# 전력설비들의 사이버 위협 사례 분석과 공격 대응 전략에 대한 연구

박윤근*, 김량수, 유학, 이현우**

KENTECH* (학부생), KENTECH** (교수), ETRI

# Study of Cyber Threat Case Analysis and Attack Response Strategies for Power Facilities

Yoon-Keun Park*, Ryangsoo Kim, Hark Yoo, Hyunwoo Lee**

KENTECH* (Undergraduate student), KENTECH** (Faculty), ETRI

요 약

전력설비는 국가 전력망의 중요한 요소로, 사이버 공격에 의한 피해는 전력 공급 중단과 국가 안보 위협을 초래할 수 있다. 본 논문은 주요 변전소 공격 사례를 분석하고, 이를 분류해 대응 전략을 제시한다. 또한 IEC 61850, DNP3, IEEE 2030.5와 같은 국제 및 국내 표준을 검토하여 보안 강화 방안을 모색한다.

## I. 서론

전력설비는 국가 전력망의 중요한 구성 요소로, 이들 시설에 대한 사이버 공격은 전력 공급 중단, 경제적 손실, 그리고 국가 안보 위협을 초래할 수 있다. 특히 최근 사이버 위협의 증가와 함께 변전소를 표적으로 한 다양한 공격 사례들이 보고되고 있어, 이러한 위협에 대한 체계적인 분석과 대응 전략 마련이 필수적이다.

본 논문에서는 전력설비들을 대상으로 한 주요 사이버 공격 사례들을 고찰한다. 사례 분석은 효과적인 방어 전략을 수립하는 데 중요한 기초가 된다. 공격의 유형에 따라 탐지 및 대응 방식이 달라질 수 있기 때문에, 공격의 성격에 맞춘 분석 작업이 필요하다. 나아가, 각 공격 유형이 시스템에 미치는 영향을 명확히 파악함으로써 공격의 특성을 이해하고, 그에 맞는 적절한 대응 방안을 마련할 수 있다.

보안 위협에 대한 효과적인 대응은 표준 문서를 통해 이루어질 수 있다. 전력설비의 안전을 확보하기 위해 여러 국제 표준들이 제정되어 활용되고 있다. IEC 61850, DNP3, IEEE 2030.5와 같은 표준들은 변전소와 스마트 그리드 내 다양한 장비 간의 안전한 통신을 보장하기 위한 프로토콜을 제공한다. 이러한 표준들을 바탕으로, 전력설비의 사이버 보안을 체계적으로 구축하고 강화할 수 있는 방법을 모색하는 것이 필수적이다.

본 연구에서 우리는 전력설비에 대한 주요 사이버 공격 사례들을 분석하고, 표준 문서들에 있는 보안 관련 명세를 검토한다. 이를 바탕으로 향후 표준 문서의 발전 방향을 제시하는 것을 목적으로 한다.

## II. 전력설비 사이버 위협 사례

본 장에서 우리는 2000대에 발생한 전력설비에 대한 사이버 위협 사례를 시간 순으로 살펴보고자 한다.

2003년에는 오하이오 David-Besse 원전이 마비되는 사건이 발생했다. 원전 계측제어관련 컴

퓨터 네트워크에 MS SQL 슬래머웜이 침투하여 냉각 시스템 등 발전소 안전지표를 모니터링 하는 SPDS가 5시간동안 정지된 것이다. 이는 유지보수 과정에서 감염된 기기를 사용하는 바람에 폐쇄망 안으로 바이러스가 침투하여 발생하였고, 소프트웨어 보안 패치를 설치하지 않은 것이 원인으로 분석되었다 [1].

2010년에는 이란 나탄즈 원전에서 원심분리기 1000대 정도가 마비되는 사건이 발생했다. 해당 사건은 스턱스넷이라는 멀웨어에 의해 발생하였다. 이 멀웨어는 감염된 USB가 원전 내부시스템에 삽입되면서 전파되었고, Siemens의 소프트웨어 및 장비에 대해 5개의 제로데이 취약점을 노리고 공격하였다 [2]. 스턱스넷은 이를 통해 원심분리기에 물리적인 손상을 입혔다.

2013년도에는 전기, 석유 등을 공급하는 1000개 이상의 북미 에너지 회사들을 대상으로 Dragonfly라는 해커 집단이 공격하는 사례가 있었다. 이들은 멀웨어를 이용해 타겟 네트워크에 침투한 후 원격 데스크톱 프로토콜을 사용하여 접속할 수 있도록 백도어를 마련하였다. 이 과정에서 전기 공급이 중단되는 등의 사례는 없었으나, 대량의 정보가 유출되었다 [3].

2015년에는 우크라이나 전력 시설이 공격당해 6시간 동안 8만 여 가구가 정전되는 사건이 발생했다. 이는 해커가 블랙에너지3라는 악성코드가 숨겨진 워드 문서를 활용한 스피어피싱 공격을 통해 망에 침투하여 발생한 것으로 밝혀졌다. 이 악성코드는 외부 C&C 서버에 접속하여 MBR 파괴 등의 추가 악성행위를 수행하였으며, 백도어도 설치하여 해커들이 원격 접속을 할 수 있도록 하였다. 해커들은 회사 내부망을 정찰하여 변전소망으로 접속할 수 있는 계정도 확보하였고, 이를 활용하여 변전소에 악성 펌웨어를 설치하여 변전소를 통제하였다. 결국 특정 시점에 다량의 변전소를 일괄 중지시켜 정전 피해를 일으켰다 [4].

2016년에도 우크라이나를 대상으로 정전을 목적으로 한 유사한 공격이 있었다. 이번에 사용된 악성코드는 인더스트로이어라는 악성코드를 이용해 변전소에서 사용하는 작업 프로세스를 방해하였고, 이를 통해 22만 여 가구에 대해 1시간 동안의 정전 피해를 입혔다 [5].

2021년에는 산업 전력망을 붕괴 시키는 '코스믹에너지' 악성 코드가 발견되었다. OT망의 ICS를 노리는 이 악성코드는 유럽, 중동, 아시아의 전기 송전 및 배전 운영에 일반적으로 활용되는 원격 단말 장치(RTU)와 같은 IEC 60870-5-104(IEC-104) 장치와 상호 작용하여 전력 중단을 일으키도록 설계되었으며, 그 양상이 우크라이나 정전 사태를 일으킨 악성코드와 유사하다고 알려져있다 [6].

이상의 전력설비를 대상으로 한 사이버 위협 사례들의 침투 경로를 살펴보면, 해커들은 망에 대한 취약한 지점을 발견하여 감염 USB를 전달하거나 백도어를 마련하고 전력설비에 접근할 수 있는 권한을 획득한 뒤 전력설비에 대한 공격을 수행한 과정을 거친다는 것을 알 수 있다. 그렇기 때문에, 전력망에서의 취약한 지점을 식별하고 보안을 강화하는 것이 중요할 것이다. 또한, 2010년대의 공격은 원격을 통한 공격 형태를 띤다는 것을 알 수 있는데, 이는 통신부에 대한 감시 제어가 중요하다는 것을 보인다.

## III. 전력설비 사이버 보안 표준

본 장에서는 전력설비를 보호하기 위한 다양한 사이버보안 표준을 살핀다.

IEC 61850은 변전소 내 기기 간의 통신을 위한 국제 표준으로, 변전소 자동화 시스템의 운영을 위해 주로 사용된다. 이 표준은 이더넷 기반으로 데이터를 교환하며, Generic Object Oriented Substation Event (GOOSE) 및 Manufacturing Message Specification (MMS)와 같은 다양한 프로토콜을 지원한다. 보안 측면에서 IEC 61850은 데이터의 암호화와 무결성을 보장하기 위해 Transport Layer Security (TLS) 등 널리 알려져 보안 프로토콜에 의존하며 이 과정에서 Public Key Infrastructure (PKI) 기반의 인증서를 사용하여 인증을 수행한다. 이를 바탕으로 역할 기반의 접근 제어를 수행한다 [7].

DNP3은 변전소의 원격 제어 및 데이터를 수집하기 위해 사용되는 프로토콜로, 주로 SCADA 시스템에서 활용된다. IEC 60870-5 표준의 일부인 DNP3은 Remote Terminal Unit (RTU) 및

Intelligent Electronic Device (IED) 간의 통신을 담당하며, 안정적인 데이터 전송을 위한 에러 검사 및 데이터 단편화 등의 기능을 지원한다 [8]. 보안 요구 사항에 있어 DNP3은 자체적으로는 보안을 고려하지 않으며, IEC 61850과 마찬가지로 TLS 같은 외부 보안 프로토콜과 결합하여 사용된다. 특히 IEC 62351-3에서 정의된 TLS 암호화를 통해 데이터의 무결성과 기밀성을 보장하며, 역할 기반 접근 제어(RBAC)를 통해 접근 권한을 제어한다.

IEEE 2030.5는 스마트 그리드에서 분산 에너지 자원을 통합하기 위한 프로토콜로, 보안을 위해 TLS 1.2를 필수로 사용하며, 기기 인증서를 통해 통신의 보안을 강화한다 [9]. TLS는 X.509 인증서를 기반으로 종단 간 암호화와 인증을 보장하며, 이는 PKI 체계에 의해 관리된다. 인증된 개체에 대해 정보 자산 단위로 접근 제어가 이루어진다.

이상의 보안 표준을 살펴보면 공통적으로 TLS를 활용한 암호화와 PKI를 활용한 인증, 그리고 역할 기반의 접근제어에 초점을 맞추고 있다는 것을 알 수 있다.

## IV. 제언 및 결론

앞서 살펴본 사이버 위협 사례를 기반으로 표준 문서의 보안 장치들을 살펴보면, 제3자 통신과 정보 자산 접근 제한을 위해 설계되어 있으나, 악성 행위자의 직접 원격 통신에 대한 보호는 미흡하다. 최근 원격 접속을 이용한 공격 사례를 고려할 때 다음을 검토할 필요가 있다.

첫째, 외부로 열려 있는 포트의 식별과 통제가 중요하다. 해커는 스피어피싱 등을 통해 원격으로 침투하여 악성코드를 심으므로, 체계적인 포트 관리를 명세서와 기관의 운용 지침서에서 다뤄야 한다. 둘째, 기존의 보안 장치(TLS, PKI, 접근제어)가 정상 통신을 전제한다는 한계를 보완하여, 이상 탐지와 사이버킬체인 전략을 통해 손상된 개체로부터의 공격에도 대비해야 한다. 마지막으로, 침입 탐지 시스템 도입과 다운로드 파일의 보안성 검토 등 구체적 탐지 연구가 활성화되어야 한다.

이 외에도, 구체적 침입 탐지에 대한 연구의 활성화가 필요하다. 예를 들어 통신부에 침입탐지시스템을 도입하거나 다운로드 파일 등에 대한 보안성 검토 및 분석이 강화될 수 있는 연구가 활발히 이루어질 필요가 있다.

본 논문에서는 전력 설비를 대상으로 한 여러 사이버 공격 사례들과 이에 대처하기 위한 국내·외 표준에 대해서 분석, 검토하였다. 전력 설비들에 대한 국제 표준들의 개정에는 3-5년이 걸리는 반면, 사이버공격은 나날이 진화하고 있다 [10]. 앞으로의 연구에서는 이들 표준의 한계와 개선점을 분석하고, 국내외 전력망에 더욱 적합한 보안 프로토콜의 개발과 적용 가능성을 모색해야 할 것이다.

## Acknowledgment

본 연구는 산업통상자원부(MOTIE)와 한국에너지기술평가원(KETEP)의 지원을 받아 수행한 연구 과제입니다. (No. 20225500000090)

## 참고문헌

[1] 김진, 김장성, 강영두, 김광조, 원자력 발전소 디지털 시스템의 보안 요구 사항, Korea Institute of Information Security & Cryptology, March, 2002.

[2] John Richardson, Stuxnet as Cyberwarfare: Applying the Law of War to the Virtual Battlefield, Journal of Computer & Information Law, Fall, 2011.

[3] Khan, F. B., Asad, A., Durad, H., Mohsin, S. M., & Kazmi, S. N., Dragonfly cyber threats: A case study of malware attacks targeting power grids, Journal of Computing & Biomedical Informatics, Mar, 2023.

[4] Liang, G., Weller, S. R., Zhao, J., Luo, F., & Dong, Z. Y., The 2015 Ukraine blackout: Implications for false data injection attacks, IEEE transactions on power systems, Nov, 2016.

[5] Gjesvik, L., & Szulecki, K., Interpreting cyber-energy-security events: experts, social imaginaries, and policy discourses around the 2016 Ukraine blackout, European Security, Jun, 2022.

[6] Skrodelis, H. K., Blumbergs, B., & Romanovs, A., Threat Scenario Generation for IEC104 Cyber Defense, In 2024 IEEE 11th Workshop on Advances in Information, Electronic and Electrical Engineering, Jul, 2024

[7] S. M. S. Hussain, T. S. Ustun and A. Kalam, A Review of IEC 62351 Security Mechanisms for IEC 61850 Message Exchanges, IEEE Transactions on Industrial Informatics, Sept, 2020.

[8] Clarke, G., Reynders, D., & Wright, E, Practical modern SCADA protocols: DNP3, 60870.5 and related systems. Newnes, Apr, 2004.

[9] Ghalib, M., Ahmed, A., Al-Shiab, I., Bouida, Z., & Ibnkahla, M, Implementation of a smart grid communication system compliant with IEEE 2030.5, 2018 IEEE International Conference on Communications Workshops, May, 2018.

[10] 이정훈, 문영석, 전력시스템 사이버보안 강화를 위한 IEA의 제언, Sep, 2021.