



Codec Networks

Coding Threats. Decoding Solutions.

INDUSTRY BROCHURE · AUTOMOTIVE & MOBILITY

Secure the Plant. Secure the Car.

Vehicle cybersecurity, embedded and OTA security, plant OT security, charging and telematics assurance for OEMs, component suppliers, EV makers, charging networks and fleet technology companies.

Vehicle Network Testing

Embedded & OTA Security

Plant OT Security

Charging API & Cloud

Supplier & Dealer Risk

24/7 IT/OT SOC

Coding Threats. Decoding Solutions.

www.codecnetworks.com

THE CHALLENGE

In automotive, a cyber incident can stop every plant and reach every car.

In September 2025 a cyberattack halted Jaguar Land Rover's global production for about five weeks—the costliest cyber event in UK history at an estimated £1.9 billion. In 2024 a ransomware attack on one dealer-software provider put 15,000 North American dealerships on paper for two weeks. Meanwhile AIS 189 and AIS 190 are bringing vehicle cybersecurity and software-update management into Indian type approval.

What keeps leadership teams awake

- Ransomware stopping plants, suppliers and dealers
- Companion apps and APIs that reach the vehicle
- OTA updates and the software supply chain
- Charging backends, OCPP and payments
- Customer, vehicle and driver data under DPDP
- AIS 189/190, CERT-In and global OEM audits



5 weeks

JLR production halted by a cyberattack (2025)

£1.9 bn

Estimated UK economic cost of the JLR attack (CMC)

15,000

Dealerships disrupted by the CDK Global attack (2024)

6 hours

To report cyber incidents to CERT-In

The rulebook has changed

Instrument	What it means for you
AIS 189 and AIS 190 under CMVR (draft notification, 2026)	Cyber Security Management System and Software Update Management System for vehicle type approval, phased from October 2026; aligned with UN R155/R156
CERT-In Directions and audit guidelines (2022, 2025)	6-hour incident reporting, 180-day logs; risk-based independent cyber audits covering IT and OT
SEBI LODR · DPDP Act and Rules	Quarterly incident disclosure for listed companies; safeguards for customer, vehicle, driver and dealer data from May 2027
Global customer and export rules	UN R155/R156, ISO/SAE 21434, TISAX for suppliers, EU Cyber Resilience Act for connected products, PCI DSS for charging payments

Codec Networks · Automotive & Mobility

Codec Networks

Coding Threats. Decoding Solutions.

One partner from plant floor to the road

Built around our primary proposition for the sector: **vehicle network testing, embedded security, OTA update reviews and charging API and cloud security.**

Vehicle Network Testing

- In-vehicle network and ECU testing (CAN, Ethernet, diagnostics)
- Telematics unit and gateway assessment
- Threat analysis and risk assessment per ISO/SAE 21434
- AIS 189 CSMS readiness and evidence

Embedded & OTA Security

- Firmware and secure boot reviews
- OTA pipeline, signing and rollout assessment
- AIS 190 SUMS readiness
- Software supply-chain and SBOM reviews

Plant OT Security

- IEC 62443-aligned plant assessments
- IT/OT segmentation and OEM remote access
- Ransomware resilience for ERP, MES and plants
- Production-aware testing

Charging API & Cloud

- CPO backend, OCPP and charger assessments
- Payment flows and PCI DSS alignment
- Companion app and cloud API testing
- Vehicle-to-cloud threat modelling

Supplier & Dealer Risk

- Tier-n supplier cyber assessments
- DMS and SaaS provider assurance
- TISAX and OEM questionnaire readiness
- Dealer network security baselines

24/7 IT/OT SOC

- Plant, enterprise and vehicle-cloud monitoring
- Anomalous vehicle and charger command detection
- Threat hunting and remote-session monitoring
- 6-hour CERT-In reporting support

Who we serve: vehicle OEMs · tier-1 and tier-2 component suppliers · EV and battery manufacturers · charging networks · dealers and mobility platforms · fleet and telematics providers.

Packaged for how automotive companies buy

Eleven Codec Networks bundles apply directly to automotive and mobility companies:

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

Component suppliers, dealers and charging start-ups

- IT and plant or backend assessment
- Backup and remote access review
- TISAX or OEM questionnaire readiness
- Policy and privacy pack

Assurance

EV makers, charging networks and mid-sized suppliers

- Vehicle, charger or product security testing
- Plant segmentation and OT review
- Annual independent audit
- 24x7 IT/OT SOC

Continuous Resilience

OEMs, tier-1 majors and fleet platforms

- AIS 189/190 CSMS and SUMS programme
- Continuous app, API and OTA testing
- Supplier and dealer risk programme
- SOC with vehicle-cloud monitoring and Board reporting

Mapped to your obligations

Requirement	How we help	Bundle
Vehicle cyber security and software update management for type approval (AIS 189/190, draft CMVR rules)	CSMS/SUMS readiness, TARA, vehicle and OTA testing	B4, B1, B2
Cyber incidents to CERT-In within six hours; 180-day logs (CERT-In Directions)	IT/OT SOC, IR retainer and reporting support	B7, B8
Risk-based independent cyber audits including OT (CERT-In audit guidelines, 2025)	Independent IT/OT audits	B4, B1
Quarterly cyber incident disclosure by listed companies (SEBI LODR)	Incident records and disclosure support	B4, B8
Customer, vehicle, driver and dealer personal data (DPDP)	DPDPA programme	B6
Global OEM, UN R155/R156, TISAX and EU CRA requirements	ISO/SAE 21434, TISAX and CRA readiness	B5, B9, B11
Card payments at chargers and dealers (PCI DSS)	Payment security review	B2, B5

Why automotive companies choose Codec Networks

CERT-In empanelled

Independent IT/OT audits recognised by regulators and OEM customers.

Certified and accountable

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

Vehicle-to-plant coverage

In-vehicle, OTA, charging, app, cloud and plant OT testing from one team.

Standards-mapped

Findings mapped to AIS 189/190, ISO/SAE 21434, IEC 62443, TISAX and ISO 27001.

Full stack, one partner

Testing, audits, SOC, forensics, privacy and supplier 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 lines, vehicle platforms and ECUs, apps and APIs, OTA pipeline, chargers, DMS and telematics platforms, suppliers and your audit and homologation 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 homologation, audit and incident a non-event.

Tell us 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, 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: Cyber Monitoring Centre (UK), public reporting on JLR and CDK Global, CERT-In, MoRTH. Confirm obligations against the official instruments.