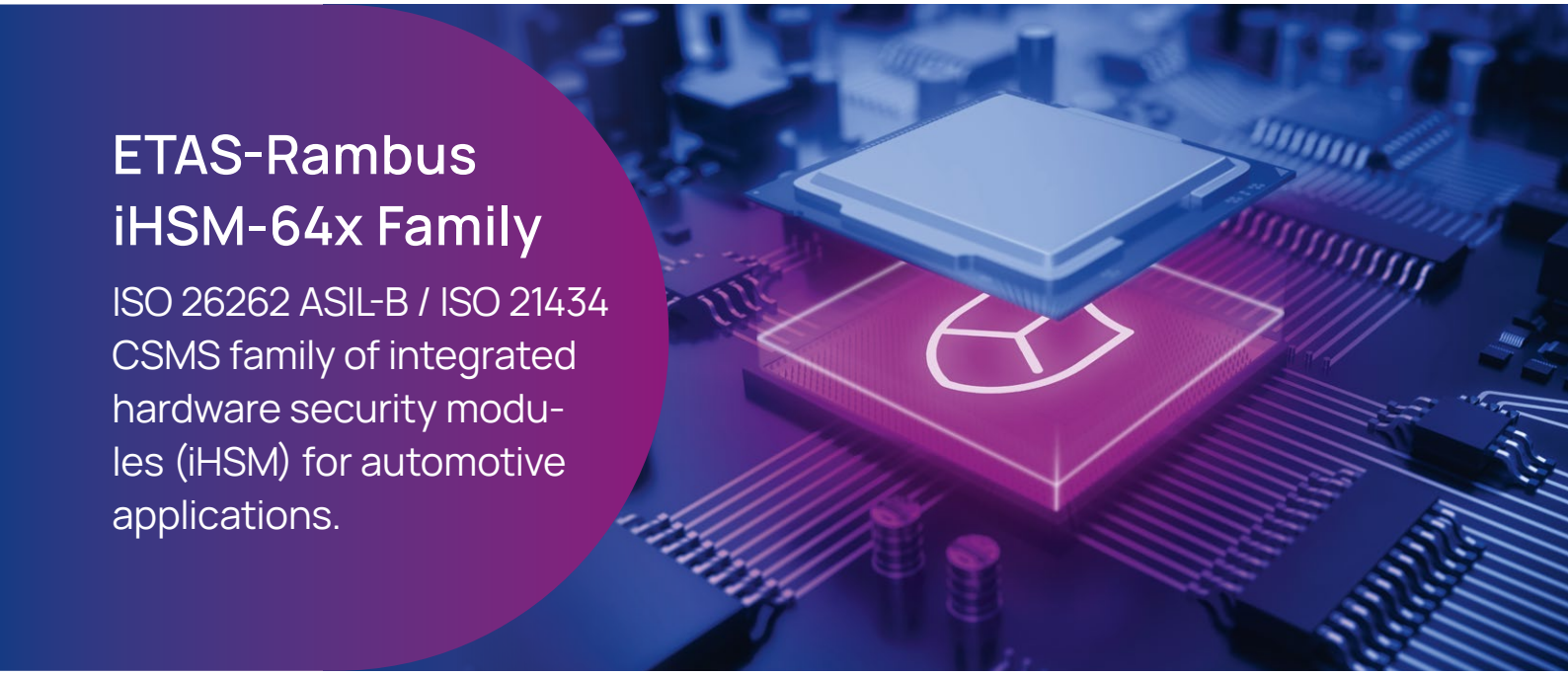


ETAS-Rambus iHSM-64x Family

ISO 26262 ASIL-B / ISO 21434 CSMS family of integrated hardware security modules (iHSM) for automotive applications.

Overview

The automotive industry is undergoing a transformative shift towards the software- defined vehicle (SDV), which will enable a new era of customer-centric mobility and create new business opportunities and revenue streams for automotive stakeholders.

However, this transformation comes with its own set of challenges that demand revolutionary approaches to navigate the ever-increasing complexity, while at the same time meeting faster time to market (TTM) demands and regulatory safety and security compliance for market access.

HSMs are dedicated hardware/software security designs instantiated in automotive SoC ICs and have become the benchmark for automotive cybersecurity.

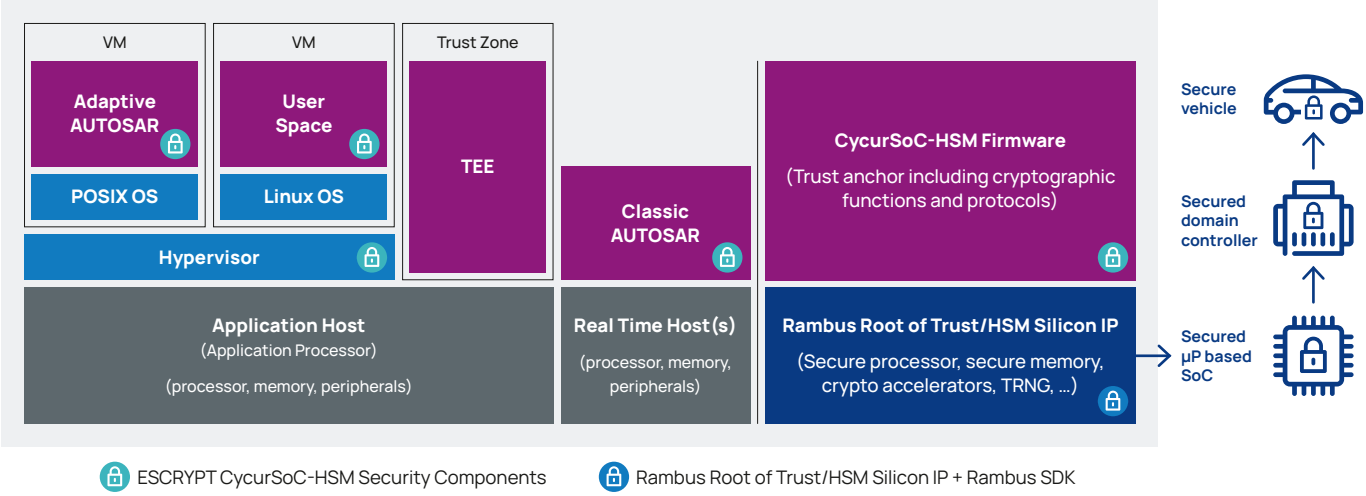
To support OEMs and SoC developers with managing design, safety, security and cost challenges, ETAS and Rambus have collaborated to develop an innovative solution that combines synthesizable HSM hardware IP with pre-integrated, pre-validated HSM software.

The full iHSM-64x stack (hardware silicon IP and software) is a pre-validated, drop-in solution critical to creating a security enclave on next-generation automotive silicon designs requiring ISO 26262 ASIL-B, ISO 21434 CSMS compliance and, optionally, Quantum Safe Cryptography.

In collaboration with Rambus

www.etas.com/cycursoc
www.rambus.com/security/root-of-trust

iHSM-64x with ESCRYPT CycurSoC and Rambus Root of Trust IP



How it Works

Hardware

The RT-64x HSM IP is a dedicated hardware security IP core for integration into automotive semiconductors. It offers a HSM that enables secure execution of authenticated user applications, tamper detection and protection, secure storage and handling of keys and security assets, and resistance to side-channel attacks. The RT-64x cores have hardware and software safety mechanisms to meet ASIL-B safety integrity levels. The RT-64x HSM IP is easily integrated with industry-standard interfaces and system architectures and includes cryptographic hardware accelerator cores. Access to crypto modules, keys, memory ranges, I/O, and other resources is enforced in hardware. Critical operations, including key derivation and storage, are performed in hardware without software access. The RT-64x HSM IP is based on a custom 32-bit processor designed specifically to provide a trusted foundation for secure processing on chips and in the system. It supports all common host processor architectures including ARM, RISC-V, x86, and others.

Software

ESCRYPT CycurSoC is an embedded cybersecurity software solution designed for contemporary and future SoC-based automotive Electronic Control Units (ECUs). It is specifically tailored to meet automotive security use cases and requirements and offers a comprehensive set of security building blocks for heterogenous SoC architectures. The solution leverages the RT-64x HSM IP capabilities to ensure optimal overall security. The software is highly efficient and has minimal impact on available system resources. Furthermore, it supports open and standardized interfaces such as SHE, SHE+, AUTOSAR Classic, Adaptive, POSIX and Hypervisor.

Integration

The pre-integrated and bundled iHSM-64x stack, which includes the RT-64x HSM IP and ESCRYPT CycurSoC-HSM software, is technology process node agnostic and can be seamlessly integrated into any SoC. This pre-validated iHSM-64x creates a security enclave on next-generation automotive silicon designs that need to meet ISO 26262 ASIL-B and ISO 21434 cybersecurity compliance requirements.

Highlights

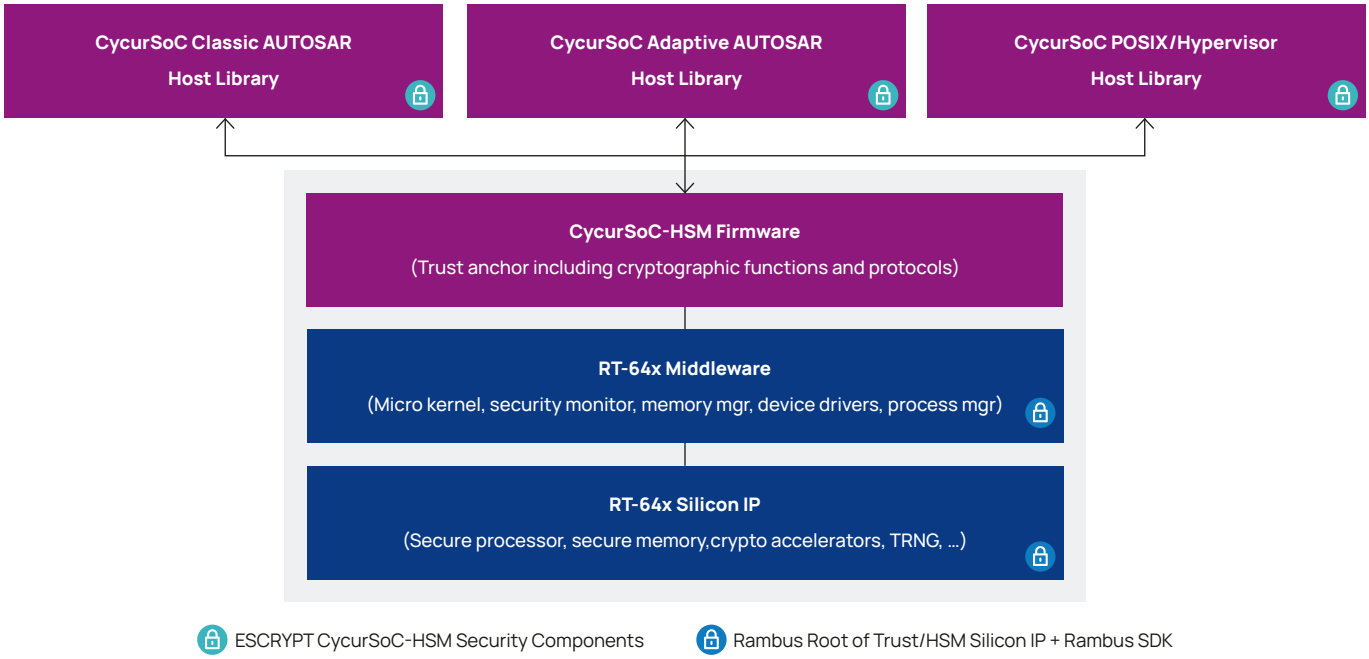
Superior Security

- State-of-the-art anti tamper techniques
- Safety mechanisms to meet and exceed ISO 26262 ASIL-B
- ISO 21434 CSMS compliant
- TRNG and PUF entropy sources
- Custom RISC-V security processor
- Multi-layered security model
- Secure HSM lifecycle management
- Secure boot, debug, update and communication
- FIPS 140-3 CAVP and CMVP compliant

Automotive Ecosystem Integration

- AUTOSAR, SHE/SHE+ support, POSIX OS and Hypervisor
- Support for multi-tenancy
- Establish trusted channel between iHSM and SoC hosts
- Automotive specific security use case support
- Support for multiple Roots of Trust
- Secure data and key store, with secure provisioning
- Certificate handling; parsing, signing, revocation, chain verification

Overview of the iHSM-64x Security Solution (Premium Version)



Features

Standard Features

- Authenticated symmetric encryption and decryption
- Symmetric encryption and decryption
- Key generation and derivation
- Key storage and trust management
- Message authentication code (MAC)
- TRNG, CSPRNG
- Hashing
- Signature generation and verification
- Security enabled host integration
- Cryptographic hardware acceleration

Premium Features

- Key wrap and transport
- Key encapsulation
- Certificate handling
- Asymmetric encryption and decryption
- Classic and Adaptive AUTOSAR, POSIX and Hypervisor integration
- SHE+ key support

Automotive Use Cases

Standard Use Cases

- Secure boot
- Secure firmware update
- Authentication and attestation
- Secure data store and key store
- Physically unclonable function
- Device personalization
- Key and data provisioning
- Secure communication
- Runtime integrity checking

Premium Use Cases

- Secure debug
- Secure lifecycle management
- Secure manufacturing provisioning
- Secure diagnostic
- Access management
- Secure logging
- OEM-specific cybersecurity use cases

RT-64x Hardware Security IP

- ISO 26262 ASIL-B certified (RT-640) and compliant (other RT-64x configurations) core with Rambus custom-designed 32-bit secure RISC-V processor, AXI Interface to SoC, and fast 64-bit addressable DMA to host memory
- Multi-layered security model including hierarchical privilege model, secure key management policy, hardware-enforced isolation/access control/protection, error management policy.
- Canary logic for protection against glitching and over-clocking, secure key derivation
- Protects all core components against a wide range of attacks
- Secure data store allowing assets generated during boot available for secure applications
- Wide range of cryptographic hardware accelerators and security modules:
  - NIST CAVP/CNSA 1.0: AES (all modes), SHA-1/2/3
  - (all modes), HMAC and CMAC, RSA up to 4K, ECC up to 521, ECDSA, EdDSA, RSA, SM2DSA sign/verify, SP 800-90a/b/c Random Bit Generator (TRNG and PRNG)
  - Optional Chinese Encryption with OSCAA SM-2-3-4
  - Optional CNSA 2.0 Quantum Safe Cryptography with LMS and XMSS hash-based signature schemes and SHAKE XOF, FIPS 203 ML-KEM (Kyber) and FIPS 204 ML-DSA (Dilithium)

ESCRYPT CycurSoC Security Software

- Implements security functionality that is critical to the creation of a security enclave on the HSM core or TEE host
- Offers cryptographic protocols and algorithms to the application
- Helps to effectively fulfill complex automotive OEM security requirements, while ensuring a smooth integration into the overall system architecture
- Retains integrity of data and functionality to achieve reliability, safety and data protection
- Is abstracted from the requirements of an OEM and the underlying silicon, thus enabling sourcing one security solution that fits all and saves on cost
- Comes as a standard and premium package
  - standard package: offering basic cryptographic and key management and acceleration.
  - premium package: adding secure application startup, secure provisioning and update, secure life cycle management, and integration into AUTOSAR, POSIX, and Hypervisor

Deliverables

Complete Documentation
- Integration guides, programming guides, reference manuals
- ISO 26262 FMEDA and safety manual
- ISO 21434 support package (including TARA) option

RTL and FW Package
- Verilog RTL for synthesis and simulation
- Standard EDA tool flow scripts and support files
- Verification test bench and test vectors
- Boot loaders and secure RTOS and security monitor firmware
- HLOS APIs for accessing RT-64x capabilities

SW Package
- SDK with QEMU emulation and debugging capabilities
- One-step install sample and reference code

ESCRYPT CycurSoC SW Package
- CycurSoC Standard: HSM firmware binary
- CycurSoC Standard: generic host component
- CycurSoC Premium: classic AUTOSAR host components
- CycurSoC Premium: adaptive AUTOSAR host components
- CycurSoC Premium: POSIX and Hypervisor host components pending the use cases and requirements
- CycurSoC Premium: OEM bootloader host components

ESCRYPT CycurSoC Product Artifacts
- CycurSoC product artifacts
- Release notes
- CycurSoC API documentation
- API header file
- User guide
- Target integration guide
- Safety advice

Are you interested in ETAS products and solutions?
Please write to us at: **info@etas.com**

Further product information:
www.etas.com/cycursoc

ETAS/COM2_AS/04/2024