參考

整合電壓監控以實現工業固定式與行動機器人中的安全電源實作

Jackson Wightman
Applications Engineer
Voltage References and Supervisors

Kristen Mogensen
Systems Engineer
Robotics Systems

摘要

在本白皮書中，我們將探索如何設計安全電源供應器，同時遵循國際電子電機委員會 (IEC) 61508 標準。我們將示範電源監控設計實務，以及電壓監控對安全開機與順利故障復原至關緊要的原因。內建自我測試 (BIST) 和閂鎖清除針腳等電壓監控器積體電路 (IC) 功能是新功能，除了精準的電壓監控外，也可大幅改善功能安全設計實務。

簡介

在現代製造設施中，工業固定式與行動機器人的馬達驅動有助於提升工廠產量、效率與安全性。不過隨著工廠員工與越來越多 (且功能越來越強大) 的自動化機器人共同作業，系統設計人員必須滿足更嚴格的安全要求。開啟電源並使用標準或新興技術必須在任何情況下皆安全無虞，才能實現員工與機器人之間的真正合作。此外，在發生故障時適當關閉電源或進行操作調整，是安全的主要因素。這些機器人或其他電子產品的安全電源設計，是達成系統級功能安全要求的重要關鍵。

電源供應器設計中的安全考量與潛在故障

在完美的環境中，電源供應器將提供穩定的電壓與電流，不會超出特定設計需求而出現波動或改變。但在現實世界中，這並不是發生的事情。電源供應器不僅具有引發錯誤的固有特性，也可能偶爾發生故障。這些失敗有各式各樣的呈現方式。**表 1** 包括一些關於電源供應器故障及其原因的範例。

電源設備故障影響	原因
無輸出電壓	電源故障
電源電壓過高	負載阻抗突然變化，對下游短路
電源電壓過低	電源不足、電源故障
微控制器 (MCU) 電壓不足	電源不足、電源故障

表 1. *電源供應器故障及其原因。*

設計定期在人員身邊運作的裝置與技術時，您必須採取適當步驟來降低電源供應器故障的危險。各種應用都是如此，其中包括工業行動機器人、協作機器人，或是一旦故障即可能造成災難性後果的其他任何技術。舉例來說，在馬達驅動應用中，如果裝置扭力無法預測，可能會造成極高的危險和風險。

不過，您該如何偵測到電源供應器已偏離規格？電源供應器變更在何時會成為問題？以及如何在整個系統中針對工業應用傳達潛在故障？

工業系統功能安全與標準簡介

定義的功能安全標準有助於判斷系統是否安全。最常用的標準是 IEC 61508 和國際標準化組織 (ISO) 13849。兩種標準都會查看故障模式診斷範圍或安全故障分數，以及硬體容錯，藉以判斷系統符合的安全完整性等級 (SIL) 或性能等級 (PL)。**表 2** 總結了這些等級。

硬體容錯 (HFT)				類別				
IEC 61508				ISO 13849				
0	1	2	SFF	DC	1	2	3	4
-	SIL1	SIL2	<60%	無				
SIL1	SIL2	SIL3	60% 至 <90%	低等	c	c	d	
SIL2	SIL3	SIL4	90% 至 <99%	中		d	e	
	SIL4	SIL4	≤99%	高等				e
類型 B								

表 2. *IEC 61508 與 ISO 13849 安全標準。*

使用 **表 2** 作為指南，您會發現可透過多種方法來取得每個 IEC 61508 SIL 或 ISO 13849 PL。透過設計具適當安全故障分數或診斷範圍與硬體容錯的系統，您即可達到其中一個層級。特別是監控電源供應器的電壓可增加診斷範圍。執行電壓監控也可提升硬體容錯能力。

如您所見，您不僅必須考慮可能的故障數量，還必須考慮發生故障的可能性。您也可以發現到透過增加診斷範圍或安全故障分數，可在 SIL 或 PL 中上移而不變更硬體容錯，反之亦然。電壓監控是判斷系統診斷範圍或安全故障分數，以及減少系統解決方案殘餘適用性的重要層面。

表 3 提供每個安全參數的詳細資訊。

測量	定義
硬體故障容錯	系統容許的最小故障數量，同時保留安全功能
安全故障分數	$\frac{\text{Total safe failures} + \text{Total detected dangerous failures}}{\text{Total safe failures} + \text{Total detected dangerous failures} + \text{Total undetected dangerous failures}}$ (1)
診斷範圍	$\frac{\text{Total detected dangerous failures}}{\text{Total detected dangerous failures} + \text{Total undetected dangerous failures}}$ (2)
SIL	功能安全評等系統

***表 3.** 重要功能安全等級術語。*

使用電壓監控器 IC 進行電壓監控

監控電壓的方法有很多。此外，您選擇監控的電壓也會有所不同。在任何工業應用中，您可能需要監控高達 48V 或低至 0.8V 的電壓，以因應過電壓或欠電壓情況。幸好有監控系統中重要電壓軌的有效方法，可實現任何功能安全設計的幾個層面。透過準確的電壓監控，協助您知悉何時應完全關閉系統、重設 MCU ，或是進行其他系統層級選擇以達到安全狀態。若不持續監控安全相關電壓軌，系統將無法在發生潛在危險情況時採取行動。

可使用離散式零組件設計電壓監控電路的方法，但在著重功能安全的系統中，若將電壓監控功能整合至單一的子系統電路，判斷診斷範圍就會變得更加容易。因此電壓監控器 IC 對功能安全特別有幫助，其中包含閾值準確度、靜態電流、重設時間延遲、鎖存能力、電壓磁滯、輸出類型和 BIST 的不同組合。

表 4 列出部分電壓監控器參數和功能。

參數或特點	說明
閾值準確度	額定臨界電壓周圍的準確度百分比。
最大輸入電壓	裝置可監控的最大電壓。
靜態電流	閒置時設備消耗的電流量。
重設延遲時間	裝置在不再發生故障時解除故障狀態所需的時間量。
電壓磁滯	閾值與解除有效閾值之間的差異。如果監控的電壓振盪，此參數有助於防止誤報。

參數或特點	說明
輸出拓撲	電壓監控器的輸出接腳 (開汲極或推拉式)，採用低電位作動或高電位作動格式。
閂鎖	發生故障後，代表故障的接腳會維持宣告狀態，直到監控器 IC 收到清除邏輯的訊號為止。
BIST	執行內部裝置診斷以檢查內部故障。

***表 4.** 重要電壓監控參數。*

電壓監控器 IC 會監控電壓；一旦電壓進入欠電壓或過電壓狀態，電壓監控器便可通知 MCU，切換電源開關或驅動閘極。電壓監控器可偵測電源供應器已變更，並快速安全有效地斷開電源供應器。同時監控欠電壓和過電壓的監控器也稱為窗型監控器。您執行的電壓監控類型也會影響功能安全等級。

表 5 會列出這些等級。

電壓監控類型	潛在診斷範圍或安全故障分數
過電壓	60%
窗型 (過電壓與欠電壓)	90% 至 99%

***表 5.** 電壓監控如何影響 DC。*

設計安全電路時，請務必考慮診斷範圍等級。此外，使用電壓監控器 IC 可減少必要電路元件的數量，進而簡化設計。

電壓監控如何影響功能安全額定值

進行目標 SIL 或 PL 設計時，請務必考量硬體容錯或安全故障分數，此分數意指設計的備援，以及您在系統中實作電壓監控的方式。採用兩種最常見的標準，定義幾種不同的方式來建立或提升您的功能安全等級。電壓監控是做出此判斷或提升功能安全的重要部分。參閱 **圖 1** 和 **圖 2**，其說明使用電壓監控器且支援 SIL 2 的設計。

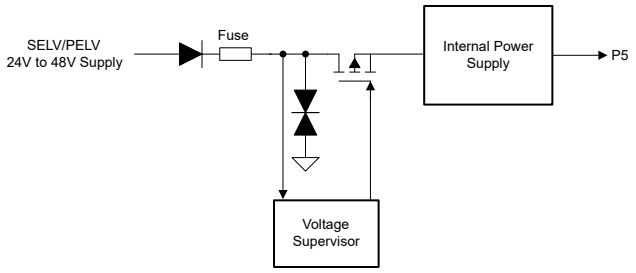

圖 1. *IEC 61800-5-2 實作高壓側安全電源供應器，可顯示電源供應器和電壓監控。*

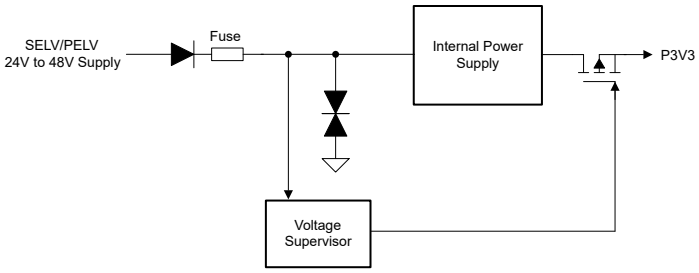

圖 2. *另一個實作 IEC 61800-5-2 的選項，即是顯示電源和電壓監控的低壓側安全電源供應器。*

在 **圖 2** 中，電壓監控器用作一個單通道，可監控過電壓和欠電壓 (若有需要)。電壓監控器的輸出可中斷超出安全操作範圍的電源供應器，或通知 MCU 發生故障情況。**圖 2** 和 **圖 1** 中的電路硬體容錯為 0，可提供安全故障分數或高達 90% 的診斷範圍。因此，**圖 1** 可提供最高 SIL 2 或 PL d 額定值。

使用此相同邏輯，提升電路配置的硬體容錯度將可增進功能安全等級。**圖 3** 顯示使用電壓監控時如何提升電路配置硬體容錯的範例。

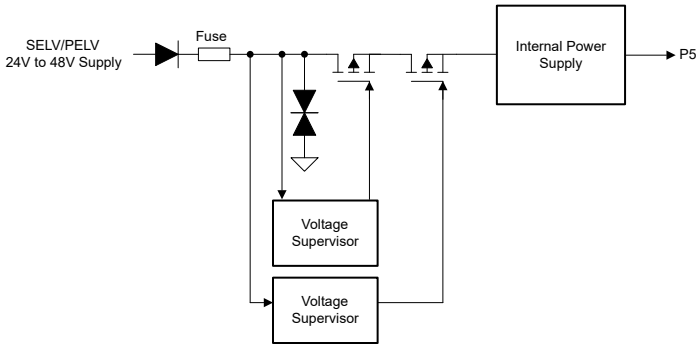

圖 3. *使用電壓監控且支援 SIL 3 電源供應器的原理圖。*

使用兩個並聯電壓監控器，可提供雙通道監控過電壓或欠電壓情況。由於這些電壓監控器會各自連結將電軌與系統其他部分斷開的專屬方法，因此如果一個電壓監控器發生故障，則在供應電壓移出規格時，另一個仍可正確安全地採取規定步驟，讓您的設計能達到高達 SIL 3 的額定值。

另一種提高電路配置功能安全的方法 (如 **圖 3** 中所示)，是使用電壓監控器實作方法的多樣性。請考量電壓監控裝置間 IEC61508 標準中所述常見故障原因的實例。若使用兩種不同的電壓監控技術監控相同的供應軌，將可降低發生共模故障的機率。

例如，選擇兩個電壓閾值不同的電壓監控器可增加多樣性。例如，在 **圖 3** 所示的電路配置中，將 TI 的 TPS3762 用於其中一個電壓監控器功能區塊，而將 TI 的 TPS37 用於另一個功能區塊，也會提供額外的功能多樣性。這是因為這兩種裝置具有兩種不同的設計。

此時您可能會有的一個疑問，在於如果電壓監控方法失敗，或是組成電壓監控電路的元件停止正常運作，則應該怎麼辦。這又是電壓監控器 IC 格外實用的另一種情況。部分電壓監控器 IC 包含 BIST 功能。這些監控器屬於窗型電壓監控器，也具有輸入接腳，使用者可在此要求裝置測試其本身的功能。電壓監控器將根據要求執行內部測試，並提供訊號以表明其仍如預期運作。

圖 4 說明了此實作方式。

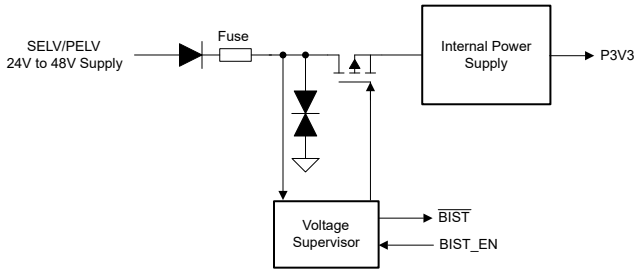

圖 4. *使用具有 BIST 功能的電壓監控器 IC 進行電壓監控。*

提供電壓監控方法本身的診斷範圍 (在此情況下由具備 BIST 功能的電壓監控器 IC 完成)，可將系統的診斷範圍增加至高達 99%，此為非常高的涵蓋範圍。在具適當硬體容錯的電路中實作此高診斷範圍時，可讓您的系統達到 SIL 3 或 PL e 級的功能安全。具有此類整合功能的裝置範例就是 TI 的 TPS3762。

使用電壓監控裝置的另一個優點是可監控高電壓。例如，TPS3762 可監控高達 65V，因此可讓其與具廣泛輸入電壓範圍的類似裝置直接連接電軌，並提供監控和其他診斷功能。舉例來說，部分設計需要超低電壓 (ELV)，而超低電壓是標準 IEC 60449-1 中定義的電壓範圍。ELV 定義現已重複使用，以定義 IEC 62368 標準中的 SELV 定義，其中部分電力能源等級不允許電源供應器輸出的電壓高於特定電壓。例如，電力能源等級 ES1 不允許電源供應器輸出超過 60V。

考慮這點，針對安全超低電壓電源供應器，將安全最大電壓位準設為 $60V_{DC}$ 最大值，安全電源供應器只能在極短的時間內超過此值，否則將無法符合安全超低電壓標準。$60V_{DC}$ 是安全標準中極常見的最大電壓，其中包括安全超低電壓和防護超低電壓。因此，TPS3762 等寬輸入電壓裝置具備可監控 65V 的最大輸入電壓。

安全扭矩關閉設計範例

馬達驅動級是許多工業製程不可或缺的要素，且在安全性至關重要的許多環境中都會使用此級。許多機器人都使用馬達與人類並肩合作。在馬達驅動應用中絕對必須採取適當動作，以在發生潛在危險狀態時關閉系統。**表 1** 中所列的情況可能會導致馬達突然危險運作。

安全馬達驅動的其中一個重要層面，即是實作安全扭矩關閉電路。每個馬達驅動的功率級皆由閘極驅動器組成，除了功率級電路外也可能會隔離。使用電壓監控器 IC 監控閘極驅動器和功率級的電源軌，對於判斷系統的功能安全等級非常有幫助。**圖 5** 是 SIL 2 或 PL d 額定安全扭矩關閉系統原理圖的範例。

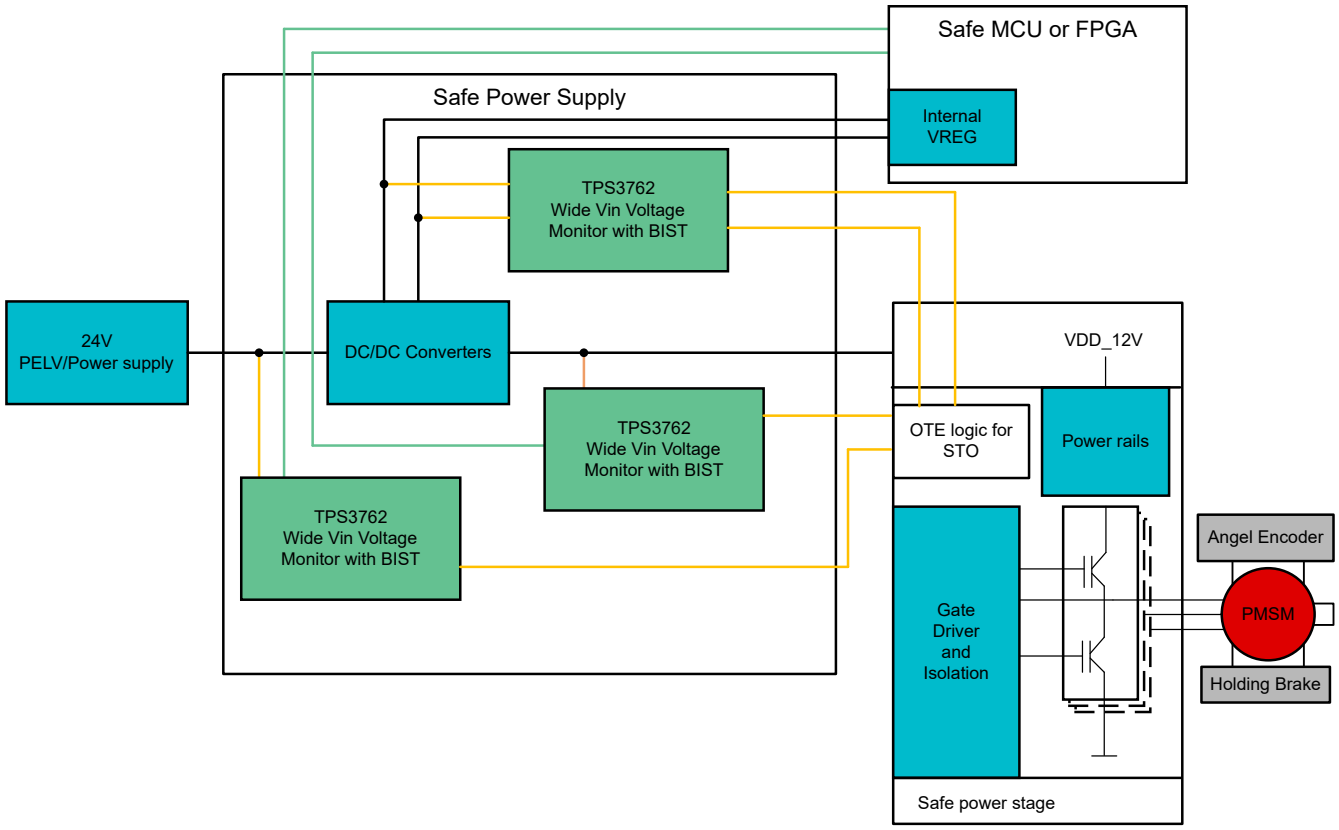

圖 5. *SIL 2 或 PL d 額定安全扭矩關閉系統原理圖。*

在 **圖 5** 中有幾個電壓監控實例：24V 電源以及用於 MCU 或現場可編程邏輯閘陣列功率級的各種隔離輸入。這些電壓監控機制的硬體容錯為零。然而由於 TPS3762 的窗型電壓監控及其 BIST 功能提供的高診斷範圍，您仍可取得 SIL 2 或 PL d 額定系統。

結論

隨著我們的技術日益先進，必須更具戰略性地瞭解這些進步如何影響人類生活。當我們學習如何有效運用機械、機器人和電子領域的新進展時，安全性至關緊要。提升任何電源供應設計的功能安全，最終將帶來更驚人且強大的馬達驅動應用。運用電壓監控器等先進晶片，可讓設計人員安全地判斷系統何時可能出現安全故障，並採取適當步驟以確保安全。

功能安全在未來幾年將變得越來越重要。透過電壓監控來瞭解並改善任何應用的功能安全，皆有助於打造更安全的世界。

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