Codec Networks
Coding Threats. Decoding Solutions.

INDUSTRY BROCHURE · SMART CITIES, WATER & URBAN UTILITIES

Keep the City Running. Keep the Water Safe.

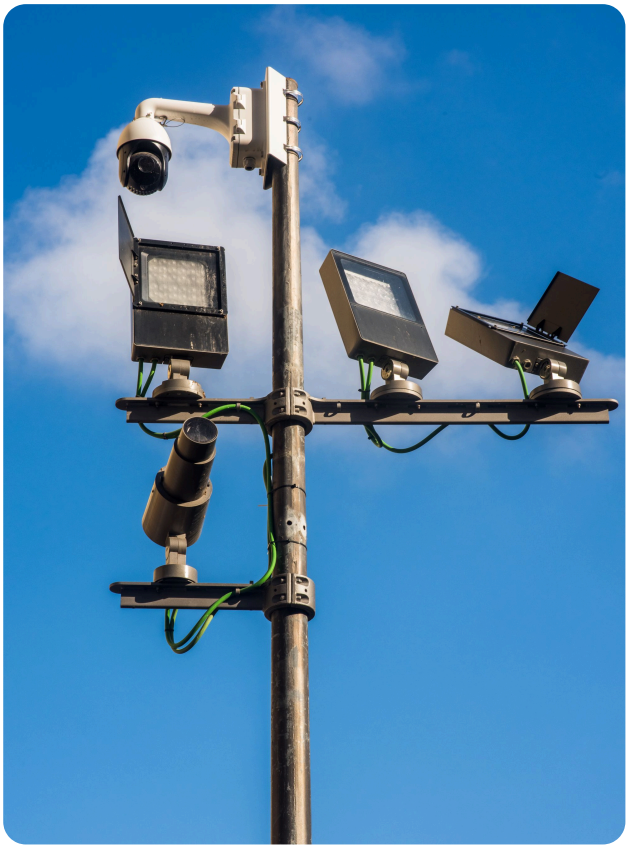
Integrated command centre security, SCADA and IoT testing, surveillance privacy and 24x7 monitoring for smart city SPVs, municipal corporations, water and wastewater utilities and urban services operators.

ICCC Security | SCADA & IoT Testing | Surveillance Privacy | Citizen Portal Security | Vendor & MSI Assurance | 24/7 City SOC

THE CHALLENGE

In a smart city, a cyber incident is a public-safety incident.

All 100 smart cities now run command centres linking cameras, traffic, water and citizen services, and utilities run plants on contractor-maintained SCADA. Intruders changed a water plant's dosing at Oldsmar (2021) and seized a PLC at Aliquippa (2023); in India ransomware has hit Goa's flood monitors and a 413-town municipal portal.



What keeps leadership teams awake

- Set-points changed at a water or sewage plant
- An ICCC or VMS taken over or encrypted
- Citizen portals and tax systems held to ransom
- Camera footage and recognition data misused
- Integrators and O&M contractors with standing access
- CERT-In reporting, audits and DPDP for citizen data

100
Smart cities with operational command centres (MoHUA)

~70%
Of US water systems inspected failed cyber checks (EPA, 2024)

413
Towns hit by the MP e-Nagarpalika portal attack (Dec 2023)

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, OT/ICS and applications
CERT-In guidelines for government entities (2023)	Baseline controls for government bodies and agencies: CISO, asset inventory, access control, third-party and cloud security
DPDP Act and Rules (2023, 2025)	Safeguards and breach intimation for citizen, commuter and surveillance data; most obligations from May 2027
NCIIPC · MeitY CCTV requirements	Protection of any notified protected systems; security requirements and STQC testing for CCTV cameras from April 2025

OUR SERVICE OFFERINGS

One partner from treatment plant to command centre

Built around our primary proposition for the sector: **integrated command centre security, SCADA and IoT testing, surveillance privacy and a 24x7 city SOC.**

ICCC Security

- ICCC platform, VMS and analytics assessment
- Segmentation of command centre, field and corporate networks
- Dashboard, API and data platform testing
- Resilience and recovery review for command centres

SCADA & IoT Testing

- Water and wastewater SCADA, PLC and HMI assessments
- Safe, passive methods planned with plant operators
- Smart meter, streetlight, signal and sensor security reviews
- IEC 62443-aligned gap assessments

Surveillance Privacy

- CCTV, ANPR and facial-recognition governance review
- Purpose, retention, access and export controls
- Alignment with MeitY CCTV essential requirements
- DPDP programme for citizen and surveillance data

Citizen Portal Security

- Portal, app and payment integration testing
- Municipal ERP and e-governance platform reviews
- Backup and recovery validation
- Collection and payment fraud controls

Vendor & MSI Assurance

- Master system integrator and OEM access brokering
- O&M contractor and concessionaire assessments
- Contract security clauses and recertification
- Handover security checks at mission closure

24/7 City SOC

- Monitoring of ICCC, SCADA, IoT and IT
- Vendor session and remote access monitoring
- Threat hunting and incident response
- 6-hour CERT-In reporting support

Who we serve: smart city SPVs · municipal corporations and councils · water supply and sewerage boards · wastewater and treatment operators · urban services concessionaires (parking, lighting, transit) · safe-city and ICCC operators.

BUNDLED SERVICE MODELS

Packaged for how cities and utilities buy

Eleven Codec Networks bundles apply directly to smart cities, water and urban utilities:

- **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 ULBs, single plants and service operators

- IT and SCADA or field system assessment
- Remote access and backup review
- Citizen portal testing
- Policy pack and CERT-In readiness

Assurance

Smart city SPVs and municipal corporations

- ICCC, SCADA and CCTV assessment
- Portal, app and data platform testing
- Annual independent audit and DPDP programme
- 24x7 city SOC

Continuous Resilience

Metropolitan utilities, state missions and parastatals

- Multi-plant and multi-city OT programme
- MSI, vendor and concessionaire risk programme
- SOC with threat hunting
- Board, state and auditor reporting

Mapped to your obligations

Requirement	How we help	Bundle
Cyber incidents to CERT-In within six hours; 180-day logs	City SOC, IR retainer and reporting support	B7, B8
Risk-based independent cyber audits incl. OT/ICS (CERT-In, 2025)	Independent IT and OT audits	B4, B1
Baseline controls for government entities (CERT-In, 2023)	Gap assessment, CISO support, evidence	B4, B5
Protection of notified protected systems (NCIIPC)	CII-aligned assessments and controls	B4, B3
Citizen, commuter and surveillance data (DPDP)	DPDPA programme and surveillance governance	B6
CCTV security and STQC testing (MeitY ER, Apr 2025)	CCTV and VMS assessment, procurement evidence	B1, B5
Lender, auditor and concession security clauses	ISO 27001, IEC 62443 and evidence packs	B5, B9

THE CODEC NETWORKS VALUE ADD

Why cities and utilities choose Codec Networks

CERT-In empanelled

Independent IT and OT audits recognised by government bodies, lenders and auditors.

Certified and accountable

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

Plant-aware OT methods

Passive discovery and planned testing coordinated with plant operators and ICCC teams—no surprise outages.

Standards-mapped

Findings mapped to CERT-In, NCIIPC, IEC 62443, ISO/IEC 27001 and MeitY CCTV expectations.

Full stack, one partner

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

Certified experts

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

How we engage

Discover & scope

Plants and pumping stations, ICCC and VMS, field devices, integrators and O&M contractors, citizen portals and data platforms, and your audit and mission 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 audit, handover and incident a non-event.

Tell us your plants, command centres, field systems, vendors and citizen platforms. We will propose a practical, plant-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: MoHUA, US EPA enforcement alert (May 2024), public reporting, CERT-In. Confirm obligations against the official instruments.