TEIA's layered approach to energy connectivity

Building a unified interoperability stack

Contents

Executive summary

The energy industry faces a pressing challenge: establishing secure, standardized interoperability across an increasingly diverse ecosystem of energy systems, devices, and data platforms.

The Trusted Energy Interoperability Alliance (TEIA) has emerged to address this challenge by creating a unified interoperability stack designed to enable seamless integration without compromising trust or security.

U.S. and EU policymakers are moving to harmonize interconnection requirements and interoperability standards in response to the sharp growth in renewable deployment and grid modernization investments, seeking to keep pace with the three- to five-fold increases in energy demand.

This reinforces the role of TEIA in enabling scalable, secure, and interoperable energy transactions.[1, 2]

By delivering open standards that bridge legacy systems with next-generation technologies, TEIA provides the foundation for more resilient, efficient, and adaptable energy ecosystems.

U.S. and EU policymakers are moving to harmonize interconnection requirements and interoperability standards in response to the sharp growth in renewable deployment and grid modernization investments.

The energy interoperability challenge

The fragmentation of today's energy landscape creates substantial inefficiencies and risks.

Technology fragmentation has left devices and systems locked within proprietary protocols, inhibiting communication across vendors. For example, virtual power plants (VPPs) struggle to integrate assets from different OEMs: a VPP platform may connect easily with one manufacturer's solar inverters but require costly custom integrations to interface with a different vendor's EV chargers or battery storage systems. Data fragmentation adds complexity by spreading energy data across incompatible formats, making aggregation and optimization difficult for grid operators.

Security fragmentation exposes vulnerabilities at integration points, as each system adopts its own mechanisms without unified safeguards. Operational fragmentation compounds these issues, forcing operators to manage multiple proprietary platforms with rising costs and declining efficiency.

The cost of fragmentation extends well beyond inconvenience. Economically, proprietary lock-in drives up infrastructure costs and stifles competition. Innovation stalls as non-standardized environments slow the adoption of new technologies and business models. Reliability suffers when limited visibility across fragmented systems compromises grid stability.

Security fragmentation exposes vulnerabilities at integration points, as each system adopts its own mechanisms without unified safeguards.

Understanding TEIA's framework

At the heart of TEIA's approach lies a layered framework designed to provide secure interoperability independent of underlying network technologies.

This framework is defined by three value pillars: scalability, security, and compliance. With its "scale by design" architecture, TEIA allows devices to authenticate once and connect multiple times without re-authentication, dramatically increasing efficiency in large-scale deployments.

Persistent security associations provide robust, reliable protection without imposing excessive computational overhead. Built-in compliance with emerging standards such as NIST and EU frameworks ensures alignment with evolving global regulations. This translates complex technical requirements into practical compliance tools that reduce costs and help regulators scale programs effectively across jurisdictions.

Building the unified interoperability stack

The TEIA interoperability stack spans every layer of the energy system, from physical devices to high-level business processes. This comprehensive framework ensures that diverse technologies, organizations, and processes can work together seamlessly while maintaining security, efficiency, and reliability at scale.

At the device layer, energy assets follow standardized interfaces and embedded security protocols, ensuring that even diverse technologies can work together reliably. Solar inverters, battery systems, electric vehicle chargers, and smart thermostats all communicate using common protocols, eliminating the compatibility barriers that have historically fragmented the energy ecosystem.

Persistent security associations provide robust, reliable protection without imposing excessive computational overhead.

The communication layer secures connectivity across multiple network types—from cellular and Wi-Fi to fiber and satellite—while the data layer governs how energy information is collected, processed, and shared in consistent formats. This ensures that a wind farm in Texas can seamlessly share operational data with a grid operator in California, or that a residential solar system can participate in demand response programs managed by utilities across state lines.

On top of this foundation, the application layer enables energy management systems, grid operations, and customer-facing tools that deliver tangible value. Whether it's a utility managing millions of smart meters, an aggregator coordinating thousands of battery systems, or a homeowner optimizing their energy usage, these applications benefit from the standardized foundation below. TEIA sits at the application level by providing a common interface across heterogeneous assets, enabling interoperability, lowering integration overhead, and ensuring that application developers can focus on delivering value instead of reinventing connectivity for every OEM system or device.

Business layer

Workflows, compliance structures, economic mechanisms, and policy integration that enable market operations and regulatory alignment

Application layer

Energy management systems, grid operations platforms, customer-facing tools, and analytics applications that deliver value to end users.

Data layer

Standardized collection, processing, and sharing of energy information in consistent formats across organizational boundaries

Communication layer

Secure connectivity protocols that work across multiple network types while maintaining data integrity and system reliability

Device layer

Physical energy assets with standardized interfaces and embedded security protocols that enable reliable interoperation
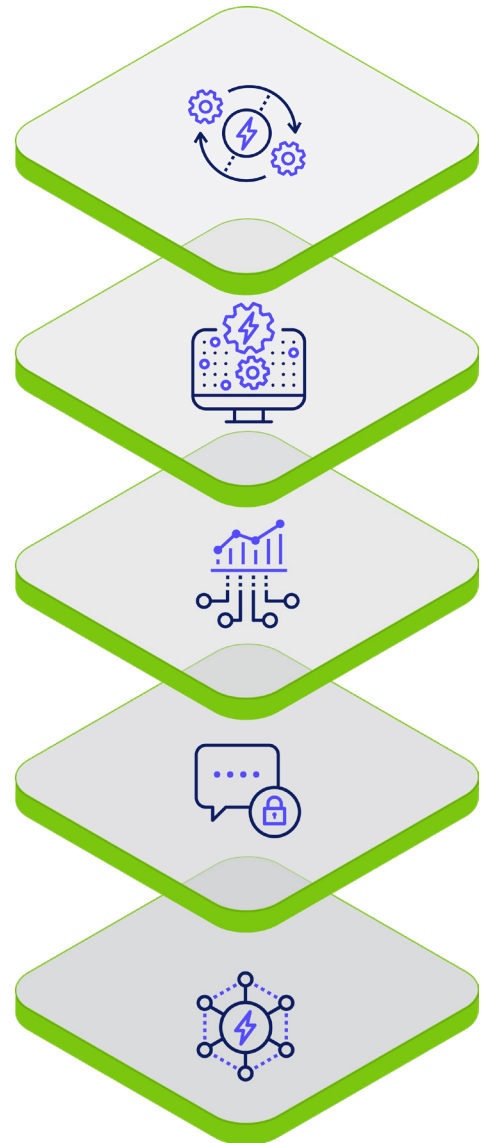
Security and trust frameworks, unified identity management and monitoring and analytics operate across all layers to ensure consistent performance and compliance.

Security and trust principles

Security is not an afterthought in TEIA's model but a foundational design principle.

TEIA's security philosophy integrates four pillars: security by design, zero trust architecture, defense in depth, and continuous monitoring. These principles manifest in practical mechanisms such as multi-factor and certificate-based authentication, role-based access controls, and robust encryption for data at rest and in transit. Real-time threat detection and automated response enhance resilience against evolving cyber threats.

Cyberattacks in the energy sector are intensifying, as recent data3 reveals:

Ransomware is surging. 67% of energy and utilities organizations were hit by ransomware in 2024 — an 80% increase year over year.

Supply chain exposure is the weak link. Nearly 45% of malicious intrusions in the sector stemmed from third-party vendors — far higher than the global average.

Repeat targeting is the norm. Nine out of ten breached companies reported being attacked multiple times through third-party vendors, with software and IT providers most often exploited.

These numbers highlight the urgent need for robust, unified security frameworks and standards to protect increasingly interconnected energy systems.

The trust framework builds on digital certificates, enabling authentication, integrity protection, and non-repudiation. Federated trust extends these mechanisms across domains, ensuring consistency in policy and reputation management.

By aligning with standards such as NERC CIP and the EU NIS Directive, TEIA provides clear pathways for compliance, reducing the burden on industry stakeholders. TEIA reduces the cost and complexity of compliance while strengthening national resilience against cyberthreats.

TEIA offers a future-proof roadmap for secure, connected, and intelligent energy systems.

Engaging with TEIA

**TEIA offers clear pathways for engagement across the energy ecosystem.**

Participation in TEIA provides opportunities to shape international standards, reduce regulatory burden, and accelerate deployment of clean energy infrastructure.

Unlike fragmented proprietary solutions, TEIA's open architecture ensures long-term investment protection while enabling rapid innovation cycles. This positions early adopters as market leaders in the transition to distributed energy resources.
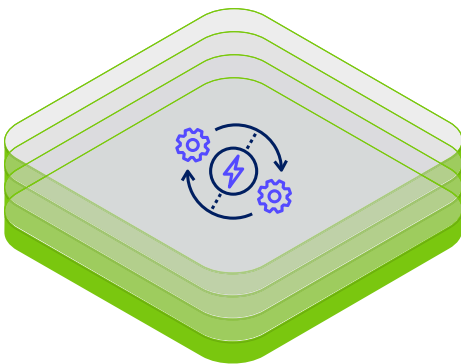
Manufacturers
Begin with device bootstrapping implementations, gaining immediate benefits in cost and interoperability.
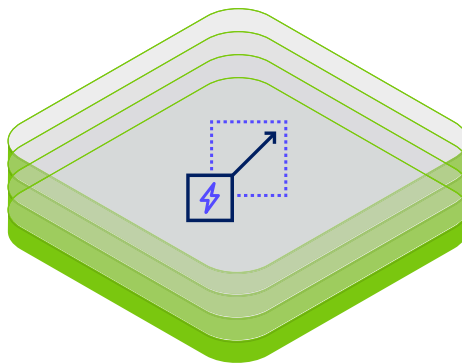
Aggregators
Leverage TEIA's scalable architecture to expand from pilot programs to millions of managed devices.

Regulators
Engage through compliance-first frameworks that simplify oversight while accelerating service adoption.

"TEIA is focused on one thing: establishing a universal trust model that can work with any standard, any device, any application."

Cameron Briggs, TEIA Chairman

trusted-energy.org

Conclusion

The Trusted Energy Interoperability Alliance represents a transformative response to one of the energy industry's most pressing challenges.

By championing open standards for secure integration, TEIA optimizes digital energy systems while maintaining the security and reliability essential for critical infrastructure. Its unified interoperability stack creates a foundation for resilience, efficiency, and innovation, equipping industry stakeholders to adapt to rapid technological and business model shifts.

TEIA provides a practical governance model to advance decarbonization, improve energy security, and promote international regulatory harmonization. As the global energy transition accelerates toward decarbonization, digitization, and decentralization, TEIA's standards framework offers the essential tools to achieve these goals. The future of energy depends on interoperability, and TEIA is building the standards that will make this future possible.
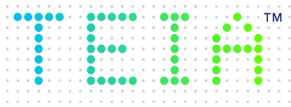
Sources

1. https://goingdigital.oecd.org/data/notes/No24_ToolkitNote_InteroperabilityEnergy.pdf

2. https://www.energy.gov/sites/default/files/2024-04/i2X%20Transmission%20Interconnection%20Roadmap.pdf

3. https://www.resecurity.com/blog/article/cyber-threats-against-energy-sector-surge-global-tensions-mount

TEIA optimizes digital energy systems while maintaining the security and reliability essential for critical infrastructure.

Trusted Energy
Interoperability Alliance