安全設計・演繹的予防措置

○加部隆史（NPO 安全工学研究所）、染谷美枝（長岡技術科学大学）

Safety Design: a priori Prevention

*Takashi Kabe(NPO The Safety Engineering Laboratory),
Mie Someya(Nagaoka University of Technology)

Labor accidents happened frequently after the industrial revolution, and the prevention of accident had been carried out in the world. It seems that, the accidents should be decreasing statistically, but huge and serious accidents show a tendency to increase at the rapid development of science and technology. The advantage due to the evolution of the information technology brought on the other hand some new kind of accidents. What were the main causes; technology, organization or human error ? If it is caused by the technology, it becomes an urgent subject, how prevention of recurrence can be practiced. First, it becomes a focus at the machinery accidents, whether the safety technology defined internationally are used, or not. It tried to examine the meaning of the safety design as a means of the deductive(a priori) prevention measure.

Key words : safety design, prevention, risk assessment, ISO/IEC Guide 51, ISO12100, IEC 61508, FMEA , third party certification

1. 科学と技術

安全規格のガイドラインである ISO/IEC Guide 51 によれば、安全とはリスクからの開放という定義がされている。リスクと言うと非常に広義であり、安全・安心に係わるすべてのものが対象となってしまう。機械の安全は技術としての裏付けがあるが、安心は情緒的なものの為、安全技術を論じる際には除外した方が整理がつきやすい。又安全を確率で論じる前に、安全技術の体系が存在する事を出発点としたい。例えば、アメリカのハインリッヒの法則（注1）と言うものがあり、これは労働災害の統計を分析した結果、「1件の重大災害（死亡・重傷）が発生する背景に、29 件の軽傷事故と300件のヒヤリ・ハットがある。」との事だが、これは発生結果の分析から傾向を示したもので、そもそも確率に過ぎない。国際的には、現在後述する確定論的アプローチが主体となっている。事故が発生した際に、確率からそれを受入れる事にするのか、或いは事前に安全技術の既知の手法を適用した予防措置を講じていたのかは大きな違いが

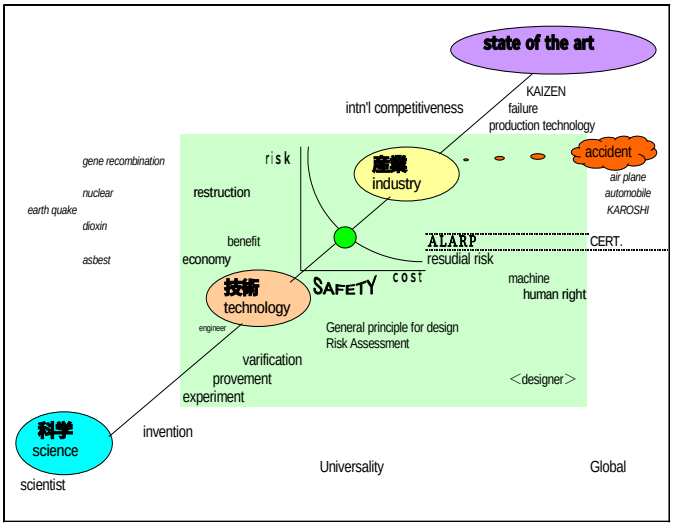

Fig.1 Science, technology, industry

出てくる。要するに前者は帰納的手法であるが、ここでは偶発性を排除する後者の演繹的予防措置の概念を適用した定性的な確定論を主体とした機械の安全設計と安全技術にある程度限定した上で、考察を重ねてゆきたい。

科学と技術はそもそも基本的に異なるもので、科学は論理的なものが中心であり、技術は多くの実験や生産現場等での検証プロセスを経て確立したものである。そして、産業はある製品が複数の技術を複合し、危険源を低減し安全な製品がその利便性を世の中に認められ、複数の製造者が登場してひとつの産業が育成される。設計者は常にその時代の最高の技術（state of the art）を追求し商品に反映させる。しかし、技術は継続的に進化を重ねその未成熟さ故に故障や事故が誘発される。そこで生産現場ではたゆまない改善を重ね、その時代の最高の技術は時代と共に常に進化するイノベーションのプロセスを踏まえている（Fig.1）。

ものづくりの現場では数多くの労働災害事故に対し、現場での安全を確保する努力が日夜行われている。これらは比較的技能面が多く、技術（工学）は普遍性を持つものである事に対し、技能は普遍性がなく人により伝承される。その意味で、技能と技術は異なるものである。航空機はこれまでのいくつもの墜落事故、国産を達成した H2ロケットの初期における何件もの打ち上げ失敗、スペースシャトルの空中分解、チェルノブイリに代表される原子力事故や国内での臨界事故、ボパール事件やセベソ事件に代表される化学プラントの重大事故などの計り知れない犠牲の上に、現代社会は成り立っており、如何に安全技術が必要かがこれら一連の事故が示している。安全技術もこれら重大事故を重ねる度に検討・改善され、新たな防止手法・規格・規制等が生まれてきた。又、科学及び技術の発展によりリスクは減少どころか、逆に多様化・複雑化・重大化してきている。又、サイバー社会と少子高齢化などの背景から誕生しつつあるサービスロボットなどは、技術的なイノベーションであるが、その安全性をどの様に立証できるかの手法が未だ確立する過程には至っていない。

技術の検証が行われると、それは製品というものに具現化されて市場に投入される。その際は機能面のほか、人にとって安全な技術、利便性や経済性を含め均整がとれたものでなくては市場が受入れない。又、市場に投入されたものでも技術は間違いを起こす為に、常に学習と進化のプロセスがつきまとう。

消費者に近いもの（製品安全）、製造現場に導入される機械類（労働安全）などはステークホルダがはっきりしており、その技術を受入れるか否かの判断は比較的早くつく。それに対し、航空機、ロケット、原子力プラント、化学プラント（プロセス安全）などは使用者や消費者の選択は皆無で、出来た技術をそれが安全であると仮定して使用せざるを得ない。しかしながら、原子力プラントなどは実証が困難な為にいきなり施設が建設され稼動される。特に高速増殖炉の様な技術的に未知な部分が多いものは、安全技術上多くの課題を抱えている。ナトリウムが漏れるとどうなるか、或いは臨界事故をおこしたらどうなるかの実証は可能でなく、実験装置そのものが現場で稼動することになる。つまり、技術になる前の科学が特定利益により一人歩きして産業化されている。

本来人と交わる技術は、基本的には安全でなければならないが、技術は前述のプロセスのように当初から潜在的に壊れる・誤る事を前提としている為に、国際的に「絶対安全はありえない」と言う通念が定着している（注2）。

2. 安全性と信頼性

安全は基本的に全ての工学に横断的に通ずるものであり、その考え方は本来設計のプロセスに組み込まれるべきものである。要するに、次項に示すような様々なエネルギーが危険源となる為にそれをどう回避するか、と言う事と事故はあくまで、危険源と人が時間的・物理的に同居した際に、そして危険現象から回避できない時に発生する為に、機械の限界を見極めその同居をどう抑制するか・回避させるかと言う事になる。

高い信頼性に基づく機械・装置において災害が生じている。確率的には災害は「レアケース」であるが、そもそも「安全」はこのレアケースにたいしてその発生を防止するものでなくてはならない。従来、国内では一般的な危険検出型は安全機器が故障した場合、危険な状態であっても信号を発する事ができない。安全な状態が確認された時のみに始動を許可する安全確認型（注3）は、安全機器が故障した場合も、安全を確認する信号が発しないので機械が停止し安全を確定するシステムである。

機械は故障し、人は間違いを起こす事を前提としての考えがフェールセーフ（失敗しても安全である）とフォールトトレランス（欠陥があってもそれを許容する）で、フォールトトレランスの典型例が制御の冗長性である。安全性は人間に危害が加わらないようにしようとする事に対して、信頼性は機械の正しい機能を維持しようとする事を目標にしている為に、安全性と信頼性はお互いに深い関係にはあるが、実際は異なった概念である（注4）。但し、後述するソフトウェアの安全性が関連した際には安全性と信頼性が併せて考慮される事になる。

航空機、ロケット、原子力プラント、化学プラント等は信頼性を基に設計されるが、それにより安全を確保しようとする為にそこで使用される部品やシステムには高い費用が付きまとう。一方で、事故を確率の観点から捉える為に、一度事故が起きてもそれは低い確率の中で運が悪かったとして受け入れられてしまうので、本来の演繹的予防措置としての安全性設計とは必ずしも結びつかない。いわゆる「止まらない安全」（注5）の為、信頼性をたゆまなく向上させてゆく。但し、背景には確率（probability）に対する工学分野での解釈の歴史的混乱がある事を考慮する事が必要である（注6）

3. 日本式と国際安全規格の相違

国際規格は、設計者が危険源を同定・評価・低減し残留リスクを認める基本的な考え方に基づいている。つまり、安全技術を適用し機械は壊れるもの、人は間違いをおこす事を前提としている。同時にISO/IEC Guide 51は絶対安全はありえないという事から残留リスクを明記している。従来日本国内では、絶対安全の思考形態で、工場では危険予知運動・指差呼称・声掛け運動を実施し、無災害記録の延長を目標とされてきた。そして特異な品質極上主義の観点から間違いを極力認めない風潮ができている。要するに技術ではなく運動・教育に主眼がおかれた。人は本来不完全である故、絶対安全を追求するとどうしてもそこで「ごまかし」が出てきてしまう。東海村での臨界事故と電力会社の手抜き、自動車会社のリコール隠し等が近年絶対安全の限界を如実に示している。一方では、設計者がstate of the artを追求する姿勢、責任、倫理観が要求されるが、それが経済性を優先し安全を後回しにする経営組織体質に染まってしまうと、たちどころにその姿勢は方向転換させられてしまう。欧米では第三者認証機関が歴史的に発達してきた効用として、これらのごまかしは第三者へ対しての説明責任とそれによる安全妥当性の検証により除外されるところがある。

1985年にWTO/TBT協定が成立し日本も同年条約に批准した。これにより日本で規格を作成する際には、国際規格との整合性が求められ、実質的にダブルスタンダートは廃止する方向性が打ち出された。そして、これ以降世界的に規格整合化の波が急速に押し寄せてきた。

欧州は1985年のいわゆるニューアプローチ指令に続き1989年の強制法規であるいわゆる欧州機械指令により、製造者責任としてのCEマーキングが製品流通の条件となり、それを支えるいわゆるピラミッド構造のABC規格の骨格が出来運用されている。それに、低電圧指令、EMC指令、マネジメント規格としての品質管理に係わるISO9000シリーズが横断的に適用される。CEマーキング自体は、製品の安全性を安全の必須要求事項に基づき「自己宣言」するものである。安全の妥当性をどの様に立証できるかの方法論に関する規則は存在せず、各製造者に一任されている。実質的には、ISO/IEC等の国際規格を適用するのが最も実利的であるとされている。ニューアプローチ指令は、それまで国が細かな技術基準を定め運用されていた安全規制の限界を察した上で、自主規制に切替えたもので、これは英国のローベンス報告（1974年）のイネーブリン・アクトの精神に則っている。

米国は当初ANSI（米国規格協会），UL，NFPA，MIL等の独自規格を主体として運営してきたが、近年頓に国際規格への整合を急速に進めている。産業用ロボットの安全性に関してはANSI RIA R15.06-1999がありそこでは包括的なリスクアセスメントを推奨しており、日本でも産業用ロボットにそのまま適用された。ハードワイヤリングのみでの緊急停止が許容さていたが、IEC60204-1:2000と整合化を計ったNFPA79:2002ではソフトウェアを許容し、又ここでは安全制御にソフトウェアを使用する際は第三者機関としてNRTL（試験所登録機関）に登録された試験所の認証書を必要条件と定めている。

機械安全に関しての規格ANSI B11シリーズにおいて個別機械の安全性要件を規定すると共に、**ANSI B11.TR3-2000**ではエ作機械のリスク評価と低減に関するガイドラインを定め、これは70を越えるANSIのサブコミティの審議を終え成立したもので、米国での過去30年間の安全規格の流れに一石を投じるパラダイムシフトの位置付けを有するものである。基本的には、設計者原則のEN292-1(ISO12100)及びリスクアセスメントの原則EN1050(ISO14121)をベースとして考慮している。電気安全

に関しては、IEC60204 の考えを NFPA79 に取り入れている。ANSI B11.TR4-2004 では工作機械のプログラマブル電子システム（PES/PLC）の選択を定めている。さらに ANSI B11.TR6 は制御の信頼性とサーボドライブを扱い、2006 年に発行予定である。これらの動向を鳥瞰し、実際の産業界での運用を考慮すると、米国での機械安全規格の骨組み及びその運用について基本線ではほぼ欧州の機械安全制度と整合されたといっても過言ではない。

4．運動の法則

サービスロボットが日本及び他の欧米諸国において近年盛んに研究され、部分的に市場に投入され始めてきている。NPO 安全工学研究所はその最初の認証行為を 2005 年 9 月に実施した。

製造者の安全に関するコンセプトは、ISO/IEC Guide 51 に則っており、本質安全設計、追加的保護方策、安全に関する情報提供の順番でリスク低減が検討されていた。本質安全設計のステップでは、基本的には,質量と加速度によりどれだけのエネルギーがもたらされ（ma=F）、それが挟まれ、巻き込まれ、押しつぶし等の危害をどの程度発生させるかと言う事が問題となる。次いで追加的保護方策のステップにおいて、工業用として実績のある制御面での冗長性、ソフトウェアについては機能安全、そしてセンサについては安全なバンパーセンサやレザースキャナなどが適用されることになる。しかしながら、利便性のあるサービスロボットを合理的な価格で市場に提供しようとした際には、これら工業用の安全デバイスをそのまま適用するとコスト高になってしまい、経済性が損なわれてしまう。

つまり、量子力学等に基づく情報通信機能を安全にするとなると機能安全（IEC61508）を考慮し、ソフトウェアの安全性につきかなり包括的なアプローチが要求される為、かなりの時間と費用が発生してしまう。

今回対象としたサービスロボットは、基本的には本質安全設計によるエネルギー制限、人間工学的な寸法と形状配慮などの措置により安全が達成されていた。そのため複数のセンサを装備したこのサービスロボットは、危険検出により安全を確保する手法ではなく、エネルギーを抑制し、これらセンサはあくまで付加的機能に留め、これらのセンサ信号は「非安全関連信号」と判断し、認証の対象としなかった。ハイテクなサービスロボットだが、機能的には勿論最新のコンピューター技術やセンサ技術を駆使してはいるが、その安全設計は古典的なニュートン力学の運動の法則の実験によりよるものが大部分をしめている。製造者は事故の予防措置としてサービスロボットの使用目的を限定し安全設計を実施し、製造者費用利便性分析を行い、利便性を発揮できるようにされていた。

NPO 安全工学研究所は例外的な危険源を残留リスクとして確認し、それを臨界危険源（クリティカル ・ハザー－CH）と命名し、安全妥当性及び残留リスクの確認をして鑑定書を発給した。サービスロボットについては、整合された規格基準並びに試験基準が現段階では未成立の為、ISO の規定に基づく適合性評価は可能でない事から正式な認証書を第三者機関として発給できる状態では無い為に、妥当性確認の行為を鑑定書に留めざるを得ない。この認証行為の結果については、日本機械学会の 2005 年年次大会並びに、SIAS 2005(4th International Conference: Safety of Industrial Automated Systems)にて発表し、関係者からの反応と意見を得た。本事例では、本質安全設計により大部分のリスクが低減された。しかしながらサービスロボットの多様性を考えれば、ISO/IEC Guide51 に示される、追加的保護方策、情報提供も含めた体系的な技術考察が必要である。

今後、サービスロボットの安全コンセプトの体系化と、これらの実験と検証を重ねた上で、サービスロボットの安全性に関する国際規格原案の提出を日本発として出来る様に検討中である。

ソフトウェアは基本的につきまとうバグ等の問題に対処する為に、機能安全（IEC61508）がプロセス産業等を背景として機械安全に影響して来た。機能安全では、従来の機械･電気に対する確定論的アプローチでは信頼性が考慮されていないとの近年の議論から、そこにプロセス安全で先行していた確率論的アプローチを導入したものである。ソフトウェアの開発の基本的なプロセスの考え方として医療機器などにも適用されている「V モデル」を採用し、複合的な部品の信頼性を例えば宇宙機器の信頼性を検討する手法としてアメリカで生まれた FMEA（注 7）,マルコフモデル等の手法を用い定量的に評価しその安全水準度を SIL（Safety Integrity Level）1－4に分類する。重要な事は、ソフトウェアの安全性とその品質確保は、出来上がってから追加するのではなく、最初から開発プロセスの中に取り込み達成してゆくと言う事である。機能安全規格でのこの全ライフサイクルにわたるシステムアプローチの考え方は、プロセス安全、鉄道安全、医療安全などでは既に適用されており、機械安全の分野では近年になって部分的に採用され始めている。ソフトウェアにおいては特に、Validation(妥当性確認)と Verification(検証)を区別する事が重要で、Verification では、ソフトウェアのライフサイクルプロセスにおいて、プロセスのインプットとアウトプットの整合性を確認し、この検証作業（Verification）を繰り返す事により、製品の妥当性が確認されていると言う確証に繋がってくる（注 8）。

5．設計者責任と危険源の同定

設計される機械の危険源はそもそも設計者が誰よりも理解しているもので、ISO14121（リスクアセスメントの原則）では例えば以下のような典型的な危険源を列挙している；

機械的 / 電気的･電子的 / 熱的
騒音･振動･放射能 /人間工学無視 等。

良識ある設計者は、当然の事ながら基本的には設計時にこれら危険源を同定した上で、リスクアセスメントを実施する事とする(Fig.2)。

危険源が同定されると、次はリスクの見積りとリスクの評価を実施する。リスクアセスメントの評価手法は複数あり、あくまで定性的評価の為に、どの手法が最適化は統一されてはいない。因みに、日本では MIL-STD882D（4x5 方式）に基づく評価方法が比較的良く知られている。

制御カテゴリーに関しては EN954-1 によると、障害の程度･危険の発生頻度･危険回避の可能性の組合せにより B/1/2/3/4 のカテゴリーに分類される。これに機能安全の信頼性を加味した ISO13849-1（rev）により B-4 のカテゴリーは、Performance Level(PL) a-b-c-d-e に分類されている。機能安全を適用した際には、前述の SIL 1-4 を適用する。

リスク評価の後には、リスク低減の作業に入る（Fig.3）。設計手順は、ISO12100 の設計原則に基づき、前述の①「本質安全設計」が最初で、それで補われないところは、安全デバイス等を利用した②「追加的保護方策」を講じ、残留リスク等については③「安全に関する情報提供」として警告表示や取扱説明書等に明記する。この三段階のアプローチは優先順位をしており、本質安全設計を如何に生かせるかにより、その後の方策とそれに係わる付加的費用がはじき出される。重要な事は、リスクアセスメントとリスク低減により残留リスクが受容許容範囲（Tolerable Region）に到

達した事を例えばISO9001に則り図書を作成し設計者が保管する事である。

6. 第三者認証

更に、複雑なシステムや新しい技術の妥当性検証については往々にして欧米の場合、第三者認証の実施が法的には例外を除き義務付けられてはいないが、説明責任の

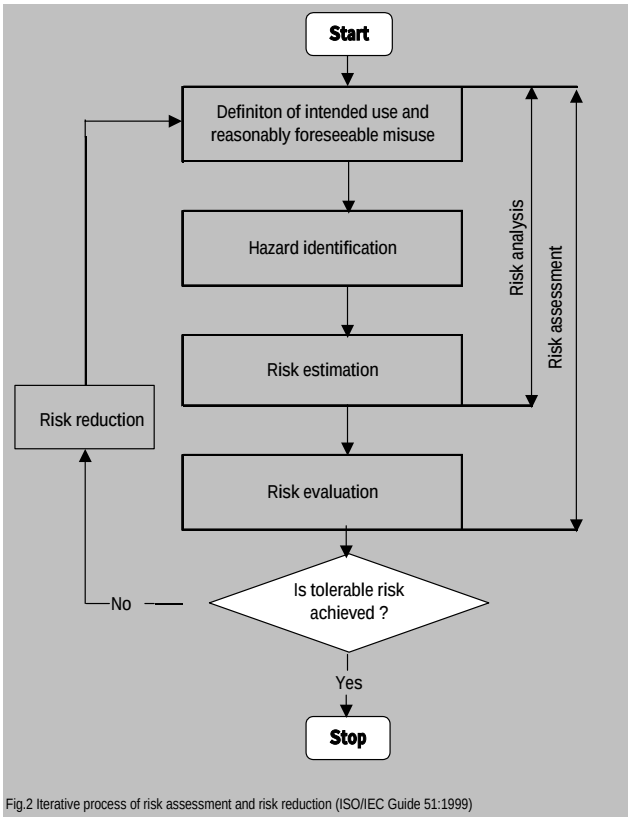

Fig.2 Iterative process of risk assessment and risk reduction (ISO/IEC Guide 51:1999)

観点からその適用が一般的である。上述の通り、産業革命時のボイラー事故や炭鉱防爆での爆発事故を未然防止する為に、ドイツやイギリスを中心として検査機関が発達し、それが年代を経ていわゆる第三者認証機関としての地位を産業界で不動なものにしてきた。これは、第一者としての製造者でも、第二者としての購入者でもない、その中間の第三者であり基本的には中立的な立場である。欧州の場合は、これら検査機関及び認証機関の要件は定められており、Notified Body（通知機関）として公式に登録される。それにより、中立機関として正式に認知され、実質的に社会で受入れられている。

事故の際の補償を確保する為に、損害保険会社がリスクを請け負うが、その際の保険支払額を極力押さえる為に、製品の検査をした事が認証制度のベースとなっており、その為に欧米の場合は損害保険会社が認証機関である場合が多々ある。そしてこれら損害保険会社は、独自に災害の研究部門と試験装置を有しており、損害保険料率を策定するのに必要なアンダーライティングの技術的ノウハウを蓄積してきている。要するに、安全工学の体系を 100 年以上の歳月をかけて蓄積してきている。この仕組みは、日本では社会制度として未熟な状態であり、企業のグローバルな活動を円滑に進める事への支障をきたしている。

損害保険会社のリスク請負を円滑にする為に、製造者責任･設計者の安全設計の担保が必要になるが、それは第5節で示した安全設計の手順が整っている為に、明確な責任分担が可能である。ここでも、設計者は製品を市場に流通する前にいわゆる「第三者」でもある損害保険会社に、安全設計達成の過程とその妥当性を立証する事が要求される。

第三者認証機関の運営に関しては、自ずからCompetency（専門性）が要求され、安全技術を適格に検査できる人、その検査結果の妥当性を中立的に検証できる経験を蓄積した専門家が必要であり、それには適切な教育を受けた専門家が必要とされている。

設計者が、認証機関へ提出する図書の第一段階で準備するものは、いわゆる安全の基本概念と適用規格の列挙である。安全の基本概念は、Safety concept, safety policy, safety requirement 等の表現として国際規格に定義されているものである。このコンセプトは設計の基本を安全規格等を参照にしてどう組み立てたかを文書で説明するもので、複雑な装置等の場合は、コンセプト部だけでもかなりの頁数になる。この安全コンセプトが基本設計として認められてから初めて詳細設計に取組むのが一般的な手順であり、この手法も国内では今までやってきていない。第三者機関の Competent Person の要求に対応するには、設計者が本来自ら Competency を有した Competent Person になっていないと、認証過程に多大な時間と費用がかかってしまう。

認証制度の中の試験機関の必須要件として、試験装置の校正があるが、国内ではこの本質的な行為と制度は汎用製品に関してはともかく、ハイテク技術の多くを国内では校正された試験装置を用いて検査できない状況があり、行政の公式発表でも、日本の校正制度を向う何年間かけて世界のトップレベルと同等に整備する計画がなされている。ここでは、科学を飛ばして技術のアプリケーションに特化した際の置忘れ現象がある。

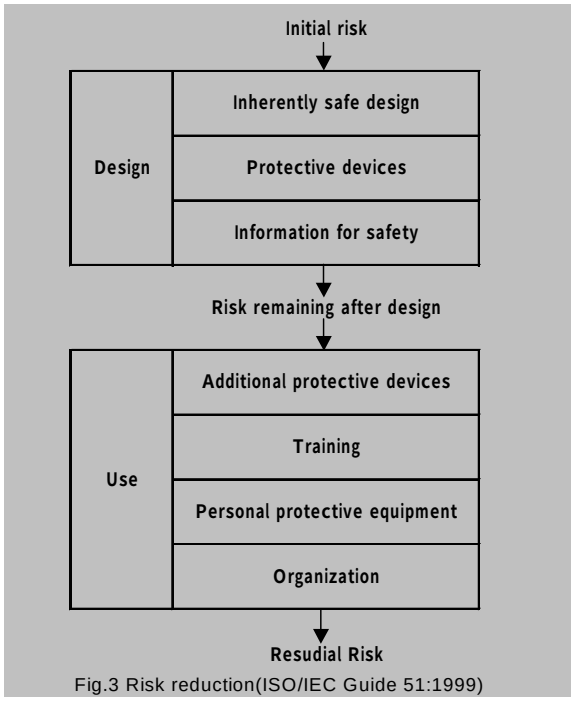

Fig.3 Risk reduction(ISO/IEC Guide 51:1999)

第三者の概念は、企業で税理士或いは税の専門家が作成した財務諸表を中立的な公認会計士が監査し Accountability をそれにより示す事と同じ仕組みである。説明責任＝アカウンタビリティの所以でもある。いくら社内の税理士だけが作成した財務諸表を上場会社の株主総会の資料として提出しようとしても通用しないのと同様、欧州では設計者が自ら作成した図書のみでは、社会的信用を獲得しづらいのが現状であり、その為に、たとえそれが自己宣言に基づき法的強制力がないとしても、第三者の認証書を取得するのが多くの場

合通例となっている所以でもある。

先述のサービスロボットの「認証行為としての鑑定」とは、一方では認証制度が国内で未整備である状況と、他方では新しい技術の為に適合性評価を実施する為の製品規格・基準・試験方法等が未だ存在していない為の過渡期での対応である。

更に、これは新しい技術で前例が無い事から、安全に関する社会制度が未熟な国内では、その保険リスクの査定が経験不足の為に困難であり、時代に見合ったあらたな損害保険の仕組みが要求される。

7．労働災害の傾向と予防措置

厚生労働省の労働災害防止計画等の最近の資料によると、「製造業における労働災害」は、休業4日以上の死傷災害で全産業の約3割、死亡災害で全産業の約2割、一度に3人以上が被災する重大災害で全産業の約2割を占めている。

「労働災害の種類別」でみると、機械設備による**挟まれ・巻き込まれ**等の災害が、死亡災害では全体の約3割を占め、休業4日以上の死傷災害では全体の5割近くを占めている。

「事業所の規模別」では、国内の労働者数の8割以上を占める労働者数 300 人未満の中小規模事業場において、労働災害の9割強が発生しており、そのうち 50 人未満の事業場で7割強を占めている。労働災害発生率を事業場の規模別に見ると、規模が小さくなるに従って労働災害発生率が高くなっており、労働者数 100 人から 299 人の規模の事業場と労働者数 30 人から 99 人の規模の事業場においては、労働者数 1, 000 人以上の規模の事業場に比べ、それぞれ労働災害発生率が約5倍、約7倍となっている。

「年齢別」の発生例率は少子化・高齢化社会の進展に伴い、労働力人口の高齢化も進み、50 歳以上の高年齢労働者の占める割合は増加傾向にあり、約3割に達している。死亡災害と休業4日以上の死傷災害で見ると、50 歳以上の高年齢労働者がそれぞれ全体の5割、4割を上回る等大きな割合を占めている。

「定常作業・非定常作業別」で見ると、業種及び被災程度にもよるが、いわゆる危険源と人が同時に混在する事により危害が生じる事から、定常作業では機械が自動運転する場合が多く、その中で加工物の搬入・搬出が人により行われる場合と、人が常に介入する非定常作業でかなり多い災害が発生している。又、一度に3人以上が被災する重大災害は減少傾向ではなく、逆に増加傾向にある。

総括すると、労働災害の発生状況は

- ○ *製造業で3割（死傷者）又は2割（死亡者）*
- ○ *労働者 300 人以下の中小企業で9割*
- ○ *挟まれ・巻き込まれが5割（死傷者）又は3割（死亡者）*
- ○ *50 歳以上が5割（死傷者）又は4割（死亡者）*
- ○ *多くが非低常時*

となり、これらに対する重点的な予防措置が講じられれば、災害件数は大幅に減少する事が可能である。

挟まれ・巻き込まれ災害の多くは予見可能であり、かつ回避可能である。具体的には、例えば、危険源の箇所にガードをつける、そのガードを開くとインターロック装置の電気接点が閉から開へとなり、電源が遮断される。さらにそのインターロック装置は無効化防止の為のタンパープルーフ構造になっていれば、簡単にいたずらは出来ない。そしてリスクの程度により、安全制御回路を適用する。非低常時の作業では、電源を遮断し不意な起動防止装置をつける或いは、低速回転での作業のみ許可をする。これらのそれ程複雑ではない安全技術を適用するだけで、事故の発生を未然に防止する事が可能である。つまり、そこに予防措置としての安全設計を適用する事により、その予防効果としての死傷者数低減は現実的に実現可能である。

追加予防措置に必要な安全デバイスとしては、タンパープルーフの為の分離式アクチュエーター及び強制乖離接点を備えた安全スイッチ、電磁ソレノイド付きの安全インターロックスイッチ、安全ライトカーテン、安全マット、片手では操作できない両手操作盤、並びにこれらの信号を安全に伝達し、接点の溶着を防ぐ為の強制ガイドと強制乖離接点を有し、電源遮断を実現する安全リレーや安全PLCとそれに通信機能を付加した安全フィールドバス・コントローラー、モーターの回転静止安全監視モニター、ホールド・ツ・ラン機能等大部分のものは既に市場で提供されている。要するに、これら既存の技術を適用して災害が発生したのか、或いはこれらの存在を知らなかったのか、又は知っていてもなんらかの理由により採用しなかったかのは、災害の責任論になった際には大きな差異が発生してくる。

梅崎によれば（注 9）国際水準の設備安全方策の中でも、固定ガード、可動ガード、保護装置、制御システムの安全関連部に関する要求事項を確実に実施すれば発生した死亡災害の8割近くに対して災害防止効果を持つことが判明したとされている。同様に事故情報、安全技術情報、リスクの定慮化手段、安全方策の提示手段、遠隔安全診断手段等を包括する安全設計支援システムが提案されている。

労働災害の所轄官庁である厚生労働省は、1999年に労働安全衛生マネジメントに関する指針並びに 2001 年に国際機械安全の概念に大方整合された「機械の包括的安全基準に関する指針」を策定しているが、いずれも通達の為に強制力をもたず、国内事業所の多くはその内容を現場に適用するに至っていない。

しかしながら、労働安全衛生マネジメントシステムは、あくまでマネジメントシステムであって、これは安全技術そのものではなく、それが実践されていると言う前提の基において、初めて有効性を発揮できるもので、危険源が同定・見積・評価・低減されていない機械が存在する作業現場に適用しようとしてもそれは本末転倒の話となる。

8．繹的予防措置とその利点

事故が発生すると日本では、報道機関が大騒ぎをしてすぐに「誰の責任か？」との犯人探しをする。その追求が済

むと「個人の処罰」が行われ、事は一件落着し「事件解決」となる（Fig.4）。

従来手法では技術の問題にたどり着かずに、特に労働災害の場合には日本の社会保障制度の恩恵を蒙り、労災認定が行われ補償金が支払われると同時に、安全設計の事は葬られてしまう。つまり、失敗の経験が設計にフィードバックされない為に事故の経験が安全技術に生きてこない。要するに、安全の原理原則、規格、リスクの同定・評価・見積りの手法、追加的ツールとしての安全デバイスは既に揃っているが、国内では設計者責任が追及される社会制度になっていない為に、残念ながら折角の指針も実践になかなか適用できない状況にある。

本来であれば演繹的な予防措置としての「安全設計」を設計者原則及びリスクアセスメント及びリスク低減等の定まった手法に則り実践していれば、事故を事前に予見並びに回避出来た可能性は大いにある。否、大部分の事故がこの予防措置のアプローチを適用せずに危険源が数多く放置されていた故に事故の発生は基本的に予見可能であった。

欧州の CE マーキング制度は、設計者責任を明確にして事故発生後にその責任が全うされていなかった事が判明すれば罰金が支払われる。その懲罰を受けないようにする為に設計者は予防措置としての安全設計を実施する。米国も ANSI B11.TR3-2000 によりリスクアセスメント及びリスク低減の実施を具体的に求めており、複数且つ多数の機械が混在し使用される自動車産業などにおいては、米国安全衛生庁（OSHA）の立会い検査等で、リスクをどれだけ低減したかの実証と図書を求められる。国際的には、残留リスクが認められているので、リスクが ALARP（As Low As Reasonably Achievable）の範囲に低減されていれば良しとされる。ここでは、リスク低減と経済性の関連性も言及されている。厚生労働省のその後の調査によれば、包括基準を適用していたとすれば、7-8 割の災害が回避できていたであろうとの観察がなされている。リスクーコストの関連性に関しては、田中・染谷の考察がある（注11）。

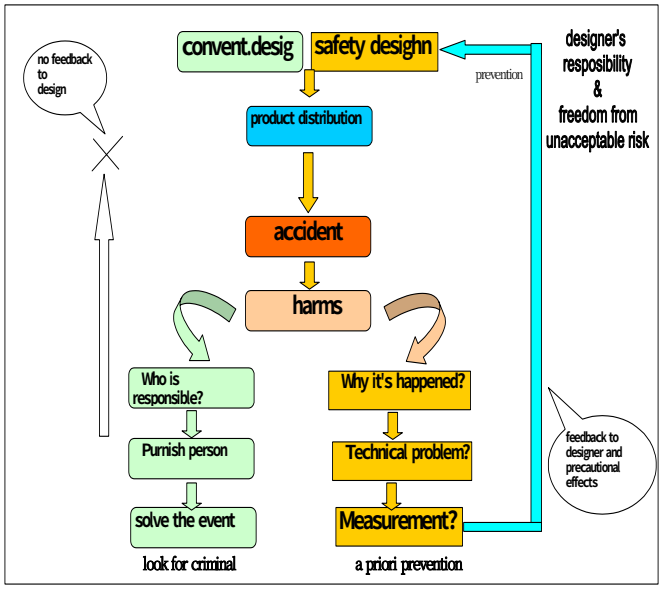

Fig.4　予防措置の効用

演繹的予防措置を実施することにより、それなりの効用がある事は国内の現段階では事例の数こそ限定されるが、産業界での独自のヒアリング調査により国内でも今までにいくつかの実証例が出てきている事の確認がとれた。

例えば

- ○ *標準化導入で無駄が減少し利益還元に貢献できた*
- ○ *後付けではなく、最初から設計に安全を取込む事によりそれ程コストアップの要因にはならないようになった*
- ○ *グローバル市場への製品提供の為、従来複数合った社内標準をひとつに統一し、対応時間の短縮及び在庫数の削減により利益還元に貢献できた*
- ○ *演繹的予防措置を講ずる事で、第三者認証機関への支出が大幅に削減できた。要するに、第三者から指摘を受けて安全設計を追加的にするのではなく、事前に国際規格に則り設計作業を進める為、やり直しを最小限に留める事ができ、大幅な後からの追加的保護方策の実施や納期対応の遅れが回避出来る様になった*
- ○ *品質管理や環境マネジメントシステムの中に、安全を採り入れ生産性が向上し、CSR にも役にたった*
- ○ *日本で初めて国際機能安全規格に準拠した制御製品を発売し、それが第三者認証書取得済み故に、その製品のみならず、非安全の他のシステムも安全のおかげで納入する事が出来るようになり、マーケティング上多大な恩恵を蒙った*
- ○ *会社にとって重要な事は生産性の向上。それを達成するには、先ず安全確認型の止まる安全と、生産技術を向上させていかに止まらないかを工夫して、「止めない安全」を達成し、稼働率がかなり向上した*

日本では、機械の危険源を洗い出すリスクアセスメントとその低減措置が法的強制力を持っていないが、その多くの国際的な手法は JIS 規格として制定済である。労働災害の事故調査でも設計者責任は追及されない。問題点を安全設計の観点に集約させれば既知の手法を用い、事故の予見可能性・回避可能性をまっとうでき、演繹的な予防措置を講ずることが可能である。同時に、設計者は充分な説明責任を果たし過失以外の責任は追及されない。これら予防措置の有効性に付き、NPO 安全工学研究所では調査活動を継続して行っており、その結果を別途公表する予定でいる。

参考文献：

(1) Herbert William Heinrich, "*Industrial Accident Prevention -A Scientific Approach-"A Safety Management approach" 1931*

(2) ISO/IEC Guide 51:1999

(3) 杉本・粂川・深谷・清水・梅崎・池田・芳司・蓬原「安全確認型安全の基本構造」、日本機械学会論文集第 505 号 C 編、1987

(4) 向殿政男「働く人の安全と健康」2000 年 4 月号ーフェールセーフとフォールトトレランス、中央労働災害防止協会

(5) 杉本旭「機械にまかせる安全確認型システム」、中央労働災害防止協会、2003

(6) 原宣一「宇宙先端　第 11 巻第 1 号ー信頼度の意味するもの」、1995 年 1 月

(7) IEC60812　Analysis techniques for system reliability - Procedure for failure mode and effects analysis (FMEA)

(8) General Principles of Software Validation; Final Guidance for Industry and FDA Staff, 2002

(9) 梅崎重夫「産業機械における災害防止手法の考察と高機能型光センシング保護装置の開発に関する研究」2004 年 11 月

(10) IEC61508, Part 5: Functional safety of electrical / electronic / programmable electronic safety related systems - Part 5: Examples of methods for the determination of safety integrity levels

(11) 田中紘一・染谷美枝ーA.ノイドルファ著「安全な機械の設計」を翻訳して考えたこと、REAJ 誌2003　Vol.25.No6