Automotive cybersecurity fully revealed

Unlocking opportunities by tackling key vehicle security challenges

Empowering Tomorrow's Automotive Software

www.etas.com

ETAS

Abstract

The era of isolated, self-contained vehicles with static configurations throughout their lifespan lies behind us. Today, digitalization and connectivity present new opportunities for enhanced user experience, innovation, and mobility solutions, thanks to features like internet capability, over-the-air (OTA) updates, and vehicle-to-infrastructure communication. While these advancements come with some challenges, they also open the door to the development of robust cybersecurity frameworks that strengthen vehicle reliability, protect road users, and safeguard privacy. In fact, cybersecurity is a unique opportunity to ensure the success of future business models within the mobility ecosystem.

Cybersecurity is now integral to a vehicle's lifecycle, from the development and manufacturing process to its interactions within a connected mobility network. As new features such as remote updates, smartphone integration, and seamless registration at charging stations become the norm, the focus shifts to ensuring the security of these innovations. Developers must stay ahead of potential risks, continuously fortifying the vehicle ecosystem while ensuring users enjoy the full benefit of cutting-edge technology. This ongoing evolution of security standards enhances the opportunity to innovate and optimize vehicle development.

This white paper serves as a strategic guide to navigating the dynamic world of automotive cybersecurity. It identifies the primary challenges and opportunities vehicle manufacturers are facing. It provides a holistic view spanning the entire vehicle lifecycle and landscape – from deeply embedded software (ECUs) to vehicle computers. Whether you are a traditional manufacturer or supplier or a software-driven startup, cybersecurity can provide you with a strategic advantage. By rethinking the classic development process, enormous potential for far-reaching optimizations can be uncovered. This paper also explores how development approaches like DevSecOps and the V-model can be enhanced through the application of four core security principles, offering a roadmap for a secure, innovative future in automotive software development.

Table of contents

1. Introduction

Digitalization makes vehicle use more comfortable, be it through over-the-air software updates, advanced driver assistance systems (ADAS), or an internet-capable entertainment system. It opens up new opportunities for manufacturers and suppliers to create innovation independently of mechanical progress and to offer services beyond sales, enabling a vehicle to produce revenue throughout its entire lifetime. While every major technological breakthrough brings new opportunities, the shift from purely mechanical vehicles to "computers on wheels" is a true evolution. It also comes with new challenges, especially in cybersecurity: the enormous opportunities for growth and innovation also involve the responsibility to safeguard sensitive personal data and to secure entire vehicle models from potential cyber-attacks. By proactively addressing these risks, manufacturers can build stronger, more resilient systems, setting the stage for long-term success and trust in an increasingly digital automotive landscape.

How to maintain a (digitally) secure vehicle is currently one of the main topics within the mobility sector. According to a recent market survey[1], cybersecurity risks are even perceived as the main external barrier to growth for automotive companies. This high awareness within the industry is generally positive: new risks have been recognized and approaches to address and manage them are being developed. This not only concerns OEMs. A modern vehicle is an interplay of numerous software and hardware components, both on-board and off-board, which contribute to safety from development right through to operation, provided by a global network of suppliers and software-centered companies. All players within the supply chain have the responsibility to know the threat landscape, minimize risks, comply with all necessary regulations, and contribute their part to holistic vehicle security.

The development towards stronger cybersecurity is not solely intrinsic. It also results from a series of legal regulations and standards that have been installed to provide guidance for a holistic cybersecurity concept and, first and foremost, keep road users safe. As we dive deeper into the specific threat areas, it is advantageous to take a closer look at the current regulatory landscape of automotive cybersecurity.

2. The regulatory landscape of automotive cybersecurity

Most vehicle manufacturers and suppliers sell their products in several countries or regions. As a consequence, they must also know and comply with all regulations of the markets they export their software, parts, or vehicles to. These regulations are constantly evolving, and new requirements are added in parallel with the growing cybersecurity threat landscape. In addition to legal regulations, common industry standards and best practices also play a decisive role. Adhering to these standards is highly recommended and, in some cases, may even be mandatory. Going global is therefore a complex challenge for manufacturing companies in the mobility sector; a dense jungle of evolving rules that need to be navigated, as depicted in figure 1.

For vehicle manufacturers, who want to sell their products in the 56 member states of the United Nations Economic Commission for Europe (UNECE), the legally binding UN R 155, which was published in 2021, is the most important regulation and currently encompasses passenger cars, busses, trucks and trailers. It requires the mandatory implementation of a Cyber Security Management System (CSMS) and refers to the ISO/SAE 21434 Road Vehicles – Cybersecurity Engineering standard as guideline. It may soon be expanded to include motorcycles and scooters, which will also put these sectors under pressure to work on their cybersecurity processes. China, the U.S., and India have their own laws and regulations. Hence, a vehicle model sold globally may have to meet several standards at once or come in different versions.

While the introduction of new mandatory regulations ensures a high level of safety for road users, it can also have a profound economic impact on OEMs and suppliers in the industry. Some already developed vehicle models might need to be re-engineered to comply with a new binding regulatory framework. This can lead to an entire series being discontinued or only available for certain countries, as was the case with Porsche's 718 Boxter[2] or the Volkswagen Up[3]. These examples underline that an optimal approach to cybersecurity requires flexibility and future-orientation throughout the whole organization, far beyond strict compliance with the regulatory status quo. Understanding the key cybersecurity threats is therefore essential to remaining competitive in this ever-changing landscape. However, companies don't have to navigate this complex landscape alone: experienced, internationally active partners provide the support and tools needed, so they don't have to start from scratch every time.

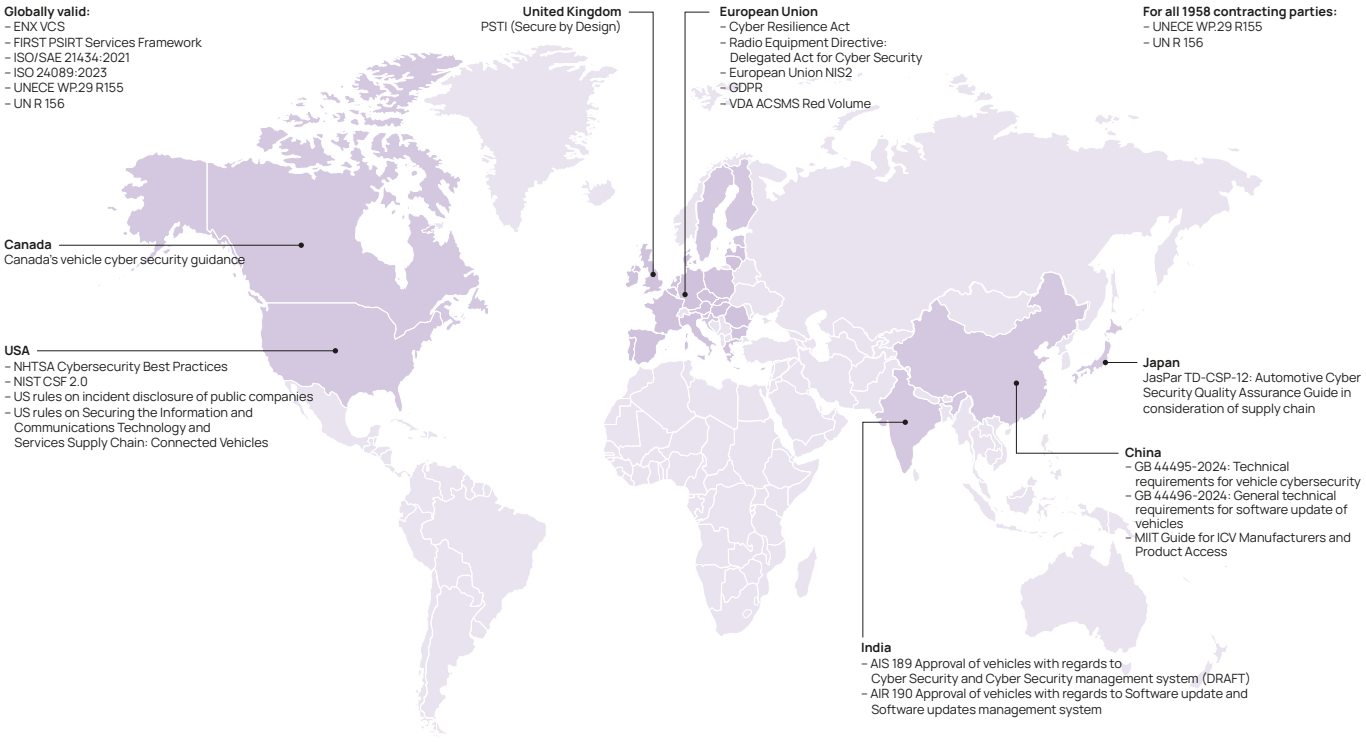

Figure 1: Cybersecurity regulations for connected devices

3. Key cybersecurity threats – an overview

As a solution provider and industry leader in automotive security with a great number of customers and use cases worldwide, ETAS always has its finger on the pulse of the automotive industry. Based on these experiences, ETAS has identified three key threat areas: vulnerabilities and risks on component/architecture level, risks and cybersecurity challenges caused by a complex supply chain and after-sales services, and challenges from a growing ecosystem. Manufacturers and suppliers must be aware of these threats and address them early in the process, as they are crucial in paving the way towards holistic cybersecurity in the final product.

THREAT #1

3.1 Software vulnerabilities on component/architecture level

Let's start with ECUs, the secret workforce of each vehicle, responsible for basic yet safety-critical functionalities. Up to 150 of these units in a single vehicle monitor and control engine performance, emissions, transmission and braking systems, thanks to their unmatched ability of real-time operations. They react instantly to input, ensuring driver safety under all circumstances. Consequently, these crucial components will remain an important part of future E/E architectures despite the shift towards the software-defined vehicle (SDV).

As ECUs are involved in safety-relevant processes in the vehicle, the possibility to alter them externally through different, permanently evolving methods entails new risks: from hijacking the whole car functions via an external CAN-Bus access to taking advantage of poorly programmed authentication processes ("security by obscurity"). Here, the manipulator can use the digital pathways of system updates via internet connectivity and does not even have to be close to the vehicle.

With vehicle ECUs being at the forefront of ensuring driver safety, comfort, and vehicle performance, a holistic security concept covering all phases of software development is key to eliminating all threats right from the start and to ensuring a state-of-the-art authentication process throughout the vehicles' entire lifecycle. Unfortunately, ECU software development is often still handled in legacy systems that can hardly cope with the fast evolution of cyber threats, leaving them "defenseless" and vulnerable. Moreover, since the focus is on fast development cycles with functionalities that stand out for customers, the further development of basic ECU software is often neglected.

The new trend towards a more zonal approach with vehicle computers bundling various domains, as shown in figure 2, is another security challenge that calls for a variety of robust security frameworks with dedicated virtual machines, hardware security modules, trusted execution environments, firewall systems, and intrusion detection mechanisms. This effort is necessary to fully utilize the advantages of the vehicle computer approach, i.e. a significant simplification of the development process analogue to app coding in the consumer electronics industry.

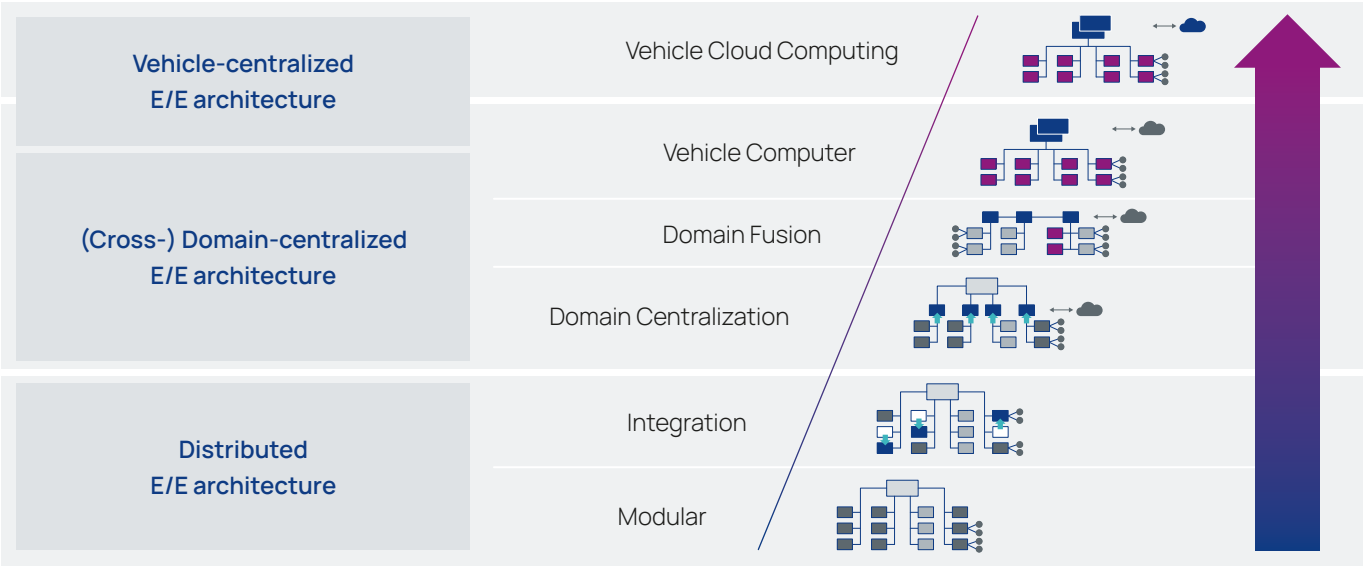

Figure 2: Ongoing evolution of vehicle E/E architectures from distributed to centralized.

THREAT #2

3.2 Cybersecurity challenges caused by a complex supply chain and after-sales services

Automotive supply chains are extremely complex ecosystems that involve numerous stakeholders, contractors and subcontractors, software providers, and shared development platforms. From early on within the supply chain, accessibility and updateability of components and systems have become a must-have. This multiplies the number of gateways for malware or data theft, as cybercriminals will specifically try to exploit these potentially less-protected systems for attacks. Choosing the right partners and making sure they meet all standards and stick to contractual obligations have become an important step for reducing third-party vulnerabilities and thus enabling a full end-to-end cybersecurity.

Once in operation, the connectivity options of modern vehicles enable OEMs to make alterations to the vehicle's software, which is crucial for a variety of use cases – from fast response to newly discovered vulnerabilities to provisioning additional functionalities or after-sales services. Whether such an update is carried over-the-air, via cable, or OBD stick: it always involves obligations for manufacturers. UN R 156 stipulates that a functioning software update management system (SUMS) must be established for every updatable component. The functionality is audited by an external organization and the certificate must be presented for type approval and re-audited every three years. Furthermore, manufacturers are now responsible for assessing whether an individual update affects the granted type approval. Consequently, enabling updateability of a specific component has also become an economic consideration for manufacturers. In principle, however, the advantages of connectivity options for complex components outweigh the additional effort, for example by avoiding cost-intensive recalls in the event of a bug.

OTA connectivity is obviously the most user-friendly method. It saves workshop visits and manual updates and is a huge time saver for large fleets. Among the various types of OTA updates are, for example, software over-the-air (SOTA), firmware over-the-air (FOTA), and over-the-air service provisioning (OTASP). Additionally, there is also a variety of other wireless connectivity options with authorized sources already utilized during the vehicle testing phase. From a security perspective, they all have several levels of system penetration and target various components of the E/E architecture. Nevertheless, they also all have one thing in common: they serve as a potential entry point for unauthorized software into the system.

A general trend with manufacturers is to use OTA interfaces as a digital revenue channel by providing various paid services to vehicle users. This requires even more effort to maintain security, as payment and usage information may also be exchanged. The main risk factor involved in OTA accessibility, however, is the two-way connectivity via mobile networks, Wi-Fi, or other wireless technologies to an external host or provider, including shifting functionalities or data storage capacities into the cloud (vehicle cloud computing) and setting up a (permanent) connection. By breaking through this on-board/off-board boundary, a whole range of new possible gateways for infiltrating malware or extracting data is opened. The retrieval of information on driving behavior, wear and tear, as well as malfunctions is important for component manufacturers, as the data flowing back enables permanent improvements. On the other hand, the more frequent data transfer also entails more risks. Hackers work on unravelling any weaknesses and learn from numerous real-life scenarios.

THREAT #3

3.3 Challenges within a growing, progressively connected ecosystem

Until now, we have focused on scenarios where vehicle manufacturers and their suppliers play a central role in managing security. However, as soon as a modern vehicle goes into operation, it is exposed to a wide variety of further potential risk situations – from unauthorized workshop visits to user-indexed updates (e.g. from third party sources) to docking onto charging points, traffic management stations, etc. These vehicle-to-everything (V2X) connectivity possibilities (or even obligations) will continue to rise: V2V (vehicle-to-vehicle), V2I (vehicle-to-infrastructure), V2P (vehicle-to-pedestrian), and V2N (vehicle-to-network) will not only become the enablers of (semi-)autonomous vehicles, but also bring commercial logistics and public transportation to a new level.

Additionally, the increasing involvement of software companies from the mobile communications and computing sectors introduces new dynamics. These providers offer valuable cloud and data storage options, as well as data analysis services for individual users and fleets. However, they also raise important concerns about data sovereignty and potential misuse, especially as these services may operate under varying security regulations around the world. Balancing the benefits of these innovations with the need for secure data handling will be crucial as the automotive ecosystem continues to evolve.

This very likely vision of the future of fully connected mobility clearly shows how closely enabling new functionalities is connected with an increase in cybersecurity-related issues. It entails the need for more efforts to secure them on a permanent basis, end-to-end along the three dimensions of lifecycle, ecosystem, and supply chain – as represented in figure 3. Hence the time has come to overhaul the current development processes with the big picture in mind.

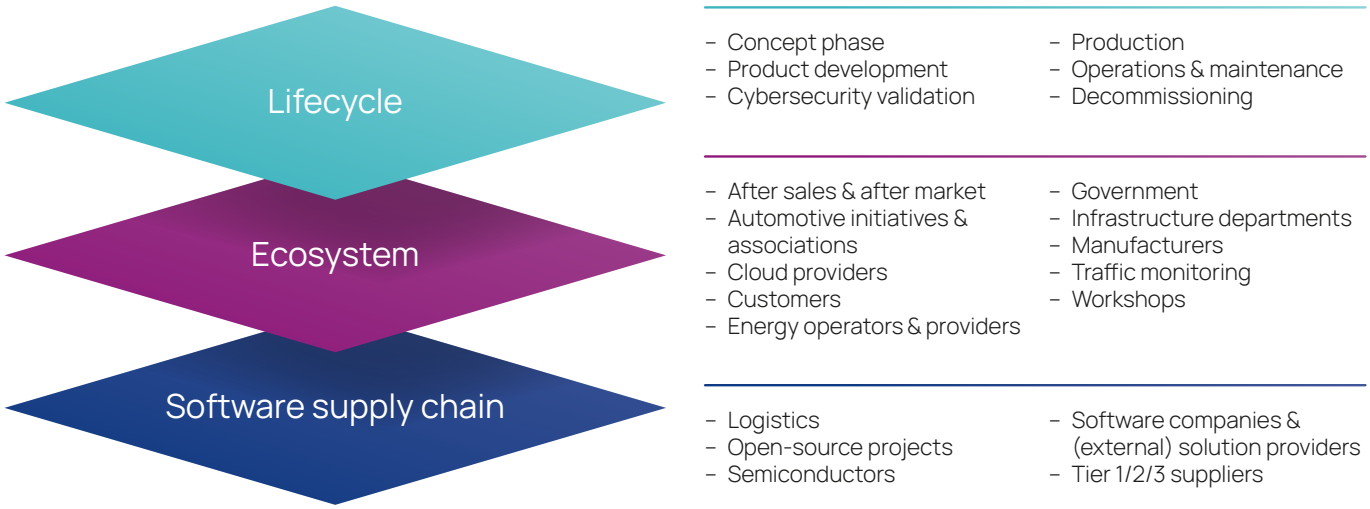

Figure 3: The three dimensions lifecycle, ecosystem, and supply chain cover all influencing factors that affect a modern vehicle.

4. DevSecOps vs. V-model: different approaches, both require cybersecurity

Modern vehicles are caught in the middle: on the one hand, many crucial vehicle functions responsible for safe operation are deeply embedded; on the other hand, a remodeling towards zonal, vehicle computer-based architectures is already taking place to satisfy the hunger for innovative SDV apps. Safety and non-safety domains cannot exist completely separately in a vehicle, as many functions rely on their interaction. Nevertheless, two distinct approaches are currently applied when it comes to developing vehicle software: the V-model (figure 5) and the DevOps cycle, depicted in figure 4. They must both be adapted according to the evolving threat landscape as well as legal safety and security requirements.

For deeply embedded functionalities, the security-enhanced V-model is the preferred process against the background of the still (partially) existing bond between hardware and software. The process involves a straightforward separation of abstraction levels; there is a final product at the clearly marked end of development, hard-coded to take care of specific, crucial functions.

The corresponding model for non-safety functionalities, the DevOps cycle, is designed as a continuous software development process that extends SOP and includes operation. For ETAS, it already evolves to the DevSecOps (development, security, operation) cycle to fully meet the new requirements of ensuring end-to-end security. The new approach does not need any major changes to the steps, just a capability upgrade out of the toolbox based on the four security principles described in chapter 5.

Generally, the V-model needs the same adaptation to become a "V-Sec-model". Built upon the premise of actively considering security at every point of the process, the subsequent introduction of the security principles must begin during the requirement specification phase, simultaneously opening the model for the required iteration circles and a shift to a more agile development process. This does not contradict the basic idea of the V-model, as it is by no means linear. The abstraction levels just need to align with their counterparts in verification and validation activities, while the order is negotiable. The baseline is: security must be implemented with each step. When it comes to ECUs with limited resources, this is not an easy job, as they require lightweight, efficient security protocols to ensure robust protection without compromising performance.

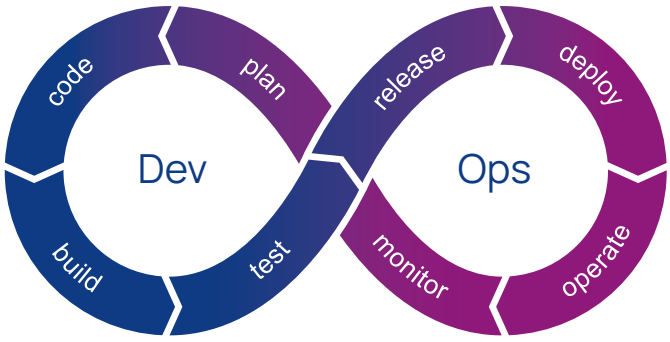

Figure 4: The DevOps circle for software development in vehicles

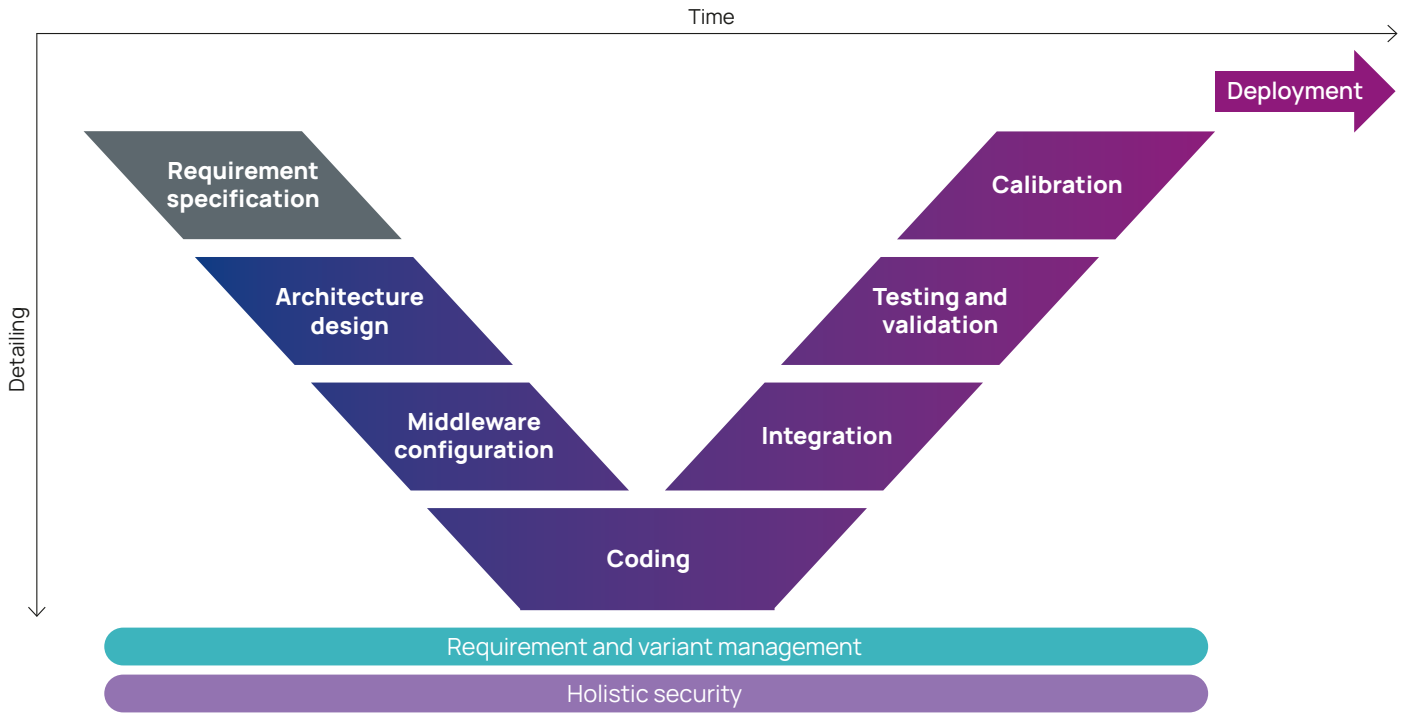

Figure 5: The V-model splits software development into two major parts. This version is adapted to the ECU software development process.

The focus on cybersecurity ultimately brings the two approaches closer together, as depicted in figure 6. In view of the changing E/E architecture towards vehicle computers and system-on-chip (SoC) setups, which blur the line between critical and general-purpose functions, this is a must. For example, when a braking system is part of a sophisticated feature for automatically induced maneuvers depending on object recognition, it is never fully completed as required in the standard V-model. The applied V-Sec-model therefore requires an -Ops appendix (or the De-V-SecOps a capital V), allowing for constant optimization of this critical functionality. The implementation of the four security principles helps to adapt development processes to cybersecurity requirements while moving towards holistic cybersecurity management.

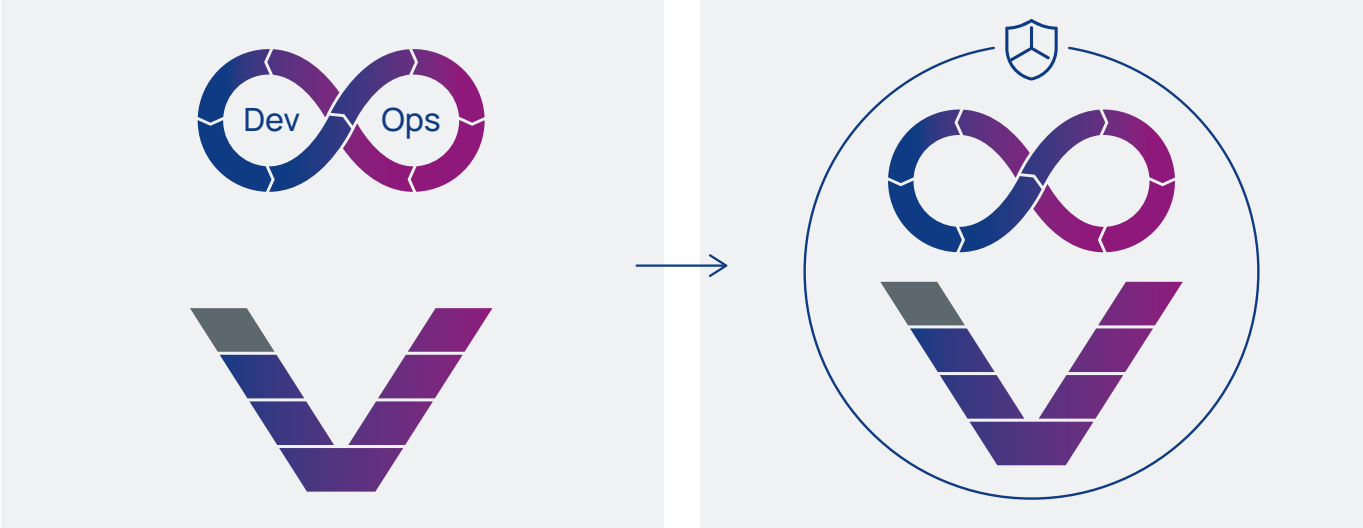

Figure 6: The holistic integration of cybersecurity throughout the entire process in both approaches, V-model and DevOps circle, blurs the boundary between the two.

5. The four security principles

Awareness of the need for change is one thing; the other is practical implementation. Here, the strategy must be gradually broken down into elements that can be translated into concrete processes. Four principles that can be used as a guide: security by design, defense in depth, risk management and monitoring, and organizational security. They should be applied and leveraged on a high maturity level to enable end-to-end cybersecurity along the three dimensions of lifecycle, ecosystem, and software supply chain. The principles cover all aspects of product security within an organization: process, technology, information, and of course also people and culture.

5.1 Principle #1: Security by design

Security is taken into account from the very beginning of the development process and in each step, including compliance with (legal) safety regulations and implementation of a suitable security architecture. Be it in the DevSecOps or the V-model, this ongoing consideration of all security aspects throughout the development process can avoid high costs for re-work in later stages of the project or after sales. A software developed according to the security by design principle is robust and resilient during its entire lifecycle. Expanding the principle in accordance with today's threat landscape also leads to permanent optimization of the time needed to fix vulnerabilities at any point.

5.2 Principle #2: Defense in depth

Having various defense lines implies that the failure of a single one does not directly compromise security. This is what the principle of defense in depth is basically about: by establishing multiple protection mechanisms, there is no single point of failure that a cybercriminal can conquer. With traditional E/E architectures, a layer-based approach reaching from deeply embedded components right up to the top (e.g. vehicle network) used to be the ideal approach, while taking advantage of the still strong hardware-based separation and isolation of functions. Now that more centralized vehicle architectures and vehicle cloud computing are entering the stage, the complexity must be addressed with additional "virtual" layers, ultimately setting the course towards a zero-trust security approach.

5.3 Principle #3: Risk management and monitoring

As the number of possible risks is rising, targeted and comprehensive management is unavoidable. For example, the performance of a threat analysis and risk assessment (TARA) is a main component within the ISO/SAE 21434 standard. It gives manufacturers and suppliers a blueprint to find potential threats and develop appropriate protective measures. In the threat analysis phase, all cybersecurity threats to the vehicle are systematically identified, including the assessment of potential cyberattack scenarios to set up suitable countermeasures. The risk assessment phase then prioritizes these risks and analyzes how they affect the development process. The general goal is to achieve the lowest possible threat level, e.g. through consistent application of the security by design and defense in depth principles. The opening ecosystem and the constantly changing threat landscape also require rethinking, as most development legacy systems lack the appropriate tooling and processes to constantly recognize risks, analyze and close security gaps.

5.4 Principle #4: Organizational security management

A general change must take place within the organization to achieve comprehensive cyber resilience. This includes, above all, a shift in the mindset of all the people involved. The complex and constantly evolving threat landscape requires cooperation, flexibility, communication, and a high and proactive cybersecurity awareness far beyond a "checklist mentality". At the same time, legal requirements detail how the process must be set up. For instance, the UNECE regulation requires a holistic CSMS covering operations, risk management/compliance, and internal audits. Following the so called "three lines of defense framework", security is no longer an isolated topic for individual departments but runs through all processes and covers the entire lifecycle of the product. This takes time and requires adjustments, especially when also fully incorporating all stakeholders within the organization and the software supply chain.

6. Dealing with complexity through guidance and solutions from mobility experts

Whether it is awareness of the threat landscape, knowledge of all regulations and standards, or familiarity with the four principles: experts are required to put this theoretical knowledge into practice. As we have outlined, providing state-of-the-art cybersecurity involves a fundamental and comprehensive realignment of the processes within development, manufacturing, and after sales for automotive manufacturers and suppliers. Ultimately, these concepts must be translated into everyday practice through software and hardware solutions, development tools, and individual instructions.

For example, adopting a multi-layered security architecture in accordance with the principles #1 and #2 implies setting up state-of-the-art encryption, authentication, intrusion detection, and secure boot mechanisms within an existing legacy system. If done from scratch, this requires a separate cybersecurity department. Therefore, many companies rely on external support to tackle this growing complexity, while saving time and resources. This trend is also visible in the automotive cybersecurity market forecast: with a compound annual growth rate (CAGR) of 18.93% between 2024 and 2031, it is projected to increase from 7.83 billion US dollars in 2023 to 31.34 billion by 2031[4], as shown in figure 7.

However, implementing external cybersecurity solutions presents its own challenges, such as vendor lock-in, incompatibilities, or integration difficulties. It is therefore crucial to choose the right partners to develop a holistic and future-proof cybersecurity concept that includes individual circumstances and legacy systems. When it comes to regulatory compliance, concrete and structured guidelines are paramount. It is not necessary to develop own solutions time and time again, since legal regulations are the same for every company. ETAS has developed the ESCRYPT Product security organization framework (PROOF) as a proven methodology to optimize cybersecurity efficiency by following eight steps to build up a CSMS according to principle #4, individually tailored to the maturity level of each customer.

A partner like ETAS is additionally able to provide solutions on a software and hardware level, with a strong focus on process optimization: a portfolio of user-friendly tools and managed platforms that minimize manual efforts have a high degree of automation and are further developed dynamically and consistently. The portfolio (see figure 8) is clustered in designing, enabling, and managing security, so that customers can individually select the support they need for their cybersecurity solutions.

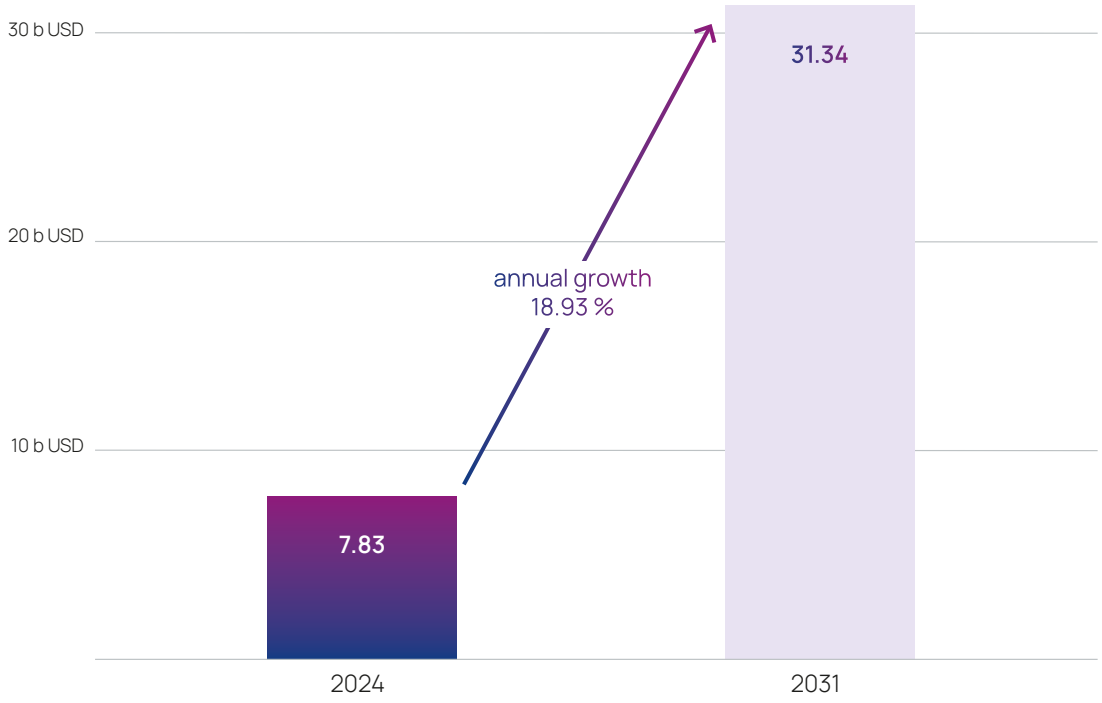

Figure 7: Automotive cybersecurity market forecast 2024 to 2031

Design security

We provide a product security organization framework to achieve ISO 21434 compliance and security tools for risk management and penetration/fuzz testing.

ESCRYPT Cybersecurity Management Systems with PROOF
A proven methodology to optimize cybersecurity efficiency

ESCRYPT CycurFUZZ
Smart fuzzer tool for automotive systems

ESCRYPT CycurRISK
Software tool for threat analysis and risk assessment

Enable security

We offer embedded software products, like Hardware Security Module and cryptographic libraries for micro controllers as well as for vehicle computers (i.e., System on a Chip) to protect from misuse of cryptographic keys. In addition, we offer solutions for intrusion detection & prevention including automotive firewall to protect from manipulation of data or communication.

ESCRYPT CycurHSM
Powerful security software for your ECU

ESCRYPT CycurSoC
Enabling safety and trust for software-defined vehicles

ESCRYPT CycurGATE
High-performance automotive Ethernet/IP firewall and router

Manage security

At ETAS we offer integrated intrusion detection and protection for vehicle fleets worldwide. We enable you to manage security with an in-vehicle intrusion detection system, security monitoring for the entire connected fleet through Vehicle Security Operations Centers and continuous risk management via over the air updates.

ESCRYPT CycurIDS
Embedded intrusion detection for CAN and Ethernet networks

ESCRYPT Vulnerability Management Solutions
Enhance product security with effective risk-based vulnerability management

ESCRYPT Vehicle Security Operations Center
Managed security service tailored to the needs of the vehicle fleet, including the integration of event sources from vehicle fleets and vehicle backend systems

ESCRYPT Intrusion detection and prevention solution
Permanent monitoring of vehicle fleets to identify rising security threats, establish dedicated incident response, and keep the security level stable over the entire life cycle

Figure 8: ETAS vehicle cybersecurity portfolio, clustered in designing, enabling, and managing security

7. Conclusion

Cybersecurity is a top issue in the automotive industry and will play an ever-greater role in the increasingly connected future. However, adapting processes to a holistic cybersecurity strategy must not and should not be seen as a burdensome duty. It is first and foremost a great opportunity for both automotive manufacturers and suppliers to take their development and production to a new level and actively leverage their market competitiveness with new after-sales services. The ETAS cyber maturity report 2024[5] clearly shows: the higher the maturity level, the stronger companies see their position in this competitive market. Regardless of where a company is situated on the journey, the good news is: for every maturity level, cyber threat, and regulatory requirement, partners like ETAS have already paved the way – or cut a patch through the jungle. Their support ranges from comprehensive blueprints for company processes to very specific software solutions for ECUs or vehicle computers; available as single purchase or as ongoing managed service to spare manufacturers and suppliers from building up and maintaining own resources. Together, cybersecurity challenges can be turned into opportunities, and road user safety can be permanently maintained on the maximum level.

About ETAS

Founded in 1994, ETAS GmbH is a wholly owned subsidiary of Robert Bosch GmbH with a local presence in all major automotive markets in Europe, North and South America, and Asia.

ETAS offers comprehensive solutions for the realization of software-defined vehicles in the areas of software development solutions, vehicle operating system, vehicle cloud services, data acquisition and processing solutions, integrated customer solutions and cybersecurity.

As industry pioneers in cybersecurity, we assist our customers in managing cybersecurity-related complexities, reducing cyber risks, and maximizing their business potentials with a proven on- and offboard portfolio of software products and professional security services.

ETAS automotive security solutions are safeguarding millions of vehicle systems around the world – and are setting standards for the cybersecurity of software-defined vehicles.

References

1) Rockwell Automation, 9th annual State of Smart Manufacturing Report: Automotive Edition, accessed 2024/11/10, https://www.rockwellautomation.com/content/dam/rockwell-automation/documents/pdf/campaigns/state-of-smart-2024-automotive/2024-state-of-smart-manufacturing-for-automotive.pdf

2) Forbes, accessed 2024/11/11, https://www.forbes.com/sites/michaelharley/2024/03/28/eu-cybersecurity-laws-kill-porsches-718-boxster-and-cayman-early/

3) Automotive IT, accessed 2024/11/11, https://www.automotiveit.eu/technology/volkswagen-streicht-modelle-wegen-cybersecurity-vorgaben-99-311.html

4) Faist Group, accessed 2024/11/11, https://www.faistgroup.com/news/growth-challenges-automotive-cybersecurity/

5) ETAS Cyber Maturity Report, accessed 2024/11/11, https://www.etas.com/download-center-files/DLC_products_ESCRYPT/etas-automotive-cyber-maturity-report-2024-en-20240719.pdf

Contact information

Christian Schleiffer
Get in touch on LinkedIn
Contact me
www.etas.com/wesecurethefuture

Last updated: 12/2024