

Codec Networks
Coding Threats. Decoding Solutions.

INDUSTRY BROCHURE · CHEMICALS, FERTILIZERS & PROCESS INDUSTRIES

Keep the Process Safe. Keep the Plant Running.

OT risk assessments, industrial network security, SOC, recovery and vendor access reviews for chemical plants, fertilizer producers, agrochemical companies and industrial process operators.

- OT Risk Assessment
- Industrial Network Security
- 24/7 IT/OT SOC
- Recovery & Resilience
- Vendor Access Reviews
- Safety System Security

THE CHALLENGE

In process industries, a cyber incident can become a safety incident.

Chemical and fertilizer plants run hazardous continuous processes through DCS, PLCs and safety instrumented systems, often maintained remotely by vendors and contractors. The TRITON attack on a petrochemical plant's safety system (2017), ransomware that halted Symrise (2020) and the Brenntag extortion (2021) show what is at stake—and fertilizer producers also depend on ERP and subsidy systems to keep selling.



What keeps leadership teams awake

- Ransomware halting continuous processes
- Tampering with set-points and safety systems
- Vendor and contractor remote access to the DCS
- ERP and subsidy or billing disruption in season
- Theft of formulations and process know-how
- CERT-In, safety regulators and customer audits

2017
TRITON malware targeted a petrochemical plant's safety system

1,000
Devices encrypted when ransomware halted Symrise (2020)

US$4.4 m
Ransom paid by chemical distributor Brenntag (2021)

6 hours
To report cyber incidents to CERT-In

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 covering IT and OT/ICS
Factories Act · MSIHC Rules · PESO	Safety duties for hazardous plants and storage that cyber incidents affecting control and safety systems can undermine
Fertiliser (Control) Order · DBT · SEBI LODR	Fertilizer quality, pricing and subsidy obligations tied to PoS and ERP data; quarterly cyber incident disclosure for listed companies
DPDP · standards	Farmer, dealer and employee data safeguards from May 2027; IEC 62443, IEC 61511 and ISO/IEC 27001 good practice

OUR SERVICE OFFERINGS

One partner from reactor to dealer

Built around our primary proposition for the sector: **OT risk assessments, industrial network security, SOC, recovery and vendor access reviews.**

OT Risk Assessment

- DCS, PLC, SIS and historian assessments
- IEC 62443 and IEC 61511-aware gap analysis
- Safe, passive testing planned with operations
- Tank farm, loading and utilities automation reviews

Industrial Network Security

- IT/OT architecture and plant DMZ design
- Zone-and-conduit segmentation
- Removal of flat and dual-homed networks
- IIoT and plant-to-cloud isolation

24/7 IT/OT SOC

- IT and plant network monitoring
- Industrial protocol threat detection
- Engineering and remote-session monitoring
- 6-hour CERT-In reporting support

Recovery & Resilience

- Immutable backups of ERP, DCS configurations and logic
- Manual-operation and restart playbooks
- Subsidy, billing and dispatch continuity planning
- Plant crisis exercises with safety teams

Vendor Access Reviews

- Brokered OEM and integrator remote access
- Contractor controls for turnarounds
- Supplier and logistics partner assessments
- Access recertification

Safety System Security

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

Who we serve: fertilizer producers · bulk and commodity chemical makers · specialty chemicals and CDMOs · agrochemical companies · paints, coatings, industrial gases and materials · industrial process operators.

BUNDLED SERVICE MODELS

Packaged for how chemical and fertilizer companies buy

Eleven Codec Networks bundles apply directly to chemical, fertilizer and process industry 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

Single plants, formulators and distributors

- IT and plant OT assessment
- Vendor remote access review
- Backup and recovery review
- Policy, media and crisis plan pack

Assurance

Multi-plant specialty and agrochemical companies

- IEC 62443 assessment and segmentation
- ERP, LIMS and dealer portal testing
- Annual independent audit
- 24x7 IT/OT SOC

Continuous Resilience

Fertilizer majors, PSUs and bulk chemical groups

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

Mapped to your obligations

Requirement	How we help	Bundle
Incidents to CERT-In in six hours; 180-day logs (CERT-In Directions)	IT/OT SOC, IR retainer, reporting support	B7, B8
Independent cyber audits incl. OT/ICS (CERT-In guidelines, 2025)	Independent IT/OT audits	B4, B1
Notified protected systems (NCIIPC)	CII-aligned assessments and controls	B4, B3
Hazardous plant and storage safety (Factories Act, MSIHC, PESO)	SIS and OT security reviews	B1, B5
Fertilizer subsidy and PoS data integrity (DBT, FCO)	ERP and integration security, continuity	B2, B3
Quarterly incident disclosure, listed companies (SEBI LODR)	Incident records, disclosure support	B4, B8
Farmer, dealer and employee data (DPDP)	DPDPA programme	B6

THE CODEC NETWORKS VALUE ADD

Why chemical and fertilizer companies choose Codec Networks

CERT-In empanelled

Independent IT/OT audits recognised by regulators and customers.

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 process safety teams.

Standards-mapped

Findings mapped to IEC 62443, IEC 61511, ISO/IEC 27001 and CERT-In expectations.

Full stack, one partner

OT testing, SOC, forensics, vendor risk and exercises connected from finding to closure.

Certified experts

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

How we engage

Discover & scope

Plants and units, DCS, PLCs and safety systems, vendors and contractors, ERP, LIMS and subsidy integrations, dealers 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 plants, control systems, vendors and business systems. 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 on TRITON, Symrise and Brenntag, CERT-In. Confirm obligations against the official instruments.