採用 MCU 協助自主系統實現自主安全性

■作者：Bob Martin
Microchip 資深應用工程技術顧問

人工智慧 (AI) 和機器學習 (ML) 技術在自主性日益增強的系統中，應用越來越普遍。這將提高各行各業對更智慧的安全系統的要求。關注重點已經從節約成本轉移到使用者便利和安全。這需要一個完整的功能安全 (FuSa) 層，其中包括安全輔助處理器與可信的輸入 / 輸出控制器，兩者協同工作來保護系統。微控制器 (MCU) 為實現這些安全輔助處理器提供了低成本的解決方案，是當今新一代自主系統的核心。

自主安全功能和規範

安全輔助處理器可以執行部署的機器學習 (ML) 模型，這種模型用於接收視訊、音訊、環境和操作員資料等外部資料流程，而在某些情況下，也可以同時接收所有這些資料流程。這些資料流程必須具有固有的可信度。

同樣重要的是，安全輔助處理器必須信任它們為馬達、繼電器、指示器和其他執行器產生的輸出

圖 1：工業機器人正在焊接大型重物

狀態的真實再現。如果發生故障，主處理器也應該能夠依靠這些輸入 / 輸出邊帶 (side band) 控制器快速做出明智的決策。

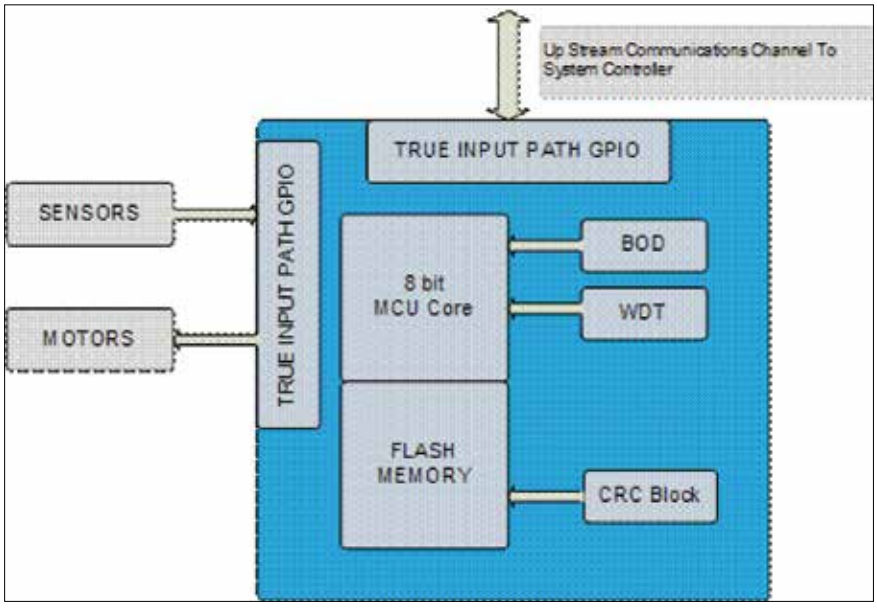
使用 MCU 作爲安全輔助處理器

在全面的開發生態系統的支援下，8 位元和 32 位元 MCU 主要用於四大功能安全領域，業內為此制定了下列工業標準規範：

- ISO 26262：汽車安全完整性等級 (ASIL)，適用於汽車應用
- IEC 61508：安全完整性等級 (SIL)，適用於工業應用
- IEC 60730：家用電器功能安全標準
- IEC 60730：醫療設備功能安全標準

開發工具生態系統有兩個重要的後端要求。第一個要求是在開發過程中以及在編譯成機器碼過程中採用穩健的編碼。使用具功能安全性的編譯器可滿足此要求，這些編譯器通過 TÜV SÜD (一家國際認可的測試機構) 等組織獲得 ISO 或 IEC 功能安全標準認證。第二個後端功能是對在典型的測試週期中執行了哪些程式碼以及遺漏了哪些程式碼進行詳細分析，這需要使用一個程式碼覆蓋率分析的外掛程式。

圖 2:8 位元微控制器的自主安全功能



自主安全功能的工作原理

與外界的主要互動是透過硬體層實現的，首先需要支援 FuSa 的 MCU (位於邊緣) 提供的直接感測器和執行器介面。請參見下面的圖 2。

主要功能包括：

欠壓檢測 (Brown Out Detect，簡稱 BOD)

擁有理想電源的工作環境十分少見。微波爐和雷射印表機會導致燈光閃爍，大型電動工具會觸發斷路器。自主系統必須提前預知其電源要發生故障，以便可以啓用備用電源，或者設置關鍵資料和輸出狀態以確保正確地關閉系統。

這些 MCU 中的 BOD 電路可以持續監視供電電壓，並以兩種特定方式對下降的電壓作出反應。首先，當電壓超過某個可選閾值時，電壓監視 (VLM) 功能將觸發中斷，允許立即執行緊急關閉任務，以避免實際的 BOD 閾值被越過。一旦越過 BOD 閾值，裝置將保持重置狀態，直到此條件被解除。同時，也可以確定重置 (Reset) 事件的原因，以確保採取適當的恢復策略，這可能與第一次的開機週期不同。

視窗看門狗計時器

現代 MCU 使用看門狗計時器作為故障恢復機制，旨在終止無限迴圈 (又稱“自旋鎖”) 條件，這種條件除了採取嚴厲的措施外沒有任何解決方法。早期版本設置了以秒或毫秒為單位的超時閾值，然後需要在達到此閾值之前對運行代碼進行某種類型的“刺激 (poke)”操作。確認後，超時閾值重置，倒計時重新開始。懶惰的程式師使用週期性中斷服務程式來更新計時器，但是即使系統的其他部分卡在某個無限迴圈中，這些程式仍會自行繼續執行，不會透過系統重置來解決這種情況。

視窗看門狗計時器通過允許指定看門狗服務視窗解決了部分問

題。這樣一來，看門狗計時器的服務速度不能太慢，也不能太快。這使得依賴已知執行時間短於最大閾值的程式碼變得更加困難。

循環冗餘檢查 (Cyclic Redundancy Check，簡稱 CRC) 程式碼掃描

一個 CRC 碼掃描周邊設備可以確保程式碼映像的完整性。它比單純的校驗碼 (checksum) 強大，因為校驗碼很容易被數學操作欺騙。可將特定的 MCU 硬體模組配置為在程式記憶體的開機程式 (bootloader) 部分、應用程式部分或整個快閃記憶體陣列上運行掃描。然後，周邊設備會將其 CRC 結果與附加在指定程式空間末尾的正確校驗碼進行比較。如果這兩個 16 位元數字匹配，則證明程式空間未遭到修改。匹配失敗可配置為產生一個不可遮罩中斷，以進一步處理該問題。

真正的輸入路徑通用輸入 / 輸出 (General Purpose Input/Output，GPIO) 周邊設備

在微控制器的早期，當一個 GPIO 接腳被配置為輸出時，驗證接腳電壓 (例如 5V) 是否與控制位值 (例如“1”) 匹配的唯一方法是使用另一個配置為輸入的 GPIO 接腳讀取電位。一個配置為輸出的 GPIO 接腳不能讀取實際電位，只能讀取寫入它的值。因此，“輸入”值始終是相同的。

真正的輸入路徑 GPIO 單元提供了一個獨立的電路通路到一個獨立的暫存器，反映了接腳設置的真實電位。雖然這個電位只能用邏輯“1”或邏輯“0”來讀取，但它仍然提供足夠的反饋來驗證輸出控制暫存器中的寫入值。這兩個值應始終保持一致。如果存在差異，就代表該特定的 GPIO 接腳上存在短路或斷路狀態，需要適當地處理。

具有這些功能的 MCU 可為完整的 FuSa 層奠定基礎。隨著基於 AI/ML 的自動化將關注重點從系統生產和維護成本節約轉向用戶體驗的安全性和便利性，FuSa 層的重要性將不斷提高。CTA

Microchip 發佈新一代 MPLAB. ICD 5 和 MPLAB. PICkit.5 線上除錯器 / 燒錄器

對於嵌入式設計人員來說，燒錄和除錯仍然至關重要，但人工作業耗時較長，Microchip 推出了 MPLAB. ICD 5 和 MPLAB PICkit 5 兩款全新的線上除錯器 / 燒錄器，為開發人員提供快速、經濟和便捷的解決方案。這兩款工具都具有遠端燒錄功能，提供更好的用戶體驗。

MPLAB ICD 5 線上除錯器 / 燒錄器為基於 PIC、AVR 和 SAM 元件以及 dsPIC 數位訊號控制器 (DSC) 的設計開發人員提供了先進的連接和電源選項。由於減少了對電源線的需求，這款開發工具可在對空間利用要求較高的環境中使用。藉由與 PC 的 USB Type-C 連接或乙太網供電 (PoE)+ 供電，MPLAB ICD 5 線上燒錄和除錯工具的使用快速、靈活和方便。PoE+ 允許設備由用於資料通信的相同電纜供電，而不需要額外電源線。除了 PoE+ 提供的靈活性外，乙太網連接還實現了遠端開發並與環境條件的隔離。

透過乙太網進行遠端除錯和燒錄，進行電源監控以優化電源設計，並與持續整合和持續部署 (CI/CD) 系統結合，在硬體和連接能力的支援下，可提供功能豐富的開發體驗。用戶可使用 Arm 單線輸出 (SWO) 追蹤以及各種燒錄和除錯介面來減少開發時間。

MPLAB PICkit 5 線上除錯器 / 燒錄器是更靈活的升級版本，既可在連接到裝有 MPLAB X 整合式開發環境 (IDE) 的電腦上使用，也可在現場使用。這款快速便攜的工具相容 Microchip 提供的所有架構，能夠透過 Microchip 最新的 Programmer-to-Go (PTG) 智慧手機應用程式進行遠端程式設計。它使用無線藍牙低能耗無線電，使開發人員能夠透過 PTG 應用程式的智慧手機與設備連接。使用 PICkit 5，使用者可以透過應用程式在 SD 卡選擇映像檔，並在現場進行燒錄。如果使用以前的版本，用戶只能在前往現場前，透過 MPLAB X IDE 或 MPLAB IPE 進行燒錄。