SIEMENS DIGITAL INDUSTRIES SOFTWARE

Capital Embedded AR Classic Cybersecurity

Secure ECU software development

Benefits

- Secure mobility with vital multi-layered elements
- Secure vehicular connectivity: diagnostics, flash and over-the-air (OTA) programming, remote access, intelligent charging
- Secure E/E architecture
- Secure internal vehicle communication: Secure Onboard Communication, data storage
- Secure ECU: data filtering, intrusion detection

Advanced ECU design with AUTOSAR software and tooling

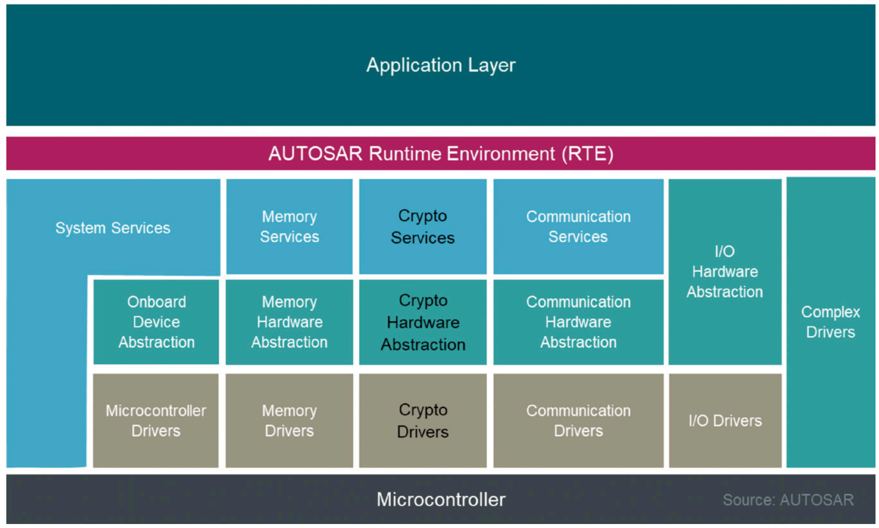
Capital™ Embedded AR Classic software is Siemens' implementation of the AUTOSAR standard. It is a complete offering with tools and software platform to meet all ECU platform needs, from ECU extract updates to software platform configurations.

Cybersecurity

Modern vehicles are increasingly connected. They contain a highly sophisticated electrical and electronics (E/E) architectures with a large number of entry points. Cybersecurity provides authenticity, integrity and confidentiality mechanisms to protect against digital threats like data tampering and denial of service.

Features

- Standard AUTOSAR components for on-board security
- AUTOSAR crypto stack: Crypto Service Manager, Crypto Interface, Crypto Driver, Key Manager
- AUTOSAR Secure Onboard Communication
- Secure Hardware Extensions (SHE)
- Transport Layer Security (TLS)
- Automotive-grade Hardware Security Module (HSM)
- Automotive-grade embedded firewall



AUTOSAR layered architecture

AUTOSAR security features

The standard AUTOSAR components for on-board cybersecurity are an integral part of Capital Embedded AR Classic. The AUTOSAR crypto stack offers standardized access to cryptographic services for applications and system functions with the following components:

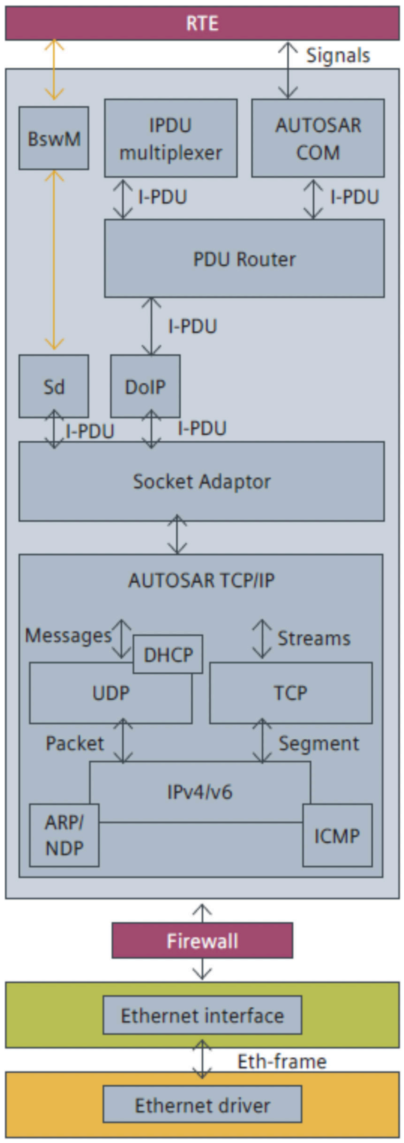
- Crypto Service Manager (CSM) provides an abstraction layer for a standardized interface to higher software layers. With synchronous or asynchronous services, it enables access to basic cryptographic functionalities.
- Crypto Interface (CryIf) is located between the low level crypto solutions, e.g. Crypto, and the upper service layer, CSM. It provides a unique interface to manage different crypto hardware and software solutions like HSM, SHE or CDDs.
- Crypto Driver (Crypto), located in the MCAL, implements a generic interface for synchronous and asynchronous cryptographic primitives. Cryptographic services, like key management functions, and objects, like an AES accelerator, are also supported.

- Key Manager (KeyM) consists of two submodules: Crypto Key and Certificate. Crypto Key provides API and configuration items for pre-defined cryptographic key material. Certificate provides API and configurations to operate on certificates.
- Secure Hardware Extensions (SHE) consists of three building blocks: a storage area for cryptographic keys, a block cipher implementation and a control logic to connect SHE components to the CPU of the microcontroller.
- Secure Onboard Communication (SecOC) communicates with PduR to provide authentication mechanisms for critical data at the PDU level. It also utilizes CSM cryptographic services and interacts with RTE to allow key and counter management.
- Transport Layer Security (TLS) provides end-to-end communication security over networks. AUTOSAR TLS extends existing Ethernet stack to enable TLS communication for selected TCP ports.

Non-AUTOSAR Security Features

Siemens Digital Industries Software expands its multi-layered cybersecurity offering with non-AUTOSAR specified components, these include:

- Hardware Security Module (HSM): Capital Embedded AR Classic's automotive-grade HSM driver supports features like true random number generation, encryption, hashing and integrity checks on generic data. It also supports digital signature functions like signature generation and verification.
- Firewall: Siemens partners with Sectigo, the industry's largest certificate authority, to provide state-of-the-art IP firewall capabilities. Capital Embedded AR Classic supports static, dynamic, deep-packet inspection, protocol and threshold filtering types.



Firewall in AUTOSAR layered architecture

Siemens Digital Industries Software

siemens.com/software

Americas
1 800 498 5351

Europe
00 800 70002222

Asia-Pacific
001 800 03061910

For additional numbers, click here.

82267-D2 2/23 IES