ANALOG DEVICES
想像を超える可能性を
AHEAD OF WHAT'S POSSIBLE™

機能的に安全な測温抵抗体（RTD）システムの設計および認証方法

Mary McCarthy、アプリケーション・エンジニア
Wasim Shaikh、アプリケーション・エンジニア

概要

本稿では、機能的に安全なシステムのための測温抵抗体（RTD）回路設計、およびルート2Sのコンポーネント認証プロセスについて説明します。障害発生の可能性のある機構に関して、システムのすべてのコンポーネントを確認する必要があり、また、障害の診断には様々な方法があるため、システムの認証は長いプロセスとなります。既に認証されている部品を用いることで、認証プロセスに伴うこの作業負荷は軽減できます。

はじめに

プロセス制御システムにおいて、温度は重要な測定項目です。これは化学反応の温度を測定する場合のように、直接測定である場合もあれば、圧力トランスデューサの温度補償のように、補償測定の場合もあります。どのシステム設計でも、この測定は正確で、信頼度が高く、堅牢であることが必要です。最終設計によっては、システムの障害を検知し、システムが正常に動作できなくなった場合には安全な状態に移行することが極めて重要です。こうした環境では、機能的に安全な設計が用いられます。認証のレベルが、設計に含まれる診断範囲のレベルを示しています。

機能安全とは

機能的に安全な設計では、どのような不具合もシステムが検知できる必要があります。タンクが満杯となっている製油所を考えてみましょう。レベル・センサーに不具合が発生した場合、この不具合を検知し、タンクのバルブをアクティブに閉じることが重要です。これによりタンクのオーバーフローが防止され、危険な爆発が発生する可能性を回避できます。または冗長性を利用することもできます。これは、2つのレベル・センサーを使用できる設計とし、最初のレベル・センサーが故障した場合に2つめのレベル・センサーを用いてシステムが機能し続けるというものです。設計を認証する場合、SILの等級付けが行われます。この等級付けは、設計によってもたらされる診断範囲を指します。SILの等級が高いほど、そのソリューションは堅牢です。SIL 2等級は、システム内の故障の90%以上が診断可能であることを示します。設計を認証するためには、設計者は、可能性のある故障についてこれらが機能安全なのか、危険な故障なのか、こうした故障をどのように診断できるのか、認証機関に対して明確にする必要があります。システムの様々なコンポーネントに対する故障モード影響診断解析（FMEDA）と共に、FITなどのデータが必要です。

温度システムの設計

本稿では、RTDに焦点を置きます。ただし、温度センサーには、RTD、サーミスタ、熱電対など、多様な種類があります。設計で使用するセンサーは、必要とされる正確性と測定する温度範囲によって異なります。センサーの種類ごとに次のような固有の条件があります。

- 熱電対のバイアス
- RTDを励起するための励起電流
- 熱電対とサーミスタのための絶対リファレンス

したがって、センサーを励起し、フロント・エンドでセンサーの条件付けを行うために、ADCやその他の構成ブロックが必要です。機能安全のためには、こうしたブロックすべてが信頼性が高く堅牢であることが必要です。更に、様々なブロックのどのような故障も検出できなくてはなりません。従来、システム設計者は複製を使用し、2つのシグナル・チェーンを用いて各シグナル・チェーンに互いをチェックさせることで、以下の点を確保してきました。

- センサーが接続されている
- 開放や短絡がない
- リファレンスのレベルが適切である
- PGAが機能し続けている

認証プロセスによって設計が堅牢であることの証明を受けるには、文書化が必要です。これは時間を要するプロセスで、また、ICメーカーから取得するのが困難な情報もあります。

ただし、現在では、AD7124-4/AD7124-8統合型アナログ・フロント・エンドに、RTD設計に必要な構成ブロックがすべて含まれています。更に、診断機能が組み込まれているため、診断のためにシグナル・チェーンを複製する必要はなくなります。デバイスの機能強化に加え、アナログ・デバイセズでは、認証機関が必要とするすべての情報（FITピンFMEDA、ダイFMEDA）を含む資料を提供しています。これにより、機能安全の認証プロセスが容易になります。

IEC 61508は、機能安全設計のための仕様です。この仕様には、SIL認証部品を開発するために必要な設計フローが記載されています。コンセプト、定義、設計、レイアウト、製造、アセンブリ、試験の各ステップで文書を作成する必要があります。これはルート1Sと呼ばれています。別のオプションはルート2Sのフローを使用することです。これは使用実績による証明のルートであるため、大量の製品が最終顧客のシステム向けに設計され、フィールドで1000時間使用された場合に、次の項目を証拠として認証機関に提出することで、製品は認証を受けることができます。

- フィールドでの使用量
- フィールドからの返品の解析、および返品がコンポーネント自体の故障によるものではないことの詳細な説明
- 診断およびその範囲に関する詳細を記載した安全データシート
- ピンおよびダイのFMEDA

3線式RTD設計

RTD

RTDは、−200°C～+850°Cの範囲の温度を測定する場合に便利で、この温度範囲でほぼ直線的な応答特性を持っています。RTDに用いられる代表的な元素は、ニッケル、銅、プラチナですが、100Ωおよび1000ΩのプラチナRTDが最も一般的です。RTDは2線式、3線式、4線式のいずれかで構成されますが、3線式および4線式が最も多く使われています。これらはパッシブなセンサーで、出力電圧を生成するには励起電流が必要です。このようなRTDの出力電圧レベルは、選択するRTDに応じて、数10ミリボルト～数100ミリボルトの幅があります。

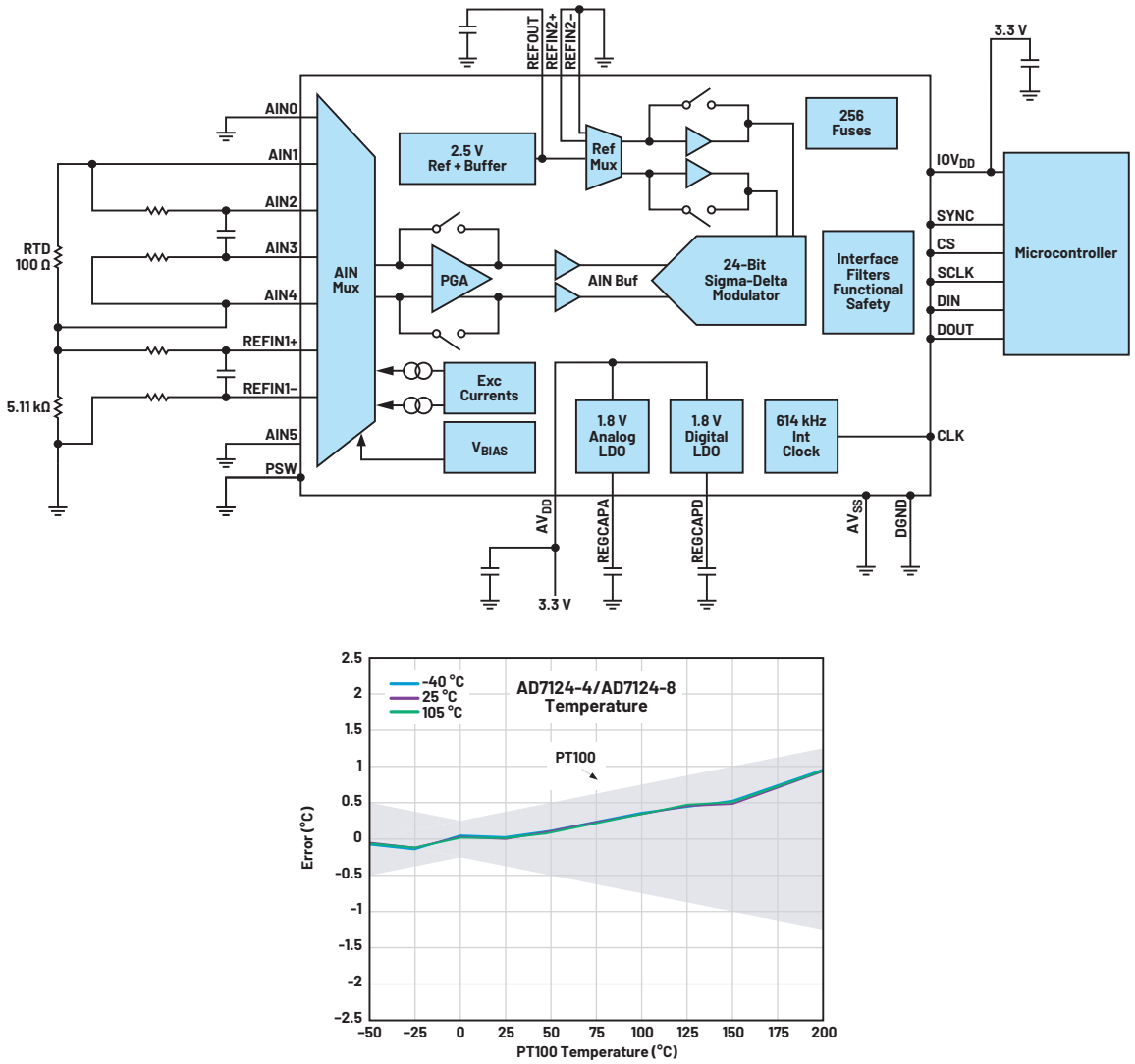

図1　3線式RTD温度システム

RTDの設計

図1に、3線式RTDシステムを示します。AD7124-4/AD7124-8は、RTD測定用の統合型ソリューションで、システムに必要なすべての構成ブロックを内蔵しています。このシステムを完全に最適なものにするためには、完全にマッチングの取れた2つの電流源が必要です。この2つの電流源を用いることで、RL1で生成されるリード抵抗誤差を相殺できます。一方の励起電流は高精度リファレンス抵抗R_{REF}とRTDの両方に流れます。もう一方の電流は、リード抵抗RL2を流れ、RL1の両端に発生する電圧降下を相殺する電圧を生成します。高精度リファレンス抵抗に発生する電圧は、ADCへのリファレンス電圧REFIN1(±)として用いられます。1つの励起電流を用いてリファレンス電圧とRTDの電圧の両方を生成しているため、電流源の精度、ミスマッチ、およびミスマッチ・ドリフトは、ADCの全体的な伝達関数にはほとんど影響を与えません。AD7124-4/AD7124-8には励起電流を選択できる機能があり、それによってADCのほとんどの入力範囲を使用するようにシステムを調整できるため、性能を向上できます。

RTDからの低レベルの出力電圧は、ADCのほとんどの入力範囲が使用されるように増幅する必要があります。AD7124-4/AD7124-8のPGAは、ゲインを1～128の範囲で設定可能であるため、励起電流値と、ゲインおよび性能のトレード・オフが可能です。アンチエイリアシングとEMCのために、センサーとADCの間でフィルタリングが必要です。リファレンス・バッファを用いることで、フィルタのRとCの部品値に制限がなくなります。つまり、これらの部品は、測定精度に影響を与えません。

ゲイン誤差とオフセット誤差を除去するために、システムにはキャリブレーションも必要です。図1に、この3線式クラスBRTDについて、内部のゼロスケールおよびフルスケール・キャリブレーション機能を使用して測定した温度誤差を示します。全体的な誤差は±1°Cを大きく下回っています。

ADC条件

温度システムでは、通常、低速で測定が行われます（典型的には最大毎秒100サンプル）。そのため狭帯域幅のADCが必要です。ただし、ADCは高分解能でなくてはなりません。狭帯域幅、高分解能ADCはシグマデルタ・アーキテクチャを用いて作り出せるため、シグマデルタADCがこうしたアプリケーションには適しています。

シグマデルタ・コンバータを用いて、アナログ入力を連続的にサンプリングしますが、このサンプリング周波数は対象となる帯域よりかなり高いものになっています。これらのADCは、ノイズ・シェーピングも使用して、対象帯域外のノイズを、変換プロセスに使用しない領域に押しやるため、対象帯域のノイズを更に低減できます。デジタル・フィルタは対象帯域外の信号をすべて減衰します。

デジタル・フィルタでは、サンプリング周波数およびその倍数にイメージが生じます。そのため、アンチエイリアシング・フィルタがいくつか必要となります。しかし、オーバーサンプリングにより、ほとんどのアプリケーションでは、簡単な一次のRCフィルタで十分です。シグマデルタ・アーキテクチャを用いることで、ピークtoピークの分解能が最大21.7ビットの24ビットADCを作り出すことができます（安定した、つまりフリッカのない21.7ビット）。その他、シグマデルタ・アーキテクチャには次のような利点があります。

- アナログ入力に対する幅広いコモンモード電圧範囲
- リファレンス入力に対する幅広いコモンモード電圧範囲
- レシオメトリックな構成に対応可能

フィルタリング（50Hz/60Hz除去）

上述のノイズ除去の他、デジタル・フィルタは、50Hz/60Hzの除去にも有用です。システムがメイン電源で動作している場合、50Hzまたは60Hzの干渉が発生します。これらはメイン電源で生成される周波数で、ヨーロッパでは50Hzおよびその倍数、米国では60Hzおよびその倍数です。狭帯域幅のADCは、主としてsincフィルタを使用しています。これは、50Hzや60Hzおよびその倍数にノッチを持つよう設定されており、これにより50Hz/60Hzおよびその倍数を除去できます。現在では、セトリング時間の短いフィルタリング方法を用いて50Hz/60Hz除去を行う必要性が増しています。マルチチャンネル・システムでは、ADCは有効化されたチャンネルすべてでシーケンシャルに動作し、それぞれに対して変換を実行します。あるチャンネルが選択されると、そのチャンネルは、そのフィルタ・セトリング時間の間に有効な変換を生成する必要があります。所定時間に変換されるチャンネルの数は、セトリング時間が短いほど多くなります。AD7124-4/AD7124-8にはポストフィルタであるFIRフィルタが内蔵されており、これによって、sinc3またはsinc4フィルタ

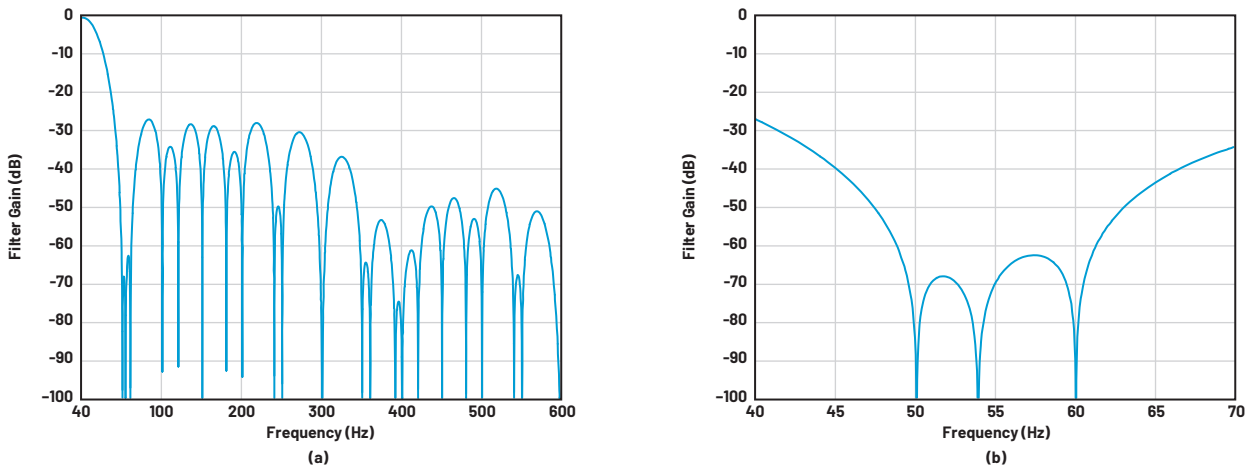

図2　周波数応答、ポストフィルタ、25SPS：(a) DC～600Hzおよび (b) 40Hz～70Hz

よりも短いセトリング時間で50Hz/60Hzの掃除除去を実現します。図2に1つのデジタル・フィルタ・オプションを示します。このポストフィルタのセトリング時間は41.53msで、62dBの50Hz/60Hz同時除去を実現します。

診断機能

機能的に安全な設計を実現するためには、RTCシステムを構成するすべての機能について診断機能が必要です。AD7124-4/AD7124-8には複数の診断機能が組み込まれており、そのため設計の複雑性が軽減され、設計時間を短縮できます。また、診断範囲に対してシグナル・チェーンを二重化する必要性もなくなります。

診断のための代表的な条件は次のとおりです。

- 電源／リファレンス電圧／アナログ入力のモニタリング
- 断線検出機能
- 変換／キャリブレーションのチェック
- シグナル・チェーンの機能性チェック
- 読出し／書込みのモニタリング
- レジスタ内容のモニタリング

組込み診断機能について詳しく見てみましょう。

SPI診断

AD7124-4/AD7124-8ではCRCが利用できます。これを有効化すると、すべての読書き動作にCRCの計算が含まれます。8ビット幅のチェックサムは、次の多項式を使用して生成されます。

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

そのため、AD7124-4/AD7124-8に書込みが行われるたびに、プロセッサはCRC値を生成し、この値がADCに送られる情報に追加されます。ADCは受信した情報から独自のCRC値を生成し、それをプロセッサから受信したCRC値と比較します。両方の値が一致すると、情報は完全であることが確認され、関連するオンチップ・レジスタに書き込まれます。CRC値が一致しない場合、伝送中にデータが破損したことを示します。この場合、AD7124-4/AD7124-8はエラー・フラグをセットし、データ破損が発生したことを通知します。また、破損した情報はレジスタに書き込まないことで、自己防衛も行います。同様に、AD7124-4/AD7124-8から情報が読み出される場合、CRC値を生成して、その情報に付加します。プロセッサは、このCRC値を処理して、伝送が有効なものか破損されたものかを判定します。

AD7124-4/AD7124-8のデータシートには、ユーザ（ユーザ・レジスタ）がアクセスできるレジスタのリストがあります。AD7124-4/AD7124-8は、アクセスするレジスタのアドレスをチェックします。ユーザがデータシートに記載されていないレジスタに対して読出しまたは書込みを行おうとするとエラー・フラグがセットされ、プロセッサが非ユーザ・レジスタにアクセスしようとしていることを通知します。この場合も、このレジスタ・アクセスに付随する情報は、デバイスのレジスタには適用されません。

AD7124-4/AD7124-8にはSCLKカウンタも内蔵されています。すべての読出し／書込み動作は、8の整数倍です。$\overline{CS}$を用いて読出し動作および書込み動作のフレーム化を行う場合、SCLKカウンタは$\overline{CS}$がローになっている間に各読出し／書込み動作で用いるSCLKパルスの数をカウントします。$\overline{CS}$がハイになるときには、この通信で用いるSCLKの数が8の倍数である必要があります。SCLKでグリッチが発生すると、過剰なSCLKパルスが生じることになります。これが生じた場合、AD7124-4/AD7124-8は再度エラー・フラグをセットし、入力された情報をすべて破棄します。

ステータス・レジスタは変換対象のチャンネルを示します。データ・レジスタが読み出されると、ステータス・ビットが変換結果に付加されます。これにより、プロセッサとADCの通信が一層堅牢になります。

したがって、上述の診断機能はいずれも、ADCとプロセッサ間の通信の堅牢性を確保します。こうした診断によって、AD7124-4/AD7124-8は確実に有効な情報のみを受け入れることができます。$\overline{CS}$を読出し動作および書込み動作のフレーム化に使用する場合、シリアル・インターフェースは、$\overline{CS}$がハイになるたびにリセットされます。これにより、すべての通信は定義された状態または既知の状態から確実に開始されます。

メモリ・チェック

オンチップのレジスタに変更が加えられる（ゲインの変更など）たびに、CRCがそのレジスタについて実行され、結果のCRC値は一時的に内部に保管されます。AD7124-4/AD7124-8は、レジスタに対する追加のCRCチェックを内部で定期的に行っています。その結果のCRC値が保管されている値と比較されます。ビット・フリップが原因で値が異なった場合、フラグがセットされます。これにより、レジスタの設定が破壊されたことが、プロセッサに通知されます。次いで、プロセッサはADCをリセットし、レジスタを再読み込みします。

オンチップのROMはデフォルトのレジスタ値を保持しています。起動時またはリセット後、ROMの内容がユーザ・レジスタに適用されます。最終出荷テストで、ROMの内容のCRCが計算され、そのCRC値がROMに保管されます。起動またはリセット時、ROM内容に対するCRCが再度実行され、そのCRC値が保管されている値と比較されます。この値が異なった場合、デフォルトのレジスタ設定が予期されたものでないことを示します。電源のオン・オフを繰り返すか、リセットが必要となります。

シグナル・チェーンのチェック

数多くのシグナル・チェーン・チェックが組み込まれています。ADC入力には電源レール（AV_{DD}、AV_{SS}、IOV_{DD}）を印加でき、これらの電源レールはモニタ可能です。AD7124-4/AD7124-8には、アナログおよびデジタルの低ドロップアウト（LDO）レギュレータが内蔵されています。これらもADCに印加できモニタ可能です。AD7124-4/AD7124-8は、クロス・ポイント・マルチプレクサを内蔵しています。更に、AV_{SS}は、内部でAIN-として使用できます。これにより、アナログ入力ピンの絶対電圧をチェックできます。そのため、ユーザは励起電流の出力先のピンをプローブでき、また、AIN+ピンとAIN-ピンをプローブできます。これによって、接続性をチェックし、様々なピンの電圧が適切なレベルにあることを確認できます。

リファレンス電圧をチェックするために、リファレンス電圧が低すぎる場合に、リファレンス検出機能がこれを示します。また、

ユーザは内部リファレンスをアナログ入力として選択することもでき、それによって、外部リファレンス抵抗の両端の電圧をモニタできます。これは、リファレンス抵抗の電圧が2.5V（内部リファレンスの電圧）よりわずかに高いことが前提です。

また、AD7124-4/AD7124-8は、20mVの電圧を内蔵しています。これはゲイン段をチェックするのに役立ちます。例えば、20mVをアナログ入力として使用して、ゲインを1から、2、4、...、128に変更できます。変換結果は、ゲインが増加するごとに2倍になり、これによって、ゲイン段が正しく機能していることを確認できます。

クロス・ポイント・マルチプレクサもスタック・ビットのチェックに役立ちます。これにより、AIN+ピンとAIN–ピンを切り替えることができます。その後、変換結果は反転されます。そのため、20mVとクロス・ポイント・マルチプレクサを併用することで、ユーザはスタック・ビットをチェックできます。

AIN+とAIN–に対し同じアナログ入力ピンを選択し、この内部短絡をバイアスすることで、ADCのノイズをチェックして、仕様範囲内にあることを確認することができます。組込みリファレンス（+2.5V）をADCへの入力として内部で選択できるため、同様に、$+V_{REF}$と$-V_{REF}$を印加することは、シグナル・チェーンが正常に機能していることを確認するのに役立ちます。

プログラマブルなバーンアウト電流は、センサーの接続性をチェックするのに便利です。PT100の抵抗値は–200°Cで18Ω（代表値）、+850°Cで390.4Ω（代表値）です。バーンアウト電流を有効化した状態で、変換を実行できます。RTDが短絡すると、0に近い変換結果が得られます。AIN+とAIN–の間がオープンになると、変換結果は0xFFFFFFに近い値となります。RTDが正しく接続されていると、0に近いコードやすべて1のコードが生じることはありません。

最後に、AD7124-4/AD7124-8には過電圧および低電圧の検出機能があります。変換されるAIN+ピンとAIN–ピンの絶対電圧は、コンパレータを通じて連続的にモニタされています。AIN+またはAIN–の電圧が電源レール（AV_{DD}およびAV_{SS}）から外れると、フラグがセットされます。

この高集積化によって、測定を実行し、広い診断範囲を提供するために必要な部品表（BOM）を削減できます。設計時間と設計の複雑さも低減されます。

変換／キャリブレーション

AD7124-4/AD7124-8の変換もモニタされます。(AIN+ – AIN–)/ゲインが、正側のフルスケールより大きいか負側のフルスケールよりも小さい場合に、フラグがセットされます。ADCからの変換はすべて1（アナログ入力が高すぎる）またはすべて0（アナログ入力が低すぎる）になるため、ユーザはフォルトが発生したことを認識できます。

変調器が飽和していないことを確認するため、変調器からのビット・ストリームがモニタされています。飽和が発生（変調器からの出力が20回連続1、または20回連続0）すると、フラグがセットされます。

AD7124-4/AD7124-8には内部オフセット機能があるため、キャリブレーションおよびシステムのオフセットとゲイン・キャリブレーションが可能です。キャリブレーションに失敗すると、フラグにより通知されます。なお、キャリブレーションに失敗した場合、オフセット・レジスタとゲイン・レジスタは更新されません。

電源

上述の電源チェックの他、AD7124-4/AD7124-8には、内部LDOレギュレータを連続的にモニタしているコンパレータが内蔵されています。そのため、これらのLDOレギュレータからの電圧が動作点未満になると、直ちにエラーが報告されます。

これらのLDOには外付けコンデンサが必要です。このコンデンサが存在することもチェックできます。

MCLKカウンタ

フィルタのプロファイルと出力データ・レートはMCLKに直接関連しています。データシートに記載されている出力データ・レートが適用できるのは、マスタ・クロックが614.4kHzの場合です。マスタ・クロックの周波数が変化すると、出力データ・レートとフィルタ・ノッチも変化します。例えば、50Hzまたは60Hz

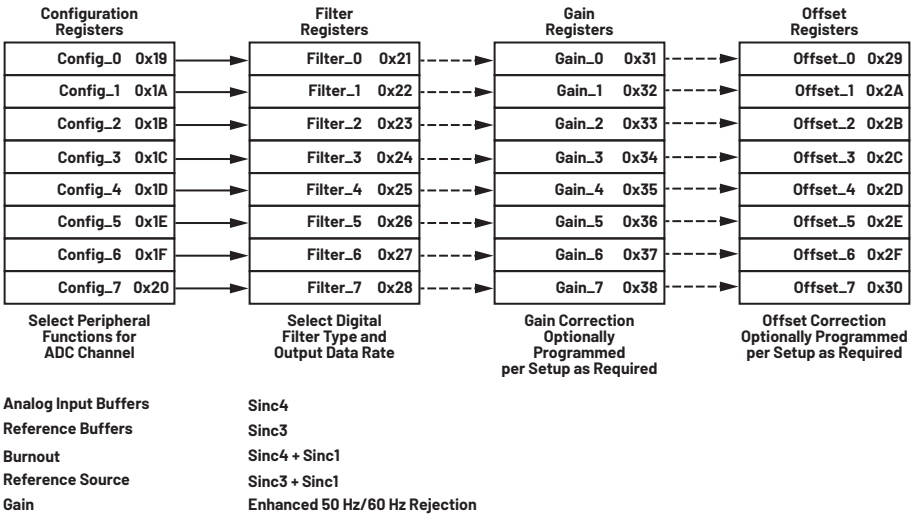

図3　チャンネルごとの構成

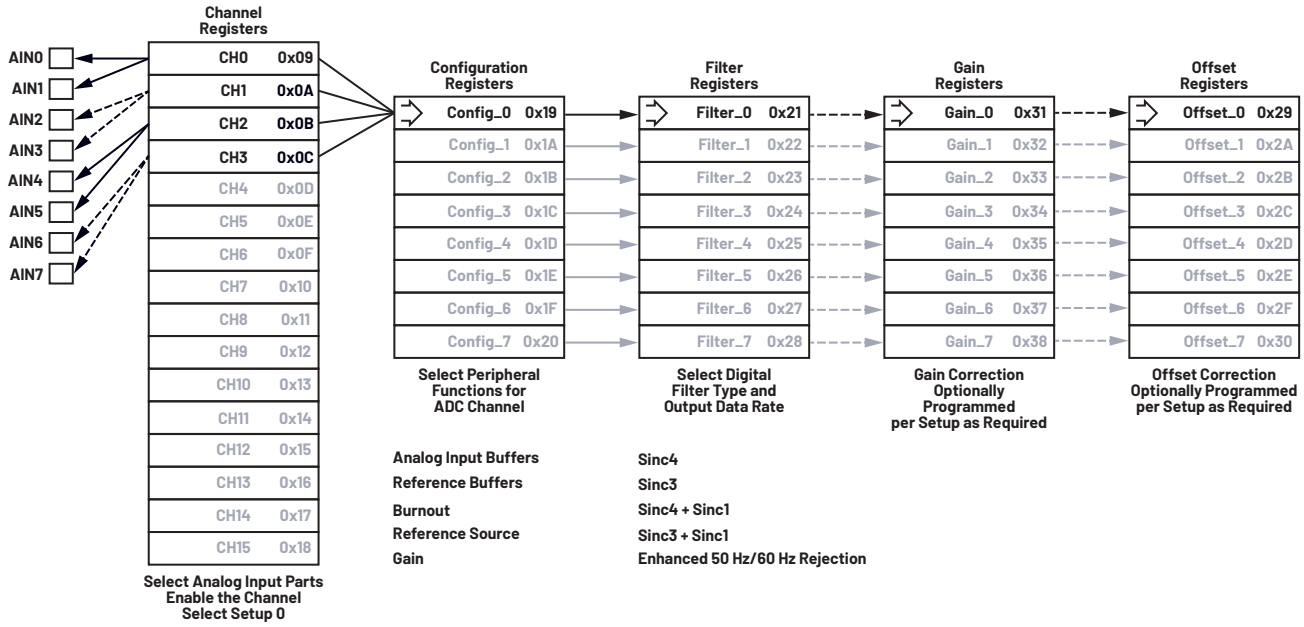

図4　チャンネルへのセットアップ割当て方法

を除去するためにフィルタ・ノッチを使用する場合は、クロックを変更すると実現できる減衰量が低下します。そのため、クロック周波数を知ることは、最大の除去を実現する上で重要です。AD7124-4/AD7124-8にはMCLKカウンタ・レジスタが内蔵されています。このレジスタは131MCLKサイクルごとに1ずつインクリメントします。MCLKの周波数を測定するには、プロセッサ内にタイマーが必要です。レジスタは時刻0で読み出すことができ、その後は、タイマーのタイム・アウト後に読み出せます。この情報を基に、マスタ・クロックの周波数を決定できます。

チャンネルごとの設定

AD7124-4/AD7124-8では、チャンネルごとの設定が可能です。つまり、リファレンス源、ゲイン設定、出力データ・レート、フィルタ・タイプからなる8種類の設定をサポートします。ユーザがチャンネルを設定する場合、この8つの設定のいずれかがチャンネルに割り当てられます。なお、チャンネルは、アナログ入力、または、電源測定（AV_{DD} – AV_{SS}）などの診断とすることができます。そのため、ユーザはアナログ入力および診断で構成されるシーケンスを設計できます。チャンネルごとの設計により、診断はアナログ入力の変換とは異なる出力データ・レートで実行できます。診断ではメインの測定と同じ精度は必要としないため、ユーザは、診断に測定をインターリーブし、また、より高い出力データ・レートで診断を実行できます。このように、これらの内蔵機能により、プロセッサの作業負荷を軽減できます。

その他の機能

AD7124-4/AD7124-8には温度センサーが内蔵されており、これを用いてダイ温度をモニタすることもできます。そちらのデバイスもESD定格は4kVであるため、堅牢なソリューションが可能です。どちらも5mm × 5mm LFCSPパッケージに収められています。このパッケージは、本質的に安全な設計に適したオプションです。

これらのデバイスを使用する代表的な温度アプリケーションのFMEDAは、IEC 61508の定める安全側故障割合（SFF）が90%を超えていることを示しています。従来の2つのADCは通常このレベルの範囲を備えていることが必要です。

組込み診断機能のその他の利点

BOMやコストの削減の他、診断機能は、設計の複雑さを回避すること、リソースの使用量を減らすこと、カスタマ市場への投入までの時間短縮を実現することによって、節約可能にします。次の例を基にして、この点について理解を深めましょう。

AD7124-4/AD7124-8にはMCLKカウンタが備わっており、これを用いると、メインのクロック周波数を測定し、提供されたマスタ・クロックのいかなる種類の不一致も捕らえることができます。マスタ・クロック・カウンタは8ビットのレジスタで、131MCLKサイクルごとに1つインクリメントします。このレジスタはSPIマスタによって読み出され、内部または外部の614.4kHzクロックの周波数を判定します。

MCLK周波数チェックをAD7124-4/AD7124-8の外部で実行しなくてはならないとしたら、どうなるでしょうか。以下のハードウェア・リソースが必要となるでしょう。

- カウンタや外部割込みコントローラのような周辺機能を備えたマイクロコントローラ
- シュミット・トリガ回路

更に、割込みサービス・ルーチンに含まれるコードを保存し実行するためにメモリが必要となる点にも注意してください。全体的な概略は図5に示すようになります。

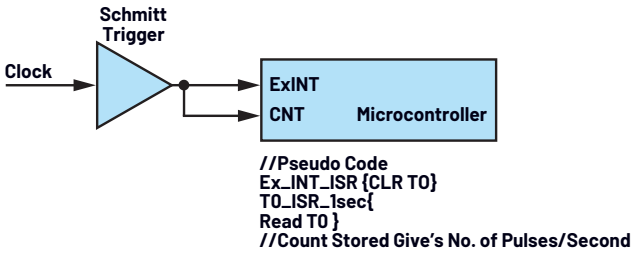

図5　マイクロコントローラによって実行されるMCLK周波数モニタリング

更に、コードがチェックされ、コード化のガイドラインと制限に沿ったものであることも確認する必要があります。そのため、全体として、診断の別のセクションを実行するための大きなオー

バーヘッドが生じます。そのため、組込み診断には以下の利点も付加されます。

- スペースとBOMの節約
- システムの信頼性が向上（部品数が少なくなるために信頼性が向上）
- 市場投入までの時間が短縮
- ソフトウェア開発 – 診断のための開発および実行ルーチン
- ハードウェアのテスト
- システムのテスト
- マイクロコントローラのメモリの節約
  - 診断を実行するためのコードが不要
  - コード化のガイドラインは多数のダブル・メモリ・コード・チェックを要求
- すぐに使える技術文書により、システムの評価時間を短縮

機能的に安全な設計の支援

AD7124-4/AD7124-8はSILの等級付けが行われていません。つまり、IEC 61508規格に従う開発ガイドラインを用いて設計や開発が行われたわけではありません。しかし、様々な診断の最終アプリケーションや使用法を理解すれば、SILの等級付けが行われる設計にAD7124-4/AD7124-8を使用する際の評価ができます。

機能安全性の用語

認証プロセスにとって重要ないくつかの概念を確認しましょう。

- 故障：系統的およびランダム
- 診断範囲
- ハードウェアのフォルト・トレランス
- SILレベル

故障：系統的およびランダム

系統的故障は、特定の原因による決定論的（非ランダム）故障であり、設計、製造工程、操作手順、文書化、またはその他の関連要因を変更することで、なくすことができます。例えば、外部の割込みピンでフィルタリングを行わないと、システムに対しノイズの多い割込みが発生します。

一方、ランダム故障は物理的な原因によるもので、システム内のハードウェア部品に当てはまります。このタイプの故障は、摩耗の他、腐食や熱ストレスなどの影響を原因とし、系統的なプロセスでそのような故障を把握するのは不可能です。

ランダム故障を扱うためには、信頼性、診断、冗長性などの方法を用いることができます。

信頼性では信頼できる部品を確実に使用し、一方で、診断を用いてこうした故障を検出し補正できるようにします。信頼性を確保する別の方法は、冗長性を追加して故障の可能性を下げることですが、この場合は、システム・コストとスペースが増加してしまいます。

ランダム故障には、検出される安全、検出されない安全、検出される危険、検出されない危険の4種類があります。

図6　ランダム故障のタイプ

例えば、温度指示値が高くなった場合に機械の電源スイッチをオープンにするという安全機能を備えたシステムを考えます。この安全機能、つまり、電源スイッチをオープンにすることに影響を与えないランダム故障は、検出される安全な故障、または検出されない安全な故障と呼ばれます。安全機能に影響するその他の不具合は、危険な故障です。最も重要なのは、検出されない危険な故障です。この故障タイプは、診断ではカバーされないため、診断機能を増加して、検出されない危険な故障を最小限に抑えることが目標となります。

診断範囲

ランダム故障は、ソフトウェアやハードウェアの形で様々な組込み検出メカニズムを用意することにより検出できます。例えば、MOSFETスイッチの故障は、出力をリード・バックすることで検出可能であり、ランダムなメモリ・ビット・フリップは一定の間隔でCRCメモリ・チェックを実行することで検出できます。

診断範囲は、システムが危険な故障を検出できる能力のことを指し、危険な故障に対する検出される危険な故障の比として数学的に定義されます。

ハードウェアのフォルト・トレランス

図7に示すようなプログラマブル・ロジック・コントローラ（PLC）システムを考えてみます。この安全機能は、入力が特定の値を超えた場合に、スイッチをオープンにして機械を停止させるというものです。HFT = 0の図では、ランダム故障（X）が1ヵ所で発生すると、システムは不具合を生じ機械は停止しません。

次に、HFT = 1の図に示すように、冗長なパスを設けると、1ヵ所でランダム故障が発生しても不具合の原因とはならず、機械を停止できます。

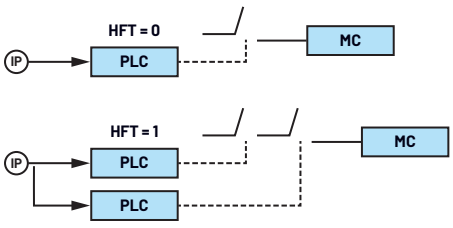

図7　PLCシステム

したがって、冗長なパスを追加することで、1ヵ所の故障に対する耐性ができます。このようなシステムはHFT 1システムと呼ばれ、1ヵ所の故障ではシステムの不具合の原因になりません。

HFT 0は1ヵ所の故障がシステムの不具合の原因になることを意味します。ハードウェアのフォルト・トレランスとは、部品やサブシステムに1つまたは複数のフォルトがあった場合での安全機能を作動できる能力を指します。

HFTは、1oo1、1oo2、2oo3といったアーキテクチャから計算できます。このアーキテクチャがMooNと書き表せる場合、HFTはN – Mと計算できます。すなわち、2oo4のアーキテクチャでは、HFTは2になります。これは、2ヵ所の故障があっても機能できることを示し、冗長性のあるアーキテクチャということになります。

SILレベルの範囲

表1に、SFF（診断範囲の量）およびハードウェアのフォルト・トレランス（冗長性）を示します。

表1　SILレベルの範囲

部品の安全な故障の割合	ハードウェアのフォルト・トレランス		
	0	1	2
<60%	許容対象外	SIL 1	SIL 2
60% to <90%	SIL 1	SIL 2	SIL 3
90% to <99%	SIL 2	SIL 3	SIL 4
≥99%	SIL 3	SIL 4	SIL 4

行は診断範囲の量を示し、列はハードウェアのフォルト・トレランスを示します。HFTが0の場合は、システムに1ヵ所のフォルトがあると安全機能が喪失することを意味します（表1参照）。

図7のように冗長性を追加して、HFT 1を達成すると、システムは、停止することなく1ヵ所の故障に耐えられます。したがって、現在冗長性のあるSIL 3を達成しているユーザは、診断範囲の大きな部品を使用すれば、冗長性がなくてもSIL 3の等級を得ることができます。

このように、診断のレベルを上げると、システムに必要な冗長性を下げることができます。あるいは、同じレベルの冗長性のソリューションのSILレベルを上げる（表1で下方に移動する）ことができます。

ここで、AD7124-4/AD7124-8の診断機能を思い出してみましょう。これらのデバイスは、電源／リファレンス電圧／AINのモニタリング、開放回路検出、変換／キャリブレーションのチェック、シグナル・チェーンの機能性チェック、読出し／書込みのモニタリング、レジスタ電流のモニタリングなど、様々な内蔵メカニズムを備えており、これらの機能によりAD7124-4/AD7124-8システムの診断範囲が増強されています。こうした診断機能がない場合、2つのADCは同じレベルを実現することが必要になります。

そのため、1つのAD7124-4またはAD7124-8は、同じレベルの範囲を備えており、その診断範囲と機能によって、機能的に安全なシステムの設計が可能です。これにより、BOMとプリント回路基板の面積を50%削減できます。

SILの等級付けが行われた設計に対応する文書化

エンド・システムのSIL認証を支援するために必要な文書は以下のとおりです。

- 安全データシート（安全マニュアルはSIL等級のある部品用）
- ピンのFMEDA（故障モード、影響、および診断解析）およびダイのFMEDA（故障モード、影響、および診断解析）
- 附属書Fのチェックリスト

これらの文書は、図8に示すように、主として4つのデータ・ソースからの入力で構成されています。そのデータとは、診断データ、設計データ、FITレート、故障挿入試験のデータです。

- データシートの診断データは、その部品で得られるすべての診断機能を含んでいます。
- 設計データは、内部データ（ダイ面積、および部品の各内部ブロックおよびあらゆる内部ブロックの影響など）のことを指します。
- 様々な部品のFIT率（10億時間あたりの故障数）は、データ・ブックから入手できます。一般的な例はSiemens Databook SN 29500です。

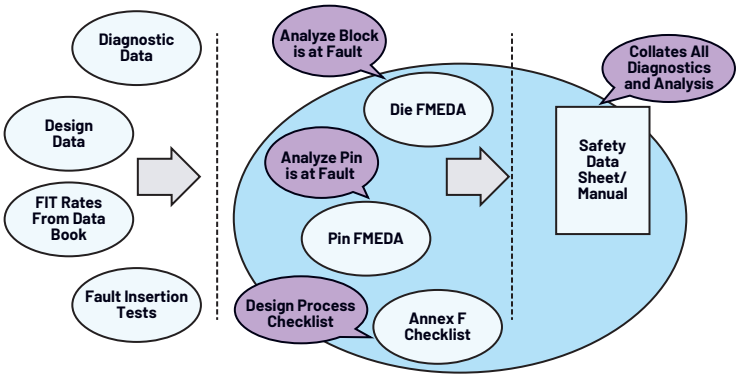

図8　機能安全文書の情報の流れ

- 故障挿入試験はブロックごとに行われ、設計データや診断データでは解析できません。これらの試験は、必要なアプリケーションを基に計画され、故障挿入試験の結果は、FMEDAやFMEAの文書を補強するために用いられます

ダイのFMEDA

AD7124-4/AD7124-8のFMEDAは、アプリケーションの回路図のメイン・ブロック解析、故障モードおよび影響の特定、特定の安全機能の診断と解析のチェックを行います。そのメカニズムを理解するために図9を見てみましょう。

RTDタイプのシステムでは、安全機能は、±x度の精度で温度を測定することです。そのアプリケーションの回路図を図9に示します。

危険なフォルトを、ADC出力またはSPI通信でのエラーの原因となる可能性のあるフォルトと定義し、出力のエラーが重大である場合には、危険な故障の原因となります。

安全な状態は以下のように定義されます。

- 出力のデータが安全機能に基づき入力を表している
- エラー・ステータス・ビットがセットされている
- ADCの出力変換結果がすべてゼロまたはすべて1である
- SPI通信がない

AD7124-4/AD7124-8は、IEC 61508に従い、タイプBのシステムとみなされます。

FMEDAを説明するために、クロック・モジュールを例にその故障モードを解析します。

表2は、クロック・ブロックが最初の列に記載された故障モードとなった場合に、それが出力、診断範囲、および最終的には解析にどう影響するかを示しています。

表2　マスタ・クロック・ブロックの故障モード、影響、診断、解析

故障モード	影響	診断範囲	解析
出力がハイにスタック	ADC変換結果がフリーズ	99	MCLKクロック・カウンタ－表A.11－「時間窓がある個別の時間基準によるウォッチドッグ」
出力がローにスタック	ADC変換結果がフリーズ	99	MCLKクロック・カウンタ－表A.11－「時間窓がある個別の時間基準によるウォッチドッグ」
出力が高インピーダンス	ADC変換結果がフリーズ	99	MCLKクロック・カウンタ－表A.11－「時間窓がある個別の時間基準によるウォッチドッグ」
出力ドリフト±10%	ADC変換結果が破損。50Hz/60Hzのノッチが有効化しない	99	MCLKクロック・カウンタ－表A.11－「時間窓がある個別の時間基準によるウォッチドッグ」
出力ジッタ	ADC変換結果が破損またはノイズが多くなる	99	0、±FSを変換－表A.13「基準センサー」、結果に対する妥当性チェック

同様に、AD7124-4/AD7124-8のその他のブロックを解析します。

なお、場合によっては安全機能に影響しない故障もあります。例えば、AIN0ピンの故障は、温度測定にとって問題の原因とはなりません。そのため、安全性の計算からは除外できます。

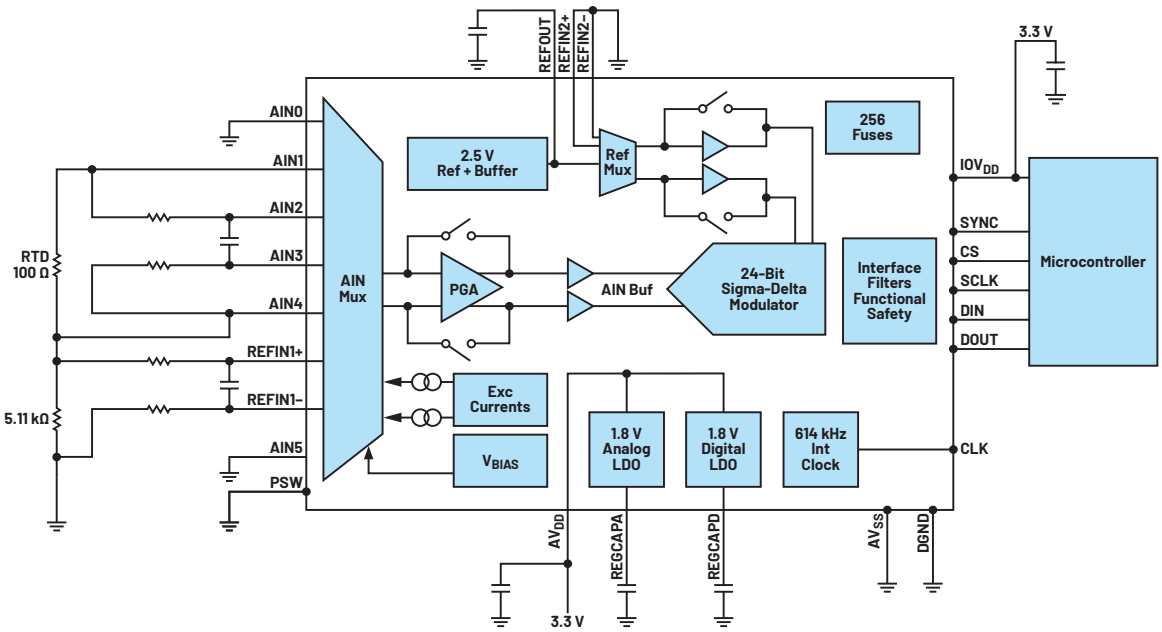

図9　RTDアプリケーション回路図

FMEDAの結果は、安全な故障、検知される危険な故障、検出されない危険な故障の故障率で、これらはSFFを計算するために用いられます。

ピンのFMEDA

ピンのFMEDAは、AD7124-4/AD7124-8のピンの様々なタイプの故障およびそのRTDアプリケーションに対する影響を解析します。順を追って、各ピンを取り上げ、ピンが電源やグラウンドに対しオープンになった場合や短絡した場合、あるいは隣接ピンに短絡した場合の影響を解析します。

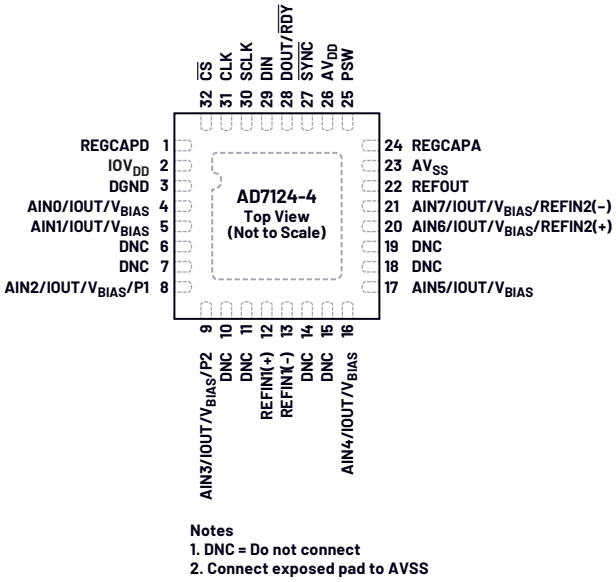

図10　32ピンLFCSPのピン配置

図10のピン29（DIN）を例に取り、図9に示したアプリケーション回路図を参照して様々な故障の結果を確認してみましょう。故障モード、影響、検出について、表3に示します。

表3　DINピンの故障モード、影響、および解析

ピン名	可能性のある故障モード	可能性のある故障の影響	検出
DIN	ピンがオープン	通信不能	システム・レベルで容易に検出可能
DIN	グラウンドに短絡	通信不能	システム・レベルで容易に検出可能
DIN	AV_{DD}またはIOV_{DD}に短絡	通信不能、損傷の可能性	システム・レベルで容易に検出可能
DIN	隣接ピンSCLKに短絡	通信不能	システム・レベルで容易に検出可能
DIN	隣接ピンDOUT/RDYに短絡	通信不能	システム・レベルで容易に検出可能

解析は図9に示したアプリケーション回路図について行ったものであり、未使用のピンの解析はどこにも影響しない点に注意してください。

附属書Fのチェックリスト

これは、ASICの系統的な故障を回避するための、設計手段に対するチェックリストです。準拠するには、IEC 61508-2:2010の完全な附属書Fのチェックリストが必要です。

安全マニュアルまたはデータシート

情報の全セットの最後は、安全マニュアルまたはデータシートで、これは、AD7124-4/AD7124-8の統合を可能にするための必要条件を記載したものです。

IEC 61508の機能安全規格に準拠していることを示す場合、様々な文書からもたらされるすべての診断と解析を安全データシートが照合します。これには以下の情報がすべて含まれます。

- 製品の概要
- アプリケーション情報
- 安全コンセプト
- 寿命予測
- FIT
- FMEDAの計算 – SFFおよびDC
- ハードウェアの安全機構
- 診断の説明
- EMC堅牢性
- 冗長構成での動作
- 附属書および文書のリスト

ルート2S（別名：使用実績による証明）

評価のための最初の方法を説明してきました。次に、使用実績による証明またはルート2Sと呼ばれる代替方法を説明します。この方法は、販売済みの部品に適用でき、顧客からの返品と出荷したデバイス数の解析に基づくものです。

この方法によって、その部品がIEC 61508規格に従って完全に開発されたように、SIL認証を受けることができます。

ルート2S、つまり使用実績による証明の主張は、モジュール設計者やシステム設計者が過去に問題なくICを用い、故障率がフィールドからのデータで分かっている場合に、利用できます。

なお、ルート2Sではフィールドからの返品の全データが必要となります。そのため、一般的には最終アプリケーションの十分な知識がなかったり、フィールドからの故障ユニットが解析のために返品される率が不明だったりするために、集積回路設計者やメーカーにとってはこの主張をすることははるかに困難です。

まとめ

RTD測定システム向けのADCやシステムの条件には、極めて厳しいものがあります。こうしたセンサーから生じるアナログ信号は微小であるため、アンプのノイズがセンサーからの信号を覆い隠してしまうことのないノイズの小さなゲイン段で増幅する必要があります。アンプに続き、センサーからの低レベル信号をデジタル情報に変換するために、高分解能ADCが必要となります。ADCおよびゲイン段の他、温度システムには励起電流などの要素も必要です。ここでも、システム精度を低下させないために、部品は低ドリフト、低ノイズでなくてはなりません。オフセットなどの初期の不正確さはキャリブレーションによりシステムから除外できますが、温度に伴う部品のドリフトは、誤差の発生を避けるために低くなくてはなりません。そのため、励起ブロックと測定ブロックを統合すると、ユーザ設計を簡略化できます。機能安全を設計する場合は、診断の必要性が追加されます。診断と励起ブロックおよび測定ブロックを統合することで、全体的なシステム設計が簡素化され、BOM、設計時間、市場投入までの時間を削減できます。

FMEDAなどの文書には、ユーザが最終設計でのコンポーネントの認証を受けるために必要な情報がすべて含まれています。ただし、自分自身でコンポーネントの確認を行うことで、認証機関とのやりとりが更に容易なものになります。ルート2Sプロセスによって、販売後の製品の認証を受けることができます。そのため、現在販売されている多くのデバイスが機能的に安全な設計に適合している場合には、便利な手段です。

更に詳しい資料

- アナログ・デバイセズの機能安全サイト
- 付随資料 – RTD測定（CN0383）
- 記事：RTDをベースとする温度計測システムの最適な設計

著者について

Mary McCarthyは、アナログ・デバイセズのアプリケーション・エンジニアです。1991年に入社し、アイルランドのコークでリニアおよび高精度技術アプリケーション・グループにおいて、高精度シグマデルタ変換を中心に従事しました。1991年、ユニバーシティ・カレッジ・コークで電子および電気工学の学士号を取得して卒業しました。

Wasim Shaikhは2015年に、インドのバンガロールにある高精度コンバータ部門のアプリケーション・エンジニアとしてアナログ・デバイセズに入社しました。認証済み機能安全のエンジニアで、2003年にプネー大学で学士号を取得しました

＊英語版技術記事はこちらよりご覧いただけます。

TA23731-7/22