KISA 한국인터넷진흥원
KOREA INTERNET & SECURITY AGENCY

스마트공장 보안위협 및 대응방안

융합기반보호팀
이향진 팀장

목차

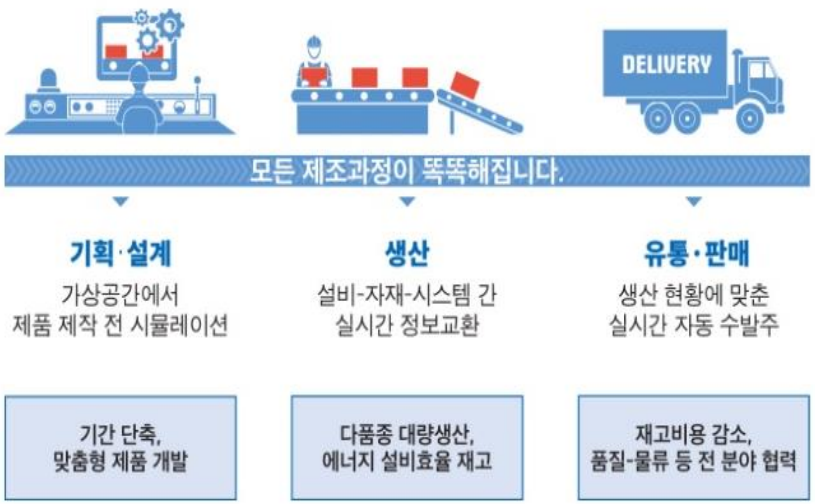
1. 스마트공장 개요

1 스마트공장 정의

스마트공장 이란?

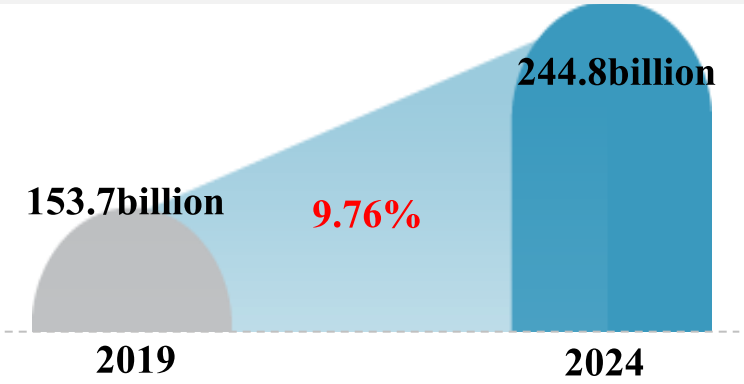
▶ 설계·개발, 제조, 유통·물류 등 생산 전체 과정에 **정보 통신 기술(ICT)**를 적용하여 생산성, 품질, 고객만족도 등을 향상시킬 수 있는 지능형 공장 (TTA 용어사전)

▶ **제조산업**에 ICT가 결합하여 제품의 기획, 설계, 생산, 유통, 판매 등 전 과정을 **ICT기술로** 통합함으로써 최소 비용 • 시간으로 고객맞춤형 제품 생산을 지향하는 공장(KS 표준, KS X 9001)



※ 출처 : 스마트제조혁신추진단

스마트공장 시장은 2019년 1,537억 달러에서
2024년 2,448억 달러로 성장 예상(CAGR : 9.76%)



※ 출처 : Markets and Markets, "Smart Factory Market", 2019

1 스마트공장 구축 동향

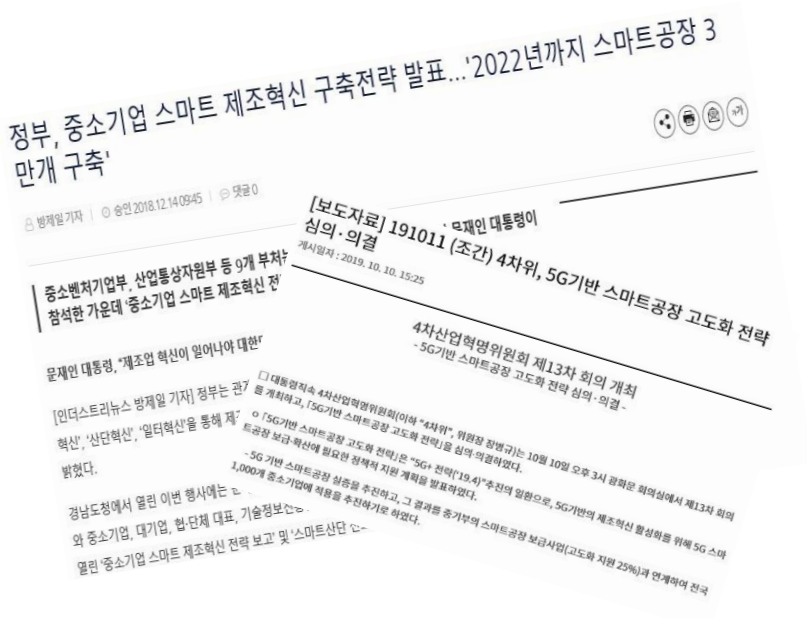
지멘스, 벤츠 등 글로벌 제조기업을 중심으로 생산성 제고를 위한 스마트화 추진

※ 지멘스는 독일 암벡에 위치한 공장에 디지털 트윈 기술 도입 및 하루 5,000만 건의 정보를 수집 분석하여, 불량률 0.0012%, 에너지효율 30% 제고 달성

정부는 스마트공장 보급, 고도화 정책을 마련하여, 국가 제조업 경쟁력 제고 노력 中

※ 중소기업 스마트제조 혁신 전략('18), 5G기반 스마트공장 고도화 전략('19) 등을 마련하며, **'22년까지 3만개 보급 추진**

[해외 스마트공장 구축 사례]



[스마트공장 정책 사례]

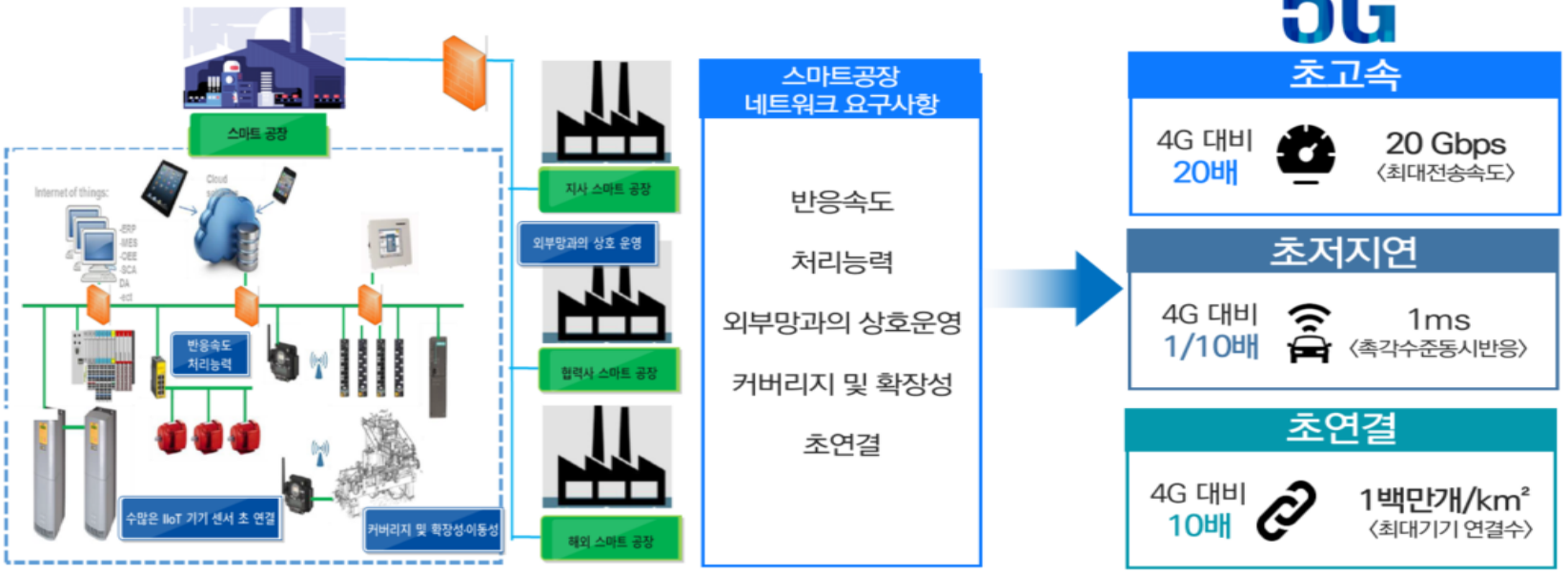
1 스마트공장 구축 활성화 배경

5G의 초고속, 초저지연, 초연결 특성은 스마트공장에서 요구하는 가용성, 연결성 지원 가능

※ 참고 : 안산 스마트제조혁신센터(데모공장) 內 5G 기술(SKT)을 활용한 스마트공장 서비스 운용 가능 환경 구축

포스트 코로나 시대, 비대면 작업의 필요성이 높아짐에 따라 '공장 디지털 전화' 가속화

※ 롯데칠성음료는 각 생산 라인별 설비 상태, 생산량, 진도율 등의 정보를 수집, 분석할 수 있는 모니터링 시스템과 실시간 제조 이력 관리 시스템 구축('20.6, 조선비즈)



1 스마트공장 구축 효과

공장 스마트화에 따른 인건비 절감, 생산성 향상이 가능하여, '리쇼어링(Reshoring)' 촉발

※ 리쇼어링(Reshoring) : 해외에 나와 있는 자국 기업이 국내로 다시 복귀하는 것을 의미

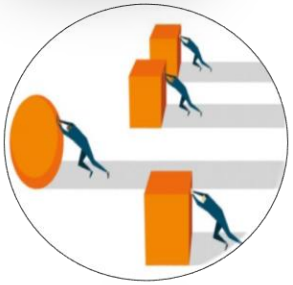
스마트공장을 도입한 중소기업의 경우, 생산성, 품질향상 등의 획기적인 성과 달성

생산원가 15.9% ↓

품질향상 43.5% ↑

납기 준수율 15.5% ↑

생산성 30% ↑

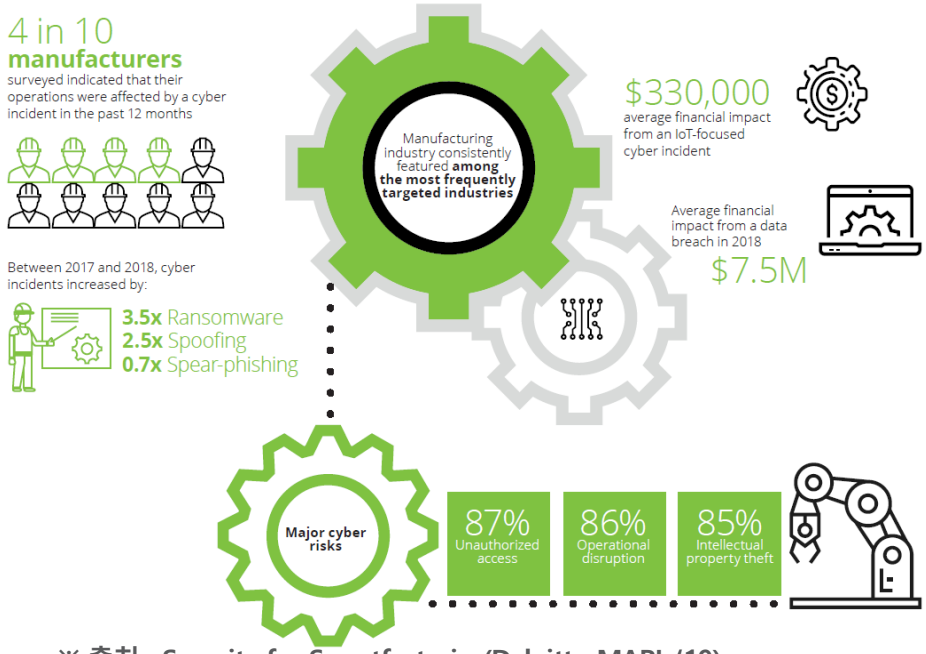


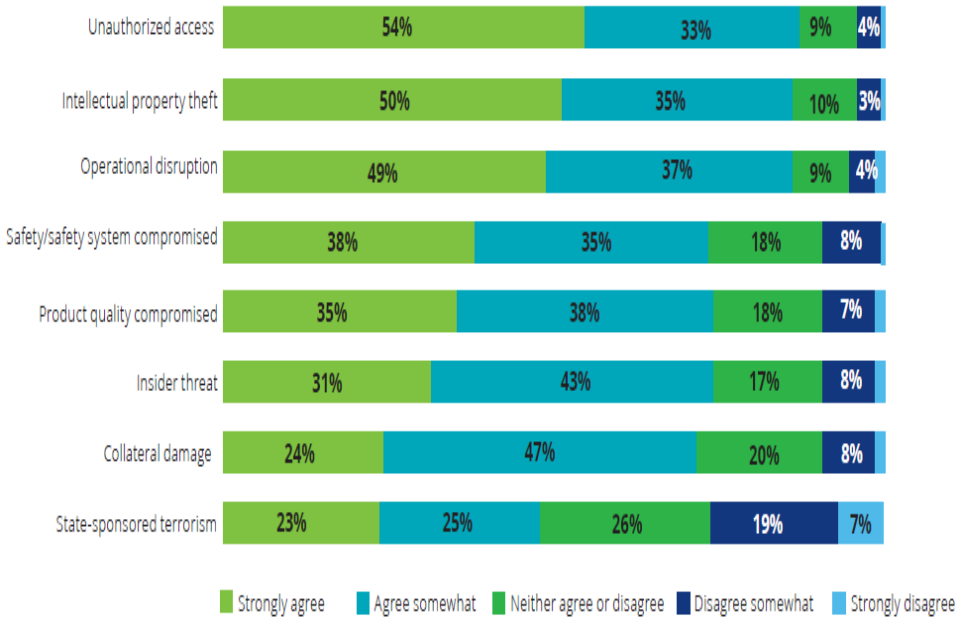
※ 출처 : 스마트팩토리 보급사업 성과분석('19, 중기부)

2. 스마트공장 보안위협 동향

2 한눈에 보는 스마트공장 보안위협

- 최근 1년간 사이버공격 피해 경험 : **40%**
- 사이버사고(1건 당) 평균 금전적 피해 규모 : **약 330,000 달러(약 3억 8천만원)**
- '17~'18년 사이버사고 증가율 : **랜섬웨어 3.5배, 스푸핑 2.5배, 스피어피싱 0.7배**
- 보안위협 유형 : **비인가자 접근 87%, 운영중단 86%, 지적재산권 탈취 85%**





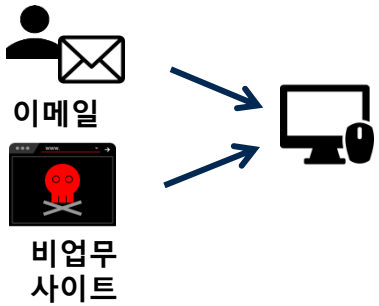
※ 출처 : Security for Smartfactories(Deloitte-MAPI, '19)

2 스마트공장 보안사고 사례①

노르스크 하이드로 랜섬웨어 감염 사례('19.04)

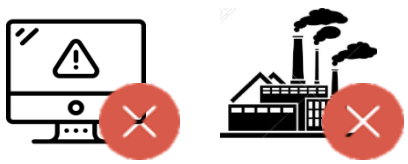
- **감염 경로** : 악성코드 유포 메일 열람, 비 업무 사이트 방문을 통한 랜섬웨어(록커고가) 감염
- **감염 범위** : 압출 성형(Extruded Solutions)공정 운영 이상 초래
- **피해규모** : 회사업무 중단, 회사 주식 3.4%하락('18년 매출 약 5,733억 원), 브라질 공장 부분 가동 중단
- **원인 및 보안문제점** : 액티브디렉터리 그룹/사용자 권한 설정의 취약점 혹은 관리자 계정의 취약점 보유
  IT 시스템과 생산정보시스템(공정 관련 시스템)의 연계 구간 보안 미흡

1 STEP 1. 랜섬웨어 감염



공장 내 근무자의 악성코드 메일 열람 /비 업무 사이트 방문을 통한 랜섬웨어(록커고가) 감염

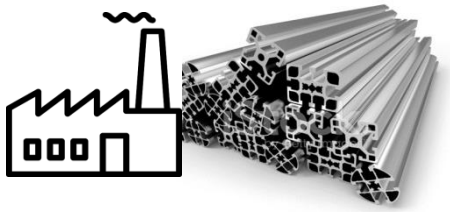
2 STEP 2. 업무 중단 초래



회사 홈페이지 다운, 자체 발전소의 일부 시설 가동 중단 등의 업무 중단 발생

→2차 확산 피해 대비 IT 시스템 사용자 접속 중단(긴급대응)

3 STEP 3. 생산공장 가동 부분 중단



브라질 공장의 부분적인 가동 중단 및 감염 사고 여파 확산

→ 전세계 알루미늄 가격 급등

2 스마트공장 보안사고 사례②

대만 반도체공장 TSMC 랜섬웨어 감염 사례('18.08)

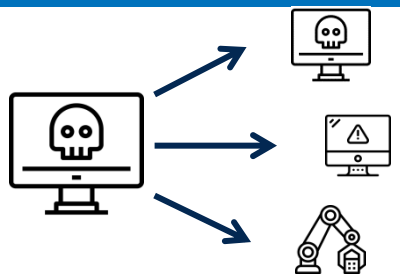
- **감염 경로** : 유지보수 업체 USB를 통해 랜섬웨어(워너크라이 변종) 감염
- **감염 범위** : 외부와 차단된 폐쇄망의 생산용 PC (1만대 이상 감염)
- **피해규모** : 48시간 공장 가동 중단으로 약 3,000억원(연매출 3%) 손해 발생
- **원인 및 보안문제점** : 유지보수 인력의 정보기기(USB 포함)에 대한 바이러스 검사 부재
  공장 네트워크 분리 미흡., SMB를 통한 파일 공유 허용 및 보안패치 미흡

1 STEP 1. 랜섬웨어 감염

USB 사용 시 별도 바이러스 검사 없이 감염된 SW설치, 랜섬웨어 감염

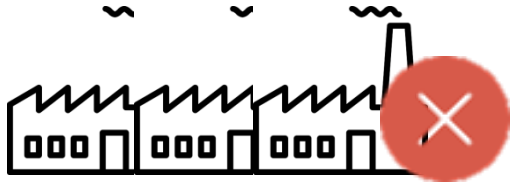
→생산용 PC 데이터 암호화/무결성 손상

2 STEP 2. SMB취약점을 통해 감염 확산



SMB 포트 취약점을 사용하는 이터널 블루 취약점을 통해 타이난, 신주, 대중 3개 공장으로 감염 확산

3 STEP 3. 생산공장 가동 중단



생산공장의 기기 1만대 이상 감염

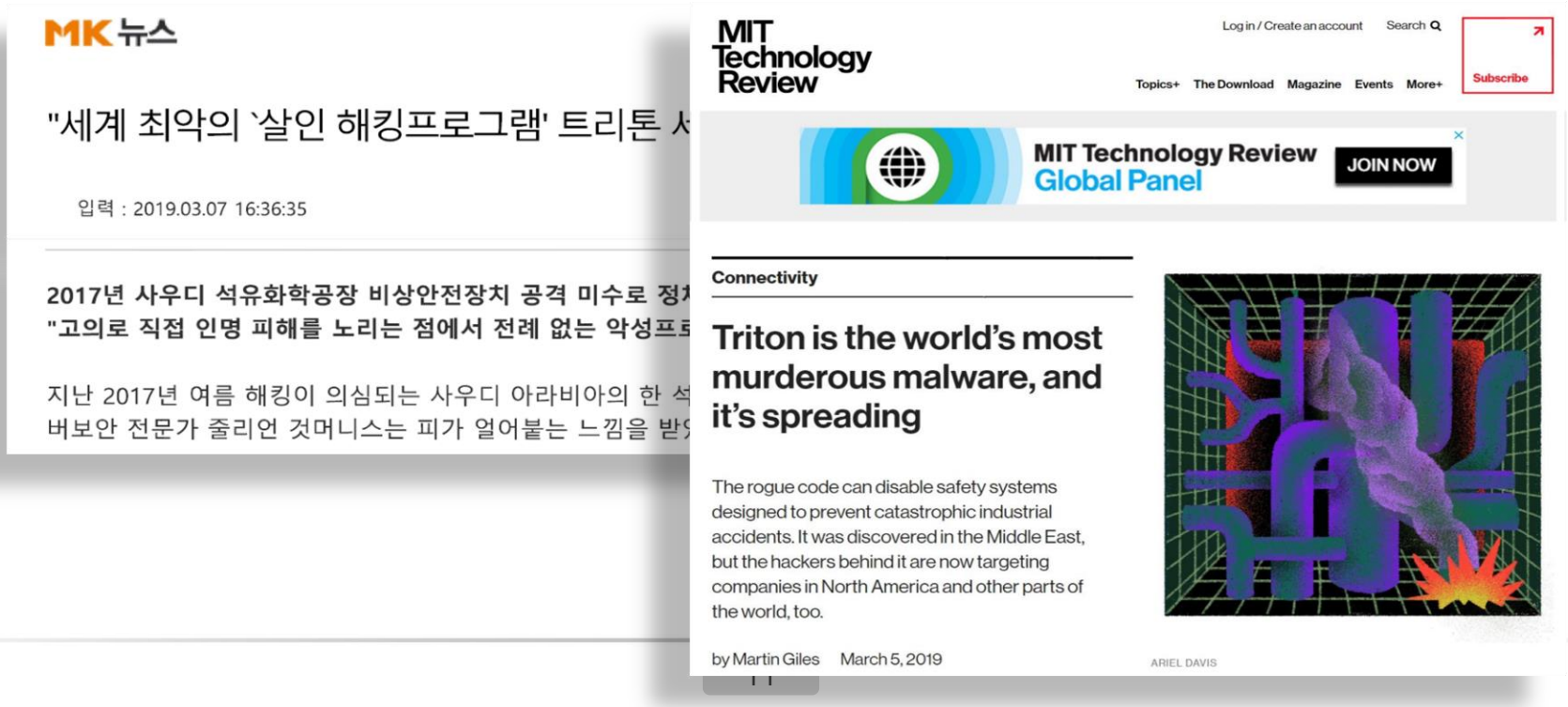
→이틀간 가동 중단

2 스마트공장 보안사고 사례③

- 파이어아이(Fireeye), 산업용 안전시스템을 공격목표로 삼는 악성코드 트리톤(Triton) 발견('17)
  - 슈나이더社의 일렉트릭 트리토넥스(Schneider Electric Triconex, 산업용 안전시스템)가 공격 타겟

※ 산업용 안전시스템 : 밸브와 터빈을 모니터링하고 감시하다 장애가 발생하기 전에 가동을 중단시키는 역할 담당

- 美 MIT, 트리톤 악성코드 전세계 확산(중동 → 북미 등) 추세 언급('19)



MK 뉴스

"세계 최악의 `살인 해킹프로그램' 트리톤 사

입력 : 2019.03.07 16:36:35

2017년 사우디 석유화학공장 비상안전장치 공격 미수로 정
"고의로 직접 인명 피해를 노리는 점에서 전례 없는 악성프로

지난 2017년 여름 해킹이 의심되는 사우디 아라비아의 한 석
버보안 전문가 줄리언 것머니스는 피가 얼어붙는 느낌을 받

MIT Technology Review

Log in / Create an account Search

Topics+ The Download Magazine Events More+ Subscribe

MIT Technology Review Global Panel JOIN NOW

Connectivity

Triton is the world's most murderous malware, and it's spreading

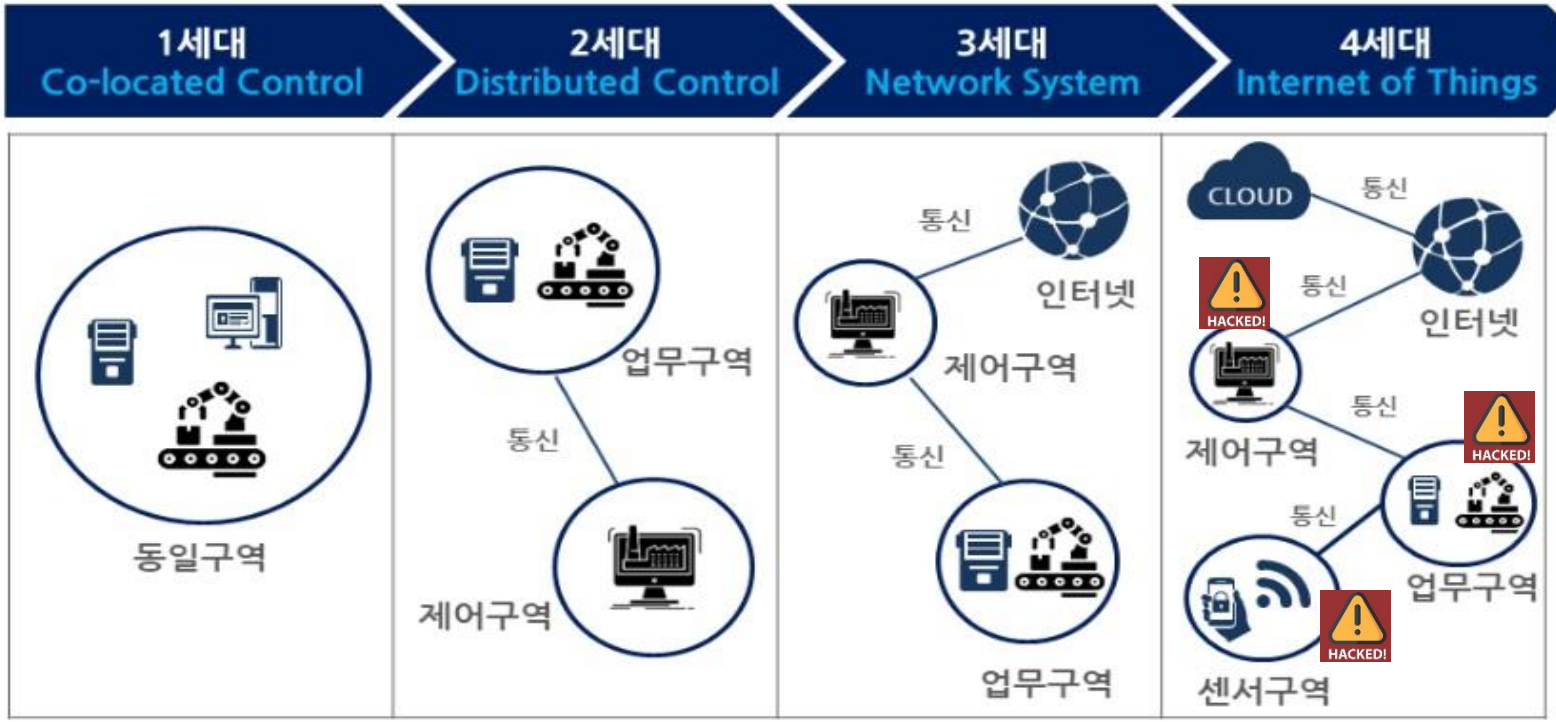
The rogue code can disable safety systems designed to prevent catastrophic industrial accidents. It was discovered in the Middle East, but the hackers behind it are now targeting companies in North America and other parts of the world, too.

by Martin Giles March 5, 2019

ARIEL DAVIS

2 왜 이런 사고가 계속 발생하는 걸까?

- PLC, 로봇 등 생산설비가 인터넷, 클라우드에 직접 연결 → **공격 경로 多**
- OT 전용 보안대응 솔루션 미설치, 생산담당자의 낮은 보안 이해도 → **공격난이도 下**
- 경쟁사 매출 하락, 산업기밀 유출 → **공격 유발 동기 多**



2 스마트공장 보안이 어려운 이유?①

스마트공장은 IT 환경과 다른 OT 환경 보유 → 기존 보안 접근 방식 전환 필요

구분	IT	OT
시스템	▸ 전사적자원관리(ERP, PLM), 공급망 관리(SCM), 생산관리(MES, WMS) 등	▸ HMI, PLC, 센서, 액추에이터 등
통신	▸ 표준 통신 프로토콜 이용	▸ 산업용 프로토콜, 표준 통신 프로토콜 혼용
역할	▸ 데이터 또는 기업자원 관리	▸ 기계 제어
사용기간	▸ 3~5년	▸ 15~20년 이상
패치(보안 패치 포함)	▸ 패치 등 유지보수 용이	▸ 패치 등 유지보수 어려움
OS	▸ 범용 OS 사용(윈도, 리눅스)	▸ 전용 OS/실시간 OS 사용
네트워크 요구사항	▸ 전체 성능(Throughput)에 초점, 응답의 신뢰성이 중요하며, 일부 통신지연 허용	▸ 견고성 및 실시간 요구사항 중시 ▸ 응답시간이 중요하면 통신지연 불허
사고영향	▸ 사고발생 시 업무 불편 및 지연 등 상대적으로 미미한 경제적 피해	▸ 사고발생 시 산업현장 운영 중단으로 인한 피해 및 대규모 물리적, 경제적 피해 발생
위험관리 목표	▸ 데이터의 기밀성, 무결성	▸ 작업자 안전 및 시스템 가용성
보안 우선순위	▸ 기밀성〉무결성〉가용성	▸ 가용성〉무결성〉신뢰성
보안인지	▸ 공공/민간 보안 중요성 인지	▸ 일반적으로 보안에 관해 잘 모름
안티바이러스 제품	▸ 일반적, 광범위하게 사용	▸ 비-일반적, 일반 IT 제품 적용하기 어려움

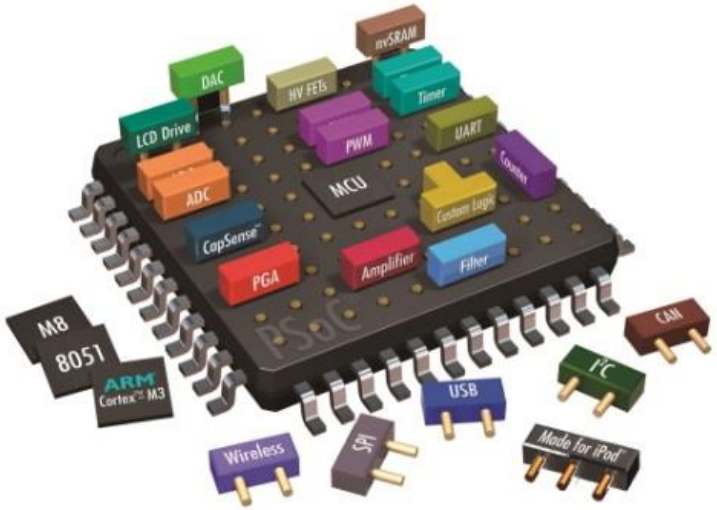
※ 출처 : 주요국 스마트공장 보안 동향 분석 및 시사점(KISA, '19)

2 스마트공장 보안이 어려운 이유?②

- TCP/IP가 아닌 **제조설비(미쓰비씨, LS산전 등) 전용 통신프로토콜**(Modbus 등)을 사용하여, **TCP/IP 기반 IT 보안솔루션 적용 어려움**

※ Modbus 프로토콜은 보안을 고려하지 않은 설계로 평문 메시지들이 암호화 없이 그대로 전송되며, 인증 없는 통신이 수행되므로 메시지 위변조와 같은 중간자 공격과 재전송 공격에 취약(Modbus IDA, '13)

- RTOS 등 **임베디드 형태(특정 기능만 수행하도록 설계)의 SW**가 제어설비에 **탑재**되어, **보안SW 추가 설치와 고성능의 IT 보안기술 적용에 한계**



2 스마트공장 보안이 어려운 이유?③

- **생산설비의 교체주기가 10년 이상으로 사후 보안이 필수적임에도 불구 보안성이 강화(보안 내재화)된 주기적 생산설비 도입 어려움**

  - 중소기업의 경우, **스마트공장 보안을 전담할 수 있는 인력, 보안 투자에 한계**

※ ’17년 기준 전체 중소기업 수는 630만개이며, 전체 기업수의 99.9% 비중을 차지(‘19, 중기부)

3. 스마트공장 보안위협 대응 방안

3 스마트공장 보안위협 대응 방안 ①

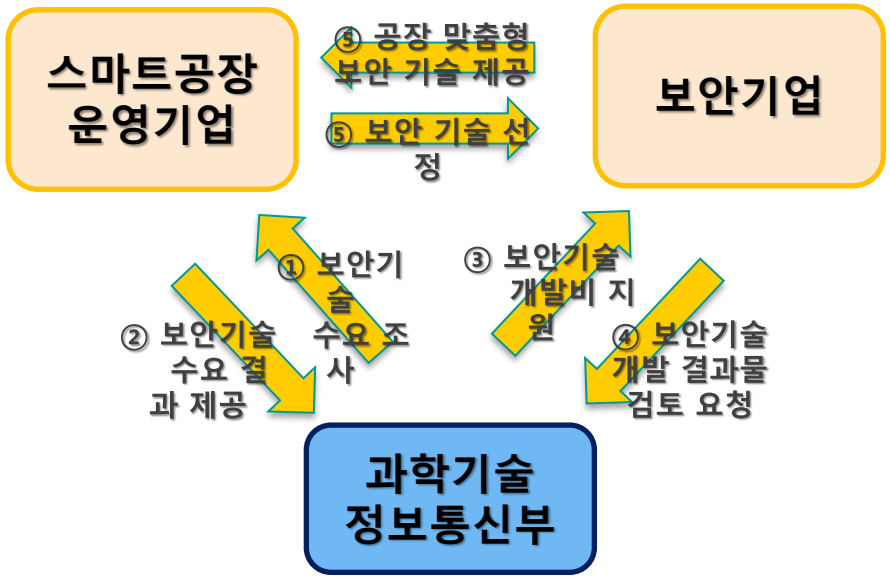
스마트공장 보안위협 대응 체계 구축

- 스마트공장 보안위협 정보 수집을 위한 제조 보안빅데이터 시스템 구축
- 스마트공장 보안사고를 분석하고, 전담 대응하는 제조Cert 구축
- 스마트공장 이해관계자(제조설비사, 스마트공장 운영자 등)로 구성된 제조 ISAC 설립

①보안위협 탐지 ② 보안위협 정보 수집 ③보안위협 분석 및 대응 ④위협대응 결과 공유

3 스마트공장 보안위협 대응 방안 ②

- 스마트공장 운영 기업과 보안업계간 매칭을 통한 맞춤형 보안기술 개발
- 생산(OT)환경을 이해하고, IT 보안 지식을 갖춘 '스마트공장 보안 인재' 육성



3 스마트공장 보안위협 대응 방안 ③

- 범부처 스마트공장 보안 협력 거버넌스 구축 및 제조보안전담 기관 설립
- 스마트공장 관련 제도 內 보안부문 반영 → 보안내재화 및 사후보안 촉진

과학기술정보통신부

- 스마트공장 보안사고 대응 총괄
- 스마트공장 보안 정책 수립 지원
- 스마트공장 보안 시험 평가 공통기준 개발

기술,정책 지원

중기부, 산업통상자원부 등

- 스마트공장 보안사고 대응 지원
- 스마트공장 보안 정책 수립
- 기존 법제도 내 스마트공장 보안 기준 반영 지원 및 운영

스마트공장 관련 제도

- 스마트공장 수준확인제도
- 안전보건진단
- 산업시설위험성 평가 제도

스마트공장 보안강화 지원

제조보안전담 기관

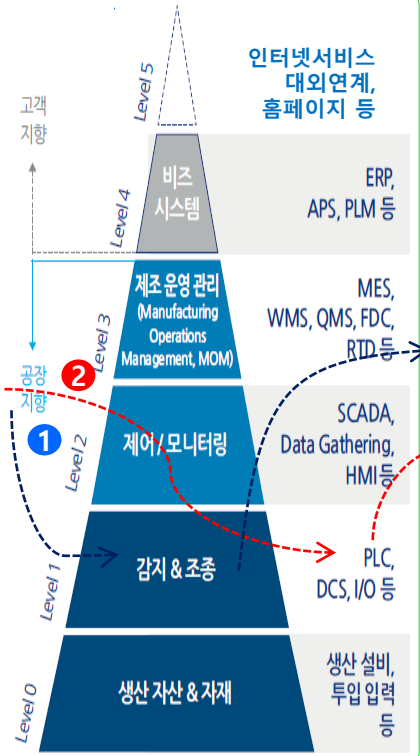
- 스마트공장 보안위협 모니터링
- 스마트공장 보안위협 분석 및 대응
- 스마트공장 보안시험 평가 지원

스마트공장 보안강화 지원

3 한국인터넷진흥원의 노력 ①

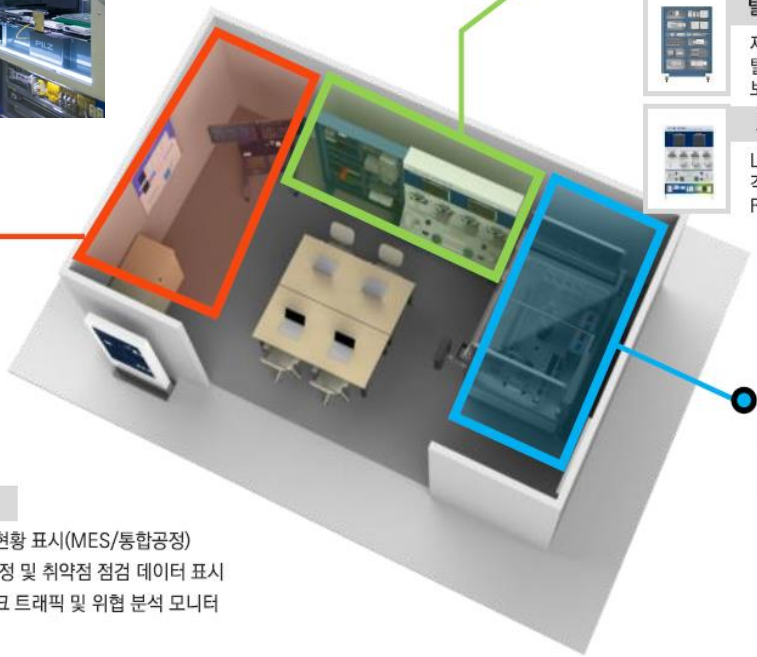
스마트공장 제어영역(OT) 대상 보안취약점 점검을 통한 보안모델을 개발하여, 스마트제조 분야 선제적 보안성 강화 지원 및 보안 내재화 확산 기반 마련

공격 위치(경로)	공격기법	공격대상	보안위협
외부 인터넷을 통한 위협 공장 업무영역을 통한 위협 (공정,업무,인터넷 등) NW를 통한 위협 산업제어시스템을 통한 위협 인력, 노후설비에 의한 위협 물리적 접근, 포트, 지원설비 통한 위협	▪ 랜섬웨어 감염 메일 전파 ▪ Supply chain 공격 ▪ 업무PC를 악성코드에 감염시킨 후 HMI 공격 ❶ NW 비인가 장비 연결, 공정 제어망 Dos 공격 ❷ NW Packet 도청 후 데이터 조작 (modbus 명령어 코드) ▪ 사용자 실수에 의한 설비전원 off ▪ USB를 통한 비인가 SW 설치	시스템/데이터 ❶ 네트워크/ 네트워크설비 ❷ 생산설비/데이터	▪ 악성코드 감염 ▪ 공정 레시피 유출 ▪ 공정 데이터 훼손 및 사용불가 ❶ 제어 및 수집 정보 송.수신 차단 ❷ 제어 장치 메모리 훼손 ▪ 현장 장치 운영 중단 ▪ 현장 장치 오동작



3 한국인터넷진흥원의 노력 ②

스마트공장 제어설비 대상 보안테스트가 가능한 '보안리빙랩'을 구축하여, 보안이 내재화된 스마트공장 장비 확산 유도 및 국내 보안기술 개발 경쟁력 제고



보안테스트 ZONE
Wall을 활용한 제어장비 보안 컴플라이언스 준수여부 분석, 제어네트워크 분석(퍼징테스트 등) 지원

탈부착월

제어장비(PLC, HMI)와 산업용 네트워크 장비 탈부착을 통해 스마트 공장 환경 축소 구현한 보안테스트 Wall 구현 및 설치

고정월

LS산전, 지멘스, 미쓰비씨 PLC를 기본 부착하고, 각 PLC별 제어프로토콜(S7Comm, Modbus/TCP, RAPIEnet)간 스위칭이 가능하도록 구현

리빙랩 관리 ZONE
보안리빙랩 관리 및 운영을 지원하는 서버로 구성

상태 모니터

- 스마트공정 현황 표시(MES/통합공정)
- 모의 침투 과정 및 취약점 점검 데이터 표시
- 제어 네트워크 트래픽 및 위협 분석 모니터

위협시연 ZONE
고정 Wall 내 PLC 해킹 등을 통해 비정상 행위 시연

모의 침투 시나리오

- 대만 TSMC 사례(USB)
- 노르스크하이드로 알루미늄 공장 해킹(랜섬웨어),
- 우크라이나 정전사례(랜섬웨어) 등의 모의침투를 통한 오작동

KISA 한국인터넷진흥원
KOREA INTERNET & SECURITY AGENCY

감사합니다

Thank You For Listening