On-Chip ECU Cyber Security

Security for all Applications on Chip Level

ProMik
Trusted Solutions

ProMik
Programmiersysteme für die
Mikroelektronik GmbH
Südwestpark 100
90449 Nuremberg, Germany

Phone: +49 (0) 911-25 26 65-0
Fax: +49 (0) 911-25 26 65-66
Email: info@promik.com
www.promik.com

Certified according to:
- ISO 9001
- ISO 14001

In the heart of microchips lies the basis for the cyber security of whole applications and therefore for the protection against multi-layer intrusion attempts. To provide sufficient security, electronics manufacturers need to act at the production stage to protect applications until they are deployed in the field. With several years of industry experience, ProMik is in a pole position to provide state-of-the-art cyber security solutions on chip level.

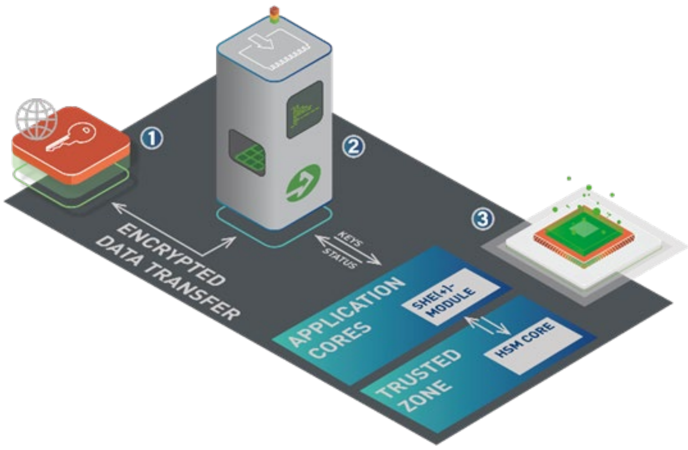

Figure 1: Cyber-Security Infrastructure

Following the programming of a special bootloader, the hardware security module (HSM) firmware is programmed and activated. This starts the highly complex HSM activation process, during which the generation and provision of cryptographic keys is also completed. ProMik ensures strong key management through comprehensive technological knowledge and implements any encryption method according to customer requirements. After key generation on the flash station, the keys are transferred to the ECU and can be written. From there, they can be transferred again to the ECU - more specifically to the HSM - and written there. Finally, the HSM firmware is deactivated via the user configuration block (UCB). After a further restart, it is possible to update the bootloader and install the application software. The UCB settings, such as the activation of the secure boot and the blocking of debug interfaces, can then be performed in the same way. During the activation process data is exchanged with the Manufacturing Execution System (MES). ProMik supports the implementation of any customer-specific software interfaces. Plug & play cyber security solutions from ProMik guarantee simple integration in production according to individual requirements, taking into account the relevant automotive standards.

Thanks to its market leadership in the development of programming solutions and bootloaders, ProMik acquired in-depth security expertise at an early stage. ProMik not only handles the entire HSM activation process, including HSM firmware programming, key programming, and provisioning as well as firmware updates, but also the locking of debug interfaces, comprehensive flash memory protection and secure boot activation.