# 가상발전소(VPP)의 잠재적 보안 위협에 대한 고찰

서유정*, 한슬기**, 이현우***

*KENTECH (대학원생), **KENTECH (학부생), ***KENTECH (교수)

# Exploring Potential Security Threats to Virtual Power Plants

Yujeong Seo*, Seulgi Han**, Hyunwoo Lee***

*KENTECH(Graduate), **KENTECH(Undergraduate), ***KENTECH(Faculty)

요 약

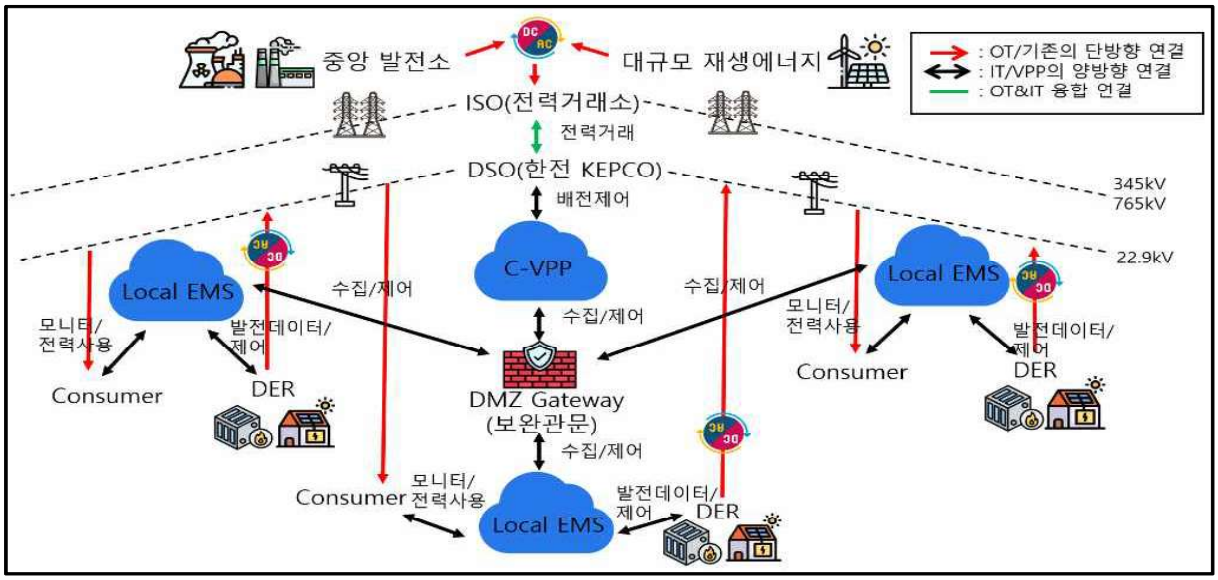
가상발전소(Virtual Power Plant, VPP)는 분산에너지자원(Distributed Energy Resource, DER)을 통합 제어·거래 가능한 하나의 가상 발전 단위로 묶어 계통 유연성과 시장 효율을 높이지만, 이로 인해 기존 배전망보다 훨씬 넓은 공격 표면에 노출된다. 본 논문은 최근 연구에서 언급된 VPP 보안 취약 지점을 정리하고, 기존 논의가 개별 구성요소 단위 분석에 머물렀다는 한계를 지적한다. 또한 우리는 공급망·유지보수 경로를 통한 악성 모듈 주입, 내부 인증 정보 탈취, OT 제어 계층으로의 확장, BPFDoor 계열 은닉형 백도어를 통한 RTU/DER 제어 신호 위·변조와 배전망 교란으로 이어지는 다단계 침투 흐름을 제시한다. 아울러 거래·메시지·호스트 로그를 단일 스키마로 통합해 공격 단계를 재구성하고, 이 체인을 기반으로 후속 조작을 예측·차단하며, 고위험 경로를 자동 완화·격리하는 보안 오케스트레이션 방향을 제안함으로써, VPP 환경에서의 선제적 대응 구조의 필요성을 강조한다.

## I. 서론

가상발전소(Virtual Power Plant, VPP)는 RE100 실현을 위한 태양광·풍력 시스템 같은 분산형 신재생 에너지 자원의 확대, 그리고 송전망의 병목에 따른 지역 단위의 분산 관리 필요성에 따라 주목받고 있다 [1]. VPP는 태양광, 풍력, 에너지저장장치(Energy Storage System, ESS) 등 분산에너지자원(Distributed Energy Resource, DER)을 마치 하나의 발전소 처럼 통합 제어하고 운영하는 디지털 기반 에너지 관리 시스템으로, 실시간 전력 수급의 최적화와 계통 유연성 확보에 기여한다. 더 나아가, VPP는 전력시장에서 하나의 거래 주체로 참여하여 소규모 DER을 모아 집합적으로 거래 단위로 만들 수 있어, 시장 접근성을 높이고 에너지 활용 효율을 극대화한다는 점에서도 중요성이 커지고 있다.

VPP의 운용을 위해서는 다양한 DER들이 기존 배전망에 연결되어야 한다. 그러나 기존 전력망은 상대적으로 폐쇄된 환경을 전제로 설계되어 왔으며, 이에 따른 최소 수준의 보안 체계를 갖추고 있다. 반면, VPP에서는 민간 사업자가 운영하는 외부 DER이 전력망에 접속함으로써 인증 경계가 모호해지고, 통신 경로가 복잡해지며, 공격 표현이 확장하는 문제가 발생한다. 이러한 보안 취약점은 단일 지점의 사고로 끝나지 않고 계통 전체로 확장될 수 있어, 기존 대비 훨씬 높은 보안 요구 수준이 필요하다.

본 논문에서는 2021년 이후에 발표된 VPP 보안 관련 주요 연구를 검토하고, 제기된 위협 요소를 유형별로 정리·비교한다. 또한, 기존 연구가 다루지 못한 보안성 검토의 한계와 추가 고려사항을 제시하고, 대표적인 관련 공격 시나리오를 통해 이러한 위협이 전력망에 미칠 영향을 살펴본다. 마지막으로, 잠재적 위협에 대응하기 위한 보안 강화 방안과 후속 연구를 제시하고자 한다.




[그림 1] VPP 운영 구조도

## II. 가상발전소(VPP)

본 장에서는 VPP의 개념과 구성, 그리고 관련 이해당사자를 다룬다.

### 2.1 가상발전소 구조

VPP는 여러 DER을 클라우드기반 소프트웨어를 이용해 사이버 공간에서 마치 하나의 발전소처럼 통합·관리하여 전력 공급과 수요조정을 수행하고, 시장 거래에 참여할 수 있는시스템이다. VPP는 내부로는 연계된 분산 자원에 대한 관리를 수행하고, 외부로는 시장참여자와 계통 운영자 간의 인터페이스 역할을 수행한다.

그림 1은 VPP의 전체 통신 및 운영구조를 나타낸다. 소비자와 VPP 내부의 DER은 지역의 에너지관리시스템(EMS)에 연결되어, EMS에는 실시간으로 소비자의 전력사용 데이터와 DER 발전데이터가 수집된다. 이 데이터는 보완 관문을 거쳐 중앙 VPP(C-VPP)로 전송된다. VPP 외부에는 배전계통운영자(Distributed System Operator, DSO)와 독립계통운영자(Independent System Operator, ISO)가 연결되어 배전제어와 전력거래를 수행한다.

### 2.2 VPP 이해당사자

VPP에는 양방향 연결 구조를 기반으로 다양한 이해당사자가 존재한다. DSO는 배전망의 전압 안정과 부하 조정을 담당하고, ISO는 실시간 계통운영과 도매전력시장 운용을 총괄한다. DER을 보유한 개인 사업자나 소규모 사업체는 태양광, 풍력, ESS 등을 통해 전력을 생산·소비하며, VPP를 통해 잉여 전력을 판매하거나 전력 소비를 조정함으로써 시장 내 수요반응 자원으로 참여한다. 지자체·정부 기관은 지역 단위의 데이터 수집·통신 인프라·보안 기준을 관리한다. 이와 같이, VPP는 개인, 기업, 공공이 동시에 참여하는 복합적 협력 구조로 운영되며, 각 주체는 OT와 IT를 매개로 긴밀히 연결되어 있다.

## III. VPP에서의 위협 연구 동향

본 장에서는 [2]-[9]에서 확인된 VPP에서의 위협 연구 동향에 대해서 다루고자 한다.

### 3.1 VPP위협 연구 동향

VPP는 분산된 자원과 다수의 통신 경로가 얽혀 있는 구조로 인해 기존 전력망보다 보안 관리가 훨씬 복잡하다. 데이터 교환 과정에서 인증 절차가 누락되거나, 접근 권한이 명확히 정의되지 않아 정보 위조나 불법·접근이 발생할 가능성이 커진다. 따라서 [2]에서는 전력망 운영자와 VPP 간 통신 구간의 암호화와 무결성 검증의 중요성을 강조한다.

| 논문 | 위협 지점 |
|---|---|
| [2] | 통신·접근제어의 분산과 불일치로 인한 데이터 인증·무결성이 손상 |
| [3] | 제어 명령 변조·데이터 탈취로 인한 실시간 제어권 훼손 및 자동화 시스템 교란 |
| [4] | 중앙집중형 클라우드 의존으로 인한 지연·단일장애점 노출로 인한 실시간 제어 불안정성과 데이터 유출·조작 위험이 증가 |
| [5] | 다계층 제어의 동기화 오류·루프 간섭 등 취약점으로 인한 제어교란 및 연쇄 장애 |
| [6] | 입찰·거래 데이터 위조 및 무결성 훼손(시장 교란 공격) 문제가 언급 |
| [7] | 우크라이나 공격 사례 기반으로 SCADA 침투를 통한 제어권 탈취 및 운영 중단 |
| [8] | VPP 에너지 시장에 대한 서비스 거부 공격, 중간자 공격, 거짓 데이터 삽입 공격 |

[표 1] VPP 관련 위협 동향

VPP의 디지털 제어 구조는 SCADA나 인공지능 운영 모듈 등 다수의 시스템이 상호 연동되는 특성 때문에 공격 표면이 넓다. 제어 명령이 변조되거나 운영 데이터가 탈취되면 시장운영과 계통 안정성이 동시에 위협받을 수 있다 [3].

중앙 서버 중심의 제어 모델은 네트워크 지연과 단일 장애점 문제를 안고 있어 VPP의 실시간성과 보안성을 동시에 저하시킬 수 있다 [4].

VPP는 여러 제어 계층이 상호 연결된 복합 시스템이기 때문에 데이터 동기화 오류나 제어 루프의 상호 간섭이 쉽게 발생한다. 이러한 구조적 특성은 사이버 공격에 대한 추가적인 취약점을 만든다 [5].

이에 따라 최근 연구는 제로 트러스트 기반 미세 접근제어와 다단계 인증, 이상 행위 기반 자동 모니터링/보안 오케스트레이션, 그리고 중앙집중형 병목을 줄이기 위한 엣지 컴퓨팅 기반 분산 제어 아키텍처를 제안하고 있다 [3][4][5]

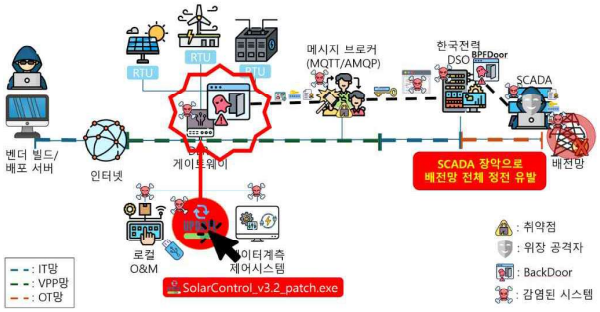
VPP가 데이터 위변조·정보 노출·불투명한 거래 구조에 취약하다. 특히 실시간 운영 데이터 무결성이 훼손될 경우 전력 시장 운영과 시스템 안정성이 직접적으로 저해되기 때문에, 암호기반 접근 제어, 위·변조 방지 저장 구조, 신뢰도 기반 거래 모델, 블록체인 결합을 통한 투명성 확보 등이 제안되고 있다 [6].

VPP가 다수의 DER을 가지고 IT망에 연결되면서 공격 표면이 확장되었다. SCADA, RTU, HMI 등의 취약점은 공격 진입점이 되며, 과거 전력망 공격 사례를 통해 데이터 위변조·서비스 교란·권한 탈취 기반 운영 마비가 현실화 될 수 있다. 이에 제로 트러스트 기반 미세 접근 제어, 지속 인증, 이상 행위 감시, AI 기반 위협 탐지 등이 제안된다 [7].

VPP에 대한 공격 중 거짓 데이터 삽입 공격은 가장 치명적인 위협으로 간주된다. 이는 전력 가격·수요·발전량 데이터를 조작해 시장 안정성과 재무적 피해를 유발할 수 있다. 기존 연구가 DoS/MITM/악성코드 등 다양한 계층 공격을 다루어 왔으나 VPP 특화 보안 분석은 여전히 부족한 실정이다 [8].

이상의 연구들은 VPP에 대한 위협 지점을 첫째, 여러 시스템 사이의 연결에 따른 위협, 둘째, 클라우드 기반 제어는 단일장애점의 문제, 셋째, 제어와 시장 교란에 치명적인 거짓 데이터 삽입을 지적하였다. 앞선 연구들은 VPP의 요소별 취약 지점을 정리하였으나, 여러 기관을 관통하는 다단계 APT 공격에 대해서는 초점을 맞추지 않았다는 한계가 있다.

## III. 잠재 위협 시나리오




[그림 2] 배전망 장악 시나리오

앞선 연구들의 한계를 고려하여 본 장에서는 VPP를 경유하여 배전망을 교란시키는 잠재적인 다단계 위협에 대해서 논의한다.

초기 침투는 공급망·유지보수 경로를 통한 악용해 정상 패치를 위장한 악성 모듈을 운영자 단말에 주입하는 방식으로 시작된다. 설치된 모듈은 내부 인증 정보를 수집 및 탈취하여 데이터계측·제어시스템으로 접근한 뒤 OT 제어층을 목표로 확장된다.

본 시나리오의 핵심은 BPFDoor 계열의 은닉형 백도어 사용이다. 공격자는 이를 특정 매직 시퀀스·조건·시간대에서만 활성화되도록 설정한 뒤 RTU·DER 제어 신호를 위조·주입하여 차단기 동작·연쇄 트립 또는 DER의 출력 조작을 유발한다.

이로 인해 발생하는 피해는 국소적 과부하로 인한 장비 손상과 정전, 전력계통 운영 불안정 등 물리적·운영적 피해로 직결된다. BPFDoor에 의한 은닉성 때문에 초기 발견이 지연되면 복구 시간과 영향 범위가 급격히 확대되며, 특히 OT 장비의 펌웨어·명령 무결성이 손상된 경우 복원·검증에 추가적 비용이 발생한다.

## V. 대응 방향

위 시나리오에 대응하기 위해 세 가지를 고려한다. 첫째, 거래·메시지·호스트 로그를 단일 스키마로 정규화하고 이들 로그를 시간·위상 기준으로 연계하여 사이버 킬체인 유사 방식의 공격 단계 체인을 자동으로 구성한다. 둘째, 구성된 공격 단계 체인을 입력으로 하여 부분적 침해 징후에서 이후의 전파·조작 행위를 체인의 정보를 기반으로 탐지·예측한다. 셋째, 예측된 고위험 경로에 대해 세션 강제종료, 거래 임시보류 등 자동화된 운영 완화 메커니즘과 허니팟·온라인 학습을 통한 지속적 성능 보강한다. 이 세 축을 결합하면 단순 이벤트 경보를 넘어 공격의 흐름을 파악하여 다음 단계를 선제적으로 차단·완화함으로써 VPP·배전망의 신뢰성과 회복력을 향상시킬 수 있다.

## VI. 결론

본 논문에서는 VPP환경에서 발생 가능한 다단계 공격 시나리오를 통해 복합 로그 기반의 공격 체인 분석 필요성을 제시하였다. 향후 이종 로그를 통합하여 공격 단계를 동적으로 재구성하고, 이를 기반으로 다음 공격을 예측· 차단할 수 있는 지능형 보안 오케스트레이션 체계의 설계와 실증적 검증을 수행하고자 한다.

## Acknowledgement

이 연구는 2025년도 산업통상자원부 및 한국산업기술기획평가원(KEIT) 연구비 지원에 의한 연구임 (과제번호: RS-2025-02653102)

## [참고문헌]

[1]분산에너지 특구의 시장 영향과, 분산에너지 산업 활성화를 위한 성공적 정착 방안 제언. 전기저널.

[2] Koza, Erfan et al., (2021). A Literature Review to Analyze the State of the Art of Virtual Power Plants in Context of Information Security.

[3] S. P. Rao et al., "Virtual Power Plants Security Challenges, Solutions, and Emerging Trends: A Review," Cyber Awareness and Research Symposium (CARS), ND, USA, 2024

[4] Venkatachary et al., (2021). Cybersecurity challenges in energy sector (virtual power plants) – can edge computing principles be applied to enhance security?. Energy Informatics.

[5] R. Khan et al., "Energy Sustainability Survey on Technology and Control of Microgrid, Smart Grid and Virtual Power Plant," in IEEE Access, 2021.

[6] Zhang, X., et al., Security scheduling and transaction mechanism of virtual power plants based on dual blockchains. J Cloud Comp 11, 4 (2022).

[7] Annamalai Alagappan et al., Augmenting Zero Trust Network Architecture to enhance security in virtual power plants, Energy Reports, Volume 8, 2022, Pages 1309-1320, ISSN 2352-4847.

[8] Singh, K.N et al., Enhancing cybersecurity in virtual power plants by detecting network based cyber attacks using an unsupervised autoencoder approach. Sci Rep 15, 32374 (2025).