일반 산업제어시설에서 사이버보안 기술적용 현황

May.11, 2016

njc@etri.re.kr
Cyber-Physical Security Lab, ETRI

목 차

들어가기 전에

연구부서의 주요 R&D 분야

Beyond OS Security

하드웨어 해킹, 이제는 현실화

- 하드웨어 자체 버그 악용 또는 펌웨어 조작
→ 버스 프루빙 공격 및 메모리 공격 대응책

Industrial IoT Security

국가 기반시설에 대한 APT 공격, 물리적인 재앙

- 실수 또는 고의적인 비정상 제어시스템 결함 증가
→ 제어시스템 심층방어 및 외부위협 원천봉쇄

<사이버물리 융합 보안관제>

<산업용방화벽>

<데이터 다이오드>

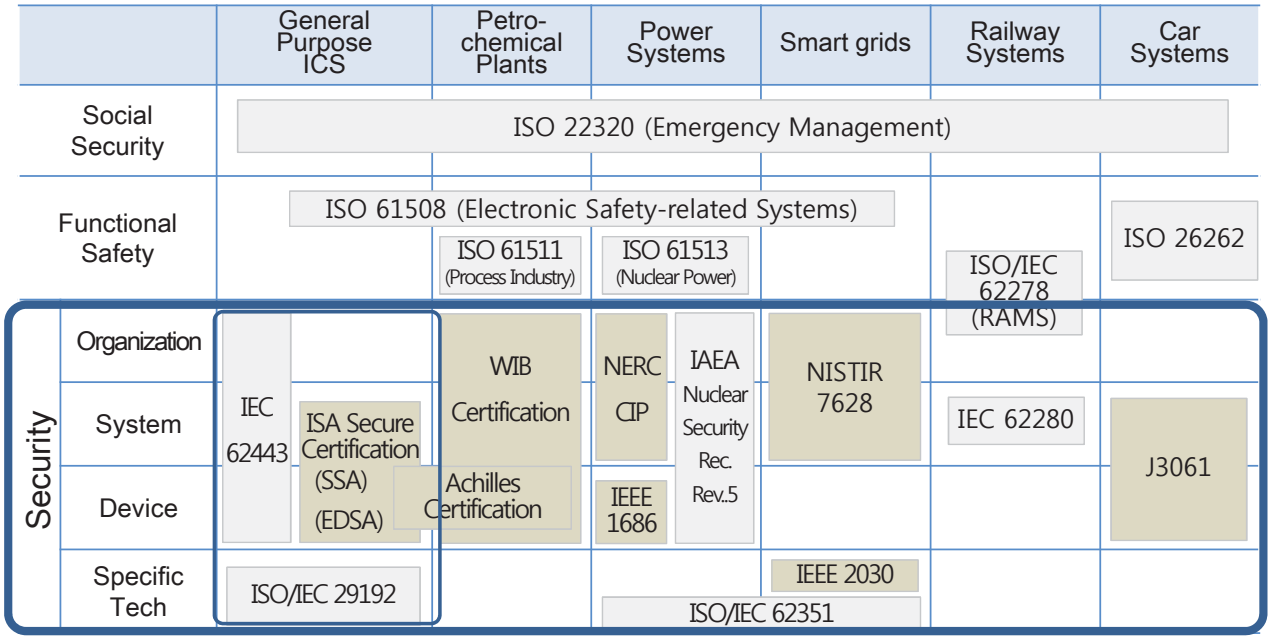
<HW/FW보안검증도구>

<모의침투도구>

제어시스템 보안 관련 동향

표준, 인증 범위 및 요구사항,
기술, 제품 중심으로 …

일반 제어시스템 보안 관련 표준



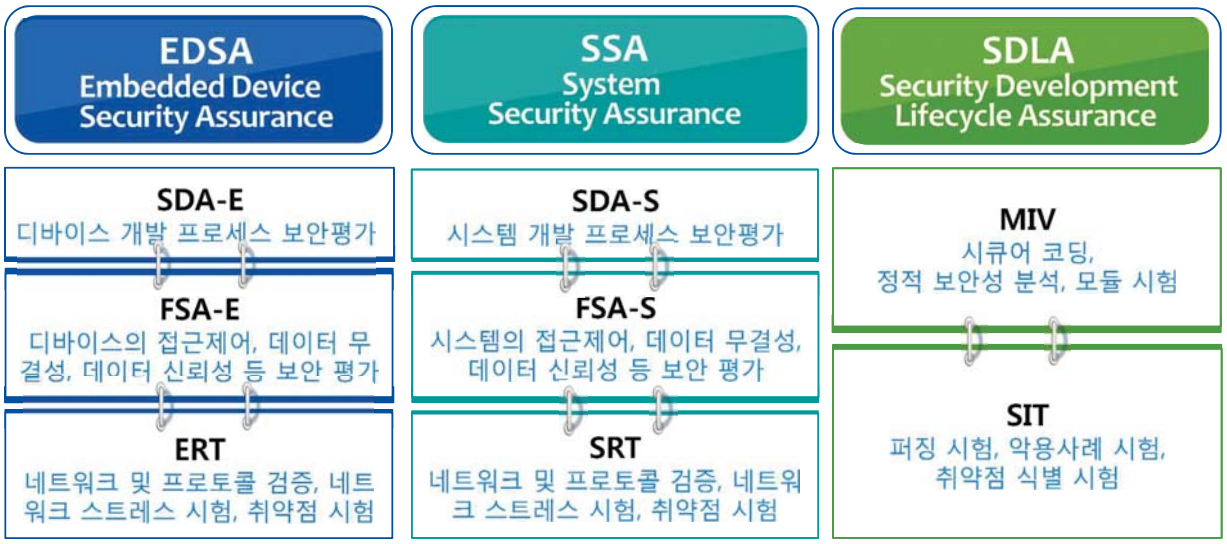
SSA: System Security Assurance
EDSA: Embedded Device Security Assurance
NERC: North American Electric Reliability Corporation
CIP: Critical Infrastructure Protection
IAEA: International Atomic Energy Agency
NISTIR: National Institute of Standards and Technology Interagency Report
RAMS: reliability, availability, maintainability and safety

International Standard
Industrial Standard

† 참조자료 : Tsutomu Yamada, et al., Trends and Developments in Security Standards for Secure Social Infrastructure Systems, Hitachi Review,2014

제어시스템 보안 관련 인증

ISA Secure™ Certification : IEC62443 기반 보안 적합성 인증 프로그램
- 네트워크 공격에 대한 대응 능력
- 알려진 취약점 공격에 대한 방어 능력
- **SAL (Security Assurance Level) 1,2,3,4 부여**

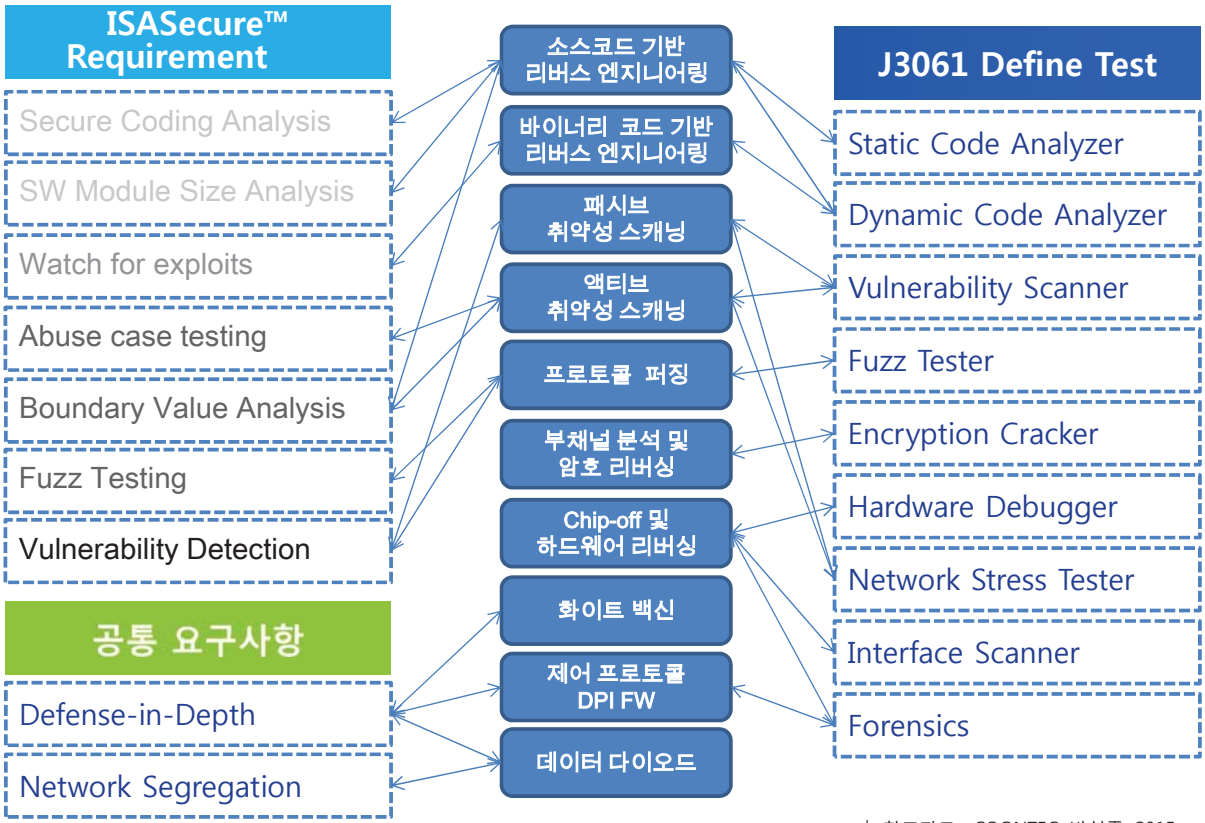


SDA-E (Security Development Artifacts for Embedded devices)
FSA-E (Functional Security Assessment for Embedded devices)
ERT (Embedded device Robustness Testing)

SDA-S (Security Development Artifacts for systems)
FSA-S (Functional Security Assessment for systems)
SRT(System Robustness Testing)

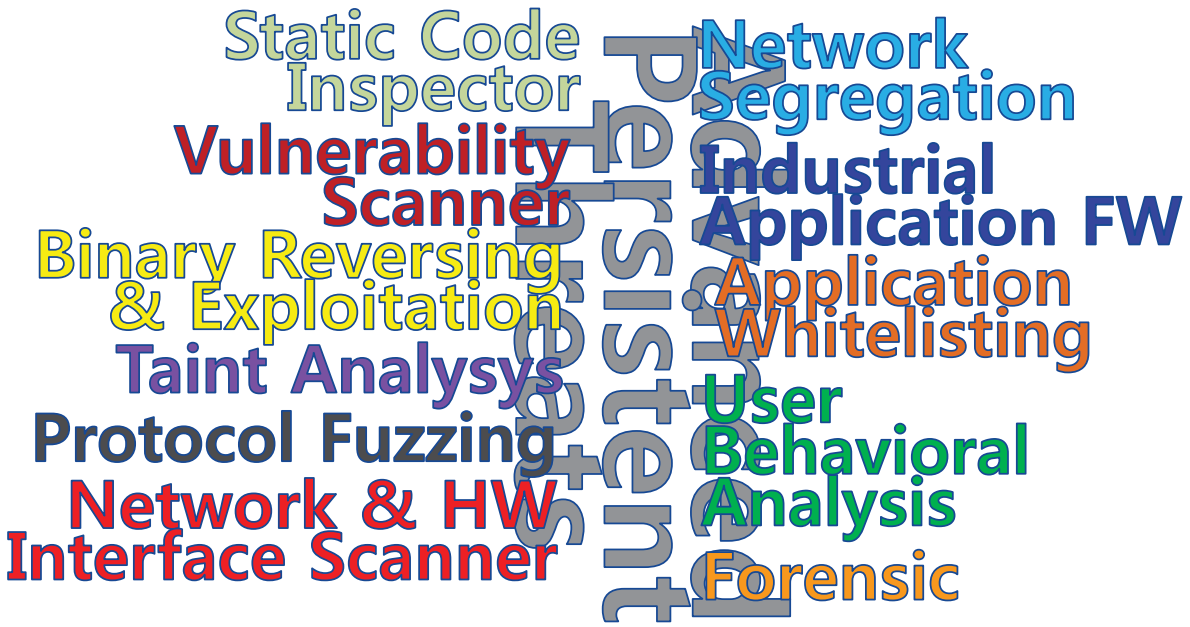
MIV (Module Implementation & Verification)
SIT (Security Integration Testing)

제어시스템 보안 관련 요구사항



† 참조자료 : COONTEC, 방혁준, 2015

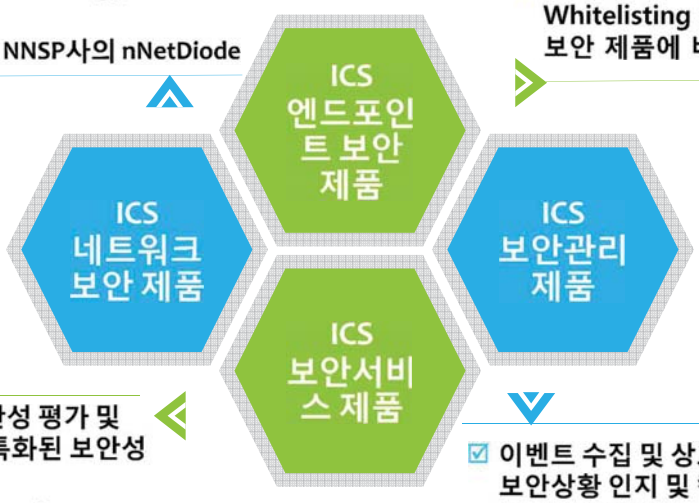
제어시스템 보안 관련 기술



제어시스템 보안 관련 상용제품

- ☑ 제어응용 패킷 검사 또는 단방향 데이터 통신을 통해 네트워크를 보호
- ☑ (국외) Tofino, Innominate Security, SecurityMatters, Owl Technology, Waterfall Security
- ☑ (국내) 제니스텍 ZCAP, NNSP사의 nNetDiode

- ☑ 정책 기반 접근제어와 시스템 자원 접근 행위 모니터링을 통한 보호
- ☑ 호스트 기반 IDS/IPS, AV, App Whitelisting 제품은 ICS 네트워크 보안 제품에 비해 아직 출시가 늦음



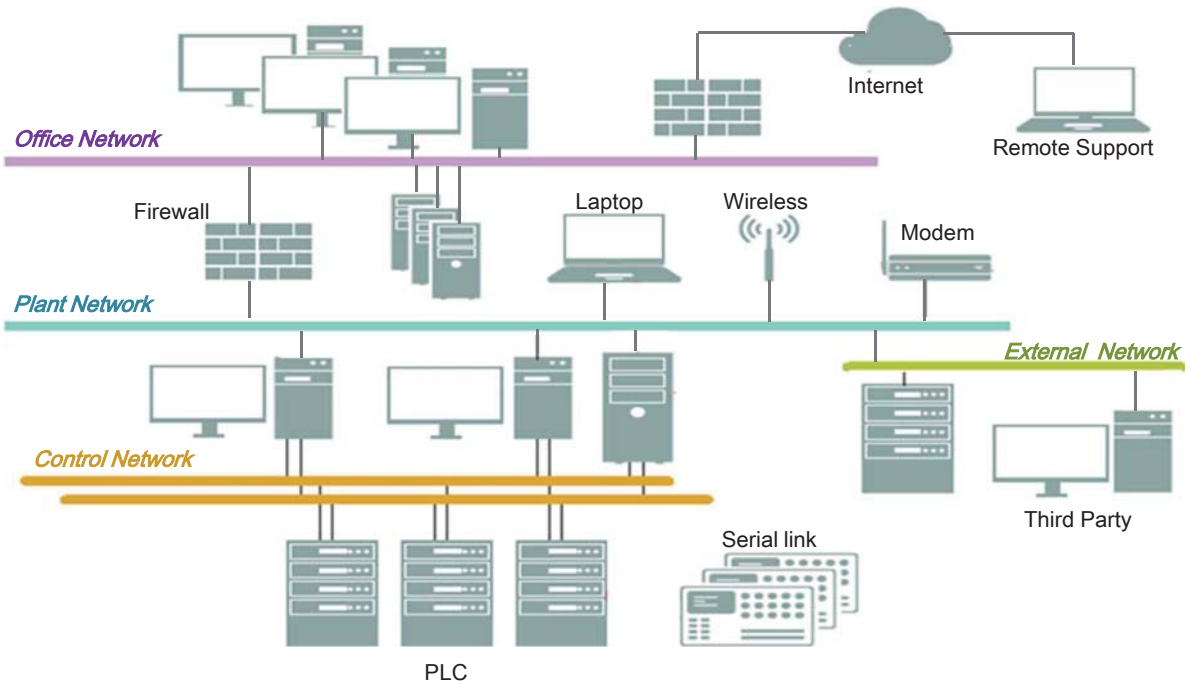
- ☑ ICS 취약점분석, 보안성 평가 및 패치 서비스, ICS에 특화된 보안성 인증 서비스 등
- ☑ Codenomicon사 Defensic, Wurldtech Security Technologies사 Achilles 등이 출시

- ☑ 이벤트 수집 및 상호연관 분석 기반 보안상황 인지 및 컴플라이언스 요구사항을 해결
- ☑ Industrial Defender사 Compliance Manager, AllenVault사 ICS SIEM 등

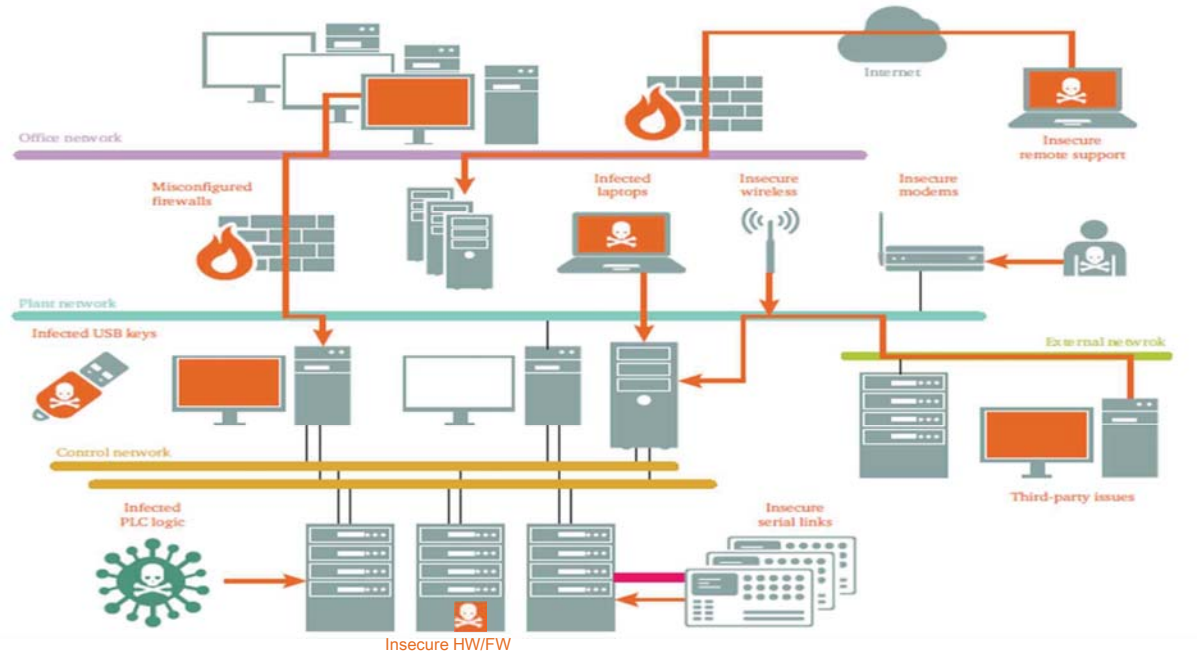
제어시스템 보안 기술 적용 현황

잠재적인 보안 취약성,
선제적과 방어적 기술 적용을 중심으로...

제어시스템 일반 구조



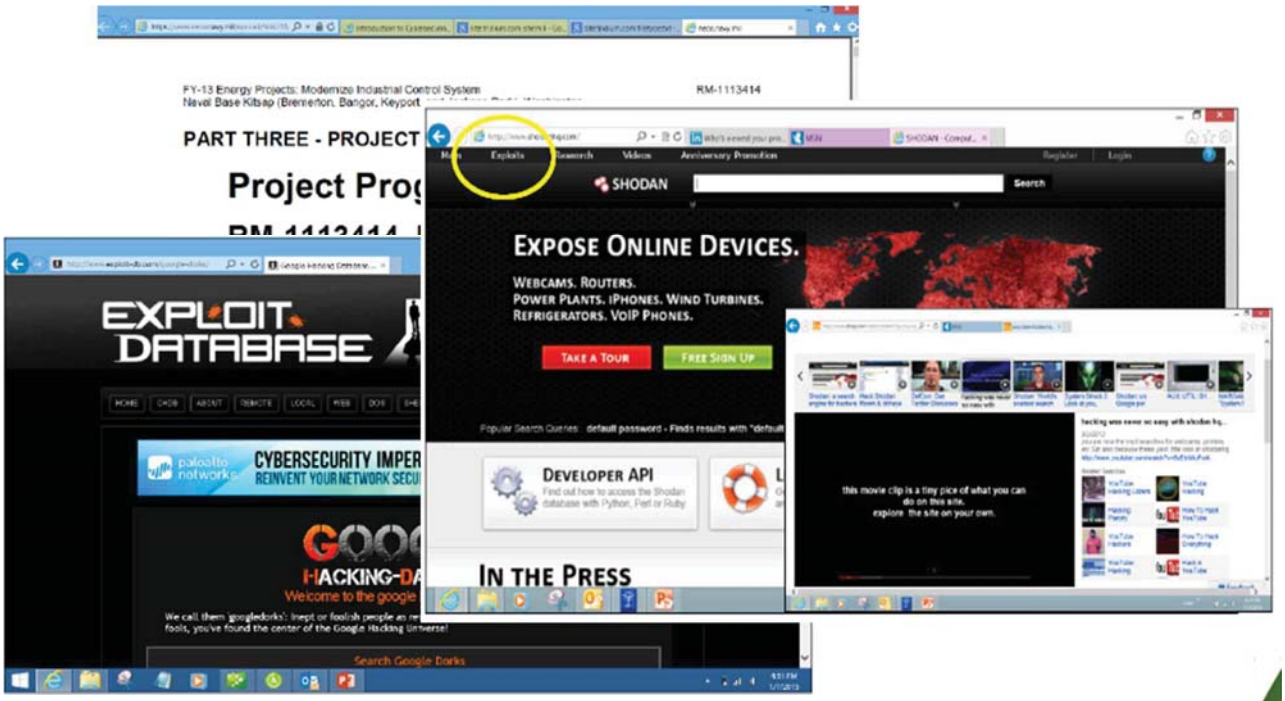
제어시스템의 잠재적인 보안 취약성



출처 : Eric Byres, Byres Security

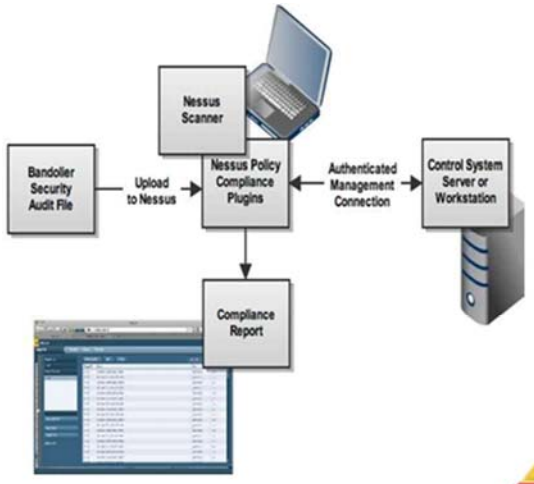
선제적인 보안(Offensive Security) 기술 적용 (1/3)

- Information Gathering



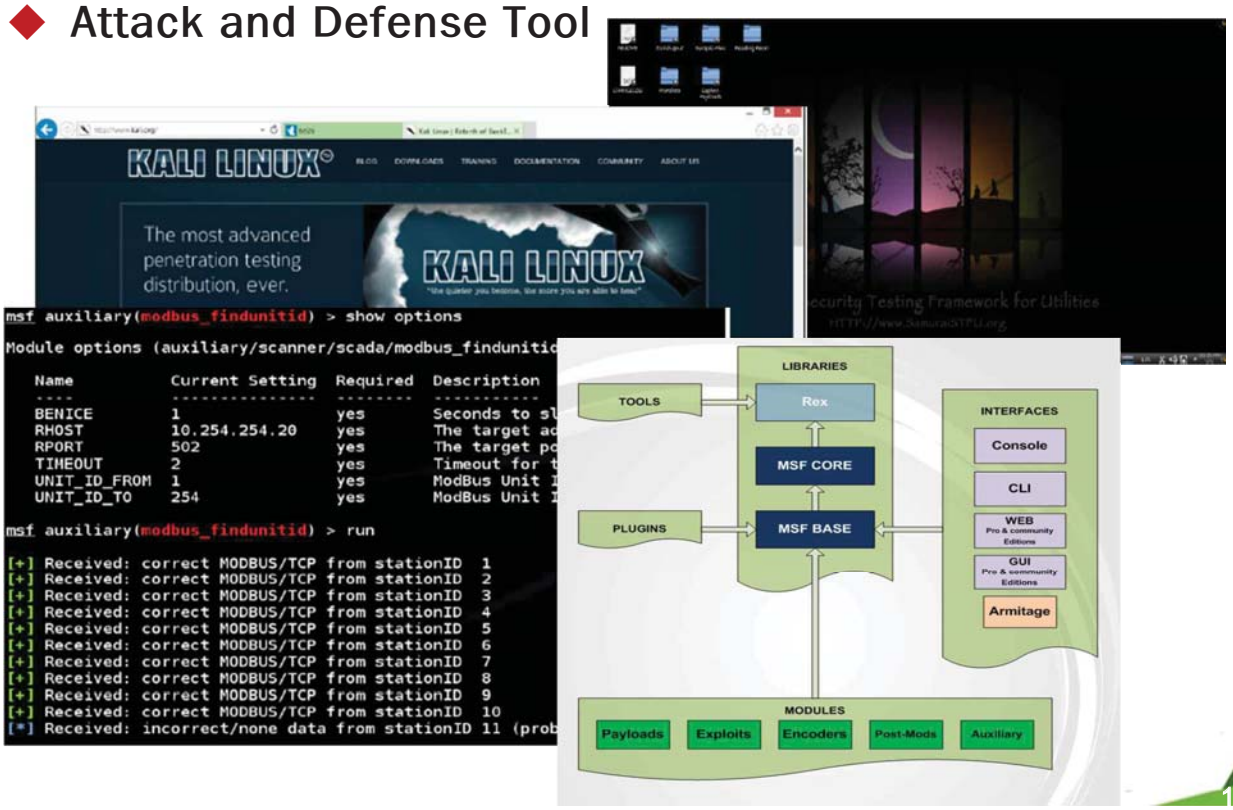
선제적인 보안(Offensive Security) 기술 적용 (2/3)

- Discovery & Monitoring



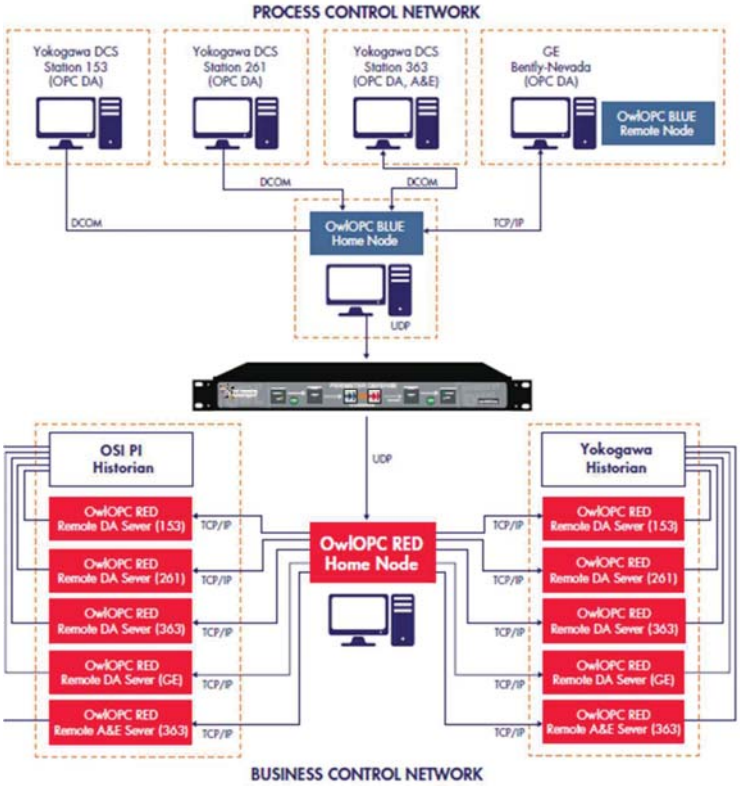
선제적인 보안(Offensive Security) 기술 적용 (3/3)

- Attack and Defense Tool



방어적인 보안(Defensive Security) 기술 적용 (1/2)

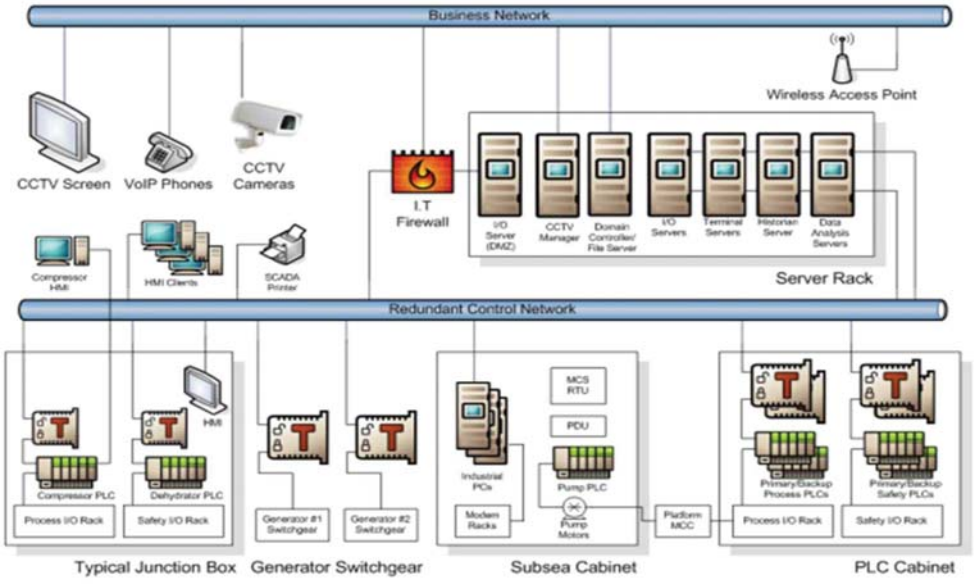
- Data Diode 적용
  - 제어망에 대한 외부 위협으로부터 원천 봉쇄 가능한 제어망 경계 보호



‡ 출처 : Beyond a Firewall: A New Class of Security Solutions to Segregate Networks, 2014

방어적인 보안(Defensive Security) 기술 적용 (2/2)

- 산업용 Security Appliance (DPI FW) 적용
  - 경계보안보다 내부위협에 대한 Defense-in-Depth 구조 구축



‡ 출처 : https://www.tofinosecurity.com/sites/default/files/CS-301-Gas-and-Oil-Platform-Cimation.pdf

It’s difficult,
but not all hope is lost.

감사합니다.