SECURE-IC
THE SECURITY SCIENCE COMPANY

Securyzr™ > Securyzr™ Secure HW Solutions > Securyzr™ iSE > SCZ_iSE_XZU+_BA471
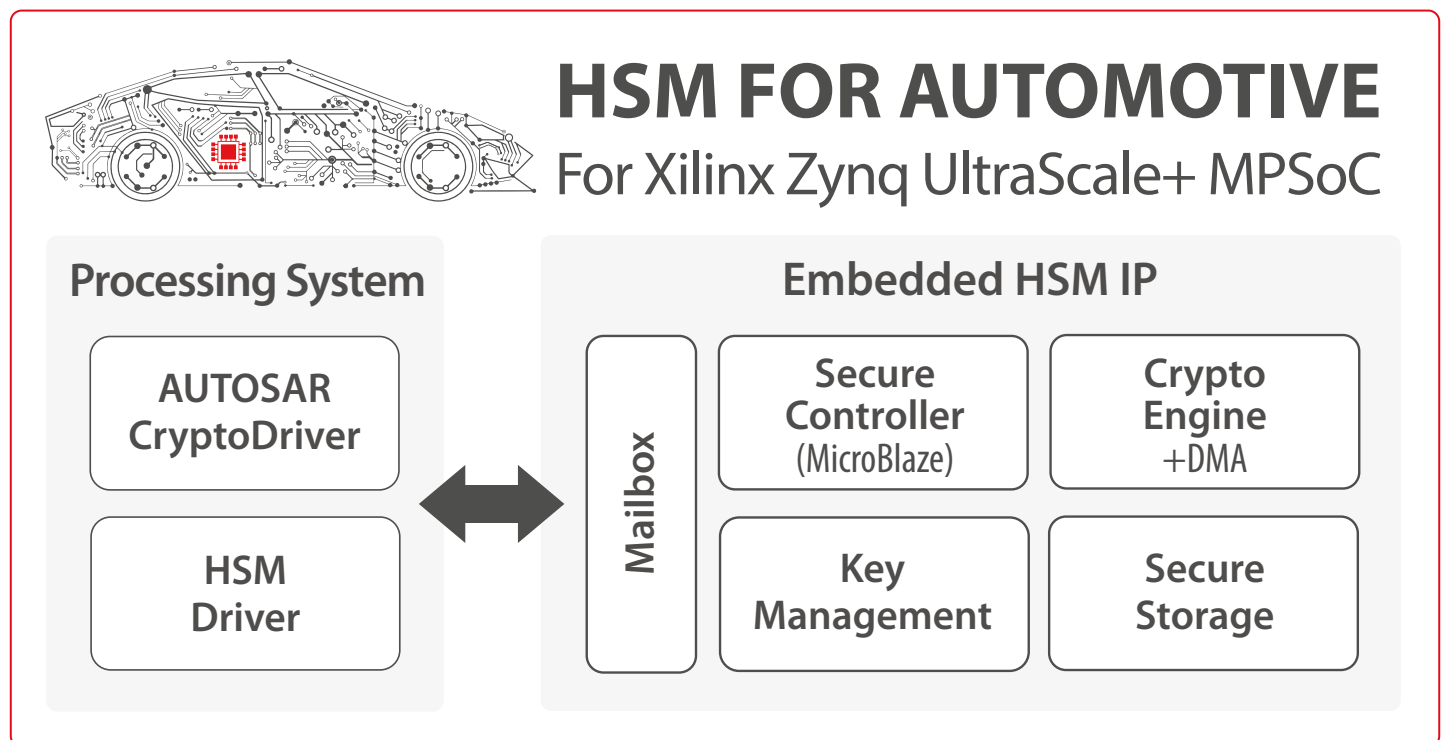
HARDWARE SECURITY MODULE (HSM) FOR AUTOMOTIVE

The HSM IP module is a Hardware Security Module for automotive applications. It is developed, validated and licensed by Secure-IC (partner of Xilinx) as an FPGA-based IP solution dedicated to the Xilinx Zynq UltraScale+ MPSoC platform.

As the connectivity of industrial systems, cars and their subsystems (like ADAS, autonomous driving, infotainment) is growing, so is the need for data integrity and system authentication. A very important aspect of this embedded security is a hardware security module (HSM), a security enclave that provides secure key management and cryptographic processing.

This HSM IP module removes the need for a dedicated HSM device and it incorporates 2 solutions:
• The **HSM hardware IP**, to be implemented in programmable logic and ready to interface with the Zynq UltraScale+ processing system.
• A **software stack** containing the HSM firmware, HSM driver code and an interface layer allowing integration.

HSM FOR AUTOMOTIVE
For Xilinx Zynq UltraScale+ MPSoC

Processing System

- AUTOSAR CryptoDriver
- HSM Driver

Mailbox

Embedded HSM IP

- Secure Controller (MicroBlaze)
- Crypto Engine +DMA
- Key Management
- Secure Storage

Features

- Secure key provisioning
- Secure key storage
- Secure counter
- Flexible anti-tampering
- Easy to integrate (AXI interface)
- Cryptographic operations offload
  • PK engine
  • Symmetric engine
  • Random number generator
- Flexible and scalable platform

SUPPORTS ISO 26262

Applications

- AD/ADAS security
- Infotainment security
- Radar/LiDAR security

Configurable, scalable and flexible solution

The hardware security module can be scaled and configured to match any requirement, even for the most demanding applications. The size and performance of the solution can be adapted for a perfect application fit while leaving room in the FPGA for other critical applications.

Xilinx Zynq UltraScale+ MPSoC platform

The XA Zynq UltraScale+ MPSoC family from Xilinx is automotive qualified, enabling development of safety critical ADAS and Autonomous Driving Systems.

Its low-power domain has been certified to meet ISO 26262 ASIL-C level requirements by Exida, an accredited certification companies specializing in automation and automotive system safety and security.

Automotive Qualified
ISO 26262 Certified

ZYNQ. MPSoC

XILINX

Deliverables

✅ FPGA netlist or encrypted RTL	✅ HSM firmware/driver	✅ AUTOSAR CryptoDriver	✅ Self-checking testbench
✅ Simulation model	✅ Reference simulation script	✅ Reference implementation script	✅ Documentation

V1.2

We are also offering Hardware Security Modules for other applications (i.e. industrial, defence…). For more detailed information, please see our dedicated product sheet.