Cyber Security Conference 2021

SAMSUNG SDS

OT보안 트렌드 및 국내·외 현황

최민화 상무 KPMG

AGENDA

Ⅰ. 개요

1. 생산환경의 디지털화
2. 디지털 위험관리
3. DX 환경에서의 공급망 관리

Ⅱ. 국내·외 현황

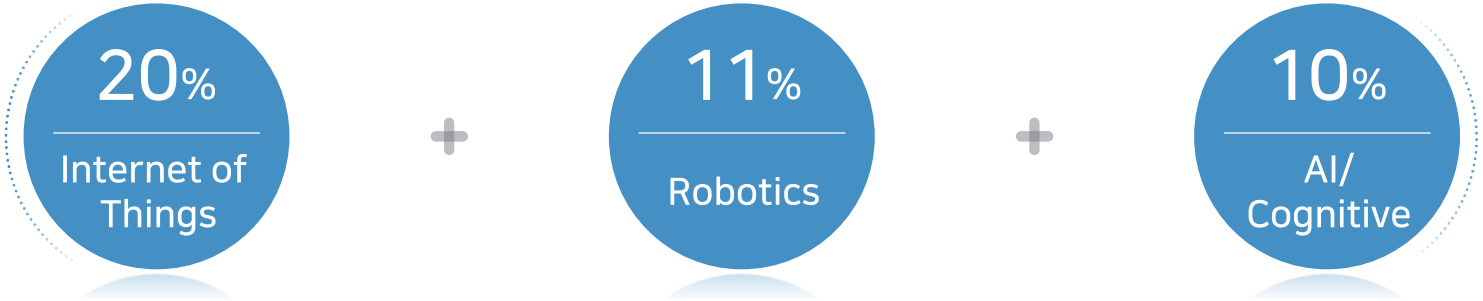
1. 국내 현황 및 현장점검 결과
2. 국내 타사 사례
3. 국내외 OT보안 인증 추진현황
4. OT보안 인증 로드맵
5. 국내·외 규제 현황

Ⅲ. 국제표준 OT체계 도입 시 기대효과

생산환경의 디지털화

4차 산업 도래에 따라 Industry 4.0, DX 등 생산환경의 디지털 전환이 가속화되고 있습니다.

“ 향후 5년간 비즈니스 변화를 주도할 주요 기술 ”



비용 대비 新가치창출

- 스마트공장 도입을 통해 맞춤형 생산으로의 패러다임 변화
- 비즈니스 소프트웨어와 컴퓨터 인텔리전스의 융합으로 비즈니스 프로세스의 빠른 속도, 낮은 비용, 오류 감소를 실현

신기술 도입 가속화

- 로봇과 자동화 고도화로 생산성 제고, 빅데이터의 실시간 축적/분석/ 패턴화로 유연한 생산 극대화
- AI-ML, Bigdata, IoT, Cloud, 무선 등 기술 변화는18C 산업혁명보다 10배 빠르고 300배 크며, 3,000배 파괴력(Source: McKinsey)

네트워크 연결성 확대

- 오프라인과 온라인이 융합하는 초연결 사회로 새로운 성장과 가치창출의 기회가 더욱 증가할 전망
- 기업 내부의 IT영역과의 연계 뿐 아니라, 단위지역 MES가 모든 국내외 공장, Supply Chain, 판매, 유통, 마케팅, 온라인으로 연결되고 확장 지속

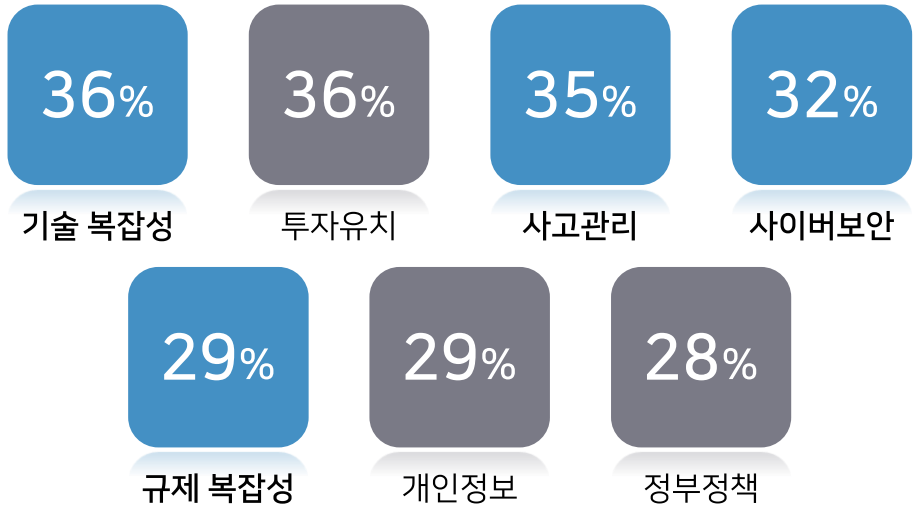
공장 데이터 폭증

- AI-ML, Bigdata 등 DX추진으로 새로운 공정 데이터 생성 및 재디지털 데이터
- 하루에 생성되는 산업 데이터량은 482억 GB으로 생산공정 데이터 폭증과 수율 레시피 등 신규 공정기밀의 생성과 집중화 현상(Source: McKinsey)

디지털 위험관리

산업환경에서의 새로운 디지털 위험을 포함한 산업리스크 관리를 위한 新산업보안체계 (OT보안) 수립의 필요성이 증가하고 있습니다.

DX 환경의 리스크 요인



빠르게 변화하는 기술환경에서 새로운 시장 개척 및 수익 창출을 위해서는
신규 리스크 사전 점검 및 최소화 필요

新산업보안체계 수립의 필요성

- DX 추진 시 부재 업무, 중복 업무 식별 및 최적화
- 신기술 도입 시 필요한 DX 수용성 높은 디지털 인프라 기반 마련
- DX 환경에서 디지털 사고 시 피해 최소화 및 신속한 생산 복귀
- DX 이행에 따른 신규 디지털 생산기밀 식별 및 유출방지

DX환경에서의 공급망 관리

코로나19로 변화된 업무 현실, 디지털혁신 가속화, 기업 리스크 변화로 공급망의 융합보안이 더욱 필요합니다.

산업현장의 디지털화, 자동화, 무인화로 기업의 디지털 영역 확산, **사무영역 넘어 산업영역까지**	• 코로나19로 온라인 공간에서의 기업 업무 처리 및 소통으로 **더 많은 연계성과 정보 흐름 발생** • 재택근무, 원격업무 증가 및 풀(Pool) 형태의 인력 채용 변화로 인한 **TF식 조직구성 및 업무환경 변화**	❶ 기업 외부의 인력 Pool, 수많은 공급망, 디지털혁신으로 연계되는 **다양한 정보 수요처를 지원 필요**
새로운 디지털 환경에서 발생하는 리스크 관리 요구 증가, **융합보안**[1]	• 기업 내부 정보를 보호를 위해 기존 IT보안 정책과 개인정보보호 활동만으로는 **기업 리스크관리 어려워짐** • **산업현장에서도 원격지**의 생산기계, 설비 접속 및 조작, 유지보수 등의 **업무수행을 허용할 수 밖에 없게 됨**	❷ 기업들은 새로운 디지털 업무 환경에 발맞춰 **기업 보안의 의미 재정의 필요**
기업이 추진하고 있던 디지털 혁신 가속화로 새로운 **융합보안체계** 마련해야	• **'금지와 규제'하는 기존 보안**에서 산업현장, 공급망 포함한 기업목표를 **'지원 및 보호'하는 융합보안으로 전환 필요** • 글로벌 하이테크 기업들은 글로벌표준 기반 융합보안 관리체계를 도입, **자사와 관련된 공급망에도 동일한 수준의 융합보안인증체계 취득 요구**	❸ 기업이 보호해야할 기밀 정보의 범위를 자사의 산업현장, 공장 내 협력업체와 **공급망 영역까지 명확하게 파악하여 보호 필요**

[1] 융합보안 : 기업의 보안 영역을 자산의 모든 인력, 디지털 정보, 디지털 자산과 함께 자사와 연계되는 공급망의 인력, 정보, 자산을 관리 대상으로 확대하는 보안 영역

국내 현황 및 현장점검 결과

프로젝트 중 확인한 국내 현황은 DX 추진 과제들이 기업의 리스크 증가로 나타나는 경우가 적지 않았습니다.

국내 기업의 DX 목표

디지털화, 자동화, 무인화로 디지털화된 생산 및
업무 환경으로 국내・외 시장 점유율 향상

高품질 高부가가치를 요구하는 높아진
소비자 눈높이에 맞춘 高신뢰성 및 高기능 제품 판매

고객 트렌드 및 Needs별 전용화 제품 대응으로
최단 시간 內 고객 맞춤 영업

고성능의 디지털화된 생산제조환경으로 제품 다양성
및 고품질의 신제품을 출시하여 사업확대

But

국내 기업의 현장 점검 결과

- Global MES 추진 및 공급망 연계 확대로 취약한 보안지점에 전체 보안 수준 수렴 **공격 가능한 경계영역 보안-백도어 발생**
- 원격 및 공정영역에서 디지털 공격에 취약한 설정/프로토콜 사용으로 인한 **설비 통제권 상실 및 사고 발생 위험 존재**
- 산업현장 내 불필요한 통신 과다/실패로 **제품 품질 저하 및 불량률 증가 위험**
- 총 디지털 자산 중 50~70%가 미식별되어 **OT보안 정책 적용 및 관리가 불가하여 사고예방이나 사고 시 피해 대응 어려움**
- 재택근무, 원격업무 등 연결접점 증가로 신규 인터넷 접근 경로를 통한 **기밀 유출 위협 우려**

국내 타사 사례 (1/2)

2017년부터 국내 기업은 DX 추진에 맞추어 Risk 관리를 위해 체계적인 개선방안을 수립하고 있습니다.

A 화학

- 공장 중단 사고 발생(악성코드)에 대한 OT보안 취약점 점검과 시스템 재설치 및 긴급 네트워크 분리 실행
- OT보안 아키텍처 표준 수립 진행 예정

B 전자

- 컨설팅을 통해 OT보안 아키텍처 모델 수립, 자사 표준 적용 기술 선정
- 국제표준 OT아키텍처로 국내 네트워크 구조 변경
- 본사의 OT보안 전담 팀 구성 후 전사 확산 시작

C 제어사

- 컨설팅을 통해 OT보안 아키텍처 모델 수립
- 전국 제어영역 가시성 확보 및 이상징후 탐지를 위한 제어시스템 보안 모니터링 센터 구축 계획 수립 중

D 그룹지주 및 자회사

- 컨설팅을 통해 계열사 OT보안 강화를 위한 OT보안 표준 아키텍처, 보호 기술, OT보안 조직 및 거버넌스 개선 방안수립
- 주요 DX 추진 계획 기준으로 OT보안체계 예산안 수립

E 반도체

- IT/OT 융합보안 표준 아키텍처 수립
- 자산 별 기준 솔루션, 조직/업무안 수립하여 보안 조직 및 인력 증원

F 반도체

- OT보안 인프라 및 요소기술 정의를 위한 마스터플랜 및 후속과제 수립 완료
- 마스터플랜에 따른 OT 솔루션 도입 예정

국내 타사 사례 (2/2)

제조업체 중에서 공급망을 포함한 통합 리스크 관리를 고민하는 곳은 국제 표준 인증 획득을 통해 자사와 공급망의 디지털 환경에 필요한 OT보안 성숙도(조직, 거버넌스, SDLC 등)를 갖추도록 요구하고 있습니다.

G 화학

- 생산 네트워크 보안 강화 방안 수립
- OT보안 국제표준기반의 네트워크 분리 완료
- 표준 기술 수립에 대한 OT 솔루션 도입

H 화학

- OT 인프라 진단 및 자산보호방안 도출, 보안 아키텍처 모델 수립 예정
- 안전한 OT보안 인프라 및 요소기술 정의를 위한 마스터플랜 및 후속과제 수립 예정

I 제어 설비사

- 자사 제품의 OT보안 IEC 62443 4-1, 4-2 인증 취득 착수
- 인증 요건인 OT보안 아키텍처를 수립하여 공장 인프라 개선 및 전략 수립
- 국내외 개선 모델 확대 적용 계획 수립

J 반도체

- 3년간 안전한 제조 생산 환경을 위해 제품의 정보흐름과 관련된 모든 현장 환경(Supply Chain 포함)을 평가하는 CC-Site Certification 인증 취득
- 최고 수준 EAL 등급을 취득하였으며 Supply Chain에 포함되는 계열사/협력사에 동일 수준의 인증 취득을 권고

K 반도체 1차 벤더

- S사의 Supply Chain에 포함되는 업무 진행을 위해 설비 환경에 CC-Site Certification 인증 취득
- 컨설팅을 통해 단시간에 보안성 향상과 S사의 물량을 성공적으로 확보하였으며 신규 공장도 인증 계획

L 설비 제조사

- 글로벌 제어 설비 고객인 R사가 OT인증 획득 요청
- 컨설팅을 통해 IEC 62443 인증 체계 사전 준비 진행
  - 국제표준 기준 OT 네트워크 설계, 조직 업무, 인프라 구조 개선

국내외 OT보안 인증 추진현황

IEC 62443 등 국제표준 기준 OT보안 인증을 획득하는 것은 DX 추진 체계 수립에 필요한 고려사항을 추진하고 단계별 목표를 달성하기에 가장 효과적인 접근방법 중 하나입니다.

新 산업보안 고려사항

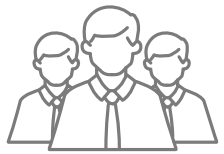
제도 산업 표준 작성	 안전한 디지털 신기술 도입 환경 제공	 핵심 공정기밀 보호	
보안 거버넌스 체계 수립	 책임추적성 명확화	 업무/절차 공식화	 업무 중복·부재 개선
시스템 구축	 이상징후 사전 탐지 및 사고예방	 사고 피해 및 복구시간 최소화	 디지털기반 공정최적화

글로벌 제조사의 OT보안 인증 동향

벤더사	인증 대상 (프로세스/제품)		인증내역	인증 일자
SIEMENS	제품	SIMATIC PCS 7	IEC 62443 3-3	2019년 11월
	프로세스	제품 공급업체 인증	IEC 624434-1:2018	2019년 09월
	제품	Scalance XC-200 Family	IEC 62443-4-1:2018 IEC 62443-4-2:2019	2019년 11월
Rockwell Automation	제품	ControlLogix 5580 Controller Family	IEC 62443-4-1:2018 IEC 62443-4-2:2019	2019년 04월
	프로세스	시스템 통합업체 인증	IEC 62443-2-4	2019년 10월
	프로세스	제품 공급업체 인증	IEC 62443-4-1:2018	2021년 01월
Cisco	제품	Cisco Catalyst IE3x00 Rugged	IEC 62443-4-1:2018 IEC 62443-4-2:2019	2019년 07월
HMS Networks	프로세스	제품 공급업체 인증	IEC 62443-4-1:2018	2020년 10월

OT보안 인증 로드맵

최근 많은 제조사들은 IEC 62443, Industrial Site CC 등 OT보안 인증체계를 도입하기 시작하였습니다.



자산 소유자 · 서비스 제공자 · SI업체

네트워크 분리 및 후속 과제 적용 시 인증 취득을 위한
기초 요구사항(FR) 및 필수 요구사항 충족

기초 다지기

OT보안체계 및
아키텍처 수립

네트워크 현황진단 및 안전한
스마트공장 기준으로 현장 적용

인증 취득을 위한 필수 요구 사항 by IEC 62443
(자산 식별 및 자산목록 최신화 네트워크 경계 분리 등)

통합프로세스 보안
(IEC 62443-2-1, 2-4, MIL>=2,3)

제어시스템 보안
(62443-3-3)

공정제품개발 프로세스 보안
(IEC 62443-4-1, MIL>=2,3)

제어설비 부품(컴포넌트) 보안
(IEC 62443-4-2, 62443-3-3)

성숙, 고도화

2년 후 재점검을 통한
수준확인 및 보정

제품 공급자

국내·외 규제 현황

생산환경 디지털화에 따라 한국을 포함한 각국은 표준과 법적규제를 통해 기업과 조직의 OT보안 수준 강화를 요구하고 있으며, 국내 제조사의 제품 또한 규제 혹은 신규 구매조건 대상에 포함될 것으로 예상됩니다.

16개 산업 산업보안 통제 법제화

- 미 대통령 행정명령 EO 13636으로 화학, 에너지, 의료, 제약, 바이오 등 16개 산업의 기반 시설 보안 및 안전 강화를 위한 **대통령 행정명령 (2013) 발표**
- 사이버 보안 강화법(Cyber Security Enhancement Act) 법제화(2014)

산업제어보안 KS국가표준 신규 제정

- 2021 KISA, 주요정보통신기반시설 취약점 평가 제어시스템 항목 강화
- 산업제어시스템 보안 KS 국가표준 제정
  - 2020.4 KS X IEC 62443-4-2(Component)

중국 "사이버 보안법" 시행

- **중국 "사이버 보안법(CSL)" 시행**(2019) 및 재중 한국기업들의 보안등급 의무화
- 사회 기반 시설에 대한 보안 강화
- 네트워크 운영을 보호하는데 초점을 맞추며, 국가안보와 공익에 영향을 미치는 **중요정보 취급에 주력하여 네트워크 안전, 핵심 정보인프라 보호, 법률 책임 등의 내용이 포함**

발전, 화학플랜트 준공 시 제3자 산업보안점검 법제화

- **유럽, 중동 등 제3자 Inspection 준공조건 강화를 통한 OT보안 규제, 처벌, 벌금 강화**
- 공정 ICS, 서비스, ICT 제품 보안 강화를 위한 ENISA "사이버보안법" 시행(2019)
- 에너지 공급, 정보 통신 네트워크를 포함한 핵심 사회기반 시설을 중심으로 "사이버 보안 인증 체계" 준비 중

Industry 4.0, DT 로 인한 스마트팩토리 산업 변화에 대한 **그룹 차원의 신속한 대응(Agility) 필요**

국제표준 OT체계 도입 시 기대효과

IEC62443 및 Industrial Site CC 프로그램을 이용하여 기업의 스마트팩토리 전환 기반을 마련한다면
디지털 Risk 에 대한 비용 효과적인 관리 수준 설정과 지속적 향상을 통해 DX추진과 확대를 지원 가능합니다.

4차 산업혁명에 따른 **기술/비즈니스 환경 변화의 대응**

- Digital 공정데이터의 수집, 전달, 교환, 가공에 효과적인 **DX 작업 영역 제공**
- 신기술 도입 시 필요한 **인프라 구성 및 변경비용을 최소화**
- 디지털 자산, 데이터흐름, 공정이벤트, 공정가용성 확보(안) 수립으로 **DX 과제 추진을 지원**
- Value Chain 프로세스 혁신으로 새로운 Cyber Risk 통제 필요 시 **중복/부재 업무 파악으로 효과적 업무 지원**

Cyber Risk 영향에 따른 **보안 패러다임의 변화 대응**

- 조직의 전략적 비전 달성/지원을 위한 **'비즈니스 기반 新산업보안 로드맵' 으로 무장**
- 기업의 사업 목표 달성을 위협하는 Cyber Risk 대응을 위한 **기업 전 직원의 '디지털 기반 보안/안전 역량'의 확보**
- Digital 및 Cyber Risk 으로 인한 사고 예방 및 신속한 생산 복구를 통한 **기업 재무적 위험 최소화**
- 파괴적 신기술(Disruptive Tech) 등장에 따른 **보안 위협 양상의 변화에 신속한 대응**

만약 경영진 주도의 新산업보안 체계를 내재화 한다면, 더 많은 규제가 출현할 수록 경쟁사 대비
새로운 시장에 대한 경쟁력을 확보하고, 국내외 신규 시장 진출과 DX 혁신 추진에도 비용을 절약될 것으로 예상합니다.

Thank you

SAMSUNG SDS