

Codec Networks

Coding Threats. Decoding Solutions.

DRONES, ROBOTICS & AUTONOMOUS SYSTEMS

Secure Every Flight. Protect Every Fleet.

Firmware, communications, control platform and cloud security, with authorised navigation resilience testing, for drone, robotics and autonomous systems businesses

Coding Threats. Decoding Solutions. · www.codecnetworks.com



What we will cover



The sector and its risks

Scale, players and the threats that matter most



What regulators now expect

Drone Rules and Digital Sky, CSUAS, CERT-In, DPDP and EU CRA



How Codec Networks helps

Services, bundles and packages built for the sector



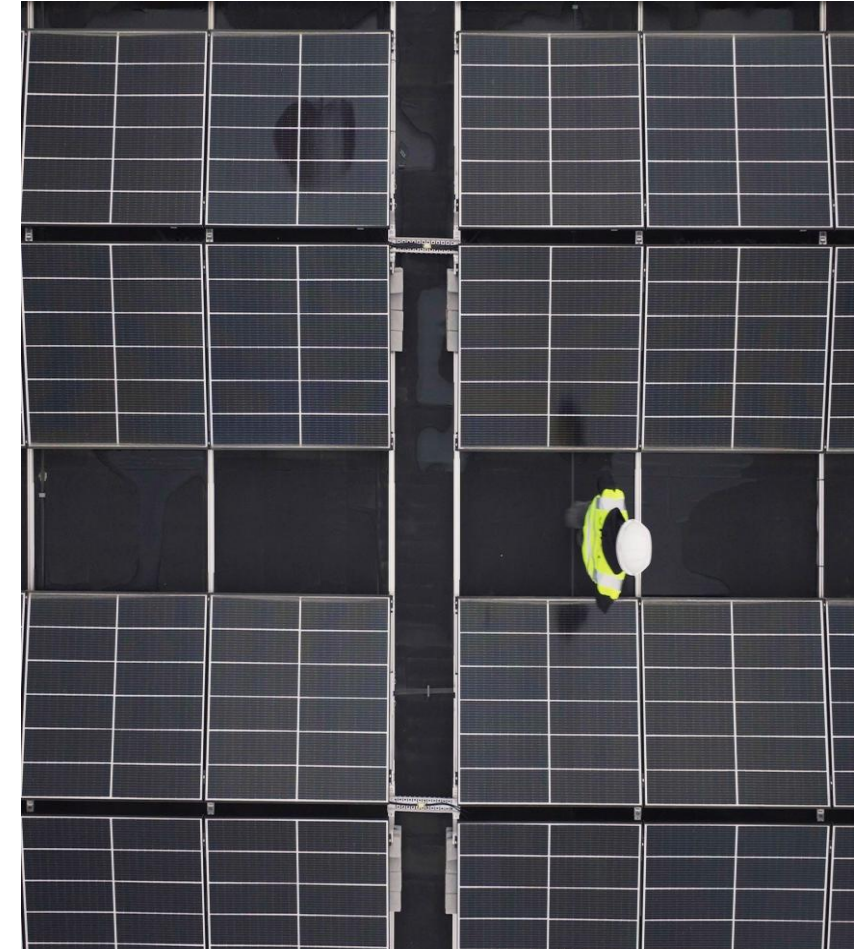
Proof in scenarios

Five new case studies and the controls that break the chain



Why Codec Networks and next steps

Our value add and how to start



Drones and robots are scaling fast, and so is their attack surface

Public figures show the scale of what must be protected

30,450

Drones registered on Digital Sky
(Feb 2025)

9,120

Industrial robots installed in
India in 2024 (IFR)

6

Airports beyond Delhi reporting
GNSS interference

6 hours

To report cyber incidents to
CERT-In

What this means: Drone makers, operators, robotics firms and fleet software providers must sign and protect every firmware update, secure command and telemetry links, lock down ground apps, fleet consoles and APIs, test navigation fail-safes under authorised conditions, protect imagery and flight data, control vendor access to robot cells and report incidents to CERT-In within six hours.

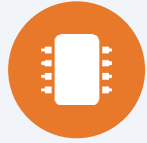
Sources: Rajya Sabha reply (March 2025), IFR World Robotics 2025, Rajya Sabha reply (December 2025), CERT-In Directions (2022).

Who we serve across drones, robotics and autonomy



Drone manufacturers

Airframes, flight controllers, OEMs



Component makers

Radios, payloads, sensors, motors



Survey and inspection

Mapping, utilities, infrastructure



Agriculture drones

Spraying, crop and field services



Drone delivery

Medical, parcel and remote logistics



Warehouse robotics

AMRs, sorters, goods-to-person



Industrial and service robots

Robot cells, inspection, hospitality

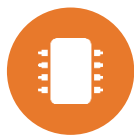


Fleet and traffic software

Ground control, fleet cloud, UTM

The threats that cost drone and robotics businesses the most

Six priorities from our 18-threat drone, robotics and autonomy assessment



Firmware tampering

Unsigned updates, backdoored builds



Link hijacking

Command, telemetry and video links



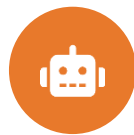
GNSS interference

Jamming and spoofing exposure



Fleet cloud takeover

Consoles, APIs, OTA pipelines



Robot controller attacks

ROS, AMR fleets, vendor tunnels



Imagery and data leaks

Survey data, video, flight logs

Attacks target every step from design to data delivery

Where Cyber Risk Sits Across the Drone and Robot Lifecycle

Every step from design to data delivery carries its own attack surface



A drone or robot is a computer that moves: one compromised update, radio link or fleet console can turn a productive fleet into a safety incident.

Source: Codec Networks analysis

Codec Networks

What regulators now expect

Drone Rules and Digital Sky, CSUAS, CERT-In, DPDP and EU CRA

The rules shaping drone and robotics security

Requirement	Frequency / deadline	Source
Registration and pilots	UINs on Digital Sky; remote pilot certificates	Drone Rules 2021, as amended
Airspace and permissions	Green, yellow and red zones; ATC permission	Drone Rules 2021; airspace map
Type certification	DGCA certificate on QCI-approved body advice	CSUAS, 26 Jan 2022
Imports	Drones prohibited, with listed exceptions	DGFT notification, 9 Feb 2022
GNSS interference	Mitigation, contingency and reporting	DGCA circular 2023; SOP Nov 2025
Cyber incident reporting	To CERT-In within 6 hours; 180-day logs	CERT-In Directions, 2022
Independent audits	Risk-based audits, including OT and ICS	CERT-In guidelines, Jul 2025
Personal data	Safeguards and breach intimation	DPDP Act 2023; Rules 2025
Products sold in the EU	Secure design, vulnerability reporting	EU CRA; reporting from Sep 2026

Key dates on the regulatory timeline

Legal and Regulatory Timeline Shaping Drone and Robotics Security

Aviation, industrial, cyber, data and export-market instruments that reach drone makers, operators, robotics firms and fleet software providers

● In force ● Upcoming (from Oct 2026)

Jun 2021	●	Explosive-laden drones strike the Air Force Station in Jammu; probe handed to the NIA
Aug 2021	●	Drone Rules 2021 notified on 25 August: Digital Sky, UINs, airspace zones, 500 kg cover
Sep 2021	●	PLI scheme of ₹120 crore approved for drones and drone components over three years
Jan 2022	●	Certification Scheme for UAS notified: QCI-approved bodies, DGCA type certificates
Feb 2022	●	DGFT prohibits drone imports with exceptions; amendment brings remote pilot certificates
Apr 2022	●	CERT-In Directions: 6-hour incident reporting and 180-day ICT logs kept in India
Nov 2023	●	DGCA advisory circular on GNSS interference; Namo Drone Didi approved for 15,000 SHGs
Dec 2024	●	EU Cyber Resilience Act enters into force for products with digital elements
Jan 2025	●	Bharatiya Vayuyan Adhiniyam 2024 replaces the Aircraft Act 1934
Jul 2025	●	CERT-In Comprehensive Cyber Security Audit Policy Guidelines, including OT and ICS
Sep 2025	●	Draft Civil Drone (Promotion and Regulation) Bill 2025 released for consultation
Nov 2025	●	DGCA SOP for real-time GNSS interference reports near Delhi; DPDP Rules notified
Sep 2026	●	EU CRA reporting of exploited vulnerabilities and severe incidents applies
May 2027	●	Most DPDP Rules obligations, incl. security safeguards and breach intimation, apply

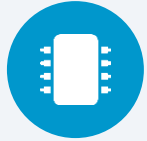
Sources: Ministry of Civil Aviation, DGCA, DGFT, PIB, Parliament replies, CERT-In, MeitY, Official Journal of the EU. Confirm against the official instruments.

Codec Networks

How Codec Networks helps

Firmware · Links · Platforms & cloud · Navigation resilience · Robotics & OT · SOC

One partner from firmware to fleet cloud



Firmware & Device Security

Controllers, boot, updates



Links & Communications

Command, telemetry, video



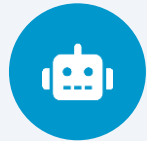
Control Platform & Cloud

Ground apps, fleet, APIs



Navigation Resilience

Authorised, controlled tests



Robotics & OT Security

Robot cells, AMRs, IEC 62443



24/7 SOC & Response

Monitoring, CERT-In, forensics

Eleven bundles from the Codec Networks catalogue

Business-ready bundles instead of 180 separate services



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

Drone start-ups, operators and RPTOs

- Drone and ground app test (B1)
- Fleet cloud quick review (B3)
- Imagery data check (B6)
- IR retainer (B8)

Assurance

Drone makers and fleet software firms

- Firmware and update security (B2)
- Fleet API and cloud VAPT (B1, B3)
- CERT-In empanelled audit (B4)
- 24x7 managed SOC (B7)

Continuous Resilience

Large OEMs, robotics and delivery fleets

- Red team of fleet and links (B1)
- Navigation resilience tests (B11)
- IEC 62443 and ISO 27001 (B5)
- Product security programme (B2)

Every obligation mapped to a bundle

Requirement	How Codec Networks helps	Bundle
Register drones and keep UIN and pilot records (Drone Rules 2021)	Record and platform integrity review	B4, B5
Type certificate on QCI-scheme recommendation (CSUAS 2022)	Firmware and product testing	B1, B2
Incidents to CERT-In in six hours; 180-day logs (CERT-In)	SOC, IR retainer, reporting support	B7, B8
Risk-based independent audits incl. OT (CERT-In guidelines 2025)	CERT-In empanelled audit	B4
Safeguards and breach intimation for personal data (DPDP Act)	DPDPA programme for imagery	B6
Secure design and vulnerability handling (EU CRA, for EU sales)	Product security programme	B2, B11
Trusted components where buyers require them (tender terms)	Supply chain assessment	B9

Five new case studies, five broken chains

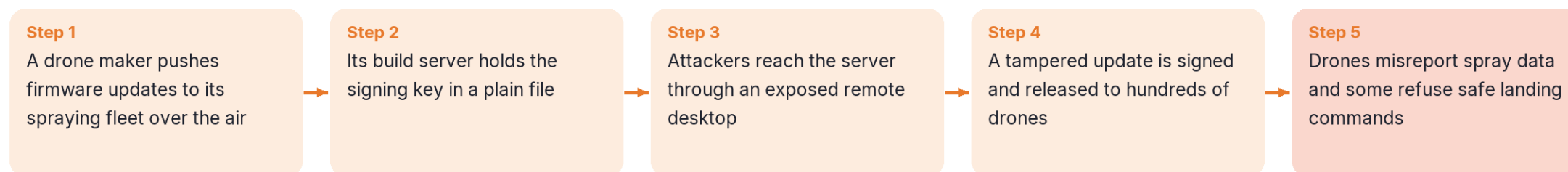
Illustrative composite scenarios written for 2026—not client engagements

1	The Update That Flew Itself	A breached build server signs a tampered firmware update; HSM keys and secure boot stop it	B2 · B3 · B8
2	The Bucket Full of Rooftops	Public cloud storage exposes utility site imagery and residents; access controls prevent it	B3 · B6 · B9
3	The Delivery Route That Drifted	GNSS interference trips fail-safes; authorised resilience testing and cross-checks prepare for it	B1 · B11 · B10
4	The Warehouse That Stopped Picking	A phished vendor account lets ransomware halt robots; named access and segmentation stop it	B3 · B7 · B9
5	The Fleet Console Anyone Could Open	A trusted client ID exposes other tenants' missions; server-side checks prevent it	B2 · B1 · B7

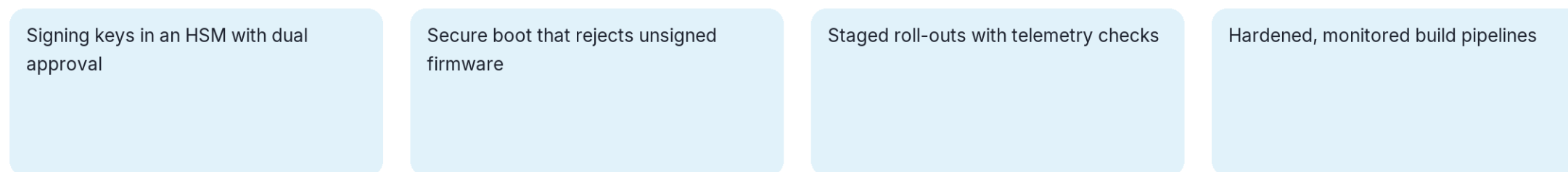
Example: catching a tampered firmware update

Case 1: The Update That Flew Itself

ILLUSTRATIVE ATTACK PATH



WHERE CONTROLS BREAK THE CHAIN



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

Codec Networks

What we test: where firmware signing keys live and who can use them, whether drones and controllers reject unsigned or downgraded images at boot, how update packages move from build server to fleet, whether staged roll-outs and telemetry checks would catch abnormal behaviour, and how the maker would recall an update, investigate and report to CERT-In and customers.

Why drone and robotics businesses choose Codec Networks



CERT-In empanelled

For information security auditing services; NISCI empanelled for application audits



Certified

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



Regulation-mapped

Mapped to the Drone Rules and CSUAS, DGCA's GNSS circular, CERT-In Directions and audit guidelines, IEC 62443, DPDP and the EU CRA



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

Controller firmware and update signing, command, telemetry and video links, ground control apps, fleet cloud and APIs, navigation fail-safes, robot cells and AMR fleets, vendor access, imagery and flight data, suppliers

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.