



주제: 스마트 팩토리 IT/OT 영역 분리와 위험 대책

1. 배경

1) Smart factory: 제품과 서비스를 파는 개념으로

마케팅과 고객 접근을 넘어, 연결성이 높고 빅데이터를
준용하여 지능을 갖춘 공장.

2) 기존 공장 대비 연결성이 뛰어나고, 연결성이
확고 ~~확고~~ 가능해짐

3) 그러나 연결성이 증가한 만큼 외부 보안
위험도 증가. 심각한 → 국가간 해킹도 인한 인력
파괴 등 ~~위~~ 사례 있음

4) ~~이러한~~ 인력을 보호하기 위해 내산하
기인 IEC 62443 표준 정립 등

2. IT 영역 OT 영역, 각 영역별 보안 위험

1) IT 영역 Internet ~~the~~ technology

인터넷 기술이 적용되는 영역. ERP 등

새로운 비즈니스 모델이 적용 판매 되는 영역

2) OT. Operational Technology

공강. 인공라르 혼성하기 위한 기술이 동 작하는 영 어
IT 영역 라는 가르기 인공성에 즉 증점을 드어
보안에 대한 개념이 없이 설게 .인용

3) 각 영역 별 보안 유형

① IT 의 보안 유형

현재 인터넷에 구현되는 모든 프로그래밍 기법이
구현될 DDoS; Man in the middle 등
공격도 다양하나 이에 대한 대응도 다 방을
기본적으로 IT와 OT 영역간 차가 DMZ를
숙경하여 방 방리

② OT 영역 보안 유형

보안 위협에 대해 무방비. 사영과 권한 구분
없고. 사영 제한, 피터 부작성 등 개념이
없을 대부분 전원 통제를 인하여 보안을
유지되나 향후 연결성 증가를 인하여 공격
위험 대폭한사 예측.

3. 대책

1) OT 영역의 대책으로 IEC 62443 적용된
부품 적용

각 설비별 Foundational 리스크를 정의하고

사용리스크 Security Level을 정의

목표 보낸 상태를 정의하고 이를 구현하고
평가 받음

2) Zone 과 Conduct를 구분

한 개 Zone으로 구현하기 않고 각 영역별

목표를 설정. 이에 맞는 콘 Components를

사용 Zone과 Zone은 최소 연결 Conduct로

구분

4. 의견

1) 현재 OT 영역은 외부 보낸 위험에 취약해

IEC 62443은 현재 제품이 출시되고 있어

관련 적용까지 시간이 필요함.

블록체인, 클라우드, 빅데이터, 사물인터넷, 인공지능 등
대체기술 적극활용

2) ITC 62443의 무역 관행으로 불국할 가능성 높음
하향 components를 타 국가에 수출시 인준증 증발
문제도 인식할수 있음

이후에 표준 제공 증이나 적극 참여를 통한
자정립이 많이 필요

3) 투자비 증가에 따른 명확한 비즈니스 모델
설정 필요.

Components, Solution 제공시 투자비 필요.

현재 같이 러플만 확대하는 적과 특 확대, 가능성
높을 난안권에 가치를 부여하고, Smart factory
를 제공하는 새로운 가치 창출, 판매필요
→ 선순환으로 경쟁력 강화 예상.