Trusted Energy Interoperability Alliance

**SOLUTION BRIEF**

# One standard. Every device. A trusted energy system.

The TEIA trust model for distributed energy.

# Contents



Founders

# The evolution of distributed energy

## Global energy is undergoing a fundamental shift.

Centralized generation is giving way to millions of distributed energy resources (DERs), arrays of solar panels, battery storage, EV chargers, and wind turbines, all operating at the grid edge, driven by decarbonization targets, falling renewable costs, and demand for grid flexibility and resilience.

Three trends are reshaping ecosystem requirements. The proliferation of IoT devices and AI automation demands trusted data flows; growing multi-vendor procurement as operators source hardware from competing manufacturers; and tightening cybersecurity regulation raising the bar for authentication and data integrity across all grid-connected assets.

Yet the energy industry lacks a common security and interoperability framework. Each OEM implements its own protocols; each operator builds bespoke integrations. Existing standards such as IEC 62443, NIST, OpenADR, and OCPP address parts of the problem, but none delivers a unified trust model across the full value chain. TEIA fills that gap.

**2.6×**

Global renewable capacity projected to grow 2.6× by 2030.

IEA, 2024

**93%**

of cybersecurity experts expect a catastrophic global cyber event likely within two years.

WEF, 2023

**$10.5T+**

Projected global cost of cybercrime by 2026.

WEF, 2023

# Today's energy ecosystem challenges

## Why scaling distributed energy is so difficult.

IEC 62443 establishes security zones and conduits that define how industrial systems should be protected—but today's interconnected reality presents new challenges.

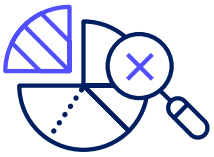
Without a shared interoperability baseline, operators cannot freely switch vendors, OEMs cannot easily enter new markets, and the entire ecosystem bears the cost of fragmentation. Three challenges are the most consequential.

### Fragmented, proprietary security

Each device manufacturer implements its own security model and communication interface, forcing operators to build and maintain separate integrations for each OEM.

### Escalating compliance requirements

Regulators across the US, UK, EU, and Australia are mandating stronger device authentication, encrypted communications, and verifiable data provenance.



### Unverified data undermining AI reliability

AI-driven VPPs are only as reliable as the data they act upon. Unverified DER data can corrupt dispatch decisions, introduce liability, and put operators at risk.

Together these challenges inflate costs, create security vulnerabilities, restrict market growth, and undermine the AI-driven flexibility programs the energy transition depends on.

# The TEIA standard

**TEIA is a global open standard for security and interoperability in digital energy systems.**

**How TEIA works**

TEIA uses a shared messaging protocol to provide a secure communications layer that ensures authentication and encrypted data exchange across multi-vendor deployments, eliminating the need for proprietary OEM security implementations. It is agnostic to device type and message payload, and extensible to support new cryptographic standards as they emerge.

Every device and software component in a TEIA-compliant ecosystem operates in a zero-trust environment, where identity is authenticated using verifiable identity credentials. This approach ensures that only authorized entities can access or control DER assets, protecting against both external attacks and internal misuse at the device level.

With a compliance-ready architecture, TEIA specifications are versioned and extensible, allowing adopters to incorporate evolving cryptographic requirements and regulatory standards without rebuilding their underlying architecture.

This protects investments made today as the regulatory landscape develops. TEIA brings standards integration, working with and extending Matter, OpenADR, OCPP, and IEC 62443, acting as the security and interoperability layer to allow those frameworks to function coherently across the full energy value chain, from generation and storage through grid management.

The standard offers open governance to participating device manufacturers, software vendors, utilities, and aggregators. TEIA members can contribute to the standard's development and access reference implementations to accelerate compliant product deployment. OEMs can join the TEIA partner program at no cost, gaining immediate access to specifications, and reference materials.

TEIA provides the foundation that energy transition requires—and that existing standards fail to offer.

# Key benefits and advantages

**TEIA delivers structural benefits to every participant in the energy value chain.**

TEIA-compliant organizations reduce integration costs, strengthen cybersecurity posture, and gain access to a growing global ecosystem of interoperable energy assets.

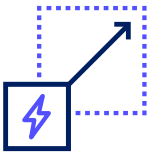
The most significant advantage is that TEIA is genuinely open: no single vendor controls the standard, no proprietary dependencies are required, and specifications are available to all. This creates a level playing field and allows the entire ecosystem to benefit from shared infrastructure rather than duplicated effort.

## Lower cost through shared infrastructure

Every OEM and operator today builds and maintains its own security stack — duplicating effort, inflating cost, and producing inconsistent outcomes. TEIA replaces this redundancy with a shared baseline. OEMs gain access to this baseline at no cost and eliminate the need to build proprietary security from scratch, freeing engineering resources to focus on core product development. Operators eliminate bespoke integration costs. Standards also bring clarity to intellectual property matters as value chains evolve from proprietary solutions to composable, multi-supplier architectures — reducing legal overhead and accelerating procurement decisions.

## Stronger security and AI trust

Every connection in a TEIA-compliant system is authenticated, every data exchange encrypted, and every device identity verifiable. This closes the security gaps that arise when devices from different manufacturers implement their own protocols inconsistently. Critically, TEIA enables operators to confirm the provenance and integrity of data before AI systems act on it — ensuring that automation and dispatch decisions are grounded in trustworthy inputs rather than manipulated or degraded signals.



## Accelerated market access and scale

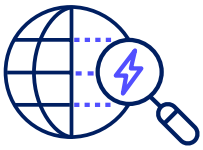
TEIA-compliant devices and software interoperate with any other TEIA-compliant system, regardless of manufacturer, geography, or application. For OEMs, the partner program provides immediate access to a global ecosystem of operators and platforms.For VPP and aggregator operators, it means faster onboarding of new device types and vendors without custom integration work. For regulators, it provides a verifiable, auditable standard against which compliance can be assessed

# Who benefits from TEIA?

**TEIA is designed for every organization operating at the intersection of energy and digital infrastructure. Three audiences benefit most directly.**

## OEMs and device manufacturers

Manufacturers of solar inverters, batteries, EV chargers, heat pumps, and wind turbines spend significant resources building proprietary security and communication layers – work that is outside their core competency and produces fragmented results. OEMs access to a shared security baseline, eliminating the need to build from scratch and accelerating time-to-market. TEIA-compliant devices are immediately interoperable with any operator platform or software system. The TEIA partner program replaces the need for custom integrations and gives manufacturers a single path to global interoperability..



## VPPs, aggregators, and energy operators

Virtual power plant operators, flexibility providers, and distributed energy management system platforms need to integrate, orchestrate, and trust data from devices made by many different manufacturers. TEIA eliminates the integration complexity and security gaps that arise from multi-vendor, multi-protocol environments.

Operators can onboard new asset types faster, dispatch more confidently on verified data, and demonstrate regulatory compliance through a recognized standard rather than a patchwork of proprietary assurances.

## Regulators and standards bodies

Governments developing cybersecurity and interoperability frameworks for grid-connected assets need a credible, technically rigorous standard to reference. TEIA complements IEC 62443, NIST, OpenADR, and OCPP with device-level security and interoperability specifications that those frameworks do not fully address. TEIA's governance model ensures that regulators can participate in shaping the standard, and its specifications provide a clear, auditable basis for compliance requirements across jurisdictions.

Trusted Energy Interoperability Alliance

**Learn more at:** trusted-energy.org
**Contact us at:** contact@trusted-energy.org
+1 408 616 1600



**TEIA membership is available to all organizations active in the digital energy ecosystem. OEMs can join the partner program at no cost.**

**To learn more about TEIA standards, membership, or to request a technical briefing, visit www.trusted-energy.org**