參考

避免馬達控制設計流程中的功能安全合規性陷阱

Texas Instruments

Bharat Rajaram
Systems Engineering Manager
Arm-Based Microcontrollers

系統設計和功能安全合規性不應以序列方式執行。遺憾的是，傳統的設計方法 (以及許多組織) 將設計流程中的這些步驟視爲不同的孤立的活動，這通常會導致設計成本增加，並拖延上市時間。

摘要

1 **定義功能安全合規性**

功能安全標準的目標是管理和排除系統故障，同時也能偵測發生的隨機硬體故障，並防止其發生 (或至少呈現為安全的)。

2 **功能安全系統設計的兩個屬性**

功能安全涉及開發系統以提供所需功能，並且符合安全完整性等級。

3 **建議用於設計功能安全馬達控制與驅動系統的方法**

設計功能安全系統的系統工程師，應該在設計流程一開始就考慮功能安全合規性，而不是事後才考慮。

在設計功能安全馬達控制應用時，是否應一開始就將功能安全合規性視同初始設計規定來處理？或者，應該將功能安全視為附加功能，並納入設計的最終階段？

功能安全應該是初始設計需求的一部分，與馬達驅動的預期功能緊密結合。這不是常態，因爲傳統的系統設計工作流程無法在安全合規性部分呈現一致地。但是，如果一開始未思考好如何滿足安全完整性合規性，可能會導致系統上市時出現代價高昂的延誤情況。

工業 4.0 的發展以及車輛電氣化和連線能力的增長，都需要我們改變功能安全合規方式。簡單來說，現在更多應用領域中都具備更多馬達系統，以及須符合功能安全的高標準。

定義功能安全合規性

國際電子電機委員會 (IEC) 61508 和國際標準化組織 (ISO) 26262 等功能安全標準的目標是管理及排除系統性故障，同時也能偵測發生的隨機硬體故障，並防止其發生 (或至少呈現為安全的)。

採用獨立驗證和確認的嚴格開發流程，可協助管理系統性故障。

可以透過以下方式偵測、預防或呈現安全的隨機硬體故障：

- 對受控設備有透徹的了解。
- 分析可能的情況危害來源及其屬性，例如發生的可能、衝擊的嚴重性和事件的可控性。

安全機制與每種情況危害配對後，可幫助設計人員符合 IEC 61508 所要求的安全故障分數 (SFF) 和每小時故障機率 (PFH) 等量化指標。舉例來說，安全完整性等級 (SIL) 2 系統必須在 10 億個作業時數以上時間內擁有 SFF≥90% 與 ≤1000 故障的 PFH。

功能安全系統設計的兩個屬性

功能安全標準會假設所有系統都失敗 (不是萬一發生時，而是遲早都會發生)，也沒有零風險這回事。

功能安全系統設計的兩項屬性：一是開發提供所需功能的系統，再來是開發符合特定 SIL 或汽車 SIL (ASIL) 等安全功能的相同系統。

設計人員通常會以不同的或序列方式處理這兩個層面。爲大量應用設計功能安全的系統，同時還要維持設計預算要求，不啻是一項艱鉅的任務。**表 1** 概述控制與驅動應用中的預期功能與安全功能範例。

要更貼切地解說這個概念，請查看 **表 1** 中的電梯電機範例。

電梯的預期功能是根據使用者的輸入將人員上移和下移。如果按下按鈕到五樓，電梯應該會帶您到五樓。

電梯的安全功能可進一步提升，其中包括：

- 順利地將您從一個樓層帶到另一個樓層。
- 停在與每一層樓平台平行的位置。
- 如果電梯超過安全速度，就自動煞車。

功能安全應用	預期功能範例	安全功能範例 (及對應的 SIL 或 ASIL 目標)
工業：電梯馬達	根據使用者請求上下移動電梯	• 安全啓動或停止電梯 (避免猛然晃動) (SIL 2) • 如果電梯行進速度過快，則應使用自動煞車功能 (SIL 3)
汽車：電動車 (EV) 牽引馬達	根據駕駛員命令，透過加速器或煞車將電動車向前和向後移動	• 預防加速時扭矩不足或過大 (ASIL C) • 預防煞車過猛 (避免後車追撞) (ASIL D)
工業：鋼壓機	控制伺服驅動系統，使其在不降低工廠生產率的情況下操作鋼壓機	• 如果發生過扭矩或超速，安全扭矩關閉 (STO) 功能會將驅動控制器斷電 (SIL 3) • 安全限速 (SLS) 可在操作員關閉時保持馬達轉速在可接受的限制範圍內 (SIL 2) • 如果 SLS 超過界限檢查，則觸發 STO (在生產率和安全性之間取得平衡，以推動更高 SIL ，例如 SIL-3)

***表 1.** 控制和驅動應用中預期的安全功能範例。*

爲了更加了解預期功能和安全功能如何協同作業，假設 20 層樓的電梯具有按鈕電路 (請參見 **圖 1**) ，當發生故障時，電梯馬達控制器會將其解釋爲將電梯運送到 25 樓或 30 樓 (即 建築物中不存在的樓層)。邊界檢查會在故障導致錯誤或最終導致故障之前揪出故障。這是普遍認可的功能安全進展：「故障」會導致「錯誤」，而有些錯誤則會導致「故障」。

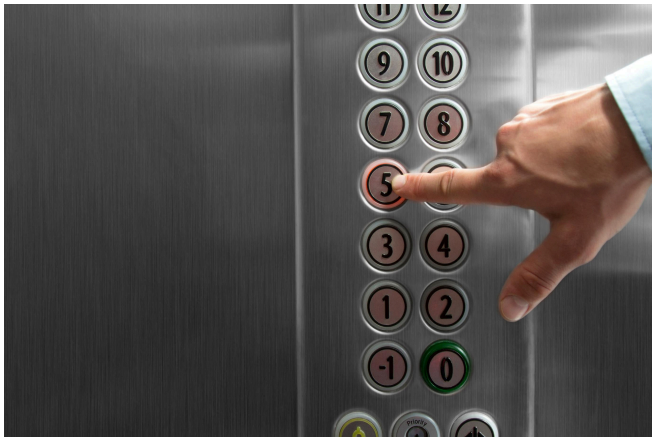

***圖 1.** 新型電梯按鈕範例。*

我們來回顧預期功能設計和安全功能設計的流程。

在馬達驅動器的預期功能設計流程中，系統工程師選擇符合預期功能需求的微控制器 (MCU)。隨後，他們會分配感測功能，例如整合式類比轉數位轉換器 (ADC) 通道，以監控轉子位置、線路電流、相位電壓及系統溫度。接著系統工程師會繼續利用 MCU 的可用處理功能，例如 CPU 每秒百萬指令數 (MIPS) 來執行馬達控制演算法，以及脈衝寬度調變器 (PWM) 等可用的驅動周邊設備來驅動馬達驅動電路。此流程通常需要花費數個月時間，其中包含設計印刷電路板 (PCB)、開發馬達控制演算法，以及開發和偵錯所有嵌入式軟體。

在有些組織中，若由不同的、甚至有點孤立的團隊負責處理安全功能設計流程，則會有另一位功能安全專家前來檢查系統工程師原本選擇的 MCU 功能安全手冊。在有些情況中，功能安全專家可能會發現獨立安全要素 (SEooC) 安全概念需要使用功能測試，其中包括錯誤測試、硬體備援、數位轉類比轉換器 (DAC) 至 ADC 回送檢查，或是透過強化擷取來監控強化型 PWM。回想一下先前的電梯範例，可能需要使用多個 ADC 通道來監控各樓層的位準感測器，以防止 MCU ADC 中發生「卡住」故障。

如果 ADC 和 PWM 通道不足，或 CPU MIPS 不足以達到功能安全之目的， 則可能需要回到製圖板，並選擇不同的

MCU 來實現功能安全的系統，這樣一來，可能會使該掉單獨系統設計團隊迄今完成的工作全部前功盡棄。

即使設計步驟不是依序連續進行，也經常發生在單獨的組織孤島中，也就是說，系統工程師一般不具備任何功能安全專業知識，而功能安全專家也不是系統工程師。這種孤立方法最終會導致同樣的問題：系統成本增加，以及延遲數個月的上市時間。

建議用於設計功能安全馬達控制與驅動系統的方法

系統工程師在設計功能安全系統時，其終極目標是在設計流程一開始就以符合功能安全合規性的方式進行。

要設計並提供符合設計預算的功能安全系統，需要對安全合規性和預期功能性進行協同分析。獨立或連續處理專案可能相當有挑戰性，甚至無法滿足系統設計目標。考量早期的範例與負責管理安全功能設計流程的團隊合作，先前的合作或許可以免除選擇新 MCU 並重新設定 PCB 的需求。

事實上，另一個範例可以說明建議的方法。人類大腦會同時運用其左腦 (邏輯性) 和右腦 (創造性) 來全面解決問題，如 **圖 2** 中所示。

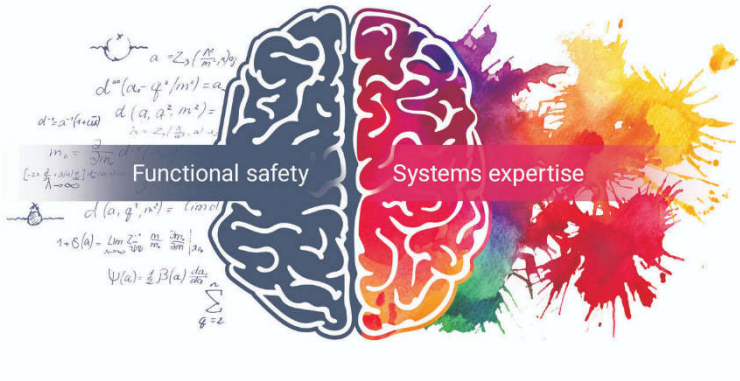

***圖 2.** 單一大腦統合了系統設計和功能安全合規這兩方面的專業知識。*

將大腦視爲一個單一的組織，每個組織代表一個不同的團隊或內部設計資源，能夠在設計流程中提出他們對特定專業的觀點。他們可以在設計工作流程中做爲一個單元來運作，用他們的專業素養來進行設計，同時保持清晰和持續的通訊。

同樣的，最有效的設計專案則使用由系統設計人員和功能安全專家組成的團隊，共同實現功能安全系統。

為了協助加快上市時間，系統工程師需要取得適當的設計資源。例如 TI 開發子系統和系統級功能安全概念，並交由第三方獨立評估。

TI 可以用何方式幫助您設計功能安全系統

TI 的產品組合範圍從馬達驅動器及閘極驅動器，到採用專利 CPU 架構的 MCU，包含 C2000™ 與 Arm® Cortex® 架構 MCU，例如 AM2434BSDFHIALVR。這些產品配備進階診斷功能與晶片內建感測周邊設備，可快速偵測故障，並對故障快速做出回應，同時減少系統停機時間 (在工業環境中提升工廠生產力)。

為幫助您尋找最有效的功能安全設計裝置， TI 定義三種適合在功能安全應用領域中使用的產品類別：TI 功能安全 (能力)、TI 功能安全品質 (管理) 和 TI 功能安全 (合規)。(我們的馬達驅動器、閘極驅動器和 MCU 通常是符合 TI 功能安全標準的產品。)

TI 設計並打造的這些產品，全部符合 IEC 61508 及 ISO 26262 的系統功能合規建議，能讓您用來組建出安全可靠的馬達控制與驅動系統。我們為每部裝置提供故障模式、影響與診斷分析 (FMEDA)、功能安全手冊和安全診斷資料庫，以及系統和子系統功能安全概念報告，可在 TI.com 取得，或可依要求取得。TI MCU 的功能安全手冊包括內文中對 SEooC 的說明，並概述範例應用中可能的故障群組。

我們設計資源的範例包括**適用於工業驅動器 (IEC 61800-5-2) 的 TUEV 評估安全扭矩關閉 (STO) 參考設計** ***中，適用於工業驅動器的 TÜV SÜD 評估的 STO 模組***。如需了解更多有關我們的功能安全產品的資訊，以及查看設計資源，請前往 **www.ti.com/technologies/functional-safety.html** 瀏覽。

TI 在符合 ISO 26262 SEooC 和 IEC 61508 規範的項目，以及使用 TI 產品的功能安全系統類型方面，均擁有豐富的經驗。 當然，要將這些優點發揮在實際應用中，需要在預期功能與安全功能開發的複雜要求當中取得平衡。

IMPORTANT NOTICE AND DISCLAIMER

TI PROVIDES TECHNICAL AND RELIABILITY DATA (INCLUDING DATA SHEETS), 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, regulatory 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 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.

TI objects to and rejects any additional or different terms you may have proposed.

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