Technical White Paper

使用集成式 FDIR 设计航天系统：TI 航天级元件指南

摘要

在太空中，维护和维修难以实施。卫星系统一旦部署到位，就必须在其预期任务期间可靠运行，无需实际干预。这使得使用故障检测、隔离和恢复 (FDIR) 策略成为所有卫星子系统的基本设计要求。 [1]

FDIR 使系统能够检测异常行为、隔离故障元件并启动恢复操作，理想情况下不会影响任务目标。然而，实施 FDIR 绝非易事。它通常会导致成本上升、元件数量增多、电路板面积扩大和开发时间延长。为提高可靠性而引入的每个额外元件自身同样会产生故障概率，从而对系统的整体故障平均时间 (MTTF) 产生负面影响。

通过提高复杂度来增强可靠性需要采用谨慎权衡的设计方法。为满足设计目标，有效的 FDIR 必须通过尽量降低设计开销来实现其目标，从而尽可能减少使用额外元件并大幅提高可靠性。依托先进的航天级半导体产品，卫星系统设计人员可打造有针对性的高效 FDIR 实施方案。

本白皮书讨论了 TI 的航天产品系列，并解释了产品如何助力 FDIR 设计，帮助工程师减轻在成本、布板空间、元件数量、功耗和开发工作量上的负担。

内容

插图清单

商标

1 引言：TI 航天级产品系列

TI 的航天级产品系列为 FDIR 实施方案提供了基础构建模块，包括用于电压、电流和温度检测、信号比较、决策逻辑、通信、切换和隔离的元件。这些器件可帮助设计人员打造能够自主识别故障并采取纠正措施的系统，同时确保设计简洁。

此外，TI 的部分航天级器件（如 TMS570LC4357-SEP ）采用了 ISO 26262 等功能安全标准的设计原则和诊断功能。此类原则可有效地重新用于满足航天应用的严苛可靠性需求。

TI 可提供两种质量等级（如 图 1-1 所示）的航天级元件，以灵活实施多种任务：

- 耐辐射 (-SEP)：专为近地轨道 (LEO) 卫星设计，这类应用中成本效益和规模至关重要。此类产品至少可耐受 30krad 总电离剂量 (TID) 和 43MeV 线性能量传递 (LET)，可抗单粒子闩锁 (SEL)。
- 抗辐射 (-SP): 专为深空、载人航天、GEO/MEO 卫星和其他高可靠性任务而设计。此类器件遵循 QML-V 和 QML-P 等严格质量标准。"-SP" 型号的辐射耐受度可达 TID 50- 300 krad，SEL 抗扰度 ≥ 60 MeV·cm²/mg。

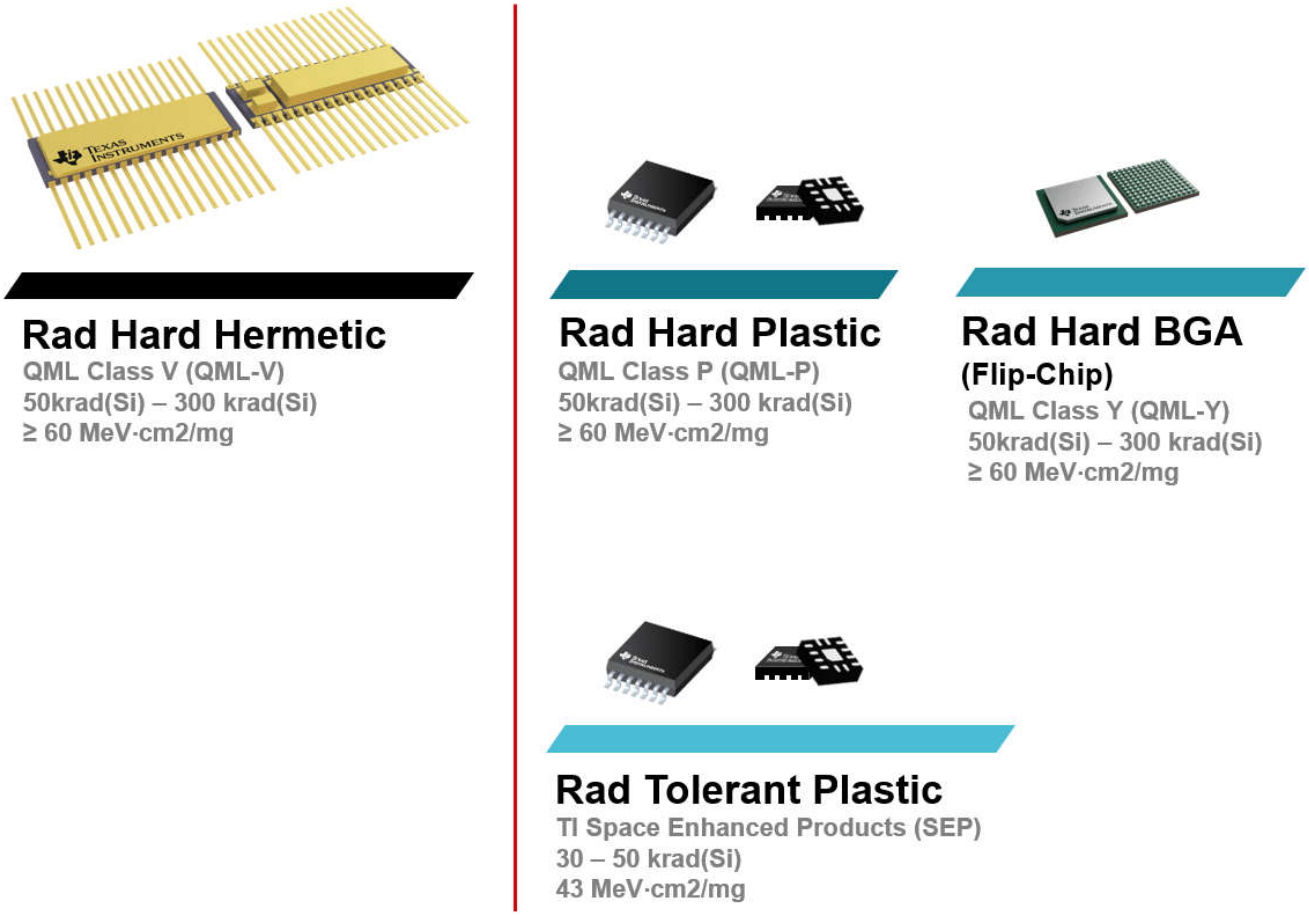

图 1-1. TI 航天级产品

这两类产品均具备材料和工艺控制，以降低封装（例如锡晶须、键合线疲劳或释气）的风险。TI 提供各种质量等级的引脚兼容型号产品和现成文档，采用基于类目的产品策略，助力降低成本、风险并缩短上市时间。对于设计 FDIR 系统的工程师，TI 的航天级元件为确保在不影响性能的前提下成功完成任务奠定了可靠基础。

TI 长期供货 QML-V 产品，同时提供具有以下优势的塑料封装航天产品：

- 引脚预先成型并修整到位，因此尺寸更小且更易于使用。
- 耐辐射 (-SEP) 和抗辐射 (QML-P/QML-Y) 型号产品之间引脚兼容，使得研发工作可跨任务场景高效复用。
- 更短的键合线可减少“封装寄生效应”，从而提高性能。
- 更强的散热能力。

航天级元件具备一个重要特性，即遵循单一受控的基线制造流程，这意味着只允许使用单一晶圆制造厂、单一封装测试设施以及单一组材料。这与商业制造流程大不相同。例如，汽车市场要求 IC 供应商确保在任何给定的时间点提供大量产品。为了满足这一需求，IC 供应商通常会建立高度灵活的制造流程，其中多个晶圆制造厂以及封装测试厂均可服务于单一器件制造，并可利用该流程快速响应需求突增。此外，对于任何大批量销售的产品，都需

要持续致力于提高产量和优化成本。预计随着时间的推移，以往通过认证或筛选的元器件与新采购的元器件在抗辐射性能方面将产生巨大差异。仅对商用元件筛选是否符合抗辐射要求与专门制造航天级器件之间存在显著差异。因此，通常只有航天级元件才能通过实际飞行验证。使用航天级组件所带来的长期财务和技术优势会随着时间推移呈指数级增长。

2 故障监测：测量关键要素

持续系统运行状况监测是实施有效 FDIR 的基础。在卫星电子设备中，需要跟踪的关键物理参数是电压、电流和温度。此类数值可及早指示出异常运行状况，使系统能够在发生永久损坏之前做出反应。

为了在恶劣的航天环境中可靠测量上述信号，德州仪器 (TI) 提供了种类齐全的抗辐射和耐辐射器件系列，这些器件通过飞行验证并可灵活应用。

2.1 电流监测

INA901-SP 是一款高精度电流检测放大器，不仅耐辐射，还符合航天标准。器件支持高达 65V 的宽域共模输入，因此适用于各种系统电压。经优化的带宽可确保快速检测过流事件，而强大的电源抑制能力和快速稳定时间有助于避免由瞬态噪声或干扰引起的误警报。由此即可在不影响可用性的情况下实现高灵敏度和精度。

2.2 电压比较和阈值检测

TLVxHx90-SEP 系列比较器支持基于受监测信号的快速决策。此类元件可快速检测来自电源轨或电流传感器输出的待测电压是否超出规范要求。

例如：

- TLV4H290-SEP 可提供四个独立的比较器通道，传播延迟小于 0.1µs，而每个通道仅消耗 25µA 的静态电流。
- TLV4H390-SEP 通过漏极开路实现相同性能，因此可以轻松将多个故障信号聚合到同一条警报线路中。

2.3 温度检测

温度监测对于早期故障检测和热管理都至关重要，可有效限制电子器件所承受的应力。TI 的航天级温度传感器 IC 具备高精度和较低的设计开销。

例如，TMP461-SP 利用器件带隙随温度变化的可预测特性实现了优于 ±0.1°C 的精度。该器件集成了多种功能，包括激励电流生成、带有输入驱动器的模数转换器 (ADC) 以及用于实际故障检测的窗口比较器。

这一集成水平降低了电路板复杂度，并通过标准 I²C 接口简化通信，从而便捷连接到主机 FPGA 或 MCU。

对于多点监测，TMP9R00-SP（如 图 2-1 所示）最多支持八个外部传感器输入。器件可以连接到 FPGA 或 ASIC 的片上温度二极管，或者连接到放置在功率 FET 等热点附近的分立式传感器。该器件还额外集成了第九个传感器，用于进行本地测量，从而实现面向整个电路板的全面热分析。

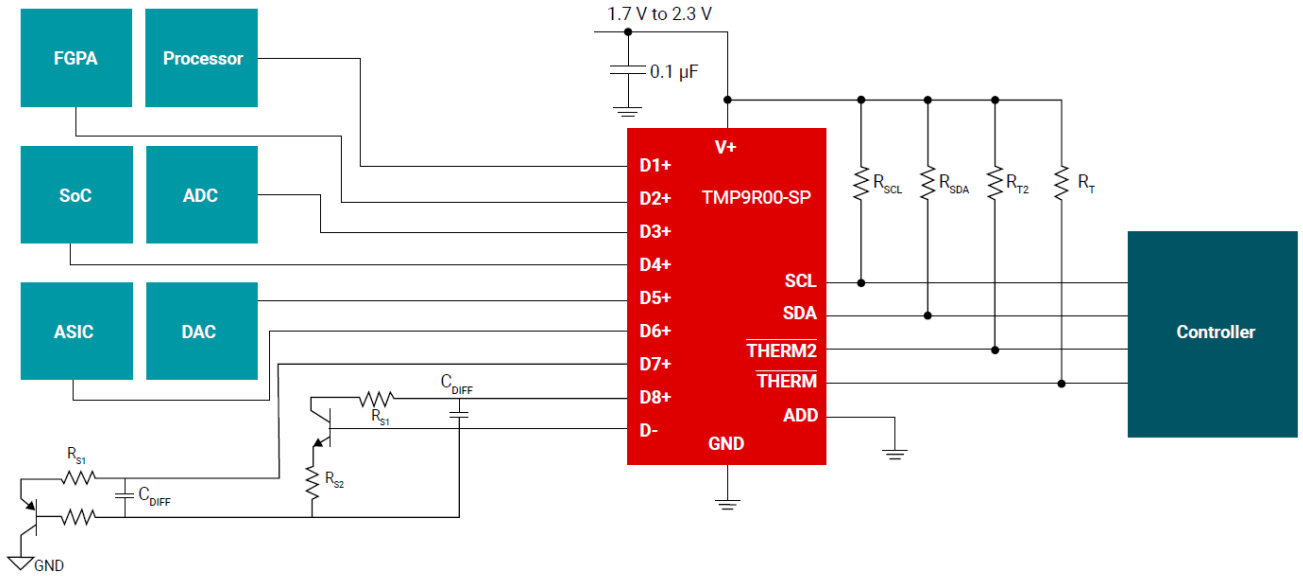

图 2-1. TMP9R00-SP 助力实现面向整个电路板的全面热分析

3 精密数据采集

对于需要对多个模拟参数进行高分辨率监测的系统，TI 提供了具有可扩展通道数、集成基准电压和自检功能的精密 ADC。

ADC128S102QML-SP 和 ADC128S102-SEP 在市场上颇受欢迎，可满足此类 FDIR 基本要求，每个器件具有八个个 12 位模数 (ADC) 通道，并支持 50kSPS 至 1MSPS 的采样率能力。

为满足更高的分辨率需求，ADC168M102R-SEP 可为多达八个 16 位 ADC 通道提供双路同步采样（采样率为 1Msps），并集成两个 DAC 以输出两个独立的基准电压。

如果需要更高的通道数，TMUX582F-SEP 支持 8:1 多路复用输入通道，输入电压可达 ±16.5V，过压保护可达 ±60V。

此类高通道数器件可实现高效、灵活的信号采集，同时兼顾可靠性，即使在恶劣条件或多变输入环境下也是如此。

4 决策：从简单逻辑到智能控制

检测到故障后，系统必须决定如何快速、可靠地响应。根据故障处理策略的复杂性，该过程涵盖从简单的逻辑操作到完全自主的智能控制流程。德州仪器 (TI) 可提供满足各类要求的全系列解决方案，帮助工程师根据任务需求打造定制化设计。

4.1 基于逻辑的决策路径

对于简单的 FDIR 实施方案，分立式逻辑元件仍是一类高效、低开销的解决方案。TI 最新推出的航天增强型 SCxT 逻辑产品系列支持在宽电压范围（1.2V 至 5.5V）内实现单一电源电平转换，助力简化系统设计，无需另配电平转换器。

SN54SC4T02-SEP（4 通道或非门）或 SN54SC4T08-SEP（4 通道与门）等标准逻辑门可实现简单而稳健的决策逻辑。

为提高灵活性，SN54SC3T97-SEP 等可配置逻辑器件通过单一可订购器件型号提供多种逻辑功能。

4.2 基于 MCU 的控制

更先进的 FDIR 策略通常需要更高层次的抽象：监测多个输入、评估合理性、分析趋势以及记录随时间推移的系统行为。在此情况下，航天级微控制器 (MCU) 为软件驱动的智能决策提供了理想平台。

MSP430FR5969-SP 专为低功耗、空间受限的应用而设计。器件在单个芯片上集成了 ADC、比较器、PWM 输出和电压基准生成以及许多其他功能，大大降低了对分立式元件的需求。器件的非易失性 FRAM 存储器尤为适于记录数据，具有快速写入周期和高耐久性。例如，使用片上 64KB FRAM 的 20KB 容量可存储多达 20,000 个数据点，数据点可用于在轨软件更新和行为调整、故障分析和根本原因识别或任务后审查和优化。

TMS570LC4357-SEP 双核锁步 MCU 进一步加强了 FDIR 功能。该器件最初是为防抱死制动系统 (ABS) 和动力转向等汽车安全系统而开发的，在构建之初就考虑了 ISO 26262 ASIL-D 合规性 [3]、[7]。

器件的关键特性包括：

- 经认证的开发流程，可显著降低系统故障概率 [5] [6]
- 双锁步 CPU 架构，可实现实时故障检测和响应
- 全方位诊断

这些特性为高完整性故障响应奠定了基础，即使在执行关键任务的实时操作期间也是如此。 [8]

TMS570LC4357-SEP 具有 41 个 ADC 通道、64 个具有计时器和 PWM 功能的 GPIO 以及多个通信接口，支持复杂的 FDIR 实施方案。通过高通道数器件（如具有 16 个 12 位 ADC 通道、12 个数模转换器 (DAC) 通道、3 个温度传感器和 8 个 GPIO 的 AFE11612-SEP），产品的可扩展性得到了进一步增强。例如，如 图 4-1 中所示，向 TMS570LC4357-SEP 添加两个 AFE11612-SEP 实例可启用具有以下特性的系统：

- 72 个 ADC 通道
- 32 个 DAC 通道
- 7 个互补 PWM 输出
- 6 个增强型捕获 (eCAP) 模块
- 2 个增强型正交编码器脉冲 (eQEP) 模块
- 用于额外 PWM 输出且具有高级计时器模块的 64 个 GPIO
- 16 个外部中断/通用输入/输出 (GPIO)
- 4 个温度传感器输入
- 2 个 2.5V 基准输出
- 10/100Mbps 以太网 MAC
- 4 个控制器局域网 (CAN) 控制器
- 2 个内部集成电路 (I2C) 模块
- 5 个多缓冲串行外设接口 (MibSPI)
- 4 个通用异步接收器/发送器 (UART) 串行通信接口 (SCI)

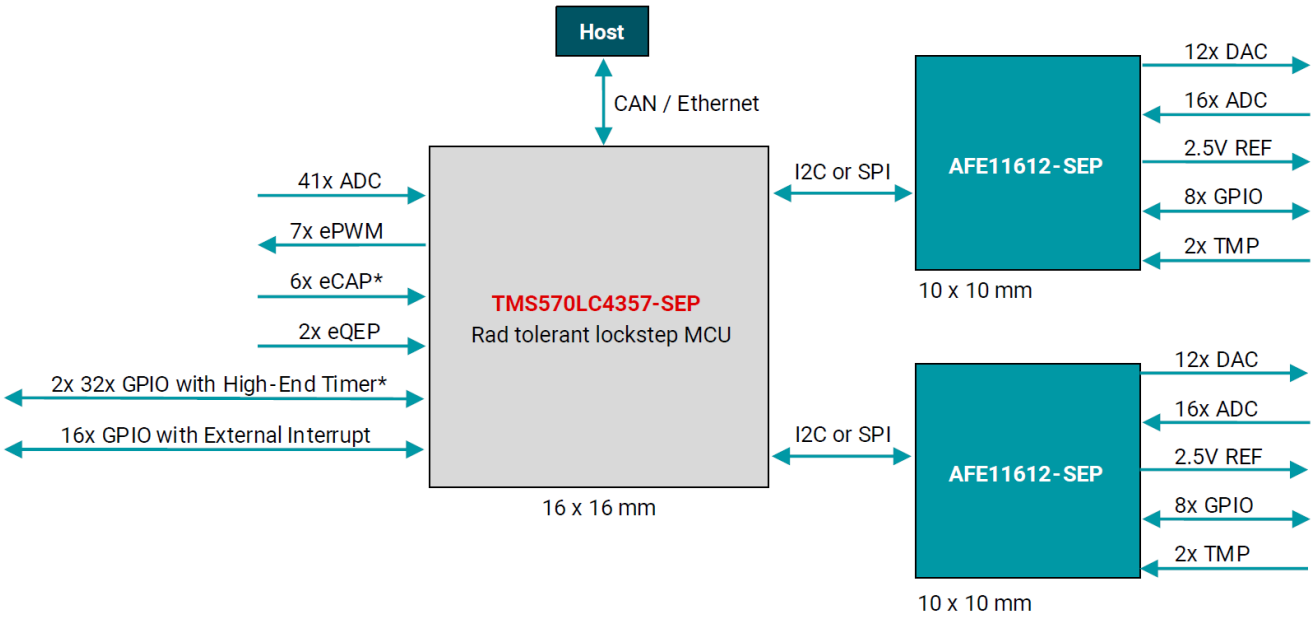

图 4-1. 基于 TMS570LC4357-SEP 和 AFE11612-SEP 的高通道密度监测和控制系统

无论是部署为整个卫星总线的中央控制器，还是作为各个 PCB 上的本地 FDIR 单元，TMS570LC4357-SEP 均可实现高可靠性和灵活性，并具有近乎即时的故障检测性能。

5 隔离和遏制：防止故障传播

在紧密集成的卫星系统中，单个 PCB 上的本地硬件故障会快速影响相邻子系统，尤其是当高压故障通过模拟或数字 I/O 连接传播时。这种现象称为故障传播，会对系统完整性和任务的成功实施带来严重风险。为降低这种风险，必须在关键电路域之间设置隔离栅。这些隔离栅将故障隔离在本地，保护健康子系统，确保系统柔性降级而非完全故障。

德州仪器 (TI) 推出耐辐射数字隔离器 ISOS141-SEP，是航天应用中数字信号隔离的有效解决方案之一。有别于传统的光隔离器，ISOS141-SEP 采用电容隔离技术，具有以下特点：

- 在恶劣环境下具有更高的可靠性
- 数据速率高达 100Mbps，可实现快速稳定的信号传输
- 使用寿命更长且功耗更低

这使其尤为适合隔离电路模块之间的高速通信，其中信号完整性和故障遏制均为任务关键型操作。

通过使用 ISOS141-SEP 实现数字隔离，设计人员可以显著提高系统层级的稳健性，确保故障隔离在本地，同时卫星上的通信即使在异常条件下也能保持正常运行。

6 通过智能冗余确保电源可用性

在航天系统中，电源稳健性不仅重要，更是攸关任务的成败与否。如果电源轨发生故障，恢复措施极其有限。因此，许多卫星设计都采用了冗余电源，用于维持重要子系统的持续运行。

初看之下，冗余电源设计似乎很简单。然而如果想要实施得当，则需要周密协调检测、隔离和时序机制。

6.1 基于二极管的冗余

实现电源冗余的最基本方法是并联两个稳压输出，每个输出都采用二极管连接。例如，可以将两个 TPS7H4011-SP 降压转换器器件配置为向单个电源轨供电。二极管设计可确保如果一个电源发生故障（如由于输出电容器的接地短路），另一个电源将不受影响并继续供电。

TPS7H4011-SP 与其引脚兼容的耐辐射型号 TPS7H4011-SEP 一样，尤为适用于此配置，原因在于其集成的保护和监测功能：

- 针对欠压和过压问题的电源正常输出监控
- 通过 FAULT 输入引脚实现灵活的故障管理
- 可选电流限制
- 热关断保护
- 可调输入使能和电源正常输出
- 单调启动进入预偏压输出
- 可调斜坡补偿和软启动
- 差分遥感

在无需外部时钟的情况下，该器件最多可配置四个并联器件以提高电流能力；或者就 FDIR 而言，仅用于实现冗余并尽可能减少设计开销。

但是，稳健的电源系统通常需要的不仅仅是无源二极管。为了防止故障反馈到主电源轨中，需要从其输入端主动断开故障转换器。

这需要：

- 开关元件来隔离故障器件
- 针对过流、欠压、过压或过热事件的故障检测逻辑
- 在根本原因消失后锁存电路以保持故障状态
- 用于实现具有适当延迟和重试限制的重试逻辑时序机制
- 消隐周期，用于抑制上电浪涌或良性瞬态等事件期间的误触发

如果未精心设计，这些附加元件实际上会增加平均故障时间 (MTTF)，从而降低整体系统可靠性。因此，智能冗余需要一个经过良好集成和测试的架构。

简化复杂冗余控制的一种方式是使用高可靠性 MCU，例如 TMS570LC4357-SEP。如果器件已装配到 PCB 并用于其他功能，仅需加装少量电路即可管理电源故障响应，从而在不增加元件数量或功率预算的情况下实现增值。

进一步来说，图 6-1 中所示的设计原则可在无点故障的情况下实现容错，这意味着冗余方案中的任何单个元件在发生故障后，不会影响向下游系统的电力输送。[2]

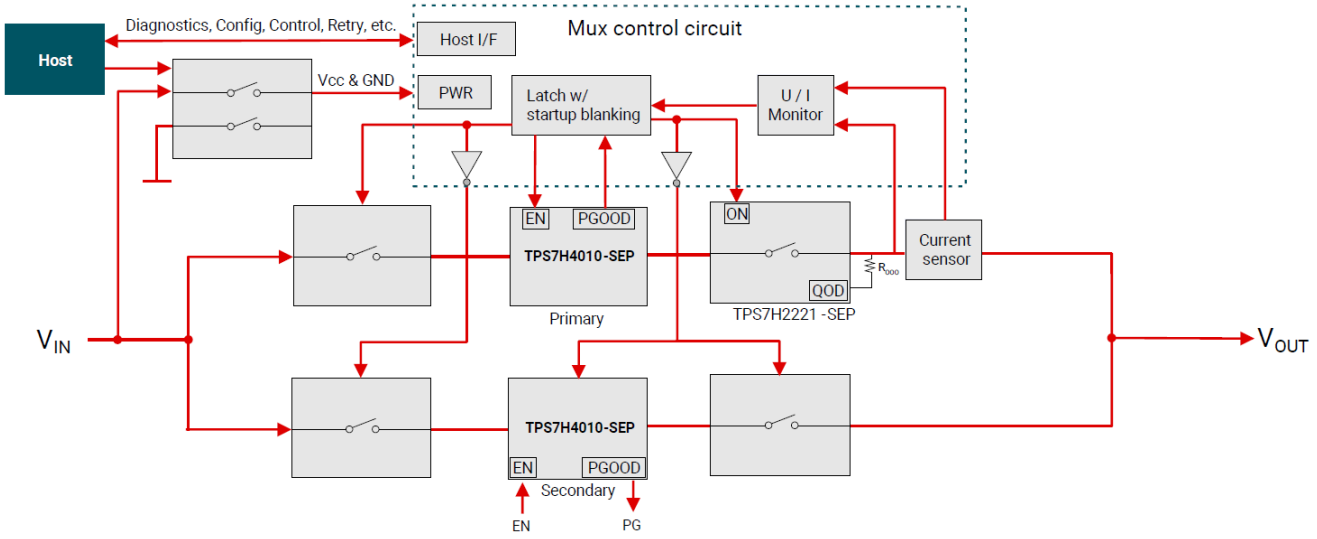

图 6-1. 通用容错电源架构

使用 TPS7H2221-SEP 作为负载开关可进一步提高稳健性和可恢复性，这得益于集成的保护功能和机制：

- 短路保护
- 浪涌电流限制，可降低上游元件的应力
- 具有自动重启功能的热关断
- 快速输出放电 (QOD)，用于恢复下游锁存负载（请参阅 图 6-2）。

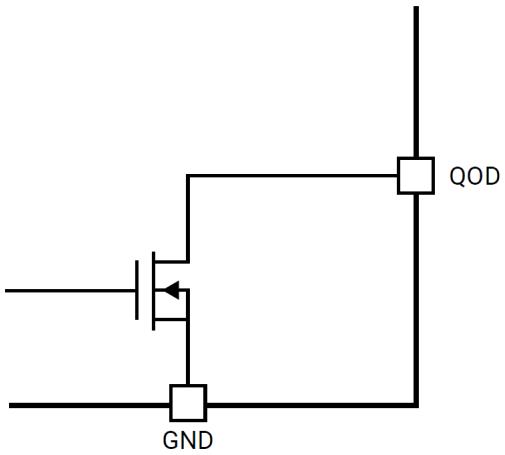

图 6-2. 快速输出放电 (QOD) 功能提供受控接地路径

德州仪器 (TI) 和 STAR-Dundee [4] 联合白皮书中介绍了优化冗余的实际示例，详细说明了 Xilinx KU060 FPGA 的故障保护电源架构（请参阅 图 6-2），如应用简报 STAR-Tiger SpaceFibre 路由交换机的电源设计所述。

白皮书展示了冗余电源输入管理、正确的电源时序以及全面的故障检测和隔离机制，仅需加装少量元件。此设计采用 TPS7H2201-SP 智能负载开关，该开关集成了过压和欠压保护、过流和电流检测、热保护以及内部或外部控制负载切换功能。

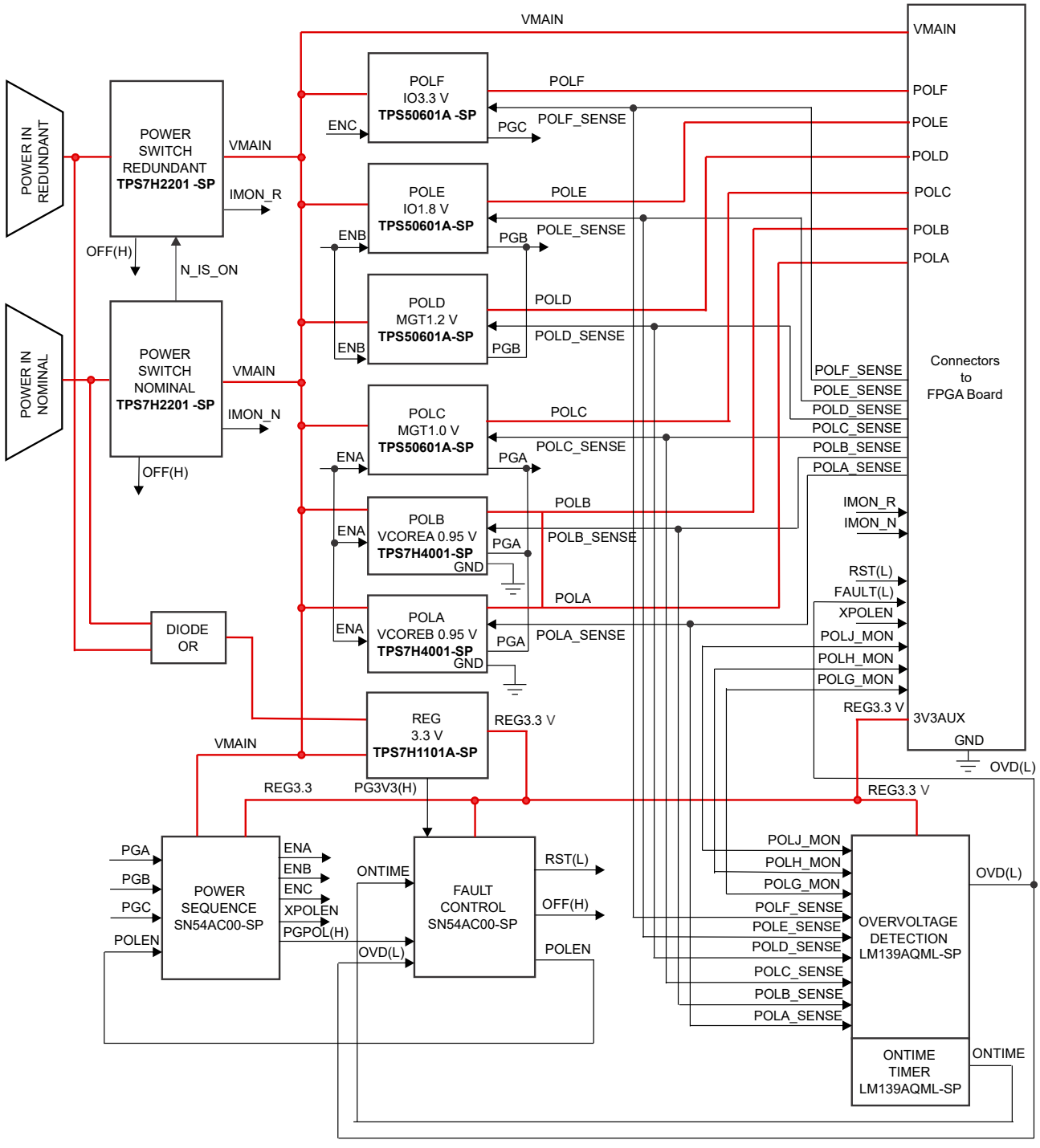

图 6-3. Xilinx KU060 FPGA 的故障保护电源架构

以上两个示例说明了如何使用高性能航天级元件，为要求严苛的卫星应用构建稳健、容错的系统级电源解决方案。

7 总结

在航天任务的电子设计中实施 FDIR 非常复杂。该设计需要能够承受辐射、极端温度和漫长任务持续时间的元件，这些条件并非标准商业元件所能满足的。

TI 的航天级产品集成诊断和故障处理功能，可帮助设计人员减少开销。专用解决方案助力实现有效隔离并避免故障传播。从简单的“切换”到基于多个传感器输入的复杂决策，TI 可以为各层次的系统恢复策略提供支持。

8 参考

1. Research and Design of Hierarchical FDIR in Spacecraft Xiaodong Jia(&), Chunping Zeng, and Yufu Cui DFH Satellite Co., Ltd., Beijing 100094, China 15811283470@163.com
2. Heimerdinger, W. L., and Weinstock, C. B., "A Conceptual Framework for System Fault Tolerance," USAF CMU/SEI-92- TR-033, ESC-TR-92-033, 1992.
3. 德州仪器 (TI)：*Hercules™ 微控制器：适用于安全关键型产品的实时 MCU*
4. 德州仪器 (TI) 和 STAR-Dundee，详细介绍了 Xilinx KU060 FPGA 的故障保护电源架构（图 7），*STAR-Tiger SpaceFibre 路由交换机的航空电源设计*
5. 德州仪器 (TI)：*TÜV NORD 功能安全软件开发流程证书*
6. 德州仪器 (TI)：*功能安全硬件流程认证*
7. 德州仪器 (TI)：*TMS570LC43x 的 TUEV SUED 认证*
8. Benefits of using functional safety in commercial space applications, Journal of Space Safety Engineering Volume 12, Issue 1, March 2025, Pages 187-194, F. Lumpe, M. Seidl

重要通知和免责声明

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 产品的相关应用。 严禁以其他方式对这些资源进行复制或展示。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