intertrust®

WHITE PAPER

Resilience and security for virtual power plants

Building trust for a connected world.

Contents

Virtual power plants and cybersecurity concerns **3**

Understanding VPP ecosystems **5**

VPP components 5

The role of trust in VPP operations 6

Virtual power plant vulnerabilities **7**

Vulnerabilities of disparate devices and networks 7

Automation and AI attacks 8

Data privacy and integrity 8

Addressing VPP vulnerabilities **9**

Intertrust XPN™ 9

XPN core capabilities 9

XPN capabilities for creating secure and interoperable VPP ecosystems 11

TEIA overview **12**

Conclusion **13**

Virtual power plants and cybersecurity concerns

A virtual power plant (VPP) is a network of distributed energy resources (DERs) such as solar panels, batteries, and smart devices that are aggregated and controlled through a centralized software platform. These DERs are involved in the production, distribution and consumption of energy that are usually owned by third parties.

Powered by sophisticated AI systems, VPPs orchestrate these DERs to work seamlessly with the grid to benefit the entire electrical distribution system through load and grid balancing and other services.

VPPs not only manage and orchestrate devices, their data is also used for financial transactions between the operators of the energy devices and the grid operator. Since these networks can provide valuable flexible services, another term for these systems is energy flexibility platform or an energy asset orchestration solution.

VPPs can increase the utilization rate of existing infrastructure and help enable the seamless transition from traditional energy systems to more decentralized, sustainable, and efficient renewable energy systems. For example, if there is an oversupply of renewable energy on a grid, the grid operator can use its VPP to direct batteries and controllable loads to store or consume energy.

VPPs can help grid operators to maintain balanced grids while increasing asset utilization which can help avoid expensive investments in transmission lines and other infrastructure. Given this value, Rethink Technology Research stated that "Virtual Power Plants (VPPs) will become the core of the future power grid.[1]"

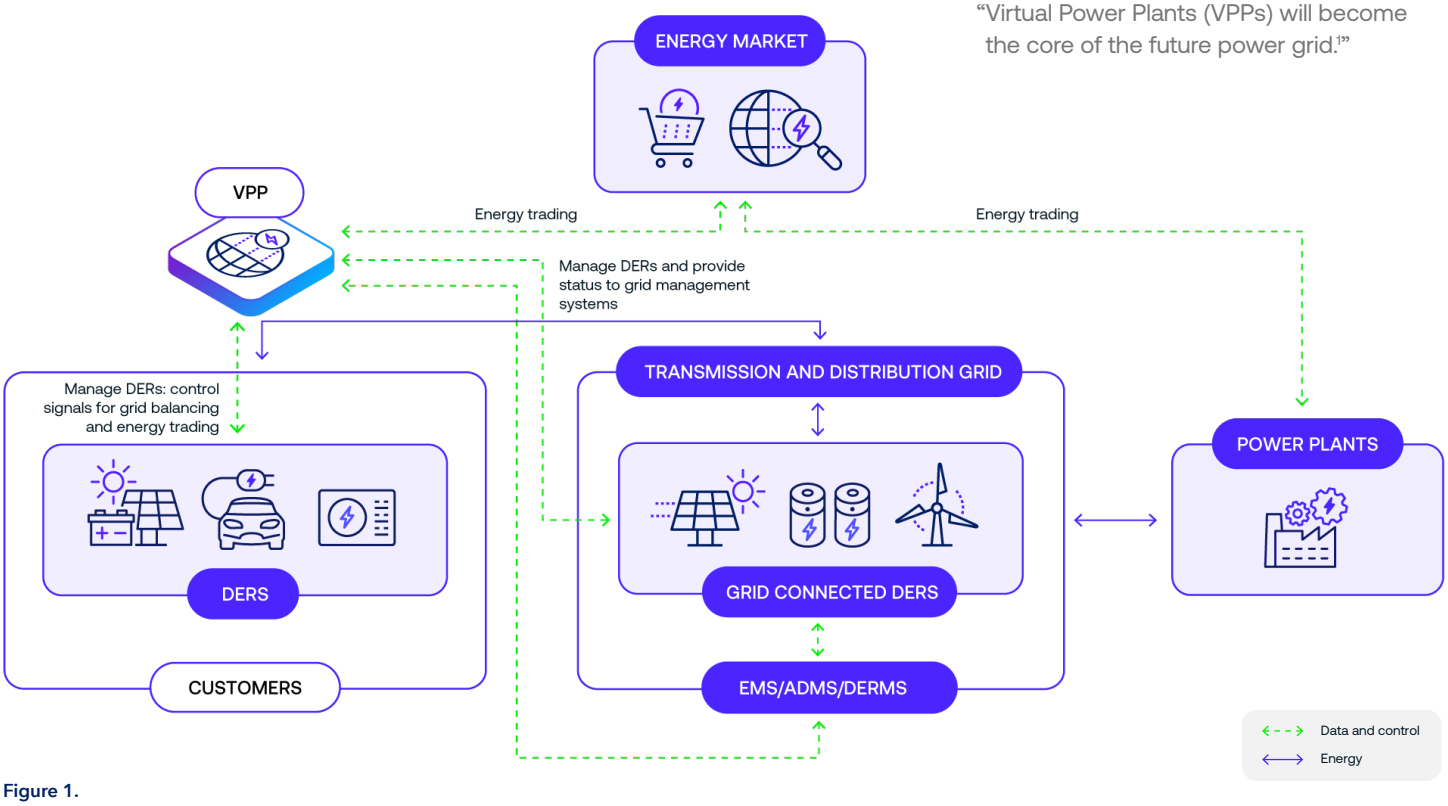

Figure 1.
Information flows between a VPP and other actors in the energy ecosystem. (EMS = energy management system, ADMS = advanced distribution management system, DERMS = distributed energy resource management system)

As VPPs continue to grow, they are increasingly becoming an integral part of critical national energy infrastructure. However, their distributed nature presents a new and attractive target for cybercriminals, often backed by malicious state actors. The growing number of distributed energy resources managed by a VPP platform represents a wide attack surface. Utilities around the world are under constant threat of attack from sophisticated cybercriminals who wish to disrupt the supply of energy.

The U.S. FBI and national security agencies of other countries have issued numerous warnings throughout 2023 and the beginning of 2024 about the dangers posed by hostile nation state actors to critical infrastructure targets such as electricity grids.

Up until now, utilities have only protected the infrastructure that they own and operate. The addition of VPPs to the grid adds an extremely complex ecosystem composed of components and software from a broad range of constantly shifting suppliers. The majority of these elements will be controlled by consumers and other third parties where security policies are uncertain at best.

Since VPPs potentially represent a very large number of consumer devices that are now used to contribute to the stability of the grid, utilities must grapple with securing these new ecosystems.

Each of the devices aggregated into the VPP ecosystem represents a potential target to exploit. If one is compromised, it can become a vector to attack the grid itself. These attacks could target utility systems that traditionally have been isolated from each other with differing security policies.

In short, without actively addressing the cybersecurity concerns of VPPs upfront, energy system operators face an even higher risk of extended exposure of large portions of their systems to cyberattacks by sophisticated cybercriminals. This paper provides details on the variety of security issues posed by VPP systems and introduces XPN (Explicit Private Networking) as a solution that can mitigate security concerns facing VPP operators.

The addition of VPPs to the grid adds an extremely complex ecosystem composed of components and software from a broad range of constantly shifting suppliers.

Understanding VPP ecosystems

VPP ecosystems bring together a wide variety of energy devices communicating with a control system over many types of networks. Given their crucial role in grid operations, maintaining trust in VPPs is vital.

VPPs can communicate over any number of network types. These can range from tightly controlled but highly vulnerable industrial and corporate networks to insecure household networks managed by consumers.

VPP components

VPPs are composed of three broad categories of components, a control system, the DERs being orchestrated, and the networks through which the control system and energy devices send data and commands to each other.

- **Control system**
  The control system is the central "brain" that manages and orchestrates distributed energy resources to create any number of benefits for the energy system. Given the complex calculations involved, these orchestration systems are driven by AI systems that work off many data feeds. On the grid side, these can include generation and grid conditions, weather predictions, electricity pricing, and forecasted energy loads. On the device side, these data feeds can include device status, consumption levels, and transaction values.

- **DERs**
  The number of energy devices that can participate in a VPP are broad. A short list includes electric vehicles (EVs) and chargers, solar panels, batteries, heat pumps and other HVAC equipment, smart water heaters, smart home appliances, commercial refrigeration systems, and industrial mechanical equipment. These devices could be under the control of single or multi-tenant dwellings, commercial buildings or industrial systems operators.

- **Networks**
  VPPs can communicate over any number of network types. These can range from tightly controlled but highly vulnerable industrial and corporate networks to insecure household networks managed by consumers. These networks involve a mixture of protocols using both wired and wireless connections. As data goes back and forth between devices and the VPP control system, it travels through a variety of networks.

The role of trust in VPP operations

As described above, VPP ecosystems are complex AI-driven systems that directly make decisions affecting grid operations and complicated financial transactions. VPPs rely on a wide variety of data inputs from multiple sources that the utility doesn't directly control.

To operate correctly, the VPP control system needs to operate with data that is trusted. This trust is created through the data being authenticated and with full confidence that it has not been tampered with. Also the commands that VPP control systems send to DERs have to be trusted to have the authority to send such commands. Without trusted data and commands, VPP operators risk any number of unwanted outcomes, some of which are expanded upon in this paper. Implementing a VPP with the proper cybersecurity elements in place is a crucial part in maintaining trust throughout the entire energy ecosystem.

VPP's operate within energy ecosystems that rely on OpenADR and many other standards. These standards address issues such as cybersecurity and data interfaces. Data trust is additive to the benefits these standards bring.

Virtual power plant vulnerabilities

The integration of diverse hardware components and software sourced from a wide array of suppliers inherently broadens the risk landscape for VPPs. Multiple points of potential failure and security threats may result.

Security approaches can differ between OEM vendors as well as between VPP operators. This introduces a tangled web of trust models that can vary significantly across vendors and operators.

Vulnerabilities of disparate devices and networks

VPP ecosystems include hardware components and software from a broad spectrum of suppliers, inherently expanding the risk landscape. Some of the vulnerabilities include:

- **Relying on untrusted devices**
  In both residential and commercial settings, an array of internet-connected energy devices play a crucial role in VPP functionality. Since VPP systems typically don't have direct control over the device, they must place implicit trust in operator and OEM security measures, which may not align with the VPP security requirements.

  For example, devices aren't usually authenticated or authorized by the VPP system itself. The VPP must rely on the authentication protocols put in place by either the device vendor or operator. Discrepancies in device authentication make it challenging to ensure that only legitimate devices and users can interact with the VPP, leaving the system vulnerable to unauthorized access and manipulation.

  Energy system operators should keep in mind that the VPP will also interact with devices under their control. Whether the device is under the control of the energy system operator or its customers, VPPs should be designed using zero trust[2] principles. This means that security policies should be designed to not trust devices or users and always authenticate an entity before interacting with it.

- **Multiple network protocol environment vulnerabilities**
  VPPs' reliance on multiple communication networks to synchronize a myriad of DERs introduces significant vulnerabilities. Commonly used protocols for residential energy devices such as Zigbee underscore this issue with their inherent security limitations.[3] The inadequate security measures of such home-based communication networks substantially increase the likelihood of exploitation by malicious actors.

- **Multi-cloud environment vulnerabilities**
  It should be kept in mind that connected energy devices are typically not isolated islands; they are interconnected with other cloud systems controlled by the device vendor or other third parties. VPP systems commonly work with energy devices through integrations with a vendor's cloud API[4]—not the actual devices themselves. These cloud systems rely on the vendor's device authentication protocols which can vary widely, may lack resilience and may even be under the control of a malicious party unknown to the vendor.

- **Lack of security interoperability**
  Security approaches can differ between OEM vendors as well as between VPP operators. This introduces a tangled web of trust models that can vary significantly across vendors and operators. This fragmentation hinders effective security monitoring and management, complicates the establishment of uniform security postures, and creates blind spots that malicious actors can exploit.

Cyber criminals can exploit vulnerabilities within VPP systems, gaining unauthorized access and leveraging these weaknesses in various ways. Here are some examples of the disruptions and data breaches they can cause.

Automation and AI attacks

AI systems driving VPPs depend highly on the quality and security of the data they process. Without stringent authentication, authorization, or integrity protections for devices and data, the data feeding into these systems can be compromised, leading to two main categories of risk:

- **Unwanted automation behavior**
  AI-driven control systems in VPPs are designed to make real-time decisions based on incoming data. These can malfunction or "go wild" if they process data that does not reflect actual conditions. Whether by deliberate falsification of data or inadvertent introduction of a bad data source into the ecosystem, the result can be catastrophic. Acting on bad data, the software might make erroneous decisions that threaten the operational integrity of the VPP, potentially leading to inefficiencies, energy waste, financial fraud or even physical infrastructure damage.
- **AI "hallucinations" from toxic data**
  AI models are particularly susceptible to the quality of the data they are trained on and analyze. When AI systems are fed toxic, manipulated, or otherwise compromised data, they can "hallucinate"—making decisions based on a distorted reality. This can result in the AI taking actions not only out of alignment with actual energy needs or grid conditions but also endanger the grid's stability.

Data privacy and integrity

Much of the vast amount of data collected, processed, and analyzed by VPPs will come from customers' energy devices, raising substantial privacy concerns. The advent of stringent privacy regulations such as the General Data Protection Regulation (GDPR) in the EU and the California Consumer Privacy Act (CCPA) in the U.S. means that VPP operators are exposed to legal risks in handling this data. Data breaches could lead to large regulatory fines, expensive legal actions and significant reputational damage.

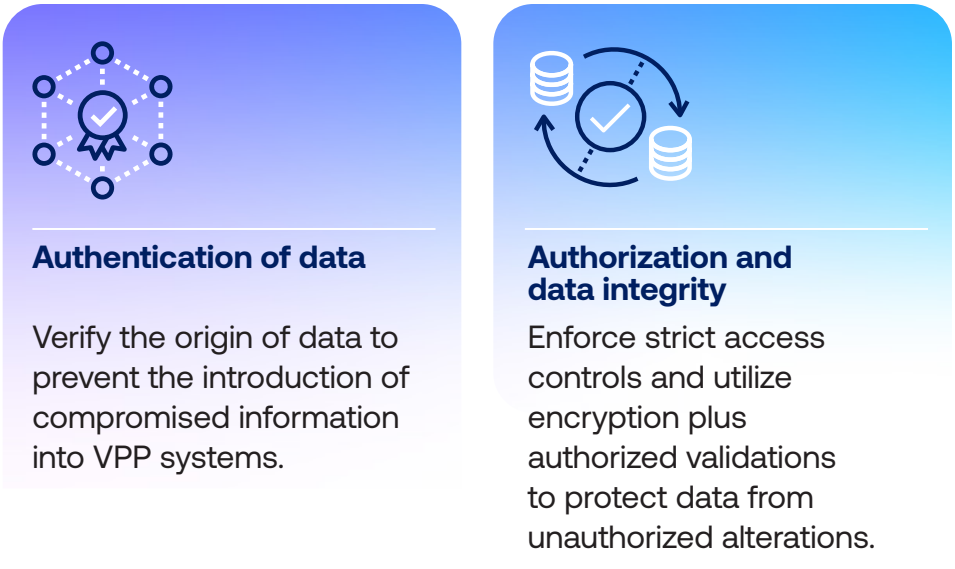

Figure 2.
Two important security measures that should be implemented to help avoid attacks on the AI-driven control systems of VPPs.

Addressing VPP vulnerabilities

While VPPs offer many advantages, they also represent significant liabilities if proper measures aren't taken to address these vulnerabilities. Energy system operators already take many measures to protect their own energy device and data assets from cybercriminals. The introduction of VPPs greatly expands the assets that energy system operators need to address. To do so, operators should look beyond traditional cybersecurity solutions.

XPN gives both VPP operators as well as the customers that participate in VPPs confidence that the orchestration of energy devices will be done with maximum trust.

Intertrust XPN™

One solution to address many of the vulnerabilities inherent to VPPs is Intertrust's XPN (Explicit Private Networking) secure communications service.[5] XPN is specifically designed to authenticate devices and persistently protect data as it travels from the originating device across untrusted networks to the cloud—and back to the device. It is not dependent on any network protocol and can maintain security throughout the data path.

This protection is not only for data streams sent from devices, it also extends to commands delivered to them. Based on a lightweight zero-trust client-server architecture, XPN leverages open standards and works interoperably across energy device vendors and cloud systems.

VPP ecosystems need to work with a wide variety of devices and cloud services operating in a multitude of networking and computing environments, making it ideal for VPPs to maintain trust throughout the entire ecosystem. It is also worth noting that XPN is not a "rip and replace" solution. It is well positioned to work with traditional cybersecurity measures to provide an additional layer of trust for VPP systems and is already being adopted in several VPP implementations.[6]

XPN core capabilities

Here are some of the core capabilities that XPN provides for VPP operators.

Tunnel through insecure protocols and devices
Many home energy devices combined into VPPs rely on networking protocols such as Zigbee with weak security. Additionally, traditional security measures such as virtual private networks (VPNs), are network protocol based and only protect data being transmitted across that network.

If a VPN is misconfigured or if the network is compromised in any way, the data ostensibly protected by the VPN is very vulnerable. The data can also be vulnerable once it leaves the network being protected as existing technologies only protect the network connection and not the data.

XPN addresses these limitations by providing persistent data protections by protecting data the moment it is generated on the device. XPN doesn't depend on connection-based security. The data remains protected even if it goes through an insecure gateway. It safeguards the data itself, offering a robust solution where other methods fall short.

VPP are vulnerable to improper data introduced by rogue devices. XPN avoids this by first having the XPN client authenticate a device before it sends data. XPN then uses optional encryption and data protection functions to protect the data when it is transmitted from the device. When the data is received by the cloud-based XPN service, it confirms the authenticity and integrity of the data. The data is then sent to authenticated cloud systems. Industry standards are used in all components, for example AES for ciphers; ECC or RSA for asymmetric cryptography; SHA for hashes.

- **Persistent edge-to-cloud protection**
  XPN's tunneling capabilities help secure data while it is both at rest and in transit. By doing so, XPN ensures continuous protection regardless of the data's location—whether on a device such as a gateway, in a network, or being handled in a third-party cloud system. XPN protects data from edge to cloud, extending trust from the point of data generation to its ultimate consumption in the cloud. Since cloud systems today are no longer limited to far away data centers, the XPN server may also be deployed at the edge.

  With the protections mentioned above, XPN ensures that the AI systems running VPPs can rely on trusted authenticated data and avoid any misbehaviors caused by incorrect data.

- **Authorized commands**
  VPPs are also vulnerable to attacks done by sending incorrect commands to the energy devices they work with. XPN avoids this by not only authenticating devices and protecting the data flows from the device to the cloud; it does the same for commands sent to the devices as well.

  The XPN authorization framework extends to software components of cloud systems and can authenticate the components responsible for sending commands to the devices. These commands are transmitted securely. With this capability, VPP ecosystem operators can ensure that XPN enabled energy devices will be able to trust both the authenticity and authority of commands it receives—a critical feature to enable industrial automation and AI without introducing vulnerabilities.

- **Bridge across IT/OT customer environments**
  XPN's tunneling capabilities are also independent of the environments the data is traveling through, whether those environments are controlled by a customer or the energy system operators' IT or OT organizations. As such, XPN can act as a trusted bridge for energy device data flows across all of these environments and enables a trusted way for data to traverse network segmentations, so called "air gaps."

XPN delivers secure and interoperable VPP ecosystems

XPN's capabilities are well suited to VPPs that have to orchestrate a large number of disparate energy devices with maximum trust. The VPP operator can rest assured that it is working with authenticated energy devices, that the AI systems it relies on are using persistently protected trusted authentic data and energy devices will only respond to authentic commands. XPN's capabilities also extend to providing an interoperable and secure ecosystem for VPP operators.

- **Interoperable device and data protection**
  XPN's device and software authentication capabilities are interoperable regardless of the device or software manufacturer. It is independent of network protocols and can easily work across disparate communication systems. This is particularly important for VPPs since they need to work with a vast variety of constantly shifting energy devices tied together over a wide variety of networks. VPP operators also have the flexibility to work with different software systems in their clouds.

- **Zero-trust compatibility**
  Given the well demonstrated capabilities of cybercriminals to breach the security of most any organization, zero trust based security solutions are mandatory. Zero trust is essential to any VPP ecosystem since it is especially difficult for a VPP operator to guarantee the security posture of all the devices in their ecosystem. As a zero trust compatible system that consistently authenticates and authorizes each device and software component in the VPP ecosystem, XPN fulfills this requirement.

- **Trusted orchestration of devices**
  With these capabilities, XPN gives both VPP operators as well as the customers that participate in VPPs confidence that the orchestration of energy devices will be done with maximum trust. Devices, data, software and commands are all authenticated and protected. The AI systems driving the VPP operations are basing decisions from trusted data. This trust can also be extended to the financial transactions that VPPs generate.

- **Based on open standards**
  Energy system operators have had long experience in utilizing components based on open standards. XPN fits in well with this tradition since it is the first software product based on the Trusted Energy Interoperability Alliance (TEIA) standard.[7] Accordingly, XPN based system users aren't locked into any particular vendor.

TEIA

The Trusted Energy Interoperability Alliance (TEIA) develops and maintains an open, global security and interoperability standard for energy devices and data.

This standard allows energy system operators to use devices and software that are interoperable to help them build new digital energy systems without fear of vendor lock-in.

Formed in June 2023, TEIA members represent over 150 GW of energy capacity across four continents.

TEIA's goal is to enable flexible ecosystems where developers can efficiently create secure applications to integrate best-of-breed devices and software from multiple vendors.

Security and interoperability data standards for a sustainable energy future.

Figure 3.
Founding members of TEIA

Conclusion

VPPs will undoubtedly be one of the core components of the modern digital clean energy-based systems needed to help decarbonize our economy. Ensuring that VPPs are a trusted part of these systems is essential for their success.

Maintaining the security of the greatly expanded attack surface that VPPs represent seems like a nearly impossible task. Yet, failure to do so could lead to any number of undesirable outcomes, including disruptions to energy supplies.

Intertrust XPN provides an important tool for operators to strengthen the security posture and resilience of VPPs. Not only do the technical capabilities of XPN contribute to this goal, because it is based on open standards and interoperates with a variety of devices and software, it gives VPP operators maximum flexibility.

Footnotes

1 *Virtual Power Plant (VPP) Forecast to 2040*, Rethink Technology Research, April 2024

2 Zero Trust Architecture is a security model based on the principle of least privilege. Zero Trust assumes that no user or device can be trusted, even if they are inside the corporate network. This is in contrast to traditional security models, which typically trust users and devices inside the network and only require authentication for users outside the network. (from https://www.sans.org/blog/what-is-zero-trust-architecture/).

3 Some potential attacks on Zigbee networks are described in *Don't Kick Over the Beehive: Attacks and Security Analysis on Zigbee*, Xian Wang, Shuang Hao, University of Texas at Dallas, https://personal.utdallas.edu/~shao/papers/wang_ccs22.pdf

4 Application Programming Interface see https://en.wikipedia.org/wiki/API

5 Information on XPN can be found at https://www.intertrust.com/xpn/

6 One example is EIPGRID's xVPP product. See https://www.intertrust.com/news/eipgrid-and-intertrust-unveil-worlds-first-secure-scalable-virtual-power-plant-technology/

7 For more information on TEIA see https://www.trusted-energy.org/

Learn more at: intertrust.com/xpn
Contact us at: energy@intertrust.com
+1 408 616 1600

intertrust®

Building trust for a connected world.