Virtual Power Plant Architecture and Resilient Design

INL/RPT-26-89692

Center for Securing Digital Energy Technology (CSDET)

JANUARY 2026

Megan Culler
Remy Stolworthy
Robert Edsall

Idaho National Laboratory

Patrick Heeter
Alex Tylecote
Joshua Kmiec
Todd Ponto

ScottMadden

Idaho National Laboratory

Battelle Energy Alliance manages INL for the U.S. Department of Energy's Office of Nuclear Energy

INL/RPT-26-89692

Virtual Power Plant Architecture and Resilient Design

Megan Culler
Remy Stolworthy
Robert Edsall
Idaho National Laboratory

Patrick Heeter
Alex Tylecote
Joshua Kmiec
Todd Ponto
ScottMadden

January 2026

Idaho National Laboratory
Idaho Falls, Idaho 83415

http://www.inl.gov

Prepared for the
U.S. Department of Energy
Under DOE Idaho Operations Office
Contract DE-AC07-05ID14517

Page intentionally left blank

ABSTRACT

Virtual Power Plants (VPPs) represent a fundamental shift in electric grid operations, aggregating distributed energy resources (DERs) to deliver utility-scale grid services traditionally provided by centralized power plants. This report examines the unique architectural, operational, and digital assurance considerations that distinguish VPPs from conventional utility infrastructure as they scale from pilot projects to mainstream deployment across the United States.

While VPPs offer significant opportunities for grid modernization and enhanced flexibility, their distributed, multi-stakeholder architecture introduces distinct security challenges that differ fundamentally from traditional generation facilities. The analysis identifies risks in VPP operations, including device-level security gaps, platform vulnerabilities, and communication protocol weaknesses that create expanded attack surfaces compared to centralized power plants.

Through examination of real-world incidents and emerging threat patterns, the report demonstrates how some VPPs' reliance on consumer-owned devices, public internet infrastructure, and complex vendor ecosystems require new approaches to digital assurance and operational security. The findings provide practical guidance for utilities, regulators, and aggregators to implement robust security frameworks and operational best practices essential for maintaining grid reliability as VPP deployment accelerates under the Federal Energy Regulatory Commission (FERC) Order 2222 and related regulatory initiatives.

Page intentionally left blank

CONTENTS

1 INTRODUCTION 13
2 VIRTUAL POWER PLANT BACKGROUND AND CONTEXT 14
2.1 Definition and Differentiation 14
2.2 History and Growth of DERs and Emergence of VPPs 15
2.3 Regulatory Drivers 16
3 COMPREHENSIVE GRID SERVICES PORTFOLIO 17
3.1 Energy Services 17
3.2 Capacity Services 18
3.3 Ancillary Services 18
3.4 Resilience Services 18
4 VPP ARCHITECTURE AND MARKET PARTICIPATION MODELS 19
4.1 VPP System Overview: DERs, Aggregators, and Grid Interfaces 21
4.1.1 Electricity Consumers Layer 21
4.1.2 VPP Provider Layer 22
4.1.3 Distribution System Operator Layer 23
4.1.4 Bulk Power System Operator Layer 23
4.2 Interoperability and Coordination Layers 24
5 VPP DIGITAL ASSURANCE CONSIDERATIONS 25
5.1 Threat Vectors and Attack Pathways in VPP Operations 25
5.1.1 Platform-to-Grid Conduits as High-Consequence Attack Paths 26
5.1.2 Device-Level Vulnerabilities 26
5.1.3 Platform and Aggregator Vulnerabilities 27
5.1.4 Communication and Protocol Vulnerabilities 27
5.2 Historical Incidents and Emerging Threat Patterns 28
5.2.1 UK VPP Platform Breach (2024) 28
5.2.2 DER Monitoring Device Compromise (May 2024): 28
5.2.3 California Heat Wave Response (September 2022) 28
5.2.4 Viasat KA-SAT (February 2022): 29
5.2.5 SolarWinds (December 2020) 29
6 DEFENSE STRATEGIES FOR VPP DIGITAL ASSURANCE AND RESILIENCE 29
6.1 Consequence-Based Assessments 29
6.1.1 Prioritizing VPP Design Practices Using NARUC's Cybersecurity Baselines 30
6.2 System-of-Systems Analysis 30
6.3 Attack Path Analysis 31
6.4 Cyber-Informed Engineering 31

7 DIGITAL ASSURANCE RECOMMENDATIONS 32
7.1 Device-Level Operational Practices 32
7.2 Platform and Aggregator Operational Practices 33
7.3 Communication and Protocol Operational Practices 34
8 CONCLUSIONS AND NEXT STEPS 35
Appendix A – Prioritization of NARUC Cybersecurity Baselines for VPPs 37
References 40

FIGURES

Figure 1. Overview of VPPs by ScottMadden Inc. 14
Figure 2: 2024 State and Utility Action on VPPs by The NC Clean Energy Technology Center 17
Figure 3. Four VPP Market Participation Models (left to right): Third-Party VPP at ISO/RTO Level, Third-Party VPP at Utility Level, Utility VPP with Vendor Platform, Utility VPP with Proprietary Platform [1] 20
Figure 4: VPP Operational Model from the DOE 2023 Pathways to Commercial Liftoff Report [1] 21

TABLES

Table 1. Illustrative Prioritization of NARUC Cybersecurity Baselines for Virtual Power Plants 37

Page intentionally left blank

ACRONYMS

ADMS	Advanced Distribution Management Systems
API	Application Programming Interface
CAISO	California Independent System Operator
CIE	Cyber-Informed Engineering
CISA	Cybersecurity and Infrastructure Security Agency
CSDET	Center for Securing Digital Energy Technology
DER	Distributed Energy Resource
DERMS	Distributed Energy Resource Management Systems
DMZ	Demilitarized Zone
DOE	U.S. Department of Energy
DR	Demand Response
DSGS	Demand Side Grid Support
ELRP	Emergency Load Reduction Program
EPRI	Electric Power Research Institute
ESS	Energy Storage System
FERC	Federal Energy Regulatory Commission
GW	Gigawatt
GWh	Gigawatt-hour
HVAC	Heating, Ventilation, and Air Conditioning
IEEE	Institute of Electrical and Electronics Engineers
INL	Idaho National Laboratory
IoT	Internet of Things
ISO	Independent System Operator
ISO-NE	ISO-New England
IT	Information Technology
KEV	Known Exploited Vulnerabilities
kWh	Kilowatt-hour
MISO	Midcontinent Independent System Operator

MW	Megawatt
MWh	Megawatt-hour
NAESB	North American Energy Standards Board
NARUC	National Association of Regulatory Utility Commissioners
NCCoE	National Cybersecurity Center of Excellence
NERC	North American Electric Reliability Corporation
NLR	National Laboratory of the Rockies
NYISO	New York Independent System Operator
OEM	Original Equipment Manufacturer
OT	Operational Technology
PJM	PJM Interconnection
RFP	Request for Proposal
RSA	Rivest-Shamir-Adleman
RTO	Regional Transmission Organization
SCADA	Supervisory Control and Data Acquisition
SLA	Service Level Agreement
SPP	Southwest Power Pool
U.S.	United States
VLAN	Virtual Local Area Network
VPP	Virtual Power Plant
VPN	Virtual Private Network

Page intentionally left blank

Virtual Power Plant Architecture and Resilient Design

1 INTRODUCTION

The electric sector is evolving from the analog, centralized, and largely manual operations of the past toward a more decentralized, digital, and bidirectional grid. Driven by the technological advancements of distributed energy resources (DERs) and digital control systems, some utilities are integrating DERs at scale with the goal of augmenting grid performance and reliability. These distributed resources include solar, wind, battery storage, smart thermostats or other load management, and other small-scale generation and storage technologies and loads that interface with the electricity system at the distribution level. Proliferation of DERs throughout utility territories introduces opportunities and challenges for grid operations.

Virtual Power Plants (VPPs) are aggregations of DERs that provide generation and deliver utility-scale grid services comparable to traditional utility infrastructure. Rather than operating DERs as individual, localized assets with limited capabilities on their own, VPPs function as a tool for flexibly managing both distributed demand and supply with precision previously achievable only through centralized generation [1]. These aggregations can serve various grid roles: some VPPs primarily shape demand by orchestrating behind-the-meter consumption and generation, while others export electricity back to the grid [1]. By harnessing the flexibility and capacity of distributed resources, VPPs provide an alternative to constructing utility-scale capacity while maintaining the ability to respond rapidly to grid needs.

This report examines the unique characteristics of VPPs and how they diverge from traditional utility operations. The increased use of VPPs creates opportunities for enhanced utility operations, but also introduces distinctive resilience, operational, and security considerations. VPPs require specialized digital architectures and assurance frameworks distinct from those used for conventional utility systems. In addition to clarifying what makes VPPs unique, this report provides practical guidance on digital assurance considerations that arise when DERs are aggregated at scale.

This analysis is focused on the following areas relevant to United States (U.S.) utilities, regulators, and aggregators:

- Technical and operational differences between VPPs and conventional utility assets.
- Regulatory structures shaping aggregator participation, particularly under the Federal Energy Regulatory Commission (FERC) Order 2222 and related state-level initiatives.
- Resilience requirements that extend beyond digital assurance to include communications reliability and operational continuity.
- Best practices for digital assurance, informed by U.S. pilots and early international programs.

Across the U.S., VPPs are moving from pilot projects to large-scale deployments. Federal and state regulators are implementing rules that allow aggregated DERs to participate directly in wholesale markets, and utilities are beginning to rely on VPPs as part of their distribution operations. VPPs primarily operate at the distribution level, though their aggregated outputs can influence transmission-level operations. This transition introduces new risks. Coordinating distributed devices increases operational complexity, creates a larger attack surface for cyber and physical threats, and challenges traditional approaches to reliability. Guidance will support utilities, regulators, and aggregators to ensure that VPPs are designed and operated in ways that enhance domestic energy security and maintain system reliability.

2 VIRTUAL POWER PLANT BACKGROUND AND CONTEXT

2.1 Definition and Differentiation

The U.S. Department of Energy (DOE) defines VPPs as "aggregations of DERs that can balance electrical loads and provide utility-scale and utility-grade grid services like a traditional power plant" [1]. A VPP uses a digital platform to forecast, optimize, and dispatch thousands of devices so that they operate as a unified portfolio rather than as isolated assets. These DERs may be located either behind the customer meter or on the distribution network, depending on program design and regulatory structure. VPPs replicate capabilities that were traditionally limited to centralized generation, such as energy production and dispatch, while also enabling functions that centralized plants could not provide, including demand-side flexibility and distributed storage coordination. These functions are often implemented through operational models that do not fall under the same regulatory frameworks applied to conventional generators. Different configurations of VPPs provide differing functions. Most existing VPPs focus on shaping net demand by adjusting consumption or storing energy for on-site use, while a smaller set of programs export electricity from behind-the-meter resources back to the grid [1].

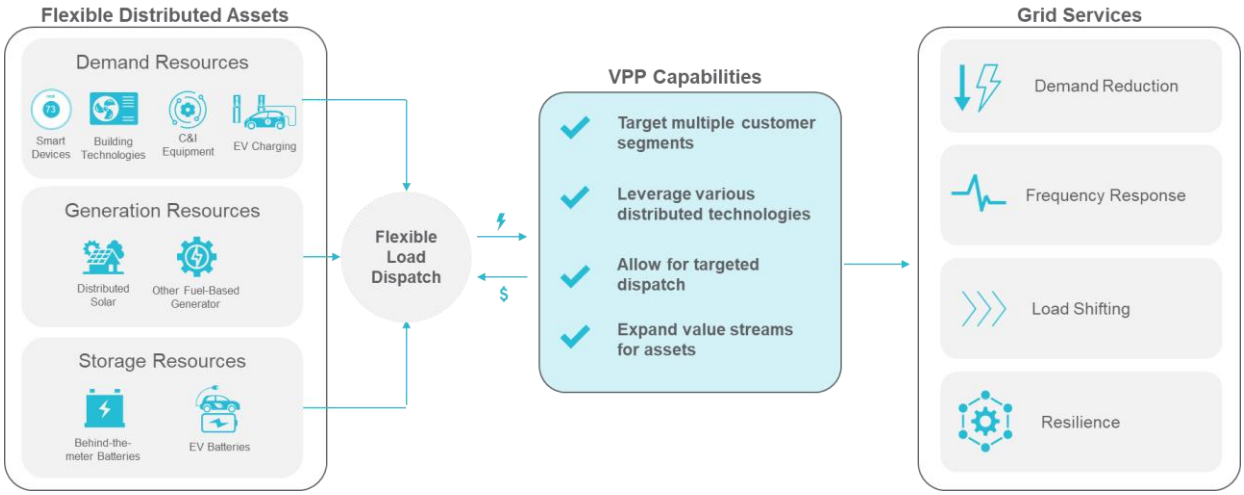

Figure 1. Overview of VPPs by ScottMadden Inc.

Terminology and Related Concepts

- **Traditional Power Plants**: Centralized generation facilities located at a single site and typically owned and operated by utilities. They provide reliable dispatchable capacity but differ in that they do not match VPPs' geographic distribution across the grid or direct integration with customer-sited resources.
- **Distributed Energy Resources (DERs)**: Physical assets located on the distribution system or behind customer meters, including storage, distributed generation, demand response, energy efficiency, thermal storage, and electric vehicles, as defined by FERC. Some resources function as flexible loads insofar as they can modulate power draw based on grid conditions, making them valuable for demand-side management [1]. DERs represent the physical assets themselves, while VPPs provide the coordination that aggregates these individual resources into a unified, dispatchable portfolio.
- **Distributed Energy Resource Management System (DERMS)**: Utility-facing software platform that monitor and control DERs in real time. DERMS track DERs and coordinate them to support both the grid and customers. For VPP operators, DERMS can serve as a bridge connecting grouped DERs with utilities or consumers. These platforms analyze patterns and

schedule resource deployment to extract maximum benefit from DER portfolios. DERMS may function independently or work in conjunction with an Advanced Distribution Management System (ADMS). Where ADMS' manage distribution grid operations, DERMS specializes in DER coordination. Although VPPs don't require ADMS integration, they are important when scaling VPP involvement in broader grid management [1].

- **Aggregators**: Entities that aggregate DERs for participation in Regional Transmission Organizations (RTOs) and Independent System Operators (ISOs) capacity, energy, and ancillary service markets, as defined by FERC [1]. While aggregators represent the market participant responsible for enrollment, metering, and settlement, VPPs constitute the portfolio of distributed resources. An aggregator typically operates a VPP to coordinate and optimize its DER portfolio, but the terms remain distinct: the aggregator is the business entity, the VPP refers to the technical system used to manage and dispatch the aggregated resources. For example, EnergyHub operates as an aggregator supporting multiple utility VPP programs across several U.S. markets.

VPPs represent a distinct grid resource: geographically dispersed technology resources coordinated through software to deliver grid flexibility at scale. This combination of decentralized assets and centralized coordination differentiates VPPs from both conventional generation facilities and traditional utility grid management platforms, such as Supervisory Control and Data Acquisition (SCADA) systems or ADMS.

2.2 History and Growth of DERs and Emergence of VPPs

The evolution of DERs in the United States spans nearly thirty years, beginning with early net energy metering programs, where utility customers received retail rates for electricity exported to the grid [2]. The regulatory foundation for aggregated DERs emerged in 2008 when FERC ordered RTOs to allow demand response aggregators to participate in wholesale markets, followed by a 2010 order requiring equal compensation for demand response providers and traditional generators, a decision upheld by the Supreme Court despite legal challenges from generation companies [3]. These early aggregation models evolved from simple demand response programs, such as the New Hampshire Electric Co-op's 1979 interruptible water heating program [1], into increasingly sophisticated VPPs that manage diverse distributed assets. The regulatory framework reached a crucial milestone with FERC Order 2222 in September 2020, which required all ISOs/RTOs to enable full DER aggregation participation in wholesale markets, formally establishing VPPs as legitimate utility-scale resources [1].

Today, more than 500 VPP projects operate in the United States [4]. The DOE estimates that today's VPP capacity of approximately 30 gigawatts (GW) could scale to 80–160 GW by 2030, representing 10–20% of projected peak forecasted load in 2030 and delivering up to $10 billion in annual system savings [5]. This anticipated growth is propelled by accelerating electricity demand driven by data centers, electrification, and manufacturing - all generation solutions will be needed to support increased electric load. However, residential adoption of DER technologies remains modest. Roughly 3.8% of households have rooftop solar, less than 1% have behind-the-meter batteries, and just over 13% have smart thermostats [5]. The slow integration of behind-the-meter residential resources constrains available capacity to use in behind-the-meter VPPs. Additionally, barriers such as high upfront costs, limited financing, and split incentives for renters further slow residential deployment of DERs.

Recent industry analysis from Wood Mackenzie shows rapid expansion in VPP adoption alongside persistent growth constraints [6]. Between 2024 and 2025, the number of active VPP deployments in North America jumped 33% to 1,940 programs [6]. Yet total VPP capacity grew much more slowly, increasing just 13.7% to reach 37.5 GW [6]. This gap suggests that VPPs are reaching more customers and locations, but enrollment caps and wholesale market rules may be limiting individual programs from growing larger [6]. Part of this growth reflects the emergence of independent distributed power producers, a new class of energy retailers that generate revenue by selling grid services and taking advantage of price

arbitrage [6]. Alongside these distributed deployments, utilities and large commercial customers are driving significant demand for VPP capacity. The number of companies procuring VPP services increased 38% year over year, with the top 25 buyers each procuring 100 megawatts (MW) or more in 2025 [6]. Much of this demand stems from data center growth. Wood Mackenzie found particularly robust VPP procurement in regions with substantial existing and projected data center capacity, including the PJM Interconnection and Electric Reliability Council of Texas [6]. VPPs help utilities procure capacity to offset data center peak demand, enabling faster grid connection [6]. American Electric Power, which operates in both regions, expects to interconnect 18 gigawatts of new data center demand by 2030, creating substantial opportunity for VPP deployment in its service territories [6].

Despite rapid momentum, persistent headwinds remain for VPP growth, including program enrollment limits, reduced capacity, accreditation in wholesale markets, and limited access for smaller customers [6]. Nonetheless, surging electricity demand and the accelerating pace of data center development are motivating both utilities and hyperscale users to scale VPP adoption, creating new revenue streams for DER owners and advancing the transition toward a more flexible, resilient grid.

2.3 Regulatory Drivers

At the federal level, FERC Order No. 2222, issued on September 17, 2020, serves as the cornerstone for driving VPP deployment by mandating that RTOs and ISOs adapt their market rules to accommodate aggregated DERs [7]. The order removes longstanding barriers, including restrictive size thresholds and technology-specific limitations, by defining DERs broadly and allowing heterogeneous aggregations to participate in energy, capacity, and ancillary services markets under flexible participation models [8]. RTOs and ISOs are required to create new tariff provisions, register DER aggregators as market participants, and ensure locational requirements are as geographically broad as technically feasible [7]. The rule also clarifies that DER aggregators, though subject to FERC jurisdiction for wholesale sales, are not subject to public utility regulation on individual DERs within the aggregation [8]. This expansion of market access is expected to accelerate the growth of DER participation, while also creating new coordination challenges for regional grid operators, distribution utilities, and state regulators. Because Order 2222 allows each RTO and ISO discretion in how they craft compliance rules, the resulting frameworks are likely to vary across regions. Such tailoring may better reflect local grid conditions, but participants active in multiple markets will need to manage differences in rules and procedures [8]. While FERC Order 2222 establishes market-participation rules, it does not address cybersecurity or digital-assurance requirements, leaving these issues to state or utility guidance.

Complementing this federal mandate, the DOE has historically provided financial and technical support through programs such as its Loan Programs Office and grid modernization initiatives, while states and utilities are developing pilots and programs that operationalize DER aggregation via VPPs. Programs such as state-mandated VPP tariffs in Colorado [9], regulatory pilots in Maryland, and VPP-specified planning targets in North Carolina and Washington, further propel VPP adoption as an integral piece of the modern U.S. power grid [10]. In 2024, 38 states and the District of Columbia advanced a total

of 105 policies and regulatory actions related to VPP (aggregated DER) , with most efforts centered on utility-level VPP, demand response, and managed charging programs [10].

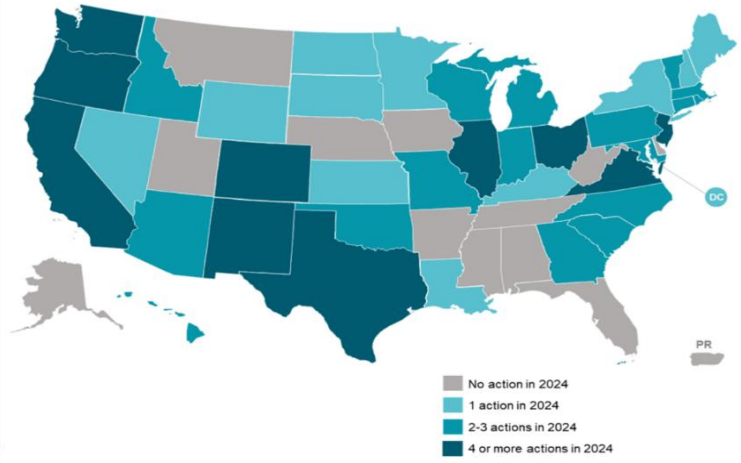

Figure 2: 2024 State and Utility Action on VPPs by The NC Clean Energy Technology Center

3 COMPREHENSIVE GRID SERVICES PORTFOLIO

VPPs deliver several grid services that maximize the value of distributed energy resources and support grid operations and service to energy consumers. Generally, it is understood that there are four grid services that VPPs provide [11]:

Energy	Capacity	Ancillary	Resilience
The production or delivery of electric power over time, measured in kilowatt-hours (kWh) or megawatt-hours (MWh), within a distribution system or microgrid.	A non-wires alternative that reduces peak loading on distribution infrastructure through targeted power reduction or load modification.	Grid support services that maintain operational reliability including frequency response, voltage regulation, and reserve management.	Backup power supply for local customers during grid outages or when operating in island mode disconnected from the main grid.

Each service addresses operational grid requirements and provides benefits for both utilities and participants:

3.1 Energy Services

VPPs are designed to optimize energy production and consumption patterns by shifting load, effectively arbitraging price and distributed resource generation availability. This dynamic energy management extends beyond demand-response to include charging and discharging cycles that align with system conditions. Rocky Mountain Power's WattSmart program demonstrates this capability through daily load cycling, charging residential batteries during low-cost off-peak periods (less than 3 cents/kWh) and discharging during peak hours when costs can reach 10 times higher [5]. This arbitrage reduces system costs while storing excess local energy that would otherwise be lost, creating economic value from existing grid volatility. Energy arbitrage capabilities were demonstrated at scale during the June 2025 heat dome, when EnergyHub (a VPP aggregator and a DERMS vendor) [12] shifted 3.5 gigawatt-hours (GWh) of energy away from peak demand periods, while CPower (a VPP aggregator and DER monetization

platform) [13] dispatched 18.5 GWh across 120 events spanning PJM, ISO-New England (ISO-NE), and New York ISO (NYISO) territories [14].

3.2 Capacity Services

VPPs provide dispatchable capacity in the form of instantaneous power that can be delivered during high-demand periods. Utilities can rely on this capacity for resource adequacy and peak demand management, reducing the demand on peaking plants. This capacity is predictable and measurable, allowing utilities to incorporate VPP resources into planning processes. Pacific Gas and Electric's Peak Power Rewards program demonstrated this service by delivering a consistent average of 27 MW over two-hour periods for 90 consecutive days during summer 2023 [11], while Arizona Public Service's Cool Rewards Program has demonstrated 140 MW of smart thermostat capacity as part of its 190 MW total VPP capacity, showcasing how residential devices can provide utility-scale resources [14]. Green Mountain Power's aggregated residential batteries reduce the utility's forward capacity obligations in ISO-NE markets by 36 MW, directly lowering capacity charges for all ratepayers [5].

This reliability has become increasingly critical during grid emergencies, but also as a consistent component of routine grid operations. The rising frequency of extreme weather events, growing electrification, and heightened peak demand are transforming what were once rare emergencies into more regular occurrences. As a result, capacity services provided by VPPs are no longer occasional supplements, but increasingly essential resources for daily grid stability. For example, Voltus [15], which experienced only one large PJM emergency dispatch in six years prior to 2025, has already responded to at least eight emergency dispatches in 2025 alone [16]. During a recent Baltimore-area transmission emergency when the Brandon Shores Power Plant went offline, VPP resources were dispatched in multiple waves based on resource readiness demonstrating operational sophistication in emergency response [16].

3.3 Ancillary Services

VPPs deliver sophisticated ancillary services that maintain grid stability through real-time balancing and power quality management. These services include frequency regulation, voltage support, spinning reserves, and ramping capabilities that have traditionally required specialized generation assets. Rocky Mountain Power's WattSmart program demonstrates this capability through secondary frequency response that rebalances system frequency in as little as three seconds, performing 153 real-time response events between October 2023 and November 2024 [5]. Similarly, Green Mountain Power expanded its battery programs' value streams in 2021 by participating in ISO-NE's regulation market, using customer-sited batteries to provide frequency regulation services to the wholesale market [11]. This capability proves especially valuable in high wind and solar markets like the Southwest Power Pool (SPP), where wind generation can exceed 90% on some days. The resulting grid volatility requires VPP resources to provide operating and spinning reserves at least once daily for 10-20 minute intervals, demonstrating how VPPs become indispensable balancing resources as grids transition toward distributed systems [17]. This multi-service capability transforms static customer assets into dynamic grid resources that respond to millisecond-level system needs.

3.4 Resilience Services

VPPs enhance system resilience through several functions, including: preventing outages through emergency response, mitigating impacts through backup power provision, and accelerating recovery through distributed black-start capability [5]. A During the June 2025 heat dome that pushed PJM to serve 161 GW of load, FERC Chair Mark Christie confirmed the essential role of demand response (DR) in a subsequent FERC press conference:

> “PJM said that demand response was essential. DR doesn’t serve load, DR reduces load. So that 161-gig peak would have actually been higher without DR, because that’s what DR does. DR lowers peak, and that’s what DR is supposed to do...” [17]

Major VPP operators delivered unprecedented response: Sunrun dispatched over 340 MW from customer-sited batteries on June 24, EnergyHub shed 900 MW of peak load while shifting 3.5 GWh of energy away from peak periods, and Uplight managed 350 MW of flexible load across 45 dispatch events in 16 utility programs during the heat dome week [14]. Resilience here refers to outage prevention and recovery functions, complementary to the capacity and ancillary services described above.

Similarly, during California's September 2022 heat wave, the Emergency Load Reduction Program (ELRP) and Demand Side Grid Support (DSGS) programs prevented rolling blackouts for nine consecutive days by mobilizing distributed resources when traditional reserves were exhausted [11]. In July 2025, California ISO (CAISO) and PG&E further validated this capability by coordinating what they termed the largest-ever VPP capability test, with Tesla's and Sunrun's programs delivering over 500 MW of flexible power to the grid [17].

For individual consumers, Green Mountain Power's Energy Storage System Leasing program has enrolled over 4,800 customers with battery systems designed to provide seamless backup power during outages and extreme weather events [5]. For system restoration, Duke Energy's Hot Springs microgrid in North Carolina, comprising 2 MW of solar and 4.4 MWh of battery storage with VPP-enabling technology, demonstrated recovery capabilities by quickly restoring power to residents after Hurricane Helene in 2024, even though the local substation was severely impacted by flooding [5]. The microgrid provided power to the town center for 143 hours in a real-world scenario that could have left the town without power for over 262 hours [18]. This distributed resilience architecture proves especially valuable during extreme weather events when transmission and distribution infrastructure is compromised but local resources remain operational.

The integration and aggregation of distributed resources into VPPs offers utilities an additional tool to complement traditional generation and enhance grid flexibility. While conventional power plants and transmission and distribution infrastructure remain the backbone of grid reliability, VPPs provide complimentary support services by dynamically shifting functions based on real-time grid conditions, improving overall asset utilization across the system. Their relatively rapid deployment timelines and ability to leverage existing customer-owned resources make VPPs a practical option for addressing near-term capacity constraints while longer-term infrastructure investments are planned and constructed. VPP operations depend on digital coordination and automated control across distributed resources, aggregators, and utilities. This distributed architecture, reliant on cloud-based platforms and internet-connected devices, introduces vulnerabilities that traditional centralized assets do not face, requiring robust cybersecurity and digital-assurance measures as these programs scale.

4 VPP ARCHITECTURE AND MARKET PARTICIPATION MODELS

No single architecture or market interface applies universally to VPPs, which operate both in vertically integrated territories, where utilities own generation, transmission, and distribution, and in deregulated regions, where retail suppliers and aggregators transact around ISO/RTO-administered wholesale markets. One useful way to organize the variation is by generalizing the relationships in terms of market participation.

DOE’s 2023 “Pathways to Commercial Liftoff: Virtual Power Plants” report gives four participation models, arranged in Figure 3 from left to right [1]. The diagram abstracts aggregator roles under the ‘VPP

provider's layer; the following text describes the four participation models represented in the figure, illustrating how VPPs can function within different utility and market structures:

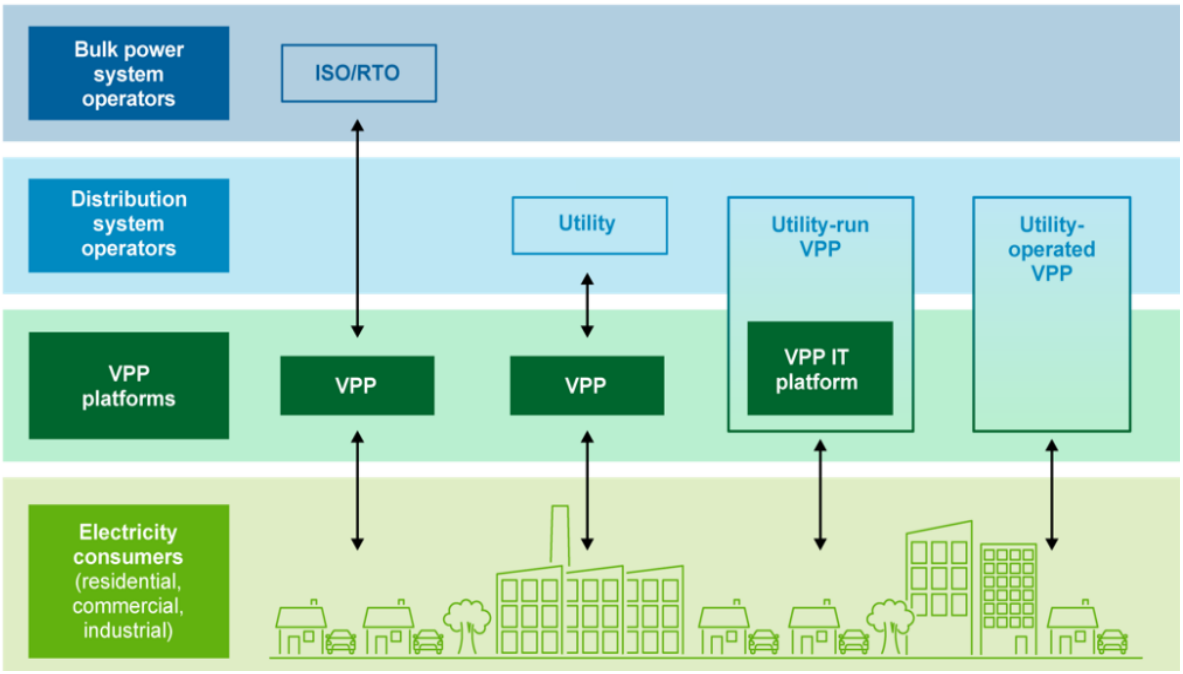

Figure 3. Four VPP Market Participation Models (left to right): Third-Party VPP at ISO/RTO Level, Third-Party VPP at Utility Level, Utility VPP with Vendor Platform, Utility VPP with Proprietary Platform [1]

- **Third-Party VPP at ISO/RTO Level**: in regions with wholesale markets, the VPP aggregator is the market participant; it enrolls customers, aggregates DERs, submits bids, receives dispatch from the ISO/RTO, and manages telemetry and settlement, subject to the applicable participation model in that market. This model depends on ISO/RTO rules and Order 2222 implementation details.
- **Third-Party VPP at Utility Level**: A VPP sells capacity or event-based load flexibility to a utility via tariff or contract; the utility is the counterparty and may, in restructured regions, also pass revenues through to customers rather than bidding directly into wholesale markets. This structure is common in vertically integrated territories and in utility demand-side portfolios.
- **Utility VPP with Vendor Platform**: The utility operates the VPP program and customer relationship while a vendor provides the orchestration platform; dispatch targets local or bulk-system needs, and wholesale participation occurs only where permitted by market rules.
- **Utility VPP with Proprietary Platform**: The utility operates and owns the VPP information technology (IT) stack and program operations; customer enrollment, telemetry, dispatch, measurement, and verification are integrated into utility systems, with optional wholesale market interfacing depending on jurisdiction.

The existence of these distinct participation models underscores the fact that VPP architecture is not monolithic. Market participation options range from aggregator-mediated wholesale market resources to vertically integrated utility programs and utility direct control VPPs. The choice of model depends on local regulatory frameworks, utility structure, and the services sought; energy, capacity, ancillary services, or resilience. Therefore, system reliability and security frameworks should consider multiple

participation pathways rather than a single “one size fits all” approach. The system overview in Section 4.1 presents a generalized DOE architecture for VPPs.

4.1 VPP System Overview: DERs, Aggregators, and Grid Interfaces

In many cases, VPPs operate through a multi-stakeholder architecture that bridges DERs with grid operators through sophisticated platform intermediaries. As depicted in Figure 4 below, this structure enables the transformation of thousands of customer-sited behind-the-meter resources into dispatchable grid assets through digital coordination across four distinct operational levels: Consumer, VPP Provider, Distribution System Operator, and Bulk Power System Operator.

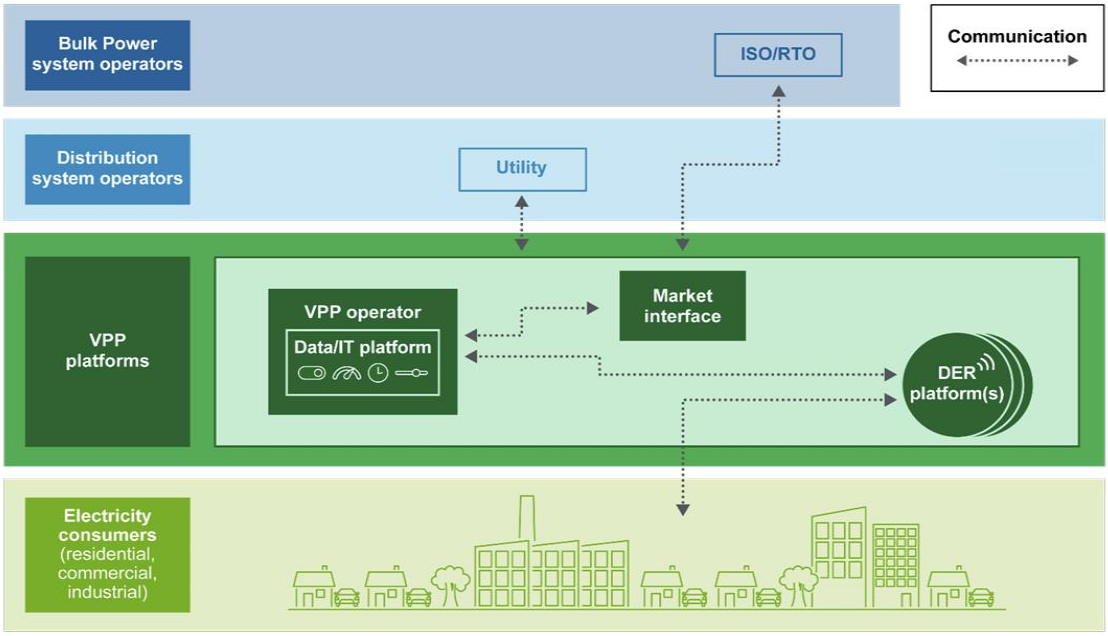

Figure 4: VPP Operational Model from the DOE 2023 Pathways to Commercial Liftoff Report [1]

The north–south communication conduits connecting the VPP Provider layer to Distribution and Bulk Power layers are logical choke points and cross-domain trust boundaries; they merit explicit hardening, monitoring, and redundancy comparable to medium-impact BES Cyber Systems. Additional explanation on this is expanded in section 5.1.1.

4.1.1 Electricity Consumers Layer

At the foundation, residential, commercial, and industrial electricity consumers host the physical distributed energy resources that form VPP capacity. These resources remain under customer ownership and primarily serve on-site energy needs while providing grid services as a secondary function. Common DER types enrolled in VPPs include:

- Residential smart thermostats controlling HVAC systems (historically the most common VPP resource)
- Commercial and industrial equipment with flexible load capabilities
- Behind-the-meter battery storage systems (5-500 kWh capacity ranges)
- Electric vehicle chargers (Level 2 and direct current fast charging)
- Rooftop solar installations with smart inverters

- Electric water heaters and pool pumps

Unlike traditional power plants, these resources are distributed across thousands of individual properties, each with distinct operational constraints, primary use cases, and participation preferences that must be preserved while delivering grid services.

4.1.2 VPP Provider Layer

The VPP Provider layer serves as the intermediary layer, employing sophisticated IT infrastructure to aggregate and orchestrate distributed resources. This layer consists of three primary components:

1. **VPP Operator with Data/IT Platform:** The centralized system that enrolls participants, forecasts available capacity, optimizes dispatch strategies, and monitors performance. Modern platforms leverage Wi-Fi, Bluetooth, and cellular connectivity to communicate with app-enabled DERs, adding new communication modes alongside existing hard-wired control systems. Communication approaches include:
    - Direct device control through manufacturer application programming interfaces (APIs) (e.g., Google Nest scheduling thermostat adjustments)
    - Behavioral signals sent to participants for manual response (e.g., OhmConnect messaging)
    - Multi-point control options (controlling EV charging through the vehicle, charger, or smart panel software)
2. **Market Interface:** The component that facilitates participation in wholesale markets, managing complex rules and requirements that vary by region. Some VPP operators maintain in-house market interface capabilities, while others contract with specialized providers to navigate wholesale market participation requirements. Three primary business models have emerged for VPP operation:
    - Utility-operated VPPs: Utilities aggregate their own customers' DERs, either through in-house operations (e.g., Green Mountain Power's battery VPP) or partnerships with third-party platforms (e.g., ConnectedSolutions operated by multiple New England utilities with EnergyHub support)
    - Manufacturer/Retailer VPPs: DER manufacturers aggregate their products across multiple utility territories (e.g., Tesla, Ford, General Motors for EVs; Sunrun, Sunnova)
    - Independent platform VPPs: Third-party aggregators enroll diverse DER portfolios across multiple manufacturers and resource types (e.g., Voltus, AutoGrid, Leap)
3. **DERs:** DERs are the decentralized generation, storage, and controllable load systems located at or near the point of consumption [19]. These resources form the physical capacity layer of VPPs and can be categorized by functionality:
    - Generation Resources:
        - Combustion generators: Natural gas and diesel generators providing reliable backup power, essential for critical infrastructure
        - Combined heat and power units: Systems that simultaneously generate electricity and thermal energy, maximizing overall efficiency
        - Fuel cells: Devices converting chemical energy into electricity with minimal emissions

- Solar photovoltaic systems: Rooftop and ground-mounted arrays that convert sunlight to electricity, increasingly paired with smart inverters for grid services beyond energy production
- Wind turbines: Small-scale wind generation systems suitable for distributed deployment

- Storage Resources:
  - Battery energy storage systems: Lithium-ion batteries dominate residential markets (e.g. Tesla Powerwall, Enphase IQ, Generac PWRcell)
  - Electric vehicle batteries: Mobile storage assets capable of managed charging and, increasingly, bidirectional power flow (vehicle-to-grid)

- Flexible Load Resources:
  - Smart thermostats: HVAC controls that adjust consumption while maintaining comfort boundaries
  - Water heaters: Thermal storage devices that can shift heating cycles based on grid signals
  - Industrial processes: Manufacturing and commercial loads with inherent flexibility in timing or intensity
  - EV chargers: Controllable charging infrastructure that can modulate power draw based on grid conditions

These resources operate in various modes such as grid-connected normal operations, islanded outages, or dynamic switching providing the foundational capacity that VPP providers aggregate into dispatchable grid services [19].

4.1.3 Distribution System Operator Layer

Distribution utilities interface with VPP providers to leverage aggregated resources for local grid management. This coordination ensures VPP dispatch aligns with distribution constraints including thermal limits, voltage boundaries, and protection settings. Although DERMS primarily support distribution-level operations, their data and control interfaces increasingly extend to bulk system coordination via VPP aggregators. Utilities increasingly deploy DERMS to:

- Balance real-time electricity demand and supply at the distribution level
- Maintain visibility into DER behavior and grid state
- Coordinate VPP dispatch with local reliability requirements
- Enable non-wires alternatives to traditional infrastructure investments

The integration of VPPs into utility IT systems enhances situational awareness and enables more sophisticated distribution grid management as DER penetration increases.

4.1.4 Bulk Power System Operator Layer

At the bulk power system level, wholesale market integration of VPP providers follows distinct pathways that vary by market structure and regional implementation. In restructured markets, VPPs can participate through multiple channels bidding directly into ISO/RTO wholesale markets as "market participant VPPs" and contracting bilaterally with utility-run platforms [1]. While FERC Order 2222 establishes the framework for DER aggregators to participate as market participants, the actual interface varies significantly. In some regions aggregators interact directly with market operators, while in others

distribution utilities serve as critical intermediaries, maintaining system reliability through review processes and operational oversight.

This layer has several key functions:

- Energy market participation for supply and demand balancing
- Ancillary service procurement (frequency regulation, spinning reserves)
- Capacity market participation for resource adequacy
- Real-time dispatch coordination with transmission constraints

FERC Order 2222, mandates that all ISOs/RTOs remove barriers to DER aggregation participation in wholesale markets. Implementation timelines vary significantly across regions [20]:

- California ISO (CAISO) has achieved partial implementation and targets completion of the rest of the order by November 2024
- SPP has proposed completion by Q3 2025
- PJM Interconnection L.L.C. has proposed completion by Q1 2026 for energy markets and DER aggregation for the 2028/2029 A Delivery Year Base Residual Auction (BRA) scheduled for December 2025 for capacity markets
- ISO-NE and NYISO have proposed completion by the end of 2026
- Midcontinent ISO (MISO) has proposed completion via a two-phase approach with phase 1 completed by 2027 and phase 2 extending to 2029-30

These varying timelines reflect differences in existing market structures, technical requirements, and regulatory frameworks across each ISO/RTO territory. Although FERC Order 2222 was issued in 2020, implementation progress remains uneven, and the protracted rollout continues to influence how quickly utilities, aggregators, and VPP providers can participate in wholesale markets. The staggered timelines also highlight ongoing challenges in aligning technical standards and coordination protocols across regions.

4.2 Interoperability and Coordination Layers

The interoperability architecture within VPPs presents unique complexity due to the need to coordinate data and control exchanges across multiple vendors, protocols, and system boundaries. At the device level, DERs communicate through diverse open protocols, and often proprietary APIs, creating significant interoperability challenges [5]. Vendor participation compounds these challenges, as utilities must integrate multiple aggregators or VPP management platforms, each with distinct data formats and communication protocols. Green Mountain Power's battery VPP illustrates this complexity, operating both a Bring-Your-Own-Device program through Virtual Peaker's platform supporting six different battery manufacturers, and a separate Energy Storage System lease program exclusively using Tesla's platform and Powerwall hardware [11]. This digital equipment mix requires utilities to maintain multiple integration points and operational procedures, increasing system complexity.

Recent standardization efforts aim to address these fragmentation challenges. The Mercury Consortium, launched in 2024, focuses on increasing the adoption of existing standards for flexible demand devices and addressing gaps in testing and certification [21]. The North American Energy Standards Board (NAESB), in partnership with DOE's Office of Electricity, is developing standardized service contracts for VPP providers to streamline utility-aggregator interfaces [22]. Additionally, the Electric Power Research Institute’s (EPRI's) FlexIT initiative is establishing technical specifications for DER discovery, visibility, and core utility-to-VPP interactions [23].

5 VPP DIGITAL ASSURANCE CONSIDERATIONS

VPPs introduce distinct security considerations that differ from traditional generation facilities. Unlike centralized plants that coordinate operations within protected industrial networks, VPPs require continuous coordination across thousands of distributed devices through internet-connected systems and public communication networks. This places critical operational coordination in adversary-accessible domains, where disruption can directly compromise VPPs' ability to deliver grid services. The DOE VPP Liftoff Report acknowledges this expanded risk, stating, "Integration of a higher volume of DERs into the grid may create a greater attack surface for malicious intruders if attackers compromise a DER vendor, VPP operator, or other party" [5].

The security architecture of VPPs is different from traditional generation facilities. First, the scale of potential entry points expands from the limited access points of traditional power plants to thousands of internet-connected devices distributed across utilities' energy consumer territories. Second, ownership complexity creates new vulnerabilities since VPP resources remain under consumer control rather than direct utility ownership, limiting the ability to enforce security standards or mandate updates. Third, communication infrastructure depends on public internet, residential Wi-Fi, and cellular networks instead of private dedicated networks used by traditional utility infrastructure. Lastly, the supply chain involves multiple device manufacturers, software platforms, aggregators, and system integrators, creating cascading trust dependencies where a security failure at any vendor could compromise the entire VPP operation. These architectural distinctions are examined in greater detail in the following section, which outlines specific threat vectors and mitigation strategies across each layer of the VPP ecosystem.

5.1 Threat Vectors and Attack Pathways in VPP Operations

The threat landscape for VPPs differs fundamentally from traditional centralized generation facilities in both scale and complexity, reflecting their distributed, digitally coordinated architecture. While conventional power plants present a limited number of highly secured access points, VPPs create an expanded attack surface spanning thousands of customer-owned devices, multiple vendor platforms, and diverse communication networks. As the North American Electric Reliability Corporation (NERC) notes in its 2023 Joint White Paper on DER Aggregators, this distributed model introduces "credible attack vectors" stemming from the inherent challenges of coordinating resources across multiple ownership boundaries and technology platforms [24].

The threat environment facing VPPs emerges from vulnerabilities that may occur in each layer of the VPP operational model:

- **Device-Level Vulnerabilities**: At the consumer layer, thousands of customer-owned DERs represent dispersed endpoints with inconsistent security implementations. These devices operate on commercial networks where security standards vary widely and are typically non-standard, firmware updates may be neglected, and default configurations often remain unchanged.
- **Platform and Aggregator Vulnerabilities**: The VPP provider layer creates high-value targets for malicious actors through centralized systems that manage vast amounts of operational data and maintain control capabilities over thousands of devices. Cloud-based infrastructures and third-party integrations expand the attack surface beyond traditional utility boundaries.
- **Communication and Protocol Vulnerabilities**: The networks connecting VPP components traverse multiple trust boundaries, from residential Wi-Fi and cellular networks to public internet infrastructure. This distributed communication architecture lacks the physical security and dedicated pathways of traditional utility operational networks. These networks have been found to use insecure protocols for communication.

Understanding these threat vectors is essential for designing and implementing appropriate defensive frameworks and maintaining the reliability that utilities and grid operators pursue with VPP resources.

5.1.1 Platform-to-Grid Conduits as High-Consequence Attack Paths

The logical north–south conduits between the VPP Provider zone and both distribution and bulk-system interfaces (illustrated in Figure 4) constitute high-leverage control surfaces. These north–south communication pathways carry command, telemetry, and market signals across trust boundaries and function as control-plane choke points for aggregated DER behavior.

Compromise or mis-operation of these conduits does not require direct exploitation of every enrolled device. Instead, adversaries or failures that gain influence over platform-level dispatch, authorization, or signaling mechanisms can induce coordinated system-level effects, including rapid net load shifts, loss of DER availability, or degradation of operator situational awareness. These conduits also present traversal opportunities, enabling lateral movement between customer-owned assets, aggregation platforms, utility systems, and market interfaces.

From a system-of-systems perspective, these pathways combine centralized leverage with distributed consequence. While exploiting them is not trivial and typically requires access to authenticated systems or upstream infrastructure, the technical mechanisms involved are well within the capabilities of sophisticated threat actors and do not rely on novel techniques. As a result, platform-to-grid conduits warrant treatment as high-consequence attack paths and should be explicitly identified, bounded, and engineered to fail safely, rather than treated as routine enterprise or application integrations. The device-, platform-, and protocol-level vulnerabilities described in Sections 5.1.2 through 5.1.4 should therefore be evaluated not only in isolation, but also in terms of how they enable access to, or manipulation of, these cross-layer conduits.

5.1.2 Device-Level Vulnerabilities

DERs (which fall in a broader category of consumer internet-of-things (IoT) devices) are being deployed and aggregated to participate in VPPs. These devices often operate on residential or commercial networks where utilities have little control or visibility. As a result, security depends on independent owners, and the devices themselves often lack secure-by-design frameworks. DER integration may not always include the communications security found in traditional utility systems, and the dynamic nature of DER operation requires automation that introduces additional cyber risk [25]. The National Laboratory of the Rockies (NLR) notes that grid-edge devices become potential points of compromise [26]. Examples of potential device-level weaknesses include:

- **Unpatched and unsupported firmware**: While firmware updates are essential for maintaining security in devices like phones and computers, it is often impractical for DER managing entities to update customer equipment due to the diversity of systems, manufacturer limitations, connectivity issues, and risk of device damage [24]. Utilities, for example, may not be able to practically push updates to customer-owned inverters or batteries, and the absence of timely patches leaves devices exposed to known exploits.
- **Multiple unregulated interfaces**: IEEE 1547-2018 requires one open standard interface, but DER equipment frequently includes additional interfaces for aggregators, owners, and original equipment manufacturer (OEM) management that are not covered by security requirements [24]. These extra interfaces create potential access points that adversaries can exploit, similar to a backdoor, providing pathways into the DER, local networks, and upstream systems. Current compliance frameworks cannot enforce controls such as certificate management or private-key protection across the diverse fleet of customer-owned devices.
- **Default passwords and weak authentication**: Many IoT products still ship with hard-coded or weak passwords and insecure default settings. Weak/hard-coded passwords are one of the most common avenues used to compromise IoT devices [27]. Insecure interfaces, such as APIs, also provide opportunities for attackers [27]. These deficiencies enable unauthorized access or lateral access across home networks, particularly when customers fail to change default credentials.

- **Insecure update mechanisms and outdated components**: Devices with insecure update processes risk installing malicious or unauthorized firmware. Using legacy or third-party components can introduce vulnerabilities that increase the attack surface. Users often fail to update devices promptly, which allows known exploits to occur [27].
- **Lack of network isolation**: Small DER devices often share Wi-Fi (or other home networks) with consumer electronics. The National Cybersecurity Center of Excellence (NCCoE) notes that these information exchanges rely on IoT devices that lack communications security [25], and NERC cautions that insufficient network segmentation allows cyber-attacks to spread across multiple systems [24]. Without separate security zones, an attacker who compromises a smart thermostat or consumer router could potentially pivot into DER controls.

5.1.3 Platform and Aggregator Vulnerabilities

VPP aggregators and DER management systems control potentially thousands of distributed devices and could present as high-value targets. VPP architecture and the hardware/software that enable the value of VPP utilization also increase the attack surface and introduce dependencies on supply chain software and third-party services. Key platform-level vulnerabilities include:

- **Remote access and authentication weaknesses**: Utilities, aggregators, and OEMs require remote access to DERs and gateways for firmware updates or configuration changes. Remote access capability becomes a credible attack vector [24]. Attackers may exploit misconfigured or unpatched controls. Improperly implemented remote access can lead to unauthorized external access, man-in-the---middle attacks, and loss of trust [24].
- **Supply -chain and software vulnerabilities**: VPP platforms aggregate operational data from thousands of devices and depend on software and firmware supplied by multiple vendors. A successful attack could allow an adversary to manipulate control signals or encrypt data for ransom. The DOE highlights the threat of sophisticated supply chain compromises, such as the SolarWinds attack, in which backdoor code was inserted into widely used network- management- software [28]. This demonstrates that advanced adversaries have exploited supply chain weaknesses to insert malicious code into legitimate software.
- **API and integration vulnerabilities**: VPPs must interface with many DER technologies, utility systems, and third-party services. Insecure or insufficiently authenticated APIs can expose control functions. Fortinet warns that insecure interfaces allow attackers to compromise devices via web or mobile APIs [27].
- **Physical security vulnerabilities.** NERC notes that wired Ethernet and fiber-optic networks can be compromised through physical access or device vulnerabilities at the site of the DER endpoint [24]. In some cases, even private networks use virtual private networks (VPNs) over the internet and therefore remain exposed if physical access controls are weak. Distribution systems often rely on fuse-based protection and lack robust security measures, exposing attack surface to tamper with network cabling or install rogue devices at poles and aggregation junctions [24].

5.1.4 Communication and Protocol Vulnerabilities

VPP operations depend on communications that span residential networks, cellular links, and the public internet. These heterogeneous channels introduce opportunities for interception, spoofing, and protocol exploitation. Specific concerns include:

- **Man-in-the-middle and spoofing attacks**: The DOE describes man-in-the-middle attacks where attackers intercept and falsify data communications between power grid devices like DER systems, aggregators, and SCADA systems [28]. These attacks can cause grid operators or automated systems to make incorrect decisions, either taking unnecessary actions or failing to respond to real problems, potentially leading to grid instability, equipment damage, and

widespread power outages. While the attacks require significant technical skill and network access to manipulate multiple communication points simultaneously, successful execution could result in outages.

- **Inconsistent and insecure protocols**: VPPs rely on a mix of communication standards and manufacturer proprietary protocols. In practice, differing implementations and unencrypted channels may leave gaps for attackers. The NCCoE identifies that information exchange mechanisms used for effective DER and IoT integration often lack the secure communication protocols present in traditional utility systems [25].
- **Lateral movement and segmentation failures**: DER devices could share home or business networks with less secure equipment. NERC warns that insufficiently segmented networks allow cyberattacks to spread across multiple systems and network segments [24]. The NLR DER Cybersecurity Framework also emphasizes that proper segmentation of IT and operational technology (OT) environments prevents an attack on one system from impacting the other [29, 26]. Without segmentation, a compromise of a consumer device, such as a router, could allow an attacker to pivot into DER communications and potentially reach the aggregation platform.

5.2 Historical Incidents and Emerging Threat Patterns

The following examples of real-world cyber and operational incidents demonstrate how these architectural characteristics have been exploited or exposed, whether through deliberate attacks, misconfigurations, or maintenance failures, highlighting critical security dependencies that must be considered in VPP implementation and management.

5.2.1 UK VPP Platform Breach (2024)

A United Kingdom researcher discovered a vulnerability within commonly used VPP software [30]. They found that the system's authentication tokens were signed with a 512-bit RSA key, which could be easily factored and compromised. By exploiting this weakness, they generated administrative credentials and the ability to access approximately 60,000 installed systems (including solar panels and batteries), representing ~200 MW of aggregated capacity across 40,000 homes. The VPP software company responded by upgrading its cryptographic key and tightening access controls. This case demonstrates that weak cryptographic implementations in an aggregator's API can permit unauthorized access on a large scale.

5.2.2 DER Monitoring Device Compromise (May 2024):

In May 2024, a cyberattack exploited known vulnerabilities in remote monitoring devices at ground-mounted solar facilities across Japan, converting them into a botnet for internet banking fraud scams [31]. Despite the remote monitoring device vendor having identified and released patches for security vulnerabilities in the software between 2021 and 2023, operators failed to apply these critical updates and continued operating the vulnerable devices with direct internet connections. The attackers installed backdoors on the monitoring systems, which ultimately caused no direct damage to the solar plants but would have enabled them to attack the plants if that had been the goal. This demonstrates how internet-connected energy infrastructure can be weaponized when basic security maintenance is neglected. VPPs can be exploited in ways similar to those used to target critical energy infrastructure operations.

5.2.3 California Heat Wave Response (September 2022)

During a severe heat wave, CAISO relied on distributed storage to avert rolling blackouts [32]. Tesla's VPP pilot with utility Pacific Gas & Electric included more than 4,500 participants and delivered up to 33 MW of peak power, including 31 MW on September 6, 2022 [32]. The state also sent emergency text messages to about 27 million residents, reducing demand by roughly 2,000 MW

within thirty minutes. Despite the success in executing response, some areas experienced unnecessary outages due to miscommunication with local utilities [33]. This highlights how successfully distributed dispatch depends on clear, timely communications among operators, utilities and customers.

5.2.4 Viasat KA-SAT (February 2022):

Attackers exploited a misconfigured VPN appliance to access Viasat's KA-SAT network and used legitimate management commands to overwrite flash memory data on thousands of connected modems, rendering them unable to connect to the network [34]. As a result, modems were disabled, and remote monitoring and control of about 5,800 wind turbines in Germany became unavailable. The turbines continued operating, but operators lost visibility and control. The disruption highlights how vulnerabilities in upstream communications infrastructure can compromise the reliability of DERs and underscores the need for redundant and secure communication channels.

5.2.5 SolarWinds (December 2020)

In December 2020, cyber attackers inserted malicious code into SolarWinds Orion network management updates, a network and asset management software tool used by utilities, among other critical infrastructure organizations [28]. The attackers had compromised SolarWinds' software development process months earlier in March 2020, inserting backdoor code that was then cryptographically signed by SolarWinds itself, effectively weaponizing the company's legitimate software distribution channel [28]. Through this breach, the attacker gained access to nine federal agencies and 100 private companies [28]. The breach highlighted the risk that an attacker can move laterally into critical infrastructure environments through a trusted vendor. Even organizations not directly using SolarWinds were potentially vulnerable through their service providers. This episode highlights the importance of rigorous scrutiny and validation of the software supply chain.

6 DEFENSE STRATEGIES FOR VPP DIGITAL ASSURANCE AND RESILIENCE

Defense strategies for VPP digital assurance and resilience must address the unique risks posed by distributed architectures, multi-vendor ecosystems, and the integration of thousands of customer-owned devices. Effective defense requires a layered approach that combines consequence-based assessments, system-of-systems analysis, attack path identification, and engineering mitigations.

6.1 Consequence-Based Assessments

By focusing on the highest-consequence grid services, utilities, aggregators, and VPP operators can ensure that the functions that can lead to significant grid impacts are thoroughly evaluated to identify proper controls and protections. This prioritization requires identifying which VPP services are available for a particular installation and then prioritizing which services are most critical for maintaining reliable grid operations, especially during periods of high demand, contingency events, or system stress.

Beyond technical reliability, economic impact must also be considered when allocating security resources and can help guide prioritization. VPP operations that are vital for market participation and capacity delivery should be assessed for their financial significance, ensuring that defense strategies are aligned with the highest stakes for both utilities and customers. This assessment of financial value may change depending on the VPP's operating structure (see Section 4.1). By mapping out the safety, reliability, and economic consequences of disruption or degraded performance for each critical service, organizations can: (1) justify investments in cyber-physical security controls and resilience measures; (2) drive Cyber-informed Engineering decisions in architecture and system design; and (3) create a repeatable basis for procurement, supply-chain choices, and continuous improvement of VPP defense planning.

6.1.1 Prioritizing VPP Design Practices Using NARUC's Cybersecurity Baselines

Building on the consequence-based assessment described in Section 6.1, the NARUC Cybersecurity Baselines provide a practical reference for sequencing cybersecurity design practices across VPP architectures based on operational consequence [35]. For VPP deployments, the application of these baselines must account for characteristics such as distributed control, reliance on customer-owned assets, and coordination across multiple organizations.

The tiers below provide an example of a consequence-based prioritization overlay to help VPP stakeholders sequence implementation; they are not part of NARUC's official structure. **This consequence-based tiering is provided for planning and illustration purposes only and does not modify or replace the underlying NARUC Cybersecurity Baselines or any applicable regulatory obligations.**

Example tier definitions (consequence-based):

- **Tier 1 – Severe Grid Impact:** Absence or failure of this baseline could directly disrupt power delivery, cause loss of DER dispatch control, or degrade real-time situational awareness—potentially leading to grid instability, safety issues, or cascading operational failures.
- **Tier 2 – Moderate Grid Impact:** Absence would not immediately destabilize the grid but would degrade reliability, extend recovery time, or reduce resilience during abnormal operations or incident response.
- **Tier 3 – Limited Grid Impact:** Absence would primarily affect compliance, administrative processes, or long-term cybersecurity posture, with little direct effect on near-term grid operations.

Appendix A provides a table illustration on how selected NARUC baseline controls can be organized by consequence to guide VPP secure design and sequencing.

6.2 System-of-Systems Analysis

Effective VPP security requires a comprehensive system-of-systems analysis that maps the complex interdependencies between aggregation platforms, DERs, and grid interfaces. By developing detailed architectural diagrams, stakeholders can visualize how each component interacts and where vulnerabilities may exist. This mapping is crucial for identifying dependencies that could become single points of failure, such as critical communication links or centralized control systems. It is also key to identifying touchpoints across different stakeholders.

Communication pathway dependencies must be scrutinized to ensure that the VPP can withstand disruptions or targeted attacks. Redundancy should be built into network architectures wherever possible, minimizing the risk that a single compromised channel could jeopardize the entire VPP operation. This includes evaluating the reliability of public internet and cellular networks, as well as the proprietary protocols used to connect DERs and aggregators. Additionally, system-of-systems analysis should extend to third-party integration points and supply-chain dependencies. Since VPPs often rely on external vendors for software platforms, device firmware, and market interfaces, vulnerabilities in these third-party systems can have cascading effects on overall security. This analysis should also account for organizational changes among service providers, such as mergers, acquisitions, or shifts in subcontractors, which may introduce new risks or alter data handling practices. Risks from dynamics in owner-operators and potential adversarial influence of both DER assets and the supply chains on which they depend are emerging areas of research, motivating modeling efforts at Idaho National Laboratory (INL) in capabilities such as TOPGEAR [36].

Service-level agreements (SLAs) should be carefully reviewed to understand security and performance obligations, incident response expectations, and data ownership or retention policies that could expose sensitive operational or customer information. Particular attention should be given to the risk of data exposure through shared platforms, cloud integrations, or vendor analytics systems, as even non-malicious data sharing can inadvertently increase the attack surface. A thorough cascading effect analysis is necessary to understand how disruptions in one part of the VPP ecosystem, such as a failure in the aggregator platform or a widespread device compromise, could propagate across interconnected systems. This analysis enables stakeholders to implement safeguards that prevent localized incidents from escalating into broader grid reliability threats.

Regular assessments of vendor security practices and contractual requirements can help mitigate risks associated with supply-chain and integration dependencies. This includes embedding cybersecurity and resilience requirements directly into requests for proposals (RFPs) and procurement language, ensuring that vendors are contractually obligated to meet baseline security and reporting standards. The CSDET Procurement, Contracting, and Supply Chain Risk Management Guide provides practical guidance to support these efforts, enabling organizations to standardize expectations for secure design, patch management, data protection, and vendor accountability throughout the supply chain [37].

6.3 Attack Path Analysis

Understanding and anticipating attack paths is a cornerstone of proactive defense for VPP operations. Through adversary targeting assessments, organizations can evaluate potential high-consequence scenarios, such as coordinated manipulation of DERs or tampering with market signals, to understand how these actions could compromise operational integrity.

Attack-path analysis must extend to cyber-physical vectors, instances where digital intrusions may result in physical impacts on grid stability or equipment integrity. For example, a coordinated cyberattack on DER control systems could produce localized load imbalances or even physical damage to grid infrastructure if protection functions are also compromised. By correlating these potential attack paths with the enabling functions and devices identified during consequence-based defense analysis, operators can determine how an adversary could reach the most consequential functions and apply appropriate mitigations. Simulating these scenarios provides a quantitative understanding of both likelihood and consequence, allowing operators to align mitigations with potential system impacts. This approach ensures that cyber and physical defense measures are prioritized by consequence, directing resources toward protecting functions whose failure would have the most significant operational or economic effects on VPP and grid reliability.

Organizations should maintain a comprehensive catalog of potential entry points across the VPP ecosystem, including cloud platforms, APIs, device-level vulnerabilities, and remote-access mechanisms. Because VPPs operate across diverse communication networks and ownership boundaries, sustained visibility into all possible intrusion avenues, including those associated with customer-owned devices and third-party integrations, is essential for continuous risk assessment and response readiness.

6.4 Cyber-Informed Engineering

Cyber-Informed Engineering (CIE) empowers engineers and technicians to implement engineering controls to help mitigate cyber-induced risk [38]. One illustrative example of an engineered control in VPP operations is the use of ramp rate and operational boundary enforcement at the device and system levels. Ramp-rate enforcement constrains how quickly DERs can increase or decrease their output, while operational-boundary limits define the maximum allowable voltage, frequency, or power setpoints an asset can reach. By embedding these limits directly in inverter firmware or local controllers, equipment behavior remains physically bounded even if compromised commands come through the network or an aggregator platform. This engineered constraint prevents destabilizing power swings, reduces the

potential for cascading grid impacts, and ensures that system responses stay within safe engineering tolerances.

In practice, these controls act as fail-safe mechanisms that maintain grid stability regardless of network state, software condition, or external influence. When integrated, they protect critical grid functions, including frequency regulation, voltage support, and capacity delivery, by ensuring that no single cyber event can push the system beyond its designed safety margins.

While ramp-rate and boundary enforcement represent one application, the underlying principle extends broadly: CIE focuses on engineering-out cyber-induced risk by designing physical and logical barriers that keep systems bounded, predictable, and recoverable, even under adverse or compromised conditions.

For help identifying and prioritizing engineered controls specific to your environment, INL offers several publicly available tools that can help utilities, aggregators, and VPP operators operationalize CIE principles:

- CIEMAT (CIE for Microgrids) – supports consequence-based risk assessment and engineering control identification for microgrid systems [39].
- CIEBAT (CIE for Battery Energy Storage Systems) – supports consequence-based risk assessment and engineering control identification for battery energy storage applications [40].

Both tools are available through the Idaho National Laboratory Software Store and are free for public use.

7 DIGITAL ASSURANCE RECOMMENDATIONS

The best practices that follow are organized by VPP architectural layer to reflect how cyber and operational risk manifests across distributed assets, centralized platforms, and the communication pathways that connect them. While these practices apply across all VPP configurations, their prioritization should be informed by consequence-based assessments as described in Section 7.1, with highest emphasis placed on functions whose disruption could directly affect grid reliability, market operations, or emergency response. Together, the device-level, platform-level, and communication-focused practices establish a layered defense strategy that addresses both localized vulnerabilities and the system-level attack paths created by VPP aggregation, enabling stakeholders to reduce the likelihood that individual failures or compromises propagate into high-consequence grid impacts.

7.1 Device-Level Operational Practices

DERs deployed at the grid edge often operate beyond direct utility control and under varied ownership models. In this environment, weak device configurations or unmaintained firmware can create cyber-physical pathways into higher-level control networks. At VPP scale, compromise of many “small” assets can produce system-level consequences, including loss of dispatch, degraded visibility, and increased risk of coordinated attacks.

Device-level operational practices should be embedded in procurement requirements, commissioning procedures, and ongoing operations and maintenance. Applied consistently, these device-level practices reduce the likelihood that compromise at the edge will translate into high-consequence impacts on VPP grid services.

Recommended device-level operational practices include:

- **Secure configuration management** – Enforce manufacturer security settings on installation; disable unused services and interfaces; verify firmware authenticity and integrity prior to deployment; document final configurations as the operational baseline.

- **Transparency and supply-chain assurance** – Request Software and Hardware Bills of Materials (SBOMs/HBOMs) from OEMs; require vendors to attest to secure development and update practices; record use of third-party code, libraries, and cloud services that support device operation.
- **Prohibit direct device-to-OEM communications** – Prohibit uncontrolled direct communications between devices and OEM infrastructure. Route updates, telemetry, and remote support through aggregator or utility gateways operated under U.S. jurisdiction or within a demilitarized zone (DMZ), enabling monitoring, policy enforcement, and compliance with applicable restrictions.
- **Coordinated patching and firmware management** – Track Cybersecurity and Infrastructure Security Agency (CISA) and vendor advisories; plan and execute patching of device firmware and associated software on a routine cadence; coordinate remediation windows with aggregators and grid operators to avoid conflicts with critical operations and market obligations; maintain an inventory that reflects patch status for all DER devices.
    - **Patch validation** – After each update, verify configurations to confirm that all devices remain properly linked and no unauthorized components were introduced.
- **Credential and access hygiene** – Remove default credentials; enforce unique credentials per device or deployment; apply multifactor authentication (MFA) where technically feasible; revoke access promptly when roles or vendors change.
- **Field-equipment controls** – Restrict use of portable media; require authorization and baseline security configurations for maintenance laptops and field tools; physically secure access ports to prevent the connection of unauthorized devices.
- **Network isolation** – Segment DER controls from home or business networks; use gateways with firewalls and virtual local area networks (VLANs) to prevent lateral movement from consumer devices and other IT systems into control pathways.
- **Continuous OT monitoring without disruption** – Use passive sensors (e.g., taps or SPAN ports) to observe DER communications and behavior without inserting active components in the control path; monitor for changes in protocol use, command patterns, and device states that could indicate compromise or misoperation. Where appropriate, transmit monitoring data from sensitive networks to analysis or enterprise environments through tightly controlled paths, including unidirectional gateways (data diodes), to avoid introducing a return path into control networks.

7.2 Platform and Aggregator Operational Practices

Aggregators operate centralized control and market-interface systems that coordinate thousands of DERs. These systems form the operational "brain" of a VPP and represent a concentrated digital dependency for grid services. Because they combine command authority, real-time operational data, and market signaling, disruptions or compromise at this layer can quickly propagate to the distribution grid and affect higher-consequence services.

Recommended platform and aggregator operational practices include:

- **Vulnerability and patch management** – Apply risk-based patching to aggregator servers and APIs; validate compensating controls for deferred updates. Monitor the CISA Known Exploited Vulnerabilities (KEV) catalog and other trusted feeds [41].
- **Continuous monitoring and detection** – Tune analytics and intrusion-detection rules to recognize VPP-specific traffic patterns and abnormal DER dispatch behaviors.
- **Log collection and retention** – Enable logging of configuration changes and access events across all systems; store logs securely off-site; review routinely for anomalies.

- **Behavioral analysis** – Establish baselines of normal VPP and DER performance; integrate anomaly detection into the aggregator's monitoring systems to identify any suspicious or unknown connections.
- **Third-party validation** – Use independent organizations (e.g., national laboratories, accredited security firms, etc.) to perform authorized security assessments and, where appropriate, penetration testing of platform and aggregator environments, under defined scope and rules of engagement, to verify vendor claims and identify weaknesses that could lead to higher-consequence impacts.
- **Secure procurement and vendor oversight** – Reference INL's Procurement Guidance for Supply-Chain Risk Management to support supply chain procurement and contracting considerations [37].
- **Secure system documentation** – Maintain complete asset inventories, and network diagrams; update them after each configuration change to spot unauthorized modifications or unexpected systems on the network.
- **Supply-chain cybersecurity principles** – Apply DOE's Supply Chain Cybersecurity Principles to ensure traceable accountability throughout equipment lifecycles [42].
- **Engineering-level risk analysis** – Leverage CIE tools (e.g., CIEBAT and CIEMAT) to help identify potential risks and mitigations within grid operations.
- **Disable unnecessary services** – Remove or disable unused services, APIs, third-party integrations, and remote-support features that expand the attack surface where possible. Review interconnection studies and operational dependencies to understand how isolation or fail-safe modes will affect grid operations during a security event.
- **Cross-functional team structure** – Establish integrated teams of power-system engineers, cybersecurity specialists, OT practitioners, and platform operators with clearly defined roles, escalation paths between IT and OT, and joint response procedures. Conduct regular cross-functional training, exercises, and other practice activities involving utilities, aggregators, and key vendors to maintain operational readiness, improve stakeholder coordination, and enhance resilience.

7.3 Communication and Protocol Operational Practices

Communications are the connective tissue of a VPP and a primary digital dependency for VPP grid services. VPP traffic traverses multiple trust boundaries, from residential networks and field-area systems to public internet infrastructure and cloud services, each introducing potential points of interception, spoofing, or disruption. Communication paths and protocols should be treated as critical control surfaces - without rigorous encryption, segmentation, and monitoring, adversaries could spoof control signals or disrupt data flows, undermining both operational reliability and grid stability.

Recommended communication and protocol practices include:

- **Encrypted and authenticated channels** – Use strong, up-to-date encryption and mutual authentication for all command and telemetry channels. Manage keys and certificates as operational assets: rotate them regularly, revoke them when roles or vendors change, and avoid hard-coded or shared credentials across devices or fleets.
- **Network segmentation and isolation** – Separate IT and OT environments; place OT systems behind firewalls; disable unnecessary remote access; use VPNs or encrypted tunnels when remote connectivity is required. Limit exposure of control interfaces to only networks and partners that require access.

- **Traffic monitoring and anomaly detection** – Deploy intrusion detection on critical communication links; monitor for spoofing, replay, or timing anomalies indicative of man-in-the-middle attacks.
- **Resilient communication architecture** – Implement redundant communication paths and fail-safe modes to maintain dispatch continuity during connectivity loss or denial-of-service conditions. Plan for degraded modes of operation under denial-of-service or partial connectivity conditions, including clear rules for how DERs and aggregators should behave when communications are disrupted.
- **Procurement and component validation** – Require network and communication-equipment vendors to document all firmware update paths and remote-management interfaces; validate component authenticity and configuration prior to deployment.
- **Use standards-based protocols** – Employ protocols that natively support encryption, authentication, and access control. Avoid proprietary or opaque vendor protocols that cannot be independently validated or secured.
- **Protocol translation gateways** – When integrating legacy DERs or proprietary interfaces, implement gateways that enforce encryption and authentication consistently across all communications.

Avoid direct OEM cloud connections – Prohibit direct communication from DER devices to manufacturer cloud services. All operational data should flow through aggregator-controlled or utility-controlled infrastructure within approved network perimeters, where monitoring, policy enforcement, and regulatory requirements can be applied.

8 CONCLUSIONS AND NEXT STEPS

This report examines the architectural, operational, and digital assurance considerations that distinguish VPPs from conventional utility infrastructure. With current VPP capacity at approximately 30 GW and projections reaching 80-160 GW by 2030, these aggregations of distributed energy resources are transitioning from pilot programs to mainstream grid operations. As VPPs scale, their value increasingly depends on digital coordination across thousands of customer-owned assets, centralized aggregation platforms, and market and utility interfaces. That same architecture, however, introduces distinct operational and cybersecurity risks that differ fundamentally from those associated with traditional centralized generation.

This report demonstrates that VPP risk is not driven by any single device, platform, or protocol in isolation. Rather, risk emerges from the aggregation of many individually low-consequence assets into coordinated systems whose failure or mis-operation can produce system-level effects. In particular, the logical conduits connecting VPP platforms to distribution and bulk power system interfaces represent high-leverage control surfaces. Disruption or compromise at these points can affect dispatch integrity, situational awareness, and grid stability without requiring the compromise of large numbers of individual devices. These characteristics require utilities, aggregators, and regulators to move beyond device-centric or compliance-only security models toward approaches that explicitly consider consequence, architecture, and attack paths.

The defense strategies outlined in this report provide a practical framework for addressing these challenges. Consequence-based assessments help stakeholders identify which VPP services and functions warrant the highest levels of protection. System-of-systems analysis exposes architectural dependencies and potential single points of failure across organizational and technical boundaries. Attack-path analysis shifts attention from abstract vulnerabilities to credible sequences of actions that could lead to operational impact. Cyber-Informed Engineering reinforces these measures by embedding physical and logical constraints that limit the consequences of cyber events, even when digital controls are degraded or

bypassed. Together, these approaches support a layered, resilient defense posture aligned with how VPPs actually operate.

Recognized cybersecurity baselines, including those developed by NARUC, can play a valuable role when applied as sequencing tools rather than static checklists. When combined with consequence-based prioritization, these baselines help utilities and aggregators focus limited resources on the controls that matter most for grid reliability, while avoiding unnecessary burden on lower-impact functions. This approach is especially important given the diversity of VPP participation models, ownership structures, and regulatory environments shaped by ongoing implementation of FERC Order 2222.

Looking ahead, advancing secure and resilient VPP deployment will require continued coordination across technical, regulatory, and organizational domains. Priorities include improving interoperability standards for DERs and aggregator interfaces, embedding cybersecurity and resilience requirements into procurement and contracting practices, and expanding the use of engineering-based safeguards that bound system behavior under adverse conditions. Continued analysis of real-world VPP operations, incidents, and near misses will also be essential to refining risk models and informing future guidance.

When designed and operated with appropriate attention to architecture, consequence, and engineered resilience, VPPs can enhance grid flexibility and reliability without introducing unacceptable risk. The frameworks and practices presented in this report are intended to support utilities, aggregators, regulators, and technology providers as they scale VPP deployments in a manner that strengthens, rather than undermines, the security and reliability of the U.S. electric grid.

Appendix A – Prioritization of NARUC Cybersecurity Baselines for VPPs

Disclaimer: The baselines selected below are illustrative and not exhaustive and the consequence-based tiering (outlined in Table 1) is provided for planning and illustration purposes only and does not modify or replace the underlying NARUC Cybersecurity Baselines or any applicable regulatory obligations. They demonstrate how consequence-based prioritization can guide VPP-specific design and sequencing while maintaining alignment with NARUC's full set of baselines.

Table 1. Illustrative Prioritization of NARUC Cybersecurity Baselines for Virtual Power Plants

Priority Tier	NARUC Baseline Control	Relevant VPP Function	Potential Grid Consequence if Absent in a VPP Environment
Tier 1 – High Impact	Prohibit Connection of Unauthorized Devices	DER field devices and maintenance interfaces	If unmanaged media or devices are connected, malware could enter control networks, enabling remote manipulation of DER controls, substation equipment, or aggregator systems - potentially causing localized or cascading grid disruptions.
	Strong and Agile Encryption	Secure command and telemetry between DERs, aggregators, and utilities	Weak or outdated encryption could allow interception or spoofing of operational data and control signals, leading to false telemetry, unauthorized switching, or loss of grid coordination.
	Network Segmentation	Isolation of aggregator control systems from IT and public networks	Lack of segmentation allows lateral movement from compromised IT assets into DER control environments, creating a direct path to disrupt real-time grid operations.
Tier 2 – Moderate Impact	Mitigating Known Vulnerabilities	Patch and mitigate high-risk flaws on aggregator and DER interfaces	Closes known exploit paths; important for resilience though typically less acute than access /segmentation failures.
	Log Collection	Collect and securely store time-synchronized security and access logs for IT/OT assets.	Without active intrusion detection systems, suspicious activity may go undetected, and investigators may lack forensic evidence, delaying detection and containment of compromise.
	Detecting Relevant Threats and Tactics and Techniques	Tune threat detection to VPP protocols and workflows	Absence of tuned detection limits awareness of attacks on aggregator-DER communications, increasing

			dwell time and incident severity but not causing instant grid instability.
Tier 3 – Lower Impact	Asset Inventory	Maintain visibility of all aggregator nodes, DER gateways, and supporting systems	Missing or outdated inventories hinder vulnerability management and decommissioning, increasing exposure but with limited direct operational consequence.
	Vendor/Supplier Cybersecurity Requirements	Procurement and lifecycle management for DER and aggregator vendors	Lack of supplier cybersecurity criteria weakens long-term supply-chain integrity but does not directly affect short-term grid stability.

Page intentionally left blank

References

[1] J. Downing, N. Johnson, M. McNicholas, D. Nemtzow, R. Oueid, J. Paladino and E. B. Wolfe, "Pathways to Commercial Liftoff: Virtual Power Plants," U.S. Department of Energy, Washington, DC. , 2023.

[2] S. Bieler, C. Goldenberg, A. McEvoy, K. Stephan and A. Walmsley, "Aggregated Distributed Energy Resources in 2024: The Fundamentals," National Associaton of Regualtory Utility Commissioners, July 2024. [Online]. Available: https://connectedcommunities.lbl.gov/sites/default/files/2024-07/NARUC_ADER_Fundamentals_Interactive.pdf.

[3] A. Peskoe, "Power Over the Twenty-First Century Electric Grid," Kleinman Center for Energy Policy, 10 April 2018. [Online]. Available: https://kleinmanenergy.upenn.edu/research/publications/power-over-the-twenty-first-century-electric-grid/.

[4] ScottMadden, Inc, "The energy industry update: The Waiting (Is the Hardest Part) - Volume 23, Issue 2: Virtual Power Plants," ScottMadden, Inc., 2023. [Online]. Available: https://publications.scottmadden.com/energy-industry-update-v23-i2/virtual-power-plants.

[5] S. Razdan, J. Downing and L. White, "Pathways to Commerical Liftoff: Virtual Power Plants 2025 Update," January 2025. [Online]. Available: https://www.smartenergydecisions.com/wp-content/uploads/2025/04/liftoff_doe_virtualpowerplants2025update.pdf.

[6] B. Martucci, "Data center demand drives 33% jump in VPP deployments: Wood Mackenzie," Utility Dive, 22 September 2025. [Online]. Available: https://www.utilitydive.com/news/data-center-vpp-virtual-power-wood-mackenzie/760731.

[7] Federal Energy Regulatory Comission (FERC), "FERC Order No. 2222: Fact Sheet," FERC, 28 September 2020. [Online]. Available: https://www.ferc.gov/media/ferc-order-no-2222-fact-sheet.

[8] Van Ness, Feldman, LLP, "FERC Issues Order No. 2222 to Increase Participation of Distributed Energy Resource Aggregations in Organized Markets," Van Ness, Feldman, LLP, 22 September 2020. [Online]. Available: https://www.vnf.com/ferc-issues-order-no-2222-to-increase-participation-of-distributed-energy-resource-aggregations-in-organized-markets.

[9] "SB24-218 Modernize Energy Distribution Systems," 22 May 2024. [Online]. Available: https://leg.colorado.gov/bill_files/45585/download.

[10] North Carolina Clean Energy Technology Center (NCCETC) and Smart Electric Power Alliance (SEPA) , "New Report Unveils How States and Utilities Are Advancing Virtual Power Plants in 2024," North Carolina Clean Energy Technology Center (NCCETC) , 10 February 2025. [Online]. Available: https://nccleantech.ncsu.edu/2025/02/10/nccetc-and-sepa-release-new-report-detailing-2024-state-and-utility-actions-on-vpps-and-supporting-ders/.

[11] K. Brehm and M. Tobin, "Virtual Power Plant Flipbook," Virtual Power Plant Partnership (VP3) and Rocky Mountain Institute (RMI), June 2024. [Online]. Available: https://rmi.org/wp-content/uploads/dlm_uploads/2024/06/VP3_flipbook_v1.1.pdf. [Accessed 8 September 2025].

[12] Energy Hub, "The edge DERMS platform that maximizes your energy resources.," Energy Hub, [Online]. Available: https://www.energyhub.com/. [Accessed September 2025].

[13] CPower Energy, "Enabling a Customer-Powered Grid through virtual power plants and DER monetization," CPower Energy, [Online]. Available: https://cpowerenergy.com/. [Accessed 8 September 2025].

[14] B. Martucci, "Virtual power plants helped save the grid during heat dome," Utility Dive, 16 July 2025. [Online]. Available: https://www.utilitydive.com/news/virtual-power-plants-helped-save-the-grid-during-heat-dome/753247/.

[15] Voltus, "DER energy platform for demand response and grid participation.," Voltus, [Online]. Available: https://www.voltus.co/. [Accessed 8 September 2025].

[16] M. Allsup, "Is this the tipping point VPP providers have been waiting for?," Latitude Media, 15 August 2025. [Online]. Available: https://www.latitudemedia.com/news/is-this-the-tipping-point-vpp-providers-have-been-waiting-for/. [Accessed 8 September 2025].

[17] Federal Energy Regulatory Commission (FERC), "FERC Press Conference | June 26, 2025," YouTube, 26 June 2025. [Online]. Available: https://www.youtube.com/watch?v=lbdMePUPZe0. [Accessed 8 September 2025].

[18] J. Leader and J. Handley, "Case Study: Hurricane Helene - Hot Springs Microgrid," Smart Electric Power Alliance (SEPA), March 2025. [Online]. Available: https://sepapower.org/resource/case-study-hurricane-helene-hot-springs-microgrid/.

[19] PowerSecure, "A Comprehensive Guide to Distributed Energy Resources," PowerSecure, Inc., Southern Company, [Online]. Available: https://powersecure.com/a-comprehensive-guide-to-distributed-energy-resources. [Accessed 8 September 2025].

[20] Federal Energy Regulatory Commission (FERC), "FERC Order No. 2222 Explainer: Facilitating Participation in Electricity Markets by Distributed Energy Resources," FERC, 25 September 2025. [Online]. Available: https://www.ferc.gov/ferc-order-no-2222-explainer-facilitating-participation-electricity-markets-distributed-energy.

[21] Kraken, "Mercury – shaping the future of consumer device interoperability," Kraken, [Online]. Available: https://kraken.tech/mercury. [Accessed 8 September 2025].

[22] North American Energy Standards Board (NAESB), "NAESB Releases Standard Distribution Grid Services Contract [Press Release]," 9 January 2025. [Online]. Available: https://www.naesb.org/pdf4/010925press_release.pdf. [Accessed 8 September 2025].

[23] Electric Power Research Institute (EPRI), "FLEXIT: Flexible Interoperable Technologies Initiative: VPP/DER Registry and Integration Interface," 7 May 2025. [Online]. Available: https://www.epri.com/research/products/000000003002031278. [Accessed 8 September 2025].

[24] North American Electric Reliability Corporation (NERC), "Privacy and Security Impacts of DER and DER Aggregators Joint SPIDERWG/SITES White Paper," September 2023. [Online]. Available: https://www.nerc.com/comm/RSTC_Reliability_Guidelines/JointWhitePaper_PrivacyAndSecurityImpactsOfDERAggregators.pdf. [Accessed 8 September 2025].

[25] National Cybersecurity Center of Excellence (NCCOE), "Securing Distributed Energy Resources," February 2022. [Online]. Available: https://www.nccoe.nist.gov/sites/default/files/legacy-files/es-iiot-fact-sheet.pdf. [Accessed 8 September 2025].

[26] National Renewable Energy Laboratory, "Cybersecurity and Distributed Energy Resources," April 2020. [Online]. Available: https://www.nrel.gov/docs/fy20osti/76307.pdf. [Accessed 8 September 2025].

[27] Fortinet, "Overview: What Makes An IoT Device Vulnerable?," Fortinet, [Online]. Available: https://www.fortinet.com/resources/cyberglossary/iot-device-vulnerabilities. [Accessed 8 September 2025].

[28] DOE's Office of Cybersecurity, Energy Security, and Emergency Response (CESER) and the Office of Energy Efficiency and Renewable Energy (EERE), "Cybersecurity Considerations for Distributed Energy Resources on the U.S. Electric Grid," October 2022. [Online]. Available: https://www.energy.gov/sites/default/files/2022-

10/Cybersecurity%20Considerations%20for%20Distributed%20Energy%20Resources%20on%20the%20U.S.%20Electric%20Grid.pdf. [Accessed 8 September 2025].

[29] National Renewable Energy Laboratory (NREL), "Distributed Energy Resource Cybersecurity Framework (DER-CF) [Web Tool]," NREL, [Online]. Available: https://dercf.nrel.gov/. [Accessed September 2025].

[30] J. Hertz, "Virtual Vulnerability: How a Hacker Infiltrated a VPP," EE Power, 5 September 2024. [Online]. Available: https://eepower.com/tech-insights/virtual-vulnerability-how-a-hacker-infiltrated-a-vpp/. [Accessed 8 September 2025].

[31] E. Bellini, "What happens when malware hits PV systems," PV Magazine, 6 November 2024. [Online]. Available: https://www.pv-magazine.com/2024/11/06/what-happens-when-malware-hits-pv-systems/. [Accessed 8 September 2025].

[32] J. St. John, "PG&E is Testing Different Flavors of Virtual Power Plant," Canary Media, 20 February 2023. [Online]. Available: https://www.canarymedia.com/articles/grid-edge/pg-e-is-testing-different-flavors-of-virtual-power-plant. [Accessed 8 September 2025].

[33] E. Hoven, "Heat wave tests state's communications strategy," CalMatters, 8 September 2022. [Online]. Available: https://calmatters.org/newsletters/whatmatters/2022/09/california-heat-wave-communications-strategy/. [Accessed 8 September 2025].

[34] J. A. Guerrero-Saade and M. v. Amerongen, "AcidRain | A Modem Wiper Rains Down on Europe," SentinalLabs, 31 March 2022. [Online]. Available: https://www.sentinelone.com/labs/acidrain-a-modem-wiper-rains-down-on-europe/. [Accessed 8 September 2025].

[35] U.S. Department of Energy and the National Association of Regulatory Utility Commissioners, "Cybersecurity Baselines for Electric Distribution Systems and DER," January 2025. [Online]. Available: https://www.energy.gov/sites/default/files/2025-01/Cybersecurity%20Baselines%20for%20Electric%20Distribution%20System%20Interim%20Implementation%20Guidance.pdf. [Accessed 27 October 2025].

[36] G. Weaver, D. A. Eisenberg and E. Stewart, "Evaluating Direct and Indirect Influence on EV Charging Stations Across the US," in *2025 IEEE PES Grid Edge Technologies Conference and Exposition*, San Diego, 2025.

[37] E. M. Stewart, R. V. Stolworthy, S. Gribbin, T. L. Briggs and M. J. Culler, "Securing Digital Energy Infrastructure: Procurement, Contracting, and Supply Chain Risk Management Guidance," October 2024. [Online]. Available: https://inldigitallibrary.inl.gov/sites/STI/STI/Sort_133245.pdf.

[38] DOE Office of Cybersecurity, Energy Security, and Emergency Response, "National Cyber-Informed Engineering Strategy," June 2022. [Online]. Available: https://www.energy.gov/sites/default/files/2022-06/FINAL%20DOE%20National%20CIE%20Strategy%20-%20June%202022_0.pdf. [Accessed 27 October 2025].

[39] V. L. Wright, B. R. Lampe, S. D. Chanoski, J. P. Meng and E. M. Stewart, "CIEMAT: Cyber-Informed Engineering Microgrid Analysis Tool [Software]," Idaho National Laboratory, 24 August 2024. [Online]. Available: https://www.osti.gov/biblio/code-144556. [Accessed 21 November 2025].

[40] B. R. Lampe, V. L. Wright, R. V. Stolworthy and E. M. Stewart, "Cyber-informed Engineeing Battery Analysis Tool [Software]," Idaho National Laboratory, 15 January 2025. [Online]. Available: https://www.osti.gov/biblio/code-149914. [Accessed 21 November 2025].

[41] Cybersecurity and Infrastructure Security Agency (CISA), "Known Exploited Vulnerabilities Catalog," U.S. Department of Homeland Security, [Online]. Available: https://www.cisa.gov/known-exploited-vulnerabilities-catalog. [Accessed 21 November 2025].

[42] DOE Office of Cybersecurity, Energy Security, and Emergency Response (CESER), "Supply Chain Cybersecurity Principles," U.S. Department of Energy, [Online]. Available: https://www.energy.gov/ceser/supply-chain-cybersecurity-principles. [Accessed 21 November 2025].