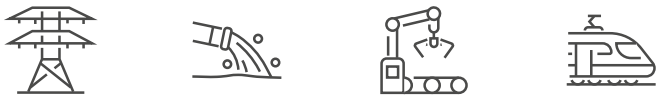
safous

Industrial Secure Remote Access for Critical Infrastructure

The ICS and OT Remote Access Challenge

Industrial Control Systems (ICS) and Operational Technology (OT) environments are the backbone of critical infrastructure – power generation, water treatment, manufacturing, and distribution systems that millions depend on. Yet securing remote access to these mission-critical systems is challenging for most organizations.



Requiring technicians to be physically present in every maintenance or emergency repair situation is impossible, as many facilities are distributed globally. Techs have to travel for hours or days, which increases costs and extends downtime. And the longer threats targeting critical infrastructure go unaddressed, the more likely they are to disrupt essential services, cause economic damage, and threaten public safety.

Safous Industrial Secure Remote Access

Safous enables secure remote access to industrial environments through:

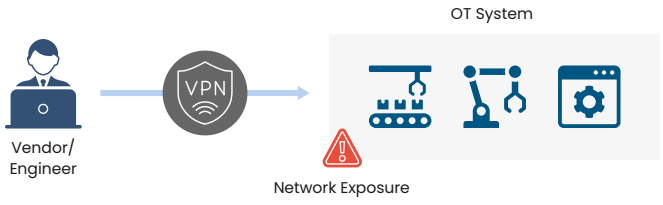
- VPN-less remote access
- Remote users never connect directly to the OT network
- Identity-based application access control
- Reduced attack surface
- Support for air-gapped environments

Why VPN and Traditional Access Fail in ICS Environments

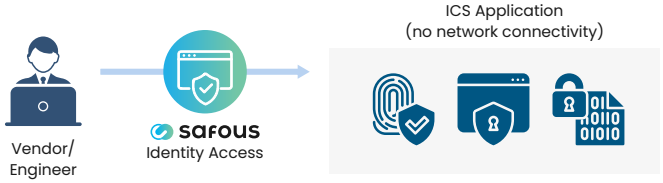
Traditional remote access methods also introduce unacceptable risk. VPN deployments flatten network architecture and expose OT networks, giving users like equipment vendors, contractors, and remote maintenance engineers broader access than they need and increasing lateral movement risk. And insider threats – whether negligent or malicious – as well as risks introduced through vendor and supply chain access can compromise systems from within.

Safous Industrial Secure Remote Access (I-SRA) reduces the attack surface in ICS and OT environments by adding identity-based and application-layer access controls. Unlike IT-focused remote access platforms or traditional VPN architectures, Safous is purpose-built to provide secure remote access where users never connect directly to the OT network.

Traditional Remote Access



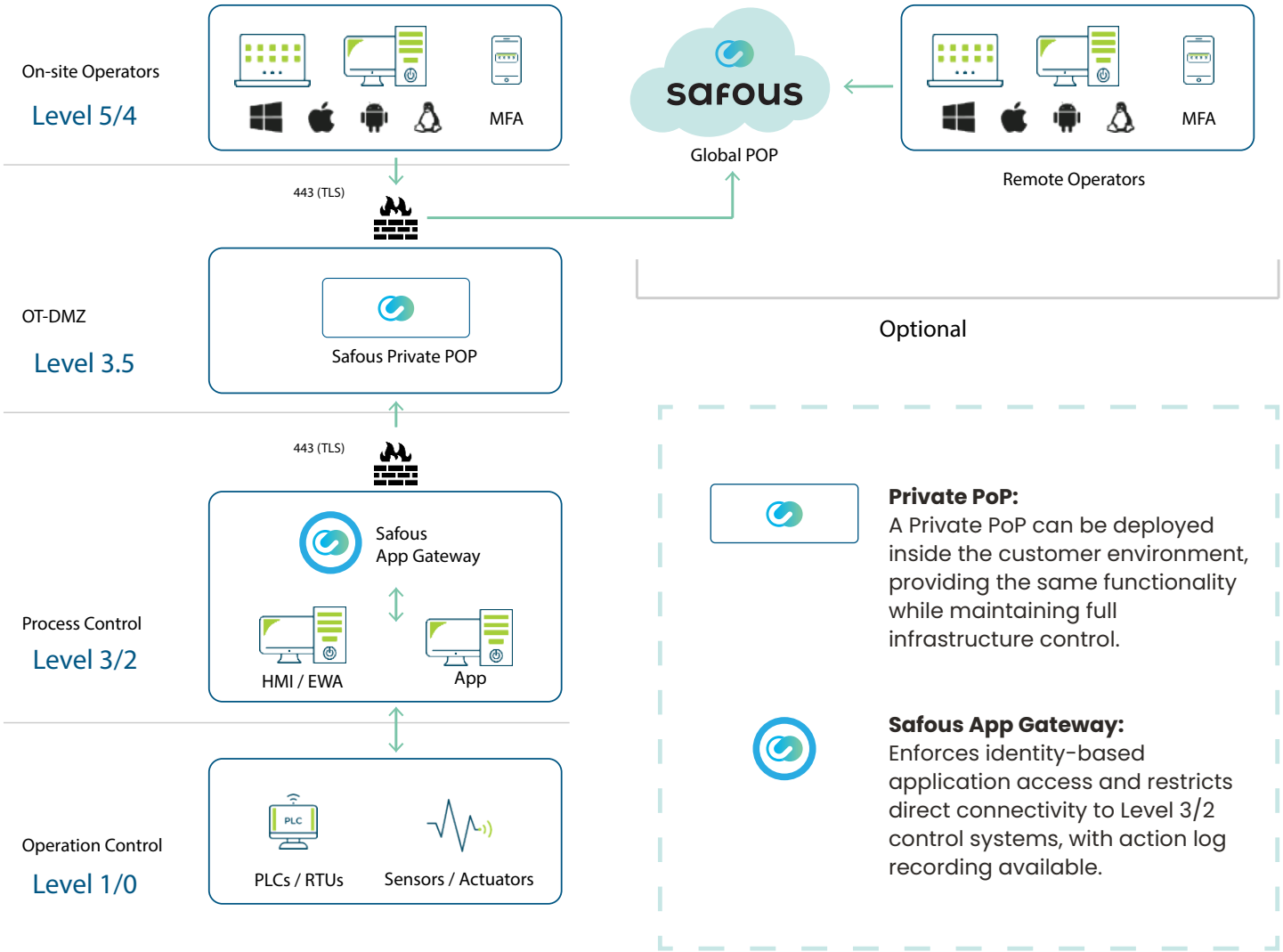
Safous Secure Access



Less than 45% of private-sector CEOs are confident in their country's ability to respond to major cyber incidents targeting critical infrastructure.

https://reports.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2026.pdf

How Safous Approaches Industrial Secure Remote Access



Private PoP:
A Private PoP can be deployed inside the customer environment, providing the same functionality while maintaining full infrastructure control.

Safous App Gateway:
Enforces identity-based application access and restricts direct connectivity to Level 3/2 control systems, with action log recording available.

Safous enforces identity-based access aligned with Purdue Model segmentation, protecting control network zones from direct external exposure and establishing a secure conduit for controlled communication between remote operators and industrial control systems. All communication is initiated outbound from the OT environment over TLS, eliminating the need to expose inbound ports.

Controlled Access to ICS Environments:
Users authenticate to Safous via identity provider integration (MFA, SSO) and receive application-layer access only to the specific ICS system they need.

No Network Exposure:
Safous does not expose inbound ports, reducing exposure to external threats by preventing users from obtaining direct network connectivity to OT networks.

Continuous Authorization & Session Control:
Safous enables IT teams to monitor sessions in real time, terminate access immediately, record session activity, and enforce action-level controls.

Reduced Attack Surface:
User access is limited to the application layer, significantly reducing the attack surface and preventing lateral movement compared to network-level or VPN-based access solutions.

Air-Gapped & On-Premises Deployment:
Safous initiates, manages, and validates sessions entirely within your environment using a hardened Docker container, operating with zero Internet dependency.

Legacy System Compatibility:
Safous eliminates operational disruptions by adding identity authentication to legacy ICS environments without requiring modification, replacement, or network re-architecture.

Deterministic Industrial Processes:
Safous security controls don't interfere with deterministic industrial processes or real-time control systems, ensuring access governance doesn't impact operational reliability.

Regulatory Compliance Support:
Session recording, audit trails, and continuous authorization help organizations align with NERC CIP, ISA/IEC 62443, NIST Cybersecurity Framework, NIST SP 800-82, and regional regulatory frameworks.

safous | THINK YOUR ACCESS

Safous provides VPN-less, identity-based access designed specifically to secure ICS and OT environments without compromising uptime, safety, or operational security – no Internet connection required.

GET STARTED TODAY.