人と共存するロボットのための 安全関連システムのモデリングと形式手法による検証

中 坊 嘉 宏* 山 田 陽 滋*

Modeling and Verification of Safety Systems using Formal Methods for Human-Coexisting Robots

Yoshihiro Nakabo* and Yoji Yamada*

Verification of safety-related systems based on safety standards are important for realizing safe human-coexisting robots. We have proposed UML modeling and an object-oriented approach to develop safety-related systems which is categorized by an international safety standard of system safety. In this study, we presented the verification of safety-related systems including hardware, such as emergency stop systems including safety relays and safety switches, using the formal methods to verify their robustness against failures, which is encouraged to apply for software verification by an international safety standard of functional safety.

Key Words: Safety Category, UML Modeling, System Safety, Safety Standard, Formal Verification

1. は じ め に

近年、人と共存して働くロボットへの期待が高まっているが、その実用化のためには安全の問題を解決しなければならない。今後、社会に広く受け入れられるためには、国際安全規格などの社会的に合意された技術を適用することが重要である。本研究ではロボットを対象とする機械類の安全についての国際規格に基づき、安全関連システムと安全要件をそれぞれ抽象化し、形式化されたモデルを作成する方法を新たに提案する。また、このようにしてモデル化された安全関連システムが、同じくモデル化された安全要件、すなわち要求仕様を満たすかどうかの検証を、形式手法 (Formal Method) を用いて行うことを提案する。

具体的には、ISO13849:1999 [1] で示されるカテゴリ概念のモデル化を行い、実際の製品に用いられているロボットの緊急停止系の安全リレー回路を例として検証を試みた。またその検証方法として、IEC61508 [2] で推奨されている、ソフトウェアの安全性を保証するための形式手法を応用し、安全リレーのハードウェアの検証に適用してその有効性を確認した。これにより、対象となるシステムと要求仕様をモデル化することで、ハードウェアでも、ソフトウェア同様に、仕様に対する適合性が形式手法により検証できることが示された。

2. 人と共存するロボットの安全性

近年、次世代サービスロボットやセル生産ロボットなど、人と共存して働くロボットへの期待が高まっているが、実用化のためには安全の問題を解決しなければならない。安全技術が社会に受け入れられるには、国際安全規格など、広く合意のとれた技術を目指すことが重要である。

現在、社会で数多く用いられているロボットはほとんどが産業用であり、その安全については、機械類の安全に関する国際規格体系に示されている。一方、次世代サービスロボットについては、いまだ国際規格等は整備されていない。国内では、近年、国がとりまとめた次世代サービスロボットについてのガイドライン [3] を発表した。その技術的な内容については、現時点では産業用ロボットに適用される国内法を引用している。このことから、国内法と同様に、国際安全規格の適用についても産業用ロボットの規格を参照するのが適当と考えられる。

我々はこれまでに、国際安全規格の考え方を基に、人とロボットとの安全な作業空間の共有など、従来の産業用ロボットにはない複雑な安全制御について提案し、実用化研究を行ってきた。具体的には、これまで安全の分野では用いられていなかったオブジェクト指向と UML (Universal Modeling Language) を用いて、安全システムの設計や安全概念のモデル化 [4]、リスクアセスメントのモデル化 [5] を提案している。

本研究では、ロボットを対象とする機械類の安全についての国際規格に基づき、安全関連システムと安全要件のモデル化を行って、形式手法を用いて対象システムが要求仕様を満たしてい

原稿受付 2008 年 12 月 20 日

*独立行政法人産業技術総合研究所

*Advanced Industrial Science and Technology(AIST)

■ 本論文は提案性で評価されました。

るかどうかの検証を行った [6]。具体的には、システム安全規格の ISO13849:1999 [1] で示されるカテゴリの概念をモデル化し、実際に工場等で用いられている製品に組み込まれているロボットの緊急停止系の安全リレー回路を例として検証を試みた。また検証方法として、機能安全規格の IEC61508 [2] でソフトウェアの安全性を保証するために推奨されている形式検証を、安全リレー回路のハードウェアの検証に適用し、その有効性を確認した。

以下では、本研究で対象とした国際安全規格の概要を説明し、安全リレー回路のモデル化と形式検証の適用方法について詳細を説明する。また実際に検証を行った結果を示す。

2.1 安全関連システムの UML モデル

ロボットを含むシステム全体のなかで、安全性にかかわる部分を安全関連部と呼ぶ。安全関連部はリスクの大きさに応じた故障耐性が必要であり、システム安全規格 ISO13849:1999 のカテゴリで分類されている。各カテゴリごとの要求事項と耐故障性は次のようになる。

カテゴリ B 安全関連部が、適切な規格に従って安全機能を満たす。故障発生時に安全機能は失われる。

カテゴリ 1 カテゴリ B を満たす。高信頼の部品を用い、安全原則に従う。故障発生時に安全機能は失われるが、その確率はカテゴリ B よりも低い。

カテゴリ 2 カテゴリ B を満たし、安全原則に従う。適切な間隔で安全機能のチェックが行われる。故障はチェック時に発見されるが、チェックの間隔では安全機能が失われる。

カテゴリ 3 カテゴリ B を満たし、安全原則に従う。単一故障では安全機能が失われない。不具合はできる限り検出される。単一故障では安全機能は失われないが、検出されない不具合が蓄積した場合に安全機能が失われる。

カテゴリ 4 カテゴリ B を満たし、安全原則に従う。単一故障では安全機能が失われない。安全機能の動作時以前に不具合が検出される。単一故障では安全機能は失われず、また安全機能が失われないよう、安全機能が動作する前に故障が検出される。

本研究ではシステムの機能仕様を検証する手法を提案し、確率的な事象については扱わない。そこで、機能が同じカテゴリ B からカテゴリ 2 までを一般のシステムと呼び、カテゴリ 3 やカテゴリ 4 のシステムとの比較を行う。

我々が提案したオブジェクト指向に基づくモデル化 [4] では、**Fig. 1** に示すように、安全関連部を示す安全システムに加えて、危険事象、安全状態、故障の三つの概念をモデル化している。

すなわち危険事象が発生したときに、これを安全状態に移行させることが安全システムの機能と考え、安全システムに故障が起こった場合に安全機能が失われないかどうか、カテゴリごとのシステムの動作をモデル化して記述する。オブジェクト指向に基づいて危険事象や安全状態、故障などの概念をモデル化し、UML を用いて図示することで、対象の安全システムの機能と性能を分かりやすく示すことができる。

ところが、人と共存するロボットなどの複雑なシステムでは、例えモデル化できても、様々な故障のすべてに対処できるかどうか、さらには、それらを含むあらゆる入力・条件の組み合わ

Fig. 1 UML model of safety system

Fig. 2 Software development V model [2]

せについても安全要件を満たすかどうか、網羅的に検証するのは困難である。そこで本研究では、近年ソフトウェアの検証方法として注目されている形式手法の導入を提案する。

2.2 形式手法による検証

機能安全規格の IEC61508 にも示されるとおり、形式手法による検証は、ソフトウェアの安全性を検証する方法として近年注目されている。

一般にソフトウェアの不具合はハードウェアにおけるランダム故障と異なり、設計時や実装時に埋め込まれたバグが原因である。それらは決定論的原因故障と呼ばれ、これを防ぐためには設計開発のプロセスを適切に進めることが重要とされている。具体的には、**Fig. 2** に示すようなソフトウェア開発 V モデルと呼ばれる、仕様から設計、実装までの工程を、開発と検証を繰り返しながら進めるモデルが推奨されている [2]。形式手法は、そのなかでも最も厳密かつ確実な検証方法の一つとされており、特に安全性が必要なソフトウェアについて利用が義務付け、または推奨されている。

ここでソフトウェア以外について考えると、ハードウェアを含むシステム全体に対して、ランダム故障だけではなく、仕様から設計の工程においてアーキテクチャや構成方法に仕様や設計上のバグが存在しないかどうか、すなわち決定論的原因故障が存在しないかどうかを検証することは重要である。実際に、先行研究として鉄道のポイントや信号系の仕様適合性を検証した例 [7] や、航空機などにおける制御系の故障の検証 [8] など、形式手法が用いられている。本研究では、ハードウェアを含む

Fig. 3 System verification by testing

Fig. 4 System verification by formal method

ロボットの安全システムの検証に形式手法を用いることを提案する。

次に形式検証の概略について説明する。一般に、ソフトウェアを含むシステムの検証は、Fig. 3 に示すように、テストによる検証が用いられている。すなわち、まずテスト用の入力を作成してシミュレーションや実機テストで結果を出力し、あらかじめ用意しておいた期待値と照合することで検証を行う。この方法の問題点は、要求仕様に対応したテスト入力と期待出力を用意しなければならず、煩雑であること。また行ったテストで要求仕様がすべて網羅されているかどうか、判定するのが困難なことである。

一方、形式手法を用いた検証では、Fig. 4 に示すように、テスト入力や期待出力の代わりに、要求仕様そのものをモデル化し、システムのモデルが要求モデルを満たしているかどうかを数学的に証明する。証明方法には定理証明を用いる方法と全探索を行う方法があるが、検証の結果、あらゆる入力と状態の組み合わせに対して求める性質が成り立っているかどうかを厳密かつ網羅的に確かめることができる。また、もし対象システムが要求仕様を満たしていなかった場合には、そのときの入力とシステムの状態が反例として出力される。これによりソフトウェアのバグやシステムの不具合を容易に見つけることができる。

以上の方法は、いくつかの商用、またはフリーのモデリング・検証ツールで行うことができる。本研究では商用の SCADE ツール [9] を用いてモデリングと検証を行った。以下では、安全リレーを用いたロボットの緊急停止系について、具体的なモデリング方法と検証結果を示す。

3. 形式検証のための緊急停止系のモデル化

本研究では、安全リレーを用いた緊急停止系とその動作を検証する。緊急停止系を先に説明した安全システムの UML モデルに当てはめると、まず緊急停止ボタンを押すのが「危険事象」であり、これに応じて安全リレー回路からなる「安全システム」が出力を遮断してモータを停止させることができれば「安全状態」となる。一方、リレーやスイッチからなる安全システムには「故障」が適用されて、これを考慮しなければならない。以上の対象システムに対して、要求される安全機能を要求モデルとして適用し、あらゆる状態、入力のすべてに対してこれが常に満たされるかどうかを形式手法で網羅的に検証する。

Fig. 5 Rudder diagram of general emergency stop system

Fig. 6 Rudder diagram of Category 3 emergency stop system

Fig. 7 Rudder diagram of Category 4 emergency stop system

3.1 安全リレー回路とその動作

リレー回路は一般にラダー図で表すことができる。ロボットの緊急停止系として用いられるリレー構成を Fig. 5 に示す。緊急停止ボタン“Stop”を押すとリレー“R”がオフになり、モータ“M”への電源供給が遮断される。再起動ボタン“Restart”を押すと再起動し、稼働状態が自己保持される。

Fig. 5 の構成ではリレーが溶着するなどした場合、ロボットが停止できなくなる。すなわち、2.1 節で示したカテゴリ B からカテゴリ 2 までの一般のシステムにあたる。そこで、リレーを 2 重化することで、単一故障でも安全機能を失わないカテゴリ 3 のシステムが構成できる。これを Fig. 6 に示す。例えば、単一故障で“R1”の接点が溶着しても、“R2”の接点が作動するので安全機能は維持される。ただしその場合でも“R1”の溶着は検出されないで、単一故障の蓄積により“R2”も溶着した場合には安全機能が失われることになる。

さらに強制ガイド式接点リレーと呼ばれる、リレーの接点が、機械的に強制して、一致して動作する安全リレーを用いることで、溶着などが起こった場合に再起動できなくて単一故障の検知が可能なカテゴリ 4 のシステムが構成できる。これを Fig. 7 に示す。“R1”か“R2”の接点で溶着が起こると“R3”がオンにならず、再起動できないので安全である。

3.2 安全リレー回路と故障のモデル化

以上の回路を形式手法で検証する。まずラダーのラングごとに、回路を流れる電流の有無を論理の 1 と 0 に対応させる。すなわち接点が閉じれば電流が流れるので 1、接点が開けば 0 となる。これをもとに回路を構成するリレーとスイッチをそれぞれモデル化し、同時に、故障の有無と、故障モードとをそれぞれ

Fig. 8 Model of push-button switch for emergency stop

Fig. 9 Safety relay circuit model

Fig. 10 Model of a single failure

れモデル化する。

3.2.1 緊急停止用押しボタンスイッチのモデル

緊急停止用押しボタンスイッチのモデルを **Fig. 8** に示す。緊急停止用押しボタンスイッチでは、ボタンを押すことにより2個の接点が同時に動作する。それぞれの接点は、オンかオフで固定する故障モードを持つ。

3.2.2 安全リレーのモデル

安全リレーのモデルを **Fig. 9** に示す。コイル部に電流が流れると、接点がオンまたはオフに切り替わる。故障の際には、全接点がオンまたはオフに固定される。

3.2.3 故障の発生モデル

最後に、故障の発生モデルの例を **Fig. 10** に示す。“PRE”は前回の値を保持するブロックである。

本研究では、2.1節のカテゴリの説明で示したように単一故障を想定しているので、“FailureSwitch”が0以外の値になった瞬間に、値が示すモジュールが故障し、同時に故障モードが1または0となって固定されるとした。なお、Fig. 10では、三つのモジュールに対する単一故障をモデル化しているが、モジュールの個数が増えた場合は、“FailureSwitch”の値の範囲と故障出力を増やせばよい。また特定のモジュールだけの故障について検証したい場合は、逆に“FailureSwitch”の値の範囲を制限

Fig. 11 General emergency stop and restart system

Fig. 12 Category 3 emergency stop system

Fig. 13 Category 4 emergency stop system

すればよい。例えば1以下に制限すればモジュール1のみが故障する可能性を検証することになり、0だけに制限すれば故障が発生しない場合を検証することになる。

3.2.4 緊急停止系のモデル化

以上の準備を基に、緊急停止系をモデル化する。一般の緊急停止、再起動系のモデルを **Fig. 11** に示す。接点出力がコイルにフィードバックされるため、モデルでは“FBY”ブロックの遅れを用いた。また簡単のために安全リレー、安全スイッチのモデルを流用しているが、接点の一つずつしか用いていないため、一般のリレー、スイッチと同様の機能しか持たない。

同様にカテゴリ3の緊急停止系のモデルを **Fig. 12** に、カテゴリ4の緊急停止系のモデルを **Fig. 13** に示す。

3.3 安全要件のモデル化

形式検証では要求仕様をモデル化して与える。今回、緊急停

Fig. 14 Model of stop requirement

Fig. 15 Model of restart requirement

Fig. 16 Model of failure detection requirement

止系に求められる安全要件の例として、停止要件、再起動要件、故障検出要件の三つをモデル化した。

3.3.1 停止要件のモデル化

緊急停止系で最も重要と考えられるのは、緊急停止ボタンを押したときに、ロボットが停止するかどうかである。これを停止要件として Fig. 14 に示すようにモデル化した。図中の “Implies” は、ブロック左上の入力が真の場合に、左下の入力をそのまま出力する。すなわち、(時間遅れを考慮して) 緊急停止ボタンを 2 時刻以上押し続けたときにモータが停止していれば、真を出力する。

3.3.2 再起動要件のモデル化

次に再起動スイッチの機能を、再起動要件として Fig. 15 に示すようにモデル化した。図中の “AlwaysAfterFirstCond” は、ブロック左下の入力条件が成り立つまでは偽を、一度でも成立した後は常に左上の値を出力する。すなわち、一度緊急停止ボタンを押した後、再起動ボタンを押すまでの間は、モータは停止してはならないという条件をモデル化している。ただしモデルでは “FBY” ブロックを用いて、緊急停止ボタンを押して 100 時刻後までしか考慮していない。これは 4.2 節で述べるように、検証を 100 時刻後までで打ち切るために追加した。

3.3.3 故障検出要件のモデル化

最後に、故障の際にシステムの安全機能が失われないかどうかを、故障検出要件として Fig. 16 に示すようにモデル化した。このモデルでも、4.2 節に示した理由で 100 時刻までの検証とするため、故障が発生し、さらに緊急停止ボタンを押した場合に、100 時刻後にモータが回転していないかどうかを示している。

4. 形式手法による検証結果

以上の 3 種類のシステムモデルと 3 種類の要求モデルについて、SCADE ツールを用いて形式検証を行った。検証のためのモデルの例を Fig. 17 に示す。中央のリレー系のモデルに対し

Fig. 17 Model for formal verification

て、左上から外部入力、左下からは故障モデルからの出力が入力される。またリレー系の出力は、右側に並んだ各要求仕様モデルに入力され、それぞれ検証が行われる。入力にはユーザが用意する必要はなく、自動的に全入力に対して検証が行われ、仕様モデルからの出力がすべて真なら、対象モデルは要求仕様を満たしていることになる。

検証結果を Table 1 に示す。3.2.3 項で示したように、故障モデル内で値を制限することで、想定する故障の種類を変えてカテゴリごとの結果を比較している。

4.1 停止要件の検証結果

まず停止要件については、故障がない場合には、一般のシステム、カテゴリ 3、カテゴリ 4 のシステムのすべてのシステムについて、要件が成り立つことが分かった。

また故障を考慮した場合は、一般のシステムでは停止要件が破れることがあり、反例として、リレーの溶着故障（リレーがオンのまま固定される故障）が示された。さらにカテゴリ 3 のシステムでは、リレーの故障では停止要件は満たされるが、スイッチの故障として、緊急停止スイッチがオフに固定される反例（緊急停止できなくなる故障）が示された。ただしこの故障は適切な緊急停止スイッチを選べば、構造上ほとんどあり得ないと考えられる。

一方、カテゴリ 4 のシステムでは、あらゆる単一故障の場合でも、緊急停止ボタンを押し続けければモータは停止することが示された。これは、Fig. 7 に示したように、緊急停止スイッチの二つの接点を用いるためである。

4.2 再起動要件の検証結果

次に再起動要件の検証を行ったが、要求仕様をそのままモデル化した場合はツールによる検証が収束せず、結果を得ることができなかった。これは一般に形式検証で問題とされている、状態組み合わせの数が膨大となって検査不能となる、いわゆる状態爆発が原因と考えられた。そこで、今回のシステムの入力の数や状態の個数を考慮し、100 時刻程度の間、条件が成り立てばよいとして、3.3 節に述べたような要求モデルとした。ここで、形式検証ではすべての入力条件が検証できるので、100 時

Table 1 Satisfaction of safety requirements for each system

Relay type	Failure type	Safety requirements		
		Pressing emergency stop button → Stop (Stop requirement)	Emergency stop → Stop until restart (Restart requirement)	Failure → No restart (Failure detection requirement)
General	With no failure	True	True	-
	With relay failure	False	False	-
Category 3	With no failure	True	True	-
	With relay failure	True	True	False
	With switch failure	False	False	False
Category 4	With relay failure	True	True	True
	With switch failure	True	False	False

刻後だけを考慮すれば 100 時刻以内の事象はすべて検証できたことになる。

Table 1 に示すように、一般のシステム、カテゴリ 3 のシステムは停止要件の結果と同様であるが、カテゴリ 4 のシステムでも、スイッチの故障の場合には再起動要件が破れることが分かった。これは緊急停止したあとに、再起動スイッチが故障して自動的にオンになる反例であった。一般にこのような故障は起こりにくいと考えられるが、あえて注意点として考えれば、緊急停止ボタンをオフにしたあとは、故障その他の原因により、いつでもリセットがかかることを考慮すべきことが分かる。

4.3 故障検出要件の検証結果

最後に故障検出要件について、カテゴリ 3 と 4 を比較して検証を行った。4.2 節と同様に、ツールでの検証が収束しなかったため、100 時刻で打ち切る条件とした。

カテゴリ 3 の場合には、リレーが故障しても再起動をかけることができるが、カテゴリ 4 の場合には、リレーが故障した場合には再起動が許可されず、安全機能が失われない、すなわち安全であることが検証できた。

5. お わ り に

安全リレーを用いた緊急停止系を例に、形式手法により、安全システムの故障耐性を検証した。危険事象、安全状態、および故障を適切にモデル化し、要求仕様をモデル化することで、形式手法を適用して、様々な入力と条件の組み合わせに対してハードウェアの検証が網羅的に行えることを示した。また要件が満たされない場合には、条件を破る場合の反例が示されて仕様上のリスクが明示されることが分かった。

本論文では安全リレーを用いたロボットの緊急停止系という比較的単純なシステムに適用したが、提案した手法はハードウェアとソフトウェアが混在した、より複雑なシステムについても適用可能である。今後は、安全リレー回路以外の人共存ロボットのハードウェア、ソフトウェア混在システムについて、実際にモデル化と検証を行って形式手法の有効性を示す予定である。

参 考 文 献

- [1] ISO 13849-1:1999 Safety of machinery – Safety-related parts of control systems – Part 1: General principles for design
- [2] IEC 61508: Functional Safety of Electrical / Electronic / Programmable Electronic Safety Related Systems – Part 3: Software requirements
- [3] 経済産業省：次世代ロボット安全性確保ガイドライン。2007.
- [4] 中坊嘉宏，山田陽滋：“人と共存するロボットのためのオブジェクト指向による安全関連システムのモデリング”，第 25 回日本ロボット学会学術講演会予稿集 CD-ROM, 3C27, 2007.
- [5] 中坊嘉宏，山田陽滋：“人と共存するロボットのためのオブジェクト指向によるリスクアセスメントのモデリング”，日本機械学会ロボティクス・メカトロニクス講演会'08，講演論文集，2A1-A19, 2008.
- [6] 中坊嘉宏，山田陽滋：“人と共存するロボットのための形式手法による安全関連システムの検証”，第 26 回日本ロボット学会学術講演会予稿集 CD-ROM, 3J3-05, 2008.
- [7] L.-H. Eriksson: “Using Formal Methods in a Retrospective Safety Case,” SAFECOMP 2004, pp.31-44.
- [8] S. Dajani-Brown, D. Cofer, G. Hartmann and S. Pratt: “Formal Modeling and Analysis of an Avionics Triplex Sensor Voter,” Proc. SPIN, pp.34-48, 2003.
- [9] J.-L. Colaco, B. Pagano and M. Pouzet: “A conservative extension of synchronous data-flow with state machines,” Proc. of the 5th ACM Int. Conf. on Embedded Software, pp.173-182, 2005.

中坊嘉宏 (Yoshihiro Nakabo)

2000 年東京大学大学院工学系研究科計数工学専攻博士課程修了。同年同大学リサーチ・アソシエート。2002 年理化研究所バイオ・ミメティックコントロール研究センター研究員。2005 年より産業技術総合研究所知能システム研究部門安全知能研究グループ研究員。超高速ビジョン，人と共存するロボットのための安全知能の研究に従事。（日本ロボット学会正会員）

山田陽滋 (Yoji Yamada)

1983 年 3 月名古屋大学大学院博士前期課程修了。同年 4 月豊田工業大学助手勤務。1992 年工学博士（東京工業大学）。1993 年豊田工業大学助教授。同年 Stanford University 客員研究員。2004 年 4 月から産業技術総合研究所知能システム研究部門。さらに，2008 年 4 月から名古屋大学大学院工学研究科機械理工学専攻。これまで，ロボットのセンサ・通信・知的制御に関する研究，および，人間-ロボット共存系の研究に従事。近年は安全知能が主題。（日本ロボット学会正会員）