Automotive Functional Safety for C2000™ Real-Time Microcontrollers

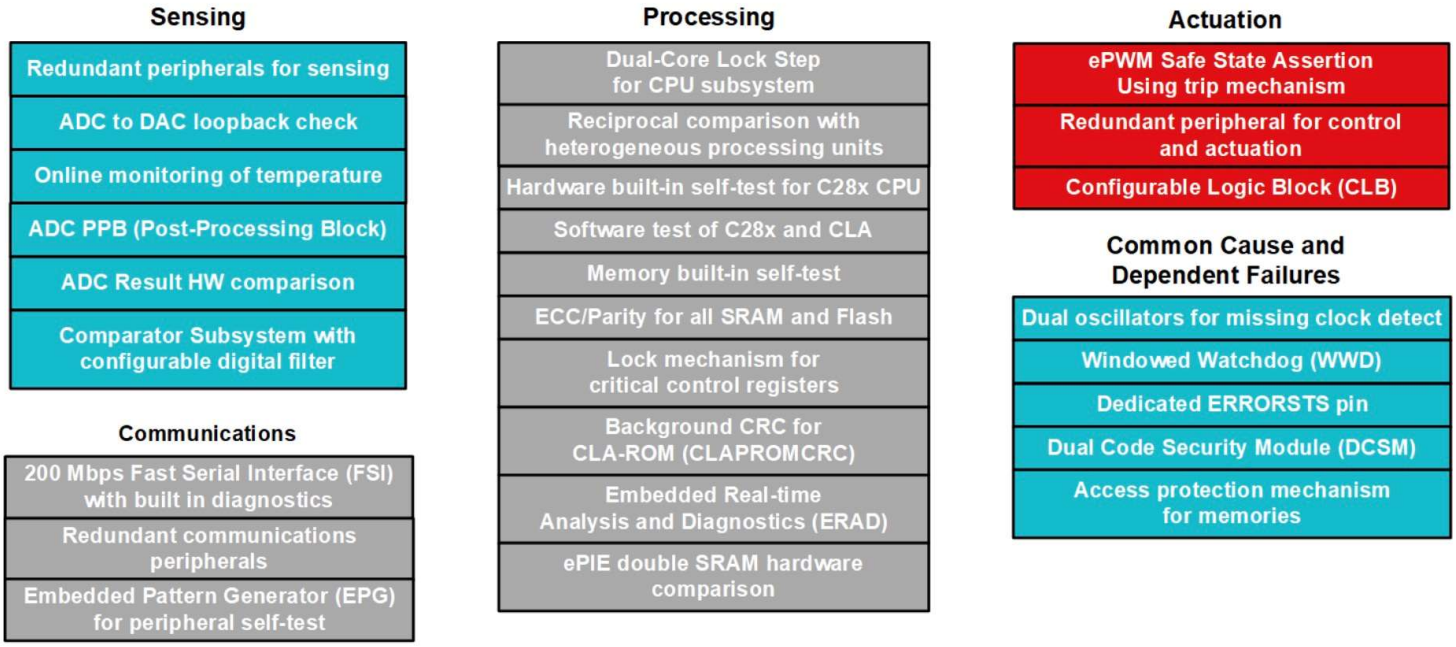
Texas Instruments

Streamline and speed up the ISO 26262 certification processes 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 TÜV SÜD to meet a systematic capability up to ASIL D and help you build automotive applications requiring functional safety. C2000 real-time MCUs also address **Industrial Functional Safety**.

Highlights of the C2000 functional safety offering are

- Device architecture tuned 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 built-in safety mechanisms defined and independently assessed by TÜV SÜD for its effectiveness, C2000 MCUs provide the required diagnostic coverage to meet a random hardware capability of ASIL B 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 ASIL D. 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 Key Safety Features

	Key safety features	F2838x	F28P65x	F2837x F2807x	F28P55x
Hardware	SIL 3 Compliant Development Process	✓	✓	✓	✓
	Random Hardware Capability	ASIL B	ASIL B	ASIL B	ASIL B
	Systematic Capability	ASIL D	ASIL D	ASIL D	ASIL D
	Single Point Fault Coverage of CPU (SPFM)	Reciprocal comparison	Reciprocal comparison (CPU1 + CLA) Lockstep C28x (CPU2)	Reciprocal comparison	Reciprocal comparison
	Memory parity	✓	✓	✓	✓
	Memory ECC	✓	Flash 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	✓
	Redundant Configurable Logic Block (CLB) option	✓	✓	✓	✓
Software	STL (Software Test Library): Permanent fault coverage of 60%+ for C28x CPU	N/A	✓	N/A	✓
	STL (Software Test Library): Permanent fault coverage of 60% for CLA	✓	✓	✓	✓
	Functional Safety Quality (FSQ) Flash APIs	X	✓	X	✓
Doc	Safety Manual: detailed product overview, capabilities and constraints, TI development process, safety elements, and safety diagnostics.	SFFS022	SFFS700	SPRUI78	SFFS779
	Device Certification	SSZQQM2	SFFS901	SWAQ009	SSZQT44

	Key safety features	F28004x	F28003x	F28002x	F280015x
Hardware	SIL 3 Compliant Development Process	✓	✓	✓	✓
	Random Hardware Capability	ASIL B	ASIL B	QM	ASIL B
	Systematic Capability	ASIL D	ASIL D	ASIL D	ASIL D
	Single Point Fault Coverage of CPU (SPFM)	Reciprocal comparison	Reciprocal comparison	N/A	Lockstep C28x
	Memory parity	✓	X	X	✓
	Memory ECC	✓	✓	✓	✓
	Memory BIST (MPOST)	✓	✓	✓	✓
	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	✓	✓	X
	Redundant and independent ADC / PWM Modules	✓	✓	✓	✓
	Automatic comparison of ADC conversion results in HW	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	✓
	STL (Software Test Library): Permanent fault coverage of 60% for CLA	✓	✓	N/A	N/A
	Functional Safety Quality (FSQ) Flash APIs	X	✓	N/A	✓
Doc	Safety Manual: detailed product overview, capabilities and constraints, TI development process, safety elements, and safety diagnostics.	SPRUID8	SFFS277	SPRUIT5	SFFS222
	Device Certification	SPRQ004	SFFS610	N/A	SFFS748

Safety collateral	
Development Process Certificate 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* *Not publicly available collateral. Contact your local TI representative to request.	By request and NDA required. Packages include below elements: **C2000 Safety Package for Automotive and Industrial MCUs** • **Technical Report on Random HW Capability** • **Technical Report on Systematic Capability** • **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. • **Device Concept Assessment** • **SAR (Safety Analysis Report)**: Contains results of safety analysis according to the targeted functional safety standards. **Device-specific self-test library package** • **C28x_STL (C28x Self-Test Library):** Library for software test of C28x CPU • **CLA_STL (CLA Self-Test Library):** Library for software test of CLA
Software diagnostic library	A library of modules and examples demonstrating safety features and mechanisms. CPU, memory, clocks/ watchdogs, HWBIST, etc. F2837x/07x supported through this library. 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.
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

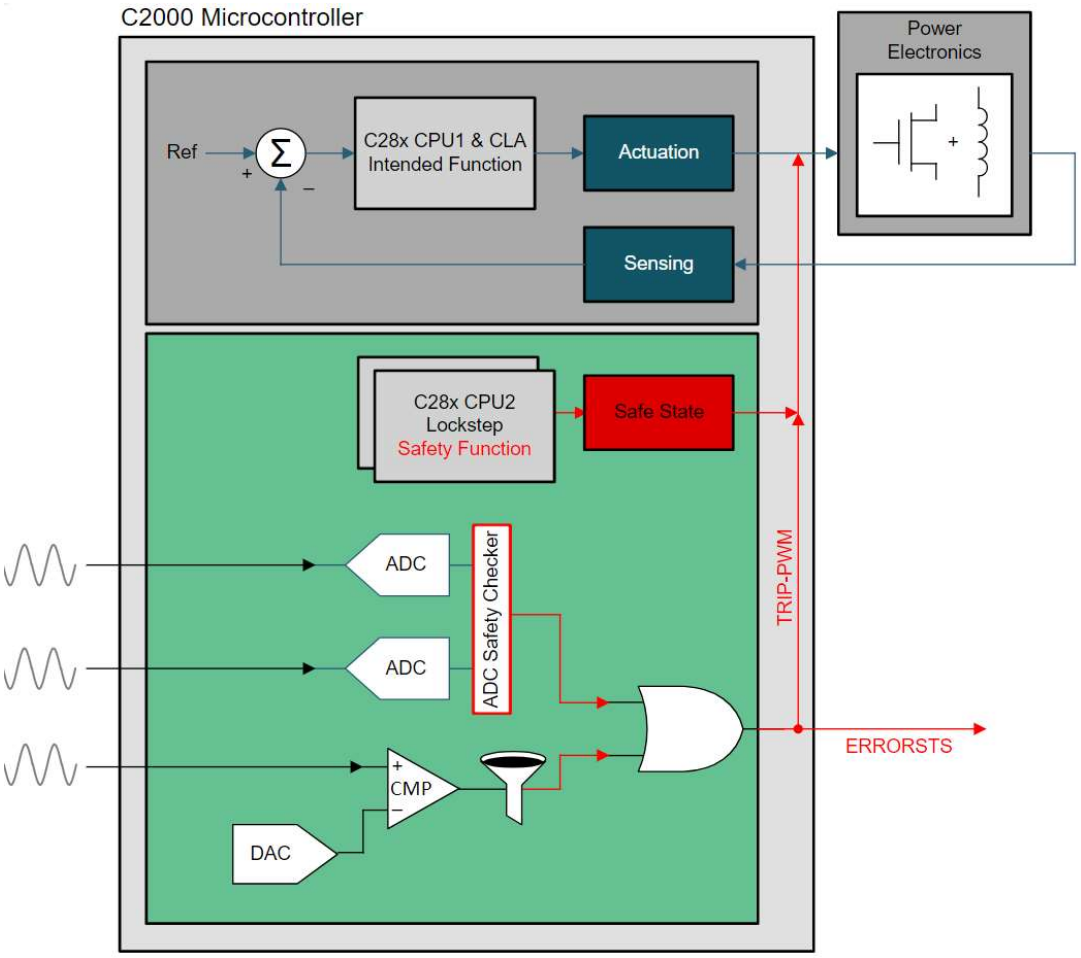


Figure 1. Automotive Functional Safety application example: on-board charger (OBC) with F28P65x-Q1.

- Intended Function: can be implemented on both C28x CPU1 and CLA
  - In example above: control functions for on-board charger (OBC) digital power control
- Safety Function: Implement using C28x CPU2 and other hardware modules such as ADC, CMPSS, SDFM secondary filter, CLB, and so forth.
  - SPFM of the safety goal can be met by hardware redundancy between the modules used in implementing safety function, **Hardware Redundancy Using Lockstep Compare Module (LCM)**, **Hardware Redundancy with ADC Safety Checker**, **Periodic Software Read Back of Static Configuration Registers** and so forth.
- Diagnostic Function: Implement with C28x CPU and other hardware modules such as LCM, ADC, CMPSS, SDFM secondary filter, CLB, and so forth
  - LFM can be met by **Software Test of CPU**, **Self-test Logic for LCM**, **Software Test of Function Including Error Tests** and so forth.
- See more details on the mentioned safety mechanisms in the F28P65x safety manual.

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