escrypt

SECURITY. TRUST. SUCCESS.

INTERVIEW

Mastering future security standards

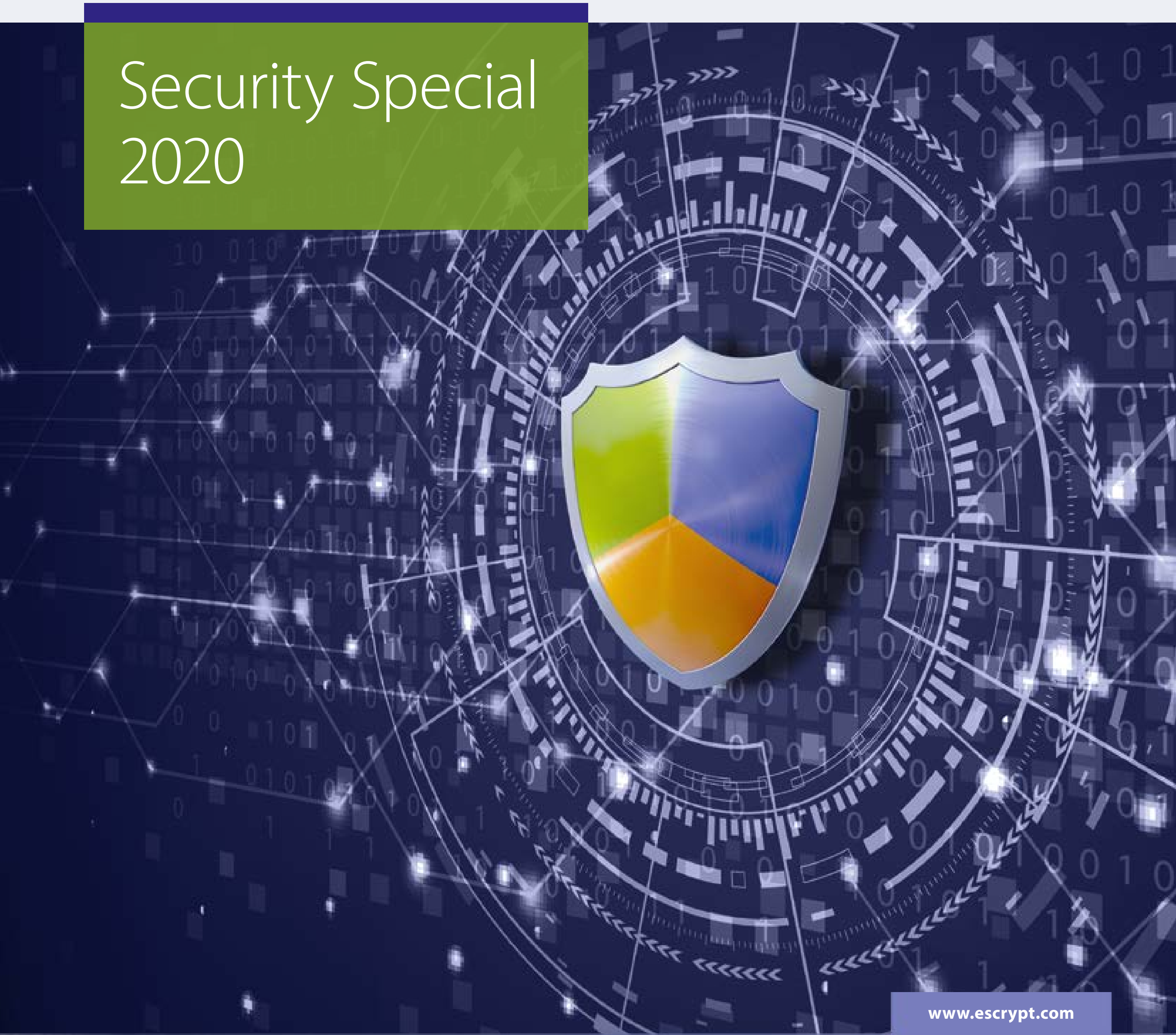
INTRUSION DETECTION

IDS and automotive firewall as complementary solutions

HARDWARE SECURITY MODULE

Next-generation HSM firmware

Security Special 2020



www.escrypt.com

“Cybersecurity is becoming a prerequisite for type approval”

Dr. Moritz Minzlaff on automotive security as a strategic task

Increasing security requirements for vehicles are manifesting themselves in a wave of new standards and regulations. In this interview, Dr. Moritz Minzlaff, Senior Manager at ESCRYPT in Berlin, explains what the automotive industry has to adapt to.

Dr. Minzlaff, efforts to create binding standards and regulations in the field of automotive security are now in full swing. Which developments deserve special attention here?

There are two initiatives that everyone is watching right now: first, ISO/SAE 21434, which sets standards at the process level; and second, the activities of UNECE WP.29, which will make cybersecurity a prerequisite for the type approval of vehicles. Both the UNECE regulations and the ISO specifications will come into force within the next three years. So there’s really not much time to prepare.

This means that in the near future the IT security for vehicles will truly be relevant for type approval!

That’s right. In the future, according to UNECE specifications, OEMs will be able to approve vehicle types in markets such as the EU or Japan only if they can demonstrate appropriate risk treatment. ISO/SAE 21434 will be the key to overcoming this hurdle by offering common security standards for the automotive industry. At the same time, further regulations and laws are constantly being developed at the regional level, which must also be kept in mind.

What are the specific challenges facing automakers and suppliers?

The big challenge is that in the future, security must be approached comprehensively right across the supply chain and life cycle. It is no longer enough to provide two or three central ECUs with security functions. Vehicle manufacturers will have to identify and secure critical elements for the entire platform – all the way through to phase-out. This means life cycle management will be a decisive topic in the future: How to provide adequate risk-based protection after start of production for connected vehicles that face many years of exposure to a constantly changing threat landscape out on the road?

As an OEM or supplier, what should I do now to make vehicle protection a permanent fixture in my corporate actions and my organization?

You need to act on two fronts. First, you should determine the security requirements of your product: vehicles and components with different degrees of connectivity, different functionalities, different safety relevance, and different degrees of automated driving each require tailored protection. To achieve the security level identified in this way, you’ll need to involve all participants: from development and production through quality assurance to sales and customer communication, responsibilities and roles must be clearly defined within the company and along the supply chain.

At the same time, you can carry out an “inventory,” in other words a standard audit or assessment. Which areas are you well positioned in? Which aspects of future regulatory requirements do you already meet? And which existing processes can you build on? A gap analysis of this kind will point out where investments in the further development of security will have the greatest impact.

Does it make sense to get a security specialist like ESCRYPT on board?

Yes, because our independent perspective and our global, industry-wide know-how is the ideal complement to your in-house expertise. The only way to achieve continuous protection of connected vehicles is by working together and taking an holistic approach. That’s why at ESCRYPT, we’ve already combined classic enterprise IT security with embedded security. Because the only way to master cybersecurity in the future is across domains, from vehicles to apps to clouds.

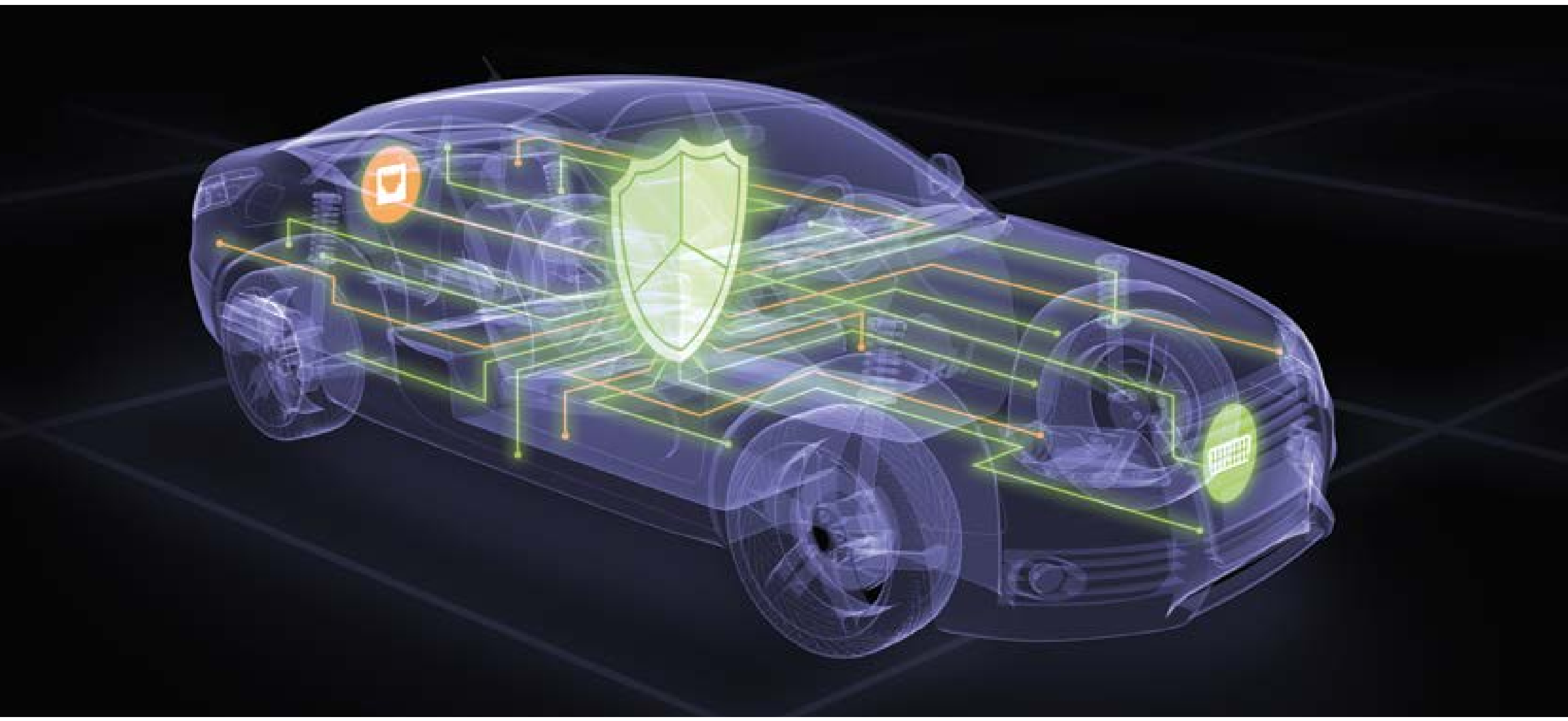
Moritz Minzlaff
Senior Manager at ESCRYPT

Due to our diverse project experience with manufacturers and suppliers in all major markets, we can also offer benchmarking. We identify exactly those aspects of security as currently practiced that should be further developed, and we help identify the necessary investments in cybersecurity. Time is short and the risk is too great not to achieve type approval according to UNECE specifications or to do so only with a delay or cost overrun. Thanks to our in-depth engineering experience, at the end of the day we at ESCRYPT know how to bring automotive security into series production. All this massively increases the chance of successfully mastering the challenges ahead. ■

"The only way to achieve continuous protection of connected vehicles is by working together and taking an holistic approach."

Intrusion detection for hybrid CAN-Ethernet networks

Tailoring security measures precisely to both worlds



Today's decentralized E/E architectures are no longer up to the challenges of connected, automated vehicles, which is why vehicle computers and automotive Ethernet will complement conventional ECUs and CAN buses. These kinds of vehicle networks require protection in the form of tailored attack detection and data traffic monitoring.

The direction of development is clear: vehicle computers (VCs) and broadband automotive Ethernet will complement today's vehicle electrical systems with dozens of ECUs connected by CAN, LIN, and FlexRay data buses. The latter remain in demand where high real-time requirements and cyclically recurring functions need to be implemented. In other instances, microprocessor-based central computers partitioned into virtual machines will take over, because they are better equipped to meet the challenges of connected, automated vehicles.

But how can hybrid CAN-Ethernet architectures and their data processes be effectively secured? Fundamentally, there are two principles: communication shielding and partitioning. Seamless monitoring of communication is required in order to detect cyber-attacks at an early stage; domain-specific virtual subnets (VLANs) minimize the penetration depth in the case of an attack. Both are feasible in hybrid electrical systems, but require different methodical approaches for the CAN and Ethernet worlds.

Efficient attack detection for CAN

An intrusion detection system (IDS) can be integrated into gateways or ECUs to monitor the CAN buses. It detects anomalies in CAN data traffic by comparing it with the "normal behavior" specified by the OEM. The embedded security component looks out, for example, for anomalies in cyclical messages and abusive diagnostic requests, which it classifies as potential attacks and logs or reports (Figure 1).

The performance of the CAN IDS (CycurIDS) depends directly on the quality of its configuration. This is why efficient initial rules from the OEM should be continuously supplemented by new detection mechanisms based on analyses of current attack vectors in order to achieve a high detection rate with as few false alarms as possible. The implementation stands and falls with the quality of the toolbox, which is used for the initial configuration and the continuous development of the rule sets. As ready-to-use software, such an IDS (CycurIDS) can be used as a CAN attack detection system in hybrid electrical systems at any time.

Automotive firewall in the Ethernet switch

In contrast, an automotive Ethernet firewall (CycurGATE) is advisable for secure, smooth Ethernet communication in hybrid electrical systems. This is implemented directly in the Ethernet switch, allowing it to monitor the complete packet flow without risking any interference with ECUs or the host controller. Balanced hardware and software co-design means that the firewall can make use of the hardware acceleration on the switch. As a result, most of the data packets are processed at wire speed. The main task is to defend against denial of service attacks. But by maintaining partitioning in all network layers, the firewall also supports secure data exchange between partitioned domains. To this end, a packet filter filters the incoming and outgoing data, checking each by way of stateful packet inspection and deep packet inspection.

So, the automotive Ethernet firewall (CycurGATE) not only protects the electrical system against unauthorized access and manipulation – it also serves to control onboard communication (Figure 2). It completely covers the Ethernet/IP including the common automotive protocols (e.g. SOME/IP), and it monitors access to networks and VLANs at MAC level. Communication is filtered by means of whitelists or blacklists that can be updated at any time, which ensures fast, effective reaction to new attack patterns.

```
…
0.010000 1  100  Rx  d 8 8A FF FF 0C 42 5F FD 97
0.011000 1  110  Rx  d 8 03 3E 3E E2 10 FF 4A 3F
0.012000 1  120  Rx  d 8 03 F7 30 27 C7 7E D9 9C
0.020000 1  100  Rx  d 8 11 F4 00 3E E2 60 6C B9
0.021000 1  110  Rx  d 8 1F AA 00 00 00 00 C0 00
0.022000 1  120  Rx  d 8 02 AA 00 00 00 00 C0 00
0.031000 1  110  Rx  d 8 86 4A 2F 01 81 05 80 7F
0.031500 1  110  Rx  d 8 E5 2B 41 0C 00 00 00 00
0.032000 1  120  Rx  d 8 02 04 78 00 FF 00 00 30
0.041000 1  110  Rx  d 8 6E 7B FF FF 3F FF 1F 8B
0.042000 1  120  Rx  d 8 00 5A 00 00 0F 55 02 00
0.043000 1  7DF  Rx  d 8 02 10 03 00 00 00 00 00
0.044000 1  7E8  Rx  d 8 02 50 03 AA AA AA AA AA
0.051000 1  110  Rx  d 8 FE 4B 2F 01 81 07 80 7F
0.052000 1  120  Rx  d 8 68 05 78 00 FF 00 00 30
…
```

Timings
- Frequency deviation
- Message infiltration
- Time-outs

Diagnostics
- Type of service
- Service conditions

Figure 1: The CAN IDS detects anomalies in cyclical messages and any abuse of diagnostic requirements

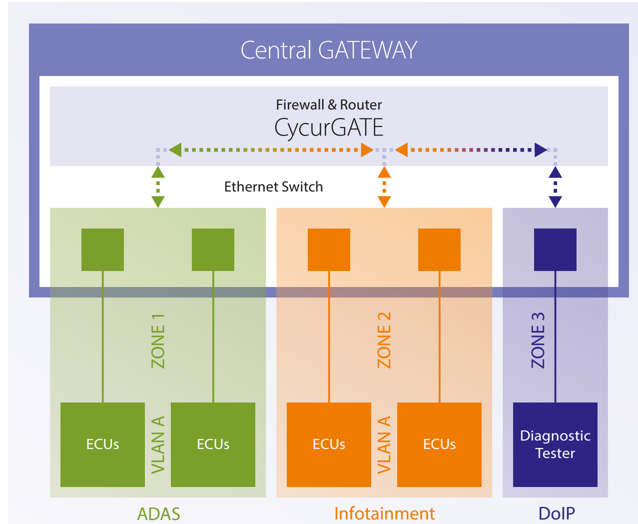


Figure 2: Automotive Ethernet firewall assumes gatekeeper and router functions

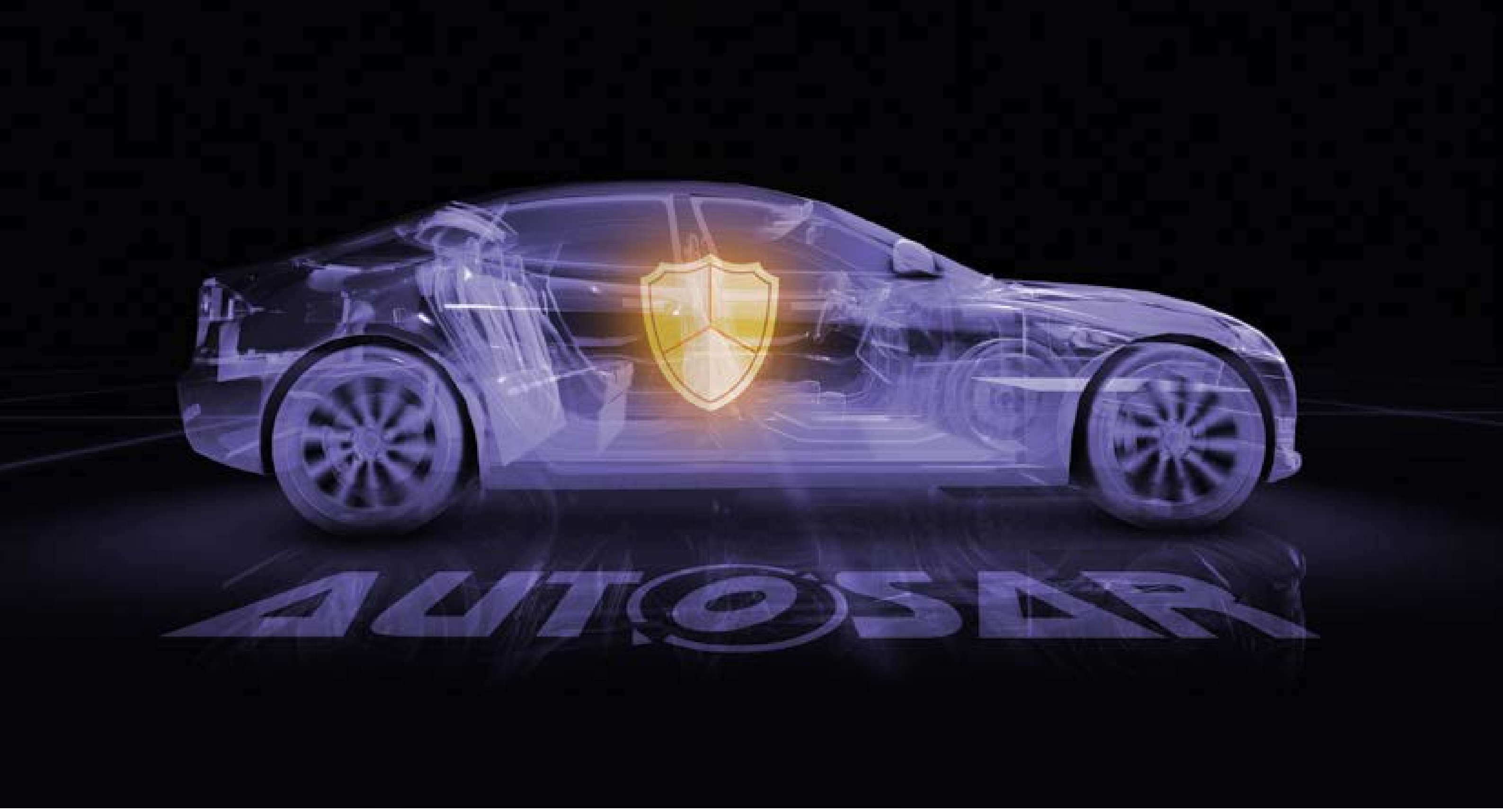
Intelligent load distribution

In addition to implementation in the central Ethernet switch, it is also possible to integrate host-based firewalls directly into ECUs. This requires high-performance solutions. The firewall must be powerful enough to check in real time and decide whether and where to route individual data packets. However, it cannot cover complex attack detection patterns, such as the frequency of stateful SOME/IP communication. Here, an additional Ethernet IDS is required that detects patterns of anomalies based on the message frequency, sequence, payload, data, and services and logs or reports them as attack attempts. For optimum performance, this approach requires intelligent load distribution between switch and microcontroller. Firewalling and intrusion detection can take place partly in the switch and partly in the target controller.

Together, CAN IDS, automotive Ethernet firewall, and Ethernet IDS can protect hybrid E/E architectures reliably and without noticeable latencies. Embedded in integrated security concepts, they are central components of risk prevention and functional safety in the connected and increasingly automated vehicle of the future. ■

Authors

Dr. Jan Holle is Product Manager for Intrusion Detection Systems at ESCRYPT. **M.Sc. Siddharth Shukla** is Product Manager for Automotive Firewall at ESCRYPT.



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 the 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 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 (Figure 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 (Figure 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).

Solution Portfolio

Design Security

Consulting, Testing, and Training

Strategic Security Consulting

- Strategic Security Development, Security Vision and Roadmap
- Security Standardization, Lobbying, and Strategic Cooperation

Security Trainings

- Security Basics
- Security Risk Analysis
- Secure Product Design
- Secure Connected Products
- Automotive Security

Enable Security

Products and Solutions

Production Key Server Crypto server for secure key injection in mass production

CycurHSM Automotive-qualified security stack for HSM

CycurIDS Intrusion detection

CycurV2X Secure V2X communication SDK

CycurGATE Automotive firewall

Manage Security

Operation, Monitoring and Incident & Response

Managed PKI Service

allows OEMs to maintain internal control over vital aspects of security such as certificate issuance, suspension, and revocation.

Security Operations Center (SOC)

acts as mission control, tracking anomalies and events in any aspect of a vehicle's operation.

Product Security Consulting

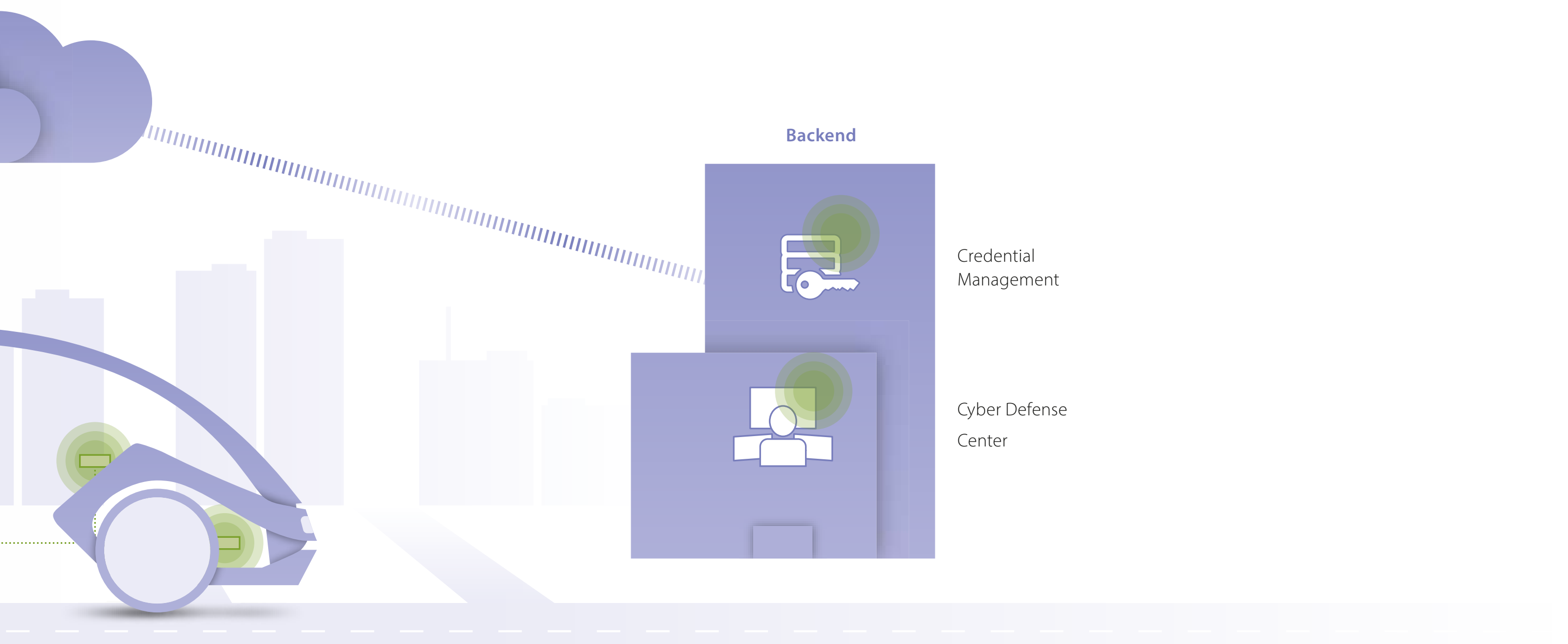
- Security Risk and Threat Analyses, Protection Requirements
- Security Concepts and Design
- Security Roles and Processes
- Custom Consulting

Product Security Engineering

- Security Specifications
- Security Implementations
- Security Integration
- Security Production
- Security Management

Security Testing

- Functional Security Testing
- Vulnerability Scans and Fuzzing
- Penetration Testing
- Code Security Audits
- Security Certifications
- Security Test Management



CycurACCESS Vehicle access and key sharing

CycurTLS Transport Layer Security (TLS) for embedded platforms

CycurLIB Cryptographic library

CycurKEYS Secure management of cryptographic keys and certificates

CycurV2X-SCMS V2X security credential management system

CycurGUARD Intrusion monitoring and analysis

Threat Intelligence and Forensics

deliver evidence-based knowledge about existing or emerging menaces to induce informed decisions and responses.

Vulnerability Management

helps uncover flaws and enables OEMs to implement a proactive threat prevention strategy.

Digital vaccination for the ECU

IT security for networked vehicles starts with ECU production

How can the cryptographic key material necessary for secure data exchange be introduced into the ECUs securely and according to requirements? The answer is an integrated solution consisting of a central key management backend and decentralized production key servers.

When it comes to protecting against cyber attacks, the control units in the vehicle play a key role – in the truest sense of the word: only cryptographic keys enable ECUs to authenticate themselves and thus legitimize data exchange within the electrical system as well as with the outside world. The special challenge here is that the ECUs for the various vehicle platforms must initially be supplied with OEM-specific key material and certificates – and ideally during their production by the ECU manufacturer.

Secure distribution of OEM key material

The effective solution combines a classic key management solution (KMS) as the central backend with decentralized production key servers (PKS) that are installed in the production facilities and communicate with the KMS. This is of benefit to the OEM because it means the process of equipping the OEM's specific ECUs with its own key material can be fully integrated into the ECU supplier's existing production infrastructure.

First, the KMS is fed the data packets with the key material provided by the respective car manufacturer. The key material is stored centrally, distributed via secure data transfer as needed among production sites, and stored on production key servers in readiness (Figure 1).

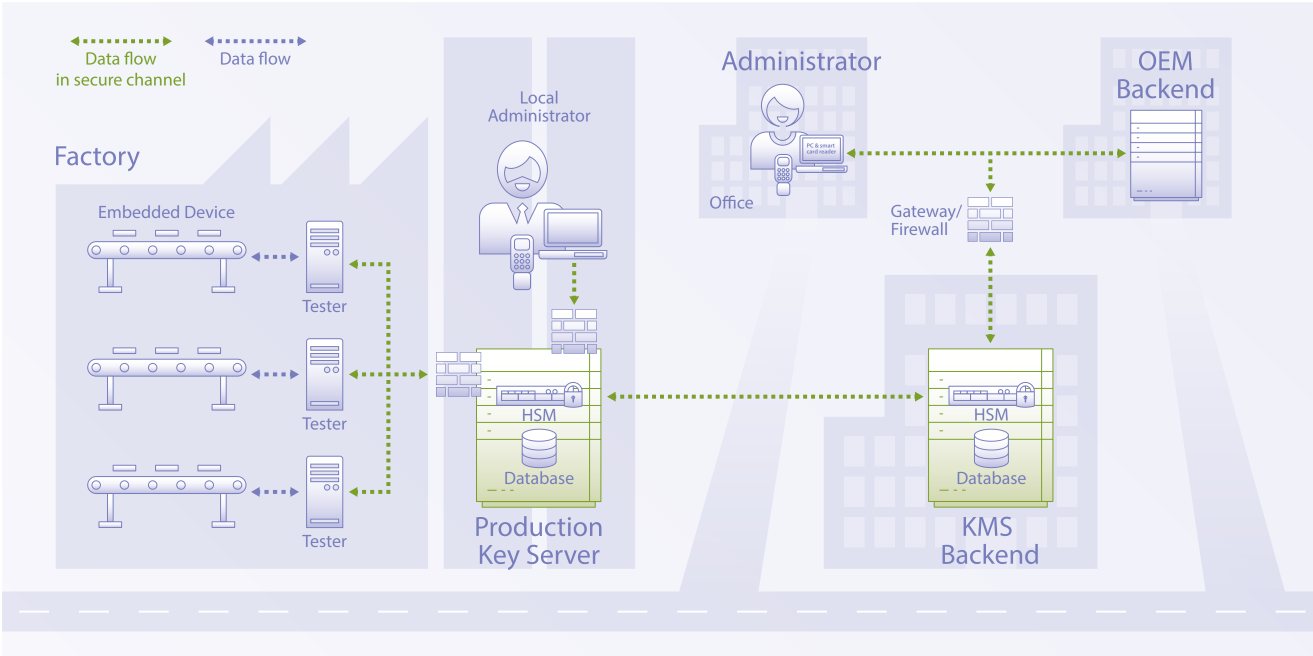


Figure 1: Integrated key distribution and injection with key management solution and production key server.

Key insertion via end-of-line tester

The key material is introduced into the ECUs on site during production by connected end-of-line testers. These then retrieve the individual key packages from the production key server in the plant and "inject" them – like a "digital vaccination" – into the individual ECUs during production. At the same time, the PKS logs which cryptographic keys have been introduced into each ECU. Finally, on request, the PKS sends back what are known as verification files from production via the central KMS backend to the OEM. This gives automotive manufacturers certainty that the ECUs are correctly equipped with key material.

The solution combines high security and availability.

Secure storage without permanent online connection

A particular advantage of the solution is the symbiosis of high security and availability. The production key servers are protected against unauthorized access both by a robust and powerful hardware security module (HSM) and by their own security software. In addition, the PKSs make contact with the backend only from time to time to synchronize data, carry out any updates, and create sufficient buffers with cryptographic data. This means that they are not dependent on a permanently stable internet connection, which means they are largely immune to potential online attacks.

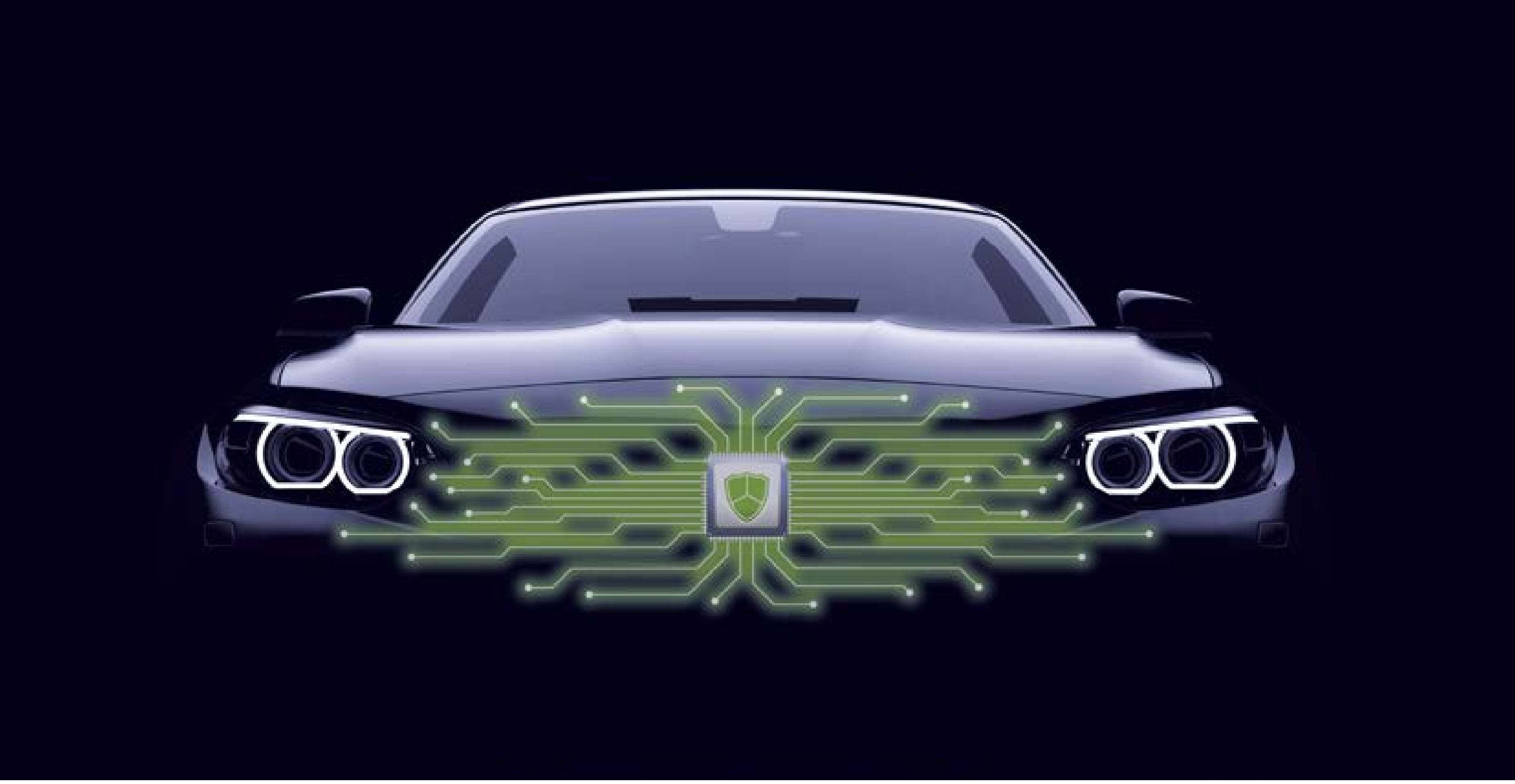
Users can freely determine how often contact should be made with the KMS backend as required. If the stock falls below a predefined minimum quota, new keys are automatically requested from the server. This ensures that there is always enough key material available for equipping the ECUs in production, which precludes a potentially costly production outage due to an interrupted network connection. The production key server always remains operational.

In use worldwide in ECU production

Secure and precise ECU data assignment with cryptographic keys forms the basis for almost all other in-vehicle IT security functions. The integrated KMS-PKS solution makes it possible to master the complex delivery mechanism for OEMs' cryptographic material, from secure key management to secure storage and injection of the key material into the ECUs and, finally, logging and verification. For good reason, today this process is used worldwide in ECU production for various automotive manufacturers. ■

Authors

Christian Wecker is Product Manager PKS at ESCRYPT.
Michael Lueke is Senior Program Manager KMS at ESCRYPT.



Performance boost for hardware security modules

New service-oriented HSM software secures future electrical system architectures

In vehicle architectures of the future, much of the software will be centralized on domain controllers, and automotive Ethernet will provide broadband onboard communication. This requires new approaches to IT security. Next-generation hardware security modules (HSMs) are becoming a central component, because they combine multi-app capability with real-time communication.

Vehicle computers (VC) are about to merge vehicle domains and their software-controlled functions. The ECUs in the periphery will increasingly develop into input/output devices whose actual applications will be running on the VC. The advantages for OEMs are far-reaching. IP is shifted to the central computers. The complexity of E/E architectures is reduced, as is the engineering effort. Instead of purchasing specific ECUs and software for each vehicle generation, OEMs can pool the development and interaction of the software applications on the vehicle computers – saving time and money.

However, centralization drives an increase in onboard communication. Rather than decentralized processing in ECUs, the domain controller must collect data, process it, and distribute it in the vehicle. Because real-time requirements often apply, the data traffic will run via automotive Ethernet. Meanwhile, in subnetworks, signal transmission will still be done via CAN bus. IT security must be adapted to these hybrid architectures.

Security by design

With a view to increasing connectivity, security by design and update by design should be firmly anchored in hybrid in-vehicle networks – especially in light of the new possibilities opened up by the decoupling of hardware and software as well as the relocation of many software applications. IT security functions can also be managed centrally in the centralized in-vehicle network. At the same time, the protection of the ECUs in the peripherals must be guaranteed.

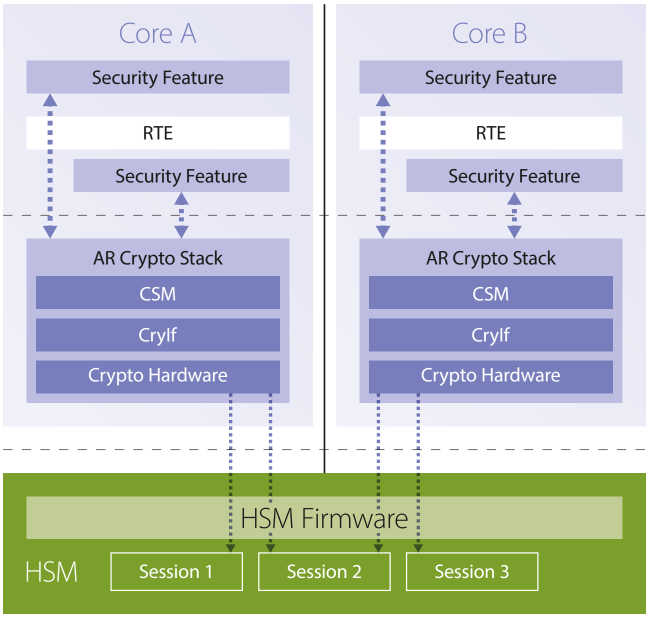


Figure 1: Requests from multiple host cores are processed by the HSM firmware in parallel sessions.

Hardware security modules (HSMs) are indispensable for completely secure onboard communication (SecOC). These help to ensure the authenticity of all data converging here and prevent attackers from gaining access to the central processor or even to the in-vehicle network by bypassing security-relevant ECU interfaces. But the challenges in centralized in-vehicle networks go beyond that: the demands on the security components also increase whenever central vehicle computers, often partitioned into many virtual machines, take over the software applications and functions of several ECUs. A new generation of hardware security modules has already been prepared for this.

Job preference and the real-time operating system

The IT security functions of the HSM are physically encapsulated in an HSM core on the microcontroller of the respective processor. There, they are activated and operated via the HSM software stack. The computer's host controller can thus devote itself to its actual tasks, while the HSM core processes security requirements: secure on-board communication, runtime manipulation detection, and secure booting, flashing, logging, and debugging. This makes HSMs much more powerful than purely software-based IT security solutions.

If software applications and ECU functions are combined on vehicle computers, it is foreseeable that there will sometimes be many applications competing simultaneously for the HSM's security functions. In this case, the HSM must provide the necessary IT security functions and manage the data streams of multiple applications in real time. This pushes standard HSMs to their limits; purely software-supported security solutions even more so. But a new generation of hardware security modules with a real-time operating system and an intelligent, flexible session concept is up to the task.

Multi-core/multi-application support

In future architectures, if several cores make parallel requests, the new HSM's firmware ensures that the HSM core processes these in up to 16 parallel sessions, with a configurable number of sessions in the modern HSM software stacks. The secret of this multi-core and multi-application support lies in the special architecture of the HSM firmware driver. This allows different virtualized applications to integrate the driver independently, paving the way for the independent development of various software parts: During integration, the "linker" step ensures that the driver's various instances use a common structure in the shared RAM of the hardware. Here, each instance creates its own structures (sessions) so that the driver can always manage several requests from the strictly encapsulated applications in parallel (Figure 1).

A central security component in this setup is the host-to-HSM bridge. As the element separating the hardware security from the host, it takes over the "inflow control" to the HSM module. In the bridge register, the queue of requests from the host cores is set up and processed in a way that ensures optimum utilization of the HSM as a limited resource to execute the requested security functions as quickly as possible. The next generation of HSM software turns the HSM's multi-app and multi-core capability into reality. OEMs can access it in a fully tested, production-ready form (Figure 2).

Bulk MAC interface provides real-time performance

A further challenge is how to secure the massive increase in communication. Dealing with the juxtaposition of CAN buses and automotive Ethernet in the centralized electrical systems and secure

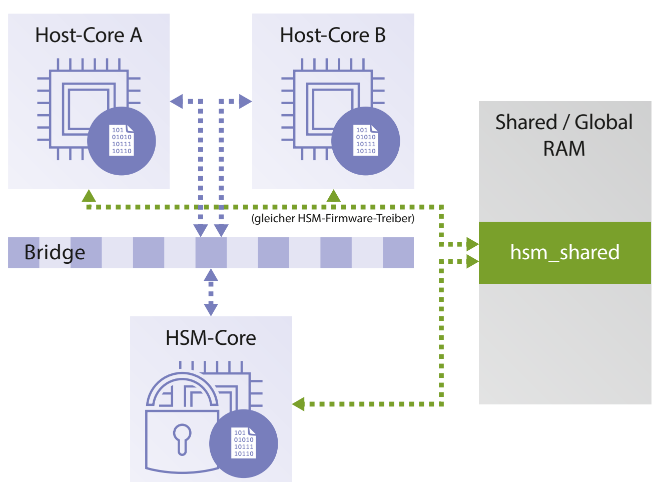


Figure 2: Multi-core/multi-application support – Job requests are processed via bridge register and shared RAM.

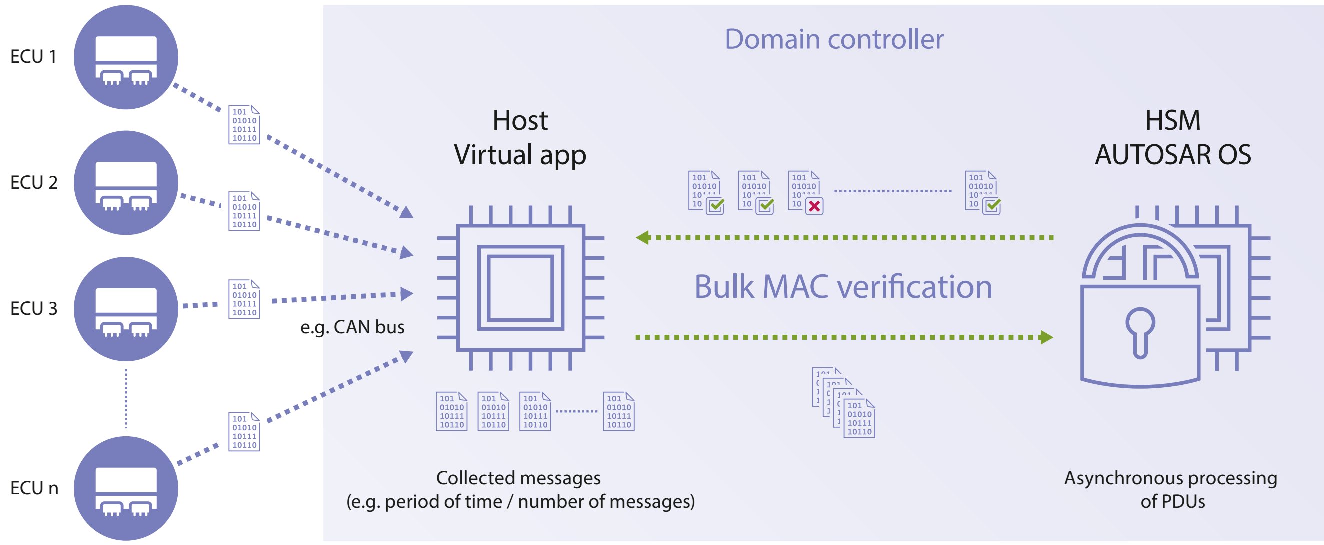


Figure 3: The bulk MAC interface provides secure real-time communication.

in-vehicle data exchange with protection for all communication protocols is demanding. The innovative HSMs also offer a solution for this, although their performance is limited in itself. Limits are set less by the HSM's hardware crypto engine than by the bridge register, because it doesn't permit data exchange in any quantity and at any speed. One solution is something known as a bulk MAC interface: first, the host collects all messages over a predetermined period of time; then it posts them en bloc as a request to the HSM via the bridge register. This way, one (!) single data transfer is sufficient. The HSM firmware processes all collected messages on the HSM hardware unit at once and transmits the results to the host (Figure 3).

This delivers a huge gain in performance. Even if each data transfer between host and HSM takes only 10 µs, the delay adds up to 1 ms for a hundred messages. This is problematic for real-time systems. Using a bulk MAC interface, those hundred messages can be handled in one-hundredth of the time. For OEMs who set up networks with central computers and domain controllers and define many PDUs in the process, a bulk MAC interface offers definite advantages. By ensuring sufficiently fast authentication of large numbers of different messages, it maintains secure real-time communication in the vehicle network. In the next HSM software generation, this bulk MAC setup is already integrated ready for production.

Future-proof hardware security firmware

As in-vehicle networks are being transformed into centralized platforms, they are driving the decoupling of hardware and software. Hardware security modules play a central role in ensuring the IT security of these platforms. Not only do they protect the data streams from peripherals, where CAN buses will continue to dominate, to the central controllers against access and manipulation (SecOC). They are also able to cover security use cases at the highest network level and secure running software applications with a high data load and real-time requirements. A new HSM generation, designed for multi-core and multi-application tasks, ensures real-time communication even with high data loads and heterogeneous formats using a bulk MAC interface.

Next-generation hardware security firmware can be mapped in dedicated OEM product variants.

In view of increasing connectivity and the trend towards automated driving, OEMs are increasingly setting their own specific security standards for E/E architectures. Next-generation hardware security firmware can be mapped in dedicated OEM product variants – and flexibly integrated into central security concepts. It runs on the latest microcontrollers and provides its host driver as source code. This gives OEMs and Tier 1 suppliers with a wealth of opportunities for reuse and customization. Thanks to this flexibility and their performance, hardware security modules with the latest firmware are a fundamental component for securing the centralized, hybrid in-vehicle networks of the future. ■

Authors

Tobias Klein is Lead Product Owner HSM at ESCRYPT.
Dr. Frederic Stumpf is Head of Product Management Cyber Security Solutions at ESCRYPT.

Preliminary plan of Mark 51°7, Bochum. © skt umbaukultur – Partnerschaft von Architekten mbB – Bonn

Dr. Uwe Müller,
Head of Application Field Cybersecurity Solutions,
ESCRYPT (Bosch Group)

ESCRYPT to build new headquarters

By early 2022, a new headquarters will be built for ESCRYPT on the site of the former Opel factory in Bochum. Construction work on the new building, designed in line with the latest structural and energy standards, will begin in the summer. It will ultimately offer an attractive working environment for up to 500 associates.

"By selecting this new location, we are consciously putting ourselves closer to the region's vibrant university and research landscape," says Dr. Uwe Müller, responsible Division Head for ESCRYPT within the Bosch Group. Moreover, ESCRYPT's new building on the former Opel site is symbolic of the automotive industry's new identity, based on digitally connected, automated, and electrified mobility. ■

"By selecting this new location, we are consciously putting ourselves closer to the region's vibrant university and research landscape."