

高信頼性システムおよび 情報セキュリティ・システム向けのデザイン・セパレーション

これまでシステム設計は、冗長性を持つことで信頼性を実現していましたが、コンポーネント数、ロジック・サイズ、システム消費電力、そしてコスト増加の原因となっていました。アルテラの「デザイン・セパレーション機能」は低消費電力、小型化、高い機能性を達成しながら、高い信頼性と情報セキュリティを維持するという、相反するニーズに応えます。

はじめに

今日、FPGA はあらゆる箇所で採用されるようになりました。その用途は、従来のグルー・ロジック・インターフェースから、コア・インターネット・ルーターや高性能コンピュータ・システムで使用する先進の情報処理システムへと進化してきました。この進化の中で常に課題となってきたのは、少ないスペースで多くの機能を集積しながら、消費電力とコストを抑えるという点でした。

高い信頼性を必要とするシステム（高信頼性システム）の設計も、期待される信頼性を維持しながら、システム・サイズ、消費電力、コストを低減することが求められるという、似たような経験をしてきました。これまで、高信頼性システムの設計においては、冗長性を持つことで信頼性の問題に対処してきましたが、この冗長性がコンポーネント数、ロジック・サイズ、システム消費電力、そしてコストの増加の原因となっています。このような信頼性に対する要件と特性は、情報セキュリティ・システム、航空宇宙システム、産業機器業界の安全システムを含む、他のシステム設計にも当てはまることです。

アルテラは、このようなアプリケーションで必要とされる低消費電力、小型化、高い機能性を達成しながら、高い信頼性と情報セキュリティを維持するという、相反するニーズに応えるソリューションを開発しました。Altera® Quartus® II 開発ソフトウェアと Cyclone® III LS FPGA で実現するデザイン・セパレーション機能は、設計者に確立されている信頼性の高い冗長設計手法を、単一 FPGA ベースのアーキテクチャに簡単に組み込む方法を提供します。

フォールト・トレランスに対するニーズ

信頼性工学に対するニーズは、第二次大戦における陸海軍設備の可用性（利用状況）に関する研究以来、米国防総省 (DoD) が推進してきました。例えば、当時爆撃機の平均故障間隔 (MTBF) は 20 時間未満であり、その修理費は元の購入価格の 10 倍を超えることが判明したなどです。それ以降、システム設計のトータル・ライフサイクル・コストという概念が、設計とシステムの選択における重要な指標として使用されています。

高保証の暗号システム（高保証暗号システム）も同様の歴史的背景を持っています。暗号システムにおける障害は、軍用システムではセキュリティ、商用システムでは商取引の観点から、システムのトータル・ライフサイクルに影響を与えます。このようなことから、高保証暗号システムには高信頼性システムと同じような設計および解析要件を有しています。

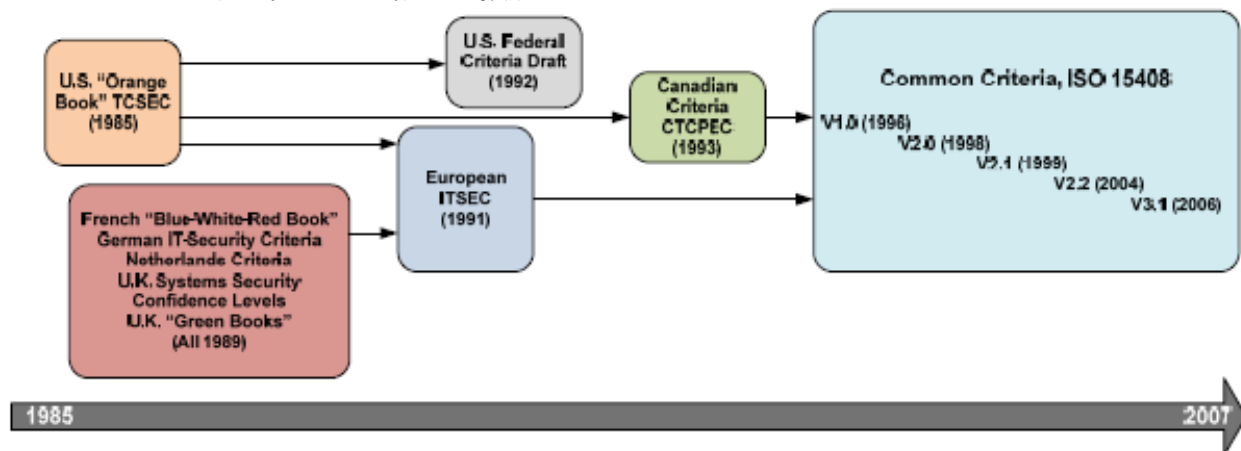
いずれの場合も、設計者の目標は、特定のアプリケーションにおいて PCB のサイズを縮小し、必要な部品点数を削減することです。これは数十年にわたりエレクトロニクス産業のトレンドであり、実現するためのソリューションは最初のシステム・オン・チップ (SoC) ASIC ソリューションから SoC FPGA ソリューションに進化しています。SoC ASIC ソリューションは、外部のデジタル論理を 1 つのデバイスに集積しました。この手法は、ASIC 開発のコストとスケジュールが、市場価格と時間的要因を上回るまでは順調に進みました。ASIC のコスト上昇に伴い、設計者は、論理回路を 1 チップに統合可能な性能とロジック集積度を持つ FPGA に移行しました。SoC デザインは長年にわたり安定して成長してきましたが、FPGA の設計と複雑さにより、冗長設計の統合は困難でした。分離され独立したデータパスを検証するための解析が必要なため、多くのシステムおよびセキュリティ・アナリストの間では扱いにくい問題と見られてきました。

アルテラは、認証機関と協力することで、複雑な FPGA デバイス解析の問題を解消し、個々の独立したデータパスを保証しています。最初からこの解析を考慮して FPGA ツールとデータ・フローを設計しているため、フェイルセーフ設計を 1 つの FPGA アーキテクチャに統合することができます。そのため設計者は、SoC における市場目標を達成するだけでなく、高信頼性および高保証アプリケーションの要件を満たすことも可能となります。

情報セキュリティ・アプリケーション

拡大する情報セキュリティ機器では、暗号化装置の設計と実装には一定水準の信頼性が求められます。複雑なシステム・デザインの保証には、信頼のおける設計基準およびシステム評価基準が必要になります。セキュリティ設計基準および評価を行う機関はいくつか存在しますが、個々の設計要件と評価基準の説明はここでは割愛し、基準の進化についての概要を図 1 に示します。

図 1. セキュリティ基準における設計と解析の進化



情報技術 (IT) システムは、最も顕著な影響を情報セキュリティに与えます。インターネット経由でアクセス可能なインフラストラクチャー制御システム、および企業/個人情報が増加しており、機密情報とシステムを世界中のハッカーから防護するためにも、IT システムがますます頼りにされています。

インターネットにおける情報セキュリティ確保のためには、ウイルス対策のためのデータ検査だけでなく、IPSec、HTTPS、およびその他のアプリケーションを使用して機密情報を保護する必要があります。HTTPS 暗号アルゴリズムは、一般にコンピュータ・プラットフォーム上で稼働するソフトウェアに組み込まれますが、IPSec と仮想プライベートネットワーク (VPN) の暗号化アプリケーションは、一般により高い性能が必要で、暗号化ハードウェアに大きく依存します。ネットワーク IT 機器の評価は、システム全体の信頼性を確保する上でも必要になります。

この信頼性は、必ずコモクライテリア (Common Criteria)、または連邦情報処理規格 (FIPS) 140-2/ 140-3 のセキュリティ要件に適合している情報セキュリティ・レベルにおいて、各 IT コンポーネントのハードウェア解析で実証する必要があります。図 1 に示すように、ハードウェア解析の複雑さが重要な要素になります。評価は徹底的に行われるため、システムのデザイン・サイクルが重要といえます。

図 1. FIPS 140-2 Security Requirements Summary

#	項目	セキュリティ・レベル1	セキュリティ・レベル2	セキュリティ・レベル3	セキュリティ・レベル4
1	暗号モジュールの仕様	暗号モジュールの仕様、暗号境界、承認済みアルゴリズム、および承認済み動作モード すべてのハードウェア、ソフトウェア、およびファームウェアのコンポーネントを含む、暗号モジュールの詳細 モジュール・セキュリティ・ポリシーの声明			
2	暗号モジュールのポートとインタフェース	必須およびオプションのインタフェース すべてのインタフェース、すべての入/出力データパスの仕様		他のデータ・ポートから論理的に分離された保護されていない重要なセキュリティ・パラメータ用のデータ・ポート	
3	役割、サービス、および認証	必須およびオプションの役割とサービスの論理的分離	役割ベースまたは ID ベースのオペレータ認証	ID ベースのオペレータ認証	
4	有限状態モデル	有限状態モデルの仕様 必須およびオプションの状態の仕様 状態遷移図と、状態遷移の仕様			
5	物理的セキュリティ	量産グレードの装置	ロックまたはタンパの証拠	カバー/ドアのタンパー検出および応答	タンパー検出および応答用遮蔽 EFP/EFT (環境故障保障/環境故障試験)
6	動作環境	単一オペレータ 実行可能コード 承認済みの統合技術	指定された任意のアクセス制御機構と監査を備え、EAL2 において評価された、基準となる PP	基準となる PP + EAL3 において評価された信頼性のあるパス + セキュリティ・ポリシーのモデル化	基準となる PP + EAL4 において評価された信頼性のあるパス
7	暗号鍵管理	鍵管理メカニズム: 乱数および鍵の生成、鍵の確立、鍵の分配、鍵の入/出力、鍵の保存、および鍵のゼロ化		手動で確立されたシークレットおよびプライベート鍵は、暗号化あるいは知識分離手順によって入/出力する必要がある	
		手動で確立されたシークレットおよびプライベート鍵は、平文テキストで入/出力可能		手動で確立されたシークレットおよびプライベート鍵は、暗号化あるいは知識分離手順によって入/出力する必要がある	
8	EMI/EMC	7 CFR FCC Part 15, Subpart B, Class A (業務用) 適用される PCC 要件 (無線機用)		7 CFR FCC Part 15, Subpart B, Class B (家庭用)	
9	自己テスト	電源投入テスト: 暗号化アルゴリズム・テスト、ソフトウェア/ファームウェア統合テスト、重要機能テスト、条件付きテスト		統計的 RNG テストは要求に応じて実施	統計的 RNG テストは電源投入時に実施
10	設計保証	構成管理 (CM) 安全なインストレーションと生成 設計とポリシーの一致 ガイダンス文書	CM システム 安全な配布 機能仕様	高級言語の実行	公式モデル 詳細な説明 (非公式な証明) 事前条件と事後条件
-	その他の攻撃の緩和	攻撃緩和の仕様 (現時点でテスト可能な要件がない)			

商用暗号化

金融業界は、商用暗号化と暗号化装置の推進力となっています。インターバンク / イントラバンクの電子データ交換 (EDI) 処理用のセキュリティ開発から、公共の現金自動預入支払機 (ATM)、e コマースを推進する高性能の暗号化アプリケーションまで、金融産業の成長によって、情報セキュリティの必要性は拡大傾向にあります。

軍用産業における情報セキュリティに対するニーズと同様に、商用 e コマースにおいても、暗号化ハードウェアの設計と評価の基準が、広く受け入れられています。金融業界では暗号化方法のインターオペラビリティが求められており、このマーケットにおける重要な差別化要因となっています。つまり、商取引は国境を越えて世界中に広がっているため、このマーケットで使用できる暗号化装置の開発が必要になるのです。商用のセキュリティ導入を困難にしているのは、暗号法が国際武器輸出規制 (ITAR) に基づく、規制技術に分類されているためです。

高性能の e コマース暗号化装置は、FIPS 140-2 認定を受けた暗号化モジュールの製造に必要な専門性と長期間にわたる設計に投資することが可能な、IBM、Sun 等の大規模なサーバー・メーカーによって、主に開発されています。

高信頼性アプリケーション

産業用アプリケーションにおいても、アルテラの FPGA を使用して、デザイン・セパレーションを行い、独立性を保つことができます。

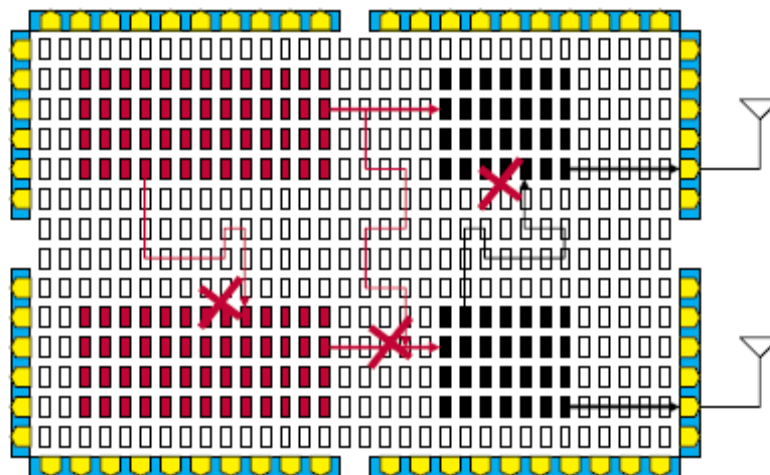
例えば、自動車で使用されるエンベデッド・コントロール・ユニット (ECU) は、その数が増加するに従い、複雑さと機能性も増えています。自動車産業の競争性により、ECU 設計者は信頼性を保証しながらサイズとコストを削減しなければなりません。デザイン・セパレーション機能を活用すると、1つの FPGA チップ内部で冗長回路を分離できるため、ハードウェア・コンポーネント数を削減しながら、故障の分離を実現することが可能となります。

デザイン・セパレーション・ソリューション

情報セキュリティ・アプリケーションや高信頼性アプリケーションにおいて、ロジックを分離し、機能を独立させるためには、これまでは少なくとも 2 チップ構成が必要でした。複数のチップを使用することにより、うち 1 つのデバイスで障害が検出されても、残りの部分が影響を受けないよう保証しています。デザイン・セパレーションが重要である例として、データ暗号化が必須である金融アプリケーションが挙げられます。障害発生によって偶発的にパスが形成されても、デザイン・セパレーションを行ってれば、データが他の部分に漏洩することを防ぐことができます。また高い信頼性が重要である例として、産業機器システムが挙げられます。産業機器システムでは、設備の一台に障害が発生すると、すべての製造ラインが停止するおそれがありますが、障害が発生しても冗長回路がシステム制御を継続し、ダウン・タイムをほとんど発生させずに済みます。

Quartus II 開発ソフトウェアのデザイン・セパレーション機能を使用することで、1つの FPGA チップ内部に重要な機能を分離し、分離した状態を保つことができます。この分離回路はアルテラの LogicLock™機能を使用して生成され、分離箇所をデバイスの特定部分に割り当てることができます。デザイン・セパレーション・フローを「有効」にすると、図 2 に示すように、それぞれの機密性の高い箇所に自動的にフェンス、あるいは「キープアウト」エリアが関連付けられます。この方法により、他のロジックが隣接して配置されることがなく、フォールト・トレランスのレベルを 1 段階引き上げることができます。

図 2. 高信頼性 / 情報保障システムのためのデザイン・セパレーション



しかしながら、真の意味で「分離」を実現するには、配線も分離する必要があります。そのため、すべての配線をデザイン・パーティションの LogicLock エリア内に制限しています。これによりフェンス・エリア内にはロジックも配線も存在せず、デバイス内の他の機能との物理的分離が保証されます。これにより、2つのデバイスを使用して分離を確保した場合と同じこととなります。

アルテラは、分離を保証すべく Cyclone III LS のファブリック・アーキテクチャを設計、厳格に評価、および最適化しており、最小のフェンス・サイズでフォールト・トレランスを向上し、チップ・リソースの 80% 以上を活用可能にしています。またデザイン・セパレーション・フローでは、バンク切り替えルールが利用でき、ファブリック内で作成された重要な箇所においても、確実に I/O を拡張することが可能です。Cyclone III LS パッケージは、このような I/O の分離もサポートするよう設計されています。

まとめ

高信頼性システムと情報保証システムの間には、設計上の要件に類似点が多く存在します。どちらのシステムも、ハードウェア障害の際に適切なオペレーションを確保するために冗長性を必要とするため、デザイン・セパレーションと独立性が求められます。従来、冗長性はボードレベルで実現していたため、システム・サイズ、重さ、消費電力およびコストの増加を招いてきました。このような問題を避けるために、低消費電力 FPGA プロセスと高保証デザイン・フローを組み合わせることで、厳格な国家安全保障局 (NSA) のフェイルセーフ・デザイン・アナリシス (FSDA) 要求事項に適合しています。

デザイン・セパレーションと独立性を保証することで、冗長回路をボードレベルから、1つの FPGA デバイスに移行することができます。低消費電力、高いロジック集積度、およびデザイン・セパレーション機能を組み合わせて利用することで、高信頼性、高保証を必要とする暗号化システム/産業機器システムにおいて、プロブラマブル・ロジックを使用して設計開発とスケジュールのリスクを最小化し、実績のあるインクリメンタル・コンパイル・デザイン・フローを使用して、生産性を向上させることが可能となります。

詳細情報

- Cyclone III FPGA—セキュリティ：
www.altera.com/products/devices/cyclone3/overview/security/cy3-security.html
- Webcast: 「冗長性と情報セキュリティのための FPGA デザインのパーティショニング」：
www.altera.com/education/webcasts/all/wc-2009-partitioning-fpga-redundancy.html
- 資料: Cyclone III デバイス関連資料
www.altera.com/products/devices/cyclone3/literature/cy3-literature.jsp
- AN 567: Quartus II デザイン・セパレーション・フロー：
www.altera.com/literature/an/an567.pdf
- 共通の脅威からの FPGA デザインの保護：
www.altera.com/literature/wp/wp-01111-anti-tamper.pdf
- Quartus II 開発ソフトウェア サブスクリプション・エディション：
www.altera.com/products/software/quartus-ii/subscription-edition/qts-se-index.html

謝辞

- Paul Quintana, Sr. Technical Manager, Military Business Unit, Altera Corporation
- Juwayriyah Hussain, Sr. Product Marketing Engineer, Low-Cost Products, Altera Corporation



101 Innovation Drive
San Jose, CA 95134
www.altera.com

Copyright © 2009 Altera Corporation. All rights reserved. Altera, The Programmable Solutions Company, the stylized Altera logo, specific device designations, and all other words and logos that are identified as trademarks and/or service marks are, unless noted otherwise, the trademarks and service marks of Altera Corporation in the U.S. and other countries. All other product or service names are the property of their respective holders. Altera products are protected under numerous U.S. and foreign patents and pending applications, maskwork rights, and copyrights. Altera warrants performance of its semiconductor products to current specifications in accordance with Altera's standard warranty, but reserves the right to make changes to any products and services at any time without notice. Altera assumes no responsibility or liability arising out of the application or use of any information, product, or service described herein except as expressly agreed to in writing by Altera Corporation. Altera customers are advised to obtain the latest version of device specifications before relying on any published information and before placing orders for products or services.