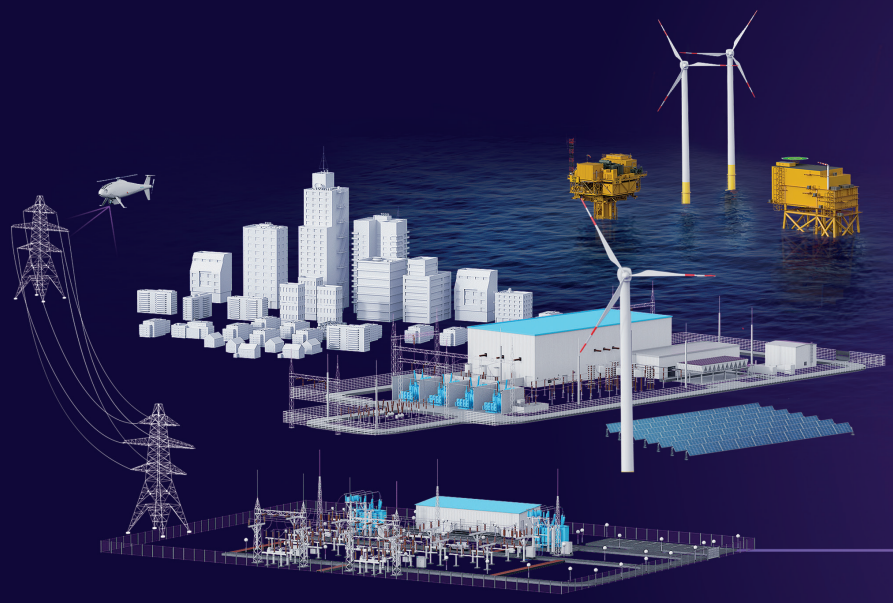
SIEMENS energy

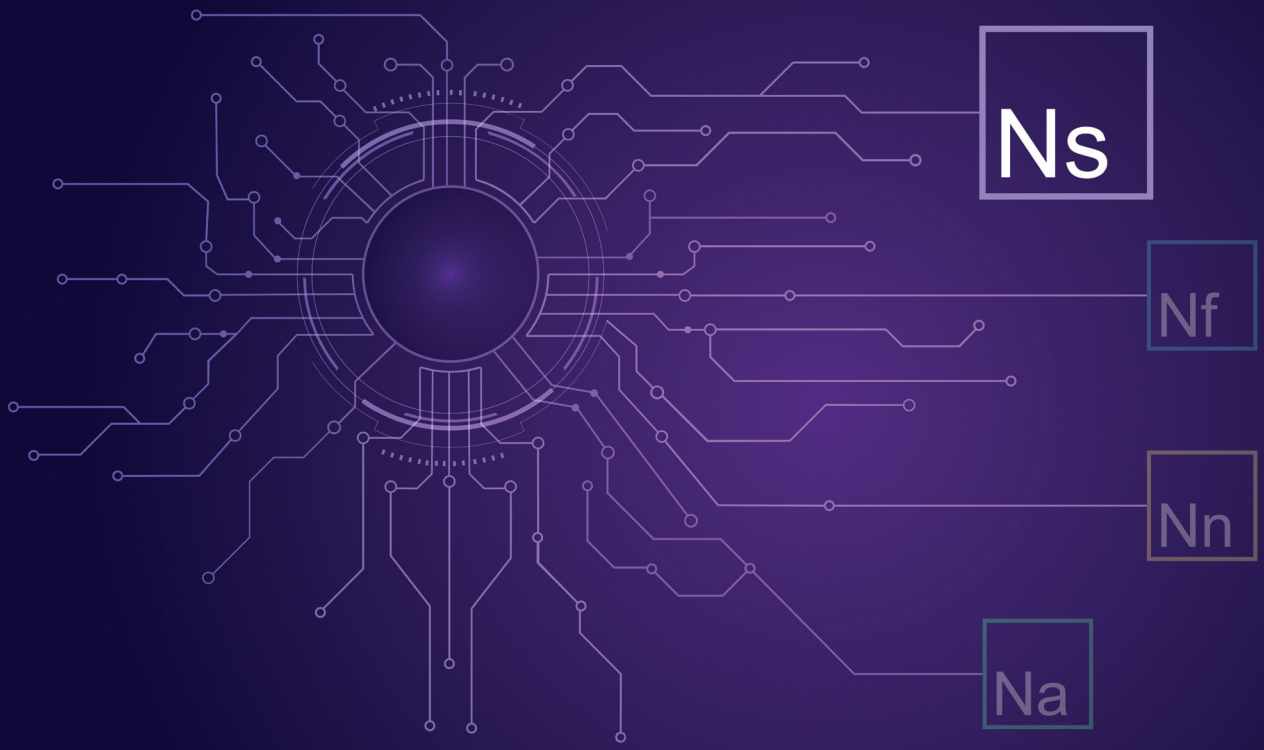
Noedra Shield suite for grid security

Standing guard over the grid.



Ns

Noedra Shield
Grid Security



The Noedra framework

Noedra is Siemens Energy's digital framework - the Mind of the Grid - connecting Grid Technologies' intelligent solutions, from sensing and control systems to software and advisory, into one coherent ecosystem.

By transforming grid data into clarity, coordination, and confident action, Noedra helps operators manage growing complexity with intelligence and control.

Each Noedra suite represents a specific way this intelligence acts across the grid.

Together, they protect, sense, structure, and guide energy systems toward a resilient future.

Shield suite – Security across the grid

Within the Noedra ecosystem, Shield provides security across the entire grid.

The Shield suite focuses on grid security, protecting OT/ICS environments, strengthening cyber-physical resilience, and ensuring regulatory compliance across substations, assets, and control infrastructures.

Connected with the other Noedra suites, Shield provides real-time situational awareness eliminating cyber-physical security blind spots - unifying visibility, protection, and control across all operational layers of the grid.

Protecting the grid in a connected world

Power grids are more connected, automated, and digitally dependent than ever before. This new reality increases exposure to cyber-physical threats, regulatory compliance requirements, and vulnerability risks - especially within OT/ICS environments.

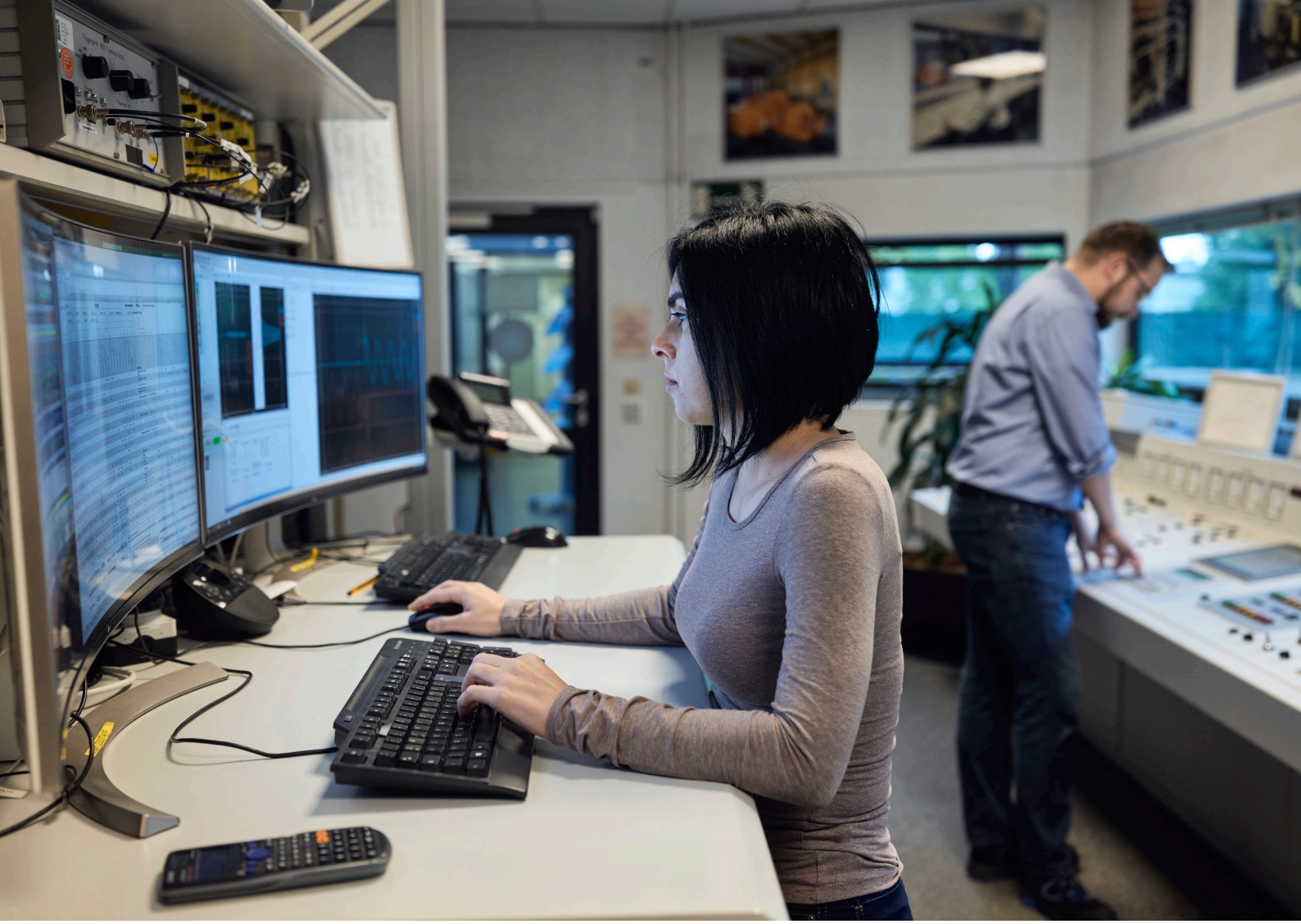
Legacy assets, siloed systems, and partial solutions impede business continuity. Control rooms and security operations centers (SOCs) need a unified cyber-physical security solution built specifically for transforming grid critical infrastructure capable of delivering real-time visibility, protection, and control, without disrupting mission-critical operations.

An effective grid cybersecurity strategy must:

- Provide a unified visualization of OT/ICS assets across all layers of the purdue OT model.
- Deliver secure remote access from the control room and SOC to the substations.
- Report compliance readiness across global cybersecurity standards.
- Identify & assess, protect, detect, respond, and recover from cyber-physical threats in real-time.

In an interconnected grid, even small, unnoticed cyber-physical incidents can escalate quickly. Latent vulnerabilities can go undetected until a crisis occurs, heightening operational and financial risks. Adhering to the NIST cybersecurity framework (CSF) - identify & assess, protect, detect, respond, and recover - helps organizations proactively minimize exposure, strengthen grid security, and ensure compliance with global standards.

The cost of inaction is high. Proactive grid security mitigates the risk of operational disruption, limits vulnerability exposure, and preserves national security and community trust of service by helping operators provide resiliency and availability.



Our offerings

Shield delivers a comprehensive, purpose-built cybersecurity ecosystem for grid operations that unifies asset visibility, threat intelligence, operational context, advisory insights, and compliance reporting into a single operational environment.

Our unified approach:

- Aggregates and visualizes OT/ICS asset, network, and security activity in one actionable view.
- Aligns cyber insights with real-time grid operations and workflows.
- Enables coordinated action across executive management, IT cybersecurity, OT cyber-physical, engineering, utility analytics data science, and compliance teams.
- Supports immediate insider and external threat detection; as well as real-time cyber AI agents for human-in-the-loop response and recover mitigation action to an attack.
- Reduces complexity while strengthening security posture.

Shield provides a grid OT cyber-physical solution that supports the full NIST CSF framework - identify, assess, protect, detect, respond, and recover from cyber vulnerabilities - to support cohesive, compliant critical infrastructure with situational awareness.

Identify & assess

OT/ICS Asset inventory and asset management

Delivers continuous visibility into all grid assets, ensuring operators always know what is deployed, how it's configured, and where risks or compliance gaps exist. It automatically discovers OT/ICS devices, tracks configuration and lifecycle changes, and links each asset to its operational and cyber physical context for smarter prioritization. The solution also delivers audit ready reporting aligned with global cybersecurity frameworks.

Risk prioritization and compliance reporting

An OT-focused approach to identifying and ranking cyber vulnerability risks by combining detailed OT/ICS device profiles, threat intelligence, compliance requirements, and operational impact. Continuous passive or active monitoring of device vulnerabilities delivers real-time, audit-ready compliance reports aligned with your organizational risk profiles and global regulatory frameworks. Dashboards highlight risk trends, configuration drift, and status.

Protect

OT Zero-touch deployment (ZTD)

Delivers the compliance requirement of secure remote access combined with human-in-the-loop controlled security policy workflows to isolate, update firmware, test, and place a device back into production - reducing operational risk of downtime, keeping devices patched, supporting operational excellence. OT ZTD reduces maintenance by allowing updates directly from the SOC while ensuring safety, accountability, and traceability.

Secure remote access

Achieve identity-based connectivity to safeguard your operations, maintain compliance, and prepare for future grid resilience without altering your current network. This solution offers outstanding flexibility, allowing easy integration with various network setups, including on-premises, hybrid, or cloud environments. Consistently enforce security policies across every network segment and record each user's access session through screen capture.

Detect

Grid insider threat detection

Defense tactic combines insider role analysis, OT/ICS asset inventory, continuous network, and grid asset monitoring to detect insider threats in real time. AI-driven analytics identify voltage tampering, line anomalies, and unauthorized access - pinpointing asset locations under attack. Automated classification differentiates malicious, negligent, and operational incidents to minimize false positives. Cyber AI agents automatically guide the SOC in response and recovery actions.

OT/ICS Network continuous monitoring

Deliver real-time, protocol-aware visibility into industrial networks, enabling operators to detect anomalies, configuration drift, and emerging cyber-physical risks early. It inspects OT communications protocols such as ICCP, DNP3, Modbus, and IEC 61850 to find deviations in commands, traffic flows, and device behavior. Automated asset discovery and network mapping create an accurate, continuously updated topology that strengthens situational awareness.

Respond

Incident response, analysis & reporting

Empowers grid operators to rapidly detect, investigate, and document cyber-physical incidents with end-to-end visibility. It correlates security events with control commands, network flows, and asset states to support deep forensic analysis and root-cause discovery. The solution captures raw data and generates automated, compliance-ready reports to streamline regulatory obligations and cross-team communication.

Threat modeling & incident mitigation

Equips utilities with cyber-physical insight and predictive intelligence to anticipate attack paths and assess their potential operational impact. It correlates telemetry, user behavior, and process commands with modeled threat scenarios to detect evolving risks early and guide prioritized mitigation. Automated playbooks provide structured, actionable response steps - from containment to configuration hardening - reducing response time and operational risk.

Recover

Incident recovery plan execution

Guides utilities from disruption back to stable OT/ICS operations by combining operational context, forensic-grade visibility, and automated recovery workflows. It maintains secure configuration backups, enables rapid rollback to trusted system states, and preserves forensic-ready evidence to support root-cause analysis and validate recovery completeness. The solution aligns recovery actions with physical process impact to ensure safe, reliable restoration without unintended operational consequences.

Why Siemens Energy

Partnering with Siemens Energy means more than just choosing a technology provider - Our value goes far beyond technology - we bring vision, reliability, and partnership to every project:

Proven expertise:

Benefit from cyber-physical security engineered for the unique operational realities of the grid, where continuous availability, safety, and real-time control take priority over traditional IT practices.

Global reach:

Leverage a unified security approach that integrates seamlessly across diverse regions and regulatory environments, ensuring consistent protection for multi vendor OT infrastructures.

Tailored solution:

Our solutions provide a unified view of grid operations - combining asset intelligence, threat detection, operational context, and compliance reporting to meet each utility's specific operational and lifecycle needs.

Trusted partnership:

Rely on Siemens Energy end-to-end support across the full cybersecurity lifecycle, helping utilities modernize the grid securely, respond effectively, and recover with confidence.

Continuous innovation:

Experience ongoing advancement in cyber-physical monitoring, AI-driven detection, and integrated OT security ecosystems delivered through advisory services, SOC integration, and managed support.

Strengthen grid security with visibility, resilience, and control.

Protect critical infrastructure across every operational layer with Noedra Shield.

Discover Siemens Energy's grid-centric cybersecurity solutions.

Published by

Siemens Energy Global GmbH & Co. KG
Grid Technologies
Siemens Promenade 9
91058 Erlangen, Germany

For more information, please visit our website:
siemens-energy.com
or contact us
E-Mail: support@siemens-energy.com
Phone: +49 911 6505 6505