WP495 (v1.0) 2017 **年** 11 **月** 21 **日**

IEC 61508 **に従った** Zynq-7000 SoC **デザインで** ISO 13849 **準拠を実現**

著者 : Paul S. Levy

このホワイト ペーパーでは、機能安全に携わる開発者を対象に、Zynq®-7000 All Programmable SoC ベースのエレメントとアーキテクチャを利用して ISO 13849 への準拠を果たし、認証コストとタイムトゥ マーケットを削減する方法について説明します。

概要

Zynq-7000 All-Programmable SoC はプログラマブル ロジックを統合した業界初の SoC で、機能安全に携わる開発者はシングル チップで提供される多様な機能を利用して安全関連システムの品質を高めることができます。Zynq-7000 SoC はプログラマブル ロジックと ARM® Cortex™-A9 というオンチップ サブシステムが独立したアーキテクチャを採用しており、カスタマーは Zynq-7000 SoC が備える多様性により、投資を抑えながらカスタマー ソリューション全体のシステム機能を向上できます。

Cat. 3 および Cat. 4 ソリューションの 2 チャネル要件を含め、ISO 13849 のパフォーマンス レベルはすべて 1 つの Zynq-7000 デバイスでサポートできます。プロセッシング サブシステムとプログラマブル ロジックの両方に診断機能が備えられているため、ユーザー デザインによる診断機能がほとんど、あるいはまったく必要なくなります。

このホワイト ペーパーでは、ISO 13849 に準拠した各パフォーマンス レベルを達成する上での課題とストラテジについて概観し、Zynq-7000 SoC ソリューションによってタイムトゥ マーケットを短縮する方法について説明します。

はじめに

機能安全の世界ではさまざまな分野に安全関連規格がありますが、IEC 61508 はこれらすべての規格に共通する基本原理を定義した親規格と位置付けられています。IEC 61508 は汎用的なリファレンスとして策定されており、さまざまな産業分野に特化した規格に対するガイドラインとして使用できます。

IEC 61508 には安全関連システムの企画から廃棄までライフ サイクル全体に対する詳細な要求事項が定義されており、安全関連の電気/電子およびプログラマブル製品に関する最も中心的な仕様と位置付けられます。

純粋な電気/電子システム以外を対象にする場合は、ISO 13849 と IEC/EN 62061 の内容をプログラマブル電子制御システムに適用します。

ISO 13849 は、機械制御システムの安全関連部の設計と実装に関する全般的な原則と具体的な要求事項を規定した国際規格で、一部のプログラマブル電子システムに加え、流体 (油、空気) およびエレクトロメカニカル システムにも適用されます。

IEC/EN 62061 は、機械類に特化した IEC/EN 61508 の派生規格です。IEC/EN 62061 は、あらゆる種類の安全関連機械/電気システムに関するシステム レベルの設計要件を規定しています。

電気/電子およびプログラマブル エレメントに関しては ISO 13849 と IEC 61508 でかなり重複した部分があり、IEC 61508 規格に準拠して設計されたエレメントは ISO 13849 の品質指標への対応が可能です。

このホワイト ペーパーはアーキテクチャ面に焦点を当てており、システマティックな問題については扱いません。システマティック故障に対して適応可能な対策の詳細は、ISO 13849-2 を参照してください。

用語について

IEC 61508 および IEC/EN 62061 では、安全関連システムの品質指標として SIL (Safety Integrity Level) を使用します。SIL には 1 ～ 4 のレベルがあり、数字が大きくなるにつれシステムの品質が向上します。

ISO 13849 では 2 つの指標を使用します。1 つはパフォーマンス レベル (PL) で、PL_a、PL_b、PL_c、PL_d、および PL_e があります (PL_e が最高品質)。各 PL 内にはカテゴリ (Cat.) と呼ばれる指標があり、Cat. B、Cat. 1、Cat. 2、Cat. 3、および Cat. 4 が定義されています。カテゴリはソリューションのアーキテクチャを定義したもので、Cat. 4 が最も信頼性が高くなります。ただし PL によっては実装に適さないカテゴリも存在します。たとえば PL_e は Cat. 1 アーキテクチャでは実装できず、Cat. 3 または Cat. 4 で実装します (どちらを選択するかはほかの要因を考慮して決定する)。

このホワイト ペーパーでは、PL とカテゴリが既知の場合の実装についてのみ取り上げます。システムの要求パフォーマンス レベルを PL_r とすると、各エレメントの PL は PL_r 以上とする必要があります。図 1 に示すように、各エレメントの PL は、カテゴリ、診断範囲 (DC)、平均危険側故障時間 ($MTTF_d$)、および共通原因故障 (CCF) を総合して決定します。つまり、Cat、DC、$MTTF_d$、および CCF の交わったところが各エレメントのパフォーマンス レベルとなります。

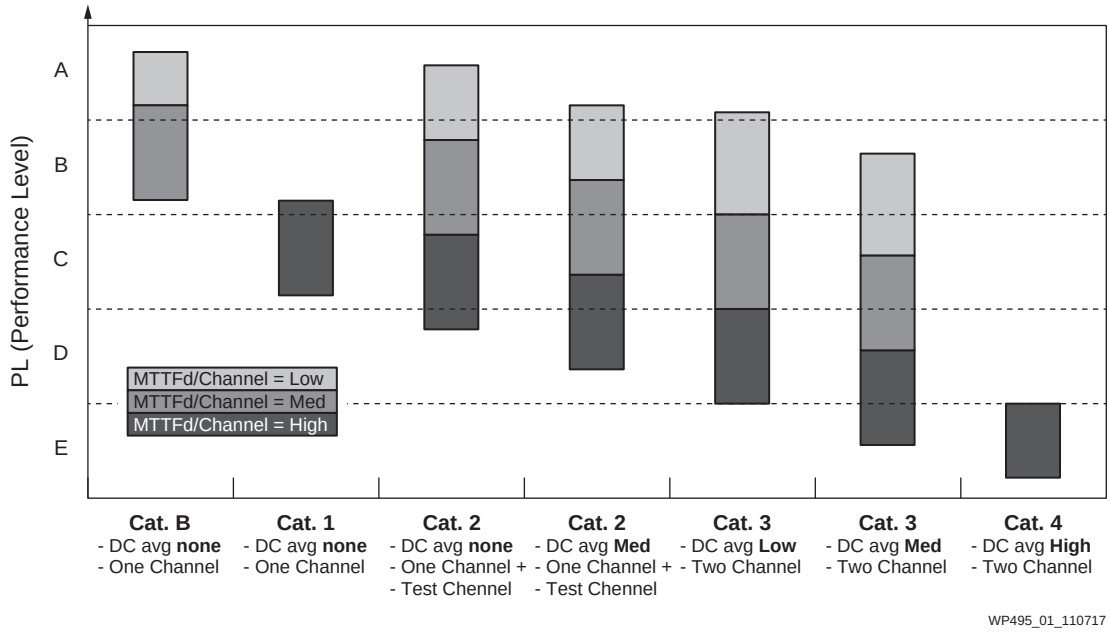

図 1: パフォーマンス レベルと Cat、DC、および $MTTF_d$ の関係

ZYNQ-7000 ALL-PROGRAMMABLE SOC

ザイリンクスの Zynq-7000 SoC と Vivado® Design Suite の TÜV SÜD 認証取得済みツール チェーンを使用して安全機能を実装すると、簡単な方法で ISO 13849 に準拠できます。Zynq-7000 SoC には 2 つの独立した、または相互に依存したサブシステムが含まれます。1 つはプロセッシング システム (PS) で、この中には 2 つの ARM Cortex-A9 CPU (L2 キャッシュ メモリを含む)、DDR メモリ コントローラー、および I/O ブロックが含まれます。もう 1 つはプログラマブル ロジック サブシステムで、この中には FPGA ロジックと統合ロジック機能が含まれます。

これらのサブシステムを独立して使用するか協調動作させるかは、安全要件に応じて決定します。Zynq-7000 SoC デザインをサポートしたザイリンクスの Vivado ツールは、IEC 61508 に準拠した機能安全アプリケーションの開発に使用できることが認証されています。

要求パフォーマンス レベル (PL_r) が PL_e のソリューションに関しては、仕様の要求事項を IEC 61508 の SIL3 に直接対応付けることができます。

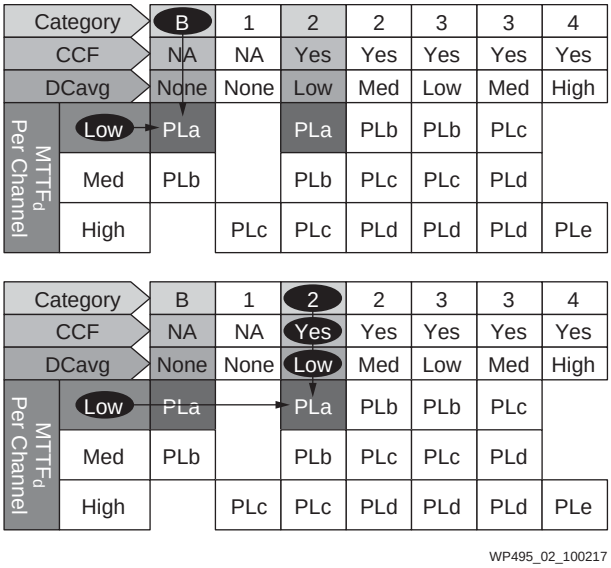

図 2: カテゴリ レベルと Cat、DC、および $MTTF_d$ の関係

表 1 に示すように、認証済み Vivado ツールを使用すると、一般的なデザイン要件を容易に満たすことができます。これらのツールとサポート資料を使用すると、使用するデバイスと安全機能に必要なリソースに基づいて PS/ロジックの FIT レートを容易に定量化できます。

表 1: パフォーマンス レベルと SIL の対応関係

パフォーマンス レベル (PL)	PFH: 1 時間あたりの危険側の平均故障率 [1/x]	SIL (IEC 61508/IEC 62061)
a	$\geq 10^{-5} \sim < 10^{-4}$	該当なし
b	$\geq 3 \times 10^{-6} \sim < 10^{-5}$	1
c	$\geq 10^{-6} \sim < 3 \times 10^{-6}$	1
d	$\geq 10^{-7} \sim < 10^{-6}$	2
e	$\geq 10^{-8} \sim < 10^{-7}$	3

Zynq-7000 SoC をロジック ソルバーとして使用する場合、同じデバイス上でのハードウェア非依存性を利用して 2 つの独立したチャネルを作成して Cat. 4 を実装できるため、PL_e をサポートできます。これは、IEC 61508 第 2 部、付属書 E に基づいて HFT = 1 をサポートした Zynq-7000 SoC デザインで実現できます。

カスタム FMEDA 診断に加え、ザイリンクスもいくつかのオンチップ診断ロジックを提供しています。これには、PS サブシステムの L1/L2 キャッシュ (パリティ) とオンチップ メモリ (パリティ)、およびロジック サブシステムのコンフィギュレーション RAM (ECC) とブロック RAM (ECC) 診断機能があります。また、カスタマーのユース ケースに基づいて各サブシステムの定量的解析を可能にする資料も提供しています。

パフォーマンス レベルの解析

ISO 13849 のパフォーマンス レベル評価に関しては、ほとんどの場合、目的のパフォーマンス レベルはいくつかのカテゴリで達成できます。通常は、要求パフォーマンス レベルの後にカテゴリを組み合わせることにより、実装要件を絞り込むことができます。

カテゴリ

ISO 13849 では、ハードウェア冗長性の観点から実装アーキテクチャを「カテゴリ」として定義しています。

Zynq-7000 SoC の機能は、ISO 13849 第 1 部 6.2 項に基づいてカテゴリ要件に容易にマップできます。

- Cat. B および Cat. 1 (1 チャネルで実装したロジック ソルバー) では、Zynq-7000 SoC ソリューションは PS またはプログラマブル ロジックのいずれかに安全機能を実装することも、これら 2 つの組み合わせに実装することもできます。
- Cat. 2 では、安全機能の動作を検証するための試験装置を追加します。試験装置が故障しても安全チャネルの動作に影響しないように、また、安全機能が故障しても試験装置の動作に影響しないように、試験装置は分離して実装する必要があります。Zynq-7000 SoC には PS とプログラマブル ロジックの 2 つの独立したリソースがあるため、試験装置は安全機能を実装していない方のリソースに実装できます。
- Cat. 3 および Cat. 4 では、安全チャネルの冗長化とチャネル間の相互監視が必要です。Zynq-7000 SoC では、2 つの安全チャネルを独立したリソースのそれぞれに実装します。つまり、1 つの安全チャネルを PS、もう 1 つの安全チャネルをプログラマブル ロジックに実装します。

$MTTF_d$ (平均危険側故障時間)

ISO 13849 では、チャネルごとの $MTTF_d$ を表 2 に示すメトリクスに基づき低、中、高の 3 つとして定義しています。

表 2: $MTTF_d$ インデックスと時間の対応関係

インデックス	範囲 (時間)
低	3 年 < $MTTF_d$ < 10 年
中	10 年 < $MTTF_d$ < 30 年
高	30 年 < $MTTF_d$ < 100 年

インデックスの境界に FIT の値を割り当てたものを表 3 に示します。

表 3: $MTTF_d$ インデックスと FIT レートの対応関係

インデックス	範囲 (故障率)
低	38,052FIT < $MTTF_d$ < 11,416FIT
中	11,416FIT < $MTTF_d$ < 3,805FIT
高	3,805FIT < $MTTF_d$ < 1,142FIT

Zynq-7000 SoC で全体の危険側 FIT を求めるには、安全機能の実装に使用するリソースの永久故障率から診断範囲を差し引いて 1/2 を掛けたものと、一時故障率から診断範囲を差し引いて 1/2 を掛けたものを合計します。1/2 を掛けているのは、故障の 50% が安全側故障で 50% が危険側故障という前提によるものです。

$$\text{全体の危険側 FIT} = 1/2\ [\ (PFR \cdot (1 - DC\%)) + (TFR \cdot (1 - DC\%))\ ]$$

ただし

PFR = 永久故障率
DC% = 診断範囲 %
TFR = 一時故障率

Zynq-7000 SoC の永久 FIT

ザイリンクスはデバイス信頼性に関するレポートを毎年 2 回、『デバイス信頼性レポート』(UG116) として発表しています。このレポートには、各ファミリの FIT レートなど継続的な信頼性試験の詳細な結果が示されています。2015 年下半期および 2016 年上半期の UG116 で報告されたすべての 7 シリーズのデータによると、7 シリーズおよび Zynq-7000 SoC の永久 FIT は 9FIT です。現在の永久 FIT は、Zynq-7000 デバイスのサイズに応じて最小規模のデバイスで 2FIT、最大規模のデバイスで 11FIT です (使用率 100% の場合)。危険側の永久 FIT は永久 FIT の半分であるため、使用率 100% の場合 1 ～ 5.5FIT となります。

Zynq-7000 SoC の一時 FIT

ザイリンクスでは、ブロック RAM およびコンフィギュレーション RAM のアレイを使用してザイリンクス プログラマブル デバイスに機能を作成しています。たとえば下半期の UG116 には、Zynq-7000 SoC の一時 FIT はブロック RAM で 66FIT/Mb、コンフィギュレーション RAM で 72FIT/Mb と記載されています。

Zynq-7000 SoC で最大規模の 7Z100 では、ロジックとエラー軽減後のブロック RAM およびエラー軽減後のコンフィギュレーション RAM (使用率 100%) を合計した危険側一時 FIT は、3,805FIT の要件を大きく下回ります。もちろん 3,805FIT は機械全体の上限値であるため、全体の危険側 FIT に与える Zynq-7000 SoC の影響を最小限に抑える必要があります。

コンフィギュレーション RAM とブロック RAM のエラー軽減には、ザイリンクスが提供するブロック RAM およびコンフィギュレーション RAM の内蔵 ECC といったカバレッジ ストラテジ (SEM-IP インフラストラクチャなど) を使用する必要があります。

診断範囲 (DC)

診断範囲とは、危険側故障を診断 (および場合によっては訂正) するために使用する手法および尺度のことです。これは、次のように定義されます。

DC = (検出した危険側故障) / (すべての危険側故障)

ISO 13849 では、DC は 4 つのレベルに分類されます (表 4 参照)。

表 4: DC レベルとパーセンテージの関係

レベル	範囲
なし	DC < 60%
低	60% < DC < 90%
中	90% < DC < 99%
高	99% < DC

最近のロジックおよびプロセッシング デバイスの永久故障は、1 ～ 50 の範囲です。

IC 設計で一時故障が最も多い構造はメモリで、その次にフリップフロップが続きます。現在、一般的に使われているメモリ保護方法にはいくつかの種類があります (表 5 参照)。

表 5: 各種診断機能と %DC の関係

方法	%DC
パリティ	60%
ECC および CRC	90%
冗長性	99%

フリップフロップ (レジスタ) の診断方法はデザインごとに異なりますが、一般的には何らかのエラー検出 (パリティ、ハミング符号など) を使用します。ロジックで使用される代表的な診断機能には、符号 (ハミング符号やその派生符号など)、エンドツー エンド CRC、冗長性、およびバス パリティなどがあります。

Zynq-7000 SoC の DC を解析する際は、PS とプログラマブル ロジックを別々に考える必要があります。PS では、L1 および L2 キャッシュがパリティで保護されています。オンチップ メモリ (OCM) もパリティで保護されています。DDR メモリは ECC で保護されています。PS の DC は、安全機能に使用される各機能ブロックの危険側故障の合計を、同じブロックに対して検出された危険側故障の合計で割って求めます。

サンプルの一時 FIT メトリクスを使用した例

データパスは USB から OCM を経由して CPU0 までとします。一時 FIT は USB が 2、OCM が 12、CPU が 33 です。

すべての危険側故障 = ½ (2+12+33) = 23.5FIT
検出されたすべての危険側故障 = ½ (2 · 0 + 12 · 0.6 + 33 · 0) = 3.6
PS の DC = 3.6/23.5 = 0.153 (すなわち 15.3%)

つまり、発生した危険側一時故障の 15% が検出されます。

この例からも明らかなように、OCM の DC が 100% でもチェーン全体で見ると危険側一時故障全体の 25.5% しか検出できません。

検出されたすべての危険側故障 = ½ (2 · 0 + 12 · 1.0 + 33 · 0) = 6
PS の DC = 6/23.5 = 0.255 (すなわち 25.5%)

この DC は、2 つの方法で大幅に改善できます。1 つはエンド ツー エンドのプロトコル チェックサム (CRC など) を使用する方法です。この場合、USB から OCM までのパスが完全にカバーされます。これは、一時故障は一般にポアソン分布に従った独立した事象 (稀にしか起こらない事象) であるためです。エラーのほとんどは、USB パケットの CRC を利用すると安全に軽減できます。この場合、CRC-5 (5 ビット) を使用するアドレス パケットがワースト ケースの条件となります。この結果、1-2-5= 0.968 すなわち 97% まで検出できるようになります。

プログラマブル ロジックの DC を計算するには、安全機能の実装に使用するロジック、ブロック RAM、およびコンフィギュレーション RAM の一時 FIT レートを考慮する必要があります。解析によると、プログラマブル ロジックに実装した安全機能の DC は、ザイリンクスの内蔵診断機能を有効にした場合に「中」レベルをサポートできます。

CPU とプログラマブル ロジックは別々のドメインに属しているため、プログラマブル ロジックを CPU の診断機能として使用する場合、IEC61508 第 2 部付属書 E 以外の共通原因故障解析は必要ありません。このようにして CPU とプログラマブル ロジックの間で結果を比較する方法を、ソフトウェアによる相互比較と呼びます。この比較のハミング距離、および比較結果を駆動する関連ロジックに基づき、最大 99% の DC を達成できます。CPU とプログラマブル ロジックという 2 つの異なるサブシステムを利用することにより、安全機能で発生する可能性のあるシステマティック故障の DC を高めることができます。

前述のように、一時 FIT は USB が 2、OCM が 12、CPU が 33 です。

検出されたすべての危険側故障 = ½ (2 · 0.96 + 12 · 0.96 + 33 · 0.95) = 22.4
PS の DC = 22.4/23.5 = 0.953 (すなわち 95.3%)

最終的な DC は、予想値にほぼ一致して「中」と「高」の境界付近となります。

共通原因故障 (CCF)

先の例では、カテゴリが上がって冗長性が必要になると CCF が重要になることを示しました。β として定義される共通原因故障率があまりに高いと、シングル チップに冗長性を実装することが問題となります。ISO 13849 の付属書 F に記載されている CCF 解析は、システム レベルで適用する必要があります。IEC/EN 62061 には、シングル チップにおけるチャネル独立性が十分明確に定義されていません。

1 つのチップに 2 つの安全チャネルが存在する場合は、IEC 61508-2 の付属書 E を参照することを推奨します。この付属書では、β_{ic} と最大許容 CCF (25%) が定義されています。Zynq-7000 SoC では、PS とプログラマブル ロジックのサブシステム間にかなりの独立性が確保されており、β_{ic} は十分低く抑えられています。このため、Zynq-7000 SoC で PS とプログラマブル ロジックに安全チャネルを 1 つずつ実装すれば、同じチップで 2 つの安全チャネルをサポートできます。

パフォーマンス レベル (PL) の割り当て

ここまでは、パフォーマンス レベルの評価に必要な定義について見てきました。次に、ある特定のパフォーマンス レベルをサポートするために必要なオプションについて説明します。

PL_a

PL_a のパフォーマンス レベルを達成する方法 (オプション) は 2 つあります (図 3)。

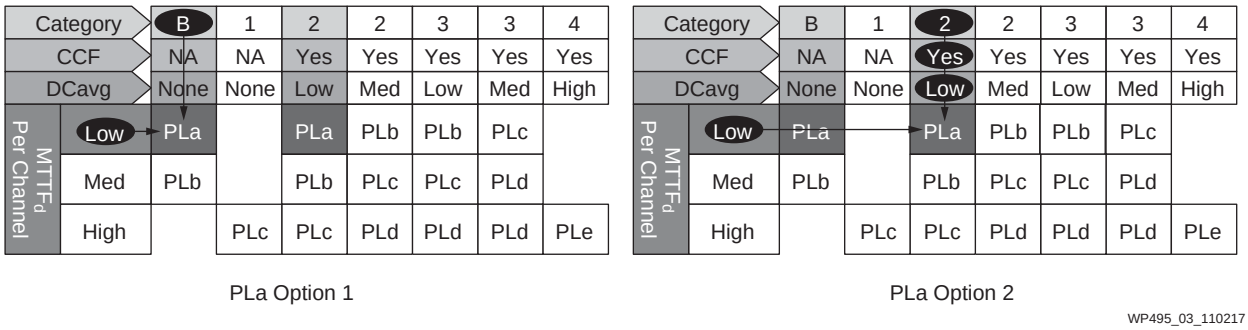

図 3: PL_a のオプション

Cat. B と Cat. 2 の違いは、カテゴリが高い方が安全機能のレジリエンス (回復力) が高いという規則に基づきます。Cat. B の場合、センサーやアクチュエーターの監視は行われず、1 つの障害で安全機能が動作を停止する可能性があります。Cat. 2 の場合、機能安全故障を検出するための診断試験装置が追加され、アクチュエーターの監視と冗長性が追加されます。

PL_a エレメントの場合、ロジック ソルバーに DC の要件はなく、3 年以上の $MTTF_d$ のみが要求されます。これは、故障率に換算すると 38,052FIT 未満です。プログラマブル ロジックの CRAM の使用率を約 20% とすると、Zynq-7000 Z-7020 デバイスの故障率は約 23FIT です。PLa のバジェットを 10% とすると、目標値は 3805FIT となります。このため、FIT のバジェットはかなりの余裕度で容易に満たすことができます。

PL_a Cat. 2 の場合、チャネルの DC を「低」レベルにする必要があります。PS のメモリ リソース、キャッシュ、および OCM に関しては、パリティ /チェックなどのシンプルなメカニズムで DC に関する要件を容易に満たすことができます。一般的なステート マシンでは、適切なハミング距離をとってステート マシンを設計するだけで、容易にロジックの DC を「高」レベルに設定できます。これは最も手早く簡単な方法で、追加のロジックもほとんど必要ありません。

PL_b

PL_b エレメントに関しては、PL_b ソリューションを得る方法は 4 つあります (図 4)。

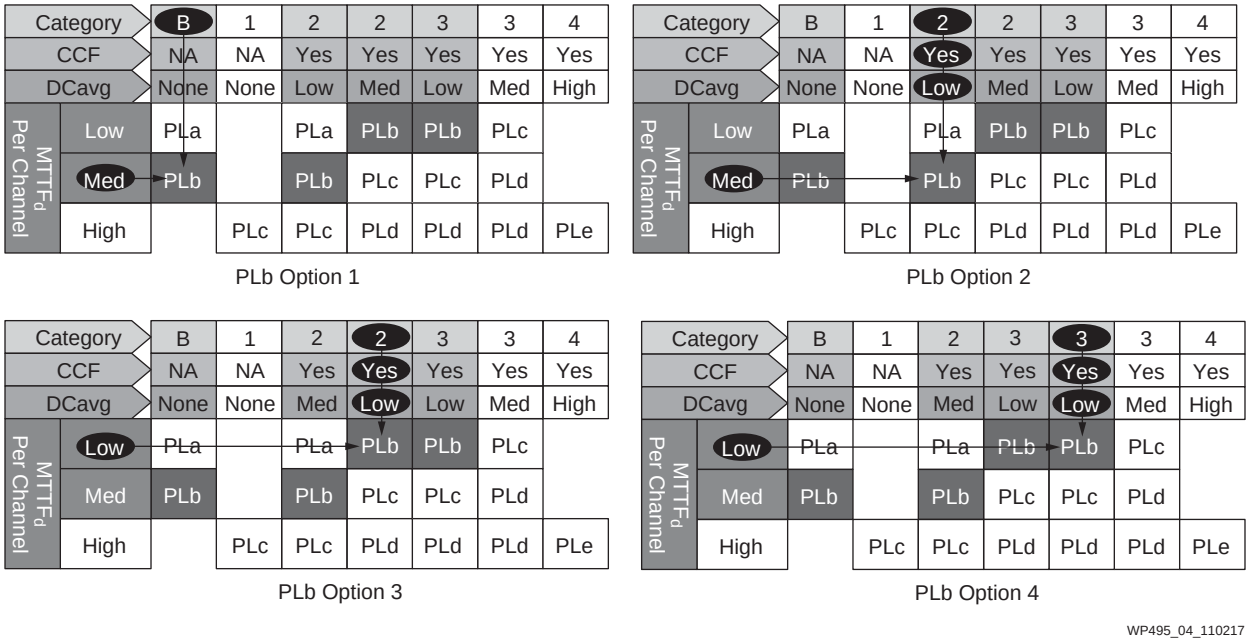

図 4: PL_b のオプション

オプションとしては、Cat. B で故障率 11,416FIT 未満 ($MTTF_d$ = 中) を達成する方法から、Cat.3 で故障率 38,052FIT 未満 (MTTFd = 低) を達成する方法まであります。

全体の許容 FIT レートは 38,052FIT から 11,416FIT まで減少します。この減少後の FIT レートは、ザイリンクスのオンボード パリティおよび ECC 診断機能を実装することにより、市販品の最大規模の Zynq-7000 SoC デバイスによって容易に満たすことができます。

PL_c

PL_c ソリューションの実装方法は 5 つあります (図 5)。Cat. 1 アーキテクチャ (Cat B に実証済みのコンポーネントと安全原則を追加したもの) を使用した場合、全体の許容 FIT レートは 11,416FIT から 3,805FIT (30 年に 1 回の故障率) まで減少します。また、故障検出率を上げるために試験装置を追加したアーキテクチャとすることもできます。

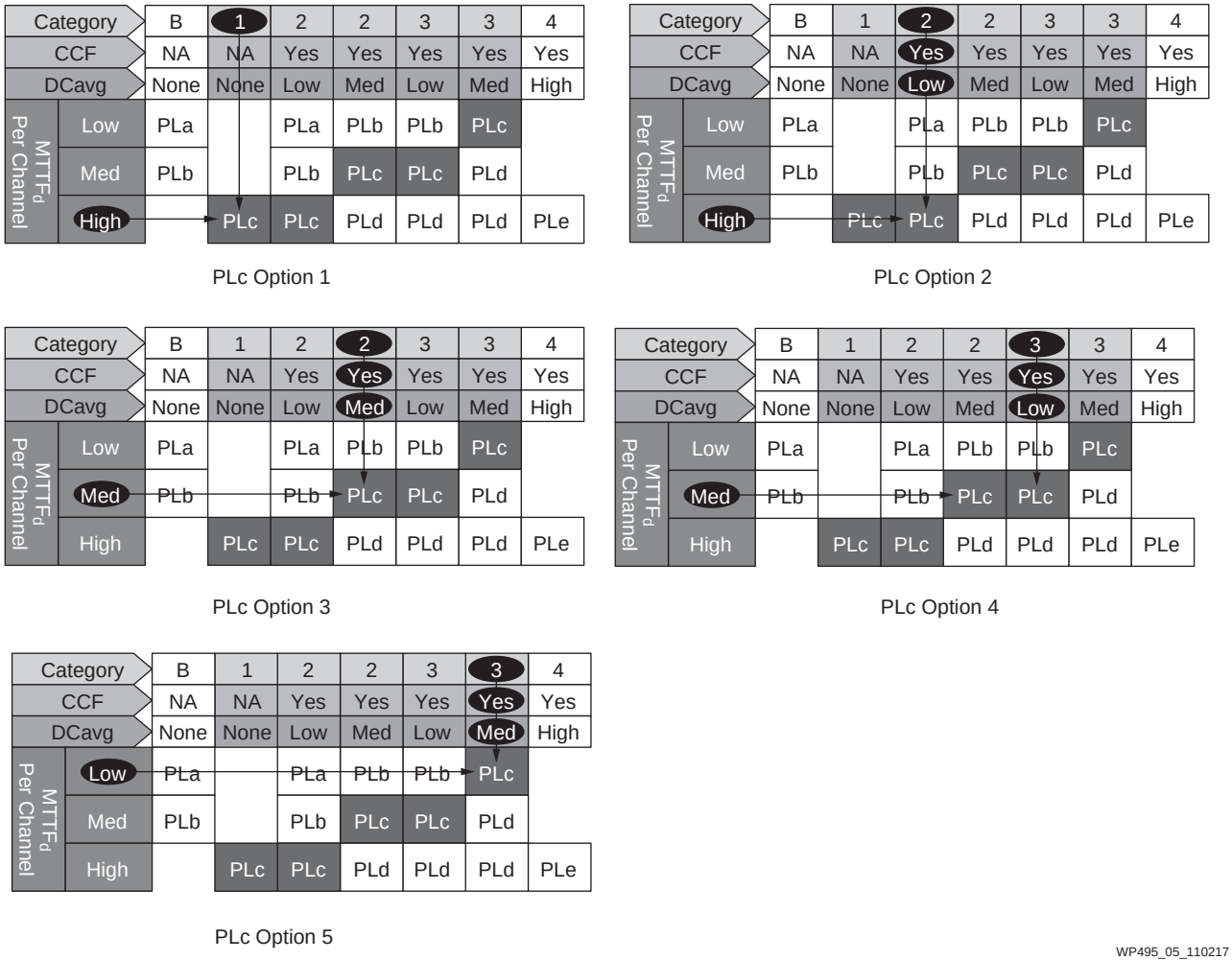

図 5: PL_c のオプション

ソリューションで使用するカテゴリは、$MTTF_d$ メトリクスを使用して実装の最も簡単なものを選択します。

PL_c Cat. 1 の場合、安全機能は任意の Zynq-7000 SoC デザインの PS またはプログラマブル ロジックに実装できます。

PL_c Cat. 2 の場合、PS への実装には DC が問題となる可能性があり、ソフトウェアによるチェッカーを追加する必要があります。どちらの場合も、PS とファブリックのいずれか一方に安全チャネル、もう一方に試験装置を実装すれば、IEC-61508 第 2 部、付属書 E に記載された CCF (β_{ic} = 8%) がチップに組み込まれます。

PL_c Cat. 3 の場合、2 つのチャネル間の相互比較 (またはチャネル間の相互監視) によって DC の問題を解決できます。ここでも、2 つの安全チャネルを PS とプログラマブル ロジックに分けて実装することにより、IEC-61508 第 2 部、付属書 E に記載された CCF がサポートされます。

PL_d

PL_d を達成する方法は 4 とおり考えられます (図 6)。そのうちの 3 つは、3,805FIT が必要です。どの方法も、何らかの冗長化が必要です。

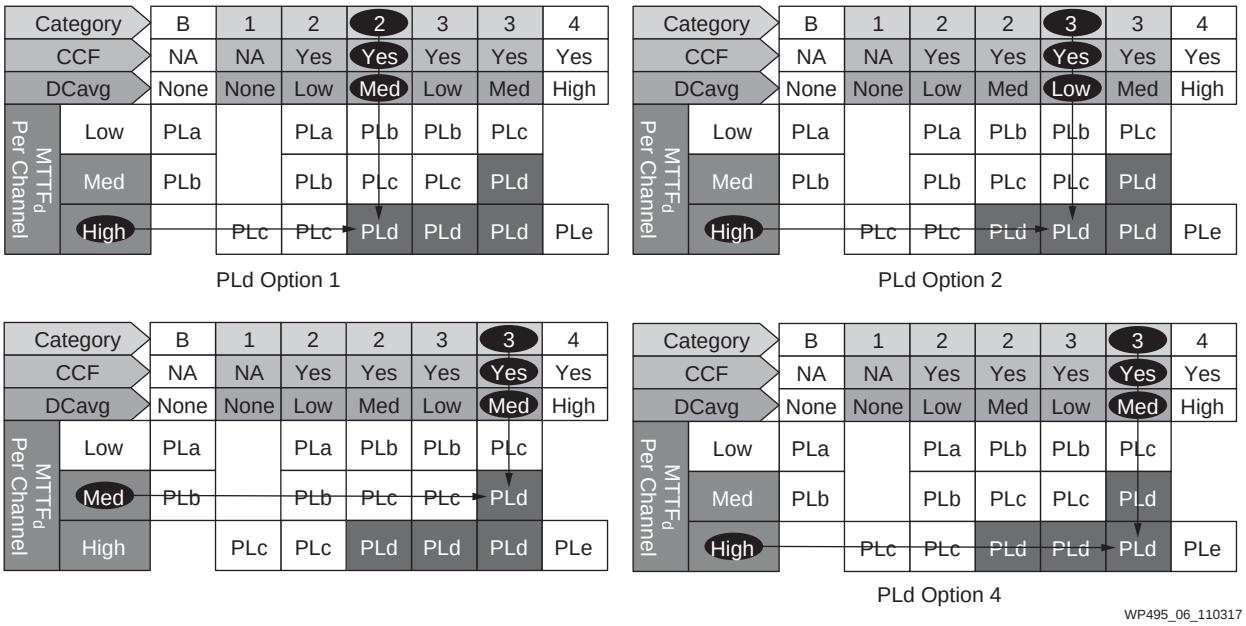

図 6: PL_d のオプション

Zynq-7000 SoC を PL_d Cat. 2 に使用するには 90% の DC が必要です。これを達成するには、プログラマブル ロジックに内蔵の診断機能を使用するのが最も簡単です。PS で 90% の DC を達成するには、安全チャネルとテスト チャネルの相互比較をソフトウェアで実装します。または、レジスタ ステート チェッカーやエンド ツー エンドのデータパス CRC などの診断機能をユーザーが独自に作成する方法もあります。

Zynq-7000 SoC で PL_d Cat. 3 ソリューションを実装する場合、「中」レベルの $MTTF_d$ と「高」レベルの DC の組み合わせ、または「高」レベルの $MTTF_d$ と「低」レベルの DC の組み合わせのいずれかをユーザーが選択できます。全体的な FIT レートは、すべての Zynq-7000 SoC デバイスで 3,805 を大きく下回ることができます。90% の DC は、2 つのチャネル間のソフトウェアによる相互比較 (またはチャネル間の相互監視) で達成できます。PS とプログラマブル ロジックでそれぞれ 1 つずつ安全チャネルをサポートするには、IEC61508 第 2 部、付属書 E を使用した CCF 解析 (β_{ic}) が必要です。ソフトウェアによる相互比較だけで「高」レベルの DC を達成することも可能ですが、具体的な方法はアプリケーションごとに異なり、適切な解析を実施してアセッサーにエビデンスを提出する必要があります。

ここでは、Zynq-7000 のうち最も一般的なデバイスである Z-7020 を例に解析してみます。

- ファブリック全体の FIT (Z-7020 の使用率 25% の場合): ロジック 16、コンフィギュレーション RAM 331.7、ブロック RAM 89.9
- すべての危険側故障 = ½ (16 + 331.7 + 89.9) = 437.6FIT
- 検出されたすべての危険側故障 = ½ (16 · 0 + 331.7 · 0.9 + 89.9 · 0.9) = 379.4FIT
- ファブリック (使用率 25%) の DC = 379.4/437.6 = 0.867 (すなわち 86.7%)
- 使用率 100% の場合の最大一時 $MTTF_d$ = 116FIT

これは理論上の計算です。プログラマブル ロジックの実際のデザインは、ロジック、コンフィギュレーション RAM、およびブロック RAM の使用率が異なります。Vivado ツールを使用すると、デザインにおけるそれぞれの正確な使用率を調べることができます。

この仮定の例で説明したように、プログラマブル ロジックに内蔵の診断機能による実際の DC は、ユーザー デザインにおけるロジック、コンフィギュレーション RAM、およびブロック RAM の使用率により変化します。いずれの場合も、プログラマブル ロジックの一時 $MTTF_d$ は 700FIT を超えないようにする必要があります。90% の DC は、2 つのチャネル間のソフトウェアによる相互比較 (またはチャネル間の相互監視) で達成できます。PS に安全チャネルを実装し、プログラマブル ロジックに冗長安全チャネルを実装するには、IEC61508 第 2 部、付属書 E を使用した CCF 解析 (β_{ic}) が必要です。ソフトウェアによる相互比較だけで「高」レベルの DC を達成することも可能ですが、具体的な方法はアプリケーションごとに異なり、適切な解析を実施してアセッサーにエビデンスを提出する必要があります。

PL_e

PL_e Cat. 4 ソリューションは、冗長化を採用した IEC 61508 SIL3 に相当すると ISO 13849 で説明されています。Zynq-7000 SoC はクロック、電源、および物理回路が分離されており、2 チャネル アーキテクチャの要件を満たしているため、シングル チップでハードウェア冗長化をサポートします (図 7 参照)。

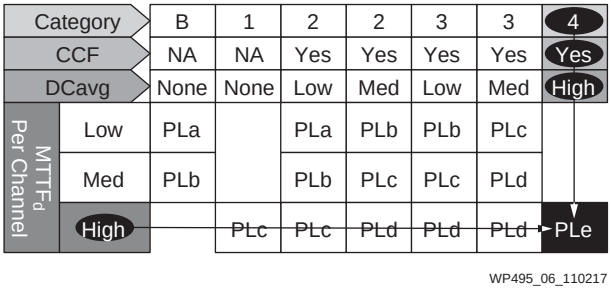

図 7: PL_e

「高」レベルの $MTTF_d$ を達成するための FIT 要件は、最大規模の Zynq-7000 SoC デバイスでザイリンクスの内蔵診断機能を有効にすることでサポートされます。

PL_e を達成する上で最も困難なのは、「高」レベルの DC を達成することです。これには、外部デバイスを使用して CCF への依存性を最小化するなど、いくつかの手法を適用できます。このシングル チップ ソリューションでは、ソフトウェアによる相互比較によって DC を大幅に高めることができます。これ以外に、CCF をさらに低減させる手法もいくつかありますが、その具体的な効果は個々のアプリケーションに適用してみないとわかりません。このため、適用した手法で危険側故障の 99% を検出できることをエビデンスとして提出するには、適切な解析が必要です。

組み合わせ例

図 8 のブロック図に示すように、Cat. 3 および Cat. 4 ソリューションで Zynq-7000 SoC を使用する場合、各チャネルの診断結果を結合するシンプルな外部エレメントと、シンプルなウォッチドッグが必要です。

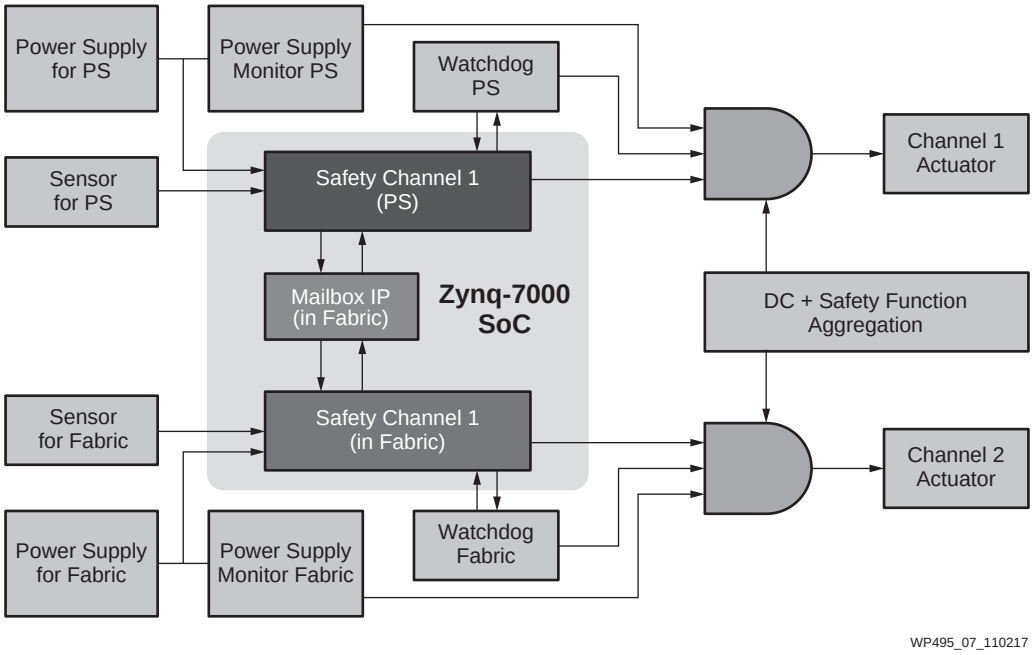

図 8: Zynq-7000 SoC の 2 チャネル ブロック図

複雑なプログラマブル安全エレメントのほとんどに共通することですが、外部監視エレメントはシンプルなロジックを使用して外部で結合します。ここでは、パワー グッドおよび外部ウォッチドッグ エレメントを使用した安全機能の品質確保に必要なロジックの集まりを示しています。

まとめ

Zynq-7000 SoC ソリューションを使用すると、ISO 13849 に準拠したロジック ソルバーを簡単な方法でサポートできます。ザイリンクス Vivado Design Suite の認証済みツール チェーンを利用すると、Zynq-7000 SoC 独自のアーキテクチャ実装を活かして ISO 13849 の全カテゴリ アーキテクチャをサポートでき、すべてのパフォーマンス レベル (PL) で共通原因エラーの軽減および診断範囲 (DC) の要件を満たすことができます。

機能安全に向けたザイリンクス製品の詳細は、次のリンク先を参照してください。
https://japan.xilinx.com/applications/industrial/functional-safety.html

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
2017 年 11 月 21 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になります。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 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。