 보상 대책을 사용할 수 있다.
2. 보상 대책은 다음 원칙을 따라야 한다.
   (1) 보상 대책은 원래 명시된 요구사항의 의도와 엄격함을 만족해야 한다. 이들은 또한 다른 요구사항들을 초과(above and beyond)한 것이어야 한다. (단순히 다른 요구사항을 준수하는 것이 아님)
   (2) 시스템 형식승인의 경우 컴퓨터기반시스템에 보상 대책이 구현되어야 한다. 즉, 선내 설치 또는 운영 절차와 관련된 장벽에 의존하지 않아야 한다.

204. 중요 시스템 가용성

1. 중요 시스템에 대한 보안 조치는 시스템 가용성에 부정적인 영향을 미치지 않아야 한다.
2. 보안 조치의 구현은 건강, 안전 및 환경 영향을 초래할 수 있는 보호 상실, 제어 상실, 시야 상실 또는 기타 중요 기능의 상실을 야기하지 않아야 한다.
3. 시스템은 선박, 선박의 시스템, 인원 및 화물의 안전에 필요한 데이터의 기밀성, 무결성 및 가용성을 보장하는 방식으로 선박이 중요한 업무를 계속할 수 있도록 적절하게 설계되어야 한다.

제 3 절 문서

301. 컴퓨터기반시스템 문서

이 장의 요구사항에 따라 검토 및 승인을 위해 다음 문서를 우리 선급에 제출해야 한다.

1. 시스템에 포함된 장비의 세부 목록 (302. 참조)
2. 각 장비에 대해 관련 하드웨어 상세 (예: 마더보드, 저장소, 인터페이스(네트워크, 시리얼) 및 모든 연결)
3. 다음을 포함하는 소프트웨어 목록:
   (1) 운영체제/펌웨어
   (2) 운영체제에서 제공하고 관리하는 네트워크 서비스
   (3) 응용 소프트웨어(303. 참조)
   (4) 데이터베이스
   (5) 구성 파일
4. 네트워크 또는 시리얼 흐름도 (출발지, 목적지, 프로토콜, 프로토콜 상세, 물리적 구현)
5. 네트워크 보안 장비 (다른 장비와 마찬가지로 고려되고 상세하게 설명되어야 함). 예를 들어, 트래픽 관리(방화벽, 라우터 등) 및 패킷 관리(IDS 등)
6. 보안 개발 수명주기 문서 (**5절** 참조).
7. 시스템 유지보수 계획
8. 복구 계획
9. 시스템 시험 계획
10. 시스템이 **3장**의 해당 요구사항을 충족하는 방법에 대한 설명 (즉, 운영 매뉴얼 또는 사용자 매뉴얼 등)
11. 변경 관리 계획

302. 물품 목록(Inventory)

1. 다음의 상세 정보가 문서화되어야 한다.
   (1) 명칭
   (2) 브랜드/제조사 (공급자)
   (3) 모델 또는 참조번호 (일부 장치는 여러개의 참조번호를 포함할 수 있음)
   (4) 운영체제 현재 버전 및 내장된 펌웨어 (소프트웨어 버전) 및 구현 일자

303. 소프트웨어 목록

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

1. 설치된 컴퓨터기반시스템의 간략한 기능 설명 및 기술적 특징과 함께 목적에 대한 간략한 설명(브랜드, 제조업체, 모델, 주요 기술 데이터)
2. 버전 정보, 만료 일자를 포함한 라이선스 정보 및 업데이트 로그
3. 유지보수 정책(예: 현장 대 원격, 주기적 대 비정기 등) 및 책임자
4. 역할 및 책임을 포함한 접근 통제 정책(예: 읽기, 쓰기 및 실행 권한)

제 4 절 시스템 요구사항

401. 일반사항

1. 이 절은 103.에 명시된 범위 내의 컴퓨터기반시스템에 필요한 보안 기능을 명시한다.
2. 이 절의 요구사항은 IEC 62443-3-3에서 선택한 요구사항을 기반으로 한다. 각 요구사항에 대한 전체 내용, 근거 및 관련 지침을 확인하기 위해선 인용한 표준을 참조해야 한다.

402. 필수 보안 기능

다음의 보안 기능은 103.에서 명시된 범위 내의 모든 컴퓨터기반시스템에 대해서 요구한다.

표 1

항목 번호	목적	요구사항	참조 표준
미인증된 개체로부터 우발적 또는 우연한 접근으로부터 보호			
1	인간 사용자 식별 및 인증	컴퓨터기반시스템은 시스템에 직접 또는 인터페이스를 통해 접근할 수 있는 모든 인간 사용자를 식별하고 인증해야 한다.	IEC 62443-3-3/SR1.1
2	계정 관리	컴퓨터기반시스템은 계정 추가, 활성화, 수정, 비활성화 및 제거를 포함하여 허가된 사용자의 모든 계정 관리를 지원하는 기능(capability)을 제공해야 한다.	IEC 62443-3-3/SR1.3
3	식별자 관리	컴퓨터기반시스템은 사용자, 그룹 및 역할별 식별자 관리를 지원하는 기능을 제공해야 한다.	IEC 62443-3-3/SR1.4
4	인증자 관리	컴퓨터기반시스템은 다음의 기능을 제공해야 한다: - 인증자 내용을 초기화 - 제어 시스템 설치 시 모든 기본 인증자를 변경 - 모든 인증자를 변경/새로고침 - 저장 및 전송 시 허가받지 않은 노출 및 수정으로부터 모든 인증자를 보호	IEC 62443-3-3/SR1.5
5	무선 접근 관리	컴퓨터기반시스템은 무선통신에 관계되는 모든 사용자(인간, 소프트웨어 프로세스 또는 장치)를 식별하고 인증할 수 있는 기능을 제공해야 한다.	IEC 62443-3-3/SR1.6
6	패스워드 기반 인증 강도	컴퓨터기반시스템은 최소 길이와 다양한 문자 유형에 기초하여 구성할 수 있는 패스워드 강도를 시행할 수 있는 기능을 제공해야 한다.	IEC 62443-3-3/SR1.7
7	인증자 피드백	컴퓨터기반시스템은 인증 과정 중에 피드백을 불명확하게 제공해야 한다.	IEC 62443-3-3/SR1.10
우발적 또는 우연한 오용으로부터 보호			
8	권한부여	모든 인터페이스에서 인간 사용자는 직무 분리와 최소 특권의 원칙에 따라서 권한이 할당되어야 한다.	IEC 62443-3-3/SR2.1
9	무선 사용 통제	컴퓨터기반시스템은 일반적으로 인정하는 보안 산업 관행에 따라 시스템에 대한 무선 연결을 위한 인가, 감시 및 사용 제한을 강제할 수 있는 기능을 제공해야 한다.	IEC 62443-3-3/SR2.2
10	휴대용 및 모바일 기기에 대한 사용 통제	컴퓨터기반시스템은 휴대용 및 모바일 기기에 사용을 지원하는 경우, 다음의 기능을 포함해야 한다. a) 휴대용 및 모바일 기기의 사용 제한 b) 휴대용 및 모바일 기기로의 코드 및 데이터 전송 제한 비고: 포트 제한/블록커 (및 실리콘)이 특정 시스템에 허용될 수 있다.	IEC 62443-3-3/SR2.3
11	모바일 코드	컴퓨터기반시스템은 자바 스크립트(java scripts), 엑티브 엑스(Active X) 및 PDF와 같은 모바일 코드의 사용을 통제(control)해야 한다.	IEC 62443-3-3/SR2.4
12	세션 잠금 (Session Lock)	컴퓨터기반시스템은 설정된 시간 동안 사용하지 않거나 수동 세션 잠금을 시작하여 추가 접속을 방지하는 기능을 제공하여야 한다.	IEC 62443-3-3/SR2.5
13	감사 이벤트	컴퓨터기반시스템은 최소한 다음의 이벤트에 대하여 보안에 관련된 감사 기록을 생성해야 한다: - 접근 통제 - 운영체제 이벤트 - 백업 및 복구 이벤트 - 구성 변경 - 통신기능의 상실	IEC 62443-3-3/SR2.8

표 1 (계속)

항목 번호	목적	요구사항	참조 표준
14	감사 저장 용량	컴퓨터기반시스템은 로그 관리에 대한 일반적으로 인정하는 권고사항에 따라 감사 기록 저장 용량을 할당하는 기능을 제공해야 한다. 이 용량을 초과할 가능성을 줄이기 위해 감사 메커니즘을 구현해야 한다.	IEC 62443-3-3/SR2.9
15	감사처리 실패 대응	컴퓨터기반시스템은 감사 처리 실패 시 필수 서비스 및 기능의 손실을 방지할 수 있는 기능을 제공해야 한다.	IEC 62443-3-3/SR2.10
16	타임스탬프	컴퓨터기반시스템은 감사 기록에 타임스탬프를 제공해야 한다.	IEC 62443-3-3/SR2.11
우발적인 또는 우연한 조작으로부터 컴퓨터기반시스템의 무결성 보호			
17	통신 무결성	컴퓨터기반시스템은 전송된 정보의 무결성을 보호하여야 한다. 비고: 암호화 메커니즘이 무선 네트워크에 적용되어야 한다.	IEC 62443-3-3/SR3.1
18	악성코드로부터 보호	컴퓨터기반시스템은 악성 코드 또는 허가되지 않은 소프트웨어로 인한 영향을 방지, 감지 및 완화하기 위해 적절한 보호 조치를 구현할 수 있는 기능을 제공해야 한다. 또한, 보호 메커니즘을 업데이트하는 기능이 있어야 한다.	IEC 62443-3-3/SR3.2
19	보안 기능성 검증	컴퓨터기반시스템은 보안 기능의 의도된 작동 검증을 지원하고 유지 관리 중 이상이 발생하면 보고할 수 있는 기능을 제공해야 한다.	IEC 62443-3-3/SR3.3
20	결정론적 출력	컴퓨터기반시스템은 공격의 결과로 정상적인 작동을 유지할 수 없는 경우 출력을 사전 결정된 상태로 설정하는 기능을 제공해야 한다. 사전 결정된 상태는 다음과 같을 수 있다. - 전원이 공급되지 않은 상태(Unpowered state) - 마지막으로 알려진 값(Last-known value) - 고정 값(Fixed value)	IEC 62443-3-3/SR3.6
도청 또는 우연한 노출을 통한 무단 정보 노출 방지			
21	정보 기밀성	컴퓨터기반시스템은 휴면(at rest)이거나 전송 중인 것과 무관하게 명시적 읽기 권한이 지원되는 정보의 기밀성을 보호하는 기능을 제공해야 한다. 참고: 무선 네트워크의 경우 전송 중인 모든 정보의 기밀성을 보호하기 위해 암호화 메커니즘을 사용해야 한다.	IEC 62443-3-3/SR4.1
22	암호 사용	암호화를 사용하는 경우, 컴퓨터기반시스템은 일반적으로 인정하는 보안 업계 관행 및 권고사항에 따라서 암호 알고리즘, 키 길이 및 메커니즘을 사용해야 한다.	IEC 62443-3-3/SR4.3
컴퓨터기반시스템 운영 모니터링 및 사고 대응			
23	감사 로그 접근성	컴퓨터기반시스템은 허가된 사용자 및/또는 도구(tool)에 의해 읽기 전용으로 감사 로그에 접근하는 기능을 제공해야 한다.	IEC 62443-3-3/SR6.1
제어 시스템이 정상적인 생산 조건에서 안정적으로 작동하는지 확인			
24	서비스거부(DoS) 방지	컴퓨터기반시스템은 DoS 사건 중에도 중요 기능들을 유지하는 최소 기능을 제공해야 한다.	IEC 62443-3-3/SR7.1
25	자원(Resource) 관리	제어시스템은 리소스 부족을 방지하기 위해 보안기능에 의한 리소스 사용을 제한할 수 있어야 한다.	IEC 62443-3-3/SR7.2
26	시스템 백업	중요한 파일의 식별, 위치, 사용자 수준 및 시스템 수준 정보(시스템 상태 정보 포함)의 백업을 수행하는 기능은 정상 운영에 영향을 미치지 않으면서 컴퓨터기반시스템에서 지원해야 한다.	IEC 62443-3-3/SR7.3

표 1 (계속)

항목 번호	목적	요구사항	참조 표준
27	시스템 복구 및 재구성	컴퓨터기반시스템은 중단 또는 고장 후 알려진 보안 상태로 복구하거나 및 재구성할 수 있는 기능을 제공해야 한다.	IEC 62443-3-3/SR7.4
28	비상 전원	제어시스템은 기존 보안 상태 또는 문서화된 성능저하 모드에 영향을 주지 않고 비상 전원으로 전환할 수 있는 기능을 제공해야 한다.	IEC 62443-3-3/SR7.5
29	네트워크 및 보안 구성 설정	컴퓨터기반시스템 트래픽은 컴퓨터기반시스템 공급자가 제공한 지침서에 기술된 권장 네트워크 및 보안 구성대로 설정할 수 있는 기능을 제공해야 한다. 컴퓨터기반시스템은 현재 배치된 네트워크 및 보안 구성 설정에 대한 인터페이스를 제공해야 한다.	IEC 62443-3-3/SR7.6
30	최소화 기능	다음의 설치, 가용성 및 접근 권한은 시스템에서 제공하는 기능에 대한 엄격한 요구로 제한되어야 한다. - 운영 체제 소프트웨어 구성 요소, 프로세스 및 서비스 - 네트워크 서비스, 포트, 프로토콜, 경로 및 호스트 접근 및 모든 소프트웨어	IEC 62443-3-3/SR7.7

403. 추가 보안 기능

1. 신뢰할 수 없는 네트워크와 네트워크 통신을 하는 컴퓨터기반시스템(즉, **2장**의 범위를 벗어난 모든 네트워크와 인터페이스)에는 다음과 같은 추가 보안 기능이 요구된다. (즉, **2장**의 범위 밖에 있는 네트워크에 대한 인터페이스)

표 2

항목 번호	목적	요구사항	참조 표준
31	인간 사용자에 대한 다중요소 인증	신뢰할 수 없는 네트워크를 통해 컴퓨터기반시스템에 접근하는 경우 다중요소 인증이 인간 사용자에게 요구된다.	IEC 62443-3-3/SR1.1, RE2
32	소프트웨어 프로세스 및 장치 식별 및 인증	컴퓨터기반시스템은 소프트웨어 프로세스와 장치들을 식별하고 인증해야 한다.	IEC 62443-3-3/SR1.2
33	로그인 시도 실패	컴퓨터기반시스템은 특정 시간 동안 신뢰할 수 없는 네트워크에서 연속적으로 유효하지 않은 로그인을 시도하는 것을 제한해야 한다.	IEC 62443-3-3/SR1.11
34	시스템 사용 알림	컴퓨터기반시스템은 인증 전에 시스템 사용 알림 메시지를 표시할 수 있는 기능을 제공해야 한다. 시스템 사용 알림 메시지는 허가된 직원에 의해서 설정할 수 있어야 한다.	IEC 62443-3-3/SR1.12
35	신뢰할 수 없는 네트워크 경유 접근	신뢰할 수 없는 네트워크에서 또는 이를 통해 컴퓨터기반시스템에 접근하는 모든 행위는 감시되고 통제되어야 한다.	IEC 62443-3-3/SR1.13
36	명시적 접근 요청 승인	컴퓨터기반시스템은 선내 허가된 직원이 명시적으로 승인하는 경우를 제외하고 신뢰할 수 없는 네트워크를 통한 접근을 거부해야 한다.	IEC 62443-3-3/SR1.13, RE1
37	원격 세션 종료	컴퓨터기반시스템은 설정된 미사용 시간 이후 자동으로 또는 세션을 시작한 사용자가 수동으로 원격 세션을 종료하는 기능을 제공해야 한다.	IEC 62443-3-3/SR2.6
38	암호화 무결성 보호	컴퓨터기반시스템은 신뢰할 수 없는 네트워크와 통신하거나 이를 통해 통신하는 동안 정보 변경 사항을 인식하기 위해 암호화 메커니즘을 사용해야 한다.	IEC 62443-3-3/SR3.1, RE1
39	입력값 검증	컴퓨터기반시스템은 프로세스 제어 입력 또는 컴퓨터기반시스템의 동작에 직접 영향을 미치는 입력으로 사용되는 신뢰할 수 없는 네트워크를 통한 입력 데이터의 구문, 길이 및 내용을 검증해야 한다.	IEC 62443-3-3/SR3.5
40	세션 무결성	컴퓨터기반시스템은 세션의 무결성을 보호하는 기능을 제공해야 한다. 유효하지 않은 세션 ID는 거부되어야 한다.	IEC 62443-3-3/SR3.8
41	세션 종료후 세션 ID 무효화	시스템은 사용자 로그아웃 또는 기타 세션 종료 시(브라우저 세션을 포함) 세션 ID를 무효화해야 한다.	IEC 62443-3-3/SR3.8, RE1

제 5 절 제품 설계 및 개발 요구사항

501. 일반사항

1. 시스템 또는 장비 개발 시 다음 단계에서 보안 측면을 포괄적으로 다루는 보안 개발 수명주기(Secure Development Lifecycle: 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. 보안 측면이 위의 단계에서 어떻게 반영되었는지를 기록한 문서를 생성하고 최소한 아래 **502.**의 **1**항에서 **7**항까지 명시된 통제된 프로세스를 통합하여야 한다. 해당 문서는 검토 및 승인을 위해 우리 선급에 제출해야 한다.

502. 관리 프로세스(Controlled process)

1. (IEC 62443-4-1/SM-8) 제조사는 승인되지 않은 접근 또는 변경으로부터 코드 서명에 사용되는 개인 키를 보호하기 위한 절차 및 기술적 통제를 마련해야 한다. 제조사는 업데이트 출시 전에 시험하기 위한 QA 프로세스가 있어야 한다.
2. (IEC 62443-4-1/SUM-2) 제품의 보안 업데이트에 대한 문서를 사용자에게 제공하는 것을 보장하는 프로세스(이는 액세스할 수 있는 사이버 보안 연락처 또는 정기 간행물을 통해 이루어질 수 있음)가 채택되어야 하며, 이는 다음을 모두 포함하지만 이에 국한하진 않는다.
   (1) 보안 패치가 적용되는 제품 버전 번호
   (2) 승인된 패치를 수동 및 자동화 프로세스를 통해 적용하는 방법에 대한 지침
   (3) 재부팅을 포함하여 제품에 패치를 적용할 때 미칠 수 있는 영향에 대한 설명
   (4) 승인된 패치가 적용되었는지 확인하는 방법에 대한 지침설명
   (5) 자산 소유자가 승인하거나 배포하지 않은 패치를 사용할 수 있는 조치와 패치를 하지 않았을 때의 발생 할 수 있는 위험
3. (IEC 62443-4-1/SUM-3) 종속 구성요소 또는 운영 체제 보안 업데이트에 대한 문서를 사용자가 이용할 수 있도록 보장하는 프로세스를 채택해야 하며, 이는 다음을 포함하지만 이에 국한하진 않는다.
   (1) 제품이 종속 구성요소 또는 운영 체제 보안 업데이트와 호환되는지 여부를 명시한다.
4. (IEC 62443-4-1/SUM-4) 지원되는 모든 제품 및 제품 버전에 대한 보안 업데이트가 보안 패치의 진위 여부를 쉽게 확인할 수 있는 방식으로 제품 사용자에게 공급할 수 있도록 보장하는 프로세스를 채택해야 한다. 추가로, 제조사는 업데이트 출시 전에 시험하기 위한 QA 프로세스가 있어야 한다.
5. (IEC 62443-4-1/SG-1) 설치, 운영 및 유지보수를 지원하기 위한 제품에 대한 심층 보안 전략을 설명하는 제품 문서를 작성하는 프로세스가 있어야 하며, 여기에는 다음을 모두 포함한다.
   (1) 심층 방어 전략에서 제품에 의해 구현된 보안 기능과 역할
   (2) 심층 방어 전략에 의해 고려된 위협
   (3) 법령(legacy code)과 관련된 위험을 포함하여 제품과 관련하여 알려진 보안 위험에 대한 제품의 사용자 완화 전략
6. (IEC 62443-4-1/SG-2) 제품이 사용될 외부 환경에서 제공할 것으로 예상되는 보안 방어 조치를 심층적으로 설명하는 제품 사용자 문서를 작성하는 프로세스를 채택해야 한다.
7. (IEC 62443-4-1/SG-3) 제품을 설치 및 유지보수할 때 제품을 강화하기 위한 지침서를 포함한 제품 사용자 문서(product user documentation)를 작성하는 프로세스를 채택해야 한다. 지침서는 다음에 대한 지침, 근거 및 권장사항을 모두 포함하지만 이에 국한하진 않는다.
   (1) 타사의 구성요소를 포함한 제품과 제품 보안 컨텍스트와의 통합
   (2) 제품의 응용 프로그래밍 인터페이스/프로토콜과 사용자 애플리케이션의 통합
   (3) 제품의 심층 방어 전략 적용 및 유지보수
   (4) 로컬 보안 정책과 각 보안 옵션/기능을 지원하는 보안 옵션/기능의 구성 및 사용(아래 모두 포함):
      (가) 제품의 심층 방어 전략에 대한 기여

(나) 각 업무 방식에 미치는 잠재적 영향과 함께 보안에 영향을 미치는 구성 가능한 기본값 및 기본값에 대한 설명
(다) 값의 설정/변경/삭제

(5) 제품 보안의 관리, 모니터링, 사고 처리 및 평가를 지원하는 모든 보안 관련 도구 및 유틸리티의 사용에 대한 지침 및 권장 사항
(6) 정기적인 보안 유지 활동에 대한 지침 및 권장 사항
(7) 제품에 대한 보안 사고를 공급자에게 보고하기 위한 지침
(8) 제품의 유지보수 및 관리를 위한 보안 모범 사례에 대한 설명 ⚓

부록

부록 1 행동 및 문서의 요약

1. 범례(Legend)

(1) 승인 : 우리 선급에 문서가 승인용으로 제출해야 한다.
(2) 검증: 검사원이 문서의 가용성 및 업데이트 상태를 검증해야 한다.
(3) 정보확인: 우리 선급에 문서가 정보 제공용으로 제출해야 한다.
(4) 유지관리 : 표시된 관계자는 문서의 최신화를 유지하고, 컴퓨터기반시스템, 네트워크 및 리스크 저감 조치의 실질적 구현과 일치하도록 해야 한다.
(5) 제시 : 표시된 관계자는 검사원이 이용할 수 있도록 문서를 제공해야 한다.
(6) 제출 : 표시된 관계자는 다른 관련된 관계자가 이용할 수 있도록 문서를 제공해야 한다.

표 3 행동 및 문서의 요약

문서	참조 요구사항	단계	공급업체	조선소 시스템통합자	선주사	선급
식별						
이 지침의 적용을 받는 컴퓨터기반시스템의 하드웨어 소프트웨어 및 이러한 시스템들을 서로 연결하거나 육상에 연결하는 네트워크 인벤토리	선내 컴퓨터기반시스템 및 선내 소프트웨어 목록	설계	제출			승인
		건조		유지관리		정보확인
		시운전		제출		승인
		운영			유지관리	
		검사			제시	검증
보호						
구역의 다이어그램, 도선 및 트래픽 필터링/쉐이핑 규칙의 구성을 포함하여, 네트워크 분할을 구성하기 위해 제공되는 제품, 장비 또는 구성품의 문서	네트워크 분할 / 분리	설계	제출			승인
		건조		유지관리		정보확인
		시운전		제출		정보확인
		운영			유지관리	
		검사			제시	검증
구현된 통제를 검증하기 위한 시험계획을 포함한 네트워크 보호 조치에 대한 문서	네트워크 보호 안전조치	설계	제출			정보확인
		건조		유지관리		정보확인
		시운전		제출		승인
		운영			유지관리	
		검사			제시	검증
설치되는 안티바이러스, 안티멀웨어 및 안티스팸 소프트웨어 또는 적용된 다른 보안 조치들	안티바이러스, 안티멀웨어, 안티스팸 및 악성코드에 대한 기타 보호	설계	제출			승인
		건조		유지관리		정보확인
		시운전		제출		정보확인
		운영			유지관리	
		검사			제시	검증

표 3 행동 및 문서의 요약 (계속)

문서	참조 요구사항	단계	공급업체	조선소 시스템통합자	선주사	선급
설치 위치, 물리적 접근 제한, 신원 관리 정책, 이동식 미디어 접근 지점	물리 및 논리 접근 통제	설계	제출			정보확인
		건조		유지관리		승인
		시운전		제출		정보확인
		운영			유지관리	
		검사			제시	검증
무선 네트워크 다이어그램, 보안 기능, 다른 네트워크와 연결	무선 통신	설계	제출			승인
		건조		유지관리		정보확인
		시운전		제출		정보확인
		운영			유지관리	
		검사			제시	검증
원격 연결 정책 및 절차, 역할 및 책임	원격 접근 통제 및 원격 유지보수	설계	제출			정보확인
		건조		유지관리		정보확인
		시운전		제출		정보확인
		운영			유지관리	
		검사			제시	검증
모바일 및 유대용 장치의 사용에 대한 정책 및 절차서, 역할 및 책임	모바일 및 휴대용 장치의 사용	설계	제출			정보확인
		건조		유지관리		정보확인
		시운전		제출		승인
		운영			유지관리	
		검사			제시	검증
탐지						
네트워크 모니터 방법에 대한 기술, 시험계획;교육 및 훈련 계획	네트워크 운영 모니터링	설계	제출			정보확인
		건조		유지관리		정보확인
		시운전		제출		승인
		운영			유지관리	
		검사			제시	검증
컴퓨터기반시스템 및 네트워크 장치의 모니터링, 경보 및 진단 기능	컴퓨터기반시스템 및 네트워크의 진단 기능	설계	제출			정보확인
		건조		유지관리		정보확인
		시운전		제출		정보확인
		운영			유지관리	
		검사			제시	검증

표 3 행동 및 문서의 요약 (계속)

문서	참조 요구사항	단계	공급업체	조선소 시스템통합자	선주사	선급
대응						
사이버 사고를 알리는데 사용되는 경보 및 기타 수단 및 이러한 사고에 대응하는 절차; 교육 및 훈련 계획	사고 대응 계획	설계	제출			승인
		건조		유지관리		정보확인
		시운전		제출		정보확인
		운영			유지관리	
		검사			제시	검증
로컬 독립 및/또는 수동 운전을 활성화하는 방법에 대한 지침 (사고 대응 계획의 일부)	로컬, 독립 및/또는 수동 운전	설계	제출			승인
		건조		유지관리		정보확인
		시운전		제출		정보확인
		운영			유지관리	
		검사			제시	검증
효과적인 방식으로 네트워크를 직원이 격리하는 지침 (사고 대응 계획의 일부)	네트워크 격리	설계	제출			승인
		건조		유지관리		정보확인
		시운전		제출		정보확인
		운영			유지관리	
		검사			제시	검증
인간 운영자 인수 요청 시 따라야 하는 절차를 포함하여 예기치 않거나 관리할 수 없는 고장 또는 사이버 이벤트의 경우 도달되는 최소 위험 조건	최소 위험 조건으로 폴백	설계	제출			승인
		건조		유지관리		정보확인
		시운전		제출		정보확인
		운영			유지관리	
		검사			제시	검증
복구						
장애 시스템의 복구를 위한 지침 및 절차; 육상으로부터 외부 지원 및 도움을 얻는 방법; 교육 및 훈련 계획	복구 계획	설계	제출			정보확인
		건조		유지관리		정보확인
		시운전		제출		승인
		운영			유지관리	
		검사			Make avail.	검증
데이터 및 소프트웨어의 백업 및 복구 절차 및 운영; 교육 및 훈련 계획	백업 및 복구 능력	설계	제출			정보확인
		건조		유지관리		정보확인
		시운전		제출		정보확인
		운영			유지관리	
		검사			제시	검증

표 3 행동 및 문서의 요약 (계속)

문서	참조 요구사항	단계	공급업체	조선소 시스템통합자	선주사	선급
제어된 종료를 실행, 초기화 상태로 재설정, 안전 상태로 롤백, 빠르고 안전한 복구를 허용하기 위한 처음부터 재시작하기 위한 방법에 대한 문서	제어된 종료, 재설정, 롤백 및 재시작	설계	제출			승인
		건조		유지관리		정보확인
		시운전		Provide		정보확인
		운영			유지관리	
		검사			제시	검증
성능 평가 및 시험						
검사원 또는 다른 제3자가 의도된 시험 조건을 선내 재현하고, 시험을 실행하고, 시험 결과를 검증하며, 공급자 및/또는 조선소/시스템가 얻은 결과와 비교가 가능하도록 시험 절차를 기술하는 시험계획. 시험 절차에는 기능 시험, 고장 시험, 정상 상태, 경고 및 경보를 알리는 데 사용되는 경보 및 기타 모니터링 수단에 대한 설명이 포함되어야 한다.	성능 평가 및 시험	설계	제출			승인
		건조		유지관리		정보확인
		시운전		제출		정보확인
		운영			유지관리	
		검사			제시	검증
리스크 평가						
사이버 위험 및 관련 완화 조치 식별을 목적으로 하는 공급 제품, 장비 또는 구성품에 대한 리스크 평가 (관련 요구사항의 제외된 적용들의 간략한 목록 포함)	요구사항 적용으로부터 컴퓨터기반시스템 제외를 위한 리스크 평가	설계	제출			승인
		건조		유지관리		정보확인
		시운전		제출		승인
		운영			유지관리	
		검사			제시	검증

사이버 복원력 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)