機能安全に対応可能なΣΔ型のADC

著者：Miguel Usach Merino

概要

産業用の装置については、新たな国際規格や規制が登場したことを受け、安全を確保するための機能（以下、安全機能）を組み込む必要性が高まっています。本稿のテーマである機能安全の目的は、人間や資産に危険が及ばないよう保護することです。機能安全は、特定のハザード（危険）を対象とする安全機能をシステムに適用することによって実現します。その際、安全機能は、センサー、ロジック回路、出力ブロックなどを含む一連のサブシステムによって構成されます。機能安全を採用する設計に向けて、適切な機能群を備えるICを提供するには、システムと集積回路という2つの領域の専門知識が必要になります。本稿では、アナログ・デバイセズ（ADI）の「AD7770」を取り上げ、機能安全に対応可能なΣΔ型のA/Dコンバータ（以下、ΣΔ ADC）について解説します。このICは、アナログとデジタルの両方のドメインで高度な機能群を備えています。この高性能のICを利用すれば、安全機能を備えるシステムの設計を簡素化することができます。

はじめに

マーフィーの法則の派生形として、「失敗をもたらす事象がいくつか想定されるとき、実際に発生するのは、最悪のダメージをもたらす事象である」というものがあります。

システムの中には、構成要素である機械類が故障すると、人命に直接的/間接的な脅威が及ぶタイプのものがあります。そのようなシステムは、故障の可能性と、故障がもたらす悪影響を最小限に抑えられるように設計しなければなりません。確率論的に発生するランダムな故障と決定論的に発生する故障を確実に最小限に抑えるには、それを目的とする方法論を適用して設計を行う必要があります。機能安全（Functional Safety）と呼ばれるその方法論では、まずシステムを細部まで解析し、潜在的に危険をもたらす可能性のある状態を特定します。そうした状態の例としては、過度な高電圧が存在したり、診断によって故障が検出されたりするケースが当てはまります。そうした状態を特定したうえで、ベストプラクティスを適用することにより、誤動作のリスクをコンポーネント、サブシステム、システムのそれぞれが許容できるレベルにまで引き下げるように設計を行います。

機能安全という概念の背景にあるのは、エラーが検出された場合でも、システムを安全な状態に保てるようにするという考え方です。例えば、外部のセンサーから得られた結果が許容範囲外の値であれば、アクティブな出力を遮断するといった具合です。

IEC 61508は、機能安全に基づく産業用装置の設計に関する基準を規格として定めたものです。これを基にして、さまざまな業界向けに策定された規格も存在します。IEC 61508をそれぞれの用途に適合するように解釈/改変することで策定されたということです。自動車向けのISO 26262やプログラマブルコントローラ向けのIEC-61131-6などがこれに当たります。

機能安全の規格に従った設計は、かなりの作業負荷を伴う可能性が高くなります。システム全体の記述から、使用するコンポーネントの内部の機能ブロックに至るまで、トップダウン方式で詳細な解析を行わなければならないからです。あらゆる危険な状態を回避できるだけの十分な保護レベルを保証し、検出されないエラーの発生確率を最小限に抑えるために、そのような解析が必要になるのです。機能安全に基づいて設計したシステム（以下、機能安全システム）とは、任意のエラーを検出して素早くそれに対処し、危険な状態の発生確率を最小限に抑えられるようにしたものです（図1）。

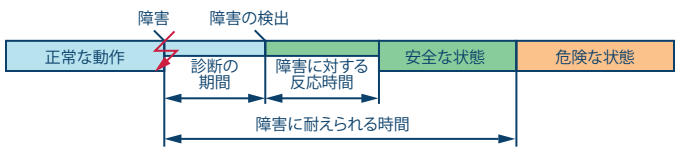

図1. 機能安全システムの反応時間

機能安全システムの設計方法

まず、人体に危害が及ぶ可能性のある状況を特定するためにハザード解析を実施します。そうした状況を明らかにしたうえで、危険な状態を回避できるようにシステムを設計するということです。回避が不可能な状況があり得る場合には、危険な状態を検出してシステムを安全な状態に移行させるための機能を追加します。

ここでは、図2のシステムを例にとることにします。このシステムでは、爆発のリスクを最小限に抑えるために、タンクの温度に基づいてタンクに接続されているバルブを開くという制御を行います。具体的には、D/Aコンバータ（DAC）を使用し、モーターを介してバルブの開口部を制御します。このシステムはオープンループのシステムです。

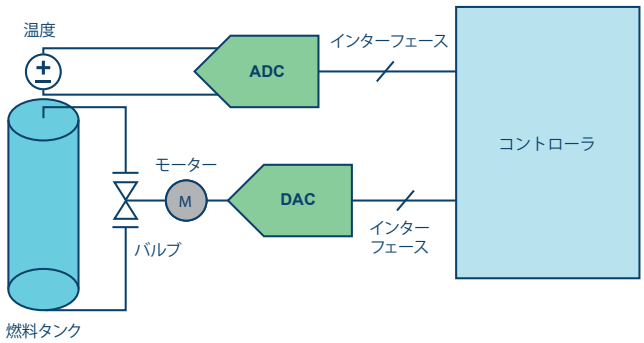

図2. オープンループのバルブ制御システムを構成するシグナル・チェーン

ハザード解析を行うと、次の2つの状況で不安定な状態が生じ得ることがわかります。

- 温度の測定値が不正確であるために、バルブの開口制御が正しく行われない
- DACに問題があり、バルブが正しく開閉されない

次に、各ハザードに伴うリスクを評価します。

［リスク］=［危険の発生確率］×［危険の深刻度］

リスクを算出したら、続いては、そのリスクを許容できるレベルまで抑えることを可能にする機能安全システムを設計します。

IEC 61508では、4つの安全度水準（SIL：Safety Integrity Level）が定められています。これは、安全機能によって達成されるリスクの低減レベルを定義したものです。同規格では、2つの確率が目標として使用されます。1つはPFD（Probability of Failure on Demand：需要時故障確率）です。これは、イベントによってトリガされるまでスタンバイの状態に保たれるシステムに適用されます。代表的な例としてはエアバッグが挙げられます。もう1つのPFH（Probability of Failure per Hour：1時間当たりの故障確率）は、図2の例のように常時稼働しているシステムに適用されます。表1に、IEC 61508のSIL、ISO 26262（ASIL）、航空用電子部品の規格で定められた基準と、PFD/PFHとの大まかな対応についてまとめました。

表1. 各規格で定められたレベルの大まかな対応

PFD	PFH	規格		
		IEC 61508のSIL	自動車	航空用電子部品
0.1 ～ 0.01	10^{-5} ～ 10^{-6}	1	A	D
0.01 ～ 0.001	10^{-6} ～ 10^{-7}	2	B	C
0.001 ～ 0. 0001	10^{-7} ～ 10^{-8}	3	C/D	B
0.0001 ～ 0.00001	10^{-8} ～ 10^{-9}	4		A

SILは、検出されない故障をどれだけ低減して最小化する必要があるかということに基づいています。その種の故障は、システムの誤動作を招き、望ましくない状態を引き起こす恐れがあります。

診断カバー率の要件

検出されない故障の発生確率は、診断カバー率（DC：Diagnostic Coverage）が高いほど低下します。システムの診断カバー率が99%であれば、SIL3を達成できます。90%ならばSIL2、60%ならばSIL1となります。検出されないエラーは冗長性を高めるほど減少します。

SIL2またはSIL3を達成するための簡単な方法は、その保護水準をすでに満たしているコンポーネントを使用することです。しかし、この方法は必ず適用できるとは限りません。その種のコンポーネントは特定用途向けのものであり、対象とする回路やシステムがその特定用途に一致するとは限らないからです。デバイスの適合性を認定する際には何らかの仮定が用いられます。その仮定が対象とするシステムには当てはまらなかったり、そもそも保護レベルが異なっていたりする可能性があります。

高い診断カバー率を達成するための方法はもう1つあります。それは、コンポーネントのレベルで冗長性を持たせることです。その場合、エラーの検出は直接的に行われるのではなく、同一になるはずの2つ（またはそれ以上）の出力を比較することによって間接的に行われます。ただし、この方法を採用するとシステムの消費電力が増加します。そして、恐らくそれよりも重要な問題は、システムの最終的なコストが増加してしまうことでしょう。

コンポーネントのレベルで、エラー検出能力と冗長性を高める

外部インターフェースにおけるデータ伝送は、エラーの一般的な発生源の1つです。伝送中にどれか1つのビットのデータが破損すると、受信側でデータが誤って解釈され、望ましくない状態が発生する可能性があります。データ伝送で発生する総エラー数を計算するには、BER（ビット誤り率）を使用します。BERは、ノイズや干渉（EMI）といった任意の物理的な要因によってデータが破損したビット数を表します。

$$[BER] = \frac{[\text{破損したビット数}]}{[\text{伝送したビット数}]}$$

BERはシステムにおいて実際に測定することができます。HDMI®など多くの規格ではBERの値が一般的に定義されていますが、推定値を使用することも可能です。現代のデータ・トラフィックでは、標準的にはBERの最小値は10^{-7}程度になります。この数値は、多くのアプリケーションにとっては悲観的な見積りだと言えるかもしれません。それでも参考値としては十分に使用できます。

BERが10^{-7}であるということは、1000万ビットごとに1ビットのデータが破損するということを意味します。SIL3のシステムでは、1時間当たりのエラーの発生確率を10^{-7}以下に抑えることが目標になります。図2のシステムにおいて、ADCとコントローラの間で32ビットのデータを1kSPS（キロサンプル/秒）の出力データレートで伝送する場合、1時間当たりの伝送ビット数は次のように求められます。

［1時間当たりのビット数］= 32 × 1000 × 3600 = 115,200,000［ビット］

この場合、エラー率は$1.5e^{-5}$まで増加します。しかも、これは1つのインターフェースにおけるエラー率です。伝送エラーは、許容される総エラーの0.1%～1%に抑える必要があります。

この場合、CRC（Cyclic Redundancy Check）のアルゴリズムを追加すればエラーを検出することができるようになります。検出可能な破損ビット数は、CRC多項式のハミング距離によって決まります。例えば、X^8+X^2+X+1というCRC多項式のハミング距離は4です。この場合、伝送フレームごとに最大3つの破損ビットを検出することができます。32ビットのデータに8ビットのCRCデータを付加して伝送する場合、CRCのハミング距離が4であれば、1時間当たりの伝送ビット数に対するエラーの発生確率は表2のようになります。

表2. CRCのハミング距離が4である場合のエラーの発生確率

1時間当たりのデータ・ビット数	1時間当たりの検出されないエラーの発生確率
144,000,000	$2e^{-14}$
432,000,000	$6e^{-14}$
2,160,000,000	$3e^{-13}$

CRCを用いた診断のレベルは、レジスタに書き込まれた値を再度読み出して、データが正しく伝送されたかどうかを確認することで高めることができます。その場合も、CRC多項式を用いたエラー検出のレベルは、BERに基づいて予想される破損ビット数を検出できるレベルにする必要があります。

故障確率を最小限に抑える方法

コンポーネントのメーカーが、「当社の製品は機能安全システム用に設計されている」とうたっているケースがあります。その場合、そのメーカーはFIT（Failure in Time：単位時間当たり平均故障発生数）だけでなく、FMEA（Failure Mode and Effect Analysis：故障モード影響解析）またはFMEDA（Failure Modes Effects and Diagnostics Analysis：故障モード影響診断解析）の結果を示す必要があります。これらのデータは、特定のアプリケーションにおいてICの解析を行うに当たり、システムの診断カバー率、安全側故障率（SFF：Safe Failure Fraction）、危険側故障率を計算するために使用されます。

FITは、デバイスの信頼性を表す指標です。ICのFITは、加速寿命試験に基づいて計算したり、IEC 62380、SN 29500といった規格に基づいて計算したりすることができます。その場合、FITは、アプリケーションにおける平均動作温度やパッケージの種類、トランジスタ数を考慮に入れて推定されます。FITには故障の根本原因に関する情報は一切含まれていません。そのため、デバイスの信頼性の推定だけに使用されます。一般に、直接的/間接的に各機能ブロックを確認しない限り、エラーの最終的な発生確率は、SIL2またはSIL3の安全機能に求められる水準を上回る結果になります。

FMEA/FMEDAの目的は、ICに集積された全てのブロックの解析結果、ブロックの故障による直接的/間接的な影響、故障の検出を可能にするさまざまなメカニズムや手法といった内容を網羅する包括的なドキュメントを作成することです。先述したとおり、このような解析は対象となるシグナル・チェーン/アプリケーションに基づいて行われます。ただ、ドキュメントは、別のシステム/アプリケーションに対するFMEA/FMEDA解析を簡単に実施できるくらい詳しく記述する必要があります。

ΣΔ ADCで発生し得る問題

ΣΔ ADCは内部構造が非常に複雑なデバイスです。このICに対する一般的な解析により、以下のような複数のエラーの発生源が存在することが明らかになっています。

- リファレンスの切断/破損
- 入出力バッファ/PGAの破損
- ADCのコア部の破損/飽和
- 内蔵レギュレータの異常
- 外部電源の異常

これらは、デバイスのブロックに故障を生じさせる恐れのある問題の一部です。他にも、以下のような発見しづらい故障の要因もあります。

- 内部ボンディングの破損
- 隣接するピンとのボンディングの短絡
- リーク電流の増加

例えば、V_{REF}のリーク電流が増加して、内部のリファレンス電圧が低下してしまっているとします。コンポーネントはそのことを検出できるでしょうか。このような種類の誤動作を検出するには、ADCにおいて、変換に使うリファレンスを複数の選択肢の中から選べるようにしておき、V_{REF}を入力信号とした場合の変換結果を確認するといった方法が必要になります。

また、内部のヒューズが再接続したり破損したりしていることは、どうすれば検出できるでしょうか。そうした故障が原因で、電源の投入時に誤った構成情報が読み込まれるといったことが起きる可能性があります。これらは、確率は非常に低いものの、発生すれば大きな問題につながる恐れのある状況の例です。あらゆる故障、特に非常にまれな故障が起きる可能性と、（存在するならば）その検出方法をFMEA/FMEDAのドキュメントとして明文化しておく必要があります。それらのドキュメントには、特定のアプリケーション/構成における故障と仮定についてまとめておきます。その目的は、故障の検出率を最大限に高め、検出されないエラーを最小限に抑えることです。

アナログ・デバイセズは、AD7770に加え、「AD7768」、「AD7764」といった最新のΣΔ ADCを提供しています。これらの製品は、デジタル/アナログの両方のブロックの機能的エラーを検出するために複数の診断機能を備えています。それにより、フォールト・トレランスな保護性能を向上しています。具体的には、以下のような機能ブロックを備えています。

- ヒューズ/レジスタ/インターフェース用のCRCチェッカー
- 過大過電圧/過小電圧の検出器
- リファレンスとLDO（低ドロップアウト）レギュレータ用の電圧検出器
- PGAのゲインをテストするための固定電圧発生器
- 外部クロックの検出器
- 複数のリファレンス電圧源

これらの回路に加えて、AD7770は診断機能を強化するために使用できる補助用のADCを搭載しています。分解能が12ビットのSAR（逐次比較）型ADCであり、例えば次のような目的に使用できます。

- 異なるレベルのEMI耐性が得られるといった具合に、何らかのメリットを提供する代替アーキテクチャの実装

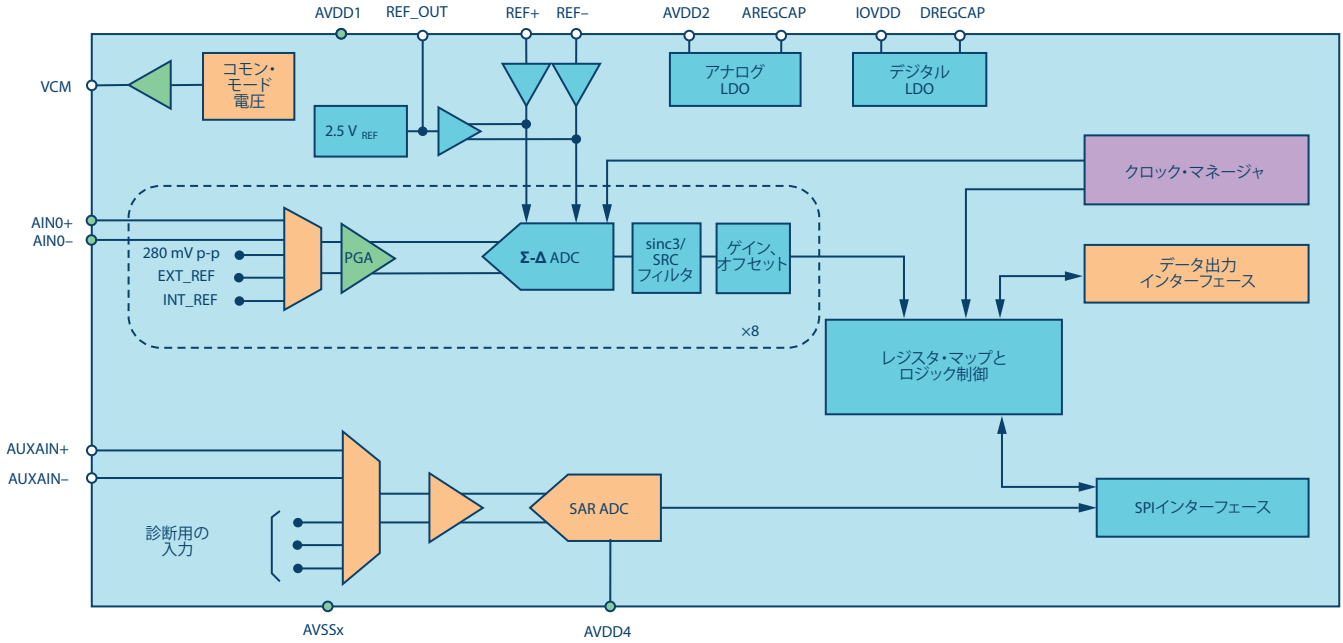

図3. AD7770の診断/監視用ブロック

- リファレンスとして使用可能な異なる電源ピンで動作する
- 十分に高速なので、8チャンネルのΣΔ ADCの監視が可能。1つのΣΔ ADCチャンネルの単一の変換に対し、精度の異なるモニターとして使用できる
- 異なるシリアル・インターフェース（SPI）を使用して、変換結果を出力できる
- 外部電源、V_{REF}、V_{CM}、LDOの出力電圧、内部の電圧リファレンスなど、あらゆる内部電圧ノードにアクセスして診断を行うことが可能

図3は、AD7770の内部ブロック図です。デバイス内部の監視用機能を含むブロックは紫色、アクティブな監視が可能なブロックは緑色、内部監視とアクティブ監視の両方の機能を搭載するブロックは青色で示しています。

まとめ

機能安全は、システム/ブロックに対する監視と診断のカバー率を高めることで、検出されないエラーの数学的な発生確率を低減しようというものです。カバー率は、冗長性を持たせれば容易に高めることができます。しかし、その方法にはいくつものデメリットがあります。特に問題なのは、システムのコストが増加することです。「AD7124」やAD7768など、アナログ・デバイセズの最新ΣΔ ADCは、内部のエラーを検出するための機能を数多く備えています。それらを利用することにより、機能安全システムの設計が簡素化されます。また、他のソリューションと比べて全体的な複雑さを抑えることが可能になります。AD7770は、そうした機能を盛り込んで設計された高精度ΣΔ ADCの良い例です。診断カバー率を最大限に高めるために補助的なADCを内蔵するなど、監視/診断用の機能が集積されています。それらの機能を利用することにより、極めて高い安全性を実現することができます。

著者：

Miguel Usach Merino（miguel.usach@analog.com）は、2008年にアナログ・デバイセズに入社しました。スペインのバレンシアでリニア/高精度技術グループのアプリケーション・エンジニアとして業務に携わっています。バレンシア大学で電子工学の学位を取得しています。

Miguel Usach Merino

この著者が執筆した他の技術文書

ADCの性能を引き出す容量性PGA

Analog Dialogue 50-08