CAN Newsletter Online

INTERNET OF THINGS

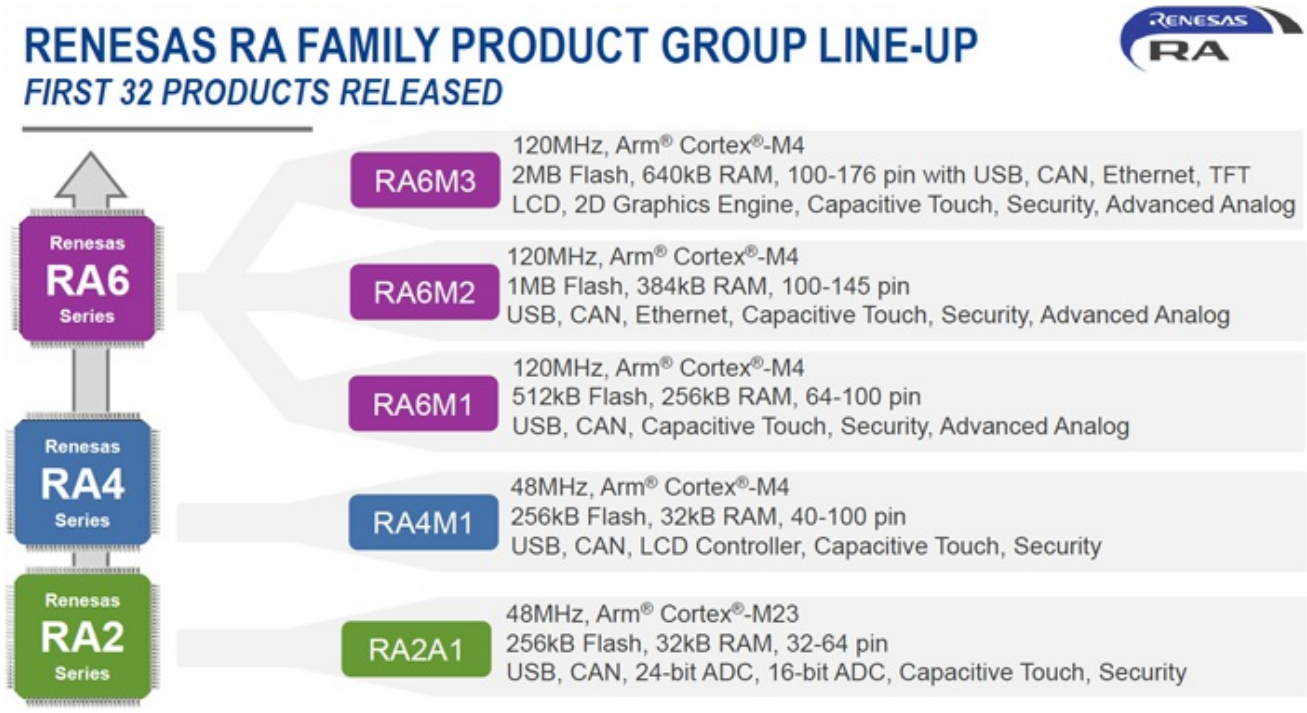
MCUs with advanced security

Renesas Electronics has unveiled the Renesas Advanced (RA) series of 32-bit Arm Cortex-M micro-controllers (MCUs). They feature CAN connectivity.

Latest 32-bit Arm Cortex-M MCU with advanced security (Source: Renesas)

They combine performance, security, connectivity, peripheral IP, and Flexible Software Package (FSP) to address embedded solutions. To support the latest series, the company has built a partner ecosystem to deliver an array of software and hardware building blocks that will work out of the box with RA MCUs.

The ecosystem will help accelerate the development of IoT (Internet of Things) applications with core technologies such as security, safety, connectivity, and HMI. Designing with RA MCUs enables engineers to develop IoT endpoint and edge devices for industrial and building automation, metering, healthcare, and home appliance applications. The product is PSA Certified Level 1 and includes the RA2 series (up to 60 MHz), RA4 series (up to 100 MHz), RA6 series (up to 200 MHz), and the dual-core RA8 series, to be released later.



RA family series line-up (Source: Renesas)

“RA MCUs offer customers the ultimate IoT security by combining our Secure Crypto Engine IP with Nist Cavp certifications on top of Arm Trustzone for Armv8-M, while also providing tamper detection and reinforcing resistance to side-channel attacks,” said Roger Wendelken, Senior Vice President of Renesas’ IoT and Infrastructure Business Unit. “Scalability and compatibility across the RA Family lets customers build a range of products, and they can quickly begin development with our flexible software package using Amazon FreeRTOS, ThreadX, or other RTOS and middleware solutions.”

“With today’s fast pace of innovation, developers need to accelerate their time-to-market without compromising on crucial features such as security and connectivity,” said Dipti Vachani, senior vice president and general manager, Automotive and IoT Line of Business, Arm. “The new RA family of MCUs is PSA Certified, demonstrating that it is built on sound security principles, enabling developers to improve security and safety in high-performing endpoint devices.”

The first five RA MCU groups available today are comprised of 32 scalable MCUs with Arm Cortex-M4 and Cortex-M23 processor cores. They feature pin counts of 32-pins to 176-pins, along with 256 KiB to 2 MiB of code flash memory, 32 KiB to 640 KiB SRAM, and connectivity such as CAN, CAN, and Ethernet. Transition is enabled within the RA Family thanks to feature and pin compatibility. Each RA MCU provides active and standby power, and features such as Renesas’ human machine interface capacitive touch technology.

The RA family FSP provides an open architecture that allows customers to re-use their legacy code and combine it with software examples from Renesas and ecosystem partners to speed implementation of complex functions like connectivity and security. The FSP features Amazon FreeRTOS and will also add out-of-box support for ThreadX RTOS and middleware on Cortex-M23 and Cortex-M33 MCUs by early 2020. This offers a device-to-cloud option for developers. These out-of-box options can be replaced and expanded with any other RTOS or middleware.

The RA family roadmap will roll out additional MCUs in 2020 with more advanced technologies. The roadmap offers PSA Certified and Trusted Firmware-M (TF-M) API compliant devices, including Cortex-M33 MCUs, low-power Cortex-M23 MCUs, and BLE / IEEE 802.15.4 wireless IoT products. MCUs with TF-M / PSA certification enable customers to deploy secure IoT endpoint and edge devices, and smart factory equipment for Industry 4.0.

The first wave of RA devices incorporates hardware-based security features from simple AES acceleration to fully-integrated crypto subsystems isolated within the MCU. The secure crypto engine provides symmetric and asymmetric encryption and decryption, hash functions, true random number generation, and advanced key handling, including key generation and MCU-unique key wrapping. An access management circuit shuts down the crypto engine if the correct access protocol is not followed, and dedicated RAM ensures that plaintext keys are never exposed to any CPU or peripheral bus. The RA family development environment offers on-chip debug, IDEs, compiler, support tools, board evaluation kits, design files, schematics, PCB layouts, and BOM.

cw