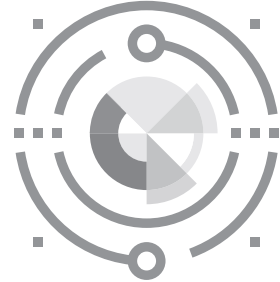


산업제어시스템 보안요구사항



이종후 국가보안기술연구소 책임연구원

김우년 국가보안기술연구소 책임연구원

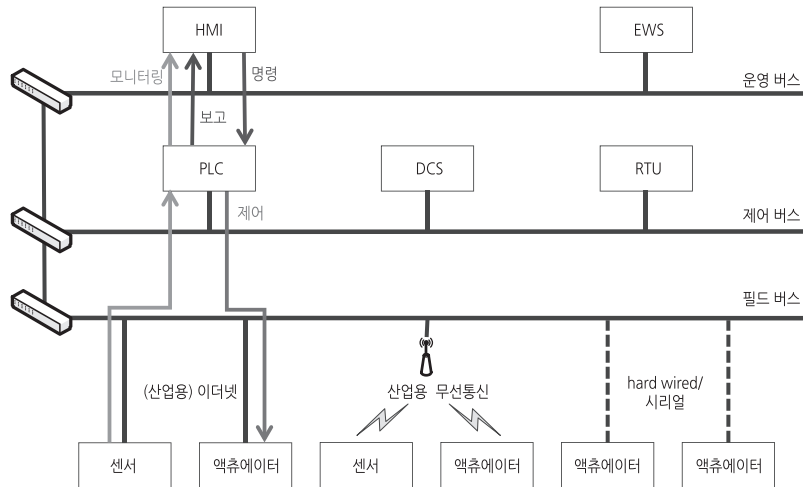
1. 머리말

산업제어시스템이란 전력, 가스, 상하수도, 원자력, 운송, 제조 등 산업 현장을 모니터링하고 제어하는데 사용되는 시스템이다. 산업제어시스템은 발전소, 가스 생산·공급기지, 댐 등 국가·사회 유지에 필수적인 기능을 제공하는 기반시설에서 주로 사용된다. 따라서 산업제어시스템이 해킹 등 사이버공격을 받아 피해를 입을 경우, 국가·사회 기능이 마비되는 등 피해 규모가 매우 큰 경우가 대부분이다.

과거에는 정보시스템과 전혀 다른 특성을 갖는 산업제어시스템은 사이버공격으로부터 비교적 안전하다고 인식되어 산업제어시스템을 설계·구축·운영하는 데 있어서 사이버보안을 크게 고려하지 않았다. 그러나 최근 들어 산업제어시스템은 IT 기술을 적극 도입하고 있어서 더 이상 사이버보안을 고려하지 않을 수 없는 상황이다. 특히 2010년 이란의 우라늄 농축 시설을 공격 목표로 한 스틱스넷(Stuxnet)이 발견된 이후, 산업제어시스템 사이버보안에 대한 관심은 급격하게 증가하였다.

정보시스템을 사이버공격으로부터 안전하게 보호하기 위한 방법에 대해서는 많은 연구가 수행되

어 왔으며, 이에 따라 정보시스템을 대상으로 하는 보안요구사항 역시 표준, 지침 등의 형태로 개발되어 있다. 현대의 산업제어시스템이 IT 기술과 접목하여 운영되는 점을 고려할 때, 이미 개발되어 있는 정보시스템 보안요구사항을 산업제어시스템에 적용할 수도 있다. 그러나 산업제어시스템은 정보시스템과 다른 여러 가지 특징을 가지고 있는데, 그 가운데서도 가장 중요한 것은 사이버보안 목표의 우선순위가 다르다는 점이다. 일반적으로 사이버보안 목표는 ‘기밀성’, ‘무결성’, ‘가용성’을 말하는데, 정보시스템에서는 정보 유출을 막기 위해서 기밀성의 우선순위가 가장 높다. 하지만 운영의 연속성이 매우 중요한 산업제어시스템에서는 가용성의 우선순위가 가장 높다. 이는 예기치 않은 산업제어시스템의 운영 중단은 정보시스템과는 비교할 수 없는 큰 피해를 일으킬 수 있기 때문이다. 이처럼 산업제어시스템에는 정보시스템과는 다른 보안요구사항이 적용되어야 하며, 이를 정의한 표준을 소개하고자 한다.



[그림 1] 산업제어시스템 네트워크 구성과 서비스 시나리오

2. 표준의 목적 및 구성

이 표준의 목적은 산업제어시스템 보안요구사항의 정의이다. 산업제어시스템은 현장장치 계층, 제어 계층, 운영 계층 등 3계층으로 구성된다.

산업제어시스템의 계층 구성에 따라 이 표준은 다음과 같이 총 4부로 구성되어 있다. 1부에서는 산업제어시스템의 보안개념과 보안참조모델을 정의한다. 2부~4부는 1부에서 정의한 보안개념과 보안참조모델에 따라 산업제어시스템의 계층별 보안요구사항을 정의한다.

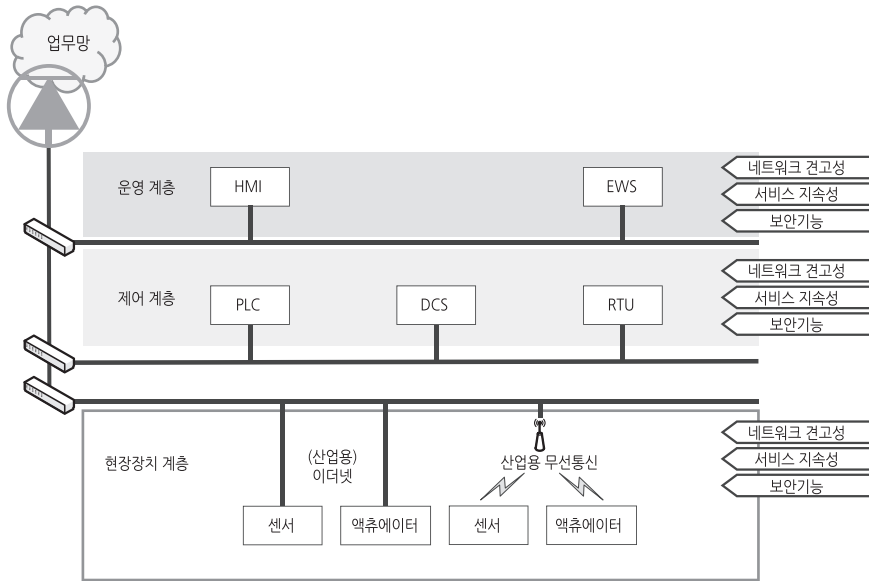
- 산업제어시스템 보안요구사항 - 1부: 개념 및 참조모델
- 산업제어시스템 보안요구사항 - 2부: 현장장치 계층
- 산업제어시스템 보안요구사항 - 3부: 제어 계층
- 산업제어시스템 보안요구사항 - 4부: 운영 계층

3. 주요 내용

3.1 개념 및 참조모델

산업제어시스템의 네트워크 구성과 서비스 시나리오는 [그림 1]과 같다. 센서, 액츄에이터 등의 현장장치는 유무선 랜, 시리얼 케이블 또는 구리선에 의한 하드 와이어드(hard wired) 방법 등을 통해 PLC, DCS, RTU 등 제어 H/W와 연결되며, 제어 H/W는 이더넷 또는 시리얼 케이블 등을 통해 HMI, EWS 등의 제어 S/W와 연결된다.

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 현장장치 상태 데이터를 모니터링하고, 이를 통해 현장장치의 상태를 확인할 수 있다. 현장에 설치된 밸브의 개폐 등 액츄에이터를 제어하기 위해서 사용자는 제어 S/W를 통해서 제어 명령을 입력한다. 사용자가 입력한 제어 명령은 제어 H/W에게 전달되며, 제어 H/W는 제어 명령에 따라 현장장치를 제어한다. 또한, 제어 H/W는 이상 상황이나 설정된 이벤트가 발생하면, 제어 S/W에 보고(알람)를 통해 해당 상황을 알릴 수 있다. [그림 1]의 ‘명령’, ‘제어’, ‘보고’, ‘모니터링’은 산업제어시스템의 필수 서비스이다.



[그림 2] 산업제어시스템 보안참조모델

한편, [그림 1]은 산업제어시스템 단일 네트워크 구성만을 나타낸 것이다. 산업제어시스템 네트워크는 다른 네트워크와 연결되어 확장된 산업제어시스템 네트워크를 구성할 수 있다.

앞서 설명한 바와 같이 산업제어시스템에서는 사이버보안 목표 가운데 가용성의 우선순위가 높다. 이런 특성을 고려하여 산업제어시스템은 다음과 같은 보안원칙에 따라 보안요구사항을 만족해야 한다.

- **네트워크 견고성:** 산업제어시스템 구성요소는 비정상적인 통신 데이터 또는 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.

[그림 2]는 산업제어시스템 보안참조모델이다. 산업제어시스템은 운영 계층, 제어 계층, 현장장치 계

층의 3계층으로 구성된다.

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

제어 계층은 현장장치 계층에서 계측·수집한 데이터를 모니터링 계층으로 전달하거나 모니터링 계층으로부터 제어 명령을 받아 현장장치를 제어하는 역할을 수행한다. PLC, DCS, RTU 등의 제어 H/W가 이 계층에 포함된다. 또한, 제어 계층에서 데이터를 주고받거나 제어 계층과 모니터링 계층의 통신에는 산업제어 전용 프로토콜이 사용된다. 이와 같은 산업제어 프로토콜은 실시간 통신, 견고성, 응답시간을 중요시하고 통신 지연을 허용하지 않는 산

업제어시스템 네트워크 성능 요구사항을 만족하는 특성을 제공한다. 대표적인 산업제어 프로토콜로는 DNP, MODBUS, EtherNet/IP, OPC 등이 있다.

현장장치 계층에는 센서, 액추에이터 등의 상태 데이터를 계측·수집하거나 제어하는 데 사용되는 현장장치가 포함된다. 현장장치는 제어 계층과 유무선 랜, 시리얼 케이블, 구리선에 의한 하드 와이어드 방법 등으로 연결된다.

산업제어시스템을 구성하는 각 계층은 계층별로 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 보안요구사항을 이 표준의 2부~4부에서 기술한다.

추가적으로 [그림 2]에서 보는 바와 같이 각 계층에서 생산·가공한 데이터는 산업제어시스템 보안참조모델 내에서만 유통되며, 별도로 정의된 경우에만 운영 계층을 통해서 외부(예: 업무망)로 전송될 수 있다. 이는 업무망 등 외부로부터 산업제어시스템으로 데이터가 유입될 수 없음을 의미한다. 이와 같은 산업제어시스템으로 구성된 망의 분리는 이 표준의 2부~4부에서 기술되는 보안요구사항을 수립하는데 가정사항으로 적용된다.

3.2 계층별 보안요구사항

산업제어시스템 보안요구사항의 2부~4부는 계층별 보안요구사항이다. 2부에서는 현장장치 계층에 위치하는 산업제어시스템 구성요소들을 관리하고 운영하는 데 있어서 필요한 보안요구사항을 정의한다. 현장장치 계층에 속하는 산업제어시스템 구성요소는 스마트 현장장치이다. 스마트 현장장치는 산업제어시스템 현장에서 사용되는 장치 중 연산 기능과 통신 기능이 적용된 장치를 의미한다. 스마트 현장장치의 예로는 현장의 데이터를 수집하여

송신하는 센서가 대표적이다. 현장장치 계층의 구성요소가 스마트 현장장치로만 한정되지는 않는다. 1부에서 기술한 바와 같이 센서, 액추에이터 등의 상태 데이터를 계측·수집하거나 제어하는 역할을 하며 제어 계층과 통신하는 구성요소는 모두 현장장치 계층에 포함된다고 할 수 있다. 그러나 연산과 통신 기능이 없는 현장장치는 보안요구사항을 구현할 수 있는 방법이 없기 때문에 이 표준의 적용 범위는 스마트 현장장치로 한정된다.

3부는 제어 계층에 대한 보안요구사항으로, 산업제어시스템 구성요소 가운데 제어 H/W에 적용된다. 제어 H/W는 제어 프로토콜을 처리하는 임베디드 장치로, 현장에서 운영되는 현장장치와 제어 S/W와 연결되어 현장장치의 상태 데이터를 수집하거나 제어 S/W로부터 제어 명령을 받아서 현장장치를 제어하는 역할을 수행한다. PLC, DCS, RTU 등이 이에 해당한다.

4부는 운영 계층 보안요구사항으로, 제어 H/W와 통신하며 현장장치의 상태를 모니터링하고 제어가 필요한 경우 제어 명령을 내리기 위해 사용되는 제어 S/W에 적용된다. 제어 S/W의 예로는 HMI, EWS 등이 있다.

각 계층에 적용되는 보안요구사항은 앞서 기술한 3개의 보안원칙에 따라 다음과 같이 동일한 구성을 가진다. 그러나 보안요구사항의 세부내용은 각 계층의 특성을 고려하여 서로 다르게 구성된다.


- **네트워크 견고성:** 패징 테스트, 스트레스 테스트
- **서비스 지속성:** 자원 가용성, 물리적 인터페이스 보호, 이벤트 대응
- **보안기능:** 보안감사, 식별·인증, 접근통제, 전송 데이터 보호, 저장 데이터 보호, 보안 기능 관리, 상태 관리

이러한 구성에 따라 분류되는 보안요구사항 항목은 ‘식별번호’, ‘항목명’, ‘항목설명’, ‘필수/선택’의 형태로 산업제어시스템 구성요소에 필요한 보안요구

<표 1> 계층별 보안요구사항 항목 수

보안원칙	분류	현장장치 계층			제어 계층			운영 계층		
		필수	옵션	합계	필수	옵션	합계	필수	옵션	합계
네트워크 견고성	퍼징 테스트	11	0	11	11	0	11	11	0	11
	스트레스 테스트	0	2	2	0	2	2	0	0	0
서비스 지속성	자원 가용성	2	1	3	2	3	5	2	0	2
	물리적 인터페이스 보호	1	2	3	1	2	3	0	0	0
	이벤트 대응	1	0	1	1	1	2	1	1	2
보안기능	보안 감사	0	5	5	4	4	8	6	3	9
	식별 · 인증	3	4	7	6	2	8	6	4	10
	접근통제	0	4	4	1	3	4	4	2	6
	전송 데이터 보호	0	4	4	0	4	4	0	4	4
	저장 데이터 보호	1	2	3	1	2	3	1	1	2
	보안기능 관리	3	0	3	3	0	3	3	0	3
	상태 관리	1	5	6	2	2	4	5	1	6
합계		23	29	52	32	25	57	39	16	55

사항의 내용을 제공한다. 각 계층의 보안요구사항 항목 수를 살펴보면 <표 1>과 같다.

시스템의 설계 및 제조 단계서 고려해야 할 보안요구사항을 제시함으로써 산업제어시스템의 안전한 관리와 운영에 기여할 것으로 기대된다. 

4. 맺음말

이 표준은 산업제어시스템 구성요소를 안전하게 관리 및 운영하기 위해서 필요한 보안요구사항을 정의한다. 표준의 2부~4부는 세부적인 보안요구사항을 기술하는 동시에 부속서를 통해서 보안요구사항의 시험 방법을 제시한다. 보안요구사항 시험 방법은 제어시스템 구성요소가 해당되는 보안요구사항을 만족하는지 확인하는 데 필요한 시험 절차, 준비사항, 통과 기준 등을 제시한다. 따라서 이 표준은 산업제어시스템 구성요소가 안전하게 관리 및 운영되기 위한 준비가 되었는지 확인하는 용도로 사용될 수 있다.

일단 운영이 시작되면 패치 등 보안조치가 어려운 산업제어시스템의 특성을 고려할 때 산업제어시스템의 설계 및 제조 단계에서부터 사이버보안을 고려하는 일은 매우 중요하다. 이 표준은 산업제어

[주요 용어 풀이]

- DCS: Distributed Control System
- EWS: Engineering Workstation
- HMI: Human Machine Interface
- PLC: Programmable Logic Controller
- RTU: Remote Terminal Unit