

Safe plants. Secure pipelines.

Industrial security, SCADA assessment, SOC, third-party access reviews and incident exercises for oil, gas and petrochemicals.

Three questions every oil and gas leader should be able to answer

Would an IT ransomware attack force us to shut down?

Mapping OT's dependencies on IT and segmenting them decides whether operations can continue.

Are our safety systems isolated?

Safety instrumented systems and their engineering workstations need the strongest protection.

Who has access during turnarounds?

Contractor devices and accounts are among the most common paths into plant networks.

May 2021

Precautionary US pipeline shutdown

2017

Safety-system-targeting malware

6 hours

Incident reporting to CERT-In

May 2027

Most DPDP obligations take effect

Built for every oil and gas company

Exploration and production companies · pipeline operators · refineries and petrochemical complexes · LNG and storage terminals · fuel retail, LPG and city gas distributors.

The rules that drive your security calendar

Instrument	Key cybersecurity expectations
CERT-In Directions · audit guidelines (2022, 2025)	6-hour reporting, 180-day logs; independent audits
NCIIPC · PNGRB · OISD	CII protection; integrity and safety standards
DPDP · standards	Consumer data safeguards; IEC 62443 and API 1164

WHAT WE DO

Industrial security, SCADA, SOC, third-party access and exercises

Industrial Security

OT inventory, segmentation, DMZ and IEC 62443-aligned reviews.

SCADA Assessment

Pipeline SCADA, RTU, DCS, historian and terminal automation reviews.

24/7 IT/OT SOC

IT and OT monitoring, threat hunting and 6-hour reporting support.

Third-Party Access Reviews

Vendor, OEM and turnaround contractor access controls.

Incident Exercises

Ransomware and OT crisis tabletops and joint drills.

Safety System Security

SIS isolation, engineering workstation and change control reviews.

Choose your starting point

Foundation

SCADA and retail automation assessment, remote access and segmentation review, policy and crisis plan. For city gas, terminals and distributors.

Assurance

Pipeline SCADA and RTU assessment, third-party access programme, annual audit, IT/OT SOC. For pipelines and mid-sized operators.

Continuous Resilience

Continuous OT testing and red teaming, safety system reviews, SOC with hunting, Board reporting. For refineries and E&P majors.

Why Codec Networks

CERT-In empanelled

for information security auditing services, and empanelled with NISCI for application audit services.

Certified

ISO 9001:2015, ISO/IEC 27001:2022 and ISO/IEC 20000-1:2018.

Regulation-mapped

Every finding mapped to CERT-In, NCIIPC, PNGRB and OISD expectations and IEC 62443.

One connected partner

Testing, audits, SOC, forensics and privacy linked from finding to closure.

Book a scoping session

Share your assets, control systems and contractors. We will propose a practical, safety-aware assessment and assurance plan.

New Delhi: 507, 5th Floor, New Delhi House, Barakhamba Road, Connaught Place – 110001

Gurugram: 707, 7th Floor, Silverton Tower, Golf Course Extension Road, Sector 50 – 122018

Call: 011 430 496 96 · +91 99716 76124 · +91 88007 88220

Email: mktg@codecnetworks.com · www.codecnetworks.com

Regulatory references reflect public instruments as of October 2026; applicability depends on each entity's licence, category and activities. Services support risk reduction and assurance and do not guarantee prevention of all incidents or regulatory compliance. Sources: public reporting, CERT-In, MeitY. Confirm obligations against the official instruments.