VicOne

The State of SDV Cybersecurity: Navigating Innovation and Risk

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

The transition to software-defined vehicles (SDVs) heralds a more connected, intelligent, and sustainable era of mobility. However, this transformation brings significant challenges, particularly in cybersecurity, software complexity, and regulatory compliance. The reliance of SDVs on over-the-air (OTA) updates, cloud connectivity, and advanced in-vehicle systems necessitates a robust framework to manage risks while ensuring safety, privacy, and resilience.

To unlock the full potential of SDVs, the automotive industry must embrace proactive strategies and innovative solutions. This requires close collaboration among automakers, suppliers, and technology providers to foster trust, prioritize security, and uphold a commitment to innovation. Ultimately, SDVs represent not just a technological evolution but a fundamental paradigm shift in mobility.

Critical Threats to SDV Cybersecurity

Cybersecurity risks are among the most significant challenges facing SDVs. Considering their reliance on software and connectivity, this is hardly surprising. These risks arise from an expanded attack surface shaped by integrated systems, external communication channels, and dependence on cloud infrastructure. Below, we summarize the key cybersecurity threats confronting SDVs.

Vehicle Control and Safety Compromises

Compromised systems can directly impact critical safety features like braking, steering, and acceleration, placing passengers and public road users at significant risk.

- **Vehicle hijacking:** Attackers can exploit vulnerabilities in SDV software to remotely control critical vehicle functions such as steering, braking, or acceleration. This poses a direct risk to passenger safety and public road security. Demonstrations have shown how compromised electronic control units (ECUs) or communication channels can lead to complete system takeovers, highlighting the severity of this risk.
- **Denial-of-service (DoS) attacks:** DoS attacks can disrupt vehicle systems, rendering them nonfunctional or significantly impaired. For example, attackers could overwhelm communication systems, preventing vehicles from receiving critical updates or real-time navigation data.
- **Virtualization risks:** SDVs leverage virtualization to consolidate functionalities such as infotainment, advanced driver assistance systems (ADASs), and autonomous driving on shared hardware. However, any breach in one virtual machine could impact other critical systems if isolation measures fail.

- **Network risks:** Traditional CAN (Controller Area Network) bus systems are inherently weak due to their lack of authentication and encryption. While the shift to high-bandwidth Ethernet networks offers improvements, it introduces new risks. Attackers could exploit improperly secured Ethernet-based architectures if features like MACsec or IPsec are not implemented.
- **Autonomy-specific risks:** Autonomous SDVs are particularly vulnerable to manipulation of sensor data or machine learning models. Corrupt inputs to cameras, lidar, or other sensors, could mislead the vehicle, causing it to misinterpret its surroundings.

Software and Update Exploitation

The reliance on OTA updates and third-party software introduces significant challenges in maintaining the integrity and security of SDVs.

- **OTA update exploits:** While OTA updates are essential for SDVs, unsecure mechanisms can introduce risks. For instance, attackers could deliver malicious updates, disable features, or inject backdoors, compromising vehicle functionality and user data.
- **Supply chain vulnerabilities:** Third-party software or hardware can introduce risks during production. Attackers could exploit unpatched vulnerabilities to insert malicious code into components used across multiple vehicle models.
- **Legacy system risks:** Vehicles can remain operational for decades, which raises the challenge of securing outdated systems. Legacy systems that no longer receive updates are particularly vulnerable to emerging threats.

Data Breaches and Privacy Violations

SDVs generate and process vast amounts of data, making them prime targets for cyberattacks. Protecting this data is vital to ensuring user privacy and maintaining trust.

- **Cloud and backend vulnerabilities:** SDVs heavily rely on cloud platforms for processing data, deploying features, and conducting real-time analytics. Compromised cloud infrastructure can give attackers access to multiple vehicles simultaneously, enabling large-scale attacks or ransomware that can target fleets. Manipulated data, such as navigation routes or OTA update configurations, could misguide autonomous driving systems, delay critical updates, or trigger false alarms, leading to safety concerns and operational disruptions.

- **Data theft and privacy breaches:** SDVs generate and store extensive customer data, including location history, driving patterns, biometrics, and personal preferences. Cyberattacks on vehicles or associated cloud platforms could lead to data theft, identity fraud, or misuse of sensitive information.
- **Third-party integration risks:** SDVs often integrate with third-party applications or external systems, such as smart homes, charging networks, and fleet management platforms. Weaknesses in third-party application program interfaces (APIs) or systems can serve as entry points for attackers to compromise vehicles, steal data, or disrupt operations.

Financial and Operational Disruption

The financial and operational fallout from cyberattacks on SDVs is substantial. From ransomware to fleet-specific attacks, these incidents disrupt businesses and erode user trust.

- **Ransomware and extortion:** Ransomware attacks that target SDVs could lock users out of their vehicles or disable critical systems until a ransom is paid. Fleetwide attacks could disrupt logistics, ride-sharing services, or other operations.
- **Fleet-specific attacks:** Fleet management systems are particularly attractive targets. Attackers could manipulate routes, disable vehicles, or access sensitive business data, causing operational delays and financial losses.

Prevalent SDV Cybersecurity Threats

In Table 1, we highlight the top SDV cybersecurity threats based on the number of vulnerabilities associated with them, as published over the 10-year period from 2014 to 2024.

Threat	Category	Count
Supply chain vulnerabilities	Software and update exploitation	1,564
Third-party integration risks	Data breaches and privacy violations	308
Vehicle hijacking	Vehicle control and safety compromises	295
Fleet-specific attacks	Financial and operational disruption	44
Cloud and backend vulnerabilities	Data breaches and privacy violations	30
Network risks	Vehicle control and safety compromises	27
Virtualization risks	Vehicle control and safety compromises	3

Table 1. The top SDV cybersecurity threats based on the number of vulnerabilities associated with them, as published from 2014 to 2024

As can be surmised from traditional IT cyberattacks and the number of published vulnerabilities, the automotive supply chain remains a prime target because of its reliance on numerous suppliers, making it a persistent challenge to ensure robust and comprehensive cybersecurity measures. Our analysis of these automotive-related vulnerabilities underscores these issues, with **supply chain vulnerabilities** ranking as the top threat, at 1,564 cases. This highlights the complexity of securing an interconnected network of suppliers and third parties.

Third-party integration risks follow as the second most prevalent threat, with 308 instances. This is largely due to the increasing reliance on external ecosystems — such as charging networks, smart home integrations, and fleet management platforms — which widen the vehicle attack surface. Weaknesses in these APIs or systems can serve as entry points for attackers, allowing them to compromise vehicles, steal data, or disrupt operations. The rapid adoption of electric vehicles (EVs) has magnified these risks, with charging network vulnerabilities adding to the urgency of addressing them.

With 295 documented vulnerabilities, **vehicle hijacking** is a significant concern that impacts vehicle control and safety. Attackers can exploit weaknesses in SDV software to take remote control of critical vehicle functions such as steering, braking, and acceleration, posing a direct threat to passenger safety and public road security. Demonstrations of incidents involving compromised ECUs or communication channels leading to complete system takeovers highlight the severity of this threat.

Beyond these risks, the transition to advanced networking architectures, such as high-bandwidth Ethernet, introduces additional challenges. For example, improper implementation of authentication mechanisms such as MACsec or IPsec can leave network systems vulnerable to exploitation. Autonomy-specific risks are also a growing concern, as attackers can manipulate sensor data or machine learning models, causing autonomous vehicles to misinterpret their surroundings.

Decoding SDV Cybersecurity: A Four-Domain Approach to Threats

To better understand the security risks to SDVs, we have categorized them into four critical domains, each representing a distinct aspect of their architecture and functionality. These domains provide a framework for addressing the unique cybersecurity challenges that SDVs face:

- **Onboard (in-vehicle software and hardware architecture):** This refers to all systems and components within the vehicle itself, such as ECUs, infotainment systems, and ADAS technologies.

- **Offboard (build-time support and tools):** This focuses on tools and systems outside the vehicle, used to develop and maintain SDV ecosystems.
- **Cloud (cloud-driven vehicle services):** This encompasses the cloud-based infrastructure and services that support the vehicle, including those that provide real-time analytics, OTA updates, and remote management capabilities.
- **Development (development tools and processes):** This represents the foundation for building and maintaining SDV software, covering tools, workflows, and methodologies.

The breakdown of vulnerabilities by year and domain, as shown in Figure 1, provides critical insights into the evolution of security risks in SDVs. By examining this data, we can identify trends, pinpoint focus areas, and better understand the shifting threat landscape across the domains.

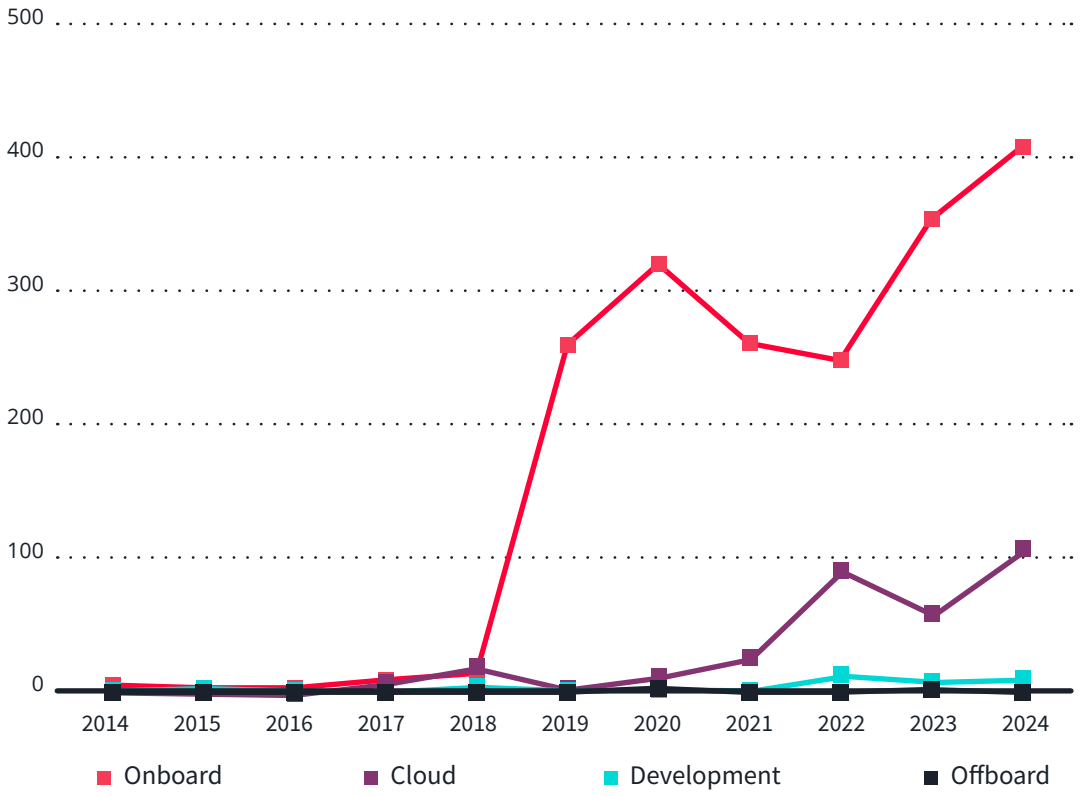

Figure 1. A comparison of vulnerabilities per SDV domain, as published from 2014 to 2024

The **onboard domain** accounts for most published vulnerabilities from the past decade (83%), driven by the increasing complexity of in-vehicle systems like ECUs, communication networks, and operating system (OS) platforms. This highlights the urgent need to implement security measures for critical vehicle functions, such as OTA updates and internal communication protocols.

The **cloud domain** has seen a significant rise in vulnerabilities in recent years, reflecting the growing dependence on cloud-based services for real-time data processing, feature deployment, and EV charging networks. This trend underscores the importance of securing cloud infrastructure and reliable vehicle-to-cloud communication.

Although the **development domain** represents a smaller share of overall vulnerabilities, risks in this area are particularly concerning. Flaws in development processes or tools can spread throughout the SDV ecosystem, emphasizing the need for secure coding practices and robust supply chain security.

Lastly, the **offboard domain**, with the lowest number of reported vulnerabilities, remains relatively secure but nevertheless requires vigilance in protecting diagnostic tools and calibration interfaces.

Building on these trends, our analysis of zero-day vulnerabilities offers deeper insights into specific system- and device-level threats. In 2024, we discovered nine zero-day vulnerabilities, which we summarize in Table 2, indicating the vulnerable system or device, threat, and SDV domain associated with each vulnerability. Notably, all but one are in the onboard domain, with critical systems like safety control, communication protocol, and head unit particularly vulnerable. Risks like third-party integration vulnerabilities and vehicle hijacking underscore the need for rigorous testing and secure integration of third-party components to safeguard these systems effectively.

Vulnerable system/device	Threat	SDV domain
Safety control system	Third-party integration risks	Onboard
Automotive booting system	Supply chain vulnerabilities	Onboard
Dongle	Third-party integration risks	Onboard
Dongle with USB interface	Third-party integration risks	Onboard
Dongle with Wi-Fi interface	Third-party integration risks	Onboard
Communication protocol	Third-party integration risks	Onboard
Head unit	Vehicle hijacking	Onboard
Automotive CPU	Supply chain vulnerabilities	Offboard
Autonomous system	Supply chain vulnerabilities	Onboard

Table 2. A summary of the nine zero-day vulnerabilities discovered by VicOne in 2024, indicating the vulnerable system or device, threat, and SDV domain associated with each vulnerability

Overall, the increasing complexity and connectivity of SDVs call for a holistic approach to security across all four domains, with this report serving as a guide in areas requiring further attention and proactive measures to mitigate emerging risks.

Future-Proofing SDVs: Predictions for the Year Ahead

Based on data from the past decade and insights from our 2024 cybersecurity threat analysis, we present the following predictions for the future of SDVs, outlining key cybersecurity events anticipated in 2025.

Supply Chain Time Bomb: Hidden Vulnerabilities Crippling SDVs

Supply chain vulnerabilities were identified as the most significant threat over the past decade, with 1,564 documented weaknesses, 279 of which were published in 2024. Historical incidents have shown how vulnerabilities in critical components such as ECUs can lead to complete vehicle safety compromises, underscoring the pivotal role of the supply chain in SDV security.

2025 Threat Prediction

Supply chain attacks will continue to increase as malicious actors exploit vulnerabilities in third-party hardware and software components integrated into SDVs.

- Attackers will leverage unpatched vulnerabilities in third-party components to orchestrate large-scale data breaches.
- Malicious code embedded during production will serve as a backdoor for future remote exploits.

Vehicles Bricked via OTA Updates

While essential for SDVs, OTA updates will remain a critical attack vector if not properly secured. Historical trends show that unauthorized or malicious updates can disrupt vehicle functionality and jeopardize user safety.

2025 Threat Prediction

Vulnerabilities in OTA mechanisms will enable attackers to deliver malicious software updates or disrupt essential update processes.

- Unauthorized OTA updates will introduce malicious firmware, rendering vehicles inoperable.
- Attackers will use malicious updates to disable critical safety functions, posing significant risks to user safety.

Cloud Under Siege: SDV Backend Systems Targeted

Over the past decade, 30 documented instances of vulnerabilities related to cloud infrastructure were identified, including two in 2024, reflecting its growing role in SDV operations. Compromises in cloud infrastructure have disrupted vehicle services, exposed sensitive data, and undermined vehicle-to-cloud communications.

2025 Threat Prediction

With SDVs increasingly relying on cloud platforms for real-time data processing and software deployment, cloud-based systems will become prime targets for cyberattacks.

- Attackers will gain control over backend cloud platforms, affecting multiple vehicles simultaneously.
- Data breaches from cloud systems will expose sensitive user data on a large scale.

Third-Party Apps Opening the Door to Cyberthreats

Third-party integration risks ranked as the second most significant threat in 2024, as 103 of the 308 documented vulnerabilities over the past decade were published just last year. Breaches through third-party systems have disrupted fleet management operations, emphasizing the need for stricter integration protocols.

2025 Threat Prediction

Reliance on third-party applications — such as smart home integrations and charging networks — will continue to present significant cybersecurity risks.

- Vulnerabilities in third-party APIs will enable attackers to gain unauthorized access to vehicle systems.
- Compromised external applications will expose users' financial and personal information.

Autonomous Deception: Manipulating the Future of Driving

Autonomous systems remain highly susceptible to sensor data manipulation, as highlighted by our 2024 analysis and historical data. Attackers have demonstrated the ability to distort sensor inputs, leading to critical misjudgments in vehicle decision-making processes.

2025 Threat Prediction

Attackers will manipulate data from cameras, lidar, and other autonomous driving sensors to mislead vehicle decision-making processes.

- Vehicles will be misdirected by falsified road signs or manipulated sensor inputs.
- Malicious actors will alter sensor data to trigger critical system malfunctions.

Ransomware on Wheels: Pay Up or Stay Locked Out

Previous incidents have shown how ransomware poses a potent threat to both individual vehicles and fleet management systems. Centralized fleet operations, reliant on interconnected systems, are particularly vulnerable to large-scale ransomware campaigns.

2025 Threat Prediction

Ransomware attacks targeting SDVs and backend management systems will increase in both frequency and sophistication.

- Attackers will lock vehicles or critical systems, demanding ransom for their restoration.
- Fleetwide ransomware attacks will disrupt logistics and ride-sharing services.

Network Takeover: Silent Sabotage Through Vehicle Ethernet Systems

Over the past decade, 27 vulnerabilities related to vehicle networking protocols were documented, with many stemming from high-bandwidth Ethernet architectures. The growing adoption of Ethernet-based communication in SDVs introduces new risks, particularly from inadequate implementation of encryption protocols such as MACsec and IPsec.

2025 Threat Prediction

As SDVs transition to Ethernet-based architectures, inadequate implementation of encryption protocols will leave systems exposed to exploitation.

- Attackers will perform man-in-the-middle (MITM) attacks to intercept or manipulate communication data.
- Network intrusions will disrupt essential vehicle control functions.

Securing the Road Ahead for SDVs

The cybersecurity landscape for SDVs is evolving rapidly, reflecting the increasing complexity, connectivity, and reliance on advanced technologies in the automotive industry. As detailed in this report, vulnerabilities in supply chains, third-party integrations, cloud systems, and autonomous operations highlight the diverse and significant risks that manufacturers, suppliers, and developers must address. A comprehensive approach to SDV security is essential, focusing on robust encryption, secure OTA mechanisms, and tighter integration protocols. Only by proactively managing these challenges can the automotive industry safeguard against potential disruptions and maintain user trust.

Looking ahead, our predictions for 2025 emphasize the urgency of addressing these vulnerabilities through innovation, collaboration, and vigilance. From securing high-bandwidth Ethernet systems to mitigating the risks of ransomware and sensor manipulation, the path forward demands a coordinated effort among stakeholders. This report serves as a guide to identifying key areas of focus and fostering the necessary collaborations to build a resilient, secure future for SDVs, ensuring that the promise of innovation is not overshadowed by preventable risks.

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