トップエスイー修了制作

組込み開発におけるリスク分析手法の適用

日本電気株式会社　開発環境技術本部　　和田　美江子　　m-wada@di.jp.nec.com

開発における問題点

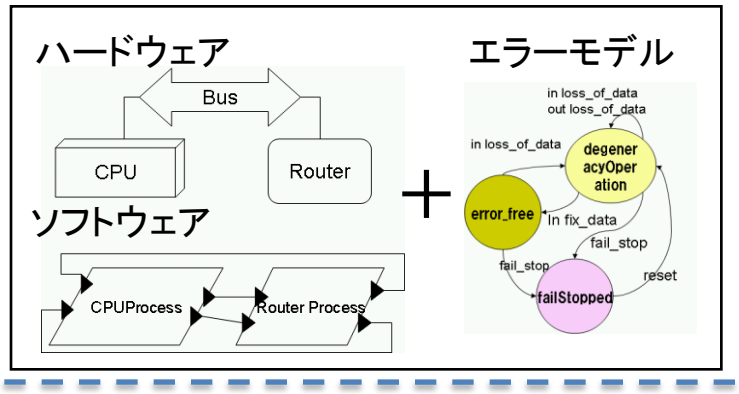
組込みシステムの複雑化に伴い，要求される信頼性を確保するための設計・分析コストが増加している．しかしながら，開発期間の短期化，開発コストの削減が要求させる場合が多く，信頼性の確保においても効率化が求められている．

手法・ツールの適用による解決

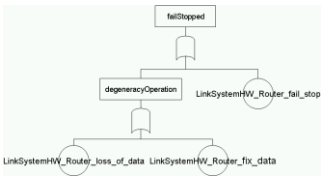
システム設計と一体となった信頼性分析を実現するため，システム設計記述にアーキテクチャ記述言語のひとつであるAADL言語を用いる方法と，品質特性に関する解析手法であるFTA分析をサポートするFTAツールを提案し，複雑なシステムに対する信頼性分析にかかる工数を低減できる可能性を示す．

手法・ツール適用の流れ

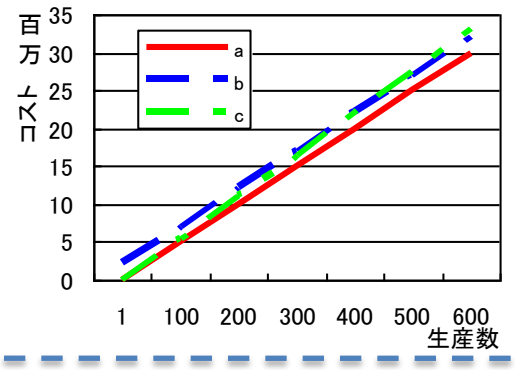
ハードウェアとソフトウェアからなるシステムと，それぞれのコンポーネントに対するエラー情報を同一の設計モデルとして表記



提案ツールによるFTA分析のサポート

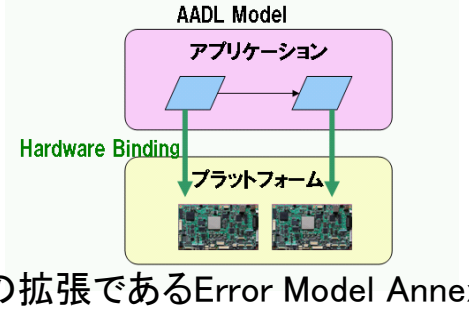


故障率を考慮した製品構成の見直し作業などで活用可能であり，信頼性分析の作業サイクルの短期化へつながると考えられる．



AADL(Architecture Analysis & Design Language)

リアルタイム組み込みシステムの設計記述に対応したアーキテクチャ記述言語．アプリケーションと実行基盤のバインディングが定義されており，ハードウェとソフトウェアをまたがった設計を記述することが可能である．



AADLの拡張であるError Model Annexにより，エラー状態とエラーイベントを定義できる．また，コンポーネント外部へのエラー伝播送出と外部からのエラー伝播入力も定義可能である．

提案ツール

提案ツールは，AADLモデルのエラー状態遷移情報を基にFTAツリーを構成するものである．構成として，Eclipseプラットフォームに実装したFTAツリーエディタと，オープンソースのAADLエディタであるOSATEプラグインの機能を利用したAADLファイルの読みこみ処理部分，AADL情報からFTAツリー生成処理部分により構成される．