2020

해상 사이버보안 형식 승인 지침

GC-31-K

한 국 선 급

“해상 사이버보안 형식 승인 지침”의 적용

1. 별도로 명시하지 않는 한, 이 지침은 2020년 7월 1일 이후 선박에 탑재되는 사이버 물리시스템(이하 사이버 시스템)에 대하여 사이버보안 형식 승인을 받고자 검사 신청하는 사이버 시스템에 적용한다.
2. 2019년판 지침에 대한 개정사항 및 그 적용일자는 아래와 같다.

적용일자 : 2020년 1월 1일

제 1 장 일반사항

제 1 절 일반사항

- 103.을 개정함

차 례

제 1 장 일반사항

제 1 절 일반사항

101. 적용

1. 이 지침은 선박에 탑재되는 원격 접속 장비, 통합 제어 및 모니터링 시스템 등을 포함하는 사이버 시스템에 적용한다.
2. 이 지침은 사이버 시스템의 사이버보안 수준 및 그 수준에 해당하는 요건을 규정하며, 적용하고자 하는 범위는 신청자의 요청에 의해 결정된다.
3. 이 지침에 따른 사이버보안 형식 승인은 **선급 및 강선규칙**에서 명시하지 않는 한 강제 사항이 아니다.
4. 이 지침에서 규정하지 아니하는 사항은 **선급 및 강선규칙과 제조법 및 형식승인 등에 관한 지침**의 각 해당 요건에 따른다. 다만, 사이버 물리 시스템에 적용할 수 없는 요건은 제외한다.
5. 이 지침에 포함되지 않은 사항에 대하여는 우리 선급이 적절하다고 인정하는 바에 따라 ISO, IEC 또는 이와 동등 이상의 인정된 기준에 따를 수 있다.
6. 본 지침의 규정 이외에 IMO 등 국제 규정에 따른 별도 요건이 있거나 정보통신기술 및 사이버위협의 발전에 따라 우리 선급이 필요하다고 인정되는 경우 추가적인 고려사항 및 요건이 요구될 수도 있다.

102. 용어의 정의

용어의 정의는 여기에 별도로 정하는 경우를 제외하고는 **선급 및 강선규칙**에 따른다.

1. **"인증**(Authentication)"이라 함은 개체의 신고된 신원을 확인하는 것을 말한다.
2. **"인증자**(Authenticator)"라 함은 개체의 신원을 확인하기 위하여 사용되는 수단을 말한다.
3. **"진본성**(Authenticity)"이라 함은 기록의 물리적 특징, 구조, 내용과 맥락 등을 포함하여, 내적·외적 증거로부터 추론할 수 있는 기록의 품질로서 어떤 기록이 위조되지 않은 원래 그대로의 것이며 훼손된 바 없는 상태인 것을 말한다.
4. **"권한**(Authorization)"이라 함은 시스템 리소스에 접속할 수 있도록 시스템 개체에 부여된 권한 또는 허가를 말한다.
5. **"가용성**(Availability)"이라 함은 시스템 정보 및 기능에 대한 시기적절하고 신뢰할 수 있는 접속을 보장하는 속성을 말한다.
6. **"구성품**(Component)"이라 함은 하나 이상의 호스트 장비, 네트워크 장비, 소프트웨어 애플리케이션 또는 임베디드 장비의 특성을 나타내는 시스템에 속한 개체를 말한다.
7. **"기밀성**(Confidentiality)"이라 함은 접근 권한이 없는 개인, 프로세스 또는 장치에 정보가 노출되지 않는다는 보장을 말한다.
8. **"사이버 물리 시스템**(Cyber-physical System)"이라 함은 컴퓨팅, 네트워킹 및 물리적 프로세스의 통합된 시스템을 말한다.
9. **"이벤트**(Event)"라 함은 특정 상황의 발생 또는 변경을 말한다.
10. **"포워더**(Forwarder)"이라 함은 통제된 네트워크 간에 데이터 스트림을 안전하게 교환할 수 있는 네트워크 인프라 장치를 말한다.
11. **"게이트웨이**(Gateway)"이라 함은 보안/제어된 네트워크를 보안/제어되지 않은 네트워크에 연결하는 데 사용되는 네트워크 인프라 장치를 말한다.
12. **"호스트**(Host)"라 함은 하나 이상의 공급업체로부터 하나 이상의 소프트웨어 애플리케이션, 데이터 저장소 또는 기능을 호스팅할 수 있는 운영 체제를 실행하는 범용 장치를 말한다.
13. **"무결성**(Integrity)"이라 함은 자산의 정확성과 완전성을 보호하는 속성을 말한다.
14. **"인터페이스**(Interface)"라 함은 논리 정보 흐름을 위한 모듈에 대한 액세스를 제공하는 논리적 진입점을 말한다.
15. **"최소 권한**(Least Privilege)"이라 함은 사용자(인간, 소프트웨어 프로세스 또는 장치)에게 할당된 업무와 기능에 맞는 가장 적은 권한을 할당하여야 한다는 기본 원칙을 말한다.
16. **"악성코드**(Malicious Code)"라 함은 컴퓨터 운영을 방해하기 위하여 사용되거나 생성된 소프트웨어를 말한다.
17. **"모바일 코드**(Mobile Code)"이라 함은 수신자에 의해 명시적인 설치 없이 실행될 수 있는 자산 간에 전송되는 프로그램을 말한다.
18. **"노드**(Node)"이라 함은 네트워크에 연결되며 인터넷 주소를 보유하는 물리적 장치를 말한다.
19. **"부인방지**(Non-repudiation)"이라 함은 신고된 사건이나 조치의 발생을 증명할 수 있는 능력을 말한다.
20. **"원격 접속**(Remote Access)"이라 함은 지정된 구역 외부에서 통신하는 사용자(인간, 소프트웨어 프로세스 또는 장

치)에 의한 구성품에 대한 접속을 말한다.

21. **"이동식 외부 데이터 저장매체(REDS)"**라 함은 컴팩트 디스크, 메모리 스틱 및 블루투스 장비를 포함하여 이에 국한되지 않는 사용자 이동식 비네트워크 데이터 소스를 말한다.
22. **"시크릿(Secret)"**이라 함은 정보를 알 의도를 제외하고 시스템 객체에 의해 알려지는 것으로부터 보호된 정보 상태를 말한다.
23. **"보안 수준(Security Level)"**이라 함은 구역 또는 도관에 대한 리스크 평가에 기초한 구역 또는 도관 내 장치 및 시스템의 필수 보안 특성 및 고유한 보안 특성에 해당하는 수준을 말한다.
24. **"세션(Session)"**이라 함은 둘 이상의 통신 구성품 간의 반영구적, 상태적인 정보 교환을 말한다.
25. **"스위치(Switch)"**이라 함은 네트워크 내 노드들을 상호연결하는데 사용하는 네트워크 인프라 장치를 말한다.
26. **"신뢰할 수 없는(Untrusted)"**이라 함은 운영, 데이터 트랜잭션 소스, 네트워크 또는 소프트웨어 프로세스가 예상대로 동작하도록 신뢰할 수 있도록 보장하기 위해 미리 정의된 요구사항을 충족하지 않음을 말한다.
27. **"사용자(User)"**라 함은 권한이 있는지 여부에 관계없이 시스템에 접속하는 개인, 조직 개체 또는 자동 프로세스를 말한다.

103. 동등효력

이 지침에 만족하지 않거나 적용할 수 없는 대체설계 및 신기술의 동등효력에 대해서는 **선급 및 강선규칙 1편 1장 104.**를 따른다. *(2020)*

104. 제외사항

우리 선급은 사이버 시스템에 대하여 이 지침에 명시되지 않은 기타 기술적인 특성에 대하여는 책임을 지지 아니한다. 다만, 위의 사항에 대하여 문의가 있을 때는 자문에 응할 수 있다. ⚓

제 2 장 사이버보안 형식 승인

제 1 절 일반사항

101. 일반사항

1. 이 지침에 적용되는 사이버 시스템은 4가지 분류로 구분된다.
   (1) 노드 : 소프트웨어 애플리케이션, 임베디드 장비 및 호스트 장비
   (2) 스위치 : 네트워크 장비
   (3) 포워더 : 네트워크 장비, 소프트웨어 애플리케이션 및 호스트 장비
   (4) 게이트웨이 : 네트워크 장비, 소프트웨어 애플리케이션 및 호스트 장비

제 2 절 승인 절차

201. 승인 신청

1. 승인 신청자는 원칙적으로 승인 신청한 사이버 장비 및/또는 시스템의 제조자로 한다. 다만, 우리 선급이 지장이 없다고 인정하는 경우에는 사이버 장비 및/또는 시스템의 제조자가 아니라도 신청할 수 있다.
2. 사이버보안 형식 승인을 받고자 하는 신청자는 형식 승인 신청서 1부 및 첨부자료 중 승인용은 3부, 참고용은 2부를 우리 선급에 제출하여야 한다. 다만, 선급기술규칙의 규정에 따라 이미 제출한 자료와 중복되는 자료에 대하여는 제출을 생략할 수 있다.
3. 우리 선급이 필요하다고 인정하는 경우에는 4항에 규정된 것 이외의 자료의 제출을 요구할 수 있다.
4. **승인용 자료**
   (1) 기능사양 명세서
   (2) 시스템 토폴로지
   (3) 시스템 도면
   (4) 자산 목록
   (5) 사이버보안 관련 시험 절차서
   (6) 사용자 및/또는 운영자 매뉴얼
   (7) 리스크 평가 보고서
5. **참고용 자료**
   (1) 구성품 간 인증 메커니즘 자료

202. 자료심사

우리 선급은 제출된 사이버보안 시험 계획서, 도면 및 자료를 심사하여 적절하다고 인정되는 경우에는 사이버보안 시험 계획 등을 승인하여 신청자에게 송부한다.

203. 사이버보안 시험

1. 사이버보안 시험은 **전** 202.에 의해 자료 심사 등이 만족되는 경우, 검사원의 입회하에 시험 제품에 대하여 승인된 사이버보안 시험 절차서 및 우리 선급이 적절하다고 인정하는 시험방법으로 시행한다.
2. **전 1항**의 사이버보안 시험에 불합격한 제품에 대하여는 원칙적으로 설계(사양) 변경 없이 동일한 제품으로 재시험을 하여서는 아니 된다. 다만, 불합격의 원인이 제품이 아닌 시험 관련 조건 등으로 우리 선급이 인정하는 경우에는 예외로 한다.
3. 사이버보안 시험은 원칙적으로 제조공장에서 한다. 다만, 우리 선급이 인정하는 경우에는 제조공장 이외에서 시행할 수 있다.
4. 우리 선급이 인정하는 선급 또는 시험기관에서 시행하는 시험성적서나 증명서를 가진 경우에는 사이버보안 시험의 일부 또는 전부를 생략할 수 있다.
5. 신청자는 형식시험 완료 후, 시험성적서 3부를 우리 선급에 제출하여야 한다.

204. 공장조사

제조법 및 형식승인 등에 관한 지침 3장 105. 공장조사에 따른다. 기자재 형식승인을 동시에 진행하거나 형식 승인을 받은 경우 공장조사를 생략할 수 있다.

205. 인증 통지 등

제조법 및 형식승인 등에 관한 지침 3장 106. 승인 통지 등에 따른다.

206. 인증 내용의 변경

제조법 및 형식승인 등에 관한 지침 3장 107. 승인내용의 변경에 따른다.

207. 인증서의 유효기간 및 갱신 등

1. 승인 증서의 유효기간은 증서 발행일로부터 3년 이내로 한다. 단, 206.에 따라 승인증서를 재교부할 경우에는 증서 유효기간을 구증서의 유효기간으로 한다.
2. 승인증서의 유효기간 갱신 및 연장은 **제조법 및 형식승인 등에 관한 지침 2장 108. 승인증서의 유효기간 갱신 및 연장 등**에 따른다. 단, 연장 종료후 다시 발생하는 증서의 유효기간은 구증서의 유효기간 말료일의 익일부터 3년 이내로 한다.

208. 확인시험 및/또는 임시공장조사

제조법 및 형식승인 등에 관한 지침 3장 109. 확인시험 및/또는 임시공장조사에 따른다.

209. 인증의 일시정지 및 취소

제조법 및 형식승인 등에 관한 지침 3장 110. 승인의 일시정지 및 취소에 따른다. ⚓

제 3 장 사이버보안 요건

제 1 절 일반사항

101. 일반사항

1. 보안 레벨의 수준은 아래와 같다.
   (1) 보안수준(SL) 1은 우발적이나 우연한 위반에 대하여 시스템을 보호할 수 있는 수준이다.
   (2) 보안수준(SL) 2는 낮은 리소스, 낮은 동기를 가지고 단순한 방법을 사용하는 의도적인 침해로부터 시스템을 보호할 수 있는 수준이다.
   (3) 보안수준(SL) 3은 중간 리소스, 중간 동기를 가지고 정교한 방법을 사용하는 의도적인 침해로부터 시스템을 보호할 수 있는 수준이다.
   (4) 보안수준(SL) 4는 확장된 리소스, 높은 동기를 가지고 정교한 방법을 사용하여 의도적인 침해로부터 시스템을 보호할 수 있는 수준이다.
2. 별도로 명시하지 않는 한 구성품이 높은 보안수준 요건을 준수하기 위해서는 하위의 보안수준 요건을 모두 준수하여야 한다.

제 2 절 식별 및 인증

201. 인간 사용자 식별 및 인증

1. 구성품은 모든 인간 사용자 접속을 지원하는 모든 인터페이스에서 ISA-62443-4-2 CR 1.1 **사용자 식별 및 인증**을 따라 모든 사용자를 식별하고 인증할 수 있는 기능을 제공하여야 한다.
2. 사용자 식별 및 인증이 신속한 현장 비상조치를 방해해서는 아니 된다.
3. 구성품은 모든 인간 사용자를 고유하게 식별하고 인증할 수 있는 기능을 제공하여야 한다.
4. 구성품은 구성품에 접속하는 모든 인간 사용자에 대해 다중요소 인증을 사용할 수 있는 기능을 제공하여야 한다.
5. **보안 레벨별 요건**
   (1) SL 1 : 201. 2
   (2) SL 2 : 201. 3
   (3) SL 3 : 201. 4
   (4) SL 4 : 201. 4

202. 소프트웨어 프로세스 및 장비 식별 및 인증

1. 구성품은 ISA-62443-4-2 CR 1.2. **소프트웨어 프로세스 및 기기 식별 및 인증**에 따라 자신을 식별하고 다른 구성품(소프트웨어 애플리케이션, 내장 장비, 호스트 장비 및 네트워크 장비)를 인증할 수 있는 기능을 제공하여야 한다.
2. 구성품은 다른 장비에 대해 자신을 고유하고 안전하게 식별하고 인증할 수 있는 기능을 제공하여야 한다.
3. **보안 레벨별 요건**
   (1) SL 1 : 해당 없음
   (2) SL 2 : 202. 1
   (3) SL 3 : 202. 2
   (4) SL 4 : 202. 2

203. 계정 관리

1. 구성품은 ISA-62443-4-2 CR 1.3. **계정 관리**에 따라 모든 계정 관리를 직접 지원하거나 계정을 관리하는 시스템에 통합할 수 있는 기능을 제공하여야 한다.
2. **보안 레벨별 요건**
   (1) SL 1 : 203. 1

(2) SL 2 : 203. 1
(3) SL 3 : 203. 1
(4) SL 4 : 203. 1

204. 식별자 관리

1. 구성품은 ISA-62443-4-2 CR 1.4. **식별자 관리**에 따라 직접 식별자 관리를 지원하거나 식별자 관리를 제공하는 시스템에 통합할 수 있는 기능을 제공하여야 한다.
2. **보안 레벨별 요건**
(1) SL 1 : 204. 1
(2) SL 2 : 204. 1
(3) SL 3 : 204. 1
(4) SL 4 : 204. 1

205. 인증자 관리

1. 구성품은 다음의 기능을 제공하여야 한다.
(1) 최초 인증자 콘텐츠 사용 지원
(2) 설치 시 이루어진 기본 인증자에 대한 변경 사항 인식 지원
(3) 정기적인 인증자 변경/교체 작업에 적합한 기능
(4) 인증자를 저장, 사용 및 전송할 때 허가받지 않은 공개와 변경으로부터 인증자 보호
2. 구성품이 의존하는 인증자는 OTP 메모리와 같은 하드웨어 메커니즘을 통해 보호되어야 한다.
3. **보안 레벨별 요건**
(1) SL 1 : 205. 1
(2) SL 2 : 205. 1
(3) SL 3 : 205. 2
(4) SL 4 : 205. 2

206. 비밀번호 기반 인증 강화

1. 비밀번호 기반 인증을 사용하는 구성품의 경우, 이러한 구성품은 최소 길이 및 다양한 문자 유형을 기반으로 구성 가능한 비밀번호 강도를 적용할 수 있는 기능을 제공하거나, 이 기능을 제공하는 시스템에 통합되어야 한다.
2. 구성품은 모든 사용자들에게 암호의 최소 및 최대 수명 제한을 적용할 수 있는 기능을 제공하거나 기능을 제공하는 시스템으로 통합되어야 한다.
3. 구성품은 구성 가능한 수의 암호를 재사용하는 것으로부터 인간 사용자 계정을 보호하는 기능을 제공하거나 기능을 제공하는 시스템으로 통합되어야 한다. 또한 구성품은 인간 사용자에게 암호의 최소 및 최대 수명 제한을 적용할 수 있는 기능을 제공하여야 한다. 또한 구성품은 인간 사용자에게 만료 전 구성 가능한 시간에 암호를 변경하도록 요청하는 기능을 제공하여야 한다. 이러한 기능은 일반적으로 수용되는 보안 업계의 관행을 준수하여야 한다.
4. 구성품은 사용자에게 만료 전 구성 가능한 시간에 비밀번호를 변경하도록 요청하는 기능을 제공하여야 한다.
5. **보안 레벨별 요건**
(1) SL 1 : 206. 2
(2) SL 2 : 206. 2
(3) SL 3 : 206. 3
(4) SL 4 : 206. 4

207. 공개 키 인프라 인증

1. 공용 키 기반 구조 (PKI)를 사용할 경우, 구성품은 ISA 62443-4-2 CR1.8에 따라 공용 키 기반 구조의 영역 내에서 상호작용하고 작동할 수 있는 기능을 제공하거나 기능을 제공하는 시스템으로 통합되어야 한다.
2. **보안 레벨별 요건**
(1) SL 1 : 해당 없음
(2) SL 2 : 207. 1
(3) SL 3 : 207. 1

(4) SL 4 : 207. 1

208. 공개 키 인증 강화

1. 공개 키 인증을 사용하는 구성품의 경우, 구성품은 다음과 같은 환경 내에서 기능을 직접 제공하거나 기능을 제공하는 시스템으로 통합하여야 한다.
(1) 지정된 인증서의 서명 유효성 확인을 통한 인증서 검증
(2) 인증서 체인 또는 자체 서명된 인증서의 경우 인증서를 발급하는 대상과 통신하는 모든 호스트에 리프 인증서를 배포하여 검증
(3) 지정된 인증서의 해지 상태를 확인하여 인증서 검증
(4) 해당 개인 키의 사용자(인간, 소프트웨어 프로세스 또는 장비) 통제 수립
(5) 인증된 ID를 사용자(인간, 소프트웨어 프로세스 또는 장비)에 매핑
(6) 공개 키 인증에 사용되는 알고리즘과 키가 503.을 준수하는지 확인
2. 구성품은 하드웨어 메커니즘을 통해 중요한 장기적인 개인 키를 보호하는 기능을 제공하여야 한다.
3. **보안 레벨별 요건**
(1) SL 1 : 해당 없음
(2) SL 2 : 208. 1
(3) SL 3 : 208. 2
(4) SL 4 : 208. 2

209. 인증자 피드백

1. 구성품이 인증 기능을 제공할 때 구성품은 인증 프로세스 동안 인증 정보의 피드백을 숨기는 기능을 제공하여야 한다.
2. **보안 레벨별 요건**
(1) SL 1 : 209. 1
(2) SL 2 : 209. 1
(3) SL 3 : 209. 1
(4) SL 4 : 209. 1

210. 실패한 로그인 시도

1. 구성품이 인증 기능을 제공할 경우 구성품은 구성 가능한 기간 동안 사용자(인간, 소프트웨어 프로세스 또는 장비)에 의한 구성 가능한 연속으로 유효하지 않은 접속 시도 횟수를 제한할 수 있는 기능과 지정된 시간 동안 또는 이 제한이 다 되도록 관리자에 의해 잠금 해제될까지 접속을 거부할 수 있는 기능을 제공하여야 한다.
2. **보안 레벨별 요건**
(1) SL 1 : 210. 1
(2) SL 2 : 210. 1
(3) SL 3 : 210. 1
(4) SL 4 : 210. 1

211. 시스템 사용 알림

1. 구성품이 로컬 인간 사용자 접속/HMI를 제공할 때 인증 전에 시스템 사용 알림 메시지를 표시하는 기능을 제공하여야 한다. 시스템 사용 알림 메시지는 인가된 작업자에 의해 구성되어야 한다.
2. **보안 레벨별 요건**
(1) SL 1 : 211. 1
(2) SL 2 : 211. 1
(3) SL 3 : 211. 1
(4) SL 4 : 211. 1

212. 대칭 키 인증 강화

1. 대칭 키 인증을 사용하는 구성품의 경우 구성품은 다음과 같은 기능을 제공하여야 한다.
   (1) 대칭 키를 사용하는 상호신뢰 확립
   (2) 공유 암호의 안전한 저장 (공유된 암호가 비밀로 유지되는 한 인증이 유효함)
   (3) 공유된 비밀에 대한 접속 차단
   (4) 대칭 키 인증에 사용되는 알고리즘 및 키가 503.을 준수하는지에 대한 확인
2. 구성품은 하드웨어 메커니즘을 통해 중요한 장기적인 대칭 키를 보호하는 기능을 제공하여야 한다.
3. **보안 레벨별 요건**
   (1) SL 1 : 해당 없음
   (2) SL 2 : 212. 1
   (3) SL 3 : 212. 2
   (4) SL 4 : 212. 2

제 3 절 사용 제어

301. 권한 부여 시행

1. 구성품은 할당된 책임을 바탕으로 모든 식별되고 권한이 인증된 사용자에 대하여 권한 부여 시행 메커니즘을 제공하여야 한다.
2. 구성품은 할당된 책임과 최소한의 권한을 바탕으로 모든 사용자들에게 권한 부여 시행 메커니즘을 제공하여야 한다.
3. 구성품은 직접 또는 보상 보안 메커니즘을 통해 모든 인간 사용자들의 역할에 대한 매핑을 정의하고 수정할 수 있는 승인된 역할을 제공하여야 한다.
4. 구성품은 구성 가능한 시간 또는 일련의 이벤트에 대하여 관리자 수동 오버라이드를 지원하여야 한다. 운영자가 현재 세션을 닫고 새로운 세션을 더 높은 권한의 인간 사용자로 설정하지 않고 비정상적인 조건에 신속하게 대응할 수 있도록 할 수 있도록 하여야 한다.
5. 구성품은 조치가 산업 프로세스에 심각한 영향을 미칠 수 있는 경우 이중 승인을 지원하여야 한다. 단, 이중 승인 매커니즘은 산업 프로세스의 비상 정지와 같이 건강, 안전, 환경을 보호하기 위해 즉각적인 대응이 필요한 경우에는 적용되어서는 아니 된다.
6. **보안 레벨별 요건**
   (1) SL 1 : 301. 1
   (2) SL 2 : 301. 3
   (3) SL 3 : 301. 4
   (4) SL 4 : 301. 5

302. 무선 사용

1. 무선 인터페이스를 통해 사용을 지원하는 구성품은 일반적으로 인정되는 산업 관행에 따라 사용 권한 부여, 모니터링 및 제한을 지원하는 시스템에 통합할 수 있는 기능을 제공하여야 한다.
2. **보안 레벨별 요건**
   (1) SL 1 : 302. 1
   (2) SL 2 : 302. 1
   (3) SL 3 : 302. 1
   (4) SL 4 : 302. 1

303. 세션 잠금

1. 구성품이 로컬 또는 네트워크를 통해 접속하거나 인간 사용자 인터페이스를 제공하는 경우 구성품은 다음의 기능을 제공하여야 한다.
   (1) 구성 가능한 시간 동안 활동이 없는 경우 또는 사용자(인간, 소프트웨어 프로세스 또는 장비)의 수동 시작을 통해 세션 잠금을 시작하여 추가 접속으로부터 보호
   (2) 세션을 소유한 인간 사용자 또는 다른 권한을 부여받은 인간 사용자까지 세션 잠금이 유효하게 유지

2. 보안 레벨별 요건

(1) SL 1 : 303. 1
(2) SL 2 : 303. 1
(3) SL 3 : 303. 1
(4) SL 4 : 303. 1

304. 원격 세션 종료

1. 구성품이 원격 세션을 지원하는 경우 구성품은 구성 가능한 시간 후에 자동으로 원격 세션을 종료하거나, 로컬 권한 인가자 또는 세션을 시작한 사용자(인간, 소프트웨어 프로세스 또는 장비)에 의해 수동으로 원격 세션을 종료할 수 있는 기능을 제공하여야 한다.

2. 보안 레벨별 요건

(1) SL 1 : 해당 없음
(2) SL 2 : 304. 1
(3) SL 3 : 304. 1
(4) SL 4 : 304. 1

305. 동시 세션

1. 구성품은 정해진 사용자(인간, 소프트웨어 프로세스 또는 장비)에 대해 인터페이스당 동시 세션 수를 제한하는 기능을 가져야 한다.

2. 보안 레벨별 요건

(1) SL 1 : 해당 없음
(2) SL 2 : 해당 없음
(3) SL 3 : 305. 1
(4) SL 4 : 305. 1

306. 감사 가능한 이벤트

1. 구성품은 다음 범주에 대한 보안 관련 감사 기록을 생성할 수 있는 기능을 제공하여야 한다.
(1) 접속 제어
(2) 요청 에러
(3) 시스템 이벤트
(4) 백업 및 복구 이벤트
(5) 구성 변경
(6) 감사 로그 이벤트
2. 개별 감사 기록은 다음을 포함하여야 한다.
(1) 타임스탬프
(2) 소스(발신 장비, 소프트웨어 프로세스 또는 인간 사용자 계정)
(3) 카테고리
(4) 형식
(5) 이벤트 ID
(6) 이벤트 결과

3. 보안 레벨별 요건

(1) SL 1 : 306. 2
(2) SL 2 : 306. 2
(3) SL 3 : 306. 2
(4) SL 4 : 306. 2

307. 감사 저장소 용량

1. 구성품은 다음을 제공하여야 한다.
(1) 일반적으로 인정되는 로그 관리 권장사항에 따라 감사 기록 저장 용량을 할당할 수 있는 기능

(2) 감사 저장 용량에 도달하거나 초과할 때 구성품의 고장으로부터 보호하는 메커니즘

2. 구성품은 할당된 감사 기록 보관이 구성 가능한 임계값에 도달할 때 경고를 발할 수 있는 기능을 제공하여야 한다.

3. 보안 레벨별 요건

(1) SL 1 : 307. 1
(2) SL 2 : 307. 1
(3) SL 3 : 307. 2
(4) SL 4 : 307. 2

308. 감사 프로세싱 실패 대응

1. 구성품은 감사 프로세싱 실패 시 필수적인 서비스와 기능 상실을 방지하는 기능을 제공하고, 일반적으로 인정되는 산업 관행 및 권고에 따라 감사 프로세싱 실패에 대응하여 적절한 조치를 지원하여야 한다.

2. 보안 레벨별 요건

(1) SL 1 : 308. 1
(2) SL 2 : 308. 1
(3) SL 3 : 308. 1
(4) SL 4 : 308. 1

309. 타임스탬프

1. 구성품은 감사 기록에 사용할 타임스탬프(날짜 및 시간 포함)를 생성하는 기능을 제공하여야 한다.
2. 구성품은 시스템 전체 시간 소스와 동기화된 타임스탬프를 생성할 수 있는 기능을 제공하여야 한다.
3. 시간 동기화 메커니즘은 무단 변경을 탐지하고 변경 시 감사 이벤트를 발생시킬 수 있는 기능을 제공하여야 한다.

4. 보안 레벨별 요건

(1) SL 1 : 309. 1
(2) SL 2 : 309. 2
(3) SL 3 : 309. 2
(4) SL 4 : 309. 3

310. 부인 방지

1. 구성품이 인간 사용자 인터페이스를 제공하는 경우, 구성품은 특정 사용자가 특정 조치를 취했는지 여부를 판단할 수 있는 기능을 제공하여야 한다. 그러한 기능을 지원할 수 없는 구성품은 구성품 목록에 열거되어야 한다.
2. 구성품은 특정 사용자(인간, 소프트웨어 프로세스 또는 장비)가 특정 조치를 취했는지 여부를 결정하는 기능을 제공하여야 한다.

3. 보안 레벨별 요건

(1) SL 1 : 310. 1
(2) SL 2 : 310. 1
(3) SL 3 : 310. 1
(4) SL 4 : 310. 2

311. 이동식 외부 데이터 저장매체 보안

1. 이동식 외부 데이터 저장매체의 연결 지점 수가 시스템 작동, 수명 유지 및 지원에 필요한 최소값으로 제한되어야 한다.
2. 이동식 외부 데이터 저장매체의 연결 지점이 도구나 인증 키 없이 사용자가 쉽게 접근할 수 없도록 차단되어야 한다.
3. 이동식 외부 데이터 저장매체의 연결 지점의 경우 키보드 또는 마우스 장치를 연결하더라도 연결된 장치를 인식하지 않고 연결된 장치로 기능 수행이 거부되어야 한다.
4. 이동식 외부 데이터 저장매체의 모든 파일 형식에 대하여 자동 실행을 금지하고, 수동 실행을 제공하는 경우 디지털 서명 또는 특수 키로 확인된 파일에만 수동 실행이 가능하여야 한다.

5. 보안 레벨별 요건

(1) SL 1 : 311. 4
(2) SL 2 : 311. 4

(3) SL 3 : 311. 4
(4) SL 4 : 311. 4

제 4 절 시스템 무결성

401. 통신 무결성

1. 구성품은 전송된 정보의 무결성을 보호할 수 있는 기능을 제공하여야 한다.
2. 구성품은 통신 중에 수신한 정보의 인증을 검증할 수 있는 기능을 제공하여야 한다.
3. **보안 레벨별 요건**
   (1) SL 1 : 401. 1
   (2) SL 2 : 401. 2
   (3) SL 3 : 401. 2
   (4) SL 4 : 401. 2

402. 보안 기능성 검증

1. 구성품은 ISA-62443-4-2 CR 3.3. **보안 기능성 검증**에 따라 의도된 보안 기능의 작동을 확인할 수 있는 기능을 제공하여야 한다.
2. 구성품은 정상 작동 중 의도된 보안 기능의 작동을 확인할 수 있는 기능을 제공하여야 한다. 단, 시스템에 대한 악영향을 방지하기 위하여 신중하게 구현될 필요가 있으며, 안전시스템에는 적합하지 않을 수 있다.
3. **보안 레벨별 요건**
   (1) SL 1 : 402. 1
   (2) SL 2 : 402. 1
   (3) SL 3 : 402. 1
   (4) SL 4 : 402. 2

403. 소프트웨어 및 정보 무결성

1. 구성품은 소프트웨어, 구성 및 기타 정보에 대한 무결성 검사를 수행하거나 지원할 수 있는 기능을 제공하여야 하며 이러한 검사 결과를 기록 및 보고하거나 무결성 검사를 수행 또는 지원할 수 있는 시스템에 통합하여야 한다.
2. 구성품은 소프트웨어, 구성 및 기타 정보에 대한 진본성 점검을 수행하거나 지원할 수 있는 기능을 제공하여야 하며 이러한 검사 결과를 기록 및 보고하거나 무결성 검사를 수행 또는 지원할 수 있는 시스템에 통합하여야 한다.
3. 구성품이 무결성 검사를 수행하는 경우 무단 변경을 시도하는 것을 발견하면 구성 가능한 객체에 자동으로 통지하는 기능을 제공하여야 한다.
4. **보안 레벨별 요건**
   (1) SL 1 : 403. 1
   (2) SL 2 : 403. 2
   (3) SL 3 : 403. 3
   (4) SL 4 : 403. 3

404. 입력값 검증

1. 구성품은 구성품의 작동에 직접적인 영향을 미치는 외부 인터페이스를 통해 산업 프로세스 제어 입력 또는 입력으로 사용되는 입력 데이터의 구문, 길이 및 내용을 확인하여야 한다.
2. **보안 레벨별 요건**
   (1) SL 1 : 404. 1
   (2) SL 2 : 404. 1
   (3) SL 3 : 404. 1
   (4) SL 4 : 404. 1

405. 결정론적 출력

1. 자동화 프로세스에 물리적으로 또는 논리적으로 연결하는 구성품은 구성품 공급업체가 정의한 정상적인 작동이 유지되지 않을 경우 출력을 미리 결정된 상태로 설정할 수 있는 기능을 제공하여야 한다.

2. 보안 레벨별 요건

(1) SL 1 : **405. 1**
(2) SL 2 : **405. 1**
(3) SL 3 : **405. 1**
(4) SL 4 : **405. 1**

406. 에러 핸들링

1. 구성품은 구성품을 공격하기 위하여 상대방이 이용할 수 있는 정보를 제공하지 않는 방식으로 오류 상태를 식별하고 처리하여야 한다.

2. 보안 레벨별 요건

(1) SL 1 : 해당 없음
(2) SL 2 : **406. 1**
(3) SL 3 : **406. 1**
(4) SL 4 : **406. 1**

407. 세션 무결성

1. 구성품은 다음을 포함하는 통신 세션의 무결성을 보호하는 메커니즘을 제공하여야 한다.
   (1) 사용자 로그아웃 또는 기타 세션 종료 시 세션 식별자를 무효화하는 기능(브라우저 세션 포함)
   (2) 각 세션에 대해 고유한 세션 식별자를 생성하고 시스템에서 생성된 세션 식별자만 인식하는 기능
   (3) 일반적으로 허용되는 무작위 소스에서 고유한 세션 식별자를 생성하는 기능

2. 보안 레벨별 요건

(1) SL 1 : 해당 없음
(2) SL 2 : **407. 1**
(3) SL 3 : **407. 1**
(4) SL 4 : **407. 1**

408. 감사 정보 보호

1. 구성품은 무단 접속, 변경 또는 삭제로부터 감사 정보, 로그, 도구(있는 경우)들을 보호하여야 한다.
2. 구성품은 하드웨어 강제 1회 쓰기(write-once) 미디어에 감사기록을 저장할 수 있는 기능을 제공하여야 한다.

3. 보안 레벨별 요건

(1) SL 1 : 해당 없음
(2) SL 2 : **408. 1**
(3) SL 3 : **408. 1**
(4) SL 4 : **408. 2**

제 5 절 데이터 기밀성

501. 정보 기밀성

1. 구성품은 명시적 읽기 허가가 지원되는 미사용 정보의 기밀성을 보호하여야 하며, ISA 62443-4-2 CR 4.1 **정보 기밀성**에 정의된 바와 같이 전송 중인 정보의 기밀성 보호를 지원하여야 한다.

2. 보안 레벨별 요건

(1) SL 1 : **501. 1**
(2) SL 2 : **501. 1**
(3) SL 3 : **501. 1**

(4) SL 4 : 501. 1

502. 정보 지속성

1. 구성품은 명시적 읽기 권한이 지원되는 모든 정보를 활성 서비스에서 해제 및/또는 해제된 구성품에서 삭제할 수 있는 기능을 제공하여야 한다.
2. 구성품은 휘발성 공유 메모리 리소스를 통한 무단 및 의도하지 않은 정보 전송으로부터 보호하는 기능을 제공하여야 한다.
3. 구성품은 정보의 삭제가 발생했음을 확인할 수 있는 기능을 제공하여야 한다.
4. **보안 레벨별 요건**

(1) SL 1 : 해당 없음
(2) SL 2 : 502. 1
(3) SL 3 : 502. 3
(4) SL 4 : 502. 3

503. 암호화 사용

1. 암호화가 요구되는 경우 구성품은 국제적으로 인정되고 입증된 보안 관행 및 권장사항에 따라 암호화 보안 메커니즘을 사용하여야 한다.
2. **보안 레벨별 요건**

(1) SL 1 : 503. 1
(2) SL 2 : 503. 1
(3) SL 3 : 503. 1
(4) SL 4 : 503. 1

제 6 절 제한된 데이터 흐름

601. 네트워크 분할

1. 구성품은 필요한 경우 논리적 세분화 및 중요도에 기반한 광범위한 네트워크 아키텍처를 지원하기 위해 분할된 네트워크를 지원하여야 한다.
2. **보안 레벨별 요건**

(1) SL 1 : 601. 1
(2) SL 2 : 601. 1
(3) SL 3 : 601. 1
(4) SL 4 : 601. 1

602. 루프 방지

1. 스위치는 RSTP, MSTP와 같은 루프 방지 매커니즘 기능을 제공하여야 한다. 네트워크 토폴로지 및 스위치 구성은 5초 이내에 정합성을 지원하여야 한다.
2. **보안 레벨별 요건**

(1) SL 1 : 602. 1
(2) SL 2 : 602. 1
(3) SL 3 : 602. 1
(4) SL 4 : 602. 1

제 7 절 사고에 대한 적시 대응

701. 감사 로그 접근성

1. 구성품은 인가된 사람 및/또는 도구에서 읽기 전용으로 감사 로그에 접근할 수 있는 기능을 제공하여야 한다.
2. 구성품은 애플리케이션 프로그래밍 인터페이스(API)를 사용하거나 감사 기록을 중앙 시스템에 전송하여 감사 기록에 대한 프로그래밍 방식의 접속을 제공하여야 한다.
3. **보안 레벨별 요건**
   (1) SL 1 : 701. 1
   (2) SL 2 : 701. 1
   (3) SL 3 : 701. 2
   (4) SL 4 : 701. 2

702. 지속적인 모니터링

1. 구성품은 보안 위반을 적시에 탐지, 특성화 및 보고하기 위하여 일반적으로 인정되는 보안 산업 관행 및 권장사항을 사용하여 지속적으로 모니터링하는 기능을 제공하여야 한다.
2. **보안 레벨별 요건**
   (1) SL 1 : 해당 없음
   (2) SL 2 : 702. 1
   (3) SL 3 : 702. 1
   (4) SL 4 : 702. 1

제 8 절 리소스 가용성

801. 서비스 거부(DoS) 보호

1. 구성품은 DoS 이벤트의 결과로 저하된 모드에서 작동할 때 필수 기능을 유지할 수 있는 기능을 제공하여야 한다.
2. 구성품은 DoS 이벤트의 정보 및/또는 메시지 범람 유형의 영향을 완화하는 기능을 제공하여야 한다.
3. **보안 레벨별 요건**
   (1) SL 1 : 801. 1
   (2) SL 2 : 801. 2
   (3) SL 3 : 801. 2
   (4) SL 4 : 801. 2

802. 리소스 관리

1. 구성품은 리소스 부족을 방지하기 위한 보안 기능을 통해 리소스 사용을 제한하는 기능을 제공하여야 한다.
2. **보안 레벨별 요건**
   (1) SL 1 : 802. 1
   (2) SL 2 : 802. 1
   (3) SL 3 : 802. 1
   (4) SL 4 : 802. 1

803. 시스템 백업

1. 구성품은 구성품의 상태(사용자 및 시스템 수준 정보)를 보호하기 위하여 시스템 수준 백업 작업에 참여할 수 있는 기능을 제공하여야 한다. 백업 프로세스가 구성품의 정상적인 작동에 영향을 미치지 않아야 한다.
2. 구성품은 해당 정보의 복원을 시작하기 전에 백업된 정보의 무결성을 확인할 수 있는 기능을 제공하여야 한다.
3. **보안 레벨별 요건**
   (1) SL 1 : 803. 1
   (2) SL 2 : 803. 2

(3) SL 3 : 803. 2
(4) SL 4 : 803. 2

804. 시스템 복구 및 재구성

1. 구성품은 중단 또는 고장 후 알려진 보안 상태로 복구 및 재구성할 수 있는 기능을 제공하여야 한다.
2. **보안 레벨별 요건**
(1) SL 1 : 804. 1
(2) SL 2 : 804. 1
(3) SL 3 : 804. 1
(4) SL 4 : 804. 1

805. 네트워크 및 보안 구성 세팅

1. 구성품은 시스템 공급업체가 제공하는 지침에 설명된 권장 네트워크 및 보안 구성에 따라 구성할 수 있는 기능을 제공하여야 한다. 구성품은 현재 배치된 네트워크 및 보안 구성 설정에 대한 인터페이스를 제공하여야 한다.
2. 구성품은 현재 배치된 보안 설정을 기계 판독 가능한 형식으로 나열하는 보고서를 생성하는 기능을 제공하여야 한다.
3. **보안 레벨별 요건**
(1) SL 1 : 805. 1
(2) SL 2 : 805. 1
(3) SL 3 : 805. 2
(4) SL 4 : 805. 2

806. 기능 최소화

1. 구성품은 불필요한 기능, 포트, 프로토콜 및/또는 서비스의 사용을 특별히 제한하는 기능을 제공하여야 한다.
2. **보안 레벨별 요건**
(1) SL 1 : 806. 1
(2) SL 2 : 806. 1
(3) SL 3 : 806. 1
(4) SL 4 : 806. 1

807. 시스템 구성품 인벤토리

1. 구성품은 ISA-62443-3-3 SR 7.8**에 따라 제어 시스템 구성품 인벤토리를** 지원하는 기능을 제공하여야 한다.
2. **보안 레벨별 요건**
(1) SL 1 : 해당 없음
(2) SL 2 : 807. 1
(3) SL 3 : 807. 1
(4) SL 4 : 807. 1

제 9 절 소프트웨어 애플리케이션 요건

901. 모바일 코드

1. 소프트웨어 애플리케이션이 모바일 코드 기술을 이용하는 경우 해당 애플리케이션은 모바일 코드 기술 사용에 대한 보안 정책을 시행할 수 있는 기능을 제공하여야 한다. 보안 정책은 최소한 소프트웨어 애플리케이션에 사용되는 각 모바일 코드 기술에 대해 최소한 다음 조치를 허용하여야 한다.
(1) 모바일 코드 실행 통제
(2) 애플리케이션으로부터 모바일 코드를 전송할 수 있는 사용자(인간, 소프트웨어 프로세스 또는 장비) 통제
(3) 코드가 실행되기 전에 모바일 코드에 대한 무결성 검사 결과에 따라 코드의 실행 통제
2. 애플리케이션은 코드가 실행되기 전에 신뢰성 점검 결과에 따라 장비가 모바일 코드의 실행을 제어할 수 있는 보안

정책을 시행할 수 있는 기능을 제공하여야 한다.

3. 보안 레벨별 요건

(1) SL 1 : 901. 1
(2) SL 2 : 901. 2
(3) SL 3 : 901. 2
(3) SL 4 : 901. 2

902. 악성코드로부터 보호

1. 애플리케이션 제품 공급자는 애플리케이션과 호환되는 악성 코드 메커니즘로부터의 보호를 확인하고 문서화하여야 하며, 특별한 구성 요구 사항을 기록하여야 한다.

2. 보안 레벨별 요건

(1) SL 1 : 902. 1
(2) SL 2 : 902. 1
(3) SL 3 : 902. 1
(3) SL 4 : 902. 1

제 10 절 임베디드 장비 요건

1001. 모바일 코드

1. 임베디드 장비가 모바일 코드 기술을 이용하는 경우 임베디드 장비는 모바일 코드 기술 사용에 대한 보안 정책을 시행할 수 있는 기능을 제공하여야 한다. 보안 정책은 임베디드 장비에 사용되는 각 모바일 코드 기술에 대해 최소한 다음 조치를 허용하여야 한다.
   (1) 모바일 코드 실행 제어
   (2) 애플리케이션으로부터 모바일 코드를 전송할 수 있는 사용자(인간, 소프트웨어 프로세스 또는 장비) 제어
   (3) 코드가 실행되기 전에 모바일 코드에 대한 무결성 검사 결과에 따라 코드 실행 제어
2. 임베디드 장비는 코드가 실행되기 전에 신뢰성 점검 결과에 따라 장비가 모바일 코드의 실행을 제어할 수 있는 보안 정책을 시행할 수 있는 기능을 제공하여야 한다.

3. 보안 레벨별 요건

(1) SL 1 : 1001. 1
(2) SL 2 : 1001. 2
(3) SL 3 : 1001. 2
(3) SL 4 : 1001. 2

1002. 물리적 진단 및 시험 인터페이스 사용

1. 임베디드 장비는 물리적 공장 진단 및 시험 인터페이스(예: JTAG 디버깅)에 대한 무단 사용을 방지하여야 한다.
2. 임베디드 장비는 기기의 진단 및 시험 인터페이스에 대한 능동 모니터링을 제공하고 이러한 인터페이스에 접속하려는 시도가 감지될 때 감사 로그 기록을 생성하여야 한다.

3. 보안 레벨별 요건

(1) SL 1 : 해당 없음
(2) SL 2 : 1002. 1
(3) SL 3 : 1002. 2
(3) SL 4 : 1002. 2

1003. 악성코드로부터의 보호

1. 임베디드 장비는 인가받지 않은 소프트웨어 설치 및 실행으로부터 보호하는 기능을 제공하여야 한다.

2. 보안 레벨별 요건

(1) SL 1 : 해당 없음
(2) SL 2 : 1003. 1

(3) SL 3 : 1003. 1
(3) SL 4 : 1003. 1

1004. 업데이트 지원

1. 임베디드 장비는 업데이트되거나 업그레이드되는 기능을 지원하여야 한다.
2. 임베디드 장비는 설치 전에 업데이트 또는 업그레이드의 신뢰성과 무결성을 확인하여야 한다.
3. **보안 레벨별 요건**
(1) SL 1 : 1004. 1
(2) SL 2 : 1004. 2
(3) SL 3 : 1004. 2
(3) SL 4 : 1004. 2

1005. 물리적 변조 저항 및 감지

1. 임베디드 장비는 장비에 대한 무단 물리적인 접근을 방지하기 위한 변조 방지나 감지 메커니즘을 제공하여야 한다.
2. 임베디드 장비는 인가되지 않은 물리적 접근이 시도되었을 때 구성 가능한 수신인에게 자동으로 통지를 하여야 한다. 모든 변경 통지는 전체 감사 기록의 일부로 기록되어야 한다.
3. **보안 레벨별 요건**
(1) SL 1 : 해당 없음
(2) SL 2 : 1005. 1
(3) SL 3 : 1005. 2
(3) SL 4 : 1005. 2

1006. 제품 공급업체 신뢰 루트 권한 설정

1. 임베디드 장비는 장비 제조 시 하나 이상의 “신뢰 루트”로 사용될 제품 공급업체 키 및 데이터 기밀성, 무결성 및 신뢰성에 대해 권한을 설정하고 보호할 수 있는 기능을 제공하여야 한다.
2. **보안 레벨별 요건**
(1) SL 1 : 해당 없음
(2) SL 2 : 1006. 1
(3) SL 3 : 1006. 1
(3) SL 4 : 1006. 1

1007. 자산 소유자의 신뢰 루트 권한 설정

1. 임베디드 장비는 “신뢰 루트”로 사용될 자산 소유자 키 및 데이터의 기밀성, 무결성 및 신뢰성을 제공하고 보호하기 위한 기능을 제공하여야 하며, 장비 보안 영역 외부에 있을 수 있는 구성품에 의존하지 않고 제공할 수 있는 기능을 지원하여야 한다.
2. **보안 레벨별 요건**
(1) SL 1 : 해당 없음
(2) SL 2 : 1007. 1
(3) SL 3 : 1007. 1
(3) SL 4 : 1007. 1

1008. 부트 프로세스 무결성

1. 임베디드 장비는 부팅 프로세스에서 사용되기 전에 구성품의 부팅 및 런타임 프로세스에 필요한 펌웨어, 소프트웨어 및 구성 데이터의 무결성을 확인하여야 한다.
2. 임베디드 장비는 부팅 프로세스에서 사용되기 전에 구성품의 부팅 프로세스에 필요한 펌웨어, 소프트웨어 및 구성 데이터의 신뢰성을 확인하기 위하여 구성품 공급업체 신뢰 루트를 사용하여야 한다.
3. **보안 레벨별 요건**
(1) SL 1 : 1008. 1

(2) SL 2 : 1008. 2
(3) SL 3 : 1008. 2
(3) SL 4 : 1008. 2

제 11 절 호스트 장비 요건

1101. 모바일 코드

1. 호스트 장비가 모바일 코드 기술을 이용하는 경우 호스트 장비는 모바일 코드 기술 사용에 대한 보안 정책을 시행할 수 있는 기능을 제공하여야 한다. 보안 정책은 호스트 장비에 사용되는 각 모바일 코드 기술에 대해 최소한 다음 조치를 허용하여야 한다.
   (1) 모바일 코드 실행 제어
   (2) 호스트 장비에 모바일 코드를 업로드할 수 있는 사용자(인간, 소프트웨어 프로세스 또는 장비) 제어
   (3) 코드가 실행되기 전에 모바일 코드에 대한 무결성 검사 결과에 따라 코드 실행 제어
2. 호스트 장비는 코드가 실행되기 전에 실행되기 전에 신뢰성 점검 결과에 따라 장비가 모바일 코드의 실행을 제어할 수 있는 보안 정책을 시행할 수 있는 기능을 제공하여야 한다.
3. **보안 레벨별 요건**
   (1) SL 1 : 1101. 1
   (2) SL 2 : 1101. 2
   (3) SL 3 : 1101. 2
   (3) SL 4 : 1101. 2

1102. 물리적 진단 및 시험 인터페이스 사용

1. 호스트 장비는 물리적 공장 진단 및 시험 인터페이스(예: JTAG 디버깅)에 대한 무단 사용을 방지하여야 한다.
2. 호스트 장비는 기기의 진단 및 시험 인터페이스에 대한 능동 모니터링을 제공하고 이러한 인터페이스에 접속하려는 시도가 감지될 때 감사 로그 기록을 생성하여야 한다.
3. **보안 레벨별 요건**
   (1) SL 1 : 해당 없음
   (2) SL 2 : 1102. 1
   (3) SL 3 : 1102. 2
   (3) SL 4 : 1102. 2

1103. 악성코드로부터의 보호

1. 악성코드로부터의 보호를 제공하기 위하여 제품 공급업체에 의해 자격을 갖춘 호스트 장비에 대한 메커니즘이 있어야한다. 제품 공급 업체는 악성코드로부터의 보호와 관련된 특별한 구성 요건을 문서화하여야 한다.
2. 호스트 장비는 (전체 로깅 기능의 일부로) 사용 중인 악성코드 보호 소프트웨어 및 파일 버전을 자동으로 보고하여야 한다.
3. 내장형 장치는 승인되지 않은 소프트웨어의 설치 및 실행으로부터 보호할 수 있는 기능을 제공해야 한다.
4. **보안 레벨별 요건**
   (1) SL 1 : 1103. 1
   (2) SL 2 : 1103. 3
   (3) SL 3 : 1103. 3
   (3) SL 4 : 1103. 3

1104. 업데이트 지원

1. 호스트 장비는 업데이트되거나 업그레이드되는 기능을 지원하여야 한다.
2. 호스트 장비는 설치 전에 업데이트 또는 업그레이드의 신뢰성과 무결성을 확인하여야 한다.
3. **보안 레벨별 요건**
   (1) SL 1 : 1104. 1

(2) SL 2 : 1104. 2
(3) SL 3 : 1104. 2
(3) SL 4 : 1104. 2

1105. 물리적 변조 저항 및 감지

1. 호스트 장비는 장비에 대한 무단 물리적인 접근을 방지하기 위한 변조 방지나 감지 메커니즘을 제공하여야 한다.
2. 호스트 장비는 인가되지 않은 물리적 접근이 시도되었을 때 구성 가능한 수신인에게 자동으로 통지를 하여야 한다. 모든 변경 통지는 전체 감사 기록의 일부로 기록되어야 한다.
3. **보안 레벨별 요건**

(1) SL 1 : 해당 없음
(2) SL 2 : 1105. 1
(3) SL 3 : 1105. 2
(3) SL 4 : 1105. 2

1106. 제품 공급업체 신뢰 루트 권한 설정

1. 호스트 장비는 장비 제조 시 하나 이상의 “신뢰 루트”로 사용될 제품 공급업체 키 및 데이터 기밀성, 무결성 및 신뢰성에 대해 권한을 설정하고 보호할 수 있는 기능을 제공하여야 한다.
2. **보안 레벨별 요건**

(1) SL 1 : 해당 없음
(2) SL 2 : 1106. 1
(3) SL 3 : 1106. 1
(3) SL 4 : 1106. 1

1107. 자산 소유자의 신뢰 루트 권한 설정

1. 호스트 장비는 “신뢰 루트”로 사용될 자산 소유자 키 및 데이터의 기밀성, 무결성 및 신뢰성을 제공하고 보호하기 위한 기능을 제공하여야 하며, 장비 보안 영역 외부에 있을 수 있는 구성품에 의존하지 않고 제공할 수 있는 기능을 지원하여야 한다.
2. **보안 레벨별 요건**

(1) SL 1 : 해당 없음
(2) SL 2 : 1107. 1
(3) SL 3 : 1107. 1
(3) SL 4 : 1107. 1

1108. 부트 프로세스 무결성

1. 호스트 장비는 부팅 프로세스에서 사용되기 전에 구성품의 부팅 및 런타임 프로세스에 필요한 펌웨어, 소프트웨어 및 구성 데이터의 무결성을 확인하여야 한다.
2. 호스트 장비는 부팅 프로세스에서 사용되기 전에 구성품의 부팅 프로세스에 필요한 펌웨어, 소프트웨어 및 구성 데이터의 신뢰성을 확인하기 위하여 구성품 공급업체 신뢰 루트를 사용하여야 한다.
3. **보안 레벨별 요건**

(1) SL 1 : 1108. 1
(2) SL 2 : 1108. 2
(3) SL 3 : 1108. 2
(3) SL 4 : 1108. 2

제 12 절 네트워크 장비 요건

1201. 무선 접속 관리

1. 무선 접속 관리를 지원하는 네트워크 장치는 무선 통신과 관련된 모든 사용자(인간, 소프트웨어 프로세스 또는 장치)를 식별하고 인증할 수 있는 기능을 제공하여야 한다.
2. 네트워크 장치는 무선 통신과 관련된 모든 사용자(인간, 소프트웨어 프로세스 또는 장치)를 고유하게 식별하고 인증할 수 있는 기능을 제공하여야 한다.

3. 보안 레벨별 요건

(1) SL 1 : 1201. 1
(2) SL 2 : 1201. 2
(3) SL 3 : 1201. 2
(3) SL 4 : 1201. 2

1202. 신뢰할 수 없는 네트워크를 통한 접속

1. 네트워크로의 장비 접속을 지원하는 네트워크 장비는 신뢰할 수 없는 네트워크를 통해 네트워크 장비에 대한 모든 접근 방법을 감시하고 제어하는 기능을 제공하여야 한다.
2. 네트워크 장비는 지정된 역할에 의해 명시적으로 승인되지 않은 한 신뢰할 수 없는 네트워크를 통해 접속 요청을 거부할 수 있는 기능을 제공하여야 한다.

3. 보안 레벨별 요건

(1) SL 1 : 1202. 1
(2) SL 2 : 1202. 1
(3) SL 3 : 1202. 2
(3) SL 4 : 1202. 2

1203. 모바일 코드

1. 네트워크 장비가 모바일 코드 기술을 이용하는 경우 네트워크 장비는 모바일 코드 기술 사용에 대한 보안 정책을 시행할 수 있는 기능을 제공하여야 한다. 보안 정책은 호스트 장비에 사용되는 각 모바일 코드 기술에 대해 최소한 다음 조치를 허용하여야 한다.
   (1) 모바일 코드 실행 제어
   (2) 네트워크 장비로부터 모바일 코드를 전송할 수 있는 사용자(인간, 소프트웨어 프로세스 또는 장비) 제어
   (3) 코드가 실행되기 전에 모바일 코드에 대한 무결성 검사 결과에 따라 코드 실행 제어
2. 네크워트 장비는 코드가 실행되기 전에 신뢰성 점검 결과에 따라 장비가 모바일 코드의 실행을 제어할 수 있는 보안 정책을 시행할 수 있는 기능을 제공하여야 한다.

3. 보안 레벨별 요건

(1) SL 1 : 1203. 1
(2) SL 2 : 1203. 2
(3) SL 3 : 1203. 2
(3) SL 4 : 1203. 2

1204. 물리적 진단 및 시험 인터페이스 사용

1. 네트워크 장비는 물리적 공장 진단 및 시험 인터페이스(예: JTAG 디버깅)에 대한 무단 사용을 방지하여야 한다.
2. 네트워크 장비는 기기의 진단 및 시험 인터페이스에 대한 능동 모니터링을 제공하고 이러한 인터페이스에 접속하려는 시도가 감지될 때 감사 로그 기록을 생성하여야 한다.

3. 보안 레벨별 요건

(1) SL 1 : 해당 없음
(2) SL 2 : 1204. 1
(3) SL 3 : 1204. 2
(3) SL 4 : 1204. 2

1205. 악성코드로부터의 보호

1. 네트워크 장비는 악성코드로부터 보호되는 기능을 제공하여야 한다.
2. **보안 레벨별 요건**
   (1) SL 1 : 1205. 1
   (2) SL 2 : 1205. 1
   (3) SL 3 : 1205. 1
   (3) SL 4 : 1205. 1

1206. 업데이트 지원

1. 네트워크 장비는 업데이트되거나 업그레이드되는 기능을 지원하여야 한다.
2. 네트워크 장비는 설치 전에 업데이트 또는 업그레이드의 신뢰성과 무결성을 확인하여야 한다.
3. **보안 레벨별 요건**
   (1) SL 1 : 1206. 1
   (2) SL 2 : 1206. 2
   (3) SL 3 : 1206. 2
   (3) SL 4 : 1206. 2

1207. 물리적 변조 저항 및 감지

1. 네트워크 장비는 장비에 대한 무단 물리적인 접근을 방지하기 위한 변조 방지나 감지 메커니즘을 제공하여야 한다.
2. 네트워크 장비는 인가되지 않은 물리적 접근이 시도되었을 때 구성 가능한 수신인에게 자동으로 통지를 하여야 한다. 모든 변경 통지는 전체 감사 기록의 일부로 기록되어야 한다.
3. **보안 레벨별 요건**
   (1) SL 1 : 해당 없음
   (2) SL 2 : 1207. 1
   (3) SL 3 : 1207. 2
   (3) SL 4 : 1207. 2

1208. 제품 공급업체 신뢰 루트 권한 설정

1. 네트워크 장비는 장비 제조 시 하나 이상의 “신뢰 루트”로 사용될 제품 공급업체 키 및 데이터 기밀성, 무결성 및 신뢰성에 대해 권한을 설정하고 보호할 수 있는 기능을 제공하여야 한다.
2. **보안 레벨별 요건**
   (1) SL 1 : 해당 없음
   (2) SL 2 : 1208. 1
   (3) SL 3 : 1208. 1
   (3) SL 4 : 1208. 1

1209. 자산 소유자의 신뢰 루트 권한 설정

1. 호스트 장비는 “신뢰 루트”로 사용될 자산 소유자 키 및 데이터의 기밀성, 무결성 및 신뢰성을 제공하고 보호하기 위한 기능을 제공하여야 하며, 장비 보안 영역 외부에 있을 수 있는 구성품에 의존하지 않고 제공할 수 있는 기능을 지원하여야 한다.
2. **보안 레벨별 요건**
   (1) SL 1 : 해당 없음
   (2) SL 2 : 1209. 1
   (3) SL 3 : 1209. 1
   (3) SL 4 : 1209. 1

1210. 부트 프로세스 무결성

1. 네트워크 장비는 부팅 프로세스에서 사용되기 전에 구성품의 부팅 및 런타임 프로세스에 필요한 펌웨어, 소프트웨어

및 구성 데이터의 무결성을 확인하여야 한다.

2. 네트워크 장비는 부팅 프로세스에서 사용되기 전에 구성품의 부팅 프로세스에 필요한 펌웨어, 소프트웨어 및 구성 데이터의 신뢰성을 확인하기 위하여 구성품 공급업체 신뢰 루트를 사용하여야 한다.
3. **보안 레벨별 요건**
   (1) SL 1 : 1210. 1
   (2) SL 2 : 1210. 2
   (3) SL 3 : 1210. 2
   (3) SL 4 : 1210. 2

1211. 구역 경계 보호

1. 구역 경계의 네트워크 장비는 위험 기반 구역 및 도관 모델에 정의된 구획화를 시행하기 위하여 구역 경계의 통신을 모니터링하고 제어하는 기능을 제공하여야 한다.
2. 네트워크 구성품은 기본적으로 네트워크 트래픽을 거부할 수 있는 기능을 제공하여야 하며 예외로 네트워크 트래픽을 허용하여야 한다.
3. 네트워크 구성품은 시스템 경계(또는 섬 모드)를 통한 통신으로부터 보호할 수 있는 기능을 제공하여야 한다.
4. 네트워크 구성품은 경계 보호 메커니즘(또는 페일-클로즈)의 작동 실패 시 시스템 경계를 통과하는 통신으로부터 보호할 수 있는 기능을 제공하여야 한다.
5. **보안 레벨별 요건**
   (1) SL 1 : 1211. 1
   (2) SL 2 : 1211. 2
   (3) SL 3 : 1211. 4
   (3) SL 4 : 1211. 4

1212. 일반 목적, 개인 대 개인 통신 제한

1. 구역 경계의 네트워크 장치는 시스템 외부의 사용자 또는 시스템으로부터 수신되는 개인 대 개인 메시지로부터 보호하는 기능을 제공하여야 한다.
2. **보안 레벨별 요건**
   (1) SL 1 : 1212. 1
   (2) SL 2 : 1212. 1
   (3) SL 3 : 1212. 1
   (3) SL 4 : 1212. 1

1213. 네트워크 접속 통제

1. 네트워크에 연결된 각 노드는 보안 영역 외부에 설치된 경우 MAC 주소로 승인되어야 하며 스위치 또는 포워더의 포트에 물리적으로 연결되어야 한다.
2. 연결 노드가 보안 영역에 설치될 경우, MAC 주소에 의한 승인을 활성화 또는 비활성화할 수 있는 수단이 제공되어야 한다.
3. 스위치 및 포워더에서의 모든 우회 및 발신 트래픽은 IP 주소와 UDP/TCP 포트 번호로 승인되어야 한다.
4. **보안 레벨별 요건**
   (1) SL 1 : 1213. 3
   (2) SL 2 : 1213. 3
   (3) SL 3 : 1213. 3
   (3) SL 4 : 1213. 3

1214. 직접 통신

1. 네트워크의 장비에 직접 통신이 필요한 경우, 전체 통신 기간 동안 관리자 또는 감독자의 권한이 감시와 함께 요구되어야 한다.
2. 제조상 기본적으로, 제어되지 않는 네트워크로부터의 직접 연결은 허용되지 않도록 설정되어야 한다.
3. 통제되지 않는 네트워크에서 노드와의 직접 연결은 방화벽의 설치 사이트 또는 네트워크 측의 조작에 의해서만 활성

화되어야 한다.

4. **보안 레벨별 요건**

(1) SL 1 : 1214. 3

(2) SL 2 : 1214. 3

(3) SL 3 : 1214. 3

(3) SL 4 : 1214. 3

1215. 무선 연결

1. 무선 게이트웨이는 클라이언트로만 운영되어야 한다.
2. 무선 네트워크에서 네트워크로의 트래픽 전달이 금지되어야 한다.
3. 무선 인터페이스를 통해 교환되는 모든 데이터는 암호화 요건을 충족하여야 한다. 제조상 기본적으로, 제어되지 않는 네트워크로부터의 직접 연결은 허용되지 않도록 설정되어야 한다.
4. 무선 연결은 인증을 가진 등록된 무선 AP에만 설정하여야 한다.
5. **보안 레벨별 요건**

(1) SL 1 : 1215. 4

(2) SL 2 : 1215. 4

(3) SL 3 : 1215. 4

(3) SL 4 : 1215. 4 ⚓

부록 1 장비 타입별 사이버보안 형식 승인요건 매핑

아래 테이블은 이해를 돕기 위하여 사이버보안 형식 승인 공통 요건을 장비 타입과 매핑한 것이다.

표 4 장비 타입별 사이버보안 요건

요건	노드	스위치	포워더	게이트웨이
식별 및 인증				
201. 인간 사용자 식별 및 인증	O	O	O	O
202. 소프트웨어 프로세스 및 장비 식별 및 인증	O	O	O	O
203. 계정 관리	O	O	O	O
204. 식별자 관리	O	O	O	O
205. 인증자 관리	O	O	O	O
206. 비밀번호 기반 인증 강화	O	O	O	O
207. 공개 키 인프라 인증	O	O	O	O
208. 공개 키 인증 강화	O	O	O	O
209. 인증자 피드백	O	O	O	O
210. 실패한 로그인 시도	O	O	O	O
211. 시스템 사용 알림	O	O	O	O
212. 대칭 키 인증 강화	O	O	O	O
사용 제어				
301. 권한 부여 시행	O	O	O	O
302. 무선 사용	O	O	O	O
303. 세션 잠금	O	O	O	O
304. 원격 세션 종료	O	O	O	O
305. 동시 세션	O	O	O	O
306. 감사 가능한 이벤트	O	O	O	O
307. 감사 저장소 용량	O	O	O	O
308. 감사 프로세싱 실패 대응	O	O	O	O
309. 타임스탬프	O	O	O	O
310. 부인 방지	O	O	O	O
311. 이동식 외부 데이터 저장매체 보안	O	O	O	O
시스템 무결성				
401. 통신 무결성	O	O	O	O
402. 보안 기능성 검증	O	O	O	O
403. 소프트웨어 및 정보 무결성	O	O	O	O
404. 입력값 검증	O	O	O	O
405. 결정론적 출력	O	O	O	O
406. 에러 핸들링	O	O	O	O
407. 세션 무결성	O	O	O	O
408. 감사 정보 보호	O	O	O	O
데이터 기밀성				
501. 정보 기밀성	O	O	O	O
502. 정보 지속성	O	O	O	O
503. 암호화 사용	O	O	O	O
제한된 데이터 흐름				
601. 네트워크 분할	X	O	O	O
602. 스위치 루프 방지	X	O	X	X
사고에 대한 적시 대응				
701. 감사 로그 접근성	O	O	O	O
702. 지속적인 모니터링	X	X	O	O

표 5 장비 타입별 사이버보안 요건 (계속)

리소스 가용성				
801. 서비스 거부 보호	O	O	O	O
802. 리소스 관리	O	O	O	O
803. 시스템 백업	O	O	O	O
804. 시스템 복구 및 재구성	O	O	O	O
805. 네트워크 및 보안 구성 세팅	O	O	O	O
806. 기능 최소화	O	O	O	O
807. 시스템 구성품 인벤토리	O	O	O	O

인 쇄 2020년 4월 6일
발 행 2020년 4월 17일

해상 사이버보안 형식 승인 지침

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

신고번호 : 제 2014-000001호 (93. 12. 01)