CASE STUDY

Thales Ebbw Vale

Transmission infrastructure plays a vital role in delivering energy to millions of homes and businesses, through extensive networks. These systems transport electricity and gas from production sites to industrial facilities, storage sites, interconnectors and to consumers, forming a critical backbone of energy security.

Ensuring operational safety, reliability, and flexibility is essential, as risks like human error, system failure, or cyberattacks (highlighted by incidents such as the 2021 Colonial Pipeline attack) can cause severe disruptions.

To strengthen resilience against these evolving threats, Thales, working alongside a number of distribution partners, has set up dedicated CNI labs, advanced facilities designed to simulate realistic cyber incident scenarios across distributed industrial networks.

The labs replicate operational technology and IT environments across multiple zones, including:

- A physical replica of field infrastructure
- A live operations control room environment
- A dedicated Security Operations Centre (SOC)

This integrated setup enables teams to rehearse, test and refine cyber incident response in a safe, controlled setting. By replicating real-world operational conditions, organisations can improve detection, coordination and decision-making under pressure - enhancing business continuity, safeguarding critical infrastructure, and protecting strategic objectives.

Why Thales

Boards are often presented with in-depth assessments, strategies, or compliance mappings. While valuable, these approaches typically stop short of addressing the hardest question regulators ask: will the controls actually work in practice, without undermining safety or availability?

Advisory-heavy models tend to distance accountability. Engineering-led programmes may underweight cyber assurance. Strategy-led initiatives can struggle to demonstrate operational proof. None of these, on their own, provide boards with confidence under retrospective scrutiny.

Thales operates differently as we advise, assure, develop and engineer cyber secure and resilient solutions for ourselves and our customers using a team of cybersecurity and industrial control experts.

For electricity and gas operators, Thales enables OT cyber security that is:

- Integrated with system operation and safety
- Proportionate and defensible under scrutiny
- Validated through practice
- Sustained over the long term

THALES

Engineering resilient energy networks

Operational technology cyber security designed for Ofgem scrutiny

Delivering OT cybersecurity aligned to regulation for electricity & gas networks

Regulatory context

Ofgem's regulatory framework places increasing emphasis on system resilience, risk management and the operator's ability to justify decisions that affect the safety and continuity of electricity and gas supply. Cyber risk to OT systems is treated as a material threat to essential services, particularly where it could lead to loss of control, unsafe states, or prolonged outages.

This means that operators are assessed for the following:

- Understanding of OT system dependencies and criticality
- Have they taken proportionate, risk-based action
- Can they demonstrate preparedness and recoverability
- Are they able to maintain confidence as systems and threats evolve

How Thales can help you address Ofgem expectations

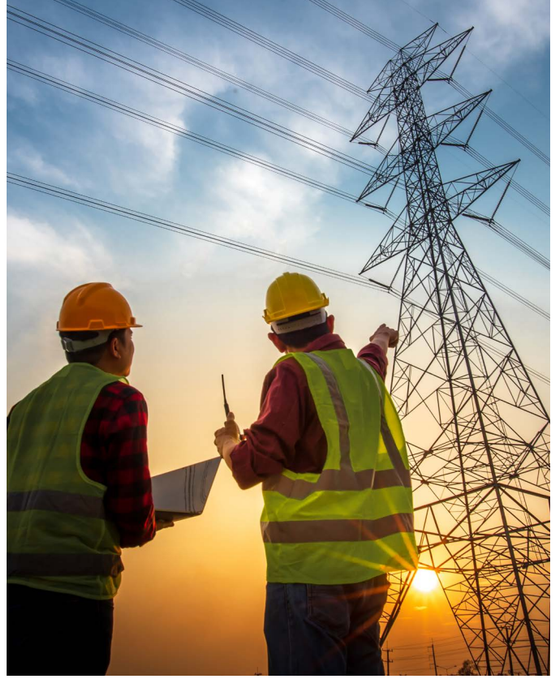
Understanding system risk and critical dependencies

Ofgem expects operators to demonstrate clear understanding of their networks and control systems, including where failures would have the greatest impact.

To address this, Thales offers the following solutions, available individually or as a package, designed to build a clear view of the current situation:

- **OT Security Assessment & Asset Discovery**
  Identifies OT assets, control systems, communication paths and operational dependencies across electricity and gas networks.
- **OT Network Architecture Assessment**
  Examines segmentation, trust boundaries and remote connectivity in relation to system stability and safety.
- **Risk & Compliance Maturity Assessment (CAF / IEC 62443 aligned)**
  Translates technical findings into Ofgem-relevant risk and resilience language.

Regulatory element addressed:
Operators must be able to evidence that they the are carrying out informed management of risks to system operation and security.



Proportionate, defensible protection of operational systems

Ofgem does not mandate specific technologies but expects controls to be appropriate to operational risk and engineering constraints.

Thales understands that organisations do not have infinite budgets so we can help prioritise controls to those areas with the highest risk or impact associated with them. Mitigating these helps improve security posture and form the basis for continuous improvement of security and resilience posture. Our solutions are as follows:

- **OT Governance, Policy & Standards Development**
  Defines how cyber risk is considered within operational and engineering decision-making, aligned to safety and resilience obligations.
- **OT Secure Remote Access**
  Provides controlled, auditable remote access for maintenance and vendor support without undermining system availability or safety.
- **OT Monitoring, Detection (IDS) & Vulnerability Management**
  Passive monitoring tailored for live OT environments, enabling early detection without operational disruption.
- **OT Backup & Restore**
  Recovery capabilities aligned to operational recovery objectives for electricity and gas systems.

Regulatory element addressed:
Controls must reduce risk without introducing new threats to system stability or safety.

THALES

Preparedness, response and recovery

Ofgem scrutiny following incidents increasingly examines whether operators were realistically prepared to respond.

It's not a question of if your systems will be penetrated, but when. When the worst does happen, it's critical that organisations have processes that work under pressure and that staff know exactly what to do. One wrong move and a bad situation can be made catastrophic. Key to responding correctly is thorough training and exercising. Thales offers the following solutions looking to ensure staff are trained to respond correctly and have experience responding under pressure to cyber incidents:

- **NCSC-aligned OT Training**
  Role-specific training for engineers, operators and decision-makers in electricity and gas environments.
- **OT Tabletop Exercises**
  Scenario-based testing of escalation, coordination and decision-making.
- **Live OT Exercising using Representative Equipment**
  Validation of response and recovery actions under realistic operating conditions.

Regulatory element addressed:
Preparedness must be demonstrable, not assumed.

Sustained assurance as networks evolve

Electricity and gas networks evolve continuously, requiring ongoing confidence in resilience. Networks and systems rarely do not stand still – new software releases, new hardware. At the same time the threat landscape is constantly changing with new exploits and attack vectors. As a result, yesterday's class-leading resilience and security is tomorrow's market laggard.

Thales offers the following solutions designed to ensure that organisations keep assessing security and ensuring that systems are resilient and secure before deployment:

- **OT Penetration Testing (OT-appropriate)**
  Assurance testing that respects safety and availability constraints.
- **OT Labs and Cyber Range Environments**
  Design, build and hosting of representative OT environments (physical and digital twins) for safe testing and change assurance.

Regulatory element addressed:
Resilience must be maintained as systems and threats change.