# 안전한 공장 원격제어 시스템 프레임 워크

이재민, 문지만, 정수환
숭실대학교
e-mail : dlwoas@ssu.ac.kr
jmmun@ssu.ac.kr
souwanj@ssu.ac.kr

# A Framework on secure remote control in plant system

Jaemin Lee, Jiman Mun, Souhwan Jung
School of Electronic Engineering, Soongsil University

**요 약**

본 논문에서는 안전한 공장 원격제어를 위한 시스템 프레임 워크를 제안한다. 공장기계와 IT 의 융합으로 기술 발전함에 따라 공장 제어 시스템을 공장내부에서는 무선 제어시스템, 공장 외부에서는 원격 시스템의 필요성이 대두되어 많은 연구들이 진행되고 있다. 기존의 공장 자동화 시스템 SCADA(Supervisory Control And Data Acquisition) 는 생산 공정 및 플랜트의 상태를 감시하고 제어하기 위한 목적으로 개발되었지만 원격제어 관련 내용이 부족하다. 공장 내부 보안을 위한 표준으로 ISA99 Security Standards 에서도 통합 공정 제어 Zone & Conduits 방식제시 공장의 각 영역을 Zone 으로 나누고 허가된 사용자만 Conduit 를 통해 다른 Zone 의 노드와 통신을 하는 방식을 제안하였다. 하지만, 전체적인 프레임워크는 정의를 하고 있으나 외부 원격 제어 내용 부족하다. 따라서 본 논문에서는 스마트폰을 활용한 공장 외부에서의 안전한 원격 제어를 제공하는 통합관제시스템 프레임워크 구조를 제시하여 향후 관련 기술에 대한 기준점을 제시한다.

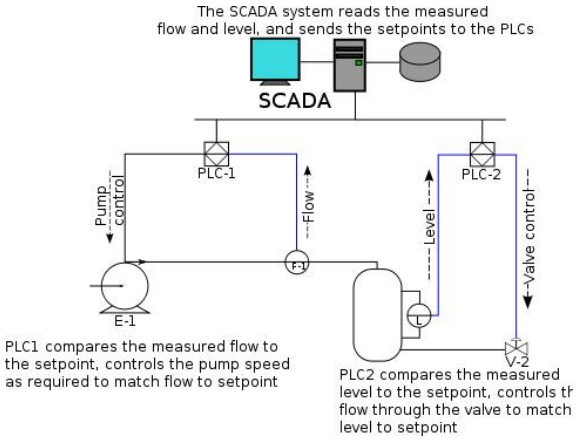
## 1. 서론

최근 컴퓨터와 IT 기술이 발전함에 따라 최근 수년간 자동화 기술은 급속하게 발전하여 왔다. 첨단의 자동화 시스템은 컴퓨터를 이용하여 단위공정의 자동화를 이루고, 이를 통하여 전체 공적을 일관되게 관리하는 방식을 채택 하고 있다. 이러한 자동화 시스템을 통하여 생산성 향상과 생산비용 절감 및 공정의 설계, 구축, 유지관리, 시공간의 절약 등의 경제적인 효과를 가져왔다. 공장자동화에서 응용 시스템의 제어방식은 서버에서 직접 장비를 제어하는 중앙제어방식 또는 장비를 일대일로 제어하는 방식을 주로 사용하였다[1]. 이러한 제어방식은 제어시스템을 확장하거나 이전할 때 드는 설치와 새로운 시스템 도입 등으로 인한 설치 및 유지비용이 더 많이 들었다. 또한, 관리 요원이 항상 현장에서 상주하여 시스템을 관리해야 하는 문제점을 가지고 있었다. 생산 현장의 문제 발생시 신속한 대처를 해야 하지만, 기존의 SCADA(Supervisory Control And Data Acquisition)와 ISA99 에서와 같은 구조는 비효율적이다. 이러한 문제점들을 개선하기 위하여 최근 산업현장에서는 스마트폰기기를 이용하여 어느 시간과 장소에 구애 받지 않고 서버와 접속하여 신속하게 대응할 수 있는 시스템을 개발 하려 하고 있다. 이러한 원격제어 기술은 현장 업무의 관리적인 측면에서 효율성이 높지만 보안적인 측면에서는 시스템이 외부에 노출되는 위험이 존재한다.

본 논문에서는 이러한 문제를 해결하고, 안전한 원격 접속을 통하여 공장 내 실시간 모니터링 및 제어 시스템프레임 워크를 제안하고자 한다. 2 장에서는 관련연구를 소개하고, 3 장은 제안프레임워크에 대해서 설명한다. 4 장에서는 결론을 기술하였다.

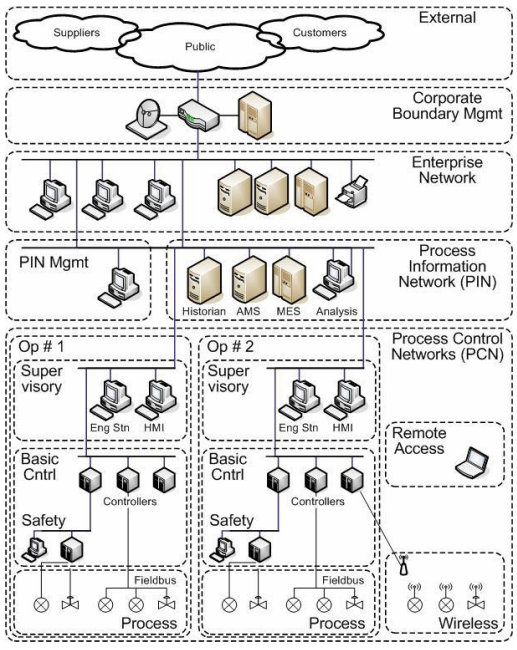
## 2. 관련연구

많이 알려진 산업 자동화 시스템인 SCADA (Supervisory Control And Data Acquisition)은 주요기반시설물뿐만 아니라 산업전반의 감시 제어에 널리 이용되는 시스템이다. 그림 1 과 같이 통합 관제 시스템으로 SCADA 와 HMI(human Machine Interface)가 존재하고 PLC(Programmable Logic Controller)제어를 통해 공정 제어와 모니터링을 받는 구조 이다.




(그림 1) SCADA 시스템

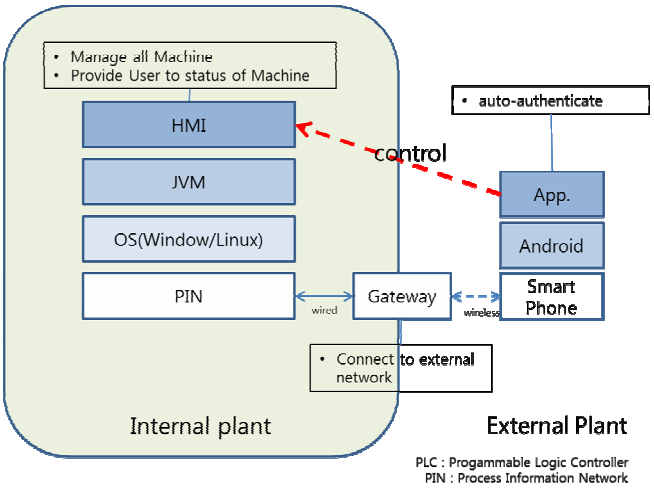
SCADA 같은 시스템은 특히 통신을 통해서 모니터링 및 제어가 이루어지는데, 원활하고 안전한 운용을 위해서 통신 데이터의 신뢰성을 유지하는 것이 중요하다. 최근 들어 SCADA 시스템의 해킹 및 의도적인 공격, 웜바이러스의 침투 등으로 인해 국가 주요 기반 시설에 문제가 발생하여 사회적인 문제로 대두되었다[9]. 이러한 산업시스템 문제를 방지 하기 위한 산업 전반적인 보안에 대한 내용은 ISA99 Security Standards 에 정의되어 있다[10]. ISA99 에서는 통합 공정 제어를 Zone & Conduits 방식으로 제시하고 있다. 공장의 각 영역을 Zone 으로 나누고 허가된 사용자만 Conduit 를 통해 다른 Zone 의 노드와 통신을 하도록 한다. 개별 Zone 은 다른 Zone 과의 Conduit 를 공동 소유하여야 둘간의 통신을 가능하게 하며, 각각의 Zone 들은 필요에 따라 각기 다른 보안 기법의 사용이 가능하다. 개별 Zone 끼리 통신 시 보안 기법의 조정 지원을 한다. 아래그림 2 은 ISA99 에서 제안하는 Zone & Conduits 방식의 산업보안시스템이다.




(그림 2) ISA99 Security Standards

## 3. 제안프레임 워크

본 논문에서는 스마트폰을 이용한 공장 내부 모니터링 및 제어 기술 설계한다. 공장 내부의 원격 제어를 위한 프로토콜 및 프레임워크 도출하고 스마트폰 기반의 안전한 공장 내부 접근을 통하여 실시간 모니터링 및 제어를 제공하는 보안 기술을 그림 3 와같이 설계하였다.




(그림 3) 원격제어 시스템 프레임워크

공장 내부의 시스템은 기존 산업환경과 같이 PLC 와 PIN 네트워크가 존재하고 외부와의 통신은 방화벽 통하여 안전하게 이루어진다. 공장 내부 센서와 기기들은 PLC 와 연결되어 있고 PLC 제어는 PIN 네트워크내에 존재하는 HMI(Human Machine Interface)를 통하여 이루어진다. 그리고 공장외부에서 스마트폰을 이용하여 원격으로 접속하는 관리자는 HMI 를 실시간으로 모니터링, 제어할 수 있는 권한을 얻게 된다.

### 가. VPN 을 이용한 HMI 원격 접속

공장외부에서 원격으로 공장내부에 접속이 가능하게 되면 시스템은 많은 보안위협에 노출되게 된다. 따라서 둘간에 접속에는 강력한 보안이 적용되어야 한다. 공장과 같은 산업시스템과 스마트폰 같은 단말간의 통신의 기밀성 및 무결성을 보장하기 위해서는 VPN 과 같은 안전한 터널링 기술이 필요하다. VPN 을 통하여 안전하게 인증이 이루어진 사용자는 안전한 터널링 기술을 통하여 서버가 속한 네트워크에 접속하게 되고, 둘간의 통신은 안전하게 보호가 되어 불가능 해야 무결성 및 기밀성이 보장 된다. 현재 안드로이드와 윈도우, 리눅스 같은 OS 에서는 PPTP 를 통한 VPN 과 L2TP/IPsec VPN, OpenVPN 등이 지원 가능하다. 표 1 에서 VPN 기술을 비교해 보았다.

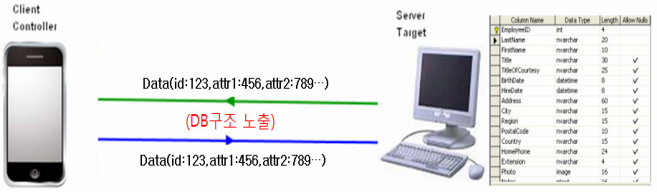
<표 1> VPN 기술 비교

| | PPTP | L2TP/IPsec | OpenVPN |
|---|---|---|---|
| 지원되는 시스템 | Windows<br>Mac OS X<br>Linux<br>iOS<br>Android<br>DD-WRT | Windows<br>Mac OS X<br>Linux<br>iOS<br>Android | Windows<br>Mac OS X<br>Linux<br>Android |
| 암호화 | 128-비트 | 256-비트 가장 안전하지만 더 많은 CPU 요구 | 160-bit 및 256-bit 지원 |
| 보안 | 기본 암호화 | 최고 수준의 암호화 데이터 완결성 확인<br>데이터를 두 번 인캡슐레이션 | 최고 수준의 암호화, 알려진 취약성은 없음<br>Static key 기반인증과<br>SSL/TLS + Certificates 인증방식 가능 |
| 안정성 | 신뢰할 수 없는 유/무선 네트워크에서 조차 가장 안정성/신뢰성이 높음 | 신뢰할 수 없는 유/무선 네트워크에서 조차 가장 안정성/신뢰성이 높음 | 신뢰할 수 없는 유/무선 네트워크에서 조차 가장 안정성/신뢰성이 높음 |
| 속도 | 적은 암호화 오버헤드로 빠름 | 가장 많은 CPU 프로세싱 필요(느림) | 최상의 성능. 지연 시간이 긴 장거리 연결에서도 빠른 속도. |
| 결론 | OpenVPN 이 지원이 불가능하고 이용의 용이함과 속도가 안전보다 우선시 할 때 선택. | PPTP 보다 더 안전하지만, 더 빠른 것은 아니며, 추가 설정이 필요. 장치에서 OpenVPN 을 사용할 수 없으며 사용의 편이 성이나 속도보다 보안이 중요한 경우 선택. | 빠르고 안전하고 신뢰할 수 있는 프로토콜 |

PPTP 기술은 가볍게 128bit 의 키 사이즈를 이용하여 보편적으로 ID/Password 기반의 인증을 통하여 VPN 서비스를 제공하여 속도가 빠르고 가장 많은 환경에서 호환이 가능하다. L2TP/IPsec VPN 기술은 256bit 기반의 키 사이즈 기반의 암호화를 하고, 가장 강력한 보안을 제공하지만 많은 CPU 점유를 사용하기 때문에 오버헤드가 발생하며, 스마트폰 같은 환경에서는 적합하지 않을 수 있다. OpenVPN 기술의 경우 160/256bit 기반의 암호화를 원하여, 강력하면서도 빠른 보안을 제공한다. 그리고 다양한 OS 에서도 호환이 가능하고 open Source 기반의 기술이기 때문에 라이선스에 대한 부담이 없다. 상황에 맞게 VPN 기술을 사용할 수 있겠지만 안전도와 비용적인 측면에서 볼 때 OpenVPN 이 적합하다 할 수 있겠다.

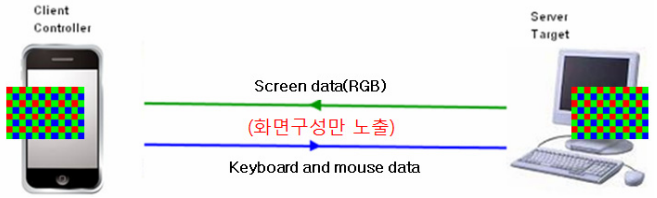
### 나. 스마트폰을 이용한 HMI 원격 제어

VPN 을 통하여 HMI 와 스마트폰간의 안전한 통신을 제공하지만 VPN 보안이 뚫릴 경우, HMI 의 시스템 구조가 외부에 노출이 되는 문제가 발생한다. 그리고 사용자 제어 어플리케이션의 리버스 엔지니어링을 통하여 HMI 구조가 외부에 노출될 위험이 존재하게 된다[7][8]. 그림 6 에서와 같이 일반제어프로토콜기반으로 원격제어가 이루어지는 경우, 프로토콜 내에 제어를 위한 메시지를 분석하거나 제어 어플리케이션동작을 분석함으로써 서버의 구조가 노출될 위험이 존재한다.




(그림 4) 일반프로토콜 기반 원격제어

따라서 제안 기법에서는 이러한 위험노출을 없애기 위해, 원격으로 접속한 스마트폰에게 서버의 화면전송 및 제어를 통하여 HMI 서버의 실시간 모니터링 및 제어가 이루어 진다. 그림 7 은 화면전송을 통한 원격제어 구조를 나타낸 것이다.




(그림 5) 화면제어 기반 원격제어

서버는 원격제어 단말에게 화면데이터만 전송하고 제어를 위한 메시지는 오직 마우스포인터 정보만 주고 받게 된다. 실시간으로 서버는 스마트폰에게 화면 스트림 정보만을 제공하게 되므로 공격자에게 제어 정보가 노출된다 하더라고 화면구조만 노출되게 된다. 이 방법을 통하여 시스템 구조에 대한 노출위협을 없앨 수 있다.

## 4. 결론

국가 주요 기반 시설물뿐 아니라 산업전반의 감시제어에 널리 이용되는 산업시스템의 통신 데이터보호는 안전한 공장 자동화 시스템의 운용 측면에서 중요한 문제이다. 원격 제어를 통한 이득과 보안 위협 노출에 손실적인 문제가 존재하게 된다.

본 논문에서는 공장 자동화 시스템의 안전한 원격제어 및 통신 데이터 보호 기술에 대해 제안하였다. 외부에 공격자가 관리자시스템을 분석 하더라도 시스템 구조 노출 위협을 최소화 하도록 하였다.

국내에서도 현재 이 분야의 연구가 초기단계의 연구가 진행되고 있는데, 특히 이 분야는 전력, 통신, 시스템 등 다양한 요소기술이 필요한 융합적인 기술분야로 추후 많은 공동 연구가 수행될 것으로 판단된다.

## 참고문헌


[1] Marco C, Domenico P, and Antonio V, "The Automatic Control Telelab: a Remote Control Engeering Laboratory," IEEE Conference on Decision and Control Orlando, Florida USA, pp.3242-3247, 2001.12.

[2] 이정식, "웹기반 공장자동화시스템(동부제강)," 첨단 FA 연구소 보고서, 2002.

[3] 김삼룡, "JMF 기반의 실시간 원격 공정 감시 및 제어시스템 설계 및 구현," 정보처리학회논문지 D, 제 11-D 권, 제 2 호, pp.453-460, 2004.4.

[4] 이태희,and 김주만, "원격제어감시제어를 위한 웹 서비스 S/W 플랫폼 설계 및 구현," 한국콘텐츠학회,Vol.7, No.12, pp.245-253, 2007.12.

[5] 목임수, "공정제어 HMI 용 통신 드라이브 및 Script language 개발, " RIST 광양분소 프로젝트, Vol.15, No.4, 2001.

[6] Alfred C, "Monitoring and control using the Internet and Java," IEEE Industrial Electronics Society, Vol.3, pp1152-1158, 1999.

[7] Chikofsky E, and Cross, J, "Reverse engineering and design recovery: a taxonomy," IEEE software, Vol.7, No.1, pp13-17, 1990.

[8] Jaen L, "Introduction to database reverse engineering," LIBD Lecture notes, 2002.

[9] Vinay M, Sean A, and Ronald D, "Security issues in SCADA networks," ELSEVIER computers&security, Vol.25, pp.498-506, 2006.2.

[10] ANSI/ISA-99, "Security or Industrial Automation and Control Systems, "American national standard, 2007.

[11] Zohaib H, "Ubiquitous Computing and Android," Digital Information Management Third International Conference on, pp.166-171, 2008.9.

[12] Choong-Bum P, Byung-Sung P, Huy-Jung U, Hoon C, and Hyoung-Shik K, "IEEE 802.15.4 based Service Configuration Mechanism for Smartphone," IEEE Transactions on Consumer Electronics, Vol.56, No.3, 2010.8.

[13] Siquan H, Yanchao Y, and Lun X, "Comparing Power Management Strategies of Android and TinyOS," Communications and System (PACCS), 2011 Third Pacific-Asia Conference on, pp1-4, 2011.7.