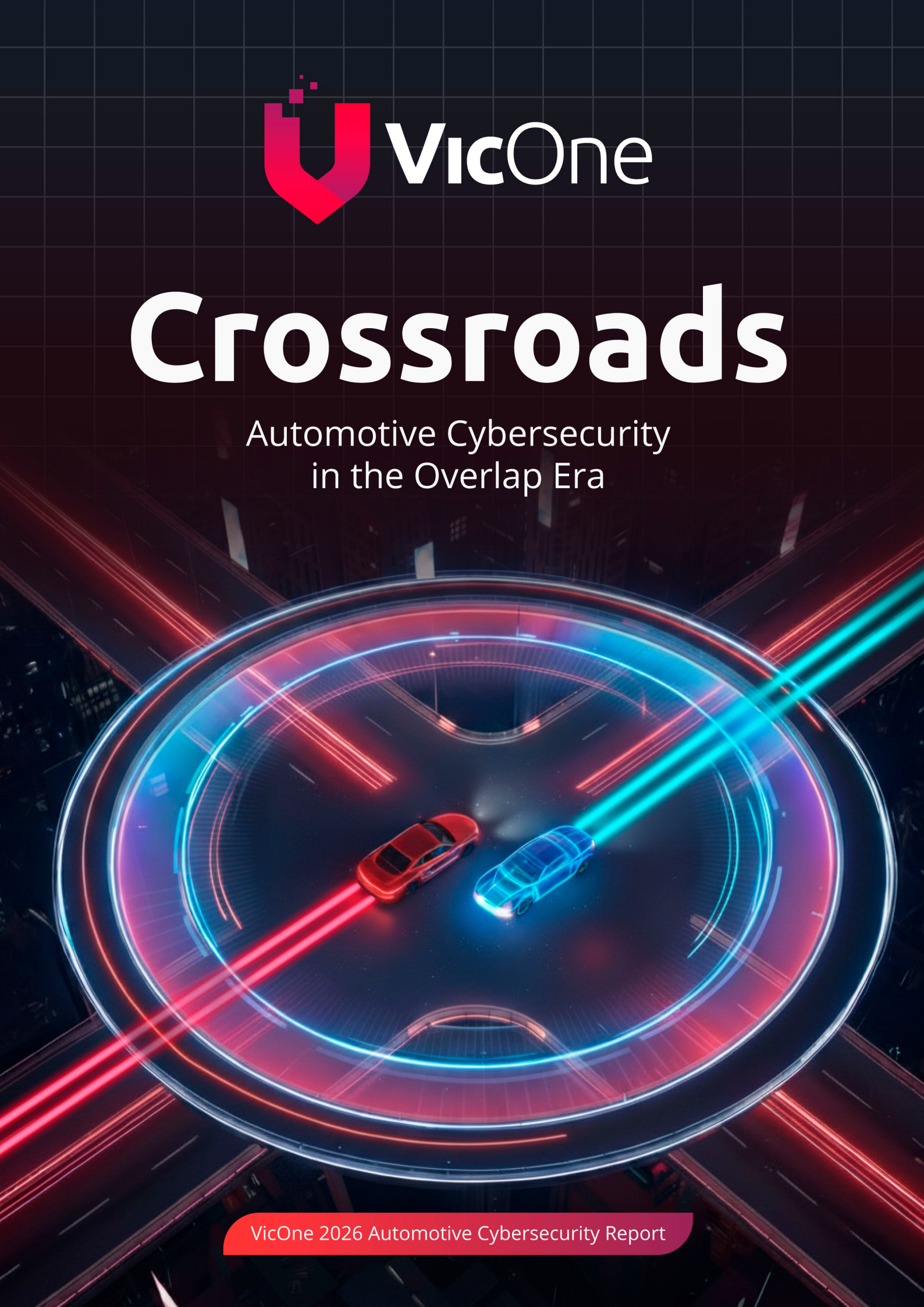
VicOne

Crossroads

Automotive Cybersecurity in the Overlap Era



VicOne 2026 Automotive Cybersecurity Report

Executive Summary

The automotive industry has entered what this report defines as the Overlap Era — a period in which traditional vehicle platforms remain dominant across global fleets, while software-defined, connected, and AI-enabled technologies rapidly move into mass production, creating often conflicting cybersecurity assumptions.

This coexistence introduces a dual-track challenge. Automotive manufacturers must continue managing the well-understood risks embedded in legacy vehicle architectures, while simultaneously preparing for emerging threats driven by cloud-native development, continuous software updates, and increasingly autonomous system behavior.

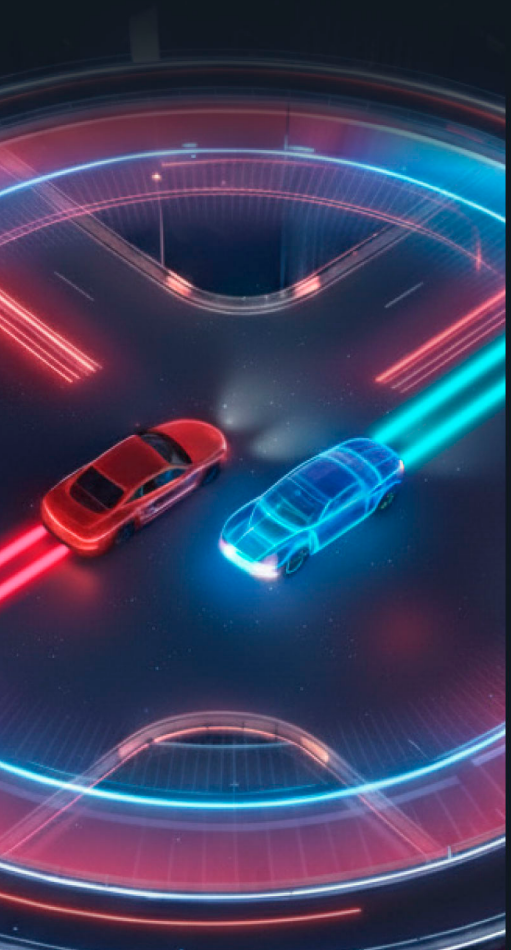
In the Overlap Era, cybersecurity responsibilities fragment, assumptions diverge, and risk outpaces governance as vehicles continue evolving long after production. This report examines the structural forces reshaping automotive cyber risk across vehicle platforms, in vehicle domains, AI, and regulation, and outlines how industry stakeholders can respond.

The report is organized as follows:

> **Chapter 1. Structural Shifts in the Automotive Threat Landscape** highlights how today's cyber threats are driven less by unexpected attacker sophistication and more by architectural complexity, governance gaps, and the growing concentration of software responsibility within safety-relevant systems.
>
> **Chapter 2. Overlapping Cyber Risks Across Vehicle Domains** presents past, present, and emerging risk patterns across vehicle functional domains, emphasizing how cybersecurity challenges extend beyond individual systems.
>
> **Chapter 3. How AI Is Reshaping Cyber Risk Management** examines how AI-related risk patterns observed in 2025 are altering the way existing vulnerabilities propagate, scale, and influence vehicle behavior.
>
> **Chapter 4. Regulatory Blind Spots in the Overlap Era** illustrates how domain-specific regulations, while essential, may leave systemic risks insufficiently governed when viewed from an end-to-end automotive cybersecurity perspective.
>
> **Chapter 5. Recommendations** and **Chapter 6. Predictions** conclude the report with strategic considerations for what must evolve in the Overlap Era, alongside forward-looking insights into how automotive cyber risk is likely to develop in the years ahead.

As the automotive industry enters an era of overlapping risk domains, fragmented responsibility is no longer sustainable. This has brought the industry to a crossroads — where decisions made today around cybersecurity governance, architecture, and accountability will shape how trust, safety, and resilience are sustained across future vehicle platforms.

Table of Contents



CHAPTER 1

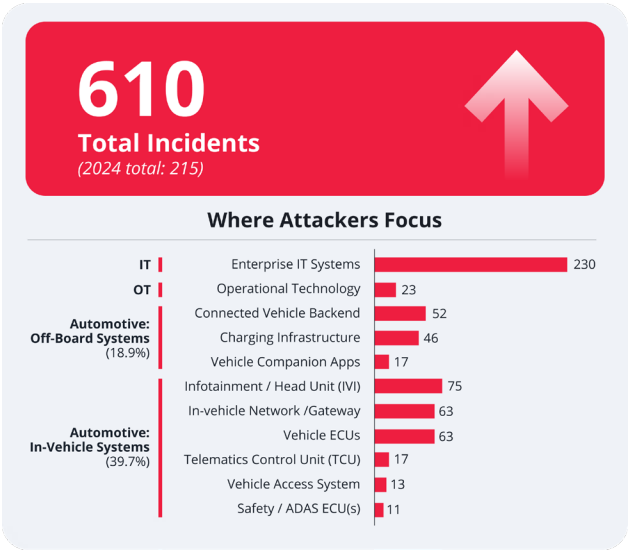
Structural Shifts in the Automotive Threat Landscape

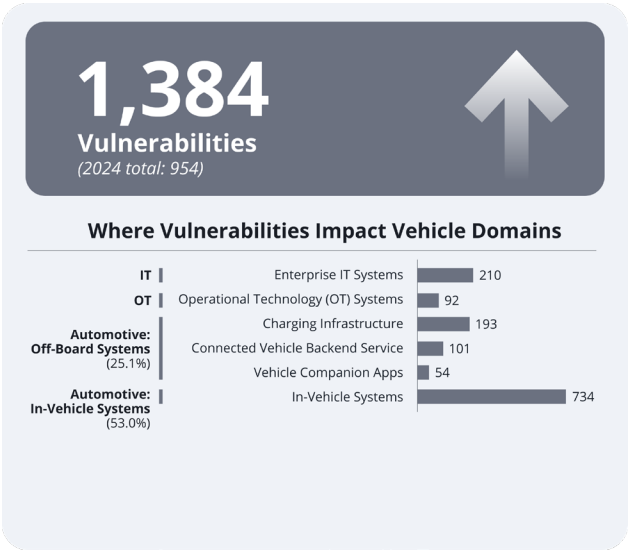
In 2025, the VicOne CyberThreat Research Lab monitored nine core coverage areas, spanning real-world security incidents, more than 1,000 unique dark and deep web sources, zero-day discoveries from Pwn2Own Automotive, public vulnerability disclosures, Tier-1 and Tier-2 supplier advisories, academic research, and intelligence from global regulatory and law-enforcement agencies.

Drawing from this extensive data set, 610 automotive-related security incidents and 1,384 vulnerabilities were reported in 2025 — representing a significant increase compared with 2024. While innovation and regulatory compliance continued to advance, attacker activity intensified in parallel. Ransomware campaigns targeting the automotive industry resulted in an estimated US$300 million in losses, while attacks against in-vehicle infotainment (IVI) systems rose sharply.

In addition to dealership-focused incidents, threat actors increasingly targeted automotive OEMs, including high-impact supply-chain disruptions such as the Jaguar Land Rover cyber incident.[1] The overview and the key findings that follow highlight the structural shifts in the 2025 automotive threat landscape.

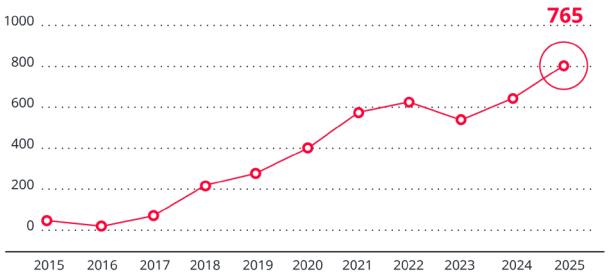
At a Glance: The 2025 Automotive Threat Landscape





Where Attackers Starts

Risk exposure driven by Critical and High-severity vulnerabilities continues to grow



Cyberattacks Now Aim for Maximum Disruption, Not Just Data Theft

Cost	2023	2024	2025 Jan - Oct
Data leakage	$9.7B	$20.0B	**$6.6B**
System downtime	$2.5B	$1.9B	**$2.5B**
Ransomware damage	$523.6M	$538.2M	**$302.3M**
Total	**$12.8B**	**$22.5B**	**$9.4B**

Finding #1: Attack surface expansion reflects governance gaps, not technical surprise

What appears to be rapid attack surface expansion is not driven by new threat innovation. It reflects a growing disconnect between how automotive systems now operate and how cyber risk is still governed.

In 2024, automotive cybersecurity incidents were largely concentrated in cloud and backend systems, as well as vehicle hijacking–related threats. These incidents commonly involved ransomware, data breaches, and social engineering attacks. Attackers consistently chose paths that offered the highest impact at the lowest cost. Enterprise IT became the primary entry point not because vehicles were less valuable, but because backend platforms had already become the operational control plane for vehicle functionality and services.

By 2025, this pattern has shifted. Analysis of 610 automotive cybersecurity incidents shows that attacks no longer remain confined to a single layer. Instead, they span enterprise IT systems, automotive off-board systems, and in-vehicle systems simultaneously. Domains that organizations traditionally treated as separate risk areas began to overlap in real-world attacks.

This apparent "attack surface expansion" does not signal a sudden evolution in attacker strategy. It reflects a more fundamental reality. Vehicles, cloud platforms, and enterprise IT have become tightly coupled by design, while risk governance, ownership, and decision-making remain fragmented. As a result, security incidents are now exposing structural gaps in governance rather than technical blind spots.

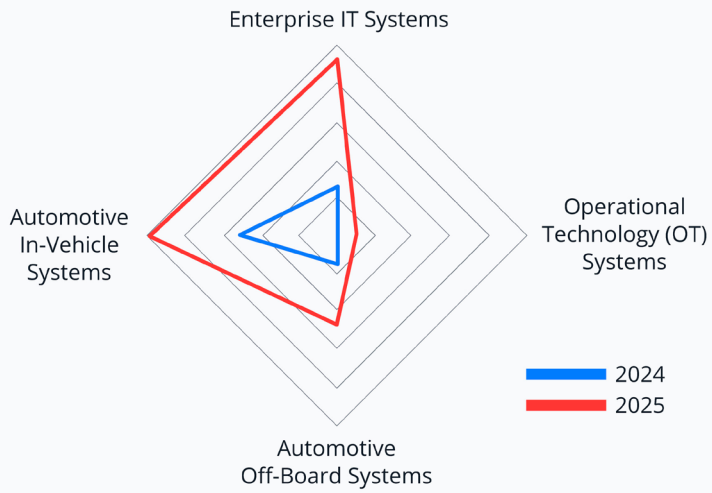


Figure 1. Cyber incidents in 2025 increasingly span multiple system domains, underscoring the growing disconnect between integrated automotive architectures and fragmented risk governance

Finding #2: Cyber risk is moving closer to the driver

In 2025, automotive attacks increasingly target in-vehicle systems that drivers interact with directly. This shift reflects rising attacker maturity, as cyber risk moves from hidden components into user-facing layers where impact becomes immediate and visible.

Analysis of 2025 automotive cybersecurity incidents shows that attackers increasingly focus on points of interaction and integration rather than on isolated, deeply embedded components. In-vehicle systems now account for the largest share of observed targeting (39.7%), narrowly surpassing enterprise IT systems (37.7%). This signals a structural shift in how automotive cyber risk is being exploited.

Within in-vehicle environments, this concentration becomes even clearer. The most frequently targeted areas include IVI or head units (12%), in-vehicle networks and gateways (10%), and electronic control units (ECUs) and embedded software (10%). These systems share a defining characteristic. They serve as the primary interfaces where drivers, vehicle functions, and external services converge. This distribution is not accidental. These systems act as natural aggregation points, where multiple domains converge: user input, connectivity, feature control, and system orchestration.

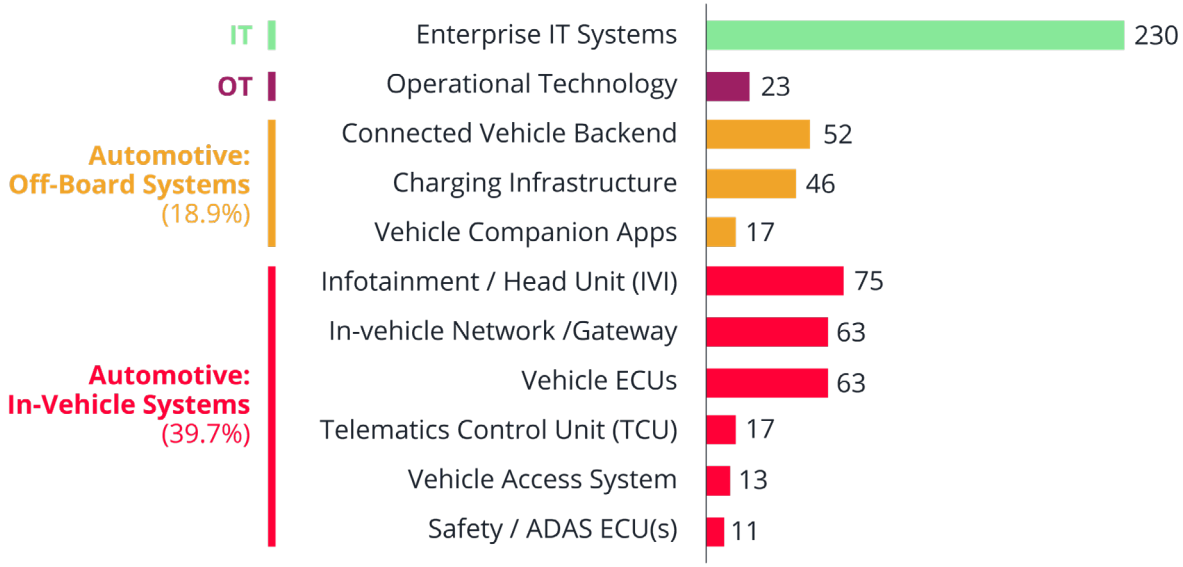


Figure 2. Where attackers focused: control points across the automotive ecosystem.

Recent incidents illustrate this shift clearly. In January 2025, research on the Mercedes-Benz head unit showed how compromise via physically exposed interfaces (notably USB and diagnostic pathways) can turn the infotainment system into a practical pivot for interacting with diagnostic functions and other ECUs.[2] In April 2025, researchers demonstrated an attack chain on the Nissan Leaf that starts from the infotainment Bluetooth stack, achieves code execution, and ultimately enables Internet-reachable control of selected body functions through subsequent in-vehicle pivots.[3] In both cases, the

entry point was not an obscure low-level component, but an externally exposed interface that bridges multiple vehicle subsystems.

As a result, automotive cyber risk is no longer primarily hidden in deeply embedded layers of the vehicle's architecture. It is increasingly introduced through interfaces that are visible, reachable, and behaviorally meaningful to drivers.

This shift reflects a rise in attacker maturity. Rather than relying on rare physical access or highly specialized hardware exploitation, attackers are demonstrating a growing understanding of how modern vehicles are actually used and integrated. Automotive cyber risk is therefore moving upward in the architecture, into user-facing integration layers, where technical vulnerabilities translate more directly into operational, safety, and reputational consequences.

Finding #3: Platform centralization has increased the blast radius of a single incident

Global automotive cyber incidents increased by approximately 250% year over year from 2024 to 2025, underscoring how centralized software platforms and shared services have reduced organizations' ability to contain security failures locally.

Among the 610 automotive cybersecurity incidents recorded in 2025, the Americas remained the most affected region, primarily driven by North America. Asia experienced the fastest growth, with incidents concentrated in Japan, India, and China, followed closely by Europe, particularly Germany and the United Kingdom.

Most notably, incidents with impact extending beyond a single subsidiary or business unit (also known as global incidents) increased to 161 cases in 2025, more than tripling year over year compared with 2024.

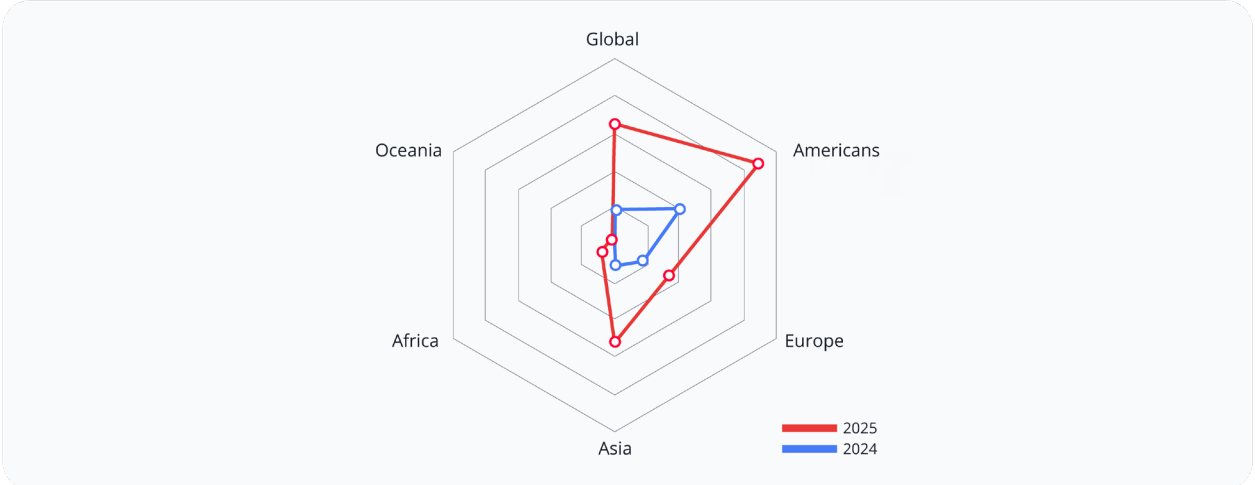


Figure 3. Regional distribution of automotive cybersecurity incidents from 2024 to 2025

These global incidents no longer affect isolated systems or individual vehicle models. Instead, they directly disrupt:

- Global over-the-air (OTA) and connected services
- Cross-market operational continuity
- Regulatory exposure, brand trust, and financial performance

In highly centralized software and OTA architectures, the blast radius of a single security incident expands rapidly. As a result, automotive cyber risk has become a board-level governance issue rather than a problem confined to individual technical or security teams.

Finding #4: Visibility without governance creates a false sense of control

When incidents span IT, cloud, and vehicle environments, visibility built around individual systems fails to support accountable, time-bound decisions. Dashboards may show alerts, but they do not resolve the questions that determine outcomes: what is impacted, who owns the decision, and when intervention is required.

According to Findings 1–3, automotive cyber risk in 2025 no longer resides within a single system domain. Incidents increasingly span enterprise IT, cloud platforms, and in-vehicle systems, creating cross-domain exposure that cannot be contained locally.

On the surface, visibility appears strong. In 2025, approximately **89% of known automotive vulnerabilities were tracked through public common vulnerabilities and exposures (CVE) databases,** suggesting a high level of transparency and reporting maturity. However, the remaining **11% emerged outside formal CVE channels,** including independent research, undisclosed vulnerabilities, and a zero-day vulnerability discovery contest. Since co-hosting Pwn2Own Automotive with the TrendAI Zero Day Initiative (ZDI) in 2024, we have uncovered a total of 174 zero-day vulnerabilities targeting connected vehicles, software-defined vehicle (SDV) and electric vehicle (EV) charging infrastructure as of 2026.[4] These non-CVE findings often remain exploitable, yet fall outside standard reporting, escalation, and oversight workflows. Not because they lack relevance, but because governance processes frequently treat CVE status as the prerequisite for action.

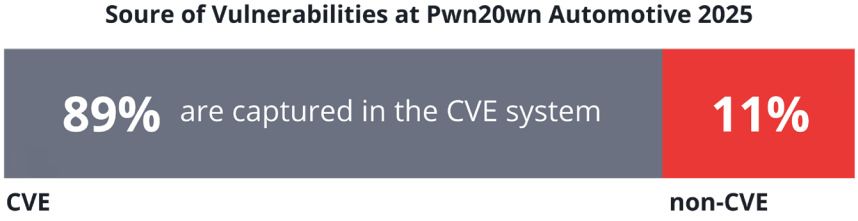


Figure 4. Percentage of CVE and non-CVE reported in 2025

As a result, many organizations rely heavily on dashboards, alerts, and CVE-based reporting to assess risk exposure. This creates the *appearance* of comprehensive visibility, but not effective risk control. The underlying governance model remains system-centric, while real-world impact propagates across platforms, services, and product lifecycles.

When incidents cross IT, cloud, and vehicle boundaries, system-centric visibility breaks down. Risk signals are evaluated within individual teams. Decision authority fragments across organizational silos. Critical actions are delayed as information is reconciled through manual coordination, meetings, and email. In practice, risk is governed by what fits existing dashboards and disclosure frameworks, rather than by exploitability, potential impact, or persistence across vehicle generations.

The result is a false sense of control. Organizations can see more signals than ever, yet still struggle to answer the questions that determine outcomes: **what is impacted, who owns the decision, and when intervention is required.**

What is required is not more alerts or broader monitoring. It is a governance model capable of continuously correlating exposure across domains, incorporating vulnerabilities beyond formal disclosure channels, and translating technical signals into accountable, time-bound decisions with clear ownership. Without this shift, increased visibility will not reduce cyber risk. It will only delay accountability as exposure continues to accumulate.

Finding #5: Vulnerability growth is becoming structurally misaligned with automotive remediation realities

Automotive vulnerabilities are accumulating faster than they can be eliminated through patches and updates, transforming cyber exposure into a persistent lifecycle risk.

Over the past decade, reported vulnerabilities across multiple automotive technology domains have followed a sustained upward trajectory, without a structural return to earlier baseline levels. In in-vehicle systems in particular, vulnerability counts have risen sharply since 2018 and, despite periodic fluctuations, have remained consistently elevated relative to historical norms.

Connected backend services and charging infrastructure show a similar stepwise growth pattern, reflecting how vulnerability exposure expands alongside vehicle software complexity and service integration. While enterprise IT and OT systems represent a smaller share of total findings, recent acceleration in these areas further broadens the overall risk footprint.

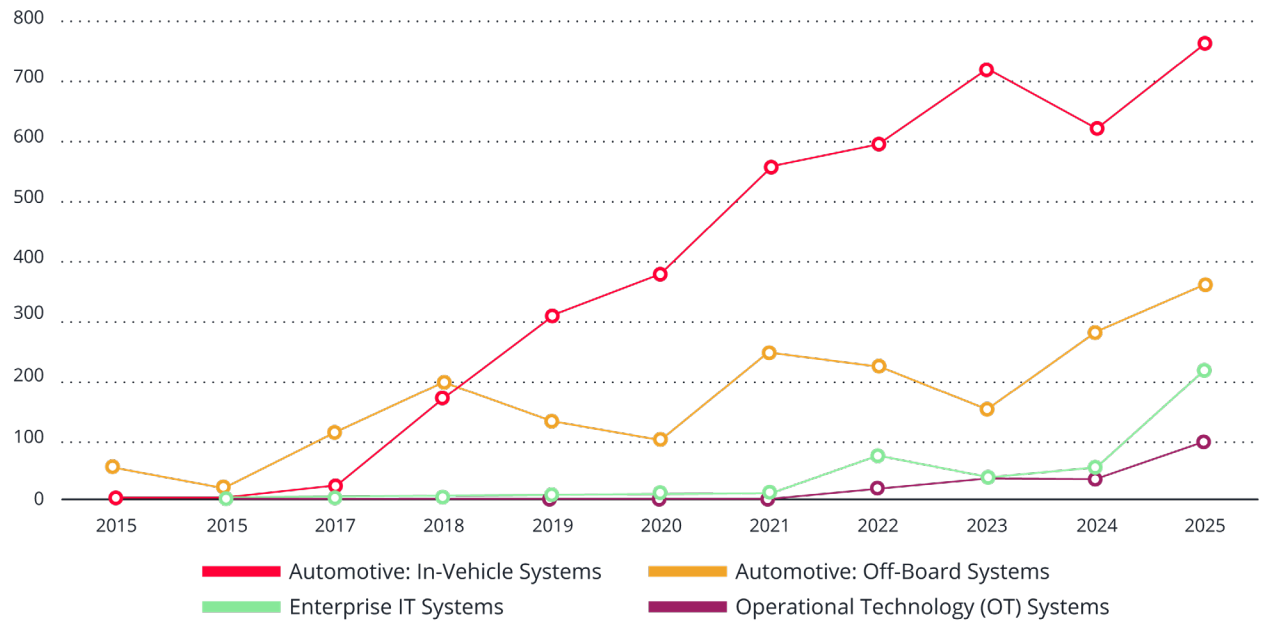


Figure 5. Long-term growth of automotive vulnerabilities across system domains from 2015 to 2025

These trends do not primarily indicate a failure to patch individual vulnerabilities. Rather, they expose a fundamental constraint: the fastest-growing sources of exposure are systems with long lifecycles, limited update windows, and tightly coupled dependencies. In such environments, even when vulnerabilities are identified and addressed, residual exposure often persists across multiple product generations and service platforms.

As a result, the central challenge facing the automotive industry is no longer whether individual vulnerabilities can be remediated, but whether long-term risk exposure can be governed when vulnerability accumulation structurally outpaces feasible remediation. Without a shift toward lifecycle-oriented risk management, cyber exposure will continue to compound even as patch activity increases.

Finding #6: High-severity vulnerabilities are extending the effective duration of automotive cyber risk

The continued rise of critical and high-severity vulnerabilities means that cyber risk increasingly persists across product generations, services, and platforms, rather than being contained within individual patch cycles.

Since 2017, the absolute number of critical and high-severity automotive vulnerabilities has shown a sustained upward trend. Even in years when overall vulnerability growth moderated, high-severity findings remained well above historical baselines and continued to accumulate.

This pattern indicates that growth in high-severity vulnerabilities is not being diluted by lower-impact findings. Instead, material risk exposure is expanding in parallel with overall vulnerability volume. From a risk perspective, the industry is not facing an inflation of minor defects, but a steady accumulation of issues with meaningful safety and operational impact.

More importantly, high-severity vulnerabilities demonstrate strong persistence over time. The data does not reflect isolated annual spikes followed by resolution, but rather a pattern of compounding exposure built on an already elevated baseline. As a result, the effective duration of cyber risk is increasing, rather than naturally declining through remediation cycles.

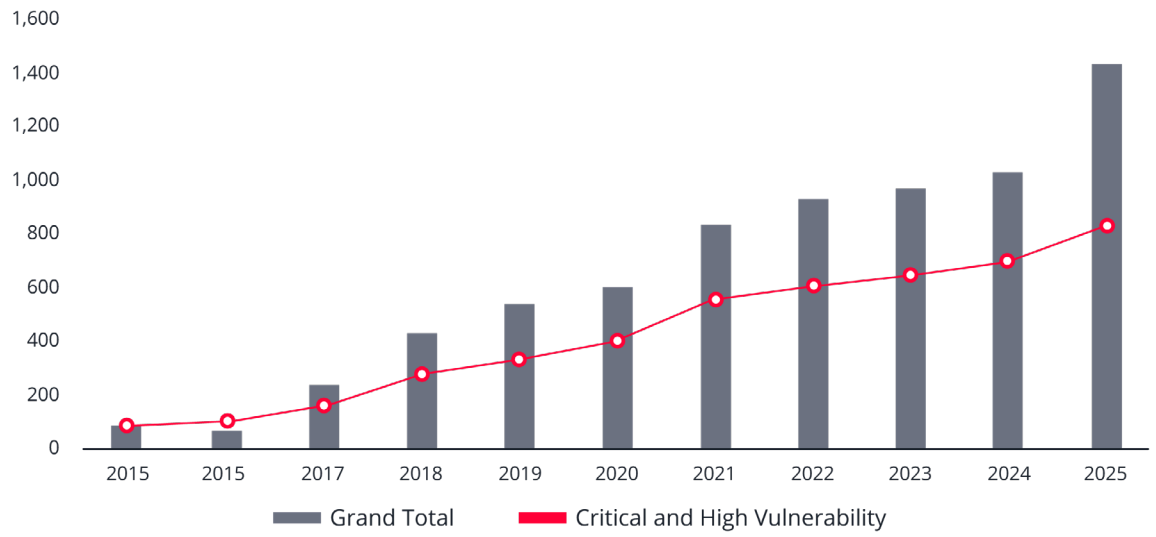


Figure 6. Growth of critical and high-severity automotive Vulnerabilities from 2015 to 2025

In an industry defined by long product lifecycles, constrained update windows, and shared platforms across vehicle models and services, the continued presence of high-severity vulnerabilities transforms cyber risk management from a prioritization problem into a governance challenge. Decisions must account for exposure that may span multiple product generations, requiring clear accountability and lifecycle-oriented risk ownership beyond traditional patch management.

Finding #7: Cyber risk is concentrating in safety-relevant in-vehicle technologies

Vulnerability exposure is now concentrated in systems that directly influence vehicle behavior, charging availability, and service continuity, elevating cybersecurity from an IT concern to a trust issue.

From 2015 through 2017, reported automotive vulnerabilities were primarily concentrated in connected backend services, reflecting the industry's early focus on cloud platforms and digital service enablement. Beginning in 2018, however, vulnerability exposure shifted decisively toward in-vehicle systems, which rapidly became the dominant source of reported weaknesses.

This shift is closely tied to the growing software complexity inside the vehicle. Expanding infotainment stacks, in-vehicle communication architectures, tighter ECU interdependencies, and the proliferation of advanced driver-assistance systems (ADASs) functions have transformed vehicles into highly modular yet strongly coupled systems. In this environment, vulnerabilities are no longer confined to isolated components. A single weakness can cascade across subsystems, directly affecting vehicle behavior, feature availability, and underlying safety assumptions.

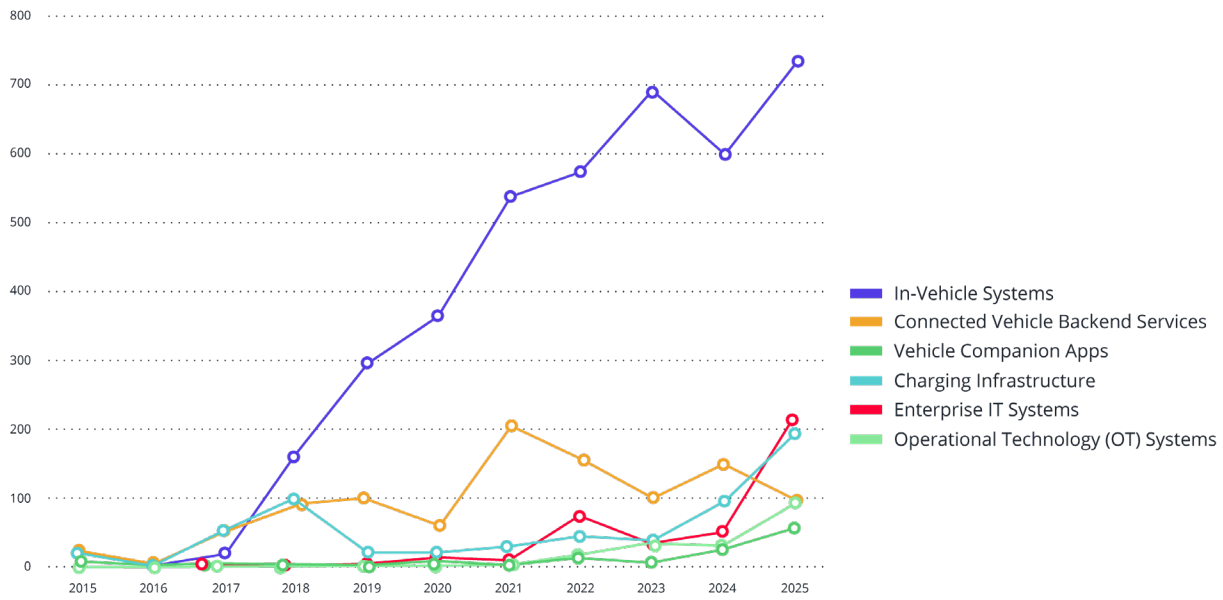


Figure 7. The shifting concentration of automotive vulnerabilities from backend services toward in-vehicle systems and electrification-related infrastructure over the past decade

At the same time, vulnerability exposure is extending into systems that directly condition vehicle usability. Charging infrastructure emerged as one of the fastest-growing vulnerability categories in 2025, reinforcing the coupling between in-vehicle systems and external dependencies that determine whether a vehicle can operate as intended. As a result, cyber exposure increasingly affects not just internal software integrity, but real-world availability and continuity of service.

This shift changes not only where automotive cyber risk resides, but what it represents. When vulnerabilities directly affect vehicle behavior, charging availability, and cross-system interactions, cybersecurity can no longer be treated as an information systems problem. It must be addressed as a core engineering and governance issue, with direct implications for safety, service continuity, and public trust.

2025 Automotive Cybersecurity Incident Highlight

Jan **Mercedes-Benz Head Unit Becomes a Cross-Domain Attack Pivot** In-Vehicle Systems: Infotainment/Head Unit (IVI)

Chained USB access with Internal head-unit messaging to pivot from IVI into other in-vehicle systems.

Jan **Subaru STARLINK Backend Access Enables Remote Vehicle Control** Connected Vehicle Backend Services

Exploited weak backend authentication and 2FA gaps to gain remote vehicle control and data access.

Jan **49 Unique Zero-Day Vulnerabilities DIscovered in 3 Days** Zero-day Vulnerability

Participants uncovered previously unknown vulnerabilities across software-defined vehicles, EV chargers, and the broader automotive ecosystem.

Apr **Remote Control of the Nissan Leaf Proven Technically Feasible** In-Vehicle Systems: Infotainment/Head Unit (IVI)

Combined Bluetooth access and backend services to remotely control vehicle functions and CAN components

May **"AirBorne" Vulnerabilities Put CarPlay IVI Ecosystem at Risk** In-Vehicle Systems: Infotainment/Head Unit (IVI)

Leveraged AirPlay protocol flaws to execute code or perform MITM attacks without user interaction

Jun **Tesla Wall Connector Becomes an Entry Point into Vehicle Networks** Charging Infrastructure

Exploited communication and memory-handling flaws in the Wall Connector to achieve remote code execution and pivot toward local vehicle networks.

Jul **PerfektBlue Enables 1-Click Bluetooth Remote Code Execution** In-Vehicle Systems: Vehicle ECU(S)/embedded software

Leveraged a Bluetooth stack vulnerability to execute arbitrary code on IVI systems after a single pairing event.

Aug **EV Charger Vulnerabilities Create Fire and Safety Risks** Charging Infrastructure

Manipulated insecure charging handshake and control logic to trigger abnormal current behavior beyond design limits.

Aug **Jaguar Land Rover Cyber Incident Disrupts Operations** Operational Technology (OT) Systems

Disrupted enterprise IT systems supporting production and logistics, cascading impact across suppliers and manufacturing lines.

Oct **Remote Maintenance Backdoors Expose Bus and Fleet Operations** Connected Vehicle Backend Services

Abused high-privilege remote access paths left for OTA updates and diagnostics to push unauthorized actions without proper authentication or runtime checks.

Dec **Hundreds of Porsches Stuck After VTS Breakdown** In-Vehicle Systems: Telematics Control Unit (TCU)

Triggered fail-secure immobilization through VTS disruption linked to GNSS anomalies, cellular connectivity loss, or trust validation failures.

Dec **Non-OEM Aftermarket Device Opens a Path to Remote Vehicle Control** In-Vehicle Systems: Infotainment/Head Unit (IVI)

Identified a previously unknown, critical vulnerability uncovered by our research team in a non-OEM aftermarket device that could enable arbitrary code execution and persistent in-vehicle access.

Dec **Hackers Shift From Corporate Extortion to Car Owner Targeting via SMS** Enterprise IT Systems

Stole customer data during a ransomware attack and used the leaked information to send extortion messages directly to vehicle owners via SMS, rather than negotiating solely with the affected company (Nanyang Industrial).

Finding #8: Persistent Low-Level and Injection Weaknesses Reveal an Engineering Maturity Gap

The 2025 vulnerability data does not indicate a surge in novel attack techniques. Instead, it reveals a persistent concentration of well-understood software weaknesses that should, in principle, be preventable during development. The structural concern is not their existence, but where they appear and how they can now be combined across modern automotive architectures.

Across 2025 data, the most frequently reported weaknesses include Use-After-Free (CWE-416), SQL Injection (CWE-89), Out-of-Bounds Read and Write (CWE-125, CWE-787), and a cluster of injection-related flaws such as CWE-74 and CWE-78. These weakness classes are not new. They have existed for decades. What has changed is the role they play in modern automotive systems.

Top Automotive CWEs in 2025	Count
CWE-416: Use-After-Free	90
CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	74
CWE-125: Out-of-bounds Read	70
CWE-787: Out-of-bounds Write	68
CWE-74: Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	59
CWE-78: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	54
CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	44
CWE-284: Improper Access Control	43
CWE-126: Buffer Over-read	40
CWE-120: Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	40

Table 1. Top 10 automotive CWEs reported in 2025

In today's vehicles, these weaknesses increasingly appear at entry points and control interfaces. Places where external input is transformed into trusted system behavior. When development-stage flaws surface at these locations, they no longer remain isolated technical defects. They become enablers of control, persistence, and cross-system reach.

The structural concern is not the presence of any single common weakness enumeration (CWE). It is that the same classes of weaknesses now span both execution layers and control surfaces, increasing the likelihood that vulnerabilities can be chained into reliable attack paths.

CWE-416: Use-After-Free at vehicle entry points

A representative example is the Use-After-Free vulnerability (CVE-2024-45434)[5] in OpenSynergy BlueSDK, where memory that has already been freed remains accessible to the program. In practice, this condition allows attackers to overwrite the freed memory region with malicious payloads, creating a path to remote code execution.

This class of weakness gained particular relevance in July 2025, when the PerfektBlue attack chain demonstrated one-click Bluetooth remote code execution against IVI systems.[6] By chaining multiple vulnerabilities (CVE-2024-45431, CVE-2024-45432, CVE-2024-45433) with a Use-After-Free flaw (CWE-416), attackers were able to bypass security checks and achieve full compromise of the head unit through a standard Bluetooth connection.

The significance of this case lies not in the exploit's complexity but in its position in the vehicle. Bluetooth is a natural entry point. user-facing, always-on, and designed for convenience. When a development-stage memory error exists at such an interface, it enables attackers to move from casual proximity to deep system control, including access to contacts, location data, and potential lateral movement toward other vehicle control units.

In-vehicle systems: Memory safety remains dominant

Within in-vehicle systems, the dominant weaknesses in both 2024 and 2025 remain memory-safety related. In 2025, the top issues include Use-After-Free, Out-of-Bounds Read and Write, Buffer Over-read, and NULL Pointer Dereference. The ranking has shifted slightly year over year, but the underlying pattern remains stable. These are foundational defects that are detectable during development and persist across platforms, vehicle models, and generations.

In-vehicle systems CWEs in 2025	Count	In-vehicle systems CWEs in 2024	Count
CWE-416: Use-After-Free	76	CWE-787: Out-of-bounds Write	91
CWE-787: Out-of-bounds Write	49	CWE-125: Out-of-bounds Read	79
CWE-125: Out-of-bounds Read	49	CWE-416: Use-After-Free	68
CWE-126: Buffer Over-read	39	CWE-126: Buffer Over-read	58
CWE-476: NULL Pointer Dereference	33	CWE-120: Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	48

Table 2. Top common weaknesses in in-vehicle systems in 2025 vs 2024

A representative case is the Mercedes-Benz NTG 6 (MBUX) head unit,[2] where researchers identified an arbitrary file write condition during USB profile import and export operations. The system allows drivers to back up and restore personal settings via USB storage. However, insufficient path validation

during file extraction allowed attackers to craft a malicious backup file and write files to arbitrary locations on the system.[7,8]

This weakness did not rely on exotic attack vectors. It leveraged normal user workflows. Backup and restore operations. The structural risk emerged because a well-understood flaw existed within a trusted, user-accessible workflow running in a high-privilege environment.

Connected vehicle backend services: Control without sanitization

In connected backend services, the weakness profile shifts from memory handling toward input validation and sanitization failures. The common thread is insufficient validation at interfaces that translate user or system input into backend actions.

Across 2025 data, code injection, SQL injection, cross-site scripting, and sensitive data exposure remain prevalent. These weaknesses reflect failures in controlling how external input is interpreted and executed, rather than failures in core computation logic.

Backend services CWEs in 2025	Count	Backend services CWEs in 2024	Count
CWE-94: Improper Control of Generation of Code (‘Code Injection’)	10	CWE-89: Improper Neutralization of Special Elements used in an SQL Command (‘SQL Injection’)	24
CWE-125: Out-of-bounds Read	8	CWE-125: Out-of-bounds Read	22
CWE-79: Improper Neutralization of Input During Web Page Generation (‘Cross-site Scripting’)	7	CWE-787: Out-of-bounds Write	19
CWE-200: Exposure of Sensitive Information to an Unauthorized Actor	7	CWE-79: Improper Neutralization of Input During Web Page Generation (‘Cross-site Scripting’)	12
CWE-89: Improper Neutralization of Special Elements used in an SQL Command (‘SQL Injection’)	5	CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer	10

Table 3. Top common weaknesses in backend services in 2025 vs 2024

In this domain, exploitation does not require deep system access. It requires proximity to management interfaces, application programming interfaces (APIs), or orchestration logic. As backend services increasingly govern identity, configuration, and service behavior, input validation failures turn administrative convenience into systemic exposure.

Charging infrastructure. From devices to infrastructure

Charging infrastructure shows a further structural shift. Compared with 2024, API-related weaknesses and authorization failures persist in 2025, but the risk profile has changed.

EV chargers are no longer treated as isolated devices. They are increasingly managed as shared infrastructure. As a result, dominant weaknesses now include authorization bypass (CWE-639), execution with unnecessary privileges (CWE-250), OS command injection (CWE-78), and SQL injection (CWE-89). These issues reflect failures in access control and identity enforcement rather than low-level device faults.

EV charging CWEs in 2025	Count	EV charging CWEs in 2024	Count
CWE-639: Authorization Bypass Through User-Controlled Key	27	CWE-787: Out-of-bounds Write	12
CWE-78: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	19	CWE-121: Stack-based Buffer Overflow	9
CWE-250: Execution with Unnecessary Privileges	11	CWE-88: Improper Neutralization of Argument Delimiters in a Command ('Argument Injection')	6
CWE-121: Stack-based Buffer Overflow	11	CWE-78: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	6
CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	8	CWE-77: Improper Neutralization of Special Elements used in a Command ('Command Injection')	6

Table 4. Top common weaknesses in EV charging systems in 2025 vs 2024

Recent examples include Vestel EVC04 configuration interfaces[9] (CVE-2024-8997),[10] Mennekes Smart and Premium charger firmware (CVE-2025-22370),[11] and the Kehua charging cloud platform[12] (CVE-2025-8347).[13] In each case, insufficient input sanitization or authorization controls allowed attackers to manipulate backend systems through management interfaces.

In an infrastructure context, these weaknesses scale differently. A single authorization or injection flaw can expose data across customers, affect multiple charging stations, or enable remote influence over fleet-scale assets. The risk is not that every vulnerability will be exploited. The risk is that infrastructure-level design errors create predictable blast paths.

The insight is that in the Overlap Era, legacy software practices are now embedded in systems that carry far greater responsibility. Vehicles have become continuously connected, software-defined platforms operating across physical, digital, and commercial domains. Yet many of the underlying engineering foundations remain vulnerable to classes of weaknesses that are well understood and largely preventable.

In this environment, vulnerability management cannot be treated as a periodic patching exercise. Persistent low-level and control-plane weaknesses create long-lived exposure that spans vehicle generations, software updates, and service lifecycles. Until foundational engineering practices evolve to address both memory safety and control integrity at points of interaction, these weaknesses will remain not anomalies, but predictable features of the automotive threat landscape.

CHAPTER 2

Overlapping Cyber Risks Across Vehicle Domains

As vehicles evolve into complex, connected, and software-defined systems, cybersecurity risks can no longer be viewed as isolated incidents or limited to individual components. Modern vehicles operate as tightly integrated platforms in which infotainment, driver assistance, powertrain, body control, and charging infrastructure continuously exchange data and influence one another. A vulnerability in one functional area can also overlap across other domains, transforming localized weaknesses into system-level risks.

This shift is occurring during a unique transitional period for the automotive industry. Traditional vehicle architectures continue to dominate global fleets, while SDVs with AI-enabled capabilities are rapidly entering mass production. The coexistence of legacy systems and next-generation technologies creates an overlap of risk models.

To better understand these dynamics, this chapter applies a Past–Present–Future risk framework across the vehicle's major functional domains. By examining how threats have emerged and matured within each domain, we can analyze the industry's shift from traditional, hardware-centric weaknesses to modern, software-driven, and network-based attack vectors.

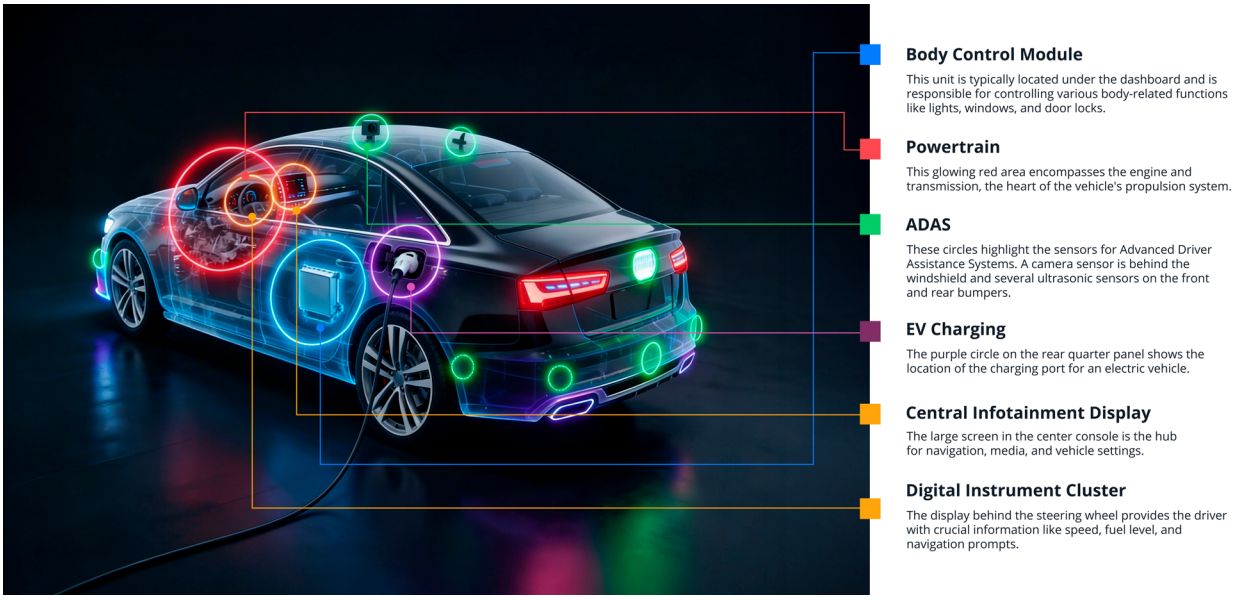


Figure 8. Conceptual view of a modern vehicle's major functional domains and their overlapping cyber risks

This perspective also provides insight into how emerging technologies, such as AI-enabled autonomy, cross-domain integration, cloud connectivity, OTA infrastructures, and vehicle-to-everything communication, are reshaping the attack landscape. The sections that follow examine a vehicle's major functional domains: IVI and smart cockpit systems, ADAS, powertrain, body control, and the EV charging infrastructure. These domain-level perspectives illustrate why the industry must rethink cyber risk management in the Overlap Era — where organizations must continue securing established platforms while preparing for the security implications of next-generation vehicle technologies.

IVI and smart cockpit systems

Past: Foundation of modern threats

Early generations of connected IVI systems established attack patterns that still define today's vehicle cockpit vulnerabilities. The 2015 Jeep Cherokee hack[14] demonstrated how an infotainment system could bridge into safety-critical ECUs via compromised cellular connectivity. Similarly, the 2016 Tesla Model S browser exploit[15] revealed how standard web vulnerabilities could escalate to vehicle control.

Common weaknesses in these early systems included:

- Inadequate network isolation between infotainment and safety-critical ECUs
- Unencrypted or weakly encrypted Bluetooth and Wi-Fi channels
- Lack of secure boot mechanisms
- USB-based attack vectors through media playback
- Browser vulnerabilities in web-enabled systems

These architectural flaws enabled routine software vulnerabilities to produce system-level consequences. In recent Pwn2Own Automotive contests, security researchers successfully demonstrated that such design weaknesses persist in production infotainment units. Notable exploit patterns included:

- Zero-click Bluetooth remote code execution (RCE) in an Alpine IVI system,[16] where improper input validation in the pairing process allowed attackers within range to execute arbitrary code without user interaction
- Multimedia parsing vulnerabilities in a Pioneer infotainment system,[17] exploited through a malicious USB device to trigger chained memory-corruption bugs and gain full system control
- Browser and privilege-escalation flaws in a Tesla IVI platform,[18] showing how medium-severity issues can be combined to bypass sandboxing and achieve root access.

Together, these findings illustrate how IVI systems have evolved from isolated components into gateways for remote vehicle compromise.

Present: Expanded attack surface

Today's smart cockpits represent a significantly more complex threat landscape. Integrations with Android Automotive, Apple CarPlay, ADAS modules, and cloud services have transformed infotainment units into connected computing hubs. Each integration expands the attack surface, creating multiple exploitation pathways.

Current high-priority threats to smart cockpit systems include:

- Supply chain compromises. Unvetted third-party apps in Android Automotive or Apple CarPlay could introduce malicious code[19] that can harvest location data, access the microphone, and potentially pivot to vehicle networks.
- OTA update manipulation. Weak certificates or verification flaws can expose man-in-the-middle attacks.[20]

> Cloud API vulnerabilities. Mobile companion apps communicating with backend services frequently expose authentication flaws, broken object-level authorization, and injection vulnerabilities.[21]
>
> AI or voice assistant exploitation. Natural language processing systems in cockpits can be manipulated through adversarial inputs, prompt injection attacks, and jailbreak attacks to execute unintended actions.[22]
>
> Sensor spoofing. Camera and radar systems integrated into smart cockpits for driver monitoring can be fooled through physical or digital manipulation.[23]

Research-driven disclosures and vulnerability discovery competitions such as Pwn2Own Automotive continue to validate these risks in production-grade systems, emphasizing that the attack surface of modern smart cockpits has expanded and continues to do so.

Future: Emerging IVI threats

The next phase of smart cockpit security will be defined by automation, AI, and distributed connectivity. Over the next five years, threat actors are expected to leverage AI, quantum computing, and increasingly sophisticated social engineering.

Predicted threat evolution:

- **AI-powered persistent threats.** Machine learning models will identify zero-day vulnerabilities in cockpit software faster than manufacturers can patch. Automated exploit development will reduce time-to-exploit from months to hours.
- **Vehicle-to-everything (V2X) attack vectors.** As V2X communication becomes standard, smart cockpits will process external data from infrastructure and other vehicles. Message spoofing and replay attacks will enable traffic manipulation and targeted vehicle disruption.
- **Deepfake voice command injection.** Advanced deepfake technology will convincingly mimic driver voices to execute unauthorized commands through voice assistants. This bypasses biometric authentication.
- **Quantum cryptography vulnerabilities.** Current encryption protecting smart cockpit communications may be vulnerable to quantum computing attacks, requiring complete cryptographic overhauls.
- **Autonomous feature manipulation.** As cockpits integrate more autonomous driving controls, attackers will target perception systems through coordinated multi-sensor attacks, creating dangerous driving scenarios.

- **Privacy weaponization.** The massive data collected by smart cockpits will become ransomware targets. Attackers can potentially threaten exposure of intimate driving behavior and personal information.
- **Exploit chain sophistication.** Future attackers will develop longer, more complex exploit chains combining vulnerabilities across multiple system components. These chains will pivot from low-privilege entry points through middleware layers into safety-critical vehicle functions.

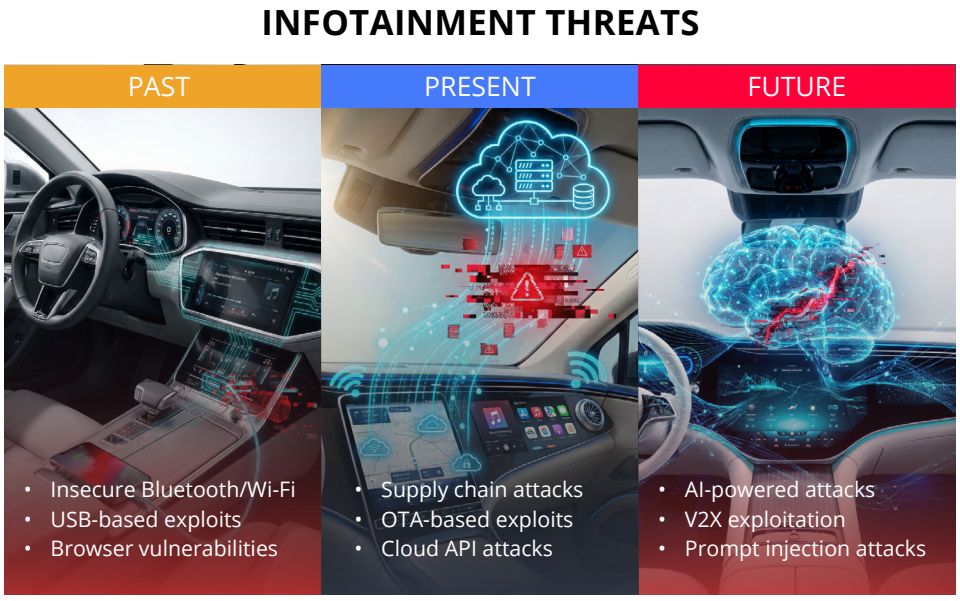


Figure 9. Past, present, and emerging cybersecurity threats affecting IVI systems

Advanced Driver Assistance Systems

Past: From functional safety to perception-based risk

When ADAS technologies first emerged, their safety logic reflected the engineering discipline of the time. The systems were built under a fault-based view of risk where safety hazards were assumed to arise from malfunctions in electrical and electronic (E/E) components. This paradigm, however, left a crucial blind spot. It did not account for how perception systems could behave unsafely even when operating as designed.

As ADAS functions became more perception-driven, vehicles began to rely on environmental cues such as lane markings, road signs, lighting, weather visibility, and camera timing to interpret the driving scene. These cues could degrade or mislead perception algorithms without any internal fault, creating performance limitations rather than malfunctions. The resulting risks were subtle but serious. A vehicle might drift when the lane paint faded, misjudge distance under glare, or brake too late when radar reflections are poor.

The industry's safety paradigm therefore evolved to recognize that intended behavior itself could be unsafe under certain conditions. What once was seen as a technical problem became a contextual and environmental risk, tightly linked to how sensors, perception models, and driver interfaces interpret the real world. This expanded risk lens reshaped ADAS development, forcing engineers to consider edge cases, ambiguous road markings, and the interaction between driver expectation and system behavior.

Phase	Dominant Risk	Primary Risk Drivers
Functional-safety era (Pre-2010s)	Fault-based: hazards traced to failures in hardware or software components.	E/E component faults, actuator reliability, sensor signal integrity.
Perception-driven systems (2010–2015)	Performance-based: safe operation under nominal but imperfect conditions.	CWE-121: Stack-based Buffer Overflow
Intended-functionality awareness (2015–2020)	Functional-limit risk: unsafe behavior without system malfunction.	Perception brittleness, misdetection, false positives or negatives in object recognition.
Human–automation interaction risk (2016–2020)	Behavioral risk: driver overtrust and misuse of partial automation.	Overreliance on automation, unclear human-machine interface (HMI) cues, and delayed human response to takeovers.
Connected and learning systems era (2020s–Present)	Data and model-based risk: vulnerability of perception and decision models.	Sensor spoofing, data poisoning, adversarial inputs, and cybersecurity linkage.

Table 5. Historical evolution of ADAS safety thinking, from fault-based system safety to functionality- and perception-based risk management, and how each phase broadened the definition of what "safe" means in practice. For additional insights into the ADAS revolution, refer to Appendices A, B, and C.

Present: Perception and sensor exploitation

As ADASs evolved beyond basic functional safety, the primary attack surface shifted from control electronics to the sensors and perception layers.

This progression created a new class of cyber risk: vehicles can be driven into unsafe behavior without altering a single line of code, simply by manipulating what their sensors perceive. Recent studies confirm that the integrity of perception and planning can be undermined not only through algorithmic manipulation but also through subtle, real-world interference at the physical interface between sensors and the environment:

- **Cross-sensor and system-level attacks.** Studies such as DejaVu[24] and multi-sensor fusion attacks[25] demonstrate that small temporal desynchronization between camera and LiDAR streams, or inconsistencies across fused modalities, can silently collapse object tracking and trajectory planning.[26] These attacks are particularly dangerous because they require no direct tampering with sensor signals yet can trigger full-stack failures and even collisions.

- **Camera-based attacks.** Invisible modulation patterns such as GhostStripe[27] and low-power laser projections on traffic-light housings can flip color classifications[28] or mislead sign recognition across consecutive frames. These attacks operate outdoors, at distances exceeding 20 meters, and require only milliwatt-level power, bridging the gap between laboratory and field conditions.

- **LiDAR attacks** have advanced from early phantom-point injection[29] to precise long-range spoofing[30,31] and removal attacks capable of deceiving production systems at highway speeds.[32] By manipulating the timing of reflected pulses, attackers can erase genuine obstacles or fabricate objects in the environment, resulting in end-to-end control failures. Such methods have been validated on open-source platforms including Autoware and Apollo, indicating a high degree of real-world maturity.

- **Radar-layer spoofing.**[33] Recent work[34] shows that a black-box adversary can estimate the parameters of a victim mmWave radar in real time, then inject, move, or remove detections using off-the-shelf transmitters. This capability transforms radar spoofing[35] from an abstract risk into a tangible, low-cost vector for manipulating object perception in real traffic.

- **Inertial measurement unit (IMU), acoustic,[36] and electromagnetic injection.** Acoustic resonance and ground-line radiation[37] can bias inertial measurements or disturb analog front ends without physical contact. Such interference exposes the fragility of sensor subsystems, which have traditionally been outside the scope of digital security mechanisms.

- **Global Navigation Satellite System (GNSS) spoofing and defense.** Research continues to address navigation integrity as a prerequisite for safe high-speed autonomy.[38] Recent sensor-fusion approaches[39] combine inertial data, steering feedback, and machine learning to detect slow-drift or turn-level spoofing in urban conditions, bringing GNSS protection closer to practical deployment.

- **Systematization studies[40]** integrate these developments into a unified taxonomy, mapping common attack paths across sensing modalities and highlighting gaps in existing defenses. This synthesis establishes a foundation for future efforts toward certified robustness in multi-sensor perception[41] and decision-making.

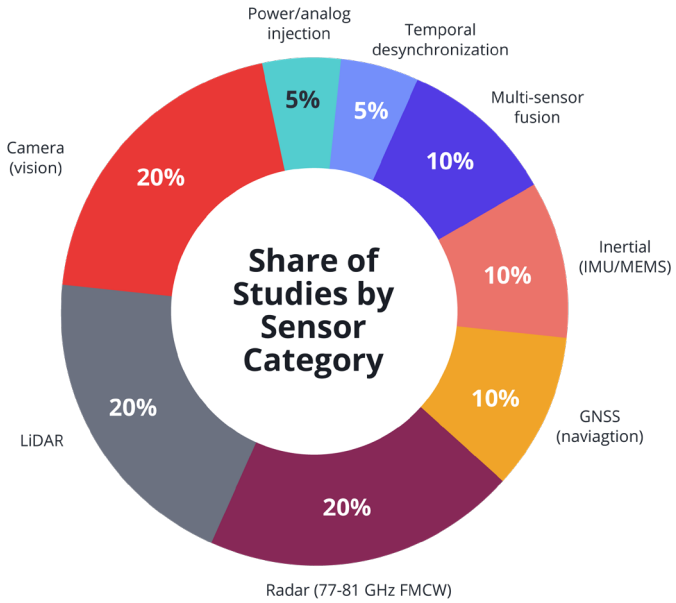


Figure 10. Distribution of perception-focused ADAS attacks by sensor type, showing the concentration of research on camera, LiDAR, and timing-based fusion weaknesses

Taken together, the risk is operational and immediate: benign environmental stimuli — ordinary signage, LED flicker, radar multipath, ambient acoustic energy, or broadcast Position, Navigation, Timing (PNT) interference — can deterministically degrade perception and planning pipelines. From the vehicle's perspective, these inputs are indistinguishable from legitimate environmental signals, yet they can cause incorrect braking, lane-keeping errors, or obstacle misinterpretation.

As a result, ADAS safety is no longer determined solely by software correctness. It now depends on the trustworthiness of perception itself, where physics-level and data-level manipulation can have the same operational impact as a traditional cyber intrusion.

Future: Networked and AI-driven ADAS

The next phase of ADAS will extend perception beyond the vehicle itself. Instead of relying on onboard cameras, radar, and LiDAR, vehicles will increasingly draw on shared, networked intelligence from nearby vehicles, roadside infrastructure, cloud services, and aerial platforms. This broader perception model promises richer situational awareness but also introduces new challenges for safety, latency, and trust. The key risk is no longer the accuracy of any single sensor or model, but the reliability and integrity of the entire cooperative network.

This evolution is already underway through the development of collective perception standards. Frameworks such as the Collective Perception Service (CPS) and Collective Perception Message (CPM) of the the European Telecommunications Standards Institute (ETSI) allow vehicles and infrastructure to exchange detected objects, traffic signals, and road conditions in near real time.

The New Radio Vehicle-to-Everything (NR-V2X) system enables both direct sidelink and cellular communication, handling short bursts of perception data while prioritizing urgent updates at the network edge. In parallel, V2X roadside units now transmit information such as lane closures and Signal Phase and Timing (SPaT) or MAP messages. These broadcasts can supplement or replace local sensor detection when timing is critical.

Navigation platforms such as Waze, Google Maps, and regional traffic management apps, as well as those from connected-vehicle probe fleets, can provide early indicators of anomalous conditions. Reports of sudden congestion, debris on the roadway, or temporary lane closures often first appear in these crowdsourced systems before being detected by infrastructure sensors.

Beyond fixed infrastructure, Unmanned Aerial Vehicles (UAVs) will become mobile perception nodes. Acting as forward scouts or terrain monitors, UAVs can detect hazards such as debris, rockfalls, or low-friction surfaces beyond the line of sight of ground-based vehicles and inject those observations into cooperative perception systems via roadside or cloud paths.

Future ADAS platforms will rely on distributed AI models for perception, prediction, and planning, operating across onboard systems, edge served, and cloud services. These models will be continuously updated and synchronized, introducing risks of model drift, poisoning, and version inconsistency across fleets. When vehicles exchange not just sensor data but inferred intent and predicted trajectories, small discrepancies in model behavior or training data can cascade into large-scale coordination failures through machine-to-machine (M2M) interaction.

In the future, ADAS safety becomes a networked property rather than a vehicle-local one. Reliability will depend not only on sensor accuracy or algorithm quality, but on whether shared data streams and distributed AI agents remain authentic, timely, and internally consistent. The challenge for next-generation ADASs is therefore not simply to see more, but to trust correctly. Vehicles must be able to benefit from cooperative and AI-driven perception while retaining the ability to fall back to local sensing and safe behavior when networked inputs become unreliable.

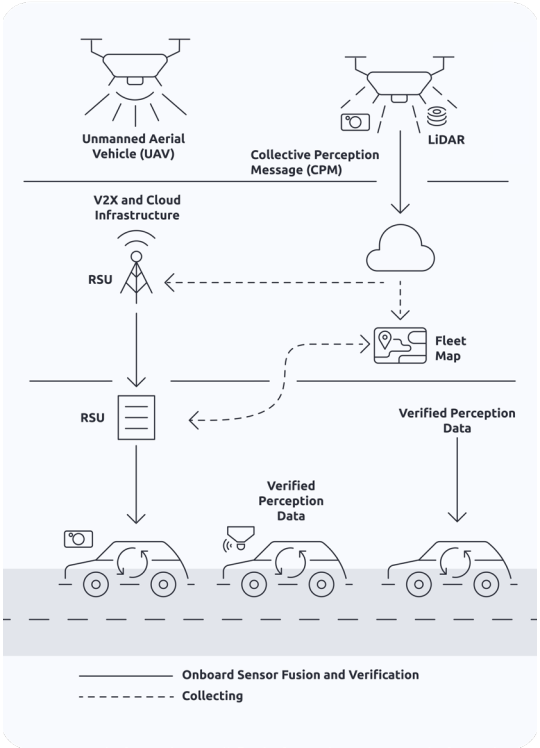


Figure 11. Cooperative perception data flow between UAVs, roadside units, and vehicles via NR-V2X and cloud paths. Vehicles fuse UAV and infrastructure data with onboard sensors while verifying authenticity, timing, and spatial consistency before acting.

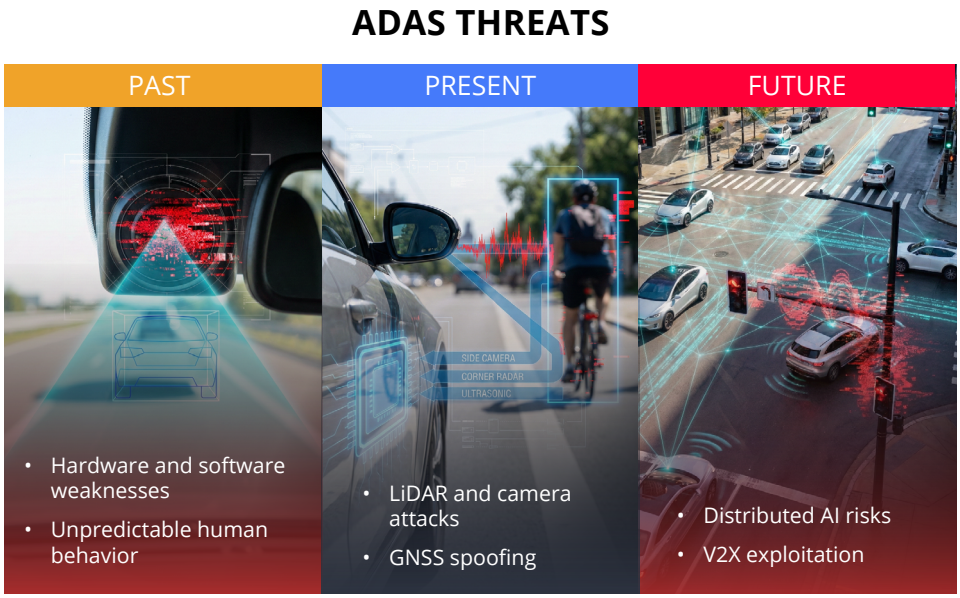


Figure 12. Evolution of ADAS risk from fault-based safety to perception security and future networked, AI-driven autonomy.

Powertrain

Past: From performance tuning to privileged access

The powertrain domain was traditionally regarded as a relatively closed and insulated system. Risks were more closely associated with mechanical failure or aftermarket tuning — not cybersecurity. For decades, “tuning” was considered a legitimate aftermarket activity in which enthusiasts modified engine or transmission behavior to improve performance, fuel economy, or drivability.

Early powertrain compromises were almost entirely mechanical or hardware-driven. Tuners desoldered and replaced erasable programmable read-only memory (EPROM) chips in ECUs to alter fuel injection, ignition timing, or turbo boost limits. As diagnostic and calibration protocols matured in the 2000s, this evolved into programming of the on-board diagnostics (OBD-II) port using services defined in ISO 14229 (Unified Diagnostic Services or UDS). Although security mechanisms such as the seed-key challenge under the UDS SecurityAccess service were intended to safeguard these operations, they were routinely reverse-engineered, brute-forced, or leaked. When diagnostic protections failed, bench flashing through JTAG or Background Debug Mode (BDM) to bypassed in-vehicle safeguards entirely.

Transmission controllers were subjected to similar methods, with shift maps, torque limiters, and clutch pressures. While these activities were generally framed as performance enhancements, these established repeatable pathways of intrusion: physical access, diagnostic unlocking, firmware reprogramming, and parameter tampering. These same pathways remain embedded in modern powertrain architecture, forming the technical lineage of today’s cybersecurity exposure.

Present: Expanded powertrain attack surface

The present-day risk environment has expanded these historic weaknesses into systemic cybersecurity concerns. The 2015 Jeep Cherokee hack demonstrated that attackers could exploit a remote vulnerability in the infotainment system, pivot onto the CAN bus, and influence functions tied to acceleration and braking. This event made clear that the powertrain domain could be compromised not only through physical diagnostic ports but also remotely via lateral movement across networked vehicle domains.

Diagnostic protocols continue to represent a prominent attack surface. Studies have shown that production ECUs allow access to enhanced UDS sessions without strong authentication, leading to denial-of-service conditions or unauthorized vehicle control. These findings underscore the challenge of balancing serviceability with cybersecurity.

Electrification has further widened the risk landscape. Battery Management Systems (BMS), inverters, and charging controllers now interact continuously with external infrastructure. Charging protocols such as ISO 15118, Open Charge Point Protocol (OCPP), and HomePlug Green PHY define intelligent charging and vehicle-to-grid (V2G) functions, but security researchers have identified vulnerabilities ranging from outdated cryptography to insecure modem firmware. These flaws allow man-in-the-middle, denial-of-service, and manipulation attacks that can disrupt charging, degrade battery health, or stress safety limits.

At the same time, unofficial performance tuning has begun to emerge in the EV domain. Aftermarket firms now offer software-based upgrades for vehicles such as the Audi e-tron and Porsche Taycan, advertising recalibrated control logic that increases output without replacing hardware. Enthusiast communities are actively exploring how to adjust motor controller parameters, alter torque curves, and bypass manufacturer-imposed power limits. What appears as customization also creates a malware-like attack surface, where adversaries can disguise themselves as tuners or exploit the same update mechanisms to inject unsafe behavior.

Recent security research has confirmed the seriousness of these risks. Vulnerability discovery competitions such as Pwn2Own Automotive have demonstrated remote code execution in Tesla components and vulnerabilities in EV chargers, highlighting that adversaries no longer need to target the infotainment domain to threaten safety-critical functions; the powertrain itself, through its growing connectivity, has become a primary target.

Future: Software-defined power and grid-level risk

In the Overlap Era, the powertrain will become even more central to cyber risk. Software-defined architectures are consolidating control over torque vectoring, regenerative braking, and driveline logic into high-performance computing platforms. This consolidation creates a single point of failure: a single vulnerability in such a controller could affect drivability across an entire vehicle fleet.

The adoption of V2G capabilities introduces infrastructure-scale consequences. If attackers manipulate charging and discharging behavior, the consequences could extend beyond individual vehicles to the stability of energy infrastructure. Emerging reliance on AI-based models for predictive power management adds another layer of vulnerability, opening possibilities for data poisoning or adversarial manipulation that could degrade performance or safety.

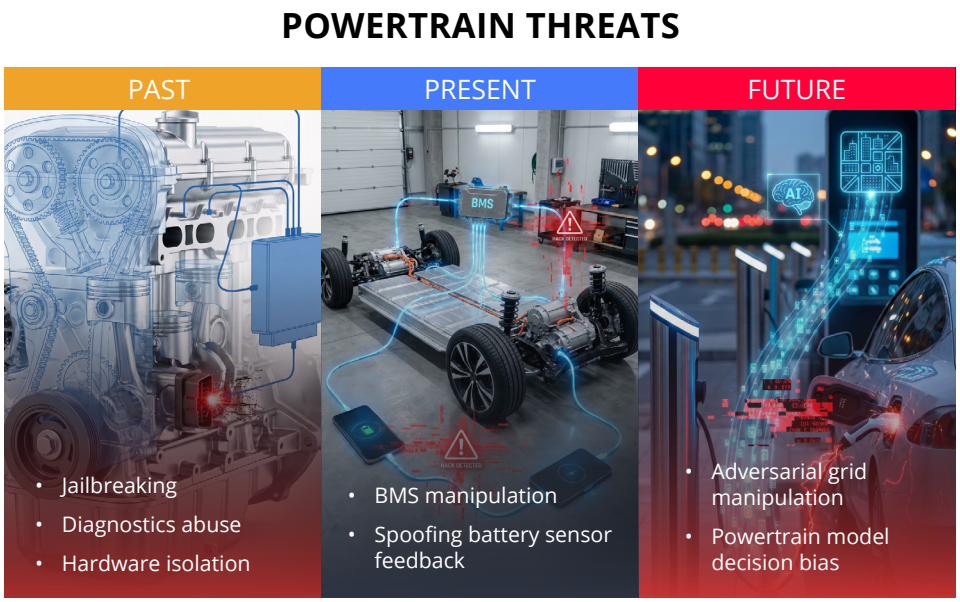


Figure 13. Evolution of powertrain cybersecurity risk from isolated firmware modification to software-defined and grid-connected exposure.

Body control and access systems

Past: From comfort and convenience wiring to software-defined access

For most of the modern era, the body domain — locks, lights, wipers, mirrors, and tailgates — were treated as comfort and convenience, not as a security boundary. These functions were implemented as distributed wiring and low-cost controllers, with investment focused on hardware rather than software assurance.

That changed when body electronics consolidated onto CAN with LIN spurs and UDS-based coding. LIN matured from 1.0 (1999) to 2.1 (2006) as the de facto low-cost sub-bus beneath body CAN, while UDS standardized how dealers and factories wrote configurations into Body Control Modules/Body Domain Controllers (BCM/BDC). At that point, body control stopped being just wiring and became a software platform.

Access technology evolved in parallel. Infrared and sub-1 GHz remote keyless entry (RKE) in the 1980s (e.g., Renault's PLIP on the Fuego) gave way to passive keyless entry (PKE) in the 1990s (e.g., C4 Corvette), where proximity triggered door unlocks, welcome lights, and mirror or trunk movement. The key was no longer just an ignition enabler. It became a live input to body behavior.

Security research then exposed how fragile this model was. Rolling-code cryptosystems and immobilizers have been repeatedly broken (KeeLoq attacks in 2008, relay attacks against PKES in 2011, Hitag2 key recovery in 2012, Megamos Crypto in 2015, and large-scale RKE weaknesses in 2016), demonstrating that weak or relayable RF assumptions can undermine the entire access chain.

By the early 2020s, phone-as-a-key and ultra-wideband (UWB)-based digital keys made access truly software-defined. Proximity governed not only entry and start, but also how the vehicle presents itself to the user. At the same time, standards such as AUTOSAR SecOC on CAN-FD/Ethernet began pushing authentication onto in-vehicle messages, shifting trust from the key fob to the communication bus.

To learn more about the evolution of access technologies and their corresponding security breaches, refer to Appendix D.

Present: When theft moved to the vehicle's communication bus

The dominant attack pattern today is body-CAN injection through exposed connectors or compromised gateways. Without native message authentication, crafted frames can steer door locks, immobilizers, and wake sequences. What was once described in technical papers is now widely covered in mainstream reporting: unauthenticated in-vehicle traffic is the root cause.

In 2025, the research community focused on methods that are reproducible on real data. Intrusion detection for body networks has moved beyond laboratory prototypes to shared datasets, multi-class evaluation, and deployable latency, making intrusion detection system (IDS) practical for actual vehicles. Research such as Controller-Area-network Instantaneous Broadcast Authentication (CAIBA work) demonstrated real-time multicast source authentication for CAN, while AUTOSAR SecOC established per-PDU authenticity and freshness as the production baseline. In the body domain, "the bus is not trusted" is now a design assumption rather than a footnote.

Digital keys have crossed from roadmap to reality, and in 2025, the emphasis was on interoperability and measurement. The Car Connectivity Consortium (CCC) expanded its certification program beyond Near-field Communication (NFC) to explicitly cover Bluetooth Low Energy (BLE) discovery and UWB distance-bounding and angle for passive entry and start.[42] This matters because proximity controls not only entry, but also handles, mirrors, welcome lighting, and tailgate behavior.

Alongside these technical controls sits a large and mature grey market. Professional boards and brand communities routinely carry requests for feature entitlements, map and navigation Feature Set

Codes (FSCs), coding recipes for ambient-lighting palettes, and driver-assistance toggles. What looks like personalization — ambient lighting themes, comfort settings, feature activation — uses the same plumbing as theft and unauthorized control. Organized crime has professionalized these channels, using encrypted platforms and purpose-built marketplaces to commission, distribute, and support tooling that targets body networks.

Put together, today's digital keys place ranging at the center of body behavior. IDS work has matured from "works on one lab trace" to reusable datasets and deployable models. Bus-level authentication has moved from "CAN can't do that" to conference-grade designs that acknowledge broadcast physics. And the grey market around feature unlocking confirms that the same plumbing that powers paid personalization will remain a target until the internal channel is authenticated, freshness-checked, and writable only by attested roles.

Future: When the body network becomes a secured platform

The next phase of the body domain be defined by identity, integrity, and freshness at every actuation point. Doors, mirrors, windows, lighting, wipers, tailgates, and seats will no longer accept unauthenticated traffic even from inside the vehicle. HSM-backed zonal controllers will enforce message-level authentication, replay budgets, and per-session keys. An attacker who reaches a harness still hears the bus but will no longer be able to conduct it.

Digital keys will evolved from entry credentials into continuous policy inputs. BLE+UWB proximity will extend beyond "can I enter and start" into "how should the body behave given where the key is." Access control and body UX collapse into the same security model.

The grey market will disappear; it will professionalize. Expect short-lived, per-vehicle identification number (VIN) feature tokens; capability-scoped grants, and personalization certificates that expire by time, ECU, and function. The same plumbing that sells upgrades can also permit lawful customization, as long as it is cryptographically accountable.

Aftermarket modules will adapt, and vehicles will respond by demanding provenance at the edge: authenticated ports; tamper-evident harnesses; and gateways that demote or quarantine unauthenticated traffic instead of merely rate-limiting it. Intrusion detection will get less "AI magic" and become more control-aware, recognizing physically implausible actuation patters, not just statistical anomalies.

In the future, the SDV business model will be finally backed by real cryptography. Feature entitlements will resemble payments: transparency logs for feature certificates, revocation that works on the road, and audit trails that make disputes resolvable. Zonal architectures will front the body domain uniform policy: secure boot, measured software, per-session keys, and mandatory access control at the message level.

The end state is not less personalization — it is safer personalization. The sustainable endgame is a body domain that treats owners, shops, and enthusiasts as first-class actors with bounded powers: tweak your ambient scenes, tune your rain sensor, program your welcome routine — inside a sandbox where every change is attributable and reversible, and where the same rails cannot be repurposed for theft. In other words, security becomes the enabler: the only way to sell upgrades at scale and let people personalize without handing the same tools to organized crime is to wire cryptography into the physics of the body network.

Two tests will tell us this future has arrived. First, when teardown photos of stolen vehicles stop showing harness taps and "emergency start" boxes, not because thieves gave up but because the bus no longer believes untrusted traffic. Second, when enthusiasts stop trading secret incantations and start trading signed presets such as lighting themes, chimes, actuator profiles that install like apps under a permission model the vehicle can enforce. When both are true, the body domain will have crossed the line from "comfort and convenience" to a secured platform and theft headlines will no longer dictate what people dare to buy.

Figure 14. Past, present, and emerging cybersecurity threats affecting body control and vehicle access systems.

EV charging infrastructure

Past: From physically isolated chargers to early connectivity

In its earliest stages, the electric vehicle supply equipment (EVSE) infrastructure was largely characterized by physical isolation and limited communication capabilities. Early EV chargers, often referred to as "dumb chargers," were designed primarily for power delivery and lacked external

communication capabilities. As a result, these devices faced risks primarily limited to hardware tampering, firmware extraction, charging protocol manipulation. Here are few notable incidents:

- The discovery of the Log4Shell vulnerability (CVE-2021-44228)[43] demonstrated how weaknesses in widely used software components could be triggered through malicious OCPP messages, thus potentially allowing attackers to seize control of entire charging networks.
- With Brokenwire,[44] researchers revealed that an attacker within a 47-meter range can use a Software Defined Radio (SDR) to transmit a weak radio signal. By mimicking the PLC preamble signal, the attacker can cause a persistent Denial of Service (DoS), preventing the vehicle and charger from establishing a handshake and effectively halting the charging process.
- EV charging stations deployed along Russia's M-11 highway were rendered inoperable in a coordinated incident following the outbreak of the Russia–Ukraine conflict.[45] While full technical details remain classified, the event is widely believed to have involved the abuse of remote maintenance access or OTA firmware update mechanisms.

Present: Industrialized exploitation

The EVSE infrastructure evolved into a fully connected ecosystem, integrating cloud management platforms, mobile applications, backend services, and OTA firmware update mechanisms. This convergence significantly expanded the attack surface, allowing vulnerabilities to propagate device, network, and cloud layers rather than remaining confined to individual charging stations.

Within this environment, EVSE exploitation entered a phase of "industrialization." The introduction of the automotive category at Pwn2Own Automotive, an ethical hacking competition, accelerated the coordinated discovery of zero-day vulnerabilities, allowing researchers to demonstrate repeatable, real-world attacks against mainstream charging equipment under controlled yet realistic conditions. It is worth noting that during Pwn2Own Automotive 2024[46] and 2025,[47] EV chargers accounted for more than half of all disclosed zero-day vulnerabilities, highlighting their growing appeal as high-value targets.

It was only a matter of time before the nature of risk shifted from service disruption toward physical safety. In 2025, researchers demonstrated that forcing EV chargers to deliver sustained maximum currents with protection disabled caused components to melt within minutes, leading to actual fires in laboratory settings.[48] These findings underscored the direct translation of cyber compromise into safety hazards.

As EVSE infrastructure becomes increasingly interconnected, present cybersecurity challenges reflect systemic design and operational dependencies rather than isolated implementation flaws.

Future: Systemic grid stability risks

In the future, the EVSE will transition from isolated hardware to the “neural endings” of the Internet of Energy (IoE). This evolution is driven by high-power Megawatt Charging Systems (MCS), the standardization of Plug & Charge, and the management of Distributed Energy Resources (DER). As charging systems increasingly interact with grid operators, energy markets, and vehicle energy management platforms, EVSE will function not merely as endpoints, but as active control nodes within national energy ecosystems.

A major challenge in this shift is managing the coexistence of modern standards and older infrastructure. While protocols like ISO 15118-20 offer stronger cryptographic protections and identity-based charging, many deployed chargers still rely on earlier standards, including OCPP 1.6J and proprietary protocols that lack mandatory encryption and robust authentication. This accumulated “technical debt” can be exploited through downgrade attacks, in which modern vehicles or chargers are forced to revert to insecure legacy protocols, enabling Man-in-the-Middle (MitM) or replay attacks.

EVSE infrastructure also faces emerging quantum-related risks. The cryptographic mechanisms currently used by ISO 15118, including RSA and elliptic curve cryptography (ECC), may become vulnerable to future cryptographically relevant quantum computers (CRQC). This could render existing digital signatures and key exchange mechanisms obsolete.

As charging capacity grows, the potential for a coordinated attack on the power grid becomes a major national security concern. By controlling a botnet of thousands of compromised EVs, attackers could synchronize charging or discharging behavior to create artificial load fluctuations across the grid. Research indicates that controlling as little as 1% to 5% of total grid load may be sufficient to trigger protective relay mechanisms, particularly when the switching frequency aligns with the grid’s low-frequency oscillation modes. Under such conditions, localized disturbances could escalate into cascading failures and large-scale blackouts, with impacts comparable to those associated with attacks against critical national infrastructure.

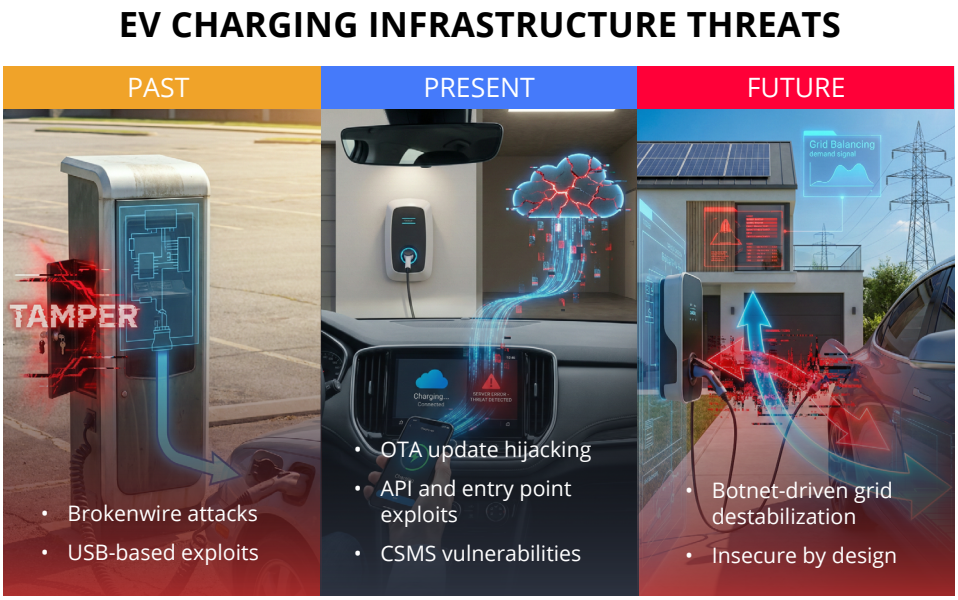


Figure 15. Past, present, and emerging cybersecurity threats affecting electric vehicle charging infrastructure.

Conclusion

The analysis of past, present, and future risks across vehicle functional domains shows that cybersecurity challenges extend beyond individual systems or components. As modern vehicles integrate more software-driven functions and connectivity features, new dependencies emerge across domains, creating risks that cannot be mitigated solely through technical measures. Addressing these risks effectively requires coordination between engineering practices, governance structures, and regulatory frameworks.

Vehicle function domain	PAST Incidents	PRESENT Current vehicle threat research	FUTURE Prediction of threat evolution
Infotainment and smart cockpit systems	Inadequate network isolation, unencrypted Bluetooth and Wi-Fi, absence of secure boot mechanisms, USB-based exploits, and browser vulnerabilities allowed attackers to compromise infotainment systems and safety-critical ECUs.	Supply chain compromises, OTA update manipulation, cloud API vulnerabilities, AI or voice assistant exploitation, and sensor spoofing enable data theft, RCE, and lateral movement into vehicle networks.	Emerging threats include AI-powered persistent attacks, V2X exploitation, deep-fake voice injection, quantum-era cryptographic breaks, manipulation of autonomous features, privacy weaponization, and complex multi-stage exploit chain.

ADAS	Early ADAS focused on fault-based safety, based on standards such as ISO 26262[49] and ASIL. The introduction of Safety of the Intended Functionality (SOTIF) addressed perception limits, shifting safety toward real-world functionality and paving the way for sensor and model security.	ADAS now face real, physics-level threats that exploit light detection and ranging (lidar), radar, camera, and fusion vulnerabilities. These can disrupt perception and planning without directly compromising software, highlighting the urgent need for sensor-level robustness in safety-critical perception.	As ADAS shifts to networked perception, using shared data from vehicles, infrastructure, and AI systems, the risks will move from sensor errors to network trust and model integrity. Distributed AI and cooperative communication can spread faults or conflicts across fleets, making safety a system-wide challenge rather than a single-vehicle issue.
Powertrain	Unauthorized firmware modifications and abuse of diagnostic tools were the primary attack vectors in these largely isolated, hardware-centric systems.	Powertrain components now interface with vehicle networks and charging systems, enabling remote compromise of powertrain functions.	Systemic compromise through software-defined architectures, AI-based control, and vehicle-to-grid integration.
Body control and management system	Convenience features such as keyless entry and remote locking were integrated via CAN, LIN, and UDS protocols, but weak RF cryptography and relay attacks undermined physical access control. The shift to phone- and UWB-based digital keys made body functions software-defined, shifting security and trust to the core body-domain risk.	Despite improvements in intrusion detection and message authentication, grey markets for coding, feature unlocking, and diagnostic bypass continue to exploit unsecured internal communications. The core risk now lies in untrusted in-vehicle communication and unauthorized control over software-defined body functions.	As theft and intrusion migrate entirely to internal networks, the next frontier of risk will be securing every communication path that can unlock or actuate vehicle systems. Without built-in identity, integrity, and freshness validation, attackers could still exploit wiring harness access or software bypasses.
EVSE	Physical and communication manipulation: Focused on hardware tampering, firmware extraction and Combined Charging System (CCS) manipulation	Industrialized exploitation: Widespread discovery of zero-day vulnerabilities in mainstream chargers	Systemic grid stability risks: A shift toward large-scale botnet attacks aimed at manipulating energy loads to trigger grid-wide blackouts and exploiting legacy «technical debt» in older protocols

Table 6. Past–Present–Future summary of key cybersecurity risks across major automotive functional domains, illustrating the industry's progression from hardware-centric vulnerabilities to software-defined and ecosystem-wide challenges.

Although the automotive industry has made steady progress in defining cybersecurity standards and best practices, regulations often evolve more slowly than technology. This creates situations where vehicles and infrastructure may fully comply with existing requirements but remain exposed to emerging or unrecognized threats.

CHAPTER 3

How AI is Reshaping Cyber Risk Management

Artificial intelligence is no longer a peripheral capability in modern vehicles. AI has extended its reach from traditional driver assistance functions to autonomous mobility services, including robotaxis and highly automated vehicles. Industry architectures have evolved from deterministic, rule-based pipelines to end-to-end or hybrid neural network models. For example, self-driving decision-making increasingly relies on multi-modal sensor fusion to improve robustness.

Aside from driving automation, generative AI is being adopted through large language models (LLM)-based voice assistants. Vehicles can also use driver monitoring systems (DMS) and in-cabin sensing, such as pressure and occupancy sensing, to infer driver state, adapt smart-cabin settings, and enable mixed or extended reality (XR) experiences. Furthermore, vehicles can leverage V2X

connectivity — together with onboard sensing and/or cloud-based information sources — to support driving decisions by incorporating real-time traffic and environmental factors to optimize power delivery and energy efficiency.

As AI is adopted more broadly in vehicles, we must consider whether these applications introduce significant safety and security risks. Vehicles are particularly sensitive to AI-related risks for at least three reasons:

1. Fleet deployment mechanisms such as Continuous Integration/Continuous Delivery (CI/CD) pipelines and OTA updates can turn a single upstream issue across thousands of vehicles.
2. Automotive systems operate across mixed trust zones, where cloud services, infotainment platforms, telematics, and safety-relevant domains coexist and interact.
3. In-vehicle interfaces and assistants function in time-constrained, high-trust environments, where drivers may act quickly on what the system presents without the opportunity for independent verification.

This chapter examines three AI-related risk patterns observed in 2025 and analyzes how these same patterns could plausibly propagate into vehicle ecosystems. Our focus is limited to model supply-chain compromise through namespace reuse, AI-orchestrated attack automation that accelerates vulnerability exploitation at scale, and assistant-mediated content injection or social engineering.

These patterns illustrate how AI reshapes cyber risk in the Overlap Era, not by introducing entirely new attack paths, but by amplifying scale, speed, and trust in ways that challenge traditional automotive security assumptions.

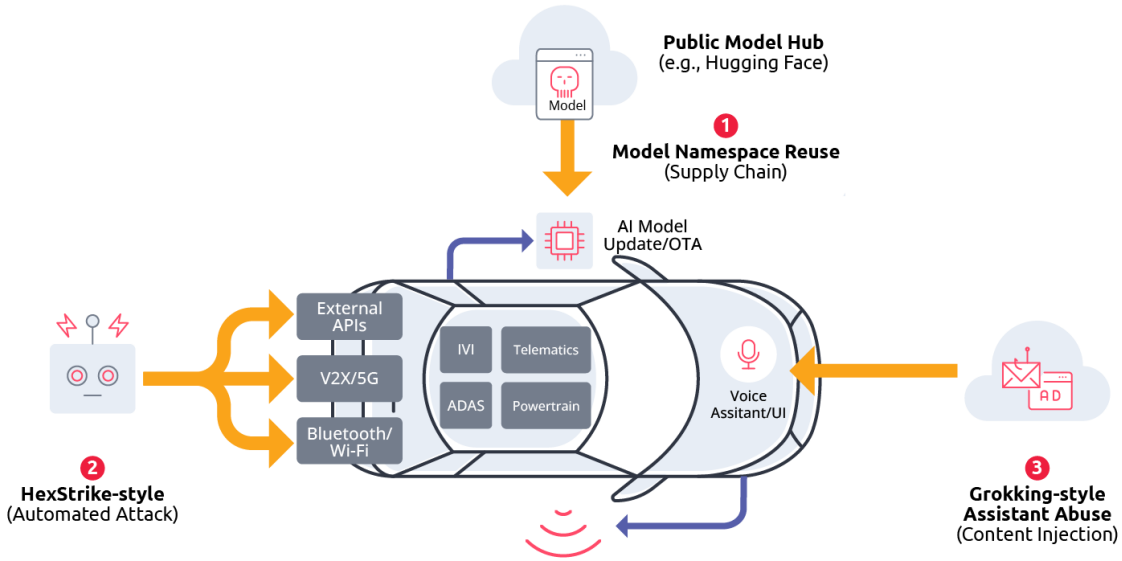


Figure 16. AI risk patterns analyzed in this chapter: model supply-chain compromise, automated exploitation through AI orchestration, and assistant-mediated content injection. These patterns demonstrate how AI amplifies cyber risk through scale, speed, and trust.

Model Namespace Reuse: Vehicle supply chain attacks

In the second half of 2025, security researchers reported an AI supply chain weakness referred to as "Model Namespace Reuse."[50] This can allow an attacker to publish a malicious model under a previously trusted identifier and, in certain deployments, lead to RCE when the model is retrieved and processed by downstream systems.

The risk was demonstrated within the Hugging Face ecosystem, where many projects reference models by a human-readable namespace, typically in the form "author/model-name." If the original author account is deleted or renamed, the old namespace may become available again. An attacker can then re-register that namespace and upload a trojanized replacement model that appears legitimate to any pipeline that trusts the model name or uniform resource locator (URL) without verifying ownership, provenance, or integrity.

This risk is amplified by the way cloud platforms integrate with third-party model hubs. Services such as Google's Vertex AI Model Garden and Microsoft's Azure AI Foundry provide native workflows for discovering, importing, and deploying external models. These integrations increase convenience but also increase the blast radius if name-based trust is used without strong verification.

In the automotive context, similar workflows are increasingly plausible. Automakers and Tier-1 suppliers may reference pre-trained models for perception, driver monitoring, speech recognition, or cabin intelligence during prototyping, CI/CD, or even production tooling. If a referenced namespace is later reclaimed by an attacker, a poisoned model could be introduced upstream and later distributed through OTA updates, supplier software development kit (SDK) updates, or third-party "model import" features.

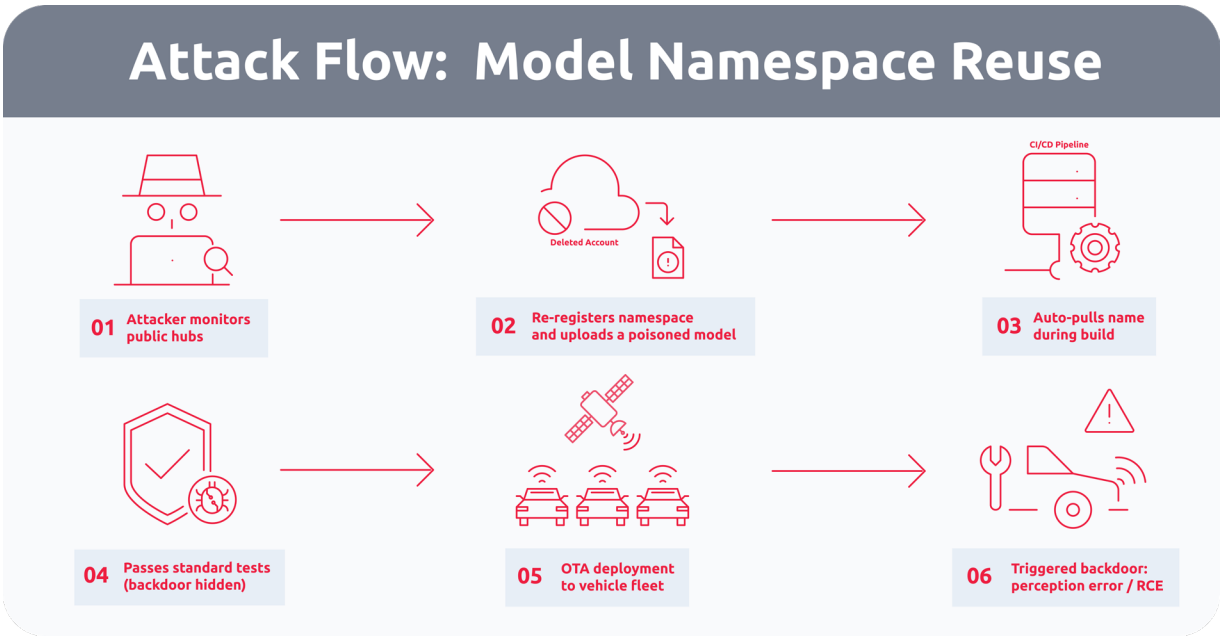


Figure 17. Attack sequence for Model Namespace Reuse, showing how name-based trust in AI model registries can enable supply-chain compromise and fleet-scale deployment of malicious models.

The Model Namespace Reuse attack chain is as follows:

1. The attacker monitors widely referenced model namespaces that are no longer controlled by their original maintainers.
2. The attacker re-registers the namespace and uploads a replacement model that looks identical on the surface in terms of metadata, documentation and baseline accuracy, but includes malicious payloads.
3. An automated build or validation pipeline retrieves the model by name, accepts it as an update, and passes standard performance testing due to preserved baseline behavior.
4. The poisoned model is packaged into a software release and deployed widely via OTA.

The resulting risks extend beyond traditional software compromise. Backdoored perception models may exhibit targeted misbehavior, creating rare-but-high-impact safety hazards. Compromised in-cabin or assistant-related models may influence data-handling workflows, increasing the likelihood of unintended audio or image exposure depending on system permissions. In environments where model loading involves unsafe deserialization or insufficient sandboxing, the Model Namespace Reuse can also enable RCE within AI workloads, potentially serving as a supply chain foothold for lateral movement if isolation boundaries are weak.

Overall, Model Namespace Reuse turns “model name trust” into a supply chain attack surface. For connected vehicles, this risk is particularly concerning because highly automated distribution mechanisms can convert a single upstream compromise into a fleet-scale incident.

HexStrike-style frameworks: Accelerated vulnerability exploitation

Recent developments in offensive security tools show that AI is increasingly being used not only to discover vulnerabilities but also to weaponize them at speed and scale.[51] Open-source, AI-assisted offensive security frameworks such as HexStrike-AI[52] demonstrate how the gap between vulnerability disclosure and large-scale exploitation can be significantly compressed. In public discussions around Citrix NetScaler vulnerabilities, researchers observed how AI-driven orchestration accelerated key stages of attack campaigns, including scanning for exposed instances, assembling exploit chains, deploying payloads, and establishing persistence.

Frameworks of this class automate core offensive tasks, including reconnaissance, vulnerability research, exploitation workflows, and reporting. Its design is typically described as agentic orchestration: user instructions are translated into tool-execution plans, results are analyzed, and the system iterates in a feedback loop to refine the next actions.

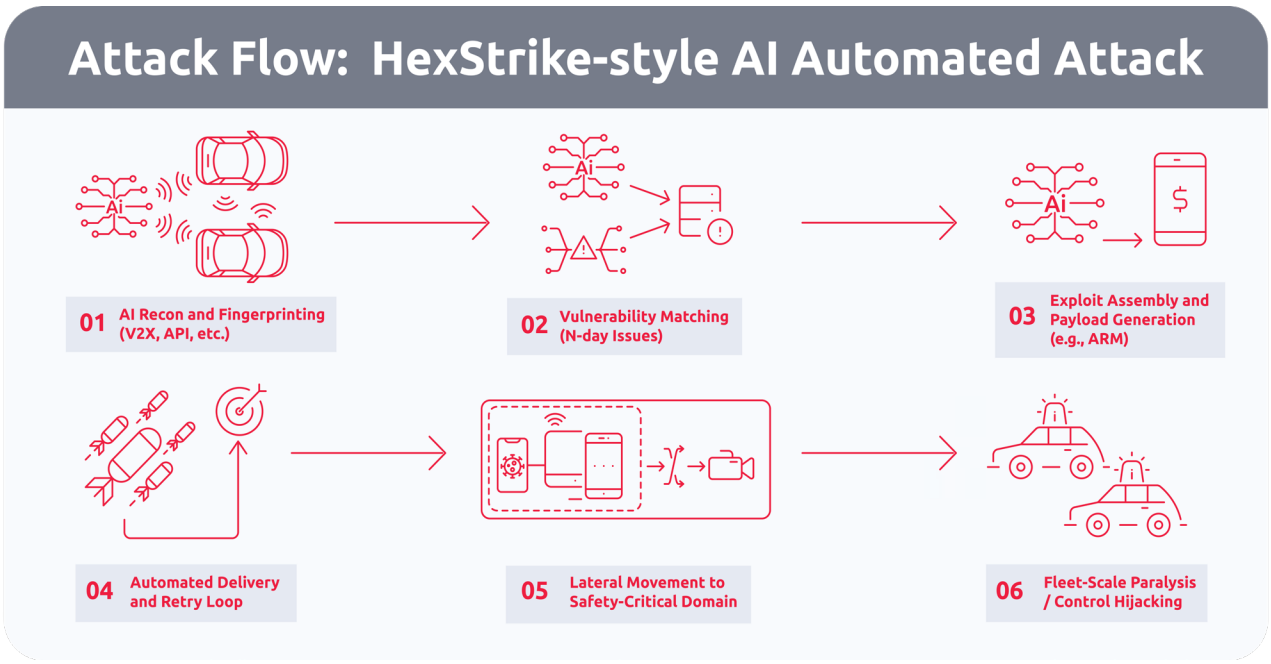


Figure 18. Sample attack flow of a HexStrike-style AI framework.

In a vehicle-relevant scenario, a "HexStrike-style framework" refers to a broader class of AI-orchestrated attack automation systems capable of chaining multiple offensive tools into end-to-end workflows. Their defining characteristic is industrialization: what was once a manual, expert-driven process becomes a repeatable pipeline that is faster and easier to scale.

Rather than manually crafting an exploit for each vehicle, an AI-driven workflow can automate the major phases of an attack campaign, especially in environments where multiple vehicles share common stacks, configurations, and where portions of the attack surface are reachable at scale via exposed APIs, widely deployed modules, or commonly used supplier components.

A representative attack flow may include:

1. **Reconnaissance and fingerprinting.** Automated scanning of reachable services, such as cellular-facing interfaces, Wi-Fi/Bluetooth stacks, or internet-exposed APIs, to infer software or firmware versions from protocol responses and subtle handshake differences.
2. **Vulnerability matching and exploit assembly.** Correlation of identified targets with known vulnerabilities, including "n-day" issues, followed by the automatic selection or generation of exploit chains tailored to the detected environment.
3. **Exploit delivery and post-exploitation.** Deployment of playloads through reachable services, with iterative retries when execution fails. Once a foothold is gained in a less critical domain, the attacker may attempt persistence and lateral movement.

The resulting risks are primarily temporal and systemic. Automated exploitation significantly compresses the defender response window, leaving OEMs and suppliers with less time to assess impact,

validate fixes, and roll out mitigations. If the same software stack or configuration is deployed across many vehicles, this compression transforms isolated compromises into campaign-style attacks.

The most severe outcomes, such as interference with powertrain, steering or other safety-critical controls, are not automatic. They typically require exploitable paths across domain boundaries. However, AI-driven automation increases the probability of finding and then chaining those weak links.

Grokking: Assistant-mediated abuse of infotainment systems

Recent abuse campaigns have shown how AI assistants can be manipulated to amplify malicious content, even when the original platform attempts to restrict it. One widely reported example involved the misuse of Grok, X's built-in AI assistant, to bypass the platform's link-posting restrictions and advertising safeguards. Attackers embedded malicious URLs in less visible metadata fields of promoted posts, then prompted the AI assistant to explain the post or provide the source link. Because Grok operated as a trusted system account, its responses can make the link appear more legitimate and significantly amplify distribution. This technique has been nicknamed "Grokking."[53]

Although observed in a social media platform, Grokking reveals a transferable risk pattern: trusted AI assistants can be manipulated into amplifying untrusted or malicious content, shifting the risk from the content itself to the interface that delivers it.

In vehicles, Grokking manifests as assistant-mediated content injection, where untrusted third-party content enters a high-trust in-vehicle assistant or infotainment interface and is transformed into an actionable output. A similar pattern can emerge when in-car voice assistants or infotainment AIs fetch, parse, summarize, or present external content and metadata, including business listings, sponsored results, navigation data, web snippets, media metadata, messaging previews, and encoded elements such as URLs, QR codes, or phone numbers.

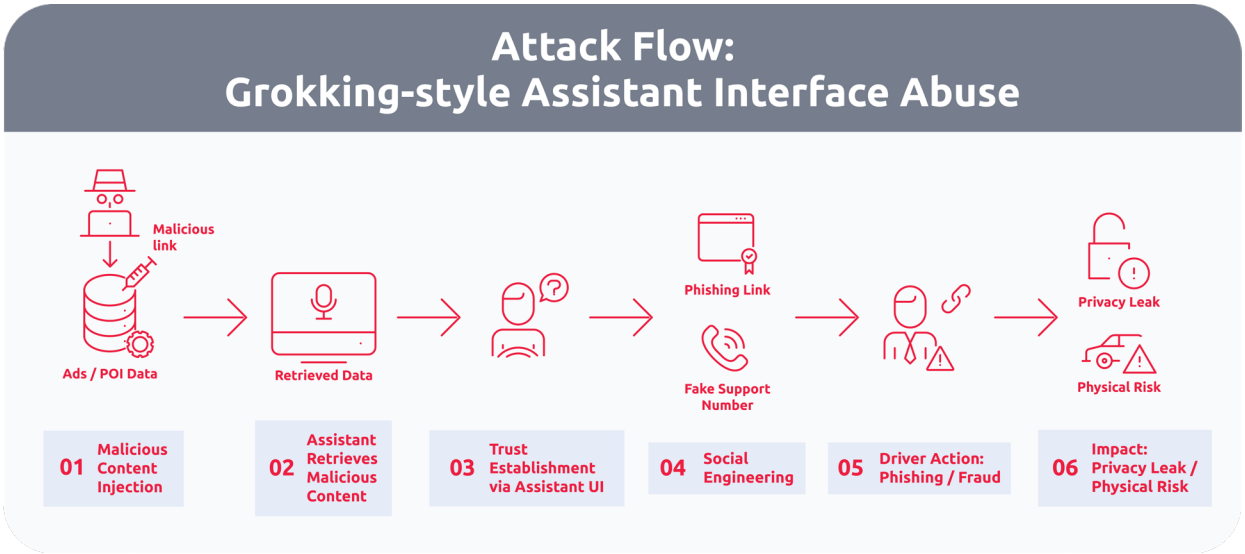


Figure 19. "Grokking" or assistant-mediated content injection attack flow, where untrusted third-party content is amplified through a high-trust AI assistant interface.

If adversaries can inject or influence any of those inputs, directly or indirectly through compromised third-party feeds, malicious ads, poisoned listings, or manipulated metadata, the assistant may inadvertently:

- surface malicious links ("Here's the link you asked for…")
- provide fraudulent phone numbers ("Call this support line…")
- suggest spoofed destinations ("Navigate to this address…"),
- repeat unsafe instructions that appear authoritative because they come from the vehicle's system user interface (UI).

Drivers typically treat built-in assistants as highly trusted system interfaces, giving their outputs disproportionate authority. As a result, the assistant's responses can become powerful social engineering channels, amplifying phishing and scam attempts within the vehicle and introducing safety externalities such as distraction, rushed decision-making, and potential navigation misuse.

The exposure increases further when assistants are allowed to initiate high-risk actions, such as navigation changes, phone calls, access to external links, app installation, device pairing, and payment and transaction workflow.

Conclusion

Artificial intelligence does not introduce entirely new categories of cyber risks to vehicles. As demonstrated across the three scenarios in this chapter — Model Namespace Reuse, HexStrike-style frameworks, and Grokking — AI instead reshapes how existing risks propagate. Its primary security impact lies in amplification rather than invention.

As connected vehicles continue to embrace AI-driven technologies, the key challenge for automotive cybersecurity is no longer whether vehicles can think, but whether they can trust correctly.

CHAPTER 4

Regulatory Blind Spots in the Overlap Era

Over the past decade, regulatory standards bodies and authorities have played an indispensable role in establishing baseline expectations for cybersecurity and safety across the automotive ecosystems. However, in the Overlap Era, certain risk scenarios emerge outside the scope of any single regulation. These exposures are not the result of regulatory shortcomings, but of system complexity arising from the coexistence of legacy vehicle architectures and advanced automotive technologies.

This chapter examines these regulatory blind spots through a “Swiss cheese” model, in which real-world dangers can still pass through despite full compliance by all participating parties. Using electric vehicle charging infrastructure and real-world ADAS incident investigations as examples, we illustrate how domain-specific regulations may leave systemic risks insufficiently governed when viewed end-to-end.

EVSE: Security gaps amid multi-standard compliance

Modern EV charging ecosystems extend beyond the charging hardware to include vehicle communication platforms, backend management platforms, cloud services, and utility-grid interfaces. This expansion introduces new risks and shared dependencies that are covered by different regulatory and certification bodies.

To address these risks, EVSE suppliers and operators have done their best to comply with existing regulations and international standards, including IEC-62443, ISO-15118-20, UN R155,[54] and NIST IR 8473.[55]

While these standards collectively create a layered defense for EV charging infrastructure, integration among these layers remains uneven.[56] For example, while UN R155 WP.29 Annex 5 provides mitigation guidance for interfaces between vehicles and external systems, its primary focus remains vehicle-centric. EVSE is referenced only indirectly, such as in Example 16.1 (Table A1), leaving implementation responsibility and verification largely outside the regulatory scope.

Standard	Primary Coverage	Key Gaps
ISO 15118-20:2022	High-level communication (HLC) between EV and EVSE, secured business transaction through TLS and PKI, customer-facing charging protocols and V2G protocols	Operating system, management plane, firmware, trusted elements
IEC 62443 (3-3 / 4-2)	Industrial control security, firmware hardening, zone segmentation, and vulnerability management	IT components of EVSE systems
ISO 21434[57]	Automotive cybersecurity engineering, supply chain management, cybersecurity management system (CSMS), Threat Analysis/Risk Assessment (TARA) across the software development lifecycle (SDLC)	Systems external to the vehicle
UN R155 WP.29	Vehicle cybersecurity regulation, Part C addresses “areas outside vehicles”, charging piles (Table B4, A16.1), and remote access (M20)	EVSE is addressed indirectly in Annex 5
NIST IR 8473	Physical security (PR.AC, PR.PT), supply chain risk management (ID. SC, ID.AM), continuous security monitoring (DE.CM, DE.AE, PR.IP), and data-in-transit protection (PR.DS)	NIST IR 8473 provides references but does not define protocol conformance, security-level–based requirements, and formal regulatory compliance artifacts.

Table 7. A comparison of EVSE standards and their respective coverage and key gaps

However, VicOne's analysis of vulnerabilities discovered in the Pwn2Own Automotive competitions indicates that compliance with one or more standards does not guarantee end-to-end protection. When mapping coverage of vulnerabilities discovered in an EV charger during the Pwn2Own Automotive competition,[58] security gaps emerged due to differences in scope and the voluntary nature of implementation across some standards.[59]

Amid this fragmented coverage, NIST IR 8473 serves as a key integrative reference. It consolidates broader frameworks, including NIST SP 800-53r5 (catalog of security and privacy controls), PCI-DSS, IEC 62443, and NERC CIP (grid-related risks), into a verifiable checklist spanning the vehicle, the EV charger, cloud platform, and the utility-grid interfaces.

NIST IR 8473 may serve as a useful reference framework for organizations seeking to evaluate whether compliance across multiple standards also translates into effective coverage of real-world attack paths.

ADAS: Perception risks despite safety regulations

From a regulatory perspective, ADAS functions are governed through a combination of safety and system assurance frameworks. UNECE R79[60] defines requirements and test procedures for steering equipment, including automated steering functions. UNECE R160 specifies event data recorder (EDR) requirements to support post-incident analysis, while UNECE R155 and R156 establish organizational governance for Cybersecurity Management Systems (CSMS) and Software Update Management Systems (SUMS).

However, two recent incidents illustrate that regulatory compliance does not necessarily ensure predictable system behavior under all real-world conditions.

- In November 2023, an Audi Q3 equipped with ADAS collided with a stationary engineering crash-cushion vehicle on Highway 1 in Taiwan.[61] Although no injuries were reported, the investigation identified several contributing factors, including driver distraction, over-reliance on ADAS, and limited understanding of system limitations. Notably, the Automatic Emergency Braking (AEB) did not activate during the incident. Subsequent tests showed that the AEB failed to respond when encountering stationary vehicles.
- In January 2025, a Hyundai IONIQ5 with one driver and seven passengers (seating capacity is only 5) crashed into a traffic island on a highway ramp and caught fire following battery damage.[62] The incident resulted in four fatalities and four serious injuries. While the vehicle was equipped with an EDR compliant with UNECE R160, local authorities were unable to decode the data due to equipment limitations. As a result, it could not be conclusively determined whether ADAS functions were enabled before EDR was decoded.

Both vehicles met SAE J3016 Level 2 automation standards,[63] with Adaptive Cruise Control (ACC), Lane Following Assist (LFA), and Lane Keeping Assist (LKA). Testing showed that while ADAS functions

successfully navigated the first turn of the entrance route, both LFA and LKA were automatically deactivated before the second left turn, requiring manual driver intervention. In repeated test runs, the system deactivated after detecting specific deceleration markings.

Incidents such as these point to a broader and more pervasive risk surface. Lawfully deployed, though occasionally non-compliant, road markings, degraded chevrons, and region-specific lane patterns may, under rolling-shutter sampling,[64] present the camera with quasi-periodic visual pulses. In current implementations where LKA and LFA rely primarily on vision-based perception, ambient perturbations can become function-disabling, rather than merely accuracy-degrading.

The security question then is not only "Can an attacker fool the model?" but also "How robust is the model to lawful, cross-jurisdictional infrastructure that may appear adversarial to the camera?"

When viewed through a regulatory lens, these perception-driven behaviors expose limitations in the scope of existing safety and cybersecurity frameworks. Existing ADAS regulations address steering performance, cybersecurity governance, software updates, and post-incident analysis. However, none of them impose explicit requirements for perception robustness under diverse real-world infrastructure conditions.

Closing this regulatory gap requires treating infrastructure variability as part of the threat model, evaluating perception robustness across markets during type approval, and ensuring that automated deactivation behavior is observable and auditable.

Conclusion

The EV charging infrastructure and real-world ADAS incidents examined in this chapter reaffirm the structural limits of regulations in the Overlap Era. These observations do not reflect deficiencies in individual regulations, but rather the cumulative effect of partial coverage across complex and interdependent vehicle systems.

At the same time, national priorities, market conditions, and technology adoption have shifted significantly in recent years. As a result, cybersecurity safeguards embedded within regulatory frameworks may no longer align uniformly across geographies, introducing additional complexity in achieving consistent end-to-end security, especially for globally deployed vehicles.

In this environment, compliance remains a necessary foundation, but it cannot serve as the sole mechanism for managing risk. Effective cybersecurity in the Overlap Era requires continuous visibility across vehicles, infrastructure, software platforms, and external dependencies — enabling automotive OEMs to identify and manage exposure that extends beyond the boundaries of any single regulation.

CHAPTER 5

Recommendations

The 2025 threat landscape, together with the risks emerging for 2026, signals a structural shift. Automotive cybersecurity is no longer defined by how many vulnerabilities are found or how quickly they are patched. It is defined by whether car manufacturers or OEMs have built a system that can continuously sense risk, interpret impact, and act decisively.

At its core, this requires a closed loop built on three forces: testing to understand how systems can be attacked, operational telemetry to understand how systems behave in reality, and continuous risk recalculation to translate technical signals into executive decisions.

The following recommendations form three strategic layers that together create an automotive cyber risk operating system for SDV, AI, OTA-centric platforms, and energy-connected mobility ecosystems.

Governance layer: Ensuring OEMs can make decisions under pressure

These recommendations determine whether risk signals can become real decisions.

- **Shift from system-based control to cross-domain risk governance.** Risk can no longer be managed by separating IT, cloud, vehicle, and charging infrastructure. Attacks now span all of them simultaneously. OEMs must govern risk by service, fleet, and impact radius, with clear ownership and escalation paths. Without unified accountability, risk assessment has no executive endpoint.
- **Integrate supply-chain platforms and dealer ecosystems into security accountability.** As attackers increasingly target centralized dealer systems and shared platforms, security must be measured by service availability and revenue continuity. Supply-side platforms will become part of OEM and dealer performance accountability under a new “security availability” standard.

Risk computation layer: Ensuring risk can be recalculated in real-time

These recommendations define whether exposure is visible dynamically rather than retrospectively.

- **Replace static TARA with event-driven, continuously operating Dynamic TARA.** Risk assessment must move from milestone documentation to real-time recalculation. Triggers include code merges, software bill of material (SBOM) changes, zero-day disclosures, threat intelligence updates, and vehicle or cloud anomalies. Risk becomes a living variable, not a quarterly report.
- **Establish Live SBOM and AI BOM as core enterprise assets.** Software and AI models must both be governed as critical assets. SBOM provides visibility into software supply-chain exposure. AI BOM provides traceability for models, training data lineage, deployment scope, and integrity validation.
- **Make context and attack-path intelligence the foundation of risk computation.** Risk can no longer be evaluated through isolated vulnerabilities. It must be computed through asset context, exposure conditions, and realistic attack paths that show how weaknesses combine into enterprise-scale impact.

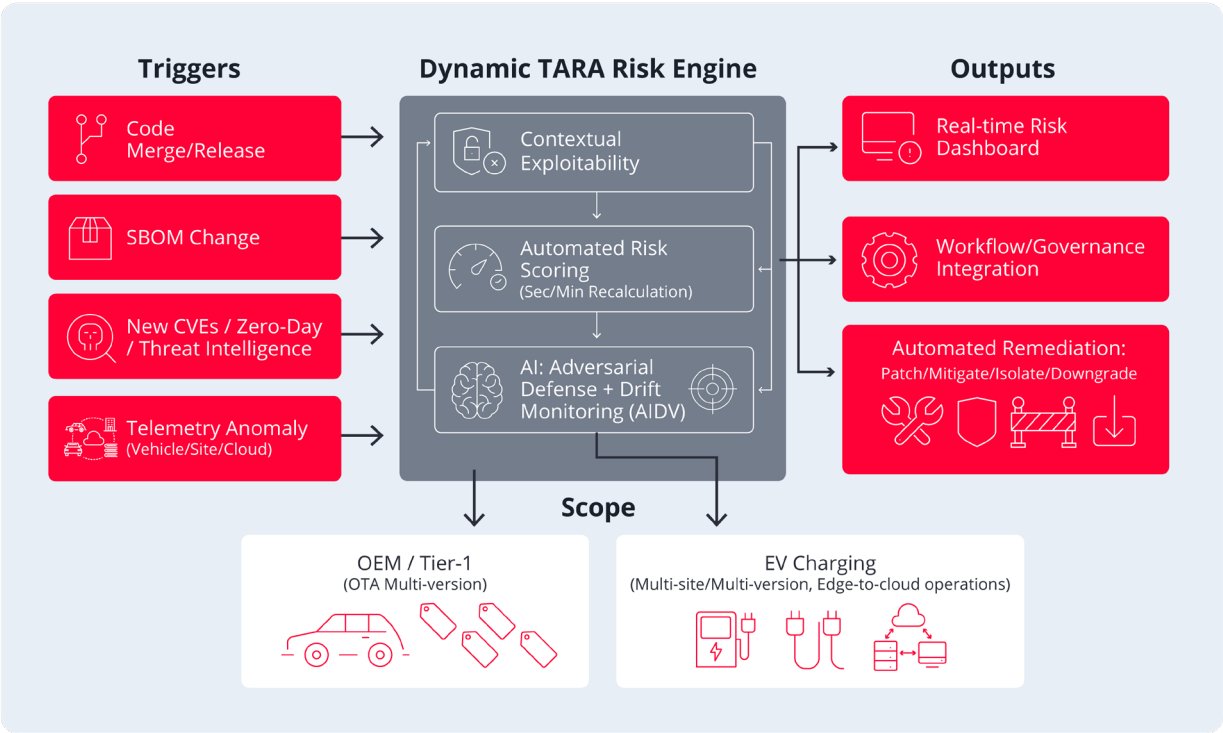


Figure 20. In a dynamic TARA model, risk evolves continuously in response to software changes, supply chain updates, and real-world system signals.

Operational feedback layer: Ensuring OEMs evolve faster than attackers

These recommendations determine whether the system can learn and adapt continuously.

- **Use AI-enhanced red teaming and attack-chain simulation.** Security testing must evolve from isolated vulnerability discovery to continuous, AI-accelerated attack-path modeling. AI enables large-scale fuzzing, exploit chaining, and scenario generation that feeds directly into risk recalculation and architectural hardening.

- **Treat user interfaces as the highest-priority trust boundaries.** IVI systems, TCUs, and in-vehicle AI assistants are the points where external input is transformed into system authority. They must be protected with the highest standards of memory safety, privilege isolation, input validation, and continuous AI behavioral monitoring at the vehicle edge for every interaction.

- **Govern EV charging infrastructure as an integrated edge-to-cloud operations asset.** Charging spans firmware, protocols, cloud platforms, operations consoles, payment systems, and energy integrations. Risk must be assessed across all layers simultaneously, supported by operational telemetry, automated mitigations, and real-time dashboards. Charging security is now part of national energy reliability and public trust.

Conclusion

Automotive cybersecurity maturity is no longer measured by vulnerability counts or patch speed. It is measured by whether an organization has built a closed-loop risk system that can continuously:

- test how systems may be attacked, using AI to explore attack paths at scale
- observe real-world behavior, using AI to detect weak signals and abnormal patterns
- recalculate exposure using automated risk intelligence that executives can act on immediately

Automotive OEMs that succeed will transform cybersecurity from a defensive function into a core capability for operational resilience, leadership credibility, and long-term market trust.

CHAPTER 6

Predictions: Navigating Automotive Cyber Risks in the Overlap Era

Today's connected vehicles are no longer isolated mechanical systems defined by on-board systems alone. They have become increasingly distributed software platforms, continuously exchanging data with OTA update servers, fleet management and mobility platforms, smart homes and energy systems, AI perception and driver-assistance engines, and EV charging infrastructure and grid operators.

Because of this transformation, the attack surface has expanded far beyond the vehicle's ECUs to now include cloud APIs, AI supply-chain data, EV charging networks, and mobility service platforms. Future automotive cyber risk will be defined less by individual vulnerabilities and more by where authority, responsibility, and decision-making intersect when disruption occurs. The following predictions outline how this shift is expected to unfold in the Overlap Era.

Cyber incidents become leadership stress tests

Vehicles are now among the most visible and safety-critical digital platforms in society. Cyber incidents are therefore no longer evaluated primarily as technical breakdowns. They are interpreted as failures of governance, accountability, and leadership credibility.

This shift will accelerate as attacks increasingly originate from the supply chain. Responsibility becomes fragmented across dealers, suppliers, and shared platforms, yet accountability becomes more centralized on the OEM. In the eyes of customers, regulators, and the public, technical ownership is irrelevant. Brand responsibility remains singular and rests with the manufacturer.

Our data already shows this transition. Dealer-related incidents have grown from 5% to 15%, confirming that the distribution channel is no longer a peripheral risk but a core attack surface. At the same time, vulnerabilities are concentrating in common IT platforms used across suppliers and dealer networks. This transforms supply-chain exposure from isolated vendor failures into systemic industry risk. One compromised dependency now has the potential to affect many brands simultaneously.

The December 2025 Nanyang Industrial incident[65] illustrates the next phase of this evolution. Attackers bypassed corporate negotiation channels and used stolen customer data to send extortion messages directly to vehicle owners via SMS. The attack no longer targeted infrastructure alone. It targeted the brand trust itself. This signals a structural change in cyber risk. Brand identity and customer confidence have become operational attack surfaces.

Over the next three years, cyber incidents in the automotive sector will increasingly be judged less by technical containment and more by executive response. Speed, clarity of communication, and decision authority will shape business impact more than vulnerability remediation timelines.

For OEM leadership, the new standard will no longer be “Have we checked every regulatory box?” It will be “Have we built governance structures, supply-chain visibility, and crisis authority that allow us to act decisively under pressure?”

AI training data becomes the new supply chain risk

With automotive AI systems heavily relying on shared and third-party training data pipelines, the attacker’s focus will shift from vehicles to the data that informs automated decision-making. Compromised training data will introduce persistent, cross-generational risk into ADAS behavior. The resulting exposure will be difficult to remediate, harder to explain to regulators, and increasingly central to questions of legal liability and insurability.

One OTA breach will become a boardroom crisis

The centralization of trust within the OTA infrastructure means that a single compromise will be sufficient to distribute malicious firmware on fleet scale. In such a scenario, the primary risk is no longer technical recovery, but executive decision latency. Leadership will be forced to determine, under extreme time pressure, whether to suspend updates, disable vehicle functionality, or accept widespread operational disruption across robotaxi, logistics, and connected fleet services.

Ransomware becomes a fleet shutdown weapon

Platform concentration across dealer systems, after-sales operations, and fleet management platforms widens the impact of ransomware, extending it from data encryption to deliberate operational paralysis. The most damaging attacks will target revenue continuity at scale, forcing OEMs and dealer groups to treat cyber incidents as direct business disruptions rather than IT failures. In this environment, cyber risk will be measured by security availability and the organization's ability to sustain revenue-generating operations during active disruption.

Cyber risk extends into energy and infrastructure accountability

Tight integration between vehicles, EV chargers, and home or grid-connected energy systems expands automotive cyber risk beyond organizational and industry boundaries. Disruptions will no longer be containable within automotive IT or product teams. Instead, leadership will face shared accountability across mobility, energy, and public infrastructure domains, often without preexisting governance or decision frameworks.

Appendices

Appendix A. ADS Standards and Specifications Timeline

Year	Standard	Description	Notes
2011	ISO 26262 (1st ed.)	First automotive functional-safety standard adapted from IEC 61508	Passenger cars only in first edition
2014	SAE J3016 (initial publication)	Six-level (0–5) taxonomy for driving automation	Subsequent clarifications in 2016 and 2021
2018	ISO 26262 (2nd ed.)	Scope expanded to (nearly) all road vehicles; adds semiconductor guidance	Second edition published Dec 2018
2019	ISO/PAS 21448 (SOTIF)[66]	First public spec for "safety of the intended functionality" (beyond malfunction)	Interim PAS before full standard
2014~	Euro NCAP adds AEB to star rating (from 2014)	Consumer-rating pull for AEB (city & later inter-urban/pedestrian/ cyclist)	Important market adoption trigger
2021	ISO/SAE 21434	Cybersecurity engineering process requirements for road vehicles	Complements ISO 26262; focuses on cybersecurity risk management
2022	ISO 21448 (SOTIF, full standard)	Replaces PAS; formalizes SOTIF argumentation & measures	First edition cancels and replaces ISO/PAS 21448:2019
2017 ~2020	UN R79 (ACSF), UN R152 (AEBS)[67]	Technical definitions & approval provisions (e.g., ACSF B1 lane-keeping; AEBS tests)	Useful for technical scoping of LKA/LFA and AEB behavior
2021	UN R160 (EDR)	Global "black-box" baseline for event data recorders	Adopted Oct 21, 2021 (M1/ N1)

Appendix B. ADAS Feature Rollout Timeline

Feature	Milestone and First Production	Year
Cruise Control	First factory cruise control ("Auto-Pilot") on Chrysler Imperial	1958
ACC (Adaptive Cruise Control)	Early lidar distance warning (Mitsubishi Debonair)	1992
	Laser ACC with throttle control (Mitsubishi Diamante)	1995
	Toyota laser ACC (Celsior/LS400 JP)	1997
	First radar ACC (Mercedes-Benz "Distronic", S-Class W220)	1999
LDW (Lane Departure Warning)	First production LDW in Europe (Mercedes Actros trucks)	2000
	First passenger-car LDW in NA (Infiniti FX/M)	2004–05

LKA / Lane-Keeping Assist (reactive)	First production LKAS (Honda Inspire, JP)	2003
	Toyota Crown Majesta adds LKA	2004
	Mercedes PRE-SAFE® Brake (autonomous braking)	2006
	Volvo “City Safety” made standard on XC60	2008
AEB (Automatic/ Autonomous Emergency Braking)	Euro NCAP includes AEB in crash-rating scheme	2014~
Lane-centering / Highway LFA (proactive)	Tesla Autopilot (lane centering + TACC) software release	2015
	Nissan ProPILOT Assist (Japan Serena global)	2016–17
	GM Super Cruise (hands-free L2, mapped highways)	2017
	Toyota Lane Tracing Assist (TSS 2.0)	2018
	Hyundai/Kia Lane Following Assist / HDA	2018–19
From feature to “most new cars”	AEB uptake accelerates (NCAP pull & OEM pledges)	2018–2022
	LDW adoption in the U.S. fleet (production share)	2018
	ACC & Lane-keeping availability across models (U.S.)	2021
	Euro NCAP Assisted-Driving gradings go public[68]	2020s

Appendix C. ADAS Feature Rollout and Corresponding Risk Evolution

Feature Generation	Representative Capabilities	New or Heightened Risk Types	Example Risk Scenarios	Risk Management Focus
Driver Aids (1950s–1990s)	Basic cruise control, passive alerts	Mechanical or control failure	Unintended acceleration or loss of throttle control	Component reliability, fail-safe design
Adaptive Systems (1990s–2000s)	Adaptive Cruise Control (ACC), early AEB	Sensor coverage and calibration risk	Radar misreads in heavy rain; false braking on reflective surfaces	Sensor redundancy, calibration checks, basic diagnostics
Lane Awareness Systems (2000s–2010s)	LDW, early LKA	Perception accuracy and environmental dependency	Lane departure due to worn paint or poor lighting	Scene validation, wider test coverage, rule-based perception safety
Integrated Lateral–Longitudinal Control (2015–2020)	Lane centering, highway assistance	Functional-limit and human interaction risk	Driver overtrust; system disengagement at boundaries	HMI clarity, ODD definition, driver monitoring
Networked and AI-Driven Systems (2020s–Present)	Sensor fusion, machine-learning-based perception, connected ADAS	Model vulnerability, data integrity, and cyber interference	Spoofed signs, adversarial images, or corrupted OTA updates	Secure model training, runtime anomaly detection, integrated safety–security governance

Appendix D. Evolution of Access Technologies

Year	Representative Capabilities	New or Heightened Risk Types	Example Risk Scenarios
1982	IR remote keyless entry(“PLIP”)	First production rollout on Renault Fuego(remote-controlled door locks).	–
1993	Early passive keyless entry (PKE)	Chevrolet Corvette (C4) adds proximity-style PKE for lock/unlock (ignition still keyed).	–
1999–2006	LIN bus emerges as the low-cost body sub-bus (windows, mirrors, wipers, rain sensors)	LIN 1.0 (1999) □ LIN 2.1 (2006) becomes the de facto spur beneath body CAN.	–
2000s	UDS (ISO 14229) standardizes diagnostics/coding over CAN	UDS becomes the default dealer/service interface for BCM/BDC coding.	–
2008	–	–	KeeLoq rolling-code RKE broken via algebraic/slide and power-analysis attacks (FSE/CRYPTO).
2011	–	–	Relay attacks on passive keyless entry/start (PKES) shown end-to-end (NDSS).
2012	–	–	Hitag2 immobilizer crypto broken; practical key recovery (USENIX Security).
2015	–	–	Megamos Crypto immobilizer fully reverse-engineered; practical attack paths (USENIX Security).
2016	–	–	Large-scale RKE weaknesses across multiple brands documented (USENIX Security) + mainstream coverage.
2020	Phone-as-a-key (NFC/BLE) in volume	BMW Digital Key for iPhone launches (CarKey, NFC), first wave of phone wallets controlling body UX.	
2021	UWB ranging enters production digital keys	BMW Digital Key Plus with UWB on iX (hands-free proximity, angle/distance used for mirrors/handles/lighting choreography).	
2022	CCC Digital Key Release 3.0(BLE+NFC+UWB)	Spec formalizes hands-free, location-aware keys with UWB distance-bounding; sets the cross-industry baseline.	

References

1 https://vicone.com/blog/when-a-cyber-incident-halts-an-automaker-a-wake-up-call-for-supply-chain-security

2 https://securelist.com/mercedes-benz-head-unit-security-research/115218/

3 https://blackhat.com/asia-25/briefings/schedule/index.html#remote-exploitation-of-nissan-leaf-controlling-critical-body-elements-from-the-internet-44048

4 https://www.vicone.com/automotive-zero-day-vulnerabilities

5 https://nvd.nist.gov/vuln/detail/CVE-2024-45434

6 https://pcacybersecurity.com/resources/advisory/perfekt-blue

7 https://nvd.nist.gov/vuln/detail/CVE-2023-34402

8 https://github.com/klsecservices/Advisories/blob/master/K-Mercedes-Benz-2023-007.md

9 https://firebasestorage.googleapis.com/v0/b/vestel-shield.firebasestorage.app/o/PRODUCTION%2F2%2FVSA-2.pdf?alt=media&token=de58d25d-9a96-4e6a-9263-4d3ec57be3cd

10 https://nvd.nist.gov/vuln/detail/CVE-2024-8997

11 https://nvd.nist.gov/vuln/detail/CVE-2025-22370

12 https://github.com/qiantx/cve/blob/main/CVE2.md

13 https://nvd.nist.gov/vuln/detail/CVE-2025-8347

14 https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/

15 https://blackhat.com/us-17/briefings.html#free-fall-hacking-tesla-from-wireless-to-can-bus

16 https://vicone.com/blog/from-pwn2own-automotive-a-critical-zero-click-rce-bluetooth-vulnerability-in-the-alpine-halo9-ivi-system

17 https://vicone.com/blog/breaking-down-the-pioneer-ivi-system-3-bug-exploit-chain-from-pwn2own-automotive-2024

18 https://vicone.com/blog/breaking-into-teslas-ivi-system-synacktivs-two-bug-exploit-chain-at-pwn2own-automotive-2024

19 https://www.rswebsols.com/news/remote-code-execution-vulnerability-in-apple-carplay-allows-for-root-access/

20 https://vicone.com/blog/exposing-the-risks-security-takeaways-from-a-successful-android-ota-decryption

21 https://vicone.com/blog/is-the-automotive-industry-prepared-to-navigate-api-security-risks-in-software-defined-vehicles

22 https://www.wardsauto.com/news/kardome-ceo-ai-voice-control-domination-carries-risks/778433/

23 https://www.techbriefs.com/component/content/article/50272-a-hack-to-trick-automotive-radar

24 https://doi.org/10.48550/arXiv.2507.09095

25 https://dl.acm.org/doi/10.1145/3636534.3649372

26 https://www.usenix.org/conference/usenixsecurity24/presentation/lou

27 https://doi.org/10.1145/3643832.3661854

28 https://www.ndss-symposium.org/ndss-paper/auto-draft-451/

29 https://dl.acm.org/doi/10.1145/3372297.3423359

30 https://www.ndss-symposium.org/ndss-paper/on-the-realism-of-lidar-spoofing-attacks-against-autonomous-driving-vehicle-at-high-speed-and-long-distance/

31 https://dx.doi.org/10.14722/vehiclesec.2024.23014

32 https://www.usenix.org/conference/usenixsecurity23/presentation/cao

33 https://ieeexplore.ieee.org/document/10199488

34 https://www.ndss-symposium.org/ndss-paper/madradar-a-black-box-physical-layer-attack-framework-on-mmwave-automotive-fmcw-radars/

35 https://arxiv.org/abs/2205.06567

36 https://www.ndss-symposium.org/ndss-paper/un-rocking-drones-foundations-of-acoustic-injection-attacks-and-recovery-thereof/

37 https://www.ndss-symposium.org/ndss-paper/powerradio-manipulate-sensor-measurement-via-power-gnd-radiation/

38 https://doi.org/10.1109/JPROC.2016.2526658

39 https://arxiv.org/abs/2401.01304

40 https://doi.ieeecomputersociety.org/10.1109/EuroSP57164.2023.00067

41 https://arxiv.org/abs/2403.02329

42 https://vicone.com/blog/from-fob-to-phone-how-ccc-digital-key-40-shapes-automotive-cybersecurity

43 https://www.trendmicro.com/en_us/research/21/l/examining-log4j-vulnerabilities-in-connected-cars.html

44 https://www.brokenwire.fail/

45 https://www.vice.com/en/article/russian-electric-vehicle-chargers-hacked-tell-users-putin-is-a-dickhead/

46 https://vicone.com/company/press-releases/pwn2own-automotive-2024-vicone-and-zdi-lead-first-hackathon-to-uncover-cyber-vulnerabilities-in-connected-vehicles

47 https://vicone.com/company/press-releases/vicone-and-zero-day-initiative-hold-worlds-largest-zero-day-vulnerability-discovery-contest-pwn2own-automotive-2025

48 https://vicone.com/blog/electric-vehicle-charger-security-risks-how-vulnerabilities-could-lead-to-fire-hazards

49 https://www.iso.org/standard/68383.html

50 https://unit42.paloaltonetworks.com/model-namespace-reuse/

51 https://blog.checkpoint.com/executive-insights/hexstrike-ai-when-llms-meet-zero-day-exploitation/

52 https://github.com/0x4m4/hexstrike-ai

53 https://www.bleepingcomputer.com/news/security/threat-actors-abuse-xs-grok-ai-to-spread-malicious-links/

54 https://unece.org/sites/default/files/2023-02/R155e%20%282%29.pdf

55 https://csrc.nist.gov/pubs/ir/8473/final

56 https://vicone.com/blog/is-iso-15118-enough-to-secure-ev-charging

57 https://www.iso.org/standard/70918.html

58 https://vicone.com/blog/from-pwn2own-automotive-2-rce-vulnerabilities-in-the-phoenix-contact-charx-sec-3100-ev-charging-controller

59 https://vicone.com/blog/from-pwn2own-automotive-how-zero-day-vulnerabilities-expose-gaps-in-evse-cybersecurity standards

60 https://unece.org/sites/default/files/2024-04/R079r5e.pdf

61 https://www.ttsb.gov.tw/1243/22385/40232/post

62 https://www.ttsb.gov.tw/1243/22385/44949/post

63 https://www.sae.org/standards/j3016_202104-taxonomy-definitions-terms-related-driving-automation-systems-road-motor-vehicles

64 https://www.usenix.org/conference/usenixsecurity22/presentation/yan

65 https://udn.com/news/story/7266/9222442

66 https://www.iso.org/standard/77490.html

67 https://unece.org/sites/default/files/2024-05/R152r2am3e.pdf

68 https://www.euroncap.com/en/ratings-rewards/assisted-driving-gradings/

VicOne

Crossroads: Automotive Cybersecurity in the Overlap Era
VicOne 2026 Automotive Cybersecurity Report

Learn more about VicOne by visiting VicOne.com or scanning this QR code: