요약본

스마트공장 보안모델

PART Ⅰ : OT 영역

2020. 12

과학기술정보통신부
Ministry of Science and ICT

KISA 한국인터넷진흥원
KOREA INTERNET & SECURITY AGENCY


스마트공장
보안모델
PART Ⅰ: OT 영역

배경

독일, 일본 등 주요국은 제조와 ICT 융합을 통한 국가 미래 제조 경쟁력 확보를 위해 노력 중이며, 특히, 독일은 인더스트리4.0 산업 정책에서 생산성 향상을 위해 기존 공장에 ICT 기술을 결합하여 생산시설을 네트워크화하고 지능형 생산시스템을 갖춘 스마트공장(Smart factory)으로의 진화를 핵심으로 추진하고 있다.

스마트공장이란 ICT 기반의 지능화, 이종 프로토콜간 통신에 대한 논리적 연결, 센서/장비/설비 등의 데이터 분석을 기반으로 하는 자동화, 기기간 협업 등을 통해 최적의 제품 생산 공정을 갖는 공장을 의미하며, 국내 역시 중소벤처기업부를 중심으로 국가 미래 제조 경쟁력 확보를 위해 스마트공장 보급·확산 노력을 기울이고 있다.

다만, 스마트공장 내 ICT 기술이 접목된 생산설비가 점차 외부 네트워크에 다수 연결되는 만큼 ICT 보안 위협이 스마트공장 전반으로 전이, 노출되고 있으며, 최근에는 공장 제어 및 운영 장치가 랜섬웨어에 감염되어, 생산 차질로 인한 제품가격 상승과 함께 제품 사용 고객에게 불편함을 초래하는 사례가 빈번히 발생 중에 있다.

이처럼 스마트공장 보안위협이 실제 발생함에도 불구하고, 스마트공장 보안 담당자들의 경우, 실제 발생 또는 향후 발생 가능한 보안위협에 대한 이해 부족과 함께 보안위협에 대한 효과적이고 실효성 있는 대응에 참고할 수 있는 기초 자료부족으로 스마트공장 보안 강화에 어려움을 겪고 있다.

이에, 본 문서는 스마트공장 보안담당자가 스마트공장 보안위협을 식별하고, 식별된 보안위협에 대응하기 위한 보안 요구사항, 보안기술, 보안 솔루션을 제시하여, 실제 스마트공장 보안 강화에 참고하고 활용할 수 있도록 지원하는데 목적이 있다. 그리고 이를 통해 국내 스마트공장 보안내재화 확산과 함께 스마트공장 보안 시장을 활성화 시키는데 기여하고자 한다.

스마트공장 보안모델 활용 방안

가상 스마트공장 사례 기반 활용 방안

가칭 KISmart Factory로 명칭을 부여하고, 스마트공장 환경을 임의적으로 제시하여 보안모델 활용 방안을 제시한다. 가상 스마트공장에 대한 환경은 다음과 같다.

KISmart Factory 현황

KISmart Factory는 진공채혈관[1] 을 개발, 생산하는 업체로 생산 제조라인의 원자재, 제품, 장비, 공정상태의 센싱 데이터를 수집하여 모니터링하고, 생산계획 대비 생산 실적의 실시간 관리를 하고 있는 스마트공장이다.

KISmart Factory는 생산공정에 채혈관 제조 자동화 기술을 적용하였으며, 진공채혈관을 구매하는 협력업체들이 인터넷을 통하여 실시간으로 확인할 수 있도록 생산실적 관리 시스템을 구축하였다.

KISmart Factory는 제품 생산을 위한 장치, 제어시스템, 생산관리시스템, 경영정보시스템을 포함한 스마트공장 자산현황을 자산목록으로 구성하여 관리하고 있다. KISmart Factory의 자산 목록은 다음표와 같다.

1 유효기간까지 최적의 진공상태를 유지, 정확한 용량의 첨가제 분사, 멸균상태 유지 등 고등의 기술이 요구되는 의료소모품

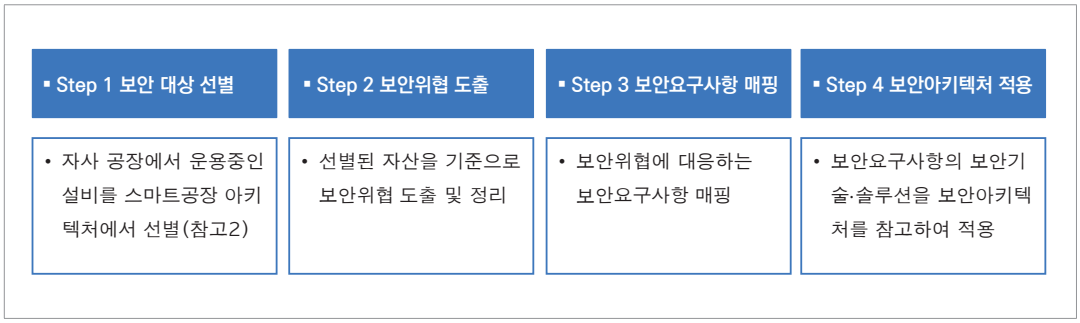
■ KISmart Factory 자산 목록

구분	자산 유형	비고
공장 설비	환경 측정 센서	-
	체혈관 자동화 제조 장비	-
	제조 제어 PLC	-
	제조 관리 HMI	-
네트워크	산업용스위치	공장망
	무선AP	공장망
	스위치	업무망
	백본	업무망
PC	업무PC	-
서버	생산관리시스템	내부 서버
	경영정보시스템/메일서버	외부 서버

■ KISmart Factory 보안아키텍처 활용 절차

가상 환경으로 제시된 스마트공장을 대상으로 보안아키텍처 활용 방안을 제시한다. 보안아키텍처 활용 절차는 다음 그림과 같다.

■ 보안아키텍처 활용 절차



step 1 보안 대상 선별

KISmart Factory에서 운용 중인 자산 중 스마트공장 아키텍처의 제어설비 및 제어네트워크에 해당하는 자산을 보안 대상으로 선별한다. KISmart Factory 보안 대상은 아래 표와 같다.

KISmart Factory 보안 대상

계층	운용 자산	보안 대상
0계층	환경 측정 센서	센서
	체혈관 자동화 제조 장비	생산 장비
1계층	제조 제어 PLC	PLC
	산업용스위치	-
	무선AP	Wi-Fi
2계층	제조 관리 HMI	HMI
	스위치	-
3계층	생산관리시스템	MES
4~5계층	경영정보시스템/메일서버	ERP/서버
	업무PC	업무PC
	백본	-

step 2 보안위협 도출

KISmart Factory의 보안 대상으로부터 발생 가능한 보안위협을 도출한다. 선별된 KISmart Factory의 보안 대상별로 정리한 보안위협은 아래 표와 같다.

KISmart Factory 보안위협

대상	보안위협 벡터	보안위협
센서	물리적인 접근, 포트, 지원설비를 통한 위협	공장 내 물리적 접근을 통한 장치 훼손
	공정 제어 네트워크를 통한 위협	펌웨어 취약점을 통한 정상 운전 설정값 변조
		과도한 상태 확인 요청을 통한 서비스 거부 공격으로 오동작 및 중단
생산장비	물리적인 접근, 포트, 지원설비를 통한 위협	물리적 인터페이스에 접속하여 펌웨어 변조
		USB 등 외부 공개된 포트를 통한 랜섬웨어 감염
	공정 제어 네트워크를 통한 위협	공정 네트워크 도청을 통해 레시피, 제어장치 계정/비밀번호 등 공정 중요 정보 유출
	인력 및 노후설비에 의한 위협	이벤트 알람 미설정으로 인한 장비 파손 및 운전 중단
		사용자 실수로 인한 가동정지 명령으로 오동작 및 중단

대상	보안위협 벡터	보안위협
PLC	물리적인 접근, 포트, 지원설비를 통한 위협	공장 내 물리적 접근을 통한 전원 등 지원설비 훼손으로 PLC 오동작 및 중단
		공정 네트워크 영역에 물리적으로 침입 후 프로토콜 취약점을 이용한 재전송 공격을 통한 정상 운전 설정값 변조
		비인가자가 물리적 접근을 통한 공정 중요 정보 유출
	공정 제어 네트워크를 통한 위협	버퍼 오버플로우 공격을 통한 공정 운전 데이터 변조
		대량의 제어 명령 전송을 통해 PLC 오동작 및 중단
	공급망을 통한 위협	유지보수 채널을 이용한 재전송 공격으로 정상 운전 설정값 변조
HMI	물리적인 접근, 포트, 지원설비를 통한 위협	비인가자가 불법적으로 접근하여 공정 임의 조작 오동작 및 중단
	공장 업무영역을 통한 위협	업무망에서 전파되어 랜섬웨어 감염
	공급망을 통한 위협	유지보수를 위한 USB를 삽입하여 트로이 목마 등 악성코드에 감염
		유지보수를 위한 USB를 삽입하여 스턱스넷 등 악성코드에 감염되어 PLC 등 제어시스템 오동작 및 중단
	외부 인터넷을 통한 위협	외부 인터넷을 통한 트로이목마 등 악성코드 감염
MES	산업제어시스템을 통한 위협	미라이봇넷 등 악성코드가 업무망에서 전파되어 오동작 및 중단
	공급망을 통한 위협	외부 공개된 서비스 및 포트를 통한 랜섬웨어 감염
		원격접속으로 OS 및 소프트웨어 취약점을 이용한 서비스 거부 공격으로 오동작 및 중단
ERP/서버	외부 인터넷을 통한 위협	업무PC에 침투하여 서버 OS 및 소프트웨어 취약점을 이용한 서비스 거부 공격
		외부 홈페이지와 연계된 내부서버 장애
업무PC	공장 업무영역을 통한 위협	비인가 이동식 저장매체를 통해 웜에 감염되어 업무 네트워크 장애
		무선 업무망에 침투하여 업무PC 침투 후 정보 탈취
	외부 인터넷을 통한 위협	이메일 및 외부 인터넷을 통한 스파이웨어 감염
Wi-Fi	공정 제어 네트워크를 통한 위협	공개된 SSID에 무차별 대입, 사전대입 공격 등으로 무선 네트워크 침입
		암호화 키를 획득하여 네트워크 패킷 도청으로 Wi-Fi 비밀번호 탈취

step 3 보안요구사항 매핑

KISmart Factory 보안 대상별로 도출된 보안위협에 대응하는 보안요구사항을 매핑하면 다음 표와 같다.

KISmart Factory 보안위협 대응 보안요구사항

보안위협 벡터	보안위협	보안 요구사항	보안기술	보안솔루션
센서				
물리적인 접근, 포트, 지원설비를 통한 위협	공장 내 물리적 접근을 통한 장치 훼손	ⓐ. 물리적 비인가자 공장 출입 통제 ⓑ. 물리적 장비 접근 제한	ⓐ. 비인가자 출입 통제 ⓑ. 물리적 장치 보호	ⓐ. 출입 통제 시스템 ⓑ. 시건 장치
공정 제어 네트워크를 통한 위협	펌웨어 취약점을 통한 정상 운전 설정값 변조	ⓐ. 벤더사 권고사항 및 최신 보안 패치 적용	ⓐ. 보안 패치 및 업데이트 적용	ⓐ. -
	과도한 상태 확인 요청을 통한 서비스 거부 공격으로 오동작 및 중단	ⓐ. 벤더사 권고사항 및 최신 보안 패치 적용	ⓐ. 보안 패치 및 업데이트 적용	ⓐ. -
생산 장비				
물리적인 접근, 포트, 지원설비를 통한 위협	물리적 인터페이스에 접속하여 펌웨어 변조	ⓐ. 포트락 등 불필요 인터페이스 접근 통제 ⓑ. 물리적 장치 접근 통제	ⓐ. 물리적 인터페이스 사용 제한 ⓑ. 물리적 장치 보호	ⓐ. 포트락 ⓑ. 시건 장치
	USB 등 외부 공개된 포트를 통한 랜섬웨어 감염	ⓐ. 포트락 등 불필요 인터페이스 접근 통제 ⓑ. 물리적 장치 접근 통제 ⓒ. 악성코드 탐지	ⓐ. 물리적 인터페이스 사용 제한 ⓑ. 물리적 장치 보호 ⓒ. 악성코드 탐지 및 차단	ⓐ. 포트락 ⓑ. 시건 장치 ⓒ. 백신
공정 제어 네트워크를 통한 위협	공정 네트워크 도청을 통해 레시피, 제어장치 계정/비밀번호 등 공정 중요 정보 유출	ⓐ. 공정 네트워크 암호화	ⓐ. 장치간 통신 암호화	ⓐ. 암호화 모듈
인력 및 노후설비에 의한 위협	이벤트 알람 미설정으로 인한 장비 파손 및 운전 중단	ⓐ. 장치 및 운전 상태 모니터링 및 알람	ⓐ. 실시간 모니터링 및 알람	ⓐ. 모니터링 시스템
	사용자 실수로 인한 가동정지 명령으로 오동작 및 중단	ⓐ. 가동 정지 등 중요 명령 인터페이스 보호	ⓐ. 물리적 장치 보호	ⓐ. 시건 장치
PLC				
물리적인 접근, 포트, 지원설비를 통한 위협	공장 내 물리적 접근을 통한 전원 등 지원설비 훼손으로 PLC 오동작 및 중단	ⓐ. 비인가자 공장 출입 통제 ⓑ. PLC 물리적 접근 통제 ⓒ. PLC 배터리 및 전원 이중화	ⓐ. 비인가자 출입 통제 ⓑ. 물리적 장치 접근 제한 ⓒ. 백업 배터리 관리 및 전원 설비 이중화	ⓐ. 출입 통제 시스템 ⓑ. 시건 장치 ⓒ. 비상 전원

보안위협 벡터	보안위협	보안 요구사항	보안기술	보안솔루션
물리적인 접근, 포트, 지원설비를 통한 위협	공정 네트워크 영역에 물리적으로 침입 후 프로토콜 취약점을 이용한 재전송 공격을 통한 정상 운전 설정값 변조	ⓐ. 비인가자 공장 출입 통제 ⓑ. PLC 운전 중 메모리 쓰기 제한	ⓐ. 비인가자 출입 통제 ⓑ. PLC 운전 중 메모리 쓰기 제한 설정	ⓐ. 출입 통제 시스템 ⓑ. -
	비인가자가 물리적 접근을 통한 공정 중요 정보 유출	ⓐ. 비인가자 공장 출입 통제 ⓑ. PLC 물리적 인터페이스 보호	ⓐ. 비인가자 출입 통제 ⓑ. 물리적 장치 접근 제한 ⓒ. 불필요한 인터페이스 사용 제한	ⓐ. 출입 통제 시스템 ⓑ. 시건 장치 ⓒ. 포트락
공정 제어 네트워크를 통한 위협	버퍼 오버플로우 공격을 통한 공정 운전 데이터 변조	ⓐ. 공장 네트워크 비인가 단말 접근 통제 ⓑ. PLC 공개된 취약점에 대한 패치 및 업데이트 수행	ⓐ. IP/MAC 기반 네트워크 접근 통제 ⓑ. 보안 패치 및 업데이트 적용	ⓐ. 보안 스위치 ⓑ. -
	대량의 제어 명령 전송을 통해 PLC 오동작 및 중단	ⓐ. 공장 네트워크 비인가 단말 접근 통제 ⓑ. 공정 네트워크 유해 트래픽 탐지	ⓐ. IP/MAC 기반 네트워크 접근 통제 ⓑ. 네트워크 유해 트래픽 탐지	ⓐ. 보안 스위치 ⓑ. 산업용 IDS
공급망을 통한 위협	유지보수 채널을 이용한 재전송 공격으로 정상 운전 설정값 변조	ⓐ. 공장 네트워크 원격 접속 통제 ⓑ. PLC에 사전 등록된 장치 및 IP 에서만 접근할 수 있도록 접근 통제	ⓐ. 원격 접속 시 안전한 보안 경로 사용 및 접근 통제 ⓑ. IP 및 기기 접근 통제	ⓐ. VPN ⓑ. -
HMI				
물리적인 접근, 포트, 지원설비를 통한 위협	비인가자가 불법적으로 접근하여 공정 임의 조작 오동작 및 중단	ⓐ. 비인가자 공장 출입 통제 ⓑ. HMI 사용자 식별 인증 ⓒ. HMI 사용자 권한 관리	ⓐ. 비인가자 출입 통제 ⓑ. 사용자 식별 인증 ⓒ. 사용자 권한 관리	ⓐ. 출입 통제 시스템 ⓑ. - ⓒ. -
공장 업무영역을 통한 위협	업무망에서 전파되어 랜섬웨어 감염	ⓐ. 공장 네트워크 망분리 ⓑ. HMI 접근 단말 제한 ⓒ. 중요 정보 백업	ⓐ. 업무망과 공장망 분리 ⓑ. IP 및 기기 접근통제 설정 ⓒ. 문서 관리 및 파일 암호화	ⓐ. 산업용 방화벽 ⓑ. - ⓒ. 문서/백업 관리
공급망을 통한 위협	유지보수를 위한 USB를 삽입하여 트로이 목마 등 악성코드에 감염	ⓐ. 비인가 이동식 저장매체 제한 ⓑ. 악성코드 탐지	ⓐ. 이동식 저장 매체 사용 통제 ⓑ. 악성코드 탐지 및 차단	ⓐ. 매체 제어 솔루션 ⓑ. 백신

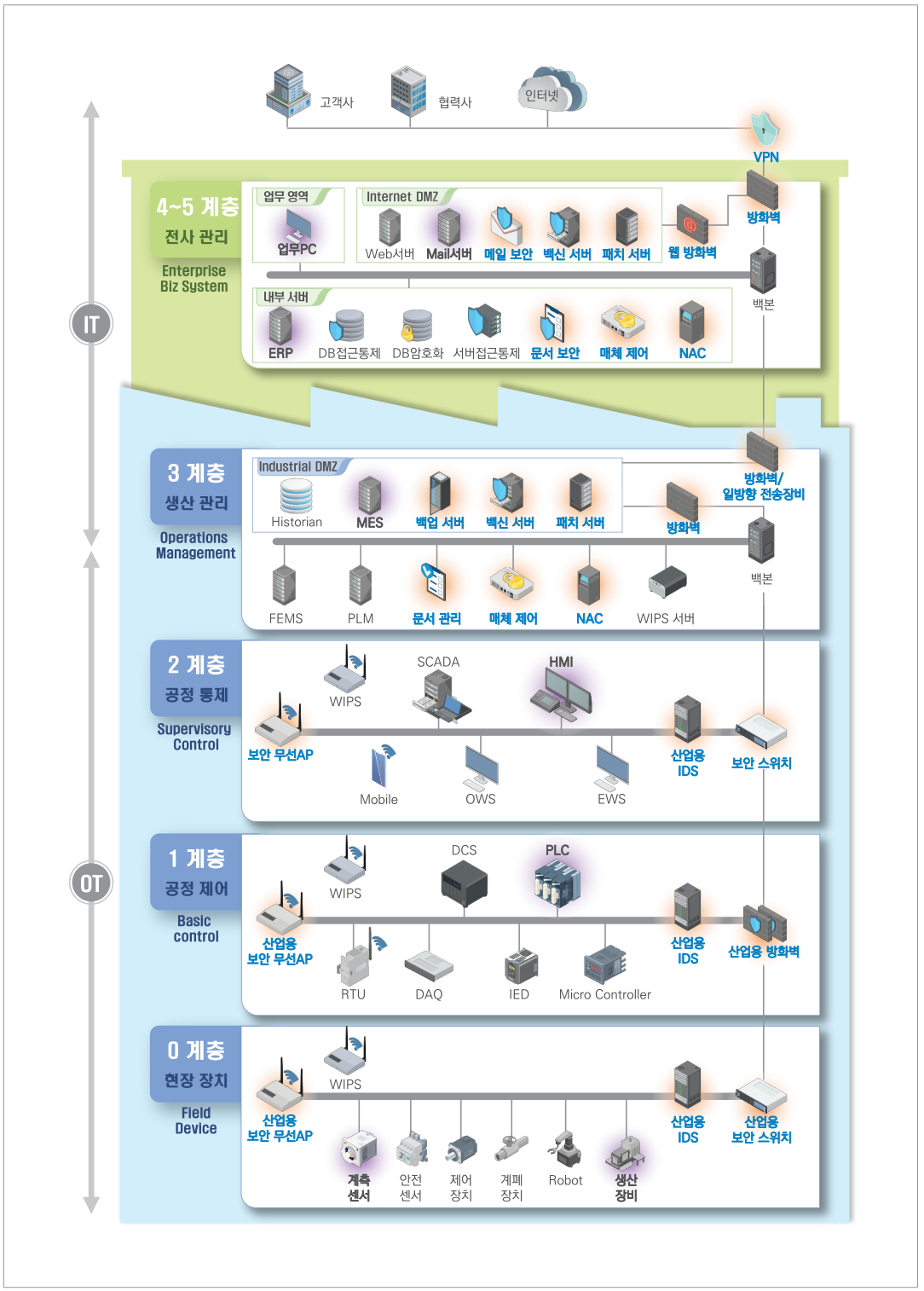
보안위협 벡터	보안위협	보안 요구사항	보안기술	보안솔루션
공급망을 통한 위협	유지보수를 위한 USB를 삽입하여 스넉스넷 등 악성코드에 감염되어 PLC 등 제어 시스템 오동작 및 중단	ⓐ. 비인가 이동식 저장매체 제한 ⓑ. 악성코드 탐지	ⓐ. 이동식 저장 매체 사용 통제 ⓑ. 악성코드 탐지 및 차단	ⓐ. 매체 제어 솔루션 ⓑ. 백신
외부 인터넷을 통한 위협	외부 인터넷을 통한 트로이목마 등 악성코드 감염	ⓐ. 외부 인터넷 접점 제거 ⓑ. 비인가 소프트웨어 사용 제한 ⓒ. 악성코드 탐지	ⓐ. 네트워크 망분리 ⓑ. 소프트웨어 사용 제한 ⓒ. 악성코드 탐지 및 차단	ⓐ. 방화벽 ⓑ. 매체 제어 솔루션 ⓒ. 백신
MES				
산업제어 시스템을 통한 위협	미라이봇넷 등 악성코드가 업무망에서 전파되어 오동작 및 중단	ⓐ. 네트워크 망분리 ⓑ. 일방향 통신 네트워크 구성 ⓒ. 악성코드 탐지	ⓐ. 네트워크 망분리 적용 ⓑ. 데이터 일방향 전송 방식 적용	ⓐ. 방화벽 ⓑ. 일방향 전송 장비
공급망을 통한 위협	외부 공개된 서비스 및 포트를 통한 랜섬웨어 감염	ⓐ. 외부 인터넷 접점 제거 ⓑ. 비인가 소프트웨어 설치 제한 ⓒ. 악성코드 탐지 ⓓ. 벤더사 권고사항 및 최신 보안 패치 적용 ⓔ. 공정 중요 정보 백업	ⓐ. 외부 인터넷 사용 제한 ⓑ. 소프트웨어 사용 제한 ⓒ. 악성코드 탐지 및 차단 ⓓ. 보안 패치 및 업데이트 적용 ⓔ. 문서 관리 및 파일 암호화	ⓐ. 방화벽 ⓑ. 매체 제어 솔루션 ⓒ. 백신 ⓓ. 문서/백업 관리
	원격접속으로 OS 및 소프트웨어 취약점을 이용한 서비스 거부 공격으로 오동작 및 중단	ⓐ. 공장 네트워크 원격 접속 통제 ⓑ. MES/Historian 접근 가능 단말 제한 ⓒ. 벤더사 권고사항 및 최신 보안 패치 적용	ⓐ. 원격 접속 시 안전한 보안 경로 사용 및 접근 통제 ⓑ. IP 및 기기 접근 통제 ⓒ. 보안 패치 및 업데이트 적용	ⓐ. VPN ⓑ. – ⓒ. 패치 관리 솔루션
ERP/서버				
외부 인터넷을 통한 위협	업무PC에 침투하여 서버 OS 및 소프트웨어 취약점을 이용한 서비스 거부 공격	ⓐ. 서버 접근 단말 제한 ⓑ. 벤더사 권고사항 및 최신 보안 패치 적용 ⓒ. 서버 보안 설정	ⓐ. IP 및 기기 접근 통제 설정 ⓑ. 보안 패치 및 업데이트 적용 ⓒ. 서버 보안 설정 적용	ⓐ. – ⓑ. 패치 관리 솔루션 ⓒ. –

보안위협 벡터	보안위협	보안 요구사항	보안기술	보안솔루션
외부 인터넷을 통한 위협	외부 홈페이지와 연계된 내부 서버 장애	ⓐ. 웹 어플리케이션 보안 ⓑ. 외부 공개된 어플리케이션 및 홈페이지 시큐어코딩 ⓒ. 서버 보안 설정	ⓐ. 웹 공격 탐지 및 차단 ⓑ. 시큐어코딩 적용 ⓒ. 서버 보안 설정 적용	ⓐ. 웹 방화벽 ⓑ. 소스코드진단 ⓒ. -
업무PC				
공장 업무영역을 통한 위협	비인가 이동식 저장매체를 통해 웜에 감염되어 업무 네트워크 장애	ⓐ. 비인가 이동식 저장매체 제한 ⓑ. 악성코드 탐지	ⓐ. 이동식 저장 매체 사용 통제 ⓑ. 악성코드 탐지 및 차단	ⓐ. 매체 제어 솔루션 ⓑ. 문서/백업 관리
	무선 업무망에 침투하여 업무 PC 침투 후 정보 탈취	ⓐ. 공장 무선 네트워크 접근 가능 단말 제한 ⓑ. 벤더사 권고사항 및 최신 보안패치 적용 ⓒ. 중요 정보 암호화	ⓐ. IP/MAC 기반 네트워크 접근 통제 ⓑ. 보안 패치 및 업데이트 적용 ⓒ. 문서 관리 및 파일 암호화	ⓐ. 네트워크 접근 통제 ⓑ. 패치 관리 솔루션 ⓒ. 문서/백업 관리
외부 인터넷을 통한 위협	이메일 및 외부 인터넷을 통한 스파이웨어 감염	ⓐ. 메일 보안 ⓑ. 중요 정보 암호화 ⓒ. 악성코드 탐지	ⓐ. 악성코드 포함된 메일 탐지 및 차단 ⓑ. 문서 관리 및 파일 암호화 ⓒ. 악성코드 탐지 및 차단	ⓐ. 메일 보안 ⓑ. 문서/백업 관리 ⓒ. 백신
Wi-Fi				
공정 제어 네트워크를 통한 위협	공개된 SSID에 무차별 대입, 사전대입 공격 등으로 무선 네트워크 침입	ⓐ. 무선 네트워크 접근 보안	ⓐ. SSID 숨김 및 비밀번호 복잡도 강화 등 보안 설정	ⓐ. 보안 AP
	암호화 키를 획득하여 네트워크 패킷 도청으로 Wi-Fi 비밀번호 탈취	ⓐ. 무선 네트워크 통신 암호화	ⓐ. WPA2 암호화 등 보안 설정	ⓐ. 보안 AP

step 4 보안아키텍처 적용

보안요구사항 매핑을 통해 KISmart Factory 보안 대상의 보안위협에 대응하는 보안기술과 보안솔루션을 확인하였다. 해당 보안요구사항을 바탕으로 KISmart Factory 보안아키텍처에 적용하면 다음 그림과 같다.

■ KISmart Factory 보안아키텍처



※ ● : 보안대상, ● : 보안솔루션

참고1 보안솔루션

앞서 살펴본 스마트공장 계층별, 제어설비, 제어네트워크 보안요구사항에서 제시한 보안솔루션의 경우, 일반적인 보안기능과 함께 스마트공장에 특화된 보안기능이 요구된다. 스마트공장 보안솔루션에 요구되는 보안기능을 살펴보면 아래 표와 같다.

표 68 스마트공장 보안솔루션

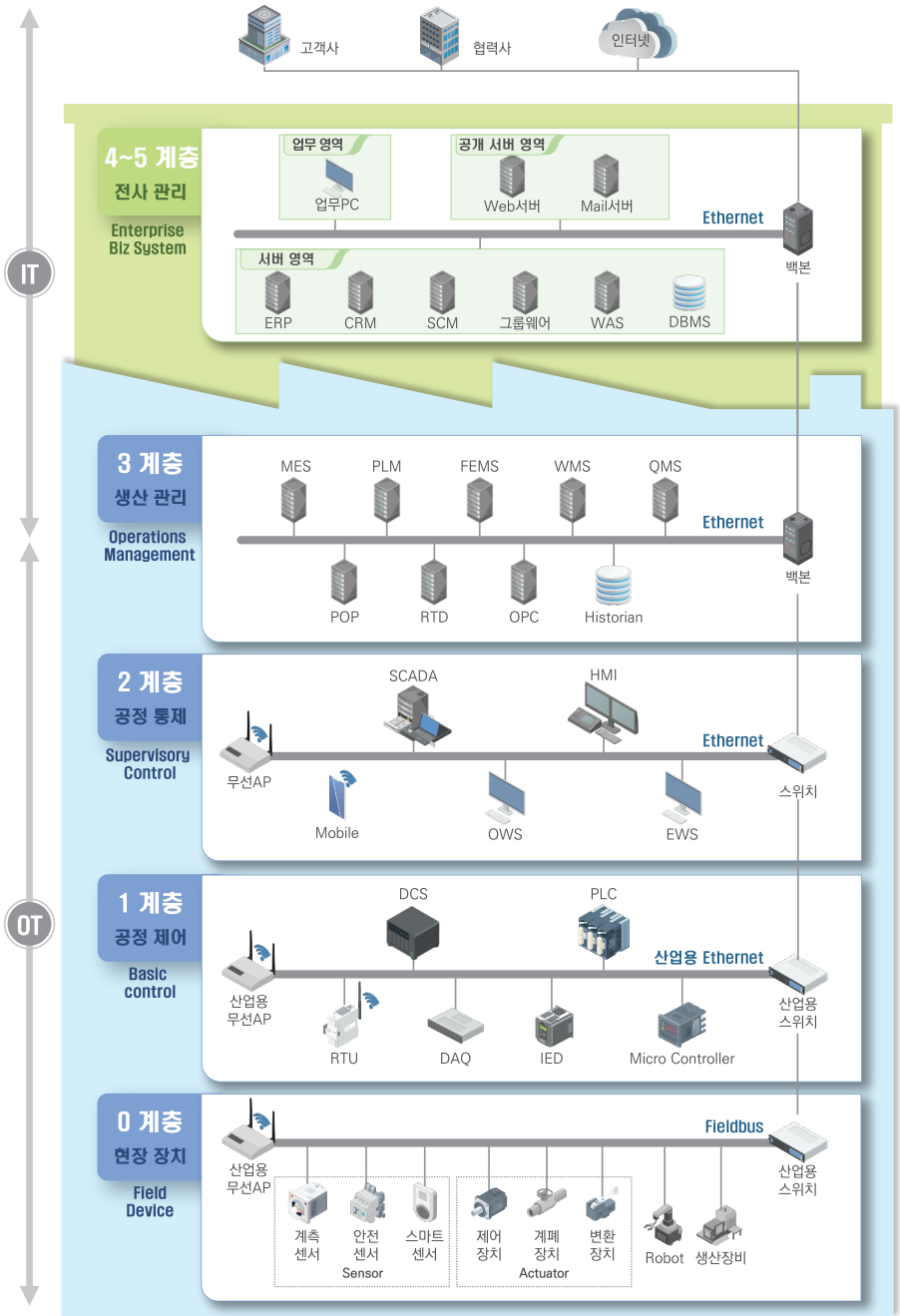
보안솔루션	목적	보안 기능
출입통제 솔루션	사전에 등록된 인원에 한하여 권한을 부여하고 출입을 통제	• 출입자 현황, 인원, 시간 등의 통합 관리 • 홍채, 얼굴, 지문, 카드 등의 다양한 인증방식 제공
포트락	비인가 장비, 인력의 이더넷 통신 접근을 통한 접근에 대해 통제	• 비어있는 포트 개방의 보안 취약점 제거 • 사전등록이 되지 않은 장비에 대한 접근통제
산업용 IDS	산업제어시스템 네트워크에서 일반적인 IT 프로토콜 과 함께 산업용 프로토콜을 통한 이상행위를 탐지	• 산업용 프로토콜 지원 • 산업용 네트워크 유해 트래픽 분석 및 탐지 • 산업제어시스템 통신 체계 감시 및 분석 • 혹독한 환경에서 안정적인 성능 제공
산업용 스위치	높은 수준의 가용성이 요구되는 산업현장(예, 변전소)에서 주로 사용 되며, 그에 따른 내구성 검증 및 안정적인 통신에 초점이 맞추어진 네트워크 장비	• 특정 산업용 프로토콜(IEC 61850, Modbus등)을 통한 자산 관리 가능 • 통신상의 문제 발생 시 보다 신속하게 복구 가능한 프로토콜 및 기능 보유 • IEC 62443, NIST등의 표준을 준수하고 그에 준하는 여러 가지 보안기능 탑재
백신	공장과 업무 영역 포함 모든 시스템에 바이러스, 웜 등 악성코드와 함께 랜섬웨어의 탐지 및 차단	• 악성코드 진단 및 대응 • 악성코드 실시간 진단 • 랜섬웨어 탐지 및 대응 • 보안 정책에 따른 악성파일 대응 및 시스템 변경 차단
산업용 방화벽	업무영역과 공장 네트워크의 접근 통제를 통한 망분리와 함께 산업제어시스템 애플리케이션 및 산업용 프로토콜에대한 탐지 및 차단	• 네트워크 접근 제어 및 패킷 필터링 • 접근 통제 정책을 통한 논리적 망분리 • 산업용 프로토콜 및 어플리케이션 제어 • 혹독한 환경에서 안정적인 성능 제공
산업용 AP	보다 안정적인 무선통신이 요구되는 산업현장(예, 물류창고, 반도체 생산라인 등) 에서 장비들 간의 상호 간섭을 최소화하면서 통신을 하기 위한 네트워크 장비	• Client 장비의 로밍이 해제 될 경우 보다 신속하게 다른 AP 및 영역 탐지를 하여 적용 어플리케이션에 있어 높은 수준의 가용성을 유지 한다 • IEC 62443, NIST등의 표준을 준수하고 그에 준하는 여러 가지 보안기능 탑재

보안솔루션	목적	보안 기능
일방향 전송 장비	분리된 공장 네트워크 영역에서 불가피한 데이터 전송을 위해 외부 네트워크와 안전한 데이터 전송 경로 확보 ※ 해당 목적을 위해 보안솔루션 적용시 일방향 전송 장비는 본 문서 보안아키텍처 중 3계층과 4~5계층 사이 방화벽을 대신하여 구성	• 일방향 파일 전송 • 일방향 통신 서비스
보안 AP	공장 무선 네트워크에 비인가 침입을 방지하기 위한 접근 통제와 무선 보안 설정을 통한 안전한 무선 네트워크 환경 구성	• 안전한 무선 통신 암호화 • SSID 숨김, 안전한 비밀번호 구성, WPS 기능 비활성화 등 보안 설정 • IP 및 MAC 기반의 사용자 단말 식별 및 네트워크 비인가 접근 차단 • 장치 관리 계정 및 권한 관리
네트워크 접근 통제 (NAC)	안전한 공장 유/무선 네트워크 환경을 위한 비인가자 및 비인가 장치의 공장 네트워크 접근 방지	• 비인가자 및 비인가 장치 유/무선 네트워크 접근 통제 • 정책 관리 및 관리 콘솔 지원
방화벽	외부 인터넷으로부터 내부망으로 비인가 접근, 네트워크 공격 등 보안 위협에 대한 탐지 및 차단	• 네트워크 접근 제어 및 패킷 필터링 • 접근 통제 정책을 통한 논리적 망분리
메일 보안	이메일을 통한 악성코드 감염 같은 보안 위협과 내부 중요 정보 유출 방지	• 이메일 첨부파일 악성 여부 검사 및 대응 • 메일 필터링 정책
VPN	업무 영역 및 공장 내부로의 원격접속이 불가피한 경우 사용자 식별/인증을 통한 접근 통제 및 암호화 통신을 통한 안전한 원격 접속 환경 구성	• 터널링 기법을 통한 네트워크 보안 • 안전한 암호화 통신 사용 • 원격접속 지원 및 접근 통제
데이터 완전삭제 솔루션	외부로 유출 되지 말아야 할 데이터의 잔재가 남지 않도록, 즉 데이터의 복구가 불가능하게 한다	• 중요 데이터 유출 방지 • 삭제 데이터 복구 불가
WIPS	공장 내 비인가 사설 무선 네트워크를 구성하여 외부 인터넷과 공장 네트워크의 접점 발생 방지	• 비인가 무선 장비 사용 탐지 및 차단
서버 접근통제시스템	서로 다른 업무망간의 인가되지 않은 접근 통제	• 작업 인력의 업무 범위에 따른 접근 권한 설정 기능 • 비인가 인력의 접근에 대한 알람 기능 및 통제
모니터링 시스템	실시간 상태 모니터링 및 이벤트 발생 시 알람기능을 통한 위험 감지	• 실시간 상태 모니터링 • 이벤트 발생 시 알람 기능 • 상태 및 이벤트 기록들에 대한 보고자료 작성

보안솔루션	목적	보안 기능
매체 제어	이동식 저장 매체, 불필요한 인터페이스를 통한 자료 유출과 악성코드 및 랜섬웨어 감염 방지	• 소프트웨어 사용 제어 • 저장 장치 및 이동식 저장장치 사용 제어 • 네트워크 카드 및 USB 등 기타 매체 사용 제어
IDS(침입탐지시스템)	주요 산업 네트워크상 유해 트래픽을 탐지, 감시, 분석 하는 보안장치	• 실시간 유해트래픽 탐지, 감시, 분석 • 데이터 수집, 책임추적성 대응
소스코드 진단 솔루션	소스 코드상 취약점을 분석하고 애플리케이션 개발 시 고려해야 하는 보안수준 및 시큐어 설계 방안 도입	• 취약점 점검 • 입력 값 검증 • 안전한 코딩
웹 방화벽	공장 및 전사 외부에 공개되어 있는 서비스의 취약점을 이용한 보안 위협 차단	• SQL 삽입, XSS 등 웹 공격 탐지 및 차단 • 유해 사이트 및 특정 콘텐츠 필터링 정책 • 변조 및 도용 등 웹 취약점 차단
보안 스위치	공장 네트워크에 비인가 침입을 방지하기 위한 접근 통제와 공장 운영에 불필요한 유해 트래픽 차단	• DDoS, Spoofing, SCAN 등 네트워크 공격 차단 • IP 및 MAC 기반의 사용자 단말 식별 및 네트워크 비인가 접근 차단 • 장치 관리 계정 및 권한 관리
IoT 게이트웨이	연결된 디바이스의 데이터를 수집하고 각각 디바이스와 인터넷이 연결할 수 있는 인터페이스 역할	• 디바이스 데이터 수집 • 수집 데이터 서버 전송
문서/백업 관리	산업제어시스템의 정상 동작 설정값과 제품 생산을 위한 레시피 등 중요 정보에 대한 안전한 관리	• 중요 정보 버전관리 및 이력관리 • 중요 저장 정보 암호화 • 백업 데이터 암호화 • 양방향 백업, 저장소 보호 등 랜섬웨어 대응
패치 관리 솔루션	폐쇄망으로 운영되는 서버 영역과 공장망에 대한 제조사에서 권고하는 최신 보안 업데이트 및 보안 패치를 통해 공개된 보안 취약점 대응	• 배포 대상 및 주기 등 정책 설정 • IT 프로토콜 및 산업용 프로토콜 연동
DB접근제어	사용자의 DBMS 접근권한을 설정하여 데이터베이스에 대한 접근을 통제하고 접근통제 현황을 모니터링	• 사용자의 데이터베이스 접근권한 설정 • 접근권한별 DBMS접근 통제 • 접근통제 기록 및 모니터링
DB암호화 솔루션	데이터베이스의 외부침입, 인가된 내부 사용자의 실수, 악의적인 접속으로부터 DB를 보호	• 보안성 강화 • DB 암/복호화 수행 • Table단위, 파일 단위 암호화 수행

참고2

스마트공장 계층구조 아키텍처



과학기술정보통신부
Ministry of Science and ICT

KISA 한국인터넷진흥원
KOREA INTERNET & SECURITY AGENCY