# Understanding security features for C2000™ Delfino™ and Piccolo™ Real-Time Control MCUs

Texas Instruments

### *Device/Family description*

The TI C2000™ microcontrollers (MCUs) are designed for real-time control applications in both industrial and automotive spaces.

The TI C2000 microcontrollers are built with real-time control in mind. All C2000 MCUs are based on the 32-bit C28x MCU core processor with speeds from 40 MHz to 200 MHz. With tightly coupled analog peripherals such as analog-to-digital converters (ADCs), comparators and fast-response digital stimuli like PWMs, there is a compelling reason to use the C2000 MCUs in a real-time control application.

## TI Embedded Security Portfolio –

***Security is hard, TI makes it easier***

### Security problem targeted: Typical threats / security measures

As in any microcontroller, a good portion of the R&D investment at the user level goes into the firmware development. As such, intellectual property (IP) housed in a product's firmware can provide key competitive advantages for a business in the marketplace and is at a high risk of theft. It is straightforward enough to do a visual component teardown of a system for purposes of copying an end product, but 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. Many times certain system firmware is outside the main engineering team, perhaps even outside the company. In these situations, one party sometimes wants to keep their firmware private, while still allowing the second to develop and test a portion of the program on the same system. Such scenarios are typically not covered by traditional run-time software protections and require protection while the MCU is in a debug state. This is especially common in automotive applications where there may be multiple companies involved in producing and debugging firmware in a highly connected system.

These types of threats can be addressed by security enablers on most C2000 devices.

### Security implementation

When a new device is shipped from TI, it arrives in a completely unlocked state. After security protocols are enabled by the user, a locked zone will only be accessible by code that also exists in the same zone. Dedicated, unlocked memory exists so that data can be transferred between zones if needed. In addition to this fundamental implementation, 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 non-volatile, will need to be locked. This is 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

**Security enablers:**

| C2000 MCU series | Security enablers | Detailed security features |
|---|---|---|
| TMS320F2837xD<br>TMS320F2837xS<br>TMS320F2833x/23x<br>TMS320F2807x<br>TMS320F28004x<br>TMS320F2806x<br>TMS320F2805x<br>TMS320F2803x<br>TMS320F2802x<br>F28M3x | Device identify | **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 |
| | Debug security | **Emulation Code Security Logic (ECSL) via CSM:** Ability for user to enable full debug access to memory via a password |

TI offers security enablers to help developers implement their security measures to protect their assets (data, code, identity and keys).

each DCSM implementation. Once the memories are allocated for protection, the next step is deciding which of these zones will have 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 will be 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/zone) for added security.
4. **CPU protection (DCSM and F2837x/07x 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 using the above measures, it may still be desirable to restrict an emulation connection if the MCU is executing from a locked region. This may be temporarily disabled during a debug session using a password.
6. **Unique Identification (UID):** By using a UID number provided on each device techniques can be implemented to further allow software to only run on known devices. **C2000 Unique Device Number**

## Additional resources

While security risks can take many forms across end applications, IP/firmware protection is a threat common to most systems. The C2000 MCU family can enable our customers to address these concerns through flexible features for multi-development environments.

For additional information on the C2000 MCU security techniques, please review the Technical Reference Manual (TRM) for the specific series of devices of interest. The TRM can be found beneath the datasheet and Errata in any C2000 MCU product folder.

- **TMS320F2837xD Product Folder**


***Security is hard, TI makes it easier***

For more information about TI's Embedded Security Solutions, visit **www.ti.com/security**



Texas Instruments

## IMPORTANT NOTICE FOR TI DESIGN INFORMATION AND RESOURCES

Texas Instruments Incorporated ('TI") technical, application or other design advice, services or information, including, but not limited to, reference designs and materials relating to evaluation modules, (collectively, "TI Resources") are intended to assist designers who are developing applications that incorporate TI products; by downloading, accessing or using any particular TI Resource in any way, you (individually or, if you are acting on behalf of a company, your company) agree to use it solely for this purpose and subject to the terms of this Notice.

TI's provision of TI Resources does not expand or otherwise alter TI's applicable published warranties or warranty disclaimers for TI products, and no additional obligations or liabilities arise from TI providing such TI Resources. TI reserves the right to make corrections, enhancements, improvements and other changes to its TI Resources.

You understand and agree that you remain responsible for using your independent analysis, evaluation and judgment in designing your applications and that you have full and exclusive responsibility to assure the safety of your applications and compliance of your applications (and of all TI products used in or for your applications) with all applicable regulations, laws and other applicable requirements. You represent that, with respect to your applications, you have all the necessary expertise to create and implement safeguards that (1) anticipate dangerous consequences of failures, (2) monitor failures and their consequences, and (3) lessen the likelihood of failures that might cause harm and take appropriate actions. You agree that prior to using or distributing any applications that include TI products, you will thoroughly test such applications and the functionality of such TI products as used in such applications. TI has not conducted any testing other than that specifically described in the published documentation for a particular TI Resource.

You are authorized to use, copy and modify any individual TI Resource only in connection with the development of applications that include the TI product(s) identified in such TI Resource. NO OTHER LICENSE, EXPRESS OR IMPLIED, BY ESTOPPEL OR OTHERWISE TO ANY OTHER TI INTELLECTUAL PROPERTY RIGHT, AND NO LICENSE TO ANY TECHNOLOGY OR INTELLECTUAL PROPERTY RIGHT OF TI OR ANY THIRD PARTY IS GRANTED HEREIN, including but not limited to any patent right, copyright, mask work right, or other intellectual property right relating to any combination, machine, or process in which TI products or services are used. Information regarding or referencing third-party products or services does not constitute a license to use such products or services, or a warranty or endorsement thereof. Use of TI Resources may require a license from a third party under the patents or other intellectual property of the third party, or a license from TI under the patents or other intellectual property of TI.

TI RESOURCES ARE PROVIDED "AS IS" AND WITH ALL FAULTS. TI DISCLAIMS ALL OTHER WARRANTIES OR REPRESENTATIONS, EXPRESS OR IMPLIED, REGARDING TI RESOURCES OR USE THEREOF, INCLUDING BUT NOT LIMITED TO ACCURACY OR COMPLETENESS, TITLE, ANY EPIDEMIC FAILURE WARRANTY AND ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT OF ANY THIRD PARTY INTELLECTUAL PROPERTY RIGHTS.

TI SHALL NOT BE LIABLE FOR AND SHALL NOT DEFEND OR INDEMNIFY YOU AGAINST ANY CLAIM, INCLUDING BUT NOT LIMITED TO ANY INFRINGEMENT CLAIM THAT RELATES TO OR IS BASED ON ANY COMBINATION OF PRODUCTS EVEN IF DESCRIBED IN TI RESOURCES OR OTHERWISE. IN NO EVENT SHALL TI BE LIABLE FOR ANY ACTUAL, DIRECT, SPECIAL, COLLATERAL, INDIRECT, PUNITIVE, INCIDENTAL, CONSEQUENTIAL OR EXEMPLARY DAMAGES IN CONNECTION WITH OR ARISING OUT OF TI RESOURCES OR USE THEREOF, AND REGARDLESS OF WHETHER TI HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

You agree to fully indemnify TI and its representatives against any damages, costs, losses, and/or liabilities arising out of your non-compliance with the terms and provisions of this Notice.

This Notice applies to TI Resources. Additional terms apply to the use and purchase of certain types of materials, TI products and services. These include; without limitation, TI's standard terms for semiconductor products http://www.ti.com/sc/docs/stdterms.htm), evaluation modules, and samples (http://www.ti.com/sc/docs/sampterms.htm).

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