CAN Newsletter Online

ISO 26262 AND ISO/SAE 21434

CAN FD MCU with selectable pin locations to switch

The PIC32CM JH 32-bit micro-controller unit (MCU) from Microchip features 512 KiB Flash, 5-V, as well as dual CAN FD. It is based on an Arm Cortex-M0+ core. Furthermore, it meets ISO 26262 functional safety and ISO/SAE 21434 cybersecurity standards.

The MCU is based on the Arm Cortex-M0+ architecture and provides Autosar support, Memory-Built-In Self-Test (MBIST), and secure boot, explained the company (Source: Microchip)

Manufacturers of electronic systems ranging from vehicles to home appliances are moving towards automating and connecting end applications. This spurs the need for industry standards related to functional safety and cybersecurity protection to ensure their products operate safely and securely, explained the company in its press release. The PIC32CM JH is equipped with components that meet ISO 26262 functional safety and ISO/SAE 21434 cybersecurity engineering standards. The MCU supports up to two CAN (FD) interfaces as well as two selectable pin locations to switch between two external CAN transceivers without the need for an external switch. LIN is also an interface option.

The product is compatible with Autosar, an open software architecture, providing suppliers with the ability to change to lower-level hardware but keep the original application code. When using Autosar, Microchip offers ASIL B micro-controller abstraction layers (MCALs) for functional safety applications — providing the lower-level hardware interface to the MCU.

Automotive industry OEMs (original equipment manufacturers) require both functional safety and cybersecurity protection for many in-vehicle applications including touch buttons and touch wheels, door controls and console controls, and body applications such as advanced driver assistance systems (ADAS), said the company. The PIC32CM JH, when paired with one of Microchip's Trust Anchor TA100 Cryptoautomotive security ICs, is compliant to ISO/SAE 21434, the cybersecurity standard for automotive, the company continued. According to Microchip, the TA100 employs ultra-secure hardware-based cryptographic key storage and cryptographic countermeasures to eliminate potential backdoors linked to software weaknesses.

"With the PIC32CM JH MCU, Microchip is addressing the growing need for micro-controller solutions that are designed with functional safety and cybersecurity protection, which is particularly important in the automotive industry," said Rod Drake vice president of Microchip Technology's 32-bit MCU business unit. "OEMs and other manufacturers now have the option to use an entry-level Arm Cortex-M0+ based MCU to meet compliance requirements previously only available on higher-end MCUs."

The secure boot is part of the hardware. It authenticates the code to make sure it is valid and prevents malicious code from being loaded onto the MCU. Other hardware features included on the MCU are Error Correction Code (ECC) with fault injection, loopbacks on the communications interfaces, system memory protection unit and MBIST, all of which are safety mechanisms used to meet ISO 26262 and IEC 60730 standards, the company further explained.

MBIST is a method of testing embedded memories and can test the integrity of the static random-access memory (SRAM) to ensure it is functioning properly before the code is run to mitigate failures. To support developers with implementation, the PIC32CM JH comes with functional safety collateral such as a safety manual, failure modes effects and diagnostic analysis (FMEDA), and diagnostic code targeting ISO 26262 ASIL B (automotive safety integrity level) safety levels.

Additionally, the product includes advanced touch with driven shield plus, providing noise and water tolerant operability. This feature is necessary for home appliances, industrial and automotive applications where the touch must work in a variety of harsh environments.

cw

© CAN Newsletter Online - 2022-09-29 - www.can-newsletter.org