

Codec Networks
Coding Threats. Decoding Solutions.

CHEMICALS, FERTILIZERS & PROCESS INDUSTRIES CYBERSECURITY

Safe process. Secure plant.

OT risk assessments, industrial network security, SOC, recovery and vendor access reviews for chemicals, fertilizers and process industries.

Three questions every chemical and fertilizer leader should be able to answer

Could someone change a set-point from outside?
Vendor remote access and flat networks are the most common paths to the DCS and the safety system.

If ERP went dark, could we dispatch and claim?
Dispatch, billing and subsidy reconciliation depend on IT; manual playbooks and tested backups decide the outcome.

Who controls contractors during turnarounds?
Contractor devices and USB media are among the most common ways malware reaches plant networks.

2017
TRITON targeted a safety system

1,000
Devices encrypted at Symrise (2020)

US$4.4 m
Brenntag ransom (2021)

6 hours
Incident reporting to CERT-In

Built for every chemical and fertilizer company

Fertilizer producers · bulk and commodity chemical makers · specialty chemicals and CDMOs · agrochemical companies · paints, coatings, industrial gases and materials · industrial process operators.

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 incl. OT
Factories Act · MSIHC · PESO · FCO	Safety and fertilizer obligations that depend on secure control and business systems
SEBI LODR · DPDP · standards	Quarterly disclosure (listed); farmer and dealer data; IEC 62443, IEC 61511

WHAT WE DO

OT risk, industrial networks, SOC, recovery, vendors and safety systems

OT Risk Assessment
DCS, PLC, SIS, historian and tank-farm assessments with safe, passive methods.

Industrial Network Security
Plant DMZ, zone-and-conduit segmentation, IIoT isolation.

24/7 IT/OT SOC
IT and plant monitoring, remote-session detection, 6-hour reporting.

Recovery & Resilience
Backups, manual-operation playbooks, subsidy and dispatch continuity.

Vendor Access Reviews
OEM, integrator, contractor and logistics partner access controls.

Safety System Security
SIS isolation, engineering workstation and change control reviews.

Choose your starting point

Foundation
IT and plant OT assessment, vendor remote access review, backup and recovery review, policy and crisis plan. For single plants, formulators and distributors.

Assurance
IEC 62443 assessment and segmentation, ERP, LIMS and dealer portal testing, annual audit, IT/OT SOC. For multi-plant specialty and agrochemical companies.

Continuous Resilience
Continuous OT testing and red teaming, safety system reviews, SOC with hunting, Board and regulator reporting. For fertilizer majors, PSUs and bulk chemical groups.

Why Codec Networks

CERT-In empanelled
for information security auditing services, and empanelled with NICSI 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 and safety-regulator expectations, IEC 62443 and IEC 61511.

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

Book a scoping session

Share 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 – 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 on TRITON, Symrise and Brenntag, CERT-In. Confirm obligations against the official instruments.