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 １８ 日現在

機関番号：１３３０１
研究種目：基盤研究(C)（一般）
研究期間：2018～2020
課題番号：１８Ｋ１１２３９

研究課題名（和文）組込みアセンブリプログラムのリアルタイム安全性のソフトウェアモデル検査手法の開発

研究課題名（英文）Software model checking of real-time safety properties for embedded assembly program

研究代表者
山根　智（Yamane, Satoshi）

金沢大学・電子情報通信学系・教授

研究者番号：７０２６３５０６

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）：本研究では，ハードウェアとの相互作用があり，タイミング制約が厳しい組込みソフトウェアのリアルタイム性の形式的検証を研究目的とする．アセンブリプログラムを対象に，ソフトウェアモデル検査技術を開発し，組込みアセンブリプログラムのリアルタイム安全性検証の開発を研究目的とする．(1)アセンブリプログラムを変換して，組込みソフトウェアの形式的意味モデルである時間Kripke 構造を生成する．(2)定理証明技術を基礎として，SMT述語抽象化，SMTモデル検査及びSMT Interpolationの精錬により，組込みソフトウェアのリアルタイム性のモデル検査技術を開発する．

研究成果の学術的意義や社会的意義
現在のトヨタ車などのプログラム不具合の解消及び，今後の大規模ソフトウェアからなる自動運転の安全性確保などの問題もあり，組込みソフトウェア安全性保証の研究は，社会的かつ科学技術上の最重要な国際的課題である．従来の研究は仕様やＣプログラムの検証であり，組込みソフトウェアのハードウェアとの相互作用の検証やタイミング制約の検証が不十分である．本研究では，ハードウェアとの相互作用及びタイミング制約を検証するために，アセンブリプログラムを，形式的意味モデルである時間Kripke構造（アセンブリ命令の実行時間付き状態遷移システム）に変換して,リアルタイム性のソフトウェアモデル検査手法を開発することである

研究成果の概要（英文）：The purpose of this research is to formally verify real-time properties of embedded software that interacts with hardware and has severe timing constraints. The research objectives are to develop software model checking techniques for assembly programs, and to develop real-time safety verification for embedded assembly programs. (1) Transform assembly programs to generate the time Kripke structure, which is a formal semantic model of embedded software. (2) Based on theorem proving techniques, we develop a model checking technique for real-time embedded software by refining SMT predicate abstraction, SMT model checking, and SMT interpolation.

研究分野：ソフトウェア検証

キーワード：ソフトウェアモデル検査　組込みアセンブリプログラム　抽象化精錬　SMT　Interpolation

様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９（共通）

１．研究開始当初の背景

(1)本研究の学術的背景

現在のトヨタ車などのプログラム不具合の解消及び，今後の大規模ソフトウェアからなる自動運転の安全性確保などの問題もあり，組込みソフトウェア安全性保証の研究は，社会的かつ科学技術上の最重要な国際的課題である(毎年開催 ACM EMSOFT 等) ．従来の研究は仕様やＣプログラムの検証であり，組込みソフトウェアのハードウェアとの相互作用の検証やタイミング制約の検証が不十分である．申請者はハードウェアとの相互作用を組み込んだモデルの構築手法を開発して，アセンブリプログラムのソフトウェアモデル検査において先導的な研究を展開している(山根 他,IEICE 2017，GCCE 2014). 本研究では，ハードウェアとの相互作用及びタイミング制約を検証するために，アセンブリプログラムを，形式的意味モデルである時間 Kripke 構造（アセンブリ命令の実行時間付き状態遷移システム）に変換して,リアルタイム性のソフトウェアモデル検査手法を開発することである.

(2)研究課題の核心をなす学術的「問い」

組込みソフトウェアのリアルタイム性の検証では，ハードウェアとの相互作用及びタイミング制約の検証が重要であるために，以下のように，Ｃプログラムよりもアセンブリプログラムを検証対象とするほうが適切である．

(a)ハードウェアとの相互作用はシステムに特化したＣプログラム言語とアセンブリ言語を用いているので，アセンブリプログラムを検証する．(B. Schlich, ACM TECS,2010)

(b)プログラムの実行時間などに関わるタイミング制約はＣプログラムよりもアセンブリプログラムを対象とするほうが正確に解析と検証ができる．(山根，IEICE,2017)

以上より，「組込みソフトウェアのリアルタイム性の検証」という本研究課題の核心をなす学術的「問い」は，アセンブリプログラムを検証対象として，アセンブリプログラムから，ハードウェアとの相互作用およびタイミング制約といった組込みソフトウェアの特性を表す形式的意味モデル（時間 Kripke 構造）へ変換を行い，そのソフトウェアモデル検査技術（抽象化精錬や定理証明によるモデル検査）の確立である.

２．研究の目的

(1)本研究の目的

本研究では，ハードウェアとの相互作用があり，タイミング制約が厳しい組込みソフトウェアのリアルタイム性のソフトウェアモデル検査の開発を研究目的とする．具体的には，アセンブリプログラムを対象に，定理証明技術を用いて，SMT 述語抽象化，SMT 抽象モデル検査，SMT 反例解析及び SMT Interpolation により，抽象化精錬のモデル検査技術を開発し，組込みアセンブリプログラムのリアルタイム安全性検証の開発を研究目的とする．

(2)学術的独自性と独創性

本研究の学術的独自性と独創性は以下である.

(a)組込みソフトウェアのハードウェアとの相互作用およびタイミング制約を検証するために，アセンブリプログラムの変数値，スタックやアドレスばかりでなく，命令の実行時間を含めて，時間 Kripke 構造（＝組込みソフトウェアの形式的意味モデル）を定義する．アセンブリプログラムを時間 Kripke 構造へ変換する手法は国内外になく独自性がある．また，リアルタイム安全性などの検証性質をリアルタイム時相論理で記述する．

(b) SMT 述語抽象化，SMT 抽象モデル検査，SMT 反例解及び SMT Interpolation による抽象化精錬で，アセンブリプログラムを変換した時間 Kripke 構造がリアルタイム時相論理式を充足するかを判定するソフトウェアモデル検査技術は他にはなく，独創性がある．

３．研究の方法

本研究では，申請者らのこれまでの研究成果をもとに，組込みアセンブリプログラムのリアルタイム安全性検証を実現するために，以下を研究する．

(1) 時間 Kripke 構造により，アセンブリプログラムのハードウェアとの相互作用およびタイミング制約の形式的意味を定義する．

(2) 時間 Kripke 構造の SMT 述語抽象化，SMT 抽象モデル検査，SMT 反例解析，SMT Interpolation により，ハードウェアとの相互作用とタイミング制約を含めたアセンブリプログラムのリアルタイム性のソフトウェアモデル検査の理論と技術の開発を行い，その実験的な評価に関する研究を行う．

以下の分担（代表者 山根がモデル検査の理論実装，分担者 櫻井がプログラム解析）で，研究

期間内に下記のことを明らかにする．(①何を ②どのように ③どこまで明らかに)
(1)時間 Kripke 構造により，アセンブリプログラムのハードウェアとの相互作用およびタイミング制約の形式的意味の定義（担当：山根）
① アセンブリプログラムのハードウェアとの相互作用およびタイミング制約などの形式的意味を時間 Kripke 構造で表現する．
② アセンブリプログラムから時間 Kripke 構造に変換して，さらに検証性質をリアルタイム時相論理で仕様記述する．
③現実の組込みアセンブリプログラムの意味及びその検証性質が時間 Kripke 構造及びリアルタイム時相論理で表現できることを，理論的及び実験的に明らかにする．
(2)アセンブリプログラムのソフトウェアモデル検査（担当：山根,櫻井,大学院生 5 名）
① アセンブリプログラムのソフトウェアモデル検査を開発する．
② アセンブリプログラムのプログラム解析及び述語抽象化からなる SMT 述語抽象化により，時間 Kripke 構造の抽象化を行う（担当：櫻井，山根）．
③ 抽象時間 Kripke 構造の SMT 述語抽象化，SMT 抽象モデル検査，SMT 反例解析，SMT Interpolation（担当：山根）により，組込みアセンブリプログラムのリアルタイム性の抽象化精錬のソフトウェアモデル検査手法を開発する．大学院生 5 名と共同で，プロトタイプを実装して，現実の組込みソフトウェアのリアルタイム性の検証が行えることを明らかにする．

４．研究成果
(1)時間 Kripke 構造により，アセンブリプログラムのハードウェアとの相互作用およびタイミング制約の形式的意味の定義をした．
① アセンブリプログラムのハードウェアとの相互作用およびタイミング制約などの形式的意味を時間 Kripke 構造で表現した．
② アセンブリプログラムから時間 Kripke 構造に変換して，さらに検証性質をリアルタイム時相論理で仕様記述した．
③現実の組込みアセンブリプログラムの意味及びその検証性質が時間 Kripke 構造及びリアルタイム時相論理で表現できることを，理論的及び実験的に明らかにした．

【論文発表】
1. Yajun Wu, Satoshi Yamane:Model Checking of Embedded Systems Using RTCTL While Generating Timed Kripke Structure. COMPSAC (1) 2018, pp.257.
2. Satoshi Yamane:Deductive Verification Method of Real-Time Safety Properties for Embedded Assembly Programs. Electronics 2019, 8(10), pp.1-16.

(2)アセンブリプログラムのソフトウェアモデル検査
① アセンブリプログラムのソフトウェアモデル検査を開発した．
② アセンブリプログラムのプログラム解析及び述語抽象化からなる SMT 述語抽象化により，時間 Kripke 構造の抽象化を行った．
③ 抽象時間 Kripke 構造の SMT 述語抽象化，SMT 抽象モデル検査，SMT 反例解析，SMT Interpolation（担当：山根）により，組込みアセンブリプログラムのリアルタイム性の抽象化精錬のソフトウェアモデル検査手法を開発して，現実の組込みソフトウェアのリアルタイム性の検証が行えることを明らかにした．また，古典的なモデル検査器 SPIN と比較して，その優位性を示した．

【論文発表】
1. Yajun Wu, Satoshi Yamane:Model Checking of Real-Time Properties for Embedded Assembly Program Using Real-Time Temporal Logic RTCTL and Its Application to Real Microcontroller Software. IEICE Trans. Inf. Syst. 103-D(4),2020, pp.800-812.
2. Satoshi Yamane, Kosuke Uemura:Comparative Experiment of SPIN and SMT in Model Checking of Embedded Assembly Program. GCCE 2020, pp.54-57.
3. Yajun Wu, Hiromu Kamide, Satoshi Yamane:Software Model Checking for Real-time Properties of Embedded Assembly Programs Based on Lazy Abstraction and Refinement. GCCE 2020, pp.62-65.
4. Satoshi Yamane, Junpei Kobashi, Kosuke Uemura:Verification Method of Safety Properties of Embedded Assembly Program by Combining SMT-Based Bounded Model Checking and Reduction of Interrupt Handler Executions. Electronics 2020, 9(7), pp.1-24.
5. Kousuke Uemura, Satoshi Yamane:SMT-Based Bounded Model Checking of Embedded Assembly Program with Interruptions. 2019 IEEE Intl Conf on Dependable, Autonomic and Secure Computing, pp.633-639.
6. Hiromu Kamide, Kosuke Uemura, Satoshi Yamane:Model Check of Real-time Property of Embedded Assembly Program Using CEGAR. COMPSAC (1) 2018, pp.799-800.

５．主な発表論文等

〔雑誌論文〕　計7件（うち査読付論文　6件／うち国際共著　0件／うちオープンアクセス　4件）

１．著者名 Kousuke Uemura, Satoshi Yamane:	４．巻 17
２．論文標題 SMT-Based Bounded Model Checking of Embedded Assembly Program with Interruptions	５．発行年 2019年
３．雑誌名 2019 IEEE Intl Conf on Dependable, Autonomic and Secure Computing	６．最初と最後の頁 633-639
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/DASC/PiCom/CBDCom/CyberSciTech.2019.00120	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 Satoshi Yamane	４．巻 8(10)
２．論文標題 Deductive Verification Method of Real-Time Safety Properties for Embedded Assembly Programs	５．発行年 2019年
３．雑誌名 Electronics	６．最初と最後の頁 1-16
掲載論文のDOI（デジタルオブジェクト識別子） 10.3390/electronics8101163	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

１．著者名 上出広夢、山根智	４．巻 2154
２．論文標題 Lazy Abstractionと精練を用いた組込みアセンブリプログラムのリアルタイム性のソフトウェアモデル検査	５．発行年 2020年
３．雑誌名 RIMS講究録	６．最初と最後の頁 1-8
掲載論文のDOI（デジタルオブジェクト識別子） なし	査読の有無 無
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

１．著者名 Yajun WU, Satoshi Yamane	４．巻 103(4)
２．論文標題 Model Checking of Real-Time Properties for Embedded Assembly Program Using Real-Time Temporal Logic RTCTL and Its Application to Real Microcontroller Software	５．発行年 2020年
３．雑誌名 IEICE Trans. Information and Systems	６．最初と最後の頁 800-812
掲載論文のDOI（デジタルオブジェクト識別子） 10.1587/transinf.2019EDP7172	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

1．著者名 Yajun Wu ; Satoshi Yamane	4．巻 42
2．論文標題 Model Checking of Embedded Systems Using RTCTL While Generating Timed Kripke Structure	5．発行年 2018年
3．雑誌名 2018 IEEE 42nd Annual Computer Software and Applications Conference (COMPSAC)	6．最初と最後の頁 257-257
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/COMPSAC.2018.00040	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 Hiromu Kamide, Kosuke Uemura, Satoshi Yamane	4．巻 42
2．論文標題 Model Check of Real-time Property of Embedded Assembly Program Using CEGAR	5．発行年 2018年
3．雑誌名 2018 IEEE 42nd Annual Computer Software and Applications Conference (COMPSAC)	6．最初と最後の頁 799-800
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/COMPSAC.2018.00126	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 Satoshi Yamane, Junpei Kobashi, Kosuke Uemura	4．巻 9(7)
2．論文標題 Verification Method of Safety Properties of Embedded Assembly Program by Combining SMT-Based Bounded Model Checking and Reduction of Interrupt Handler Executions	5．発行年 2020年
3．雑誌名 Electronics	6．最初と最後の頁 1-24
掲載論文のDOI（デジタルオブジェクト識別子） 10.3390/electronics9071060	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

〔学会発表〕　計0件

〔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	櫻井　孝平 (Sakurai Kohei) (80597021)	金沢大学・電子情報通信学系・助教 (13301)	

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