Codec Networks
Coding Threats. Decoding Solutions.



AUTOMOTIVE & MOBILITY CYBERSECURITY

Secure the plant. Secure the car.

Vehicle network testing, embedded and OTA security, plant OT security and charging API and cloud security for automotive and mobility.

Three questions every automotive leader should be able to answer

Could a supplier's or dealer platform's incident stop us?
JLR, Toyota and CDK Global show that plants and dealers stop when one connected party fails.

Can our app or API reach the car?
Companion apps, dealer portals and telematics APIs are the fastest route from the internet to the vehicle.

Are we ready for AIS 189 and AIS 190?
A cyber security management system and a software update management system will be part of type approval.

5 weeks
JLR production halted (2025)

£1.9 bn
Estimated cost of the JLR attack

15,000
Dealerships hit by CDK Global attack

6 hours
Incident reporting to CERT-In

Built for every automotive and mobility company

Vehicle OEMs · tier-1 and tier-2 component suppliers · EV and battery manufacturers · charging networks · dealers and mobility platforms · fleet and telematics providers.

The rules that drive your security calendar

Instrument	Key cybersecurity expectations
AIS 189/190 · CMVR (draft, phased from 2026)	Vehicle CSMS and SUMS for type approval; aligned with UN R155/R156
CERT-In · SEBI LODR · DPDP	6-hour reporting; quarterly disclosure (listed); personal data safeguards
Global rules	ISO/SAE 21434, TISAX, EU CRA, PCI DSS for charging payments

WHAT WE DO

Vehicle, OTA, plant, charging, supplier and SOC

Vehicle Network Testing
ECU, CAN/Ethernet, telematics and TARA per ISO/SAE 21434; AIS 189 readiness.

Embedded & OTA Security
Firmware, secure boot, OTA pipeline and signing; AIS 190 readiness.

Plant OT Security
IEC 62443 assessments, segmentation, ransomware resilience.

Charging API & Cloud
CPO backends, OCPP, chargers, apps, cloud APIs and payments.

Supplier & Dealer Risk
Tier-n suppliers, DMS and SaaS providers, TISAX readiness.

24/7 IT/OT SOC
Plant, enterprise and vehicle-cloud monitoring; 6-hour reporting.

Choose your starting point

Foundation
IT and plant or backend assessment, backup and remote access review, TISAX or OEM questionnaire readiness, policy and privacy pack. For suppliers, dealers and charging start-ups.

Assurance
Vehicle, charger or product testing, plant segmentation and OT review, annual audit, IT/OT SOC. For EV makers, charging networks and mid-sized suppliers.

Continuous Resilience
AIS 189/190 programme, continuous app, API and OTA testing, supplier and dealer risk programme, SOC with Board reporting. For OEMs, tier-1 majors and fleet platforms.

Why Codec Networks

CERT-In empanelled
for information security auditing services, and empanelled with NICSI for application audit services.

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

Regulation-mapped
Every finding mapped to AIS 189/190, ISO/SAE 21434, IEC 62443, TISAX, CERT-In expectations and your OEM customers' requirements.

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

Book a scoping session

Share your vehicles, plants, platforms and partners. We will propose a practical, production-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: Cyber Monitoring Centre (UK), public reporting on JLR and CDK Global, CERT-In, MoRTH. Confirm obligations against the official instruments.