[정보보호] ITU-T SG17 산업제어시스템의 안전한 펌웨어 갱신

개요

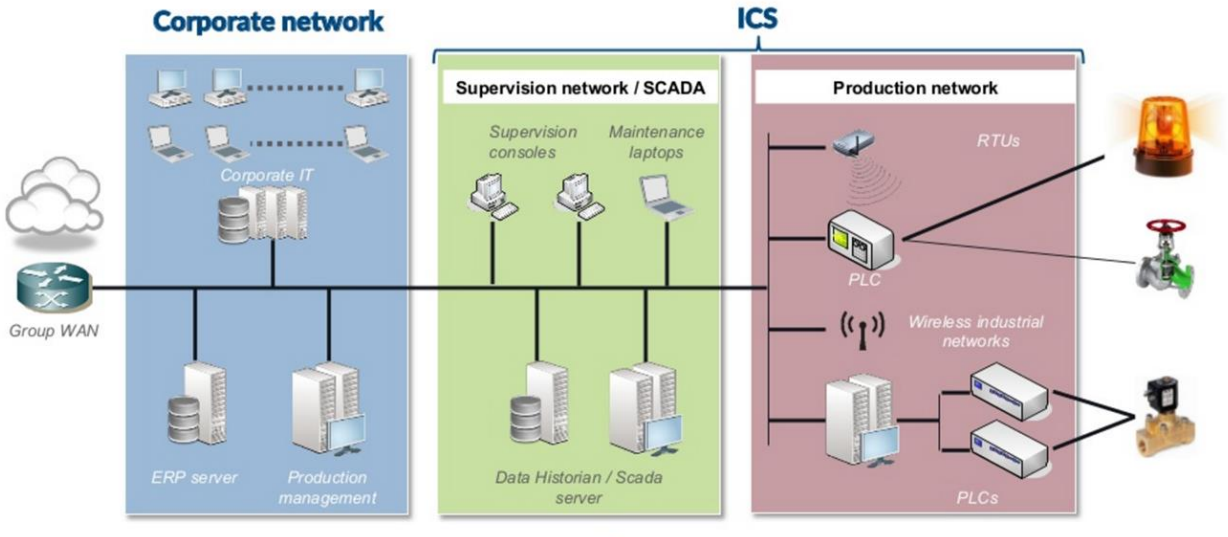
초기의 산업제어시스템은 독립적인 네트워크를 구성하고 있어서 외부 네트워크와는 분리되어 있어 안전하다는 의견을 갖고 있었으나, 악성코드에 의한 우회적 공격이 발생함으로 단순 공극(Air-gap)으로 대처하는 것에는 한계가 들어났다. 또한 정보통신(ICT: Information & Communication Technology) 기술의 발달로 산업제어네트워크는 비즈니스, 정보 공유 그리고 유지보수를 위하여 외부 네트워크와 연결이 필요하게 되었고, 이로 인하여 ICT의 보안 취약점도 전수되는 상황이 되었다. 그러나 산업제어시스템은 독립적인 플랫폼과 제어기술로 구축되어 있어서, ICT의 기 개발된 보안 메카니즘이 그대로 적용될 수 없다는 것이 문제로 인식되고 있다. 산업제어시스템 보안을 위하여 단 품의 보안 제품이나 서비스로 대응하는 것으로는 보안강도를 충족하지 못하는 것이 일반적이며, '심층 방어' 체계를 구축하여 종합적이고, 체계적인 보안 대책이 필요하다. 이와 상응하여 산업제어시스템 영역에 최적의 보안 수준을 유지하기 위하여 장비의 호환성을 제공하는 표준 기술의 필요성이 대두되고 있다.

산업제어시스템 이라는 용어는 산업생산 영역에서 사용되고 있는 여러 형태의 제어시스템이라는 용어가 일반화된 것이다. 산업제어시스템은 보통 SCADA (Supervisory Control And Data Acquisition), DCS (Distributed Control Systems), 그리고 PLC (programmable logic controllers)와 같은 제어시스템을 포함하며, 전력, 수자원, 석유, 가스, 교통과 같은 산업에서 보편적으로 활용되고 있다. 원격지에서 수신된 데이터를 기반으로, 자동화되거나 운영자에 의한 관리 명령은 원격지의 밸브나 차단기의 개폐와 센서로부터 데이터를 수집, 그리고 현장의 알람 상태를 모니터 하는 제어 장비들에게 전달될 수 있다. 산업 제어시스템은 주요 기반시설을 포함하며, 사이버 공격으로 인해 기능이 마비되면 국민의 생명, 생활, 재산, 국가 경제에 중대한 영향을 끼쳐 국가경제에 혼란을 초래할 수 있으므로, 일반 ICT (Information Communication Technology) 시스템과 비교해 볼 때 폐쇄성, 자원의 특수성, 운용 가용성 등의 측면에서 차이점이 있다. 산업제어시스템의 구조와 ICT와 비교하여 산업제어시스템 보안의 차이점과 산업제어시스템 관련 보안사고를 살펴본다.

산업제어시스템 구조

산업제어시스템은 산업 공정을 운영 또는 자동화하기 위하여 사용되는 장비, 시스템, 네트워크 그리고 제어로 구성되어 있다. SCADA 네트워크는 관리 목적으로 운영을 위한 데이터와 그리고 공정관리를 위한 제어능력을 제공하기 위하여 ICS (Industrial Control System)와 소통을 하는 시스템 또는 네트워크가 된다. 자동화는 계속적으로 진화하고 또 점점 중요한 위치를 차지하게 되었으며, 산업제어시스템(ICS)/SCADA의 사용은 널리 보급되고 있다.

산업제어시스템의 전통적인 구조는 인터넷과는 파이어월을 이용하거나, 아니면 공극(Air-gap)으로 분리가 되어있다. 그림1에서 산업제어시스템은 하부구조의 생산라인에서 작업공정의 상태를 알 수 있도록 센서가 존재하며, 이러한 센서로부터 데이터를 수집하여 상위 관리 사이트로 전달을 한다. 데이터는 관리서버에 지속적으로 저장되면서 현황판에 작업공정을 실시간적으로 상황을 알리며 정책에 의하여 사전 정의된 작업이면 조건에 따라 바로 다음 작업공정 지시가 하부 작업 네트워크로 전달되고, 액츄레이터를 통하여 작업공정의 조치가 이루어진다. 이러한 작업을 위하여 하부구조에는 현장 사이트들이 독립된 형태로 구성되어 있으며 이들 현장 사이트들을 상하 및 상호 통신을 위하여 SCADA가 교량역할을 한다.



[그림1] 산업제어시스템 구성도

(출처 : Industrial Control Systems, https://www.blackhat.com/docs/eu-14/materials/eu-14-Soullie-Industrial-Control-Systems-Pentesting-PLCs-101.pdf)

ICT와 산업제어시스템과의 비교

초기 산업제어시스템은 릴레이, 카운터 및 타이머 배치를 통한 하드웨어 형태로 구현하였으나, 프로그램이 가능한 집적회로 및 마이크로프로세서의 등장으로 PLC 제어기 형태로 발전되었다. 현재 산업제어시스템 설비들은 상호연결성과 원격 접근성 향상을 위한 ICT 기술 적용으로 보안 취약점 발생 가능성이 증대되는 단점을 가지게 되었다. 아래 [표1]은 일반 ICT 시스템과 산업제어시스템은 많은 차이점을 가지고 있어 보안관리체계 구축에 대하여 ICT와는 다른 접근방법을 고려 하여야 함을 보이고 있다. 즉, 산업제어시스템은 ICT (Information & Communication Technology)와 같이 정보를 획득하는 것에 주력을 하는 것이 아니고, 획득한 정보를 가지고 기반 설비를 제어하는 것이므로, 시스템의 정지는 재산상의 피해는 물론 안전에 큰 문제를 일으킬 수 있으므로 허용되지 않는다.

구분	ICT	제어시스템
요구성능	비 실시간	실시간
가용성	재시동 허용, 가용성 편차 허용	재시동 불허, 계획된 정지, 고 가용성
보호대상	정보	필드 장치, 프로세스
시스템운영	표준 OS 사용	전용 OS 사용
생명주기	단기[3~5년]	장기[15~20 년]
통신 프로토콜	TCP/IP 기반	전용프로토콜
SW변경관리	보안정책에 따라 자동적용	사전 시험 후 점진적 적용, 계획된 정지 시기에 적용
접근 용이성	지역에 국한, 접근 용이	넓은 영역에 퍼짐, 물리적 접근 노력 필요
보안솔루션	일반 ICT 시스템 대상 솔루션	사전 시스템 영향성/가용성 평가
파급효과	제한적 피해	재산 수준의 사회/경제적 피해
자원 제한	추가SW설치가능	백신,IDS등의 설치 어려움
A/S 지원	다향한 지원	단일 벤더지원

[표1] ICT와 산업제어시스템의 차이점

산업제어시스템 관련 보안사고(Incident)

산업제어시스템과 관련하여 발생된 사건, 사고를 정리하면 다음과 같다.

- 퇴사한 직원이 무선 네트워크를 이용하여 호주 퀸즈랜드의 폐수처리 제어 시스템을 해킹하여 오작동 유발, 세 달 동안 총 46차례 해킹하여 80만 리터의 폐수 무단 방출 (‘00)
- 미국 오하이오 주 데이비스-베시(Davis-Besse) 원자력발전소가 내부는 방화벽으로 보호되고 있었지만 설계사의 회사 네트워크에서 발전소로 원격 접속이 가능한 허점을 이용하여 슬래머 웜(Slammer Worm)에 감염. 원전 비안전 계통 신호 이상이 발생하여 원자력발전소 가동 중지(‘03)
- 슬래머 웜에 의한 스카다(SCADA) 시스템 감염으로 8시간 동안 해양 설비 플랫폼(Offshore Production Platform) 가동 중단. 생산 중단 및 재가동으로 약 1,200만 달러의 손실 발생(‘04)
- 다임러크라이슬러(DaimlerChrysler)의 미국 공장 시스템에서 사용 중인 마이크로소프트(Microsoft)의 Windows 2000 서버와 XP가 조톱 웜(Zotob Worm)에 감염되어 자동차 제조 공장 13곳 모두 1시간 가량 운영 중단(‘05)
- 이란 나탄즈(Natanz) 우라늄 농축시설 시스템의 유지보수를 위한 데스크톱이 유지보수 업체 직원의 실수로 스턱스넷에 감염되면서 IR-1 타입 원심 분리기 1,000여개 고장 및 교체(‘10)
- 미국 일리노이주 스프링필드 외곽의 상수도 시설에 원격 접속이 가능한 점을 악용한 해킹으로 제어 펌프에 장애 발생(‘11)
- 사우디아라비아의 정유회사인 아람코(Aramco)가 샤문(Shamoon)이라는 이름의 악성코드 감염으로 네트워크 마비(‘12)
- 카타르에서 두 번째로 큰 LNG 생산 시설인 라스가스(RasGas)가 알 수 없는 악성코드 공격에 의해 네트워크 마비(‘12)
- 스카다 시스템 업체 텔벤트(Telvent) 제품에 악성코드가 삽입(‘12)
- 마약 및 총기 밀수에 악용할 목적으로 벨기에 앤트워트항 콘테이너 관리 시스템 해킹(‘13)
- 전쟁 대피소로 사용되는 이스라엘 카멜(Carmel) 터널 개폐 장치 해킹으로 악성코드 감염, 이틀간 엄청 난 교통 혼잡 발생(‘13)
- 일본 몬주 원자력발전소 내부 작업자가 동영상 재생 프로그램을 업데이트하던 도중 악성코드에

감염, 42,000개 이상의 직원 개인 정보 노출('14)

향후 전망

산업제어시스템(사이버·물리시스템) 보안은 사물인터넷과는 구조와 대상이 다르지만, ICT기술을 이용한다는, 앞으로 이용하게 된다는 관점에서는 동일한 구조와 기술을 공유한다. 산업제어시스템은 사물인터넷과의 융합은 한국의 기술동향이나 정책의 흐름 관점에서 자연스럽게 보고 있다. 독립적으로 운영되고 있던 산업제어시스템은 ICT의 이점을 활용하기 위하여 융합을 추진하여 단방향 게이트웨이와 같은 상용화 장비가 출시되어 운영되고 있다. 그러나 마치 파이어월과 같이 경계를 방어하는 기법도 필요하지만 네트워크의 게이트웨이를 우회하는 공격에 대한 방어도 필요하다. 특히 발생하는 사고들을 분석한 결과 Zero-day 공격과 같이 이미 알려진 취약점에 대한 공격이 주요 기법으로 활용되고 있는 것을 고려해 볼 때에 기 알려진 취약점에 대한 유지보수, 즉 보안 업데이트가 적절히 수행되는 것이 필요하다. 이에 ITS, 사물인터넷, 산업제어시스템등과 같은 분야에 적용 가능한 펌웨어(소프트웨어) 갱신 메커니즘에 대한 논의가 ITU-T SG17 8월회의에서 있었으며, 타 표준문서와의 중복성 검토와 사물인터넷의 다양한 센서네트워크 구조를 반영하여 신규 표준제안에 대하여 한국, 일본, 영국간의 합의가 있었다.

나재훈 (전자통신연구원 정보보호연구본부 전문위원, ITU-T SG17 Q.7 라포처, jhnah@etri.re.kr)