平成19年度 情報工学コース卒業研究報告要旨

高田・冨山 研究室	氏　　名	吉村 悠
卒業研究題目	AADL を用いた自動車制御システムの エラーモデル記述	

近年，車の高機能化による制御システムの複雑化が進み，要求されるディペンダビリティを確保するための手間とコストが増大している．そのため，体系的なディペンダブルな設計と分析をアーキテクチャレベルで支援することが注目されており，AADL (Architecture Analysis & Design Language) をはじめ複数のアーキテクチャ記述言語が提案されている．AADL にはエラーの仮定を記述するエラーモデルが含まれている．AADL の前身である MetaH は飛行機の設計に使われ，飛行機システムで一般的なディペンダブル設計である 2 重系や 3 重系の耐故障メカニズムが MetaH のエラーモデルにより記述された．一方，自動車制御システムはフェイルセーフと呼ばれる常に安全側へ制御を倒す動作によってディペンダビリティの確保を図っているが，フェイルセーフを目的にしたエラーモデル記述例は存在しない．

本研究では自動車制御システムのフェイルセーフを目的とした AADL を用いたエラーモデル記述を提案し，システム全体のディペンダビリティを分析できるような合成方法を検討し，合成を試行した．

エラーモデルを付加する前段階として，自動車制御システムの AADL アーキテクチャモデルを記述した．AADL アーキテクチャモデルとは，AADL の特徴である実行時環境を表現したコンポーネントとその接続で記述されたアーキテクチャである．エラーモデルは AADL アーキテクチャモデルに付加することで実行時環境と結び付けられ，エラーがアーキテクチャ全体に及ぼす影響を表現することを支援する．AADL アーキテクチャモデルにエラーモデルを付加したモデルを AADL ディペンダビリティモデルと呼ぶ．記述対象として操舵動作を担当する中核制御システムである EPS （電動パワーステアリング）を選択した．

次に自動車の一般的な開発体制を考慮してエラーモデルを記述した．具体的には，水平かつ階層的に分業化された開発においてディペンダビリティを含んだ設計と分析が円滑に行えるための条件を考慮した．その条件を満たしたエラーモデルの記述を提案し，AADL ディペンダビリティモデルを設計することで，エラーの伝播および伝播の網羅を視覚的に表現できた．さらに，エラー検知を目的としたエラーモデル記述を追加することによってフェイルセーフ移行後のエラー伝播の食い止めを確認し，ディペンダブル設計の可視化を図れた．また，提案したエラーモデル記述を用いることで，エラーの発生確率と検知する確率を記述することができたが，システム全体のエラー確率が分かりにくいことが明らかになった．

システム全体のディペンダビリティ分析を支援するために，AADL ディペンダビリティモデルに付加されたエラーモデルの合成手法を検討し，合成を行った．エラーモデルの合成とは複数のエラーモデルを表現する１つのエラーモデルを生成することである．AADL アーキテクチャモデルで表現されたデータの流れである論理的接続と，ハードとソフトの組み合わせである構造的接続を考慮した合成方法を検討した．検討した合成方法を用いて，フェイルセーフの設計されてないモデルと，フェイルセーフの設計されたモデルでエラーモデルの合成を試行した．生成されたエラーモデルは確率遷移のみで表され，システム全体のエラー確率を表現できた．また，2 つの合成結果を比べることにより，アーキテクチャレベルでの設計妥当性を確認できることを示した．