Product Overview

MSP Arm® Cortex®-M33 MCUs Enable Enhanced Performance and System Security

Address evolving security and system demands with MSPM33

Across industrial, automotive and enterprise markets there is increased demand to protect systems from potential threats and cyberattacks. These evolving security requirements along with the ever consistent need to optimize boards for cost, efficiency and time to market have lead engineers to look for not just one microcontroller (MCU) to meet the multifaceted needs of a single design, but a broad portfolio of MCUs that can fulfill the requirements of multiple platforms and system variations.

To address these challenges Texas Instruments has added MSPM33C321A into the scalable MSP portfolio of Arm® Cortex®-M MCUs. This 160MHz Arm Cortex-M33 MCU delivers fast processing, high-speed analog performance and enhanced security features while maintaining hardware and software compatibility with the MSPM0 portfolio of Arm Cortex-M0+ MCUs. MSPM33C321A enables engineers to maximize design investments, address system level security concerns and integrate more functionality into a single MCU.

Reduce system cost with MSPM33C321A

MSPM33C321A is a 160MHz MCU based on the Arm Cortex-M33 CPU with TrustZone®, memory protection unit (MPU), digital signal processing extension (DSP), and a floating-point unit (FPU) to enable developers to do more with a single chip. Including up to 1MB of dual-bank flash, 256kB of SRAM and error correction code (ECC) for both, this device is equipped to support in-field updates and maintain long-term operation. MSPM33C321A is also equipped with 32kB of high endurance data flash that can be used to support EEPROM operations from the MCU.

Engineers can optimize their board and remove external components by taking advantage of the integrated advanced analog. With two simultaneous sampling 12-bit, 9.4Msps ADCs and two high-speed, low-power comparators with 8-bit reference DACs, MSPM33C321A supports high-speed signal conversion, increased oversampling and higher number of effective bits (ENOB) for signal processing. This MCU also offers up to 30 PWM channels and includes two advanced control timers to support up to four DC motors or two BLDC motors.

MSPM33C321A offers a robust set of communication protocols for interfacing with external components, including two CAN-FD channels, four serial audio interface channels supporting I2S, and one QSPI channel operating at up to 20MBps for high throughput data storage and display functions. Additional design flexibility is provided through the device's configurable serial interfaces where channels can be dynamically assigned in software as either UART, I2C or optionally SPI. With a range of VQFN, LQFP, and BGA packages and pin count options from 48 to 100-pins, engineers can select the right combination for their design and implement the configurable serial interface to help optimize their GPIO usage.

The combination of performance, memory, and rich feature integration on MSPM33C321A enables developers to get more out of their MCU.

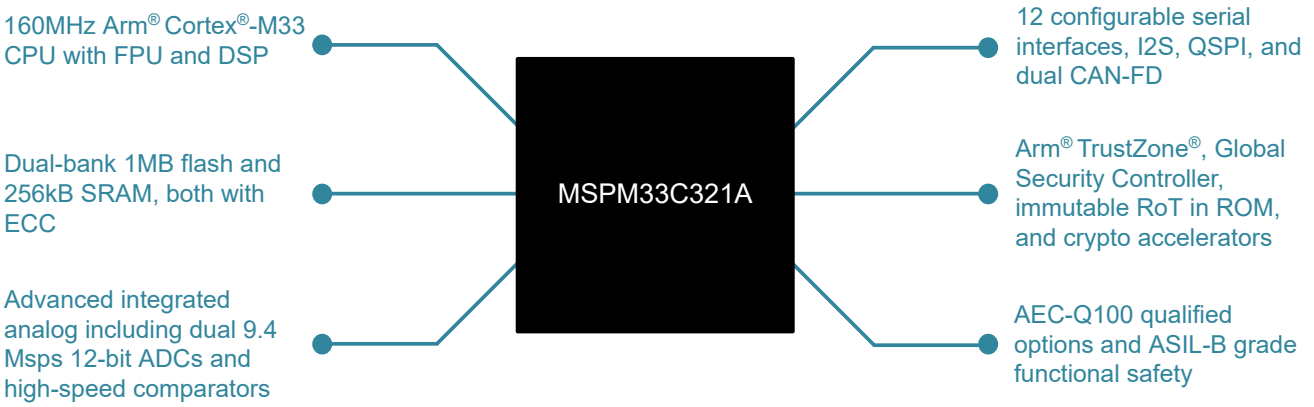

Figure 1. MSPM33C321A feature overview

Design with security in mind

The more critical the MCU role within a system, the higher the value of the application firmware and consequently, the stronger the need to shield against external threats. MSPM33C321A provides an expansive set of hardware and software features that can be used to build secure applications for industrial, data centers, and automotive applications.

The foundation for enhanced system level security starts with Arm TrustZone technology. The TrustZone architecture is enabled through the Arm Cortex-M33. TrustZone allows the programmer to partition peripherals and sections of memory as secure and non-secure, allowing the programmer to restrict sections of memory from unauthorized users. MSPM33C321A also includes a Global Security Controller (GSC), a unique peripheral to MSP that adds an extra layer of security on top of the TrustZone architecture. The GSC configures both secure and privilege attributes for peripherals, flash, and SRAM. This allows the programmer to use one IP to protect all their resources against non-secure peripherals accessing secure regions of memory.

The next layer of enhanced security is provided through the Immutable Root of Trust (i-RoT) in ROM, which supports secure boot and key provisioning. The i-ROT provides an irrefutable mode to verify the authenticity of the device and ultimately protects the application firmware from being tampered with at production and beyond. This hardware implementation of i-ROT is in line with requirements for Security Evaluation Standard for IOT Platforms (SESIP) Level 2 and Platform Security Architecture (PSA) Level 2.

MSPM33C321A also includes cryptographic hardware accelerators such as Advanced Encryption Standard with 256-bit key length (AES-256), Secure Hash Algorithm 256-bit (SHA-256), and a Public Key Accelerator (PKA) module to offload computation of intensive public cryptographic operations such as elliptic curves (ECC) and RSA asymmetric cryptography. These features address many classical security concerns, but developers are also looking to implement post-quantum cryptography (PQC) algorithms to protect their designs against the potential of new threats. With MSPM33 software development kit (SDK), engineers are able to implement software support for target post-quantum algorithms consistent with the Commercial National Security Algorithm Suite (CNSA) 2.0 restrictions including Module-Lattice-Based Digital Signature Algorithm (ML-DSA-87), SHA-384, and SHA-512. The combination of hardware and software-based protections available with MSPM33C321A provides engineers with the tools they need to protect their applications from various threats.

Streamline development with MSP Development Ecosystem

The rich features on the MSPM33C321A make the device a great fit for a wide variety of use cases. TI provides users with comprehensive software and tools ecosystem to bring those applications to life. With options for multiple development environments such as Code Composer Studio (CCS) and IAR, as well as support for bare metal, FreeRTOS, and Zephyr, engineers can choose to design their application firmware using their preferred tools and environment. Quickly evaluate with our MSPM33C321A LaunchPad development kit evaluation module and accelerate development with the 100+ code examples and the SysConfig graphical

system configuration tool. From initial design evaluation to production level resources – the MSP ecosystem is equipped to support engineers at every step of the way.

An MSP MCU for every design

As a part of the scalable portfolio of MSP Arm Cortex-M MCUs, MSPM33C321A is hardware and software compatible with the MSPM0 devices. With common pin-to-pin compatible packages and software development environments across MSPM0 and MSPM33, users can maximize design investments and easily move up and down in performance and feature integration across the entire MSP portfolio. Designing with MSPM33C321A provides engineers with not just one great MCU choice, but hundreds of options to be implemented across many designs.

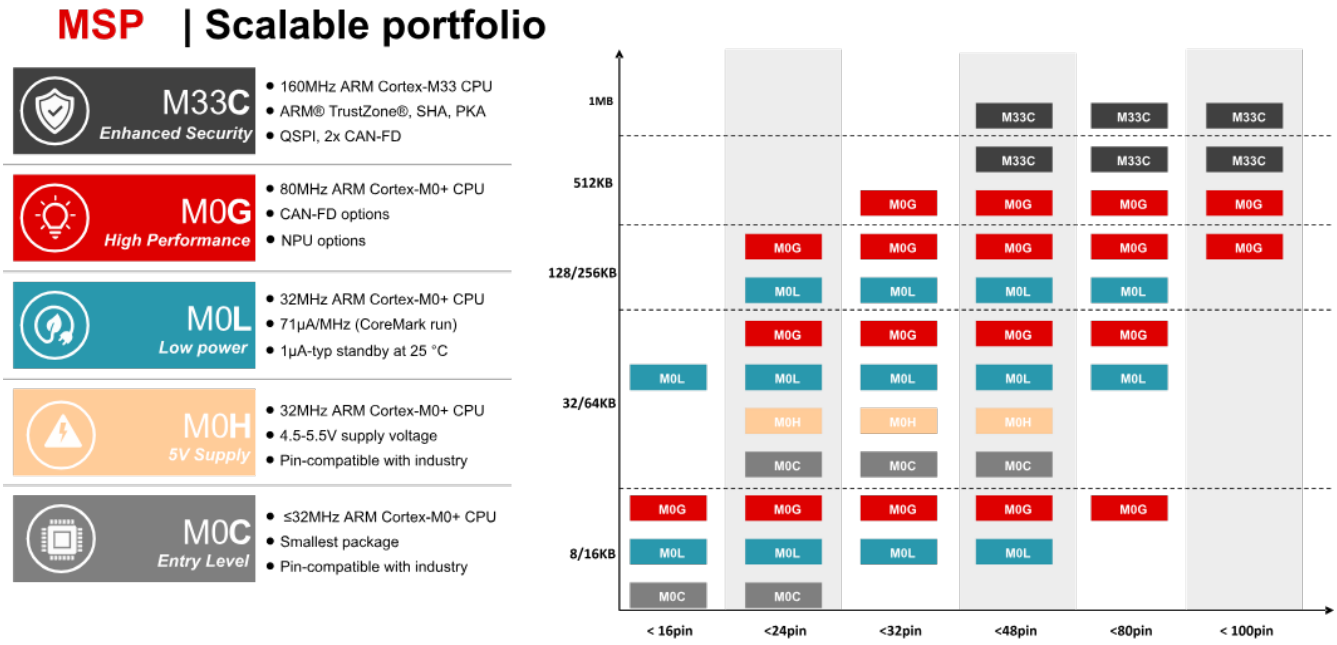

Figure 2. TI's scalable portfolio of MSP Arm® Cortex®-M MCUs

Conclusion

MSPM33C321A enables you to enhance your system security and MCU performance without compromising on cost or portfolio scalability.

Resources

To start evaluating MSPM33, order an MSPM33C321A LaunchPad development kit! Jump start your design with MSPM33 code examples and additional resources available at these links:

- MSPM33C321A Product Page
- LP-MSPM33C321A
- MSPM33 Software Development Kit
- MSPM33C Security User's Guide
- Migration Guide between MSPM0Gx5x9 and MSPM33C32xx
- LVGL Use on MSPM33C
- Advance Your Automotive Design with the MSPM33C321A-Q1 Device Technical White Paper
- General Purpose MCUs Portfolio Page

IMPORTANT NOTICE AND DISCLAIMER

TI PROVIDES TECHNICAL AND RELIABILITY DATA (INCLUDING DATASHEETS), DESIGN RESOURCES (INCLUDING REFERENCE DESIGNS), APPLICATION OR OTHER DESIGN ADVICE, WEB TOOLS, SAFETY INFORMATION, AND OTHER RESOURCES “AS IS” AND WITH ALL FAULTS, AND DISCLAIMS ALL WARRANTIES, EXPRESS AND IMPLIED, INCLUDING WITHOUT LIMITATION ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT OF THIRD PARTY INTELLECTUAL PROPERTY RIGHTS.

These resources are intended for skilled developers designing with TI products. You are solely responsible for (1) selecting the appropriate TI products for your application, (2) designing, validating and testing your application, and (3) ensuring your application meets applicable standards, and any other safety, security, regulatory or other requirements.

These resources are subject to change without notice. TI grants you permission to use these resources only for development of an application that uses the TI products described in the resource. Other reproduction and display of these resources is prohibited. No license is granted to any other TI intellectual property right or to any third party intellectual property right. TI disclaims responsibility for, and you fully indemnify TI and its representatives against any claims, damages, costs, losses, and liabilities arising out of your use of these resources.

TI’s products are provided subject to TI’s Terms of Sale, TI’s General Quality Guidelines, or other applicable terms available either on ti.com or provided in conjunction with such TI products. TI’s provision of these resources does not expand or otherwise alter TI’s applicable warranties or warranty disclaimers for TI products. Unless TI explicitly designates a product as custom or customer-specified, TI products are standard, catalog, general purpose devices.

TI objects to and rejects any additional or different terms you may propose.

Last updated 10/2025