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

内容

- 全体
- 形式的検証とテスト段階の修復
- 回路・アーキテクチャによる故障検出・障害回避
- 統合・最適化
- まとめ

全体

- 背景
- 研究目標
- 研究の進め方
- 全体計画・スケジュール
- 成果物

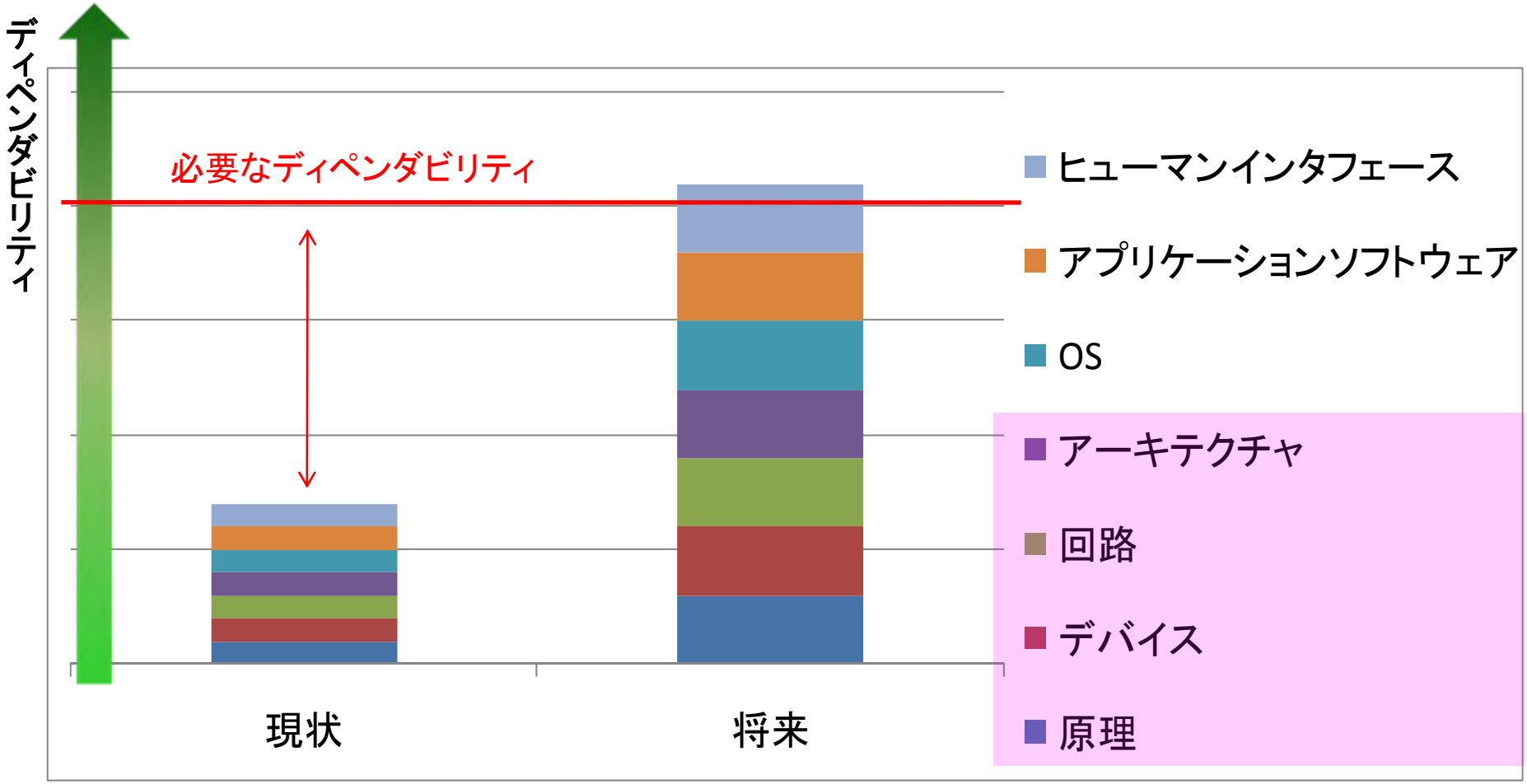
情報ディペンダビリティ＝ITの安心安全

- ディペンダビリティ （定義）
  - 「提供するサービスの内容に見合う情報処理システムの信頼

    the trustworthiness of a computing system which allows reliance to be justifiably placed on the service it delivers （by IFIP WG10.4: *Dependable Computing and Fault Tolerance*）
  - 安全性、信頼性、可用性、堅牢性、拡張性などを統合する概念
- なぜいまディペンダビリティ？
  - VLSIの微細化・高集積化による設計・テストの複雑化とPVTI耐性の低下
  - ソフトウェアの複雑化による検証困難と脆弱性の混入
  - ベストエフォート文化の浸透による生産者の責任を問えない体制
  - ユーザの爆発的増加と情報システムのブラックボックス化
  - 悪意あるユーザの遍在
  - うっかりミスなどヒューマンファクタの増大・増加
- 本提案は、VLSIシステムの信頼性の飛躍的向上が課題

情報処理の階層とディペンダビリティ

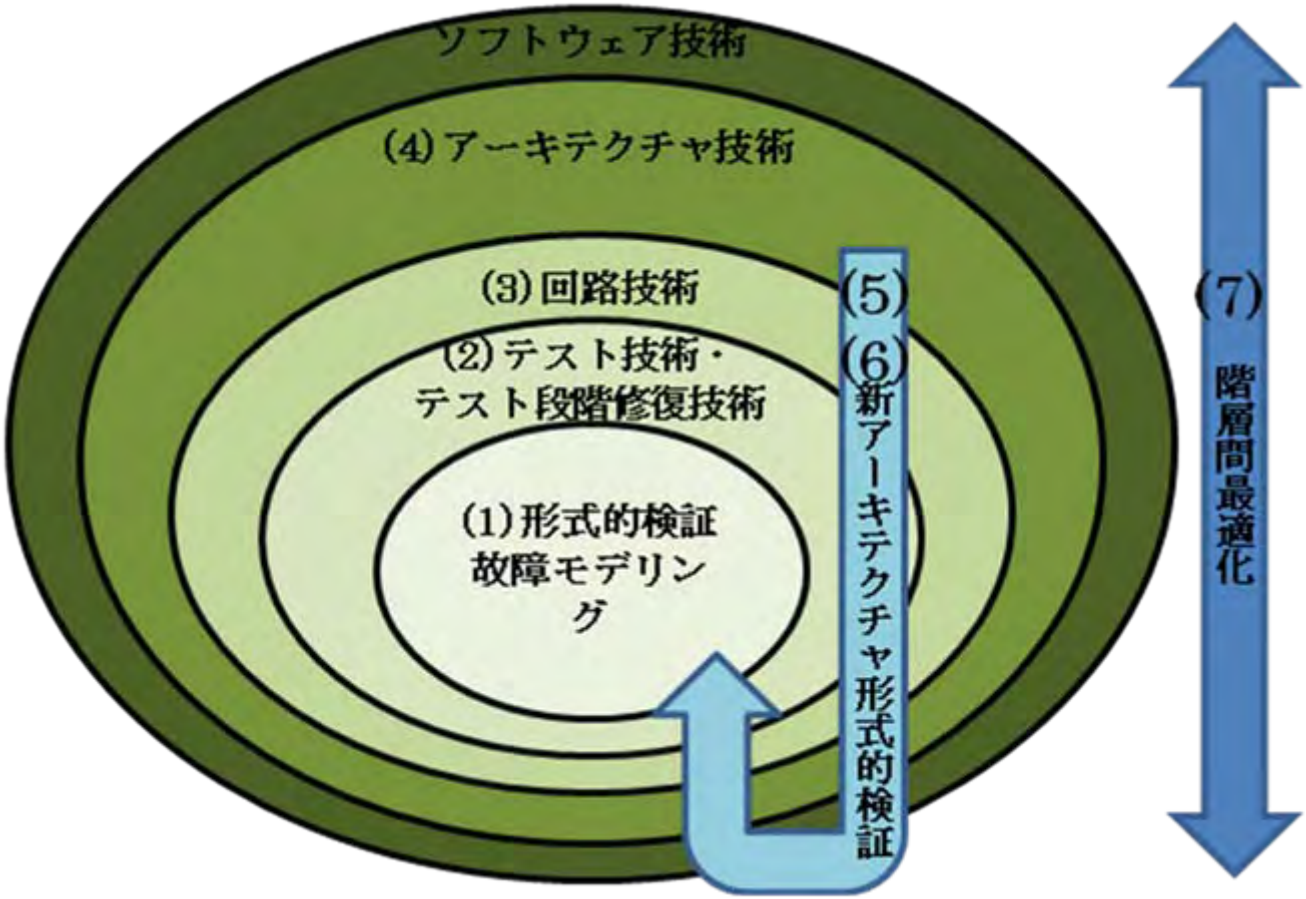
- ディペンダビリティ　＝　ユーザに提供するサービス
  - 総合的に達成されなければならない（されればよい）



研究課題

- C/C++言語ベースVLSI高位設計において、形式的検証手法を高度に進めることで、近未来のマイクロプロセッサを含むVLSI設計の信頼性を飛躍的に高める
- C言語記述の対話・自動ドキュメント化（マニュアル化）のための要素技術の確立をめざす
- 上位設計からテストを陽に意識しテスト容易化・検証容易化を実現する設計手法の確立を通してテスト・検証コストの大幅な削減を図る
- 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も併用することで、形式的検証でとりきれない設計ミスや製造上の故障についても、テスト段階でとることができるようにする
- 形式的検証、テスト段階の修正でも取り切れない製造ミスや故障について、これを回路技術で検出・回復
- 以上でとりきれない設計ミスや製造故障をアーキテクチャのレベルで解決するディペンダブルアーキテクチャを開発する
- 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する
- 既存のアーキテクチャに加えて最新のアーキテクチャを形式的に検証する
- 各設計階層間のディペンダビリティ役割分担を最適化し、最終的に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する

本研究で扱うディペンダビリティ階層



何がうれしいか

- VLSIユーザ
  - 設計の正しさが向上し、リコールなどが減少する
  - VLSI製作後のバグフィックスや機能修正によって利便性が向上する
  - 保証される動作速度が向上する
  - 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
  - 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
  - 従来最悪値の積算でなされていたVLSI設計が、「典型値＋回路・アーキテクチャによる補正」によって実現可能となる

最終成果物・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
  - 永久故障用テストベッド
- 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

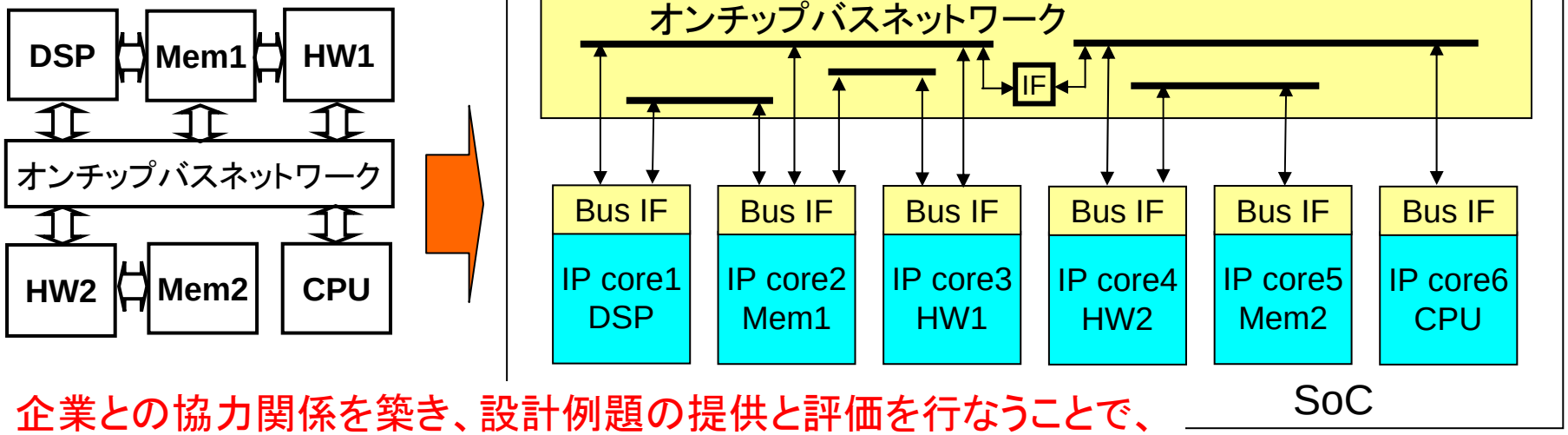
形式的検証とテスト段階の修復

藤田昌宏研究室

- 研究のねらい
- 等価性検証ツールの構成
- プログラマブル素子自動挿入による自動修復
- 期待される設計効率の向上
- 予定・計画

研究のねらい

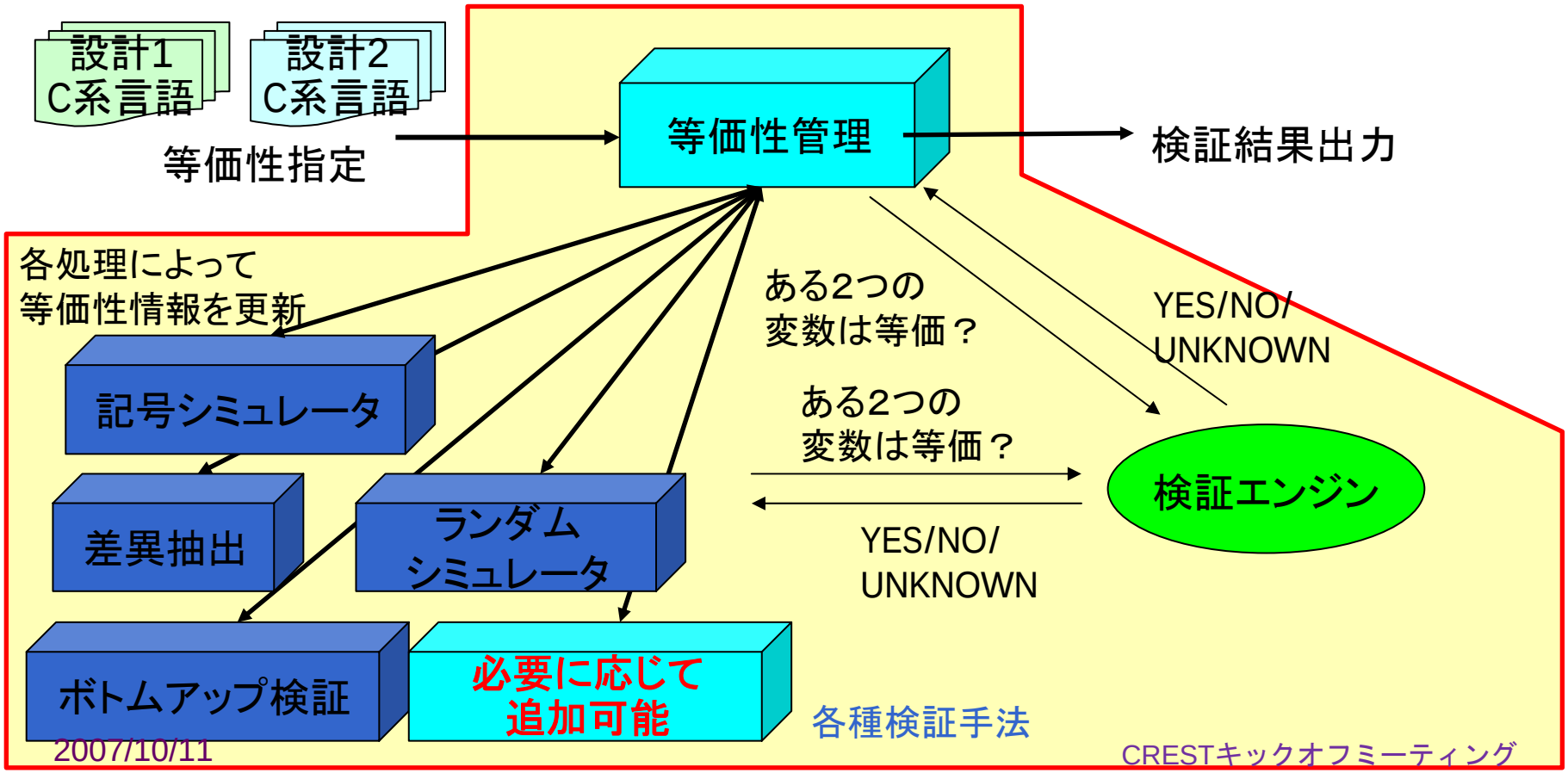
- 設計における Separation of concerns の実現
  - 通信部分と計算部分を分離して、検証・合成時に独立に扱かう
- C系言語設計に対する形式的等価性検証ツール
  - 最新の（ディペンダブル）プロセッサアーキテクチャを形式的に検証可能
- プログラマブル素子の自動挿入による設計自動修復ツール
  - 設計デバッグ支援や、製造段階での故障等をプログラマブル素子により修正
- 両ツールを融合した設計手法の確立
  - C系言語に基づく「テストを陽に意識したテスト容易化・検証容易化」の実現
  - C系言語に基づく設計ドキュメント作成手法の確立



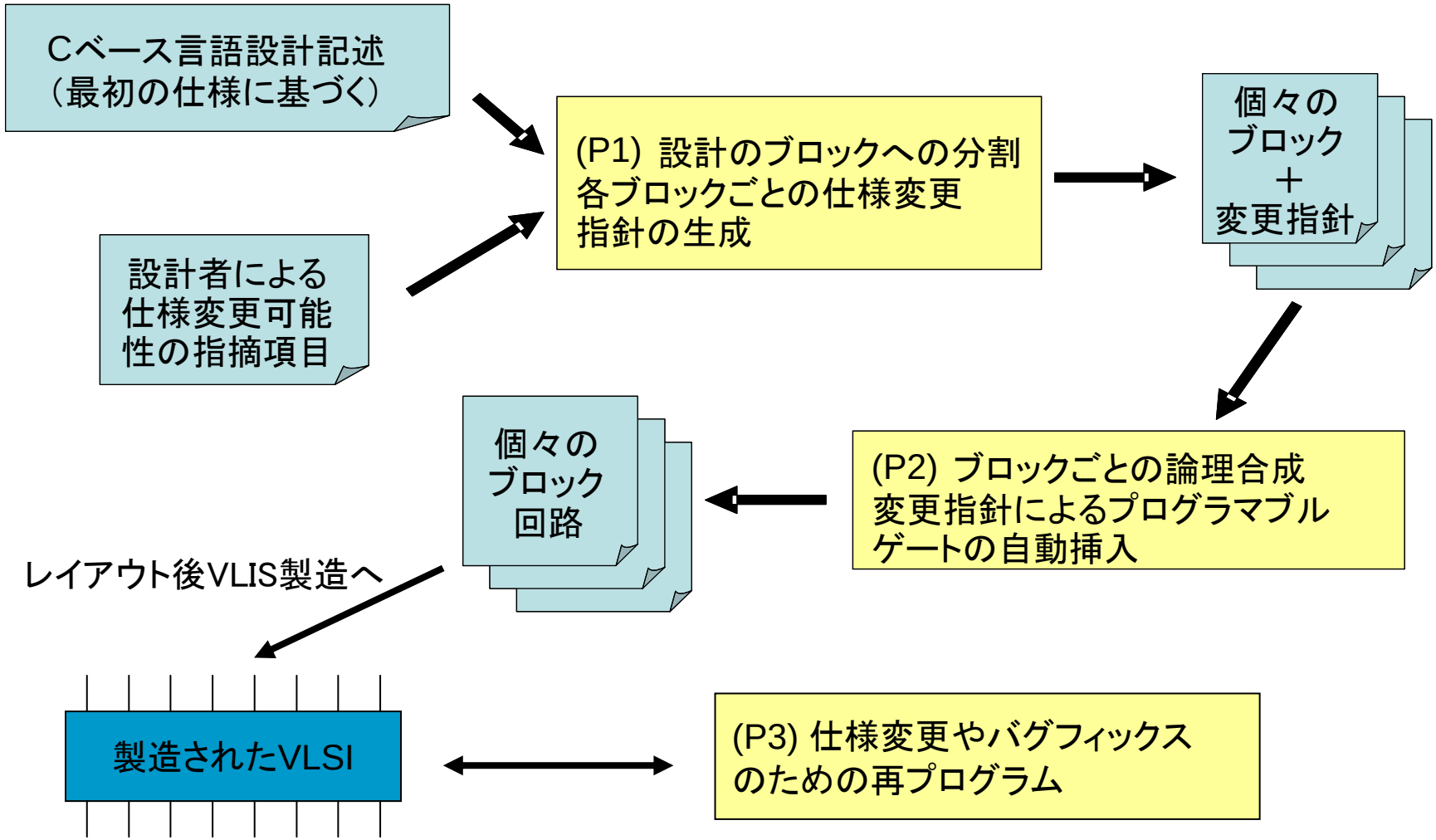
企業との協力関係を築き、設計例題の提供と評価を行なうことで、
その有効性を実証するとともに、商用ツール提供の目処をつける

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

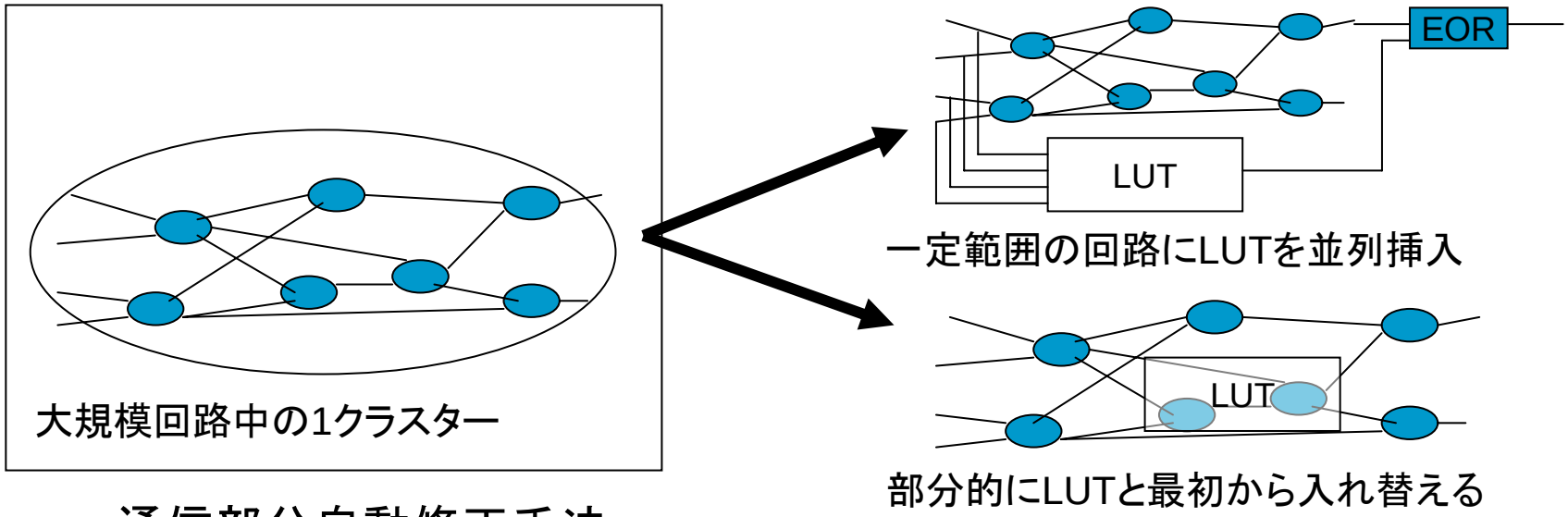


プログラマブル素子自動挿入による設計自動修復

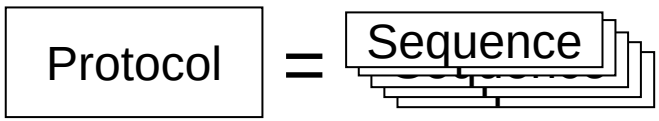


In-field自動修正のための回路アーキテクチャ

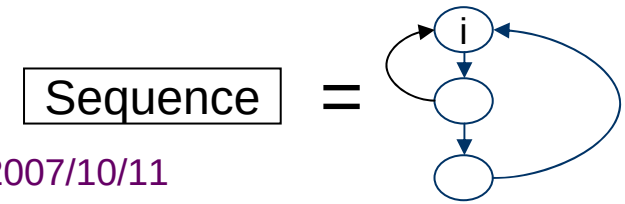
- 基本：部分的にLUT（Look Up Table プログラマブル素子）を導入（挿入）



- 通信部分自動修正手法
  - In-field修正可能なバスインターフェイスを自動生成（自動修正）
    - プロトコルレベルの形式的検証　＋ プロトコル変換器（自身で開発）
    - 一定範囲内の任意のプロトコルへの修正が可能



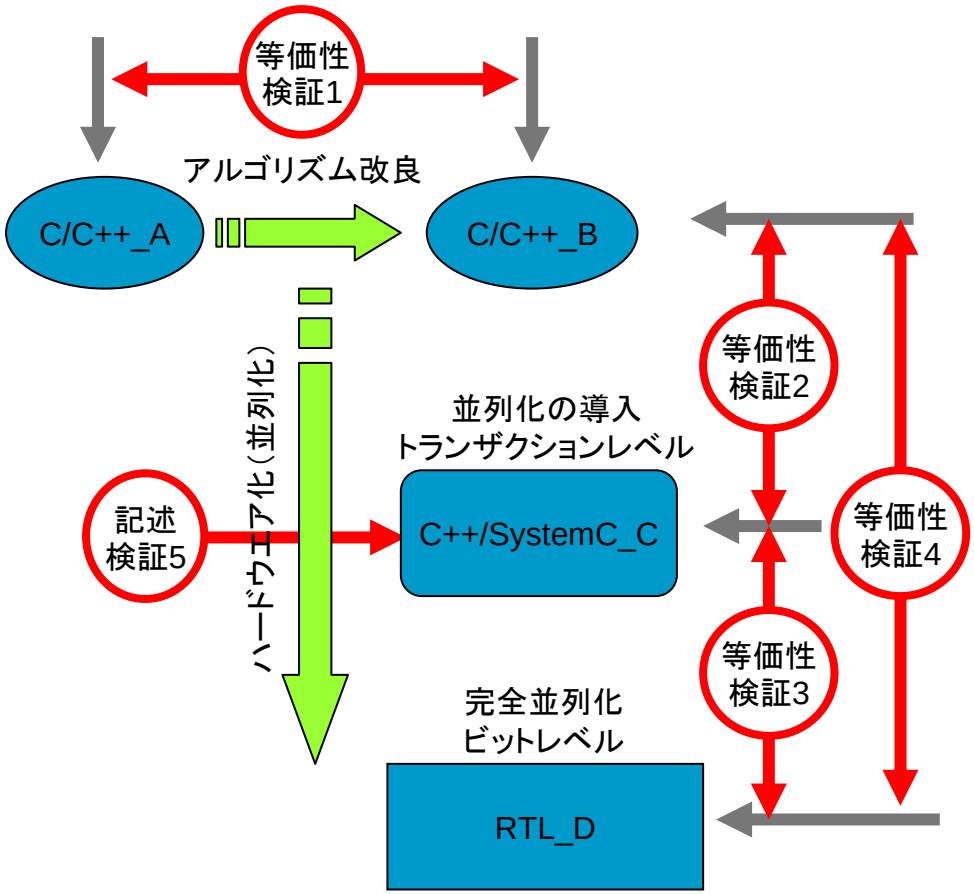
プロトコルはシーケンスの集まりで表現
OCPやAXIなど最新プロトコルの表現が可能



各シーケンスはオートマトンで定義
OCPやAXIに対応するオートマトンを既に記述済

期待される設計効率の向上

- 企業の設計者の説明とインタビュー結果： ２年後
  - 従来のC系言語ベース設計との比較　　100万ゲート規模の論理設計の場合



対象	従来手法	新規手法
AとB	C/C++ シミュレーション 3ヶ月	等価性検証1 シミュレーション 1ヶ月
BとC	C++/SystemC シミュレーション 3ヶ月	等価性検証2 シミュレーション 1ヶ月
CとD	RTL シミュレーション 6ヶ月	等価性検証3 シミュレーション 2ヶ月
BとD （Cを経由 しない）	RTL シミュレーション 12ヶ月	等価性検証4 シミュレーション 4ヶ月
まとめ	品質向上：従来より数段向上 TAT短縮：約1/3	

２年後に約１／３に短縮、後半さらに１／３に短縮することを目指す

回路・アーキテクチャによる耐故障性の実現

坂井修一・五島正裕研究室

- 研究のねらい
- 動的なタイミング故障検出・障害回避
- エラー回復手法
- 耐永久故障アーキテクチャ

研究のねらい

設計段階・テスト段階で取り切れないミス・故障の検出・回復

- 回路による耐故障性
  - タイミング故障の動的検出・障害回避
- アーキテクチャによる耐故障性
  - エラー回復機構
  - 永久故障の検知・回復

動的タイミング故障検知・障害回避

- 高度な微細加工による遅延時間ばらつきの拡大　⇒　最悪値設計の困難化
- Shadow latchによる実行時タイミング故障検出・障害回避利点

  ○動作周波数と電源電圧で与えられる回路の動作範囲の拡大と歩留まりの向上
  - 動作時のクリティカルなパス によって決まる最高動作周波数、最低電圧での動作が可能になる

  × 最小パス遅延の揺らぎによるエラーの発生は検知できない
- 提案手法：　XXXXのタイミングを監視することでタイミング故障の発生を検知

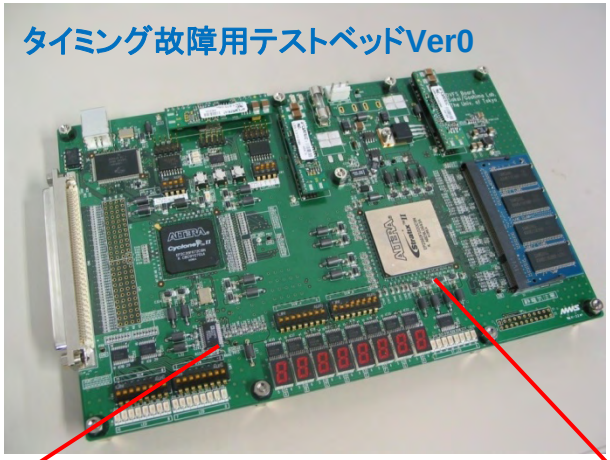
（現在、特許申請中）

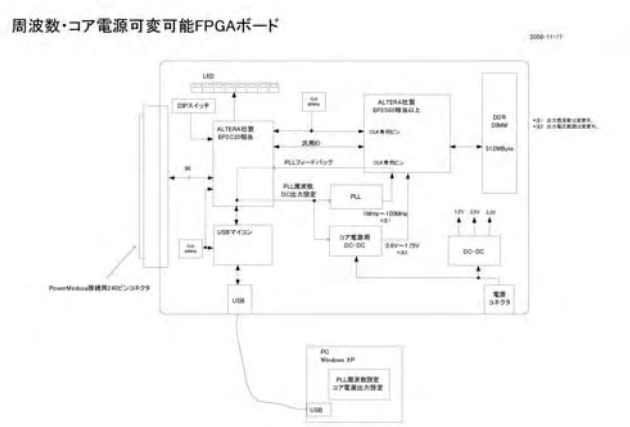
○ 遅延ゆらぎによる故障を動的に検出・回避できる
- 最悪値設計不要
- 個々の回路・個々の入力パターン・任意の時点の遅延ゆらぎに個別に対応できる

アーキテクチャによるエラー回復手法

制御系を含む、OOOプロセッサ内のいかなる場所で発生したエラーからも回復可能な手法を提案・評価する

- エラー回復手順:
  1. エラーに影響を受けた命令の実行結果によってプロセッサ・ステートが更新されることを防ぐ
  2. エラー発生時には、プロセッサをリセット。その後、保護されたプロセッサ・ステートを起点として動作を再開すればよい。
- エラー回復方式
  - 命令の実行結果は、プログラム・オーダにしたがって論理レジスタファイルを更新する。このことを拡張し、エラーに影響されていない結果によってのみ、論理レジスタファイルを更新する新方式を提案・評価する
- 評価ボード





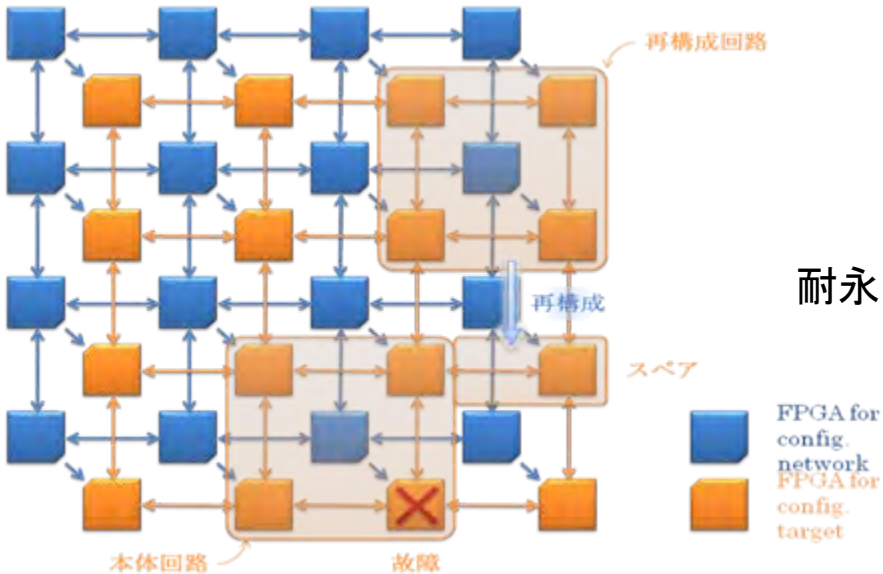
動作中に周波数・電圧を変えられる
タイミングエラーや、
DVFS制御によるエラー回復を再現可能

スーパスカラプロセッサ+αを十分実装可能な大容量FPGA
ディペンダブル機能をもつスーパスカラプロセッサの動作実証が可能

アーキテクチャによる故障耐性

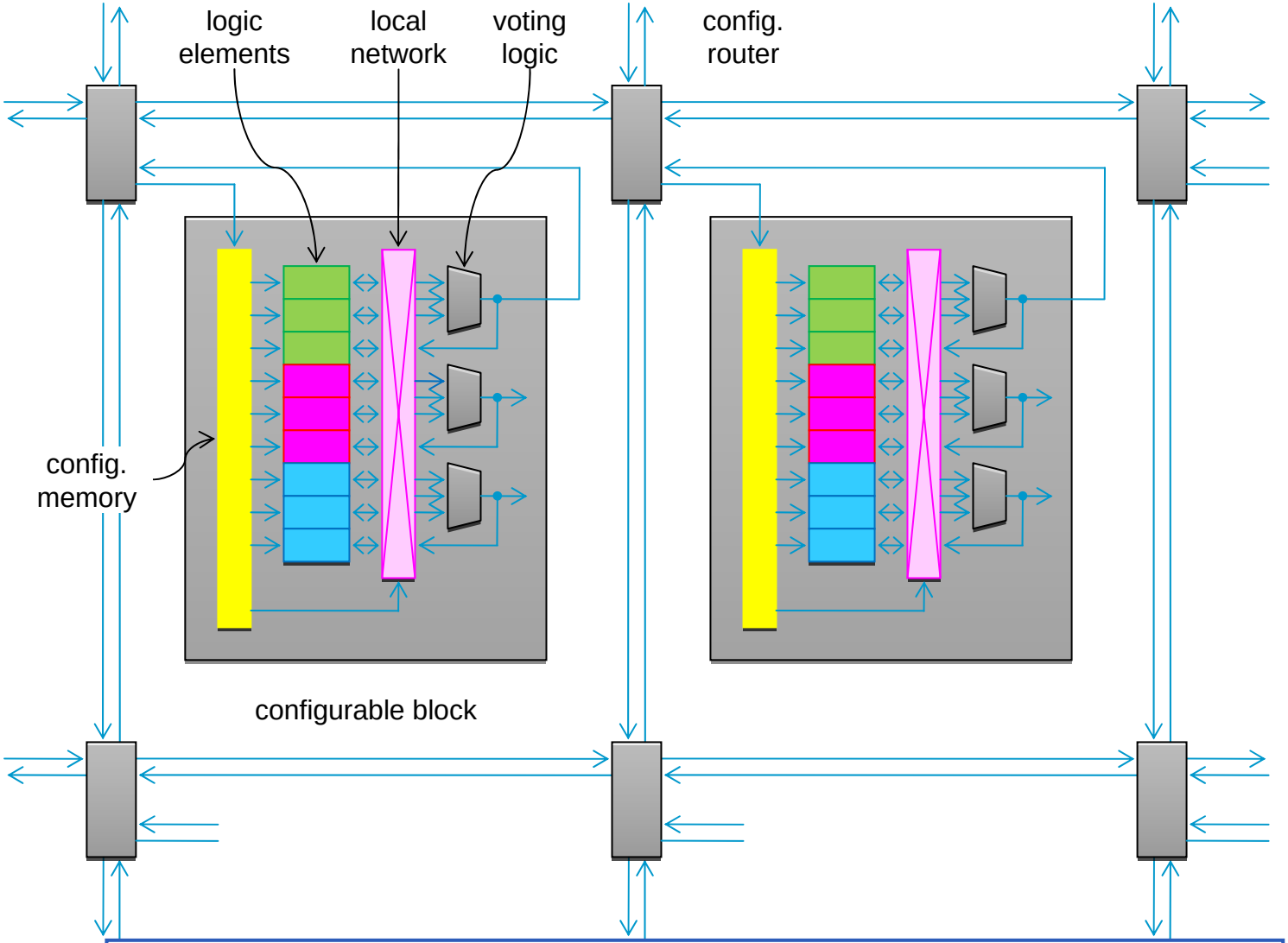
高いソフトエラー耐性と耐永久故障性をもつFPGAベースのVLSIアーキテクチャ

- 既存方式：
  - TMR ＋ 多数決回路： 故障検出
  - スペアの再構成可能な論理ブロックを用いて新たにモジュールを構成し、故障を含むモジュールを置き換えてTMR状態を回復
  - × 再構成を行う回路自体には冗長性がなく、single failure pointとなる
- 提案方式： 再構成を行う制御回路をも、本体回路と同様の再構成対象として実現する
  - 再構成回路自身も本体回路と同様のTMRで構成し、故障時には自分自身を再構成することでTMR状態を回復
  - 再構成制御回路を含むVLSIのいかなる部分も再構成可能であるようなチップ・アーキテクチャ
  - 現在、方式提案を行い、プロトタイプの製作を計画中



耐永久故障FPGAアーキテクチャ

耐故障アーキテクチャ： 原理図

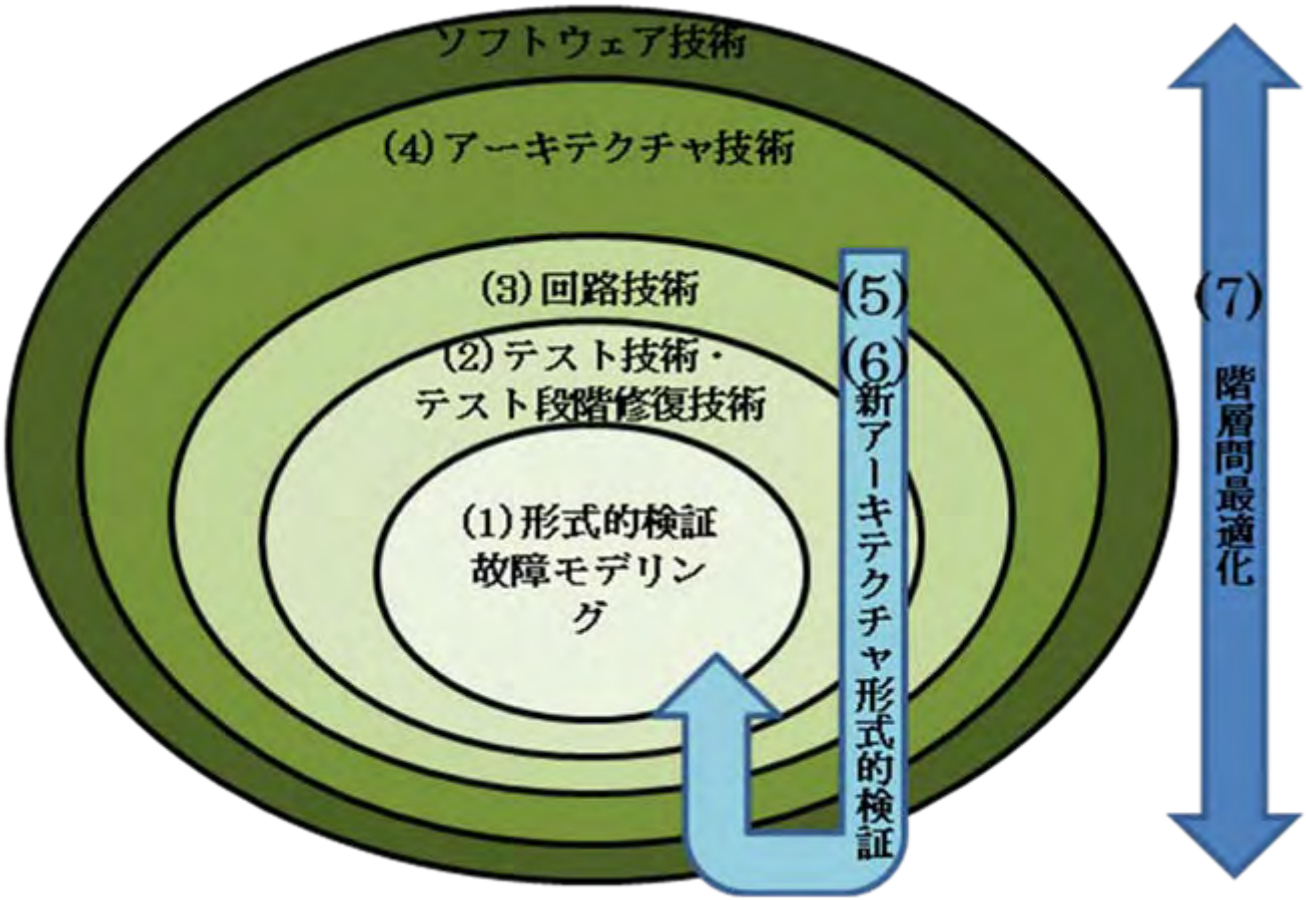


永久故障用テストベッド → 多数のFPGAをつないだ基板
再構成制御部のソフトウェア的実現

全体統合・最適化

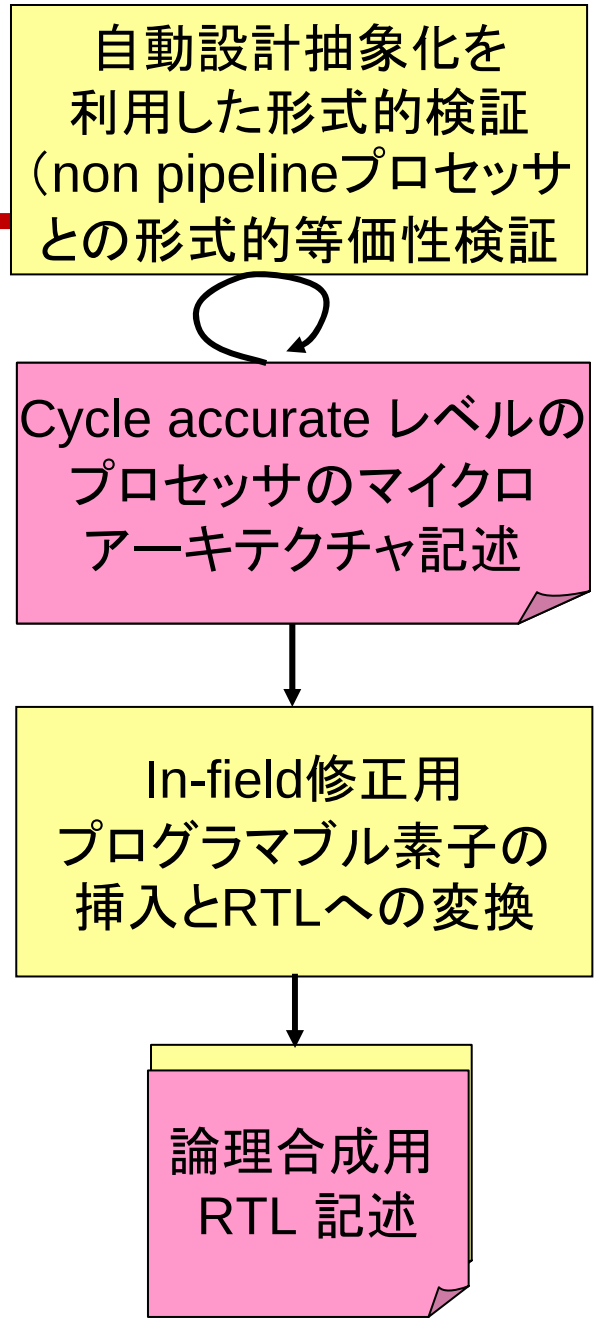
- 最新ディペンダブルアーキテクチャの形式的検証
- 最適化

ディペンダビリティ階層と技術統合



最新ディペンダブルプロセッサの形式的検証

- RTL記述を直接形式的に検証することは、その規模から非常に困難
  - 論理合成可能なRTL設計記述には、合成品質を向上させるための様々な工夫（記述上のトリックなど）があるため直接取り扱うと効率が落ちる
- プロセッサのマイクロアーキテクチャをcycle accurateなレベルで記述する
  - SystemCなどを利用したプロセッサアーキテクチャ記述手法を確立
  - 形式的検証のための設計の自動抽象化が可能
    - Single pipelineプロセッサならstate-of-the-artが検証可能
    - 等価性検証技術の応用によりさらに複雑なものも検証
  - 論理合成用RTL設計記述を自動生成する
    - In-field修正機能付合成も適用



全体統合・トレードオフポイント

設計対象によって、各種法にかけるコストを最適化
⇒　連携して総合的戦略を作り上げる

用途	形式的検証	テスト段階の修復	回路・アーキテクチャによる検出・回避・回復
家電・カメラ	◎	○	△
PC・サーバ	○	○	◎
交換できない組み込み系（宇宙など）	○	○	◎

統合化目標

1．各設計階層間のディペンダビリティ役割分担を行い、最終的に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する

2．用途に応じて各手法の最適な適用について検討し、「ディペンダブルVLSI製作方法論」を確立する

まとめ

- まとめ
- 研究の独創性・新規性
- ディペンダビリティの測定・定量化
- 研究実施の基盤および準備状況
- 2007年度研究項目・計画
- ５年間研究計画
- 将来計画

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

- 高位設計における形式的検証手法の開発
- テスト容易化・検証容易化を実現する設計手法・ドキュメント化技術の基盤の確立
- 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
  - 設計ミスや製造上の故障をテスト段階でとる
- 回路技術による製造ミスや故障の除去
  - タイミングエラー検出・回復
- ディペンダブルアーキテクチャ
  - 永久故障検出回復
- 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・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

研究の独創性・新規性

- 形式的検証
  - ワードレベルの解析手法の新規提案ならびにビットレベル解析の融合。具体的なアーキテクチャに適用して実証。
  - C言語記述の対話・自動ドキュメント化（マニュアル化）のための要素技術の確立
- 製造故障テスト手法
  - 上位設計手法の中でテスト設計を捉える。テスト設計の大きな効率改善が期待、信頼性の向上、テストのためのコストの大幅な削減が期待できる。
- 製造後の手法
  - プログラマブル素子を部分的に要所に導入する回路構成。自動設計修正を形式的検証手法とテスト手法を融合したアプローチで実現。最小限のプログラマブル素子の導入で、最大限の設計上の自由度が得られるようになる
- 動的タイミング故障対策
  - タイミング故障を動的に回避する手法の提案。高速で正確な動作を保証
- 再構成アーキテクチャ
  - 再構成制御回路も含めたディペンダビリティの実現
- 既存回路・最新ディペンダブルアーキテクチャの形式的検証
- 形式的検証、テスト、回路、アーキテクチャの諸技術が連携し、相互補完することで、各技術では達成不可能なレベルのディペンダビリティを獲得

ディペンダビリティの測定・定量化

1. 従来は得られなかった信頼性が得られることを示す（質的な評価）

   耐永久故障アーキテクチャによるsingle failure pointの解消など

2. 最悪値設計に対する性能向上

   動的エラー回復技術を用いて、動作速度を向上させることの効果を定量的に評価

3. 設計時間の短縮（2年後：3ヶ月　⇒　1ヶ月；　5年後：さらに1／3を目指す）

4. 面積・電力・性能オーバヘッドの低減

   VDECを使った設計により、ディペンダビリティ機能の導入による面積・電力・性能のオーバヘッドを測定し、これが許容範囲（一例として5%以内）にあることを示す。逆に、オーバヘッドの許容範囲を提示された場合に、どのようなディペンダビリティ機構を導入すればよいかを示すことも考えられる

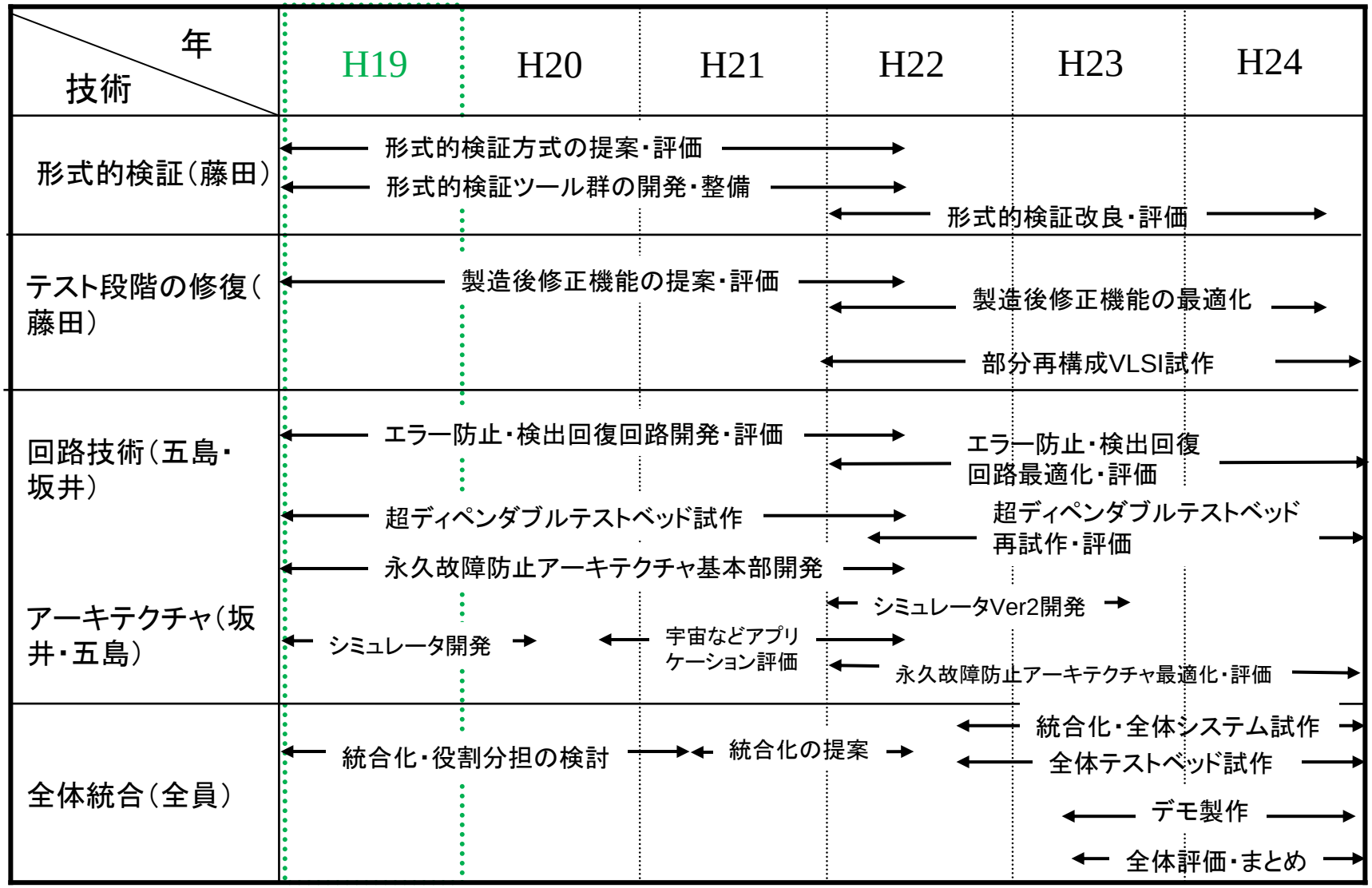
研究実施の基盤および準備状況

- 形式的検証、テスト技術
  - 基礎研究
    - 2分決定グラフの実用的な変数順決定手法の提案とその論理合成への応用
    - モデルチェッキングにおける限定手法の提案
  - 基盤技術
    - C/C++言語ベースの上位設計記述に対する新しい形式的検証手法の提案、実装、ツール化（科研、共同研究など）。レジスタ転送レベルやゲートレベル設計では実現不可能な規模の設計の検証が可能となることを示している
    - ジャーナル、国際会議、展示会での形式的検証ツールのデモ、研究開発した形式的検証ツールのウェブからの配布
- 回路技術、アーキテクチャ技術
  - 基盤技術
    - タイミング故障耐性を持つレジスタファイル構成方式、ソフトエラー耐性を持つキャッシュの構成方式、ディペンダビリティ制御機構など
    - 国際会議・ジャーナル論文での発表、特許申請
- 両者の協力によって真のディペンダビリティの実現を！

2007年度研究項目

- 等価性形式的検証ツール
  - 基本フレームワークの確立と企業との共同評価体制の確認
    - 現共同研究成果の確認と今後の指針の確立
  - 数万行規模のC系言語設計記述対応のための技術項目のリストアップ
    - 等価性管理手法の技術項目
    - 各種検証手法の整理と新規技術項目
    - 検証エンジン部分での新規研究項目
- 設計自動修正ツール
  - 既存研究、既存ツールの整理
    - デバッグ技術、プロトコル（インターフェイス）自動生成技術
  - 基盤となる自動論理修正アルゴリズムの提案
    - 既存論理合成ツールの整合性の検討
  - 通信部分の基本手法の提案
    - プロトコル変換器の利用法の検討
- 動的タイミング故障検知・障害回避
  - タイミング故障耐性をもつフリップフロップの提案
- 耐故障アーキテクチャ
  - プロセッサシミュレータをディペンダビリティ用に改良
  - FPGAを用いたテストベッドの整備
  - 設計ミスや製造エラーに対する耐性をアーキテクチャで受け持つ方式について検討
- アーキテクチャ形式的検証の初期検討

全体計画・スケジュール



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

将来展望

- 本研究の効果
  - VLSI設計の省力化と動作保証が、低いコストと高い信頼性で得られる
  - 回路・アーキテクチャの開発者に対して、その検証を確実に行い、さらにディペンダブル回路やディペンダブル機構を加えることでこれらをコスト低く安全にVLSIに組み入れることを提案できる
  - 研究開発した技術を、研究者・技術者コミュニティに還元することで、産業界においてディペンダビリティの高いVLSIの開発をうながすことができる
  - VLSI（とくにマイクロプロセッサ）のディペンダビリティが飛躍的に高まり、これを基盤とする社会全体を現在より「安心・安全」なものにすることに貢献できる
- インキュベーションのために
  - 産学連携のコンソーシアムによる産業化
  - 学会協会などを通じた標準化
  - ディペンダビリティを認定する中立的な機構
  - 産業的には、従来のインテルプロセッサや組込プロセッサの次世代のヘゲモニーを狙う可能性を秘めている。上記の標準化なども含め、利潤構造を示しにくい半導体産業・情報基盤産業を活性化するひとつの軸になることが期待される。
- 各種連携
  - セキュリティ基礎理論、オペレーティングシステム、アプリケーションソフトウェア、ヒューマンインタフェースなどの情報処理学の諸分野との連携融合
  - 心理学・法学・社会学など文科系諸分野との協力

ディペンダブル関係イベントなど

- JST　CREST　「情報社会」 シンポジウム：　2007年10月12日　於　日本科学未来館
  - 坂井、千葉「ディペンダブル情報処理基盤」
- 日本学術会議情報学委員会主催講演会「情報処理で社会を守る」：　2007年11月20日
  - セキュリティ・ディペンダビリティ分科会：　今井秀樹主査
- 電子情報通信学会DC/CPSY：　ディペンダブル特集2008年4月　於　東京（予定）
- 情報処理学会論文誌「ディペンダブル情報処理」特集号：　2008年6月号
  - 南谷崇（ゲストエディタ）、坂井(副)
  - 論文募集は〆切