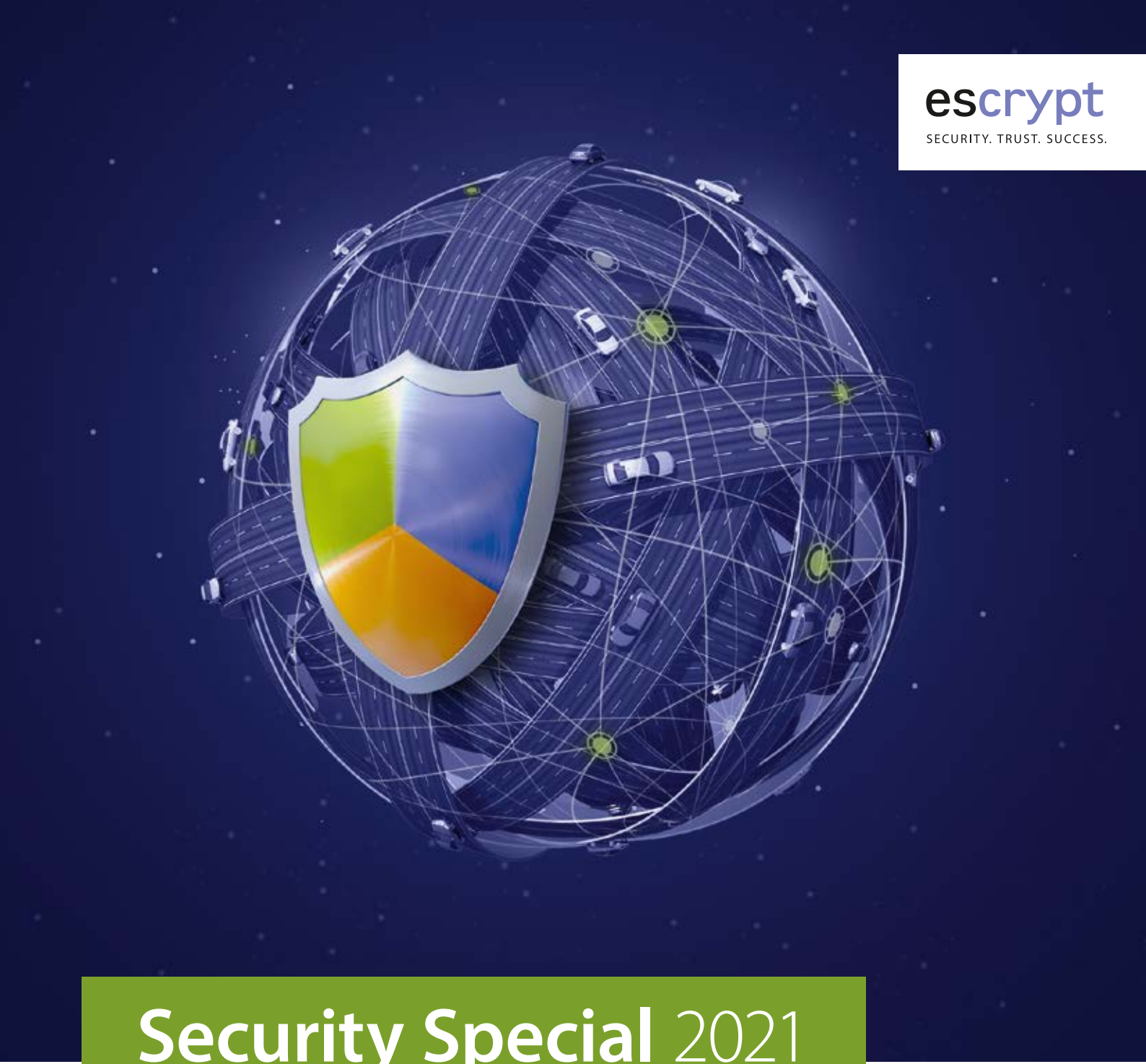
escrypt
SECURITY. TRUST. SUCCESS.



Security Special 2021

INTERVIEW

AUTOSAR meets intrusion detection

PENTESTING

Putting automotive security to the test

SECURITY MONITORING

An eye on the vehicle fleet

www.escrypt.com

“Securing vehicles permanently and in a multilayered way”

Marcel Mulch and Dr. Michael Peter Schneider link AUTOSAR and IDS

In the future, the continuous risk management of vehicles in the field must be based on effective intrusion detection. Marcel Mulch, Security Architect Intrusion Detection System (IDS), and Dr. Michael Peter Schneider, Project Manager AUTOSAR Security and representative in the AUTOSAR consortium, explain the important role that the AUTOSAR standard plays and where it reaches its limits.

Mr. Schneider, we know that AUTOSAR is the software standard for E/E architecture. To what extent is it important for vehicle cybersecurity?

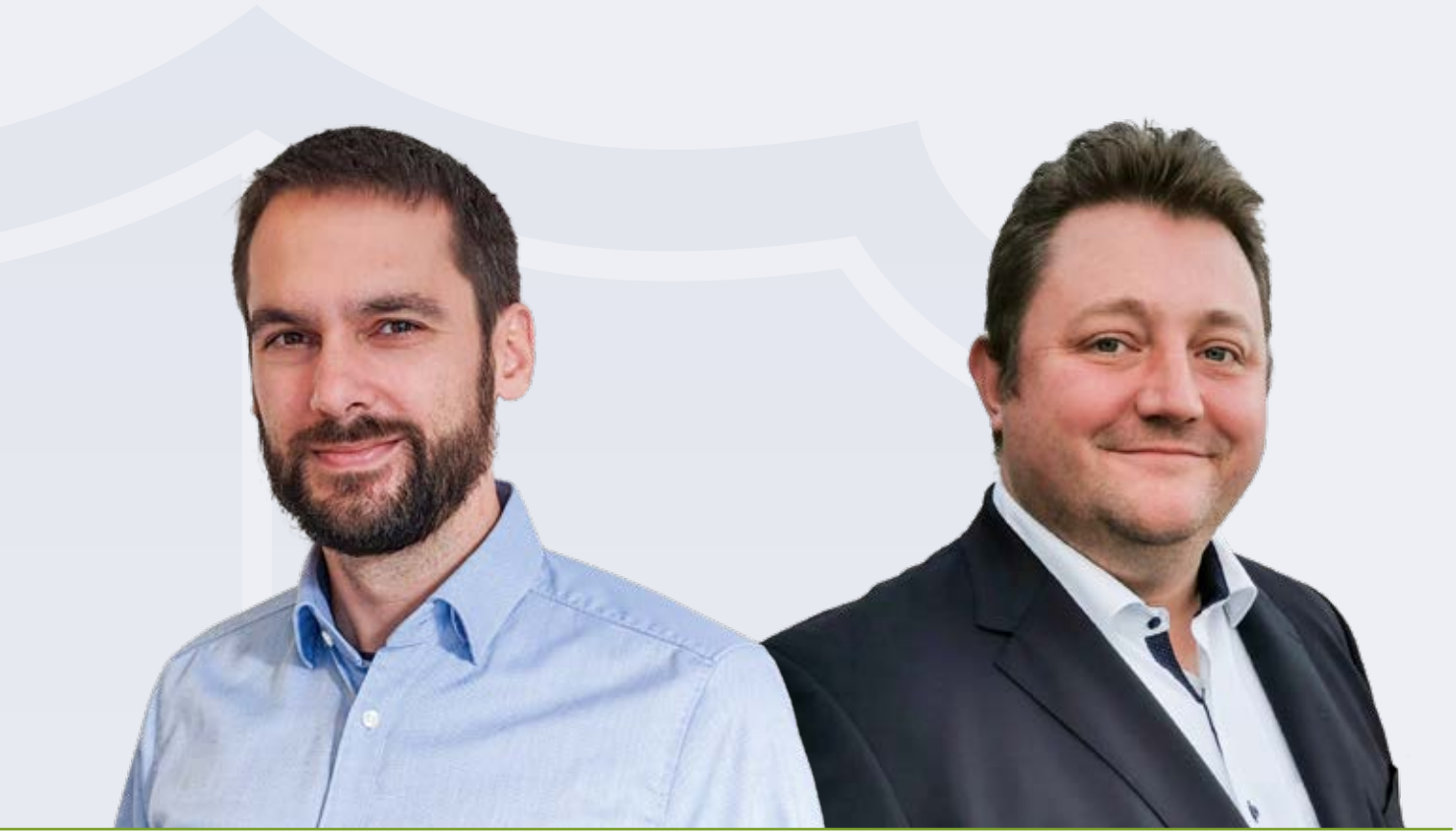
Michael Peter Schneider: It’s quite straightforward. The broad range of AUTOSAR components that can be used for in-vehicle applications includes several security modules. One great example is the SecOC. This is a well-known standardized protocol specially developed by the AUTOSAR consortium to secure onboard communication in the vehicle. There are now quite a few specific AUTOSAR security components of this type, including a crypto stack or one for identity and access management. AUTOSAR defines the specifications that embedded software providers such as ETAS need to implement in their AUTOSAR stacks for OEMs and suppliers.

Since the end of 2020, there have also been AUTOSAR specifications for intrusion detection in the vehicle using an intrusion detection system, or IDS for short. Why IDS and why now?

Marcel Mulch: The main reason is the new UNECE regulations for automotive cybersecurity. In order to receive type approval in the future, manufacturers must prove that they can detect and mitigate cyberattacks on their vehicle fleets. An IDS, which monitors communication in the electrical system and detects anomalies and typical intrusion signatures, is essential. That is why the sensors for intrusion detection in the vehicle network are standardized according to AUTOSAR. What is known as the IDS manager then collects the potential security events registered by the sensors and pre-filters them for forwarding to a vehicle security operations center in the backend. The big advantage is that, since AUTOSAR is now widely used for E/E architectures and is already applied in many ECUs, it is relatively easy to integrate the IDS components specified by AUTOSAR.

Are the security modules contained in AUTOSAR enough to adequately protect the vehicle against cyberattacks?

Schneider: Not really. AUTOSAR and its security modules are only one aspect of this, albeit an important one. It’s not only AUTOSAR ECUs that are built into the vehicle, but also microprocessor-based systems such as telematics units, infotainment systems, and vehicle computers that rely on native operating systems such as Linux, QNX, or Android. In addition, vehicle networks are becoming increasingly complex and automotive Ethernet is becoming more and more important. That is why



Dr. Michael Peter Schneider
Project Manager AUTOSAR Security

Marcel Mulch
Security Architect Intrusion Detection System

network sensors that, for instance, monitor Ethernet traffic on domain controllers are also needed. And even on classic ECUs, IT security beyond AUTOSAR can be further improved with, say, hardware security modules for the secure management of key material or with automotive-specific crypto libraries.

"AUTOSAR makes it easy to integrate IDS components"

Mulch: That also applies to the continuous security monitoring required by UNECE. The IDS components specified by AUTOSAR are important elements here. But in addition to AUTOSAR, it's also important to have an IDS reporter in the vehicle to report all potential security events to the backend – the vehicle security operations center – for evaluation, where the alleged attacks are investigated using software and security analysts. And it requires a security update management system, which ultimately – again with AUTOSAR support – closes security gaps and, if necessary, adapts the IDS sensors to the new risk situation. In other words, from a security point of view, the only thing that matters is which attack vectors the particular E/E architecture has and how it can be protected. I'm happy to use AUTOSAR security modules wherever they fulfill the purpose; otherwise, I use additional security measures.

What are your thoughts on the future? What role will AUTOSAR still have in the E/E architecture in ten years' time, and what role will intrusion detection then play in the vehicle?

Mulch: I am convinced that in ten years' time, AUTOSAR will still play a central role in vehicle architecture as a common software standard. But then the weight will definitely have shifted from AUTOSAR Classic to AUTOSAR Adaptive. The E/E architectures will be tailored to a few powerful central computers and will move toward using microprocessors instead of microcontrollers. But that's exactly what AUTOSAR Adaptive is designed for.

Schneider: At the same time, the new binding rules and regulations show how important security is for increasingly connected and automated mobility. For the safety of all of us, we will have to secure the vehicles and fleets permanently and in a multilayered way. I am sure that onboard IDS solutions and the associated monitoring of the fleets by a vehicle security operations center will be standard in future vehicle generations.

The acid test for cybersecurity

Penetration testers simulate attacks on automotive systems

With increasing vehicle connectivity and automation, IT security functions have long since become an indispensable part of the in-vehicle network and its components. But when it comes down to it, how safe are the ECU and vehicle network really from unauthorized access and manipulation? Penetration testing, or pentesting, is one of the most effective methods for answering this question. It involves the tester uncovering potential IT security gaps by attempting to penetrate the system – similar to the way a real attacker would.

In the automotive sector, pentesting is typically used to test individual ECUs, several ECUs in a network, or even complete vehicle platforms. It often starts at a late stage in the development process, when at least some of the functions essential for the test are complete. Unlike purely automated test procedures, pentesting includes an in-depth, customized examination of the system by a security expert under realistic conditions. The results are often decisive for the system's marketability and approval for market launch in terms of IT security. And in some cases, pentests can also be useful and necessary even after the start of production – for example, if security gaps unexpectedly appear when the vehicle is in the field, key tests are missed, or new attack techniques become known (Figure 1).

Comprehensive testing expertise required

As a rule, penetration testers start off by using automated testing tools – ideally ones that can be adapted to the specifications of certain vehicle platforms or even individual ECUs. These automated tools quickly find known weaknesses in widely used services and protocols. However, this serves only as a basis for the pentesters' actual work, which involves analyzing in depth the anomalies that the testing tool reveals. They do this by scrutinizing every last detail of the underlying data, data traffic, processes, and source code. They also consult other experts, search databases for attacks on similar targets, and piece together several errors that may appear harmless on their own but, when combined, create complex and potentially dangerous chains of attack. Manual pentesting by a security expert is the only way to gain a comprehensive understanding of the IT security that the test system offers in the event of an elaborate cyberattack.

White box: The more information, the more efficient the test

Accordingly, the pentesting team draws on all the available techniques and test methods, conducts fuzz tests, vulnerability scans, and side-channel analyses, and carries out code audits as well as tests of the physical system and its security functions. It should be noted that the more a pentester knows about the system, the better equipped they are to effectively test its level of cybersecurity, identify weak points, and make suggestions for improvement. For that reason, pentests should ideally be carried out as white-box tests, which means the customer should provide as much information as possible: source code, residual bus simulation, complete documentation, development and diagnostic tools, access to the backend, etc. With black-box or grey-box testing, however, this information is available only in part or not at all. For that reason,

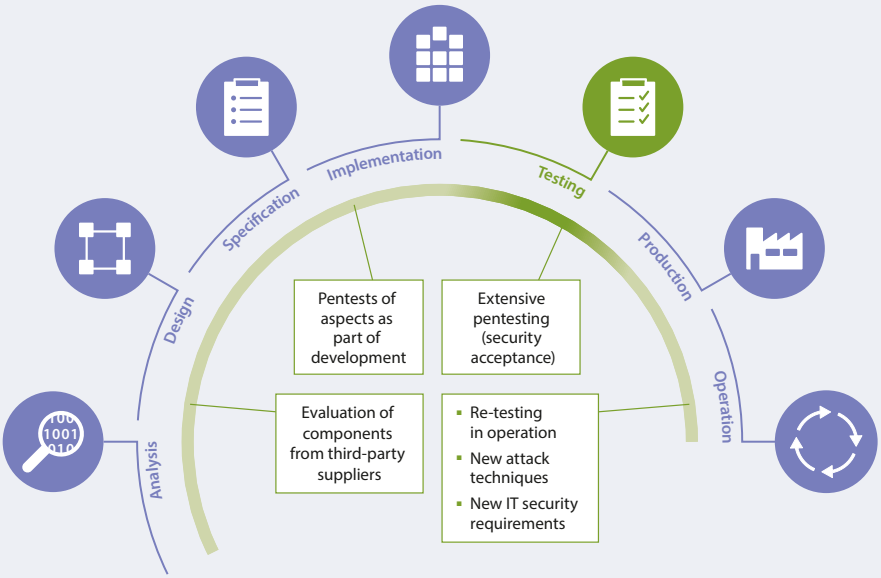


Figure 1: Penetration tests are often performed toward the end of the development process; in some cases, they are also useful in other phases of the product lifecycle.

these methods are used only if the tester is not authorized to access the information, for example for legal reasons, or if the customer's source code is not available.

Iterative approach

Penetration testing always takes an iterative approach: identify potential points of attack and locate and probe existing weaknesses. The testing team then presents the existing security gaps and associated risks to the customer, and advises them on effective countermeasures. Accordingly, a detailed test report is provided at the end of each pentest. This report lists the identified points of attack, applied test procedures, and all findings in detail. It also highlights possible solutions. The customer uses this report to close the identified IT security gaps, and retests confirm that either the system is sufficiently protected or that further security measures are required (Figure 2).

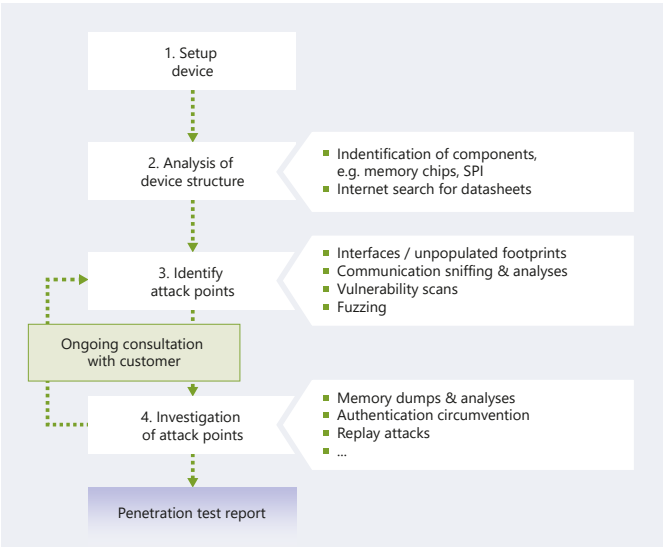


Figure 2: Sequence of automotive pentesting operations.

The highly sophisticated discipline of pentesting

With the new UNECE WP.29 regulations and the forthcoming ISO/SAE 21434 standard, certified cybersecurity management will very soon become a prerequisite for type approval. A security test strategy that fully penetrates the vehicle platforms, includes the supply chain, and addresses the vehicle lifecycle is crucial. This is where the highly sophisticated discipline of pentesting comes in as the acid test for cybersecurity: by encompassing the test system both in detail and as a whole, pentesting uncovers IT security gaps before an attacker has the chance.

Authors:
Thomas Enderle is Lead Security Specialist in Security Testing at ESCRYPT.
Dr. Martin Moser is Head of Consulting & Testing Munich at ESCRYPT.

UNECE security mandate

New UN regulations require management of cyberrisks throughout the entire product lifecycle

Once the UNECE WP.29 regulations go into effect, automotive cybersecurity will finally be mandatory. OEMs that want type approval for their vehicles in the signatory countries will soon have to demonstrate that they have a certified cybersecurity management system in place.

In June 2020, the UNECE World Forum for Harmonization of Vehicle Regulations adopted long-awaited regulations on cybersecurity (UN R 155) and software updates (UN R 156) for connected vehicles. In the EU, the new regulations will be binding for type approval of new models starting in mid-2022. The regulations will apply to existing architectures as of 2024. Japan and South Korea plan to join the agreement as well. Automotive manufacturers that want to sell vehicles on these markets must fulfill the new cybersecurity requirements. At the same time, the industry expects the ISO/SAE 21434 standard in 2021 and, in the following year, the ISO/AWI 24089 standard to come into effect, which will further specify the implementation of the UNECE regulations.

Four disciplines

UNECE WP.29 outlines clear core requirements, namely: the operation of a certified cybersecurity management system (CSMS) and a software update management system (SUMS) as well as the implementation thereof during development of the vehicle type. Taking a risk-based approach, OEMs must consistently determine, reach, and maintain an appropriate level of IT security for each vehicle type, its external interfaces, and its subsystems. They are explicitly called on to take into account security-relevant dependencies and information from suppliers, service providers, and other players as well (Figure 1). Furthermore, the new regulations also focus on the phase after the start of production and on continuous risk management for vehicles in the field. Accordingly, the regulations specify four disciplines:

- Managing cyberrisks to vehicles
- Securing vehicles "by design" to mitigate risks along the value chain
- Detecting and responding to security incidents across vehicle fleets
- Safely and securely updating the vehicle software, including a legal basis for over-the-air updates

Organization and procedural hurdles

This is the first time that automotive industry regulations have stipulated a process approach to organizing IT security management. The first discipline – managing cyberrisks to vehicles – is especially important. As a superordinate maxim for action, it must map the other "sub-" disciplines – security by design, risk management for the fleet on the road, and over-the-air security updates – at the company and process level. Extensive expertise from management system experience, compliance, and automotive security must all be brought together to establish an effective CSMS (Figure 2).

Type approval: Cybersecurity management during development

The time pressure is intense: even before the new regulations become binding, OEMs have to demonstrate that they are taking appropriate security measures. To this end, they have to establish a CSMS with a valid certificate of compliance and apply it when developing new vehicle types. They must identify potential points of attack and define, implement, and verify protective measures throughout the entire development process. To achieve type approval, OEMs need to answer the following questions:

- *Are all necessary artifacts available to prove that development was in line with the CSMS?*
  Even if they have not yet established a certified CSMS, OEMs must create and document artifacts (risk analyses, proof of security measures, security architecture, security tests, etc.) to demonstrate that they have designed their development process to be governed by a CSMS.
- *What are the critical elements of the E/E architecture?*
  A readiness check plus analysis answers three questions: what technical measures in the E/E architecture have already been affected, what potential security gaps there are, and what it will take to close them.
- *How can OEMs implement appropriate technical cybersecurity measures in accordance with UNECE WP.29?*
  In its specifications, UNECE WP.29 requires the vehicle manufacturer to provide a differentiated risk assessment for the vehicle type as well as proof that it has taken appropriate action to mitigate the identified risks. This means that during the development process, the OEM must implement those IT security components and mechanisms that ensure security is sufficient at the time of type approval for the E/E architecture, both in its individual systems as well as in their communication with each other and with the outside world.

Appraisals lead to a future-ready CSMS

This relevance for type approval means it is necessary to implement all requirements as efficiently as possible on the first attempt.

Figure 2: The CSMS domains cover the four disciplines of the regulations.

Appraisals provide a basis for this as a way to identify building blocks already in place, such as tried-and-true functional safety processes or existing management systems. They also highlight existing gaps and guide OEMs in drawing up bespoke implementation plans. When conducting appraisals, it is important to note that UNECE-compliant CSMS will be required for existing architectures as of 2024. If cybersecurity programs are to succeed, OEMs need automotive security partners with CSMS experience who can help them mobilize their own potential.

Authors:
Dr. Moritz Minzlaff is Senior Manager at ESCRYPT.
Dipl.-Ing. Thomas Stimm is Security Engineer at ESCRYPT.

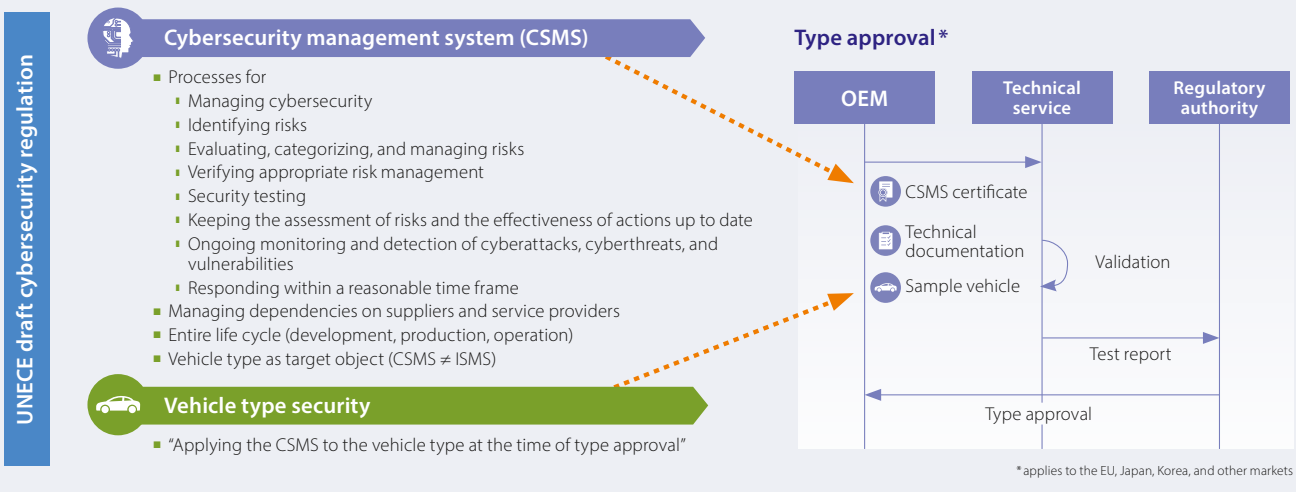
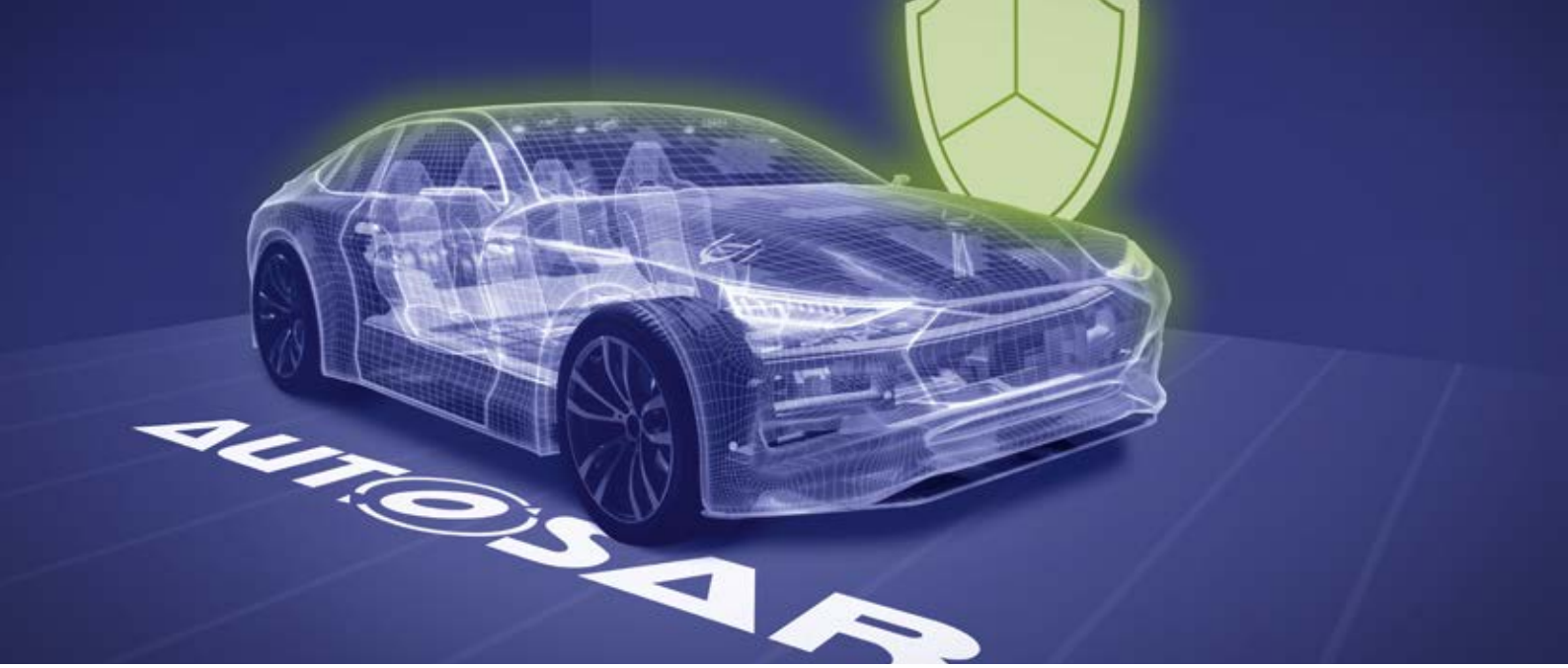


Figure 1: Certified cybersecurity management system (CSMS) and type approval according to UNECE regulations.



Cybersecurity included

Security for AUTOSAR Adaptive architectures

The path to a smart connected vehicle goes through AUTOSAR Adaptive. To provide reliable protection against cyberattacks, this standard features security functions that can be integrated today into tomorrow's E/E architectures.

AUTOSAR Adaptive provides the framework for new E/E architectures. In smart, highly automated vehicles, high-performance domain controllers (DCUs) and vehicle computers (VCs) will take control. Against this backdrop, high data loads under real-time conditions call for powerful security mechanisms, which is why a range of security functions have been integrated into AUTOSAR Adaptive today (Figure 1).

Security modules in AUTOSAR Adaptive

- In AUTOSAR Adaptive, the targeted provision of cryptographic primitives, keys, and certificates is performed by the **crypto stack** (crypto API). Regardless of the crypto implementation, the applications access only the interfaces provided by the crypto stack, which increases the portability of applications to different ECUs.
- **Secure communication** is provided in AUTOSAR Adaptive with the help of TLS and IPSec. Both protocols enable the simple establishment of secure connections not only within the vehicle, but also with external instances such as the OEM backend. In addition, since the end of 2020, specifications have called for a protocol for SecOC (secure onboard communication) that is specific to AUTOSAR Adaptive.
- The AUTOSAR **identity and access management** module ensures that only authorized applications gain access to certain critical resources (e.g. sensitive data in the persistent memory, communications channels, cryptographic keys). These access rights can be configured in AUTOSAR Adaptive as required and updated at any time.
- An important component of effective security management throughout the vehicle lifecycle is an **intrusion detection system** (IDS) that detects attacks on the vehicle and reports them to a backend. For this reason, the IDS manager (IdsM) is the latest feature to be integrated into AUTOSAR as a crucial control point for a distributed IDS.
- The **secure update function** in AUTOSAR Adaptive then helps fix any identified weaknesses by receiving and processing security updates for individual applications or even for the entire platform. The individual update blobs are signed by the backend, so that only updates from trustworthy sources are executed.
- ECU, DCU, and VC applications must also be verified at regular intervals. This task is conducted by either secure boot or the **trusted platform function** in AUTOSAR, which verifies all applications as well as the platform itself. This ensures that only trusted software is executed.

RTA-VRTE: Platform software framework for AUTOSAR Adaptive

An ideal basis for implementing AUTOSAR Adaptive-compliant processes along with security functions is the ETAS Realtime Application Vehicle Runtime Environment (RTA-VRTE) platform software

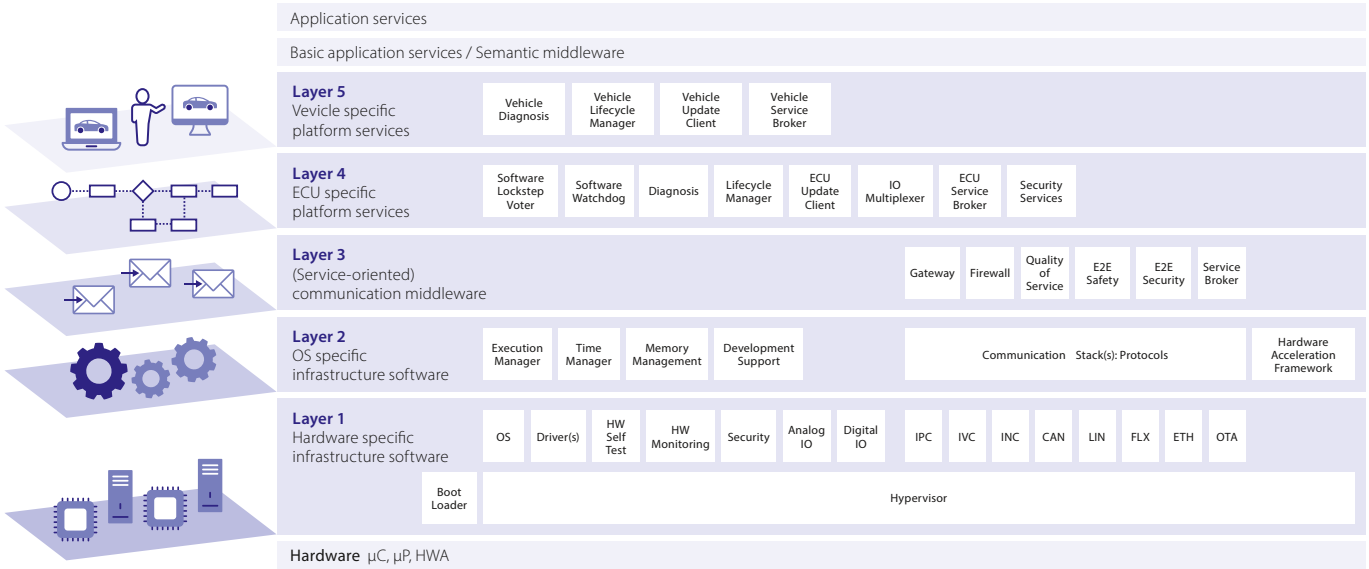


Figure 2: The RTA-VRTE layer model supports the important software functions and requirements on five levels.

framework. RTA-VRTE contains all the important middleware elements for microprocessor-based vehicle computers and enables the function of virtual ECUs to be simulated on conventional desktop PCs and networked via Ethernet. RTA-VRTE creates a virtual machine consisting of four layers of basic software architecture, with a fifth layer for vehicle-specific platform services (Figure 2).

Levels 1 and 2 contain the infrastructure software for the hardware used (e.g. device drivers) and a POSIX-compliant operating system. Level 2 also contains execution management, which enables the platform to manage the dynamically assigned applications, ensure that they are started and stopped correctly, and monitor the resource and execution limits. Execution management is thus a key function in IT security, providing the trusted platform and verifying the integrity and authenticity of Adaptive applications.

Early Access Program as start-up aid

On level 3, communication middleware ensures that the dynamic Adaptive applications and the other software applications can be integrated into the system. At the same time, the RTA-VRTE communication management controls the exchange between the levels and guarantees the smooth operation of the encapsulated software, including the ECU- and vehicle-dependent platform services on levels 4 and 5. Such a level of security in end-to-end communication among authenticated applications is extremely crucial for cybersecurity.

RTA-VRTE is already being used worldwide in the development of AUTOSAR Adaptive vehicle platforms ready for large-scale production. In addition, ETAS and ESCRYPT offer an Early Access Program (EAP) that enables OEMs and suppliers to explore the development methodology for future E/E architectures, including the security components already available through AUTOSAR Adaptive.

Authors:
Dr. Michael Peter Schneider is Project Manager AUTOSAR Security at ESCRYPT.
Dr. Stuart Mitchell is Senior Product Manager RTA-VRTE at ETAS.

Security components in AUTOSAR Adaptive

- **Crypto stack** for managing key material and access to crypto primitives
- **Secure communication** via established protocols TLS and IPSec
- **Access protection** for sensitive resources (e.g. keys) through the Identity & access management module
- **Intrusion detection** by IDS sensors and distributed IDS managers (IdsM)
- **Secure updates** for everything from individual applications to the complete platform
- **Authentic software** thanks to continuing the secure-boot trust chain as part of the trusted platform

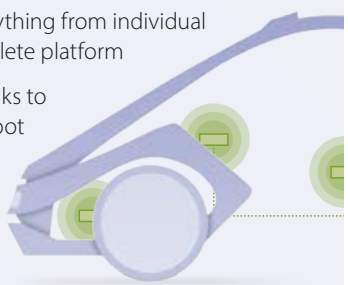


Figure 1: AUTOSAR Adaptive provides key security modules.

A constant eye on the vehicle fleet

Efficient risk management through integrated intrusion detection and protection

The cybersecurity of connected vehicles is short-lived. Consequently, UNECE regulations require that OEMs and fleet operators provide effective security risk management throughout the entire vehicle lifecycle. The key elements for achieving this are attack detection via IDS in the vehicle and a vehicle security operations center (VSOC).

No matter how high the level of protection against cyberattacks established during development, it will inevitably diminish over the course of the vehicle's service life. For that reason, vehicles and vehicle fleets will require an active, ongoing security approach in the future, one that monitors known risks and attack vectors and also identifies and mitigates new risks. This is especially important because when the UNECE WP.29 regulations come into force, it will become mandatory for type approval to furnish proof of appropriate risk management throughout the vehicle lifecycle.

Obtaining a meaningful picture of the overall threat situation requires examination of several areas and action on several levels. Two key components are necessary: first, embedded in-vehicle attack detection in the form of an intrusion detection system (IDS); and second, a vehicle security operations center (VSOC) in the backend, where the attacks are aggregated and evaluated to prevent scaling of attacks across the entire fleet.

In-vehicle intrusion detection system

A connected vehicle fleet is comparable to a distributed hierarchical IT system; merely protecting access to the system (protect at the gate) is not enough. Truly effective security monitoring calls for attack detection that is embedded deep in the distributed system. In particular, to detect local attacks on a specific vehicle – such as attempted manipulation via the OBD interface or unauthorized access to the locking system – intrusion sensors, integrated into the E/E architecture of the individual vehicle, are indispensable. In following the UNECE-compliant risk-based approach for lifecycle security, two important tasks emerge: first, investigate right from the vehicle development stage what potential vulnerable points could exist in the E/E architecture; and second, incorporate this knowledge into a consistent monitoring concept based on a distributed intrusion detection system (IDS) in the vehicle's internal network.

The core components of this kind of IDS are the IDS sensors, which monitor data traffic and system behavior in the ECUs and, among other things, compare them to the "normal behavior" specified by the OEM. Suspicious activities (such as anomalies in cyclical messages or abusive diagnostic requests) are logged by the IDS sensors as security events. Sensible placement of smart IDS sensors (in a gateway, for example) allows them to monitor all CAN data traffic and also keep track of all Ethernet communication via an automotive firewall/IDS solution built into the Ethernet switch. In this way, even highly complex attacks can be detected and false-positive security events can be filtered out.

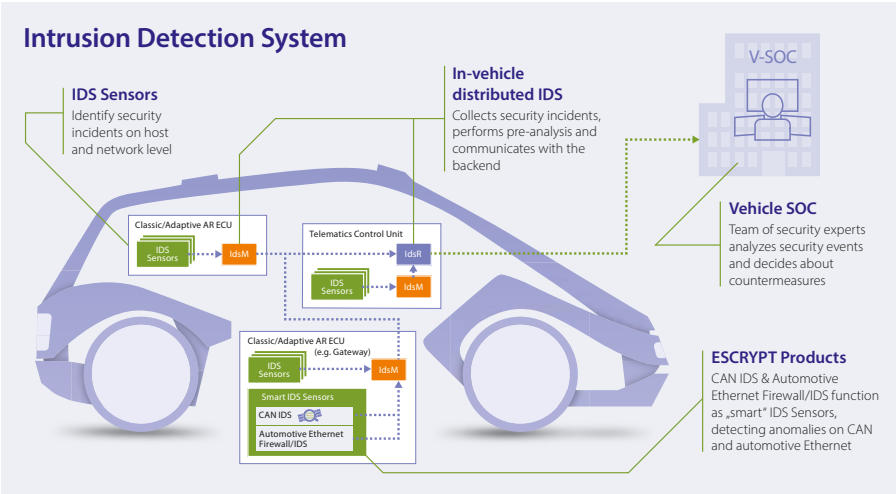


Figure 1: Distributed system for attack detection in the vehicle – from the IDS sensor to the IDS manager to the IDS reporter.

It is important to group together the information from the individual IDS sensors in a productive way and to run data through an initial analysis inside the vehicle so as to optimize it for transmission to the vehicle security operations center (VSOC) in the backend. This task is performed by distributed IDS managers (IdsMs) in the ECUs; they collect the security events from the IDS sensors allocated to them, filter out non-relevant events and noise, and pass the cleaned-up information on to the IDS reporter (IdsR) in the telematics unit. There, in the IdsR, all security events from the vehicle converge and are transmitted to the VSOC following further preliminary analysis (Figure 1).

VSOC: Intelligence in the backend

The vehicle security operations center (VSOC) has four tasks: continuously evaluate security events from the entire fleet as communicated by the in-vehicle IDS, plus further data relevant to IT security from the connected automotive ecosystem; validate the events and data with regard to particular anomalies; analyze acute and potential threats; and derive suitable countermeasures. To carry out these tasks, the VSOC draws on two instances that work together in a complementary fashion: automated analysis by security incident and event management (SIEM) and in-depth review of individual incidents by specialized automotive security analysts.

First, SIEM collects all IT security events reported to the OEM backend and subjects them to automated real-time investigation and analysis. To do so, modern SIEM solutions can develop their own models using machine-learning functionalities. Via dashboards and security reports, SIEMs directly illustrate the current risk situation. However, SIEM solutions are ill-suited to detecting intrusion scenarios that are new and unknown. Specifically in automotive security environments, moreover, with components that are specially developed for the vehicle platform, there are no standard vulnerability management solutions that could be directly connected to SIEM.

This is why it is essential to technically implement a SIEM solution in the VSOC so as to complement specialized technical- and content-related functionalities. This includes an integrated threat intelligence solution, which looks for new indicators of compromise and attack methods in its own database and also shares the resulting findings with other (V)SOC operators. But most of all, the VSOC needs highly specialized automotive security experts who analyze the attack pathways and expand the methodology for threat detection, such that SIEM and IDS sensors will automatically register new threat scenarios in the future and check the fleet retrospectively for the existence of such attacks. By bringing together automatic analysis and human expertise, a VSOC supplies the fleet operator with actionable information that enables the latter to develop and roll out suitable countermeasures (Figure 2).

Alignment of vehicle components and VSOC

The ongoing risk minimization is based on distributed intrusion detection in the vehicles and in-depth incident assessment in the VSOC. However, the processing of data from connected vehicles is not without its own challenges. And given how limited and poten-

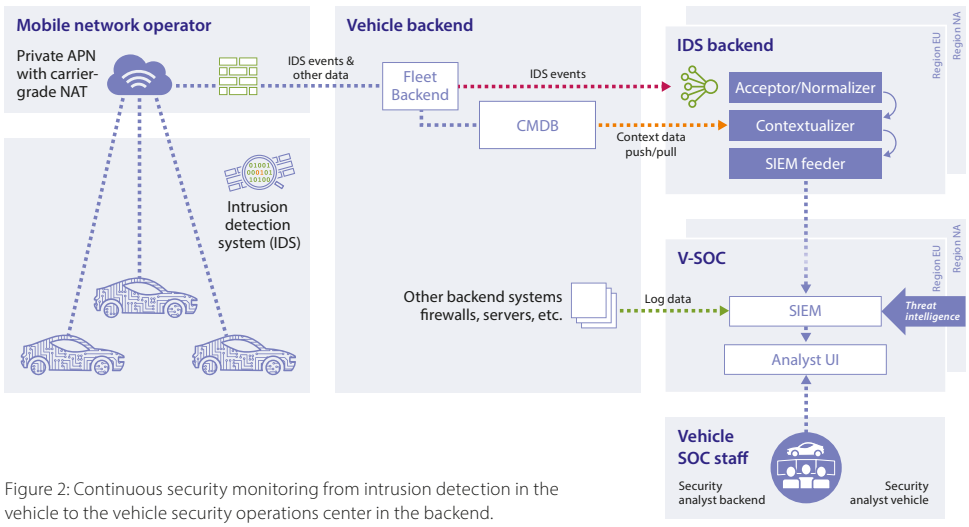


Figure 2: Continuous security monitoring from intrusion detection in the vehicle to the vehicle security operations center in the backend.

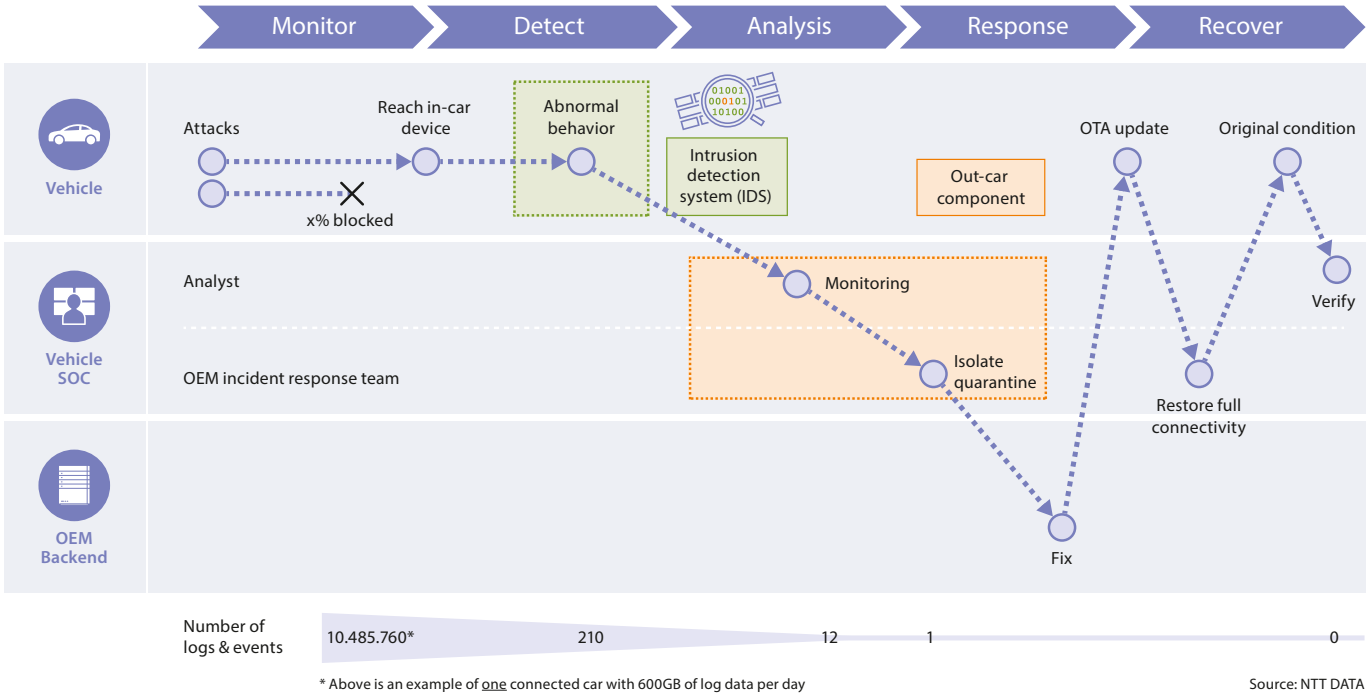


Figure 3: Security incident management journey – The IDS detects anomalies and typical attack signatures, thus reducing the bandwidth requirements for security monitoring information.

tially expensive data transmission is with today's vehicles, it is important to determine exactly what data the VSOC actually needs for its assessment. Preprocessing and aggregating the data in the vehicle can reduce its volume accordingly – this is a sensible approach also because, in the future, VSOCs may be collecting data from millions of vehicles.

In addition, the VSOCs need to enrich the data in an automotive-specific way, taking into account typical threat scenarios and specific knowledge of vehicle architecture and the components used there. Then SIEM's automated processing should prepare and group the data and events so that analysts can further process them in a focused and efficient fashion. Ideally, this means the findings from the field data for millions of vehicles will be "encoded" in the rules by the automotive security experts on an ongoing basis. Among other things, that will optimize the classification of "false reports" and steadily improve the detection rate in the system. The result is a learning system for intrusion detection and prevention (IDPS), which traces the traditional cycle from monitoring to response and recovery (Figure 3).

Worldwide security infrastructure

The new UNECE regulations will require OEMs and fleet operators to protect their vehicle fleets from cyberattacks across their entire lifecycles. With in-vehicle attack detection using IDS, an effective solution is already at hand: IDS components are mature and their standardization, in AUTOSAR and elsewhere, ensures their interoperability. In addition, the regulations call for VSOCs to be prepared to analyze detected attacks and irregularities and respond with appropriate countermeasures.

But cyberattacks recognize no national borders, and thanks to global supply chains, any vulnerabilities are rarely restricted to just one OEM or Tier 1 supplier. The situation demands a global infrastructure for constant vehicle security monitoring – ideally with partners who offer the right technologies and the necessary automotive security expertise on a global scale.

Authors:
Dr. Jens Gramm is Senior Project Manager Vehicle Security Operations Center at ESCRYPT.
Dr. Jan Holle is Lead Product Manager Intrusion Detection & Prevention Solutions at ESCRYPT.

ESCRYPT partners with NTT on IT security for fleet vehicles

ESCRYPT has joined forces with the security division of the IT technology and service provider NTT on cyberresilience for vehicle fleets. The two companies will be jointly offering holistic solutions that combine embedded IT security in vehicles with continuous monitoring and central security management, making them particularly suited for the security of vehicle fleets.

Automotive manufacturers and fleet operators will need powerful protection systems whose effectiveness extends beyond the vehicle to the mobile network and backend. Such systems also have to monitor all IT and telecommunication systems associated with the connected car throughout the vehicle lifecycle to detect anomalies and shield the systems from attack. This is precisely where the ESCRYPT-NTT partnership comes in: it combines in-depth know-how in automotive security with experience in enterprise IT security and in designing and running security operations solutions.

CycurLIB fulfills ASIL D requirements

In accordance with ISO 26262, the process ESCRYPT used to develop the current version of its CycurLIB crypto library is in line with ASIL D. This means that OEMs and suppliers can now easily integrate the cryptographic library into all safety-relevant vehicle systems up to the highest security level, without runtime overhead, loss in performance, or interference with other applications.

ASIL D classification means that it is possible to use CycurLIB in conjunction with safety-critical software on a shared controller – with freedom from interference. CycurLIB provides suitable algorithms, formats, and encryption protocols for safety-relevant use cases in the vehicle (e.g. driver assistance systems, steering, and braking system). It is also platform-independent and its configuration system is compatible with AUTOSAR. The crypto library thus supports a range of functions, including secure flashing and booting of the systems, signature verification for firmware updates, and access via the OBD2 interface.