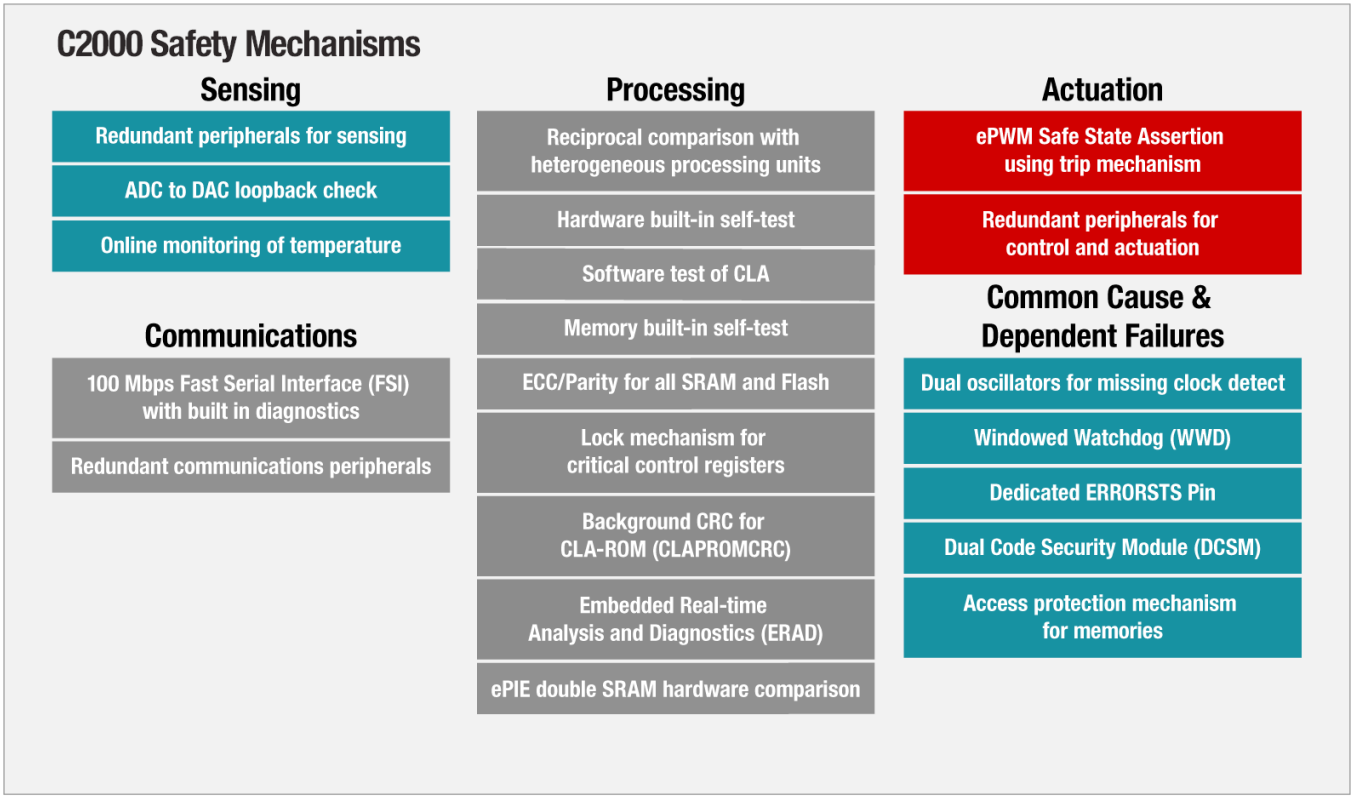
C2000™ Safety Mechanisms



Introduction

According to the International Electrotechnical Commission (IEC), safety is defined as freedom from unacceptable risk of physical injury or damage to the health of people, either directly or indirectly, as a result of damage to property or to the environment. The IEC defines functional safety as the part of overall safety that depends on a system or equipment operating correctly in response to its inputs.

The focus on functional safety has grown significantly in recent years. As a result, development of functional safety-compliant systems capable of ensuring safe operation in the event of dangerous failures has become a priority for companies and engineers alike. These functional safety-compliant systems can not only detect potentially dangerous conditions; they can also deploy appropriate safety mechanisms to take a system to a safe state.

C2000™ SafeTI™ products provide more than 300 safety mechanisms to use in the development of functional safety-compliant systems up to the safety integrity levels of ASIL D/SIL 3 as defined by the International Organization for Standardization ISO 26262 and IEC 61508 standards, respectively.

Sensing

- **Redundant peripherals for sensing**
  - Hardware redundancy on peripherals like a sigma-delta filter module (SDFM), analog-to-digital converter (ADC), enhanced capture (eCAP) and enhanced quadrature encoder pulse (EQEP) is possible by having multiple instances of the peripheral sample the same input and simultaneously perform the same operation followed by a cross-check of the output values.
- **ADC-to-DAC loopback check**
  - Monitoring digital-to-analog converter (DAC) outputs using ADCs checks DAC and ADC integrity. Applying this technique during runtime ensures that proper voltage levels are being driven from the DAC.

- **Online temperature monitoring**
  - An internal temperature sensor measures the junction temperature of the device. The ADC can sample the output of the sensor through an internal connection to detect temperature variations.

Processing

- **Reciprocal comparison with heterogeneous processing units**
  - The C28x central processing unit (CPU) and control law accelerator (CLA) are a 1oo1D architecture providing high diagnostic coverage for the processing units (per ISO 26262-5, Table D.4.).
  - Cross-checking enables hardware and software diversity, since the C28x CPU and CLA are diverse processing units with a different architecture, instruction set and completely orthogonal toolchains. Executing algorithms on both the cores can further increase the diversity.
- **Hardware BIST**
  - The hardware built-in self-test (BIST) provides high diagnostic coverage on C28x CPUs during startup and application time.
  - There are options to run all tests or only a subset of the tests based on the execution time allocated to the hardware BIST diagnostic.
  - A time-sliced test feature enables the hardware BIST to be used effectively as a runtime diagnostic with the execution of test in parallel with the application.
  - Read the application report, "C2000 Hardware Built-In Self-Test."
- **CLA software test**
  - A software-based self-test library (STL) makes it possible to test the integrity of various CLA blocks such as the register bank, control unit and data path.
  - This test may be performed at startup (synchronized with key on/off cycles) or time-sliced and run in-system to fit within the process safety time (PST) or fault-tolerant time interval (FTTI).
- **Memory BIST**
  - The memory BIST can identify embedded memory circuitry that has degraded during system use.
  - This startup test (synchronized with key on/off cycles) can protect against latent memory faults.
  - Read the application report, "C2000 CPU Memory Built-In Self-Test."
- **ECC/parity for all SRAM and flash**
  - A single error correction, double error detection (SECDED) error-correcting code (ECC) diagnostic supports the on-chip flash memory.
  - Selected on-chip static random access memory (SRAM) supports the SECDED ECC diagnostic with separate ECC bits for data and address, as well as the parity diagnostic with separate parity bits for data and address.
  - Read the application report, "Error Detection in SRAM."
- **Lock mechanism for critical control registers**
  - After configuring the control registers, configuring the associated lock register locks write access. Locked registers cannot be updated by software. Once locked, only reset can unlock the registers.
- **Background CRC for CLA ROM**
  - This safety feature performs a cyclic redundancy check (CRC) on a configurable block of memory in the CLA program read-only memory (CLAPROMCRC) space.
- **ERAD module**
  - The embedded real-time analysis and diagnostics (ERAD) module provides system analysis capabilities that can detect faults in the CPU and other logic on the MCU by configuring bus comparator units that monitor CPU buses and counter units that count events.
- **ePIE double SRAM hardware comparison**
  - The enhanced peripheral interrupt expansion (ePIE) module interfaces peripheral interrupts to the C28x CPU.
  - The PIE SRAM address space is duplicated and data is placed in two memories.
  - During write operations, both SRAMs update simultaneously and compare the values from both memories on reading.
  - In case of an error during comparison, the CPU will branch to a predefined location that will have the interrupt service routine (ISR) for error management.

Actuation

- **ePWM safe-state assertion using trip mechanism**
  - The enhanced pulse-width modulator (ePWM) safe state can be asserted using any of the general-purpose input/output (GPIO) pins. These pins can be flexibly mapped to be the trip-zone input and/or trip inputs to the trip-zone submodule and digital compare submodule.

- The digital compare submodule compares signals external to the ePWM module to directly generate PWM events/actions that then feed to the event-trigger, trip-zone and time-base submodules.
- Blanking window functionality filters noise or unwanted pulses from the digital compare event signals.

- **Redundant peripherals for control and actuation**
  - Hardware redundancy on peripherals like GPIO, crossbar (XBAR), PWM, OTTO (high-resolution PWMs), DAC, comparator subsystem (CMPSS) and transmit interrupt (XINT) is possible by having multichannel parallel outputs where independent outputs transmit information. Failure detection is carried out through internal or external comparators or by input comparison, which compares independent inputs to ensure compliance with a defined tolerance.

Communications

- **100 Mbps FSI with built-in diagnostics**
  - A proprietary Fast Serial Interface (FSI) with up to 100 Mbps across isolation provides several intrinsic diagnostic capabilities such as CRC framing checks, ECC framing checks, frame overrun detection and frame watchdog timeout.
- **Redundant communications peripherals**
  - Hardware redundancy on peripherals like CAN (Controller Area Network), Serial Peripheral Interface (SPI), serial communications interface (SCI) and Inter-Integrated Circuit (I^2C) during signal reception is possible by having multiple instances of the peripheral receive the same data, followed by comparison to ensure data integrity.
  - Hardware redundancy during transmission is possible by having a completely redundant signal path from the transmitter to the receiver, or sampling the transmitted data with a redundant peripheral instance followed by a data integrity check.

Common cause failure and dependent failure analysis (CCF/DFA)

- **Dual oscillators and MCD**
  - The missing clock detect (MCD) can detect a failure of the phase-locked loop (PLL) reference clock. The MCD uses the embedded 10 MHz internal oscillator (INTOSC1).
- **WWD**
  - The internal watchdog has two modes of operation: normal watchdog (WD) and windowed watchdog (WWD).
  - For WWD, programming an upper bound and a lower bound creates a time window during which the software must provide a predetermined WDKEY to the watchdog.
  - Failure to receive the correct response within the time window or an incorrect WDKEY triggers an error response.
  - The WWD can issue either a warm system reset or a CPU-maskable interrupt upon detection of a failure.
- **Dedicated ERRORSTS pin**
  - The ERRORSTS pin is an “always output” pin and remains low until an error is detected inside the chip. Upon detection, the ERRORSTS pin goes high until the corresponding internal error status flag for that error source clears.
- **DCSM**
  - The dual-code security module (DCSM) prevents access and visibility to on-chip secure memories (and other secure resources) to unauthorized persons.
  - It also prevents duplication and reverse engineering of proprietary code.
  - Read the white paper, “Achieving Coexistence of Safety Functions for EV/HEV”
- **Access protection mechanism for memories**
  - This mechanism enables or disables specific access (fetch, write) to individual RAM blocks from individual masters.
  - Reads are always allowed from masters that have access to the RAM block. This configuration can be changed during runtime and allows memory to block access from specific masters or specific application threads within the same master.
  - This capability helps support freedom from interference requirements.

To learn more about C2000 Functional Safety, please visit www.ti.com/c2000safeTI

IMPORTANT NOTICE FOR TI DESIGN INFORMATION AND RESOURCES

Texas Instruments Incorporated ('TI") technical, application or other design advice, services or information, including, but not limited to, reference designs and materials relating to evaluation modules, (collectively, "TI Resources") are intended to assist designers who are developing applications that incorporate TI products; by downloading, accessing or using any particular TI Resource in any way, you (individually or, if you are acting on behalf of a company, your company) agree to use it solely for this purpose and subject to the terms of this Notice.

TI's provision of TI Resources does not expand or otherwise alter TI's applicable published warranties or warranty disclaimers for TI products, and no additional obligations or liabilities arise from TI providing such TI Resources. TI reserves the right to make corrections, enhancements, improvements and other changes to its TI Resources.

You understand and agree that you remain responsible for using your independent analysis, evaluation and judgment in designing your applications and that you have full and exclusive responsibility to assure the safety of your applications and compliance of your applications (and of all TI products used in or for your applications) with all applicable regulations, laws and other applicable requirements. You represent that, with respect to your applications, you have all the necessary expertise to create and implement safeguards that (1) anticipate dangerous consequences of failures, (2) monitor failures and their consequences, and (3) lessen the likelihood of failures that might cause harm and take appropriate actions. You agree that prior to using or distributing any applications that include TI products, you will thoroughly test such applications and the functionality of such TI products as used in such applications. TI has not conducted any testing other than that specifically described in the published documentation for a particular TI Resource.

You are authorized to use, copy and modify any individual TI Resource only in connection with the development of applications that include the TI product(s) identified in such TI Resource. NO OTHER LICENSE, EXPRESS OR IMPLIED, BY ESTOPPEL OR OTHERWISE TO ANY OTHER TI INTELLECTUAL PROPERTY RIGHT, AND NO LICENSE TO ANY TECHNOLOGY OR INTELLECTUAL PROPERTY RIGHT OF TI OR ANY THIRD PARTY IS GRANTED HEREIN, including but not limited to any patent right, copyright, mask work right, or other intellectual property right relating to any combination, machine, or process in which TI products or services are used. Information regarding or referencing third-party products or services does not constitute a license to use such products or services, or a warranty or endorsement thereof. Use of TI Resources may require a license from a third party under the patents or other intellectual property of the third party, or a license from TI under the patents or other intellectual property of TI.

TI RESOURCES ARE PROVIDED "AS IS" AND WITH ALL FAULTS. TI DISCLAIMS ALL OTHER WARRANTIES OR REPRESENTATIONS, EXPRESS OR IMPLIED, REGARDING TI RESOURCES OR USE THEREOF, INCLUDING BUT NOT LIMITED TO ACCURACY OR COMPLETENESS, TITLE, ANY EPIDEMIC FAILURE WARRANTY AND ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT OF ANY THIRD PARTY INTELLECTUAL PROPERTY RIGHTS.

TI SHALL NOT BE LIABLE FOR AND SHALL NOT DEFEND OR INDEMNIFY YOU AGAINST ANY CLAIM, INCLUDING BUT NOT LIMITED TO ANY INFRINGEMENT CLAIM THAT RELATES TO OR IS BASED ON ANY COMBINATION OF PRODUCTS EVEN IF DESCRIBED IN TI RESOURCES OR OTHERWISE. IN NO EVENT SHALL TI BE LIABLE FOR ANY ACTUAL, DIRECT, SPECIAL, COLLATERAL, INDIRECT, PUNITIVE, INCIDENTAL, CONSEQUENTIAL OR EXEMPLARY DAMAGES IN CONNECTION WITH OR ARISING OUT OF TI RESOURCES OR USE THEREOF, AND REGARDLESS OF WHETHER TI HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

You agree to fully indemnify TI and its representatives against any damages, costs, losses, and/or liabilities arising out of your non-compliance with the terms and provisions of this Notice.

This Notice applies to TI Resources. Additional terms apply to the use and purchase of certain types of materials, TI products and services. These include; without limitation, TI's standard terms for semiconductor products http://www.ti.com/sc/docs/stdterms.htm), evaluation modules, and samples (http://www.ti.com/sc/docs/sampterms.htm).

Mailing Address: Texas Instruments, Post Office Box 655303, Dallas, Texas 75265