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

平成　２９　年　　６　月　２３　日現在

機関番号：　１２６１４
研究種目：　基盤研究(C)（一般）
研究期間：　2014～2016
課題番号：　２６４２０４１０

研究課題名（和文）国際規格化を目指した制御システムのディペンダビリティ評価・管理技術の確立

研究課題名（英文）Dependability evaluation and management of control systems for possible publication in international standards

研究代表者

陶山　貢市（SUYAMA, Koichi）

東京海洋大学・学術研究院・教授

研究者番号：８０２２６６１２

交付決定額（研究期間全体）：（直接経費）　　3,800,000円

研究成果の概要（和文）：制御システムには様々な構造と機能があり，IEC 規格の定義に沿ったアベイラビリティの汎用性の高い解析は難しい．本研究では，LFT 表現を用いることで様々な構造に対応し，また，マルコフ解析の際の状態遷移図上で制御システムの機能が維持されている状況に対応する“available state”を考えることで，機能の違いをマルコフ解析に反映させる．そして，広いクラスの制御対象に対する様々な構造・機能を有するシステムを扱うことができる解析の枠組みを確立した．アベイラビリティ性能指標値を解析結果とするこの枠組みにより，様々な手法で実現される制御システムのフォールトトレランスの定量的な評価が可能になった．

研究成果の概要（英文）：Since there are the varieties in structures and functions of control systems, it is difficult to analyze their dependability according to international standards. In this research, we use the LFT description of control systems in order to absorb the variety of system structures and an idea of "available states" on state-transition diagrams used in continuous-time Markov analysis in order to absorb the variety of designed control functions. We then establish a general framework of availability analysis of control systems according to IEC standards, which is based on continuous-time Markov analysis and gives the value of steady state availability as the analysis result. It enables us to quantitatively evaluate fault tolerance of control systems in various application areas, and thus it succeeds in improving the practicality of fault-tolerant control.

研究分野：　工学

キーワード：　制御工学　システム工学　ディペンダビリティ　アベイラビリティ　国際規格

１．研究開始当初の背景

(1) 産業界における国際規格の重要性の増大と日本の対応の遅れ

ドイツは，四半世紀以上の長期にわたって，国際競争力に直結する国際規格（ex. IEC 61508: Functional safety of electrical / electronic / programmable electronic safety-related systems）の制定・改訂・普及へ貢献し，自国産業界に有利な方向へ誘導するとともに，テュフなどの世界的な認証機関を国策として育成してきた．この国際規格を中心に据えた長期的戦略が現在のドイツの国力につながっている．その集大成とも言うべきものが，IEC 61508 を基礎として 2011 年に発行された自動車の電子制御システムの安全性に関する ISO 26262: Road vehicles ― Functional safety ― である．この国際規格への対応のため，世界中の企業は競って「ドイツもうで」,「テュフもうで」を行っている．自動車産業以外の産業分野においても，すでに多くの組織・機関で認証やそのサポートが行われている欧米諸国に比較して，認証などの制度・システム面や資金面，すべてにわたり，日本は重要な国際規格への対応が遅れていると言われている．その結果，日本の国際競争力は全体的に低下する一方であることは論を待たない．また，何よりも国際規格そのものに対する貢献が決定的に不足している．

(2) 制御システムのディペンダビリティ評価法の未確立

その一方で，信じられないことであるが，多くの工業製品に含まれる制御システムに関して，その本来の機能に注目するディペンダビリティ（広義の信頼性）の評価法は技術的に未だに確立されておらず，産業界が「よりどころ」とする国際規格も制定されていない．ISO 26262 においても，主に安全性に関わるエアバッグの制御システムとエネルギー効率に関するロックアップの制御システムが同列に扱われるなど，制御システムの安全性とディペンダビリティが明確に区別されていない．ディペンダビリティが安全性に置き換えられ，外部への危害・悪影響に注目する安全性の評価法が準用されることも多く，高機能な制御技術を用いている日本の工業製品が必ずしも適正かつ正当に評価されていない，すなわち国際競争力へ結び付いていないのが現状である．

２．研究の目的

(1) 世界に先駆けた制御システムのディペンダビリティ評価法の確立

コンポーネントの結合体としての制御システムがソフトウエアで駆動されている，すなわち制御システム本来の機能の実現にソフトウエアが重要な役割を担っているような状況は，これまで信頼性の分野では議論されていなかった．様々な構造・機能を有する制御システムが存在することもあって，ディペンダビリティを評価する汎用的な枠組みの構築は難しい．本研究では世界に先駆けて，国際規格に準拠した形で，制御システムのディペンダビリティ評価法を確立する．

(2) 制御ロジックによるディペンダビリティ管理技術の確立

(1)に基づいて，制御ロジックにより制御システムのディペンダビリティを向上させる技術を確立する．制御ロジックの良し悪しがディペンダビリティを左右することを明確にする，さらにはディペンダビリティの観点での制御設計の重要性を示すという意義がある．制御ロジックにより安全性を向上させる高安全性制御設計は日本が世界をリードしてきた分野であり，それを基礎として，また新たな日本発の技術を世界に送り出す．

さらに，この日本発の新技術は，制御工学にとっては新しい技術的方向性を示すことになるのは言うまでもない．信頼性の分野からしても，従来にない全く新しいディペンダビリティ管理手法が提示されることのインパクトは計り知れない．さらに，信頼性工学と制御工学との間の境界領域に位置する日本発の世界に冠たる新技術であり，将来にわたって日本が世界を技術的にリードすることができる分野の新規確保にもつながる．国際競争力の観点から非常に意義が高く，企業関係者からも広く注目されている．また，国際規格関係者からも非常に高い評価を受けている．

(3) 日本発の新技術による世界に対する貢献と将来の国際規格化

本研究で確立する制御システムのディペンダビリティ評価・管理技術を日本発の新技術として発信し，世界に対して大きな貢献をする．それだけでも日本の国際競争力を向上させる効果があると考えているが，さらにそれを確固たるものにするには，日本の主導で将来の国際規格化につなげることが望ましく，それこそが本研究の究極の目的である．

３．研究の方法

(1) 制御システムのディペンダビリティを評価する新技術の確立

① 全体像

信頼性の分野では，各コンポーネントの故障率・修復率が与えられ，ハードウエア全体としてのアベイラビリティ指標の値（一般的には，機能が維持されている確率）を求めるというディペンダビリティ評価法しか確立されていない．そこで，制御ロジックにより実現される制御システムの本来の機能の高さが適正に反映されるようなディペンダビリティ評価法を構築する．具体的には，故障率・修復率などのハードウエアの情報とす

でに設計されているソフトウエア（制御ロジックなど）の情報を両方使った評価法である．現在に至るまで，IEC の Technical Committee 56: Dependability がこれまでに制定した国際規格も含め，信頼性の分野の国内外の著名な書籍・ハンドブックなどには，制御ロジックなどのソフトウエアを取り込んでのディペンダビリティ評価法は紹介されていない．そのため，世界に先駆けて確立することができるのである．

② 制御システムの様々な構造への対応

様々な構造の制御システムに対応するため，制御システムの機能の解析・評価や制御ロジック（コントローラ）に機能を埋め込むための解析・設計で広く用いられている LFT (Linear Fractional Transformation) 表現の上で統一的に議論する．

③ 制御システムの様々な機能の扱い

一般に，アベイラビリティ指標の値を算出するには，連続時間マルコフ解析が必要である．様々な構造・機能を有する制御システムに汎用的に適用できる評価法とするためには，マルコフ解析の際の状態遷移図上で機能の違いを吸収する工夫が必要である．研究代表者は，平成 22-25 年度基盤研究(C)(一般)「国際規格に準拠してレンジ逸脱に対する安全性を制御則で実現する日本発の新技術」において，安全性の一環として制御システムの最低限の機能を維持するという信頼性の観点からの対策を制御ロジックの機能として実現した．その際に行ったマルコフ解析は，レンジ逸脱が発生するまでの平均時間を求める吸収マルコフ解析である．本研究では，それを基礎とする．

④ 国際規格への準拠

実用性を産業界に広くアピールする，さらには将来の国際規格化まで視野に入れるためには，ディペンダビリティ及びアベイラビリティの定義，アベイラビリティ指標の定式化から，(故障モードなど) 使用する用語，マルコフ解析手法に至るまで，国際規格に準拠することが必須であるのは言うまでもない．本研究では，ディペンダビリティ関連のすべての IEC 規格が準拠する用語集 IEC 60050-192: International electrotechnical vocabulary — Part 192: Dependability に基づいて，制御システムのディペンダビリティを評価する新技術を構築する．

(2) 制御ロジックによりディペンダビリティを管理する新技術の確立

(1)の評価の意味で，制御システムのディペンダビリティは状態遷移図上の機能が維持されている状態の集合と同一視することができる．そこで，アベイラビリティ指標の与えられた目標値をクリアするその集合の可能性１つ１つについて，それを実現しつつ，正常時の機能(制御性能)を最適化する制御ロジックを求める．そして，それらの中からもっとも正常時の機能が高いものを選べばよい．本研究では，その集合の可能性の列挙など，平成 22-25 年度の基盤研究(C)(一般)による研究成果を基礎として，そのような制御ロジックによるディペンダビリティ管理技術を確立する．

(3) 研究成果を具現化するソフトウエアの開発

(1),(2)の研究成果である制御システムのディペンダビリティを評価する技術，及び制御ロジックによりディペンダビリティを管理する技術を，コンピュータ上のソフトウエアとして具現化する．そのようなソフトウエアがあることは，これら新技術の実用性をアピールする際に，重要なポイントとなると考えられる．

(4) 研究成果の国際規格への反映

IEC TC56: Dependability や IEC 61508 の改定作業委員会などの国際規格関係者に対して，(1)-(3)の研究成果を日本からの貢献としてアピールし，将来の国際規格化を目指す．

４．研究成果

(1) 制御システムのディペンダビリティを評価する新技術の確立

以下の５ステップからなるディペンダビリティ評価法を確立した．

① ステップ１：正常時の機能評価

解析対象の(正常時の) 制御システムが図１に示すような LFT 表現により与えられているとする．G は，一般に LFT 表現で用いられる，制御対象 P の情報，及びコントローラ K をつないで制御システムとしたときの機能評価の情報を中に含んだ一般化プラントと呼ばれる部分である．制御システムの機能は w から z までの伝達特性 T_{zw} として表現される．その H_∞ノルムの値が制御システムの正常時の機能の指標である（値が小さいほど高機能)．

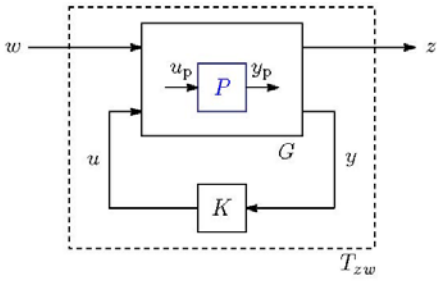

図１　LFT 表現

② ステップ２：故障モードの想定

制御システムが n 個のデバイスを含む．j 番目のデバイスの正常(0)あるいはフォールト(1)を i_j で表現すれば，制御システムの置かれた状況は $(i_1, i_2, \ldots, i_n)$ により表現できる．それがそのままステップ５の連続時間マルコ

フ解析における状態遷移図上の状態の表現となる．

③ ステップ３：故障時の制御システムの表現

状況 $(i_1, i_2, \ldots, i_n)$ における制御システムは，図１中の P を図２の P' で置き換えることにより得られる．ここで，P 以外の Fa, Fs の部分を適当に設定することで，スタック故障，出力低下，ドリフト故障など，様々な故障モードを扱うことができる．

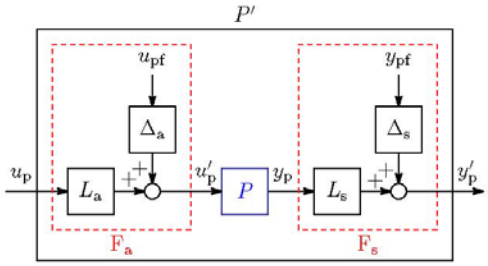

図２　故障状況の表現

④ ステップ４：機能が許容範囲内に維持されている状況の把握

制御システムの機能が許容範囲内に維持されているための条件を整理して，そのようになっている状況をすべて把握する．

⑤ ステップ５：連続時間マルコフ解析による定常アベイラビリティの算出

ステップ４で求めた制御システムの機能が許容範囲内に維持されている状況に対応する状態を “available state” と呼ぶ．すなわち，available state に対応する状況では，制御システムの機能は維持されている．状態遷移図上のある状態が available state であるか否かは制御システム本来の機能，制御ロジックなどにより決まる．同じ制御システムであっても，考える機能が異なれば，結果として available states の集合は異なる．したがって，機能の違いを available states の集合の違いに反映させることが可能となっている．そのため，様々な制御システムの機能を扱うことができるのである．

図３のように，状態遷移図上すべての available states の集合を把握する．その集合内の available state のいずれかが発現している確率を連続時間マルコフ解析（特に定常マルコフ解析）によって求めれば，それが機能が維持されている確率，すなわちアベイラビリティ指標となる．また，システムダウンまでの平均時間（狭義の信頼性の代表的指標）は初めてその集合から出るまでの平均時間として得られる．制御システムを駆動するソフトウエアとしての制御ロジックがディペンダビリティ評価に反映されていることに注意されたい．

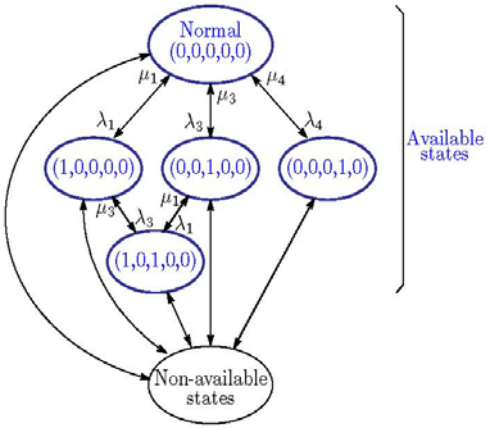

図３　状態遷移図の例

アベイラビリティ指標としての定常アベイラビリティを解析結果とするこの評価法により，様々な手法で実現される制御システムのフォールトトレランスの定量的な評価が広く可能になった．これは制御工学の発展に大きな貢献をすると考えられる．

以上の研究成果は，日本信頼性学会誌に採録された雑誌論文⑤を通じて，国内の信頼性関係者に向けて発信することができた．将来の国際規格化のためには，まずは国内のコンセンサスが不可欠であるからである．

(2) 制御ロジックによりディペンダビリティを管理する新技術の確立

ディペンダビリティ管理という観点では，アベイラビリティ性能指標の目標値を達成しつつ，正常時の機能（制御性能）を最適化する制御ロジックを求めることが必要となる．その最適な制御ロジックの候補は，制御システムのディペンダビリティと同一視できる available states の集合により与えることになる．そこで，アベイラビリティ指標の与えられた目標値をクリアする available states の集合の可能性１つ１つについて，多目的設計の手法により，正常時の機能を最適化する制御ロジックを求める．そして，それらの中からもっとも正常時の機能が高いものを選ぶ．これが本研究で確立した制御ロジックにより制御システムのディペンダビリティを管理する新技術である．

従来，産業界では，また国際規格上も，システムのハードウエアとしてディペンダビリティを確保するという考え方・手法が一般的であった．それに対して，新技術は制御ロジックというソフトウエアのレベルのディペンダビリティ確保策の可能性を確立した．従来からのハードウエアによる確保策を補完するものとして，制御の分野が貢献できることを示した意義は大きく，この日本発の新技術への期待は国際規格関係者の間でも非常に大きい．

また，制御ロジック，すなわち(理論面，実際面両方で整備が遅れている)ソフトウエ

アの確率的評価・管理という意味からも，一つの方向性を示すものとして，国際規格関係者の注目を集めている．

なお，(2)に関する研究成果は，(1)に関する研究成果と合わせて，今後，英文の論文にまとめ，欧米の国際規格関係者へ情報を伝達する予定である．

(3) 新技術の実用化へ向けた研究

新技術の適用事例・実績をあげるべく，自動車用エアバッグシステム，自動車用安全制御システムなど，具体的なシステムを想定して実用化へ向けた基礎的研究を行った．

(4) 本研究を進める過程で得られたシステムの切替 L_2 ゲイン解析などの研究成果

システムの切替発生直後の応答の最悪な乱れに注目するまったく新しい切替 L_2 ゲイン解析を確立した．そして，この切替 L_2 ゲイン解析を故障の影響の評価へ応用した．また，コントローラのリセットが効果的に遂行可能か否かを制御システムの状況から瞬時に判断する技術へも応用した．

ディペンダビリティを向上させるためには，故障対策だけではなく，修理しやすさを含めた保全性を向上させる必要がある．制御システムのフォールトトレランスは，その保全性の向上に貢献することができるが，それは本研究で見出したフォールトトレランスのまったく新しい意義である．また，保全性の定量的な評価は信頼性の分野においても難しい課題である．本研究では，保全後の制御システムのリスタートのしやすさという観点から，上記の新しい切替 L_2 ゲインが保全性の性能指標となり得ることを明らかにした．

なお，以上(1)-(4)の研究成果に関しては，IEC TC56: Dependability や IEC 61508 の改訂作業委員会などの国際規格関係者へ，折に触れて情報提供を行っている．将来の国際規格への反映も視野に入れているので，そのための事前活動である．

(5) 学術的な特色・意義

国際規格は個々の企業にとってはその利益に直結しかねないので，本研究のような内容は，特に規格の策定/改定過程では，企業と一線を画して中立的に行われるべきであると考える．その意味では科学研究費補助金を使った大学レベルの非営利かつ学術的な研究がもっとも適当である．

また，本研究のような国際規格を中心とした「泥臭い」，しかし非常に実際的な研究は，特に制御の分野では，貴重な存在であり，新しく打ち出される方向性のインパクトはきわめて大きいと考えられる．

さらに，本研究は，成果を国際規格に実際に反映させるところまで視野に入れるという稀有なものであり，大学の学術的な研究の枠を広げるというきわめて重要な意義がある．

国際規格に基づく認証は品質，環境に続く第３の世界的なうねりとして欧米から今まさに押し寄せようとしている．日本が立ち遅れない，さらには主導権を握るには，ここ数年の活動・研究がきわめて大事であり，それが日本の国際競争力，ひいては将来を左右すると言っても過言ではない．本研究の重要性をここに強調する次第である．

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１４件）

① Koichi Suyama and Noboru Sebe, Controller reset strategy for anti-windup based on switching L2 gain analysis, Asian Journal of Control, 査読有, 2017 (採録決定済み), 14 pages, DOI: 10.1002/asjc.1530

② Koichi Suyama and Noboru Sebe, Switching L2 gain for analyzing the magnitude of a system switch, Proceedings of the 55th IEEE Conference on Decision and Control, 査読有, 2016, pp.6395-6402, DOI: 10.1109/CDC.2016.7799253

③ Koichi Suyama and Noboru Sebe, Evaluation of the ease of restarts in fault-tolerant control systems using multiple switching L2 gains, Proceedings of the 42nd Annual Conference of the IEEE Industrial Electronics Society, 査読有, 2016, pp.140-147, DOI: 10.1109/IECON.2016.7793652

④ Ryosuke Nakamura, Noboru Sebe, and Koichi Suyama, A study on semi-active fault tolerant servo systems by switching passive fault tolerant controllers, Proceedings of the International Conference on ICT Robotics, 査読有, 2016, 4 pages, DOI なし

⑤ 陶山貢市, 制御システムのアベイラビリティ解析の IEC 規格に準拠した一般的枠組み ― マルコフ解析による定常アベイラビリティの算出 ―, 日本信頼性学会誌, 査読有, Vol.38, No.2, 2016, pp.129-145, DOI なし

⑥ Koichi Suyama and Nobuko Kosugi, A new approach to Bezout equations derived from multivariate polynomial matrices and real entire functions, Linear and Multilinear Algebra, 査読有, Vol.63, Issue 11, 2015, pp.2318-2331, DOI: 10.1080/03081087.2015.1008969

⑦ Koichi Suyama and Noboru Sebe, Tolerance against multiple fault modes and its application to corrective maintenance of faulty actuators in servo systems, Proceedings of the 20th IEEE International Conference on Emerging Technologies and Factory Automation, 査読有, 2015, 8 pages, DOI: 10.1109/ETFA.2015.7301535

⑧ Koichi Suyama and Noboru Sebe, New switching L2 gain analysis for a restart with controller resets after maintenance, Proceedings of the 8th IFAC Symposium on Robust Control Design, 査読有, 2015, pp.349-356, DOI: 10.1016/j.ifacol.2015.09.482

⑨ Kenta Toyoda, Noboru Sebe, and Koichi Suyama, Effects of diagonal dominance on performance of passive fault tolerant servo systems, Proceedings of the 10th Asian Control Conference, 査読有, 2015, 6 pages, DOI: 10.1109/ASCC.2015.7244644

⑩ Koichi Suyama and Nobuko Kosugi, Bezout equations over bivariate polynomial matrices related by an entire function, Linear and Multilinear Algebra, 査読有, Vol.63, Issue 6, 2015, pp.1138-1153, DOI: 10.1080/03081087.2014.922968

⑪ Koichi Suyama and Noboru Sebe, Fault-tolerant servo systems using integrators with variable limits, Proceedings of the 19th IEEE International Conference on Emerging Technologies and Factory Automation, 査読有, 2014, 8 pages, DOI: 10.1109/ETFA.2014.7005076

⑫ Noboru Sebe and Koichi Suyama, Passive fault tolerant servo control against one device failure out of sensors and actuators, Proceedings of the 13th European Control Conference, 査読有, 2014, pp.644-651, DOI: 10.1109/ECC.2014.6862322

⑬ Koichi Suyama and Noboru Sebe, Dependability analysis of fault-tolerant servo systems using limited integrators, Proceedings of the 13th European Control Conference, 査読有, 2014, pp.652-659, DOI: 10.1109/ECC.2014.6862235

⑭ Isshi Koyata, Koichi Suyama, Yoshinobu Sato, Mean fault time for estimation of average probability of failure on demand PFDavg, Proceedings of the 12th International Conference on Probabilistic Safety Assessment and Management, 査読有, 2014, 8 pages, DIO なし

〔学会発表〕(計 1 件)

① 大崩光平, 瀬部昇, 陶山貢市, 故障発生時の過渡特性を考慮した耐故障性を有するサーボ系の設計, 第 57 回自動制御連合講演会, 2014 年 11 月 10 日, ホテル天坊 (群馬県渋川市)

〔図書〕(計 1 件)

① 日本信頼性学会編, 陶山貢市 他著, 日科技連出版社, 新版 信頼性ハンドブック, 2014, 915 pages (pp.503-506)

６．研究組織

(1)研究代表者

陶山　貢市 (SUYAMA, Koichi)

東京海洋大学・学術研究院・教授

研究者番号：８０２２６６１２