배전 계통에 대한 사이버 공격 테스트 베드 구축 연구

박규찬, 원동준*
인하대학교 전기공학과, *인하대학교 전기공학과
kyuchan100@gmail.com, *djwon@inha.ac.kr

Development of the Testbed for Cyber-attack to Distribution System

Kuchan Park, Dongjun Won*
Inha University, *Inha University

요 약

본 논문에서는 배전 계통에 대한 사이버 공격 모의 시뮬레이션을 위해 실시간 기반 테스트 베드 구축에 대한 연구를 진행하였다. IEEE(Institute of Electrical and Electronics Engineers)에서 제공하는 모델인 IEEE 13 node test feeder를 기반으로 배전 계통을 설계하였다. 실시간 환경에서의 시뮬레이션을 위해 OPAL-RT와 MATLAB/Simulink를 연동하였으며, 라즈베리 파이를 이용하여 배전 계통의 EMS(Energy Management System)를 구현하였다. 사이버 공격에 대한 시뮬레이션 효과를 검증하기 위해 MitM(Man-in-the-Middle) attack을 모의하였으며, 해당 공격으로 EMS에서 ESS(Energy Storage System)로 전달되는 무효 전력 지령 값이 변경되는 시나리오를 적용하였다. 해당 시뮬레이션의 결과로 본 논문에서 제안한 테스트 베드의 사이버 공격에 대한 적합성을 검증하였다.

Ⅰ. 서 론

최근 신재생에너지, 에너지 저장장치, 전기자동차, 제어 가능한 부하 등 다양한 분산에너지자원의 투입으로 전력 계통을 대상으로 한 사이버 공격과 관련된 연구의 중요성이 강조되고 있다.[1] 실제로 2015년 12월 우크라이나 전력망을 대상으로 한 BlackEnergy 악성 코드 공격은 대표적으로 알려진 전력시스템에 대한 사이버 공격이다.[2] 따라서 사이버 공격을 예방, 탐지, 대응하기 위한 연구는 필수적이다. 하지만 CPS(Cyber-Physical Security) 테스트 베드의 시설 부족으로 대부분의 최근 연구들은 실제의 실시간 사이버 이벤트가 고려되지 않은 침투 기반 공격 시나리오 검증에 중점을 두고 있다.[3] 하여 본 논문에서는 실제 사이버 공격을 고려할 수 있는 테스트 베드를 구성하고, 이를 활용하여 MitM attack에 대한 실시간 기반의 계통 시뮬레이션을 진행하였다.

Ⅱ. 본론

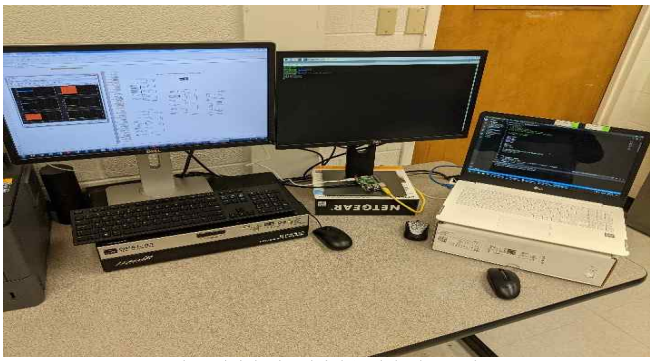

그림 1 실시간 시뮬레이션을 위한 테스트 베드

본 논문에서 사용한 배전 시스템은 1개의 ESS, 1개의 풍력 발전기, 1개의 태양광 발전 시스템을 포함한다. 시스템 주파수는 60Hz이며 공칭 전압은 4.16kV이다. 풍력 발전 및 태양광 발전 시스템의 스마트 인버터는 MPPT(Maximum Power Point Tracking)제어를 수행한다. 634 버스의 풍력 발전기는 PMSG(Permanent Magnet Synchronous Generator) 모델이며 정격 전력은 2.2MVA이다. 태양광 시스템은 675 버스에 위치하며 정격 출력은 1MW이다. 680 버스의 ESS 용량은 1MWh이며, 리튬 이온 배터리 모델을 사용하였다. 발전원들이 연결되어 있는 버스를 제외한 나머지 버스에는 부하들이 연결되어있다. 배전 계통 모델의 선로 데이터는 IEEE 13 Node Test Feeder에서 제공하는 값을 적용하였다.

사이버 공격은 Kali Linux를 기반으로 한 MitM attack을 적용하였다. Kali Linux는 공개적으로 잘 알려진 사이버 공격을 구현하기 위한 수백가지 도구를 제공하는 오픈 소스 플랫폼이다.

Ⅲ. 결론

MitM attack으로 배전 계통의 EMS에서 ESS로 전달되는 무효전력 지령 값이 변경되었다. 사이버 공격이 없을 때, 무효전력 지령 값은 0VAR이다. 사이버 공격으로 변경된 무효전력 지령 값은 80kVAR이다. 계통 연계형 배전 계통이기 때문에 무효전력 지령 값이 변경된 효과는 배전 계통이 Utility와 연결된 PCC(Point of Common Coupling)에서 나타난다. 사이버 공격의 영향으로 송전 계통에서 구입하는 무효전력량이 줄어든 것을 볼 수 있다.

ACKNOWLEDGMENT

본 연구는 과학기술정보통신부 및 정보통신기획평가원의 글로벌핵심인재양성지원사업의 연구결과로 수행되었음 (2020-0-01540)

참 고 문 헌

[1] B. Ahn, T. Kim, J. Choi, K. Park, and D. Won, “A cyber kill chain model for distributed energy resources (DER) aggregation systems,” in Proc. 2021 IEEE EEE Innovative Smart Grid Technologies Conference North America, in press.

[2] SANS Industrial Control Systems and E-ISAC, “Analysis of the cyber attack on the Ukrainian power grid – Defense use case,” Mar. 2016.

[3] S. Sahoo, T, Dragicevic, and F. Blaabjerg, “Multilayer resilience paradigm against cyber attacks in DC microgrid, IEEE Trans. Power Electronics, vol. 36, no. 3, pp. 2522-2532, Mar. 2021.