# Industrial Functional Safety for C2000™ Real-Time Microcontrollers

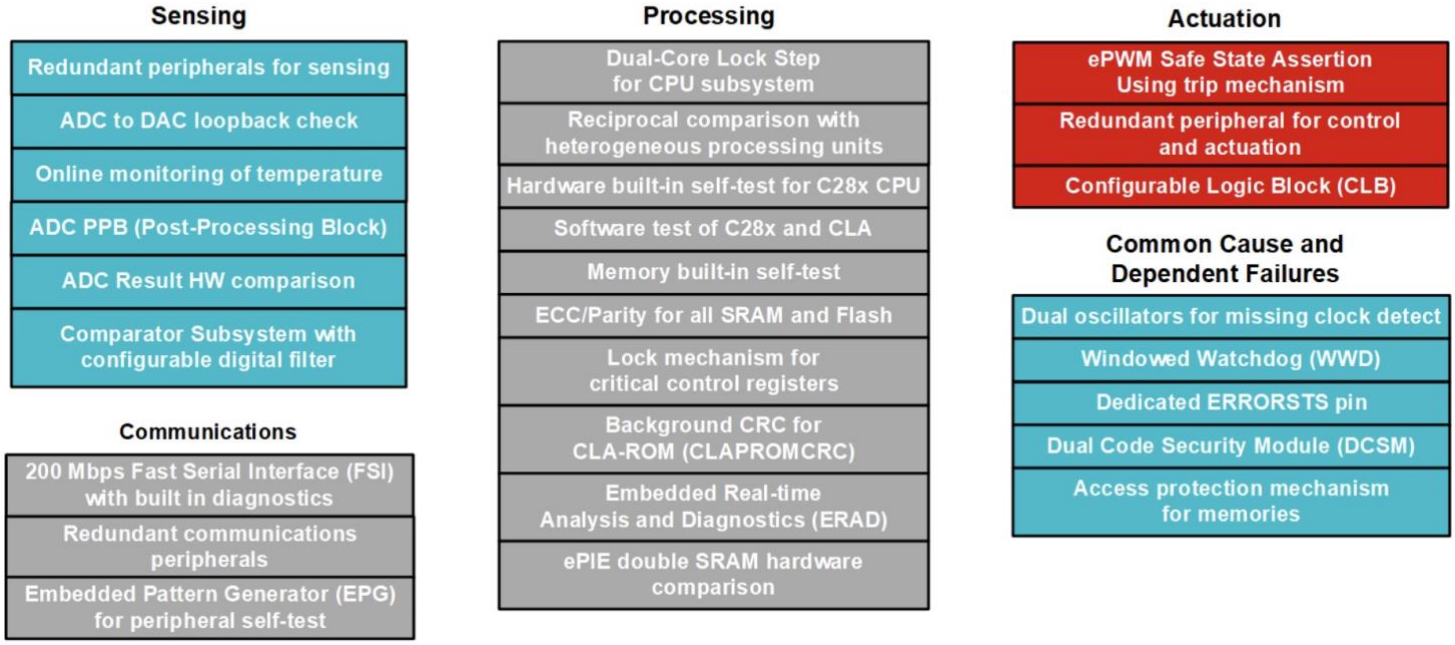
Texas Instruments

Streamline and speed-up IEC 61508 (SIL) and ISO13849 (PL) certification process with our Functional Safety-Compliant products, documentation, software and support from our knowledgeable experts. Our C2000™ real-time MCUs are independently assessed and certified by TUV SUD to meet a systematic capability up to SIL 3 and help you create industrial applications requiring functional safety. C2000 real-time MCUs also address **Automotive Functional Safety**.

Highlights of the C2000 functional safety offering are

- Device architecture for functional safety
- Documentation to support to ease customer's safety assessment at system level
- Software library to implement the safety mechanisms

## C2000 Key Safety Mechanisms




**Safety mechanisms** play a key role in the overall safety of a system by detecting potentially dangerous failures and consequently helping place the system in a safe state. With over 300 safety mechanisms defined and independently assessed by TUV SUD for its effectiveness, C2000 MCUs provide the required diagnostic coverage to meet a random hardware capability of SIL 2 at a component level. Functional safety manuals provide detailed information on the safety mechanisms, techniques for achieving non-interference between elements and avoiding dependent failures, to aid customers in the development of compliant systems up to SIL 3. The tunable FMEDA provides increased flexibility to customize and calculate HW metrics with features such as package FIT estimation, product function tailoring, safety mechanism tailoring and custom diagnostics allowing customers to **tune the FMEDA** to their own application specific needs.

**Learn More about C2000 real-time MCU Safety Mechanisms**

| Key safety features | | F2838x | F2837x F2807x | F28003x | F28002x | F280015x | F28P65x |
|---|---|---|---|---|---|---|---|
| Hardware | ASIL D Compliant Development Process | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| | Random Hardware Capability | ASIL B | ASIL B | ASIL B | QM | ASIL B | ASIL B |
| | Systematic Capability | ASIL D | ASIL D | ASIL D | ASIL D | ASIL D | ASIL D |
| | Single Point Fault Coverage of CPU (SPFM) | Reciprocal comparison | Reciprocal comparison | Reciprocal comparison | N/A | Lockstep C28x | Reciprocal comparison (CPU1 + CLA) Lockstep C28x (CPU2) |
| | Memory parity | ✓ | ✓ | X | X | ✓ | ✓ |
| | Memory ECC | ✓ | ✓ | ✓ | ✓ | ✓ | Flash ECC only |
| | Memory BIST (MPOST) | ✓ | X | ✓ | ✓ | ✓ | ✓ |
| | Dual Core Security Module (DCSM) to achieve non-interference between software elements | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| | Windowed watch-dog timer with independent clock | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| | Hardware CRC acceleration | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| | Hardware BIST (HWBIST): Permanent fault coverage of 90%+ for C28x CPU | ✓ | ✓ | ✓ | ✓ | X | ✓ |
| | Redundant and independent ADC / PWM Modules | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| | Automatic comparison of ADC conversion results in HW | X | X | X | X | X | ✓ |
| | Redundant Configurable Logic Block (CLB) option | ✓ | ✓ | ✓ | ✓ | N/A | ✓ |
| Software | STL (Software Test Library): Permanent fault coverage of 60%+ for C28x CPU | N/A | N/A | N/A | N/A | ✓ | Coming soon |
| | STL (Software Test Library): Permanent fault coverage of 60% for CLA | ✓ | ✓ | ✓ | N/A | N/A | Coming soon |
| | Functional Safety Quality (FSQ) Flash APIs | X | X | ✓ | N/A | ✓ | Coming soon |
| Doc | Safety Manual: detailed product overview, capabilities and constraints, TI development process, safety elements, and safety diagnostics. | SFFS022 | SPRUI78 | SFFS277 | SPRUIT5 | SFFS222 | Beta available contact TI |
| | Device Certification | SSZQQM2 | SWAQ009 | SFFS610 | **N/A** | SFFS748 | Coming soon |

| Safety collateral | |
|---|---|
| Development Process Certificate<br>Hardware \| Software | TUV-SUD certificate for QRAS-AP00210. Functional safety development process for IEC 61508-2 and ISO 26262-5 Compliant Components |
| C2000 Safety package* | By request and NDA required. Package includes below elements:<br>• **Technical Report on Random HW Capability**<br>• **Technical Report on Systematic Capability**<br>• **FMEDA**: A failure mode, effects and diagnostic analysis (FMEDA) is used in the development stage to provide a detailed analysis of different failure modes, the associated effects of failure modes, diagnostics and the impact of any implemented diagnostics/ safety mechanisms in terms of diagnostic coverage. 5 part FMEDA training video series.<br>• **Device Concept Assessment**<br>• **SAR (Safety Analysis Report)**: Contains results of safety analysis according to the targeted functional safety standards. |
| Software diagnostic library | A library of modules and examples demonstrating safety features and mechanisms. Examples include CPU, memory, clocks/ watchdogs, HWBIST, etc.<br><br>F2837x/07x supported through this library.<br>All other F28x series supported by libraries released in C2000Ware. |
| Functional safety flash APIs | Library is available in C2000Ware. Contact local TI representative for further compliance support package offerings. |
| CLA co-processor self-test library* | Library to perform start-up and periodic tests for CLA logic integrity |
| Compiler qualification kit | Compare compiler coverage for customer use cases against coverage of TI compiler release validations |
| Safety certified RTOS (SafeRTOS) | Pre-certified safety Real Time Operating System (RTOS) |
| MathWorks simulation & code generation | IEC certification kit helps you qualify MathWorks code generation and verification tools to streamline certification of your embedded systems |

*Not publicly available collateral. Contact your local TI representative to request.

**Industrial Safety Architectures** common in machinery applications typically require a dual channel safety approach (hardware fault tolerance = 1). C2000 devices offer unique capability and scalability to implement two different architectures for SIL-2 (or cat 3 PL d) and SIL-3 (or cat 3 or cat 4 PL e) systems; a C2000 MCU for each of two safety channels (Figure 1) or a C2000 MCU for one safety channel and a C2000 MCU for the second safety channel and the controller combined in single device (Figure 2).

However, for several industrial applications such as mobile robots, **single** channel architectures can be used to fulfill the safety requirements (hardware fault tolerance = 0). A C2000 device together with external test equipment result in an optimal architecture to achieve the required SIL-2 (or cat 2 PL d); a C2000 MCU can be used as the motor controller as well as for diagnostics and as test equipment an external power supply with diagnostics is used to diagnose and ensure the proper functionality of the C2000 MCU (Figure 3).

Further, compared to general purpose MCUs being used for safety functions C2000 devices offer superior compute performance and device features for implementing complex safe motion functions beyond just Safe Torque Off (STO) that requires real-time monitoring of parameters such as SLS (Safe Limiting Speed), Safe Brake Control (SBC), Safe Direction (SDI), Safe Speed Monitor (SSM) and fast actuation of the safe state.

Further details – including a TUV report on these concepts and architectures - are available under NDA in the C2000 Safety package.

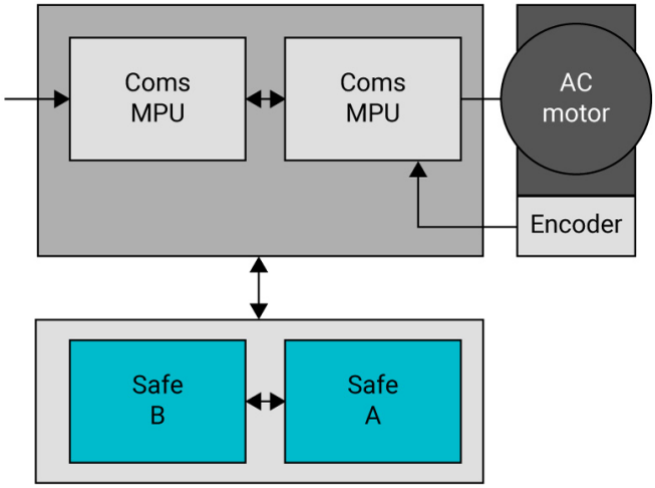



*Figure 1. Architecture 1 with dual safety MCUs (HFT=1, SIL 2 or SIL 3 ).*

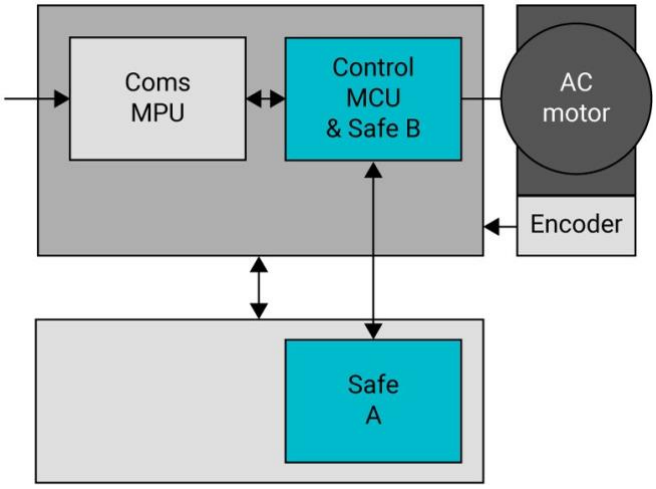



*Figure 2. Architecture 2 with single safety MCU and safety integrated functions into the Drive MCU (HFT=1, SIL 2 or SIL 3 ).*

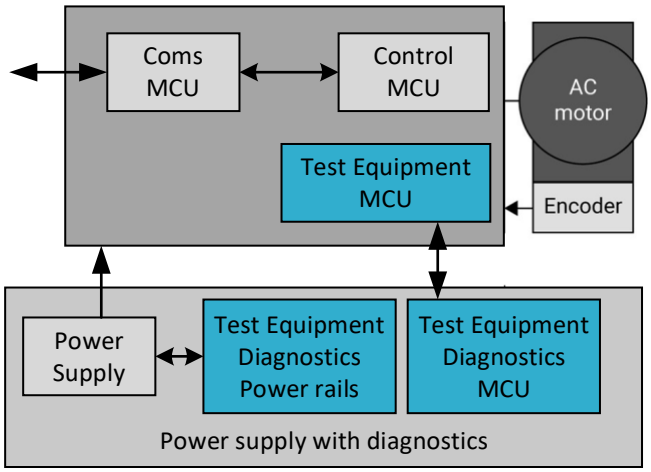



*Figure 3. Architecture 3 with single safety MCU and PMIC (HFT=0, SIL 2)*

# 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