招 待 論 文

次世代ロボット安全：技術の現状と課題

名古屋大学大学院　工学研究科
教　授　山田　陽滋

1　はじめに～次世代ロボット安全技術の概要

次世代のロボットは，ロボットが人間と物理的に共存し，福祉現場や公共の場で，人に対して直接･間接のサービスを施すことが期待されている．したがって，次世代ロボットにとって安全性が重要であることは，申し上げるまでもないであろう．その安全技術とは，人間･ロボットが共存する状況において，想定されるリスクを網羅的に取り上げて分析評価し，それらがすべて許容できるレベルまで低減されるために，ロボットやロボットシステムの要素に要求される技術のことである．ロボット安全の分野では，ロボットのユーザーや周囲の人間のヒューマンエラーを事故に結び付けさせないことも含め，彼らの安全が確保されるように，ロボットのリスク抑制性能を向上させる技術が，研究開発の対象として展開されてきている．

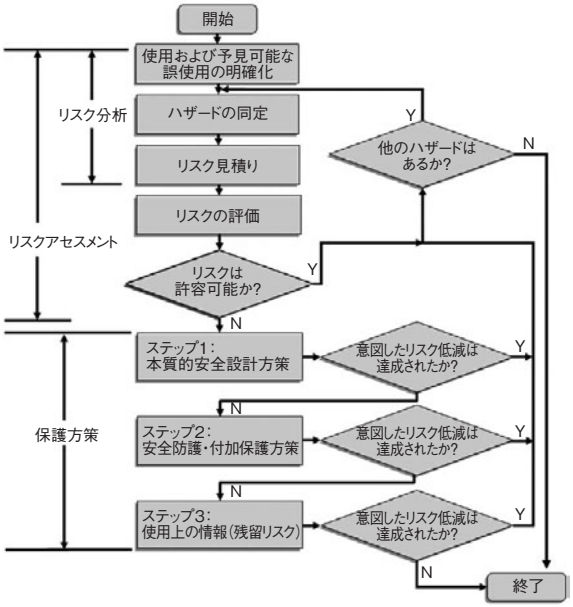
2　安全技術の概要と本質

2.1　機械安全のための設計原則

次世代ロボットといえども機械システムの一部にほかならない．そこで，さまざまな産業分野を支える機械システムを対象として，その設計から開発，製造，運用から廃棄までのさまざまなフェーズ（ライフサイクル）にかかわる人間の安全性確保のための議論を機械安全と称する．この機械安全には，以下に述べるような，リスクアセスメントと保護方策で構成されるプロセス（**第1図**）の反復を範とする設計原則が存在する[1].

2.2　リスクアセスメント

リスクアセスメントとは，FMEA（Failure Mode and Effects Analysis：故障モード・影響解析）などの手法を用い，ロボットのライフサイクルを通して同定されたハザード（後述）それぞれに対してリスクを見積もり，評価する活動のことである．その実施手順は，先の規格において，



第1図　リスクアセスメントとリスクと保護方策

①ロボットの使用などに関する制限の決定（合理的に予見可能な誤使用を含む）
②ハザード（危険源）の同定
③リスク見積り
④リスクの評価

に従うことと規定されている．

リスクアセスメントでは，はじめに①でロボットに関するさまざまな制約事項，つまり使用上の制限，空間的･時間的制限などを列挙する．「合理的に予見可能な誤使用」とは，例えば，過去にこういうことがあったから，という理由とともに述べることができる，人間による誤った使用の仕方，という意味である．

次に，②のハザード同定のプロセスに進む．ハザードは，国際安全規格でも定められており「危険源」としばしば訳されるもので，危害を引き起こす原因となる因子のことである．これを網羅的に分析し抽出することは，メーカーにとっては，不法行為責任および製造物責任の

両方に共通する，予見義務の観点から重要になる．ハザードは安全技術の入り口に位置づけられていながら，理解しにくい．そこで，ハザード状況（hazardous situation）として，以下に示す3要素が条件的にそろった状況でリスクは顕在化するという説明を筆者は行っている．3要素とはすなわち，1）人間，2）機械，3）危害を人間に及ぼす機械のメカニズム，つまり有害作用，である．これらのうち，いずれが欠けても危害にはならない．さらに，1）と2）はそもそも前提とも言える要素であるので，結局3）の条件要素がハザードになる．そこで3）について，本質的あるいは実用的な観点から，ハザードはリストアップされていくことになる．

具体例を示せば，搭乗型ロボットとともに搭乗者が壁にぶつかって彼（彼女）に危害が及ぶという状況では，ロボットの力学的な運動量の変化あるいは力積によって危害が引き起こされるという意味で「運動性」，あるいは，危害発生をもたらす直接のメカニズムである「衝突」がそのハザードであるという同定の仕方をする．

③では，同定されたそれぞれのハザードから想起されるリスクをひとつひとつシナリオ事象形式で取り上げ，あらかじめ離散的に目盛って定められた重篤度と頻度の程度について見積もっていく．そして最後に，リスクアセスメントの④の段階では，リスクグラフやリスクマトリクスを用いて評価を行う．④の結果，許容できないリスクが設計上に残るとなれば，すぐ後に述べる保護方策と呼ばれるプロセスに従って，許容されないリスクそれぞれについて，その低減を図らなければならない．

機械安全の分野では，この保護方策の第2ステップの段階で国際規格ISO-13849[2]がしばしば適用される．この規格ではリスクグラフに基づいて，機械の安全性に直接かかわる制御系のリスク抑制性能として要求すべきレベルを定める．リスク評価を個別に定める際に，粒度をより高く設定できるのは，リスクマトリクスである．リスクマトリクスを使って，いかに評価を行うかは，メーカーの基本方針にかかわる問題であり，これについては後の4.1節で再び取り上げる．

2.3　保護方策

保護方策の段階では，3ステップ法に従う必要があると先の設計原則の規格には規定されており，各ステップで取り得る方策の内容も規格[1]に詳細に紹介されている．すなわち，

ステップ1　本質的安全設計方策
ステップ2　安全防護策および／または付加保護方策
ステップ3　使用上の情報

である．以上の手順は，少なくとも機械安全の枠組みでは，すべて順序まで決まっており，ステップの順序を入れ替えたり，飛び越したりしてはいけない．以下に，それぞれのステップの平易な説明を試みる．

〔1〕本質的安全設計（ステップ1）

本質的安全設計とは，設計や運用上の改良によりハザードそのものを取り除くことである．例えば，先の倒立2輪型ロボットでも搭乗を目的としないロボットについて考える．このロボットに関するハザードとして衝突を取り上げるならば，これが周囲の人間に危害を及ぼすことがないように，出力の小さい駆動モータをあらかじめ選定し，減速比の高い駆動伝達機構を設計に組み込んで．最大速度を十分低減するなどの方策をとることができる．本質的安全設計のための技術は極めて広範にわたり，それらの設計指針もまた，当該規格[1]に網羅的に掲げられている．

〔2〕安全防護策および／または付加保護方策（ステップ2）

もし，ロボットの仕様を満たすために，本質的安全設計によってはハザードが取り除けない，あるいはリスクが十分に低減できないとなれば，次のステップである安全防護策および付加的な保護方策をもって，リスクの低減を図ることになる．安全防護とは，防護のための柵と保護装置のことで，保護装置には，インターロック装置やイネーブル装置，光電式存在検知装置や機械的な運動制限装置が含まれる．付加保護装置は，緊急停止装置や脱出装置のことである．

ところで，このステップ2の方策指針に関しては，近年，ロボット安全に限らず機械安全など広い分野をカバーする機能安全[3]と呼ばれる概念が登場し，諸産業分野に多大な影響を与えつつある．機能安全とは，対象機器の中で安全を確保する機能をつかさどるものとしてE/E/PE（電気・電子・プログラマブル電子）機器がかかわる場合に，安全と関連づけてこれらの機器の信頼性観点における目標を設定し達成しようとする概念である．対象機械のライフサイクルを見渡し，その中で安全上要求される機能が果たされないリスクがある場合に，これを要求レベルまで低減しようとする考え方である．ここで安全関連系とは，対象機械を安全状態に導く，あるいはこの状態を維持するために，必要な安全機能を上記のE/E/PEによって実行する上で，部品1つに至るまで，かかわりをもつサブシステムのすべてである．

先の例で位置づけると，安全防護策は以下の機能を果たす安全関連系に対して講じられる．すなわち，搭乗型ロボットが人間を運ぶ際に，人間を含む周囲環境と衝突するという危険な状態に陥ることを防ぐために，周囲環境を見張る機能や，周囲の障害物を検出した場合に，ロ

ボットの運転速度を低減したりゼロにしたりする機能である. これは, ロボットの走行制御系が普通につかさどっている機能の中で，安全にかかわる規定速度を管理する機能に関する信頼性を問うことになる.

安全関連系の信頼性評価には，安全度水準（SIL：Safety Integrity Level）と呼ばれる指標が用いられる．この性能指標は，安全関連系におけるハードウェアとソフトウェアの両方が対象となる. まず, ハードウェアにとってのリスクは，確率的な部品の故障である．安全関連系を構成する部品のライフサイクルにおける寿命曲線（通常は，故障率がバスタブ形状のワイブル分布でモデル化される）の底面部分の一定値に対応し，統計的にランダム故障と位置づけられるものである．特に，安全関連系の故障が機器を危険に導くと考えられる故障で，さらに自己診断機能でそれを検出できないことが問題になるので，危険側故障にならない，その割合の大きさを安全側故障割合：SFF（Safety Failure Fraction）として評価の対象にする.

つぎに，ソフトウェアの機能安全で対象にするのは，系統的故障と呼ばれる決定論的観点で評価されるリスクが主である．これは，評価の対象がE/E/PE系（の中で安全機能を実行する部分）であることによる．つまり，ソフトウェアの重要な機能は, 安全機能を制御することと，プログラマブル電子系が誤ったデータマネジメントをしないか，そしてつぎに自己診断アーキテクチャが機能しているか，をそれぞれチェックすることである.

ソフトウェアはコマンドとして書けば，そのとおり決定論的にふるまうので，コマンド系がもつ仕様そのものの健全性やチェック機能に対する忠実度がソフトウェアの信頼性能として問われる．そして，ソフトウェア開発は，仕様決定に始まり，アーキテクチャ，システム構成，モジュールの決定を経てコマンド実装までの設計とそれぞれの単位での検証を重層的に展開して，ソフトウェアの信頼性を確保する．このスキームは，大枠の概念構築から最小単位のコマンド実装までをトップダウンで設計し, ボトムズアップで検証していくスキームの形状から，V字モデルと呼ばれる.

〔3〕使用上の情報（ステップ3）

ステップ2までのリスク低減方策によって，リスクアセスメントで評価の対象になったすべてのリスクが許容し得るレベルにまで達しても，リスクはまだ残っているので，これらのさらなる低減を目的として，ロボットの使用者に残留リスク情報の伝達を行う作業がステップ3として位置づけられている．あるいは，ステップ3まででは，費用対効果の観点で適切な方策が講じられない場合に，このステップで呈示された使用上の情報の運用側における順守を，リスクの許容条件とする場合もある.

3　次世代ロボット安全の特徴

3.1　産業用ロボットの人間共存条件

製造環境におけるロボットの安全要求事項を記述した，いわゆる産業用ロボットの国際安全規格ISO 10218[4]は，2006年の発行以降，産業用ロボットの稼働中であっても，人間と共存することが以下に示す技術的な条件下で可能となり，ロボットの次世代化が加速されてきている．すなわち，2011年発行の現行規格では，1）協調作業環境への人間の侵入時にロボットが安全関連系によって停止できる場合，2）手動ガイドによって操作されている場合，3）操作者までの距離とスピードがモニタされ，安全距離を保つことができる場合，にそれぞれ人間との共存・協調作業が許されると規定している.

3.2　非産業用ロボットは移動ロボットが中心

先行する類似規格[4]でも移動ロボットに関する議論が十分に尽くされておらず，現在策定中のISO/DIS 13482［5］では，**第2図**に示す移動ロボットと身体アシストロボットを対象として，安全要求事項の策定が進められている．これらの中で，中心的に議論されている移動ロボットは，さらに，マニピュレータを搭載し，これを通して人間に物体の提供や彼らとのコミュニケーションを行う移動マニピュレータのタイプと，人を搭乗させるタイプに大きく分類できるが，安全要求事項として両者に重なる項目は多い．例えば，人間の乗降時や負荷搭載時を含めたロボットの静的／動的安定性に関するもの, 人間を含む周囲環境との衝突回避に関するもの, バッテリーに関するもの，さらには，直接触れることから，形状や表面の化学的物性，振動や静電気，環境条件に対しても概念的にではあるが要求事項が細分化され整備されつつある.

第2図　規格[5]が対象としている移動ロボット（左と中）と身体アシストロボット（右）

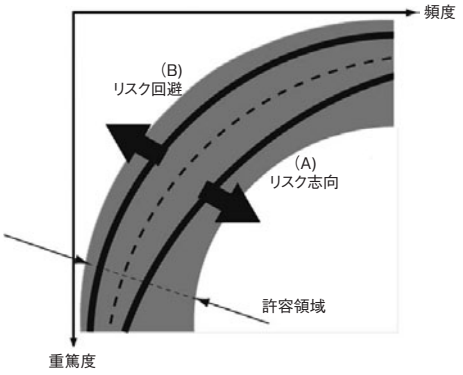
3.3 パワーアシストは，本質安全指向

[5]で取り上げられている身体アシストロボットも，安全要求事項については，意外に移動ロボットと類似項目が多い．このタイプのロボットは，人間によって直接装着されるもので，その安全性にはとくに注意を払う必要があると容易に推断される．そこで，規格上は人間のパワーを超えるような高出力ロボットまで考慮されているが，現実には，本質的安全設計に則った比較的小出力のロボットが対象となる．また，機能安全の観点では，仮に危険側故障に陥った場合でも，保護停止機能を発揮すると，その後人間は，急激な動作の変化を強いられ，転倒するなどかえってリスクが増大することが懸念される．そこで，故障時の安全関連機能としては，むしろ人間の操縦に任せることが重要となり，減速機の機械的粘性を利用して安全な減速を達成させるなど本質安全指向の方策が講じられる．

4 課題と対策

4.1 リスクの許容領域幅と，リスク志向／回避態度

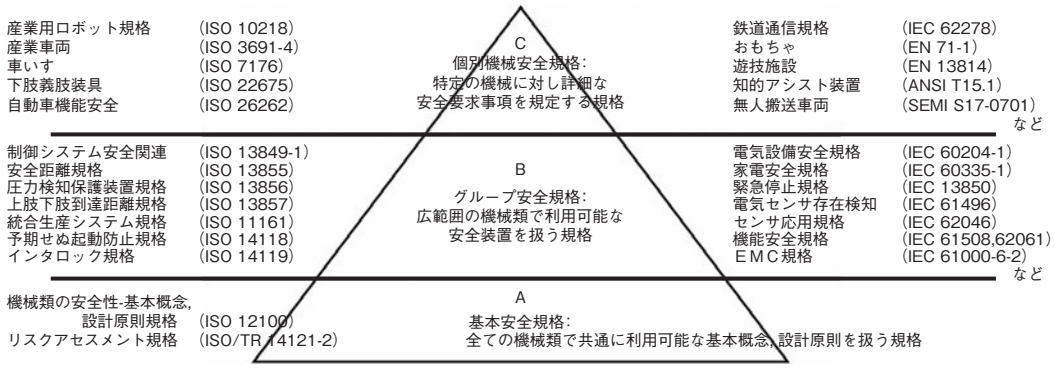
本節では，個別の課題に対するメーカーの取り組み指針を述べようと考えているが，その前に基本方針として考慮すべきリスクの許容の仕方に関する概念を述べる．第一は，リスクの許容幅である．これは，ALARP（As Low As Reasonably Practicable）[6]と呼ばれるもので，リスクが許容される幅，つまり許容領域の中に収まるレベルまでリスクを低減させるために，合理的に実現可能な“state-of-the-art”の安全技術が選択できる領域である．それは，**第3図**において灰色の幅をもった領域として示されるものであり，リスク評価の結果，条件付きで製品を実現可能とできる領域である．ALARP領域の大きさは，適用可能な安全技術のバリエーションに依存してくる．より具体的には，次世代ロボットと使用状況が類似



第3図　リスク志向／回避態度

する機械類で標準化が先に進んでいる製品の安全規格（C規格）や，それらの製品で共通に使われる要素技術の安全にかかわるグループ規格（B規格）への精通の度合いに依存するといっても過言ではない．したがって，これは，後に4.4節で述べる「いつのタイミングから，安全技術構築に取り掛かるか」にも大きく影響する．参考までに，次世代ロボットに関連する安全規格体系を**第4図**に示す．同図のB，C規格欄には，一部の地域規格も含めて，特に次世代ロボットと関連が深いと筆者が考える国際安全規格を紙面の許す範囲で示した．

つぎは，リスク志向／リスク回避態度である．同図の2本の太実線でそれぞれ示すように，（A）リスクをとる（志向する；risk seeking），（B）リスクを回避する（risk aversion）の2つの態度がある．いずれも，曲線の左上側のリスクを許容するという意味である．これらは，許容領域の形状を左右するメーカーの基本的方針（態度）であり，採用する安全技術のレベルや目標販売数，事前事後いずれの責任を強化するか，またできるか，といった多様な観点に基づいて，メーカーは部署横断的な議論と決断（コミットメント）を行う必要がある．



第4図　次世代ロボットに関連する主な国際安全規格

4.2 本質安全の線引きをいかに行うか

対象であるロボットが，本質的に安全であることをメーカー自らが検証できれば，安全技術の導入負荷は，それだけ軽減される．従来は，自動車分野において，比較的重篤度の高い傷害を対象とした傷害耐性値[7]が数多く報告されてきたが，近年は，ロボティクスの分野でも痛み耐性[8]や，より低い傷害耐性値を与える研究結果[9]が報告されるようになってきていて，線引きが可能な分野が少しずつ増えてきている．

そして，これらを考慮に入れる場合に，リスクカーブを導入できると，リスクの許容幅が広げられる可能性がある[10]．つまり，最悪値として最も高い傷害だけを考えると，リスク評価の結果，安全確保のハードルが高くなってしまうが，その確率（頻度）も考慮すると，リスク評価結果を下げることができる可能性が出てくる．

4.3 機能安全に環境の不確定性をいかに取り込むか

先に述べたように，ソフトウェア機能安全は，E/E/PE機器の高信頼な運用を目的とした物理層のデータチェックが対象である．しかし，実際のソフトウェアでは，今後さらに上位の目的を達成するためのアルゴリズムが安全関連系に含まれ得る．その際に人間の操作性を含めた環境をいかに考慮しているかが該当する規格の安全要求事項として策定されつつある．

この動向に対し，環境の認識アルゴリズムでは環境の外乱に対する耐性，制御アルゴリズムでは使用者の操作特性を含む環境外乱に対する制御系の安定性がそれぞれ評価されることになるであろうが，いずれもを満足に満たす研究報告はなされておらず，未開拓な領域である．

このように，ロボットが1）いかなるヒューマン・インターフェース情報を管理し，2）想定される環境のいくらほどの外乱の中で，3）どの程度複雑なタスクの遂行を要求されるかが，今後ソフトウェア機能安全の対象となると想像される．これらの3因子は，実は自律の程度を表わす次元[11]であるとされていることに気づくことは重要である．つまり，これらを同時に考慮して，ロボットの「使用上の制限」や仕様を決定することが重要なのである．

例えば，人間による操縦を前提とする搭乗型ロボットの場合でも，自律化をある程度導入する必要がある．しかし，レーザースキャナーを用いた人間の検出技術は，現行該当規格に見られる技術的な制約から，速度情報を安全関連に属する（高信頼な）データとして利用することはできない．しかし，環境の複雑さや操縦性を考慮しつつ，自律化の程度を状況に応じてうまく設定すれば，多くの場合リスクを回避できるソリューションを見いだすことは可能である．

4.4 開発段階からどのような安全技術を導入するか

開発段階において，次世代ロボットの有用性を示し生産性を評価する実証試験は，ロボットの市場創出性を見積もる上で，極めて重要な役割を演じる．そこで，文献[12]で筆者は，実証試験を安全技術構築の観点から3段階（第1次～第3次）に分けて，段階的にどのような安全技術を導入していくのがよいかの議論を行った．

すなわち，第1次の研究段階における実証試験では，ロボットの有用性検証を最も重視し，周到な安全管理と緊急停止装置など最低限の付加保護装置の搭載によって，リスクの顕現化を抑える方策にとどめる．第2次の実証試験に向けては，第1次実証試験の結果に基づき，リスクアセスメントのレビューを行うと同時に，4.1節での検討に基づいて，妥当な安全要求仕様の策定を行う．並行して，認証機関とのコンタクトと，安全に関する要素技術開発も始める．第3次実証試験に向けては，先に定めた安全度水準を達成する目的で，機能安全を中心とした第三者機関による安全認証を見据えた安全技術の装備を行う．

5 おわりに

以上，本稿では，人間と物理的に共存して彼らに直接・間接にサービスを行うことができる，次世代の産業を創出すると期待されているロボットの安全技術に関する基本事項と現状動向を取り上げ，メーカーによる課題への取り組み指針に言及した．すなわち，安全技術の設計原則に関するリスクアセスメントと導入的な説明，次世代ロボットに関する安全技術の特徴，さらに，同技術の課題とこれらに対するメーカーの対策指針について述べた．

昨今は，持続性社会の到来要求とともに，生産性よりも，安全性，信頼性，忠実性などディペンダブルな品質を個々の製品に求める声が大きくなってきている．メーカー自体も「安全は最低のコストで」とした一昔前の意識からは脱しつつあると現状を推察するものである．

安全技術の導入努力は，自ずと幅広い技術視野をもった次世代を担える技術者の育成に結実する．安全工学という，実はロボットとは隔たりのある分野の技術領域を取り込むことによって，リスクとベネフィットの両方を考慮しながら製品開発に取り組むことができるようになる．折しも，2009年度から5年間の国家プロジェクトとして，安全技術のための社会構造構築を目指した（独）新エネルギー・産業技術総合開発機構「生活支援ロボット実用化プロジェクト」が進行中である．これは，パナ

ソニック（株）を含め25機関でコンソーシアムを構成し，その中で参画機関相互の交流を密に行ってきている．これに加えて，さらに総数223機関で構成される日本ロボット工業会ロボットビジネス推進協議会へも情報展開が進められている．このように，ロボット分野において，さまざまな立場の技術者の間で安全技術に関する感心が高揚してきていることを喜ばしく感じる．筆者は，国際安全規格作りにも取り組んでいる立場にあるが，まず読者の方々におかれては，上記協議会や同規格国内対策委員会のコミュニティにぜひ関心をもって，あるいは参加していただき，より幅の広い技術知見を収集して，今後の製品開発に役立てていただきたいと願う次第である．

参考文献

[1] ISO 12100, Safety of machinery—General principles for design—Risk assessment and risk reduction, 1210.

[2] ISO 13849-1, Safety of machinery—Safety-related parts of control systems—Part 1: General principles for design, 2006.

[3] IEC 61508-1, Functional safety of electrical/electronic/programmable electronic safety-related systems—Part1: General requirements, 2010.

[4] ISO 10218-1, Robots and robotic devices—Safety requirements for industrial robots—Part 1: Robots, 2011.

[5] ISO/DIS 13482, Robots and robotic devices—Safety requirements—Non-medical personal care robot, 2010.

[6] IEC 61508-5, Functional safety of electrical/electronic/programmable electronic safety-related systems—Part5: Examples of methods for the determination of safety integrity levels, 2010.

[7] Human Tolerance To Impact Conditions As Related To Motor Vehicle Design, Surface Vehicle Information Report, SAE International, J885, 1986.

[8] Y. Yamada et al., “Fail-safe human/robot contact in the safety space,” IEEE International Workshop on Robot and Human Communication, pp.59-64, 1996.

[9] S. Haddadin et al., “Requirements for safe robots: measurements, analysis and new insights,” The International Journal of Robotics Research, vol.28, no.11-12, pp.1507-1527, 2009.

[10] T. Fujikawa et al., “Evaluation of injury level and probability for risk assessment of mobile robots,” ON-LINE Proceedings of THE 7TH INTERNATIONAL CONFERENCE ON THE SAFETY OF INDUSTRIAL AUTOMATED SYSTEMS (SIAS2012), SESSION 5: ROBOT SAFETY, Montreal, Canada, 2012.

[11] H. Huang et al., “Autonomy level specification for intelligent autonomous vehicles,” Interim Progress Report, Proceedings of the 2003 Performance Metrics for Intelligent Systems Workshop, Gaithersburg, MD, USA, pp.1-7, 2003.

[12] 山田陽滋,“実証試験における次世代ロボット安全技術の段階的構築,”第28回日本ロボット学会学術講演会予稿集（CD-ROM）, RSJ2010AC1E2-8, 名古屋工業大学, 2010.

《 プロフィール 》

山田 陽滋（やまだ ようじ）

1980	名古屋大学 工学部 卒業
1983	名古屋大学大学院 修士課程卒業
1983	The University of Texas at Austin Degree of Master of Science in Engineering
1983-1990	豊田工業大学 助手
1990	東京工業大学 工学博士
1990-1993	豊田工業大学 講師
1993-2004	豊田工業大学 助教授
1993	Stanford University 客員研究員
2004-2008	産業技術総合研究所 主任研究員 （知能システム研究部門 安全知能研究グループ長）
2005-2008	筑波大学大学院 システム情報工学研究科 教授（併任）
2008-現在	名古屋大学大学院 工学研究科 教授

専門技術分野：
ロボット学，安全学

主な著書：
ロボットテクノロジー（オーム社，2011）
機械工学便欄（日本機械学会，2007）
新版ロボット工学ハンドブック（コロナ社，2005）