技 術 解 説 1

国際安全規格の動向と安全確認型システムの概要

佐藤　国仁*

わが国にもいよいよ国際安全規格の制度が導入されようとしている。この制度の特徴は、1）全ての機械に対して適用される、2）信頼性に基づく安全管理から確定的な構造による安全の構築、3）製造者がその責任を負う、というものである。3つの階層に構成される規格体系により、リスクアセスメントを行い、その結果にしたがってリスク低減を実施するという手順および判断の基準が定められる。将来は、全ての機械の製造を、この手順で行うことが必要となるであろう。
リスク低減方策の有力な手法が、安全確認型システムである。わが国発のこの安全理論は、安全システム構築方法を具体的に明らかにする。

1. 機械安全の新しい潮流

機械の安全を構築する原則が大きく変わり始めた。第一に、個々の機械毎に安全規則を定める方法から、全ての機械に対して包括的に安全構築のルールを定める方式への転換。第二に、信頼性に基づく安全管理から、確定的な構造による安全の構築への転換。第三に、機械の安全は、製造者がその責任を負う原則の採用である。

安全を構築する技術に注目すれば、第二の点が特に重要である。従来は、主として機器の信頼性を増すことによって安全性を高める努力がなされてきた。すなわち、確率に基づく安全確保である。しかし、安全を要素機器の信頼性によって実現しようとする限り、必ずいつかは故障して事故に結びついてしまう。しかも、やっかいなことに、それがいつおこるのかは、ほとんどの場合、予測できない。

新しい安全方策は、機器の個別の信頼性によらず、機器の構成によって確定的な安全を構築する。この方策によれば、機器の故障は、機械装置を停止させてしまうが、ただそれだけのことであって、暴走して人を傷つけることはない。機器の信頼性は、機械装置の稼働率、運転性能には大いに影響を与えるから、もちろん無視して良いものではない。しかし、安全の観点からは、考慮しなくてもよい特性となった。

確率による安全と、確定による安全を表す事例として、図1に2種類の制動装置を示す。a)では、電源、配線、ソレノイド等、制動装置に係わる全ての機器が正常に働いたとき初めて、所定の制動力が発生する。一方 b)では、これらのいずれの機器が故障しても、不要時に制動が掛かることはあっても、必要なときに制動が掛からないことはあり得ない。

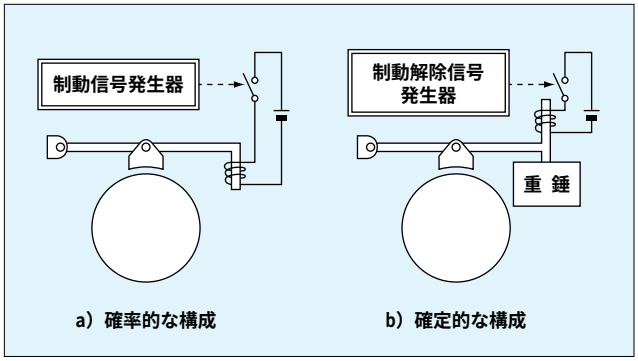

図1　制動装置

このように、確率的安全と確定的安全を定義すると、表1のような得失が明らかとなる。確率的安全では、システム全体の信頼性の厳密な評価は非常に困難で、特に一般民生品において、十分な信頼性設計を行うことは多くの場合困難である。そのため、十分な信頼性設計を行っていないことを理由に、直ちに製造者の責任を追及できるものではない。また、管理者に対しても、複雑な機械装置の全ての要素の点検の確実な実行を求めることも、非現実的である。こうして、本来の責任の所在も不明確となってしまう。

表1　確率的安全と確定的安全の対照

	確率的安全システム	確定的安全システム
事故発生	いつかは事故が発生する。 いつ発生するか分からない。	機械の予期せぬ停止はあるが、事故は発生しない。
責任	責任の所在が不明確。 無責任になりやすい。	責任の所在が明確。
限界	安全性の限界が不明確。	安全性の限界が明確。
成果	投資の成果が不明確。	投資の成果が明確。
適用対象	機能を確保しなければならない（機械の運転と人の接近の双方を止められない）場合は、確率的に安全を確保するしかない。	機能の停止が可能（機械停止可、人の接近阻止可）であれば、システム構築は可能。
事例	航空機 介護ロボット	多数の機械（例：工作機械、産業用ロボット） 鉄道（衝突防止）

＊安全技術応用研究会

一方、確定的安全の場合は、機械の使用方法を定め、そこにおいて生じるであろうリスクに対応して安全設計を行うので、そこに組み込まれる安全システムの限界を明確に定義しやすい。そして、安全システムの設計の妥当性を客観的に評価することも可能であり、製造者の責任の有無を判断することも容易となる。

さて、現実に使用されている機械には、停止することで安全を確保できる機械と、ひたすら運転を続けなければ安全を保持できない機械とがある。そして、前者の機械に対しては確定的安全を組み込み、後者の機械に対しては信頼性に基づく安全を適用する、という考え方が新しい機械安全の潮流である。

この技術が適用されることによって、包括的な安全基準の設定が可能となり、責任の所在を明確にすることも可能となるのである。以下に述べる国際安全規格も、安全確認型もこの考えに基づいて、安全の構築を行う。

2. 国際安全規格の動向

2-1 欧州における機械安全確保の歴史

機械安全の新しい流れを理解するには、EUの機械安全の取り組みの歴史を知る必要がある。

第二次大戦後、欧州は経済統合による巨大な共同市場の創設を目指し、着々と準備を進めてきた。共同市場を創設するには、物の自主流通が保証されなければならない。ここで生じた大きな課題が、機械類についてその安全性に関する法規が加盟国毎に、またその分野ごとに大きく異なっていることであった。

EC閣僚理事会は当初、機械ごとに個別の安全基準の設定を試みたが失敗に終わった。この経験を踏まえて、1985年、ECは新しい方法を採用した。「技術整合化と規格へのニューアプローチ」に関する決議を採択したのである。

その特徴は、次の通りである。

(1) 個別機械それぞれを対象とせず、機械類全体を包括的に対象とする。
(2) 構造、仕様等の安全達成の手段を具体的に規制するのでなく、安全達成の必須要求事項を示すに留め、達成方法は製造者が定める。
(3) 製造する機械が必須要求事項へ適合していることを宣言し、その証としてCEマーキングを添付することを、製造者に強制する。

こののち、欧州標準化機関の規格であるEN規格を、欧州各国はその国家規格に採用することが義務づけられる。そして、機械安全の包括的な規格が続々と誕生し、運用されることとなったのである。

機械安全に関するEN規格の実績を踏まえ、ISOおよびIECは、EN規格をそれぞれの規格原案とすることを決めた。

そして、WTO-TBT協定（技術的障害に関する協定）により、各国の国内規格は、ISO、IEC規格に整合しなければならない。このような仕組みによって、欧州の機械安全制度は、グローバルスタンダードとなった。JISにも、新しい機械安全の規格が続々と導入され始めている。

2-2 国際安全規格の体系

国際安全規格の体系は、ISO/IECガイド51に規定されている。図2に示すように、3つの階層構造を備える。

(1) 基本安全規格（A規格）
全ての機械類で共通に適用できる概念を定める。
(2) グループ安全規格（B規格）
機械類に共通の仕様を定める。および、機械類に共通の安全機器について定める。
(3) 個別製品規格（C規格）
個別の機械についての安全基準を定める。

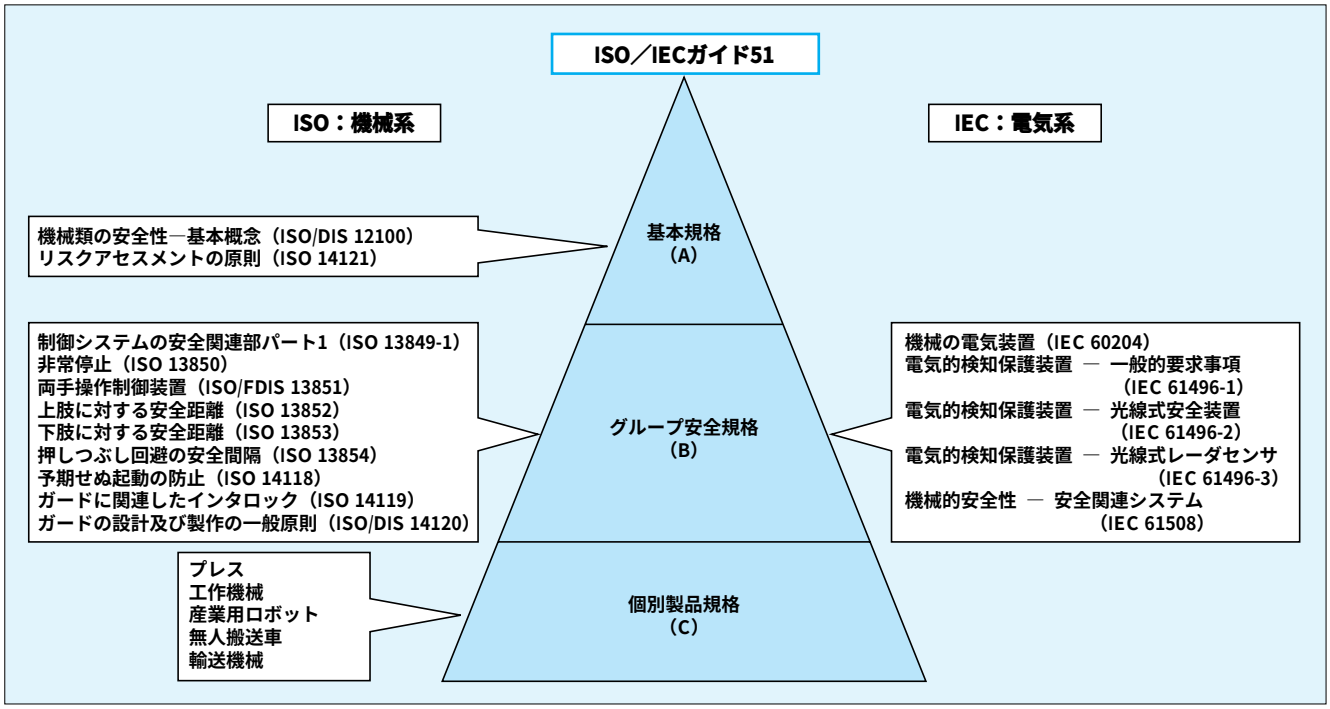

図2　国際安全規格の体系

いま、ある製品Xについての安全を考察するとき、その製品についての個別製品規格（C規格）が制定されていれば、その規格をまず参照する。そして、その規格の規定に基づいて、要求安全仕様を満たしているかどうかを評価する。個別製品規格（C規格）が定められていない場合は、その上位規格である、グループ安全規格（B規格）あるいは、基本安全規格（A規格）の中から、その製品に適用できる（適用しなければならない）条項を参照し、その製品の安全性を評価する。このような手続きをとることによって、全ての機械の安全評価を、国際安全規格に基づき実施することが可能となるのである。

2-3 国際安全規格の特徴

国際安全規格の特徴は次の通りである。

（1）安全の定義
国際規格では、安全を「受容できないリスクにさらされないこと」（ガイド51）と定義した。この定義の最大の特徴は、機械と人が共存して存在する限り、完全な安全は実現不可能だということを認めたところにある。限られた資源を、まず、重篤な災害の撲滅に振り向けようという考え方であり、小さなリスクは受容せざるを得ないということである。さらに、リスクを、傷害のひどさと、発生の可能性の度合いで定められるものと定義した。ここで、2つのパラメータは、必ずしも、かけ算の関係にあるものではなく、さまざまな評価因子によって定められる。一般的に、発生可能性よりも、傷害のひどさへの考慮が重要とみなされる。

（2）機械の安全を包括的に規定
安全規格を階層構造として定めているため、全ての機械類の安全性を包括的に規定することができた。製造しようとする機械の安全規格がC規格に定められていれば、それに従って製造する。もし定められていなければ、AおよびB規格に基づき、製造者が自己の責任においてその機械に必要な安全方策を定め実施する。

（3）リスクアセスメントに基づく安全
個々の機械のリスクは、（原則として）法律等によって天下り的に定めない。製造者が個別にリスクアセスメント（リスクの評価）を行い、実際の機械の使用状況に合わせたリスクの評価を行う。そして、その結果に基づき、必要なリスク低減方策の適用を行うのである。

（4）製造者による安全の確保
機械類の安全性は、第一に、製造者が構築するべきことが明確に規定された。そして、リスクアセスメントの一連の作業によって、製造者が、製造する機械類の安全性を、使用者に対して立証することとなる。使用者は製造者の立証を承認し、製造者が残留したリスクを引き受けて、機械を受け入れる。その後は、使用者が、その機械の作業者の安全確保のために、追加の安全方策を実施し、安全確保の体制を整える義務が発生する。

これらの特徴の背景には、機械は必ず故障し、人は必ず誤った行動をするという前提がある。それゆえ、機械は、故障によって暴走するようなことは絶対に起こさない。人の誤った行動によって機械に巻き込まれることは絶対に許さない。このような硬い信念が底に流れているのである。

また、この目的を実現するため、常に技術の進歩を取り入れられるよう、規格はできる限り安全の要求事項を定めるに止め、達成方法は製造者が定めることとしている。ただ、制御システムに関しては、安全関連部への電子装置の適用を排除している。これは、規格制定時の電子装置の安全レベルを反映したものであるが、現在の技術進歩を正確に反映したものとは言えない。今後、電子装置の安全関連部への導入が、大きな課題となるであろう。

2-4 国際安全規格各論

（1）基本規格：ISO 12100、機械類の安全性。基本概念、設計のための一般原則
この規格では、安全性の確保の方法が規定されている。図3に示すとおり、製造者は機械類のリスクアセスメントを行ってそのリスクを評価し、もし許容不可能なリスクがあれば、リスク低減の方策を実施することが要求される。全ての機械は、この手順を踏んで設計しなければならない。

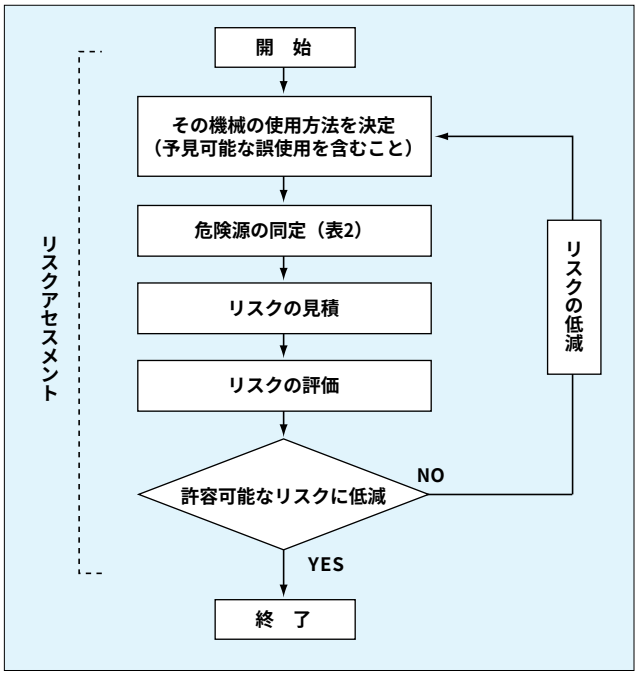

図3　リスクアセスメントとリスク低減の手順

（2）基本規格：ISO 14121、リスクアセスメントの原則
リスクアセスメントの方法に関する一般的原則が規定されている。ここでは、機械類に想定される各種の危険源がリスト（表2）として示されている。このリストに掲載された危険源が、評価しようとする機械において存在するかどうかを判定する作業がリスクアセスメントである。

表2　危険源リスト（抄）

1	機械的危険源		2	電気的危険源
	1.1	押しつぶし	3	熱的危険源
	1.2	せん断	4	騒音による危険源
	1.3	切断	5	振動による危険源
	1.4	巻き込み	6	放射の危険源
	1.5	引き込み	7	有毒、爆発、生物の危険源
	1.6	突き刺し	8	人間工学原則無視の危険源
	1.7	衝撃	9	その他

（3）グループ安全規格：ISO　13849、制御システムの安全関連部

機械の安全を確保する最も確実な方法は、人と機械を隔離することである。そして、どうしても人が機械に接近しなければならないときは、機械を停止する。ここに、機械の運転と停止を司る制御システムが必要となる。制御システムは必ず故障する。故障しても、危険側動作としないためのシステムが各種準備され、その安全度の程度を、安全カテゴリーと呼ぶ。

リスクアセスメントによってリスクの大小を定め、リスク大の対象には、高度な安全を保証できる制御システムを適用する。リスクのレベルと安全方策カテゴリーを対応させたものがこの規格である。その対応関係を図4に示す。

（4）グループ安全規格：IEC　60204、機械の電気装置、一般的要求事項

この規格は、機械類の電気装置一般に対して、その安全手段、素材、機器、ソフトウェア、文書作成など、全ての要素を規定している。機械の電気設備に関する規格の集大成であり、機械の電気設備を扱うとき、必ず参照しなければならない規格である。

（5）グループ安全規格：IEC 61508、機能的安全性

電気回路、電子回路およびマイクロプロセッサを用いた安全性の確保の方法について規定する。この規格では、機械の安全は、機器の信頼性に基づいて確保される。第1部は、組織の運営と評価方法を定める。第2部はハードウェアの構成方法。第3部はソフトウェア。第4部以下では、それらの応用方法を示す。

2-5 国際安全規格の拡大―ロボット規格（米国）

1999年6月、米国産業用ロボットの安全規格、ANSI/RIA R15.06：1999「産業用ロボットおよびロボットシステムの安全性に関する要求事項」が採択された。この安全規格は、次のように、国際安全規格の影響を強く受けている。

（1）リスクアセスメント

ロボット規格が定めるリスクアセスメントの概要を図5に示す。ロボット規格は、製造者および使用者の双方を対象としているため、設計上のリスクアセスメントのみならず、フィールド上のリスクアセスメントを加えているところが国際安全規格と異なるが、その手順、内容共に類似している。

（2）安全方策の振り当て

ロボット規格においても、国際安全規格と同様、リスク見積もりの結果（リスクカテゴリー）に対して、採用するべき安全回路の性能が設定されている。これは、国際安全規格（ISO 13849）が定める、安全方策カテゴリーとおおむねの対応を見ることができる[1)]。それを表3に示す。

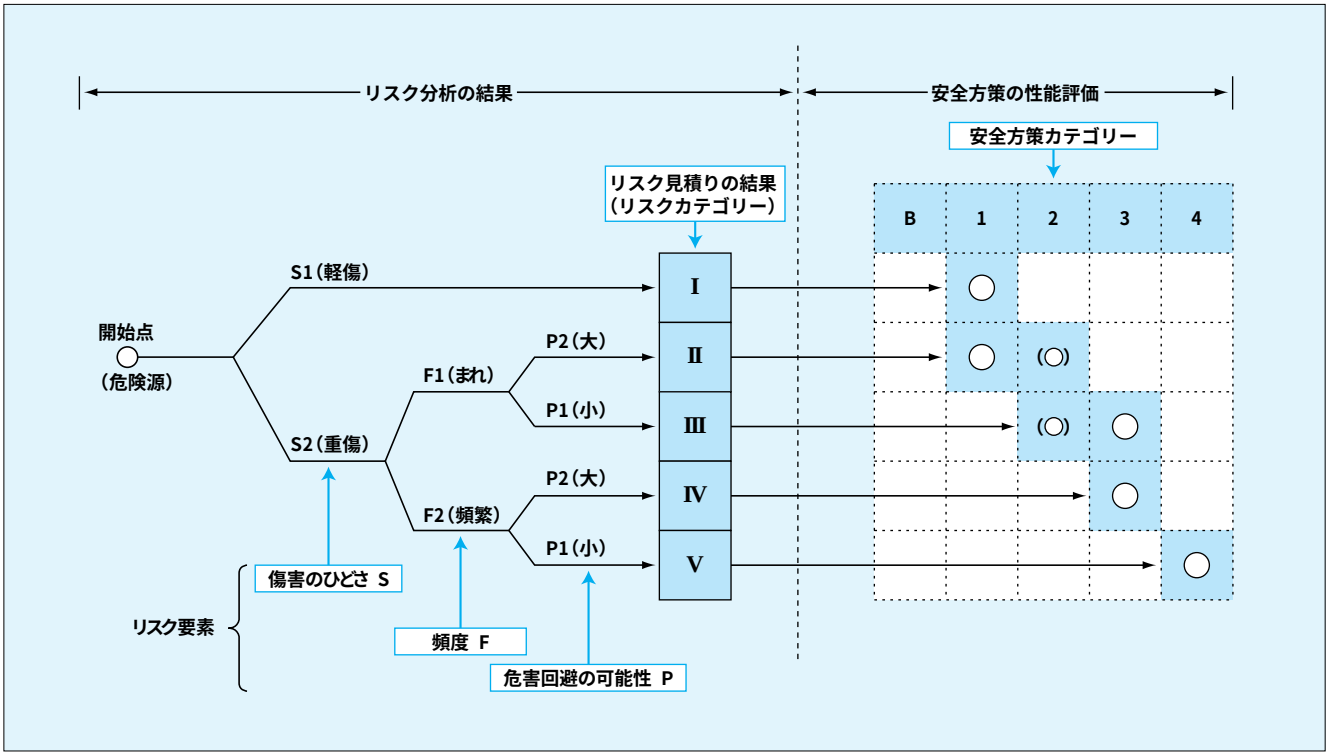

図4　リスク見積りと安全方策カテゴリー

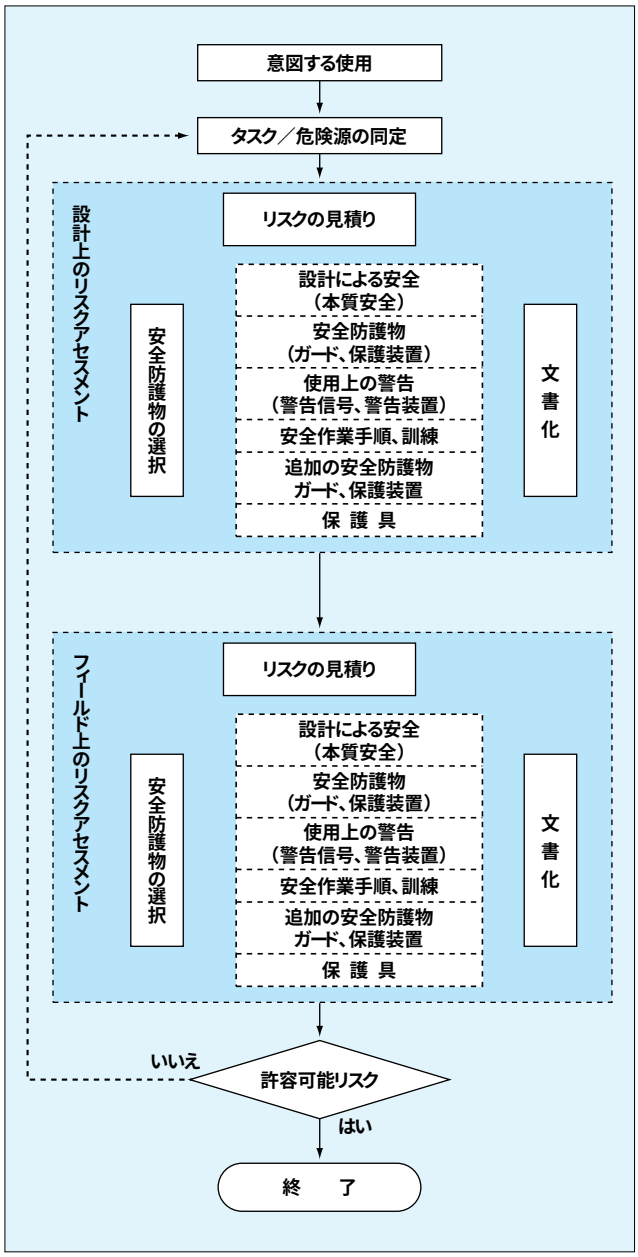

図5　米国ロボット規格におけるリスクアセスメント

表3　リスクの見積り方法と安全方策の振り当て

米国ロボット規格（ANSI/RIA R15.06）					国際安全規格（ISO 13849-1）	
傷害のひどさ	暴露の頻度	回避の可能性	リスクカテゴリー	採用すべき安全回路の性能	安全方策カテゴリーとその安全方策性能要約	
S2 重傷	E2 頻繁	A2（不可能）	R1	信頼できる制御	4	機能の常時自動監視
		A1（可能）	R2A		3	機能監視付き2重素
	E1 稀な	A2（不可能）	R2B	監視付き単一チャンネルシステム	2~3	安全要素カテゴリー2は機能監視付き
		A1（可能）	R2B		1~2	
S1 軽傷	E2 頻繁	A2（不可能）	R2C	単一チャンネルシステム	1	高信頼化制御機能
		A1（可能）	R3A			
	E1 稀な	A2（不可能）	R3B	単純回路		
		A1（可能）	R4		B	通常の制御機能

2-6 国際安全規格の拡大―機械の包括的な安全基準に関する指針（日本）

労働省は、1999年4月、「労働安全衛生マネジメントシステムに関する指針」を公表した。これによれば、事業者は事業場における機械等の危険要因を特定する手順を定め、危険要因を特定することが義務付けられた。そして、その手順として、リスクアセスメント手法も明示された。

さらに、厚生労働省は、2001年6月、「機械の包括的な安全基準に関する指針」を公表した。内容は、基本的に国際安全規格に準拠しており、国際安全規格に則った安全確保の方策をわが国においても導入することを宣言したものである。指針の文言上の国際安全規格との相違は、包括指針においては、事業者によるリスク低減を明示している点である。

しかし、本当に相違しているところは、EUの場合は、機械指令という、域内共通の強制法規が制定されている点である。EN規格は、この強制法の下にあるということを忘れてはならない。強制法がなくても、どの事業者も安全を大事と思わなければダメだという意見もある。理想はそうであろうが、現実は、この意見を支持しない。19世紀から20世紀初頭に頻発したボイラの爆発事故を、第三者機関が抑制、防止に成功するに至った歴史を見れば、政府による強制法の制定と、第三者機関の技術力との有機的な結合によって初めて達成できたことが理解できる。競争条件を平等化するための強制法の存在は、生産性に直結しない安全を達成するための必須要件であるといわなければならない。

しかしながら、わが国の行政が、安全のグローバルスタンダードを公式に採用することを宣言した意味は大きいと思われる。本年4月、ソニーは、ISO 12100に対応した「安全設備指針」を実施することを発表した。行政の動きによって、民間の動きが加速することを期待したい。

3. 安全確認型システムの概要

3-1 安全確認型システムの定義

確定的な安全を構築する方法を、実機に実際に適用できる形で提案したものが、「安全確認型システム」である。これは、「安全が確認できたときだけ、機械の運転を許可するシステム」と定義される。あるいは、もっと具体的に言えば「作業者が機械の運転範囲にいないことを直接検出したとき、機械の起動と運転の継続を許可するシステムであるといってもよい。この理論は、杉本および蓬原によって、1987年に発表された[2)]。まだ国際安全規格が成立する以前に確立した理論であるが、その後制定された国際安全規格の区分で評価すれば、最高度の安全システムとして位置付けることができるものである。

安全確認型システムの特長を、図6に示す。ここでは、安全と危険の概念の捉え方を示している。実際の機械の使用時には、安全の状態、危険の状態の他に、そのどちらとも明確に区分できない不安の状態が存在する。安全確認型システムにおいては、図6に示すように、不安の状態の時には危険とみなすのである。一方、これまでよく使われてきた危険検出型システムでは、不安状態は危険信号が発せられないことから、機械の運転が許可されてしまう。安全の観点からは、どちらが適切なシステムであるかは明白である。

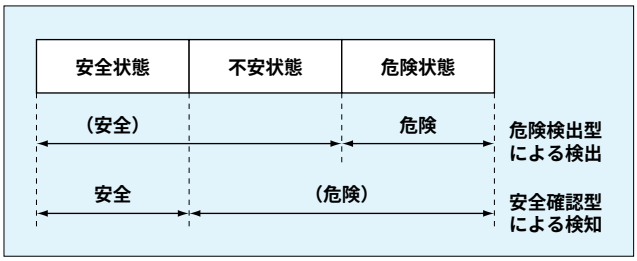

図6　安全に関する3つの状態

3-2 安全確認型システムの構成

安全確認型システムの基本構成を、図7に示す。「安全状態を検出するセンサの信号と、機械の運転を命令する始動信号の双方がONとなったときだけ、起動信号を発する」ことが、その機能である。

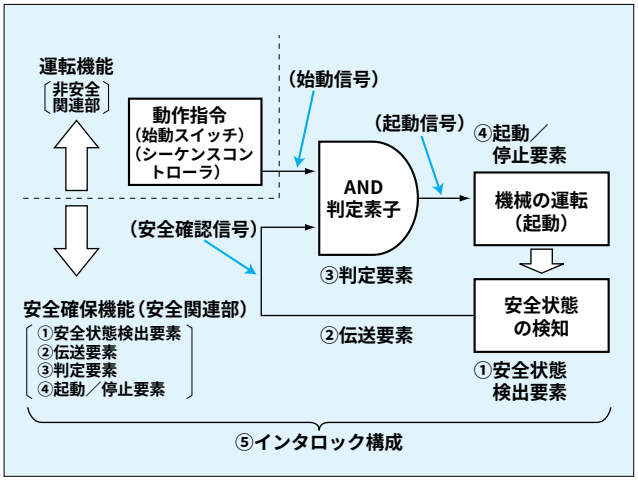

図7　安全確認型システムの基本構成

・運転機能（非安全関連部）

機械システムの運転を司る部分であり、始動信号を発する。ここでは、安全についての配慮は一切不要であり、所定の機能遂行だけを目指してシステム構築をすればよい。基本的にこれまでの設計手法がそのまま使える。国際安全規格では「非安全関連部」と呼ばれる。

・安全確保機能（安全関連部）

安全確保を司る部分である。「安全が確認できたときだけ、機械の運転を許可する」機能を持たなければならない。国際安全規格では「安全関連部」と呼ばれる。

この部分は、以下の5つのサブシステムにて構成される。

（1）安全状態検出要素

機械の安全状態を検出する要素である。ここでは、安全状態を直接検出することがもっとも望ましい。高いエネルギー状態が安全状態である場合には、検出は容易である。例えば、ボイラへの燃料供給はボイラが着火しているときが安全状態である。この状態はボイラ内に熱電対温度計を設置すれば、それがボイラの熱エネルギーを電圧に直接変換して安全信号として出力することができる。

機械が安全状態にあるときに、その雰囲気が高いエネルギー状態でない場合には、外部からエネルギーを供給して高いエネルギー場を人工的に作り出す手法もある。ある場所に人がいないことが安全状態であるとき、その場所の一端に光源をおいて光を通過させ、他端に置いた受光器に光エネルギーを投入する。光エネルギーが受光器に到達することは途中に人がいないこと、すなわち安全状態を示す。こうして受光器は光エネルギーを直接電流に変換し、それを安全信号として出力することができる。安全確認型検出器はこのようにして安全状態を検出することが基本である。

（2）伝送要素

安全確認型信号伝送とは、安全信号を高いエネルギーによって送受信することを指す。これによって、伝送路の遮断という故障によってシステムが危険側動作に移行することを防止する。この手法の他に、電源枠外処理、あるいは、ダイナミックフェールセーフなどの、さらに高度な伝送技術が開発されている。

（3）判定要素

判断要素は、機械の始動指令と安全確認信号とを受けて、両者が共にOKを示すときのみ、機械運転信号（起動信号）を発信する機能を持つ。この要素は完全なフェールセーフ特性を持たなければならない。

（4）起動／停止要素

停止要素には、駆動のための新たなエネルギー供給を遮断し、現在持っている運動エネルギー等を消散させる（制動）機能が求められる。また停止命令は全てに優先され、停止命令解除で、直ちに再起動させないことが必要である。

制動は、電気や圧力の供給を遮断すると制動力が発生するタイプのものを使う。これをノーマルクローズタイプのブレーキと呼ぶ。

（5）インタロック構成

機械が安全確認型システムであるためには、各要素がそれぞれ安全確認型の原則に従うものであることだけでは足りない。それぞれの要素が適切に配置され、人と機械の安全でない接触を防止するための十分なインタロックを構成しなければならない。

実際の機械に適用されるインタロックの基本構成は、図8の通りである。機械の停止を検出する手段と、人の不在を確認する手段とを備え、機械と人とが互いに相手方の停止あるいは不在を検出したときだけ、運転あるいは作業を開始することを許可する機能を備える。

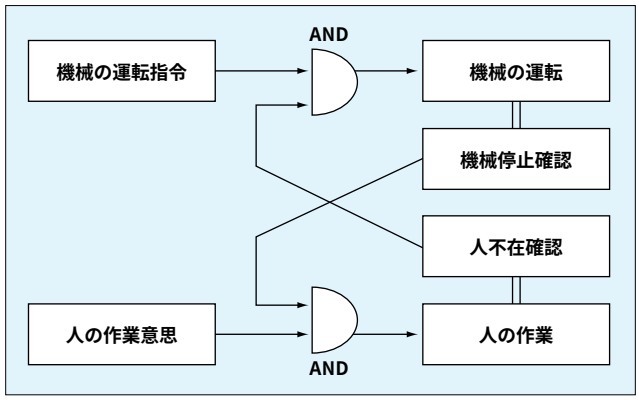

図8　インタロックの基本システム

3-3 安全確認型システムの適用

安全確認型システムは、このようにして高度の安全性を作り出すことができる。さらにこのシステムを生産ラインに適用することで、安全性を向上させるだけでなく、生産性まで向上させた事例も報告されるようになってきた。

これからは、下記の条件を満たすシステムには、安全確認型システムを導入するべきである。

(1) 停止安全が成立する機械
(2) 安全状態が定義できる機械
(3) 安全確認型システムを構築する要素部品が存在する。
（特に安全状態の検出手段は、現在、必ずしも入手可能と言うわけではない。新たな開発が望まれる分野である。）

4. おわりに

国際安全規格は、機械の安全を作る手続きを、図3に示すように、リスクアセスメントとリスク低減として明確に定めた。安全確認型システムは、この中のリスク低減の手法として位置付けられる。

国際安全規格においては、機械の制御システムの安全確保の考え方として、「安全関連部」と「非安全関連部」の区分が重要である。制御システムをこのように明確に区分した上で、「安全関連部」について、厳格な安全性評価を行うという考え方である。もし明確な区分ができない場合は、制御システムの全ての部分を「安全関連部」とみなす。

安全確認型システムの場合も、図7に示したとおり、運転機能と安全確保機能とに区分し、後者の優先判断の元に、前者の機能を実施する。安全確認型システムのもっとも大きな特長は、この明確な概念の元に、安全システムの構築方法を、具体的な形で提示したところにある。安全確認型システムのさらなる普及を目指したいものである。

〔参考文献〕

1) 蓬原弘一：「米国の産業用ロボット安全規格の考え方（1)」、ロボット、№133、P52-59、社団法人日本ロボット工業会、(2000)
2) N. Sugimoto, K. Futsuhara: Safety and Technology of Safety Confirmation Type-Coordination with Robots, Proc. of the Annual International Industrial Ergonomics and Safety Conf. in Maiami, Florida, U.S.A.1987-7