

報告番号	※甲	第	号
------	----	---	---

主 論 文 の 要 旨

論文題目 アシュアランス・ケースを活用した
 ソフト部品評価方式の研究

氏 名 宇都宮 浩之

論 文 内 容 の 要 旨

自動車業界の今後の動向として、自動運転に代表されるような車輻とネットワーク、および車輻とあらゆるデバイスが繋がり、協調動作することによってより価値の高いサービスを提供していくことになると考えられる。このような状況においては、車輻ソフトウェアもバリエーションが多種多様となり、かつ各々の製品を非常に短いサイクルで提供し続けなくてはならなくなると予想される。

短納期で多種多様な製品群に対応するため、ソフトウェアプロダクトライン(SPL)開発手法を用いた車輻ソフトウェアの開発が進展すると考えられる。車輻ソフトウェアの開発においては長らく派生開発と呼ばれる方法が選択されてきた。しかしながら、派生開発には派生を重ねるうちに、アーキテクチャが元の設計意図と異なる変更をされるなどして予期せぬ不具合が多発してしまう可能性があった。こういった問題点を解決するための手法として、ソフトウェアプロダクトラインが注目されている。ソフトウェアプロダクトラインとは、同じ系列の製品群を効率よく開発するための手法である。製品群の共通部分と変化する部分を予め可変性分析で見通し、適切なアーキテクチャをソフトウェアの開発前に定義するため、製品開発のたびにアーキテクチャが変形していくこともない。従って、予期せぬ不具合を防ぐことができ、短納期で複数の製品群に対応できるようになることが期待される。このようにソフトウェアプロダクトライン開発手法の適用は、生産性向上に対する高い効果が期待されるが、その品質保証方法は各製品に対して全件テストで対応している場合が多くなっており、テスト段階で不具合が発見されて大きな手戻りを発生させ、生産性が低くなるという問題がある。

近年ではデバイスが進化し、あらゆるデバイスが通信機能を持ってネットワークに繋がるIoT(Internet of Things)化が進んでいる。このような世界では、開発対象製品を保証する範囲を明確に定めることができず、各デバイス製品の品質は高いにも関わらず結合した際に予期せぬ不具合が発生する可能性が高い。このようなシス

テムはオープン・システムと呼ばれる。車輛ソフトウェア業界においても、車輛からより価値の高いサービスを提供するため、多種多様なデバイスを結合して協調動作させることが主流になると考えられる。多種多様、かつ複数企業が提供するデバイス製品を結合したオープン・システムに対しては、企業間での安全性の確認に漏れが生じる問題がある。

車輛ソフトウェア開発において、上述した問題に対応していかなければ、企業はエンドユーザが安心して利用できる製品・サービスを継続的に提供できなくなってしまうことが予想される。本研究ではこれらの問題に対応するために必要な、以下の3つの課題を設定した。

課題①：プロダクトライン開発製品の品質確認方法の構築

課題②：複数のデバイスを結合したシステム全体の安全性確認方法の構築

課題③：製品の品質確認や安全性確認を支援する仕組みやツールの構築

また、これらの課題についてアシュアランス・ケースを活用した確認方法や仕組みを開発することで、同時に製品を提供する企業の説明責任の達成も支援することも考慮した。アシュアランス・ケースはテスト結果や検証結果を根拠にシステムの特長(安全性など)を議論し、システムの特長が保証されていることをステークホルダやユーザに説明する、あるいは確信させる(assure)ための文書の総称である。課題を解決するため、アシュアランス・ケースを活用した5つの研究を実施した。

1つ目の研究では、課題①を解決するため、プロダクトライン開発手法の可変性分析で用いられるフィーチャモデルからGSN表記法で表現されるアシュアランス・ケースを作成する方法を開発した。本研究では、フィーチャモデルのノードとノード間の関係をGSNで表現する際の変換ルールを定義して、具体例を用いて変換ルールの正しさと変換の容易さを確認した。研究成果として、プロダクトラインを導入している企業が、アシュアランス・ケースを用いてシステムを高信頼化する際に有効と思われるアシュアランス・ケース作成手法を提案した。

2つ目の研究では、課題①を解決するため、1つ目の研究結果を用いてプロダクトライン開発手法で開発されたソフトウェア製品の品質確認方法を開発した。プロダクトライン開発では、実際のソフトウェア開発に入る前に、製品群の特長を整理するフィーチャモデルが作成される。このフィーチャモデルを用いて実際のソフトウェア製品の品質を見通すことができれば、テスト段階で不具合が検出されて手戻ることが減り、生産性が高まると予想される。本研究では、フィーチャモデルをアシュアランス・ケースに変換し、実際にソフトウェアのコードを記述する前にソフトウェア製品の品質を確認する手法を定義した。研究成果として、本研究で述べた手法を用いることで、各製品間の特長を分析する可変性分析の段階で各製品の品質を見通すことができる可能性があることを示唆した。

3つ目の研究では、課題②を解決するため、自動運転システムを題材に複数デバイスが協調動作するシステムにおける安全性の確認方法を開発した。複数のデバイスを結合する場合、各々の品質保証範囲が不明瞭となる懸念がある。各々の品質保証範囲が不明瞭となると、品質確認されていない部分が発生し、思わぬ事故を引き起

こす要因ともなりえる。本研究では、複数デバイスが協調動作する自動運転システムを題材に、アシュアランス・ケースを活用した安全性の確認方法を定義し、その妥当性を確認した。研究成果として、企業間で共通理解を得るために、互いのシステムの妥当性を前提と証拠を元に客観的に説明できることを確認した。また、企業文化の差異から発生する不具合を防止できる可能性があることを示唆した。

4つ目の研究では、課題③を解決するため、Microsoft Excelを拡張したGSN表記形式のアシュアランス・ケース作成ツールを開発した。アシュアランス・ケースは企業が説明責任を達成するためのツールとしても利用可能である。企業が市場に投入するソフトウェア製品は年々複雑化・大規模化し、要求変更や設計変更が多発する状況にある。このような状況にあっても、説明責任を達成するためには変更に従うようにアシュアランス・ケースも更新しなければならない。しかし、アシュアランス・ケースの記述は時間がかかるため追従が難しいという欠点がある。本研究では、ソフトウェア製品の設計段階で使用されるUMLなどのモデルからアシュアランス・ケースを自動で作成できるツールを開発し、その効果を確認した。研究成果として、あらゆるモデルはノードとその関係で表現できることに着目し、EA, UML, SysMLなどの垣根無くXML等でソフトウェアの設計モデルが記述できれば、短時間で誤りなくアシュアランス・ケースに変換することができ、アシュアランス・ケースを用いて直ちにステークホルダ間で合意形成が可能となることを示唆した。

5つ目の研究では、課題③を解決するため、O-DAテンプレートを適用したソフトウェアのアーキテクチャ検証ツールの導入方法を提案した。O-DA(Open Dependability through Assuredness)とは、The Open Groupが発行したディペンダビリティ保証フレームワークである。O-DAの開発現場への導入を支援する研究成果として、名古屋大学 山本修一郎教授によってO-DAテンプレートが考案されている。このテンプレートはシステムアーキテクチャの評価サービスを事例としたサービス構想書の雛形となっており、ソフトウェア開発企業におけるソフトウェアの品質検証サービスに適用できる可能性がある。本研究では、開発現場にソフトウェアの品質検証サービスを導入する際に、O-DAテンプレートを用いることで効率よくサービスを導入できることを確認した。研究成果として、O-DAテンプレートと提案方法の有効性と再利用性を示すとともに、ソフトウェア検証サービスがO-DAで表現できることを示唆した。

以上の5つの研究成果により、アシュアランス・ケースを有効活用した提案手法が車輻ソフトウェア業界の問題に寄与し、説明責任の達成とステークホルダ間の合意形成に役立つことが確認できた。