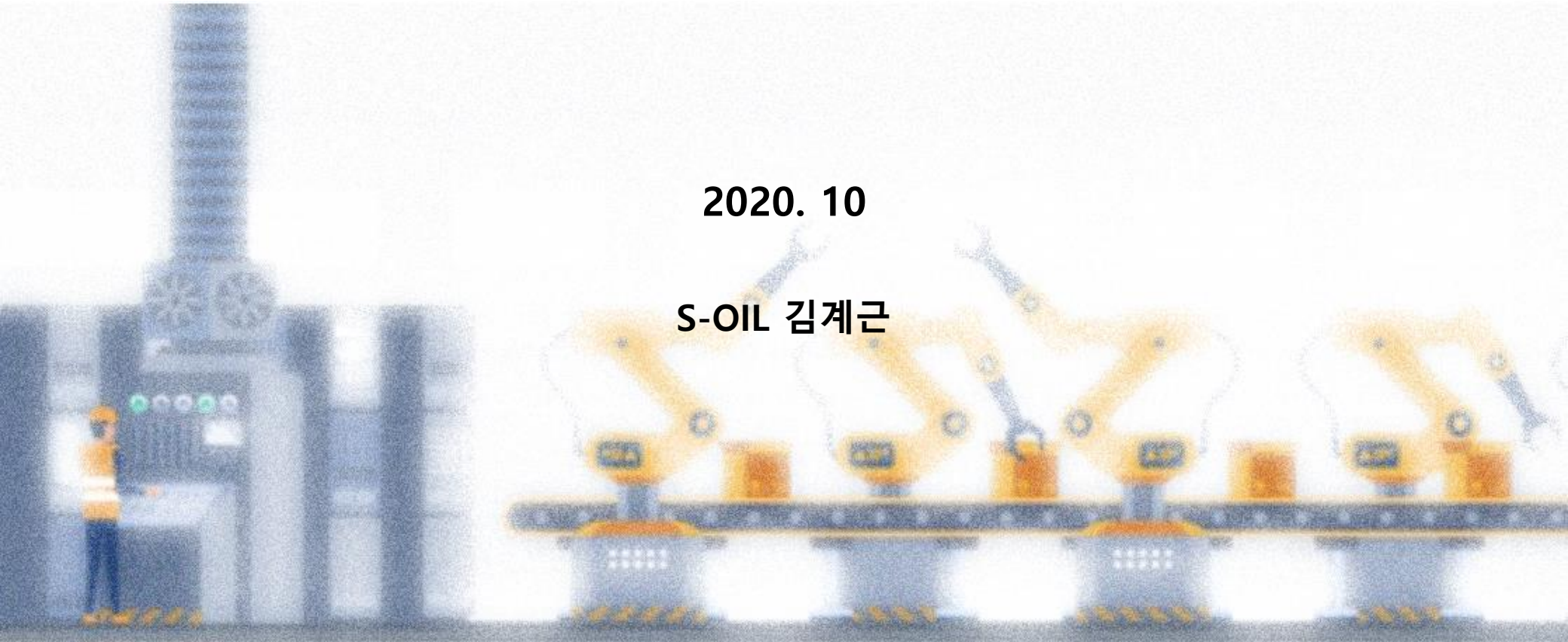
스마트공장 사이버보안 체계



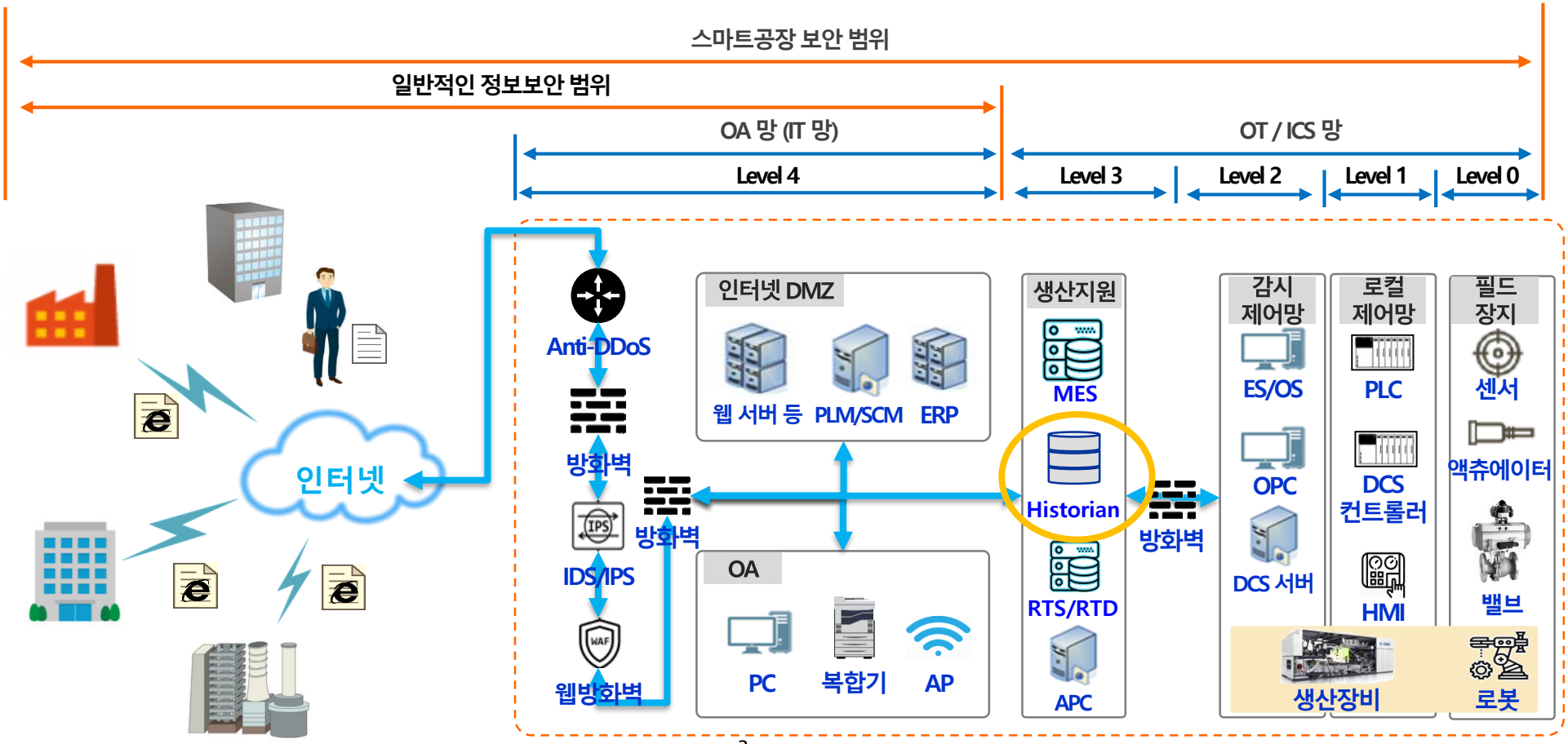
2020. 10

S-OIL 김계근

Contents

1. 정보 보안 vs. 스마트공장 보안

정보 보안	**정보**의 기밀성, 무결성 및 가용성을 제공하기 위해 정보 혹은 정보시스템에 대한 불법적인 접근, 사용, 공개, 중단, 수정 또는 파괴 등의 행위로부터 **보호하는 것**
스마트공장 보안	**스마트 공장**의 운영을 사이버공격으로부터 **보호하거나 방어하는 것**



2. 제조기업 보안 사고 사례

번호	발생년월	대상	내용	피해 규모 (추정)	피해영역(추정)	비고
	2020. 09	뒤셀도르프대 종합병원	• 병원 내 서버 감염 - **수술 차질로 인명 피해 발생**	• 수술 등 업무차질로 인명피해 발생	IT	
1	2020. 08	테슬라 (자동차 제조)	• 내부 직원을 통한 악성코드 유포 시도 - 기업 내부정보를 담보로 금전 협박		-	• 사전 체포
2	2020. 06	혼다 (자동차 제조)	• 생산라인관리시스템 마비 - **미국, 인도, 브라질 공장 등 11곳 가동 중단**	• 1일 이상 가동 중단 (약 9,000억원)	IT/OT	• 생산 차질
3	2020. 06	Lion (맥주 제조)	• 제조 프로세스 및 고객 처리 시스템 장애 - 제품 제조 공장 폐쇄	• 7일 이상 가동 중단	IT/OT	• 생산 차질
4	2020. 05	톨 (선박 회사)	• 기업 내부정보 유출 - 개인정보 및 거래계약내용	• 알 수 없음	IT	• 정보유출
5	2020. 05	블루스코프 (철강 회사)	• IT 및 생산 운영시스템 마비 - **용광로 운전을 수동으로 전환**		IT/OT	• 생산 차질

※ 혼다의 피해 금액은 기사의 내용을 참조로 전년도 매출액을 감안하여 추정한 금액임

3. Case : 스마트 공장 도입 시작 기업

조직 및 보안 현황

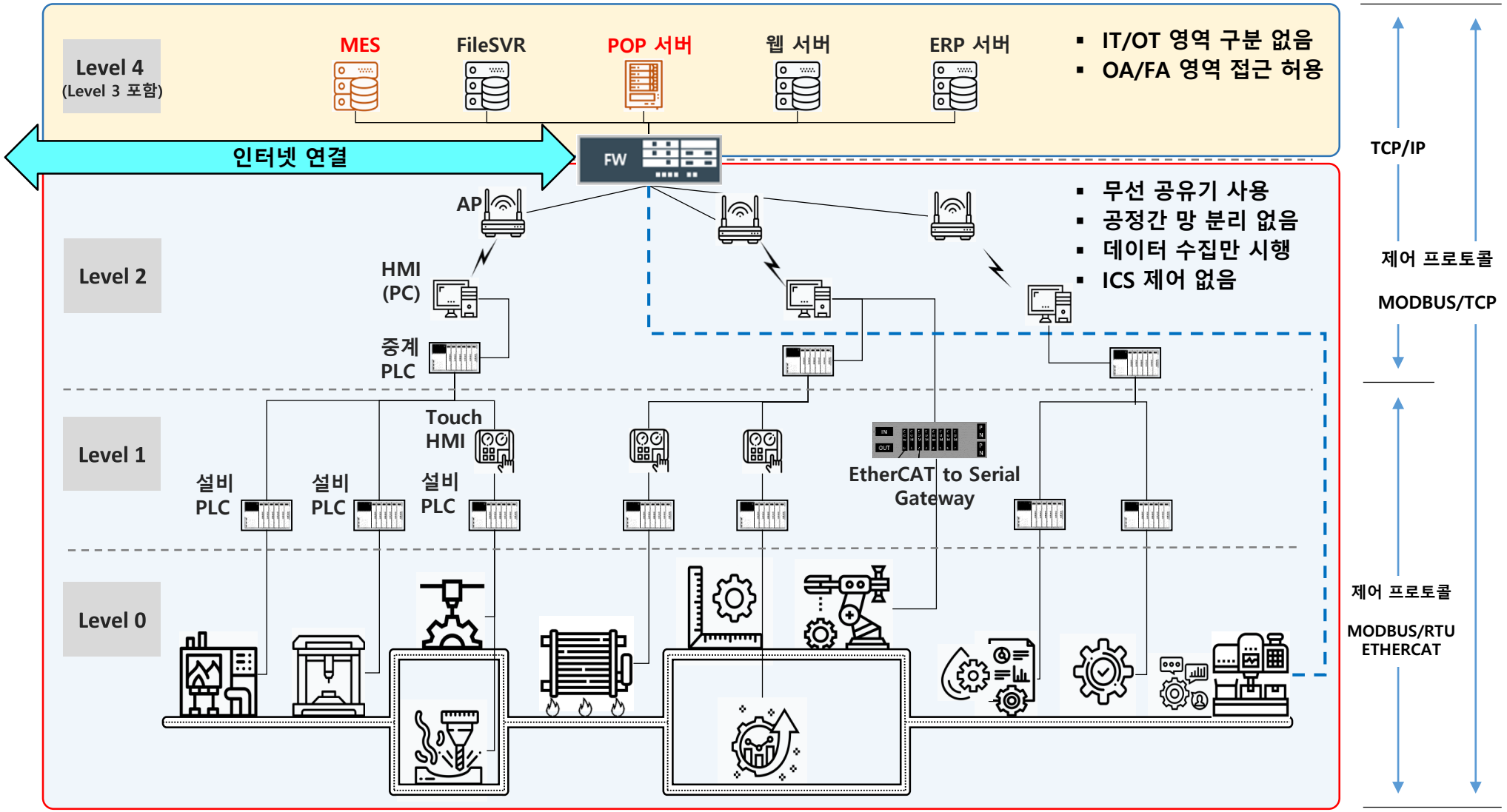
- **조직 구성**
  - IT 업무 : IT 담당부서에서 시스템 운영 업무를 담당, **보안 솔루션 운영 및 유지보수는 외부 협력업체 활용**
  - OT 업무 : 생산전담 부서가 운영만을 담당하며 **생산지원시스템, 생산장비, 설비 등** 의 **유지보수는 외부 아웃소싱**

- **보안 현황**
  - 정보시스템 영역의 일부 영역에 대해 ISMS 인증 획득, 생산지원 시스템 등 OT 영역은 인증 범위에서 제외
  - 네트워크 및 서버 기반 보안 솔루션 운영, DRM, DLP 등 정보유출 방지 솔루션 없음
  - 정보시스템에 대한 사내 보안정책, 지침, 가이드 보유, OT 영역 적용에 현황과 맞지 않는 점이 있음

- **외부 협력업체 업무**
  - IT : 정보 시스템 유지보수, 정보시스템에 대한 백업 지원, **백업자료를 협력업체 NAS 서버에 저장**
    인터넷 접점 구간에 UTM (FW, VPN, IDS 기능) **보안 솔루션 운영**
  - OT : 제어기기 (PLC, HMI, ES, OS) 유지보수 업체와 생산장비 유지보수 업체로 구분
    : **그래픽 파일, 기기 설정 값** 등 공정 정보는 **유지보수 업체에서 관리**

3. Case : 스마트 공장 도입 시작 기업

시스템/네트워크 구성 현황



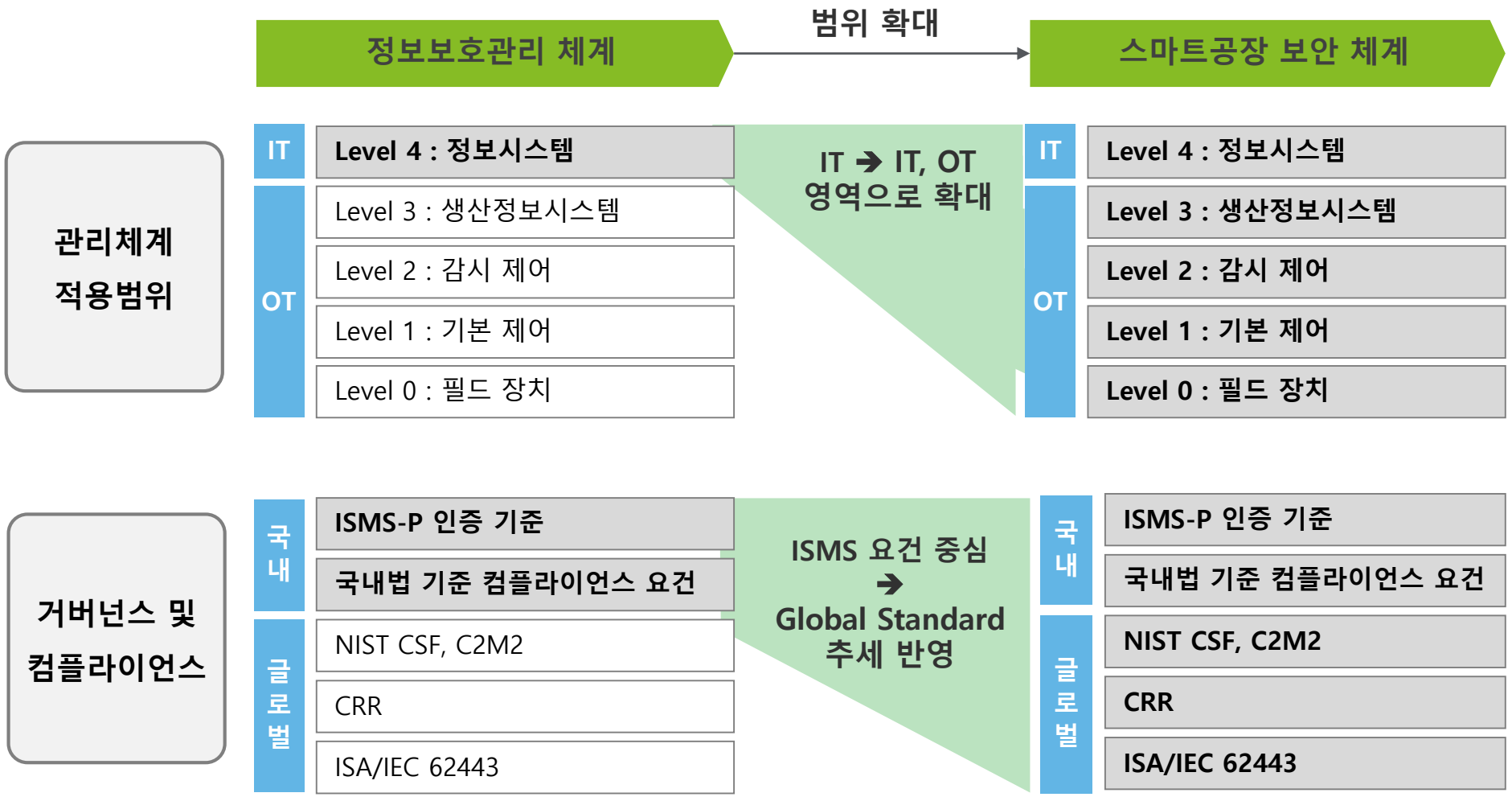
4. 정보보안과 스마트공장 보안 차이점

스마트공장 보안을 위한 고려사항

항목	정보보안	스마트공장 보안
목적	정보가 생성되어 소멸되기까지 그 처리 및 생명 주기 전반에 걸쳐 기밀성, 무결성, 가용성을 확보	제품 생산을 위한 생명 주기 전반에 걸쳐 공장 운영의 가용성, 무결성, 기밀성을 확보
보호 대상	정보와 저장매체, 처리시스템, 처리과정, 통신구간 등	제품생산에 영향을 주는 정보, 정보시스템, 생산장비, 산업제어기기, 생산관리/지원시스템, 통신구간 등
대상 시스템	IT 시스템 (Unix/Windows 서버, 스토리지, 모바일 기기, Embedded 시스템 등)	IT 시스템, OT 시스템(OPC, Historian, ES/OS 등) , 생산장비, 산업자동제어장치(DCS controller, PLC 등), IIoT 기기 등
대상 네트워크	IT 네트워크 (TCP/IP 기반의 Ethernet 및 네트워크 장비)	IT 네트워크, 산업용 필드버스 (Ethernet/IP, ControlNet, ProfiNet, DeviceNet, Profibus, Foundation Fieldbus), Realtime 지원 Network 장비 등
프로토콜	TCP/IP protocol suite	TCP/IP protocol suite, 산업용 프로토콜

5. 스마트공장 보안 범위의 확대

기존 정보시스템 영역에 대한 보안의 적용범위를 스마트공장 보안을 위하여 확대 적용할 필요성이 있음



[Backup] NIST CSF(Cyber Security Framework)

CSF

- 위험(Risk)을 중심으로 식별, 보호, 탐지, 대응, 복구의 5개 Function을 기반으로 구성됨
- Core (5개 Function 23개 Category, 108개 Sub-Category), 프로파일(현재, 목표), Tier (4단계) 로 구성
- IT, OT 모두 적용 가능

프로파일: 현재 → 목표

Tier: 부분 적용 → 위험 인지 → 반복 수행 → 적응형

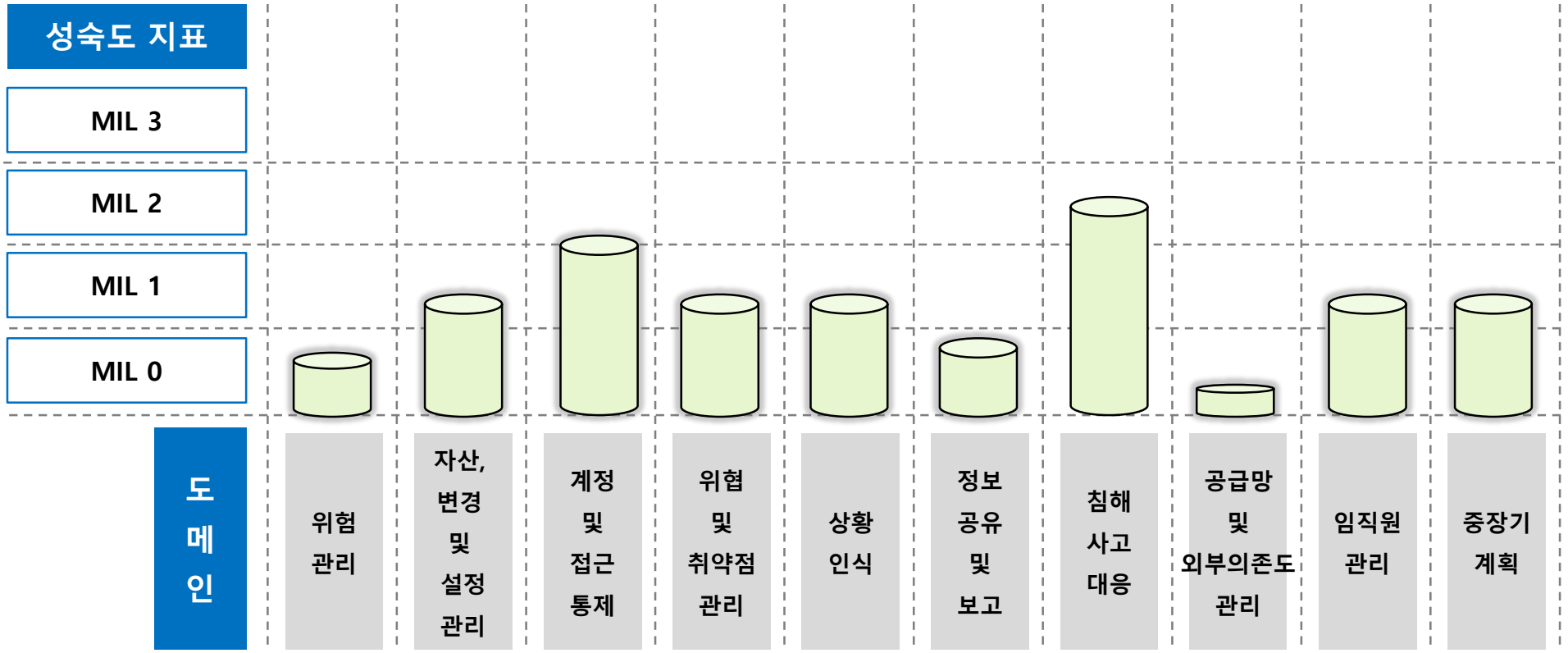
IT, OT 사이버보안 프레임워크

식별	보호	탐지	대응	복구
자산 관리	계정 및 접근통제	비정상행위 및 이벤트	사고대응 계획	복구 계획
Biz. 환경	인식제고 및 훈련	지속적인 보안 모니터링	보고 및 상황전파	개선
거버넌스	데이터 보안	탐지 프로세스	분석	보고 및 상황전파
위험평가	정보보호 프로세스 및 절차		완화	
위험관리 전략	유지 보수		개선	
공급망 위험관리	보호 기술			

[Backup] C2M2 (Cybersecurity Capability Maturity Model)

C2M2

- 사이버보안 성숙도를 평가하기 위한 모델로 10개 도메인 3단계 성숙도 수준을 가짐
- ES-C2M2 (Electric Subsector)와 ONG-C2M2 (Oil & Natural Gas) 가 있음
- IT, OT 모두 적용 가능 (ONG-C2M2 기준 312개 평가항목)



[Backup] CRR, ISA/IEC 62443

Cybersecurity Resilience Review

CRR

- 사이버 침해(부정적 이벤트)에도 의도한 성과/결과물을 지속적으로 전달 할 수 있는 능력 (복원력)
- 카네기멜론대의 CERT-RMM 을 기반으로 미 국토안보부에서 작성
- 10개 영역 (자산, 보안대책, 구성 및 변경, 취약점, 사고, 서비스 연속성, 위험 등)으로 구성
- 42개의 목표와 167개의 실천사항을 포함

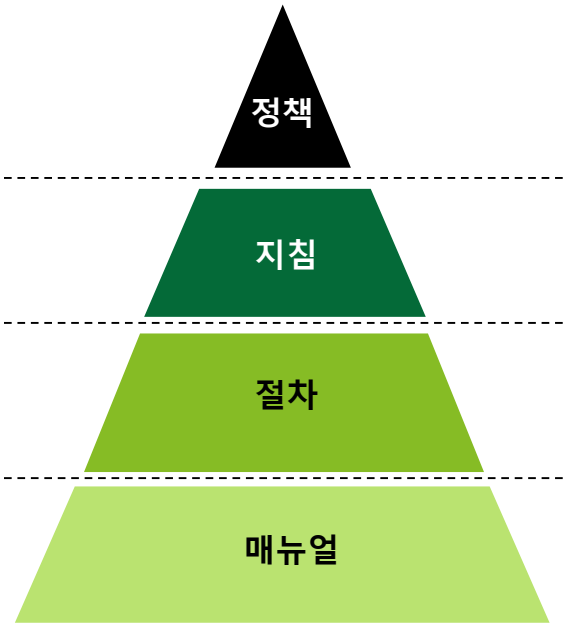
ISA/IEC 62443 Series

ISA/IEC 62443

- 미국 ISA 99 표준을 ISA/IEC 62443 으로 발간
- 4 Series (일반, 정책 및 절차, 시스템, 컴포넌트 보안 요건)아래 14개 문서로 구성
- 산업자동제어시스템을 이용한 서비스 사업자, 구축 사업자는 2, 3 Series
- 산업자동제어기기를 만드는 제조사는 3, 4Series를 참조하도록 구성
- ISA/IEC 62443을 기반으로 하는 보안인증 발행 (CSA, SSA, SDLA)

6. 스마트공장 사이버보안 체계 구조

정책체계의 수직적 구조



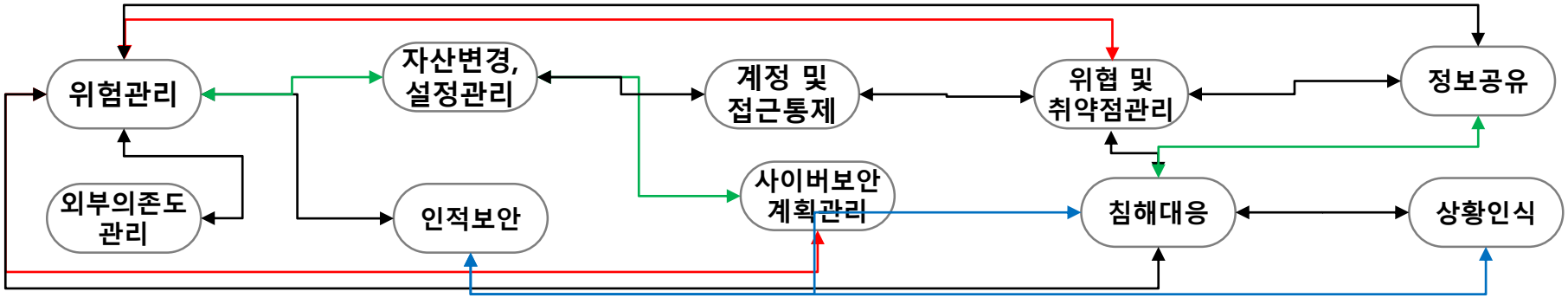
- 스마트공장 보안의 **목표와 원칙을 정의**
- IT, OT를 하나의 정책으로 포괄적 정의

- IT, OT, 개인정보 등을 영역을 나누어 표현할 수 있음
- **주요 통제 요건 및 기준**을 정의

- 보안 영역을 세분화하여 **상세 통제 요건 및 절차 정의**
- 통제 활동 별 **책임 및 권한 정의**

- 각 IT & OT 자산 별 **상세 보안 설정 및 단계별 수행 절차** (Step by step) 를 위한 실무 지침 작성

정책체계의 수평적 구조



7. 기준 수립 – 현장을 위한 매뉴얼 까지

(예시) 산업자동제어기기 보안 요건 및 설정 기준 수립

- 현장에서 사용중인 ICS 기기의 종류에 따른 보안기준을 수립
- 구형 장비의 경우 해당 보안 기능이 없으므로 대체 방안 마련 후 변경 수요 발생 시 도입 보안요건으로 반영

영역	점검기준	보안 요구사항	설정 기준
1. 자원 가용성 관리	1.1 비상전원	ㅇ 제어기기의 경우 비상 배터리를 통해 전력 공급이 중단되었을 때를 대비한다. - PLC : CPU 모듈 내 배터리 장착, 배터리는 주기적으로 교체 ㅇ 중요한 역할을 수행하는 PLC의 경우 전력의 공급이 중단되었을 때를 대비하여 이중전원 구성을 한다.	생략
	1.2 최소 기능 모드	ㅇ 제어기기의 기능 중 사용하지 않는 기능은 해당 기능을 사용하지 않도록 제한한다. - OPC-UA를 지원하는 PLC의 경우 OPC classic을 사용한다면 웹 [illegible]버 기능을 중단 ㅇ PLC의 자원관리 기능이 존재할 경우 자원할당 우선 순위를 [illegible]	생략
	1.3 백업	ㅇ PLC의 주요 프로그램 및 데이터를 Memory Card에 [illegible]iemens PLC의 경우 기본적으로 Memory Card를 통해 적재하기 때문에 자동적으로 백[illegible]나, 타사의 PLC의 경우에는 Memory Card를 통해서 프로그램이나 설정값을 적재하지 [illegible]문에 Memory Card에 백업을 저장하도록 한다. ㅇ (선택) 중요 PLC의 경우에는 동일한 [illegible]설정 값, 데이터가 내장된 PLC CPU 모듈을 별도로 보관한다.	생략
	1.4 복구	ㅇ PLC의 메모리 카드에 저장된 백업데이터를 통해 복구가 가능하도록 준비한다. ㅇ (선택) 중요 PLC의 경우에는 고장 발생 시를 대비한 동일 PLC CPU 모듈을 교체하도록 한다. (프로그램 및 데이터 동일)	생략
	1.5 자원 영역 분리	ㅇ 사이버 침해 혹은 물리적 사고(화재, 정전 등)을 대비하여 별도의 물리적 영역에 보관하거나 중요 기기의 경우 이중화 구성을 통해 사고에 대비한다.	생략

PLC 예 시

7. 기준 수립 – 현장을 위한 매뉴얼 까지

취약점 구분	코드보호	항목코드	PLC-07
대상 장비	PLC	적용여부	권고

위협 분석

액세스 수준의 Know-how 보호를 하지 못하여 다운로드 권한을 제한하지 못하여 CPU 를 무단으로 수정할 수 있으며, 메모리 카드의 블록을 무단으로 쓰기/읽기가 가능하여 프로그램 코드의 변경으로 장애 및 심각한 피해를 초래할 수 있음.

점검 방법

[적용 기준]

Know-how 보호를 통한 프로그램 코드 보호

[확인 방법]

■ **SIEMENS Simantic Manager v5.5**

1. SIMANTIC manager > Tools > Block protection..." 선택 또는 마우스 오른쪽 버튼 "차단방지" 선택
2. 암호화하려는 블록을 마우스 오른쪽 버튼으로 클릭하고 팝업 메뉴에서 "Block Encryption" 선택
3 "Block Encryption" 대화창에서 12 자 이상의 암호 입력
4. 암호 반복 입력후 확인 "OK"

※ S7 Block Privacy Tool 을 사용하여 블록 암호화 설정

위에 제시한 설정이 해당 파일에 적용되지 않은 경우 아래의 보안설정 방법에 따라 설정을 변경 함

보안설정방법

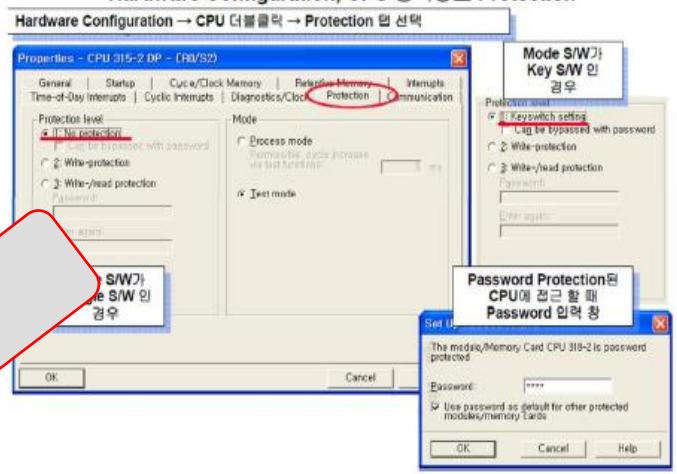
[조치 방법]

■ **SIEMENS Simatic Manager v5.5**

1. SIMANTIC manager > Tools > Block protection..." 선택 또는 마우스 오른쪽 버튼 "차단방지" 선택
2. 암호화하려는 블록을 마우스 오른쪽 버튼으로 클릭하고 팝업 메뉴에서 "Block Encryption" 선택
3 "Block Encryption" 대화창에서 12자 이상의 암호 입력
4. 암호 반복 입력 후 확인 "OK"

[조치 방법]

Hardware Configuration, CPU 등록정보 Protection



예 시

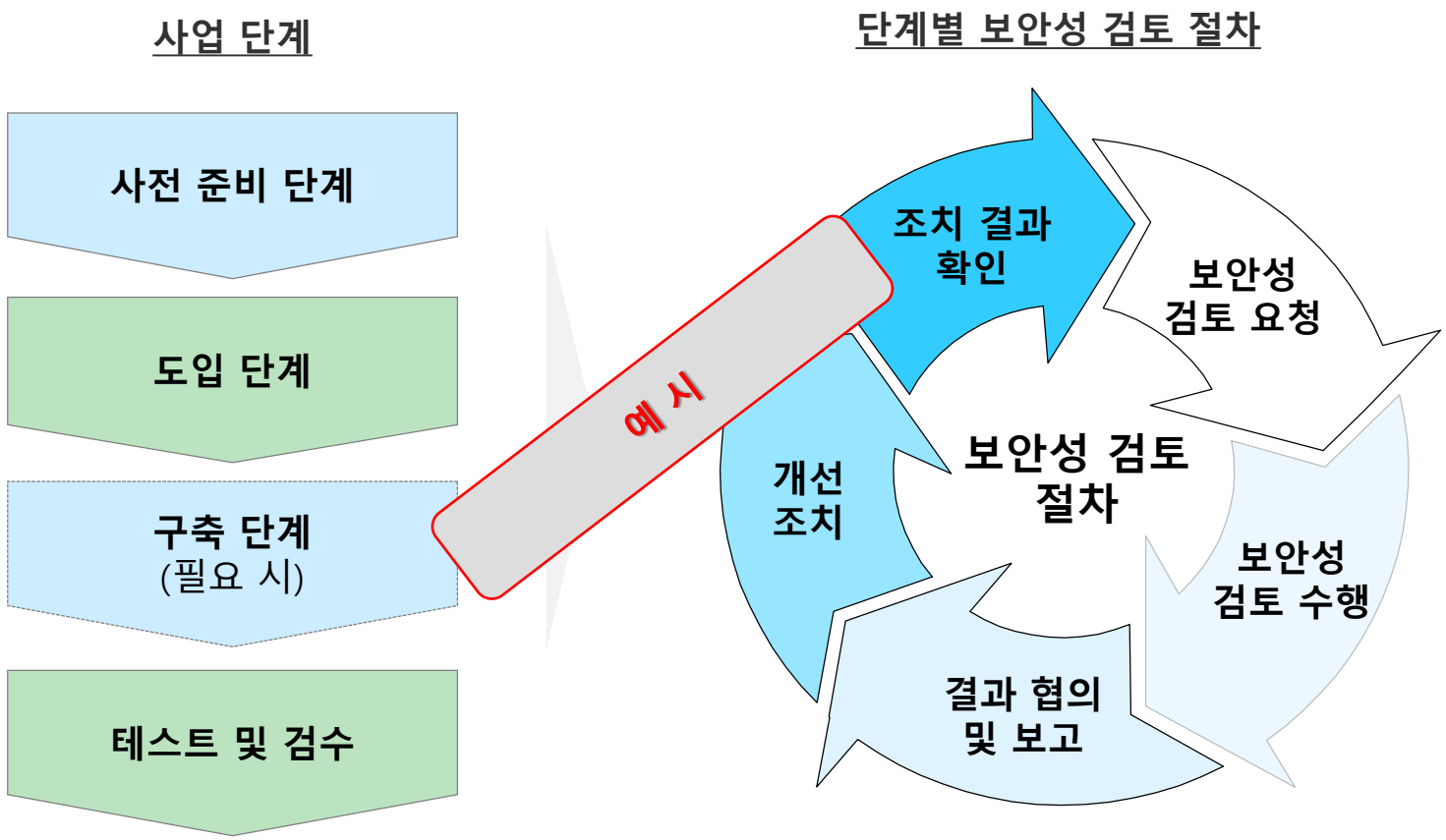
■ SIEMENS Simatic Manager v5.5

1. "HW config" Tool 실행
2. 해당 CPU 클릭
3. Properties 팝업 메뉴창 > " Protection Level "설정
   - 가. Access protection for F CI (Can be bypassed with password 체크박스)
   - 나. Write-protection
   - 다. Read/write-protection
4. 체크박스 "3. Read/write-protection" 선택 후 > password/Reenter password 설정

※ SIMANTIC MANAGER 메뉴 > PLC > Access Rights > Setup 에서도 설정 가능

8. 사이버보안 Task 정의

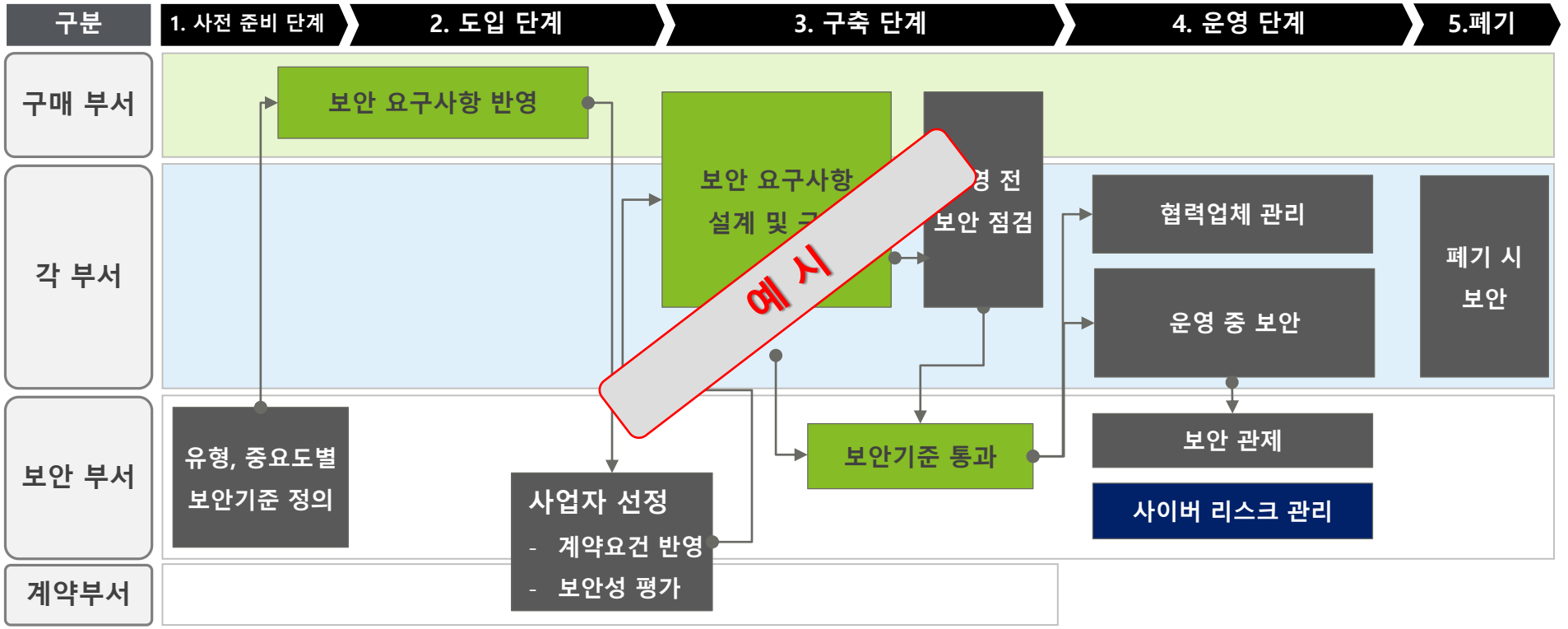
도메인 지침 내 사이버보안 세부 수행업무 정의



9. Task별 프로세스, R&R, RACI 정의

자산의 생명주기 단계 별 보안 통제 활동

프로세스 정의

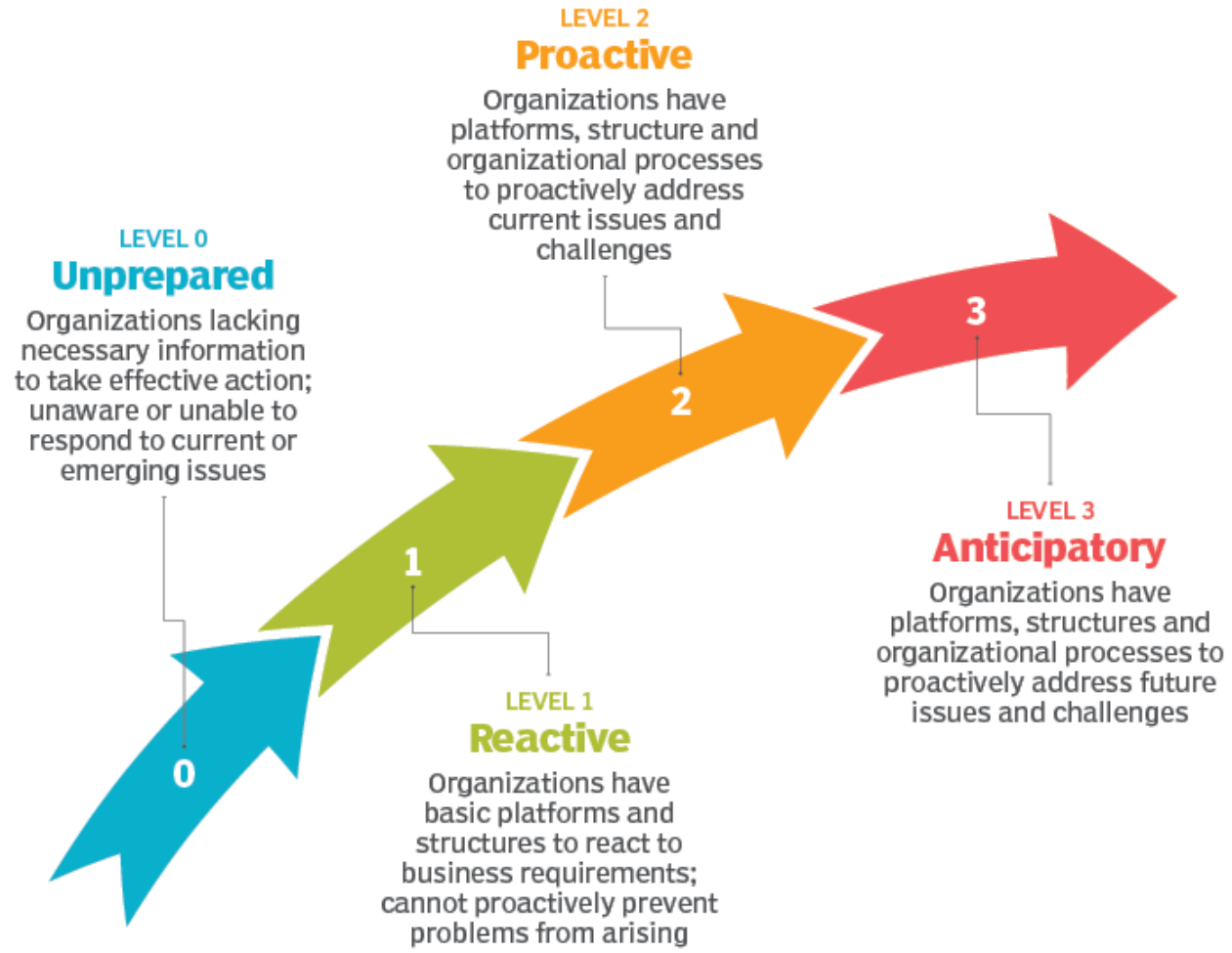


R&R 및 RACI 정의

- 각 역할담당자간 생명주기에 따른 R&R을 정의
- 수행(R), 승인(A), 지원(C), 정보공유(I)를 각 수행업무 별로 담당자를 지정

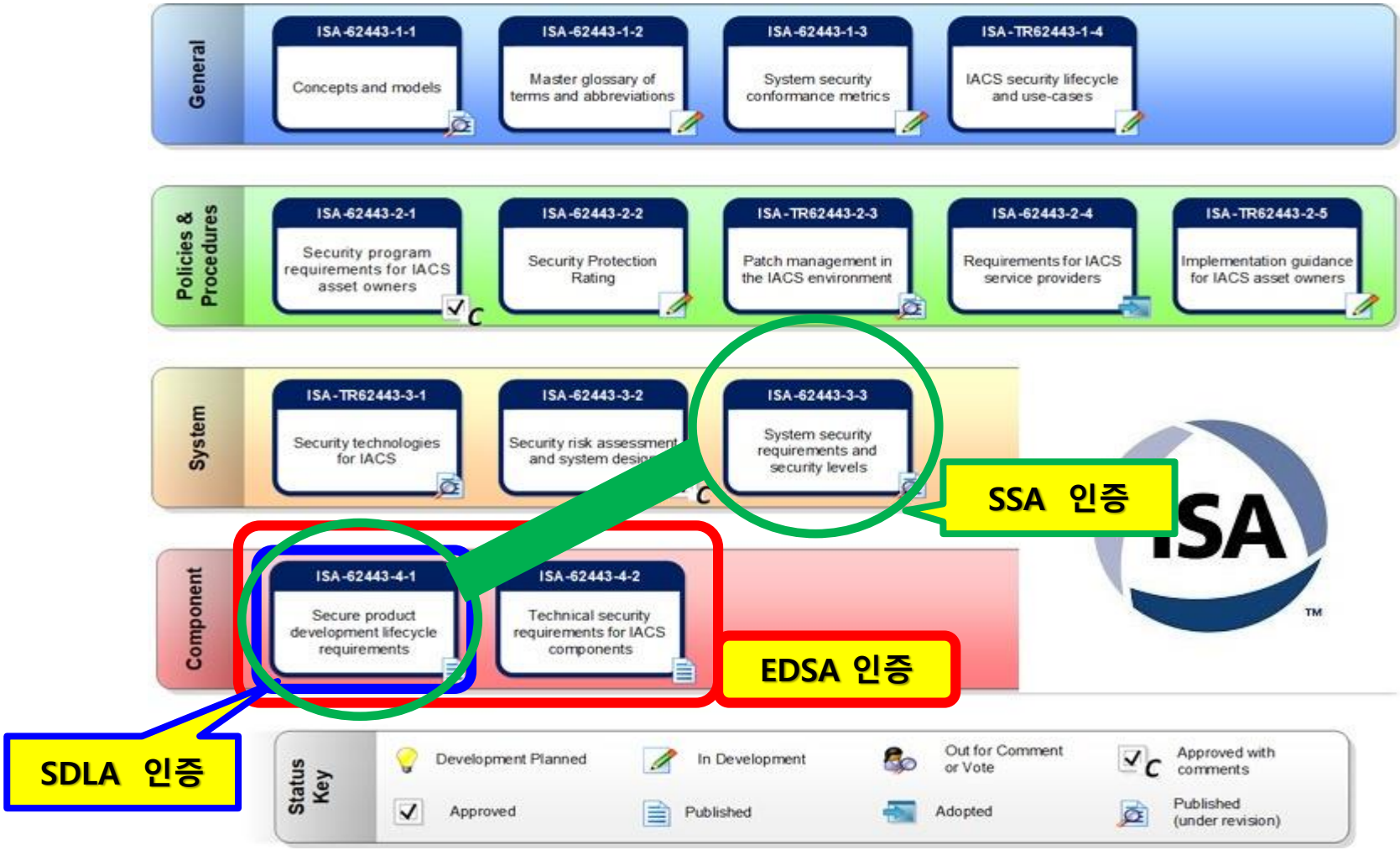
10. 지속적인 개선 활동

- 스마트공장을 운영하는 기업 전반에 걸쳐서 사이버보안 활동이 진행되고 성숙되어 가는지 지속적으로 점검하고 개선하여 스마트공장의 사이버보안 성숙도를 높여 가야 함



[Backup] ISASecure 인증을 이용한 보안성 평가시간 단축

- OT 영역에 설치 운영되는 산업자동화기기의 보안요구사항을 정의하는 단계에서 ISA/IEC 62443 기반의 ISASecure 인증 획득 시 보안검증을 생략하는 절차를 둘 수 있음



감사합니다!!