様式 C-19

科学研究費補助金研究成果報告書

平成２３年６月１０日現在

機関番号：８２６２６
研究種目：基盤研究（C）
研究期間：2008～2010
課題番号：２０５００１７５
研究課題名（和文）　ＵＭＬモデリングによる人と共存するロボットの安全設計と評価方法の研究
研究課題名（英文）　Safety Design and Evaluation of Robots Coexisting with Humans by UML Modeling
研究代表者
中坊　嘉宏（NAKABO YOSHIHIRO）
独立行政法人産業技術総合研究所・知能システム研究部門・主任研究員
研究者番号：７０３６０６０９

研究成果の概要（和文）：人と共存するロボットの実用化には，安全について十分に配慮する必要があり，リスクアセスメントを行って適切な保護方策をとることが重要である．本研究ではリスクアセスメントについての国際安全規格 ISO 14121-1:2007 を参照し，モデル化方法としてオブジェクト指向に基づく UML モデルの利用を提案してリスクアセスメントデータベースを開発した.これにより,複雑かつ膨大な量のリスクアセスメントを効率よく網羅的に行い，統一したモデルデータのもとに分析と管理が可能となった.

研究成果の概要（英文）：I have proposed to introduce a UML modeling and an object-oriented approach to risk assessment of human-robot cooperating systems. Risk assessment is based on the international safety standard ISO 14121, and our UML-based, hierarchical unified model includes its elements of machinery, human, environments, origin and consequences of hazards and their types of group. By using the model, different viewpoints of safety factors such as an exhaustive list of hazards, scenario of tasks or potential hazardous situations can be derived from a unique dataset. Also, an iterative process of risk assessment and system modification are executed easily.

交付決定額

（金額単位：円）

	直接経費	間接経費	合　計
2008 年度	1,300,000	390,000	1,690,000
2009 年度	1,100,000	330,000	1,430,000
2010 年度	1,100,000	330,000	1,430,000
年度			
年度			
総　計	3,500,000	1,050,000	4,550,000

研究分野：安全，ロボティクス
科研費の分科・細目：情報学・知覚情報処理・知能ロボティクス
キーワード：国際安全規格，リスクアセスメント，形式検証，オブジェクト指向，UML モデル，共存ロボット，次世代サービスロボット，安全関連系

１．研究開始当初の背景

従来，実用化されたロボットのうち，工場等で用いられる，出力の大きい産業用ロボットについては，作業員の安全を確保するために柵等で囲って隔離することが原則であった．一方，家庭用では玩具程度の，出力が小さく危険の少ないロボットがほとんどであった．ところが，近年，より出力の大きなロボットでも，人と空間を共有してサービスを提供したり，人を抱え上げるなどの力学的なインタラクションのニーズがある．また工場等でも，ロボットの可動領域に作業員が入り，互いに近接して作業したいという強い要求がある．これに対して次世代ロボット安全性

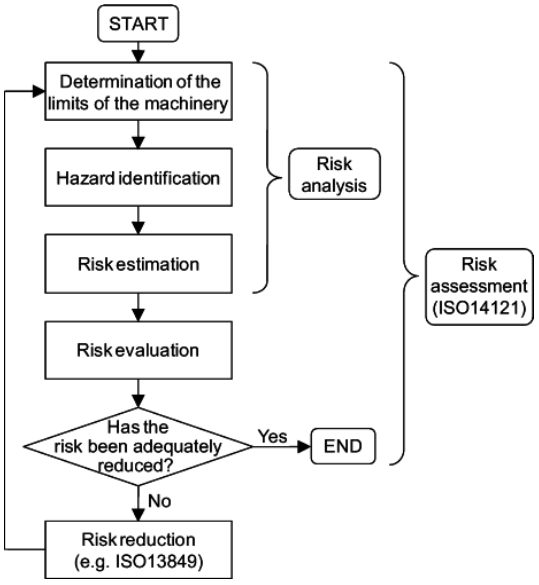
確保ガイドラインが発表され，人と共存するロボットの，安全性確保のための基本的な考え方が示されている．その中で，安全性確保の最初のステップとして，リスクアセスメントの必要性が示されている．

一方，ロボットの安全に関する学術的な研究では，ロボットの危険な部分を個別に解決して安全化したり，安全に関わる機能の信頼性を高めたりする研究が多かった．このような研究の場合，ロボットの安全性が向上したとしても，実用化の際に，結果としてそれが十分安全と言えるレベルに達しているのかどうか，判断できないということが多かったと考えられる．すなわち，実用化のためには安全性の向上だけではなく，安全性の保証も重要だと考えられる．

実際，前述のガイドラインや，その基となっている機械安全についての国際規格 ISO 12100 では，対象とするシステムについての安全性の基準を明確に定め，決められた手順に従って安全性を確保することを定めている．このようなガイドラインや規格は，広く現状の技術や手法を考慮して取り入れた State of the art を示すものと言え，これらの規範に従うことは，一般に社会に受け入れられる安全技術を構築する方法のひとつと考えられる．

２．研究の目的

上述の ISO 12100 は，ロボットを含む一般の産業用機械を対象とした国際安全規格で，機械安全に関わる規格階層構造の最も上位の A 規格，概念規格に属するものである．一方，産業用以外のロボットに関する国際規格は未だ存在しないため，本研究ではこの ISO 12100 に基づいて，共存ロボットの安全性を考える．



上図に示すように，ISO 12100 では安全を確保するための反復的プロセスを定めている．具体的には，まず対象システムのリスクアセスメントを行い，あらゆるリスクが許容可能な水準まで低くなったと判断できれば，対象は安全として終了する．もし安全と判断されなかった場合には，何らかのリスク低減方策（Risk reduction）を行って，改めてリスクアセスメントを行う．このうち，リスクアセスメントについては，さらに別の国際安全規格 ISO 14121-1 を参照することとしている．本研究では，このリスクアセスメントのプロセスを研究対象とした．

リスクアセスメントは，網羅的に危険の同定，分析，評価を行うことが重要である．ISO 14121 は 2007 年に，以前の 1999 年版から改訂され，その基本部分は変わらないものの，より詳細化し，整理された．考慮すべき危険の各項目は組み合わせで示されるようになり，さらに新たにライフサイクルという概念が導入されて，製造から廃棄までの全期間が対象となった．結果として膨大な量の考察が必要で，対象のあらゆるリスクを見つけ出し，分析し，最後に全てが許容水準に達したことを保証しなければならない．またそのプロセスを記録，管理することも必要とされている．

特にロボットの場合は一般の機械装置と異なり，動作が複雑で，かつ自律的に動作するなど，考慮すべき危険事象や状況が多岐にわたる．さらに人と共存するロボットの場合，人とのインタラクションの影響も考えなくてはならず，従来よりも格段に複雑さが増していると考えられる．すなわち，従来のリスクアセスメントで行われていた，紙ベースの，人の直感に頼った方法では不十分であり，システム化された新しい方法が必要だと言える．

本研究では，オブジェクト指向と UML という一貫したモデルに基づいて，ISO 14121 に基づくリスクアセスメントをモデル化し，データベースを作成する．データベースを用いてデータと表現を分離することで，統一的なデータ管理と，様々な表現による多視点からの分析を同時に達成することができる．具体的には UML を用いることで，機械的な要素，あるいは安全概念の整理や構造化にはクラス図を用い，動作や手順の記述についてはシーケンス図を用いた表現が可能となる．またライフサイクルを考慮した作業や環境についてはユースケースで表現することが可能である．

このように，様々な表現形態を用いて多次元のデータを保存し，データの整合性を保ちつつ，多様な表現を可能にすることで，システム化され，整理された形でのアセスメントが可能となる．

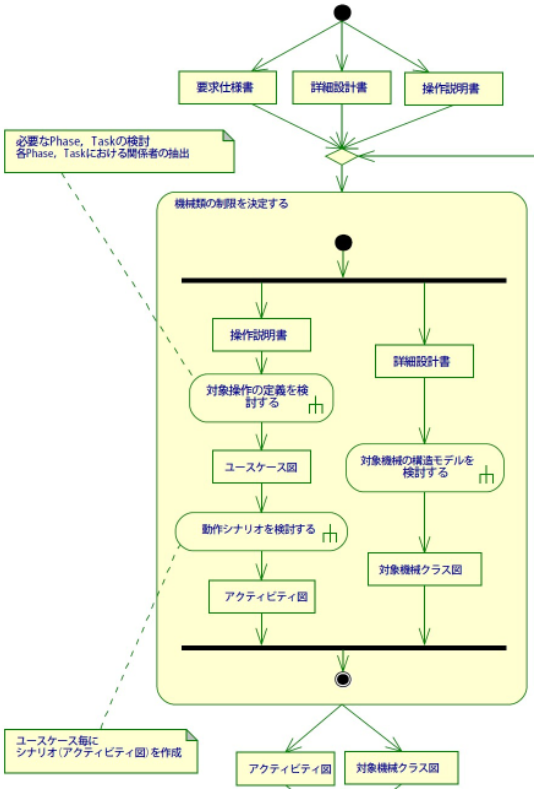
３．研究の方法

リスクアセスメントの具体的なモデル化について，ISO 14121 の記述に沿って説明する．前出の図に示すように，リスクアセスメントは，リスク分析(Risk analysis)とリスク評価(Risk evaluation)に分けられる．さらに，リスク分析は，機械類の制限(Limits of the machinery)，危険源の同定(Hazard identification)，リスク見積り(Risk estimation)の順番で行われる．

機械類の制限は，機械の使用方法を定めるものである．まず対象となるロボットの機械的な構成を，詳細設計書に基づいてクラス図で表現し，各部分要素ごとに階層化してモデル化する．各クラスは必要に応じて詳細化し，以下の危険源の同定により危険性に関するパラメータを持つ．

一方，ISO 14121 では，ロボットのライフサイクル全般に渡るタスクの同定が重要であるとされている．すなわち，次に行う危険源の同定において，設置，テスト，教示/プログラミングなど，通常稼働時以外も含むライフサイクルの各フェーズ全てを考慮し，どのような作業が，どのような機械で，誰によって，どのような環境で行われるかを明確にしなければならない．そのため操作説明書に基づいて，上記を記載したユースケースモデルを作成する．

続いて，上記のそれぞれのユースケース図に含まれる全てのタスクについて，具体的にどのようなシーケンスで，どのような要素（人，装置，環境）が作用しているか，アクティビティ図で定義する．これを下図に示す．



以上のタスクの定義，及び機械のクラス図に基づいて，それぞれのタスクにおける危険源と因果を関連づけることで，危険源の同定を行う．具体的には，まず ISO 14121 の Annex A.1 に示される危険源のリストを参照する．

危険源は種類ごとに，機械的危険源，電気的危険源などのグループに分けられ，各グループごとに，危険の原因となる要素と，危険を引き起こす因果関係を，それぞれリストにして示している．ここで，要素と因果関係は，順番に関係なく，任意の組み合わせで可能性を考えなければならない．すなわち，押しつぶし(Crush)の危険については，落ちてくる物体(Falling Objects)や，固定物体と移動物体の間に挟まれる(Approach of a moving element to a fixed parts)などの原因について，どれも可能性があるとして考慮しなくてはならない．これらは Annex A.2 に例示されている．

４．研究成果

安全概念をモデル化した研究として，人，環境，装置の三要素を考慮してエラーを解析する三要素 FMEA¥cite{3youso}があるが，分析手法に表を用いており，リスクを様々な観点から分析できないという問題があった．また，共存ハザードアボイダンス技術の提案では，ロボットの空間的な動作を構造的に整理して分析しているが，分析のベースとなる，要素データの構造については特に考慮されていない．それ以外にも，従来から多くの安全規格や手法で，リスクアセスメント結果を記述し，また安全の要素を整理するため，表やリストが用いられてきた．しかし，表やリストでは表現できる情報の構造が 1 次元や 2 次元に限られ，要素間の複雑な関係や多視点からの分析に問題がある．

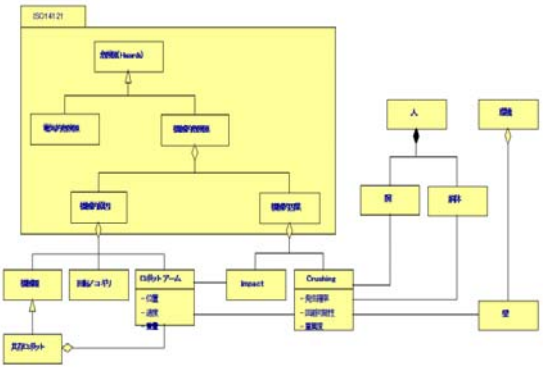
例えば，システムの動作，特にロボットの動作と，人や環境との関係を考える上で，シナリオをベースとして状況や動作手順を考えながら安全を考察することが有効とされている．具体的には，ISO 14121 の Annex A では，後で述べる危険源(Hazards)の内容リスト(Table A.1，A.2,)と，それがどのような状況(Situation)で(Table A.3)，どのようにして起こりうる(Events)か(Table A.4)という，リストとストーリの二通りの表現が示されている．このように，様々な視点からのリスクアセスメントを行った場合，その結果を 2 次元の表にまとめるのは困難である．また様々な要素が関わることで，アセスメント結果の可読性と理解が妨げられ，結果としてアセスメントの網羅性，完全性に疑問が生じることになる．

オブジェクト指向手法は，主にソフトウェア開発で用いられ，システム内の多くのデータや処理を整理してモデル化し，開発するの

に適している．またソフトウェアだけでなく，システムの概念レベル設計にも用いられており，特に UML を用いて，具体的な物や事象と抽象的な概念とを，統一的に整理して記述することが可能である．

これまでに，安全関連でオブジェクト指向を取り入れた研究として，安全に関わるソフトウェアをオブジェクト指向で開発したものがあるが，本研究のように，安全概念そのものを抽象化してモデル化するものではなかった．またオブジェクト指向の標準化団体である Object Management Group (OMG)では，2008 年に Quality of Service と Fault Tolerance に関する UML Profile を発表しているが，抽象度が高く，ロボットアプリケーション向けの具体的なモデルとはなっていない．また ISO 14121 との整合もとれていない．

本研究では，危険源について，オブジェクト指向に基づき UML でモデル化した．これを下図に示す．

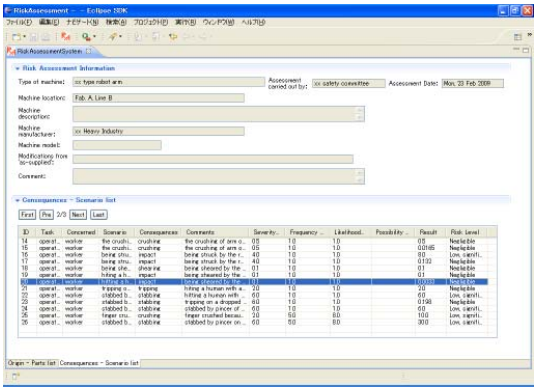


機械類クラスに共存ロボットクラスを考えた一方，危険源クラスの機械的危険源クラスにも，ロボットアームをクラスとして考えて，両者を関連で結び付けた．これは，共存ロボットの各パーツごとに，機械的危険源となる場合もあれば，電気的危険源となる場合もあることから，実態と役割（ロール）としてクラスを分けた方が良いと考えたためである．

また，ひとつの原因（ロボットアーム）について，押しつぶし(Crush)や，衝撃(Impact)のそれぞれについて，関係を考えることとしている．モデルでは，ロボットアームの持つ，位置，速度，重量などのパラメータがそれぞれの因果クラスに渡され，そこで，後で述べるようにリスクの見積もりがなされる．その際には，人のどの部位に危害が加えられようとしているのか，また壁などの環境との関係はどうなっているかということも関わると考えられるので，関連で結び付けた．

以上の構造に従い，前述のタスクに基づくシナリオベースと，網羅的なリストベースの 2 通りの解析を関連づけ，データベースを作成することができる．

具体的には，ロボットの機械的な構成を示すクラス図において危険源となり得る要素を抽出し，あるいは，シナリオにあたるタスクのアクティビティ図から危険事象が起こりうる可能性を検討して，両者を互いに関連づけて具体的な因果関係の要素を決定する．その際に，ユースケースに基づいて，関連する人情報や環境情報も追加して登録する．これらを具体的なリスクとしてデータベースに登録していく．以上を，様々な原因と因果の可能性に対して，可能な組み合わせごとに網羅してデータを作成する．実際に作成したデータの例を下図に示す．



作成されたデータについては，次の工程で評価を行うことになる．その際，例えば人の胴体がハンドグリッパに挟まれるといったような，可能性の非常に低い組み合わせは，解析の効率化のために除外してもよい．これら可能性の判定は，共存ハザードアボイダンス技術でも詳しく考察されている．また Annex A.1 の危険源リストはあくまで例であるから，これを参考にしながら，
解析に都合のよいように，因果を適切に階層化してクラスとしてまとめればよい．

危険源の同定に続いて行うリスク見積りでは，構造モデルに基づいて定量評価を行う．規格では，考慮すべきパラメータとして，発生確率算出のための危険への暴露頻度，発生可能性，回避可能性の 3 つ，及び，もしも発生した場合の重篤度が，それぞれ示されている．これらは構造化された危険源クラスごとに，関連で結び付けられた人や環境，タスクの各クラスからパラメータを得て，クラスの手続きとして確率や重篤度を計算すればよい．実際の計算部分については，今回のデータベースの範囲外となる．今後プラグインとして実装する予定である．

またデータベースでは，危険源と，そのパラメータとなる確率や重篤度などの数値は，別々に分けてデータを持つ．これは，例えば構造の分析は設計者が行い，定量的な解析については計算方法のみ定義して，計算を自動

化するなど，データと構造を分離することによる効率化が可能と考えられる．

リスクアセスメントの最後には，リスク評価を行う．リスク評価は，得られたリスクの大きさを基に，残ったリスクが許容可能かどうかを判断する．また同時に，ここまでの分析が正しいかどうか，すべてのリスクを網羅しているかどうかを，チェックすることも必要である．これらは，データベースの可視化方法を変えることにより，任意のパラメータやクラスごとに，リストなどの様々な表現を生成することが可能である．これにより，解析の妥当性や，許容可能性の判定を容易に行うことができると考えられる．今回開発したデータベースでは，この可視化部分は実装されていない．これについても今後プラグインとして実装する予定である．

最後に規格で定められる文書化について述べる．上記すべてのリスクアセスメントの過程と結果は，適切に文書化し，関係者に提示しなければならない．通常，その文書は膨大なものとなり，また繰り返しのプロセスで仕様が変わっていくため，管理が非常に困難となる．これまでに説明した，データベースを用いることで，解析結果を一貫して記録し，蓄積していくことが可能となる．具体的には，リスクアセスメント作業を行うごとに作業参加者による承認を行う．また承認ごとの記録を保存し，必要に応じて随時出力することが可能である．

データベースによる文書管理の結果，管理者とリスクアセスメントに参加した人が承認者として登録され，また登録の日時が記録された．このように，プロセス管理を自動化することで，アセスメントの繰り返しプロセスを素早く回して，細かいトライアンドエラーを繰り返す，アジャイル開発が可能になると考えられ，複雑なシステムの開発効率向上に役立つと言える．

５．主な発表論文等

〔雑誌論文〕（計１件）

①中坊嘉宏，山田陽滋：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，日本ロボット学会誌,査読有，Vol.27，No.8，2009,pp.27-32

〔学会発表〕（計２件）

①中坊嘉宏，山田陽滋，人と共存するロボットのための形式検証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，2008 年 9 月 11 日，神戸

②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，ロボティクス・メカトロニクス講演会 2008，2008 年 6 月 7 日，長野

〔その他〕

国際標準化団体 Object Management Group, System Risk Assessment Metamodel 規格化のための Requests For Information
http://www.omg.org/cgi-bin/doc?sysa/2010-9-8

６．研究組織

(1)研究代表者

中坊 嘉宏（NAKABO YOSHIHIRO）
独立行政法人産業技術総合研究所・知能システム研究部門・主任研究員
研究者番号：70360609