様　式　Ｃ－１９、Ｆ－１９、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

平成 ２７ 年　 ５ 月 ２８ 日現在

機関番号：１４４０１
研究種目：基盤研究(C)
研究期間：2012～2014
課題番号：２４５６０５４７

研究課題名（和文）高信頼な離散事象システム設計のためのリライアブルな分散型故障診断

研究課題名（英文）Reliable Decentralized Failure Diagnosis for Design of Discrete Event Systems

研究代表者
高井　重昌（TAKAI, Shigemasa）

大阪大学・工学（系）研究科（研究院）・教授

研究者番号：６０２４３１７７

交付決定額（研究期間全体）：（直接経費）　　3,900,000円

研究成果の概要（和文）：ネットワーク化された離散事象システムに対するリライアブルな分散型故障診断法を確立するための理論的成果が得られた．ネットワークの不具合，ローカル診断器自体の故障などにより，幾つかのローカル診断器の判断が利用できなくなった状況を考慮した可診断性の検証アルゴリズム，故障の発生からその検出までの最長ステップ数を計算するアルゴリズムを開発した．また関連して，事象センサの故障を考慮した故障診断，スーパバイザ制御に関する理論的成果が得られた．

研究成果の概要（英文）：Theoretical results have been obtained to establish a theory for reliable decentralized failure diagnosis of networked discrete event systems. It may be possible that some local diagnosis decisions are not available, due to some reasons including breakdown of local diagnosers and disconnection of the network. Motivated by this, an algorithm is developed for verifying whether the system is diagnosable even if some of the diagnosis decisions are not available. In addition, an algorithm is presented for computing the maximum detection delay of a failure in such a case. As related work, theoretical results on failure diagnosis subject to sensor failures and supervisory control have also been obtained.

研究分野：システム理論

キーワード：システム理論　離散事象システム　分散型故障診断　スーパバイザ制御　リライアビリティ

１．研究開始当初の背景

輸送機器や大規模プラントなどは，その制御系の故障や不具合が人々の安全を脅かすことになりかねないセイフティクリティカルシステムの代表例である．このようなシステムに対しては，安全・高信頼が重要なファクタとなっている．安全・高信頼なシステムを実現するには，仕様通りにシステムが動作することを保証する高信頼な制御系機能に加え，故障の検出などを行う診断機能が重要となる．

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動的システムは離散事象システムと呼ばれる．近年，多くのシステムにおいて組込み制御系が用いられているが，離散的，事象駆動的な側面に着目することで，それらのシステムを離散事象システムとしてとらえ，論理的な振舞いの診断問題を離散事象システム理論の枠組みで取り扱うことができる．

離散事象システムの論理的な振舞いに基づく故障診断に関しては，Sampath らによって先駆的な論文が 1995 年に発表されて以来，その成果を拡張した多くの研究が行われており，離散事象システム理論の主要な研究テーマの一つとなっている．特に，ネットワーク化されたシステムに対しては，診断システムの構成・維持・更新などの容易さの面から，集中型よりも複数のローカル診断器による分散型診断が有効である．また，診断システム自体の信頼性を高める意味でも，複数の診断器により冗長性をもたせることは有効である．これまでの分散型診断に関するほとんどの研究では，すべてのローカル診断器が正常に動作し，それらのローカル判断がすべて診断に利用可能と仮定されていた．しかし，複数のローカル診断器による分散型診断システムにおいては，診断システムもネットワーク化されることになり，ネットワークの不具合などにより，あるローカル診断器の判断が診断に利用できなくなる場合が考えられる．また，ローカル診断器自体が故障することにより，その判断が得られなくなる場合もありうる．従って，分散型診断システム自体の信頼性を保証することは重要な問題である．

２．研究の目的

幾つかのローカル診断器の判断が利用できない可能性がある場合の離散事象システムの分散型故障診断については，文献

[1] J. C. Basilio and S. Lafortune: Robust codiagnosability of discrete event systems, Proceedings of the 2009 American Control Conference, pp. 2202-2209 (2009)

で考察されている．しかし，この論文の成果は以下の点から不十分であると考えられる．

・故障の発生が単一の故障事象の生起で表現できる特別な場合のみを扱っている．

・すべてのローカル診断器の判断が利用できる場合の従来の可診断性の検証に比べ，n 個のローカル診断器の内，最悪 k 個の診断器の判断のみが利用可能な場合，nCk 通りの診断器の組合せすべてに対して，従来の意味での可診断性を検証する必要があり，検証のための計算量が大幅に増加する．

・高々1 個の診断器の判断が利用できなくなる場合においては，従来の可診断性の検証の計算量と同じオーダで検証できる方法も示されているが，複数の診断器の判断が利用できなくなる場合への拡張については触れられておらず，そのような拡張は自明ではない．

・故障が発生してから検出されるまでのステップ数である検出遅れについて考察されていない．

そこで本研究では，上記の問題点を解決することで，幾つかの診断器の判断が利用できなくなったとしても対象システムで発生する故障の検出が可能であるという意味で，リライアブルな分散型故障診断法を確立することを目的とする．

３．研究の方法

本研究では，数学モデルに基づくシステム理論的アプローチを用いる．

まず，本研究で考察するリライアブルな分散型診断問題の定式化を行う．前述の文献[1]においては，故障の発生が単一の故障事象の生起で表現できる特別な場合のみを扱っており，診断の対象となる故障のクラスが制限されている．そこで本研究では，故障の発生を故障事象列の生起により，より一般的に表現する．各ローカル診断器は，システムの振舞いに関するローカルな観測情報に基づき，故障が発生したと判断した際に 1 を出力するとする．そして，分散型診断器全体として，少なくとも 1 個のローカル診断器が 1 を出力したとき，故障が発生したと判断するとする．つまり，ローカルな判断を OR で統合する．この場合，n 個の診断器の内，最悪，ある k 個の診断器の判断のみが利用可能な場合でも分散型診断器による故障の検出を保証するためには，n-k+1 個以上の診断器が 1 を出力する必要がある．そこで，分散型診断器は，

(i)　故障発生後に有限ステップ内で n-k+1 個以上のローカル診断器が 1 を出力する

(ii) 故障が発生していない状況では，どのローカル診断器も 1 を出力しない

という二つの要求を満足する必要がある．要求(ii)は，故障が発生していない状況で，誤った診断結果を出さないために必要となる．この分散型診断問題は，すべてのローカル診断器の判断が利用できる場合の従来の診断問題を k=n とした特別な場合として含む，より一般的な問題設定である．

そして，上記の二つの要求(i)，(ii)を満足するような分散型診断器の存在性を特徴づけるため，(n,k)-リライアブル可診断性の概念を定義する．そして，(n,k)-リライアブ

ル可診断性が，要求(i)，(ii)を満足するような分散型診断器の存在のための必要十分条件であることを証明する．この結果により，(n,k)-リライアブル可診断性の定義の正当性を示す．さらに，(n,k)-リライアブル可診断性を検証するために，テストオートマトンと呼ばれる検証用有限オートマトンを構成する．そして，そのテストオートマトンの構造に基づき，(n,k)-リライアブル可診断性を検証するアルゴリズムを開発し，その計算量解析を行う．

次に，n 個の診断器の内，最悪，ある k 個の診断器の判断のみが利用可能な場合において，故障の発生からその検出までの最長ステップ数の計算を，検証のために構成したテストオートマトンを用いて理論的に行う．この最長ステップ数は最悪の検出遅れに対応し，分散型診断システムの性能の尺度として重要である．

また，分散型診断器全体として，すべてのローカル診断器が 1 を出力したとき，故障が発生したと判断する，つまり，ローカルな判断を AND で統合する場合についても同様の研究を行う．ローカル診断器の判断を OR で統合する場合と AND で統合する場合とでは，診断可能なクラスが異なることが従来研究において知られており，それぞれ両方の場合を研究する必要がある．

ネットワークの不具合などにより幾つかの診断器の判断が利用できなくなる場合以外にも，事象の生起を観測するためのセンサの故障などにより，幾つかの事象の生起に関する情報が十分に得られなくなるような状況や，対象システムのモデルに不確かさが存在するような状況も考えられる．そこで，これらの状況のもとでの診断問題についても考察する．

さらに，高信頼な離散事象制御系の設計において必要となる，離散事象システムのリアルタイム制御，対象システムの状態遷移に非決定な不確かさが存在する場合のスーパバイザ制御に関する研究も行う．

なお，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，分散型診断システムの設計ツール，リライアブル可診断性の検証ツール，シミュレーションなどに用いる．

４．研究成果

(1) 離散事象システムのリライアブルな分散型故障診断法を確立するための理論的成果が得られた．

まず，n 個のローカル診断器の内，最悪 k 個の診断器の判断のみが利用可能な場合でも故障の発生を検出できるという意味でリライアブルな分散型故障診断問題を定式化した．そして，

・利用可能なローカル診断器の判断のうち，故障発生という判断が少なくとも一つあれば，分散型診断器全体として故障が発生したと判断する，つまりローカルな判断を OR で統合する場合
・利用可能なローカル診断器のすべての判断が故障発生であれば，分散型診断器全体として故障が発生したと判断する，つまりローカルな判断を AND で統合する場合

のそれぞれの場合において，n 個のローカル診断器の内，最悪 k 個の診断器の判断のみにより故障の発生を有限ステップ内で検出できることを保証する(n,k)-リライアブル可診断性の概念を定義し，対象システムにおいてそれが成立するか否かを有限オートマトン上で判定するアルゴリズムを開発した．さらに，最悪 k 個の診断器の判断のみが利用可能なもとで，故障の発生からその検出までの最長ステップ数を計算するためのアルゴリズムを開発した．

ローカルな判断を OR で統合する場合の結果は，先行研究の結果を拡張・補完するものである．一方，ローカルな判断を AND で統合する場合は，前者の場合に比べ，可診断性の検証，故障の発生からその検出までの最長ステップ数の計算がより難しい問題となり，先行研究では考察されていなかった．後者の場合に関する研究成果は，リライアブルな分散型故障診断において新たな知見を与えるものである．

分散型故障診断に関する既存研究において，各ローカル診断器の判断に条件付き判断を導入することの有効性が示されている．条件付き判断を用いたリライアブルな分散型故障診断への本研究の成果の拡張は，今後の研究課題と考えられる．

(2) 離散事象システムの故障診断において，事象の生起を観測するためのセンサの故障などにより，幾つかの事象の生起に関する情報が十分に得られなくなるような状況が考えられる．

そこで，このような状況を考慮した故障診断問題の定式化を行い，幾つかの事象の生起に関する情報が十分に得られなくなったとしても，故障の発生が有限ステップ内で検出できることを保証する可診断性の概念を定義した．そして，その可診断性が対象システムにおいて成立するか否かを有限オートマトン上で判定するアルゴリズム，故障の発生からその検出までの最長ステップ数を計算するアルゴリズムを開発し，これらのアルゴリズムの計算量解析を行った．

事象センサの故障を考慮した故障診断に関する従来研究では，最初からセンサが故障している状況を想定しており，システムの動作中にセンサが故障する場合には適用できない．一方，本研究は，システムの動作中に発生したセンサの故障により，これまで得られていた事象の生起情報が不完全にしか得られなくなることを許したより一般的なものであり，従来研究の成果をより現実的な状況へと拡張したものである．

(3) 本研究で用いるモデルベーストアプローチにおいては，対象システムのモデルにおける不確かさへの対処が重要な課題となる．

そこで，対象システムのモデルにおけるある種の不確かさのもとで，故障の発生が予知できることを保証する予知診断可能性の概念を定義した．そして，その予知診断可能性が成立するか否かを有限オートマトン上で判定するアルゴリズムを開発し，その計算量解析を行った．さらに予知診断器の構成方法を明らかにした

離散事象システムの故障予知診断に関する従来研究では，対象システムのモデルの不確かさは考慮されておらず，モデルの不確かさのもとでの故障予知診断は本研究で初めて考察されたものであり，得られた研究成果は故障予知に関する新たな知見を与えるものである．ただし，本研究はある特別な場合の不確かさについて考察したものであり，より一般的な不確かさのクラスへの拡張は今後の研究課題である．

(4) 高信頼な分散型離散事象制御系の設計においては，与えられた制御仕様が満足されるように，システムの動作を制限するコントローラであるスーパバイザを構成する必要がある．そこで，スーパバイザ制御に関する研究も行い，以下の成果が得られた．

① 組込みシステムなどで見られるリアルタイム仕様にも対応できるように，時間付き離散事象システムとしてモデル化されたシステムを対象とした分散スーパバイザ制御に関する研究を行った．

与えられた制御仕様に対してそれを満足する分散スーパバイザが構成できない場合，スーパバイザが構成できるような制御仕様の部分言語を計算する必要がある．そこで，そのような部分言語を計算するためのアルゴリズムを提案した．そして，そのあるアルゴリズムによって計算された部分言語に対する分散スーパバイザの構成方法を提案した．

与えられた制御仕様に対して，分散スーパバイザが構成できるための必要十分条件は従来研究で明らかにされていたが，その条件が満足されない場合において，分散スーパバイザが構成可能な制御仕様の部分言語の計算については考察されていなかった．本研究で得られた成果は，時間付き離散事象システムの分散スーパバイザ制御に関する従来研究を補完するものである．

② 状態遷移に非決定な不確かさが存在するような離散事象システムを非決定性オートマトンでモデル化し，同じく非決定性オートマトンで表現される制御仕様に対するスーパバイザ制御に関する研究を行った．

まず，スーパバイザは事象の生起だけでなく，遷移先の状態も観測できるという仮定のもとで，制御されたシステムが制御仕様と双模倣となるようなスーパバイザが存在するための必要十分条件を明らかにした．そして，スーパバイザの存在条件の判定アルゴリズムを提案し，その計算量解析を行った．

また，与えられた制御仕様に対して，制御されたシステムが双模倣となるようなスーパバイザが存在しない場合には，制御されたシステムが制御仕様に模倣されることのみを要求する模倣制御が考えられる．そこで，そのような模倣制御における最大許容スーパバイザの構成方法を提案し，その構成のための計算量の解析を行った．

非決定性オートマトンでモデル化された離散事象システムに対する従来研究においては，与えられた制御仕様に対して，制御されたシステムが双模倣となるようなスーパバイザの存在性を検証し，そのようなスーパバイザを構成するためには，スーパバイザの候補となるあるクラスの非決定性オートマトンをしらみつぶしに探索する必要があり，その計算量は対象システムと制御仕様の状態数に関して二重指数関数のオーダとなる．一方，本研究では，スーパバイザは事象の生起だけでなく，遷移先の状態も観測できるという仮定を課しているが，その仮定のもとでは，スーパバイザの存在性の検証，およびスーパバイザの構成が多項式オーダで行えることを示している．より弱い仮定のもとで，実用的な計算量でのスーパバイザの存在性の検証，およびスーパバイザの構成を可能とすることは今後の研究課題である．

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 10 件）

① Naoki Kanagawa, Shigemasa Takai, Diagnosability of discrete event systems subject to permanent sensor failures, International Journal of Control, 査読有, 2015, 掲載確定, DOI: 10.1080/00207179.2015.1051587

②串 直紀, 高井重昌, トランジションシステムの模倣制御における出力フィードバックコントローラの最大許容性, 電子情報通信学会論文誌, 査読有, Vol. J98-A, No. 3, 2015, pp. 255-266, http://search.ieice.org/bin/summary.php?id=j98-a_3_255

③Shigemasa Takai, Robust prognosability for a set of partially observed discrete event systems, Automatica, 査読有, Vol. 51, 2015, pp. 123-130, DOI: 10.1016/j.automatica.2014.10.104

④ Takashi Yamamoto, Shigemasa Takai, Reliable decentralized diagnosis of discrete event systems using the conjunctive architecture, IEICE Transactions on Fundamentals, 査読有, Vol. E97-A, No. 7, 2014, pp. 1605-1614,

DOI:10.1587/transfun.E97.A.1605

⑤ Katsuyuki Kimura, Shigemasa Takai, Maximally permissive similarity enforcing supervisors for nondeterministic discrete event systems under event and state observations, IEICE Transactions on Fundamentals, 査読有, Vol. E97-A, No. 7, 2014, pp. 1500-1507, DOI:10.1587/transfun.E97.A.1500

⑥ Katsuyuki Kimura, Shigemasa Takai, Bisimilarity control of nondeterministic discrete event systems under event and state observations, IEICE Transactions on Information and Systems, 査読有, Vol. E97-D, No. 5, 2014, pp. 1140-1148, DOI:10.1587/transinf.E97.D.1140

⑦ブートゥンナム, 高井重昌, 出力フィードバックによるトランジションシステムの模倣制御, 電子情報通信学会論文誌, 査読有, Vol. J97-A, No. 3, 2014, pp. 140-149, http://search.ieice.or.jp/bin/summary.pph?id=j97-a_3_140

⑧ Shuhei Nakata, Shigemasa Takai, Reliable decentralized failure diagnosis of discrete event systems, SICE Journal of Control, Measurement, and System Integration, 査読有, Vol. 6, No. 5, 2013, pp. 353-359, DOI: 10.9746/jcmsi.6.353

⑨ Masashi Nomura, Shigemasa Takai, A synthesis method for decentralized supervisors for timed discrete event systems, IEICE Transactions on Fundamentals, 査読有, Vol. E96-A, No. 4, 2013, pp. 835-839, DOI:10.1587/transfun.E96.A.835

⑩ Masashi Nomura, Shigemasa Takai, Computation of sublanguages for synthesizing decentralized supervisors for timed discrete event systems, IEICE Transactions on Fundamentals, 査読有, Vol. E96-A, No. 1, 2013, pp. 345-355, DOI:10.1587/transfun.E96.A.345

〔学会発表〕(計 5 件)

① Shoichi Yokota: Computation of the delay bound in decentralized diagnosis of discrete event systems with conditional decisions, The 53rd IEEE Conference on Decision and Control, 2014 年 12 月 17 日, Los Angeles (USA)

② Shigemasa Takai: Verification and synthesis for failure diagnosis of discrete event systems subject to permanent sensor failures, The 19th IEEE International Conference on Emerging Technologies and Factory Automation, 2014 年 9 月 17 日, Barcelona (Spain)

③ Shigemasa Takai: Abstraction-based verification of observability for discrete event systems, The SICE Annual Conference 2013, 2013 年 9 月 15 日, 名古屋大学（愛知県・名古屋市）

④ Takashi Yamamoto: Conjunctive decentralized diagnosis of discrete event systems, The 4th IFAC Workshop on Dependable Control of Discrete Systems, 2013 年 9 月 5 日, York (UK)

⑤ Katsuyuki Kimura: Bisimilarity enforcing supervisory control of nondeterministic systems under event and state observations, The 11th International Workshop on Discrete Event Systems, 2012 年 10 月 3 日, Guadalajara (Mexico)

〔その他〕
ホームページ等
http://is.eei.eng.osaka-u.ac.jp/takai/

６．研究組織

(1)研究代表者
高井　重昌 (TAKAI, Shigemasa)
大阪大学・大学院工学研究科・教授
研究者番号：60243177

(2)研究協力者
野村　雅司 (NOMURA, Masashi)
横谷　美怜 (YOKOTANI, Misato)
ブートゥンナム (VU TUNG, Nam)
金川　直樹 (KANAGAWA, Naoki)
木村　克行 (KIMURA, Katsuyuki)
山本　聖 (YAMAMOTO, Takashi)
横田　翔一 (YOKOTA, Shoichi)