統合的高信頼化設計のための モデル化と検出･訂正･回復技術

九州大学 安浦チーム

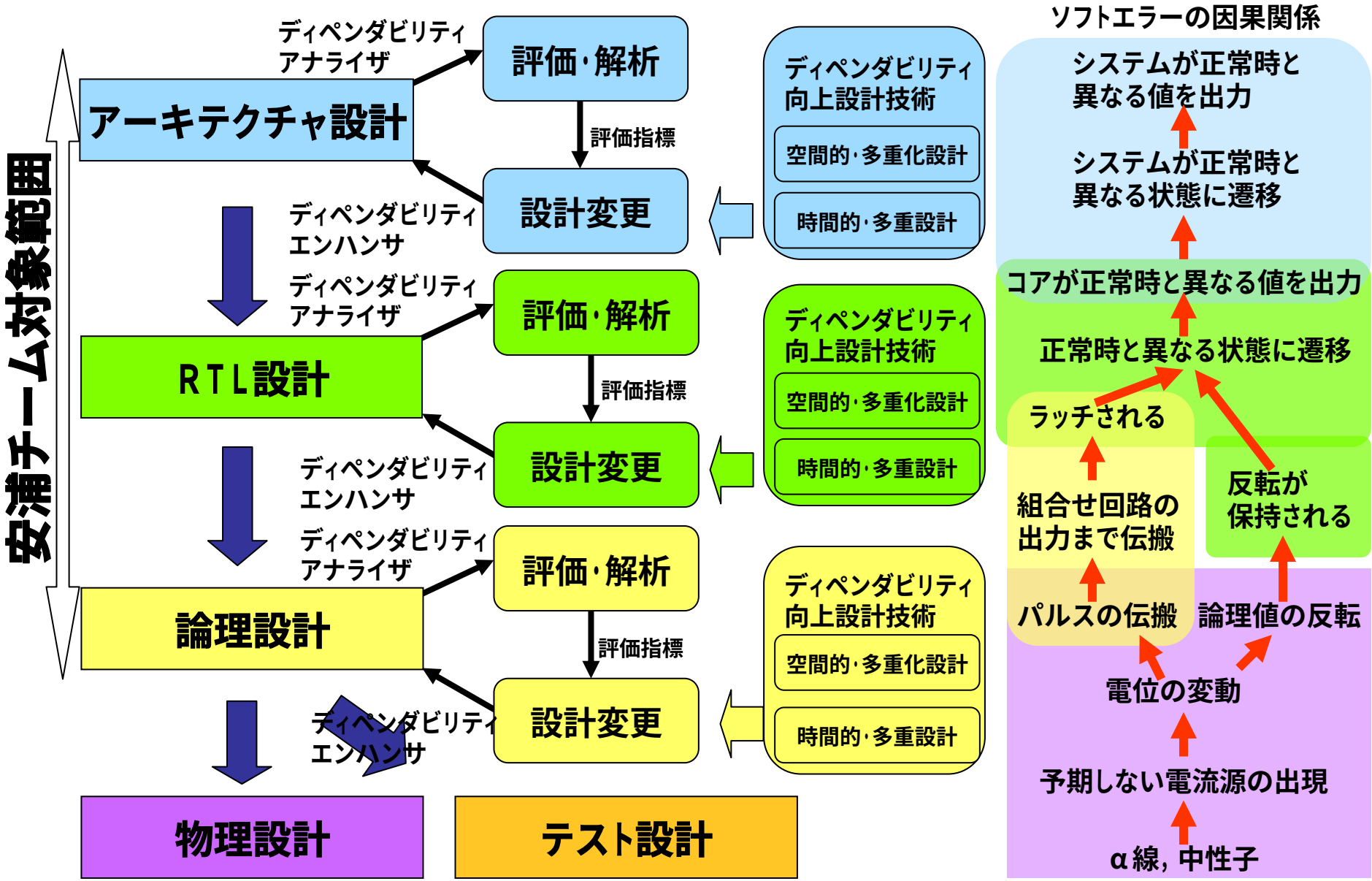
九州大学
システム情報科学研究院
安浦寛人教授，松永裕介准教授，
馬場謙介助教，吉村正義助教
システムLSI研究センター
佐藤寿倫特任教授(福岡大)，
豊橋技術科学大学
杉原真講師

研究の目標とアプローチ

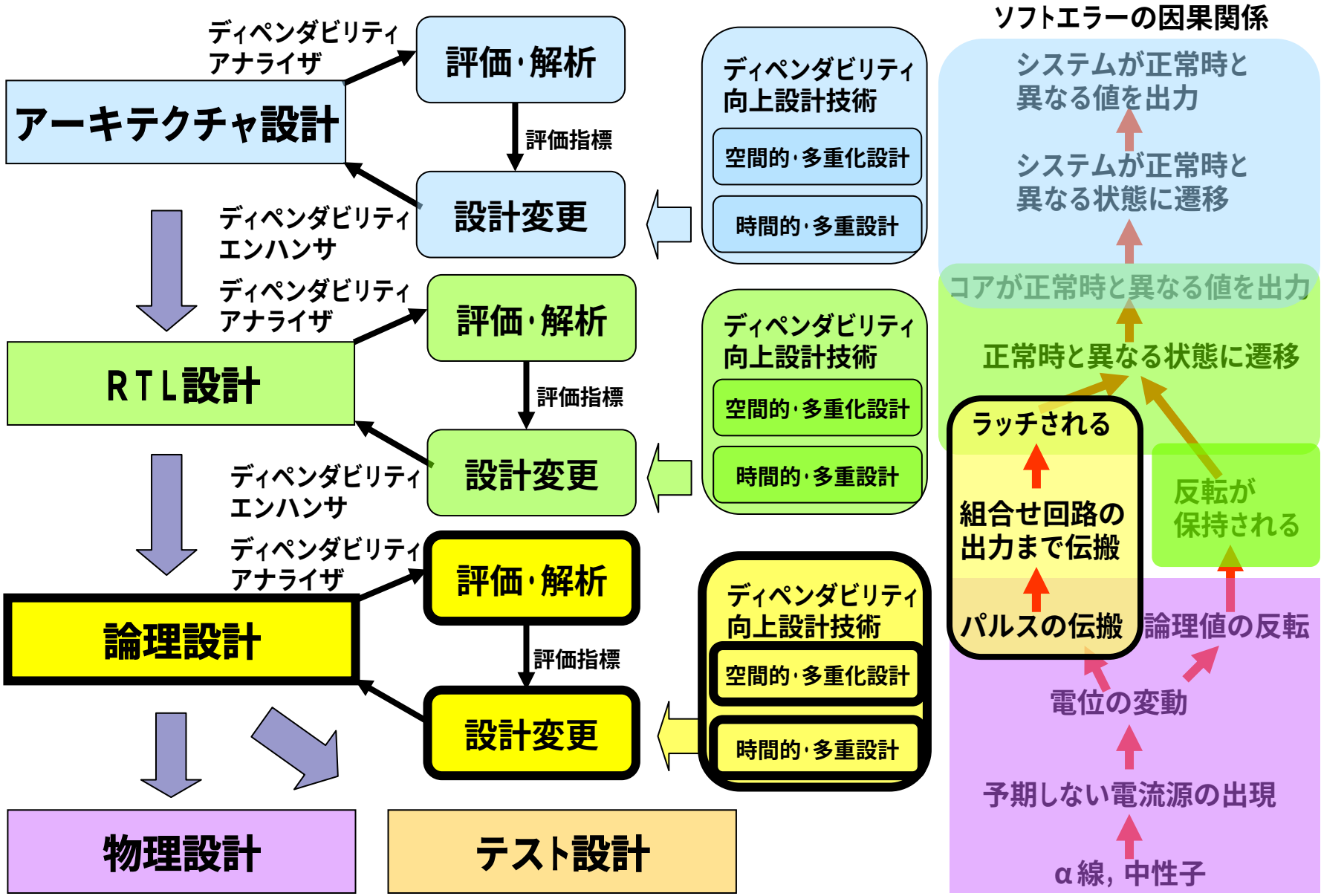
- さまざまな種類のエラー(製造故障、ソフトエラー、タイミングエラー、設計誤り、不完全な仕様に基づく誤り、悪意のある攻撃など)に対して、**統一的な視点からディジタルVLSIシステムのディペンダビリティを確保するための設計技術**の確立を目指す。
- ディペンダビリティの解析と対策回路の合成を行う**EDAツール**を核とした、ディペンダブルLSI向け設計フローを構築する。
- **具体的な問題から、一般化、ツール構築、フロー構築へ**と展開する。

ソフトエラーやセキュリティを考慮したEDAツールが存在しない

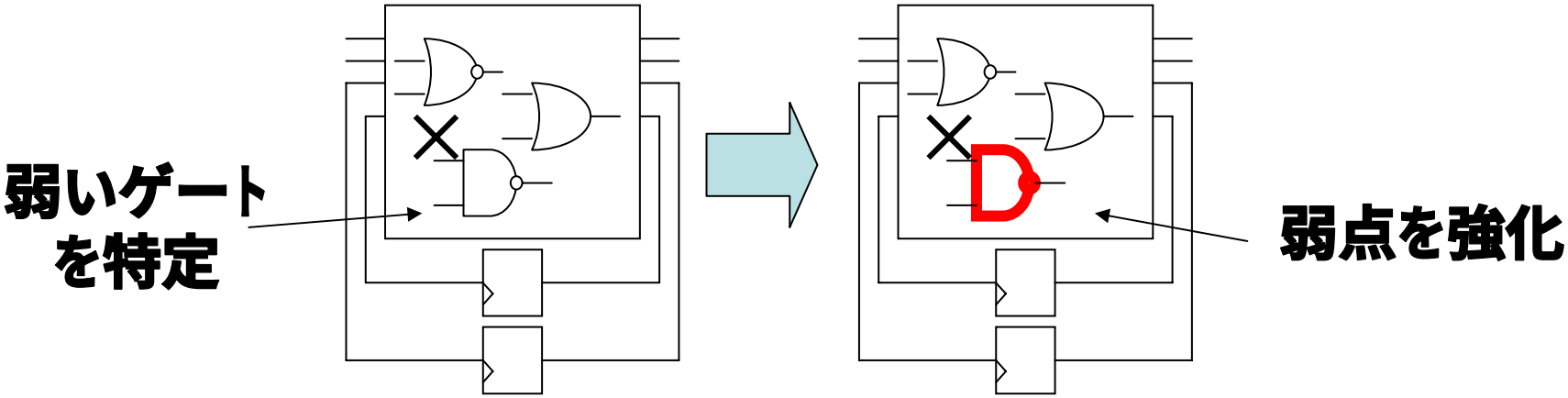
設計ツールとフローの構築



論理設計


ディペンダビリティ
アナライザ
評価・解析
アーキテクチャ設計
評価指標
設計変更
ディペンダビリティ
向上設計技術
空間的・多重化設計
時間的・多重設計
ディペンダビリティ
エンハンサ
ディペンダビリティ
アナライザ
評価・解析
RTL設計
評価指標
設計変更
ディペンダビリティ
向上設計技術
空間的・多重化設計
時間的・多重設計
ディペンダビリティ
エンハンサ
ディペンダビリティ
アナライザ
評価・解析
論理設計
評価指標
設計変更
ディペンダビリティ
向上設計技術
空間的・多重化設計
時間的・多重設計
物理設計
テスト設計
ソフトエラーの因果関係
システムが正常時と
異なる値を出力
システムが正常時と
異なる状態に遷移
コアが正常時と異なる値を出力
正常時と異なる状態に遷移
ラッチされる
組合せ回路の
出力まで伝搬
パルスの伝搬
反転が
保持される
論理値の反転
電位の変動
予期しない電流源の出現
α線，中性子

組み合わせ回路用ソフトエラー耐性解析ツールの開発(1) (松永, 吉村)



- 組み合わせ回路中に生じたソフトエラーが, FFまで到達し, FFに取り込まれる確率を計算するツールを開発
  - 厳密手法を論理回路の構造に着目して, 1.2〜2倍高速化する
  - 既存近似手法との速度差 : 数〜数十倍
- 解析結果に基づいて, テクノロジマッピングや論理最適化を行う手法を検討中

評価指標

$$P_{er} = P_{se}(g) \cdot P_{prop}(g)$$

P_{er}:ゲートgでソフトエラーが発生し, FFに取り込まれる確率

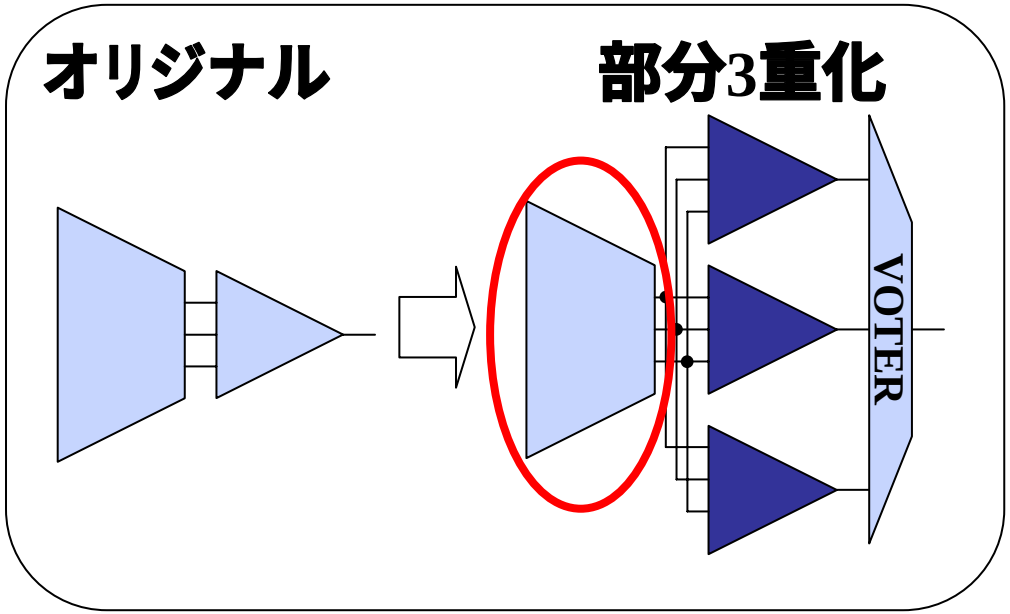
$P_{se}(g)$:ゲートgでのソフトエラーの生起確率

$P_{prop}(g)$:gのソフトエラー伝搬率

組み合わせ回路用ソフトエラー耐性解析ツールの開発(2) (松永，吉村)

既存の近似手法の問題点

・部分3重化した場合，3重化されていない部分も，3重化されたと誤判定する



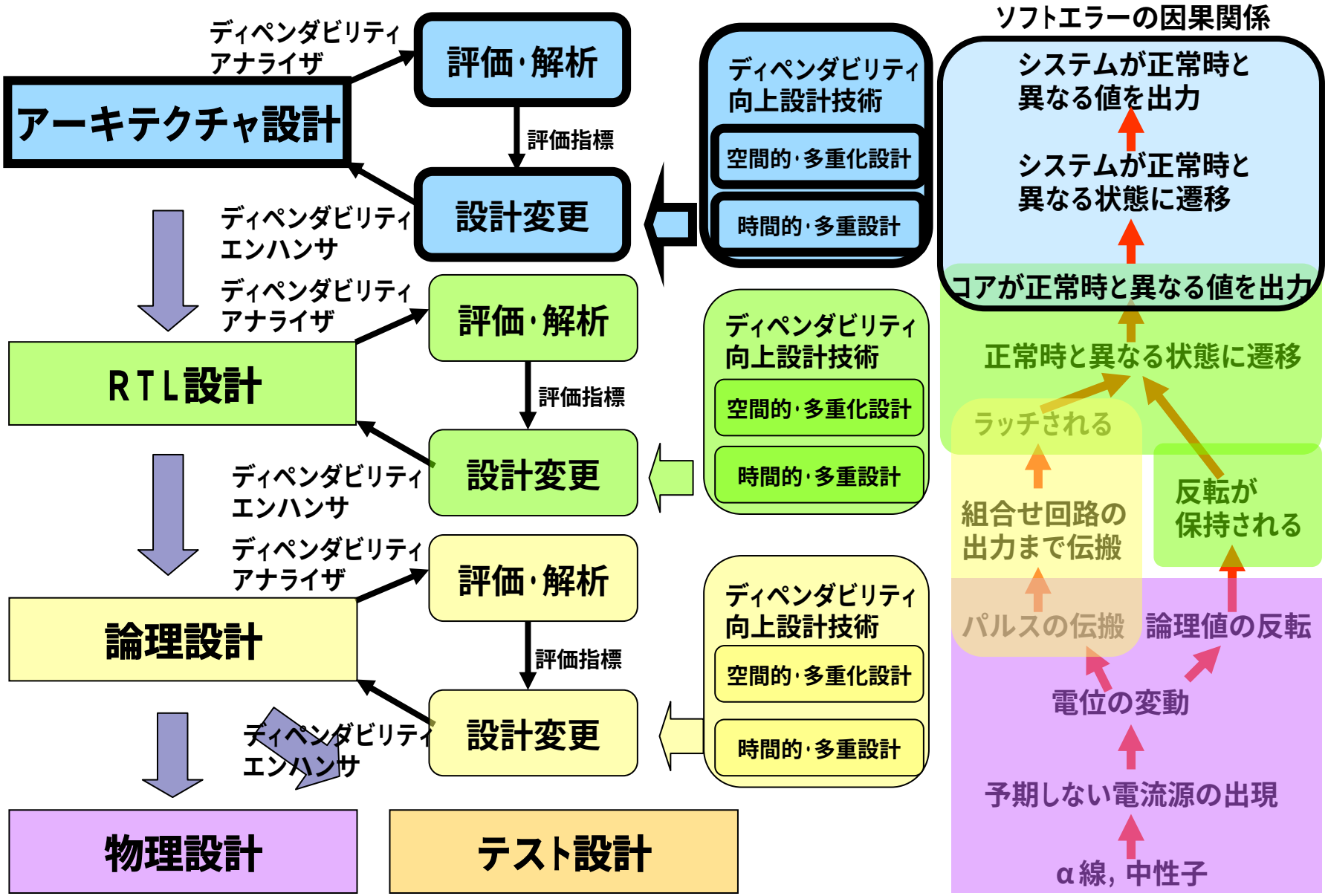
回路のソフトエラー耐性UP

⇩

近似手法による測定誤差UP

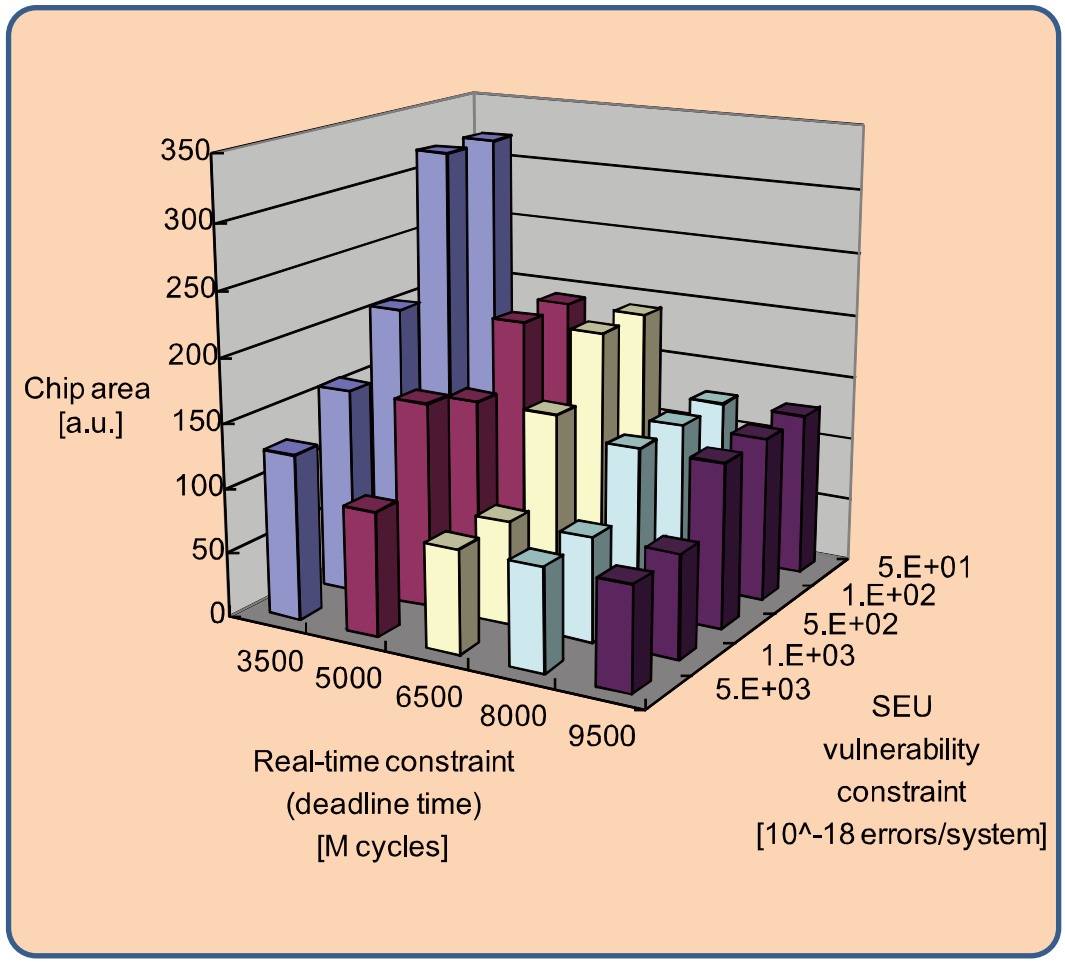
既存の近似手法はNG

アーキテクチャ設計

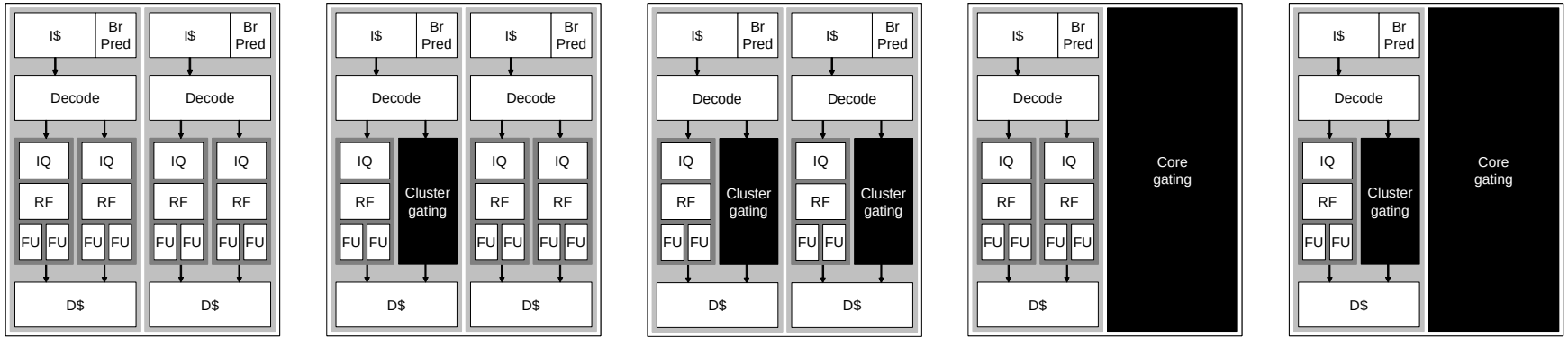

ディペンダビリティ
アナライザ
評価・解析
アーキテクチャ設計
評価指標
設計変更
ディペンダビリティ
エンハンサ
ディペンダビリティ
向上設計技術
空間的・多重化設計
時間的・多重設計
ディペンダビリティ
アナライザ
評価・解析
RTL設計
評価指標
設計変更
ディペンダビリティ
エンハンサ
ディペンダビリティ
向上設計技術
空間的・多重化設計
時間的・多重設計
ディペンダビリティ
アナライザ
評価・解析
論理設計
評価指標
設計変更
ディペンダビリティ
エンハンサ
ディペンダビリティ
向上設計技術
空間的・多重化設計
時間的・多重設計
物理設計
テスト設計
ソフトエラーの因果関係
システムが正常時と
異なる値を出力
システムが正常時と
異なる状態に遷移
コアが正常時と異なる値を出力
正常時と異なる状態に遷移
ラッチされる
反転が
保持される
組合せ回路の
出力まで伝搬
パルスの伝搬
論理値の反転
電位の変動
予期しない電流源の出現
α線，中性子

信頼性と性能を考慮したマルチプロセッサのキャッシュ構成最適化(杉原)

- キャッシュサイズに対する信頼性と性能の要求は相反する
- 以下の設定で最適化を行う
- 制約
  - 信頼性(単位処理あたりのソフトエラー数)
  - 性能(処理時間)
- 目的関数
  - 面積最小
- パラメータ
  - プロセッサ数
  - 各プロセッサのキャッシュサイズ



マルチコアプロセッサにおける信頼性と電力と性能の関係 (佐藤)



(a) Dual large core (b) Hetero core (c) Dual small core (d) Single large core (e) Single small core

- クラスタ・ゲーティング & コア・ゲーティング
  - 様々なスケールと構成を実現可能
- 電力と性能とのトレードオフを考慮可能
  - 要求性能に必要な電力のみを供給⇒電力利用効率改善
- 異なる構成における個々の指標の評価中

その他の研究テーマ(1)
タイミングエラーを予報する技術(佐藤)

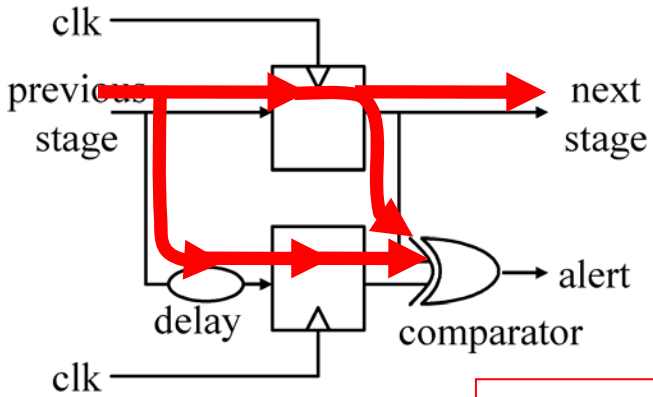
- DVS (Dynamic Voltage Scaling)で限界まで動作電圧を落としたいが，設計時には電圧を判定できない

  ⇩

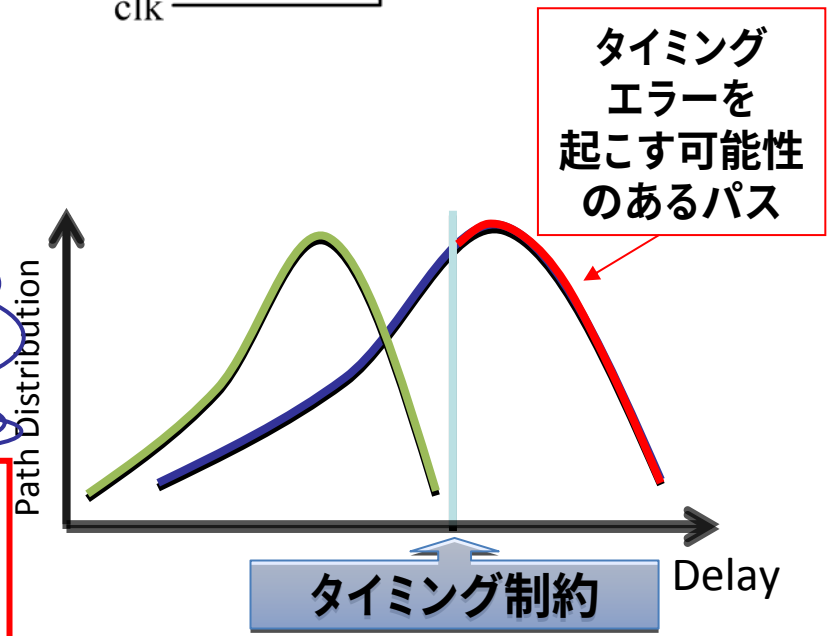
  動作時にカナリアFFを用いて判定する
- すべてのFFをカナリアFFに置き換えると，オーバーヘッドが大

  ⇩

  全てのFFをカナリアFFに置き換える必要はない



タイミングエラーを起こさないパスを特定し挿入するカナリアFFを限定することで面積のオーバーヘッドを抑制する

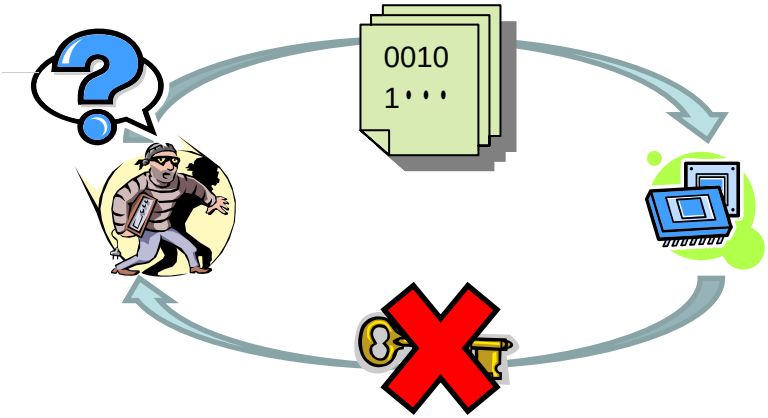


面積の増加：
MeP**コアで約**11%，M32R**で約**2%

その他の研究テーマ(2)

セキュリティとテスタビリティを両立するテスト容易化設計技術(吉村)

人為的攻撃による脅威



何がスキャンインされて，何がスキャンアウトされてはいけないのかを整理

どんな値をスキャンイン，入力されても鍵を特定できる情報はスキャンアウト，出力されないことを保障

暗号アルゴリズムとハードウェアの関係からスキャン化するFFを決定

防御法を実験で評価

DESの実装例に対する適用例

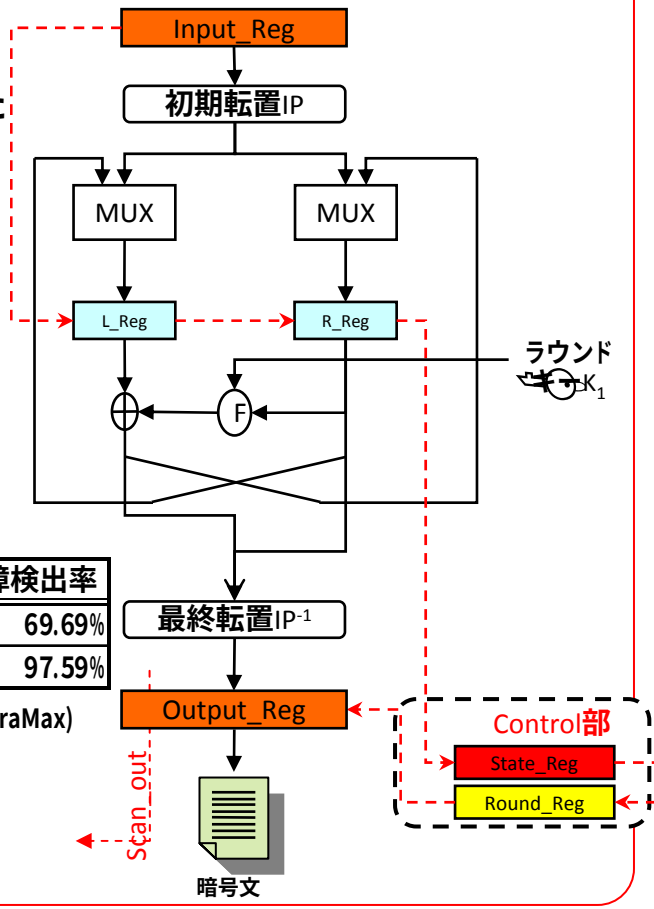
故障検出率を高めつつスキャンパスを利用した攻撃を防ぐためのスキャンパス構成

観測/制御可能

観測可能

制御可能

いずれも不可



可観測性/可制御性	故障検出率
入出力レジスタのみ可	69.69%
提案手法	97.59%

ATPGツール(シノプシス社製 TetraMax)

まとめ

- ソフトエラー関するアーキテクチャ設計から物理，テスト設計までのディペンダブルVLSI向け設計フローを提示
- ディペンダブルVLSI向け設計フローにおける5つの要素技術を紹介