Automotive iQ

AUTOMOTIVE CYBERSECURITY
DETROIT 2024

FACT FILE: AUTOMOTIVE CYBERSECURITY RISKS & CHALLENGES IN 2024

1.
The Impact of AI on Automotive Cybersecurity

2.
Cyber Regulations: A Shifting Compliance Landscape

3.
New Cybersecurity Challenges of Software-Defined Vehicles

#AUTOCYBERSEC24

Visit Site

Register to Attend

FACT FILE: AUTOMOTIVE CYBERSECURITY RISKS & CHALLENGES IN 2024

Cybersecurity threats are not static; it's a dynamic environment that's ever-changing. Every day, there is a new potential threat, and while technology is becoming more sophisticated, so are threat actors with new security dangers emerging constantly, making cybersecurity not only valuable but essential for the automotive industry.

At the same time, the regulatory landscape is presenting further challenges. Last year, ISO/SAE 21434 was new and automotive companies were trying to figure out what it meant; OEMs are now implementing and responding to it. There is now a June/July 2024 deadline by which pretty much all vehicles impacted by UN ECE R155/R156 will need to be compliant.

There is a lot of fear and uncertainty around how security in the automotive industry will be impacted by artificial intelligence (AI). And as AI, vehicle autonomy and connectivity increase exposure to attacks, it has never been more important to be fully aware of emerging threats and strengthen cybersecurity programs.

Reflecting on the ever-evolving environment of cybersecurity, this fact file uncovers the top risks and challenges that the automotive industry is facing in January 2024:

1. The Impact of AI on Automotive Cybersecurity
2. Cyber Regulations: A Shifting Compliance Landscape
3. New Cybersecurity Challenges of Software-Defined Vehicles

1. THE IMPACT OF AI ON AUTOMOTIVE CYBERSECURITY

As the application of artificial intelligence in the automotive industry gains momentum, and threat actors become more and more intelligent, it's never been more important to prepare for emerging cybersecurity threats and understand the risks and opportunities that AI presents for OEMs and suppliers.

General Motors is just one of the major OEMs exploring the benefits of implementing artificial intelligence into their vehicles, with the OnStar Virtual Assistant providing responses to common user enquiries as well as routing & navigation assistance.

However, Dennis Kengo Oka, Principle Automotive Security Strategist at Synopsys Software Integrity Group, says that the use of a digital assistant as part of the vehicle could be abused to run unauthorized commands or clone keys, which could lead to attackers stealing cars. These attacks are already happening; hackers are using controlled area network (CAN) injection to send fake messages that unlock access to a car's smart key receiver. It can reportedly be carried out in seconds, with the technology available to buy online.

Research into CAN-injection theft by cybersecurity expert Ian Tabor – inspired by the theft of his own car – found that vulnerabilities in the security mechanism used in the car's internal messaging system were allowing threat actors to gain easy access.

As threat actors become more intelligent, experts are warning about the security risks posed by the greater implementation of generative AI tools, and according the GM Vice President Scott Miller, "ChatGPT" is going to be in everything.[4] Chat GPT and other Large Language Models are already being abused by threat actors to create and improve malware, despite safety measures that are designed to prevent the improper use of these tools.

Generative AI tools can also be implemented to stop sophisticated hackers. For example, large language models can analyze vast amounts of data to look for anomalies, whether it be times a vehicle is normally driven, or in a vehicle's typical driving patterns. When these anomalies occur, the technology could automatically alert the owner, or shut the vehicle down.

This highlights the need for the automotive industry to mitigate generative AI security risks. There is understandable uncertainty about the power AI could give to hackers.

Research and development is crucial to finding solutions to the evolving risks and challenges of AI in cybersecurity. Reportedly more than 1.7 million patents have been filed across the automotive industry alone in the last three years for smart vehicle anti-theft technologies. And as a result, innovations are beginning to emerge. Early in 2023, Kia and Hyundai rolled out free anti-theft software updates affecting more than 8 million vehicles to stop an unprecedented rise in high-tech car thefts.

OEMs can also accelerate innovation through collaboration with suppliers. Ford has teamed up with ADT, a security systems company, to develop a vehicle security system powered by AI, known as Canopy. It uses AI-powered security cameras, a mobile app for remote monitoring and acoustic sensors, with AI used to identify and report credible threats.

Canopy has collaborated with Ambarella – experts in AI camera solutions – to implement an AI-powered chip into its camera system. This will give the system the ability to better detect threats such as tampering, while helping to power a live stream that vehicle owners can view at any time when away from their vehicle.

2. CYBERSECURITY REGULATIONS: ACHIEVING COMPLIANCE WITH ISO/SAE 21434 AND UNECE R155/R156

Hackers are not the only ones presenting cybersecurity challenges to OEMs. We are also entering an era of greater regulatory scrutiny that aims to drive better protection for consumers.

R155 and R156 – introduced by the United Nations Economic Commission for Europe (UNECE) – apply to all new vehicles, commercial or private, from July 2024.

Under R156, OEMs must implement procedures for delivering secure software updates for onboard control systems. This includes establishing a robust Software Update Management System (SUMS).

Under R155, OEMs must obtain a Cybersecurity Management System (CSMS) certification that covers all stages of a vehicle's creation including development, production and post-production. The certification must also be assessed and renewed every few years.

According to Darren Schelcusky, Senior Consultant Vehicle & Mobility Cybersecurity at Ford Motor Company, "R155/R156 is a complex regulation, and it can be difficult to understand all the requirements. The shift from moving from best practices and engineering practices to documented and auditable process and evidence to demonstrate compliance can introduce additional work products for OEMs." You can read more on Darren's insights into UNECE R155/R156 compliance here.

The unprecedented nature of the regulations is challenging, but one solution has been to collaborate with experts in cybersecurity who can bridge knowledge gaps. To help OEMs achieve certification of compliance for vehicle type approval, Continental has collaborated with cybersecurity experts at Argus to create a robust CSMS framework that will provide a blueprint for each phase of the implementation journey. Meanwhile, Ford announced in September 2023 that it has partnered with Upstream Security to support its R155 compliance efforts ahead of the impending deadlines.

A key element of R155 for OEMs is ensuring compliance across the supply chain. Weaknesses in the supply chain have led to direct cybersecurity breaches for a reported 93% of OEMs. Information sharing will be crucial to ensuring compliance, and suppliers are now signing production agreements with OEMs that incorporate and encourage R155-friendly processes.

For example, Karamba Security announced it had signed an agreement with a 'world-renowned truck OEM' to increase security in around one million of its trucks. Once implemented, Karamba's XGuard software will run continuously to detect and stop cyber-attacks, reporting the data to the OEM to help prove R155 compliance.

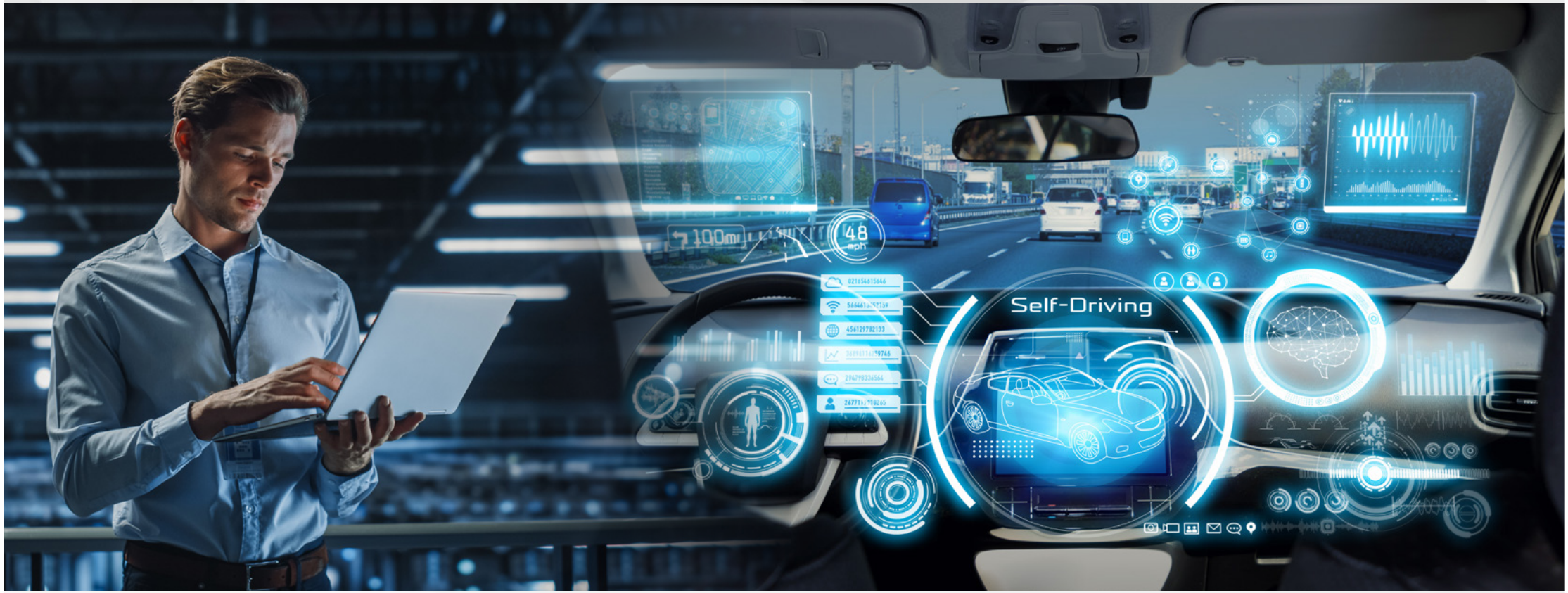
With the R155/R156 compliance deadlines fast approaching, OEMs can also look to industry standards for help. Jillian Goldberg, CRO at Guardknox, wrote in June 2023 that there are two approaches OEMs can take to achieve R155 compliance. These are: "Define, implement, and follow a proprietary cybersecurity method that makes sure they meet the specific UNECE R155 requirements, or adopt ISO/SAE 21434 which covers all the processes required by the OEM to comply to UNECE R155."[14]

NXP's Timo van Roermund said in August 2022: "UN R155 and ISO/SAE are complementary and together they prescribe the requirements for cybersecurity in future vehicles."[15]

Understanding of these regulations is growing across the industry, with the likes of Continental achieving compliance with ISO/SAE 21434 in May 2023.[16] Yutong announced in April 2023 that it was the first in the Chinese commercial vehicle industry to obtain CSMS certification under R155.[17]

Suppliers are also playing their part by becoming compliant. HARMAN, for example, announced in October 2023 it had achieved ISO/SAE 21434 compliance, and says it is well-placed to support OEMs with R155 compliance.[18]

While the battle for ISO/SAE compliance is ending soon, this is only the first version of the standard, and will be amended, updated and changed in the next 12-18 months as the cybersecurity landscape continues to evolve.



3. NEW CYBERSECURITY CHALLENGES OF SOFTWARE-DEFINED VEHICLES

Software-Defined Vehicles (SDV) will transform the work of engineers, as well as the industry's understanding of collaboration and supplier relationships. Volvo, for instance, has collaborated with Google to offer its personal assistant, maps, and entertainment systems as standard in its vehicles.[19] These kinds of relationships will become more expected as SDVs are adopted on a greater scale.

At the same time, SDVs are set to fundamentally change the role of cybersecurity engineers in the automotive space. For example, SDVs are driving a shift from ECU-based architecture towards one built around high-performance computers (HPCs), which are powerful enough to meet the vehicle's more complex demands. It changes the landscape for cybersecurity engineers who must be able to manage risks around SDV features, such as enhanced drivervehicle communication and continuous software updates.[20]

In March 2023, Alois Kliner, VP Automotive & IoT Manufacturing, Utimaco, said this is exactly why regulations such as ISO/SAE 21434 and UN R155 has been devised. He cited examples of the kinds of systems that will become essential to security teams in the SDV era. These include:

- → **Key management**
- → **Over the Air (OTA) updates for components**
- → **Asymmetric encryption for in-car communication**
- → **Device attestation[21]**

New approaches to security must be in line with how vehicles are evolving, as they move further away from traditional vehicle architecture and become more aligned with the Internet of Things (IoT) and arguably more like a personal device, such as a smartphone.

There are endless opportunities for OEMs in a world where a car owner can continuously update and add services to their vehicle. But with those opportunities come inevitable security challenges.

As such, Francesca Forestieri, Automotive Lead at GlobalPlatform, believes the user's role in the security process is set to become of increased importance. "If the user's data isn't protected appropriately and proper caution isn't exercised when downloading services and applications, the user can be a direct or indirect risk to vehicle security," she said in November 2023.[22]

However, this doesn't mean that OEMs and suppliers have less responsibilities with SDVs, simply that their responsibilities will change or evolve.

As OEMs embrace software-defined architectures, their cybersecurity strategies will have to keep pace and evolve to stay aligned with developments in the SDV market. Adopting zero-trust principles – which remove assumed trust in users or devices and require authentication with every connection – could help cybersecurity engineers to enhance SDV security.

Zero-trust security components can be deployed by OEMs across not just software, but also data and networks, hardware, and electronic architecture. For example, an Intrusion Detection System can inspect network traffic throughout a vehicle to ensure endto-end communications are secure. Meanwhile, software can be protected with methods such as code reviews and penetration testing.

NAVIGATING UNCERTAINTY IN A COMPLEX INDUSTRY

Cybersecurity is an ever-evolving space; what was relevant in 2023 might not be relevant in 2024. However, while the landscape may be uncertain, we know that staying on top of regulatory compliance and cybersecurity challenges will be crucial.

The topics covered in this report will be explored extensively at the **14th Annual Automotive Cybersecurity Detroit 2024**. Automotive IQ is inviting industry professionals that are in charge of making decision and implementing strategies to the conference, with the objective of exposing you to new ideas and concepts, industry best practices and use cases, and networking opportunities with OEMs, Tier-1s and suppliers of new technologies.

This year's event addresses the dynamic environment of cybersecurity threats, exploring the strategies and technologies for compliance, cybersecurity of the connected car, protecting autonomous and software-defined vehicles from cybersecurity threats, and what's expected from future iterations of ISO/SAE 21434. In addition, the event takes a deep dive into AI technology for automotive cybersecurity – giving attendees the opportunity to discuss the possibilities of AI, including Generative AI tools, quantum computing & machine learning.

WHAT TO EXPECT AT AUTOMOTIVE IQ'S CYBERSECURITY DETROIT CONFERENCE

50+ Speakers
Experts from leading OEMs, Tier-1s, and suppliers of new technologies

250+ Attendees
Senior Directors, VPs, Lead & Technical Engineers from Cybersecurity, Vehicle Connectivity, and Artificial Intelligence

20+ Event Partners
Showcasing the Latest Cybersecurity Technologies, Solutions & Services

45+ Hours of Content
Technical Presentations, Panel & Roundtable Discussions, Fireside Chats & More

Women in Automotive Breakfast
Open to All Attendees

#AUTOCYBERSEC24

Visit Site

Register to Attend

Automotive IQ's 14th Annual

AUTOMOTIVE CYBERSECURITY DETROIT 2024

March 19 – 21, 2024 • **Sheraton Ann Arbor Hotel, Michigan**

Steven Wicks, Editor, Automotive IQ

Endnotes

1 xxxxxx

2 VICE, 2023 – https://www.vice.com/en/article/v7beyj/car-thieves-tech-hidden-old-nokia-phones-bluetooth-speakers-emergency-engine-start-keyless

3 Hackread, 2023 – https://www.hackread.com/thieves-use-can-injection-steal-cars/

4 Just Auto, 2023 – https://www.just-auto.com/data-insights/innovators-cybersecurity-smart-vehicle-anti-theft-automotive/?cf-view

5 The Verge, 2023 – https://www.theverge.com/2023/2/14/23599300/hyundai-kia-car-theft-software-update-free-tiktok-challenge

6 Ford, 2022 – https://media.ford.com/content/fordmedia/fna/us/en/news/2022/01/18/ford-and-adt.html

7 New Electronics, 2023 – https://www.newelectronics.co.uk/content/news/ambarella-s-edge-ai-soc-selected-for-intelligent-vehicle-security-system/

8 Solwit, 2023 – https://solwit.com/en/blog/r155-r156-a-quick-guide-to-the-updated-cybersecurity-regulations-for-automotive/

9 TUV SUD, 2023 – https://www.tuvsud.com/en-gb/industries/mobility-and-automotive/automotive-and-oem/autonomous-driving/automotive-cybersecurity-management-system-assessment

10 Continental, 2023 – https://www.continental-automotive.com/en/news/2023/csms-implementation-approach.html

11 Telematics Wire, 2023 – https://www.telematicswire.net/ford-teams-up-with-upstream-to-secure-connected-trucks/

12 Deloitte, 2023 – https://www2.deloitte.com/content/dam/Deloitte/de/Documents/risk/Deloitte-Automotive-Cyber-Security-EN.pdf

13 Globe Newswire, 2023 – https://www.globenewswire.com/en/news-release/2023/05/24/2675068/0/en/Karamba-Security-Announces-Production-Agreement-to-Secure-One-Million-Trucks.html

14 Guardknox, 2023 – https://blog.guardknox.com/unece-r155-a-guide-for-oems-part-2

15 NXP, 2022 – https://www.nxp.com/company/blog/heres-how-the-auto-industry-is-taking-cybersecurity-seriously:BL-THE-AUTO-INDUSTRY-IS-TAKING-CYBERSECURITY

16 Continental, 2023 – https://www.continental-automotive.com/en/news/2023/automotive-cyber-security-tightened.html

17 Bus News, 2023 – https://bus-news.com/yutong-obtains-certification-on-un-r155-csms-compliance/

18 HARMAN, 2023 – https://news.harman.com/releases/harman-bolsters-its-automotive-cybersecurity-program-with-new-certification

19 Volvo, 2023 – https://www.volvocars.com/intl/v/connectivity/infotainment-page

20 Continental, 2023 – https://www.continental-automotive.com/en/solutions/smart-e-e-architecture/high-performance-computers.html#accordion-7de3cbe937-item-9206fc14b0

21 Fleet World, 2023 – https://fleetworld.co.uk/comment-software-defined-vehicles-and-the-future-of-automotive-security/

22 Wards Auto, 2023 – https://www.wardsauto.com/industry-news/sdvs-greater-connectivity-equals-greater-cybersecurity-risk