VedeniEnergy
Plugged Into The Energy Industry

AUGUST 2025 - IV

IT/OT Convergence

for Smarter Grid Operations and Cybersecurity

WHITEPAPER

VedeniEnergy
Plugged Into The Energy Industry

+1 463-266-4496
www.vedeni.energy
info@vedeni.energy
Whitestown, in 46075, US.

Introduction

Bridging IT and OT for a Smarter, Safer Grid

The modern electric grid is undergoing a digital transformation that blurs the traditional lines between information technology (IT) and operational technology (OT). IT/OT convergence in the power industry means combining the data-driven, connected world of IT systems with the equipment and controls of OT systems that maintain the flow of electricity. For years, utility OT systems—such as substation controls, SCADA networks, protective relays, and energy management systems—worked separately from enterprise IT networks. OT priorities focused on real-time control, safety, and reliability, often using proprietary or specialized technologies. Meanwhile, IT systems managed business processes, data analysis, and communications on separate platforms. Today, however, utilities are increasingly integrating these areas to create a more intelligent and more resilient smart grid. By merging IT and OT, power companies can utilize vast amounts of operational data in real-time, apply advanced analytics and AI, and control grid assets with greater accuracy. This IT/OT integration offers significant benefits, ranging from predictive maintenance that prevents outages to dynamic management of renewable energy sources. At the same time, this convergence presents technical and organizational challenges, especially in cybersecurity. A connected, digital grid must be protected against cyber threats without jeopardizing the reliability and safety of critical infrastructure.

This white paper explores how IT/OT convergence is transforming grid operations and security. It offers an overview of the entire ecosystem affected by this trend, discusses key drivers and use cases, examines technical solutions such as common data standards and new network architectures, reviews applicable U.S. regulatory requirements, and considers how to balance innovation with the fundamental need for a reliable, safe, and secure electric power system. While focusing on the U.S. context, we also include global examples to illustrate how countries worldwide are adopting IT/OT convergence in their electric grids. The narrative is designed for energy industry professionals, offering a detailed yet high-level overview of this crucial aspect of grid modernization.

The Evolving Grid and the Convergence of IT and OT

In traditional utilities, IT and OT operated in separate domains. OT includes field systems and control technologies that directly monitor and influence physical grid equipment. This involves devices such as sensors, relays, programmable logic controllers, and SCADA (Supervisory Control and Data Acquisition) systems, which manage power plants, transmission lines, and distribution networks. These OT systems focus on deterministic responses, uptime, and safety, for instance, instantly opening a circuit breaker if a fault is detected on a line. They were typically closed systems, utilizing specialized hardware and communication protocols, and were managed by engineers and operators. Conversely, IT encompasses the computing and networking infrastructure supporting business operations, including corporate data centers, enterprise software, databases, customer information systems, and modern cloud platforms. IT handles tasks such as billing, market transactions, workforce management, and big data analytics. These systems prioritize data throughput, flexibility, and cybersecurity in protecting information confidentiality and integrity. Historically, there was little overlap: engineering groups managed OT, while the corporate IT department handled information systems. Any interaction was minimal and tightly controlled.

Several factors have driven a convergence of these worlds. One major force is the digitalization of the electric grid, often referred to as the smart grid revolution. Utilities are installing millions of intelligent electronic devices and sensors across the grid, from smart meters at homes to phasor measurement units on transmission lines. These devices generate continuous streams of data about equipment status, power quality, and consumption patterns. At the same time, advanced IT capabilities, including cloud computing, IoT (Internet of Things), and AI, have undergone significant advancements. Utilities see an opportunity to leverage OT data with IT tools to enhance operational efficiency. For example, instead of manually inspecting equipment on a fixed schedule, a utility can use sensor data combined with machine learning analytics to predict which transformer is likely to fail and schedule replacement just in time. This approach to data analytics relies on IT/OT integration, where OT sensor readings must be integrated into IT data stores and analytical models to generate actionable insights. Early deployments have demonstrated their value; for instance, one large U.S. utility unified data from sensors, maintenance records, and weather feeds to train an AI model for asset health. As a result, it reportedly reduced transformer failures by nearly half through predictive maintenance, saving millions in outage and repair costs each year. These successes highlight why utilities are investing in converged systems that treat information and operational technologies as a unified ecosystem.

Another key factor is the rise of distributed energy resources (DERs) and renewable power, which is transforming how the grid operates. Unlike the traditional model of one-way power flow from large central power plants, today's grid is much more dynamic and spread out. Solar panels on rooftops, wind farms, battery storage, and electric vehicles are all injecting or drawing power at the edges of the network. Managing this complexity requires tight coordination and real-time decisions that involve operational controls and higher-level optimization. IT/OT convergence enables an approach where edge devices and central systems work together in collaboration. For example, in a neighborhood with abundant solar energy, local control software (an OT function) at

a transformer might automatically adjust the voltage or activate a battery if cloud cover suddenly reduces solar output, maintaining stable service. At the same time, a cloud-based DER management platform (an IT system) can gather data from thousands of sites to predict trends and deploy resources across the region, resulting in improved efficiency and reliability. This interaction needs seamless data sharing between field controllers and enterprise systems. Integrating DERs has spurred convergence—utilities understand that only by connecting OT systems (which provide quick control at substations and feeders) with IT systems (which offer a global view and intelligence) can they balance supply and demand in real time across a complex, decentralized grid.

Cybersecurity considerations have also brought IT and OT closer together. Traditionally, OT environments were often air-gapped or isolated for safety; however, this is no longer practical or desirable. Grid operators want the ability to securely access substation systems remotely, apply patches, retrieve data for analysis, and even allow vendors to update their equipment. The flip side is that any connection between OT and IT systems creates potential pathways for cyber intrusions. High-profile incidents have highlighted this risk. In the 2015 Ukraine grid cyberattack, attackers penetrated the corporate IT networks of electric companies via phishing and then accessed the control systems, ultimately opening breakers and causing a blackout. Similarly, in 2021, a ransomware attack on a U.S. pipeline company's IT network prompted operators to halt pipeline operations as a precaution, underscoring that an IT breach can disrupt OT functionality. These examples make it clear that IT and OT security can no longer be managed separately. Utilities are unifying their cybersecurity strategies across both domains, adopting integrated cybersecurity frameworks that address converged risks. This often involves IT security teams and OT engineers working together on network defenses, monitoring, and incident response. In practice, the push for stronger security is speeding up convergence: OT networks are adopting IT-like security tools (such as firewalls, identity management, and intrusion detection), and IT teams are learning the unique constraints of OT systems (such as 24/7 uptime requirements and legacy device limitations). Regulatory pressures also play a role—North American electric utilities face mandatory cybersecurity standards (NERC CIP) for critical grid systems, which effectively require coordination between IT and OT personnel to ensure compliance.

Ultimately, organizational and economic factors also play a significant role in IT/OT integration. Utilities aiming to boost efficiency have learned that maintaining separate, duplicate technologies and teams is not an ideal approach. For example, not long ago, a utility might operate two communication networks: one proprietary system for SCADA traffic and a separate telecom network for corporate data. Moving toward shared, standards-based networks and infrastructure can reduce costs and simplify management. It also helps prevent gaps in responsibility—for instance, ensuring critical tasks like software updates or data backups are not neglected because each team assumed the other was handling them. Many utilities have responded by restructuring, sometimes uniting OT telecom and control system support under the same leadership as IT, or at least creating cross-domain working groups. A culture shift is underway: OT specialists are gaining knowledge about IP networking and cloud platforms, while IT staff are being trained on grid operations and safety. This cross-pollination is crucial because IT/OT convergence involves people, processes, and technology in equal measure. A common theme among early adopters is that success occurs when everyone works from a shared plan rather than guarding their territory. In short, the power industry is recognizing that the entire system—the generation, transmission, distribution, and customer interfaces—functions best when information flows freely and securely between traditionally separate areas. The following sections examine the tangible benefits this brings and the methods by which they are achieved.

Smarter Grid Operations

Through IT/OT Integration

By integrating IT and OT capabilities, utilities can operate the grid more intelligently and proactively than ever before. One of the most significant advantages is the ability to perform predictive maintenance and asset management through advanced data analytics. In the past, equipment maintenance was primarily time-based or reactive — components were inspected or serviced according to fixed schedules, and problems were addressed only after alarms or failures occurred. IT/OT convergence enables a shift to a predictive approach, where continuous OT data feeds (such as temperatures, load levels, and vibration readings) are analyzed by IT systems to detect anomalies and potential issues. For instance, sensors on a high-voltage transformer may detect subtle temperature increases or gas buildup in the oil, signaling early faults. This data is sent to a central data historian and analytics engine, which compares it to models and past patterns to forecast potential failures weeks in advance. The utility can then plan a controlled replacement of the transformer at a convenient time, preventing an unexpected outage. This method maximizes asset lifespan and reduces unplanned downtime. It also lowers costs by avoiding catastrophic failures and focusing maintenance where it's most needed, rather than over-servicing everything. Many U.S. utilities have implemented "asset health" programs as part of their grid modernization efforts, often combining previously separate data sources by merging OT sensor and SCADA data with IT databases, such as work order systems and equipment inventories. The results have been impressive. Predictive analytics have enabled some operators to significantly cut feeder interruptions and extend equipment life. Essentially, utility data analytics driven by IT/OT integration transforms raw real-time data from field devices into actionable insights for grid managers.

Another area transformed by IT/OT integration is outage management and grid reliability. When a power disturbance or fault occurs on the grid, speed and information are critical for restoring service quickly. In a converged environment, operators can leverage both OT automation and IT-level analysis to respond in real time. For instance, many utilities are deploying FLISR (Fault Location, Isolation, and Service Restoration) schemes—a classic example of a smart grid application. OT-side devices, such as

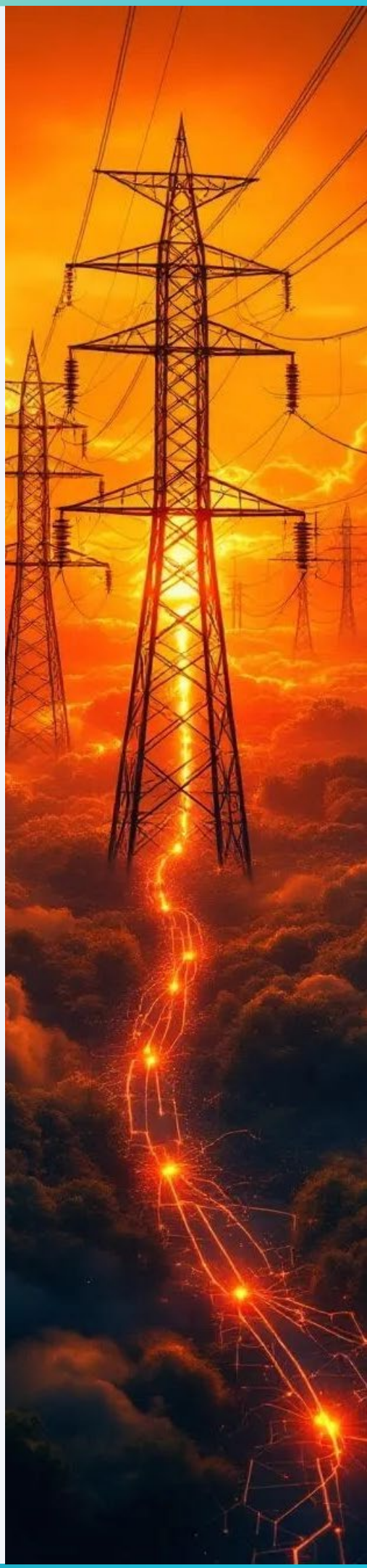
reclosers and intelligent switches, can autonomously isolate a faulted section of a distribution feeder within seconds. However, IT systems enhance this process by immediately collecting telemetry data on which devices were operated and where the fault is likely located, then providing operators with a visualization and even dispatch instructions for crews. An integrated Outage Management System can automatically correlate customer smart meter outage reports (an IT system input) with SCADA data from the field to pinpoint the extent of the outage. It can also trigger customer notifications via automated texts or calls to inform them of the estimated time until power is restored. This closed loop of OT sensing/control with IT data integration significantly boosts reliability metrics. Some utilities have reported significant reductions in outage durations thanks to such schemes—what used to require field staff to manually patrol for a downed line can now be done by algorithms within seconds. Even transmission grids benefit: high-speed monitors can detect and locate faults on transmission lines, then share that data with central systems that reconfigure power flows or alert neighboring grid operators. Overall, IT/OT convergence enables the grid to be self-healing, minimizing the impact of disruptions and increasing transparency for both operators and customers.

The integration of distributed energy resources is perhaps the best example of IT/OT convergence, enabling new capabilities and functionalities. Renewable and distributed resources—such as solar PV arrays, wind turbines, battery storage, demand response from smart thermostats, and more—bring variability and complexity that cannot be managed by traditional manual or siloed methods. Utilities are therefore turning to layered control architectures. On the OT level, many deploy local controllers and intelligent inverters that can make quick adjustments to keep voltage, frequency, and power flows within limits. For example, if solar generation spikes on a feeder at noon, a local controller may adjust capacitor banks or instruct smart inverters to absorb reactive power, thereby maintaining voltage stability. However, these local actions need to be coordinated at a higher level to maximize overall efficiency and avoid conflicts. This is where IT systems like DERMS come into play. A DERMS is a software platform, often cloud-based or running on enterprise servers, that gathers data from thousands of DERs and optimizes their operation based on grid conditions and market signals. It might forecast the day's solar output, schedule battery dispatch during peak hours, or send price signals to electric vehicles to encourage charging at specific times. DERMS relies on continuous data streams from the field (smart inverters, feeder sensors, weather feeds, etc.) and sends control set-points back. This is only possible with an integrated communications and data

environment connecting IT and OT. In practice, many utilities utilize edge computing in conjunction with cloud analytics. Edge controllers located at substations or community levels execute immediate control strategies for groups of DERs, ensuring local reliability and the overall stability of the power grid.

Meanwhile, a centralized IT system manages broader strategies, such as setting targets for how much each feeder should contribute to peak shaving or initiating a demand response event across a city. The benefits are clear: utilities can support higher levels of renewable energy without sacrificing stability and can actively use DERs to bolster the grid. For example, during high demand, a utility might enlist a thousand home batteries and thermostats to reduce load within minutes—something only possible through automated IT/OT integration. In short, combining IT and OT allows the grid to operate as an interactive, adaptable platform rather than a one-way delivery system. This not only improves reliability and efficiency but also creates new business opportunities that were previously impossible.

Customers benefit from IT/OT integration through improved services and increased engagement. Smart meters exemplify this; they sit at the boundary of OT and IT, measuring consumption, running software, and communicating with networks back to the utility. By integrating smart meter data into IT systems, utilities can offer customers detailed insights into their usage, alerts for outages or high consumption, and time-based pricing options. For example, some utilities provide real-time web portals or smartphone apps powered by meter data, allowing customers to see how turning on an appliance affects their bill or receive instant notifications if power is out at their home. Additionally, the utility's customer information system can connect with operational data to customize solutions, such as proactively reaching out if a customer's usage pattern indicates HVAC issues or remotely verifying whether an outage is due to a neighborhood problem or just a tripped breaker. These enhancements increase customer satisfaction and promote energy efficiency and demand response, as customers become more informed and proactive about managing their energy use. On the utility side, having an integrated view of customer consumption and grid operation enables more efficient planning: IT analytics can analyze meter data to improve load forecasts at the feeder or transformer level, guiding investments and reducing overload risks. Essentially, by merging IT and OT, utilities are transforming from basic energy suppliers into data-savvy service providers capable of anticipating and addressing customer needs more flexibly.



EDGE COMPUTING

Distributed Intelligence at the Grid Edge

A key technology enabling IT/OT convergence is edge computing. Edge computing involves placing computing and data processing resources closer to where data is generated, rather than relying solely on centralized cloud or data center processing. In the context of the electric grid, the "edge" refers to devices and controllers located in substations, on distribution feeders, or even on customer premises, such as smart meters or solar inverters. By deploying intelligence at the network's edge, utilities can achieve real-time responsiveness and autonomy that would be challenging if every decision had to be sent to a central system and then returned. This is vital for the power grid, where control actions often need to be taken in milliseconds to seconds to maintain system stability.

One advantage of edge computing is the ability to make rapid decisions for critical grid operations. By analyzing data directly at the source, edge devices can detect and respond to local events almost instantly. For example, a secondary distribution substation serving a neighborhood can immediately adjust a voltage regulator or tap changer if a sudden voltage fluctuation occurs due to a large change in solar PV output or an industrial motor startup. If that data had to be sent to a remote server, the delay could cause unacceptable voltage deviations. Edge computing helps ensure the grid is more agile and resilient, automatically handling routine disturbances. In generation, wind turbines and solar farms utilize edge controllers to adjust their output in real-time based on local conditions, thereby maintaining stability. Transmission grids also benefit from dynamic line rating sensors, which calculate safe loading limits on the spot (based on local temperature and sag measurements) and feed that information into automated controls to adjust power flows.

Another advantage is bandwidth optimization and communication reliability. Not all data needs to be sent upstream, and not all decisions require cloud involvement. By filtering and pre-processing

data at the edge, utilities reduce the load on their communication networks and central systems. For example, a sensor that measures grid frequency hundreds of times per second can process data locally and only send alerts if thresholds are exceeded, conserving network bandwidth and storage while also improving cybersecurity by reducing data exposure. In remote or critical facilities, edge processing can enable continued operation even if the connection to central systems is lost. For instance, a microgrid can run autonomously during outages, managed by local edge controllers, and then reconnect to the main grid once communication is restored. This capability for the grid to gracefully degrade into autonomous cells and later reassemble enhances resilience against cyber threats and physical disasters.

Edge computing is essential for integrating large amounts of DERs through platforms like DERMS. A modern utility might oversee thousands of DERs. A purely centralized system would struggle with the volume and detail of data. Instead, a hierarchical approach is used: edge devices manage local optimization and control in milliseconds, while a centralized DERMS in the cloud or data center handles broader coordination every few minutes. This distributed intelligence setup enhances reliability: if the central system fails, edge controllers can maintain basic safe operation, and if an edge device fails, the system can adapt accordingly. Examples from around the world demonstrate this: European utilities are deploying standardized edge platforms at secondary substations for applications such as real-time voltage control and power quality analytics. In the U.S., some utilities have installed rugged servers at substations to run AI models locally for equipment diagnostics, reducing data transfer needs and boosting response times. Modern smart meters are also becoming edge devices, capable of detecting anomalies and connecting directly with local DER assets.

In summary, edge computing helps the grid meet the twin challenges of speed and scale by placing intelligence where it's needed most. It complements centralized IT systems by managing real-time actions locally while sending distilled insights upstream for system-wide optimization. Together, they create a more adaptive grid nervous system capable of reacting locally and thinking globally.

Data Integration and Standards for Interoperability

A significant technical challenge in IT/OT convergence is integrating a diverse range of devices, applications, and data formats into a unified system. Utility OT environments encompass equipment from various vendors and generations—legacy RTUs that communicate using protocols like Modbus or DNP3, newer IEDs that utilize IEC 61850, smart meters adhering to other standards, and so forth—while IT systems have their own data schemas and interfaces. To enable these systems to communicate effectively, common data standards and integration architectures are essential. Without standards, utilities have relied on custom point-to-point integrations, which are fragile and costly to maintain. The industry's solution has been to develop standardized data models and protocols designed for the smart grid.

One key element is the Common Information Model (CIM), defined by IEC 61970/61968. CIM offers a semantic model for grid components (transformers, lines, and generators) and business objects (work orders and outage events). By adopting CIM, utilities can ensure that various IT and OT applications reference assets and events consistently. For example, an EMS can export a

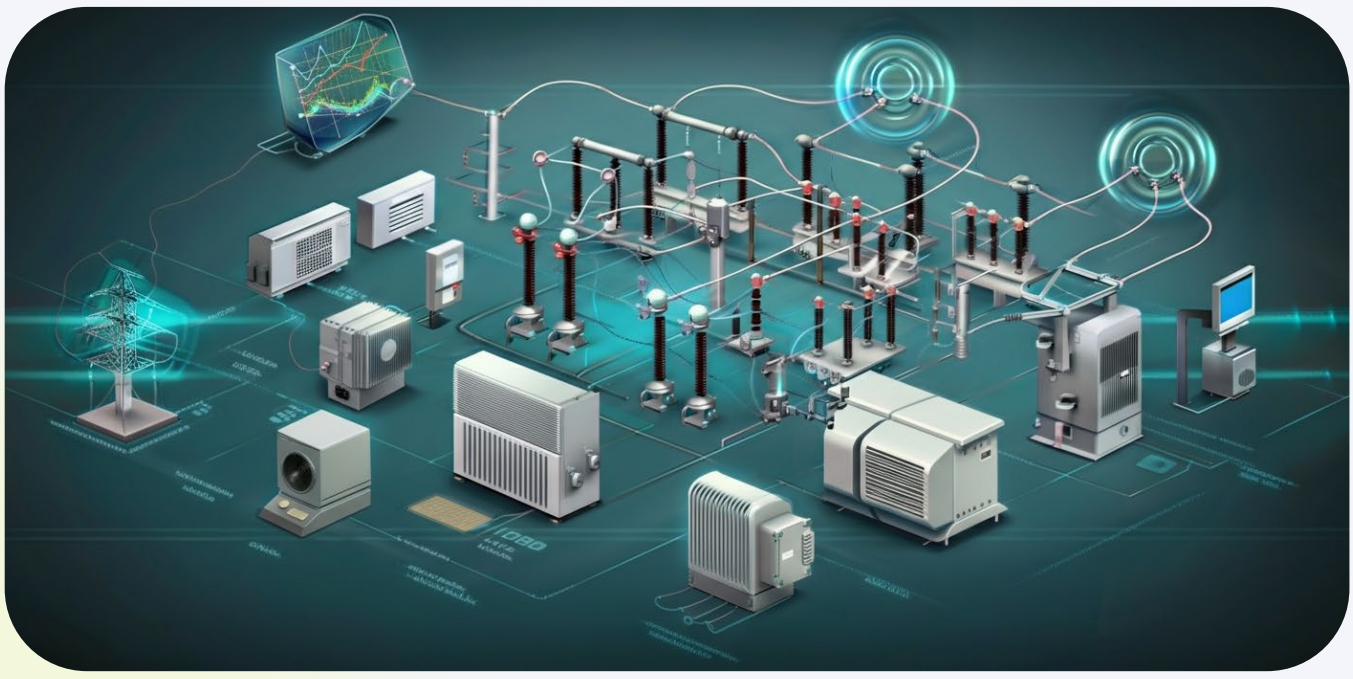
transmission network model in CIM format, which a planning tool can import directly without manual remapping. CIM facilitates plug-and-play interoperability among systems from different vendors and has become essential in many data exchanges, especially among regional transmission operators.

On the operational side, communication protocol standards like IEC 61850 have transformed substation automation. 61850 is an Ethernet-based standard that defines message formats and device data models, allowing IEDs (Intelligent Electronic Devices) to connect using standard networking equipment and services. Substation gateways can translate 61850 data into CIM or other enterprise formats, facilitating easier integration with IT systems. Additionally, the move to IP networking across the grid—replacing serial links and circuit-switched telecom—permits OT devices to utilize the same network infrastructure as IT, with appropriate segmentation and quality of service.

Other standards support DER integration (IEEE 2030.5, IEEE 1547), industrial-to-IT data exchange (OPC UA), and time-series/event data (COMTRADE/C37.118 for synchrophasors, MQTT/DDS for IoT). Many utilities deploy enterprise service buses or middleware as data integration platforms, which ingest OT streams, transform them into a common model, and distribute them to IT applications. This prevents point-to-point connections and centralizes integration logic.

The U.S. government's NIST Smart Grid Interoperability Framework identified essential standards and promoted industry adoption of these standards. Utilities involved in standards development and interoperability testing events ("plug-fests") benefit from easier integration and increased vendor options. Although many still operate legacy equipment, protocol converters and gateways offer temporary solutions by translating older protocols into modern formats. APIs and web services that adhere to industry standards further enhance integration with enterprise applications, thereby improving the overall integration experience.

Common data standards and interoperability are essential for IT/OT convergence. They enable the various components of a smarter grid to work together as a cohesive system, reduce custom engineering costs, and protect investments by preventing vendor lock-in.



Network Architecture

Connecting Substations to the Cloud

Achieving IT/OT integration requires rethinking the network architecture that connects field devices, substations, control centers, and cloud platforms. Legacy OT networks employed strict layering (e.g., the Purdue model), which isolated field devices from enterprise networks. In a converged approach, we need architectures that enable timely and secure data flow from deep within OT environments to IT systems—and sometimes control commands back—while maintaining strong security boundaries.

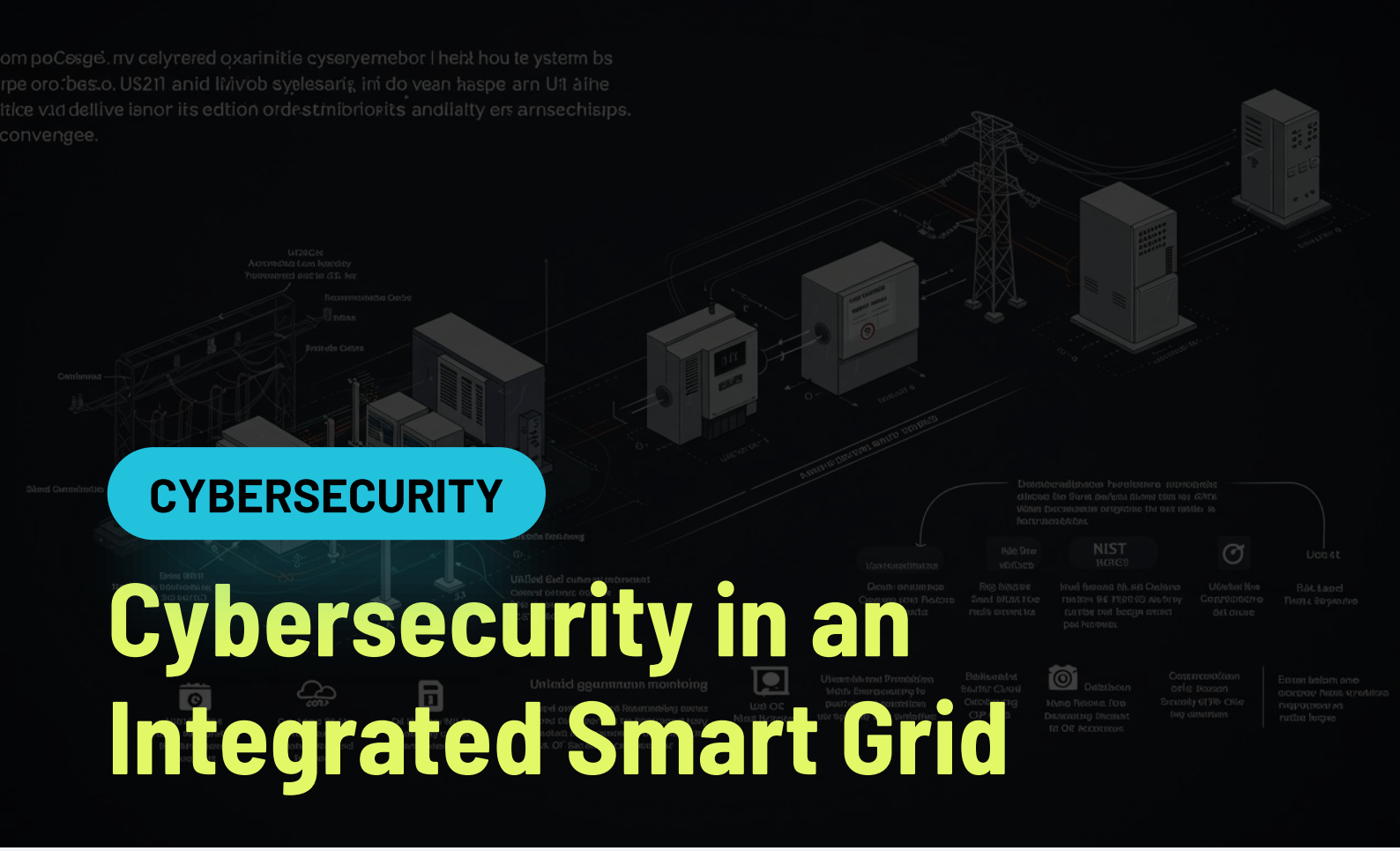
A common approach maintains a separation between the core control network and the enterprise network while using a secure OT DMZ to mediate exchanges. The DMZ hosts intermediary servers—such as data historians, API gateways, and jump hosts—that transfer data northbound and southbound under strict access controls. Firewalls, one-way diodes, and protocol filters ensure limited, audited pathways. For unidirectional requirements, data diodes physically block inbound traffic while streaming OT data to cloud analytics, ensuring there is no return path for attackers.

Where bidirectional control is needed—such as in cloud-based DERMS—utilities often set up outbound-only VPN or brokered communication channels initiated by edge gateways. The substation controller maintains an encrypted tunnel to the cloud, accepting commands only through that pre-established link. Zero Trust Network Access models are emerging, continuously authenticating and authorizing each session, rather than relying solely on perimeter defenses.

Communication media have also undergone modernization: private LTE (4G/5G) networks, expanded fiber, and public cellular slices (APNs) offer high bandwidth and IP connectivity for OT and IT traffic, with QoS guarantees. Quality-of-Service (QoS) tagging and network engineering ensure that time-sensitive OT traffic, such as teleprotection and FLISR commands, is prioritized over less critical data.

Software-Defined Networking (SDN) is being tested in substations to offer programmable, reliable traffic paths and quick failover, ensuring both resilience and security by implementing "deny-by-default" policies. Monitoring and layered defenses—intrusion detection systems, passive network sensors, and security event collection in unified SOCs—provide situational awareness across converged networks.

The architecture effectively connects necessary components, isolates sensitive parts, and maintains visibility at all layers. By integrating modern IP-based networks with strict segmentation, encryption, and monitoring, utilities support IT/OT convergence without compromising the reliability or security of essential operations.



CYBERSECURITY

Cybersecurity in an Integrated Smart Grid

As IT and OT systems become increasingly interconnected, cybersecurity is both a significant challenge and a vital enabler of convergence. A connected, digitized grid presents a broader attack surface for adversaries, including nation-state actors, criminal groups that deploy ransomware, and hacktivists. Incidents like the 2015 Ukraine grid attack and the 2021 Colonial Pipeline ransomware breach demonstrate that IT breaches can disrupt OT operations. The industry must develop a unified security approach that covers the entire converged landscape, combining IT best practices with OT safety and reliability priorities.

Network segmentation and access control remain essential. Utilities implement strict firewalls and electronic security perimeters around OT, often required by NERC CIP, permitting only minimal, tightly regulated connections to IT systems. Inside OT, micro-segmentation further isolates substations and field networks. Identity management systems (such as extending Active Directory to OT) and multi-factor authentication for remote access eliminate shared accounts and default passwords.

Intrusion detection and continuous monitoring combine logs and network traffic from IT and OT. Specialized ICS IDS solutions monitor for abnormal commands or malware patterns, feeding into security operation centers that use threat intelligence sharing via E-ISAC and DOE's CRISP. Machine–learning–based anomaly detection is also developing to spot new threats in control networks.

Unified governance frameworks—such as NIST CSF, ISA/IEC 62443, and NIST SP 800-82—guide comprehensive security programs that encompass processes, technology, and personnel. Change management processes now include OT patching and updates, striking a balance between security and operational safety through lab testing and staged deployments. Cyber-informed engineering integrates security into system design by selecting devices with secure boot,

cryptography, and strong authentication.

Regulatory mandates (such as NERC CIP versions and state commission requirements for distribution utilities) enforce controls on critical assets, incident response plans, and supply chain risk management (CIP-013). Utilities map controls to compliance matrices to facilitate audits and ensure adherence to compliance standards. However, compliance alone is not enough: risk-based, adaptive security—such as threat hunting, red-team exercises, and cyber resilience drills—is crucial to stay ahead of threats.

Zero Trust principles are being adapted for OT, with device-level authentication, least-privilege communications, and cryptographic protocol versions (such as DNP3-SA and IEC 62351) replacing traditional trust-based networks. Supply chain security ensures that vendor hardware and software are vetted and signed. Defense-in-depth layers—such as firewalls, data diodes, jump hosts, and endpoint protection—limit attacker lateral movement and protect critical controls.

Resilience and recovery planning ensure that operations can safely degrade in the event of an attack, thereby minimizing the impact on critical infrastructure. Local analog protections, fail-safe relays, and backup manual controls ensure grid integrity in the event of a digital system compromise. Incident response exercises test coordination between IT and OT teams, as well as external partners. Cybersecurity, far from hindering innovation, supports it by enabling a trusted, visible, and protected converged infrastructure.

- **Compliance & Risk-Based Security:** Utilities follow regulatory mandates (e.g., NERC CIP, CIP-013) but also adopt adaptive measures like threat hunting, red-teaming, and resilience drills to go beyond compliance.
- **Zero Trust & Defense-in-Depth:** OT networks apply device-level authentication, least-privilege access, vetted supply chain components, and layered protections (firewalls, diodes, jump hosts, endpoint security) to reduce attack surfaces.
- **Resilience & Recovery:** Fail-safes such as analog protections, backup manual controls, and coordinated incident response ensure grid continuity and minimize impact during cyber incidents.

Regulatory and Compliance Landscape

In the U.S., IT/OT integration is overseen by NERC and FERC. The NERC CIP standards require robust cybersecurity measures for the bulk electric system, including identifying critical assets, protecting perimeters, enforcing access controls, applying patches, and reporting incidents. Although CIP primarily covers transmission and large-scale generation, many utilities voluntarily implement CIP-like measures for distribution and DER integration to manage risk and prepare for potential future mandates.

Some state public utility commissions are increasingly focusing on cybersecurity for smaller entities, often recommending plans based on DOE's C2M2 or NIST frameworks. Federal agencies like DOE (through CESER) and CISA provide guidance, threat advisory feeds, and voluntary programs (such as the 2021 100-day action plan) that shape industry practices. Standards organizations (e.g., ISA/IEC 62443, NIST SP 800-82) and industry groups (e.g., NIST Smart Grid Framework, plug-fests) address gaps and promote interoperability.

Regulations also overlap with reliability and safety standards (NERC PRC/MOD) and data privacy laws that govern the collection and use of smart meter and customer information. Utilities maintain compliance mappings that link various requirements to unified controls, conduct both internal and external audits, and proactively engage regulators when testing cloud or new architectures. The regulatory environment thus both promotes secure IT/OT integration and ensures that innovations serve the public interest by safeguarding reliability and security.

Balancing Innovation with Reliability and Safety

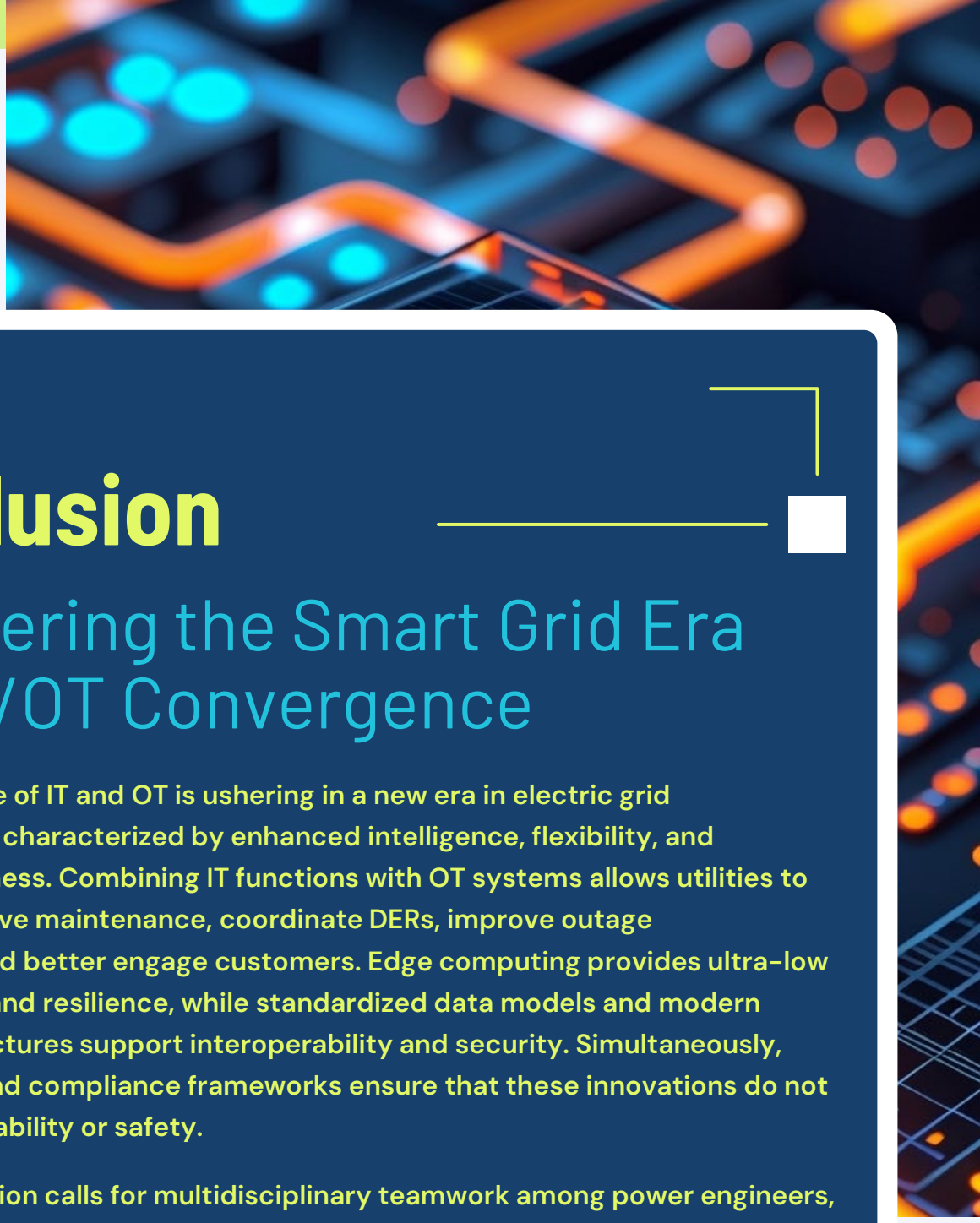
Integrating IT and OT requires striking a balance between innovation and the grid's stringent reliability and safety standards. OT systems develop over more extended periods than IT systems; to manage risks, utilities test new technologies alongside legacy systems, conduct extensive testing (including digital twins and hardware-in-the-loop), and use gradual rollouts. Automated systems support, rather than replace, human expertise: AI and analytics offer decision support while experienced operators retain ultimate authority.

Intrinsic safety mechanisms—protective relays with hard-coded limits and local overrides—ensure that even if remote systems fail, grid stability and personnel safety are maintained. Manual controls and fallback modes offer resilience during emergencies. Cross-training IT and OT staff promotes shared understanding, while human-centered interface design prevents confusion amid automation.

Regulatory and rate structures require utilities to justify investments through reliability improvements or cost savings, ensuring that digital transformation aligns with customer interests. Ultimately, convergence is about enhancing grid capabilities while maintaining the trust that the lights stay on and operations remain safe and secure. By proceeding with caution, collaboration, and a focus on results, the industry can create a smarter, more resilient, and secure grid.

Utilities balance innovation with safety by testing IT/OT integrations alongside legacy systems, using digital twins, gradual rollouts, and ensuring human expertise remains central with AI and automation as decision-support tools.

Safety, resilience, and trust are preserved through intrinsic protections, manual overrides, staff cross-training, and regulatory alignment—ensuring digital transformation enhances grid reliability and customer confidence.



Conclusion

Engineering the Smart Grid Era with IT/OT Convergence

The convergence of IT and OT is ushering in a new era in electric grid operations—one characterized by enhanced intelligence, flexibility, and interconnectedness. Combining IT functions with OT systems allows utilities to perform predictive maintenance, coordinate DERs, improve outage management, and better engage customers. Edge computing provides ultra-low latency control and resilience, while standardized data models and modern network architectures support interoperability and security. Simultaneously, cybersecurity and compliance frameworks ensure that these innovations do not compromise reliability or safety.

This transformation calls for multidisciplinary teamwork among power engineers, IT architects, cybersecurity specialists, and field operators. It demands thorough testing, strong governance, and a culture that values both technological progress and the grid's essential reliability. Looking forward, deeper integration—such as AI-driven control loops, zero-trust architectures, and transactive energy platforms—appears imminent, promising even greater efficiency and sustainability.

For U.S. utilities and regulators, the goal is clear: to enable IT/OT convergence and realize its benefits while carefully managing associated risks. By integrating information and operational technologies within a secure and resilient framework, the electric industry can create a truly smart grid—one that senses, thinks, and acts to address the challenges of the 21st century, all while maintaining the reliability that society expects.

References

01

R. J. Campbell

Evolving Electric Power Systems and Cybersecurity, Congressional Research Service Report R46959, Nov. 4, 2021

02

Utilities Technology Council

IT/OT Convergence Issue Brief, Sept. 2018

03

Cisco Systems

IT/OT Convergence in Critical Infrastructure and Industrials, White Paper, Sept. 30, 2022.

04

Energy Central

The Convergence of OT and IT: A Transformation in the Electric Business, Oct. 2023.

05

Owl Cyber Defense

Best Practices for OT-to-Cloud Connectivity, Blog Post, Aug. 9, 2021

06

P. A. Manos

IT/OT Convergence, T&D World (Smart Grid Special Issue), 2017.

07

Utility Dive

A New Era for Smart Meters: Shifting Intelligence to the Edge, Mar. 20, 2023

08

C3 AI

Predictive Maintenance for Electric Grid" (Case Study).
https://c3.ai/customers/predictive-maintenance-for-electric-grid/ (accessed Jul. 2025)

09

Iberdrola

Edge Computing on the Electricity Grid.
https://www.iberdrola.com/about-us/our-innovation-model/edge-computing-electricity-grid (accessed Jul. 2025)

10

B. Achaal, M. Adda, M. Berger, H. Ibrahim, and A. Awde

Study of Smart Grid Cyber-Security, Examining Architectures, Communication Networks, Cyber-Attacks, Countermeasure Techniques, and Challenges," Cybersecurity, vol. 7, art. 10, May 2024

11

North American Electric Reliability Corporation

Quick Reference Guide: Security Integration, Feb. 2025.
https://www.nerc.com/pa/Documents/Security_Integration__Quick%20Reference%20Guide.pdf (accessed Jul. 2025)

12

Cybersecurity and Infrastructure Security Agency

Draft NSTAC IT-OT Convergence Report, Aug. 2022.
https://www.cisa.gov/sites/default/files/publications/Draft%20NSTAC%20IT-OT%20Convergence%20Report%20%288-12-2022%29_508_0.pdf (accessed Jul. 2025).

13

International Society of Automation

IT/OT Convergence Whitepaper, 2024.
https://programs.isa.org/it-ot-convergence (accessed Jul. 2025).

14

J. Doe et al.

Edge Intelligence in Smart Grids: A Survey on Architectures, Internet of Things, vol. 11, no. 3, art. 47, Mar. 2023.
https://www.mdpi.com/2224-2708/11/3/47 (accessed Jul. 2025).

15

Verve Industrial

IT vs OT Explained: Differences, Integration Challenges, and Convergence Strategies, Jan. 18, 2024.
https://verveindustrial.com/resources/blog/it-vs-ot-explained-differences-integration-challenges-and-convergence-strategies/ (accessed Jul. 2025).

16

Armis

Securing IT & OT in Industrial Environments, White Paper, 2022.
https://www.armis.com/white-papers/securing-it-ot-in-industrial-environments/ (accessed Jul. 2025).

17

SINTEF

Improving Smart Grid Cyber Security through 5G Enabled IoT and Edge Computing, 2020.
https://www.sintef.no/projectweb/cineldi/cineldi-knowledge-base/2020/improving-smart-grid-cyber-security-through-5g-enabled-iot-and-edge-computing/ (accessed Jul. 2025).

18

Asimily

NERC CIP Compliance, 2025.
https://asimily.com/compliance-nerc-cip/ (accessed Jul. 2025).

19

B. Achaal et al.

Study of Smart Grid Cyber-Security, cybersecurity, vol. 7, no. 1, May 2024, doi: 10.1186/s42400-023-00200-w.

Disclaimer

About Vedeni Energy

VedeniEnergy

Vedeni Energy offers specialized services designed to help businesses navigate the complexities of the modern energy landscape. Our offerings are tailored to meet the unique needs of utilities, independent power producers, regulatory bodies, and other stakeholders, ensuring success through strategic insights, expert guidance, and innovative solutions.

Vedeni.Insights+

Vedeni.Insights+ is Vedeni Energy's subscription-based service, granting subscribers full access to Vedeni Energy's extensive library of whitepapers and in-depth technical analyses. These authoritative resources offer comprehensive examinations of the energy sector's critical topics, from market trends and regulatory changes to emerging technologies and strategic investment opportunities.

Vedeni.IQ+

Vedeni Energy's **Vedeni.IQ+** service provides actionable wholesale electric power market intelligence that enables clients to make informed decisions confidently. Our expert analysis and reporting distill complex energy market information into clear, concise insights, helping organizations elevate their market strategies, influence policy, and identify new opportunities.

Vedeni.Spark+

Vedeni.Spark+, a service provided by Vedeni Energy, is designed to help startups and established companies secure the capital funding necessary for growth and success. Our team of seasoned advisors works closely with clients to develop tailored funding strategies that align with their business goals and financial requirements.

TO LEARN MORE, VISIT US AT

WWW.VEDENI.ENERGY