Secure IT/OT network architecture for solar power plants

An energy-sector organisation was building the IT/OT infrastructure for three solar power plant sites from the ground up. KleoSEC delivered a complete secure network architecture blueprint — segmentation, security device placement and a phased implementation roadmap — which the client adopted as the foundation for the entire build-out.

Challenge

The client was building IT and OT infrastructure for three sites from scratch and needed expert guidance so that the network would be secure by design from day one rather than patched later. They required a comprehensive architecture plan covering network segmentation, security device placement and data protection, aligned with good practice for critical infrastructure. A further condition: their integrator had to be able to implement the plan in phases without stalling the build.

Approach

01 Requirements gathering and greenfield architecture planning with the client and their integrator.

02 Threat modelling specific to energy-sector infrastructure: remote access, equipment vendors, links to control systems.

03 Full network topology design from scratch on defence-in-depth principles.

04 Firewall placement strategy and zone design: IT, OT, DMZ and control zone, with clearly defined crossings.

05 NAS and backup infrastructure positioned so that the data copy is separated from production zones.

06 Segmentation plan: VLANs, subnets and ACL rules per zone.

07 Documentation and a phased implementation roadmap the integrator can follow step by step.

Outcome

The client received a complete greenfield network architecture blueprint: a segmentation plan, a security device placement strategy and a phased implementation roadmap. The design was adopted as the foundation for the entire IT/OT infrastructure build-out, so security zones and crossing rules were built into the network from day one. The project documentation now serves the client as design evidence in conversations with auditors and insurers.

What this means for a NIS2 / ISO 27001 audit

The elements designed here are exactly what an auditor expects from every energy-sector entity. A network finding from a gap analysis is closed with the same approach, whether the network is built from scratch or an existing one is remediated.

Delivered in the project	ISO 27001:2022 Annex A	NIS2 Art. 21(2)
Threat modelling for energy infrastructure	A.5.7 threat intelligence, A.8.8	(a) risk analysis
Zones, firewalls and crossing rules	A.8.20 network security, A.8.21, A.8.22 segregation	(e) network and system security
VLAN / ACL segmentation per zone	A.8.22	(e)
Separated NAS and backup	A.8.13 backup, A.8.14 redundancy	(c) business continuity
Documentation and phased roadmap	A.5.37 documented procedures	(f) assessing effectiveness of measures

WHO WE ARE

KleoSEC is a security integrator based in Croatia: we implement the technical measures an ISO 27001 or NIS2 audit prescribes and deliver the evidence that they are in place. Certifications: OSCP+, PNPT, CNPen, eWPT, eJPT; ISA/IEC 62443 in preparation.

CONTACT

Mislav Kovač

mislav.kovac@kleosec.com

+385 99 367 7737

kleosec.com

KleoSEC d.o.o. · Kralja Zvonimira 8, 40000 Čakovec, Croatia