



WP511 (v1.0.1) 2019 年 7 月 1 日

# 医療機器のエンベデッド システムにおけるリスク管理

Zynq UltraScale+ MPSoC テクノロジーを医療機器および医療システムの設計に使用すると、機能安全およびサイバーセキュリティの規格に適合した、より堅牢なデザインを短期間で開発できます。

## 概要

このホワイト ペーパーでは、さまざまな法規制があるために複雑になりがちな医療機器の開発における、機能安全とサイバーセキュリティの対策方法について概要を説明します。

医療機器の監督機関が定義するリスクを適切に管理するには、堅牢な機能安全の方法およびサイバーセキュリティの要求事項の両方を理解する必要があります。適切なリスク管理により、機器のハードウェアとソフトウェアは本来の正しい動作を継続できます。これと同じ目標は産業オートメーション分野にも存在し、独立行政機関によって IEC 61508 および IEC 62443 規格に基づいて監督されています。

ザイリンクスが提供するシリコンおよび開発ツールには、これらの規格に準拠した実装を可能にする機能が幅広く用意されています。IEC 61508 と IEC 62443 の両規格に対応した Zynq® UltraScale+™ MPSoC プラットフォームを医療機器に利用すると、電子医療システムにおける安全とセキュリティの目標を同時に達成できます。

© Copyright 2019 Xilinx, Inc. Xilinx, Xilinx のロゴ、Alveo、Artix、ISE、Kintex、Spartan、UltraScale、Versal、Virtex、Vivado、Zynq、およびこの文書に含まれるその他の指定されたブランドは、米国およびその他の各国のザイリンクス社の商標です。PCI、PCIe、および PCI Express は PCI-SIG の商標であり、ライセンスに基づいて使用されています。すべてのその他の商標は、それぞれの所有者に帰属します。

この資料は表記のバージョンの英語版を翻訳したもので、内容に相違が生じる場合には原文を優先します。資料によっては英語版の更新に対応していないものがあります。日本語版は参考用としてご使用の上、最新情報につきましては、必ず最新英語版をご参照ください。

# はじめに

医療機器市場の製品は、コンピューター断層撮影法 (CT)、磁気共鳴画像 (MRI)、超音波検査など非侵襲的な画像診断装置のほか、手術ロボット、人工呼吸器などの生命維持装置、ペースメーカーなどの体内植え込み装置といった侵襲的装置まで多岐にわたります。患者に与えるリスクのレベルは、これら製品のカテゴリごとに異なります。このため、米国食品医薬品局 (FDA) や欧州連合 (EU) 医療機器指令 (MDD) CE マーキング チームなどの監督機関は、さまざまな製品設計基準を利用してこのリスクを管理することを機器メーカーに求めています。

## 医療機器の設計における留意事項

医療機器を設計する際、開発チームは臨床での応用に有効な機器を開発することだけに注意するのではなく、患者の安全保護 (IEC-60601-1、1-4 「ハードウェア電気デザイン」、IEC-62304 「ソフトウェア ライフ サイクル プロセス」 など)、システムを流れるデータの情報保証 (HIPAA など)、動作のログ記録や製品アップデートの配布を含む、機器のライフ サイクル (FDA CFR 21 など) にも留意する必要があります。

このように、機器本来の動作に加え、動作の安全が求められるのは医療機器産業だけではありません。自律化が進む機械と人間が同じ場所で作業するような業界全般が影響を受けます。現在の産業用ロボットはオペレーターの指示に従って動くだけでなく、完全に独立した共同作業者となりつつあり、人間の安全を最優先して動作することが求められています。たとえば自動車の場合、自動運転の発展に伴い安全機能の改良も進んでおり、人間のドライバーが安心して身を任せられるようになってきています。

産業オートメーションにおいて、システムの安全に直接影響する機械の実装は、「機能安全」の分野で扱われます。機能安全とは、これらの要件を満たすための一連の規格および設計手法を総称した用語です。機能安全の設計手法では、機器本来の動作と故障経路を考慮しますが、近年は攻撃者がシステム本来の動作を改ざんしようとするサイバーセキュリティの脅威レベルも上がっていることに注意が必要です。したがって、現在の医療機器の製品開発において完全なリスク管理の方法を検討するには、機能安全とサイバーセキュリティの両方を患者の安全に不可欠な要素として考える必要があります。製品設計において機能安全を考慮せずサイバーセキュリティ対策のみを講じることは可能ですが、サイバーセキュリティ対策なしに機能安全を実装することはできません。

このホワイト ペーパーは、機能安全とサイバーセキュリティの大きく 2 つのトピックで構成されています。

1. 「機能安全」のセクションでは、機能安全の概要および各種安全度水準 (SIL) の製品を実現するための一般的な設計手法について説明します。
2. 「サイバーセキュリティ」のセクションでは、サイバーセキュリティの概要および予測される脅威に対するセキュリティ レベル (SL) の実装の評価方法について説明します。

# 機能安全

機能安全とは、機械の「主機能」を監視して人間や環境に危害が及ぶリスクを軽減することを目的としたシステムを指し、これらはいくつかの規格に示された手法やガイダンスに従って開発されます。一般に、機能安全は被制御機器 (EUC) を常時監視し、機械の故障など何らかの動作異常が発生した場合や、外部からの力によって危険な状態が発生した場合に作動します。機械メーカーは、設計時にハザード/リスク評価を実施し、どのようなリスク軽減対策が必要かを理解します。

機能安全システムには、電源に接続するリミット スイッチのような単純なものから、製造フロアで人間が危険区域に立ち入らない (たとえば、組み立てラインで動いているトラック シャーシに近付きすぎない) ように監視する LiDAR システムのように複雑なものまで、さまざまあります。

機能安全は、サッカーやアメリカン フットボールなどの試合にたとえることができます。被制御機器 (EUC) が選手で、安全関連システムが審判です。審判はルールを把握しており、さまざまな事象の発生に応じてプレイを中断したり続行したりして、試合の進行をコントロールします。また、反則のあったチームや選手に対して適切なペナルティを課すのも審判の重要な役割です。

## 医療機器設計における機能安全の留意事項

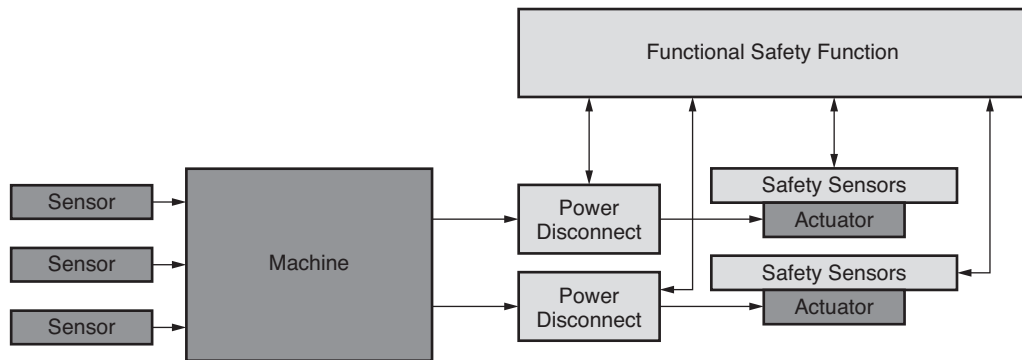
米国で医療機器を販売する場合、機器メーカーは事前に FDA (食品医薬品局) へ届け出の義務があります。これは「市販前届」と呼ばれ、連邦食品医薬品化粧品法 (FFDCA) の 510(k) 項で規定されていることから、510(k) とも呼ばれます。この条項に基づき、FDA は届け出のあった機器が過去に合法的に販売された機器と実質的同等であると認められる場合、販売のためのクリアランスレター (許可書) を発行します。

ただし、実質的同等な機能を構築するのに使用する機器はそれぞれ実装も物理的屬性も異なるため、機能安全に関する実質的同等性の議論には問題があります。

FDA の管轄を受けない機器や機械については、UL (旧 Underwriters Laboratories) などの独立系機関から認証を取得して安全規格に適合することが、各国政府によって義務付けられています。<sup>1)</sup> この独立性により、テクノロジーおよび市場の原理に基づいて規格が進展でき、利益相反も最小限に抑えることができます。

機能安全システムの目的はリスクを軽減することにあります。機械が機能不全を起こした場合、機能安全システムはこの機械を強制的に「安全状態」に移行させる必要があります。つまり、リスク軽減の観点では安全システムの可用性 (システムが将来のある時点で動作している確率) が重要な要因となります。必要なときに機能安全システムが動作しないという事態は避けなければなりません。機能安全システムには 24 時間 365 日の可用性が求められるため、機能安全システムの設計とテストは国際規格によって管理されており、独立系認証機関によって検証されます。

図 1 は、濃いグレーで表した被制御機器 (EUC) と薄いグレーで表した機能安全システムの関係を示したものです。機能安全システムは、EUC の動作を常時監視します。図 1 では、アクチュエーターの電源を遮断した状態が安全状態です。EUC の動作が境界違反を起こして危険な状態が生じた場合、機能安全システムがアクチュエーターへの電源供給を遮断します。安全機能は、独立したセーフティ ネットと考えることができます。安全機能が故障しても EUC は動作を継続できるかもしれませんが、それはセーフティ ネットなしでの動作となります。



WP511\_01\_30519

図 1: 安全機能と被制御機器 (EUC)

1. 非営利機関の Underwriters Laboratories は、2012 年 1 月 1 日に米国の営利企業となりました。Underwriters Laboratories の製品テスト/認証事業は、UL LLC という名前の新しい子会社が引き継いでいます。(出典: Wikipedia、「UL (安全機関)」、最終アクセス日 2019 年 3 月)

## 安全機能の3つのブロック

通常、安全機能自体は3つのブロックで構成されます(図2)。すなわち、(1)センサーが(2)ロジックソルバーへの入力を駆動し、ロジックソルバーが(3)アクチュエーターを駆動します。これら3つのブロックで構成される安全機能は、「安全ループ」とも呼ばれます。また、これら3つのブロックすべてに基づいて決定される安全ループの品質を、安全度水準(SIL)と呼びます。

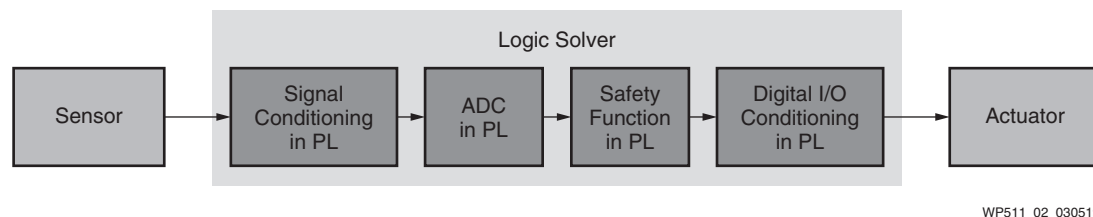


図2: 安全機能の3つのブロック

## 故障、リスク軽減、安全度水準

業界では、「故障 (failure)」は本来のサービスが終了した状態、「障害 (fault)」は機能の故障の原因となった異常な状態、そして「エラー (error)」は予測される正しい値と実際の値が一致しないこと、と定義されます。

故障は大きく2つのカテゴリに分類されます。安全ループの動作に影響せず、機器が「安全状態」に移行しない故障は安全側故障と呼びます。「安全ループ」の動作に影響するものは危険側故障と呼びます。すなわち、障害が原因となってエラーが生じ、エラーが原因となって故障が生じます。

## IEC 61508

IEC 61508 (電子/電気/プログラマブル電子システムの機能安全規格) には、SIL1 ~ SIL4 の4つの安全度水準があります。これらのレベルにより、EUCを監視する機能安全システムまたは安全ループのリスク軽減を客観的に定義します。各SILの定義を、表1に示します。

SILは、2つの要素によって決定します。1つは決定論的能力で、これは人的エラーによってデザインで生じる潜在的なバグの量を定性的に測定する品質メトリクスです。このメトリクスは、規格で定義されたプロセスに従っていることの証拠に基づいて決定します。もう1つの要素は、ランダムハードウェア障害を軽減するための診断機能の実装です。システムのSILは、これら2つの要素のうち、いずれか低い方のメトリクスによって決まります。

表1: 1時間あたりの危険側故障率

安全度水準	安全可用性要求 (RSA)	高頻度作動要求モード (<1年)		
		1時間あたりの危険側故障平均確率 (PFH)	時間あたりの故障率 ( $\lambda$ )	1時間あたりのリスク低減係数 (RRF)
SIL 1	90 ~ 99%	0.00001 ~ 0.000001	10億時間の稼働あたりの危険側故障回数 <10,000	100,000 ~ 1,000,000
SIL 2	99 ~ 99.9%	0.000001 ~ 0.0000001	10億時間の稼働あたりの危険側故障回数 <1,000	1,000,000 ~ 10,000,000
SIL 3	99.9 ~ 99.99%	0.0000001 ~ 0.00000001	10億時間の稼働あたりの危険側故障回数 <100	10,000,000 ~ 100,000,000
SIL 4	99.99% ~ 99.999%	0.00000001 ~ 0.000000001	10億時間の稼働あたりの危険側故障回数 <10	100,000,000 ~ 1,000,000,000

## 安全状態

安全状態は、機械がどのように稼働するか、およびメーカーによるハザードおよびリスク評価に基づいて機械メーカーが定義する必要があります。安全状態の例としては、モーターの主電源を遮断したり、機械の主電源を遮断して内蔵のパッシブ機構を動作させ、システムからエネルギーを取り除いたりするものがあります。これは、ハザードの種類に応じて決定します。

MRI 装置などの医療機器では、患者を機器外部へ搬出できるなら、電源遮断を安全状態とすることが考えられます。一方、集中治療室で使用する生体情報モニターなどの医療機器で電源遮断を安全状態としてしまうと、患者のリスクが増大するおそれがあります。特に、人工心肺装置や人工呼吸器などで電源遮断を安全状態とすると、患者の生命に重大な危険をもたらすことが考えられます。

システムが安全状態に移行する条件は2つあります。1つは、EUC または何らかの外部要因によって危険状態が生じ、安全機能によって検出された場合です。もう1つは、安全ループのシステム障害が安全機能自体によって検出された場合です。

EUC が故障して安全ループが EUC を安全状態に移行させた場合、EUC の可用性を維持するには、EUC デザイン自体を冗長化する必要があります。

機器を安全状態に移行することが許容できず、かつ安全ループが故障した場合は、安全ループ自体のアーキテクチャを冗長化します」。これにより安全ループの可用性が向上し、その結果、安全ループによって保護される EUC の可用性も向上します。

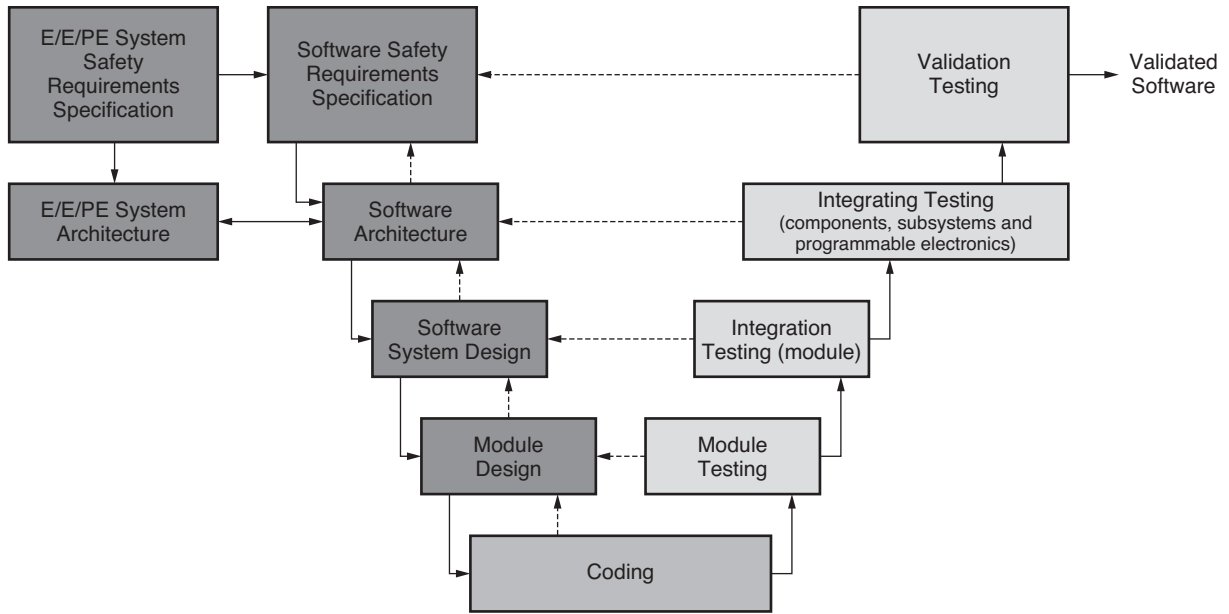
## 可用性

どのようなシステムも、時間の経過と共に故障の確率が高くなります。安全ループでは、この点に特に注意が必要です。システム故障の大きな原因には、ランダム ハードウェア障害とシステムティック故障の2つがあります。

ハードウェア故障はランダムに発生するため、システム故障の検出を目的とした機能安全システムは、高い可用性を維持する必要があります。このようなシステムの設計を支援するため、機能安全の親規格である IEC 61508 『電気/電子/プログラマブル電子安全関連システムの機能安全』には、これらシステムの設計に使用すべき推奨アーキテクチャの一覧が示されています。この規格では、安全ループの動作故障を検出する手段、および故障時に安全機能の動作を継続する「フェイルオペレーショナル」が必要な場合に冗長性を追加する手段が記載されています。

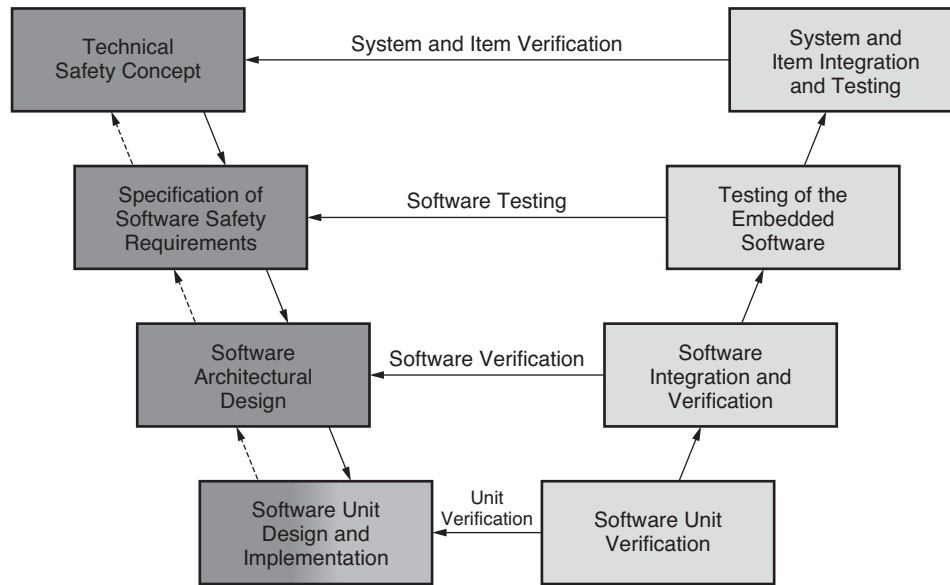
システムティック故障は、IEC 61508 に記載されている十分にテストされた最先端の対策を採用した設計プロセスによって軽減されます。このプロセスは、システム メーカー内部の利益相反の影響を受けないように、独立して管理する必要があります。このようなプロセスは、現在さまざまなものが使用されています。現在最先端のソフトウェア設計プロセスとして、図 3 (出典: IEC 61508) や図 4 (出典: ISO 26262) のような V モデルがあります。いずれのプロセスも、左側が設計シーケンスで、右側が検証シーケンスを示しています。

V モデルの左側は、プロジェクトの定義と設計を表しています。V モデルの右側は、プロジェクトのテストと統合を表しており、中央の底の部分がユニット コーディングを表しています。実際のユニット コーディングは、テストの基盤が完成するまでは開始されません。



WP511\_03\_30519

図 3: IEC 61508:2010 Part 3 に記載されたソフトウェア設計フロー



WP511\_04\_30519

図 4: ISO 26262:2018 Part 6 に記載されたソフトウェア設計フロー

このプロセスは、最終的な状態を完全に理解した上で開始します。まず、設計プロセスの最初に要求事項のリストを作成します。要求事項に対するレビューと承認が完了したら、次にアーキテクチャ仕様を作成します。アーキテクチャ仕様では、要求事項を満たすように機能をブロック単位に分割し、インターフェイスを作成します。アーキテクチャ定義と仕様作成、およびピアレビューが完了したら、各ブロックとインターフェイスに対するテスト要件を作成します。テスト要件に対するピアレビューと検証が完了したら、テストベンチのコーディングを開始します。

この時点で、設計スケジュールはほぼ半分を経過していることとなりますが、アプリケーションコードはまだ1行も作成されていません。

次に、テストベンチのコーディングにスケジュールを割り当てます。テストベンチが完成すれば、コーディング時点で機能を正しく設計できる確率が非常に高くなるため、開発は成功したも同然です。最後に、ユニットコーディングを開始し、検証と妥当性確認を過不足のないように実施します。このプロセスでバグが残る確率はそれほど高くありませんが、それは最初に作成した要求事項のリストがどれほど網羅的であるかによります。要求事項とそれに対応するテストベンチが網羅的であればあるほど、バグが残る確率は低くなります。

もう1つの考慮事項として、ランダムハードウェア故障があります。ランダムハードウェア故障をどのような手段で検出(および場合によっては訂正)するかは、電子デバイスの故障の種類によって異なります。デジタルICの故障の原因としては、製造エラー、外部からの粒子衝突、メタルマイグレーションによるデバイス損傷などがあります。ランダムハードウェア故障には永続的なものと一時的なものがありますが、機械の動作に影響を与えるかどうかは障害の性質によります。機械の動作に影響を与えるものは「危険側故障」と呼び、影響を与えないものは「安全側故障」と呼びます。これらの障害を検出し、場合によっては訂正するための対策を「診断機能」と呼びます。現在広く使用されている診断機能には、次のものがあります。

- **噴水符号:** 基地局と携帯電話の間では、必ずランダムな信号干渉があり、伝送エラーが発生します。現在の携帯電話通信システムはすべて噴水符号を使用して、このエラーを訂正しています。
- **メモリ保護:** 現在稼働しているすべてのサーバーで、破損したメモリデータの検出と訂正にエラー訂正符号(ECC)が使用されています。
- **冗長化:** 主機能の実行に必要なリソースを二重化して並列に実行します。

この3つの中で最も完全な診断機能が得られるのは冗長化ですが、コストも最大となります。冗長化として最も一般的なのは、「1oo2 (One out of Two)」(図5)と「2oo3 (Two out of Three)」(図6)と呼ばれる方式です。

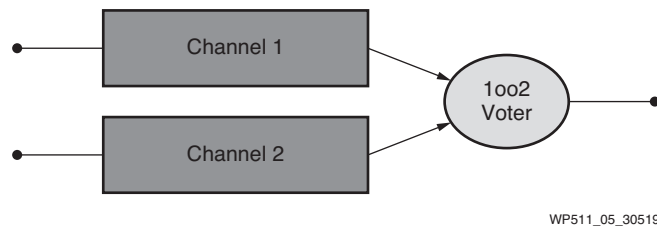


図 5: 1oo2 (One out of Two) 安全アーキテクチャ

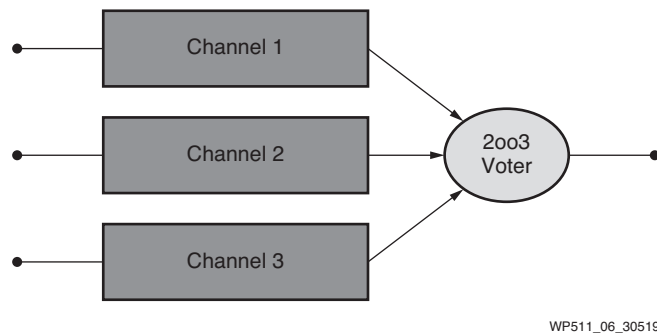


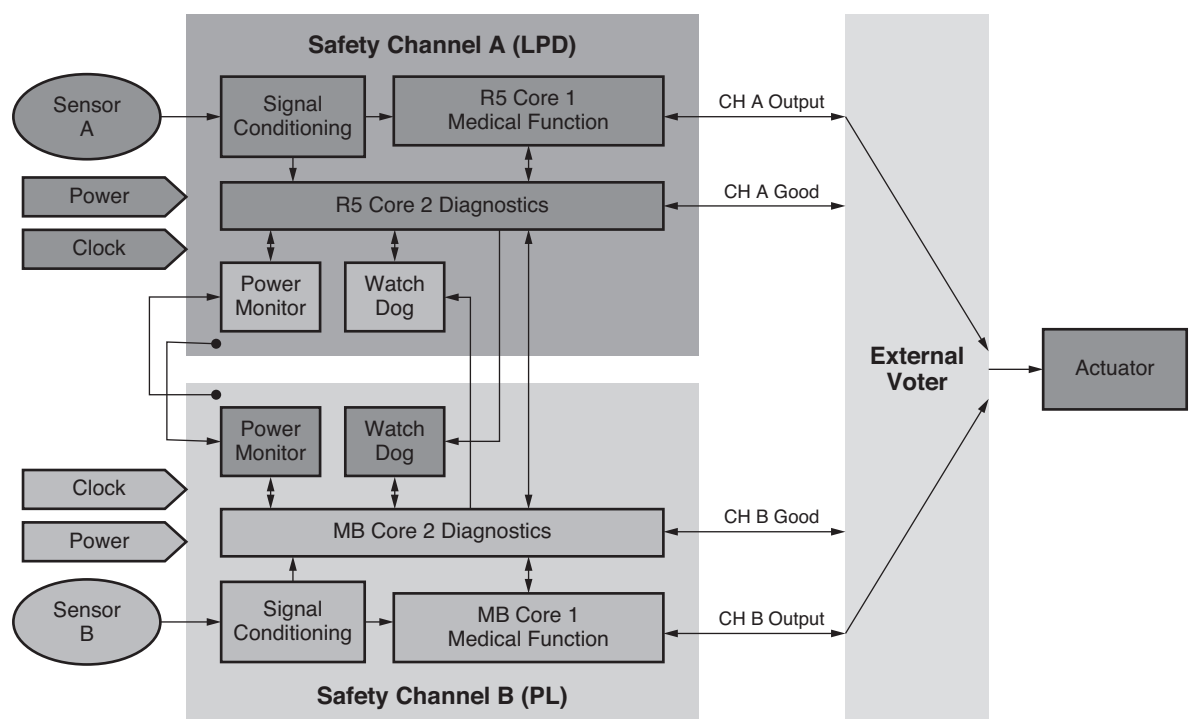
図 6: 2oo3 (Two out of Three) 安全アーキテクチャ

## 応用例

図 7 に示す例では、1oo2 の安全アーキテクチャに診断機能を追加して「1oo2D (One out of Two Diagnostics)」アーキテクチャを構成し、2つのチャンネルのどちらが故障したかを判定できるようにしています。このアーキテクチャは、2oo3 アーキテクチャの代わりに使用できます。

この例では、濃いグレーで示した安全チャンネル A と薄いグレーで示した安全チャンネル B の 2 つの安全チャンネルがあります。各チャンネルにはそれぞれ専用の電源とクロック ソースがあります。Zynq UltraScale+ デバイスは、電源モニターとウォッチドッグ タイマーを監視対象とは別のドメインに置いて動作させることができます。標準規格の認証に適合するには、これらのモニターが必要です。また、各チャンネルの診断率は 98% を超えており、使用する CPU とデザイン アーキテクチャもチャンネルごとに変えてあるため、多様性が確保されています。このように、1つの環境に異なるアーキテクチャを混在させることで、システムの能力が向上します。

アーキテクチャ全体で見ると、両方のチャンネルの結果を比較することにより、99% 以上の診断確率で単一障害 (1 個の電源またはクロック ジェネレーター の損失やメモリ故障など) が検出されます。障害が検出されると、チャンネルベースの診断機能がもう一方のチャンネルと多数決回路に故障を報告します。すると、多数決回路は故障していない方のチャンネルの結果に従います。



WP511\_07\_30519

図 7: 1oo2 アーキテクチャにチャンネル間の診断機能を追加した 1oo2D の例

## IEC 60601

IEC 60601 規格は、危害を与える可能性のある有害なエミッションについて説明していますが、安全ループの品質 (SIL) および危害を与える側の機器を安全状態に移行させる能力を記述する体系的な方法についてはほとんど論じていません。このリスク管理プロセスは各医療機器メーカーに任されており、ISO 14971 規格に基づく文書化により正当性が証明されます。これは手始めとしてはよい方法ですが、問題も残ります。つまり、リスク軽減に使用する安全ループにはどの程度の品質 (機能安全で定義された SIL1 ~ SIL4) が必要かという点です。

IEC 61508 規格は、安全ループの最終的な用途は問わず、すべての電気/電子/プログラマブル電子システムに適用されるガイダンスとプロセスを規定しています。このため、リスクを特定さえすれば、目的の標準 SIL レベルを満たすように設計された安全ループを使用して、必要なリスク軽減を達成できるといえます。

## ISO 26262

ISO 26262 仕様のアプローチは大きく異なり、機械自体が本質安全となるように設計します。たとえば、最近の自動車には電子サイドブレーキが搭載されるようになってきました。電子サイドブレーキは、通常の運転状態で自動車を停止するメインブレーキから完全に独立した従来の機械式サイドブレーキを置き換えるものです。最近の電子式サイドブレーキ（パーキングブレーキ）は、安全でない速度での走行中はシステムが作動しないような安全機能を内蔵しています。速度が安全速度上限の 8km/h (5mph) を超えている場合、システムは警告を発するだけで、作動しません。その理由は、次のとおりです。

1. メインブレーキシステムは油圧回路を冗長化している。
2. 油圧システムを駆動するアクチュエーターの故障率が非常に低い。

これらが完全に故障する確率は歴史的に見ても非常に低いため、完全に冗長なサイドブレーキを廃止し、その代わりに安全機能を内蔵した電子パーキングブレーキを導入しようというのが目的です。

本来の意図した機能に基づいてハザードを調査し、安全目標を決定します。次に、さまざまな診断対策や故障モード（フェイルセーフかフェイルオペレーショナル）を使用して各安全目標を実装し、アーキテクチャを決定します。このようにして、主機能が本質安全となるように設計していきます。

パーキングブレーキの安全目標は次のとおりです。

1. 意図せずシステムが作動するようなことがないこと。
2. 主電源を完全に喪失してもシステムが動作すること。
3. システムが制御不能な状態を引き起こすような動作をしないこと。

最後に、これらの安全目標を達成するようにデザインを作成し、安全目標が確実に達成されるように方法と対策を発行します。

## サイバーセキュリティ

サイバーセキュリティとは、デジタルハードウェアまたはソフトウェアを使用する機器全般で生じる多くの懸念とリスクを包含した広義の用語です。機器メーカーおよびサイバーセキュリティ専門家は、通常これらの懸念を次の 2 つのカテゴリに分けて考えます。

1. **オペレーショナルセキュリティ**: システムの動作が攻撃を受けないように保護しながら、機器が定義された動作条件の範囲内で本来の動作を維持できるようにします。
2. **デバイスおよびソフトウェアのクローニング**: デバイスの位置的所有権、およびデバイス内部の独自 IP を保護すると同時に、正規製品と外観が同じで機能が不完全なクローン デバイスの作成を防ぐ必要があります。この結果、IP の盗難、クローン デバイスの流通、およびクローン デバイスを組み込んだシステムの故障などによる金銭的な損失を防ぐことができます。

システムをネットワークに接続しなければ、サイバー脅威を受けないという誤解があります。これがなぜ誤解かという、ネットワークにまったく接続していないシステムというのはきわめてまれであるためです。電子医療機器を含め、ほとんどの電子機器はシステム全体の効率を高めるために何らかの接続を利用します。医療機器の場合、画像診断装置を院内ネットワークに接続して放射線技師と画像を共有することがあります。また、1 人の看護師が複数の患者を同時にモニターするために、生体情報モニターを院内 Wi-Fi 経由でナースステーションに接続することもあります。こうした意図しない接続を突破口として攻撃者が不正にアクセスし、より重要な、保護の弱い機器への侵入を成功させてしまうことがあります。

完全にネットワークから遮断されたシステムであっても、有名な Stuxnet ワームのように物理インターフェイス（Stuxnet の場合は USB フラッシュドライブ）から不正なコードを侵入させ、最終的に装置や運転をダウンさせてしまう攻撃が可能なことが知られています。このように、攻撃者はシステムの中で「最も弱い鎖の輪」を標的に攻撃を仕掛けてくるため、サイバーセキュリティおよびデバイスに対する脅威はシステム レベルで解析する必要があります。

サイバーセキュリティの脅威からデバイスを保護する手段として、いつまでも効果が長続きする万能な解決策は存在しません。脅威の種類、ハッカーの能力、そしてサイバー攻撃に対抗するためのテクノロジーは、いずれも刻々と変化しています。ハッカーからの執拗な攻撃を完全に防ぐ機器を開発することは、事実上ほぼ不可能です。また、現時点で考えられるサイバー攻撃への対策をすべて実装するのも、コストがかかりすぎます。したがって、機器を開発する際にはサイバー脅威のリスクを適切に管理し、最終デザインにどの対策を優先的に盛り込むかを決定することが重要となります。

## セキュリティ規格

産業分野で使用される製品には、個々の製品に必要なサイバーセキュリティ対策を分析するための共通の「性能指数」が長く待ち望まれていました。このような性能指数があると、製品が共通の定義に基づくセキュリティレベルを満たしていることを独立系機関で認証できるようになります。こうした目的で発表されたのが、マルチパート規格の IEC 62443 です。IEC 62443 では、システムが直面すると予測されるサイバーセキュリティ脅威に基づいて 5 つのセキュリティ保証レベル (SL) を定義し、各 SL のシステムに含めるべき対策も規定しています。表 2 に、IEC 62443 による各 SL の定義を示します。

- **システムの特定:** ネットワークに接続された場合と接続されていない場合で機器が検出/特定可能かどうか
- **リソース:** 攻撃者が利用可能なリソース (時間、資金など) の量
- **スキル:** サイバー攻撃を仕掛けようとする人物に必要な全体的なスキルレベル
- **動機:** サイバー攻撃を成功させようとする動機のレベル

表 2: IEC 62443 の SL の定義

セキュリティレベル	システムの特定	リソース	スキル	動機
0	保護なし	-	-	-
1	カジュアル	なし	なし	なし
2	単純な手段	低	一般的	低
3	複雑な手段	中	システム固有	中
4	複雑な手段	拡張	システム固有	高

各セキュリティレベルについて簡単に説明します。

- **SL0:** サイバー脅威に対する意図的な保護を持たない製品
- **SL1:** カジュアルハッカーや「スクリプトキディ」による攻撃からの保護
- **SL2:** それほど高度でないハッカーによる攻撃からの保護
- **SL3:** 十分なリソースを持った高度なハッカーによる長期的な攻撃からの保護
- **SL4:** 重要インフラや同様の資産に対する国家レベルの攻撃に対する保護

現在、いくつかの機関が IEC 62443 規格の認証を実施しています。認証は個々の SL ごとに可能で、UL、TUV、Exida の各社が実施しています。

## オペレーショナルセキュリティ

医療機器のオペレーショナルセキュリティを保護するには、セキュリティの 3 要素 (CIA)、すなわち機密性、完全性、可用性のうち、どの要素を優先するかを考慮する必要があります。そしてその結果をふまえ、システムレベルのリスクをどのように管理するかを決定し、システムの機能安全設計について検討する必要があります。IT (Information Technology) 機器と OT (Operational Technology) 機器では、サイバー攻撃に対する対処の方法が異なります。

人工呼吸器などの能動的な生命維持装置では、OT システムとしての全体的な動作の可用性が最優先されます。したがって、人工呼吸器の場合はデータ機密性が侵害されるような攻撃をシステムが受けても、患者の呼吸機能を補助するというシステムレベルの目標を損なうことなくシステムのサービスを停止できる機会が訪れるまで、システムの動作を継続できるように設計しておく必要があります。これとは対照的に、IT システムを保護する場合は、攻撃を検出した時点で直ちにシステムを無効化して被害の軽減を図るのが一般的です。

## デバイスおよびソフトウェアのクローニング

デバイスを販売する際は、ハードウェアとエンベデッドソフトウェアを悪意のある第三者による複製や改ざんから保護する方法を設計時に検討しておく必要があります。このサイバーセキュリティ保護は、アルゴリズムなど製品差別化のためのソフトウェア投資を保護するだけでなく、機能が不完全なクローン製品が市場に出回って製品のブランド価値が損なわれるのを防止する上で重要な役割を果たします。悪意のある第三者が、正規製品と外観が同じクローンデバイスを作成し、フィールドエンジニアが気付かずに最終システムに組み込んだ場合、そのデバイスをゲートウェイとしてより高度なシステム攻撃が仕掛けられる可能性があります。

## デバイスのセキュリティ設計手法

どのようなデバイスであれ、セキュリティ設計に万能のソリューションなど存在しないことを理解しておくことが重要です。IEC 62443 で説明されているように、設計者は製品が受ける可能性のある攻撃を想定し、予算の範囲内で最も重要なセキュリティ機能から優先的に製品に実装する必要があります。製品ライフサイクルの間には、新しいセキュリティ脅威やテクノロジーが登場することが考えられるため、定期的なアップデートを前提とした多層的な保護を目指したセキュリティアプローチをとる必要があります。このようなアプローチをとらない場合、図 8 に示すようにシステムの全体的なセキュリティ強度が時間と共に低下するリスクがあります。

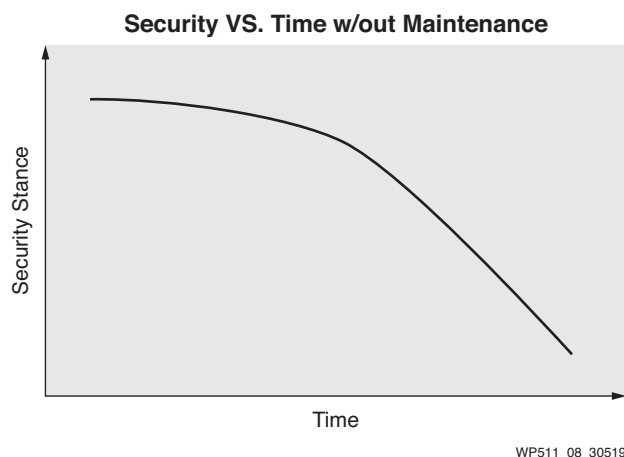


図 8: 時間の経過とシステムのセキュリティ強度

サイバーセキュリティの専門家は、「多層防御」アプローチによるシステム保護を推奨しています。多層防御とは、何種類ものテクノロジーを多重的に組み合わせることにより、異なる種類の攻撃を防御しようというアプローチです。たとえば、玄関にしか鍵をかけていない家の場合、鍵のかかっていない窓や裏口に回れば簡単に侵入できます。多層防御とは、「システム全体」を保護することを意味します。たとえ第三者にシステムの一部へのアクセスを許しても、それが隔離されたアクセスであれば、プラットフォーム全体の動作が乗っ取られることはありません。

セキュアなランタイム環境を維持する上で、多くのセキュリティ専門家が「トラストチェーン(信頼の鎖)」を維持することの重要性に言及しています(Ukil, Sen, Koilakonda, 2011年)。トラストチェーンとは、ハードウェアベースのセキュリティデバイスを「信頼のルート」(起点)として、その信頼を維持しながらデバイスの動作およびソフトウェアの各ステージのハンドオフを実行しようという考え方です。ソフトウェアは本質的に可変であるため、この信頼のルートはハードウェアをベースにすることが推奨されます。ハードウェアがソフトウェアリセットを解放したら、セキュアブートなどの方法によって、信頼できることがわかっているソフトウェアのみをブートし、デジタル署名された認可済みアプリケーションのみを実行するようにします。

図 9 に、トラスト チェーン の概念を示します。

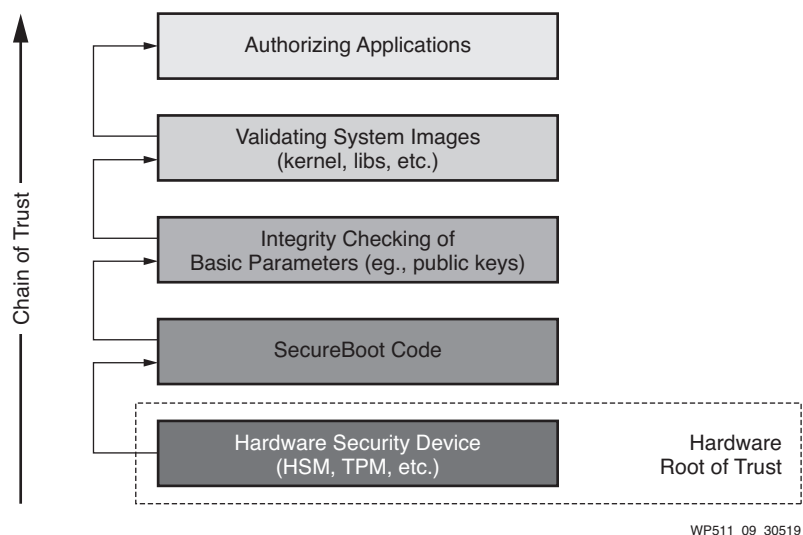


図 9: トラスト チェーン (Ukil, Sen, Koilakonda, 2011 年)

現在のデジタル システムには、製品のライフサイクル全体を通じてアップデートできる仕組みも必要です。これは、サイバー攻撃が巧妙化の一途をたどっており、現在システムを保護しているテクノロジーが今後も通用するとは限らないためです。運用中のシステムに新しい脆弱性が見つかり、ゼロデイ攻撃を受ける可能性も現実存在します。このため、攻撃を受けたシステムを検出する機能、重要な機器の動作の耐性、および攻撃を受けた機器を修復するセキュアアップデート メカニズムが必要となります。図 10 に、デバイスのセキュリティ ライフサイクルの模式図を示します。

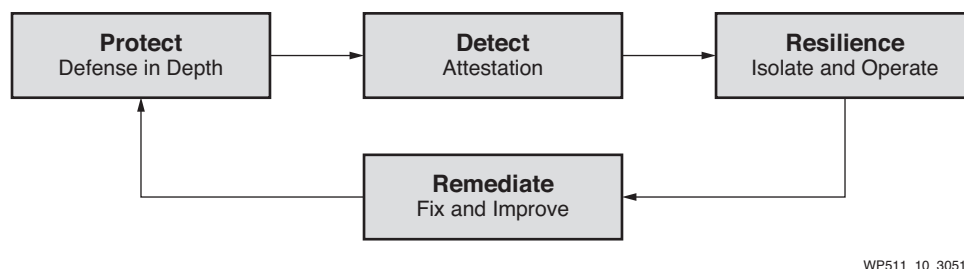


図 10: サイバーセキュリティ ライフサイクル設計

## データ プライバシーと情報保護

医療機器を設計する際は、米国の HIPAA 法 (医療保険の携行性と責任に関する法律) や EU の GDPR (一般データ保護規則) などの法律に従い、機器を通過するデータや機器に保存するデータを保護する必要があります。このような電子医療機器には、患者の特定につながるすべてのデータを保護できるようにセキュリティ メカニズムを実装する必要があります。GDPR は現在、侵入検知方法 (図 10 の「Detect」フェーズ) やシステムに対する定期的なペネトレーション テストなど、具体的なセキュリティ要件の定義を開始しており、これらのベスト プラクティスは IEC 62443 にも記載されています。

データ機密性を維持するには、プラットフォームは移動中のデータと保存データの両方に対して暗号手法を利用して認証と暗号化を実行します。暗号化アルゴリズムにはさまざまな種類がありますが、業界で最も広く使用されているのは AES と RSA です。いずれのアルゴリズムもビット数の大きい鍵を使用できるため、暗号のクラッキングは非常に困難です。ただし鍵長が大きいほど高い処理性能が必要となるため、実装にはトレードオフがあります。暗号鍵の長さは、機器がフィールドで運用される期間、およびその期間に予測されるコンピューターの演算性能の向上に基づいて NIST などいくつかの機関が推奨事項を出しており、IEC 62443 などの規格でその推奨鍵長が引用されています。

# ザイリンクスのテクノロジー

ザイリンクス Zynq UltraScale+ MPSoC のアーキテクチャには、機能安全とセキュリティを考慮した重要なテクノロジーが導入されており、これらを使用することで、デバイス開発者は安全で効果的な医療機器の実装を可能にする強力なソリューションを構築できます。また、安全およびセキュリティ向けシリコン機能を補完するツールフロー、IP、およびソフトウェアソリューションもインダストリアル/ヘルスケア IoT ソリューション スタックの一部として提供されています。

これらのテクノロジーの中には、機能安全とセキュリティのいずれかに特化したものもあれば、両方を兼ね備えたものもあります。

Zynq UltraScale+ MPSoC の機能安全向けテクノロジーには、次のものがあります。

- **3つの独立したコンピューティングドメイン:** クロックと電源をドメインごとに分離することで、共通要因故障を軽減
- **複数の温度センサー:** 動作境界条件を検出
- **オンチップ診断 (ECC):** ユーザーおよびコンフィギュレーション RAM のランダム ハードウェア故障を検出
- **リアルタイム コンピューティングドメインの決定論的能力**
- **安全規格認証済みのツールおよびメソッド**
- **安全規格認証済みの Zynq UltraScale+ MPSoC シリコンおよびソフトウェア**

Zynq UltraScale+ MPSoC のサイバーセキュリティ向けテクノロジーには、次のものがあります。

- **ハードウェア デバイス セキュリティ:** 不変のデバイス ID、保護されたデータストア、および強力な耐タンパー機能
- **セキュアブート:** 信頼されたファームウェアおよびソフトウェアのみをシステム上でブート
- **暗号アクセラレータ:** 動作時の通信、およびアプリケーションのデジタル署名検証に AES および RSA オフロード エンジンを使用
- **システム モニター:** システムの変更を監視し、メジャーブートをサポート
- **セキュアストレージ:** eFuse ベースの内部ストレージに鍵を格納
- **Arm® TrustZone**
- **デバイスの真正性保護:** 一意のパッケージマーキング
- **ハードウェア デバイス セキュリティ:** セキュリティ モニター、DPA 保護
- **一意のデバイス ID:** 保護された一意の ID をハードウェアに内蔵
- **カスタマーキーの保護:** eFuse およびサプライチェーンメカニズムを使用してカスタマーキーを内部ストレージに格納
- **トレーサビリティ:** 偽造防止策により、サプライチェーンを検証

Zynq UltraScale+ MPSoC の機能安全およびセキュリティ向けテクノロジーには、次のものがあります。

- **アイソレーションテクノロジー:** データパスの分離、およびハードウェア障害の分離
- **ヘテロジニアスハードウェア設計:** システムティック故障を軽減し、単一のバグが動作に影響する可能性を低減

## ザイリンクスの機能安全テクノロジー

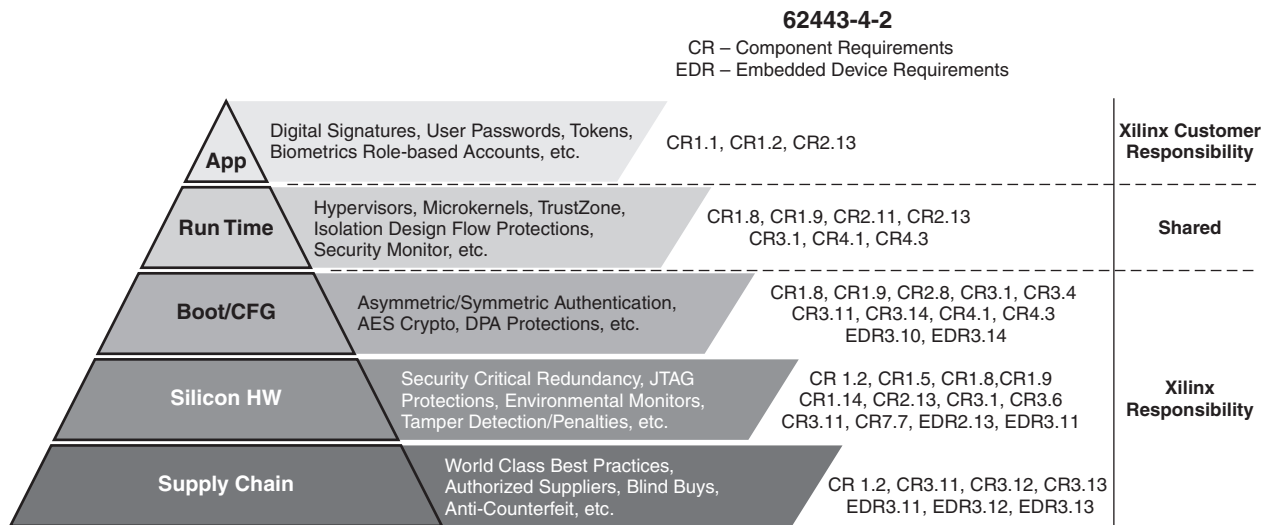
ザイリンクスの機能安全テクノロジーは、機能安全設計の2つの重要な面に対処します。1つは決定論的能力で、これにはザイリンクスの認証済みツールチェーンおよび評価済みのヘテロジニアス製品で対処します。もう1つはランダムハードウェア障害のフォールトトレランスで、これにはコンピューティングドメイン内の選択的ハードウェア冗長化、SRAM診断機能、ヘテロジニアスコンピューティングリソース間の冗長化などの診断機能を組み合わせて対処します。

オンチップの診断機能に加え、ザイリンクスはデザイン固有および製造に関する独自の技術を導入することにより、デバイスレベルでのシングルイベントアップセット (SEU) 耐性も強化しています。

# ザイリンクスのサイバーセキュリティ テクノロジ

ザイリンクスが提供するクラス最高のサイバーセキュリティ プラットフォーム テクノロジは、サイバーセキュリティ に対する要求が非常に厳しい防衛産業で広く採用されています。これら防衛産業の要求事項を満たしたザイリンクスのランタイムおよびサプライチェーンセキュリティ テクノロジは、いずれも業界をリードしています。これらの本質的なセキュリティ機能は、医療産業にもメリットをもたらします。

ザイリンクスは、強力なセキュリティ保護の層を1つずつ積み重ねた「セキュリティピラミッド」を構想しています(図 11)。最も下層にあるのはサプライチェーンの保護で、純正以外のデバイスが正規チャネルを流通したり、カスタマー デバイスの構築に使用されたりするのを防いでいます。次に、悪用されることの多い JTAG などのデバッグ インターフェイスに対する保護、デバイス改ざんの検出、およびペナルティの執行などをシリコン レベルで組み込んでいます。ブート/コンフィギュレーションの層には、ブート時の認証や暗号化機能、およびダイナミック消費電力解析 (DPA) の保護機能を組み込んでおり、ブート時の攻撃によってデバイスに不正侵入されたり、機密情報が漏洩したりするのを防いでいます。これらセキュリティ機能のほとんどはザイリンクス プラットフォームによって自動的に提供されますが、一部はプラットフォーム上で動作するユーザー アプリケーションのコンフィギュレーションによって有効にする必要があります。



WP511\_11\_31919

図 11: ザイリンクスのセキュリティピラミッド

Zynq UltraScale+ MPSoC には、実行時アプリケーションのセキュリティアイソレーションの機能として、Arm TrustZone、ハイパーバイザー、ザイリンクス アイソレーション デザイン フロー (IDF) などいくつかのオプションがあります。また、ザイリンクス プラットフォーム セキュリティ モニター (SecMon) や実行時にソフトウェアの完全性を監視する FPGA ベースのソフトウェア アプライアンスなど、オプションのランタイム モニター機能もあります。また、プラットフォームのブート初期段階を保護するのに使用される AES および RSA ハードウェア アクセラレータなどの暗号化ハードウェアを、システム起動後にユーザー空間から利用することもできます。これらのハードウェア オフロード機能を使用すると、AES 暗号化が最大 53 倍、RSA 暗号化が最大 9 倍に高速化し、暗号処理を必要とするアプリケーションに大きなメリットがあります。

これらのセキュリティ機能と IEC 62443 の要求事項には、対応関係があります。図 11 には、ザイリンクスのセキュリティ機能の横に、それぞれに対応する IEC 62443 規格を示しています。サイバーセキュリティに関するこれらの要求事項は、医療機器の保護にも同様に適用されます。事実、FDA の認知規格でも IEC 62443 が引用されています。

## まとめ

医療機器の開発に関しては、さまざまな監督機関や設計手法がリスク管理について説明しています。このホワイト ペーパーでは、機能安全とサイバーセキュリティに関連して、特に機器メーカーによる製品リスクの評価と管理について説明しました。医療機器を設計する際は、製品の安全 (IEC 61508 など) およびサイバーセキュリティ保護 (IEC 62443 など) に関して産業分野で採用されているリスク対策のベスト プラクティスを取り入れることが求められます。

このホワイト ペーパーでは、機能安全の設計手法およびザイリンクスの機能を医療機器の設計に応用することで安全の向上、リスク評価の改善、開発期間の短縮が実現し、1 回で認証の取得に成功するほか、製品リコールの可能性も減らせることについて説明しました。監督機関および設計エンジニア双方の立場から、この構造化された機能安全設計プロセスは全体的な製品設計、製品のトータル コスト、そして最終的には患者の安全に好影響をもたらすことが見てとれるものとザイリンクスは考えています。適切なサイバーセキュリティ保護を講じなければ、システムの安全エレメントが攻撃を受けて本来の動作ができなくなる可能性があるため、安全とセキュリティは別々に論じることはできません。サイバーセキュリティに関しては、動作の完全性およびデジタル制御製品のサプライ チェーン保護について説明しました。このサイバーセキュリティに関するトピックは、すべての業界に当てはまります。

また、このホワイト ペーパーではすべてのデジタル製品に含めるべきザイリンクスのテクノロジーおよびセキュリティ ライフ サイクルの留意事項、さらにはザイリンクス SoC が提供するハードウェア ベースの堅牢な信頼のルートを使用することでセキュアな医療機器を構築できることについても説明しました。ザイリンクスの SoC プラットフォームは、1 つのデバイスに安全機能と冗長機能を柔軟に実装できます。セキュリティと機能安全の機能を 1 つの SoC に統合したこのソリューションにより、設計期間と製品コストの大幅な削減が可能になります。

ザイリンクスのテクノロジーを使用して機能安全とサイバーセキュリティの設計要件に対処するための設計ガイドなど、具体的なトピックについて詳しく解説したザイリンクスの資料は、「[関連資料](#)」のセクションで紹介しています。

## 関連資料

次に、本稿で取り上げた各トピックについての関連資料を示します。

注記: 日本語版のバージョンは、英語版より古い場合があります。

### 機能安全

ザイリンクスの機能安全ウェブサイト: <https://japan.xilinx.com/products/technology/functional-safety.html>

ザイリンクス Functional Safety Working Group: <https://japan.xilinx.com/products/technology/functional-safety.html#functionalSafety>

ザイリンクス ホワイト ペーパー 『IEC 61508 に従った Zynq-7000 SoC デザインで ISO 13849 準拠を実現』(WP495: [英語版](#)、[日本語版](#))

ザイリンクス ホワイト ペーパー 『IEC61508 および ISO26262 に準拠した安全アプリケーションのリスク軽減と効率向上』([WP461](#))

ザイリンクス ホワイト ペーパー 『フォールト トレラント システム開発用のアイソレーション デザイン フロー』([WP412](#))

### サイバーセキュリティ

ザイリンクスのデザイン セキュリティ ウェブサイト: <https://japan.xilinx.com/products/technology/design-security.html>

ザイリンクス セキュリティ ワーキング グループ: <https://japan.xilinx.com/products/technology/design-security.html#workingGroup>

ザイリンクス ホワイト ペーパー 『Zynq-7000 SoC 向け FIPS 140-2 入門』([WP467](#))

ザイリンクス ホワイト ペーパー 『Zynq-7000 All Programmable SoC を使用したアプリケーションのセキュリティを強化する非対称認証』([WP468](#))

ザイリンクス ホワイト ペーパー 『Zynq-7000 SoC における TrustZone テクノロジーのサポート』([WP429](#))

ザイリンクス ホワイト ペーパー 『インテリジェント IIoT エッジプラットフォームの重要な特性』(WP493: [英語版](#)、[日本語版](#))

ザイリンクス アプリケーション ノート 『Zynq UltraScale+ デバイスでの不正操作防止デザインの開発』(XAPP1323: [英語版](#)、[日本語版](#))

ザイリンクス アプリケーション ノート 『暗号化と認証を使用して UltraScale/UltraScale+ FPGA のビットストリームを保護』(XAPP1267: [英語版](#)、[日本語版](#))

ザイリンクス アプリケーション ノート 『Zynq-7000 SoC のセキュアブート』(XAPP1175: [英語版](#)、[日本語版](#))

## 改訂履歴

次の表に、この文書の改訂履歴を示します。

日付	バージョン	内容
2019年7月1日	1.0	誤植修正。
2019年4月15日	1.0	初版

## 免責事項

本通知に基づいて貴殿または貴社(本通知の被通知者が個人の場合には「貴殿」、法人その他の団体の場合には「貴社」。以下同じ)に開示される情報(以下「本情報」といいます)は、ザイリンクスの製品を選択および使用することのためにのみ提供されます。適用される法律が許容する最大限の範囲で、(1)本情報は「現状有姿」、およびすべて受領者の責任で(with all faults)という状態で提供され、ザイリンクスは、本通知をもって、明示、黙示、法定を問わず(商品性、非侵害、特定目的適合性の保証を含みますがこれらに限られません)、すべての保証および条件を負わない(否認する)ものとします。また、(2)ザイリンクスは、本情報(貴殿または貴社による本情報の使用を含む)に関係し、起因し、関連する、いかなる種類・性質の損失または損害についても、責任を負わない(契約上、不法行為上(過失の場合を含む)、その他のいかなる責任の法理によるかを問わない)ものとし、当該損失または損害には、直接、間接、特別、付随的、結果的な損失または損害(第三者が起した行為の結果被った、データ、利益、業務上の信用の損失、その他あらゆる種類の損失や損害を含みます)が含まれるものとし、それは、たとえ当該損害や損失が合理的に予見可能であったり、ザイリンクスがそれらの可能性について助言を受けていた場合であったとしても同様です。ザイリンクスは、本情報に含まれるいかなる誤りも訂正する義務を負わず、本情報または製品仕様のアップデートを貴殿または貴社に知らせる義務も負いません。事前の書面による同意のない限り、貴殿または貴社は本情報を再生産、変更、頒布、または公に展示してはなりません。一定の製品は、ザイリンクスの限定的保証の諸条件に従うこととなるので、<https://japan.xilinx.com/legal.htm#tos>で見られるザイリンクスの販売条件を参照してください。IP コアは、ザイリンクスが貴殿または貴社に付与したライセンスに含まれる保証と補助的条件に従うこととなります。ザイリンクスの製品は、フェイルセーフとして、または、フェイルセーフの動作を要求するアプリケーションに使用するために、設計されたり意図されたりしていません。そのような重大なアプリケーションにザイリンクスの製品を使用する場合のリスクと責任は、貴殿または貴社が単独で負うものです。<https://japan.xilinx.com/legal.htm#tos>で見られるザイリンクスの販売条件を参照してください。

## 自動車用のアプリケーションの免責条項

オートモーティブ製品(製品番号に「XA」が含まれる)は、ISO 26262 自動車用機能安全規格に従った安全コンセプトまたは余剰性の機能(「セーフティ設計」)がない限り、エアバッグの展開における使用または車両の制御に影響するアプリケーション(「セーフティアプリケーション」)における使用は保証されていません。顧客は、製品を組み込むすべてのシステムについて、その使用前または提供前に安全を目的として十分なテストを行うものとします。セーフティ設計なしにセーフティアプリケーションで製品を使用するリスクはすべて顧客が負い、製品の責任の制限を規定する適用法令および規則にのみ従うものとします。

この資料に関するフィードバックおよびリンクなどの問題につきましては、[jpn\\_trans\\_feedback@xilinx.com](mailto:jpn_trans_feedback@xilinx.com) まで、または各ページの右下にある[フィードバック送信] ボタンをクリックすると表示されるフォームからお知らせください。いただきましたご意見を参考に早急に対応させていただきます。なお、このメールアドレスへのお問い合わせは受け付けておりません。あらかじめご了承ください。