

SMART CITIES, WATER & URBAN UTILITIES CYBERSECURITY

Keep the city running. Keep the water safe.

Integrated command centre security, SCADA and IoT testing, surveillance privacy and 24x7 monitoring for smart cities, water and urban utilities.

Three questions every city and utility leader should be able to answer

Could someone change a set-point from outside?

Remote-desktop tools and exposed PLCs are how intruders reached water plants at Oldsmar and Aliquippa.

Who can log in to our command centre?

Integrators and O&M contractors usually hold standing access to ICCC, VMS and SCADA that nobody monitors.

If the portal went dark in tax season, what then?

Tested backups, manual counters and a citizen-data breach plan decide whether it is a bad day or a bad quarter.

100

Smart cities with operational ICCCs

~70%

US water systems failing cyber checks (EPA)

413

Towns hit by one portal attack (MP, 2023)

6 hours

Incident reporting to CERT-In

Built for every city and utility

Smart city SPVs · municipal corporations and councils · water supply and sewerage boards · wastewater and treatment operators · urban services concessionaires · safe-city and ICCC operators.

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 incl. OT/ICS
CERT-In government-entity guidelines · NCIIPC	Baseline controls, CISO and third-party duties; protected systems
DPDP · MeitY CCTV ER (2023–25)	Citizen and surveillance data safeguards; CCTV security testing

WHAT WE DO

Command centres, SCADA, surveillance, portals, vendors and SOC

ICCC Security

ICCC, VMS, analytics and data platform assessment; segmentation; recovery review.

SCADA & IoT Testing

Water and wastewater SCADA, PLC, HMI, smart meter and field device assessments.

Surveillance Privacy

CCTV, ANPR and facial-recognition governance aligned to DPDP and MeitY requirements.

Citizen Portal Security

Portal, app, payment and municipal ERP testing; backup and fraud controls.

Vendor & MSI Assurance

Integrator, OEM, O&M and concessionaire access controls and assessments.

24/7 City SOC

Monitoring of ICCCC, SCADA, IoT and IT; 6-hour reporting support.

Choose your starting point

Foundation

IT and SCADA or field system assessment, remote access and backup review, portal testing, policy pack. For smaller ULBs, single plants and service operators.

Assurance

ICCC, SCADA and CCTV assessment, portal and data platform testing, annual audit and DPDP programme, city SOC. For smart city SPVs and municipal corporations.

Continuous Resilience

Multi-plant and multi-city OT programme, vendor and concessionaire risk programme, SOC with hunting, state and auditor reporting. For metropolitan utilities and state missions.

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

One connected partner

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

Book a scoping session

Share 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 – 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: MoHUA, US EPA enforcement alert (May 2024), public reporting, CERT-In. Confirm obligations against the official instruments.