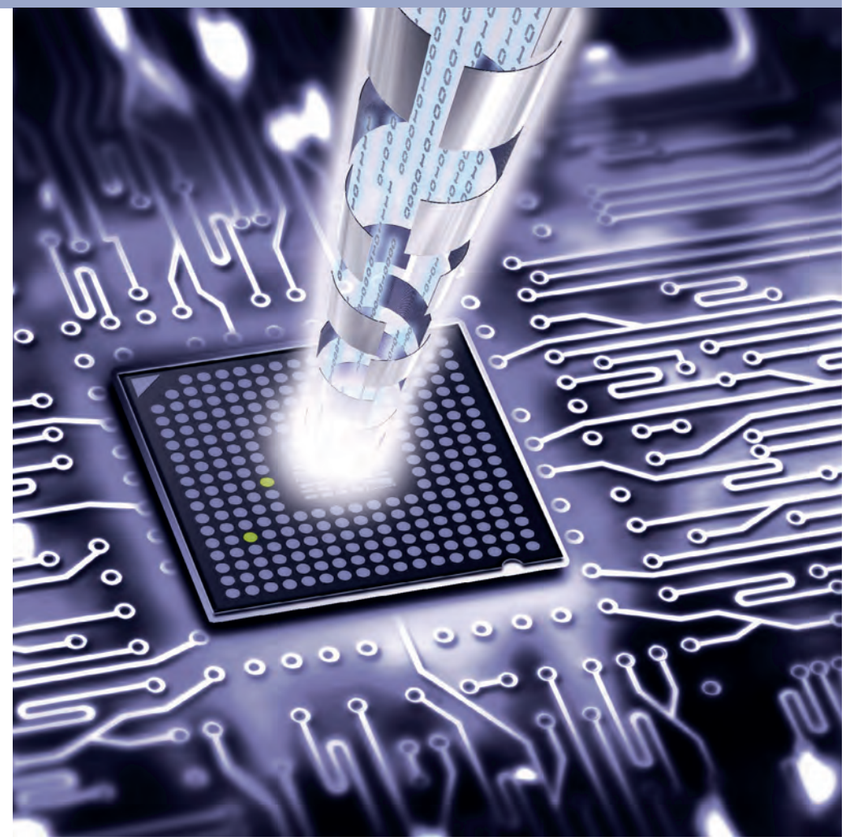
Protection against Unauthorized Access

Intelligent interaction between software and hardware safeguards ECUs

Connected vehicle systems require protection against unauthorized access. Hardware Security Modules (HSMs) provide this, but have always been unsuitable for automotive applications. This is no longer the case, thanks to Bosch's HSM and its derivatives implemented by various semiconductor manufacturers. Timed to coincide with the growing popularity of these products, ESCRYPT has brought out CycurHSM – a matching firmware solution that makes an HSM a viable security solution for automotive ECUs.



AUTHORS

Christopher Pohl is Senior Security Engineer at **ESCRYPT GmbH** in Bochum.

Dr. Frederic Stumpf is Head of **ESCRYPT's Branch Office** Stuttgart.

A side window has been smashed; the airbags and satnav are gone. Extremely annoying, yes – but at least the damage is obvious. Not so when the vehicle's IT systems have been tampered with. Unauthorized interventions of this kind pose an invisible threat, and the potential risks are growing as vehicles and ECUs become increasingly connected.

What is needed are strategies to defend against hackers and their potential attacks, virus contamination, and unauthorized uploads. Bosch recognized this several years ago, and identified Hardware Security Modules (HSMs) as a suitable protective technology. HSMs have their own processor core, their own RAM, ROM, and flash memory, and come with specific security features. However, the HSMs available at the time were too expensive, too sensitive, and too limited in terms of their functionality. This led Bosch to develop specifications for an automotive-compatible HSM and shared these with semiconductor manufacturers in a bid to speed up market penetration. A strategy that is paying off, as various manufacturers have now implemented derivatives of the Bosch HSM and are pushing these onto the market.

Standardized software stack for Bosch HSM and its derivatives

In July 2015, ESCRYPT released a compatible firmware solution: CycurHSM. By interacting intelligently with the hardware, CycurHSM protects vehicle systems against unauthorized access during all operating phases including initial boot, normal operation, and software updates or upgrades.

Hardware and software work hand in hand to offer this comprehensive protection. Each Bosch HSM contains a processor, sufficient memory, and a true random number generator (TRNG). In addition, it has accelerator hardware that enables it to calculate cryptographic message authentication codes in accordance with the Advanced Encryption Standard (AES) at lightning speed. It was on the basis of this hardware that ESCRYPT was able to realize functions such as secure boot, runtime tuning detection, and secure flashing in its CycurHSM. The software also relies on ETAS' RTA-OS, which was developed as a real-time operating system for automotive applications.

Maximum flexibility when choosing hardware

ESCRPYT began to brainstorm CycurHSM in mid-2013, and the vision was to develop a standardized software stack for the Bosch HSM and all its derivatives. This objective has been achieved. By standardizing processes at software level, customers can opt for whichever controller they like, regardless of their hardware setup.

In accordance with the open philosophy behind CycurHSM, the software's CSAI interface (Client Server Architecture Interface) makes it compatible not only with AUTOSAR, but also with all other applications beyond this standard.

Comprehensive protection

CycurHSM is embedded in ESCRYPT's modular product portfolio, as is the firmware's secure flashing function, which verifies sender authenticity for updates and upgrades. The secret keys required for this process are generated in the backend of the vehicle manufacturer or specialized service provider, and are shared only with trustworthy partners. As well as providing key management services and processing of this kind in high-security data centers, ESCRYPT also issues licenses for software that can generate such cryptographic keys. Gatekeeper functions such as secure flashing are prerequisites for vehicles using Car-to-X communication and over-the-air updates. If the source attempting to connect with the vehicle is unable to provide the required digital signatures, the HSM prohibits the data transfer. Encryption technology also lies at the heart of the CycurHSM secure boot function, which uses secret keys during the booting process to unequivocally determine whether ECU software is still authentic.

The process is sequential: As the system powers up, each component launched as part of the ECU boot chain verifies the integrity of the next. This ensures that malware is detected, at the very latest, the next time the system starts up – even if the entry route was via a trustworthy source such as through a diagnostic device in the workshop. Since the HSM records every single change, manipulation can still be detected even when the ECU software has been restored to its original state. In this way, CycurHSM brings the almost incidental added bonus of creating legal certainty within the notoriously gray area of chip tuning.

During operation, the CycurHSM's runtime tuning detection performs cyclical checks to establish the con-

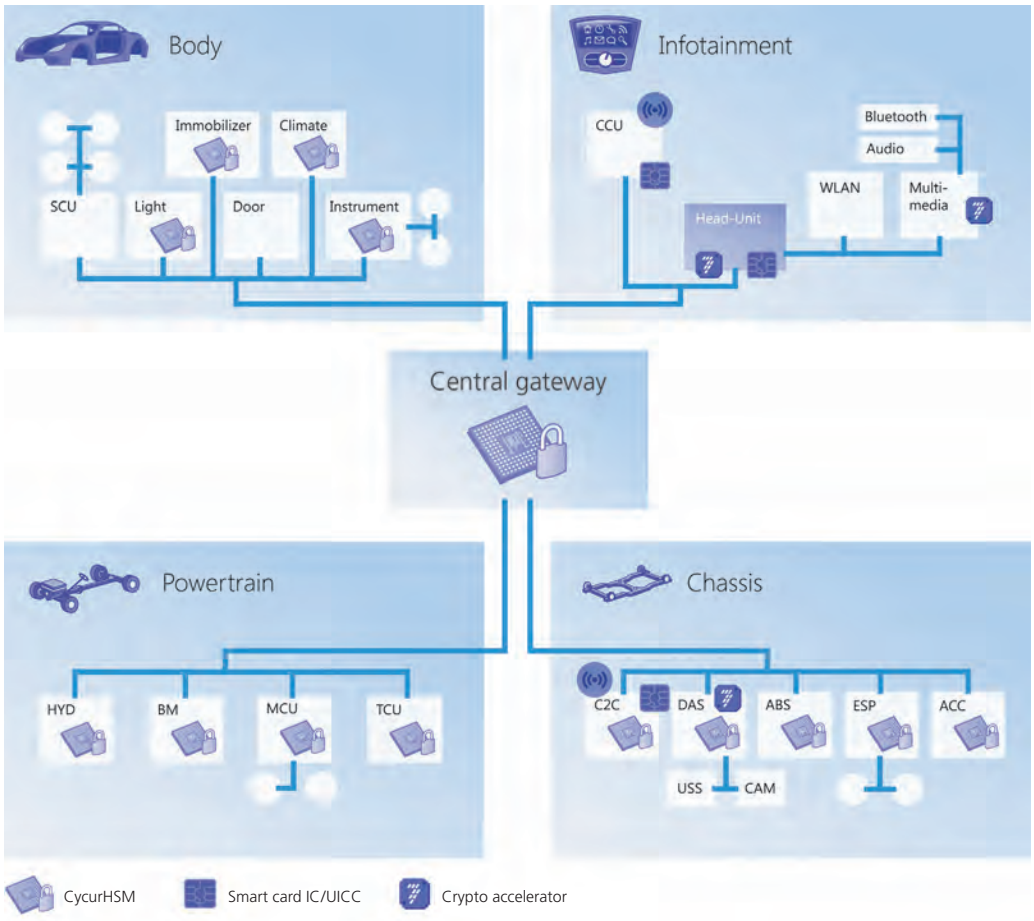
tinued authenticity of ECU data. Accelerator hardware makes this testing, which is based on symmetric AES signatures, a very efficient process.

With its secure on-board communication function, CycurHSM provides a fourth method of protecting data passing from ECU to ECU in the vehicle. It protects the data traffic running through the vehicle bus against threats attempting to gain entry through gateways such as wireless interfaces. For this, the CycurHSM issues data on its way from ECU to ECU with AES-based message authentication codes, generating and verifying these codes so the relevant ECUs don't have to. It handles all cryptographic calculations and keeps the keys secure, thereby acting as an integrated security service provider for the ECUs.

Outlook

ESCRYPT is convinced that HSM technology will evolve over the next ten years to become a standard feature of new vehicles. The standardized CycurHSM software represents an important building block that will help this technology to break through. In conjunction with the HSM hardware, it protects safety-related IT systems in the vehicle against unauthorized access. Considering the pace at which connected technologies are advancing, CycurHSM can certainly be considered a future-ready solution.

Vehicle board network in 202x.



SCU	Seat Control Unit
CCU	Communication Control Unit
HYD	Hybrid Drive
BM	Battery Management
MCU	Motor Control Unit
TCU	Transmission Control Unit
C2C	Car-to-Car Communication
DAS	Driver Assistance System
ABS	Anti-lock Braking System
ESP	Electronic Stability Program
ACC	Adaptive Cruise Control
USS	Ultrasonic Sensor
CAM	Camera
IC/UICC	Integrated Circuit/ Universal Integrated Circuit Card