別表５
⑶

主　論　文　要　旨

No.1

報告番号	甲 乙 第　　号	氏　名	加藤　淳

主 論 文 題 名：

連携部分に着目した分割統治法および安全性プロパティ導出ルールを用いた
複雑な組込みシステムに対するモデル検査適用手法

（内容の要旨）

特定の機能を実現するために機械や機器に組み込まれるコンピュータシステム（組み込みシステム）において，その信頼性を向上させることは，安心・安全な社会を実現する上で重要な課題である．これは，近年，組込みシステムは，社会的なインフラストラクチャを始め，日常生活に深く浸透しており，その不具合が社会に大きな影響を与えるためである．一方，求められる機能が高度になることで，組込みシステムは複雑化している．その結果，放射線照射装置の事故，アリアン 5 の爆発事故など，社会に大きな影響を与える不具合が発生している．

複雑な組込みシステム（以降，システムという）の信頼性を向上させる技術として，形式手法の 1 つであるモデル検査が注目されている．モデル検査とは，仕様書などから抽出した検証対象の状態遷移が，検証対象として満たすべき性質（以降，プロパティという）を満足するか否かを，計算機により網羅的に検証する技術である．モデル検査を用いることにより，システム開発の早期の段階において，複雑な条件に起因する検証対象の不具合を検出することができる．このような複雑な条件に起因する不具合は，人手による検出が困難であるため，高い信頼性が求められるシステム開発において有用な技術である．

しかし，複雑なシステムに対するモデル検査の適用には，つぎに示す 2 つの課題がある．1 つ目の課題は，モデル検査が現実的な時間で終了しない状態爆発という現象がしばしば発生することである．複雑なシステムは，それを構成する複数の要素で構築される．システムの構成要素およびその連携部分を考慮してモデル検査を実施する場合，システムの構成要素のすべてを対象に,一括してモデル検査を実施する方法が考えられる．その際，モデル検査では，各構成要素におけるすべての変数の組み合わせを網羅的に検証するため，状態の組み合わせが膨大になる．

2 つ目の課題は，具体的な安全性プロパティの導出において，導出すべき安全性プロパティに見逃しが生じる可能性や，具体化が不十分になる可能性が生じることである．モデル検査を実施する際には，例えば「列車がロードユーザ（自動車や歩行者）と衝突する」など，高次な複雑さを有するシステムの望ましくない事象から，モデル検査への適用が可能な具体的な安全性プロパティを導出する必要がある．複雑なシステムは，考

慮すべき機能や条件が多く複雑であるため，具体的な安全性プロパティを系統立てて導出する必要がある．しかし，実際の導出は，モデル検査実施者の経験やスキルに基づくことが多い．

本研究では１つ目の課題を解決するために，システムの構成要素および構成要素の連携に関連する部分を，それぞれ個別にモデル検査する手法を提案する．連携に関連する仕様は，アーキテクチャ設計プロセスで作成するトレーサビリティマトリクスを用いて，構成要素の仕様書および構成要素間のインタフェースの仕様書から漏れなく抽出する．すべての構成要素に対して一括してモデル検査を実施するのではなく，構成要素および構成要素の連携部分に着目し，モデル検査を実施することで，状態爆発を回避する．本手法の評価実験において，状態爆発を発生させることなく，構成要素を組み合わせなければ発見できない不具合を検出することができた．

また２つ目の課題を解決するために，「Must Work Function（MWF）非起動」および「Must Not Work（MNWF）起動」の観点を用いて，モデル検査に適用可能な具体的な安全性プロパティを導出する手法を提案する．導出するプロパティの網羅性向上に寄与すると考えられる「MWF 非起動」および「MNWF 起動」の２つの観点を用いて，システムの望ましくない事象を具体化する．これらの観点に基づき，望ましくない事象の具体化を繰り返すことで，より具体的な事象を導出する．望ましくない事象の具体化の後，具体化した事象の否定（¬）を取ることで，具体的な安全性プロパティを導出する．本手法の評価実験において，導出する安全性プロパティの網羅性および具体性が向上することを確認した．

本研究で取り上げた２つの課題解決を通して，複雑な組込みシステムに対するモデル検査適用のハードルを下げることができた．それにより，モデル検査の研究領域の発展および産業界における組込みシステムの信頼性向上に貢献することができた．