アーキテクチャと形式的検証の協調による超ディペンダブルVLSI

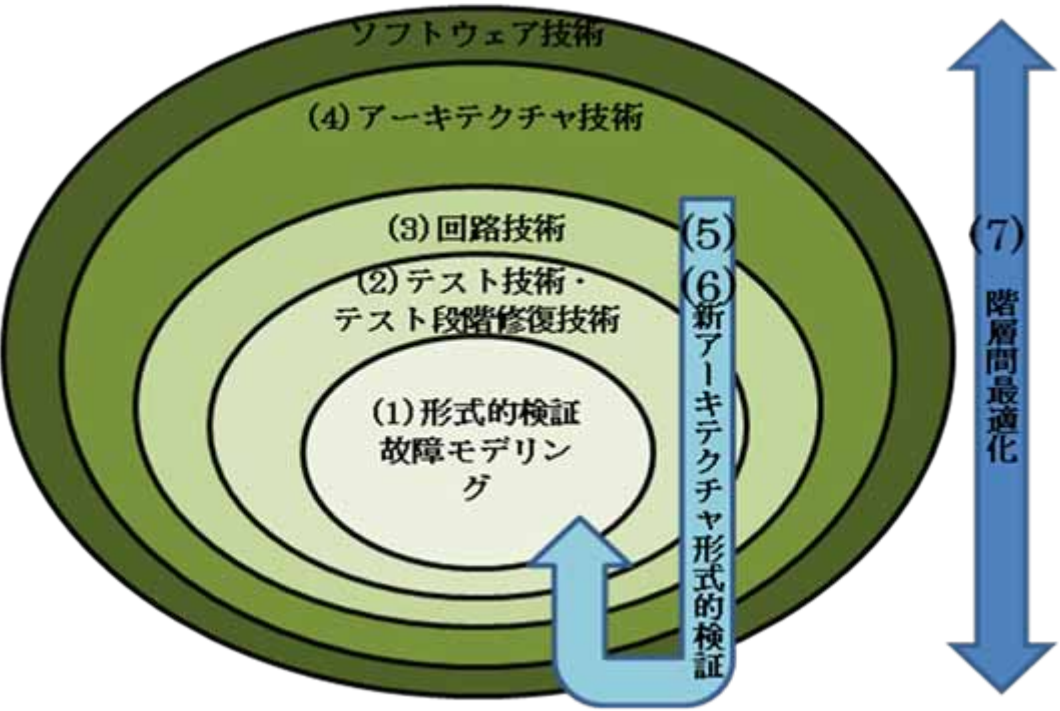
戦略的創造研究推進事業
「ディペンダブルVLSIシステムの基盤技術」

東京大学　大学院情報理工学系研究科　坂井　修一（代表者）
五島　正裕

東京大学　大規模集積システム設計教育研究センター（VDEC）　藤田　昌宏

東京工業大学　大学院情報理工学研究科　吉瀬　謙二

全体マップ： ディペンダビリティ階層



それぞれの階層で技術開発
＋ 全体を通した最適化
＋ 最新アーキテクチャの検証

Best Effort Design
Run Time Recovery

前半3年： 方式検討、基本設計、実験システム構築・評価
後半2年： プロトタイプ試作と評価、要素技術の統合

2008/12/6

(1) 形式的検証手法

- C/C++言語ベースVLSI高位設計
- 対話・自動ドキュメント化のための要素技術

(2) テスト技術・テスト段階修復技術

- テスト容易化・検証容易化を実現する設計手法
- フィールドプログラマブル性を部分的に導入可能な合成手法 = テスト段階でデザインミスをとる

(3) 回路技術

- タイミング制約緩和回路

(4) アーキテクチャ技術

- 故障検出・回復機構の提案・実現
- 制御部を含めたFPGA仮想化
- 耐故障高機能ルータ
- 超ディペンダブルプロセッサ

(5)(6) 新アーキテクチャ形式的検証

- ディペンダブルアーキテクチャ技術自体を形式的に検証
- 既存のアーキテクチャ、最新のアーキテクチャを形式的に検証

(7) 各設計階層間のディペンダビリティ役割分担を最適化

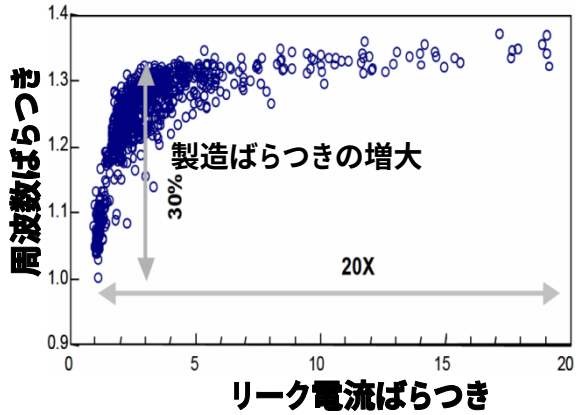
期待される成果

- VLSIユーザ
  - 設計の正しさの向上、リコール減少
  - VLSI製作後のバグフィックスや機能修正による利便性向上
  - 保証される動作速度の向上
  - 宇宙・深海などの環境でも高い信頼性をもって情報処理ができるようになる
- VLSI設計・製造者
  - 「上位で設計の正しさを保ちながら、設計の詳細化を行い実装設計につなげる」ことができるようになる
    - 設計効率一桁向上
  - 並列処理・パイプライン処理・キャッシュなどの機構が効率的に検証できるようになる
  - 「最悪値の積算」が、「典型値＋回路・アーキテクチャによる補正」によって緩和される

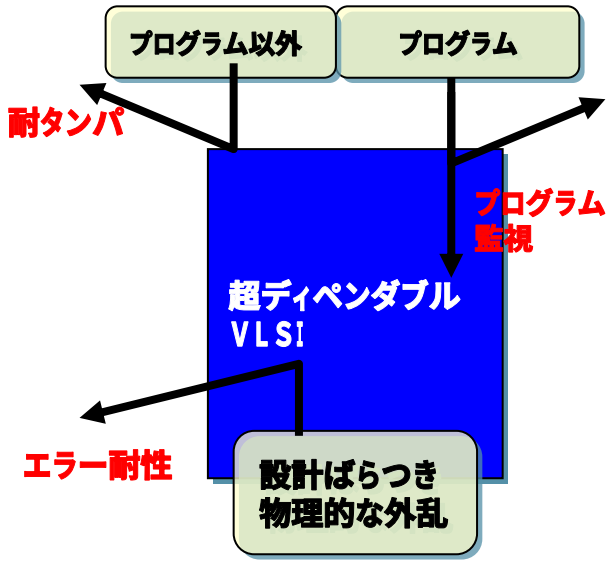
- 成果物・デモ
  - 形式検証ツール
    - 等価性検証ツール
    - 上位設計からの製造故障用テスト生成ツール
  - テスト段階修復技術
    - インフィールドで論理修正が可能な論理回路生成（論理合成）ツール
  - ディペンダブル回路技術
    - 回路（IP）
  - ディペンダブルアーキテクチャ技術
    - 要素技術仕様、IP
    - PVTIテストベッド
    - 耐故障テストベッド
  - デモ・展示：
    - 形式検証デモ
    - 試作VLSI
    - 超ディペンダブルVLSIテストベッド
  - 特許、知財
  - 書き物
    - 論文：ジャーナル、国際会議、研究会、全国大会
    - 報告書

回路技術・アーキテクチャ技術による設計制約の緩和 ／ 動的故障検知・回復

- 設計ばらつき
  - best effort design
  - run time recovery
- タイミング制約緩和技術
  - 遅延保証フリップフロップ
  - 耐タイミング故障クロッキング方式
- 故障検知・回復機構
  - 検知・コミットの抑止・全体機構
  - 制御回路を含む仮想化： 穴のない耐故障性
- ディペンダビリティ向け多機能ルータ
  - 送受信パケットのレベルで冗長実行を実現
- 超ディペンダブルプロセッサ
  - 耐故障性
  - 耐タンパ性
  - プログラム監視
  - 性能・電力との最適なトレードオフ

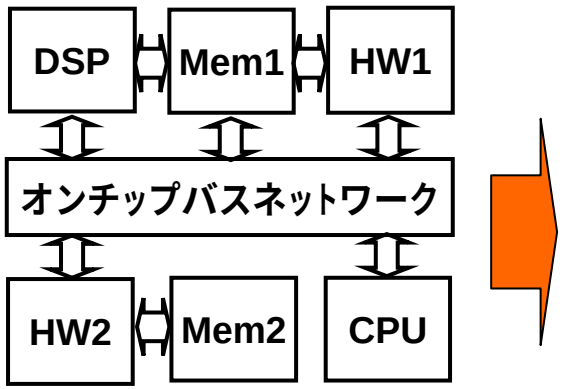


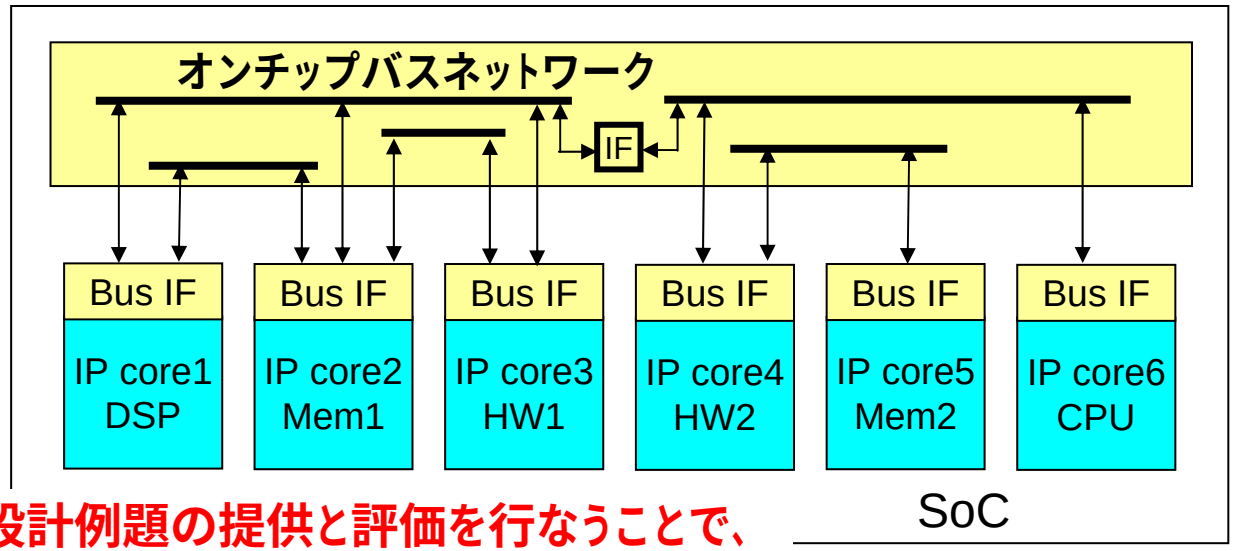
S.Borkar, et al., “Parameter Variations and Impact on Circuits and Microarchitecture, “ Design Automation Conf. (DAC 2003). Jun. 2003, pp 338-342



形式的検証： 研究のねらい

- 設計における Separation of concerns の実現
  - 通信部分と計算部分を分離して、検証･合成時に独立に扱かう
- C系言語設計に対する形式的等価性検証ツール
  - 最新の（ディペンダブル）プロセッサアーキテクチャを形式的に検証可能
- プログラマブル素子の自動挿入による設計自動修復ツール
  - 設計デバッグ支援や、製造段階での故障等をプログラマブル素子により修正
- 両ツールを融合した設計手法の確立
  - C系言語に基づく「テストを陽に意識したテスト容易化･検証容易化」の実現
  - C系言語に基づく設計ドキュメント作成手法の確立

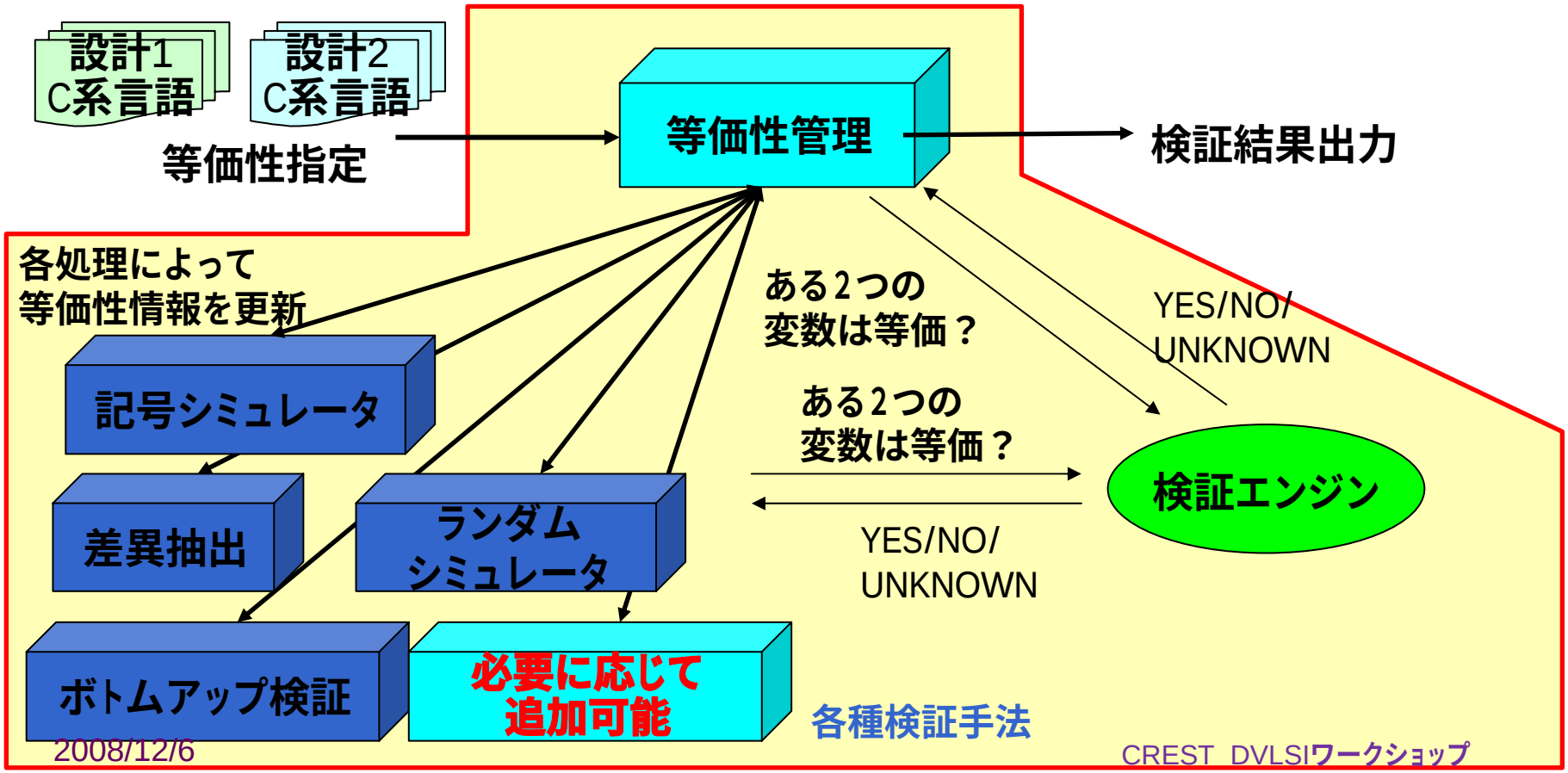




企業との協力関係を築き、設計例題の提供と評価を行なうことで、
その有効性を実証するとともに、商用ツール提供の目処をつける

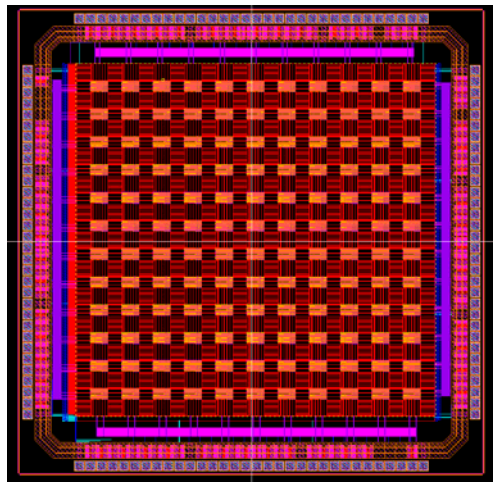
等価性検証ツールの構成

- 既共同研究成果としてプロトタイプツールが存在
  - 数千行程度のC系言語設計記述を数十秒で検証　(MPEGエンコーダHW)
  - ツール開発、および企業との評価のためのフレームワークとして利用
- 数万行程度 (100万ゲート以上) まで扱えるように、機能改良・拡張を行う
- 最新プロセッサの形式的検証を実際に行なうことにより、その有効性を実証

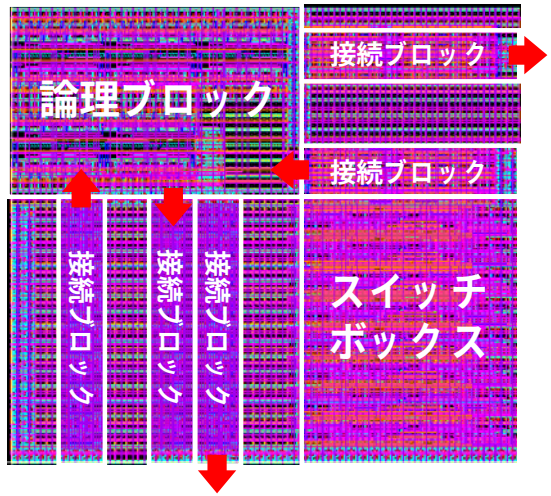


研究成果： 形式的検証

- **等価性検証／解析ツール**
  - 拡張システム依存グラフによる統一的な内部表現
  - 形式的検証手法、テスト容易化のための解析手法、設計理解のための解析手法を実装
  - 各種法の基本的な実装ほぼ完了。C++ 9万行超
  - 国内メーカとの連携による実応用への適用： ***45000行の依存グラフを50分で生成など***
- **ハードウェア・ソフトウェア協調実行による検証高速化**
  - PC-汎用FPGA協調実行により、PCのみの実行に比べて***約7倍の高速化***
  - ***検証高速化& ディペンダブルFPGA アーキテクチャ***の提案・試作
- **テスト容易化のための上位設計解析手法**
  - 上位設計において、指定された条件を満たす入力パタンを生成
  - 記号・具体混合シミュレーション
    - ***SpecC で700行程度***の記述に対して10サイクル以上の混合シミュレーションおよびアサーション違反検出に成功
    - ***SpecC で3000行程度***の記述に対して未初期化変数の値の参照，配列オーバーラン等の検出に成功
  - 動的スライシング技術



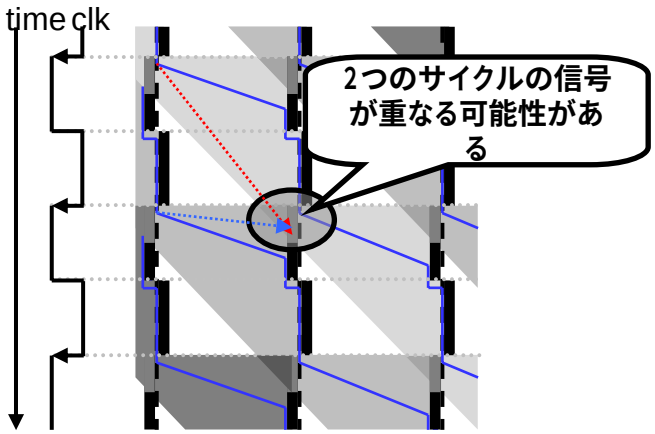
検証高速化専用FPGA
ROHM 0.18um (VDEC)
完全フルカスタム設計



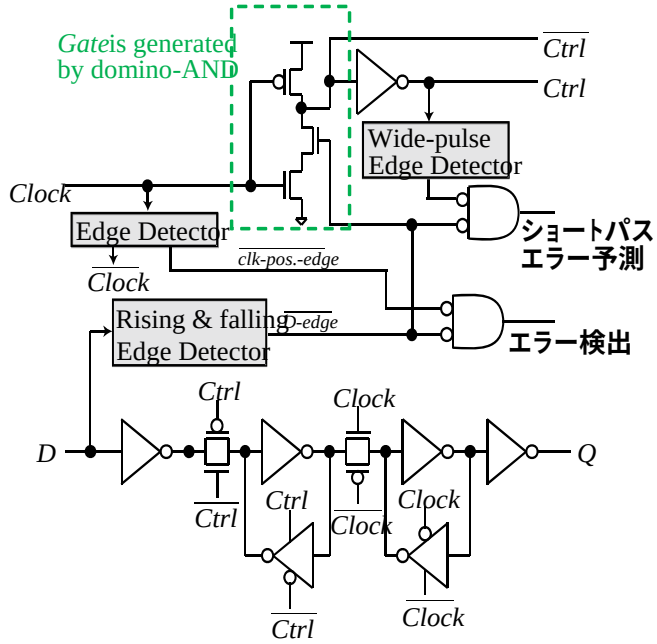
FPGAの基本タイル

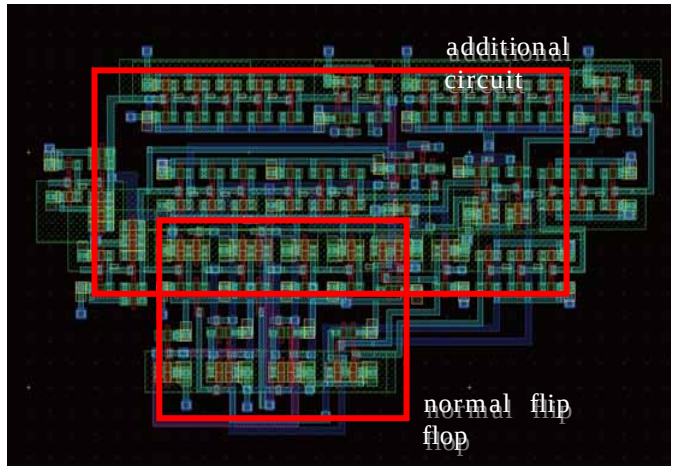
研究成果： 回路・アーキテクチャ

- **タイミング条件緩和技術**
  - 遅延保証フリップフロップ： 信号遷移タイミング監視による適応処理
  - **タイミング制約を緩和するクロッキング方式**
- **故障回避・回復機構**
  - ***FPGAテストベッド試作＋基本動作確認***
- **耐故障アーキテクチャ**
  - 新規方式提案・FPGAテストベッド試作： **再構成制御部を含む仮想化による穴のない耐故障性の実現**
- **高機能ルータ**
  - 基本方式提案、基本ルータチップ試作
- **新アーキテクチャ形式的検証**
  - 超ディペンダブルプロセッサHDL記述 → 形式検証へ



タイミング制約を緩和するクロッキング方式

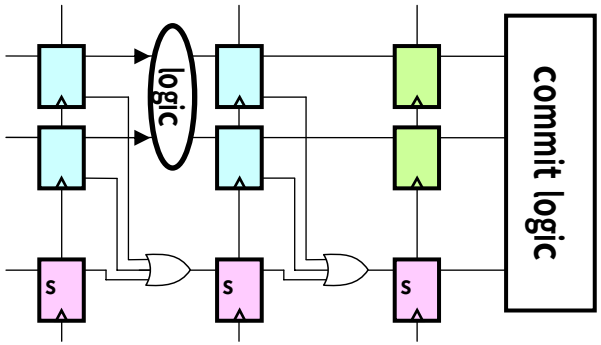




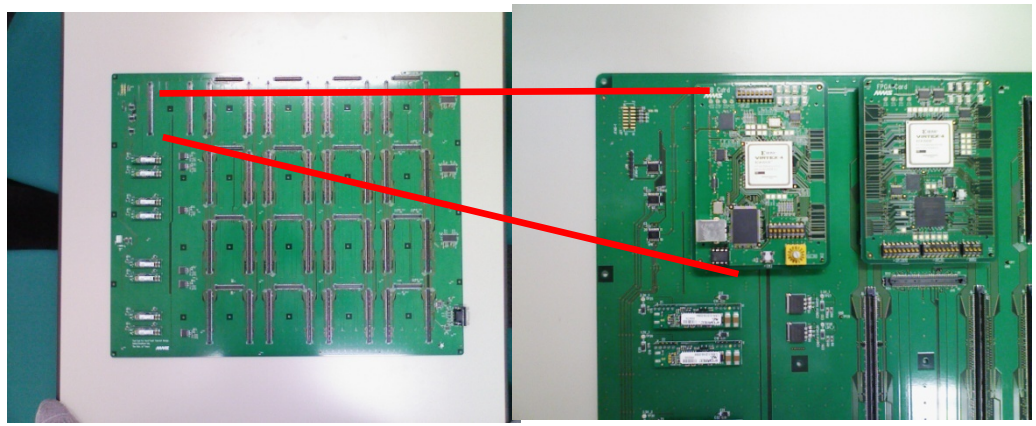
遅延保証FF (約180um^2)

ローム社0.18 um 5-metal CMOS

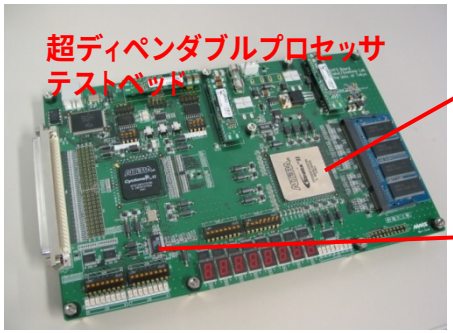
研究成果：アーキテクチャ



故障の動的検知・回復



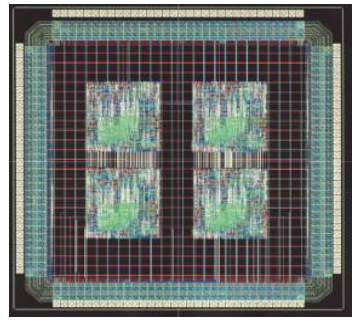
耐故障テストベッド
＝　再構成制御による「抜けのない」耐故障性の実現



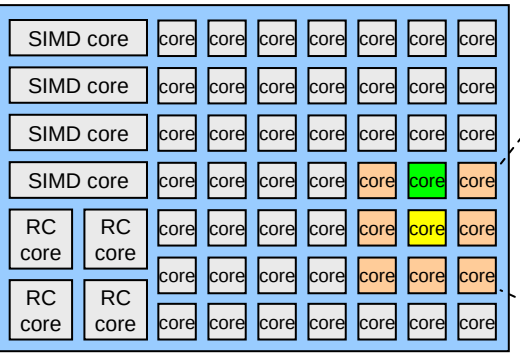
大容量FPGA
ディペンダブル機能をもつ
スーパスカラプロセッサ

動作中に周波数・電圧を
変えられる
→ タイミングエラーやDVFS制御による
エラー回復を再現

耐故障FPGAアーキテクチャ

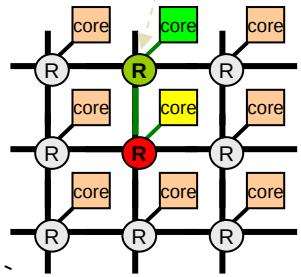


2 x 2 のメッシュ接続の
ルータ
ローム0.18umチップ
設計締切 2008/09/16
納品・試作完了
2009/01/26



(a) 汎用メニーコアプロセッサ

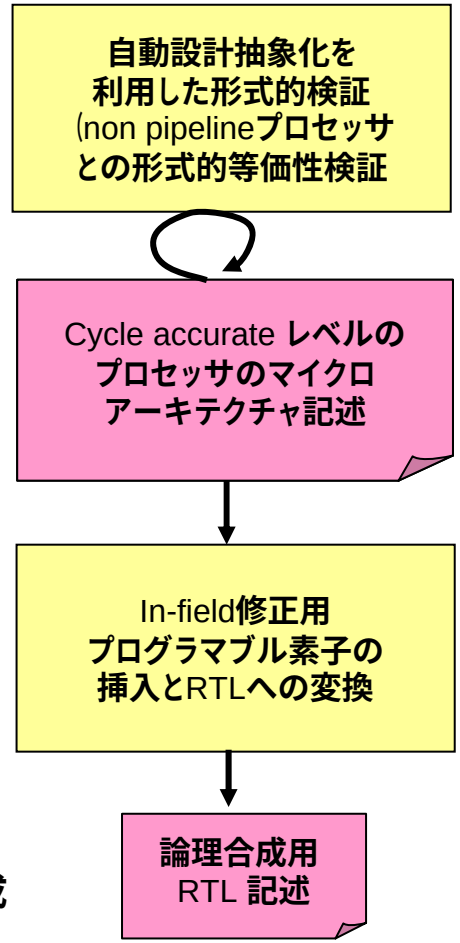
超ディペンダビリティ支援高機能ルータ



(b)ルータを中心とする超ディペンダビリティ支援

全体統合・最適化

- 超ディペンダブルプロセッサの形式的検証
  - 超ディペンダブルプロセッサの検証
    - cycle accurateなシミュレータによる記述
      - Verilog HDL（記述済） → System Cへの移行
    - single pipelineプロセッサを検証
    - 等価性検証により最新プロセッサを検証
- 超ディペンダブルメニーコア技術の確立
  - 多機能ルータの動作検証・試作
  - プロセッサ部との統合
- 統合化・最適化
  - 検証技術とアーキテクチャ技術の統合
    - これまでの手段では得られなかったVLSIのディペンダビリティを達成
  - コスト最適化
    - 各手法の最適な適用
  - セキュリティ技術との統合



論文発表、特許、表彰、新聞報道

- 論文
  - 欧文誌　(4)
  - 査読付主要国際会議　(5)
  - 学会誌　(1)
  - 国際ワークショップ (7)
  - 研究会　(7)
- 特許　(2)
- 受賞 (3)
- 新聞等報道 (2)
  - 「東大が乗算器の等価性チェックを高速化する技術を併設学会のMEMOCODE‘08で発表」,日経BPネット, http://techon.nikkeibp.co.jp/article/NEWS/20080607/152975/, Jun 2008
  - 「CPUの不具合　自動復旧　– 信号伝達の異常を削除　-」、日経産業新聞7/2, 2008.

外部連携

- ***海外大学：NDA下によるCADソースコード提供***
  - Indian Institute of Science
  - University of Florida
  - New York City College
- ***海外機関：CADオブジェクトコード提供***
  - NASA
  - Bremen University (ドイツ)
- ***海外大学：ディペンダブルアーキテクチャ研究協力(検討中)***
  - Carnegie Mellon University
  - Cornell University
  - University of Texas, Austin
- ***学会・協会***
  - 電子情報通信学会CPSY・DC： CREST共同企画による研究会(2008/4)
  - 情報処理学会 (全国大会企画など)
- ***国内企業：CADソースコード提供***
  - **国内4社 (NDA)**
- ***国内企業： 回路***
  - 東大TLOを介してLSIベンダ (NDA) と交渉中
- ***国内企業： アーキテクチャ***
  - 超ディペンダブルマイクロプロセッサ：
    - 2社と交渉中
  - メニーコア用ルータ
    - 1社と交渉予定

今後

- **欧米大学**
  - **ツール提供による共同研究**
  - **アーキテクチャ共同開発**
- **マイクロプロセッサベンダ (1社)**
  - **知財提供**
- **国内SoCベンダ**
  - **CADツール、アーキテクチャ共同開発**

まとめ

VLSIシステムの信頼性を飛躍的に高める技術の研究

＝ 形式的検証とアーキテクチャの最適な協調

- **形式的検証手法**
  - C/C++言語ベースVLSI高位設計
  - 対話・自動ドキュメント化のための要素技術
- **テスト技術・テスト段階修復技術**
  - テスト容易化・検証容易化を実現する設計手法
  - フィールドプログラマブル性を部分的に導入可能な合成手法 = テスト段階でデザインミスをとる
- **回路技術**
  - タイミング制約緩和回路
- **アーキテクチャ技術**
  - 故障検出・回復機構の提案・実現
  - 制御部を含めたFPGA仮想化
  - 耐故障高機能ルータ
  - 超ディペンダブルプロセッサ
- **新アーキテクチャ形式的検証**
  - ディペンダブルアーキテクチャ技術自体を形式的に検証
  - 既存のアーキテクチャ、最新のアーキテクチャを形式的に検証
- **各設計階層間のディペンダビリティ役割分担を最適化**

今後の展開・課題

- **形式的検証手法**
  - 企業からの実用的例題に対する評価
  - ルールベース検証手法の実装・評価
- **HW・SW協調実行による検証高速化**
  - 試作チップのテスト・実証実験
  - ディペンダビリティを強化したチップの設計・試作
- **回路技術**
  - タイミング制約緩和回路の評価
- **アーキテクチャ技術**
  - 故障検出・回復機構の改良・評価
  - 制御部を含めたFPGA仮想化： 実装・評価
  - 耐故障高機能ルータ： 詳細提案・実装・評価
  - 超ディペンダブルプロセッサ： 設計・評価
- **新アーキテクチャ形式的検証**
  - ディペンダブルアーキテクチャ技術の検証
  - 既存のアーキテクチャ、最新のアーキテクチャを形式的に検証
- **各設計階層間のディペンダビリティ役割分担**
  - 実例による最適化実験