

Codec Networks

Coding Threats. Decoding Solutions.

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, fertilizer and process industry companies

Coding Threats. Decoding Solutions. · www.codecnetworks.com



What we will cover



The sector and its risks

Scale, players and the threats that matter most



What regulators now expect

CERT-In, NCIIPC, safety regulators, the Fertiliser Control Order and DPDP



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 process industries stop plants and threaten safety

Global incidents show the operational and safety stakes

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

What this means: chemical and fertilizer companies must separate the plant from IT, protect safety systems, control vendor and contractor access, make ERP and subsidy systems recoverable, monitor IT and OT around the clock and report incidents within six hours.

Sources: public reporting on TRITON, Symrise and Brenntag, CERT-In.

Who we serve across chemicals, fertilizers and process industries



Fertilizer producers

Urea, DAP, NPK, PSUs and cooperatives



Bulk and commodity chemicals

Chlor-alkali, soda ash, acids, polymers



Specialty chemicals and CDMOs

Intermediates, performance chemicals



Agrochemicals

Crop protection, formulations



Paints and coatings

Decorative and industrial coatings



Industrial gases and materials

Gases, adhesives, advanced materials



Process operators

Contract and toll manufacturing



Distributors and dealers

Chemical distribution, dealer networks

The threats that cost chemical and fertilizer companies the most

Six priorities from our 18-threat sector assessment



Ransomware shutdowns

Continuous processes and ERP stopped



Safety and set-point tampering

DCS and SIS reached from outside



Vendor and contractor access

Standing VPNs and turnaround devices



Subsidy and billing disruption

ERP and DBT integrations down in season



Formulation and IP theft

Recipes and process know-how



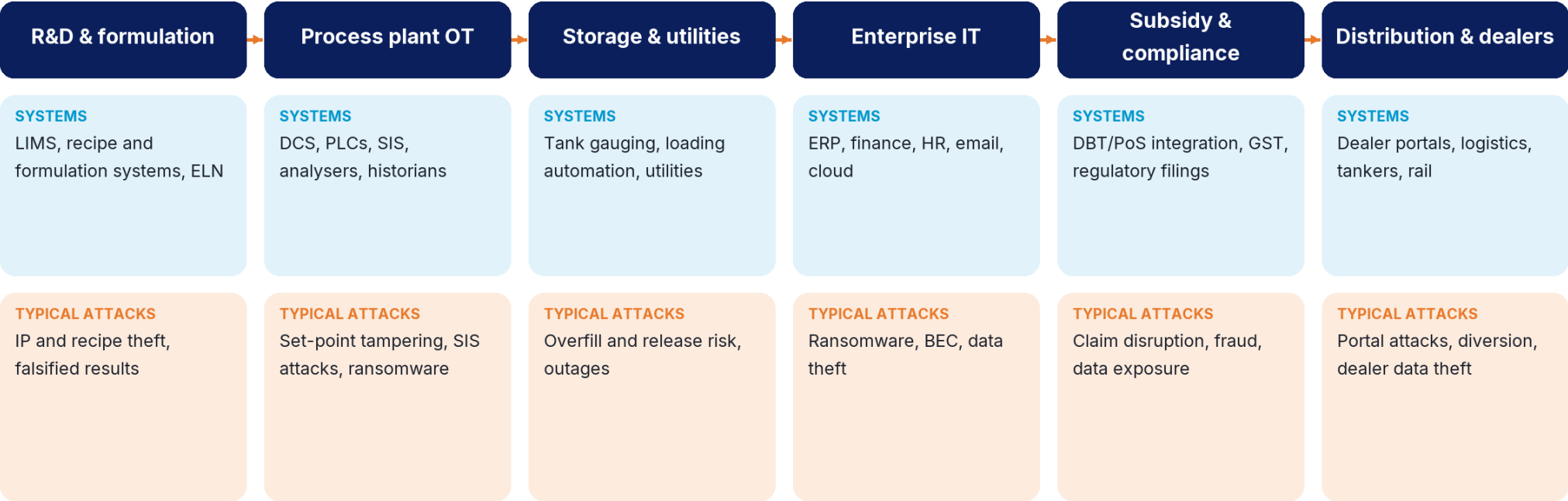
Slow detection & reporting

Missing the 6-hour window

Attacks target every stage from R&D to the dealer

Where Cyber Risk Sits Across the Chemical and Fertilizer Value Chain

Every stage from R&D to the dealer carries its own attack surface



In process industries, OT security and process safety are inseparable—and a plant that cannot bill its subsidy cannot keep selling.

Source: Codec Networks analysis

Codec Networks

What regulators now expect

CERT-In, NCIIPC, safety regulators, the Fertiliser Control Order and DPDP

The rules and standards shaping chemical and fertilizer 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, incl. OT/ICS	CERT-In audit guidelines, 2025
Protected systems	Per notification	NCIIPC (IT Act Section 70A)
Hazardous plant and storage safety	Continuous duties	Factories Act 1948; MSIHC Rules 1989; PESO
Fertilizer quality, pricing and subsidy data	Per order and DBT scheme	Fertiliser (Control) Order 1985; DBT
Cyber incident disclosure (listed companies)	Quarterly corporate governance report	SEBI LODR, 2023
Farmer, dealer and employee data	Most obligations from May 2027	DPDP Act 2023 and Rules 2025
Industrial and safety system security good practice	Standards	IEC 62443; IEC 61511

Key dates on the regulatory timeline

Regulatory and Standards Timeline Shaping Chemical and Fertilizer Cybersecurity

Safety, sector and cross-sector instruments and the standards that connect them

● In force ● Upcoming (from Oct 2026)

1948	● Factories Act, 1948: safety duties for hazardous process plants
1985	● Fertiliser (Control) Order under the Essential Commodities Act
1989	● Manufacture, Storage and Import of Hazardous Chemical Rules under the Environment (Protection) Act
2000	● Information Technology Act, 2000; Chemical Weapons Convention Act, 2000
2008	● IT Act amendment: CERT-In and critical information infrastructure (Section 70A)
2016–18	● Direct Benefit Transfer in fertilizers rolled out through Aadhaar-authenticated PoS devices at retailers
Apr 2022	● CERT-In Directions: 6-hour incident reporting, 180-day ICT logs in India
Jul 2023	● SEBI LODR amendment: listed companies disclose cyber incidents quarterly
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: MeitY, CERT-In, SEBI, Department of Fertilizers, MoEFCC. Confirm obligations against the official instruments.

Codec Networks

How Codec Networks helps

OT risk · Industrial networks · IT/OT SOC · Recovery · Vendor access · Safety systems

One partner from reactor to dealer



OT Risk Assessment

DCS, PLCs, SIS, historians, tank farms



Industrial Network Security

Plant DMZ, segmentation, IIoT isolation



24/7 IT/OT SOC

Monitoring and threat hunting



Recovery & Resilience

Backups, playbooks, subsidy continuity



Vendor Access Reviews

OEMs, integrators, contractors



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

Single plants, formulators and distributors

- IT and plant OT assessment (B1)
- Vendor remote access review (B3, B9)
- Backup and recovery review (B3)
- Policy, media and crisis plan pack (B5)

Assurance

Multi-plant specialty and agrochemical companies

- IEC 62443 assessment and segmentation (B1, B3)
- ERP, LIMS and portal testing (B2)
- Annual independent audit (B4)
- 24x7 IT/OT SOC (B7)

Continuous Resilience

Fertilizer majors, PSUs and bulk chemical groups

- OT testing and red teaming (B1, B10)
- Safety system reviews (B1, B5)
- SOC with threat hunting (B7)
- Board and regulator reporting (B4, 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 including OT/ICS (CERT-In audit guidelines, 2025)	Independent IT/OT audits	B4, B1
Protection of notified protected systems (NCIIPC)	CII-aligned assessments and controls	B4, B3
Safety of hazardous plants and storage (Factories Act, MSIHC Rules, PESO)	SIS and OT security reviews	B1, B5
Fertilizer subsidy and PoS data integrity (DBT, Fertiliser Control Order)	ERP and integration security, continuity planning	B2, B3
Quarterly cyber incident disclosure by listed companies (SEBI LODR)	Incident records and disclosure support	B4, B8
Farmer, dealer and employee personal data (DPDP)	DPDPA programme	B6

Five new case studies, five broken chains

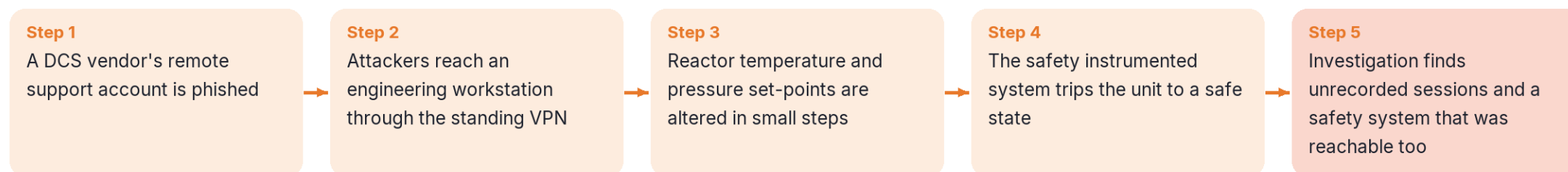
Illustrative composite scenarios written for 2026—not client engagements

1	The Set-point Nobody Changed	A phished vendor account alters reactor set-points; brokered access and SIS isolation stop it	B9 · B1 · B7
2	The Fertilizer Plant That Couldn't Claim Its Subsidy	Ransomware stalls PoS reconciliation and subsidy claims; segmentation and tested backups prevent it	B3 · B7 · B2
3	The Formulation That Left With the Contractor	A contractor copies recipes over months; DLP and offboarding controls catch it	B3 · B6 · B8
4	The Dealer Portal Payment Diversion	Phished bank details divert dealer payments; verification and monitoring stop it	B2 · B10 · B7
5	The Turnaround USB on the DCS Network	Contractor media infects the historian and operator stations; kiosks and segmentation prevent it	B9 · B3 · B7

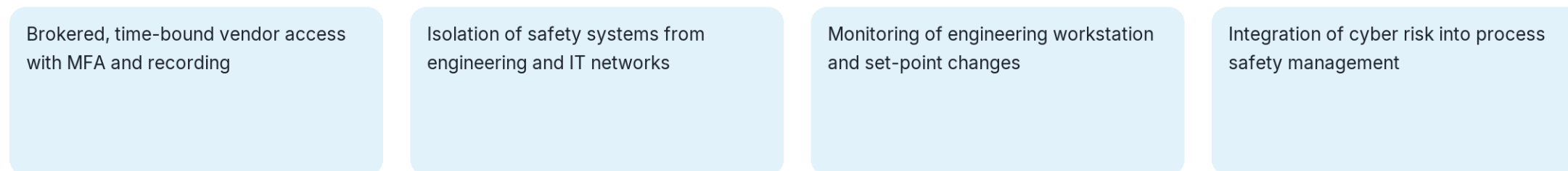
Example: breaking a vendor-access-to-safety-system chain

Case 1: The Set-point Nobody Changed

ILLUSTRATIVE ATTACK PATH



WHERE CONTROLS BREAK THE CHAIN



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

Codec Networks

What we test: which vendors can reach the DCS and engineering network, whether access is brokered and recorded, whether safety systems are isolated and in run mode, whether set-point and logic changes are monitored, and how operations and safety teams respond in a tabletop exercise.

Why chemical and fertilizer companies choose Codec Networks



CERT-In empanelled

For information security auditing services; NISIR empanelled for application audits



Certified

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



Regulation-mapped

Mapped to CERT-In, NCIIPC and safety-regulator expectations, IEC 62443 and IEC 61511



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 MTDD and MTTR metrics

Let's start with a scoping session

1 Scoping session

Plants, DCS and safety systems, vendors and contractors, ERP, LIMS and subsidy integrations, dealers and your 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.