TTA Standard

정보통신단체표준(국문표준)

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

산업제어시스템 보안요구사항 - 1부: 개념 및 참조모델

Security Requirements for Industrial Control System - Part 1: Concepts and Reference Model

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 산업제어시스템의 보안요구사항을 정의하는데 있다. 산업제어시스템은 현장장치 계층, 제어 계층, 운영 계층 등 3계층으로 구성된다. 본 표준의 1부에서는 산업제어시스템 보안요구사항을 정의하는데 필요한 보안개념과 보안참조모델을 기술한다. 2부에서는 현장장치 계층에 적용되는 보안요구사항을 정의하고, 3부에서는 제어 계층에 적용되는 보안요구사항을 정의한다. 4부에서는 운영 계층에 적용되는 보안요구사항을 정의한다.

2 주요 내용 요약

산업제어시스템은 운영 계층, 제어 계층, 현장장치 계층 등 3계층으로 구성된다. 본 표준에서는 산업제어시스템을 구성하는 각 계층에 적용되는 보안요구사항을 정의하기 위해서 필요한 보안개념과 보안참조모델을 기술한다. 산업제어시스템은 IT 시스템과 비교하여 가용성의 중요도가 매우 높다. 본 표준에서는 이와 같은 산업제어시스템의 특징을 반영하여 산업제어시스템 보안개념과 보안참조모델을 정의한다.

3 인용 표준과의 비교

- 해당 사항 없음

Preface

1 Purpose

This standard is to define security requirements for ICS (Industrial Control System). ICS is consist of 3 layers – Field Device layer, Control layer and Operational layer. Part 1 describes the security concepts and the security reference model of ICS to define security requirements for ICS. Part 2 defines security requirements for Field Device layer, part 3 defines security requirements for Control layer. And part 4 defines security requirements for Operationa lyer.

2 Summary

ICS is consist of 3 layers – Operation layer, Control layer and Field Device layer. The standard is to define the security concepts and the security reference model of ICS and the security concepts and the security reference model of ICS will be used to define security requirements of ICS layers. Compared to IT system, the priority of availability requirements is very high. The standard defines ICS security concept and security reference model taking in consideration the characteristics of ICS

3 Relationship to Reference Standards

N/A

목 차

산업제어시스템 보안요구사항 - 1부: 개념 및 참조모델 (Security Requirements for Industrial Control System - Part 1: Concepts and Reference Model)

1 적용 범위

1.1. 표준 범위

본 표준에서는 산업제어시스템의 보안요구사항을 정의한다. 보안요구사항은 외부 위협 및 내부 정보 유출 위협 등에 대응하기 위해 필요하다. 산업제어시스템은 운영 계층, 제어 계층, 현장장치 계층 등 3계층으로 구분할 수 있는데, 본 표준에서는 각 계층별로 적용되는 보안요구사항을 정의한다.

1.2. 표준 구성

본 표준은 총 4부로 구성되어 있다. 1부에서는 산업제어시스템 보안개념과 보안참조모델을 정의하며, 2 ~ 4부는 1부에서 정의한 보안개념과 보안참조모델을 고려하여 다음과 같이 각 계층별로 보안요구사항을 정의한다.

산업제어시스템 보안요구사항 - 2부: 현장장치 계층
산업제어시스템 보안요구사항 - 3부: 제어 계층
산업제어시스템 보안요구사항 - 4부: 운영 계층

2 인용 표준

해당 사항 없음

3 용어 정의

3.1. 스마트 현장장치
연산 및 통신 기능을 제공하는 현장장치

3.2. 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

3.3. 제어 S/W

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

3.4. 현장장치

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

3.5. 히스토리안(Historian)

Operational Historian이라고도 하며, 공정 데이터, 알람, 운전원 이벤트 등의 정보를 시간 순으로 저장・관리하는 데이터베이스 기능의 프로그램

3.6. hard wired

제어시스템의 연결 방법 가운데 구리선을 이용한 연결 방법

4 약어

DCS	Distributed Control System
DNP	Distributed Network Protocol
EWS	Engineering Workstation
HMI	Human Machine Interface
ICS	Industrial Control System
IED	Intelligent Electronic Device
PLC	Programmable Logic Controller
RTU	Remote Terminal Unit

5 산업제어시스템 보안 개념

5.1. 산업제어시스템 개요

산업제어시스템이란 전력, 가스, 상하수도, 원자력, 운송, 제조 등의 산업 현장을 모니터링하고 제어하는데 사용되는 시스템을 의미한다. 산업제어시스템은 물리적 장치의 상태를 계측・모니터링하고 물리적 장치를 직접 제어한다. 따라서 산업제어시스템이 사이버 공격을 받게 되면 물리적 피해를 유발하게 되며 특히 사람의 안전과 환경에 영향을 끼칠 수 있다.

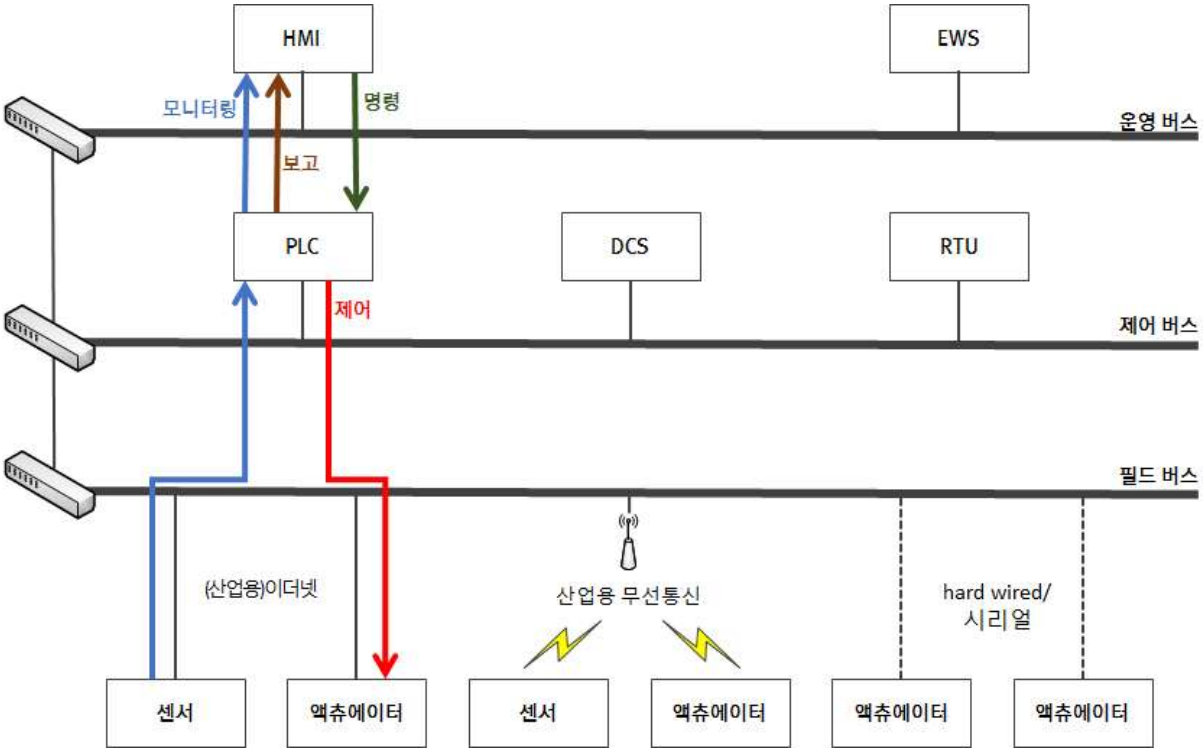
이와 같은 산업제어시스템은 일반적으로 발전소, 가스 생상・공급 기지, 댐 등 국가・사회 운영에 있어서 필수적인 기능을 제공하는 기반시설에서 사용된다. 따라서 산업제어시스템이 사이버공격을 받을 경우 국가・사회 기능이 마비되는 등 피해 규모가 매우 큰 경

우가 대부분이다.

일반적인 산업제어시스템 네트워크 구성 및 서비스 시나리오는 (그림 4-1)과 같다. 센서, 액츄에이터 등의 현장장치는 유무선 랜, 시리얼 케이블 또는 구리선에 의한 hard wired 방법 등을 통해 PLC, DCS, RTU 등 제어 H/W와 연결되며, 제어 H/W는 (산업용) 이더넷 또는 시리얼 케이블을 통해 제어 S/W와 연결된다.

(그림 4-1)에서 제어 H/W는 센서를 통해 수집된 압력, 온도 등의 현장장치 상태 데이터를 취합하여 제어 S/W로 전송하며, 사용자는 HMI 등 제어 S/W를 이용해서 취합된 현장 데이터를 모니터링 함으로써 현장장치의 상태를 확인할 수 있다. 현장에 설치된 밸브의 개폐 등 액츄에이터의 제어가 필요한 경우, 사용자는 HMI 등 제어 S/W를 이용해서 제어 명령을 입력할 수 있다. 사용자가 입력한 제어 명령은 제어 H/W에게 전달되며, 제어 H/W는 제어명령에 따라 현장장치를 제어한다. 또한 제어 H/W는 이상 상황 또는 설정된 이벤트가 발생한 경우에는 제어 S/W에 보고(알람)를 통해 해당 상황을 알릴 수 있다. 이와 같은 명령, 제어, 보고, 모니터링을 산업제어시스템의 필수 서비스로 정의할 수 있다.

한편, 제어 S/W 가운데 EWS는 제어 H/W에 사용되는 제어로직을 개발하여 제어 H/W에 설치하는 기능을 제공한다. 따라서 EWS는 산업제어시스템 필수 서비스를 직접 제공하지는 않지만, 제어 S/W로 분류할 수 있다.



(그림 4-1) 산업제어시스템 네트워크 구성 및 서비스 시나리오

(그림 4-1)은 산업제어시스템 단일 네트워크 구성만을 나타낸 것이다. 산업제어시스템

네트워크는 다른 네트워크와 연결되어 확장된 산업제어시스템 네트워크를 구성할 수 있다.

5.2. 산업제어시스템 특징

산업제어시스템에서는 IT 시스템에 비해서 운영의 연속성이 매우 중요하다. 예기치 않은 산업제어시스템의 운영 중단은 IT 시스템과는 비교할 수 없는 큰 피해를 일으킬 수 있기 때문이다. 따라서 산업제어시스템의 유지·보수는 일반적으로 사전에 계획되고 운영에 끼치는 영향 분석이 완료된 후에 이루어지는 것이 일반적이다. 그러나 산업제어시스템에서 사이버보안 사고에 의한 피해가 발생하더라도 운영은 지속되어야 한다. 즉, 산업제어시스템의 경우 사이버공격에 의한 피해가 탐지된다고 하더라도 IT 시스템과 같이 탐지 즉시 시스템을 중단하고 사고조사 및 대응을 수행할 수 없음을 의미한다.
일반적으로 IT 시스템에서는 정보의 기밀성 유지가 높은 우선순위를 갖는 요구사항이라고 한다면, 산업제어시스템에서는 가용성이 가장 높은 우선순위의 요구사항이다. 산업제어시스템을 관리 및 운영하는데 있어서 지연 또는 중단이 발생하지 않도록 운영 환경을 유지하는 것이 중요하며, 산업제어시스템의 핵심 기능이 제어 기능 유지를 위해서 다른 기능을 일시적으로 제공하지 않는 상황이 발생할 수도 있다. IT시스템과 비교하여 산업제어시스템의 특징을 살펴보면 <표 4-1>과 같다.

<표 4-1> IT 시스템과 산업제어시스템의 특성 비교

항목	IT 시스템	산업제어시스템
하드웨어 및 소프트웨어	짧은 교체 주기 (3 ~ 5년)	장기간의 교체 주기 (15 ~ 20년)
	다양한 애플리케이션 및 범용 프로토콜 사용	전용 애플리케이션 및 비공개 전용 프로토콜(제어 프로토콜) 사용
	패치 등 유지·보수가 용이	패치 등 유지·보수가 어려움
	범용 OS 사용 (윈도우, 리눅스 등)	전용 OS/ 실시간 OS 사용
네트워크 성능 요구사항	전체 성능(throughput)에 초점	견고성 및 실시간 요구사항 중시
	응답의 신뢰성이 중요하며 일부 통신 지연 허용	응답 시간이 중요하며 통신 지연 불허
위험관리 목표	데이터의 무결성 중요	인간의 안전 및 시스템 가용성 중요
	일부 고장 및 장애 허용	운전 정지가 허용되지 않음
사고 영향	사고 발생 시 업무 불편 및 지연 등 상대적으로 미미한 경제적 피해 발생	사고 발생 시 산업현장 운영 중단으로 인한 인명 피해 및 대규모 물리적·경제적 피해 발생
정보보호 우선순위	기밀성 > 무결성 > 가용성	가용성 > 무결성 > 기밀성

5.3. 산업제어시스템 보안원칙

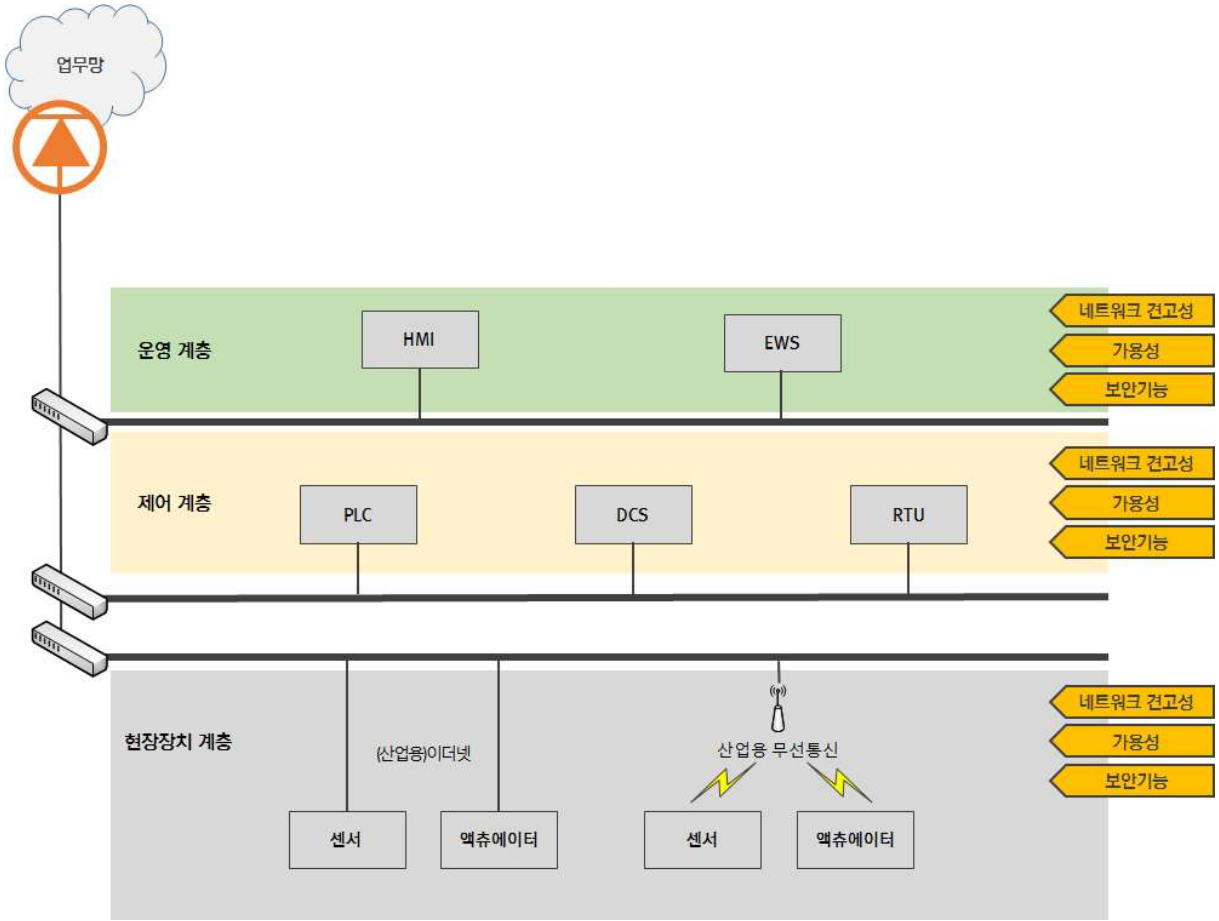
가용성의 우선순위가 높은 특성을 고려하여 산업제어시스템은 다음과 같은 보안원칙에 따라 보안요구사항을 만족시켜야 한다.

네트워크 견고성: 산업제어시스템 구성요소는 비정상적인 통신 데이터 및 과도한 양의 통신 데이터가 유입되는 경우에도 명령, 제어, 보고, 모니터링 등 산업제어시스템 필수 서비스를 제공해야 한다.

서비스 지속성: 산업제어시스템 구성요소는 업무 연속성 확보를 위한 기능을 제공해야 한다. 이는 전원, 저장장치 등 산업제어시스템이 사용하는 자원의 가용성 확보와 물리적인 공격에 대한 보호 기능 등을 포함한다.
보안기능: 식별・인증, 접근통제, 전송 및 저장 데이터 보호 등 산업제어시스템 구성요소의 보안성 확보를 위한 보안기능을 제공해야 한다.

6 산업제어시스템 보안참조모델

(그림 5-1)은 산업제어시스템 보안참조모델이다. 산업제어시스템은 운영 계층, 제어 계층, 현장장치 계층 등 3 계층으로 구성된다.



(그림 5-1) 산업제어시스템 보안참조모델

운영 계층은 제어 계층으로부터 전달 받은 데이터를 통해 현장장치 상태를 모니터링하거나 제어 명령을 전송하는 역할을 하며, HMI, EWS 등을 포함한다. 히스토리안, 관리콘솔, 백신관리서버 등 산업제어시스템을 관리·운영하는데 필요한 IT 요소들도 이 계층에 위치하나, 현장장치 계층과 제어 계층에 포함되는 현장장치와 제어 H/W 제어하는데 직접 사용되지 않기 때문에 산업제어시스템 보안참조모델의 구성요소로 분류하지는 않는다.

제어 계층은 현장장치에서 계측·수집한 데이터를 모니터링 계층으로 전달하거나 모니터링 계층의 제어 명령을 받아 현장장치를 제어하는 역할을 수행한다. PLC, DCS, RTU 등의 제어 H/W가 이 계층에 포함된다. 또한 제어 계층에서 데이터를 주고받거나, 제어 계층과 모니터링과의 통신에는 산업제어 전용 프로토콜이 사용된다. 이와 같은 산업제어 프로토콜은 앞서 <표 4-1>에서 기술한 네트워크 성능 요구사항을 만족시키는 특성을 갖고 있다. 대표적인 산업제어 프로토콜로는 DNP, MODBUS, Ethernet/IP 등이 있다.

마지막으로 현장장치 계층에는 센서, 액츄에이터 등의 상태 데이터를 계측·수집하거나 제어하는데 사용되는 현장장치가 포함된다. 현장장치는 제어 계층과 유무선 랜, 시리얼 케이블, 구리선에 의한 hard wired 방법 등으로 연결된다.

산업제어시스템을 구성하는 각 계층은 계층 별로 네트워크 견고성, 서비스 지속성, 보안기능 등 산업제어시스템 보안원칙을 제공한다. 즉, 각 계층에서 준수하는 보안원칙은 서로 독립적으로 어느 한 계층의 보안원칙이 다른 계층의 보안원칙에 영향을 주지 않는다. 보안원칙을 제공하기 위해 필요한 보안요구사항은 별도 표준에서 기술한다.

추가적으로 (그림 5-1)에서 보는 바와 같이 각 계층에서 생산·가공한 데이터는 산업제어시스템 보안참조모델 내에서만 유통되며, 별도로 정의된 경우에만 운영 계층을 통해서 외부로 전송될 수 있다. 또한 업무망 등 외부로부터 산업제어시스템으로 데이터가 유입될 수 없다. 이와 같은 산업제어시스템으로 구성된 망의 분리는 본 표준의 2부 ~ 4부에서 기술되는 보안요구사항의 수립하는데 가정사항으로 적용된다.

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 - 2부: 현장장치 계층

‘산업제어시스템 보안요구사항 - 1부: 개념 및 참조모델’에서 정의된 보안개념과 보안 참조모델을 고려하여 산업제어시스템을 구성하는 3계층 가운데 현장장치 계층에 위치하는 산업제어 시스템 구성요소들에 대한 보안요구사항을 정의하고 있음

Ⅰ-3.2 산업제어시스템 보안요구사항 - 3부: 제어 계층

‘산업제어시스템 보안요구사항 - 1부: 개념 및 참조모델’에서 정의된 보안개념과 보안 참조모델을 고려하여 산업제어시스템을 구성하는 3계층 가운데 제어 계층에 위치하는 산업제어 시스템 구성요소들에 대한 보안요구사항을 정의하고 있음

Ⅰ-3.3 산업제어시스템 보안요구사항 - 4부: 운영 계층

‘산업제어시스템 보안요구사항 - 1부: 개념 및 참조모델’에서 정의된 보안개념과 보안 참조모델을 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)