Optimized solutions for safe motion control applications

Texas Instruments

Jamal Karim
Member Group Technical Staff
Principal Field Application Engineer
Texas Instruments, Germany

Designers have always combined hardware and software to ensure functional safety in industrial motor drive. Today's designs have increasingly complex hardware, such as microcontrollers (MCUs), microprocessor units, field-programmable gate arrays and application-specific integrated circuits.

Software now includes sophisticated control algorithms, state machines and user interface functions. So assessing and implementing the complexity of hardware and software integration is challenging for designers.

Note: This paper was first published in the conference proceedings for PCIM Europe, held May 8th 2019.

In addition, depending on the architecture (isolation barrier), safety implementation at a system level requires a specific split of subsystems with dedicated hardware and software diagnostics to achieve the targeted safety integrity level (SIL), which requires huge development resources.

For a high SIL with hardware fault tolerance (HFT) requirement equal to 1, we recommend a diverse dual-chip solution based on the Texas Instruments (TI) non-ARM® 32-bit C2000™ MCU as safety elements out of context for low-latency close control loops and a new TI multicore ARM-based system on chip with a safe island for a safe communication. Safety is achieved by following a TUV certified (TI-internal) development process that helps the company manage and mitigate the probability for systematic faults that could lead to failures. Both devices provide built-in safety hardware and software diagnostics for high SILs.

Introduction to industrial drives

Many industrial automation sectors such as packaging, material handling, and food and beverage machines use industrial drives. Such variable-speed electrical drive systems can directly affect machine and human safety in smart factories, where industrial robots/co-robots and autonomous guided vehicles interact with humans in a shared workspace. This environment is often hostile to operators and demands safety and protection so that the machine, material and operator are safe in the event of an electrical, electronic or mechanical failure.

For the safe operation of high-voltage motors and motion during both power up and sustained operation, the system architect and safety manager have to consider all safety requirements for their new product designs according to these international standards:

- International Electrotechnical Commission (IEC) 61800-5-2: safety requirements for adjustable-speed electrical power drive systems.
- Safety integrity levels defined in IEC 61508.
- Performance levels (PLs) as defined by the International Organization for Standardization (ISO 13849) machinery safety standard.
- ISO/Technical Specification 15066 as a standard for co-robots.

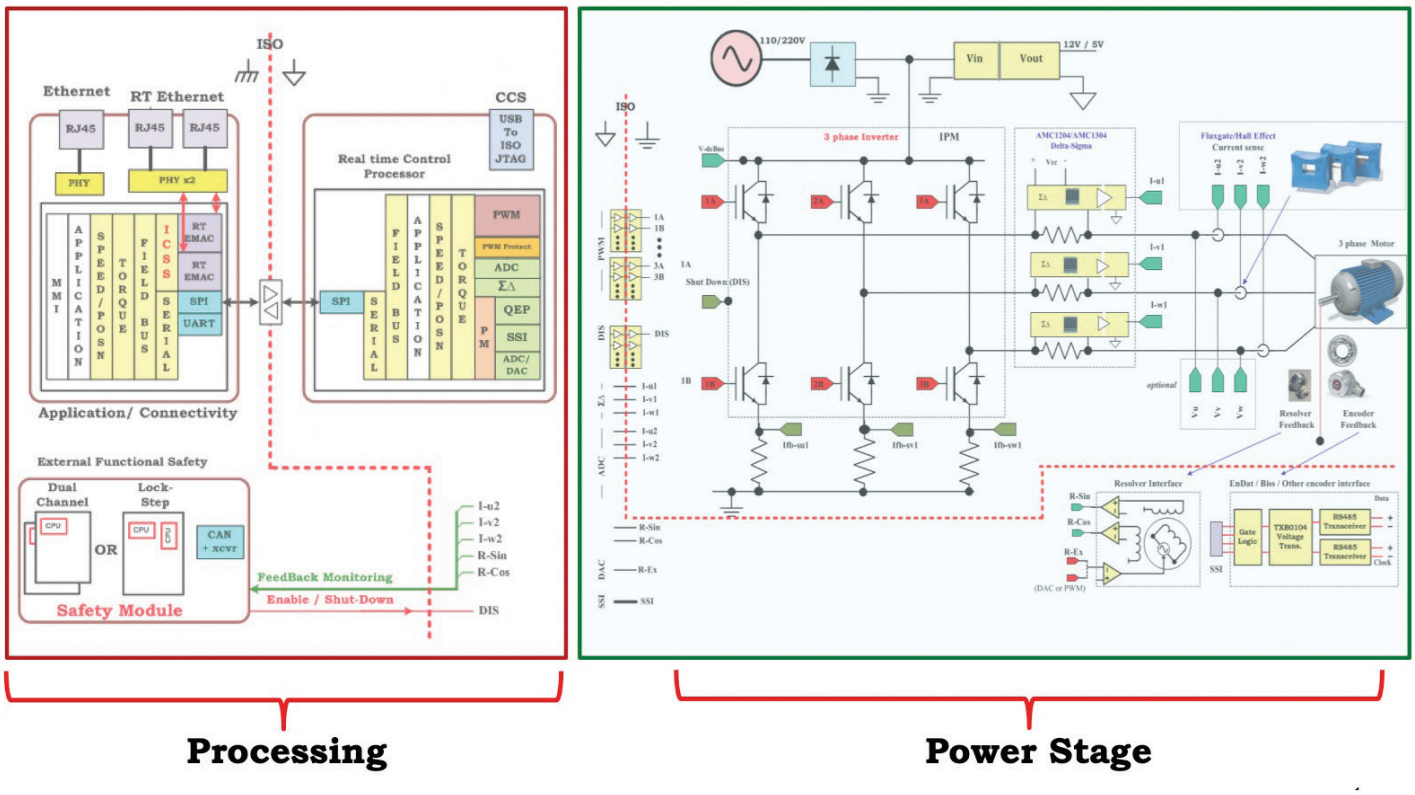

Figure 1. *A common drive topology*

- American National Standards Institute/Industrial Truck and Standards Foundation B56.5-2012, Safety Standard for Driverless, Automatic Guided Industrial Vehicles.

Industrial drive topologies

An industrial drive consists of a power stage and a processing unit that covers control and communication tasks. Depending on the voltage level in the power stage, the designer splits the system by defining isolation barriers between hot and cold sides (basic and reinforced isolations). Isolation is required because it prevents electrical shock to human operators and damage to expensive integrated circuits in high-voltage drives. It protects the signals that need to sense on the hot side but are operated by the controller on the cold side. Traditionally, the controllers reside on the cold side, as shown in **Figure 1**.

Communication interfaces like industrial field buses must be isolated from the high-voltage side. Adding a safety module based on two MCUs can achieve SIL 3/PL-e.

Looking closely at **Figure 1**:

- It is possible to simplify the architecture by setting the real-time controller on the hot side (power stage) and using reinforced isolation through a serial path to the applications and communication controller on the cold side.
- The junction temperature, especially in closed housing (impact drives) has a direct impact on the MCU's power-on hours.
- For a servo drive, encoders and input/output modules are on the cold side and considered in the safety implementation at a system level.

The safety certification of a system takes time and resources, so the effective way to speed time to market is defining a platform instead of multiple designs.

Real-time control with TI C2000 MCUs

An MCU for real-time control has to manage multiple tasks in parallel with the lowest latency.

Using one single core for all of these tasks is challenging and can't be solved by increasing the million instructions per second (megahertz). An ARM-based system suffers from latency caused by interrupt handling and wait-states while accessing the internal memory.

The TI C2000 MCU uses multiple co-processors and logic blocks on-chip to execute real-time tasks in parallel without involving the main core all the time as shown in **Figure 2**.

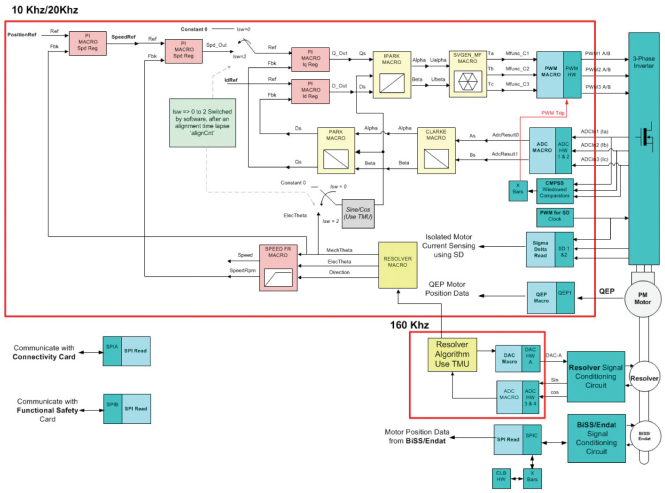

Figure 2. *Split of real-time system tasks*

How does it work?

A dedicated co-processor unit called the control law accelerator (CLA) runs the control loop without involving the main central processing unit (CPU).

The integrated control logic block (CLB) is used as a position manager to decode the encoder feedback

The trigonometric math unit (TMU) calculates the atan2 for an angular position in 14 cycles (while an ARM Cortex M4 processor needs 100+ cycles).

This MCU is able to run a fast current loop in less than 1 µs.

Looking at the software algorithms typically used for field-oriented control to spin a three-phase motor (**Figure 3**), the C2000 MCU uses on-chip resources for sensing, actuating and decoding feedback for a precise closed control loop.

FCL Functional Split on F2837x

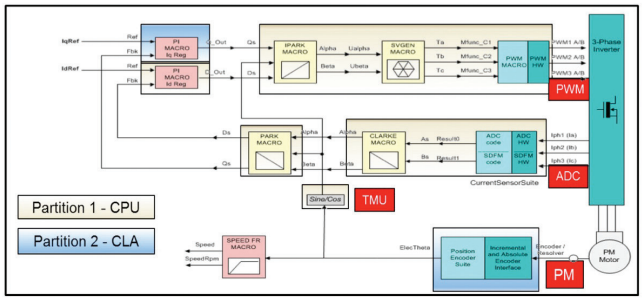

Figure 3. *Real-time algorithm view*

Safety in real-time control with C2000 MCUs

TI develops C2000 MCU-based SafeTI™ automotive and industrial products using its QRAS AP00210 hardware development process, which has been independently assessed and certified by TÜV SÜD to support systematic fault coverage of safety integrity level (ASIL) D/SIL 3 applications according to the ISO 26262 and IEC 61508 standards.

C2000 MCU-based SafeTI products are designed to meet the highest standards by managing both systematic as well as random hardware faults.

With over 300 built-in safety mechanisms, C2000 MCU-based SafeTI products provide the required diagnostic coverage to meet a random hardware capability of ASIL B/SIL 2 at a component level by addressing the motor control tasks as shown in **Figure 4**.

Functional safety manuals provide detailed information on the safety mechanisms to aid in the development of compliant systems up to ASIL D/SIL 3.

C2000 MCU-based tunable failure modes, effects and diagnostic analysis (FMEDA) provides increased flexibility by allowing customized tuning of the FMEDA to application-specific needs.

C2000 MCU-based tunable FMEDA

A typical FMEDA in the development stage of a system provides a detailed analysis of the different

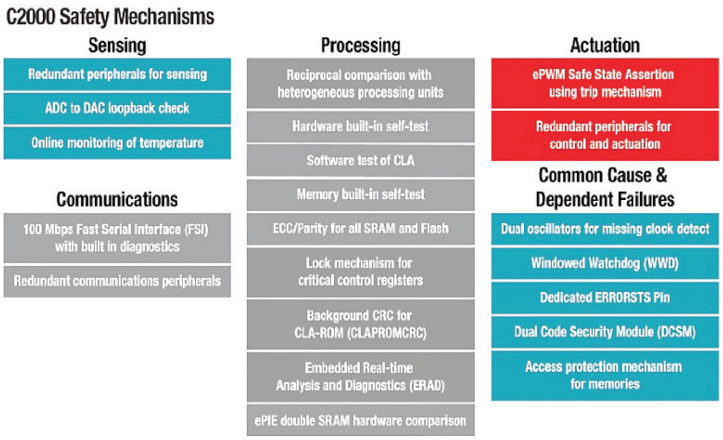

Figure 4. *C2000 MCU safety mechanisms*

failure modes and the associated effects of those failure modes, as well as safety mechanisms and the impact of any implemented safety mechanisms in terms of diagnostic coverage.

The C2000 MCU-based FMEDA comes with the added benefit of being tunable (**Figure 5**), enabling you to tune the FMEDA to your own application-specific needs. This is an important part of implementing safety at a system level.

SafeTI diagnostic library

The SafeTI diagnostic library provides easy-to-call application programming interfaces that helps implement the safety mechanisms outlined in the safety manual and enable fault injection testing and control-loop profiling.

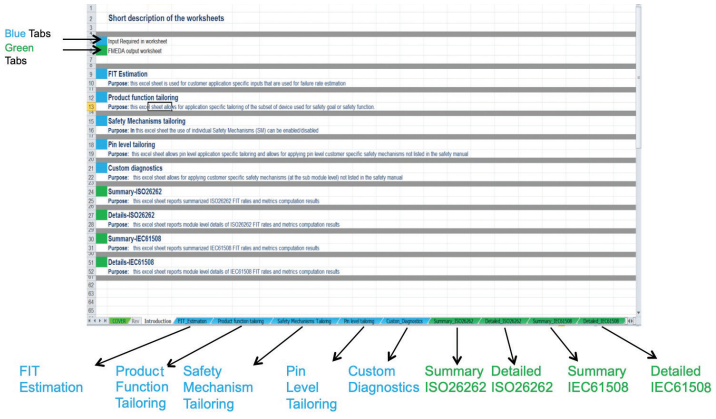

Figure 5. *C2000 MCU-based tunable FMEDA*

Accompanying compliance support packages provide necessary documentation and reports in order to assist with compliance to a wide range of standards for automotive, industrial and other applications.

The product function tailoring feature allows you to select only those parts and subparts of the MCU that you use in your end application, marking them "yes" if they are functional safety related or "no" if they are not. The C2000 MCU FMEDA sets the default utilization of on-chip resources at 100%. But in reality, the application may not even use all of the peripherals and memories available on the device.

The benefit of the product function tailoring feature is that it enables you to easily select the required on-chip resources in the FMEDA to exactly match your end application, thereby yielding accurate results.

The package failure-in-time (FIT) estimation feature is related to the operating mission profile. There may be situations where there is a change in the operating mission profile of the application, and the default setting in the FMEDA no longer accurately represents the application.

For example, the operational profile on the C2000 MCU FMEDA is set to the mission profile for automotive motor control applications by default. If the MCU were used in any other application, chances are that parameters such as package type and maximum power dissipated would also change, requiring the FMEDA to be tuned accordingly. The FIT estimation feature enables a level of customization by allowing you to enter values for your own application-specific operational profile.

Implementing safety mechanisms described in the safety manual satisfies the hardware functional safety requirements at the MCU level. However, existing safety mechanisms with their diagnostic coverages may not be adequate in some situations when there is a change in functional safety requirements at the application level. In such situations, additional safety mechanisms may need to be defined for the MCU to meet the

new functional safety goal. The safety mechanism tailoring feature enables you to view all available safety mechanisms and provides a way to select the ones you require, depending on the functional safety requirements of your end application.

The custom diagnostics feature is an extension of safety mechanism tailoring, and allows you to add additional custom safety mechanisms and input the corresponding diagnostic coverage values depending on the functional safety concept implemented in the application. This is an important function because it offers added flexibility, giving you the option to define your own custom diagnostics in situations where the available safety mechanisms are not sufficient for the application.

C2000 MCU safety concepts for real-time control

With three to four integrated high-speed analog-to-digital converter (ADC) modules (12 bits at 3.4 MSPS or 16 bits at 1 MSPS), the C2000 MCU has the ability to sense hall sensors, shunt and demodulate the sigma-delta signals.

The co-processor CLA can run the second sensing channel and use the direct memory access (DMA) to transfer results independently from the C2000 main core.

The CLB can compare the results of both channels and generate a fault response.

When HFT = 1, the Sitara™ RF5 safe sub-system can act as an external safety monitor, with the possibility to execute direct safe task/safe torque off, or set safety-limited speeds to the motor.

Safe actuating with the C2000 MCU

Much like sensing, the pulse-width modulators generated by independent channels can be routed back into the control logic block for a logical comparison, in order to result a fault response or adjust the duty cycle for a safe function.

Safe feedback with C2000 MCUs

There are two ways to for implementing a safe feedback: Either you rely on a safe encoder or you calculate the position/speed with two independent channels.

C2000 has a position manager that supports both analog and digital encoders as well as software observer in ROM as a second channel to measure the motor position and speed.

Safe multi-axis control with C2000 MCUs

For multi-axis real time control, you can use a low-cost C2000 MCU derivative as a smart sensor for a cross-sensing.

These smart sensors can communicate throughout the isolation barrier either through the FSI **(Figure 6**) or Ethernet (Media Independent Interface/Reduced Media Independent Interface) to the Sitara system on chip (SoC).

Additional built-in diagnostics in C2000 MCUs

The parallel execution of multiple real-time tasks with multiple coprocessors requires additional

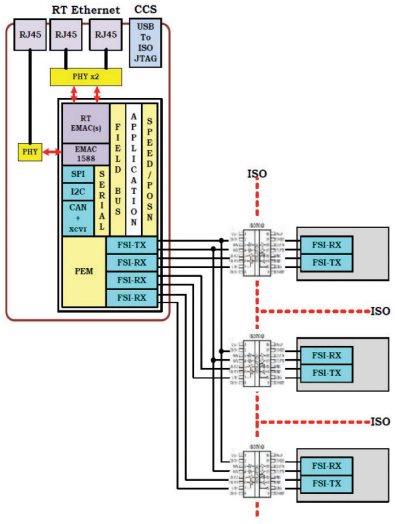

Figure 6. *Multi-axis control via the TI Fast Serial Interface (FSI)*

built-in features to avoid the interference of safety-implemented functions on the device, such as:

C2000 devices are a mix of dedicated and shared static random access memories (SRAMs). Shared SRAMs are configurable to achieve control for write, read and fetch access from different masters, such as the CPU, CLA, and DMA. This gives system integrators the flexibility to resize the allocation of memory to each master, based on the application. However, this also introduces the possible risk of interference.

Embedded real-time analysis and diagnostic (ERAD): The ERAD module provides system analysis capabilities that can detect faults in the CPU and other logic on the MCU by configuring the bus comparator units that monitor CPU bus accesses, and counter units that count events. This module, accessible by the application software, consists of enhanced bus comparator units and benchmark system event counterunits. The enhanced bus comparator units monitor various CPU buses and generate events. The activity monitored and detected by these units can generate breakpoints, watch-points or an interrupt (RTOSINT). After the application code sets up the ERAD module, the module can work independently to generate a RTOSINT interrupt when an event match occurs. This module can detect the presence of interference originating from the lower ASIL/SIL software implemented on the CPU by continuously monitoring its buses.

Dual zone code security module (DCSM): The DCSM is a security feature incorporated on C2000 devices. It blocks access and visibility of on-chip secure memories from unauthorized users, to combat duplication and reverse engineering of proprietary code. Each CPU subsystem has its own DCSM for code protection. The DCSM can be used for functional safety where functions with different SILs execute from different security zones (zone1, zone2, and unsecured zone), acting as firewalls and thus mitigating the risk due to interference from one secure zone to another.

Memory access protection schemes: It is possible for one of the unauthorized masters (CPU, CLA, DMA) to accidentally access or corrupt the memory locations containing critical variables used by a safety function with a higher SIL. Memory access protection logic is implemented per instance of local and global shared SRAMs to detect access violations of write, read, or fetch. The respective flag bit is set and the interrupt is generated to the CPU, thus alerting users to possible interference and helping achieve a safe state for the device. The access violation information is captured in the register in order for the software to take further corrective action.

Flash memory: Flash memory is a secured resource, and each sector can be allocated to a particular secure zone. Each zone has its own code security module (CSM) password: for example, read and write accesses are not allowed to access resources assigned to Zone 1 by a code running from memory allocated in Zone 2, and vice versa. Before programming or erasing any secure flash sector from unsecured memory or another zone's memory, you must unlock the flash sector's zone. One flash pump is shared for erase/program operations on flash memory. A semaphore mechanism is provided to avoid the conflict between Zone 1 and Zone 2. A zone must grab this semaphore to successfully complete the erase/program operation on the flash sectors allocated to that zone. Accidental attempts by erroneous or faulty software code implemented with a lower integrity level to program or erase the flash sector will be blocked, thus preventing the interference.

- Critical configuration registers protection: The integrity of safety functions depends on the MCU's critical configuration registers, which manage power, clock, reset, and so forth. If the critical registers are corrupted by faulty software that coexists on the same lower SIL hardware, the safety functions can be compromised. This interference must be either prevented or detected.

  C2000 devices have critical registers designed with the EALLOW protection mechanism, which uses special CPU/CLA instructions EALLOW/MEALLOW and EDIS to enable and disable access to protected registers. This register protection is enabled by default at startup. While protected, all writes to protected registers by the CPU are ignored. Thus, software with a lower integrity level cannot corrupt the critical configuration of the device.

  The integrity of critical control registers, such as clock source selection, phase-locked loop (PLL) multiplication, pre-scalar and post-divider are essential to operate the device at the correct speed. Corruption of these registers due to faulty software can drastically affect the performance and safety of the overall system. On C2000 devices, it is possible to program and lock many of these registers by configuring the LOCK field, preventing any further programming of the configuration until a system reset. Also, writes to some critical control registers are protected by a specific KEY field embedded in the register definition, which enables or disables writes to it. Thus, you can mitigate software interference from a lower integrity level affecting the safety function.

  Peripherals: Peripherals on a device are also shared resources. These are responsible for critical functions such as control and communication peripherals for a safety function. C2000 devices provide access to these peripherals by multiple masters, orthogonally between CPUs, CLAs and DMAs. There is a risk of interference from a master implementing a lower ASIL function by corrupt accesses to the peripherals. Control peripherals, (ADCs, enhanced PWM, sigma-delta filter modules, comparator subsystems, digital-to-analog converters, and programmable gain amplifiers) and communication peripherals (Controller Area Network, Serial Peripheral Interface, Local Interconnect Network, Power Management Bus and FSI) are protected by master access control logic in each instance. When programmed, this feature completely blocks access from certain masters, reducing or eliminating the possibility of interference from a lower ASIL safety function.

Industrial communication with the Sitara PRU-ICSS

TI's innovation for industrial communications is the programmable real-time unit (PRU)-industrial communication subsystem (ICSS), which has been integrated into Sitara devices such as AM335x, AM437x and AM57x processors. There are three next-generation ICSSs, each containing four PRUs running at up to 250 MHz. PRUs are reduced instruction set computer cores with no cache and no pipeline to enable deterministic, single-cycle processing.

The PRU-ICSS provides versatile, programmable industrial Ethernet and serial field-bus communications to accommodate protocols such as Profibus, Profinet, EtherCAT, EtherNet/Internet Protocol (IP), Sercos III and Powerlink. The current generation of PRU-ICSS enables 100 Mbps of real-time Ethernet data throughput while achieving industrial protocol cycle times as low as 31.25 ms.

For the industrial network evolution to Time Sensitive Networking (TSN), TI created a more powerful, scalable processing solution, the PRU_ICSSG, by upgrading the existing ICSS architecture with additional PRUs and accelerators. The design

of the PRU_ICSSG does not force a software rework of industrial Ethernet protocols already implemented on current PRU-ICSS devices. The next generation of PRU_ICSSG integrated into AM6x processors achieves 1-Gbps throughput and delivers the same real-time industrial Ethernet protocol cycle times. With a total of 1 GHz of real-time, deterministic PRU processing capability, hardware accelerators for common Ethernet processing tasks and increased high-bandwidth memory, the PRU_ICSSG is flexible and open for new standards.

Each PRU_ICSSG has two Reduced Gigabit Media Independent Interface (RGMII)-based Ethernet ports to support industrial switch implementations in gigabit speeds. There is also an additional Ethernet media access controller supporting RGMII. In total, a single AM6x can enable seven concurrent Ethernet ports.

The AM6x is available in pin-compatible quad- and dual-core Arm® Cortex®-A53 (**Figure 7**)

TI made some unique investments in the AM6x processor design to enhance reliability and reach higher levels of functional safety. The AM6x provides at least one year of operation at a maximum junction temperature with extended longevity estimates for those interested in longer lifetimes for their systems. To allow the implementation of functionally safe systems, the AM6x processor has integrated dual-core R5F-based MCU technology from the TI Hercules™ product family.

Enhanced features for functional safety and enhanced reliability

The Sitara AM6xxx SoC was architected for mixed-criticality functional safety applications up to SIL 3. The microcontroller subsystem (MCUSS) leverages TI's experience with Hercules functional safety MCUs to create a "safe island" within the SoC, just as if the MCU was external to the SoC (**Figure 8**).

The MCUSS is heavily protected by hardware diagnostic measures focused on power, clocks, CPUs, memories and interconnect. Once the correct operation of the MCUSS safe island is established, the logic in this region can provide diagnostic coverage in other regions of the SoC. The MCUSS stays alive even if the main SoC

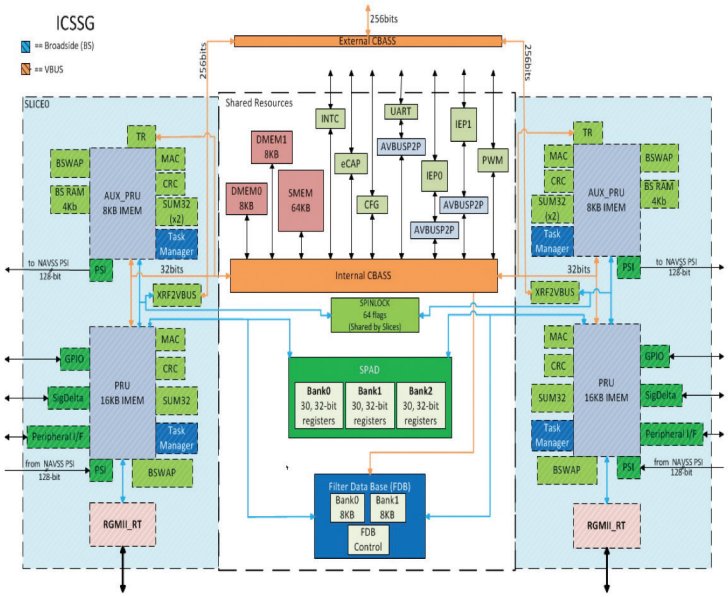

Figure 7. *AM654x functional block diagram*

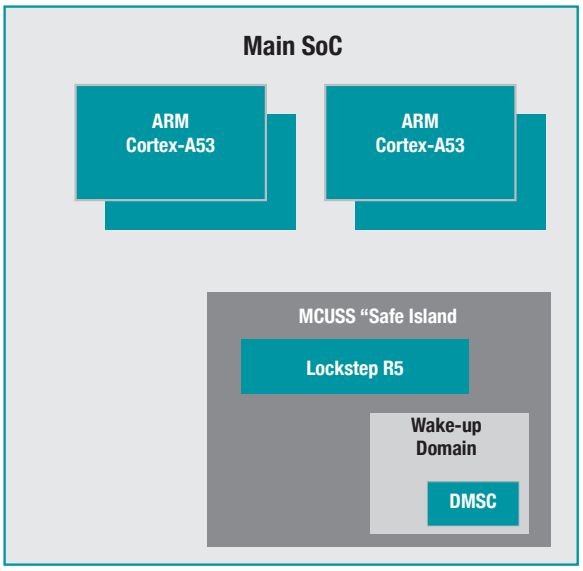

Figure 8. *The safe-island MCUSS in the Sitara AM65xx processor*

domain crashes (and can reboot it). This partitioning and separation provides a basis for effective functional safety metrics while providing benefits to minimize the overall bill of materials.

The split of functional safety tasks and the separation of safe from non-safe software remains flexible and dependent from the application. In some instances, the usage of a safe operating system is useful. The separation of power and clocks between the MCUSS and the main SoC domain is essential for freedom from interference. Each domain has its own separate clock sources, separate PLLs and independent watchdogs. There are no shared power rails between the MCUSS and the main SoC domain. Each domain has its own voltage sources.

For AM6x devices with functional safety enabled, it's possible to boot the dual R5F cores into a lock-step mode. All R5F memories and memories within the MCUSS are covered by single-error correct dual-error detect error-correcting code (ECC). Additionally, there are integrated ECC aggregators (one per core) with support for error injection to all R5F ECC memory blocks to test the ECC functionality for safety-critical applications. This error injection feature is unique to TI's R5F implementation.

In the main SoC domain, functional safety also guided the Cortex-A53's integration into the design. There is ECC protection for the L1 data cache (data random access memory [RAM]), the L2 cache (data RAM and tag RAM) and L1 snoop control unit duplicate tags. There is parity protection for the L1 instruction cache (data RAM and tag RAM), L1 data cache (tag RAM and dirty bits) and translation lookaside buffers. TI also added error injection capability for all supported ECC memory blocks for each A53 core with ECC aggregators.

The AM6xxx SoC safety package is a compliance support package with quality records to support customer certification efforts.

Sitara processor built-in control for IP access

You have the flexibility to define your black channel and split the internal resources to logical subsystems controlled by an IP access from the device management and security controller (DMSC).

The DMSC is an integral part of the multicore AM6x SoC device family and acts as a central authority for device management, boot sequence, power management and security. All critical assets (keys, configuration data) are secured in the DMSC, which reduces the opportunity for attacks. The DMSC ensures that all secure resources are working in harmony and that a security hack in one part of the device does not lead to the collapse of the entire SoC.

TI owns the secure part of the DMSC firmware and makes it available only in binary. The AM6x architecture design supports an enhanced firewall architecture that permits dynamic access control to all SoC resources (memories, peripherals, cores, etc.). The DMSC provides the ability to promote or demote firewall access to resources. DMSC resources are accessible through defined application programming interfaces as shown in **Figure 9**.

Dual-chip solution for safe motion control

A dual-chip solution has these advantages:

- It is a scalable and flexible platform for real time control and industrial communication.
- Sitara processors can be used for designs such as human machine interface (HMI), programmable logic control and backplane, which speeds time to market.
- The C2000 MCU can be used for power conversions (AC/DC, charging, power-off brakes).
- A platform approach uses the same integrated development environment for software development.

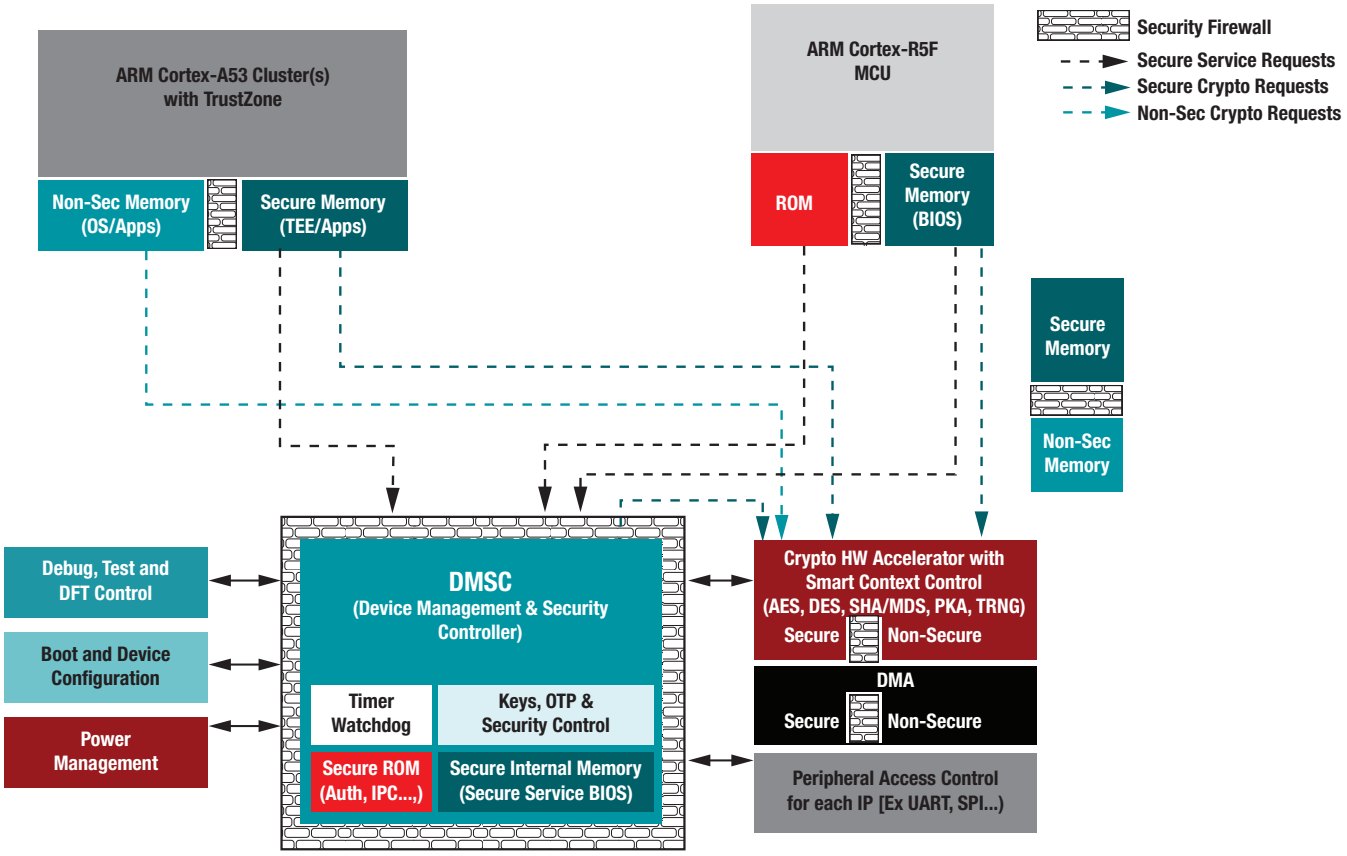

Figure 9. *DMSC features in the Sitara AM65xx processor*

- Free Code Composer Studio™ license.
- Diversity of cores (non-ARM C2000 MCU plus ARM-based Sitara processor).
- Safety on-chip hardware/software diagnostics.
- Identical safety processes.
- Uses the same SafeTI packages.
- A functional safety manual that describes the on-chip safety mechanisms.
- A detailed, tunable quantitative FMEDA allows you to calculate contributory FIT to your systems.
- Safety diagnostic libraries can be included in the final software project, providing easy-to-use routines for power-on self-test and periodic self-test.

TI provides also compiler-qualification-kits that consist of an instrumented compiler that you can use while compiling code for the target. The instrumented compiler will record all compiler settings and generate a report that documents your specific settings.

Decomposition using the Sitara processor and C2000 MCU for high SIL levels with a HFT = 1

The biggest benefit of decomposition is being able to meet systematic aspects of required SILs and overall system safety goals. Both Sitara processors and C2000 MCUs are SIL 2 at the component level. Using the MCUSS from the Sitara device as external safety MCU for the C2000 device enables systems to be certified for SIL3 and Category 4 PLe.

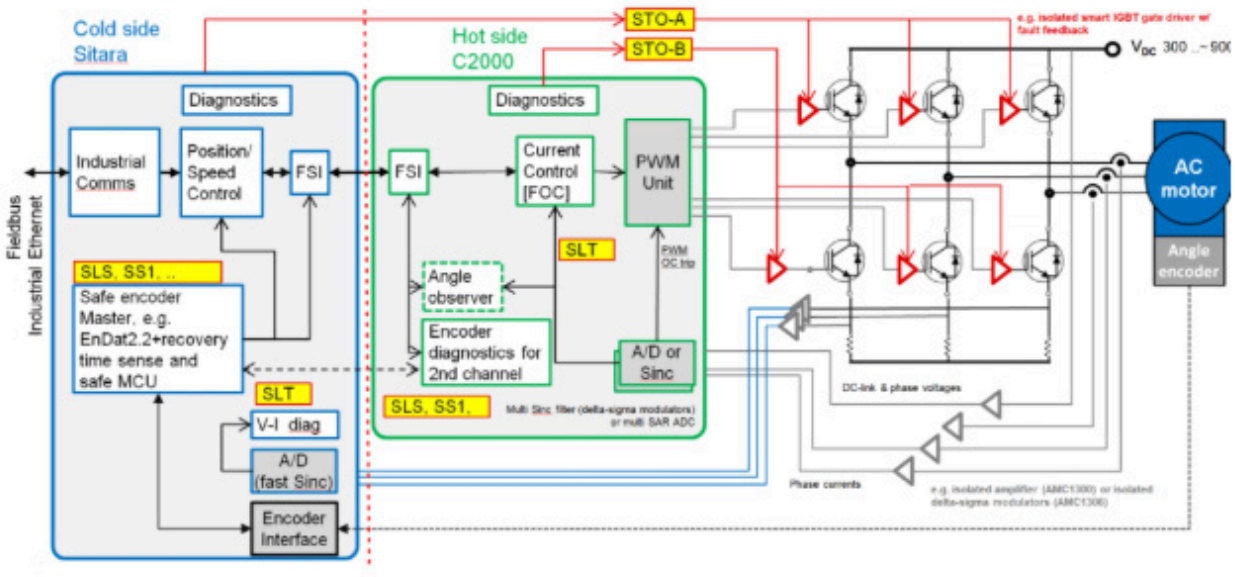

Figure 10. *Example of safe implementation of Servo Drive*

The Sitara ARM core domain can be used for other applications and running the communication stacks.

TI also offers quality managed power-management integrated circuits and gate drivers, which could contribute to a high safety implementation at system level (**Figure 10**).

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