了解并延续Σ-Δ ADC的安全运行

作者：Miguel Usach Merino

摘要

新的国际标准和法规加速了工业设备对安全系统的需求。功能安全的目标是保护人员和财产免受损害。这可以通过使用针对特定危险的安全功能来实现。安全功能由一系列子系统组成，包括传感器、逻辑和输出模块，因而需要系统层面和集成电路层面的专门技能来提供具有适当功能组合的IC。本文以AD7770 Σ-Δ ADC为例，探讨如何构思和设计高性能IC以提供模拟域和数字域中的先进特性组合，从而简化安全系统的设计。

简介

墨菲定律变体之一："如果几件事都可能出错，首先出错的往往是会造成最大损失的那一件。"

如果一个系统可能产生直接或间接的致命威胁，例如机器故障等，那么设计该系统时，必须最大程度地降低故障可能性及其导致的负面影响。为了确保发生随机性和确定性故障的概率尽可能低，必须遵循特定的设计方法。工业中将这种设计方法称为功能安全方法。这种方法要求对系统进行细致入微的分析，确定所有潜在的危险情况，并运用最佳做法来将器件、子系统和系统的故障风险（例如电压过高或诊断失败等）降至容许的水平。

功能安全背后的理念是当检测到错误时让系统保持安全状态，例如：若来自外部传感器的转换结果超出范围，则断开使能的输出连接。

IEC-61508是工业设备功能安全设计参考标准，已针对不同行业进行了修改或阐释，例如ISO-26262适用于汽车行业，IEC-61131-6适用于可编程控制器。

根据功能安全标准进行设计可能相当繁琐，因为必须完成从上至下的细致分析，从整体系统描述到所用器件的内部功能模块都不能遗漏。为了保证系统具备足够高的保护水平，避免出现任何危险情况，并使未检出差错的发生概率最小，这种分析是有必要的。设计功能安全系统时，必须确保系统能够检测到所有错误，并以足够快的速度作出反应，使危险情况的发生概率最小，如图1所示。

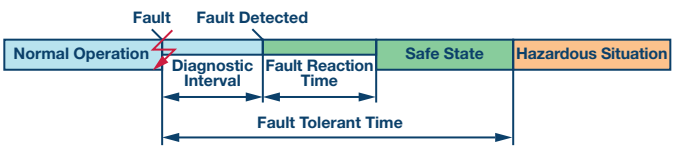

图1. 功能安全系统的反应时间

如何设计功能安全系统

危害分析的第一步是确定可能致人受伤的方式。对这些情况进行分析之后，系统设计应确保避免危险情况发生。如果存在无法避免的情况，应增加安全系统来检测该不安全状态并让系统处于安全状态。

为了更好地说明这个问题，假设存在图2所示的系统。根据油箱温度，一个连接到油箱的阀门打开一定的百分比以使爆炸风险最低。一个DAC通过一台电机控制阀门开口大小。所述系统称为开环式。

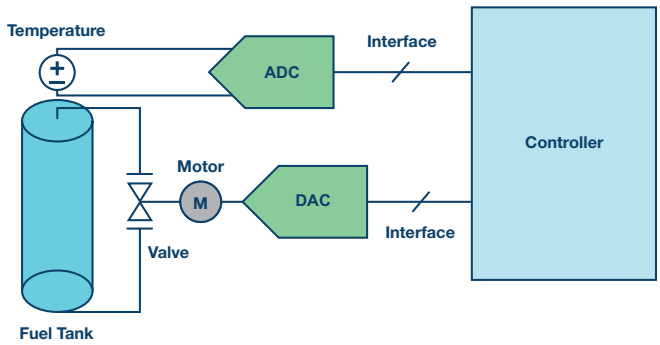

图2. 开环阀门控制系统信号链

危害分析揭示出有两种情况可能产生不确定状态：

- 温度测量错误。因此，阀门开口大小也不正确。
- DAC未能正确打开/关闭阀门。

下一步是评估各种危害的风险，公式如下：

$$Risk = probability\ of\ occurrence\ of\ harm \times severity\ of\ the\ harm$$

确定风险之后，下一步便是设计一个能将风险降至容许水平的功能安全系统。

IEC-61508定义了四个安全完整性等级(SIL)，这些等级规定了安全功能应将风险降至何种水平。有两种不同的目标概率：一是需要时失效，适用于处于待命状态且由事件触发的系统（安全气囊是一个很好的例子）；二是每小时失效，适用于持续运行的系统，上例就是这种情况。表1总结了以下标准的SIL之间的大致等效性：IEC61508、ISO 26262 (ASIL，汽车) 和航空电子关于期望需要时失效和每小时失效的标准。

表1. 不同标准的风险水平概算

PGA	阻性PGA	标准		
		IEC 61508 SIL 等级	汽车	航空电子
0.1 至 0.01	10^{-5} - 10^{-6}	1	A	D
0.01 至 0.001	10^{-6} - 10^{-7}	2	B	C
0.001 至 0. 0001	10^{-7} - 10^{-8}	3	C/D	B
0.0001 至 0.00001	10^{-8} - 10^{-9}	4		A

SIL等级是基于对未检出故障的降低和最小化程度来制定的，这里的未检出故障是指会使系统功能失常并可能触发不利状况的故障。

诊断覆盖率要求是多少？

未检出故障的概率随着诊断覆盖率的提高而降低。若系统能提供99%的诊断覆盖率，则可实现SIL3；若诊断覆盖率为90%，则可实现SIL2；若诊断覆盖率只有60%，则可实现SIL1。换言之，未检出故障的发生概率随着冗余程度的提高而降低。

实现SIL2或SIL3的较简单方法是采用已通过相应保护等级认证的器件。但这并非总是可行的，因为此类器件针对的是特定应用，其与您的电路或系统可能不完全相同。因此，之前通过SIL等级认证的器件，它们当初使用的认证标准可能不适用你的系统，而且你的系统保护等级也可能不相同。保护水平可能不相同。

实现高诊断覆盖率的另一种方法是在器件层面使用冗余设计。这种情况下，错误检测不是直接进行，而是间接进行，即比较两个（或更多）理应相同的输出。然而，这种方法会增加功耗、面积和系统的最终成本（成本问题可能最为关键）。

提高器件层面的错误检测水平和冗余度

一个常见的差错来源是外部接口中的数据传输：如果任何一位在传输中被破坏，数据便可能被接收器误解，并且可能产生不利状况。为了计算数据传输中发生的总差错，可以使用BER（误码率）。BER表示因为噪声、干扰(EMC)或任何其他物理原因而遭到破坏的位数和传输的总比特数的比值。

$$BER = \frac{bits\ corrupted}{bits\ transmitted}$$

系统的BER可通过物理方法加以测量。一般而言，许多标准规定了这一数值，例如HDMI®，或者可以使用估计值。现代数据传输的最低标准BER为10^{-7}。对许多应用来说，此数值可能太过保守，但可用于参考。

10^{-7}的BER意味着每1000万位中有1位遭到破坏。对于SIL3系统，每小时的目标最大差错概率为10^{-7}。如果系统在ADC和控制器之间传输32位数据，输出数据速率为1 kSPS，则1小时传输的位数为：

$$bits\ per\ hour = 32 \times 1000 \times 3600 = 115{,}200{,}000\ bits$$

这种情况下，误码率会提高到$1.5e^{-5}$，这只是一个接口的贡献；传输差错的总贡献应保持在总差错预算的0.1%到1%之间。

对于这种情况，可通过增加CRC算法来检测差错。可检测到的损坏位数由CRC多项式的Hamming距离定义，例如$X^8 + X^2 + X + 1$的Hamming距离为4，能够在传输的每帧中检测到最多3个损坏位。表2总结了CRC Hamming距离为4时根据每小时传输的不同位数得出的差错概率，假设传输32位数据加8位CRC。

表2. CRC Hamming距离为4时的差错概率

每小时数据位数	每小时未检出差错的概率
144,000,000	$2e^{-14}$
432,000,000	$6e^{-14}$
2,160,000,000	$3e^{-13}$

CRC诊断水平可通过如下方式来加强：回读写入的寄存器，确认数据传输正确。此操作会提高诊断水平，但所用CRC多项式的差错检测水平必须能够检测BER概率所决定的预期损坏位数。

如何使故障概率最小？

若制造商宣称某个器件针对功能安全系统而设计，其应能够提供FIT以及更为重要的故障模式、影响和诊断分析(FME(D)A)。此数据用于分析特定应用中的IC，计算系统的诊断覆盖率(DC)、安全失效系数(SFF)和危险故障率。

FIT衡量器件的可靠性。IC的FIT可根据加速寿命测试或IEC62380、SN29500等工业标准来计算；工业标准将应用的平均工作温度、封装类型和晶体管数量视为产生FIT预测结果的因素。FIT只是关于器件可靠性的预测，并不提供关于故障根源的任何信息。一般而言，除非能够直接或间接检查每个功能模块，否则最终差错概率将会太高而无法满足任何SIL2或SIL3安全功能的SIL目标。

FME(D)A的目的是提供一个全面的文件来分析芯片中实现的所有模块、模块失效的直接或间接后果以及支持故障检测的不同机制或方法。如之前所述，这些分析是基于特定信号链/应用而完成的，但其详细程度应足够高，据此可以轻松生成针对其他系统/应用的FME(D)A分析。

∑-Δ ADC可能出什么错？

对∑-Δ ADC的一般分析揭示出了此类器件的内部复杂性所引起的多种错误来源：

- 基准电压断开连接/受损
- 输入/输出缓冲器/PGA受损
- ADC内核受损/饱和
- 内部稳压器电源不正确
- 外部电源不正确

只有某些问题会在器件模块中产生故障，但存在其他不像上面所列那么明显的故障原因：

- 内部键合线受损
- 键合线与邻近引脚短路
- 漏电流增加

例如，若V_{REF}漏电流增加以致在内部基准电压上产生压降，器件能否检测到这一情形？为检查此类故障，ADC应能选择不同的基准电压进行转换，并将V_{REF}用作转换输入。

若内部熔丝位再生或发生其他损坏，可能导致上电时加载不正确的配置，对此应如何进行检测？这些都是可能出错的一些事例，即使其发生概率非常低。所有潜在故障（尤其是非常罕见的故障）及其检测方式（如有），都必须在FME(D)A文件中做好记载。此文件总结了基于特定应用和/或配置的故障及所做的假设，目的是最大程度地提高检测水平，使未检出差错最少。

ADI公司的现代化Σ-Δ ADC，比如AD7770、AD7768或AD7764，通过多个诊断检测器来提高容错保护，并检测数字模块和模拟模块中的功能错误。下面是此类模块的一些例子：

- 用于熔丝位、寄存器和接口的CRC校验器
- 过压/欠压检测器
- 基准电压和LDO电压检测器
- 用于PGA增益测试的内部固定电压
- 外部时钟检测器
- 多个基准电压源

除了这些特性，AD7770 ADC还集成了一个辅助12位SAR型ADC，它可以用来提高器件的诊断能力，例如：

- 实现其他架构以得到某些好处，比如提供不同的EMC抗扰度
- 它通过不同的电源引脚供电，故而可以用作基准电压源
- 其速度非常快，用作监视器时，在一个Σ-Δ 通道的单次转换期间，它可以监视8个Σ-Δ通道，但该SAR型ADC的精度和Σ-Δ ADC的精度不同
- 它利用不同的串行接口(SPI)提供转换结果
- 提供所有内部电压节点的测量进行诊断，比如外部电源、V_{REF}、V_{CM}、LDO输出电压或内部基准电压。

图3显示了AD7770 ADC的内部框图。内置监视器的模块用绿色突出显示，对红色突出显示的模块可以进行主动监视。

结语

为保证功能安全，须提高系统/模块监视和诊断覆盖率，以降低未检出错误的数学概率。提高覆盖率的较简单方法是增加冗余，但这会给系统带来多方面的不利影响，尤其是成本。ADI公司最近的一些Σ-Δ ADC，比如 AD7124或AD7768，实现了许多内部错误检测器，这样可以简化功能安全系统的设计，使整体复杂度低于其他解决方案。AD7770是精密Σ-Δ ADC设计的典范，集成了监视和诊断能力，包括通过内置冗余转换器来使诊断覆盖率达到最大，这使其成为超越一切可能的卓越产品。

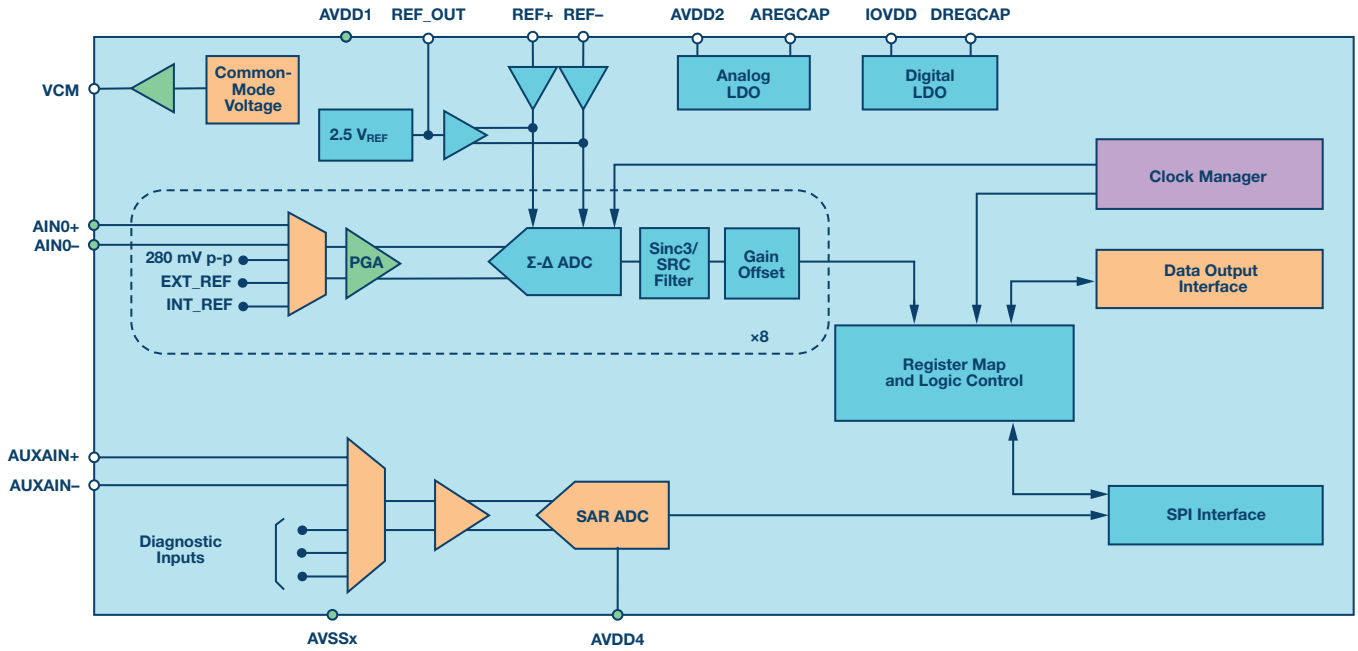

图3. AD7770 ADC的诊断和监控模块

Miguel Usach Merino [miguel.usach@analog.com]获瓦伦西亚大学电子工程学位，2008年加入ADI公司，任西班牙瓦伦西亚线性与精密技术部的应用工程师。

Miguel Usach Merino

该作者的其它文章：

ADC中的集成式容性PGA：重新定义性能

第50卷第3期