The past and next decade of automotive cybersecurity

André Weimerskirch
Block Harbor Cybersecurity
andre@blockharbor.io

August 2025

1 Introduction

I began working on embedded systems cybersecurity in 2002. My very first project involved designing a secure feature activation system for navigation maps for an automotive supplier. In 2002, navigation maps were provided on CDs, and automotive navigation systems were quite expensive. The supplier had the idea to allow customers to purchase navigation services for a limited area and time period. This required robust cybersecurity to protect the business model. My customer was not the first to have this idea, so my colleagues and I examined a competitor who already had such a system in the market to find vulnerabilities and activate their maps without payment. (We disclosed the vulnerability and received a lawsuit threat in response if we ever discussed it publicly.) More than 20 years later, we have a space that is heavily regulated and moderately mature, and companies are more likely than not to threaten with a lawsuit after a vulnerability disclosure. Passenger vehicles are still regularly compromised to undermine business models and facilitate theft, but we have never experienced a breach that endangers safety (we have only learned about research results that demonstrate such breaches are possible). About 10 years ago, this space underwent a significant pivot, generating hype that resulted in today's regulations, standards, and stakeholder readiness. I believe we are at the point of another pivot towards a new path that will have a major impact on our community.

2 The Last Decade: From Zero to Hero

Automotive cybersecurity began to gain traction around 2010 when a research team from UC San Diego and the University of Washington analyzed passenger vehicle security [1] and demonstrated in 2011 that it was possible to compromise vehicles in various ways, including remote attacks over cellular connections [2]. Miller and Valasek repeated this feat in 2014 [3] and 2015 [4], truly kickstarting the push toward enhanced vehicle cybersecurity. This led to an avalanche of change as government agencies pushed for regulation, corporate boards became concerned about liability, and corporations worried about losing end-consumers and customers. Consequently, corporations acted quickly, either acquiring automotive security startups or hiring security experts to rapidly build teams and expertise while significantly improving vehicle and component security in a short timeframe. Many corporations included cybersecurity leaders at the executive level (Vice President), with these leaders regularly reporting to the board. Simultaneously, companies pushed forward the establishment of an information-sharing entity (Auto-ISAC) and the creation of automotive product cybersecurity standard ISO/SAE 21434. Additionally, countries under the UN ECE umbrella for type approval (homologation) defined UN ECE Regulation No. 155 to require evidence of proper cybersecurity as part of type approval.

3 Today: Compliance, Overshot, and Cash Crunch

Today, we have a mature standard, ISO/SAE 21434 [5] that most global corporations have mastered. Corporations have established governance, processes, and teams that conform to the standard, which means that they have also largely mastered type approval and UN ECE R155. In fact, many industry stakeholders are learning that they are far ahead of auditors, that passing security audits is surprisingly easy, and that they probably overshot the target. Naturally, this will lead car manufacturers and suppliers to reduce effort and requirements for suppliers. Extensive security research has been and continues to be conducted in this space, with many research results discovered and published. Much of this research reveals highly critical vulnerabilities and exploits, such as attacks that would allow an attacker to unlock doors or start engines across an entire vehicle fleet, and attacks that would enable manipulation of vehicle driving behavior, thus compromising safety. However, no such attacks have ever been reported in the field, and real-world attacks continue to be limited to undermining theft protection (to steal vehicles and modules) and undermining business models (such as chip tuning to modify vehicle driving behavior). The apparent reason we have not seen wide-scale or safety-critical attacks in the field seems to be the lack of attacker incentive—perhaps because equally difficult attacks in other industries, such as finance, result in much higher financial gains, or because endangering safety could lead to much harsher law enforcement responses. For about two years, the industry has been under cost pressure, which has intensified recently. Considering the overall picture, it seems logical to reduce cybersecurity expenses and teams, decrease the time product security updates receive during board meetings, lay off cybersecurity executives and experts, and move positions to lower-cost countries. Corporations are also reducing non-labor expenses such as leaving security associations and cutting back on sponsored research. I often hear comments about companies not only targeting ISO/SAE 21434 conformance and type approval but going above and beyond. I also frequently hear criticism that car manufacturers and suppliers are unwilling to pursue ”true” security and instead only target ISO/SAE 21434 conformance. I think both views reflect a misunderstanding of ISO/SAE 21434 and stakeholder objectives. I believe there are two aspects at play for stakeholders: (1) protecting their interests, such as revenue, profit, and protection against liability claims, and (2) protecting end-consumers and broader society's interests. An example of #1 is that a car manufacturer needs to protect a feature activation mechanism to safeguard revenue. An example of #2 is that a car manufacturer needs to protect vehicles against data extraction that could lead to privacy violations. ISO/SAE 21434 is designed so that outcomes for both areas are sufficient—namely, that mitigations are in place to reduce residual risk to acceptable levels for both stakeholders and society. The standard is built around the concept of Threat Analysis and Risk Assessment (TARA), which pursues exactly this: reducing risk to acceptable levels. Therefore, meeting the ISO/SAE 21434 target is sufficient. If you find that security is not at an appropriate level, I would argue that the implementer did not properly follow ISO/SAE 21434 and/or lacks proper security experience to perform a sound TARA. My experience shows that while security controls and process rigor are sometimes too low, they are frequently too high, with deeply embedded modules like seating modules featuring surprisingly sophisticated and expensive security controls. A recent development is that the US government is taking steps to protect connected and automated vehicles against nation-state attackers. A recent Department of Commerce regulation addresses national security concerns and prohibits hardware and software integrated into vehicle connectivity systems, as well as software integrated into automated driving systems, that are ”designed, developed, manufactured, or supplied by” entities under the control or jurisdiction of ”foreign adversaries”—namely China and Russia [6]. While this could be labeled a supply chain topic, many industry stakeholders address it under cybersecurity. This makes sense since the natural approach to satisfying this regulation directly relates to hardware and software bill of materials (BOM) which were particularly pushed over the last years by cybersecurity teams and organizations as means to improve cybersecurity. It also makes sense because only cybersecurity teams can fully analyze the impact of affected hardware and software.

4 The Future: Cybersecurity as Commodity

I see two clear trends that will become more apparent over the next decade: (1) Cybersecurity will become a topic where financial return on investment is measured, and (2) companies will increasingly have to deal with, and probably struggle with, a growing number of regulations. I also expect that the number of regulations to follow and the risk of failing type approval will continue to grow. Simultaneously, car manufacturers will increasingly feel the burden of maintaining cybersecurity for a growing number of long-lived vehicle platforms. Additionally, we will likely begin seeing private corporations having to consider nation-state attackers who compromise entire fleets without ”pulling the trigger." In fact, I predict researchers will start finding traces of successfully placed backdoors within the next 10 years, after which the government will push car manufacturers to significantly increase their security thresholds. While this could lead to an investment push and reverse the outlined trend, I believe that it will lead to a speed-up of the outlined trend since this threat is abstract and not a direct threat around a company's liability. I believe we will see cybersecurity shift toward becoming a commodity with a clear focus on financial value and return-of-investment rather than an area for advertising. This means car manufacturers will likely reduce expenses for public demonstration of security expertise and focus on tangible returns on their investments. This could also mean that the support for collaborative efforts will be further reduced. Altogether, I predict we will see a race to minimize costs while administrative complexity to meet all regulations explodes. The combination of cost pressure and increased complexity could mean companies need to invest more in automation and tools to handle this complexity level. I also expect continued replacement of current cybersecurity executives. The leaders who built current capable teams will find it difficult to shift direction from excellence toward low-cost solutions and compliance. This will require new leaders who are not emotionally invested in the history of building current teams, who understand utilizing automation, tools, and AI to reduce costs, and who understand how to grow and retain teams in lower-cost countries. I have had discussions for almost a decade about whether it makes sense to build larger dedicated cybersecurity teams or whether expertise should be embedded and integrated into development teams (systems, hardware, and software developers). Note that this is mainly how functional safety is handled today: Originally, companies established specialized functional safety teams to manage new ISO 26262 standard requirements, and over a decade, development teams absorbed the expertise. So far, I have believed that cybersecurity is different and that the functional safety model will not work for cybersecurity since cybersecurity is quite fluid and constantly evolving. On the other hand, we are beginning to see companies attempting to reduce security team sizes and integrate expertise into existing development teams. Time will tell how this works out. I still believe the functional safety model will not work, but I suspect a model supported by powerful tools could work. For instance, a tool could provide the newest research and vulnerability results to each developer, enabling the developer to focus on development rather than staying current with threats. Nonetheless, I expect continued efforts to shift much of the work from expensive cybersecurity experts in high-cost countries to engineers in lower-cost countries. In fact, I expect the number of dedicated cybersecurity experts to be significantly reduced, with development engineers taking on cybersecurity expert tasks. For instance, TARAs will no longer be created by cybersecurity experts but by systems, hardware, and software engineers under cybersecurity expert supervision and hence allowing one cybersecurity expert to supervise multiple programs.

5 Conclusions

We are currently at a pivotal moment, with many companies facing challenging financial situations. This comes at a time when the only visible security breaches by malicious actors involve vehicle theft and undermining business models, but not safety. We don't know if this is due to lack of attacker motivation, effective security efforts, or both. Meanwhile, it is becoming clear that many stakeholders are either reducing team sizes or moving resources to lower-cost countries to reduce expenses. We are also seeing the first indications that car manufacturers are reducing efforts around demonstrating leadership in this topic while focusing on actual value propositions. The future can unfold in many ways, and we have outlined what we feel is most likely. Of course, this could go in many different directions—all it would take is a serious incident or the discovery of dormant nation-state malware in a fleet tomorrow.

References

[1] K. Koscher, A. Czeskis, F. Roesner, S. Patel, T. Kohno, S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, and S. Savage, "Experimental Security Analysis of a Modern Automobile", IEEE Symposium on Security and Privacy, Oakland, CA, May 16-19, 2010.

[2] S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, S. Savage, K. Koscher, A. Czeskis, F. Roesner, and T. Kohno, "Comprehensive Experimental Analyses of Automotive Attack Surfaces", USENIX Security, August 10-12, 2011.

[3] C. Valasek and C. Miller, "A Survey of Remote Automotive Attack Surfaces", White Paper, 2014.

[4] C. Valasek and C. Miller, "Remote Exploitation of an Unaltered Passenger Vehicle", Technical White Paper, 2015.

[5] Road Vehicles - Cybersecurity Engineering ISO/SAE 21434, available at https://www.sae.org/standards/content/iso/sae21434/

[6] Department of Commerce, Bureau of Industry and Security, Securing the Information and Communications Technology and Services Supply Chain: Connected Vehicles, 15 CFR Part 791, Docket No. 250107-0005, RIN 0694-AJ56.