簡化汽車及工業領域的功能安全認證

Miro Adzan
總經理
工業系統
工廠自動化與控制
德州儀器

Arun Vemuri
總經理
汽車系統
車身電子元件與照明
德州儀器

功能安全設計需縝密考量、紀錄和時間才能獲得最佳結果。不管您是爲工廠或高速公路進行設計，本白皮書將說明 **TI** 設計積體電路 **(IC)** 的方式將如何提供您所需資源，以簡化您的功能安全設計。

自動化使得工業與汽車領域對功能安全的需求提高。工業應用普遍要求功能安全，特別是在工廠自動化與控制系統。

在汽車產業中，安全氣囊與煞車系統已納入功能安全多年，提升電氣化和自動駕駛功能需要能控制電池管理、感測器融合與汽車操控的系統，也因此增加設計對功能安全的需求。

不管是爲工廠、居家設備還是明日車輛設計機器人系統，設計工程師越來越需要提供能符合應用相關功能安全標準的專案。

在不需符合標準的應用中，設計安全系統已成爲從競爭對手中脫穎而出的重要因素。

功能安全標準

功能安全是系統整體安全的一部份，並需以預期方式對特定輸入或故障狀態進行反應。功能安全標準接受危害永遠存在，因此所有系統都有其固有的故障率。

功能安全標準闡明如何透過將風險降至可忍受程度的方式，來進行系統開發。含功能安全的系統設計不僅需降低不當操作造成的風險，也需偵測故障並將影響降到最低。

爲了滿足功能安全合規性，工程師必須：

- 預測並定義危險狀況。
- 判斷可處理這些狀況的安全功能。
- 評估安全功能可達到之風險降低。
- 確保安全功能依設計原意執行。

由相關產業企業參與之標準組織會定義功能安全標準，透過幫助定義系統中安全功能，並設定評估和評等安全程度的規範，爲設計人員提供指引。德州儀器 (TI) 積極參與標準組織，可幫助確保企業在開發產品初期，就將功能安全納入考量。

常用安全標準包含適用工業運用的國際電工技術委員會 (IEC) 61508、適用汽車應用的國際標準化組織 (ISO) 26262，以及適用居家設備的 IEC 60730。

安全標準的共同點是有風險降低與安全完整性等級 (SIL)。舉例來說，根據 IEC 61508 的定義，SIL 的範圍從 SIL 1 到 SIL 4，SIL 4 最爲嚴格。SIL 1 需要 90% 到 99% 的安全可用性，0.1 到 0.01 平均失效機率 (PFDavg) 及 10 到 100 風險降低因素 (RRF)。SIL 4 則要求 >99.99% 安全可用性、0.0001 至 0.00001 PFDavg，以及 10,000 至 100,000 的 RRF。

ISO 26262 則有類似 SIL，範圍從 ASIL A 到 ASIL D，ASIL D 最爲嚴格。

功能安全程序

一般功能安全開發程序會從決定危害與功能安全目標開始。接著工程師常會開始檢視系統架構、模組和 IC。IC 便會成爲功能安全標準相符系統的主要基礎。

爲了預測系統行爲，工程師必須對模組操作進行量化與預測。爲了達到此目的，他們必須在開發過程

中針對系統進行結構定性安全分析，以辨識各種失效模式，其中包含原因與影響。

功能安全標準會定義工程師所需的 IC 資訊，讓他們也能執行自己的失效模式、影響和診斷分析 (FMEDA)。視 IC 複雜程度而定，系統安全分析需要設計、晶粒與封裝資訊。

選擇來自可靠供應商的適當產品是重要關鍵。不管是目標爲符合功能安全標準的設計，還是競爭激烈追求差異的安全系統，TI 都讓工程師能更輕鬆尋找並使用其產品。

以功能安全類別簡化裝置選擇

傳統工業與汽車應用需要大量且複雜程度不等的 IC，包括單一或多個感測器和致動器、微控制器 (MCU) 或處理器，以處理來自感測器、類比多工器、運算或儀器放大器、類比至數位轉換器 (ADC) 及數位至類比轉換器的資料，這些裝置可能會也可能不會與處理器、DC/DC 轉換器、低壓降穩壓器或電源管理 (PMIC)，以及 LED 驅動器、馬達驅動器、電磁閥驅動器、場效電晶體 (FET) 與隔離式閘極雙極電晶體閘極驅動器等不同驅動器元件，還有電源開關與負載開關進行整合。此外，應用也包含通訊界面，例如 RS-485、控制器區域網路 (CAN)、乙太網路、FPD-Link 和周邊元件連接Express (PCIe)。

表 **1** 說明適合功能安全設計的 TI 產品類別，也反應標準 IC 複雜性類別背後的邏輯。這些類別包括：TI 功能安全 (提供)、TI 功能安全品質 (管理) 和 TI 功能安全 (符合)。

功能安全 (符合) 產品

這些產品通常較爲複雜，可自成一個系統，例如 MCU 和處理器或類比馬達驅動器，並可整合安全功能。

TI 採用通過 Technischer Überwachungsverein (TÜV) SÜD 等機構認證之功能安全開發流程，來進行產品開發。此認證可幫助確保此類產品在開發時，遵循功能安全標準 ISO 26262 與 IEC 61508 所指定之規範。

例如以下複雜功能安全相符裝置：

- 通過國際汽車電子協會 (AEC)-100 認證且適合先進驅動器輔助系統的 **Jacinto™ TDAx** 晶片系統，可整合固定和浮點 TMS320C66x 數位訊號處理器 (DSP) 產生核心、Vision AccelerationPac

		功能 安全 (提供)	功能 安全品質 (管理)	功能 安全 (符合)
開發程序	TI 品質管理程序	✓	✓	✓
	TI 功能安全程序			✓
分析報告	功能安全 FIT 率計算	✓	✓	✓
	故障模式分配 (FMD) 和/或接腳 FMA**	✓	包含在 FMEDA 中	包含在 FMEDA 中
	FMEDA		✓	✓
	故障樹分析 (FTA)**			✓
診斷說明	功能安全手冊		✓	✓
認證	功能安全產品認證***			✓

表 ***1***。功能安全設計中的 *TI* 產品類別。

** 可能僅適用類比電元和訊號鏈產品。

*** 適用選擇產品。

嵌入式視覺引擎和雙 ARM® Cortex®-M4 處理器，以及適合低電壓差動訊號環景系統、顯示器、CAN 和 Gigabit 乙太網路語音視訊橋接等多攝影機介面的周邊裝置。這些裝置支援許多功能安全系統要求，包含錯誤修正程式碼 (ECC) 保護 M4、ECC 保護 32 位元雙資料速率介面、各中央處理單元 (CPU) 專屬記憶體管理單元、記憶體保護單元、溫度監控感測器以及供系統監控之八通道 ADC。

- TPS6594-Q1多軌電源管理積體電路(PMIC)支援汽車和工業市場採用的TI Jacinto TDAx 片上系統。高準確度及靈活的PMIC適合要求功能安全的汽車和工業應用，並會提供功能安全文檔。 TPS6594-Q1爲主域和MCU域提供可擴展的電源管理解決方案，並支持ASIL-D/SIL-3級別的功能安全。
- Hercules™ MCU 整合足夠安全與診斷功能，讓工程師可以 SIL 3 爲目標。這代表 MCU 可取得約 99% 故障範圍。舉例來說，在 MCU 上整合兩個 Cortex-R CPU lockstep 可比較各週期的輸出，在發生錯誤時，也可比較非屏蔽中斷的產生。CPU 自我測試可在工業應用啓動時或時間片段中執行。
- DRV3245E-Q1 是適合三相馬達驅動應用的 FET 閘極驅動器 IC。其中三個半橋式驅動器皆可驅動高低側 N 通道金屬氧化半導體 FET。此閘極驅動器專爲 ISO 26262 適用要求而設計，整合各內部區塊的診斷與保護，並支援通用系統診斷檢查，每個都可透過序列周邊介面進行實例化及通報。此功能彈性讓 DRV3245E-Q1 可流暢地整合在許多安全架構中。
- TPS65381A-Q1多軌PMIC採用雙核同步或鬆散耦合的體系結構，支援汽車和工業市場上的TI Hercules TMS570和C2000™ MCU系列產品。配備內部FET的異步降壓開關式電源轉換器可將輸入電源（電池）電壓轉換爲6-V前置調節器輸出電壓。然後由6-V的前置調節器爲其他調節器供電。它的監控和保護模塊，包括電壓檢測、模擬內建自測、時鐘丟失檢測、接點溫度檢測、電源電流限制和MCU誤差信號監測等，都能提高診斷覆蓋率並降低未檢測到的故障率。
- TI 在此類別中提供更多裝置，例如 C2000 即時控制器和 AWR1843 76-GHz 至 81-GHz 汽車雷達感測器，搭配車載 DSP、MCU 和雷達加速器。所有產品都隨附專屬功能安全相關文件，以支援系統開發程序：
  - 功能安全失效率 (FIT) 計算。
  - 故障模式分配 (FMD)。
  - FMEDA。
  - 故障樹分析。
  - 功能安全手冊說明 IC 安全功能，以及如何使用外部元件達成特定故障範圍與診斷。
  - 功能安全產品認證。

功能安全品質 (管理) 產品

第二個產品類別包含較爲複雜的產品，這些產品內部具有診斷功能，且特別爲了需功能安全的系統而設計。但此產品類別並未依符合功能安全產品類別所使用的認證功能安全開發流程進行開發，而是採用 TI 全公司標準品質管理開發流程。

此類別的產品包括但不限於：

- TCAN4550-Q1是業界首創的汽車系統基礎晶片（SBC），含整合式CAN FD控制器和收發器。這款高度整合的設備利用現有的SPI端口簡化CAN FD總線擴展，這樣設計師就可以在升級至更高寬帶CAN FD接口協議時維持當前基於微控制器的結構體系。
- LP87702-Q1是一款雙降壓和5-V升壓轉換器，符合ASIL的毫米波雷達系統要求的整合診斷功能，其中包括視窗監控器和一個監控其輸出電源的獨立參考電壓、以及兩個外部電源。

至於功能安全 (符合) 裝置，我們提供各種文件來幫助功能安全系統設計，其中包含功能安全 FIT 率計算、FMEDA 和功能安全手冊，但跟符合功能安全裝置不同的是，並不包含故障樹分析或產品認證。

功能安全 (提供) 產品

第三類產品包含以 TI 標準品質管理開發程序開發的簡單 IC，與功能安全品質管理產品類別相似。

提供功能安全產品通常不會整合安全功能，因此一般不具 TI 其他功能安全產品類別中裝置常見的內部監控和診斷功能。

由於產品沒有整合全方位的安全功能，因此不具其他類別中裝置常見的內部監控和診斷功能。

此類產品仍是功能安全系統的重要基礎，但 TI 因此爲設計人員提供功能安全 FIT 率與 FMD 等重要資訊，以運用在安全分析中。

此類別的產品包括但不限於：

- 業界超小型的線性熱敏電阻 **TMP61-Q1** 的長期感測器漂移 < 1%和精確度方面比傳統熱敏電阻更受歡迎。 我們的熱敏電阻替代方案 **TMP235-Q1** 是一款精密溫度感測器 IC、無需校準即可達到 ±1.5°C。
- **TPS3840-Q1** 電壓監控器和重設 IC。符合 AEC-Q100 裝置可在 1.5 V 至 10 V 廣泛電壓範圍中運作，一般供應電流僅 350 nA，最大供應電流則爲 700 nA。
- 符合 **TPS7A16A-Q1** AEC-Q100 的 60-V、5-µA 靜態電流 100-mA 低壓降電壓穩壓器專爲持續或偶發 (電源備援) 電池供電應用而設計，超低靜態電流爲其重點。此裝置非常適合從多芯解決方案產生低電壓供應，範圍可從高電池芯數電源工具套件至汽車應用。TPS7A16A-Q1 不僅可供應經過適當穩壓的電壓軌，也可在電壓暫態間耐受並維持穩壓。

TI 開發程序

由於功能安全開發的複雜性，您可能會需要 TÜV SÜD 認證以外更多資訊，以了解企業安全文化與程序。這也是 TI 爲系統化與隨機故障管理建立開發程序的原因 (請參閱表 **2**)。

我們所有產品皆遵循品質管理開發流程，以降低發生系統化故障的機率。此標準開發程序如下頁圖 **1** 所示，具備管理系統故障的許多必要因素。此外，您可使用這些產品的文件和報告，來協助符合各種終端應用標準，包含符合 ISO 26262-4 或 IEC 61508-2 的汽車與工業系統。

此程序將開發分爲以下階段：

- 評估。
- 計畫。
- 建立。
- 驗證。

評估	計畫	建立	驗證	永續與產品壽命終結
判斷是否需執行功能安全程序	定義元件目標 SIL/ASIL 能力	開發元件級功能安全要求	在 SILicon 中驗證功能安全設計	記錄任何通報問題 (視需要)
提名功能安全經理	產生功能安全計畫	在設計規格中包含功能安全要求	賦予功能安全設計特性	執行永續經營事件通報 (視需要)
階段結束稽核	驗證功能 安全案例	驗證設計規格	認證功能安全設計 (依 AEC-Q100)	更新工作產品 (視需要)
	啓動功能 安全案例	開始功能 安全設計	終結功能 安全案例	
	分析目標應用以產生系統級功能安全假設	執行設計定性分析 (即失效模式分析)	執行專案 評估	
	階段結束稽核	驗證定性分析	推出功能安全手冊	
		驗證功能安全設計	推出功能安全分析報告	
		執行設計定量分析 (即 FMEDA)	推出功能安全報告	
		驗證定量分析	階段結束稽核	
		視需要重設功能安全設計		
		階段結束稽核		

表 ***2***。在 *TI* 標準開發程序上重疊功能安全活動。

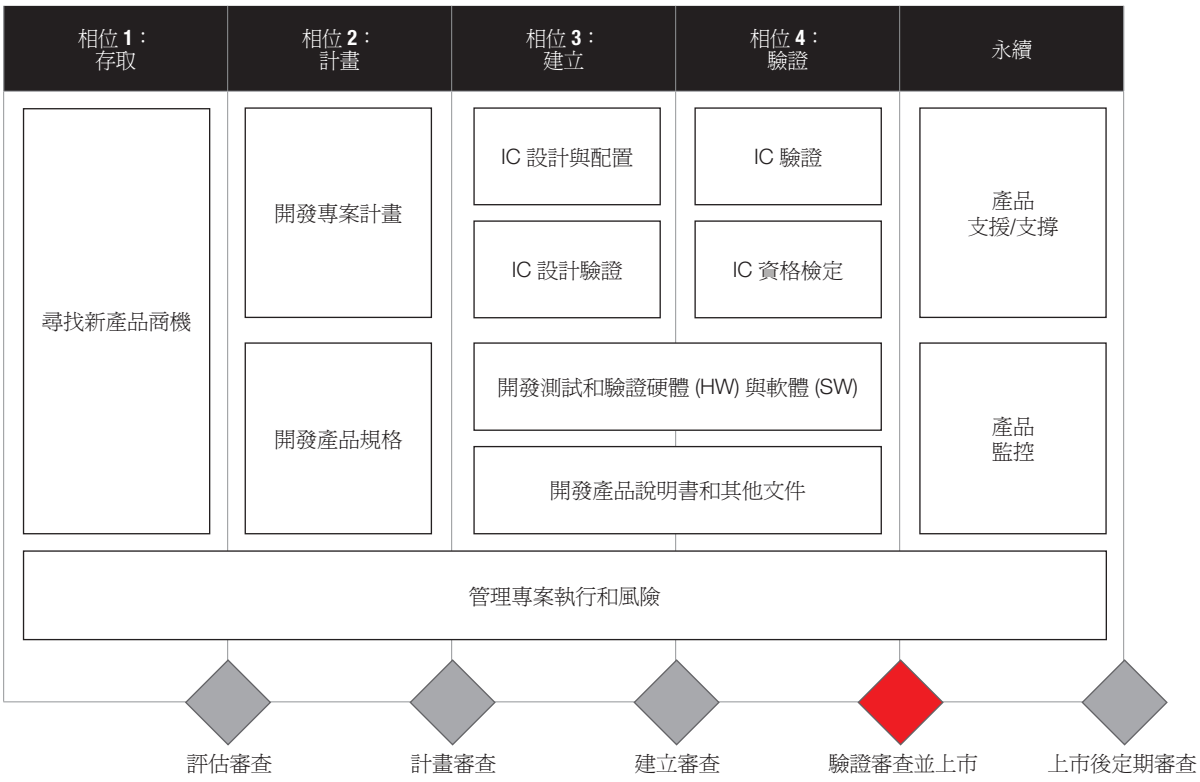

圖 ***1***。標準品質管理開發程序，其他功能安全活動可能會重疊。

TI 功能安全開發流程源自 ISO 26262 和 IEC 61508。我們爲每個標準新產品開發程序階段新增幾個功能安全特定活動，發展出三個標準 IC 複雜性類別。

如 ISO 26262-2:2018 附件 A 所述，TI 開發程序支援並鼓勵有效實現功能安全。開發程序鼓勵所有參與產品開發的團隊，彼此交換功能安全相關資訊。

TI 團隊遵守適當標準來維持組織功能安全規定，TI 程序則可確保解決發現的安全異常狀況。TI 透過遵循工業標準來維持支援功能安全的品質管理系統，爲客戶提供支援。

成長中的安全產品代表產品

功能安全設計中心從概念階段進行危害、失效與風險降低計畫。其中包含符合標準的系統失效分析，以及判斷執行診斷機制的有效性。內容主要與進入系統建置的每項產品資料有關。

TI 持續開發相關產品來幫助解決這樣的需求，並提供與產品相關的所有必要資料與文件，供客戶在功能安全應用中使用。

[了解 TI 功能安全技術]

更多資源

- 影片：[了解ADC的功能安全及系統級故障檢測]。
- 影片系列：[C2000™ MCUs的功能安全]。
- 白皮書：[電動汽車和自動駕駛汽車功能安全系統的執行器設計趨勢]。
- 白皮書：[利用Jacinto™ 7處理器功能安全特性的汽車設計]。
- 白皮書：[C2000™ MCU SafeTI™ 控制解決方案：ASIL分解和SIL合成簡介]。

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