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

令和　３ 年　 ６ 月 １０ 日現在

機関番号：６２６１５
研究種目：基盤研究(B)（一般）
研究期間：2017～2020
課題番号：１７Ｈ０１７２７

研究課題名（和文）保証付き多段階システムモデルの柔軟・継続的な洗練・進化

研究課題名（英文）Continuous and Flexible Sophistication and Evolution of Assured Multi-Level System Models

研究代表者

石川　冬樹（Ishikawa, Fuyuki）

国立情報学研究所・アーキテクチャ科学研究系・准教授

研究者番号：５０４５５１９３

交付決定額（研究期間全体）：（直接経費）　　11,000,000円

研究成果の概要（和文）：実世界・社会に踏み込むソフトウェアシステムにおいては，その仕様と想定環境のかみ合わせにより要求が満たされることの検証が重要かつ困難な課題である．これに対し多段階の抽象度からなるモデルを用い，複雑さを軽減しつつシステムモデルの記述と検証を行うアプローチが注目されている．しかし整合性検証に適した多段階モデルを設計し，また検証済みの整合性を壊さず継続的に変更していくことは難しい．これに対し本研究では，断片的な記述を逐次的に与えて多段階モデルを洗練させていく手法に取り組んだ．また自律制御システムにおける先端的な題材に対し提案手法を適用しその有効性を確認した．

研究成果の学術的意義や社会的意義
多数の構成要素を含むソフトウェアシステム全体について安全性を一括で論じることは困難です．このため，単純な場合からはじめて，システムをとらえる抽象度（解像度）を少しずつ上げながら，安全性を論じていく方法があります．しかし，「単純な場合ではよかったが，この要素が入ると安全性保証がやり直しになる」ことが起きてしまいます．本研究では，「既存の安全性保証を壊さずに追加要素を加える」という技術を軸に，段階的に安全性の保証を論じる方法論を確立しました．これにより，ますます複雑になるソフトウェアシステムに対し，強力な安全性保証をより容易に行うことができるようになりました．

研究成果の概要（英文）：A key challenge in software systems that work in the real word and society is to verify that requirements are satisfied by the combination of system specification and expected environments. There is an emerging approach to use multi-step models with different levels of abstraction to mitigate complexity of specification and verification. However, it is difficult to design multi-step models for consistency verification and also to continuously update without breaking the consistency. In this research work, we tackled to provide a methodology to gradually refine multi-step models by gradually constructing and combining partial specification models. We evaluated the effectiveness of the proposed methodology with scenarios of advanced autonomous systems.

研究分野：ソフトウェア工学

キーワード：ソフトウェア開発効率化・安定化　形式手法　システムモデリング　段階的詳細化　Cyber-Physical Systems

様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９（共通）

１．研究開始当初の背景

Cyber-Physical Systems（CPS）など，ソフトウェアによるスマートな（迅速で適切な）制御を実世界・社会で活用するパラダイムが注目されている．その根幹となるソフトウェアは，外部環境，すなわち制御下にない様々なものごと（物理的実体や社会的概念）を踏まえ適切な振る舞いをとる必要がある．このためには，ソフトウェアの振る舞いを定める仕様と，外部環境に関する知識・仮定との双方をシステムモデルとして明確に記述し，それらのかみ合わせにより要求が満たされることを検証することが重要，かつ困難な課題である．

近年注目されている形式手法 Event-B では，このシステムモデル全体を対象とし，段階的にシステムをとらえ詳細化していくことで記述と検証の複雑さを軽減するアプローチを採っている（図 1）．Event-B においてはまず，システムの特定側面に注目して抽象的なモデルを構築し，その整合性を検証する．整合性とは，すなわち，安全性や信頼性などの要求に対して違反する可能性があるような振る舞いが与えられていないということである．その後別の側面に注目してより詳細化されたモデルを構築し，その整合性，および以前のモデルとの整合性を検証する．この詳細化を反復することで，検証済みの複雑なシステムモデルを得ることができる．この詳細化は，仕様をプログラムに「言い換えていく」ための古典的な詳細化とは異なり，新たな概念・観点を「導入していく」自由度の高いものである．Event-B については，実世界の連続値を扱うための拡張など，盛んな研究が継続的に行われている．

一方，Event-B における自由度の高い詳細化には，適切な設計が必要となる．しかし多段階のモデルを整合性の要件を踏まえ設計することは容易ではない．特に，初期に記述する抽象モデルは，後の具体モデルに現れる様々な状況の記述と整合するよう，十分に一般的でなければならない．すなわち後の具体モデルのことを，最初からある程度意識し見据える必要がある．つまり，開発者にとってとらえやすい「段階的」な進め方が自由にできるわけではない．具体モデルにおいて適当な記述を行ってしまうと，抽象モデルにおける定義や検証済みの性質との不整合が生じてしまう．特に後者については，コストがかかる検証が一からやり直しになるとともに，アプリケーションにとって重要な性質を維持する適切な変更を追求する難しさとコストがある．

ここで，従来のプログラムや，プログラムにつながる設計モデルにおいては，特定の側面（関心事とも呼ぶ）の分離のための取り組みが多数なされてきた．例えば，アスペクト指向においては，オブジェクト指向では複数のモジュールに重複して横断的に現れてしまうような側面を分離してまとめて記述し，後から統合することができる．これにより，セキュリティなど特定の側面を考えないモデルに対して，セキュリティに関するデータや振る舞いを後から差し込んだり変更したりすることができるようになっている．また，アジャイル開発におけるビヘイビア駆動開発では，具体的・限定的な状況に関する断片記述を一つずつ検討し，段階的にプログラムを拡張しつつ都度テストする．この際には，ステークホルダーにとっての重要性や実装の困難性などを踏まえ，段階的に進める手順をある程度柔軟に定めていく．

このように，複数の側面を含む複雑なシステムに対して，各側面を別途扱い，断片的な記述の追加を段階的に行うことは，ソフトウェア工学の原則として非常に重要となる．このため，Event-B などの形式モデルにおいても，断片的な記述の追加，そして検証を通し，対象とする側面に応じた変更・拡張を段階的に行えることが望ましい．

２．研究の目的

上記の背景を踏まえ本研究においては，整合性検証がなされた Event-B 多段階モデルに対し，整合性を壊すことなく，変更・拡張を行うための方法論に取り組む．具体的な手法として，以下のような手法に取り組む．

【手法１】　整合性検証がなされた Event-B 多段階モデルに対し，整合性を壊すことなく，各段階で導入される側面の導入順序を変更する技術を確立する．機能や振る舞いの変化は伴わず，証明を伴う形式モデルのリファクタリングを行うものであると言える．

【手法２】　整合性検証がなされた Event-B 多段階モデルに対し，機能や振る舞いの変更内容が仮にでも定まった際に，整合性が壊れるのか，壊れるとしたらどの部分なのか（証明対象となる性質のいずれなのか）を判断できるようにする．すなわち，整合性証明の観点からの変更影響分析に取り組む．

【手法３】　応用に特化した深い支援として，CPS において典型的な関心事であるセンシングの不確実性について，安全性など主たる性質の証明と切り離して扱い，柔軟に追加・変更ができるようにする．すなわち，センシングの不確実性が導入されても，整合性を保つようにモデルを自動変更したり，あるいは必要な妥協を導出したりする手法に取り組む．

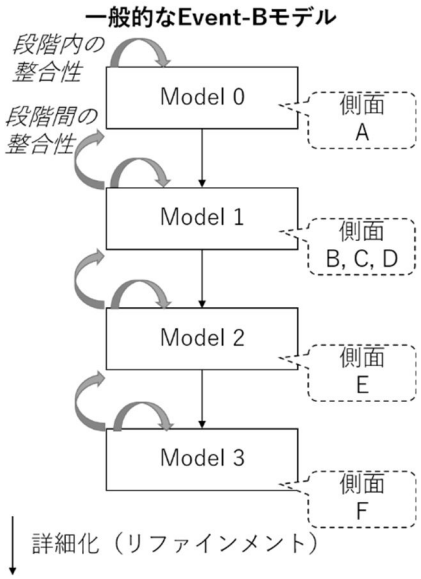

図 1 Event-B モデルにおける整合性の検証

なお，本研究の取り組みにおいては，現状において実用的なツールが整っている Event-B を対象とする．しかし，理論上の本質としては，振る舞いがガード条件（あるいは事前条件）とアクションとして部品化されており，ホーア論理に基づき各機能の実行前後に成立する条件を検討する一般的な形式モデルであれば，本研究のアプローチは適用可能である．

３．研究の方法

本研究で取り組む手法のうち，手法１は非常に一般性が高いものであり，理論的な基盤を要するものである．これについては，研究代表者らの以前の成果[1]を発展させて取り組む．この成果においては，整合性検証がなされた Event-B 多段階モデルに対し，整合性を壊すことなく，各段階で導入される側面の分割操作およびマージ操作に取り組んだ．分割とマージを組み合わせれば，任意の導入順序変更が可能になる．ここで問題になるのは，分割の際に，既存の証明に用いられていた変数と仮定が切り分けられるために，単純な分割では証明が維持できなくなることである．これについては，クレイグの補間と呼ばれる論理式を用いることにより，分割後において扱う側面（Event-B モデル上では変数）が減った場合にも，変数に関する仮定を最大限維持することで解決できる．しかし以前の成果は，自動化および一般性において限られており，手法１についてはこれらの観点から取り組む．

手法２および手法３においては，変更のパターンを整理し，それぞれにおける変更の影響，特に既存の整合性証明の維持可否についての検討を行うことになる．手法２については，変更の種類に対して網羅的な検討を行う．一方で手法３については，センシングの不確実性の導入という典型的な変更について検討することになる．これらの検討を通し，整合性証明の維持可否を事前に把握し，必要な場合は整合性維持に必要な変更の提示についてもパターン化することで，整合性証明を活かしつつ，モデルを反復的，探索的に変更していくことを容易とする．

４．研究成果

手法１における多段階モデルの再構成に関する考え方を図 2 に示す．この例では，図の左から右への変更として，詳細化の再構成を行っている．この例では，多数の側面を含み複雑になってしまった Model 1 を分割し，側面 B，C，D を個別の段階に分散させている（その上で側面 B は側面 A と同じ段階に含めている）．また Model 2-3 における側面 E，F の導入順序を逆にし，側面 E を除いた部分の再利用や，E に関する変更を容易としている．このような柔軟な再構成を，段階の分割とマージを単位操作として実現している．

このような再構成において問題となるのが，検証済みである整合性の維持である．ここではその要点を単純化して示す．例えば $a < 15$ を示すことが整合性要件であり，その仮定となる制約として $a > 0$ ，$b > 0$，$a + b < 10$ が含まれる段階を考える．これらの仮定からは $a < 9$ が導けるため，整合性要件も示すことができる．ここで，変数 a で表される側面だけを切り出し新たな段階を作る（段階の分割をする）ため，変数 a だけで表される情報だけを構文的に切り出すとする．この場合，整合性要件 $a < 15$ と，仮定 $a > 0$ を含む新たな段階が得られる．しかしこの仮定だけでは要件を証明できず整合性が失われている．そこで元の段階で整合性検証に効

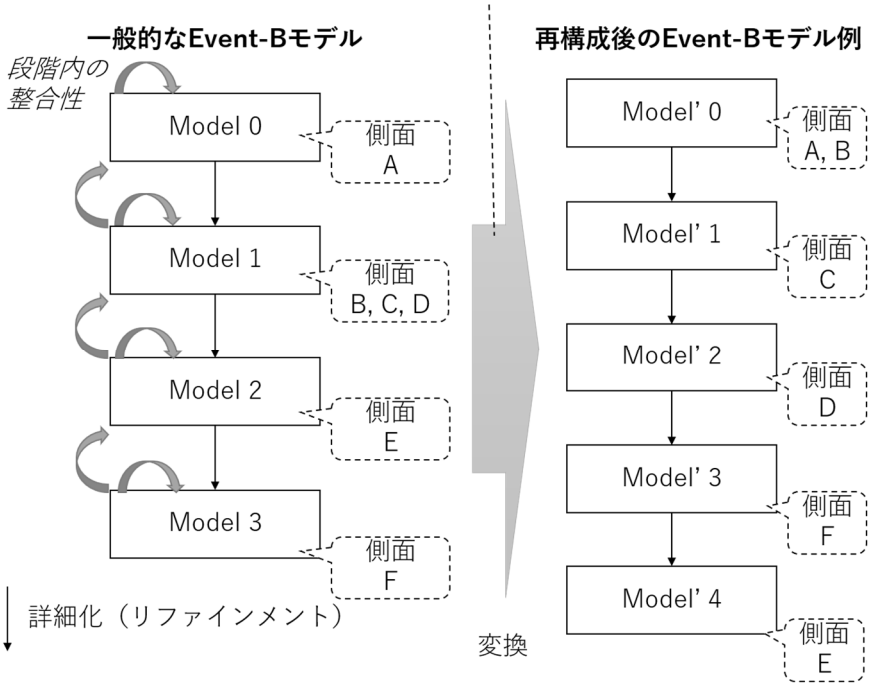

図 2 証明を維持したモデルの再構成

いており，変数 a のみを含む補題 $a < 9$ （または必要最弱な $a < 15$ ）も，新たな段階の仮定として含めればよい．このような整合性検証の復元について，元のモデルのける証明ログの探索と再利用，クレイグ補間と呼ばれる式の導出・利用などの手段により，自動的に行うようにした[2]．

さらにこの自動化により，異なるリファインメント戦略，すなわち多段階モデルの異なる設計について，多くのサンプルを生成して比較することが可能になった．これにより，記述および証明の分割度合いに応じた自動証明率の比較などを行える．リファインメント戦略に関するこのような実験は斬新であり，形式手法分野の国際会議において最優秀賞を受賞した[3]．

手法２については，変更のパターンを整理し，それぞれにおける変更の影響，特に既存の整合性証明の維持可否についての検討を行った．変更の種類に対して網羅的な検討を行うことで，整合性証明の維持可否という観点から，変更影響分析手法を確立した[4]．

手法３については， CPS において典型的な関心事であるセンシングの不確実性について，導入した際の整合性証明の維持可否や，不可能である場合の必要な妥協を導出する手法を示した．[5]．これにより，安全性など主たる性質の証明を行った上で，適用環境やセンサー性能の可能性（あるいは不確実性）を踏まえた Event-B モデルの分析，検証を増分的に行うことができるようになった（図 3）．

以上の取り組みにより，整合性証明を伴うがゆえにリファインメントによる段階的な構築・検証が難しいシステムモデルに対し，柔軟な変更を増分的に行ったり反復したりすることが容易となった．

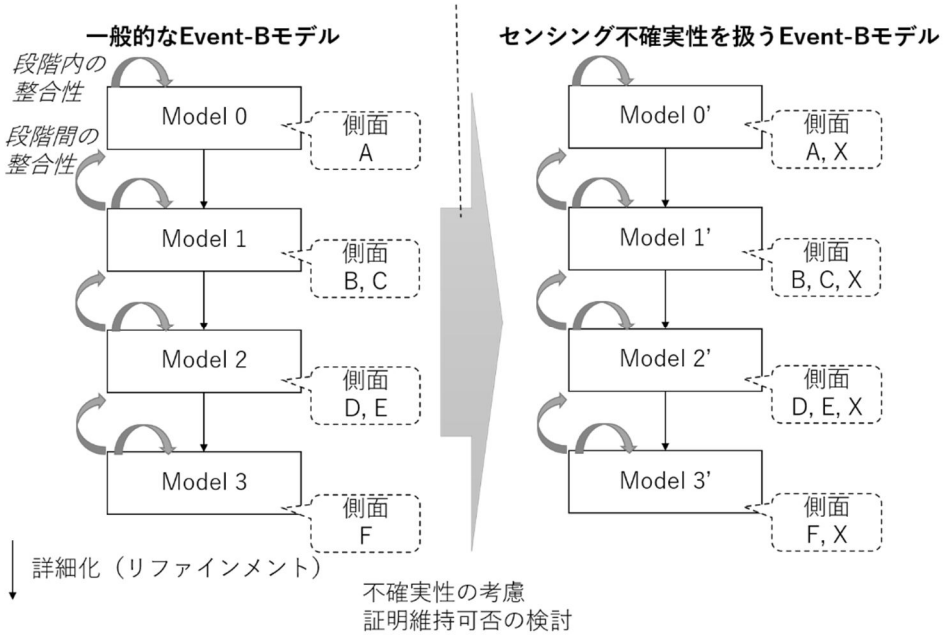

図 3 センシング不確実性の柔軟な導入

[1] Tsutomu Kobayashi, Fuyuki Ishikawa, Shinichi Honiden, Refactoring Refinement Structures of Event-B Machines, The 21st International Symposium on Formal Methods (FM 2016), pp.444-459, November 2016
[2] Tsutomu Kobayashi, Fuyuki Ishikawa, Shinichi Honiden, Consistency-Preserving Refactoring of Refinement Structures in Event-B Models, Formal Aspects of Computing, Vol. 31 No.3, pp.287-320, February 2019
[3] [Best Paper Award] Tsutomu Kobayashi, Fuyuki Ishikawa, Analysis on Strategies of Superposition Refinement of Event-B Specifications, The 20th International Conference on Formal Engineering Methods (ICFEM 2018), November 2018
[4] Shinnosuke Saruwatari, Fuyuki Ishikawa, Tsutomu Kobayashi, Shinichi Honiden, Change Impact Analysis for Refinement-based Formal Specification, IEICE Transactions on Information and Systems, Special Issue on Formal Approach, Vol. E102-D No. 8, pp.1462-1477, August 2019
[5] Tsutomu Kobayashi, Rick Salay, Ichiro Hasuo, Krzysztof Czarnecki, Fuyuki Ishikawa, Shin-ya Katsumata, Robustifying CPS Controller Specifications Against Perceptual Uncertainty, The 13th NASA Formal Methods Symposium (NFM 2021), May 2021

５．主な発表論文等

〔雑誌論文〕　計2件（うち査読付論文　2件／うち国際共著　0件／うちオープンアクセス　0件）

１．著者名 Tsutomu Kobayashi, Fuyuki Ishikawa, Shinichi Honiden	４．巻 31
２．論文標題 Consistency-Preserving Refactoring of Refinement Structures in Event-B Models	５．発行年 2019年
３．雑誌名 Formal Aspects of Compupting	６．最初と最後の頁 287-320
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/s00165-019-00478-z	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

１．著者名 SARUWATARI Shinnosuke、ISHIKAWA Fuyuki、KOBAYASHI Tsutomu、HONIDEN Shinichi	４．巻 E102.D
２．論文標題 Change Impact Analysis for Refinement-Based Formal Specification	５．発行年 2019年
３．雑誌名 IEICE Transactions on Information and Systems	６．最初と最後の頁 1462-1477
掲載論文のDOI（デジタルオブジェクト識別子） 10.1587/transinf.2018FOP0006	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

〔学会発表〕　計8件（うち招待講演　1件／うち国際学会　8件）

１．発表者名 Tsutomu Kobayashi, Rick Salay, Ichiro Hasuo, Krzysztof Czarnecki, Fuyuki Ishikawa, Shin-ya Katsumata
２．発表標題 Robustifying CPS Controller Specifications Against Perceptual Uncertainty
３．学会等名 The 13th NASA Formal Methods Symposium (NFM 2021)（国際学会）
４．発表年 2021年

１．発表者名 Guillaume Dupont, Yamine Ait Ameur, Neeraj Singh, Fuyuki Ishikawa, Tsutomu Kobayashi, Marc Pantel
２．発表標題 Embedding Approximation in Event-B: Safe Hybrid System Design using Proof and Refinement
３．学会等名 The 22nd International Conference on Formal Engineering Methods (ICFEM 2020)（国際学会）
４．発表年 2020年

１．発表者名
Paulius Stankaitis, Alexei Iliasov, Tsutomu Kobayashi, Yamine Ait-Ameur, Alexander Romanovsky, Fuyuki Ishikawa

２．発表標題
Formal Distributed Protocol Development for Reservation of Railway Sections

３．学会等名
The 7th International Conference on Rigorous State Based Methods (ABZ 2020)（国際学会）

４．発表年
2020年

１．発表者名
Tsutomu Kobayashi, Fuyuki Ishikawa

２．発表標題
Analysis on Strategies of Superposition Refinement of Event-B Specifications

３．学会等名
The 20th International Conference on Formal Engineering Methods (ICFEM 2018)（国際学会）

４．発表年
2018年

１．発表者名
Daichi Morita, Fuyuki Ishikawa and Shinichi Honiden

２．発表標題
Construction of Abstract State Graphs for Understanding Event-B Models

３．学会等名
Symposium on Dependable Software Engineering (SETTA 2017)（国際学会）

４．発表年
2017年

１．発表者名
Shinnosuke Saruwatari, Fuyuki Ishikawa, Tsutomu Kobayashi, Shinichi Honiden

２．発表標題
Extracting Traceability between Predicates in Event-B Refinement

３．学会等名
The 24th Asia-Pacific Software Engineering Conference (APSEC 2017)（国際学会）

４．発表年
2017年

１．発表者名 Tsutomu Kobayashi
２．発表標題 Refactoring Refinement Structure of Formal Specification in Event-B
３．学会等名 The 6th Asian Workshop of Advanced Software Engineering (AWASE2017)（国際学会）
４．発表年 2017年

１．発表者名 Fuyuki Ishikawa
２．発表標題 Emerging Challenges in Software Dependability under Uncertain World
３．学会等名 The 1st International Conference on Advanced Information Technologies (ICAIT)（招待講演）（国際学会）
４．発表年 2017年

〔図書〕　計0件

〔産業財産権〕

〔その他〕

―

６．研究組織

	氏名 （ローマ字氏名） （研究者番号）	所属研究機関・部局・職 （機関番号）	備考
研究分担者	本位田　真一 (Honiden Shinichi) (70332153)	早稲田大学・理工学術院・教授（任期付） (32689)	

７．科研費を使用して開催した国際研究集会

〔国際研究集会〕　計0件

８．本研究に関連して実施した国際共同研究の実施状況

共同研究相手国	相手方研究機関