

DARTシステムにおける機能安全

CREST/DVLSI 領域会議

2010年10月2日

九州工業大学

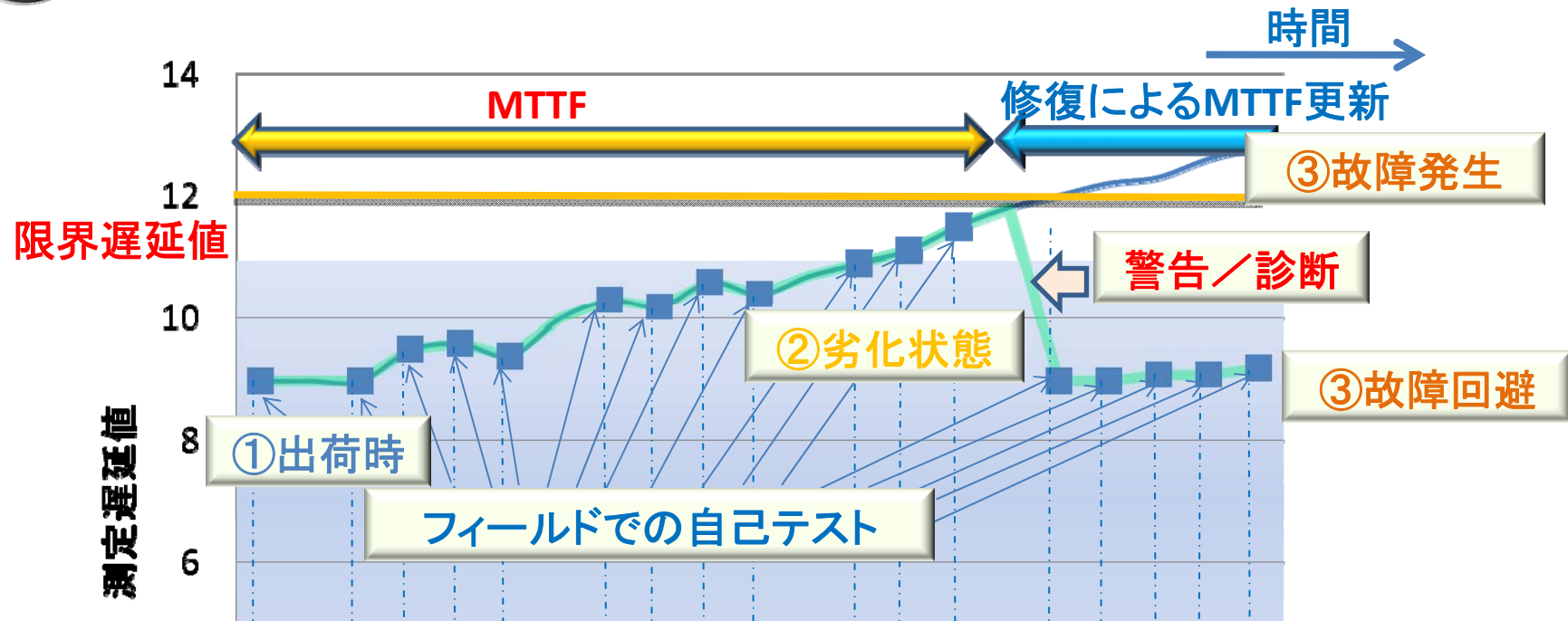
梶原誠司





DARTの基本コンセプト

2



- フィールドで、パワーオン・オフ時／定期的に自己テスト
- テストモードで遅延測定(ログ保存)
- 故障検出／劣化検知による警告・診断

突然のシステムダウンを回避・・・安全・安心

ディペンダブル システム … ユーザーの頼りになるシステム



アプリケーションニーズ

| | 車載・医療 | プラント制御 | ネットワーク・サーバ | LSI生産 |
|-------------------|--------------------|-----------------------|-------------------------|-------------------|
| 使用期間 | 長期 (~20年) | 超長期 (20~50年) | 通常 (~10年) | — |
| フィールド テスト | パワーオン時 のテスト | テストモード | 無休止 (動作中) | — |
| テストリソース (メモリ等) | LSIピン, メモリ 等ひっ迫 | 制約あり (冗長設計等 採用) | 制約あり (劣化データ 蓄積興味) | 制約小 (ATE利用) |
| テスト時間 | ~10ms | ~100ms | 数10~ 数100ms | 物理制約小 (コスト制約有) |

従来のLSIテストと異なる厳しい物理制約あり



機能安全規格との関連

□ 機能安全の国際規格 IEC 61508

- 電気式／電子式／プログラマブル電子式安全関連**システム**の機能安全性
- システムを構成する要素や部品の**故障リスク**を軽減し、安全性を高める

安全に関わる故障・障害

ランダムハードウェア故障

- 部品の劣化, 製造ばらつき, ソフトエラー等
- 故障確率で定量的に規定

決定論的原因故障

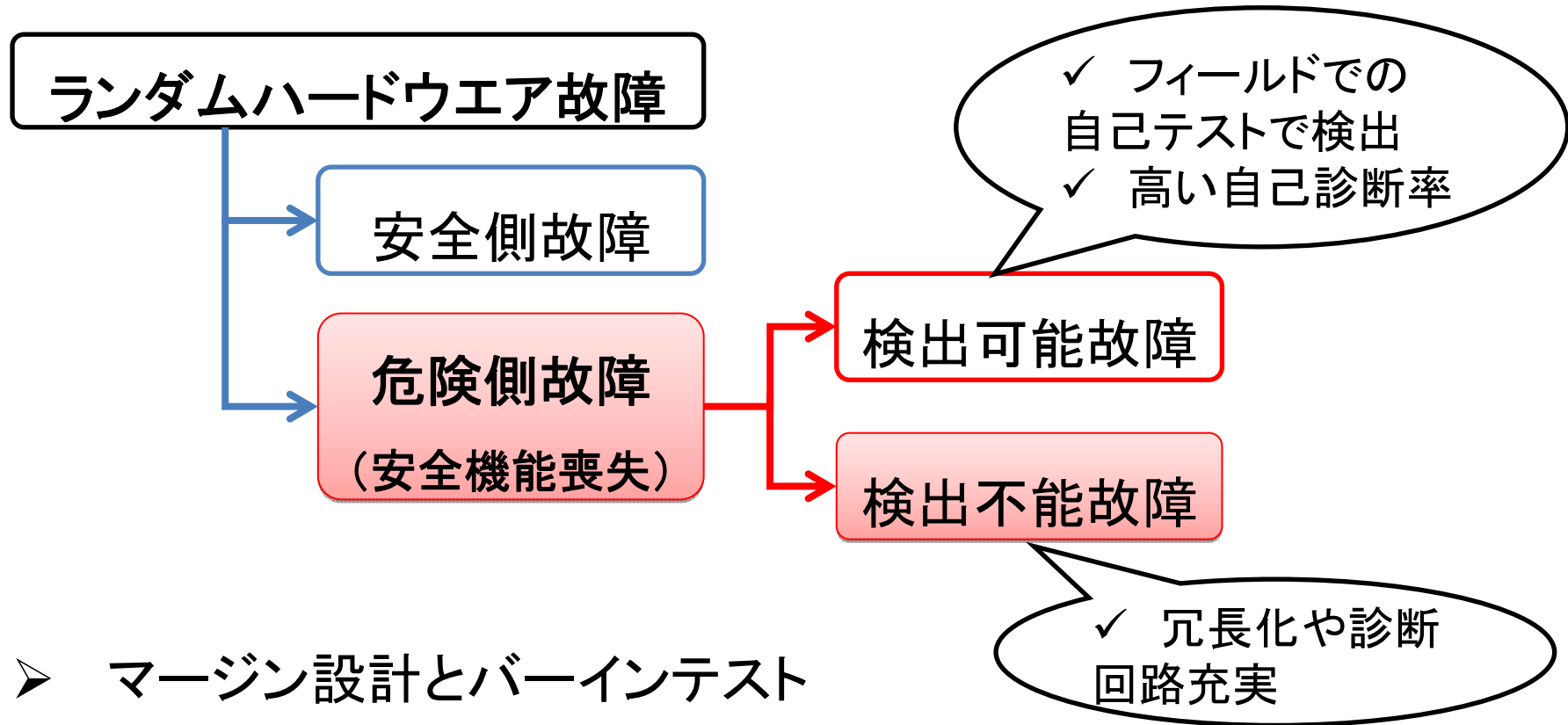
- 設計誤り, 製造欠陥, 運用ミス等
- 安全ライフサイクルで定性的に規定

□ 安全度水準 (SIL: Safety Integrity Level)

- 安全性のレベルを4段階 (SIL1~SIL4) で表現



ランダムハードウェア故障への対応



- マージン設計とバーインテスト
 - 劣化・ばらつきに対応
- 冗長設計
 - ソフトエラー・劣化に対応



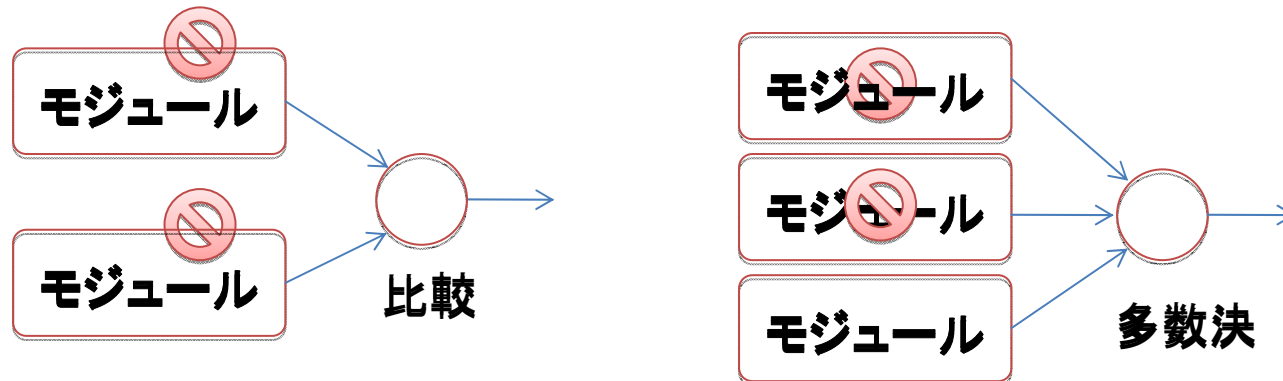
DARTの機能安全へのインパクト

□ マージン設計とバーインテスト

- 微細化により, 劣化の見積もりが難しく, **マージン過剰・過小評価**
- 劣化の進度は, 動作環境や使用データへの依存性が高い
- DARTによるフィールドテスト, 内部の「見える化」で対応

□ 冗長設計(SIL3以上)

- 同じ環境で, 同じ動作を行うことで, 多重化したモジュールが同時に劣化 → **共通原因故障(CCF: Common Cause Failure)**

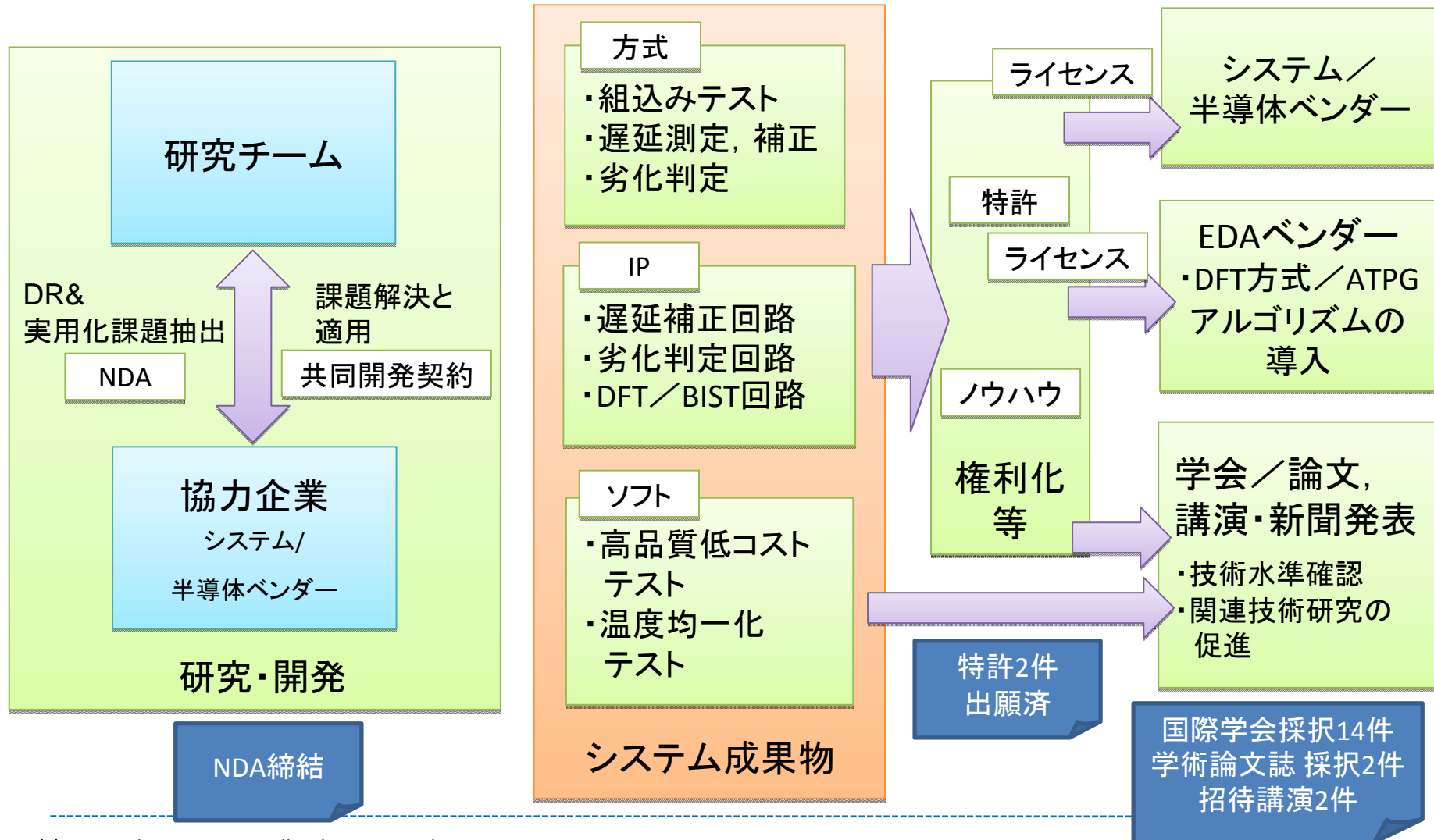


- DARTによる遅延計測による劣化検知で共通原因故障にも対応

SIL3以上が要求されるLSIの標準技術に！



■ システム／要素の複数切り口での実用化を目指す





フィールドテスト適用：遅延測定用DFT

