User's Guide

为 C2000 实时微控制器实现 IEC 60730/UL 1998 合规性

摘要

如果电机驱动器、白色家电、电器和其他设备的某个组件发生故障，这些设备的运行可能会变得不安全。这些设备须符合国际电工委员会 (IEC) 的测试和资质要求。具体而言，需要满足 IEC 60730-1“家用及类似用途的自动电气控制”安全标准。美国也遵循类似的做法，采用 UL 1998“可编程组件中的安全软件”。

与微控制器 (MCU) 最相关的方面是 IEC 60730 附录 H 和 UL 1998 附录 A.2，其中详细说明了支持家用电器安全功能的诊断测试要求。

本文档简要概述这些适用于 MCU 的规范，并介绍如何利用 C2000™ 功能安全特性来满足诊断测试要求。

内容

商标

1 引言

如果电机驱动器、白色家电、电器和其他设备的某个组件发生故障，这些设备的运行可能会变得不安全。这些设备须符合国际电工委员会 (IEC) 的测试和资质要求。具体而言，需要满足 IEC 60730-1 标准中涵盖的“家用及类似用途的自动电气控制”要求。

尽管在系统级实现了 IEC 60730 合规性，但了解选择微控制器的正确标准对于实现合规性非常重要。IEC 60730 附录 H“电子控制要求”中的表 H.1 介绍了微控制器 (MCU) 等电子元件的使用。附录 H 规定了适用于 MCU 的可接受诊断技术和措施，旨在支持设备的安全功能。

虽然 IEC 60730 主要在欧洲使用，但美国也遵循类似的做法，采用 UL 1998“可编程组件中的安全软件”。附录 A 中的表 A2.1 提供了符合 IEC 60730 表 H.1 要求的微电子硬件故障模式的可接受措施示例。这些要求源自 IEC 61508 标准“电气/电子/可编程电子 (E/E/PE) 系统的功能安全”。

2 IEC 60730 和 UL 1998 分级概述

为了奠定故障控制技术的基础，IEC 60730 和 UL 1998 规范均将产品分为多个等级。等级的分配取决于应用于具体控制功能的危险和风险分析。该分析基于故障的可能性和故障产生的后果。

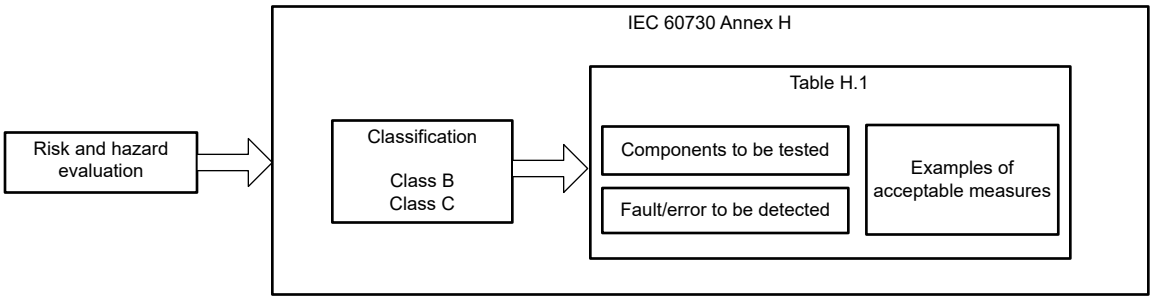

图 2-1. IEC 60730 附录 H

IEC 60730 定义了 3 个等级：A、B 和 C：

- A 级：控制功能与安全无关
- B 级：旨在防止不安全运行的控制功能
- C 级：旨在防止危险的控制功能

UL 1998 定义了两个等级：1 和 2。UL 1998 1 级与 IEC 60730 B 级相当，UL 1998 2 级与 IEC 60730 C 级相当。如需了解等级定义和示例，请参阅表 2-1。

表 2-1. 等级定义和示例

等级	定义 #none#	示例
IEC 60730 A 级	“H.2.22.1 A 级控制功能 - 并非出于应用安全考虑而依赖的控制功能”	室内恒温器、温度控制。
IEC 60730 B 级 和 UL 1998 1 级	“H2.2.22 B 级控制功能 - 旨在防止设备处于不安全状态的控制功能”注意：控制功能失效不会直接导致危险情况。	热断路器。洗衣设备门锁。
	“A3.1 软件 1 级 - 旨在控制功能以降低与设备相关风险可能性的软件部分”	
IEC 60730 C 级 和 UL 1998 2 级	“H.2.22.3 C 级控制功能 - 旨在防止特殊危险（如爆炸）或故障可能直接导致设备危险的控制功能”	自动燃烧器控制。封闭式热水器系统的热断路器。
	“A3.2 软件 2 级 - 旨在控制功能以降低设备相关特殊风险（如爆炸）可能性的软件部分”	

这些标准定义了必须测试的组件以及用于检测该组件的故障/错误的可接受措施示例。根据等级，要测试的组件包括 CPU、时钟、易失性和非易失性存储器、内部数据路径、I/O 和通信接口（表 2-2）。一般而言，对于每个组件，开发人员可以选择几种类型的措施来验证/测试组件功能。这些建议的措施可以：

- 基于硬件
- 基于软件
- 基于硬件和基于软件的组合

实施 IEC 60730 可接受措施旨在检测和防止与设备相关的不安全状况和危险。这些要求源自 IEC 61508 标准“电气/电子/可编程电子 (E/E/PE) 系统的功能安全”。IEC 61508 的重点是如何应用、设计和维护称为安全相关系统的自动保护系统。

表 2-2. IEC 60730/UL 1998 说明的故障模式汇总

要测试的组件		要检测的硬件故障/错误 (1)	
		B/1 级	C/2 级
1.CPU	1.1 寄存器	固定型	直流故障
	1.2 指令解码和执行	不适用 (2)	解码和执行错误
	1.3 程序计数器	固定型	直流故障
	1.4 寻址	不适用	直流故障
	1.5 数据路径	不适用	直流故障
2.中断		无或过于频繁	与不同来源相关，无或过于频繁
3.时钟		频率错误	频率错误
4.内存	4.1 非易失性	所有 single-bit 故障	所有 single-bit 和 double-bit 错误
	4.2 易失性	直流故障	直流故障和动态交叉链路
	4.3 寻址	停留在	直流故障
5.内部数据路径	5.1 数据	固定型	直流故障
	5.2 寻址	地址错误	地址错误、多重寻址
6.外部通信	6.1 数据	所有 single-bit 和 double-bit 错误	所有 single-bit、double-bit 和 triple-bit 错误
	6.2 寻址	地址错误	寻址错误和多重寻址
	6.3 时序	时间点错误	时间点错误
		顺序错误	顺序错误
7.输入/输出外设	7.1 数字 I/O	开路和短路或按产品标准规定	开路和短路或按产品标准规定
	7.2 模拟 I/O 7.2.1 模数和数模转换器	开路和短路或按产品标准规定	开路和短路或按产品标准规定
	7.2 模拟 I/O 7.2.2 模拟多路复用器	寻址错误	寻址错误

表 2-2. IEC 60730/UL 1998 说明的故障模式汇总（续）

要测试的组件	要检测的硬件故障/错误 (1)	
	B/1 级	C/2 级
8.监控器件和比较器	不适用	超出静态和动态功能规格的任何输出
9.1-8 未涵盖的组件。 定制芯片、ASIC、GAL、门阵列	超出静态和动态功能规格的任何输出	超出静态和动态功能规格的任何输出

(1) 参考：IEC 60730-1 表 H.1 和 UL 1998 表 A.2
(2) 不适用：该特定等级的标准不要求检测此错误/故障。

2.1 C2000 各器件系列的功能

表 2-3 中的 C2000 器件功能以映射到建议器件诊断和功能安全特性的 IEC 60730 示例故障/错误检测方法为基础。此映射将在本文档的其余部分中进行介绍。

表 2-3. C2000 各器件系列的 IEC 60730/UL 1998 功能

器件系列	B/1 级	C/2 级
F28002x	✓	✓
F28003x	✓	✓
F28004x	✓	✓
F2807x	✓	✓
F2837xD、F2837xS	✓	✓
F2838x	✓	✓

3 C2000 安全配套资料

TI 提供了安全相关的配套资料以帮助进行系统开发和评估。本节介绍可用于满足 IEC 60730 和 UL 1998 要求的配套资料。

3.1 使用入门

为了熟悉 C2000 功能安全功能，建议参阅以下文档：

- *C2000™ 安全机制*：介绍支持功能安全的 C2000 器件特性。
- *C2000 实时微控制器的工业功能安全*：重点介绍支持工业功能安全标准的特定器件功能、配套资料和文档。

本章将进一步讨论更深入的配套资料：

- 功能安全手册 (FSM)：器件特定的全面功能安全相关文档。
- 诊断和自检软件配套资料。

备注

本文档不包括 F2806x、F2803x、F2805x、F2802x、F2833x 和 F2823x C2000 系列。对于这些器件，请参阅 *IEC60730 安全应用用户指南中的 C2000 MCU 安全手册*。

3.2 功能安全手册

设备设计人员和制造商有责任确保系统满足所有适用的安全、法规和性能要求。大多数 C2000 功能安全手册都是功能安全合规型设计包的一部分，旨在帮助满足 ISO 26262 或 IEC 61508 功能安全标准。

安全手册的其中一部分可以帮助进行符合 IEC 60730 要求的设计。表 3-1 列出了侧重于 IEC 60730 的设计人员感兴趣的主题。其他不直接与 IEC 60730 相关的主题也可能有帮助。

表 3-1. 功能安全手册主题

侧重于 IEC 60730 的开发人员应特别注意：	**其他主题可能会有所帮助，其中包括：**
• 映射到节 5 中 IEC 60730 可接受措施的建议安全特性和诊断的说明。 • 诊断实施指南。 • 软件诊断库和自检库的说明。 • 虽然某些唯一 ID 可能不会直接映射到 IEC 60730，或者可能仅提供部分覆盖，但强烈建议实施。节 4.3 中讨论了此类最佳实践的示例。	• 产品概述。 • 突出安全特性的器件架构图。 • 所有安全特性和诊断的完整列表。 • 特定于外设的安全特性列表。 • 诊断说明、诊断测试和故障避免措施。 • 关于提升抗干扰能力的建议。 • 关于解决共因失效问题的建议。

在功能安全手册中，C2000 唯一标识符（唯一 ID）标识了特定的安全特性和诊断。这些诊断可分为：

- 安全诊断
- 安全诊断测试
- 故障避免技术

实施可以是：

- 硬件：在 TI 器件中实施
- 软件：必须在应用软件中实施
- 硬件加软件：需要在器件中实施硬件并需要在应用中实施软件
- 系统：在微控制器外部实施

本文档旨在帮助将 IEC 60730 要求映射到建议的 C2000 唯一 ID（节 5）。然后，针对每个唯一 ID，系统设计人员可以参考功能安全手册的说明和实施建议。节 5 中对此方法进行了说明。

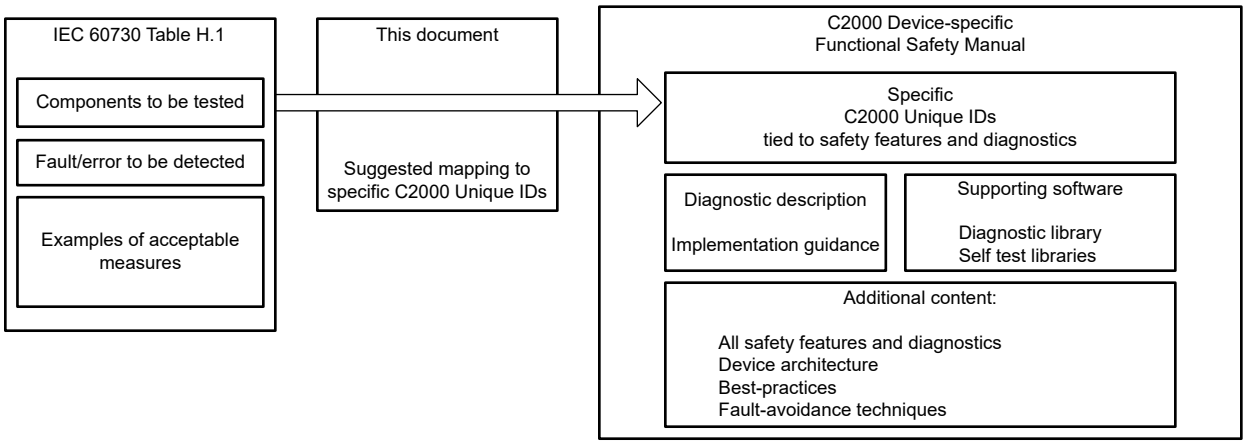

图 3-1. 将可接受措施映射到 C2000 功能安全手册

3.3 软件配套资料

虽然 C2000 器件具有多种硬件安全特性，但应用级诊断软件会增加硬件特性的价值。C2000 提供以下与安全相关的软件包：

- C28x 自检库 (C28x_STL)
- CLA 自检库 (CLA_STL)
- 软件诊断库 (SDL)

软件诊断库

特性:

- 有一组可通过 C 语言调用、经优化、独立的测试函数。
- 由用户的应用程序调用和管理。
- 检测到故障时，应用程序确定系统相应的操作。
- 每个函数执行一个特定任务来验证组件的功能。
- 采用符合安全标准的安全机制。
- 对 MCU 实时控制性能的影响极小。
- 用户指南包含基准测试。
- 支持上电测试和/或定期测试。
- 演示库用法和诊断功能配置。

示例包括：

- CAN 消息 RAM March 和奇偶校验逻辑测试
- 用于通信和存储器测试的 CRC 代码
- CPU HWBIST 功能接口
- PIE RAM 冗余测试
- 时钟频率测试
- CPU 寄存器测试
- PIE RAM 冗余测试

请参阅安全手册的“C2000 安全诊断库”一章。

获取方式：

- F2837xS、F2837xD 和 F2807x 在此处下载。
- 其他器件 SDL 位于 C2000Ware 中。请参阅库/诊断目录。

C28x 和 CLA 自检库

自检库 (STL) 使用 CPU 本身来检查 CPU 的逻辑完整性。STL 经 TÜV SÜD 独立评估，发现其分别适合集成到高达 ASIL D (ISO 26262:2018) 和 SIL 3 (IEC 61508:2010) 等级的安全相关系统中。

C28X_STL 特性：

- 代表着一种能够检测 C28x CPU 永久性故障的安全机制。
- 涵盖 CPU、FPU、TMU、VCU 和 VCRC 指令集。
- 仅支持启动测试。
- 适用于不带硬件内置自检 (HWBIST) 的 C 级、SIL-2 和 SIL-3 功能器件。
- 包含用户指南和合规性支持包 (CSP)。

CLA_STL 特性：

- 代表着一种能够检测控制律加速器 (CLA) 永久性故障的安全机制。
- 涵盖 CLA 寄存器组、控制单元、数据路径等。
- 支持启动测试和定期测试。
- 适用于任何具有 CLA 的器件。
- 包含用户指南和合规性支持包 (CSP)。

获取方式：

- CLA_STL 和 C28X_STL 未在 TI.com 上发布。请联系您的 TI 代表以申请访问权限。

4 在 C2000 实时 MCU 上实施可接受措施

本节详细介绍如何采用分步式方法确定功能安全诊断和软件，从而实施 IEC 60730 和 UL 1998 可接受措施。

4.1 实施步骤

为规划可接受措施的实施，建议的步骤如下：

步进	说明	参考文献
步骤 1	**将可接受措施映射到 C2000 唯一 ID：** 规范中通常为开发人员提供了用于检测特定故障的可接受措施选项。本文档介绍了一些可接受措施到唯一 ID 的映射。在某些情况下，可能有多个适用的唯一 ID。	• IEC 60730 或 UL 1998 规范 • 本文档：节 5
步骤 2	**规划实施：** 阅读有关实施唯一 ID 的说明和指南或建议。您还将了解唯一 ID 的实施是基于硬件、软件还是两者。	器件特定的功能安全手册：安全特性和诊断汇总
步骤 3	**确定支持软件：** 确定唯一 ID 是否受 SDL 或 STL 支持。	• 器件特定的功能安全手册：安全诊断库 • 本文档：节 3.3 • SDL 或 STL 文档
	在某些情况下，SDL/STL 模块不支持唯一 ID。当唯一 ID 与具有最低软件要求或没有软件要求的硬件机制相对应时，或者唯一 ID 需要系统相关的实施时，便属于这种情况。	在这些情况下，请参考： 1. FSM 唯一 ID 说明，了解实施指南和建议。 2. C2000Ware 软件开发套件软件示例，根据 FSM 指南实现相关要求。例如： • 填充 PIE 向量，包括未使用的向量。 • 嵌入式实时分析和诊断模块 (ERAD) 示例。 • 用于计算 CRC 的 VCRC 模块库。 • 外设配置。
步骤 4	**确定要实施的其他唯一 ID：** 某些 ID 可能不直接映射到 IEC 60370，但仍然强烈建议使用。在这些 ID 中，许多采用了硬件实施，在系统中占用的开销很小。	• 器件特定的功能安全手册 • 本文档：节 4.3

4.2 映射示例

表 4-1 展示了将可接受措施映射到 C2000 唯一 ID 的示例。规范允许针对给定类别使用一种或多种可接受措施。由系统设计人员决定哪种最适合其应用。此外，C 级措施可用于检测 B 级故障/错误。因此，在示例 1 中，系统设计人员也可以使用示例 2 中所示的 C 级可接受措施。

表 4-1. 映射到唯一 ID 的示例和实施指南

示例	可接受措施到 C2000 唯一 ID [1]	实施指南 (FSM)
示例 1： 组件：CPU 寄存器 器件：F28003x 等级：B 故障“固定型”	映射到措施“定期自检”的唯一 ID： • CPU2：CPU 硬件内置自检 (HWBIST) • CLA2：CLA 软件测试 注意：规范指出也可以选择 C 级措施来覆盖 B 级故障。	FSM 说明了： • 诊断覆盖率信息。 • 如何应用测试来检查每个 CPU 的完整性 • 实施该测试的详细信息 • 让开发人员参阅诊断和自检软件文档。
示例 2： 组件：CPU 寄存器 器件：F28003x 等级：C 故障“直流故障”	映射到 ID： • CPU1/CLA1：通过软件进行相互比较，实现可接受措施的“相互比较” • CPU2：CPU 硬件内置自检 (HWBIST)，实现可接受措施的“内部错误检测”	FSM： • 说明了 HWBIST 硬件特性。 • 提供实现相互比较的思路。该诊断高度依赖于系统。 • 让开发人员参阅 HWIBST 软件接口的诊断软件文档。

1. 如需更多信息，请参阅节 5 中的表。

4.3 其他最佳实践

本文档重点介绍专门映射到 IEC 60730 和 UL 1998 要求的 C2000 唯一 ID。器件特定的安全手册提供了可为系统设计人员提供帮助的其他信息。强烈建议查看以下功能安全手册章节：

- *关于提升抗干扰能力的建议*
- *关于解决共因失效问题的建议*
- *安全特性和诊断汇总*
  - 故障避免技术
  - 低开销/零开销硬件诊断
  - 安全特性和诊断测试。

表 4-2 列出了一些示例。要确定具体器件系列的其他最佳实践，请参阅器件特定的功能安全手册。

表 4-2. 相关的其他唯一 ID 示例

	C2000 唯一 ID 示例 (1)	说明
故障避免	CLK14	外设时钟门控
	CPU6	禁用 JTAG 端口
	DMA9	禁用未使用的 DMA 触发源
	FLASH3 (2)	闪存存储器阵列中的位多路复用
	RST2	复位原因信息
	SRAM4 (2)	SRAM 存储器阵列中的位多路复用
	SYS1 (2)	针对控制寄存器的多位使能键
	SYS2	针对控制寄存器的锁定机制
	SYS7	外设软复位 (SOFTPRES)
零开销或低开销/硬件特性	CLK1	时钟丢失检测
	CPU8	内部看门狗
	CPU5	存储器访问保护机制
	CPU14	栈溢出检测
	PIE7	为未使用的中断维护中断处理程序
	PWM8	使用 X-BAR 进行 ePWM 故障检测
	SYS8	关键寄存器的 EALLOW/MEALLOW 保护功能
最佳实践/强烈推荐	PWR1	外部电压监视器
	CLK7	外部安全装置
	SRAM7	清理数据以检测/校正存储器错误
	CLK10	特性/诊断测试。例如，CLK10 是针对看门狗运行情况的软件测试。

(1) 安全特性或诊断可通过多个 ID 进行引用。例如，CPU5 也是 CLA9、SRAM11 和 DMA8 以及其他 ID。为简单起见，该表仅列出其中一个 ID。
(2) 默认启用且无法禁用。

5 将可接受控制措施映射到 C2000 唯一标识符

本文档中建议的映射仅供参考。系统和设备设计人员或制造商有责任确保终端系统符合 IEC 60730/UL 1998 要求。

备注

本节引用了适用于微控制器的 IEC 60370 附录 H 表 H.1 和 UL 1998 附录 A 表 A.2。虽然这两个表是兼容的，但确切的措辞可能有所不同。有关具体的措辞、说明和定义，请参阅规范的原始副本。

映射汇总如下表：

表 5-1. 可接受措施到唯一标识符的映射

组件	部分
CPU	节 5.2
中断相关故障	节 5.3
时钟故障	节 5.4
内存	节 5.5
内部数据路径故障	节 5.6
输入和输出外设故障	节 5.7
其他故障：外部通信、监控器件和定制芯片故障	节 5.8

在查看可接受措施到唯一 ID 的映射表时，请参考以下文档：

IEC 60730/UL 1998 规范：	器件特定的功能安全手册：
• 每个等级可接受控制措施的具体定义。 • 此处未列出其他可接受控制措施。 • 此处未包含说明和其他注释。	• C2000 唯一 ID 定义。请参阅“安全特性和诊断汇总”一章以获取简短说明以及指向详细说明（包括实施指南）的链接。 • 支持软件。 完成后，请不要忘记查看节 4.3 中介绍的其他最佳实践。

节 5.1 提供了本节中引用的唯一 ID 的汇总。更多详细信息，请参阅器件特定的功能安全手册。

5.1 唯一标识符参考

表 5-2 是本节中引用的唯一 ID 的汇总。更多详细信息，请参阅器件特定的功能安全手册。

备注

- 表 5-2 中的 ID 可能并不适用于所有 C2000 器件系列。要确定 ID 是否适用于您的器件，请参阅映射表和功能安全手册。
- 如果映射表引用的 ID 未在此处列出，可能是疏忽导致。更多信息，请参阅器件特定的功能安全手册。

表 5-2. 引用的 C2000 唯一 ID 汇总

唯一 ID	简短描述	注释/软件支持
ADC2	DAC 至 ADC 环回检查	
ADC8	ADC 输入信号完整性检查	
ADC10	硬件冗余	
CAN3	SRAM 奇偶校验	
CLA1	软件相互比较	
CLA2	CPU 软件测试	CLA_STL
CLA3	对于非法操作和非法结果的处理	
CLK2	使用 CPU 计时器实现完整性	SDL 模块：STL_OSC_CT
CLK3	使用 HRPWM 实现完整性	SDL 模块：STL_OSC_HR
CLK4	双时钟比较器（DCC 类型 0）	
CLK16	双时钟比较器（DCC 类型 1）	注意：DCC 类型 1 与类型 2 相同。
CLK17	双时钟比较器（DCC 类型 2）	
CPU1	软件相互比较	
CPU2	CPU 硬件内置测试	SDL 模块：STL_HWBIST
CPU3	CPU 软件测试	C28X_STL
CPU7	对于非法操作、非法结果和指令陷入的处理	
DCSM2	链路指针的多数表决和错误检测	
ECAT6	SRAM 奇偶校验	
EFUSE2	EFUSE ECC（仅数据）	
FLASH1	闪存 ECC（数据 + 地址）	
FLASH2	存储器的 VCU CRC 校验	SDL 模块：STL_CRC
FLASH6	ECC 逻辑的软件测试	SDL 模块：sdl_ex_ram_ecc_parity_test 和 sdl_ex_flash_ecc_test
GPIO4	使用 I/O 环回的功能软件测试	
GPIO5	硬件冗余	
INC1	包括错误测试在内的功能软件测试	
INC8	传输冗余	
INC9	硬件冗余	
MCAN8	SRAM ECC（数据 + 地址）	

表 5-2. 引用的 C2000 唯一 ID 汇总（续）

唯一 ID	简短描述	注释/软件支持
PIE1	PIE 双 SDRAM 硬件比较	
PIE2	SRAM 软件测试	
PIE3	包括错误测试在内的 ePIE 软件测试	
PIE6	PIE 双 SRAM 比较检查	SDL 模块：STL_PIE_RAM
PIE8	在线监测中断和事件	
PIE13	使用锁步比较的硬件冗余	
ROM1	存储器的 VCU CRC 校验	SDL 模块：STL_CRC
ROM9	CLA 程序 ROM 的背景 CRC	
ROM10	存储器开机自检 (MPOST)	
ROM15	ROM 奇偶校验	
SRAM1	SRAM ECC（数据 + 地址）	
SRAM2	SRAM 奇偶校验	
SRAM3	SRAM 软件测试	SDL 模块：STL_March
SRAM8	存储器的 VCU CRC 校验	SDL 模块：STL_CRC
SRAM14	奇偶校验逻辑的软件测试	SDL 模块：sdl_ex_ram_ecc_parity_test
STL_CPU_REG	诊断库中的 CPU 寄存器测试示例	对于不包含 HWBIST 的器件，可以对 CPU 寄存器执行定期测试。STL_CPU_REG 不直接映射到 C2000 唯一 ID。STL_CPU_REG 是指诊断库中的一个 CPU 寄存器测试示例。如果需要，也为其他器件提供此示例。请参阅诊断库文档。

5.2 CPU 相关故障

表 5-3. CPU 故障

CPU 组件	B/1 级 (1)	C/2 级 (1)	可接受措施 (2)		C2000 唯一 ID (3)				
			定义	说明	F2837x F2807x	F2838x	F28004x	F28002x	F28003x
1.1 寄存器	rq		H.2.16.5 A5.5	功能测试	- CLA2	- CLA2	CPU3 CLA2	- -	- CLA2
			H.2.16.6 A5.6	定期自检	CPU2 CLA2 -	CPU2 CLA2 -	- CLA2 -	CPU2 - -	CPU2 CLA2 -
		rq	H.2.18.15 A7.1.19	相互比较	CPU1 CLA1	CPU1 CLA1	CPU1 CLA1	- -	CPU1 CLA1
			H.2.18.3 A7.1.6	独立硬件比较器	-	-	-	-	-
			H.2.18.9 A7.1.10	内部错误检测	CPU2	CPU2	-	CPU2	CPU2
1.2 指令解码和执行		rq	H.2.18.15 A7.1.19	相互比较	CPU1 CLA1	CPU1 CLA1	CPU1 CLA1	- -	CPU1 CLA1
			H.2.18.3 A7.1.6	独立硬件比较器	-	-	-	-	-
			H.2.18.9 A7.1.10	内部错误检测	CPU2 CPU7 CLA3	CPU2 CPU7 CLA3	- CPU7 CLA3	CPU2 CPU7 -	CPU2 CPU7 CLA3

表 5-3. CPU 故障（续）

CPU 组件	B/1 级 (1)	C/2 级 (1)	可接受措施 (2)		C2000 唯一 ID (3)				
			定义	说明	F2837x F2807x	F2838x	F28004x	F28002x	F28003x
1.3 程序计数器	rq		H.2.16.5 A5.5	功能测试	- CLA2	- CLA2	CPU3 CLA2	- -	- CLA2
			H.2.16.6 A5.6	定期自检	CPU2	CPU2	-	CPU2	CPU2
			H.2.18.10.4 A7.1.13	时隙监控	PIE8	PIE8	PIE8	PIE8	PIE8
		rq	H.2.18.10.3 A7.1.14	独立时隙监控和逻辑监控	PIE8	PIE8	PIE8	PIE8	PIE8
			H.2.18.15 A7.1.19	相互比较	CPU1 CLA1	CPU1 CLA1	CPU1 CLA1	- -	CPU1 CLA1
			H.2.18.3 A7.1.6	独立硬件比较器	-	-	-	-	-
1.4 寻址		rq	H.2.18.15 A7.1.19	相互比较	CPU1 CLA1	CPU1 CLA1	CPU1 CLA1	- -	CPU1 CLA1
			H.2.18.3 A7.1.6	独立硬件比较器	-	-	-	-	-
			H.2.18.9 A7.1.10	内部错误检测	CPU2	CPU2	-	CPU2	CPU2
1.5 数据路径		rq	H.2.18.15 A7.1.19	相互比较	CPU1 CLA1	CPU1 CLA1	CPU1 CLA1	- -	CPU1 CLA1
			H.2.18.3 A7.1.6	独立硬件比较器	-	-	-	-	-
			H.2.18.9 A7.1.10	内部错误检测	CPU2	CPU2	-	CPU2	CPU2

(1) rq：所示等级的标准需要故障模式的覆盖率（请参阅表 2-2）。可能有多个可接受措施供选择。
(2) 请参阅 IEC/UL 规范，了解可接受措施及其定义的完整列表。
(3) 请参阅功能安全手册，了解每个 ID 的说明和实施建议。

5.3 中断相关故障

表 5-4. 中断故障到唯一 ID 的映射

组件	B/1 级 (1)	C/2 级 (1)	可接受措施 (2)		C2000 唯一 ID (3)				
			定义	说明	F2837x F2807x	F2838x	F28004x	F28002x	F28003x
2.中断	rq		H.2.16.5 A5.5	功能测试	PIE1 PIE2 PIE3 PIE6	PIE1 PIE2 PIE3 PIE6	PIE1 PIE2 PIE3 PIE6	PIE1 PIE2 PIE3 PIE6	PIE1 PIE2 PIE3 PIE6
			H.2.18.10.4 A7.1.13	时隙监控	PIE8	PIE8	PIE8	PIE8	PIE8
		rq	H.2.18.15 A7.1.19	相互比较	CPU1 CLA1	CPU1 CLA1	CPU1 CLA1	- -	CPU1 CLA1
			H.2.18.3 A7.1.6	独立硬件比较器	-	-	-	-	-
			H.2.18.10.3 A7.1.14	独立时隙监控和逻辑监控	PIE8	PIE8	PIE8	PIE8	PIE8

(1) rq：所示等级的标准需要故障模式的覆盖率（请参阅表 2-2）。可能有多个可接受措施供选择。
(2) 请参阅 IEC/UL 规范，了解可接受措施及其定义的完整列表。
(3) 请参阅功能安全手册，了解每个 ID 的说明和实施建议。

5.4 时钟相关故障

表 5-5. 时钟故障到唯一 ID 的映射

组件	B/1 级 (1)	C/2 级 (1)	可接受措施 (2)		C2000 唯一 ID (3)				
			定义	说明	F2837x F2807x	F2838x	F28004x	F28002x	F28003x
3.时钟	rq		H.2.18.10.1 A7.1.11	频率监控	CLK3	CLK3	CLK3	CLK3	CLK3
			H.2.18.10.4 A7.1.13	时隙监控	PIE8	PIE8	PIE8	PIE8	PIE8
		rq	H.2.18.15 A7.1.6	独立硬件比较器	CLK2 CLK5 - - - -	CLK2 CLK5 - CLK16 APLL1 APLL7	CLK2 CLK5 CLK4 - - -	CLK2 CLK5 - CLK17 - -	CLK2 CLK5 - CLK17 APLL1 APLL7

(1) rq：所示等级的标准需要故障模式的覆盖率（请参阅表 2-2）。可能有多个可接受措施供选择。
(2) 请参阅 IEC/UL 规范，了解可接受措施及其定义的完整列表。
(3) 请参阅功能安全手册，了解每个 ID 的说明和实施建议。

5.5 存储器相关故障

表 5-6. 存储器故障到唯一 ID 的映射

组件	B/1 级 (1)	C/2 级 (1)	可接受措施 (2)		C2000 唯一 ID (3)				
			定义	说明	F2837x F2807x	F2838x	F28004x	F28002x	F28003x
4.1 非易失性	rq		H.2.19.3.2 A7.2.5	多重校验和	-	-	ROM10	ROM10	ROM10
			H2.19.8.2 A7.3.2	字保护，single-bit 奇偶校验	-	-	-	-	ROM15
		rq	H.2.18.15 A7.1.19	相互比较	CPU1 CLA1	CPU1 CLA1	CPU1 CLA1	- -	CPU1 CLA1
			H.2.18.3 A7.1.6	独立硬件比较器	-	-	-	-	-
			H.2.19.5 A7.2.8	冗余存储器，支持比较	DCSM2	DCSM2	DCSM2	DCSM2	DCSM2
			H.2.19.4.2 A7.2.7	周期性 CRC，双字	FLASH2 ROM1 - -	FLASH2 ROM1 - -	FLASH2 ROM1 ROM9 -	FLASH2 ROM1 - -	FLASH2 ROM1 - ROM13
			H2.19.8.1 A7.3.1	字保护，支持 multi-bit 冗余	FLASH1 EFUSE2	FLASH1 EFUSE2	FLASH1 EFUSE2	FLASH1 EFUSE2	FLASH1 EFUSE2
4.2 易失性	rq		H.2.19.6 A7.2.9	定期静态存储器测试	SRAM3	SRAM3	SRAM3	SRAM3	SRAM3
			H2.19.8.2 A7.3.2	字保护，single-bit 奇偶校验	SRAM2 CAN3 - -	SRAM2 CAN3 ECAT6 -	SRAM2 CAN3 - -	SRAM2 CAN3 - -	- CAN3 - -
		rq	H2.19.5 A7.2.8	冗余存储器，支持比较	PIE1	PIE1	PIE1	PIE1	PIE1
			H.2.19.8.1 A7.3.1	字保护，multi-bit 冗余	SRAM1 -	SRAM1 MCAN8	SRAM1 -	SRAM1 -	SRAM1 MCAN8

表 5-6. 存储器故障到唯一 ID 的映射（续）

组件	B/1 级 (1)	C/2 级 (1)	可接受措施 (2)		C2000 唯一 ID (3)				
			定义	说明	F2837x F2807x	F2838x	F28004x	F28002x	F28003x
4.3 寻址（易失性和非易失性存储器）	rq		H2.19.8.2 A7.2.9	字保护，single-bit 奇偶校验	SRAM2 - CAN3 - -	SRAM2 - CAN3 ECAT6 -	SRAM2 - CAN3 - -	SRAM2 - CAN3 - -	- ROM15 CAN3 - -
		rq	H.2.19.4.2 A7.2.7	周期性 CRC - 双字	SRAM8 (4) - FLASH2 ROM1 - -	SRAM8 SRAM24 FLASH2 ROM1 - -	SRAM8 - FLASH2 ROM1 ROM9 -	SRAM8 SRAM24 FLASH2 ROM1 - -	SRAM8 SRAM24 FLASH2 ROM1 - ROM13
			H.2.19.8.1 A7.3.1	字保护，multi-bit 冗余，包括地址	FLASH1 SRAM1	FLASH1 SRAM1 MCAN8	FLASH1 SRAM1	FLASH1 SRAM1	FLASH1 SRAM1 MCAN8

(1) rq：所示等级的标准需要故障模式的覆盖率（请参阅表 2-2）。可能有多个可接受措施供选择。
(2) 请参阅 IEC/UL 规范，了解可接受措施及其定义的完整列表。
(3) 请参阅功能安全手册，了解每个 ID 的说明和实施建议。
(4) F2807x 器件没有 VCRC 模块。CRC 由 CPU 执行。请参阅器件特定的软件诊断库。

5.6 内部数据路径故障

表 5-7. 内部数据路径故障到唯一 ID 的映射

组件	B/1 级 (1)	C/2 级 (1)	可接受措施 (2)		C2000 唯一 ID (3)				
			定义	说明	F2837x F2807x	F2838x	F28004x	F28002x	F28003x
5.1 数据	rq		H.2.19.8.2 A7.3.2	字保护，支持 single-bit 奇偶校验	SRAM2 -	SRAM2 -	SRAM2 -	SRAM2 -	- ROM15
		rq	H.2.18.15 A7.1.19	相互比较	CPU1 CLA1	CPU1 CLA1	CPU1 CLA1	- -	CPU1 CLA1
			H.2.18.3 A7.1.6	独立硬件比较器	-	-	-	-	-
			H.2.19.8.1 A7.3.1	字保护，支持 multi-bit 冗余，包括地址	FLASH1 SRAM1	FLASH1 SRAM1	FLASH1 SRAM1	FLASH1 SRAM1	FLASH1 SRAM1
			H.2.18.22 A7.1.24	测试模式	SRAM3 SRAM13 SRAM14 FLASH6	SRAM3 SRAM13 SRAM14 FLASH6	SRAM3 SRAM13 SRAM14 FLASH6	SRAM3 SRAM13 SRAM14 FLASH6	SRAM3 SRAM13 SRAM14 FLASH6
					-	-	-	-	-
			H.2.18.14 A7.1.18	协议测试	INC1 INC8 INC9	INC1 INC8 INC9	INC1 INC8 INC9	INC1 INC8 INC9	INC1 INC8 INC9

表 5-7. 内部数据路径故障到唯一 ID 的映射（续）

组件	B/1 级 (1)	C/2 级 (1)	可接受措施 (2)		C2000 唯一 ID (3)				
			定义	说明	F2837x F2807x	F2838x	F28004x	F28002x	F28003x
5.2 寻址	rq		H.2.19.8.2 A7.3.2	字保护，支持 single-bit 冗余，包括地址	SRAM2	SRAM2	SRAM2	SRAM2	-
		rq	H.2.18.15 A7.1.19	相互比较	CPU1 CLA1	CPU1 CLA1	CPU1 CLA1	- -	CPU1 CLA1
			H.2.18.3 A7.1.6	独立硬件比较器	-	-	-	-	-
			H.2.19.8.1 A7.1.6	字保护，支持 multi-bit 冗余，包括地址	FLASH1 SRAM1	FLASH1 SRAM1	FLASH1 SRAM1	FLASH1 SRAM1	FLASH1 SRAM1
			H.2.18.22 A7.1.24	测试模式，包括地址	FLASH6	FLASH6	FLASH6	FLASH6	FLASH6

(1) rq：所示等级的标准需要故障模式的覆盖率（请参阅表 2-2）。可能有多个可接受措施供选择。
(2) 请参阅 IEC/UL 规范，了解可接受措施及其定义的完整列表。
(3) 请参阅功能安全手册，了解每个 ID 的说明和实施建议。

5.7 输入/输出相关故障

表 5-8. 输入/输出外设故障到唯一 ID 的映射

组件	B/1 级 (1)	C/2 级 (1)	可接受措施 (2)		C2000 唯一 ID (3)				
			定义	说明	F2837x F2807x	F2838x	F28004x	F28002x	F28003x
7.1 数字 I/O	rq		H.2.18.13 A7.1.17	合理性检查	GPIO4	GPIO4	GPIO4	GPIO4	GPIO4
		rq	H.2.18.8 A7.1.9	输入比较	GPIO5	GPIO5	GPIO5	GPIO5	GPIO5
			H.2.18.11 A7.1.15	多个并行输出	GPIO5	GPIO5	GPIO5	GPIO5	GPIO5
			H.2.18.12 A7.1.16	输出验证	GPIO4	GPIO4	GPIO4	GPIO4	GPIO4
7.2 模拟 I/O 7.2.1 模数和数模转换器	rq		H.2.18.13 A7.1.17	合理性检查	ADC2 ADC8	ADC2 ADC8	ADC2 ADC8	ADC2 ADC8	ADC2 ADC8
		rq	H.2.18.8 A7.1.9	输入比较	ADC10	ADC10	ADC10	ADC10	ADC10
7.2 模拟 I/O 7.2.2 模拟多路复用器	rq		H.2.18.13 A7.1.17	合理性检查	ADC2 ADC8	ADC2 ADC8	ADC2 ADC8	ADC2 ADC8	ADC2 ADC8
		rq	H.2.18.15 A7.1.19	输入比较	ADC10	ADC10	ADC10	ADC10	ADC10

(1) rq：所示等级的标准需要故障模式的覆盖率（请参阅表 2-2）。可能有多个可接受措施供选择。
(2) 请参阅 IEC/UL 规范，了解可接受措施及其定义的完整列表。
(3) 请参阅功能安全手册，了解每个 ID 的说明和实施建议。

5.8 通信、监控器件和定制芯片故障

表 5-9. 外部通信、监控器件和定制芯片故障

组件	B/1 级	C/2 级	可接受措施	C2000 唯一 ID
6.数据	请参阅 60730 标准			有关通信端口安全机制，请参阅器件特定的功能安全手册。由于此列表太长而无法完全复制，此处仅提供了几个示例： • 使用环回进行软件测试 • CRC 组帧/消息检查 • ECC 组帧检查 • 校验和错误检测 • 数据超限和欠运转检测 • 物理总线错误检测 • FIFO 活动超时
6.2 寻址				
6.3 时序				
8.监控器件和比较器	请参阅 60730 标准			要求和实施取决于系统。有关在实施中可以利用的安全机制，请参阅器件特定的功能安全手册。
第 1-8 项未涵盖的组件。定制芯片（ASIC、GAL、门阵列）	请参阅 60730 标准			要求和实施取决于系统。有关在实施中可以利用的安全机制，请参阅器件特定的功能安全手册。

6 术语表

表 6-1. 术语和定义

术语和缩写	定义
A.x...	UL 1998 标准中的参考。例如：A.7.1.19 是该标准的附录 A 中的具体定义
C28x	C2000 中央处理单元
CLA	C2000 控制律加速器：独立的 32 位浮点处理器
CLA PROM	CLA CPU 的程序 ROM
CLB	C2000 可配置逻辑块
B/1 级	IEC 60730 B 级和 UL 1998 1 级。根据功能安全评估结果指定的等级。请参阅 c
C/2 级	IEC 60730 C 级和 UL 1998 2 级：根据功能安全评估结果指定的等级。请参阅表 2-1
CLK	时钟
CPU	中央处理单元
CPU 计时器	C2000 通用计时器外设
CRC	循环冗余校验
直流故障	(IEC/UL) 信号间短路
DCC	C2000 双时钟比较器
DCSM	C2000 双代码安全模块
ECC	错误校正码
E/E/PE	(IEC/UL) 电气/电子/可编程电子
EMC	(IEC/UL) 电磁兼容性
ePIE	C2000 增强型外设中断扩展块。也可称为 PIE
ePWM	C2000 增强型脉宽调制外设。也可称为 PWM
FPU	C28x CPU 的浮点单元指令集扩展
FSM	• 本文档使用 FSM 表示功能安全手册（节 3.2） • (IEC/UL) FSM 用于表示功能安全管理
GPIO	C2000 通用输入/输出引脚
H.x...	IEC 60730 标准中的参考。例如：H.2.16.5 是该标准的附录 H 中的具体定义
HRPWM	C2000 ePWM 模块的高分辨率特性
HW	硬件（微控制器）
HWBIST	C2000 硬件内置自检
IEC	国际电工委员会
IEC 60730	术语“IEC 60730”、“UL 1998”、“IEC/UL 标准”、“60730”和“标准”可互换用于指代以下两者： • IEC60730-1 版本 5.0 2013-11，附录 H 和表 H.1（版本 3 的 H.11.12.7）– “处理故障/错误的可接受措施” • 可编程组件中的安全软件 UL 标准，UL 1998，第三版，日期 2013 年 12 月 18 日，附录 A 和表 A2.1 – “微电子硬件故障模式的覆盖率”
IEC 61508	IEC 61508 电气/电子/可编程电子安全相关系统的功能安全，国际电工委员会，2.0 版，2010 年
ISO 26262	ISO 26262 – 道路车辆 - 功能安全，国际标准 ISO，26262 卷，2018 年
IEC/UL	标准的缩写或表示取自标准的内容，例如此列表中标记为 (IEC/UL) 定义。请参阅 IEC 60730
MPOST	存储器开机自检
PIE	请参阅 ePIE
PWM	请参阅 ePWM
PEST	定期自检
POST	开机自检
ROM	只读存储器

表 6-1. 术语和定义（续）

术语和缩写	定义
SDL	软件诊断库
SRAM	静态随机存取存储器
STL	自检库
固定型	(IEC/UL) 开路故障或信号电平不变
SW	软件
TI	德州仪器 (TI) 公司
TMU	C28x CPU 的三角函数加速器指令集扩展
UL	Underwriters Laboratories Inc.（美国保险商实验室公司）
UL 1998	请参阅 IEC 60730
唯一 ID	在功能安全手册中分配给功能安全特性或诊断的 C2000 唯一标识符，例如 CLK2 或 GPIO4
VCRC	请参阅 VCU
VCU	C28x CPU 的指令集扩展。添加的指令的一部分是专用于 CRC 计算的指令。某些器件支持 CRC 指令，简称为“VCRC”

7 参考文献

备注

在器件产品文件夹的技术文档部分可以找到器件特定的功能安全手册。产品文件夹 URL 的格式为 *ti.com/product/<器件>*。例如：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. 德州仪器 (TI)：C2000 Academy 在线培训
4. 德州仪器 (TI)：适用于 C2000 MCU 的 C2000Ware 软件开发套件
5. 德州仪器 (TI)：*C2000™ 实时微控制器的工业功能安全特性*
6. 德州仪器 (TI)：*C2000™ 安全机制*
7. 德州仪器 (TI)：*C2000™ 硬件内置自检*
8. 德州仪器 (TI)：*C2000™ CPU 存储器内置自检*
9. 德州仪器 (TI)：*C2000™ 存储器开机自检 (M-POST)*
10. 德州仪器 (TI)：*适合控制应用的嵌入式实时分析和响应 (ERAD)*

重要声明和免责声明

TI“按原样”提供技术和可靠性数据（包括数据表）、设计资源（包括参考设计）、应用或其他设计建议、网络工具、安全信息和其他资源，不保证没有瑕疵且不做出任何明示或暗示的担保，包括但不限于对适销性、某特定用途方面的适用性或不侵犯任何第三方知识产权的暗示担保。

这些资源可供使用 TI 产品进行设计的熟练开发人员使用。您将自行承担以下全部责任：(1) 针对您的应用选择合适的 TI 产品，(2) 设计、验证并测试您的应用，(3) 确保您的应用满足相应标准以及任何其他功能安全、信息安全、监管或其他要求。

这些资源如有变更，恕不另行通知。TI 授权您仅可将这些资源用于研发本资源所述的 TI 产品的应用。严禁对这些资源进行其他复制或展示。您无权使用任何其他 TI 知识产权或任何第三方知识产权。您应全额赔偿因在这些资源的使用中对 TI 及其代表造成的任何索赔、损害、成本、损失和债务，TI 对此概不负责。

TI 提供的产品受 TI 的销售条款或 ti.com 上其他适用条款/TI 产品随附的其他适用条款的约束。TI 提供这些资源并不会扩展或以其他方式更改 TI 针对 TI 产品发布的适用的担保或担保免责声明。

TI 反对并拒绝您可能提出的任何其他或不同的条款。

邮寄地址：Texas Instruments, Post Office Box 655303, Dallas, Texas 75265