PRODUCT SECURITY ENGINEERING SERVICES FOR THE AUTOMOTIVE SECTOR

CENSUS
Cybersecurity Engineering

CONTENT

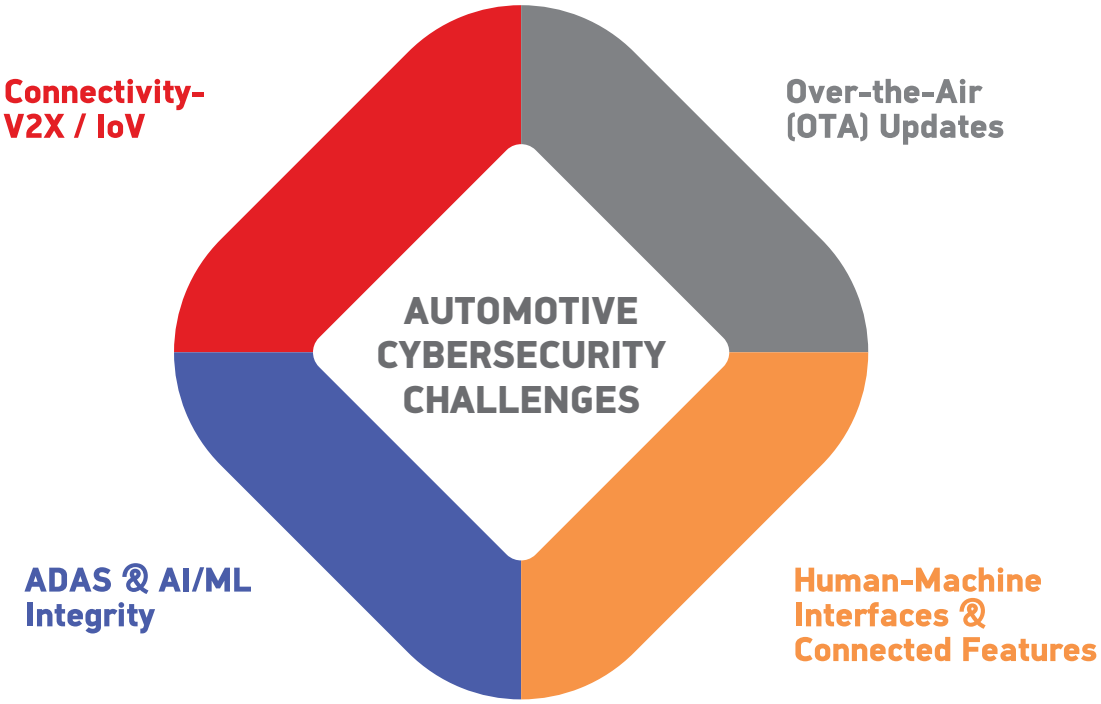
CYBERSECURITY CHALLENGES ON MODERN VEHICLES
Overview of the Automotive Cybersecurity Landscape

1. AUTOMOTIVE CYBERSECURITY LANDSCAPE

The rapid evolution of automotive technology has transformed vehicles into interconnected systems, heavily reliant on software to manage powertrain operations, safety features, navigation, and entertainment. While these advancements enhance safety and convenience, they also introduce significant cybersecurity risks. Modern vehicles now operate as part of larger ecosystems involving communication networks, cloud services, and external devices, significantly expanding their attack surfaces and increasing the risk of unauthorized access or control.

Vehicles today, including software-defined vehicles (SDVs) and AI-driven Advanced Driver-Assistance Systems (ADAS), are inherently safety-critical. Their complexity and interconnectivity demand meticulous design to address associated risks. Remote functionalities, such as smartphone-controlled access, further broaden attack vectors, exposing vehicles to high-risk threats like data breaches, vehicle hijacking, and fleet disruptions. Neglecting these challenges can lead to privacy violations, operational inefficiencies, compromised system integrity, and erosion of consumer trust.

Effectively mitigating these risks requires robust cybersecurity strategies, aligned with emerging threats and compliant with regulatory standards, to ensure secure, reliable, and trusted automotive systems.



1.1. Connectivity: Vehicle-to-Everything (V2X) and Internet-of-Vehicles (IoV)

Modern automotive connectivity—encompassing Vehicle-to-Everything (V2X), Vehicle-to-Cloud (V2C), Vehicle-to-Vehicle (V2V), and Vehicle-to-Grid (V2G)—is revolutionizing vehicles into intelligent, interconnected systems. While these advancements enhance functionality and user experience, they also introduce significant cybersecurity challenges, including the need to manage expanded attack surfaces, ensure data integrity, and safeguard critical systems.

V2X connectivity enables real-time interaction between vehicles, infrastructure, and the cloud, but it introduces significant cybersecurity challenges. These include managing the increased attack surface created by external communication gateways like Telematics Control Units (TCUs) and infotainment systems, which are often targeted as entry points for adversaries. The integration of mixed-criticality workloads in central compute architectures amplifies the complexity of securing these systems, necessitating advanced protections such as virtualization, process isolation, and hardware-backed cryptographic mechanisms. Additionally, the reliance on Cloud APIs and communication protocols demands robust encryption, lifecycle management, and continuous monitoring to protect sensitive data and ensure resilience in the face of evolving threats.

Beyond V2X, V2C communications require robust encryption, secure API management, and resilient network designs to protect sensitive data and enable reliable fleet management. Similarly, V2V communications depend on secure authentication, data integrity, and effective key management to defend against spoofing, denial-of-service (DoS) attacks, and system disruptions.

V2G connectivity presents unique challenges at charging port interfaces, where attackers could exploit vulnerabilities to gain unauthorized access to vehicle systems or manipulate billing data. Effective mitigation strategies include implementing secure communication protocols, deploying physical security measures, and adhering to stringent industry standards. Together, these measures form a comprehensive approach to safeguarding modern vehicle ecosystems against evolving cybersecurity threats.

1.2. Over-the-Air (OTA) Updates

OTA updates have revolutionized automotive technology by enabling vehicles to receive software upgrades remotely, transforming them into dynamic, software-defined systems. However, this advancement introduces significant cybersecurity challenges, particularly for safety-critical subsystems.

Cyberattacks targeting OTA updates can exploit vulnerabilities at multiple stages, including manipulating firmware in backend storage, tampering with updates during transmission, or compromising in-vehicle processing. Weaknesses in verification mechanisms may allow adversaries to bypass security checks, inject malicious code, or revert systems to older, insecure firmware versions, posing severe risks to vehicle safety and functionality.

Addressing these challenges requires advanced authentication protocols, comprehensive integrity verification, and robust mechanisms to prevent rollbacks to vulnerable firmware versions. Additionally, securing the update delivery process against tampering and denial-of-service (DoS) attacks, along with enforcing secure boot protocols and strengthening the supply chain, is essential. As vehicles increasingly rely on continuous software updates, these measures are critical to ensuring system reliability, user safety, and trust in the evolving automotive ecosystem.

1.3. Advanced Driver Assistance Systems (ADAS) & AI/ML Integrity

Advanced Driver Assistance Systems (ADAS) and autonomous driving technologies are revolutionizing road safety and transportation efficiency. These safety-critical systems control essential vehicle functions, such as steering, acceleration, and braking, using real-time sensor data and decision-making models. Hosted on centralized compute systems, ADAS integrates high-performance ECUs, cameras, radar, and lidar to enable advanced driving features. However, this extensive integration also introduces potential vulnerabilities to cyber-attacks.

As vehicle architectures transition to centralized and heterogeneous computing, mixed-criticality systems with varying safety and security requirements coexist within shared computational units. This convergence increases the risk of adversaries exploiting telematics or head units to compromise safety-critical subsystems. Ensuring system integrity and availability requires robust isolation mechanisms, strict resource control, and protection against hardware vulnerabilities, such as side-channel attacks.

The security of AI models powering ADAS is paramount, as these systems play a critical role in enabling safe and reliable vehicle operation. Adversarial attacks, data tampering, or model corruption can compromise the integrity of decision-making processes, resulting in potentially dangerous driving scenarios. To address these risks, robust security strategies must include secure communication channels, advanced model verification methods, and regular updates to safeguard against tampering. Given the dynamic nature of AI technologies, traditional firmware protections are insufficient. Instead, specialized safeguards must be implemented to ensure the integrity, resilience, and trustworthiness of AI models in real-world conditions.

Comprehensive security measures, including secure data processing, effective system isolation, and scalable hardware-backed protections, are essential to safeguard ADAS and autonomoussystems. These strategies help prevent unauthorized access, data corruption, and system manipulation, ensuring resilience, safety, and sustained trust in these transformative technologies.

1.4. Human-Machine Interfaces and Connected Features

Modern vehicles are equipped with advanced user-facing features such as infotainment systems, remote supervisory controls, and smart key technologies, which enhance convenience and user experience but also introduce significant cybersecurity risks by expanding the attack surface. Infotainment systems provide access to entertainment, navigation, and connectivity through interfaces like Wi-Fi, Bluetooth, and cellular networks, making them frequent targets for adversaries seeking to exploit vulnerabilities in communication stacks or third-party applications. Human-Machine Interfaces (HMIs), including touchscreens and voice controls, add further risks, as attackers can exploit software flaws to access sensitive data or compromise vehicle functions. A successful compromise of these systems can escalate attacks to critical components such as the Controller Area Network (CAN) bus or Advanced Driver-Assistance Systems (ADAS), potentially threatening vehicle safety.

Remote supervisory controls, such as engine start and unlocking features, rely on cloud- connected applications, making them vulnerable to API exploitation. Weak or missing authentication mechanisms can allow unauthorized access to sensitive functions or data, including real-time vehicle locations and driver identities. Compromising these interfaces may provide attackers with a foothold to target other in-vehicle systems, amplifying risks across the vehicle's ecosystem.

Smart key technologies—including Near Field Communication (NFC), Bluetooth, and smartphone integration—offer convenience but remain susceptible to proximity-based attacks. Adversaries can bypass authentication protocols or manipulate signals to gain unauthorized physical access to the vehicle. These interconnected systems, while enhancing functionality, demand robust security measures such as advanced authentication, encryption, and software integrity checks to mitigate risks and safeguard against unauthorized access or tampering.

2. CENSUS SERVICES: COMPREHENSIVE SOLUTIONS FOR EMERGING CHALLENGES

CENSUS delivers advanced security consulting and engineering services tailored to the evolving challenges of modern automotive systems. By embedding innovation, rigorous research, and engineering-driven methodologies, we provide end-to-end solutions for securing vehicle ecosystems, aligning with global standards while addressing emerging threats.

2.1. Security Foundations Consulting

CENSUS delivers innovative, secure solutions for modern automotive systems by bridging high-level security programs with actionable engineering strategies. Through our **Requirements Engineering** and **Technology Maturity Analysis**, we align with global standards like UNECE WP.29 and ISO/SAE 21434 to translate security objectives into robust, adaptable designs while evaluating the readiness of cutting-edge technologies.

Our expertise spans OTA update integrity, ensuring secure mechanisms that resist tampering and rollback attacks, and AI/ML model protection, safeguarding critical ADAS and autonomous systems against adversarial interference. By leveraging hypervisor-based isolation and secure virtualization, we enable robust multi-tenant systems, while V2X secure communications and edge computing frameworks ensure data integrity, scalability, and resilience in connected vehicle ecosystems.

Through advanced **Security Architecture Blueprints**, we provide modular, reusable solutions that integrate cutting-edge innovations like confidential computing and decentralized trust models. These designs emphasize compliance, lifecycle adaptability, and readiness to address emerging threats, empowering OEMs and suppliers to build future-proof, resilient automotive platforms.

2.2. Architecting and Enhancing Secure Automotive Systems

Architecture & Design Engineering (ADE) focuses on embedding security throughout every layer of automotive systems to ensure robust protection against emerging threats. By integrating advanced techniques such as virtualization, hardware-backed cryptography, and edge confidential computing, we develop scalable systems aligned with modern zero-trust security models. Our design methodology incorporates proactive enhancements, ensuring systems remain resilient through real-time protection of critical components, secure V2X communication, and defense-in-depth strategies. These solutions meet regulatory standards while addressing emerging cybersecurity risks and ensuring safe operation across complex, interconnected systems like software-defined vehicles (SDVs).

We prioritize a comprehensive, engineering-driven approach to threat modeling and security design. Through detailed profiling of a vehicle's attack surface, we identify applicable vectors across hardware, software, and communication channels, implementing targeted risk mitigations. Our proactive strategies include enhancing access controls, isolating critical systems, and embedding defense-in-depth measures. By leveraging technologies such as post-quantum cryptography, zero-trust models, and confidential computing, we ensure vehicles are adaptable to evolving threats. Our holistic approach strengthens system security, enabling vehicles tomaintain long-term resilience, comply with regulatory standards, and meet the demands of both regulators and consumers.

2.3. Comprehensive Security Testing and Assessment

The Security Posture Assessment (SPA) provides a comprehensive evaluation of automotive systems, ensuring they are resilient against evolving cybersecurity threats. Using a 360-degree methodology, our service thoroughly assesses every layer of the vehicle ecosystem, from silicon to cloud, to identify vulnerabilities and validate system robustness. The assessment includes extensive testing across hardware, software, and communication channels, evaluating critical components such as Electronic Control Units (ECUs), Over-the-Air (OTA) update mechanisms, and Vehicle-to-Everything (V2X) and Vehicle-to-Grid (V2G) communication systems for vulnerabilities, tampering resistance, and operational disruptions.

In addition to identifying vulnerabilities, the assessment includes targeted testing of key subsystems and interfaces such as infotainment systems, smart key features, and cloud-backend infrastructure. Compliance with global standards like UNECE WP.29 and ISO/SAE 21434 is ensured through regulatory audits, providing actionable insights for certification. The comprehensive Security Posture Assessment offers proactive vulnerability identification, tailored security enhancements, and validation of layered security measures, empowering stakeholders to strengthen defenses, ensure regulatory compliance, and build resilient, future-ready automotive systems.

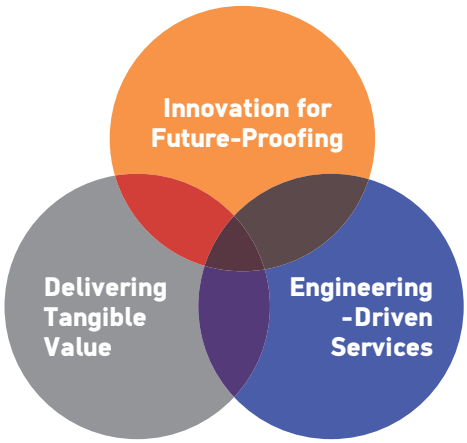
2.4. Applied Research and Future-Ready Solutions

Addressing the dynamic challenges of automotive cybersecurity requires a forward-looking approach rooted in cutting-edge research and advanced engineering principles. By exploring emerging technologies like post-quantum cryptography, confidential computing, and Trusted Execution Environments (TEEs), vehicle ecosystems are equipped with robust defenses against future threats. These innovations safeguard sensitive data, ensure the integrity of critical processes, and protect communication channels against quantum-era vulnerabilities and unauthorized tampering. Additionally, security controls are hardened through measures such as ECU exploitation protection and white-box cryptography, reinforcing the resilience of systems even in exposed environments.

Applied research drives the development of next-generation security features tailored to meet the unique demands of connected and autonomous vehicles. Innovations like AI/ML model integrity validation and hardware-backed attestation enhance the reliability of critical systems, ensuring robustness against adversarial manipulation. By proactively mitigating threats and aligning with domain-specific needs, these solutions future-proof vehicle architectures against evolving risks. This comprehensive approach empowers OEMs and stakeholders to deliver secure, trustworthy automotive experiences, meeting the expectations of an advancing industry while addressing regulatory and consumer demands.

3. CENSUS: YOUR TRUSTED PARTNER IN AUTOMOTIVE CYBERSECURITY

CENSUS stands out as a trusted partner for addressing the complex cybersecurity needs of the automotive industry. By combining in-depth expertise, innovative engineering, and a comprehensive approach, CENSUS delivers solutions that empower OEMs, suppliers, and integrators to build secure, resilient, and future-ready vehicle systems.



3.1. Unparalleled Domain Expertise

CENSUS brings extensive expertise in addressing the unique cybersecurity challenges of the automotive sector, covering critical areas such as secure communication, OTA updates, V2X protocols, and ADAS systems. With a deep understanding of global regulatory frameworks like UNECE WP.29 and ISO/SAE 21434, CENSUS ensures that solutions not only meet compliance requirements but also foster innovation. This proficiency extends to mitigating emerging threats across the entire automotive ecosystem, including in-vehicle networks, edge computing platforms, cloud backends, and connected infrastructure, enabling resilient and future-ready vehicle systems.

3.2. Engineering-Driven Innovation

Our services adopt a practical, hands-on approach to automotive cybersecurity, integrating advanced security techniques such as hypervisor-based isolation, confidential computing, and hardware-backed cryptography. Solutions are tailored to meet the complex demands of modern software-defined vehicles (SDVs) and mixed-criticality systems, ensuring robust protection while maintaining optimal performance. With a focus on future-proofing vehicle security, CENSUS proactively incorporates forward-looking technologies, including AI/ML integrityvalidation and advanced cryptographic methods, to address evolving threats and safeguard against emerging vulnerabilities.

3.3. Comprehensive End-to-End Support

CENSUS provides comprehensive end-to-end support throughout the entire product lifecycle, from initial design and development to post-market updates. Our holistic approach includes services such as requirements engineering, technology maturity analysis, security architecture development, and security posture assessments. With a focus on lifecycle security management, we implement strategies for continuous updates, telemetry monitoring, and adaptive defenses, ensuring that systems remain resilient and aligned with evolving cybersecurity threats.

3.4. Value-Driven Partner for Automotive Security

CENSUS fosters a collaborative engagement model, seamlessly integrating with client teams to provide expert support without disrupting workflows or timelines. Our resilient and scalable solutions are designed to address immediate needs through modular and reusable designs while remaining adaptable to future challenges and market demands. Backed by a proven track record, CENSUS consistently delivers precision, innovation, and reliability in tackling domain-specific challenges, earning trust across the automotive cybersecurity landscape.

> Choosing CENSUS for automotive cybersecurity means investing in a **partner** that not only ensures **compliance** but also drives **innovation**, enabling secure vehicle ecosystems that meet the **demands of today and tomorrow**.

USA
607 Boylston Street,
Suite 165L, Boston, MA 02116
T. +1 8882 029 846
E. usa@census-labs.com

UK
Unit 2.15 Barley Mow Centre
10 Barley Mow Passage
W4 4PH, London
T. +44 1293 324 069
E. uk@census-labs.com

EUROPE
128 A. Siggrou Ave.,
Athens 117 45, Greece
T. +30 210 220 8989-90
E. eu@census-labs.com

ABU DHABI
Office 110 - First Floor
Incubator Building
Masdar City, Abu Dhabi
United Arab Emirates
T. +971 8003 110 047
E. uae@census-labs.com

DUBAI
Unit GA-00-SZ-L1-RT-201, Level 1
Gate Avenue - South Zone
Dubai International Financial Centre
Dubai, United Arab Emirates
T. +971 8003 110 047
E. uae@census-labs.com

www.census-labs.com