様式 C-19

科学研究費補助金研究成果報告書

平成２１年　５月１９日現在

研究種目：基盤研究(C)
研究期間：2006～2008
課題番号：18560433
研究課題名（和文）　フォールトトレラントな分散スーパバイザ制御系のためのエラー検出とリカバリ機能
研究課題名（英文）　Error Detection and Recovery Mechanisms for Fault-Tolerant Decentralized Supervisory Control Systems

研究代表者
高井　重昌（TAKAI　SHIGEMASA）
京都工芸繊維大学・工芸科学研究科・准教授
研究者番号：60243177

研究成果の概要：大規模離散事象システムに対して，故障診断の機能とリカバリ制御の機能を備えた，フォールトトレラントな分散スーパバイザ制御系を設計するための基礎理論を構築した．まず，故障診断機能に関して，システムにおける故障事象の生起を有限時間内に検出できるための条件，およびその判定法などを明らかにした．そしてリカバリ動作を実現するためのスーパバイザ制御に関して，制御判断の曖昧さを陽に取り扱う分散スーパバイザ制御法などの成果を得た．

交付額

（金額単位：円）

	直接経費	間接経費	合　計
２００６年度	1,000,000	0	1,000,000
２００７年度	1,000,000	300,000	1,300,000
２００８年度	1,000,000	300,000	1,300,000
年度			
年度			
総　計	3,000,000	600,000	3,600,000

研究分野：システム制御理論
科研費の分科・細目：電気電子工学・制御工学
キーワード：(1) 制御工学　(2) 離散事象システム　(3) 故障診断　(4) スーパバイザ制御　(5) フォールトトレランス

１．研究開始当初の背景

生産システム，通信ネットワークなどのように事象が非同期，離散的に生起することにより，その状態が遷移するシステムは離散事象システムと呼ばれる．離散事象システムにおいては事象の生起順序が重要であり，例えばデッドロックに陥ることがないように，各事象の生起を制御する必要がある．事象の生起順序に関する離散事象システムの制御問題は，与えられた仕様を満足する事象列のみが生起するようにシステムの振舞いを制限する問題に帰着できる．このような制御問題を解くシステム理論的なアプローチとして，スーパバイザ制御理論が知られている．

スーパバイザ制御は，これまでに生起した事象の観測情報に基づき，可制御事象の生起を制御することにより，システムにおいて望ましくない事象列が生起しないことを保証するための手法である．しかし，制御系における故障など何らかのエラーにより，望ましくない事象が生起してしまった場合，有限時間内にその生起を検出し，制御モードをリカバリ動作に切り替える必要がある．また近年，ネットワーク化された大規模システムが

様々な分野で見られるようになってきた．制御対象である離散事象システムが大規模になると，そのコントローラの構成・維持・更新などの容易さの面から，集中制御よりも分散制御が有効である．このような背景から，故障事象など望ましくない事象の生起を検出する診断機能とリカバリ動作のためのスーパバイザ制御機能を組み合わせることで，フォールトトレラントな分散スーパバイザ制御系を設計することは重要な研究課題である．

２．研究の目的

大規模離散事象システムを対象とし，故障事象などの望ましくない事象の生起を有限時間内に検出するための診断機能とリカバリ動作を実行するためのスーパバイザ制御機能を有するフォールトトレラントな分散スーパバイザ制御系の実現を目指した研究を行う．制御系においては，高速・高効率といった従来からの要求に比べ，むしろ安全・高信頼がより重要なファクタとなりつつある．近年，システムの安全性を保証することの重要性は益々増しており，本研究は制御系の安全性に関する基礎理論に貢献するものである．

研究内容の詳細は以下の通りである．

(1) 離散事象システムの診断において，
・正常な事象列に対しては「異常」という診断をしない．
・故障事象を含んだ事象列に対しては「正常」という診断をしない．
・故障事象が生起した場合，高々有限個の事象の生起後に必ず「異常」という診断をする．
という三つの項目を満足することが故障検出を行う診断器に要求される．そこで，各ローカル診断器が，対象システムで生起した事象列に関するローカルな情報に基づき診断を行うような，分散型診断器の存在を効率的に判定できる条件を導出し，その計算量を解析する．さらに，その存在条件が満足される場合において，分散型診断器の構成方法を明らかにする．

(2) 故障事象など望ましくない事象の生起が検出された場合，システムに対してリカバリ動作のためのスーパバイザ制御が必要となる．そこで，大規模システムを対象とし，各ローカルスーパバイザが，対象システムで生起した事象列に関するローカルな情報に基づき制御判断を下すような，分散スーパバイザ制御系の開発を目的とする．具体的には，分散スーパバイザの存在条件の導出，その判定のためのアルゴリズムの開発，およびその計算量を明らかにする．さらに，存在条件が満足される場合において，スーパバイザの構成法を開発する．

３．研究の方法

本研究では，システム理論的アプローチにより，フォールトトレラントな分散スーパバイザ制御系を実現するための故障診断機能，リカバリ動作を行うスーパバイザ制御機能に関する研究を行う．システム理論的アプローチでは，対象システムの振舞いを表現する数学モデルを作成し，その数学モデルに基づき，システマチックなシステムの解析，設計手法を開発する．

本研究では，対象とする離散事象システムをオートマトン，もしくはペトリネットといった形式モデルによりモデル化を行う．それにより，システムの振舞いを事象集合上の形式言語で記述することができる．そして，形式言語の枠組みを用いて，故障診断問題，スーパバイザ制御問題を数学的に定式化し，理論的研究を行う．

本研究を実施するために使用する主な設備はパーソナルコンピュータであり，フォールトトレラントな分散スーパバイザ制御系の設計，検証およびシミュレーションなどに用いる．

４．研究成果

大規模離散事象システムを対象とし，故障診断機能とリカバリ制御の機能を備えた，フォールトトレラントな分散スーパバイザ制御系を設計するための基礎理論を構築した．故障診断，リカバリのためのスーパバイザ制御に関して，得られた主結果を以下に述べる．

(1) 現実の多くの大規模離散事象システムは，複数のサブシステムが並行的に動作する並行システムとみなすことができる．このような並行システムに対して，従来研究にある故障事象検出が可能であるための必要十分条件を判定する場合，並行システム全体のモデルが必要となり，いわゆる状態空間爆発の問題が生じる．

そこで本研究では，全体システムを構成することなく，各サブシステムのモデルのみを用いて判定できる，故障事象検出のための十分条件を導出した．この条件は十分条件であるが，システム全体のモデルを構成する必要がなく，計算量の観点からの利点を有する．さらに，得られた十分条件のもとでは，各サブシステムをローカル診断器により診断する分散型診断が可能であることを明らかにした．

並行システムにおける故障事象検出のための十分条件に関する従来研究では，故障事象は一つのサブシステム内部

で起こると仮定されており，複数のサブシステムに関係する故障事象を取り扱うことはできない．一方，本研究ではそのような制限は課しておらず，得られた条件は従来研究よりも広いクラスのシステムに対して適用可能である．

(2) 離散事象システムに対する診断器は，観測した可観測事象列に基づき故障事象の検出を行うが，予期せぬ事象センサの故障により，ある可観測事象の生起を診断器が観測できなくなるような状況が考えられる．そこで，センサ故障により高々一つの可観測事象が不可観測になる可能性がある場合においても，故障事象の生起を検出できるような診断器が存在するための必要十分条件を導出した．さらに，その必要十分条件を多項式オーダで判定する方法を明らかにした．

従来研究において，事象センサのエラーを考慮した確率的離散事象システムの診断問題が考察されている．そこでは，センサエラーを許容するような診断器が存在するか否かを判定する方法が示されているが，その計算量は指数オーダである．一方，本研究では，確定的な離散事象システムを対象とし，上述の従来研究とは異なる状況を考えている．さらに，本研究で導出した診断器の存在のための必要十分条件は多項式オーダで判定が可能であるという計算上の利点を有する．

(3) 分散スーパバイザ制御においては，各ローカルスーパバイザはシステムで生起した事象のローカルな情報により，制御判断を行う．しかしローカル情報のため，対象システムで生起した事象列が完全には特定できない不確かさのもとで各ローカルスーパバイザは制御判断を下すことになる．このため，ローカルスーパバイザの制御判断にはある意味で曖昧さが存在する．また，事象列に関する不確かさは各ローカルスーパバイザよって異なってくる．このため，判断の曖昧さもローカルスーパバイザによって異なったものとなる．しかし従来研究では，このような判断の曖昧さを定量的に取り扱う試みはなされていない．

そこで本研究では，判断の曖昧さを定量的に評価するような分散スーパバイザ制御法を提案した．そして，そのような制御系により制御仕様が達成されるための必要十分条件を導出した．さらに，その条件の判定アルゴリズムを提案した．本提案手法を用いることにより，従来研究の方法より，より広いクラスの制御仕様に対して，分散スーパバイザ制御系が構成可能となった．

また，与えられた制御仕様が，提案した分散スーパバイザ制御により達成できない場合には，制御仕様の近似に対して，分散スーパバイザ制御系を構成する方法を提案した．そして，従来研究との関連も含め，その近似に関していくつかの有用な性質を明らかにした．

(4) 複数の事象の同時生起を許したコンカレント離散事象システムに対するスーパバイザの存在条件の簡単化について考察した．従来研究において，コンカレント離散事象システムに対するスーパバイザが存在するための必要十分条件は，制御仕様として与えられた閉じた言語が可制御かつ Concurrently Well-Posed (CWP) であるということが示されている．しかし，CWP 性を判定するためのアルゴリズムは指数オーダである．

そこで本研究では，対象システムと制御仕様がともにコンカレント同期合成でモデル化されるという仮定のもとでは，制御仕様は常に CWP 性を満足し，スーパバイザが存在するための必要十分条件は，制御仕様の可制御性のみとなり，多項式オーダで判定できることを示した．このスーパバイザの存在条件の簡単化により，上述の仮定のもとでは，スーパバイザの存在条件を判定するための計算量が軽減されることが明らかになった．さらに，各サブシステムにおいて，ローカルな制御仕様が可制御ならば，全体システムにおける制御仕様が可制御となることを証明した．つまり，各サブシステムにおいて制御仕様が可制御ならば，全体システムのモデルを構成し，可制御性を判定する必要がないことが示された．

(5) ペトリネットは，並行システムの動作を表現する有力なモデルである．本研究では，ペトリネットによってモデル化された離散事象システムに対するスーパバイザの設計法についても考察した．一般に，ペトリネットの状態数は無限となるため，有限状態システムに対して提案されているスーパバイザの設計アルゴリズムをそのまま適用することはできない．

本研究では，状態数が無限となる非有界ペトリネットを有限オートマトンで近似する方法を新たに提案し，その近似モデルに対して最大許容スーパバイザを構成した．提案した近似モデルは非負整数値をとるパラメータを有し，そのパラメータ値を大きくすることにより，構成されたスーパバイザが許容的になるという望ましい性質を明らかにした．しかし，近似モデルに対して構成されたスーパバイザは，一般に，もとの非有界ペトリネットに対する最大許容スーパバイザとはならない．そこで，構成されたスーパバイザが最大許容スーパバイザとなるための，決定可能な十分条件を導出した．

５．主な発表論文等
（研究代表者、研究分担者及び連携研究者には下線）

〔雑誌論文〕（計５件）

① 河本　大，高井重昌，事象センサの故障を考慮した離散事象システムの診断，電子情報通信学会論文誌，vol. J92-A, 2009，印刷中，査読有
② Shigemasa Takai, Ratnesh Kumar, Synthesis of inference-based decentralized control for discrete event systems, IEEE Transactions on Automatic Control, vol. 53, pp. 522-534, 2008, 査読有
③ Ratnesh Kumar, Shigemasa Takai, Inference-based ambiguity management in decentralized decision-making: Decentralized control of discrete event systems, IEEE Transactions on Automatic Control, vol. 52, pp. 1783-1794, 2007, 査読有
④ 北村敦司，高井重昌，森　武宏，コンカレント同期合成でモデル化された離散事象システムにおけるスーパバイザの存在条件，電子情報通信学会論文誌，vol. J90-A, pp. 742-749, 2007, 査読有
⑤ Shigemasa Takai, Yongming Bai, Computation of controllable sublanguages for unbounded Petri nets using their approximation models, IEICE Transactions on Fundamentals, vol. E89-A, pp. 3250-3253, 2006, 査読有

〔学会発表〕（計９件）

① Shigemasa Takai, Inference-based decentralized prognosis in discrete event systems, The 47th IEEE Conference on Decision and Control, 2008年12月9日, Cancun, Mexico
② Shigemasa Takai, A sufficient condition for diagnosability of large-scale discrete event systems, The 23rd International Technical Conference on Circuits/Systems, Computers and Communications, 2008年7月7日, 山口
③ Shigemasa Takai, Decentralized prognosis of failures in discrete event systems, The 9th International Workshop on Discrete Event Systems, 2008年5月30日, Göteborg, Sweden
④ Shigemasa Takai, Inference-diagnosability: Nonconvergence and other complexity results, The SICE Annual Conference 2007, 2007年9月18日, 高松
⑤ Shigemasa Takai, Synthesis of over-approximating inference-based decentralized supervisors for discrete event systems, The 2007 American Control Conference, 2007年7月13日, New York, USA
⑥ Shigemasa Takai, Synthesis of inference-based decentralized control for discrete event systems, The 45th IEEE Conference on Decision and Control, 2006年12月13日, San Diego, USA
⑦ Shigemasa Takai, Computation of controllable sublanguages for unbounded Petri nets using their approximation models, The 2006 International Symposium on Nonlinear Theory and its Applications, 2006年9月12日, Bologna, Italy
⑧ Shigemasa Takai, Decentralized diagnosis for nonfailures of discrete event systems using inference-based ambiguity management, The 8th International Workshop on Discrete Event Systems, 2006年7月11日, Ann Arbor, USA
⑨ Ratnesh Kumar, Inference-based ambiguity management in decentralized decision-making: Decentralized diagnosis of discrete event systems, The 2006 American Control Conference, 2006年6月16日, Minneapolis, USA

６．研究組織
(1)研究代表者
高井　重昌（TAKAI　SHIGEMASA）
京都工芸繊維大学・工芸科学研究科・准教授
研究者番号：60243177

(2)研究分担者

(3)連携研究者

(4)研究協力者
ラトネッシュ　クマール（RATNESH KUMAR）
アイオワ州立大学・工学部・教授