機械安全のデジタル制御とアナログ制御
～人と機械の協働へ向けての方向転換

加部　隆史　（NPO 安全工学研究所）

1. はじめに

機械類の安全を配慮する際，福島原発震災が示す通り，安全が達成されない場合，社会に多大な影響を及ぼす事から考え始めたい. 福島原発震災の場合，今回の様な過酷事故(severe accident=SA)は，現実として工学的に起りえないという政府の公式見解の基に，SA に係わるリスクを配慮の対象外としてしまった事が大きな問題である．欧米のリスクベース社会では，SA への対応は事前に予防策として講じるが，事後責任に基づく日本社会においては，問題が事後になって初めて討議される．

これらを考えると，安全とは技術により達成し，社会へ安心をもたらすという社会性の観点から，安全を取巻く様々な要素を配慮する事で，初めて安全安心社会が達成されうるという事になる．

オックスフォード大学が提唱した PESTEL 分析に基づき，安全安心社会達成の要素を，政治（P)，経済（E),社会（S),技術（T),環境（E)， 法律（L)の６要素から考察すると，おおまか図１の様になる．福島原発震災が語るように，技術は本来第一義的に重要であるが，実際の社会においてはリスクベース社会か否かの要素も加わり，複合的要素により，事後の動向が変化してくる．福島原発震災での教訓は，事業者が法規制通り設備を運転し，かつ第三者機関による定期監査を受けていて遵法が証明されても，実際に事故が起き危害が発生した際には，第一義的に事業者が責任を問われるという事である．

それ故，事故の要因となる危険源を，予防概念に則り如何に事前に処理できるかが課題となる．

2. 人と機械の協働へ向けて

機械類の安全技術は，欧州協定に基づき，1980 年代半ばに発令された欧州機械指令に端を発し，労働者の安全を守る人権の観点及び，自由貿易の確保の観点から, ISO12100 の安全に関する設計原則で求められる様に，リスクアセスメントに基づきリスク低減の方策を講じるという事前の予防措置に基づく手法による国際規格で整備されてきた.

当初の欧州機械指令 98/37/EC では，原則として，人に対し危険な動きをする機械は，その様な機械を防護し，危険な動きの際には機械を停止するという基本思想（隔離と停止の原則）に基づいている.

2006 年 2 月に，ドイツ職業保険組合中央研究所 BGIA(現在 IFA)が，機械の安全装置の無効化に関する報告書（ISBN 3-88383-698-2）を出版し，重大災害の多くの部分が，安全装置の無効化に起因し，かなりの割合の労働現場で無効化が定常的に実施され，かつ会社責任者がその事態を把握しているという状況を把握した. 安全装置の無効化の主要因としては，安全装置により機械が停止する事に係わる労働生産性の低下の回避，或いは機械設計者と機械使用者の間での不十分な情報伝達等があげられた.

すなわち，事故の大部分は，機械の自動運転中ではなく，機械の非定常作業において実施され，そこでの安全確保の解決案が未だ理想的な形で提案されてきていない．筆者は，この問題を安全工学シンポジウム 2006 で，安全技術のフレームワークの中の UDF(un defined factor)として，指摘してきた.

更に，産業安全研究所（現在 JNIOSH)は 2005 年に危険点近接作業の災害防止戦略に関する基礎的考察を発表し，以下に述べるプロセス・モニタリングに通じる問題点を指摘している.

その為，欧州機械指令 2006/42/EC に於いては，隔離の原則につき, IEC61800 関連の機能安全規格の整備も相まり，特定の条件下においては，人と機械の協働を可能とする選択が追加された．工作機機械の

	Parameter	Examples
P	Political	human right free trade(WTO/TBT)
E	Economic	competitiveness productivity avairability
S	Social	ethics Risk-based society, safe life
T	Technical	safety of machinery A-B-C standards ISO9000 management system
E	Environmental	e.g.ROHS directive design for disposal
L	Legal	e.g. in case of EU: Machinery Directive 2006/42/EC EMC Directive Low Voltage Directive e.g. in case of Japan: OHS law Art.28-2: Risk Assesmet , but only recommendation

図 1. PESTEL 分析

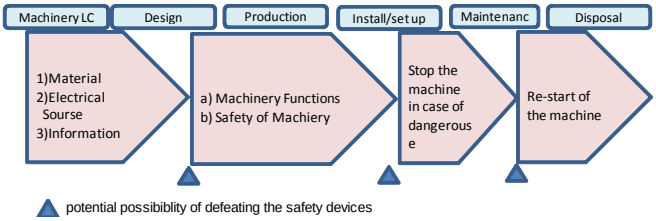

図 2. 機械のライフサイクルと安全

安全性に関する EN12417 に基づくマシニングセンタにおけるプロセス･モニタリングでの mode 4 の導入等は，一つの例としてあげられる．インターロッキング・デバイスに関する EN1088 では，無効化を防止する為の追加的要求事項が付加された．着目すべき点は，技術的に他に方策が無く，機械使用者がそれを受諾した場合に限り mode4 の適用が容認される，という事で，隔離と停止の原則に基づく機械安全の限界を，従来の労働安全により補完し，人と機械の協働を容認するという考え方である．

同様に当欧州機械指令では，とりわけ危険な特別機械については第三者機関の型式認定が義務付けられていたが，製造者が安全の妥当性を自らの品質保証システムにより証明する事が出来れば，必ずしも第三者機関の介入をしなくても良い事となった．実力のあるものづくり企業において，その実践は可能である．

2007 年に制定された，安全ドライブシステムに関する IEC61800-5-2 では，従来のように機械を停止せずに安全な減速，安全な静止，安全な停止，不意な軌道の防止等の機能を定めており，これにより，従来の安全インターロック機器等によるデジタル I/O の処理以外に，モータの速度制限を実施する事により，機械を止めずに安全状態を確保出来る技術を示している．

本来機械は，自動化技術の進化に伴い，使用者へ多大な利便性と効率をもたらすもので，図 2 に示す通り，機械へは W.バイツの工学設計が示す様に，

1) 材料 2)駆動源への電気エネルギ 3)制御のた

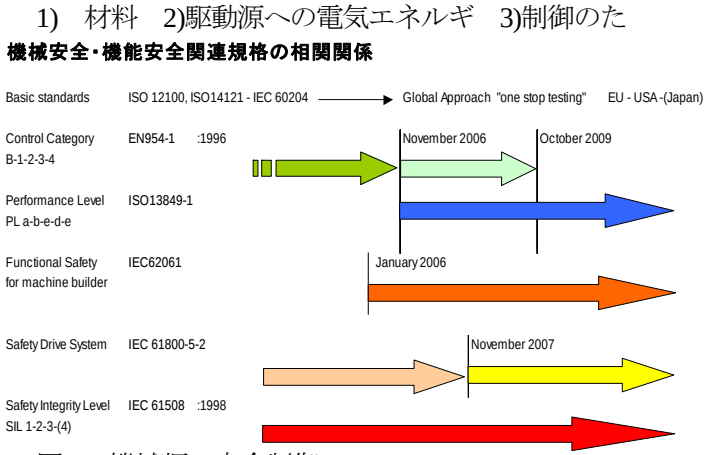

図 3. 機械類の安全制御

めの必要情報が入力される．機械の機能を実現する為に，安全原則に基づき機械を運転すると，場合により，機械の機能を発揮できない．或いはその生産が低下する為，上述の安全装置の無効化が往々にしてり，機械の機能を発揮できない，或いはその生産が実施される事になる．かつ，その無効化の潜在的可能性は，機械の設置・試運転で始まり，生産物の荷崩れ，保守点検の段階等，機械の全ライフサイクルに亘り存在している．

機械の安全性を確保し，かつ従来それに対し反目的であった労働生産性の向上を促進する可能性は，機械の駆動源であるモータの速度を如何に安全に制御するかに係わってくる．安全と生産性の向上を両立させる要素技術が，欧州では近年市場に流通し始めており，これは隔離と停止の原則(止める安全)から，人と機械が協働する安全（止めない安全）への転換の可能性を示している．

3．安全な制御

安全な機械は，図 3 に示す通り，先ずリスクアセスメントに基づき，機械の使用目的を限定し，そこでの危険源を同定し，人と機械が同居する危険状態でのリスクを見積もり，その評価を基に，リスク低減を実施するというリスクベースド・アプローチが国際規格で示されている．安全な機械の設計原則に関する ISO12100 では，3 段階方式を定め，機械の本質安全設計を最初の優先順位に上げている．

制御安全については，出発点として IEC60204-1 で求められる電気安全に対応し感電対策，非常停止装置，電源管理等を実施する．

制御安全では，例えば多くの機械が該当する制御カテゴリ 3 或いは，ISO13849-1 のパーフォーマンス・レベル d の場合，図 4 に示す制御機能が求められる. 重要なのは, 冗長性及び故障検出機能である. 従来は，基本的に安全インターロック及び安全コントローラのフェールセーフな AND 回路により安全を達成する事が主流となっている．これは，安全機器のデジタル I/O 信号を, 機械の危険な動きの際に, 送信し駆動源を遮断する方法である．

機能安全 IEC61508 は，ソフトウェアに関連するアンブレラ規格であり，化学プラント，鉄道，産業用自動化機器等幅広い適用範囲がある．自動車の車載用電子機器については，別途 ISO26262 がある．

欧州では，機能安全の一種である安全ドライブシステムの規格 IEC61800-5-2 が国際規格として成立するかなり前から，EN9054-1 に基づきモータの速度・トルク・停止位置等を監視し，機械の危険な動きの際にパルスブロックする事より電源を一時的に遮断し，安全な状態になった際に，モータを再起動させる方法が実施されてきている．この場合，電源遮断による再起動までの手間を省略し，短時間でモ

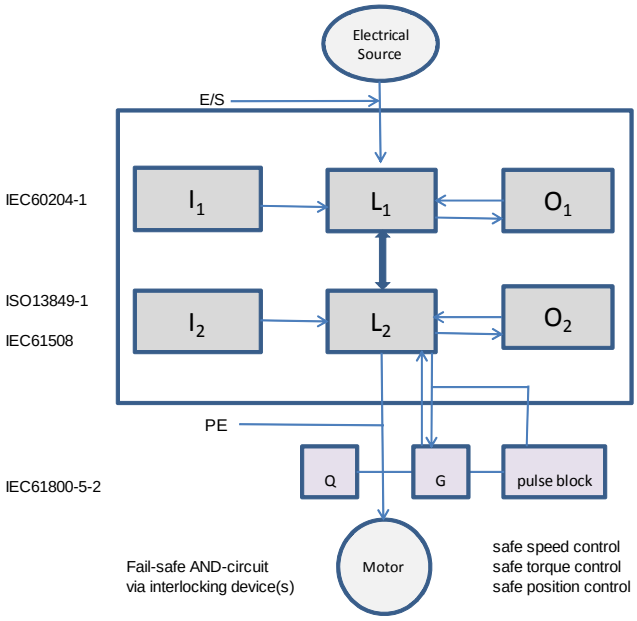

図 4. PL d のアーキテクチャ

ータの駆動を復帰させることが可能となり，アベイラビリティが向上する(利点１).

更に，サーボドライバの位置指令を制御する為，従来のハードウェアとしての外付けセンサは不要となり，機器構成上もコンパクト化と簡素化が図れる（利点 2）.

又，電流をパルスブロックする機能の為，停止並びに再起動に要する時間が顕著に短縮され，生産性の向上にも寄与する（利点 3）.

ハードな防護柵を必要としないバーチャルフェンスにより，工場敷地での多大な省スペース化が実現可能となる（利点４）.

この安全ドライブシステムは，どの機能を達成するかにより，必ずしも IEC61508 に則らず，ISO13849-1 のパーフォーマン・レベルに基づき達成する事も可能である．ISO13849-1 に関する BGIA-Report 2/2008 では，通常の機器の組み合わせによりパーフォーマンス・レベルを達成する手法も示されている．どちらの機能安全の規格を適用するかにより，設計者の負荷がかなり異なってくるため，その見極めが重要である.

４．安全要素技術の進化

これら制御安全の規格の進化と共に，安全要素技術も段階的に発展を遂げている．図 5 に示す通り大まかな区分けとして，第１段階は，安全なインターロック装置で，例えば，フェールセーフな安全スイッチと，電源遮断を確実に行い不意な軌道を防止する安全リレーユニットであり，これらは全てハードワイヤリングで結線されてきた．当初，非常停止つ抜いてはソフトウェアを介さずに，ハードワイヤリングで直接コンタクタを通し電源遮断する事が求められていた.

第 2 段階は，1998 年に機能安全規格 IEC61508 が成立したのと同時に，安全 PLC や安全フィールドバス・コントローラ，そして安全レーザースキャナ等が，この規格を基に市場に提供されてきた．機械的スイッチ等にも，電子基板を装着するものが出て来た．IEC60204-1 の関連個所の変更に伴い，これらの規格及び安全要素技術の整備により，安全に係わる停止の信号もソフトウェアを使用し処理する事が可能となった. 化学プラントの DCS についてもソフトウェアで遮断する事が多用されるようになった.

安全装置の無効化の主要因である生産性の低下に係わる問題を克服する為には，機械を安全な領域まで減速し，そこで労働者が作業をし，それを終えたらすぐに機械が再起動する事により，逆に安全を実施しかつ労働生産性が低下しないという目標が達成可能となる.

第 3 段階は，機能安全規格により，安全機能をソフトウェアに組み込み，通常機器と同じ様な扱いで安全を達成する方向性で，１）機械の暴走防止及び２）人の進入検知の組み合わせであり，安全に関する世界的な研究開発プロジェクトからして，次世代の要素技術とされている.

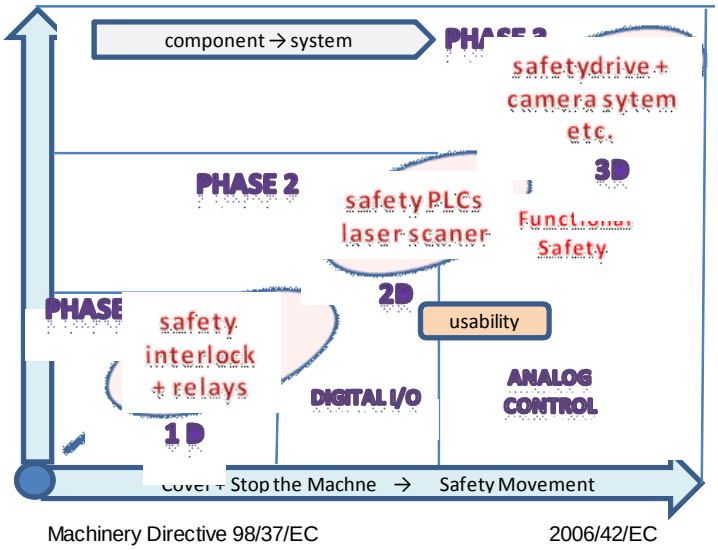

図 5. 安全技術の進化

SIEMENS は，デジタル I/O 及び安全ドライブシステムの安全制御システムを Safety Integrated のモットーの基に 19190 年代後半から市場に提供している．BOSCH/Indramat は 2008 年に，安全ドライブシステムを Safety on Board，Functional Safety in Automation Technology - Safe Motion の概念で提供している．IEC61800-5-2 による STO,SS1,SS2, SOS,SLS,SD1, SLP, SMS,SBS,等を基本とし，このシステムを適用する事により，設備の生産性が向上する事を強調している.

ロボットメーカ ABB は，Don't let safety fence you in

の標語で，Electronic Position Switch and SafeMove を 2007 年から紹介している(図 6 参照). 2009 年に ABB はドイツの自動車メーカ BMW から 2100 代のロボット包括的契約を受注し，これは，ドイツの REIS-ELAN 社の協働特許に基づく安全コントローラにより対象ロボットは全てバーチャルフェンスを構築可能である．この安全コントローラが上市されたのは, 機能安全規格が発表される直前の 1997 年であった.

2010 年 5 月に，ドイツ大手のロボットメーカである KUKA が，REIS-ELAN 社のバーチャルフェンスの特許ライセンスを取得したと報道された．バーチャルフェンスは，従来のロボット用フェンスを必要とせずに，人とロボットが直接協働する作業を要素技術として提供するもので，今後これにより，生産現場での生産革命をもたらす可能性を含んでいる．

これらの動きに対し，国内では数社のドライブメーカが最近になり，安全ドライブシステムを部分的に採用し，市場に提供し始めて来た．安全ドライブシステムへの対応は，世界市場における日本の AC サーボモータの市場シェアと甚だしく不均衡なものであり，その遅れの改善が，日本のものづくり競争力にとっては不可欠であると思われる．

上述の技術は，機械の暴走検知技術であり，反応速度が＜100ms の安全無線装置も既に流通している．人と機械の協働を安全に実践する為には，それに加え人の進入検知が必要とされる．従来の 1 D の安全ライトカーテン或いは単光軸，２D の安全レーザースキャナに加え，３D のカメラシステムの研究開発が現在実践されている．欧州の科学技術政策である FP6 或いは FP7 に於いては，安全技術を前提とした研究開発プロジェクトが多数存在するが，日本においてこの分野では, 残念ながら安全の研究開発自体, たこ壺に入り込み，横断的かつ体系的なものになっていない.

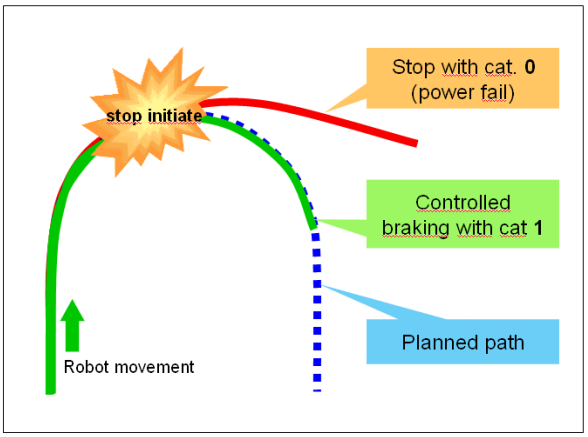

図 6.　ABB SafeMove(soruce: ABB White Paper)

５．おわりに

体系化された機械安全の法規並びに規格類は，科学および技術の進歩並びに市場での実践上の問題点を加味し，確実に進化してきた．リスクベースド・アプローチにより，事故を安全設計により未然に防止する為の規格が体系化され，更に進化をつづけている．とりわけ，現在は人と機械の協働を実現する為，機能安全関連規格並びにそれを受けた安全要素技術が次の段階へと進んでいる．

従来の機械安全は，隔離及び停止の原則によりリスク低減を達成してきた．安全装置の無効化問題に代表される通り，安全と生産性とのトレードオフの問題解決が望まれている．そこで，人と機械の協働を可能とする要素技術として従来のデジタル制御中心から，アナログ制御に基づく安全ドライブシステムの考え方が大分普及してきている．

人と機械の協働の形態は，１）生産現場における自動化技術と２）新産業としての消費者をも対象としたサービスロボットに大別される．１）につき欧米のリスクベース社会において，これを実践するにはおそらく時間の問題であるが，日本国内の場合，労働安全衛生法で現在のところ人と機械の協働を必ずしも容認していない. 安全ドライブシステムの JIS 化さえも，現段階では進んでいない．その為，人とロボットが共存し作業をするこれからの要素技術の一つとしての検討の土俵にさえも上がっていない．又，２）のサービスロボットについては，安全要素技術が未開発であるのに加え，日本の場合，予防と補償に基づく社会制度が未発達の為，製品が出来てもなかなか流通しにくいという問題がある．

機能安全といった場合，それはデジタル I/O の処理のみならず，アナログ技術である速度制限を如何に安全に制御できるかで，制御構成が全く異なって来る．安全ドライブシステムの利点については本文で 4 点説明した．すなわち，現在の日本は安全技術の動向につき，とりわけ欧州と大きなギャップを抱えている．日本の産業競争力としてのものづくりに安全要素が加味されないとなると，気がついた時にはガラパゴス化していたというこれまでの複数事例が示す事と同じ現象が起こらないという保証はどこにも存在しない.

機能安全規格 IEC61508 は多大な設計負荷と認証費用及び必要時間が伴う為, 量産品の場合でないと, その費用が償却できず，製品が上市できにくい事を最後に明記する．すなわち，サービスロボットの場合は，大量生産品でない場合，適用が困難であるという事である．PL d の場合，大部手間は省ける．