情 報 保 護 學 會 誌
第19卷 第5號, 2009. 10

산업제어시스템 정보보호: 개요

전 용 희*

요 약

산업제어시스템은 전기, 수도, 수송, 화학, 제지, 자동차, 석유 및 가스와 같은 국가 주요 기반시설을 제어하는 시스템이다. 산업제어시스템이 기존의 고립적이고 폐쇄적인 시스템에서 점차 개방적이고 표준화된 시스템으로 전환되고 있으며, IT 망과의 통합이 이루어지고 있다. 산업제어시스템의 정보보호 기술은 일반적인 IT 정보보호 기술과는 특성상 여러 가지 차이점이 존재한다. 국내에서의 산업제어시스템 정보보호 기술에 대한 연구는 아직 미약한 수준이다. 따라서 본 논문에서는 국가 주요 정보하부구조를 구성하고 있는 산업제어시스템의 정보보호 기술 개요에 대하여 제시하고자 한다.

Ⅰ. 서 론

산업제어시스템(ICS: Industrial Control System)이란 산업 부문 및 주요 하부구조에서 자주 사용되는 여러 가지 형태의 제어 시스템을 포함하는 일반적인 용어이며, SCADA(Supervisory Control And Data Acquisition) 시스템, DCS(Distributed Control System), PLC (Programmable Logic Controllers), PCS(Process Control System) 등을 포함한다.

SCADA 시스템은 중앙 데이터 획득 및 감시 제어를 사용하여 분산된 장치를 제어하기 위하여 일반적으로 사용된다. DCS는 감시 및 조정 제어(supervisory and regulatory control)를 사용하여 공장과 같은 근거리 지역 내의 생산 시스템을 제어하기 위하여 일반적으로 사용된다. PLC는 특정 응용을 위한 이산 제어(discrete control)를 위하여 일반적으로 사용되며 조정 제어를 제공한다. PCS는 특정 프로세스의 출력을 제어하기 위한 구조, 메커니즘 및 알고리즘을 다루는 시스템이다. 통상적으로 사용되는 PCS는 PLC로 구현될 수 있으며, 좀 더 복잡한 시스템은 DCS나 SCADA 시스템에 의하여 제어될 수 있다.

산업 제어 시스템의 동작은 매우 유사하나, 몇 가지 측면에서 다르다. SCADA는 지역적으로 분산된 현장 사이트를 위한 것인 반면에, DCS와 PLC-제어 서브시스템은 더욱 한정된 공장이나 공장-중심 지역 내에 보통 위치한다. DCS와 PLC 통신은 보다 신뢰적이고 고속의 근거리 통신망(LAN)을 통하여 이루어지는 반면, SCADA 시스템은 장거리 통신 시스템에 의하여 이루어진다. DCS와 PLC 시스템은 SCADA 시스템 보다 높은 정도의 폐루프 제어(closed-loop control)를 채택하고 있다. 이러한 차이점이 분명히 존재하지만, ICS의 정보보호 관점에서는 이러한 차이점이 그 다지 크다고 생각할 수 없다. 따라서 본 논문에서는 이 들 사이를 따로 구분하지 않으며, 공통적으로 ICS로 부르기로 한다. 특별히 제한적으로 명기될 필요가 있을 경우에만, 특정 시스템의 이름을 사용하기로 한다.

ICS는 전기, 수도, 수송, 화학, 제지, 자동차, 석유 및 가스와 같은 광범위한 산업에 사용되고 있다. 원격 스테이션으로부터 받은 정보를 기반으로, 자동화된 혹은 운영자-구동 감시 명령이 필드 장치인 원격 스테이션 제어 장치로 보내진다. 필드 장치는 밸브와 차단기 개폐, 센서 시스템의 데이터 수집, 경보 조건에 대한 지역 환경 감시와 같은 지역 운용을 통제한다.

초기에는 ICS가 특별한 하드웨어와 소프트웨어를 사용하여 독점적인(폐쇄적인) 제어 프로토콜을 수행하는 고립 시스템이었기 때문에 전통적인 IT 시스템과는 상당히 거리가 있었다. 근래에 와서, IP(Internet Protocol) 장치가 독점적인 솔루션들을 대체하고 있어, 사이버 보안 취약성 및 사고의 가능성을 증대시키고 있다. 그러나 ICS의 보안 특성은 기존 IT 시스템 보안과는 큰 차이가

* 대구가톨릭대학교 컴퓨터정보통신공학부(yhjeon@cu.ac.kr)

존재한다. 예를 들어, 일반적으로 기존 IT 시스템의 보안 목적은 기밀성, 무결성, 가용성(CIA: Confidentiality, Integrity, Availability)의 순서를 따르나, ICS에서는 그 순서가 AIC로 바뀐다. 그러므로 ICS 환경에 적합한 새로운 정보보호 솔루션이 필요하다고 할 수 있다.

본 논문에서는 ICS 정보보호를 위한 전반적인 개요에 대하여 다루고자 한다. 이를 위하여 먼저 ICS 관련 시스템에 대한 설명을 제시하고, ICS와 기존 IT 시스템의 특성 차이점을 분석해보고, ICS의 보안 위협 및 취약성을 제시하고, ICS 보안 사고에 대하여 분석 기술하고자 한다.

Ⅱ. 관련 시스템

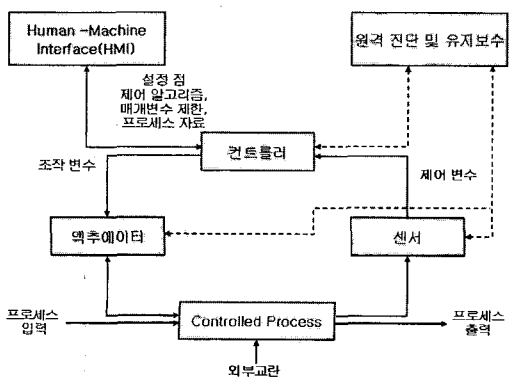
2.1 산업제어시스템(ICS)

산업 제어 프로세스는 일반적으로 다음과 같은 두 가지가 있다:

- 연속 제조 프로세스: 연속적인 프로세스로 운영되며, 다른 등급의 제품을 제조하기 위하여 전이(transition)할 수 있다. 대표적인 제조 프로세스로는 발전소의 연료 혹은 스팀 플로, 정유소의 석유, 화학 공장의 증류 과정 등이 있다.
- 배치(batch) 제조 프로세스: 일정한 량의 물질로 수행되는 분명한 제조 단계를 가지며, 한 배치 프로세스를 위한 분명한 시작 및 종료 단계가 있다. 식품 제조가 대표적인 배치 제조 프로세스이다.

[그림 1]은 ICS의 기본 동작을 보여준다.

주요 컴포넌트는 다음과 같다:



[그림 1] ICS 동작

- 제어 루프: 측정용 센서, PLC와 같은 컨트롤러 하드웨어, 제어 밸브, 스위치 및 모터, 차단기와 같은 액추에이터(actuator), 변수들의 통신으로 이루어진다. 센서로부터 컨트롤러로 제어 변수가 전송된다. 컨트롤러는 신호를 해석하고, 설정 점(set point)을 기초로 해당 조작 변수를 생성하여 액추에이터로 전송한다.
- HMI(Human-Machine Interface): 운영자와 엔지니어는 HMI를 사용하여 설정 점을 감시하고 구성하며, 알고리즘을 제어하고, 컨트롤러의 파라미터를 조정하고 확립한다. 이를 통하여 프로세스 상태 정보와 히스토리 정보도 디스플레이 한다.
- 원격 진단 및 유지보수 설비: 비정상 동작이나 실패를 방지하고, 식별하고, 복구하기 위하여 사용되는 설비이다.

ICS의 주요 제어 컴포넌트는 다음과 같다: 제어 서버, SCADA 서버 혹은 MTU(Master Terminal Unit), RTU(Remote Terminal Unit), PLC, IED(Intelligent Electronic Devices), HMI, 데이터 히스토리안(Historian), I/O 서버. IED는 지능형 센서/액추에이터를 의미하며, 데이터 히스토리안은 ICS 내의 모든 프로세스 정보를 기록하기 위한 중앙 데이터베이스이다.

ICS 네트워크의 주요 컴포넌트는 다음과 같다:

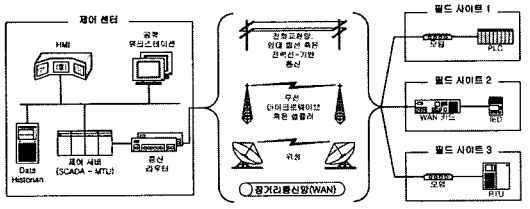
- 필드버스 네트워크: 센서와 다른 장치들을 PLC나 다른 컨트롤러에 연결한다.
- 제어 네트워크: 감시 제어 레벨을 하위-레벨 제어 모듈로 연결한다.
- 통신 라우터: 두 네트워크 사이의 메시지를 전달하는 통신 장치이다. LAN을 WAN에 연결하거나, MTU와 RTU를 SCADA 통신을 위한 장거리 통신 매체에 연결하기 위하여 사용된다.
- 방화벽: 미리 정해진 필터링 정책을 이용하여 통신 패킷을 감시하고 제어하여 네트워크 상의 장치를 보호한다. ICS 네트워크 분리(격리) 정책을 관리하는데도 유용하다.
- 모뎀: MTU와 원격 현장 장치 사이의 장거리 통신을 위하여 SCADA 시스템에서 흔히 사용된다.
- 원격 액세스 포인트: 원격으로 제어 시스템을 구성하거나 프로세스 데이터를 접근하기 위한 제어 네트워크의 별도 장치, 지역 및 위치를 의미한다.

2.2 SCADA 시스템

SCADA 시스템은 중앙 데이터 획득이 제어만큼 중요한 분산된 자산을 제어하기 위하여 사용된다. SCADA 시스템은 수많은 프로세스 입력과 출력에 대한 중앙 감시 및 제어 시스템을 제공하기 위하여 데이터 획득 시스템과 데이터 전송 시스템 및 HMI 소프트웨어를 통합한다. 필드 정보를 수집하여 중앙 컴퓨터 설비로 전달하여 운영자에게 정보를 디스플레이하고, 실시간으로 중앙 위치에서 전체 시스템을 감시하거나 제어하도록 해준다.

SCADA 시스템은 하드웨어와 소프트웨어로 구성된다. 대표적인 하드웨어로는 제어 센터에 설치된 MTU, 무선/전화선/케이블/위성과 같은 통신 장비, 액추에이터를 제어하고 센서를 감시하는 RTU 혹은 PLC로 구성된 한 개 이상의 지역적으로 분산된 필드 사이트를 포함한다. MTU는 RTU 입력 및 출력 정보를 저장하고 처리하며, RTU나 PLC는 지역 프로세스를 제어한다.

[그림 2]는 SCADA 시스템의 컴포넌트와 일반적 구성을 보여준다.



〔그림 2〕 SCADA 시스템 일반적 배치

SCADA 서버(MTU)와 통신 라우터는 제어 센터에 위치한다. 다른 제어 센터 컴포넌트로는 LAN에 의하여 모두 연결된 HMI, 공학 워크스테이션, 데이터 히스토리안(Data Historian)이 있다. 제어 센터는 필드 사이트에서 수집된 정보를 모으고 기록하며, HMI에게 정보를 디스플레이하고, 탐지된 이벤트에 따라서 조치를 내릴 수 있다. 또한 중앙 경보, 동향 분석 및 보고에 대한 책임도 진다. 필드 사이트는 액추에이터의 지역적 제어와 센서 감시를 수행한다. 필드 사이트는 필드 운영자가 네트워크 연결을 통하여 원격 진단을 수행하고 통상적인 보수작업을 할 수 있도록 원격 접근 능력을 갖춘 장비를 보유하고 있다.

2.3 분산 제어 시스템(DCS)

DCS는 정유공장, 수도 및 폐수 처리, 발전소, 화학 제조 공장, 제약 처리 설비와 같은 산업을 위한 동일 지역 위치 안의 생산시스템을 제어하기 위하여 사용된다. 이런 시스템은 대부분 프로세스 제어나 이산 부분 제어 시스템이다. DCS는 전체 생산 프로세스를 수행하는 전반적 업무를 공유하는 한 그룹의 지역 컨트롤러들을 중재하기 위하여 중앙 감시 제어 루프를 사용한다. 생산시스템을 모듈화하여 전체 시스템에 대한 단일 결점의 충격을 감소시킨다. 많은 현대적인 시스템에서 DCS는 생산의 비즈니스 운영 관점을 주기 위하여 사내망과 연동된다.

DCS는 하위 레벨의 생산 프로세스부터 사내 혹은 엔터프라이즈 계층까지 전체적인 설비를 포함한다. 감시 제어기(제어 서버)는 제어 네트워크를 통하여 하부 설비와 통신한다. 제어 서버는 분산 필드 컨트롤러에게 설정 점을 전송하고 데이터를 요구한다. 분산 컨트롤러는 제어 서버 명령과 프로세스 센서로부터의 센서 피드백을 기반으로 프로세스 액추에이터를 제어한다.

2.4 PLC

PLC는 피드백 제어를 통한 지역 프로세스 관리를 제공하기 위하여 전체적인 계위 시스템의 제어 컴포넌트로서 SCADA와 DCS 시스템에 사용된다. SCADA 시스템의 경우에는 RTU와 같은 기능을 제공한다. DCS에 사용될 때에는 감시 제어 스킴 안의 지역 컨트롤러로 구현된다. 소규모 제어 시스템 구성에서는 주요 컴포넌트로 구현되기도 한다.

I/O 제어, 로직, 타이밍, 카운팅, 제어, 통신, 연산 및 데이터 파일 처리 같은 특정 기능을 구현할 목적으로 명령어를 저장하기 위한 사용자-프로그램 가능 메모리를 가진다. 공학 워크스테이션에 위치한 프로그래밍 인터페이스를 통하여 접근이 가능하며, LAN 상에 연결된 데이터 서버에 데이터가 저장된다.

2.5 산업 부문 의존성

대표적으로 전력 송배전망에서 지역적으로 분산된 SCADA 제어 기술을 사용한다. SCADA 시스템이 지역 원격 필드 제어 스테이션으로부터 데이터를 수집하

여 전력 분배를 감시하고 제어하며 중앙 위치로부터의 명령을 내린다. 또한 물, 석유 및 가스 분배, 하수 처리 수집 시스템 등을 감시하고 제어하기 위하여 사용된다.

SCADA와 DCS는 흔히 네트워크로 서로 연결된다. 이것은 전력 제어 센터와 발전 설비의 경우에 해당한다. 발전 설비 운영이 DCS에 의하여 제어되지만, DCS는 전송과 배전 명령과 생산 출력을 조정하기 위하여 SCADA 시스템과 통신하여야 한다.

국내 주요 하부구조(Critical Infrastructure)도 물리적이고 또한 수많은 정보 통신 기술을 통하여 복잡하게 고도로 연결되어 있으며 상호 의존적이다. 한 하부구조에서의 사고가 연속적으로 증폭되어 다른 하부구조에 직·간접적으로 영향을 미칠 수 있다.

전력이 상호의존적인 주요 하부구조의 가장 광범위한 소스 중의 하나로 여겨진다. 한 예로써, 전력 전송 SCADA 시스템에서 사용되는 마이크로웨이브 통신 네트워크의 붕괴로 연속적인 실패가 개시될 수 있다. 감시 및 제어 능력이 없어 대규모 발전 단위가 격리되고 전송 변전소에서의 전력 손실을 초래하는 이벤트가 발생할 수 있다. 이런 손실이 주요 불균형을 일으키고 전력 그리드를 통한 연속 실패를 야기 시킬 수 있다. 이것은 다시 대규모 정전 사태를 불러오고, 석유 및 가스 생산, 정유소 운영, 수 처리 시스템, 폐수 수집 시스템과 같은 전력에 의존하는 모든 산업에 심각한 영향을 미칠 수 있다.

특히 우리나라에서는 지능형 전력망(Smart Grid)을 개발하고 적극적인 도입을 계획하고 있어, 이런 국가적인 주요 하부구조에 대한 정보보호 대책을 철저하게 강구해야 될 것으로 생각한다.

Ⅲ. ICS 특성 분석

서론에서도 기술한 바와 같이, ICS가 연결성과 원격 접근 능력을 증진시키기 위하여 IT 솔루션들을 점차적으로 채택하고 있다.

IT 시스템과 산업제어시스템과의 통합이 증가하고 있지만, 여전히 많은 차이가 존재한다. [표 1]에 몇 가지 중요한 차이점이 요약되어 있다. 산업제어시스템 보안 관련 연구를 위하여 이런 개별적인 특성을 잘 이해하는 것이 필요하다.

요약하면, ICS와 IT 시스템 사이의 운영 및 위험 차이가 보다 정교화 된 정보보호 전략 적용에 대한 필요성을 증대시킨다. 제어 시스템 운영과 관련된 보안 솔루션의 설치, 운영 및 유지보수가 가지는 가능한 의미를 이해하기 위하여, 제어 엔지니어, 제어 시스템 운영자

〔표 1〕 IT 시스템과 산업제어시스템 차이

분류	IT 시스템	산업 제어 시스템
성능 요구	비실시간, 일정한 응답, 처리력 속도에 대한 엄격한 요구, 지연 및 지터 허용	실시간, 시간에 민감한 응답, 적당한 처리력 속도 허용, 지연 및 지터는 심각한 문제
가용성 요구	rebooting 허용, 시스템 운영 요구사항에 따라 가용성 편차가 허용됨	rebooting 불허용, 높은 가용성 요구, 계획된 가동 정지
위험 관리 요구	데이터 비밀성과 무결성이 가장 중요, 일시적인 가동 중지 허용(결함 감내 시스템 불급), 비즈니스 운영 방해가 최대 위험	인명 및 생산 시스템 관점의 안정성이 가장 중요, 일시적 가동 중지 불허용(결함 감내 시스템 중요), 인명, 프로세스 장비 혹은 생산 능력의 손실이 최대 위험
보안 구조	컴퓨터 관련 자산 및 저장/전송 정보 보호 목적, 중앙 서버 보안	제어 장치와 PLC 같은 필드 장치 보호
보안 솔루션	대표적인 IT 시스템을 대상으로 설계	ICS 운영을 보증하도록 설계되지 않음
시간 민감 상호작용	비상사태 시 상호작용이 덜 민감, 원하는 정도로 시스템 자원에 대한 접근 통제 제한	비상사태 시 인간 혹은 다른 상호작용에 대한 대응이 매우 중요, 제어 시스템에 대한 접근이 엄격이 규제되어야 함.
시스템 운영 및 변경 관리	표준 운영 체제 사용하도록 설계, 갱신이 단순하고 자동화된 도구 이용가능	특별히 채택된 운영체제와 표준 운영체제 혼용, 소프트웨어 변경은 단계적 수행, 공급자 참여 필요
자원 제한	보안 솔루션과 같은 제3자 응용의 추가를 지원하는 충분한 자원이 이용가능	산업 프로세스를 위한 특화된 설계, 보안 솔루션을 위한 메모리 용량 및 컴퓨팅 자원이 제한
통신	표준 통신프로토콜, 주로 유선 네트워크 및 지역 무선 네트워크, 대표적인 IT 네트워크 실제 기반으로 구축	많은 독점적 통신 프로토콜 존재, 전용선/광섬유/무선링크/위성과 같은 다양한 형태의 매체 사용, 네트워크가 복잡하고 제어시스템에 대한 지식 요구
관리지원	다양한 지원형태 가능	소수의 벤더에 의해서만 가능
서비스 생명	3~5년의 짧은 생명주기	15~20년의 긴 생명주기
요소접근	지역에 설치되고 접근용이	고립되고 지역적으로 원격지에 있어 접근이 어려움

및 보안 전문가의 협동 팀이 밀접하게 일할 필요가 있다.

Ⅳ. ICS 취약성 분석

4.1 위협 요소

제어 시스템에 대한 위협은 산업 스파이, 불만을 품은 종업원, 악성 침입자 및 시스템 복잡성, 인간 실수 및 사고, 장비 실패 및 자연 재해와 같은 자연적 소스와 같이 다양한 소스로부터 발생할 수 있다. 자연적 위협뿐만 아니라 악의적인 위협에 대하여 보호하기 위하여, ICS 심층 방어 전략을 세울 필요가 있다. 다음은 ICS에 대하여 가능한 위협을 보여주는 목록이다:

- 스파이웨어/멀웨어: 스파이웨어 및 멀웨어를 생성하고 배분하는 공격을 수행할 수 있다. 각종 컴퓨터 바이러스 및 웜 등이 여기에 해당한다.
- 봇-넷(Bot-Net): 공격을 조정하기 위하여 수많은 좀비 컴퓨터들을 장악할 수 있다. 최근 국내에서 발생한 7.7 분산 서비스 거부(DDoS: Distributed Denial of Service) 공격 대란처럼 침해된 머신들이 이용될 수 있다.
- 스팸 메일: 피싱 공격, 스파이웨어/멀웨어 분배, DoS 공격 등을 수행하기 위하여 스팸 메일을 이용할 수 있다.
- 외부 공격: 금전적인 이득을 위한 외부자 공격이나 외국 기관의 정보 수집 및 스파이 활동 등이 가능하다.
- 내부 공격: 불만을 품은 내부자 공격 발생이 가능하다.
- 피싱(Phishing): 금전적인 이득을 위하여 신원이나 정보를 훔치려는 시도가 가능하다. 스팸/스파이웨어/멀웨어 등을 이용할 수도 있다.
- 기타: 국가 안보를 위협하는 테러리스트 그룹이나 산업 스파이 등에 의한 위협도 존재한다.

이런 위협은 아래와 같은 요인에 의하여 점점 더 증대되고 있다:

- 표준 프로토콜 및 기술의 채택: ICS에 사용되는 프로토콜이 독점적인 시스템에서 MS 윈도우, Unix, TCP/IP와 같은 표준 기술 및 네트워킹 프로토콜로 옮겨가고 있다. 이런 표준 프로토콜 및 기술에는 통상적으로 알려진 취약성이 존재하며, 정교한 공격 툴에 의하여 영향을 받을 수 있다.
- 제어 시스템의 증가된 연결성: ICS와 기업 IT 시스템이 정보 관리, 운영 및 비즈니즈 필요에 의한 여러 가지 변화의 결과로 빈번하게 서로 연결된다. 제어시스템은 원격이나 지역 스테이션과 개별 장비들에게 데이터를 전송하기 위하여 WAN이나 인터넷을 더 많이 사용한다. 이런 제어시스템의 공중망과 기업망과의 통합이 제어 시스템 취약성에 대한 접근성을 증가시키고 있다.
- 불안전한 연결: 기업망과 ICS의 상호연결은 다른 통신 표준을 가진 시스템의 통합을 요구한다. 결과적으로 두 개의 별개의 시스템 사이에 데이터를 성공적으로 이동하기 위하여 설계된 인프라가 이용된다. 상이한 시스템의 통합에 따른 복잡성 때문에, 제어 기술자들은 보안 위험에 대한 추가된 부담을 다루지 않는다. ICS 보안 설계에도 보안 전문가들이 배제되는 경우가 많다.
- 제어시스템 정보 공개: ICS 설계, 유지보수, 상호연결 및 통신에 관한 공개 정보들이 인터넷을 통하여 쉽게 구할 수 있다. 이런 공개 정보를 이용한 사이버 공격 발생이 가능하다. 실제로 2000년 봄에 발생한 호주의 Maroochy Shire 하수처리장 사고가 제어시스템 운영에 대한 내부 지식을 이용하여 발생하였다.

4.2 취약성

이 절에서는 대표적인 ICS의 취약성을 간단히 열거한다. 취약성은 아래와 같은 세 개의 범주로 나뉠 수 있다:

- 정책 및 절차: ICS 보안에 관한 정책 및 구현 지침이 불완전하거나, 부적절하거나, 혹은 없는데서 오는 취약성이다.
- 플랫폼: 하드웨어, 운영체제 및 ICS 응용을 포함하는 플랫폼의 결점, 잘못된 구성 및 열악한 유지보수로 인하여 발생하는 취약성이다. 이런 취약점은 운영체제 및 응용 패칭, 물리적 접근 제어 및 항바이러스 소프트웨어와 같은 보안 소프트웨어 등의 보안 제어를 통하여 완화될 수 있다.
- 네트워크: ICS 네트워크와 다른 네트워크와의 연결에서의 결점, 잘못된 구성 및 열악한 관리로 발생할 수 있다. 심층 네트워크 설계, 통신 암호화,

네트워크 트래픽 흐름 제한 및 네트워크 컴포넌트에 대한 물리적 접근 제어를 통하여 없애거나 완화될 수 있다.

V. 사고분석

5.1 사고 근원지

ICS와 프로세스에 직접 영향을 미치는 사이버 보안 성질을 추적하기 위하여 설계된 ISID(Industrial Security Incident Database)가 존재한다. 여기에는 우연적인 사이버-관련 사고뿐만 아니라, 불법 원격 접근, DoS 공격 및 멀웨어 침투와 같은 고의적 사건 모두를 포함한다. 데이터는 공공연히 알려진 사고에 대한 연구 및 멤버조직으로부터의 개별 보고를 통하여 수집된다. 모든 사고가 조사되며 신뢰성에 따라서 등급화 되었다.

2006년 6월까지, 119 건의 사고가 조사되었고 데이터베이스에 기록되었다. 분석 결과에 따르면, 공격의 근원지는 간접적으로 사내망을 통하거나 혹은 직접적으로 인터넷을 통한 공격, 가상사설망(VPN), 무선 네트워크 및 다이얼-업 모뎀 등과 같이 여러 장소로부터 발생하고 있음을 보여준다. 제어시스템 사고는 아래와 같이 세 가지의 광범위한 범주로 구분될 수 있다:

- 파일에 대한 허용되지 않는 접근, DoS 공격 수행, E-mail 스푸핑(예를 들어, 송신자의 신분 위조)과 같은 의도적인 타깃 공격
- 비의도적인 결과 혹은 웜, 바이러스 혹은 제어 시스템 실패에 따른 부차적 손실
- 운용 시스템의 부적절한 시험 혹은 허용되지 않는 시스템 구성 변경과 같은 비고의적 내부 보안 결과

위의 세 개중에서, 타깃 공격이 가장 작았다. 타깃 공격은 가장 피해 가능성이 많은 공격으로 시스템과 지원 하부구조에 대한 세부적인 지식을 필요로 한다. 그러므로 가장 가능성 있는 위협 에이전트는 비고의적 위협과 불만을 품은 고용자, 전직 고용자 및 조직에 관련된 다른 사람들로 분석하고 있다.

5.2 주요 사고 일지

본 절에서는 보고된 주요 사고에 대하여 위의 범주에 따라 간략히 소개한다. 먼저 고의적 사고는 아래와 같다:

- Maroochy Shire 하수 범람: 2000년 봄에 발생한 사고로, 공장 제조 소프트웨어를 개발하는 호주의 한 전직 종업원이 지역공무원에 응시하였으나 실패하자, 무선 전송장치를 이용하여 하수처리시스템 제어를 원격으로 침투하였다. 특정 하수 펌프장의 전자 데이터를 변경하고 오동작을 일으킴으로써 결과적으로 인근 강과 공원에 약 264,000 갤런의 미처리 하수를 방출하게 하였다.

비고의적 결과로는 다음과 같은 것이 있다:

- CSX 열차 신호 시스템: 2003년 8월, Sobig 컴퓨터 바이러스가 미국 동해안의 열차 신호 시스템을 정지시키는 원인이 되었다. 바이러스가 플로리다 잭슨빌에 있는 CSX사의 본부 컴퓨터 시스템을 감염시켜 신호, 급전 및 다른 시스템을 정지시킨다. 이 사고로 많은 열차 운행이 중지되거나 지연되었다.
- Davis-Besse 원자력 발전소: 2003년 1월에 MS SQL 서버 웜인 Slammer가 미국 Ohio주에 위치한 정지된 Davis-Besse 원자력 발전소의 사설 컴퓨터 네트워크를 감염시켰다. 이 사고로 거의 5시간동안 안전감시시스템이 불능화되고, 발전소의 프로세스 컴퓨터가 고장 나서 다시 동작하기 까지 약 6시간이 소요되었다. 이 슬래머 웜은 적어도 다섯 개의 다른 유틸리티의 제어망 통신에 영향을 미친 것으로 보고되었다.
- 미국 북동부 정전 사고: 2003년 8월, 한 전력회사의 SCADA 시스템의 경보 처리기 실패로 제어실 오퍼레이터가 전력망에 대한 주요 운용 변화의 적절한 상황 인식을 못하게 된다. 추가적으로 토폴로지 변경에 대한 불완전 정보로 상태 평가시스템이 고장 나고, 효과적인 신뢰성 분석이 되지 않아, 비상사태 분석을 하지 못하게 된다. 결과적으로 초고압 송전선의 연속적인 과부하를 발생시키고 전력망의 통제되지 않는 연쇄적인 실패를 초래하게 된다. 265개의 발전소에 있는 508개의 발전기가 트립(trip)되고 약 6,200만 KW의 부하가 손실되었다.
- Zotob 웜: 2005년 8월 일련의 인터넷 웜이 크라이슬러 자동차 공장 13곳을 감염시켜, 윈도우 시스템 컴퓨터를 빈번하게 정지시키고 리부팅시키는 사고가 발생하였다. 그 이외에도 중장비 제조사인 Caterpillar사, 항공기 제조사인 Boeing, 여러 곳의 대규모 뉴스 조직의 컴퓨터 정지를 야기 시켰다.

· Taum Sauk 저수댐 실패: 2005년 12월, Taum Sauk 저수댐이 10억 갤런의 물을 방류하는 대재앙적 실패를 당하였다. 댐의 게이지와 네트워크를 통하여 원격으로 감시하고 운용하는 발전소에 있는 게이지 수치차이 때문에 사고가 발생하였다.

비고의적 내부 보안 결과로는 다음과 같은 사건이 있다:

· 취약점 스캐너 사고: 재고 조사 목적으로 SCADA 네트워크에 연결된 모든 호스트를 식별하기 위하여 Ping Sweep가 수행되었다. 이것이 공장 안에 있는 고가의 웨어퍼의 파괴를 가져왔다.

· 침투 시험 사고: 천연 가스 용역회사가 자사 IT 망에 대한 침투 시험을 수행하기 위하여 보안 시험을 행하는 과정에서, SCADA 시스템에 직접 연결된 일부 네트워크에 부주의하게 들어가게 되었다. 이 침투 시험이 SCADA 시스템을 정지시키고 4 시간 동안 가스 공급이 중단되었다.

5.3 가상사고 시나리오

본 절에서는 ICS에 대하여 발생 가능한 가상적 사고 시나리오를 소개한다. 이를 통하여 ICS 보안 대책 수립에 참고가 될 것으로 생각한다. 아래와 같은 많은 사고 시나리오가 가능하다:

· 사내망이나 제어 네트워크를 통한 정보 흐름 지연이나 차단에 의한 제어 시스템 운영 방해가 제어시스템 운용자에게 네트워크의 가용성을 거부하거나, 정보 전달 병목현상 초래, DNS와 같은 IT 서비스에 대한 서비스 거부를 발생시킬 수 있다.

· PLC, RTU, DCS, 혹은 SCADA 컨트롤러 내의 프로그램 된 명령어에 대한 불법 변경, 경보 경계치 변경, 혹은 제어 장비에 발행된 불법명령 등이 장비 손실, 프로세스 조기 정지를 가져와서, 환경적 사고 혹은 제어 장비를 불능화 시킬 수도 있다.

· 불법 변경을 위장하거나 부적절한 조치를 개시하도록 제어 시스템 운영자에게 거짓 정보 전송

· 제어 시스템 소프트웨어나 배열 세팅을 변경하여 예측할 수 없는 결과를 가져올 수 있다.

· 안전 시스템 운영이 방해받는다.

· 바이러스, 웜, 트로이 목마 같은 악성 소프트웨어가 시스템에 유입된다.

· 생산품, 장비 혹은 인명에 대한 손실을 가져오기 위하여 제품 제조 방법이나 작업 지침서에 대한 수정이 가능하다.

게다가 넓은 지역을 포함하는 제어시스템에서, 원격 시스템의 침해로 인한 제어네트워크에 대한 위협이 존재한다. 다음은 두 가지의 가상적인 ICS 사고 시나리오이다.

· 모뎀 검색을 위한 연속적인 전화 번호 다이얼 프로그램을 이용하여 송전 제어 시스템의 프로그래머블 차단기에 연결된 모뎀을 찾아, 차단기 접근을 제어하는 패스워드를 찾아내고 지역 정전이나 장비 손상을 일으키는 제어 세팅을 변경할 수 있다. 어떤 회선차단기의 전류 설정을 낮추어서 서비스 안 되게 하거나 이웃 회선으로 전력을 우회시킬 수 있다. 반대로 설정값을 상향하여 회선차단기가 트립되는 것을 막아 회선의 과부하를 초래할 수 있다. 이렇게 함으로써 변압기와 다른 주요 장비에 심각한 손상을 주고, 장기간의 수리를 위한 정전을 발생시킬 수 있다.

· 사내망과 연결된 제어네트워크에 사고로 바이러스가 유입될 수 있다. 이를 통하여 운영자 컴퓨터가 고장 나고 시스템이 정지될 수 있다.

VI. 맺음말

산업제어시스템(ICS)은 전기, 수도, 수송, 화학, 제지, 자동차, 석유 및 가스와 같은 광범위한 산업에 사용되고 있으며, 국가적인 주요 기반시설에 해당된다. 여러 가지 환경적인 변화로, 특별한 하드웨어와 소프트웨어를 사용하여 폐쇄적인 제어 프로토콜을 수행하는 고립 시스템에서, MS 윈도우, Unix, TCP/IP와 같은 표준 기술 및 프로토콜로 전환되고 있고 IT 망과의 통합이 이루어지고 있어, 정보통신 인프라에 존재하는 사이버 보안 취약성 및 사고의 가능성이 산업제어시스템에도 그대로 재현될 가능성이 증대되고 있다. 그러나 ICS의 보안 특성은 기존 IT 시스템 보안과는 큰 차이가 존재한다. 그러므로 ICS 환경에 적합한 새로운 정보보호 솔루션이 필요하다고 할 수 있다.

본 논문에서는 이를 위해 ICS 관련 시스템에 대하여 살펴보고, ICS의 특성 분석 및 취약성 분석 내용을 제시하였다. 또한 ICS에서 사고의 발생 근원지, 현재 까지 발생한 사고 일지 및 향후 발생 가능한 가상적 사고

시나리오를 제시하였다.

향후 연구로써 보다 자세한 산업제어시스템 취약점 분석과 정보 보호 기술에 대하여 연구가 수행되어야 할 것이다. 앞으로 국가적으로 개발이 추진될 지능형 전력망(Smart Grid)과 산업제어시스템과의 연관성 측면에서의 정보보호 기술 개발도 향후 연구과제의 하나로 생각된다.

참고문헌

[1] Arvid Kjell, Guide to Increased Security in Process Control Systems for Critical Societal Functions, The Swedish forum for information sharing concerning information security-SCADA and Process control systems(FIDI-SC), Swedish Emergency Management Agency, Oct. 2008.

[2] NIST(National Institute of Standards and Technology), U.S. Department of Commerce, Special Pub. 800-82, Final Public Draft, Guide to Industrial Control Systems (ICS) Security, Sep. 2008.

[3] Wikipedia encyclopedia, Industrial Control Systems, May, 2009.

[4] Wikipedia encyclopedia, Distributed Control System, July, 2009.

[5] Wikipedia encyclopedia, SCADA, July, 2009.

[6] 이철수, "산업제어시스템 정보보안 감리 프레임워크 연구", 정보보호학회논문지, 제 18권 제 1호, pp. 139-148, 한국정보보호학회, 2008년 2월.

〈著者紹介〉

전 용 희 (Yong-Hee Jeon)

종신회원

1971년 3월~1978년 2월: 고려대학교 전기전자전파공학부, 학사

1985년 8월~1987년 8월: 미국 플로리다 공대 대학원 컴퓨터공학과

1987년 8월~1992년 12월: 미국 노스캐롤라이나주립 대학원 Elec. and Comp. Eng. 석사, 박사

1978년 1월~1978년 11월: 삼성중공업(주)

1978년 11월~1985년 7월: 한국전력기술(주)

1979년 6월~1980년 6월: 벨기에 벨가톰사 연수

1989년 1월~1989년 6월: 미국 노스캐롤라이나주립대 Dept of Elec. and Comp. Eng. TA

1989년 7월~1992년 9월: 미국 노스캐롤라이나주립대 부설 CCSP (Center For Comm. & Signal Processing) RA

1992년 10월~1994년 2월: 한국전자통신연구원 광대역통신망연구부 선임연구원

1994년 3월~현재: 대구가톨릭대학교 컴퓨터 · 정보통신공학부 교수

2001년 3월~2003년 2월: 대구가톨릭대학교 공과대학장

2004년 2월~2005년 2월: 한국전자통신연구원 정보보호연구단 초빙연구원

2007년 1월~2007년 12월: 한국정보보호학회 학회지 편집위원장

2008년 1월~현재: 한국정보보호학회 부회장

2009년 1월~현재: 한국정보과학회 정보보호연구회 위원장

<관심분야> 네트워크 보안, DDoS 탐지 및 대응 기술, 산업제어 시스템 정보보안, 통신망 성능분석