Technical White Paper

在航天应用中实现功能安全的好处

摘要

最初发表于《空间安全工程杂志》（第 12 卷、第 1 期）

根据 IEC61508，只要产品或系统包含执行安全关键型功能的电气、电子或可编程电子元件，功能安全就很重要。功能安全应用于许多技术领域，例如工艺（比如能源部门）、汽车（运输部门）、机械工程和航空工业。本文将基于 IEC61508 和 ISO26262 的功能安全方法及概念与航天工业的 RAMS（可靠性、可用性、可维护性和安全性）方法，尤其是故障检测隔离和恢复 (FDIR) 方法进行了比较。

本文专门针对复杂的集成电路 (IC) 深入探讨了如何大幅降低元件级风险。过去，航天工业一直侧重于验证所使用的元件是否符合极端环境参数，以及通常能否在太空中长时间使用。但是，随着 IC 变得越来越复杂，在元件本身的开发过程中以及设计人员使用其来开发实际电路板组件时，发生系统故障的风险显著增加。

此外，由于体积较大，元件成本是卫星星座发展的一个主要因素，因此必须在可靠性和成本之间找到平衡。

本白皮书讨论了如何减少其他市场部门中的系统性故障、以及如何借助纠错码 (ECC)、锁步或内置自检 (BIST) 等半导体的适当性能特性，尽快检测“随机故障”，以及在理想情况下消除或至少更大限度降低这些故障的影响。

本文提供的建议可帮助您了解如何充分利用为在航天应用其他市场领域实现功能安全而开发的半导体的现有特性。

内容

插图清单

商标

所有商标均为其各自所有者的财产。

1 简介

对太空飞行领域的私人投资开启了所谓的“新太空”时代。然而，“新太空”一词不仅代表了私营公司的崛起及其对优化投资回报的兴趣；也代表了太空产品开发方式的范式转变。[1] 这种转变不仅是由私营部门推动的，而且在不同程度上也是由国家机构推动的，而这些机构正在积极推动这种转变。

设计人员和设计经理面临管理不断增长的系统级复杂性风险的挑战。因此，通过采用各种方法（例如已制定的确认和验证流程）来大幅减少故障比以往任何时候都更加重要。这还需要从项目一开始就大幅减少故障，在这期间，系统架构师、系统工程师、软件、硬件设计人员和产品保证工程师需要密切合作。此外，这还涉及避免开发工具（如编码编译器、电子设计软件和 RAMS 工具）出现故障。

商业化推动航天部门在成本、绩效、时间和风险之间取得平衡。这四个因素将共同主导未来竞争激烈的工业市场，没有人能够只关注其中一个因素，而仍然期望取得成功。这四个因素必须由基于 ISO 9001 或其他相关管理标准的稳健管理系统进行监控。[2]

自上而下意味着在工程层面上缩短设计、制造、测试和部署的开发周期。以指定解决方案为导向，重点关注主要方面。为了优化投资回报，必须避免代价高昂的过度设计。例如，可以通过尽可能重复使用合格零件和电子元件的模块化设计来实现这一目的。通信行业对新太空的推动力很大，该行业需要大量生产卫星来支持超级星座。[3]

由于 Starlink 已经将数百颗卫星送入太空，卫星的大规模生产是航天工业最大的转变之一，因为大多数现有太空标准都是为定制系统而设计的。

因此，值得关注面向大规模生产和高可靠性要求的其他行业，例如汽车行业。

2 其他工业领域的太空发展优势和概述

航天和汽车工业有相似之处，但从既定的角度来看，某些属性完全不同。例如，太空系统的特点是其系统高度复杂。这是因为像卫星这样的产品在太空中是无法触及的，这就要求工程师预测和减轻极端外星环境带来的风险，比如真空、温度循环、微重力和长时间执行任务。这一特性，再加上许多航天飞行任务都是由科学问题驱动的，这本身就会导致科学进步，并推动突破技术界限。对于大多数任务而言，需要有一个量身定制的地面设计，这种设计需要既坚固又可靠。产品安全至关重要，因为不可能对硬件进行维修或维护。这对于载人任务尤其重要，使得产品安全对工程师来说是一个挑战。

与太空相反，描述汽车工业的创新属性除了高可靠性和安全性之外，还包括高成本压力和高效量产的优化。在这种背景下，工程师需要专注于重用和模块化。高度集成的半导体元件可提供显著的成本优势。

产品安全性和高可靠性对航天和汽车工业同样重要。然而，背后的原因对其中任一行业而言都有所不同。

2.1 汽车领域产品安全动机

当然，主要的动机是需要采用类似于太空技术的强大（可靠）的安全功能技术，以保护人们在日常交通出行中可能面临的危险情况（如刹车或安全气囊弹出），以便在危急情况下挽救生命，并符合公法要求。第二个动机是更高的经济性: 昂贵的产品召回给汽车行业带来了巨大业务风险，甚至可能导致公司停业。汽车行业通过基于基础标准 IEC61508 的专用标准 ISO26262，来解决功能安全领域各个方面的问题。

2.2 航天领域产品安全动机

鉴于航天飞行任务，特别是载人航天飞行任务所涉及的高风险，开展 RAMS 活动对于确保宇航员的生存至关重要。但是，重要的是要认识到，并非所有任务都是载人的，而产品安全，或者更准确地说是产品保证的必要性仍然至关重要。这种必要性源于这样一个事实，即太空探索是一项全球性的工作，受旨在防止可能产生严重政治影响的灾难性失败的国际标准和要求的支配。

对太空活动的巨大财政和时间投资进一步强调了强有力产品保证做法的重要性。此外，随着对太空碎片和太空环境可持续性的日益关注，现在比以往任何时候都应更加迫切需要采取全面的安全措施。

在“新太空”时代，人们越来越多地采用汽车工业属性，例如大规模生产、成本优化等已经讨论过的属性，摘要参见 图 2-1。

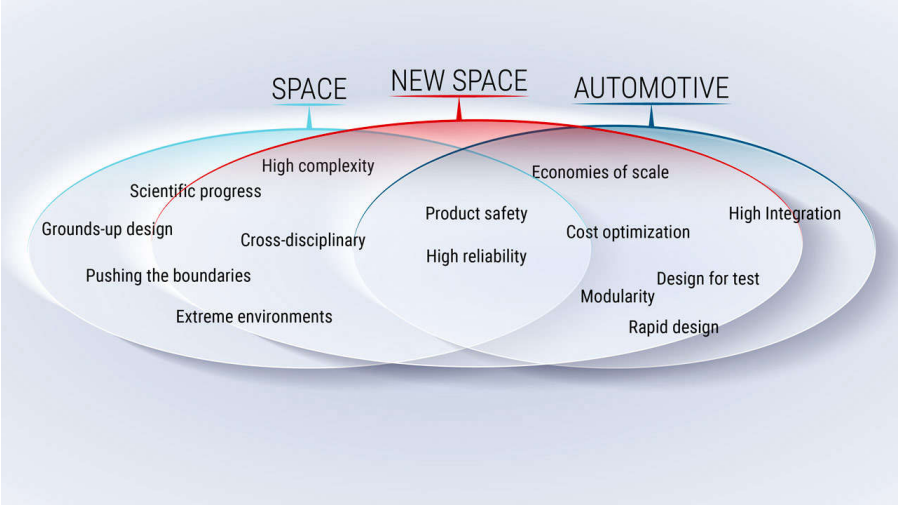

图 2-1. 太空和汽车属性

基础标准 IEC61508 [4] 代表了大多数行业领域的基本标准。然而，航天领域不遵循 IEC61508 标准。这也意味着航空、加工、汽车和机械工程等行业遵循相同的方法，如 图 2-2 中所示。然而，每个行业也有自己的特定行业标准，以及符合其特殊需要的详细方法和实例。航天工业采用一种相当通用的方法和流程来处理和管理系统的功能安全。

在 ISO61508 中，该功能的特点是安全完整性等级 (SIL) 为 1 到 4；在航空领域，这称为设计保证等级 (DAL)，而在汽车行业，根据 ISO26262，这称为汽车安全完整性等级 (ASIL) [5]。

图 2-2. 不同行业，不同的标准

在不采用 IEC61508 的航天工业领域，采用称为可靠性、可用性、可维护性和安全性 (RAMS) 的标准，这个术语涵盖了所有这些方面并定义了质量和可靠性要求 [9]。一个特殊的卷轴会引导进行故障检测隔离和恢复 (FDIR) [7]，这是一个概念，可以在检测到异常时隔离和恢复系统。此概念超越了仅要求达到安全状态的功能安全要求。

3 RAMS 和 IEC61508 功能安全标准的共性

功能安全标准和 RAMS 具有相同的目标，即“避免不可接受的风险”（如 图 3-1 中所示），其中两者都将风险定义为损害的严重程度与发生这种损害的概率的乘积。

图 3-1. 避免不可接受的风险

IEC61508 功能安全标准专门针对电气、电子或可编程系统的整个生命周期内的安全性，这些系统集成到产品的安全仪表系统 (SIS) 中以执行安全功能，这些功能必须可靠地定义并包含传感器、逻辑和执行器，如果有必要，还应采用冗余架构（通道）。

功能安全标准概述了特定流程，并包括其实现的工具和方法。

首字母缩略词 RAMS 定义了有关 [8] 的所有方面：

- 可靠性：执行特定功能的能力；可作为设计可靠性或运行可靠性指标：在给定环境中保持正常运行状态的能力。
- 可维护性：轻松、及时地进行维护（保养、检查和核查、维修和/或改造）的能力。
- 安全性：在整个产品生命周期内防止对人员、环境和资产造成损害的能力。

与功能安全标准相比，RAMS 不仅涵盖电子安全功能，还全面满足系统的所有质量要求。它还涉及材料和机械的各个方面，以及如何执行维护以及如何在特定时间和时间间隔提供相应功能。所有这些能力都有助于实现可靠、可用、可维护且安全的性能。虽然可靠性、可用性和维护不仅仅是安全功能，它们对于操作也至关重要。

功能安全主要指安全功能，但可编程电子功能也可应用于具有 RAMS 属性的基本操作功能。

功能安全和 RAMS 都有共同之处，它们的不同之处在于：

- 随机失效
- 系统性失效

3.1 随机失效

硬件元件中会发生随机失效，例如电阻器短路或晶体管栅穿。这些失效本质上是不可避免的，随时可能不期而至，只能通过数学概率对发生这些失效的可能性进行估算。一旦检测到这些失效，就不能逆转，因为它们会对受影响的元件造成全面、不可逆转的损坏。

因此，主动管理这些风险至关重要，通常是采用冗余机制来减轻其影响。可以通过以合理的精度对硬件可靠性进行统计建模来预测适用的硬件可靠性：

- 失效率 [9]：失效率是指在 t=0 时全新、且在时间间隔 (0,t] 内未失效的条件下，时间间隔 (t, t+ δ t)] 内失效的条件概率与 δ t 之比，当 δ t→0 时的极限值（若存在）。
- FIT [9]：每 10^9 小时失效一次，是半导体行业的通用失效率单位
- PFH [10]：每小时发生危险失效的平均概率
- PFD [10]：按需发生危险失效的平均概率
- MTTF [9]：MTTF= $(t_1+\cdots.+t_n)/n)$，其中，$t_1 \cdots t_n$ 是统计学上相同项目的无失效时间

总之，随机失效是指一种定量方法，仅与硬件元件有关，软件不会出现随机失效。[9] 中的主要浴盆曲线显示了三个阶段：

- 第 1 阶段，早期失效：例如，材料、元件或生产过程中的缺陷。
- 第 2 阶段，失效率恒定（或几乎恒定）的失效：此期间的失效是泊松分布的、并且经常突然发生。
- 第 3 阶段，耗损失效率：该阶段的失效归因于器件老化、磨损、疲劳等。

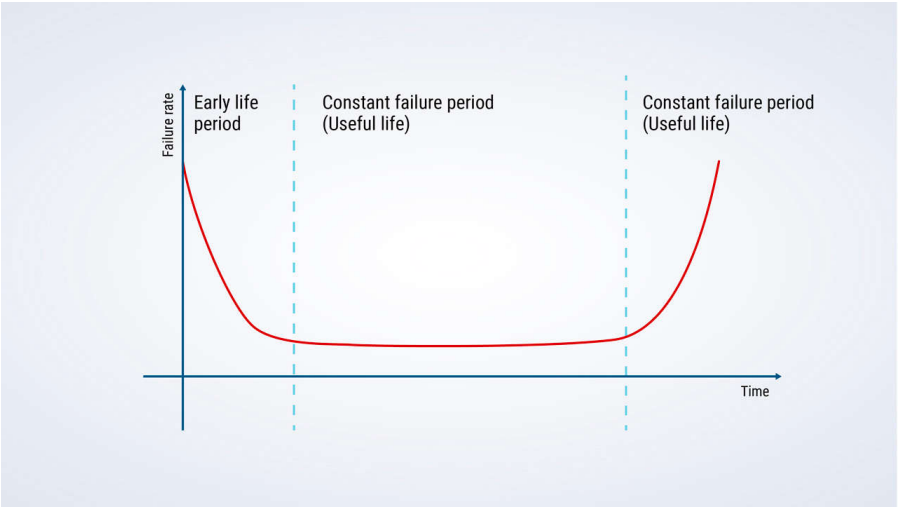

图 3-2. 简单设备浴盆曲线的随机失效率

可靠性工程侧重于曲线的中间部分，也称为使用寿命。需要采用相应方法来避免早期失效，例如老化；通过限制系统使用时间可避免耗损失效。

3.2 系统性失效

硬件和软件项都可能发生系统性失效。在处理、存储和使用的特定条件下，始终会发生这些失效 [9]。系统性失效本质上是由人为错误引起的。它们基本上是可以避免的，必须在开发过程中通过各种方法尽量减少。通过应对这些情况并采取预防措施，可以大幅减少系统性失效，否则会影响整个产品生命周期。这些问题可能源于各种因素，例如规格不正确、工艺缺陷、设计错误、制造错误或软件错误。虽然通常可以通过测试或调试过程消除软件错误，但解决错误规格问题可能需要对系统设计进行更全面的变更。

但是，由于项目的复杂性，这些类型的失效在 t=0 时可能不会出现，并且可能会随着时间的推移而出现。[9] 正因如此，IEC61508 标准指出：统计模型通常不适用于量化系统性失效。这些问题通常可通过定性方法来解决，包括通过系统分析和管理流程来识别和避免此类失效。在 图 3-3 中，您可以看到软件产品质量生命周期的概念视图，尽管此概念也可应用于硬件产品。

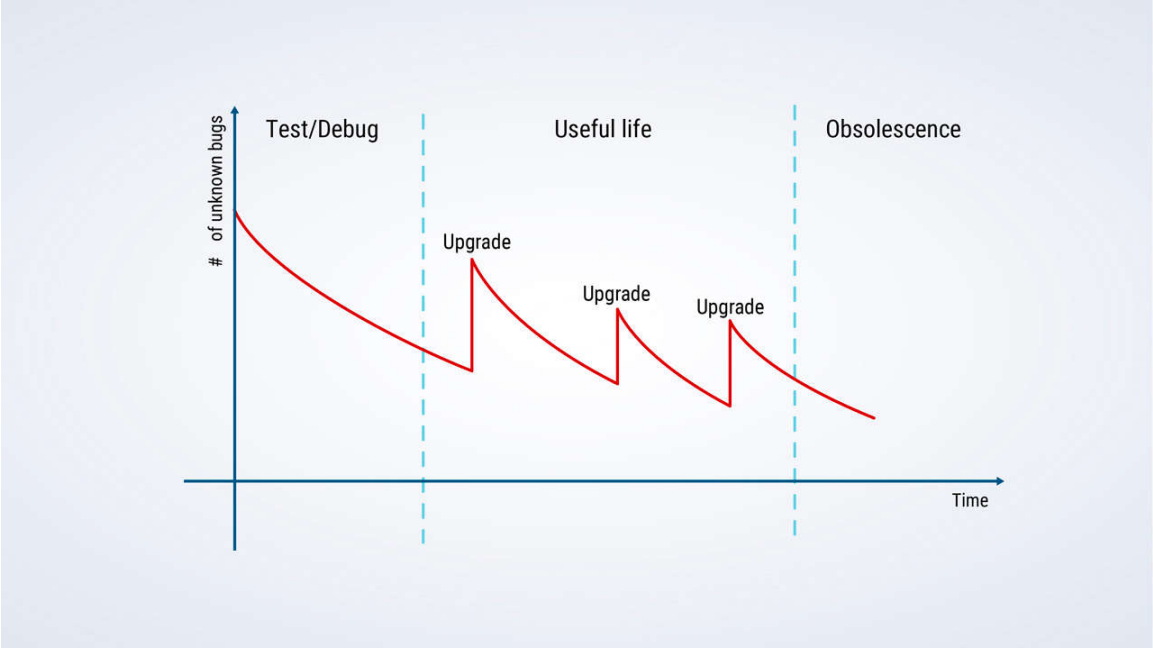

图 3-3. 软件产品的高质量生命周期

在产品生命周期开始时，通常会通过调试和测试来发现未知软件错误。随着时间的推移，错误数量会减少，可靠性会逐步提高。当软件升级时，会重复相同的周期。这种由系统性失效和消除错误引起的现象称为学习曲线或可靠性增长。[9]

4 片上系统 (SoC)：航天领域功能安全优势

SoC 器件的高集成度使设计人员能够在单个电路板组件 (CBA) 上构建高度复杂的功能。

如今，所用 SoC 的复杂性通常比其周围用于构建实际 CBA 的电路要高得多。

至关重要的是，在 SoC 设计阶段，供应商应尽可能避免任何系统故障。

高可靠性系统的设计人员依赖 SoC 本身的可靠性及其随附的所有开发工具。换言之，SoC 必须是根据托管流程开发的，以便能够正确评估 SoC 对 CBA 构成的风险水平。

电路越复杂，监控其正常运行和检测任何故障的工作量就越大。由于电流集成水平达到数亿个门，因此几乎不可能仅通过外部电路来测试和监控此类 SoC 的正常运行。SoC 供应商必须在硬件中内置自检和监控功能、才能实现令人满意的诊断覆盖率和有效的故障控制，详情请参阅 图 4-1。

根据 IEC61508 标准，所使用的 SoC 预先定义了完整设计中可达系统功能的限制 [11]。

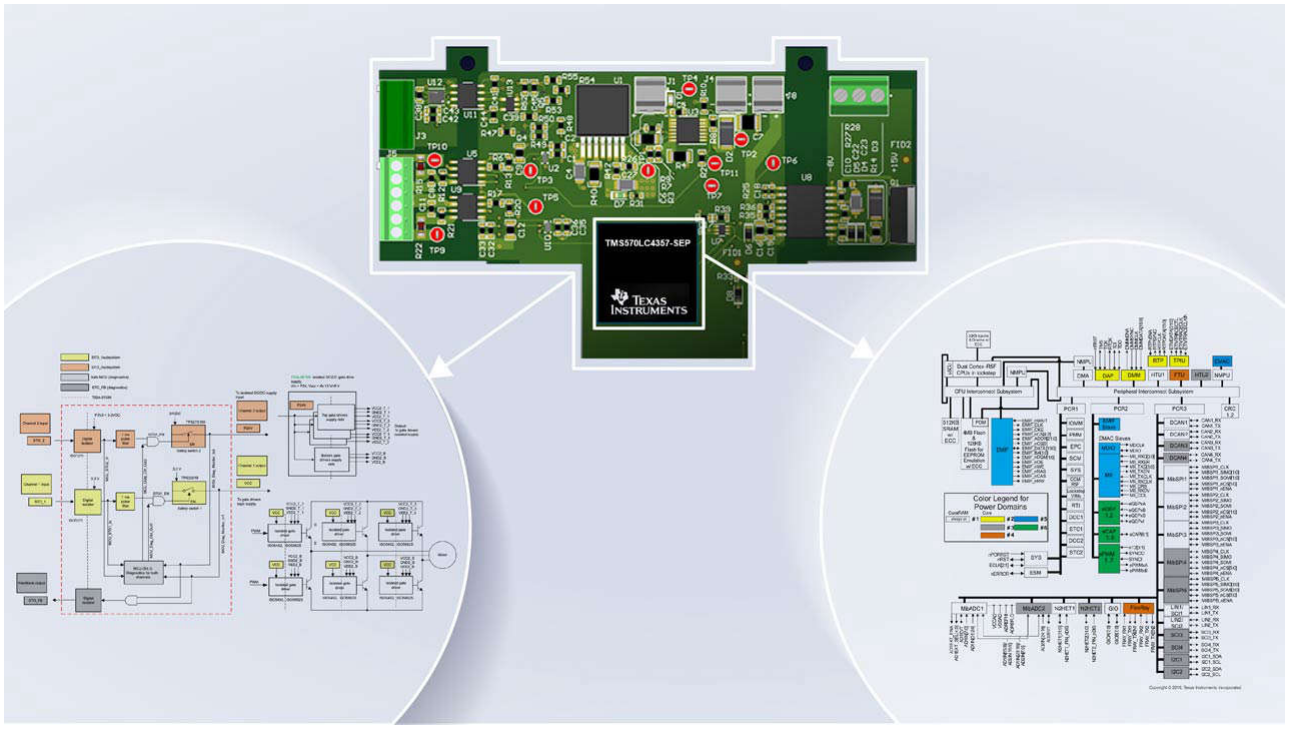

图 4-1. SoC 的复杂性远高于周围的电路

5 不断增长的系统级复杂性要求我们与半导体行业密切合作

硬度保证的特征是元件必须具有足够低的失效率，可满足实现 CBA 的可靠性目标所需的可靠性要求。硬度保证始终取决于元件所处的环境。随着航天工业的发展，人们对严苛和非常复杂的太空环境有了充分了解，并借助丰富的专业知识开发出了相应的测试方法，能够根据任务需要对电子元件进行验证。

可以对随机硬件失效进行统计建模，并获得可靠性灵敏值，例如按需平均失效概率 (PFDavg)、每小时危险失效平均频率 (PFH) 或平均失效时间 (MTTF)。

重要的是要明白，此类可靠性数据都是特定于环境条件的。

无法将商用现货 (COTS) 或车规级 (Q100) 器件的 FIT 失效率以纯数学形式外推到太空环境。当然还有一条途径，可以在不同环境之间应用修正因子 [12]。但是，太空处于一个严苛的环境条件中，会产生许多辐射。由于辐射测试不是 COTS 或汽车半导体器件特性的一部分，因此没有起始值可用于从中推断或应用任何修正因子。必须始终单独添加耐辐射特性。在超出其指定环境参数范围的情况下运行产品被视为系统故障。[9]

5.1 确认和验证 – 避免系统故障

硬件和软件开发流程必须遵循严格的流程，包括用于尽可能避免系统故障的所有开发工具。必须在整个开发阶段确认和验证复杂的 SoC。用户无法通过回顾方式合理确认和验证 SoC 的所有功能。

系统故障本质上是由人为错误造成的。

5.2 自监控功能

尽管我们一直在努力尽可能降低随机硬件故障的可能性或避免出现系统故障，但仍有发生漏检故障的可能性。快速检测此类故障并控制其影响非常重要。元件越复杂，集成此类故障的检测和控制功能就越重要。

强大的自监控功能允许在目标失效率方面做出很小的妥协，但只能在非常有限的范围内。如果随机失效过于频繁，系统需要同时处理多个故障，否则可能最终导致永久重新启动，从而导致可用性问题。通常，系统一次只能处理一个故障。发生故障的概率必须保持在非常低的水平，才能满足整体可靠性目标。

自监控和故障管理功能在各个行业之间仅实现部分重叠。

例如，汽车和航天领域确实都存在来自宇宙辐射的单比特和多比特干扰。但是，如果检测到此类故障，汽车系统通常会通过命令立即停止运行，然后立即检查（这可能包括调用牵引车）来寻求保持安全状态。卫星系统必须超越此类安全状态，必须在没有任何实际操作交互的情况下，在轨道上自主寻求系统的完全恢复。

快速可靠的故障检测是各个行业面临的一个常见挑战。图 5-1 显示了风险缓解的链接。

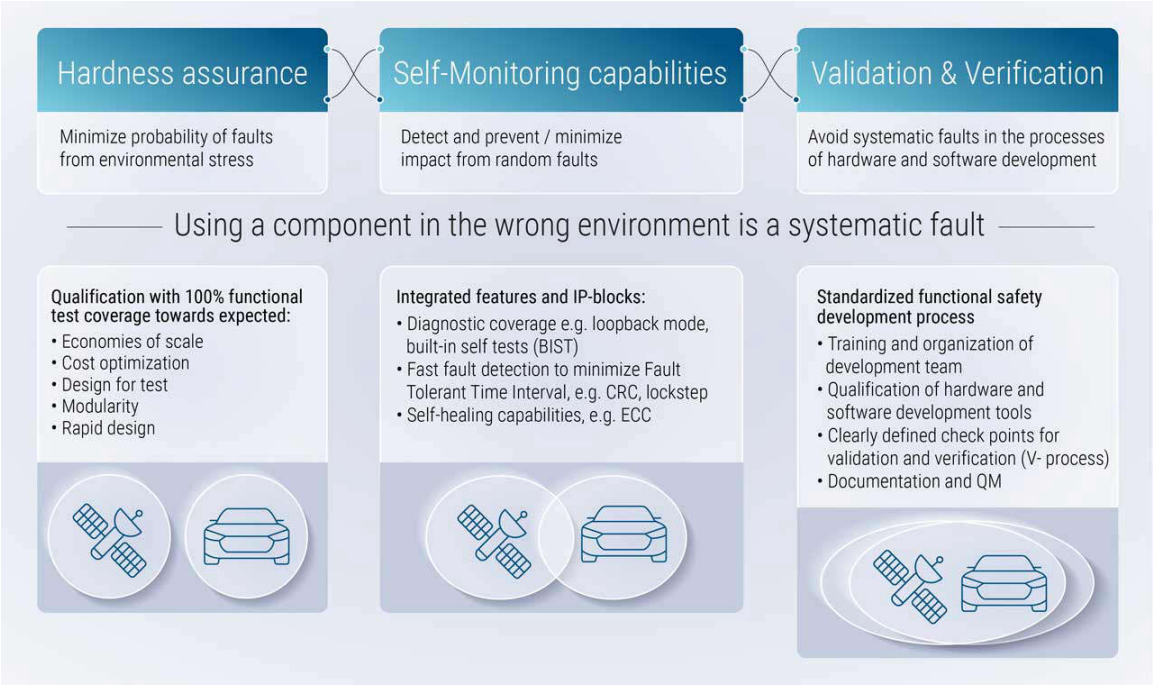

图 5-1. 缓解风险以实现“避免不可接受的风险”的三个链路

6 航天领域功能安全 SoC 示例

下面以 TMS570LC4357-SEP 为例进行了详细介绍，说明最初为 IEC63508 SIL-3/ISO26262 ASIL-D 应用开发的具有强大功能安全性的现有 SoC 如何根据其特性进行扩展，以适用于太空飞行领域，详情请参阅 图 6-1。

6.1 硬度保证

在航天应用领域，最需要考虑的是电子元件所处的严苛环境。必须根据电离辐射总剂量 (TID) 和单粒子效应来评估耐辐射性。对于数字或混合信号器件，采用 CMOS 工艺的单粒子闩锁 (SEL) 是器件因重离子而损坏的最常见原因。

TMS570LC4357-SEP 可耐受 30krad 的 TID 和高达 43MeVcm2/mg 的 SEL。

这款 MCU 可以在 -55°C 到 125°C 的极端温度下运行，并且可耐受近地轨道 (LEO) 卫星在极端温度之间的极速循环。这款 MCU 中使用的所有材料都符合太空需求，包括禁止使用纯锡来避免出现锡晶须，以及使用特殊的模塑化合物来使释气远低于典型要求。

TMS570LC4357-SEP 遵循 TI 航天增强型产品 (SEP) 标准。这包括受控基线等要求：单个制造基地、单个封测基地和单个材料组；延长产品生命周期、延长产品变更通知周期、提供产品可追溯性以支持长期产品安全。

6.2 确认和验证 – 避免系统故障

TMS570LC4357 产品系列的开发适用于汽车安全关键要求高达 ASIL D 或工业机械安全关键要求高达 SIL 3 的应用。该设计和相关工具的开发遵循 IEC61508:2010 和 ISO26262:2011 流程。TI 的硬件和软件开发流程已经过 TÜV Süd（硬件）[13] 和 TÜV Nord（软件）[14] 的审核和认证。

软件产品包括 HALCoGen（硬件抽象层代码生成器）、用于 TMS570 MCU 的基于 GUI 的初始化、配置和驱动程序代码生成器、以及相应的 HALCoGen 合规性支持包 (CSP)，从而帮助客户使用 HALCoGen 生成的软件来符合 IEC61508 和 ISO26262 等功能安全标准。此外，HALCoGen 测试自动化单元 (HALCoGen TAU) 可帮助用户为 HALCoGen 生成的驱动程序生成动态覆盖分析报告和回归报告，从而支持 ISO26262 和 IEC61508 评估。[15]

借助 TMS570LC4357-SEP 硬件和软件产品，用户可以开始进行高可靠性设计。

6.3 自监控功能

TMS570LC4357-SEP 的安全架构包括多种片上诊断功能，可实现高诊断覆盖率和近即时故障检测。

值得一提的一个非常重要的功能是 CPU 系统的锁步安全机制。

锁步 CPU 方案增加了一个“Checker CPU”，其执行的代码与主 CPU 完全相同。所谓的失效防护单元会比较两个内核的结果，并可以在随机故障导致结果差异时几乎立即进行检测。

为了验证共因失效是否无法逃逸，两个内核分别执行 1.5-2 个周期的代码，并且它们也实现了旋转和反转，以提供时间和物理多样性。

此外，会永久监控时钟和电压，并对所有存储器进行 ECC 保护，以保持软件执行产生的可靠结果。

硬件诊断包括用于 CPU、N2HET 协处理器以及外设 I/O 上片上静态随机存取存储器和环回功能的自检 (BIST) 逻辑。[16]

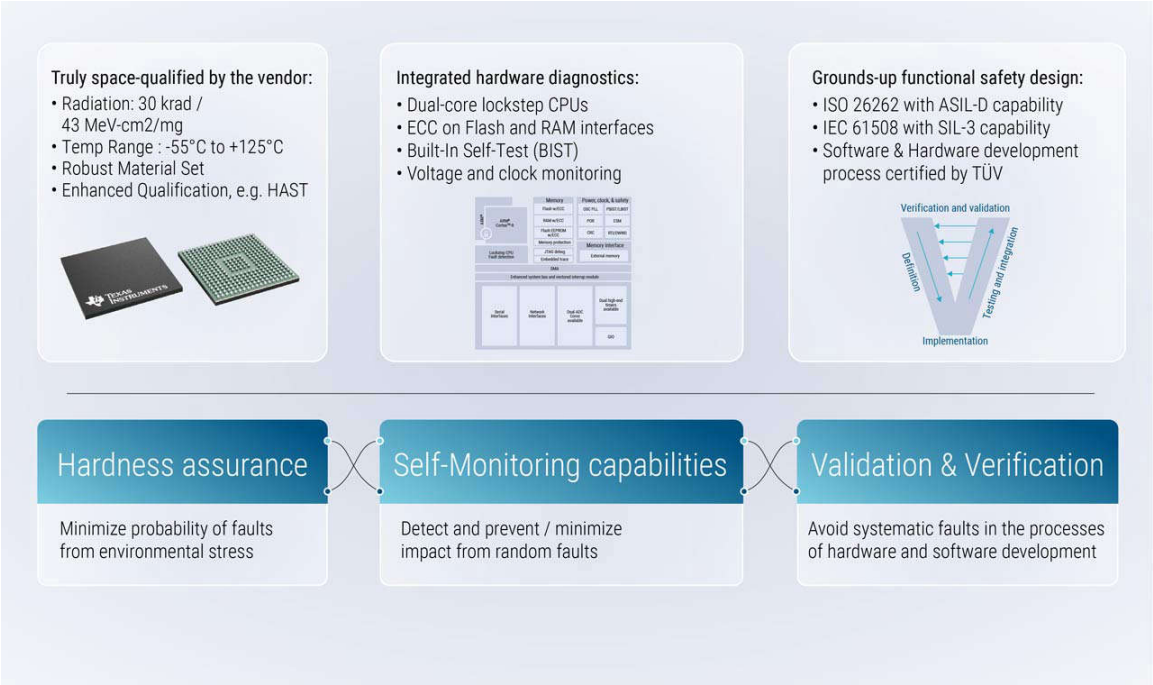

图 6-1. 功能安全 MCU TMS570LC4357-SEP：应用了风险缓解措施以实现“避免不可接受的风险”

6.4 近即时故障检测和恢复

图 6-2 展示了如何使用两个 TMS570 MCU 来构建冗余系统。当在主 MCU 器件上检测到随机故障时，会“通知”FPGA 出现不安全情况，以切换到冗余 MCU。由于能够近乎即时地检测任何故障，该系统可以满足飞行控制器、推进器、防撞或扩展坞系统等任务关键型子系统的非常严格的实时安全保护要求。以下示例展示了复杂 SoC 的精心设计的架构和依据功能安全标准进行的严格开发如何实现高可靠性，即使对于高度复杂的时间关键型应用场景也是如此。

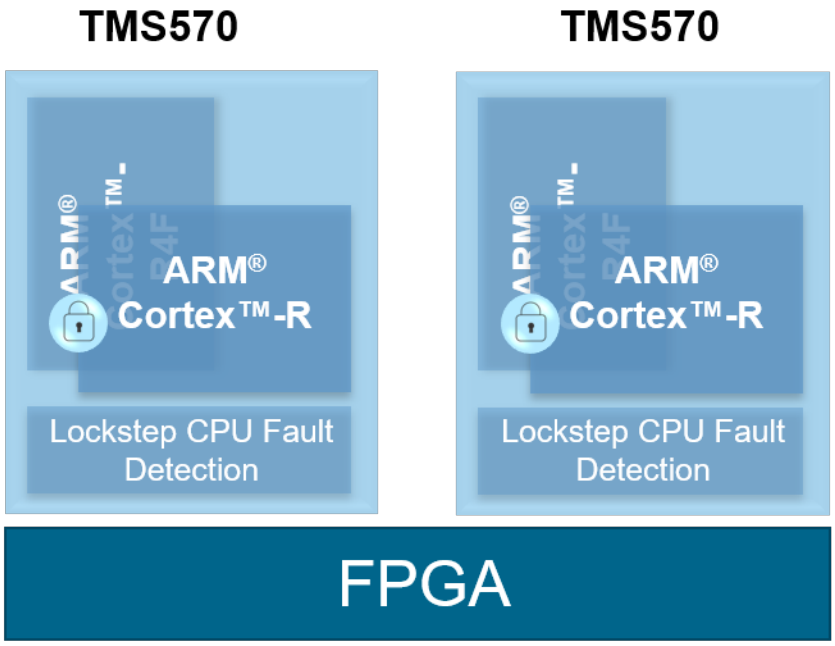

图 6-2. 两个 TMS570 MCU 构成高弹性实时系统

7 航天领域的未来发展需要新的战略思维

为满足航天工业对降低电子设计成本和加快其开发周期的日益增长的需求，汽车等以大规模生产为导向的行业可以在某些方面作为蓝图。E. W. Dijkstra 说：“简单是提高可靠性的先决条件”。这是非常正确的，但现代电子设计极其复杂，远非简单那么轻松。但是，如果将符合功能安全标准的 SoC 视为符合 RAMS 标准的子系统，则可以显著简化整体 RAMS 流程。值得关注的是，RAMS 标准可以为如何处理符合功能安全标准的电子设计提供更多指导，从而进一步有利于我们在太空设计中使用符合功能安全标准的 SoC。

8 摘要

“新太空”时代不断为太空电子设计师带来诸多挑战，他们必须处理越来越复杂的功能，他们被要求集成到单个电路板组件上、加快其开发周期，同时还需要控制成本，并且绝不允许牺牲可靠性。人们实际上可以观察到一种发展趋势，即，航天工业的需求逐渐转向满足汽车工业发展需求，汽车工业传统上也需要高可靠性和产品安全性，但必须长期应对成本压力。

高度集成的 SoC 可增加所需的功能。同时，如此复杂的 SoC 是对其设计的实际 CBA 整体可靠性水平的重要影响因素。通常，此类 SoC 由汽车工业驱动，因此适用于汽车设计的功能安全标准 IE C61508/ISO26262 为半导体行业提供了有力指导，可帮助提供强大的功能安全支持。

本文将基于 IEC61508/ISO26262 的功能安全方法与航天工业的 RAMS 方法进行了比较，并特别关注它们的主要共性：

它们有着相同的目标，即“避免不可接受的风险”，这两种方法都将风险定义为损害的严重程度与发生该损害的概率的乘积。

此外，这两个行业都将失效分为随机失效和系统性失效，旨在开发必要的方法来大幅减少失效并在失效仍然发生时控制其影响，从而降低总体风险。

基于这一点，我们将对复杂 SoC 及其支持工具可靠性的分析拆分为三个方面：硬件保证：量化随机失效的概率；确认和验证：尽可能降低系统性失效的概率；以及自监控功能：消除或至少减轻任何失效带来的影响。

符合 IEC61508 和 ISO26262 的功能安全标准提供了一种紧凑且结构良好的方法，通过定义的流程来设计符合功能安全要求的电子产品。我们使用安全完整性等级 (SIL) 对系统功能进行评级，从而能够对软件和硬件进行评估。这种方法代表了汽车、航空电子和工业机械等各个领域的先进电子设计水平。具体而言，由于 IEC61508 中定义了流程和指定方法，因此，可以避免硬件和软件出现系统性失效。特别是涉及强大软件的复杂设计（无论是作为开发工具还是作为实际产品的一部分）都受益于这种基于单一标准处理电子设计的所有可靠性和安全相关方面的方法，从而节省了工作量、迭代次数和时间。

功能安全 MCU TMS570LC4357-SEP 及其软件元件就是一个很好的例子，这些元件已通过 TÜV 等公告机构的安全合规性认证。其结果是降低了基于这种功能安全 SoC 的设计验证过程的复杂性。

9 参考资料

1. K. Bousedra (2023). Downstream Space Activities in the New Space Era: Paradigm Shift and Evaluation Challenges. Space Policy. BETA CNRS 7522，斯特拉斯堡大学，法国。 Space Policy 64 (2023) 101553.
2. ISO 9001:2015 (2015)，质量管理体系 – 要求第 9 章 - 绩效评估 (ISO 9001:2015)。
3. VDE (2023) Verband der Elektrotechnik Elektronik Informationstechnik e.V.Informationstechnische Gesellschaft im VDE (VDE ITG): VDE Positionspapier NeSC – NewSpace Communications NeSC – NewSpace Communications（德国法兰克福）。
4. IEC 61508-1:2010 (2010)，电气/电子/可编程电子安全相关系统的功能安全 - 第 1 部分：一般要求。国际电工委员会。
5. ISO 26262 (2018)。道路车辆 - 功能安全。Part 1: 词汇表。国际标准化组织。
6. 德国航空航天 DLR 中心（2024 年），图片来源：DLR (CC BY-NC-ND 3.0)。
7. NASA DFE 7 (1996) Fault-Detection, Fault-Isolation, and Recovery (FDIR) Techniques, Page 1 of 6 NASA. (1996). Design for Environment (DFE-7): Preferred Reliability Practices. 肯尼迪航天中心。美国国家航空航天局：https://extapps.ksc.nasa.gov/Reliability/Documents/Preferred_Practices/dfe7.pdf。
8. ECSS-S-ST-00-01C (2023) – 术语表，RAMS 第 50 页，可靠性 - 第 2.3.189 章第 39 页，可用性 - 第 2.3.21 章第 16 页，可维护性 - 第 2.3.149 章第 32 页，安全性 - 第 2.3.199 章第 40 页。
9. A. Birolini (2017) 8th edition- Reliability Engineering- Theorie and Practice, λ-Rate p. 390, FIT p. 36, MTTF p. 393 RAMS p. 407, bath tube- curve p. 6-7, environment p. 82, Springer-Verlag GmbH Deutschland.
10. DIN EN 61508-4 (VDE 0803-4) based on IEC 61508-4:2010 (2010), Part 4: Definitions and abbreviations, p. 5.
11. Gerry Creech (2014) IEC 61508 Systematic Capability (sagepub.com), Measurement and Control 2014, Vol. 47(4) 125 – 128 © The Institute of Measurement and Control 2014 Reprints and permissions: sagepub.co.uk/journalsPermissions.nav DOI: 10.1177/0020294014528895 mac.sagepub.com。
12. MIL-HDBK-217 MIL Handbook
13. P.Weiß, A. Köhnen, Matthias Ramold, Report of the Functional Safety Audit, 2013, TÜV SÜD Rail GmbH, Generic Safety Systems, Barthstraße 16, D-80339 München Functional Safety Audit: SafeTI Functional Safety Hardware Development (Rev. A).
14. Bianca Pfuff, Certificate QRAS AP00213 – SafeTI – Functional Safety Software Development Process, 2015, TÜV NORD Systems GmbH & Co. KG, Große Bahnstarße 31, 22525 Hamburg, Germany SEBS_A.165253_14_Cert_Process_TI_EN_V0_1.
15. 德州仪器 (TI)：*HALCoGen-CSP 用户指南*
16. 德州仪器 (TI)：*Hercules™ 微控制器：适用于安全关键型产品的实时 MCU*。

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