해상 사이버보안 형식승인 지침 개정(안)

(개발검토 : 내부의견조회용)

2021. 01.

기 관 규 칙 개 발 팀

2021.07.01.일자 시행사항

(건조계약일 기준)

현 행	개 정 안	개 정 사 유
제 1 장 전기설비 **제 1 절 일반사항** 101. **적용** 1. - 2. **〈생략〉** 3. 이 지침에 따른 사이버보안 형식 승인은 **선급 및 강선규칙**에서 명시하지 않는 한 강제 사항이 아니다. 4. - 6. **〈생략〉** 102. **용어의 정의** 용어의 정의는 여기에 별도로 정하는 경우를 제외하고는 **선급 및 강선규칙**에 따른다. 1. - 21. **〈생략〉** 22. **"시크릿(Secret)"**이라 함은 정보를 알 의도를 제외하고 시스템 객체에 의해 알려지는 것으로부터 보호된 정보 상태를 말한다. 23. - 27. **〈생략〉** 103. - 104. **〈생략〉**	**제 1 장 전기설비** **제 1 절 일반사항** 101. **적용** 1. - 2. **〈현행과 동일〉** 3. 이 지침에 따른 사이버보안 형식승인은 **선급 및 강선규칙**에서 명시하지 않는 한 강제 사항이 아니다. *(2021)* 4. - 6. **〈현행과 동일〉** 102. **용어의 정의** 용어의 정의는 여기에 별도로 정하는 경우를 제외하고는 **선급 및 강선규칙**에 따른다. 1. - 21. **〈현행과 동일〉** 22. **"시크릿 비밀(Secret)"**이라 함은 정보를 알 의도를 제외하고 시스템 객체에 의해 알려지는 것으로부터 보호된 정보 상태를 말한다. *(2021)* 23. - 27. **〈현행과 동일〉** 103. - 104. **〈현행과 동일〉**	(개정) - 국가기술표준원(e나라표준인증)의 인증제도 명칭을 따라 개정함. (개정) - 명칭 변경.

현 행	개 정 안	개 정 사 유
제 2 장 사이버보안 형식 승인	**제 2 장 사이버보안 형식승인 *(2021)***	
제 1 절 일반사항	**제 1 절 일반사항**	
101. 일반사항 1. 이 지침에 적용되는 사이버 시스템은 4가지 분류로 구분된다. (1) - (2) 〈생략〉 (3) 포워더 : 네트워크 장비, 소프트웨어 애플리케이션 및 호스트 장비 (4) 게이트웨이 : 네트워크 장비, 소프트웨어 애플리케이션 및 호스트 장비	**101. 일반사항** 1. 이 지침에 적용되는 사이버 시스템은 4가지 분류로 구분된다. (1) - (2) 〈현행과 동일〉 (3) 포워더 : 네트워크 장비~~, 소프트웨어 애플리케이션 및 호스트 장비~~ *(2021)* (4) 게이트웨이 : 네트워크 장비~~, 소프트웨어 애플리케이션 및 호스트 장비~~ *(2021)*	(개정) - IEC 61162-460의 용어 정의에 따라 (3)호 및 (4)호의 소프트웨어 어플리케이션 및 호스트 장비에 대한 분류를 삭제함.
제 2 절 승인 절차	**제 2 절 승인 절차**	
201. 승인 신청 1. 〈생략〉 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. - 5. 〈생략〉**	**201. 승인 신청** 1. 〈현행과 동일〉 2. 사이버보안 형식승인을 받고자 하는 신청자는 형식승인 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. *(2021)* **3. - 5. 〈현행과 동일〉**	(개정) - 국가기술표준원(e나라표준인증)의 인증제도 명칭을 따름.
202. - 203. 〈생략〉	**202. - 203. 〈현행과 동일〉**	
204. 공장조사 **제조법 및 형식승인 등에 관한 지침 3장 105.** 공장조사에 따른다. 기자재 형식승인을 동시에 진행하거나 형식 승인을 받은 경우 공장조사를 생략할 수 있다.	**204. 공장조사** **제조법 및 형식승인 등에 관한 지침 3장 105.** 공장조사에 따른다. 기자재 형식승인을 동시에 진행하거나 형식승인을 받은 경우 공장조사를 생략할 수 있다. *(2021)*	(개정) - 국가기술표준원(e나라표준인증)의 인증제도 명칭을 따름.

현 행	개 정 안	개 정 사 유
205. - 206. 〈생략〉	205. - 206. 〈현행과 동일〉	
207. 인증서의 유효기간 및 갱신 등	207. 인증서의 유효기간 및 갱신 등	(개정) - 오타 수정.
1. 〈생략〉 2. 승인증서의 유효기간 갱신 및 연장은 **제조법 및 형식승인 등에 관한 지침 23장 108. 승인증서의 유효기간 갱신 및 연장 등**에 따른다. 단, 연장 종료후 다시 발생하는 증서의 유효기간은 구증서의 유효기간 말료일의 익일부터 3년 이내로 한다.	1. 〈현행과 동일〉 2. 승인증서의 유효기간 갱신 및 연장은 **제조법 및 형식승인 등에 관한 지침 23장 108. 승인증서의 유효기간 갱신 및 연장 등**에 따른다. 단, 연장 종료후 다시 발생하는 증서의 유효기간은 구증서의 유효기간 팔만료일의 익일부터 3년 이내로 한다. *〈2021〉*	

현 행	개 정 안	개 정 사 유
제 3 장 사이버보안 요건 **제 1 절 〈생략〉** **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**	**제 3 장 사이버보안 요건** **제 1 절 〈현행과 동일〉** **제 2 절 식별 및 인증** **201. 인간 사용자 식별 및 인증** *(2021)* **1.** 구성품은 모든 인간 사용자 접속을 지원하는 모든 인터페이스에서 ~~ISA-62443-4-2 CR 1.1~~ ISA-62443-3-3 SR 1.1 **사용자 식별 및 인증**을 따라 모든 사용자를 식별하고 인증할 수 있는 기능을 제공하여야 한다. ~~**2.**~~ 단, 사용자 식별 및 인증이 신속한 현장 비상조치를 방해해서는 아니 된다. ~~**3.**~~**2.** 구성품은 모든 인간 사용자를 고유하게 식별하고 인증할 수 있는 기능을 제공하여야 한다. ~~**4.**~~**3.** 구성품은 구성품에 접속하는 모든 인간 사용자에 대해 다중요소 인증을 사용할 수 있는 기능을 제공하여야 한다. ~~**5.**~~**4. 보안 레벨별 요건** (1) SL 1 : **201. ~~2~~1** (2) SL 2 : **201. ~~3~~2** (3) SL 3 : **201. ~~4~~3** (4) SL 4 : **201. ~~4~~3**	(개정) - IEC 62443 4-2의 원문에 따라 개정함.

현 행	개 정 안	개 정 사 유
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. - 3. **〈생략〉**	202. **소프트웨어 프로세스 및 장비 식별 및 인증** 1. 구성품은 ~~ISA-62443-4-2 CR 1.2.~~ ISA-62443-3-3 SR 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. *(2021)* 2. - 3. **〈현행과 동일〉**	(개정) - IEC 62443 4-2의 원문에 따라 개정함.
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. **〈생략〉**	203. **계정 관리** 1. 구성품은 ~~ISA-62443-4-2 CR 1.3.~~ ISA-62443-3-3 SR 1.3. **계정 관리**에 따라 모든 계정 관리를 직접 지원하거나 계정을 관리하는 시스템에 통합할 수 있는 기능을 제공하여야 한다. *(2021)* 2. **〈현행과 동일〉**	(개정) - IEC 62443 4-2의 원문에 따라 개정함.
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. **〈생략〉**	204. **식별자 관리** 1. 구성품은 ~~ISA-62443-4-2 CR 1.4.~~ ISA-62443-3-3 SR 1.4. **식별자 관리**에 따라 직접 식별자 관리를 지원하거나 식별자 관리를 제공하는 시스템에 통합할 수 있는 기능을 제공하여야 한다. *(2021)* 2. **〈현행과 동일〉**	(개정) - IEC 62443 4-2의 원문에 따라 개정함.
205. - 206. **〈생략〉**	205. - 206. **〈현행과 동일〉**	
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. **〈생략〉**	207. **공개 키 인프라 인증** 1. 공~~용~~개 키 기반 구조 (PKI)를 사용할 경우, 구성품은 ~~ISA 62443-4-2 CR1.8~~ ISA 62443-3-3 SR1.8에 따라 공~~용~~개 키 기반 구조의 영역 내에서 상호작용하고 작동할 수 있는 기능을 제공하거나 기능을 제공하는 시스템으로 통합되어야 한다. *(2021)* 2. **〈현행과 동일〉**	(개정) - KISA 암호 키 관리 안내서 (KISA-GD-2014-0013)의 용어 정의에 따라 Public Key의 번역을 「공개키」로 통일함.
208. - 212. **〈생략〉**	208. - 212. **〈현행과 동일〉**	

현 행	개 정 안	개 정 사 유
제 3 절 사용 제어	**제 3 절 사용 제어**	
301. **권한 부여 시행**	301. **권한 부여 시행**	
1. - 4. **〈생략〉**	1. - 4. **〈현행과 동일〉**	(개정) - 국립국어원 표준국어대사전에 따라 개정함.
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.	5. 구성품은 조치가 산업 프로세스에 심각한 영향을 미칠 수 있는 경우 이중 승인을 지원하여야 한다. 단, 이중 승인 메커니즘은 산업 프로세스의 비상 정지와 같이 건강, 안전, 환경을 보호하기 위해 즉각적인 대응이 필요한 경우에는 적용되어서는 아니 된다. *(2021)*	
6. **〈생략〉**	6. **〈현행과 동일〉**	
302. - 311. **〈생략〉**	302. - 311. **〈현행과 동일〉**	
제 4 절 시스템 무결성	**제 4 절 시스템 무결성**	
401. **〈생략〉**	401. **〈현행과 동일〉**	
402. **보안 기능성 검증**	402. **보안 기능성 검증**	(개정) - IEC 62443 4-2의 원문에 따라 개정함.
1. 구성품은 ISA-62443-4-2 CR 3.3. **보안 기능성 검증**에 따라 의도된 보안 기능의 작동을 확인할 수 있는 기능을 제공하여야 한다.	1. 구성품은 ~~ISA-62443-4-2 CR 3.3.~~ ISA-62443-3-3 SR 3.3. **보안 기능성 검증**에 따라 의도된 보안 기능의 작동을 확인할 수 있는 기능을 제공하여야 한다. *(2021)*	
2. - 3. **〈생략〉**	2. - 3. **〈현행과 동일〉**	
403. - 408. **〈생략〉**	403. - 408. **〈현행과 동일〉**	

현 행	개 정 안	개 정 사 유
제 5 절 데이터 기밀성	**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. **〈생략〉**	**501. 정보 기밀성** 1. 구성품은 명시적 읽기 허가가 지원되는 미사용 정보의 기밀성을 보호하여야 하며, ~~ISA-62443-4-2 CR 4.1~~ ISA-62443-3-3 SR 4.1 **정보 기밀성**에 정의된 바와 같이 전송 중인 정보의 기밀성 보호를 지원하여야 한다. *(2021)* 2. **〈현행과 동일〉**	(개정) - IEC 62443 4-2의 원문에 따라 개정함.
502. - 503. **〈생략〉**	502. - 503. **〈현행과 동일〉**	
제 6 절 제한된 데이터 흐름	**제 6 절 제한된 데이터 흐름**	
601. **〈생략〉**	601. **〈현행과 동일〉**	
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. **〈생략〉**	**602. 루프 방지** 1. 스위치는 RSTP, MSTP와 같은 루프 방지 매메커니즘 기능을 제공하여야 한다. 네트워크 토폴로지 및 스위치 구성은 5초 이내에 정합성을 지원하여야 한다. *(2021)* 2. **〈현행과 동일〉**	(개정) - 국립국어원 표준국어대사전에 따라 개정함.
제 7 절 〈생략〉	**제 7 절 〈현행과 동일〉**	

현 행	개 정 안	개 정 사 유
제 8 절 리소스 가용성	**제 8 절 리소스 가용성**	
801. - 806. 〈생략〉	801. - 806. 〈현행과 동일〉	
807. 시스템 구성품 인벤토리 1. 구성품은 ISA-62443-4-2 CR 7.8.**에 따라 제어 시스템 구성품 인벤토리를** 지원하는 기능을 제공하여야 한다. 2. **〈생략〉**	**807. 시스템 구성품 인벤토리** 1. 구성품은 ~~ISA-62443-4-2 CR 7.8.~~ ISA-62443-3-3 SR 7.8.**에 따라 제어 시스템 구성품 인벤토리를** 지원하는 기능을 제공하여야 한다. *(2021)* 2. **〈현행과 동일〉**	(개정) - IEC 62443 4-2의 원문에 따라 개정함.
제 9 절 소프트웨어 애플리케이션 요건	**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) - (3) 〈생략〉 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. **〈생략〉**	**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. *(2021)* (1) - (3) 〈현행과 동일〉 2. 애플리케이션은 코드가 실행되기 전에 ~~신뢰성~~진본성 점검 결과에 따라 장비가 모바일 코드의 실행을 제어할 수 있는 보안 정책을 시행할 수 있는 기능을 제공하여야 한다. *(2021)* 3. **〈현행과 동일〉**	(개정) - 국립국어원 표준국어대사전에 따라 개정함.

현 행	개 정 안	개 정 사 유
제 10 절 임베디드 장비 요건	**제 10 절 임베디드 장비 요건**	
1001. 모바일 코드 1. 〈생략〉 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. 〈생략〉	**1001. 모바일 코드** 1. 〈현행과 동일〉 2. 임베디드 장비는 코드가 실행되기 전에 ~~신뢰성~~진본성 점검 결과에 따라 장비가 모바일 코드의 실행을 제어할 수 있는 보안 정책을 시행할 수 있는 기능을 제공하여야 한다. *(2021)* 3. 〈현행과 동일〉	(개정) - 국립국어원 표준국어대사전에 따라 개정함.
1002. - 1003. 〈생략〉	**1002. - 1003. 〈현행과 동일〉**	
1004. 업데이트 지원 1. 〈생략〉 2. 임베디드 장비는 설치 전에 업데이트 또는 업그레이드의 신뢰성과 무결성을 확인하여야 한다. 3. 〈생략〉	**1004. 업데이트 지원** 1. 〈현행과 동일〉 2. 임베디드 장비는 설치 전에 업데이트 또는 업그레이드의 ~~신뢰성~~진본성과 무결성을 확인하여야 한다. *(2021)* 3. 〈현행과 동일〉	(개정) - 국립국어원 표준국어대사전에 따라 개정함.
1005. 〈생략〉	**1005. 〈현행과 동일〉**	
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. **〈생략〉**	**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 ~~신뢰성~~진본성에 대해 권한을 설정하고 보호할 수 있는 기능을 제공하여야 한다. *(2021)* 2. **〈현행과 동일〉**	(개정) - 국립국어원 표준국어대사전에 따라 개정함.

현 행	개 정 안	개 정 사 유
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. 〈생략〉**	**1007. 자산 소유자의 신뢰 루트 권한 설정** 1. 임베디드 장비는 “신뢰 루트”로 사용될 자산 소유자 키 및 데이터의 기밀성, 무결성 및 ~~신뢰성~~진본성을 제공하고 보호하기 위한 기능을 제공하여야 하며, 장비 보안 영역 외부에 있을 수 있는 구성품에 의존하지 않고 제공할 수 있는 기능을 지원하여야 한다. *(2021)* **2. 〈현행과 동일〉**	(개정) - 국립국어원 표준국어대사전에 따라 개정함.
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. 〈생략〉**	**1008. 부트 프로세스 무결성 *(2021)*** 1. 임베디드 장비는 ~~부팅~~부트 프로세스에서 사용되기 전에 구성품의 ~~부팅~~부트 및 런타임 프로세스에 필요한 펌웨어, 소프트웨어 및 구성 데이터의 무결성을 확인하여야 한다. *(2021)* 2. 임베디드 장비는 ~~부팅~~부트 프로세스에서 사용되기 전에 구성품의 ~~부팅~~부트 프로세스에 필요한 펌웨어, 소프트웨어 및 구성 데이터의 ~~신뢰성~~진본성을 확인하기 위하여 구성품 공급업체 신뢰 루트를 사용하여야 한다. *(2021)* **3. 〈현행과 동일〉**	(개정) - IEC 62443 4-2의 원문(boot)에 따라 「부트」로 개정함.
제 11 절 호스트 장비 요건	**제 11 절 호스트 장비 요건**	
1101. 모바일 코드 1. 〈생략〉 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. 〈생략〉**	**1101. 모바일 코드** 1. 〈현행과 동일〉 2. 호스트 장비는 코드가 실행되기 전에 실행되기 전에 ~~신뢰성~~진본성 점검 결과에 따라 장비가 모바일 코드의 실행을 제어할 수 있는 보안 정책을 시행할 수 있는 기능을 제공하여야 한다. *(2021)* **3. 〈현행과 동일〉**	(개정) - 국립국어원 표준국어대사전에 따라 개정함.
1102. - 1103. 〈생략〉	**1102. - 1103. 〈현행과 동일〉**	

현 행	개 정 안	개 정 사 유
1104. 업데이트 지원 1. 〈생략〉 2. 호스트 장비는 설치 전에 업데이트 또는 업그레이드의 신뢰성과 무결성을 확인하여야 한다. **3. 〈생략〉**	**1104. 업데이트 지원** 1. 〈현행과 동일〉 2. 호스트 장비는 설치 전에 업데이트 또는 업그레이드의 ~~신뢰성~~진본성과 무결성을 확인하여야 한다. *(2021)* **3. 〈현행과 동일〉**	(개정) - 국립국어원 표준국어대사전에 따라 개정함.
1105. 〈생략〉	**1105. 〈현행과 동일〉**	
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. 〈생략〉**	**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 ~~신뢰성~~진본성에 대해 권한을 설정하고 보호할 수 있는 기능을 제공하여야 한다. *(2021)* **2. 〈현행과 동일〉**	(개정) - 국립국어원 표준국어대사전에 따라 개정함.
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. 〈생략〉**	**1107. 자산 소유자의 신뢰 루트 권한 설정** 1. 호스트 장비는 “신뢰 루트”로 사용될 자산 소유자 키 및 데이터의 기밀성, 무결성 및 ~~신뢰성~~진본성을 제공하고 보호하기 위한 기능을 제공하여야 하며, 장비 보안 영역 외부에 있을 수 있는 구성품에 의존하지 않고 제공할 수 있는 기능을 지원하여야 한다. *(2021)* **2. 〈현행과 동일〉**	(개정) - 국립국어원 표준국어대사전에 따라 개정함.
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. 〈생략〉**	**1108. 부트 프로세스 무결성** 1. 호스트 장비는 ~~부팅~~부트 프로세스에서 사용되기 전에 구성품의 ~~부팅~~부트 및 런타임 프로세스에 필요한 펌웨어, 소프트웨어 및 구성 데이터의 무결성을 확인하여야 한다. *(2021)* 2. 호스트 장비는 ~~부팅~~부트 프로세스에서 사용되기 전에 구성품의 ~~부팅~~부트 프로세스에 필요한 펌웨어, 소프트웨어 및 구성 데이터의 ~~신뢰성~~진본성을 확인하기 위하여 구성품 공급업체 신뢰 루트를 사용하여야 한다. *(2021)* **3. 〈현행과 동일〉**	(개정) - IEC 62443 4-2의 원문(boot)에 따라 「부트」로 개정함.

현 행	개 정 안	개 정 사 유
제 12 절 네트워크 장비 요건	**제 12 절 네트워크 장비 요건**	
1201. - 1202. **〈생략〉**	1201. - 1202. **〈현행과 동일〉**	
1203. **모바일 코드** 1. 〈생략〉 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. **〈생략〉**	1203. **모바일 코드** 1. 〈현행과 동일〉 2. 네크워트 장비는 코드가 실행되기 전에 ~~신뢰성~~진본성 점검 결과에 따라 장비가 모바일 코드의 실행을 제어할 수 있는 보안 정책을 시행할 수 있는 기능을 제공하여야 한다. *(2021)* 3. **(현행과 동일)**	(개정) - 국립국어원 표준국어대사전에 따라 개정함.
1204. - 1205. **〈생략〉**	1204. - 1205. **〈현행과 동일〉**	
1206. **업데이트 지원** 1. 〈생략〉 2. 네트워크 장비는 설치 전에 업데이트 또는 업그레이드의 신뢰성과 무결성을 확인하여야 한다. 3. **〈생략〉**	1206. **업데이트 지원** 1. 〈현행과 동일〉 2. 네트워크 장비는 설치 전에 업데이트 또는 업그레이드의 ~~신뢰성~~진본성과 무결성을 확인하여야 한다. *(2021)* 3. **〈현행과 동일〉**	(개정) - 국립국어원 표준국어대사전에 따라 개정함.
1207. **〈생략〉**	1207. **〈현행과 동일〉**	
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. **〈생략〉**	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 ~~신뢰성~~진본성에 대해 권한을 설정하고 보호할 수 있는 기능을 제공하여야 한다. *(2021)* 2. **〈현행과 동일〉**	(개정) - 국립국어원 표준국어대사전에 따라 개정함.

현 행	개 정 안	개 정 사 유
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. **〈생략〉**	**1209. 자산 소유자의 신뢰 루트 권한 설정** 1. 호스트 장비는 “신뢰 루트”로 사용될 자산 소유자 키 및 데이터의 기밀성, 무결성 및 ~~신뢰성~~진본성을 제공하고 보호하기 위한 기능을 제공하여야 하며, 장비 보안 영역 외부에 있을 수 있는 구성품에 의존하지 않고 제공할 수 있는 기능을 지원하여야 한다. *(2021)* 2. **〈현행과 동일〉**	(개정) - 국립국어원 표준국어대사전에 따라 개정함.
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. **〈생략〉**	**1210. 부트 프로세스 무결성** 1. 네트워크 장비는 ~~부팅~~부트 프로세스에서 사용되기 전에 구성품의 ~~부팅~~부트 및 런타임 프로세스에 필요한 펌웨어, 소프트웨어 및 구성 데이터의 무결성을 확인하여야 한다. *(2021)* 2. 네트워크 장비는 ~~부팅~~부트 프로세스에서 사용되기 전에 구성품의 ~~부팅~~부트 프로세스에 필요한 펌웨어, 소프트웨어 및 구성 데이터의 ~~신뢰성~~진본성을 확인하기 위하여 구성품 공급업체 신뢰 루트를 사용하여야 한다. *(2021)* 3. **〈현행과 동일〉**	(개정) - IEC 62443 4-2의 원문(boot)에 따라 「부트」로 개정함.
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. **〈생략〉**	**1210. 부트 프로세스 무결성** 1. 네트워크 장비는 ~~부팅~~부트 프로세스에서 사용되기 전에 구성품의 ~~부팅~~부트 및 런타임 프로세스에 필요한 펌웨어, 소프트웨어 및 구성 데이터의 무결성을 확인하여야 한다. *(2021)* 2. 네트워크 장비는 ~~부팅~~부트 프로세스에서 사용되기 전에 구성품의 ~~부팅~~부트 프로세스에 필요한 펌웨어, 소프트웨어 및 구성 데이터의 ~~신뢰성~~진본성을 확인하기 위하여 구성품 공급업체 신뢰 루트를 사용하여야 한다. *(2021)* 3. **〈현행과 동일〉**	(개정) - IEC 62443 4-2의 원문(boot)에 따라 「부트」로 개정함.

현 행	개 정 안	개 정 사 유
1211. **구역 경계 보호** 1. - 2. **〈생략〉** 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. **〈생략〉** 1212. - 1215. **〈생략〉**	1211. **구역 경계 보호** 1. - 2. **〈현행과 동일〉** 3. 네트워크 구성품은 시스템 경계(~~또는 섬 모드~~)를 통한 통신으로부터 보호할 수 있는 기능(아일랜드 모드)을 제공하여야 한다. *(2021)* 4. 네트워크 구성품은 경계 보호 메커니즘(~~또는 페일-클로즈~~)의 작동 실패 시 시스템 경계를 통과하는 통신으로부터 보호할 수 있는 기능(페일 클로즈)을 제공하여야 한다. *(2021)* 5. **〈현행과 동일〉** 1212. - 1215. **〈현행과 동일〉**	(개정) - IEC 62443 4-2의 원문에 따라 개정함.

현 행	개 정 안	개 정 사 유
부록 1 장비 타입별 사이버보안 형식 승인 요건 매핑 아래 테이블은 이해를 돕기 위하여 사이버보안 형식 승인 공통 요건을 장비 타입과 매핑한 것이다. **표 4 〈생략〉**	**부록 1 장비 타입별 사이버보안 형식승인요건 매핑 *(2021)*** 아래 테이블은 이해를 돕기 위하여 사이버보안 형식승인 공통 요건을 장비 타입과 매핑한 것이다. *(2021)* **표 4 〈현행과 동일〉**	(개정) - 국가기술표준원(e나라표준인증)의 인증제도 명칭을 따름.