WHITE PAPER

Priya Thanigai
产品营销工程师
德州仪器

Texas Instruments

TI MSP430™ FRAM 微控制器的安全特性提供最优的系统安全性能

简介

当今世界的联系十分密切，因而解决¬安全问题正成为一种普遍的需求。 但这涉及到保护日益繁多的各种“链接”，大到数据服务器，小到连接节点。 近期针对支付交易的攻击频有报道，它们证实了系统的安全性取决于系统的各个节点。 这些节点是什么？ 我们该如何着手执行可确保实现所需安全级别的任务？我们应采取什么措施来保护自己免遭侵袭？ 可能会出现哪些威胁？它们针对哪些系统功能？ 面对可能削弱系统功能或使其功能尽失的各种威胁，回答上述问题俨然成为弥补安全缺陷并确保系统免遭威胁的首要步骤

以已连接的端到端家庭自动化系统为例。 此系统中的部分“链接”包括：

- 测量周边环境的温度、一氧化碳和入侵行为等信息的节点，例如，智能传感器
- 传输来自传感器的测量数据并根据预设条件接收操作的连接外设，例如，无线收发器；它们也可以是节点的一部分
- 将未启用互联网的节点连接至互联网的网关元件，例如，路由器
- 存储或记录来自多个节点的大量数据并处理和分析传输数据的云服务器

具有不同的安全需求等级且完全连接的智能家庭显示元件

每个链接均需要不同的安全等级且针对不同的威胁或攻击类型。 没有一种万能的途径可以实现保护应用程序的目的，保护方法及其复杂性取决于需要保护的元件和信息的重要程度。 本文识别出系统中部分器件的威胁因素并提供了风险缓解措施，而此案例中的传感器节点通常由微控制器驱动。 例如，温度或照明控制元件、车库门摇控开关和其他类似的家庭自动化节点。 微控制器通常是这些节点的核心，由于应用不同，弥补安全缺陷的流程也不尽相同。

有一个重要问题： 您希望保护什么？ 对微控制器而言，保护对象通常是 (1) 代码或敏感的片上数据，或者 (2) 向片外移动数据的通信通道。 我们将逐个分析这些对象以及 TI 的 MSP430™ FRAM 微控制器 (MCU) 如何提供内置功能，以便让传感器节点更加安全。

(1) 保护代码或片上数据： 它可分为以下方式。

(a) 利用标准调试或固件升级渠道，保护代码或数据免遭外部读取攻击： 对微控制器进行编程的两个常用方法是通过 JTAG 等编程接口，或通过引导加载程序（主要用于固件升级功能）。

MSP430 FRAM 微控制器提供的方式如下：利用密码保护 JTAG；或通过在 FRAM 中对熔丝位标识进行编程来完全禁用 JTAG。 如果 JTAG 已禁用，则只能通过引导加载程序 (BSL) 访问器件。 BSL 需要密码才可读出或接收数据。 此密码是中断矢量表（用于此应用的中断服务例程的地址或位置列表）的内容。 在基于 FRAM 的 MSP430 器件上，如果提供的密码错误，会导致整个 FRAM 代码区遭到大范围擦除。 但从本质上看，此方法是安全的，因为它可以防止攻击者从微控制器中读出任何敏感信息。 进一步提高密码强度的方法是使用有效地址值填充中断矢量表中未使用的地址空间；或创建一个双跳转表，使蛮力破解更难以执行。 在诸多已将此类节点部署到相应字段的系统中，理想的情况下，各个节点均会包含填充中断矢量表的随机（或伪随机）值，这些值是该节点的唯一值（可能会使用设备标识符、制造¬商时间戳等）。 在这种情况下，对某个节点进行蛮力进攻毫无成效可言，因为针对各个节点重复发动此类进攻效率很低且成本昂贵。

如果无需固件升级，那么部署时可禁用 JTAG 和 BSL。

(b) 避免未经授权访问敏感的知识产权 (IP)： 许多情况下，MCU 代码区会分为安全区和非安全区。 以智能计量应用为例，其中的显示算法会存储在非安全区，而计费算法（需要保护的 IP）会存储在安全区。 虽然现场升级会修改显示算法，但计费 IP 会被视为机密且需加以保护。 攻击者可能会企图通过引入可读出或更改算法的代码来修改至关重要的 IP。 为防止此类威胁，MSP430 FRAM MCU 提供了 IP 封装 (IPE) 功能，允许将代码或数据存储在安全区。 在工厂等安全环境中，需要进行 IP 封装的地址区域会存储在 FRAM 中。 首次重启之后，该地址会映射到启动代码区域。 此后，对该地址的任何修改将不再奏效，代码区域在设备的使用寿命内都可保持安全。 IP 封装区域无法通过 JTAG、BSL、使用 DMA 的系统内读取或直接寄存器读取等方式进行访问。 IPE 区域中的访问代码函数需从安全区域外部调用。 只有执行了安全区域内部的代码，才会读取 IPE 区域的数据。 此操作对身份验证算法（其中的节点需要验证签名，例如在配对时）行之有效。 在这种情况下，用于身份验证的签名密钥和算法均位于 IPE 区域。 外部应用会根据算法结果（已识别/拒绝签名）执行函数调用和行为。

(c) 避免内存遭到物理攻击：

MSP430 MCU 带来的其中一个关键优势是 TI 创新型的非易失性铁电随机存取存储器 (FRAM) 技术。 在系统架构中，除了具备阻止未经授权而对应用代码和数据执行读写操作的功能，MCU 还必须防止为访问敏感信息而执行的恶意操纵参数的行为，以及针对物理 MCU 自身发起的侵入式攻击。 MCU 容易遭受各种攻击，这些攻击会试图窃取存储于内存的数据、应用代码或安全密钥。

许多情况下，针对 MCU 的攻击旨在篡改存储在设备上的数据。 例如，自动化公用事业计量表上的使用数据会遭到更改，以便显示低于实际使用量的数据，从而减少每月账单费用。 通常情况下，黑客会企图篡改应用代码本身，而非修改收集的数据。 为达上述目的，他们首先需要获取应用代码图像以执行逆向工程，然后在系统中成功覆盖已修改的版本。

目前已开发的方法不计其数，目的就是迫使系统暴露机密信息，甚至其应用代码。 例如，故障攻击会诱导错误操作：让系统陷入不可预知状态，从而泄露安全密钥或应用代码块。 此外，黑客还可能会借助物理方式攻击系统：拆卸 MCU 或利用光学手段诱导故障发生。 以下是几种常见攻击：

显微镜： 经证实，使用原子力显微镜 (AFM) 或扫描凯尔文探针显微镜 (SKPM) 能够在背面剥层后检测到 EEPROM 中的浮置栅极电荷水平，以便记录存储在内存位置或经数据线路传输的数据。 就带 FRAM 的 TI MSP430 器件而言，位线读写的物理位置位于极化分子的一侧，因此减少芯片层次可能会破坏内存内容。

电压篡改： 此类攻击多年来一直针对 EEPROM 和闪存器件，尤其用于破解手机卡。 实际上就是篡改设备输入电压，使其超过标准范围，然后对位单元进行强制编程。 请注意，提供工作时间比 EEPROM 位单元完成编程所需时间更长的欠压及过压保护电路系统非常困难。 不过，FRAM 具有较快的读写速度，因此可防止电压篡改攻击。 TI 可提供内部欠压复位 (BOR) 和电源电压监控器 (SVS)，它们能够保护读/写操作过程中的电压并支持安全的回写式电路，以便 FRAM 正确完成写入流程，从而达到上述目的。

光篡改： 有证据表明，EEPROM 位单元可能会遭到光纤故障感应攻击，从而篡改数据值。 激光或紫外线辐射均不会影响 FRAM 位单元（忽略强光热效应），因此基于 FRAM 的设备可安全应对此类攻击。

辐射： 阿尔法粒子可导致 EEPROM 发生位翻转。 经证实，TI FRAM 架构不受-阿尔法粒子及其它辐射源的影响。 此外，由于 FRAM 具有铁电属性，它也不受磁场的影响。

请注意，上述攻击方案并非适用于所有应用。 某种攻击是否发生和能否起作用取决于应用的类型和危险数据的价值。 第二部分讲述了保护用于将数据传出并传回微控制器的通信通道的方法。

(2) 保护通信通道的安全性：
如上文示例所述，传感器节点需要快速且安全地传递数据（例如，环境温度和其他环境数据）。 同样，智能仪表必须有能力记录公用事业公司产生的使用测量数据。 此外，许多此类系统将 Internet 用作他们的主要通信通道，以便控制基础设施成本。 通过公共网络破坏信息交易的方式数不胜数。 例如，窃听交易信息可捕获合法交易中的敏感数据。 同样，现已开发了大量有效对策来回击上述行为。 下文主要介绍了 MSP430FRxx MCU 在保护通信时发挥优势的区域及其保护方法：

(a) 加密： 当今用于保护交易的主要技术就是加密。 MCU 使用加密技术来确保数据的保密性；并通过身份验证来证明交易双方的身份。 加密还可以确保数据的完整性（例如，检测数据是否遭到任何形式的损坏）并拒绝被发现不再可信的任何成员的凭证。

常见的加密标准包括 3DES、AES、RSA 和 ECC。 这些标准成熟可靠且已通过实际应用的验证，能够为敏感数据的交易提供充分的保护。 许多制造商已在 ZigBee、Wi-Fi 和 Bluetooth 等协议的使用过程中掌握了上述标准。 虽然此技术目前易于实施，但却增加了总体代码大小和功耗，而这两个因素在便携式电池供电应用中至关重要。

为采取一种高效节能的加密实施方法，MSP430FR5xx 和 MSP430FR6xx 系列微控制器提供了一个 256 位 AES 加速器。 该加速器可执行 256 位加密，满足了软件算法的高效节能要求。此外，AES 加速器可用于即时对数据进行加密和解密，即无需将机密信息存储于 RAM/EEPROM 或其他非安全区域，从而节省了等待加密/解密操作完成的时间。

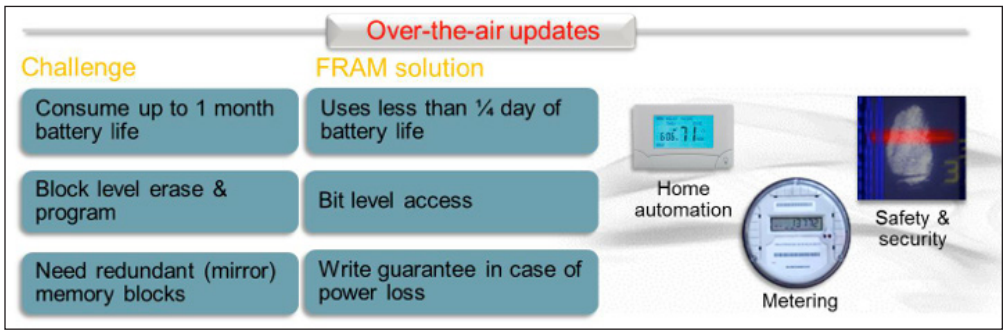
(b) 密钥存储： 加密算法的基本需求即安全存储密钥。 FRAM 微控制器可轻松高效地实现这一需求，原因是它易于为每次会话生成新密钥并将其存储于 FRAM 中。 传统的电池供电系统并不一定能够提供执行高能量闪存写入的选项。 相反，对窥探系统电源轨的攻击者来说，如果启动闪存电荷泵时能够在存储密钥之前产生巨大能量，攻击者就会轻易放弃。 由于 FRAM 写入无需预擦除或电荷泵，因此可极其快速地完成密钥存储过程，从而更加便捷安全地实现此目标。 FRAM 还可提供几乎无限的寿命（10^15 个周期），确保在产品的整个生命周期内多次重写这些密钥位置。

(c) 密钥生成： AES 密钥用于对明文（需要收发的敏感数据）进行加密和解密。 密钥长度越长，加密信息就越安全。 密钥生成的一个重要参数即是否存在真正的随机数种子。 MSP430FR5xx 和 MSP430FR6xx 器件可提供设备专有的随机数种子。 设备描述符信息 (TLV) 部分包含一个真正的 128 位随机种子，用于运行可创建密钥的决定性随机数生成器。

(d) 集成外部存储器： 在多数应用中，大量数据存储于片外，如外部闪存、EEPROM 或 FRAM 芯片。 但就安全传输往返于外部存储器的数据而言，它又带来了另一个挑战。 TI 的 MSP430 FRAM MCU 可提供 4kB 至 128kB 的 FRAM，支持将外部存储器需求集成到 MCU，从而提供更安全节能的信息存储方式。

电源注意事项

采用无线连接的便携式应用需具备节能的设计理念。 例如，加密通道会在执行信号交换和身份验证的过程中大大增加交易负担。 该过程不但延长了无线电的工作时间，还延长了 CPU 的工作时间。 如果使用传统的闪存或 EEPROM 等存储技术，无线更新至非易失性存储器 (NVM) 的操作需在大于 5-10 mA 的恒定电流下执行且耗时较长。 这对电池寿命有很大的负面影响。



图： FRAM 微控制器可提供更快速安全的无线更新方式

MSP430FR5x/FR6x MCU 具备高效集成型 AES 256 加速器和 FRAM 存储技术的双重优势，支持快速、低功耗写入，其消耗的能量仅占传统技术所需能量的极小部分。 在标准的操作过程中，高效 FRAM 还会对电能和内存使用效率产生影响。 闪存和 EEPROM 必须一次擦除一个内存块并对其进行编程。 因此，要更改单位系统标识，就必须从闪存中读取完整的 256 字节块，并对其执行擦除和写回操作。 有了 FRAM，开发人员可对所有内存进行位级访问。

最后，由于 EEPROM 和闪存的读取、擦除和写入操作是续发事件，开发人员必须使用额外的内存块备份数据，以便在可能发生断电时确保数据的完整性。 例如，如果擦除块和写入块的操作之间发生断电，块的数据将会丢失。 为防止此类事件发生，系统必须先读取块，然后将数据备份在额外的块中，最后再依次执行擦除和写入操作。 如果擦除完成后出现断电，系统会在电源复位后检测未执行的写入操作并利用备份块完成此操作。 片上电容器可保证有充足的电能完成电流写入操作，因而能够确保完成所有 MSP430 FRAM 微控制器中的写入操作。 该电容器尺寸很小，完全可以集成到 MCU 中，这得益于 FRAM 写入的快速高效及其较低的电流消耗。 这样一来，FRAM 无需进行备份。

FRAM 较高的功效可延长电池寿命。 此外，与使用 EEPROM 或闪存时相比，FRAM 微控制器能够以更低的功耗存储更多数据，从而让开发人员能够选择容量更大的数据缓冲区或事件日志。 这样微控制器可降低检查频率，从而减少无线电或其他高耗电量通信通道的使用频率。

在运行所有安全操作的情况下，MSP430FR5969 MCU 的有效功耗仅为 100 uA/MHz。 此外，高效的加密引擎使得加密运行更加快速，能够让 MCU 迅速降至降低的工作电流或进入低功耗待机模式。

利用 MSP430 FRAM 系列解决日益增长的安全需求

任何应用都无法确保百分之百安全。 而且，攻破系统的好处越多，攻击者为侵入系统而付出的努力就越多。 MSP430 FRAM MCU 可提供保护实时嵌入式系统关键部分所需的性能、外设和功效。 借助 32x32 倍增器、3 通道直接存储器存取 (DMA) 和高达 16 MHz 的工作频率，开发人员可确保实时管理实时任务。 MCU 还支持各种串行接口，包括 SPI、I2C、UART、电容式触控 I/O 和最多 83 个 GPIO。 它们还可集成模拟，例如，支持高达 16 个通道的 12 位 ADC，具有单端或差动输入和窗口比较器功能、16 通道比较器、上电复位、欠压复位、实时时钟和监视器计时器。

由于器件的连接功能不断增加，开发人员越来越注重于将安全性融入产品。 开发人员具备阻止、检测和回击恶意操作（已超出器件预期的工作范围）的能力，他们能够阻止数据泄露、保护应用代码免遭重写、为敏感数据的交易提供安全的通信通道，从而达到保护客户信息及其知识产权的目的。

MSP430 FRAM MCU 系列的高效架构集成了可降低软件复杂性的硬件，以便简化安全的系统设计，从而在不损坏数据完整性或可靠性的条件下降低功耗。 最终在节约成本的前提下将低功耗应用的安全性能提升至一个全新的层次。

资源

有关超低功耗 FRAM MCU 的详细信息，请访问 www.ti.com/FRAM

1) 《实施以市场为导向的安全微控制器》(Implement Market-driven Secure Microcontrollers)，ECN：
http://www.ecnmag.com/articles/2010/08/implement-market-driven-secure-microcontrollers
2) 《FBI：智能仪表黑客可能会蔓延》 (FBI:Smart Meter Hacks Likely to Spread)，KrebsOnSecurity：
http://krebsonsecurity.com/2012/04/fbi-smart-meter-hacks-likely-to-spread/

重要声明

德州仪器(TI) 及其下属子公司有权根据 JESD46 最新标准, 对所提供的产品和服务进行更正、修改、增强、改进或其它更改， 并有权根据 JESD48 最新标准中止提供任何产品和服务。客户在下订单前应获取最新的相关信息, 并验证这些信息是否完整且是最新的。所有产品的销售都遵循在订单确认时所提供的TI 销售条款与条件。

TI 保证其所销售的组件的性能符合产品销售时 TI 半导体产品销售条件与条款的适用规范。仅在 TI 保证的范围内，且 TI 认为 有必要时才会使用测试或其它质量控制技术。除非适用法律做出了硬性规定，否则没有必要对每种组件的所有参数进行测试。

TI 对应用帮助或客户产品设计不承担任何义务。客户应对其使用 TI 组件的产品和应用自行负责。为尽量减小与客户产品和应 用相关的风险，客户应提供充分的设计与操作安全措施。

TI 不对任何 TI 专利权、版权、屏蔽作品权或其它与使用了 TI 组件或服务的组合设备、机器或流程相关的 TI 知识产权中授予 的直接或隐含权限作出任何保证或解释。TI 所发布的与第三方产品或服务有关的信息，不能构成从 TI 获得使用这些产品或服 务的许可、授权、或认可。使用此类信息可能需要获得第三方的专利权或其它知识产权方面的许可，或是 TI 的专利权或其它 知识产权方面的许可。

对于 TI 的产品手册或数据表中 TI 信息的重要部分，仅在没有对内容进行任何篡改且带有相关授权、条件、限制和声明的情况 下才允许进行复制。TI 对此类篡改过的文件不承担任何责任或义务。复制第三方的信息可能需要服从额外的限制条件。

在转售 TI 组件或服务时，如果对该组件或服务参数的陈述与 TI 标明的参数相比存在差异或虚假成分，则会失去相关 TI 组件 或服务的所有明示或暗示授权，且这是不正当的、欺诈性商业行为。TI 对任何此类虚假陈述均不承担任何责任或义务。

客户认可并同意，尽管任何应用相关信息或支持仍可能由 TI 提供，但他们将独力负责满足与其产品及在其应用中使用 TI 产品 相关的所有法律、法规和安全相关要求。客户声明并同意，他们具备制定与实施安全措施所需的全部专业技术和知识，可预见 故障的危险后果、监测故障及其后果、降低有可能造成人身伤害的故障的发生机率并采取适当的补救措施。客户将全额赔偿因 在此类安全关键应用中使用任何 TI 组件而对 TI 及其代理造成的任何损失。

在某些场合中，为了推进安全相关应用有可能对 TI 组件进行特别的促销。TI 的目标是利用此类组件帮助客户设计和创立其特 有的可满足适用的功能安全性标准和要求的终端产品解决方案。尽管如此，此类组件仍然服从这些条款。

TI 组件未获得用于 FDA Class III（或类似的生命攸关医疗设备）的授权许可，除非各方授权官员已经达成了专门管控此类使 用的特别协议。

只有那些 TI 特别注明属于军用等级或“增强型塑料”的 TI 组件才是设计或专门用于军事/航空应用或环境的。购买者认可并同 意，对并非指定面向军事或航空航天用途的 TI 组件进行军事或航空航天方面的应用，其风险由客户单独承担，并且由客户独 力负责满足与此类使用相关的所有法律和法规要求。

TI 已明确指定符合 ISO/TS16949 要求的产品，这些产品主要用于汽车。在任何情况下，因使用非指定产品而无法达到 ISO/TS16949 要求，TI不承担任何责任。

	产品		应用
数字音频	www.ti.com.cn/audio	通信与电信	www.ti.com.cn/telecom
放大器和线性器件	www.ti.com.cn/amplifiers	计算机及周边	www.ti.com.cn/computer
数据转换器	www.ti.com.cn/dataconverters	消费电子	www.ti.com/consumer-apps
DLP® 产品	www.dlp.com	能源	www.ti.com/energy
DSP - 数字信号处理器	www.ti.com.cn/dsp	工业应用	www.ti.com.cn/industrial
时钟和计时器	www.ti.com.cn/clockandtimers	医疗电子	www.ti.com.cn/medical
接口	www.ti.com.cn/interface	安防应用	www.ti.com.cn/security
逻辑	www.ti.com.cn/logic	汽车电子	www.ti.com.cn/automotive
电源管理	www.ti.com.cn/power	视频和影像	www.ti.com.cn/video
微控制器 (MCU)	www.ti.com.cn/microcontrollers		
RFID 系统	www.ti.com.cn/rfidsys		
OMAP应用处理器	www.ti.com/omap		
无线连通性	www.ti.com.cn/wirelessconnectivity	德州仪器在线技术支持社区	www.deyisupport.com

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