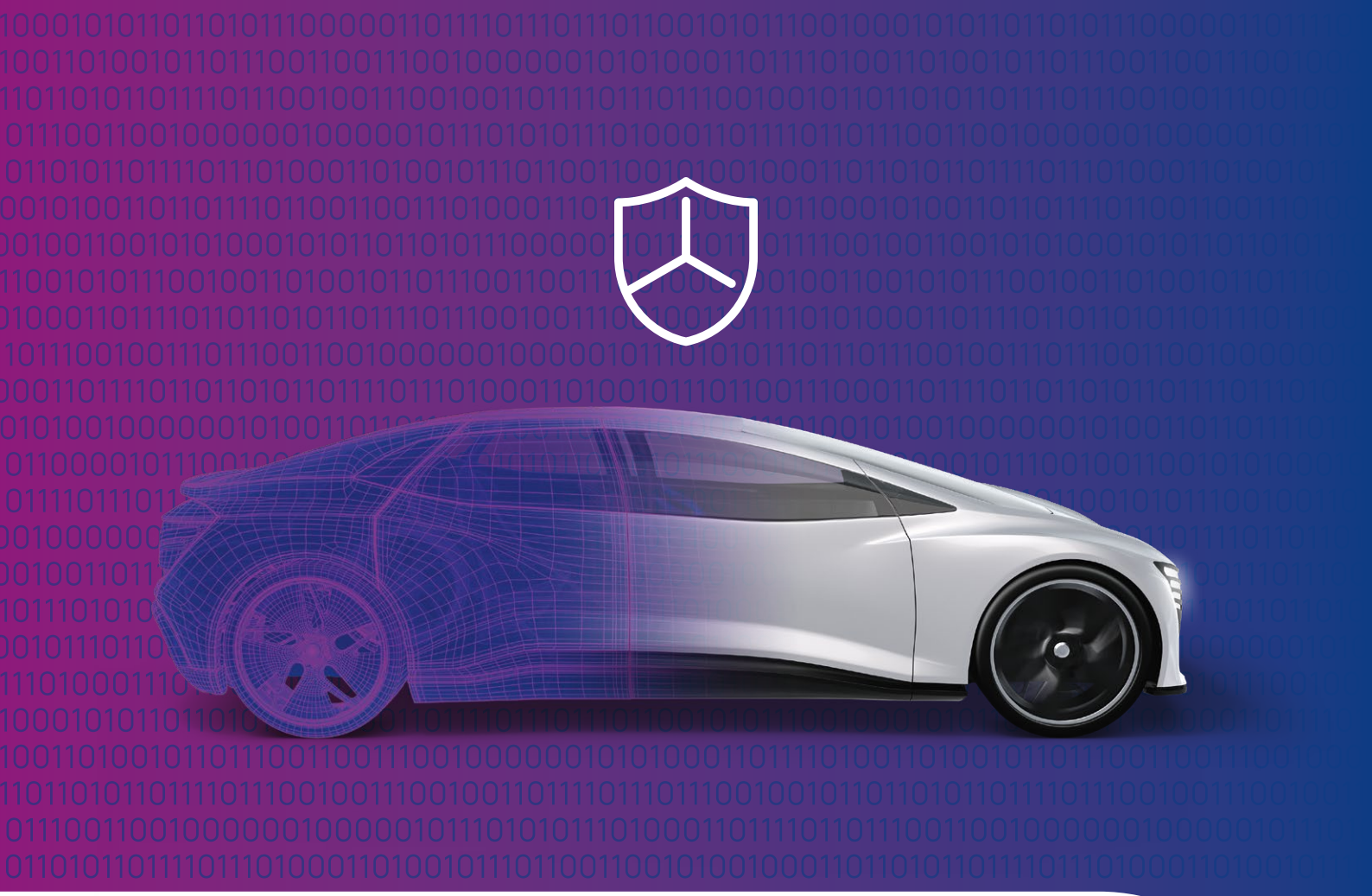


Cybersecurity for the software-defined vehicle

Michael Lüke & Dr Moritz Minzlaff, May 2023

Empowering Tomorrow's Automotive Software
www.etas.com

Table of contents

1. The software-defined vehicle challenges boundaries and mindsets 3

1.1 Challenging the on-board/off-board boundary 3

1.2 Challenging assumptions about automotive software 4

1.3 Challenging the development mindset 4

1.4 The new end-to-end security 4

2. Keeping up with the speed of software 5

2.1 DevSecOps – Development, security, and operations 5

2.2 To the software-defined vehicle in three phases 6

3. Four security principles for SdV-level cyber maturity 8

3.1 Principle #1: Security by design 8

3.2 Principle #2: Defense in depth 8

3.3 Principle #3: Risk management & monitoring 9

3.4 Principle #4: Organizational security management 9

4. Reaching SdV-level cyber maturity 10

4.1 Assessing current maturity 10

4.2 Identifying target maturity 11

4.3 Executing a gap closure program 11

Bibliography & Contacts 13

1. The software-defined vehicle challenges boundaries and mindsets

Cybersecurity has become a major business factor for modern cars: software vulnerabilities have led to safety recalls [1], automotive-specific regulations mandate security in the largest markets [2], [3], and the majority of manufacturing and automotive companies recently ranked cyber incidents as a top 5 business risk [4].

Automotive software is closely linked with automotive security. As the industry moves toward the so-called software-defined vehicle (SdV), it needs a strong understanding of cybersecurity. This whitepaper provides the industry with a compass and a map to successfully navigate the risks.

From a consumer perspective, the software-defined vehicle will feature app stores much like a smartphone and functions that require off-board data processing. Imagine, for example, a rental car that is automatically fully personalized to your preferences: from radio settings to seat configuration to climate controls. From a manufacturer's perspective, the SdV allows new data-centric business models such as pay-per-use functions that are already found in some modern cars. The SdV is built on two technological advances that allow abstraction from the physical vehicle: vehicle computers and vehicle clouds. These innovations challenge a classical vehicle's boundaries and prevalent mindsets. Automotive companies must therefore adapt their approach to automotive security: cybersecurity for the SdV must be defended end-to-end along the three dimensions of lifecycle, ecosystem, and software supply chain (see Figure 3).

1.1 Challenging the on-board/off-board boundary

The software-defined vehicle leverages and relies on off-board functions, known as vehicle cloud computing. Interactions with smartphones, data processing in the backend, all this will have a direct impact on where the vehicle is going and how it interacts with drivers, passengers, and road users. Off-board security problems can have an on-board impact [5], [6]. From a security perspective, this abolishes the on-board/off-board boundary: automotive companies and the vendors and operators of IT systems must ensure security in the automotive ecosystem (see Figure 1) to protect the software-defined vehicle and the safety of road users.

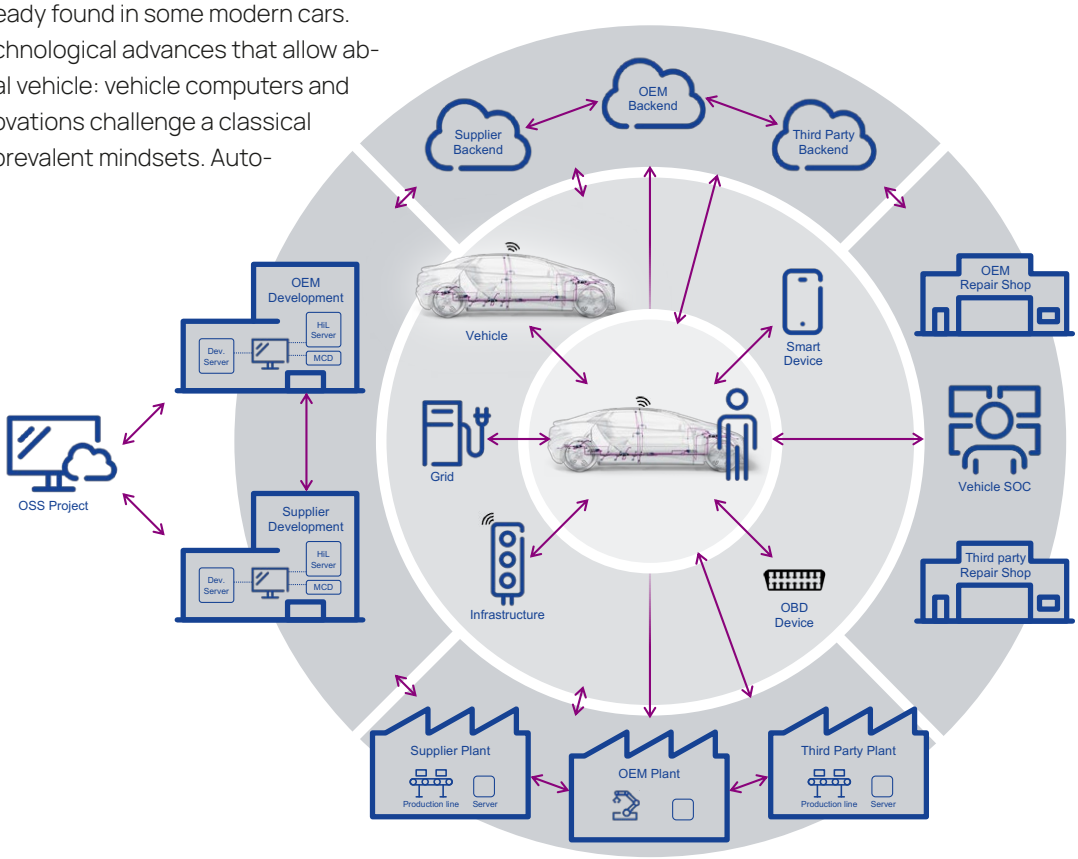


Figure 1: The automotive ecosystem and its data flows across players in the ecosystem.

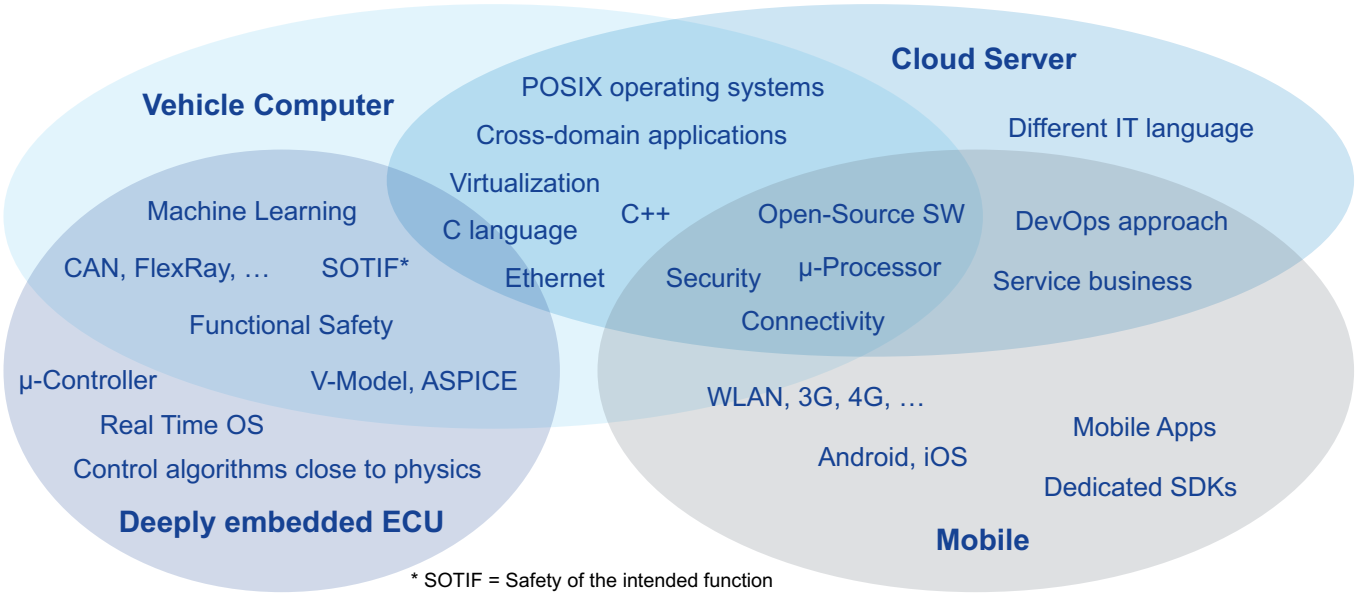


Figure 2: The SdV introduces many new types of automotive software in addition to classical deeply embedded software.

1.2 Challenging assumptions about automotive software

The software-defined vehicle is more than a vehicle with connectivity. Essential, differentiating features are implemented in new software inside the vehicle on so-called vehicle computers and in new software outside the vehicle on so-called vehicle clouds. This results in an increasing number of lines of code and thus increasing potential for vulnerabilities. More crucially, this shift breaks down existing assumptions about what automotive software is: vehicle computers and vehicle clouds use new programming languages, virtualization and server technologies, numerous open-source components, and new third-party contributors (see Figure 2). Software vulnerabilities in any of these components and sources impact the security of the software-defined vehicle. The SdV must be protected along a drastically expanded and much more diverse software supply chain.

1.3 Challenging the development mindset

This new automotive software differs in another crucial aspect: it is never finished; it is always evolving. The understanding that a vehicle's development ends with start of production does not hold anymore: the SdV is always evolving, and frequent updates are a characteristic feature. Without a traditional on-board/off-board boundary, the SdV is continuously exposed to an always evolving threat landscape. Consequently, reports show that cyberattacks on cars are increasing, especially via remote connections that can come at any point in the SdV's lifecycle [7]. This applies to the manufacturing phase as well. Between 2020 and 2021, "[a]ttacks against manufacturing increased from 7% [of all attacks] last year to 22%," and there was an "[u]p to 300% increase in attacks from opportunistic targeting" [8]. Automotive manufacturers and suppliers need to monitor, protect, and update software consistently and quickly along the entire lifecycle.

1.4 The new end-to-end security

This is, then, the meaning of new end-to-end security: protection must be ensured from design to production to end of life (lifecycle dimension), from customers to manufacturers to existing and new software suppliers including open-source software projects (software supply chain dimension), and from in-vehicle components to mobile devices, vehicle clouds, and infrastructure vendors and operators (ecosystem dimension).

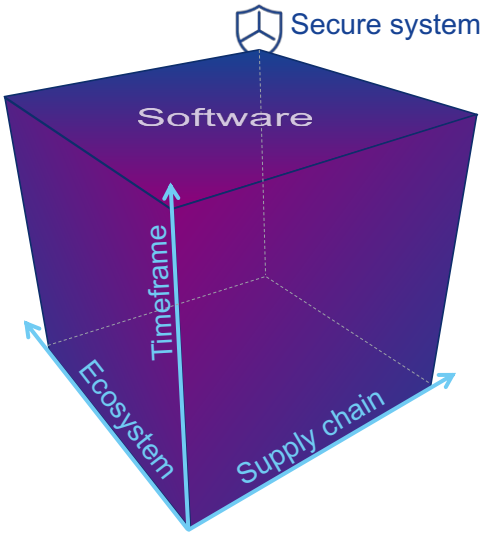


Figure 3: Cybersecurity for the SdV must be defended end-to-end along the three dimensions of lifecycle, ecosystem, and software supply chain.

Building on our experience in helping automotive companies implement this new end-to-end security, this whitepaper is structured as follows: Section 2 looks to the software and tech industry for lessons learned, in particular the DevOps paradigm, and discusses automotive industry specifics. This allows Section 3 to define the new SdV-level cyber maturity that matches the increased cyber risk of the SdV. This paper concludes in Section 4 with an outlook on how automotive companies can achieve this SdV-level cyber maturity.

2. Keeping up with the speed of software

The software-defined vehicle is a reality, so it is prudent to look to more established software industries for lessons learned and best practices. A key factor that sets high-performing software companies apart is their grade of automation and software delivery capabilities. The faster that automotive manufacturers and suppliers can troubleshoot and fix their software systems, the better they can protect their customers and business models against cyber threats. Incidents do and will happen, but a comprehensive, well-implemented set of measures can reduce cyber risks associated with sophisticated, targeted attacks [9], developer protests [10], or simple bugs [11] to an acceptable level. Key metrics in this context are mean time to detect (MTTD) and mean time to repair (MTTR), and high security awareness and cyber maturity are hallmarks of technology companies.

2.1 DevSecOps – Development, security, and operations

But even with the best development practices, some bugs will inevitably remain undiscovered or unaddressed, leaving software vulnerable to attack. In this context: "It turns out that patching vulnerable software, if implemented consistently, would stop most hackers cold and significantly reduce risk" [12]. DevOps, if done right, clearly helps implement this consistency, and it can help accelerate the software development and deployment throughout the software lifecycle.

However, in today's cybersecurity landscape, it is crucial to take DevOps to the next level by adopting DevSecOps to ensure end-to-end security of the software supply chain.

DevSecOps embeds security capabilities in the development and operation of software, from source code to the minds and hearts of software developers and everyone who interacts with the software systems (see Figure 4).

Given the growing integration between classical automotive software and IT software, adopting DevSecOps is no longer just an option but a critical imperative. For instance, as brake systems rely on deeply embedded software, they will continue to be developed using the security-enhanced V-model. But the growing integration between classical automotive software and IT software demands this more focused approach to DevSecOps, particularly in the case of vehicle computers and system-on-chip (SoC) architectures. These systems bring together safety-critical and general-purpose functions, blurring the lines between traditional brake systems and features such as roadside object recognition, both inside and outside the car (see Figure 6).

Developing and deploying software to such SoC architectures requires rigorous validation of components and source code, regardless of whether they are in-house or from external third parties, open or closed source. This validation represents an important aspect of the required end-to-end security of the software supply chain. Starting at the source-code level is essential, as zero-day exploits can come from any line of code, and malicious source-code manipulation is nothing new in the software world. Targeted attacks can not only exploit such vulnerabilities, but they can also insert them in a first place. Cultivating the right mindset is crucial to protecting against these kinds of cyber threats and requires a multifaceted approach that includes both technological and organizational measures.

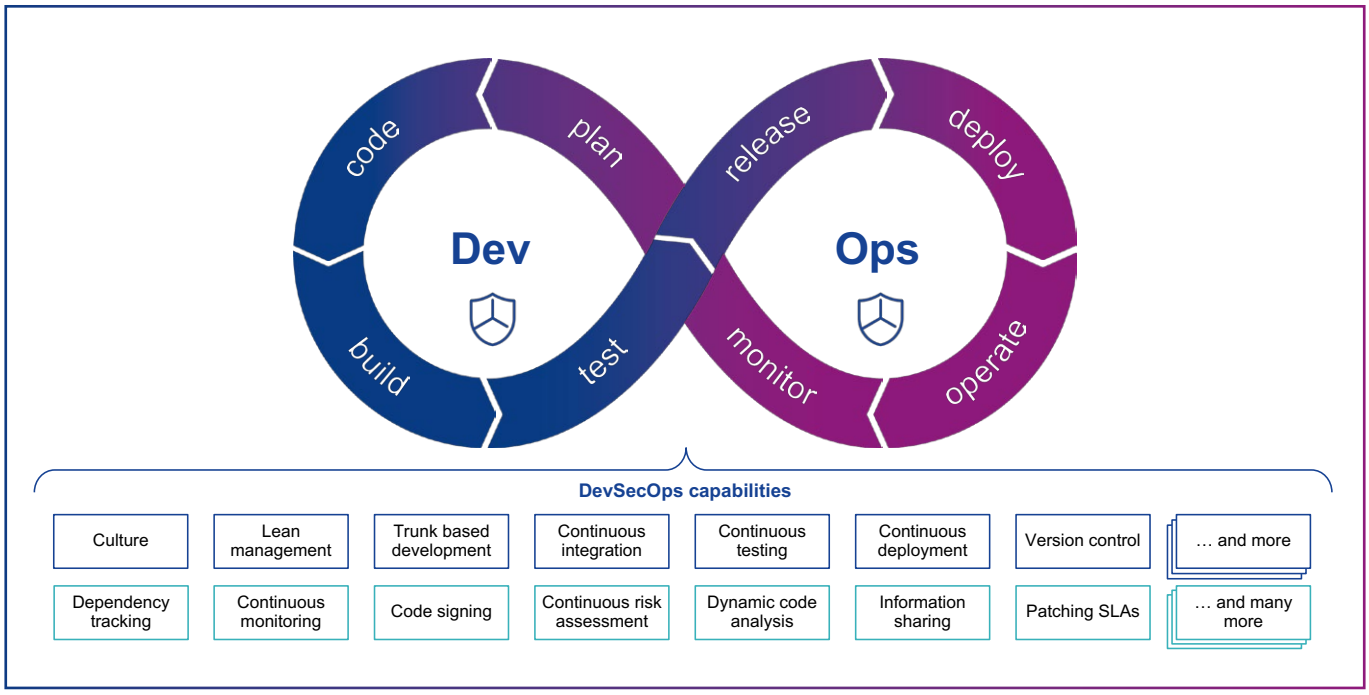


Figure 4: DevSecOps augments DevOps capabilities with dedicated security capabilities (green).

The complexity behind cybersecurity in this context is driven by the ever-growing volume of software used across the ecosystem, supply chain, and timeline (see Figure 5). To manage this complexity effectively, systems and organizations must keep pace with this constant expansion. This is the only way to control the risk landscape for the software-defined vehicle in an effective way.

This challenge must not be underestimated. To address it effectively, teams must work together seamlessly, with information flowing smoothly across different tools and functions. Speed is of the essence, making automation essential in security engineering. Achieving this level of collaboration and transparency requires excellent skills in cross-functional teamwork, particularly across departmental boundaries and even across organizations. This ability to collaborate effectively is a crucial factor in the success of DevSecOps and an essential aspect of maintaining a secure system. In Sections 3 and 4, we continue this topic and present how to manage cyber risk and capitalize on the potential of the SdV.

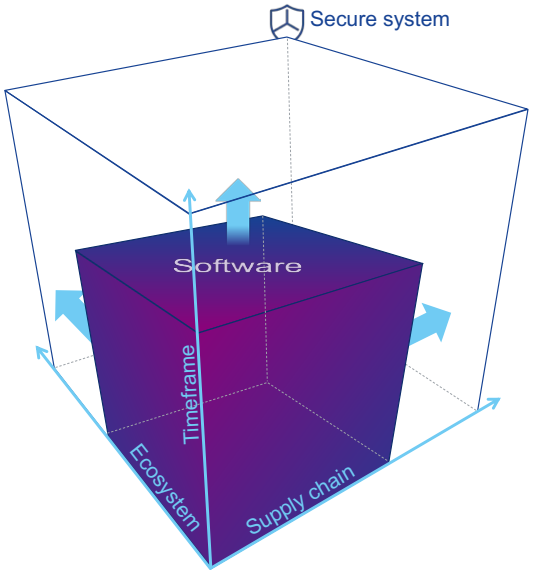


Figure 5: The cyber risk space grows due to the growing volume of software in the automotive ecosystem.

2.2 To the software-defined vehicle in three phases

The software industry adopted DevOps several years ago and learned a lot about how much value transparency can generate and how to break down silos. This new level of communication will be equally relevant for automotive companies, as E/E architectures continue to develop and increasingly implement vehicle computers and cloud-based functionality (see Figure 7). Vehicle centralized architectures break the former boundary between on-board and off-board functions. However, remaining company silos create weaknesses such as incompatible risk scoring or unaligned software patching strategies within and across organizations.

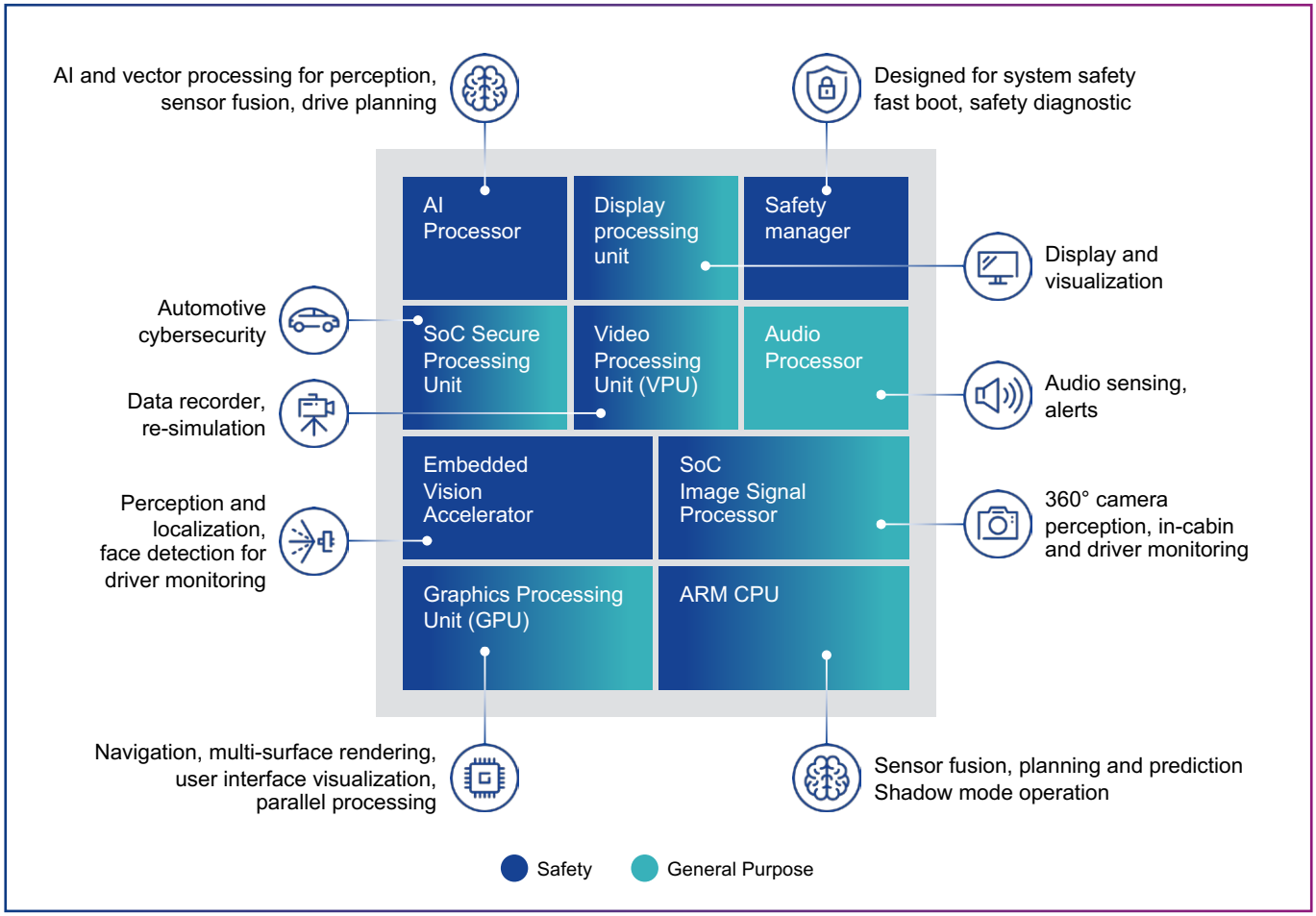


Figure 6: A system-on-chip used in a vehicle computer integrates functions of different criticality (safety, data protection, infotainment).

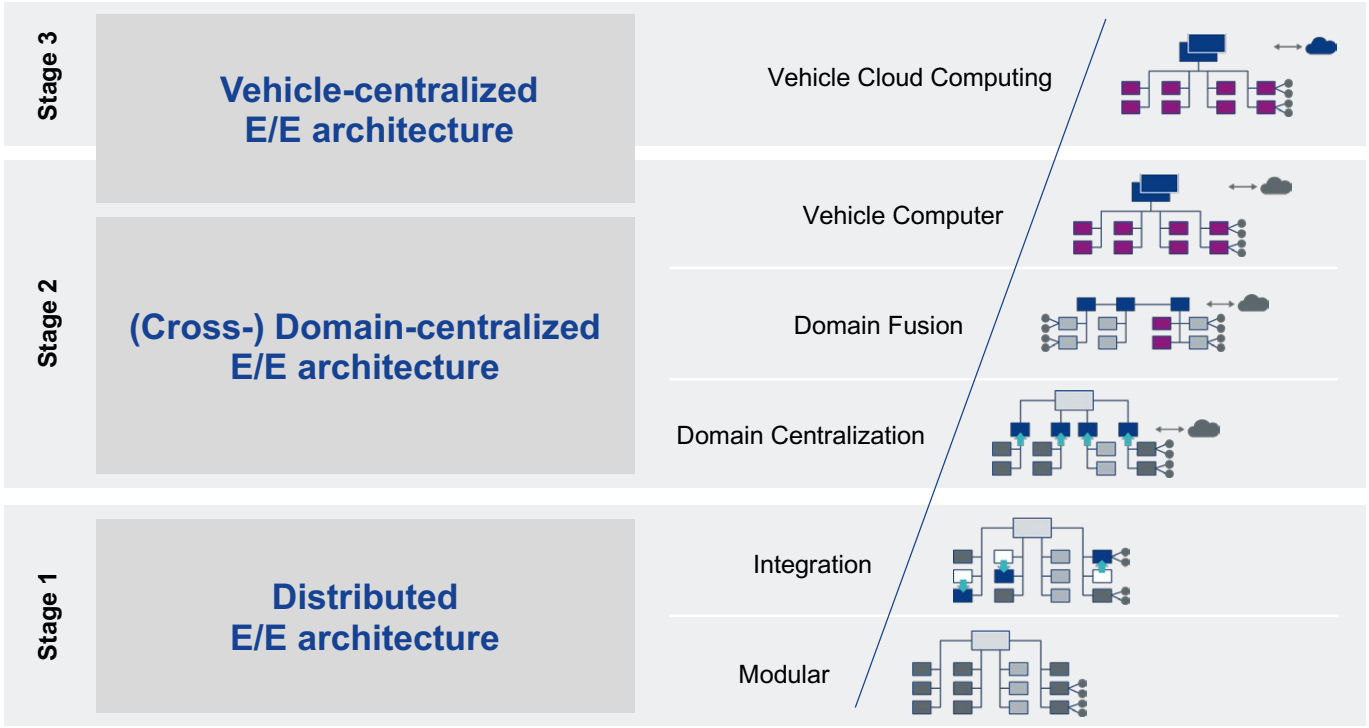


Figure 7: Developments of E/E architectures that enable the SdV.

Consequently, the automotive industry can learn from the software industry and adapt the lessons learned to its specific requirements, for example in the context of a longer product lifecycle. Furthermore, functional safety requirements and regulations in the automotive industry require extensive verification and validation activities, so any implementation of DevSecOps will need to pay attention to safety aspects as well. However, DevOps and automation can help perform this verification even faster. And not every functionality is safety relevant, so the industry needs to learn to work with different velocities for the same product.

In addition, the automotive industry must keep up with the latest advances in the software industry. For example, the zero-trust initiative is important for the future of the software-defined vehicle because it provides a security framework that can help secure communication and data exchange between the various components of a connected vehicle.

The zero-trust approach helps ensure that only authorized and verified entities can access the vehicle systems and data, which is crucial for maintaining the security and privacy of both the vehicle and its occupants. Adoption in the automotive business is inevitable, maybe not today but certainly in Phase 3 (see Figure 8).

To avoid a waste of time and resources, it is essential not to reinvent the wheel. DevOps methodologies should be copied with pride by the automotive industry, adapted, and applied together with an approach to tear down silos between development and IT operations departments. The successful implementation of continuous integration and delivery requires increased collaboration and faster feedback loops and, moreover, a sense for security to make it fast and secure.

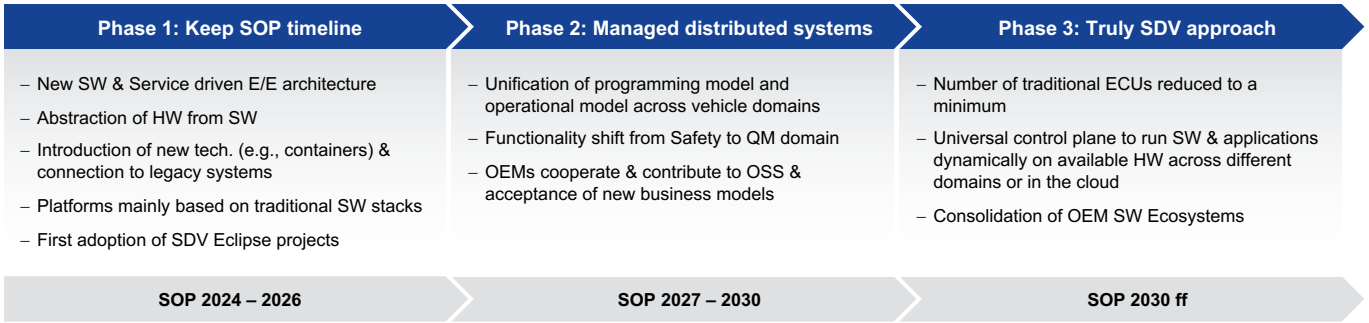


Figure 8: The implementation of SdV will happen in three phases.

3. Four security principles for SdV-level cyber maturity

Successful security programs adhere to four principles: security by design, defense in depth, risk management & monitoring, and organizational security. These principles have allowed organizations to establish product security with their people, processes, and technology. However, the software-defined vehicle challenges existing boundaries and mindsets. As the risk space grows (see Figure 5), the automotive industry must re-think these four principles in order to match risk and security. Manufacturers and suppliers must take their implementations of the principles to a new maturity level to properly protect the SdV end-to-end along the lifecycle, ecosystem, and software supply chain dimensions (see Figure 9). Just as individual activities in the DevOps loop have only limited impact in isolation, it is only when an organization reaches SdV-level maturity in all four principles and becomes cyber resilient that it will truly master cybersecurity for the software-defined vehicle.

3.1 Principle #1: Security by design

Security by design means that security is built in to the product from the very beginning. This is often a process-focused principle. The established implementation of this is a security-enhanced V-model. Considering the permanent exposure of the SdV to potential attackers, automotive companies must expand this understanding: security by design must also mean a relentless optimization of the mean time to repair (or fix) of vulnerabilities for the entire SdV lifecycle. High automation and a focus on resilience are needed to close the DevOps loop.

3.2 Principle #2: Defense in depth

Defense in depth is the practice of establishing multiple protection mechanisms without a single point of failure that compromises the entire product. Specific security technology (software and hardware) is a focus of this principle. Pre-SdV, this commonly meant a layered approach from deeply embedded components to on-board domains to the entire vehicle network. The new vehicle centralized architectures with vehicle computers and vehicle clouds require an ecosystem-level view with additional layers for on- and off-board components including an evolution toward zero trust.

Mature organizations think and act differently

The description of higher maturity levels in Figure 9 is based on ETAS's decades of experience in supporting automotive companies with cybersecurity as well as the annual, industry-leading ESCRYPT Automotive Cyber Maturity Survey. The data paint a striking picture: high-maturity companies approach cybersecurity stakeholders differently, prioritize regulatory requirements differently, and set higher budgets for cybersecurity. Increasing cyber maturity correlates with increasing satisfaction, increasing DevSecOps mentality, and increasing end-to-end coverage of security. Read our full Automotive Cyber Maturity Report from 2022, based on hundreds of responses from automotive professionals worldwide, and follow ETAS social media channels to be notified of this year's report and upcoming survey.

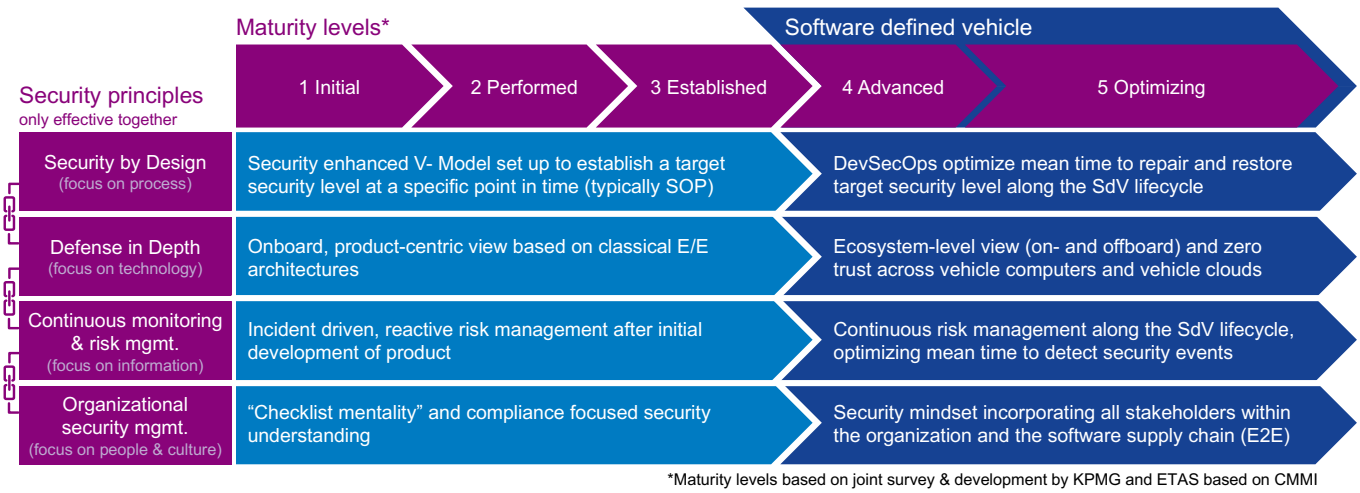


Figure 9: The SdV requires a new level of cyber maturity in each of the four security principles.

3.3 Principle #3: Risk management & monitoring

Risk management and monitoring must be at the heart of all security activities. This principle focuses on information and data assets within the SdV ecosystem. Threat and risk analyses (TARA) are one of the first steps automotive companies take as they progress from initial to established maturity. TARAs identify the risk and measure whether mitigations reduce risk to an acceptable level, e.g., through consistent application of the security-by-design and defense-in-depth principles. However, the initial processes and tooling that manufacturers and suppliers have established often do not lend themselves to the high-frequency changes that the SdV demands. Continuous monitoring of the threat landscape – including vulnerabilities in the ecosystem, optimizing mean time to detect security events, and quickly updated TARAs until the end of an SdV's lifetime – are distinguishing marks of organizations with advanced or optimizing maturity.

3.4 Principle #4: Organizational security management

A review of cyber incidents in recent years demonstrates that security needs technical and organizational solutions, and so this principle looks to people and culture. Automotive manufacturers and suppliers must implement cybersecurity management systems in operations, in risk management and compliance, and in internal audits (the so-called "three lines of defense"). Building up all areas takes time and effort, so initial-maturity organizations typically focus just on one line of defense, for example with a clear focus on "compliance" and a related checklist mentality. This is understandable and can help a company initially stay in business. However, the SdV with its data-centric business models requires an expanded security mindset covering all three lines of defense and integrating all stakeholders including the software supply chain (see Figure 10).

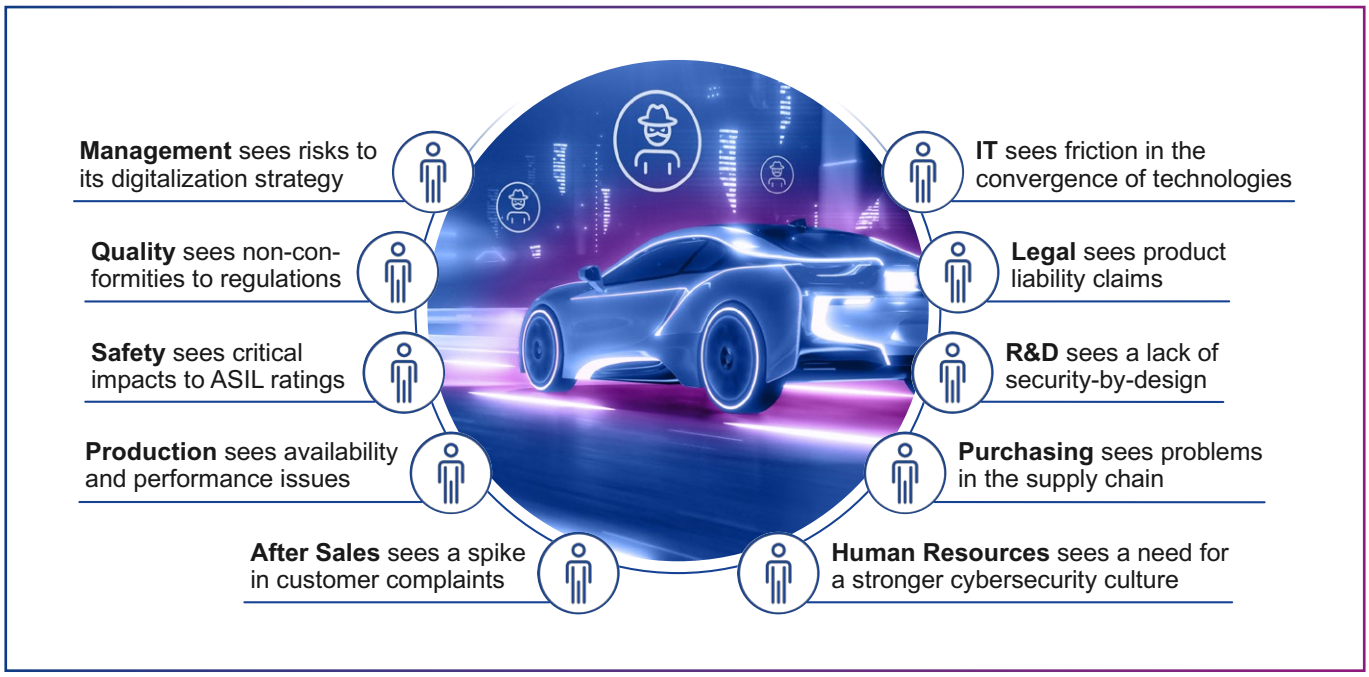


Figure 10: High-maturity security organizations integrate the perspectives of all stakeholders within the company, from its customers, and in its software supply chain.

4. Reaching SdV-level cyber maturity

ETAS has unique expertise in upgrading the cyber maturity of automotive manufacturers and suppliers: ESCRYPT cybersecurity solutions have positively shaped and helped pass cybersecurity milestones in the automotive industry for almost two decades. From authoring the very first research papers in the early 2000s, to implementing hardware security modules in millions of cars, to establishing a DevSecOps organization that can roll out patches within hours and minutes, we can identify successful and proven patterns in advancing cyber maturity in the automotive industry.

Reaching SdV-level cyber maturity is a three-step process of 1) assessing current maturity, 2) setting target maturity, and 3) executing a gap closure program (see Figure 11). Let us now consider each in turn.

4.1 Assessing current maturity

Assessing the current cyber maturity of people and processes allows an organization to focus its resources where they contribute the most to a timely and cost-efficient achievement of the targeted new maturity level. Indeed, in our consulting projects we often uncover existing capabilities, for example from the software or the functional safety domain, upon which a company can more quickly build advanced product security capabilities. The responses from the ESCRYPT Automotive Cyber Maturity survey support this point: participants from initial-maturity companies selected functional safety standards, a domain that is well understood by many, as highly relevant for their cybersecurity program. This is why we have designed the PROOF automotive cyber maturity model (see text box) that is available to automotive companies to assess their maturity.

Similarly, a stock-taking on the technical level is especially meaningful in brownfield situations where E/E architectures are not designed from scratch, and where legacy architectures potentially feature (implicit) security measures. Crucially, assessing the status quo across people, processes, and technology must consider not only the organization itself but also with whom and how it collaborates in the ecosystem as well as its supply chain (see Figure 12).

PROOF automotive cyber maturity model

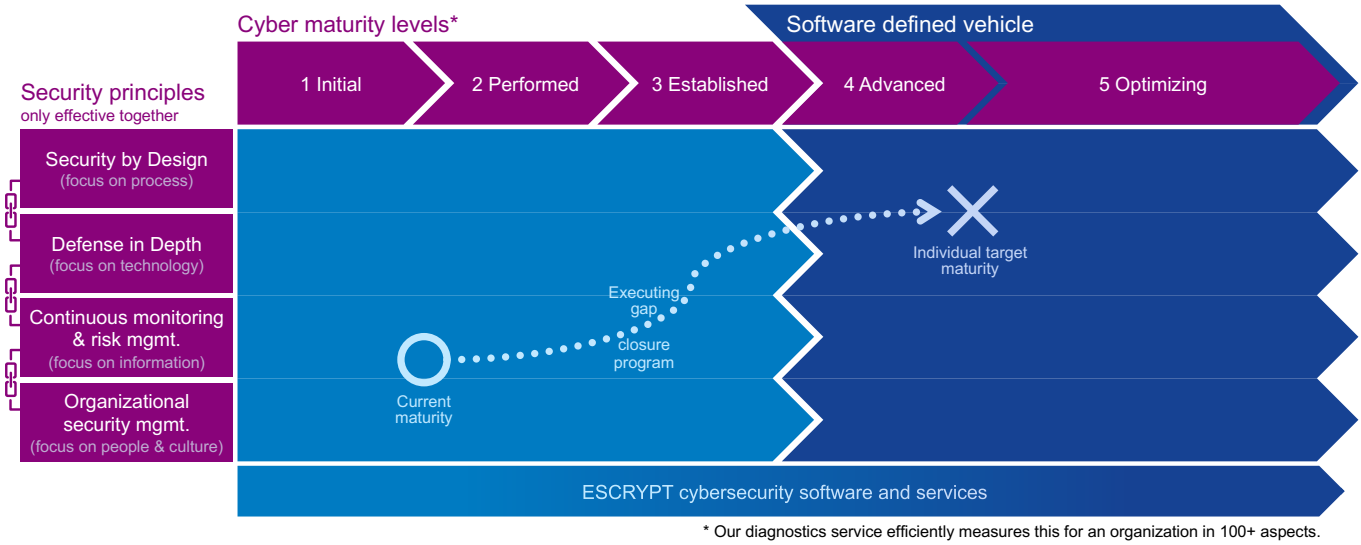
Figure 9 shows an extract of the PROOF (product security organization framework) cyber maturity model. Since its release in 2019, automotive companies ranging from specialized suppliers to globally leading manufacturers have used PROOF.

PROOF is built for automotive

- Diagnoses cyber maturity with over 120 automotive specific controls
- Considers national and international automotive security regulations and standards (incl. UNECE, ISO, CN, EU, JasPar, NHTSA)

PROOF is standards-based

- Based on ISO 33000 series (see Automotive SPICE)
- Uses five maturity levels like CMMI
- Developed by ETAS and KPMG in Germany, leveraging decades of experience in advancing cyber practices and building secure automotive systems.



* Our diagnostics service efficiently measures this for an organization in 100+ aspects.

Figure 11: Balancing cyber maturity and cyber risk of the SdV is a three-step process of assessing current maturity, setting target maturity, and executing a gap closure program.

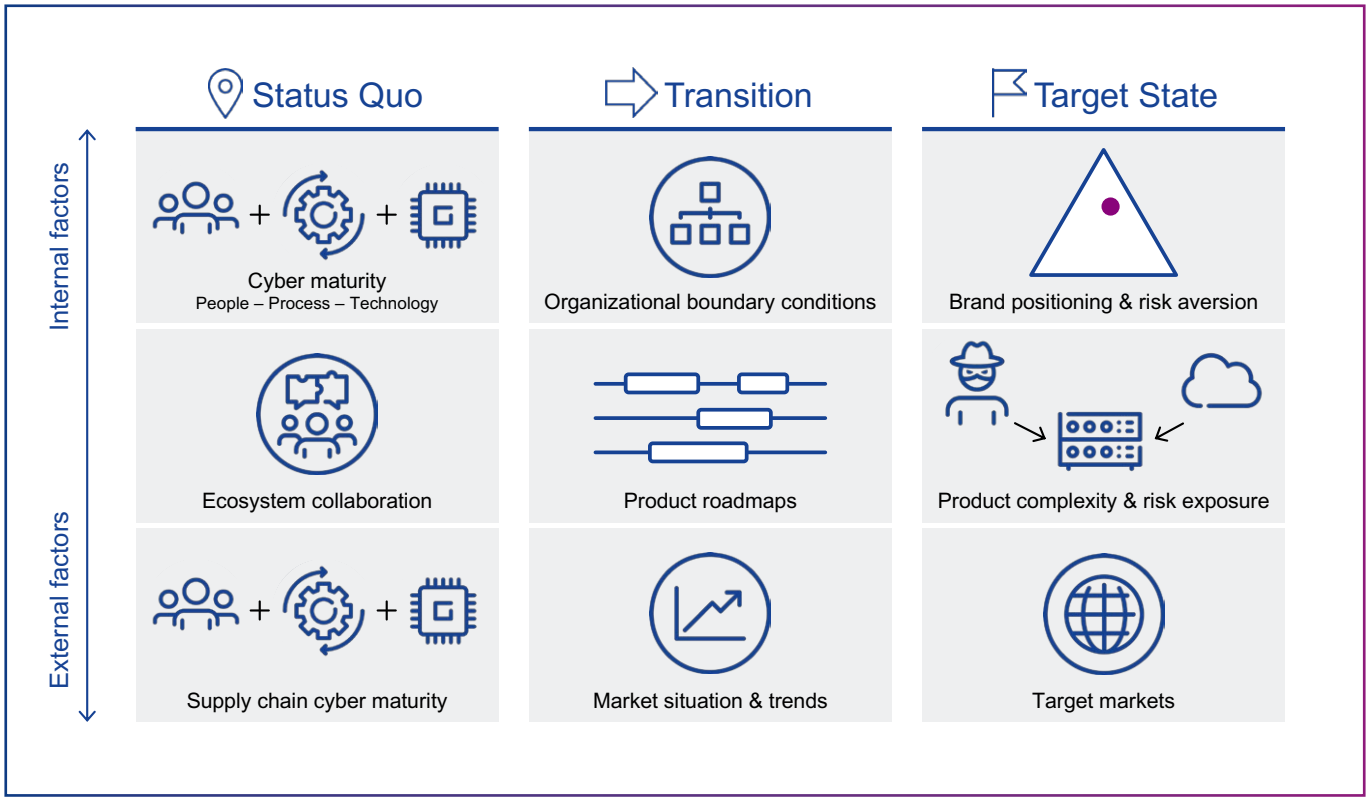


Figure 12: The automotive cyber maturity canvas maps relevant factors for a cyber maturity improvement program in two dimensions: factors that are internal/external and factors that relate to the status quo, the transition, and the target state.

4.2 Identifying target maturity

Identifying the target maturity is necessary to match the increasing cyber risk of the SdV with higher capability to secure road users, customers, and business models. If the growing capabilities and opportunities of (potential) attackers (see Figure 5) outpace the maturity of an organization, this will lead to unacceptable business risks. Conversely, setting the new target maturity too high risks a failure of the cybersecurity program due to wasted resources and overstretching the organization's ability to absorb and implement the necessary changes. We have found that three main factors decide the target level: the company's brand positioning and risk aversion, the complexity and risk exposure of its products, as well as requirements from target markets such as regulations and compliance requirements (see Figure 12). As each of these factors typically changes over time, we have found it helpful to introduce a stable interface between the requirements stemming from them along with the organizational and technical security controls a company considers.

4.3 Executing a gap closure program

Maturing an organization toward a new target state happens in multiple steps, much like the technical evolution towards the SdV happens in multiple phases (see Figure 8). This makes sense, as the goal is to match increasing cyber risk with increasing cyber maturity. Gross misbalance between risk and maturity will lead to failure, as discussed in the previous section.

Whereas initial-maturity organizations can be brought to the beginnings of established maturity in a waterfall-style planned project, the leap from established maturity to SdV-level maturity introduces the complexity typical of large-scale organizational change initiatives.

At initial maturity, organizations can directly benefit from our comprehensive library of tried and tested templates and process outlines. Technical security baselines, sometimes also referred to as security architectures, have proven effective in aligning security controls internally as well as with suppliers and customers. Together with the product roadmap,

the baseline can evolve and ensure that security measures continue to adequately protect from an increasing attack surface.

As organizations reach higher maturity levels, an iterative approach becomes more prevalent. Companies frequently assess their maturity and develop advanced capabilities through smaller, targeted changes (see Figure 13). This method ensures that organizations can accommodate boundary conditions, such as broader digitalization strategies or rapid market developments.

ETAS's unique experience can significantly reduce the number of iterations needed in this context. As an automotive company ourselves and with a robust professional services division that has supported automotive manufacturers and suppliers through numerous cybersecurity evolutions, we are adept at synchronizing the introduction of changes with the requirements of affected departments, including automotive engineering.

In conclusion, organizations can better reduce cyber risk and realize the potential of software-defined vehicles through a partnership with ETAS. Our integrated approach of automotive cybersecurity solutions with software and services covers all four security principles. Together, we will master the challenges and ensure a secure and reliable SdV landscape.

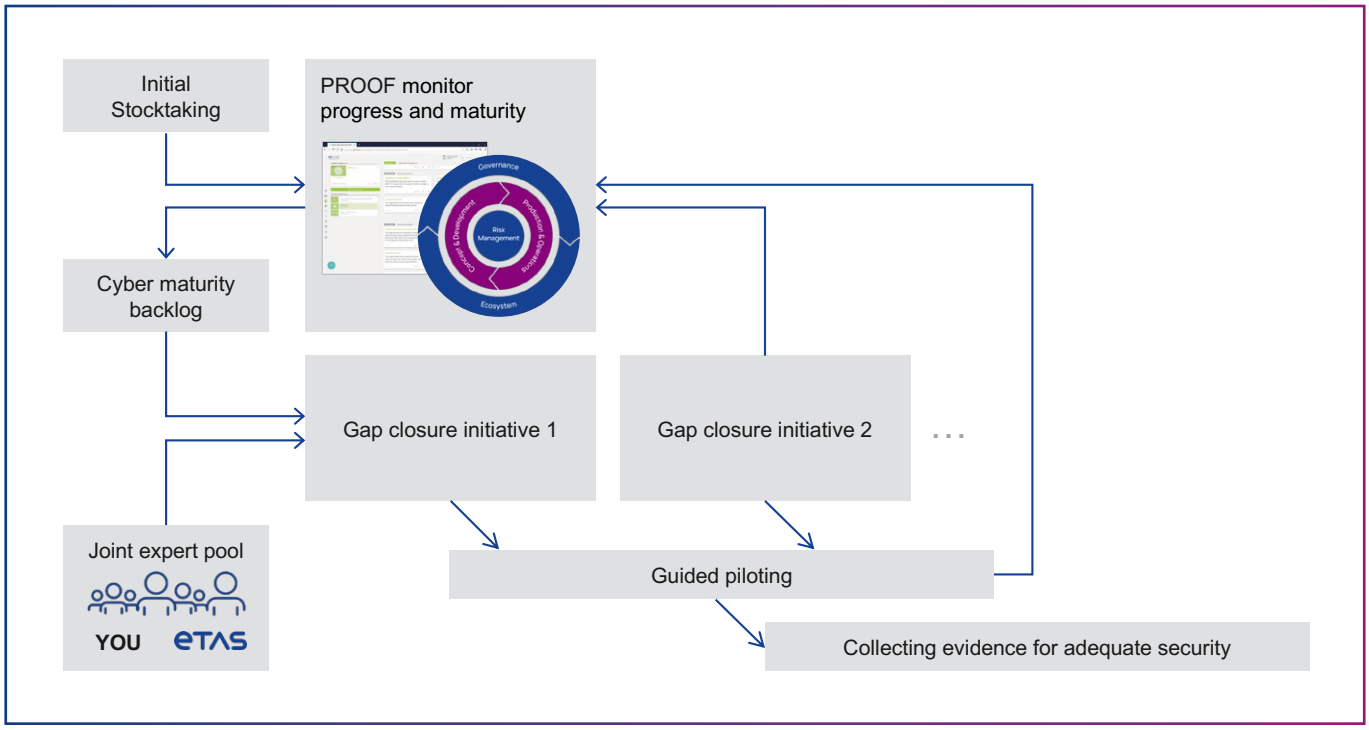


Figure 13: Focused and fast iterations ("gap closure initiatives") and transparent monitoring of current maturity allow companies to advance their maturity in an effective and targeted way.

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.

Bibliography

[1] **NHTSA,** "Safety Issues & Recalls (NHTSA ID 15V461000)," 23 07 2015. [Online]. Available: **https://www.nhtsa.gov/recalls** [Accessed 10 11 2022].

[2] **UNECE,** "UN Regulation No. 155 - Cyber security and cyber security management system," 04 03 2021. [Online]. Available: **https://unece.org/sites/default/files/2021-03/R155e.pdf** [Accessed 27 10 2022].

[3] **The State Council / The People's Republic of China,** "Opinions on Strengthening the Access Management of Intelligent Connected Vehicle Manufacturers and Products," 12 08 2021. [Online]. Available: **http://www.gov.cn/zhengce/zhengceku/2021-08/12/content_5630912.htm** [Accessed 28 10 2022].

[4] **Allianz,** Allianz Risk Barometer 2022, Munich, 2022.

[5] **E. Montalbano,** "Hackers remotely steer Tesla Model S using autopilot system (The security ledger)," 03 04 2019. [Online]. Available: **https://securityledger.com/2019/04/hackers-remotely-steer-tesla-models-using-autopilot-system/** [Accessed 27 10 2022].

[6] **S. Curry,** "Web Hackers vs. The Auto Industry: Critical Vulnerabilities in Ferrari, BMW, Rolls Royce, Porsche, and More," [Online]. Available: **https://samcurry.net/web-hackers-vs-the-auto-industry/** [Accessed 02 04 2023].

[7] **Upstream,** "Upstream's 2022 Global Automotive Cybersecurity Report," 26 January 2022. [Online]. Available: **https://www.israel21c.org/cyberattacks-on-cars-increased-225-in-last-three-years/**. [Accessed 05 09 2022].

[8] "NTT Global Threat Intelligence Report," 11 05 2021. [Online]. Available: **https://services.global.ntt/ja-jp/news-room/ntt-global-threat-intelligence-report-2021** [Accessed 05 09 2022].

[9] **E. Gately,** "Insured Losses from SolarWinds Hack Mount, But Could Be Worse," 20 Jan 2021. [Online]. Available: **https://www.channelfutures.com/mssp-insider/insured-losses-from-solarwinds-hack-mount-but-could-be-worse**

[10] **A. Bannister,** "NPM maintainer targets Russian users with data-wiping 'protestware'" 21 03 2022. [Online]. Available: **https://portswigger.net/daily-swig/npm-maintainer-targets-russian-users-with-data-wiping-protestware** [Accessed 11 05 2023].

[11] **CIS Center for Internet Security,** "Log4j Zero-Day Vulnerability Response," 07 01 2022. [Online]. Available: **https://www.cisecurity.org/log4j-zero-day-vulnerability-response** [Accessed 11 05 2023].

[12] **R. A. Grimes,** "Zero-days aren't the problem – patches are," 01 June 2016. [Online]. Available: **https://www.csoonline.com/article/3075830/zero-days-arent-the-problem-patches-are.html** [Accessed 16 05 2023].

Contacts

Michael Lüke
Senior Manager
michael.lueke@etas.com

Dr. Moritz Minzlaff
Head of Professional Security Services
moritz.minzlaff@etas.com