New E/E architectures

To prevent the joint venture from becoming a cyber risk

Automakers are rapidly moving towards Software-Defined Vehicles (SDVs). Partnerships with other OEMs promise greater development power and better access to regional markets. But how can necessary cybersecurity for vehicles be guaranteed, given the different technologies and processes used by these partners?

Cybersecurity in collaboratively developed E/E architectures.

Picture: ETAS

Volkswagen and Rivian, Daimler Truck and Volvo – the automotive industry is increasingly recognizing that there is strength in numbers. The development of new vehicle platforms for software-defined vehicles (SDVs) is putting OEMs under pressure in terms of both time and cost. Sharing responsibilities and pooling expertise is therefore a logical step.

Challenge for Automotive Security

Joint ventures pose significant challenges for the cybersecurity of vehicles. While the SDV, with its decoupling of hardware and software, its extended ecosystem, and its high connectivity, already presents new and demanding security requirements, a vehicle architecture assembled from components of different partners adds a further dimension to the complexity. Essentially, three key problem areas can be identified:

- **Harmonizing security concepts:** The partners typically bring with them cybersecurity processes, technologies, and software solutions that have evolved over years. The challenge is to merge these diverse "security postures" into a unified, robust whole.
- **Balancing security and efficiency:** Cybersecurity must not negate the anticipated benefits of the partnership. Security measures must be integrated from the outset in such a way that they do not hinder agility.
- **Potential new attack vectors:** Shared architectures create new technical challenges. While formerly separate systems from different partners are integrated, new interfaces inevitably arise that must be secured.

Therefore, a holistic approach is required that ensures consistent and sustainable automotive cybersecurity at both the organizational and technical levels (Figure 1).

Organizational decisions

At an organizational level, it is essential to establish clear structures and responsibilities from the outset. Instead of treating cybersecurity as an afterthought, it must be firmly embedded in the partnership's governance, ideally through a joint committee comprised of senior security experts from both partners. This committee requires clear decision-making authority regarding cybersecurity standards, technologies, and processes. A key aspect is defining clear interfaces, which can be documented, for

example, in a Cybersecurity Interface Agreement (CIA) according to ISO/SAE 21434. It is also essential to consider the cooperation from the end-of-life perspective. Vehicle lifecycles of 15 years and more outlast many corporate partnerships. Therefore, obligations for the post-production period (post-SOP)—such as continuous vulnerability monitoring, incident response, and the provision of security updates—must be contractually and unambiguously defined. Only in this way can the vehicle's cybersecurity be ensured throughout its entire lifecycle, even long after the joint venture has been dissolved.

Harmonization of networked security controls

In collaboratively developed new E/E architectures, the harmonization of security controls depends primarily on the type and degree of their networking. Purely local protection mechanisms that operate autonomously within individual electronic control units (ECUs) generally require little or no harmonization. Security controls that do not communicate internally within the vehicle but only with an external instance (e.g., a backend) require a more nuanced approach; the best example of this is Secure Update. Depending on the desired collaboration model, it may be advantageous to either harmonize the controls or maintain separate backends.

Security controls, which require communication between various components in the vehicle's electrical system, present a completely different situation. Here, the harmonization of security mechanisms is a fundamental prerequisite for their functionality. This is especially true for protection mechanisms that rely on input from other security controls and other vehicle components. The category of networked security controls typically includes secure communication within the vehicle (including Secure Onboard Communication SecOC, TLS, MACSec), secure updates, the intrusion detection system (IDS), and the key management system (KMS).

Secure on-board network communication

Securing communication between ECUs is the backbone of automotive cybersecurity. In traditional networks (e.g., CAN, FlexRay) as well as for signal-based communication via Ethernet, AUTOSAR, with its Secure On-

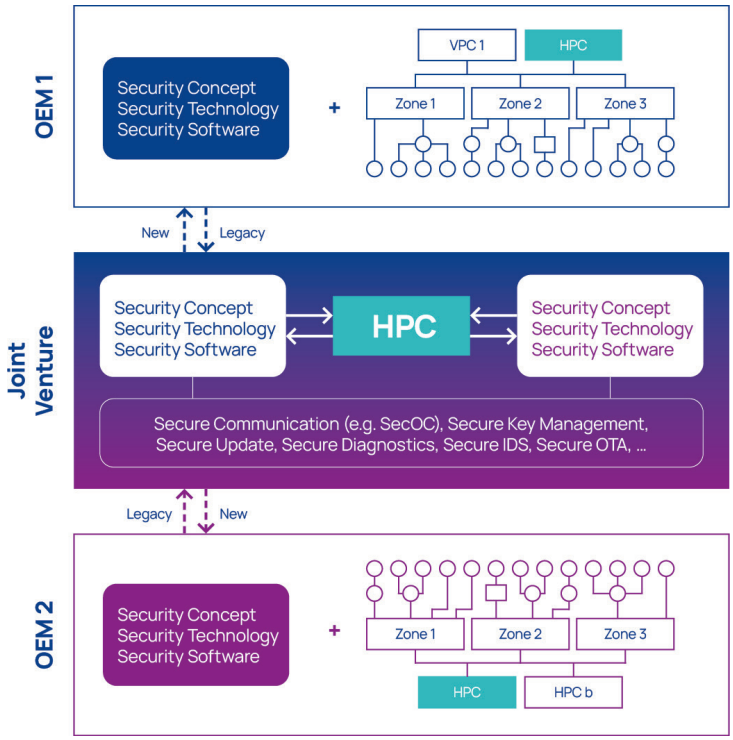

Figure 1: New E/E architectures developed in a joint venture require an agreement between the partners regarding security concept, technology, and software.

Picture: ETAS

board Communication (SecOC), continues to provide sufficient assurance of the authenticity and timeliness of transmitted data. However, the standard by itself is not a plug-and-play solution. It leaves important implementation details open, which must be harmonized within a partnership, such as...

- the **freshness value**, which must be matched between sending and receiving ECUs to prevent replay attacks.
- the **key management**, which must feed the symmetric keys required for SecOC into the control units in a uniform manner and assign them to the individual messages (see below).
- the **parameterization** of the SecOC protocol to ensure interoperability.

Depending on the network topology, this harmonization does not necessarily have to encompass the entire vehicle architecture. In a zonal E/E architecture, it is sometimes sufficient to standardize SecOC within the individual subnets, while the zone controllers connected via an Ethernet backbone secure their communication in a different way (Figure 3).

For Ethernet communication, TLS in particular—as an established IT standard—provides an authenticated and encrypted end-to-end connection. For compatibility reasons, partners should use widely adopted cipher suites. If a KMS for SecOC already exists, TLS can use pre-shared symmetric keys for authentication. Otherwise, certificates are required, and it must be ensured that all ECUs trust the partner's root certificates.

Secure software updates

For increasingly software-defined vehicles, the ability to securely update software is of paramount importance. Updates are therefore typically authenticated using asymmetric cryptography. Each ECU has a root certificate from a public key infrastructure (PKI), which serves as a trust anchor for verifying the backend signature.

Depending on the partnership, two different scenarios arise: Either the ECUs jointly developed for both OEMs in the joint venture are updated in their respective vehicles via their own backends. Or, independently developed ECUs from the partners are merged into a common architecture. Accordingly, the technical adaptation takes place either in the backend, which then creates signatures adapted for different ECUs, or it takes place in the control unit itself, where software is extended to accept multiple algorithms or keys from the partners. Several questions must be considered when choosing the appropriate strategy:

- Does the timeframe allow for changes to the basic software of the ECUs?
- Do all ECUs have the necessary hardware or computing power to support all algorithms?
- Can the relevant keys and certificates be dynamically imported via a key management system (KMS), or are they hard-coded into the ECU software?
- How much effort is required for adjustments in the respective backend systems of the partners?

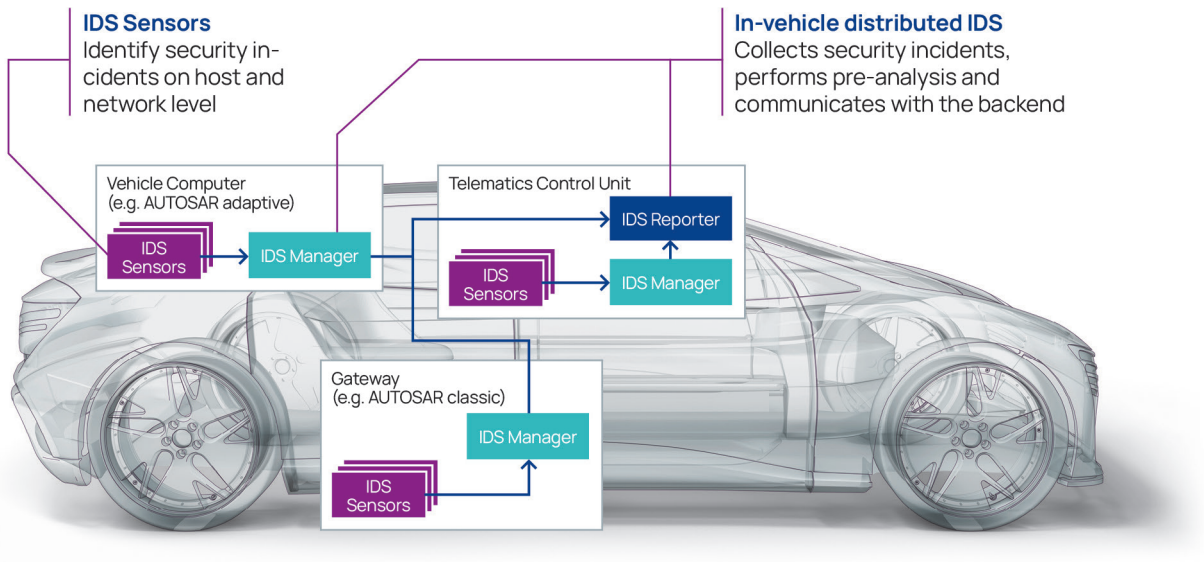

Figure 2: In collaboratively developed architectures, ideally both uniform trigger conditions for security events detected by the IDS sensors and a uniform data format for forwarding to the backend via the IDS manager are specified.

Picture: ETAS

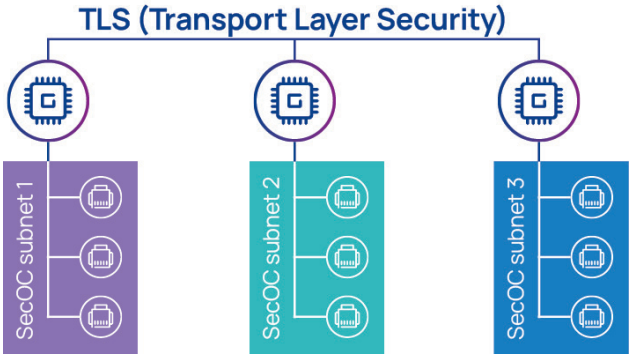

Figure 3: In zonal architectures, standardization via SecOC at the subnet level is usually sufficient. TLS provides an authenticated and encrypted end-to-end connection for the overlying Ethernet backbone.
Picture: ETAS

Harmonized key management is essential

A harmonized key management system (KMS) is essential for most networked security functions in the collaboratively developed E/E architecture; it ensures the secure distribution and updating of the required cryptographic keys. However, there are hardly any overarching standards in the automotive sector; AUTOSAR's KeyM module, for example, only specifies the handling of keys within(!) a control unit, but not the overarching distribution process. A compromise between two established, proprietary KMS solutions from the partners is therefore usually not technically feasible. The partners must either choose one of their existing systems or jointly define a new one.

There are two basic models for key management: external generation of the key material in the backend followed by injection into the vehicle (usually during production), or dynamic generation and exchange of keys directly between the ECUs in the field. The former enables, among other things, the generation of use-case-specific key material for the same ECU. The latter, on the other hand, offers greater flexibility in onboard communication and less dependence on the backend in production. Both approaches require an initial trust anchor that allows the ECUs to authenticate the key material.

Unifying intrusion detection

An intrusion detection system (IDS) in the vehicle serves to detect potential cyberattacks early, enabling countermeasures to be initiated via the backend before an attack spreads to the entire fleet. Sensors monitor the subsystems and their communication, reporting unusual activity and anomalies as "security events" to the IDS managers in the control units. These managers then review and filter the data, forwarding it to the central IDS reporter in the vehicle, which makes it available for the simplest possible automated analysis in the backend (Figure 2). In a collaboratively developed architecture, the various components and instances of intrusion detection must be well-coordinated. For example, the conditions under which a security event is triggered, as well as the format of the event messages, must be consistent. The IDS manager specified by AUTOSAR, for example, provides a common framework; it collects information from all sensors and forwards it in a defined format. In doing so, AUTOSAR also specifies certain security events and their trigger conditions. If complete harmonization of intrusion detection is not possible, at least different event IDs or markers should be used in the context data. This allows the backend to recognize which of the different partner assumptions the message follows and to take this into account during analysis.

Added value for SDV security

For OEMs, collaborations to develop new vehicle platforms have become a proven means of succeeding in the race for SDV. For such joint ventures to reach their full potential without compromising vehicle cybersecurity, cybersecurity must be understood as an integral part of the collaboration from the very beginning. Early harmonization at both the organizational and technical levels is therefore essential. It is also crucial to take a holistic view of cybersecurity from the start of production throughout the entire vehicle lifecycle. Vulnerability management and updates, for example, are essential for homologation according to UN R 155 and for maintaining customer trust. A significant opportunity lies in jointly addressing these post-SOP tasks: By pooling experience and expertise, partners can elevate vehicle protection to a higher level. This collaborative development will generate genuine added value for the cybersecurity of tomorrow's software-defined vehicles. ■

Authors: Dr. Christoph Stadtmüller, Engagement Manager Automotive Cybersecurity at ETAS, Lena Steden, Principal Global Market Access at ETAS