様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

平成　３０　年　　６　月　１１　日現在

機関番号：　３２６６５
研究種目：　若手研究(B)
研究期間：　2015～2017
課題番号：　１５Ｋ１５９７１

研究課題名（和文）概念モデルとアシュアランスケースによる国際規格認証ドキュメント生成に関する研究

研究課題名（英文）Generation of International Standard Certification Documents based on Metamodel and Assurance Cases

研究代表者

松野　裕（MATSUNO, Yutaka）

日本大学・理工学部・准教授

研究者番号：７０５３４２２０

交付決定額（研究期間全体）：（直接経費）　　2,100,000円

研究成果の概要（和文）：システムの安全性保証は重要である。システムの安全性を保証するために、国際規格の認証は重要な手段である。自動車の機能安全分野では、ISO26262国際規格が日本においても準拠が前提になっている。そのような状況の中で、システムの複雑化に伴い、国際規格の認証ドキュメントの生成が困難になりつつある。本研究では、我々が企業と共同で国際規格化を行っているDependability Assurance Framework(DAF)をもとに、認証ドキュメントの生成に関する研究を行った。

研究成果の概要（英文）：Dependability assurance of the system is important. In order to ensure the dependability of the system, certification of international standards is an important means. In the functional safety field of automobiles, compliance is also premised on ISO 26262 international standards in Japan. Under such circumstances, along with the complexity of the system, it is becoming difficult to generate certified documents of international standards. In this research, we conducted research on generation of certified documents based on the Dependability Assurance Framework (DAF), which we are collaborating internationally with companies.

研究分野：　情報科学、システム保証、プログラミング言語

キーワード：　アシュアランスケース　システム保証

１．研究開始当初の背景

システムの安全性、セキュリティ、信頼性を統合した概念であるディペンダビリティ(Avizienies etal, 2004) の保証が重要になってきている。主に欧米において進められてきた安全性やセキュリティの国際規 格策定、認証は、製品開発のさらなるグローバル化に伴い日本企業もより強く対応を迫られている。特に 2011 年に策定された自動車の電子部品の機能安全性に関する国際規格 ISO26262 は日本自動車企業に強い影響を持つようになった。しかしながら国際規格の曖昧さ、規格適合手段の不明確さなどの理由のため、国際規格適合に莫大なコストがかかることが大きな問題になっている。さらに、安全性などを統合した複合属性である ディペンダビリティの認証手法は、いまだ基礎研究段階にある。

研究提案者は、トヨタ、富士通、産総研、IPA と共同で、自動車など消費者機械システムのディペンダビリティを保証する枠組みとして、Dependability Assurance Framework for Safety-Sensitive Consumer Devices (DAF)という国際規格を、ソフトウエア国際規格の策定組織である OMG に おいてトヨタ、富士通、産総研、IPA(情報処理推進機構)と共同策定中であった。DAF は、国際規格の曖昧さの解消のため、ディペンダビリティの概念を UML クラス図でモデル化し(Dependability Concept Model(DCM))、 規格適合手段の不明確さの解決のため、認証ドキュメントのひな形として、近年安全性国際規格適合のためのドキュメントとして主流になりつつあるアシュアランスケース (Assurance Case) のパターンである Dependability Assurance Case Pattern (DAC)を定義した。

２．研究の目的

上記、DCM から、DAC を自動的に生成することを研究の目的とした(図 1)。対象国際規格は重要度の高い ISO26262 とする。27 年度は DCM を基に ISO26262 の部分的メタモデルを作成する。DCM と ISO26262 のメタモデルが包含関係などどのような数学的関係になるのか明らかにする。ISO26262 は機能安全規格であるから、DCM の安全性部分を拡張したモデルになると予想される。作成された 概念モデルの妥当性を ISO26262 の専門家と検討する。次に DCM と ISO26262 の部分的概念モデルの関係から、DAC から ISO26262 のためのアシュアランス ケース・パターンを作成するためのアルゴリズムを検討し、ツール設計を行う。28 年度は研究提案者がすでに実装しているアシュアランスケース・エディターをベースに ISO26262 のためのアシュアランスケース・パターンの (半) 自動生成機能を実装する。

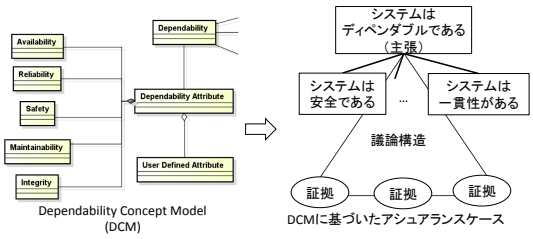

図１ 研究目的:概念モデルからアシュアランスケースの自動生成

３．研究の方法

以下のステップにより行う。

ステップ１

DAF 国際規格を策定した企業の方らと議論し、現状の DCM (Dependability Concept Model) の概念モデルを基に、ISO26262 の一部（システムの既存の部分は、運用実績によって保証を行うという、Proven In Use 概念、ISO26262 のプロセスの一部など）の 概念モデルを作成する。得られた概念モデルと DCM の関係を図 2 のような定義する。

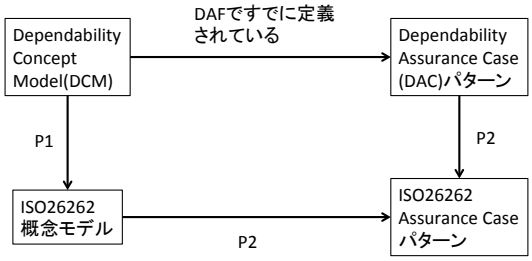

図２　概念モデルと DCM の関係図

ステップ２

ISO26262 のアシュアランスケース・パターン DAF 国際規格の DCM, DAC (Dependability Assurance Case) の対応関係を基に自動生成するアルゴリズムを検討する。

ステップ３

研究提案者が開発したアシュアランスケース・エディター「D-Case Editor」の機能を拡張し、ステップ 2 で設計したアルゴリズムを実装する。ステップ 2 でアルゴリズムが設計できなかった場合、アシュアランスケースから通常の認証ドキュメントフォーマットに変換する機能や、自動化できる部分の実装を行う。

ステップ４

研究協力者などが行っている ISO26262 規格の適合事例を基に、ステップ 1-3 で得られた手法、ツールの実証評価を行う。 得られた知見から、他の国際規格への適用へ向けて、手法の一般化への考察を行う。

４．研究成果

ステップ１においては、DAF 国際規格の策定が遅れ、実際に策定されたのは 2016 年 2

月であった。このため、研究活動の大半は国際規格策定活動に当てられた。国際規格策定において、概念モデルの精緻化、それに基づくアシュアランスケースのテンプレートを改良した。このことから、得られた概念モデルとテンプレートのマッピングを行った。

ステップ２においては、ステップ１で得られた概念モデルとアシュアランスケースのテンプレートをもとにした自動生成の検討を行った。しかしながら基礎検討を行う段階で、OMG DAF 国際規格で規定されている概念モデルが、ネットワークが複雑であり、全自動化を行うことは難しいことが判明した。そこでまず概念モデルの内、主要な構造である、差分開発の概念をもとにしたアシュアランスケースのテンプレートを開発した。そのテンプレートをソフトウエアテストの専門家と議論したところ、そのテンプレートを実際のソフトウエアテストで活用してもらい、その有効性を確認することができた。

ステップ３においては、「D-Case Editor」ではなく、新たに開発したウエブベースツール「D-Case Communicator」において得られた知見をもとにした追加機能の実装を行った。具体的には、登録されたアシュアランスケースのテンプレートを呼び出す機能である。しかしながら、テンプレートを自動的に生成する機能は部分的な実装にとどまった。

ステップ４においては、ステップ３までの、部分的な成果をもとに、企業の方にアシュアランスケーステンプレートを評価して頂いた。そこで評価を受け、実際のソフトウエアテストにおける監査者とテスト実施者の間における合意形成に、１０数件使っていただいている。

研究成果を実際の企業の方に活用していただくために、アシュアランスケースのワークショップを、研究期間中に４回開催した(詳細は www.dcase.jp にある)。　本研究で開発したテンプレートを使ってアシュアランスケースを記述する手法を開発し(学会発表 1,4)、その演習として、差分開発のテンプレートを用いてアシュアランスケースを記述する演習を行った。

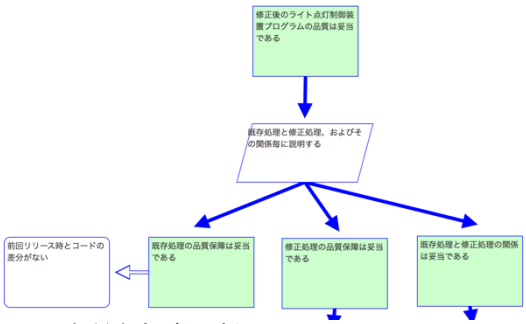

図３ 演習参加者が描いたアシュアランスケース

図３を見ると、DAF で定義された概念モデルに基づいたアシュアランスケースを、テンプレートを用いて、演習参加者が記述できていることがわかる。他の演習者は、このテンプレートを用いて、セキュリティ国際規格を前提としたアシュアランスケースを記述するなど、テンプレートが有効に活用されていることがわかる。

本研究の成果をまとめる。本研究では OMG 国際規格 Dependability Assurance Framework の策定に協力して、ディペンダビリティの概念モデルとアシュアランスケースのテンプレートを開発した。その対応をもとに、概念モデルからアシュアランスケースを自動生成することを目的として研究を行った。結果としては、アシュアランスケースの自動生成は部分的な実装に留まった。また目標とした ISO26262 の概念モデルをもとに ISO26262 適合のためのアシュアランスケースの生成も基礎的な段階にとどまった。しかしながら、Dependability Assurance Framework の基本概念の一つである差分開発をもとにしたアシュアランスケーステンプレートを用いたワークショップにより、ワークショップ参加者がアシュアランスケースを記述することができたことは、本研究の成果と言える。

今後、本研究の成果をもとに、ISO26262 準拠のためのアシュアランスケースのためのテンプレートを、概念モデルから生成することを目指していく。

５．主な発表論文等

〔学会発表〕(計　４　件)

① 大沼祐人、松野裕, D-Case ワークショップの試行及び評価, 信学技報, vol. 117, no. 465, KBSE2017-61, pp. 133-137, 2018 年

② 松野裕、「はじめての D-Case」の紹介, D-Case 研究会、2017, www.dcase.jp

③ 宮崎比呂志、石崎直哉、田口研治、松野裕、春山浩行, “Dependability Assurance Framework for Safety Sensitive Consumer Devices” 標準化, 研究報告ソフトウエア工学、2016-SE-193

④ 石津流弥、松野裕, D-Case ： ステークホルダーを明確化した GSN による合意形成手法, IEICE technical report ： 信学技報 116(284), 1-6, 2016

〔図書〕(計　１　件)

OMG Dependability Assurance Framework, OMG, 2016, https://www.omg.org/spec/DAF/About-DAF/ (国際標準化にあたり協力者として参加)

〔その他〕

ホームページ www.dcase.jp

研究成果、研究会、ワークショップの内容を

公開している。

６．研究組織

(1)研究代表者
松野裕（MATSUNO, Yutaka）
日本大学・理工学部・准教授
研究者番号：70534220
(2)研究協力者
田口 研治（TAGUCH, Kenji）