

Technical White Paper

嵌入式处理器供应链中的 CRA 角色



Josue Zamitiz-Ayala, Frangline Jose, and Amrit Mundra

摘要

欧盟的《网络弹性法案》(CRA, 即法规 (EU) 2024/2847) 规定了投放欧盟市场的含数字元素产品的网络安全要求, 其中包括出售给产品制造商用于集成的微处理器等硬件元件。CRA 在整个供应链中分配合规性要求: 元件供应商和产品制造商根据各自在供应链中所承担的角色, 分别承担明确规定的一组要求。本文介绍了 TI 作为元件制造商在芯片和软件开发套件 (SDK) 层面所承担的责任, 以及产品制造商 (包括一级电路板供应商、模块上系统 (SoM) 供应商和原始设备制造商 (OEM) 系统集成商) 根据 CRA 仍需承担哪些责任。本文不构成法律建议; 读者需要咨询其法务与合规团队, 以获得针对具体产品的指导。

1 简介

欧盟的《网络弹性法案》(CRA) 是一个强制性法律框架, 为在欧盟市场销售的所有含有数字元素的硬件和软件产品制定了统一的网络安全要求。CRA 将于 2027 年 12 月 11 日开始实施。漏洞报告要求已于 2026 年 9 月 11 日生效。对于构建集成第三方半导体元件的联网器件的产品制造商而言, CRA 带来一项无法通过孤立观察芯片或软件来解决的合规难题: 该法规将要求分配给供应链中的各个角色, 凡是以自身名义将含数字元素产品投放到欧盟市场, 均需承担相应责任。

在欧盟销售的产品必须遵循安全设计原则, 在整个支持期间保持更新, 并维持可信的漏洞处理流程。合规性挑战源于大多数嵌入式产品的供应链结构。构建联网的物联网网关、工业控制器或协作机器人的 OEM 通常会集成芯片供应商提供的微处理器、一级制造商或模块上系统 (SoM) 供应商提供的板级支持包 (软件), 以及自身的应用软件。各方均已将元件投放到市场, 并各自承担 CRA 规定的责任。

产品制造商不能通过选择已满足 CRA 要求的供应商提供的元件来规避 CRA 要求。元件供应商的合规情况无法满足产品制造商的风险评估、符合性声明 (即产品符合所有 CRA 要求的正式声明), 以及向产品制造商所在国家的 CSIRT (国家网络安全事件响应团队) 和 ENISA (欧盟网络安全局) 报告的要求。这两组要求并行适用; 一组要求不能替代另一组要求。不合规将处以高达公司全球年收入 2.5% 的罚款。元件供应商和中间集成商也不能豁免。

本文介绍 TI 对供应链边界的解读、TI 作为元件制造商在芯片和 SDK 层面为满足相关要求所采取的措施, 以及集成产品制造商为确保完整产品合规必须采取的措施。合规性认定需要由具备相应资质的法务与合规顾问进行。

2 CRA 范围和元件供应商问题

2.1 法规涵盖范围

CRA 适用于“在欧盟市场上提供的、其预期用途或合理可预见的用途包括与器件或网络建立直接或间接逻辑或物理数据连接”的含数字元素产品。¹ 实际上, “间接”连接涵盖可通过 USB、串行接口或本地网络访问的任何器件。几乎所有嵌入式产品都符合条件。CRA 明确将单独出售的软件或硬件元件 (例如出售给 OEM 用于集成的微处理器) 纳入含数字元素产品的定义范围。

作为集成到大型系统中的元件出售的 TI 微处理器和微控制器是含数字元素的产品。根据这一定义, 将 TI 芯片集成到成品器件的 TI 和 OEM 均为制造商, 但其生产的产品不同, 因此要求也不同。

CRA 将若干产品类别排除在其适用范围之外, 包括受法规 (EU) 2019/2144 管辖的机动车辆、受法规 (EU) 2017/745 管辖的医疗器械以及受法规 (EU) 2018/1139 管辖的民用航空设备。最终产品受行业法规管辖的客户, 需要与其法务团队确认适用的合规路径。

2.2 CRA 如何对 TI 产品进行分类

CRA 将产品分为四个风险类别。大多数含数字元素的产品均属于默认类别，需要满足一组基线要求。高风险产品类型被归类为重要类别，即 I 类或 II 类。最敏感的产品被指定为关键产品。

根据 CRA，任何包含内置安全功能的微处理器或微控制器均为 I 类。I 类适用于具有加密加速器、硬件安全引导或受保护密钥存储的微处理器。II 类是一个单独且要求更严格的类别，适用于具有硬件防篡改功能的芯片，例如采用物理防护措施，即使攻击者能够直接接触器件，也无法提取机密信息或修改器件行为。不具备防篡改功能的微处理器属于 I 类，即使这些微处理器支持虚拟化也是如此。在器件上运行的虚拟机监控程序软件单独进行分类。

TI 的 Jacinto™ 和 Sitara™ 处理器系列属于 I 类。TDA54x SoC/处理器也属于 II 类，因为该器件集成了防篡改功能。

I 类和 II 类产品在欧盟销售之前必须经过更严格的审批流程。该法规规定了三种证明合规性的方法。第一种方法是通过自我评估流程（仅适用于 I 类），该流程基于正式认可的欧洲技术标准，即协调标准（EN50765，正在制定中）。第二种方法是通过指定机构。例如，欧盟指定的第三方实验室可以对产品进行审核与认证（适用于 I 类和 II 类）。模块 H 是第三个选项。指定机构将对制造商的设计、开发和漏洞处理流程进行一次审核。审核通过后，制造商无需再次接受审核，即可对后续产品进行认证。模块 H 适用于 I 类和 II 类产品以及关键产品。

这一分类适用于 TI 的产品以及 TI 承担的符合性义务，不适用于 OEM 的成品。将默认类别或 I/II 类 TI 元件集成到联网系统中的 OEM 必须单独确定其最终产品的分类。

2.3 集成边界

集成 TI 元件并将成品系统投放到欧盟市场的产品制造商，不会因此继承 TI 在元件层面的合规性。

CRA 适用于以自身名义将产品投放到欧盟市场的任何实体。当 OEM 将搭载 TI 处理器的联网器件投放到欧盟市场时，该 OEM 即成为该器件的制造商，并需承担该产品整体的全部合规要求。TI 作为元件制造商的要求是额外的，而不是替代产品制造商的要求。

TI 提供的合规资料和硬件功能可直接纳入产品制造商的证据包。OEM 在产品层面的 SBOM 以 TI 的 SBOM 为基础构建，并涵盖整个产品。TI CVE 安全公告作为输入信息，纳入 OEM 的漏洞处理流程。

3 责任共担模式

3.1 供应链分层架构

大多数包含 TI 芯片的嵌入式产品都遵循分层供应链：以 TI 芯片为基础，TI SDK 在芯片之上提供固件和软件栈，一级制造商或 SoM 供应商将芯片和 SDK 集成到电路板或模块中，而 OEM 在顶层构建最终产品。供应链责任分层架构映射了这一分层架构，并将 CRA 要求与各层相对应。

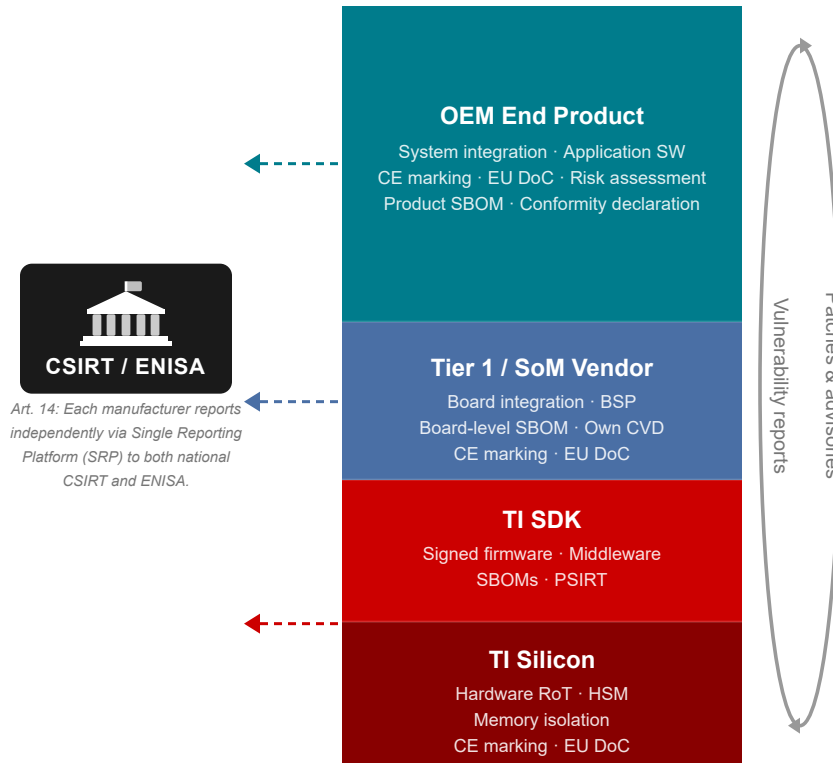


图 3-1. 整个供应链中的 CRA 共担责任

节 3.1 显示如何在整个供应链中共担 CRA 责任。TI 满足硬件和元件层面的要求（底层两层）。一级供应商和 SoM 供应商承担中间集成要求。OEM 承担完整产品层面的符合性责任。补丁、安全公告和漏洞报告共同构成一个循环披露链（右侧椭圆，顺时针方向）。第 14 条要求供应链中的每家制造商独立报告遭到积极利用的漏洞；各制造商层面会同时通知国家 CSIRT 和 ENISA（虚线箭头）；有关各层面的报告时限和义务，请参阅“第 14 条 — 制造商的报告义务”。法规 (EU) 2024/2847（《网络弹性法案》）。

供应链责任分层架构中的漏洞披露链展示了安全公告和补丁义务如何沿分层架构向上传递：

1. TI 通过 TI-PSIRT 发布 CVE 安全公告
2. 一级供应商或 SoM 供应商将该安全公告整合到板层面更新，并将安全公告传递其 OEM 客户
3. OEM 修补产品，并将更新交付给最终用户。如果该漏洞遭到积极利用，TI 将根据第 14 条的规定，同时通知国家 CSIRT 和 ENISA。

如果一级供应商或 SoM 供应商以及 OEM 中的任何一方获悉最终产品中存在遭到积极利用的漏洞，则相关各方分别承担同样的义务。

CRA 要求制造商报告两类安全事件，每类事件均包含三个步骤的通知序列。第一类（途径 1）适用于遭到积极利用的漏洞，例如攻击者利用产品中的已知缺陷对用户发起攻击的情况。途径 2 适用于对产品安全造成影响的严重事件，例如影响或可能影响产品保护数据或功能可用性、真实性、完整性或机密性的事件，或者导致或可能导致在产品或用户系统中引入或执行恶意代码的事件。两个途径下的所有通知均通过 CRA 单一报告平台同时提交给指定为协调方的国家 CSIRT 和 ENISA。

表 3-1. 第 14 条 — 制造商的报告义务

时限	内容 (原文)
途径 1：遭到积极利用的漏洞 (第 14(1)-(2) 条)	
获悉后 24 小时内	“关于遭到积极利用的漏洞的预警通知……在适用的情况下，应指明制造商获悉其含数字元素的产品已在其境内提供的成员国”

表 3-1. 第 14 条 — 制造商的报告义务（续）

时限	内容 (原文)
途径 1：遭到积极利用的漏洞（第 14(1)-(2) 条）	
获悉后 72 小时内	“漏洞通知……应根据可获得的信息提供有关所涉及含数字元素的产品、漏洞利用方式的一般性质以及相关漏洞的一般性质的信息，以及已采取的任何纠正或缓解措施，和用户可采取的纠正或缓解措施”
在提供纠正或缓解措施后 14 天内	“最终报告……至少包括：(i) 对漏洞的描述，包括其严重性和影响；(ii) 在可获得的情况下，有关已利用或正在利用该漏洞的任何恶意行为者的信息；(iii) 有关为修复该漏洞而提供的安全更新或其他纠正措施的详细信息”
途径 2：对安全产生影响的严重事件（第 14(3)-(4) 条）	
获悉后 24 小时内	“针对影响含数字元素产品安全性的严重事件发出的预警通知……至少应包括该事件是否涉嫌由非法或恶意行为引起”
获悉后 72 小时内	“事件通知……应根据可获得的信息提供有关事件性质的一般信息、对事件的初步评估，以及已采取的任何纠正或缓解措施，和用户可采取的纠正或缓解措施”
72 小时事件通知提交后 1 个月内	“最终报告……至少包括：(i) 对该事件的详细描述，包括其严重性和影响；(ii) 可能引发该事件的威胁类型或根本原因；(iii) 已采取和正在实施的缓解措施”

途径 1 适用于产品中已知的缺陷遭到积极利用的情况，报告时限与漏洞发现和修复相关。途径 2 适用于安全事件已经对产品或用户造成影响的情况，无论是否已确定具体漏洞。途径 2 的报告时限与事件的发生相关。两种途径并非互斥。遭到积极利用的漏洞如果导致安全破坏事件，则会同时触发两种途径，并且每个事件都需要一组独立的通知。

3.2 根据 CRA 要求分配责任

节 3.2 列出了供应链中各方承担的主要 CRA 要求。如果制造商未在欧盟境内设有实体，则 CRA 要求其指定授权的欧盟代表。该代表是当地注册的实体，可以接收监管通信，并代表制造商行事。这一分配反映了 TI 对典型嵌入式产品供应链的解读。具体产品和供应链安排可能导致不同的责任分配；但节 3.2 不能替代针对具体产品的合规性分析。

表 3-2. 整个供应链中的 CRA 义务分配

CRA 要求	法规依据	TI (元件制造商)	一级/SoM 供应商	OEM 产品制造商
网络安全风险评估	第 13(2) 条	芯片层面威胁模型；安全数据表	板层面风险评估	涵盖整个系统的产品层面风险评估
SBOM — 顶级依赖项	附录 I，第 II 部分，第 1 项	SBOM (SPDX、CycloneDX)；使用 MySecure 获取的安全软件	板级 SBOM	集成所有供应商 SBOM 和自有应用的产品 SBOM
发布时未发现可利用的漏洞	附录 I，第 I 部分，第 2(a) 项	每次发布前已扫描 SDK	发布前已扫描板 (BSP) 软件。供应商还提供 SDK 和其他软件。	在投放欧盟市场之前，对完整产品进行已知漏洞扫描
默认安全配置	附录 I，第 I 部分，第 2(b) 项	提供硬件信任根和安全引导功能；在强制安全型器件型号上由 ROM 强制执行	配置板默认设置	产品以安全默认状态发货；提供客户说明；强制要求客户更改密码等默认设置
可能的安全更新	附录 I，第 I 部分，第 2(c) 项	通过 CI/CD 流水线或安全文件夹提供固件补丁（基于灵敏度）。PSIRT/PSAP 跟踪并传达补丁状态。	板更新机制	向最终用户提供更新；免费
防止未经授权的访问	附录 I，第 I 部分，第 2(d) 项	硬件访问控制；调试端口控制	板层面身份验证	产品层面身份验证和访问管理
集成保护	附录 I，第 I 部分，第 2(f) 项	签名的固件架构支持引导完整性；在安全强制型器件型号上以加密方式强制执行	电路板元件的固件签名	系统层面的完整性验证
限制攻击面	附录 I，第 I 部分，第 2(j) 项	硬件隔离	板接口配置	产品接口最小化和加固
产品安全测试和漏洞处理的安全测试报告	附录 I 第 I 部分、附录 I 第 II 部分和附录 VII(6)	涵盖元件层面安全功能的测试报告。更新了每个元件层面漏洞修复的报告。	涵盖板层面安全集成的测试报告。更新了每个板层面漏洞修复的报告。	涵盖最终产品安全功能的测试报告。更新了每个产品层面漏洞修复的报告。

表 3-2. 整个供应链中的 CRA 义务分配（续）

CRA 要求	法规依据	TI (元件制造商)	一级/SoM 供应商	OEM 产品制造商
CE 标识	第 29-30 条	投放到欧盟市场的 TI 元件必须加贴	如果一级供应商独立将模块投放到欧盟市场，则必须加贴	最终产品必须加贴
授权的欧盟代表	第 18 条	TI 在欧盟设有实体	如果未在欧盟设立一级供应商，则必须指定	如果未在欧盟设立 OEM，则必须指定
协调漏洞披露 (CVD) 政策	附录 I，第 II 部分，第 5 项	TI PSIRT 政策	一级供应商自己的 CVD 政策	OEM 针对其产品自己的 CVD 政策
漏洞报告联系方式	附录 I，第 II 部分，第 6 项	psirt@ti.com	一级供应商安全联系方式	向最终用户发布的 OEM 安全联系方式
报告遭到积极利用的漏洞	第 14 条	TI 使用 CRA 单一报告平台同时通知国家 CSIRT 和 ENISA；有关完整的通知序列，请参阅“第 14 条 — 制造商的报告义务”。	一级供应商同时通知国家 CSIRT 和 ENISA；有关完整的通知序列，请参阅“第 14 条 — 制造商的报告义务”。	OEM 同时通知国家 CSIRT 和 ENISA；有关完整的通知序列，请参阅“第 14 条 — 制造商的报告义务”。
支持期限声明	附录 II，第 7 项	每个器件系列的生命周期指南	声明的模块支持期限	向最终用户声明的产品支持期限
技术文档	第 31 条	元件层面的技术文档	模块层面的技术文档	完整产品的技术文档

3.3 一级和 SoM 供应层面

许多 TI 客户都通过一级电路板制造商或 SoM 供应商开展业务，后者在 TI 与 OEM 之间搭建桥梁。当一级供应商或 SoM 供应商以自身名义将电路板或模块投放到欧盟市场时，该供应商即为制造商，并需满足 CRA 要求。如果供应商作为合同制造商在 OEM 的指导下开展业务，且未以自身名义将产品投放到市场，则 CRA 规定的制造商义务完全由 OEM 承担。同样，在芯片直接集成设计中，OEM 直接集成 TI 芯片，中间没有一级供应商或 SoM 供应商，因此 OEM 独自承担产品层面的义务。

作为制造商的一级供应商或 SoM 供应商必须生成板级 SBOM，其中集成 TI 的 SDK SBOM，保留自己的 CVD 政策和披露联系人，并向下游集成商提供安全文档。

通过符合 CRA 合规流程的一级供应商选择板或模块不会免除 OEM 进行产品层面风险评估、生成产品层面 SBOM 以及声明成品符合性的要求。每个角色的要求均适用于其以自身名义投放到市场的产品。

4 TI 与 CRA 相关的安全功能

TI 设计支持安全功能的器件系列，以满足附录 I 中的硬件和元件级要求。有关器件特定实施指南，请参阅适用的器件数据表、安全用户指南和 [保障未来：借助 TI 的 Jacinto 和 Sitara 处理器实现 CRA 合规性](#) 技术白皮书。

4.1 硬件安全功能

具备安全功能的 TI 处理器包括一个专用安全子系统，该子系统在与主应用处理器隔离的内核上运行，并通过 TI 提供的固件 (TI Foundational Security - TIFS) 实现硬件信任根。在新一代器件上提供了用于客户 HSM 软件栈第二个专用安全内核，从而能够在不向应用域软件暴露密钥材料的情况下启用加密服务。

在生产时永久预置到芯片中的公钥为安全引导提供了锚点。对于安全强制 (HS-SE) 器件型号，引导 ROM 会在执行前验证主固件映像上的数字签名，并拒绝失败验证的映像，从而在上电后提供硬件强制完整性和真实性验证。

硬件访问控制将片上存储器划分为分配给各个处理域的区域，从而防止跨工作负载边界进行未经授权的读取或写入。

对于具备安全功能的器件型号，可以对生产单元永久禁用调试接口，或者将其限制为仅在通过签名证书完成请求身份验证后才能访问，从而关闭利用调试工具进行攻击的常见攻击向量。

除了器件型号以外，每个芯片都带有唯一的芯片 ID，从而能够精确识别特定的芯片实例并满足产品识别要求。

4.2 SDK 和软件安全

TI 为在 ti.com 上作为 SDK 组成部分提供开源代码的所有产品提供 SPDX 和 CycloneDX 格式的 SBOM。可通过 TI 的 MySecure 访问计划获取安全软件组件的 SBOM。

在每次发布之前都会扫描 TI 处理器 SDK 检查已知漏洞。TI 通过 PSIRT 管理完整的漏洞处理生命周期：通知接收、分类、技术分析、补救以及基于 CVSS v3.1 严重性评分和 CVE 分配协调的公开披露。该流程符合 ISO/IEC 30111 和 ISO/IEC 29147 标准。TI 免费提供安全补丁及安全公告消息。

TI 通过产品安全公告门户 (PSAP) (网址：ti.com/psap) 发布补丁和安全公告。PSAP 为客户提供一个结构化渠道，使其能够通过 myTI 帐户报告漏洞、订阅针对其设计中 TI 产品的安全公告信息源，并以 CSAF v2.0 机器可读格式访问披露信息。CSAF v2.0 安全公告指明受影响的具体软件组件，使客户能够根据其 SBOM 自动关联，并在 CRA 报告时限内评估风险暴露情况。

TI 根据 BSI TR-03183-3 和 RFC 9116 标准，在 ti.com/well-known/security.txt 发布了 security.txt 文件。该文本文件包含 PSIRT 联系地址、CVD 政策 URI 和 CSAF 提供商元数据。TI 受德国司法管辖，对于第 14 条规定的报告，TI 指定的国家 CSIRT 为由德国联邦信息安全办公室 (BSI) 运营的 CERT-Bund。TI 通过 CRA 单一报告平台在规定时限内提交事件通知。

第 14 条要求制造商在“获悉”遭到积极利用的漏洞后 24 小时内通知相应的国家 CSIRT。该法规没有规定在多人组织中何时视为已经获悉漏洞。制造商会提前定义在其组织内何种情况构成“获悉”，无论是在接收确认时，还是由负责的技术团队成员首次审查报告时；但是，如果这一时间点未作定义，就会产生合规风险。24 小时的时限从定义的时刻开始，而不是从某位工程师审查报告时开始。PSAP 的自动截止日期跟踪功能通过在时限结束前升级处理报告来强制执行此规定。任何 TI 已知的、遭到积极利用的漏洞都会触发这一 24 小时时限，无论相关信息来自安全研究人员、客户还是内部发现。随后将在 72 小时内提交后续通知，并附上更全面的评估，通过 CRA 单一报告平台同时提交给国家 CSIRT 和 ENISA。

4.3 文档和生命周期资料

TI 为每个器件系列发布了详细的数据表，记录了硬件安全功能和接口规格。专门的更新策略说明了 TI 何时以及如何提供固件补丁。每个器件的生命周期指南明确了支持期限和保修范围。

用户指南涵盖了安全引导设置、调试端口配置和 HSM 集成。

5 结语

含数字元素的互联产品要实现 CRA 合规，需要整个供应链采取协调一致的行动。各方均有不同的要求，任何一方的要求都不能替代另一方的要求。

TI 履行其作为元件制造商的职责：在具备安全功能的器件型号上提供硬件信任根和存储器隔离、签名固件、SBOM、符合 CRA 第 14 条报告时限要求的 PSIRT 流程，以及涵盖 CRA 信息要求的器件层面文档。产品制造商和一级供应商可将这些功能和资料纳入其合规工作。他们仍需负责 TI 无法代其承担的产品层面合规要求。

将联网器件投放到欧盟市场的产品制造商必须进行产品层面网络安全风险评估、生成产品层面 SBOM、声明符合性、加贴 CE 标志；如果未在欧盟设立，还必须指定欧盟授权代表。此外，他们还必须建立相关流程，在获悉存在遭到积极利用的漏洞后 24 小时内，同时通知国家 CSIRT 和 ENISA，并在 72 小时内完成更全面的评估：有关完整的通知序列，请参阅“第 14 条 — 制造商的报告义务”。TI 的 PSIRT 安全公告和 SBOM 将纳入该流程。

要评估 TI 的器件功能如何对应您的 CRA 要求，请联系 TI 安全团队，并查阅 ti.com/quality-reliability/quality/ti-psirt.html 上的 PSIRT 政策。请咨询您的法务与合规团队，以获得针对具体产品的指导。第 14 条规定的漏洞报告要求已经生效。CRA 将于 2027 年 12 月全面实施；面向欧盟市场打造联网器件的产品制造商现在就需要开始进行合规性评估。

6 参考资料

1. 欧洲议会和欧洲联盟理事会 (2024 年 11 月 20 日)。“欧洲议会和理事会关于含数字元件产品横向网络安全要求的法规 (EU) 2024/2847 (《网络弹性法案》)”。欧盟官方公报，L 系列。
2. 德州仪器 (TI)。“TI PSIRT”网页
3. 德州仪器 (TI)。“《网络弹性法案》(CRA)”网页
4. 德州仪器 (TI)，保障未来：借助 TI 的 Jacinto 和 Sitara 处理器实现 CRA 合规性 技术白皮书
5. 德州仪器 (TI)，加强合规性：简化网络安全漏洞管理 应用简报

重要通知和免责声明

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任何明示或暗示的担保，包括但不限于对适销性、与某特定用途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安全、安保法规或其他要求。

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 产品的相关应用。严禁以其他方式对这些资源进行复制或展示。您无权使用任何其他 TI 知识产权或任何第三方知识产权。对于因您对这些资源的使用而对 TI 及其代表造成的任何索赔、损害、成本、损失和债务，您将全额赔偿，TI 对此概不负责。

TI 提供的产品受 [TI 销售条款](#)、[TI 通用质量指南](#) 或 [ti.com](#) 上其他适用条款或 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。除非德州仪器 (TI) 明确将某产品指定为定制产品或客户特定产品，否则其产品均为按确定价格收入目录的标准通用器件。

TI 反对并拒绝您可能提出的任何其他或不同的条款。

版权所有 © 2026，德州仪器 (TI) 公司

最后更新日期：2025 年 10 月