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　６ 年　 ６ 月 １３ 日現在

機関番号：１２１０１
研究種目：基盤研究(C)（一般）
研究期間：2018～2023
課題番号：１８Ｋ１１２３４

研究課題名（和文）組込みシステムのモデルベース設計のためのハイブリッドモデル検査手法の確立

研究課題名（英文）A Hybrid Model Checking Method for Model-Based Design of Embedded Systems

研究代表者
上田　賀一（Ueda, Yoshikazu）

茨城大学・理工学研究科（工学野）・教授

研究者番号：００２１３３７２

交付決定額（研究期間全体）：（直接経費）　　3,300,000円

研究成果の概要（和文）：組込みシステムのモデルベース設計のため，SysMLのブロック定義図，内部ブロック図，ブロックの内部構造，パラメトリック図により，対象システムの制御ソフトの要求や制約をモデル記述で表現した．このモデルをSimulinkとSMTソルバ上に記述展開したうえでハイブリッドモデル検査するにあたり，SMT-LIB2.6を用い，スクリプトのカスタマイズで，Simulinkと任意のSMTソルバを連動させたハイブリッド検証を可能とした．考案した制御ソフトの解空間獲得手法の処理手順を実装し，解空間を２次元マップにて可視化し，対話的に把握できることを事例ベースで確認した．

研究成果の学術的意義や社会的意義
組込みシステムの機能安全性を担保する手法として，制御モデルをシミュレーションで評価する方法が取られている．加えて，モデル検査を適用した検証を実現することで安全性を網羅的に担保できる．しかし，モデル検査手法は，モデル記述そのものが難しく，検証結果の把握や解釈も難しい．本研究では，SMTソルバで制御可能領域の解空間を探索する処理手順を実現し，開発現場で利用される実用的なモデルベース開発環境MATLAB/Simulink上で，従来の制御対象のプラントモデルのシミュレーションによる解析に，解空間の探索結果を反映し，影響を可視化し，把握や解釈を容易にすることを可能とした．

研究成果の概要（英文）：Using SysML, the requirements and constraints of the control software of the target system are expressed in a model description. The model is deployed on Simulink and SMT solvers, and SMT-LIB 2.6 is used to enable hybrid verification by linking Simulink and an arbitrary SMT solver. We implemented the procedure of the solution space acquisition method for control software, and confirmed its usefulness on a case study basis.
As a method to guarantee functional safety of embedded systems, in addition to evaluating control models by simulation, safety can be comprehensively guaranteed by realizing verification by applying model checking. However, model checking methods are also difficult to describe models and to interpret verification results. Our method reflects the results of model verification by constraints in the simulation-based evaluation of plant models used at development sites, making it possible to visualize the effects and facilitating understanding and interpretation.

研究分野：ソフトウェア工学

キーワード：モデルベース開発　協調解析　モデル検査　ハイブリッド検証　SMTソルバ　SysML

１．研究開始当初の背景

自動車を始めとする駆動型組込みシステムでは，制御ソフトウェアの開発に多大な労力とコストをかけているという実状がある．従来の制御ソフトウェアの設計プロセスは，実装プロセスを含み，試作実装を繰り返しながら設計するという労力のかかる手順を踏んでいる（図１参照）．今後，産業界はますますの労力およびコストの削減を目指し，モデルベース開発の導入を進める方向にあり，制御設計プロセスと実装プロセスを分離することが必要不可欠である（図２参照）．モデルベース開発において制御設計を行うには，要求・制約の獲得と制御対象モデルの開発が必要である．そして，検証作業をシミュレーションにより行うには，リアルとバーチャルの両面での評価を取り入れ，入出力関係の最適化に向けた実装の再定義作業を繰り返す制御設計が必要である（図３参照）とされている．

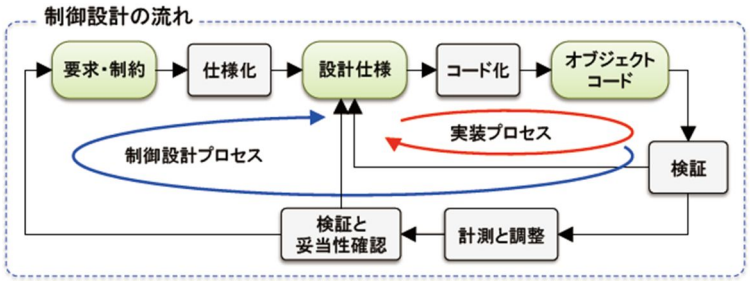

図1．実装プロセスを含む制御設計プロセス

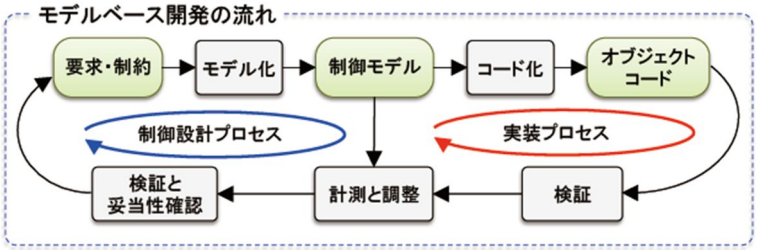

図2．モデル・ベース開発

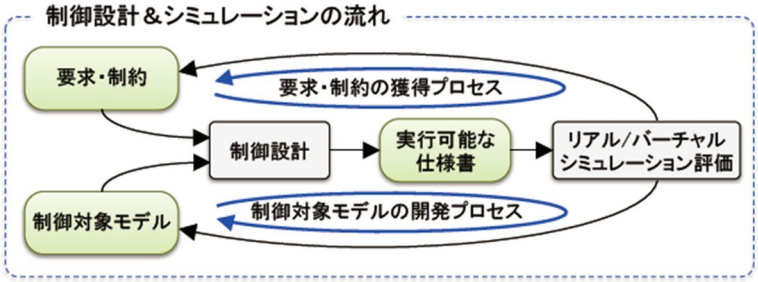

図3．要求・制約獲得プロセスと制御対象モデル開発プロセス

駆動型組込みシステムの産業界においては，実現に苦慮している問題として，①制御対象のモデリング，②制御システム設計，③モデル検証，④モデルベース開発の統合開発環境が挙げられている．特に，モデルベース開発の定義と方向性が開発コミュニティで共有されておらず，制御対象モデルの構築に時間がかかることから，開発基盤は脆弱であり，プラントモデル化や制御設計，検証の領域で必要な技術が確立されていない[1]．自動車産業界では今なお，これらの問題が本質的に解決できていないという話をよく聞く．また，駆動型組込みシステムには高い機能安全性が求められ，産業機械分野におけるソフトウェアや制御システムの機能安全規格 ISO 13849，産業機械の電気/電子/プログラマブル電子の制御システムの機能安全規格 IEC 62061，自動車分野の機能安全規格 ISO 26262 などの規格が定められている．ソフトウェアの機能安全規格としては IEC 61508-3 がある．Safety Integrity Level(SIL)-3,4 では形式手法が必要とされ，テスト検査から脱却したモデル検証が求められている．機能安全性を高めるためには，シミュレーションだけではなく，モデル検査を取り入れることは必須である．しかし一方で，モデル検査だけでは実用性が低いものとなってしまう．両者の利点を取り入れるためにはハイブリッドモデル検査の実現が学術的にも産業的にも有用である．

２．研究の目的

本研究では，機能安全性を担保する手法により前述の問題①～④を解決することを目的とする．そのため，制御対象をプラントモデルと制御モデルに分けて扱う．プラントモデルはハードウェアとして，制御モデルはソフトウェアとして実現される．この制御モデルをシミュレーションで評価するだけでなく，モデル検査を適用し，網羅性を伴った検証を実現する．モデルベース開発において本研究が扱う部分を図４に示す．　組込みシステムは，アナログ駆動しているハードウェアプラント部分とデジタル駆動しているソフトウェア制御部分からなるハイブリッドシステムである．これまでのモデル検証では，ハイブリッドシステムを一体として線形ハイブリッドオートマトンで捉え，モデル検証するものであった[2]～[6]．しかし組込みシステムを線形ハイブリッドオートマトンとして捉えること自体が開発者には難しい．本研究のハイブリッドモデル検査手法では，制御モデルはモデル検査により網羅性をもって安定可能解を探索するための制約の形式記述を必要とするものの，制御対象のプラントモデルはシミュレーションによる

評価結果を得ることができるため，制御対象の振舞いを把握しやすい．本研究が目指すモデル検査は，実用面において開発者が利用できるものでなければならないと考えている．この点では，産業界で広く利用されている MATLAB/Simulink をベースに組み入れることも大切である．

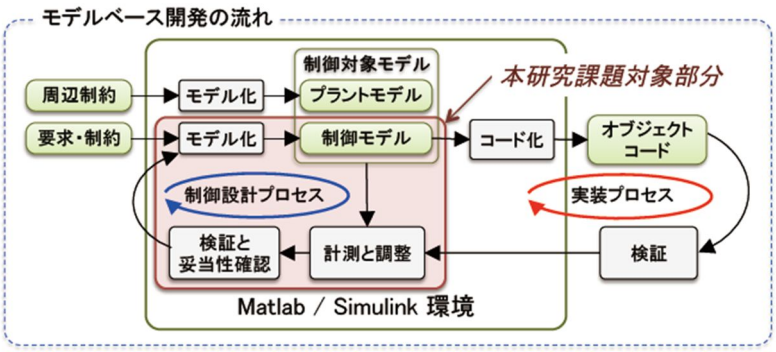

図4．プラントモデルと制御モデルを分けたモデルベース開発

3．研究の方法

ハイブリッドモデル検査を取り入れたモデルベース開発の利用イメージを図５に示す．前述の問題①の制御対象のモデリングについては，制御モデルはソフトウェア実現部分で評価を反映することが可能である．プラントモデルへの反映は難しいが，物理シミュレーションを適用できる．問題②の制御システム設計，および③のモデル検証は，ハイブリッドモデル検査に取り入れ，評価を反映した設計アプローチを提供できる．問題④のモデルベース開発の統合開発環境について，製品レベルは難しいが，試作は可能であると考えている．

（1）まず始めに，ハイブリッドモデル検査のためのモデル表現方法を解決する．具体的には，制御ソフトの要求や制約を SysML[7]で表現する方法を規定，検査可能記述に変換し SMT (Satisfiable Modulo Theories，背景理論付き充足可能問題)ソルバで解法する手順を開発する．

（2）次に，SMT ソルバにより，制御ソフトの安定可能な解空間を得るための効率よい手法を検討し，考案する．

（3）さらに，制御ソフトの解空間獲得手法と MATLAB/Simulink を連動させ，ハイブリッドモデル検査手法を確立し，モデルベース開発の統合開発環境の試作に取り組む．

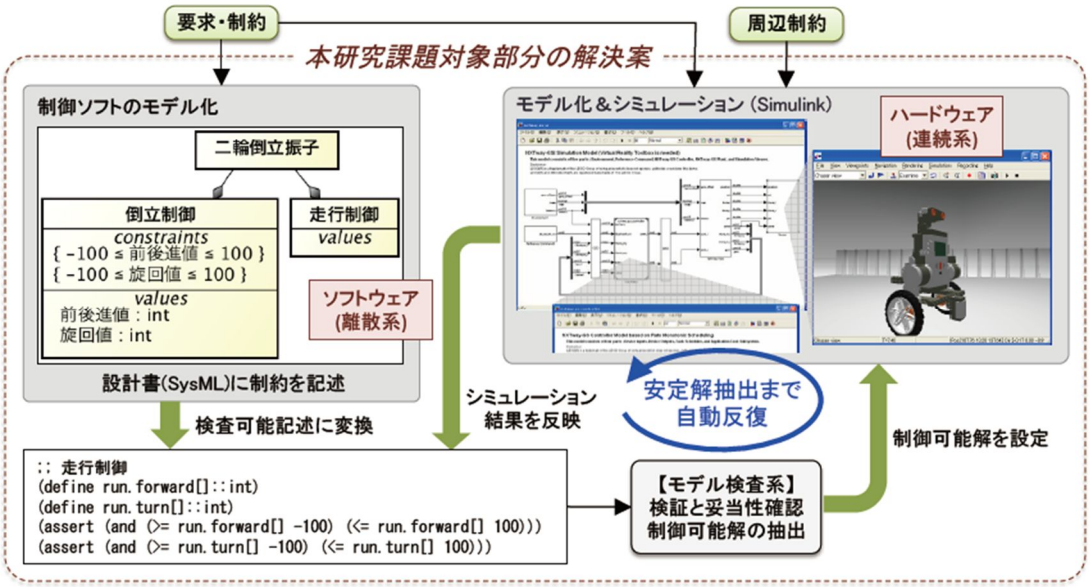

図5．ハイブリッドモデル検査を取り入れたモデルベース開発

4．研究成果

前述の研究方法に則り実施した研究成果を以下に述べる．

（1）制御ソフトの要求や制約のモデル記述は，SysML を用い，ブロック定義図でシステムの階層性とシステムや構成要素の分類を表現し，内部ブロック図で，サブシステムのパーツ・ポート・コネクタの相互接続の観点からブロックの内部構造を表現した.SMT ソルバで解決すべき制約は，パラメトリック図を用い，システムに現れる様々な値の間の制約として表現した．これらにより対象システムを SysML でモデル記述した(図６)．

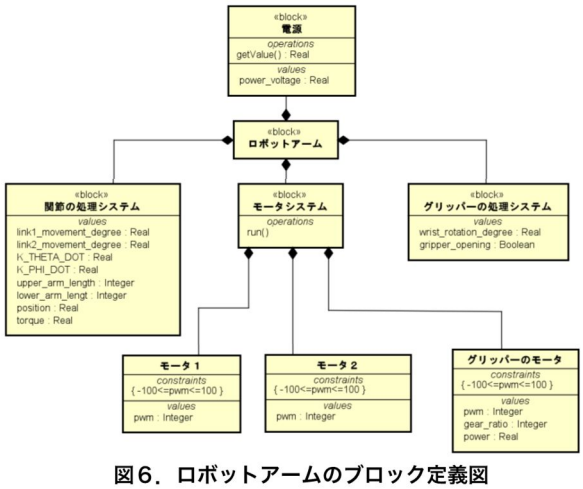

図６．ロボットアームのブロック定義図

（2）制御ソフトの安定可能な解空間を得るための効率よい手法の検討にあたり，様々な SMT ソルバを比較した．比較・検討した SMT ソルバは，Yices[8]，Z3[9]，Alt-Ergo[10]，AproVE[11]，argoSMT[12]，Boolector[13]，CVC4[14]，MathSAT5[15]，Minkeyrink[16]，OpenSMT2[17]，Q3B[18]，SMTInterpol[19]，SMT-RAT[20]，STP[21]，veriT[22]である．本研究の従前の取り組みでは，Yices を用いており，非線形性と量子化が扱えることから Z3 へ展開した．対象システムの制約検査にあたり，多様な検査を可能とし，個別の SMT ソルバへの依存を避けるため，標準言語である SMT-LIB2.6[23]を用いることで SMT ソルバの切り替えが可能となるように実装を進めた．Simulink と SMT-LIB2.6 を介して，SMT ソルバとデータ交換を行う機能ブロックを Simulink 上に S-Function で実装し，SMT ソルバでの検証のための処理を記述したスクリプトを用意した(図７)．このスクリプトのカスタマイズで，MATLAB/Simulink と任意の SMT ソルバを連動させたハイブリッド検証が可能となった．

```
;;タッチセンサ
(declare-const touch.value Bool)
;;モータ1
(declare-fun moter1.pwm () Int)
(define-fun moter1. theta () Int 0)
;;モータ2
(declare-fun moter2.pwm () Int)
(define-fun moter2.theta () Int 0)
;;制約ブロックからの抽出
;;アームの回転角度
(declare-fun w.theta () Real)
(declare-const w.theta (Array Int Int))
(declare-fun w.psi () Real)
(assert(= w.theta (+ (/ (+ (* DEG2RAG (select w.theta 0)))
  (* DEG2RAG (select w.theta 1))) 2) w.psi)))
```

図7．SMT-LIB2.6記述

（3）制御ソフトの解空間獲得手法として次の処理手順を取り，MATLAB/Simulink と連携させ，Simulink 上で解空間を注目する２変数の２次元マップにて可視化し，対話的に把握できることを事例ベースで実装し確認した．

① Simulink から受け取ったデータから SMT-LIB のスクリプト記述を更新する
② スクリプトを実行し，検証性質の充足可能性判定を行う
(②a)充足しない場合，不具合とみなし解析を終了する
(②b)充足する場合，充足解を複数抽出する
③ SMT ソルバから抽出した複数の充足解をログに記録する．
④ 充足解の解空間を可視化（画像出力，GUI 更新）する．
⑤ 解空間の過去の推移を確認し，充足解を選択する．

以上の処理を繰り返すことで解空間の推移を捉える．

ハイブリッドモデル検査手法として手順および特定事例に特化した可視化を実現したが，対話的なアプローチであり，モデルベース開発の統合開発環境の試作には及ばなかった．

しかしながら，組込みシステムのハイブリッドモデル検査手法として制御可能領域の解空間を探索する処理手順を実用的なモデルベース開発環境 MATLAB/Simulink 上に構築できたことは，意義があると考えている．残念ながら，現状の問題点として，SMT ソルバの充足可能問題の解法処理に要する時間が掛かるため，小さな問題でも解空間獲得には多大な時間を必要とし実用性が低いことがあげられる．この対策としては，モデル検査対象を真に必要とされる範囲に限定することが良いと考えられるが，対象範囲の限定そのものが対象分野の高い知見や豊富な経験を必要とする．ハイブリッドモデル検査を一般化するには，効率の良い解空間探索や獲得の手法の開発が望まれる．

引用文献

[1] 大畠 明（トヨタ自動車）：講演「自動車制御システム開発におけるモデルベース開発の状況と展望」，MATLAB EXPO 2009 (2009/12)
[2] 電子情報通信学会「知識ベース」，3 章モデル検査(2010/02)
[3] 畠中克也ほか：組込みシステムを対象とした線形ハイブリッドオートマトンのモデル検査器の開発と検証，情報処理学会論文誌，Vol.53，No.12，pp.2671-2681 (2012/12)．
[4] 小林孝一ほか：モデル予測制御のための ハイブリッドシステムの離散抽象化，システム制御情報学会誌（システム/制御/情報），Vol.61，No.2，pp.51-56 (2017/08)．
[5] Roberta Piscitelli et.al.: Design Space Pruning through Hybrid Analysis in System-level Design Space Exploration, DATE ’12 (2012/3)
[6] Kai Lampka et.al.: Analytic Real-Time Analysis and Timed Automata: A Hybrid Method for Analyzing EMSOFT09, pp.107-116 (2009/12)
[7] OMG SysML, https://www.omgsysml.org
[8] Yices, https://yices.csl.sri.com
[9] Z3-Microsoft Research, https://www.microsoft.com/en-us/research/project/z3-3/
[10] The Alt-Ergo SMT solver by OCamlPro, https://alt-ergo.ocamlpro.com/
[11] Automated Program Verification Environment Web Interface, http://aprove.informatik.rwth-aachen.de/
[12] ARGO: Automated Reasoning Group, http://argo.matf.bg.ac.rs/?content=research

[13] Boolector, https://boolector.github.io/
[14] CVC4, https://cvc4.github.io/
[15] MathSAT 5: An SMT Solver for Formal Verification and More, https://mathsat.fbk.eu/
[16] Minkeyrink, https://minkeyrink.com/
[17] OpenSMT 2-Formal Verification and Security Lab, http://verify.inf.usi.ch/opensmt
[18] Q3B, https://github.com/martinjonas/Q3B
[19] SMTInterpol, https://ultimate.informatik.uni-freiburg.de/smtinterpol/
[20] SMT-RAT: Toolbox for Strategic and Parallel Satisfiability-Modulo-Theories Solving, http://smtrat.github.io/
[21] STP: The Simple Theorem Prover, https://stp.github.io/
[22] The veriT solver, https://verit.loria.fr/
[23] SMT-LIB The Satisfiability Modulo Theories Library, https://smtlib.cs.uiowa.edu/

５．主な発表論文等

〔雑誌論文〕　計0件

〔学会発表〕　計1件（うち招待講演　0件／うち国際学会　0件）

１．発表者名 Engielista Anak Norman, 上田賀一
２．発表標題 SimulinkとSMTソルバの連携による協調解析支援ツールの開発
３．学会等名 電子情報通信学会
４．発表年 2023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

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