WHITE PAPER

Jeff Stafford,
TI Motor Solutions
Texas Instruments

Texas Instruments

Accelerating motor control design for functional safety

Introduction

Designing a differentiated motor drive is a complex task. Often these drives are single processor that combine constraints of real-time embedded designs such as limited memory size and processing time, with the complications that motors bring – electrical noise and faults.

When you add functional safety and certification requirements – the new design, test and documentation deliverables require a significant amount of additional effort. The additional functional safety requirements are often seen as an even bigger constraint and too difficult to deliver a differentiated, functional safety motor drive on time or on budget.

Safety certification efforts directly impact time to market and can often have drastic impact on project costs. Recertification for product updates often becomes a reason to delay or a rationale for skipping design updates altogether.

To help ease the functional safety design process, SafeTI™ design packages from Texas Instruments (TI) for functional safety help solve these issues by easing the design and certification process for designers and allow the engineering and marketing teams' to focus on delivering successful, differentiated products.

Safety is everywhere in today's world

Functional safety standards in a variety of applications, such as automotive systems, industrial automation, household appliances and more, make the world safer for all of us. They also provide an additional opportunity to differentiate your product from competition. The SafeTI design packages for functional safety help designers achieve compliance to international functional safety standards (IEC 61508, IEC 60730 and ISO 26262) and get to market quickly. In some cases, designers will be able to go beyond meeting the basic requirements of the current industry standards and position their products for longer life cycles, avoiding redesign due to evolving standards.

Today, systems are more complex and more dependent on the electronic control of motoring operations that need to meet strict functional safety standards. Whether it is the motor in control of the power steering assist in a car, controlling the lift and doors of an elevator or directly connected to the drum of a front-load washing machine without belts or gears, functional safety in motor operation is fundamentally important. A motor system designed with functional safety will have a lower level of risk from improper operation. When a failure does occur, whether it is a random or systematic fault, the functionally safe design will detect this fault and respond to minimize impact.

SafeTI™ design packages speed functional safety designs and certification

To help designers more easily achieve industry standards, such as IEC 61508, IEC 60730 and ISO 26262, TI's new SafeTI design packages can help accelerate design and certification in areas such as industrial, transportation, energy and medical. This functional safety platform augments TI's 20+ years of safety-critical design expertise and includes design packages with analog companion devices and embedded processors – from microcontrollers to digital signal processors – as well as software, supporting documentation and independent third-party evaluation and certification.

All SafeTI functional safety-enabled embedded processing and analog semiconductor devices include components offered as part of TI's broad product portfolio and are tested to work together in a system. These SafeTI™ hardware components allow designers of safety systems to more easily meet their safety goals without using multiple channels or vendors of system-level hardware.

But it doesn't stop with the hardware. SafeTI design packages include five key components for functional safety:

1. **Functional safety-enabled semiconductor components** developed as safety-standard-compliant items to help enable designers to build safe systems with confidence.
2. **Safety documents, tools and software** to decrease development and certification time. SafeTI documents include a *Safety Manual*, detailing product safety architecture and recommended usage; *Safety Analysis Report* including details of safety analysis and *Safety Report*, summarizing compliance to targeted standards.
3. **Complementary embedded processing and analog components** work together to help designers meet safety standards.
4. **Quality manufacturing process** has been applied to help assure that SafeTI components meet the component-level requirements concerning ISO 9001 or ISO/TS 16949 (including AEC-Q100 for automotive), helping enable the customer to deliver robust solutions.
5. **Safety development process** that follows ISO 26262, IEC 61508 and IEC 60730 requirements, which is assessed by auditors as prescribed by safety standards.

Meeting stringent industry safety standards

International functional safety standards are defined to ensure that functional safety techniques are detailed for a specific industry sector and that these techniques are consistently applied. IEC 61508 is a basic safety standard, which is the basis of all IEC and some ISO functional safety standards. It is used as a basis for sector-specific standards but where these do not yet exist, it is also intended for direct use. Some standards that refer to IEC 61508 include:

- EN 50128 – railway
- IEC 60601 – medical equipment
- IEC 61511 – process industry
- ISO 13849/ IEC 62061 – industrial machinery
- IEC 60880 – nuclear power industry
- IEC 50156 – furnaces

For these specific industry standards, **SafeTI-61508** design packages for functional safety include component-level-compliance to IEC 61508:2010, which supports SIL levels from SIL-1 to SIL-3 and system level compliance to SIL-4. The above standards can be daunting, but the SafeTI™ functional safety design package provides confidence to tackle stringent safety requirements and ease the design and certification process.

Automotive designers can use **SafeTI-26262** design packages for component-level compliance to ISO 26262 safety requirements to support ASIL-A to ASIL-D for applications such as steering, braking, transmission, electric vehicle battery management and advanced driver-assistance systems (ADAS). TI is a member of U.S. and international working groups for ISO 26262.

Designers for household appliances can use **SafeTI-60730** design packages to meet IEC 60730, or related standards UL 1998 and IEC 60335. SafeTI-60730 design packages for functional safety include software certified to IEC 60730 for household appliances supporting Class A to Class C.

Development tools and software for SafeTI design packages

As part of the SafeTI design packages, several development tools and software pieces are available to further ease the design and certification process:

- **Safety-enabled hardware** supports standards-based, safety integrity levels (SIL) enabling designers to build systems with confidence.
- **Safety documents** decrease development and certification time.
- **Compilers for safety:** The SafeTI ARM Compiler Qualification Package establishes confidence in development tools. The kit will help designers document, analyze, validate and qualify use of the TI ARM compiler to help meet the requirements of the ISO 26262 and IEC 61508 standards.
- **GUI-based peripheral configuration tools:** SafeTI HALCoGen graphical user interface works to configure peripherals, interrupts, clocks and other µC parameters and generates peripheral and driver code. Developers can use this to accelerate development on new projects and can import this into **TI's Code Composer Studio™** integrated development environment (IDE) v.5 and select third-party IDEs.
- **MCAL and Safe AutoSAR for ISO 26262:** Designers can get the Microcontroller Abstraction Layer (MCAL) 4.0 from TI and Safe Automotive Open System Architecture (AutoSAR) from TTTech/Vector. ISO 26262 AutoSAR support is available from Vector and Elektrobit.
- **Certifiable RTOS Support for IEC 61508:** Real-time operating system support is available from Wittenstein High Integrity System's SAFERTOS, Micrium's µC/OS, Express Logic's ThreadX and SCIOPTA RTOS.

Integrating safety in motor control systems

A typical motor control system block diagram consists of processing feedback from motor rotor sensors, as well as measuring voltages and currents from the inverter (strategically and deterministically), and then processing this data to be used as inputs to regulate compensation of torque, speed and position control loops to finally generate an appropriate pulse-width modulator (PWM) output to the inverter (Figure 1 on the following page). These closed loops are standard and depend on a great number of components, both hardware

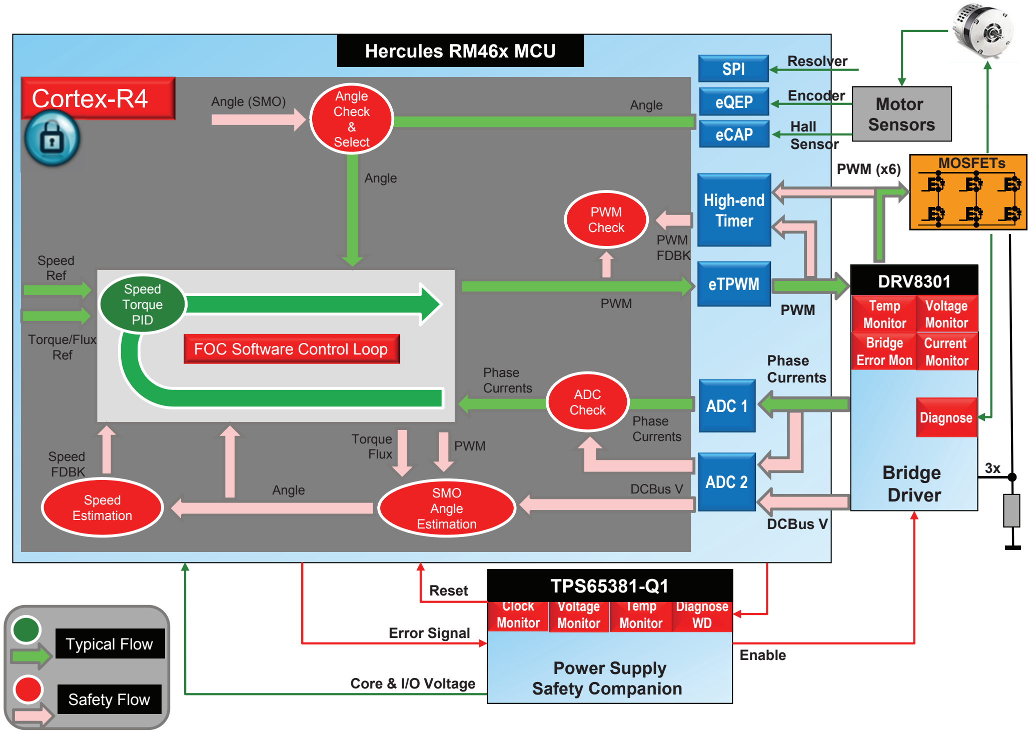


Figure 1. Motor control system block diagram with safety checks.

and software. TI's embedded processors in the SafeTI design package (in this case, microcontrollers) support functional safety throughout these processes.

When measuring the inverter voltages and currents, designers must know if the analog-to-digital converter (ADC) is both functional and producing correct results. A common technique connects a PWM output to an ADC input through a filter. The full-scale ADC range can then be tested. Some TI microcontrollers even integrate a digital-to-analog converter (DAC) to serve this purpose. One method to gain safety coverage is to have multiple ADCs converting the same control signals. This allows a comparison to occur on the actual signal used in the control process. Because many SafeTI MCUs provide multiple ADCs, the same sensor signal can be converted with two separate ADCs, thus reducing common cause failures.

Knowing the motor's exact rotor position is critical to most motor systems. For safety-critical systems using a resolver, encoder or hall sensor, TI provides software that estimates the rotor angle to compare to the angle measured by the electro-mechanical sensor. Microcontrollers in SafeTI design packages include safety features in the hardware (Figure 2 on the following page) versus software to provide the performance headroom to easily include these "self-sensing" angle-estimation routines. This capability, having two separate and diverse channels to obtain the motor's rotor angle, can enable the designer the option to reduce system costs by replacing a more expensive SIL-3 resolver or encoder with a standard version.

The next step is processing these signals. As the leader of commercial lock-step microcontroller architectures, SafeTI microcontrollers provide cycle-by-cycle diagnostics for the CPU. While two CPUs execute the

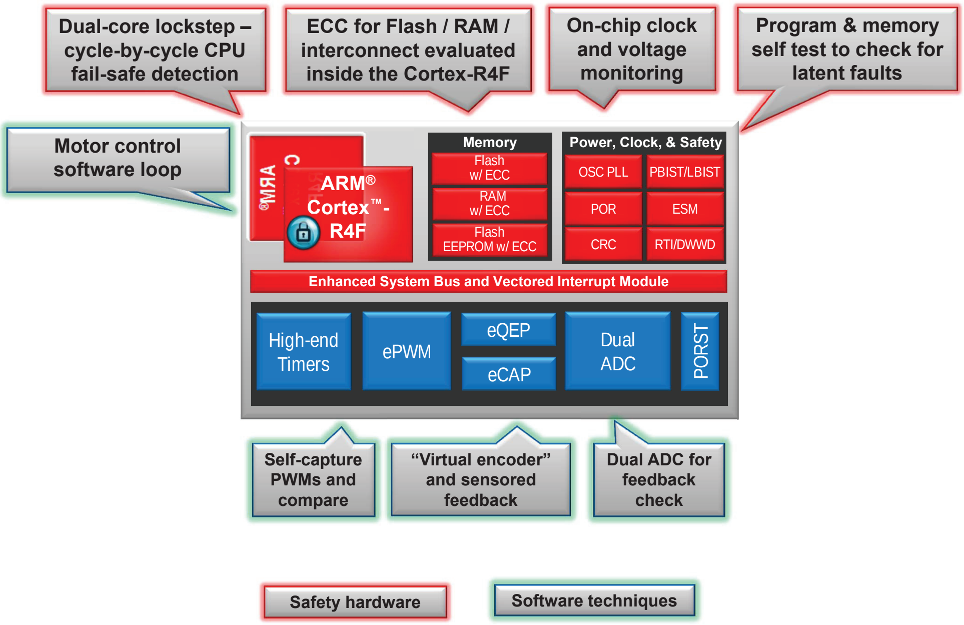

Dual-core lockstep – cycle-by-cycle CPU fail-safe detection
ECC for Flash / RAM / interconnect evaluated inside the Cortex-R4F
On-chip clock and voltage monitoring
Program & memory self test to check for latent faults
Motor control software loop
ARM®
ARM® Cortex™-R4F
Memory
Flash w/ ECC
RAM w/ ECC
Flash EEPROM w/ ECC
Power, Clock, & Safety
OSC PLL
PBIST/LBIST
POR
ESM
CRC
RTI/DWWD
Enhanced System Bus and Vectored Interrupt Module
High-end Timers
ePWM
eQEP
eCAP
Dual ADC
PORST
Self-capture PWMs and compare
"Virtual encoder" and sensored feedback
Dual ADC for feedback check
Safety hardware
Software techniques

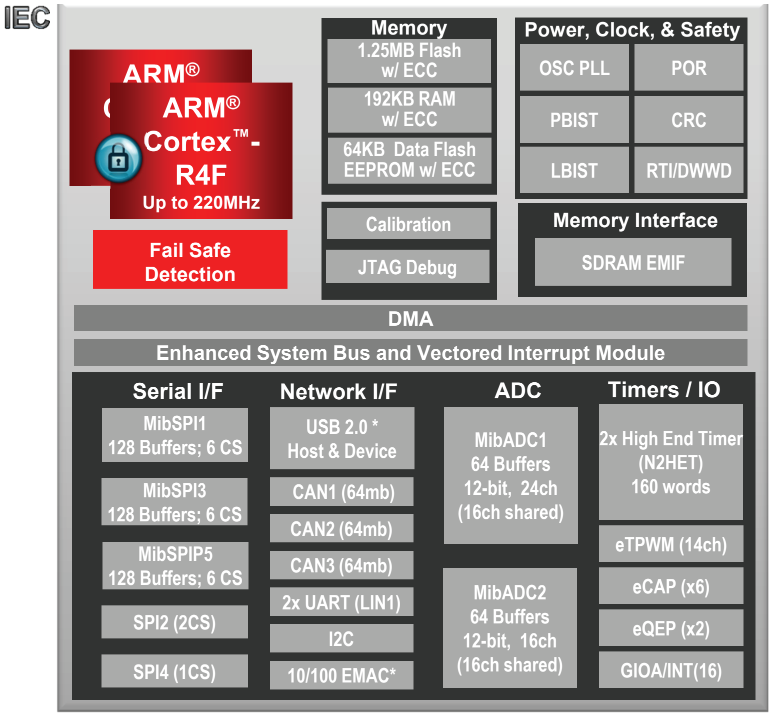
Figure 2. Block diagram of TI safety microcontrollers with hardware safety features.

same code, comparison logic guarantees that each software instruction is executed exactly the same for both CPUs and notifies the system immediately if they do not match. Also, every local Flash and RAM access by these CPUs is checked by a single-bit error correcting and double-bit error detecting (SECDED) error code correction controller (ECC). To extend coverage further, both the CPU and memory have hardware BIST (built-in self test) to verify functionality at start up. Embedded diagnostics also include self-test capability to ensure proper operation before start of safety-critical operation.

With the processing now complete, the next step is to output appropriate PWMs to the inverter. These outputs can be verified by connecting them to input captures. SafeTI microcontrollers provide extra input captures for this purpose with eCAP and high-end timer modules. To get more system coverage, a designer can connect the motor phases to the input captures, using appropriate signal conditioning, to verify that the transitions are within expectations.

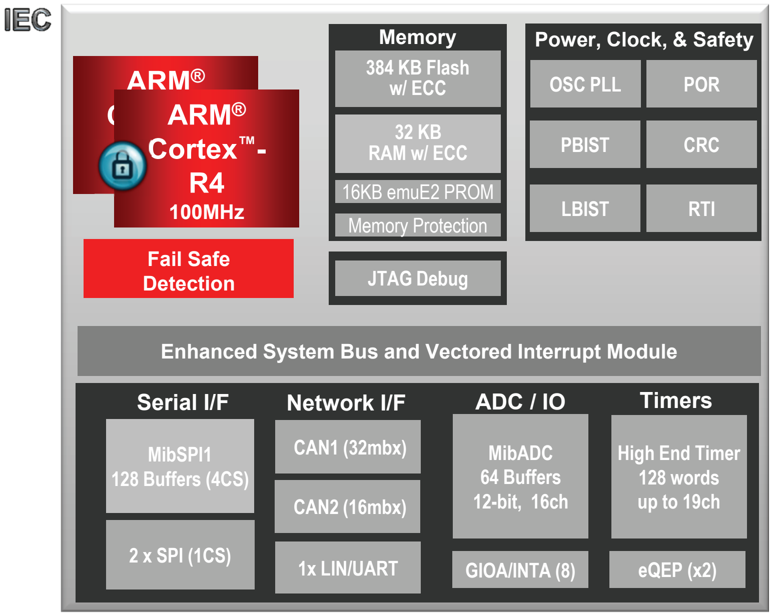
Industrial, medical and energy functional safety motor control SafeTI design packages

The latest microcontrollers introduced as new SafeTI-61508 design packages are optimized for motor control in safety-critical designs. They include the Hercules™ RM46x and RM42x ARM® Cortex™-R4 safety microcontrollers, designed for motor control in industrial automation, medical monitoring and energy applications. The Hercules RM46x/RM42x safety microcontrollers include 15 devices, offer USB and CAN, and operate across the full industrial temperature range. **Hercules RM46x floating-point safety microcontrollers** (Figure 3 on the following page) provide additional memory and performance configurations with expanded motor-control capabilities and pin compatibility with production-qualified **Hercules RM48x safety**



Packages: LQFP: 144pin -20x20; nfBGA: 337 pin-16x16, 0.8mm;
-40 to 105 C Temperature Range

Figure 3. Hercules RM46x safety microcontrollers



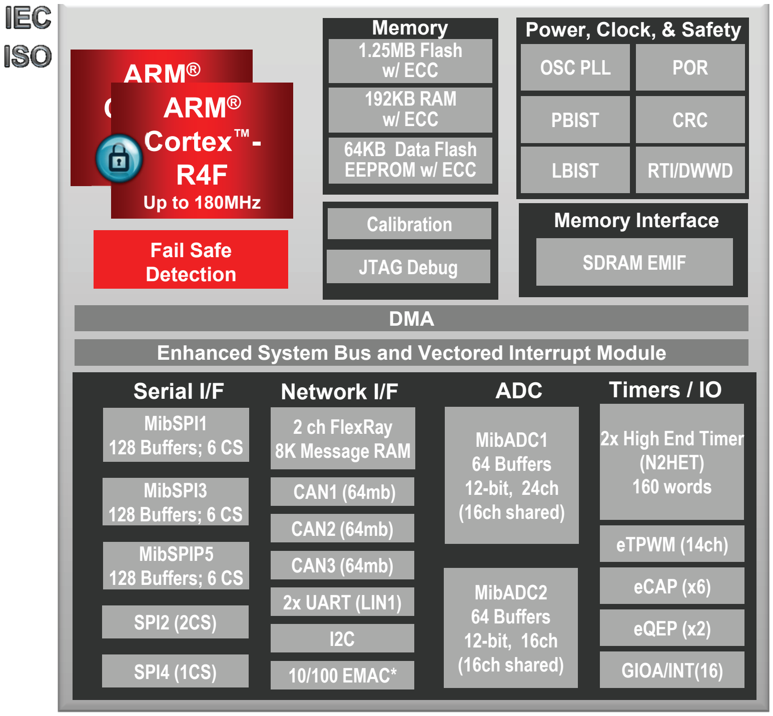
Package: LQFP: 100pin
-40 to 105 C Temperature Range

Figure 4. Hercules RM42x safety microcontrollers

microcontrollers, introduced last year. The new **Hercules RM42x safety microcontrollers** (Figure 4 on the previous page) provide a smaller package, lower cost, entry-line solution with integrated motor control interfaces while also meeting safety standards.

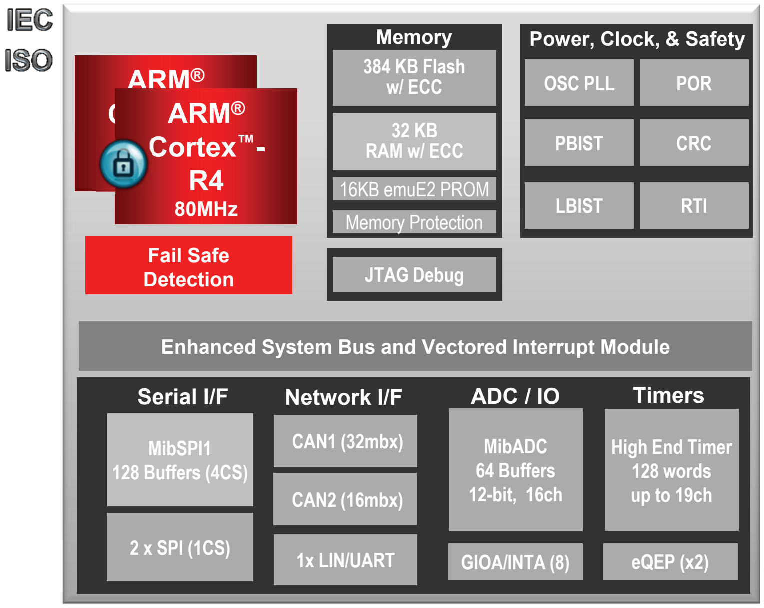
Automotive and transportation functional safety motor control SafeTI design packages

To help speed design and certification for automotive and transportation designs, TI introduced 12 new Hercules TMS570 ARM Cortex-R4 safety microcontrollers as part of the SafeTI-26262 and SafeTI-61508 design packages. These new devices and add FlexRay™ (a safety-centric protocol used primarily in automotive), are AEC-Q100 compliant and operate from –40°C to +125°C for transportation motor applications, such as rail propulsion control, aviation anti-skid control, electric power steering, air-bag deployment, hybrid and electric vehicles, pumps and compressors and more. The newest Hercules TMS570 safety microcontrollers expand the product line to include 36 configurations from which customers can choose to meet application-specific needs. The new **Hercules TMS570LS12x/11x floating-point safety microcontrollers** provide additional memory and performance configurations with expanded motor control capabilities (see Figure 5) while the **Hercules TMS570LS04x/03x safety microcontrollers** provide a smaller package, lower cost, entry-line solution with integrated motor control interfaces (see Figure 6 on the following page).



Packages: LQFP: 144pin -20x20; nfBGA: 337 pin-16x16, 0.8mm;
-40 to 125 C Temperature Range

Figure 5. Hercules TMS570LS12x / LS11x safety microcontrollers



Package: LQFP: 100pin
-40 to 125 C Temperature Range

Figure 6. TMS570LS04x / LS03x safety microcontrollers

TI makes it easier for customers to get started today with the Hercules RM4x safety microcontrollers included in SafeTI-61508 and SafeTI-26262 design packages:

- **Safety documentation** including a safety manual and safety analysis reports, details how to implement Hercules microcontrollers in safety-critical applications, as well as failure modes, effects and diagnostic analysis (FMEDA) that provides the failure rate information needed to meet safety standards.
- **Hercules Development Kits** – Get up and running quickly with a low-cost USB stick for Hercules RM4x microcontrollers (**TMDXRM48USB**) or Hercules TMS570 microcontrollers (**TMDXLS31USB**). Full-featured kits for Hercules RM4x microcontrollers (**TMDXRM42HDK** or **TMDXRM46HDK**) and Hercules TMS570 microcontrollers (**TMDXLS04HDK** or **TMDXLS12HDK**) include a development board, TI's Code Composer Studio™ integrated development environment (IDE), the HALCoGen peripheral configuration tool and a safety demo that showcases BIST execution and error-forcing modes.
- **Hercules Motor Control Kit** – Spin motors more safely in minutes with the Hercules RM46x Motor Control Kit (**DRV8301-RM46-KIT**) or the Hercules TMS570 Motor Control Kit (**DRV8301-LS12-KIT**). Included in the kit is an RM46x controlCARD (**TMDXRM46CNCD**) or TMS570 controlCARD (**TMDXLS12CNCD**), also available standalone, with the TPS65381-Q1 power supply, a DRV8301 EVM and a Teknic servo motor. Also included in the kit is TI's MotorWare™ software, which includes field-oriented-control (FOC) algorithms that support "self-sensing" feedback as a redundant/safe channel to a rotor position sensor and example projects that leverage the ARM® CMSIS DSP library and the HALCoGen peripheral library with built-in safety support.

- **SafeTI ARM® Compiler Qualification Kit** – Establish confidence in your development tools with TI's new Compiler Qualification Kit. The kit will help you document, analyze, validate and qualify your use of the TI ARM compiler to more easily meet the requirements of the ISO 26262 and IEC 61508 standards. An early adopter release was released in October 2012, with a full-featured release following in 1Q 2013.
- **AutoSAR® software for ISO 26262** – Hercules TMS570 microcontroller designers can get the Safe Automotive Open System Architecture (AutoSAR) with protection mechanisms to ASIL D from TTTech/Vector. ISO 26262 AutoSAR support is available from Vector and Elektrobit.

Household appliance motor control SafeTI design packages

The SafeTI-60730 design package includes a safety manual and supervisory software functions and library for added safety. Targeted for cost-effective **C2000™ Piccolo™ microcontrollers**, this package allows the designer to more easily meet IEC 60730 requirements without losing critical real-time motor control performance.

Complementary analog

As part of SafeTI-61508 and SafeTI-26262 design packages, a complementary multi-rail power supply, the TPS65381-Q1 power management integrated circuit (PMIC) combines multiple power supplies and safety features such as voltage monitoring in a single device to reduce design time and board space (Figure 7). Functional safety architecture in the PMIC integrates features such as question-answer watchdog, MCU error-signal monitor, clock monitoring on internal oscillators, self-check on clock monitor, CRC on non-volatile memory and a reset circuit for the microcontroller. In addition, a BIST allows for monitoring the device functionality

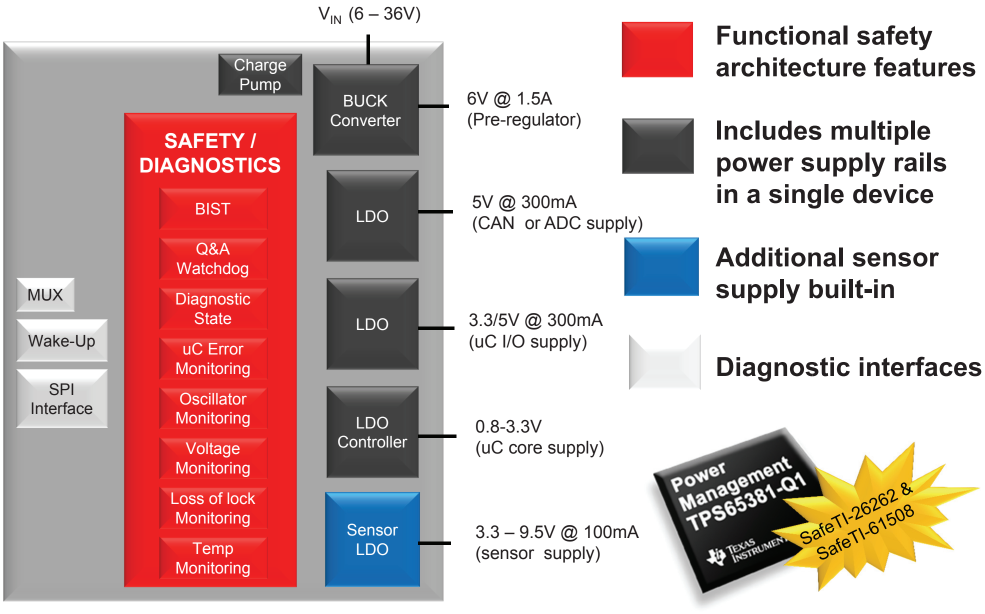

V_{IN} (6 – 36V)
Charge Pump
BUCK Converter
6V @ 1.5A (Pre-regulator)
SAFETY / DIAGNOSTICS
BIST
Q&A Watchdog
Diagnostic State
uC Error Monitoring
Oscillator Monitoring
Voltage Monitoring
Loss of lock Monitoring
Temp Monitoring
MUX
Wake-Up
SPI Interface
LDO
5V @ 300mA (CAN or ADC supply)
LDO
3.3/5V @ 300mA (uC I/O supply)
LDO Controller
0.8-3.3V (uC core supply)
Sensor LDO
3.3 – 9.5V @ 100mA (sensor supply)
Functional safety architecture features
Includes multiple power supply rails in a single device
Additional sensor supply built-in
Diagnostic interfaces
Power Management TPS65381-Q1
Texas Instruments
SafeTI-26262 & SafeTI-61508

Figure 7. The TPS65381-Q1 multi-rail safety PMIC

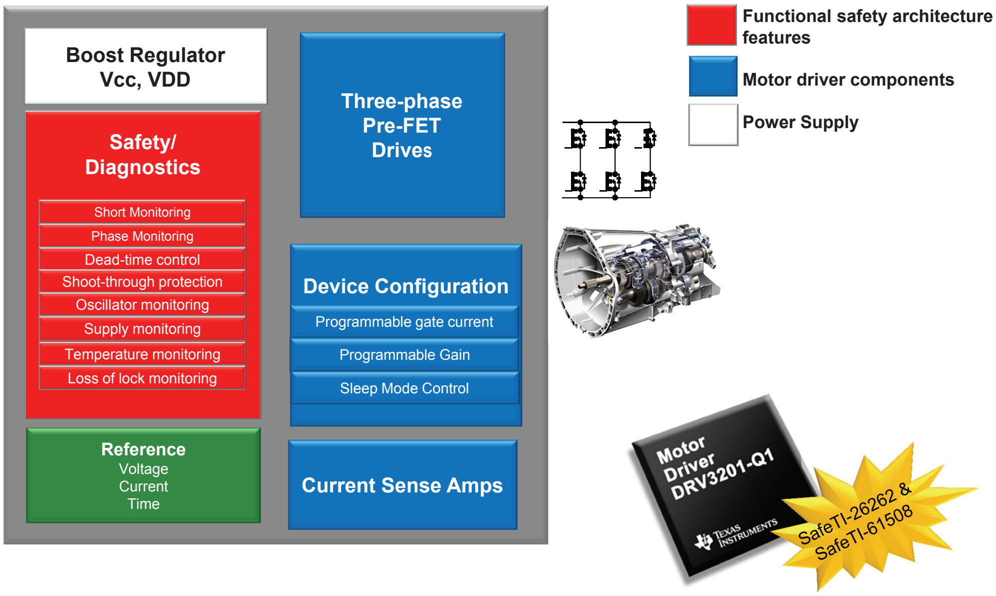


Figure 8. DRV3201-Q1 safety motor driver

at start-up and a dedicated diagnostic state allows the microcontroller to check the PMIC safety functions. These embedded safety features can help remove the need for an additional monitoring microcontroller and reduces cost, board space and software development time.

Also available for functional safety automotive and transportation motor control designs is the DRV3201-Q1 safety motor driver (see Figure 8). First on the market to support start/stop functionality, the motor driver integrates functional safety architecture, such as VDS monitoring, phase comparators, shoot-through protection, dead-time control, temperature warning and protection and battery voltage detection for under- and over-voltage protection. The motor driver also contains a bridge driver dedicated to an automotive three-phase brushless DC motor, providing six dedicated drivers for normal level N-Channel MOSFET transistors up to 250nC charge.

Conclusion

While the world of safety is ever evolving and industry standards become more strict, designs become more complex and certification becomes increasingly complicated. But you can be one click away from easier functional safety designs with the SafeTI design packages that can be found on **www.ti.com/safeti**. On this website, you can search by application or industry standard to find everything for your motor control functional safety designs. And of course, augmented by the largest support network, designers are never left on their own. Learn more today at **www.ti.com/safeti**.

Important Notice: The products and services of Texas Instruments Incorporated and its subsidiaries described herein are sold subject to TI's standard terms and conditions of sale. Customers are advised to obtain the most current and complete information about TI products and services before placing orders. TI assumes no liability for applications assistance, customer's applications or product designs, software performance, or infringement of patents. The publication of information regarding any other company's products or services does not constitute TI's approval, warranty or endorsement thereof.

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