# 배전자동화 현장 단말장치의 인공지능 기반 안전한 펌웨어 업그레이드 방안 연구

홍예진, 김태훈, 김민용, 현무용, 이준영*

*한전KDN㈜

hongyj_28@kdn.com, thkim_5117@kdn.com, kmyong_0902@kdn.com, my_hyun05@kdn.com, ljy.953386@kdn.com

# A Study on the secure firmware upgrade method based on artificial intelligence for field terminal devices in distribution automation system

Hong YeJin, Taehun Kim, Minyong Kim, Muyong Hyun, Junyoung Lee*

*KEPCO KDN

요 약

배전자동화시스템은 다양한 배전 서비스와 편리한 원격 펌웨어 업그레이드를 지원하기 위해 TCP/IP 기반 통신기술 도입을 검토 중이다. 하지만 TCP/IP 기반 통신 기술 도입에 따른 원격 펌웨어 업그레이드 시 배전자동화시스템 서버에서 단말로 파일을 전송하는 과정이나 서버에서 파일을 등록하는 과정에서 단말장치 오작동을 유발할 수 있는 파일 위변조와 같은 보안 위협이 발생할 수 있다. 배전 시스템에서 악의적인 목적으로 변조된 펌웨어가 적용된 단말장치로 인한 오작동은 광역 정전과 같이 기반시설 문제를 발생시킬 수 있기에 본 논문은 이러한 보안 위협을 사전에 방지하기 위하여 인공지능 기술을 활용하여 배전자동화 현장 단말장치의 안전한 원격 펌웨어 업그레이드 방안을 제안한다.

## Ⅰ. 서론

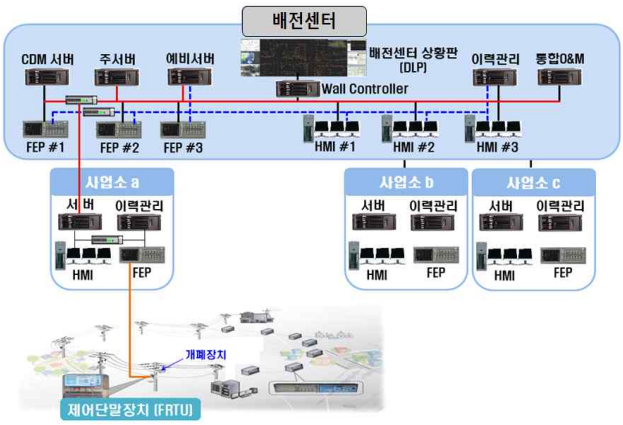
최근 국제적으로 핵심 기반 인프라에 대한 침투 위협이 커지고 있다. 이에 따라 정부도 미래 전략기술 분야 국정과제로 대통령 직속 '국가 사이버안보위원회' 설치를 공헌하며 사이버 보안의 필요성을 강조하고 있다. 특히 국가 핵심 기반시설은 디지털 전환이 빠르게 이루어지고 있기에 발생할 수 있는 위험을 놓치지 않고 파악하는 것이 중요하다. 배전자동화시스템(DAS, Distribution Automation System)은 배전선로 자동화용 단말장치에서 정보를 취득하여 정전 및 고장 조치 시간을 단축하는 시스템이다[1]. 해당 시스템에 IP 기반 통신기술을 도입할 경우 작업자가 직접 현장에 갈 필요가 없어지기에 지속적인 펌웨어 업그레이드에 대한 시간과 인력에 대한 낭비를 줄일 수 있게 된다. 하지만 원격으로 펌웨어 파일을 전송하는 과정에서 파일 위변조를 노린 공격이 발생할 수 있으며 기반시설에서 이러한 위협은 국가적 손실을 발생시킬 수 있기에 해당 과정을 보완하기 위한 보안기술이 요구된다.

따라서 본 논문에서는 IP 기반 통신기술 도입 시 펌웨어 업그레이드 과정에서 발생할 수 있는 펌웨어 파일 위변조 위협을 방지하기 위한 보안기술을 제안한다.

## Ⅱ. 본론

### 2.1. 배전자동화시스템 구성

배전 센터는 주장치 서버와 HMI(Human-Machine Interface), FEP(Front-End Processor)으로 구성되어 있다. HMI는 주장치 서버에서 원격제어 운전용으로 발생하는 데이터나 알람을 인지할 수 있도록 작동하며, FEP은 주장치 명령을 FRTU로 송신하는 장치이다[2]. 센터에서 사업소의 서버로 다시 데이터와 신호를 전달하면 사업소의 FEP이 DAS의 구성요소 중 하나인 제어단말장치 FRTU로 전달하여 동작한다. 배전자동화시스템 구성도는 그림 1과 같다.



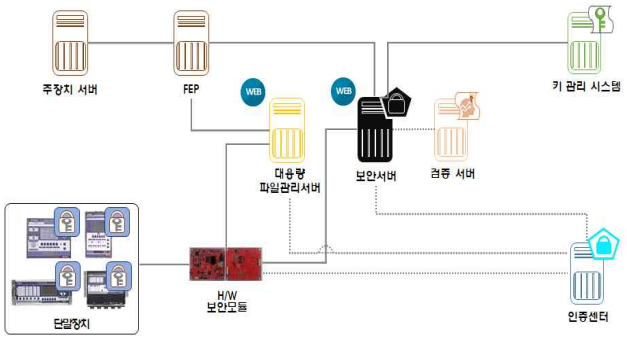

[그림 1] 배전자동화시스템 구성도

현재 배전자동화시스템은 배전자동화시스템 주장치와 현장 단말장치는 Serial 통신으로 FEP과 단말장치에 보안 통신이 적용되지 않은 상태로 연결되어 있다. 이러한 구조에서 TCP/IP 통신을 적용하면 대용량 파일 전송과 같은 다양한 배전 서비스와 원격 펌웨어 파일 업그레이드가 가능하게 된다. 하지만 전송하는 데이터가 보호되지 않기 때문에 단말장치에 펌웨어 파일을 전송하는 과정에서 파일 위변조, 탈취와 같은 공격이 발생할 수 있다.

### 2.2. 인공지능 기반 안전한 원격 펌웨어 업그레이드 방안

주장치 서버와 FEP에서 단말장치로 바로 전달되었던 기존 구성과 달리 FEP와 H/W 보안모듈 간 보안 통신 프로토콜을 지원하는 보안서버, 개인키 및 인증서와 같이 중요정보를 저장하는 키 관리

시스템이 존재한다. 또한 H/W 보안모듈을 이용하여 보안서버와 단말장치 간의 통신에도 보안 프로토콜을 지원할 수 있도록 한다. 그림 1의 배전자동화시스템에서 안전한 펌웨어 업그레이드가 이루어지도록 보완한 환경은 그림 2와 같다.



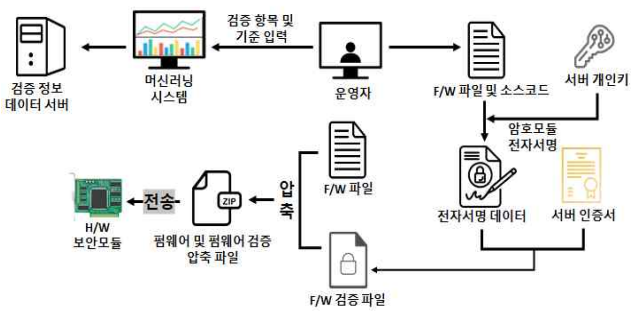

[그림 2] 인공지능 기반 안전한 펌웨어 업그레이드 시스템 구성도

본 논문에서는 이러한 구성도에 따라 대용량 파일 관리 서버에서 H/W 보안모듈로 펌웨어 업그레이드 파일을 보낼 때 검증 파일을 별도로 생성하여 펌웨어 파일을 보호하는 방식과 인공지능을 활용하여 검증시스템을 운영하는 방식으로 이중 검증을 제안한다.

2.3 안전한 원격 펌웨어 생성 및 검증 절차

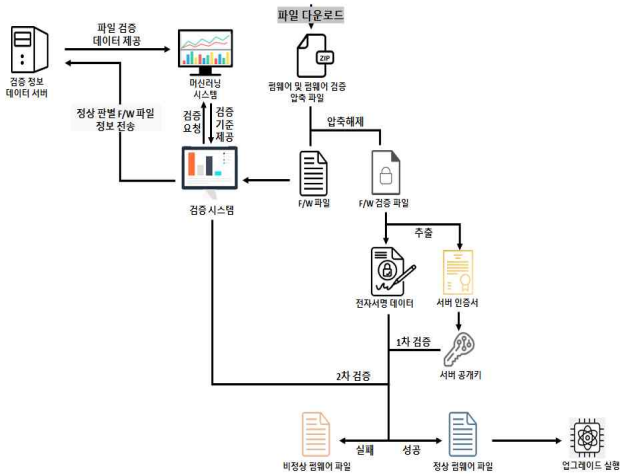
검증 파일을 별도로 생성하는 절차는 펌웨어 업그레이드 파일을 전송하기 전 대용량 파일 관리 서버에서 이루어진다. 전송하는 H/W 보안모듈에게 해당 파일이 변조되지 않았음을 증명하기 위해서 펌웨어 파일에 전자서명을 수행한다. 그 후 전자서명을 수행한 파일과 전자서명이 유효함을 증명하는 인증서, 원본 펌웨어 파일, 전자서명의 해시값을 함께 압축하여 H/W 보안모듈에게 전송한다.

해당 파일을 받은 보안모듈은 압축을 해제하여 다시 검증 파일과 원본 파일을 추출하고 서버의 개인키를 통해 검증 파일에 포함되어 있던 전자서명을 검증한다. 전자서명 검증 결과를 통해 해당 파일이 정상적인 대용량 파일 관리 서버에서 생성해서 만들어졌다는 것을 확인할 수 있으며, 해당 전자서명의 해시값과 함께 전송된 해시값을 비교했을 때 동일한 경우 파일이 훼손되지 않았다는 무결성을 확인할 수 있다. 이처럼 파일을 보낸 서버가 정상적이며 해당 파일이 변조되지 않았음을 확인한 경우, 보안모듈은 파일이 훼손되지 않았음을 1차적으로 판단할 수 있다.




[그림 3] 펌웨어 검증 파일 생성 절차 개념도

검증시스템은 사전에 운영자가 설정한 기준들에 따라 작동한다. 기준들은 모듈의 오동작을 유발시키는 소스코드, 파일 시그니처, 모듈 정보, 파일 버전 정보로 이루어져 있다. 대용량 파일 관리 서버로부터 전송받은 펌웨어 파일이 자동으로 검증 시스템에 입력되면 펌웨어 파일은 디컴파일되어 해당 파일에 기준으로 설정한 소스코드가 포함되어 있는지를 확인한다. 또한 파일 구조 분석을 통해 파일 시그니처가 이전 정상 파일들과 동일한지, 실행될 H/W 보안모듈의 정보가 정상적으로 삽입되어 있는지, 파일 버전은 이전의 파일 버전과 비교했을 때 정상적으로 올라가 있는지를 검증하고 모든 검증에 대한 종합적인 결과를 운영자에게 보여준다. 이때 검증이 끝난 펌웨어 파일은 자동으로 머신러닝 시스템에서 학습 데이터로 재입력되어 후의 검증에 활용할 수 있도록 한다.




[그림 4] 펌웨어 파일 검증 절차 개념도

이처럼 전자서명을 이용한 1차 검증과 인공지능 기술을 활용한 시스템 검증을 통해 모두 정상으로 판별된 경우에만 정상 파일로 간주하여 H/W 보안모듈에서 업그레이드 파일이 실행되도록 한다. 이중 검증을 통해 보안성이 검증된 펌웨어 업그레이드를 진행할 수 있으며, 검증 기준을 시스템 구축 시 정한 것이 아니라 지속해서 축적한 데이터를 통해 최신화된다는 점에서 산업 변화에 따라 나타나는 새로운 위협들에 빠르게 대응할 수 있을 것으로 예상된다.

## Ⅲ. 결론

코로나 팬데믹과 디지털 전환 가속화로 인하여 전력망에도 다양한 기술 활용이 늘면서 사이버공격에 대한 위험성도 커지고 있다. 기술의 활용은 운영효율의 증가와 기술 고도화와 같은 성과를 불러일으킬 수 있겠지만 해당 과정에서 발생할 수 있는 보안 위협에 대한 파악과 그에 대한 대비책 마련이 중요하다. 본 논문에서는 IP 기반 통신기술 도입에 따라 다양한 서비스를 제공할 수 있지만 동시에 보안 위험도 발생할 수 있는 환경을 보완하는 기술을 제안하였다. 이처럼 지속적으로 전력망 보안에 대한 연구와 개발을 통해 배전자동화시스템을 보다 안전하게 운영할 수 있을 것으로 기대한다.

## 참 고 문 헌

[1] 오종욱, “원격감시와 배전자동화를 위한 통합 배전관리시스템”, 석사학위논문, 경북대학교, 2012

[2] 이태윤, “배전자동화시스템 보안성 향상을 위한 PCIe Card 형태의 암호모듈 구현 방안 연구”, 한국통신학회 학술대회 논문집, 1,050-1,051, 2020