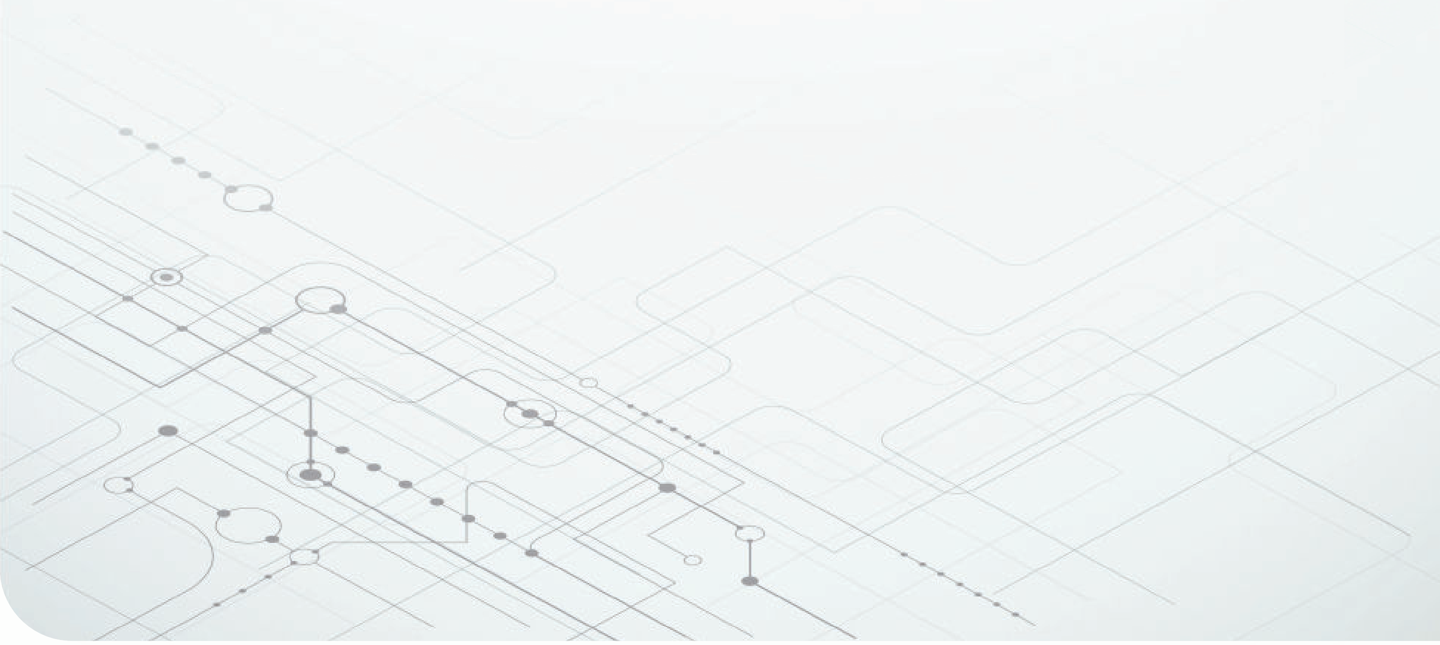
Actuator Design Trends for Functional Safety Systems in Electric and Autonomous Vehicles

Anuj S. Narain
Product Marketing Engineer
Motor Drivers
Texas Instruments



Analog components developed for functional safety applications are enabling the creation of sophisticated electrical actuation systems for electrified, by-wire and fail-operational vehicle architectures.

Four automotive trends – connected, autonomous, shared and electric, also known as CASE – are the most exciting automotive developments since the first Model-T rolled off the assembly line over a century ago. Cleaner, safer and more efficient cars will keep cities clean while reducing our dependence on nonrenewable energy sources.

These trends are intersecting in an interesting way at the powertrain and chassis architectural levels. Traditional driver-directed functions are being replaced with automated functions that have the intelligence to operate in safer, more efficient ways. In this white paper, I focus on the impact of CASE trends on electrically actuated systems.

Welcoming the by-wire era – this time with trust

Technologies like steer-by-wire, brake-by-wire, shift-by-wire and electrified powertrains present a whole new set of exciting challenges for designers of these systems.

The transition to electrical actuation of vehicle functions inherently means fewer mechanical components, which in turn reduces weight, eliminates common mechanical failure modes and enables the integration of smart features. For example, a steer-by-wire system that can intelligently adapt steering responses to road and weather conditions will improve vehicle dynamics and increase efficiency.

Another example is automatic shift and shift-by-wire technology, where an electrical actuator handles the transmission's shift functionality in conjunction with the most efficient operating points of the engine. These systems have a safety benefit of helping prevent inactive or parked vehicles from rolling forward or backward.

Figure 1 shows actuators in a by-wire system that includes steering, transmission and breaking.

Although the hardware and software components required for by-wire systems have been available for several years, trust from consumers has been elusive.

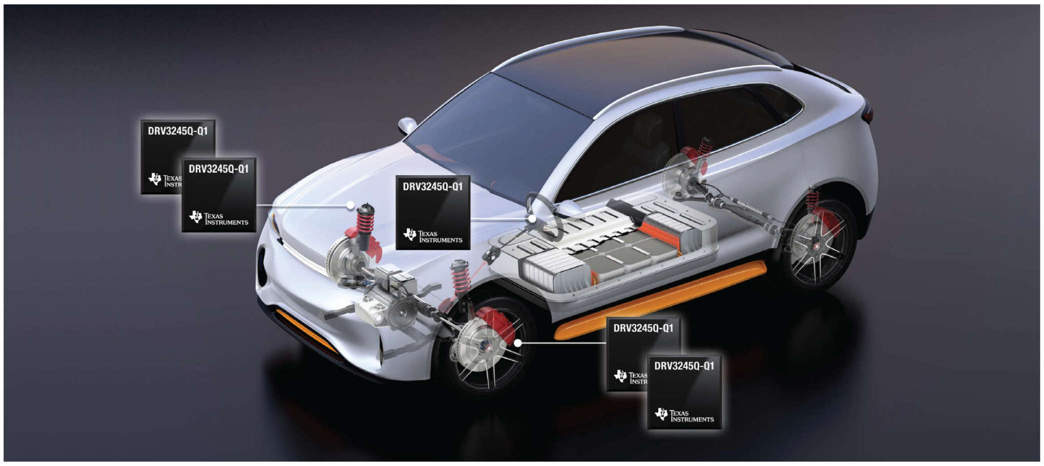


Figure 1. Automotive Actuators That Will Transition to By-wire Control – Steering, Braking and Transmission – Can Benefit from Using TI Motor Drivers for Functional Safety Applications.

“Fail-safe” systems transition to “fail-operational” systems

As actuators move from using mechanical to electrical energy, safety architectures will need to evolve. Most electric actuators in safety systems today retain their original mechanical components for redundancy.

Take an electric braking system, for example, where the mechanical linkage of the pedal to the brake cylinder provides redundancy against failure of the electric system – albeit with a gargantuan stomp on the brake pedal. Electrical braking systems are architected as “fail-safe,” which means that if they were to fail, they would fail in a manner that would not impede the motion of any redundant measures (in this case, the stomp).

As autonomous architectures evolve, the reliance on mechanical redundancy diminishes because humans are removed from the control loop, leading to a whole new class of “fail-operational” systems. An example of a fail-operational system is this same braking system in an autonomous vehicle where the driver is unavailable for a period of time after the electrical brake actuation system has failed. The system (note, not the integrated circuits) is expected to continue operation in this event and brake the vehicle.

The main safety considerations for designing such a system are:

- The fault tolerance and Automotive Safety Integrity Level (ASIL) of the system.
- The allowable functional degradation of the system after the first fault has occurred.
- The emergency function, driver warning and its emergency operational duration.
- The required ASIL level for the system as it transitions to and from safe states.

In order to analyze the safety goals and safe states for fail- operational systems (using **Figure 2** for guidance), we can refer to the second edition of International Organization for Standardization (ISO) ISO26262-3:2018 Clause 7, which states that a safety goal violation can be prevented by transitioning to or maintaining one or more “safe states.” A safe state can be interpreted as “maintained functionality in the case of failure over a defined time,” which fits well into the considerations I’ve discussed for fail-operational systems. This state, described in **Figure 2** as “Safe state with reduced functionality,” requires consideration and analysis of the driver warning and the risk exposure time for the state. Additionally, ISO26262-5:2018,9.2 can be applied when analyzing the emergency operation and the emergency operation duration after the transition from one safe state to the next.

System designers have adopted several techniques in order to improve the intermediate safe states, risk exposure times and emergency operation time interval. Several of these techniques rely on electromechanical redundancy concepts like dual-winding motors. These new motors, also known as dual-stator or dual-inverter motors, are built with two individually driven stator coils and a single rotor. This design helps ensure that if one of the stators fails, a redundant stator – and hence the rotor – will remain active. In this case, the expected safety requirement of the failing path is in fact “designed to fail-safe,” so as to not impede the motion of the healthy stator path. In the context of **Figure 2**, this single stator operation would be classified as “Safe state with reduced functionality.”

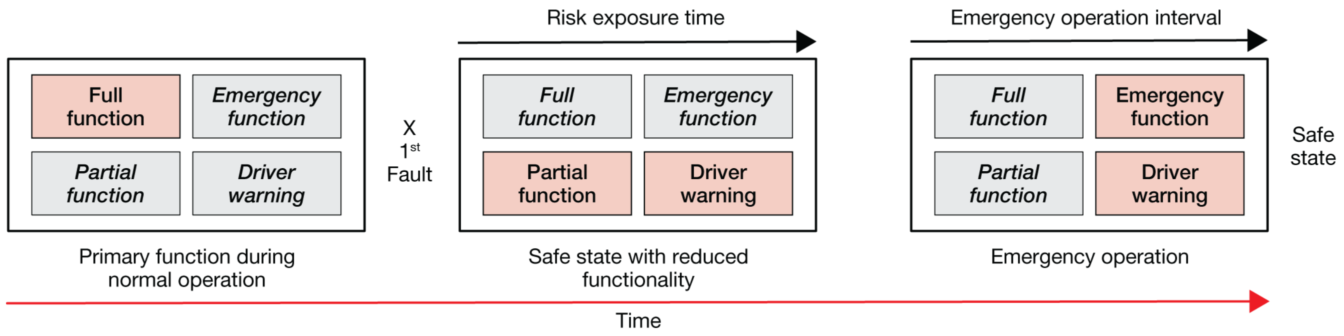


***Figure 2.** The States of Operation of a Fail-operational System; the Light Red Boxes Show the Active Function, and the Light Grey Boxes Show the Inactive Function.*

Other approaches to reduce the residual risk of a safety goal violation to the 1 FIT (Failure in Time) level include increasing this redundancy to encompass separate supply sources (batteries), separate communication channels, and even integrating systems with independent 12-V/48-V or 12-V/600-V power nets.

Electrification of the powertrain and the added considerations for functional safety

The white paper, "**Analog Components Advance Functional Safety Development for Automotive Applications**," focuses on electrically actuated systems, such as power steering and braking. Electrification of the powertrain and the introduction of lithium-ion batteries increases the need to design these systems with safety standards in mind. While the safety goals in electrified powertrains are similar to those analyzed for actuators (move when told, do not move when not, do not impede motion), lithium-ion batteries have the safety goal of preventing battery operation outside voltage and temperature safety limits.

One concern with regenerative charging systems is the ability of a generating system like a motor generator to overcharge batteries. This possibility requires new and innovative safety features and practices to prevent violation of the safety goal.

Functional safety in high-temperature applications

The actuator and the drive electronics are often mounted directly on the transmission block and exposed to ambient temperatures as high at 150°C. Having the electronics function through these temperatures requires specially designed integrated circuits (ICs) that can withstand semiconductor junction temperatures as high as 175°C. Given the exponential dependence on temperature, designers must consider the mission profiles for these high-temperature applications carefully when assessing FIT rates. In order to meet these requirements, TI offers AEC-Q100 Grade 0 functional safety parts (identified with the designation "E" after the part number) that are designed and qualified for ambient temperatures up to 150°C and junction temperatures up to 175°C.

Human factors

The ISO TC22/SC32/WG8 working group introduced the concept of safety of the intended function (SOTIF) for future publication in ISO/publicly available specification (PAS) 21448. The purpose of SOTIF is to create a framework to identify, verify and validate unreasonable risks for advanced driver assistance systems (ADAS) and autonomous vehicles, even in the absence of malfunctions (failure) of hardware and software.

So far, I've focused on fail-safe and fail-operational systems (emphasis on the word "fail"), but autonomous systems require further considerations in the absence of failures. Autonomous by-wire systems simulate haptic feedback to make up for the mechanical feedback that drivers are accustomed to. In steer-by-wire systems, a motor is mounted on the steering wheel to simulate the mechanical feedback from the steering column.

By-wire braking systems often implement a similar haptic actuator. These haptic mechanisms rely on a combination of sensors and complex algorithms that actuate the haptic actuator to provide feedback.

While the application of ISO26262:3:2018 is suitable for analyzing situations where the feedback actuator fails, it does not address situations where the feedback actuator is operational but the algorithm is presented with unexpected sensor information that it cannot interpret correctly. This scenario could lead to incorrect haptic feedback to the driver, resulting in an unknown and unsafe steering maneuver. SOTIF attempts to provide a framework for these scenarios.

Meeting the challenges of evolving functional safety systems

With the evolution of safety systems from fail-safe to fail-operational systems and the rapid advancements in electrified drivetrains and transmissions, developers need to implement innovative methods for fault avoidance and fault detection, while also planning strategies for potential transitions to and from safe states.

TI's portfolio of power management and analog signal chain products can provide a complete system solution to meet these challenges. Safety power management ICs, like the **TPS653853-Q1**, along with motor drivers, like the **DRV3245Q-Q1** (AEC-Q100 Grade 1) and **DRV3245E-Q1** (AEC-Q100 Grade 0), solve several system integration challenges in fail-operational, by-wire and high-temperature safety systems.

Some of these benefits include:

- Offering scalable, pin-to-pin and software-compatible AEC-Q100 Grade 1 (Ta = 125°C) and AEC-Q100 Grade 0 (Ta = 150°C) versions.
- Providing systematic capability of ASIL-D in single-stator or dual-stator motor systems.
- Reducing the cost impact of doubling the semiconductor content on the board with an architecture optimized for performance and bill of materials.
- Enabling integration of IC FIT rates into system-level FIT-rate calculations, including mission-profile tailoring for high-temperature safety applications.
- Providing FIT rates and failure mode effects and diagnostic analysis at the IC level.

Additionally, TI provides the assumptions of IC-level hardware metrics and support for adjusting the IC-level hardware metric for the developer's specific system.

To get started with safety development for a motor system, consider pairing the **DRV3245Q-Q1 evaluation module**, which ships with a host of TI safety peripherals, with the **Hercules™ TMS570LS12x LaunchPad™ Development Kit**. **Figure 3** below shows the DRV3245Q-Q1 evaluation module paired with the development kit.

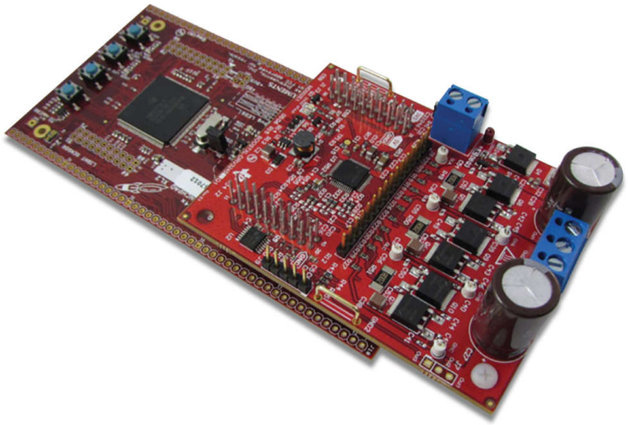


Figure 3. *DRV3245Q-Q1 Automotive 3-Phase Motor Gate Driver Evaluation Module (BOOSTXL-DRV3245AQ1).*

Related content

- See the **ISO 26262-2:2018 standard**.
- Download the **DRV3245Q-Q1 data sheet** and the **DRV3245E-Q1 data sheet**.
- Learn more about the **Hercules LaunchPad development kit**.
- Read the white paper, "**Driving the Green Revolution in Transportation**."

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