ARC SEM130FS Safe and Secure Processor

Highlights

- ASIL D compliant dual-core, lockstep safety processor supports ISO 26262 automotive safety standards and provides advanced security to protect against evolving threats
- Secure privilege mode orthogonal to kernel/user mode
- Integrated self-checking safety monitor capable of time diversity
- Uniform instruction timing and timing/power randomization for side channel resistance
- Includes hardware safety and security features: ECC, integrated user-programmable windowed watchdog timer, lockstep safety monitor, side-channel protection, fault-injection protection, enhanced memory protection and SecureShield™ technology
- Performance and area-efficient safe and secure processors for auto and embedded applications
- MetaWare Toolkit for Safety with ASIL D Ready certified compiler
- Comprehensive safety documentation eases SoC certification process

Target Applications

- Automotive hardware secure modules
- ADAS SoCs
- Automotive sensors
- Automotive controllers
- IoT Industrial/Smart cities

The DesignWare® ARC® SEM130FS Safe and Secure Processor simplifies development of safety-critical automotive applications while enabling designers to integrate security into their SoC to protect against logical, hardware and physical attacks. The ASIL D compliant SEM130FS processor is a pre-verified dual-core lockstep implementation including a self-checking safety monitor, error correction code (ECC), and a windowed watchdog timer.

The ARC SEM130FS processor (Figure 1) includes SecureShield™ technology to enable creation of a Trusted Execution Environment (TEE) to isolate multiple execution contexts and protect secure functions from software vulnerabilities in user code. In addition, the safe and secure processor provides protection from side-channel attacks featuring uniform instruction timing, timing randomization and power randomization.

The ARC SEM130FS processor is supported by a comprehensive set of safety work products and the ARC MetaWare Toolkit for Safety with ASIL D Ready certified compiler to generate ISO 26262 compliant code.

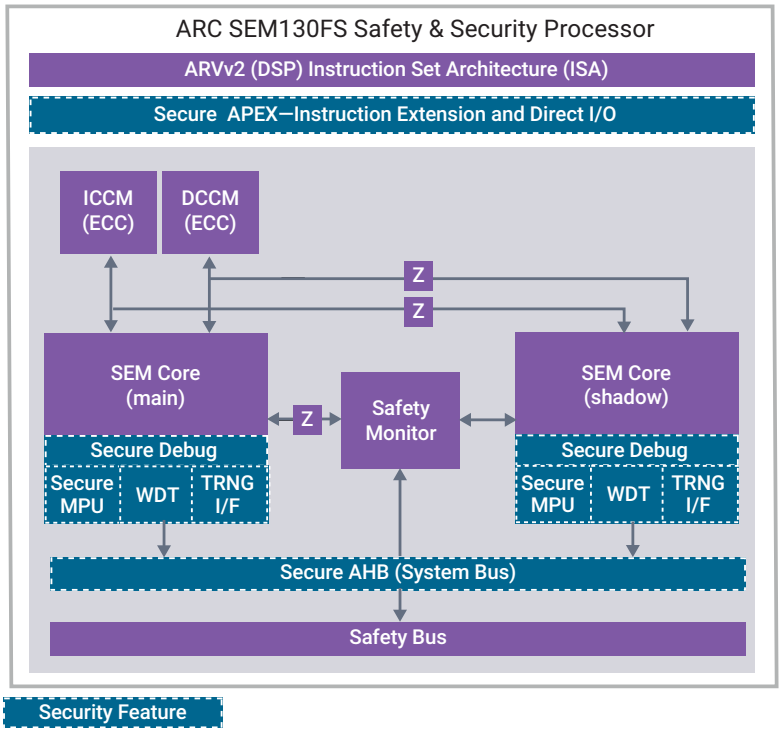

Figure 1: ARC SEM130FS Secure and Safe Processor block diagram

Hardware Safety and Security Features

The ARC SEM130FS processor includes hardware safety features that simplify the implementation of safety in an SoC and ease the ISO26262 certification process. The safety processor supports error detection and correction logic for data and address errors on closely coupled memories. Also, hardware stack protection is included to check overflow and underflow of reserved stack space. An integrated watchdog timer helps recover from a deadlock situation. The integrated memory protection unit (MPU) defines variable regions and assigns access attributes to help protect against malicious or misbehaving code in critical applications.

Lockstep Monitor

The SEM130FS implements a dual core lockstep solution that includes a self-checking safety monitor. The safety monitor provides monitoring to ensure the main core and the shadow core maintain lockstep operation. Support of time diversity is also available, whereas the inputs of one core are delayed by N clock cycles and the outputs of the other core are delayed by the same duration and the results are compared. In this approach, the second core would be performing the same operation N clock cycles after the first one, significantly reducing the probability of a noise pulse hitting both cores and affecting their function. Time diversity buffers include parity checking to reduce single point failures.

SecureShield

SecureShield technology is a set of core features that enable system designers to develop a trusted execution environment to isolate security related and standard core operations on a single ultra-low power processor, eliminating the area and power that an additional security core and associated memories would require. SecureShield technology includes protected access control for their critical core registers and system bus and features a secure MPU with up to 16 configurable memory regions.

Side-Channel Attack Protection Features

The SEM130FS Processor offers additional system protection features including side-channel attack resistance and in-line instruction. These side-channel countermeasures increase resistance to simple and differential power analysis. The ARC safe and secure family of processors incorporates support for power randomization on the data path, pipeline and ALU.

Additionally, as instruction timing information can also be used to learn about the cryptography operations being performed, the SEM130FS processor supports uniform instruction timing and have the capability to randomly insert instructions without side effects into the pipeline.

Development Tools and Software

To facilitate rapid development with ARC processors, they are supported by a complete suite of development tools that generates highly efficient code ideal for deeply embedded applications. For developing safety-related software to meet ISO 26262 compliance requirements, certified versions of the MetaWare Development Toolkit and the MetaWare Compiler are available. These products have been certified by SGS-TüV Saar GmbH as ASIL-D compliant and include a Safety Guide and Safety Manual for using MetaWare tools in safety applications. The suite of development tools also includes ARC simulators including xCAM and nSIM, and the ARChitect core configuration tool.

Documentation

The following documentation is available for the DesignWare ARC SEM130FS processor:

- ARCv2 ISA Programmers Reference Manual
- ARC SEM130FS Databook
- ARC SEM130FS Integration Guide
- ARC SEM130FS Safety Manual
- ARC SEM Security Guidelines

Testing, Compliance, and Quality

Verification of the ARC SEM130FS follows a bottoms-up verification methodology from block level through system level and includes coverage for systematic and random failures. Use of MIPS tools for fault injection and analysis aid in development of robust and comprehensive diagnostic tests to verify ARC processors ability to meet the stringent automotive safety standards.

Additional Licensable Options

To enhance functionality of the ARC SEM130FS, options are also available for license that have been tested and verified with the solution. These options include µDMA, Floating Point Unit(FPU), and CryptoPack cryptographic accelerator. The DesignWare ARC CryptoPack option provides the ability to speed up software encryption implementations by adding custom instructions and registers to the ARC SEM130FS processor using the ARC Processor Extension (APEX) interface allowing it to have safe and secure options while supporting software algorithms such as Advanced Encryption Standard (AES), Triple Data Encryption Standard (3DES), Elliptic Curve Cryptography, Secure Hash Algorithm with 32-bit words (SHA-256) and River-Shamir-Adleman (RSA) encryption.

Compliance

- The ASIL B and ASIL D Compliant ARC SEM130FS Processor is developed and assessed specifically for ISO 26262 random hardware faults and ASIL D systematic development flow.
- The Certified ASIL D Compliant ARC MetaWare Development Toolkit for Safety is certified as ASIL D Compliant according to ISO 26262-8 2018 as suitable for the development of safety related software up to ASIL D.

About MIPS:

MIPS by GlobalFoundries delivers software to silicon with RISC-V for building physical AI platforms. MIPS delivers software-hardware co-design, optimized AI, and custom ASSP design and manufacturing. Together with ARC, MIPS delivers the open, standards-based processor IP portfolio for embedded applications. Physical AI is built on MIPS.

For more information, visit **www.mips.com/arc.**