CREST「ディペンダブルVLSIシステムの基盤技術」研究領域
平成24年度 第2回 領域会議 向 資料

ディペンダブルVLSIシステムへの期待

自動車向マイコンから見た機能安全(ISO26262)を通して

ルネサス エレクトロニクス株式会社
自動車事業統括部　自動車コア技術部

安増 貴志

takashi.yasumasu.jy@renesas.com

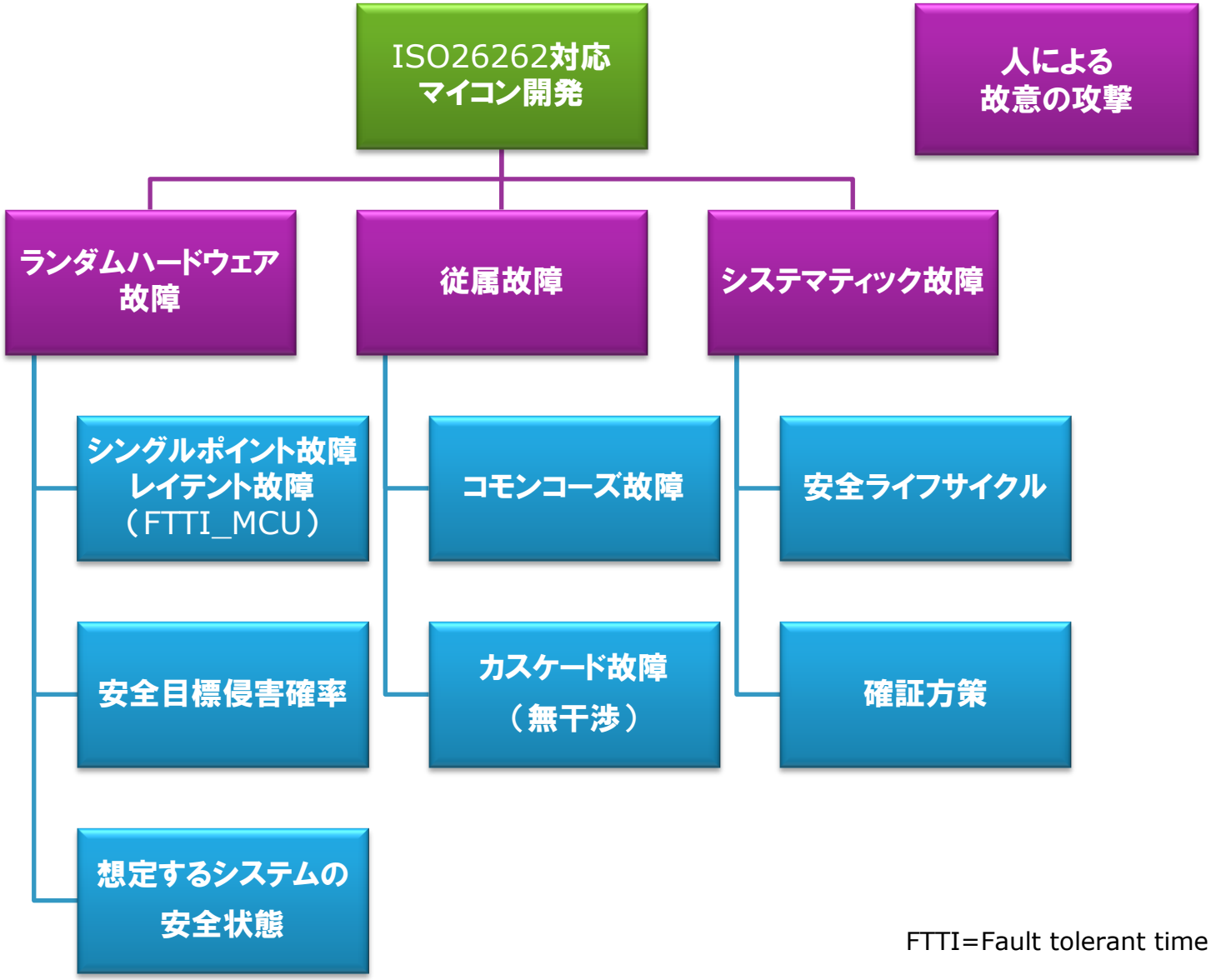
2013/03/16　Rev. 1.00

ISO26262(自動車向け機能安全規格)と将来の技術

- ISO26262:自動車向の新しい安全の指標
  - State of the art としての機能安全規格
  - 開発プロセスと技術両面からの対応
  - クルマの安全目標から技術安全要求を導出 ： V字開発モデル

- 将来の技術
  - 運転支援→自動走行が可能な技術
  - ISO26262 を対応する上での一般的な技術的課題
    - 性能(ミッションロジック)と故障検出技術のバランス
    - ASIL-x (SPFM, LFM, PMHF), 想定されるシステムの安全状態・時間的制約(フォールトトレラントタイムインターバル)
    - 安全機構定量化時の説明容易性
    - 性能向上・機能統合・協調制御に伴う新しい故障モード
    - 量産性(パッケージ・熱・コスト)

ISO26262から見たディペンダブルVLSIでケアすべき故障



FTTI=Fault tolerant time interval

故障率

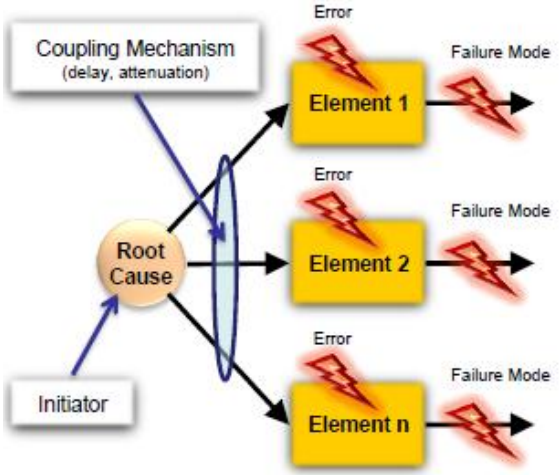
	Method (Part5 8.4.3)	Outline	feature
1	Using hardware part failure rates data from a recognized industry source	•IEC62380や SN29500等 のハンドブック	•皆が活用でき普遍的 •故障率の実態と乖離している 可能性が排除できない （活性化エネルギーが一定・ パッケージ故障率が支配的）
2	Using statistics based on field returns or tests. In this case, the estimated failure rate should have an adequate confidence level	•市場データ	•信頼できるデータ収集に難しさあり • 統計手法の明確な基準無し
3	Using expert judgment founded on an engineering approach based on quantitative and qualitative arguments. Expert judgment shall be exercised in accordance with structured criteria as a basis for this judgment. These criteria shall be set before the estimation of failure rates is made	•Expert Judge	•エキスパートによる判断に対して 幅広く受け入れられるかがポイント •他部品と整合取る為、スケーリング が必要なケースあり

故障率はハンドブックが採用されるケース多い→ダイアグカバレッジ向上が必要

従属故障

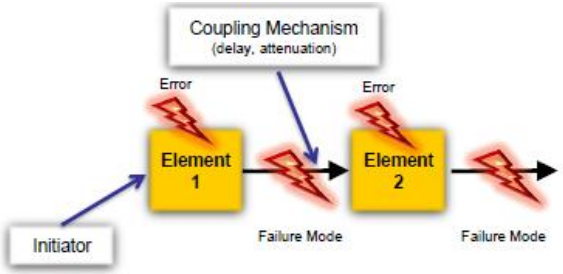
従属故障

- **共通原因故障**(Common Cause failure)
  - **特定の単一事象または元の原因に起因するアイテム内の二つ以上のエレメントの故障**
- **カスケード故障**(Cascading failure)
  - **同一アイテム内の他のエレメントの故障原因となる，エレメントの故障**
  - Coexistence of elements **におけるインターフェアランスフリー分析**



共通原因故障

（例） 電源、クロック等でDCLSのリダンダント回路に影響



カスケード故障

（例） 低いASIL ソフトウェアによるレジスタ値破壊

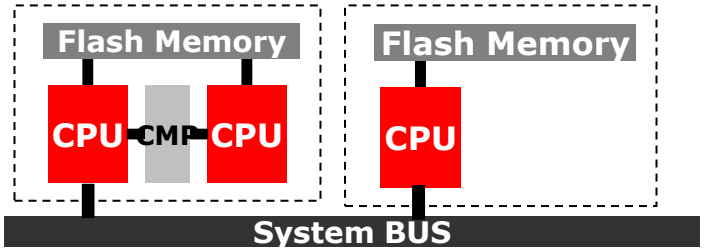
ディペンダブルVLSIにおいて、従属故障対策は重要(統合化・マルチタスク)

ルネサスマイコンでのアプリ別マルチコア展開例

40nm Architecture

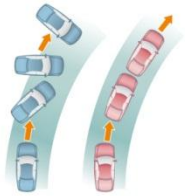
Performance

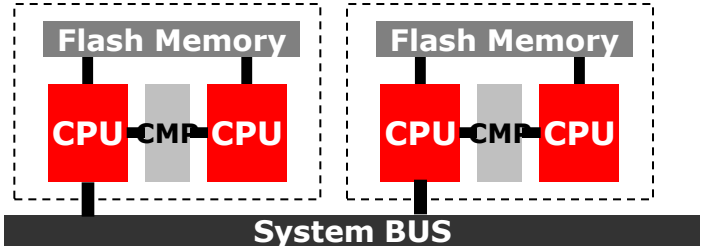
Fast time to detect the faults



Hybrid (DCLS plus single core)
Engine Control, ADAS

High performance
Real time operation



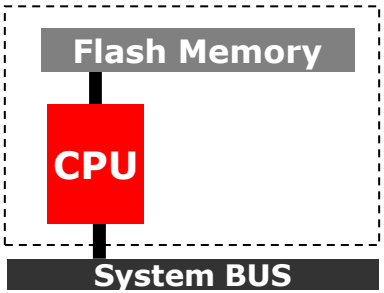


Dual DCLS
ADAS, Server

- **Dual lock step architecture**

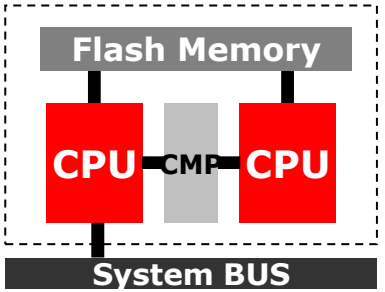
- **Cost and performance**
- **1oo1D Architecture**

- **No latency for error detection**
- **Dual core lock step**



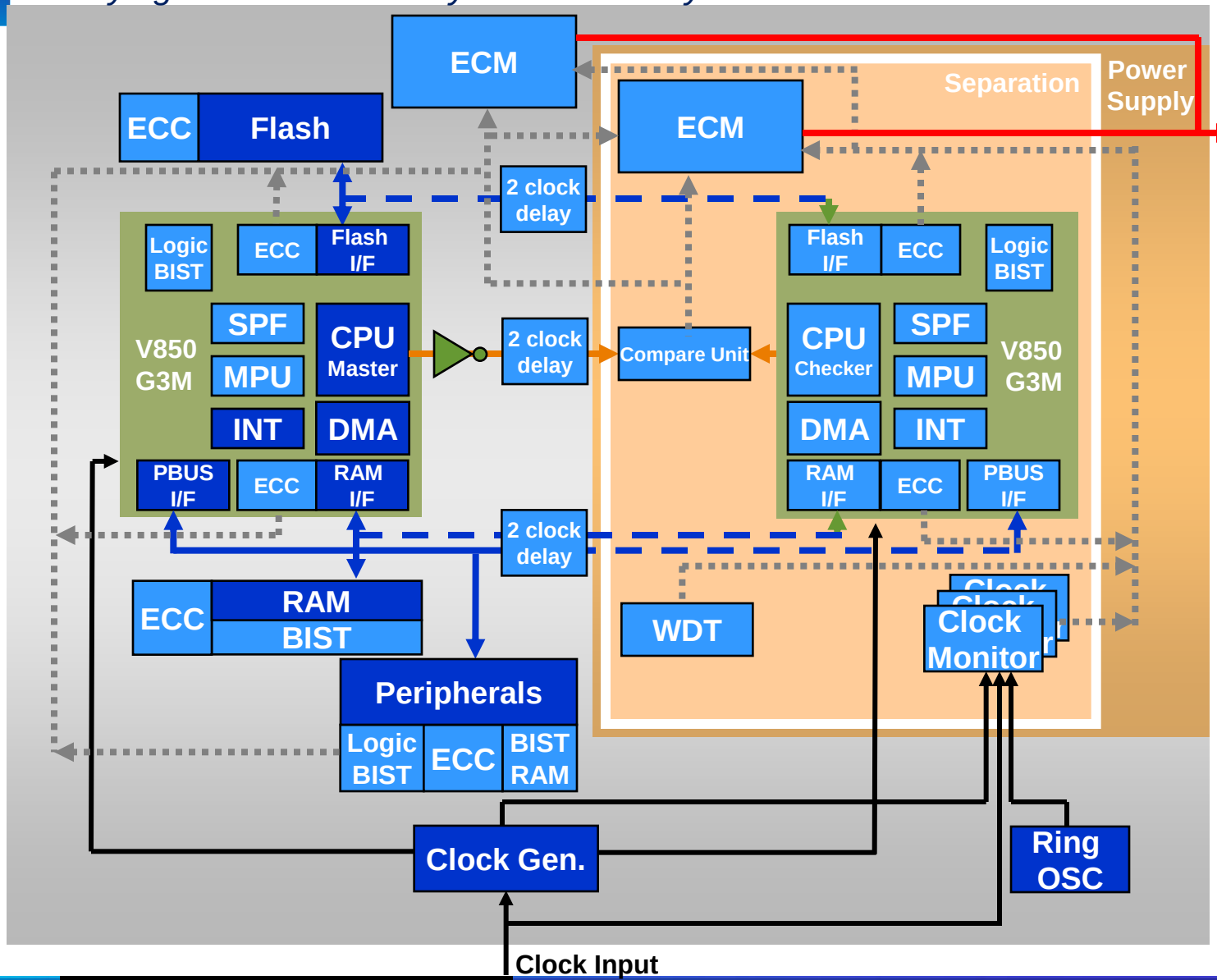
Single Core
Airbag/Body
Central gateway

DCLS
(Dual Core Lock Step)
Braking/Steering
Motor Control



安全機構検討例(アプリ非依存部)

Trying to have rich safety mechanism by hardware to achieve fast FTTI



- Standard MCU
- Error Correction
- Systematic Faults
- Built In Self Test
- Redundancy
- Clock Monitors
- ECM
- Common Cause

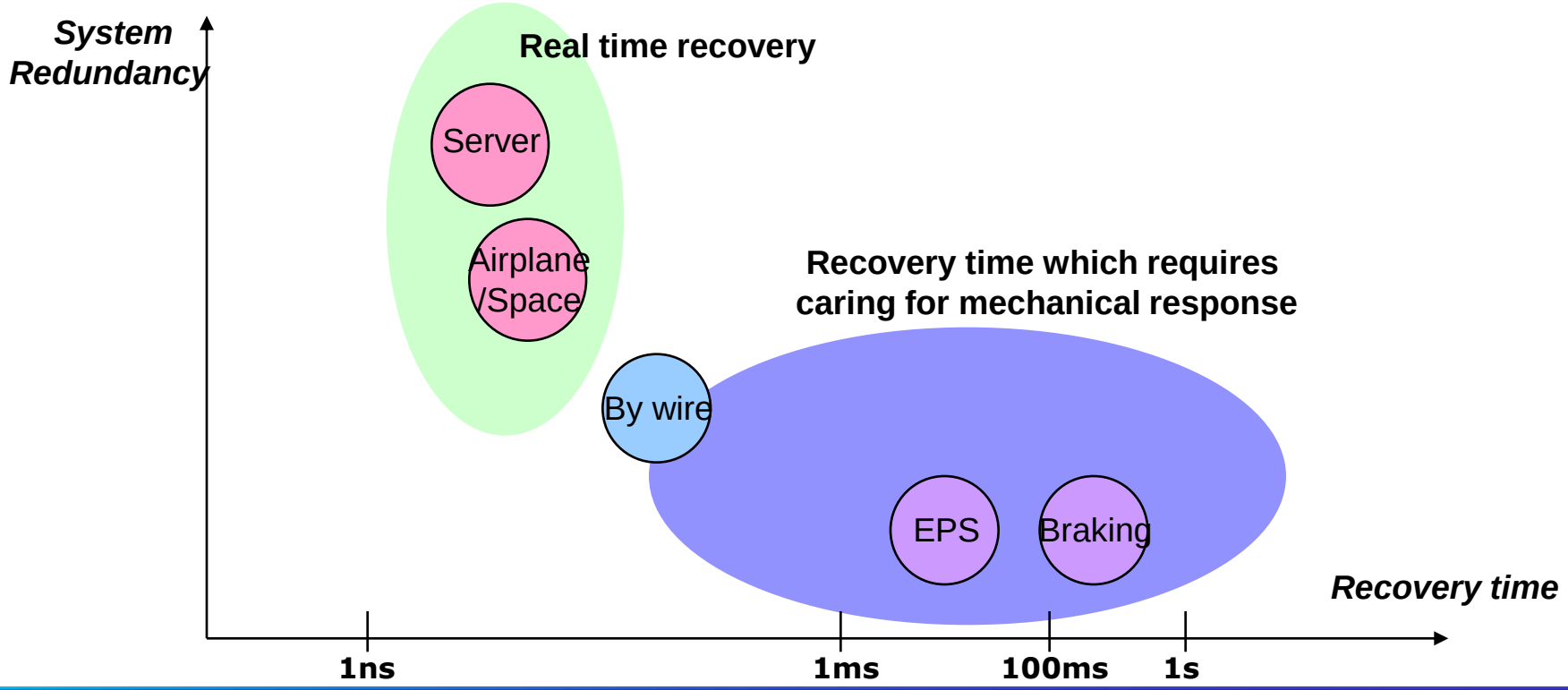
- Inverted signals
- 2-clock delay
- Layout Separation
- Power separation
- Cross talk analysis

In-/Outputs
Inputs
Outputs
Error
Clock

Safety Block
Functional Block

様々なシステムでの想定リカバリ時間例

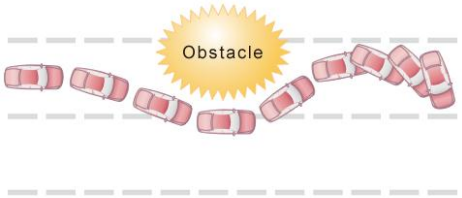
- Recovery time：After 1st fault, to make system in the safe state
  - The behavior after detecting the fault depends on system
    - Server and Airplane　　: Real time switch
    - Automotive　　: Mechanical response time
  - Key is Fault identification time and its recovery system



フェイルオペレーショナルシステムの時間的制約

- フェイルオペレーショナルシステムにおけるFTTIの例

システムにおける時間的制約を踏まえ、かつ動作の継続に向けた安全機構を用意



More Controllability

Retry & Recovery→
Try the same sequence again,
Diagnosis again etc.

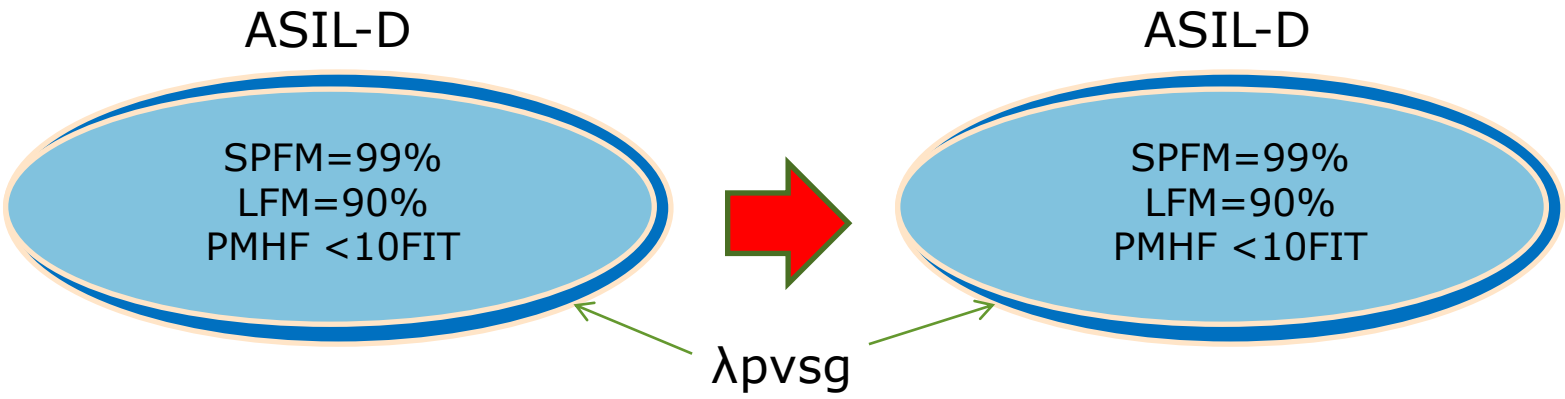
ディペンダブルVLSIへの期待

1回目の故障後も主機能を継続し ASIL-D → ASIL-D を実現する技術

ディペンダブルVLSI研究への期待

- 1回目の故障後(*)も主機能を継続しASIL-D →ASIL-D を実現する技術
- 車載向けにISO26262を考慮された技術
  - SPFM/LFM/PMHF/従属故障/フォールトトレラントタイムインターバル
- 車載量産に向けた　オーバーヘッド(コスト・消費電力)の少ない技術
- システムと連携した　新しい技術でのブレークスルー

(＊)主にPermanent fault



$$M_{PMHF} = \lambda_{RF} + \lambda_{m,DPF} \times \lambda_{sm,DPF\ det.} \times T_{fail\ operational}$$

PMHF: Probabilistic Metric for random Hardware Failures
RF : Residual Fault, DPF:Dual Point Fault

ルネサス エレクトロニクス株式会社