ETAS

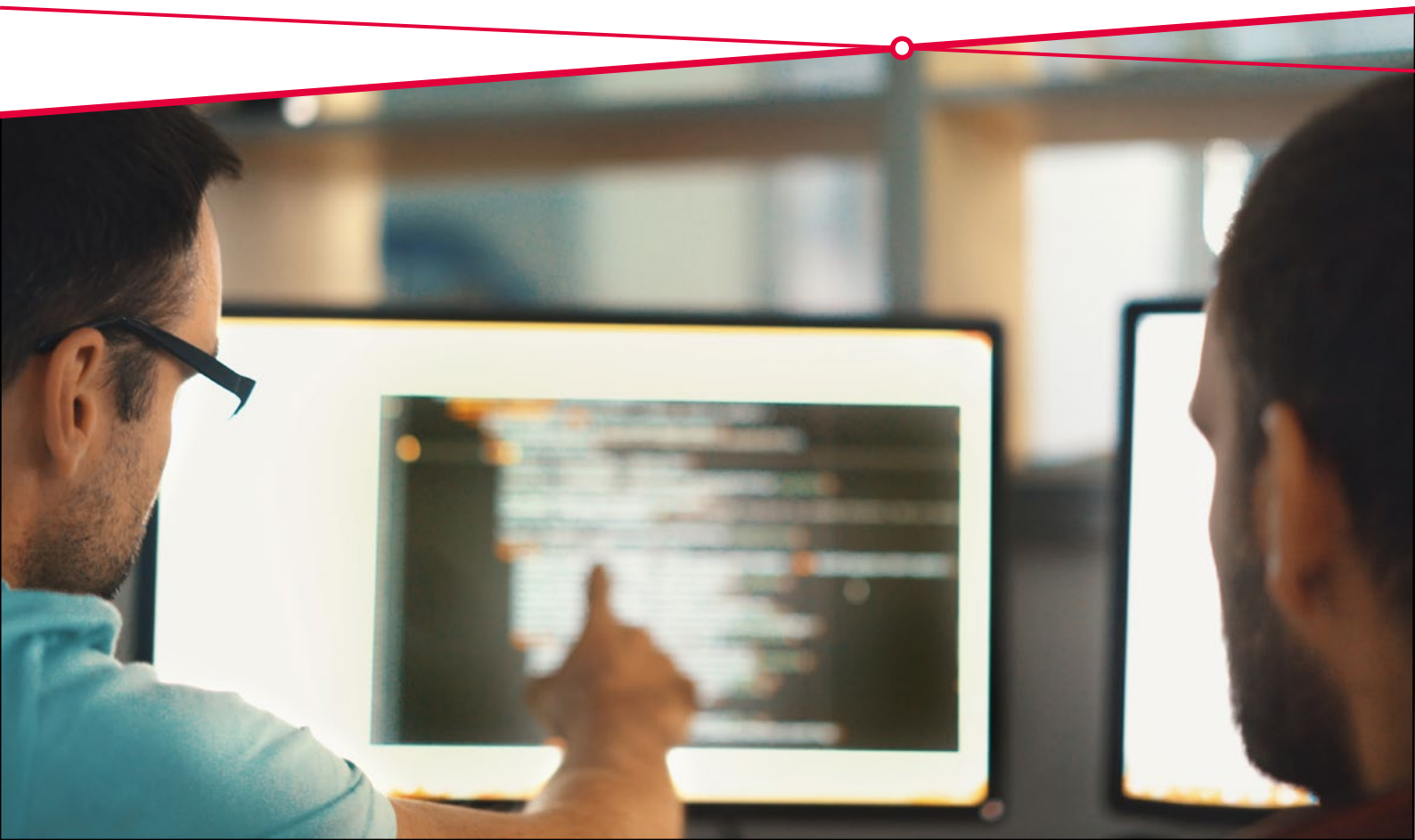
DRIVING EMBEDDED EXCELLENCE

Translated article "Schlanker Hypervisor für unterwegs," Design & Elektronik online, Oct. 11, 2018

Virtual ECUs in Production Vehicles?

ETAS Lightweight Hypervisor provides flexibility, efficiency, and security

Agile software development is a growing trend in the automotive industry. The idea is that customers should be able to upgrade and update software-controlled vehicle functions without any safety or security concerns. This presupposes a strict separation between individual software functions. For hardware, however, the trend is moving in the opposite direction, with more and more functions running on central ECUs. To resolve this contradiction, Bosch Automotive Electronics is using the new Lightweight Hypervisor from ETAS.



After three accident-free years, the day has come. Leon's parents log onto the OEM website to finally remove his car's software-controlled power limiter, which was activated when he got his driver's license. While they are at it, they also install the new multimedia package Leon wants and for which he pays half. A prerequisite for function upgrades carried out at a later date and ongoing (over-the-air) updates is that modifications should never affect other software. But how can we guarantee that, when the current trend is toward concentrating ever more connected functions on a few central ECUs? And in such an environment, is it even possible to use tests to validate and verify in advance the functional safety of the overall system after the upgrades and updates? These two questions illustrate how critically important it is to reliably separate software functions from each other.

Practical partitioning is needed

Reasons other than functional safety argue for this separation, too. For one, it simplifies the workflows in development when software from different manufacturers runs on a single ECU. In addition, it ensures that ECUs are harder to attack, a very relevant aspect in times of increasing cyber crime. If hackers gain access to a function, the hypervisor places an additional high hurdle in their way. This is a strong disincentive for cyber criminals, who seek to inflict maximum damage. There are various possible ways to achieve this separation. For example, you could allocate software functions strictly to their own control hardware. However, the hardware costs and system complexity this would entail are prohibitive. A more realistic option is an AUTOSAR-based architecture with defined partitioning and separation concepts. On this basis, it is possible to upgrade individual functions while also making sure that other functions cannot be impaired. This ensures that the modification of one function does not necessitate a comprehensive revalidation of all the software on the ECU in question. However, add-ons are required to implement the AUTOSAR concepts.

Hypervisor offers a solution – but how?

This is where a hypervisor offers an effective solution: it partitions an individual ECU into various virtual machines (VM). Although the functions in fact run on the same ECU, the respective software believes itself to be in a state whereby each function has its own hardware. The functions are so strictly separated

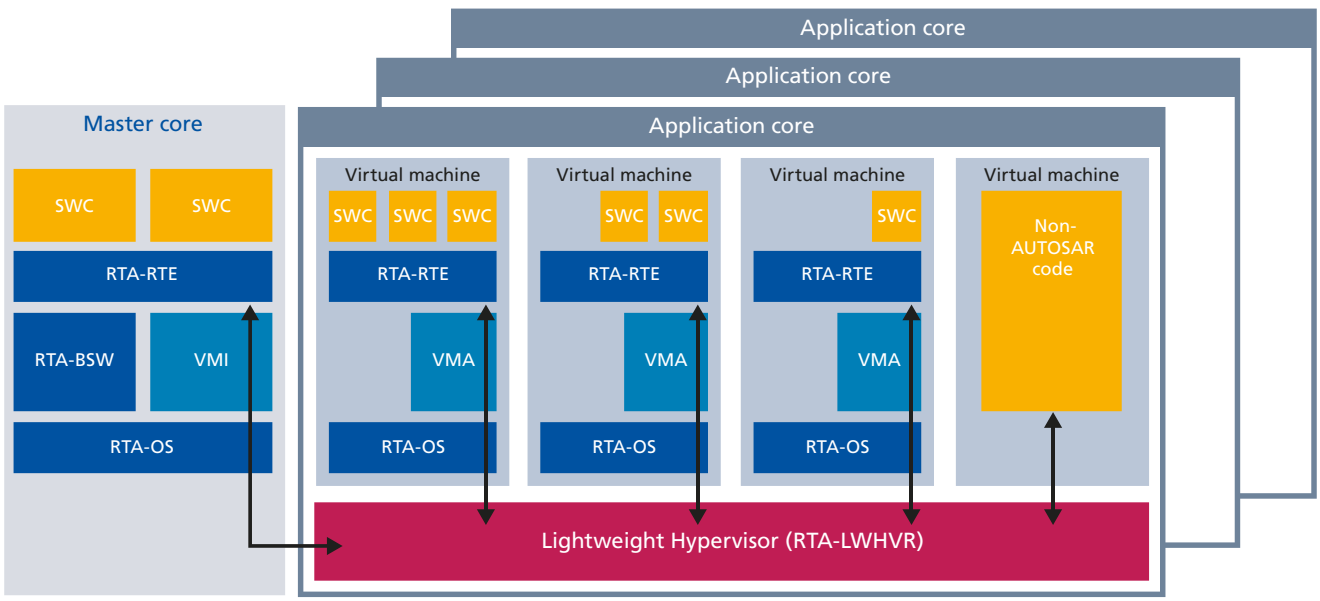


Fig. 1: ETAS COSYM – System overview.

RTA-BSW	AUTOSAR basic software
RTA-OS	Operating system
RTA-RTE	Runtime environment
SWC	Software component in secure application
VMA	Virtual machine adapter
VMI	Virtual machine interface
⟶	Inter-core communication (ICC)

that they can be modified individually without a complete revalidation – and their various manufacturers can work independently of all other manufacturers, even during development of the ECU. Software errors or malicious intruders are contained locally on a single virtual machine and prevented from spreading. And it becomes possible to operate software with different Automotive Safety Integrity Levels (ASILs) – from the lowest level (QM) to the highest (ASIL D) – on a single ECU.

For all its advantages, however, the success of hypervisor solutions depends on their implementation. Unless you adapt it to the specific environment in the vehicle, you can run into trouble. For example, a hypervisor usually needs its own memory management as well as a hypervisor privilege mode to control access authorizations. In classic versions, this has three stages: the hypervisor itself, the basic software, and the calibration functions. However, neither the corresponding memory management nor the three-stage privilege mode are supported by the vehicle microcontrollers generally used today, which has held back the wide-spread use of hypervisor technology in vehicles to date. In a project for a large OEM, Bosch Automotive Electronics – Body Electronics (AE-BE) has now managed to defuse these troublesome issues with the ETAS Lightweight Hypervisor (ETAS RTA-LWHVR). As well as reducing the memory capacity requirements of the optimized automotive hypervisor to 5 kilobytes (kB), access times were also improved by a factor of four to five. The new solution ensures that there are no influences between the virtual machines. In the specific project, a central body ECU was partitioned into eleven virtual machines, each of which was reserved for software from different suppliers. The ASIL ratings ranged from QM to B.

Lightweight Hypervisor goes beyond AUTOSAR

Despite the quantity and heterogeneity of software functions, they worked without any problems when encapsulated by the lightweight hypervisor. This succeeded because although the virtual machines access a shared memory, the access and runtimes are clearly regulated on the core. The high performance of the solution is made possible by splitting up the computer cores into a master core and various application cores.

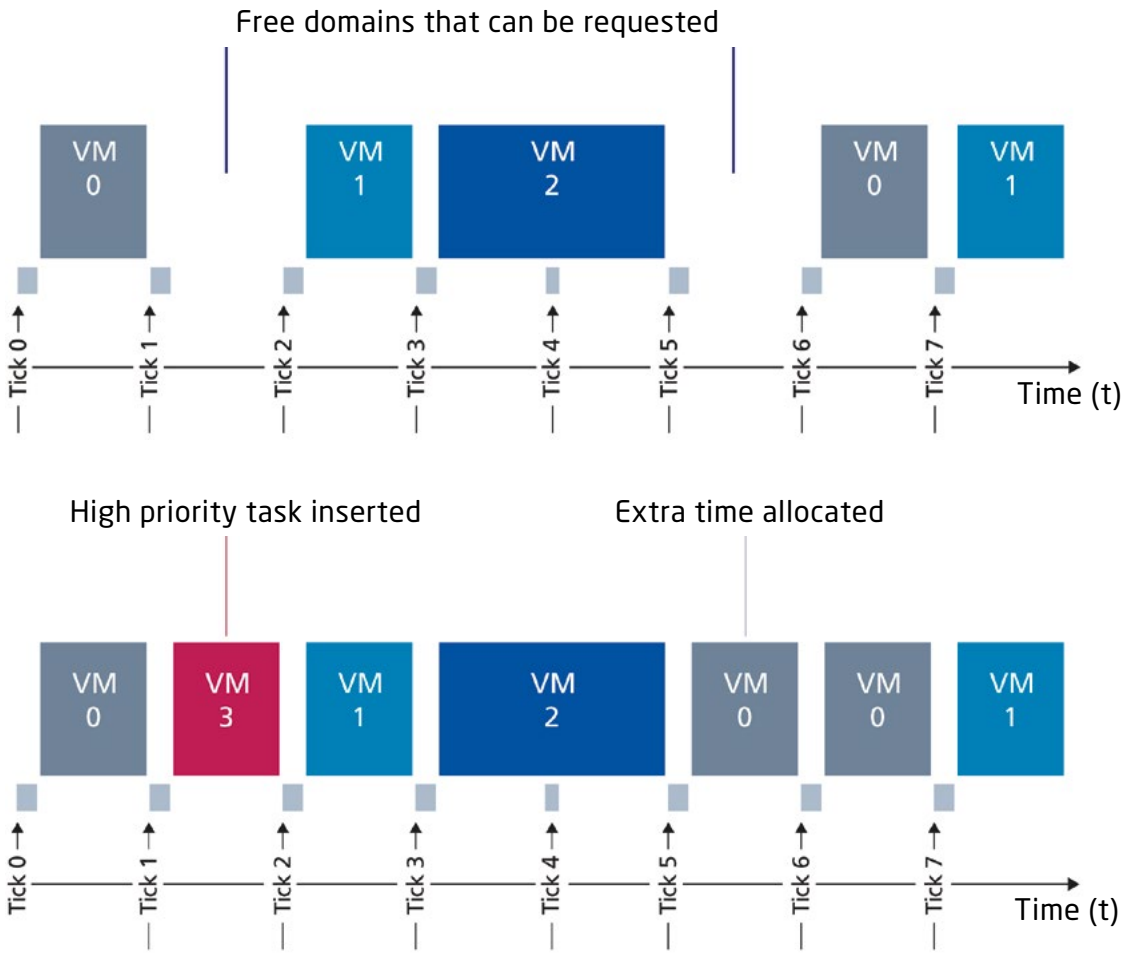


Fig. 2: Time management in an application core.

While the master core is given the job of hardware management, operation of the centralized basic software, and some software applications, the application cores contain the strictly separated virtual machines (see Figure 1) – optionally with partitioned runtime environments (RTE) as per AUTOSAR or else with non-AUTOSAR-compliant software. And all this takes place on a single ECU. With this approach, the corresponding inter-core communication (ICC), developed by Bosch AE-BE, is an important element. In addition to the execution time guaranteed under all circumstances, functions can request further time budgets without curtailing the execution of other functions (see Figure 2). Consequently, the real-time requirements are guaranteed at all times. When high runtime requirements threaten to overload their capacity, the virtual machines may ask the hypervisor if they can temporarily access additional reserved runtime windows. In such cases, the hypervisor will add the virtual machines to a queue waiting for a reserved runtime window to become available. When such a runtime window is free, the hypervisor will permit the first queued virtual machine to use it, thereby minimizing the effects of high system loading. However, each virtual machine may only request the use of one reserved window, to avoid the situation where a rogue virtual machine can attempt to gain control of the system.

Future-ready solution available today

Compared to the classic hypervisor, the overhead has been brought down to a mere 5 kB memory capacity requirement and power consumption has been reduced to 5 percent of the available core capacity. Thanks to these improvements, RTA-LWHVR fits without any difficulty into the specific boundary conditions for embedded systems in vehicles. It offers full flexibility for a wide range of applications and is available for numerous microcontrollers. At the same time, it guarantees the reliable, high-performance partitioning of ECUs, on which software from different manufacturers and safety classes can then be operated in the future. Thanks to intelligent inter-core communication and strict encapsulation, it is possible to develop softwarecontrolled functions independently of each other and – including for vehicles already owned by customers – modify them at any time without the need for time-consuming revalidation of the overall system. In this way, the Lightweight Hypervisor creates a secure basis for agile software and function development in the automotive industry, which also facilitates dynamic security systems with regular security updates as required. This removes all obstacles to individual configurations and subsequent vehicle upgrades, such as those used by Leon and his parents.

Authors

Michael Hauser is Team Leader for Software Development at Bosch Automotive Electronics in Stuttgart.
Dr. James Dickie is Product Manager RTA Solutions at ETAS Ltd in York, United Kingdom.
Dr. Nigel Tracey is General Manager at ETAS Ltd in York, United Kingdom.