Application Brief

了解 C2000 实时控制 MCU 的安全特性

器件/系列说明

TI C2000™ 微控制器 (MCU) 专为工业和汽车领域的实时控制应用而设计。因此，TI C2000 微控制器出于对实时控制的考虑进行构建。所有 C2000 MCU 均基于 32 位 C28x MCU 内核处理器，频率范围为 40MHz 至 200MHz。C2000 MCU 具有紧密耦合的模拟外设（如模数转换器 (ADC)、比较器以及 PWM 等快速响应数字激励），有充分理由在实时控制应用中使用。

TI 嵌入式安全产品系列

表 1. 信息安全机制

C2000 MCU 系列	信息安全机制	详细的安全特性
TMS320F28003x TMS320F28002x TMS320F2838x TMS320F28004x TMS320F2837xD TMS320F2837xS TMS320F2807x TMS320F2806x TMS320F2805x TMS320F2803x TMS320F2802x TMS320F2833x/23x F28M3x	器件识别	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
	调试安全	通过 CSM 提供仿真代码安全逻辑 (ECSL)：用户能够通过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
TMS320F28003x TMS320F2838x	附加调试安全性	JTAGLOCK：能够阻止器件的仿真；可通过密码解锁
	加密加速	硬件高级加密标准（AES 128/192/2566 位）引擎，可提升性能
	安全启动	该选项可启用 AES128 基于密码的消息认证码 (CMAC)，以便在传输代码执行之前对闪存的前 16KB 进行预先验证。

针对的安全问题：典型威胁/安全措施

与任何微控制器一样，用户级研发投资有很大一部分用于固件开发。因此，产品固件中包含的知识产权 (IP) 可以为市场中的企业以及具有较高遭窃风险的企业提供关键的竞争优势。为了复制最终产品而拆卸系统的视觉组件可以轻松完成，而且保护在 MCU 上运行的固件可以防止完全重复的工作系统。

另一种日益普遍的情况是共同开发固件。很多时候，某些系统固件由主要工程团队以外，甚至可能是公司以外的人员开发。在这些情况下，一方有时希望保持其固件的私有性，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，需要在 MCU 处于调试状态时进行保护。

这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。大多数 C2000 器件上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。在您启用安全协议后，锁定区域将只能由同样处于同一区域中的代码访问。还有专用的解锁存储器，以便在需要时可以在区域之间传输数据。除了该基本实现之外，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，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将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/区），以增强安全性。
4. CPU 保护（仅限 DCSM 和 F2837x/07x）：

   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，可能仍然需要限制仿真连接。这可以在调试会话期间使用密码暂时禁用。
6. 唯一标识 (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/调试应用。
8. AES 加速：

   世界上常见的加密算法之一以其速度和简易性而闻名。即便如此，实时微控制器中 AES 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。硬件加速器显著缩短了处理加密消息的周期时间，同时释放了处理过程中的 CPU 带宽。提供多种不同的模式和位大小。
9. 安全启动：

   作为另一层固件保护，可以选择在启动时运行安全启动，然后再将执行权移交给用户闪存代码。除了安全逻辑中内置的编程保护外，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 AES128 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。

附加资源

虽然终端应用中的安全风险可能有多种形式，但 IP/固件保护是大多数系统常见的威胁。C2000 MCU 系列可让我们的客户通过适用于多开发环境的灵活特性来解决这些问题。有关 C2000 MCU 安全技术的更多信息，请参阅 C2000 MCU 功能安全页面。有关特定器件信息，请参阅技术参考手册，该手册可在任何 C2000 MCU 产品文件夹的数据表和勘误表下方找到。

备注

信息安全是一项艰巨的工作，TI 让这项工作变得更加简单。

更多有关 TI 嵌入式安全解决方案的信息，请访问 https://www.ti.com/technologies/security/overview.html。

商标

C2000™ is a trademark of Texas Instruments.
所有商标均为其各自所有者的财产。

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