データ・アクイジション・システムにおける機能安全

著者: Chris Norris

はじめに

多くの業界では、安全に関する総合的な戦略の1つとして機能安全の実現が求められています。機能安全では、人体や稼働中の装置に害が及ぶ確率を許容できるレベルまで低減することを目指します。近年、システムの機能的な安全性に関する要件は、大幅に拡大しています。原子力発電所から医療用機器まで、システムにエラーが存在しないことが理想的だとされている分野もあれば、エラーが存在しないことは必須だと位置づけられている分野もあります。システムの種類や潜在的なリスクのレベルにもよりますが、例えば、センサーによって収集したデータに誤りや損傷があると、壊滅的な状況に陥ったり、人命に関わる事態を招いたりする可能性があります。

センサーICで取得したデータの質（インテグリティ）を保証するためには、診断や故障防止のメカニズムを製品の中に組み込まなければなりません。従来は、その責任をシステム開発者が負っていました。ただ、そうしたメカニズムを組み込もうとすると、プリント配線基板の面積や、部品点数、診断などの処理に伴うオーバーヘッドに影響が及びます。したがって、最終的にはコストが大きく増大していました。その後、広範な領域を対象として、ICメーカーとシステム設計者が連携を図った結果、この問題の解決に向けたソリューションが開発されるようになりました。つまり、機能安全を実現するための機能がICに実装されるようになったのです。

現在では、データ・アクイジション・システムにおいて全体的な質を保証するために、機能安全に向けた機能がA/Dコンバータ（ADC）に盛り込まれるようになっています。本稿では、その潜在的な能力について解説します。

機能安全に向けた旧来の手法、より優れた最新の手法

図1は、機能安全に対応する旧来のシステムと最新のソリューションを比較したものです。システムの中心にあるのは、データ・アクイジション用のADCです。それにより、アナログの入力信号をデジタル値に変換し、そのデータをマイクロコントローラに転送します。旧来のシステムでは、ADC以外にも多くの外付け部品を使用しなければなりませんでした。また、SPI（Serial Peripheral Interface）を使用したトランザクションが繰り返されるほか、ADCの冗長化も必要になります。そうした要因により、部品点数、プリント基板の面積、各種の処理に伴うオーバーヘッド、コストが増大します。加えて、このようなソリューションを開発するためには、多くの時間を要します。更に、信頼性を高めるためには、システム設計者の負担が増大することになります。

それに対し、現在では、必要な外付け部品を最小限に抑えつつ機能安全を実現可能な、シングルチップのADCによるソリューションが提供されるようになっています。

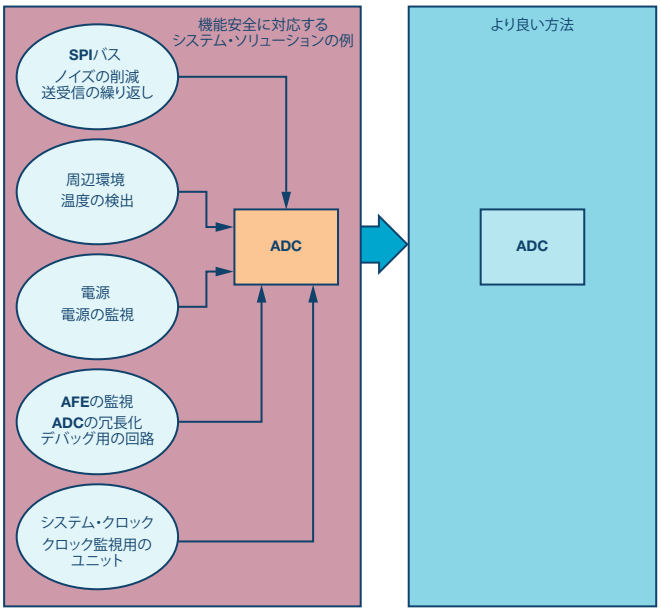

図1. 機能安全に対応するシステムの比較。
従来は、複数の部品を使用することにより、機能安全を実現していました。アナログ・デバイセズは、それらをシングルチップのソリューションとして統合しています。

機能安全向けの要件を備えたシステムの例

ADCを使用するデータ・アクイジション・ システムでは、アプリケーションに依存して、人体や装置の健全性に対するリスクを増大させる可能性のある多くの障害が発生します。したがって、システム設計者は、許容できるリスクと許容できないリスクを区別しなければなりません。

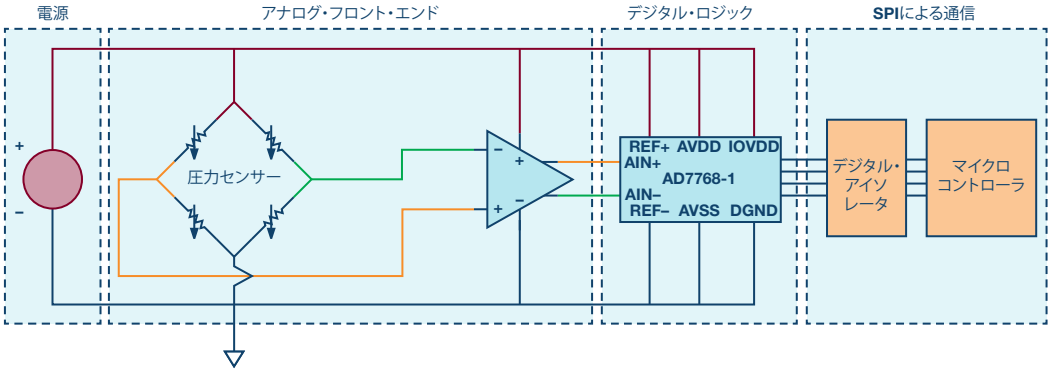

図2. 圧力センサーを使用するシステムの例。
障害の発生源として想定される部分には、色付けしてあります。

一例として、ガス・チャンバの圧力を計測／制御するシステムにおいて、許容誤差が5%の圧力センサーを使用するとします。この誤差は、タンクの内部の圧力が外圧と大きく異なっていなければ、許容できるリスクだと見なされるかもしれません。但し、マイクロコントローラがADCから誤ったデータを受信してしまうとどうなるでしょうか。その場合、チャンバ内の圧力によって、近くにいる人の生死に関わる内破や爆発といった致命的な事故が起きる可能性があります。言うまでもなく、このようなレベルのリスクを許容することはできません。こうした理由から、コントローラが受信する情報の質を保証するために、機能安全に向けたいくつかの計測を導入すべきです。

致命的な問題を引き起こす可能性のある障害の発生源としては、以下のようなものがあります。

- 電源：電源電圧が低すぎたり、ADCが内蔵するLDO（低ドロップアウト）レギュレータの出力電圧が低すぎると問題が生じます。
- アナログ・フロント・エンド（AFE）：ADCが、損傷したセンサーやアンプによって不適切な電圧で駆動されるおそれがあります。
- デジタル・ロジック：デジタル領域のビット・エラーによって、変換結果に影響が及ぶ可能性があります。例えば、工場から出荷された際に設定されたゲイン／オフセットを調整するための係数に誤りがあると、そのようなことが生じます。
- SPIによる通信：雑音が多い環境に通信ラインが存在する場合、A/D変換後のデータの伝送時やコマンドの受信時にビット・エラーが生じることがあります。
- 周辺環境：ICの周囲温度が仕様の範囲外になると、問題が発生する可能性があります。

アナログ・デバイセズは、機能安全に向けた数多くの機能を備えるADC製品を提供しています。そうした機能安全対応のADCの例としては「AD7768-1」が挙げられます。これはシグマ・デルタ（ΣΔ）方式のADCですが、ユーザがエラーの検出などを行えるようにするための多様な診断機能を備えています。図2に示したのは、圧力センサーを使用する標準的なシステムの例です。ADCとしては、機能安全に対応するAD7768-1を採用していると仮定しています。また、故障の発生源として想定される部分には色付けしてあります。次のセクションでは、このようなシステムを例にとって解説を進めます。

ADCによるシステム・エラーの診断

機能安全対応のADCを採用すれば、システムにエラーが生じていないかどうか診断したり、エラーを削減したりすることができます。システムとして正確な計測が行える状態を維持するためには、このシステム・エラーの測定能力が重要な意味を持ちます。機能安全に関する要件が課せられているシステムでは、その精度が非常に重要になります。

システムのゲイン誤差は、リファレンス入力を基準とする正と負のフル・スケール電圧を使って測定します。オフセット誤差は、ADC内部でショートさせることで得られるゼロ・スケールを使って測定します。ユーザは、ADCが備えるゲイン／オフセットの調整用レジスタを使うことにより、システムとしてのオフセット／ゲイン誤差を補正することができます。

温度センサーは、ICの周囲温度（仕様の範囲外を含む）の変化を検出します。この機能は、温度によるオフセット／ゲイン誤差のドリフトに弱いシステムでは、特に有効なものとなります。大きな温度変化が生じた場合に、変化後の温度の下でゲイン／オフセットの誤差を補正することも可能です。図3は、AD7768-1の内部で、ADC機能とアナログ診断機能用のマルチプレクサがどのように接続されているのかを表しています。

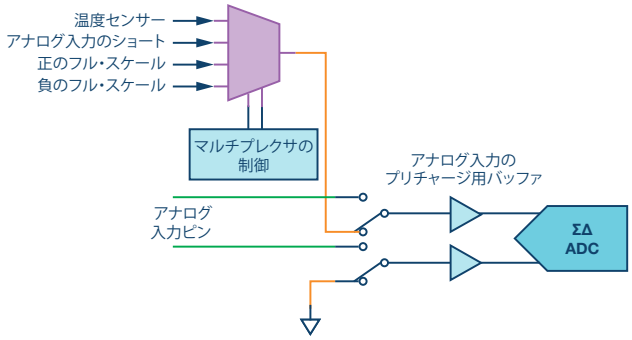

図3. アナログ診断機能用のマルチプレクサとADC機能の接続

診断エラー・フラグ：レジスタ・マップによる状態表示

いくつかの診断機能をイネーブルに設定すると、ユーザに対し、レジスタ・マップを介してそのときの状態をフラグとして示すことが可能になります。障害が発生した場合には、レジスタにはエラー・フラグがセットされます。そのようにして障害に関する警告が示されたら、ユーザはより詳細な調査に乗り出すことができます。

実際に発生する可能性があり、機能安全対応のADCを使って診断できる障害としては、どのようなものがあるでしょうか。例として、ある工場に、圧力センサーを備えるシステムが設置されているケースを考えます。その場合、温度の変動や、必ず実施しなければならないメンテナンスによる電源のシャットダウン、周囲の環境からシステムのプリント基板に影響を及ぼすEMI（電磁妨害）などの事象が発生する可能性があります。

ADCの電源のエラー

ADCを使用している際には、周囲温度が上昇したり、システムの電源の状態が変化することによって突入電流が生じたりすることがあります。それらが原因となり、ADCが内蔵するLDOの出力コンデンサが劣化し、損傷に至る可能性があります。そうした事態を避け、LDOの出力を本来の値に保って正確な動作を得るには、外付けのコンデンサが必要になります。上記のような事柄が原因でコンデンサが損傷すると、A/D変換後のデータの質や、他の機能の性能が予測できない状態になります。LDOの監視機能をイネーブルにすることにより、電圧のレベルがある値よりも低下したときにエラー・フラグをセットし、ユーザに対してLDOの出力に問題があるという警告を発することができます。

アナログ・フロント・エンドのエラー

ここで想定しているシステムでは、ADCの入力がそのフル・スケール範囲を超えることはないと仮定します。ところが、ゲインを設定するためのレジスタにユーザが誤った値を設定し、ADCのフル・スケール範囲よりも入力電圧が大きくなってしまったとしましょう。その場合、システムのゲイン誤差に大きな影響が及び、重大なリスクが生じている状態になります。しかし、機能安全対応のADCを採用していれば、フィルタの飽和という問題が生じていないかどうかを監視することができます。つまり、ADCの出力が監視され、ユーザに対してアナログ入力が許容範囲外にあるという警告が発せられます。

デジタル・ロジックのランダムなビット・エラー

デジタル・ロジック部やメモリ・ブロック部では、ランダムなビット・エラーが発生することがあります。本稿で例にとっている圧力計測システムでは、工場から出荷されるときにオフセットに関するデフォルトの設定が用意されているとしましょう。電源を投入した際にその設定がロードされるわけですが、その最中にビット・エラーが発生したと仮定します。そうすると、システムのオフセット誤差を正しく補正することができず、変換結果に悪影響が及びます。つまり、これは許容できない障害だということになります。機能安全対応のADCは、定期的に各種メモリ・ブロックに対して巡回冗長検査（CRC）を実行し、ビット・エラーが検出された際には、障害の発生を示すフラグを立てる機能を備えています。なお、この種の障害は、システムをリセットすることによって解消されます。

SPI通信のエラー

媒体を介したデータ伝送を伴うすべてのシステムでは、データの伝送中にビット・エラーが発生する可能性があります。

その発生頻度は、システムごとに予測することが可能であり、ビット・エラー・レート（BER）という指標で表されます。

本稿で例にとっている圧力計測システムでは、同じプリント基板上で10cm離れたマイクロコントローラにデジタル・アイソレータを介してデータを伝送する場合、BERは10^{-7}未満に抑えられると考えられます。

SPIの信号ラインがEMIの影響を受け、そのことがAD7768-1の出力データをマイクロコントローラに伝送する際のビット・エラーの要因になっていると仮定します。そのビット・エラーにより、ガス・チャンバ内の圧力が上昇しているという事実が隠蔽されてしまうかもしれません。そうすると、壊滅的な結果に及ぶ可能性があります。送信データの末尾にCRC用のデータを付加することで、送信中にビット・エラーが生じたか否かを把握することができます。エラーが生じていることが明らかになれば、ADCからのデータを再確認するという対処を図れるようになります。

外部マスタ・クロックのエラー

圧力センサーを使用するアプリケーションにおいて、主電源に含まれる50Hz/60Hzの周波数成分を除去したいと考えているとします。その場合、デジタル・フィルタの周波数応答において、50Hz/60Hzの位置にノッチが現れるように正確に調整を実施することになるでしょう。そのためには、精度が高くジッタの小さい外部マスタ・クロック・ソースを使用することが重要になります。クロック・ソースが切り離されたり、劣化したり、損傷したりすると、主電源の周波数成分の一部がADCの出力データ中に現れてしまうかもしれません。したがって、マスタ・クロックは非常に重要です。

外部クロック用の診断回路を使用すれば、外部クロック・ソースが正しく接続されていなかったり、除去されていたりした場合、その事実がエラー・フラグによって示されます。なお、外部マスタ・クロック・ソースに対して必須の保守作業が行われている間は、ADCが内蔵するRC発振器を使って変換処理を実施するという方法もあります。

PORのフラグ

システムのパワー・アップあるいはリセットが問題なく行われたら、ADCの内部でPORフラグがセットされます。

予期しないリセットが発生した場合、ADCの出力データが想定外の結果になっているかもしれません。そのような場合には、PORフラグを確認することによって、予期しないリセットが発生したことを把握することができます。

上述したように、AD7768-1は様々な診断機能を内蔵しています。図4は、それらの診断機能によってどのような事柄を監視できるのかを示したものです。

AD7768-1による完全な機能安全ソリューション

AD7768-1を採用した場合、どのようなデータ・アクイジション・システムを構築できるのでしょうか。同製品を活用すれば、以下のような機能安全機能を実現できます。

- SPIの健全性の監視
- LDOの出力レベルの監視
- フィルタの飽和の検出
- 外部クロックの診断
- 内部ロジック／メモリのCRC診断

システムのキャリブレーションについては、ADCが内蔵するアナログ診断機能用のマルチプレクサを活用することで検証できます。LDOの出力もこの方法により確認することが可能です。

また、診断機能をイネーブルに設定すると共に、8ビットのステータス・データを24ビットのデータ・ストリームの末尾と8ビットのSPI用のCRCワードに付加したとします。8ビットのCRCは、8ビットのコマンド・ワード、24ビットのデータ・ストリーム、8ビットのステータス・ワードを使って計算されます。処理に伴うオーバーヘッドの量が気になる場合、連続リードバック・モードを有効にして8ビットのコマンドを不要にします。その代わり、図5に示すように、レジスタの内容を、ADCに供給されているシリアル・クロックを使って出力することになるでしょう。

この処理の結果、データ・アクイジション・システムのゲイン／オフセットの誤差が確認されます。そして、ADCの出力データをリードバックするたびに、診断に関する情報がユーザに提供されます。

LDOの出力、アナログ・フロント・エンドの入力、内部のデジタル・ロジック、メモリは、常に監視されています。また、SPIによる通信品質を確保できるほか、ICの温度を把握することも可能です。

まとめ

多くの業界では、機能安全に関する要件が拡大している状況にあります。当然のことながら、それに対応するための技術も増強していかなければなりません。もちろん、アナログ・デバイセズは、そうした技術の開発を続けています。そして、ADC製品に、自身の機能が安全に動作しているか否かを診断する機能を追加することで、システム設計者を支援しています。

AD7768-1はより小型かつシンプルな製品でありながら、システム設計者の負担軽減に大いに貢献します。これを採用すれば、ソリューションの構築に必要な部品点数と、各種処理のオーバーヘッドを削減することができます。この単一ICを使用するアプローチにより、自身が行った設計について、安全度水準（SIL：Safety Integrity Level）の認証を取得したいと考えているシステム設計者の負担も軽減できます。

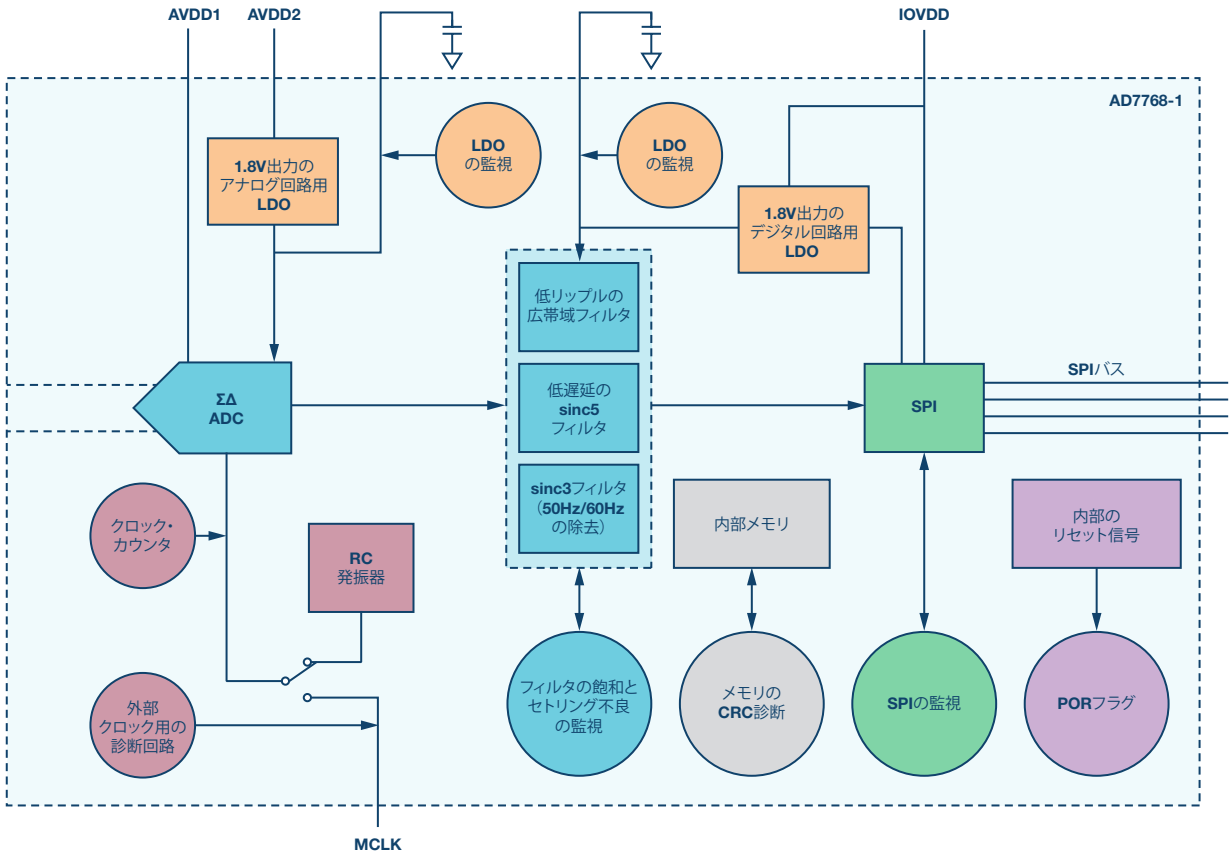

図4．AD7768-1が内蔵する診断機能

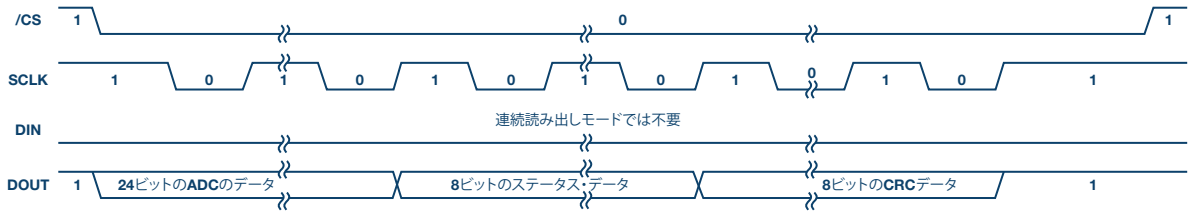

図5. AD7768-1の連続リードバック・モード。付加されたステータス・データとCRCデータを使ってレジスタの内容をリードバックします。

著者：

Chris Norris（christopher.norris@analog.com）は、アナログ・デバイセズでADCの設計の評価を担当しています。アイルランド リメリックの事業所に所属しています。2012年にウォーターフォード工科大学で電子工学の学士号を取得し、アナログ・デバイセズに入社しました。