

DEEP INFOSEC / PUBLIC GUIDE

Smart Energy, Metering & Utility Resilience

Smart metering, energy quality, loss analysis, secure OT data and field maintenance in one operational programme.

Engineering, security and operating capability — brought together around the outcome your organisation needs.

deepinfosec.com • sales.general@deepinfosec.com

What this means for your organisation

Explore how a utility, industrial operator or campus can move from fragmented measurements to secure, actionable supervision.

Energy & minerals

Energy programmes deliver value only when measurement improves the operation of the network. We connect metering, power quality, asset health, maintenance and investment decisions in a single practical design. A first diagnostic identifies where visibility is weak; a pilot tests the instruments and dashboards; expansion then follows measured value, equipment compatibility and the ability of local teams to maintain the system.

IoT & connected systems

A connected device is part of an operational chain, not an isolated sensor. We design device identity, trusted communication, edge processing, firmware lifecycle, secure integration and maintenance around the actual use case. Whether the deployment serves a campus, fleet or utility network, the customer needs both useful data and a manageable device estate years after installation.

Industrial OT security

Industrial cybersecurity cannot disrupt the process it is meant to protect. We map safety-critical assets, maintenance windows, control-network dependencies and recovery conditions before recommending segmentation, monitoring or access changes. The engineering package gives operations and security teams a common, site-specific plan that can be tested and handed over.

Workstreams and outputs

Energy & minerals

Feasibility, design assistance, technical procurement, cybersecurity engineering and operator enablement; physical construction and electrical certification are separately contracted where applicable.

- Energy infrastructure engineering: risk and feasibility reviews for generation, distribution, remote supply, electrical dependencies and continuity objectives.
- Renewable and distributed energy: solar, storage, backup and microgrid architecture studies linked to load profiles, site constraints and procurement choices.

What you receive: Critical energy dependency and site risk map

IoT & connected systems

Device design review, integration engineering or fleet-security operations; partner hardware and protocols are assessed within the engagement.

- Embedded and connected-product security: threat models, secure boot and firmware update strategy, device identity, signing keys and lifecycle protection.
- Edge and communication: gateway architecture, segmentation, secure protocols, local failover and resilience when cloud links are unavailable.

What you receive: Device threat model and secure-design control matrix

Industrial OT security

Assessment first, architecture next, implementation under operator change authority; IEC 62443 approaches used as appropriate to the specific installation.

- Industrial discovery: inventory PLCs, HMIs, historian, SCADA, engineering workstations, remote access and process dependencies through passive or site-approved methods.
- Secure zone architecture: design Purdue-aligned segmentation, conduits, gateways, maintenance access and monitoring, avoiding assumptions that office IT controls fit plant operations.

What you receive: OT/ICS asset and communication-zone inventory

A practical engagement, from first scope to handover

01 Define the decision

We agree what must change, which systems matter, what the organisation already owns and what constitutes an acceptable outcome.

02 Evaluate on the right perimeter

A scoped assessment or pilot gives engineering teams sufficient information to choose a realistic deployment and acceptance plan.

03 Deliver with evidence

The team delivers designs, implemented controls or services, records decisions, tests outcomes and explains operating responsibilities.

04 Transfer operational capability

Documentation, knowledge transfer, maintenance pathways and follow-up are part of a sustainable programme.

Talk directly to the specialist team

Explore the full offering at deepinfosec.com and select the specialty matching your objectives. Public introductions are freely available; confidential technical and commercial dossiers follow a controlled customer process.

deepinfosec.com · sales.general@deepinfosec.com