Adaptive AUTOSAR for high-performance in-car computers
Adaptable for the future

elektrobit.com
Adaptive AUTOSAR paves the way for greater flexibility in ECU software in vehicles. The systems are expandable – a major step in the direction of fully automated and networked driving. Adaptive AUTOSAR is not a replacement for Classic AUTOSAR. Its strength lies instead in a smart combination of both standards.

By Dr. Roman Pallierer and Börge Schmelz

Developments such as the trend toward alternative drive concepts and automated driving place high demand on the E/E architecture inside vehicles. Automated driving functions, in particular, call for more and more powerful control units. In addition, functions are becoming increasingly networked with each other and with connected infrastructure, such as back-end systems (Figure 1). Using data from various vehicle sensors as well as external sources (such as highly precise map material) the software creates accurate environment models, for example, which are used by multiple driving functions simultaneously. At the same time, it has to be possible to update the software over the lifetime of the vehicle to take into account new functions or new security risks. The more driving tasks the software assumes, and the more connections there are to the outside world, the greater the demand is on functional safety, security, reliability, and integrity of control units.

Given these complex requirements, today’s largely static systems are soon stretched to their limits. For that reason, a small number of very powerful control units are replacing the trusted domain controller architectures. This increases flexibility and allows a dynamic distribution of functions across domain boundaries. This new architecture is enabled on the hardware side by the development of (multi-core) processors as well as the availability of Automotive Ethernet, which removes the bandwidth limitations for the exchange of information between individual modules.

Figure 1. Evolution of the E/E architecture inside vehicles. While Classic AUTOSAR was designed for control units with static functions, control units with Adaptive AUTOSAR can be enhanced with additional functions and security updates, etc. during the life cycle.
Software must become more flexible

The corresponding software requires a more flexible architecture to suit, which can represent these dynamics. That is why Classic AUTOSAR, which has established itself as the standard architecture for control units, is being supplemented with the Adaptive AUTOSAR platform. This enables a dynamic software configuration and, with service-based communication and heterogeneous computation, it provides mechanisms that ensure the necessary performance. In addition, it is easier to update or add software functions without having to restart the entire system.

Nevertheless, Classic AUTOSAR is not obsolete. This standard was designed for control units with a limited computing capacity and, unlike Adaptive AUTOSAR, it offers only a static configuration of the operating system. However, aside from the disadvantages of the major configuration effort and the limited possibilities for software enhancements, this static configuration does offer numerous advantages with the implementation of safety-relevant software components.

It therefore makes sense to combine a Classic AUTOSAR system with Adaptive AUTOSAR in order to achieve the necessary performance as well as the security of the E/E architecture for technologies like autonomous driving. But how can both standards work together meaningfully on a central control unit? Elektrobit has already gained some experience with this combination in a pilot project for series development.

Multi-core architecture with performance and safety cores

The combination of safety-relevant in particular and CPU-intensive functions begins at the hardware level. The central control unit, which uses Elektrobit software, contains a high-performance computer comprising a combination of several multi-core processors (Figure 2). These processors are divided into performance cores with integrated security hardware and safety cores. Running on the performance cores are multiple performance partitions, in which CPU-intensive vehicle and user functions are executed. They also have a security partition, which guarantees a secure startup and ensures that applications are authenticated. The safety cores, in turn, enable the execution of safety-critical functions, plausibility checks, monitoring, and validation of the results of the performance cores. The quantity and composition of the performance and safety cores are flexible in principle and based on the project requirements of the control unit. The central control unit is also connected to other control units via an Ethernet switch with multiple Gbit Ethernet channels.

There are already initial hardware solutions available for a high-performance central control unit of this nature, such as Renesas’ R-Car H3, Intel’s Denverton, and Nvidia’s Parker (T186), which integrate a combination of powerful performance processors with a safety controller.

A central control unit of this kind forms the basis for a software architecture that fulfills five key requirements:
- integration of vehicle functions on one control unit
- execution of safety-relevant functions
- secure startup of the overall system
- optimized communication
- updating and addition of vehicle functions
Integration of vehicle functions on one control unit

Functions which previously ran on various (individual) control units can now be bundled on one central unit. The hardware resources of the performance cores are separated by a hypervisor. The hypervisor virtualizes the hardware and, in so doing, provides the partitions as virtual machines. In this way, the integrator creates various Adaptive AUTOSAR partitions as well as a Classic AUTOSAR partition. The latter uses an operating system and basic software which are based on Classic AUTOSAR. Vehicle functions which exist as software components (SWCs) can be integrated just like in a Classic AUTOSAR control unit. The Adaptive AUTOSAR partitions use a POSIX-compatible operating system and Adaptive AUTOSAR basic software. This structure allows vehicle functions based on Classic AUTOSAR as well as those based on Adaptive AUTOSAR to be integrated on a control unit.

In contrast to the performance cores, the hardware of the safety core is designed for a higher safety level (Automotive Safety Integrity Level, ASIL) in accordance to ISO 26262 and offers special mechanisms for detecting errors. Established safety concepts of existing Classic AUTOSAR control units are applied.

Controllers designed to ASIL D combined with a safety-certified operating system and other certified basic software components for run-time monitoring and securing communication enable the integration of functions with the highest safety requirements according to ASIL D. As a result of an overarching concept for monitoring the performance cores, these powerful cores can also satisfy the required safety requirements despite not being designed with safety in mind.

Figure 2. Architecture of a central control unit with performance and safety cores.
Secure system startup

An overarching boot concept allows the central control unit to be started up securely (see Figure 2: Secure Boot) within a defined time frame. The sequence and interaction of the units in the boot process are particularly important for fulfilling the time requirements in terms of the availability of the systems and for enabling the security specifications to be configured as quickly as possible. For this purpose, the roles of individual cores are defined such that the slaves and their assigned components are started from a master.

The safety core is started first for logical reasons, namely its monitoring function and shorter start time. The need to provide multiple Ethernet ports requires the use of a high-performance Ethernet switch. This is connected via the safety controller in order to enable quick availability of Ethernet communication. Then the performance cores are started, beginning with the security partition which serves as the anchor point for protecting all the lower-level and higher-level applications.

Optimized communication

To improve communication between the vehicle functions, both Classic AUTOSAR and Adaptive AUTOSAR use the service-based communication concept SOME/IP. To ensure regulated access by the various partitions to the Ethernet hardware switch within the central control unit, a special virtual Ethernet switch driver is required. Not only does this regulate communication with other control units, it also simultaneously regulates efficient internal communication between the partitions (Figure 3).

One of the main features of Adaptive AUTOSAR is the ability to update individual functions on the control unit retroactively and during run-time. In contrast to Classic AUTOSAR, this can be done without replacing and restarting the entire software of the control unit. However, it does need to be done in a controlled manner to prevent any faulty or even detrimental updates. Therefore, cryptographic processes which run on the security partition are used for all Adaptive AUTOSAR applications. They review the signature of the functions to be loaded and only allow them to be updated once they have been authenticated successfully.

Figure 3. A virtual Ethernet switch driver regulates communication with other control units and between the partitions.
More flexible software development with embedded Linux?

In Classic AUTOSAR the operating system was also specified, whereas the use of existing POSIX operating systems is a fundamental component of Adaptive AUTOSAR. This forms the basis for flexible software development. The standardized programming interface enables developers to create applications independently of one another and to distribute them freely to the control units in the vehicle. The prerequisite here is that the operating system provides the applications with interfaces in accordance with the POSIX profile PSE51 of IEEE 1003.13. Alongside proprietary operating systems, such as Wind River’s VxWorks, Green Hills’ Integrity, and QNX, the free software operating system Linux is a promising alternative. But is it suitable for use in Adaptive AUTOSAR systems?

Unlike commercial POSIX operating systems, when tend to be supplied precompiled as binary code, Linux is available as source code during development and for integration. This enables a more transparent development process, partly through improved debugging for the customer. The Linux kernel is also open to expansion, which means that customers have the opportunity, for example, to add their own kernel modules. In addition, Linux offers great functionality far in excess of the required POSIX standard. Linux is also already in use in a variety of industries and is optimized using feedback from billions of installations and users. The automotive sector, too, already uses Linux, with the focus to date on infotainment and human machine interfaces. The kernel itself is constantly optimized and enhanced comprehensively by the Linux community. Linux is available under a free software license (GPLv2), so there are no license fees. Costs are incurred by the customer through services such as configuration, customization, and provision as well as qualification and maintenance of customized deliveries.

Nevertheless, using Linux with Adaptive AUTOSAR does present a number of automotive-specific challenges, as encountered by Elektrobit in its pilot project (Figure 4).

Figure 4. For the use of Linux with Adaptive AUTOSAR a number of automotive-specific requirements must be met.
Software updates and security

A control unit with a connection to the internet is exposed to persistent attacks. These may come from outside, but they can also be triggered by harmful applications on the control unit itself. Alongside the cryptographic processes described above, special extensions, such as seccomp-bpf, are added to the kernel to restrict the system calls of applications.

In addition to development releases, each year a special version of the Linux kernel is introduced with two years of long-term support. For a vehicle with a typical four year development cycle, the system must be specifically designed by the manufacturer and supplier so that the kernel can be replaced during development and in later operation while the system retains binary compatibility with existing applications. The use of Linux containers ensures consistency at levels such as the memory and CPU, and for shared resources. It also enables the separate replacement of individual containers. This solution has proven its worth in other industries and is being used by Elektrobit for the first time in this automotive industry project.

Many sensitive functions and applications in the vehicle, such as the speedometer and reversing camera, need to be available or executed within a time span of well under two seconds. This is achieved through configuration and optimization of the Linux kernel, removal of unnecessary services, and organization of the startup process based on urgency or demand for availability.

The ability to test and secure such complex systems is a prerequisite for the use of Linux in the automotive industry. The options include freely available and commercial test environments or subcontracting to specialized companies. Organizations such as the Open Source Automation Development Lab (OSADL) offer support services.

Getting Adaptive AUTOSAR ready for series production

With its four main versions, Classic AUTOSAR has matured over ten years – the goal is to develop Adaptive AUTOSAR into a mature standard much more quickly. To this end, every delivery of the specification comes with a reference implementation, which is used as a proof of concept (POC). In addition, the use of existing and sometimes free implementations, such as Linux, saves time and effort.

The challenge now is to transform the implementation parts of Adaptive AUTOSAR into software suitable for series production. The quality of the implementation parts will be checked using established methods from Classic AUTOSAR. These requirements include defining quality features for code and test coverage, which must be used to check the implementation parts according to the release process. Based on these results, the decision will be made to either adopt and extend or to use Adaptive AUTOSAR implementation parts.

The Adaptive AUTOSAR standard is still being developed. For use in a series project it is vital the necessary functional components are provided on time - any delays or the absence of these elements in the planned AUTOSAR releases will impact project progress. Any further requirements or requirements that have yet to be fully defined must be provided to the projects and fed back into the standard.

It is crucial that the new developments needed for Adaptive AUTOSAR, and their possible uses, are evaluated with the customer quickly in order to continue to drive forward the development of the standard. There is obvious potential for a clever combination of Classic and Adaptive AUTOSAR on the central control unit, which uses Elektrobit software. At the same time, many established solutions from Classic AUTOSAR will be used, such as the certified safety operating system. This will significantly speed up the introduction of Adaptive AUTOSAR for high-performance computers for future generations of vehicles.
Adaptive AUTOSAR for high-performance in-car computers

Authors

Dr. Roman Pallierer
studied Computer Engineering at the Vienna University of Technology (TU Wien) and wrote his doctoral thesis on the validation of embedded communications protocols. Starting in 2002, he was responsible for tool development for FlexRay projects at Elektrobit. Since 2007, he has been working as Product and Solution Manager for the AUTOSAR basic software.

Börge Schmelz
studied electrical engineering at the Technical University of Cologne (TH Köln). Since 2005, he has been involved in the development of AUTOSAR control units at Elektrobit. In 2010, he took over the management of global service projects with a view to successfully realizing series production ramp-ups globally with the use of EB products. In 2017, he switched to product management for high-performance computers and Adaptive AUTOSAR.
Adaptive AUTOSAR for high-performance in-car computers
Adaptive AUTOSAR for high-performance in-car computers

About EB Automotive

Elektrobit (EB) is an award-winning and visionary global supplier of embedded software solutions and services for the automotive industry. A leader in automotive software with over 25 years serving the industry, EB’s software powers over 70 million vehicles and offers flexible, innovative solutions for connected car infrastructure, human machine interface (HMI) technologies, navigation, driver assistance, electronic control units (ECUs), and software engineering services. EB is a wholly owned, independent subsidiary of Continental AG.