機能安全はインダストリ4.0に何をもたらすのか？

著者: Tom Meany
Analog Devices, Inc.

概要

インダストリ4.0は、将来の工場に新しいビジョンをもたらします。そして、そうした工場においては、安全（safety）が非常に重要な要素になります。安全について語る際には、機能安全という概念について把握しておかなければなりません。機能安全とは、各種の機器が必要に応じて高い信頼性で自身の安全機能を実行できるようにするための仕組みのことです。他の安全とは異なり、機能安全では能動的に安全を確保します。そして、機能安全の実現にはICが不可欠な要素となります。ICはインダストリ4.0の実現に向けても必須の要素だということです。本稿では、機能安全がインダストリ4.0にもたらす影響について説明します。特に、ネットワーク、セキュリティ（security）、ロボット／コボット、ソフトウェアや、それらに関連する機能を実現するために使用されるICについて詳しく解説します。機能安全を実現するためのICについては、それに向けた要件が存在します。本稿では、そうした要件に注目することにします。

はじめに

上述したとおり、機能安全とは、各種の機器が必要に応じて高い信頼性で自身の安全機能を実行するための仕組みのことです。例えば、ガード・ドアを開けたオペレータに危害が及ばないようにモータを素早く停止させたり、人間が近くにいる場合にはロボットの動作速度や出力を落としたりといったことが行われます。

一方、インダストリ4.0とは次世代の製造工場の在り方を表す概念です。インダストリ4.0を導入すれば、工場における柔軟性の向上とコストの削減が約束されると言われています。

本稿では、機能安全がインダストリ4.0にもたらす影響について考察します。

機能安全

まずは、機能安全について詳しく見ていくことにしましょう。

A. 様々な規格

機能安全の基本になる規格は、IEC 61508[1]です。この規格の初版は1998年に発行され、2010年には改定版である第2版が発行されました。現在は、2020年の第3版の発行に向けて更新作業が行われています。1998年に初版が発行されて以来、基本規格であるIEC 61508を基にして、各種の分野に適合させるための変更が加えた規格がいくつも策定されました。代表的なものとしては、自動車向けのISO 26262[2]、プロセス制御向けのIEC 61511[3]、PLC（プログラマブル・ロジック・コントローラ）向けのIEC 61131-6[4]、機械類向けのIEC 62061[5]、可変速駆動システム向けのIEC 61800-5-2[6]などがあります（図1）。IEC 61508の内容は非常に広範にわたります。各派生規格はより限定された分野向けになっているので、IEC 61508の内容を理解する上でも役に立ちます。

IEC 61508から派生したものではありませんが、ISO 13849[7]も重要な規格です。これは、欧州のEN 954規格（廃止済み）から派生したものであり、機械類を対象にしています。

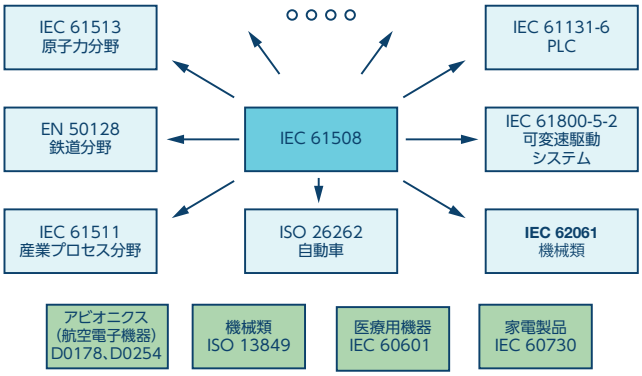

図1. 代表的な機能安全規格

機能安全においてより基本的な概念になるのは、安全機能です。安全機能とは、安全を達成／維持するために実行しなければならない動作のことです。標準的な安全機能は、入力サブシステム、論理サブシステム、出力サブシステムから成ります。一般的には、安全ではない潜在的な状態が検知されると、検知した値を基に何らかの機構による判断が行われます。危険の可能性があると判断された場合には、あらかじめ定義された安全な状態にシステムを移行するよう出力サブシステムに指示が出されます。

安全ではない状態から安全な状態を達成するまでにかかる時間は重要です。代表的な安全機能は、次のような要素によって構成されます。すなわち、機械に取り付けられているガードが開いていることを検出するセンサー、データを処理するPLC、機械に入れられた手が作動部に到達する前にモータを停止する安全トルク・オフ入力を備える可変速駆動システムで構成されるといった具合です。これらを組み合わせて安全機能が実現されます。

B. SILという指標

SILとは、Safety Integrity Levelの頭文字をとったものであり、安全度水準と訳されます。SILは、許容可能なレベルまでリスクを抑えるために必要なリスクの低減の度合いを表します。IEC 61508では、SILを1～4の4段階に分けています。1段階上がるごとに安全性の要件は厳しくなります。SIL 4は、危険にさらされる人数が1人までにとどまる機械類や工場のオートメーション・システムには適用されません。数百人から数千人規模の被害が生じ得る原子力、鉄道などの分野に適用されます。機能安全の規格は他にも存在します。例えば、自動車にはASIL（Automotive Safety Integrity Levels）のA～DとISO 13849が適用されます。そのパフォーマンス・レベル A～Eは、SIL 1～SIL 3に対応づけることができます。

C. 故障の原因

一般に、機能安全の規格は、ランダム・ハードウェア故障、決定論的原因故障の2つを対象とします。その上で、それぞれに対処する方法を提案しています。

ランダム・ハードウェア故障は、その名が示すとおり、機器の予期しないランダムな故障に起因して発生します。これは、故障としては最も理解しやすいものでしょう。ランダム・ハードウェア故障の生じる確率は、システムのPFH（1時間あたりの危険側故障率：Probability of Failure on Demand per Hour）で表されます。許容されるPFHの値は、達成すべきSILに応じて異なります。その範囲は、SIL 1の10^{-5}/時からSIL 3の最小値である10^{-7}/時までです。

もう一方の決定論的原因故障（システマティック故障）とは、設計に内在している故障のことです。これは、設計を変更することによってしか修正することができません。例えば、EMC（電磁両立性）に対する耐性の不足は、決定論的原因によるエラー（故障）だと考えられます。要件の不備、検証と妥当性確認の不足、あらゆるソフトウェア・エラーも、決定論的原因故障に含まれます。同故障の原因は、個々のユニットが内在するのではなく、生産されるすべてのアイテムに内在する事実上の弱点です。条件がそろえば、この故障は100%の確率で発生します。

いずれにせよ、設計者は求められるSILに対応する安全機能を実現しなければなりません。そのような状況下で使用するのに適した機能を実現するには、SILの規格で指定されているランダム・ハードウェア故障と決定論的原因故障の両方に関する要件を満たす必要があります。つまり、ハードウェアの要件に適合しているだけでは不十分だということです。

D. ランダム・ハードウェア故障への対処

機器の信頼性がどれだけ高くても、ある時間内に故障が発生する可能性はゼロではありません。ランダム・ハードウェア故障に対処するためには、診断カバレッジの要件や冗長性の使用といった事柄を活用できます。安全機能については、SILに応じて最小のPFHまたはPFD（Probability of Failure on Demand：作動要求あたりの機能失敗確率）が定められています。また、SILに応じて、最低限必要なSFF（Safe Failure Fraction：安全側故障割合）も定められています。SFFは、SIL 1からSIL 3までの範囲で60%から99%までの値を取ります（レベルが高いほどSFFの値も高くなります）。この規格により、診断とシステムの冗長性の間のトレードオフが可能になります。その以外に、ディレーティングやより品質の高い部品の採用といった手法も有効です。

E. 決定論的原因故障への対処

決定論的原因故障は、ランダム・ハードウェア故障とは無関係に生じます。先述したように、決定論的原因故障を回避するためには、設計変更が必要になる可能性があります。

決定論的原因故障への対処策は、厳格な開発プロセスに従うことです。特に、様々な作業の成果物について第三者によるレビューを実施することが重要になります。多くの場合、そうした開発プロセスは複雑さの異なるVモデルで表現されます（図2）。レビューに必要とされる厳格さと、レビューの担当者に求められる独立性は、SILが高いほど厳しくなります。

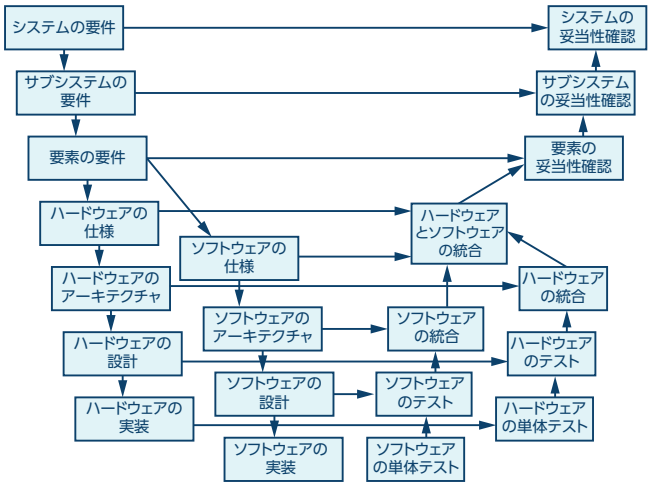

図2. システム・レベルの設計におけるVモデル

決定論的原因故障については、多様な冗長性を用いることで対処できるケースがあります。各システムで同時に同じような故障が起きる可能性が下がるからです。なお、ランダム・ハードウェア故障に対処するために使われる診断機能は、決定論的原因故障の検出に役立つこともあります。

上述した作業の多くは、システム・エンジニアリングやエンジニアリングに関する優れたプラクティスを必要とします。それらには、「State of the Art（最先端）」という言葉が付加されるケースもあります。加えて、ドキュメント化の作業も不可欠です。機能安全を達成できることを証明できる状態にしておくことは、実際に機能安全を達成するのと同じくらい重要です。

インダストリ4.0

インダストリ4.0[8]は、Industrie 4.0、IIoT（Industrial IoT）、中国製造2025、インダストリ・プラス、スマート・ファクトリといった名前でも知られています。「4.0」というのは、第4次産業革命という意味を表しています。つまり、オートメーションを活用した電子機器の製造やITの普及が始まった1970年ごろからの第3次産業革命に続くものだという意味です。

IIoTは、各種の記事、学会、マーケティング活動などでよく取り上げられるテーマです。ただ、IIoTの広範な普及に向けては、まだキラー・アプリケーションが不足しています。キラー・アプリケーションになり得るものとしては、障害の予知や適応型の診断、状態基準保全（Conditional Based Maintenance）などが挙げられます。

インダストリ4.0の中心となる概念は、サイバーフィジカル・システム（CPS：Cyber-physical System）です。CPSは、「情報の交換、動作の開始、独立した相互制御を自律的に行うことができるスマート・マシン／ストレージ・システム／生産設備」[9]で構成されます。言い換えると、あらゆるものがインテリジェント化され、計測／制御のための機器を備え、相互接続されている状態が求められるということです。この定義は、とりわけネットワークやセキュリティなどの懸念事項において重要な意味を持ちます。

インダストリ4.0に関連する設計では、以下のような主要な原則を実現することが求められます。

- 相互運用性：すべてのものがつながっている
- 仮想化：プラントとシミュレーションのモデルを利用可能
- 分散化：ローカルのインテリジェンス化
- リアルタイム性：リアルタイムに実世界に対応できる
- サービス指向：インターネット経由でサービスを利用できる
- モジュール性：必要に応じた再構成が可能

センサー・フュージョンとデータの分析を活用すれば、新たな知見を得ることができます。例えば、スマート機器から収集した診断結果とクラウドでの分析を活用することにより、予防保全を実現するといった具合です。また、システム間で老朽化の度合いを比較することで、冗長化されたアイテムを切り替えて生産性を向上させることも可能になります。このように、機械の状態は重要な関心事になるはずです。

A. ネットワーク

旧来のシステムでは、専用のネットワークを用いて孤立したオートメーションを実現する傾向がありました。4～20mAの電流ループをベースとしたアナログ・ネットワークは、現在でも広く使われています。この手法には、EMC性能が高い、最大3kmの伝送距離を実現できるといった多くの長所があります。加えて、本質的に安全であり、同期も確立されます。しかし、インダストリ4.0での利用を考えると柔軟性に欠けます。また、速度も十分ではありません。

インダストリ4.0では、あらゆるものがつながっていて、あらゆるものと通信できる状態にすることを標榜しています。この状況を表すものとして、M2M（Machine to Machine）やP2M（Process to Machine）といった用語がよく使われています。そのような接続を利用すれば、以下のようなことを実現できます。

- 製造効率の向上
- 製造に関する柔軟性の向上
- 運用に関する知識の向上
- 製造コストの削減

イーサネットをベースとする接続ソリューションは、上述した要件への対応に適したものです。但し、ネットワークの安全とセキュリティに関する要件にも対処しなければなりません。効率化が新たなレベルに到達すれば、新たなサービスがより高い費用対効果で提供されるようになるでしょう。

B. セキュリティ

デジタル・ネットワークを利用するということは、セキュリティの問題に直面するということを意味します。映画（「Zero Days」など）やメディアで取り上げられた最近の事例を見ると、StuxnetやBlackEnergyといったウイルスの問題が発生していたことがわかります。ネットワークがクラウドに接続される場合、1つのクラウド・プロバイダをハッキングするだけで、多くの工場がダウンしてしまう可能性があります。以前であれば、一度に1つの工場がハッキングされることしかなかったので、大きな変化が生じたことになります。ハッカー（クラッカ）にとって、クラウドはスケール・メリットが得られる魅力的な獲物になり得るということです。実際、IoTというのは「Internet of Threats（脅威のインターネット）」の略だと主張する専門家も存在します。

一般に、ITに関するセキュリティの要件を産業用ネットワークに適用するのは容易ではありません。ITの分野では、セキュリティを確保するために、ソフトウェアの頻繁な更新など、製造には適さないいくつかの手法が使われているからです。ソフトウェアを変更すると、意図しない形で製造が停止してしまうといったリスクが存在します。そのため、製造業の分野ではソフトウェアの変更は好まれません。安全が関係する場合、機能安全に対応するシステムの認証コストがかさむと共に、変更管理のプロセスが必要になります。結果として、ソフトウェアの変更に対する嫌悪感は更に高まります。

産業分野で行われる制御に関するセキュリティの要件を対象としていて、国際的にコンセンサスを得ている規格はIEC 62443[10]です。同規格は、IACS（Industrial Automation and Control System）の設計、実装、管理を対象としています。

C. ロボットとコボット

かつて、ロボットは檻の中に設置される大きくて恐ろしい機械でした。一方、コボット（Collaborative Robot）は人を傷つけることがないよう配慮されたものであり、それほど怖くはありません。コボットは、センサーとソフトウェアの融合によって実現されるものであり、作業者から隔離する必要はありません。産業環境で利用されるコボットは、1本のアームまたは1対のアームで構成されています。代表的なものとしては、Universal Robotsの「UR5シリーズ」やABBの「YuMi®」があります。将来の工場において、コボットはオペレータを支援する存在になります。また、一緒に作業をしている人が右利きなのか左利きなのかといったことも認識するようになるはずです。

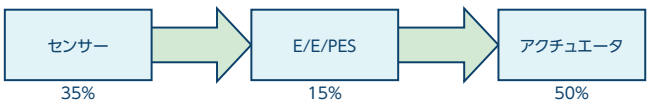

図3. 代表的な安全システムにおける
エラーのバジェット

無人搬送車（AGV：Automated Guided Vehicle）は、移動型のロボットに分類できます。また、特別な種類のコボットだと捉えることもできるでしょう。AGVは、製造現場で製品や材料を運搬する際に役立ちます。実際、インダストリ4.0においては不可欠な要素だと考えられています。

ただ、動的な機械が環境内に存在するということは、新たな危険が潜在的に存在するということを意味します。したがって、それらへの対処策を考えなければなりません。コボットやAGVの設計には、2つの選択肢があります。1つは、重大な危害につながる可能性がないレベルまで十分に力を弱くするというものです。それにより、本質的に安全なシステムとして完成させることができます。もう1つは、関連する機能安全の規格に基づいたソリューションを設計するというものです。AGVについて言えば、ビジョン、レーダー、レーザの各システム、あるいは床に埋め込まれた軌道を用意することによって衝突を防止することができます。

機能安全とネットワーク

通常、機能安全を実現するためのシステムは、センサー、ロジック、出力といったサブシステムで構成されています。これら3つの要素を組み合わせることで安全機能を実装するということです。SIL、PFH、SFF、HFT（Hardware Fault Tolerance：ハードウェア障害許容度）に対する要件の対象になるのは、安全機能全体です。そうした要件が満たされているということは、それらサブシステムの間の通信も安全な状態で維持されているということになります。IEC 61508では、フィールドバス規格であるIEC 61784-3を参照して機能安全の要件を定義しています。具体的な要件として、ランダム・ハードウェア故障と決定論的原因故障の原因に対処することも求められています。

ここで図3をご覧ください。これは、1時間あたりに許容できる最大の機能失敗確率の割り当てとして、一般に受け入れられているエラー・バジェットを示したものです。多くの場合、このモデルの改良版では、各インターフェースに1%のバジェットが割り当てられます。安全機能がSIL　3である場合、最大許容PFHは10^{-7}/時なので、インターフェースに対する1%の配分は10^{-9}/時となります。

表1は、通信について考慮する必要がある潜在的な危険についてまとめたものだと言えます。これは、IEC　61784、EN　50159、IEC 62280[11]などの規格に記載されています。

表1の各行については、少なくとも1つの防御手段によって対処しなければなりません。防御手段については、IEC　61784-3[9]、IEC　62280-1/EN　50159[12]に詳細に記載されています。例えば、破損については、予想されるBER（Bit　Error　Rate：ビット誤り率）、SILの要件、1時間あたりの送信ビット数に応じ、ハミング距離をベースとするCRC（Cyclic Redundancy Check：巡回冗長検査）を使用することで対処することが可能です。

産業環境では、安全に関連するデータとそうでないデータを同じネットワーク上で通信できれば非常に便利であるはずです。これを実現するために、上記の要件は更に複雑になります。

IEC 61508-2:2010には、次の2つのオプションが用意されています。1つは、ホワイト・チャンネル・アプローチと呼ばれるものです。この手法では、通信チャンネル全体をIEC 61508に準拠する形で開発します。もう1つは、ブラック・チャンネル・アプローチと呼ばれるものです。この手法においては、通信チャンネルの性能についていかなる仮定も行わず、各安全機器の特別なレイヤによって安全を確保します。この安全レイヤによる防御手段によって、表1に示した一連の脅威に対処するということです。それらの防御手段は、基盤であるフィールドバスの規格が備えるあらゆる防御手段に追加されます。例えば、基盤である通信プロトコルで定義されたCRCに加え、ビットの破損を検出するために別のCRCを追加するといった具合です。ブラック・チャンネル・アプローチは、広く使用されています。その一例がPROFIsafeです。これは、PROFIBUS®またはPROFINET®の最上位に位置する安全レイヤです。

機能安全とセキュリティ

多くの言語（自然言語）は、security（セキュリティ）とsafety（安全）の2つを区別していません。それぞれに相当する2つの単語が存在するわけではなく、英語のsecurityとsafetyに相当する概念が1つの単語で表現されます。しかし、産業分野ではこれらはそれぞれに異なる概念を表します。両者は、時に矛盾をはらむ概念でもあります。安全の1つの定義は、意図しない行動による危害を防ぐというものになります。それに対し、セキュリティの定義は意図的な行動による危害を防ぐというものです。安全とセキュリティには共通点があります。それは、アーキテクチャのレベルで対処を図らなければならないというものです。それを怠ると、非常に困った状況に陥る可能性があります。後になって対処策を追加するというのは非常に困難だからです。ただ、両者には矛盾した部分があります。というのは、予期せぬ事象に対して安全を確保するための一般的な対応はシステムをシャット・ダウンすることだからです。ただ、そのシャット・ダウン機能はハッカーが利用できるものでもあります。つまり、DoS（Denial of Service）攻撃を通じてその機能を働かせることが可能だということです。そして、セキュリティとは、そうした機能からシステムを保護するためのものなのです。通常、セキュリティを確保するための機能には、認証用のパスワードが使われます。ただ、パスワードの入力中に、安全を確保するための機能の反応を遅くしたいと考える人はいるでしょうか。あるいは、安全な人物だということはわかっているのに、その人がパスワードを3回間違えて入力したら積極的に拒絶したいと考える人はいないはずです。

2010年に発行されたIEC　61508の第2版には、セキュリティに関する要件はほとんど含まれていません。ただ、セキュリティは考慮しなければならないと明言されており、ガイダンスとして未リリースのIEC 62443シリーズを参照しています。また、機械や原子力の分野の機能安全とセキュリティの関係を取り扱うための規格も策定されつつあります。

表1. ネットワークにおける脅威、防御手段

脅威	防御手段							
	シーケンス番号	タイム・スタンプ	タイム・アウト	送信元と送信先の識別子	フィードバックするメッセージ	識別手順	安全コード	暗号化技術
反復								
喪失								
挿入								
シーケンスの修正								
破損								
遅延								
偽装								

IEC 61508のSILと同様のものとして、IEC 62443ではSL（Security Level）を定義しています。そのレベルとしては1～4が用意されています。SL 1を満たすシステムは、偶発的な第三者に対してセキュアです。それに対し、SL 4を満たすシステムは、国家の支援を受けた集団によるハッキングの試みに対してもセキュアな状態が維持されます。なお、SILとSLの間には直接的な対応関係はありません。

IEC 62443では、IEC 62443-4-2において7つの基本的な要件（FR：Fundamental Requirement）を定義しています。それにより、所定のSLを達成するために必要な各FRに関するガイダンスを提供しています。7つのFRとは以下のようなものです。

- 識別と認証制御（IAC：Identification and Authentication Control）
- 使用制御（UC：Use Control）
- システムの完全性（SI：System Integrity）
- データの機密性（DC：Data Confidentiality）
- 制限されたデータ・フロー（RDF：Restricted Data Flow）
- イベントに対するタイムリーな応答（TRE：Timely Response to Events）
- リソースの可用性（RA：Resource Availability）

SL 1は（1, 1, 1, 1, 1, 1, 1）というセキュリティのベクトルで表すことができます。ベクトル内の各項目は、7つのFRのうちの1つに対応しています。SL 1は、偶発的な攻撃を対象にしています。このことから、SL 1は予測可能な誤用を考慮しなければならない安全アプリケーションの最小限の要件だと考えられます[13]。SILが1を超える安全アプリケーションに適したベクトルは（N1, N2, N3, 1, 1, N6, 1）と表現できます[13]。産業用の機能安全アプリケーションでは、データの機密性、制限されたデータ・フロー、リソースの可用性については、それほどの懸念はないと認識されているということになります。なお、SILが2、3、4のうちいずれであるとしても、N1、N2、N3、N6の値の間に明確な相関はありません。

すべてのセキュリティ・システムに、機能安全の要件が存在するわけではありません。重要なのは、安全に関連するすべてのシステムではセキュリティについて必ず考慮しなければならないということです。

機能安全とロボット

ISO 10218[14]は、コボットを含む産業用ロボットの安全に関する要件を対象とした規格です。同規格では、停止、ティーチング、速度、分離監視に加え、動力／力の制限が取り上げられています。ISO 10218-1:2011の5.4.2項では、制御システムにおいて安全に関連する部分について、ISO 13849-1:2006のカテゴリ3におけるPL＝D、またはIEC 62061:2005のHFT（Hardware Fault Tolerance：ハードウェア障害許容度）が1のSIL 2に準拠するよう設計することを求めています。このことは、事実上少なくとも2チャンネルの安全システムにおいて、各チャンネルの診断カバレッジとして60%以上が求められるということを意味しています。なお、ISO 13849とIEC 62061では、ソフトウェアに関する要件についてはIEC 61508-3に従っています。

ISO 10218では、AGVについてはあまり深く掘り下げていません。自動運転車は車載規格であるISO 26262で扱われていますが、産業分野では自動運転車の適用範囲は非常に限定されています。AGVは、自動車の中でも特殊な存在だと言えます。一方で、AGVは機械指令の適用範囲には含まれています。ただ、特定の規格は存在しないので、汎用規格であるIEC 61508の要件を適用することになります。

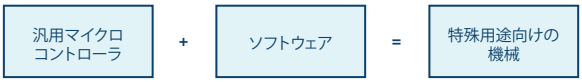

図4. ソフトウェアの主な長所

固定型のロボットの場合、ネットワークとしてはイーサネットをベースとしたものが使われるケースが多いでしょう。AGVの場合にはワイヤレスになるでしょうが、それに向けては、安全とセキュリティに関する追加の要件が生じます。

機能安全とソフトウェア

品質の高いソフトウェアを実装するための詳細な要件は、安全とセキュリティのどちらを対象にするのかによらず、ほとんど同じになります。例えば、プログラマに起因するエラーは、条件がそろえばシステムの故障につながり、エラーが明らかになる可能性があります。その確率を判断するのは困難ですが、機能安全の規格の中には、その確率を100%と見なすべきだと規定しているものもあります[15]。ただ、99.99%バグが含まれていないプログラムであれば、通常は安全上の問題を起こすことはないと考えるのが妥当なようです。ところが、ハッカーは残りの0.01%を突いて攻撃を仕掛けてきます。そのため、機能安全と同様に、セキュリティについても決定論的原因故障を排除するのは重要なことです。とはいえ、100%バグのない完璧な安全関連のソフトウェアであっても、セキュリティ上の重大な課題を抱えている可能性はあります。

以前は、安全システムには様々な状態が存在することから、本質的に完全なテストは行うことができず、ソフトウェアの使用は認められないとされていました。しかし、新たな規格ではライフサイクルのモデルが提供されるようになりました。それに従えば、安全であるという主張が可能になります。なぜなら、それらの規格で提唱されている手法を採用すれば安全なシステムを構築できるということが過去に実証されているからです。ソフトウェアを使用すれば、汎用的な機械を非常に特殊な機械として動作させられます。つまり、ソフトウェアの適用は、非常に魅力的なことであるように思えます。しかし、そうした柔軟性は弱点の1つにもなり得ます。

ESDA-312[16]などのドキュメントを見ると、IEC 61508の多くの手法は産業分野のセキュリティの要件に適合するために使用できると記載されています。適切なプロセスに従えば、作業の成果物に関する記録が残り、安全が実現されたことを証明する上で役に立ちます。

有用な手法としては、デザイン・レビューの実施、コーディング規約の適用、ツールの使用計画の策定、単体レベルでの検証、要件のトレーサビリティの確保、第三者による検証、アセスメントなどが挙げられます。機械類とは異なり、ソフトウェアは摩耗／劣化することはありません。しかし、それを実行するハードウェアは故障する可能性があります。そのため、ソフトウェアはそのような状況に対処できるものにしなければなりません。機械やロボットについては、ISO 13849のカテゴリ3／カテゴリ4などで示されている冗長アーキテクチャを適用する方法が考えられます。そうすると、ICのレベルで診断機能を実装する必要性は低くなります。但し、様々なソフトウェアを用意しなければならなくなります。

機能安全とIC

スマート・システムの実現にはICが不可欠です。例えば、ICを利用すれば、コンテナそのものだけではなく、コンテナ内の各アイテムを追跡することができます。また、ロボット全体ではなく、各ロボット・アームの位置を追跡することが可能になります。加えて、さほど重要性の高くない機械の状態も追跡できます。更に、クラウドに対し、データではなく、情報を送信できるようにデータを処理する手段を提供することも可能です。あるいは、モータの制御用に新たなICを適用すれば、モータの効率を高めたり、バッテリの寿命を延ばしたりすることもできます。

ICは頭脳として働きます。ただ、特にエッジでは、その頭脳がコンパクトかつ低消費電力で機能することが求められます。また、ICは、レーダー、レーザ、磁気センサー、カメラ、超音波センサーといった検出技術も提供します。AMR（Anisotropic Magnetoresistance：異方性磁気抵抗）などの新たなセンサー技術を活用することにより、外付けの機械部品を使うことなく速度や位置を測定することも可能になります。ICには、ネットワークの物理インターフェース層とMAC（Media Access Control）層の両方を実装できます。ワイヤレス通信の各レイヤは、すべてICに実装することが可能です。

同様に、ICを使用すれば、PUF（Physically Unclonable Function：物理的複製防止機能）や、暗号化用のアクセラレータ、改ざん検出機構などによってセキュリティ機能を強化することができます。高いレベルの集積化が可能になったことから、従来はシステム・レベルの要件であったものがICレベルの要件に変化しつつあります。

しかし、産業分野向けの機能安全規格にはICに関する記述はほとんどありません。セキュリティ規格では更に記述が少なくなります。車載分野では、2018年に発表予定のISO 26262-11のドラフトが優れた情報源になります。多くの内容が、産業分野のアプリケーションで使用されるICの開発においても役に立つでしょう。IEC 61508の第2版には、ASICのライフサイクル・モデルが示されています。その内容は、ソフトウェア向けのものとほとんど同一です。実際、Verilogなどで記述されたHDLのコードはソフトウェアなのか、それともハードウェアについての表現なのかという議論は興味深いものだと言えます。IEC 61508-2:2010の附属書Eでは、単一のシリコン・チップを使用している場合の冗長性について言及しています。具体的には、そのチップ内で冗長性を実現する場合の要件が記載されています。ただ、その対象はデジタル回路のみに限定されています。アナログ回路とミックスド・シグナル回路については、冗長化の対象としては捉えられていません。一方、IEC 61508-2:2010の附属書Fも情報源として非常に有用です。なぜなら、決定論的原因故障を回避するためにICの開発中に講じるべき手段のリストが提供されているからです。その要件は、SILごとに提供されていますが、やはりその対象はデジタル回路に限定されています。アナログICやミックスド・シグナルICに関する具体的なガイダンスは存在しないということです。

ICでは、集積度を高めることが大きな価値になります。しかし、それはトラブルの原因にもなり得ます。IC上の個々のトランジスタは、ディスクリートのコンポーネントと比べて非常に信頼性が高いと言えます。多くの場合、ICの中で最も信頼性が低いのはピンの部分です。例として、SiemensのSN 29500規格を信頼性の予測に利用するケースを考えます。その場合、50万個のトランジスタを搭載したICのFIT（Failure In Time：平均故障率）は70となります。トランジスタの数が10倍の500万個であったとしても、FITは80までしか増加しません。では、それぞれ50万個のトランジスタを搭載した2個のICを使用する場合にはどうなるでしょうか。それぞれのFITは70なので、全体では140となります。FITを140から80に低減するというのは、集積度を上げるだけで実現されていることなのです。プリント基板上の実装面積、基板のパターン、外付け受動部品の削減などについて考慮することなく、FITを低減できるというのは大きなメリットです。基板に実装する場合よりもはるかに小型なアンテナをICに内蔵すれば、EMIの問題を抑制できるといった検討を行うことなく改善を図れるということです。ただ、集積度を上げることには欠点もあります。それは、ICの複雑化が進むことによって、故障のモードを特定するのが難しくなる可能性があるということです。安全を実現する上で、シンプルであることが有利に働きます。そして、個別にパッケージングされた2個のマイクロコントローラは、2つのマイクロコントローラを内蔵する1個のICよりもシンプルだと言えます。IEC 61508-2:2010の附属書Eは、いくつかのガイダンスを提供しています。十分な独立性を確保できる場合もそうですが、ほとんどの安全規格では、係数β（2つのチャンネルが同一の原因で同時に故障する尺度）が10%未満であれば非常に良好であるとされています。

ICのメーカーは、安全とセキュリティの両面からサプライヤを支援します。例えば、認証済みのIC製品、安全マニュアル、リリース済みの製品の安全データシート、内蔵ハードウェア・アクセラレータ、内部／外部の診断機能、重大／非重大なソフトウェア（どちらも安全とセキュリティの面で重要）の分離手段などを提供しています。安全とセキュリティに関する機能は、最初からデザイン・インの形で実現しなければなりません。ICを設計した後に安全とセキュリティに関する機能を追加しようとすると、システムが更に複雑になり、部品を追加しなければならなくなるでしょう。

機能的に安全なシステムで使用するためのICの開発方法には、複数のオプションがあります。各種の規格には、それに準拠するICしか使ってはならないという要件はありません。ただ、モジュール／システムの設計者は、選択したICがシステムでの使用に適しているか否かを確認する必要があります。独立系の評価機関による審査を受けた安全マニュアルはぜひ活用すべきです。ただ、それが唯一の選択肢であるというわけではありません。採用可能なオプションとしては、以下のようなものがあります。

【オプション1】外部の評価機関を利用し、安全マニュアルを参照して、IEC 61508に完全に準拠する形で開発を行う

【オプション2】外部の評価機関は利用せず、安全マニュアルを参照して、IEC 61508に準拠する形で開発を行う

【オプション3】安全データシートを公開しているICメーカーの標準的な開発プロセスに従って開発を行う

【オプション4】ICメーカーの標準プロセスに従って開発を行う

なお、IEC 61508に準拠して開発されているわけではない製品については、混同を避けるために、安全マニュアルのことを安全データシートなどと呼ぶことがあります。どちらであっても、内容と形式はほぼ同じです。

オプション1は、ICメーカーにとって最もコストのかかるものです。しかし、モジュール／システムの設計者にとっては最も都合の良いアプローチである可能性があります。システムとICにおいて安全という概念の内容が合致していれば、モジュール／システムを外部機関で評価する際に問題に遭遇するリスクが低下します。SIL 2の安全機能を設計するためには、20%以上に上る追加の作業が発生する可能性があります。ICメーカーは、機能安全には対応していないものの、既に厳格な開発プロセスを設けている場合があります。そうしたメーカーの製品を採用する場合を除くと、おそらくは更に多くの追加の作業が必要になるでしょう。

オプション2では、外部の評価機関による評価のコストがかからないことを除けば、オプション1と同等の効果が得られるはずです。このアプローチは、いずれにせよお客様がモジュール／システムの社外認定を受けるつもりでいて、ICがシステムの重要な要素であるケースに適しているかもしれません。

オプション3は、ICが既に提供されており、安全データシートを参照することによって、モジュール／システムの設計者がより高いレベルの安全設計に必要な追加の情報を入手できる場合に最も適しています。そうした情報の例としては、実際に適用された開発プロセスの詳細、ICのFITのデータ、診断機能の詳細、ISO 9001の認証を得た製造施設の登録証などが挙げられます。

ICの現実の開発で最もよく使われるのはオプション4です。そのようにして開発されたICを使用して安全モジュール／システムを設計する場合、追加のコンポーネントやコストが必要になるでしょう。おそらく、そのICは、シングルチャンネルのアーキテクチャで実現されているでしょう。つまり、比較が可能なデュアルチャンネルのアーキテクチャを使用する診断機能は備えていないはずなので、追加の対応が必要になるということです。また、そうしたICによる診断テストの実施間隔は一般には最適ではありません。可用性に影響を与える可能性がある障害が発生した場合でも、どの部分が故障したのか特定することもできないはずです。結果として可用性が低下することになります。安全データシートが存在しない場合、モジュール／システムの設計者は、保守的な仮定に基づいてICをブラック・ボックスとして扱わなければなりません。その場合、信頼性の数値が低下する可能性があります。

機能安全の実装を簡素化するために、ICメーカーはIEC 61508について独自の解釈を行うことがあります。アナログ・デバイセズの場合、ADI61508という社内規格を定めています。これは、ICの開発向けにIEC 61508を解釈したものです。IEC 61508の7つのパートすべてを解釈し、1つのドキュメントとしてまとめています。IEC 61508のうちICに関係がない部分を省略し、残りの部分をIC向けに解釈するということを行っています。

システム・レベルの規格としてどのようなものが適用されるのかに関わらず、車載用のものを除けば、アナログ・デバイセズのICはIEC 61508に準拠して開発されます。車載アプリケーション用のICとソフトウェアは、ISO 26262をベースとして開発されます。

まとめ

インダストリ4.0では、IEC 61508に基づく様々な機能安全規格が活用されます。例えば、ソフトウェア、ハードウェア、ネットワーク、セキュリティ、ロボットに関する規格などです。ただ、現在は複数の規格に情報が分散している状態にあります。また、インダストリ4.0では、求められる柔軟性を得るために、絶え間なく生じる変化に対応するための独自の機能が用いられます。理想的には、インダストリ4.0に焦点を絞った単一の規格が提供されるべきです。新たな世界に向けた基本的な安全規格の解釈に基づいて、より容易に規格に準拠できるようにするべきでしょう。この考え方は、「セーフティ4.0」あるいは「スマート・セーフティ」と呼ばれることになるはずです。同様に、十分な安全性の達成／実証を可能にするためには、IEC 61508にICに関連するより多くの情報を盛り込む必要があります。今後、インダストリ4.0が現実のものとなり、成功に至るまでは、その機会と課題に注目する必要があります。

機能安全は、インダストリ4.0に対して数多くの好影響をもたらします。なぜなら、将来の工場にとっては安全という要素が不可欠だからです。また、機能安全は高い信頼性、高度な診断、レジリエンス、冗長性を実現する手法を提供します。そのため、インダストリ4.0に多いに貢献できることは明らかだと言えるでしょう。

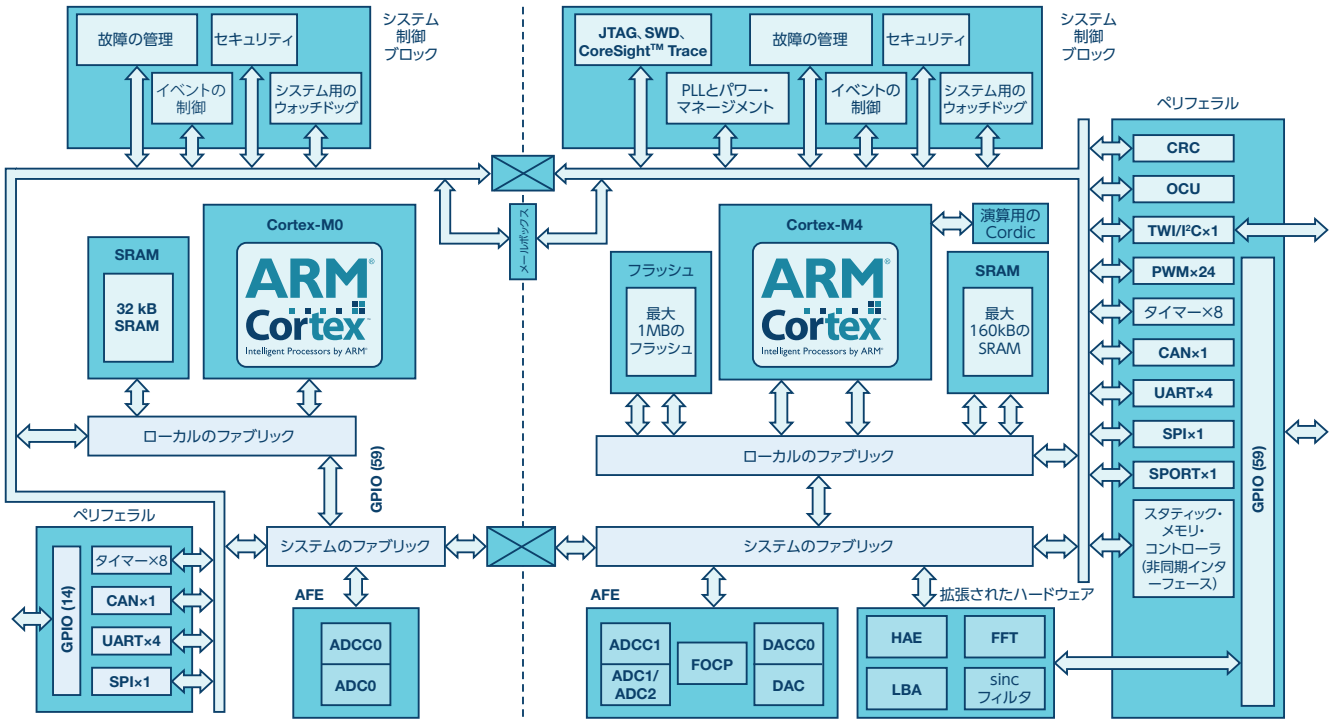

図5. アナログ・デバイセズの「ADSP-CM41xシリーズ」。
数多くの安全機能とセキュリティ機能を備えています。

参考資料

[1] IEC 61508 All Parts, Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems（IEC 61508 全パート：電気／電子／プログラマブル電子安全関連系の機能安全）、International Electrotechnical Commission、2010年

[2] ISO 26262 All Parts, Road Vehicles Functional Safety（ISO 26262 全パート：自動車の機能安全）、International Organization for Standardization、2011年

[3] IEC 61511 All Parts, Functional Safety－Safety Instrumented Systems for the Process Industry Sector（IEC 61511 全パート：機能安全－プロセス産業分野の安全計装システム）、International Electrotechnical Commission、2016年

[4] IEC 61131-6 Programmable Controllers－Part 6: Functional Safety（IEC 61131-6 プログラマブル・コントローラ 第6部：機能安全）、International Electrotechnical Commission、2012年

[5] IEC 62061－Safety of Machinery－Functional Safety of Safety-Related Electrical, Electronic, and Programmable Electronic Control Systems（IEC 62061：機械類の安全性－安全関連の電気／電子／プログラマブル電子制御システムの機能安全）、International Electrotechnical Commission、2005年

[6] IEC 61800-5-2 Adjustable Speed Electrical Power Drive Systems－Part 5-2: Safety Requirements－Functional（IEC 61800-5-2：可変速駆動システム－第5-2部：安全要求事項－機能安全）、International Electrotechnical Commission、2016年

[7] ISO 13849 All Parts, Safety of Machinery－Safety-Related Parts of Control Systems（ISO 13849 全パート：機械類の安全性－制御システムの安全関連部）、International Organization for Standardization、2015年

[8] 「Recommendations of Implementing the Strategic Initiative Industrie 4.0: Final Report of the Industrie 4.0 Working Group（戦略的イニシアチブ　インダストリ4.0の実施勧告：インダストリ4.0作業部会の最終報告書）」Forchungsunion and acatech、2013年4月

[9] IEC 61784-3 Industrial Communication Networks－Profiles－Part 3: Functional Safety Fieldbuses－General Rules and Profile Definitions（IEC 61784-3：工業用通信ネットワーク－プロファイル－第3部：機能安全フィールドバス－一般規則およびプロファイルの定義）、International Electrotechnical Commission、2016年

[10] ISO/IEC 62443 All Parts, Security for Industrial Automation and Control Systems（ISO/IEC 62443 全パート：産業用オートメーションおよび制御システムのセキュリティ）

[11] IEC 62880, Railway Applications－Communication, Signaling, and Processing Systems－Part 1: Safety-Related Communication in Closed Transmission Systems（IEC 62280：鉄道分野－通信、信号および処理システム－第1部：クローズド伝送システムにおける安全関連通信）、International Electrotechnical Commission、2017年

[12] EN 50159, Railway Applications－Communication, Signaling, and Processing Systems－Part 1: Safety-Related Communication In Closed Transmission Systems（EN 50159：鉄道分野－通信、信号および処理システム－第1部：クローズド伝送システムにおける安全関連通信）、European Committee for Electrotechnical Standardization、2010年9月

[13] Jens Braband「What's Security Level got to do with Safety Integrity Level?（セキュリティのレベルと安全度のレベルにはどのような関係があるのか？）」8th European Congress on Embedded Real-Time Software and Systems（ERTS 2016）、2016年1月

[14] ISO 10218-1, Robots and Robotic Devices－Safety Requirements for Industrial Robots－Part 1: Robots（ISO 10218-1：ロボットおよびロボティック・デバイス－産業用ロボットのための安全要求事項－第1部：ロボット）、International Organization for Standardization、2011年

[15] Chris Hobbs「Embedded Software Systems For Safety Critical Systems（セーフティ・クリティカル・システム向けの組み込みソフトウェア・システム）」Auerback Publications、2015年10月

[16] ISA Security compliance institute－EDSA-312－Embedded Device Security Assurance－Software Development Security Assessment（EDSA-312：組み込みデバイスのセキュリティ保証－ソフトウェア開発セキュリティ・アセスメント）、International Electrotechnical Commission、2016年7月

著者について

Tom　Meany（tom.meany@analog.com）は、アナログ・デバイセズで30年にわたり業務に携わってきました。IEC 61508-2、IEC 61508-3、IEC 61800-5-2など、機能安全の分野に関連するIECの様々な作業部会に所属しています。また、TÜV　Rheinlandの機能安全技術者（機械類）の資格も取得。米国特許を8件保有しています。電子工学の学士号、応用数学／コンピューティングに関する理学修士号を優秀な成績で取得しました。

オンライン・サポート・コミュニティ

EngineerZone™
SUPPORT COMMUNITY

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。

ez.analog.com にアクセス

＊英語版技術記事はこちらよりご覧いただけます。

アナログ・デバイセズ株式会社
本　　社　〒105-6891　東京都港区海岸1-16-1　ニューピア竹芝サウスタワービル 10F
大 阪 営 業 所　〒532-0003　大阪府大阪市淀川区宮原3-5-36　新大阪トラストタワー 10F
名古屋営業所　〒451-6038　愛知県名古屋市西区牛島町6-1　名古屋ルーセントタワー 38F

TA16602-0-3/18

www.analog.com/jp

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