Codec Networks

Coding Threats. Decoding Solutions.

SMART CITIES, WATER & URBAN UTILITIES

Keep the City Running. Keep the Water Safe.

Integrated command centre security, SCADA and IoT testing, surveillance privacy and a 24x7 city SOC for smart cities, water and urban utilities



What we will cover

The sector and its risks

Scale, players and the threats that matter most

What regulators now expect

CERT-In, NCIIPC, DPDP and the CCTV requirements that reach every city and utility

How Codec Networks helps

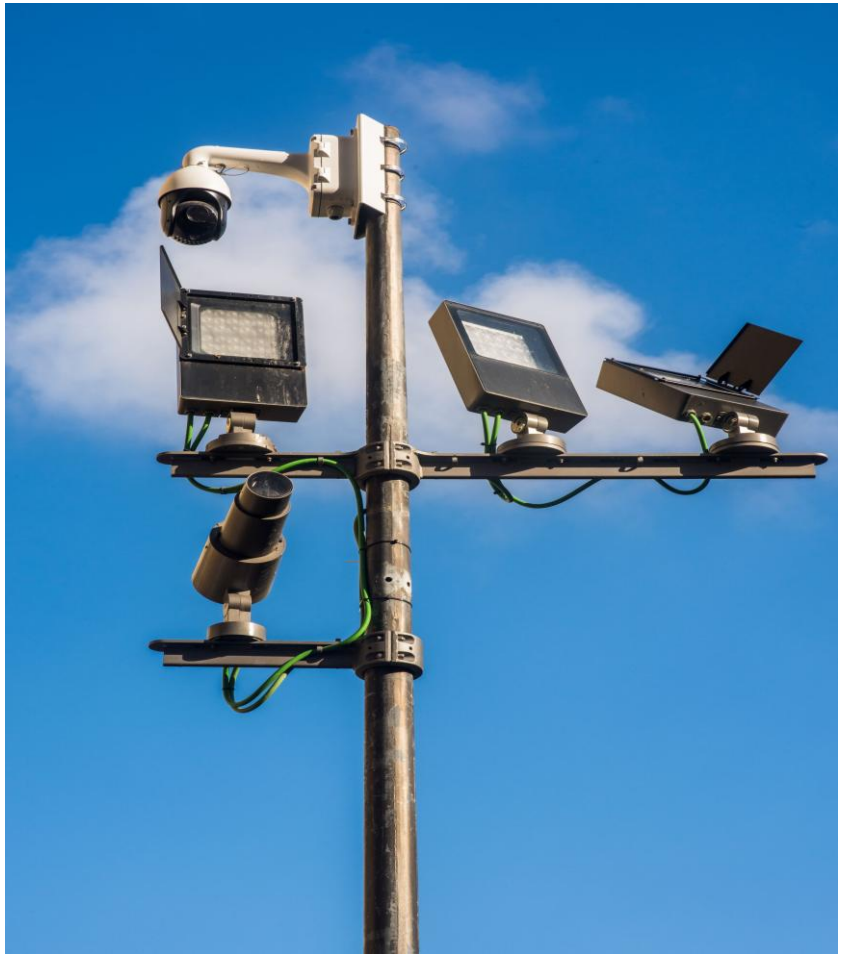
Services, bundles and packages built for the sector

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 cities and utilities are public-safety incidents

Global and Indian incidents show the stakes

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

What this means: cities and utilities must separate plants, command centres and citizen systems, control integrator and contractor access, test SCADA and field devices safely, govern surveillance data, make portals recoverable, monitor around the clock and report incidents within six hours.

Sources: MoHUA, US EPA enforcement alert (May 2024), public reporting, CERT-In.

Who we serve across smart cities, water and urban utilities

Smart city SPVs

ICCCs, city platforms, post-mission O&M

Municipal corporations

Civic services, tax, e-governance

Water supply utilities

Treatment plants, pumping, distribution

Sewerage and wastewater

STPs, pumping stations, reuse

Command centre operators

ICCC, VMS, analytics, dashboards

Safe city and surveillance

CCTV, ANPR, recognition, police users

Traffic, parking and transit

Signals, parking, bus and metro systems

Lighting and urban services

Streetlights, meters, waste, concessions

The threats that cost cities and utilities the most

Six priorities from our 18-threat sector assessment

SCADA manipulation

Set-points and pumps changed from outside

Command centre takeover

ICCC, VMS and dashboards encrypted or blind

Ransomware on portals

Tax, billing and e-governance held to ransom

Surveillance exposure

Camera and recognition data misused

Vendor remote access abuse

Integrators and O&M tunnels hijacked

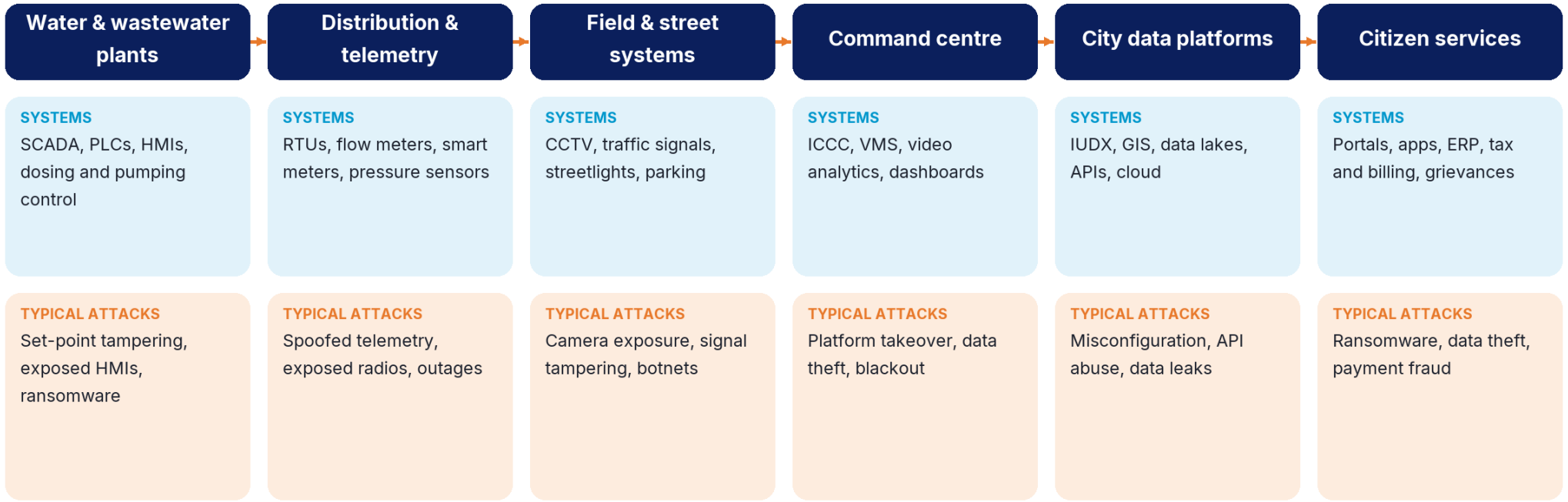
Slow detection & reporting

Missing the 6-hour window

Attacks target every layer from treatment plant to citizen app

Where Cyber Risk Sits Across City and Utility Operations

Every layer from treatment plant to citizen app carries its own attack surface



In cities and utilities, a cyber incident becomes a public-safety and public-trust event—water quality, traffic, surveillance and services fail in front of citizens.

Source: Codec Networks analysis

Codec Networks

What regulators now expect

CERT-In, NCIIPC, DPDP and the CCTV requirements that reach every city and utility

Codec Networks
Coding Threats. Decoding Solutions.

The rules and standards shaping smart city and utility 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
Baseline controls for government entities	Continuous; CISO designated	CERT-In guidelines, June 2023
Independent cyber audits	Risk-based, incl. OT/ICS	CERT-In audit guidelines, 2025
Protected systems	Per notification	NCIIPC (IT Act Section 70A)
Citizen, commuter and surveillance data	Most obligations from May 2027	DPDP Act 2023 and Rules 2025
CCTV security requirements	In effect from April 2025	MeitY Compulsory Registration Order
Urban mission and O&M obligations	Per scheme and contract	AMRUT 2.0; Smart Cities Mission; concessions
Industrial and security good practice	Standards	IEC 62443; ISO/IEC 27001

Key dates on the regulatory timeline

Policy and Regulatory Timeline Shaping Smart City and Urban Utility Cybersecurity

Urban missions, cross-sector Indian cyber and privacy rules and the CCTV requirements that reach every city

In force · Upcoming (from Oct 2026)

1992	74th Constitutional Amendment: municipalities recognised as local self-government
2000	Information Technology Act, 2000; CERT-In and protected systems (Section 70A) added in 2008
Jun 2015	Smart Cities Mission and AMRUT launched; 100 smart cities selected in rounds from 2016
Feb 2021	National Urban Digital Mission and India Urban Data Exchange (IUDX) launched
Oct 2021	AMRUT 2.0 launched: water security for all statutory towns, 2021-22 to 2025-26
Apr 2022	CERT-In Directions: 6-hour incident reporting, 180-day ICT logs in India
Jun 2023	CERT-In guidelines on information security practices for government entities
Aug 2023	Digital Personal Data Protection Act, 2023 enacted
Dec 2024	MoHUA reports operational ICCCs in all 100 smart cities
Mar 2025	Smart Cities Mission financial closure; remaining projects completed by cities
Apr 2025	MeitY essential security requirements for CCTV cameras take effect
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: MoHUA, MeitY, CERT-In. Confirm obligations against the official instruments.

Codec Networks

How Codec Networks helps

ICCC · SCADA & IoT · Surveillance privacy · Citizen portals · Vendors & MSIs · City SOC

Codec Networks
Coding Threats. Decoding Solutions.

One partner from treatment plant to command centre



ICCC Security

Platforms, VMS, analytics, segmentation



SCADA & IoT Testing

Plants, PLCs, meters, streetlights, sensors



Surveillance Privacy

CCTV, ANPR, recognition governance



Citizen Portal Security

Portals, apps, payments, municipal ERP



Vendor & MSI Assurance

Integrators, OEMs, O&M, concessions



24/7 City SOC

Monitoring and threat hunting

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

Smaller ULBs, single plants and service operators

- IT and SCADA or field assessment (B1)
- Remote access and backup review (B3, B9)
- Citizen portal testing (B2)
- Policy pack and CERT-In readiness (B5)

Assurance

Smart city SPVs and municipal corporations

- ICCC, SCADA and CCTV assessment (B1, B3)
- Portal, app and data platform testing (B2)
- Annual audit and DPDP programme (B4, B6)
- 24x7 city SOC (B7)

Continuous Resilience

Metropolitan utilities, state missions and parastatals

- Multi-plant OT programme (B1, B3, B10)
- MSI and concessionaire risk programme (B9)
- SOC with threat hunting (B7)
- Board, state and auditor 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	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

Five new case studies, five broken chains

Illustrative composite scenarios written for 2026—not client engagements

1	**The Dosing Screen at Three in the Morning**	An exposed HMI lets an intruder raise chemical set-points; brokered access and limits stop it	**B1 · B3 · B7**
2	**The Command Centre That Went Dark**	Stolen integrator credentials spread ransomware across the ICCC; access controls and backups prevent it	**B9 · B3 · B8**
3	**The Property Tax Portal Nobody Backed Up**	An unpatched portal is encrypted in tax season; testing, backups and SOC limit it	**B2 · B3 · B7**
4	**The Footage That Left the Control Room**	A contractor exports surveillance data for months; governance and logging catch it	**B6 · B1 · B9**
5	**The Streetlights That Joined a Botnet**	Default-credential gateways reach pumping telemetry; isolation and device controls prevent it	**B11 · B3 · B7**

Example: breaking a remote-access-to-dosing-screen chain

Case 1: The Dosing Screen at Three in the Morning

ILLUSTRATIVE ATTACK PATH

Step 1
A city water board's treatment plant HMI is reachable through a remote-desktop tool left for the O&M contractor

→

Step 2
A shared password is guessed; the intruder opens the chemical dosing screen

→

Step 3
The chlorine and alkali set-points are raised far beyond safe limits

→

Step 4
A night operator sees the cursor move and resets the values within minutes

→

Step 5
Investigation finds no MFA, no session logs and a Windows 7 workstation

WHERE CONTROLS BREAK THE CHAIN

SCADA and HMI assessment with safe, passive methods	Removal of direct remote-desktop access; brokered vendor access with MFA	Set-point limits, alarms and change monitoring in the control system	OT monitoring and a 24x7 city SOC

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

Codec Networks

What we test: which plants and pumping stations are reachable from the internet or through remote-desktop tools, whether contractor access is brokered and recorded, whether set-point limits and alarms would catch a malicious change, whether SCADA, corporate and ICCC networks are separated, and how operators and the city respond in a tabletop exercise.

Why cities and utilities choose Codec Networks

CERT-In empanelled

For information security auditing services; NICSI empanelled for application audits

Certified

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

Regulation-mapped

Mapped to CERT-In, NCIIPC, DPDP and MeitY CCTV expectations and your lenders' and auditors' requirements

Tests the whole chain

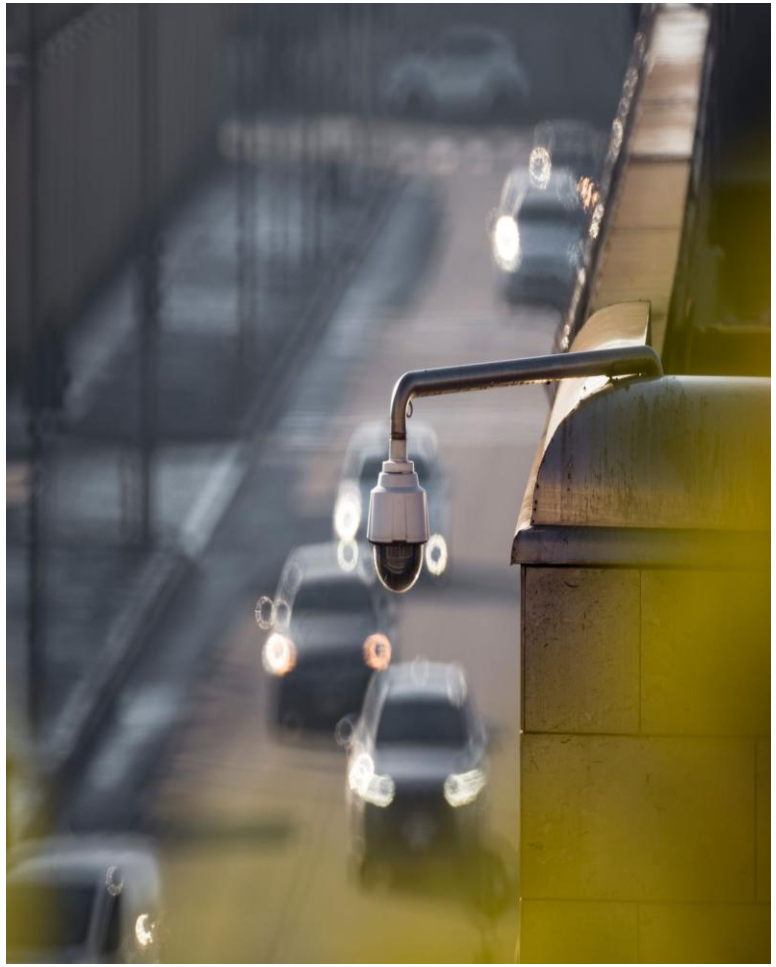
Technical, process and monitoring tests together

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 MTTD and MTTR metrics

Let's start with a scoping session

1 Scoping session

Plants and pumping stations, ICCC and VMS, field devices, integrators and contractors, citizen portals and data platforms, and your audit and mission 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.

Codec Networks
Coding Threats. Decoding Solutions.