様式 C-19

科学研究費補助金研究成果報告書

平成２３年 ３ 月３１日現在

機関番号：１２６１４
研究種目：基盤研究（C）
研究期間：2007～2009
課題番号：１９５６０４３８
研究課題名（和文） 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
研究課題名（英文） New technology from Japan for well-balanced system design between safety and control performance according to international standards
研究代表者
陶山 貢市（SUYAMA KOICHI）
東京海洋大学・海洋工学部・教授
研究者番号：８０２２６６１２

研究成果の概要（和文）：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「安全性も重要な品質である．安全性と制御性能の間にはトレードオフがあり，バランスが重要」と広く認識されるようになってきた．本研究では，この漠然と意識されていたトレードオフの明確化を強く意識し，そのバランスを国際安全規格に準拠したオーサライズされた形で制御則というロジックでとる新しい技術を確立し，国際規格の分野での日本の世界に対する貢献とした．

研究成果の概要（英文）：Against the background where the social environment surrounding system safety has changed rapidly, it has been widely recognized that because there is a trade-off relation between safety and control performance, well-balanced system design is important. This research clarifies quantitatively such an intuitively-understood trade-off relation, and establishes a new technology for well-balanced system design between safety and control performance by control laws according to international safety standards. The new technology is one of important contributions to the world of international standards from Japan.

交付決定額

（金額単位：円）

	直接経費	間接経費	合 計
２００７年度	2,300,000	690,000	2,990,000
２００８年度	700,000	210,000	910,000
２００９年度	600,000	180,000	780,000
総 計	3,600,000	1,080,000	4,680,000

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，制御性能，トレードオフ，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要求の高まり

たとえば，「制御性能は落ちるが，ゆるやかに変化させれば，モータなどにかかる負担も小さく，より安全」という意識は様々な制御の現場などで従来から漠然と共有されている．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の中にもそのように設計されているものも多い．しかし，そのような意識があるにもかかわらず，制御性能（目標追従誤差や耐ノイズ特性など）を考慮するだけであるのが現状である．定量的な安全性評価がなされていなかったため，安全性と制

御性能の間に存在するトレードオフは見て見ぬふりをしてきたというのが実情であろう．すなわち，「安全性も重要な品質である」という昨今では広く認識されるようになってきたいわば当たり前のことも未だに当たり前のように扱われてはいないのである．

(2) 国際安全規格の重要性の増大と日本の対応の遅れ

品質としての安全性を定量的に評価する上できわめて重要なキーとなるIEC 61508 は，IEC (International Electrotechnical Commission) 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「安全性も重要な品質である．安全性と制御性能の間にはトレードオフがあり，そのバランスが重要」と広く認識されるようになってきた．今後はその理解の程度・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．何となれば，制御則を制御システムの安全設計に用いるという考え方自体，安全性は安全装置などの外付けの措置により確保するという現在の安全計装からしても，非常に斬新である．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．

本研究では，まず，この従来漠然と意識されていたトレードオフの定量的な明確化を行う．そして，近年，世界的にその重要性が増している国際安全規格 IEC 61508 に準拠した形で，すなわちオーサライズされた形で，その間のバランスを制御則というロジックのレベルでとるというまったく新しい技術を確立する．さらに，実用面を強く意識して，その設計・解析をコンピュータ上で効率的に行うための汎用的なソフトウエアを開発することも目的とした．

それは，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おり，将来は国際規格への反映も視野に入れて本研究を行った．

３．研究の方法

(1) 制御則の確率的安全性評価の枠組みの整備（安全性の分野）

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）がいくつか故障すると制御システム全体が不安定かつ危険な状況に陥る．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．

具体的には，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．

(2) 安全機能を有する制御則設計の枠組みの整備（制御の分野）

制御対象，考慮する制御性能指標(目標追

従性能や耐ノイズ特性などをH∞ノルムなどにより表現したもの)に加えて，要求される安全機能が与えられたとき，それを実現した上で制御性能指標を最適化する制御則を求める設計アルゴリズムを確立する．

(3) 安全性と制御性能の間のトレードオフの存在の定量的明示
(1),(2)を用いて，安全性と制御性能の間のトレードオフの存在を定量的に示す．解析的かつ一般的に示すことは困難であるため，第一歩としては，数値例で示す．

(4) 安全性と制御性能の間のバランスをとる制御則設計の枠組みの構築
作動要求頻度の目標値をクリアする制御則の中で制御性能指標を最適化することにより，安全性と制御性能の間のトレードオフのバランスをとる制御則設計の枠組みを構築する．その結果，安全性の分野での目標値が高ければ（低ければ）達成可能な制御性能は低くなる（高くなる）という，きわめて直観的に理解しやすいシステム設計が可能となる．

(5) 研究成果を具現化するソフトウエアの開発
(4)で得られる安全性と制御性能の間のトレードオフのバランスをとる制御則設計をコンピュータ上で効率的に行うためのソフトウエアを開発する．

(6) 研究成果の国際規格への反映
筆者がIEC 61508 の改定委員会，IEC TC56の会議などにおいて，(1)-(5)の研究成果をアピールして，国際規格への日本からの貢献を目指す．

４．研究成果

(1) 安全性と制御性能のトレードオフの定量的明示
数値例を用いて，安全性と制御性能の間に存在するトレードオフの関係をはじめて定量的に明確に示した．図１に示す．横軸は作動要求頻度の目標値で，左へ行くほど安全性が高い．縦軸は（実現できる最高の正常時の）制御性能指標値で，下へ行くほど制御性能が高い．故障時の制御性能に対する目標値に関して３通り（高い方から緑，赤，青）示されているが，いずれの場合にも，左肩上がり，すなわち，安全性が高ければ（低ければ）実現可能な制御性能は低くなる（高くなる）ことが分かる．
このようなトレードオフは従来は経験的にしか認識されていなかった．トレードオフのバランスをとる新技術の背景としてだけではなく，広くシステム工学・理論の観点からも，定量的に示されたことの意義は大きいと考えられる．

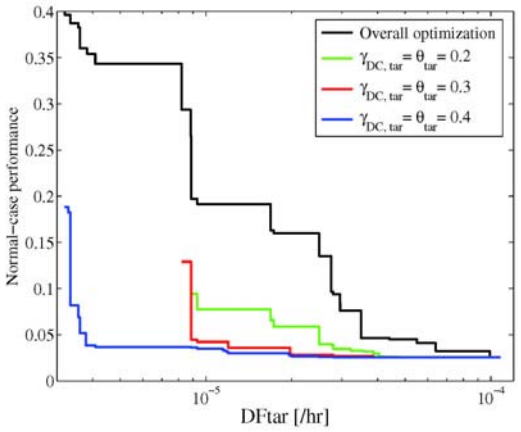

図１　安全性と制御性能のトレードオフ

(2) 安全性と制御性能のトレードオフのバランスをとる新技術
国際安全規格 IEC 61508 にオーサライズされた形で，安全性と制御性能の間のバランスを制御則というロジックのレベルでとる新しい技術を確立した．
従来の安全計装の現場では，また IEC 61508 など国際規格上も，制御系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，国際規格関係者の間で大いに注目されている．

(3) 新技術によるシステム設計の IEC 61508 との整合性に関する基礎的研究
新技術によるシステム設計は，安全度水準を中心とする IEC 61508 の確率的評価との間の整合性が，必ずしもよくなかった．そこで，IEC 61508 の確率的評価の中心である安全度水準，危険事象率などの算出法の整理・明確化などを，新技術によるシステム設計を視野に入れて行った．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．

(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，強制給排気式石油温風暖房機，右折衝突防止支援システム，ナイトビジョンシステム，車間距離警報システムなど，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．

なお，以上(1)-(4)の研究成果に関しては，2007 年 9 月東京・三田共用会議所で開催された IEC TC56: Dependability の全体会議や IEC 61508 の改訂作業委員会などにおいて，またメール審議などにおいても，国際規格関係者への情報提供を行っている．その結果，「品質としての安全性」,「ロジックによる安全性管理」に関するプロポーザルの前段階として，現状の制御ロジックまわりの安全機能を取り巻く問題点の解決のため，議論を進めている．

(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制御工学・技術の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カバーす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１９件）

① Noboru Sebe and Koichi Suyama, ` L2 gain analysis of linear systems with a single switching, International Journal of Robust and Nonlinear Control (published online in Wiley InterScience), 査読有, 2010, 11 pages

② 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，査読無，Vol.32，No.4，2010，pp.252-260

③ 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

④ 櫛引豪，陶山貢市，佐藤吉信，機械類の安全制御に関する国際規格の整合性について，日本信頼性学会誌，査読有，Vol.32，No.1，2010，pp.69-79

⑤ Koichi Suyama and Nobuko Kosugi , Probabilistic safety assessment and management of control laws based on strict Markov analysis, Proceedings of the 35th Annual Conference of the IEEE Industrial Electronics Society, 査読有, 2009, pp.1706-1711

⑥ Koichi Suyama , Trade-Off between Safety and Normal-Case Control Performance Based on Probabilistic Safety Management of Control Laws, Proceedings of the European Control Conference 2009 , 査読有 , 2009 , pp.2524-2529

⑦ 小杉のぶ子，陶山貢市，拡張優先ANDゲートの概念を応用した回復系のダイナミックフォールトツリー解析，電子情報通信学会論文誌，査読有，Vol.J92-A，No.9，2009，pp.613-623

⑧ 小杉のぶ子，陶山貢市，優先ANDゲートの拡張とその優先遷移ルールを用いたマルコフ解析，電子情報通信学会論文誌，査読有，Vol.J92-A，No.5，2009，pp.361-372

⑨ 陶山貢市，瀬部昇，正常時制御性能と安全性，故障時制御性能との間のバランスを考慮した制御系設計，システム制御情報学会論文誌，査読有，Vol.22，No.1，2009，pp.29-36

⑩ Koichi Suyama, Safety function in a control law and its assessment and management, Proceedings of the 2008 American Control Conference, 査読有, 2008, pp.4068-4074

⑪ Koichi Suyama, A General Framework of Safety Assessment for a Control Logic and Its Application to Balancing between Safety and Control Performance, Proceedings of the 9th International Conference on Probabilistic Safety

Assessment and Management, 査読有, 2008, 8 pages

⑫ Koichi Suyama and Nobuko Kosugi, Unavailability of a Redundant System with One Repair Team, Proceedings of the 9th International Conference on Probabilistic Safety Assessment and Management, 査読有, 2008, 8 pages

⑬ Hitoshi Muta, Koichi Suyama and Yoshinobu Sato, Functional Safety of Safety Related Systems with Safe Shutdown, Proceedings of the 9th International Conference on Probabilistic Safety Assessment and Management, 査読有, 2008, 6 pages

⑭ 陶山貢市, 瀬部昇, 安全性と制御性能のトレードオフを考慮した制御系設計, システム制御情報学会論文誌, 査読有, Vol.21, No.3, 2008, pp.89-99

⑮ 田辺安雄, 下平庸晴, 陶山貢市, 佐藤吉信, 事故シナリオの違いに基づく優先ANDゲートのタイプと出力特性解析, 日本信頼性学会誌, 査読有, Vol.30, No.2, 2008, pp.181-193

⑯ Tateki Nishi, Koichi Suyama and Yoshinobu Sato, Safety Analysis of Forced-draft-balanced Flue Stoves Being Oiled, Proceedings of Asia Pacific Symposium on Safety, 査読有, 2007, pp.203-206

⑰ Toru Oki, Koichi Suyama and Yoshinobu Sato, Formulation of Hazardous Event Rate for Imperfectly-Repaired Safety-Related Systems, Proceedings of Asia Pacific Symposium on Safety, 査読有, 2007, pp.252-255

⑱ Takeshi Kushibiki, Koichi Suyama and Yoshinobu Sato, Consistency between Principal Requirements in Machinery Safety Standards, Proceedings of Asia Pacific Symposium on Safety, 査読有, 2007, pp.449-452

⑲ Hideyuki Tanabe and Koichi Suyama, Multi-input multi-output robust model predictive control with pairs of process models, Proceedings of the 2007 IEEE International Symposium on Industrial Electronics, 査読有, 2007, pp.209-214

〔学会発表〕(計２６件)

① 井野孝, 順序依存故障論理をもつ非コヒーレントシステムのリスク解析, 電子情報通信学会安全性研究会, 2010年3月26日, 東京海洋大学海洋工学部

② 陶山貢市, 国際規格に準拠した制御ロジックの確率的安全性評価・管理の試み, 日本機械学会北陸信越支部特別講演会, 2010年1月22日, 信州大学工学部

③ 井野孝, 作動要求のみによって検出できるフォールトのある安全関連系における危険事象率の推定, 日本信頼性学会第17回春季信頼性シンポジウム, 2009年6月25日, 日本科学技術連盟千駄ヶ谷本部ビル

④ 牟田仁, 安全トリップのある安全関連系の機能安全について, 電子情報通信学会安全性研究会, 2009年5月22日, 東京海洋大学海洋工学部

⑤ 陶山貢市, 拡張優先ANDゲートの概念を応用したダイナミックFT解析, 電子情報通信学会信頼性研究会, 2008年12月12日, 東京・機械振興会館

⑥ 陶山貢市, 拡張優先ANDゲートのマルコフ解析における優先遷移ルール, 電子情報通信学会信頼性研究会, 2008年10月17日, 九州工業大学天神サテライトキャンパス

⑦ 瀬部昇, 切替が一回だけ生じる線形システムのL2ゲイン解析, 第37回制御理論シンポジウム, 2008年9月18日, 霧島いわさきホテル

⑧ 陶山貢市, 国際規格に準拠したソフトウエアの安全設計の現状とソフトウエアの定量的な安全性評価の試み, CDAJ CAE Solution Conference 2008, 2008年6月30日, パンパシフィック横浜ベイホテル東急

⑨ 陶山貢市, 優先ANDゲートの拡張とその定量的解析, 電子情報通信学会信頼性研究会, 2008年6月20日, 東京・機械振興会館

⑩ 牟田仁, 安全トリップのある安全関連系の機能安全について, 電子情報通信学会安全性研究会, 2007年12月14日, 東京・機械振興会館

⑪ 櫛引豪, 機械類の安全に関するISO/IEC規格群における主要な要求事項間の整合性, 日本信頼性学会第20回秋季信頼性シンポジウム, 2007年11月30日, 日本科学技術連盟千駄ヶ谷本部ビル

⑫ 西干機, 強制給排気式石油温風暖房機のFTA : フォールトツリーアナリシス, 電子情報通信学会安全性研究会, 2007年7月25日, 東京海洋大学海洋工学部

⑬ 西干機, 強制給排気式石油温風暖房機の安全解析, 第37回信頼性・保全性シンポジウム, 2007年7月17日, 国立オリンピック記念青少年総合センター

⑭ 小杉のぶ子, 単一チームにより修理される冗長システムのアンアベイラビリティ解析 － マルコフ解析の問題点とその解決, 電子情報通信学会信頼性研究会, 2007年6月22日, 東京・機械振興会館

６．研究組織

(1)研究代表者

陶山　貢市（SUYAMA KOICHI）
東京海洋大学・海洋工学部・教授
研究者番号：８０２２６６１２