様　式　Ｃ－１９、Ｆ－１９、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

平成　２８　年　　５　月　２７　日現在

機関番号：　１２１０１
研究種目：　基盤研究(C)（一般）
研究期間：　2013～2015
課題番号：　２５３３００７５

研究課題名（和文）情報制御システムの高機能安全性検証の実用化

研究課題名（英文）Practical model checking for high-performance safety of information control systems

研究代表者
上田　賀一（Ueda, Yoshikazu）

茨城大学・工学部・教授

研究者番号：００２１３３７２

交付決定額（研究期間全体）：（直接経費）　　2,900,000円

研究成果の概要（和文）：　情報制御システムの分野固有の特性に基づき，段階的なモデル検査手法を開発した．従来手法より少ないメモリで検証でき，大規模モデルでは本手法の方が短時間で検証可能である．次に，システム分割によるモデル検査を可能とする分割的モデル検査手法を考案した．分割されたサブシステムの相互関係を失うことなく検証でき，無分割より短時間で検証できる．更に，両手法の欠点を解決するモジュラ検証手法を考案した．モジュラ分割を因果関係の稀薄な物理的分割，構造的対称性による分割，独立性の高い振舞いの分割という異なる3タイプの分割によるモデル検証を可能とする．この手法の効果は属性数比率により判断して利用できる．

研究成果の概要（英文）：This study developed stepwise model checking techniques based on the domain-specific properties of the information control system. This method can verify the model with less memory and shoter period of time in a more large-scale model than the conventional method. Next, this study proposed a divided model checking technique that allows the checking of model by the system division. This method can achieve model checking without losing the interrelationship of the divided sub-systems in a shorter time than non-dividing.
In addition, this study has devised a modular verification approach to solve the drawbacks of the two methods. This approach enable modular model checking by the module division of the 3 types which are physical divisions of the dilute cause-and-effect relationship, divisions in the structural symmetry, divisions of the highly independent behavior. The effect of this approach can be determined by ratio of number of independent attributes and common ones.

研究分野：　ソフトウェア工学

キーワード：　モデル検査　モジュラ検証　ソフトウェア安全性検証　情報制御システム　機能安全

１．研究開始当初の背景

現在の社会では社会インフラ系の情報制御システムが安全かつ安定的に稼働し続けることが望まれ, それらの中枢を担っているコンピュータシステム中の情報制御ソフトウェアの信頼性や安全性を確保することが重要である. そのため, 非常に多くのレビューやテストを行い, 極めて高い開発コストを掛けて品質確保に取り組み, 開発は進められている. しかし, 高品質ソフトウェアの開発を一連の工程の中で系統的に行うには, 実装工程で品質を向上させることが困難であることや, 品質は設計工程での作り込みが重要であることが指摘されている. このことに加え, 機能安全に関する国際規格 IEC61508 では, ソフトウェア設計手法との関わりで形式的手法の適用が推奨されている.

対応策のひとつとして, 実現しようとする情報制御ソフトウェアの品質を設計工程で評価あるいは検証できれば, ソフトウェア開発の効率を上げ, 信頼性や安全性を向上させることができる. しかし状況を鑑みると, 品質評価法や検証法の研究は進められているが, 実用ソフトウェアの規模には適用そのものが難しく, 計算コストがかかりすぎるという問題を抱えている. そのため, 検証すべき着目点に合わせたモデルを作成し, それを検証するという限定的な手段を採っている.

本研究では, 設計の品質評価や仕様検証を可能な限りの実用コストでモデル検査を実現する手法を考える.

２．研究の目的

本研究の目的は, 列車運行システムのような社会インフラ系の大規模情報制御システムのソフトウェア品質を確保するために, モデル駆動開発とモデル検査を同時に取り入れた開発環境を導入することで, ドメイン技術者が記述した設計モデルを形式仕様に自動変換し, コンピュータ上の検証系を用いて, 機能安全性などをモデル検査することである. 従来の研究では, システムの特定側面や部分的範囲に限った検証しか行えず, 実用的な規模のソフトウェアに適用するには状態爆発(管理すべき状態数が過多となる)の問題を解決しなければならない. しかも実装ソフトウェアとの等価保証は人による低レベルなものである. 本研究では, これらの問題を解決するため, 情報制御システム規模のソフトウェアでも実用的な計算コストで状態爆発問題を回避してモデル検査できる手法を築き上げる.

３．研究の方法

本研究では, 研究の区切りとして「情報制御ドメインの形式仕様の段階的･分割的モデル化」「形式仕様変換とモデル検査支援のツール化」「設計モデルの機能安全性の評価・可視化」の３段階を計画し, それぞれの理論的展開および支援ツール試作を実施する. 支援ツール試作では大学院生の協力を得る. また, (株)日立製作所・インフラシステム社の協力を得て, 実用レベルの情報制御システムへの適用による評価提供の協力を得る.

これまでにも関連研究の文献調査を進めてきたが, さらに調査範囲を広げて研究調査や文献調査を進め, 知識の収集を図る. 本研究の基盤となる情報制御システムの設計モデルを仕様記述するモデリング言語は既に開発し, その言語自体の実用的検証も行った. 図１に情報制御システムの対象世界とモデル駆動開発の言語の構成要素と記法の関係を示す. このモデリング言語を, 本研究の基盤とし, 3 段階の計画に取り組む. 以下に段階毎の手順を示す.

(1)「情報制御ドメインの形式仕様の段階的・分割的モデル化」について手順を示す. まず, モデリング言語を用い, 情報制御システムのドメイン特化された特性（制御処理プロセスとシステム状態空間）に基づき, 段階的・分割的なモデル化を図る. このモデル化の手法開発が本研究の核となる. それゆえ, 段階的手法や分割的手法の有用性を評価するためにソフトウェア実験を繰り返す. その後, 情報制御ドメインに適した知識の体系化の検討を行い, 設計モデルの仕様に取り入れる. 機能安全の検証項目を仮設定し, 変換アルゴリズムを開発し, 検証系を用いたモデル検査ツールを試作する. 試作ツールでは, 安全性を検証するとともに, 使用実験を繰り返し行い, 段階的手法と分割的手法の有用性評価を収集する. 現実的なレベルにある情報制御システム, 特に社会インフラ系システムを対象とし, これには, 企業の情報提供などの協力を得て研究を進める. 特定の社会基盤システムのソフトウェア設計を対象に, 設計仕様記述言語のメタモデル化と形式仕様への変換およびモデル検査に要する時間コストの削減に関する検討を進める. この結果を踏まえて, 設計モデル仕様そのものの形式仕様への変換について検討を進め, SPIN などのモデル検証系に適用する方法の開発を進める.

(2)「形式仕様変換とモデル検査支援のツール化」について手順を示す. 機能安全性評価のための検証項目を検討するため

に，できるだけ多くの検証項目を対象としたモデル検査を行う．その上で，設計モデルと検証項目の見直しを行い，設計モデルから形式仕様への変換と検証支援を実用レベルに引き上げる検討に取り組む．また，この見直しを試作ツールにも反映する．企業協力を得て，情報制御ドメイン内のいくつかのシステムの設計モデルに適用を広げ，想定ドメイン内の仕様変換とモデル検査を支援できる範囲の検討を進める．

(3)「設計モデルの機能安全性の評価・可視化」では以下の事項に取り組む．分割モデル検証アプローチを情報制御ドメイン内のいくつかのシステムの設計モデルに適用し，想定ドメイン内の仕様変換とモデル検査を支援できる範囲の検討を進める．加えて，実用化検討を踏まえた検証項目に対する機能安全性のモデル検査を行い，実用レベルで検査結果を導出し，ドメイン技術者に可視化する支援ツールを試作・検討する．

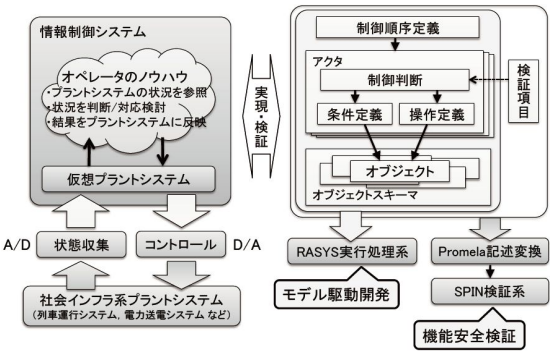

図１．情報制御システムの対象世界とモデル駆動開発言語の構成要素と記法の関係

４．研究成果

(1)「情報制御ドメインの形式仕様の段階的・分割的モデル化」において，以下の研究観点の成果を導いた．

① 情報制御システムのドメイン特化された特性に基づき，段階的なモデル検査手法を開発し，有効性を評価した．その結果，従来手法より少ないメモリで検証可能であり，従来手法では検証可能範囲を広げた．また，モデル規模が大きくなると，本手法の方が短時間で検証可能となることを導いた．次に，システム分割によるモデル検査を可能とする分割的モデル検査手法を考案し，有効性を評価した．その結果，サブシステム分割して検証を行っても相互関係を失うことなく検証を進められ，無分割より短時間で検証できることを示した．

② 現実の情報制御システムの規模に対する段階的および分割的モデル検査手法の有用性に関する検討を行い，現状の限界や問題点を探った．その結果，段階的モデル検査では，属性抽出の難しさが課題となることが分かった．また，分割的モデル検査では，サブシステム分割時に，制御判断を大域ルールと局所ルールに分けるための一般的な手法が必要となることを導いた．

③ 情報制御システム向け設計モデリング言語のメタモデル化を図り，検証系 Alloy による正当性検証を行い，言語としての問題がないことを確認した．加えて，第３段階の予備研究として，モデル検査時に生じる反例（正常の終了状態に至らない事例）を容易に取り扱うための視覚化のあり方と原因箇所を推定するために必要な情報の検討を行った．この予備研究では，いくつかの限界点や問題点が認められたが，一般的な状況設定のもとでの検討であるため，段階的・分割的モデル化を考慮すれば，その特徴を効果的に解決できる見通しを得ることができた．

(2)「形式仕様変換とモデル検査支援のツール化」において，以下の研究観点の成果を導いた．

① 情報制御システムのドメイン特化された特性に基づき開発した段階的モデル検査手法は，従来手法より検証可能範囲を広げることができた．また，システム分割によるモデル検査を可能とする分割的モデル検査手法を考案した．その結果，モデル規模が大きいと本手法の方が短時間で検証可能となることを導き，サブシステム分割で検証しても相互関係を失うことなく検証を進められ，無分割より短時間で検証できることを示した．

② 現実の情報制御システムの規模に対する段階的および分割的モデル検査手法の有用性を検討し，限界や問題点を探った．その結果，段階的モデル検査では，属性抽出の難しさが課題となり，分割的モデル検査では，サブシステム分割時に制御判断を大域ルールと局所ルールに分けるための一般的な手法が必要となることを導いた．これらの問題に対し，解決策としてモジュラ検証アプローチを考案した．これは，モジュラ分割を因果関係の稀薄な物理的分割，構造的対称性による分割，独立性の高い振舞いの分割という異なる３タイプの分割によるモジュラ検証を可能とする．このアプロー

チの効果は属性数比率により判断できるため，必要性を考慮して利用できるという利点がある．

③ 第3段階の予備研究として，モデル検査時に生じる反例から原因箇所を推定するために必要な情報抽出手法の検討を行った．この研究では，いくつかの問題点が認められたが，一般的な状況設定のもとでの検討であるため，段階的・分割的モデル化やモジュラ検証を考慮すれば，その特徴を効果的に利用できる見通しを得ることができた．

(3)「設計モデルの機能安全性の評価・可視化」において，検証項目に対する機能安全性のモデル検査手法の実用化を踏まえた検討を行い，問題点となる反例とその原因の抽出や可視化について検討した．

① ドメイン特化された特性に基づき開発した段階的モデル検査手法，および本研究で考案した分割的モデル検査手法により情報制御システムの分割によるモデル検査を行い，サブシステム分割で検証しても相互関係を失うことなく検証を進められ，無分割より短時間で検証できることを確認した．しかし，現実の情報制御システムの規模や複雑さに対する段階的および分割的モデル検査手法を探った結果，モデル検証を一般化する際の問題点を見出した．

② 段階的モデル検査では属性抽出が難しいこと，分割的モデル検査ではサブシステム分割時に制御判断を大域ルールと局所ルールに分けるための汎用手法が必要となる問題に対する解決策のひとつとして，モジュラ検証アプローチを考案し，因果関係の稀薄な物理的分割，構造的対称性による分割，独立性の高い振舞いの分割という異なる3タイプの分割によるモジュラ検証を可能とした．このアプローチを支援するモデル検証ツール群を試作した．その効果は属性数比率により判断できるため，必要性を考慮して利用できる．

③ モデル検査時に生じる複数の反例から原因箇所を推定するために，適用ルールの順序や組合せの問題を発見する手法を探り，推定アルゴリズムを検討した．段階的・分割的モデル化やモジュラ検証を考慮した上で，原因推定を支援するソフトウェアの試作を行った．

5．主な発表論文等

〔学会発表〕（計 11 件）

① 小飼敬, 宮島卓巳, 上田賀一, 山形知行, 武澤隆之,『段階的検査法にモジュラ化手法を用いたモデル検査の実用化』, 日本ソフトウェア科学会 第22回ソフトウェア工学の基礎ワークショップ, 2015.11.26-28, ほほえみの宿滝の湯（山形県天童市）

② 大森祐貴, 小飼敬, 上田賀一, 山形知行, 武澤隆之,『段階的検査法を用いたモデル検査の反例分析手法』, 日本ソフトウェア科学会 第32回大会, 2015.9.8-11, 早稲田大学西早稲田キャンパス（東京都新宿区）

③ 宮島卓巳, 小飼敬, 上田賀一, 山形知行, 武澤隆之,『モジュラ化手法によるモデル検査の検討とモジュラ検証の実用化』, 電子情報通信学会 知能ソフトウェア工学研究会技術報告, 2015.3.5-6, 電気通信大学（東京都調布市）

④ 小飼敬, 宮島卓巳, 上田賀一,『情報制御システムに対するモジュラ検証と課題』, 情報処理学会 ソフトウェア工学研究会ウィンターワークショップ 2015, 2015.1.22-23, カルチャーリゾートファストーネ（沖縄県宜野湾市）

⑤ 宮島卓巳, 小飼敬, 上田賀一, 山形知行, 武澤隆之,『情報制御システムにおける段階的検査法を用いたモジュラ検証』, 日本ソフトウェア科学会 第 31 回大会, 2014.9.7-10, 名古屋大学東山キャンパス（愛知県名古屋市）

⑥ 大森祐貴, 小山恭平, 小飼敬, 上田賀一,『情報制御システムのモデル検査における反例分析支援ツールの開発』, 情報処理学会 ソフトウェア工学研究会研究報告, 2014.3.19-20, 化学会館（東京都千代田区）

⑦ Kei Kogai, Yoshikazu Ueda,『Realistic Validation of Specification for Modeling Language using Alloy』, Asia-Pacific Conference on Computer Aided System Engineering 2014, 2014.2.10-12, Bali（Indonesia）

⑧ 小山恭平, 小飼敬, 上田賀一,『情報制御システムのモデル検査における状態爆発対策と課題』, 情報処理学会 ソフトウェア工学研究会ウィンターワークショップ 2014, 2014.1.23-24, 大洗ホテル（茨城県茨城郡大洗町）

⑨ 小飼敬, 宮島卓巳, 小山恭平, 上田賀一,『情報制御システムのモデル検査に対する分割アプローチと課題』, 情報処理学会 ソフトウェア工学研究会ウィンターワークショップ 2014, 2014.1.23-24,

大洗ホテル（茨城県茨城郡大洗町）

⑩ 宮島卓巳, 小山恭平, 小飼敬, 上田賀一, 山形知行, 武澤隆之,『情報制御システムにおける部分モデルと相互関係を用いたモデル検査の実用化』, 日本ソフトウェア科学会 第20回ソフトウェア工学の基礎ワークショップ, 2013.11.28-30, ゆのくに天祥（石川県加賀市）

⑪ 小山恭平, 小飼敬, 上田賀一, 山形知行, 武澤隆之,『SPIN を用いた情報制御システムに対する段階的モデル検査手法』, 日本ソフトウェア科学会 第 30 回大会, 2013.9.10-13, 東京大学本郷キャンパス（東京都文京区）

６．研究組織

(1)研究代表者

上田　賀一（UEDA Yoshikazu）

茨城大学・工学部・教授

研究者番号：00213372

(2)研究分担者

無し

(3)連携研究者

無し

(4)研究協力者

武澤　隆之（TAKEZAWA Takayuki）

(株)日立製作所・インフラシステム社

山形　知行（YAMAGATA Tomoyuki）

(株)日立製作所・インフラシステム社