

機械安全におけるリスク低減に関する概念整理

—労働安全と機械安全・電気安全・制御安全・機能安全—

か べ たか し†
加 部 隆 史†

生産現場での人への危害は機械の危険源と人が同居し発生する。従来の労働安全は人に依存し、作業者の安全を確保するために、主として作業者への教育を重視し、事故が起きると作業者の不注意とされることが多かった。機械の確定的危険源にアプローチし、危険源を除去あるいはリスク低減することで安全を達成しようとするのが、機械安全の基本であり、この場合、事故が起きても人を責めないことが原則である。この機械安全におけるリスクベースド・アプローチの方法論も近年拡大・進歩しているために、グローバルな観点からこれらの概念ならびにそれに関連する安全要素技術の現状を整理し、時代の要求に則した対応が、各ステークホルダに求められてくる。隔離の原則・停止の原則に加え、これから人と機械の協働を実現するためには、新たに共存の原則というものが必要とされてきているが、基本は予防概念としての安全設計を適切に低減されたリスクまで事前に行い、機械設計者がやるべきことを成した後の残留リスクによる事故は社会が許容し、被災者は保険により救済・補償されるということである。科学技術の進歩に応じた社会制度の整備も必要とされる。

キーワード：労働安全，機械安全，電気安全，制御安全，機能安全

1. はじめに

従来の人の注意に頼る労働安全に対し、人は間違え、機械は壊れるという前提で、機械の確定的危険源を人と隔離、あるいは機械の危険な動きを停止することにより、人と機械が同一空間・同一時刻に共存しない条件を育成するリスクベースでの機械安全の概念が近年普及してきている。

最近の調査によると、危険源から演繹される危害は、重大な労働災害に関するデータベースでの解析結果によると、事前に機械安全の予防概念を適用することにより、本来は8割以上が未然防止可能であったとしている¹⁾。

安全の原理²⁾において安全を確保するために機械の駆動源に対し、制御的には非対称故障特性を有するインターロック構造を適用することにより、工学的に安全制御に人の判断を含まないことが論理的に証明され、同様の概念は機械類の安全に関する欧州機械指令と安全な機械のみ流通するCEマーキング制度の実践課程の方法論として適用・実践されている。

この基本概念は、機械設計者を対象とし機械安全という包括的な意味あいのほかに、実際のリスク低減に当たっては、機械設計を中心とした本質的安全設計、電気および電源管理等に関する電気安全、安全デバイス等に関する制御安全、そしてソフトウェアの安全性に関する機能安全に区分けされ、実際にはこれらのリスク低減方策が適用されても、絶対安全は存在しないために、リスク評価の結果としてのリスク低減後の残留リスクに関し、実際の機械使用者は従来どおりの人に対する教育等を柱とした労働安全での補完をもって、初めて安全は確保される。

本稿では、これらの概念整理に始まり、現実の事故の要因に焦点を当て、機械設計者にとっての安全技術の適用可能性と限界および課題を述べ、残留リスクの使用者側にとっての管理の必要性を明確にすると同時に、安全を取り巻く環境から今後の課題を提案する。

2. 事故対策としての機械安全概念の発展

機械安全に関する国際規格は、これまでの制定過程から、その実践適用に伴う新たな問題を解決するために恒常的に進化しており、国内で初めて機械安全の概念に取り組む際に、多岐多様にわたり理解が伴わない場合が多くなってきている。そのために、つぎのよう

† NPO 安全工学研究所：〒167-0054 東京都杉並区松庵3-39-8

E-mail: kabe@safetylabo.com

に概念を整理する。なお、その出発点として ISO/IEC Guide 51³⁾ に安全に関する用語の定義ならびに哲学が述べられていることを言及しておく。

2.1 事故要因と隔離の原則・停止の原則

労働現場での危害は、図1のベン図が示すとおり危険源（機械）と人が同一空間にかつ同一時刻に共存するという二つの AND 条件が満たされて初めて発生する。リスクという概念は流通後に、危険源と人が同居して初めて発生するものであり、それゆえ機械の流通前に、確定的危険源に対する方策が必要ということになる。流通後に対応しても、不可逆性を伴う危害の場合、すでに手遅れであり、失われた人体の一部あるいは生命は戻らない。そのために、機械設計者が危険源の同定を行い、リスクを見積もり、評価した結果に基づき、リスク低減を実施することが、リスクアセスメントの原則⁴⁾ および設計に関する安全の一般原則⁵⁾ に予防概念の方法論として国際規格と同時に JIS に定められている。

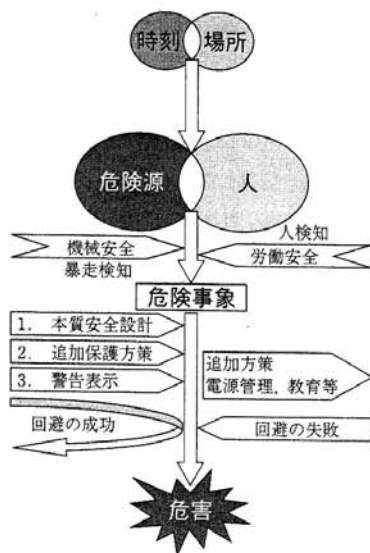


図1 危害の要因と回避

すなわち、① 危害の要因としての危険源と人の共存を回避するための防護柵等による「隔離の原則」ならびに、② 機械の危険な動きに人が接近した際に、人の意志と無関係に安全なセンサ等で電気の駆動源を停止するフェールセーフなセンサ等による「停止の原則」および、③ エネルギーの放出とエネルギー・ゼロの状態維持を確実にする「エネルギー・ゼロの原則」（アメリカでは ZMS：zero mechanical state）の実践が、適切なリスク低減過程で要求される。

2.2 国内の状況

国内で 2006 年に労働安全衛生法第 28 条の 2 が施行され、事業者は「危険性又は有害性の調査を実施し、その結果に基づく方策を講じる」ことが求められるようになった。これはまずハザードを特定するという欧

米諸国で定着している機械安全の概念に基づきリスクアセスメントを実施し、その結果に基づきリスク低減を実施することを意味しており、従来の人の教育を中心とした国内の労働安全に対し、事故要因を人ではなく、危険源に求めるというリスクベースド・アプローチ（risk based approach：RBA）による安全のパラダイムシフトを意味している。

すなわち、本来 RBA の場合、事故が起きた際に従来のように犯人探しをするのではなく、確定的な危険源に伴う事故の原因を解明し、それに基づき機械設備に過失要因があったか否かを調査する方法となる。

これを受けて、2007 年に改定された機械の包括的な安全基準に関する指針およびその解説はリスク低減方法につき、WTO/TBT 協定の取り決めに則り、国際規格と整合された JIS を引用しており、この RBA の基本的事項は、国内でも国際規格を引用することなく、すべて日本語で説明することが可能となっている。

さらに、2008 年に施行された労働契約法第 5 条では、安全配慮義務が明記され、現在事業者は、例えば事故が起きた際に、作業者の安全に対する配慮義務をまっとうしたかを説明する義務を担っていることになる。

しかしながら、労働安全衛生法の対象はあくまで事業者であり、機械の設計者は直接対象となっていない。危険源を処理する設計者の責任が不在のまま RBA を実践しようとしても限界があり、当初は事業者が調達する機械へリスクアセスメントを実施し、その結果を機械とともに納品時に提出することを求めることが現実的である。事業者は、提出されたリスクアセスメントの内容につき妥当性を判断できることが本来の姿である。

実際にはこれまでの労働災害統計によると、国内での死亡事故の要因の 3 割を占める挟まれ・巻き込まれは駆動源と人が共存する危険状態から発生している。そしてそもそも労働安全衛生規則に歴史的に労働現場における機械の危険源およびその対処方法が示されており、これらの危険事象は機械安全概念が導入されたとしても機械の使用者側での電源投入・再起動という人の行為に頼るところで発生する。挟まれ・巻き込まれ対策として、電気安全の基本（ZMS）として使用者側での電源管理を徹底的に実践することが本来急務である。

2.3 ドイツの状況

欧州の場合は、1993 年に導入された CE マーキング制度による機械設計者の製造者責任があり、基本的に機械設計者は機械の流通時にその機械が安全であることを自己宣言し CE マーク表示により明示することが

求められている。

ドイツは数年前のドイツ職業保険組合 HVBG の「安全機器の無効化状況に関する実態調査」⁶⁾の結果、調査対象事業所のおよそ3割が、安全装置を無効化しているという深刻な実態がその報告書により明示された。かつ、事業者責任を担う経営陣がその実態を承知しているということである。無効化の主要因として上げられたことは、第一に生産性である。

すなわち、欧州機械指令が求める「隔離の原則」および「停止の原則」では部分的に機械の機能性あるいは生産性に悪影響を与えるということである。それを改善する方法は、機械を囲み・止めるという当初の欧州機会指令の限界を示しており、法制度の改善および各種安全要素技術の開発が必要とされるが、現在でもおおかた実験段階から実践段階へ移行中である。

2.4 共存の原則

機械の機能性や生産性を維持するには、これまでの「隔離の原則」および「停止の原則」では部分的に限界がある事から、将来に向けてのパラダイムシフトとして、状況に応じ人と機械の協働を認める「共存の原則」(図2参照)が検討される必要がある。すなわち、危害の構成要素である危険源と人がつねに共存するという、図1における危険状態(リスク)が常時発生しているために、ここでは隔離および停止ならびにエネルギー・ゼロの原則はおおかた通用しなくなる。ドイツでは、欧州機械指令の改正、それを実現するためのセンサ・エバリュエーション・アクチュエータというエネルギー・情報伝達系にかかわる安全の要素技術の開発、そしてさまざまな実証試験が実践され、一部実用化され始めている。

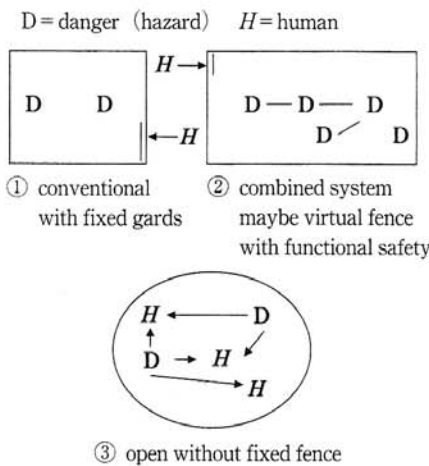


図2 隔離の原則から共存の原則

例1：マシニングセンタの安全性に関する最新の欧州規格 EN12417 における Mode 4.

例えば従来の機械安全の概念に頼ると、どうしても機能的に果たせないところが出てくるため、技術的に

解決方法がなく、使用者が同意しそれを文書で機械設計者と取り決めた際には、例えば運転速度などを規格に定めた値よりも速くすることを可能とするものである。速度制御の前提として IEC61800-5-2 に定める安全ドライブシステムがある。同時に、特定作業者に権限が委ねられるために、例えばその作業者はモード切替スイッチに RFID が組み込まれた物を使用する等の対応が必要とされる。

これは、従来の機械にまかせる安全の概念を根底から覆すもので、機械設計者が機械使用者へ契約により危険移転をする新たな危険管理の責任体系である。最新の欧州機会指令 2006/42/EC の 1.2.5 項ではこの可能性を「プロセスモニタリング」として規定している。この背景には、機能を達成するために安全装置を無効化するよりも、使用者側の判断によりよしとした際には、一定の条件を満たした場合、例外的に認めるというものであり、無効化により生じる高いリスクよりもこの方策を適用したほうがリスクは小さいという判断が伴っている。ただしその運用については現時点では、欧州域内で法の解釈が統一されるところまで行き着いていない。

例2：産業用ロボットでバーチャルフェンスを構築する柵なし安全の実践、REIS 社等。

これは、現在の IEC61800-5-2 の安全ドライブシステムにより、ロボットの動きの安全な減速、安全な静止、安全な停止・不意な起動の防止など速度制限と監視が確実に行われるという前提に立ち、3次元のバーチャルフェンスを制御的に構築し、その領域からロボットアームがはみ出すと駆動源が緊急遮断される仕組みである。ただし、この場合、バーチャルフェンス内への人の存在および侵入を監視する安全なセンサが別途該当領域に適用されることが必須条件となる。このロボットが市場に流通し始めたのは、1990年代後半である(図3参照)。KUKA 社の場合は、短軸制御

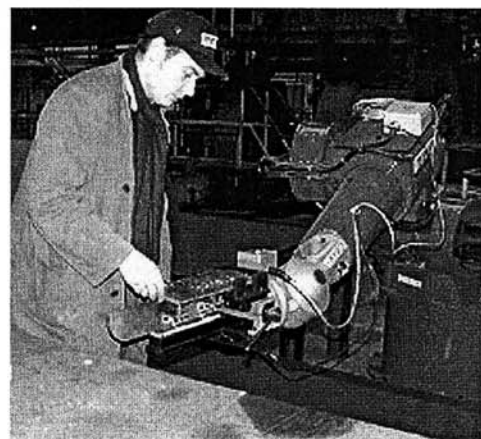


図3 生産現場での人とロボットの協働 (REIS-ELAN 社)

での安全なロボットを市場化している。

例3：安全ライトカーテンのブランキング機能により，加工物が移動する部分をセンサにより無効化し，人と機械の協働を可能とするもので，数年以上前から実践されている。

とりわけ例1や例2は，以下に述べる機能安全規格を前提としている。これらの状況は，従来の隔離の原則・停止の原則から共存の原則という新たな概念への要望と兆候を明示している。

3. 機械安全概念の発展

リスク低減にかかわる機械安全関連の表題の概念を以下のとおり整理する（図4参照）。

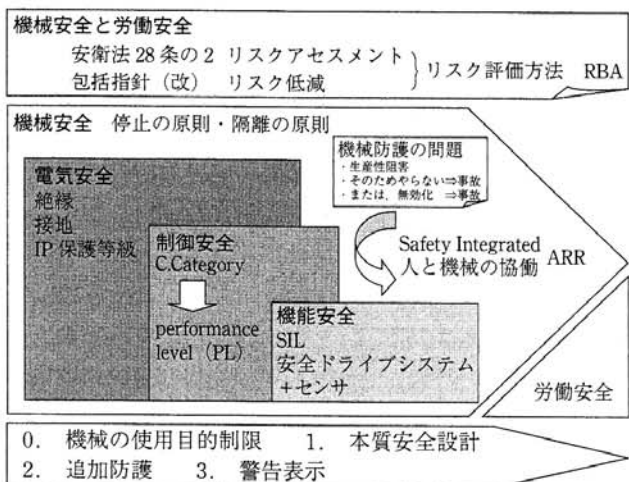


図4 機械安全の概念

3.1 機械安全

前述のとおり，リスクアセスメントの原則⁴⁾，安全のための一般設計原則⁵⁾あるいは，別な表現として隔離の原則，停止の原則，エネルギー・ゼロの原則（電源管理の原則）等を含めた総称。WTO/TBT 協定に基づき，国際規格として機械関連で ISO，電気関連で IEC 規格が，A-B-C 規格として三層構造が体系化されている。主要な規格は，JIS がそれらに整合している。

国際規格はそもそも自由貿易を確保し，障害をなくすための手段として整備されており，技術的には以下の2点の制約に関する認識が重要である。

(a) 規格は妥協の産物（技術水準の制約）

多くの異なる風俗，習慣，歴史，文化，技術水準をもつ多数の国々が共通して使用できるもので，最高の技術にしてしまうとそれに対応できない国々が出てくるため，規格における技術水準は妥協の産物であり，必ずしも最高の技術ということにはなり得ない。

(b) 国際規格の策定には数年必要（時間の制約）

国際規格が成立するまでには，複数の審議段階を得

て整合性を図るため，どうしても数年間という期間が必要となる。安全技術等については，ドイツが国内規格（案）を技術指針として提示し，第三者認証機関がそれを参考にして，製品の安全の妥当性を検証し，認証書を発給する例が多々ある。別の表現をすると，国際規格ができるのを待ちわびて新製品を開発する場合，古い機械の設計しかできないということになる。

リスク低減の優先順位として3段階方式が提唱され

1. 本質安全設計
2. 追加的保護方策
3. 警告表示

が示されている。リスクアセスメントの図書を作成することも要求されている。

3.2 電気安全

感電や火災に対する方法ならびに電源管理手法を定めており，詳細は IEC60204-1 に定められている。電源の停止について，停止カテゴリ 0-1-2 があり，とりわけ惰性回転を管理する際には停止カテゴリ 1 に基づく時間管理等が必要とされる。ZMS に伴うロックアウトは特に重要である。

3.3 制御安全

本質安全設計において危険源が除去しきれない場合，つぎの段階として制御安全による追加的保護方策が検討の対象となる。1996 年に制定された EN954-1 に基づき，制御関連部に対しリスクグラフによるリスク評価を実施し，その結果制御カテゴリ B-1-2-3-4 を選択し，それに応じた適切な安全デバイスの適用により，リスク低減の結果を社会が認める目安とされている「適切に低減されたリスク」(adequate reduced risk: ARR) を実現する。ARR に達する手法は，ISO13849-1:2006 に図式化されており（図4），リスク低減を，最初に機械的，つぎに制御的に行うことにより ARR に達するとしている。

カテゴリ 3 では冗長性，カテゴリ 4 では冗長性に加え自己診断機能画が求められる。

カテゴリ 3 の典型例は，工作機械の主扉，ロボットブースへの入口の扉等で，カテゴリ 4 の典型例はプレス機械等が挙げられる。

従来の確定的な要素に基づく制御カテゴリは不十分との批判から，EN954-1 は，信頼性の概念 MTTFd, DC, CCF 等を配慮し，制御カテゴリはパフォーマンス・レベル：PL a-b-c-d-e へと 2006 年 ISO13849-1 の成立により変更された。同様に，つぎに述べる機能安全の中核となるソフトウェア開発のためのプロジェクトマネジメント手法である V モデルが導入されている。

ISO13849 は機械・油空圧・電気制御を含み対象と

しているが、後述の機能安全は、電気・電子・プログラマブルコントローラのみを対象としているために、それ以外の要素は対象外となっている。

3.4 機能安全

1960年代にジェット機やミサイル制御をベースとしてアメリカで生まれたシステム安全の確率的概念と方法論に、多角的な検討が加えられ、ドイツ国防省により開発されたVモデル等も配慮され、石油化学プラント、原子力、医療、鉄道等の分野での検討も加わり、機械安全でのソフトウェア安全性については、IEC61508が各分野における専門家の慎重な議論の末1998年に成立した。この機能安全規格は全7巻からなり、①技術的要求事項のほかに、②ライフサイクルマネジメントの概念、③専門家の要員認定も視野に入れた包括的なアンブレラ規格で、その難解さ、複雑さから、プラント用ではIEC61511、機械安全用にはIEC62061が別途用意された。安全水準度SIL1-2-3-4が適用されている。機械安全ではSIL4は対象外とされている。なお、機能安全の妥当性に関しては、製造者が第三者機関での認証を実施することが通例となっており、世界的に使用者がほとんどの場合その認証書の提示を要求する。

安全技術ならびにシステム安全の発展段階を図5と図6に示す。図6においては、安全の出発点である労働者の権利、知る権利等基本的人権にかかわる発展段階および国際協定、国際規格等のグローバルな諸要素が示されている。これらの事項については、経済産業省の2006年度の報告書に記載がある⁷⁾。

3.5 労働安全

人に頼らない安全を確保する機械安全の概念は、おおむね危険源を有する機械の設計者をステークホルダ

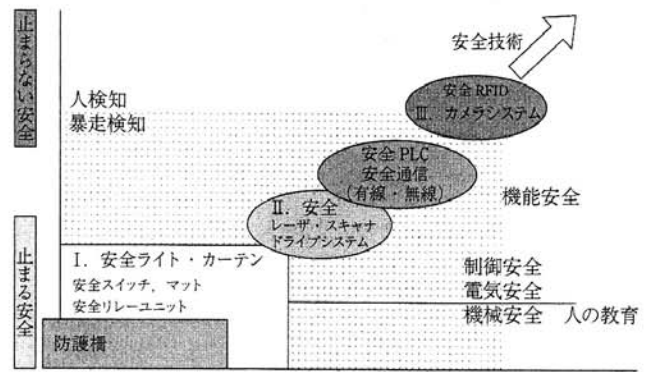


図5 安全技術の発展段階

として定めている。そのため、設計者はリスク評価に基づき、適切な安全方策を実施することが求められ、その結果の残留リスクは危険情報として機械使用者へ流通とともに移管される。それゆえ、危険状態に応じ安全の諸原則や安全の原理を踏まえたフェールセーフなインターロック装置、フールプルーフ、フォールトトレランス(冗長性)等を配慮した安全に設計された機械を使用者が要求し、適切に保守点検、管理運営されなければ、危害につながる。

とりわけ、非常常作業等では、電源が遮断される状態において安全の原理の役割はひととき中断する。その際、作業員が複数の際には、人に頼る機械停止後の再起動時における作業員の安全確保を万全に行わないと、危害につながる。それゆえ、ロックアウト・タグアウト等を配慮したZMSの実践による電源管理を主体とした使用者の残留リスクの管理は、機械安全概念導入後においても、引き続き重要である(図7参照)。

3.6 リスク低減の目安

3.6.1 技術的解釈

械安全規格では当初許容リスク(acceptable risk, cf.

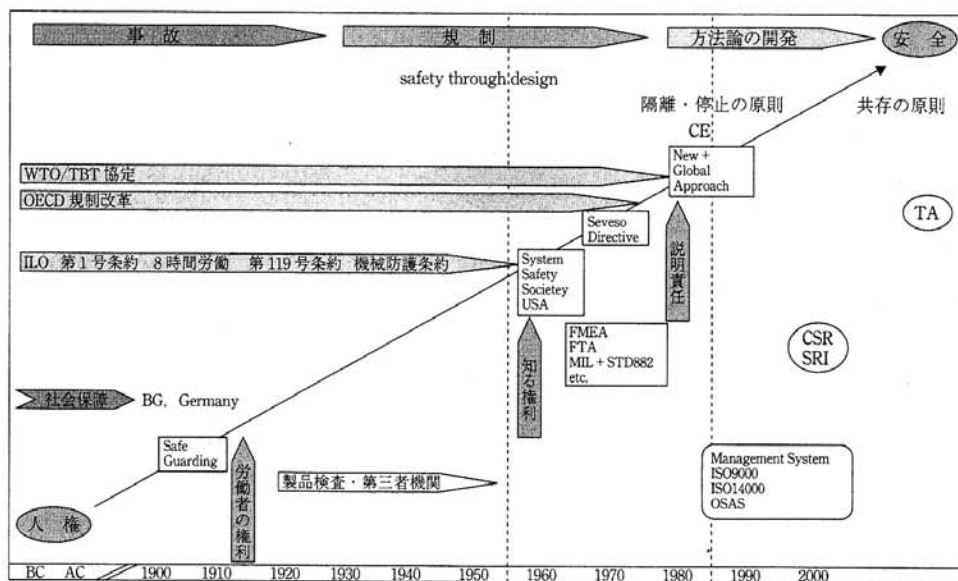


図6 システム安全図

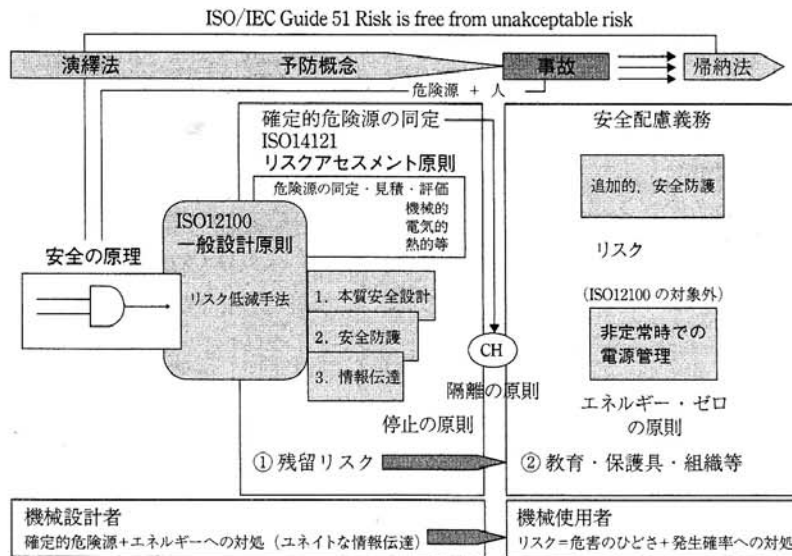


図7 設計者と使用者の関係

ISO/IEC Guide 51 : 1999) という表現が使われ、その後受容リスク (tolerable risk) に変わり、現在 ISO12100-1 では、適切に低減されたリスク (ARR) という表現が使われている。IEC61508 ではちなみに ALARP が引用されている (図8)。ただし ALARP の場合確率論の観点から目標を定めるに留まり、具体的なリスク低減方策との関連付けがないために、ここでは対象外とする。ARR の達成方法は、ISO13849-1 : 2006 で定義され、現段階ではこれがリスク低減をどこまでやるか

の最新の目安となっている。その方法論の実践については、以下の規格がその手法を定めている。リスクアセスメントは ISO14121、機械的リスク低減は ISO12100-1, -2、制御的リスク低減は ISO13849-1, -2、機能安全規格は IEC61508-1~7 である。

3.6.2 法的解釈

製造物責任法において、従来は消費者期待基準。現在は合理的代替設計基準 (reasonable alternative design : RAD) が存在したか否かが問われる (図9)。RAD が存在したか否かについては、基本的に前述の技術的解釈に基づく安全設計が適用されていたかが重要な決定要素となる。

合理的な代替設計とは、一般人が考えても技術的および経済的に達成可能な代替設計を意味しており、それはその時代の技術水準を満たしていることは自明の理となる。

この基準は、設計にかかわる過失に対し従来の消費者期待基準は主観的で、客観的な基準に欠くという批判から永年の専門家の議論を経て、アメリカ法律協会が策定した第3次レストイメントで定められた危険効用基準で、ハンドの定式 $B < P$ に基づき、法と経済学の論理を踏まえた PL 法法理と学説では最新のものとなっている⁸⁾。この基準の転換により、設計の過失は、従来の無過失責任から過失責任へ転換されたという重要な意味がある。PL 法先進国のアメリカでは、この基準が多くの判例において適用されている。前述の機能安全規格に引用されている ALARP も基本的には、この費用便益分析を基準としている。

4. 今後の課題

不可逆性を伴う人体への危害は、事前に演繹的な予

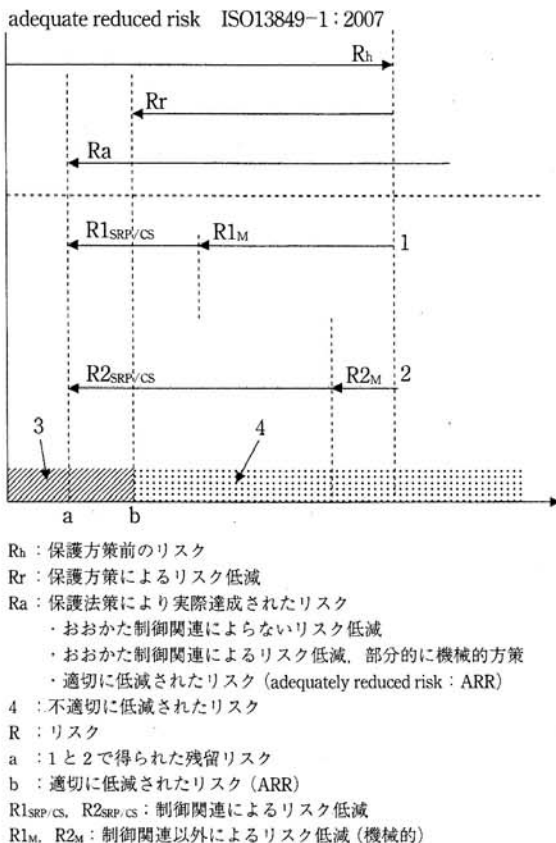


図8 適切に低減されたリスク低減 (ARR)

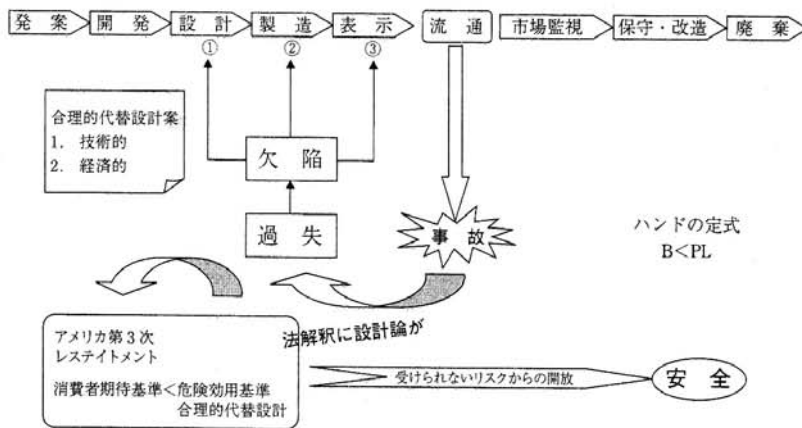


図9 合理的代替設計基準 RAD

防概念としての安全設計を適用することにより、おおかた回避可能であり、それをどうやるかはすでに一連の関連規格で述べられている。これを適用するかは、人工物を創造する技術者いかにあり⁹⁾、技術者は危険源を制御する権限を有している。

品質工学（タグチ・メソッド）あるいは開発管理工学（品質機能展開：QFD）等は、製品が市場に出たからの品質問題にかかわることは大きな損失であるとして、設計段階で、事前にその不確定要素を極力排除する方法論を提示している。その発明者である田口玄一氏は、その方法論の有益性と、結果としての経済的な効果を評価され、アメリカの自動車殿堂入りを果たした。日本発のQFDも現在世界的に、普及活動が行われている。すなわち、日本は品質問題における経済性とのトレードオフの問題を見事に解決して、世界に手本を示した。

環境分野においても、下流の問題解決では追いつかず、上流の設計段階での対処が求められている。このように、人工物を製造・販売する以前の設計段階での予防措置の効用はさまざまな分野で実証されている。

国内では、2.2節で述べたRBAの導入が現状での安全のパラダイムシフトとすれば、電源管理という現実的なこれまでの事故の主要因に対する使用者への徹底した実践を促すことは、ある面では初心への回帰という観点からルネッサンス的な過去へ向かったパラダイムシフトとも言える。

さらに将来へ向かったパラダイムシフトは、情報通信技術の急速な進歩により、ソフトウェアの安全性確保手段が整備されてきたのに基づき、技術的、経済的および社会的問題点を解決するものとして、隔離および停止の原則（止まる安全・止める安全）から人と機械の接触を前提とした共存が望まれてきており、それに伴う安全関連の要素技術が整備されつつあるため、共存の原則というものが新たに定義される必要が出てきている。それを実現するには、とりわけ駆動源の暴

走検知および人の存在・進入検知を安全距離とのかかわりから理想的な反応速度で達成可能な各種要素技術ならびに、共存を可能とする法整備が必要とされる。

同様に日本の場合、国が定めた安全にかかわる分野におけるロードマップでは、欧州の同分野における研究開発の実態ならびに、開発済の要素技術を比較検討すると、必ずしも世界に発信できる状態とはなっておらず、この分野においても大幅な改善が必要とされる。

また、一般人にサービスを提供するサービスロボットが新技術として研究開発され実用化に向けての段階にあるが¹⁰⁾、こちらはつねに共存の原則に基づく安全性確保が要求される。欧米諸国の場合、軍事産業と関連した最先端技術がこれらの分野に適用されている。サービスロボットについての説明は本稿では省略する。

このように、機械安全という概念は多様性を持ち、基本的に、図10に示すとおり以下の構成要素に大別できる。

- ① 倫理 おもに科学技術を制御する技術者
- ② 技術 グローバルな安全設計体系
- ③ 経済 機能性・生産性と安全の均衡



図10 安全の四要素

④ 法 安全を確保するための社会システム

これらは科学技術の進歩に伴い近年恒常的に進化しつつ、これら安全の四要素は相互に密接に関連している。受け入れられないリスクからの開放を意味する安全 (ISO/IEC Guide 51:1999) を実践する際、これらの概念と方法論を正しく理解し、機能性と安全性、生産性と安全性等のトレードオフの関係を整理し、機械製造者、機械使用者、学協会を含む各種団体、そして国等関連するすべてのステークホルダが納得する社会的合意を踏まえた社会制度が必要となる。

さまざまな学問分野と産業界の経験と知識が要求される設計というプロセスを得て、とりわけ安全に関する製品は、第三者機関がその妥当性を検証するということが、欧米諸国では社会制度として、産業革命以来歴史的に定着している。

その第三者機関の多くが、例えばアメリカの FM, UL あるいはドイツの BG 等、同時にその母体が保険会社であり、予防手段としての安全機器の技術的妥当性を検査し、それでも事故が起きた際には、保険で補償 (被害者救済) を行うという RBA を支える仕組みは日本で、おおかた欠如している。とりわけ、将来的に共存の原則が適用されるようになると、そこで重要な役割を果たす帰納安全規格に基づき設計されたソフトウェアは、第三者機関の認証を得ずして産業界は受容しない傾向にある。それゆえ、日本で欠如している認証の仕組みをどうするかという課題を解決することは、すべてのステークホルダにとり急務のはずである。

5. おわりに

従来の労働安全は人に焦点を当てたのに対し、機械安全は危害をもたらす要因のもう一方の要素である「確定的危険源」に焦点を当てている。

このパラダイムシフトは、事故発生の際に、人を責めることから技術的な原因追求をし、RBA の責任体制に導くことにある。

同時に、不可逆性を伴う取り返しのつかない危害を予防するために、安全設計を実施し、事前に問題を除去するという明確な理念に基づき、おおかたの先進国諸国ではすでに実践されている RBA の基本的な考え方である。

これまでの事故を踏まえた帰納的集積としての安全規制や規格で明示されているリスク低減の方法論を、事前に設計段階で適用することにより、技術的には適

切に低減されたリスク (ARR) は達成され、法律的には合理的な代替設計 (RAD) がないことが裏付けされ、機械製造者は、科学技術の負の側面への対処としての製造物責任法における設計過失を問われないことが証明可能である。

しかしながら、安全は機能性・生産性という経済的側面からの制約もあり、それに伴いリスク低減の方法論としての機械安全・電気安全・制御安全・機能安全と安全技術が進化しており、これは隔離の原則から、共存の原則へという将来に向けてのパラダイムシフトを意味している。

急速に進化する科学技術ならびに社会状況に適用し、その負の側面に対し安全を確保し、正の側面に対する社会福祉の増進の均衡を得て、結果として社会的受容を獲得するためには、単に工学の分野のみでは解決できない問題が残存する。そのために、安全を倫理・技術・経済・法 (社会システム) から構成される複合的な学問領域としてとらえ、多角的かつ体系的なアプローチが必要とされる。

工業先進国としての日本は、これまで蓄積してきたものづくりの英知を、これら安全の要素を踏まえて、世界に発信するという未来への責任を担っており、同時にこの期待を多くの国々から背負っている。これら機械安全に関する潮流と背景の理解を踏まえた、今後の発展的な議論に期待する。

参考文献

- 1) 加部隆史, 田中紘一, 染谷美枝, 杉本 旭: 予防策としての安全設計の有効性—事故データベースの解析—, 日本機械学会論文集, 73-734C (2007)
- 2) 杉本 旭, 蓬原弘一, 向殿政男: 安全作業システムの原理とその論理的構造, 電気学会誌, 107-D-9 (1987)
- 3) ISO/IEC Guide 51:1999 Safety aspects—Guidelines for their inclusion in standards (1999)
- 4) ISO14121:1999, Safety of machinery—Principles of risk assessment (1999)
- 5) ISO 12100-1, -2:2003, Safety of machinery—Basic concepts of general principles for design (2003)
- 6) 安全装置の無効化ドイツ職業保険組合 HVBG 報告書, Manipulation von Schutzeinrichtungen an Maschinen (2006)
- 7) 2006 年度 経済産業省委託調査, 機械安全の普及促進事業, NPO 安全工学研究所 (2007)
- 8) 加部隆史, 梅崎重夫: 予防概念の安全設計と製造物責任法との関連性, 安全工学研究発表会予稿集 (2007)
- 9) 杉本泰治: 技術者資格—プロフェッショナル・エンジニアとは何か, 地人書館 (2006)
- 10) 加部隆史: サービスロボットの安全認証, 日本ロボット学会誌, 25-8 (2007)