Application Brief

了解 C2000 实时控制 MCU 的安全特性

器件和系列说明

TI C2000™ F28x 系列微控制器专为工业和汽车领域的实时控制应用而设计。所有 F28x 微控制器都具有速度为 40MHz 至 200MHz 的 32 位 C28x CPU，通常与控制律加速器 (CLA) 等加速器内核搭配使用。凭借紧密耦合的模拟外设（如模数转换器 (ADC)）、比较器以及高级数字驱动外设（如高分辨率 PWM 模块），有许多充分的理由在嵌入式实时控制应用中使用 C2000 微控制器。

TI 嵌入式安全产品系列

表 1. 常见的信息安全机制

C2000™ MCU 系列	信息安全机制	详细的安全特性
F28P55x+ F28P65x+ F280015x+ F280013x+ F28003x+ F28002x+ F2838x+ F28004x+ F2837xD+ F2837xS+ F2807x+ F2806x F2805x F2803x F2802x F2833x、 F2823x F28M3x	器件标识	唯一标识 (UID) 号：用户能够启用通信中的器件识别机制、数据完整性算法的种子机制、身份验证和加密或解密的矢量初始化机制，或防止代码克隆机制。
	软件 IP 保护	代码安全模块 (CSM)：用户能够阻止在未经授权的情况下对存储在片上存储器中的固件进行访问或编程。标有 (+) 的器件具有双代码安全模块 (DCSM)，带有两个独立的安全区域。
	调试安全	使用 CSM 提供仿真代码安全逻辑 (ECSL)：用户能够使用密码实现对存储器的完全调试访问。

表 2. 最新的信息安全机制

C2000™ MCU 系列	信息安全机制	详细的安全特性
F28P55x F28P65x F280015x F280013x F28003x F2838x	附加调试安全性	JTAGLOCK：能够阻止调试器访问器件；可通过密码解锁。
	安全启动	该选项可启用 AES-128 基于密码的消息认证码 (CMAC)，以便在转移代码执行之前对闪存的前 16KB 进行预先验证。
F28P55x F28P65x F28003x F2838x	加解密加速	硬件高级加密标准（AES 128/192/256 位）引擎，可提升性能。
F28P55x	闪存写入和擦除保护	永久锁定闪存特定区域以使内容不可更改的选项。该选项可用于在软件中实施额外的加密功能来进行代码和数据身份验证，从而扩充安全启动能力。

针对的安全问题：典型威胁、安全措施

在实时控制系统的设计中，嵌入式固件开发占据了很大一部分研发投资。因此，产品固件中包含的知识产权可为用户提供关键的竞争优势，但也容易被盗。要复制最终产品，对系统进行可视化组件拆解相对容易，但要有效保护 MCU 上运行的固件，就不能完全复制正常工作的系统。

另一种日益普遍的情况是共同开发固件。在这些情况下，系统固件的某些部分是由核心工程团队以外的团队开发，可能是由第三方供应商开发。在这些情况下，一方可以选择保持固件的私有性，同时仍允许另一方在同一系统上开发和测试应用程序的一部分。此类情况通常不在传统的运行时软件保护范围内，并且在通过调试器访问 MCU 时需要硬件保护机制。

这种情况在汽车应用中尤为常见，在这些应用中，可能有多家公司涉及在高度连接的系统中生产和调试固件。C2000 器件上提供的信息安全机制可以解决这些类型的威胁。

安全实现

从 TI 发出的新器件在到达时处于完全解锁状态。在用户启用安全协议后，任何锁定的存储器区域只能由同样处于同一区域中的代码访问。还提供专用的解锁存储

器，以便在需要时可以在区域之间传输数据。除了该基本构建块之外，还可以选择性地启用其他选项或层：

1. 选择要保护的存储器块：

   在许多情况下，并非所有存储器（无论是易失性还是非易失性）都需要锁定。对于在不同子系统之间共享或包含非专有 IP 的某些固件，情况也是如此。
2. 区域所有权（仅限 DCSM）：

   除了保护各种存储器块之外，每个 DCSM 实现中还有两个区域。分配存储器以进行保护后，下一步就是确定这些区域中的哪个区域对选定的存储器进行控制。但是，如果不需要对同一器件的不同开发人员实行代码保护，则可以使用单区域配置。
3. 仅执行保护（仅限 DCSM）：

   如果一个区域仅用于执行而不用于内部数据存储，则程序员可以启用*仅执行保护*来阻止任何读取访问（即使来自同一区域或区），以增强安全性。
4. CPU 保护（仅限 DCSM）：

   如果 DCSM 检测到从任何锁定区域执行代码，也会阻止对中央处理器 (CPU) 寄存器的调试访问。
5. 仿真代码安全逻辑 (ECSL)：

   即便使用上述措施，如果 MCU 从锁定区域执行，用户仍可以限制仿真连接。在调试会话期间可使用密码暂时禁用此安全功能。
6. 唯一标识号 (UID)：

   通过使用每个器件上提供的 UID 号，可以实施技术来进一步允许软件仅在已知器件上运行。如需更多信息，请参阅 *C2000™ 唯一器件编号*。
7. JTAGLOCK：

   可以使用用户选择的密码禁用和保护 JTAG（仿真器）接口。这有助于确保只有经过授权的人员才能查看和调试应用。
8. AES 加速：

   广泛使用的 AES 对称密码因其速度和简单性而闻名。即便如此，嵌入式微控制器中 AES 算法的软件实现速度也相对较慢，无法满足实时控制系统的需求。硬件 AES 加速器显著缩短了处理加密消息的时间，同时释放了处理过程中的 CPU 带宽。有多种不同的操作模式和密钥大小可用。
9. 安全启动：

   为了保持器件中存储的固件的完整性，可以启用安全启动来验证闪存存储器中存储的代码，然后再将执行转移到存储的代码。除了安全逻辑中内置的固件编程保护外，这还有助于确保在器件上运行的代码为正版代码。使用的算法是 AES-128 CMAC 算法。可使用工具将所需的 MAC 值嵌入到最终代码映像中。如需更多信息，请参阅 *C2000 器件上的安全启动*。
10. 闪存写入和擦除保护：

    在某些情况下，用户可以选择通过实施其他加密身份验证算法来扩展安全启动功能，包括 ECDSA 等基于椭圆曲线的功能。在具有闪存写入和擦除保护的器件中，可以将这些功能放置在代码入口点的闪存区域中，并使其不可更改（即永久不可更改和不可修改）。此功能可实现更强的加密功能，还可用于实现安全的固件更新功能。

其他资源

虽然终端应用中的安全风险可能有多种形式，但固件知识产权保护是大多数系统常见的威胁。借助 C2000 微控制器，用户能够通过适用于多用户开发环境的灵活功能来解决这些问题。有关 C2000 微控制器的更多信息，请参阅 TI.com/C2000。有关各个 C2000 器件中安全功能的具体信息，请参阅 TI.COM™ 产品页上提供的产品数据表和技术参考手册。

备注

保障安全绝非易事。TI 提供更简单易用的网络安全解决方案。

更多有关 TI 嵌入式安全设计的信息，请访问 TI.com/security。

商标

重要声明和免责声明

TI“按原样”提供技术和可靠性数据（包括数据表）、设计资源（包括参考设计）、应用或其他设计建议、网络工具、安全信息和其他资源，不保证没有瑕疵且不做出任何明示或暗示的担保，包括但不限于对适销性、某特定用途方面的适用性或不侵犯任何第三方知识产权的暗示担保。

这些资源可供使用 TI 产品进行设计的熟练开发人员使用。您将自行承担以下全部责任：(1) 针对您的应用选择合适的 TI 产品，(2) 设计、验证并测试您的应用，(3) 确保您的应用满足相应标准以及任何其他功能安全、信息安全、监管或其他要求。

这些资源如有变更，恕不另行通知。TI 授权您仅可将这些资源用于研发本资源所述的 TI 产品的应用。严禁对这些资源进行其他复制或展示。您无权使用任何其他 TI 知识产权或任何第三方知识产权。您应全额赔偿因在这些资源的使用中对 TI 及其代表造成的任何索赔、损害、成本、损失和债务，TI 对此概不负责。

TI 提供的产品受 TI 的销售条款或 ti.com 上其他适用条款/TI 产品随附的其他适用条款的约束。TI 提供这些资源并不会扩展或以其他方式更改 TI 针对 TI 产品发布的适用的担保或担保免责声明。

TI 反对并拒绝您可能提出的任何其他或不同的条款。

邮寄地址：Texas Instruments, Post Office Box 655303, Dallas, Texas 75265