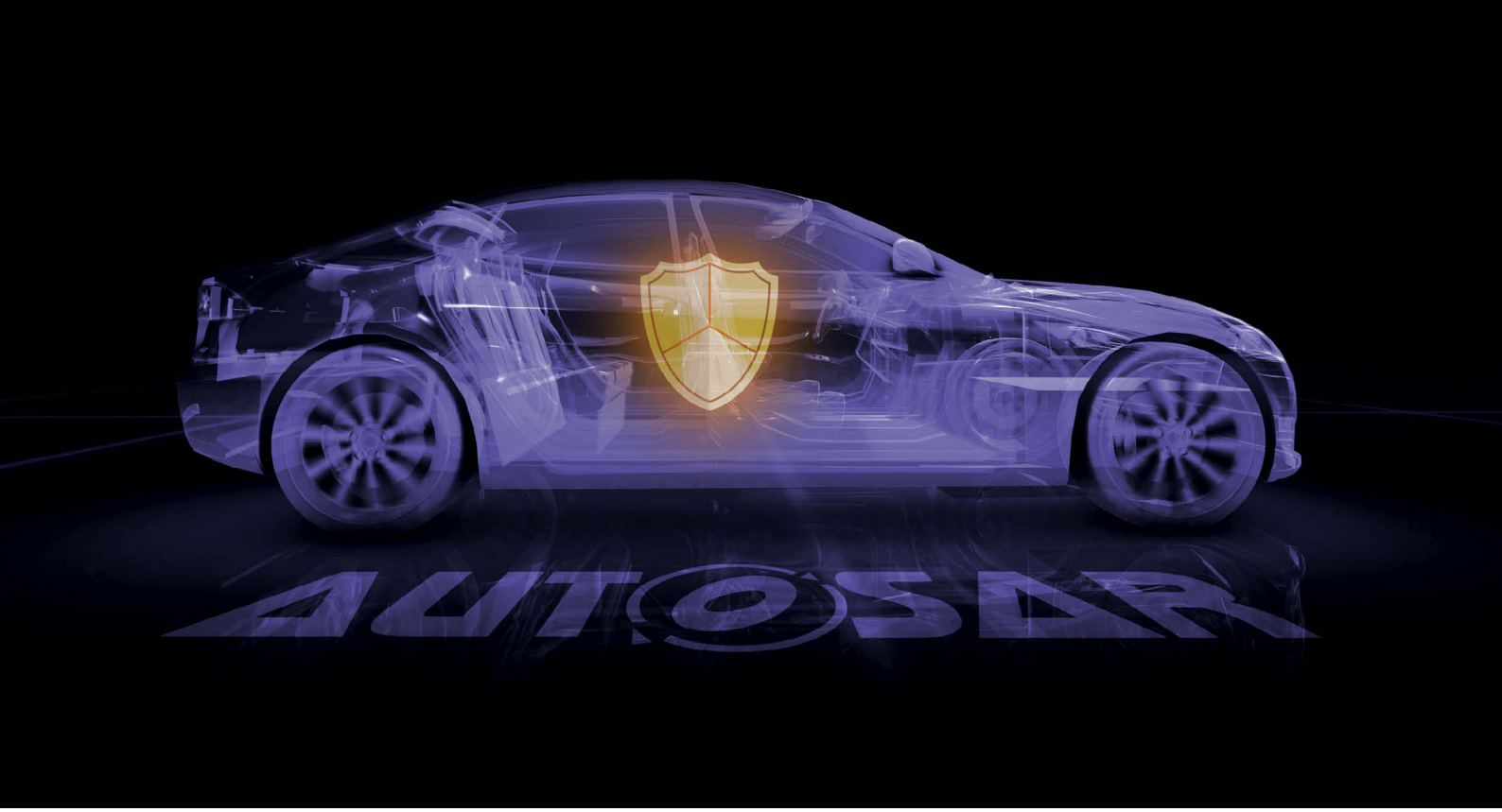

AUTOSAR security

Adaptive platform must focus on holistic vehicle protection

Automated driving functions and increasing connectivity call for more flexible software architecture – and a high degree of IT security. AUTOSAR delivers on this. With the adaptive platform and the deployment of critical security components.

AUTOSAR Classic, the standard middleware for most vehicle platforms, still meets the usual requirements. But in the future, vehicle computers will shape E/E architectures as central applications and the vehicle will become a software-dominated system. This is why AUTOSAR Adaptive will successively replace AUTOSAR Classic in many areas as the new future-oriented set of rules – setting new standards for automotive security in the process.

Security modules in AUTOSAR

AUTOSAR already incorporates various IT security applications, for instance for securing in-vehicle communication or protecting confidential data. However, Classic and Adaptive AUTOSAR currently offer partly identical and partly different security applications due to their different architectures (Fig. 1).

- **Crypto Stack:** Determines the cryptographic procedures and keystores implemented and provides the necessary key material to the various applications via uniform interfaces. The applications then access only the interfaces provided, independent of their crypto implementations, and remain portable to different ECUs. In addition, the AUTOSAR crypto stack can support multiple crypto implementations in parallel.
- **SecOC, TLS, and IPsec:** As an AUTOSAR Classic-specific protocol, SecOC specifically secures CAN communication. SecOC ensures authentication and freshness of the messages, but not their confidentiality, and allows OEMs to fine-tune their specific security levels. On the other hand, with automotive Ethernet in vehicles, TLS and IPsec are becoming increasingly important. Both standards support authentic and confidential communication; TLS is also suitable for external communication.
- **Identity and Access Management:** The AUTOSAR Identity and Access Management module ensures that only authorized applications access certain resources. These access rights can be freely configured in AUTOSAR and updated at any time.

- **Secure diagnostics:** AUTOSAR supports the logging of IT security events in secure memories. It also monitors authorized access to this data using the UDS services 0x27 (SecurityAccess) and 0x29 (Authentication). For example, the diagnostic test apparatus gains access to logged security incidents only if it has previously carried out a challenge-response communication or authenticated itself using a certificate.

Security engineering process

The decisive factor is to apply the security modules contained in AUTOSAR and adapt them individually to the security requirements of the vehicle platform. In other words, AUTOSAR must be integrated throughout the security engineering process. This involves three crucial steps: risk analysis, configuration, and testing. Taking the example of SecOC, this would be as follows (Fig. 2):

- **Risk analysis:** A risk analysis of all messages identifies those that need to be protected by SecOC. If different security profiles are stored, the message is assigned to the correct profile.
- **Configuration:** In the next step, SecOC and the crypto stack are configured for all ECUs involved in the data exchange according to the risk assessment and security profiles. Care is required here: a misconfiguration in a single ECU may result in secured messages not being verified and thus discarded.
- **Testing:** From a security perspective, several tests must be carried out before an ECU can be released for production – code review of the security critical components (e.g., SecOC module, CryptoStack), penetration test of the ECU, functional test of the SecOC module.

AUTOSAR Adaptive must follow an integrated security approach

On the way to connected, automated driving, the number of safety-relevant in-vehicle functions is increasing. This means it is becoming more important than ever to have more elaborate security measures and a high security level in place for vehicle platforms. In the future, OEMs will also increasingly establish new business models based on high connectivity that will need to be secured. This gives the further development of AUTOSAR Adaptive a clear mandate to integrate security applications much more strongly than before.

AUTOSAR configuration according to security needs

Example: Authentic ECU communication

- ✔ Identify security-relevant messages
- ✔ Configure messages in SecOC
- ✔ Select keys and algorithms in the Crypto Stack
- ✔ Align configuration across the vehicle
- ✔ Code review of security-critical components
- ✔ Penetration test of the ECU
- ✔ Function test of the SecOC module

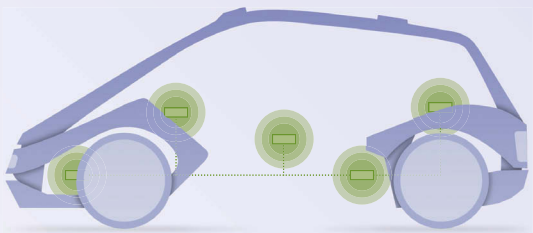

Figure 2: AUTOSAR configuration according to security requirements using SecOC as an example.

The guiding principle for AUTOSAR Adaptive must be an integrated automotive security approach: additional IT security components such as hardware security modules and the possible implementation of intrusion detection and prevention solutions will therefore have to be taken into account in the further development of AUTOSAR Adaptive. ■

Authors

Dr. Alexandre Berthold is Team Leader for Consulting and Engineering at ESCRYPT. **Dr. Michael Peter Schneider** is Project Manager AUTOSAR Security at ESCRYPT.

	Crypto Stack	SecOC	TLS	IPSec	Secure Log/Diag	Identity & Access Mgmt
AUTOSAR Classic 4.4	✔	✔	✔	✖	✔	✖
AUTOSAR Adaptive R19-03	✔	✖	✔	✔	✖	✔

Figure 1: Security application in AUTOSAR Classic and Adaptive (as of August 2019).