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　５ 年　 ６ 月 １２ 日現在

機関番号：８２６４５
研究種目：若手研究
研究期間：2019～2022
課題番号：１９Ｋ２０２４９

研究課題名（和文）ソフトウェアの整合性証明情報を演繹的に用いた環境変化への妥協付き適応

研究課題名（英文）Software adaptation with reasonable compromise using information on deductive proof of consistency

研究代表者

小林　努（Kobayashi, Tsutomu）

国立研究開発法人宇宙航空研究開発機構・研究開発部門・研究開発員

研究者番号：１０８０３４０５

交付決定額（研究期間全体）：（直接経費）　　3,200,000円

研究成果の概要（和文）：物理的な対象を制御するソフトウェアに対し、制御器とその環境の形式的なモデルを構築し検証を行う手法は安全性の保証に有効である。中でも、同じ対象に対し複数の抽象度のモデルを構築するアプローチが複雑さ軽減に効果的である。しかし、環境モデルを現実に合わせるために更新し、制御器モデルもそれに合わせて更新する（適応する）必要がある。我々は、多段階の抽象度を持つ制御器の形式モデルの適応に関する研究を行い、センサの不確かさに自動で対処する手法や、自動運転車が安全に目標を達成することを保証するソフトウェアアーキテクチャの構築・検証手法、宇宙機が故障から復帰する手続きの検証のためのモデル作成手法などを提案した。

研究成果の学術的意義や社会的意義
本研究はコンピュータだけでなく人間にも理解・説明可能である形式的モデルの安全な変更・適応という工学的に発展中の工程に対し、多段階の抽象度の視点から切り込み成果を挙げた点で学術的に意義深いと考える。また、実世界で動作するソフトウェアシステムを（一部の研究ではAIを用いたブラックボックスシステムを）対象とし、その安全性を保証しつつ現実の開発問題に対処する手法を提供している点で社会的にも意義深いと考える。

研究成果の概要（英文）：Mathematically proving the safety of software that controls things in the real world by using formally specified models of the controller and its environment provides a strong safety guarantee. In particular, specifying formal models in multiple abstraction levels (stepwise refinement) for reducing the complexity of modelling and verification has been attracting increased interest. In practice, however, there are gaps between the constructed environment model and the real environment. Therefore, after updating the environment model, developers should make adaptations to controller models so that the controller safely interacts with the real environment. We constructed methods for the adaptation to formal models in multiple abstraction levels, such as automatic robustification of the controller against perceptual uncertainty, safety architecture for autonomous vehicle software, and ensuring the safe recovery from faults of spacecraft.

研究分野：ソフトウェア工学

キーワード：形式手法　段階的詳細化　定理証明　自己適応ソフトウェア　Internet of Things　物理情報システム　AI安全性

様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９（共通）

１．研究開始当初の背景

IoT などに代表される、ソフトウェアシステムを用いて実世界や社会の事物を適切に制御するアプリケーションの重要性が高まっている。このようなシステムでは、ソフトウェア（制御器）の動作に加え、周囲の環境の動作や性質も考慮することが必須になる上、実世界に影響を及ぼすシステムであるため安全性やセキュリティの重要性が非常に高い。また、環境を含めた多数の構成要素・側面を考慮する必要があり、複雑性が高い。従って、コードレベル・アルゴリズムレベルの詳細な動作以前に、仕様レベルで、「動作の結果何が実現されるか」を体系的に分析することが重要である。

そのために、環境と制御器についての知識や仮定、仕様を（人間にも計算機にも厳密に理解できる）形式的な言語でモデル化し、それらの動作の結果、要求が満たされることを数学的証明などで検証する手法（形式仕様記述手法）が有効である。中でも、システムの各種側面を段階的にモデルに導入し多段階の抽象度のモデルを構築する（段階的詳細化）ことで、システムの厳密な構築・検証の複雑さを軽減するアプローチが注目されている。代表的なものに、シャルル・ド・ゴール空港の自動運転シャトルの構築などに使われた手法の後継である手法 Event-B がある。

このような手法を用いた開発では強力な保証が可能だが、実際には、現実を適切に反映した環境モデルをはじめから構築することは非常に困難である。そのような場合、環境モデルを現実に合わせて更新することになるが、元の環境モデルの下で制御器モデルが満たしていた（安全性などの）性質が満たされなくなる場合がある。そのため、環境モデルの変更に伴い制御器モデルも適切に変更（適応）し、性質を保証する必要がある。

２．研究の目的

本研究では、制御器の多段階形式モデルの適応手法の構築を目的としている。それにあたり、特に次の３つの問題に取り組むことを目的としていた。

問題１：体系的に適切な適応を行うには？　環境モデルが E から E'に変化した時、ある要求 r を満たすように、また E'と整合性を持つように制御器 C を変更し C'にすることは単純な問題ではない。また、実際に整合性や要求 r を満たすことの証明を与える必要がある。これらを体系的に行うことは容易ではない。

問題２:適応時に賢く妥協するには？　さらに、要求は複数存在し、互いに関係し合っている。適応を試みても、E'によっては、全ての要求を同時に満たすような C'がそもそも存在しないような場合がある。この場合は適切に「妥協」して、要求のうちの一部のみを満たすような C'を構築することが望ましい。

問題３：必要な側面にのみ絞った適応を行うには？　環境と制御器のモデルには、多くの側面が含まれることになる。一方、多くの場合、一度に起こる環境の変化は、対象となる環境のうち一部の側面にのみ関係するものである。複雑に絡み合うモデルとその証明に対し、制御器の変更を最低限に抑えた適応が望ましい。

これらの問題に取り組み、厳密でありながら人間にも理解できる制御器と環境モデルに対して、多段階の抽象度を考慮して適切な適応を行うことを目的とした。

３．研究の方法

多段階の抽象度の形式モデルをそれらの間の整合性を確かめつつ構築し、定理の証明という形で安全性などの性質の検証を行うための手法 Event-B [1]で構築された環境と制御器のモデルを主な対象とした。対象とするモデルとして、物理情報システムを意識し、自動運転領域などのシステムのモデルを扱った。提案手法は適応の方法論およびモデルの分析・変更アルゴリズムであり、必要に応じて Event-B のモデリング環境 Rodin platform (http://www.event-b.org/platform.html) のプラグインとして提案手法を実装した。

他にも、微分方程式を Event-B に組み込んだ拡張に対する整合性検証の理論の構築、また、人間による理解のためよりも自動検証を指向したモデル検査ツール NuSMV [2]で用いられるモデルで、対象システムの異常を検知してから回復するまでの動作のモデルの構築手法も提案した。

[1] J. R. Abrial, "Modeling in Event-B: System and Software Engineering," Cambridge University Press, 2010.
[2] Cimatti, A., Clarke, E., Giunchiglia, F. et al. NUSMV: a new symbolic model checker. STTT 2, 410-425 (2000).

４．研究成果

（１） センサ不確かさに対する自動適応

想定と異なる環境の振る舞いは、外部環境の情報の取得を担うセンサが想定と異なる値を検知することにつながる。本研究では、センサが想定通りの値を検知した場合にのみ安全に動作する制御器のモデルを入力として、センサが想定と異なる値を検知した場合も安全性を保つように制御器を自動で適応する手法（適応パターン、適応の変更限界の算出手法、自動適応手法）を構築した。この手法では「妥協版」もあわせて提案しており、ここでは元の制御器の振る舞いを完全に保つことを諦めることで、通常版では対応できない環境の逸脱がある程度あっても適応後の制御器が安全性を保つことを可能にしている。

本手法を用いることにより、開発者は想定通りの環境動作に対する制御器さえ構築すればよく、環境の逸脱は本手法が引き受けて安全性を保証できる。通常、制御器ソフトウェアを設計する際には念のために安全マージンを設計することが多いが、そのマージンは適切な根拠・保証のついたものでないことが多く、過信するとかえって危険である。一方、本手法を用いることで適応の限界も含めた分析も行うことができ、安全な制御器の設計の体系化・低コスト化に寄与する手法と言える。

[a] Kobayashi, T., Salay, R., Hasuo, I., Czarnecki, K., Ishikawa, F., Katsumata, Sy. (2021). Robustifying Controller Specifications of Cyber-Physical Systems Against Perceptual Uncertainty. In: Dutle, A., Moscato, M.M., Titolo, L., Muñoz, C.A., Perez, I. (eds) NASA Formal Methods. NFM 2021. Lecture Notes in Computer Science, vol 12673. Springer, Cham.

（２） 自動運転車の安全性の数学的保証ルール構築

自動運転車の安全性を保証するためのルールとして RSS (Responsibility-Sensitive Safety) が提案されていたが、これは「１車線で前の車に追突せずに追う」ような非常に単純な交通状況にのみ対応するものだった。

[b]では、「自動運転車が高速道路上で緊急避難のために他の車との接触を避けながら車線変更を繰り返し、最終的に路肩の特定位置で止まる」といったような、安全性を保ちながら特定の目標を達成することが求められている状況で、ある動作がその要求を満たすことを数学的に保証する手法として、RSS を拡張した手法「Goal-Aware RSS」を、形式的推論のための論理や形式的シナリオ記述のワークフローと共に提案している。

研究代表者はこの中で、自動運転車の振る舞いとその安全性、達成目標としてどのようなものが適切かという問いのもとで、具体例の構築・解析を通じて、制御器に組み込まれる適応ルールの開発に携わった。

[b] I. Hasuo et al., "Goal-Aware RSS for Complex Scenarios via Program Logic," in IEEE Transactions on Intelligent Vehicles, vol. 8, no. 4, pp. 3040-3072, April 2023.

（３） 自動運転車が安全に複雑な目標を達成するための適応アーキテクチャ構築

[c]では、上記[b]の成果である GA-RSS ルールを利用し、自動運転車を対象として、既存の安全アーキテクチャ(Simplex architecture)を用いた制御器のモデルの構築・検証手法を提案した。GA-RSS ルールの利用により、達成目標と振舞いを定めたときに、どのような場合に適応が必要かが明らかになり、また特定の前提のもとで安全性と目標達成が両立できることが数学的に保証されているため、この前提を環境の状態と比較することで安全性が保証された適切な適応が可能になる。この際、多段階の抽象度でモデルを構築することで、見通しが良く、他のドメインにも適用可能なアーキテクチャとなっている上、「誤差に適応する」「異なる達成目標に適応する」といった異なる適応を、必要最低限の変更操作で行えるようなものとなっている。また、安全アーキテクチャを用いることにより、高い性能を得るためのブラックボックス制御器(機械学習を用いたものなど)を持つ制御器に対しても安全性と目標達成を確実にする適応が可能になっている。このように、現実的な問題に対する制御器の安全・適切な適応に寄与することができた。

[c] Kobayashi, T., Bondu, M., Ishikawa, F. (2023). Formal Modelling of Safety Architecture for Responsibility-Aware Autonomous Vehicle via Event-B Refinement. In: Chechik, M., Katoen, JP., Leucker, M. (eds) Formal Methods. FM 2023. Lecture Notes in Computer Science, vol 14000. Springer, Cham.

（４） 宇宙機の異常に関する自動適応機構の検証手法構築

[d]では、JAXA において、宇宙機で発生し得る異常に対する検知・隔離・適応(Fault detection, isolation, and recovery)のための一連の手続きに対し、前提が満たされるならばどのような場合でも適切な適応がなされるか否かを自動で検証するためのモデル構築手法を提案した。このような問題の検証には自動のモデル検査器 NuSMV などの利用が考えられるが、場合の数が膨大となり、現実的な時間で検証が終了しないという問題があった。この問題に対し、[d]では対象モデルを多段階の抽象度で構築し、検証する性質に合わせてモデルの抽象化を行うことで、必要最低限の要素数のモデルに対する検証を行うことを可能にし、結果として検証にかかる時間の短縮を可能にしている。

研究代表者はこの中で、手法の体系化・定式化を行った。

[d] Horikawa et al., Detecting Faulty Sequences of FDIR Functions on Spacecrafts Using Model Checking, IEEE Aerospace Conference 2023

（５） 微分方程式で記述された物理情報システムモデルの複数抽象度間の整合性検証の近似

物理情報システムにおける検証においては、物理的要素に関する検証を厳密に行う際に微分方程式を用いてモデルの記述を行う必要がある場合がある。このようなモデルを段階的詳細化を用いて記述・検証することは複雑さの軽減に有用だが、抽象版のモデルと具体版のモデルの整合性を厳密に解析的に検証することは困難であるという問題があった。これに対し[e]では、近似的整合性のための検証ルールを定義し、十分な精度の整合性を現実的に検証することを可能にした。

研究代表者はこの中で、近似的整合性の構築に貢献した。

[e] Dupont, G., Aït-Ameur, Y., Singh, N.K., Ishikawa, F., Kobayashi, T., Pantel, M. (2020). Embedding Approximation in Event-B: Safe Hybrid System Design Using Proof and Refinement. In: Lin, SW., Hou, Z., Mahony, B. (eds) Formal Methods and Software Engineering. ICFEM 2020. Lecture Notes in Computer Science, vol 12531. Springer, Cham.

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　2件／うちオープンアクセス　0件）

１．著者名 Stankaitis Paulius、Iliasov Alexei、Kobayashi Tsutomu、Ait-Ameur Yamine、Ishikawa Fuyuki、Romanovsky Alexander	４．巻 33
２．論文標題 A refinement-based development of a distributed signalling system	５．発行年 2021年
３．雑誌名 Formal Aspects of Computing	６．最初と最後の頁 1009～1036
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/s00165-021-00567-y	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 該当する

１．著者名 Hasuo Ichiro、Eberhart Clovis、Haydon James、Dubut Jeremy、Bohrer Rose、Kobayashi Tsutomu、Pruekprasert Sasinee、Zhang Xiao-Yi、Pallas Erik Andre、Yamada Akihisa、Suenaga Kohei、Ishikawa Fuyuki、Kamijo Kenji、Shinya Yoshiyuki、Suetomi Takamasa	４．巻 8
２．論文標題 Goal-Aware RSS for Complex Scenarios via Program Logic	５．発行年 2023年
３．雑誌名 IEEE Transactions on Intelligent Vehicles	６．最初と最後の頁 3040～3072
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/tiv.2022.3169762	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 該当する

〔学会発表〕　計5件（うち招待講演　0件／うち国際学会　5件）

１．発表者名 Stankaitis Paulius、Iliasov Alexei、Kobayashi Tsutomu、Ait-Ameur Yamine、Ishikawa Fuyuki、Romanovsky Alexander
２．発表標題 Formal Distributed Protocol Development for Reservation of Railway Sections
３．学会等名 ABZ 2020（国際学会）
４．発表年 2020年

１．発表者名 Dupont Guillaume、Ait-Ameur Yamine、Singh Neeraj K.、Ishikawa Fuyuki、Kobayashi Tsutomu、Pantel Marc
２．発表標題 Embedding Approximation in Event-B: Safe Hybrid System Design Using Proof and Refinement
３．学会等名 ICFEM 2020（国際学会）
４．発表年 2020年

１．発表者名
Tsutomu Kobayashi, Rick Salay, Ichiro Hasuo, Krzysztof Czarnecki, Fuyuki Ishikawa, Shin-ya Katsumata

２．発表標題
Robustifying Controller Specifications of Cyber-Physical Systems Against Perceptual Uncertainty

３．学会等名
NFM 2021（国際学会）

４．発表年
2021年

１．発表者名
Tsutomu Kobayashi, Martin Bondu, Fuyuki Ishikawa

２．発表標題
Formal Modelling of Safety Architecture for Responsibility-Aware Autonomous Vehicle via Event-B Refinement

３．学会等名
FM 2023（国際学会）

４．発表年
2023年

１．発表者名
Masatoshi Horikawa, Tsutomu Kobayashi, Shoma Takatsuki, Hiroki Umeda, Yasushi Ueda

２．発表標題
Detecting Faulty Sequences of FDIR Functions on Spacecrafts Using Model Checking

３．学会等名
2023 IEEE Aerospace Conference（国際学会）

４．発表年
2023年

〔図書〕　計0件

〔出願〕　計1件

産業財産権の名称	発明者	権利者
情報処理装置、制御設計支援方法およびプログラム	小林努、リックサレイ、蓮尾一郎、クリストフツァーネッ	同左
産業財産権の種類、番号	出願年	国内・外国の別
特許、特願2021-087649	2021年	国内

〔取得〕　計0件

〔その他〕

http://research.nii.ac.jp/robustifier/

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

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			
英国	ニューカッスル大学			
フランス	ENSEEIHT			
カナダ	ウォータールー大学			
フランス	ソルボンヌ大学			