利用Jacinto™ 7 处理器功能安全特性进行汽车设计

Jacinto™ 处理器工程经理
Yashwant Dutt

Jacinto 处理器功能安全经理
Sam Visalli

Jacinto 处理器
系统架构师
Mahmut Cifti

Jacinto 处理器汽车网关
和娱乐系统总经理
Dave Maples

嵌入式处理器质量经理
Krishna Gopalakrishnan

德州仪器 (TI)

简介

自动驾驶、互联汽车和电动汽车/混合动力电动汽车的出现正在改变汽车行业的范式。功能安全是这些技术的核心，并且功能安全不再局限于传统的微控制器 (MCU)，也需要在应用处理器中受到支持。发动机控制单元 (ECU) 计算需求不断增长，这推动了对用于满足应用需求、功能更强大的处理器、硬件加速器和数字信号处理器 (DSP) 的需求。考虑这些参数时，现有内核处理与安全相关的数据和托管混合关键性功能将变得更具挑战性。混合关键性系统在共享平台上运行具有不同关键性级别的任务。在混合关键性系统中，必须严格保证安全关键任务的时序。

用于汽车的 TI Jacinto™ 7 片上系统 (SoC) 系列不仅集成了隔离式 ASIL-D 安全 MCU，而且为所有处理内核提供了更高级别的 ASIL 功能安全特性。在本白皮书中，我们将回顾 Jacinto 7 SoC 系列中内置的安全诊断功能，其中包括 TDA4x 和 DRA8x 器件、可用于支持混合关键性系统的各种隔离机制、软件架构、软件产品以及如何构建完整的解决方案。

什么是功能安全？

功能安全是系统以最大程度减小损害的方式响应故障行为（无论是随机故障、硬件故障还是环境压力）的功能。根据 ISO 26262，这意味着可以避免不可接受的风险。尽管功能安全概念已经在汽车行业中存在了相当一段时间，但在应用处理器中却刚刚开始采用该概念。牢记符合 ASIL-D 标准的应用，Jacinto 7 处理器将曾经仅限于 MCU 级器件的安全概念引入到应用处理器中。这些处理器使用支持混合关键性系统的硬件辅助隔离技术。在一个器件上无缝托管安全关键型任务和非安全关键型任务的功能有助于降低系统成本。

Jacinto 7 处理器系列提供了涉及硬件和软件的全面安全解决方案。该处理器系列使用经独立功能安全评估机构（如 TÜV SÜD）认证的硬件开发流程针对 ASIL-D 功能进行了系统设计。该处理器系列具有能够检测随机故障的诊断电路，这些诊断电路可以分为三大类：

基本诊断，涵盖存储器、时钟、电源、内核和互联的测试电路。

硬件隔离功能，如独立的电压/电源/复位、 防火墙、存储器管理单元 (MMU) 和微处理器 (MPU)，可简化支持混合关键性操作的系统中的防止干扰 (FFI)（例如：ASIL-B 和 ASIL-D)。

特定于应用的硬件诊断，如冻结帧检测。

Jacinto 7 处理器系列还将在满足目标终端设备所需的 ASIL 级别的背景下在外部认证为系统元件。与硬件开发流程类似，软件开发流程也通过了独立功能安全评估机构（如 TÜV SÜD）的认证。具有安全要求的 Jacinto 7 软件组件可满足高达 ASIL-D 的功能安全要求。软件组件未经外部认证。利用认证支持包，可以对最终软件/系统进行认证。提供了软件诊断库以及片上诊断使用示例。TI 为兼容的硬件和软件提供了功能安全认证。

Jacinto 7 处理器安全架构的一个主要不同之处在于集成了 MCU 功能，这简化了系统设计，减少了板上的组件数量并缩减了空间。应用处理器分为两个独立的域：主域和 MCU 域。主域提供高性能计算内核，如 MPU 和图形处理单元 (GPU)、多媒体和视觉硬件加速器（包括 DSP）以及必要的外设。MCU 域是具有高 FFI、用于实现安全功能的独立域。

Jacinto 7 处理器是符合安全要求的器件，附带功能安全文档，其中包括：

安全手册，其中提供的信息可帮助您使用受支持的 Jacinto 7 处理器系列创建安全关键型系统。该文档包含有关开发流程、功能安全架构和实现的功能安全机制的详细信息。

安全分析报告，其中包含有关器件达到规定的功能安全目标的能力的信息。

功能安全定量分析（也称为故障模式、影响和诊断分析 [FMEDA]）也是安全性分析报告的一部分，但它是单独的文档。该文档包含有关 适用于基于诊断功能安全机制定制应用进行 计算的组件不同部分的详细信息，并包含有关 FIT、诊断范围、SPFM/LFM 和故障模式的信息。

软件功能安全概述

软件是实现产品总体安全目标的重要元素。Jacinto 7 软件的安全性包括以下两个方面：

安全路径中使用的软件组件的系统功能。

对硬件诊断的全面软件支持和参考示例代码。

为了实现系统功能，TI 采用在其各个团队中使用的定义明确的通用软件开发流程和工具。一个独立的软件质量组织负责核准所有软件产品。TI 的整体功能安全可交付成果包括：

流程合规性：功能安全软件开发流程已通过 TÜV SÜD 的 ISO 26262 ASIL-D 和 IEC 61508 认证。

项目合规性：通过内部审查来确保项目合规性，并根据 ISO 26262 或 IEC 61508 流程执行。任何不合规情况都将通过改进计划和措施予以纠正。

支持客户认证：提供所有按照安全流程开发的软件以 及合规性支持套件 (CSP)。CSP 包含：

- TI 内部审查报告。
- 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/汽车工业软件可靠性联合会 C (MISRA-C)报告。
- 功能安全诊断库和手册。
- 编译器资质审核套件。
- 软件故障模式和影响分析报告。

统一的 Jacinto 7 软件开发套件 (SDK) 还提供使您能够构建安全解决方案的软件支持。根据 TI 的功能安全软件开发流程开发了应“按原样”在系统中使用且属于安全回路一部分的组件。该流程包括用于所有关键安全 IP 和功能软件（如微控制器抽象级驱动程序、IPC 和 DMA）的软件诊断库。

TI 还提供了各种参考示例，可帮助您了解如何在应用中使用这些安全功能。由于安全功能可能因应用而异，因此参考软件不是使用安全流程开发的，而是遵循 TI 基准流程。

表 1 显示了有关 SDK 中包含的诊断软件、功能软件和参考软件所提供内容的各种示例。

安全应用的部署

为数据中心和移动应用构建的典型 SoC 架构缺少汽车应用所必需的安全功能，从而需要额外的计算性

软件诊断	功能软件	参考软件
软件诊断库 (SDL) – 用于实现各种安全特性的软件功能和响应处理程序 •各 种模块的LBIST/PBIST •外设 viz CAN, SPI •安 全 IP：CRC, ECC, RTI, DCC, ESM •注入错误功能 •具有系统功能的软件	安全路径中的组件 – 使用系统功能构建的 SDK 组件 •AUTOSAR MCAL （CAN, DIO, SPI, ETH, IPC, ADC, PWM, WDG, GPT） •ECC, CRC, DCC, ESM, BIST, VTM, PGD, POK, ADC 等安全 IP 的 CSL-FL •SCI 客户端、DMA •SYSFW 固件 •TI-RTOS •安全路径中所有 IP 的 CSL-FL •MMA,TIDL 库 •CSI2, VHWA, IPC 的 LLD •编译器资质审核套件	•FI, Main/MCU Island隔离和其他安全特性的示例代码 •说 明使用案例环境中的安全 IP 用法的参考软件 •说 明安全手册中列出的诊断的参考软件
功能安全软件开发流程 软件合规性支持包 (CSP)		标准软件开发流程

表 1.软件功能安全产品。

能来添加基于软件的安全诊断。Jacinto 7 处理器系列的各种硬件和软件安全功能在最终应用中使用时有助于降低对计算性能的需求。

图 1 说明了一个典型的基于视觉的系统。通过摄像头串行接口捕获输入摄像头数据，然后将其发送到视觉处理硬件引擎，以便从原始数据转换为 YUV 数据。在处理器的片上 C7x DSP、MMA 和 Arm® Cortex®-A72 内核上运行各种分析和深度学习算法，如物体分类和可用空间检测。MCU 域充当每个步骤的检查器，定期验证和监视正在处理的数据。MCU 域还根据其他传感器输入来最终确定安全功能，然后通过控制器局域网 (CAN) 等通信协议将其传送到其他汽车 ECU。

图 1 中的每个块都是 Jacinto 7 处理器中的模块，包括硬件诊断，可在不使用 CPU 资源的情况下达到总体安全目标。表 2 对应了先前提到的同一视觉应用，并显示了 Jacinto 7 处理器系列与典型 SoC 之间在功能安全方面的差异。

与 Jacinto 处理器兼容的电源管理解决方案

TI 在开发 Jacinto 处理器系列的同时开发了两款灵活的高精度电源管理集成电路 (PMIC)，这两款

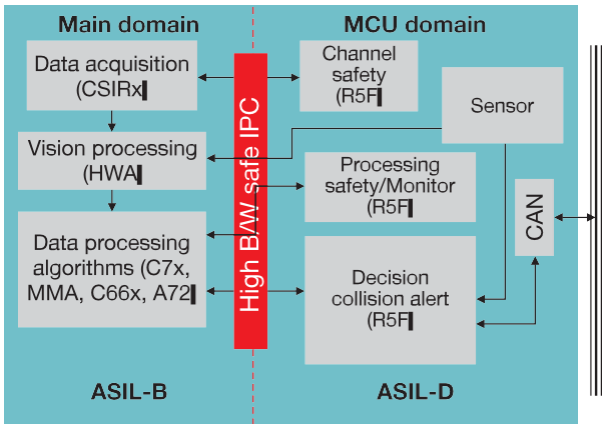

图 1. 典型视觉处理。

电路适用于需要功能安全的汽车应用且随附了功能安全文档。这些 PMIC（TPS6594-Q1 和 LP8764-Q1 PMIC）为主域和 MCU 域提供了可扩展的电源管理解决方案，并支持高达 ASIL-D 的功能安全。

正确设计的系统可满足各种功能安全要求，包括：

SoC 检查传感器数据

MCU 检查 SoC

MCU 控制传动器

MCU 检查传动器是否以预期方式对控制做出反应

安全域	特性	典型汽车系统	Jacinto 7 处理器系列优势
•架构	•集成 MCU Island •异构安全内核	•使用外部 MCU •使用虚拟化管理器和外部 MCU；虚拟化需要额外的 CPU 负载	•降低系统成本 •可对安全性能进行扩展 •无需虚拟化即可实现失效防护和恢复
•基础安全 •瞬态和永久故障	•内核、存储器和硬件加速器的内置自检 •存储器的错误校正码 •锁步 DMIPS •CRC、看门狗、时钟比较器 •互联安全	•通常在应用处理器中不可用 •针对软件诊断在所有内核上产生额外的负载	•在硬件中都可用 •产生的额外 CPU 负载可忽略不计
•隔离 •FFI	•MU、MPU、防火墙、超时垫圈	•虚拟化管理器 – 基于软件的方法 – 会带来处理内核占用率 •针对软件诊断在所有内核上产生额外的负载	•在安全任务和非安全任务之间进行硬件隔离 •产生的额外 CPU 负载可忽略不计
•应用安全特性	•黑帧 •冻结帧 •摄像头遮挡 •深度学习网络参数安全	•基于软件的方法 – 会带来处理内核占用率 •针对软件诊断在所有内核上产生额外的负载	•冻结帧监视器：硬件辅助冻结帧检测。无 CPU 负载 •基于硬件 CRC 的深度学习网络安全。无额外的 CPU 负载

表 2. 到应用的安全映射。

PMIC 监视 MCU 硬件和软件执行

PMIC 监视应用处理器硬件运行

如果 PMIC 检测到错误操作，那么它会强制将 ENDRV 输出引脚置为低电平，从而使系统处于安全状态。错误示例包括：

MCU 或 SoC 电源电压故障

PMIC 输入电源电压故障

MCU 软件或硬件错误

SoC 的 ESM 报告的 SoC 硬件错误

TPS6594-Q1 和 LP8764-Q1 器件可用作独立的 PMIC，但是在将多个 PMIC 一起用于实现处理器或 MCU 的可扩展性的系统中，PMIC 通过带有 CRC 协议的两线制接口相互通信。可以通过该接口在各个 PMIC 之间同步电源状态和错误处理。总线定期轮询会检查通信总线上所有 PMIC 的运行状况。该实现可确保对系统故障情况的快速响应，因此使该解决方案能够实现更高的终端系统功能安全目标。图 2 说明了两个 PMIC 之间的一个示例连接以及一个Jacinto 7 处理器系统使用案例。大多数应用将使用一个 TPS6594-Q1，但使用一个额外的 LP8764-Q1 将支持更多的系统功能和更高的性能。这种使用一个或多个 PMIC 通过一个“虚拟”PMIC 为 SoC 供电的功能可以在需要较低功耗的使用案例中优化系统成本，同时还可以实现性能最高的系统。

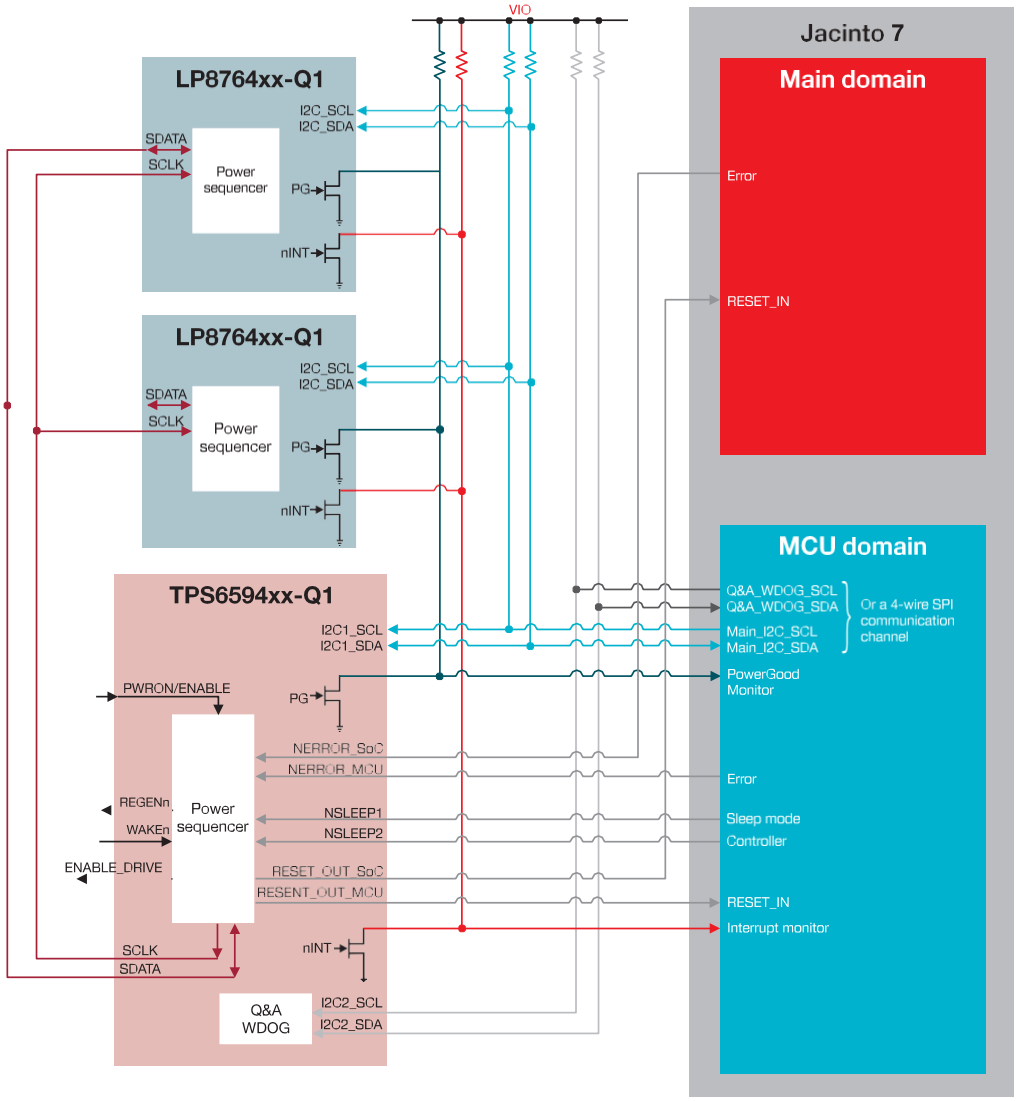

图 2.作为“虚拟”PMIC 的 TPS6594-Q1 + LP8764-Q1 + LP8764-Q1 通信

结论

TI 的新 Jacinto 7 处理器系列具有片上集成功能安全特性，使客户能够更好地实现其安全认证和最终产品目标。丰富的安全功能有助于降低系统BOM，并且可以节省各个内核的性能开销。此外，TI的软件SDK提供了与安全相关的驱动程序和诊断库，以帮助客户实现其安全软件开发目标。简化的安全架构和软件产品可帮助客户节省大量的工程开发工作。

其他资源

VC Kumar。“工业 4.0 中的功能安全状态”。德州仪器 (TI) 白皮书 SPRY329，2018 年。

Thomas、Jay 和 Siddharth Deshpande。“用于功能安全的基础软件”。德州仪器 (TI) 白皮书 SPNY007，2015 年。

功能安全硬件认证。

功能安全软件认证。

Chitnis, Kedar, et al.“Enabling Functional Safety ASIL Compliance for Autonomous Driving Software Systems.”Electronic Imaging, Autonomous Vehicles and Machines 2017, Society for Imaging Science and Technology (Jan. 29, 2017), pp. 35 - 40.

Haworth, David, Tobias Jordan and Alexander Much.“Freedom from Interference from AUTOSAR-Based ECUs: A Partitioned AUTOSAR Stack.”Automotive - Safety & Security, LNI 210 (2012), pp. 85 - 98.

重要声明和免责声明

TI 均以“原样”提供技术性及可靠性数据（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，不保证其中不含任何瑕疵，且不做任何明示或暗示的担保，包括但不限于对适销性、适合某特定用途或不侵犯任何第三方知识产权的暗示担保。

所述资源可供专业开发人员应用TI 产品进行设计使用。您将对以下行为独自承担全部责任：(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、安保或其他要求。所述资源如有变更，恕不另行通知。TI 对您使用所述资源的授权仅限于开发资源所涉及TI 产品的相关应用。除此之外不得复制或展示所述资源，也不提供其它TI或任何第三方的知识产权授权许可。如因使用所述资源而产生任何索赔、赔偿、成本、损失及债务等，TI对此概不负责，并且您须赔偿由此对TI 及其代表造成的损害。

TI 所提供产品均受TI 的销售条款 (http://www.ti.com.cn/zh-cn/legal/termsofsale.html) 以及ti.com.cn上或随附TI产品提供的其他可适用条款的约束。TI提供所述资源并不扩展或以其他方式更改TI 针对TI 产品所发布的可适用的担保范围或担保免责声明。

邮寄地址：上海市浦东新区世纪大道 1568 号中建大厦 32 楼，邮政编码：200122