TTA Standard

정보통신단체표준(국문표준)

TTAx.xx-xx.xxxx/R1 제(개)정일: 20xx년 xx월 xx일

산업제어시스템 보안요구사항 - 2부: 현장장치 계층

Security Requirements for Industrial Control System - Part 2: Field Device Layer

TTA 한국정보통신기술협회
Telecommunications Technology Association

표준초안 검토 위원회 응용보안 및 평가인증 프로젝트그룹(PG504)

표준안 심의 위원회 정보보호기술위원회(TC5)

	성명	소 속	직위	위원회 및 직위 표준번호
표준(과제) 제안	이종후	ETRI 부설 국가보안기술연구소	책임연구원	PG504 위원
표준 초안 작성자	이종후	ETRI 부설 국가보안기술연구소	책임연구원	PG504 위원
	조영준	ETRI 부설 국가보안기술연구소	연구원	
	최승오	ETRI 부설 국가보안기술연구소	연구원	
	박경미	ETRI 부설 국가보안기술연구소	선임연구원	
	신동훈	ETRI 부설 국가보안기술연구소	선임연구원	
	김경민	ETRI 부설 국가보안기술연구소	연구원	
	민법기	ETRI 부설 국가보안기술연구소	연구원	
	이진경	ETRI 부설 국가보안기술연구소	연구원	
	김우년	ETRI 부설 국가보안기술연구소	책임연구원	
사무국 담당				-

본 표준 발간 이전에 접수된 지식재산권 확약서 정보는 본 표준의 '부록(지식재산권 확약서 정보)'에 명시하고 있으며, 이후 접수된 지식재산권 확약서는 TTA 웹사이트에서 확인할 수 있습니다.
본 표준과 관련하여 접수된 확약서 외의 지식재산권이 존재할 수 있습니다.

발행인 : 한국정보통신기술협회 회장
발행처 : 한국정보통신기술협회
13591, 경기도 성남시 분당구 분당로 47
Tel : 031-724-0114, Fax : 031-724-0109
발행일 : 20xx.xx

서문

1 표준의 목적

본 표준의 목적은 산업제어시스템 보안참조모델에서 현장장치 계층의 보안요구사항을 정의하는데 있다.

2 주요 내용 요약

본 표준에서는 산업제어시스템을 구성하는 구성요소 가운데 현장장치 계층에 속하는 구성요소들을 안전하게 관리 및 운영하는데 필요한 보안요구사항을 정의한다. 본 표준은 산업제어시스템 보안요구사항 - 1부: 개념 및 참조모델에 따라 네트워크 견고성, 서비스 지속성, 보안기능 등 3개 분야에서 12개 분류를 정의하고 총 52개의 세부 보안요구사항을 정의한다.

분야	분류
네트워크 견고성	퍼징 테스트
서비스 지속성	자원 가용성
	물리적 인터페이스 보호
	이벤트 대응
보안기능	보안 감사
	식별・인증
	접근통제
	전송 데이터 보호
	저장 데이터 보호
	보안기능 관리
	상태 관리

3 인용 표준과의 비교

- 해당 사항 없음

Preface

1 Purpose

This standard is to define security requirements for Field Device Layer in ICS (Industrial Control System) Security Reference Model.

2 Summary

The standard is to define the security requirements for managing and operating components of Layer 1(Field Device Layer). The standard defines totally 52 security requirements in 12 functions in 3 areas. 3 areas are based on 'Security Requirements for Industrial Control Systems – Part 1: Concepts and Reference Model'.

Areas	Functions
Network Robustness	Fuzzing Test
	Stress Test
Service Continuity	Resource Availability
	Physical Interface Protection
	Event Response
Security Functions	Security Audit
	Identification and Authentication
	Access Control
	Transmission Data Protection
	Stored Data Protection
	Security Function Management
	State Management

3 Relationship to Reference Standards

N/A

목 차

산업제어시스템 보안요구사항 - 2부: 현장장치 계층
(Security Requirements for Industrial Control System - Part 2: Field Device Layer)

1 적용 범위

1.1. 표준 범위

본 표준은 산업제어시스템을 구성하는 3계층 가운데 현장장치 계층에 위치하는 산업제어시스템 구성요소들을 관리하고 운영하는데 있어서 외부 위협 및 내부 정보 유출 위협에 대응하기 위해 필요한 보안요구사항을 정의한다.

현장장치 계층에 속하는 산업제어시스템 구성요소는 스마트 현장장치이다. 스마트 현장장치는 산업제어시스템 현장에서 사용되는 장치들 중 연산 기능과 통신 기능(무선 또는 이더넷)이 적용된 장치를 의미한다. 이러한 스마트 현장장치의 예로는 현장의 데이터를 수집하여 송신하는 센서가 대표적이다. 이와 같은 현장장치 계층에 위치하는 구성요소가 본 보안요구사항의 적용 대상이 된다.

그러나 현장장치 계층의 구성요소가 스마트 현장장치로만 한정되지는 않는다. 산업제어시스템 보안요구사항 1부에서 기술한 바와 같이 센서, 액츄에이터 등의 상태 데이터를 계측·수집하거나 제어하는 역할을 하며 제어 계층과 통신하는 구성요소는 현장장치 계층에 포함된다고 할 수 있다.

한편, 현장장치 가운데 시리얼 케이블, 구리선 등 hard wired 방식의 연결만 지원하고 연산 기능을 제공하지 않는 장치는 본 표준의 적용 대상이 아니다.

1.2. 표준 구성

본 표준은 산업제어시스템을 구성하는 3계층 가운데 현장장치 계층의 보안요구사항을 정의한다. 산업제어시스템을 대상으로 하는 전체적인 보안개념과 보안참조모델은 산업제어시스템 보안요구사항 - 1부: 개념 및 참조모델에서 정의하고 있다.

2 인용 표준

해당 사항 없음

3 용어 정의

3.1. 서비스 제한 대역폭
시험대상의 모든 기능이 정상적으로 동작할 수 있는 최대 네트워크 대역폭

3.2. 스마트 현장장치
연산 및 통신 기능을 제공하는 현장장치

3.3. 재밍 공격(Jamming Attack)
GPS 전파 교란 등 서비스 거부를 목적으로 전파신호를 의도적으로 발산시켜 정당한 무선통신을 방해하는 공격

3.4. 제어 H/W
제어 프로토콜을 처리하는 임베디드 장치로써, 현장장치의 상태를 수집하거나 제어 S/W의 명령을 받아 현장장치를 제어하고, 이벤트 사항을 통보하는 장치로 제어 계층에 위치

3.5. 제어 S/W
제어 H/W 등과 통신하며 관련 기기들의 상태를 모니터링 및 제어하기 위해 사용되는 S/W로 운영 계층에 위치

3.6. 현장장치
산업제어 현장에서 스팀, 액체, 가스 등 각종 물질을 계측하거나 제어하는데 사용되는 센서, 액추에이터(구동기) 등의 장치

4 약어

DCS	Distributed Control System
HMI	Human Machine Interface
ICS	Industrial Control System
IED	Intelligent Electronic Device
PLC	Programmable Logic Controller
RTU	Remote Terminal Unit

5 가정사항 및 보안위협

5.1. 가정사항

현장장치 계층에 속하는 구성요소들은 실외에 설치·운영되는 경우가 많다는 특징을 갖

는다. 또한 산업제어시스템 보안요구사항 - 1부: 개념 및 참조모델과 일반적인 운영 환경에 따라 다음과 같은 가정사항을 따른다.

A1. 안전한 관리: 현장장치 계층에 포함되는 구성요소들의 인가된 관리자는 안전한 방식으로 관리할 수 있도록 관리방법을 숙지하고 있으며 이에 따라 안전하게 관리·운영한다.

A2. 안전한 프로그램 설치: 인가된 관리자는 현장장치 계층 구성요소에 악의적인 코드가 포함되지 않음을 확인한 뒤에 펌웨어, 응용 프로그램을 설치한다.

A3. 재밍 공격(Jamming Attack) 대응: 현장장치 계층 구성요소들은 재밍 공격으로 인한 통신 두절 시 다른 장치나 다른 통신 경로를 통해 통신을 수행하는 등 재밍 공격에 대한 대응 방안이 마련되어 있다.

5.2. 보안위협

현장장치 계층을 대상으로 하는 보안위협은 다음과 같다. 보안위협원은 현장장치 계층 구성요소에 불법적인 접근을 시도하거나 비정상적인 방법으로 현장장치 계층 구성요소에 위해를 가하는 사용자 또는 IT 실체이다. 현장장치 계층에 대한 보안위협은 이러한 보안위협원이 기밀성, 무결성, 인증, 접근통제, 가용성 관점에서 현장장치 계층 구성요소에게 피해를 줄 수 있는 행위를 의미하며, 보안위협원은 중간 수준의 전문지식, 자원 및 동기를 가진다고 가정한다.

T1. 자원의 과도한 사용: 메모리, 저장공간, 전력, 네트워크 인터페이스 등의 과도한 사용으로 인해 1계층 구성요소의 동작이 멈추는 사태가 발생할 수 있다. 이 위협은 가용성에 피해를 초래할 수 있다.

T2. 물리적 접근을 통한 조작: 실내 공간보다 통제가 어려운 현장장치 계층의 특성을 고려할 때, 상대적으로 손쉽게 공격자가 현장장치 계층 구성요소에 직접 접근할 수 있다. 공격자는 물리적 접근을 통해 현장장치 계층에서 획득한 다양한 정보를 이용하여 정상 구성요소로 위장할 수 있다. 이를 이용하여 정상적인 통신을 방해할 수 있다. 이 위협은 현장장치 계층의 가용성 및 제어 계층과 운영 계층에 속하는 산업제어시스템 구성요소의 가용성에 영향을 미칠 수 있다.

T3. 허용되지 않은 접근: 공격자는 네트워크를 통해 정상적인 인증 절차를 우회하거나 인가되지 않은 방식으로 현장장치 계층 구성요소에 접근하여 악의적으로 장악할 수 있다.

T4. 허용되지 않은 기능 사용: 현장장치 계층 구성요소의 기능 중 허용되지 않은 기능을 사용함으로써 장치 오작동을 유발하여 모든 계층의 구성요소에 피해를 줄 수 있다. 이는

주로 내부자에 의해서 발생하는 위협이다. 이 위협은 서비스 가용성과 무결성에 영향을 미칠 수 있다.

T5. 저장 데이터의 위·변조: 현장장치 계층 구성요소에 저장된 데이터를 공격자가 임의로 변경해 저장된 데이터를 사용하는 사용자 또는 제어 H/W 등이 잘못된 정보에 기반하여 그릇된 판단을 내리도록 할 수 있으며, 이는 현장장치 계층의 데이터 무결성에 영향을 미칠 수 있다.

T6. 통신 데이터의 위·변조: 현장장치 계층 내 구성요소 간 또는 다른 계층의 구성요소와 통신과정에서 메시지를 공격자가 중간에서 변조 또는 위조한 후 최종목적지로 전달함으로써 최종목적지의 수신자가 잘못된 현장상태 정보를 얻도록 할 수 있다. 이는 데이터 무결성에 피해를 줄 수 있으며, 피해의 결과로 현장장치 계층 가용성에 영향을 미칠 수 있다.

T7. 저장 데이터의 유출: 현장장치 계층 구성요소가 저장하고 있는 중요 데이터에 공격자가 무단으로 접근하여 유출할 수 있다. 이는 데이터 기밀성을 손상시키는 것이며, 민감한 데이터의 경우 2차 공격을 위해 악용될 수 있다.

T8. 통신 데이터의 유출: 현장장치 계층 내 구성요소 간 또는 다른 계층의 구성요소와 통신과정에서 송·수신되는 메시지를 공격자가 획득함으로써 중요 데이터가 유출될 수 있다. 이는 데이터 기밀성을 손상시키는 것이며, 민감한 데이터의 경우 2차 공격을 위해 악용될 수 있다.

T9. 정상 서비스의 동작 방해: 현장장치 계층 구성요소가 수행하는 서비스가 정상적으로 수행되지 않도록 비정상 메시지 송신, 전력 차단 등 불법적인 행위로 오동작을 유발시킬 수 있다. 이는 1계층 가용성에 피해를 초래할 수 있다.

T10. 취약한 펌웨어, S/W 업데이트: 현장장치 계층 구성요소에서 운용중인 펌웨어 또는 S/W 업데이트 시, 악성코드가 포함된 파일을 이용하도록 하여 악의적으로 장악할 수 있다. 이는 가용성과 무결성에 영향을 미칠 수 있다.

6 보안요구사항

현장장치 계층 보안요구사항은 산업제어시스템 보안요구사항 – 1부: 개념 및 참조모델에 따라 네트워크 견고성, 서비스 지속성, 보안기능 등 3개 분야, 12개 분류로 구성된다.

보안요구사항의 기술 방식은 다음과 같다.

[항목번호: 보안요구사항을 식별하기 위해서 사용되는 식별번호] [항목명: 보안요구사항의 항목 명칭] [항목 설명: 해당 항목에서 요구하는 사항에 대한 설명] **[M/O: 필수/선택 사항의 구분. 항목이 필수적으로 요구되는 경우에는 'M'이며, 운영환경, 보안정책 등에 따라 필수적이지 않은 항목인 경우에는 'O'로 구분]**

항목번호는 보안요구사항을 식별하기 위해서 사용하며, 구성은 다음과 같다.

[계층]_[분류].[일련번호]

[계층]은 보안요구사항이 적용되는 계층을 나타내다. 2부는 현장장치 계층에 적용되므로 2부의 모든 보안요구사항에는 SF가 부여된다. [분류]는 다음과 같이 부여된다.

FT: 퍼징 테스트
ST: 스트레스 테스트
AV: 자원 가용성
PP: 물리적 인터페이스 보호
RE: 이벤트 대응
AU: 보안 감사
IA: 식별·인증
AC: 접근통제
SC: 전송 데이터 보호
DP: 저장 데이터 보호
SF: 보안기능 관리
SS: 상태 관리

6.1. 네트워크 견고성

6.1.1. 퍼징 테스트 (SF_FT)

SF_FT.1 (필드 순서 위반 처리) 규정되지 않은 순서로 필드가 구성된 패킷을 수신하더라도 서비스를 지속적으로 제공해야 한다. **[M]**

SF_FT.2 (부분 절삭패킷 처리) 일부분이 절삭된 필드를 포함하는 패킷을 수신하더라도 서비스를 지속적으로 제공해야 한다. **[M]**

SF_FT.3 (필드 최소길이 위반 처리) 규정된 최소길이보다 짧은 길이로 구성된 필드를 포함하는 패킷을 수신하더라도 서비스를 지속적으로 제공해야 한다. **[M]**

SF_FT.4 (필드 최대길이 위반 처리) 규정된 최대길이보다 긴 길이로 구성된 필드를 포함하는 패킷을 수신하더라도 서비스를 지속적으로 제공해야 한다. **[M]**
SF_FT.5 (필드 지정길이 위반 처리) 규정된 길이를 위배하는 필드를 포함하는 패킷을 수

신하더라도 서비스를 지속적으로 제공해야 한다. [M]

SF_FT.6 (최소 반복횟수 위반 처리) 규정된 최소 반복횟수보다 적게 하위필드를 반복하는 패킷을 수신하더라도 서비스를 지속적으로 제공해야 한다. [M]

SF_FT.7 (최대 반복횟수 위반 처리) 규정된 최대 반복횟수보다 많게 하위필드를 반복하는 패킷을 수신하더라도 서비스를 지속적으로 제공해야 한다. [M]

SF_FT.8 (지정 반복횟수 위반 처리) 지정된 반복횟수와는 다른 횟수만큼 하위필드를 반복하는 패킷을 수신하더라도 서비스를 지속적으로 제공해야 한다. [M]

SF_FT.9 (고정 필드값 위반 처리) 규정된 고정값과는 다른 값이 입력된 필드를 포함하는 패킷을 수신하더라도 서비스를 지속적으로 제공해야 한다. [M]

SF_FT.10 (필드값 유효범위 위반 처리) 규정된 유효범위 밖의 값이 입력된 필드를 포함하는 패킷을 수신하더라도 서비스를 지속적으로 제공해야 한다. [M]

SF_FT.11 (프로토콜 문맥 위반 처리) 프로토콜 문맥상 부적절한 값을 포함하는 패킷을 수신하더라도 서비스를 지속적으로 제공해야 한다. [M]

6.1.2. 스트레스 테스트 (SF_ST)

SF_ST.1 (유효 패킷 플러딩 처리) 서비스 제한 대역폭과 네트워크 처리 최대 대역폭에 해당하는 플러딩이 발생하더라도 서비스를 지속적으로 제공해야 한다. [O]

SF_ST.2 (초과된 접속시도 처리) 최대 동시 네트워크 접속 허용수에 해당하는 접속이 발생하더라도 서비스를 지속적으로 제공해야 한다. [O]

6.2. 서비스 지속성

6.2.1. 자원 가용성 (SF_AV)

SF_AV.1 (자원 관리) 배터리 사용시간 관리 기능을 제공해야 한다. [O]

SF_AV.2 (백업) 스마트 현장장치에서 사용하는 중요 정보(예 : 기기 설정 정보)에 대한 백업 기능을 제공해야 한다. [O]

SF_AV.3 (복구) 장애, 고장 등 발생 시 백업본을 활용하여 백업을 수행하였던 시점의 정상 상태로 복구할 수 있어야 한다. [O]

6.2.2. 물리적 인터페이스 보호 (SF_PP)

SF_PP.1 (무선모듈 통제) 스마트 현장장치에서 무선통신 기능을 제공하고, 해당 무선통신을 사용하지 않을 경우 무선통신과 관련된 기능을 제한(예 : Disable 설정)하는 기능을 제공해야 한다. **[M]**

SF_PP.2 (디버그 인터페이스 사용 제한) 스마트 현장장치에서 디버깅 등의 용도로 사용되는 인터페이스(예 : UART, JTAG 등의 디버그용 핀)가 존재하는 경우 물리적으로 제거하거나 사용을 제한(예 : Disable 설정)하는 기능을 제공해야 한다. **[O]**

SF_PP.3 (물리접근 탐지) 인가되지 않은 물리적인 접근 시도를 탐지하는 기능을 제공해야 한다. **[O]**

6.2.3. 이벤트 대응 (SF_RE)

SF_RE.1 (통신장애 대응) 네트워크 통신두절 발생 시 연결을 재설정(예 : 입출력 대기상태 초기화) 할 수 있어야 한다. **[M]**

6.3. 보안기능

6.3.1. 보안 감사 (SF_AU)

SF_AU.1 (감사로그 생성) 다음과 같은 중요 이벤트에 대해 감사로그를 생성하는 기능을 제공해야 한다.

- 스마트 현장장치의 가동/중지
- 로그 생성기능의 시작/종료
- 식별·인증의 성공/실패
- 네트워크 및 보안 설정의 변경

또한, 감사로그에 기록된 각 이벤트에는 다음의 정보가 포함되어야 한다.

- 이벤트 발생일시
- 이벤트 유형
- 이벤트 발생 주체(가능한 경우)
- 작업내역 및 결과(성공/실패) **[O]**

SF_AU.2 (감사로그 포화 경고) 저장된 로그가 설정된 용량을 초과하는 경우, 다음의 항목을 포함하는 사전 정의된 방식에 따라 관리자에게 통보해야 한다.

- 제공 방법(예 : 경고등 점등)
- 알람발생 임계치(예 : 저장공간 90% 포화) **[O]**

SF_AU.3 (감사로그 전송) 감사로그를 주기적으로 별도 시스템 또는 저장매체로 전송(예

: syslog, Historian 등)하는 기능을 제공해야 한다. [O]

SF_AU.4 (타임스탬프 사용) 외부 장치로부터 신호를 받아 시각정보를 동기화하는 기능을 제공해야 한다. [O]

SF_AU.5 (감사로그 보호) 감사로그를 위·변조, 무단 삭제 등으로부터 보호하는 기능을 제공해야 한다. [O]

6.3.2. 식별·인증 (SF_IA)

SF_IA.1 (사용자 식별·인증) 사용자의 신원을 확인하기 위해 서비스 제공 이전에 식별·인증 기능을 제공해야 한다. [M]

SF_IA.2 (장치 식별·인증) 사용자를 대신하여 접근하는 장치의 신원을 검증하기 위해 서비스 제공 이전에 식별·인증 기능을 제공해야 한다. [O]

SF_IA.3 (패스워드 변경) 사용자 로그인 패스워드는 하드코딩 되어 있지 않아야 하며 관리자가 지정한 주기에 따라 또는 사용자가 임의로 변경할 수 있어야 한다. 또한, 패스워드의 변경은 스마트 현장장치의 동작에 영향을 미치지 않아야 한다. [M]

SF_IA.4 (복잡한 패스워드) 복잡한 패스워드의 사용을 강제화할 수 있는 기능을 제공해야 한다(최소 6자리 이상의 패스워드 사용을 강제하는 기능). [O]

SF_IA.5 (패스워드 보호) 패스워드의 전송 및 저장 시 암호화 기법이 적용되어야 한다. 또한, 사용자가 입력을 위해 입력하는 패스워드는 노출 방지를 위해 마스킹(예 : ****) 처리되어야 한다. [M]

SF_IA.6 (인증 실패 대응) 인증 실패 시 출력되는 메시지는 공격에 사용될 수 있는 추가 정보(예 : “Invalid ID”, “Invalid Password” 등)를 포함하지 않아야 하며, 일정횟수 이상 인증 실패 반복 시 계정을 차단하는 기능을 제공해야 한다. 접근이 차단된 계정은 관리자가 확인 후 직접 해제하거나 관리자가 정한 시간 이후 차단 해제되어야 한다. [O]

SF_IA.7 (PKI 인증서) 스마트 현장장치에서 PKI 기반 인증을 지원하는 경우, 관련 표준을 준용하는 인증체계 및 안전한 비도를 가지는 인증서를 사용해야한다. [O]

6.3.3. 접근통제 (SF_AC)

SF_AC.1 (권한 분리) 관리자 모드와 일반 사용자 모드를 구분하고 모드에 따라 사용할 수 있는 권한을 제한하는 기능을 제공해야 한다. [O]

SF_AC.2 (접근제한) 관리자의 정책에 따라 사용자 또는 장치별 접근을 제한하는 기능을 제공해야 한다. [O]

SF_AC.3 (관리자 세션 잠금) 스마트 현장장치는 접속 후 일정시간 동안 입력이 없는 관리자 로그인 세션에 대해 자동으로 잠금 또는 종료하는 기능을 제공해야 한다. [O]

SF_AC.4 (동시 세션 제한) 관리자의 접속에 대해 동시에 접속가능한 세션 수를 제한하는 기능을 제공해야 한다. [O]

6.3.4. 전송 데이터 보호 (SF_SC)

SF_SC.1 (전송 데이터 무결성) 민감한 전송 데이터(예 : 제어명령, 상태정보 등)에 대해 위·변조 여부와 재사용 공격에 대비한 최신성 여부를 확인할 수 있도록 무결성 보장 기능을 제공해야 한다. [O]

SF_SC.2 (전송 데이터 기밀성) 민감한 전송 데이터(예 : 제어명령, 상태정보 등)에 대해 기밀성 보장 기능을 제공해야 한다. [O]

SF_SC.3 (통신세션 자동 종료) 일대일 통신에 있어 다음과 같은 세션에 대해 종료하는 기능을 제공해야 한다.
- 사용목적을 달성한 세션
- 설정시간을 초과한 세션
- 설정시간 동안 미사용중인 세션 [O]

SF_SC.4 (멀티캐스트/브로드캐스트 통신 관리) 멀티캐스트 통신과 브로드캐스트 통신을 지원하지 않거나, 지원하는 경우 제한할 수 있어야 한다. [O]

6.3.5. 저장 데이터 보호 (SF_DP)

SF_DP.1 (잔여정보 보호) 제어 H/W의 불용처리 등에 대비하여 민감한 정보(예 : 계정 및 패스워드 정보, 감사로그, 설정 정보 등)를 삭제하는 기능(예 : 공장 초기화)을 제공해야 한다. [M]

SF_DP.2 (저장 데이터 기밀성) 민감한 데이터(예 : 감사로그, 설정 정보 등)가 평문으로 저장되지 않도록 보호기능(예 : 인코딩, 암호화 등)을 제공해야 한다. [O]

SF_DP.3 (저장 데이터 무결성) 민감한 데이터(예: 감사로그, 설정 정보 등)에 대해 위·변조 여부를 확인할 수 있도록 무결성 보장 기능을 제공해야 한다. [O]

6.3.6. 보안기능 관리 (SF_SF)

SF_SF.1 (네트워크 및 보안 설정 관리) 관리자가 스마트 현장장치의 현재 네트워크 설정과 보안 설정을 확인할 수 있어야 하며, 네트워크 정책과 보안정책에 따라 해당 설정을 변경할 수 있어야 한다. **[M]**

SF_SF.2 (암호연산) 암호연산을 사용하는 경우 안전한 암호 알고리즘 및 암호키 길이를 사용하여 암호연산이 수행되어야 한다. **[M]**

SF_SF.3 (암호키 관리) 암호연산을 위해 사용하는 암호키에 대해 안전한 키 생성/설정/저장/파기 방법을 사용해야 한다. **[M]**

6.3.7. 상태 관리 (SF_SS)

SF_SS.1 (실행코드 무결성) 실행코드에 대한 변조 여부를 식별 또는 방지할 수 있도록 무결성 검증을 수행해야 한다. **[O]**

SF_SS.2 (자체시험) 스마트 현장장치의 주요 기능에 대한 정상동작을 확인하는 자체시험을 주기적(예 : 시동 시, 1일 1회 등)으로 또는 관리자의 요청에 따라 수행하는 기능을 제공해야 한다. **[O]**

SF_SS.3 (펌웨어 무결성) 스마트 현장장치 펌웨어 업데이트 시 무결성을 검증할 수 있는 기능을 제공해야 한다. **[O]**

SF_SS.4 (쓰기 보호) 운전 중 메모리 쓰기, 수정을 방지하는 메커니즘을 적용해야 한다. **[O]**

SF_SS.5 (예정된 출력) 스마트 현장장치가 정상 작동을 하지 못하는 상황이 발생할 경우, 미리 정해진 출력을 유지해야 한다. **[O]**

SF_SS.6 (취약점 대응) 스마트 현장장치에 보안 취약점이 존재하지 않아야 한다. **[M]**

부 속 서 A
현장장치 계층 보안요구사항 시험 방법

A.1 구성

보안요구사항 시험 방법은 시험대상이 각 보안요구사항을 만족하는지에 대한 확인을 위해 필요한 시험 절차, 준비사항, 통과 기준 등을 제시한다. 시험 방법은 <표 A-1>과 같은 방식으로 구성된다.

<표 A-1> 보안요구사항 시험 방법 구성

구성	설명
시험 목적	각 보안요구사항에 따른 시험 목적을 제시
준비사항	해당 보안요구사항에 대한 시험 수행을 위해 피시험자가 제출해야하는 문서 또는 정보, 추가적인 설비 등을 제시
시험 세부항목	시험을 통해 확인해야 할 목록 제시
통과 기준	보안요구사항을 만족한 것으로 판단할 수 있는 기준 제시
주의사항(추가사항)	시험과 관련하여 추가적인 사항 또는 주의해야 할 내용을 기술
시험항목 예시 (SF_AV.1)	□ 시험 목적 ㅇ 배터리 사용시간 관리를 위한 기능 지원 확인 □ 준비사항 ㅇ 공통 준비사항 참고 □ 시험 세부항목 ① 배터리 전원 사용시간 기능(예: 사용 모드 선택, 배터리 잔여량에 따라 제공하는 서비스 제한 등)을 지원하는지 확인 □ 통과 기준 ㅇ 시험 세부항목 ①에서 배터리 사용시간 관리 기능을 지원하는 경우 □ 주의사항(추가사항) ㅇ 배터리 사용시간 관리 기능을 지정할 수 없으나 시험 대상 내부에 기본적으로 구현되어 있음을 관련 문서에서 확인할 수 있는 경우 '통과'로 간주 ㅇ 배터리를 사용하지 않고 상시 전원 공급을 받는 시험 대상의 경우 시험을 수행하지 않음

A.2 네트워크 견고성 시험항목

□ 시험 공통사항

- ㅇ 시험대상이 비정상 패킷의 폐기 등과 같은 일반적인 대응방법 이외의 대응방법을 사용하는 경우, 시험자는 시험의 목적을 위배하지 않는 범위에서 피시험자와 협의하여 다른 시험방법을 채택할 수 있다.
- ㅇ 스마트 현장장치 네트워크 견고성은 제어 H/W 네트워크 견고성 시험환경에 준하여 구성한다.

※ 시험환경은 시험대상의 특성에 따라 피시험자와 협의하여 진행할 수 있다.

□ 스마트 현장장치 서비스의 정상 동작 판단기준

- ㅇ 관측 장비를 통해 일정시간(예 : 1초)마다 시험대상에게 스마트 현장장치의 고유 기능을 확인하는 명령(예 : 센싱 정보 수집)을 전송한 후, 명령에 따라 기능이 수행되는 경우 정상 동작으로 판단

※ 시험대상의 특성에 따라 피시험자와 협의하여 현장장치의 기능 확인을 수행할 수 있다.

□ 공통 준비사항(피시험자의 제출물)

- ㅇ 시험대상
- ㅇ 제품 매뉴얼, 사용자/관리자 매뉴얼 등 시험대상을 구매하는 고객에게 제공되는 문서
- ㅇ 네트워크 인터페이스 및 제어 프로토콜 설명자료
- ㅇ 스마트 현장장치의 서비스를 모니터링하는데 필요한 각종 H/W 및 S/W

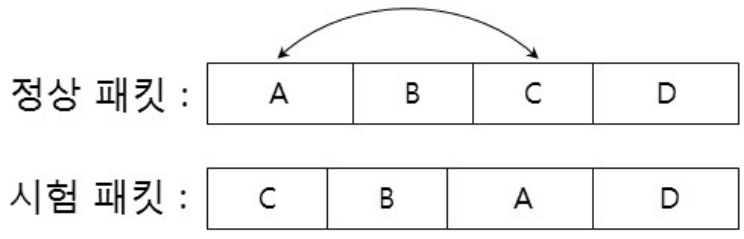
※ 시험기관이 소요 장비를 이미 갖추고 있는 경우, 제출을 생략할 수 있다.

A.2.1 퍼징테스트(SF_FT)

A.2.1.1 필드 순서 위반처리(SF_FT.1)

□ 시험 목적

- ㅇ 프로토콜에 규정되지 않은 방법으로 필드의 순서가 변경된 패킷이 시험대상에게 전송되는 경우, 시험대상이 정상 동작하는지 확인



(그림 A-1) 필드 순서 위반 예제

□ 준비사항

ㅇ 공통 준비사항 참고

□ 시험 세부항목

① 고정 길이의 PDU 헤더에서 임의로 복수 쌍의 필드를 선택하고 교환 연산하여 생성된 PDU를 시험대상에게 전송한 후, 서비스 지속 여부 확인

② 가변 길이의 PDU 헤더에서 임의로 복수 쌍의 필드를 선택하고 교환 연산하여 생성된 PDU를 시험대상에게 전송한 후, 서비스 지속 여부 확인

□ 통과 기준

ㅇ 시험 세부항목 ① 및 ②에서 시험대상의 서비스가 정상 동작하는 경우

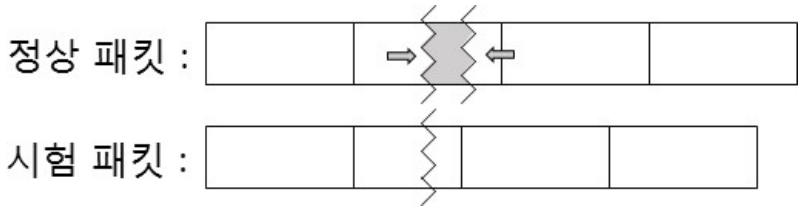
□ 주의사항(추가사항)

ㅇ 시험대상에서 지원하는 각 프로토콜별 임의의 필드 선택방법 및 선택 개수는 시험절차서(별도 문서) 준용

A.2.1.2 부분 절삭패킷 처리(SF_FT.2)

□ 시험 목적

ㅇ 프로토콜에 규정되지 않은 방법으로 필드의 일부분이 절삭되어 시험대상에게 전송되는 경우, 시험대상이 정상 동작하는지 확인



(그림 A-2) 부분 절삭패킷 예제

□ 준비사항

ㅇ 공통 준비사항 참고

□ 시험 세부항목

ㅇ ① 프로토콜에 규정된 헤더 데이터 일부를 임의로 삭제한 PDU를 시험대상에게 전송한 후, 서비스 지속 여부 확인

□ 통과 기준

ㅇ 시험 세부항목 ①에서 시험대상의 서비스가 정상 동작하는 경우

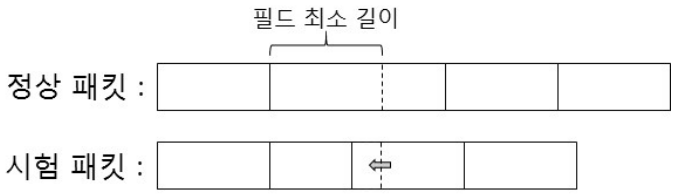
□ 주의사항(추가사항)

ㅇ 시험대상에서 지원하는 각 프로토콜별 분할 대상 필드의 선택 방법 및 선택 개수는 시험 절차서(별도 문서) 준용

A.2.1.3 필드 최소길이 위반처리(SF_FT.3)

□ 시험 목적

ㅇ 프로토콜에 규정된 최소길이보다 짧은 길이로 필드를 구성하여 시험대상에게 전송하는 경우, 시험대상이 정상 동작하는지 확인



(그림 A-3) 필드 최소길이 위반 예제

□ 준비사항

ㅇ 공통 준비사항 참고

□ 시험 세부항목

ㅇ ① 필드의 최소 길이가 규정되어 있는 필드에 대해서 제한된 길이보다 임의 길이만큼 짧은 길이의 데이터로 구성한 PDU를 시험대상에게 전송한 후, 서비스 지속 여부 확인

□ 통과 기준

ㅇ 시험 세부항목 ①에서 시험대상의 서비스가 정상 동작하는 경우

□ 주의사항(추가사항)

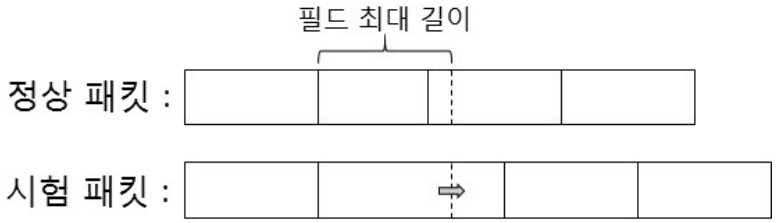
ㅇ 시험대상에서 지원하는 각 프로토콜별 임의의 필드 길이 선택 방법은 시험 절차서(별도 문서) 준용

ㅇ 최소길이가 규정된 필드가 1개 이상인 경우 모든 해당 필드에 대해 각각 상기 시험 세부항목을 적용

A.2.1.4 필드 최대길이 위반처리(SF_FT.4)

□ 시험 목적

ㅇ 프로토콜에 규정된 최대길이를 초과하는 길이로 필드를 확장하여 시험대상에게 전송하는 경우, 시험대상이 정상 동작하는지 확인



(그림 A-4) 필드 최대길이 위반 예제

□ 준비사항

ㅇ 공통 준비사항 참고

□ 시험 세부항목

① 필드의 최대 길이가 규정되어 있는 필드에 대해서 제한된 길이보다 임의 길이만큼 긴 길이의 데이터로 구성한 PDU를 시험대상에게 전송한 후, 서비스 지속 여부 확인

□ 통과 기준

ㅇ 시험 세부항목 ①에서 시험대상의 서비스가 정상 동작하는 경우

□ 주의사항(추가사항)

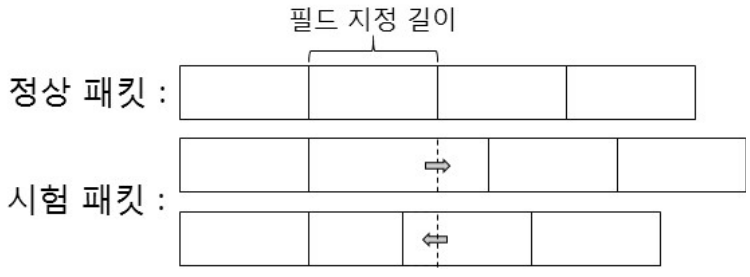
ㅇ 시험대상에서 지원하는 각 프로토콜별 임의의 필드 길이 선택 방법은 시험 절차서(별도 문서) 준용

ㅇ 최대길이가 규정된 필드가 1개 이상인 경우 모든 해당 필드에 대해 각각 상기 시험 세부항목을 적용

A.2.1.5 필드 지정길이 위반처리(SF_FT.5)

□ 시험 목적

ㅇ 프로토콜 상 필드의 길이가 고정값으로 규정되어 있거나 패킷 내부의 다른 필드에 의해 지정되는 필드에 대해 규정된 길이와 다른 길이로 패킷을 구성하여 시험대상에게 전송하는 경우, 시험대상이 정상 동작하는지 확인



(그림 A-5) 필드 지정길이 위반 예제

□ 준비사항

ㅇ 공통 준비사항 참고

□ 시험 세부항목

① 필드의 길이가 고정적으로 규정되어 있는 필드에 대해서 규정된 길이보다 임의 길이만큼 긴 길이의 데이터로 구성한 PDU를 시험대상에게 전송한 후, 서비스 지속 여부 확인

② 필드의 길이가 고정적으로 규정되어 있는 필드에 대해서 규정된 길이보다 임의 길이만큼 짧은 길이의 데이터로 구성한 PDU를 시험대상에게 전송한 후, 서비스 지속 여부 확인

□ 통과 기준

ㅇ 시험 세부항목 ① 및 ②에서 시험대상의 서비스가 정상 동작하는 경우

□ 주의사항(추가사항)

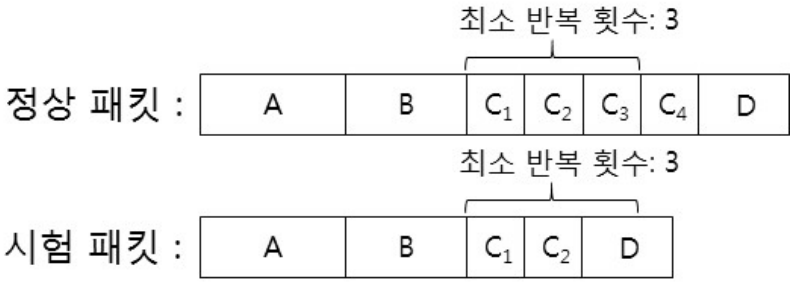
ㅇ 시험대상에서 지원하는 각 프로토콜별 임의의 필드 길이 선택 방법은 시험 절차서(별도 문서) 준용

ㅇ 필드의 길이가 고정값 또는 다른 필드에 의해 규정되는 필드가 1개 이상인 경우 모든 해당 필드에 대해 각각 상기 시험 세부항목을 적용

A.2.1.6 최소 반복횟수 위반처리(SF_FT.6)

□ 시험 목적

ㅇ 프로토콜 상 최소 반복횟수가 규정된 하위필드에 대해 최소 반복횟수를 미달하는 하위필드로 구성된 패킷이 시험대상에게 전송되는 경우, 시험대상이 정상 동작하는지 확인



(그림 A-6) 최소 반복횟수 위반 예제

□ 준비사항

ㅇ 공통 준비사항 참고

□ 시험 세부항목

① 최소 반복횟수가 규정되어 있는 하위필드에 대해서 제한된 반복횟수를 미달하여 반복되는 하위필드로 구성한 PDU를 시험대상에게 전송한 후, 서비스 지속 여부 확인

□ 통과 기준

ㅇ 시험 세부항목 ① 및 ②에서 시험대상의 서비스가 정상 동작하는 경우

□ 주의사항(추가사항)

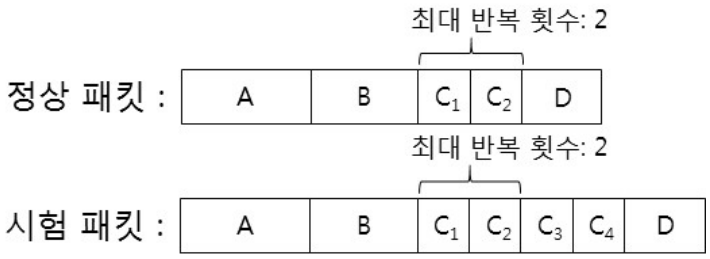
ㅇ 시험대상에서 지원하는 각 프로토콜별 임의의 하위필드 반복횟수 선택 방법은 시험 절차서(별도 문서) 준용

ㅇ 최소 반복횟수가 규정된 하위필드가 1개 이상인 경우 모든 해당 하위필드에 대해 각각 상기 시험 세부항목을 적용

A.2.1.7 최대 반복횟수 위반처리(SF_FT.7)

□ 시험 목적

ㅇ 프로토콜 상 최대 반복횟수가 규정된 하위필드에 대해 최대 반복횟수를 초과하는 하위필드로 구성된 패킷이 시험대상에게 전송되는 경우, 시험대상이 정상 동작하는지 확인



(그림 A-7) 최대 반복횟수 위반 예제

□ 준비사항

ㅇ 공통 준비사항 참고

□ 시험 세부항목

① 최대 반복횟수가 규정되어 있는 하위필드에 대해서 제한된 반복횟수를 초과하여 반복되는 하위필드로 구성한 PDU를 시험대상에게 전송한 후, 서비스 지속 여부 확인

□ 통과 기준

ㅇ 시험 세부항목 ①에서 시험대상의 서비스가 정상 동작하는 경우

□ 주의사항(추가사항)

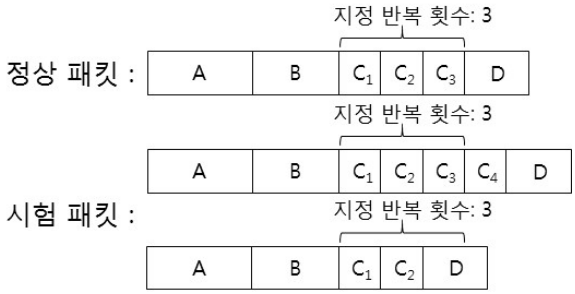
ㅇ 시험대상에서 지원하는 각 프로토콜별 임의의 하위필드 반복횟수 선택 방법은 시험 절차서(별도 문서) 준용

ㅇ 최대 반복횟수가 규정된 하위필드가 1개 이상인 경우 모든 해당 하위필드에 대해 각각 상기 시험 세부항목을 적용

A.2.1.8 지정 반복횟수 위반처리(SF_FT.8)

□ 시험 목적

ㅇ 프로토콜 상 반복횟수가 고정되어 있거나 다른 필드에 의해 규정되는 하위필드에 대해 규정된 반복횟수와 다르게 반복되도록 구성된 패킷이 시험대상에게 전송되는 경우, 시험대상이 정상 동작하는지 확인



(그림 A-8) 지정 반복횟수 위반 예제

□ 준비사항

ㅇ 공통 준비사항 참고

□ 시험 세부항목

① 반복횟수가 고정적으로 규정되어 있는 하위필드에 대해서 규정된 반복횟수를 초과하여 반복되는 하위필드로 구성한 PDU를 시험대상에게 전송한 후, 서비스 지속 여부 확인

② 반복횟수가 고정적으로 규정되어 있는 하위필드에 대해서 규정된 반복횟수를 미달하여 반복되는 하위필드로 구성한 PDU를 시험대상에게 전송한 후, 서비스 지속 여부 확인

□ 통과 기준

ㅇ 시험 세부항목 ① 및 ②에서 시험대상의 서비스가 정상 동작하는 경우

□ 주의사항(추가사항)

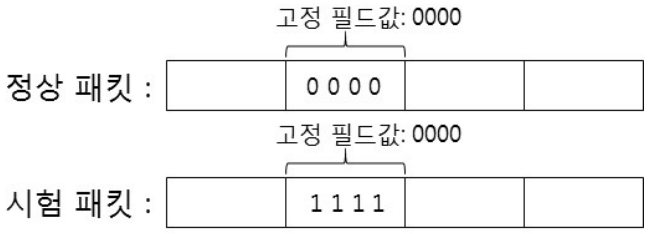
ㅇ 시험대상에서 지원하는 각 프로토콜별 임의의 하위필드 반복횟수 선택 방법은 시험 절차서(별도 문서) 준용

ㅇ 반복횟수가 고정값 또는 다른 필드에 의해 규정되는 하위필드가 1개 이상인 경우 모든 해당 하위필드에 대해 각각 상기 시험 세부항목을 적용

A.2.1.9 고정 필드값 위반처리(SF_FT.9)

□ 시험 목적

ㅇ 프로토콜 상 필드값이 고정되어 있는 필드에 대해 고정값과는 상이한 필드값으로 구성된 패킷이 시험대상에게 전송되는 경우, 시험대상이 정상 동작하는지 확인



(그림 A-9) 고정 필드값 위반 예제

□ 준비사항

ㅇ 공통 준비사항 참고

□ 시험 세부항목

① 필드값이 고정되어 있는 필드에 대해 해당 필드의 길이만큼 임의 작성된 데이터로 구성한 PDU를 시험대상에게 전송한 후, 서비스 지속 여부 확인

□ 통과 기준

ㅇ 시험 세부항목 ①에서 시험대상의 서비스가 정상 동작하는 경우

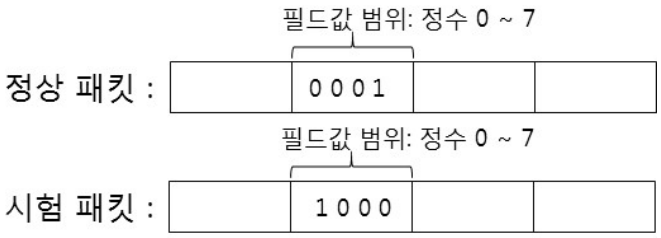
□ 주의사항(추가사항)

ㅇ 필드값이 고정된 필드가 1개 이상인 경우 모든 해당 필드에 대해 각각 상기 시험 세부항목을 적용

A.2.1.10 필드값 유효범위 위반처리(SF_FT.10)

□ 시험 목적

ㅇ 프로토콜 상 필드값의 유효범위가 규정된 필드에 대해 유효범위의 경계값, 중앙값 및 해당 이웃값을 이용하여 생성한 패킷을 시험대상에게 전송하는 경우, 시험대상이 정상 동작하는지 확인



(그림 A-10) 필드값 범위 위반 예제

□ 준비사항

ㅇ 공통 준비사항 참고

□ 시험 세부항목

① 필드값의 유효범위가 정수로 정의되어 있는 필드에 대해 최소한 유효범위의 경계값, 중앙값 및 해당 이웃값으로 구성한 PDU를 시험대상에게 전송한 후, 서비스 지속 여부 확인

② 필드값의 유효범위가 열거형으로 정의되어 있는 필드에 대해 최소한 첫 번째 요소값, 마지막 요소값, 중간 요소값 및 해당 이웃값으로 구성한 PDU를 시험대상에게 전송한 후, 서비스 지속 여부 확인

□ 통과 기준

ㅇ 시험 세부항목 ① 및 ②에서 시험대상의 서비스가 정상 동작하는 경우

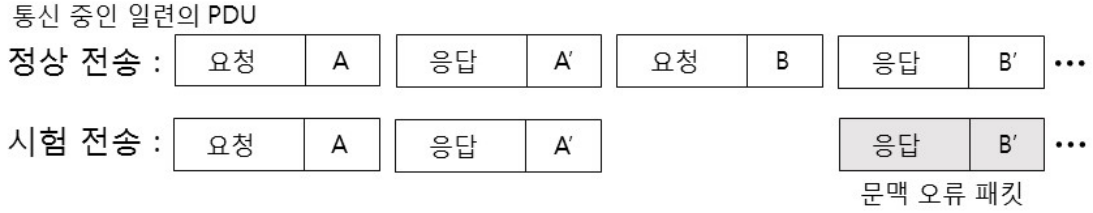
□ 주의사항(추가사항)

ㅇ 필드값의 유효범위가 정의된 필드가 1개 이상인 경우 모든 해당 필드에 대해 각각 상기 시험 세부항목을 적용

A.2.1.11 프로토콜 문맥 위반처리(SF_FT.11)

□ 시험 목적

ㅇ 프로토콜 문맥(Context)상 부적절한 값으로 구성된 패킷이 시험대상에게 전송되는 경우, 시험대상이 정상 동작하는지 확인



(그림 A-11) 프로토콜 문맥 위반 예제

□ 준비사항

ㅇ 공통 준비사항 참고

□ 시험 세부항목

① 프로토콜 데이터 전송과정에서 이전 PDU 또는 이후 PDU와 비교할 때, 문맥상 부적절한 의미를 포함하는 PDU를 시험대상에게 전송한 후, 서비스 지속 여부 확인 (예 : 요청-응답 형식의 데이터 전송 방식에서 요청이 없는 상태에서 응답을 전송하는 경우 등)

② 단일 PDU 내에서 프로토콜 문맥상 동시에 설정될 수 없는 값이 설정된 필드들을 포함하는 PDU를 시험대상에게 전송한 후, 서비스 지속 여부 확인 (예 : PDU 내부의 1개의 필드가 다른 필드의 타입 지시자(Type Indicator)로 사용될 때, 해당 필드의 타입과 상이한 타입 지시자가 설정되는 경우 등)

□ 통과 기준

ㅇ 시험 세부항목 ① 및 ②에서 시험대상의 서비스가 정상 동작하는 경우

□ 주의사항(추가사항)

ㅇ 프로토콜 문맥이 고려되어야 하는 필드가 1개 이상인 경우 모든 해당 필드에 대해 각각 상기 시험 세부항목을 적용

A.2.2 스트레스 테스트(SF_ST)

A.2.2.1 유효 패킷 플러딩 처리(SF_ST.1)

□ 시험 목적

ㅇ 시험대상의 서비스 제한 대역폭과 네트워크 처리 최대 대역폭(시험대상의 네트워크 인터페이스 하드웨어 사양)에 상응하는 유효 패킷 플러딩에 대해 시험대상이 정상 동작하는지 확인

□ 준비사항

ㅇ 공통 준비사항 이외의 피시험자의 제출사항

- 네트워크 부하처리 기능에 대한 설명자료
  - 네트워크 부하처리 방법 및 회복 방법에 대한 설명자료
  - 시험에 영향을 줄 수 있는 방어동작(예 : IP 차단) 설명자료
  - 네트워크 최대 대역폭 및 서비스 제한 대역폭 설명자료
  - 시험대상에게 네트워크 최대 대역폭까지 부하를 발생시키는 방법 및 부하 상태를 확인할 수 있는 방법에 대한 설명자료

※ 시험에 영향을 줄 수 있는 방어 기능이 포함되어 있는 경우, 피시험자와 시험방법을 협의하여 시험을 진행한다.

□ 시험 세부항목

① 시험도구를 통해 서비스 제한 대역폭까지 유효 패킷을 발생시켜 시험대상에게 전송하면서 시험대상의 서비스가 정상 동작하는지 확인

② 시험도구를 통해 네트워크 인터페이스에서 지원하는 최대 대역폭(시험대상의 하드웨어 사양)을 초과하는 대역폭으로 유효 패킷을 발생시켜 일정시간(예 : 5초) 동안 시험대상에게 전송하고 이후 전송 속도를 줄이면서 서비스 제한 대역폭 이하로 패킷이 전송될 때, 시험대상의 서비스가 정상 동작하도록 회복하는지 확인

□ 통과 기준

ㅇ 시험 세부항목 ①에서 시험대상이 정상 동작하고, 시험 세부항목 ②에서 서비스 제한 대역폭 이하로 패킷이 줄어든 후 합리적인 시간(예 : 30초) 내에 시험대상의 동작이 정상으로 회복되는 경우

□ 주의 사항(추가 사항)

ㅇ 최대 대역폭 이상의 패킷에 대해 네트워크 부하처리 설명 자료에 따라 시험대상의 동작이 중단되는 경우 시험을 실패한 것으로 간주하지 않음

ㅇ 시험 환경에 따라 발생시키는 부하를 조정할 수 있음(예: 서비스 제한 대역폭 또는 네트워크 인터페이스 최대 대역폭의 70%의 부하 발생)

A.2.2.2 초과된 접속시도 처리(SF_ST.2)

□ 시험 목적

ㅇ 시험대상의 최대 동시 네트워크 접속수를 초과하도록 접속을 시도한 후 시험대상이 정상 동작하는지 확인

□ 준비사항

ㅇ 공통 준비사항 이외의 피시험자의 제출사항

- 최대 동시 접속 허용수에 대한 설명자료

□ 시험 세부항목

① 시험도구를 통해 시험대상에게 연결을 시도하고 연결이 수락되면 기존 연결을 유지한 상태로 지속적으로 새로운 연결을 시도하여 시험대상의 최대 동시 접속 허용수를 초과하도록 한 후, 서비스 지속 여부 확인

□ 통과 기준

ㅇ 시험 세부항목 ①에서 시험대상의 연산 및 통신 기능이 정상 동작하는 경우

□ 주의 사항(추가 사항)

ㅇ 연결지향 프로토콜을 지원하지 않는 경우 시험을 수행하지 않음

A.3 서비스 지속성 시험항목

□ 공통 준비사항(피시험자의 제출물)
- ㅇ 시험대상
- ㅇ 제품 매뉴얼, 사용자/관리자 매뉴얼 등 시험대상을 구매하는 고객에게 제공되는 문서
- ㅇ 시험대상에서 직접 설정확인이 어려운 경우, 설정을 확인할 수 있는 별도의 장치 일체

A.3.1 자원 가용성(SF_AV)

A.3.1.1 자원 관리(SF_AV.1)

□ 시험 목적
- ㅇ 배터리 사용시간 관리를 위한 기능 지원 확인

□ 준비사항
- ㅇ 공통 준비사항 참고

□ 시험 세부항목
① 배터리 사용시간 관리 기능(예: 저전력 모드 선택, 배터리 잔여량에 따라 제공하는 서비스 제한 등)을 지원하는지 확인

□ 통과 기준
- ㅇ 시험 세부항목 ①에서 배터리 사용시간 관리 기능을 지원하는 경우

□ 주의사항(추가사항)
- ㅇ 배터리 사용시간 관리 기능을 지정할 수 없으나 시험 대상 내부에 기본적으로 구현되어 있음을 관련 문서에서 확인할 수 있는 경우 '통과'로 간주
- ㅇ 배터리 사용시간 관리 기능 지원하지 않으나 관련 문서에서 배터리 수명에 관한 내용이 명시되어 있는 경우(예: 60초마다 값 업데이트 설정 시 10년 사용 보장) '통과'로 간주
- ㅇ 배터리를 사용하지 않고 상시 전원 공급을 받는 시험 대상의 경우 시험을 수행하지 않음

A.3.1.2 백업(SF_AV.2)

□ 시험 목적
- ㅇ 중요 정보에 대한 백업 기능 확인

□ 준비사항

ㅇ 공통 준비사항 이외의 피시험자의 제출사항

- 백업되는 정보(데이터) 및 저장 위치에 대한 설명자료
- 백업 파일의 생성 위치가 시험대상이 아닌 다른 기기인 경우, 백업 파일을 업로드・다운로드할 수 있는 장치 일체

□ 시험 세부항목

① 다음의 중요 정보에 대해 백업이 수행되는지 확인

0 네트워크 및 보안 설정을 포함한 기기 설정정보 일체

□ 통과 기준

ㅇ 시험 세부항목 ①에서 백업이 정상적으로 수행되는 경우

□ 주의사항(추가사항)

ㅇ 없음

A.3.1.3 복구(SF_AV.3)

□ 시험 목적

ㅇ 장애, 고장 등 발생 시 기존 백업하였던 정상 상태로의 복구 기능 확인

□ 준비사항

ㅇ 공통 준비사항 이외의 피시험자의 제출사항

- 백업되는 정보(데이터) 및 저장 위치에 대한 설명자료
- 백업 파일의 생성 위치가 시험대상이 아닌 다른 기기인 경우, 백업 파일을 업로드・다운로드할 수 있는 장치 일체

□ 시험 세부항목

① 백업 파일 또는 여타 저장된 정보를 이용하여 이전의 정상 상태로 복구하는 기능이 정상 동작하는지 확인

□ 통과 기준

ㅇ 시험 세부항목 ①에서 이전 정상 상태로 복구되는 경우

□ 주의사항(추가사항)

ㅇ 없음

A.3.2 물리적 인터페이스 보호(SF_PP)

A.3.2.1 무선모듈 통제(SF_PP.1)

□ 시험 목적
- ㅇ 인가되지 않은 무선 접근을 제한하는 기능 확인

□ 준비사항
- ㅇ 공통 준비사항 참고

□ 시험 세부항목
① 무선 통신모듈에 대한 비활성화 설정이 동작하는지 확인

□ 통과 기준
- ㅇ 시험 세부항목 ①에서 무선 통신모듈이 정상적으로 비활성되는 경우

□ 주의사항(추가사항)
- ㅇ 시험대상에 무선 통신모듈이 사용되지 않는 경우 '통과'로 간주
- ㅇ 무선 통신만을 수행할 수 있는 시험대상의 경우 시험을 수행하지 않음

A.3.2.2 디버그 인터페이스 사용 제한(SF_PP.2)

□ 시험 목적
- ㅇ 디버그 인터페이스의 제거 또는 디버그 인터페이스의 사용을 제한하는 기능 확인

□ 준비사항
- ㅇ 공통 준비사항 이외의 피시험자의 제출사항
  - 통신 인터페이스 목록 및 용도에 대한 설명자료

□ 시험 세부항목
① 디버깅 등의 용도로 사용되는 인터페이스(예 : UART, JTAG 등)의 물리적인 제거 여부 확인
② 물리적인 인터페이스에 대해 이를 비활성하는 기능이 있는지 확인

□ 통과 기준
- ㅇ 시험 세부항목 ①에서 물리적인 제거가 확인되었거나, 또는 시험 세부항목 ②에서 이에 대한 비활성화가 수행되는 경우

□ 주의사항(추가사항)

ㅇ 없음

A.3.2.3 물리접근 탐지(SF_PP.3)

□ 시험 목적

ㅇ 인가되지 않은 물리적인 접근 시도를 탐지하는 기능 확인

□ 준비사항

ㅇ 공통 준비사항 이외의 피시험자의 제출사항

- 물리적인 접근 시도 탐지에 적용된 기술 및 동작 조건 설명자료

□ 시험 세부항목

① 물리적인 접근 시도를 탐지하는 기능(예 : 외부 함체를 이용하여 함체에 납봉인, 열쇠 잠금 장치 등)이 존재하는지 확인

□ 통과 기준

ㅇ 시험 세부항목 ①에 대해 탐지기능이 존재하는 경우

□ 주의사항(추가사항)

ㅇ 시험대상 자체가 탐지 기능을 제공하지 않더라도, 물리적으로 통제된 환경에 설치·운용되어야 함이 매뉴얼에 명시되어 있으면 '통과'로 간주

A.3.3 이벤트 대응(SF_RE)

A.3.3.1 통신장애 대응(SF_RE.1)

□ 시험 목적

ㅇ 네트워크 통신두절 발생 시 연결 초기화 모드 확인

□ 준비사항

ㅇ 공통 준비사항 이외의 피시험자의 제출사항

- 네트워크 연결 초기화 조건 및 초기화 시 동작 세부사항 설명서

□ 시험 세부항목

① 네트워크 통신두절 발생 시 입출력 대기상태 초기화 등 연결을 재설정하도록 되어 있는지 확인

□ 통과 기준

ㅇ 시험 세부항목 ①에서 통신두절 시 연결을 초기화하는 경우

□ 주의사항(추가사항)

ㅇ 시험대상에서 연결을 자동으로 재설정하지 않더라도, 관리자가 통신두절을 실시간으로 인지할 수 있고 수작업으로 재설정하는 방법을 매뉴얼을 통해 제시하는 경우 '통과'로 간주

ㅇ 대량의 트래픽 발생으로 인해 통신 연결 상태가 불안정한 경우 상위 시스템에 통보하는 것을 권고

A.4 보안기능 시험항목

□ 공통 준비사항(피시험자의 제출물)

ㅇ 시험대상

ㅇ 제품 매뉴얼, 사용자/관리자 매뉴얼 등 시험대상을 구매하는 고객에게 제공되는 문서

ㅇ 시험대상에서 직접 설정확인이 어려운 경우, 설정을 확인할 수 있는 별도의 장치 일체

A.4.1 보안 감사(SF_AU)

A.4.1.1 감사로그 생성(SF_AU.1)

□ 시험 목적

ㅇ 감사로그를 생성하는 기능 확인

□ 준비사항

ㅇ 공통 준비사항 이외의 피시험자의 제출사항

- 로그파일의 저장 위치 및 로그 확인방법 설명자료

□ 시험 세부항목

① 다음과 같은 중요 이벤트에 대해 감사로그가 생성되는지 확인

- 시험대상의 가동/중지
- 로그 생성기능의 시작/종료
- 식별·인증의 성공/실패
- 네트워크 및 보안 설정의 변경

② 감사로그에 기록된 각 이벤트가 다음과 같은 정보를 포함하는지 확인

- 이벤트 발생일시
- 이벤트 유형
- 이벤트 발생 주체

- 작업내역 및 결과(성공/실패)

□ 통과 기준

ㅇ 시험 세부항목 ①에서 모든 이벤트 유형에 대해 감사로그가 생성되고, ②에서 각 이벤트에 대해 명시된 정보가 모두 포함되어 있는 경우

□ 주의사항(추가사항)

ㅇ 스마트 현장장치에서 직접 감사로그 생성기능을 제공하지 않더라도, 상위 장치 등에서 시험항목에서 제시하는 모든 감사로그를 기록하는 것이 가능할 경우 '통과'로 간주

A.4.1.2 감사로그 포화 경고(SF_AU.2)

□ 시험 목적

ㅇ 저장된 로그의 용량이 사전 설정된 용량을 초과하는 경우 관리자에게 통보하는 기능 확인

□ 준비사항

ㅇ 공통 준비사항 이외의 피시험자의 제출사항

- 설정된 용량만큼 로그가 저장되어 있는 상태의 시험대상

□ 시험 세부항목

① 새로운 로그를 발생시켜 설정된 용량을 초과하게 한 후, 관리자가 이를 인지할 수 있게 통보(예 : 경고등 점등 등)가 이루어지는지 확인

□ 통과 기준

ㅇ 시험 세부항목 ①에서 사전 설정된 용량 초과 시 통보가 이루어지는 경우

□ 주의사항(추가사항)

ㅇ 스마트 현장장치의 특성으로 인해 저장용량이 매우 적게 할당되어 있는 경우, 다른 장치 또는 저장장치에 전송하여 기록하는 기능이 존재하고, 해당 기능이 정상적으로 동작하면 '통과'로 간주

ㅇ SF_AU.1 항목의 이벤트에 대한 로그기록을 스마트 현장장치와 연결된 다른 기기에서 저장하고 있는 경우 본 시험은 수행하지 않음

A.4.1.3 감사로그 전송(SF_AU.3)

□ 시험 목적

ㅇ 감사로그를 외부로 전송하는 기능 확인

□ 준비사항

ㅇ 공통 준비사항 참고

□ 시험 세부항목

① 백업기능 또는 여타 방식의 로그 전송기능(예 : syslog, Historian 등)을 통해 로그를 시험대상의 외부 시스템으로 전송할 수 있는지 확인

□ 통과 기준

ㅇ 시험 세부항목 ①에서 외부로 로그 전송을 수행할 수 있는 경우

□ 주의사항(추가사항)

ㅇ SF_AU.1 항목의 이벤트에 대한 로그를 스마트 현장장치와 연결된 다른 기기에서 저장하고 있는 경우 본 시험은 수행하지 않음

A.4.1.4 타임스탬프 사용(SF_AU.4)

□ 시험 목적

ㅇ 시각 동기화 기능 확인

□ 준비사항

ㅇ 공통 준비사항 이외의 피시험자의 제출사항

- 시각 동기화 방식에 대한 설명자료
- 시험대상에 시각 신호를 전송시킬 수 있는 시각 동기화 서버

□ 시험 세부항목

① 시각 동기화 서버와 연결하여 동기화 기능의 정상 작동 여부 확인

□ 통과 기준

ㅇ 시험 세부항목 ①에서 시각 동기화가 정상적으로 이루어지는 경우

□ 주의사항(추가사항)

ㅇ 시각 동기화 프로토콜(예 : NTP, PTP 등) 지원기능이 없더라도, 신뢰성 있는 자체 클럭을 보유하고 적정 주기로 수작업으로 시각을 보정해야 함을 매뉴얼에 명시할 경우 '통과'로 간주

A.4.1.5 감사로그 보호(SF_AU.5)

□ 시험 목적

ㅇ 로그를 위·변조, 무단 삭제 등으로부터 보호하는 기능 확인

□ 준비사항

ㅇ 공통 준비사항 참고

□ 시험 세부항목

① 감사로그에 기록된 이벤트의 수정 또는 무단 삭제 가능 여부 확인

② 전체 로그파일에 대해 무단 삭제 가능 여부 확인

□ 통과 기준

ㅇ 시험 세부항목 ①에서 이벤트의 수정 또는 삭제가 불가능하고, ②에서 전체 로그파일의 무단 삭제가 불가능한 경우

□ 주의사항(추가사항)

ㅇ 유일한 관리자 계정만이 시험대상에 접근할 수 있는 경우 관리자가 전체 로그파일을 삭제할 수 있더라도, 개별 이벤트의 수정/삭제가 불가하다면 '통과'로 간주

A.4.2 식별・인증(SF_IA)

A.4.2.1 사용자 식별・인증(SF_IA.1)

□ 시험 목적

ㅇ 유무선 네트워크를 통해 접근하는 사용자 신원에 대한 식별・인증 기능 확인

□ 준비사항

ㅇ 공통 준비사항 참고

□ 시험 세부항목

① 시험대상에 유무선 네트워크를 통해 접근하는 사용자의 신원을 식별・인증하는지 확인

□ 통과 기준

ㅇ 시험 세부항목 ①에서 사용자 식별・인증 기능 메커니즘(예 : 계정/패스워드, 보안토큰/패스워드 등)이 존재하는 경우

□ 주의사항(추가사항)

ㅇ 시험대상이 사용자 식별 기능을 제공하지 않는 경우, 인증 기능만 제공(예 : ID 입력 없이 패스워드만 입력)해도 '통과'로 간주

ㅇ 사용자 식별・인증 기능을 자체적으로 제공하지 않더라도 연동하는 시스템을 통해 사 사용자 식별・인증이 가능하고, 관련 내용이 매뉴얼에 명시되어 있는 경우 '통과'로 간주

A.4.2.2 장치 식별·인증(SF_IA.2)

□ 시험 목적

ㅇ 시험대상에 접속하는 각종 장치에 대한 식별·인증 기능 확인

□ 준비사항

ㅇ 공통 준비사항 이외의 피시험자의 제출사항

- 접속 장치에 대한 식별·인증 방식 설명자료
- 시험대상에 실제 접속을 수행할 수 있는 장치 일체

□ 시험 세부항목

① 접속하는 개별 장치를 유일하게 식별·인증하는지 확인

□ 통과 기준

ㅇ 시험 세부항목 ①에서 장치 식별·인증 기능이 정상적으로 수행되는 경우

□ 주의사항(추가사항)

ㅇ 명시적으로 인증 절차를 수행하지 않더라도, 식별값에 기반하여 비인가 장치를 차단할 수 있는 기능(예 : 화이트리스트 기반 접속차단 등)이 존재하는 경우 '통과'로 간주

A.4.2.3 패스워드 변경(SF_IA.3)

□ 시험 목적

ㅇ 패스워드가 하드코딩 되어 있지 않고 사용자가 패스워드를 변경할 수 있도록 지원하는 패스워드 관리기능 확인

□ 준비사항

ㅇ 공통 준비사항 참고

□ 시험 세부항목

① 패스워드가 하드코딩 되어 있지 않고, 사용자가 임의로 패스워드를 변경할 수 있도록 지원하는지 확인

② 패스워드 변경이 시험대상의 일시 중지, 재시작 등 운영에 영향을 초래하지 않는지 확인

□ 통과 기준

ㅇ 시험 세부항목 ①에서 패스워드가 하드코딩 되어 있지 않고, 변경이 가능하며 ②에서 패스워드 변경이 운영에 영향을 주지 않는 경우

□ 주의사항(추가사항)

ㅇ 초기 설치 시 주어지는 초기 패스워드를 변경하도록 강제 또는 안내하는 것을 권고함

A.4.2.4 복잡한 패스워드(SF_IA.4)

□ 시험 목적

ㅇ 복잡한 패스워드의 사용을 강제화할 수 있는 기능 확인

□ 준비사항

ㅇ 공통 준비사항 참고

□ 시험 세부항목

① 최소 6자리 이상의 복잡한 패스워드를 강제화할 수 있는지 확인

□ 통과 기준

ㅇ 시험 세부항목 ①에서 6자리 이상의 패스워드를 강제화하는 경우

□ 주의사항(추가사항)

ㅇ 영문 대/소문자, 숫자 및 특수문자의 조합을 강제화 권장

A.4.2.5 패스워드 보호(SF_IA.5)

□ 시험 목적

ㅇ 관리자 및 사용자 인증에 사용되는 패스워드 보호 기능 확인

□ 준비사항

ㅇ 공통 준비사항 이외의 피시험자의 제출사항

- 패스워드 파일의 저장 위치 및 확인방법 설명자료

□ 시험 세부항목

① 로그인 시 전송되는 패스워드를 암호화 또는 해독하기 어려운 방식으로 인코딩 하는지 확인

② 패스워드를 저장 시 암호화 또는 해독하기 어려운 방식으로 인코딩하는지 확인

③ 패스워드 입력 시 입력한 문자가 마스킹 처리되는지 여부 확인

□ 통과 기준

ㅇ 시험 세부항목 ① 및 ②에서 패스워드가 평문으로 전송 및 저장되지 않고, ③에서 입력 문자가 마스킹 처리되는 경우

□ 주의사항(추가사항)

ㅇ 패스워드를 암호화하여 전송 및 저장하는 것을 권고함

A.4.2.6 인증 실패 대응(SF_IA.6)

□ 시험 목적

ㅇ 일정 횟수의 인증 실패 반복 시 해당 계정을 차단하는 기능 확인

□ 준비사항

ㅇ 공통 준비사항 참고

□ 시험 세부항목

① 사용자 계정에 일정 횟수의 인증 실패 반복 시 계정 차단기능(예 : 일정시간 또는 관리자가 해제 시까지 계정 정지 등) 보유여부 확인

② 잘못된 패스워드 입력 시 제공되는 오류 메시지에서 공격에 사용될 수 있는 추가 정보(예 : “Invalid ID”, “Invalid Password” 등)의 포함 여부 확인

□ 통과 기준

ㅇ 시험 세부항목 ①에서 계정 차단기능이 있고, ②에서 공격에 사용될 수 있는 추가 정보가 포함되지 않는 경우

□ 주의사항(추가사항)

ㅇ 시험대상에 관리자 계정만 사용하고 사용자 계정을 지원하지 않는 경우 ‘통과’로 간주

ㅇ 산업제어시스템 가용성에 영향을 미치는 긴급한 상황에서의 조작을 위한 관리자 계정에 한해 계정 차단을 적용하지 않을 수 있음

A.4.2.7 PKI 인증서(SF_IA.7)

□ 시험 목적

ㅇ PKI 인증서 사용 시 안전한 표준절차 준용 여부 확인

□ 준비사항

ㅇ 공통 준비사항 참고

□ 시험 세부항목

① 사용되는 인증서가 [RFC] 5280에 따른 X.509 방식인지 확인

② 인증서를 통한 인증 시 인증서 유효기간 검증을 수행하는지 확인

③ RSA 키 길이가 2048비트 이상인지 확인

□ 통과 기준

ㅇ 시험 세부항목 ①에서 X.509 방식의 인증서를 사용하고, ②에서 인증서 유효기간 검증을 수행하며, ③에서 키 길이가 2048비트 이상인 경우

□ 주의사항(추가사항)

ㅇ ③에서 RSA 외의 알고리즘을 사용하는 경우에는 대칭키 기준 112비트 이상인지 확인

A.4.2 접근통제(SF_AC)

A.4.2.1 권한 분리(SF_AC.1)

□ 시험 목적

ㅇ 관리자, 일반 사용자 등 사용자에 따라 권한을 분리하는 기능 확인

□ 준비사항

ㅇ 공통 준비사항 참고

□ 시험 세부항목

① 관리자 모드와 일반 사용자 모드에 대해 접근가능한 메뉴, 명령어 등이 차등 적용되어 있는지 확인

□ 통과 기준

ㅇ 시험 세부항목 ①에서 일반 사용자로 로그인 시 관리기능에 접근이 불가능하도록 설정되어 있는 경우

□ 주의사항(추가사항)

ㅇ 사용자 계정 생성 시 기본적으로 최소한의 권한만 부여하거나 역할에 기반하여 사용자별 권한을 자동 부여하는 메커니즘의 적용 권장

A.4.2.2 접근제한(SF_AC.2)

□ 시험 목적

ㅇ 시험대상과 연결되는 장치에 대해 관리자의 정책에 따라 해당 장치/프로세스에 대한 접근을 제한하는 기능 확인

□ 준비사항

ㅇ 공통 준비사항 참고

□ 시험 세부항목

① 장치별 접근을 차단하는 기능이 정상적으로 동작하는지 확인

□ 통과 기준

ㅇ 시험 세부항목 ①에서 장치별 접근제한이 이루어지는 경우

□ 주의사항(추가사항)

ㅇ 시험대상에 장치별 접근차단 기능이 없더라도 운영환경(예 : 방화벽 등)의 지원을 받아 차단할 수 있고 이를 매뉴얼에 명시하는 경우 '통과'로 간주

A.4.2.3 관리자 세션 잠금(SF_AC.3)

□ 시험 목적

ㅇ 일정시간 동안 입력이 없는 관리자 로그인 세션에 대해 자동으로 잠금 또는 종료가 이루어지는 기능 확인

□ 준비사항

ㅇ 공통 준비사항 참고

□ 시험 세부항목

① 일정시간 경과 후 관리자 세션을 잠금 또는 종료하는지 확인

□ 통과 기준

ㅇ 시험 세부항목 ①에서 일정시간 경과 후 관리자 세션의 잠금 또는 종료가 이루어지는 경우

□ 주의사항(추가사항)

ㅇ 없음

A.4.2.4 동시 세션 제한(SF_AC.4)

□ 시험 목적

ㅇ 동시에 접속할 수 있는 관리자 세션 수를 제한하는 기능 확인

□ 준비사항

ㅇ 공통 준비사항 참고

□ 시험 세부항목

① 최대 허용 세션 수가 제한되어 있고 최대 세션 수를 초과하는 관리자 세션에 대해는 연결이 거부되는지 확인

□ 통과 기준

ㅇ 시험 세부항목 ①에서 추가적인 세션 생성이 거부되는 경우

□ 주의사항(추가사항)

ㅇ 없음

A.4.3 전송 데이터 보호(SF_SC)

A.4.3.1 전송 데이터 무결성(SF_SC.1)

□ 시험 목적

ㅇ 민감한 전송 데이터의 무결성 보장 기능 확인

□ 준비사항

ㅇ 공통 준비사항 참고

□ 시험 세부항목

① 다음의 전송 데이터에 대해 위·변조를 방지할 수 있는 메커니즘(예 : 암호화된 해시값, 전자서명 등)이 구현되어 있는지 확인

- 제어명령
- 현장장치 상태정보

② 다음의 전송 데이터에 대해 재사용 공격에 대비하여 데이터의 최신성을 확인할 수 있는 수단(예 : 난수, 타임스탬프, 챌린지-리스폰스 등)을 사용하고 있는지 확인

- 제어명령
- 현장장치 상태정보

□ 통과 기준

ㅇ 시험 세부항목 ①에서 위·변조 방지 메커니즘이 구현되어 있고, 시험 세부항목 ②에서 최신성 확인 수단을 사용하고 있는 경우

□ 주의사항(추가사항)

ㅇ 없음

A.4.3.2 전송 데이터 기밀성(SF_SC.2)

□ 시험 목적

ㅇ 전송 데이터의 기밀성 보장 기능 확인

□ 준비사항

ㅇ 공통 준비사항 참고

□ 시험 세부항목

① 다음의 민감 정보를 암호화 또는 해독하기 어려운 방식으로 인코딩하여 전송하는지 확인

- 제어명령
- 상태정보

□ 통과 기준

ㅇ 시험 세부항목 ①에서 민감한 정보를 평문으로 전송하지 않는 경우

□ 주의사항(추가사항)

ㅇ 암호화 관련 사항은 SF_SF.2 및 SF_SF.3 참조

ㅇ 민감한 정보를 암호화하여 전송하는 것을 권고함

A.4.3.3 통신세션 자동 종료(SF_SC.3)

□ 시험 목적

ㅇ 일대일 통신세션에 대한 자동 종료 기능 확인

□ 준비사항

ㅇ 공통 준비사항 참고

□ 시험 세부항목

① 사용목적을 달성한 세션의 종료 여부 확인

② 사전 설정된 접속시간을 초과한 세션의 종료 여부 확인

③ 사전 설정된 유휴시간을 초과하여 미사용중인 세션의 종료 여부 확인

□ 통과 기준

ㅇ 시험 세부항목 ① ~ ③에서 모두 세션을 종료하는 경우

□ 주의사항(추가사항)

ㅇ 없음

A.4.3.4 멀티캐스트/브로드캐스트 통신 관리(SF_SC.4)

□ 시험 목적

ㅇ 멀티캐스트 통신과 브로드캐스트 통신의 제한 여부 확인

□ 준비사항

ㅇ 공통 준비사항 참고

□ 시험 세부항목

① 멀티캐스트/브로드캐스트 통신 기능을 비활성화할 수 있는지 확인

② 멀티캐스트/브로드캐스트 통신에 대한 진원지 및 무결성 검증이 가능하고, 인가된 장치로 수신을 제한할 수 있는지 확인

□ 통과 기준

ㅇ 시험 세부항목 ①에서 멀티캐스트/브로드캐스트 통신을 비활성화할 수 있거나, 멀티캐스트/브로드캐스트 통신을 지원하지 않고, ②에서 진원지 및 무결성 검증 기능을 제공하고 인가된 장치로 수신을 제한할 수 있는 경우

□ 주의사항(추가사항)

ㅇ 멀티캐스트/브로드캐스트 통신 이용에 대한 주의사항에 대해 매뉴얼에 명시하고 있는 경우, '통과'로 간주

A.4.4 저장 데이터 보호(SF_DP)

A.4.4.1 잔여정보 보호(SF_DP.1)

□ 시험 목적

ㅇ 수리, 불용처리 등으로 외부 반출 사유 발생 시 저장된 민감한 정보를 삭제하는 기능 확인

□ 준비사항

ㅇ 공통 준비사항 참고

□ 시험 세부항목

① 잔여 정보를 모두 삭제하는 기능(예 : 공장 초기화)을 통해 다음과 같은 민감 정보가 삭제되는지 확인

- 계정/패스워드 정보
- 감사로그
- 네트워크 및 보안 설정
- 개인키, 공개키, 시드 등 암호연산에 사용되는 정보(존재하는 경우)

□ 통과 기준

ㅇ 시험 세부항목 ①에서 모든 민감 정보에 대해 삭제가 이루어지는 경우

□ 주의사항(추가사항)

ㅇ 잔여정보 삭제기능을 직접 제공하지 않더라도, 매뉴얼을 통해 수동으로 삭제하는 방법을 제시하는 경우 '통과'로 간주

A.4.4.2 저장 데이터 기밀성(SF_DP.2)

□ 시험 목적

ㅇ 시험대상에 민감 데이터를 평문으로 저장하지 않도록 하는 기능 확인

□ 준비사항

ㅇ 공통 준비사항 이외의 피시험자의 제출사항

- 저장 데이터에 대한 기밀성 보장 메커니즘 설명자료

□ 시험 세부항목

① 다음의 민감 정보를 암호화 또는 해독하기 어려운 방식으로 인코딩하여 저장하는지 확인

- 감사로그
- 네트워크 및 보안 설정

□ 통과 기준

ㅇ 시험 세부항목 ①에서 민감한 정보를 평문으로 저장하지 않는 경우

□ 주의사항(추가사항)

ㅇ 암호화 관련 사항은 SF_SF.2 및 SF_SF.3 참조

ㅇ 민감한 정보를 암호화하여 저장하는 것을 권고함

A.4.4.4 저장 데이터 무결성(SF_DP.3)

□ 시험 목적

ㅇ 시험대상에 민감 데이터 저장 시 무결성 보장 기능 확인

□ 준비사항

ㅇ 공통 준비사항 참고

□ 시험 세부항목

① 다음의 민감 정보에 대해 위·변조를 방지할 수 있는 메커니즘(예 : 암호화된 해시값, 전자서명 등)이 구현되어 있는지 확인

- 감사로그
- 네트워크 및 보안 설정

□ 통과 기준

ㅇ 시험 세부항목 ①에서 위·변조 방지 메커니즘이 구현되어 있는 경우

□ 주의사항(추가사항)

ㅇ 없음

A.4.5 보안기능 관리(SF_SF)

A.4.5.1 네트워크 및 보안 설정관리(SF_SF.1)

□ 시험 목적

ㅇ 네트워크 및 보안 설정에 대한 조회 및 변경 기능 확인

□ 준비사항

ㅇ 공통 준비사항 참고

□ 시험 세부항목

① 네트워크 및 보안 설정(예 : 네트워크 조인키)에 대한 조회 및 변경이 가능한지 확인

□ 통과 기준

ㅇ 시험 세부항목 ①에서 조회 및 변경이 정상적으로 이루어지는 경우

□ 주의사항(추가사항)

ㅇ 없음

A.4.5.2 암호연산 (SF_SF.2)

□ 시험 목적

ㅇ 암호연산 시 안전한 암호 알고리즘이 사용되는지 확인

□ 준비사항

ㅇ 공통 준비사항 이외의 피시험자의 제출사항

- 사용되는 암호 알고리즘, 운영모드, 키 길이 등에 대한 설명서
- 시험대상에 사용되는 암호모듈의 안전성에 대해 국내·외 전문기관이 발급한 공인 시험성적서 또는 인증서(보유 시)

□ 시험 세부항목

① 안전한 암호 알고리즘, 운영모드 및 키 길이를 사용하고 있는지 확인

□ 통과 기준

ㅇ 시험 세부항목 ①에서 암호문의 해독 또는 위·변조가 가능한 심각한 취약점이 공개되지 않은 안전한 암호 알고리즘 및 운영모드를 사용하고, 키 길이가 대칭키 기준 112 bit 이상의 비도를 가지는 경우

□ 주의사항(추가사항)

ㅇ 본 시험항목은 시험대상에 암호연산이 사용되는 경우에만 적용

ㅇ 시험대상의 운영환경 또는 특수성에 따라 키 길이가 112 bit 미만인 경우, 피시험자와 협의하여 통과 여부를 결정

A.4.5.3 암호키 관리(SF_SF.3)

□ 시험 목적

ㅇ 암호연산에 사용되는 암호키가 안전하게 관리되는지 확인

□ 준비사항

ㅇ 공통 준비사항 이외의 피시험자의 제출사항

- 암호키 생성/설정/저장/파기 방법에 대한 설명서
- 시험대상에 사용되는 암호모듈의 안전성에 대해 국내·외 전문기관이 발급한 공인 시험성적서 또는 인증서(보유 시)

□ 시험 세부항목

① 암호키의 생성/설정을 위해 공신력 있는 표준방식(예 : 국내·외 암호모듈 검증제도에서 허용하는 방식 등)을 채택하고 있는지 확인

② 개인키, 시드 등 암호연산에 사용되는 민감 정보에 대해 인가되지 않은 접근을 방지할 수 있는 보호대책(예 : 암호화, 물리적/논리적으로 안전한 장소에 보관 등)을 구비하고 있는지 확인

③ 개인키, 시드 등 암호연산에 사용되는 민감 정보를 세션 종료 후 메모리에서 반환(제로화)하는 기능을 보유하고 있는지 확인

□ 통과 기준

ㅇ 시험 세부항목 ①에서 공신력 있는 키 생성/설정 방식을 사용하고, ②에서 접근방지 보호대책을 구비하고 있으며, ③에서 제로화 하는 기능이 존재하는 경우

□ 주의사항(추가사항)

ㅇ 시험대상에 암호연산이 사용되지 않는 경우 본 시험을 수행하지 않음

ㅇ 시험대상의 운영환경 또는 특수성에 따라 표준방식이 아닌 자체적으로 고안한 방식으로 암호키를 생성/설정하는 경우, 시험기관과 협의하여 추가적인 문서검토 및 시험 실시

ㅇ 암호연산에 사용되는 민감 정보가 별도의 안전한 모듈에서 호출되어 사용되는 경우 제로화 기능이 없더라도 '통과'로 간주

A.4.6 상태 관리 (SF_SS)

A.4.6.1 실행코드 무결성(SF_SS.1)

□ 시험 목적

ㅇ 실행코드에 대한 무결성 검증 기능 확인

□ 준비사항

ㅇ 공통 준비사항 이외의 피시험자의 제출사항

- 실행코드에 대한 무결성 검증 메커니즘 설명자료

□ 시험 세부항목

① 실행코드의 변조를 식별 또는 방지할 수 있는 메커니즘(예 : 체크섬, 해시값, 코드 사인 등)이 정상 동작하는지 확인

□ 통과 기준

ㅇ 시험 세부항목 ①에서 변조된 실행코드를 식별하거나 설치 또는 실행되지 않도록 차단하는 기능이 정상 동작하는 경우

□ 주의사항(추가사항)

ㅇ 무결성 검증 메커니즘이 자동화된 방식으로 구현되어 있지 않더라도 수작업 확인 방법을 매뉴얼을 통해 제시하는 경우 '통과'로 간주

ㅇ 네트워크 및 보안 설정에 대해서도 무결성 검증 메커니즘 적용 권고

A.4.6.2 자체시험(SF_SS.2)

□ 시험 목적

ㅇ 주요 기능이 정상적으로 동작되는지 확인을 위한 자체시험 기능 확인

□ 준비사항

ㅇ 공통 준비사항 이외의 피시험자의 제출사항

- 자체시험의 대상/방식/시점 등에 대한 설명자료

□ 시험 세부항목

① 자체시험 시 다음과 같은 중요사항에 대해 테스트를 수행하는지 확인

- 식별·인증 관련 프로세스의 정상 구동 여부

- 감사로그 생성 관련 프로세스의 정상 구동 여부
- 제어 관련 필수 서비스의 정상 구동 여부
- 설정 파일에 대한 무결성 유지 여부

② 가동 시 뿐 아니라 관리자의 요청에 따라 임의의 시점에서 자체시험을 수행할 수 있는지 확인

□ 통과 기준

ㅇ 시험 세부항목 ①에서 각 사항에 대한 테스트가 수행되고, 시험 세부항목 ②에서 관리자가 설정한 시점에 테스트 수행이 가능한 경우

□ 주의사항(추가사항)

ㅇ 없음

A.4.6.3 펌웨어 무결성(SF_SS.3)

□ 시험 목적

ㅇ 펌웨어의 무결성을 검증할 수 있는 기능 확인

□ 준비사항

ㅇ 공통 준비사항 이외의 피시험자의 제출사항
- 펌웨어 무결성 검증 방법 및 절차에 대한 설명서

□ 시험 세부항목

① 펌웨어의 위·변조를 식별할 수 있는 안전한 기술적 방법(예 : 코드사인 등)이 사용되고 있는지 확인

② 무결성 훼손 시 펌웨어 업데이트가 불가능하도록 되어 있는지 확인

□ 통과 기준

ㅇ 시험 세부항목 ①에서 심각한 취약점이 공개되지 않은 안전한 암호 알고리즘을 사용하고, ②에서 무결성이 훼손된 펌웨어의 설치가 불가능하도록 되어 있는 경우

□ 주의사항(추가사항)

ㅇ 없음

A.4.6.4 쓰기 보호(SF_SS.4)

□ 시험 목적

ㅇ 시험 대상 운전 중 메모리 쓰기/수정을 방지하는 기능 확인

□ 준비사항

ㅇ 공통 준비사항 참고

□ 시험 세부항목

① 시험 대상의 운전 모드 상태에서 메모리 쓰기/수정을 방지하는 메커니즘의 지원 여부 확인

□ 통과 기준

ㅇ 시험 세부항목 ①에서 메모리 쓰기/수정을 방지하는 메커니즘을 지원하는 경우

□ 주의사항(추가사항)

ㅇ 쓰기 보호 메커니즘이 On/Off 가능한 기능으로 제공되는 경우 On으로 설정하기를 권고함

A.4.6.5 예정된 출력(SF_SS.5)

□ 시험 목적

ㅇ 정상 작동이 불가능한 경우 정해진 출력을 유지하는 기능 확인

□ 준비사항

ㅇ 공통 준비사항 참고

□ 시험 세부항목

① 시험 대상이 정상 작동할 수 없는 상황에서의 출력 상태를 다음 중 하나로 지정 가능 여부 확인

- 전원 꺼짐 상태 출력 (Unpowered)
- 최근 정상 출력 상태 유지 (Hold)
- 정해진 값 출력 (Fixed)

□ 통과 기준

ㅇ 시험 세부항목 ①에서 출력 상태를 지정할 수 있는 경우

□ 주의사항(추가사항)

ㅇ 정상 작동 불가 상황에서의 출력 상태를 사용자가 지정할 수 없으나 관련 문서에 정해진 출력 상태가 기술되어 있는 경우 '통과'로 간주

A.4.6.6 취약점 대응(SF_SS.6)

□ 시험 목적

ㅇ 알려진 취약점에 대한 보안조치 여부 확인

□ 준비사항

ㅇ 공통 준비사항 이외의 피시험자의 제출사항

- 알려진 취약점에 대한 조치사항 기술서

□ 시험 세부항목

① 시험대상 자체의 알려진 취약점 또는 유사 제품을 통해 공개된 공통적인 취약점에 대해 피시험자가 조치를 하였는지 조치사항 기술서 확인

② 침투테스트를 통해 기존 알려진 주요 취약점에 대한 조치 여부 및 최신 제로데이 취약점의 존재 여부 확인

□ 통과 기준

ㅇ 시험 세부항목 ①에서 모든 취약점에 대해 조치되었거나 조치 계획이 있음을 확인하고, ②에서 침투테스트 시 취약점이 발견되지 않은 경우

□ 주의사항(추가사항)

ㅇ 피시험자는 CVE(https://cve.mitre.org), CWE(https://cwe.mitre.org), ICS-CERT (https://ics-cert.us-cert.gov/advisories) 등에 제시된 취약점 목록에 대해 취약점 조치 및 조치사항 기술서 작성

ㅇ 시험 세부항목 ①에서 조치 계획을 제출하는 경우에는 조치 일정에 대한 협의가 이루어져야 하며, 협의된 일정 내에 취약점 조치 여부를 확인해야 함

부 록 Ⅰ-1

(본 부록은 표준을 보충하기 위한 내용으로 표준의 일부는 아님)

지식재산권 확약서 정보

해당 사항 없음

※ 상기 기재된 지식재산권 확약서 이외에도 본 표준이 발간된 후 접수된 확약서가 있을 수 있으니, TTA 웹사이트에서 확인하시기 바랍니다.

부 록 Ⅰ-2

(본 부록은 표준을 보충하기 위한 내용으로 표준의 일부는 아님)

시험인증 관련 사항

Ⅰ-2.1 시험인증 대상 여부

본 표준의 2부 ~ 4부에서 기술하고 있는 3가지 계층으로 구분해서 시험인증을 실시할 계획이 있음

Ⅰ-2.2 시험표준 제정 현황

다음과 같이 본 표준의 2부 ~ 4부에서 시험항목을 기술하고 있음

- '산업제어시스템 보안요구사항 - 2부: 현장장치 계층'의 부속서 A 현장장치 계층 보안요구사항 시험 방법
- '산업제어시스템 보안요구사항 - 3부: 제어 계층'의 부속서 A 제어 계층 보안요구사항 시험 방법
- '산업제어시스템 보안요구사항 - 4부: 운영 계층'의 부속서 A 운영 계층 보안요구사항 시험 방법

부 록 Ⅰ-3

(본 부록은 표준을 보충하기 위한 내용으로 표준의 일부는 아님)

본 표준의 연계(family) 표준

Ⅰ-3.1 산업제어시스템 보안요구사항 - 1부: 개념 및 참조모델

산업제어시스템 보안요구사항을 정의하기 위해서 산업제어시스템 보안개념과 보안참조모델을 정의하고 있으며, '산업제어시스템 보안요구사항 - 2부: 현장장치 계층'는 1부에서 정의된 보안개념과 보안참조모델을 고려하여 산업제어시스템을 구성하는 3계층 가운데 현장장치 계층에 위치하는 산업제어 시스템 구성요소들에 대한 보안요구사항을 정의하고 있음

Ⅰ-3.2 산업제어시스템 보안요구사항 - 3부: 제어 계층

1부에서 정의된 보안개념과 보안참조모델을 고려하여 산업제어시스템을 구성하는 3계층 가운데 제어 계층에 위치하는 산업제어 시스템 구성요소들에 대한 보안요구사항을 정의하고 있음

Ⅰ-3.3 산업제어시스템 보안요구사항 - 4부: 운영 계층

1부에서 정의된 보안개념과 보안참조모델을 고려하여 산업제어시스템을 구성하는 3계층 가운데 운영 계층에 위치하는 산업제어 시스템 구성요소들에 대한 보안요구사항을 정의하고 있음

부 록 Ⅰ-4

(본 부록은 표준을 보충하기 위한 내용으로 표준의 일부는 아님)

참고 문헌

해당 사항 없음

부 록 Ⅰ-5

(본 부록은 표준을 보충하기 위한 내용으로 표준의 일부는 아님)

영문표준 해설서

해당 사항 없음

부 록 Ⅰ-6

(본 부록은 표준을 보충하기 위한 내용으로 표준의 일부는 아님)

표준의 이력

판수	채택일	표준번호	내용	담당 위원회
제1판	2017.03.21.	제정 TTAx.xx-xx.xxxx	-	응용보안/평가인증PG (PG504)