电动汽车和自动驾驶车辆功能安全系统的执行器设计趋势

Anuj S. Narain
Product Marketing Engineer
Motor Drivers
Texas Instruments

借助为功能安全应用开发的模拟元件，可为电动、线控和失效操作车辆架构打造复杂的电气驱动系统。

互联、自动、共享和电动（也统称为 CASE）是自一个多世纪前第一辆 Model T 汽车驶下装配线以来，汽车领域最激动人心的四大发展趋势。而更环保、更安全、更高效的汽车不仅可以使城市保持清洁，同时还能减少我们对不可再生能源的依赖。

这些趋势正在以一种有趣的方式在动力总成和底盘架构级别交汇。传统的驾驶员主导功能正在被自动化功能所取代，这些功能非常智能，能够以更安全、更高效的方式操控汽车。本白皮书将重点介绍 CASE 趋势对电力驱动系统的影响。

欢迎来到线控时代 – 这一次充满信任

线控转向、线控制动、线控换档和电气化动力总成等技术为这些系统的设计人员带来了一系列激动人心的全新挑战。车辆功能向电气驱动过渡从本质上意味着机械部件会减少，进而可以减轻重量、消除常见的机械故障模式并实现智能功能集成。例如，当线控转向系统能够根据道路和天气状况智能地调整转向响应时，便可以改善车辆动力学性能并提高效率。

另一个例子是自动换档和线控换档技术，其中电动执行器结合发动机最高效的工作点来处理变速箱的换档功能。这些系统具有安全优势，有助于防止未起动或停放的车辆发生前溜或后溜。

图 1 显示了线控系统（包括转向、变速和制动）中的执行器。

尽管线控系统所需的硬件和软件组件已经面世多年，但消费者一直对线控系统缺乏信任。

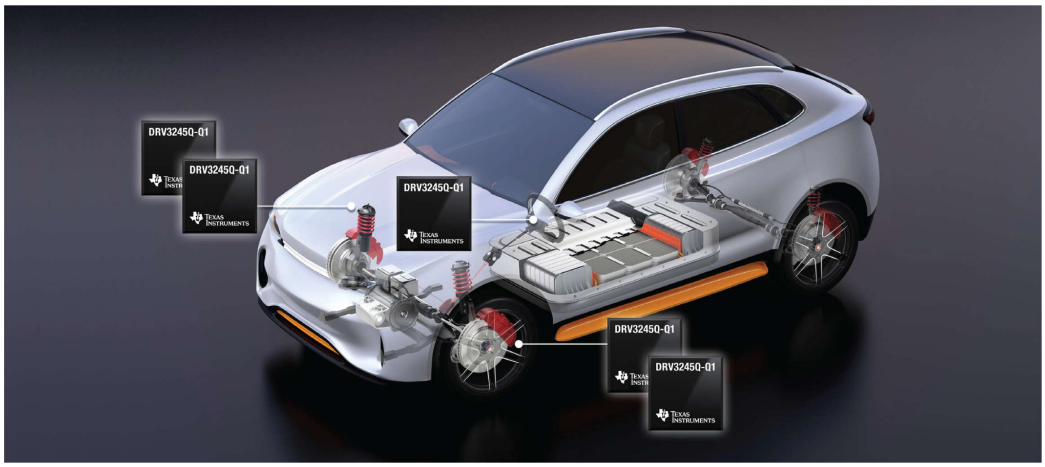

***图 1.** 采用 TI 电机驱动器实现功能安全应用，对于向线控（转向、制动和变速）过渡的汽车执行器来说大有裨益。*

从“失效防护”系统过渡到“失效操作”系统

随着执行器从使用机械能转向使用电能，安全架构需要不断发展。如今，安全系统中的大多数电动执行器都会保留其原始机械部件以实现冗余。

以电气制动系统为例，踏板与制动缸之间的机械连杆机构可以提供冗余，这样一来，当电气系统发生故障时，用力重踩制动踏板也可以制动。电气制动系统采用的是“失效防护”架构，这意味着如果这些系统发生故障，其故障方式不会妨碍任何冗余措施（本例中为重踩踏板）正常工作。

随着自主架构的发展，我们对机械冗余的依赖逐渐减弱，因为控制环路已经不再需要人为干预，这时一类全新的“失效操作”系统随之出现。例如，自动驾驶车辆中的制动系统便是一种失效操作系统。在自动驾驶车辆中，当电气制动系统发生故障后，而驾驶员又一时无法操控车辆

时，该系统（请注意，不是集成电路）应能在这种情况下继续运行并制动车辆。

设计此类系统时，主要安全考虑因素包括：

- 系统的容错能力和汽车安全完整性等级 (ASIL)。
- 第一个故障发生后系统允许的功能降级。
- 紧急功能、驾驶员警告及其紧急操作持续时间。
- 系统进入和退出安全状态时所需的 ASIL 级别。

为了分析失效操作系统的安全目标和安全状态（以**图 2** 作为指导），我们可以参考国际标准化组织 (ISO) 第二版 ISO26262-3:2018 第 7 条，其中说明了可以通过转换到或保持一个或多个“安全状态”来防止违反安全目标。安全状态可以解释为“发生故障后在规定的时间内保持功能”，这与我前面讨论的失效操作系统注意事项正好相符。这种状态（**图 2** 中称为“功能简化的安全状态”）需要考虑并分析驾驶员警告和相应状态的风险暴露时间。此外，在分析紧急操作和从一个安全状态转换到下一个安全状态后的紧急操作持续时长时，可以遵循 ISO26262-5:2018,9.2。

系统设计人员采用了多种技术来改善中间安全状态、风险暴露时间和紧急操作时间间隔。其中一些技术依赖于双绕组电机等机电冗余概念。这些新型电机也称为双定子或双反逆变器电机，由两个独立驱动的定子线圈和一个转子构建而成。该设计有助于确保当其中一个定子发生故障时，冗余定子以及转子将保持活动状态。在这种情况下，故障路径的预期安全要求实际上是“设计为失效防护”，以免妨碍正常定子路径的运动。在**图 2** 所示的情况下，这种单定子操作将归类为“功能简化的安全状态”。

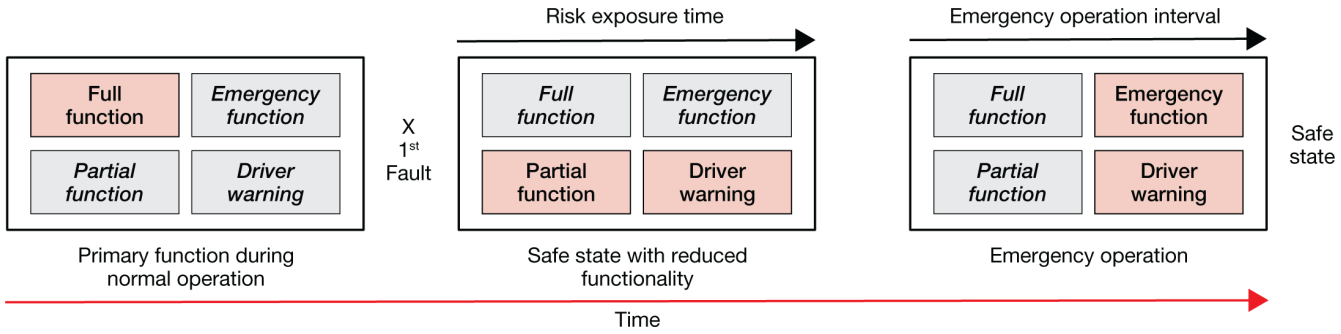

***图 2.** 失效操作系统的操作状态；浅红色框显示活动功能，浅灰色框显示非活动功能。*

还有其他方法可以将违反安全目标的残余风险降低到 1 FIT（时基故障）级别，其中包括增加这种冗余，以包含单独的电源（电池）；单独的通信通道；甚至是将系统与独立的 12V/48V 或 12V/600V 电源网进行集成。

动力总成电气化以及额外的功能安全考量

“**模拟组件推动汽车应用的功能安全开发**”白皮书重点介绍了助力转向和制动等电动系统。随着动力总成的电气化和锂离子电池的引入，在设计这些系统时，更加需要考虑相关安全标准。虽然电气化动力总成的安全目标类似于适用于执行器的安全目标（收到指令时运动、未收到指令时不运动、不妨碍运动），但锂离子电池的安全目标是防止电池在超出电压和温度安全限制的条件下运行。

关于再生充电系统，一个问题是电机发电机等发电系统可能给电池过度充电。这种可能性需要新的创新安全功能和做法来防止违反安全目标。

高温应用中的功能安全

执行器和驱动电子设备通常直接安装在变速模块上，并暴露在高达 150°C 的高温环境中。要让电子设备在这些温度下正常工作，需要专门设计的集成电路 (IC)，此类电路可以承受高达 175°C 的半导体结温。鉴于时基故障率与温度之间具有指数相关性，设计人员在评估时基故障率时必须仔细考虑这些高温应用的任务剖面。为了满足这些要求，TI 提供了 AEC-Q100 0 级功能安全器件（器件型号后标有“E”），这些器件经过精心设计，能够在高达 150°C 的环境温度和高达 175°C 的结温条件下工作。

人为因素

ISO TC22/SC32/WG8 工作组引入了预期功能安全 (SOTIF) 概念，以便将来在 ISO/公共可用规范 (PA) 21448 中发布。SOTIF 旨在建立一个框架，用于识别、验证和确认高级驾

驶辅助系统 (ADAS) 和自动驾驶车辆的不合理风险，甚至是包括没有硬件和软件故障（失效）的情况下。

到目前为止，我重点介绍了失效防护和失效操作系统（强调“失效”一词），但自主系统需要进一步考虑没有失效的情况。自主线制系统会仿真触觉反馈，以弥补驾驶员习惯的机械反馈。在线控转向系统中，电机安装在方向盘上，用于模拟来自转向柱的机械反馈。线控制动系统通常会实现类似的触觉执行器。这些触觉机制依赖传感器和复杂算法的组合驱动触觉执行器来提供反馈。

虽然 ISO26262:3:2018 适用于分析反馈执行器发生故障的情况，但它不能处理这样的情况，即反馈执行器工作正常，但算法收到无法正确解析的意外传感器信息。这种情况可能会导致向驾驶员提供错误的触觉反馈，从而导致未知且不安全的转向操控。SOTIF 试图为这类情况提供一个框架。

应对功能安全系统不断发展而带来的挑战

随着安全系统从失效防护系统发展到失效操作系统，以及电气化传动系统和变速器的快速发展，开发人员需要实施创新的方法来避免故障和检测故障，同时还需要规划与进入和退出安全状态相关的策略。

TI 的电源管理和模拟信号链产品系列可以提供完整的系统解决方案来应对这些挑战。安全电源管理 IC（比如 **TPS653853-Q1**）以及电机驱动器（**DRV3245Q-Q1**（AEC-Q100 1 级）和 **DRV3245E-Q1**（AEC-Q100 0 级））解决了失效操作、线控和高温安全系统中的多种系统集成挑战。

其中的一些优势包括：

- 提供引脚对引脚且软件兼容的 AEC-Q100 1 级 (Ta = 125°C) 和 AEC-Q100 0 级 (Ta = 150°C) 可扩展版本。
- 在单定子或双定子电机系统中提供 ASIL-D 系统功能。
- 借助针对性能和物料清单进行优化的架构，降低电路板上半导体元件数量翻倍而产生的成本影响。
- 能够将 IC 时基故障率整合到系统级时基故障率计算中，包括为高温安全应用定制的任务剖面。
- 提供 IC 级别的时基故障率、故障模式影响和诊断分析。

此外，TI 提供 IC 级硬件指标的假设，并支持开发人员针对特定系统调整 IC 级硬件指标。

要开始进行电机系统安全开发，请考虑将 **DRV3245Q-Q1 评估模块**（随附多个 TI 安全外设）与 **Hercules™ TMS570LS12x LaunchPad™ 开发套件**配合使用。下面的 **图 3** 显示了与该开发套件配合使用的 DRV3245Q-Q1 评估模块。

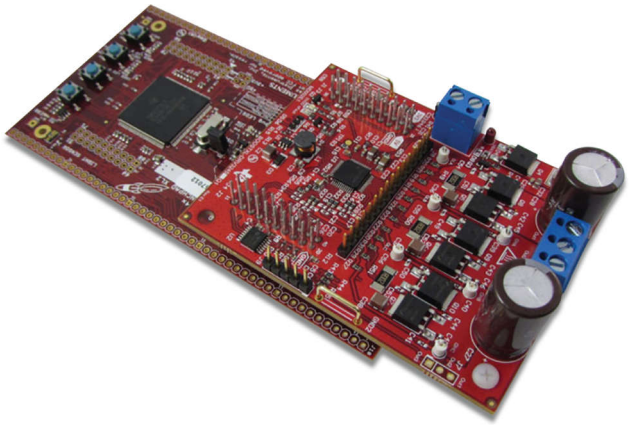

图 3. *DRV3245Q-Q1 汽车类三相电机栅极驱动器评估模块 (BOOSTXL-DRV3245AQ1)。*

相关内容

- 请参阅 **ISO 26262-2:2018 标准**。
- 下载 **DRV3245Q-Q1 数据表**和 **DRV3245E-Q1 数据表**。
- 了解更多有关 **Hercules LaunchPad 开发套件**的信息。
- 阅读白皮书“**推动交通运输领域的绿色革命**”。

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