Technical Article

Protecting Your Software Investment

Katie Pier

After years of work, way too little sleep and way too much coffee, you've developed an innovative new product that will disrupt the market and change the world. How do you protect the code that you've poured your blood, sweat and tears into developing?

While there is no perfect solution to protect against unauthorized access or reverse engineering, there are some precautions you can take to make your code more difficult to access. Using layers of security with different methodologies to control code access is typically your best bet.

TI's MSP430™ microcontroller (MCU) families provide a number of features that you can use together to increase layered protection of your code, enabling software IP protection, debugging security and secure storage. In this blog post, I'll explain these features.

IP Encapsulation for Software IP Protection and Secure Storage

MSP430FR5xx/6xx ferroelectric random access memory (FRAM) MCUs include an IP encapsulation (IPE) feature that you can use to encapsulate and protect a configurable area of FRAM memory from read or write access anywhere outside the IPE area by JTAG port, bootloader (BSL) or other code within the device.

This can be desirable when working with a third party; you can program code with your critical IP in the IPE area of a device, and even a third party partner who is later loading code into that same device can't read it out– they can only tell their code to execute functions from within the area. You can also store your encryption keys and encryption routines in the IPE area for added security. The application note "MSP430 Code Protection Features" includes many more details on enabling IPE in your system, including best practices and an example IPE project.

JTAG Locking Features for Debugging Security

All MSP430 microcontrollers contain some form of JTAG lock. The implementation varies across families, but the general idea is that in any MSP430 device, you can disable JTAG access to prevent someone from reading out the code. MSP430FR5xx/6xx FRAM MCUs, like the MSP430FR5994 device, also allow you to set a password on JTAG instead, so that authorized users can still access the device but other methods lock out all users. Again, the application note “MSP430 Code Protection Features” includes more details on different JTAG lock implementations across families and includes an example project using JTAG lock with a password.

BSL Security Features

Most applications need to have a way for authorized users to access the device but still prevent device readout. Most MSP430 devices include a BSL and a number of features to help prevent unauthorized readout. Commands that allow readout of the device are password-protected, usually with a 32-byte password. By default, an incorrect BSL password results in a mass erase of the device – this helps prevent someone from doing a brute-force attack on the password by trying every possible combination, because on the first attempt when the password is wrong, the device will erase itself and your IP will no longer be there to be read out. Alternately, you can totally disable the BSL if firmware updates aren’t going to be necessary.

With MSP430 MCUs, you can use layers of code-protection features to help secure your software investment. Now you can focus on what groundbreaking IP you’ll create next.

Additional Resources

- Check out the white paper, “Closing the security gap with TI’s MSP430 FRAM-based microcontrollers.”
- Find out more about device BSLs with these user’s guides:
  - MSP430FR5xx/6xx FRAM MCUs.
  - MSP430FR2xx/4xx FRAM MCUs.
  - MSP430 flash MCUs.

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