自動車の機能安全とディペンダビリティ

京都高度技術研究所　神原弘之

ディペンダビリティ課題 ＝ 高信頼化と高速化の両立

- **車載ネットワーク**

  FlexRay 等のプロトコル処理の高速化と高信頼化

- **リアルタイム制御**

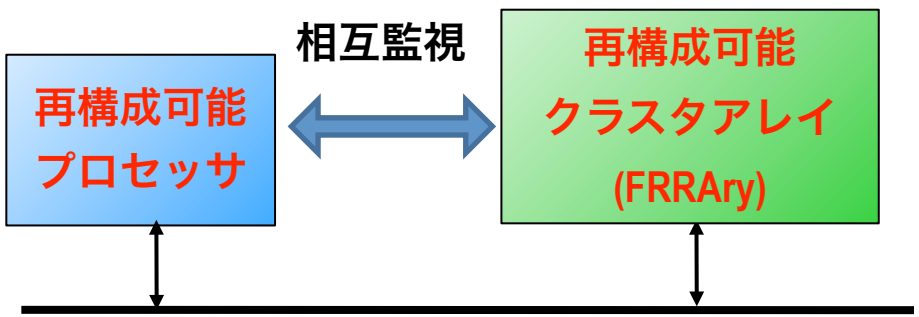
  タスクの実行優先度の状態遷移の高信頼化と高速化

自動車電装分野の ディペンダビリティへの対応

提案プラットフォームでの「高信頼化と高速化の両立」

→ 従来ソフトウェアで実現されていた機能を再構成可能クラスタアレイ（FRRAry）にマッピングして実現

→ 再構成可能プロセッサが「監視」機能を提供



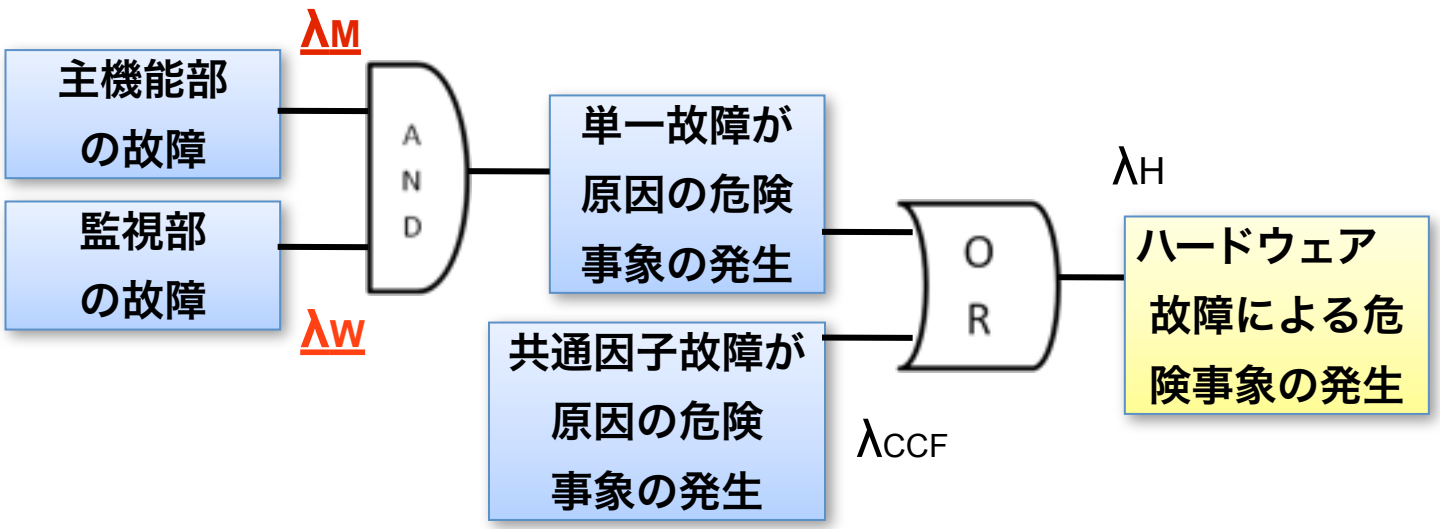
→システム構成要素が相互監視を行い、低コストでディペンダビリティ要求に対応

自動車電装向け機能安全規格（ISO26262）に基づく VLSI のディペンダビリティの定義

ハードウェア故障による危険事象の発生率

$$\lambda H = \lambda M \times \lambda W + \lambda CCF$$ （※近似式）

- λH　：危険事象の発生率
- λM　：主機能部の故障率
- λW　：監視部の故障率
- λCCF　：共通因子故障の発生率

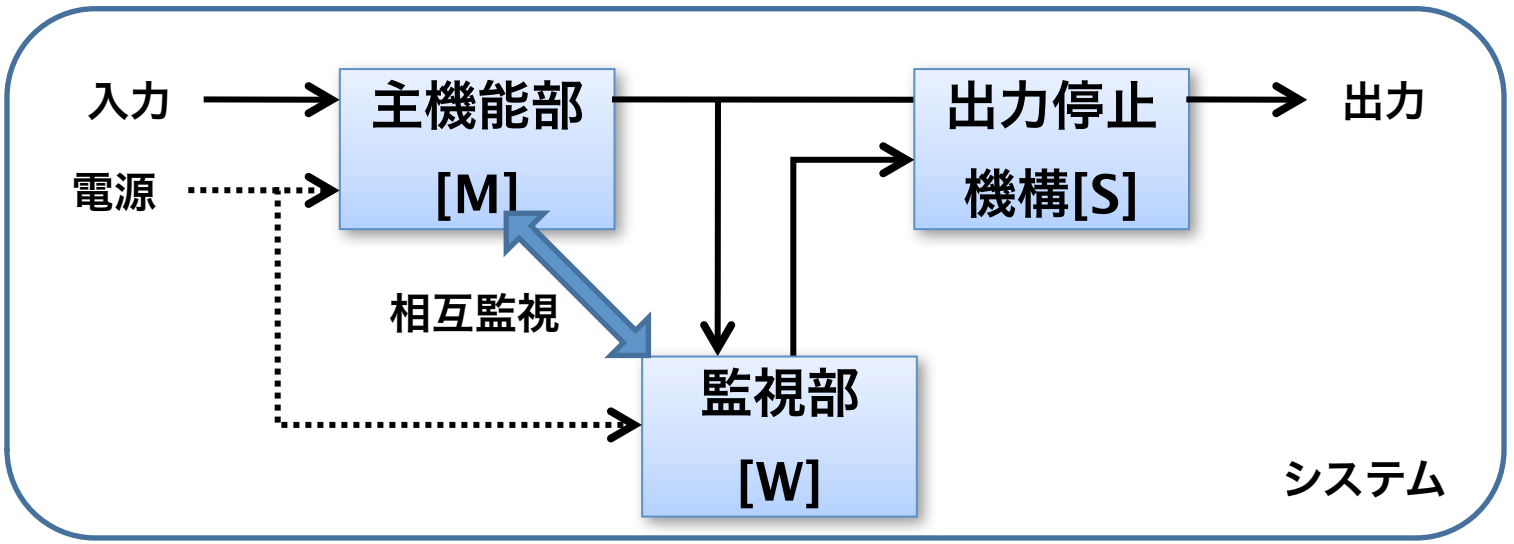


自動車電装向け機能安全規格（ISO26262）に基づく VLSI のディペンダビリティの定義（つづき）

ディペンダビリティの確保 ＝ 相互監視手段の提供

- 他のシステムによる監視
- システム内の他のハードウェアにより行われる監視
- 同一のハードウェア上に実現された監視機能
- ソフトウエアのみによる監視

※主機能部と監視部の動作の独立性が必要



自動車電装向け機能安全規格（ISO26262）について

目的

- 車載電子・電気システムの機能に失陥が発生した時でも、安全性を確保する開発プロセスの標準化
- ISO 規格化は 2011 年中頃？

- IEC61508 （機能安全）をベースに改修
- 自動車用の安全性レベル（ASIL）を（電子システムが提供する）各機能ごとに定義