ANALOG DEVICES
超越一切可能™

如何设计和认证功能安全电阻温度检测器(RTD)系统

Mary McCarthy，应用工程师
Wasim Shaikh，应用工程师

摘要

本文将讨论功能安全系统的电阻温度检测器(RTD)电路设计和Route 2S元件认证流程。系统认证是一个漫长的过程，系统中的所有元器件都必须进行审查以了解潜在的故障机制，诊断故障的方法则多种多样。使用已经过认证的部件可以减轻认证流程中的工作量。

引言

温度是过程控制系统中的一个关键测量指标。它可以是直接测量，例如测量化学反应的温度。它也可以是补偿测量，例如压力传感器的温度补偿。对于任何系统设计，准确、可靠、稳健的温度测量都很重要。对于某些终端设计，检测系统故障至关重要，系统如果发生故障，就会转换到安全状态。在这些环境中应使用功能安全设计。认证级别表明设计的诊断覆盖率水平。

什么是功能安全

在功能安全设计中，系统需要检测到任何故障。考虑一座炼油厂，其中的一个储罐正在装油。如果液位传感器发生故障，系统必须检测到此故障，以便可以主动关闭储罐的阀门，防止储罐溢出，避免潜在的危险爆炸事故。另一个方案是冗余。也就是说，设计中可以使用两个液位传感器，当其中一个液位传感器发生故障时，系统可以继续使用另一个液位传感器运行。设计通过认证后，将获得SIL等级。此等级表示设计提供的诊断覆盖率。SIL等级越高，解决方案越稳健。SIL 2等级表示可以诊断系统内超过90%的故障。为了对设计进行认证，系统设计人员必须向认证机构提供有关潜在故障的证据——无论是安全故障还是危险故障，以及如何诊断故障。必须获取FIT等数据，以及故障模式影响和对系统中不同元器件的诊断分析(FMEDA)。

温度系统设计

本文重点介绍RTD。然而，温度传感器有许多不同类型——RTD、热敏电阻和热电偶等。设计中使用的传感器取决于所需的精度和测量的温度范围。每种类型的传感器都有自己的要求：

- 热电偶偏置
- 激励RTD的激励电流
- 热电偶和热敏电阻的绝对基准

因此，除了ADC之外，还需要其他构建模块来激励传感器并调理前端的传感器。为实现功能安全，所有这些模块都必须可靠且稳健。此外，不同模块的任何故障都必须可检测。传统上，系统设计人员使用复制方法，也就是使用两个信号链，信号链彼此检查以确保：

- 传感器已连接
- 没有开路或短路
- 基准电压处于正确的电平
- PGA仍在正常运行

为了证明设计的稳健性，认证流程需要文档记录。这是一个耗时的过程，有时候很难从IC制造商那里获得某些信息。

但是，AD7124-4/AD7124-8集成模拟前端现在包括了RTD设计所需的所有构建模块。此外，嵌入式诊断功能使得设计人员无需出于诊断目的而复制信号链。除了芯片增强之外，ADI公司还提供文档记录，其中包括认证机构所需的所有信息（FIT引脚FMEDA、裸片FMEDA）。因此，功能安全的认证过程得以简化。

IEC 61508是功能安全设计方面的规范。此规范记录了开发SIL认证产品所需的设计流程。从概念、定义、设计、布局到制造、装配、测试的每个步骤都需要生成文档。这被称为Route 1S。另

一种选择是使用Route 2S流程。这是一条经过实际使用验证的路线，当大批量产品被导入最终客户的系统中并在现场使用了数千小时时，仍然可以通过向认证机构提供如下证据来认证产品：

- 现场使用的数量
- 现场退货的分析，并详细说明退货不是由于元器件本身的故障造成的
- 安全数据手册，详细说明诊断及其提供的覆盖率
- 引脚和裸片FMEDA

3线RTD设计

RTD

RTD适合测量-200°C至+850°C的温度，在该温度范围内，其响应接近线性。RTD使用的典型元素有镍、铜和铂，100 Ω和1000 Ω铂制RTD较为常见。RTD有两线、三线或四线形式，其中3线和4线形式较为常用。RTD是无源传感器，需要一个激励电流来产生输出电压。RTD的输出电平从数十毫伏到数百毫伏不等，具体取决于所选的RTD。

RTD设计

图1显示了一个3线RTD系统。AD7124-4/AD7124-8是用于RTD测量的集成解决方案，包含系统所需的所有构建模块。为了全面优化该系统，需要2个理想匹配的电流源。这两个电流源用于抵消RL1产生的引线电阻误差。一个激励电流流过精密基准电阻R_{REF}和RTD。另一个电流流过引线电阻RL2，所产生的电压与RL1上的压降相抵消。精密基准电阻上产生的电压用作ADC的基准电压REFIN1(±)。由于仅利用一个激励电流来产生基准电压和RTD上的电压，因此，该电流源的精度、失配和失配漂移对ADC整体转换函数的影响极小。AD7124-4/AD7124-8允许用户选择激励电流值，从而调整系统以使用ADC的大部分输入范围，提高性能。

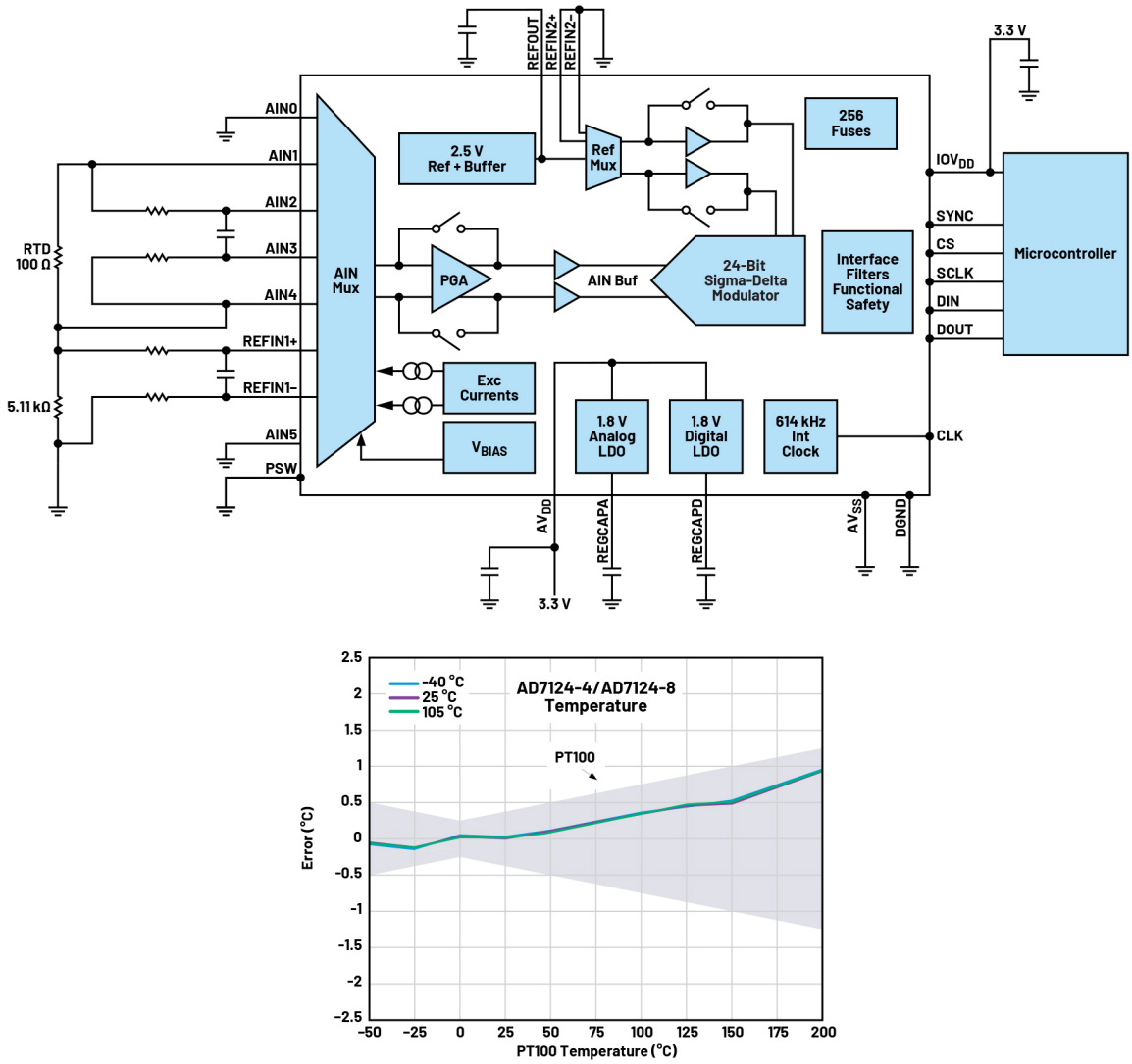

图1. 3线RTD温度系统

RTD的低电平输出电压需要放大，以便利用ADC的大部分输入范围。AD7124-4/AD7124-8的PGA可以设置1到128的增益，允许用户在激励电流值和增益与性能之间进行取舍。出于抗混叠和EMC目的，传感器与ADC之间需要滤波。基准电压缓冲器支持无限的滤波器R、C元件值，也就是说，这些元件不会影响测量精度。

系统还需要校准以消除增益和失调误差。图1显示了此3线B级RTD在执行内部零电平和满量程校准后的实测温度误差，总误差远小于±1°C。

ADC要求

温度测量系统以低速测量为主（最高速度通常是每秒100次采样），因而需要低带宽ADC。但是，该ADC必须具有高分辨率。Σ-Δ型ADC适合此类应用，因为利用Σ-Δ结构能够开发出低带宽、高分辨率ADC。

采用Σ-Δ型转换器时，对模拟输入连续采样，采样频率比目标频段高很多。它还使用噪声整形，将噪声推到目标频段之外，进入转换过程未使用的区域，从而进一步降低目标频段内的噪声。数字滤波器会衰减任何处在目标频段之外的信号。

数字滤波器在采样频率和采样频率的倍数处有镜像，因此，需要一些外部抗混叠滤波器。然而，由于过采样，简单的一阶RC滤波器即足以满足大部分应用的要求。Σ-Δ架构允许24位ADC实现最高达21.7位的峰峰值分辨率（21.7个稳定或无闪烁位）。Σ-Δ架构的其他优势有：

- 宽共模范围的模拟输入
- 宽范围的基准输入
- 能够支持比率式配置

滤波（50 Hz/60 Hz抑制）

除了如上所述的抑制噪声以外，数字滤波器还用于提供50 Hz/60 Hz抑制。系统采用主电源供电时，会发生50 Hz或60 Hz干扰。交流电源会产生50 Hz及其倍数（欧洲）和60 Hz及其倍数（美国）的噪声。低带宽ADC主要使用sinc滤波器，可将其陷波频率设置在50 Hz和/或60 Hz及其倍数处，从而提供50 Hz/60 Hz及其倍数的抑制。现在越来越多地要求利用建立时间较短的滤波方法提供50 Hz/60 Hz抑制。在多通道系统中，ADC顺次处理所有使能的通道，在每个通道上产生转换结果。选择一个通道后，便需要滤波器建立时间以产生有效转换结果。若缩短建立时间，则可提高给定时间内转换的通道数。AD7124-4/AD7124-8的后置滤波器或FIR滤波器可提供50 Hz/60 Hz同时抑制，并且其建立时间比sinc3或sinc4滤波器要短。图3显示了一个数字滤波器选项：此后置滤波器的建立时间为41.53 ms，并且提供62 dB的50 Hz/60 Hz同时抑制。

诊断

对于功能安全设计，构成RTD系统的所有功能都需要诊断。AD7124-4/AD7124-8具有多个嵌入式诊断功能，因此设计复杂性得以简化，设计时间得以缩短。另外还无需复制信号链以实现诊断覆盖。

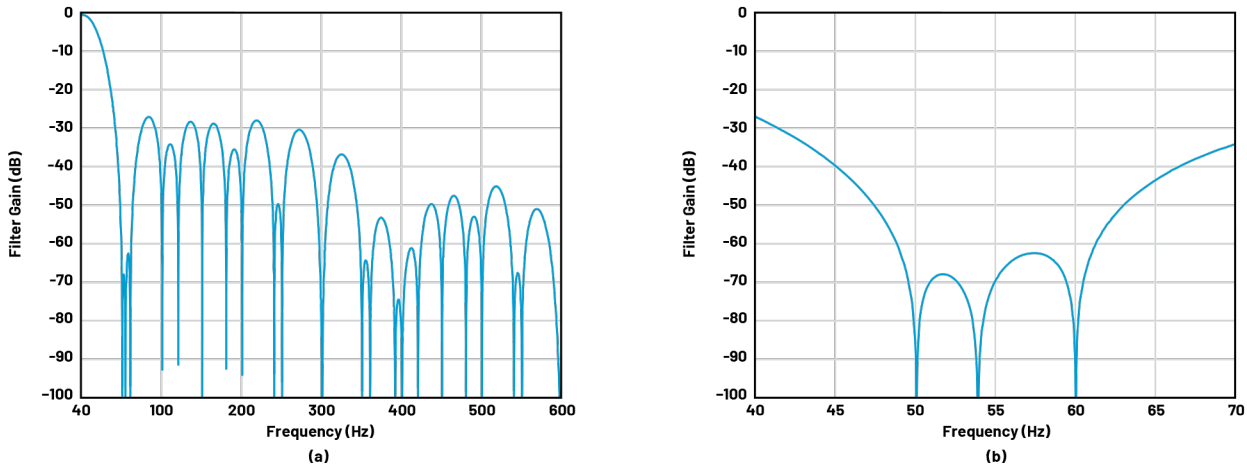

图2. 频率响应，后置滤波器，25 SPS：(a) DC至600 Hz，(b) 40 Hz至 70 Hz。

典型诊断要求如下：

- 电源/基准电压/模拟输入监控
- 开路检测
- 转换/校准检查
- 信号链功能检查
- 读/写监控
- 寄存器内容监控

下面详细说明嵌入式诊断。

SPI诊断

AD7124-4/AD7124-8提供CRC。使能后，所有读操作和写操作都包括CRC计算。校验和为8位宽，使用如下多项式生成：

$$x^8 + x^2 + x + 1$$

因此，对于AD7124-4/AD7124-8的每次写操作，处理器都会生成一个CRC值，该值会附加到发送至ADC的信息中。ADC根据接收到的信息生成自己的CRC值，并将其与从处理器接收到的CRC值进行比较。如果两个值一致，则可确定信息完好无损，从而将其写入相关的片内寄存器。如果CRC值不一致，则表明传输过程中发生了位损坏。在这种情况下，AD7124-4/AD7124-8会设置一个错误标志，指示发生了数据损坏。损坏的信息不会被写入寄存器，从而实现自我保护。同样，当从AD7124-4/AD7124-8读取信息时，也会生成一个CRC值并伴随该信息。处理器将处理此CRC值，以确定传输有效还是发生了损坏。

AD7124-4/AD7124-8数据手册列出了客户可以访问的寄存器（用户寄存器）。AD7124-4/AD7124-8会检查所访问寄存器的地址。如果用户尝试读取或写入数据手册中未记载的寄存器，就会设置一个错误标志，表示处理器正在尝试访问非用户寄存器。同样，伴随此寄存器访问的任何信息都不会应用于寄存器。

AD7124-4/AD7124-8还有一个SCLK计数器。所有读写操作都是8的倍数。当$\overline{CS}$用于使能帧读写操作时，SCLK计数器计数每个读/写操作中使用的SCLK脉冲数，与此同时$\overline{CS}$为低电平。当$\overline{CS}$变为高电平时，通信中使用的SCLK数量应为8的倍数。如果SCLK上出现毛刺，这将导致SCLK脉冲过量。如果发生这种情况，AD7124-4/AD7124-8会再次设置错误标志，并放弃输入的任何信息。

状态寄存器指示正在转换的通道。读取数据寄存器时，可以将状态位附加到转换结果中。这会进一步增强处理器/ADC通信的稳健性。

上面提到的所有诊断功能都是为了确保ADC与处理器之间的通信稳健，只有有效信息才被AD7124-4/AD7124-8接受。当$\overline{CS}$用于使能帧读写操作时，每次拉高$\overline{CS}$时，串行接口便复位。这确保了所有通信都从已定义的或已知的状态开始。

存储器检查

每次更改片内寄存器（例如更改增益）时，都会对寄存器执行CRC，并将生成的CRC值临时存储在内部。AD7124-4/AD7124-8内部定期对寄存器执行额外的CRC检查。得到的CRC值与存储的值进行比较。如果值由于位翻转而不同，就会设置一个标志，以向处理器表明寄存器设置已损坏。处理器随后可以复位ADC，并重新加载寄存器。

片内ROM保存寄存器的默认值。上电时或复位后，ROM内容将应用于用户寄存器。在最终的生产测试中会计算ROM内容的CRC，并将得到的CRC值存储在ROM中。在上电或复位时会再次对ROM内容执行CRC，并将得到的CRC值与保存的值进行比较。如果二者不同，则表明默认寄存器设置与预期不同，因而需要重启或复位。

信号链检查

器件包括许多信号链检查。电源轨（AV_{DD}、AV_{SS}和IOV_{DD}）可应用于ADC输入，从而可以监视电源轨。AD7124-4/AD7124-8内置一个模拟和一个数字低压差(LDO)稳压器。这些也可以应用于ADC并进行监视。AD7124-4/AD7124-8包括x路复用。此外，AV_{SS}可在内部用作AIN-，这样就可以检查模拟输入引脚上的绝对电压。客户可以探测输出激励电流的引脚，并探测AIN+和AIN-引脚。这将检查连接，并确保各个引脚上的电压处于正确的电平。

对于基准电压检查，基准电压检测功能会指示基准电压过低的情况。客户还可以选择内部基准电压作为模拟输入，这样就可以用来监视外部基准电阻上产生的电压，前提条件是基准电阻两端的电压略高于2.5 V（内部基准电压的幅度）。

AD7124-4/AD7124-8还有一个内部20 mV电压，这对于检查增益级很有用。例如，使用20 mV作为模拟输入，增益可以从1变为2、4、... 128。每次提高增益时，转换结果放大2倍，从而证实增益级工作正常。

检查锁定位时，X路复用也很有用。它允许交换AIN+和AIN-引脚，导致转换结果反转。因此，使用20 mV和x路复用时，用户可以检查锁定位。

为AIN+和AIN-选择相同的模拟输入引脚并偏置此内部短路，以便检查ADC噪声，确保其在规定范围内工作。内部可以选择嵌入式

基准电压(+2.5 V)作为ADC的输入。同样，应用+V_{REF}和-V_{REF}可确认信号链正常工作。

可编程的开路测试电流可用来检查传感器连接。PT100在-200°C时电阻典型值为18 Ω，在+850°C时为390.4 Ω。使能开路测试电流后，可以执行转换。如果RTD短路，获得的转换结果将接近0。AIN+和AIN-之间开路会导致转换结果接近0xFFFFFF。在RTD正确连接的情况下，永远不会获得接近0或全1的代码。

最后，AD7124-4/AD7124-8具有过压和欠压检测功能。正在转换的AIN+和AIN-引脚上的绝对电压通过比较器持续监控。当AIN+或AIN-上的电压超出电源轨（AV_{DD}和AV_{SS}）时，就会设置标志。

这种高集成度减少了执行测量和提供诊断覆盖所需的物料(BOM)，并缩短了设计时间，降低了设计复杂性。

转换/校准

AD7124-4/AD7124-8上的转换也受到监控。如果(AIN+ – AIN-)/增益大于正满量程或小于负满量程，就会设置一个标志。ADC的转换结果变为全1（模拟输入过高）或全0（模拟输入过低），因此客户知道发生了故障。

对来自调制器的比特流进行监控，以确保调制器不会饱和。如果发生饱和（调制器连续输出20个1或20个0），则设置一个标志。

AD7124-4/AD7124-8包括内部偏移和校准以及系统偏移和增益校准。如果校准失败，就会设置一个标志以告知用户。请注意，如果校准失败，偏移和增益寄存器不会更新。

电源

除了前面讨论的电源检查外，AD7124-4/AD7124-8还有用于持续监控内部LDO稳压器的比较器。因此，如果这些LDO稳压器的电压低于跳变点，就会立即报告错误。

这些LDO稳压器需要一个外部电容。也可以检查该电容存在与否。

MCLK计数器

滤波器曲线和输出数据速率与MCLK直接相关。当主时钟为614.4 kHz时，数据手册中列出的输出数据速率是正确的。如果主时钟改变频率，输出数据速率和滤波器陷波频率也会改变。例如，若使用滤波器陷波频率来抑制50 Hz或60 Hz，则变化的时钟会减少所获得的衰减。因此，了解时钟频率对于确保获得最佳抑制很有价值。AD7124-4/AD7124-8包含一个MCLK计数器寄存器。每计数131个MCLK周期，该寄存器便加1。为了测量MCLK频率，处理器需要一个定时器。可以在时间0读取该寄存器，然后在定时器超时后再次读取。有了这些信息，便可确定主时钟的频率。

各通道独立配置

AD7124-4/AD7124-8允许按通道进行配置，也就是说，器件支持八种不同的设置，一个设置由基准电压源、增益设置、输出数据速率和滤波器类型组成。当用户配置一个通道时，可将八种设置中的一种分配给该通道。请注意，通道可以是模拟输入通道，也可以是诊断通道，例如测量电源(AV_{DD}-AV_{SS})。因此，客户可以设计一个由模拟输入和诊断组成的序列。各通道独立配置允许以与模拟输入转换不同的输出数据速率运行诊断。诊断不需要与主要测量相同的精度，因此客户可以将诊断与测量交错，并以较高输出数据速率运行诊断。这些嵌入式特性可减少处理器的工作量。

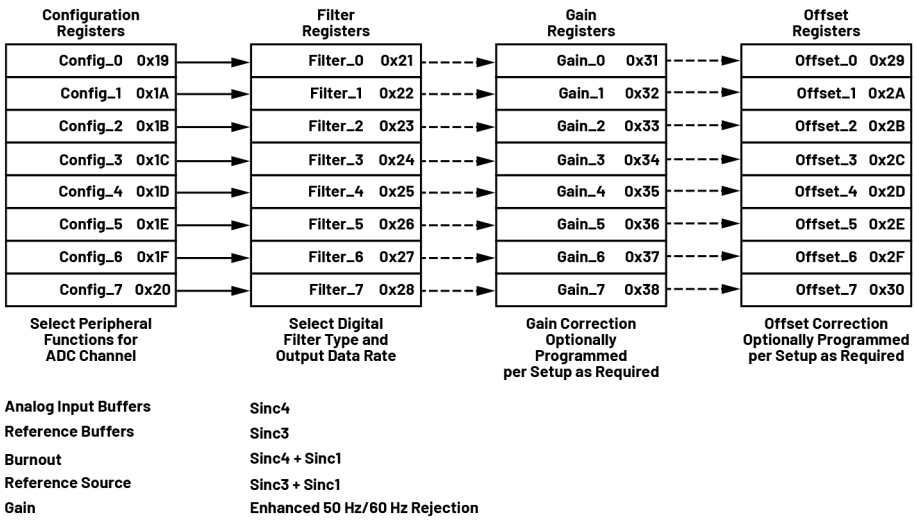

图3. 各通道独立配置

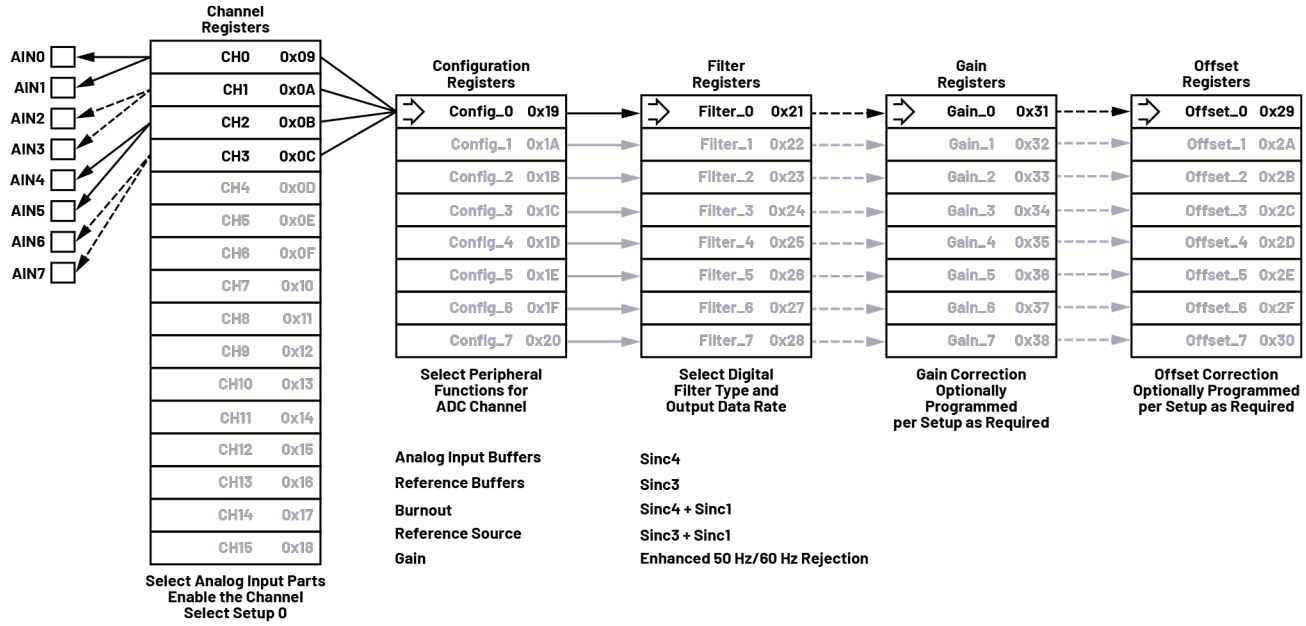

图4. 将设置分配给通道

其他功能

AD7124-4/AD7124-8包含一个温度传感器，该传感器也可用于监控芯片温度。这两款器件的ESD额定值均为4 kV，支持实现稳健的解决方案。这些器件采用5 × 5 mm LFCSP封装，适合本质安全设计。

根据IEC 61508，使用这些器件的典型温度应用的FMEDA表明安全失效比率(SFF)大于90%。一般需要两个传统ADC才能达到这一水平。

内置诊断的其他好处

除了BOM和成本节省之外，诊断还能从其他方面节省成本：避免设计复杂性，减少资源使用，以及加快客户产品上市时间。让我们借助下例来理解这一点：

AD7124-4/AD7124-8有一个MCLK计数器，用于测量主时钟频率并捕捉所提供的主时钟的任何不一致。主时钟计数器是一个8位寄存器，每131个MCLK周期递增一次。该寄存器由SPI主机读取，以确定内部/外部614.4 kHz时钟的频率。

如果必须在AD7124-4/AD7124-8外部实施MCLK频率检查该怎么办？这将需要如下硬件资源：

- 带外设（如计数器和外部中断控制器）的微控制器
- 施密特触发电路

另外请注意，存储和运行代码（包括中断服务例程）需要存储器。总之，实施方案将如图5所示。

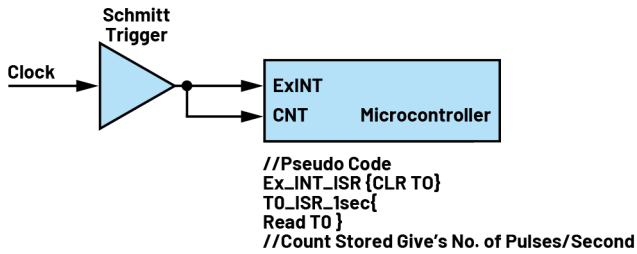

图5. 由微控制器实现的MCLK频率监视器

此外，我们必须确保代码经过检查并符合编码准则和限制。总之，实施单独的诊断部分会产生很大的开销。因此，内置诊断有诸多好处：

- 节省空间和BOM
- 提高系统可靠性；更少元器件 = 更高的可靠性
- 加速产品上市
- 软件开发——开发和运行诊断程序
- 硬件测试
- 系统测试
- 节省微控制器存储器
  - 不需要代码来运行诊断
  - 编码准则要求进行大量双重存储器代码检查
- 即用型安全文档节省系统评估时间

助力功能安全设计

AD7124-4/AD7124-8不是按照IEC 61508标准中的开发指南进行设计和开发的，因此无SIL等级。但是，通过了解各种诊断的最终应用和使用情况，可以评估AD7124-4/AD7124-8是否适用于SIL等级设计。

功能安全术语

让我们回顾一下认证过程中的一些重要概念：

- 故障：系统性和随机性
- 诊断覆盖率
- 硬件容错
- SIL等级

故障：系统性和随机性

系统性故障是由特定原因引起的确定性（非随机）故障，可通过修改设计或制造过程、操作程序、文档或其他相关因素来消除。例如，由于外部中断引脚上缺乏滤波，系统会因为高噪声而发生中断。

随机故障则是由作用于系统内硬件组件的物理原因引起的。此类故障是由腐蚀、热应力、磨损等效应引发的，无法通过系统化流程来发现此类故障。

为了处理随机故障，我们可以使用可靠性、诊断和冗余等方法。

在可靠性方面，我们确保使用可靠的元器件，而通过诊断，我们确保可以检测和排解这些故障。确保可靠性的另一种方法是增加冗余以降低故障概率，但这样做会增加系统成本和空间。

随机故障有四种类型，即安全检测型、安全未检测型、危险检测型和危险未检测型。

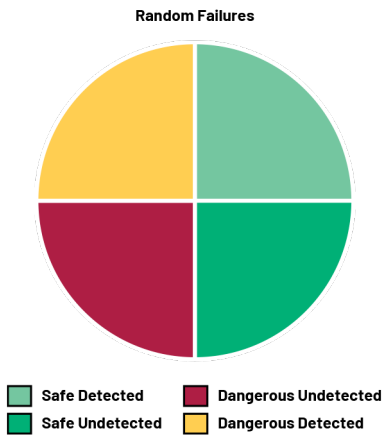

图6. 随机故障类型

例如，考虑一个系统，其安全功能是在温度读数很高时断开机器的电源开关。任何不影响安全功能（即断开电源开关）的随机故障，称为安全检测型故障或安全未检测型故障。影响安全功能的其他故障则是危险故障。对我们来说，重要的是危险未检测型故障。这类故障是诊断未覆盖的故障，我们的目标是提高诊断覆盖率，以尽可能将危险及未检测到的故障减少。

诊断覆盖率

随机故障可以通过软件或硬件形式的各种内置检测机制来检测。例如，MOSFET开关故障可以通过回读输出来检测，随机存储器位翻转可以通过定期运行CRC存储器检查来检测。

诊断覆盖率衡量系统检测危险故障的能力，数学上定义为危险检测型故障与危险故障的比率。

硬件容错

考虑一个可编程逻辑控制器(PLC)系统，例如图7所示，其安全功能是在输入超过特定值时断开开关以停止机器。在HFT = 0图中，如果存在单一随机故障(X)，系统就会发生故障，机器不会停止。

现在，如果我们有HFT = 1图中所示的冗余路径，那么单一随机故障将不再引起故障，我们将能够停止机器。

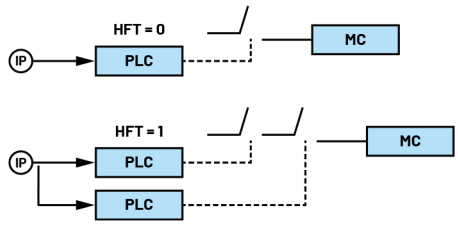

图7. PLC系统

因此，通过增加冗余路径，系统便可容忍单一故障。此系统被称为HFT 1系统，表示一个故障不会导致系统失效。HFT 0表示一个故障可能导致系统失效。硬件容错是当存在一个或多个危险故障时，元器件或子系统执行安全功能的能力。

HFT可以从1oo1、1oo2、2oo3等架构来计算。如果将架构表示为MooN，则HFT计算式为N-M。换句话说，2oo4架构的HFT为2。这意味着它可以容忍两个故障并继续工作，因此它是一个具有冗余的架构。

SIL等级覆盖率

表1显示了SFF（即诊断覆盖率）和硬件容错（意味着冗余）

表1. SIL等级覆盖率

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

行表示诊断覆盖率，列表示硬件容错。HFT为0表示如果系统出现一个故障，安全功能就会丧失（见表1）。

如果增加冗余以实现HFT 1，如图7所示，那么系统可以容忍一个故障而不会停机。目前通过冗余达到SIL 3等级的客户，如果使用具有更高诊断覆盖率的部件，则可以在没有冗余的情况下达到SIL 3。

因此，更高水平的诊断可以减少所需的系统冗余量，或者在相同冗余量下，我们可以提高解决方案的SIL等级（在表1中向下移动）。

现在，让我们回顾一下AD7124-4/AD7124-8中的诊断功能，其支持多种内置机制，例如电源/基准电压/AIN监控、开路检测、转换/校准检查、信号链功能检查、读/写监控、寄存器内容监控等，这些诊断功能可提高AD7124-4/AD7124-8系统的诊断覆盖率。在没有这些诊断的情况下，需要两个ADC才能达到相同的水平。

因此，一个AD7124-4或AD7124-8可提供相同水平的覆盖范围，其诊断覆盖率和特性支持设计功能安全的系统。这可节省50%的BOM和印刷电路板空间。

支持SIL等级设计的文档

辅助终端系统SIL认证所需的文档包括：

- 安全数据手册（安全手册用于SIL等级部件）
- 引脚FMEDA（故障模式、影响和分析）和FMEDA（故障模式、影响和诊断分析）
- 附录F 检查清单

这些文档由主要来自四个数据源的输入组成，如图8所示。这些数据是诊断数据、设计数据、FIT率和来自故障插入测试的数据。

- 数据手册中的诊断数据涉及部件提高的所有诊断特性。
- 设计数据是指内部数据——例如，裸片面积和部件每个内部模块的影响。
- 数据手册中提供了各种元器件的FIT率（故障率）。一个常见例子是Siemens Databook SN 29500。
- 对无法使用设计和诊断数据进行分析的模块应进行故障插入测试。这些测试是根据应用需求而规划的，故障插入测试的结果用于加强FMEDA和FMEA文件。

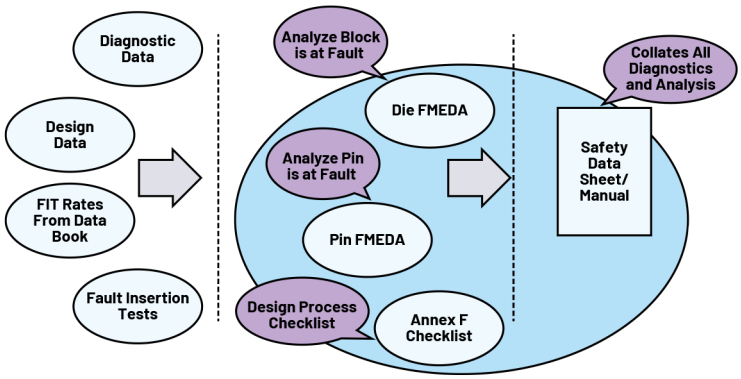

图8. 功能安全文档信息流

裸片FMEDA

AD7124-4/AD7124-8 FMEDA分析应用原理图中的主要模块，识别故障模式和影响，并检查特定安全功能的诊断和分析。让我们通过图9了解该机制。

对于RTD型系统，安全功能是以±x度的精度测量温度。应用原理图如图9所示。

我们将危险故障定义为可能导致ADC输出或SPI通信出现错误的故障，如果输出中的错误很严重，则可能导致危险故障。

安全状态定义为：

- 根据安全功能，输出数据代表输入
- 错误状态位已置位
- ADC输出转换结果为全0或全1
- 无SPI通信单

根据IEC 61508，AD7124-4/AD7124-8被认定为B类系统。为了解释FMEDA，让我们以时钟模块为例，分析其故障模式。

表2显示了当时钟模块面临第一列中描述的故障模式时会发生什么，它对输出的影响，诊断覆盖率，最后是分析。

表2. 主时钟模块故障模式、影响、诊断和分析

故障模式	影响	诊断覆盖率	分析
输出锁在高电平	ADC转换结果冻结	99	MCLK时钟计数器—表A.11—“具有独立时基和时间窗口的看门狗”
输出锁在高电平	ADC转换结果冻结	99	MCLK时钟计数器—表A.11—“具有独立时基和时间窗口的看门狗”
输出高阻抗	ADC转换结果冻结	99	MCLK时钟计数器—表A.11—“具有独立时基和时间窗口的看门狗”
输出漂移±10%	ADC转换结果损坏，50 Hz/60 Hz陷波频率无效	99	MCLK时钟计数器—表A.11—“具有独立时基和时间窗口的看门狗”
输出抖动	ADC转换结果损坏或有噪声	99	A.13“参考传感器”，检查结果合理性

同样，我们随后分析AD7124-4/AD7124-8中的其余模块。

请注意，可能存在一些可能不会影响安全功能的故障；例如，AIN0引脚上的故障不会导致温度测量出现问题，因此可以从安全计算中排除。

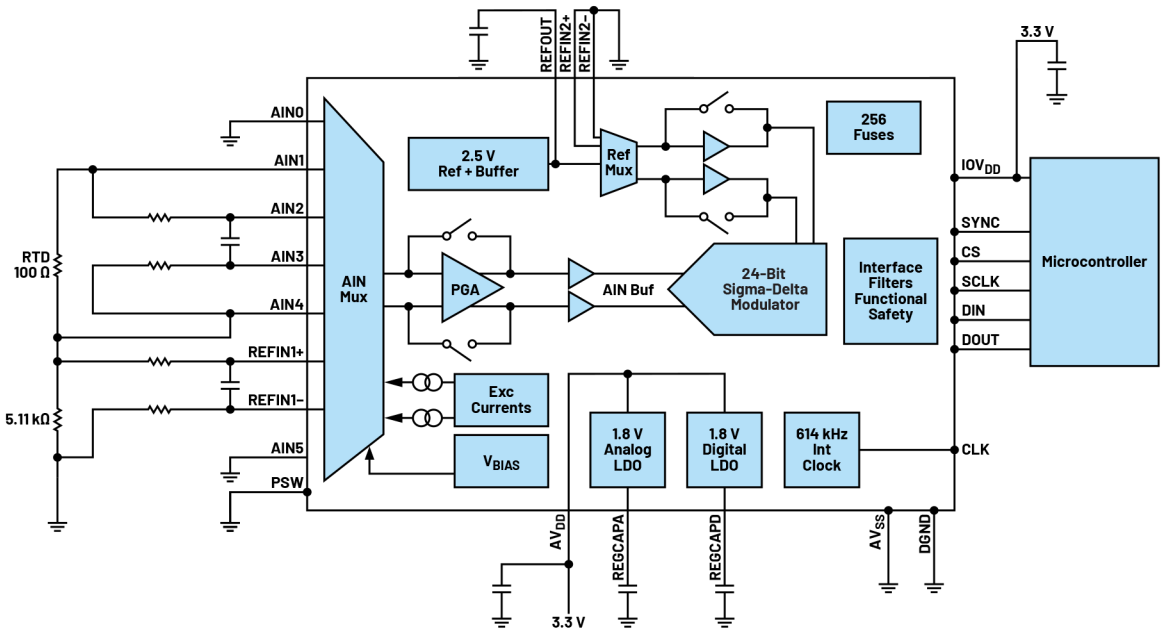

图9. RTD应用原理图

FMEDA的结果将是安全故障、危险检测型故障和危险未检测型故障的故障率，用于计算SFF。

引脚FMEDA

引脚FMEDA分析AD7124-4/AD7124-8引脚上的各类故障及其在此RTD应用中的后果。选取每个引脚，一步一步地分析引脚开路、短接到电源/接地或短接到相邻引脚会有什么后果。

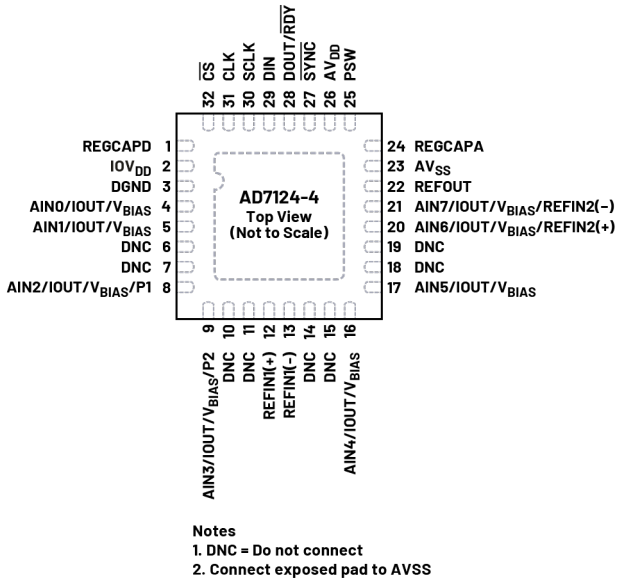

图10. 32引脚LFCSP引脚配置

例如，以图10中的引脚29 (DIN)为例，参考图9所示的应用原理图，检查不同故障的后果。表3显示了故障模式、影响和检测。

表3. 引脚DIN的故障模式、影响和分析

引脚名称	引脚故障模式	故障的潜在影响	检测
DIN	引脚开路	丧失通信	在系统级别很容易检测
DIN	短接到地	丧失通信	在系统级别很容易检测
DIN	短接到AV_{DD}或IOV_{DD}	丧失通信；可能损坏	在系统级别很容易检测
DIN	短接到相邻引脚SCLK	丧失通信	在系统级别很容易检测
DIN	短接到相邻引脚DOUT/RDY	丧失通信	在系统级别很容易检测

请注意，分析是针对图9所示的应用原理图进行的，因此对未使用引脚的分析不会产生任何影响。

附录F 检查清单

这是ASIC避免系统性故障的设计措施清单。合规需要一份完整的IEC 61508-2:2010附录F检查清单。

安全手册或数据手册

一整套信息最终进入安全手册或数据手册，提供实现AD7124-4/AD7124-8集成的必要要求。

当显示符合IEC 61508功能安全标准时，安全数据手册会整理来自各种文档的所有诊断和分析。它将包含所有信息，例如：

- 产品概述
- 应用信息
- 安全理念
- 终身预测
- FIT
- FMEDA计算——SFF和DC
- 硬件安全机制
- 诊断描述
- EMC稳健性
- 以冗余配置工作
- 附件和文件清单

Route 2S，也称为“经过使用证明”

我们已经讨论了第一种评估方法。现在我们讨论另一种方法，称为“经过使用证明”或Route 2S。此方法适用于已发布器件，并且基于对客户退货的分析和已发货数量。

这样可以进行SIL认证，就好像该部件是完全按照IEC61508标准开发的一样。

如果模块/系统设计者过去曾成功使用某一IC，并且了解现场故障率，那么他可以宣称其“经过使用验证”(Route 2S)。

请注意，Route 2S需要完整的现场退货数据，因此对于集成电路设计者或制造商来说，作出这种宣称要困难得多，因为他们一般不太了解最终应用或拥有完备的现场失效器件收集、失效分析流程及数据。

结论

RTD测量系统对ADC和系统的要求非常苛刻。这些传感器产生的模拟信号很小。这些信号需要用增益级放大，同时放大器的噪声必须非常低，不至于淹没传感器的信号。放大器之后需接一

个高分辨率ADC，以将传感器的低电平信号转换为数字信息。除了ADC和增益级之外，温度系统还需要其他元器件，例如激励电流。同样，这些元件必须是低漂移、低噪声元件，不致于降低系统精度。诸如失调等初始精度误差可以通过校准从系统中消除，但元件随温度的漂移必须非常低，以免引入误差。集成激励模块和测量模块可简化客户设计。针对功能安全进行设计时，还需要诊断。将诊断与激励和测量模块集成在一起，可以简化整体系统设计，减少BOM，缩短设计时间，加速产品上市。

FMEDA等文档包含客户认证最终设计中的元器件所需的全部信息。但是，对元器件本身进行认证可以进一步简化与认证机构的交流。Route 2S流程允许对发布后的产品进行认证，鉴于目前有很多已发布的器件适合功能安全设计，因此这是一条很有用的途径。

了解更多

- ADI功能安全网站
- 相关资料—RTD测量(CN0383)
- 文章：如何选择并设计理想RTD温度检测系统

作者简介

Mary McCarthy是ADI公司应用工程师。她于1991年加入ADI公司，在爱尔兰科克市的线性与精密技术应用部工作，主要关注精密Δ-Σ型转换器。她于1991年毕业于科克大学，获得电子与电气工程学士学位。

Wasim Shaikh于2015年加入ADI公司，在精密转换器部门担任应用工程师，工作地点在印度班加罗尔。Wasim是一名获认证的功能安全工程师，于2003年获得普纳大学学士学位。

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

TA23731sc-7/22