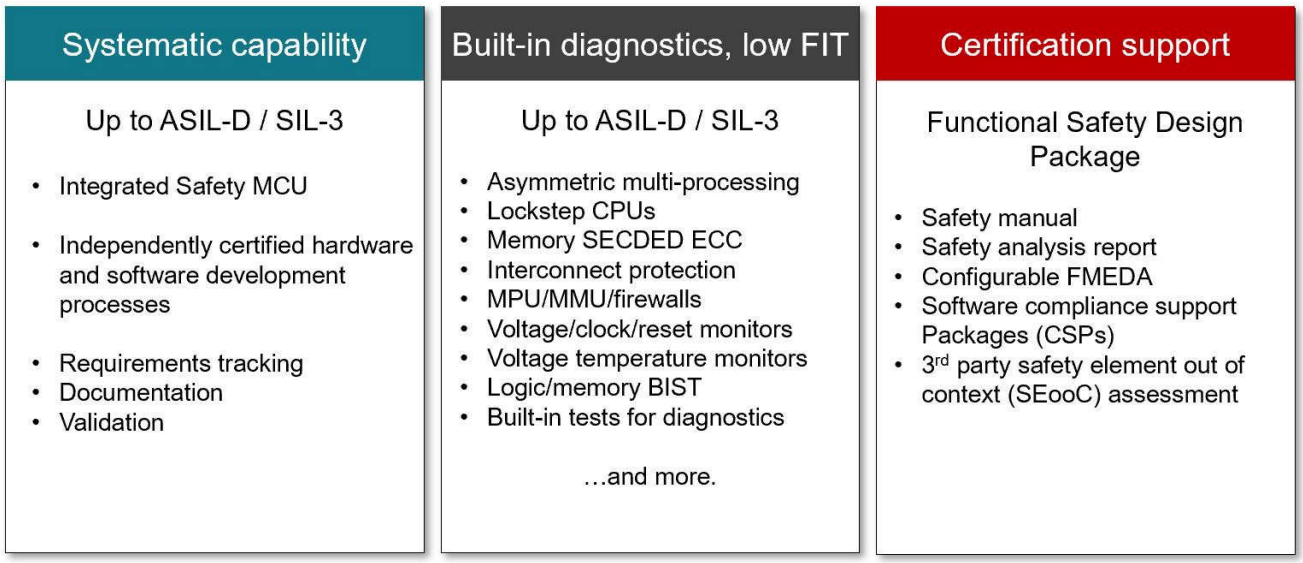
Product Overview

Jacinto™ 7 安全产品概述

摘要

在本文档中，我们将介绍有关 Jacinto 7 的安全基础知识，以及 TI 为客户功能安全实现提供的配套资料。

Jacinto SoC 是根据 ISO26262/IEC61508 标准流程开发的独立功能安全元素 (SEooC)，可实现 ASIL-D/SIL-3 等级的系统故障完整性，并包含硬件诊断功能，助力达到 ASIL-D/SIL-3 等级的随机故障完整性。该器件已通过经认证的第三方 (TUV-SUD) 安全评估，可提供证书。



内容

1 Jacinto™ 7 安全架构概念 1
1.1 安全架构概述：MCU 岛和扩展 MCU 岛 2
1.2 实现混合关键性 - 无干扰 (FFI) 3
2 安全机制概述 3
3 系统中的安全实现 4
3.1 硬件配套资料 4
3.2 软件支持 4
4 修订历史记录 4

商标

1 Jacinto™ 7 安全架构概念

有关 Jacinto 器件的完整架构概述，请参阅相应 SoC 的器件技术参考手册。Jacinto 7 SoC 采用异构架构，以混合关键性为设计目标，在性能、外设和功能安全要求方面具有可扩展性。Jacinto 系列中各个器件的安全元件分区和安全目标均略有不同，表 1 对此进行了总结。

表 1. 安全完整性表

	主域	MCU 域	扩展 MCU 岛	总 DMIPS (ASIL-D/SIL-3)
DRA829/TDA4VM	ASIL-B/SIL-2	ASIL-D/SIL-3	不适用	高达 2K
DRA821	ASIL-B/SIL-2	ASIL-D/SIL-3	ASIL-D/SIL-3	高达 4K

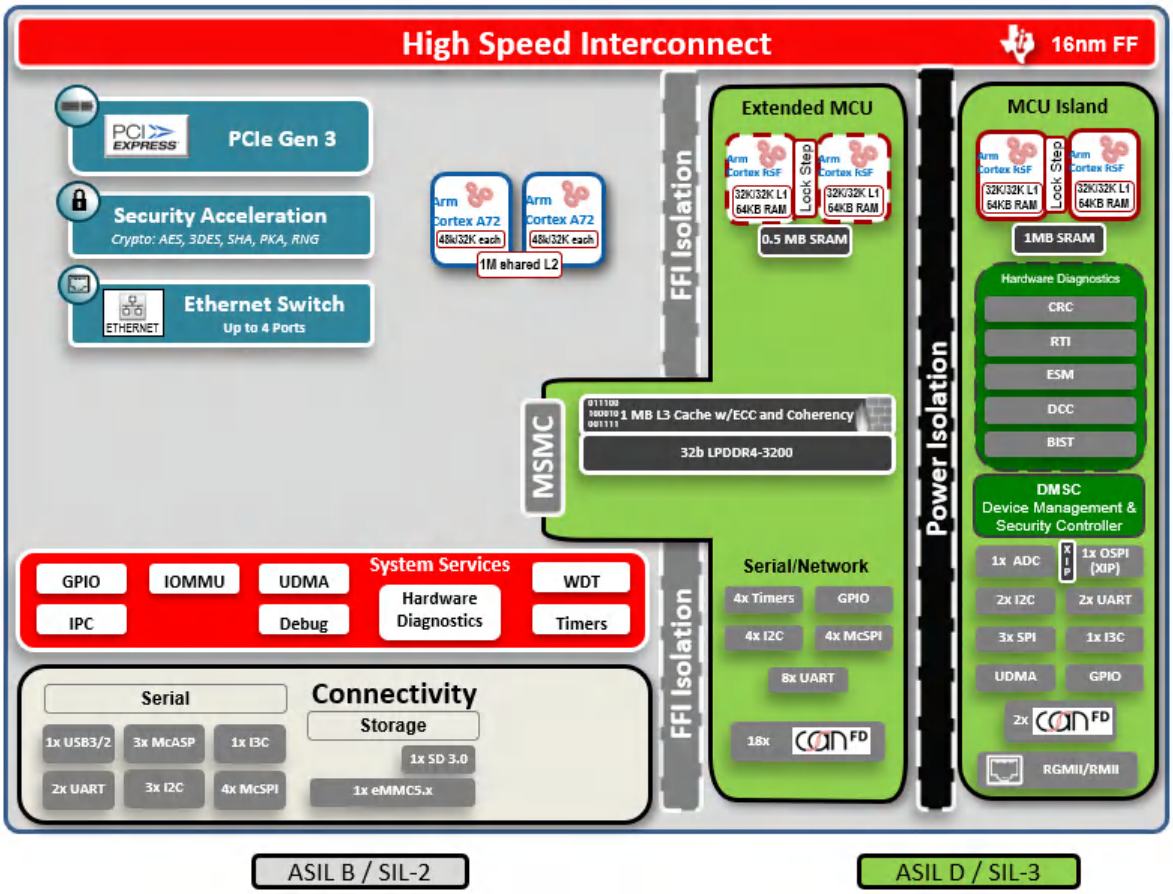


图 1. DRA821 器件

1.1 安全架构概述：MCU 岛和扩展 MCU 岛

整个芯片可实现达 ASIL-D/SIL-3 等级的系统故障完整性。每个相应域的随机故障指标完整性均假设使用了充分的硬件诊断与建议的软件/系统诊断，并实施了使用假设 (AoU)。

MCU 岛：Jacinto 7 系列产品在 SoC 内部集成了安全 MCU，用于监测安全关键功能和信号。该部分称为 MCU 岛，如上方绿色方框图所示。MCU 岛可提供安全分区，其具有丰富的硬件诊断功能，可实现达 ASIL-D/SIL-3 等级的随机故障完整性。MCU 岛由一对可以在锁步模式下运行的 R5F 内核，用于域内通信的安全互连以及各类外设组成。

扩展 MCU 岛：Jacinto 7 系列的某些器件（请参阅表 1：安全可扩展性表）配有扩展 MCU 岛。该分区为上面方框图中的绿色部分，借助额外的 R5F 内核提高 ASIL-D/SIL-3 DMIPS 性能，并增加外设实例以实现达 ASIL-D/SIL-3 等级的随机故障完整性。扩展 MCU 还可为 DDR 提供达 ASIL-D/SIL-3 等级的访问能力，这在需要安全数据访问并且安全岛或扩展安全岛内的片上存储器不足时具备显著优势。

SOC 的其余部分（主域如 图 1 的灰色区域所示）满足最高 ASIL-B/SIL-2 等级的随机故障完整性要求。

1.2 实现混合关键性 - 无干扰 (FFI)

当系统中混合 ASIL 等级的元件共存时，ISO26262 标准要求实现无干扰。这可以防止来自较低关键性元素的级联故障影响较高关键性元素。Jacinto 系列产品通过实施多种架构功能助力实现 FFI。

- **硬件隔离**：MCU 安全岛是独立域，相对于 SoC 其余部分具有强大的无干扰性能。这是通过单独电压、时钟和复位域及其自有的一组专用外设和资源来实现的。如果主域崩溃、挂起或需要复位，MCU 域仍然可以继续执行安全关键型功能。
- **防火墙**：防火墙是一个根据配置设置限制传入总线事务访问的模块。防火墙可针对某些策略配置，以确保非安全或安全性较低的元件无法访问或操作安全关键型内核、外设或存储器。通过设置策略即可监测传入事务的地址和属性（读取、写入、安全等），以阻止或允许访问。
- **隔离垫片**：MCU 岛和扩展 MCU 岛都设置了隔离垫片，充当与整个 SoC 共享的低等级安全关键型资源的容错连接。
- **PVU/MMU**：除了支持虚拟化等功能外，MMU 还通过内存映射隔离内存路径，从而支持混合关键性用例。通过配置模块，即可确保低等级安全关键型内核只能访问其自身的地址空间和外设。

2 安全机制概述

为了确保系统级安全，面向基本操作的强大硬件诊断功能搭配系统和软件诊断，助力满足 SoC 的随机故障完整性指标。诊断覆盖有三种基本类别：

- *硬件安全机制*：此类机制启用一旦，会持续运行。
  - 相关示例包括但不限于：用于存储器和互连的 SECDED ECC 和奇偶校验、PLL 滑动和失锁检测、过压/欠压检测。
- *硬件 + 软件安全机制*：此类机制基于硬件，但需要定期的软件交互来启动或维持运行。
  - 相关示例包括但不限于：看门狗计时器、存储器和寄存器校验的 CRC 硬件支持、双时钟比较器。
- *软件安全机制*：此类机制基于旨在执行部分测试和校验结果的软件。
  - 相关示例包括但不限于：信息冗余技术、传输冗余、基本功能的软件测试。此类机制的实现通常取决于客户应用和用例。

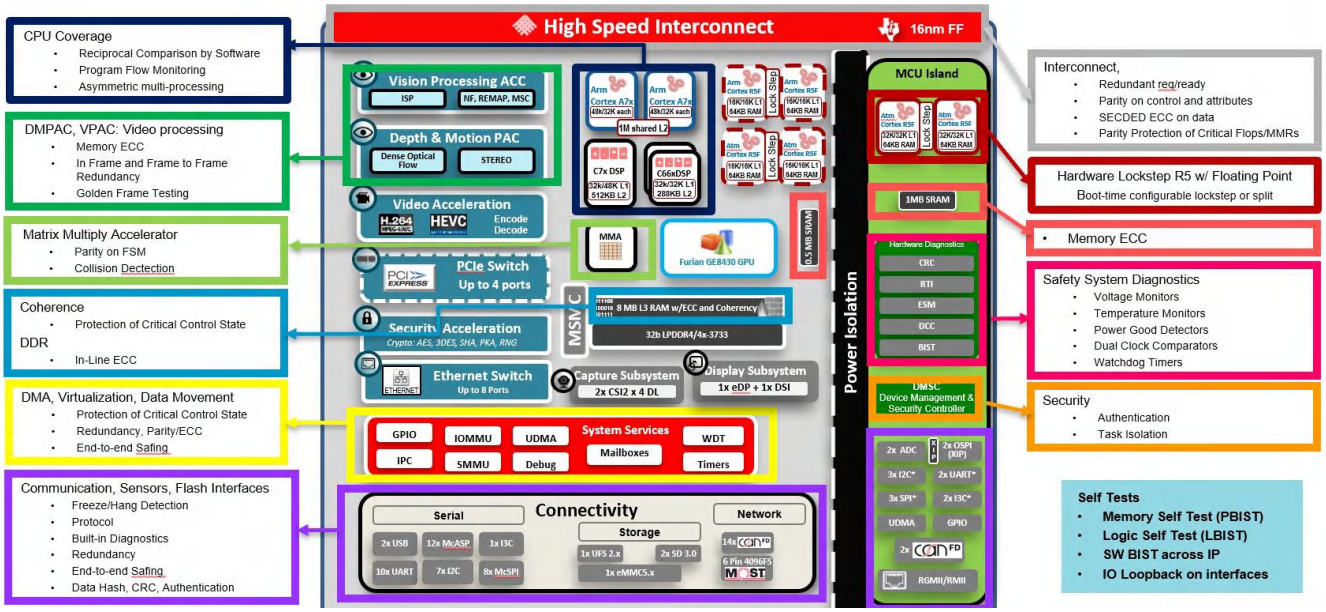


图 2. 选择 TDA4VM 的诊断功能

图 2 显示了可以在 SoC（基于 TDA4VM）中实施的部分安全机制。此图仅供参考，并不包含所有内容。请参阅 SoC 专用安全参考手册，以深入了解诊断以及 SOC 特定模块和外设。

3 系统中的安全实现

3.1 硬件配套资料

TI 提供了全面的配套资料和交付产品，助力实现安全支持，协助认证作为系统中独立安全元素 (SEooC) 的 SoC。

- **器件安全手册**：产品安全架构和建议用法的详细说明。在系统设计过程中使用
- **安全分析报告**：基于 IEC 61508 和/或 ISO 26262 对器件等级的 FIT 率和诊断覆盖率汇总。
- **FMEDA（失效模式影响和诊断分析）**：FMEDA 是一类完全可定制的文档，用于确保安全用例满足客户在安全分析期间制定的目标指标和安全目标。在系统设计过程末期使用
- **评估证书**：IEC 61508 和/或 ISO 26262 合规性内容汇总。作为系统安全案例一部分

客户必须持有有效的安全 NDA，才能访问上述安全文档。此文档可通过 mysecuresw 获取，可在此申请访问。

3.2 软件支持

为助力客户的安全设计，TI 提供通过了 ASIL-D/SIL-3 安全评估的软件诊断库 (SDL)，涵盖系统级诊断和安全功能。SDL 是一组包含初始化/配置、自检、运行时和响应处理程序的 API 集合，支持各种安全机制。SDL 是一个完全自包含的库，不依赖于外部软件，可提供操作系统抽象层 (OSAL)，支持在操作系统和非操作系统（裸机）环境中实施。在提供 SDL 的同时，还提供合规性支持包 (CSP)，以支持客户在其系统上重新认证。

SDL 和 CSP 均可通过 mysecuresw 访问，也可在此申请访问。

表 2. SDL 和 CSP 交付产品汇总

SDL 支持的功能	CSP 交付产品
诊断：存储器 BIST、逻辑 BIST、ECC 和奇偶校验、ECC 聚合器、错误信令模块、R5F 锁步 (CCM) **安全功能：**时钟监测器、电压监测器、温度传感器、超时/隔离垫片、看门狗计时器、R5F MPU、PMU、VIM 和 RAT 支持	• 要求、测试计划和报告 • 可追溯性报告 • 动态代码覆盖分析报告 • 静态代码分析/MISRA-C 报告 • 包含安全手册的用户指南 • 软件 FMEA 报告

4 修订历史记录

注：以前版本的页码可能与当前版本的页码不同

日期	修订版本	注释
2022 年 8 月	*	初始发行版

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。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