Analog components advance functional safety development for automotive applications

Texas Instruments

Anuj S. Narain
Systems, Marketing and Applications Manager
Motor Drivers
Texas Instruments

Analog SafeTI™ components can make it easier for manufacturers to design products that meet functional safety standards while getting to market quickly with their safety-critical systems.

As automotive manufacturers race to relieve drivers of the mundanity of their daily commutes with the arrival of self-driving and autonomous vehicles, the role of functional safety in the electronics that enable this fascinating future is larger and more critical than ever. Increasing focus on safety-critical applications in automotive environments presents a unique challenge to the engineering teams designing electronic control units (ECUs) for these applications.

Hardware and software engineers who have traditionally focused on designing electronics for the highest performance, efficiency, robustness and cost must also ensure that their designs can meet the functional safety requirements of the applications. This white paper aims to explain how this safety development process can be simplified through the adoption of analog safety components.

Introduction

The ISO 26262 standard released in 2011 provides a common framework within which safety-related electrical systems can be developed [1]. While adherence to functional safety opens up new business opportunities, the complexity of developing these solutions and the interaction between hardware teams, software engineers and safety experts often generate more questions than answers. Adding to this is the complexity and interaction between the many semiconductor components on each ECU, along with each component's unique failure modes.

Developing products with functional safety involves a risk-based analysis and concurrent application of best practices and measures in the development process. Analyzing system-failure-modes with their frequency and severity, while including monitoring and redundancies, attempts to ensure that a system's failure rate is low enough for safety-critical applications. The ISO 26262:2011 standard provides a common framework that enables the electronics supply chain, including car manufacturers, Tier1, Tier2 and integrated circuit (IC) suppliers, to design and develop their products with common development practices. This standard ensures that compliance and safety information can freely transcend the supply chain.

Functional safety system developers evaluated that the system's safety-related failures in-time (FIT) rate is one of the most important design parameters. A system's FIT rate is determined by the number of random failures that can be expected in one billion (10^9) device-hours of operation. The FIT rate of each safety-related element is calculated and combined for the overall system. The objective

is to ensure that the residual risk of a safety goal violation due to random hardware failures is sufficiently low. **Table 1** lists the target FIT values versus the Automotive Safety Integrity Level (ASIL) requirements. **Table 2** lists examples of automotive systems and their associated ASIL requirements.

ASIL	Random hardware failure target values
D	< 10-8 h-1 (10 FIT)
C	< 10-7 h-1 (100 FIT)
B	< 10-7 h-1 (100 FIT)

Table 1. *Probabilistic metric for random hardware failures (PMHF) target values for the maximum probability of the violation of each safety goal due to random hardware failures.*

Level	Application
ASIL-D	Electric power steering , braking
ASIL-C to D	Engine (ICE) management, transmission
QM to B	Pumps, instrument cluster

Table 2. *Examples of automotive systems and the highest target ASIL requirement.*

Functional safety beyond microcontrollers

As the ISO 26262 specification matured, IC suppliers introduced safety innovations using microcontrollers to maximize failure detection and mitigation, while minimizing software overhead. Developed using ISO 26262 certified processes, these microcontrollers use techniques like dual-CPUs in lock-step with built-in self-test (BIST), error-correcting code (ECC), loopback, and so on. The TI Hercules™ TMS570 ARM® Cortex® based microcontroller is among the industry's first automotive safety microcontrollers.

While safety microcontrollers provide a crucial first step in functional safety development, IC suppliers like Texas Instruments (TI) continue to expand their focus on developing analog components for functional safety applications, especially in the areas of motor drives and power management. Bringing functional safety capability into analog components allows the system to be architected where analog components no longer need to be treated as safety "black boxes" for safety analysis. Additionally, analog products architected specifically for functional safety applications also can be leveraged for more effective and elegant integration of safety functions for the ECU.

Functional safety in analog IC components

Functional safety development for analog IC components is performed as a safety element out of context (SEooC) development. SEooC are safety-related components designed in a way that they can be deployed into any system. IC design and development requirements are derived by the assumption that the component may be integrated into a generic and representative end application. Motor system ECUs used in electric power steering (EPS) and braking are examples of system assumptions for SEooC developments. Motor system ECUs used in EPS include a microcontroller, sensors, power management IC (PMIC) motor driver, and field-effect transistors (FETs). The motor driver is used to control and sequence the power FETs that drive the motor. **Figure 1** illustrates the typical components of an EPS ECU.

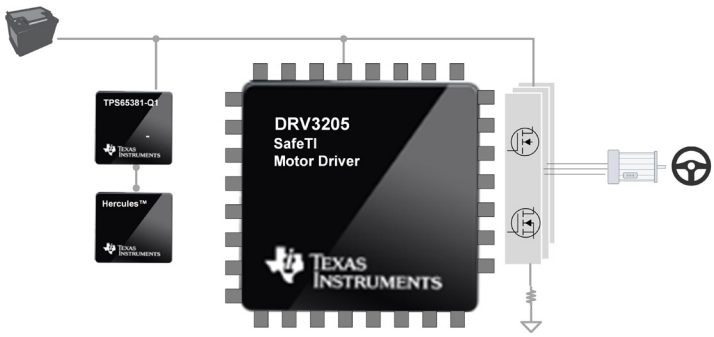

Figure 1*. Typical circuit components of an electric power steering ECU.*

During SEooC development, a failure-mode analysis of the analog component in the context of the assumed system is performed. This analysis reveals various system failure modes and allows the IC definer to add and design circuitry that can help diagnose and protect the system from system failures. Potential failures inside the analog IC component include the loss of critical functions like internal voltage regulators, voltage references and clocks. These failure modes can be mitigated through a combination of built-in self-test methods, as well as design layout practices to ensure that critical signals are routed with physical (spatial) separation.

The SEooC development always commences with a target hardware safety requirement and ASIL level. These mitigation actions are implemented with the goal of demonstrating the target requirements in the assumed system.

The DRV3205-Q1, a three-phase automotive gate driver with three current shunt amps and enhanced protection and diagnostics, is the world's first motor driver in mass production that is developed with ISO 26262 as an SEooC with ASIL Level D, or ASIL-D systematic capability.

Managing random and systematic faults

Meeting safety requirements requires the management of both random and systematic failures. Random failures result from random defects inherent to the process, design or usage condition. Examples of random failures in analog ICs include failure of internal clocks, internal voltage regulators, and data corruption failures. Techniques to detect and handle these random faults include clock monitoring, internal voltage regulator monitoring and checksum schemes.

The DRV3205-Q1 motor driver features several unique circuit implementations for management of random faults:

- **Clock Monitoring:** Monitors loss of clock to detect failure of internal oscillators
- **Internal Regulator Monitoring:** Monitors internal regulators that power digital or analog circuits for failure.
- Built-in self-test: Detects latent faults by implementing circuits to inject or emulate faults at power-up, and verifies that detection circuits are responsive using logic built-in self-tests to test the digital circuitry.
- **Checksums:** Ensures that the IC configuration is not altered during operation by implementing safety-critical registers and memory blocks

Figure 2 depicts some of the unique circuit implementations for management of random faults on the DRV3205-Q1.

Systematic faults, on the other hand, result from inadequacies in the design or manufacturing process. Examples of systematic failures include gaps in development processes and adherence to best practices. The rate of systematic failure can be reduced through continual and rigorous development process improvements as well as through applying robust manufacturing processes.

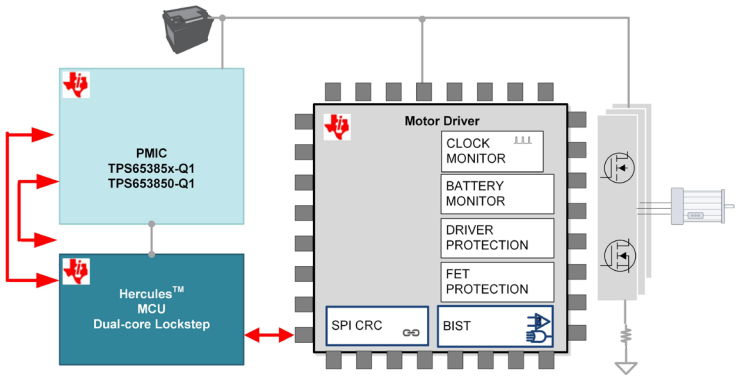

***Figure 2**. Random fault management for a motor driver.*

At TI, development of analog products for functional safety applications is done in adherence with specifications that define the work flow, documentation, planning, reviews, checklists and audits necessary to develop hardware to comply with the ISO 26262 standard.

System safety considerations

While the microcontroller and each analog component can be independently developed to meet system safety targets, the SEooC approach allows IC developers to comprehend system safety requirements during definition of the IC. Broadly speaking, we have two possible approaches, depending on the ECU developer's choice of safety architecture. These architectures with their typical configurations are shown in **Figure 3**.

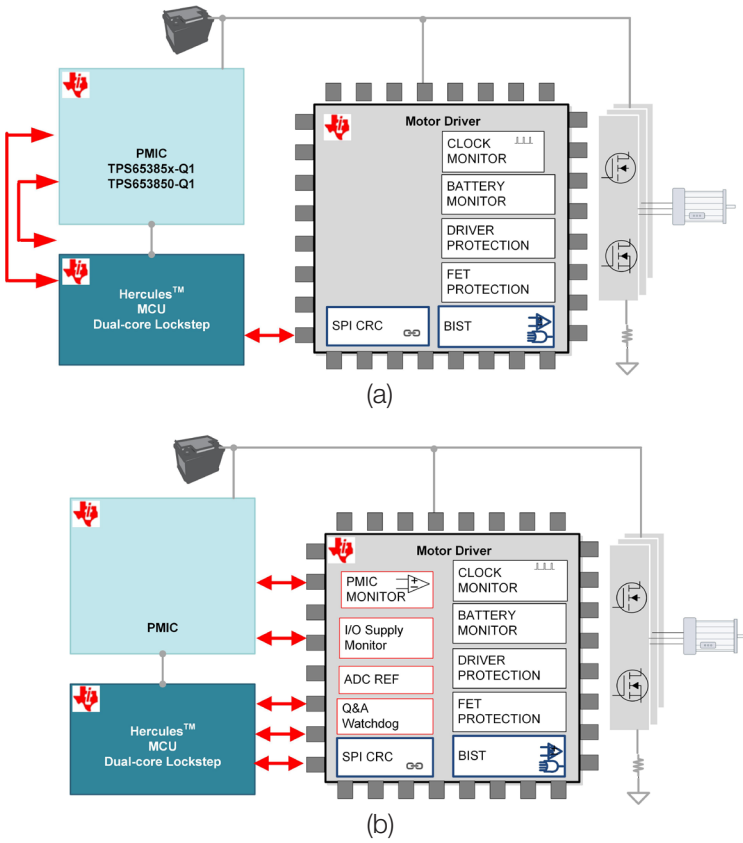

***Figure 3**. Illustration depicts both distributed and integrated safety concepts (a and b, respectively).*

The first approach to comprehend system safety requirements is the *distributed safety concept*. This approach typically distributes the system monitoring functions across various components on the ECU and can include discrete system monitoring components. Oftentimes discrete watchdog timers, voltage references or supervisor microcontrollers are added for system monitoring.

Alternatively, the *integrated safety* concept integrates system monitoring functions on one of the analog safety components present on the board. Examples of functions that can be integrated on the analog safety components are microcontroller watchdog timers, PMIC monitors, input/output (I/O) supply monitors, and analog-to-digital converter (ADC) reference monitors. Integrating these functions on a single IC can simplify safety development considerably given that fewer components are required in the safety analysis.

Both the distributed and integrated safety concepts each have their own merits. Making the choice is purely a decision based on system and business priorities. TI architects its products to fit into both concepts, enabling a more diverse and flexible product offering for system developers.

The DRV3205-Q1 motor driver was developed for the highest integration of system safety monitoring functions.

- *Question and answer watchdog timers* ensure that the generated challenge question is answered only after exercising the arithmetic logic unit (ALU) on the microcontroller.
- *ADC reference monitor* ensures that the measured system parameters are referred to the intended analog voltage scale by independently monitoring the ADC reference voltage.
- *I/O supply monitor* ensures that the I/O signals are at strong levels

How does all of this FIT

ECU developers of functional safety systems require the FIT rate analysis of the various IC components used in the ECU. These individual FIT rates are used to calculate a system FIT rate for the ECU, and to subsequently assess whether the system's desired ASIL metric has been met.

For analog components, FIT rates vary by products and manufacturers as well as the functional safety approach of choice. FIT is an important selection criterion for the ECU developer because it determines the system's safety architecture and length and effort of the safety development cycle. The three most common FIT rates and analysis that IC suppliers provide are depicted in **Figure 4**.

As depicted in **Figure 4**, following are the three most common FIT rates and analysis that IC suppliers typically provide:

- **Black box:** This FIT rate analyzes the IC as a black box and are agnostic to the mode of failure within the IC, or the interactions between the failures. Any failures are viewed as single points of failure, and only comprehend the FIT rates of the IC process and IC package.
- **Black box with a window:** These FIT rates are calculated by analyzing each IC block and circuit for failure, and reporting the FIT rates and the distribution/probability of the failure modes.
- **White box:** These FIT rates can be provided only through the SEooC development under the guidelines of ISO 26262. White box FIT rates are calculated by analyzing each IC block and circuit for failure rates and failure rate distributions, then applying the effect of the added diagnostic circuits added to mitigate those failures.

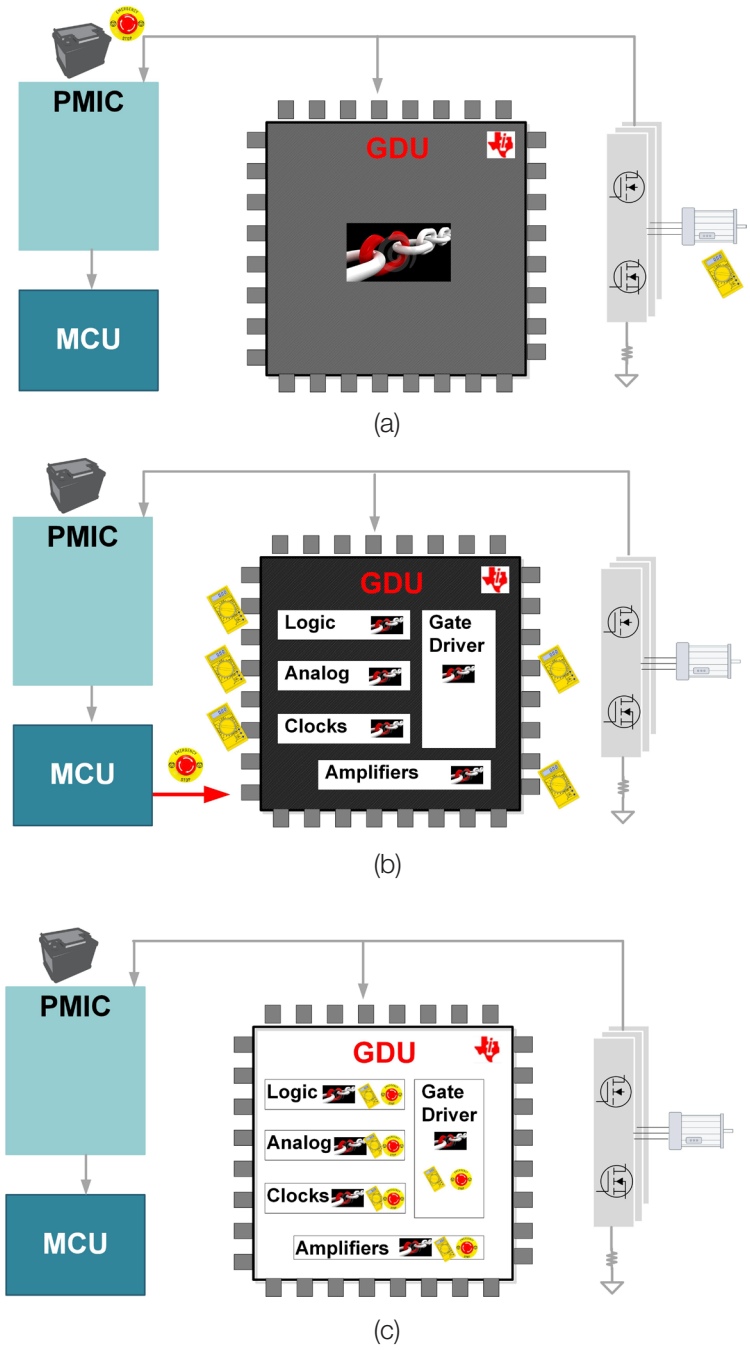

***Figure 4**. Common approaches to FIT rate calculation in analog components: black box, black box with a window, and white box (a, b and c, respectively).*

With the SafeTI design package, ICs such as the DRV3205-Q1 that are designated as SafeTI products with an ASIL systematic capability assigned to them, can support ECU developers with white box FIT rates.

Some benefits of the FIT rates available with the SafeTI design package are:

- IC FIT rates can be easily integrated into the system-level FIT rate calculations.
- Information and distribution of each failure mode so the ECU developer can comprehend failure modes and make informed failure mitigation decisions based on the application.
- FIT rates and failure mode effects and diagnostic analysis (FMEDA) are available at the IC level.
- Safety analysis is available at the ECU level.
- TI support to recalculate FIT rates for the ECU developer's specific system.

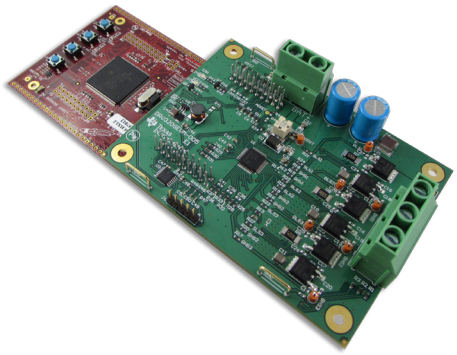

***Figure 5**. DRV3205-Q1 evaluation module paired with the Hercules™ MCU Launchpad development kit.*

To get started with safety development for a motor system, the DRV3205-Q1 evaluation module (EVM), which ships with a host of TI safety peripherals, can be paired easily with the Hercules TMS570LS12x LaunchPad™ Development Kit (**Figure 5**).

Industry leadership in analog safety

With demand for functional safety products increasing, ECU developers need to consider fault management techniques, safety architectures and component FIT rates while selecting analog IC components. Powerful advancements in the development of analog IC components for functional safety applications helps to make the development process easier and faster while saving on development costs.

TI's broad portfolio of analog products in power and signal chain enables unparalleled synergy in the development of analog ICs for safety applications.

References

1. ISO 26262-1:2011 standard
2. Reliability terminology
3. Download the DRV3205-Q1 data sheet
4. Learn more about the Hercules Launchpad
5. Q&A Watchdog Timer Configuration for DRV3205-Q1, Texas Instruments Application Report (SLVA831) October 2016
6. DRV3205-Q1 Negative Voltage Stress on Source Pins, Texas Instruments Application Report (SLVA805) September 2016
7. DRV3205-Q1 Applications in 24-V Automotive Systems, Texas Instruments Application Report (SLVA777) August 2016
8. Electric Power Steering Design Guide With DRV3205-Q1 Texas Instruments Application Report (SLVA722), October 2016

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