

Keep the lines running.

IEC 62443-aligned assessments, OT segmentation, ransomware resilience and ERP security for manufacturing and industrial production.

Three questions every manufacturing leader should be able to answer

If ERP went dark tonight, could we ship tomorrow?

Mapping the plant's dependencies on IT and testing backups decides whether a ransomware incident is a bad day or a bad quarter.

Who can reach our PLCs from outside?

OEM maintenance tunnels and supplier integrations are the most common unmonitored paths into plant networks.

Which supplier could stop our lines?

Single-source and just-in-time suppliers need cyber assessment, contract clauses and a buffer plan.

5 years

Most attacked industry worldwide

> 50%

Of industrial ransomware victims

14 plants

Halted by one supplier incident

6 hours

Incident reporting to CERT-In

Built for every manufacturer

Capital goods and heavy engineering · electronics and EMS · industrial machinery and equipment · components and contract manufacturers · smart factories · engineering PSUs and strategic units.

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
SEBI LODR · DPDP	Quarterly incident disclosure (listed); personal data safeguards
Customer and export rules	EU CRA, NIS2, OEM questionnaires; IEC 62443, ISO 27001

IEC 62443, segmentation, resilience, ERP, suppliers and SOC

IEC 62443 Assessments

OT inventory, zone-and-conduit review, PLC, SCADA, robot and MES assessments.

OT Segmentation

IT/OT DMZ, flat-network removal, secure vendor remote access, IIoT isolation.

Ransomware Resilience

Attack-path tests, immutable backups, manual-operation playbooks, exercises.

ERP & MES Security

Configuration, access and portal testing; payment and master-data controls.

Supplier Cyber Risk

Critical supplier assessments, contract clauses, joint exercises.

24/7 IT/OT SOC

IT and plant monitoring, threat hunting, 6-hour reporting support.

Choose your starting point

Foundation

IT and plant assessment, backup and recovery review, OEM remote access review, policy and questionnaire pack. For component makers, MSMEs and single plants.

Assurance

IEC 62443 assessment and segmentation, ERP and portal testing, annual audit, IT/OT SOC. For mid-sized manufacturers and multi-plant groups.

Continuous Resilience

Continuous OT testing and red teaming, supplier cyber risk programme, SOC with hunting, Board and customer reporting. For large manufacturers, exporters and PSUs.

Why Codec Networks

CERT-In empanelled

for information security auditing services, and empanelled with NISCI for application audit services.

Certified

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

Regulation-mapped

Every finding mapped to IEC 62443, ISO/IEC 27001, CERT-In expectations and your customers' security requirements.

One connected partner

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

Book a scoping session

Share your plants, control systems, suppliers and customers. We will propose a practical, production-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: IBM X-Force Threat Intelligence Index 2026, Dragos OT Cybersecurity Report 2025, public reporting, CERT-In. Confirm obligations against the official instruments.