運用 Jacinto™ 7 處理器的汽車設計功能安全特性

Yashwant Dutt
Jacinto™ 處理器
工程經理

Sam Visalli
Jacinto™ 處理器
功能安全經理

Mahmut Cifti
Jacinto 處理器
系統架構師

Dave Maples
Jacinto 處理器
汽車閘道與資訊娛樂
總經理

Krishna Gopalakrishnan
嵌入式處理
品質經理

德州儀器

介紹

自動駕駛、連線汽車和電動車輛/混合動力電動車的發展改變了汽車產業典範。這些技術的核心是功能安全，雖不受傳統微控制器 (MCU) 限制，但也需要應用處理器支援。引擎控制單元 (ECU) 的運算要求不斷增加，因而需要功能更強大的處理器、硬體加速器與數位信號處理器 (DSP)，才能滿足應用需求。在考慮這些參數時，現有核心處理安全相關資料與主機混合關鍵性功能也變得更具挑戰性。混合關鍵系統會在共用平台上執行各種關鍵等級的任務。在混合關鍵系統中，必須嚴格確保重要安全任務的時序。

TI Jacinto™ 7 汽車晶片系統 (SoC) 系列不僅整合獨立 ASIL-D 安全 MCU，也為所有處理核心提供更高階 ASIL 功能安全。我們將在本白皮書中回顧 Jacinto 7 SoC 系列內建安全診斷功能，包含 TDA4x 和 DRA8x 裝置、各種支援混合關鍵系統的可用隔離機制、軟體架構、軟體產品方案，以及完整解決方案的建構方式。

何謂功能安全？

功能安全是以降低損害方式，反應隨機故障、硬體故障或環境應力等故障行為的系統功能。根據 ISO 26262，即代表免受不可接受風險的影響。雖然功能安全概念在汽車產業已行之有年，但在應用處理器上的運用仍處於萌芽階段。Jacinto 7 處理器延續採用 ASIL-D 相容應用，並將僅適用 MCU 級裝置的安全概念引入應用處理器。這類處理器運用硬體輔助隔離技術，來實現混合關鍵系統。在單一裝置上搭載重要安全和非重要安全任務的功能，有助於減少系統成本。

Jacinto 7 處理器系列提供完整硬體與軟體安全解決方案。運用 TÜV SÜD 等獨立功能安全評估機構認證的硬體開發程序，以系統方式專為 ASIL-D 功能設計。此外也具備偵測隨機故障的診斷電路，並可分為三種廣泛類別：

- 基本診斷，包含記憶體、時脈、功率、核心與互連的測試電路。
- 獨立電壓/電源/重設、防火牆、記憶體管理單元 (MMU) 與微處理器 (MPU) 等硬體隔離功能，可簡化系統中支援混合關鍵運作的免受干擾 (FFI) (例如：ASIL-B 和 ASIL-D)。
- 應用特定硬體診斷，例如凍結畫面偵測。

Jacinto 7 處理器系列通過外部認證，為目標終端設備的 ASIL 等級獨立系統要素。與硬體開發程序相同，軟體開發程序也通過 TÜV SÜD 等獨立功能安全評估機構認證。具安全要求的 Jacinto 7 軟體元件專為支援最高 ASIL-D 功能安全要求而設計。軟體元件未經過外部認證。認證支援套件讓您可進行最終軟體/系統驗證。軟體診斷程式庫隨附晶片診斷使用範例。TI 也為硬體和軟體提供功能安全認證。

Jacinto 7 處理器的重要安全架構差異之一，是整合 MCU 功能簡化系統設計、降低電路板元件數量並減少佔用空間。應用處理器可分為兩種獨立網域：主要網域與 MCU 網域。主要網域可提供高性能運算核心，例如 MPU 和圖形處理單元 (GPU)、多媒體、DSP 等視覺硬體加速器及必要周邊設備。MCU 網域是具備高 FFI 的安全功能獨立網域。

Jacinto 7 處理器為安全相容裝置，隨附的功能安全文件包括：

- 安全手冊，提供資訊幫助您以支援的 Jacinto 7 處理器系列建立重要安全系統。本文件內含開發程序、功能安全架構與執行功能安全機制等詳細資訊。
- 安全分析報告包含裝置達成所述功能安全目標的相關功能資訊。
- 量化功能安全分析 (又稱為故障模式、影響與診斷分析 [FMEDA]) 也是安全分析報告的內容之一，但為單獨文件。其中包含元件各部分資

訊，適合以診斷功能安全機制自訂應用為基礎的運算，例如 FIT、診斷範圍、SPFM/LFM 與故障模式等資訊。

軟體功能安全概覽

軟體是達成產品整體安全目標的重要元素。Jacinto 7 軟體安全包含以下兩個層面：

- 安全路徑使用的軟體元件系統功能。
- 對硬體診斷的全方位軟體支援及參考範例程式碼。

在系統化功能方面，TI 於各團隊中使用定義完整的通用軟體開發程序和工具。另外由獨立軟體品質組織負責核准所有軟體產品。TI 提供的整體功能安全包含：

- 程序合規性：功能安全軟體開發程序經過 TÜV SÜD 認證，採用 ASIL-D 與 IEC 61508 的 ISO 26262。
- 專案合規性：依 ISO 26262 或 IEC 61508 程序透過內部稽核確保專案合規性。任何不符合情況都將以改善計畫與行動加以修正。
- 客戶可進行認證：所有依照使用安全程序開發的軟體皆提供 Compliance Support Package (CSP)。CSP 包含：
  - TI 內部稽核報告。
  - 相關要求、測試計畫與報告。
  - 追蹤報告。
  - 動態程式碼範圍分析報告。
  - 靜態程式碼分析/汽車工業軟體可靠性協會 C 報告。
  - 功能安全診斷資料庫與手冊。
  - 編譯器資格套件。
  - 軟體故障模式與影響分析報告。

整合 Jacinto 7 軟體開發套件 (SDK) 也提供軟體支援，幫助您建置自己的安全解決方案。在系統中「按原樣」使用和屬於安全循環的元件，會依 TI 功能安全軟體開發程序進行開發。程序包含微控制器抽象層驅動器、IPC 與 DMA 等所有重要安全 IP 與功能軟體之軟體診斷資料庫。

TI 也提供各種參考範例，幫助您了解如何在應用中使用這些安全功能。各應用的安全功能各有不同，參考軟體並非利用安全程序來進行開發，而是採用 TI 基準程序。

表 1 說明 SDK 中診斷軟體、功能軟體與參考軟體提供內容的各種範例。

安全應用對應

資料中心與行動應用的傳統 SoC 架構缺乏汽車應用所需安全功能，必須具備額外運算性能才能增加軟體安全診斷。在終端應用中使用 Jacinto 7 處理器系列各種硬體與軟體安全功能時，可幫助減少對運算性能的需求。

軟體診斷	功能軟體	參考軟體
軟體診斷資料庫 (SDL)—各種安全特性之軟體功能與反應處理程式 • 各模組的 LBIST / PBIST • 周邊 (CAN, SPI) • 安全 IP：CRC, ECC, RTI, DCC, ESM • 注入錯誤功能 • 具系統功能的軟體	安全路徑中的元件—具系統功能的 SDK 元件 • AUTOSAR MCAL (CAN, DIO, SPI, ETH, IPC, ADC, PWM, WDG, GPT) • 安全 IP 的 CSL-FL, 例如 ECC, CRC, DCC, ESM, BIST, VTM, PGD, POK, ADC • SCI 用戶端，DMA • SYSFW 韌體 • TI-RTOS • 安全路境中所有 IP 的 CSL-FL • MMA, TIDL 資料庫 • CSI2, VHWA, IPC 的 LLD • 編譯器資格套件	• FFI, 主要/MCU 獨立單元隔離範例程式碼與其他安全特性 • 參考軟體展示使用案例內容中的安全 IP 使用 • 參考軟體展示安全手冊中所列診斷
功能安全軟體開發程序 Software Compliance Support Package (CSP)		標準軟體開發程序

表 1。軟體功能安全產品。

圖 1 說明典型視覺系統。輸入攝影機資料會自攝影機序列介面擷取，之後傳送到視覺處理硬體引擎，由原始格式轉為 YUV。處理器晶片 C7x DSP、MMA 和 Arm® Cortex®A72 核心會執行物體分類與閒置空間偵測等各種分析與深度學習演算法。MCU 網域會在各步驟中扮演檢查器的角色，並定期驗證和監控處理資料。MCU 網域也會採用安全功能根據其他感測器輸入所做的最終決定，透過控制器區域網路 (CAN) 等通訊協定與其他汽車 ECU 進行通訊。

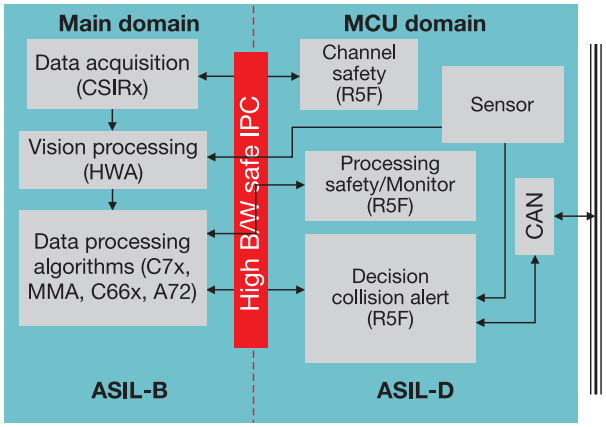

圖 1。傳統視覺處理。

圖 1 中每個區塊都是 Jacinto 7 處理器的模組，並包含硬體診斷，不需 CPU 資源即可滿足整體安全目標。表 2 則對應先前提到的視覺應用，並說明 Jacinto 7 處理器系列與傳統 SoC 的功能安全差異。

與 Jacinto 處理器相容的電源管理解決方案

除了 Jacinto 處理器系列外，TI 也開發了兩種具高準確性的靈活電源管理積體電路 (PMIC)，適合需功能安全的汽車應用，並提供功能安全相關文件。PMIC、TPS6594-Q1 和 LP8764-Q1 PMIC 為主要網域和 MCU 網域提供可擴充電源管理解決方案，最高可支援 ASIL-D 功能安全。

適當建構的系統支援功能安全要求，其中包含：

- SoC 檢查感測器資料
- MCU 檢查 SoC
- MCU 控制致動器
- MCU 檢查致動器是否以預期方式對控制進行反應
- PMIC 監控 MCU 硬體和軟體執行
- PMIC 監控應用處理器硬體操作

若 PMIC 偵測到錯誤操作，便會強制 ENDRV 輸出接腳 low 讓系統進入安全狀態。錯誤範例包括：

- 供應 MCU 或 SoC 電壓時發生故障
- 輸入供應電壓至 PMIC 時發生故障

安全網域	特點	傳統汽車系統	Jacinto 7 處理器系列優點
• 架構	• 整合 MCU 獨立單元 • 異質安全核心	• 使用外部 MCU • 使用虛擬機器監控器與外部 MCU，虛擬機器監控器需額外 CPU 負載	• 系統成本最佳化 • 可擴充安全性能 • 無虛擬機器監控器之故障安全與復原
• 基礎安全 • 暫態與永久故障	• 內建核心、記憶體與硬體加速器自我測試 • 記憶體錯誤修正程式碼 • Lockstep DMIPS • CRC、看門狗、時脈比較器 • 互連安全	• 應用處理器通常不提供 • 所有核心需額外負載以進行軟體診斷	• 在硬體中可用 • 額外 CPU 負載微乎其微
• 隔離 • FFI	• MMU、MPU、防火牆、逾時墊片	• 虛擬機器監控器 – 軟體方法 – 負載處理核心 • 所有核心需額外負載以進行軟體診斷	• 安全與非安全任務的硬體隔離 • 額外 CPU 負載微乎其微
• 應用安全特性	• 黑色畫面 • 凍結畫面 • 攝影機受阻 • 深度學習網路參數安全	• 軟體方法 – 負載處理核心 • 所有核心需額外負載以進行軟體診斷	• 凍結畫面監控器：硬體輔助凍結畫面偵測。無 CPU 負載 • 硬體 CRC 深度學習網路參數安全。無額外 CPU 負載

表 2。與應用之安全對應。

- MCU 軟體或硬體錯誤
- SoC 的 ESM 回報 SoC 硬體錯誤

TPS6594-Q1 與 LP8764-Q1 裝置可作為獨立 PMIC 使用，但需使用在採用多個 PMIC 的系統以便與處理器或 MCU 進行擴充，PMIC 間會透過 CRC 協定範圍內的雙線介面進行通訊。此介面可在 PMIC 間進行電源狀態同步與錯誤處理。匯流排定期輪詢會檢查通訊匯流排所有 PMIC 的健康狀態。此動作可確保對系統故障狀況的快速反應，進而提供解決方案以因應更高的終端系統功能安全目標。圖 2 說明兩個 PMIC 連線範例與 Jacinto 7 處理器系統使用案例。多數應用會採用一個 TPS6594-Q1，但使用額外 LP8764-Q1 可支援額外系統功能與更高性能。透過「虛擬」PMIC 以一個以上 PMIC 提供 SoC 電源的功能，可在需較少電源的使用案例中進行系統最佳化，並可提供最高性能系統。

結論

TI 的全新 Jacinto 7 處理器系列具備晶片整合功能安全特性，讓客戶能輕鬆達到安全認證與終端產品目標。各種安全特性有助於減少系統 BOM，並可降低各核心的性能負擔。此外，TI 的軟體 SDK 可提供安全相關驅動器和診斷資料庫，幫助客戶達成安全軟體開發目標。簡化安全架構和軟體功能有助客戶大幅減少工程開發心力。

其它資源

- Kumar, VC.「工業 4.0 功能安全狀態」。2018 德州儀器白皮書 SPRY329。
- Thomas、Jay 與 Siddharth Deshpande。「功能安全的基礎軟體」。2015 德州儀器白皮書 SPNY007。
- 功能安全硬體認證。
- 功能安全軟體認證。
- Chitnis、Kedar 等人。「實現自動駕駛軟體系統功能安全 ASIL 合規性。」Electronic Imaging, Autonomous Vehicles and Machines 2017, Society for Imaging Science and

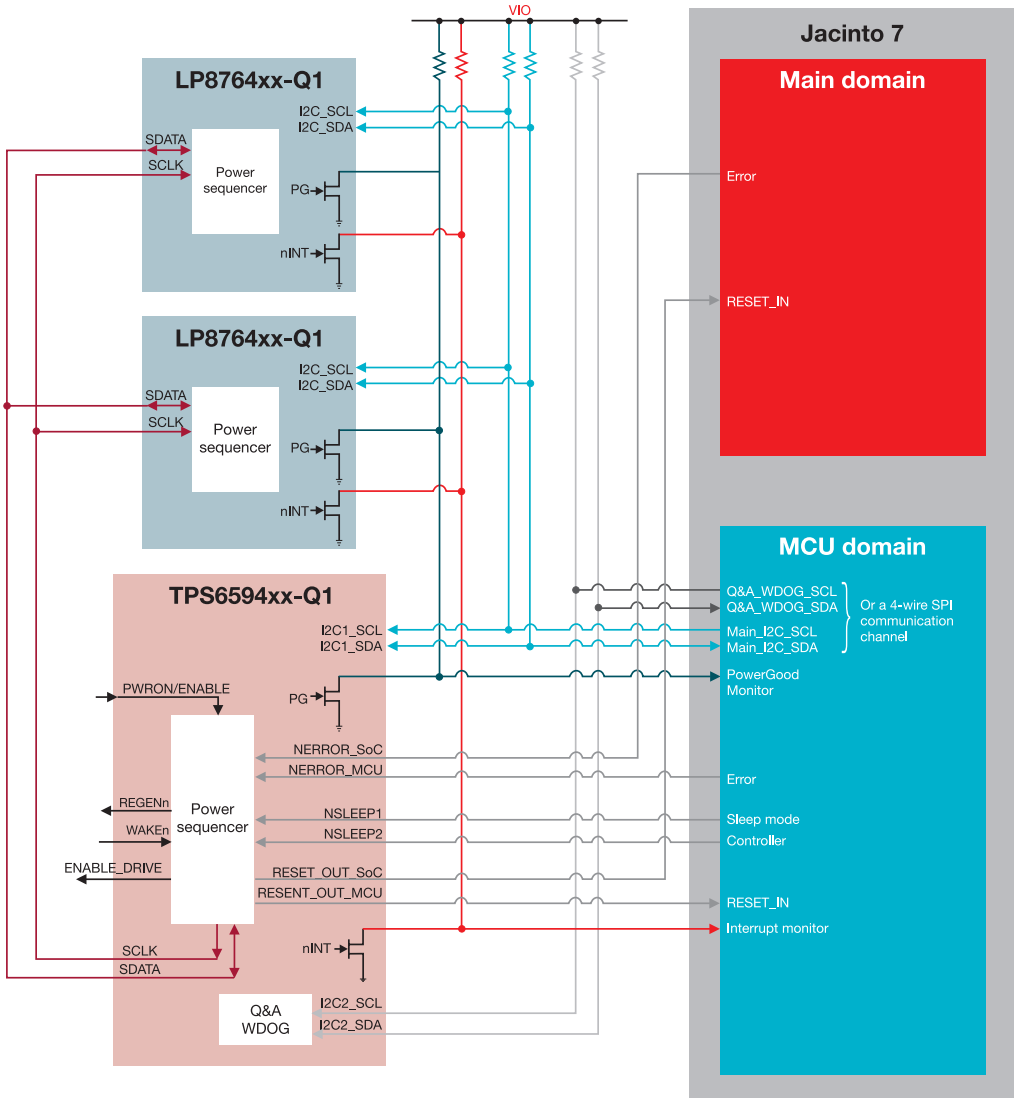

圖 2。TPS6594-Q1 + LP8764-Q1 + LP8764-Q1 通訊為「虛擬」PMIC

Technology (2017 年 1 月 29 日), pp. 35 – 40.

- Haworth、David、Tobias Jordan 與 Alexander Much。 「從基於AUTOSAR 的 ECU中免受干擾：分區的AUTOSAR堆棧」Automotive – Safety & Security, LNI 210 (2012), pp. 85 – 98.

IMPORTANT NOTICE AND DISCLAIMER

TI PROVIDES TECHNICAL AND RELIABILITY DATA (INCLUDING DATASHEETS), DESIGN RESOURCES (INCLUDING REFERENCE DESIGNS), APPLICATION OR OTHER DESIGN ADVICE, WEB TOOLS, SAFETY INFORMATION, AND OTHER RESOURCES “AS IS” AND WITH ALL FAULTS, AND DISCLAIMS ALL WARRANTIES, EXPRESS AND IMPLIED, INCLUDING WITHOUT LIMITATION ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT OF THIRD PARTY INTELLECTUAL PROPERTY RIGHTS.

These resources are intended for skilled developers designing with TI products. You are solely responsible for (1) selecting the appropriate TI products for your application, (2) designing, validating and testing your application, and (3) ensuring your application meets applicable standards, and any other safety, security, or other requirements. These resources are subject to change without notice. TI grants you permission to use these resources only for development of an application that uses the TI products described in the resource. Other reproduction and display of these resources is prohibited. No license is granted to any other TI intellectual property right or to any third party intellectual property right. TI disclaims responsibility for, and you will fully indemnify TI and its representatives against, any claims, damages, costs, losses, and liabilities arising out of your use of these resources.

TI’s products are provided subject to TI’s Terms of Sale (www.ti.com/legal/termsofsale.html) or other applicable terms available either on ti.com or provided in conjunction with such TI products. TI’s provision of these resources does not expand or otherwise alter TI’s applicable warranties or warranty disclaimers for TI products.

Mailing Address: Texas Instruments, Post Office Box 655303, Dallas, Texas 75265