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　元 年　 ６ 月　 １ 日現在

機関番号：２５４０３
研究種目：基盤研究(C)（一般）
研究期間：2015～2018
課題番号：１５Ｋ００８１

研究課題名（和文）ディペンダブル・サイバーフィジカルシステムを指向した組込みLSIの動作合成法

研究課題名（英文）A method for behavioral synthesis of embedded LSI for dependable cyber-physical systems

研究代表者
井上　智生（INOUE, Tomoo）

広島市立大学・情報科学研究科・教授

研究者番号：４０２５２８２９

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）：本研究は、自動車の運転支援・自動運転のような高性能で高い信頼性・安全性を必要とするコンピュータシステム（サイバーフィジカルシステム：CPS という）を安価で実現するための効率のよい設計法を提案するものである。
主な成果として、CPS の正常時と故障時の振る舞いを適切に表現する動作モデル、システムのコストを抑えながら高い信頼性・安全性を実現するためのシステムの構成法、ならびに、それを自動で合成・設計するためのアルゴリズム、が挙げられる。

研究成果の学術的意義や社会的意義
サイバーフィジカルシステム（CPS）は実社会に直接作用するコンピュータシステムであり、それに対する信頼性・安全性は重要である。これまでも当然ながら、信頼性、安全性を指向したコンピュータシステムは開発・実用化されているが、鉄道や旅客機などの大規模高価格のシステムが対象であったり、サイバー空間のみの信頼性（特にセキュリティ）に主眼を置くものが多かった。本研究の成果は、自動車の自動運転システムなど一般市民が生活の中で利用する CPS の信頼性・安全性を安価で実現することで、安心して暮らせる高度情報化社会の実現に貢献できるものと期待される。

研究成果の概要（英文）：This research aims to develop an efficient method for designing high-performance, reliable and safe computer systems, called cyber-physical systems (CPSs), with reasonable cost. The results of this research includes a behavioral model of fault-free and faulty CPSs, architecture of CPSs which has high reliability and safety, and a heuristic algorithm for synthesizing such systems.

研究分野：計算機工学、コンピュータの設計とテスト、ディペンダブル・コンピューティング

キーワード：サイバーフィジカルシステム　動作合成　モデルベース設計　信頼性　安全性　リアルタイム性　ディペンダビリティ

１．研究開始当初の背景

急速に発展する情報通信技術 (ICT) は我々の普段の生活に深く浸透するようになった。例えば、ITS (高度交通システム)・交通制御・運転支援・自動運転、拡張現実 (AR) による人間行動支援、及びこれらを統合するスマートシティ構想などがある。このようなシステムは、実社会 (Physical 空間) をセンシングして得られる環境情報をネットワーク経由で入手可能な多様なビッグデータを計算機 (Cyber 空間) で分析・処理し、実空間をリアルタイムに制御 (アクチュエーション) することで実現される。これをサイバーフィジカルシステム (CPS) という [1]。

CPS は、実空間にある大量で多様なデータを分析・処理し，それにもとづき実空間をリアルタイムに (すなわち時間制約の下で) 制御するために、高いスループットが必要である一方で，システム構成を軽量・小型で安価に実現できる必要があり、ハードウェア資源にも強い制約がある。さらにその対象は社会や人命に関わるため、高い信頼性・安全性も要求される。

２．研究の目的

厳しいハードウェア制約と時間制約の下で高い信頼性・安全性を有する CPS を実現するための組込み LSI の設計法・合成法を提案する。CPSでの計算処理における時間的なゆとり(時間制約下での処理時間のマージン) と演算結果に対する許容誤差を利用して、システムの稼働状況に応じて適切な誤り訂正を行うことで、信頼性・安全性を実現できるディペンダブル CPS (D-CPS) アーキテクチャを考案し、それを最適化する動作合成法を考察する。

３．研究の方法

(1) D-CPS のモデルベース設計環境の構築

サイバーフィジカルシステム (CPS) を設計するための動作モデルを構築する。サイバー空間は一般的に同期式順序回路として実現され、その動作モデルはクロックで動作する有限状態機械で表現される。一方実空間（フィジカル空間）は連続的でその動作を制御するクロックは存在しない。サイバーフィジカルシステムを設計する上では、これら2つの動作モデルをあわせて表現する必要がある。

また、ディペンダブル CPS (D-CPS) を設計するためには、このモデル上での故障とその振る舞い、すなわち、CPS としての故障モデルを表現可能にする必要がある。

これらを表現可能なモデルを構築するため、連続量と離散的動作を表現可能な Hybrid-Automata と時間制約下で動作を表現する Timed-Automata、およびこれらに基づいて設計された月面走行車のモデル例 [3] を参考にしながら、より一般的な CPS モデルを開発する。さらに、この CPS モデルに故障モデルを定義し、動作レベルの故障シミュレーションを可能とする。

(2) 時間制約と誤り許容性に着目した誤り訂正機構の提案

高信頼性を実現する代表的な方法として多重系がある。同じ機能を持つモジュールを2つ備え、出力を比較することで誤りを検出する2重系 (DMR) や 3 つの同機能モジュールの出力を多数決で選択し、誤りをマスクする（訂正する）3重系 (TMR) が一般的である。一時的な誤りを訂正するためには、前者の DMR 等を用いて誤りを検出し、チェックポイント (誤りのない状態) ロールバックする方法が採られる。2重系は3重系よりもハードウェアコストが小さいが、処理時間のペナルティが大きく、時間制約の厳しい CPS には単純なロールバックはできない。

一方、CPS のサイバー空間が入力とするフィジカル空間からのセンシングデータには常に揺らぎがあり、また、フィジカル空間への出力に対しても、一定量の時間的・空間的な誤りは共用される。

これらの点に着目し、大きく2つのアプローチを採用する。１つは、精度切り替え可能な演算

器アーキテクチャを提案する。サイバー空間で誤りが検出され、ロールバックのための再計算が必要になることを想定し、再計算時に（一時的に）演算精度を下げる代わりに演算時間（演算遅延）を小さくできる演算精度切り替え可能な演算器を提案する。近似演算により演算遅延を削減する乗算器の例として [5] などがあり、これを参考にして設計する。

もう一つは、一定の誤りを許容しながら近似的に誤り訂正を行う誤り補正機構の提案を行う。文献 [4] では、2つのモジュールからの出力をチェックし、閾値以下の誤りの場合は2つの出力の平均値を訂正結果として出力するアーキテクチャ IDMR が提案されている。本研究ではこれを参考に、CPS として許容可能な出力誤りに基づく近似誤り訂正機構の設計法を検討する。

(3) DMR/TMR混合型高信頼システムの動作合成法

レーテンシ (実行時間) 制約と面積制約の2つの制約の下で D-CPS を実現するために、システム全体を複数の動作ブロック (サブシステム) に分割し、各ブロックに対して DMR/TMR のいずれかを適用することで信頼度を高める。各ブロックを構成するハードウェアコストが信頼度を決定すると仮定したときに、ブロックの構成要素 (演算器など) と共有の仕方 (バインディング) によってその信頼度は異なる。また、ブロックのレーテンシによってはロールバック可能となり、よって小面積で信頼度を向上させることも可能となる。一方、リアルタイム制約の厳しいブロックには TMR によりハードウェアコストをかけて高信頼度を実現する方法が考えられる。この考え方に基づく、各ブロックの DMR/TMR の選択により信頼度を最大化する動作合成法を提案する。

４．研究成果

(1) ディペンダブル CPS (D-CPS) の動作モデル

CPS を設計するための動作モデルを提案した。提案モデルは、(i) サイバー空間とフィジカル空間をつなぐ時計を持つ、(ii) フィジカル空間の動作を表現する運動モデルを離散的に切り替えられる、(ii) サイバー空間に故障を挿入できる、などの特徴を持つ。提案モデルを MathWorks 社の Simulink を利用して実装した。例題として、自動車の運転支援機能の一部 (先行車追従、ABS (アンチロックブレーキシステム)) などを製作した。シミュレーションによりこれらの機能を再現し、サイバー空間の要求仕様 (リアルタイム制約など) が確認できる。

サイバー空間の故障モデルとして、センサ部および速度制御における演算回路の縮退故障 (出力値の一部が固定される故障) や遅延故障 (正しい演算結果の出力が遅れる故障) を想定し、シミュレーションを行った。一部の縮退故障や遅延故障では、CPS の動作として許容できるものがあることを確認した。

(2) 誤り許容性に基づく低面積誤り訂正機構

TMR (3重系) よりも低面積で誤り訂正可能なアーキテクチャを提案した。通常時の演算について、時間制約にゆとりがある場合、その限られた時間内でロールバックを行うための近似演算回路 (加算回路・乗算回路) を設計した。一時故障に対して有効である。ロールバック後の再計算時に演算器の演算精度を下げて実行する。低精度時の演算は通常時に比べて小さな遅延時間を持ち、時間制約下でロールバック可能となる。

CPS が許容できる誤りの大きさに着目した近似2重系 (IDMR) の設計法を開発した。[4] で提案されている IDMR アーキテクチャを参考に、与えられた許容誤差に対して面積最小となる IDMR の設計法を示した。

前者の演算器アーキテクチャ、後者の IDMR について、運転支援機構を想定して、一時故障発生時のシミュレーションを行った。それぞれについて、サイバー空間の故障時でも CPS が安定動作を継続できること、動作が不安定になる許容できない故障が存在することを示した。

(3) DMR/TMR混合型高信頼システムの動作合成法

レーテンシ制約 (リアルタイム制約) 下および面積制約下で信頼度を最大化する最適データパスを合成するためのヒューリスティックアルゴリズムを提案した。システムを構成する (合成に使用する) 演算器の信頼度が与えられるものとする。データパス全体を複数のブロックに分割し、各ブロックは、2重系よる誤り検出とロールバック、または、3重系によって信頼度を高めることができるが、3重系はより多くの面積を要する。各ブロックの信頼度向上方法を選択し、データバス全体の信頼度を最大化する。

自動車の運転支援機構の一部 (自動追従機能、走行車線維持、信号認識) のデータパス部を対象に、提案法を適用した。与えられたレーテンシ制約、面積制約の下で信頼度が最大となる合成結果が得られた。

＜引用文献＞

[1] 中島, 加藤 (編), “特集サイバーフィジカルシステム,” 情報処理, Vol.55, No.9, pp.908–954, 2014.

[2] Stavros Tripakis, Thao Dang, “Modeling, Verification and Testing using Timed and Hybrid Automata,” Model-Based Design for Embedded Systems, CRC Press, pp.383–427, 2009.

[3] Q. Wang, Y. Gang, X. Zhou, Y. Yang, “Behavior Modeling of Cyber-Physical System Based on Discrete Hybrid Automata,” Computational Science and Engineering, IEEE 16th International Conference, pp.680–684, 2013.

[4] Ke Chen, and Jie Han, and Fabrizio Lombardi, “Two Approximate Voting Schemes for Reliable Computing,” IEEE Trans. Comput., Vol.66, No.7, pp.1227–1239, 2017.

[5] H. R. Mahdiani, A. Ahmadi, S. M. Fakhraie, and C. Lucas, “Bio-Inspired Imprecise Computational Blocks for Efficient VLSI Implementation of Soft-Computing Applications,” IEEE Trans. Circuit & Syst. I: Reg. Papers, Vol. 57, No. 4, pp.850-862, 2010.

[6] Simulink, The MathWorks, Inc. (https://jp.mathworks.com/products/simulink.html).

５．主な発表論文等

〔学会発表〕（計 4 件）

行廣和倫, 岩垣剛, 市原英行, 井上智生, "MATLAB/Simulink を用いた自動運転システムの 性能低下故障に関する考察," 機能集積情報システム研究会, 2018年3月.

川嶋聖也, 岩垣剛, 市原英行, 井上智生, "精度切り替え可能な演算回路の設計とその応用について," 機能集積情報システム研究会, 2017年3月.

三藤泰武, 川嶋聖也, 岩垣剛, 市原英行, 井上智生, "自動追従制御のサイバーフィジカルモデルとその実装," 機能集積情報システム研究会, 2016年3月.

石森裕太郎, 川嶋聖也, 三藤泰武, 岩垣剛, 市原英行, 井上智生, "ディペンダビリティを考慮したサイバーフィジカルシステムのモデル化について," 機能集積情報システム研究会, 2016年3月.