ANALOG DEVICES
AHEAD OF WHAT'S POSSIBLE™

SIL 2準拠のICにより、SIL 3の機能安全を実現可能なアナログ出力モジュールを設計する

著者：Brian Condell、プロダクト・アプリケーション・エンジニア

概要

あるメーカーが、SIL（Safety Integrity Level）3に準拠したソリューションを必要としていたとします。そのメーカーは、SIL 2に対応するコンポーネントを使用して、そのようなソリューションを実現したいと考えました。この考え方に誤りがあるわけではありません。ただ、そのメーカーは実際にソリューションを開発する際、様々な課題に直面することになるでしょう。なぜなら、産業分野向けの機能安全規格であるIEC 61508のリビジョン3に準拠するために、新たな手法を採用しなければならなくなるからです。本稿では、SIL 3に準拠するために必要な課題の解決を図りつつ、製品を市場に投入するまでにかかる時間を短縮可能なソリューションを紹介します。

はじめに

ここ数年、機能安全に対応した産業用システムの数が著しく増加しています。その背景には、以下に挙げるような複数の要因があります。

- 多くのメーカーが、コストを削減するために複雑な新技術を採用したいと考えている。例えば、2つ目の接触器を追加する代わりにセーフ・トルク・オフ（STO：Safe Torque Off）を採用したいといったニーズが存在する
- 多くの工場が、ロボット（特に協働型のロボット）を導入することにより、製造フロアの生産性を高めることに成功している
- 安全性に関する認証を得た機器を採用すれば、信頼性が全般的に高まるという認識が広がっている
- 工場やプラントに診断システムを導入すれば、スループットが向上するということが理解されてきた
- 安全に関する新たな要件への対応が進んでいる

また、エネルギー、石油、ガスなどの業界では、新たな規制への準拠が求められるようになりました。それにより、非常に厳しい要件が課せられるようになったことも、機能安全の導入を後押しする要因の1つです。

以下では、本稿の内容を理解できるようにするために、いくつかの基本的な事柄について整理しておくことにします。

「安全」とは何か？

そもそも安全とは何でしょうか。これについては「許容できないレベルのリスクが生じないこと」と定義することができます。例えば、製造フロアに適切な保護機能が適用されていない回転機械が配備されている状態は、安全ではないと見なされます。

「安全機能」とは何か？

安全機能とは、「安全を実現する、または維持するために行う必要がある動作」のことです。安全機能は、システムに関連するリスクを低減することを目的として導入されます。例えば、安全機能を実現するための手段として、回転機械の前部にライト・カーテンが用意されていることがあります。その場合、手によって光が遮られたら、そのことが検出されます。その結果、手が機械に触れる前に回転機械が停止します。このような動作を実現するのが安全機能です。

一般に、安全機能は以下に示す3つのサブシステムによって実現されます。

- 値や状態を検出するために使用される入力サブシステム。例えば、レベル検出などを実現するセンサーがこれに相当する
- 危険な状態であるか否かを判定するロジック・サブシステム。例えば、PLC（Programmable Logic Controller）がこれに相当する
- 安全を維持するための措置を講じる出力サブシステム。例えば、アクチュエータがこれに相当する

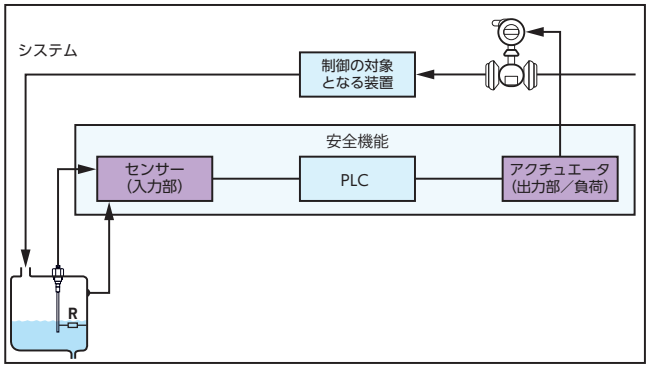

図1. 安全機能を実現する
システムの例

図1に示したのは安全機能を提供するシステムの構成例です。このシステムは、タンク内の液体のレベルを検知します。タンクが満杯になったら、危険を回避するために液流が停止されます。

「機能安全」とは何か？

上述したように、システムは何らかの安全機能を実行する必要があると判断したときに、その機能を実行することになります。機能安全は、その信頼性に関する概念です。つまり、その機能がどれくらいの信頼性で実行されるのかということを表します。先ほど、安全機能の例として回転機械に設置されたライト・カーテンを取り上げました。その安全機能は、光が遮られたときに停止処理を行います。機能安全については、それに関わる技術者が、その安全機能が適切に作動することをどの程度確信しているのかを表す指標だと言うことができます。

システムは、次のような要件を満たしている場合に機能安全に対応していると見なされます。すなわち、システムのハードウェア・メトリック（ランダム故障）、決定論的能力（SC：Systematic Capability）、共通原因故障（CCF：Common Cause Failure）に起因して、安全機能を提供するシステムの誤動作、人間の怪我や死亡、環境に対する悪影響、製造ロスが生じることがない場合です。

ここまで、安全に関する基本的な定義をいくつか示してきました。以下では、機能安全に対応したシステムを設計する際に準拠する必要のあるいくつかの規格を紹介します。また、それらの規格がもたらすメリットについて解説します。

機能安全向けの規格には、IEC 61508やISO 26262などがあります。そうした規格で定められた機能安全向けの開発プロセスに従うことで、メーカーは以下のような多くのメリットを享受することができます。

- 要件が事前により明確になる
- テストの時点で発覚するバグの数を減らせる
- コード（ソフトウェア）の記述の一貫性が高まる
- 統合の段階で発覚する欠陥の数が減少する
- より徹底的なテストを実施できる
- 現場で生じる欠陥の数が減少する
- 競合他社に対し、より明確な差別化が図れる

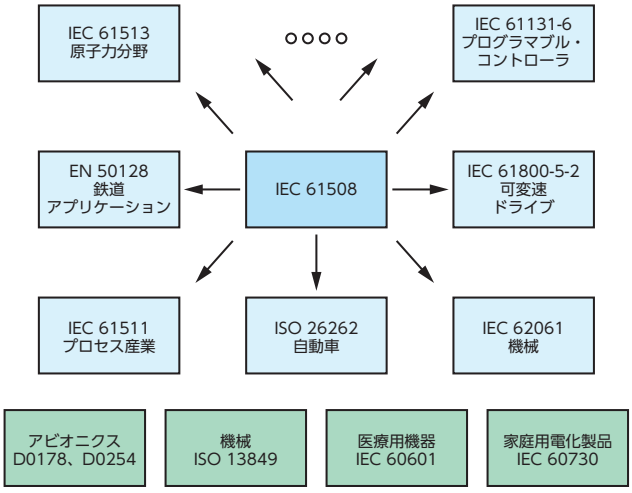

図2. 代表的な安全規格

図2に示すように、安全規格は数多く存在します。その大半は、産業分野向けの規格であるIEC 61508から派生したものです。実際、IEC 61508で規定された要件の90%～95%は、すべての規格に似たような形で盛り込まれています。

本稿では、産業分野向けの規格であるIEC 61508を取り上げます。特に冗長性（Identical Redundancy）を活用することにより、SIL 2に対応するICを使用してSIL 3に準拠するソリューションを実現する方法について詳しく説明します。

冗長性、高可用性、HFTの概要

どれだけ信頼性の高いシステムであってもいずれは故障します。一般に、故障はシステマティック故障（決定論的原因故障）とランダム故障の2つに分類されます（図3）。

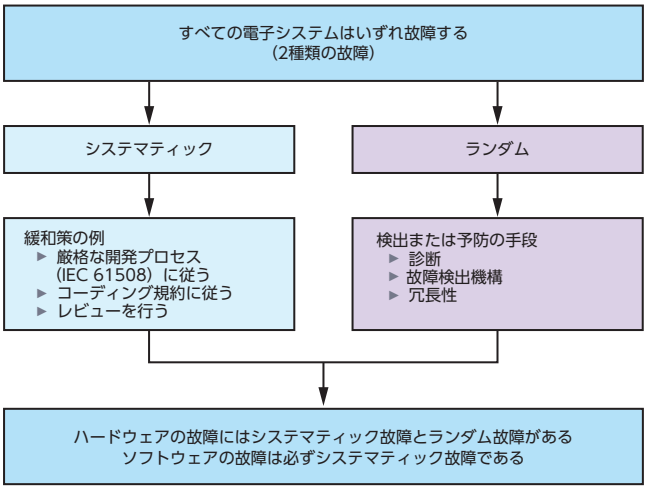

図3. システマティック故障と
ランダム故障

冗長性を持たせるというのは、簡単に言えば予備の（冗長な）パスを設けるという意味になります。その目的は、システムで故障が発生した際に、意図した安全機能を実行できるようにすることです。ただ、システムに何らかの冗長性が設けられているからといって、それだけで可用性が高くなるわけではありません。冗長パスが自動的に作動する（または有効化される）場合に限り、可用性は高まります。IEC 61508では、もう1つ一般的に使用される用語があります。それがハードウェア・フォールト・トレランス（HFT：Hardware Fault Tolerance）です。例えばHFTがNである場合、N＋1回の故障が発生した際、初めて安全機能が失われる可能性があるということを意味します。ここで、故障による影響を制御できる可能性のあるその他の措置（診断など）は考慮に入れてはならない点には注意が必要です。HFTは、故障に対するハードウェアの堅牢性を保証するための手段だと言えます。また、HFTと安全側故障比率（SFF：Safe failure fraction）はトレードオフが可能です（表1）。

表1. HFTとSFFの関係

要素のSFF	HFT		
	0	1	2
60%未満	不可	SIL 1	SIL 2
60%以上、90%未満	SIL 1	SIL 2	SIL 3
90%以上、99%未満	SIL 2	SIL 3	SIL 4
99%以上	SIL 3	SIL 4	SIL 4

SILは「安全度の水準」

SILは、安全機能の完全性と、リスクを低減するために提供される効果の相対的なレベルを表します。IEC 61508では、SILを4段階で定義しています。SIL 1は安全に対する完全性が最も低く、SIL 4が最も高いレベルに相当します。一方、ISO 26262では自動車の安全水準としてASIL（Automotive Safety Integrity Level）を定めています。表2は、SIL、ASIL、アビオニクス（航空電子機器）の安全水準の関係を示したものです。

SILが1から4に高くなるにつれ、許容される故障率（FIT：Failures in Time）は低下します。1 FITというのは、10億（1e9）時間にわたる稼働時間の中で1回だけ故障が生じるということを意味します。10億時間というのは約10万年に相当します。そのように長く稼働し続ける機器など存在しません。しかし、10万台の機器を1年間稼働させた場合、いずれかのハードウェアに1回のランダム故障が発生すると想定できます。この点には注意が必要です。SFFは、安全機能の全故障に占める安全側故障と、検出される危険側故障の割合を表します（以下参照）。

$$SFF = \frac{(\lambda_{DD} + \lambda_S) \times 100}{(\lambda_{DD} + \lambda_{DU} + \lambda_S)} \quad (1)$$

- λ_{DD} = *Dangerous Detected Faults*
- λ_{DU} = *Dangerous Undetected Faults*
- λ_S = *Safe Faults*

ここで、各変数の意味は以下のとおりです。

- λ_{DD}：検出される危険側故障
- λ_{DU}：検出されない危険側故障
- λ_S：安全側故障

表2. 様々な安全度の水準

IEC 61508	ISO 26262	アビオニクス
SIL 1	ASIL A	D
SIL 2	ASIL B	C
SIL 3	ASIL C/D	B
SIL 4		A

表3. SILとSFFの関係

SIL	SFF	高頻度の作動要求に対する1時間あたりの危険側故障	理論的に許容される危険側故障
1	60%	$1e^{-5}$（10,000 FIT）	10年に1回の危険側故障
2	90%	$1e^{-6}$（1,000 FIT）	100年に1回の危険側故障
3	99%	$1e^{-7}$（100 FIT）	1000年に1回の危険側故障

表3は、HFTがゼロの場合のSFFとSILの関係についてまとめたものです。

既存のソリューションが抱える課題

設計に機能安全を適用する際には、いくつかの課題に直面します。1つは、認証を取得するための作業が難しく、コストも増える可能性があるというものです。ただ、機能安全の規格に準拠しないというのは、非常に深刻なリスクを抱えるということを意味します。設計で使用するICについては、特に注意を払わなければなりません。システム・レベルのFMEDA（Failure Modes Effects and Diagnostics Analysis：故障モード影響診断解析）を行い、ASICを以下の項目が不明なブラック・ボックスとして扱う必要があります。

- トランジスタの数
- 内部故障のメカニズム
- ブロックのレイアウトのサイズ
- ICの信頼性

その結果、SILの全般的な目標を達成するために、技術者はFITの計算を過度に保守的に行うことになるでしょう。また、安全システムで使用するその他の部品についても過度に安全側に振った選択を行うことになるはずです。そして、一般的には外付けのA/Dコンバータ（ADC）などを用いた外部診断機能を利用することになるという結果を招きます。そうすると、以下のような問題が生じます。

- コストが高くなる（部品点数が増加する）
- 実装面積が大きくなる
- 複雑さが増す
- システムにおいてソフトウェアのオーバーヘッドが増加する
- 開発時間が長くなる

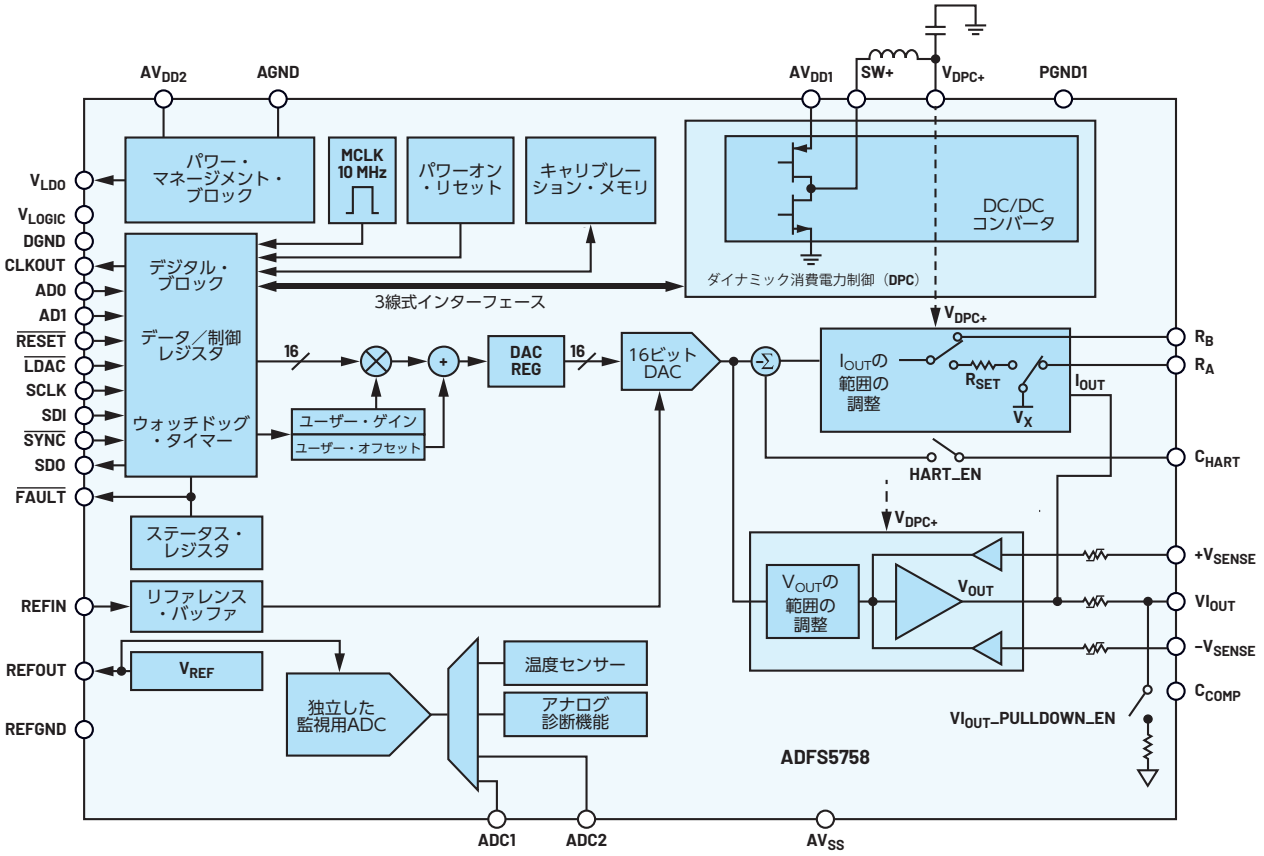

図4. ADFS5758のブロック図

また、これらの問題を更に増大させる要因が浮上しています。それは、IEC 61508の新版であるリビジョン3の存在です。

IEC 61508のリビジョン3

IEC 61508のリビジョン3ではいくつかの変更が計画されています。例えば、IEC 61508に準拠していないICが、オンチップの診断機能を使用して、そのIC上の故障を検出することに関しては、明示的な警告が盛り込まれる見込みです。また、自動車向けの規格であるISO 26262のLFM（Latent Fault Metric：潜在的な故障検出率）にも、似たような要件が導入されることが計画されています。診断機能に対するSFFのようなものに加えて、診断用の回路に対してSCの要件も課される予定です。

世界で初めて機能安全の認証を取得したD/Aコンバータ

「ADFS5758」は、分解能が16ビットの電流出力型D/Aコンバータ（DAC）です。シングルチャンネルの製品であり、ダイナミック消費電力制御（DPC：Dynamic Power Control）機能や内部リファレンスに加えて、数多くの診断機能を内蔵しています（図4）。

ADFS5758が備える診断機能や安全対策機能には以下のようなものがあります。

- メインの診断機能はADCを使用することによって実現します。先述したとおり、IEC 61508のリビジョン3では、IEC 61508に準拠していないICにおいて、オンチップの診断機能を使用してそのICの故障検出を行うことは一般的に許容されないと明記される予定です。
- 読み出しアドレス／書き込みアドレスが有効であることの確認
- ECC（Error-Correcting Code）による訂正
- ウォッチドッグ・タイマー
- 構成用のレジスタをロックする機能
- 内部バイアス電圧の監視機能
- 温度の監視機能

また、ADFS5758は以下のようなアプリケーションの要件に対応するように設計されています。

- 産業用のファクトリ・オートメーション（FA）
- プロセス制御のアプリケーション
- フォーム・ファクタが小さい高密度のPLC用のアナログI/Oカード

加えて、安全機能としては、入力されたデジタル・コードを受け取り、フルスケール・レンジ（FSR）の±2.5%の範囲内の出力電流を生成するように設計されています。

更に、同DACはIEC 61508に準拠するように設計されています。そのレベルについては以下のとおりです。

- ハードウェア・メトリックについては SIL 2 に準拠
- システマティックな要件については SIL 3 に準拠

ADFS5758は、その機能安全について、TÜV Rheinland（ドイツの認証企業）からの認証を得ています（図5）。

図6に示したのは、ADFS5758の使用例です。同ICを適用することで、安全機能を提供する一般的なアプリケーションを実現しています。

SILの要件を満たすシステムを実現するには、ハードウェア・メトリックとSCの両方についてSILの目標を達成する必要があります。なお、ハードウェア・メトリックは構造的制約（AC：Architectural Constraints）とも呼ばれます。

Certificate

TÜVRheinland CERTIFIED
Functional Safety
www.tuv.com
ID 0600000000

No.: 968/FSP 2055.00/20

Product tested	16-bit Current Output DAC with Dynamic Power Control	**Certificate holder**	Analog Devices International Raheen Business Park Raheen Limerick Ireland
Type designation	see latest "Revision List"		
Codes and standards	IEC 61508 parts 1-2:2010		
Intended application	The 16-bit Current Output DAC with Dynamic Power Control is a compliant item and complies with the requirements of SC 3 according to IEC 61508-2. The implemented diagnostics are suitable to achieve a hardware integrity up to SIL 2 / HFT=0 and thus can be used in safety-related applications up to SIL 2 according to IEC 61508.		
Specific requirements	The instructions in the safety manual shall be considered.		

Valid until 2025-06-24

The issue of this certificate is based upon an examination, whose results are documented in Report No. 968/FSP 2055.00/20 dated 2020-06-24.
This certificate is valid only for products which are identical with the product tested.

TÜV Rheinland Industrie Service GmbH
Bereich Automation
Funktionale Sicherheit
Am Grauen Stein, 51105 Köln

Köln, 2020-06-24
Certification Body Safety & Security for Automation & Grid
Dipl.-Ing. Gebhard Bouwer

www.fs-products.com
www.tuv.com

TÜVRheinland®
Precisely Right.

図5. ADFS5758の
機能安全に関する認証書

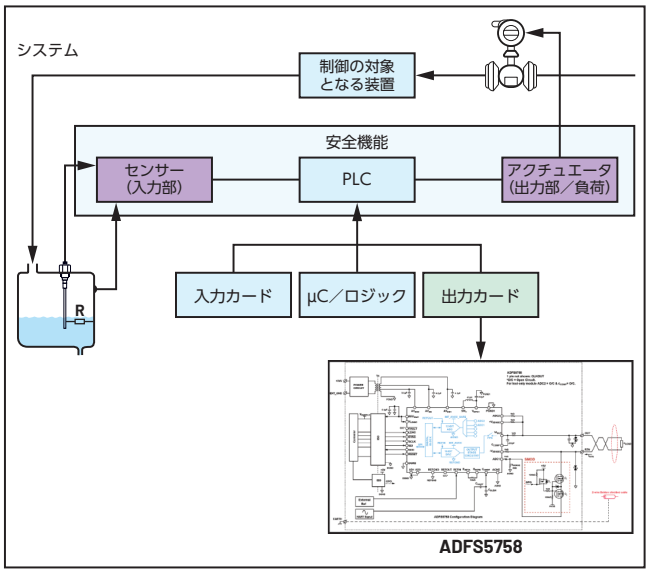

図6. ADFS5758を適用した
一般的なアプリケーション

ACに関する対応

ハードウェア・メトリックについては、SIL 2に準拠する2つの要素（同一の要素または異なる要素）を並列に配置することでSIL 3のレベルを達成することが可能です（図7）。

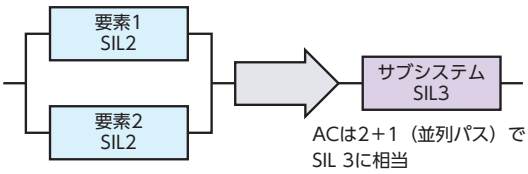

図7. ACに関する対応。
SIL 2に準拠する2つの要素を使用することで、
SIL 3対応のソリューションを実現できます。

SCに関する対応

冗長性は、異なる要素を使用することでも実現できますし、同一の要素を使用することでも実現可能です。

同一の要素

SCが等しい同一の要素を複数使用しても、全般的なSCは高くなりません。なぜなら、CCFが発生した場合などには、両方の要素に同等の温度スパイクや電圧降下が生じる傾向があるからです。つまり、1つの故障によって両方の要素が機能不全に陥る可能性が高いということです（図8）。

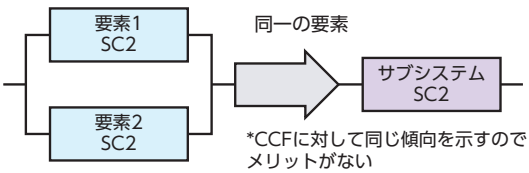

図8. 同一の要素を使用した例。
この構成ではSCは高くなりません。

異なる要素

異なる要素を使用して冗長構成を実現すれば、システムの能力は全般的に高くなります（図9）。なぜなら、2つの要素が異なるものであることから、1つの故障によって両方の要素が同時に機能不全に陥る可能性が低くなるからです。

ただ、この方法にも問題はあります。安全システムにおいて異なる要素を使用すると、デザイン・インとテストの作業負荷が大幅に増加します。結果として、コストが増大する可能性があるのです。

従って、理想的な解決策は、同じ要素を2つ使用しつつ、機能安全の要件に対するSCとランダム故障／ハードウェア・メトリックの両方を満たすというものになります。

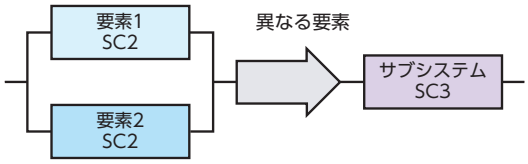

図9. 異なる要素を使用した例。
この構成であればSCは高くなります。

SILより1つ上のレベルになるようにSCを実現する

ここでは、SCがSILよりも1つ上のレベルになるように設計された要素をシステムで採用するケースを考えます。その場合、同一の要素を2つ使用することで、安全システムに冗長性を持たせることができます。同時に、全般的なSCを高めることが可能になります。図10に示したのはその一例です。

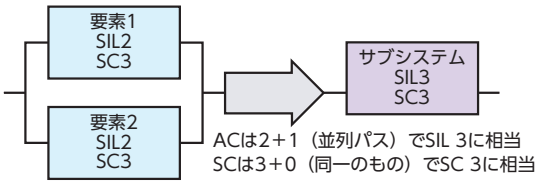

図10. 冗長性を利用して
SIL 3を実現した例

ADFS5758は、SCがハードウェア・メトリックよりも1つ上のレベルになるように設計されています。そのため、ハードウェア・メトリック（つまりランダム故障）についてはSIL 2の認証しか取得していません。しかし、これを使うことでも、SIL 3に対応するアナログ出力モジュールを設計することが可能だということです。

まとめ

ADFS5758は、機能安全に関する認証を取得した製品です。これを安全システムで使用すれば、以下のような様々なメリットを得ることができます。

- TÜV が認定しているとおり、リスクを低減できる
- オンチップの診断機能を使用できる（ADC と分散型の診断機能）
- （内蔵 ADC を使用できるので）ソリューションのサイズを小さく抑えたり、与えられたスペースにおいてチャンネル数を増やしたりすることができる
- 外付けコンポーネントの数を最小限に抑えられる（信頼性の向上につながる）
- ターゲットを絞った診断が可能になる（検出時間を短縮しつつ、カバレッジを高められる）
- システムを担当する技術者に対して、重要な数値情報が提供される（FMEDA）
- システムにおいてソフトウェアのオーバーヘッドを低減できる（ソフトウェア・ベースの診断機能を削減できる）
- 想定している環境に対する信頼性の解析が可能になる
- 顧客の開発時間を短縮できる
- 関連ドキュメントが提供される（安全マニュアルや TÜV による評価レポート）
- IEC 61508 のリビジョン 3 への準拠という将来的な保証が得られる

ADFS5758を採用すれば、他にも重要なメリットを得ることができます。それは、SIL 2に準拠するICを使用することにより、冗長性を基盤とするSIL 3対応のソリューションを設計できるというものです。

機能安全やADFS5758について更に詳しく知りたい方は、以下のような方法をご検討ください。

- ADFS5758 の製品ページを参照する
- ADFS5758 の評価用キットを発注し、同 IC に対する理解を深める
- アナログ・デバイセズの産業用機能安全ソリューションのページを参照する
- 安全について論じたアナログ・デバイセズのブログ記事を参照する

著者について

Brian Condellは、アナログ・デバイセズのプロダクト・アプリケーション・エンジニアです。産業用コネクティビティ／制御グループ（アイルランド リムリック）でIO-Link®を担当しています。入社は1997年で、25年以上にわたり半導体業界で業務に従事。FABの保守や、ICのレイアウト設計、アナログ設計、機能安全に関する設計、更にはアプリケーション設計などに携わってきました。IEC 61508に準拠するハードウェア／ソフトウェアの設計に関して、TÜV Rheinlandから機能安全エンジニア（FSE：Functional Safety Engineer）の認定を受けています。2003年にリムリック大学で電気工学の優等学位を取得しました。

EngineerZone®
オンライン・サポート・コミュニティ

アナログ・デバイセズのオンライン・サポート・コミュニティに参加すれば、各種の分野を専門とする技術者との連携を図ることができます。難易度の高い設計上の問題について問い合わせを行ったり、FAQを参照したり、ディスカッションに参加したりすることが可能です。

ADI EngineerZone™
SUPPORT COMMUNITY

Visit *ez.analog.com*

*英語版技術記事はこちらよりご覧いただけます。

ANALOG DEVICES
AHEAD OF WHAT'S POSSIBLE™

アナログ・デバイセズ株式会社

VISIT ANALOG.COM/JP

お住いの地域の本社、販売代理店などの情報は、analog.com/jp/contact をご覧ください。

オンラインサポートコミュニティEngineerZoneでは、アナログ・デバイセズのエキスパートへの質問、FAQの閲覧ができます。

TA24579-9/23