用于 Hercules™ TMS470M ARM® 安全微控制器的安全手册

User's Guide

Literature Number: ZHCU036
April 2012

内容

图片列表

图表列表

用于 Hercules™ TMS470M ARM® 安全微控制器的安全手册

1 简介

作为一个系统和设备制造商或者设计人员，您有责任确保您的系统（和任一 TI 硬件或者包含在您系统内的软件组件）符合全部应用安全、规定、和系统级性能要求。 本文档中的所有应用和安全相关信息（包括应用说明、建议安全措施、推荐 TI 产品、和其它材料）只用作参考。 您了解并同意对在安全应用中使用 TI 组件负责，并且您（作为买家）同意对在此类应用中的造成的所有损失、索赔、诉讼、或者费用为 TI 辩护、保护 TI 不受伤害。

本文档是针对德州仪器 (TI) 的赫丘利斯 TMS470M 安全微控制器产品系列的安全手册。 此产品系列使用一个常见的安全架构，此架构在针对多应用中被执行。 这本安全手册涉及的产品工具包括：

- TMS470M 车用安全微控制器
  - TMS470MF06x
  - TMS470MF04x
  - TMS470MF03x

这本安全手册提供系统开发人员所需的信息以帮助他们使用一个受支持的赫丘利斯 TMS470M 微控制器来创建一个安全系统。 这个文档包含：

- 扩展集产品架构概述
- 用于减少系统故障的开发过程的概述
- 针对随机故障管理的安全架构的概述
- 架构分区、实施的安全机制、和推荐用法的详细资料

我们认为，使用本文档的用户应该大体上熟悉赫丘利斯 TMS470M 产品系列。 可从以下网站获得更多信息：http://www.ti.com/hercules。 本文档的目的是与相关数据表、技术参考手册、和其它处于开发阶段产品的文档一起使用。 这个技术内容部分是为了简化开发、减少内容重复、并避免混淆。

2 TMS470M 产品概述

在已经验证的 TMS470 平台架构中执行 ARM Cortex™-M3 CPU 的产品系列。 图 1中显示了一张产品扩展集架构的简化图。 这张图只是此架构的基本表示而非包含全部内容。 例如，此系列中的产品可以按照外设的数量、分离的或者合并的二级总线标准、或者内存数量进行升级-但是程序设计者的模型仍然保持一致。

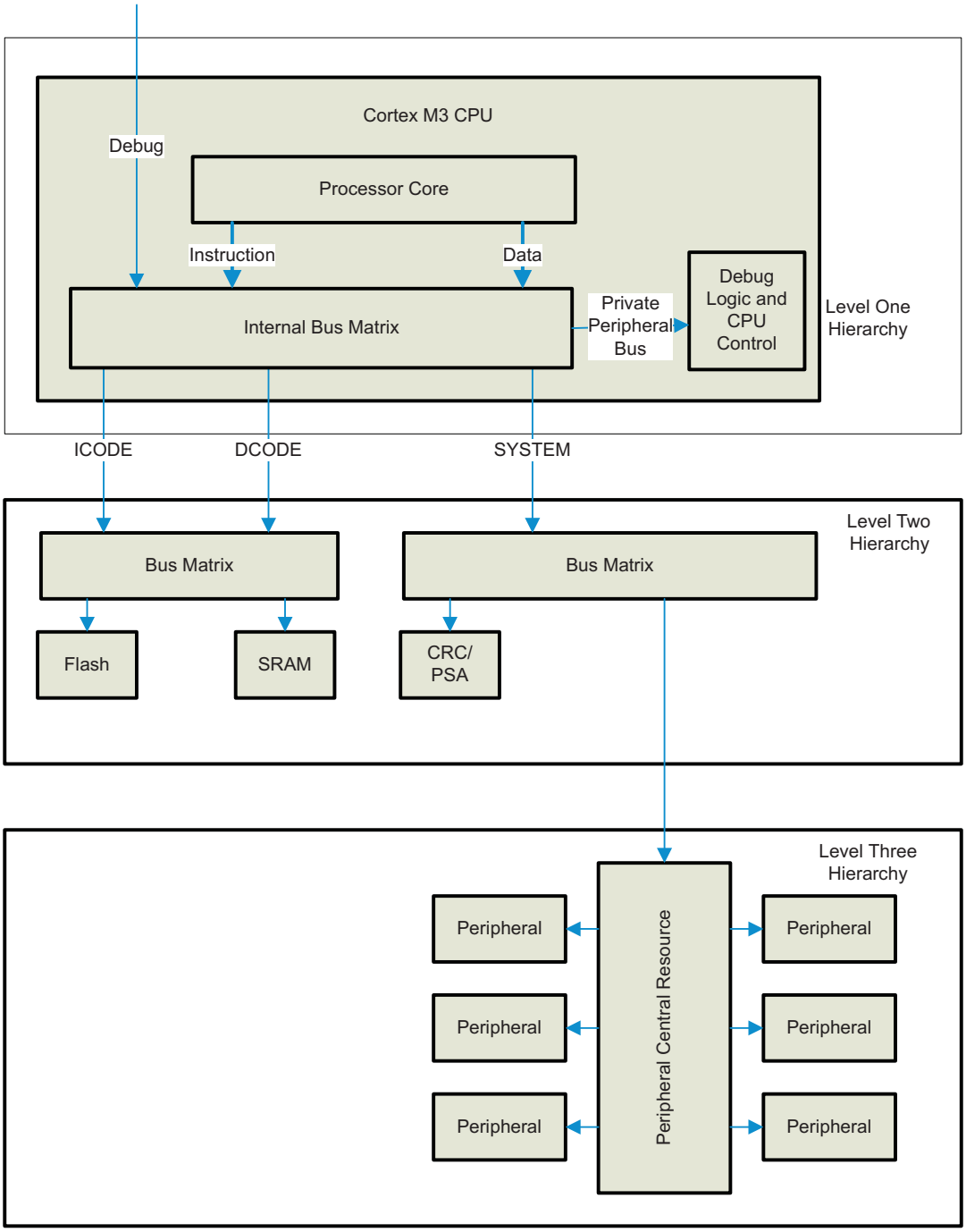

图 1. Hercules TMS470M 产品架构概述

此Hercules TMS470M 产品架构可被解释为三个层次。 一级层次包括 ARM Cortex-M3 CPU。 Cortex-M3 CPU 包括一个处理内核、调试逻辑电路、和一个内部总线矩阵。 在内部总线矩阵上有三个总线主控和四个总线受控。 内部总线主控包括处理器内核指令和数据以及外部调试。 总线受控为 ICODE 总线（用于从闪存和 SRAM 中提取指令），DCODE 总线（用于从闪存和 SRAM 的数据读取/写入），系统 (SYSTEM) 总线（用于外设读取/写入访问），和私有外设总线（用于调试逻辑电路和 CPU 控制功能的配置）。 内部总线矩阵为总线事务处理提供仲裁、优先级划分、路径选择、和解码功能性。

二级器件等级由两个总线矩阵（也被称为开关中央资源或者交叉开关矩阵 (crossbar)）控制。 这是一个器件级互连，此互连在实现 Cortex-M3 CPU 到多总线受控的访问的同时提供仲裁、优先级排序、路径选择、解码、和解码功能性。 到二级器件等级的总线主控包括 ICODE，DCODE，和来自 Cortex-M3 CPU 的系统总线。 二级等级上的总线受控包括闪存存储器，SRAM，一个 CRC/PSA 引擎、和到三级外设等级的访问。

三级等级主要由外设组成。 外设被分成一个或者多个外设总线段，由一个外设中心资源统一管理。 这个外设中心资源为总线事务处理目标外设提供地址解码功能。

2.1 目标应用

Hercules TMS470M MCU 系列针对通用安全应用。 在概念阶段，对多重安全应用进行过分析。 目标应用示例包括：

- 车辆刹车系统，包括轮胎防锁死系统 (ABS)、带有牵引控制的轮胎防锁死系统 (ABS+TC)、和电子稳定性控制系统 (ESC)
- 电机控制系统，特别是电子助力转向 (EPS) 系统和电动汽车 (EV) 动力传动系统
- 通用安全计算，例如主动安全系统中的集成传感器集群处理
- 工业自动化，例如用于安全流程控制的可编程逻辑控制器 (PLC) 和可编程自动化控制器 (PAC)

虽然 TI 在开发这些器件时考虑了特定的应用情况，但是这不应限制客户执行其它系统。 借助于所有安全组件，组件安全概念到系统安全概念的合理化转化必须由系统集成人员来完成。

2.2 产品安全约束

对于按照很多安全标准开发的安全组件，组件安全手册将提供产品安全约束列表。 对于一个简单组件，或者被开发用于一个单一应用的更加复杂的组件，这是一个合理的答复。 然而，Hercules 产品系列既是复杂设计，又非针对一个单一、特定应用而开发的器件。 因此，一个单一的产品安全约束集不能管理该产品所有可行的使用。 《*Hercules TMS470M ARM 安全微控制器安全分析报告摘要》(SPNU561)*提供一个带有相关产品安全约束的通用系统中 TMS470M 产品的示例工具。

3 针对系统故障管理的 TMS470M 开发过程

对于安全开发，有必要对系统和随机故障同时进行管理。 Hercules TMS470M 产品由一个由标准质量管理的开发过程创建，此开发过程大大减少了系统故障的发生。

3.1 TI 标准 MCU 汽车用开发过程

德州仪器 (TI) 从事针对安全和非安全汽车应用的汽车用微控制器开发已经超过二十年。 汽车市场对于产品的质量管理和高可靠性有着很强的需求。 虽然不是明确针对符合功能安全标准进行开发，TI 标准 MCU 汽车开发过程已经特有了很多管理系统故障所必须的要素。 这个开发过程可以被看成是质量管理 (QM)，但是并未达到 IEC 61508 安全完整性级别 (SIL) 或者 ISO 26262 汽车安全完整性级别 (ASIL)。 TI 标准 MCU 汽车开发过程经认证符合 ISO TS 16949，此认证由 Det Norske Veritas 认证公司 （Katy，德克萨斯州）在证书 CERT-07319CC10-2004-AQ-HOU-IATF 下评定（IATF 证书编号 0113679）。 此开发经认证也符合 ISO 9001:2008，此认证评估由 DNV 认证 B.V.（荷兰） 在证书 CERT-06185-2003-AQ-HOU-RvA 修订版本 2 下评定。

此标准过程将开发分成以下三个阶段：

- 商业机会预先筛分
- 程序计划编制
- 创建
- 验证、采样、和辨别
- 证明
- 产量增加和持续生产

标准过程显示在图 2中。

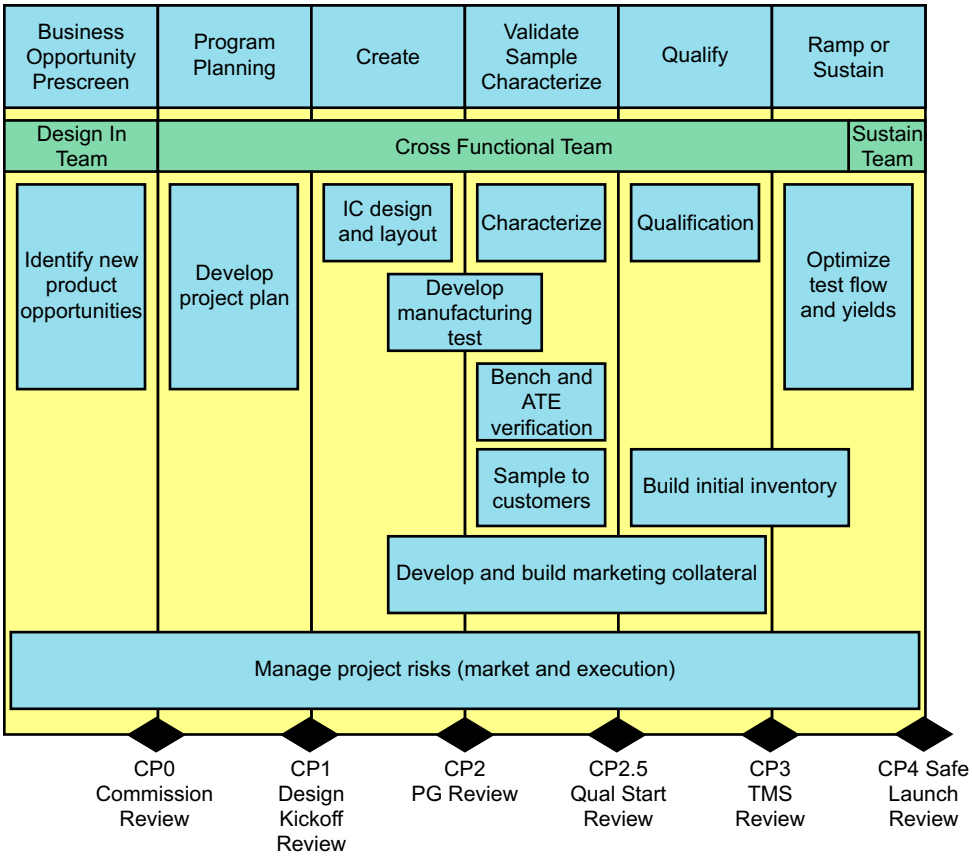

图 **2. TI** 标准 **MCU** 汽车用 **QM** 开发过程

3.2 IEC 61508 和 ISO 26262 的开发过程差距

Hercules TMS470M 产品的开发早于 IEC 61508:2010 和 ISO 26262:2011 功能安全标准。 这样的话，这些标准推荐的开发过程对Hercules TMS470M 产品不适用。 在 exida 咨询公司的帮助下，德州仪器 (TI) 已经进行了已采用的过程与 IEC 61508 标准间的差距分析。 由于是相似的标准，此分析活动的结果也可应用于 ISO 26262 开发。 所得结果汇总如下。

差距分析的关键发现：

- 硬件开发过程已经符合 IEC 61508-2 IEC 第二版的附录 F。
- 已经认识到一些差距，大多数与功能安全所独有的要求相关，例如：
  - 没有采用一个功能安全管理计划来管理程序开发期间的安全。
  - 没有为功能安全文档创建标准所建议的模版和检查清单中的一个或者全部。
  - 功能安全评估没有被组合进开发过程。
  - 安全要求并未明确定义和验证。

这一分析的所有结果已经在随后的 Hercules 产品系列中进行了解决。

4 针对随机故障管理的 TMS470M 的产品架构

对于一个安全开发，有必要管理系统和随机故障。 Hercules TMS470M 产品架构包括很多安全机制，当正确使用时，安全机制能够检测并对随机故障做出响应。 此文档的这一部分对于针对 MCU 的架构安全概念进行了说明。

4.1 针对安全分析的架构划分

Hercules TMS470M 处理器共用一个通用安全加固。 这个基本概念涉及到硬件诊断应用和软件诊断间的一个平衡以在管理功能安全的同时平衡成本。 在这个方法中，一个元件的内核集被分配硬件安全机制。 这个元件内核集，其中包括电源和时钟以及复位、CPU、闪存存储器、和可被用于确保软件功能正确执行的 SRAM。 为了在其它器件元件上，例如外设，提供基于软件的诊断，一旦这些元件的正确运行被确认，软件就能够在这些元件上执行。

图 3用图例显示了覆盖在 Hercules TMS470M 产品架构扩展集配置上的安全概念。

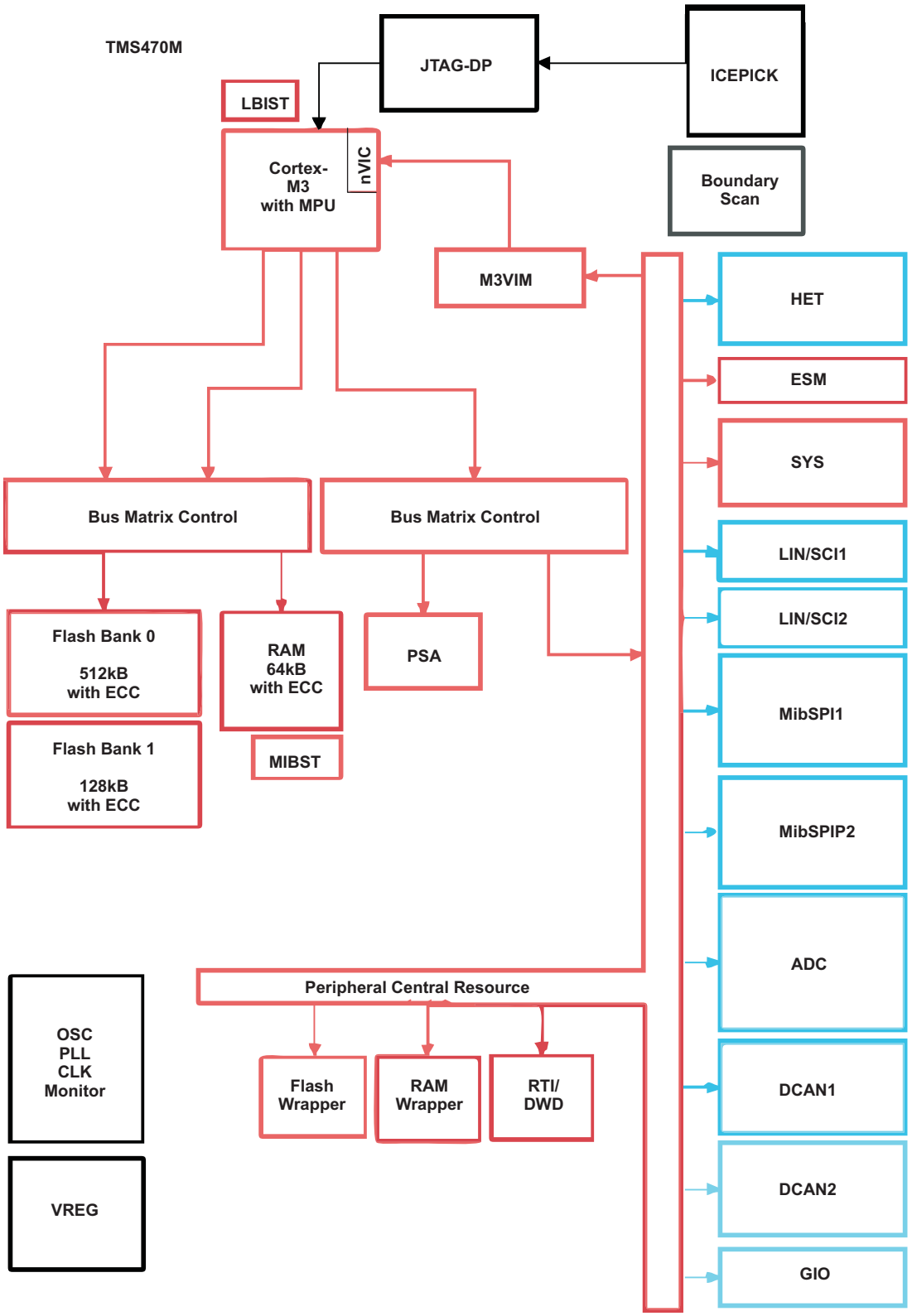

图 **3. Hercules TMS470M MCU** 用于安全分析的部分

图 3用图例显示了三个架构划分：

- “硬件层（红色）”-此区域为所有处理操作所需的逻辑电路。 这个逻辑电路受到主板硬件诊断和特定使用假定的重要保护以确保对于安全运行的高级别信心。 一旦这个区域是安全的，它可被用于在其它设计元件上提供综合性的软件诊断。
- “混合层”（蓝色）-这个区域是包含大多数安全外设的区域。 这个区域相对不太依赖于硬件诊断。 软件诊断和应用协议被置于它们之上以提供必需诊断覆盖的剩余项。
- “离线层”（黑色）-这个区域的逻辑电路具有最少的或者没有集成硬件诊断。 这一层中的很多特性只用于调试、测试、和校准功能；在安全运行期间，闪存未激活。 这个区域的逻辑电路可被用于安全运行，假定系统集成人员已经添加了适当的软件诊断或者系统级措施。

4.2 系列变量管理

Hercules TMS470M 系列架构支持多个产品变量。 这些产品能够作为唯一芯片设计被执行或者它们可以是共享芯片设计，在这些设计中，有些元件，即使出现在芯片中，也被禁用或者不被技术规范所相信。 只有在特定器件数据表和技术参考手册中进行明确说明的扩展集架构的元件才能被确保出现并运行。 当进行 Hercules TMS470M 平台开发时，建议安全概念应基于扩展集产品架构以在系列变量范围内启用最大扩展性。 上一个部分中显示的扩展集架构针对安全手册介绍部分中注释的所有器件部件号有效。

4.3 运行状态

Hercules TMS470M MCU 产品有一个运行状态的通用架构定义。 这些运行状态应该由系统开发人员在他们的软件和系统级设计概念中进行观测。 运行状态机显示在图 4中并说明如下。

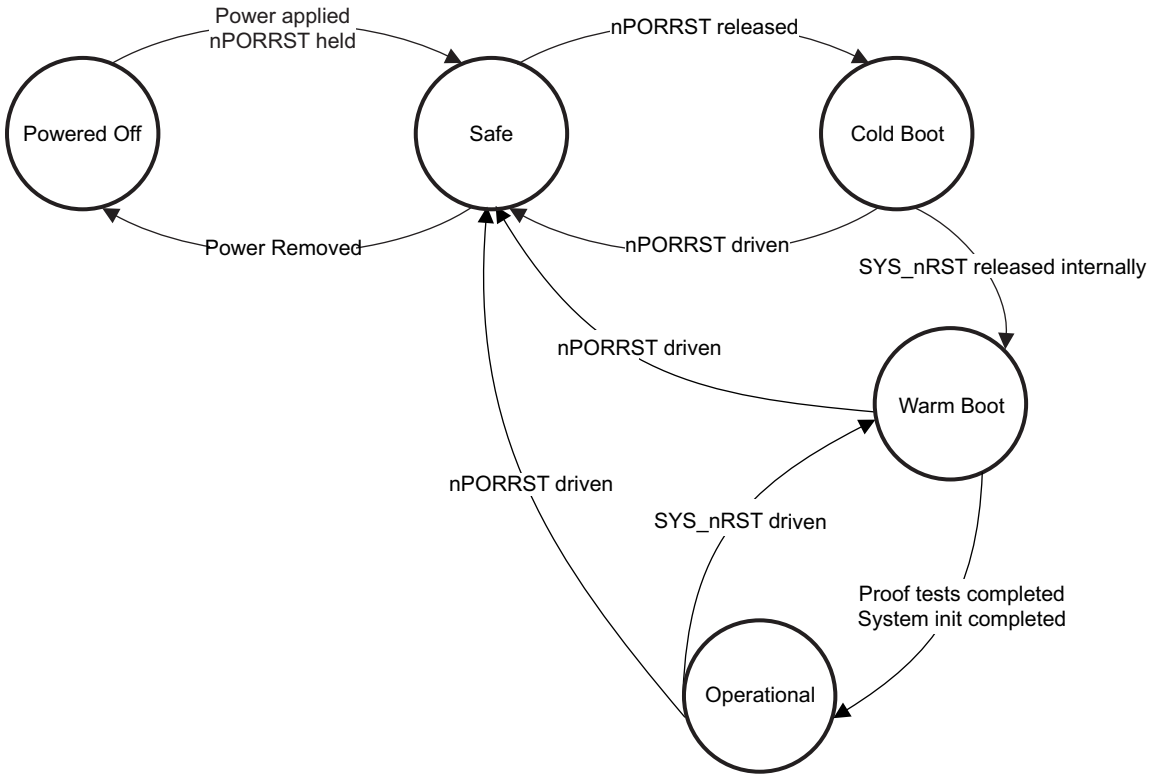

图 4. Hercules TMS470M MCU 运行状态

- “断电”-这是 Hercules TMS470M MCU 的初始运行状态。 内核或者 I/O 电源均未加电，器件处于非功能状态。 这个状态只能转换到安全状态，并且只能通过安全状态到达此状态。
- “安全”-在安全状态中，Hercules TMS470M MCU 被加电但还不可用。 nPORRST（加电复位、也被成为冷启动）由系统置成有效，但是在电源缓慢上升为稳定状态之前不被释放。 如果电源不在一个最小运行

范围内，内部电压监视 (VMON) 安全机制也会继续将 nPORRST 置为器件内部有效。 当产品处于安全状态时，CPU 和外设不可用。 输出驱动器是被保持在一个只输入状态的三态和输入/输出引脚。

- “冷启动”-在冷启动状态中，关键模拟元件、数字控制逻辑电路、和调试逻辑电路被初始化以为未来使用。 CPU 保持供电状态但不可用。 当冷启动过程完成时，SYS_nRST 信号被内部释放，导致热启动级。 SYS_nRST 信号过渡改变能在 SYS_nRST I/O 引脚上被外部监控。
- “热启动”-热启动模式将信号逻辑电路复位并启用 CPU。 CPU 开始从闪存存储器中执行软件并且器件的软件初始化开始。 没有硬件连环显示热启动已经完成；这由软件决定。
- “可用”-在可用模式期间，器件能够支持安全功能性。

4.4 错误管理

当诊断检测到一个故障，这个错误必须被标出。 Hercules TMS470M 产品架构使用一个被称为外设错误信令模块 (ESM) 的外设逻辑电路来提供来自内部安全机制的故障指示集合。 ESM 提供了一些机制来将错误按照严重性分类并提供可编程错误响应。 在表 1中，对 ESM 中的错误分类进行了汇总。

表 1. ESM 错误标示概要(1)

错误组	中断响应	注释
1	可编程中断和可编程中断优先级	对于一般为非关键严重的错误
2	生成不可屏蔽的中断	对于一般为关键严重的错误
3	无中断响应	对于那些在 CPU 中执行的诊断发现的关键错误

(1) 与其它 Hercules 产品不同，由于精简引脚数量的要求，赫丘利斯 TMS470M 系列没有器件错误引脚。

当一个错误被标明后，MCU 或者系统对此错误做出响应。 Hercules TMS470M 产品的错误响应有多种可能。 系统集成人员负责确定应该采取哪种错误响应并确保此响应与系统安全概念一致。

- CPU 异常结束-对于在 CPU 中执行的诊断，这个响应在 CPU 中直接执行。 在异常中断期间，此程序序列将环境转化为一个异常中断句柄并且软件有机会来管理此故障。
- CPU 中断-这个响应可由 CPU 外的诊断来执行。 在软件有机会来管理此故障的地方，一个中断允许 CPU 外部事件来生成一个程序序列环境并将其转化为中断句柄。
- SYS_nRST 生成-这个响应使得器件能够从操作状态变为热启动状态。 SYS_nRST 可以从一个外部监视器生成或者在内部由软件复位或者安全装置生成。 当不可能恢复到操作状态时，重新进入热启动状态使得软件恢复成为可能。

- nPORRST 生成-这个响应允许器件的状态变为冷启动状态、热启动状态、或者操作状态。 当不能从热启动状态中恢复时，有可能从这个状态重新进入冷启动状态来尝试恢复。 如果需要，也有可能进入断电状态来执行一个系统级安全状态。 这个响应可从内部电压监视器生成，但是主要由 MCU 外部监视器驱动。

ESM 提供了可由 CPU 读取的多个寄存器来确定诊断的当前状态。 对于严重分组 2 中的错误，提供一个不是由 SYS_nRST 复位的影子寄存器。 这使得热复位有可能重新初始化以识别一个启动外部复位的分组 2 错误。

对于 CPU，有可能手工触发错误响应来测试系统运行。 CPU 负责清除 ESM 中显示的错误。

可以通过使用 TI 系统基础芯片（专为与 Hercules TMS470M 系列一起使用而开发）来简化外部错误响应的系统级管理。

5 TMS470M 架构安全机制和使用假设

作为一个系统和设备制造商或者设计人员，您有责任确保您的系统（和任一 TI 硬件或者包含在您系统内的软件组件）符合全部应用安全、规定、和系统级性能要求。 本文档中的所有应用和安全相关信息（包括应用说明、建议安全措施、推荐 TI 产品、和其它材料）只用作参考。 您了解并同意对在安全关键应用中使用 TI 组件负责，并且您（作为买家）同意对在此类应用中的造成的所有损失、索赔、诉讼、或者费用为 TI 辩护、保护 TI 不受伤害。

在这一部分中，对 Hercules TMS470M 架构每个主要功能块的安全机制进行了总结并给出了使用方面的一般假设。 这些信息应该被用于确定采用安全机制的策略。 每一个安全机制的细节可在用于 MCU 的特定器件技术参考手册中找到。 硬件安全机制的有效性在*《 Hercules TMS470M ARM 安全微控制器安全分析报告摘要》(SPNU561) 中进行了注释*。

针对这一部分中安全机制的使用，TI 将技术文档分成了几个类别。 不应该认为 TI 建议绝对无错。 有很多不同的方法来执行安全系统并且替代的安全机制也有能提供支持来实现所需的安全标准。 建议的类别如下：

- 强制的-一个强制的标志表明在正常功能运行期间安全机制一直可用并且不能由用户禁用。
- 强烈推荐-一个强烈推荐的标志表明，TI 相信这个安全机制能够提供很难由其它方法执行的且具有较高价值的诊断。 由于安全机制的启用或者禁用需要用户的干预，用户保留在他们的设计中使用或者不使用此安全机制的权利。
- 推荐-一个推荐标志表明，TI 相信这个安全机制能够提供可使用其他方法执行的有价值的诊断。 由于安全机制的启用或者禁用需要用户的干预，用户保留在他们的设计中使用或者不使用此安全机制的权利。
- 可选-一个可选标志表明，TI 相信这个安全机制能够提供可使用其他方法执行的价值较低的诊断。 由于安全机制的启用或者禁用需要用户的干预，用户保留在他们的设计中使用或者不使用此安全机制的权利。

根据安全标准和目标端设备的不同，也许需要对单点故障和潜在故障进行管理。 依照 ISO 26262：2011，当在功能和安全机制中同时出现故障时，则认为有潜在故障。 在故障耐受时间间隔内，并不需要对潜在故障进行测试，但是可以在引导时间、关断时、或者定期执行对此类故障的测试，这可由系统开发人员确定。 本部分中所描述的很多安全机制可被用作初次诊断、针对潜在故障的诊断，或者二者兼备。 当从潜在故障管理角度来考虑系统设计时，针对通过软件执行的任何初次诊断，请注意将 CPU 和内存故障考虑在内。

5.1 电源 + 电压稳压器 (VREG)

Hercules TMS470M 器件系列产品包含一个内部电压稳压器 (VREG)，此稳压器可提供正确运行所需的内部电压。

5.1.1 VREG 嵌入式内核电压监控器

Hercules TMS470M VREG 组装有一个简单嵌入式电压监控器，此监控器能够大体检测超出范围的电源电压。 这个监控器持续运行并不要求软件配置或者 CPU 开销。 当电源远远高于或者低于额定电压（对于产品特定电压值，请参阅特定器件数据表）时，电压监控器从内部驱动 nPORRST（加电复位）信号。 这个响应将器件保持在安全运行状态。 当电源处于范围之内，电压监控器将不会干预 nPORRST 信号。 要获得更多与 VREG 和电压监控器操作相关的信息，请参阅特定器件数据表。

电压监控器是一个持续处于运行状态的诊断。 不能将电压监控器诊断禁用。 电压监控器诊断的系统内测试通常是不可行的，这是因为需要对外部电压进行严密控制来触发 监控器错误响应。 如果应用不当，这样一个电压会引起对 MCU 的永久损坏。 电压监控器的使用是强制的。

5.1.2 外部电压监视器

Hercules TMS470M 平台强烈建议使用一个外部电压监视器来监控所有的电压轨-包括 I/O 和内核电压。 这个电压监视器应该被配置成过压和欠压阀值与目标器件所支持的电压范围相匹配（特定器件数据表对此进行了注释）。 错误响应、诊断的可测试性、以及任一所需的软件要求由系统集成人员所选择的外部电压监视器来定义。

5.1.3 注释

- 器件可由用于组合在系统印刷电路板 (PCB) 上的多个电源轨来执行。 为了电源诊断的正确运行，建议在每一个成组的电源轨安排一个电压监视器。
- 外部电压监视器的共模故障分析也许对于在电压生成和监视电路中确定从属关系有所帮助。

5.2 时钟

Hercules TMS470M 器件系列产品主要为同步逻辑器件并且同样要求用于正确运行的时钟信号。 时钟管理逻辑电路包括时钟源、时钟生成逻辑电路，此逻辑电路包括锁相环路 (PLL) 、时钟分配器、和时钟分配逻辑电路。 这些被用于设计时钟管理逻辑电路的寄存器位于系统模块内。

5.2.1 低功耗振荡器时钟检测器 (LPOCLKDET)

低功耗振荡器时钟检测器 (LPOCLKDET) 是一个可被用于检测主时钟振荡器故障的安全诊断。 LPOCLKDET 采用嵌入式高频、低功耗振荡器 (HF LPO)。 时钟检测电路工作方式为检验一个其它时钟上升沿之间的某一个时钟（振荡器或者 HF LPO）上的上升沿。 结果就是除了标记不正确、频率重复，电路也会由于瞬态情况发生故障。 时钟检测窗口的低端会在至少 12 个 HF LPO 周期内忽略一个瞬态低相位。 请注意，这个瞬态响应的过滤不会改变输入频率范围。

加电复位状态期间，LPOCLKDET 电路默认被启用。 此诊断可通过软件禁用。 强烈建议使用 LPOCLKDET。

5.2.2 PLL 差异检测

PLL 逻辑电路包括一个能够检测一个 PLL 输出时钟差异的嵌入式诊断。 差异是由基准时钟和反馈时钟间的相位锁定损失造成。 错误响应和指示取决于系统模块内的 PLL 控制寄存器的设计。 当检测到 PLL 差异时，一个 ESM 错误指示可被生成或者被屏蔽。 此外，万一检测到 PLL 差异错误，则有可能生成一个内部复位或者从振荡器时钟返回运行状态。 要获得更多与设计这个诊断相关的信息，请参阅特定器件技术参考手册。

只要 PLL 被启用，PLL 差异检测诊断被激活并锁定在一个目标频率上。 此诊断不能由软件禁用，但是错误指示和错误响应可由软件修改。 强烈建议使用 PLL 差异检测诊断。

5.2.3 外部时钟输出监控 (ECLK)

Hercules TMS470M 平台提供将经选择的内部时钟信号输出用作外部监控的功能。 通过编辑系统模块内的寄存器，可由软件对此特性进行配置。 要确定所执行的外部时钟输出的数量和与可被输出的内部时钟相映射的寄存器，请参阅特定器件数据表。

默认情况下，ECLK 输出上内部时钟的输出并不启用而必须由软件启用。 可通过软件将这个诊断禁用并对其进行配置。 可选择将 ECLK 特性用于对内部时钟的外部监控。

5.2.4 内部安全装置

Hercules TMS470M 平台支持一个在实时中断 (RTI) 模块中实现的内部数字安全装置。 对于此内部安全装置的编程细节，请见特定器件技术参考手册。

DWD 是一个传统的单阀值安全装置。 用户为安全装置设定一个超时值并且必须在超时计数器终止前提供一个到安全装置的预先确定的“第一”响应。 超时计数器的终止或者一个不正确的“第一”响应会触发一个错误响应。 在检测到一个故障时，DWD 能够发布一个内部（热）系统复位或者一个 CPU 非屏蔽中断。 复位后，DWD 不启用。 一旦由软件启用，除了系统复位或者加电复位，DWD 不能被禁用。 DWD 功能的使用是可选的。

5.2.5 外部安全装置

当使用一个外部安全装置时，由于安全装置能够采用与被监控的系统分离的时钟、复位、和功率，有可能使用 MCU 时钟系统来减少共模故障。 错误响应、诊断的可测试性、以及任一所需的软件要求由系统集成人员所选择的外部安全装置来定义。 Hercules TMS470M 平台强烈建议使用一个外部安全装置而非内部提供的安全装置。

5.2.6 配置寄存器的定期回读

配置寄存器的定期回读能够为无意写入或者这些寄存器的混乱提供一个诊断。 错误响应、诊断的可测试性、以及任一所需的软件要求由系统集成人员所选择的软件来定义。 推荐使用配置寄存器的回读机制。

5.2.7 写入配置的软件回读

为了在系统模块中确保内存映射控制寄存器的正确配置，强烈建议软件执行一个测试来确认所有控制寄存器写入的正确运行。 为了支持这个软件测试，强烈建议将系统模块内存空间配置为一个使用 Cortex-M3 内存保护单元的严格排序的、不可缓冲的内存区域。 这一配置在回读被启动之前确保寄存器写入完成。

5.2.8 注释

- 可以通过使用一个 TI 为 Hercules TMS470M 系列开发的系统基础芯片来简化对系统级上外部安全装置功能的管理。
- 用户能够通过编辑 HF LDO 中的调整值来改进 LPOCLKDET 诊断的精度。 这将要求客户在制造测试期间通过与一个经校准的时钟源进行比较来确定 LPO 调整值。
- 有很多安全装置工具可被用来提供时钟和 CPU 诊断。 总的来说，由于能够减少共模故障，TI 建议使用一个外部安全装置而非内部安全装置。
- 在 ECLK 引脚上驱动一个高频时钟输出有可能会产生电磁干扰 (EMI) 。

5.3 复位

Hercules TMS470M 器件系列产品需要一个外部冷启动复位和加电复位 (nPORRST) 来将所有异步和同步逻辑电路置于一个已知状态。 作为启动过程的一部分，加电复位会生成一个内部热启动 (nRST) 信号来将大多数数字逻辑电路复位。 nRST 信号在器件级上作为 I/O 引脚提供；当被内部置为有效时，此信号将接通并可由外部驱动来生成一个热复位。 有关复位功能的更多信息，请见特定器件数据表。

5.3.1 热复位的外部监控 (nRST)

nRST 热复位信号被执行为一个 I/O。可使用一个外部监控器来检测对内部热复位控制信号状态的预期的或者意外改变。 错误响应、诊断的可测试性、以及任一所需的软件要求由系统集成人员所选择的外部监控器来定义。 这一特性的使用是可选的。

5.3.2 最后一次复位原因的软件检查

此系统模块提供了一个状态寄存器 (SYSESR)，此寄存器锁存大多数近期复位事件的原因。 一个检查这个寄存器的状态以确定最近一次复位事件原因的启动软件通常由软件开发人员执行。 这些信息可被软件用来管理故障恢复。 强烈建议使用 SYSESR 来检查最近一次复位的原因。

5.3.3 软件热复位生成

此系统模块为软件提供生成一个内部热复位 (nRST) 的功能。 这通过在 SYSECR 控制寄存器中写入适当的控制位来完成。 软件可以利用这一特性来尝试故障恢复。 软件热复位的使用是可选的。

5.3.4 nRST 和 nPORRST 上的毛刺脉冲过滤

毛刺脉冲滤波器在器件的冷复位和热复位引脚上生效。 这些构造过滤出了输入复位引脚上的噪声和瞬态信号峰值以减少复位电路的意外激活。 毛刺脉冲滤波器持续运行并且它们的运行方式不能由软件改变。 毛刺脉冲滤波器的使用是强制的。

5.3.5 影子寄存器

在器件上使用一个二级冷复位和热复位机制可允许影子寄存器的执行。 影子寄存器只在加电复位时被复位。这些寄存器可被用于存储器件状态或者其它关键信息，这些信息在系统状态被热复位改变之后仍然保持。 此系统模块包括影子寄存器，通过软件，此寄存器可被用于支持故障恢复。 强烈建议启动软件使用影子寄存器状态信息。

5.3.6 外部安全装置

一个外部安全装置可提供二级诊断。 要获得此类诊断的更多信息，请见 外部安全装置。

5.3.7 配置寄存器的定期回读

配置寄存器的定期回读能够为无意写入或者这些寄存器的混乱提供一个诊断。 错误响应、诊断的可测试性、以及任一所需的软件要求由系统集成人员所选择的软件来定义。 推荐使用配置寄存器的回读机制。

5.3.8 写入配置的软件回读

为了在系统模块中确保内存映射复位控制寄存器的正确配置，强烈建议软件执行一个测试来确认所有控制寄存器写入的正确运行。 为了支持这个软件测试，强烈建议将系统模块内存空间配置为一个使用 Cortex-M3 内存保护单元的严格排序的、不可缓冲的内存区域。 这一配置在回读被启动之前确保寄存器写入完成。

5.3.9 注释

- 可以通过使用一个 TI 为 TMS470M 系列开发的系统基础芯片来简化对系统级上复位的管理。
- 由于受监控的复位信号与内部安全装置相互作用，内部安全装置不是一个用于复位诊断的可行选项。

5.4 系统模块

系统控制模块包含到接口时钟、复位、和其它系统相关控制和状态逻辑电路的内存映射寄存器。 此系统控制模块也负责生成系统复位的同步并传递系统热复位 nRST。

5.4.1 优先模式访问和多位使能密钥

系统模块设计包括一些特性以支持意外控制寄存器编程避免。 这些特性包括限制写入命令以优先处理总线主控事务处理和执行用于关键控制的多位密钥。 此多位密钥对于意外激活避免特别有效。 要获得更多寄存器安全机制和错误响应方面的信息，请见特定器件技术参考手册。

这个安全机制的运行是连续的并且不用由软件变更。 可通过生成软件事务且检查器件响应来测试这个机制。 这个安全机制的使用是强制的。

5.4.2 写入配置的软件回读

为了在系统模块中确保内存映射控制寄存器的正确配置，强烈建议软件执行一个测试来确认所有控制寄存器写入的正确运行。 为了支持这个软件测试，强烈建议将系统模块内存空间配置为一个使用 Cortex-M3 内存保护单元的严格排序的、不可缓冲的内存区域。 这一配置在回读被启动之前确保寄存器写入完成。

5.4.3 配置寄存器的定期回读

配置寄存器的定期回读能够为无意写入或者这些寄存器的混乱提供一个诊断。 错误响应、诊断的可测试性、以及任一所需的软件要求由系统集成人员所选择的软件来定义。 推荐使用配置寄存器的回读机制。

5.4.4 注释

- 根据目标标准，用户能够选择在系统模块中执行一个针对静态配置寄存器的定期软件测试。 这个测试能够提供一个针对由软件错误引起的中断的附加诊断覆盖。
- 检查时钟和复位部分，这是因为这些特性由系统模块严密控制。

5.5 错误信令模块 (ESM)

ESM 提供板载硬件诊断错误的统一集合和优先级排序。 有关详细信息，请分别参阅 错误管理

5.5.1 配置寄存器的定期回读

配置寄存器的定期回读能够为无意写入或者这些寄存器的混乱提供一个诊断。 错误响应、诊断的可测试性、以及任一所需的软件要求由系统集成人员所选择的软件来定义。 推荐使用配置寄存器的回读机制。

5.5.2 错误路径报告的软件测试

一个软件测试可被用于注入诊断错误并检验报告的正确性。 这样一个测试可在启动时执行，或者定期执行。 必要的软件需求由系统集成人员执行的软件定义。 强烈建议使用一个错误路径报告的引导时间软件测试。 建议使用一个错误路径报告定期软件测试。

5.5.3 影子寄存器

在器件上使用一个二级冷复位和热复位机制可允许影子寄存器的执行。 影子寄存器只由加电复位来复位。 这些寄存器可被用于存储器件状态或者其它关键信息，这些信息在系统状态被热复位改变之后仍然保持。 错误信令模块包括影子寄存器，此寄存器可被用于通过软件来支持故障恢复。 强烈建议由启动软件使用影子寄存器状态信息。

5.5.4 写入配置的软件回读

为了在 ESM 中确保内存映射控制寄存器的正确配置，强烈建议软件执行一个测试来确认所有控制寄存器写入的正确运行。 为了支持这个软件测试，强烈建议将 ESM 内存空间配置为一个使用 Cortex-M3 内存保护单元 的严格排序的、不可缓冲的内存区域。 这一配置在回读被启动之前确保寄存器写入完成。

5.5.5 注释

- ESM 错误路径的软件测试可与硬件诊断的引导时间延迟测试组合在一起以减少引导时间。

5.6 CPU 子系统

Hercules TMS470M 产品系列依赖 ARM Cortex-M3 CPU 来提供通用处理。

5.6.1 CPU 逻辑内置自检 (LBIST) 自检控制器 (STC)

Hercules TMS470M 系列架构支持硬件逻辑 BIST (LBIST) 引擎自检控制器 (STC) 的使用。 这个逻辑电路用于在晶体管级锁步 CPU 上提供一个非常高的诊断覆盖。 为了快速执行高质量的制造测试，这个逻辑电路采用被插入器件的一样的测试设计 (DFT) 结构，但是使用的是一个内部测试引擎而非外部自动测试设备 (ATE)。 这个技术的效率已经被证明远高于基于软件的逻辑测试，对于一个最新 CPU 中使用的复杂逻辑结构更是如此。

LBIST 测试必须由软件触发。 用户可以选择运行所有测试，或者根据可被分配给 LBIST 诊断的执行时间只运行这些测试的一个子集。 这个时间分片测试特性使得 LBIST 能够被高效用作一个运行时间诊断，此诊断可以根据安全关键环路执行测试时间片，也可以作为一个在 MCU 初始化期间对 CPU 故障的综合性测试。

由于此测试的高效率，LBIST STC 的执行会在每个时钟周期内引起比正常软件执行期间高很多的晶体管开关电平。 STC 内执行的软件控制使得用户能够在测试期间减少 CPU 时钟。 这一特性使用户能够在流耗更高的快速执行或者流耗较小的较慢速执行之间做出折中的选择。

测试时，LBIST 机制要求 CPU 从器件逻辑的剩余部分隔离。 在执行 LBIST 之前，还需执行一个完整环境保存。 当测试执行完成时，CPU 将被复位。 器件逻辑的其余部分将继续正常运行。 CPU 复位后，软件应该读取系统模块 SYSESR 来识别复位的原因并可随后恢复 CPU 环境。

LBIST 逻辑包括对诊断正常运行进行测试的功能。 由于对诊断的测试时间是确定的，一个能够检测故障的超时计数器也被包括在内以使测试能够在预计的时间内完成。 此外，有可能强制生成一个输入错误来在系统级检验错误检测和错误响应的传播。 这个测试的执行步骤如下：

- 启用 STCSTSCR 寄存器中的 self_check_key 和 fault_ins 位。
- 启用 STC 测试间隔零并执行复位
- 一旦测试完成，应该将 STC 全局状态寄存器中的故障位置为 1。
- 禁用 STCSTSCR 寄存器中的 self_check_key 位和 fault_ins 位中的一个或者全部。
- 通过对 STCGCR 中的位 0 进行编程来重新启动自检，这将使自检重新启动。
- 一旦测试完成，应该将 STC 全局状态寄存器中的故障位置为 0。

强烈建议在启动时使用 LBIST 逻辑。 在正常执行期间定期执行 LBIST 逻辑电路是可选的。 LBIST 模块采用的循环校验提供了一个自检的固有电平（自动覆盖），可考虑将其应用在延迟故障诊断中。

5.6.2 CPU 内存保护单元 (MPU)

Cortex-M3 CPU 的 Hercules TMS470M 工具包括一个 MPU。 MPU 逻辑可被用于提供器件内存中软件任务的空间分离。 根据每一个任务的需求，操作系统控制 MPU 并改变 MPU 设置。 违反一个已设置的内存保护策略会导致一个 CPU 异常中断。 强烈建议使用 MPU。

MPU 也可被用于配置内存系统的内存排序策略。 默认情况下，所有外设访问是严格排序的-这意味着所有在序列中完成的事务被终止并且没有写入事务被缓冲。 如果需要，操作系统可以配置到器件的访问-这意味则写入被缓冲。 这样可以改进一个严格排序模型的性能，此改进是以损失一些确定性为代价的。 强烈建议系统模块和其它被认为具有关键配置的模块被设定为严格排序访问模型。

当执行 CPU 测试时，LBIST STC 诊断提供了一个 MPU 检验。 附加的基于软件的对 MPU 正常运行的测试和错误响应是可选的。

5.6.3 内部和外部安全装置

一个内部或者外部安全装置能够提供二次诊断。 对于这些诊断的更多信息，请见 内部安全装置或者 外部安全装置。

5.6.4 无效操作和指令陷阱

Cortex-M3 CPU 包括针对无效操作的诊断和可被用作安全机制的指令。 很多此类陷阱在复位后不启用且必须由软件配置。 强烈建议安装软件句柄以支持硬件无效操作处理和指令陷阱。 CPU 无效操作和指令陷阱的示例包括：

- 无效指令
- 优先级违反

5.6.5 写入配置的软件回读

为了确保 CPU 协处理器控制寄存器的正常配置，强烈建议软件执行一个测试来确定所有控制寄存器写入的正常运行。 CPU 控制寄存器并不是内存映射的且必须通过 CPU 协处理器读写命令进行访问。

5.6.6 注释

- 相对于诸如 TI LBIST STC 硬件机制，很多安全微控制器采用一个 CPU 功能性的基于软件的测试。 TI 不建议在诸如 Cortex-M3 的中等或者高级复杂程度的 CPU 上执行这些测试。 与等效的 LBIST STC 解决方案相比，基于软件的选项具有较高的内存成本、较低的检测能力、和更长的执行时间。

5.7 嵌入式闪存

Hercules TMS470M 上的嵌入式闪存存储器是非易失性片载内存，虽然也可进行数据访问，但是 此内存主要用于 CPU 指令访问。 对于闪存存储器的访问要经历多个 CPU 周期。 一个闪存包装程序逻辑提供多个管道式读缓冲来改进连续地址提取方面的 CPU 访问时间。

5.7.1 闪存 ECC

片载闪存存储器由位于闪存包装程序内的单纠错、双纠错 (SECDED) 误差校正代码 (ECC) 诊断支持。 它由一个 64b 数据接口连接至器件总线矩阵。 在这个 SECDED 机制中，一个 8 位代码字被用于当 ECC 数据在针对每一个 64 位数据有效载荷进行计算时存储该数据。 由闪存包装程序内的闪存 ECC 检测到的错误被报告给 ESM。 然后 ESM 向 Cortex-M3 CPU 提供错误通知。

用于闪存的 ECC 逻辑电路在复位时被禁用并且必须在闪存包装程序内进行配置。 强烈建议使用闪存 ECC。 ECC 模块采用的循环校验提供了一个自检的固有电平（自动覆盖），可考虑将其应用在延迟故障诊断中。

5.7.2 硬件冗余校验码 (CRC) 闪存内容检查

这个平台包括一个硬件循环冗余校验 (CRC)，此校验执行 ISO CRC-64 标准多项式。 通过计算一个针对所有闪存内容的 CRC 并将得出的值与一个之前生成的“极佳” CRC 相比较，此 CRC 模块能被用于测试闪存内容的完整性。 结果比较、故障指示、和故障响应由管理此测试的软件负责。 强烈建议在启动时执行一个闪存内容的 CRC 完整性检查。 建议在运行时间内定期执行 CRC 完整性检查。 硬件 CRC 模块所采用的循环校验提供了一个自我校验的固有电平（自动覆盖），可考虑将此电平应用于延迟故障诊断中。

5.7.3 闪存存储器阵列中的位复用

Hercules TMS470M 架构中执行的闪存模块执行一个位复用机制，这样被存取用来生成一个逻辑 (CPU) 字的位在物理上不相邻。 这一机制有助于减少会导致逻辑多位故障的物理多位故障的可能性；相反的它们多表现为多个单一位故障。 由于 SECDED 闪存 ECC 不能校正一个逻辑字中的单一位故障，这个机制提高了闪存 ECC 诊断的有效性。 位复用是此架构的强制特性并且不能由软件更改。

5.7.4 闪存扇区保护

通过闪存包装程序的软件配置可以防止扇区上的写入操作。 扇区保护寄存器，组扇区使能寄存器 (BSE)，包含一个针对闪存组中每一个扇区的位，这个位能够启用或者禁用对扇区的写入操作。 BSE 寄存器只能在特权模式下被写入，同时软件 PROTLIDIS 保护位被置为高电平。 这一机制能够减少闪存存储器意外编程的可能性。 强烈建议使用闪存扇区保护特性。

5.7.5 配置寄存器的定期回读

配置寄存器的定期回读能够为无意写入或者这些寄存器的混乱提供一个诊断。 错误响应、诊断的可测试性、以及任一所需的软件要求由系统集成人员所选择的软件来定义。 推荐使用配置寄存器的回读机制。

5.7.6 写入配置的软件回读

为了在闪存包装程序中确保内存映射控制寄存器的正确配置，强烈建议软件执行一个测试来确认所有控制寄存器写入的正确操作。 为了支持这个软件测试，强烈建议将闪存包装程序内存空间配置为一个使用 Cortex-M3 内存保护单元的严格排序的、不可缓冲的内存区域。 这一配置在回读被启动之前确保寄存器写入完成。

5.7.7 注释

- 通过执行一个闪存内容的 CRC 回读，同时在闪存上启用 ECC，就有可能并行执行闪存的两个诊断。
- 根据产品配置的不同，闪存模块也许会有唯一的电源引脚。 强烈建议如电源部分描述的那样在这些引脚上执行电压监控。
- 根据产品配置的不同，闪存模块也许会有唯一的测试信号引脚。 对于这些信号的正确板级管理，请见特定器件数据表。

5.8 闪存 EEPROM 仿真 (FEE)

器件上嵌入式闪存的第二组可被用作标准闪存，或者用来支持 EEPROM 仿真。 所有针对标准闪存的建议同样适用于 FEE 组。

5.9 初级嵌入式 SRAM

初级嵌入式 SRAM 是一个非易失性内存，此内存虽然也可用于指令存取，它主要用于 CPU 数据存取。 SRAM 的存取时间比闪存存储器快很多，这样在最大 CPU 频率时无需等待状态。

5.9.1 数据 ECC

片载 SRAM 由 SRAM 包装程序内嵌入的 SECDED ECC 诊断支持。 SRAM 包装程序由一个 64b 数据接口连接至总线矩阵。 在这个 SECDED 机制中，一个 8 位代码字被用于在 64 位数据有效载荷上进行计算的 ECC 数据。 由 SRAM 包装程序中 SRAM ECC 检测到的错误被报告给 ESM。 然后 ESM 向 Cortex-M3 CPU 提供错误通知。

用于 SRAM 的 ECC 逻辑电路在复位时被禁用并且必须在 SRAM 包装程序内进行配置。 强烈建议使用 SRAM ECC。 ECC 逻辑采用的循环校验提供了一个自检的固有电平（自动覆盖），可考虑将其应用在延迟故障诊断中。

5.9.2 可校正 ECC 参数描述

SRAM 包装程序包括一个计算检测到的可校正 ECC 错误数量的功能。 当错误数量超过一个用户设定的阀值时，一个错误事件信号被发送给 ESM。 这个机制被默认启用并且必须由 SRAM 包装程序中的软件启用。 推荐使用可校正 SRAM ECC 参数描述特性。

5.9.3 可编程内存 BIST (MBIST)

Hercules TMS470M 系列架构支持使用一个硬件内存 BIST (MBIST) 引擎。 这个逻辑电路用于在晶体管级上执行的 SRAM 上提供一个非常高的诊断覆盖。 MBIST 逻辑采用与 TI 针对制造测试所使用的一样的测试设计 (DFT) 逻辑电路和算法。 这一技术的效率以被证明远远高于 SRAM 的基于软件的测试，特别是对于具有复杂 CPU 的器件，在这样的器件中，寻址模式不会启用一个最优的基于软件的测试。

MBIST 测试必须由软件触发。 根据可被分配给 MBIST 诊断的执行时间，用户能够选择在一个 SRAM 或者一组 SRAM 上运行 MBIST。 MBIST 测试会破坏内存中的内容，正因如此，此测试通常只在 MCU 初始化时运行 然而，当 CPU 可用时，用户可在任一时间启动这些测试。

由于此测试的高效率，MBIST 的执行会在每个时钟周期内引起比正常软件执行期间高很多的晶体管开关电平。 如果在运行期间需要较低的电流，MBIST 内存测试可由软件连续运行，而不是并行运行。

TI 已知的最有效 SRAM 测试要求在一个完全物理内存模块上进行测试并且会破坏之前的存储器内容。 如果要在运行期间执行 MBIST，建议在测试执行前将数据从将要测试的 SRAM 中复制到一个未经测试的内存中并在测试完成时恢复此数据。 当测试执行完成时，SRAM 可被用于正常运行。 SRAM 测试期间，器件逻辑电路的其余部分继续正常运行。 MBIST 检测到的任何故障会导致一个在 MBIST 状态寄存中标示出的错误。

强烈建议在器件初始化时使用 MBIST 逻辑。 在正常执行期间定期执行 MBIST 逻辑是可选的。 MBIST 逻辑采用的循环校验提供了一个自检的固有电平（自动覆盖），可考虑将其应用在延迟故障诊断中。

5.9.4 SRAM 位复用

Hercules TMS470M 架构中执行的 SRAM 执行一个位复用机制，这样的话，被存取用来生成一个逻辑 (CPU) 字的位在物理上不相邻。 这一机制有助于减少会导致逻辑多位故障的物理多位故障的可能性；相反的它们多表现为多个单一位故障。 由于 SECDED SRAM ECC 能够校正一个逻辑字中的单一位故障，这个机制提高了 SRAM ECC 诊断的有效性。 位复用是此架构的强制特性并且不能由软件更改。

5.9.5 SRAM 硬件 CRC-64

这个平台包括一个硬件 CRC，此校验执行 ISO CRC-64 标准多项式。 通过计算一个针对所有静态内容的 CRC 并将得出的值与一个之前生成的“极佳” CRC 相比较，此 CRC 模块能被用于测试静态内容的完整性。 结果比较、故障指示、和故障响应由管理此测试的软件负责。 由于大多数静态值被存储在闪存中，在 SRAM 的静态内容上执行一个 CRC 是可选的。 CRC 逻辑采用的循环校验提供了一个自检的固有电平（自动覆盖），可考虑将其应用在延迟故障诊断中。

5.9.6 配置寄存器的定期回读

配置寄存器的定期回读能够为无意写入或者这些寄存器的混乱提供一个诊断。 错误响应、诊断的可测试性、以及任一所需的软件要求由系统集成人员所选择的软件来定义。 推荐使用配置寄存器的回读机制。

5.9.7 写入配置的软件回读

为了在 SRAM 包装程序中确保内存映射控制寄存器的正确配置，强烈建议软件执行一个测试来确认所有控制寄存器写入的正确操作。 为了支持这个软件测试，强烈建议将 SRAM 包装程序内存空间配置为一个使用 Cortex-M3 内存保护单元的严格排序的、不可缓冲的内存区域。 这一配置在回读被启动之前确保寄存器写入完成。

5.9.8 注释

- 通过执行一个 SRAM 内容的 CRC 回读，同时在 SRAM 上启用 ECC，就有可能并行执行 SRAM 的两个诊断。
- 根据产品配置的不同，SRAM 模块也许会有唯一的电源引脚。 强烈建议如电源部分描述的那样在这些引脚上执行电压监控。
- 冗余地址解码不提供硬件容错。 这样的话，按照某些安全标准中冗余的定义，不认为此逻辑电路是完全冗余的。

5.10 互连子系统

此互连子系统提供 CPU 总线主控和闪存，SRAM，和外设总线受控间的数据通路。 这个子系统为总线事务处理提供仲裁、优先级排序、路由、和解码功能。

5.10.1 错误捕捉

这个互连子系统包括一定数量的机制来检测和捕捉错误。 如果一个总线事务处理没有被解码为一个有效目标，诊断中的地址解码器使用一个总线错误对初始方进行响应。 逻辑电路也可检测特定事务处理的超时并且使用一个总线错误对事务处理初始方进行响应。

互连错误捕捉功能性默认被启用且不能被软件禁用。 这个安全机制的使用是强制的。 通过插入无效总线事务处理，可由软件对这些特性进行测试。

5.10.2 外设中央资源 (PCR) 访问管理

外设中央资源 (PCR) 提供两个能够限制到外设访问的安全机制。 根据 PCR 中的外设芯片选择，外设可被时钟选通。 这可被用于禁用未使用的特性，这样它们就不会干扰激活的安全功能。 此外，可对每一个外设芯片选择进行编程以限制基于事务处理优先级的访问。 这一特性可被用于将对于全部外设访问只限于特许操作系统代码。

复位后，这些安全机制被禁用。 软件必须配置且启用这些机制。 强烈建议使用这些机制。

5.10.3 内部/外部安全装置

一个内部或者外部安全装置可以提供一个事务的二级标示，此事务由于一个互连问题已经超时。 对于这些诊断的更多信息，请见 内部安全装置或者 外部安全装置。

5.10.4 信息冗余技术

信息冗余技术可由软件应用为一个互连上的附加运行时间诊断。 可应用很多技术，例如已写入值的回读和与结果相比较的同一目标数据的多次读取。 错误响应、诊断的可测试性、以及任一所需的软件要求由系统集成人员所选择的软件来定义。 建议在互连事务处理中使用信息冗余技术。

5.10.5 配置寄存器的定期回读

配置寄存器的定期回读能够为无意写入或者这些寄存器的混乱提供一个诊断。 错误响应、诊断的可测试性、以及任一所需的软件要求由系统集成人员所选择的软件来定义。 推荐使用配置寄存器的回读机制。

5.10.6 基本功能性的软件测试

一个软件测试可被用于注入诊断错误并检验适当的错误响应。 这样一个测试可在启动时执行，或者定期执行。 必要的软件需求由系统集成人员执行的软件定义。 强烈建议使用基本功能性的引导时间软件测试。 建议使用一个基本功能性报告定期软件测试。

5.10.7 写入配置的软件回读

为了在 PCR 中确保内存映射控制寄存器的正确配置，强烈建议软件执行一个测试来确认所有控制寄存器写入的正确操作。 为了支持这个软件测试，强烈建议将 PCR 内存空间配置为一个使用 Cortex-M3 内存保护单元的严格排序的、不可缓冲的内存区域。 这一配置在回读被启动之前确保寄存器写入完成。

5.10.8 注释

- 在一个联网外设上执行端到端通信安全机制在 L2 和 L3 互连上提供了一个信息冗余诊断的间接形式。
- L2 L3 互连子系统中的唯一一个具有内存映射寄存器的模块为 PCR。

5.11 M3 矢量中断模块 (M3VIM)

矢量中断模块 (M3VIM) 被用于将外设中断连接至 Cortex-M3 CPU 的 NVIC 接口。 M3VIM 提供可编程中断优先级、屏蔽、和睡眠模式唤醒功能。 M3VIM 包括一个本地 SRAM，此 SRAM 被用于保持每个通道的中断句柄的地址。

5.11.1 M3VIM 运行的定期软件测试

依照 IEC 61508 中的指南，一个用于检测连续中断、无中断、和交叉中断的软件测试可以被实现。 这样的测试可包括软件强制中断来检查 VIM 和 CPU 响应，或者来自 RTI 模块专门用于 VIM 测试目的的定期中断。 错误响应、诊断的可测试性、以及任一所需的软件要求由系统集成人员所选择的软件来定义。 强烈建议使用对 VIM 运行的定期软件测试。

5.11.2 配置寄存器的定期回读

配置寄存器的定期回读能够为无意写入或者这些寄存器的混乱提供一个诊断。 错误响应、诊断的可测试性、以及任一所需的软件要求由系统集成人员所选择的软件来定义。 推荐使用配置寄存器的回读机制。

5.11.3 写入配置的软件回读

为了在 M3VIM 中确保内存映射控制寄存器的正确配置，强烈建议软件执行一个测试来确认所有控制寄存器写入的正确操作。 为了支持这个软件测试，强烈建议将 VIM 内存空间配置为一个使用 Cortex-M3 内存保护单元的严格排序的、不可缓冲的内存区域。 这一配置在回读被启动之前确保寄存器写入完成。

5.11.4 内部和外部安全装置

一个内部或者外部安全装置可以提供一个事务的二级标示，此事务由于一个互连问题已经超时。 对于这些诊断的更多信息，请见 内部安全装置 外部安全装置。

5.12 实时中断 (RTI)

实时中断 (RTI) 模块提供针对器件的操作系统定时器。 OS 定时器被用于生成内部事件触发或者所需的中断来提供安全功能的定期运行。

5.12.1 使用第二个计数器作为诊断

RTI 模式包含至少两个上数计数器，此计数器可被用于提供操作系统时间记号。 当一个上数计数器被用作操作系统时基时，可使用第二个计数器作为第一个技术器的诊断，即通过软件对两个定时器中的计数器的值进行定期检查。 错误响应、诊断的可测试性、以及任一所需的软件要求由系统集成人员所选择的软件来定义。 建议使用一个第二计数器来诊断 RTI 内的故障。

5.12.2 内部/外部安全装置

一个内部或者外部安全装置可以提供 RTI 模块内故障的标示。 对于这些诊断的更多信息，请见 内部安全装置 外部安全装置。

5.12.3 配置寄存器的定期回读

配置寄存器的定期回读能够为无意写入或者这些寄存器的混乱提供一个诊断。 错误响应、诊断的可测试性、以及任一所需的软件要求由系统集成人员所选择的软件来定义。 推荐使用配置寄存器的回读机制。

5.12.4 注释

- 当使用一个计数器作为操作系统时基计数器时，一个时钟源、比例因数等的多种配置可被用于减少共模故障的可能性。

5.13 高端定时器 (HET)

HET 模块是一个具有输入/输出功能的可编程定时器。 HET 被执行为一个带有指令集（专门用于定时操作）的简单 RISC 处理器。 复杂输入可被捕捉并由 HET 进行预处理，随后由 CPU 处理。 输出生成通常为脉宽调制 (PWM)，但是也可以为简单通用输入/输出 (GIO) 类型信号。

5.13.1 使用 I/O 回路的功能的软件测试

一个软件测试可被用于注入诊断错误并检验适当的错误响应。 这样一个测试可在启动时执行，或者定期执行。 必要的软件需求由系统集成人员执行的软件定义。 强烈建议使用基本功能性的引导时间软件测试。 使用一个基本功能性报告的定期软件测试是可选的。

HET 工具支持针对 I/O 的数字和模拟回路功能。 数字回路测试到模块边界的信号路径。 模拟回路测试从模块至 I/O 单元的信号路径，此时输出驱动器被禁用。 为了获得最佳的测试结果，对于 HET 功能性的任何测试应该包括 I/O 回路。

5.13.2 HET SRAM 奇偶校验

HET SRAM 包括一个奇偶校验诊断，此诊断能够检测内存中的单一位错误。 当检测到一个奇偶错误时，ESM 被告知此错误。 这一特性在复位后被禁用。 软件必须配置和启用这个特性。 强烈建议使用 HET SRAM 奇偶校验特性。

5.13.3 HET 和 SRAM MBIST

HET SRAM 可使用 MBIST 内存测试进行测试。 强烈建议在复位后在 HET SRAM 上执行 MBIST 测试。 要获得这一诊断的更多信息，请见 PBIST。

5.13.4 HET SRAM 位复用

HET SRAM 由一个内存设计实现，这样逻辑上邻近的位的物理位置不相邻。 这个安全机制的使用是强制的。 对于这一安全机制的更多细节，请见 SRAM 位复用。

5.13.5 HET SRAM CRC-64 测试

HET SRAM 内容可使用硬件 CRC-64 诊断进行定期测试。 要获得这一诊断的更多信息，请见 SRAM 硬件 CRC-64。

5.13.6 配置寄存器的定期回读

配置寄存器的定期回读能够为无意写入或者这些寄存器的混乱提供一个诊断。 错误响应、诊断的可测试性、以及任一所需的软件要求由系统集成人员所选择的软件来定义。 推荐使用配置寄存器的回读机制。

5.14 多缓冲模数转换器 (MibADC)

MibADC 模块用于将模拟输入转换为数字值。 结果被存储在内部 MibADC SRAM 缓冲器内以用于之后的 CPU 传递。

5.14.1 输入自检

Hercules TMS470M MiADC 模块执行一个输入自检引擎，此引擎能够检测到 ADREFLO，ADREFHI 的短路或者开路输入。 软件必须配置、启用和评估这个诊断的结果。 错误响应、诊断的可测试性、以及任一所需的软件要求由系统集成人员所选择的软件来定义。 强烈建议使用输入自检机制。

5.14.2 转换器校准

Hercules TMS470M MiADC 模块执行校准逻辑，此逻辑通常用于提升转换器准确性。 这个逻辑电路也可被用作一个安全机制。 来自校准逻辑电路的对已知基准值转换的软件比较能够提供一个对转换器功能性的诊断。 校准例程的重复执行可被用于检测应用期间的漂移。

软件必须配置、启用和评估这个诊断的结果。 错误响应、诊断的可测试性、以及任一所需的软件要求由系统集成人员所选择的软件来定义。 强烈建议在启动时使用转换器校准机制。 定期使用转换器校准机制是可选的。

5.14.3 信息冗余技术

信息冗余技术可由软件应用为一个 ADC 转换上的附加运行时间诊断。 有很多技术可被应用，例如在同一个转换器上使用多重通道或者按照比较结果在同一通道上进行的多重转换。

对于已被转换值的过滤和处于预计范围内的真实性检验也可提升诊断的覆盖。

错误响应、诊断的可测试性、以及任一所需的软件要求由系统集成人员所选择的软件来定义。 强烈建议在 ADC 转换上使用信息冗余技术。

5.14.4 ADC SRAM 奇偶校验

MibADC SRAM 包括一个奇偶校验诊断，此诊断能够检测内存中的单一位错误。 当检测到一个奇偶错误时，ESM 被告知此错误。 这一特性在复位后被禁用。 软件必须配置和启用这个特性。 强烈建议使用 MibADC SRAM 奇偶校验特性。

5.14.5 ADC SRAM MBIST

MibADC SRAM 可使用 MBIST 内存 BIST 引擎进行测试。 强烈建议复位后在 MibADC SRAM 上执行 MBIST 测试。 要获得这一诊断的更多信息，请见 PBIST。

5.14.6 ADC SRAM 位复用

MibADC SRAM 由一个内存设计实现，这样逻辑上邻近的位的物理位置不相邻。 这个安全机制的使用是强制的。 对于这一安全机制的更多细节，请见 SRAM 位复用。

5.14.7 ADC SRAM CRC-64 测试

MibADC SRAM 内容可使用硬件 CRC-64 诊断进行定期测试。 由于 MibADC SRAM 内容往往动态性更强，因此这个诊断的使用是可选的。 要获得这一诊断的更多信息，请见 SRAM 硬件 CRC-64。

5.14.8 配置寄存器的定期回读

配置寄存器的定期回读能够为无意写入或者这些寄存器的混乱提供一个诊断。 错误响应、诊断的可测试性、以及任一所需的软件要求由系统集成人员所选择的软件来定义。 推荐使用配置寄存器的回读机制。

5.14.9 注释

- 应该如 电源中注释的那样对 ADC 模块电压进行监视。

5.15 多缓冲串行外设接口 (MIBSPI)

MibSPI 模块提供与 MibSPI 协议兼容的串行 I/O。 MibSPI 通信通常用于到智能传感器和传动器，串行存储器、和诸如安全器件的外部逻辑电路的通信。 MibSPI 模块包含内部 SRAM 缓冲器。 如果不被用于 MibSPI 通信，MibSPI 模块的 I/O 可被用于通用 I/O。

5.15.1 使用 I/O 回路的功能的软件测试

一个软件测试可被用于注入诊断错误并检验适当的错误响应。 这样一个测试可在启动时执行，或者定期执行。 必要的软件需求由系统集成人员执行的软件定义。 强烈建议使用基本功能性的引导时间软件测试。 使用一个基本功能性报告的定期软件测试是可选的。

MibSPI 工具支持针对 I/O 的数字和模拟回路功能。 数字回路测试到模块边界的信号路径。 模拟回路测试从模块至 I/O 单元的信号路径，此时输出驱动器被禁用。 为了获得最佳的测试结果，对于 MibSPI 功能性的任何测试应该包括 I/O 回路。

5.15.2 消息奇偶校验

Hercules TMS470M MIBSPI 支持在由硬件发出的每一个 MIBSPI 消息数据的有效载荷中插入一个奇偶位。硬件也支持进入的消息奇偶校验的评估。 检测到的错误生成一个到 CPU 的中断。 强烈建议使用这一特性。

5.15.3 信息冗余技术

信息冗余技术可由软件应用为一个针对 MIBSPI 通信的附加运行时间诊断。 可应用很多技术，例如已写入值的回读和与结果相比较的同一目标数据的多次读取。 替代的冗余技术可通过在系统中执行多重通道来实现。错误响应、诊断的可测试性、以及任一所需的软件要求由系统集成人员所选择的软件来定义。 强烈建议在 MIBSPI 事务处理中使用信息冗余技术。

5.15.4 MIBSPI SRAM 奇偶校验

MIBSPI SRAM 包括一个奇偶校验诊断，此诊断能够检测内存中的单一位错误。 当检测到一个奇偶错误时，ESM 被告知此错误。 这一特性在复位后被禁用。 软件必须配置和启用这个特性。 强烈建议使用 MIBSPI SRAM 奇偶校验特性。

5.15.5 MIBSPI SRAM MBIST

MIBSPI SRAM 可使用 MBIST 内存 BIST 引擎进行测试。 强烈建议在复位后在 MIBSPI SRAM 上执行 MBIST 测试。 要获得这一诊断的更多信息，请见 PBIST。

5.15.6 MIBSPI SRAM 位复用

MIBSPI SRAM 由一个内存设计实现，这样逻辑上邻近的位的物理位置不相邻。 这个安全机制的使用是强制的。 对于这一安全机制的更多细节，请见 SRAM 位复用。

5.15.7 MIBSPI SRAM CRC-64 测试

MIBSPI SRAM 内容可使用硬件 CRC-64 诊断进行定期测试。 由于 MIBSPI SRAM 内容往往动态性更强，因此这个诊断的使用是可选的。 要获得这一诊断的更多信息，请见 SRAM 硬件 CRC-64。

5.15.8 配置寄存器的定期回读

配置寄存器的定期回读能够为无意写入或者这些寄存器的混乱提供一个诊断。 错误响应、诊断的可测试性、以及任一所需的软件要求由系统集成人员所选择的软件来定义。 推荐使用配置寄存器的回读机制。

5.15.9 注释

- 在标准 SPI 模式中也可使用 MIBSPI。

5.16 本地互连网络 (LIN)

LIN 模块提供与 LIN 协议兼容的串行 I/O。 LIN 是一个低吞吐量时间触发协议。 这个模块可被配置成 SCI 模式并被用作一个通用串行接口。 一个外部收发器被用于 LIN 通信。

5.16.1 使用 I/O 回路的功能的软件测试

一个软件测试可被用于注入诊断错误并检验适当的错误响应。 这样一个测试可在启动时执行，或者定期执行。 必要的软件需求由系统集成人员执行的软件定义。 强烈建议使用基本功能性的引导时间软件测试。 使用一个基本功能性报告的定期软件测试是可选的。

LIN 工具支持针对 I/O 的数字和模拟回路功能。 数字回路测试到模块边界的信号路径。 模拟回路测试从模块至 I/O 单元的信号路径，此时输出驱动器被禁用。 为了获得最佳的测试结果，对于 LIN 功能性的任何测试应该包括 I/O 回路。

5.16.2 包括端到端安全状态恢复的信息冗余技术

信息冗余技术可由软件应用为一个针对 LIN 通信的附加运行时间诊断。 可应用很多技术，例如已写入值的回读和与结果相比较的同一目标数据的多次读取。

为了提供对于 MCU 之外网络元件的诊断覆盖（线束、连接器、收发器），必须采用端到端安全状态恢复机制。 这些机制也可提供 MCU 内部的诊断覆盖。 可采用多种不同的机制，例如附加消息校验和、冗余传输、传输中的时间多样性等等。 大多数通用校验和被添加到一个传输的有效载荷部分以确保传输的正确性。除了任何协议级奇偶和校验和，这些校验和也被采用。 由于校验和由通信任一端的软件生成和评估，整个通信路径是安全的，实现端到端安全状态恢复。

错误响应、诊断的可测试性、以及任何必须的软件要求由系统集成人员定义。 强烈建议使用这一机制。

5.16.3 配置寄存器的定期回读

配置寄存器的定期回读能够为无意写入或者这些寄存器的混乱提供一个诊断。 错误响应、诊断的可测试性、以及任一所需的软件要求由系统集成人员所执行的软件来定义。 推荐使用配置寄存器的回读机制。

5.17 控制器局域网络 (DCAN)

DCAN 接口提供与基于事件的触发互连的中等吞吐量，与 CAN 协议兼容。 DCAN 模块要求一个外部收发器以在 CAN 网络上运转。

5.17.1 使用 I/O 回路的功能的软件测试

一个软件测试可被用于注入诊断错误并检验适当的错误响应。 这样一个测试可在启动时执行，或者定期执行。 必要的软件需求由系统集成人员执行的软件定义。 强烈建议使用基本功能性的引导时间软件测试。 使用一个基本功能性报告的定期软件测试是可选的。

DCAN 工具支持针对 I/O 的数字和模拟回路功能。 数字回路测试到模块边界的信号路径。 模拟回路测试从模块至 I/O 单元的信号路径，此时输出驱动器被禁用。 为了获得最佳的测试结果，对于 DCAN 功能性的任何测试应该包括 I/O 回路。

5.17.2 包括端到端安全状态恢复的信息冗余技术

信息冗余技术可由软件应用为一个针对 CAN 通信的附加运行时间诊断。 可应用很多技术，例如已写入值的回读和与结果相比较的同一目标数据的多次读取。

为了提供对于 MCU 之外网络元件的诊断覆盖（线束、连接器、收发器），必须采用端到端安全状态恢复机制。 这些机制也可提供 MCU 内部的诊断覆盖。 可采用多种不同的机制，例如附加消息校验和、冗余传输、传输中的时间多样性等等。 大多数通用校验和被添加到一个传输的有效载荷部分以确保传输的正确性。 除了任何协议级奇偶和校验和，这些校验和也被采用。 由于校验和由通信任一端的软件生成和评估，整个通信路径是安全的，实现端到端安全状态恢复。

错误响应、诊断的可测试性、以及任何必须的软件要求由系统集成人员定义。 强烈建议使用这一机制。

5.17.3 DCAN SRAM 奇偶校验

DCAN SRAM 包括一个奇偶校验诊断，此诊断能够检测内存中的单一位错误。 当检测到一个奇偶错误时，ESM 被告知此错误。 这一特性在复位后被禁用。 软件必须配置和启用这个特性。 强烈建议使用 DCAN SRAM 奇偶校验特性。

5.17.4 DCAN SRAM MBIST

DCAN SRAM 可使用 MBIST 内存 BIST 引擎进行测试。 强烈建议在复位后在 DCAN SRAM 上执行 PBIST 测试。 要获得这一诊断的更多信息，请见 PBIST。

5.17.5 DCAN SRAM 位复用

DCAN SRAM 由一个内存设计实现，这样逻辑上邻近的位的物理位置不相邻。 这个安全机制的使用是强制的。 对于这一安全机制的更多细节，请见 SRAM 位复用。

5.17.6 DCAN SRAM CRC-64 测试

DCAN SRAM 内容可使用硬件 CRC-64 诊断进行定期测试。 由于 DCAN SRAM 内容往往动态性更强，因此这个诊断的使用是可选的。 要获得这一诊断的更多信息，请见 SRAM 硬件 CRC-64。

5.17.7 配置寄存器的定期回读

配置寄存器的定期回读能够为无意写入或者这些寄存器的混乱提供一个诊断。 错误响应、诊断的可测试性、以及任一所需的软件要求由系统集成人员所执行的软件来定义。 推荐使用配置寄存器的回读机制。

5.18 通用输入/输出 (GIO)

GIO 模块提供数字输入捕捉和数字输入/输出。 在这个块中没有处理功能。 GIO 通常用于静态的或者很少发生改变的输出，诸如收发器使能信号、报警光等。 GIO 也可被用于提供外部中断输入功能。

5.18.1 使用 I/O 检查的功能的软件测试

一个软件测试可被用于注入诊断错误并检验适当的错误响应。 这样一个测试可在启动时执行，或者定期执行。 必要的软件需求由系统集成人员执行的软件定义。 强烈建议使用基本功能性的引导时间软件测试。 使用一个基本功能性报告的定期软件测试是可选的。

使用 I/O 检查的功能的软件测试 然而它有可能支持使用正常功能性的 I/O 检查。 为了实现这一功能，软件生成输出并回读和检验输入寄存器中的同一个值。 这个工具的功能性与其它模块中的模拟回路相似。 为了获得最佳的测试结果，对于 GIO 功能性的任何测试应该包括 I/O 回路。

5.18.2 信息冗余技术

信息冗余技术可由软件应用为一个对 GIO 功能的附加运行时间诊断。 可采用很多技术，诸如多重输入和使用一个输入通道的输出回读。 如果不被用于主要功能，来自很多其它外设的信号可被用作 GIO。 为多通道工具使用一个 GIO 模块信号和一个非 GIO 模块信号能够减少共模故障的可能性。

错误响应、诊断的可测试性、以及任一所需的软件要求由系统集成人员所执行的软件来定义。 强烈建议在 GIO 功能上使用信息冗余技术。

5.18.3 配置寄存器的定期回读

配置寄存器的定期回读能够为无意写入或者这些寄存器的混乱提供一个诊断。 错误响应、诊断的可测试性、以及任一所需的软件要求由系统集成人员所执行的软件来定义。 推荐使用配置寄存器的回读机制。

5.18.4 注释

- 为了减少共模故障的可能性，用户应该考虑执行使用非邻近引脚的多重通道。

5.19 JTAG 调试和测试访问

Hercules TMS470M 平台支持在 IEEE 1149.1 JTAG 调试端口上实现调试和测试。 物理调试接口被内部连接至一个 TI 调试复用器逻辑电路 (ICEPICK)，此电路对到测试、调试、和校准逻辑电路的访问进行仲裁。 为了实现最简单的制造板测试，边界扫面被并行连接至 ICEPICK 以支持不含前导码扫描序列的用法。

5.19.1 JTAG 端口的硬件禁用

JTAG 调试端口能够被物理禁用以防止已部署系统中的 JTAG 访问。 虽然其它替代系统配置也是可行的，但这个建议推荐的系统配置是为了保持测试时钟 (TCK) 到接地并保持测试模式选择 (TMS) 为高电平。 建议采用 JTAG 端口的硬件禁用。

5.19.2 注释

- 一个安全装置可提供意外激活的标示。

5.20 Cortex-M3 中央处理单元 (CPU) 调试

Hercules TMS470M 平台支持与 ARM CoreSight 标准兼容的 CPU 调试。 每一个 CoreSight 元件可通过一个内存映射调试总线进行访问，此总线可由 CPU 或者 JTAG 端口进行访问。 CPU 调试逻辑电路包含一个独立的调试总线主控 (AHB-AP)，CPU 内的调试单元。 不建议在安全操作和安全机制正在禁用这个逻辑电路期间使用这些模块。

5.20.1 禁用 JTAG 端口以限制功能访问

大多数调试和跟踪活动由一个外部调试工具启动，此调试工具使用 JTAG 端口将命令写入器件。 如 JTAG 调试/跟踪/校准/测试访问中所示，JTAG 端口可在生产硬件上被禁用。 强烈建议禁用 JTAG 端口以限制调试模块访问。

5.20.2 阻止到内存映射调试的访问

可通过一个内存映射调试总线对 CoreSight 调试外设进行访问。 对于这一区域的访问可通过使用基于内存保护的总线主控进行阻止。 要获得与内存保护相关的更多信息，请见 CPU 内存保护单元 (MPU)。 强烈建议阻止到内存映射调试组件的访问。

5.20.3 CoreSight 调试逻辑密钥使能

为了开启内存映射 CoreSight 调试组件的运行，有必要在每一个调试模块中的解锁寄存器中写入一个已定义的 32 位密钥。 这个调试锁保护为限制非所需激活提供了一个额外的保护机制。 强烈建议使用调试模块解锁密钥。

5.20.4 注释

- 一个安全装置可提供意外激活的标示。
- 并不是所有封装变量可包含跟踪功能

6 您安全开发中的下几个步骤

TI 对于您的安全开发并不仅仅限于这本安全文档。 客户可选择多种类型的支持方式，诸如：

- 随时在线访问包括安全文档和应用报告在内的 Hercules 文档：http://www.ti.com/hercules
- 使用 TI 互连社区（E2E 论坛）与 TI 专家和其它赫丘利斯开发人员探讨问题和关心的事项：http://www.ti.com/hercules-support
- Hercules TMS470M 维基网页提供对于很多常见问题的解答：http://www.ti.com/hercules-wiki

我们随时欢迎您对于安全手册的反馈和参与，并且可以通过点击本文档每页底部的反馈链接将您的意见在线提交给我们。

Appendix A 建议的安全特性用法总结

表 2提供了5 节中注释的安全概念建议的总结并按照器件分区进行组织。 每个建议都被指定了一个唯一的标识符以在需求管理中提供帮助。 对于每一个安全特性或者诊断，建议通过以下的简化形式进行注释：

- M --> 强制应用
- ++ --> 强烈推荐
- + --> 建议
- O --> 可选

此外，还提供了对于每一个器件分区的可能潜在的诊断方法和安全特性以及诊断组合列表。 对于每一个安全特性或者诊断的详细信息，请见5 节。

表 2. 安全特性和诊断的总结

器件分区	唯一标识符	安全特性或者诊断	特性建议	可能潜在诊断
电源 + VREG	PWR1	VREG 嵌入式内核电压监控器	M	外部电压监视器
	PWR2	外部电压监视器	++	内核电压监控器
时钟	CLK1	LPOCLKDET	++	ECLK，安全装置
	CLK2	PLL 滑动检测器	++	ECLK，安全装置
	CLK3	通过 ECLK 的外部监控	O	LPOCLKDET，PLL 滑动检测器，安全装置
	CLK4A	内部安全装置 - DWD	+	外部安全装置，安全装置配置和错误响应的软件测试
	CLK4B	外部安全装置	++	内部安全装置，安全装置配置和错误响应的软件测试
	CLK5	静态时钟配置寄存器的定期软件回读	+	LBIST
	CLK6	已写入配置的软件回读	++	LBIST
复位	RST1	热复位的外部监控	O	安全装置
	RST2	最后复位的软件检查	++	LBIST
	RST3	软件热复位生成	O	LBIST
	RST4	复位引脚上的毛刺脉冲过滤	M	外部安全装置
	RST5	状态影子寄存器的使用	++	LBIST
	RST6	外部安全装置	++	外部安全装置配置和错误响应的软件测试
	RST7	静态配置寄存器的定期软件回读	+	LBIST
	RST8	已写入配置的软件回读	++	LBIST
系统控制	SYS1	优先模式访问和多位使能密钥	M	寄存器配置和错误响应的软件测试
	SYS2	已写入配置的软件回读	++	LBIST
	SYS3	静态配置寄存器的定期软件回读	+	LBIST
错误信令模块 (ESM)	ESM1	静态配置寄存器的定期软件回读	+	LBIST
	ESM2A	错误路径报告的引导时间软件测试	++	LBIST
	ESM2B	错误路径报告的定期软件测试	+	LBIST
	ESM3	状态影子寄存器的使用	++	LBIST
	ESM4	已写入配置的软件回读	++	LBIST
Cortex-M3 中央处理单元 (CPU)	CPU1A	LBIST STC 引导时间执行	++	LBIST 自动覆盖
	CPU1B	LBIST STC 的定期执行	+	LBIST 自动覆盖
	CPU2	MPU	++	LBIST
	CPU3A	内部安全装置 - DWD	+	外部安全装置，安全装置配置和错误响应的软件测试
	CPU3B	外部安全装置	++	内部安全装置，安全装置配置和错误响应的软件测试
	CPU4	无效操作和指令陷阱	++	LBIST
	CPU5	已写入配置的软件回读	++	LBIST

表 2. 安全特性和诊断的总结 (continued)

器件分区	唯一标识符	安全特性或者诊断	特性建议	可能潜在诊断
嵌入式闪存	FLA1	闪存数据 ECC	++	LBIST，ECC 自动覆盖
	FLA2A	闪存存储器内容的引导时间硬件 CRC 检查	++	CRC 自动覆盖
	FLA2B	闪存存储器内容的定期硬件 CRC 检查	+	CRC 自动覆盖
	FLA3	闪存阵列中的位复用	M	ECC，CRC 测试
	FLA4	闪存扇区保护	++	CRC 测试
	FLA5	静态配置寄存器的定期软件回读	+	LBIST
	FLA6	已写入配置的软件回读	++	LBIST
闪存仿真 EEPROM (FEE)	FEE1	闪存数据 ECC	++	LBIST，ECC 自动覆盖
	FEE2A	闪存存储器内容的引导时间硬件 CRC 检查	++	CRC 自动覆盖
	FEE2B	闪存存储器内容的定期硬件 CRC 检查	+	CRC 自动覆盖
	FEE3	闪存阵列中的位复用	M	ECC，CRC 测试
	FEE4	闪存扇区保护	++	CRC 测试
	FEE5	静态配置寄存器的定期软件回读	+	LBIST
	FEE6	已写入配置的软件回读	++	LBIST
初级嵌入式 SRAM	RAM1	数据 ECC	++	LBIST，ECC 自动覆盖，MBIST
	RAM2	可校正 ECC 参数描述	+	LBIST
	RAM3A	RAM 引导时间 MBIST 校验	++	MBIST 自动覆盖
	RAM3B	RAM 定期 MBIST 检查	O	MBIST 自动覆盖
	RAM4	SRAM 阵列中的位复用	M	ECC
	RAM5	SRAM 内容的定期硬件 CRC 检查	O	CRC 自动覆盖
	RAM6	静态配置寄存器的定期软件回读	+	CRC 自动覆盖
	RAM7	已写入配置的软件回读	++	LBIST
互连子系统	INC1	错误捕捉	M	基本功能性和错误响应的软件测试
	INC2	PCR 访问管理	++	基本功能性和错误响应的软件测试
	INC3A	内部安全装置 - DWD	O	外部安全装置，安全装置配置和错误响应的软件测试
	INC3B	外部安全装置	++	内部安全装置，安全装置配置和错误响应的软件测试
	INC4	信息冗余	+	
	INC5	静态配置寄存器的定期软件回读	+	LBIST
	INC6A	基本功能性的引导时间软件测试	++	LBIST
	INC6B	基本功能性的定期软件测试	+	LBIST
	INC7	已写入配置的软件回读	++	LBIST
M3 矢量中断模块 (VIM)	VIM1	VIM 功能性的定期软件检查	++	LBIST
	VIM2	静态配置寄存器的定期软件回读	+	LBIST
	VIM3	已写入配置的软件回读	++	LBIST
	VIM4A	内部安全装置 - DWD	O	外部安全装置，安全装置配置和错误响应的软件测试
	VIM4B	外部安全装置	++	内部安全装置，安全装置配置和错误响应的软件测试
实时中断 (RTI) 操作系统定时器	RTI1	使用第二个计数器作为诊断	+	LBIST
	RTI2	内部安全装置 - DWD	O	外部安全装置，安全装置配置和错误响应的软件测试
	RTI2B	外部安全装置	++	内部安全装置，安全装置配置和错误响应的软件测试
	RTI3	静态配置寄存器的定期软件回读	+	LBIST

表 2. 安全特性和诊断的总结 (continued)

器件分区	唯一标识符	安全特性或者诊断	特性建议	可能潜在诊断
高端 定时器 (HET)	HET1A	使用 I/O 回路的功能的引导时间软件测试	++	LBIST
	HET1B	使用 I/O 回路的功能的定期软件测试	O	LBIST
	HET2	HET SRAM 数据奇偶校验	++	MBIST
	HET3A	HET RAM 的引导时间 MBIST 检查	++	MBIST 自动覆盖
	HET3B	HET RAM 的定期 MBIST 检查	O	MBIST 自动覆盖
	HET4	HET RAM 阵列中的位复用	M	MBIST，奇偶校验
	HET5	NET SRAM 内容的定期硬件 CRC 检查	O	MBIST
	HET6	静态配置寄存器的定期软件回读	+	LBIST
多缓冲模拟 数字转换器 (MibADC)	ADC1	引导时间自检	++	LBIST
	ADC2A	引导时间转换器校准	++	LBIST
	ADC2B	定期转换器校准	O	LBIST
	ADC3	信息冗余技术	++	ADC 转换器校准、ADC 自检
	ADC4	MibADC SRAM 数据奇偶校验	++	MBIST
	ADC5A	MibADC RAM 的引导时间 MBIST 检查	++	MBIST 自动覆盖
	ADC5B	MibADC RAM 的定期 MBIST 检查	O	MBIST 自动覆盖
	ADC6	MibADC RAM 阵列中的位复用	M	MBIST，奇偶校验
	ADC7	MibADC SRAM 内容的定期硬件 CRC 检查	O	MBIST
	ADC8	静态配置寄存器的定期软件回读	+	LBIST
多缓冲串行 外设接口 (MibSPI)	MSP1A	使用 I/O 回路的功能的引导时间软件测试	++	LBIST
	MSP1B	使用 I/O 回路的功能的定期软件测试	O	LBIST
	MSP2	信息奇偶校验	++	LBIST
	MSP3	信息冗余技术	++	LBIST
	MSP4	MibSPI SRAM 数据奇偶校验	++	MBIST
	MSP5A	MibSPI RAM 的引导时间 MBIST 检查	++	MBIST 自动覆盖
	MSP5B	MibSPI RAM 的定期 MBIST 检查	O	MBIST 自动覆盖
	MSP6	MibSPI RAM 阵列中的位复用	M	MBIST，奇偶校验
	MSP7	MibSPI SRAM 内容的定期硬件 CRC 检查	O	MBIST
	MSP8	静态配置寄存器的定期软件回读	+	LBIST
本地 互连网络 (LIN)	LIN1A	使用 I/O 回路的功能的引导时间软件测试	++	LBIST
	LIN1B	使用 I/O 回路的功能的定期软件测试	O	LBIST
	LIN2	包含端到端安全状态恢复的信息冗余技术	++	LBIST
	LIN3	静态配置寄存器的定期软件回读	+	LBIST
控制器局域 网络 (DCAN)	CAN1A	使用 I/O 回路的功能的引导时间软件测试	++	LBIST
	CAN1B	使用 I/O 回路的功能的定期软件测试	O	LBIST
	CAN2	包含端到端安全状态恢复的信息冗余技术	++	LBIST
	CAN3	DCAN SRAM 数据奇偶校验	++	MBIST
	CAN4A	DCAN RAM 的引导时间 MBIST 检查	++	MBIST 自动覆盖
	CAN4B	DCAN RAM 的定期 MBIST 检查	O	MBIST 自动覆盖
	CAN5	DCAN RAM 阵列位复用	M	MBIST，奇偶校验
	CAN6	DCAN SRAM 内容的定期硬件 CRC 检查	O	MBIST
	CAN7	静态配置寄存器的定期软件回读	+	LBIST
通用 输入/输出 (GIO)	GIO1A	使用 I/O 检查的功能的引导时间软件测试	++	LBIST
	GIO1B	使用 I/O 检查的功能的定期软件测试	O	LBIST
	GIO2	信息冗余技术	++	LBIST
	GIO3	静态配置寄存器的定期软件回读	+	LBIST
联合技术行动 组 (JTAG) 调试/跟踪/ 校准访问	JTG1	JTAG 端口的硬件禁用	+	影响程序流的意外激活的安全装置检测
Cortex-M3 中央处理 单元调试	DBG1	JTAG 端口的硬件禁用	+	影响程序流的意外激活的安全装置检测
	DBG2	使用 MPU 来阻止到内存映射调试的访问	++	影响程序流的意外激活的安全装置检测
	DBG3	使用 CoreSight 调试逻辑密钥使能系统配置	++	影响程序流的意外激活的安全装置检测

Functional Safety Disclaimer for Safety Critical Solutions

TI's safety critical solutions, including integrated circuits, software and tools help TI's customers create end products that may be used in appropriately designed safety-critical applications to comply with functional safety standards or requirements.

Buyers represent and agree that they have all the necessary expertise to design, manage and assure effective system-level safeguards to anticipate, monitor and control system failures in safety-critical applications. Buyers agree and accept sole responsibility to meet and comply with all applicable regulatory standards and safety-related requirements concerning their systems and end-products which use TI's safety-critical applications. Buyers will fully indemnify TI and its representatives against any damages arising out of the use of TI products in safety-critical applications.

TI integrated circuits are not authorized for use in FDA Class III (or similar life-critical medical equipment) unless authorized officers of the parties have executed a special agreement specifically governing such use.

重要声明

德州仪器(TI) 及其下属子公司有权在不事先通知的情况下, 随时对所提供的产品和服务进行更正、修改、增强、改进或其它更改，并有权随时中止提供任何产品和服务。客户在下订单前应获取最新的相关信息，并验证这些信息是否完整且是最新的。所有产品的销售都遵循在订单确认时所提供的TI 销售条款与条件。

TI 保证其所销售的硬件产品的性能符合TI 标准保修的适用规范。仅在TI 保证的范围内，且TI 认为有必要时才会使用测试或其它质量控制技术。除非政府做出了硬性规定，否则没有必要对每种产品的所有参数进行测试。

TI 对应用帮助或客户产品设计不承担任何义务。客户应对其使用TI 组件的产品和应用自行负责。为尽量减小与客户产品和应用相关的风险，客户应提供充分的设计与操作安全措施。

TI 不对任何TI 专利权、版权、屏蔽作品权或其它与使用了TI 产品或服务的组合设备、机器、流程相关的TI 知识产权中授予的直接或隐含权限作出任何保证或解释。TI 所发布的与第三方产品或服务有关的信息，不能构成从TI 获得使用这些产品或服务的许可、授权、或认可。使用此类信息可能需要获得第三方的专利权或其它知识产权方面的许可，或是TI 的专利权或其它知识产权方面的许可。

对于TI 的产品手册或数据表，仅在没有对内容进行任何篡改且带有相关授权、条件、限制和声明的情况下才允许进行复制。在复制信息的过程中对内容的篡改属于非法的、欺诈性商业行为。TI 对此类篡改过的文件不承担任何责任。

在转售TI 产品或服务时，如果存在对产品或服务参数的虚假陈述，则会失去相关TI 产品或服务的明示或暗示授权，且这是非法的、欺诈性商业行为。TI 对此类虚假陈述不承担任何责任。

TI 产品未获得用于关键的安全应用中的授权，例如生命支持应用（在该类应用中一旦TI 产品故障将预计造成重大的人员伤亡），除非各方官员已经达成了专门管控此类使用的协议。购买者的购买行为即表示，他们具备有关其应用安全以及规章衍生所需的所有专业技术和知识，并且认可和同意，尽管任何应用相关信息或支持仍可能由TI 提供，但他们将独力负责满足在关键安全应用中使用其产 品及TI 产品所需的所有法律、法规和安全相关要求。此外，购买者必须全额赔偿因在此类关键安全应用中使用TI 产品而对TI 及其 代表造成的损失。

TI 产品并非设计或专门用于军事/航空应用，以及环境方面的产品，除非TI 特别注明该产品属于“军用”或“增强型塑料”产品。只 有TI 指定的军用产品才满足军用规格。购买者认可并同意，对TI 未指定军用的产品进行军事方面的应用，风险由购买者单独承担，并且独力负责在此类相关使用中满足所有法律和法规要求。

TI 产品并非设计或专门用于汽车应用以及环境方面的产品，除非TI 特别注明该产品符合ISO/TS 16949 要求。购买者认可并同意，如果他们在汽车应用中使用任何未被指定的产品，TI 对未能满足应用所需要求不承担任何责任。

可访问以下URL 地址以获取有关其它TI 产品和应用解决方案的信息：

	产品		应用
数字音频	www.ti.com.cn/audio	通信与电信	www.ti.com.cn/telecom
放大器和线性器件	www.ti.com.cn/amplifiers	计算机及周边	www.ti.com.cn/computer
数据转换器	www.ti.com.cn/dataconverters	消费电子	www.ti.com/consumer-apps
DLP® 产品	www.dlp.com	能源	www.ti.com/energy
DSP - 数字信号处理器	www.ti.com.cn/dsp	工业应用	www.ti.com.cn/industrial
时钟和计时器	www.ti.com.cn/clockandtimers	医疗电子	www.ti.com.cn/medical
接口	www.ti.com.cn/interface	安防应用	www.ti.com.cn/security
逻辑	www.ti.com.cn/logic	汽车电子	www.ti.com.cn/automotive
电源管理	www.ti.com.cn/power	视频和影像	www.ti.com.cn/video
微控制器 (MCU)	www.ti.com.cn/microcontrollers		
RFID 系统	www.ti.com.cn/rfidsys		
OMAP 机动性处理器	www.ti.com/omap		
无线连通性	www.ti.com.cn/wirelessconnectivity		
	德州仪器在线技术支持社区	www.deyisupport.com	

邮寄地址： 上海市浦东新区世纪大道 1568 号，中建大厦 32 楼 邮政编码： 200122