

機能安全とディペンダビリティ

撫原 恒平 (NADEHARA, Kouhei)
kouhei.nadehara.jy@renesas.com

Renesas Electronics Corporation
Brand Strategy, 1st MCU Div.

Jun. 9, 2012

なぜ「機能安全」というのか？

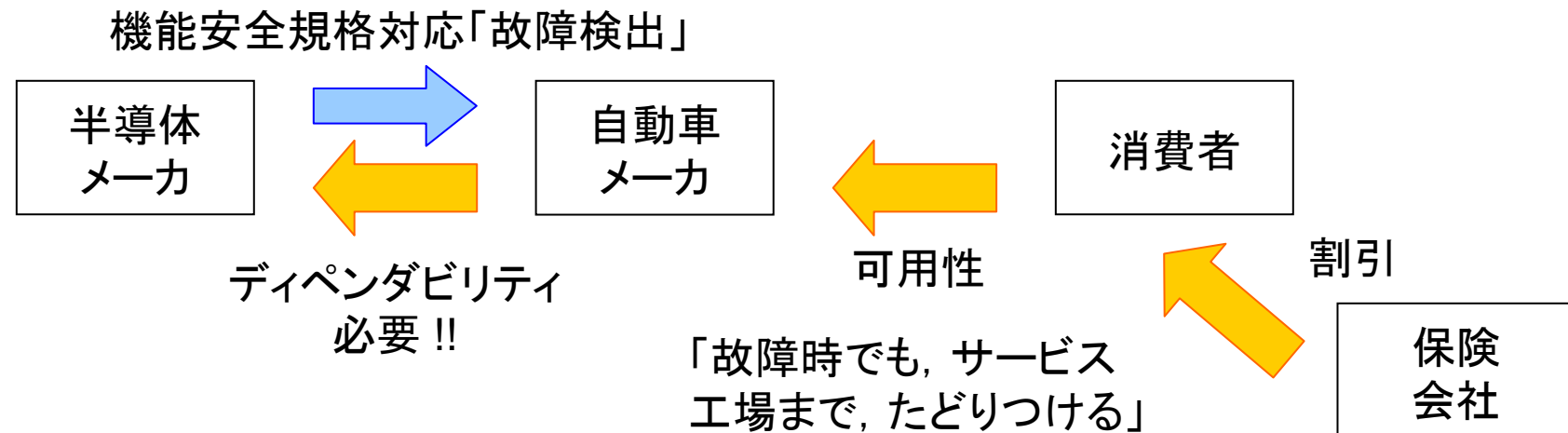
- 「ディペンダビリティ」を「見える化」したい
 - ディペンダビリティを製品の価値 (LSI の価格) につなげたい

- 基準がないと説明しにくい
 - 「他の LSI より壊れにくいです」
「無くても一応動くし...あればいいのかもしれないが, 必須ではないね...」
- 機能安全対応可否はわかりやすい区別
 - 車載の例: 「機能安全規格 ISO26262 ASIL D に対応しています」

- こう問われたら, どう答えるか?
 - 「それは機能安全に対応するための最良 (最低コスト) の手段ですか?」
(= 故障の検出だけで充分, 動き続ける必要はないのでは?)

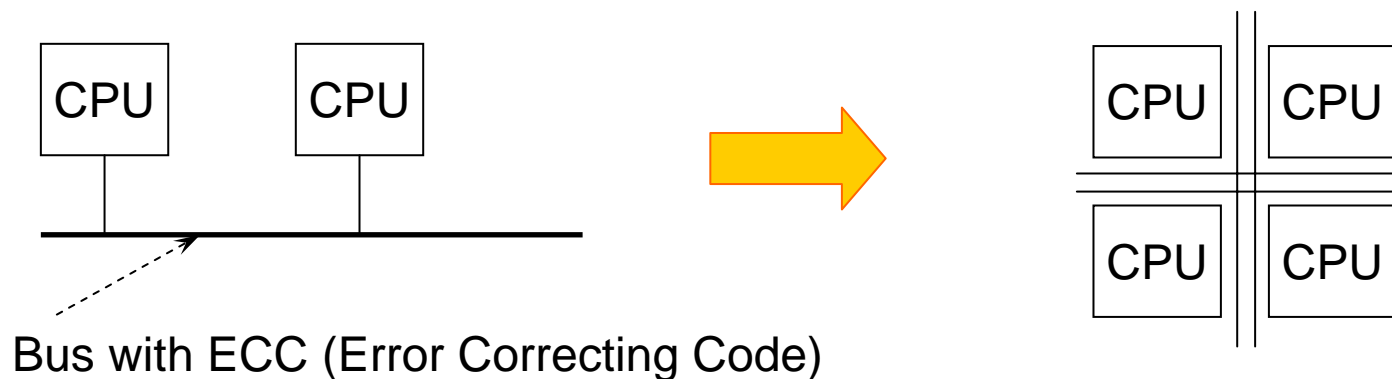
最終顧客の利便性として見せる

- 消費者の利点を強調し、自動車メーカーの「安全目標」を変更
- 「安全目標」を「故障時は、止まる」に設定
→ 検出機構があれば規格を満たせる
- 「安全目標」を「故障時、最寄のサービス工場までたどりつける」に設定
→ 可用性が必要 → ディペンダビリティの必要性
 - 「消費者の声」として自動車メーカーに届ける
 - 金銭的インセンティブを付与すると、強力
「自動車保険料/会費の割引」



ディペンダビリティの手段としての NoC

- マルチコア、メニーコア時代のオンチップ・コネクティビティの姿は?
- 「安全目標」を「故障時は、止まる」に設定
 - 「伝統的バス + パリティ」で故障検出すれば達成できる
- 「安全目標」を「故障時、最寄のサービス工場までたどりつける」に設定
 - 可用性が必要 → 最適な実装は?
- 「伝統的バス + ECC」
 - コア数が少なければ...
 - 一品種だけ設計なら...
- Network-on-Chip
 - コア数の増減によるスケラビリティ実現が容易. 開発期間短縮.



まとめ

- 機能安全の観点から、ディペンダビリティを実現する手段を探索
- 前提として、可用性の必要性が要説明
 - 機能安全をみたすだけなら、可用性は必須ではない
 - 消費者にとって便利な「安全目標」を設定すると、可用性が必須に
- 可用性＋スケーラビリティ
 - 可用性をみたすだけなら、伝統的な手法でよい
 - コア数の異なる品種を短期間で開発するには、NoC が最適



Renesas Electronics Corporation

© 2011 Renesas Electronics Corporation. All rights reserved.