

# Is your energy infrastructure ready for AI attacks?

Why distributed energy needs explicit trust frameworks now.

## The challenge

AI agents autonomously conduct cyberattacks at machine speed, exploiting energy systems that assume device identities are trustworthy.

## The solution

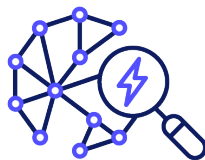
TEIA standards provide a unified interoperability framework simplifying integration, and enabling scalable growth without rising costs.

### 4 steps to explicit trust



#### 1. Cryptographic authentication

Ensure every device and agent proves its identity through unforgeable cryptographic credentials, not network presence.



#### 2. Provable data origin

Bind all data and instructions to verifiable sources so tampering and spoofing become immediately detectable.



#### 3. Policy-driven authorization

Leverage consistent security and compliance Enforce machine-readable policies that govern what each entity can access, control, and execute in real-time.



#### 4. Lifecycle traceability

Track every device, dataset, and action from deployment through decommissioning to maintain continuous security assurance.

**Build trust infrastructure before AI adversaries exploit your vulnerabilities.**

[Learn more](#)

