解説

設計工学
Vol. 45No. 11
pp. 521-526

サービスロボットの安全設計
危険源処理の概念と方法論

Safety Design of Service Robot
-Concept and Methodology-

加部隆史*
(Takashi KABE)

1. はじめに

安全とは、安全の用語を定める ISO/IEC Guide 51[(1)]によると、受け入れられないリスクが無いことと定義している。又そのリスクを評価し低減する方法論等の基本概念を定めている。

図 1 に示すとおり危険源(hazard)と人が、同一空間で同一時刻に遭遇した際に、それが危険状態となりリスク(risk)が発生し、これを放置すると危害が発生する確率(リスク)が生じる。放置せずに、危険源を予防概念に基づき、事前に設計段階で除去或いはリスクを低減する事により危害を大方避ける事が可能となる[(2)]。すなわちリスク発生以前の、その要因のひとつとしての危険源がどのように処理されるかが問われてくる。

人工物としてのサービスロボットは本来人に危害を加える危険源を有している。人工物を設計するのは設計者であり、設計者しか設計対象の人工物の危険源は的確に把握できない。それ故、この危険源を処理できるのは設計者であり、又設計者しかいないという事から、そこに設計者としての技術者倫理が存在する。

1.1 機械安全

従来の労働安全は人への教育を重視し、間違いを起こさない為に目標をたてた。これでは、限界があるとして、機械安全では危害のもうひとつの発生要因としての危険源が着目された。機械的・電気的・熱・放射線・人間工学原則の無視等の危険源は、確定的であり因果決定論により、危害を発生させる。病原菌と同様に、放置していても無くならない特性を有している。それ故、人の安全を確保する為に機械安全という概念が新たに生まれ、それは基本的に危険源と人を隔離する図 1 のハウスドルフ空間としての「隔離の原則」並びに機械の危険な動きに人が接近した際に安全なインターロック装置等により駆動源を遮断する「停止の原則」或いは「エネルギ・ゼロの原則」等を中心として達成される。

機械安全の概念は例えば、危険源を同定－リスクの見積－リスク評価－それに基づくリスク低減－残留リスクの明示と、これらプロセスの文書化を求めているリスクアセスメントの原則につき ISO14121[(3)],* そしてリスク低減に関する安全設計の原則については、3 段階方式として第 1 に機械的な本質安全設計、第 2 に安全インターロック装置等による追加的保護方策、第 3 に残留リスクの取扱説明書等への明示が ISO12100[(4)]に定められている。

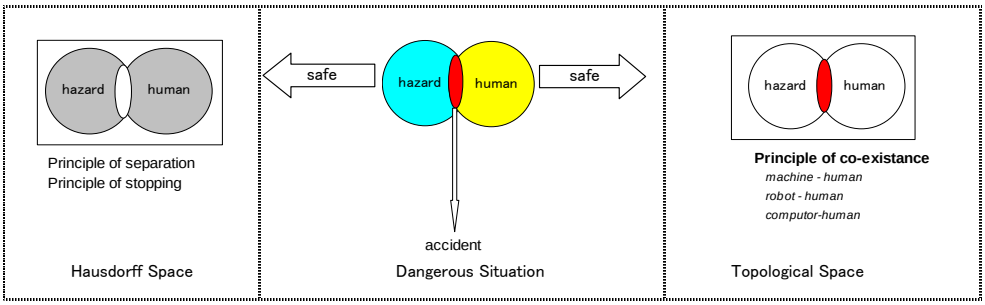

Fig.1 Cause of accident and it's prevention

原稿受付：2010 年 4 月 23 日

*1 非会員，NPO 安全工学研究所(〒167-0054 杉並区松庵 3-39-8) E-Mail: kabe@safetylabo.com

1930 年以降のドイツを中心とした設計論研究のひ

とつの体系としてのポール&バイツの工学設計・体系的アプローチ[5]がある。ここに機械安全の概念を加えたノイドルファーの安全な機械の設計[6]は豊富な図を用いて、機械安全の概念を説明している。

安全設計は、決してそれ単独で主語となるものではなく、本来製品のライフサイクルを配慮した設計論の流れの部分集合であると解釈する事が出来る。

設計論的には、従来の労働安全のように人に頼らず、人が間違えても機械に頼り安全設計を事前に施す事で安全確保する事になり、これは安全達成方法の一つ目のパラダイムシフトとなる。

1.2 人と機械の共存

サービスロボットという概念は未だその産業が幼年期であり、定義づけできる事は出来ないが、それは多くの駆動源やセンサを用いており、れっきとした機械である事には違いない。そして人にサービスを提供する役割を持つ事から、人との接触・共存・協働が機能及びそれによりもたらされる利便性を満足する為に要求される。すなわち図１の本来危険状態である位相空間上で安全を確保する事が要求される。それ故、従来の機械安全の概念としての隔離の原則・停止の原則はサービスロボットの場合、機能を発揮する為には意に反するという事にならないか？その為に、従来の機械類の安全の概念を踏まえた新たなリスク低減方策が必要とされてくる。機械安全の主要な原則が適用しきれない部分については、新たな安全要素技術の開発及び安全達成方法につき「共存の原則」というものが改めて構築される必要もある。

1.3 サービスロボットの安全

サービスロボット特有の安全規格は未制定だが、産業用ロボットの安全性に関する ISO10218[7]において、例えば 80W以下のモータ、150N以下の力、250mm /sec 以下の動きの際には防護策を設置しなくても良い事が定められている。現時点でこの規格は見直しの為審議中で、近い将来に新たな安全関連事項が追加される予定である。

2005 年に開催された愛知万博において多数のサービスロボットが紹介、展示された。その際に、安全専門委員会で定められた安全原則は、ISO/IEC Guide 51 の精神に則り、リスクアセスメント(ISO14121)を実施し、その結果に基づきリスク低減(ISO12100)を実施し、残留リスクの管理を展示者に委託するという事であった。サービスロボットに適した安全要素技術が世界的にも殆ど未開発の為、機械設計による本質安全設計を中心にする事が強調された[8]。

2. リスクアセスメント

対象とする機械の使用制限を明確にした上で、事故の要因のひとつとしての危険源を同定し、それに伴うリスクを見積・評価し、その結果に基づきリスク低減を実施する事が ISO14121 で求められている。

サービスロボットの安全については、具体的なリスク低減手法としての安全設計を開始する前に、図２の ΔR1 に示す通り充分に対象のサービスロボットが、誰を対象として、何処で、どのように使用されるかの使用制限を厳密に行う事が、先ず安全設計を実践する前にリスク低減の効果として期待される[9]。すなわち、これは技術的方策を講じる前の段階におけるリスク低減の有効な手段となる。

そのリスク制限結果に基づき、初めて事項に述べるリスク低減方策が設計的に要求される事になる。

例えば、国内で開発され既に市場に適用されているある巡回ロボットの場合、昼間はあらゆる人たちが行き来するショッピングアーケードで案内ロボットの役目を果たし、夜間にその建物から一般消費者が立ち去った後巡回の役目を果たすという二つの全く異なる機能を有している。一台二役で利便性は高いが、リスク対処方法がこの場合全く異なってくる為、これを概念設計として事前に充分に評価し、その結果詳細設計をする事が合理的となる。

すなわち R2 の対象となる人、R3 の場所、R4 の時刻の３要素の複合関係が、直接リスクの度合いに係わってくるという事である。産業用ロボットは、R3:工場という隔離空間、R2:教育を受けた作業者という制限の元で作業が行われるが、一般消費者を対象としたサービスロボットの場合は、その制限範囲が一般的に広くなる。それ故、この段階でのリスク評価が極めて重要となる。

おりしも国内の労働安全衛生法第 28 条の２では、事業者は危険を調査し、その結果に基づき方策を講じる事が述べられている。前者の危険の調査は、リスクアセスメントに基づく事故の予見可能性、後者は危険源を除去或いはリスクを低減する事であり、これは事故の結果回避可能性を意味している。すなわち、事故がおきた際には、因果決定論による危険源の存在及びそれによりもたらされる事故の潜在的可能性を認識していたか、そしてそれを事前に回避する設計手法が適切に講じられたかが問われてくる。労働安全衛生法の本条項並びに機械類の安全に係わる国際規格は、これらに対する説明責任を全うする事を可能とする手段である。

3. リスク低減

リスクアセスメントの結果に基づき、相応なリスク低減が必要となるが、その方法論は安全な機械の設計に関する基本原則 ISO12100 に定められている主として確定的危険源に対する設計方策となる。

本規格で特筆すべき事は、この方法論を 3 段階方式で示している事である。すなわち、これは図 2 の ΔR2 に該当するもので、

1) 機械的な本質安全設計（センサ等に頼らない）
2) 追加的保護法策（防護策やセンサ等を使用）
3) 残留リスクの使用者への情報提供（銘板表示や取扱説明書への記載事項）

であり、これは同時に設計の優先度を示している。

但しそれ以外に多くの個別設計原則が本規格に含まれているが、概ねこれらは機械設備を対象としている為に、必ずしもサービスロボットに適用しきれないものが多い。

ISO/IEC Guide51 では、絶対安全というものは有り得ないとしており、リスク低減後でも機械の機能と利便性を発揮する為に、残留リスクを定めており、機械使用者がその扱いを適切にする事が求められている。これは図２の ΔR3 に該当する。

一般消費財などでも、取扱説明書に明記される危険・警告・注意等は、残留リスクの適切な管理を求めており、とりわけ機械安全特有の概念ではなく、本来残留リスクという概念は上記の理由から、一般消費者にとって馴染みのあるものである。

新技術であるサービスロボットでは、第 2 段階の追加的防護方策を講じようとしても、安全センサ及び安全コントローラ等適切な安全要素技術が未だ殆ど開発されていない。それ故、第 1 段階の本質安全設計において、機械設計の段階で、極力人と接触しても痛くない、危なくないサービスロボットを設計する事が求められてくる。実際に発生しうる危害の状況はロボットの形状・寸法・質量・駆動力等による異なってくる。サービスロボット用の本質安全設計の手法は、規格などで現段階では明示されておらず、サービスロボットの特性並びに各種エネルギをどう抑制出来うるかを、個別に検討するしか無い。

全体的にはニュートンの運動法則 ma=F の相関関

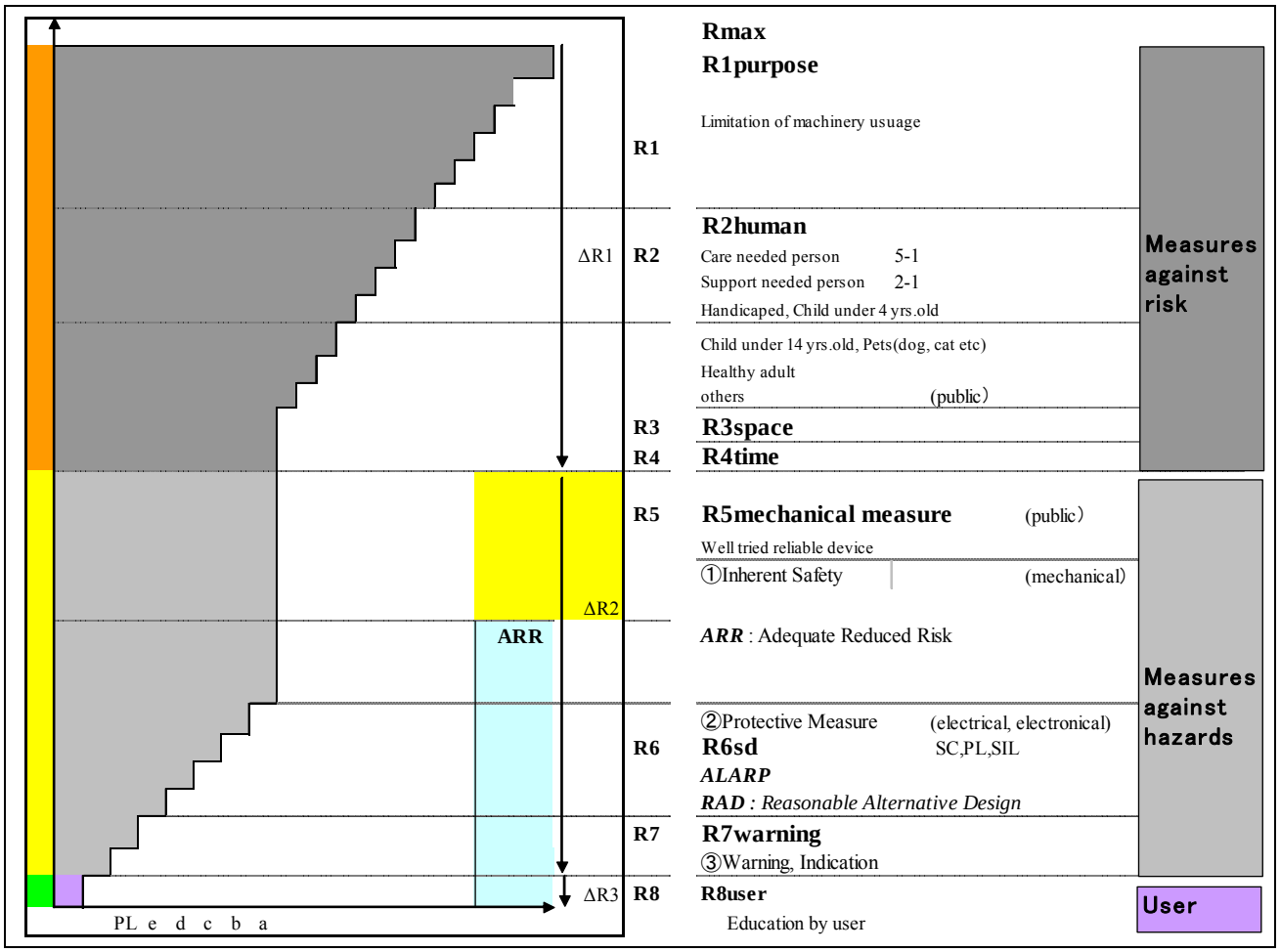

Fig.2ΔR: Limitation of machine-use and 3 step-method of risk reduction

係の人への作用において重大な危害が発生しない事が理想的と言える。そして発生するFが人に危害を与えない程度であれば、例えば機械安全で定める安全インターロック装置や安全制御までは必要となくなる為に、本質安全設計は大きな利点をもたらす事ができる。そのほか、ロボットの形状によるはまされ・巻き込まれ・突っつき等の箇所の処理が必要とされる。

安全要素技術として重要なソフトウェアの安全性に関する機能安全規格 IEC61508 シリーズ[10]は、第三者認証を実施する事が市場の要求事項となっているが、幼年期の産業で大量生産形態にいたっていないものに適用するには、認証に必要とされる期間と費用が大きな欠点となってくる。それ故、機能安全規格の適用は、それなりの量産体制が整った際に実践する方が、望ましいと思われる。

4. 安全達成の目標目安

その次に、リスク低減は何処まで行うべきかという疑問が生じてくる。前述のリスクアセスメント及びリスク低減という国際規格に定められた方法論は最低限配慮の上実践する事により、科学及び技術の知見(state of the art)に適合している事となり、万が一の事故がおきても機械設計者は、やるべきことを事前に実施した事の説明責任を果たす事が可能となる。

機械類の安全関連規格及び不法行為法における3つの基準を以下の通り説明する。

4.1 ARR:Adequate Reduced Risk

ARR は ISO12100 及び制御関連部の安全に関する ISO13849 -1[11]に定められた「適切に低減されたリスク」を示す。これは、ISO12100 に定める 3 段階方式により、機械的及び制御的リスク低減方策を講じた後に残る残留リスク情報を使用者に提供する事により達成される。すなわち、これらの規格及びそれらの引用規格に基づき、そこに示されている技術的リスク低減方策を配慮したか否かが問われる。

4.2 ALARP(As Low As Reasonably Practicable)

ALARP(アラープ)は、ソフトウェアの安全性に関する IEC61508 の第 5 部でアラープ原則及び許容可能なリスクが説明されている。この概念はイギリス安全衛生庁 HSE が提唱したもので、出発点はプロセス産業におけるリスクを取り扱ったものである。ALARP 概念は、4.1 項のような技術的方策よりも、以下に述べる費用便益分析とリスク概念に基づいている。

4.3 RAD: Reasonably Alternative Design Standard

RAD は「合理的代替設計基準」と呼ばれ、従来のアメリカ法律協会が編集した 1965 年の第 2 次リステイトメントによる無過失責任を基盤とする消費者期待基準によるその主観性の問題を改善し、1998 年の第 3 次レステイトメントにより図 3 に示す通り、リスク効用基準が採用された事による。ここでは製造物欠陥を 1)製造上の欠陥 2)設計上の欠陥 3)指示又は警告上の欠陥と区別した。これにより、消費者期待基準に基づく無過失責任は、影が薄まった。

RAD は、代替設計案を採用して得られる便益とそれを採用する事に伴う費用を比較し判断するもので、法と経済学の概念及び費用便益分析(CBA)の基準となるハンドの定式(B<Pl) [12]、すなわち実際に発生する損害(L)とその確立(P)よりも負荷(B)は少なくて良いという考え方に基づいている。逆に、技術的に可能でかつ、その実践が合理的な費用の範囲でそれを実践しない場合は、過失を問われやすくなる。

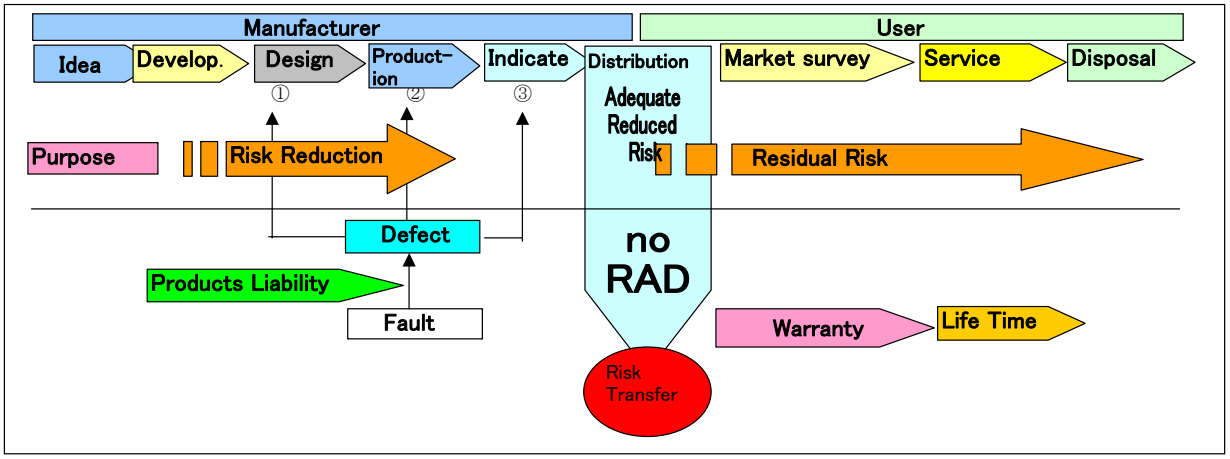

Fig.3 No RAD as a consequent of prevention measurement

アメリカではこれに基づく判例が数多く存在している。

ARR により事前に技術的方策が講じられ、それが ALARP の範囲におさまっていれば、社会はそれを受容するようになり、同時に RAD 基準によれば、合理的代替設計が無いという事になり、設計者の過失は問われないという事になる。

5. おわりに

人への危害は危険源と人が同一空間・同一時刻に共存する危険状態において、それを放置する事により発生する。従来の労働安全は人への対処を重点とし、機械安全は不可逆性を伴う危害の要因として因果決定論に基づく危険源への方策をリスクアセスメントの実施として強調してきた。これが、一連のリスクベースド・アプローチ(Risk Based Approach: RBA)である。

これは、設計者が危険源を適切に処理していれば万が一の事故が発生しても、社会に有益な人工物を提供する設計者をその利便性の観点から社会が守ろうとする思想が背景にある。例えば、何年か前にオーストリアのカプルーンでケーブルカーの火災が発生し、乗客 150 名以上が全員焼死した大事故があったが、その後の事故調査で、ケーブルカーの安全装置は適切であり、ケーブルカーの運用上の安全管理は適切であったとして、機械の設計者及び使用者は過失を問われなかった。日本の場合、誰が悪いと犯人探しをするが、RBA の場合、安全技術とその管理が適切であったかが、第一義的に問われる。社会に役立つ人工物を作り出す技術者を尊重する社会であると言っても良い。

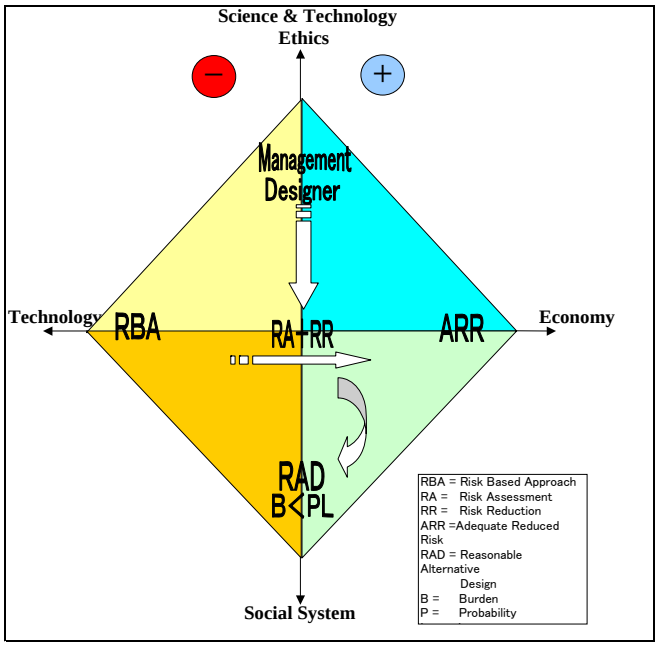

Fig.4 Four factors on safety

サービスロボットは、危険源を多数有する機械として人と共存する危険状態で機能及び便益を発揮する事が条件となる。それ故、これは安全のパラダイムシフトとなるが、従来の安全原則と提示されているリスクアセスメント及びリスク低減に関する方法論のうち適用可能なところを実践する事で、サービスロボットの安全は達成される。本論では、その方法論とリスク低減を何処までやるかの基準も示した。

具体的には、個々のサービスロボットの設計者がこれら方法論を適用し、危害を最小限に抑え、実践した設計過程を図書により情報開示し説明責任をまっとうできる準備をする事が必要となる。

本稿では、安全技術の観点から何を何処まですべきかの概念を図 4 に示す通り説明したが、新産業としてのサービスロボットが社会に受容され市民権を獲得する為には、技術以外に、倫理・経済・社会システムの安全の四要素を配慮した上で、今後以下の問題点を解決する必要がある。

－不可逆性を伴う危害は取り返しが付かない為に、事故がおきる前に設計段階で危険を処理するという予防概念を技術者の倫理として制度化する。
－安全技術のイノベーションとしての新たな要素技術の開発。
－設計者が実践した安全方策の第三者機関による妥当性確認（認証制度）の確立。
－それを実践する為には、妥当な判断が出来る安全専門家の教育とそれを、学協会の協力を得た上でどう実践するかの検討が必要。
－製品の市場投入後に、安全が確保されているかの市場監視制度の導入。
－設計者による安全を前提として、使用者を含めた全体的なリスクマネジメントの導入。
－その一環としての適切なリスクコミュニケーションの実施。
－サービスロボットの特性として、BtoB(Business to Business)から BtoC(Business to Customer)への転換に並びに顧客満足度の高まり等の観点から、新たなサービス工学[13]の配慮。
－事故がおきた際の補償としての保険制度の確立。
－上記を含め、グローバルな観点からあるべき法制度を踏まえた適切な社会システムの設計と構築。
－日本の場合リスクアセスメントは法律で定められているものの、罰則規定がなく実行力が弱まってしまう事の検討が必要。

ここで述べた大枠の概念が、新規産業としてのサ

ービスロボットの設計に参考となれば幸いである。同時に、安全を担保するためのあらたな社会システム構築につき、今後多くの関係者が協議･協働する必要性があることを申し述べておく。

参考文献

1)ISO/IEC Guide 51: 1999 Safety aspects – Guidelines for their inclusion in standards (1999)
2）Kabe T., Tanaka K. Someya M., Sugimoto N., Safety Design of Machinery, a priori prevention, Journal of JSME Vo.73-734 C, pp.2796-2804(2007)
3) ISO 14121:1999,Safety of machinery – Principles of risk assessment (1999)
4)ISO 12100-1,-2:2003,Safety of machinery – Basic concepts of general principles for design (2003)
5)Paul&Beitz, Engineering Design-a systematic approach, japanese version by The Design Council, Baifukan (1988)
6)Alfred Neudoerfer, Construction of safety machines, Japanese version by Koichi Tanaka, NPO The Safety Engineering Laboratory(2002)
7)ISO10218:2006, Robots for industrial environments-Safety requirements-Part1(2006)
8)Takashi Kabe, Safety Certification of Service Robots, Journal of the Robotics Society of Japan, Vol.25 No.8, pp.1181-1184(2007)
9) Takashi Kabe, Tetsuya Kimura et.al., Safety of Service Robots, Basic Consideration on Methodology of Risk Reduction-ΔR., Journal of Japan Society of Mechanical Engineers, Vol.75,No.754, pp.1812-1820(2009)
10) ISO61508:Functional Safety of electrocal/ elec tronic/ programmable electronic safety-related systems (1999)
11) ISO13849-1, Safety of machinery-Safety-related parts of control systems(2006)
12) Takashi Kabe, Koichi Tanaka et.al. Criterion for the Validity of Safety Design of Service Robot-Critical Hazard(CH) and Reasonably Alternative Design(RAD) Standard, Journal of Japan Society of Mechanical Engineers, Vol.75,No.758,pp.2837-2845,(2009)
13) Y. Shimomura: Service Engineering: background, basis and growth - Innovation with high-level integration of manufacturing and service development, 2nd National Workshop on Functional Products Development and Sales, Lulea University of Technology / Vinnova, 2007.

1952 年生まれ、ドイツでの企業コンサルタント活動の後、1986 年より技術系ドイツ企業の日本国内での会社設立を複数実践し、2002 年に NPO 安全工学研究所を設立、代表理事に着任し現在に至る。2010 年 4 月より、日本機械学会産業・化学機械と安全部門部門長。