



Arm Functional
Safety Partner
Software & Tools

Application Areas

- + Automotive
- + Avionics
- + Industrial
- + Railway
- + Medical
- + Agricultural

Links

- + [COQOS Hypervisor SDK](#)
- + [COQOS Micro SDK](#)
- + [Safe Cockpit Controller](#)
- + [Safe and Secure DMS](#)

Goal

OpenSynergy provides embedded software products for the next generation of vehicles. It has developed the virtualization platform COQOS Hypervisor SDK to support the convergence of software-based vehicle functions with different requirements on safety. The design is suitable for multi-display cockpit controllers, telematics systems, or powerful domain controllers using a mix of AUTOSAR technology and open solutions, such as Linux and Android. COQOS Micro SDK is a variant of this hypervisor to be used for automotive virtualization on microcontrollers.

Challenge

A significant challenge for automobile manufacturers is the large number of control units in the vehicle. The more cars become highly automated or even partially autonomous, the larger the number of functionalities. This high number of functionalities has a relevant effect on the Bill of Material (BOM), the car's weight, and its fuel consumption. A further increase in hardware in vehicles would be neither ecologically nor economically justifiable. Therefore, manufacturers and suppliers will not be able to avoid integrating several functions on central control units.

OpenSynergy's COQOS Hypervisor has been designed as a low-complexity embedded hypervisor, especially fitting to automotive applications. It allows customers to build highly compartmentalized systems that can be tailored to the specific requirements.

Solution

COQOS Hypervisor SDK enables the convergence of several functionalities on a single System-on-Chip (SoC) while providing freedom from interference between systems of different criticality (assigned to different ASIL levels such as QM, A, B). The core technology of COQOS Hypervisor SDK is the hypervisor. The hypervisor makes it possible to run several guest Operating Systems (including Linux, Android, AUTOSAR, or other operating systems) in separated virtual machines.

A typical use case is the safe cockpit controller that runs an instrument cluster and an in-vehicle infotainment system simultaneously, on a single processor. On the system level, utilizing our fine-grained permission system, it is possible to limit the virtual machines to the required resources and detect and handle malicious behavior. Random hardware faults are detected/treated by utilizing the safety architecture of state-of-the-art safety hardware.

Benefits

- ✦ Using COQOS Hypervisor to integrate several functionalities on a single SoC leads to a system that has a lower BOM cost, uses less space, weighs less, and consumes less energy than distributing the same functionality across several individual ECUs.
- ✦ COQOS Hypervisor SDK is highly configurable so that customers can, for example
 - change the number of VMs
 - assign to physical cores and temporal behavior
 - connect via inter-VM communication channels
 - grant access rights of VMs to devices
 - use it as security features of the hardware
- ✦ It is minimalistic in its design and therefore is small, fast, and certifiable.

How does the product/solution/service relate to Arm technology?

The design of COQOS Hypervisor SDK follows the multi-kernel architecture of the Armv8 architecture and takes advantage of the hardware virtualization of the SOC using this architecture. Virtualization adds a new dimension to the hardware abstraction ecosystem, i.e. the built-in extensions that make running a hypervisor very efficient.

The Armv8-R architecture has added extensions for virtualization to the "R" (Real-Time) family used in the [Arm Cortex®-R52 core](#), adopted by new controllers. OpenSynergy's hypervisor variant for microcontrollers, COQOS Micro SDK, has been one of the first hypervisors taking advantage of these extensions: OpenSynergy implemented the NXP S32S safety microcontroller as the lead platform for the development of the first Arm Cortex-R based hypervisor. OpenSynergy's COQOS Micro SDK can also support other chips using the Arm Cortex®-R52, such as the STMicroelectronics Stellar family.

OpenSynergy utilizes trained personnel and specific technical resources in the development of functionally safe products. The Quality Department is responsible for the independent confirmation that product development complies or surpasses industry safety standards when relevant. It includes the administration and improvement of a Quality Management System that provides the knowledge for safe development of SEooC software to Automotive Safety Integrity Level D. Regular training in the use of the QMS are provided to the engineers. The toolchain for safety projects comprises certified and qualified tools that comply with the Tool Confidence requirements of ISO26262:2018. Additionally, specialist consultants support the engineers working on safety-relevant development as necessary.