Codec Networks

Coding Threats. Decoding Solutions.

OIL, GAS & PETROCHEMICALS

Safe Operations. Secure Control.

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



What we will cover

The sector and its risks

Scale, players and the threats that matter most

What regulators now expect

CERT-In, NCIIPC, PNGRB and OISD expectations and IEC 62443

How Codec Networks helps

Services, bundles and packages built for the sector

Proof in scenarios

Five new case studies and the controls that break the chain

Why Codec Networks and next steps

Our value add and how to start



Cyber incidents in oil and gas can stop supply

Global incidents show the operational and safety stakes

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

What this means: oil and gas companies must separate OT from IT, protect safety systems, control contractor and vendor access, monitor IT and OT around the clock and report incidents within six hours.

Sources: public reporting, CERT-In, MeitY.

Who we serve across oil, gas and petrochemicals

Exploration and production

Onshore and offshore fields

Pipeline operators

Crude, product and gas

Refineries

Refining complexes

Petrochemicals

Chemical complexes

LNG and storage terminals

Regasification and tank farms

Fuel retail

Retail outlets and automation

LPG and city gas

Bottling and distribution

EPC and contractors

Projects and turnarounds

The threats that cost oil and gas the most

Six priorities from our 18-threat oil and gas assessment



Ransomware shutdowns

IT incidents stopping operations



Safety system attacks

Tampering with SIS



Pipeline SCADA compromise

Remote sites and RTUs



Contractor access

Turnaround laptops and accounts



Destructive malware

Wiped workstations and data



Slow detection & reporting

Missing the 6-hour window

Attacks target every stage from wellhead to retail outlet

Where Cyber Risk Sits Across the Oil and Gas Value Chain

Every stage from wellhead to retail outlet carries its own attack surface

Upstream	Midstream pipelines	Refining & petrochemicals	Terminals & storage	Distribution & retail	Corporate IT & trading
SYSTEMS Wellhead controls, offshore platforms, seismic data	**SYSTEMS** Pipeline SCADA, RTUs, leak detection	**SYSTEMS** DCS, SIS, analysers, historians	**SYSTEMS** Tank gauging, loading automation	**SYSTEMS** Retail automation, payments, LPG systems	**SYSTEMS** ERP, billing, trading, email
TYPICAL ATTACKS Process disruption, data theft	**TYPICAL ATTACKS** Remote shutdown, manipulated readings	**TYPICAL ATTACKS** Safety system tampering, plant outages	**TYPICAL ATTACKS** Overfill risk, inventory fraud	**TYPICAL ATTACKS** Payment fraud, outage at pumps	**TYPICAL ATTACKS** Ransomware, BEC, operational dependency

In hazardous industries, OT security and process safety are inseparable.

Source: Codec Networks analysis

Codec Networks

What regulators now expect

CERT-In, NCIIPC, PNGRB and OISD expectations and IEC 62443

Codec Networks
Coding Threats. Decoding Solutions.

The rules and standards shaping oil and gas cybersecurity

Requirement	Frequency / deadline	Source
Cyber incident reporting	To CERT-In within 6 hours	CERT-In Directions, 2022
ICT log retention	180 days, in India	CERT-In Directions, 2022
Independent cyber audits	Risk-based	CERT-In audit guidelines, 2025
Critical information infrastructure	Per notification	NCIIPC (IT Act Section 70A)
Pipeline technical and integrity standards	Per regulations	PNGRB
Installation safety standards	Per standard	OISD
Consumer personal data	Most obligations from May 2027	DPDP Act 2023 and Rules 2025
Industrial security good practice	Standards	IEC 62443; API 1164

Key dates on the regulatory timeline

Regulatory and Standards Timeline Shaping Oil and Gas Cybersecurity

Cross-sector instruments and industry standards

In force Upcoming (from Oct 2026)

2006	PNGRB Act establishes the Petroleum and Natural Gas Regulatory Board
2008	IT Act amendment establishes protection of critical information infrastructure (Section 70A)
Apr 2022	CERT-In Directions: 6-hour incident reporting, 180-day ICT logs in India
Aug 2023	Digital Personal Data Protection Act, 2023 enacted
Jul 2025	CERT-In Comprehensive Cyber Security Audit Policy Guidelines
Nov 2025	DPDP Rules, 2025 notified with phased commencement
May 2027	**Most DPDP Rules obligations, incl. breach intimation, take effect**

Sources: PNGRB, CERT-In, MeitY. Confirm obligations against the official instruments.

Codec Networks

How Codec Networks helps

Industrial security · SCADA · IT/OT SOC · Third-party access · Exercises · Safety systems

Codec Networks
Coding Threats. Decoding Solutions.

One partner from wellhead to retail outlet

Industrial Security

OT inventory, segmentation, IEC 62443

SCADA Assessment

Pipelines, RTUs, DCS, terminals

24/7 IT/OT SOC

Monitoring and threat hunting

Third-Party Access Reviews

Vendors, OEMs, contractors

Incident Exercises

Ransomware and OT crisis drills

Safety System Security

SIS isolation and change control

Eleven bundles from the Codec Networks catalogue

Business-ready bundles instead of 180 separate services

- **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

Bundle numbers follow the Codec Networks Bundled Service Models. Scope, frequency and pricing are confirmed during scoping.

Three packages, sized to where you are

Foundation

City gas, terminals and distributors

- SCADA and retail assessment (B1, B2)
- Remote access review (B3)
- OT segmentation review (B3)
- Policy and crisis plan (B5)

Assurance

Pipelines and mid-sized operators

- Pipeline SCADA assessment (B1)
- Third-party access programme (B9)
- Annual independent audit (B4)
- 24x7 IT/OT SOC (B7)

Continuous Resilience

Refineries, petrochemicals and E&P majors

- OT testing and red teaming (B1, B10)
- Safety system reviews (B1, B5)
- SOC with threat hunting (B7)
- Board and regulator reporting (B5)

Every obligation mapped to a bundle

Requirement	How Codec Networks helps	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

Five new case studies, five broken chains

Illustrative composite scenarios written for 2026—not client engagements

1	**The Pipeline That Stopped for an IT Attack**	IT ransomware forces a precautionary shutdown; dependency mapping prevents it	**B3 · B7 · B10**
2	**The Safety System Somebody Reprogrammed**	Attackers reach SIS controllers; isolation and monitoring stop them	**B1 · B7 · B8**
3	**The Contractor Laptop on the Refinery Network**	Turnaround malware spreads to operator stations; device controls prevent it	**B9 · B3 · B7**
4	**The Fuel Station Network Payment Fraud**	Stolen remote-management access alters prices; MFA and testing prevent it	**B2 · B3 · B7**
5	**The Wiper on the Exploration Company's Network**	Destructive malware wipes workstations; PAM and offline backups limit it	**B3 · B7 · B10**

Example: breaking an IT-to-operations shutdown chain

Case 1: The Pipeline That Stopped for an IT Attack

ILLUSTRATIVE ATTACK PATH

Step 1
Ransomware encrypts a pipeline operator's billing and IT systems

→

Step 2
OT is not directly hit, but operations depend on IT

→

Step 3
Pipeline is shut down as a precaution

→

Step 4
Fuel supply to a region is disrupted

→

Step 5
Recovery, reporting and public scrutiny

WHERE CONTROLS BREAK THE CHAIN

- Mapping of OT dependencies on IT systems
- IT/OT segmentation and independent OT operation
- Immutable backups and tested recovery
- Crisis exercises with operations teams

Illustrative composite scenario prepared by Codec Networks. Not a client engagement.

Codec Networks

What we test: which operational processes depend on IT systems, IT/OT segmentation and DMZ design, the ability to run OT independently, immutable backups and recovery times, and crisis decision-making in a tabletop exercise.

Why oil and gas companies choose Codec Networks

CERT-In empanelled

For information security auditing services; NICSI empanelled for application audits

Certified

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

Regulation-mapped

Mapped to CERT-In, NCIIPC, PNGRB and OISD expectations and IEC 62443

Tests the whole chain

Technical, process and monitoring tests together

Full stack, one partner

VAPT, audits, SOC, forensics, privacy and Board advisory connected

Specialist experts

CEH, OSCP, CPENT, CISA, ISO 27001 LA/LI, CHFI; OWASP, MITRE ATT&CK, NIST



How we deliver, and what you receive

Codec Networks Delivery Methodology

Nine stages, from scoping to continuous improvement



Source: Codec Networks project and service delivery methodology

Codec Networks

- Executive summary for the Board or its committee
- Technical findings with evidence and CVSS ratings
- Compliance gap matrix mapped to your obligations
- Prioritised remediation roadmap and retest reports
- Audit evidence tracker for regulators and partners
- SOC dashboards with MTTD and MTTR metrics

Let's start with a scoping session

1 Scoping session

Assets, control and safety systems, contractors, retail networks and audit calendar

2 Proposal

Regulation-mapped scope, methodology, timeline and deliverables

3 Kick-off

Testing, audit or SOC onboarding, with Board-ready reporting

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

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

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.

Codec Networks
Coding Threats. Decoding Solutions.