WHITE PAPER

Priya Thanigai
Product Marketing Engineer
Texas Instruments

TEXAS INSTRUMENTS

Closing the security gap with TI's MSP430™ FRAM-based microcontrollers

Introduction

Given how connected our world is today, addressing security concerns is becoming a ubiquitous need. However this involves securing a diverse and evolving range of "links" starting from large data servers down to the smallest connected node. Recent attacks on payment transactions have made the news and prove that a system is only as secure as each of its nodes. What are these nodes? How do we start approaching the task of ensuring the required level of security and what measures can we take to arm ourselves against threats? What are the expected threats and what system functions do they target? Answering these questions is the first step towards closing security gaps and ensuring your system is protected from threats that can weaken it or make it non-functional.

As an example, consider an end-to-end, connected home automation system. Some of the "links" in this system are:

- Nodes such as smart sensors to measure the environment around them e.g. temperature, carbon monoxide, intrusion
- Connectivity Peripherals such as wireless transceivers to transmit measured data from the sensors and receive actions based on preset conditions; these can also be a part of the nodes
- Gateway elements such as routers to connect the non-internet enabled nodes to the internet
- Cloud servers to store or log large amounts of data from multiple nodes and to process and analyze transmitted data

A fully connected smart home showing elements with different levels of security needs

Each link requires different levels of security and is subject to different types of threats or attacks. There is no single approach to securing an application, and the methods as well as their complexity vary depending on the element that needs to be secured as well as the criticality of the information. This paper identifies threats and offers risk mitigation methods for a portion of the system, in this case the sensor nodes that are typically driven by a microcontroller. An example of this can be temperature or lighting control elements, a remote garage-door opener and other similar home automation nodes. A microcontroller is often at the heart of these nodes and depending on the application, the process of closing the security gaps may vary.

An important question to ask is: What do you want to protect? For a microcontroller, this is typically either **(1)** Code or sensitive data on-chip or **(2)** communication channels that move data off-chip. We look at each of these aspects individually and at how TI's MSP430™ FRAM Microcontrollers (MCUs) provide built-in functions to make sensor nodes more secure.

(1) Protecting Code or Data on-chip: This can be divided into the following.

(a) Protecting from external readout attacks using the standard debug or firmware upgrade channels: Two commonly used methods to program microcontrollers are via the programming interface such as JTAG and through a boot strap loader (used mainly for firmware upgrade functions).

MSP430 FRAM Microcontrollers provide the means to either secure JTAG using a password or to disable it completely by programming a fuse signature in FRAM. In cases where the JTAG is disabled, access to the device is possible only using bootstrap loader (BSL). The BSL requires a password to read out or receive data. This password is the content of the interrupt vector table – which is a list of addresses or locations for interrupt service routines used in the application. On the FRAM-based MSP430 devices, providing an incorrect password will result in the entire FRAM code area being mass erased. This approach is inherently secure since it prevents the attacker from reading out any sensitive information from the microcontroller. One further way to increase the strength of the password is by filling any unused address spaces in the interrupt vector table with valid address values or by creating a double jump table making it harder to perform a brute force attack. In a system where many such nodes are deployed to the field, ideally, each node would contain random (or pseudo-random) values populating the interrupt vector table that are unique to that node (perhaps using the device identifier, manufacturer time stamp, etc.). In such a case applying a brute force attack to one node is not useful since it is inefficient and expensive to replicate such an attack on every node.

If firmware upgrades are not needed, then both JTAG and BSL can be disabled at the time of deployment.

(b) Protecting from unauthorized access of sensitive intellectual property (IP): In many cases the MCU code area is divided into secure and non-secure zones. An example of this could be a smart metering application that has both a display algorithm stored in an unsecure zone and a billing algorithm, an IP that needs to be protected. While field upgrades can modify the display algorithm, the billing IP is considered confidential and needs to be secured. An attacker may attempt to modify the critical IP, by introducing code that can read out or change the algorithm. To protect against such threats, MSP430 FRAM MCUs provide IP Encapsulation (IPE), a feature that allows code or data to be stored in a secure zone. In a secure environment, such as the factory, the address area that needs to be IP encapsulated is stored in FRAM. After the first power cycle, this address is mapped into the boot code area. Any further modification of this address is no longer possible and the area stays secure for the lifetime of the device. An IP encapsulated area cannot be accessed via JTAG, BSL or even in-system reads using DMA or direct register reads. To access code functions in the IPE area are called from outside the secure zone. Data reads in the IPE area are only possible when code inside the secure area is executed. This is useful for authentication algorithms where the nodes need to verify a signature (for example when pairing). In this case the signature key and the algorithm that is used for the authentication are both located in the IPE Area. The external application performs a function call and acts according to the results of the algorithm (signature identified/ denied).

(c) Protecting from physical attacks to the memory:

One of the key advantages MSP430 MCUs bring is TI's innovative non-volatile Ferroelectric Random Access Memory (FRAM) technology. In addition to features in the system architecture that prevent unauthorized reading and writing of application code and data, MCUs must also protect against malevolent manipulation of parameters to gain access to sensitive information as well as against invasive attacks against the physical MCU itself. MCUs can be vulnerable to a variety of attacks to extract data, application code or secure keys stored in memory.

In many cases, the goal of an attack on an MCU is to alter data stored on the device. For example, the usage data on an automatic utility meter can be modified to show lower than actual usage to result in a reduced monthly bill. In general, rather than attempt to modify the data that is collected, hackers will attempt to alter the application code itself. To achieve this, they need to be able to first obtain an image of the application code to reverse engineer and then overlay a modified version successfully within the system.
There are numerous methods that have been developed to force systems to expose confidential information or even their application code. For example, fault attacks can induce faulty operation by placing systems in an unpredictable state where they may output security keys or blocks of application code. Alternatively, hackers may attack a system physically, either by taking an MCU apart or inducing faults using optical means. Below are several common attacks:

Microscopy: The use of Atomic Force Microscopy (AFM) or Scanning Kelvin Probe Microscopy (SKPM) has been shown to be able to detect charge levels of the floating gate in an EEPROM after back side deprocessing so that data stored in memory locations or being transmitted on data lines can be recorded. For TI's MSP430 devices with FRAM, the bit write and read lines are physically located on either side of the polarized molecule, so delayering the chip is likely to destroy the contents of the memory.

Voltage manipulation: This type of attack has been used on EEPROM and Flash devices for several years, specifically for defeating phone cards. Effectively the input voltage to the device is manipulated outside the standard range to force-program bit cells. Note that it is difficult to provide brown-out and over-voltage protection circuitry that can operate longer than the time needed to complete programming of EEPROM bit cells. However, because of the fast read/write time for FRAM, it is possible to protect against voltage manipulation attacks.
TI achieves this by providing internal brown-out circuitry (BOR) and Supply Voltage Supervisors (SVS) that protects the voltage during read/write operations and allows the safe write-back circuitry to allow the FRAM to complete the write process correctly.

Light manipulation: There is evidence that Optical Fault Induction attacks are possible on EEPROM bit cells to alter data values. As neither laser light nor UV radiation impact FRAM bit cells (ignoring the heat effect of intense light), FRAM-based devices are secure against these types of attacks.

Radiation: Bit flips in EEPROM can be caused by alpha particles. TI's FRAM architecture has been shown to exhibit no effect from alpha particles and other radiation sources. In addition, given the ferroelectric nature of FRAM, they are also not affected by magnetic fields.

Note that not all of these attack scenarios apply to all applications. The likelihood of a particular attack being appropriate depends upon the type of application and the value of the data at risk. The next section talks about the methods to secure communication channels that move data to and from microcontrollers.

(2) Securing the communication channel:
In the example provided above, the sensor nodes need to communicate data (such as ambient temperature and other environmental data) quickly and securely. Similarly, a smart meter must be able to log usage measurements with the utility company. In addition, many such systems use the Internet as their primary communication channel to keep infrastructure costs down. There are a multitude ways to compromise the exchange of information over public networks. For example, by eavesdropping on an exchange, sensitive data from a legitimate transaction can be captured. Similarly, there are a wide range of effective countermeasures that have been developed to defeat them. The following section briefly describes some areas and methods where MSP430FRxx MCUs bring advantages when securing communication:

(a) Encryption: The primary technology used to protect exchanges today is cryptography. MCUs use encryption to ensure the confidentially of data as well as authentication to establish the identity of both parties in a transaction. It can also verify the integrity of data (i.e., detect if data has been corrupted in any way) as well as repudiate the credentials of any participant who is discovered to no longer be trustworthy.

Commonly known cryptographic standards include 3DES, AES, RSA and ECC. These standards are well-established and have been proven in real-world applications to provide sufficient security for the exchange of sensitive data. Many manufacturers are already familiar with them through their use in protocols such as ZigBee, Wi-Fi and Bluetooth. Today, such technology is straightforward to implement, but it does have impact on overall code size and power consumption that are especially important in portable, battery powered applications.

To enable an efficient and low power means to implement cryptography the MSP430FR5xx and MSP430FR6xx family of microcontrollers provide a 256-bit AES accelerator. This accelerator can perform 256-bit encryption in a fraction of the time and power required by software algorithms. In addition, the AES accelerator can be used to encrypt and decrypt data on-the-fly i.e. without having to store confidential information in RAM/EEPROM or other unsecured areas while waiting for an encryption/decryption operation to complete.

(b) Key storage: A common need with encryption algorithms is secure storage of the key. This can be achieved with FRAM microcontrollers easily and efficiently, since it is easy to generate a new key for every session and store it in FRAM. In traditional battery powered systems the option to perform a high-energy flash write is not always available. Also for an attacker snooping the power rails of the system it is an easy give-away if there is a huge spike in power exactly before storing the key due to a the flash charge pump being turned on. FRAM makes this easier and more secure because FRAM writes do not require pre-erase or charge pumps and complete very quickly. FRAM also provides near infinite endurance (10^15 cycles) ensuring that these keys locations can be overwritten multiple times over the life time of the product.

(c) Key generation: AES keys are used to encrypt and decrypt the plaintext (sensitive data that needs to be transmitted or received). The longer the length of the key, the more secure the encrypted information. An important parameter for key generation is the availability of a true random number seed. The MSP430FR5xx and MSP430FR6xx devices provide a random number seed that is unique to the device. The Device Descriptor Information (TLV) section contains a 128-bit true random seed that can be used to implement a deterministic random number generator for key creation.

(d) Integrating external memory: In many applications, a bulk of the data is stored off-chip either in external Flash, EEPROM or FRAM chips. This presents another challenge in terms of securely transmitting the data to and from the external memory. TI's MSP430 FRAM MCUs are available from 4kB FRAM to 128kB FRAM sizes allowing external memory requirements to be integrated into the MCU – providing a more secure and power efficient form of information storage.

A note on power

Portable applications that employ wireless connectivity need to be designed with power efficiency in mind. For example, an encrypted channel substantially increases transaction overhead through the handshaking and authentication processes used. This process increases the length of time a wireless radio is active, for example, but also how long the CPU is active. With traditional memory technologies like Flash or EEPROM, wireless updates to non-volatile memory (NVM) can take on the order of seconds at a constant current of over 5-10 mA. The negative impact on battery life is prohibitive.

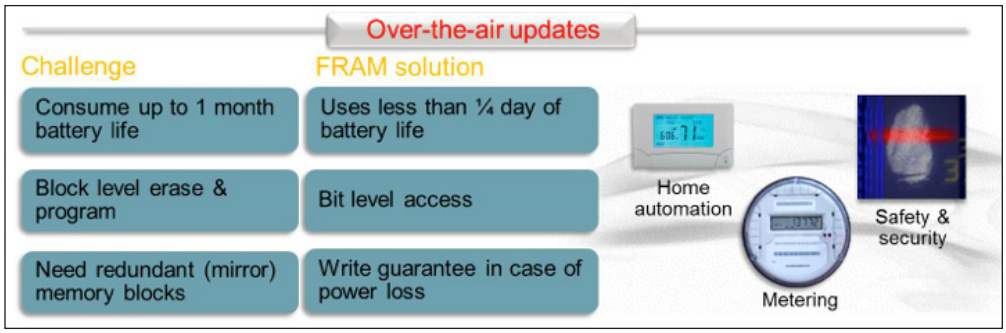

Figure: FRAM Microcontrollers provide a quicker and more secure means of wireless updates

MSP430FR5x/FR6x MCUs bring a double advantage in both the efficiency of the integrated AES 256 accelerator and FRAM memory technology allowing fast and low power writes consuming a fraction of the energy previously required. FRAM's efficiency also impacts power and memory usage efficiency during standard operation. Flash and EEPROM must erase and program memory a block at a time. Thus, to change a single-bit system flag, an entire block of 256 bytes must be read from Flash, the block erased and the block written back. With FRAM, developers have bit-level access to all of memory.

Finally, because of the read, erase, write sequence for EEPROM and Flash, developers must mirror data using redundant memory blocks to guarantee the integrity of data during a potential power loss. For example, if power is cut between the block erase and write, the data of the block will be lost. To prevent this, the system must read the block, mirror it in a redundant block, perform the erase and then write the block. If the power fails after the erase, when the system powers resets, it will detect the failed write operation and complete it using the mirrored block. On all MSP430 FRAM microcontrollers, write operations are guaranteed to complete through the use of an on-chip capacitor that ensures that there will be enough power to complete the current write operation. Because of the fast speed and lower current of FRAM writes, this capacitor can be small enough to be integrated into the MCU. Thus, there is no need for mirroring with FRAM.

The higher power efficiency of FRAM can be used to support a longer battery life. Alternatively, since devices can store more data for less power than when using EEPROM or Flash, developers have the option of having larger data buffers or event logs. This enables devices to check in less frequently, thus reducing how often a radio or other power-hungry communications channel must be used.

The active power consumption of the MSP430FR5969 MCU while running all secure operations is only 100 uA/MHz. In addition, because of the efficiency of the encryption engine, encryption is performed much faster, enabling the MCU to quickly drop to a lower operating current or into a low-power standby mode.

Addressing evolving security needs with the MSP430 FRAM family

No application can be completely secure. In addition, the more incentive there is to break a system, the more effort attackers will expend on trying to break into it. MSP430 FRAM MCUs offer the performance, peripherals and power efficiency required for securing critical portions of real-time embedded systems. With a 32x32 multiplier, 3-channel direct-memory access (DMA), and operation of up to 16 MHz, developers can ensure that real-time tasks are managed real-time. The MCUs also support a wide range of serial interfaces, including SPI, I2C and UART, capacitive touch I/O, and up to 83 GPIO. Devices also integrate analog such as a 12-bit ADC supporting up to 16 channels with single or differential inputs and a window comparator function, 16-channel comparator, power on reset, brownout reset, real-time clock and watch dog timer.

Given the increasing connectivity of devices, integrating security into products is becoming more prevalent amongst developers. Through the ability to prevent, detect and respond to malevolent behavior outside of a device's expected realm of operation, developers can protect both their customers' information as well as their own intellectual property by preventing exposure of data, protecting application code from being overwritten and providing secure communication channels for the exchange of sensitive data.

The highly efficient architecture of the MSP430 FRAM MCU family integrates hardware that reduces software complexity to simplify secure system design without compromising data integrity or reliability, all while lowering power consumption. The result is the ability to cost-effectively bring security to a whole new level of low-power applications.

Resources

For more information on the Ultra-low-power FRAM MCUs, visit www.ti.com/FRAM

1) Implement Market-driven Secure Microcontrollers, ECN:
http://www.ecnmag.com/articles/2010/08/implement-market-driven-secure-microcontrollers
2) FBI: Smart Meter Hacks Likely to Spread, KrebsOnSecurity:
http://krebsonsecurity.com/2012/04/fbi-smart-meter-hacks-likely-to-spread/

E010208

IMPORTANT NOTICE

Texas Instruments Incorporated and its subsidiaries (TI) reserve the right to make corrections, enhancements, improvements and other changes to its semiconductor products and services per JESD46, latest issue, and to discontinue any product or service per JESD48, latest issue. Buyers should obtain the latest relevant information before placing orders and should verify that such information is current and complete. All semiconductor products (also referred to herein as “components”) are sold subject to TI’s terms and conditions of sale supplied at the time of order acknowledgment.

TI warrants performance of its components to the specifications applicable at the time of sale, in accordance with the warranty in TI’s terms and conditions of sale of semiconductor products. Testing and other quality control techniques are used to the extent TI deems necessary to support this warranty. Except where mandated by applicable law, testing of all parameters of each component is not necessarily performed.

TI assumes no liability for applications assistance or the design of Buyers’ products. Buyers are responsible for their products and applications using TI components. To minimize the risks associated with Buyers’ products and applications, Buyers should provide adequate design and operating safeguards.

TI does not warrant or represent that any license, either express or implied, is granted under any patent right, copyright, mask work right, or other intellectual property right relating to any combination, machine, or process in which TI components or services are used. Information published by TI regarding third-party products or services does not constitute a license to use such products or services or a warranty or endorsement thereof. Use of such information 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.

Reproduction of significant portions of TI information in TI data books or data sheets is permissible only if reproduction is without alteration and is accompanied by all associated warranties, conditions, limitations, and notices. TI is not responsible or liable for such altered documentation. Information of third parties may be subject to additional restrictions.

Resale of TI components or services with statements different from or beyond the parameters stated by TI for that component or service voids all express and any implied warranties for the associated TI component or service and is an unfair and deceptive business practice. TI is not responsible or liable for any such statements.

Buyer acknowledges and agrees that it is solely responsible for compliance with all legal, regulatory and safety-related requirements concerning its products, and any use of TI components in its applications, notwithstanding any applications-related information or support that may be provided by TI. Buyer represents and agrees that it has all the necessary expertise to create and implement safeguards which anticipate dangerous consequences of failures, monitor failures and their consequences, lessen the likelihood of failures that might cause harm and take appropriate remedial actions. Buyer will fully indemnify TI and its representatives against any damages arising out of the use of any TI components in safety-critical applications.

In some cases, TI components may be promoted specifically to facilitate safety-related applications. With such components, TI’s goal is to help enable customers to design and create their own end-product solutions that meet applicable functional safety standards and requirements. Nonetheless, such components are subject to these terms.

No TI components are authorized for use in FDA Class III (or similar life-critical medical equipment) unless authorized officers of the parties have executed a special agreement specifically governing such use.

Only those TI components which TI has specifically designated as military grade or “enhanced plastic” are designed and intended for use in military/aerospace applications or environments. Buyer acknowledges and agrees that any military or aerospace use of TI components which have ***not*** been so designated is solely at the Buyer's risk, and that Buyer is solely responsible for compliance with all legal and regulatory requirements in connection with such use.

TI has specifically designated certain components as meeting ISO/TS16949 requirements, mainly for automotive use. In any case of use of non-designated products, TI will not be responsible for any failure to meet ISO/TS16949.

Products		**Applications**	
Audio	www.ti.com/audio	Automotive and Transportation	www.ti.com/automotive
Amplifiers	amplifier.ti.com	Communications and Telecom	www.ti.com/communications
Data Converters	dataconverter.ti.com	Computers and Peripherals	www.ti.com/computers
DLP® Products	www.dlp.com	Consumer Electronics	www.ti.com/consumer-apps
DSP	dsp.ti.com	Energy and Lighting	www.ti.com/energy
Clocks and Timers	www.ti.com/clocks	Industrial	www.ti.com/industrial
Interface	interface.ti.com	Medical	www.ti.com/medical
Logic	logic.ti.com	Security	www.ti.com/security
Power Mgmt	power.ti.com	Space, Avionics and Defense	www.ti.com/space-avionics-defense
Microcontrollers	microcontroller.ti.com	Video and Imaging	www.ti.com/video
RFID	www.ti-rfid.com		
OMAP Applications Processors	www.ti.com/omap	**TI E2E Community**	e2e.ti.com
Wireless Connectivity	www.ti.com/wirelessconnectivity		

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