Virtual Open Systems: Automotive mixed-critical virtualization done right

Case Study

Goal

The VOSySmonitor hypervisor enables safety-critical virtualization in all types of vehicle, providing a solution that maximizes performance, security, scalability and openness. VOSySmonitor meets ISO 26262 requirements and has been certified to ASIL C.

Challenge

Vehicle software complexity is increasing exponentially, with a strong demand for solutions to optimize resource utilization, ease development/maintenance of new features, to enable secure over-the-air updates. In addition, pervasive connectivity and user device interactions increases vulnerabilities on the vehicle attack surface. Hackers have already demonstrated their ability to exploit such vulnerabilities by taking control of the vehicle and accessing personal user data. For this reason, security and isolation of safety-critical applications are key challenges to be addressed in modern automotive solutions.

Finally, the industry has seen Tier 1 and OEM innovation capability limited by software stacks created within closed software ecosystems with expensive license fees and technical limitations due to legacy architectures. In this context, Tier 1s and OEMs risk a technology and business lock-in which could prevent them from being able to optimize system architecture, increase scalability and reduce overall system costs.

Solution

VOSySmonitor is an ISO 26262 ASIL C certified safety-critical hypervisor built on Arm TrustZone that enables the concurrent execution of multiple operating systems with different levels of criticality. The innovative VOSySmonitor architecture splits the system in two main compartments, one for the safety critical and the other for standard applications, isolating them with the use of Arm TrustZone.

Such isolation is of pivotal importance to provide security, with safety critical applications running fully protected (in a separate memory address space with tagged caches and isolated devices) from the standard applications. Moreover, VOSySmonitor is positioned in the lowest level of the vehicle software stack (Arm monitor layer), providing strongest control on the system resources partitioning and highest flexibility. In fact, VOSySmonitor does not impose any closed solution (e.g., RTOS, AUTOSAR system, etc.) and is fully compliant with open source technologies like XEN, KVM, Linux, Android, Automotive Grade Linux, etc.

Benefits

- **Simplified virtual electronic control units:** VOSySmonitor enables the execution of multiple operating systems on the same platform with no performance overhead, reducing hardware and wiring costs, easing software maintenance and prototyping.
- **Highest security and safety:** VOSySmonitor partitions the system resources isolating safety critical applications in a protected compartment. It is ISO 26262 ASIL C certified and supports security Trusted Execution Environment implementations like OPTEE.
- **Scalability and openness:** VOSySmonitor provides a scalable solution with increasing complexity from simple use cases (for instance with Linux running with an RTOS) to ADAS applications with a high number of operating systems working together. VOSySmonitor's ecosystem is fully open and supports open source hypervisors for non safety-critical applications.

Automotive applications

- Consolidation of multiple functions in a single hardware platform (e.g., IVI and instrument cluster and BCM, eCockpit
- Automotive emergency call, secure connectivity and telematics
- Autonomous driving applications with multiple safety-critical and non safety-critical workloads

Why Arm

VOSySmonitor is based on Arm TrustZone technology, which enforces among others, memory, CPU and interrupt isolation between the RTOS and the GPOS. These characteristics help to provide security isolation, upon which co-execution of critical operations can be implemented, while based on a secure TrustZone foundation.

VOSySmonitor has been specifically designed to ensure highest security leveraging on Arm TrustZone. By implementing virtualization at the TrustZone level, Virtual Open Systems not only offers the highest security available, but also lets customers freely use virtualization extensions in automotive applications (e.g., using open source hypervisors like XEN). This is the key to VOSySmonitor innovation.

What's next?

- Virtual Open Systems is leading the Automotive Grade Linux (AGL) Virtualization Expert Group. The company is working with Arm in this domain to enable open source virtualization in AGL.

- VOSySmonitor is also a good fit for IoT, healthcare and industry 4.0 use cases.

For more information on Virtual Open Systems

VOSySmonitor
http://www.virtualopensystems.com/en/products/VOSySmonitor/

VOSySmonitor based automotive software stack solution
http://www.virtualopensystems.com/en/products/vosysmcs/

VOSySmonitor video demo
http://www.virtualopensystems.com/en/solutions/demos/VOSySmonitor-emcos-ew2019/

VOSySmonitor ASIL C certificate
http://www.virtualopensystems.com/en/company/VOSySmonitor-iso26262-asilc/

VOSYS twitter account
https://twitter.com/VOSySofficial

Email
contact@virtualopensystems.com

See these related links for more information:

Arm Automotive solutions - https://www.arm.com/solutions/automotive

Arm Safety Ready - https://www.arm.com/why-arm/technologies/safety

Arm TrustZone - https://developer.arm.com/ip-products/security-ip/trustzone