Vol.2011-SE-171 No.25
2011/3/15

モデル検査における 安全性プロパティの系統的な導出手法

加藤淳† 狼嘉彰†

モデル検査を実施するにあたり検査対象システムとして満たすべき性質（プロパティ）を導出する必要がある．しかしプロパティの導出方法が確立されておらずプロパティの導出がモデル検査実施者の経験やスキルに依存して行われる．その結果，導出したプロパティが検証すべき性質を網羅しておらずモデル検査において検証漏れが生じる可能性がある．本論文ではプロパティのうち安全性プロパティに着目する．システム開発においてモデル検査を適用する際の安全性プロパティの系統的な導出手法を提案する．本提案手法では安全性・信頼性解析手法である Fault Tree Analysis（FTA）を適用し安全性プロパティを導出する．論理的な対称性を考慮し FTA を実施することで安全性プロパティにおける網羅性の向上を図る．産業用ロボット開発において本提案手法を適用した事例を示す．適用事例における安全性プロパティの網羅性の向上を確認することで本提案手法の有効性を示す．

A Systematic Method for Deriving Safety Properties in Model Checking

Atsushi Katoh† and Yoshiaki Ohkami†

When applying model checking, properties which a target system should satisfy must be derived. However, a method for deriving properties is not established. Deriving properties depends on experiences or skills of model checking conductors. Thus, there are some cases that properties to be derived are not exhaustive, and there is a possibility that verification by model checking is insufficient. This paper focuses on safety properties on model checking. It proposes a systematic method for deriving safety properties in applying model checking on the system development. In this method, safety properties are derived by adopting Fault Tree Analysis (FTA) which is a method for safety and reliability analysis. Improvement of exhaustiveness on safety properties is expected through conducting FTA by taking into account for logical symmetry. This method is applied in the development of industrial robot. Effectiveness of this method is demonstrated by confirming the improvement of exhaustiveness on safety properties in the case.

1. はじめに

近年，科学技術の進歩により電子機器システムや情報システムなどの技術システム（以降，システムという）は社会に深く浸透している．その一方で求められる機能の高度化や目的の異なる複数のシステムが結びつき新たなシステムを形成する system of systems の登場などによりシステムは複雑化の一途をたどっている．システムの複雑化によりシステムの不具合が多発し社会に大きな影響を与えている[1][2][3]．システム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．

システムの信頼性を向上させる技術としてモデル検査[4]が注目されている．モデル検査とは検査対象システムの状態遷移が検査対象システムとして満たすべき性質（以降，プロパティという）を満たすか否かを計算機により網羅的に検証する技術である．モデル検査に関するプロセスを図 1 に示す．モデル検査は次に示す 6 つの工程で構成される．

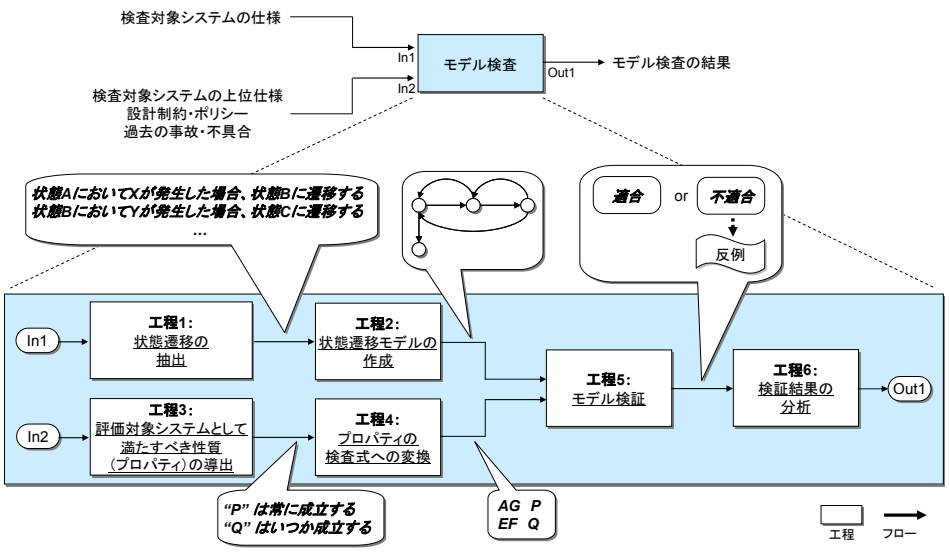

図 1 モデル検査のプロセス
Figure 1 Process of Model Checking

† 慶應義塾大学大学院システムデザイン・マネジメント研究科
Graduate School of System Design and Management, Keio University

工程 1. **状態遷移の抽出**：検査対象システムの仕様から検査対象システムの状態遷移を抽出する．

工程 2. **状態遷移モデルの作成**：適用するモデル検査ツールの表現形式に従い抽出した検査対象システムの状態遷移をモデル化する．

工程 3. **評価対象システムとして満たすべき性質（プロパティ）の導出**：検査対象システムの上位仕様，設計制約・ポリシー，過去の事故・不具合などから非形式的な形でプロパティを導出する．

工程 4. **プロパティの検査式への変換**：検査対象システムのプロパティを時相論理の表現形式に従い形式的な検査式に変換する．

工程 5 **モデル検証**：計算機上のモデル検査ツールに対してモデルと検査式を入力しモデル検証を実施する．

工程 6 **検証結果の分析**：モデルと検査式の適合結果を分析する．適合結果が不適合の場合，モデルにおいて検査式が成り立たない状態に至るまでの状態遷移が反例として出力される．反例を分析しモデルに誤りがない場合，モデルの基になった検査対象システムの仕様に誤りがあることを意味する．

モデル検査ではプロパティを導出し作成したモデルに対するモデル検証を実施する．プロパティに対するモデルの適合性をしらみつぶしに確認する．それにより人手では検出が困難な複雑な条件で発生する検査対象システムの問題点を検出することができる．

モデル検査を適用しシステムの信頼性の向上を図る際には工程 4.において正確な検査式を作成する必要がある．それに加え工程 3.において検査対象システムのプロパティを抜けなく導出することも重要である．工程 4.についてはプロパティの検査式への変換を系統的に実施する方法が提案されている[5]．しかし工程 3.については系統的な方法が確立されていない．そのためプロパティの導出がモデル検査実施者の経験やスキルに依存して行われる．その結果，導出したプロパティが本来検証されるべき性質を網羅しておらずモデル検査において検証漏れが生じる可能性がある．

そこで本論文ではプロパティのうち安全性プロパティに着目しシステム開発においてモデル検査を適用する際の安全性プロパティの系統的な導出手法を提案する．モデル検査におけるプロパティは安全性プロパティおよび活性プロパティに大別される[6]．安全性プロパティとは望ましくない状態に決して到達しない性質である．活性プロパティとは望ましい状態にいつかは到達する性質である．本論文において安全性プロパティに着目した理由は，検査対象システムとして望ましい状態と比べ望ましくない状態を定義することの方が一般に困難であり検証漏れが生じる可能性が高いためである．

本提案手法では検査対象システムのドメイン知識からシステムとして望ましくない状態を識別する．識別した望ましくない状態に対して安全性・信頼性解析手法である Fault Tree Analysis[7]（以降，FTA という）を適用する．それにより評価対象システムにおける安全性プロパティを系統的に導出し導出結果における網羅性の向上を図る．また本論文では産業用ロボット開発において本提案手法を適用した事例を示す．適用事例を基に本提案手法の有効性および課題を述べる．

本論文の構成は次の通りである．2 章において関連研究を述べる．3 章において提案手法を述べる．4 章において本提案手法の評価実験として産業用ロボット開発において本提案手法を適用した事例を述べる．5 章において本提案手法の有効性および課題を考察する．6 章において本論文をまとめる．

2. 関連研究

モデル検査におけるプロパティの関連研究として非形式的に表現されるプロパティを基に時相論理による正確な検査式を作成する Spec Pattern が提案されている[5]．Spec Pattern ではプロパティをスコープとパターンの 2 つの観点で捉える．スコープとは global（常に），before（～の前に），after（～の後に）など検査対象システムの時系列においてある状態やイベントが生じる範囲を定めたものである．パターンとは absence（ある状態やイベントが指定されたスコープ内で決して生じないこと），universality（ある状態やイベントが指定されたスコープ内で常に生じること），response（指定されたスコープ内で 1 つ目の状態やイベントの発生後に 2 つ目の状態・イベントが常に生じること）などスコープにおける状態やイベントの出現・順序形態を表したものである．Spec Pattern はパターンおよびスコープとそれらに対応する形式表現とのマッピングを提供している．Spec Pattern を用いることで時相論理体系に精通していない技術者であっても LTL や CTL などによる正確な検査式を作成することが期待できる．しかし Spec Pattern を適用する際の源泉となるプロパティそのものの導出方法は確立されていない．本論文ではプロパティのうち一般に導出が困難な安全性プロパティに着目しその系統的な導出方法を提案する．本提案手法により導出される安全性プロパティに対して Spec Pattern を適用することができる．このように本提案手法および Spec Pattern を組み合わせることでシステムの高信頼化に繋がる高品質なモデル検査を実施することが可能となる．

3. 提案手法

図 2 に安全性プロパティの導出プロセスを示す．安全性プロパティの導出プロセスは 1.望ましくない状態の識別，2.望ましくない状態の詳細化，3.安全性プロパティの生成の 3 つの工程で構成される．まずモデル検査の検査対象もしくは検査対象が属するシステムのドメイン知識を基に検査対象システムもしくはそれが属するシステムとして望ましくない状態を識別する．次に識別した望ましくない状態をモデル検査対象

の設計レベルまで詳細化する．そして詳細化された望ましくない状態を基に検査対象の安全性プロパティを生成する．

次にそれぞれの工程の詳細を述べる．

3.1 望ましくない状態の識別

システム開発におけるモデル検査の適用時に安全性プロパティを導出する場合，検査対象における望ましくない状態は検査対象の仕様書などに定義されない場合がほとんどである．例えば産業用ロボットの場合，望ましくない状態として「ロボットシステムが暴走する」が挙げられる．しかし産業用ロボットの仕様書には「ロボットシステムが暴走しないこと」とは明に定義されない場合がほとんどである．そこで検査対象もしくは検査対象が属するシステムのドメインにおける規格，公的機関や業界団体が発行するハンドブックなどから検査対象もしくはそれが属するシステムとして望ましくない状態を識別する．

3.2 望ましくない状態の詳細化

3.1 節で述べたドメイン知識から識別した望ましくない状態は通常システムレベルにおいて避けるべき状態である．検査対象の設計レベルと比べ抽象度が高い．ドメイン知識から識別した望ましくない状態を詳細化し検査対象レベルまで具体化された望ましくない状態を導出する必要がある．3.1 節で述べた産業用ロボットの場合，「ロボットシステムが暴走する」という状態に関する検査対象レベルの具体的な状態を抜けなく導出する必要がある．本提案手法では安全性・信頼性解析手法である FTA[7]を適用することで検査対象レベルの具体的な状態を抜けなく導出する．FTA とはシステムにおいて発生することが望ましくない事象を頂上事象として設定し頂上事象を発生させる事象を再帰的に解析しながら根本原因となる事象を網羅的に導出する解析手法である．FTA は 1960 年代に提案され安全性および信頼性に関する系統的な解析手法として確立されている技術である．産業用ロボットに対して FTA を実施した際の例を図 3 に示す．図 3 における二重線の四角ボックスは頂上事象を表す．単線の四角ボックスは頂上事象などから導出された中間事象を示す．白抜きの丸ボックスはそれ以上解析することができない（解析しない）末端事象を表す．網掛けの丸ボックスは解析の目的上それ以上の解析を必要としない末端事象を示す．いずれかの事象の発生が直上の事象を引き起こす場合は OR ゲートを用いて事象間の関係を表す．図 3 には示していないもののすべての事象の発生が直上の事象を引き起こす場合は AND ゲートを用いて事象間の関係を表す．

望ましくない状態の詳細化では，まずドメイン知識から識別した検査対象もしくは

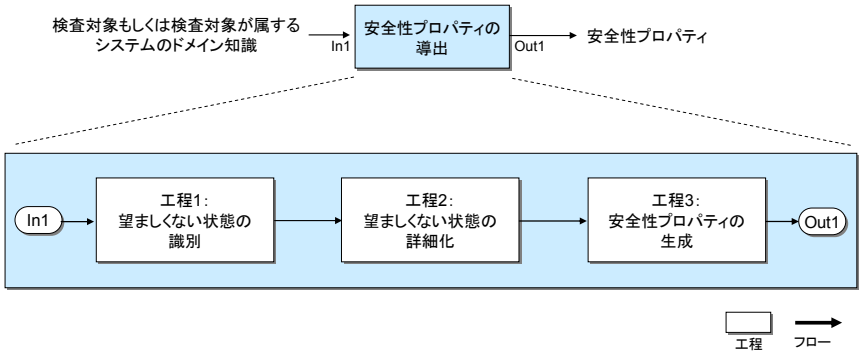

図 2　安全性プロパティの導出プロセス
Figure 2　Deriving Process of Safety Properties

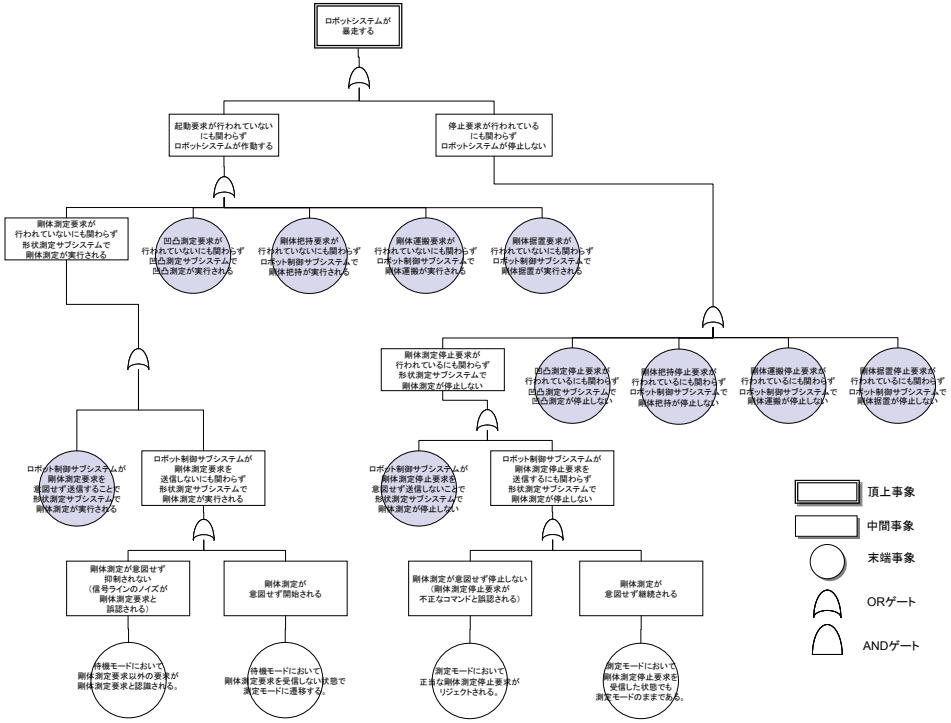

図 3　FTA
Figure 3　FTA

それが属するシステムとして望ましくない状態を FTA の頂上事象とする．次に頂上事象を引き起こす状態を再帰的に導出し Fault Tree を作成していく．再帰的な導出においては以下の 2 つの観点から Fault Tree の作成を進める．

1. 論理的な対称性

論理的な対称性とは図 3 の場合「起動要求が行われていないにも関わらずロボットシステムが作動する」および「停止要求が行われているにも関わらずロボットシステムが停止しない」の間の関係，「剛体測定が意図せず抑制されない」および「剛体測定要求が意図せず開始される」の間の関係などを指す．論理的な対称性を考慮することで導出する状態における網羅性の向上を図る．

2. システムを構成する要素

検査対象としてシステムの一部のみを対象とする場合，システムを構成する要素を考慮しながら要素ごとに望ましくない状態を詳細化する．それにより検査対象における望ましくない状態にスコープを絞る．図 3 ではモデル検査対象は産業用ロボットを構成する要素の 1 つである形状測定サブシステムである．その場合，産業用ロボットを構成するサブシステムに着目する．「起動要求が行われていないにも関わらずロボットシステムが作動する」をサブシステムごとに詳細化し形状測定サブシステムに関する状態を導出する．「停止要求が行われているにも関わらずロボットシステムが停止しない」の場合も同様である．

このような詳細化のプロセスを繰り返し末端事象として表される状態が検査対象の設計レベルでかつ前述した Spec Pattern におけるスコープおよびパターンの識別が可能になるまで FTA を実施する．図 3 におけるそれぞれの末端事象からは Spec Pattern におけるスコープとして global，パターンとして absence もしくは universality が識別される．

3.3 安全性プロパティの生成

3.2 節で導出した検査対象レベルにおける望ましくない状態に対しその否定をとることで安全性プロパティを生成する．図 3 の末端事象が表す状態「待機モードにおいてロッド測定要求以外の要求がロッド測定要求と認識される」の場合，その否定をとることで安全性プロパティ「待機モードにおいてロッド測定要求以外の要求がロッド測定要求と認識されないこと」を生成する．

4. 評価実験

本章では本提案手法の評価実験として産業用ロボット開発において本提案手法を適用した事例を示す．産業用ロボット開発においてモデル検査を適用する際の安全性プロパティについて，従来の経験・スキルに基づく導出結果と本提案手法による導出結果を比較する．従来方法に対する安全性プロパティの網羅性の向上を確認することで本提案手法の有効性を評価する．

4.1 適用事例

本提案手法の適用事例として我々が産業用ロボットメーカと共同で開発する不定形剛体運搬ロボットシステムを選定した．不定形剛体運搬ロボットシステムとは形状・寸法が一定ではない重量のある剛体の把持，運搬，据置を行う産業用ロボットである．不定形剛体運搬ロボットシステムの特徴は不定形剛体の把持および据置作業に対して強い自律性が求められる点である．システムにおいて剛体を把持する領域は限定されているものの，剛体の形状・寸法，剛体を把持する位置，剛体の姿勢は剛体ごとに変化する．システムは剛体を把持するにあたり形状・寸法，位置，姿勢を正確に知る必要がある．また剛体を据え置く領域は限定されているものの，その領域の中で剛体を据え置く位置が変化する．システムは剛体を据え置くにあたり他の剛体が存在しない位置もしくは剛体が敷き詰められた領域において最も標高が低い位置を正確に知る必要がある．

図 4 に不定形剛体運搬ロボットシステムの構成を示す．不定形剛体運搬ロボットシステムは形状測定サブシステム，凹凸測定サブシステム，ロボット制御サブシステムで構成される．形状測定サブシステムは不定形剛体の形状・寸法，位置，姿勢を測定する．凹凸測定サブシステムは剛体を据え置く領域の凹凸状況を測定する．ロボット制御サブシステムは形状測定サブシステムおよび凹凸測定サブシステムに対して測定

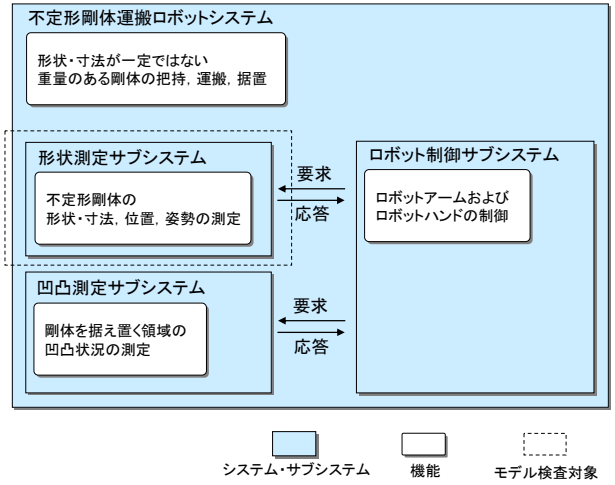

図 4　不定形剛体運搬ロボットシステム
Figure 4　Irregular-Rigid-Body Transport Robot System

などの要求を送信する．それぞれのサブシステムから応答として通知される測定結果を基にロボットアームおよびロボットハンドを制御し剛体の把持, 運搬, 据置を行う．

本システム開発では形状測定サブシステムの開発においてモデル検査を適用している．その理由は形状測定サブシステムには 3 次元形状を測定するレーザスキャナおよびレーザスキャナ上下動機構が搭載される．それらを制御する機能・処理が複雑なためである．

4.2 従来方法および提案手法の実施者

形状測定サブシステム開発におけるモデル検査の実施においてモデル検査に精通するエンジニアが従来の経験・スキルに基づく方法で安全性プロパティを導出する．一方で前述とは異なるエンジニアが本提案手法を適用し安全性プロパティを導出する．従来方法の実施者は実開発におけるモデル検査の適用経験が 10 年を超えるエンジニアである．本提案手法の実施者は実開発におけるモデル検査の適用経験が 5 年のエンジニアである．それぞれのエンジニアによる安全性プロパティの導出は同時期に行われたものの安全性プロパティに関する相互の情報交換はない．安全性プロパティの導出にあたりそれぞれのエンジニアは以下の開発文書を参照した．

- 不定形剛体運搬ロボットシステム仕様書
- 形状測定サブシステム仕様書
- ロボット制御サブシステムー形状測定サブシステム間インタフェース仕様書

4.3 従来方法による安全性プロパティの導出

従来の経験・スキルに基づく方法により導出した安全性プロパティを表 1 に示す．従来手法により 1 つの安全性プロパティを導出した．表 1 の安全性プロパティにおける測定モードとは剛体の形状を測定する際の制御モードである．待機モードとはロボット制御サブシステムからの要求を待つ際の制御モードである．剛体測定停止要求とは剛体の測定を停止する要求である．

4.4 提案手法による安全性プロパティの導出

4.4.1 望ましくない状態の識別

本提案手法を用いて安全性プロパティを導出するにあたり，モデル検査対象が属するシステムのドメイン知識からシステムとして望ましくない状態を識別する．形状測定サブシステムは産業用ロボットである不定形剛体運搬ロボットシステムの一部である．従って，文献8）を基に以下の不定形剛体運搬ロボットシステムとして望ましくない状態を識別した．

- ロボットシステムが暴走する
- ロボットシステムが動作しない

4.4.2 望ましくない状態の詳細化

FTA を用いて検査対象が属するシステムとして望ましくない状態を詳細化する．それにより検査対象レベルの望ましくない状態を導出する．形状測定サブシステムの場合，4.4.1 項で識別した不定形剛体運搬ロボットシステムとして望ましくない状態を頂上事象とする FTA を実施した．「ロボットシステムが暴走する」を頂上事象とする FTA を図 3 に示す．「ロボットシステムが動作しない」を頂上事象とする FTA を図 5 に示す．以降，図 5 を用いて望ましくない状態の詳細化を詳述する．論理的な対称性を考慮しながら頂上事象「ロボットシステムが動作しない」を「起動要求が行われているにも関わらずロボットシステムが作動しない」および「停止要求が行われていないにも関わらずロボットシステムが停止する」に詳細化した．検査対象である形状測定サ

表 1　従来方法により導出された安全性プロパティ
Table 1　Safety Properties by Traditional Method

No.	安全性プロパティ
1	測定モードにおいて剛体測定終了条件が満たされない状態で待機モードに遷移しないこと（剛体測定停止要求を受信した場合を除く）。

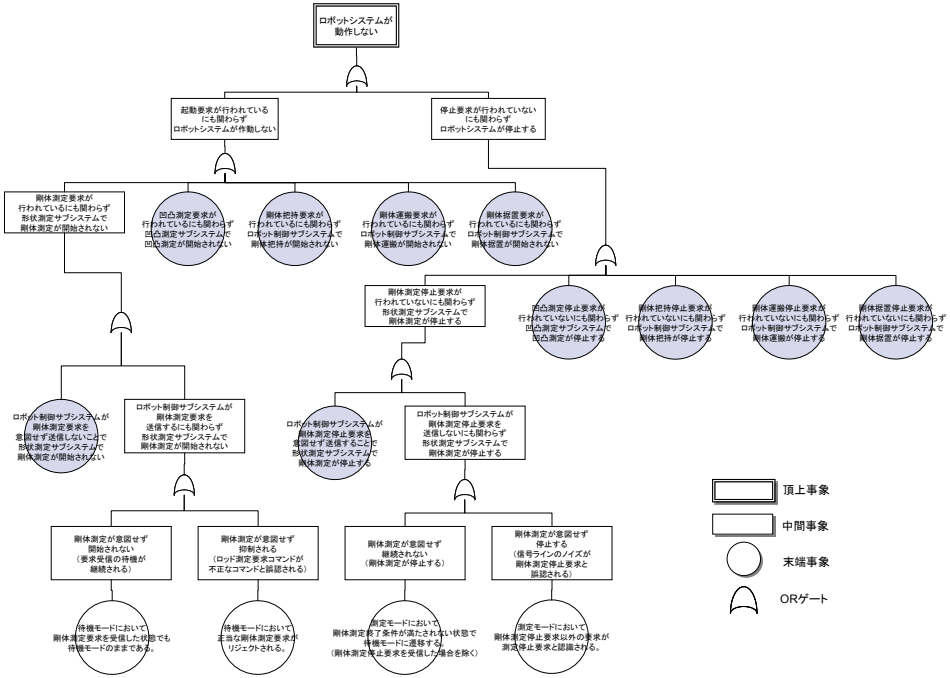

図 5　「ロボットシステムが動作しない」を頂上事象とする FTA
Figure 5　FTA on Top Event “Robot System Not Operate”

ブシステムとして望ましくない状態を導出するために「起動要求が行われているにも関わらずロボットシステムが作動しない」および「停止要求が行われていないにも関わらずロボットシステムが停止する」についてシステムを構成する要素であるサブシステムに着目し分解した．FTA の過程で導出した検査対象以外のサブシステムに関する状態については末端事象としそれ以上の解析は行わなかった．その後も論理的な対称性を考慮しながら形状測定サブシステムの設計レベルでかつ Spec Pattern におけるスコープおよびパターンの識別が可能になるまで状態を詳細化した．図 3 において頂上事象「ロボットシステムが暴走する」から導出した形状測定サブシステムとして望ましくない状態を以下に示す．剛体測定要求とは剛体を測定する要求である．

- 待機モードにおいて剛体測定要求以外の要求が剛体測定要求と認識される．
- 待機モードにおいて剛体測定要求を受信しない状態で測定モードに遷移する．
- 測定モードにおいて正当な剛体測定停止要求がリジェクトされる．
- 測定モードにおいて剛体測定停止要求を受信した状態でも測定モードのままである．

図 5 において頂上事象「ロボットシステムが動作しない」から導出した形状測定サブシステムとして望ましくない状態を以下に示す．

- 待機モードにおいて剛体測定要求を受信した状態でも待機モードのままである．
- 待機モードにおいて正当な剛体測定要求がリジェクトされる．
- 測定モードにおいて剛体測定終了条件が満たされない状態で待機モードに遷移する．（剛体測定停止要求を受信した場合を除く）
- 測定モードにおいて剛体測定停止要求以外の要求が測定停止要求と認識される．

4.4.3 安全性プロパティの生成

FTA により導出した検査対象レベルにおいて望ましくない状態について，その否定をとることで安全性プロパティを生成する．形状測定サブシステムの場合，4.4.2 項で導出した形状測定サブシステムとして望ましくない状態の否定をとることで安全性プロパティを導出した．本提案手法により導出した安全性プロパティを表 2 に示す．本提案手法により 8 つの安全性プロパティを導出した．

4.5 実験結果

不定形剛体運搬ロボットシステムにおける形状測定サブシステム開発のモデル検査適用時において従来方法および本提案手法により安全性プロパティを導出した．表 1 に示す従来方法による安全性プロパティおよび表 2 の No.7 に示す本提案手法による安全性プロパティは同一のプロパティであった．表 2 の No.1～No.6 および No.8 に示す通り，従来方法では識別できなかった安全性プロパティを本提案手法により導出することができた．これらの結果を踏まえると安全性プロパティの導出結果は以下の関係にある．

表 2　提案手法により導出された安全性プロパティ
Table 2　Safety Properties by Proposed Method

No.	安全性プロパティ
1	待機モードにおいて剛体測定要求以外の要求が剛体測定要求と認識されないこと。
2	待機モードにおいて剛体測定要求を受信しない状態で測定モードに遷移しないこと。
3	測定モードにおいて正当な剛体測定停止要求がリジェクトされないこと。
4	測定モードにおいて剛体測定停止要求を受信した状態で測定モードのままとならないこと。
5	待機モードにおいて剛体測定要求を受信した状態で待機モードのままとならないこと。
6	待機モードにおいて正当な剛体測定要求がリジェクトされないこと。
7	測定モードにおいて剛体測定終了条件が満たされない状態で待機モードに遷移しないこと（剛体測定停止要求を受信した場合を除く）。
8	測定モードにおいて剛体測定停止要求以外の要求が測定停止要求と認識されないこと。

従来方法による導出結果 ⊂ 本提案手法による導出結果

従って今回の評価実験から本提案手法を適用することにより安全性プロパティの網羅性が向上することを確認した．

5. 考察

本章では本提案手法の有効性を示す．また本提案手法の課題を述べる．

5.1 提案手法の有効性

4 章に示した適用事例の結果を基に本提案手法の有効性を示す．今回，不定形剛体運搬ロボットシステムという産業界の実例に対して本提案手法を適用した.その結果，従来方法で導出した安全性プロパティが本提案手法により導出した安全性プロパティに含まれることを確認した．また従来方法では導出できなかった安全性プロパティを本提案手法により導出することができた．従来手法および本提案手法の両方で導出した同一の安全性プロパティは図 5 における右から 2 番目の末端事象に対応する．その末端事象に対応する頂上事象は「ロボットシステムが動作しない」である．従来手法の実施者は経験・スキルに基づく導出の過程において産業用ロボットの望ましくない状態として「ロボットシステムが動作しない」のみを想定した可能性がある．一方で本提案手法では文献 8）の産業用ロボットの安全に関するハンドブックから産業用ロボットの望ましくない状態として「ロボットシステムが暴走する」および「ロボットシステムが動作しない」を識別した．ドメイン知識からの望ましくない状態の識別が

安全性プロパティの網羅性の向上に貢献していると考える．また本提案手法では安全性・信頼性に関する解析手法として既に確立されており頂上事象に結びつく事象を系統的に導出することが可能な FTA を適用している．さらに導出結果の網羅性を向上させるために論理的な対称性を考慮した FTA を実施している．FTA そのものが有する系統性および対称性という 2 値で状態を分解することによるカバレッジの確保についても安全性プロパティの網羅性の向上に貢献していると考える．

また FTA の過程においては Fault Tree を作成する．Fault Tree は安全性プロパティを導出する際の思考プロセスの可視化の結果である．安全性プロパティの導出過程を可視化することで本提案手法の実施者以外がその導出プロセスを評価することができる．要すれば導出プロセスおよび導出結果を追加・修正することもできる．それにより安全性プロパティの更なる網羅性の向上が期待できる．

5.2 課題

本論文 5.1 節において本提案手法の有効性を確認することができた．しかし本提案手法には解決すべき課題がある．本提案手法ではモデル検査の検査対象もしくは検査対象が属するシステムとして望ましくない状態を識別する．その際に望ましくない状態を抜けなく識別する方法が必要である．本提案手法では検査対象もしくは検査対象が属するシステムとして望ましくない状態を起点として安全性プロパティを導出する．望ましくない状態に抜けが生じた場合，導出する安全性プロパティにも抜けが生じてしまう．しかし今回の適用事例から本提案手法の「望ましくない状態の詳細化」を通して望ましくない状態の抜けを発見する可能性があることがわかった.「望ましくない状態の詳細化」の結果を「望ましくない状態の識別」にフィードバックし，それを繰り返すことで最終的な安全性プロパティが得られる可能性がある．

6. まとめ

本論文ではシステム開発においてモデル検査を適用する際の安全性プロパティの系統的な導出方法を提案した．産業事例に対して従来方法および本提案手法を適用し安全性プロパティを導出した．それぞれの導出結果を比較したところ従来方法により導出した安全性プロパティが本提案手法による安全性プロパティに含まれることを確認した．また，従来方法では導出できなかった安全性プロパティを本提案手法により導出することができた．従って本提案手法は安全性プロパティ導出における網羅性の向上に有効な技術であることを確認した．ただし本提案手法の課題として FTA の頂上事象とする望ましくない状態に関して網羅性の高い識別方法が確立されていないことを識別した．この課題を解決することで本提案手法の品質向上を図る．また本論文で対象外とした活性プロパティについて，その系統的な導出方法は明らかにされていない．活性プロパティの系統的な導出方法を明らかにすることでモデル検査における包括的なプロパティ導出手法の確立を目指す．

謝辞 本研究に協力頂いた有人宇宙システム株式会社の星野伸行氏に感謝する．また本論文の作成にあたり多くの助言を頂いた有人宇宙システム株式会社の川口真司氏に感謝する．

参考文献

1) Leveson, G. N.: SAFEWARE: SYSTEM SAFETY AND COMPUTERS, pp.515-553, Addison-Wesley(1995).
2) 清水久二：アリアン 5 の爆発事故とソフトウェア安全性に関する国際規格，安全工学会安全工学誌，Vol.41，No.1，pp.39-42（2002）.
3) 国土交通省：FDP システムの障害の原因調整の結果，国土交通省（オンライン），入手先 <http://www.mlit.go.jp/kisha/kisha03/12/120312_.html>（参照 2010-12-31）.
4) Clarke, M. E., Grumberg, O. and Long, E. D.: Model Checking and abstraction, ACM Transactions on Programming Languages and Systems, Vol.16, No.5, pp.1512-1542(1994).
5) Dwyer, B. M., Avrunin, S, G. and Corbett, C, J.: Pattern in Property Specification for Finite-State Verification, In Proceedings of the: 21th International Conference on Software Engineering, pp.411-420(1999).
6) Alpern, B. and Schneider, B. F.: Defining liveness, Information Processing Letters, Vol.21, No.4, pp.181-185(1985).
7) Leveson, G. N.: SAFEWARE: SYSTEM SAFETY AND COMPUTERS, pp.317-326, Addison-Wesley(1995).
8) 厚生労働省安全課編：産業用ロボットの安全管理, pp.161-322, 中央労働災害防止協会（2002）.