德州仪器 (TI) Hercules™ MCU: 适合在高铁中使用的各种功能

Texas Instruments

Hoiman Low
作者：德州仪器（TI）
微控制器业务发展经理

中国于 2008 年引入高速铁路，到 2014 年底高铁网络已增长至 16,000 公里。它是世界上最大的高铁网络，每天运载 200-300 万乘客。这些高速列车每列运载 1000 多人，以超过 300 公里/小时的速度不分昼夜地运行。它们的运行频率很高，例如，每 5 至 10 分钟就有一辆往返于深圳和广州之间的高速列车。

考虑到巨大的旅客数量和极长的运行时间，安全成为了人们最为关切的问题。除了 2011 年由于信号故障在温州附近发生重大撞车事故，造成 40 人死亡 190 人受伤之外，中国的高铁系统目前已证明是非常安全的。这突出表明了用于支持故障检测并在检测到故障之后及时消除风险的安全信号和控制系统的重要性。

高铁信号和控制系统

中国的高铁信号和控制系统与由地面系统和车载系统组成的欧洲列车控制系统（ETCS）非常相似。列车位置、列车速度、交通管制和容许速度等信息不断在列车和地面系统之间进行交换。车载计算机会根据实时数据来确定列车速度和制动模式。

高铁信号和控制方面的安全要求

中国高铁在安全方面遵循 CENELEC（欧洲电工标准化委员会）EN 5012x 铁路安全标准：

- 50126：铁路应用 – 是关于可靠性、可用性、可维护性和安全性（RAMS）方面的规范和示范。
- 50128：铁路应用 – 主要应用于 通信、信号和处理系统。
- 50129：铁路应用 – 主要应用在通信、信号和处理系统中与安全相关的信号电子系统

EN 5012x 以行业功能安全标准 IEC 61508 为参考。EN 50126 涵盖了铁路系统在整个生命周期的可靠性、可用性、可维护性和安全性（RAMS）。EN 50128 涉及铁路控制系统的软件开发方面，EN 50129 涉及到铁路信号电子系统。

EN 50129 的风险降低水平和故障率与 IEC 61508 基本上是统一的 – 表 1。

Standard	System	Safety Integrity	Architectural Metric	Architectural Requirement	Failure Rate	Specific MCU self-test requirements
IEC 61508	Programmable E/E systems	SIL – 1,2,3,4	SFF	HFT>0 for SIL 4	PFD, PFH	No
EN 50129	Railway	SIL – 1,2,3,4	N/A	Follow IEC 61508	THR	CPU, Memory

表 1

- 安全故障比例 (SFF)
- 硬件故障容错 (HFT)
- 按需故障概率 (PFD)
- 每小时故障概率 (PFH)
- 可容忍危险率 (THR)

与 IEC 61508 类似，EN 50129 系统风险降低水平要求是按照安全完整性水平 (SIL) 来进行分类，SIL 1 为最低，SIL 4 为最高 - 表 2。

但是，EN 50129 是通过 THR 来指定故障率，而不是通过 IEC 61508 中的 PFD/PFH - 表 2。

由于高速列车系统故障可能会造成严重的后果，因此系统 SIL 水平大多为 SIL 4，即系统的故障率必须低于每 1E8 或 1 亿运行时 1 次故障。

(注： 对于半导体组件，可达到的最高 SIL 水平为 SIL 3，能实现 SIL 4 的只有系统本身，而不包括要进入系统的组件。)

可容忍危险率 每个功能每小时的 THR	安全完整性水平 (SIL)
10-9 ≤ THR < 10-8	4
10-8 ≤ THR < 10-7	3
10-7 ≤ THR < 10-6	2
10-6 ≤ THR < 10-5	1

表 2

IEC 61508 和 EN 50129 的另外一个显著差异在于对大型集成电路的故障检测要求。EN 50129 提供了一系列有关 CPU 和存储器自检的规定性要求，而 IEC 61508 提供的是有关故障检测技术和措施的指导准则。

德州仪器 (TI) Hercules MCU 如何能够帮助客户开发在高速列车系统中使用的产品

除了功能实现，高速列车系统开发人员面临的安全方面的挑战为:

1. 实现一个符合 SIL 4 标准的系统
2. 实现特定的 CPU 和存储器自检要求（需具有业经证明的有效性）
3. 提供可靠的系统间通信接口
4. 提供系统间的高速通信接口
5. 配套模拟组件
6. 系统认证

1. 符合 SIL 4 标准的系统

如表 1 中所示，EN 50129 在硬件架构方面要求与 IEC 61508 一致。SIL 4 要求硬件故障容错 (HFT) = 1（冗余架构），且单一故障比例 >=99%

HFT = 1 且达到 SIL4的系统，它系统内至少具有两个SIL3通道，且系统内的危险故障不会阻止安全功能的执行 - 见表 3。

TI 的 Hercules TMS570 MCU 经 TÜV SÜD 认证达到 IEC 61508 要求中的 SIL 3 标准（MCU 可达到的最高 SIL 水平）。TÜV SÜD 是质量和安全标准合规方面的国际公认的独立评审机构。 客户可以设计一个双通道系统（两个通道均配备支持 SIL 3 标准的 Hercules MCU），作为必须满足 HFT =1 和 SIL 4 要求的整体系统的一部分。

Maximum allowable SIL for Type B (High Demand) safety-related elements			
Safe Failure Fraction of an Element (SFF)	Hardware Fault Tolerance		
	No Redundancy	Single Redundancy	Double Redundancy
<60%	Not Allowed	SIL1	SIL2
60% - <90%	SIL1	SIL2	SIL3
90% - <99%	SIL2	SIL3	SIL4
≥99%	SIL3	SIL4	SIL4

表 3: 注： 类型 B 产品均为复杂产品，在这些产品中，故障模式未知。大多数半导体均被归为类型 B。

2. CPU 和存储器自检

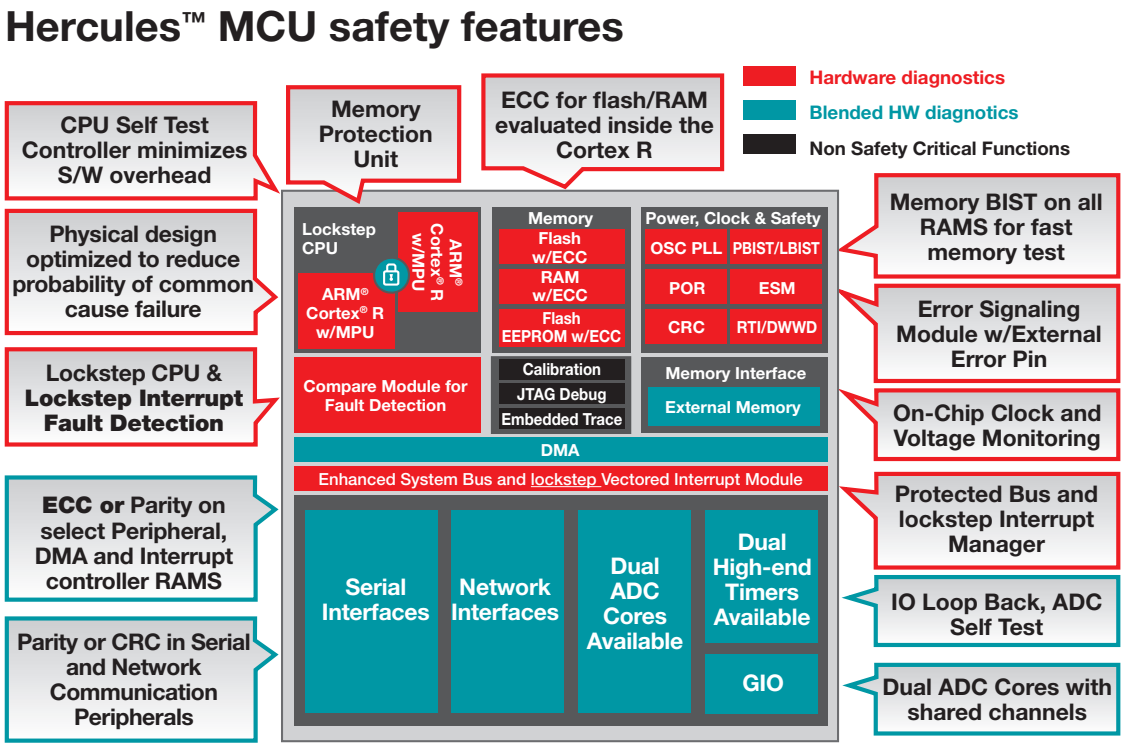
EN 50129 表 D.1 指定了要在大型集成电路（如 MCU）中实施的故障检测措施。 它包括 CPU、易失性存储器和非易失性存储器自检要求。

TI Hercules TMS570 MCU 提供双核 CPU 锁步/比较和存储器错误校正代码 (ECC) 实时诊断，以及基于硬件的 CPU 逻辑内置自检 (LBIST) 和 SRAM 可编程内置自检 (PBIST) - 见图 1。

这些基于硬件的安全功能可帮助在任关键模块中诊断错误，并以最低的软件开支提供高诊断覆盖率。

- 双核（ARM® Cortex® -R）锁步架构可以对CPU进行逐一时钟的高覆盖率诊断
- 错误校正代码 (ECC)电路是内置在CPU中，它的优点是不但对SRAM/Flash本身，也对SRAM/Flash的地址数据总线进行单位错误校正与双位错误检测 (SECDED)。
- CPU LBIST 和 SRAM PBIST 提供高覆盖率故障检测。

TI Hercules MCU 锁步 CPU（具有比较功能）、存储器 ECC、LBIST 和 PBIST 片上硬件诊断电路可促进按照 EN50129 表 D.1 要求以高测试覆盖率实施系统，同时将软件开支降到最低。



Bold items are introduced with the new Cortex®-R5 devices

图 1

此外，TI 还提供了 Hercules SafeTI™ 诊断库，在系统启动和正常运行期间提供易于使用的 API 功能来实施 CPU 和存储器自检。它还能提供针对初始化、意外处理、错误处理和故障注入的 API 支持 – 图 2。

您可以从 http://www.ti.com/tool/SAFETI_DIAG_LIB 下载 Hercules SafeTI 诊断库。

能。如果想了解 FlexRay 的详细信息，请查阅 TI FlexRay 的培训幻灯片：www.ti.com/lit/SPRT718.

4. 高速以太网系统间通信接口

要确定列车速度和制动模式，需要交换大量数据（如列车速度、列车位置、交通和跟踪数据）。当列车以 300 公里/小时运行时，高速通信接口是一个极为需要的功能。

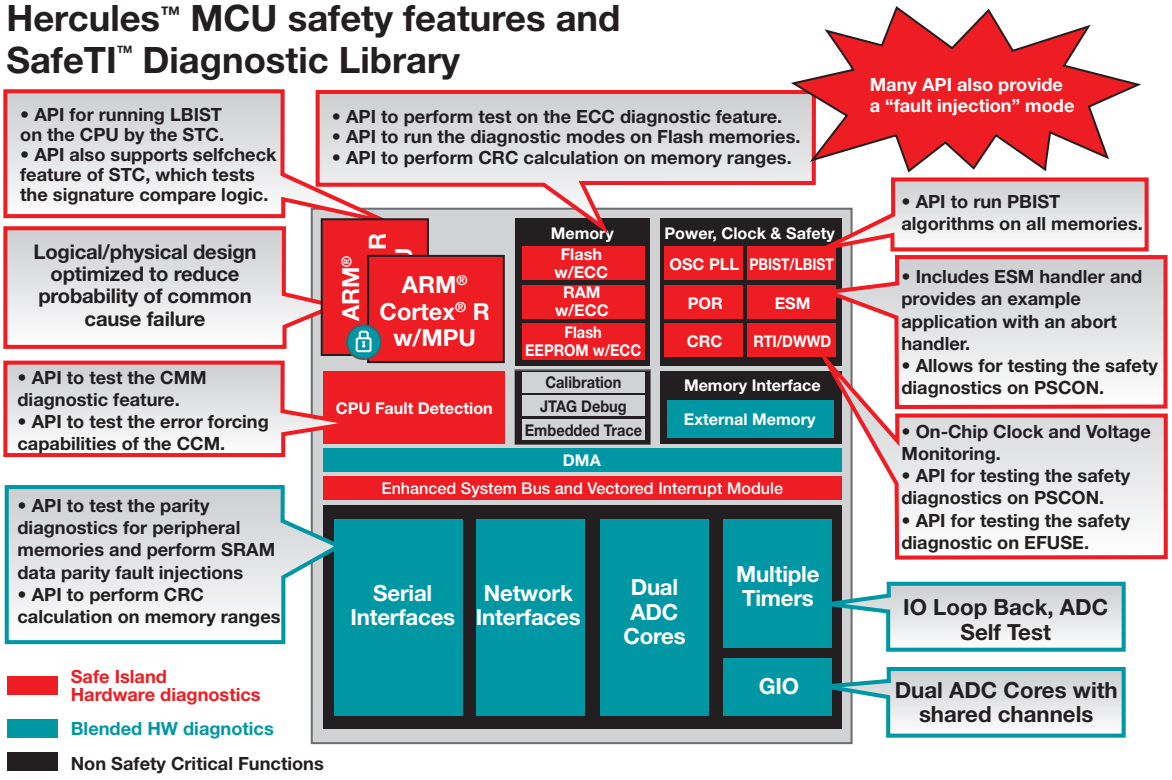


Figure 2

3. FlexRay 汽车级标准系统间通信接口

MCU 间和系统间通信是整个列车地面和车载系统中的关键任务。SPI 和 CAN 都是成熟可靠的通信接口，通常用于安全控制应用。这些事件驱动的非确定性通信接口对于许多安全控制应用都是有效的。但是它们不具备容错能力。FlexRay 是汽车行业专为需要硬件故障容错能力的安全应用（如 21 世纪初的线控制动和线控转向）而开发的。

TI Hercules MCU 中的 FlexRay 模块提供可在高铁信号和控制系统中使用的高速确定性故障容错功

TI Hercules MCU 中的以太网模块可为系统间通信提供标准的高速接口。

5. 配套模拟组件

TI 丰富的模拟组件产品组合可提供广泛的供电电路、接口和信号调节电路选择，将 Hercules MCU 与现实世界连接起来。

TPS65381-Q1（安全关键型应用中微控制器的多轨汽车电源）常被用作 Hercules MCU 的理想电源选择。 它可为 MCU 提供监控式电源。它还可用作监视器，监视 MCU 的运行。它直接与 Hercules MCU

错误信号模块连接，以在 MCU 之外进行错误处理。此外，它还包括内部模拟和数字电路的内置自检。

如果想了解 TPS65381-Q1 的详细信息，请访问 http://www.ti.com/product/TPS65381-Q1/description&lpos=Middle_Container&lid=Alternative_Devices

6. 系统认证

MCU 最高可获得某个特定的安全完整性水平（或“SIL”）认证。“获得认证”的 MCU 意味着其开发过程经过审核且达到了功能安全系统要求中的指定 SIL 标准。这些标准要求提供支持文档和工具（如安全手册以及故障模式影响与诊断分析 (FMEDA) 工具），以帮助系统开发人员了解 MCU 安全机制和计算 MCU 故障率。

经认证，TI 的 Hercules TMS570 MCU 达到了前面所提到的 IEC 61508 要求中的 SIL3 标准。MCU 开发流程、系统性故障的管理和随机故障的管理均已经过认证机构的检验。这些 MCU 的安全文档包括一本安全手册和一份安全分析报告，前者可通过普通下载获得（无保密协议要求），后者还会随同提供 FMEDA 工具（需签署保密协议）。这些文档和工具也已在 MCU 认证期间经过认证机构的审核。

TMS570 MCU 得到基础软件组件的支持，例如由 HALCoGen 工具生成的外设驱动程序以及 SafeTI 诊断库。这些软件组件的软件开发过程已通过 TÜV NORD 的认证，最高达到 IEC 61508 SIL 3 级安全完整性。TÜV NORD 是质量和安全标准合规方面的国际公认的独立评审机构。 SafeTI™ 合规性支持套件 (CSP) 根据 TI 的认证软件开发流程开发而成，可用于 HALCoGen 和 SafeTI™ 诊断库。这些 CSP 提供了一个有益的起点，有助于客户在系统认证期间针对功能安全相关软件提供类似证据。有关 SafeTI 合规性支持套件的更多信息，请参阅 http://www.ti.com/lit/wp/spny007/spny007.pdf

这些经过认证的 MCU 及其支持文档和工具的投入使用可为客户在安全系统开发方面提供帮助，并减少他们的认证工作。

概要

TI Hercules MCU 系列产品可为客户在系统开发和行业功能安全标准认证工作方面提供帮助：

1. 获得 SIL 3 认证的 MCU 可帮助客户设计出能满足SIL4要求的HFT=1的整体系统。
2. 基于硬件及具有高分辨率的 CPU 和存储器自检（达到或超出了 EN 50129 表 D.1 要求）和 Hercules SafeTI 诊断库（具有最低的软件开支）.
3. FlexRay 模块，提供确定性故障容错系统间通信接口
4. 以太网模块，提供高速列车所需要的标准的高速通信接口
5. 广泛的配套模拟组件选择，包括 TPS65381-Q1 电源和监视器
6. IEC 61508 SIL 3 认证 MCU 及安全手册和 FMEDA 工具以及基础软件组件（HALCoGen 外设驱动程序和 SafeTI 诊断库），根据 TI 的 IEC 61508 SIL 3 认证软件开发过程开发而成。

The platform bar and MSP430 are trademarks of Texas Instruments.
All other trademarks are the property of their respective owners.

© 2015 Texas Instruments Incorporated

重要声明

德州仪器(TI) 及其下属子公司有权根据 JESD46 最新标准, 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， 并有权根据 JESD48 最新标准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 保证其所销售的组件的性能符合产品销售时 TI 半导体产品销售条件与条款的适用规范。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。除非适用法律做出了硬性规定，否则没有必要对每种组件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 组件或服务的组合设备、机器或流程相关的 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中 TI 信息的重要部分，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。TI 对此类篡改过的文件不承担任何责任或义务。复制第三方的信息可能需要服从额外的限制条件。

在转售 TI 组件或服务时，如果对该组件或服务参数的陈述与 TI 标明的参数相比存在差异或虚假成分，则会失去相关 TI 组件 或服务的所有明示或暗示授权，且这是不正当的、欺诈性商业行为。TI 对任何此类虚假陈述均不承担任何责任或义务。

客户认可并同意，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与其产品及在其应用中使用 TI 产品 相关的所有法律、法规和安全相关要求。客户声明并同意，他们具备制定与实施安全措施所需的全部专业技术和知识，可预见 故障的危险后果、监测故障及其后果、降低有可能造成人身伤害的故障的发生机率并采取适当的补救措施。客户将全额赔偿因 在此类安全关键应用中使用任何 TI 组件而对 TI 及其代理造成的任何损失。

在某些场合中，为了推进安全相关应用有可能对 TI 组件进行特别的促销。TI 的目标是利用此类组件帮助客户设计和创立其特 有的可满足适用的功能安全性标准和要求的终端产品解决方案。尽管如此，此类组件仍然服从这些条款。

TI 组件未获得用于 FDA Class III（或类似的生命攸关医疗设备）的授权许可，除非各方授权官员已经达成了专门管控此类使 用的特别协议。

只有那些 TI 特别注明属于军用等级或“增强型塑料”的 TI 组件才是设计或专门用于军事/航空应用或环境的。购买者认可并同 意，对并非指定面向军事或航空航天用途的 TI 组件进行军事或航空航天方面的应用，其风险由客户单独承担，并且由客户独 力负责满足与此类使用相关的所有法律和法规要求。

TI 已明确指定符合 ISO/TS16949 要求的产品，这些产品主要用于汽车。在任何情况下，因使用非指定产品而无法达到 ISO/TS16949 要求，TI不承担任何责任。

	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应用处理器	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

Mailing Address: Texas Instruments, Post Office Box 655303, Dallas, Texas 75265
Copyright © 2015, Texas Instruments Incorporated