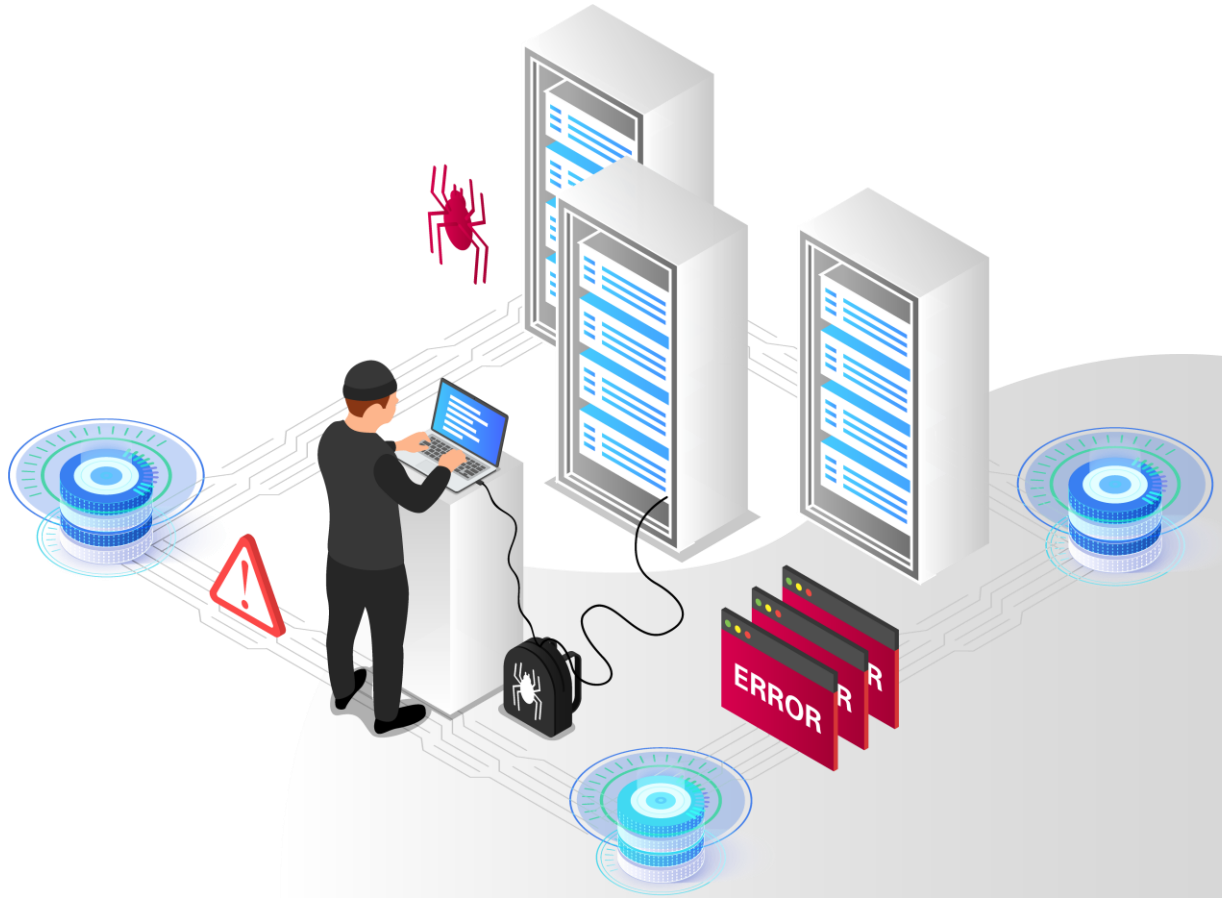
OT 설비(PLC) 모의해킹 사례

2021. 5.

LG CNS RED팀 신성훈 선임



LG CNS

Contents

OT 설비(PLC) 모의해킹 사례

1. OT 설비 모의 해킹 범위

생산계획 및 실행을 담당하는 IT시스템 외에도, 제품 생산 및 제어를 위한 PLC 및 이에 연결된 시스템을 포함하여 수행

IT 보안

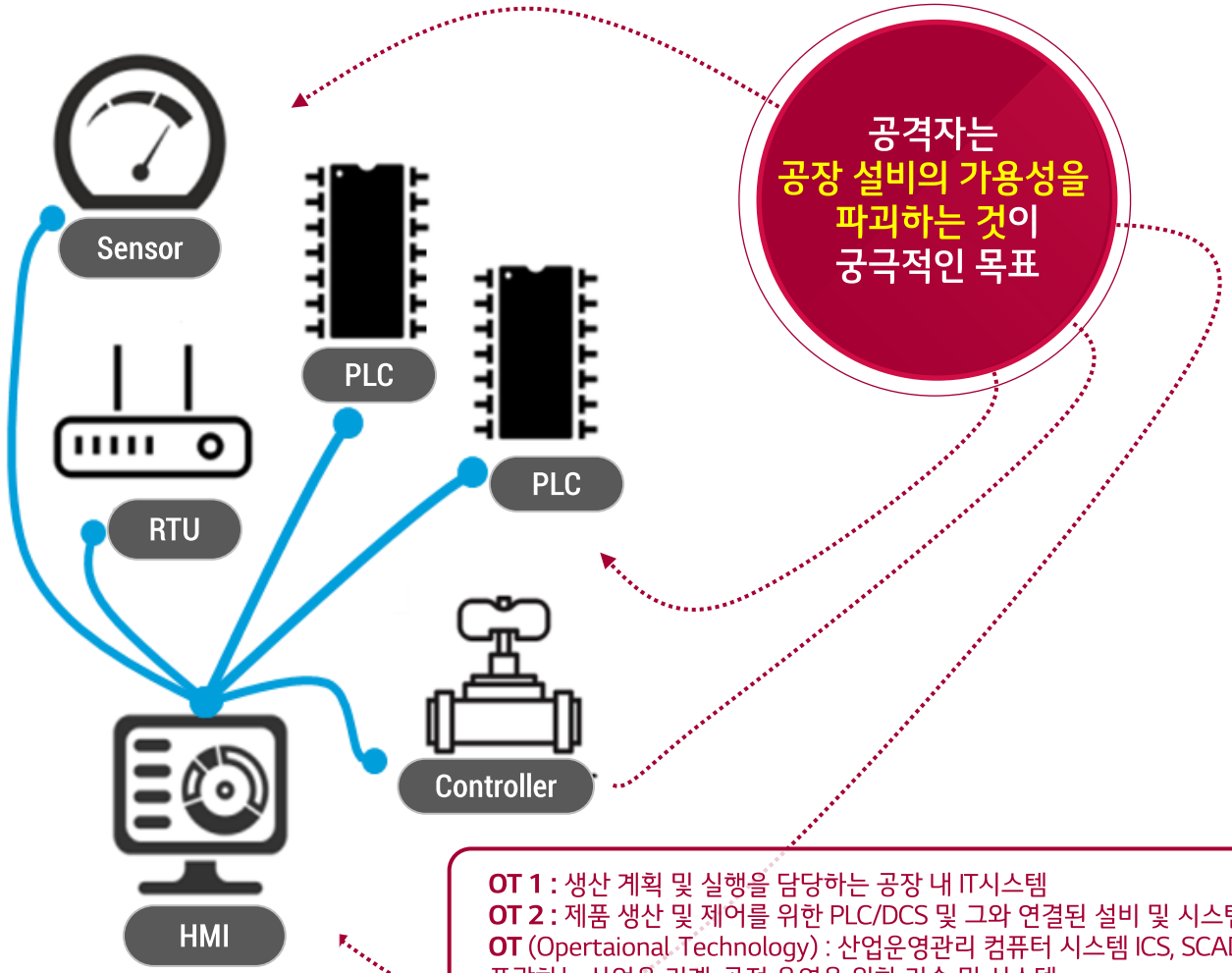
- DMZ망 (웹서버)
- Lv 5 — OA망 (사무용 서버, PC)

OT 1

- 산업 DMZ — 완충영역 (Historian, 공용서버)
- Lv 4 — 공장망 (생산 서버, 공장PC)

OT 2

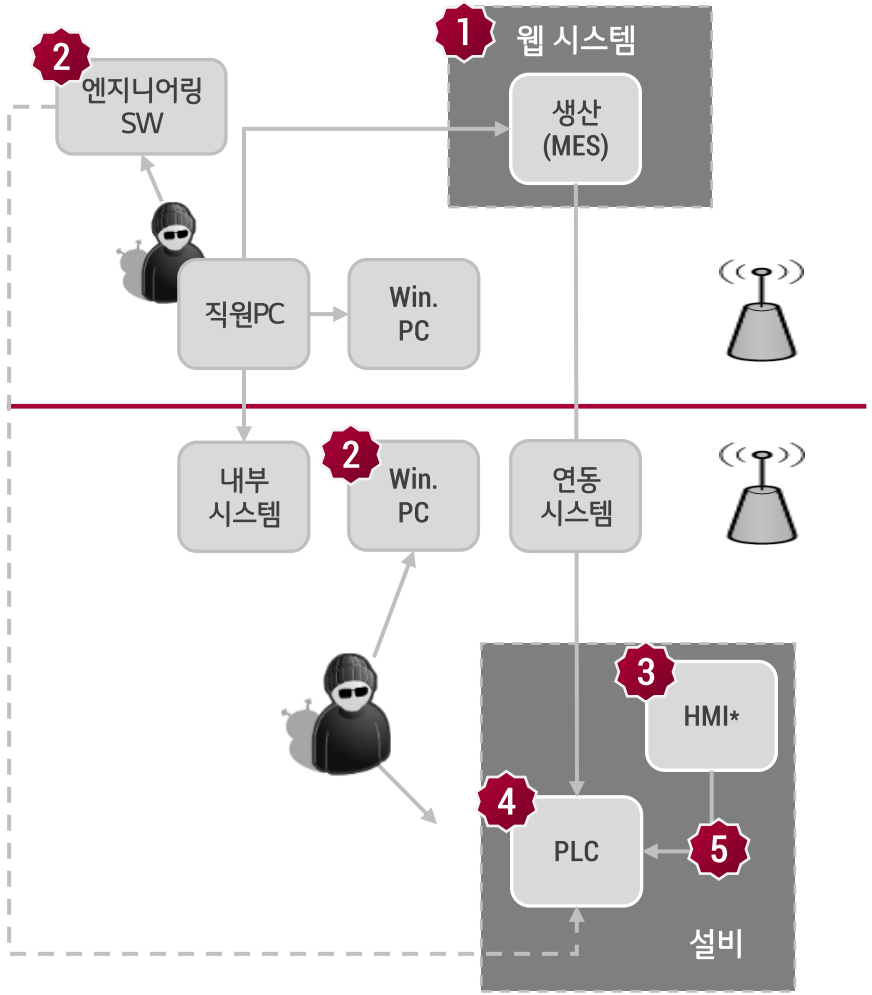
- Lv 3 — 설비제어망 (IP기반 PLC/DCS)
- Lv 2 — 제어공정 장비망 (PLC/DCS)
- Lv 1 — 제어공정 설비 (공정PC/서버, 센서)



OT 1 : 생산 계획 및 실행을 담당하는 공장 내 IT시스템
OT 2 : 제품 생산 및 제어를 위한 PLC/DCS 및 그와 연결된 설비 및 시스템
OT (Opertaional Technology) : 산업운영관리 컴퓨터 시스템 ICS, SCADA 등을 포괄하는 산업용 기계, 공정 운영을 위한 기술 및 시스템

2. OT 설비 모의 해킹 결과

OA망, FA망, PLC 설비에서 공장의 가용성을 침해할 수 있는 취약점 발견



발견 취약점 및 시나리오	발생 가능성	영향
1/ 직원PC에서 해킹을 통해 MES 웹 관리자로 로그인 후 생산 오더 변경 가능	상	상
2/ Windows PC에 최신 패치 미적용으로 WannaCry 악성코드 감염 위험	하	상
3/ HMI 엔지니어링 SW의 취약점으로 PLC 설정 변경 가능	하	중
4/ PLC 프로그램 다운로드 시 인증 과정 부재로 FA망 내에서 PLC 로직 변경 가능	하	상
5/ 조작된 데이터를 PLC에 전송하여 장애 유발 가능	하	상

*HMI(Human Machine Interface) 프로세서 시스템과 운영자 간의 인터페이스

2. OT 설비 모의 해킹 결과

1) 취약점으로 알아낸 HMI 잠금 해제 패스워드를 입력 후 PLC 설정 변경

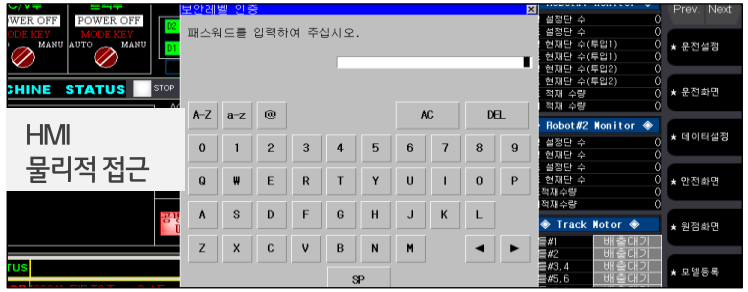
시나리오	내용
취약한 HMI 패스워드를 사용한 PLC 설정 변경	HMI 엔지니어링 SW의 취약점을 이용해 HMI 관리자 권한의 패스워드를 획득한 후, (물리적 접근 시) HMI를 관리자 권한으로 접근하여 PLC 설정을 변경 가능

STEP 01

가상환경을 구성하여
HMI Level2 로그인 시
패스워드 값을 확인

STEP 02

수집한 패스워드로
로그인 시도



STEP 03

Level 1 PM 모드로
로그인 성공
(제한 기능)

STEP 04

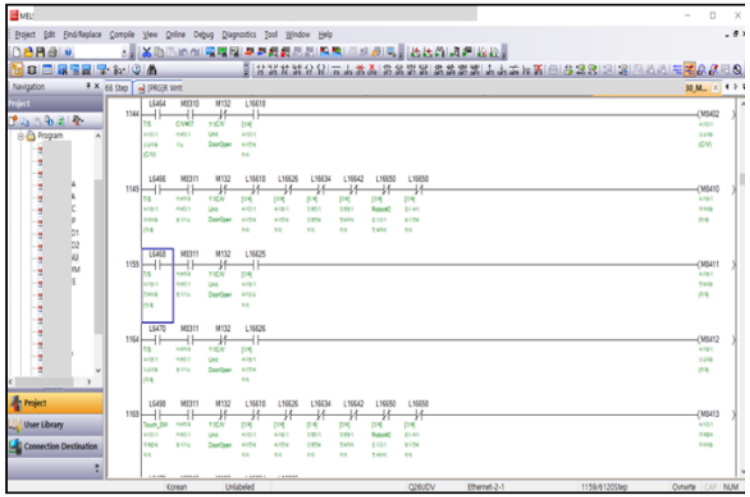
Level 2 Marker 모드로
로그인 성공
(설정 변경 기능)

2) Ladder Logic 다운로드 시 인증 과정이 없어 PLC 로직 변경

시나리오	내용
프로젝트 파일 업로드 및 다운로드 시 취약한 인증절차	프로젝트 파일을 업로드 또는 다운로드 시, 인증 절차 부재로 악의적인 사용자가 PLC에 파일을 무단으로 업/다운로드 가능

STEP 01

PLC Ladder Program* 변경



* PLC(Programmable Logic Controller)

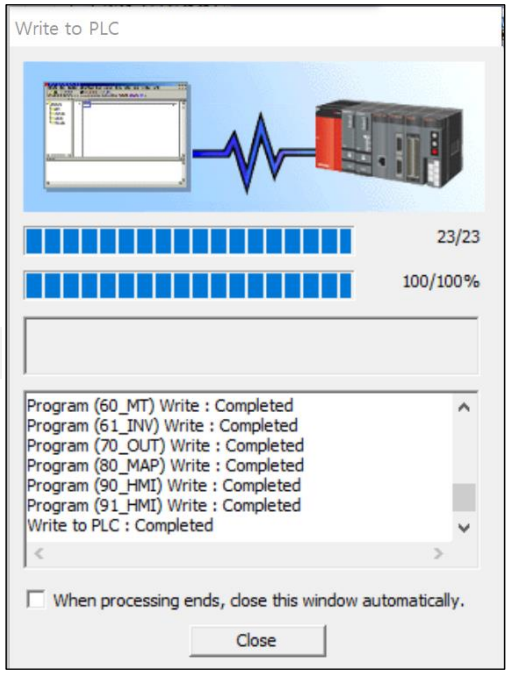
기계장치의 입출력이 어떤 시퀀스에 따라 동작하도록 제어할 때 사용하는 장치

STEP 02

임의의 사용자가 Write 성공

(PLC 오동작 가능)

FA망 접근

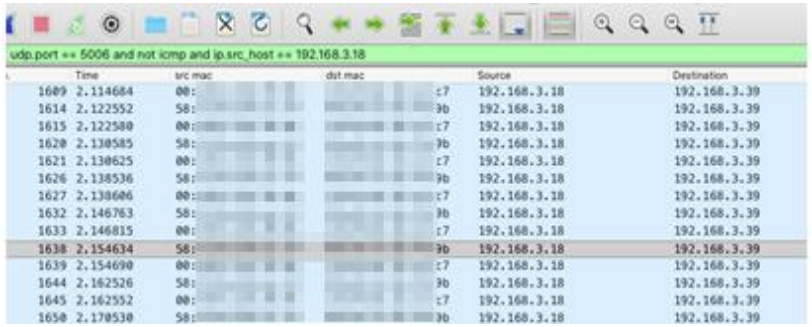


3) FA 네트워크 상에서 조작(재생)된 데이터를 PLC에 전송

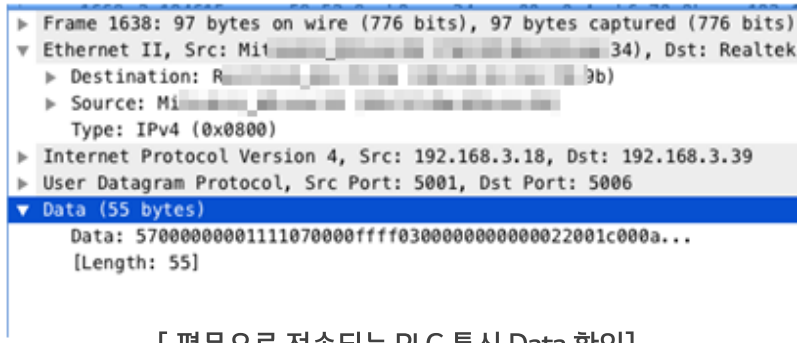
시나리오	내용
ICS 프로토콜 패킷 수집 및 데이터 위/변조	일반적으로 산업제어시스템에서 사용되는 필드버스 프로토콜은 평문으로 통신을 하기 때문에 송수신 데이터 MITM 및 Replay Attack 가능

STEP 01

PLC 모델 1개를
별도 환경으로
구성하여 확인



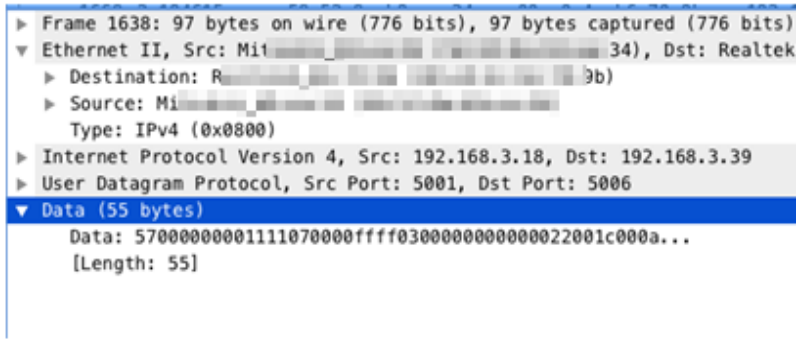
[Wireshark로 PLC와 HMI 통신 간 UDP 패킷 캡처]



[평문으로 전송되는 PLC 통신 Data 확인]

STEP 02

재생 공격으로
오동작 유발



3. 결론. OT2 보안 취약점 대응 방안

취약점 해결

- FA망 내 Windows PC 보안 패치
- 방화벽 룰 재 점검
- 취약한 패스워드 변경
- PLC 다운로드 시 인증 적용
- Technician PC 및 PLC Project File의 보안 관리
- PLC/HMI 및 Engineering SW 취약점 패치 (제조사)

OT 보안 환경 구축

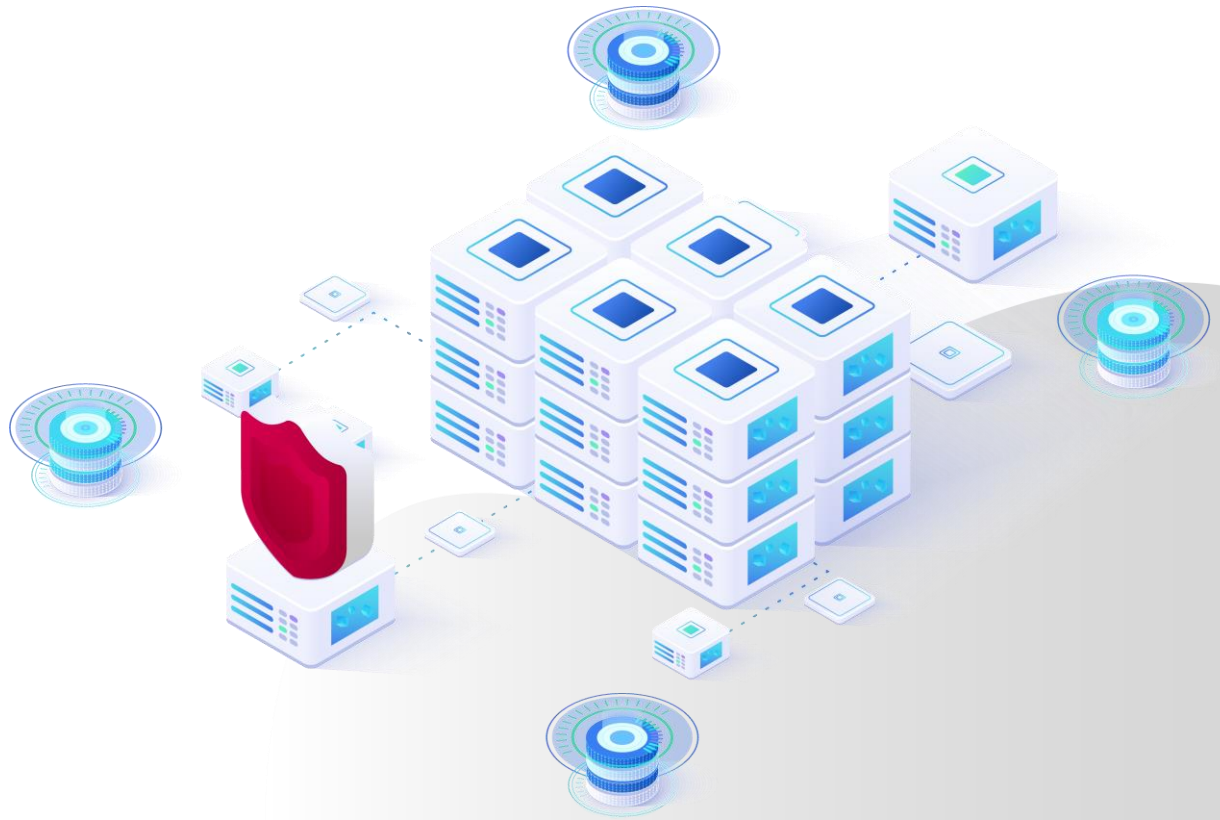
다음 발표에서 계속됩니다...

LG CNS

OT환경 보호를 위한

보안 아키텍처 구축 사례

2021. 5.
LG CNS 사이버시큐리티팀 박태석 책임



Contents

OT환경 보호를 위한 보안 아키텍처
구축 사례

1. OT 환경변화 및 보안의 필요성

신기술 도입 및 Open NW 지향 등 OT 환경변화에 따라, 신속한 보안대책 수립으로 기업 경영활동 연속성 확보 필요

OT 환경 변화

내부적 변화

- Analog 에서 Digital 환경으로 변화 (ICS System)
- AI, Bigdata 등 신기술 도입에 따라, Closed Network에서 Open Network 및 IT Network 간의 접점구간 발생
- IT 정보보안 조직의 관리범위 내로 OT 보안 포함
  → NW 아키텍처, 보안 통제방안, ICS System 보안 대책 등

외부적 변화

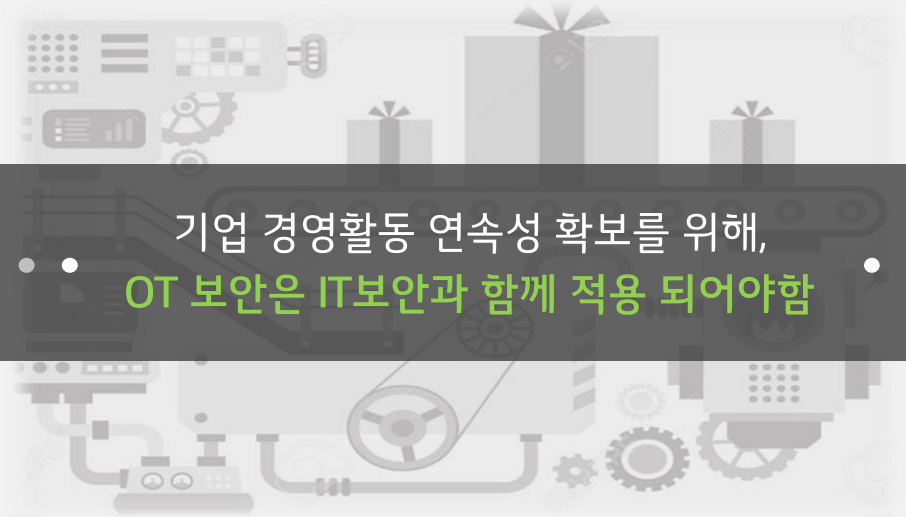
- 해킹에 의한 OT영역 침해사고 국내·외 발생사례 급증
- Industry 4.0, Smart Factory 등 제조산업 분야 자동화 및 지능화를 통한 생산성 극대화
- ICS 전용 방화벽, 전용장비 기반 Secure Channel 생성 , OT 가시화 솔루션 등 영역별 Global 솔루션 출시

내·외부적 환경 변화에 의해 OT 보안에 대한 위협이 증대됨에 따라 기업의 OT 환경을 이해하고 보안 대응방안 수립 및 즉 적용이 필요함

보안의 필요성

침해 사고 영향도

- 랜섬웨어(Ransomware) 감염으로 인한, **수일 ~ 수십일간 생산 중단 발생 (금전적 손해 포함)**
- 백업 시스템을 통한 대응방안 미구축 시, **피해 복구에 있어 막대한 소요 시간 발생 (금전적 손해 포함)**
- 대외적 기업 신뢰도 하락으로, **기업 경영에 피해 발생**



기업 경영활동 연속성 확보를 위해,
OT 보안은 IT보안과 함께 적용 되어야함

2. Global 표준 (IEC 62443 Series) International Electrotechnical Commission

IEC 62443 Series 는 계층별로 표준화 개발 진행 중이거나, 위원회 승인 완료 항목 존재 등 아직 진행중인 상태임
→ Global 컨설팅 회사에 따라 다양한 대응방안이 존재함

General	62443 – 1 – 1 Concepts & Models	62443 – 1 – 2 Master glossary of Terms & abbreviations	62443 – 1 – 3 System Security conformance metrics	62443 – 1 – 4 IACS* security lifecycle & use-cases	
Policies & Procedures	62443 – 2 – 1 Security program requirements for IACS asset owners	62443 – 2 – 2 IACS protection levels	62443 – 2 – 3 Patch Mgt. in the IACS environments	62443 – 2 – 4 Requirements for IACS services provider	62443 – 2 – 5 Implementation guidance for IACS asset owner
System	62443 – 3 – 1 Security technologies for IACS	62443 – 3 – 2 Security risk assessment & system design	62443 – 3 – 3 System security requirements & security levels		
Component	62443 – 4 – 1 Security product development lifecycle requirement	62443 – 4 – 2 Technical security requirements for IACS components			

Status Key

- Development Planned
- In Development
- Out for Comment or Vote
- Approved with comments
- Approved
- Published
- Adopted
- Published (Under revision)

* IACS : Industrial Automation & Control System

3. OT Security Protection Level

IEC 62443에 정의한 Protection Level의 평가를 위해 SL & ML Model 수립

Security Level (Technical)

Safe	SL 4	• Protection against intentional violation using sophisticated means with extended resources, IACS specific skills and high motivation
Medium	SL 3	• Protection against intentional violation using sophisticated means with moderate resources, IACS specific skills and moderate motivation
Caution	SL 2	• Protection against intentional violation using simple means with low resources, generic skills and low motivation
Danger	SL 1	• Protection against casual or coincidental violation
Critical	SL 0	• No Protection

Threat Level

Maturity Level (Procedural)

ML 4	• **Improved** . Process measured, controlled and continuously improved
ML 3	• **Defined** . Process characterized, proactive deployment
ML 2	• **Managed** . Process characterized, reactive
ML 1	• **Initial** . Process unpredictable, poorly controlled and reactive

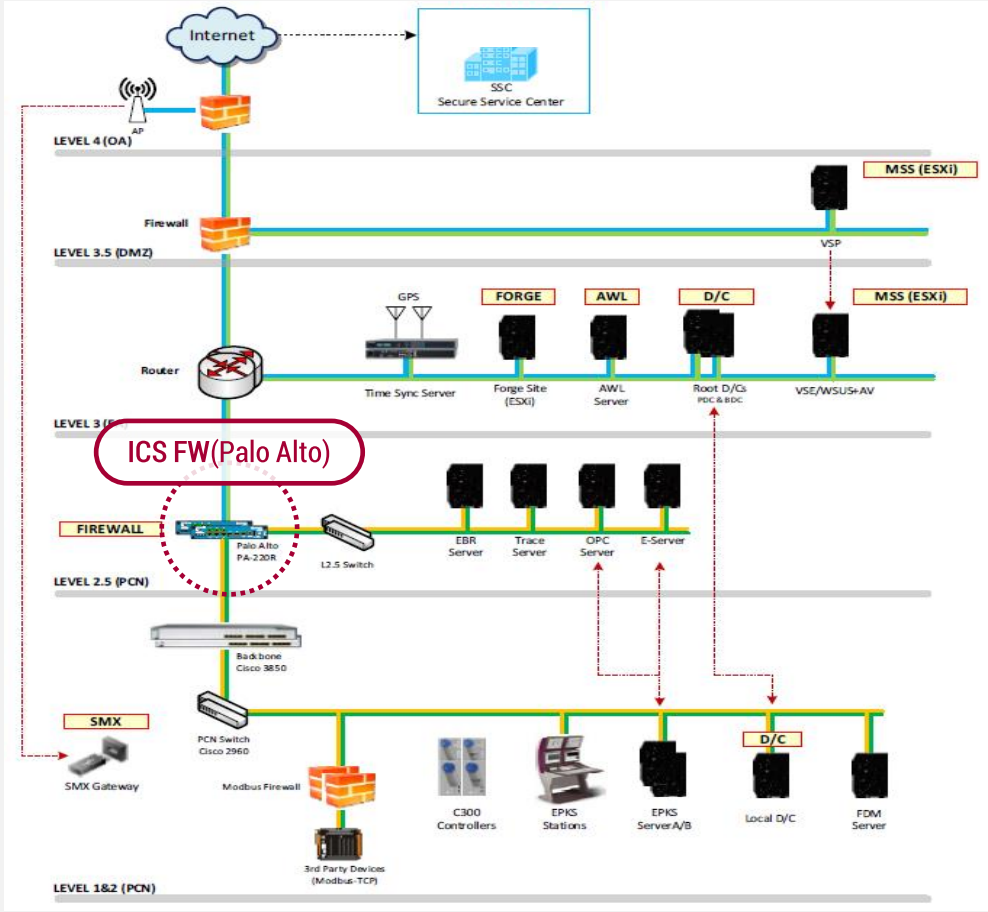
Protection Level

SL 4	D +	C +	B +	A +
SL 3	D	C	B	A
SL 2	D -	C -	B -	A -
SL 1	D -	C -	B -	A -
	ML 1	ML 2	ML 3	ML 4

4. OT 보안 아키텍처 (H社 사례)

DCS 적용 OT 환경하에 보안 위협 대응을 위해 시스템 아키텍처를 정의하고, Global 솔루션 간 협업 추진

OT Security System Architecture (DCS)



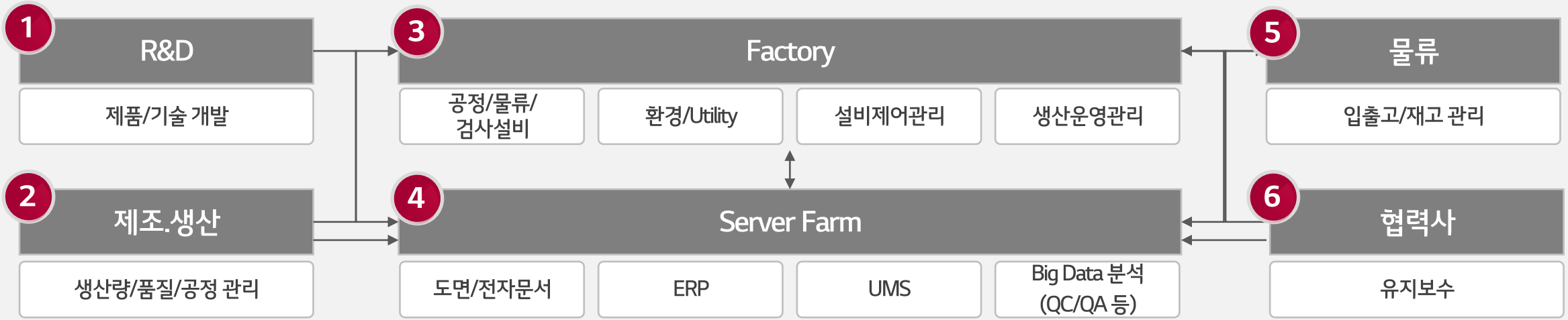
적용 솔루션

MSS	• **Managed Security Service** . Patch & Signature file 자동 / 수동 Update . System, NW & Performance 모니터링
Forge	• **Cyber Risk Manager** . OT Asset 에 대한 Security Risk 실시간 모니터링 . ICS Security 취약점, 위협 분석 및 대응 가이드
AWL	• **Application Whitelisting** . 허용된 Application 실행관리 . 미허가 실행파일 차단관리
D/C	• **Domain Controller** . ID/PW 통합관리 . User data Encryption, PC Hardening
EBR	• **Experion Backup and Restore** . DCS System Backup, 실시간 Backup 지원
SMX	• **Secure Media Exchange** . IT/OT 환경내 USB 사용 통제

5. LG CNS OT 보안 Coverage

생산과 관련된 유관부서 및 Work Flow에 따른 취약점을 분석하고, OT보안 Governance 수립

구성 요소별 보안 취약점



1

- 핵심기술 유출 (파일/출력 문서/사진촬영)
- 악성코드전파→공정중단 (→Server Farm)
- 비인가자 무단 출입

2

- 생산정보 유출
- 악성코드전파→공정중단 (→Factory, Server Farm)
- 비인가자 무단 출입

3

- 악성코드감염→공정중단 (외부 N/W, USB, 노트북)
- 환경/Utility센싱정보 조작
- 설비 내 생산정보 유출 (설비 접근, NW정보 갈취)
- 비인가자 무단 출입

4

- DB 정보 무단 조작
- 악성코드전파→공정중단 (→Factory)
- 비인가자 무단 출입

5

- 비인가 차량/화물 출입
- 비인가자 무단 출입

6

- 외부매체(USB,노트북)를 통한 악성코드 전파 (→Factory, Server Farm)
- 설비접근→정보유출
- 비인가 장비 반출입
- 비인가자 무단 출입

6. LG CNS OT 보안 Solution Suite

LG CNS는

해킹/악성코드 대응, 핵심기술보호,
통합 보안관리를 위한 16개 모듈 /
26개 솔루션으로 Suite을 구성함

해킹/악성코드 대응

iDMZ 구성	• Firewall / IPS / Switch
외부매체 Control	• 안랩 내PC지킴이/Smart Keeper PortLock
원격접근 통제	• Modoosone GATEONE-Z • Rsupport RemoteView
악성코드 Protection	• Cylance CylancePROTECT • 안랩 V3 • Symantec Endpoint Protection
설비 인증	• AirCUBE AirFront / 범용 802.1x지원 스위치
무선망 비인가 단말 차단	• WIPS

핵심기술보호

• LG CNS 무인 방문카드발급기	공장Gate 무인화
• LG CNS 지능화 X-Ray (봉인지 훼손 자동인식)	Risk기반 선별검색
• DLP	주요문서 접근통제
• 신도리코 MPS • LG CNS printChaser / Paper-X	출력문서 생명주기 관리
• LG CNS XID(홍채인증) & IDP	공정정보 접근제어
• LG CNS Intelli-VMS (VA for smart factory)	지능형 영상감시

해킹/바이러스 Event

정보유출/영상 Event

설비 / 네트워크 가시화

• Cisco StealthWatch • NOZOMI SCADA Guardian • Honeywell RiskManager

팩토리 보안 Portal

• LG CNS Factory Security Portal

설비 / 서버 백업 및 복구

• Acronis Backup

보안관리 기준

• Policy / Process / Guide / Checklist

통합 보안관리

Digital Innovation Enabler

Thank You

LG CNS