SEU、故障和系统级安全

Martin Cornes，ControlSafe 产品构架师；Dan Weed 可靠性和安全性工程师
2018 年 6 月

SEU 或单粒子翻转是设备或系统内存储元件的状态变化。这属于某种系统故障，但这种故障可能长达数年都悄无声息，因为系统会继续按预期运行。本文论述了如何能通过系统级方法减缓 SEU 和其他影响功能安全系统的潜在故障的负面影响。在不增加用户其他周期性或验证性测试要求的前提下，这能在系统寿命范围内将功能安全系统的预计危险故障率降低一个数量级。

ARTESYN™
EMBEDDED TECHNOLOGIES

设计或采购功能安全应用系统时，很多事项要考虑。最大问题之一是过于关注单独模块的主要或特定安全功能。这意味着，有时候可能会忽视整个系统安全性和可用性的大局。

目前有很多针对工业领域的功能安全标准，其中多数以 IEC 61508 为基础。EN 50129 是一个常用的铁路标准，部分内容源自 IEC 61508。这些标准的主要功能是确保系统安全流程能生产出安全的产品，并确定满足所需安全等级的各种要求。IEC 61508 和 EN 50129 均通过安全完整性等级 (SIL) 对安全程度进行了分类。最难达到的最高安全等级为安全完整性等级四级 (SIL4)。

并非所有功能安全认证都是对等的。两种产品经过认证达到一定安全完整性等级，并不意味着它们都同样适用于某个应用。这取决于产品提供的安全功能以及有哪些操作约束。

此外，经过某等级的 SIL 认证并用于系统中，并不意味着其满足您的需求。

安全功能和架构

让我们先看看安全功能和构架。为通过最高安全等级需要做些什么？概述如下：

- 系统必须通过有资质认证机构的认证。认证注重两个属性。首先，系统架构是否严格限制了产品生命周期内出现危害性故障的概率？第二，产品是由定义良好的流程开发的，目的是尽量减少设计失误的概率。
- 系统或模块必须清楚地定义由其执行的安全功能，以及必须由用户执行的功能。例如，用户可能必须执行定期测试或以特定方式使用系统（我们称之为“导出约束”并在安全手册中明确指出）。
- 虽然可能存在许多不同架构，但是对于较高等级的 SIL，安全相关功能需要有冗余。通常，这包括冗余传感器和多样性，以及主检查器配置，又叫二取二 (2oo2) 比较器，或三取二 (2oo3) 表决安排。
- 出于实际原因，某些安全关键数据经常必须通过未经过安全认证的网络元素进行传输，称为“黑通道”通信。这种情况下，系统端点必须进行某些形式的表决或检查，从而确认端点处数据交易的正确性。
- 冗余元素必须彼此真正独立。这意味着它们之间不存在共同的子系统，例如电源；它们之间的接口受到保护，以避免连锁故障，即一个故障的出现可能导致另一个故障的出现；冗余元素必须对振动、温度、污染、电磁干扰等任何其他常见因素具有抵抗性。
- 故障检测是关键！必须足够快速地检测和缓解任何影响安全功能的故障，以避免出现危险情况，并且必须足够快速到避免出现二次故障。通常在冗余通道中，二次故障可能导致安全功能无法运行。

冗余通道

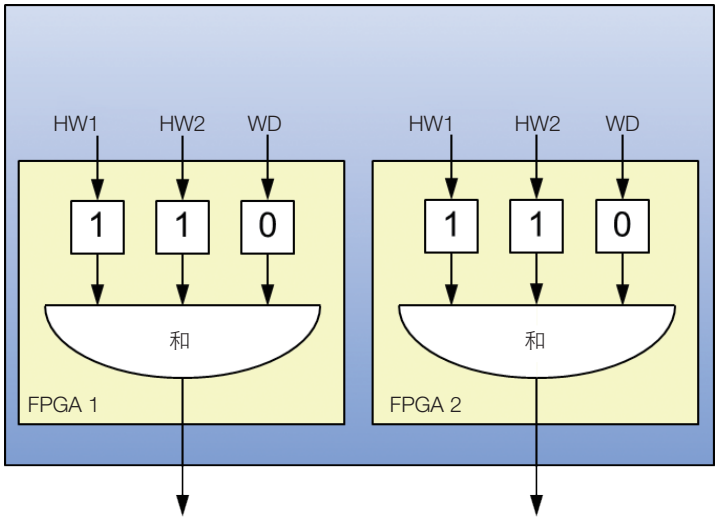
冗余通道不是能解决所有问题吗？冗余可以解决很多问题，但并不能解决所有问题。我们来看个简单实例。

安全系统能持续运行数周、数月甚至数年而不出任何故障。随着时间的推移，内部故障可能导致安全功能无法检测或响应自身故障。如果系统长时间保持健康状态，我们如何知道需要时它能检测/响应故障呢？

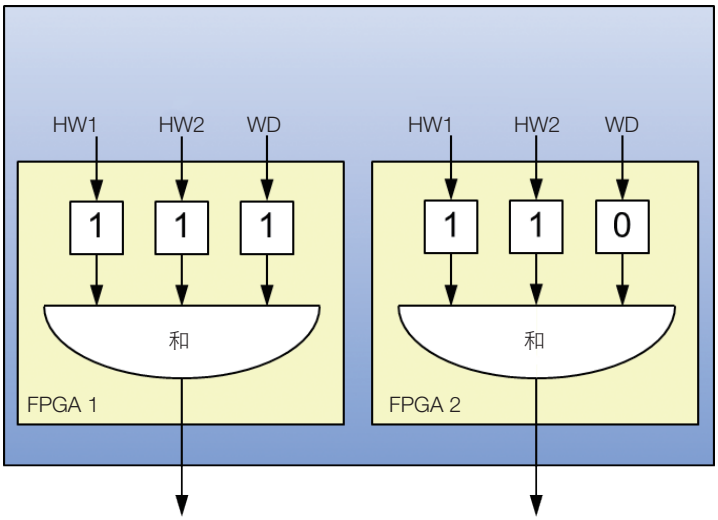
要解决这个问题，一个方案是向系统内注入故障，从而强制使系统响应故障。但这种“验证性测试”难度较大，较为耗时，一般需要将系统从运行状态下剥离。

让我们再深入一步，看看冗余安全监视器的实施实例。

下例中，两个 FPGA 分别监测 3 个信号，其中 2 个来自硬件（HW1 和 HW2）和一个软件监视器（WD）。监视器是冗余 FPGA 上一个简单的寄存器接口。在此场景中，软件应用程序需要将 WD 位设置为 1，告知 FPGA 它依然处于活跃状态；在该典型要求下，一旦软件应用程序出现不可预见的严重错误，监视器不会重置，硬件将启动故障安全功能。

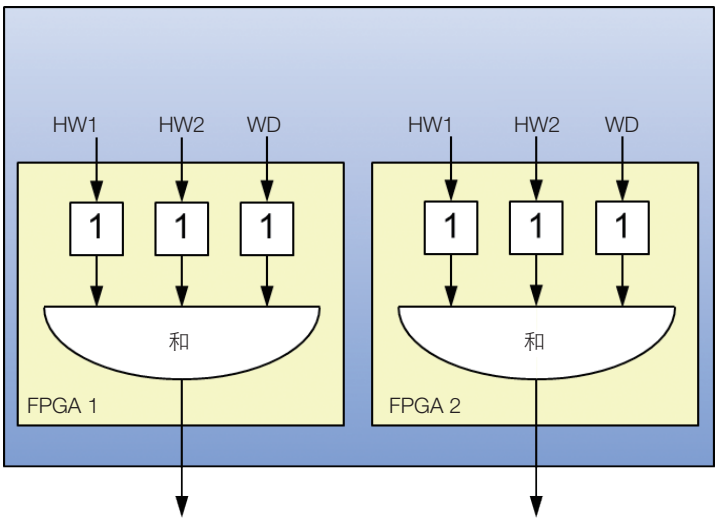


对我们的场景进行演练，如果软件运行状况良好，连续多年没有问题，但 WD 信号本身出现问题，或 FPGA1 内部出现卡位故障或单粒子翻转 (SEU) 等问题，那会如何呢？现在 WD 位停留在 1 位置，即使软件并未对其刷新。至此我们遇到如下问题。



我们遇到的是潜伏故障，这种故障无法检测出。但是至此我们依然没关系，如果该应用锁定且 FPGA1 WD 没有被重置，那么 FGPA2 依然会发现这种情况并启动故障安全功能。很好，那就是冗余的目的，不是吗？

如果过一阵子或过几年后，类似事件发生在 FPGA2 上，会怎样呢？该应用仍运行良好，未出现问题，但现在我们遇到如下情况。



该应用的运行情况一直良好。又过了几年，该应用遇到一个模糊的错误路径，无法重置监视器。因为硬件“看不到”该错误路径！现在我们面临潜在危险情况。这种危险情况很罕见，或许不太可能发生，但我们将在本白皮书下文中探讨该情况。

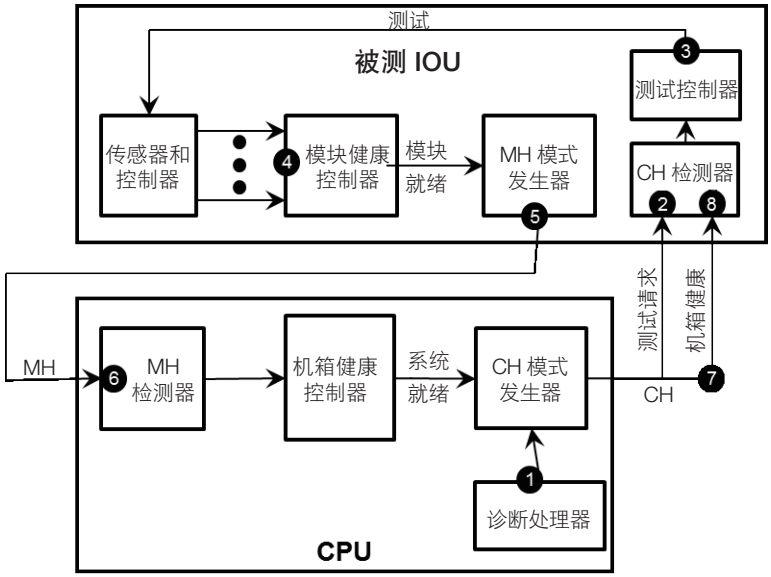
预防

那么您如何防止这种情况出现呢？

上述场景仅仅是一种可能出现的故障类型的实例。某些故障可从某个模块本地检测出，而有些则不然，至少在没有实际切换位以强制执行错误并观察其如何被检测到的情况下无法检测出。需要给出全机箱级解决方案，以使机箱内的任何故障都与控制模块通信，允许机箱启动故障安全功能，并将控制功能切换到另一台备用的正常机箱。这种附加保护可以将安全等级提高一个数量级，同时还能确保高可用性。

如上所述，验证性测试过程是实现这一点的办法之一。系统离线后强行注入故障，从而验证故障能否被检测和缓解。这种操作过程复杂且比较昂贵。例如，在雅特生科技 ControlSafe™ 计算机中，对进出 CPU 的以太网数据包逐位对比。为了验证这种比较结果，必须从每个 CPU 发送一个不匹配的数据包。这需要定制的应用软件。

为消除这种离线测试的需要，雅特生科技使用了一项获得专利的运行时间诊断流程。该流程可以检测出这类潜伏故障，并能验证系统对故障检测的响应。我们设计出一种可以周期性插入临时故障的系统，从而可以了解系统其他模块能否检测出故障。这些插入的故障持续时间短于 200µs，因此不会影响系统功能，也不会导致故障转移。



1. 诊断处理器向其中一个模块（自身、对等 CPU 或 IOU）发出测试请求
2. 所有模块都检测该测试请求，并忽略健康信号状态，直到测试结束
3. 目标模块操作板载逻辑，模拟故障发生
4. 模块的健康控制寄存器检测到该故障
5. 并导致模块健康信号被禁能

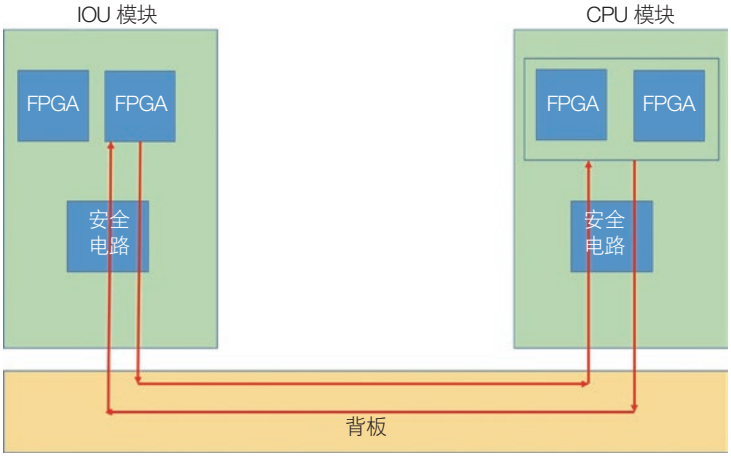
6. CPU 模块检测到被测模块异常
7. 这导致 CPU 机箱健康控制器将机箱健康状态禁能
8. 被测模块检测出机箱健康状态已禁能，断定测试成功并恢复正常运行
9. 将安排下一个待执行的测试

同样，所有这些动作在硬件中完成，因此完成时间不到 200µs。并且，这种内部故障测试可以通过标准测试协议在 CPU 模块内部或 CPU 模块之间完成，也可以在 ControlSafe™ 机箱内的所有模块之间进行。一般来说，24 小时内会自动执行完整的测试序列。

详细了解下这类测试为您提供的覆盖范围，我们先从源头注入一个短暂的故障开始。例如，可能会创建不匹配的数据包以供 FPGA 表决，或调整温度传感器的校准，导致其会在正常温度范围内跳闸。然后，我们就能通过如下项目测试是否检测到了故障：

- FPGA 响应了故障；
- 该模块上的安全电路响应了该故障并切换了状态；
- 安全电路内部生成信号，并将信号经背板传输至 CPU 模块；
- CPU 模块上的安全电路识别到故障；
- CPU 模块上的冗余 FPGA 可以正确处理信号，并将正确的响应发送到故障安全；
- 从 CPU 模块发出信号并经背板传输到被测模块；
- 信号经安全电路返回被测 FPGA，以检查是否生成正确的故障安全信号

至此，完整的端到端路径测试结束。这些测试通过全局健康测试控制器 (GHTC) 在 ControlSafe™ 机箱内按顺序执行。机箱中各模块都有自己的局部健康测试控制器 (LHTC)，在 GHTC 指令控制下安排内部测试。测试通过后，GHTC 安排下一次测试，并在各模块上继续执行。这功能为用户提供了极高级别的安全诊断覆盖范围，而该诊断对系统的正常运行是透明的。



计算

让我们从数学角度来看。如上所述，根据安全标准，需在设计时考虑许多注意事项，从而能检测并减轻故障，然而硅设备总存在一些无法检测到的硬件故障或 SEU，尤其是某些故障下，信号卡死在某个状态，导致设备表面看上去处于正常运行状态。问题是，如果第一个故障没检测出，冗余通道下出现类似故障时，能被检测出的几率又能有多大呢？如果出现这种情况，使用该信号的安全功能将失效，且没人知道情况。

安全标准对处理该问题有几种方法。IEC 61508 考虑系统生命周期内危险故障的整体概率；分析结果中必须包括未检测出的故障有何影响，周期性测试下某时间段内（数日至数月）检测出的故障有何影响，以及基本上当即检测出的故障有何影响。EN 50129 也根据故障出现的概率和冗余量对未被检测出的潜伏故障的持续时长进行了数学约束。

让我们通过一则实例了解下在一定样本量下，内部诊断是如何影响整体危险故障率的。

FPGA 和其他组件的故障率一般可以合理估算出。许多这种组件还受软错误率 (SER) 的影响。造成软错误的因素包括封装衰减、中子、外部 EMI 噪声、内部串扰以及诸如位置、纬度或高度等其他因素。SER 不确定性很大，因此所采用的假设结果十分保守。

在该实例中，我们采用的硬件故障率为 20 次故障/10 亿小时。这又叫 FIT 率（失效时间）。针对 SER 故障，我们需添加 200 FIT。这种总故障率表示单通道安全功能，即双通道系统的一部分。

并非所有故障都是危险且无法检测的。有些故障可以立刻检测出，例如即使温度正常，温度传感器也跳闸。我们感兴趣的是同一温度传感器无法跳闸的其他故障。在这个实例中，我们假设一半故障已检测出，另一半没检测出。实际情况下，针对每个组件会进行更为复杂的分析。但是在该实例中，假设每个通道未检测出的、具有潜在危害的总故障为 110 FIT。

接着，考虑运行达 25 年以上的大量系统。运行超过 25 年、平均每年 8,000 小时的 5,000 辆列车，总系统时间达到 10 亿小时。该预测很有用，因为在最高安全完整性等级下，目标是每十亿小时危险故障数小于一个。

下例显示以上文实例数据为基础得到的运行 10 亿小时时，单通道和双通道配置下 25 年后的故障概率和预计故障数量。

	HW FIT	SEU FIT	总 FIT	每年小时数	年数	单位运行小时数	单位故障概率	列车数量	系统运行小时数	系统故障数	25 年内系统故障数
首次潜伏故障	10	100	110	8,000	25	200,000	2.200%	5,000	1,000,000,000	110.0	110.0
二次潜伏故障	10	100	110	8,000	25	200,000	0.048%	5,000	1,000,000,000	2.42	2.420

第二独立通道的加入显著减少了预期危险故障总数，但其预期危险故障总数仍然比安全关键系统高出近 2.5 倍。问题在于，这些故障是随机且独立的，在整个系统寿命内可能会随时出现。一旦某通道出现未检测出的危险故障，整个系统实际上就会从双通道变为单通道。

对比该实例与下例。在此，每季度我们都进行内部诊断，检测未被检测到的内部故障。

	HW FIT	SEU FIT	总 FIT	每年小时数	年数	单位运行小时数	单位故障概率	列车数量	系统运行小时数	系统故障数	25 年内系统故障数
首次潜伏故障	10	100	110	8,000	0.25	2,000	0.022%	5,000	10,000,000	1.1	110.0
二次潜伏故障	10	100	110	8,000	0.25	2,000	>0.001%	5,000	10,000,000	0.00	0.024

请注意：25 年后单通道故障总数仍然与上文相同。差别在于两个通道出现故障的概率。一旦某个通道出现故障，在诊断程序运行并检测出第一个故障之前第二个通道得一直维持运行。在 25 年使用寿命中，两个通道同时出现故障并且都未被检测到的概率得到大幅度降低，在一定样本量中每 25 年出现该故障的概率低于一次。需注意的是，ControlSafe™ 系统一般每隔 24 小时周期就执行一次这些测试流程，不同于本例中按季度执行测试流程。

从上表不难看出，为什么这些安全标准需要平行冗余通道并强调故障检测功能。这有利于各模块实现安全所需的 FIT 级别。

如此看来，10 亿小时并不算很久！

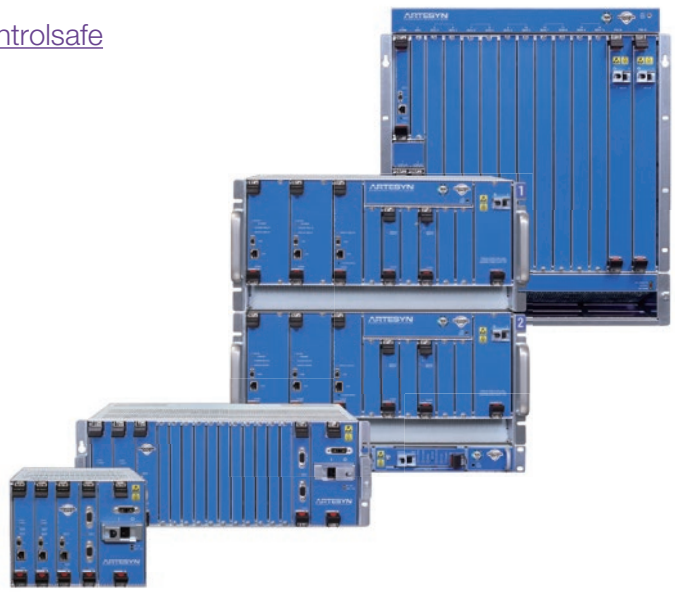
结论

在实施上述机箱或系统范围测试协议后，系统寿命周期内的预期危险故障率降低了一个数量级，而用户无需增加额外的周期性或验证性测试。基于马尔可夫 (Markov) 模型的更复杂分析表明：危险故障的概率减少了 4 至 50 倍，具体因安全功能而异。

机箱中所有模块成为自动化、系统化内部检测序列的一部分。机箱中每个模块都能进行其自身的内部测试，但它们通过通用协议处理这些测试并发送状态，以便 ControlSafe™ 计算机确定系统的整体健康状态，并在出现错误时切换至备用计算机，确保服务不被中断。

确保单个组件满足安全标准的同时得兼顾整个系统的安全性，这一点十分重要。这样做时，需要测试整个安全路径的一整套机箱级或系统级测试方案，以确保系统安全和最大程度减少对客户的影响，这种需求日益明显且必要。

如需了解雅特生科技 ControlSafe 平台的详情，请访问
https://zh-cn.artesyn.com/computing/products/category/controlsafe



ARTESYN™
EMBEDDED TECHNOLOGIES

关于雅特生科技

雅特生科技是电源转换和嵌入式计算解决方案设计和制造领域的全球领导者，其解决方案适用于多种行业，包括通信、计算、消费电子、医疗、军事、航天和工业。

凭借在开发高度可靠和可用的嵌入式计算机系统方面逾 30 年的专业技术，雅特生科技在商业现货 (COTS) 容错型计算机系统方面，已成为轨道系统集成商和轨道应用提供商的首选供应商。

根据长期以来的经验，我们深知客户对准时、一致、高质量产品以及出色客户支持的需求。我们的所有产品均从雅特生科技全球顶级工厂出货，并配有经验丰富的专家为客户提供支持。

为使客户尽快盈利，为确保开发过程尽量简单，雅特生科技不遗余力。通过当地的系统架构师和现场应用工程师 (FAE)，产品功能在全球范围内得到鼎力支持，帮助您保持进度。

我们灵活又敏捷。我们认识到，您可能需要赋予自有系统独特的品牌效果。没问题，我们已对此习以为常。通过我们提供的服务，您可以定义与贵公司品牌和审美标准一致的外观设计和格调。

我们的灵活性并不局限于外观和格调。我们设计了集成服务、独特的支持要求、长期供给、直发/直运和更多服务，旨在让您更轻松与我们展开业务并更快融入市场，确保部署更顺利。

四十多年来，客户一直信任雅特生科技，帮助他们缩短上市周期，让他们可以专注于新产品开发和增值服务。

雅特生科技总部位于美国亚利桑那州坦佩市，全球拥有超过 15,000 名员工，设立有多个卓越的工程中心、世界顶级的全资制造工厂以及全球销售和支持办事处。

联系方式

美洲 +1 888 412 7832

欧洲、中东和非洲 +44(0) 1384 842 211

亚太 +852 2176 3548

技术支持

美洲 +1 888 412 7832

欧洲、中东和非洲 0 800 0321546（英国）
+44 800 0321546（英国以外国家或地区）

亚太 +400 88 99 130（中国）
+86 29 8874 1895（中国以外国家或地区）

zh-cn.artesyn.com

联系地址
Artesyn Embedded Technologies
2900 S. Diablo Way, Suite 190
Tempe, Arizona 85282