



WP461 (v1.0) 2015 年 4 月 9 日

IEC61508 および ISO26262 に準拠した セーフティアプリケーションのための リスク低減と効率性向上

著者: Ed Hallett, Giulio Corradi, Steven McNeil

ザイリンクス製品では、セーフティ機能とそれ以外の機能を 1 つのデバイスに統合できます。ザイリンクスが提供する現在クラス最高のツールと技術により、安全性に関する IEC/ISO 認定の取得が容易になります。

概要

このホワイトペーパーでは、ザイリンクス FPGA および SoC デバイスを使用してセーフティアプリケーション用のプログラマブルな電子機器を設計/開発する産業およびオートモーティブ分野の顧客向けに、ディペンダビリティの重要性について説明します。ここでは、主に IEC 61508/ISO 26262 規格を対象とした高集積、高性能なシステムでソリューションを作成する方法について説明しています。目標は、リスク軽減、コンプライアンス向上、認定取得時間の短縮、システム コスト削減を実現することです。

この資料の内容は次のとおりです。

- セーフティデザインの主なディペンダブル属性
- ザイリンクスのテクノロジーと設計手法を利用して、セーフティシステムのデザインに関する基本的な課題を解決する方法

ザイリンクスが過去 10 年にわたって入念に策定してきた定義、分割、および検証の各手順について詳しく説明します。実績あるツールやプロセスを採用することで、機能安全認証の取得につながるセーフティブロック デザインのエレメントを作成できます。

このホワイトペーパーでは、ザイリンクスが数十年にわたって定期的に公開してきた品質/信頼性データが、セーフティデザイン (FIT レートとアップセットの低減など) の定量化の基準となった経緯についても説明します。プログラマブルであるというザイリンクスデバイスの特性により、ディペンダビリティの目標/要件を満たすアーキテクチャや機能を構築できます。

ザイリンクスの開発ツールチェーンとアイソレーション デザイン フロー (IDF) 設計手法を用いると、チャネルの多様性と冗長性の実装、共通原因故障の削減、ランダム エラーの軽減といったメリットがデザインに活かされ、これまでになかったシステム セキュリティとディペンダビリティを実現できます。

はじめに

ビジネス上の背景

今日の経済環境において、メーカー各社は可能な限りコストを削減し、生産性を高めて価値を創出する必要に迫られています。過去数年にわたるむやみなコスト削減の結果、メキシコ湾での原油流出などの大規模な事故が発生し、企業とその顧客、利害関係者、従業員にさまざまな影響を及ぼしました。そのため、このような有害事象のリスクを低減する効果的な安全戦略が必須となりました。多くの調査から、安全上の事故の70%は人的要因(疲労、過積載、不注意、過信など)によって起きることがわかっています。よりインテリジェントなオートメーションに投資すれば、人的影響を減らし、安全上の意思決定を向上させ、望ましくない事象が起こる可能性を早期に検出し、ダウンタイムを減らし、生産性を高めることができます。よりインテリジェントで優れたオートメーションは、ディペンダビリティを高めます。

ディペンダビリティとは、正当に信頼できるサービスを提供する能力を意味します。一般消費者の日常生活における懸念事項としては、自動車の信頼性、水道システムの可用性と安全性、住宅の保守性、医療の安全性、日常生活の安全保障などがあります。これらは互いに影響し合うため、慎重に対処する必要があります。

ビジネス上の観点から見ると、製品メーカーが抱える懸念事項は次のようなことです。

- 製品の信頼性(保証期間中の返品を避けるため)
- エネルギーや資材の入手可能性(オペレーションを継続するため)
- 機械の保守性
- 工場や従業員の安全性
- 設備やIT インフラストラクチャのセキュリティ

これらの懸念事項には、慎重かつ一貫して対処する必要があります。

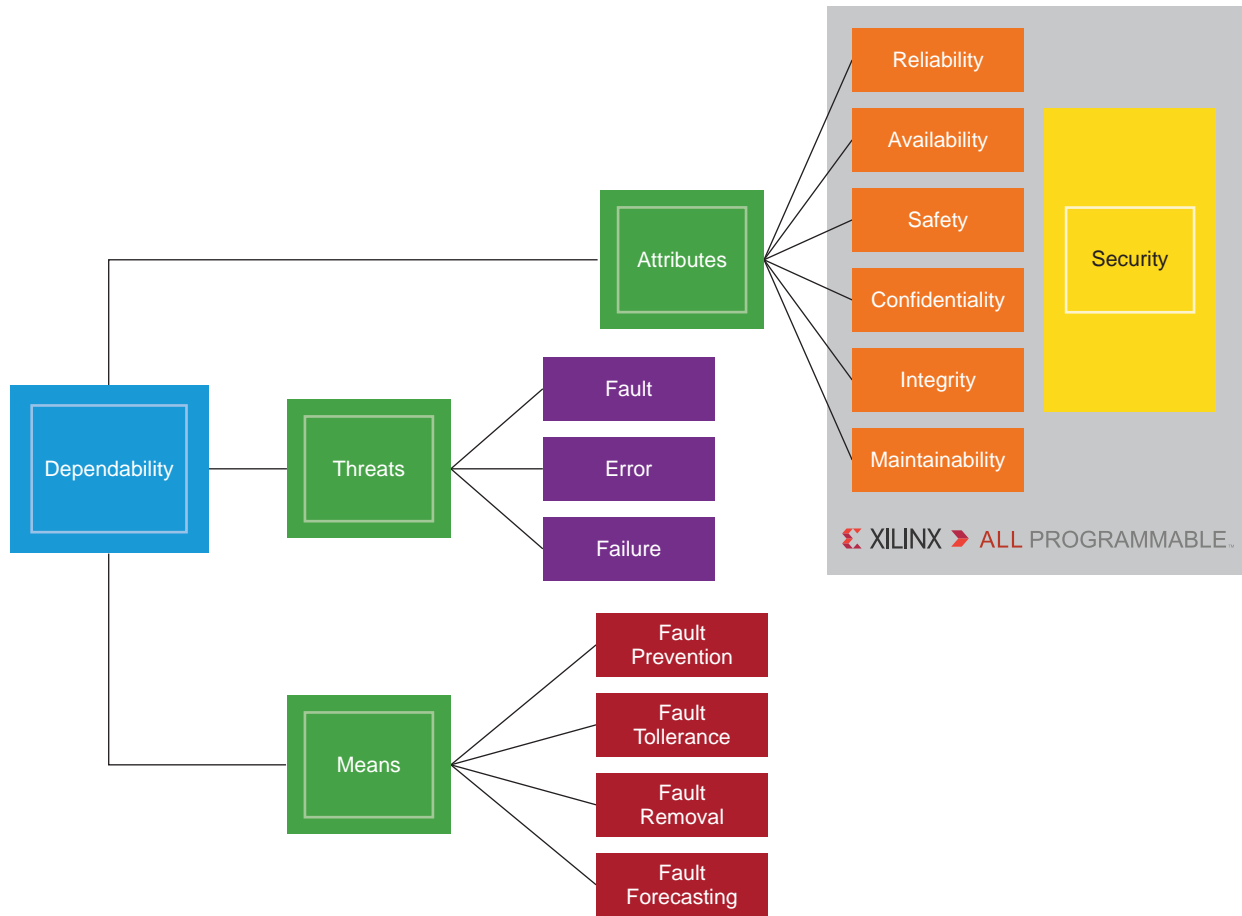
多くの事業経営者や管理者は、ディペンダビリティを向上および管理するテクノロジーとソリューションへの投資が必要と認識しています。高いディペンダビリティを実現および維持するには、安全性、セキュリティ、可用性を最優先にする必要があります。優秀な企業は、最新のディペンダビリティテクノロジーに投資することが重要であり、それによって複雑性と稼働中断を最小限に抑えながら関係規制や規格への準拠認定を取得できることを理解しています。

ただし、さらに重要なことは、機器の故障、オペレーターのミス、不適切なセキュリティ介入から起こり得る予想外のダウンタイムを避けるため、重大な問題を発生前に特定することです。予想外のダウンタイムが多額の経済損失につながることは明らかのため、信頼できるテクノロジーに投資することが賢明な選択です。企業の全体的な生産性とディペンダビリティを高めるには、資産のダウンタイムが発生する理由を、理解する必要があります。

システム上の課題

ザイリンクスは 15 年以上前に、ディペンダビリティが自社の顧客にとって重要な資産となることに気付き、ディペンダブルシステム的设计に役立つソリューションの提供に取り組んできました。ザイリンクスによるシステムのディペンダビリティ向上の取り組みは、信頼性、安全性、セキュリティ、保守性、高可用性のアーキテクチャに重点を置いています。また、規制機関によって認定されたプロセスやツールも、ディペンダブルシステム的设计に役立ちます。ザイリンクスの認定は、顧客によるシステムの具現化と認定取得にかかる時間を短縮するため、顧客に直ちにメリットをもたらします。

ザイリンクスの目的は、ディペンダブルシステムの保護に必要なツールや機能を提供することです。図 1 に、課題解決の属性、脅威、手段を示します。



WP461_01_110514

図 1: ディペンダビリティの属性、脅威、手段

ディペンダビリティは一連の属性から成り、各種脅威による影響を受けますが、これらの脅威はディペンダブルシステムを正しく管理する手段を講じることで低減できます。このホワイトペーパーでは、デザイン チームが共通認識を持って最終システム的设计にあたることできるように、最初にディペンダビリティの属性、脅威、手段について定義します。

ディペンダビリティの属性:

- 信頼性:
 - システム サービスがエラーなく継続すること、または
 - システムが所定のミッションを所定の時間内に完了できる可能性。
- 可用性: システムが所定の期間中に常に稼働していること。
- 保守性: システムにすばやくアクセスし、点検および修理できること。
- 安全性: ユーザーや環境に損傷を与える可能性のある、意図しないアクションや対応からシステムを適切に保護できること。
- セキュリティ: システム保護/防御に対する電子的な不法侵入によるデータの流出や損失を防止できること。
- インテグリティ: システムに不適切な変更が加えられないこと。
- 機密性: 情報の無断開示からシステムを効果的に保護できること。

ディペンダビリティの脅威:

- エラー: 計算/観測/測定された値と、真の/指定された/論理的に正しい値または条件に相違があること。ランダム エラーと系統的エラーがあります。基本的に、故障の原因となるシステム状態はすべてエラーになります。
- 障害: 機能ユニットが必要な機能を実行する能力を低下させる/失わせる可能性のある異常状態。障害は、システム故障の原因となります。
- 故障: システムや機能ユニットが必要な機能を実行する能力が停止すること (サブシステムの故障は、上位層のシステムの障害を引き起こす可能性がある)。

エラー、障害、故障を正しく回避または軽減して、望ましくない事態を最小限に抑えることで、ディペンダビリティ属性を満たす設計が実現します。ディペンダビリティに対する脅威を防ぐには、次の 4 つの手段を講じます。

- 障害防止: 障害の導入または発生を回避および防止する方法。
- フォールト トレランス: 障害が発生しても仕様を満たすサービスを提供する方法。
- 障害除去: 障害の数と重大度の両面で障害の存在を減らす方法。
- 障害予測: 障害の発生と結果を予測する方法。

デザイン エラーを回避する適切なプロセスを作成するには、製品のライフサイクル全体を通してこれらの属性とその手段を管理する、適切なツールを適用する必要があります。それにはまず、具体的な方法で脅威を定量化および定量化し、次に、適切なアーキテクチャと技術を用いて修正手段を製品自体に実装します。

機能安全

IEC 61508 および ISO 26262 は、機能的な安全装置の認定を統制している 2 大規格です。どちらの規格も、設計プロセス全体のセーフティ ライフサイクルについて具体的に定めています。製品認定を取得では、デザインの詳細、メーカーの安全管理システム、製品開発に携わる専門家の能力が評価されます。ザイリンクスの従業員は、セーフティプログラムに必要な IEC 61508 および ISO 26262 の必須研修を受けています。

- 機能安全は、安全性の下位区分です(図 2 を参照)。全体的な安全性のうち、アクティブ システム (温度測定、エネルギー源の供給停止など) や、設計したセーフティ機能に従って動作する機器に依存する部分を指します。
- 非機能安全とは、パッシブ システムに依存する手段 (導電部の絶縁など) によって実現される安全性を指します。

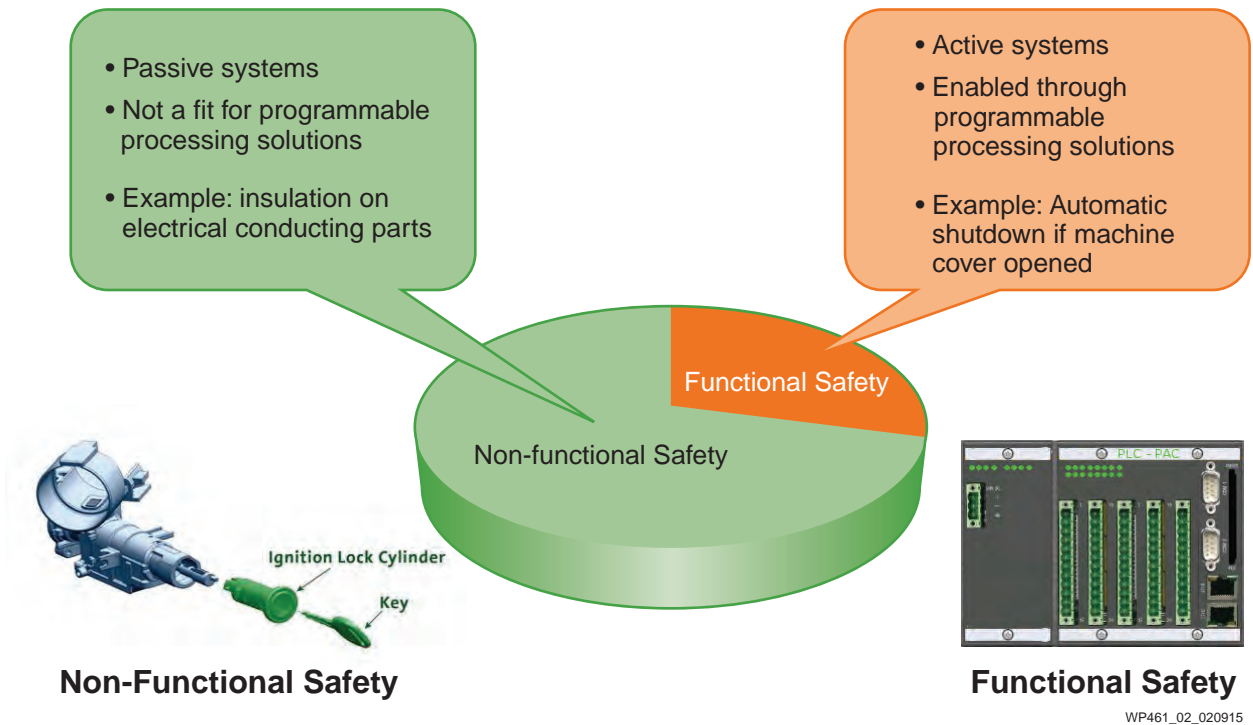


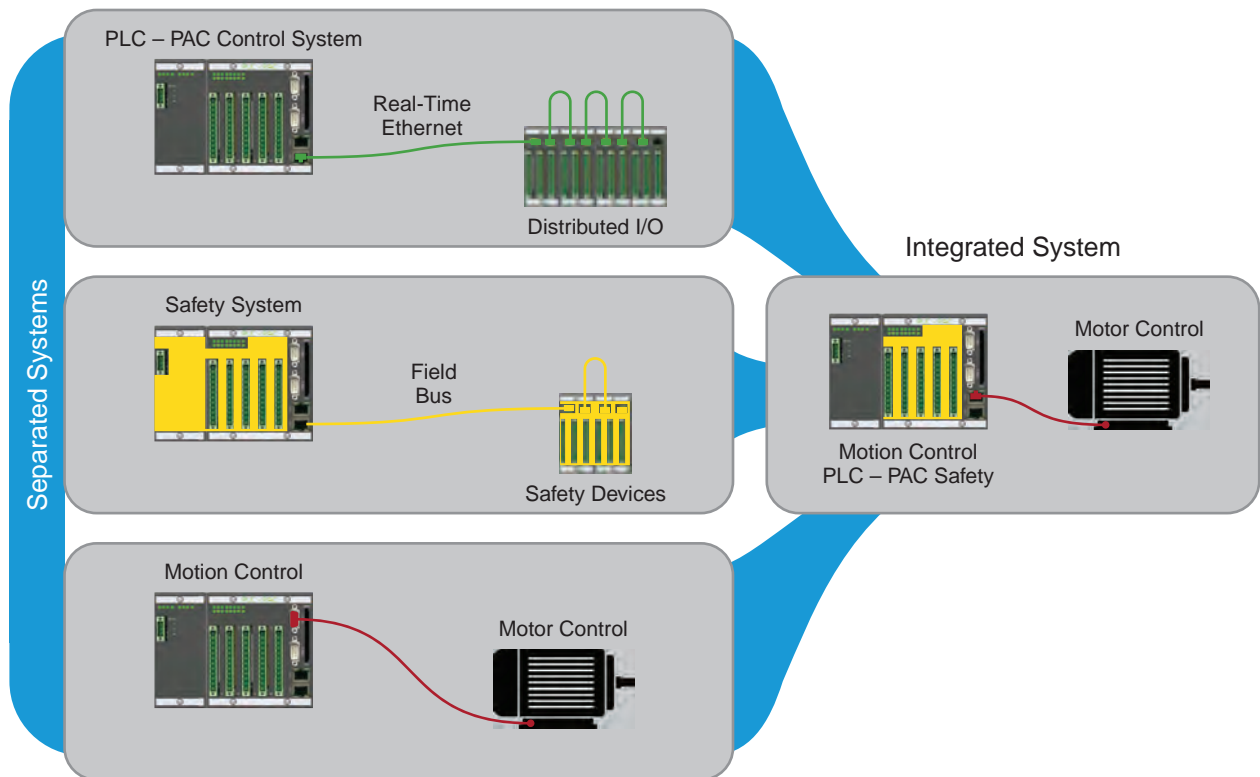
図 2: 全体的な安全性の下位区分としての機能安全

プログラマブルな電子安全機器開発の基本概念は、業界では次のように定義されています。

セーフティ システムが機能的に安全と言えるのは、ランダム故障/系統的故障/共通原因故障が発生しても、死亡や怪我、環境汚染、機器または生産上の損失を招くセーフティシステムの誤動作が起きない場合です。

産業アプリケーション分野

産業、オートモーティブ、アビオニクス、通信などの分野ではシステムの統合化が急速に進んでいます。図 3 に、一般的な産業オートメーション機器とその統合の傾向を示します。



WP461_03_112014

図 3: オートメーションシステムの統合

従来のオートメーションシステムは、ローカルまたは分散 I/O をアクティブ化するプロセスの順序付けを担うプログラマブルロジックコントローラー (PLC) などの機器を組み合わせて構成されます。モーションコントローラーは一連のモーターコントローラーの動きと軌道を制御し、一方、モーターコントローラーは自動部品を動かす電気モーターを駆動します。セーフティコントローラーは、セーフティ入力トランスデューサーとセーフティ出力アクチュエーターを用いてシステム全体を管理して、違反が発生した場合に制御対象プロセスを安全な状態に戻します。安全制御システムには、通信ネットワーク (リアルタイムイーサネットバスとフィールドバス) もあります (図 3 参照)。これらのセーフティシステムは、安全上のリスクや工場停止にもつながる違反を防止するため、セキュリティと機密性が求められます。

従来の構成はごく一般的で、後から考案されたものです。初期のシステムは、機能面のみを備えるように設計されていました (PAC + モーションコントローラー + モーターコントローラーなど)。その後、ほかの属性 (安全性、セキュリティ) が加わったためにシステムが複雑化し、ディペンダビリティの評価が非常に難しくなりました。このような複雑性はごく一部の専門家以外は理解できず、ときには専門家でさえ、起こり得るシステム動作を完全には理解できないことがあります。あらゆるタイプの複雑性が増すと、設計者は起こり得るシステム状態をすべて把握することが難しくなり、オペレーターはあらゆる正常状態と異常状態および障害状態を安全かつ効果的に処理することが難しくなります。実際に、一線級の専門家達は複雑性を「情報管理不可能性」と定義しています [参照 1]。

複雑性を軽減するための最新のアプローチは、小型化したシリコン形状の利点とマイクロエレクトロニクスの省スペース性を活かして、図 1 に示すデペンダブルな手段を組み込むことです。効果を高めるには、このアプローチにデザインプロセスと製品の耐用期間を含めて、関連するデペンダブル条件すべてに対応する必要があります。図 3 で、「統合システム (Integrated System)」の下に示された 3 つのシステムをすべてまとめたものが、この統合に該当します。

当然、この統合システムには、分離システムの諸機能を維持できるだけの十分なパフォーマンスが必要です。ソフトプロセッサ IP コアでプログラムされた FPGA (Zynq@-7000 デバイスなどの SoC が望ましい) はパフォーマンスが高いため、必要なディペンダビリティ属性を維持しながら、必要な機能を維持および拡張できます。

基本的に、分離した機能をシリコンに統合すると、デペンダブル機能が下位のシステム レベルで組み込まれるため、デカップルが向上します。そのため、結果論としてではなく問題の発生源でディペンダビリティを管理できます。このアプローチならば複雑性が低減するため、システムの管理不可能性も低減します。

従来のアーキテクチャは、このアプローチによって旧式化したわけではありません。統合型のディペンダビリティ管理ではリスクが低下し、診断機能が向上しますが、システム レベルでは依然として、適切なディペンダビリティアーキテクチャを実装する必要があります。たとえば、統合部分に影響を与える一般的な障害によってシステム全体が使用できなくなることが懸念される場合は、機器レベルでの二重化(冗長構成)が適切(または必須)になることが多々あります。

ザイリンクスでは、すべてのディペンダビリティ属性に対して認定手段を提供し、デザインを適切に調整可能にすることで、この統合に取り組んでいます。図 4 に、属性の調整をザイリンクスで実現することで、適切な割り当てを可能にする方法の例を示します。

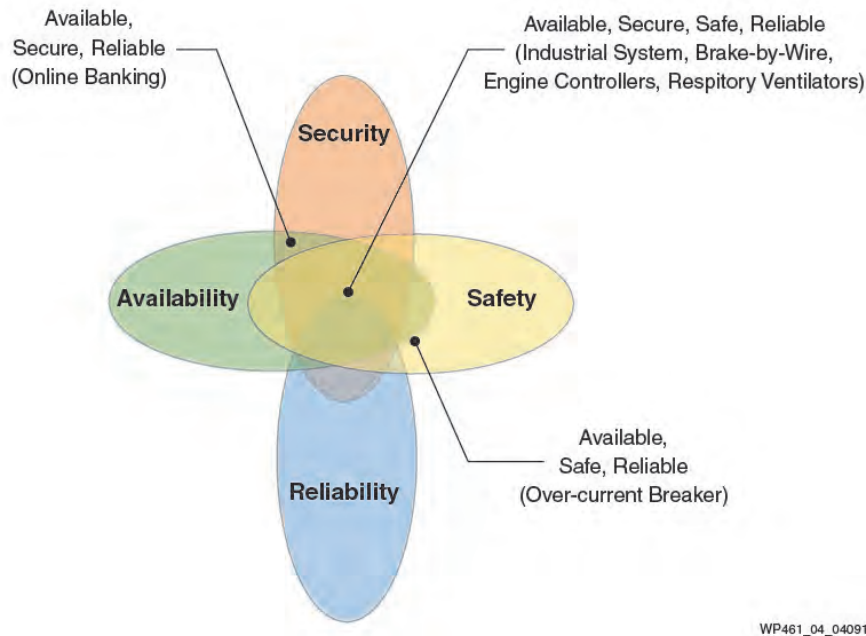


図 4: ディペンダビリティの調整

安全性に関係のない高信頼性、高可用性、高セキュリティのシステム (オンラインバンキング、証券取引所のリアルタイムデータ処理、ビジネスに不可欠なウェブサイトによく見られるシステムなど) でも、ザイリンクスのセキュリティソリューションと可用性パターンを活用できます。製造プロセスのターゲット (産業システム、エンジンコントローラー、人工呼吸器、ブレーキワイヤシステム、電源システムなど) は中央のセクションに該当し、高セキュリティ、高信頼性、高可用性で安全性重視のシステムと重なります (図 4)。図 4 の右下のセクションには、セキュリティに関係のない高安全性、高信頼性、高可用性のシステム (過電流遮断スイッチなど) が該当します。

相乗作用のあるデザインと機能

図 4 は、やや「奥深い」解釈をすることもできます。各属性は、ディペンダビリティ要件を満たすべく一連のレイヤー セットとして連携します。これはレイヤード アプローチとも呼ばれます。レイヤード アプローチは、必要な属性を特定および管理するのに役立ち、その方法は、各レイヤーが特定のディペンダビリティ属性に対応するというもので、属性の共通部分によってシステム全体の動作が決まります。

レイヤー化は、適切に実装すればかなりの効果を上げることができます。ただし、レイヤー化の適切な実装だけでは不十分です。たとえば、適切に実装されたセキュリティ属性の要件として、不正なパスワードが使われた場合は、システムへのアクセス ポータルをすべてロックする必要があるとします。このアクションは、バンキング アプリケーションでは非常に適切かつ妥当と言えますが、別の環境 (化学工場など) では非常に危険な可能性があります。

化学工場で、不正なパスワードに続いて非常に危険性の高いコマンドが使用された場合は、不測の事態 (工場の完全停止や爆発など) を回避するために直ちに人的介入が必要です。すべての入力ロックされると、必要な時間内に人的介入ができない可能性があります。

このためザイリンクスでは、すべてのディペンダビリティ属性を、総合的で相乗作用のある実装に組み込むことを推奨します。つまり、すべてのサブシステムがその他の各サブシステムのオペレーション方式を認識し、当該環境で予測どおりに安全に連携する必要があります。

ディペンダブル システムにおける相乗作用の重要性については、スイス チーズ モデルで説明します。

スイス チーズ モデル

前の化学工場の例のように、メキシコ湾原油流出/爆発事故 (2010 年)、スペースシャトル チャレンジャー 打上爆発事故 (1986 年)、スリーマイル島原発事故 (1979 年) などの有名な歴史的災害の多くは、スイス チーズ モデルですべて説明および分析できます。

認知心理学者 James T. Reason 氏の著書『Human Error』で初めて提唱されたスイス チーズ モデルは、複数の要因が重なって起きる、複雑なシステムが関係している事故の因果関係に焦点を置いています。個別に見れば、これらの要因が引き起こす問題は深刻ではありませんが、要因が重なると危険事象や大惨事にまで発展する可能性があります。

スイス チーズ モデルでは、故障に対する防御が一連の防壁としてモデル化され、それぞれが一切れのチーズで表現されます。チーズの穴は、システムの各部における相乗作用の欠如（つまり弱点）を表しています。このモデルでは、穴は静的なものではなく、サイズや位置が絶えず変化します。各チーズの穴の位置がその他すべてのチーズの穴の位置と瞬間的に揃うと、システムに故障が発生し、(Reason 氏が言う)「事故機会の軌道」を許してしまいます。チーズの穴の位置が瞬間的に揃うと、不測の故障シナリオに発展する可能性があります。

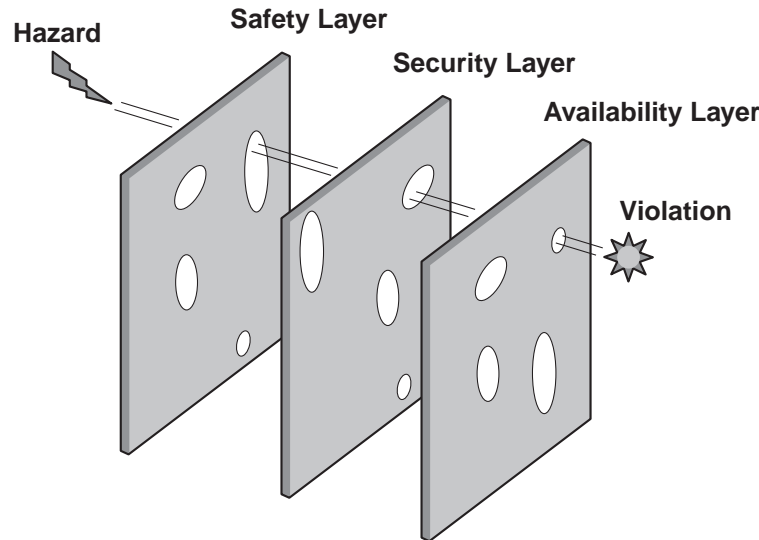


図 5: スイス チーズ モデル

Reason 氏がディペンダビリティ分野に貢献した重要な点は、「最後のチーズの穴が最終的な事故を引き起こすが、潜伏していた前の一連の故障がなければ、その事故が起きた可能性は低い」という概念です。

ザイリンクスはスイス チーズ モデルの効果を認め、全体論的なアプローチに従ってディペンダブルシステムのアーキテクチャを設計することを推奨しています。文化、組織、プロセス デザインをすべて考慮に入れて、エラーの不可避性を十分に低減させる相互認識型の防御レイヤーを設ける必要があります。

ザイリンクスの認定プロセス

システム デザインにおけるスイス チーズ モデルは、最終システムを作り出すために用いるプロセスを実質的に作成したエンジニアリング組織の構造、管理、手順で表すことができます。(a) 事実を把握してディペンダビリティを実現するか、(b) 当て推量に頼ってディペンダビリティの実現を望むかを分けるのは、優れたプロセスの有無だけでなく、認定プロセスの有無でもあります。

顧客にとっての安心を確保するため、ザイリンクスでは自社製品のライフサイクル全体を通して全要素を連携させる、次のような最新の完全認定プロセスを導入しています [参照 2]。

- ザイリンクスでは品質管理活動を定期的に内部監査し、活動の有効性と、定められた手順に従っているかどうかを確認しています。
- ザイリンクスでは真の根本原因分析を実施して問題を解決し、それを基に機能を改良しています。下請業者やサプライヤーと協力して、チームベースの Eight Discipline (8D) 調査アプローチを用い、次に、データ主導型のアプローチに従って恒久的かつ効果的なソリューションを開発しています。
- ザイリンクスは 1995 年以来、ISO 9001 認定 (品質管理システム) を取得し、さらに ISO 9001:2008 (カスタムのエンベデッド ソフトウェア デザインおよびロジック デザインの設計、試験、運用) にも準拠しています。
- ザイリンクスは 2004 年以来、TL 9000 認定 (通信) を取得しています。
- ザイリンクスの品質管理マニュアルは、ISO 9001:2000、TL 9000、TS 16949、Military (QML) やその他の業界標準に従って作成されています。
 - このマニュアルが SoC、FPGA、CPLD、およびコンフィギュレーション デバイスの設計、製造、試験に適用されています。

- Xilinx Ireland (XIR) は、Authorized Economic Operator (AEO) 認定を取得しています。
 - 現在、米国および EU が協力して AEO の相互理解に取り組んでいます。
- ザイリンクスは 2004 年以来、SoC STACK International、StackTrak - Supplier Certification Program (IC 品質および信頼性要件)、AEC-Q100 Component and Device Qualification (自動車産業向けの PPAP フルサポートあり) に準拠しています。
- ザイリンクスは、Department of Defense MIL-PRF-38535 Custom Microcircuit Certification (Class Q および N) に準拠しています。
- ザイリンクスは 2008 年以来、ISO 14001:2004I 認定、RoHS および Pb-free 認定、OHSAS 18001:2007 認定を取得しています。
- ザイリンクスは、機能安全規格に準拠しています [参照 3] (このページにアクセスするには登録が必要)。
 - IEC 61508 (ISE® Design Suite 14.2 ~ 14.7 に対する TÜV SÜD 認定)
 - ISO 26262 (ISE Design Suite 14.2 ~ 14.7 に対する TÜV SÜD 認定)
- ザイリンクスでは、ザイリンクス製品の満足度を最大限に高めるため、コンポーネント、ツール、ボード、ケーブルの返品のための正式な RMA (Return Material Authorization) 手順を策定しました。
- ザイリンクスでは、因果関係分析を用いて重大な異変の発生源を最小限に減らし、製品の収益、品質、信頼性を最大限に高めることを目的として、品質問題の防止に重点を置いたプロセスを策定し、すべてのパートナー メーカーに導入しています。

信頼性

ザイリンクスが公開している品質および信頼性情報には長年の実績があります [参照 2]。信頼性モニタープログラムにより、社内プログラム、国際規格、および個別の顧客要件で指定された信頼性仕様を満たすか、またはそれ以上の製品性能を実現しています。品質モニターでは完成品からサンプルを取ります。プログラム結果は四半期ごとに『デバイス信頼性レポート』(UG116) に公開されます [参照 4]。品質だけでなく、ディフェクトゼロの目標と品質重視の文化を重視する姿勢は、PPM データ、故障率 (FIT)、シングル イベント アップセット (SEU) データからわかります (詳細は、『デバイス信頼性レポート』参照)。

アップセット イベント効果

プログラマブルか否かを問わず、すべての集積回路はシングル イベント効果 (SEE) の影響をある程度受けやすくなっています。シングル イベント ラッチアップ (SEL) など致命的となり得る場合もありますが、データの反転や、プログラマブル デバイスの場合はコンフィギュレーション メモリの反転 (SEU) など回復可能なものもあります。これらの現象を確認し始めて以来、ザイリックスでは各イベントの影響を解消する方法と、発生したイベントを軽減する方法を積極的に研究しています。ザイリックスでは各テクノロジープロセス ノードを用いて、SEU による生来の FIT レートを低減しています (図 6 参照)。

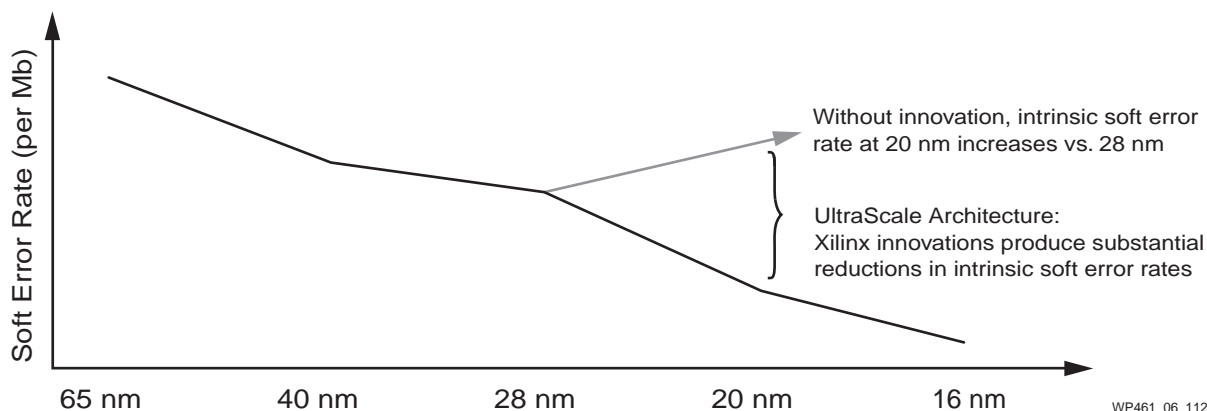


図 6: ザイリックス FPGA のソフト エラー率の傾向

ただし、シリコン機能だけでは、商用として安全なデバイスはできません。セキュリティ分野と同様に、ザイリックスではこの問題にもレイヤード アプローチで対応しています (図 7 参照)。

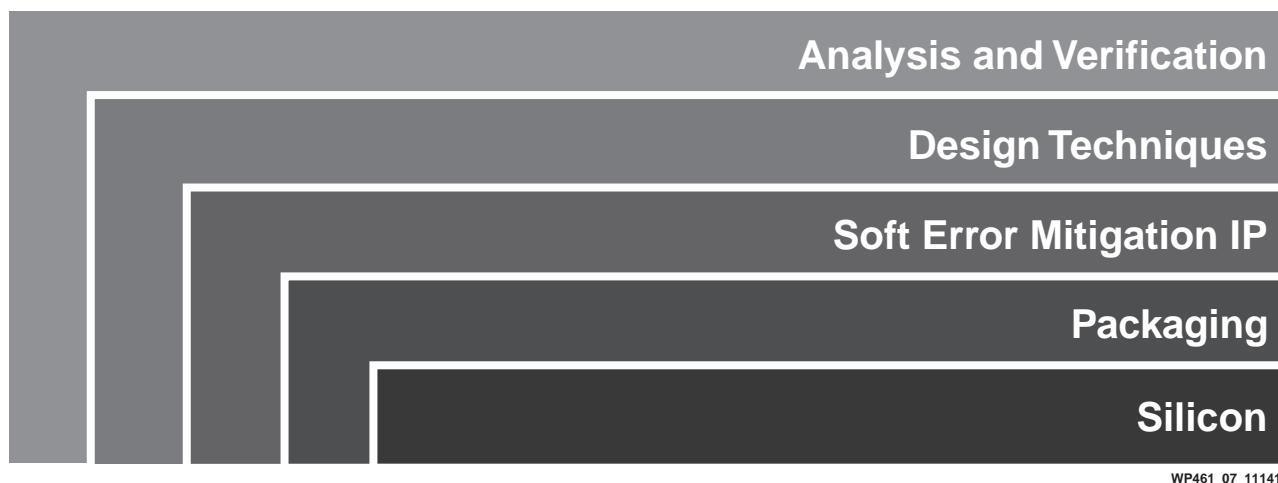


図 7: ザイリックスのマルチレベル SEU 低減ソリューション

まず、このソリューションはベースシリコンから始めます。次に、パッケージング素材に取り組みます。その上で、Soft Error Mitigation IP (SEM IP) と、フェイルセーフでフォールトトレランスを持つデザインを実現するさまざまな実装方式を提供します。さらにザイリックスでは、パフォーマンスを定期的に測定し、世代ごとにシリコンと IP の両面を改善するよう努めています。最後に、真に安全な環境を実現するために追加すべきレイヤーがわかるよう、顧客固有の動作環境の影響を判断するためのツールも用意しています。

SEU FIT レートなど、信頼性に関するデータ [参照 4] が公開されています。詳細は、ザイリックスウェブサイトのシングル イベント アップセットに関するページ [参照 5]、ザイリックス ホワイトペーパー『FPGA、ASIC、プロセッサにおけるシングル イベント効果についての考察』 [参照 6]、ザイリックス ホワイトペーパー『シングル イベント アップセット (SEU) の軽減』 [参照 7] を参照してください。

シリコンに内在する FIT レートの低減

シリコン機能

前述のとおり、最初に必要な低減レイヤーはデバイスに内在する FIT レートの低減を目的としています。まずは、FPGA/SoC のコア要素であるコンフィギュレーション メモリ セルから始めます。ザイリンクスでは、SEU 耐性の高いコンフィギュレーション メモリのベスト プラクティスに関する研究に力を入れています。デザインとレイアウトの両方に関する独自のデザイン技術、広範囲なシミュレーション、チップ動作試験、実際のビーム試験により、ザイリンクス デバイスの FIT レートは世代ごとに着実に低下しています。

パッケージ技術

シリコンに加え、ザイリンクスではデバイスのパッケージ素材も厳しく管理しています。これにより、アルファ線による SEU を大幅に低減できます。

ユーザー機能

ザイリンクスでは、メモリ セルアーキテクチャの実際のデザインを積極的に管理することに加え、バックグラウンドでの SEU 検出および訂正にも独自の設計手法を導入しています。ユーザー デザインに FRAME_ECC プリミティブを挿入すると、コンフィギュレーション フレーム レベルでシングルエラー訂正とデュアルエラー検出が可能になります。拡張コンフィギュレーション フレーム インターリーブにより、マルチビット アップセット (MBU) の影響がこれまで以上に低減しているため、ほとんどネゲートしなければ、デザインのパフォーマンスにまったく影響を与えずに MBU の影響を大幅に低減できます。

ただし、このカテゴリはコンフィギュレーション メモリだけに留まりません。ザイリンクスのユーザー メモリ アレイ (ブロック RAM) には堅牢なアーキテクチャとエラー訂正機能が組み込まれており、シングルビット エラーの訂正と、ダブルビット エラーの検出 (自己訂正ではない) が可能です。

ツールによる低減、分類、予測

レイヤード アプローチ方式と共に、ザイリンクスでは SEU および MBU の影響の分類と低減に役立つ SEM IP も提供しています [参照 8]。SEM IP はザイリンクス デバイスの内蔵シリコン機能をベースに構築され、エラー分類やエラー挿入などの機能が加わります。エラーの分類と発生源の特定は、デバイス全体の FIT 低減の基本となります。ザイリンクス デバイスは、コンフィギュレーション フレーム アレイ (それぞれで FRAME_ECC を使用) を中心に構築されます。この大規模なメモリ アレイには多数のビットが含まれていますが、ユーザー デザインの動作に実際に影響するビットはわずかです。デザインによっては、少数であってもユーザー IP の重要なセーフティ機能に影響を及ぼす場合があります。これらのビットはすべて、次のように分類できます。

- デバイス コンフィギュレーション ビット: デバイス コンフィギュレーション アレイ内の全ビット
- エッセンシャルビット: ユーザー デザインに関連するビット [参照 9]
- 優先エッセンシャルビット: 安全性に関するユーザー定義のクリティカルビットに関連するビット
- クリティカルビット: ステートが変化すると機能障害を引き起こすビット

ザイリンクス ソリューションの長所は、これらのビットの識別機能がザイリンクスの基本デザイン ツールに組み込まれており、ユーザーが必要に応じてカスタマイズできる点です [参照 8]。

これほど堅牢な SEU ソリューションは必要としない動作環境やアプリケーション向けに、ザイリンクスは SEU FIT レート カリキュレーター [参照 7] も提供しており、これを利用すると、所定の環境におけるアプリケーションの推定 FIT レートがわかります。詳細は、ザイリンクスのアビオニクスに関するページを参照してください [参照 10] (このページにアクセスするには登録が必要)。

FPGA に関する IEC 61508 要件

IEC 61508 の要件をすべて扱うのはこのホワイトペーパーの範囲を超えるため、ここでは FPGA に関する主な要件のみを説明します(この規格に関する基本知識が必要)。ランダム故障や系統的错误に対処するための設計手法やハードウェア/ソフトウェアでは、セーフティ ライフサイクルを考慮する必要があります。このライフサイクルは、安全装置の実装担当者が管理する必要があります。IEC 61508 はいくつかの措置を推奨しており、特に IEC 61508-2 (パート 2) の第 7.1.3.1 項では、セーフティ ライフサイクルに V モデル (各開発フェーズと検証/有効性検査フェーズが対応するモデル) を推奨しています。

さらに第 7.4.4.2 項では、次の 6 つの主要要件について定めています。

1. ハードウェア安全度に関するアーキテクチャ上の制約を入力要件として定義すること
2. 到達可能な安全度を判断するために、ランダム故障の影響を定量化すること
3. オンチップの冗長構成を目的とするアーキテクチャの場合は、パート 2 の付録 E を使用すること
4. パート 3 の規定に従い、ラベルに文字「S」(systematic safety integrity: 系統的な安全度)を表す)が付いた 3 つのルートを使用して、系統的な安全度(「適当な能力」とも呼ばれる)を満たすこと
 - a. ルート 1S: 系統的故障の管理については、パート 3 の規定に従うこと
 - b. ルート 2S: 当該機器が使用中であると証明すること
 - c. ルート 3S: 既存のソフトウェアを信頼する必要がある場合は、そのソフトウェアがパート 3 に準拠していると証明すること
5. 障害検出時のシステム動作(適切な安全措置の実行)に関する要件を定義すること
6. 交換される情報の完全性を確保するためにデータ通信プロセスに関する要件を定義すること

さらに IEC 61508-2 の第 7.4.4 項では、ハードウェア安全度に関するアーキテクチャ上の制約について定めています(パート 2 の付録 C に記載される論理式を参照)。

6 つの指示はどれも詳細に説明するには内容が多すぎるため、ここでは最優先事項としてすべての指示に従うことを覚えておくだけで十分です。

さらに IEC 61508-2 では、ハードウェアの安全度水準を定義するためのルートを 2 つ定めており、セーフティ機能ではそのいずれかを要求できます。ルート 1H および 2H はアプリケーション固有のため、IEC 61508-2 では、どちらを用いるかの判断を具体的なアプリケーション規格に委ねています。

1. ルート 1H: ハードウェアのフォールトトレランスと安全側故障割合の概念に基づく
2. ルート 2H: エンドユーザーのフィードバックから得たコンポーネントの信頼性データ、向上した信頼性レベル、特定の安全度水準に対するハードウェアのフォールトトレランスに基づく

ISO 26262 でも、安全度を実現する方法に関する同様の要件を定めています(それほど厳格でない場合もある)。

安全規格への準拠がプロセスに含まれていることの判断は簡単ですが、それに加え、少なくとも 10 ~ 15 年の耐用期間にわたって製品のサポートを提供できるようにすることが必要です。

ザイリンクスによる機能安全上の課題の解決方法

FPGA は IEC 61508-2 で具体的に扱われており、必要な安全度水準を実現する方法として冗長設計が推奨されています。ザイリンクスの FPGA と SoC は、より高いレベルの統合によって冗長設計を実現しやすくすることで、ほかのソリューションよりも少ないコンポーネント数でセーフティ設計を実装し、それによりシステムコストを削減します。ザイリンクス製品は、次の 2 つのアプローチで冗長構成を実装しています。

- アプリケーション規格によりシングルチップソリューションが不可能な場合は、デュアルチップソリューションを用います(比較的成本が高くなる)。
- アプリケーション規格によりシングルチップソリューションが可能な場合は、この方法でセーフティ機能を実装します(たとえば、IEC 61508-2 付録 E は SIL3 まで許容)。このオプションを実現可能にするのは、ザイリンクスの FPGA および SoC の性能です。ほかのセクター固有の規格で明示的に除外されていない限り、このソリューションが推奨されます。

ザイリンクスのツールおよび実装方式

認定ツール

実装担当者は、IEC 61508-2 の項目 4 に記載されたシステムの「FPGA に関する要件」を確実に満たすため、認定された開発ツールを利用する必要があります。ザイリンクスでは、FPGA ユーザーが適切な設計手法と手順に従ってセーフティ設計を実装できるようにする機能安全パッケージを作成し、自社のツールチェーンを認定しました。セーフティマニュアル『セーフティガイドライン、IEC 61508、ISO 26262 に準拠するための要素』(機能安全ラウンジ [参照 3] で入手可能) では、ザイリンクスの ISE FPGA プログラミング ツールチェーン、バージョン 14.2 ~ 14.7 を扱っています。このマニュアルは、IEC 61508 Edition 2 および ISO 26262 に従って安全性に関する FPGA アプリケーション デザインを開発する際に利用します。また、SIL1 ~ SIL3 または ASIL-A ~ ASIL-D に関する要件も扱われています。

認定ツールチェーンでは、安全な FPGA デザインを作成するためのザイリンクス ツールに基づく設計手法とフローについて説明しています。また、干渉なく必要な冗長性レベルを実現するために、必要な機能構築ブロックを分割/分離してデザインフローを適用できるよう説明しています。これにより、所定の SIL または ASIL を満たす FPGA の最終ビットストリームを合成できます。また、IEC 61508 Edition 2 で推奨される V モデルに従って実装(タイミング、温度、消費電力、デザインルール違反、分離違反など)を検証およびテストするためのガイダンスも記載されています。

ISE Design Tool Suite 14.2 ~ 14.7 FPGA プログラミング ツールチェーン

ザイリンクスは現在、次の安全規格に対応する ISE Design Suite 14.2 FPGA プログラミング ツールチェーン [参照 3] および ISE Design Suite 14.7 (図 8) に対して TÜV SÜD 認定を取得しています。

- IEC 61508 Edition 2.0 2010-04
- ISO 26262 First Edition 2011-11-15



WP461_08_110514

図 8: ISE Design Suite FPGA プログラミング ツールチェーンの TÜV SÜD 認定

アイソレーション デザイン フロー (IDF)

ザイリンクスのアイソレーション デザイン フロー (IDF) [参照 11] は、ある論理機能と別の論理機能を論理的および物理的に分離可能にするツール設計手法です。IDF は、次の 2 段階になっています。

- アイソレーション: ISE PlanAhead™ フロアプラン ツールを使用したファンクションブロックの物理的および論理的分離。
- アイソレーション検証: アイソレーション検証ツール (IVT) と呼ばれるツールで、ファンクションブロックの物理的な分離と、ブロック間の配線接続の適切な分離を検証します。

この 2 段階のデザイン フローは、IEC 61508 および ISO 26262 に対する TÜV SÜD 認定を受けています。

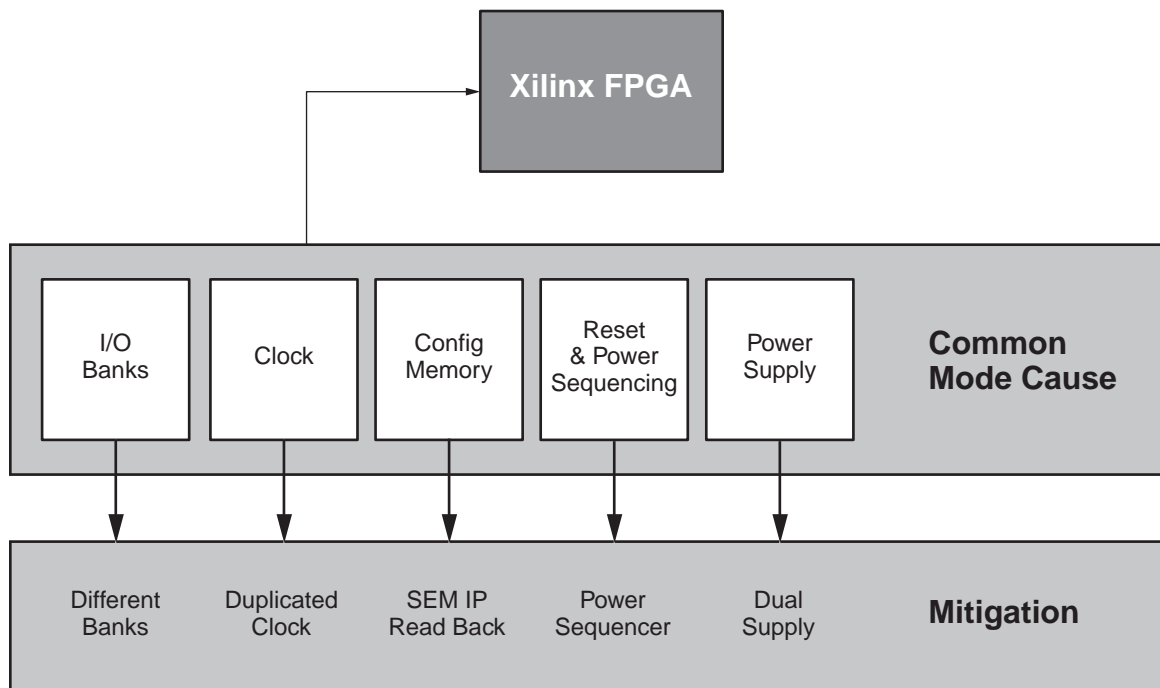
IDF を用いると、各機能の間に未使用のデバイス コンポーネントから成るフェンスを利用して、物理的に分離された複数の独立機能を 1 つの FPGA に実装できます。分離された各機能はこのフェンスで区切られるため、デバイス内に分離領域が形成されます。このフローでは、早期のフロアプラン、モジュール デザイン、モジュール合成、一連のガイドラインへの準拠、必要な機能間を確実に分離するための考慮事項を採用しています。

デザインを実装したら、IVT を使用して、アイソレーションのデザインルール (分離モジュールの間にフェンスを設けること) が正しく実装されているか検証する必要があります。IEC 61508-2 規格の表 E.2 に定めるとおり、物理ブロックを分離およびデカップリングする構造体として、アイソレーションブロックを検討することもできます。

共通原因故障の低減

共通原因は、入念に構築されたデザインにさえ深刻な影響を及ぼす恐れがあるため、あらゆるセーフティ アプリケーションにとって問題となります。IEC61508-2 付録 E では、ベータ係数アプローチを用いて FPGA の共通原因に具体的に対処しており、いくつかの低減メカニズムの実現を義務付けています。

図 9 に、セーフティ システムに影響する恐れのある一般的な共通原因と、それらに対処するためにザイリンクスが採用している低減策を示します。SEM IP は、ザイリンクスの Soft Error Mitigation IP を指します [参照 8]。



WP461_09_040715

図 9: FPGA の同相原因とザイリンクスの低減策

セーフティ システムでは共通原因故障が複数発生する可能性があり、対処が必要です。表 1 に、これらの原因の一部と、ザイリンクスの FPGA/SoC で採用している低減策を示します。

表 1: 共通原因故障とザイリンクスの低減策 (Zynq-7000 SoC)

共通/同相原因	ザイリンクスの低減策 (Zynq-7000 SoC)
電源: ノイズ、電磁妨害の伝搬、PS スイッチオン (ラッチアップなど)、過電流引き込み	分離および独立した電源 (PL、PS) と電源投入シーケンス (IEC 61508-2、表 E.1 を参照)
多様性の欠如: 1 つの故障でシステム全体がダウンする	複数の冗長構成スキーム: 診断機能付きの複数のセーフティチャネル (PL、PS)
セーフティチャネルと非セーフティチャネルの分離	アイソレーション デザイン フローを用いたオンチップの冗長構成 (IEC 61508-2、付録 E、表 E.2 を参照)
ファンクションブロックへのアップグレード	機能アップグレードのためのデザイン保持 (変更しないブロックについては QoR を保持)

IEC 61508 に対する Zynq-7000 SoC の答え

電源には同相による懸念事項が 1 つあります。別々の電源プレーンを使用できれば、独立した冗長回路を実現できます。

PS および PL の電圧ドメイン

IEC 61508-2、付録 E (E.1 から抜粋) では、次のように記載されています。

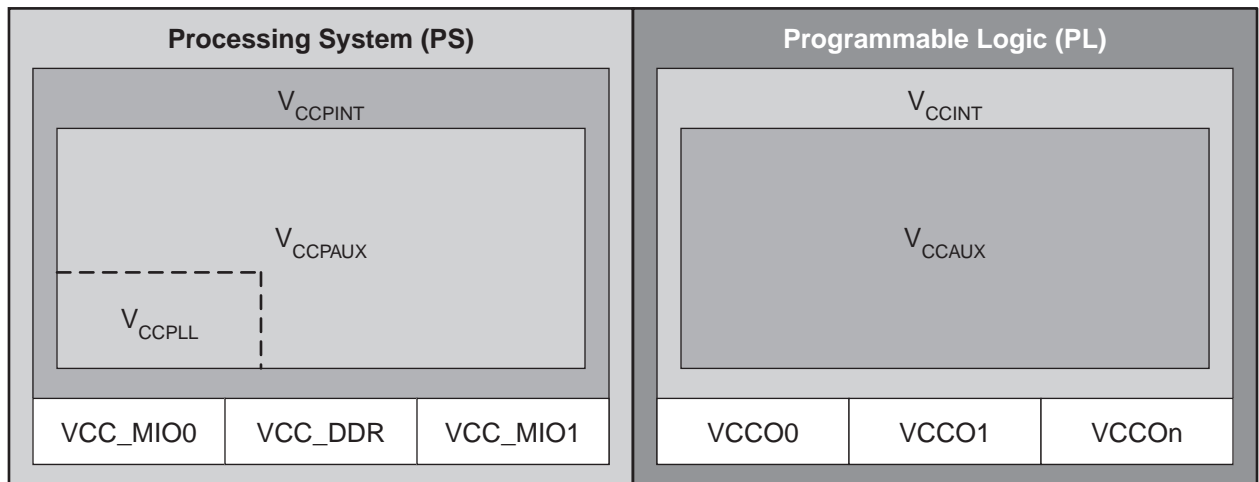
- e) 電源障害を原因とする危険な故障 (共通原因故障など) を避けるため、適切な手段を講じること。

注記 5: 電源障害には、次のものが含まれる (ただしこれに限らない):

- o ノイズ
- o 電源ラインによる電磁妨害の伝搬
- o 非同時の電源スイッチオン (ラッチアップや高突入電流などの原因となり得る)
- o 短絡による過電流引き込み

Zynq-7000 SoC は、PS および PL 用に分離した独立電源を採用することで、この電源上の問題に対処しています (図 10 参照)。

PS and PL Separate Voltage Domains for Managing Power



WP461_10_112014

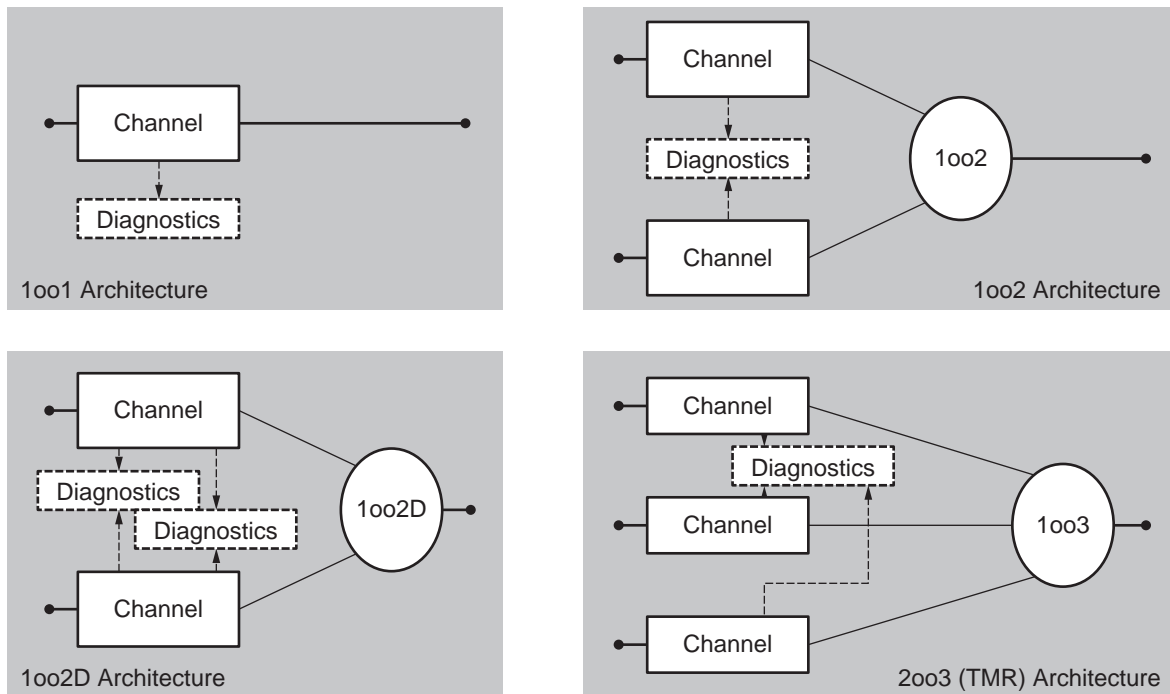
図 10: PS および PL 用の分離電源

Zynq-7000 SoC の冗長構成スキーム

冗長構成によって故障を低減する方法は複数あります。既存の機能を二重化すると、冗長機能が実現されます。冗長スキームにすると、システムの可用性と堅牢性を高めることができます。

冗長スキームは、満たすべき要件に応じてさまざまなシステム レベルで実装できます。安全性に関する機能の完全二重化は非常に複雑で高コストになる可能性があるため、通常は機能の特定部分のみを二重化します。

Zynq-7000 デバイスでは複数のアーキテクチャが利用可能です。どのスキームも、同相による故障対策としてブロックのアイソレーション デザイン フロー (IDF) を必要とします。Zynq-7000 SoC で利用可能な 4 つのアーキテクチャについては、[図 11](#) を参照してください。

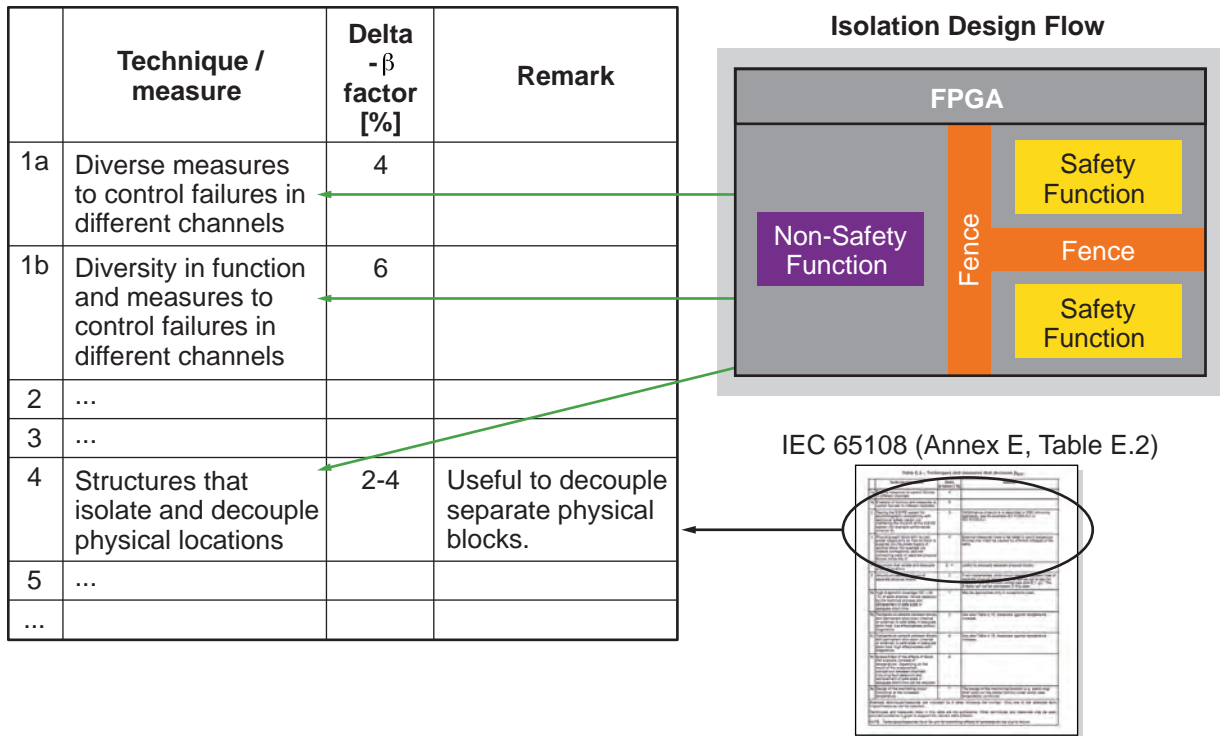


WP461_11_020915

図 11: Zynq-7000 SoC で利用可能なアーキテクチャのブロック図

アイソレーション デザイン フローを使用したオンチップの冗長スキーム

共通原因故障が冗長型機器の安全性と可用性に悪影響を及ぼす可能性があることは広く知られています。IDF [\[参照 11\]](#) を使用すると、いくつかの点で、冗長型システムが共通原因故障の影響を受けにくくなります。IEC 61508-2 (付録 E、表 E.2) には、基本的なベータ係数 (IC による影響の受けやすさ) を低減する技法と手段が記載されています。[図 12](#) に、表 E.2 の一部と、IDF によってオンチップ冗長型 (OCR) システムの β_{IC} を大幅に低減する 3 つの技法/手段を示します。たとえば、「フェンス」(IDF で定義されるアイソレーション領域) は、「分離した物理ブロックをデカップリングするのに役立つ構造体」(IEC 61508-2、表 E.2、項目 4) に該当します。



WP461_12_110514

図 12: アイソレーション デザイン フローを使用したオンチップの冗長スキームおよび分離

実装の多様性

多様性とは冗長性の一種であり、冗長型コンポーネントが一般的な開発エラーの影響を受けないよう、さまざまな実装を提案します。

安全性が重要なシステムにおいて、デザインの多様性は同相原因または共通原因による開発エラーの対策となります。多様性は、1つの機能故障パスで一般的な開発エラーから故障が生じ、別の機能故障パスにも影響を及ぼす可能性を減らそうとするシステム設計の概念です。多様性を実現するには、類似性の低い特性を持つ機能故障パスを設計して、エラーが別のコンポーネントにも現れる可能性を最小限に抑えます。発生した障害は、システム内で正常にマスキングされた後に無視されます。

多様性は、ソフトウェアでもハードウェアでも実現できます。ハードウェアでは、さまざまなメーカーが設計および提供している初期仕様の同じコンポーネントまたはサブシステムを用いてこれを実現します。

Zynq-7000 ファミリーでセーフティ チャンネルを多様化する方法は複数あります。

- プログラマブル ロジック (PL) とプロセッシング システム (PS)
- PL と MicroBlaze™ プロセッサと PS (APU)
- PL と PS (APU) とデュアル ロックステップ MicroBlaze プロセッサ

Zynq-7000 デバイスで使用できる多様性オプションは、図 13 および図 14 を参照してください。

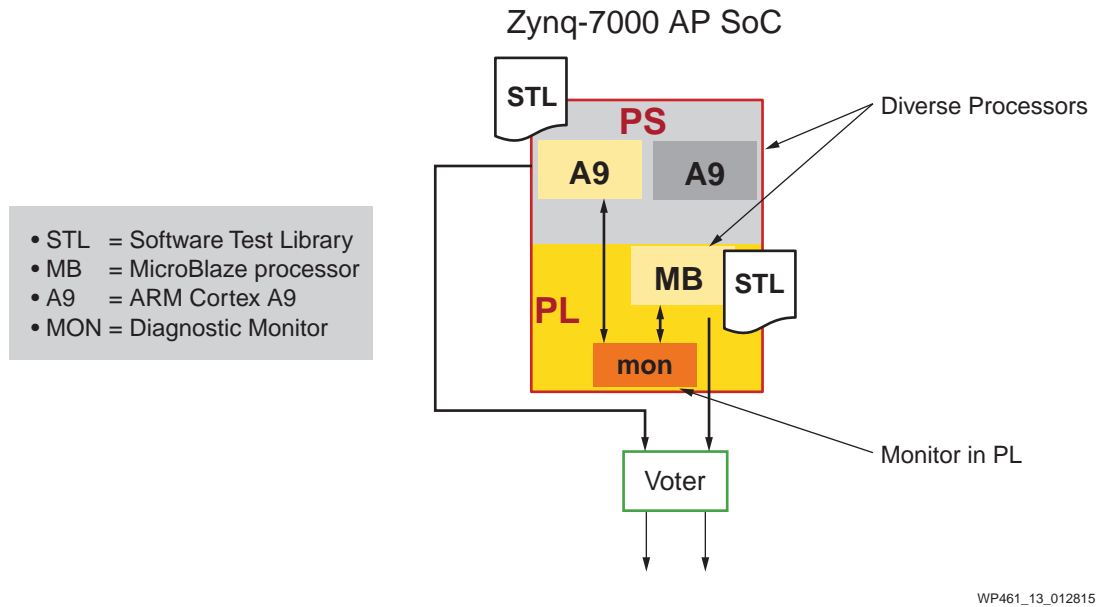


図 13: Zynq-7000 SoC の多様性オプション: 単体の MicroBlaze IP プロセッサを使用

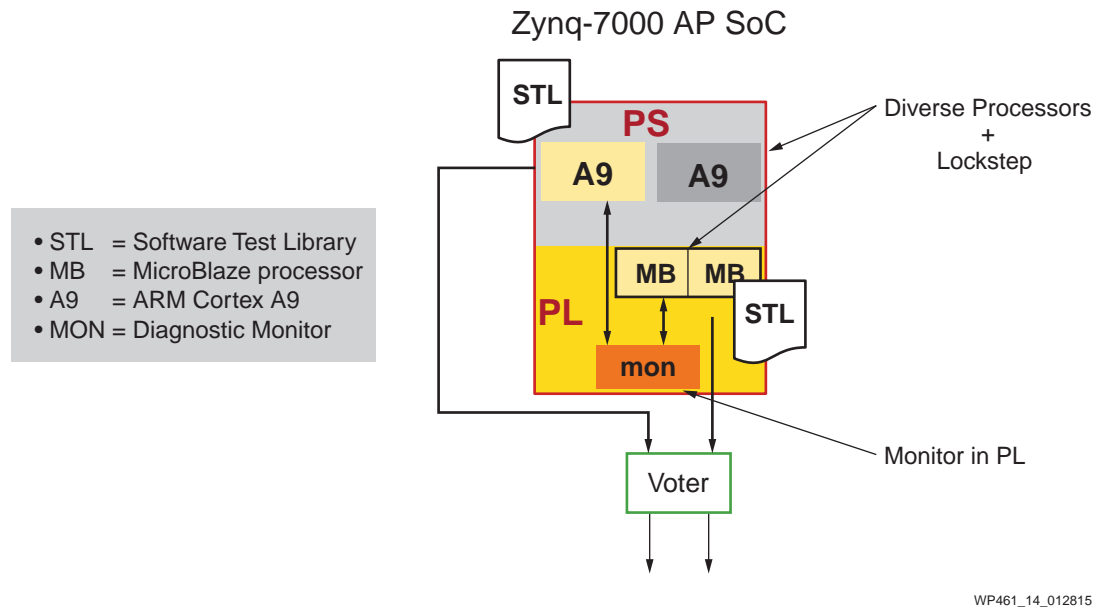


図 14: Zynq-7000 SoC の多様性オプション: デュアル コア ロックステップ MicroBlaze IP プロセッサを使用

ロックステップの概念

ロックステップアーキテクチャでは、2つのプロセッサ(マスターとチェッカー)が厳密な同期で同じコードを実行します。マスターはシステムメモリへのアクセス権を持ち、すべてのシステム出力を実行します。チェッカーは、マスタープロセッサによってフェッチされた命令を連続的に実行します。チェッカーによって生成された出力(アドレスとデータの両方)は、比較ロジック(モニター)に送られます。比較ロジックは、マスターとチェッカーのデータ、アドレス、制御ラインの一貫性をチェックします。二重化されたバスラインのペアの値が一致しない場合は、いずれかのCPUに障害があります(どちらのCPUに障害があるかは特定されない)。図 15 に、デュアルロックステップ MicroBlaze プロセッサシステム [参照 12] [参照 13] のブロック図を示します。

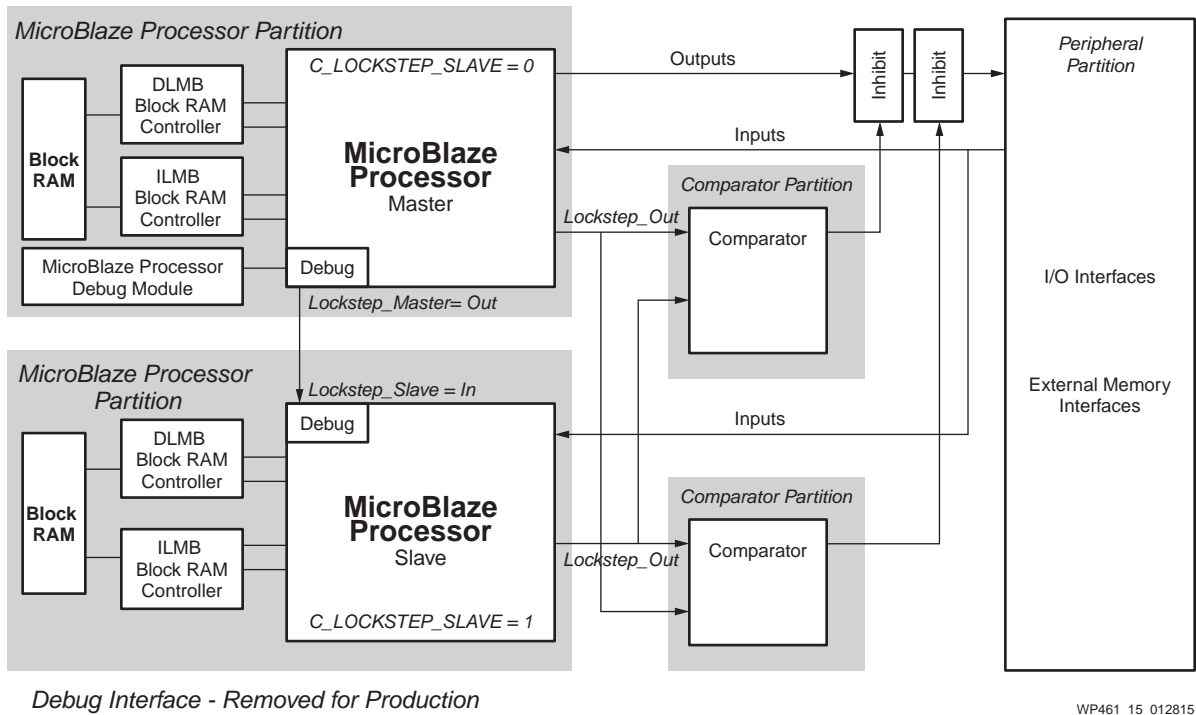


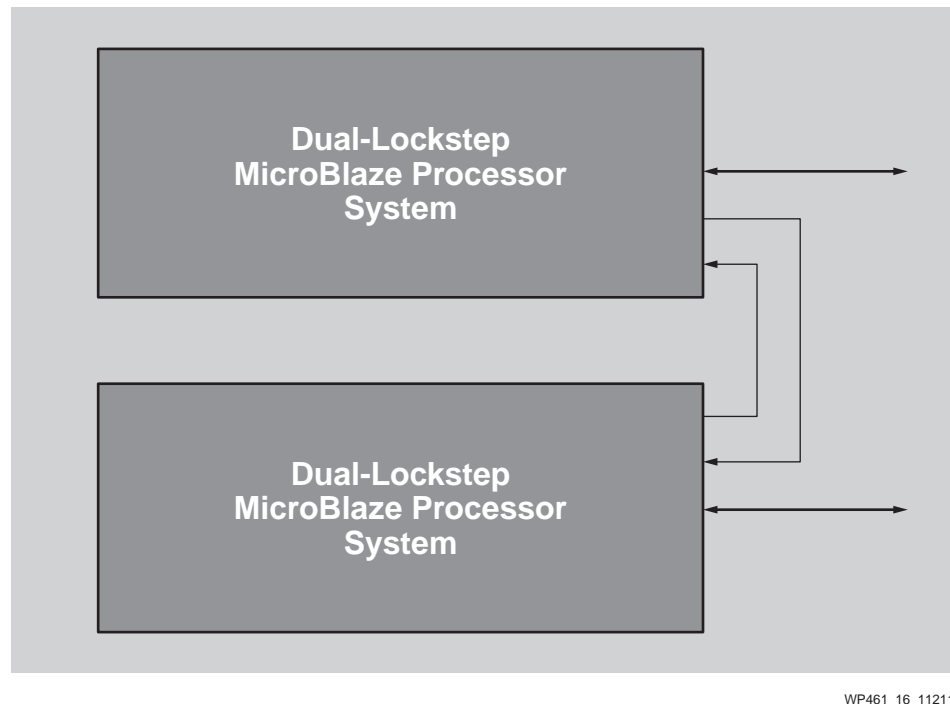
図 15: ザイリンクス デュアル ロックステップ MicroBlaze プロセッサのブロック図

ロックステップの実装には、いくつかの制限事項があります。モニターはバスエラーとメモリエラーを検出できません。これらのエラーは同相による故障の原因となり、両方の CPU に同様の故障が発生します。バスとメモリは、パリティビット (エラー訂正コード) などのエラー検出 (訂正) 技法を用いて障害から保護する必要があります。

ロックステップアーキテクチャは、CPU、メモリ、または通信サブシステムで無差別に発生するカバレッジ 100% のエラー (永続的または一時的) を検出できるフェイルサイレントノードとして採用できます。

冗長デュアルロックステップの概念

冗長デュアルロックステップ MicroBlaze [参照 12] [参照 14] プロセッサの実装を採用すると、いくつかの制限事項に対処できます。図 16 に、考えられる冗長デュアルロックステップ MicroBlaze プロセッサシステムの大まかなブロック図を示します。



WP461_16_112114

図 16: 冗長デュアル ロックステップ MicroBlaze のブロック図

- デュアル ロックステップ アーキテクチャでは、2つのフェイル サイレント チャンネルが同じメモリ サブシステムを共有します。
- 冗長デュアル ロックステップ アーキテクチャの実装方式は、フォールトトレラント特性が同じ三重モジュール式冗長 (TMR) ソリューションにも対応します。
- フェイルオペレーショナル機能が必要な場合は、ロックステップ モードで2つのチャンネルを配置できます。
 - TMR ソリューションと同様に、CPU 障害のマスキング機能を実現する
 - 完全並列型の2つのフェイル サイレント チャンネルとして使用し、パフォーマンスを2倍にする

システム セキュリティ

Virtex®-II Pro ファミリ以降、ザイリンクスは何世代もの製品にわたってセキュアな FPGA ソリューションを提供しています。世代ごとに、進化する脅威を分析し、それに対処する機能を加えてきました。ザイリンクスは、まずシリコン機能に取り組み、そこから完全統合型のセキュリティ IP (Security Monitor) へと発展させることで、FPGA/SoC 開発者向けのセキュア ソリューション提供におけるリーダーシップを実証してきました。ザイリンクスのセキュア ソリューションの概要は、ザイリンクスのウェブサイトを参照してください [参照 15]。

シリコン機能

ザイリンクスでは、前のレイヤーをベースに新しいレイヤーを構築していくレイヤードアプローチでセキュリティに取り組んでいます。この取り組みでは、開発者が構築のベースにできるセキュアな基盤が作られます。最初のレイヤーは、もちろんシリコン自体です。基本レイヤーがセキュアでなければ、プラットフォームをセキュアにすることはできません。基盤が安定していなければ、砂地に家を建てるようなものです。ザイリンクスでは、認証と FPGA ロードの機密性実現の両方に、256 ビットの HMAC 認証スキームを用いた AES256 暗号化などのシリコン セキュリティ機能を採用しています。また、Zynq-7000 SoC の FSBL (第 1 段階ブートローダー) の認証には RSA2048 を用い、この認証をすべての後続デバイスのロードにまで拡張するのに必要なコードも備えています。ザイリンクスではこのセキュリティレイヤーをベースとして、JTAG コントローラーなどの外部インターフェイスを無効化することで、FPGA/SoC の「ドアをロックする」方法を提案しています。また、この物理的な保護に加え、システム モニターまたは XADC でデバイスの環境電圧/温度をモニターする方法も紹介しています。この内容および詳細は、『Virtex-6 および 7 シリーズ FPGA での不正操作防止デザインの開発』で公開されています [参照 16]。これらすべてをベースにすることで、Zynq-7000 SoC などのデバイスの電源を入れた瞬間から、セキュアなプラットフォームが実現されます。

知的所有権 (IP)

セキュリティ最優先の環境を運用しているが、独自のカスタム セキュリティ ソリューションは構築したくないというユーザー向けに、ザイリンクスではセキュア ソリューションを 1 つのパッケージで提供しています。このソリューションが Security Monitor です。ここには、堅実なセキュリティレイヤーが 1 つの IP コアにまとめられています。Security Monitor は、前述のザイリンクス アプリケーション ノート [参照 16] で説明している内蔵のセキュア機能を採用しているだけでなく、デバイス コンフィギュレーション メモリをモニターして最初のコンフィギュレーションからの変更がないか確認することで、セキュリティレベルを高めています。バックグラウンドで動作するシステム正常性モニタリングは、攻撃者やシングル イベント アップセット (SEU) によるコンフィギュレーション メモリの変更を検出し、必要に応じて訂正できます。問題が検出された場合、ユーザーはその問題を訂正して安全な状態に戻すことができます。また、必要に応じてデバイスの内容を初期化して、ユーザーの IP を保護することもできます。Security Monitor IP コアの全機能についての詳細は、『Security Monitor IP コアの製品概要』 [参照 17] を参照してください。

まとめ

セーフティ機能とそれ以外の機能を 1 つのデバイスに緊密に統合できるザイリンクス製品にはさまざまな利点がありますが、なかでもクラス最高の品質、FIT、SEU の処理に加え、顧客の厳格な安全性目標を満たす、これまでにないツールと技法 (IDF、IVT など) を特長としています。ザイリンクスのセーフティ テクノロジは規格準拠認定を受けているため、顧客はリスクのないセーフティ ソリューションとして利用できます。

ザイリンクスの機能安全ソリューションの概要は、ザイリンクス製品概要『ザイリンクス機能安全デザイン フロー ソリューション』 [参照 18] を参照してください。

機能安全に向けたザイリンクスのサポート

ザイリンクスでは、機能的に安全なシステムを構築する顧客向けに、幅広いサポートを提供しています。

- TÜV SÜD 認定セーフティ データ パッケージ [参照 3]
 - ザイリンクスの FPGA/SoC でセーフティ設計を実現するための認定ツール (ISE 14.2 – 14.7) および設計手法
 - セーフティ マニュアル [参照 3]、認定証、テスト レポート
 - V モデル、QM、デバイスの信頼性データ
 - アイソレーション デザイン フロー (IDF) およびアイソレーション 検証 フロー (IVT) [参照 11]
 - セーフティ アプリケーションとそれ以外のアプリケーションを分離した状態で 1 つのデバイスに統合する
 - 以降の認定取得の手間とリスクを減らす
- SEU 低減 IP [参照 8]
 - コンフィギュレーション メモリのアップセットを検出し、訂正する
- FIT レート分析ツール [参照 7]
 - FIT レート カリキュレーター、エッセンシャル/クリティカル ビット 分析により、セーフティ アプリケーションの FIT レートに関する考慮事項を軽減する
- 消費電力解析ツール [参照 19]
- ザイリンクスとサプライチェーンによる品質および品質管理
 - ISO9000/QML/TL9000/TS16949
- セキュア ソリューション [参照 15]
 - シリコン セキュリティ 機能
 - セキュリティ IP [参照 17]
 - Security Monitor
 - 資料 [参照 16]

表 2 に、ザイリンクスの FPGA/SoC で達成可能な機能安全仕様および安全度水準 (SIL) を示します。

表 2: 機能安全仕様および達成可能な SIL/ASIL

機能安全仕様	安全度水準
IEC 61508 Edition 2.0 2010-04	SIL1 ~ SIL3
ISO 26262 First Edition 2011-11-15	ASIL-A ~ ASIL-D

参考資料

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。

1. 「A New Accident Model for Engineering Safer Systems」、Nancy Leveson 著、『Safety Science』、Vol. 42、No. 4、2004 年 4 月、pp. 237 ~ 270
2. ザイリンクス年次品質レポート: [2013 年 3 月](#)
3. ザイリンクス ウェブサイト: [機能安全パッケージ](#) ランディング ページ (ページにアクセスするには登録が必要)
4. ザイリンクス ユーザー ガイド: 『デバイス信頼性レポート、2013 年第 4 四半期』(UG1165: [英語版](#)、[日本語版](#))
5. ザイリンクス ウェブサイト: [シングル イベント アップセット](#)
6. ザイリンクス ホワイトペーパー: 『FPGA、ASIC、プロセッサにおけるシングル イベント効果についての考察』(WP395: [英語版](#))
7. ザイリンクス ホワイトペーパー: 『シングル イベント アップセット (SEU) の軽減』(WP395: [英語版](#)、[日本語版](#))
8. ザイリンクス製品ガイド: 『LogiCORE IP Soft Error Mitigation Controller v4.1』(PG036: [英語版](#)、[日本語版](#))
9. ザイリンクス アプリケーション ノート: 『優先エッセンシャルビットを使用したソフト エラーの軽減』(XAPP538: [英語版](#)、[日本語版](#))
10. ザイリンクス ウェブサイト: [アビオニクス](#) ランディング ページ (ページにアクセスするには登録が必要)
11. ザイリンクス ウェブサイト: [アイソレーション デザイン フロー \(IDF\)](#)
12. ザイリンクス アプリケーション ノート: 『アイソレーション デザイン フローを使用した Spartan-6 FPGA デュアル ロック ステップ MicroBlaze プロセッサ』(XAPP584: [英語版](#))
13. ザイリンクス ユーザー ガイド: 『MicroBlaze プロセッサ リファレンス ガイド (EDK 14.7)』(UG081: [英語版](#)、[日本語版](#))
14. Logiccircuit Inc. ウェブサイト: DO-254 MicroBlaze 1.00a
<http://logiccircuit.com/products/do-254-microblaze-1-00a>
15. ザイリンクス ウェブサイト: [デザイン セキュリティ ソリューション](#)
16. ザイリンクス アプリケーション ノート: 『Virtex-6 および 7 シリーズ FPGA での不正操作防止デザインの開発』(XAPP1084: [英語版](#)、[日本語版](#))
17. ザイリンクス製品概要: 『Security Monitor IP コア』([CS1140 AD](#))
18. ザイリンクス製品概要: 『ザイリンクス機能安全デザイン フロー ソリューション』([PB015](#))
19. ザイリンクス ユーザー ガイド: 『Xilinx Power Estimator』(UG440: [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
2015/04/09	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(第三者が起こ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、(I)エアバッグの展開、(II)車のコントロール(フェイルセーフまたは余剰性の機能(余剰性を実行するためのザイリンクスの装置にソフトウェアを使用することは含まれません)および操作者がミスをした際の警告信号がある場合を除きます)、(III)死亡や身体傷害を導く使用、に関するアプリケーション)を使用するために設計されたり意図されたりもしていません。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 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。