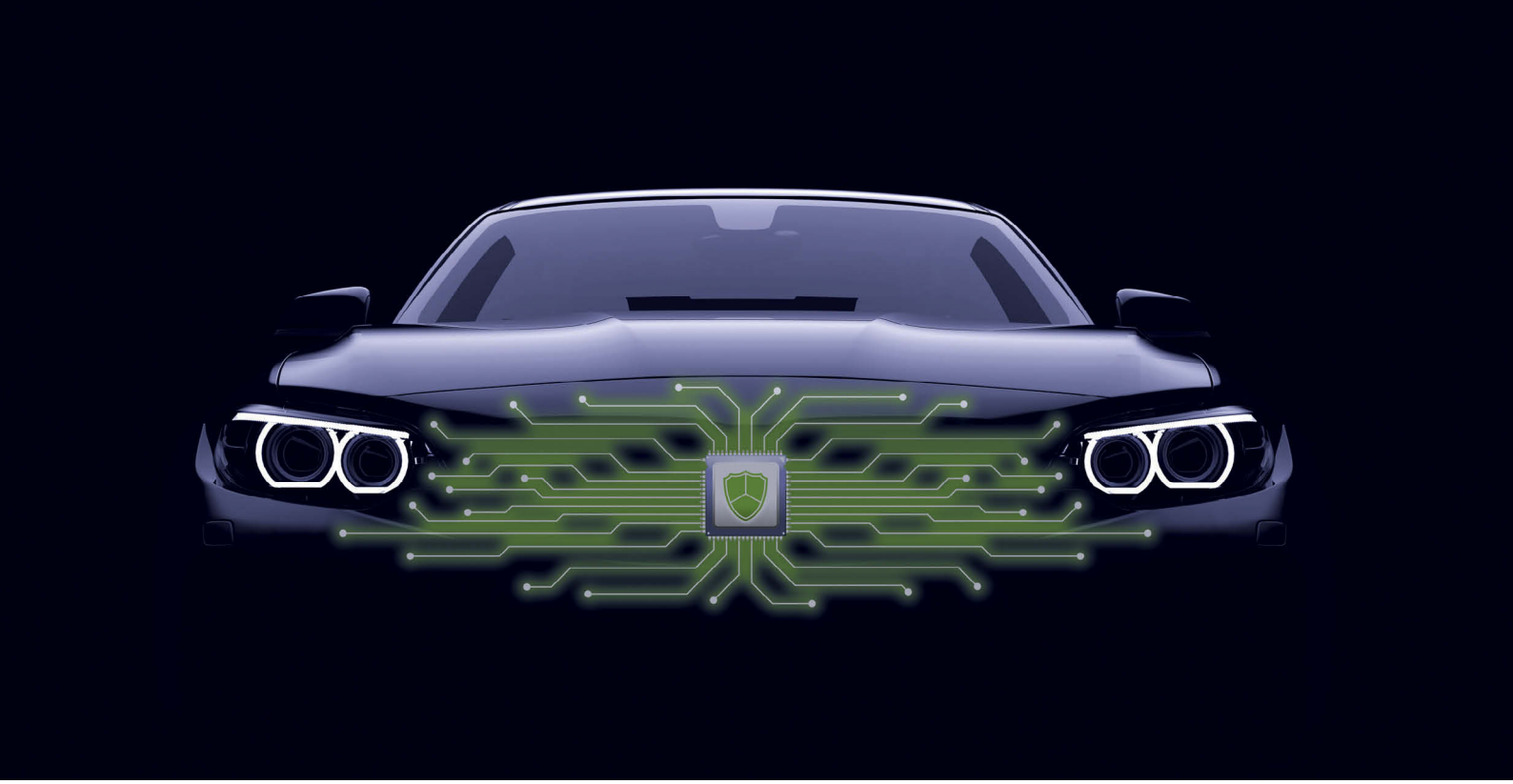

Performance boost for hardware security modules

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 (VCs) 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.

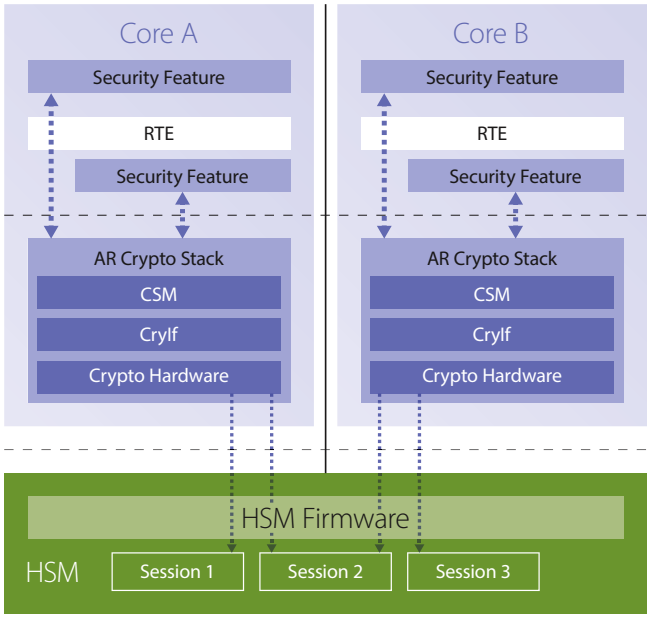

Figure 1: Requests from multiple host cores are processed by the HSM firmware in parallel sessions.

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 onboard 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 (Fig. 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. 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 (Fig. 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

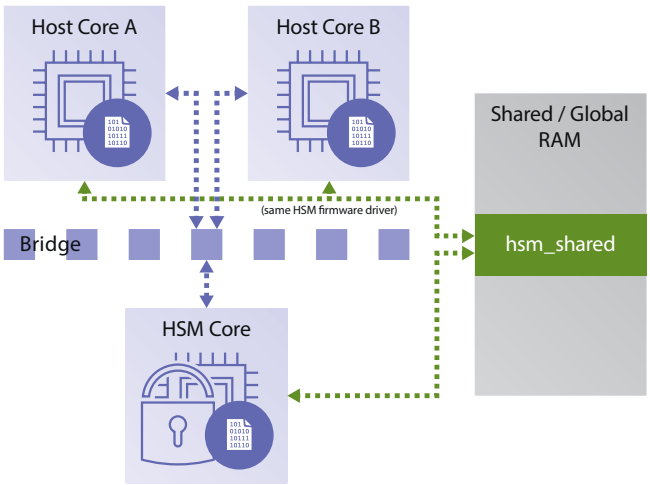

Figure 2: Multi-core/multi-application support – job requests are processed via bridge register and shared RAM.

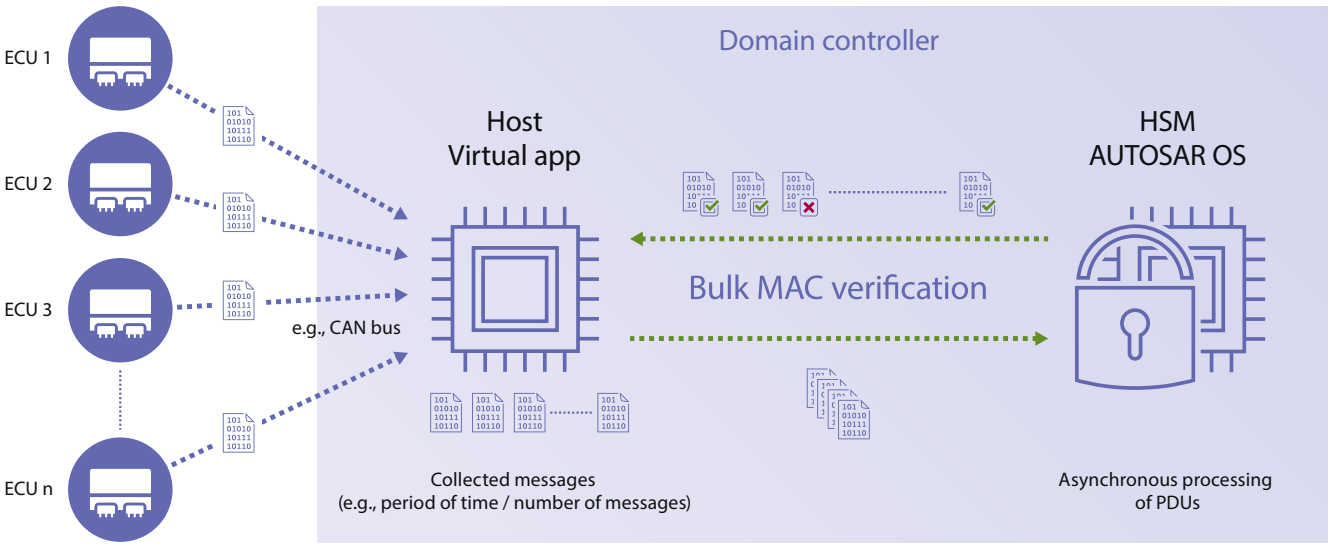

Figure 3: The bulk MAC interface provides secure real-time communication.

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 (Fig. 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 toward 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 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 Cybersecurity Solutions at ESCRYPT.