Application Brief

Understanding Security Features for C2000 Real-Time Control MCUs

Device and Family Description

The TI C2000™ F28x family of microcontrollers is designed for real-time control applications in both industrial and automotive spaces. All F28x microcontrollers feature 32-bit C28x CPUs, with speeds from 40MHz to 200MHz, often paired with accelerator cores such as the Control Law Accelerator (CLA). With tightly coupled analog peripherals such as analog-to-digital converters (ADCs), comparators, and sophisticated digital actuation peripherals, such as high resolution PWM modules, there are many compelling reasons to use C2000 microcontrollers in embedded real-time control applications.

TI Embedded Security Portfolio

Table 1. Common Security Enablers

C2000™ MCU Series	Security Enablers	Detailed Security Features
F28P55x^{+} F28P65x^{+} F280015x^{+} F280013x^{+} F28003x^{+} F28002x^{+} F2838x^{+} F28004x^{+} F2837xD^{+} F2837xS^{+} F2807x^{+} F2806x F2805x F2803x F2802x F2833x, F2823x F28M3x	Device identification	Unique Identification (UID) Number: Ability for user to enable mechanisms for device identification in communications, seed for data integrity algorithms, initialization vector for authentication and encryption or decryption, or to protect against code cloning.
	Software IP protection	Code Security Module (CSM): Ability for user to block unauthorized access or programming of firmware stored in on-chip memories. Devices marked with ($^{+}$) feature a Dual Code Security Module (DCSM), with two independent security zones.
	Debug security	Emulation Code Security Logic (ECSL) using CSM: Ability for user to enable full debug access to memory using a password.

Table 2. Latest Security Enablers

C2000™ MCU Series	Security Enablers	Detailed Security Features
F28P55x F28P65x F280015x F280013x F28003x F2838x	Additional Debug Security	JTAGLOCK: Ability to block debugger access to the device; unlockable with password.
	Secure Boot	Option to enable AES-128 Cipher-based Message Authentication Code (CMAC) to pre-authenticate the first 16KB of flash prior to transferring code execution.
F28P55x F28P65x F28003x F2838x	Cryptographic Acceleration	Hardware Advanced Encryption Standard (AES 128-, 192-, 256 bit) engine to boost performance.
F28P55x	Flash write and erase protection	Option to permanently lock sections of Flash, making the contents immutable. This can be used to extend secure boot capabilities by implementing additional cryptographic functions in software for code and data authentication.

Security Problem Targeted: Typical Threats, Security Measures

In the design of real-time control systems, a good portion of the research and development investment goes into embedded firmware development. As such, intellectual property housed in the firmware of a product can provide key competitive advantages for users, and can be vulnerable to theft. Performing a visual component tear-down of a system is relatively easy for the purpose of replicating the end product, but effective protection of the firmware running on the MCU prevents full duplication of the working system.

Another scenario that is increasingly common is co-development of the firmware. In these cases, certain portions of system firmware are developed outside the core engineering team, and perhaps by a third party vendor. In these situations, one party can opt to keep the firmware private, while still allowing the second party to develop and test a portion of the application on the same system. Such scenarios are typically not covered by traditional runtime software protections, and require hardware protection mechanisms while the MCU is being accessed by a debugger.

This scenario is especially common in automotive applications, where there can be multiple companies involved in producing and debugging firmware in a highly connected system. These types of threats can be addressed by the security enablers available on C2000 devices.

Security Implementation

When a new device is shipped from TI, the device arrives in a completely unlocked state. After security protocols are enabled by the user, any locked memory zone is only accessible by code that also exists in the same zone. Dedicated unlocked memory is available so that data can be transferred between zones if needed. In addition to this fundamental building block, there are other options or layers that can be selectively enabled:

1. Selection of memory blocks to be protected:

   In many cases, not all the memory, either volatile or nonvolatile, needs to be locked. This case can be true for certain pieces of firmware shared across different sub-systems, or that contain non-proprietary IP.
2. Zone ownership (DCSM only):

   In addition to protecting various blocks of memory, there are two zones in each DCSM implementation. Once the memories are allocated for protection, the next step is deciding which of these zones has control over the selected memories. However, if there is no need for code protection between developers on the same device, a single-zone configuration can be used.
3. Execute-only protection (DCSM only):

   If a region is used only for execution, rather than internal data storage, the programmer can enable *execute-only protection* to block any read access (even from the same region or zone), for added security.
4. CPU protection (DCSM only):

   Debug access to the core processing unit (CPU) registers is also blocked if the DCSM detects code executing from any locked region.
5. Emulation Code Security Logic (ECSL):

   Even with the above measures, users can restrict an emulation connection if the MCU is executing from a locked region. This security feature can be temporarily disabled during a debug session using a password.
6. Unique Identification Number (UID):

   By using a UID number provided on each device, techniques can be implemented to further allow software to only run on known devices. For more information, see *C2000™ Unique Device Number* .
7. JTAGLOCK:

   The JTAG (emulator) interface can be disabled and protected with a user-chosen password. This helps make sure only authorized individuals can view and debug the application.
8. AES acceleration:

   The widely used AES symmetric cipher is known for speed and simplicity. Even given that, a software implementation of the AES algorithm in an embedded microcontroller is relatively slow to the demands of a real-time control system. The hardware AES accelerator vastly improves processing time for cryptographic messages, while freeing up the CPU bandwidth in the process. Several different operational modes and key sizes are available.
9. Secure Boot:

   To maintain the integrity of firmware stored in the device, secure boot can be enabled to verify code stored in Flash memory before transferring execution to the stored code. Along with the firmware programming protections built into the security logic, this helps make sure the code that runs on the device is authentic. The algorithm used is an AES-128 CMAC algorithm. Tools are available to embed the required MAC value into the final code image. For more information, see *Secure Boot on C2000 Device* .
10. Flash Write and Erase Protection:

    In certain cases, users can opt to extend secure boot functionality by implementing other cryptographic authentication algorithms, including elliptic curve-based functions such as ECDSA. In devices with Flash write and erase protection, these functions can be placed in Flash regions at the entry point of code, and made immutable (that is, permanently unchangeable and unmodifiable). This feature enables stronger cryptographic capabilities, and can also be used to enable secure firmware update functions.

Additional Resources

While security risks can take many forms across end applications, firmware intellectual property protection is a threat common to most systems. C2000 microcontrollers enable users to address these concerns through flexible features for multiuser development environments. For more information on C2000 microcontrollers, see TI.com/C2000. For specific information on the security features present in each C2000 device, see the product data sheet and technical reference manual available on the TI.COM™ product page.

Note

Security is hard. TI makes cybersecurity easier.

For more information about TI's Embedded Security Designs, visit TI.com/security.

Trademarks

C2000™ and TI.COM™ are trademarks of Texas Instruments.
All trademarks are the property of their respective owners.

IMPORTANT NOTICE AND DISCLAIMER

TI PROVIDES TECHNICAL AND RELIABILITY DATA (INCLUDING DATA SHEETS), 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 will 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 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.

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

Mailing Address: Texas Instruments, Post Office Box 655303, Dallas, Texas 75265