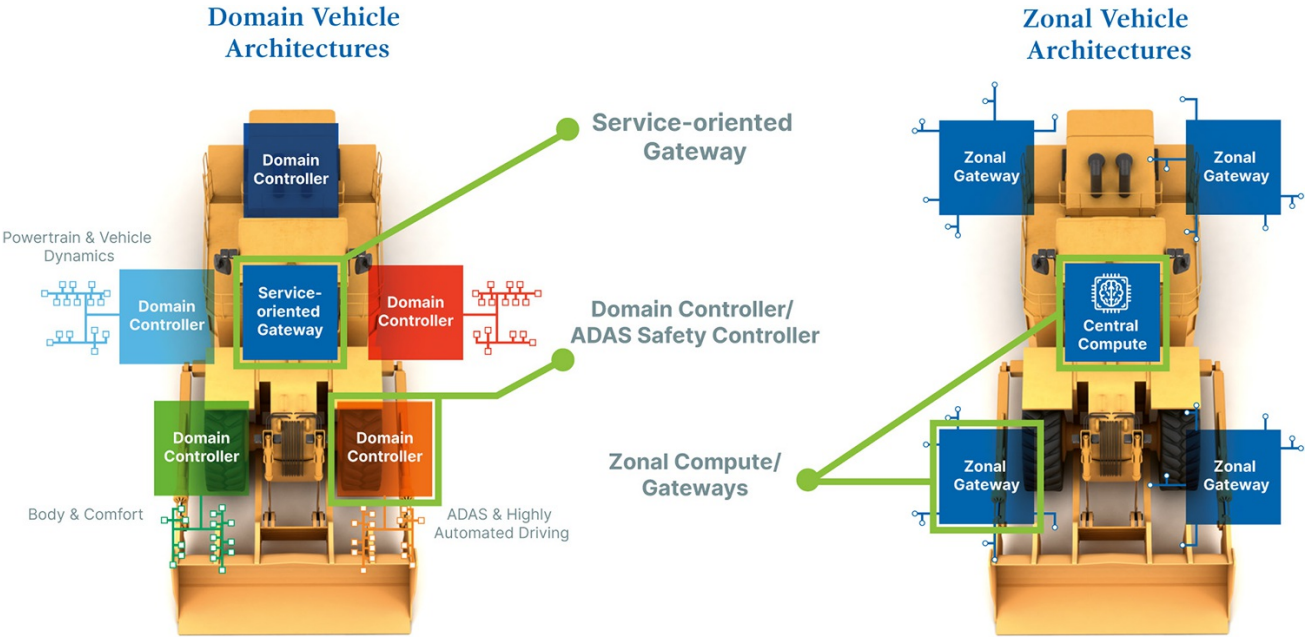
CAN Newsletter Online

CAN NEWSLETTER MAGAZINE

Vehicle network processing platform with functional safety

The NXP S32G274A vehicle network processor supports hardware security and functional safety according to ISO 26262. Microsys has integrated it in a system-on-module (SOM) with typical applications in connected vehicles, mobile machines, and automotive test equipment.



NXP S32G2 automotive processors power service-oriented gateways, domain controllers and ADAS safety controllers, or serve as zonal computers or gateways (Source: Microsys)

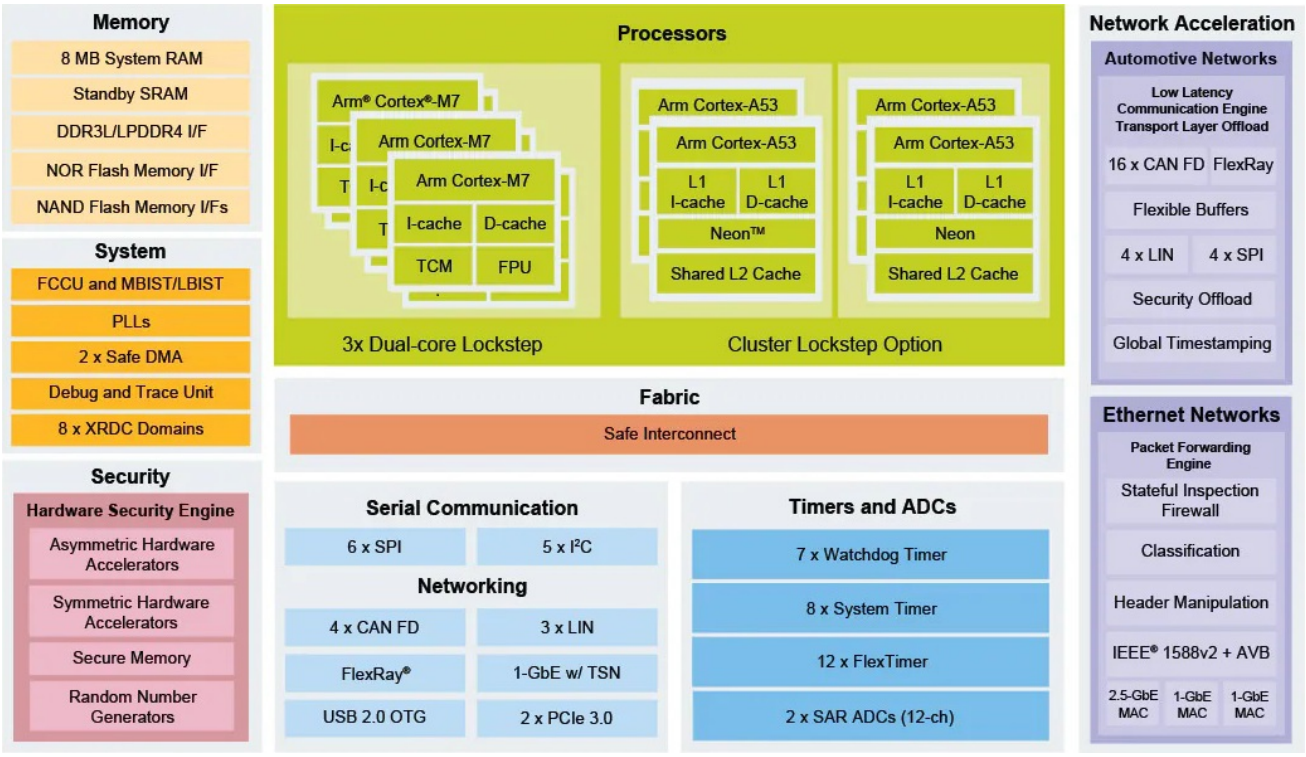
The complete article is published in the September issue of the CAN Newsletter magazine 2022. This is just an excerpt.

In today's age of digitalization, Industry 4.0, and the Internet of Things (IoT), high-throughput connectivity is one of the most critical functions for the interconnected devices. This particularly applies to the smart mobility sector, where the number of vehicles that is connected 24/7 via 5G to the service-oriented gateways, is growing. This continuous connectivity makes it possible to exploit the full potential of the vehicle data and to deploy new services and functional enhancements quickly and efficiently. Other domain controllers support functions such as infotainment and in-vehicle experience, body and comfort, powertrain and vehicle dynamics, as well as safety and security for ADAS (advanced driver assistance systems). Increasingly, autonomous driving functions are also required. The data transfer between the individual domain controllers or zonal computers/gateways and the local sensors and actuators must be processed and orchestrated with as little latency as possible.

Increasing data throughput

Such gateways are expected to deliver increasing processing performance and data throughput to satisfy recent requirements such as cloud connectivity for fleet management or vehicle subscriptions, V2X (vehicle-to-everything) communication, ADAS functions, and autonomous driving. The zero-downtime OTA (over-the-air updates) capability has to be considered as well. In addition, they must be real-time capable and secured in terms of ASIL D (automotive safety integrity level) safety and hardware security. This applies not only to major vehicle and mobility brands, but also to any latest commercial, construction or agricultural vehicle, overland and subway trains, and other types of mobile vehicles such as autonomous warehouse robots, and drones.

Compared to NXP's previous automotive gateway platforms, the S32G274A delivers 15900 Dhrystone Mips (million instructions per second), which translates into more than ten times faster real-time and network performance. To achieve this performance leap, the S32G2 processors integrate micro-controllers, application processors, network accelerators and a dedicated hardware security engine (HSE) on a single chip. This gives developers access to enough high-bandwidth processing power and high-performance connectivity to run tactile Internet applications with real-time 5G communication. The performance boost is possible by integration of several previously separate functions in a single-chip design, thereby combining more overall performance on one die. This also allows direct communication via the integrated safe fabric offers and lowers latencies. The integrated lockstep functionality for detecting errors during execution and data transmission, along with monitoring of other hardware-related faults, is yet another feature for safety applications.



NXP S32G2 processor block diagram (Source: NXP)

On-chip interfaces and processing cores

Connected vehicles and mobile machines also require native support of all relevant peripheral interfaces, such as CAN (FD), Flexray, and LIN. Alternative connected vehicle designs using generic extension components to connect CAN controllers generate high interrupt loads that slow the main processor down unnecessarily. FPGAs (field-programmable gate arrays) are not a cost-effective alternative either and require additional development resources for FPGA programming. Providing on-chip automotive interfaces (up to 20 CAN FD, 2 Flexray, and 7 LIN) ensures that the most complex sub-systems are addressed without the latencies caused by the otherwise required USB-to-network components. This also avoids the need for expensive FPGA designs. The low-latency communication engine (LLCE) for CAN (and others), and the packet forwarding engine (PFE) for processing IP packets from Ethernet networks, reduce the CPU (central processing unit) workload. A fire-walled hard-ware security engine (HSE) for secure boot, security services, key management, and encrypted data transfer provides a root of trust, which is essential for secure IoT edge systems.

The processor orchestrates four 1-GHz Arm Cortex-A53 cores organized in two clusters for applications and services. They provide up to 23 Dhrystone Mips percore for multi-purpose applications. In addition, there are also three integrated Arm Cortex-M7 dual-core lockstep processors. Applications requiring dedicated co-processors, e.g. for motion control applications, can take advantage of the three dual-cores. They support real-time operating systems such as Autosar or FreeRTOS.

Integrated functional safety and safe communication

For safety-critical applications, the Arm Cortex-M7 and A53 cores can be operated in lock-step mode. Where required, the M7 cores can work in a 2oo3 (two-out-of-three) voting mode to ensure that when the three core pairs provide different results, the same result provided by two core pairs is valid. This way, the heterogeneous computing cores can support ASIL D applications as well as any other functional safety standard according to IEC 61508.

The integrated HSE provides comprehensive security functions for data and application security. These include data encryption and decryption as well as the generation and verification of MACs (media access control), and signatures. Secure boot provides a memory check at system startup. In addition, the engine provides real-time, hardware-accelerated SSL/TLS (secure socket layer, transport layer security) network communication and supports IPsec. It also provides random number generation capabilities and secure key management capabilities, along with resistance against side-channel attacks.

System-on-module

Developers of applications for commercial vehicles, mobile machines and e-mobility solutions that are only manufactured in industrial batch sizes, cannot afford to develop and integrate such complex gateway processor technology, along with all the required additional components and complex BSP (board support packages), into their systems from scratch. Instead, they have to concentrate on their core competencies, which are primarily in application development and which differentiate them from the competition. This is where application-ready COTS (commercial off-the-shelf) platforms help as they enable the development of customized solutions without the need to spend a lot of time on the design of the central computing core.

But if you would like to read the full article, you can download it free of charge or you download the entire magazine.