報告番号	※甲　　第　　号

主　論　文　の　要　旨

論文題目　組込みシステムにおける状態遷移図に基づく安全分析手法

氏　　名　金周慧

論 文 内 容 の 要 旨

近年，飛行機や自動車などの組込み制御システムが複雑化する中で，従来確保してきた安全性を維持・向上することが求められている．システムの安全性を確保するためには，システムの安全性を損なう故障とその要因を抽出する安全分析が重要である．さらに，深刻な危害をもたらす逸脱に対しては，仕様策定や設計の段階で安全性を確保するか，システムに安全機能を追加して危害の深刻度を許容可能なレベルまで低下させる必要がある．システムのより高い安全性を確保する上では，故障の要因となるあらゆるハザードを本質安全により取り除くことが望ましいが，一般的に，多くの組込みシステムでは，利用状況の幅広さやコスト制約の観点から，本質安全を実現することは困難な場合がある．そのため，一部のハザードに対しては，機能安全により安全性を確保する必要がある．機能安全に関する国際規格としては IEC61508（2000 年）と ISO26262（2011 年）が策定され，特に高い安全性を要求される原子力発電所や工業プラントなどのシステム設計においては，機能安全の考え方が早期に取り入れられ，普及が進んでいる．

従来の組込みシステムにおいては，システムの安全を左右する安全関連システムにソフトウェアが含まれていない場合や，含まれていても小規模である場合が多く，その安全分析は比較的容易であった．それに対して，飛行機や自動車などの組込みシステムでは，特にソフトウェアの大規模化が顕著になっていることから，ソフトウェアに対する安全分析において，ソフトウェアの不具合と，ハードウェア故障によるソフトウェア動作への影響を，網羅的に列挙することは困難な状況にある．
それにも関わらず，ソフトウェアに対する安全分析手法が十分に確立していないのが現状である．

経済産業省の調査（2010 年）では，組込みシステム開発の約 8 割のプロジェクトに，状態遷移図と状態遷移表が用いられている．状態遷移を対象にした安全分析手法を用いると，多くの組込みシステムの分析に適用できることに加えて，分析の専門家以外の技術者も安全分析に参加し易くなるという利点がある．

本論文では，状態遷移図を用いてモデル化された組込みシステムの安全分析を行うため，状態遷移図に着目した安全分析手法を提案する．単一の状態遷移図に基づく安全分析手法は，状態遷移図の逸脱をより容易に列挙するためのガイドワードを提案する．小規模な組込みシステムに，単一の状態遷移図に基づく安全分析手法を適用し，従来多く用いられた分析手法 FMEA（Failure Mode and Effect Analysis）と比較する．しかし，複雑なシステムでは，１つの状態遷移図の状態数が多くなる場合，または状態遷移図が多階層になる場合もある．また，２つ以上の状態遷移図が並列に動作する場合は，単一の状態遷移図に基づく安全分析手法を適用し難いという問題がある．これらの問題を改善するため，階層型状態遷移図に基づく安全分析手法と並列型状態遷移図に基づく安全分析手法を提案する．また，より多くの組込みシステムの設計者が利用できるように，安全分析する過程と安全分析結果について述べる．

本論文の具体的な内容は，次の３つである．

１つ目に，状態遷移図を用いてモデル化された組込みシステムの安全分析をより容易に行うため，状態遷移図の逸脱を列挙するためのガイドワードを提案し，単一の状態遷移図に基づく安全分析手法 SASTD（Safety Analysis method based on a State Transition Diagram）を提案する．状態遷移図に対する逸脱の分析を，システム状態に対する分析と，状態遷移に対する分析の２段階で逸脱を分析する．分析を２段階に分ける理由は，システムがある状態に留まっている状況と，イベントが発生した際にシステムが取りうる振る舞いとで逸脱の性質が異なるため，異なる視点から逸脱を分析する必要があるからである．分析者が逸脱を列挙することを補助するために，各段階で使用するガイドワードと属性を提案する．状態遷移図に適用できるガイドワードを用いることで，組込みシステムの設計段階で，すべての故障を把握することが難しい状況においても，より網羅的に逸脱を分析できる．また，これらのガイドワードを用いることで，ソフトウェアのように，分析対象の逸脱が分かり難い場合でも，より網羅的に逸脱を列挙することができる．逸脱により発生する危害の深刻度を分析した結果，許容できない深刻な危害をもたらす逸脱が存在する場合には，その逸脱に対して，許容可能なレベルまで危害の深刻度を低減する対策を検討する．SASTD と FMEA の安全分析した結果を比較し，単一の状態遷移図に基づく安全分析手法がより網羅的に分析できることを明らかにする．

２つ目に，１つの状態遷移図の状態数が多くなる場合または状態遷移図が多階層になる場合の安全分析を行うため，SASTD を拡張した，階層型状態遷移図を対象とした安全分析手法 SAHSTD（Safety Analysis method based on Hierarchical State Transition Diagram）を提案する．SAHSTD は，階層型の状態遷移図に記述された，各状態で満たすべき性質と，状態が遷移する際に実行される処理に対して，それらが正常に満たされない，もしくは実行されないという逸脱を，ガイドワードを用いてより網羅的に列挙する手法である．階層型状態遷移図の上位と下位に分けて分析することにより，１つの状態遷移図に含まれる状態遷移する数を減らすことができる．その結果，SASTD に比べて，より容易に安全分析ができる．SAHSTD の適用性を確認するため，小規模なシステム仕様に対して SAHSTD を適用し，SASTD と安全分析した結果を比較し，SAHSTD が SASTD より容易に分析できることを明らかにする．

３つ目に，状態遷移図が並列に動作する場合の安全分析を行うため，SASTD を拡張した，並列型状態遷移図を対象とした安全分析手法 SAPSTD を提案する．SAPSTD（Safety Analysis method based on Parallel State Transition Diagram）は，並列型の状態遷移図に記述された，各状態で満たすべき性質と，状態が遷移する際に実行される処理に対して，それら

が正常に満たされない，もしくは実行されないという逸脱を，ガイドワードを用いてより網羅的に列挙する手法である．並列型状態遷移図の分析シートにおいて，直交する状態遷移図の状態／状態遷移の分析項目に並列に動作する状態と状態遷移を列挙することにより，並列に動作する状態と状態遷移を参照せずシステムが動作する際の影響を定められる場合は逸脱の分析数を減らすことができる．その結果，SASTD に比べて，並列に動作する状態遷移図をより容易に安全分析ができる．SAPSTD の適用性を確認するため，システム仕様に対して SASTD と SAPSTD を適用し，SASTD と安全分析した結果を比較し，SAPSTD が SASTD より並列に動作するシステムに対しては，容易に分析できることを明らかにする．

本研究では，組込みシステムを設計する際に，状態遷移図と状態遷移表を用いた設計が多いことから，状態遷移図に基づく安全分析手法を提案した．まず，単一の状態遷移図を対象とした安全分析手法 SASTD を提案した．次に，より複雑なシステムに適用するため，SASTD を拡張した分析手法，階層型状態遷移図の安全分析の場合は SAHSTD と並列型状態遷移図の安全分析の場合は SAPSTD を提案した．提案した手法の有効性を確認するため，小規模な組込みシステム(話題沸騰ポット)に適用し,SASTD より,拡張した安全分析手法(SAHSTD と SAPSTD) が有効であることを安全分析した結果から明らかにした．また，安全分析する過程と安全分析結果について述べているので，より多くの組込みシステムの設計者が安全分析する際に利用できると考えられる．これらの成果により，組込みシステムの安全分析をする際には，状態遷移図を作成し，小規模な組込みシステムでは SASTD を，大規模な組込みシステムは SAHSTD と SAPSTD を適用し，より効率的な安全分析手法として貢献できることを期待する．

学位関係