가상발전소 환경의 제로트러스트 보안 아키텍처 도입 제안

박지민, 윤성우*, Ma Xiyuan**, 이석준***

가천대학교

jimin030907@gachon.ac.kr, *borok2311@gachon.ac.kr, **mhe6814@hotmail.com, ***junny@gachon.ac.kr

Proposal for Implementing a Zero Trust Security Architecture in Virtual Power Plant Environments

Jimin Park, Sungwoo Yun, Ma Xiyuan, Sokjoon Lee

Gachon Univ.

요 약

VPP는 DER을 연계·통합해 하나의 발전소처럼 제어·운영하는 시스템이다. 이때 DER은 지리적으로 분산된 구조와 많은 통신량으로 인해 공격 표면이 확대되며 중앙 통합 운영 구조로 인해 일부 지점에서 발생한 침해가 시스템 전반에 영향을 미칠 수 있다. 본 논문은 이러한 환경에서 발생 가능한 기밀성·무결성·가용성 위협을 정리하고, 이에 대한 대응으로 제로트러스트 보안 아키텍처를 제안한다. 이에 따라 VPP 상의 PDP, PEP의 설계 방안을 제시하고, 제로트러스트 성숙도 모델의 핵심요소에 따라 VPP에 적용 시 우선 고려사항을 제시한다.

Ⅰ. 서 론

가상발전소(Virtual Power Plant, VPP)는 여러 개의 분산 에너지 자원(Distributed Energy Resources, DER)의 네트워크를 통합하여 제어·운영함으로써 전력자원 배분과 활용을 최적화하는 에너지 관리 시스템이다[1]. VPP는 IoT/ICT를 기반으로 소규모 태양광 발전 시설, 연료전지 등 다양한 DER과의 연계를 통해 발전 데이터 및 전력시장 데이터를 수집·통합하여 하나의 발전소처럼 운영한다.

VPP 상에서 DER은 지리적으로 분산되어 있을 뿐만 아니라 벤더, 사양, 통신 방식이 상이하여 통합된 통신 및 제어 구조를 구성하는 데 높은 복잡성을 갖는다. 하지만 전력 제어가 실시간으로 수행되어야 하므로 배전계통, VPP 및 DER 간의 빈번한 정보교환이 필요하여 통신량이 많다. 또한, 중앙에 위치한 하나의 VPP 코어가 다수의 DER을 조율하는 시스템으로 데이터 조작 및 가용성 침해 공격에 취약하다. 이때 소수의 DER에 발생한 공격이 다른 DER 및 VPP 전반으로 확대되어 전체 전력서비스에 영향을 끼칠 가능성이 존재한다.

이러한 VPP 상에 대한 접근을 지속적으로 인증, 검증하는 제로트러스트 모델을 적용 시, 데이터 조작 공격 및 공격 확산 예방에 기여할 수 있다. 그러나 VPP 운영 구조를 대상으로 제로트러스트 보안 아키텍처를 체계적으로 설계하고 PDP·PEP 배치 관점을 제시한 연구는 아직 제한적이다. 이에 본 논문에서는 VPP에서 발생 가능한 위협을 정리하며, 이에 대응하기 위한 VPP 상의 제로트러스트 보안 아키텍처 도입 방안을 제안한다.

Ⅱ. VPP 상에 발생 가능한 위협

VPP는 다수의 DER을 하나의 자원처럼 집합 운영·제어하는 구조를 갖는다. 중앙의 VPP 코어, 현장 DER 및 배전 관리 시스템(Distribution Management System, DMS)이 지속적으로 데이터를 주고받으며 운영된다. 이때 계측·상태 데이터, 제어 명령 및 시장·정산 데이터 등 여러 종류의 데이터가 사용되며, 전압지원 등 빠른 반응이 필요한 기능은 통신 주기가 짧기 때문에 통신량이 많다. 또한 각 DER은 벤더, 운영자, 사양 등이 상이하므로 보안 수준의 편차가 존재할 수 있다. 많은 통신량과 DER의 보안 수준 편차는 공격 표면으로 작용하여 다음과 같이 기밀성, 무결성, 가용성 침해가 발생할 가능성이 존재한다[2].

- **기밀성 침해 :** 통신 구간에서 MITM 공격 발생 시 전압·출력 상태, 운영 데이터 등이 유출될 수 있음
- **무결성 침해 :** 데이터 위·변조 또는 FDIA로 인해 계측·상태 정보가 왜곡되어 전압지원 판단 오류가 발생할 수 있음
- **가용성 침해 :** 빠르게 이루어져야 하는 전압지원 등에 대해 DoS 공격이 수행될 경우 통신이 지연·누락될 수 있음

이때 VPP는 각 DER의 정보를 통합해 전체 시스템 제어를 조절하기 때문에 일부 DER 정보에 대한 데이터 조작이나 통신 지연·차단이 발생하는 경우 전체 VPP의 제어 입력을 왜곡해 전반적인 성능 및 안전성에 영향을 줄 수 있다[3]. 또한, VPP 상에서 각 DER의 보안성이 보장되지 않은 채 연계 운영될 경우 웜 등의 악성코드로 인해 일부 DER에 발생한 침해가 전염을 통해 다른 DER 혹은 VPP 코어, 통합 시스템 등 상위 시스템으로 이동할 수 있다[4]. 이러한 VPP의 제어 오류는 전력 시스템과 직접 연계되어 동작하므로, 전력 기반시설의 안전한 운영을 위해 충분한 보안 요구사항이 고려되어야 할 것이다.

Ⅲ. 제로트러스트 아키텍처 구성요소 및 핵심원칙

제로트러스트는 기존의 경계기반보안 방식을 벗어나 네트워크 등의 위치만으로 신뢰를 부여하지 않고 모든 접근을 검증하여 정책에 따른 접근과 시행이 수행되도록 하는 것을 뜻한다. 제로트러스트 아키텍처의 접근 제어 정책은 다양한 정보를 통해 정책결정지점(Policy Decision Point, PDP)에서 결정되며, 이는 각 경계의 정책시행지점(Policy Enforcement Point, PEP)에서 실행된다. PDP는 인증 수준, 행위 로그, 보안 이벤트 등 다양한 입력 신호를 통해 정책에 따라 접근 주체의 리소스 접근 허용·거부 여부를 판단한다. PEP는 이러한 결정을 전달받아 통신 경로의 연결을 허용·거부하는 등 정책에 따른 제어를 수행한다.

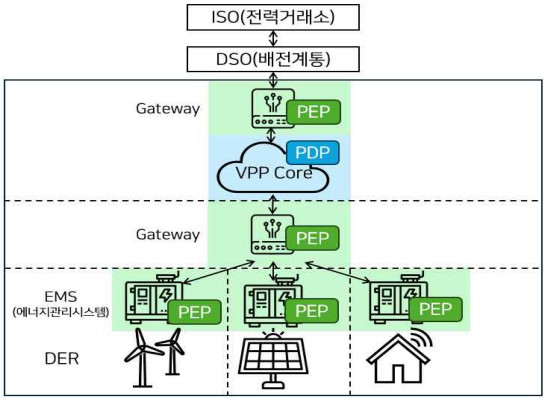
제로트러스트 성숙도 모델(Zero Trust Maturity Model)은 제로트러스트 아키텍처 구현을 위한 여섯 개의 핵심 요소를 정의하며 이는 식별자·신

원, 기기 및 엔드포인트, 네트워크, 시스템, 애플리케이션 및 워크로드, 데이터로 구성된다. 또한 각 영역은 요소별 기능으로 세분화되며, 각 기능에 대한 세부역량을 성숙도 단계에 따라 제시함으로써 점진적인 제로트러스트 도입이 가능하도록 한다[5].

Ⅳ. VPP 상의 제로트러스트 도입

본 절에서는 VPP 운영 구조를 전제로 제로트러스트 아키텍처 도입 방안을 구체적으로 설명한다. 먼저 제로트러스트 아키텍처의 필수 구성요소인 PDP, PEP을 VPP 제어 경계상에서의 배치 방안을 제시하며, 제로트러스트가 실제로 VPP 보안 위협을 보완하는 방법을 연관되는 제로트러스트 성숙도 모델 세부역량에 따라 제시한다.

4.1. VPP 제어 경계 기반 PDP·PEP 배치 방안



〔그림 1〕 VPP 상의 PDP/PEP 배치 구조

PDP는 VPP의 접근제어 정책을 중앙에서 일관되게 수행해야 하므로 VPP 코어가 위치하는 운영 계층에 배치한다. PDP는 다양한 정책정보지점(Policy Information Point, PIP)으로부터 제공되는 운영자·서비스·장치의 인증 및 권한 정보, DER 게이트웨이 등록·보안상태, 접속 구간 등 요청 컨텍스트, 보안 이벤트·탐지 정보 등 입력정보를 통해 신뢰도 판단을 수행할 수 있다. 정책에 따라 접근 허용 여부와 세션 조건을 결정한 뒤 그 결정을 정책시행지점(PEP)에 전달한다.

PEP는 PDP의 결정에 따라 주체와 리소스 간 연결을 설정, 종료, 모니터링하는 실행 기능으로서 정책에 따라 트래픽을 허용 또는 거부한다. 따라서 PEP는 외부 연계 계층, 운영 계층, 현장 계층의 경계와 각 DER 접속 구간 등 트래픽이 실제로 통과하는 제어 경계마다 분산 배치하는 형태로 구현해야 한다.

4.2. VPP 보안 위협 완화를 위한 제로트러스트 핵심요소 고려사항

제로트러스트 성숙도 모델에 정의된 핵심요소 6개에 대해 VPP에 적용될 때 우선적으로 고려해야 할 사항을 다음과 같이 정리하였다.

- **식별자/신원**
  - VPP 관리자, DER 운영자 및 DER·게이트웨이·외부 연계시스템(ISO/DSO) 등 장치 식별·인증 및 위험성 평가
  - 식별 대상의 VPP코어 등 운영계층 등 주요 시스템 접근 시 다중요소인증 및 지속인증 적용
  - 최소권한 접근을 통해 정산·입찰 변경 등 고위험 행위에 권한을 가진 사용자를 제한
- **기기 및 엔드포인트**
  - VPP 기업은 VPP 내 모든 하드웨어 기기에 대한 목록을 유지해야 하며, 접근하려는 기기의 신뢰도를 평가하여 신뢰할 수 없는 기기가 리소스에 접근하는 것을 막을 수 있어야 함
  - 다양한 보안 수준을 가진 DER, EMS, 인버터, 게이트웨이가 통합되므로 기기 상태 및 보안수준 기반 권한부여 등을 사용
- **네트워크**
  - 네트워크 환경상에 VPP코어, 시장·정산 연계구간, DER 등을 각 제어 경계로 분리하여 업무 통신만 정책적으로 허용하도록 설정
  - 제어 경계 간의 접근통제 및 데이터 흐름 매핑, 트래픽 암호화 적용
  - 전력 시스템과 직접적으로 연결된 VPP는 가용성이 중요하므로 이중화, 장애 조치, 복구절차 등을 통한 네트워크 회복성 설계 필요
- **시스템**
  - 시스템의 주요 파일 읽기, 쓰기, 명령어 사용 등 시스템 리소스 접근에 관한 상세한 접근제어 필요
  - VPP 코어, 시장·정산 연계 서버, 운영서버는 접근통제, 자격증명 관리가 핵심적이며 특권접근관리(Privileged Access Management, PAM)를 통해 권한 있는 사용자의 악성 행위를 제한할 수 있음
- **애플리케이션 및 워크로드**
  - 기업에서는 애플리케이션 계층 및 컨테이너 등을 보호 및 관리하고 데이터의 안전한 전달을 보장해야 함
  - 분산된 환경에서 동작하는 VPP 특성상 원격접속이 존재하므로 애플리케이션 단위의 정책 기반 접근통제와 세션 모니터링 적용
- **데이터**
  - 계측·제어 데이터와 시장·정산 데이터가 혼재하기에 데이터 라벨링 및 태그 지정을 통한 분류 적용
  - 데이터 암호화를 적용하며 허가받지 않은 데이터 유출에 대응하기 위한 기법 적용

Ⅴ. 결론

본 논문에서는 VPP의 구조적 특징으로 인해 발생하는 기밀성, 무결성, 가용성 측면의 보안 위협을 정리하고, 이를 바탕으로 VPP 상의 제로트러스트 보안 아키텍처 도입 방안을 제시하였다. PDP, PEP의 배치 방안을 제안하고, VPP 보안 위협 완화를 위한 제로트러스트 상의 고려사항을 제안하였다.

다만 본 연구는 VPP 운영 구조를 기능적으로 추상화하여 설계를 제안한 것으로, 실 환경의 네트워크 구성, 통신 프로토콜 등의 차이를 반영한 실증에 대한 추가 연구가 필요하다.

ACKNOWLEDGMENT

이 논문은 2026년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임(No. RS-2024-00396797, 지능형 오픈랜(Open RAN) 보안 플랫폼 핵심 기술 개발).

참 고 문 헌

[1] Alajlan, R. et al., “A Literature Review on Cybersecurity Risks and Challenges Assessments in Virtual Power Plants: Current Landscape and Future Research Directions,” IEEE Access, 2024. 12.

[2] Singh, K. N. et al., “Enhancing cybersecurity in virtual power plants by detecting network based cyber attacks using an unsupervised autoencoder approach,” Scientific Reports, 2025. 09.

[3] Chen, J. et al., “Vulnerability Analysis of Virtual Power Plant Voltage Support under Denial-of-Service Attacks,” 2023 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT), 2023. 01.

[4] U.S. Department of Energy (DOE), “Cybersecurity Considerations for Distributed Energy Resources on the U.S. Electric Grid,” Report, 2022. 10.

[5] 과학기술정보통신부, 한국인터넷진흥원(KISA), 한국제로트러스트포럼, “제로트러스트 가이드라인 2.0,” 2024. 12.