

IT Architecture Consulting

Secure by Design — because retrofitting security into critical infrastructure is always too late. Renewable energy infrastructure presents a unique and systematically underestimated attack surface. The convergence of OT and IT in photovoltaic parks, wind farms, and smart grid installations creates exploitable entry points that traditional IT security frameworks are not built to address. A compromised remote access point on a solar inverter management system can cause physical disruption, regulatory breach, and reputational damage simultaneously and immediately.

600%**INCREASE**

in cyberattacks targeting energy sector infrastructure since 2020

78%**OT EXPOSURE**

of OT devices in the energy sector carry known unpatched vulnerabilities

\$8.2M**AVG COST**

of a cyberattack on critical energy infrastructure including full downtime

NIS2**MANDATORY**

energy operators are classified as essential entities under OUG 155/2024

Our Architecture Services

1

Secure by Design Networks

Communication networks designed from the ground up with security embedded at the architecture level — not retrofitted after deployment when the cost is far higher.

3

SCADA & ICS Protection

Specialized security assessment and hardening of industrial control systems and supervisory environments specific to photovoltaic and wind energy installations.

5

Encrypted Telemetry

End-to-end encryption of monitoring and control communications between field devices, data aggregators, and management platforms across the full installation.

2

OT / IT Convergence Security

We assess and harden the critical intersection of operational and information technology — where SCADA, inverter management, and corporate IT systems converge.

4

Network Segmentation

Isolation architectures that prevent lateral movement between control systems and corporate networks — a mandatory NIS2 requirement for all energy sector operators.

6

Regulatory Compliance Support

We help project developers and asset owners satisfy the security requirements of financing institutions, grid operators, and NIS2 regulatory authorities simultaneously.

Why Energy Infrastructure Is a Prime Target

Physical Consequences

A successful OT attack causes equipment damage, grid instability, and supply disruption — consequences extending far beyond any typical IT security incident in scope.

Weak OT Security Baseline

Most energy OT systems were engineered for reliability, not security. Legacy protocols, default credentials, and exposed management interfaces remain extremely common.

Regulatory Pressure Intensifying

NIS2 classifies energy operators as essential entities with the strictest compliance tier. Financing institutions increasingly require certified security postures before releasing funds.

What You Gain

A

Resilient Infrastructure

Architecture designed to absorb attacks, isolate compromised segments, and maintain critical operations — meeting NIS2 continuity requirements by design from day one.

B

Investment Protection

Certified security postures directly satisfy lender requirements, insurance underwriting criteria, and grid operator access conditions — protecting your full capital investment.

C

Long-Term Partnership

We remain your dedicated security partner through construction, commissioning, and full operational life — adapting posture as both threats and regulations evolve.

Secure your energy infrastructure from day one. Request a free architecture review. secureintel.ro