在功能安全应用中使用电压监控器监控电压轨

作者：Mathew Jacob
应用工程团队

引言

“功能安全”概念要求任何与安全相关的系统以可预测的安全方式正确运行或进入失效模式。这是一个宽泛的主题，相关的一些标准主要涉及汽车应用（国际标准化组织 26262）和工业应用（国际电工委员会 61508）中的电子产品。

自动驾驶汽车或协作机器人对先进电子系统的需求不断增长，引发了人们对功能安全的担忧，这促使工程师想要深入了解各种失效模式以及如何设计失效防护系统。

本文重点讨论汽车摄像头系统的电压轨监控。与其他分立式解决方案相比，电压监控器在功率、尺寸和时基故障 (FIT) 率方面具有优势，并且可帮助工程师在设计中达到更高的安全等级。汽车摄像头系统或域控制器通常需要对整个电源架构进行重要的电压轨监控。

电压轨系统故障

电压轨监控功能是每个电子系统的一部分，可确保关键元件在建议的工作电压范围内正常工作。发生电压轨故障的原因有很多，包括电源内部故障导致电压调节不正确、被动失效导致短路或开路故障，甚至是意外的负载电流导致电源轨电压骤降。电压监控器可监控电压轨是否有电压错误，并允许它们提供由安全系统用于诊断用途的响应输出。

负载点故障的一个常见示例是微控制器 (MCU) 的欠压问题。为 MCU 供电的电压轨低于预期电压时便会发生“欠压”，这一问题会导致 MCU 处于不明状态。解决 MCU 欠压问题的一种常见方法是监控进入 MCU 的电压轨是否存在欠压情况，并向 MCU 提供复位输出。复位输出会将 MCU 关闭，直到欠压问题得到解决。

图 1 是汽车摄像头系统的基本电源架构示例，其中采用了 TPS37043-Q1 电压监控器，这是一款符合功能安全标准的器件，可满足 ISO 26262 要求和汽车安全完整性等级。在此电源架构中，监控器的作用是识别系统中的潜在故障，并防止图像传感器或摄像头系统出现任何运行错误。没有任何保障措施的电压轨故障会降低故障指标等级，从而降低整体系统安全性，而电压轨监控功能则有助于提高电源架构的故障指标等级。此功能为系统提供了更多信息，从而支持受控的决策过程，并避免可能导致危险情况的安全违规行为。

在图 1 中，安全运行意味着使用中的汽车摄像头始终可靠工作，时刻确保用户不会面临严重受伤的风险。可能发生的故障类型有两种：系统性故障和随机故障。开发用于电源架构的部件时，遵守正确的设计规则有助于消除系统性故障；然而，按照定义，随机故障是随机的。没有人知道它们是否以及何时会发生。

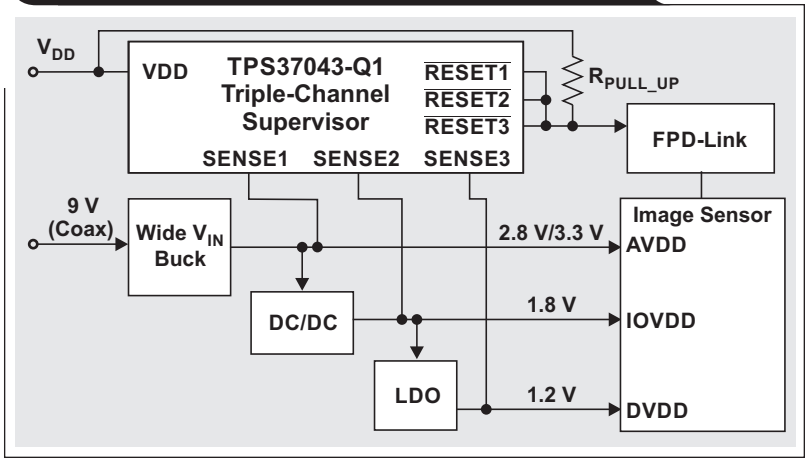
现在来看一个采用了备用摄像头的故障示例。如果电源架构的任何部件发生随机故障并且驾驶员的显示屏出现黑屏，该事件会被认定为可察觉的故障；驾驶员仍可通过后视镜安全倒车。然而，该摄像头用于车道保持辅助功能或障碍物检测系统时，用户不会意识到故障的发生，这种情况会导致危险。触发该故障的因素可能是通向图像传感器的其中一个电压轨低于图像传感器的绝对最大值或最小值，从而导致其进入挂起状态。在这种情况下，电压监控器的任务是在出现挂起状态时使图像传感器复位，以便系统重新启动。

一个明显的问题是，重启所花费的时间本身是否会被视为安全隐患？这种情况下容错时间间隔 (FTTI)将发挥作用。这是指系统必须在不使驾驶员或其他人处于危险之中的情况下进行更正的时间。监控器的复位延时时间将是根据 FTTI 选择的设计参数。在系统复位期间，安全的做法是在故障触发时立即向驾驶员发出视觉和听觉警报。该警报将使驾驶员警觉，并避免出现可能导致危险的不可察觉的故障。

下一个问题是如何保证电压监控器始终可靠工作？这就是可能出现故障的环节。例如，假设会触发直接运行错误的临界电压轨是 1.2V，如果负责监控 1.2V 电压轨的 TPS3704 的比较器 (SENSE3) 不能正常工作，会发生什么情况呢？故障检测功能失效有四种可能的原因（这称为失效模式分布）：

- 过压阈值太高。
- 欠压阈值太低。
- 比较器完全无法工作。
- 比较器可以工作，但复位线卡在高电平，因此无法传达故障。

图 1：具有监控功能的汽车摄像头电源架构



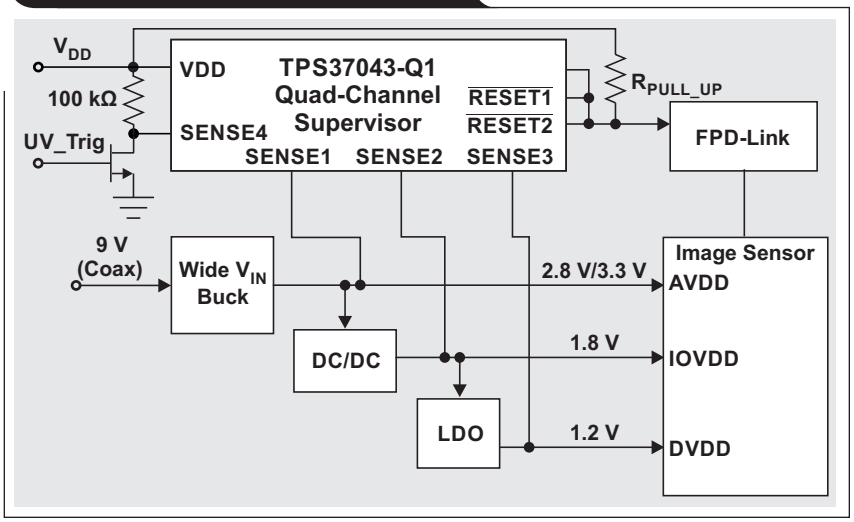
如果比较器进入这些失效模式之一，则系统中不会有任何指示，直到监控器作出反应。这种未被检测到的监控器故障会导致运行错误，如果未在 FTTI 内发现，驾驶员可能会受伤。因此，比较器的故障是潜在的并且处于休眠状态，直到监控器作出反应。

运用一种称为内置自检 (BIST) 的机制可防止监控器故障情况。理想情况下，BIST 应该是自动的，并且在每次给监控器供电（点火开关接通）时运行。图 2 所示为欠压故障的手动自检，而图 3 为过压和欠压跳闸点的手动检查。

在图 2 中，SENSE4 过压 (V_{IT+}) 设置为 5.5V，欠压 (V_{IT-}) 设置为 2V。V_{IT+} 是设置的过压跳闸点，V_{IT-} 是设置的欠压跳闸点。能够设计启动机制，以便每次打开点火开关时，都会触发手动欠压，从而将 SENSE4 拉低至其欠压跳闸点以下，并将 RESET2 置为低电平。此过程将确认欠压比较器和 RESET 逻辑工作正常。这是一种低覆盖率的自检方案，因为它只检查一个 SENSE 通道并作为其他通道的伪表示。

图 3 显示的方案用于检查高于或低于阈值的过压和欠压跳闸点，并在 SENSE 通道上实施检查（此处对于汽车摄像头的运行至关重要）。在该方案中，LM10011 与电压识别 (VID) 接口结合使用。VID 接口的不同逻辑组合在三个值（标称值、过压测试值和欠压测试值）之间改变 LM10011 的内部 DAC 输出电流 (I_{DAC_OUT})。公式 1、2 和 3 说明了如何使用 LM10011 来触发过压和欠压故障。

图 2：针对欠压故障的手动自检



$$V_{SENSEx} = \frac{1.2}{R1+R2} \times R2 - I_{DAC(nom)} \times R2 = 0.8 \quad (1)$$

其中 V_{SENSEx} 为感应电压，1.2V 为监控的电压。

根据公式 1，对于要检查的标称输出电压，选择 R1 和 R2 可以在 SENSEx 引脚上获得 0.8V 电压。

应设置公式 2 的值，以便在设置用于过压测试的 I_{DAC_OUT} 时越过 1.2V 电压轨的选定过压跳闸点。

$$I_{DAC(ovtest)} \quad R2 \quad (2)$$

应设置公式 3 的值，以便在设置用于欠压测试的 I_{DAC_OUT} 时越过 1.2V 电压轨的选定欠压跳闸点：

$$I_{DAC(uvtest)} \quad R2 \quad (3)$$

其中，$I_{DAC(ovtest)} > I_{DAC(nom)} > I_{DAC(uvtest)}$。

现在考虑图 3 所示实施的 BIST 方案直接影响的功能安全指标。在计算功能安全指标时，有两个关键方面会很重要：单点故障诊断覆盖率和潜在故障诊断覆盖率。使用了窗口监控器来提高单点故障诊断覆盖率的成绩，因此通过实施 BIST 方案，潜在故障诊断覆盖率从 0% 跃升至 60%。这有助于降低潜在时基故障率。

图 3：针对过压和欠压跳闸点的手动检查

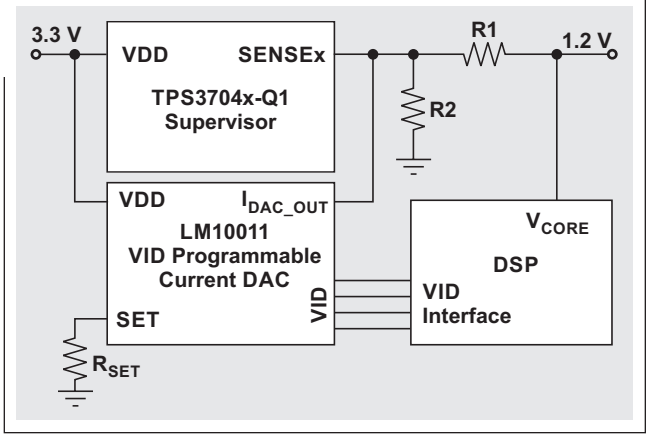
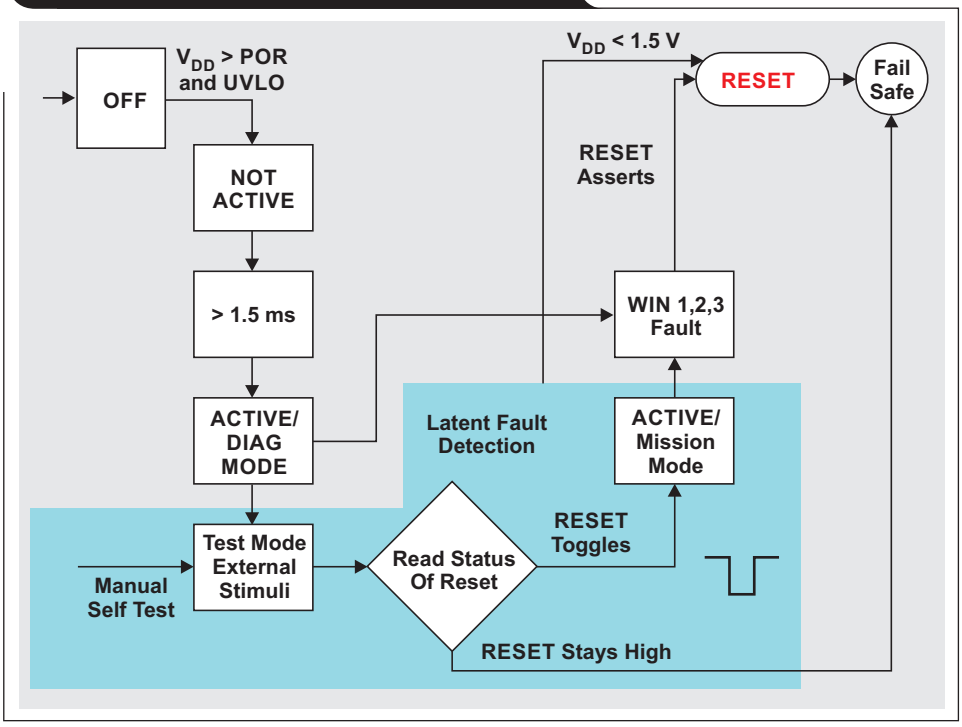


图 4：显示自检方案实施情况的流程图



各种自检方法都可提高潜在故障指标，以确保监控器始终有效。为了将自检作为一种安全机制，需要在每次接通点火开关时或在一个行驶周期中或者在激活摄像头系统功能的任何时候进行一次测试。图 4 所示的流程图展示了该方案。目标是在系统进入活动状态或任务工作模式之前执行自检方案。图 4 中的着色区域显示了自检方案的附加模块，这些模块可提高潜在故障指标。

结论

根据应用选择合适的监控器很重要，一旦选定，就可使用简单的机制来改善潜在故障指标并避免电源轨故障转化成危险。

相关网站

产品信息：

TPS3704x-Q1

LM10011

TI 全球技术支持

TI 支持

感谢您的订购。如有疑问或需联系我们的支持中心，请访问

www.ti.com.cn/support

中国： http://www.ti.com.cn/guidedsupport/cn/docs/supporthome.tsp

日本： http://www.tij.co.jp/guidedsupport/jp/docs/supporthome.tsp

技术支持论坛

在 TI 的 E2E™ 社区（工程师对工程师）中搜索数百万个技术问题和答案，网址

e2e.ti.com

中国： http://www.deyisupport.com/

日本： http://e2e.ti.com/group/jp/

TI 培训

从技术基础到高级实施，我们提供点播和直播培训以帮助您实现下一代设计。即刻体验，请访问

training.ti.com

中国： http://www.ti.com.cn/general/cn/docs/gencontent.tsp?contentId=71968

日本： https://training.ti.com/jp

A011617

ZHCT353

重要声明和免责声明

TI 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安全、安保或其他要求。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 (https:www.ti.com.cn/zh-cn/legal/termsofsale.html) 或 ti.com.cn 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。

邮寄地址：上海市浦东新区世纪大道 1568 号中建大厦 32 楼，邮政编码：200122