Product Overview

Implementing IEC 60730 / UL 1998 Compliance for C2000 Real-Time Microcontrollers

TEXAS INSTRUMENTS

ABSTRACT

Motor drives, white goods, appliances, and other equipment can become unsafe to operate if one of their components fail. These equipments are subject to the testing and qualification requirements of the International Electrotechnical Commission (IEC). Specifically, the IEC 60730-1 “Automatic electrical controls for household and similar use” safety standard. Similar practices are followed in the United States leveraging UL 1998 “Safety Software in Programmable Components.”

The aspects most relevant to microcontrollers (MCUs) are IEC 60730 Annex H and UL 1998 Annex A.2, which detail the diagnostic test requirements to support safe function of home appliances.

This document provides a high-level overview of these specifications as applied to an MCU and describes how C2000™ functional safety features can be leveraged to meet the diagnostic test requirements.

Trademarks

C2000™ is a trademark of Texas Instruments.
All trademarks are the property of their respective owners.

Introduction

Motor drives, white goods, appliances, and other equipment may become unsafe to operate if one of their components fail. These equipments are subject to the testing and qualification requirements of the International Electrotechnical Commission (IEC). Specifically, the IEC 60730-1 standard covers automatic electrical controls for household and similar use.

Although compliance to IEC 60730 is attained at a system level, understanding the correct criteria for choosing a microcontroller is important to achieve compliance. The use of electronic components such as microcontrollers (MCU) is addressed by Table H.1 in Annex H of IEC 60730 "Requirements for electronic controls". Annex H specifies acceptable diagnostic techniques and measures applicable to an MCU in order to support the safe function of equipment.

While IEC 60730 is primarily used in Europe, similar practices are followed in the United States leveraging UL 1998 “Safety Software in Programmable Components.” Table A2.1 in Appendix A, provides examples of acceptable measures for microelectonic hardware failure modes that are consistent with the requirements of IEC 60730 Table H.1. These requirements are derived from the IEC 61508 standard, “Functional safety of electrical/electronic/programmable electronic (E/E/PE) systems.”

Overview of IEC 60730 and UL 1998 Classifications

To create a foundation for fault control techniques, both the IEC 60730 and UL 1998 specifications divide products into classes. The class assignment is determined by a hazard and risk analysis applied to the specific control. This analysis is based on both the likelihood of the failure and the resulting consequence of the failure.

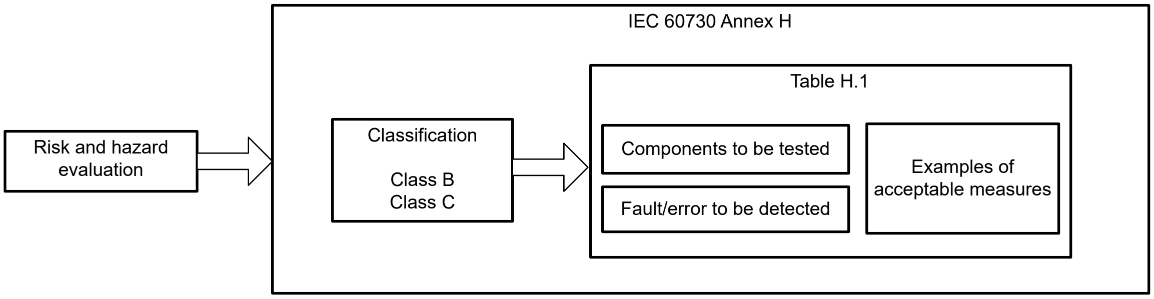
Risk and hazard evaluation
IEC 60730 Annex H
Classification
Class B
Class C
Table H.1
Components to be tested
Fault/error to be detected
Examples of acceptable measures

Figure 1. IEC 60730 Annex H

IEC 60730 defines 3 classes: A, B and C:

- Class A: controls are not related to safety
- Class B: controls intended to prevent unsafe operation
- Class C: controls intended to prevent dangerous hazards

UL 1998 defines two classes: 1 and 2. UL 1998 class 1 is comparable to IEC 60730 class B and UL 1998 class 2 is comparable to IEC 60730 class C. For class definitions and examples, see Table 1.

Table 1. Class Definitions and Examples

Class	Definition [1]	Examples
IEC 60730 class A	"H.2.22.1 class A control function - control functions that are not intended to be relied upon for the safety of the application"	Room thermostats, temperature control.
IEC 60730 class B and UL 1998 class 1	"H.2.22.2 class B control function - control functions that are intended to prevent an unsafe state of the appliance. Note: Failure of the control function will not lead directly to a hazardous situation.	Thermal cut-out. Door locks for laundry equipment.
	"A3.1 Software Class 1: Sections of software intended to control function to reduce the likelihood of a risk associated with the equipment."	
IEC 60730 class C and UL 1998 class 2	"H.2.22.3 class C control function - control functions that are intended to prevent special hazards such as explosion or whose failure could directly cause a hazard in the appliance"	Automatic burner controls. Thermal cut-outs for a closed water heater system.
	"A3.2 Software Class 2 – Sections of software intended to control functions to reduce the likelihood of special risks (for example, explosion) associated with the equipment."	

[1] Reference: IEC 60730-1 Annex H and UL 1998 Appendix A

The standards define the components that must be tested along with examples of acceptable measures to detect faults/errors of that component. Depending on the class, the components to test include the CPU, clocks, volatile and non-volatile memory, internal data path, I/O and communication interfaces (Table 2). In general, for each component there are a few types of measures that the developer can choose from to verify/test component functionality. These suggested measures can be:

- Hardware-based
- Software-based
- A combination of both hardware- and software-based

The implementation of IEC 60730 acceptable measures are meant to detect, and prevent, unsafe conditions and hazards associated with the equipment. These requirements are derived from the IEC 61508 standard "Functional safety of electrical/electronic/programmable electronic (E/E/PE) systems." The focus of IEC 61508 is how to apply, design, and maintain automatic protection systems called safety-related systems.

Table 2. Summary of Failure Modes Described by IEC 60730 / UL 1998

Component to be Tested		Hardware Fault / Error to Detect [1]	
		Class B / 1	Class C / 2
1. CPU	1.1 Registers	Stuck-at	DC fault
	1.2 Instruction decode and execution	N/A [2]	Wrong decode and execution
	1.3 Program counter	Stuck-at	DC fault
	1.4 Addressing	N/A	DC fault
	1.5 Data paths	N/A	DC fault
2. Interrupts		None or too frequent	None or too frequent related to different sources
3. Clock		Wrong frequency	Wrong frequency
4. Memory	4.1 Non-volatile	All single bit faults	All single and double bit errors
	4.2 Volatile	DC fault	DC fault and dynamic cross links
	4.3 Addressing	Stuck at	DC fault
5. Internal data path	5.1 Data	Stuck-at	DC fault
	5.2 Addressing	Wrong address	Wrong address, multiple addressing

Table 2. Summary of Failure Modes Described by IEC 60730 / UL 1998 (continued)

Component to be Tested		Hardware Fault / Error to Detect [1]	
		Class B / 1	Class C / 2
6. External communication	6.1 Data	All single-bit and double bit errors	All single-bit, double-bit and triple-bit errors
	6.2 Addressing	Wrong address	Wrong and multiple addressing
	6.3 Timing	Wrong point in time	Wrong point in time
		Wrong sequence	Wrong sequence
7. Input/output periphery	7.1 Digital I/O	Open and short circuit or as specified in the product standard	Open and short circuit or as specified in the product standard
	7.2 Analog I/O 7.2.1 A/D and D/A converter	Open and short circuit or as specified in the product standard	Open and short circuit or as specified in the product standard
	7.2 Analog I/O 7.2.2 Analog multiplexer	Wrong addressing	Wrong addressing
8. Monitoring devices and comparators		N/A	Any output outside the static and dynamic functional specification
9. Components not covered by 1-8. Custom chips, ASIC, GAL, Gate array		Any output outside the static and dynamic functional specification	Any output outside the static and dynamic functional specification

[1] Reference: IEC 60730-1 Table H.1 and UL 1998 Table A.2

[2] N/A (not applicable): detection of this error/fault is not required by the standards for this specific class.

C2000 Capability by Device Family

The C2000 device capability in Table 3 is derived based on IEC 60730 example fault/error detection methods mapped to suggested device diagnostics and functional-safety features. This mapping is described in the remainder of this document.

Table 3. IEC 60730 / UL 1998 Capability per C2000 Device Family

Device Family	Class B / 1	Class C / 2
F280013x	✓	
F280015x	✓	✓
F28002x	✓	✓
F28003x	✓	✓
F28004x	✓	✓
F2807x	✓	✓
F2837xD, F2837xS	✓	✓
F2838x	✓	✓

C2000 Safety Collateral

TI provides safety-related collateral to aid in system development and assessment. This section describes collateral that can be leveraged to meet IEC 60730 and UL 1998.

Getting Started

To become familiar with C2000 functional safety capabilities the following documents are recommended:

- *C2000™ Safety Mechanisms*: introduction to C2000 device features that supports functional safety.
- *Industrial Functional Safety for C2000 Real-Time Microcontrollers*: highlights specific-device capabilities, collateral, and documentation to support industrial functional-safety standards.

The next level of collateral is further discussed in this chapter:

- Functional Safety Manuals (FSMs): comprehensive, device-specific, functional-safety related documentation.
- Diagnostic and self-test software collateral.

Additionally, the following collateral is useful for further information on the C2000 Software Diagnostic Library:

- *Obtain UL/IEC 60730-1/60335-1 Class B Certification Based on C2000™ MCU Diagnostic Library in Appliances*: in-depth explanation of various software diagnostic library modules and how these are applicable to UL/IEC 60730-1/60335-1.

Note

The F2806x, F2803x, F2805x, F2802x, F2833x and F2823x C2000 families are not included in this document. For these devices, see the *Safety Manual for C2000 MCUs in IEC60730 Safety Applications User's Guide.*

Functional Safety Manuals

The equipment designer and manufacturer are responsible for ensuring a system meets all applicable safety, regulatory, and performance requirements. Most C2000 Functional Safety Manuals are part of a Functional Safety-Compliant design package to aid in compliance with ISO 26262 or IEC 61508 functional safety standards.

A subset of the safety manual can aid in designing for IEC 60730 requirements. Topics of interest to the IEC 60730-focused designer are listed in Table 4. Additional topics not directly applicable to IEC 60730 may also be helpful.

Table 4. Functional Safety Manual Topics

The IEC 60730-focused developer should pay particular attention to:	Additional topics may be helpful. These include:
• Description of suggested safety features and diagnostics that are mapped to IEC 60730 acceptable measures in Section Mapping Acceptable Control Measures to C2000 Unique Identifiers. • Guidelines for implementing diagnostics. • Description of the software diagnostic library and self-test libraries. • While some Unique IDs may not map directly to IEC 60730, or may only provide partial coverage, implementation is highly-recommended. Examples of such best-practices are discussed in Section Additional Best Practices.	• Product overview. • Device architecture drawing with safety features highlighted. • Comprehensive list of all safety features and diagnostics. • List of safety features specific to peripherals. • Descriptions of diagnostics, test for diagnostics, and fault avoidance measures. • Suggestions for improving freedom from interference. • Suggestions for addressing common cause failures

Within the functional safety manual, a C2000 Unique Identifier (Unique ID) identifies specific safety features and diagnostics. These diagnostics can be divided into:

- A safety diagnostic
- A test of a safety diagnostic
- A fault avoidance technique

The implementation can be:

- Hardware: implemented in TI silicon
- Software: must be implemented in the application software
- Hardware plus software: requires both hardware implemented in silicon and software within the application
- System: implemented externally to the microcontroller

This document is meant to aid in mapping a IEC 60730 requirement to a suggested C2000 Unique IDs (Section Mapping Acceptable Control Measures to C2000 Unique Identifiers). The system designer can then reference the Functional Safety Manual's description and implementation suggestions for each Unique ID. This approach is described in Section Mapping Acceptable Control Measures to C2000 Unique Identifiers.

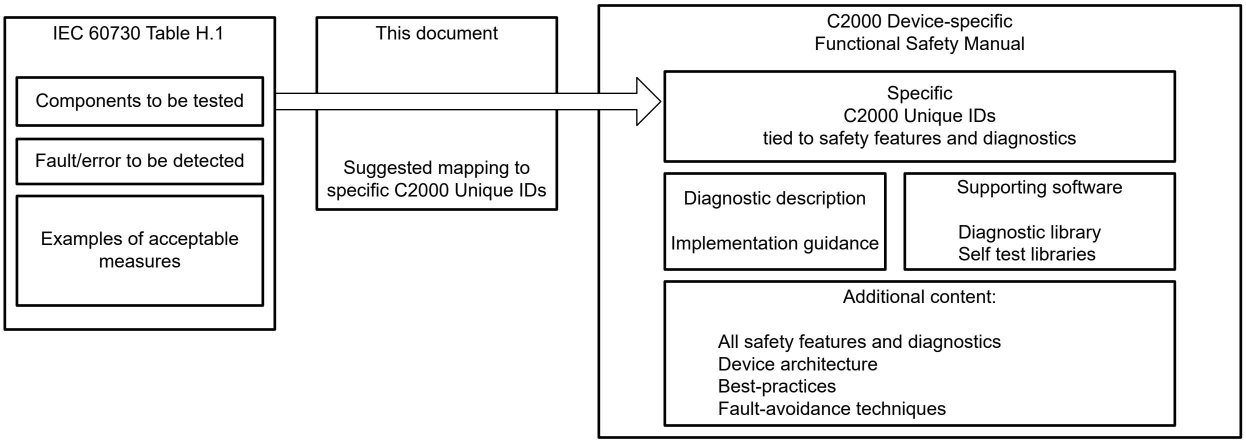
IEC 60730 Table H.1
Components to be tested
Fault/error to be detected
Examples of acceptable measures
This document
Suggested mapping to specific C2000 Unique IDs
C2000 Device-specific Functional Safety Manual
Specific C2000 Unique IDs tied to safety features and diagnostics
Diagnostic description
Implementation guidance
Supporting software
Diagnostic library
Self test libraries
Additional content:
All safety features and diagnostics
Device architecture
Best-practices
Fault-avoidance techniques

Figure 2. Mapping Acceptable Measures to C2000 Functional Safety Manuals

Software Collateral

While C2000 devices have several hardware safety features, the application level diagnostic software adds value to the hardware features. C2000 provides the following safety-related software packages:

- C28x Self-Test Library (C28x_STL)
- CLA Self-Test Library (CLA_STL)
- Software Diagnostic Library (SDL)

Software Diagnostic Library

Features:

- A collection of C-callable, optimized, independent test functions.
- Called and managed by the user's application.
- When a failure is detected, the application determines the system-appropriate action.
- Each function executes a specific task to verify the functionality of a component.
- Leverages safety mechanisms consistent with safety standards.
- Has minimal impact on the MCU's real-time control performance.
- The User's Guide includes benchmarks.
- Supports power-on test, periodic test, or both.
- Demonstrates library usage and configuration of diagnostic features.

Examples include:

- CAN message RAM March and parity logic test
- CRC code for communications and memory tests
- Interface to CPU HWBIST capabilities
- PIE RAM redundancy test
- Clock frequency test
- CPU register test
- PIE RAM redundancy test

Refer to the safety manual's C2000 Safety Diagnostics Libraries chapter.

Availability:

- F2837xS, F2837xD and F2807x download here
- Other device SDLs are in C2000Ware. See the libraries/diagnostic directory.
- Documentation for each device SDL is located in the device-specific 'docs' folder.

C28x and CLA Self-Test Libraries

The self-test libraries (STL) check the CPU's logic integrity using the CPU itself. The STLs are independently assessed by TÜV SÜD and found to be suitable for being integrated into safety related systems up to ASIL D and SIL 3 according to ISO 26262:2018 and IEC 61508:2010 respectively.

C28X_STL Features:

- Represents a safety mechanism with the capability to detect permanent faults of the C28x CPU.
- Covers the CPU, FPU, TMU, VCU, and VCRC instruction sets.
- Supports only start-up testing.
- Available for Class-C, SIL-2 and SIL-3 capable-devices without hardware built-in self test (HWBIST).
- Includes a user's guide and compliance support package (CSP).

CLA_STL Features:

- Represents a safety mechanism with the capability to detect permanent faults of the Control Law Accelerator (CLA).
- Covers the CLA register bank, control unit, datapath, and so forth.
- Supports both start-up and periodic testing.
- Applies to any device with a CLA.
- Includes a user's guide and compliance support package (CSP).

Availability:

- The CLA_STL and C28X_STL are not released on TI.com. Contact your TI representative to request access.

Implementing Acceptable Measures on C2000 Real-Time MCUs

This section details a step-by-step approach to identifying functional safety diagnostics and software to implement IEC 60730 and UL 1998 acceptable measures.

Implementation Steps

To plan implementation of an acceptable measure, the suggested steps are:

Step	Description	References
Step 1	**Map acceptable measures to C2000 Unique IDs:** The specifications typically present the developer with a choice of acceptable measures to detect a specific fault. This document presents a mapping of some acceptable measures to Unique IDs. In some cases more than one Unique ID may apply.	• IEC 60730 or UL 1998 specification • This document: Section Mapping Acceptable Control Measures to C2000 Unique Identifiers
Step 2	**Plan the implementation:** Read the description and guidelines, or suggestions, for implementing Unique ID. You will also learn if the Unique ID implementation is based on hardware, software or both.	Device-specific Functional Safety Manual: Summary of Safety Features and Diagnostics
Step 3	**Identify supporting software:** Identify if the Unique ID is supported by the SDL or an STL.	• Device-specific Functional Safety Manual: Safety Diagnostics Libraries • This document: Section Software Collateral • SDL or STL documentation
	In some cases, a Unique ID is not supported by an SDL/STL module. This occurs when the Unique ID corresponds to a hardware mechanism with minimal, or no, software requirements, or the Unique ID requires a system-dependent implementation.	In these cases reference: 1. The FSM Unique ID description for implementation guidance and suggestions. 2. The C2000Ware Software Development Kit software examples to implement the requirements based on the FSM guidance. For example: • Populating PIE vectors, including unused vectors. • Embedded real-time analysis and diagnostic module (ERAD) examples. • VCRC module library to calculate CRCs. • Peripheral configuration.
Step 4	**Identify additional Unique IDs to implement:** Some IDs may not directly map to IEC 60370 but are still highly recommended. Many of these are hardware implementations and take little overhead in a system.	• Device-specific Functional Safety Manual • This document: Section Additional Best Practices

Example Mapping

Table 5 shows examples of mapping acceptable measures to C2000 Unique IDs. The specifications give the option to use one or more acceptable measures for the given class. It is up to the system designer to determine what is best suited for the application. In addition, a class C measure can be used to detect a class B fault/error. In example 1, the system designer could also use the acceptable measures for class C shown in example 2.

Table 5. Examples of Mapping to Unique IDs and Implementation Guidance

Example	Acceptable Measure to C2000 Unique ID 1	Implementation Guidance (FSM)
Example 1: Component: CPU registers Device: F28003x Class: B fault "Stuck at"	Maps to unique IDs for the measure "periodic self-test": • CPU2: CPU hardware built-in self test (HWBIST) • CLA2: Software test of CLA Note: The specifications indicate that a class C measure can also be selected to cover a class B fault.	The FSM describes: • Diagnostic coverage information. • How testing can be applied to check the integrity of each CPU • Details on implementing the test • Refers the developer to the diagnostic and self-test software documentation.
Example 2: Component: CPU registers Device: F28003x Class: C fault "DC fault"	Maps to the IDs: • CPU1/CLA1: Reciprocal comparison by software for the acceptable measure "reciprocal comparison" • CPU2: CPU hardware built-in self-test (HWBIST) for the acceptable measure "internal error detection"	The FSM: • Describes the HWBIST hardware feature. • Provides ideas for implementing reciprocal comparison. This diagnostic is highly system dependent. • Refers the developer to the diagnostic software documentation for the HWIBST software interface.

1. For more information, see the tables in Section Mapping Acceptable Control Measures to C2000 Unique Identifiers.

Additional Best Practices

This document is focused on C2000 Unique IDs that specifically map to IEC 60730 and UL 1998 requirements. The device-specific safety manual includes additional information that may assist the system designer. Review of the following functional safety manual sections is highly recommended:

- *Suggestions For Improving Freedom from Interference*
- *Suggestions for Addressing Common Cause Failures*
- *Summary of Safety Features and Diagnostics*
  - Fault avoidance techniques
  - Low/zero overhead hardware diagnostics
  - Tests of safety features and diagnostics.

Table 6 lists some examples. To determine additional best practices for your specific device family, refer to the device-specific functional safety manual.

Table 6. Example Additional Unique IDs of Interest

	Example C2000 Unique ID (1)	Description
Fault avoidance	CLK14	Peripheral clock gating.
	CPU6	Disable of JTAG port.
	DMA9	Disabling of unused DMA trigger sources
	FLASH3 (2)	Bit multiplexing in flash memory array
	RST2	Reset cause information
	SRAM4 (2)	Bit multiplexing in SRAM memory array
	SYS1 (2)	Multi-bit enable keys for control registers.
	SYS2	Lock mechanism for control registers
	SYS7	Peripheral soft reset (SOFTPRES).

Table 6. Example Additional Unique IDs of Interest (continued)

	Example C2000 Unique ID [(1)]	Description
Zero or low overhead / hardware feature	CLK1	Missing clock detect
	CPU8	Internal watchdog
	CPU5	Access protection mechanism for memories
	CPU14	Stack overflow detection
	PIE7	Maintain interrupt handlers for unused interrupts
	PWM8	ePWM fault detection using X-BAR
	SYS8	EALLOW/MEALLOW protection for critical registers
Best practices / highly recommended	PWR1	External voltage supervisor
	CLK7	External watchdog
	SRAM7	Data scrubbing to detect/correct memory errors
	CLK10	Testing of a feature / diagnostic. CLK10, for example, is a software test of the watchdog operation.

(1) A safety feature or diagnostic may be referenced by multiple IDs. For example, CPU5 is also CLA9, SRAM11, and DMA8 along with other IDs. This table only lists one of the IDs for simplicity.
(2) Enabled by default and cannot be disabled.

Mapping Acceptable Control Measures to C2000 Unique Identifiers

The proposed mapping in this document is for reference. The system and equipment designer, or manufacturer, is responsible to ensure the end system meets the IEC 60730 / UL 1998 requirements.

Note

This section references IEC 60370 Annex H table H.1 and UL 1998 Appendix A table A.2 as they apply to microcontrollers. While these two tables are compatible, the exact wording may differ. For specific wording, clarifications, and definitions, see an original copy of the specifications.

The mapping is summarized the following tables:

Table 7. Acceptable Measure to Unique Identifier Mapping

Component	Section
CPU	Section CPU Related Faults
Interrupt related faults	Section Interrupt Related Faults
Clock faults	Section Clock Related Faults
Memory	Section Memory Related Faults
Internal data path faults	Section Internal Data Path Faults
Input and output periphery faults	Section Input/Output Related Faults
Other faults: external communication, monitoring devices, and custom chip faults	Section Communication, Monitoring Devices, and Custom Chip Faults

When reviewing the acceptable measure to Unique ID tables, reference the following documentation:

IEC 60730 / UL 1998 specifications:	**Device-specific Functional Safety Manual:**
• Specific definitions of acceptable control measures for each class. • Additional acceptable control measures not listed here. • Clarifications and other notes not included here.	• C2000 Unique ID definitions. Refer to the Summary of Safety Features and Diagnostics chapter for a short description and a link to a longer explanation with implementation guidance. • Supporting software. Once done, do not forget to review the additional best practices described in Section Additional Best Practices.

Section Unique Identifier Reference includes a summary of Unique IDs referenced in this section. For further details, see the device-specific Functional Safety Manual.

Unique Identifier Reference

Table 8 is a summary of Unique IDs referenced in this section. For further details, see the device-specific Functional Safety Manual.

Note

- IDs in Table 8 may not apply to every C2000 device family. To determine if an ID applies to your device, see the mapping tables and functional safety manual.
- If the mapping tables reference an ID not listed here it was an oversight. For more information, see the device-specific Functional Safety Manual.

Table 8. Summary of Referenced C2000 Unique IDs

Unique ID	Short Description	Notes / Software Support
ADC2	DAC to ADC loopback check	
ADC8	ADC input signal integrity check	
ADC10	Hardware redundancy	
CAN3	SRAM Parity	
CLA1	Software reciprocal comparison	
CLA2	Software test of CPU	CLA_STL
CLA3	Handling of illegal operation and illegal results	
CLK2	Integrity using CPU timer	SDL module: STL_OSC_CT
CLK3	Integrity using HRPWM	SDL module: STL_OSC_HR
CLK4	Dual clock comparator (DCC type0)	
CLK16	Dual clock comparator (DCC type1)	Note: DCC type 1 is identical to type 2.
CLK17	Dual clock comparator (DCC type2)	
CPU1	Software reciprocal comparison	
CPU2	Hardware built-in test of CPU	SDL module: STL_HWBIST
CPU3	Software test of CPU	C28X_STL
CPU7	Handling of illegal operation, illegal results and instruction trapping	
DCSM2	Majority voting and error detection of link pointer	
ECAT6	SRAM parity	
EFUSE2	EFUSE ECC (data only)	
FLASH1	Flash ECC (data + address)	
FLASH2	VCU CRC check of memory	SDL module: STL_CRC
FLASH6	Software test of ECC logic	SDL modules: sdl_ex_ram_ecc_parity_test and sdl_ex_flash_ecc_test
GPIO4	Software test of function using I/O loopback	
GPIO5	Hardware redundancy	
INC1	Software test of function including error tests	
INC8	Transmission redundancy	
INC9	Hardware redundancy	
MCAN8	SRAM ECC (data + address)	
PIE1	PIE double SDRAM hardware comparison	
PIE2	Software test of SRAM	
PIE3	Software test of ePIE including error tests	
PIE6	PIE double SRAM comparison check	SDL module: STL_PIE_RAM
PIE8	Online monitoring of interrupts and events	
PIE13	Hardware redundancy using lockstep compare	
ROM1	VCU CRC check of memory	SDL module: STL_CRC

Table 8. Summary of Referenced C2000 Unique IDs (continued)

Unique ID	Short Description	Notes / Software Support
ROM9	Background CRC for CLA program ROM	
ROM10	Memory power-on Self-test (MPOST)	
ROM15	ROM parity	
SRAM1	SRAM ECC (data + address)	
SRAM2	SRAM Parity	
SRAM3	Software test of SRAM	SDL module: STL_March
SRAM8	VCU CRC check of memory	SDL module: STL_CRC
SRAM14	Software test of parity logic	SDL modules: sdl_ex_ram_ecc_parity_test
STL_CPU_REG	CPU register test example from the diagnostic library	For a device that does not include HWBIST, a periodic test of the CPU registers can be performed. STL_CPU_REG does not map to a C2000 Unique ID directly. STL_CPU_REG refers to an example CPU register test within the diagnostic library. This example is also provided for other devices if needed. Refer to the diagnostic library documentation.

CPU Related Faults

Table 9. CPU Faults

CPU Component	Class B/1 [1]	Class C/2 [1]	Acceptable Measure [2]		C2000 Unique IDs [3]						
			Definition	Description	F2837x F2807x	F2838x	F28004x	F28002x	F28003x	F280013x	F280015x
1.1 Registers	rq		H.2.16.5 A5.5	Functional test	- CLA2	- CLA2	CPU3 CLA2	- -	- CLA2	- -	CPU3 -
			H.2.16.6 A5.6	Periodic self-test	CPU2 CLA2 -	CPU2 CLA2 -	- CLA2 -	CPU2 - -	CPU2 CLA2 -	- - STL_CPU_REG [4]	- - -
		rq	H.2.18.15 A7.1.19	Reciprocal comparison	CPU1 CLA1	CPU1 CLA1	CPU1 CLA1	- -	CPU1 CLA1	- -	- -
			H.2.18.3 A7.1.6	Independent hardware comparator	-	-	-	-	-	-	CPU21
			H.2.18.9 A7.1.10	Internal error detection	CPU2	CPU2	-	CPU2	CPU2	-	-
1.2 Instruction decode and execution		rq	H.2.18.15 A7.1.19	Reciprocal comparison	CPU1 CLA1	CPU1 CLA1	CPU1 CLA1	- -	CPU1 CLA1	- -	- -
			H.2.18.3 A7.1.6	Independent hardware comparator	-	-	-	-	-	-	CPU21
			H.2.18.9 A7.1.10	Internal error detection	CPU2 CPU7 CLA3	CPU2 CPU7 CLA3	- CPU7 CLA3	CPU2 CPU7 -	CPU2 CPU7 CLA3	- CPU7 -	- CPU7 -

Table 9. CPU Faults (continued)

CPU Component	Class B/1 [1]	Class C/2 [1]	Acceptable Measure [2]		C2000 Unique IDs [3]						
			Definition	Description	F2837x F2807x	F2838x	F28004x	F28002x	F28003x	F280013x	F280015x
1.3 Program counter	rq		H.2.16.5 A5.5	Functional test	- CLA2	- CLA2	CPU3 CLA2	- -	- CLA2	- -	CPU3 -
			H.2.16.6 A5.6	Periodic self-test	CPU2	CPU2	-	CPU2	CPU2	-	-
			H.2.18.10.4 A7.1.13	Time slot monitoring	PIE8	PIE8	PIE8	PIE8	PIE8	PIE8	PIE8
		rq	H.2.18.10.3 A7.1.14	Independent time-slot monitoring and logical monitoring	PIE8	PIE8	PIE8	PIE8	PIE8	PIE8	PIE8
			H.2.18.15 A7.1.19	Reciprocal comparison	CPU1 CLA1	CPU1 CLA1	CPU1 CLA1	- -	CPU1 CLA1	- -	- -
			H.2.18.3 A7.1.6	Independent hardware comparator	-	-	-	-	-	-	CPU21
1.4 Addressing		rq	H.2.18.15 A7.1.19	Reciprocal comparison	CPU1 CLA1	CPU1 CLA1	CPU1 CLA1	- -	CPU1 CLA1	- -	- -
			H.2.18.3 A7.1.6	Independent HW comparator	-	-	-	-	-	-	CPU21
			H.2.18.9 A7.1.10	Internal error detection	CPU2	CPU2	-	CPU2	CPU2	-	-
1.5 Data paths		rq	H.2.18.15 A7.1.19	Reciprocal comparison	CPU1 CLA1	CPU1 CLA1	CPU1 CLA1	- -	CPU1 CLA1	- -	- -
			H.2.18.3 A7.1.6	Independent hardware comparator	-	-	-	-	-	-	CPU21
			H.2.18.9 A7.1.10	Internal error detection	CPU2	CPU2	-	CPU2	CPU2	-	-

(1) rq: coverage of the failure mode (see Table 2) is required by the standards for the indicated class. More than one acceptable measure may be available to choose from.

(2) For a complete list of acceptable measures and their definitions, see the IEC/UL specifications.

(3) For a description and implementation suggestions for each ID, see the device-specific Functional Safety Manual.

(4) This device does not include HWBIST (ID CPU2). Therefore, a periodic test of the CPU registers is suggested. STL_CPU_REG refers to an example CPU register test within the diagnostic library. Refer to the diagnostic library documentation.

Interrupt Related Faults

Table 10. Interrupt Faults to Unique ID Mapping

Component	Class B/1 [1]	Class C/2 [1]	Acceptable Measure [2]		C2000 Unique IDs [3]						
			Definition	**Description**	**F2837x F2807x**	**F2838x**	**F28004x**	**F28002x**	**F28003x**	**F280013x**	**F280015x**
2. Interrupts	rq		H.2.16.5 A5.5	Functional test	PIE1 PIE2 PIE3 PIE6	PIE1 PIE2 PIE3 PIE6	PIE1 PIE2 PIE3 PIE6	PIE1 PIE2 PIE3 PIE6	PIE1 PIE2 PIE3 PIE6	- PIE2 PIE3 -	- PIE2 PIE3 -
			H.2.18.10.4 A7.1.13	Time slot monitoring	PIE8	PIE8	PIE8	PIE8	PIE8	PIE8	PIE8
		rq	H.2.18.15 A7.1.19	Reciprocal comparison	CPU1 CLA1	CPU1 CLA1	CPU1 CLA1	- -	CPU1 CLA1	- -	- -
			H.2.18.3 A7.1.6	Independent hardware comparator	-	-	-	-	-	-	CPU21
			H.2.18.10.3 A7.1.14	Independent time-slot and logical monitoring	PIE8	PIE8	PIE8	PIE8	PIE8	PIE8	PIE8

(1) rq: coverage of the failure mode (refer to Table 2) is required by the standards for the indicated class. More than one acceptable measure may be available to choose from.
(2) For a complete list of acceptable measures and their definitions, see the IEC / UL specifications.
(3) For a description and implementation suggestions for each ID, see the device-specific Functional Safety Manual.

Clock Related Faults

Table 11. Clock Faults to Unique ID Mapping

Component	Class B/1 [1]	Class C/2 [1]	Acceptable Measure [2]		C2000 Unique IDs [3]						
			Definition	**Description**	**F2837x F2807x**	**F2838x**	**F28004x**	**F28002x**	**F28003x**	**F280013x**	**F280015x**
3. Clock	rq		H.2.18.10.1 A7.1.11	Frequency monitoring	CLK3	CLK3	CLK3	CLK3	CLK3	CLK3	CLK3
			H.2.18.10.4 A7.1.13	Time-slot monitoring	PIE8	PIE8	PIE8	PIE8	PIE8	PIE8	PIE8
		rq	H.2.18.15 A7.1.6	Independent hardware comparator	CLK2 CLK5 - - - -	CLK2 CLK5 - CLK16 APLL1 APLL7	CLK2 CLK5 CLK4 - - -	CLK2 CLK5 - CLK17 - -	CLK2 CLK5 - CLK17 APLL1 APLL7	CLK2 CLK5 - CLK17 APLL1 APLL7	CLK2 CLK5 - CLK17 APLL1 APPL7

(1) rq: coverage of the failure mode (refer to Table 2) is required by the standards for the indicated class. More than one acceptable measure may be available to choose from.
(2) For a complete list of acceptable measures and their definitions,see the IEC / UL specifications.
(3) For a description and implementation suggestions for each ID, see the device-specific Functional Safety Manual.

Memory Related Faults

Table 12. Memory Faults to Unique ID Mapping

Component	Class B/1 (1)	Class C/2 (1)	Acceptable Measure (2)		C2000 Unique IDs (3)						
			Definition	Description	F2837x F2807x	F2838x	F28004x	F28002x	F28003x	F280013x	F280015x
4.1 Non-volatile	rq		H.2.19.3.2 A7.2.5	Multiple checksum	-	-	ROM10	ROM10	ROM10	ROM10	ROM10
			H2.19.8.2 A7.3.2	Word protection, single-bit parity	-	-	-	-	ROM15	ROM15	ROM15
		rq	H.2.18.15 A7.1.19	Reciprocal comparison	CPU1 CLA1	CPU1 CLA1	CPU1 CLA1	- -	CPU1 CLA1	- -	- -
			H.2.18.3 A7.1.6	Independent hardware comparator	-	-	-	-	-	-	CPU21
			H.2.19.5 A7.2.8	Redundant memory with comparison	DCSM2	DCSM2	DCSM2	DCSM2	DCSM2	DCSM2	DCSM2
			H.2.19.4.2 A7.2.7	Periodic CRC, double word	FLASH2 ROM1 - -	FLASH2 ROM1 - -	FLASH2 ROM1 ROM9 -	FLASH2 ROM1 - -	FLASH2 ROM1 - ROM13	NWFLASH5 ROM1 - -	NWFLASH5 ROM1 - -
			H2.19.8.1 A7.3.1	Word protection with multi-bit redundancy	FLASH1 EFUSE2	FLASH1 EFUSE2	FLASH1 EFUSE2	FLASH1 EFUSE2	FLASH1 EFUSE2	NWFLASH1 EFUSE2	NWFLASH1 EFUSE2
4.2 Volatile	rq		H.2.19.6 A7.2.9	Periodic static memory test	SRAM3	SRAM3	SRAM3	SRAM3	SRAM3	SRAM3	SRAM3
			H2.19.8.2 A7.3.2	Word protection, single-bit parity	SRAM2 CAN3 - -	SRAM2 CAN3 ECAT6 -	SRAM2 CAN3 - -	SRAM2 CAN3 - -	- CAN3 - -	SRAM2 CAN3 - PIE11	SRAM2 CAN3 - PIE11
		rq	H2.19.5 A7.2.8	Redundant memory with comparison	PIE1	PIE1	PIE1	PIE1	PIE1	-	-
			H.2.19.8.1 A7.3.1	Word protection, multi-bit redundancy	SRAM1 -	SRAM1 MCAN8	SRAM1 -	SRAM1 -	SRAM1 MCAN8	SRAM1 MCAN8	SRAM1 MCAN8

Table 12. Memory Faults to Unique ID Mapping (continued)

Component	Class B/1 [1]	Class C/2 [1]	Acceptable Measure [2]		C2000 Unique IDs [3]						
			Definition	**Description**	**F2837x F2807x**	**F2838x**	**F28004x**	**F28002x**	**F28003x**	**F280013x**	**F280015x**
4.3 Addressing (volatile and non-volatile memory)	rq		H2.19.8.2 A7.2.9	Word protection, single-bit parity	SRAM2 - CAN3 - -	SRAM2 - CAN3 ECAT6 -	SRAM2 - CAN3 - -	SRAM2 - CAN3 - -	- ROM15 CAN3 - -	SRAM2 ROM15 CAN3 - PIE11	SRAM2 ROM15 CAN3 - PIE11
		rq	H.2.19.4.2 A7.2.7	Periodic CRC - double word	SRAM8 [4] - FLASH2 ROM1 - -	SRAM8 SRAM24 FLASH2 ROM1 - -	SRAM8 - FLASH2 ROM1 ROM9 -	SRAM8 SRAM24 FLASH2 ROM1 - -	SRAM8 SRAM24 FLASH2 ROM1 - ROM13	SRAM8 [4] - NWFLASH2 ROM1 - -	SRAM8 - NWFLASH2 ROM1 - -
			H.2.19.8.1 A7.3.1	Word protection, multi-bit redundancy including address	FLASH1 SRAM1	FLASH1 SRAM1 MCAN8	FLASH1 SRAM1	FLASH1 SRAM1	FLASH1 SRAM1 MCAN8	NWFLASH1 SRAM1 MCAN8	NWFLASH1 SRAM1 MCAN8

(1) rq: coverage of the failure mode (refer to Table 2) is required by the standards for the indicated class. More than one acceptable measure may be available to choose from.
(2) For a complete list of acceptable measures and their definitions, see the IEC / UL specifications.
(3) For a description and implementation suggestions for each ID, see the device-specific Functional Safety Manual.
(4) The F2807x and F280013x devices do not have a VCRC module. The CRC is performed by the CPU. For more information, see the device-specific software diagnostic library.

Internal Data Path Faults

Table 13. Internal Data Path Faults to Unique ID Mapping

Component	Class B/1 [1]	Class C/2 [1]	Acceptable Measure [2]		C2000 Unique IDs [3]						
			Definition	**Description**	**F2837x F2807x**	**F2838x**	**F28004x**	**F28002x**	**F28003x**	**F280013x**	**F280015x**
5.1 Data	rq		H.2.19.8.2 A7.3.2	Word protection with single-bit parity	SRAM2 -	SRAM2 -	SRAM2 -	SRAM2 -	- ROM15	SRAM2 -	SRAM2 -
		rq	H.2.18.15 A7.1.19	Reciprocal comparison	CPU1 CLA1	CPU1 CLA1	CPU1 CLA1	- -	CPU1 CLA1	- -	- -
			H.2.18.3 A7.1.6	Independent hardware comparator	-	-	-	-	-	-	CPU21
			H.2.19.8.1 A7.3.1	Word protection with multi-bit redundancy including the address	FLASH1 SRAM1	FLASH1 SRAM1	FLASH1 SRAM1	FLASH1 SRAM1	FLASH1 SRAM1	NWFLASH1 SRAM1	NWFLASH1 SRAM1
			H.2.18.22 A7.1.24	Testing pattern	SRAM3 SRAM13 SRAM14 FLASH6	SRAM3 SRAM13 SRAM14 FLASH6	SRAM3 SRAM13 SRAM14 FLASH6	SRAM3 SRAM13 SRAM14 FLASH6	SRAM3 SRAM13 SRAM14 FLASH6	SRAM3 SRAM13 SRAM14 NWFLASH14	SRAM3 SRAM13 SRAM14 NWFLASH14
					-	-	-	-	-	NWFLASH15	NWFLASH15
			H.2.18.14 A7.1.18	Protocol test	INC1 INC8 INC9	INC1 INC8 INC9	INC1 INC8 INC9	INC1 INC8 INC9	INC1 INC8 INC9	INC1 INC8 INC9	INC1 INC8 INC9

Table 13. Internal Data Path Faults to Unique ID Mapping (continued)

Component	Class B/1 [1]	Class C/2 [1]	Acceptable Measure [2]		C2000 Unique IDs [3]						
			Definition	Description	F2837x F2807x	F2838x	F28004x	F28002x	F28003x	F280013x	F280015x
5.2 Addressing	rq		H.2.19.8.2 A7.3.2	Word protection with single bit redundancy including the address	SRAM2	SRAM2	SRAM2	SRAM2	-	SRAM2	SRAM2
		rq	H.2.18.15 A7.1.19	Reciprocal comparison	CPU1 CLA1	CPU1 CLA1	CPU1 CLA1	- -	CPU1 CLA1	- -	- -
			H.2.18.3 A7.1.6	Independent hardware comparator	-	-	-	-	-	-	CPU21
			H.2.19.8.1 A7.1.6	Word protection with multi-bit redundancy including the address	FLASH1 SRAM1	FLASH1 SRAM1	FLASH1 SRAM1	FLASH1 SRAM1	FLASH1 SRAM1	NWFLASH1 SRAM1	NWFLASH1 SRAM1
			H.2.18.22 A7.1.24	Testing pattern including the address	FLASH6	FLASH6	FLASH6	FLASH6	FLASH6	NWFLASH15	NWFLASH15

(1) rq: coverage of the failure mode (see Table 2) is required by the standards for the indicated class. More than one acceptable measure may be available to choose from.
(2) For a complete list of acceptable measures and their definitions, see the IEC / UL specifications.
(3) For a description and implementation suggestions for each ID, see the device-specific Functional Safety Manual.

Input/Output Related Faults

Table 14. Input/Output Periphery Faults to Unique ID Mapping

Component	Class B/1 [1]	Class C/2 [1] [1]	Acceptable Measure [2]		C2000 Unique IDs [3]						
			Definition	Description	F2837x F2807x	F2838x	F28004x	F28002x	F28003x	F280013x	F280015x
7.1 Digital I/O	rq		H.2.18.13 A7.1.17	Plausibility check	GPIO4	GPIO4	GPIO4	GPIO4	GPIO4	GPIO4	GPIO4
		rq	H.2.18.8 A7.1.9	Input comparison	GPIO5	GPIO5	GPIO5	GPIO5	GPIO5	GPIO5	GPIO5
			H.2.18.11 A7.1.15	Multiple parallel outputs	GPIO5	GPIO5	GPIO5	GPIO5	GPIO5	GPIO5	GPIO5
			H.2.18.12 A7.1.16	Output verification	GPIO4	GPIO4	GPIO4	GPIO4	GPIO4	GPIO4	GPIO4
7.2 Analog I/O 7.2.1 A/D and D/A converter	rq		H.2.18.13 A7.1.17	Plausibility check	ADC2 ADC8	ADC2 ADC8	ADC2 ADC8	ADC2 ADC8	ADC2 ADC8	ADC2 ADC8	ADC2 ADC8
		rq	H.2.18.8 A7.1.9	Input comparison	ADC10	ADC10	ADC10	ADC10	ADC10	ADC10	ADC10
7.2 Analog I/O 7.2.2 Analog multiplexer	rq		H.2.18.13 A7.1.17	Plausibility check	ADC2 ADC8	ADC2 ADC8	ADC2 ADC8	ADC2 ADC8	ADC2 ADC8	ADC2 ADC8	ADC2 ADC8
		rq	H.2.18.15 A7.1.19	Input comparison	ADC10	ADC10	ADC10	ADC10	ADC10	ADC10	ADC10

(1) rq: coverage of the failure mode (see Table 2) is required by the standards for the indicated class. More than one acceptable measure may be available to choose from.
(2) For a complete list of acceptable measures and their definitions, see the IEC / UL specifications.
(3) For a description and implementation suggestions for each ID, see the Functional Safety Manual.

Communication, Monitoring Devices, and Custom Chip Faults

Table 15. External Communication, Monitoring Devices, and Custom Chip Faults

Component	Class B/1	Class C/2	Acceptable Measure	C2000 Unique IDs
6. Data	Refer to the 60730 standard			For communication port safety mechanisms, see the device-specific functional safety manual. While this list is too long to replicate, a few examples are: • Software test using looopback • CRC framing / message checks • ECC framing checks • Checksum error detection • Data overrun and underrunn detection • Physical bus error detection • Timeout on FIFO activity
6.2 Addressing				
6.3 Timing				
8. Monitoring devices and comparators	Refer to the 60730 standard			Requirement and implementation is system-dependent. For safety mechanisms which might be leveraged in your implementation, see the device-specific functional-safety manual.
Components not covers by items 1-8. Custom chips (ASIC, GAL, gate array)	Refer to the 60730 standard			Requirement and implementation is system-dependent. For safety mechanisms which might be leveraged in your implementation, see the device-specific functional-safety manual.

Glossary

Table 16. Terms and Definitions

Terminology and Abbreviations	Definition
A.x...	Reference from the UL 1998 standard. For example: A.7.1.19 is a specific definition found in appendix A of the standard.
C28x	A C2000 central processing unit.
CLA	C2000 Control Law Accelerator: an independent 32-bit floating-point processor.
CLA PROM	Program ROM for the CLA CPU
CLB	C2000 Configurable Logic Block
Class B / 1	IEC 60730 Class B and UL 1998 Class 1. Class assigned based on a functional safety assessment. Refer to c.
Class C / 2	IEC 60730 Class C and UL 1998 Class 2: Class assigned based on a functional safety assessment. Refer to Table 1.
CLK	Clock
CPU	Central Processing Unit
CPU Timer	C2000 general timer peripheral
CRC	Cyclic Redundancy Check
DC fault	(IEC/UL) Short circuits between signals.
DCC	C2000 dual clock comparitors
DCSM	C2000 dual code-security module
ECC	Error correction code
E/E/PE	(IEC/UL) Electrical/Electronic/Programmable Electronic
EMC	(IEC/UL) Electromagnetic compatibility
ePIE	C2000 enhanced peripheral interrupt expansion block. May also be referred to as PIE.
ePWM	C2000 enhanced Pulse Width Modulation peripheral. May also be referred to as PWM.
FPU	Floating-point Unit instruction set extension to the C28x CPU

Table 16. Terms and Definitions (continued)

Terminology and Abbreviations	Definition
FSM	• This document uses FSM to indicate a Functional Safety Manual (Section Functional Safety Manuals). • (IEC/UL) FSM is used to indicate Functional Safety Management.
GPIO	C2000 general purpose input/output pin
H.x...	Reference from the IEC 60730 standard. For example: H.2.16.5 is a specific definition found in annex H of the standard.
HRPWM	High-resolution feature of the C2000 ePWM module
HW	Hardware (the microcontroller)
HWBIST	C2000 hardware built-in self test
IEC	International Electrotechnical Commission
IEC 60730	The terms "IEC 60730", "UL 1998", "IEC / UL standards", "60730" and "the standards" are used interchangeably to refer to both: • IEC60730-1 Edition 5.0 2013-11, Annex H and Table H.1 (H.11.12.7 of edition 3) – "Acceptable measures to address fault/errors" • The UL Standard for Safety for Software in Programmable Components, UL 1998, Third Edition, Dated December 18, 2013, Appendix A and Table A2.1 – "Coverage for microelectronic hardware failure modes"
IEC 61508	IEC 61508 Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems, International Electrotechnical Commission, Edition 2.0 2010.
ISO 26262	ISO 26262–Road Vehicles-Functional Safety, International Standard ISO, vol. 26262, 2018.
IEC / UL	Short for the standards or indicates something taken from the standards. Such as (IEC/UL) marked definitions in this list. See IEC 60730
MPOST	Memory power-on self-test
PIE	See ePIE.
PWM	See ePWM.
PEST	Periodic self-test
POST	Power-on self-test
ROM	Read only memory
SDL	Software Diagnostic Library
SRAM	Static random-access memory
STL	Self-Test Library
Stuck-at	(IEC/UL) An open circuit fault or non-varying signal level
SW	Software
TI	Texas Instruments Inc.
TMU	Trigonometric Math Unit instruction set extension to the C28x CPU
UL	Underwriters Laboratories Inc.
UL 1998	See IEC 60730
Unique ID	A C2000 unique identifier assigned to a functional safety feature or diagnostic in the functional safety manual. For example CLK2 or GPIO4.
VCRC	Refer to VCU
VCU	Instruction set extension to the C28x CPU. Part of the added instructions are CRC calculation specific. The CRC instructions are supported on some devices as simply the "VCRC".

References

Note

The device-specific Functional Safety Manual can be located in the technical documentation section of the device product folder. Product folder URLs are of the form *ti.com/product/<device>*. For example: www.ti.com/product/TMS320F280049.

1. *IEC 60730-1 Automatic Electrical Controls - Part1: General Requirements*, International Electrotechnical Commission, Edition, Edition 5.0 2013-11
2. *UL 1998 Standard for Safety for Software in Programmable Components*, ANSI/UL, Third Edition, December 18 2013
3. Texas Instruments: C2000 Academy Online Training
4. Texas Instruments: C2000Ware Software Development Kit for C2000 MCUs
5. Texas Instruments: *Industrial Functional Safety for C2000™ Real-Time Microcontrollers*
6. Texas Instruments: *C2000™ Safety Mechanisms*
7. Texas Instruments: *C2000™ Hardware Built-In Self-Test*
8. Texas Instruments: *C2000™ CPU Memory Built-In Self-Test*
9. Texas Instruments: *C2000™ Memory Power-On Self-Test (M-POST)*
10. Texas Instruments: *Embedded Real-Time Analysis and Response for Control Applications (ERAD)*

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