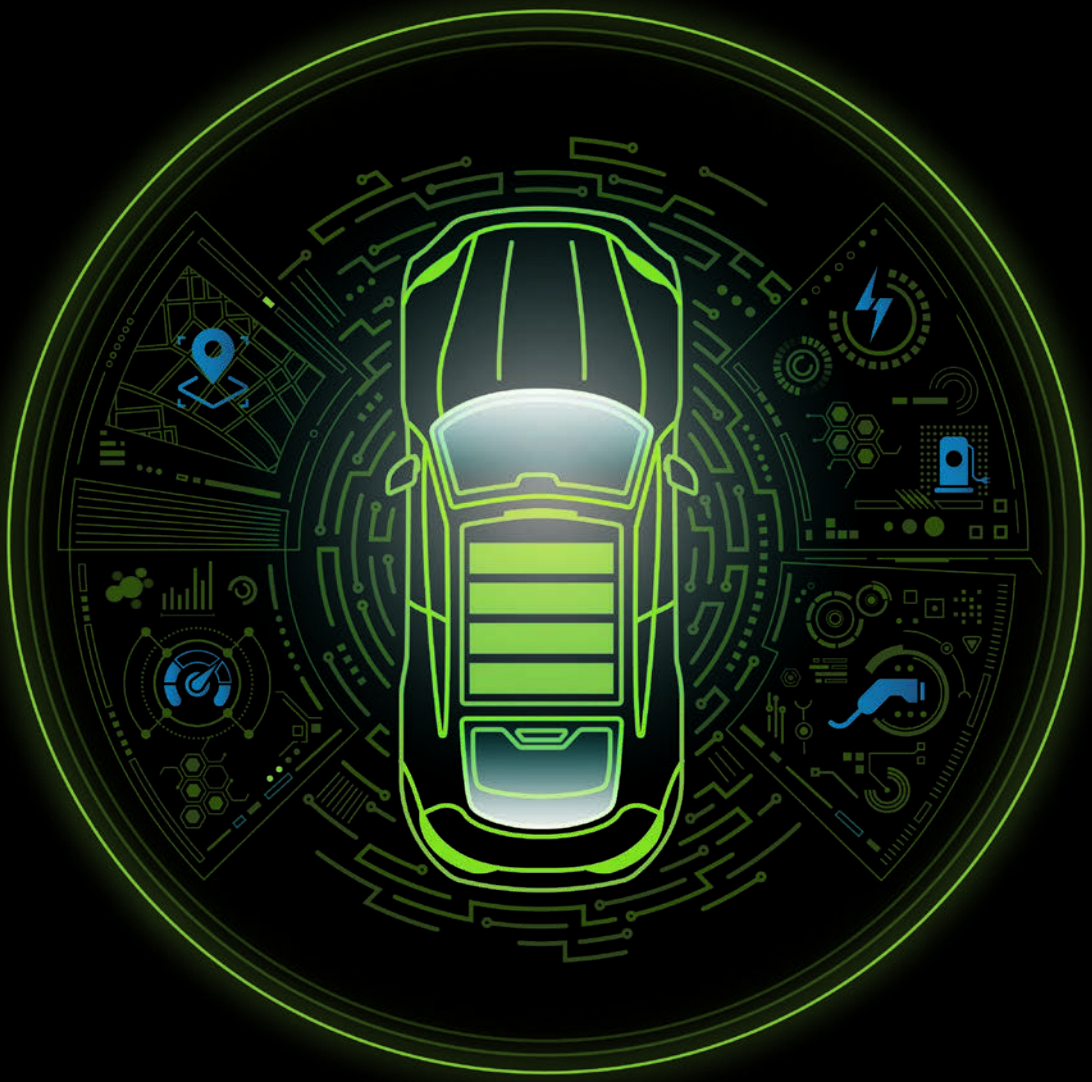
Deloitte.



Wheels of the future, risks of today
Reimagining EV security for India

April 2025

Table of contents

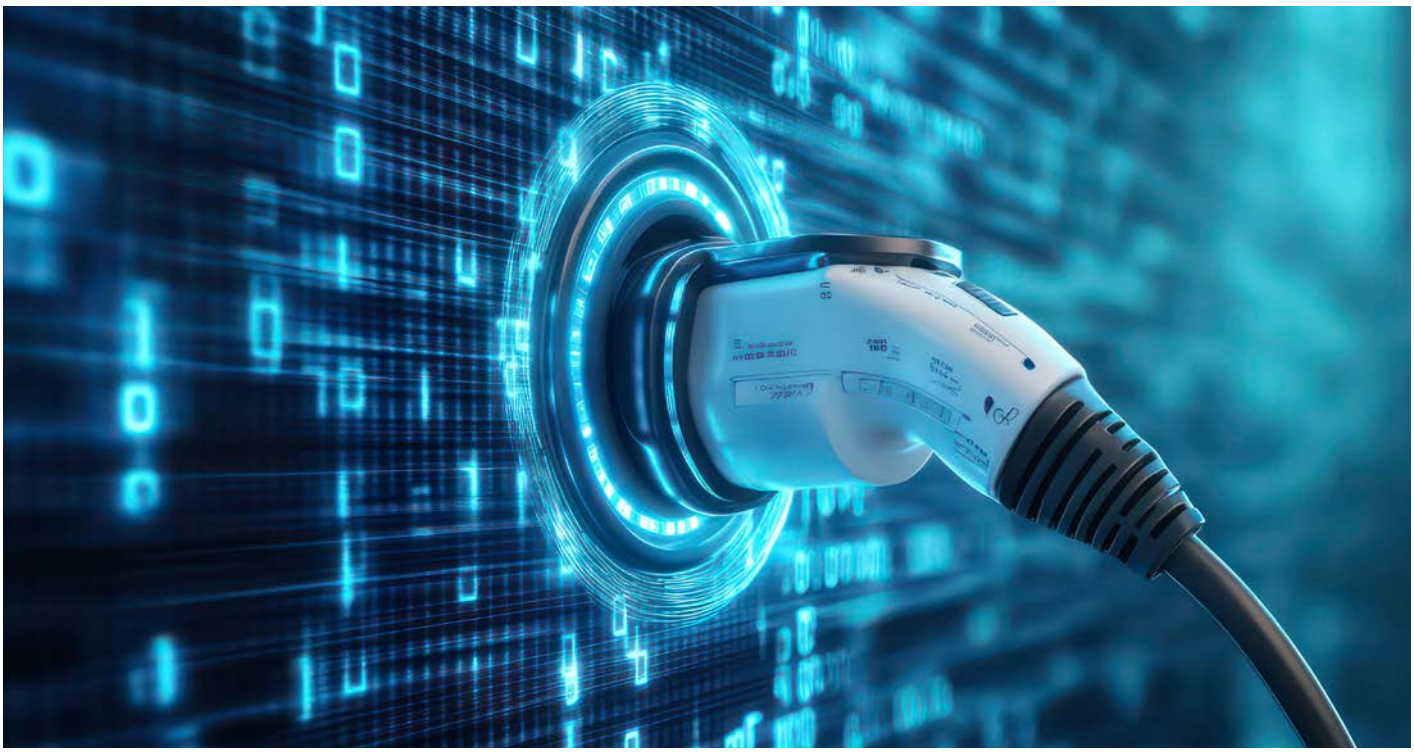
Introduction: A surge in electric mobility

Electric Vehicles (EVs) are rapidly transforming the automotive landscape, offering sustainable and efficient transportation solutions. Over the past decade, the global EV market has witnessed exponential growth. According to the International Energy Agency (IEA),[1] global EV sales surged by 35 percent in 2023, reaching ~14 million vehicles, accounting for 18 percent of all cars sold that year. Projections for 2024 suggest sales will hit ~17 million, making up more than one in five vehicles sold globally. According to the IEA[2], the global number of EVs could reach 145 million by 2030, with an annual growth rate of 29 percent.

India is making significant strides in EV adoption, with the government aiming for 30 percent of all vehicle sales to be electric by 2030[3]. The Indian EV market is projected to grow from US$3.21 billion in 2022 to US$113.99 billion by 2029[4] at a CAGR of 66.52 percent. This rapid growth is fuelled by increasing investments and government incentives, such as the Faster Adoption and Manufacturing of Hybrid and Electric Vehicles (FAME-II) scheme.

However, this transition brings challenges, including substantial investments in charging infrastructure and the need for workforce reskilling. Collaborative efforts are underway between the government and private sector to establish extensive charging networks and support battery energy storage systems.[5]

[1] Global EV Outlook 2024, https://www.iea.org/reports/global-ev-outlook-2024/executive-summary
[2] Ibid #1
[3] India's Electric Vehicle Market, https://www.ibef.org/industry/electric-vehicle#:~:text=India's%20electric%20vehicle%20market%20is,%2C%20with%20a%2066.52%25%20CAGR.
[4] Ibid #2
[5] Invest India, https://www.investindia.gov.in/team-india-blogs/indias-ev-economy-future-automotive-transportation



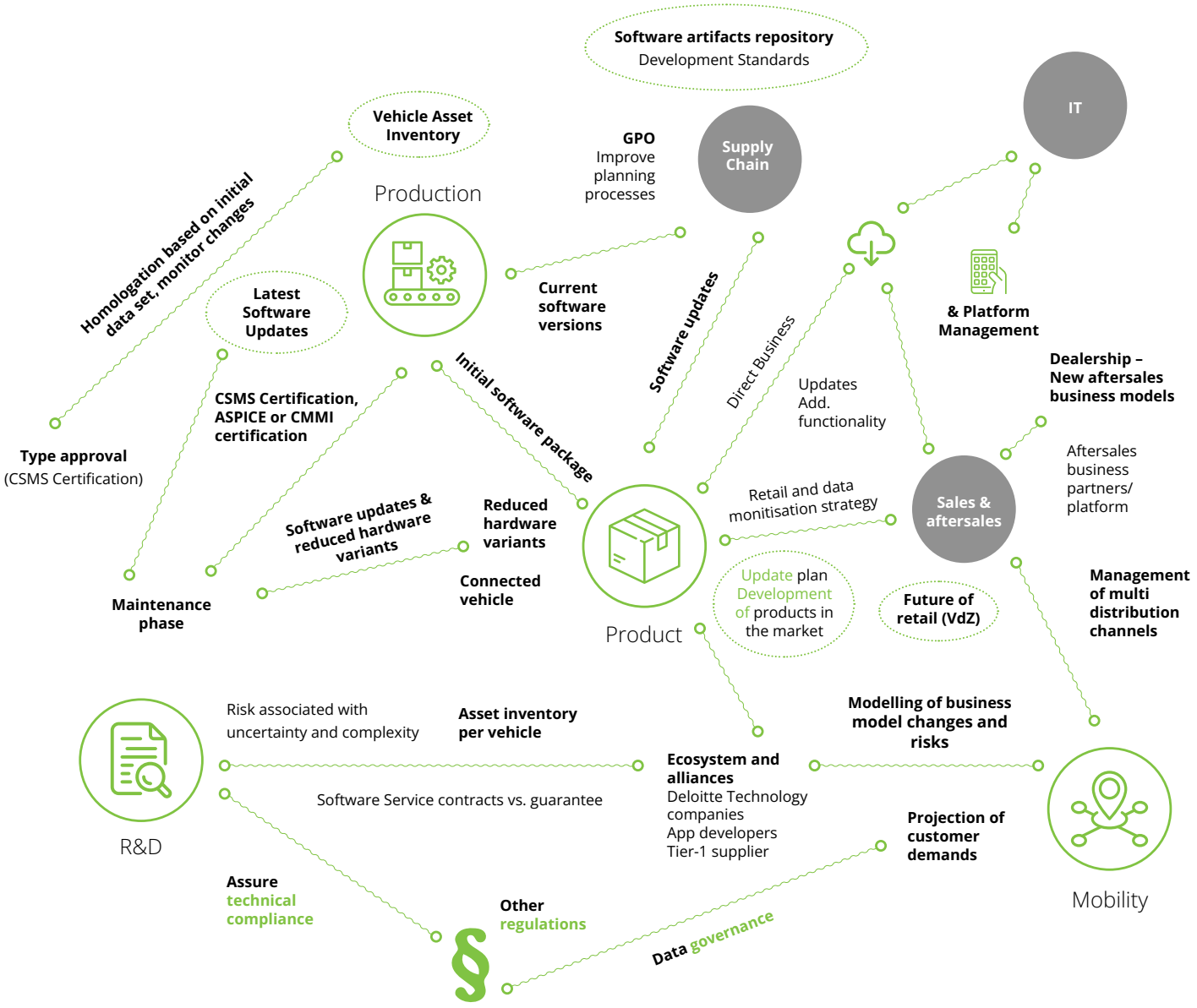
State of cybersecurity in the digital transformation of EVs

The EV landscape spans much more than vehicles; it includes batteries, charging stations, telematics, mobile apps, cloud systems and real-time data flows. While this interconnectivity enhances user experience and operational efficiency, it expands the cyberattack surface exponentially.

The shift to EVs has revolutionised traditional automotive infrastructure, replacing mechanical systems with software-driven technology. Modern EVs rely heavily on connected systems, Over-The-Air (OTA) updates and cloud integration, enhancing performance and introducing new cybersecurity challenges. With complex ECUs and advanced power management, securing software and hardware has become more critical.

Automotive ecosystem

New work organisations and a changed view on the product are necessary



Cyberattacks in the EV world are increasingly targeting data and critical systems, risking user privacy and even passenger safety. For instance, a breach in the EVgo mobile app exposed over 10,000 user accounts,[6] and a ransomware attack on ChargePoint[7] disrupted numerous charging stations. These incidents highlight how hackers can manipulate data and interfere with essential services, emphasising the need for stronger cybersecurity measures. They are a warning sign of what will come if security is not embedded into the core of EV infrastructure.

[6] Security Magazine, https://www.securitymagazine.com/articles/98760-evgo-data-breach-exposes-user-accounts
[7] Nasdaq, https://www.nasdaq.com/articles/chargepoint-updates-data-risks-vital-warning-chpt-shareholders?utm_source=chatgpt.com

Key cybersecurity challenges in the EV and connected vehicles landscape

1

Lack of S-HDLC (Secure Hardware Design Lifecycle):
The EV industry needs a more security-focused approach to hardware design. Without embedding security into the hardware development lifecycle, EVs remain vulnerable to evolving cyber threats.

2

Extreme complexity due to software and hardware overlap:
EV software operates across multiple layers, interfacing with various hardware components. This overlap introduces security risks that must be addressed holistically.

For example, cyberattacks can target the Powertrain Control Unit (PCU)[8], which manages motor operation and battery performance. These attacks could disrupt power delivery, potentially causing dangerous scenarios such as unexpected acceleration.

Similarly, the Battery Management System (BMS)[9] is vulnerable to attacks that could alter charging controls, posing significant safety risks. CAN Bus[10] security is equally critical—without proper segregation, attackers could manipulate braking or acceleration through infotainment systems or OBD-II access.

Hackers may also target complex power electronics that regulate power delivery, potentially resulting in vehicle control loss. Furthermore, Advanced Driver Assistance Systems (ADAS) increase complexity, with potential cyberattacks that manipulate sensor data and cause unsafe actions, such as sudden braking.

[8] Powertrain Control Unit, https://en.wikipedia.org/wiki/Powertrain_control_module
[9] Battery Management System, https://en.wikipedia.org/wiki/Battery_management_system
[10] CAN Bus, https://en.wikipedia.org/wiki/CAN_bus

3

Lack of integrated security features:
The absence of integrated security features makes EV components vulnerable to attacks such as unauthorised access, data breaches and control hijacking. Such vulnerabilities pose serious risks in EV infrastructure where system integrity and availability are critical.

4

Weaknesses in EV charging stations/chargers:
Weak authentication mechanisms, unsecured firmware and API vulnerabilities in EV charging stations can be exploited for payment fraud, data theft or even disruption of power grids.

5

Enlarged attack surface:
A larger attack surface increases the risk of exploitation. Attackers can target multiple components across the EV infrastructure—charging stations, control systems and communication networks—to disrupt operations or exfiltrate sensitive information.

6

Manipulation of hardware behaviour:
Without robust security measures, attackers can manipulate hardware behaviour, enabling malicious firmware uploads, unauthorised access to data and compromised system integrity. This poses severe threats to critical systems within the EV infrastructure.

7

Difficulty and expense of patching:
The complexity and cost of patching hardware vulnerabilities often result in prolonged exposure to known threats, especially in safety-critical EV environments. Delayed responses increase the risk of exploitation.

8

Lack of standardisation in EV security:
Despite frameworks such as ISO 26262 and ISO/SAE 21434, the absence of universally enforced regulations leads to inconsistencies in EV security practices. This results in higher software development costs, compatibility issues, limited functionality and greater exposure to cyber threats. For example, attackers can spoof signals or manipulate data without proper authentication, disrupting traffic flow and vehicle coordination.

9

Supply chain security concerns:
The security of the EV supply chain is a growing concern, particularly with OTA (Over-the-Air) and FOTA (Firmware Over-the-Air) updates. If compromised, these updates can introduce malicious code, allowing remote access or complete control over critical vehicle functions.

10

Privacy concerns in EV security:
Balancing EV integration with data privacy requires a strategic approach to safeguard user data while fostering innovation. EVs collect extensive information on driving patterns, locations and telematics, raising significant privacy concerns and regulatory scrutiny.

As EV adoption grows, smart charging systems gather detailed data such as payment information, charging times and locations—further increasing privacy risks. This interconnected ecosystem also exposes EVs and personal devices to malware, phishing and data breaches, jeopardising user privacy and vehicle security. To combat these risks, companies must implement strong compliance programmes with precise data mapping, updated policies and tight vendor oversight.

Common vulnerabilities encountered in EVs

1. **Charging Control Board (CCB) read protection disabled – Leads to Firmware Dump:** Disabling firmware read protection can expose critical vulnerabilities. Attackers may extract or modify the firmware to alter charging behaviour, potentially damaging the battery or causing safety hazards such as overheating.

2. **Business logic flaws – Free charging exploits:** Weaknesses in payment enforcement logic can be exploited to bypass billing mechanisms, enabling unauthorised free charging and resulting in significant revenue losses for charging station operators.

3. **UDS fuzzing leads to system crash:** Vulnerabilities in the vehicle's CAN network allow unauthorised fuzzing of UDS (Unified Diagnostic Services), causing crashes, remote unlocking and system control. Insecure access to the EPAS ECU can lead to instrument cluster failures and vehicle immobilisation.

4. **Vehicle malfunction due to OBD port exploit:** Shorting PIN 1 and PIN 9 of the OBD-II port may crash the vehicle's internal systems, rendering it unresponsive. This can trigger cascading malfunctions, including TPMS errors, hill-hold control issues and engine start failures.

5 **Authorisation flaw – Remote charging disruption:** A lack of proper authorisation checks in EV charging infrastructure can allow unauthorised users to remotely stop charging sessions. Often caused by Insecure Direct Object Reference (IDOR), this flaw can be exploited to interrupt services for other users.

6 **Malicious USB – Unauthorised AC control:** The infotainment system may be vulnerable to malicious Human Interface Device (HID) attacks. Devices such as Rubber Ducky or Bash Bunny can be inserted to remotely manipulate in-car features such as air conditioning settings, exploiting insufficient USB port protection.

7 **Wi-Fi de-authentication attack:** Even when using WPA2, the vehicle's onboard Wi-Fi is susceptible to de-authentication attacks. Attackers can disconnect users, capture handshake packets, and crack Wi-Fi credentials using tools such as Aircrack-ng and Hashcat.

8 **TPMS data leakage – Unauthorised tracking risk:** Vulnerabilities in the Tyre Pressure Monitoring System (TPMS) can expose sensitive information such as tyre pressure, temperature, model and serial numbers. Attackers can use this data to track vehicles remotely, compromising security and privacy.

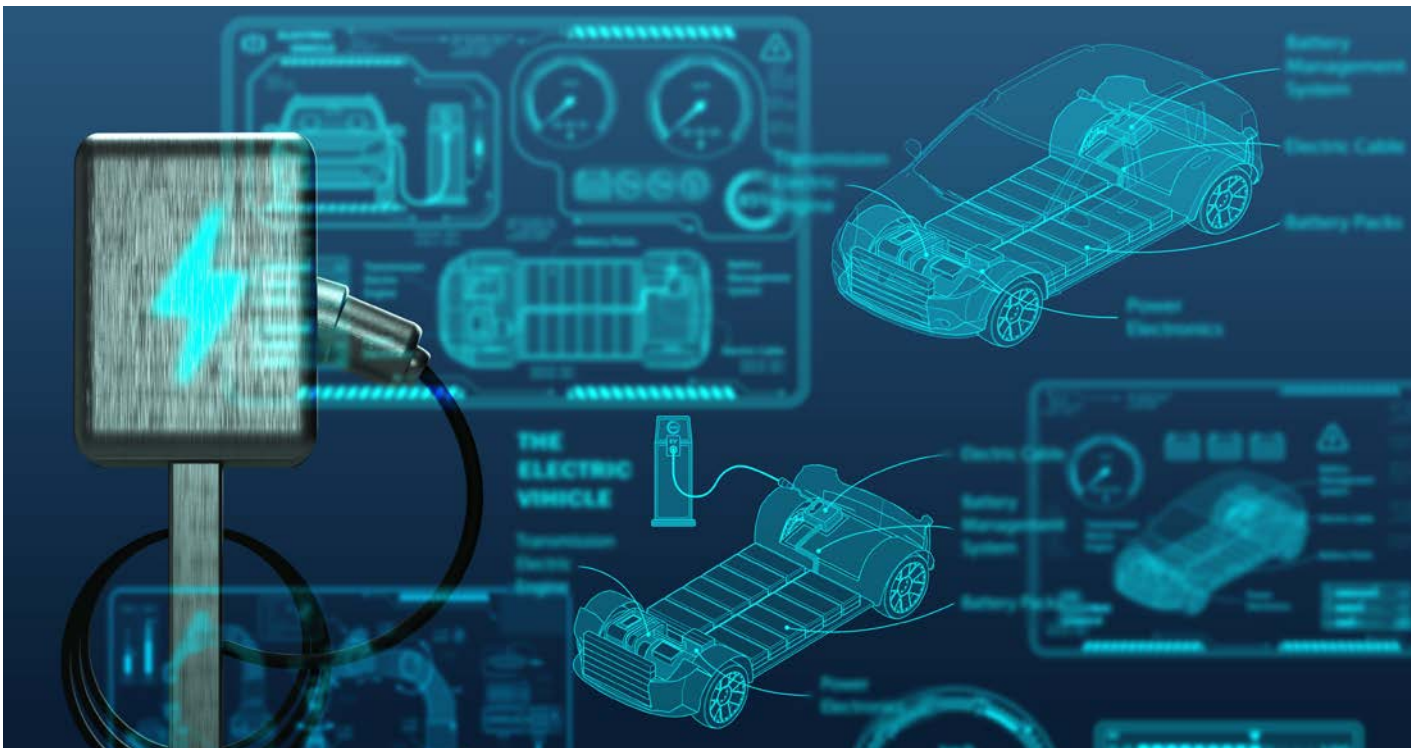
Emerging cyber threats: What's new in 2024 and beyond?

AI-powered attacks on telematics: Attackers are beginning to use AI to spoof telematics systems, enabling vehicle tracking, manipulating predictive maintenance logs, or impersonating vehicle diagnostics to deceive service stations.

Digital twin hijacking: As OEMs adopt digital twins for EV development, cybercriminals can manipulate simulations or feed erroneous data, leading to faulty vehicle/ production behaviour or disrupted supply chain analytics.

EV grid manipulation through coordinated charging attacks: Malicious actors could simultaneously activate or deactivate a fleet of EV chargers, triggering localised blackouts or power surges and risking national grid security. This is possible in poorly designed mobile applications for customers, where the APIs used to interact with the charging stations are exposed without authentication and authorisation.

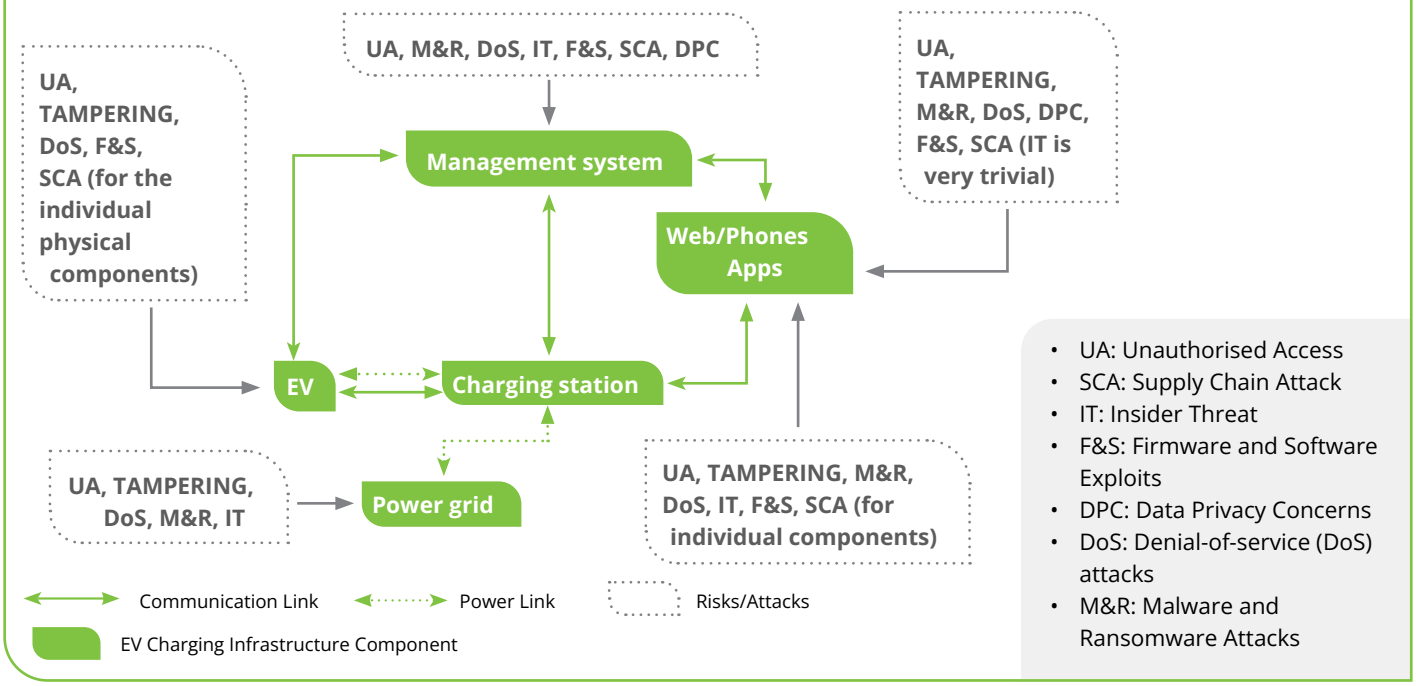
Quantum risks on the horizon: With quantum computing gaining traction, traditional encryption used in EV communication (e.g., TLS, RSA) will become breakable. Future-proofing systems with Post-Quantum Cryptography (PQC) must begin now.



Mitigating EV security risks: A multi-layered blueprint

EVs are transforming transportation, but it is crucial to secure the entire ecosystem, including vehicles, chargers and networks.

Mapping cyber risks/attacks against EV charging infrastructure



A multi-layered approach is essential. While not exhaustive, the following measures are key:

1. **Security and privacy by design:** EV security should be embedded from the ground up, incorporating strong encryption, secure coding practices and compliance with data privacy laws such as GDPR. Data collection should be minimised, and sensitive information must be securely stored to prevent breaches.

2. **Comprehensive security testing:** Regular security assessments of EV software, charging stations, mobile applications, and associated cloud systems and services help identify and remediate vulnerabilities. Penetration testing, firmware validation, and third-party assessments are essential to maintain robust protection.

3. **Zero trust architecture:** All access requests must be authenticated and authorised, adhering to a strict least privilege principle. Network segmentation and continuous monitoring enable early detection and prevention of unauthorised activities.

4. **Secure communication and encryption:** Data exchanged between EVs, chargers and backend systems must be encrypted using secure protocols. Effective key management is critical to prevent unauthorised access or data leaks.

5. **Supply chain security:** Third-party components should undergo rigorous security vetting. Implementing firmware signing and integrity verification ensures malicious code is not introduced through the supply chain.

6. **Secure OTA updates:** OTA updates must be encrypted and authenticated before installation. Timely vulnerability patching through secure updates is vital to maintaining system integrity.

7. **Physical security of chargers:** Charging stations must be designed to resist tampering and unauthorised access to underlying hardware and firmware. Strong physical access controls, surveillance and user authentication can help protect against sabotage or misuse.

Global EV trends: Expansion and technological progress

The EV market is accelerating, with sales surpassing 10 million in 2022[11] – a 55 percent jump from the previous year. Declining battery costs, government incentives and a strong push for sustainability drive the growth. China leads the charge, followed by Europe and the US[12], with increasing demand for electric SUVs and commercial EVs. To maintain this momentum, expanding charging infrastructure and implementing supportive policies remain crucial.

With EVs becoming more connected, cybersecurity must be a top priority. A breach of vehicle systems or charging networks could disrupt operations, expose sensitive data, or even compromise passenger safety. To protect against cyber threats, manufacturers must embed security from the ground up, using encryption, delivering regular software updates and ensuring robust compliance measures.

A secure EV ecosystem is key to long-term success, ensuring safety, reliability and trust in the future of mobility.

[11] Global EV Outlook 2023, https://www.iea.org/reports/global-ev-outlook-2023/trends-in-electric-light-duty-vehicles
[12] Times of India, China Drives 80% of Global EV Sales Growth in 2024, IEA Report Reveals - Times of India

Accelerating EV cybersecurity: End-to-end protection for a connected future

Security and privacy by design
Security should be integrated into every stage of EV development, from secure coding practices to privacy-compliant data handling. Frameworks must align with GDPR, ISO 21434 and other industry standards to safeguard sensitive information.

Comprehensive security testing
Thorough vulnerability assessments and penetration testing are essential across EV software, charging stations, mobile apps and cloud platforms. Simulating real-world attack scenarios helps identify and mitigate security gaps before exploitation.

Zero trust architecture
Every access request should be verified, following a strict least-privilege model. Network segmentation and continuous monitoring help detect and block unauthorised activities.

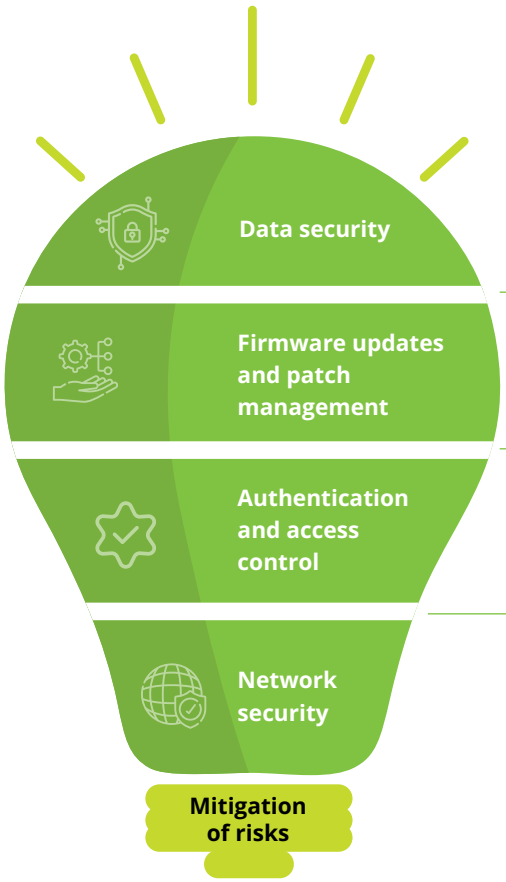
Supply chain security
Third-party components must be evaluated to ensure hardware and software suppliers meet stringent security requirements. Supply chain risk management should include firmware integrity verification, vulnerability assessments and compliance audits.

Physical security of chargers
Charging stations must be designed with tamper-resistant hardware, surveillance integration and strong access controls. These measures help minimise the risk of physical attacks, fraud or unauthorised access.

Secure communication and encryption (PKI)
Encryption strategies should employ strong cryptographic protocols such as TLS and PKI-based authentication. This ensures secure communication between EVs, chargers and cloud systems, preventing data breaches and man-in-the-middle attacks.

Security Operations Centre (SOC)
A dedicated SOC enables 24/7 monitoring, threat detection and rapid incident response across EVs, charging stations and cloud infrastructure. SIEM tools and automated threat intelligence enhance visibility, compliance and cyber resilience across the EV ecosystem.

Mitigation of cyber risks in the automotive landscape



Use strong encryption protocols to safeguard user information, charging history and payment details during transmission and storage.

It is crucial to address vulnerabilities to effectively mitigate potential security risks. One way to achieve this is by ensuring that the firmware of charging stations is always kept up-to-date. This will help maintain compatibility with new security protocols and standards.

Use RFID cards to ensure that only authorised users can access the charging stations. Enhance user authentication by developing mobile applications with secure login features.

Numerous EV infrastructures are linked to the Internet, which exposes them to potential cyberattacks and outgoing network traffic. It is imperative to establish robust network security measures to safeguard against these vulnerabilities.

CXO watch: Why EV cybersecurity is a boardroom agenda

For CXOs—particularly CISOs, CIOs, CTOs and CROs—EV infrastructure security is no longer just a technical concern but a strategic business priority. The EV ecosystem touches national grid infrastructure, consumer trust, urban mobility and digital commerce. One breach in a charging station or a vehicle's control system can lead to reputational damage, regulatory fines, service disruptions and safety risks.

Cybersecurity in EVs is not about avoiding hypothetical threats. It is about protecting critical infrastructure, maintaining customer trust and enabling secure growth at scale. To secure the EV ecosystem, CXOs should embed cybersecurity into their core digital and product transformation strategy:

1

Executive-backed secure-by-design mandate
Adopt a zero-trust approach across the EV lifecycle—from design to decommissioning. Make security architecture reviews and threat modelling a board-level KPI.

2

Proactive regulatory alignment
Prepare for converging global EV and cybersecurity laws, including India's DPDP Act, UNECE WP.29, ISO/SAE 21434 and the evolving EU Cyber Resilience Act. Early compliance = market edge.

3

Cybersecurity-as-a-Service (CaaS) models
Collaborate with cybersecurity providers to adopt SaaS-like Managed Detection and Response (MDR) for real-time monitoring of charging stations, vehicle software and backend platforms.

4

Digital twin + red team testing
Simulate attacks on digital twins of EV ecosystems to test real-world resilience. Red teaming can uncover flaws that traditional testing misses, especially in EV networks and ADAS.

5

Secure IT and firmware supply chain
Introduce firmware signing, attestation mechanisms and third-party Software Bill of Materials (SBOM) validation to reduce risk from component suppliers.

6

Post-quantum encryption pilots
Start deploying hybrid cryptographic protocols to future-proof EV-to-cloud communications. A quantum-safe EV roadmap is now a competitive differentiator.

7

Build trust, not just technology
The future of EVs is undeniably electric, but trust will be its true fuel. As vehicles become smarter, their attack surfaces will only grow. For CXOs, the opportunity lies in mitigating risks and turning cybersecurity into a brand promise, regulatory shield and revenue enabler. A resilient EV infrastructure can accelerate consumer adoption by ensuring privacy and safety, preventing business downtime through robust threat detection, enabling regulatory compliance globally, protecting R&D investments and IP and driving investor confidence in long-term growth.

Conclusion: Cyber resilience is the new horsepower

As EVs transform transportation, integrating cybersecurity into every aspect of this ecosystem is essential. With the rapid growth of EV adoption, security must extend across vehicles, charging infrastructure, software platforms and communication networks. This interconnected landscape demands a proactive, collaborative and adaptive security approach from businesses, governments and innovators alike.

Cybersecurity is not a luxury; it is the bedrock of sustainable e-mobility. For organisations, embedding robust cybersecurity practices ensures long-term growth, regulatory compliance and customer trust. Governments play a crucial role by creating secure infrastructure, enforcing standards and fostering innovation within the EV ecosystem.

As we accelerate toward a greener, more efficient future, cybersecurity must be integrated from the ground up—protecting vehicles, infrastructure and data. Those prioritising security today will safeguard their fleets and consumers and lead the charge into tomorrow's transportation revolution. Ultimately, cybersecurity is a strategic growth driver, and as the EV ecosystem expands, it will differentiate those who are prepared for the next era of mobility.

True transformation lies not just in electrifying transportation but in securing it. Cyber resilience must become the new horsepower—powering performance, trust, safety and long-term growth. Tomorrow's EV landscape leaders will act today—embedding security by design, strengthening digital trust and driving a secure, sustainable future on wheels.

Connect with us

Sathish Gopalaiah
President, Technology & Transformation
Deloitte South Asia
sathishtg@deloitte.com

Deepa Seshadri
Partner and Leader – Cyber
Deloitte South Asia
deseshadri@deloitte.com

Gaurav Shukla
Partner
Deloitte India
shuklagaurav@deloitte.com

Santosh Jinugu
Partner
Deloitte India
sjinugu@deloitte.com

Contributors

Anas Jamal

Buvanasri A K

Harsh Shahi

Meenakshi R

Saubhagya Srivastava

Sunita Kumari

Zahir Pathan

Deloitte.