Migration Guide
SPRUIV2–April 2020

C2000™ Gen 2 to Gen 3 MCUs Functional Safety Enablers

Prasanth Viswanathan Pillai and Bharat Rajaram

ABSTRACT

C2000 real-time control MCUs are a portfolio of high-performance microcontrollers that have been optimized for processing, sensing and actuation to improve closed loop performance for functional safety compliant systems. These MCUs address wide-ranging real-time control applications and are broadly classified into two categories, namely Generation 2 and Generation 3, based on performance and peripheral compatibility.

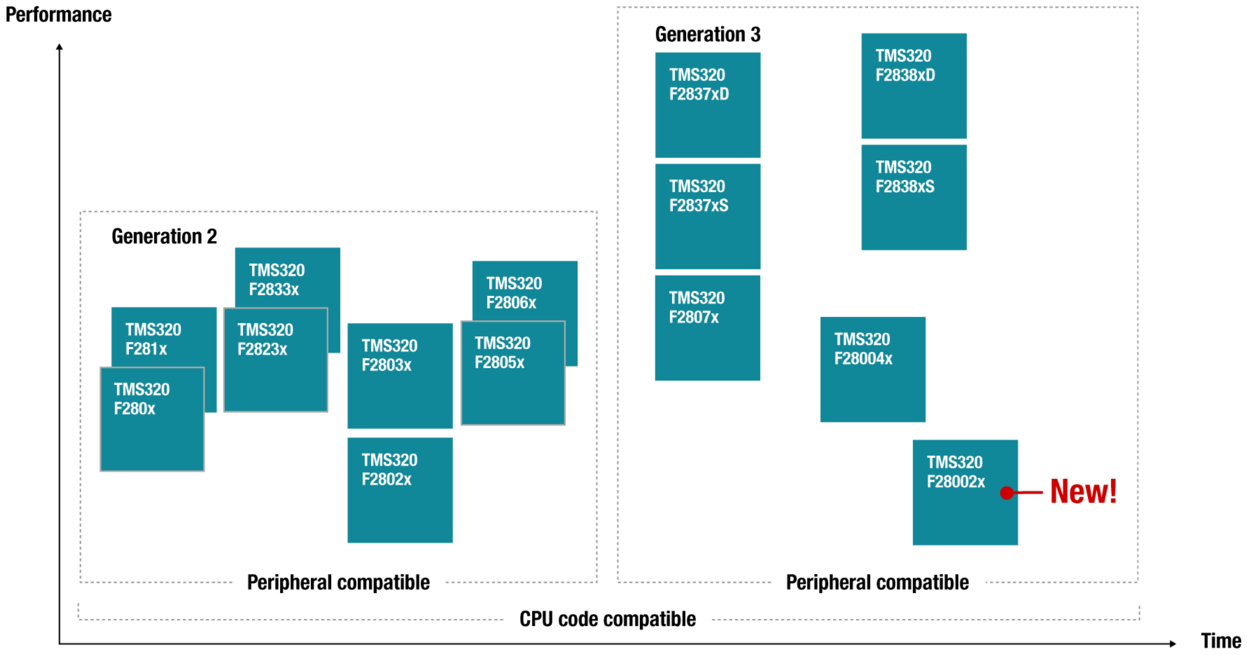

Figure 1. C2000 Microcontroller Portfolio

Contents

List of Figures

List of Tables

Trademarks

C2000 is a trademark of Texas Instruments.

1 Introduction

Safety mechanisms play an important role in safe-ing sensing, processing, actuation, communications and infrastructure capabilities that could be susceptible to permanent and transient faults. Figure 2 shows some of the key safety mechanisms that are available on the latest C2000 Generation 3 MCUs.

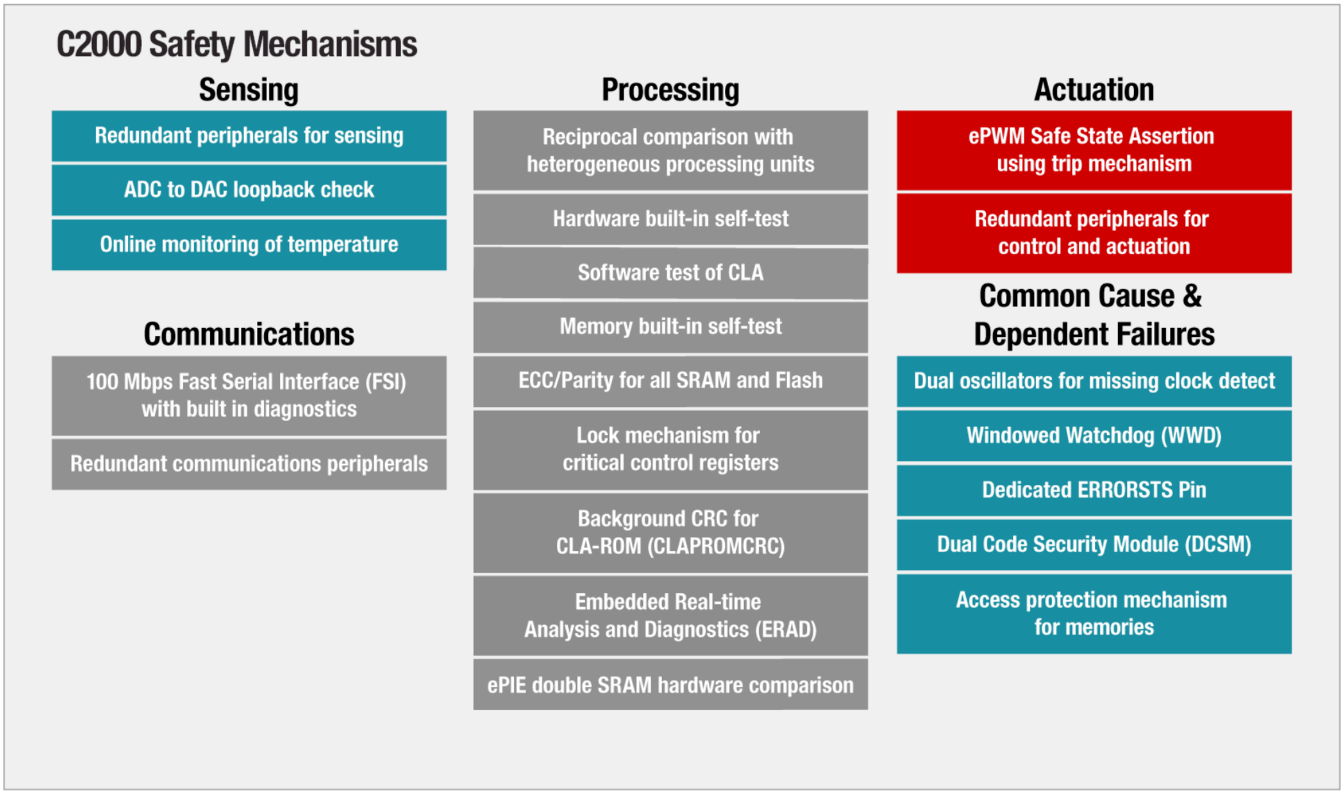
C2000 Safety Mechanisms
Sensing
Redundant peripherals for sensing
ADC to DAC loopback check
Online monitoring of temperature
Communications
100 Mbps Fast Serial Interface (FSI) with built in diagnostics
Redundant communications peripherals
Processing
Reciprocal comparison with heterogeneous processing units
Hardware built-in self-test
Software test of CLA
Memory built-in self-test
ECC/Parity for all SRAM and Flash
Lock mechanism for critical control registers
Background CRC for CLA-ROM (CLAPROMCRC)
Embedded Real-time Analysis and Diagnostics (ERAD)
ePIE double SRAM hardware comparison
Actuation
ePWM Safe State Assertion using trip mechanism
Redundant peripherals for control and actuation
Common Cause & Dependent Failures
Dual oscillators for missing clock detect
Windowed Watchdog (WWD)
Dedicated ERRORSTS Pin
Dual Code Security Module (DCSM)
Access protection mechanism for memories

Figure 2. Key Safety Mechanisms in the Latest C2000 Generation 3 MCUS

These safety mechanisms enable enhancing system safety capability without compromising the real-time-control latency requirements. Some of the key safety mechanisms featured on our generation 3 MCUs include:

- Background-CRC (BGCRC): Allows CRC checking program code without using CPU MIPs
- Embedded Real-time Analysis & Diagnostics (ERAD): can be used for advanced system level diagnostics
- Configurable Logic Block (CLB): used for implementing complex system-level PWM protection schemes while also reducing overall system BOM costs

C2000 provides over 300 safety mechanisms to use in the development of functional safety-compliant systems up to the safety integrity levels of ASIL D and SIL 3 as defined by the ISO 26262 and IEC 61508 functional safety standards, respectively. This document outlines some of the new safety mechanisms that have been introduced in the latest C2000 Generation 3 MCUs that customers can take advantage of in the development of their next generation functional safety compliant systems. Table 1 outlines the capability supported in our Generation 2 MCUs and the new (more effective or more efficient) capabilities on our Generation 3 MCUs.

Table 1. New/Improved Safety Mechanisms in the Gen3 Devices

NO	Safety Requirement	Capability Supported by Gen2 Devices	New Capability Supported by Gen3 Devices	Description	F2807x/ F2837xS/D	F28004x	F28002x
1	Clock integrity check	External clock monitoring or software based clock monitoring using Timer or HRPWM module	Dual Clock Comparator (DCC)	Dedicated hardware based clock monitor freeing up CPU MIPS and peripherals for application usage		√	√
2	CPU integrity check (CPU permanent fault detection)	Customer developed test. No quantified structural coverage	C2000™ Hardware Built-In Self-Test	Patented technology to provide high diagnostic coverage in a very short duration	√		√
3	Real time analysis and diagnostics for the CPU	No hardware support. Complex software based checks required	Embedded Real Time Analysis and Diagnostics (ERAD) engine	Dedicated hardware module to help with system analysis and diagnostics		√	√
4	Data integrity check, end to end (E2E) safeing	Software based CRC computation	Accelerators: Enhancing the Capabilities of the C2000 MCU Family Technical Brief	Co-processor with new instructions to make CRC computations faster	√	√	√
5	Continuous independent monitor for the CPU. Support for diagnostic execution without impacting critical control loop execution	No capability existed	CLA background task	CLA is enhanced with interruptible background task capability whereby the diagnostic (monitoring) software can be executed as a lower priority task without compromising the real time control performance		√	√
6	CLA integrity check (CLA permanent fault detection)	Customer developed test. No quantified structural coverage	C2000™ CLA Self-Test Library	Developed to be used for both start-up and application time self-test	√	√	√
7	Interrupt vector memory integrity check	Software based periodic checks	PIE double SRAM hardware comparison	Dual modular redundancy for interrupt vector memory	√	√	√
8	Flash integrity check	No capability existed	ECC	Flash memory supports Single Error Correction, Double Error Detection (SECDED) Error Correcting Code (ECC) diagnostic with coverage for both address and data bits	√	√	√
9	SRAM and ROM integrity check	No capability existed	ECC or parity	Selected on-chip SRAMs and ROMs support SECDED ECC or parity diagnostic with coverage for both address and data bits	√	√	√
10	SRAM and ROM integrity check at boot-up	Software based boot-time checks	C2000 Memory Power-On Self-Test (M-POST)	Fast power-on self-test of memory using dedicated hardware		√	√
11	SRAM and ROM integrity check during application	Software based periodic checks	Background CRC	Patented technology to perform CRC check of static memory content and scrubbing of dynamic memory contents without application MIPS consumption			√
12	CLA program ROM integrity check during application	Software based periodic checks	Background CRC for CLA program ROM	Patented technology to perform CRC check of CLA program ROM in the background without application MIPS consumption.		√	
13	Advanced PWM fault detection	Fault detection using external components like CPLD or FPGA	ePWM fault detection using CLB	Configurable Logic Block (CLB) can be used for detecting different erroneous conditions (e.g. Wrong dead-band, incorrect waveform, and so forth) which the PWMs will generate in the presence of faults	√	√	√
14	ADC conversion plausibility check	Software based checks	ADC post processing block	Additional hardware added to ADC module to perform plausibility check	√	√	√
15	ADC pin integrity check	No capability existed	Opens and shorts detection circuit for ADC input pin	Built in diagnostics which can be executed during start-up or during application time to identify opens or shorts on the ADC pin	√	√	√

Table 1. New/Improved Safety Mechanisms in the Gen3 Devices (continued)

NO	Safety Requirement	Capability Supported by Gen2 Devices	New Capability Supported by Gen3 Devices	Description	F2807x/ F2837xS/D	F28004x	F28002x
16	Comparator reference integrity check	No capability existed	VDAC conversion by ADC	Correct functioning of comparator is very critical from a system safety perspective. The reference voltage of the comparator can be checked using this.	√	√	√
17	Reliable high-speed communication across isolation barriers	Serial Peripheral Interface	Fast Serial Interface (FSI)	Several built in diagnostics (e.g. hardware ping to detect line breaks, data ECC, CRC, and so forth.) and hardware features (skew compensation, Double Data Rate (DDR), and so forth.) to support high speed reliable communication		√	√
18	Watchdog with separate time base and time-window	Watchdog with separate time base	Windowed watchdog	Windowed watchdog with counter running on an independent clock	√	√	√
19	Prevention of unintended register programmation due to faults	Periodic software read-back of register	Multi-bit enable keys for control registers	Prevents unintentional activation/deactivation as multiple bits need to be correct to enable or disable the critical functionality.	√	√	√
20	Prevention of unintended register programmation due to faults	Periodic software read-back of registers	Lock mechanism for registers	Write access to the registers can be blocked or enabled by configuring the lock bits	√	√	√
21	Critical error intimation to external world	GPIO based critical error intimation using software	ERRORSTS pin	Dedicated (configurable pin) to intimate critical errors to external world without software intervention	√	√	√
22	Freedom from interference - avoid interference from unused modules	Software intensive check	Peripheral soft reset	This capability can be used to keep the unused peripherals in reset.	√	√	√
23	Freedom from interference - access (e.g. fetch, write) gating for individual RAM blocks from different masters (viz. CPU,CLA,DMA)	No capability existed	Access protection mechanism for memories	This configuration can be changed during run-time and allows memory to block access from specific masters or specific application threads within the same master	√	√	√
24	Freedom from interference – access gating for individual peripherals from different masters	No capability existed	Peripheral access protection	This configuration can be changed during run-time and allows peripherals to block access from specific masters or specific application threads within the same master		√	√
25	Freedom from interference - ability to run two independent application threads without interference	No capability existed except for F2805x	Achieving Coexistence of Safety Functions for EV/HEV Using C2000 MCUs	Application threads with different safety integrity levels can be executed from different security zones (for example, zone1, zone2.) thus mitigating the risk due to interference from one function to another	√	√	√

Detailed descriptions for each of the above mentioned safety mechanisms can be found in the Functional Safety Manual for the corresponding C2000 Generation 3 MCUs. For a list of Functional Safety related collateral for C2000 including Functional Safety Manuals, Diagnostic Software Library, compiler qualification kits, third party operating systems and development tools and additional Functional Safety related documentation, see the *C2000 Functional Safety Enablers*. To learn more about C2000 Functional Safety, see http://www.ti.com/microcontrollers/c2000-real-time-control-mcus/overview.html#safety.

2 References

- *C2000 Functional Safety Enablers*

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