物理的相似則に基づいた統合モデルによる
複合システムの安全設計支援

（研究課題番号 １３６８０５２０）

平成13年度～平成14年度科学研究費補助金（基盤研究(C)(2)）

研 究 成 果 報 告 書

平成15年３月

研究代表者 幸 田 武 久
（京都大学工学研究科助教授）

物理的相似則に基づいた統合モデルによる複合システムの安全設計支援

（研究課題番号 １３６８０５２０）

平成13年度～平成14年度科学研究費補助金（基盤研究(C)(2)）

研 究 成 果 報 告 書

平成15年３月

研究代表者 幸 田 武 久

（京都大学工学研究科助教授）

平成13年度～平成14年度科学研究費補助金（基盤研究(C)(2)）
研究成果報告書

課題番号　１３６８０５２０

研究課題　物理的相似則に基づいた統合モデルによる複合システムの安全設計支援

研究組織

研究代表者　幸　田　武　久（京都大学工学研究科助教授）
研究分担者　井　上　紘　一（京都大学工学研究科教授）
研究協力者　西　見　英　之（京都大学工学部学生）
研究協力者　下　谷　篤　史（京都大学工学部学生）

研究経費

平成13年度　１，９００千円
平成14年度　１，５００千円
計　　３，４００千円

研究発表

（１）学会誌等

・ Takehisa Kohda, Michio Yoshida, and Koichi Inoue: Failure Diagnosis Procedure Based on System Behavior Model, Safety & Reliability (Ed. by E. Zio, M. Demichela, N. Piccinni), 2001, Vol. 1, pp. 1-8.
・ 幸田武久、井上紘一：ヒューマンインタフェース技術とシステム安全・信頼性設計、ヒューマンインタフェースシンポジウム2001論文集, 2001、pp. 539-540.
・ Takehisa Kohda, and Koichi Inoue: Design of Failure Diagnosis System Based on System Bond Graphs, Proc. ESS2001, 2001, pp. 780-782.
・ 幸田武久、井上紘一：統合システム挙動モデルに基づくシステム安全対策の構築、第34回安全工学研究会発表講演予稿集, 2001、pp. 129-132.
・ Takehisa Kohda, and Koichi Inoue: Safety Design of Complex Systems Using Global System State Equations, Proc. Asia Pacific Symposium on Safety APSS2001, 2001, Vol. 1, pp. 79-82.
・ Takehisa Kohda, and Koichi Inoue: Probability Evaluation of System Failure Occurrence Based on Minimal Cut-Sets, 2002 Proc. - Annual Reliability and Maintainability Symp., 2002, pp. 190-194.

- 幸田武久、井上紘一：システム安全設計について、第６回「信頼性とシステム安全学」予稿集、2002、pp. 70(1)-(4).
- Takehisa Kohda, and Koichi Inoue: System Failure Occurrence Conditions Considering Protection and Latency, Proc. lm13-ESREL2002 European Conference, 2002, pp. 325-329.
- Takehisa Kohda, and Koichi Inoue: Risk-Based Design of Safety Actions for Potential Accident Causes Based on System Behavior Model, Probabilistic Safety Assessment and Management (PSAM6) (Ed. by E. J. Bonano et al.), 2002, Vol. 1, pp. 791-796.
- 幸田武久、西見英之、井上紘一：ミニマルカットセットを用いたシステム故障発生確率の評価について、第35回安全工学研究会発表講演予稿集、 2002、pp. 49-52.
- 下谷篤史、幸田武久、井上紘一：ベィジアンネットワークを用いた診断システムの構築、第７回「信頼性とシステム安全学」予稿集、2003、pp. 62-69.

（２）口頭発表

- 幸田武久、井上紘一：ヒューマンインタフェース技術とシステム安全・信頼性設計、ヒューマンインタフェースシンポジウム2001, 2001年10月3日.
- 幸田武久、井上紘一：統合システム挙動モデルに基づくシステム安全対策の構築、第34回安全工学研究発表会, 2001年11月27日.
- Takehisa Kohda, and Koichi Inoue: Safety Design of Complex Systems Using Global System State Equations, Asia Pacific Symposium on Safety APSS2001, November 28, 2001.
- Takehisa Kohda, and Koichi Inoue: Probability Evaluation of System Failure Occurrence Based on Minimal Cut-Sets, Annual Reliability and Maintainability Symp., January 23, 2002.
- 幸田武久、井上紘一：システム安全設計について、電気通信大学大学院情報システム学シンポジウム第６回「信頼性とシステム安全学」、2002年2月27日.
- Takehisa Kohda, and Koichi Inoue: System Failure Occurrence Conditions Considering Protection and Latency, lm13-ESREL2002 European Conference, March 20, 2002.
- Takehisa Kohda and Koichi Inoue: Risk-Based Design of Safety Actions for Potential Accident Causes Based on System Behavior Model, Probabilistic Safety Assessment and Management (PSAM6), June 25, 2002.
- 幸田武久、西見英之、井上紘一：ミニマルカットセットを用いたシステム故障発生確率の評価について、第35回安全工学研究会発表講演予稿集、 2002年12月5日.
- 下谷篤史、幸田武久、井上紘一：ベィジアンネットワークを用いた診断システムの構築、第７回「信頼性とシステム安全学」、2003年2月28日.

研究成果の概要

原子力燃料施設での事故やロケットの発射失敗など、最新の先端技術を用いたシステムでも依然として事故が発生している。コンピュータ技術や通信技術の発展により生産性、性能や効率は飛躍的に

向上したが、安全性や信頼性の面では必ずしも向上したとはいえない。製造物責任法の施行とともにあらためて安全性や信頼性への要求が高まり、システムの設計段階から故障や異常の影響を検討することが必須となってきている。しかし、従来の設計では要求性能目標を満たすことが優先され、安全性や信頼性の検討は性能とは分離して行われ、その検討結果が設計に十分反映されるとはいえなかった。システムは一般的に電気系、機械系や油圧系など異なる系からなり、その性能は各分野ごとに個別の物理的挙動モデルに基づき解析される一方、故障解析や安全性解析では全体システムの機能関係モデルーシステム機能とその達成のために必要な要素機能との論理関係―に基づいて故障要因の導出とその影響評価が行われた。システムの安全性を確保するためには、各分野の想定現象を統合したシステムモデルに基づいて故障解析や安全性評価を設計段階で行うことが必須である。本研究は、電気系、機械系や流体系などの異なる系からなる複合システムに対して、物理的相似則に基づく統合モデルによるシステム安全設計支援方法の確立を目的とする。

研究計画の初年度である平成13年度は、システム安全設計を検討する際に必須となるシステム事故の原因を導出する方法ならびに、想定される要素故障を検出するためのセンサ配置とその診断方法について検討を行った。

システム故障を生じる原因としては、システムを構成するハードウェア、ソフトウェアならびに人間行動を考慮する必要がある。基本的にはハードウェアの挙動は物理的法則に従うが、ソフトウェアや人間行動はこれらに拘束されることない。そこで、前者に対しては電気系、機械系、油圧系などをエネルギー流の観点から統一的に表現できるボンドグラフにより表現し、その各要素の特性を変化させる入出力関係の連鎖としてソフトウェアや人間の行動を表現して、統合システムモデル表現を構築し、それを基にしてシステム事故を生じうる因果系列を導出する。システムの防護系の効果を考慮して、システム事故の発生条件を導出する方法を提案し、簡単な化学プロセスの要素に応用し、その有効性を確認した。

また、要素故障の時間順序を考慮したシステム故障発生確率の簡単な評価方法を提案し、故障確率の評価手法であるマルコフ解析と比較してその有効性を検証した。また、システム安全設計の一つとして、ボンドグラフで表現された複合システムにおいて検出すべき要素故障を同定するために必要な検出点（観測点）の設定法、ならびに観測点の検査順序法を導出した。ボンドグラフから得られるシステム状態方程式を基にして、要素故障同定に必要な観測点の最小組み合わせを求め、その観測点の検査順序は診断過程における曖昧度を表す情報エントロピーを最小にする決定法を導出した。簡単な複合システムに適用してその有効性を確認した。

研究計画の第２年度である平成14年度は、前年度に提案した定性的解析方法による解析支援方法に対してさらに定量的な評価方法を検討することにより安全設計支援システムの枠組みを完成し、簡単な事例解析を通して解析方法の総合評価を行った。また、システム挙動モデルと故障遷移モデルからなる統合システムモデルの枠組みを利用した診断方法として、ダイナミックベィジアンネットの有効性を検討した。

安全監視システムなどの多層防御がシステム安全設計の基本であり、そのためには対策を立てるべき異常事象を同定し、その損失を評価することが重要である。前年度に提案した解析方法を適用することにより、設計対象であるシステム異常を発生させる潜在的異常伝播系列を導出し、その発生頻度を評価して許容できるかどうかを検討する。許容できなければ、異常伝播系列を防止できる防御系を同定して現状の防御におけるリスクを評価する。リスクが許容できなければ、さらに安全対策を検討してリスクの低減を図る枠組みを段階的な安全設計検討の支援枠組みとして検討した。簡単な化学プロセスの蒸留塔の事故系列を導出し、設置されている安全装置の故障によるシステム事故発生条件を導出し、その事故発生系列の発生条件を導出して、解析枠組みの妥当性を確認した。

システム異常を検出して事故を未然に防止するためには、故障診断は重要な役割を担う。そこで、システムの物理的挙動を表すシステム挙動モデルと、システム故障や要素故障の時間的な遷移を表す確率モデルを統合したダイナミックベィジアンネットを用いることにより、システム状態変数の推定ならびに異常状態の診断が簡単に行えることを確認した。

本研究を実施するにあたり、ご協力頂いた京都大学工学部学生、西見英之君ならびに下谷篤史君に感謝する。