学位報告 4

報告番号	※甲　　第　　号

主　論　文　の　要　旨

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
氏　　名	小林 展英

論 文 内 容 の 要 旨

従来の自動車業界では，運用後の振る舞いが固定化できることを前提とした自動車単体で実現されるシステムを中心に品質保証に取り組んできた．しかしながら，今後の自動車業界は，様々な機器が有する情報を連携させることで，自動運転をはじめとする高度なシステムの実用化を目指している．この分野におけるシステムの障害は，ユーザの生命に対する危険，およびユーザの個人情報の流出をもたらし，大きな社会問題を招く．また，このようなシステムの多くは，自動車単体で実現されるのではなく，自動車が置かれた状況に合わせて動的に着脱される他車，IoT 機器，社会インフラのような他システム群，実世界の状況に合わせて常に進化する知識群，さらにそれら膨大な情報群を効率的に扱う人工知能，などと連携することで実現される．これらのシステムは運用開始後も進化することに価値があり，従来の自動車業界が品質保証の前提としてきたシステム特性とは大きく異なっている．このように，今後の自動車業界では，品質に対する価値観が互いに異なるシステムが相互に連携して一つのシステムを実現していくこととなり，こうした状況は，前述した問題の解決をさらに難しくしている．

このような状況下で，システムのディペンダビリティを保証する手段として O-DA (Open Dependability through Assuredness)が注目されている．O-DA は，The Open Group で標準化されたオープンシステムに対するディペンダビリティ品質保証フレームワークであり，開発活動は TOGAF (The Open Group Architecture Framework)に基づいている．O-DA の特徴は，TOGAF に基づいて作成した設計成果の品質状況をアシュアランスケースを用いて確認し，その結果を関係者と常に合意形成できている点にある．アシュアランスケースは，議論の前提条件を明らかにし，その前提条件に基づいて議論を構造的に分解して記述できる文書である．システムのディペンダビリティに関する議論にアシュアランスケースを用いることで，異なる価値観を有したステークホルダ間の前提条件を揃え，議論内容を正しく共有することが可能となる．

しかしながら，車載システム開発における従来のアシュアランスケースの研究には，次に示す 5 つの欠陥と，その解決に不可欠な後述する 5 つの課題が存在している．

- 欠陥①：車載システム開発で利用されているセーフティ分析手法とアシュアランスケースを統合する方法が考慮されていないため，課題①の解決が必要である．
- 欠陥②：セキュリティに関するアシュアランスケース作成手法の有効性が車載システム開発において確認されていないため，課題②の解決が必要である．
- 欠陥③：セーフティ要求とセキュリティ要求が背反した場合など要求が対立した際の解決手法が考慮されていないため，課題③の解決が必要である．
- 欠陥④：車載システム開発にゴール指向分析手法を適用する際に有用な参照モデルとの関係が議論されていないため，課題④の解決が必要である．
- 欠陥⑤：セーフティ，セキュリティ以外の要求の保証にも適用できるアシュアランスケースの統一的な作成手法が存在していないため，課題⑤の解決が必要である．

課題①：従来分析手法と統合したセーフティケース作成法の導入

現在, 車載ソフトウェア開発では, HAZOP（Hazard and Operability Studies）, FTA（Fault Tree Analysis）といった分析手法を用いて安全性を分析し，その結果に基づいて車載ソフトウェアの開発を進めている．ISO26262 の本格導入を想定すると，これに加えて開発した車載ソフトウェアの安全性を第三者に納得してもらうためのアシュアランスケースの作成が必要になる．アシュアランスケースの作成には，記述品質の安定化を図るために，D-Case などの図式言語の採用が期待されるが，従来の D-Case 作成法では，HAZOP，FTA の分析結果を証拠として用いる，という分析過程が反映されない単純で間接的なガイドラインしか存在していなかった．このため，開発現場では具体的な安全分析結果に基づいた説明が間接的になるという問題があった．この問題を解決するためには，HAZOP，FTA と D-Case を対応づけるとともに，その手順を提示する必要がある．

課題②：車載分野に対するセキュリティケース生成法の有効性確認

モバイルサービスを保証対象としたセキュリティケースの効果的な生成法は考案されているが，その手法を車載分野のサービスに適用した際の有効性について議論されていない．車載分野のサービスは，AUTOSAR が策定したアーキテクチャに基づいたシステム上で実現されるため，前述した研究成果を適用する際に，そのアーキテクチャをどのように表現するか考案する必要がある．また，考案した表現方法を用いた車載分野の事例に対して，前述の生成法を適用し，その有効性と他分野のシステムへの適用性を議論する必要がある．

しかしながら，本研究では，課題②に対応するセキュリティケース生成法に関して述べていない．この部分については，その他の実施範囲と相互に依存が少なく、分けて考えても問題がない．この部分については今後の課題として扱う．

課題③：品質特性の異なる要求の対立問題解消法の導入

ディペンダビリティは，セーフティ，セキュリティのように品質特性の異なる要求で構成されるため，それらの要求間で対立問題が発生する可能性を含んでいる．この問題を解消するためには，それらに対する達成度を定量的に評価できる手法が必要となる．

課題④：車載ソフトウェア向け参照モデルの活用法の導入
車載ソフトウェア開発において必要とされる知識は，車載ソフトウェアの大規模，複雑化に従って大幅に増加している．このため，一人のエンジニアが独力で開発全体の知識を備えることは非常に困難な状況となっている．こうした状況下において，適切なゴール指向分析を実施するためには，ゴールの分解根拠となる参照モデルを適切に定義し，それに基づいた分析手順を明らかにする必要がある．

課題⑤：品質特性に基づくアシュアランスケース作成手法の導入
O-DA を運用するためには，セーフティ要求，セキュリティ要求と同様に，ディペンダビリティを構成する様々な品質特性の要求に対して，高品質なアシュアランスケースを統一的に作成できる必要がある．

本研究では，O-DA を運用するための要となるアシュアランスケースの作成法に関して，課題②を除く上記 4 つの課題に対する研究を実施し，以下の結論を得た．

課題①に対する結論として，「D-Case を用いた安全分析結果の説明手法の提案」を実施した．本研究では，HAZOP，FTA を用いた安全分析の結果を D-Case を介して論理的に統合する手法を考案した．提案手法では，システムの安全性を主張した最上位のゴールを，HAZOP，FTA を用いたリスク分析結果に基づいて，最小単位になるまで下位のゴールに分割する．さらに，最下位のゴールにはそのゴールの合格基準として FTA を用いて抽出したリスク原因の対策を紐付け，その基準を達成できる証拠を関連付けることで D-Case を完成させる．さらに，エンジニア 10 名を対象として，HAZOP, FTA を個別に用いた従来形式の分析結果と上述した提案手法を用いて作成した D-Case の比較実験を行った．本実験では，それぞれの分析結果に対して同一の質問を行い，正答率に関しては本手法が 90%前後，従来形式が 50%程度であり，回答時間に関しては本手法が約 4 分，従来形式が約 9 分という結果であった．この結果から，本手法を用いて作成した D-Case が従来形式の分析結果より優れることを確認できた．

課題③に対する結論として，「非機能要求の定量評価手法の提案」を実施した．本研究では，NFR フレームワークを拡張して，分解に関する重み付けをソフトゴールの属性として持たせる記法を考案し，子ノードの間のトレードオフ関係を評価できるようにした．これにより，熟練者の有する非機能要求に関する知識の体系化と重み付けによる設計方針の満足度の定量化が可能となった．また，上記内容をテーブル形式で表現し，定量化の計算を容易にするための変換則を考案した. IoT 機器との接続が一般的となる今後の車載システム開発では，従来重視されてきたセーフティ要求に加えて，セキュリティ要求の考慮も不可欠となる．本手法は，相反するセーフティ要求，セキュリティ要求のトレードオフ関係を定量的に評価できる有用な手法になると予想される．

課題④に対する結論として，「7 人の侍フレームワークを用いた標準ソフトウェア資産の評価知識」を実施した．本研究では，ゴール指向分析手法におけるゴールの分解根拠に利用可能な参照モデルとして，7 人の侍フレームワークを用いた車載ソフトウェア開発活動メタモデルを定義した。さらに，このメタモデルを利用して，プロダクトラインを適切に運用する際に重要となる標準ソフトウェア資産のアーキテクチャ評価手法を提案した．アーキ

テクチャ評価に用いる NFR フレームワークの SIG を作成するためには，プロダクトラインで扱う対象に応じて可変要素を想定し，その内容を構造化したソフトゴールとして定義する必要がある．しかしながら，開発経験の浅いエンジニアが開発活動全体を把握することは困難であり，その状況下で可変要素を抽出して構造的にソフトゴールを定義することは難しい．本研究では，熟練者が有する開発活動に関する知識を 7 人の侍フレームワークに基づいて整理した車載ソフトウェア開発活動メタモデルの構造に従い，ソフトゴールを段階的に分解する手法を提案した．さらに提案手法の妥当性を確認するため，特性の異なる下記 2 つのアーキテクチャの評価実験を行った．

・　他社製品，市販開発環境と互換性のない自社独自のアーキテクチャ
・　自動車業界標準である AUTOSAR を部分的に採用したアーキテクチャ

提案手法を用いて評価した結果は，上記 2 つのアーキテクチャの特性と整合しており，車載ソフトウェア開発活動メタモデル，および提案した評価手法の妥当性を確認できた．

課題⑤に対する結論として，「品質特性に基づくアシュアランスケース作成法の提案」を実施した．本研究では，SPRME を用いた分析結果とアシュアランスケースの対応関係を明らかにし，統一的なアシュアランスケースの作成手法とその有効性を確認した．SPRME は，アシュアランスケースの保証対象を 5 つの観点（Subject：保証対象の構造，Property：保証対象に期待される特性，Risk：特性の達成を阻害するリスク，Measure：リスクを解消する対策，Evidence：対策が備わっている証拠）で整理できるメタモデルを提供している．本研究では，このメタモデルとアシュアランスケースの構成要素の対応関係を定義することで，アシュアランスケースを統一的に生成する変換則を明らかにした．また，本手法を用いて作成したアシュアランスケースの有効性を確認するために，ソフトウェアレビューを対象とした従来手法との比較実験を行った．本実験の事例とした従来のレビュー手法は，レビューアの能力に依存して実施しており，網羅性の観点で抜け漏れが発生していた．一方，提案手法では，確認すべき事項と対象の組み合わせがゴールツリー形式で提示されるため，網羅性の観点で従来手法よりも高い欠陥検出能力を有していることが確認できた．さらに，レビュー記録についても，従来のレビュー記録の形式には欠陥に関する指摘は記録できるが，レビューアが問題ないと判断した範囲に関する記録を残すことができない．このため，マネージャが最終的な品質を判断する際に，レビューアの確認した範囲を踏まえて判断することが難しい状況となっていた．一方，提案手法では，確認した範囲がアシュアランスケースとして漏れなく提示されるため，マネージャがレビューアの確認範囲を踏まえて品質を判断することが可能となる．

上述の結果から、SPRME を用いて作成したアシュアランスケースは、セーフティ、セキュリティを保証する際だけでなく、その他の品質特性を保証する際においても有用であることが確認できた。