



# Codec Networks

Coding Threats. Decoding Solutions.

INDUSTRY BROCHURE · RENEWABLE ENERGY & ENERGY STORAGE

## Clean Power. Secure by Design.

OT/IoT security, telemetry and cloud assessment, vendor access controls and monitoring for solar and wind operators, battery storage operators, renewable asset managers and smart meter providers.

OT/IoT Security

Telemetry & Cloud Assessment

Vendor Access Controls

24/7 Monitoring

CEA Compliance

Supply-Chain Assurance

Coding Threats. Decoding Solutions.

[www.codecnetworks.com](http://www.codecnetworks.com)

## THE CHALLENGE

# Your fleet runs remotely. So can an attacker.

Renewable plants and storage are operated through inverters, controllers and OEM clouds across hundreds of remote sites. The CEA Cyber Security Regulations, 2026—in force from 1 April 2027—cover generators and storage of 50 MW and above, as reported.

### What keeps leadership teams awake

- OEM cloud portals that can control whole fleets
- Undocumented communication modules in equipment
- Default credentials and exposed controllers at sites
- Loss of telemetry from third-party connectivity
- Battery and smart meter systems with weak controls
- CEA Regulations, CERT-In and lender requirements



### 50 MW

Generators and storage covered by CEA Regulations (as reported)

### 1 Apr 2027

CEA Cyber Security Regulations in force

### 6 hours

To report incidents to CSIRT-Power and CERT-In (as reported)

### May 2027

Most DPDP obligations take effect

## The rulebook has changed

| Instrument                                                                          | What it means for you                                                                                                              |
|-------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------|
| <b>CEA (Cyber Security in Power Sector) Regulations, 2026</b> (in force 1 Apr 2027) | Cover generators, captive plants and storage of 50 MW and above; CISO, policy, crisis plan, audits and OT separation (as reported) |
| <b>Incident reporting</b>                                                           | Incidents to CSIRT-Power and CERT-In within six hours (as reported); CERT-In Directions apply to all                               |
| <b>Smaller assets</b>                                                               | Entities below thresholds are encouraged to adopt CERT-In's basic controls for MSMEs (as reported)                                 |
| <b>DPDP · contracts</b>                                                             | Consumer metering data safeguards from May 2027; PPA, EPC, O&M and OEM obligations                                                 |

# One partner from inverter to portfolio

Built around our primary proposition for the sector: **OT/IoT security, telemetry and cloud assessment, vendor access controls and monitoring.**

## OT/IoT Security

- Inverter, controller and BMS testing
- Site network segmentation
- Firmware and hardware inspection
- Default credential and exposure reviews

## Telemetry & Cloud Assessment

- OEM cloud and portal security reviews
- Telemetry pipeline and data integrity
- Connectivity resilience reviews
- Asset management platform testing

## Vendor Access Controls

- OEM and O&M remote access brokering
- Named accounts, MFA and recording
- Fleet command approval controls
- Vendor security assessments

## 24/7 Monitoring

- Fleet-wide OT and cloud monitoring
- Anomaly detection on commands and output
- Threat intelligence for renewable OEMs
- 6-hour reporting support

## CEA Compliance

- CEA Regulations gap assessment
- Cyber security policy and crisis plan
- Annual audit of critical systems
- Evidence for lenders and regulators

## Supply-Chain Assurance

- Equipment and component inspection
- Firmware provenance and update review
- Procurement security requirements
- OEM due diligence

**Who we serve:** utility-scale solar operators · wind farm operators · battery energy storage operators · hybrid and round-the-clock renewable parks · renewable asset managers and O&M providers · smart meter and AMI service providers.

# Packaged for how operators buy

Eleven Codec Networks bundles apply directly to renewable energy, storage and metering operators:

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

Smaller and single-site operators

- Site exposure and credential review
- Vendor portal access review
- Basic CERT-In MSME controls
- Policy pack

## Assurance

Portfolio operators (50 MW and above)

- CEA Regulations gap assessment
- Inverter, controller and BMS testing
- Vendor access controls
- 24x7 fleet monitoring

## Continuous Resilience

Large IPPs, storage and AMI providers

- Continuous OT and cloud testing
- Supply-chain and equipment assurance
- SOC with fleet-command signals
- Board, lender and regulator reporting

## Mapped to your obligations

| Requirement                                                                           | How we help                                | Bundle  |
|---------------------------------------------------------------------------------------|--------------------------------------------|---------|
| Generators and storage of 50 MW and above covered (CEA Regulations 2026, as reported) | Applicability and gap assessment           | B4      |
| Senior CISO, policy and crisis management plan (as reported)                          | Governance, policy and crisis plan support | B5, B10 |
| Annual audit of critical systems (as reported)                                        | Independent OT and IT audits               | B4, B1  |
| Incidents to CSIRT-Power and CERT-In within six hours (as reported)                   | Fleet monitoring, IR and reporting support | B7, B8  |
| OT separation and vendor accountability (as reported)                                 | Segmentation and vendor access controls    | B3, B9  |
| Equipment and supply-chain security                                                   | Equipment inspection and OEM assessments   | B9, B1  |
| Consumer metering data safeguards (DPDP)                                              | DPDPA programme for metering providers     | B6      |

# Why renewable operators choose Codec Networks

## CERT-In empanelled

Independent OT and IT audits recognised by regulators and lenders.

## Certified and accountable

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

## Field-to-cloud depth

Inverters, controllers, BMS, connectivity and OEM clouds assessed together.

## CEA-mapped

Findings mapped to the CEA Regulations 2026, CERT-In and lender requirements.

## Full stack, one partner

OT testing, monitoring, forensics and compliance connected from finding to closure.

## Certified experts

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

## How we engage

### Discover & scope

Portfolio and sites, OEMs and vendor clouds, connectivity, storage and metering, and your compliance 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 MTTR/MTTD metrics.



START WITH A SCOPING SESSION

# Let's make your next audit, commissioning and incident a non-event.

Tell us your portfolio, OEMs and obligations. We will propose a practical, OT-safe 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](mailto:mktg@codecnetworks.com)  
[www.codecnetworks.com](http://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. Source: CEA (Cyber Security in Power Sector) Regulations, 2026, as reported; confirm against the official gazette notification.