

論文審査の結果の要旨および担当者

報告番号	※ 甲 第	号
------	-------	---

氏 名 小林 展英

論 文 題 目 車載システム開発における
ディペンダビリティ保証手法に関する研究

論文審査担当者

主 査	名古屋大学教授	山本 修一郎
委員	名古屋大学教授	高田 広章
委員	名古屋大学准教授	森崎 修司

論文審査の結果の要旨

小林 展英君提出の論文「車載システム開発におけるディペンダビリティ保証手法に関する研究」は、高いディペンダビリティが求められる車載システムのためのアシュアランスケース作成に関する一連の研究をまとめたものであり、全体は7章から構成される。

第1章は序論であり、車載システムのディペンダビリティを保証する上で安全性やセキュリティなどの品質特性が重要になっているが、そのために必要なアシュアランスケースの作成技術には限界があることを指摘して、この問題を解決することが本論文の目的であるとしている。さらに、本論文の概要と構成についても述べている。

第2章では、関連研究について述べている。本研究の背景となる O-DA (Open Dependability through Assuredness), セーフティケース, 対立ゴール解消法, 車載システム参照モデル活用法, 品質特性に基づくアシュアランスケース作成法の関連研究について述べている。

第3章では、HAZOP, FTA, 対策確認表, およびアシュアランスケースを組み合わせた新しい安全分析結果の説明手法を提案している。本手法により、第三者確認で不可欠の情報を可視化した上で安全分析結果を説明できることを明らかにした。また、車載ヘッドライト制御システムへの適用事例に基づき、その有効性を確認している。

第4章では、NFR(Non Functional Requirements) フレームワークのソフトゴールへの重み付け属性の付与により、非機能要求間のトレードオフを定量的に評価する手法を提案している。本手法の評価実験により、実現方式の品質を定量的に判断できることと、車載システムのアーキテクチャ選定に適用できることを明らかにしている。

第5章では、Martin の「7人の侍フレームワーク」に基づく車載ソフトウェア開発知識の可視化手法とそれに基づく標準ソフトウェア資産評価方法を提案している。

第6章では、保証対象となるソフトウェアの構造(S), 期待される品質特性(P), 想定されるリスク(R)と対策(M), およびその対策結果(E)に基づいてアシュアランスケースを生成する SPRME 手法を提案している。また、ソフトウェアレビューを対象とした比較実験により SPRME 手法で作成したアシュアランスケースは、従来のレビュー方法よりも高い欠陥検出能力を持つことを明らかにしている。

第7章は結論であり、本論文の成果をまとめるとともに、今後の課題を論じている。

以上のように、本論文は車載システム開発におけるアシュアランスケース作成の効率化を目的に、①従来の安全分析手法とアシュアランスケースを組み合わせた新しい安全分析結果の説明手法②対立する非機能要求の定量的トレードオフ評価手法③車載ソフトウェア開発知識の可視化ならびに資産評価手法④保証対象、品質特性、リスク、対策、証拠に基づくアシュアランスケース作成手法の研究に取り組み、有効な成果を挙げている。提案技術はいずれも学術的な新規性があるだけでなく、実用性も高く、情報科学の学術上・技術上の寄与が大きい。よって、本論文提出者、小林 展英君は、博士(情報科学)の学位を受けるに十分な資格があるものと判定した。