

Securing Energy & Utilities Critical Infrastructure

Secure Remote Access for Power Grid Operations

Powered by Safous Privileged Remote Access

Safous Privileged Remote Access for Power Grid Operations

Smart grids, renewable assets, IoT-enabled monitoring systems, and Industry 5.0 have modernized how energy providers generate and manage power. Yet this modernization comes with a major vulnerability: every new connected device, third-party vendor connection, remote access point, and IT/OT integration expands the attack surface of critical infrastructure.

Cyberattacks on energy infrastructure are escalating, with **ransomware attacks targeting the utilities sector jumping 80% year-over-year in 2025.**¹ However, a successful cyberattack on the energy and utilities sector doesn't just cost money – it impacts economies, threatens public safety, and undermines national security. Threat actors know this.

Securing remote access to critical OT systems like SCADA, PLCs, grid control systems, and renewable energy management platforms requires a purpose-built approach. Safous Privileged Remote Access is designed to protect complex IT and OT environments, combining privileged access management, identity and access management, and zero-trust network access into a unified platform that secures critical systems while maintaining the operational reliability the sector demands.

Energy & Utilities Security Risks



The energy and utilities sector depends on systems that are becoming more digitally connected. But while connectivity increases efficiency and lowers costs, it also introduces new security risks.

Check out these recent industry statistics:²

70% of energy CEOs believe cybercrime will impact organizational prosperity through 2028.

The rate of vulnerable US power grid points is growing by about 60 per day.

72% of energy firms increased their cybersecurity investments to protect operations in 2024.

1. <https://www.levelblue.com/resources/research-reports/spiderlabs-research-cybersecurity-challenges-for-energy-and-utilities-in-2025/>
2. <https://kpmg.com/sa/en/insights/ai-and-technology/cybersecurity-considerations-2025-energy-and-natural-resources-sector.html>

Case Study: Global Energy Provider



Scope:

45+ generation facilities across North America, Europe, and APAC



Users:

300+ field technicians, 150 remote engineers, 200+ third-party vendors



The Need:

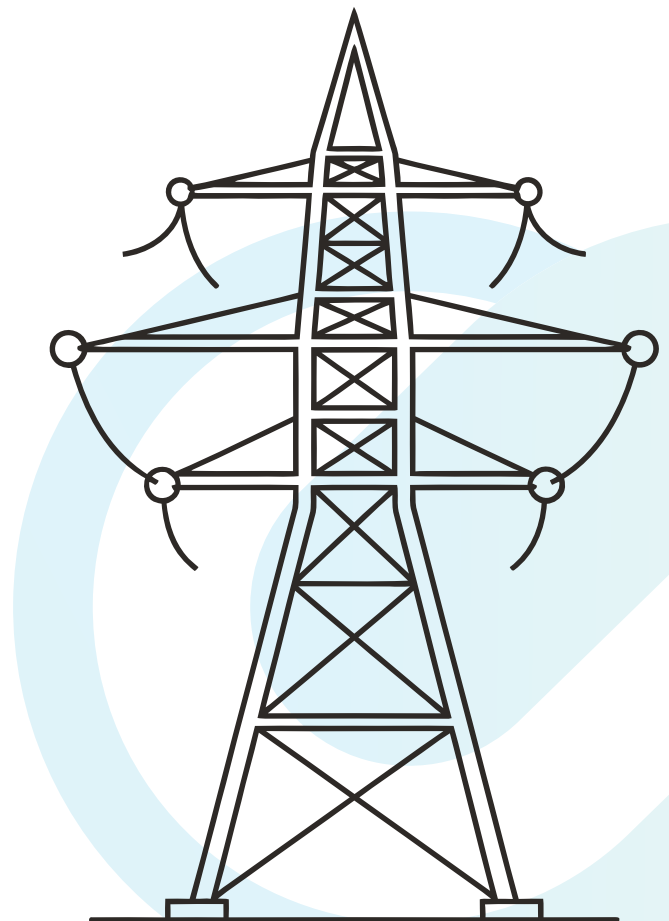
Securely connect remote teams and third-party suppliers to critical OT systems.

Challenges:

- ❌ Multiple legacy SCADA systems and PLCs couldn't support modern access controls
- ❌ Needed centralized oversight of all privileged access across geographically dispersed sites
- ❌ Regulatory compliance standards mandated comprehensive audit trails and access controls
- ❌ Managing privileged access for hundreds of third-party vendors and contractors

Outcomes:

- ✅ Agentless, auditable remote access deployed across 45+ generation facilities with zero operational downtime
- ✅ Centralized governance for 200+ third-party vendors and remote engineers
- ✅ Complete visibility and recording of all privileged OT sessions
- ✅ Reduced operational risk across distributed energy infrastructure
- ✅ Compliance-ready audit trails supporting NERC CIP and regional regulations



Industry Outcomes

- Secure remote access to SCADA, PLC, and grid control systems
- Controlled access for third-party vendors and field technicians
- Reduced operational risk across generation and transmission sites
- Centralized governance across distributed energy facilities
- Full audit visibility for privileged OT sessions
- Compliance-ready logging aligned with NERC CIP and energy sector regulations

How Safous Supports Energy & Utilities Operations



Secure Remote Maintenance

Enable field techs and remote engineers to safely access OT systems and grid control infrastructure for maintenance without installing agents or requiring VPN connectivity.



Grid Control Center Access

Protect access to grid control systems, energy management platforms, and distribution automation networks with identity-based authentication, session recording, and audit trails.



Renewable Energy Management

Secure remote access to distributed renewable energy management systems, inverter controls, and monitoring platforms across geographically dispersed solar and wind installations.



Centralized Session Oversight

Real-time alerts, supervised access, and action-level controls ensure every privileged connection is traceable, auditable, and compliant with regulatory requirements.



Global Multi-Site Operations

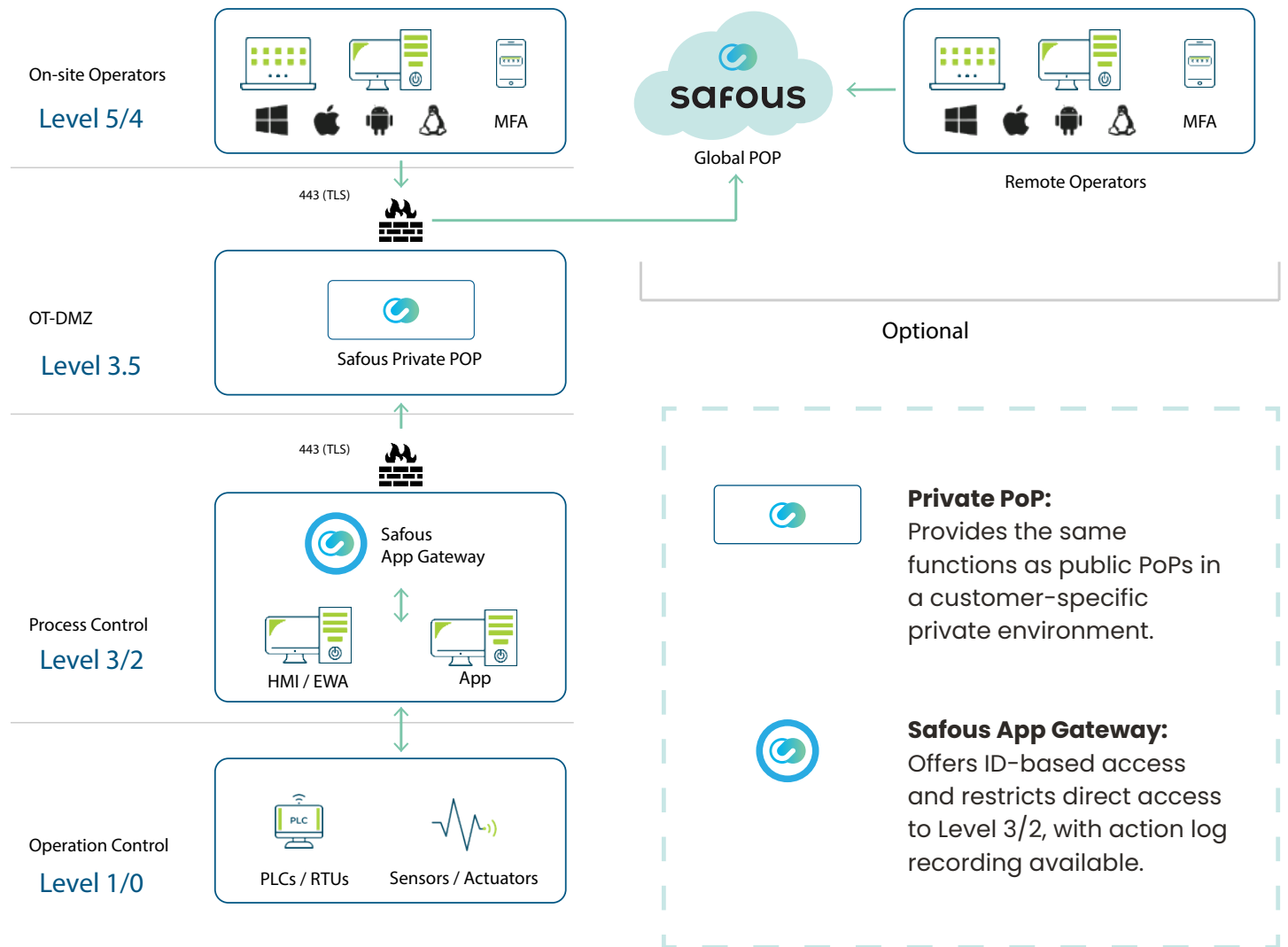
Centrally manage access governance across generation facilities, transmission substations, distribution centers, and renewable energy sites worldwide from a single admin console.



Compliance-Ready Logging

Capture privileged sessions in real time to align with NERC CIP, NIS2, NIST Cybersecurity Framework, and regional energy sector compliance mandates.

How Safous Secures Critical Infrastructure



Safous Privileged Remote Access Benefits

- ✔ No software to install on OT networks, endpoints, or control systems
- ✔ SaaS + one outbound App Gateway deploys in 3–5 business days
- ✔ Flat subscription covers all PRA, PAM, and IAM services
- ✔ Secures remote connections to isolated networks
- ✔ Protect internet-facing access points to critical OT infrastructure
- ✔ On-prem & air-gapped with Industrial Secure Remote Access

Secure Access for the Energy & Utilities Sector, Simplified

Safous provides secure, compliant remote access for IT and OT environments with a zero-trust platform specifically designed for organizations managing critical infrastructure across complex, distributed networks.

GET STARTED TODAY. →

Safous | THINK YOUR ACCESS