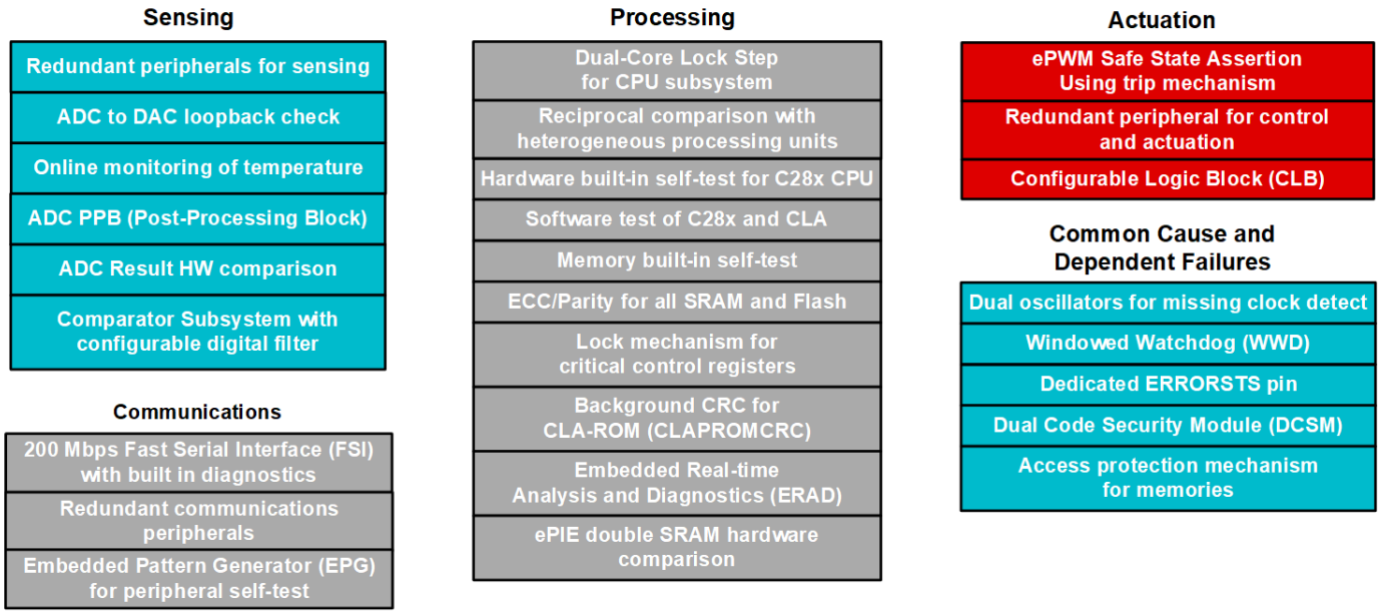
C2000™ real-time MCU Safety Mechanisms

TEXAS INSTRUMENTS

C2000 Key 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, the 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 components can detect potentially dangerous fault conditions and deploy an appropriate safe state to take the overall system to a defined 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 redundantly 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.
- **ADC PPB (Post-Processing Block)**
  - Each ADC with four PPB can do processing of ADC results such as removing offset and subtracting a reference value. PPB can also flag a zero-crossing or perform high/low comparison with a reference value, etc. The output of the PPB can interrupt the CPU or generate a direct trigger for actuating a safe state independent of the CPU.
- **ADC Results HW Comparison**
  - ADC Results safety checker feature can automatically compare two ADC conversion results and check the integrity between them with programmable tolerances. This eliminates the comparison of the results in SW thereby saving valuable CPU cycles for implementing ADC Hardware Redundancy for each conversion.
- **CMP Subsystem with digital filter**
  - The Comparator Subsystem (CMPSS) consists of analog comparators with built-in DAC for reference and supporting circuits that are useful for implementing safety functions such as voltage monitoring. The configurable digital filter on the CMPSS output event can eliminate the spurious events being reported. CMP module can generate an interrupt to the CPU or trigger the safe state using XBAR architecture independent of the CPU.

Processing

- **"Dual Core Lock-Step" and "Reciprocal comparison with heterogeneous processing units"**
  - Dual Core Lock-step configuration of the C28x CPU cores along with the Lock-step Comparator Module (LCM) implements the HW redundancy as per 1oo1D safety architecture in HW to provide detection of faults inside the CPU during runtime of the safety function.
  - The Reciprocal comparison by SW between C28x central processing unit (CPU) and control law accelerator (CLA) is an alternate 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 different ISA (Instruction Set Architecture) and completely orthogonal toolchains. Executing algorithms on both 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 the 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 a 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 the key on/off cycle) 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."
- Parity detection mechanism in C2000 MCUs is implemented to provide 'High' diagnostic coverage (DC>=99%) for Soft Errors (SER). Please contact TI for more details on this.

- **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 the 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 action on the input trip event (High-Impedance, Force to High state, or Force to Low state) can be configured independently for each PWM output.
- **Configurable Logic Block (CLB)**
  - The configurable logic block (CLB) is a collection of configurable blocks that can be inter-connected to implement custom digital logic functions as a safety mechanism independent of the CPU to trigger the safe state. This can eliminate the need for custom logic in the system for implementing certain functional safety functions.
  - 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.

- **EPG Embedded Pattern Generator**
  - The Embedded Pattern Generator (EPG) module is a customizable pattern and clock generator that could serve as test and application scenarios.
  - On-chip pattern generation capability can be used to test serial communication peripherals like CAN with error conditions. This can build confidence in the error detection capability of the safety mechanism inside CAN and help improve the Latent Fault Metric without requiring complex error injection at the system.

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™ Automotive Functional Safety offerings, see www.ti.com/lit/swab014

For C2000™ Industrial Functional Safety offerings, see www.ti.com/lit/swab013

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