参考文献

集成电压监控功能，以便在工业固定式和移动式机器人驱动系统中实现安全电源

Jackson Wightman
Applications Engineer
Voltage References and Supervisors

Kristen Mogensen
Systems Engineer
Robotics Systems

内容概览

在本白皮书中，我们将探讨如何在遵守国际电工委员会 (IEC) 61508 标准的同时，设计安全的电源解决方案。我们将演示电源监控设计实践，并阐释为何电压监控是安全启动和顺畅故障恢复的关键所在。还介绍了电压监控集成电路 (IC) 特性（如内置自测试 BIST）和锁存清除引脚，这些新功能不仅能提供精确的电压监控，还能显著提升功能安全设计的实践效果。

简介

在现代制造设施中，工业固定式和移动式机器人驱动系统有助于提高工厂产出、效率和安全性。然而，随着工厂中自动化机器人数量的增加及其性能的提升，员工越来越多地与机器人协作，系统设计人员必须满足更严格的安全要求。在任何情况下，启动并使用标准或新兴技术都必须是安全的，这样才能实现员工与机器人之间的真正协作。此外，在发生故障时，适当断电或进行运行调整是安全设计的主要因素。为了满足系统级功能安全要求，为这些机器人或其他电子设备设计安全电源方案至关重要。

电源设计中的安全注意事项和潜在故障

在理想情况下，电源应始终提供恒定的电压和电流，并且不应超出特定设计要求。但在现实世界中，情况并非如此。电源不仅因其固有特性可能引入误差，还可能偶尔出现故障。这些故障有多种形式。**表 1** 列出了一些电源故障及其原因。

电源故障影响	原因
无输出电压	电源本身故障
电源电压过高	负载阻抗突然变化、短接至下游
电源电压过低	电源能力不足、电源本身故障
微控制器 (MCU) 欠压	电源能力不足、电源本身故障

表 1. *电源故障及其原因。*

在设计经常与人类协作的器件和技术时，必须采取适当的措施来缓解电源故障带来的安全隐患。这一点适用于广泛的应用场景，包括：工业移动机器人、协作机器人以及任何可能因故障导致灾难性后果的技术。例如，在电机驱动应用中，如果器件的输出力矩变得不可预测，将会带来巨大的危险和风险。

但是，如何检测电源偏离其设计规格？电源变化在什么时候会成为问题？在工业应用中，如何有效地将潜在故障信息传递到整个系统中？

工业系统中的功能安全和相关标准简介

功能安全标准的制定有助于评估系统是否安全。最常用的标准是 IEC 61508 和 ISO 13849。这两项标准都通过评估失效模式的诊断覆盖率或安全失效分数，以及硬件故障容错，来确定系统满足的安全完整性等级 (SIL) 或性能等级 (PL)。**表 2** 列出了这些等级。

硬件故障容错 (HFT)					类别			
IEC 61508				ISO 13849				
0	1	2	SFF	DC	1	2	3	4
-	SIL1	SIL2	<60%	无				
SIL1	SIL2	SIL3	60% 至 <90%	低	c	c	d	
SIL2	SIL3	SIL4	90% 至 <99%	中		d	e	
	SIL4	SIL4	⩽99%	高				e
类型 B								

表 2. *IEC 61508 与 ISO 13849 安全标准。*

按照表 2，系统可以通过多种方式达到 IEC 61508 SIL 或 ISO 13849 PL 的要求。通过设计具有适当安全失效分数或诊断覆盖率以及硬件容错的系统，您可以实现目标安全等级。特别是，对电源轨的电压进行监控可以显著提高诊断覆盖率。而电压监控的实施还能进一步提升硬件故障容错能力。

需要注意的是，不仅要评估可能出现的故障数量，还需要评估故障发生的可能性。还可以看到，通过提高诊断覆盖率或安全失效分数，可以在不更改硬件容错的情况下提高 SIL 或 PL 等级，反之亦然。电压监控可以有效支持确定系统诊断覆盖率或安全失效分数，并有助于减少系统解决方案的剩余 FIT。

表 3 提供了每个安全参数的更多信息。

衡量指标	定义
硬件故障容错	系统在保持安全功能的前提下容许的最小故障数
安全失效分数	$\frac{\text{Total safe failures} + \text{Total detected dangerous failures}}{\text{Total safe failures} + \text{Total detected dangerous failures} + \text{Total undetected dangerous failures}}$ (1)
诊断覆盖率	$\frac{\text{Total detected dangerous failures}}{\text{Total detected dangerous failures} + \text{Total undetected dangerous failures}}$ (2)
SIL	功能安全等级系统

表 3. *重要的功能安全等级术语。*

使用电压监控 IC 实现电压监控

有许多方法可以监控电压，并且可以选择监控不同的电压范围。在任何工业应用中，都可能需要监控高至 48V 或低至 0.8V 的电压，以判断是否存在过压或欠压情况。幸运的是，现有的电压监控方法可以有效地监控系统中的关键电压轨，进而支持功能安全设计的多方面需求。通过精确的电压监控，系统能够在需要时完全关闭设备、复位 MCU 或采取其他系统级措施以达到安全状态。如果不持续监控与安全相关的电压轨，系统在潜在危险情况下将无法做出及时响应。

尽管可以使用分立元件设计电压监控电路，但对于以功能安全为重点的系统来说，如果电压监测功能集成到一个子系统电路中，则确定诊断覆盖率会容易得多。因此，电压监控 IC 对于确保功能安全尤为重要。这些 IC 结合了不同的功能和特性，包括阈值精度、静态电流、复位延时时间、锁存功能、电压迟滞、输出类型和 BIST。

表 4 列出了一些电压监控器的参数和特性。

参数或特性	说明
阈值精度	标称阈值电压附近的精度百分比。
最大输入电压	器件可监控的最大电压。
静态电流	器件空闲时消耗的电流量。
复位延时时间	故障消失后，器件从故障状态恢复所需的时间。
电压迟滞	阈值与置为无效阈值之间的差值，有助于在监测电压波动时防止误置为无效。
输出拓扑	电压监控器的输出引脚（开漏或推挽），支持低电平有效或高电平有效格式。
锁存	故障发生后，故障指示引脚仍然有效，直到监控 IC 接收到清除逻辑信号。
BIST	器件内部诊断功能，用于检查器件内部故障。

表 4. *重要的电压监控器参数。*

电压监控 IC 可以在监测到电压进入欠压或过压状态时，通知 MCU，切换电源或驱动栅极信号。电压监控器可以检测到电源是否发生了变化，并快速安全有效地断开电源。能够同时监控欠压和过压的监控器也称为窗口监控器。选择使用哪种类型的电压监控方法也会影响功能安全等级。

表 5 列出了这些额定值。

电压监控类型	潜在诊断覆盖率或安全失效分数
过压	60%
窗口（过压和欠压）	90% 至 99%

表 5. *电压监控如何影响直流。*

在设计安全电路时，务必要考虑诊断覆盖率的级别。此外，使用电压监控 IC 可以减少必要电路元件的数量，从而简化设计。

电压监控如何影响功能安全等级

在设计满足目标 SIL 或 PL 时，需要重点考虑硬件容错或安全失效分数。这些参数反映了设计的冗余程度以及系统中电压监控功能的实现方式。这两种最常见的标准提供了多种方法来确定或提升功能安全等级，而电压监控在此过程中起到了关键作用。请参见**图 1** 和**图 2**，了解如何利用电压监控实现具有 SIL 2 功能的设计。

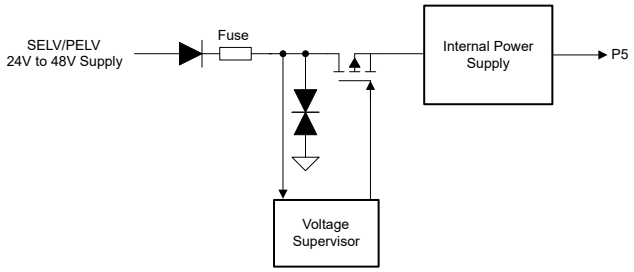

图 1. *IEC 61800-5-2 标准中的高侧安全电源实现（包括电源和电压监控模块）。*

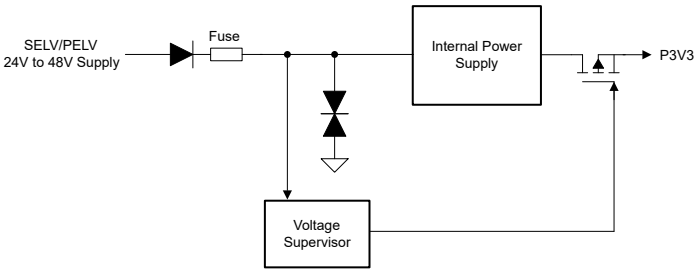

图 2. *IEC 61800-5-2 标准中的低侧安全电源实现（包括电源和电压监控模块）。*

在**图 2** 中，电压监控器用作一个通道，可以监控过压和欠压（如果该功能也是设计目标）。电压监控器的输出可以在电源工作超出安全范围时断开电源，或者向 MCU 发送故障通知信号。在 **图 1** 和 **图 2** 中，电路的硬件故障容错为 0，但可以提供高达 90% 的安全失效分数或诊断覆盖率。因此，**图 1** 能够满足 SIL 2 或 PL d 等级的安全要求。

基于相同的逻辑，增加电路配置的硬件容错能力可以进一步提高功能安全的等级。**图 3** 展示了如何在电路配置中结合电压监控来增加硬件故障容错，从而提升功能安全性。

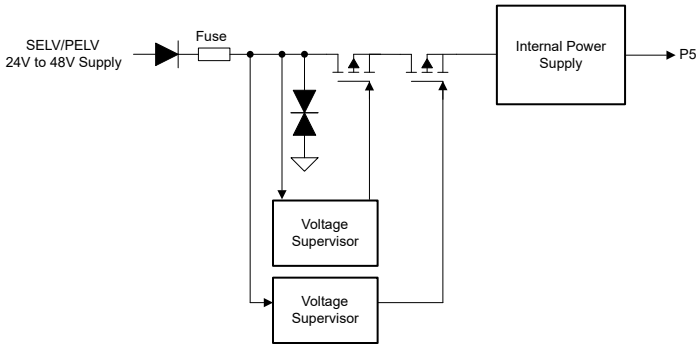

图 3. *使用电压监控功能实现 SIL 3 功能的电源框图。*

并联使用两个电压监控器可提供两个通道来监控过压或欠压情况。由于每个电压监控器都连接到各自独立的电源断开机制，即使一个电压监控器发生故障，另一个仍可在电源电压超出规格时采取正确且安全的措施，从而使设计达到 SIL 3 等级的要求。

另一种提升电路配置功能安全性的方法是通过采用不同的电压监控器实现技术，以实现多样性设计，如**图 3** 所示。例如，IEC 61508 标准中提到的常见原因故障可能影响使用相同技术的电压监控器设备。如果在同一电源轨上使用两种不同技术的电压监控器，可显著降低发生共模故障的概率。

例如，选择具有不同电压阈值的两种电压监控器，可以增加系统的多样性。再例如，在某些电路配置中，如**图 3** 所示，可使用 TI 的 TPS3762 作为一个电压监控功能模块，同时使用 TI 的 TPS37 作为另一个监控模块。这两款设备采用不同的设计。

在此过程中，可能会产生一个问题：如果电压监控方法失效，或者电压监控电路的组成元件失效，该怎么办？这正是电压监控 IC 显示其独特价值的场景之一。某些电压监控 IC 内置 BIST 功能。这些监控器是窗口电压监控器，且带有一个输入引脚，用户可通过该引脚请求设备对其自身功能进行测试。收到请求后，电压监控器会执行内部测试，并提供一个信号，确认其仍然正常运行。

图 4 展示了此类实现方案。

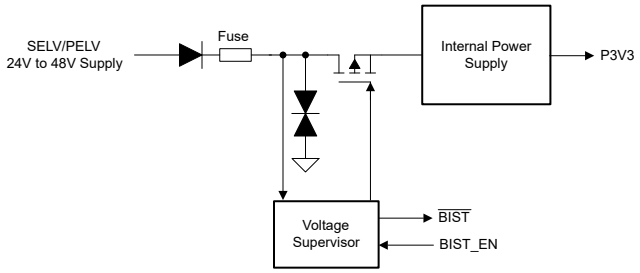

图 4. *使用具有 BIST 功能的电压监控 IC 实现电压监控。*

通过采用具有内置 BIST 功能的电压监控 IC，可以对电压监控方法本身提供诊断覆盖率。使用这种方法，系统的诊断覆盖率可以提升至高达 99%，这是一个非常高的覆盖水平。如此高的诊断覆盖率，配合适当的硬件故障容错设计，可以使系统达到 SIL 3 或 PL e 等级的功能安全要求。TI 的 TPS3762 就是一款集成了此类功能的器件。

此外，使用电压监控器的另一个优势是可以监控高电压。例如，TPS3762 可以监控高达 65V 的电压。此类具有宽输入电压范围的器件可以直接连接到电源轨，同时提供监控和其他诊断功能。某些设计需要超低电压 (ELV)，这是一种在 IEC 60449-1 标准中定义的电压范围。ELV 的定义也被重用于 IEC 62368 标准中的 SELV 定义，该标准要求某些电能源等级在电源输出端的电压不得超过特定限制。例如，ES1 级不允许电源输出端电压超过 60V。

考虑到这一点，在安全超低电压电源中，$60V_{DC}$ 被设定为安全的最大电压水平，且安全电源仅允许在短时间内超过该值，否则将不符合安全超低电压标准。$60V_{DC}$ 是许多安全标准中一个常见的最大电压限制，包括安全超低电压和保护性超低电压。因此，像 TPS3762 这样具有宽输入电压范围的器件，其最高可监控电压为 65V。

安全转矩关闭设计示例

电机驱动级是许多工业工艺中的关键元件，尤其在注重安全性的环境中更为重要。许多机器人在与人类协同工作时依赖电机驱动。在电机驱动应用中，当检测到潜在的危险状态时，必须采取适当措施，安全地关闭系统。某些情况下（如**表 1** 所列示的情况），可能会导致电机突然进入危险的运行状态。

为了实现电机的安全运行，设计安全转矩关闭电路是一个关键环节。每个电机驱动系统都包含一个功率级电路，该电路通常包括栅极驱动器、电源轨，还可能包括隔离元件。使用电压监控 IC 来监控栅极驱动器和功率级的电源轨，对确定系统的功能安全等级至关重要。**图 5** 是一个满足 SIL 2 或 PL d 等级的安全转矩关闭系统方框图的示例。

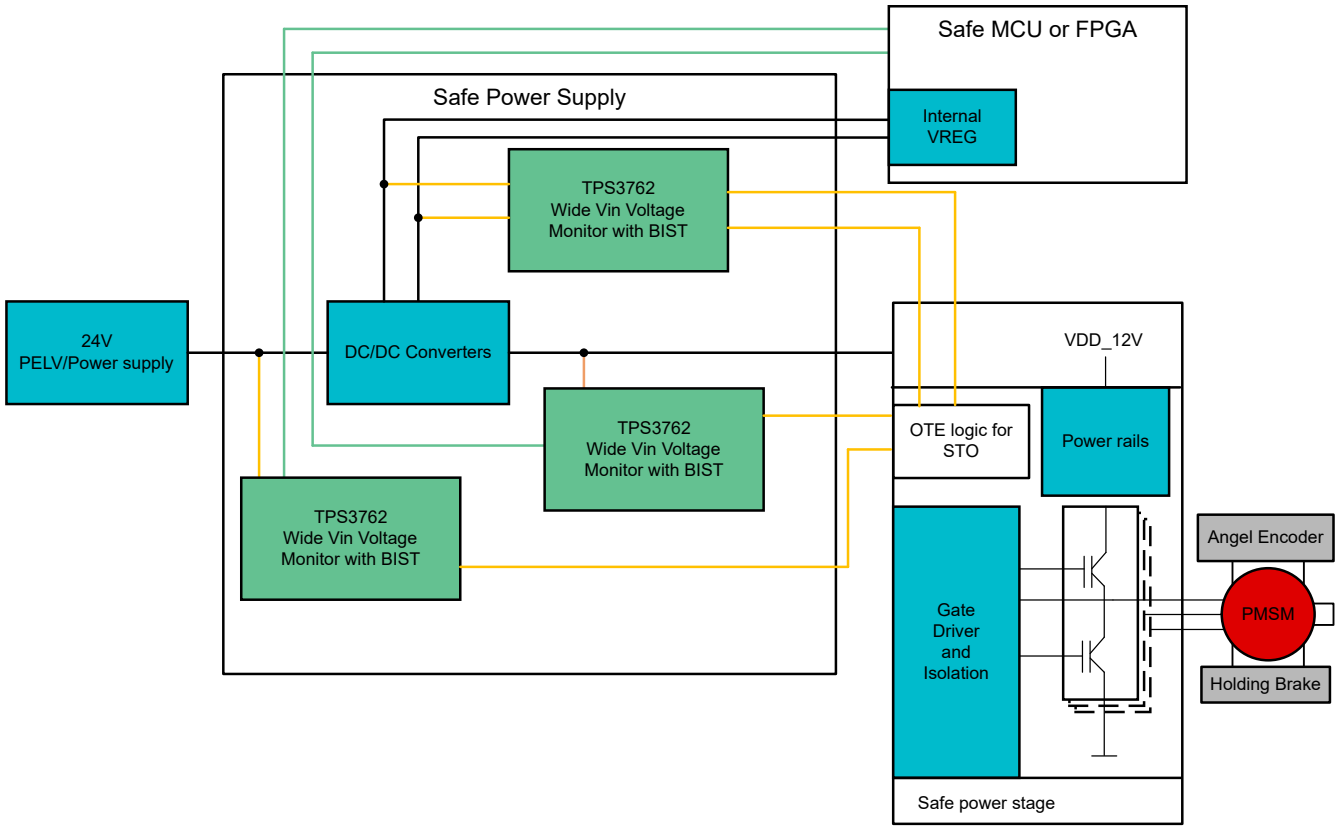

图 5. *满足 SIL 2 或 PL d 等级的安全转矩关闭系统方框图。*

在图 5 中，可以看到电压监控的多种应用场景：24V 电源的监控，以及功率级中用于 MCU 或现场可编程门阵列的各种隔离输入的监控。这些电压监控方案的硬件容错为零。然而，通过使用 TPS3762 的窗口电压监控功能及其 BIST 特性，即使在这种情况下，系统仍然能够满足 SIL 2 或 PL d 等级的要求。

结语

随着技术的不断进步，我们需要更加战略性地考虑这些进步对人类生活的影响。在探索如何高效利用先进机械、机器人和电子技术的过程中，安全性始终是首要考虑因素。提升电源设计的功能安全性能，最终将推动更强大、更高效的电机驱动应用的发展。借助电压监控器等先进的芯片，设计人员可以安全地确定系统何时出现安全故障，并采取适当的措施确保安全。

在未来几年，功能安全将变得越来越重要。利用电压监控来了解和改进应用的功能安全性，将有助于建设一个更安全的世界。

重要声明和免责声明

TI“按原样”提供技术和可靠性数据（包括数据表）、设计资源（包括参考设计）、应用或其他设计建议、网络工具、安全信息和其他资源，不保证没有瑕疵且不做出任何明示或暗示的担保，包括但不限于对适销性、某特定用途方面的适用性或不侵犯任何第三方知识产权的暗示担保。

这些资源可供使用 TI 产品进行设计的熟练开发人员使用。您将自行承担以下全部责任：(1) 针对您的应用选择合适的 TI 产品，(2) 设计、验证并测试您的应用，(3) 确保您的应用满足相应标准以及任何其他功能安全、信息安全、监管或其他要求。

这些资源如有变更，恕不另行通知。TI 授权您仅可将这些资源用于研发本资源所述的 TI 产品的应用。严禁对这些资源进行其他复制或展示。您无权使用任何其他 TI 知识产权或任何第三方知识产权。您应全额赔偿因在这些资源的使用中对 TI 及其代表造成的任何索赔、损害、成本、损失和债务，TI 对此概不负责。

TI 提供的产品受 TI 的销售条款或 ti.com 上其他适用条款/TI 产品随附的其他适用条款的约束。TI 提供这些资源并不会扩展或以其他方式更改 TI 针对 TI 产品发布的适用的担保或担保免责声明。

TI 反对并拒绝您可能提出的任何其他或不同的条款。

邮寄地址：Texas Instruments, Post Office Box 655303, Dallas, Texas 75265