

Codec Networks
Coding Threats. Decoding Solutions.

INDUSTRY BROCHURE · OIL, GAS & PETROCHEMICALS

Safe Operations. Secure Control.

Industrial security, SCADA assessment, SOC, third-party access reviews and incident exercises for refineries, exploration companies, pipelines, LNG terminals and fuel distributors.

- Industrial Security
- SCADA Assessment
- 24/7 IT/OT SOC
- Third-Party Access Reviews
- Incident Exercises
- Safety System Security

THE CHALLENGE

In oil and gas, a cyber incident can become a safety incident.

Refineries, pipelines and terminals run hazardous processes through DCS, SCADA and safety instrumented systems, often supported by contractors and vendors. Major incidents worldwide—from the 2021 Colonial Pipeline shutdown to attacks on safety systems—show what is at stake.



What keeps leadership teams awake

- Ransomware forcing precautionary shutdowns
- Attacks on safety instrumented systems
- Pipeline SCADA and remote site compromise
- Contractor and vendor access during turnarounds
- Destructive malware on corporate networks
- CERT-In, NCIIPC and safety obligations

May 2021
Ransomware led to a precautionary US pipeline shutdown

2017
Malware targeted a petrochemical plant's safety system

6 hours
To report cyber incidents to CERT-In

May 2027
Most DPDP obligations take effect

The rulebook has changed

Instrument	What it means for you
CERT-In Directions and audit guidelines (2022, 2025)	6-hour incident reporting, 180-day logs; risk-based independent cyber audits
NCIIPC (IT Act Section 70A)	Protection of systems notified as critical information infrastructure in the energy sector
PNGRB and OISD	Technical, integrity and safety standards for pipelines, refineries and installations that cyber risk can affect
DPDP · international standards	Consumer data safeguards from May 2027; IEC 62443 and API 1164 good practice

OUR SERVICE OFFERINGS

One partner from wellhead to retail outlet

Built around our primary proposition for the sector: **industrial security, SCADA assessment, SOC, third-party access reviews and incident exercises.**

Industrial Security

- OT asset inventory and architecture review
- IT/OT segmentation and DMZ design
- IEC 62443-aligned assessments
- OT endpoint and removable media controls

SCADA Assessment

- Pipeline SCADA and RTU assessments
- DCS and historian reviews
- Terminal and tank-gauging automation
- Safe, passive OT testing

24/7 IT/OT SOC

- IT and OT monitoring
- Industrial protocol threat detection
- Threat hunting for destructive and state actors
- 6-hour CERT-In reporting support

Third-Party Access Reviews

- Vendor and OEM remote access brokering
- Contractor access for turnarounds
- Supplier security assessments
- Access recertification

Incident Exercises

- Ransomware and OT crisis tabletop exercises
- Joint drills with operations and safety teams
- Recovery and restart planning
- Crisis communication rehearsals

Safety System Security

- Safety instrumented system isolation reviews
- Engineering workstation controls
- SIS change management review
- Integration with process safety management

Who we serve: exploration and production companies · pipeline operators · refineries and petrochemical complexes · LNG and storage terminals · fuel retail, LPG and city gas distributors.

BUNDLED SERVICE MODELS

Packaged for how oil and gas companies buy

Eleven Codec Networks bundles apply directly to oil, gas and petrochemical companies:

- **B1** Cyber Assessment & VAPT Assurance
- **B2** Application, API & DevSecOps Security
- **B3** Cloud, Infrastructure & Zero Trust
- **B4** Regulatory Cyber Audit & Compliance
- **B5** GRC, ISO, SOC 2 & PCI DSS Maturity
- **B6** Data Privacy & DPDPA Program
- **B7** Managed SOC, MDR & Threat Monitoring
- **B8** Forensics, Incident Response & Malware RCA
- **B9** Third-Party & Supply-Chain Risk
- **B10** Cyber Simulation, Awareness & Tabletop
- **B11** Emerging Tech, AI & Web3 Security

Foundation

City gas, terminals and distributors

- SCADA and retail automation assessment
- Remote access review
- OT segmentation review
- Policy and crisis plan pack

Assurance

Pipelines and mid-sized operators

- Pipeline SCADA and RTU assessment
- Third-party access programme
- Annual independent audit
- 24x7 IT/OT SOC

Continuous Resilience

Refineries, petrochemicals and E&P majors

- Continuous OT testing and red teaming
- Safety system security reviews
- SOC with threat hunting
- Board and regulator reporting

Mapped to your obligations

Requirement	How we help	Bundle
Cyber incidents to CERT-In within six hours; 180-day logs (CERT-In Directions)	IT/OT SOC, IR retainer and reporting support	B7, B8
Risk-based independent cyber audits (CERT-In audit guidelines, 2025)	Independent IT/OT audits	B4, B1
Protection of notified critical information infrastructure (NCIIPC)	CII-aligned assessments and controls	B4, B3
Pipeline integrity and safety standards (PNGRB, OISD)	OT and safety system security reviews	B1, B5
Third-party and contractor controls	Third-party access programme	B9, B3
Consumer data in retail, LPG and city gas (DPDP)	DPDPA programme	B6
Card payments at fuel stations (PCI DSS)	Retail payment security review	B2, B5

THE CODEC NETWORKS VALUE ADD

Why oil and gas companies choose Codec Networks

CERT-In empanelled
Independent IT/OT audits recognised by regulators.

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

Safety-aware OT methods
Passive discovery and planned testing coordinated with operations and safety teams.

Standards-mapped
Findings mapped to CERT-In, NCIIPC, IEC 62443 and API 1164 good practice.

Full stack, one partner
IT/OT testing, SOC, forensics and exercises connected from finding to closure.

Certified experts
CISA, ISO 27001 LA/LI, CEH, OSCP and CHFI professionals.

How we engage

Discover & scope
Assets and sites, DCS, SCADA and safety systems, contractors and vendors, retail networks and your audit calendar.

Assess & test
Threat-led testing and regulatory audits executed by certified specialists.

Report in business terms
Findings, risk ratings and a compliance gap matrix for the Board and regulators.

Remediate
Practical, prioritised fixes with technology and compliance teams.

Validate & prove
Retesting and an evidence tracker for auditors, regulators and partners.

Monitor & improve
Managed SOC, recurring testing and quarterly governance reviews.

What you receive: executive summary for the Board or its committee · technical findings with evidence and CVSS ratings · compliance gap matrix · prioritised remediation roadmap · retest reports · audit evidence tracker · SOC dashboards and MTTD/MTTR metrics.



START WITH A SCOPING SESSION

Let's make your next turnaround, audit and incident a non-event.

Tell us 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, New Delhi – 110001

Gurugram

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

Call

011 430 496 96 · 011 437 522 99
+91 99716 76124 · +91 88007 88220 · +91 88003 31124

Write

mktg@codecnetworks.com
www.codecnetworks.com

Codec Networks

Coding Threats. Decoding Solutions.

Secure Today. Innovate Tomorrow. Regulatory references reflect public instruments as of October 2026; applicability depends on each entity's licence, category and activities. Packages are proposed groupings of Codec Networks bundles, finalised through scoping. 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.