科学研究費助成事業　　研究成果報告書

平成　２６　年　　５　月　１４　日現在

機関番号：　１２６１４
研究種目：　基盤研究(C)
研究期間：　2010～2013
課題番号：　２２５６０４４０

研究課題名（和文）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

研究課題名（英文）New technology from Japan for realization of safety function against deviations from normal operating-range in control laws according to international standards

研究代表者
陶山　貢市（Suyama, Koichi）

東京海洋大学・海洋科学技術研究科・教授

研究者番号：８０２２６６１２

交付決定額（研究期間全体）：（直接経費）　　3,600,000円、（間接経費）　　1,080,000円

研究成果の概要（和文）：本研究では，制御則のレベルで制御レンジからの逸脱対策という安全機能を考えた．制御レンジからの逸脱は，制御系の不安定化だけでなく，制御デバイス故障直後の過渡応答の乱れによっても生じる可能性がある．そのため，過渡応答の乱れの指標を導入し，故障直後の制御レンジからの逸脱の頻度を定量的に求め，IEC 61508 などの国際規格に準拠した形で制御則の安全性を評価する枠組みを構築した．さらに，その指標を抑制する制御則設計の枠組みを構築した．この日本発の新技術が従来の安全計装を補完できる可能性を提示することができた．

研究成果の概要（英文）：This research clarified safety function in control laws to reduce the frequency of events that a physical value in a control system deviates from its normal operating-range. The deviations can be caused not only by system destabilization but also by fluctuations of transient responses. In order to quantitatively establish the contribution of the safety function in control laws for risk reduction, this research established a quantitative assessment framework for obtaining the frequency of the deviations by using a performance index for the fluctuations of transient responses. Furthermore, this research also established a realization framework for the safety function in control laws, which can supplement ordinary safety-related systems in risk reduction according to international safety standards such as IEC 61508.

研究分野：　工学

科研費の分科・細目：　電気電子工学・制御工学

キーワード：　安全性　国際規格　制御システム　制御レンジ　制御性能　制御則　耐故障性　ソフトウエア

１．研究開始当初の背景

(1) 制御システムの安全性に対する社会的な意識・要求の高まり

航空機の飛行制御系では，舵角，飛行速度などの異常値を検出すると，安全のための緊急処理に入る．制御システム内の物理量が制御レンジの上下限を超えることで異常を検知し，オーバーライドやトリップ処理に入るという安全性確保の考え方・手法は，安全計装の現場で一般的である．また，日常生活のあらゆるところに存在する制御システムにもそのように設計されているものが多い．

しかし，そのような異常が起きた後の安全対策だけでは，近年の制御システムの安全性に対する社会的な意識・要求の高まりに十分答えているとは言い難い．緊急処理の中での操作者のミスの可能性などを考慮しても，物理量が制御レンジから逸脱すること自体，低頻度であることが安全上望ましい．異常を検出してからだけでなく，それより以前の，異常を検出する前の早い段階からの安全対策の重要性も広く認識されるようになった．

(2) 国際安全規格の重要性の増大と日本の対応の遅れ

安全性を定量的に評価する上できわめて重要となる IEC 61508 は，International Electrotechnical Commission（IEC）が 1998-2000 年に各部ごとに順次発行した安全性に関する国際規格で，電気/電子/プログラマブル電子技術を用いた安全関連系，いわゆる「安全装置」の性能を確率的に評価することを要求する．その適用範囲はプロセス産業，機械製造業，交通運輸，医療機器など，きわめて広範に及び，欧米を中心にすでに認証が行われている．最近，（輸出先の国/地域の規則に基づき）日本から輸出するプラントの安全計装に関して IEC 61508 への対応が要求されるケースが増えている．システムの安全性評価の枠組みをはじめて体系的に示した IEC 61508 が，貿易の際に世界共通の「よりどころ」として用いられるのは当然であり，そのようなケースが(IEC 加盟国に限らず)世界中で今後も増えていくことは確実である．したがって，IEC 61508 に限らず国際規格への対応の不備・遅れは国際競争力の低下につながることを覚悟しなければならない．

このように，今後その重要性は飛躍的に増大することが確実な国際規格であるが，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 IEC 61508 などのきわめて重要な国際規格への対応が遅れていると言わざるを得ない．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．研究の目的

システムの安全性に対する社会的な意識の向上に伴い，昨今では，異常を検出する前の早い段階からの安全対策の重要性も広く認識されるようになってきた．今後はその具体的内容が問われるが，日常生活のあらゆるところに存在する制御システム，さらには制御工学・技術ではそのような意識に基づく議論はまだ十分なされていない．すなわち，制御デバイス故障，プラント破損などの初期事象からレンジ逸脱に至る過程の定量的解析とその評価に基づく対策に関して，これまで体系的議論は行われていない．

制御工学・技術において，レンジ逸脱以前の段階での安全対策の中心となるのは制御則である．本研究では，IEC 61508 など近年産業界で特に重要性を増している国際規格に準拠した形で，制御則というソフトウエアのレベルで制御レンジからの逸脱対策という高度かつ実際的な安全機能を考える．そして，その安全機能を評価・実現する新しい技術を安全性，制御の両分野の境界領域に確立することを目的とする．この日本発の新技術により，従来の安全計装の枠を超えてそれを補完する新しい安全対策の可能性を提示することができる．特に近年注目されている，従来の安全計装の手法では安全性確保が困難な環境関連の事例への適用可能性を探るという意味でも非常に大きな意義がある．

また，国際規格で大きな課題となっているソフトウエアの安全性評価・管理の一つの方向性を示して，日本が世界に対して大きな貢献をすることも目的である．

さらに，その日本発の新技術は，制御工学・技術にとっては新しい方向性を示すことになるのは言うまでもない．安全性の分野からしても，従来にない全く新しい安全性確保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，安全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しい技術であり，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．研究の方法

(1) 制御レンジ逸脱に対する安全機能の明確化

制御レンジからの逸脱に対する安全機能を考える上では，安全性と信頼性の区別が不可欠である．システムの信頼性(正確には，ディペンダビリティ)の観点では，システムが制御デバイスの故障を内包する「状態」に陥っても，その機能をどれだけ維持できるかが評価点であり，「状態」への対応が必要となる．それに対して，安全性の観点では，危険事象がどれだけ低頻度であるかが評価点であり，「事象」への対応が必要となる．

制御レンジからの逸脱は，制御デバイス故

障などの初期事象に起因する制御システムの不安定化・制御性能低下だけでなく，初期事象直後の過渡応答の乱れによっても生じる可能性がある．したがって，それに対する安全機能には，以下の両方が必要である．

(a) 制御システムの最低限の機能の維持
(b) 過渡応答の乱れという「事象」に対する対策

研究代表者は，平成 19-21 年度 基盤研究(C)(一般)「国際規格に準拠して安全性と制御性能のトレードオフのバランスをとる日本発の新技術」で，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（異常/故障検出を前提としない）対策を制御則の機能として実現した．その成果を上記(a)への対策という形で基礎とする．さらに，本研究では(b)のために過渡応答の乱れという「事象」の定量的指標を新たに導入する．それにより，制御レンジからの逸脱に対する安全機能の内容を定量的に規定する．

(2) 制御レンジ逸脱に対する安全性を評価する新技術

制御レンジからの逸脱に対する安全機能を，異常/故障検出を前提とする制御システムの外側の従来の安全措置を補完する安全対策として確立するには，(IEC 61508 などの国際規格に準拠した)従来の安全措置の評価と整合性のある評価の枠組みが不可欠である．すなわち，故障直後の制御レンジからの逸脱を低頻度化の効果を定量的に評価する必要がある．

制御則によっては，制御デバイス（センサやアクチュエータ）が故障すると，不安定化あるいは制御性能の低下により，あるいは故障の影響による過渡応答の乱れにより，制御レンジからの逸脱が発生する．そのときには制御システムの外側で待機している安全関連系に対して作動要求が発生するので，その頻度を考えることで制御則がどの程度デバイス故障の影響を吸収できるかという評価ができる．

ここで，注意しなければならないのは，故障直後の過渡応答の乱れの程度が故障発生時の状況にも依存する点である．想定する故障にとって，それが発生する際に過渡応答が大きく乱れて制御レンジからの逸脱が生じ得るようなまずい稼働状況を考え，その状況になっている確率を評価する必要がある．

解析手法としては，すべてのデバイスの正常/故障状況により制御システムがどのような状態にあるかをデバイスコンテキストとして表現する．それに加えて，故障率や MTTR（Mean Time To Restoration）といった各デバイスのデータが与えられれば，国際規格 IEC 61165 に準拠してマルコフ解析を行うことにより，作動要求頻度を求めることができる．作動要求頻度による評価は IEC 61508 の安全性評価にも直接的につながり，国際規格への準拠という点できわめて有効である．

(3) 制御レンジ逸脱に対する安全性を制御則により管理する新技術

(2)の安全性評価の意味で，与えられた安全目標を達成し，かつ，正常時制御性能がもっとも良好な制御則を求める技術を確立する．

故障直後の制御レンジからの逸脱を低頻度化するためには，ベースとなる「故障時安定性・制御性能の確保」のための設計（平成 19-21 年度の基盤研究(C)(一般)ですでに確立済み）と同時に，(1)で導入した故障直後の過渡応答の乱れの指標を抑制する制御則設計を行う必要がある．

なお，与えられた安全目標を達成する安全機能には膨大な数の可能性がある．そこで，平成 19-21 年度の基盤研究(C)(一般)で確立した 代表的安全機能（Representative Safety Functions）の概念を用いて，候補を実用的に絞り込むこととした．

(4) 研究成果を具現化するソフトウエアの開発

(2),(3)で得られる制御レンジからの逸脱に対する安全機能の評価する技術ならびにその安全機能を制御則で実現する技術をコンピュータ上で効率的に実現するためのソフトウエアを開発する．

(5) 研究成果の国際規格への反映

代表研究者が IEC 61508 の改定作業委員会，IEC TC56: Dependability などの国際規格関係者に対して，(1)-(4)の研究成果をアピールして，日本からの貢献を目指す．

４．研究成果

(1) 制御レンジ逸脱の定量的明確化

制御の分野で，制御システムの切替に起因する過渡応答の乱れを評価・抑制する研究にはいくつかあるが，ほとんどが制御器の意図的な切替を想定している．すなわち，既知の切替時刻にあわせて付加型の制御器を動作させ，過渡応答の乱れを抑制するため，いつ発生するか分からない故障による制御システムの切替わりを扱うことはできない．

そこで，本研究では，切替わり前後の外乱に対する応答を考慮した全時間における切替 L2 ゲインを過渡応答の乱れの指標とする．故障発生時刻は切替 L2 ゲインの値に影響しない．また，切替 L2 ゲインの値を与える「最悪な」外部入力は，その切替わりが発生する際の「最悪な状況」に対応している．すなわち，その状況で考えている制御デバイス故障が発生すると，評価出力がもっとも大きなエネルギーを持つ．したがって，切替 L2 ゲインの値をできるだけ小さく抑えるような制御則設計により，評価出力のエネルギーを抑制できる．その結果，間接的にではあるが，過渡応答の乱れを抑制することができる．

(2) 制御レンジ逸脱に対する安全性を評価する新技術の確立

（IEC 61508 などの国際規格に準拠した）従来の安全措置の評価と整合性のある安全性評価の枠組みとして，制御レンジからの逸脱の発生頻度，すなわち従来の安全措置への作動要求頻度を求める技術を確立した（図 1）．

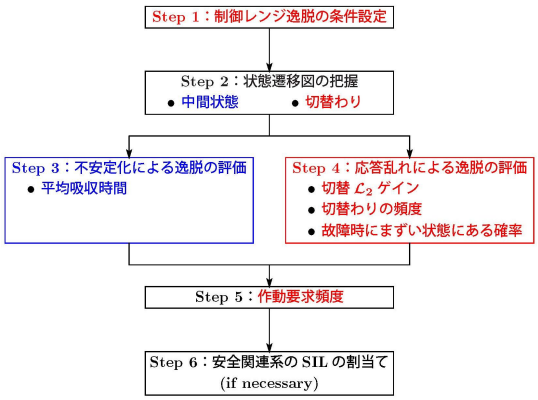

図 1　安全性評価の枠組み

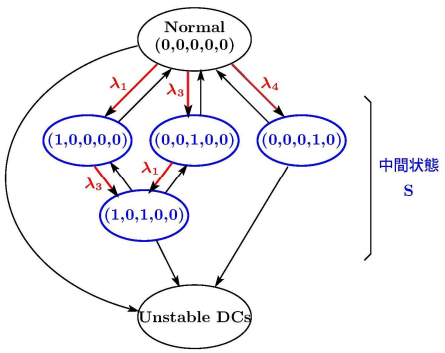

図 2　安全性評価での状態遷移図の例

制御レンジからの逸脱は，(a)制御デバイス故障などの初期事象に起因する制御システムの不安定化・制御性能低下だけでなく，(b)初期事象直後の過渡応答の乱れによっても生じる可能性がある．

まず，(a)による発生頻度は，図 1 の青色の部分で求めている．すなわち，図 2 の状態遷移図の例のように，制御システムの最低限の機能の維持されている故障状況（デバイスコンテキスト）を中間状態として抽出する（図 2 の青色の状態）．正常あるいは中間状態以外のデバイスコンテキストに初めて吸収されるまでの平均時間を吸収マルコフ解析で求めることで，(a)による発生頻度を求めることができる．

一方，(b)による発生頻度は，図 1 の赤色の部分で求めている．まず，中間状態への故障による遷移を「切替わり」として抽出する（図 2 の赤色の矢印）．個々の切替わりについて，切替 L2 ゲイン解析により，それが発生する際に過渡応答が大きく乱れて制御レンジからの逸脱が生じ得るようなまずい稼働状況を求め，さらに，稼働状況の全可能性の中でその状況になっている確率を求める．切替わり自体の発生頻度はマルコフ解析の中で得られるので，それとあわせることにより，個々の切替わりによる制御レンジからの逸脱の発生頻度が求められる．後は，すべての切替わりについて和をとればよい．

最終的に，制御レンジからの逸脱の発生頻度，すなわち従来の安全措置への作動要求頻度は(a)による発生頻度と(b)による発生頻度の和として得られる．このように状態遷移図上で，平均吸収時間と状態間遷移の発生頻度を結び付けて，制御レンジからの逸脱という一つの事象の発生頻度を求める手法は，連続時間マルコフ解析の中でもきわめて斬新である．

(3) 制御レンジ逸脱に対する安全性を制御則により管理する新技術の確立

国際安全規格 IEC 61508 にオーサライズされた形で，制御レンジ逸脱に対する安全性を制御則により管理する新しい技術を確立した．

図 3 に安全性管理例を示す．制御デバイス故障による制御システムの不安定化・制御性能低下を避けるディペンダビリティ機能だけを組み込んだ制御則では，黒線・青線の応答のように，制御レンジからの逸脱が生じる状況であっても，故障直後の過渡応答の乱れを抑制する安全機能を組み込んだ制御則であれば，赤線の応答のように，制御レンジからの逸脱は生じない．すなわち，制御レンジ逸脱の頻度を制御則によって低減しているのである．

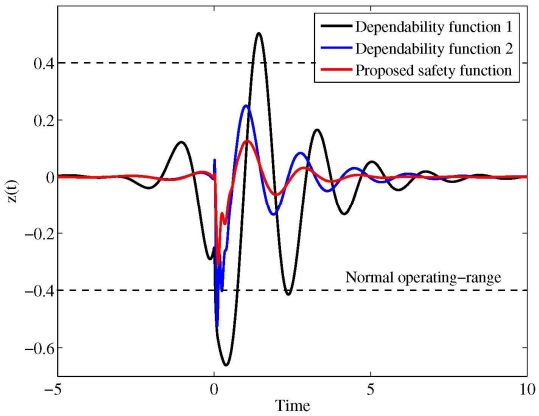

図 3　安全性管理例

従来の安全計装の現場では，また IEC 61508 など国際規格上も，制御システムの外側に安全関連系を必要なだけ取り付けることにより，システム全体としての安全性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，新技術は制御則というロジックのレベルの安全対策の可能性を広げ，従来からの安全対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い．そのため，この日本発の，日本が世界に冠たる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，制御則というロジック，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安全性評価・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．

(4) 新技術の実用化へ向けた研究

新技術の IEC 61508 への適用事例・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．

(5) 本研究を進める過程で得られた制御システムの安全性に関する新技術

安全性評価で用いた切替 L2 ゲイン解析に関連して，切替を伴う制御システムの安全性に非コヒーレント性が存在し得ることをはじめて明らかにし，あわせてその定量的な解析法も与えた．また，サーボ系などを念頭に置いたコントローラのリセットが安全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を確立した．新技術における安全性評価に用いているマルコフ解析の基礎的かつ実用的研究とともに，新技術の実用性の確立には不可欠な研究成果である．そのため，本研究の中心的な成果ではないものの，研究成果として位置づけられよう．

なお，以上(1)-(5)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．

(6) 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，特に制御工学・技術の分野では，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２８件）

① Koichi Suyama and Nobuko Kosugi, Controller reset strategy for anti-windup based on L2 gain analysis, Proceedings of the 39th Annual Conference of the IEEE Industrial Electronics Society, 査読有, 2013, pp.3443-3448, DOI: 10.1109/IECON.2013.6699682

② Koichi Suyama, Fault-tolerant servo systems against actuator failures using limited integrators, Proceedings of the 39th Annual Conference of the IEEE Industrial Electronics Society, 査読有, 2013, pp.3534-3540, DOI: 10.1109/IECON.2013.6699697

③ Noboru Sebe, Kohei Sumida, and Koichi Suyama, A design of fault-tolerant servo systems against sensor failures, Proceedings of the 2nd International Conference on Control and Fault-Tolerant Systems, 査読有, 2013, pp.208-215, DOI: 10.1109/SysTol.2013.6693947

④ Nobuko Kosugi and Koichi Suyama, Digital redesign of infinite-dimensional controllers based on numerical integration of new representation, Systems & Control Letters, 査読有, Vol.62, Issue 7, 2013, pp.531-538, DOI: 10.1016/j.sysconle.2013.03.007

⑤ Koichi Suyama and Noboru Sebe, Fault-tolerant servo systems against sensor failures using limited integrators, Proceedings of the 12th European Control Conference, 査読有, 2013, pp.3796-3802, DOI なし

⑥ 竹市正彦, 佐藤吉信, 陶山貢市 , 自動車用エアバックシステムの機能安全アセスメント, 自動車技術会論文集, 査読有, Vol.44, No.2, 2013, pp.627-633, DOI なし

⑦ Nobuko Kosugi and Koichi Suyama, Finite spectrum assignment of multi-input systems with non-commensurate delays, International Journal of Control, 査読有, Vol.85, Issue 9, 2012, pp.1197-1208, DOI: 10.1080/00207179.2012.679974

⑧ Koichi Suyama and Nobuko Kosugi,

Safety assessment of control laws using Markov analysis, Applied Mathematical Sciences, 査読有, Vol.6, No.95, 2012, pp.4737-4762, DOI なし

⑨ Nobuko Kosugi and Koichi Suyama, A new method for solving Bezout equations over 2-D polynomial matrices from delay systems, Systems & Control Letters, 査読有, Vol.61, Issue 6, 2012, pp.723-729, DOI: 10.1016/j.sysconle.2012.03.009

⑩ Noboru Sebe and Koichi Suyama, Fault-tolerant servo systems against actuator failures, Proceedings of the 7th IFAC Symposium on Robust Control Design, 査読有, 2012, pp.499-504, DOI:10.3182/20120620-3-DK-2025.00175

⑪ Koichi Suyama and Nobuko Kosugi, Non-coherence in safety dynamics against locking in switching control systems, Proceedings of the 37th Annual Conference of the IEEE Industrial Electronics Society, 査読有, 2011, pp.362-367, DOI: 10.1109/IECON.2011.6119345

⑫ Nobuko Kosugi and Koichi Suyama, Non-coherence in safety of switching control systems and its Markov analysis, International Journal of Control, 査読有, Vol.84, Issue 11, 2011, pp.1796-1806, DOI: 10.1080/00207179.2011.626456

⑬ Koichi Suyama and Nobuko Kosugi, Realization of safety function against deviations from normal operating-range in control laws, Proceedings of the 18th IFAC World Congress, 査読有, 2011, pp.5332-5340, DOI:10.3182/20110828-6-IT-1002.00387

⑭ Nobuko Kosugi and Koichi Suyama, New coprimeness over multivariable polynomial matrices and its application to control of delay systems, Systems & Control Letters, 査読有, Vol.60, Issue 6, 2011, pp.414-419, DOI: 10.1016/j.sysconle.2011.03.006

⑮ 陶山貢市, 瀬部昇, 制御レンジからの逸脱に対する制御則の安全性評価, 電子情報通信学会論文誌(A), 査読有, Vol.J94-A, No.5, 2011, pp.350-361, DOI なし

⑯ Noboru Sebe and Koichi Suyama, L2 gain analysis of linear systems with a single switching, International Journal of Robust and Nonlinear Control, 査読有, Vol.23, Issue 8, 2011, pp.827-837, DOI: 10.1002/rnc.1617

⑰ Koichi Suyama and Nobuko Kosugi, Safety function in control laws against deviations from normal operating-range, Proceedings of the 36th Annual Conference of the IEEE Industrial Electronics Society, 査読有, 2010, pp.211-218, DOI: 10.1109/IECON.2010.5675025

⑱ Koichi Suyama and Noboru Sebe, Probabilistic safety management of control laws against deviations from normal operating-range, Proceedings of the 1st International Conference on Control and Fault-Tolerant Systems, 査読有, 2010, pp.442-449, DOI: 10.1109/SYSTOL.2010.5676087

⑲ 陶山貢市, マルコフモデル技法の標準化について, 日本信頼性学会誌, 査読有, Vol.32, No.4, 2010, pp.252-260, DOI なし

⑳ 陶山貢市, 瀬部昇, 安全性を考慮して故障直後の過渡応答の乱れを抑制する制御系設計, システム制御情報学会論文誌, 査読有, Vol.23, No.4, 2010, pp.65-73, DOI: 10.5687/iscie.23.65

〔学会発表〕(計 4 件)

① 小谷田一詞, 陶山貢市, 佐藤吉信, 作動要求時平均機能失敗確率(PFD)算定のための平均フォールト時間について, 電子情報通信学会安全性研究会, 2013 年 9 月 26 日, 機械振興会館

② 竹市正彦, 佐藤吉信, 陶山貢市, 自動車用安全制御システムに関する機能安全アセスメント, 自動車技術会 2013 年春季大会学術講演会, 2013 年 5 月 24 日, パシフィコ横浜

③ 大山和也, 瀬部昇, 陶山貢市, ヘリコプターの数学モデルに対する耐故障性を有した制御系の設計と確率的安全性評価, 第 31 回計測自動制御学会九州支部学術講演会, 2012 年 12 月 8 日, 熊本大学工学部

④ 隅田紘平, 瀬部昇, 陶山貢市, センサにおける耐故障性を考慮したサーボ系の設計, 第 31 回計測自動制御学会九州支部学術講演会, 2012 年 12 月 8 日, 熊本大学工学部

６．研究組織

(1)研究代表者

陶山　貢市（SUYAMA, Koichi）

東京海洋大学・海洋科学技術研究科・教授

研究者番号：８０２２６６１２

(2)研究分担者

(　　)

研究者番号：