使用SIL 2器件设计功能安全的SIL 3模拟输出模块

Brian Condell，产品应用工程师

摘要

需要安全完整性等级(SIL)3解决方案的制造商，在使用SIL 2器件时面临着多项挑战。随着工业功能安全标准IEC 61508第3版的发布，制造商必须采用新的方法。本文概述了一种能够克服挑战以成功实现SIL 3并加速产品上市的解决方案。

简介

过去几年，受以下多项因素的驱动，工业功能安全系统开始加速普及：

- 制造商希望使用新的复杂技术来降低成本（例如，使用安全扭矩关闭而不是再添加一个接触器）
- 实践证明，使用机器人（特别是协作机器人）可以提高许多工厂车间的生产率
- 认识到使用安全认证设备可以提高整体可靠性
- 确认使用诊断可以提高许多工厂和设备的产量
- 引入新的安全要求

另一个驱动因素是对能源、石油和天然气行业提出了严格的要求和监管义务。

在展开详细讨论之前，我们先看一些基本定义，以帮助各类读者更好地理解本文。

什么是安全?

安全就是指能避免发生不可接受的风险。例如，工厂车间内未加防护的旋转机器就是不安全的。

什么是安全功能?

安全功能是指为实现或确保安全必须执行的操作。安全功能的目的是降低系统风险。例如，如果上述旋转机器的前面安装了光幕，当手穿过光幕时，安全功能将会检测到光束中断，从而在手接触到旋转机器之前使其停止运转。

安全功能通常包括三个子系统。图1的安全系统用于检测危险液体的液位，并在充满时切断液流。

- 输入子系统（传感器，如液位传感器）用于检测值或状态
- 逻辑子系统（可编程逻辑控制器(PLC)）用于判断该状态是否危险
- 输出子系统（执行器）可采取行动来确保安全

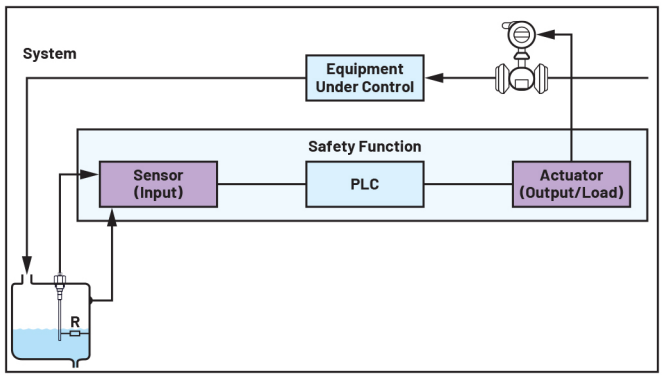

图1. 典型安全功能

什么是功能安全?

指系统在需要时执行预期安全功能的可靠性。它能有效地衡量功能安全工程师对光束中断时光幕和电机的停机安全功能会运行的信任度。

如果硬件指标（随机错误）、系统能力(SC)和共因失效(CCF)不会导致安全系统故障、人员伤亡、环境受损或生产损失，则认为该系统功能安全。

除了上述基本安全定义，还需了解设计功能安全系统时必须遵循的一些功能安全标准，及其相关优势。

制造商进行功能安全开发时，遵循IEC 61508或ISO 26262等标准，具有以下好处：

- 前期需求更清晰
- 测试期间较少出错
- 软件编写保持一致
- 集成过程中发现的缺陷更少
- 测试更全面
- 现场缺陷更少
- 与竞争对手相比，差异化程度更高

安全标准有很多（见图2），其中大部分源自工业IEC 61508标准。值得注意的是，所有标准的90%到95%要求都与IEC 61508的要求类似。

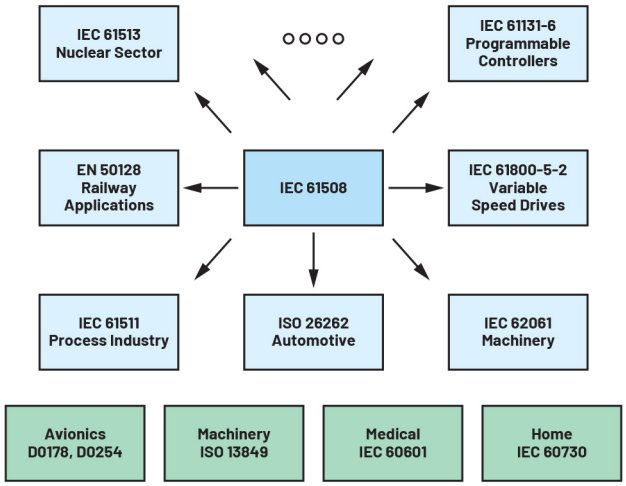

图2. 安全标准

本文重点介绍针对工业应用的IEC 61508标准，特别是如何使用SIL 2器件以相同冗余设计SIL 3解决方案。

冗余、高可用性和硬件容错

无论系统多么可靠，系统最终都会失效！两种常见的故障类型是系统性故障和随机故障。参见图3。

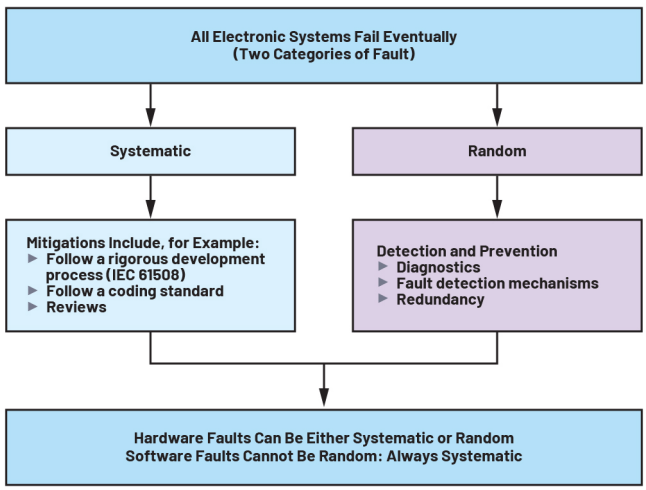

图3. 系统性故障和随机故障

冗余实际上是备用或冗余路径，当安全系统中发生故障时，它能执行预期的安全功能。值得注意的是，系统具有一定程度的冗余，并不意味着同时具有高可用性。只有冗余路径能够自动开启或激活时，它才具有高可用性。IEC 61508中常用的另一个术语是硬件容错(HFT)。HFT为N意味着至少出现N + 1个故障才可能导致安全功能丧失。需注意一点，不应考虑其他可能控制故障影响的措施，例如诊断。HFT是一种有效的手段，可确保硬件能够抵御故障，同时允许用户权衡HFT和SFF。参见表1。

表1. 硬件容错

元件的安全失效比率	硬件容错		
	0	1	2
<60%	不允许	SIL 1	SIL 2
60%至<90%	SIL 1	SIL 2	SIL 3
90%至<99%	SIL 2	SIL 3	SIL 4
≥99%	SIL 3	SIL 4	SIL 4

安全完整性等级

SIL描述了安全功能的完整性及其提供的降风险能力的相对水平。IEC 61508规定了四级SIL，SIL 1的安全完整性等级最低，SIL 4的安全完整性等级最高。表2比较了工业IEC 61508安全等级(SIL)、汽车(ISO 26262)安全等级(ASIL)和航空电子安全等级。请注意，这些只是近似比较。

表2. 各种SIL等级

IEC 61508	ISO 26262	航空电子
SIL 1	ASIL A	D
SIL 2	ASIL B	C
SIL 3	ASIL C/D	B
SIL 4		A

随着SIL等级的提高（从SIL 1到SIL 4），允许的故障率(FIT)依次降低。1 FIT相当于每运行十亿(1e9)小时发生一次故障。1e9小时约为10万年！有一点要注意，没有任何设备能够持续运行10亿小时，但如果100,000台设备运行一年，在此期间可能会出现一次随机硬件故障。安全失效比率(SFF)是检测到的安全加危险故障总数与安全功能中的故障总数之比。

$$Safe\ Failure\ Fraction\ (SFF) = \frac{(\lambda_{DD} + \lambda_S) \times 100}{(\lambda_{DD} + \lambda_{DU} + \lambda_S)} \quad (1)$$

- λ_{DD} = *Dangerous Detected Faults*
- λ_{DU} = *Dangerous Undetected Faults*
- λ_S = *Safe Faults*

表3显示了硬件容错为零(HFT = 0)时安全失效比率(SFF)和SIL之间的对应关系。

表3. SIL和SFF

SIL	SFF	每小时高需求率危险故障	理论上允许的危险故障
1	60%	$1e^{-5}$ (10,000 FIT)	每10年发生1次危险故障
2	90%	$1e^{-6}$ (1,000 FIT)	每100年发生1次危险故障
3	99%	$1e^{-7}$ (100 FIT)	每1,000年发生1次危险故障

问题/现有解决方案

对于许多采用功能安全的设计人员而言，尤其是使用IC进行设计时，问题在于获得认证可能很困难且成本高昂，而且还存在非常现实的不合规风险。设计人员必须创建系统级FMEDA，并且必须将ASIC视为黑匣子，因为他们不知道：

- 晶体管数量
- 内部故障机制
- 布局块大小
- IC的可靠性

因此，为了实现总体SIL目标，设计人员在FIT计算中必然会过于保守，在安全系统的其他部分中也会过度确保安全。这通常意味着需要使用外部诊断，例如外部ADC。这样做的问题是：

- 更加昂贵(BOM)
- 尺寸更大
- 更加复杂
- 系统软件存在额外开销
- 开发时间更长

除了这些问题，新版IEC 61508标准（第3版）的推出进一步加大了困难。

IEC 61508第3版

IEC 61508第3版目前计划的变更包括：明确警告慎用片内诊断来检测同一芯片上的故障，除非IC是按照IEC 61508开发的。它还计划包括类似于汽车ISO 26262潜在故障指标的要求。除了针对诊断功能的SFF之外，诊断电路也会有SC要求。

ADFS5758：率先通过认证的数据转换器

ADFS5758是一款单通道、16位电流输出DAC，集成动态功率控制(DPC)，具有内部基准电压源和众多片内诊断功能。图4显示了其功能框图。

ADFS5758的诊断/安全措施

- 主要片内诊断功能由ADC提供；如前所述，IEC 61508第3版计划澄清，一般不允许使用片内诊断来检测片内故障，除非IC是按照IEC 61508开发的
- 检查有无有效的读/写地址
- ECC校正
- 看门狗定时器
- 锁定配置寄存器的能力
- 内部偏置电压监视器
- 温度监控器

旨在满足以下要求：

- 工业工厂自动化
- 过程控制应用
- 高密度小尺寸PLC模拟I/O卡

安全功能：

接收数字输入码，产生精度在±2.5%满量程范围(FSR)内的输出电流。

根据IEC 61508开发：

- 硬件指标达到SIL 2
- 系统要求达到SIL 3

图5是ADFS5758的TUV Rheinland功能安全证书副本。

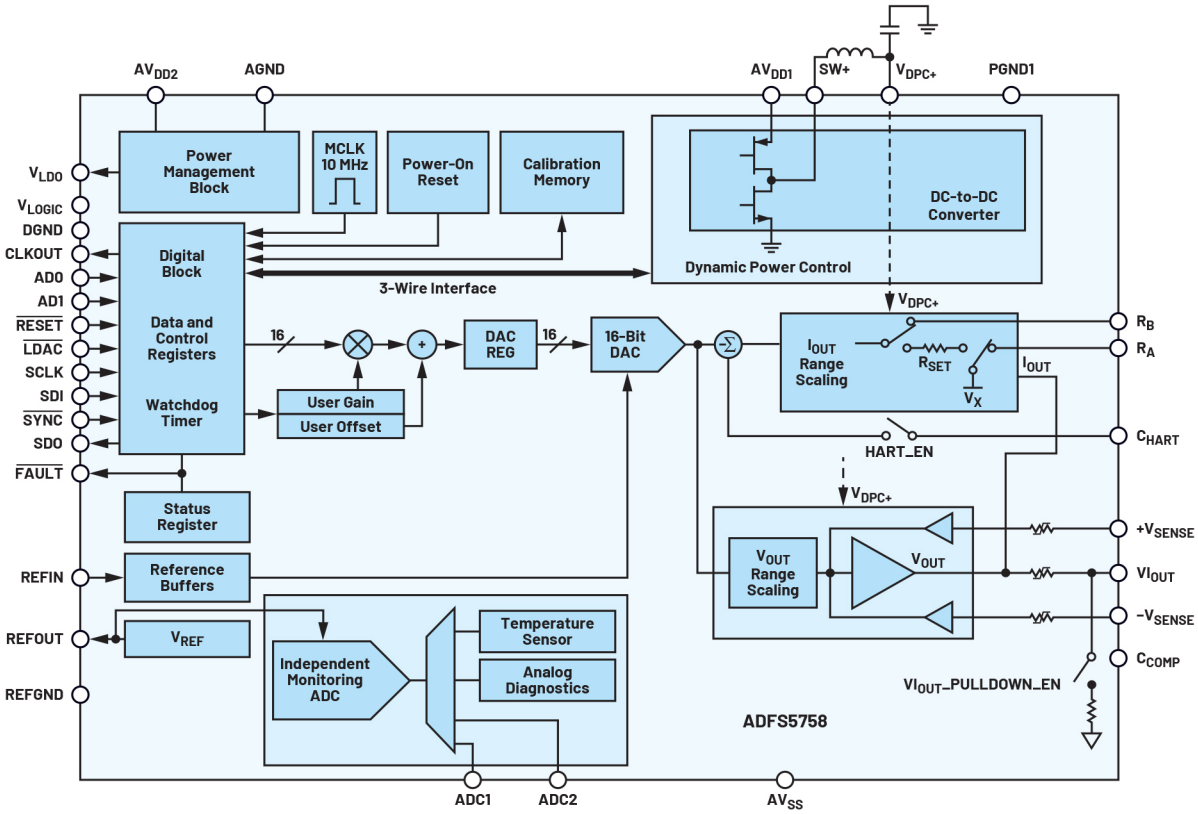

图4. ADFS5758框图

Certificate

TÜVRheinland CERTIFIED — Functional Safety — www.tuv.com ID 0600000000

No.: 968/FSP 2055.00/20

Product tested	16-bit Current Output DAC with Dynamic Power Control	**Certificate holder**	Analog Devices International Raheen Business Park Raheen Limerick Ireland
Type designation	see latest "Revision List"		
Codes and standards	IEC 61508 parts 1-2:2010		
Intended application	The 16-bit Current Output DAC with Dynamic Power Control is a compliant item and complies with the requirements of SC 3 according to IEC 61508-2. The implemented diagnostics are suitable to achieve a hardware integrity up to SIL 2 / HFT=0 and thus can be used in safety-related applications up to SIL 2 according to IEC 61508.		
Specific requirements	The instructions in the safety manual shall be considered.		

Valid until 2025-06-24

The issue of this certificate is based upon an examination, whose results are documented in Report No. 968/FSP 2055.00/20 dated 2020-06-24.
This certificate is valid only for products which are identical with the product tested.

TÜV Rheinland Industrie Service GmbH
Bereich Automation
Funktionale Sicherheit
Am Grauen Stein, 51105 Köln

Köln, 2020-06-24

Certification Body Safety & Security for Automation & Grid

Dipl.-Ing. Gebhard Bouwer

www.fs-products.com
www.tuv.com

TÜVRheinland®
Precisely Right.

图5. ADFS5758功能安全证书

图6显示使用ADFS5758的典型安全应用。

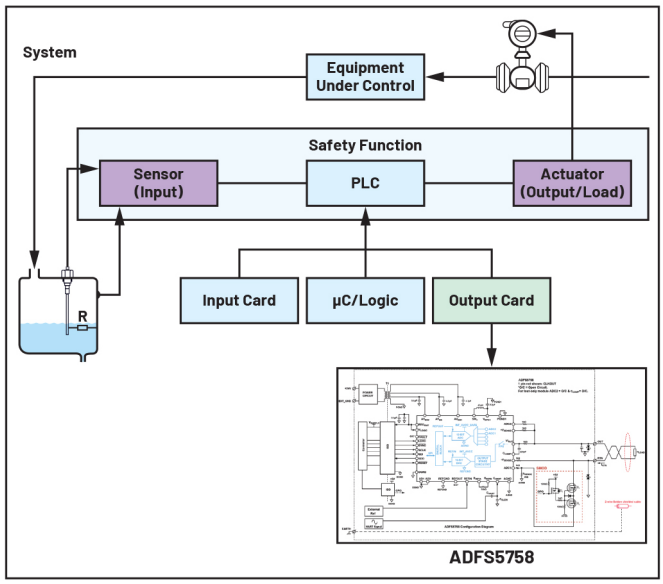

图6. 使用ADFS5758的典型应用

为使系统满足SIL要求，硬件指标（也称为架构约束）和SC都必须满足SIL目标。

架构约束

从硬件指标的角度看，并行放置两个SIL 2元件（相同或不同）可以让客户实现更高的SIL 3等级。参见图7。

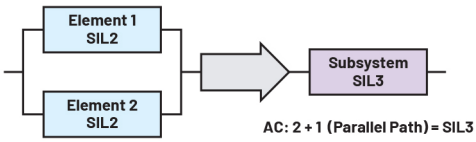

图7. 使用两个SIL 2元件实现硬件指标达到SIL 3的解决方案

系统能力

冗余可以通过多样化（不同）元件或相同元件来实现。

相同元件

使用具有同样SC的相同元件并不能改善整体系统能力，因为它们容易出现相同的类似CCF的温度峰值或压降，并且同一故障可能会导致两个元件同时失效。参见图8。

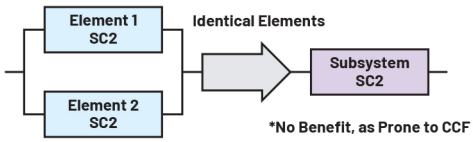

图8. 使用相同元件不会提高系统能力

不同元件

在冗余配置中使用不同的元件可以提高整体系统能力。参见图9。

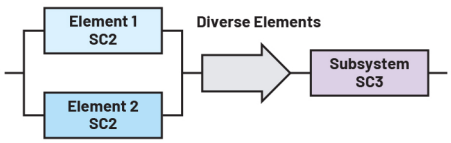

图9. 使用不同元件可以提高系统能力

由于两个元件不相同，所以同一故障不太可能使两个元件同时失效。

但在安全系统中使用不同元件时，相应的设计导入和测试工作量会显著增加，因此这种方法可能成本较高。

理想方法是使用两个相同元件来同时满足功能安全要求的整体能力和随机/硬件指标。

开发的系统能力比SIL高一级的重要性：相同冗余

如果系统中可以采用某个元件，并且该系统是按照比元件的SIL高一个等级的系统能力开发的，则可以在安全系统中使用两个相同元件来提供冗余，并提高整体系统能力。示例参见图10。

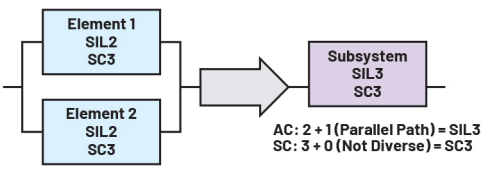

图10. 使用相同冗余实现SIL 3的示例

ADFS5758是按照比硬件指标高一级的系统能力开发的，因此，即使它在硬件指标或随机故障方面只通过了SIL 2认证，也可使用它来设计SIL3模拟输出模块。

结语

在安全系统中使用经过认证的ADFS5758可带来许多优势：

- 风险更小：满足TÜV要求
- 可以使用片内诊断（ADC和分布式诊断）
- 解决方案尺寸更小/给定空间中通道更多（由于使用集成ADC）
- 仅需少量外部元件（可靠性更高）
- 针对性的诊断（检测时间更短，覆盖率更高）
- 为系统级工程师提供关键数据(FMEDA)
- 系统软件的开销更少（软件中的诊断更少）
- 提供针对假设环境的可靠性分析
- 缩短客户的开发时间
- 提供相关文件（安全手册和TÜV评估报告）
- 适应未来的IEC 61508第3版标准

除了上述优势之外，ADFS5758还允许使用SIL 2器件以相同冗余设计SIL 3解决方案。

如希望进一步探索功能安全和ADFS5758：

- 请访问ADFS5758产品网页以了解更多信息。
- 订购ADFS5758评估套件以熟悉该器件。
- 浏览ADI公司的工业功能安全网页。
- 阅读ADI公司的安全事项博客。

作者简介

Brian Condell是ADI公司位于爱尔兰利默里克的工业连接和控制部门的IO-Link®产品应用工程师。Brian 1997年开始在ADI工作。他于2003年毕业于利默里克大学，获得电气工程荣誉学位。他拥有超过25年的半导体行业从业经验，先后担任过多种职位，包括FAB维修技术人员、IC布局工程师、模拟设计工程师、功能安全工程师，以及最近的应用工程师。他是经过TUV Rheinland认证的IEC 61508硬件/软件设计功能安全工程师。

在线支持社区

ADI EngineerZone™ 中文技术论坛

访问ADI在线支持社区，与ADI技术专家互动。提出您的棘手设计问题、浏览常见问题解答，或参与讨论。

请访问ez.analog.com/cn

©2023 Analog Devices, Inc. 保留所有权利。商标和注册商标属各自所有人所有。

“超越一切可能”是ADI公司的商标。