数据采集系统的功能安全

作者：Chris Norris

简介

功能安全是诸多行业整体安全策略的一部分，其目的是将对人或作业设备造成伤害的概率降至可接受的范围以内。近年来，人们对系统功能安全的要求显著增长。从核电站到医疗设备，无故障系统已成为部分应用的理想选择，也是其他应用的必备条件。例如，在传感领域，获取的数据如果不正确或遭到损坏，结果可能具有破坏性，甚至可能致命，具体取决于系统和所涉及的风险级别。

传统上，系统开发人员有责任将诊断和故障预防机制集成到其产品当中，确保来自传感IC的数据的完整性。但其代价是会增加PCB面积、物料成本和处理开销，最终会导致费用增加。从那时起，通过与系统设计工程师的广泛合作，人们开发出了一种解决方案来解决这个问题。为此，人们已经开始在IC级设计中考虑功能安全特性。

本文旨在从确保数据采集系统整体完整性的角度，探讨通过ADC实现功能安全的潜力。

传统的功能安全解决方案与更佳的方式

在图1中，我们看到的例子是一个多年以前的功能安全系统，我们将它与更现代的解决方案进行比较。其核心是数据采集ADC，它负责转换模拟输入并将数据传输到微控制器。然而，要实现这一解决方案，需要采用许多外部元件，重复执行SPI事务，甚至需要一个冗余ADC，结果极大地增加了物料成本、PCB面积、处理开销和成本。同时还会给系统设计人员带来额外的负担，比如，增加开发时间，降低可靠性等。

有一种单IC解决方案，只需极少的外部元件即可运行功能安全特性。

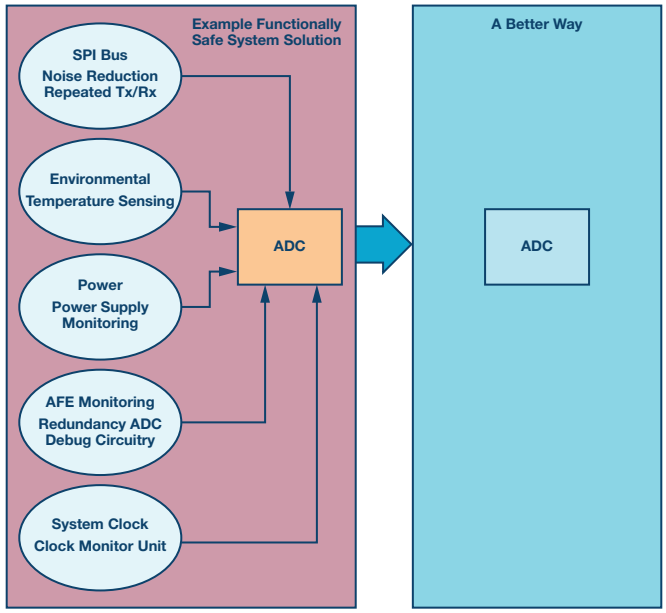

图1. 从多组件功能安全系统到单芯片ADI解决方案的集成。

具有功能安全要求的示例系统

在包含ADC的数据采集系统中，可能发生多种故障，根据具体的应用，这些故障可能会增加人或机器的健康风险。系统设计师必须区分可接受的风险和不可接受的风险。

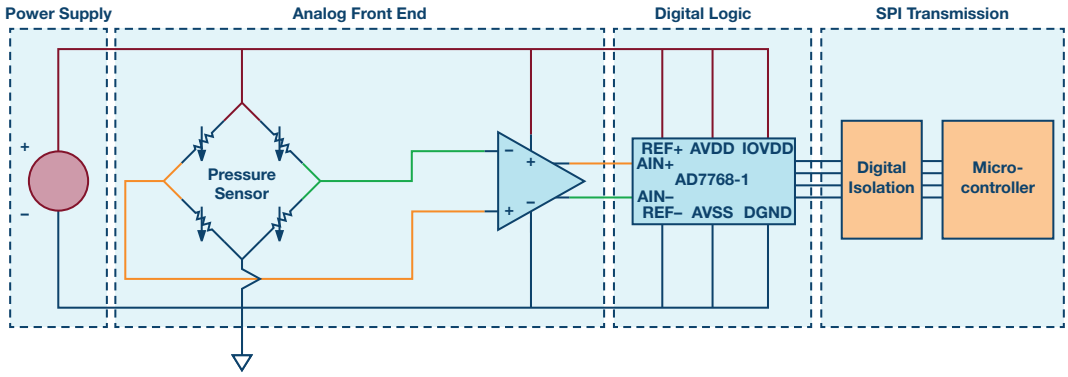

图2. 识别压力传感器系统中的潜在故障源。

例如，在气室压力测量和调节系统中，如果罐内压力不能大幅偏离外部压力，则可将使用容差为5%的传感器的做法视为可接受的风险。然而，如果微控制器接收到错误的ADC数据，结果可能导致致命的事故，腔室中的压力可能导致内爆或外爆，这两种情况都有可能导致附近的人受伤或死亡。这种风险水平是不可接受的。因此，必须实施一些功能安全措施，确保控制器接收的信息的完整性。

可能导致这类错误的一些故障源为

- 电源：电源电压低，低压差 (LDO) 调节器的输出电压低。
- 模拟前端 (AFE)：传感器受损，或放大器驱动到 ADC 的电压不正确。
- 数字逻辑：数字域中发生可能影响转换结果的误码。例如，工厂增益或偏移调整系数。
- SPI 传输：由于传输线环境嘈杂，转换数据的传输和命令的接收中存在误码。
- 环境：超出 IC 的额定环境温度。

AD7768-1是ADI公司功能安全产品组合中的Σ-Δ ADC之一，具有广泛的诊断特性，能赋予用户误码检测和诊断以及其他能力。图2突出显示了典型压力检测系统中的部分可能故障源。

用ADC诊断系统错误

借助ADI公司的ADC功能安全产品组合，用户可以用ADC帮助诊断和/或减少系统错误。这种系统误差测量能力对于保持精确测量极为重要，并且在具有功能安全要求的系统中，这种准确性甚至更加重要。

从参考输入获取的正负满量程电压用于测量系统的增益误差。通过零电平内部短路测量失调误差。然后，用户可以使用ADC的增益和失调调整寄存器来调整系统的失调和增益误差性能。

温度传感器识别IC局部温度的变化，包括超范围温度。在对失调和增益误差温度漂移敏感的系统中，这可能是一项具有吸引力的功能。如果温度变化较大，用户可能会决定在该新温度下调整增益和失调误差。图3说明了如何在AD7768-1内部将模拟诊断多路复用器连接到ADC。

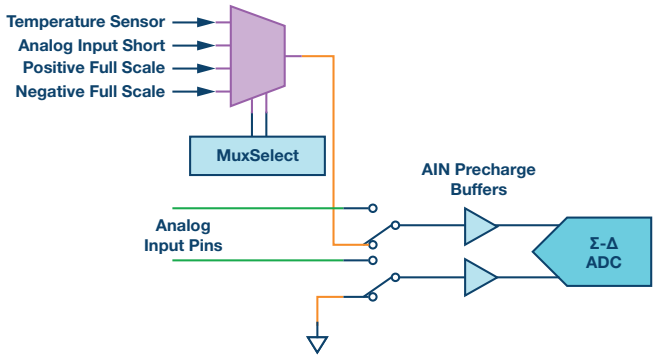

图3. 模拟诊断多路复用器转换开关。

诊断错误标志：寄存器映射诊断状态指示器

可以使能多个诊断特性，并且通常可以通过寄存器映射将其状态告知用户。发生故障时，会在寄存器中设置错误标志。用户可以在收到故障警报后进一步调查。

接下来，我们探讨可能发生并且可以通过ADI功能安全ADC产品组合进行诊断的一些真实故障。我们首先假设，我们的压力传感器系统装在一个工厂里，其工作温度波动不定，由于基本维护工作而多次停电，并且周围工业环境产生的电磁干扰(EMI)有可能被传导至系统PCB上。

ADC电源错误

我们假设，由于工作环境温度高，并且系统功率循环会引起电流冲击，所以，负责ADC的LDO电源输出的LDO电容已经磨损和损坏。使这些输出维持在已知电压，需要采用一个外部电容，这对于整个系统正常工作至关重要。如果电容器因该故障损坏，用户可能会发现，转换后的ADC数据或其他功能的性能会出乎意料。通过使能LDO监视器，一旦电压电平降至某个跳变点以下，系统会设置错误标志以提醒用户LDO输出的问题。

模拟前端错误

我们假设，在该系统中，ADC的输入不得超过ADC的满量程范围。如果用户意外地将不正确的值编程到增益寄存器，导致ADC看到的电压大于满量程范围，结果就会极大地影响系统的增益误差性能，我们应该将此视为一种严重的风险。但是，**滤波器饱和**错误检查器监视ADC输出，会提醒用户注意超出范围的模拟输入。

数字逻辑随机误码

在数字逻辑和存储器模块中偶尔会发生随机误码。在我们的示例压力系统中，我们假定，在上电期间加载默认出厂失调设置时发生了一个误码。这是一种无法容忍的故障，因为它会扰乱系统的默认失调误差，影响转换结果。在ADI功能安全ADC系列产品中，有一些功能可以定期在各种存储器模块上运行循环冗余校验(CRC)，并在发生误码时向用户指示故障。通过重置系统可以解决所有这些故障。

SPI传输错误

每个沿介质传输数据的系统都会产生一些误码。

可以估算每个系统出现这种情况的速率，我们将其称为误码率(BER)。

在我们的示例压力系统中，可以假设BER小于10^{-7}，通过数字隔离传输到同一PCB上的微控制器，传输距离为10厘米。

我们假设，部分电磁干扰被传导到SPI线路上，结果导致从AD7768-1到微控制器的转换ADC数据传输中出现误码。如果掩盖了气室中任何正在积聚的压力，ADC数据中的误码可能造成极大的破坏性。通过在发送数据的末尾附加CRC，用户可以识别传输期间是否发生了误码，并且可以重新检查ADC转换结果。

外部主时钟错误

如果用户需要在压力传感器应用中拒绝主电源的频率(50 Hz/60 Hz)，那么精确的低抖动外部主时钟源对于将数字滤波器陷波与正确的频率对齐至关重要。如果源断开、破损或损坏，结果会成为一个大问题，因为主电源的某些频率成分可能在转换后的ADC数据中可见。

如果外部时钟源未成功连接或已被移除，则外部时钟认定器可向用户指示错误。然后，用户可以使用内部RC振荡器执行紧急转换，同时在外部主时钟源上执行基本维护。

POR标志

系统上电或成功复位后，ADC中的POR标志将置1。

但如果发生意外复位，用户可能会在ADC数据中看到意外结果。他们可以通过检查POR标志来识别这种意外复位。

图4显示了AD7768-1中有多少这些内部诊断特性与它们要监控的功能相关联。

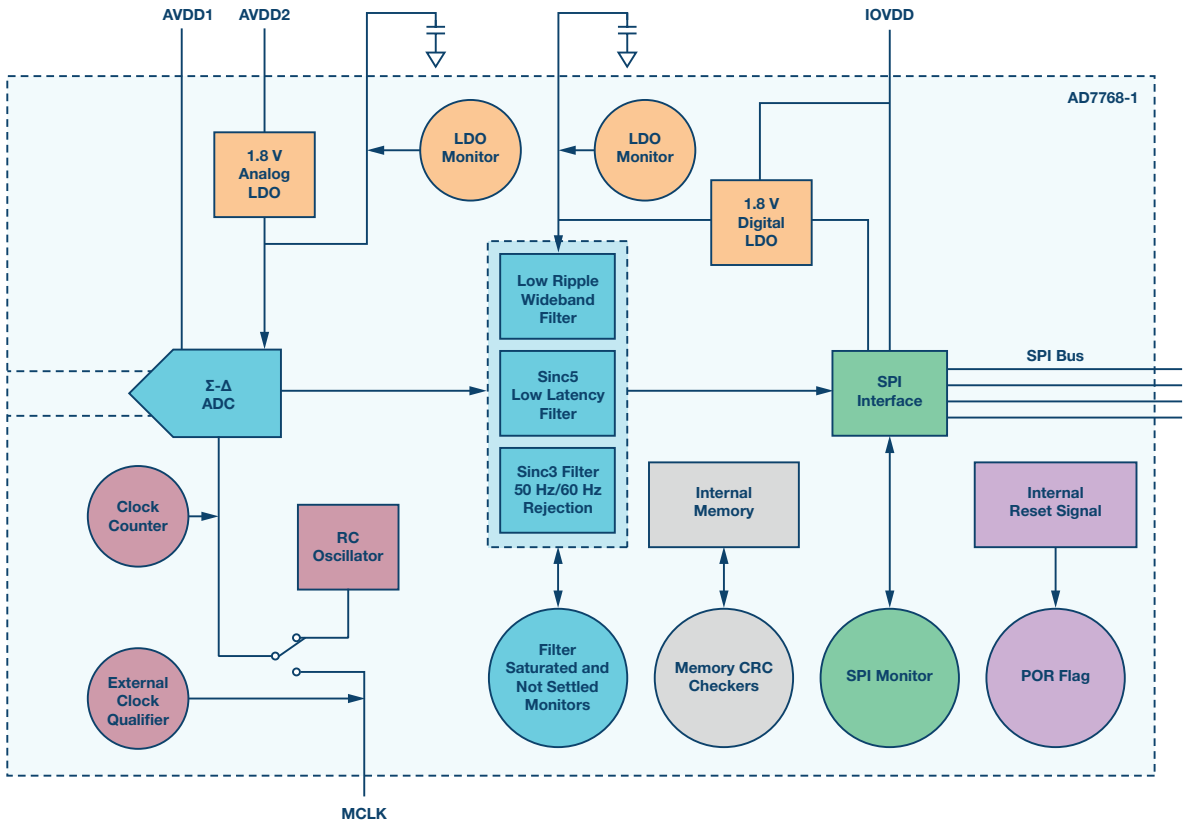

图4. AD7768-1的内部诊断监视器。

基于AD7768-1的终极功能安全解决方案

使用AD7768-1提供的功能安全特性，可以实现以下数据采集系统。用户可以启动器件并使能以下功能安全特性：

- SPI 完整性监视器
- LDO 调节器输出电平监控
- 滤波器饱和度监视器
- 外部时钟认定器
- 内部逻辑和存储器 CRC 监视器

可以使用内部模拟诊断多路复用器验证系统校准。LDO调节器输出也可以通过这种方式进行验证。

接下来，用户可以使能这些功能，将8位状态字节附加到24位数据流和8位SPI CRC字的末尾。基于8位命令字、24位数据流和8位状态字计算8位CRC。如果用户关注处理开销量，可以使能连续回读模式，这样就无需提供8位命令。相反，用户可以在为器件提供串行时钟时输出数据寄存器的内容，如图6所示。

这样即可实现一种数据采集系统，其增益和失调误差已经过验证，每次回读ADC数据时都会向用户提供诊断信息。

连续监视LDO调节器输出、模拟前端输入、内部数字逻辑和存储器。用户可以确定SPI通信的完整性，确保IC温度已知。

结论

许多行业对功能安全的要求不断提高，对于对这些要求起到支撑作用的技术的要求也要相应提高。ADI公司将在我们的产品组合范围内继续开发这种技术，帮助系统设计师实现功能安全理想。

AD7768-1可以大幅减轻客户的负担，并且该解决方案更紧凑、更简单，还能降低处理开销，满足所需解决方案对物料成本的要求。这种单一组件模式还可以减轻系统设计师的负担，帮助他们取得设计安全完整性等级(SIL)认证。

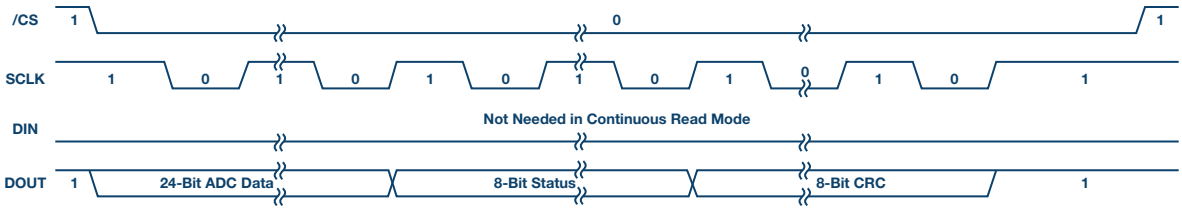

图5. 在连续回读模式下，使用AD7768-1的附加状态字节和CRC字节读回数据寄存器。

Chris Norris [christopher.norris@analog.com]是爱尔兰利默里克市ADI公司的ADC设计评估工程师。他于2012年获得沃特福德理工学院电子工程理学学士学位，并于同年加入ADI公司。

Chris Norris