止めない安全と労働安全

正　加部隆史，NPO 安全工学研究所

１．はじめに

機械安全の概念と方法論は，1980 年代の半ばに欧州で法律として発令された一連のニューアプローチ指令により体系化された．危害は，そもそも機械の危険源と人が共存する事で発生する．これは，従来の安全確保が人への教育に頼っていたが，これでは限界がある為，その対象を人でなく，機械の危険源へと変更した．

機械安全は，＜機械の使用目的の制限ー危険源の同定ーリスク見積ーリスク評価ーリスク低減ー残留リスクの提示＞という手順により達成され，これらは ISO と IEC の国際規格により，A-B-C の三層構造で体系化されてきた．リスク低減は 1．本質安全設計 2．追加的保護方策 3．使用者への情報提供の三段階方式が，優先順位順に規定されている．前述の法律による強制力と，その目標達成は任意の規格に準ずるという構造になっている．

機械安全の基本は，危険源に対しての隔離と停止の原則に集約され，使用者の安全教育は範疇外と定義している．機械の全ライフサイクルを考慮すると，開発ー設計ー製造ー販売ー設置・運転・保全ー廃棄の流れがあるが，機械安全は基本的に，機械設計者を対象としており，それは機械の開発から販売までである．その後の機械の使用は，使用者にゆだねられる．

運転には，人が介入しない定常運転（自動運転）と人が介入する非定常運転があり，基本的に事故は非定常運転作業において発生する．同時に，機械は物を生産する為のものであり，資本主義社会においては生産性と作業効率が要求され，隔離と停止の原則に基づく機械安全の概念とは利害対立が生じる．そして，事故の大半は危険な機械でのはさまれ･巻き込まれである．これが，現状の機械安全の限界であり，その状況を記述し方策を考察するのが本稿の目的である．

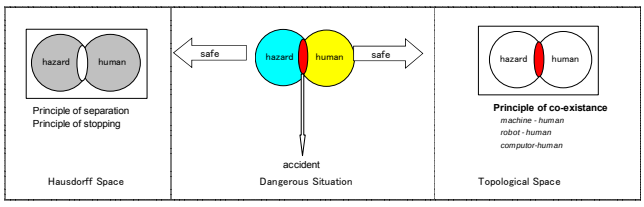

図 1．止まる安全と止まらない安全

２．非定常作業

図 1．のベン図中央は，危険源と人が共存し危険状態となり放置すると危害に繋がる事を示す．左のベン図は隔離の原則或は停止の原則による止まる安全を示す．ベン図が合わさったところに人は接近できず安全を確保する状態で，右側のベン図は，危険源と人が共存する危険状態であり，そこで止まらない安全を確保する状態を示す．

止まらない安全とは，危険状態において機械と人が共存して重大な危害が発生せずに，危害は受入可能な程度に留まる事を意味する．

それを達成する為に以下の方策が存在する：
ー本質安全設計により機械の速度とトルクを管理する
ー安全なドライブシステムを適用する

その為に，危険源と人が共存する非定常作業の実態を先ず考察する事にする．

２．１．非定常作業の実態

非定常作業は，先ず機械への加工物の設置と調整の段階，自動運転中の製品の不具合の場合，保守点検や清掃の場合等，機械使用者が機械を使用する際に頻繁に実施される．安全確保の為には本来機械を停止した状態でこれらの作業を実施すべきではあるが，ものづくりを実践する場合，機械を動かさないとできない作業が多々発生する．

機械安全の設計原則を定める ISO 12100 は設計者を対象としている為，その範囲はあくまで機械が市場に流通迄で，ここに機械安全の限界が明示されている．その後は使用者側で，労働安全の概念から機械を調整，運転，保全，廃棄する必要がある．

産業用ロボットの場合は，教示モードへ切換え，ホールドツランを実施する教示デバイスの使用が該当規格で定められている．

旋盤の場合，主軸回転は 50 rpm/min.以下，サーボ軸は 2m/min.以下での作業が定まっている．マシニングセンタの場合，モード 1-3 の規定はあるが，回転速度や移動速度につき，旋盤程の閾値は定められていない．

多くの製造現場では，単体の機械が結合されひとつのラインとして初めて機能を発揮する例が多々あり，これらは**統合生産システムとして ISO11161** でその安全要求事項やシステムインテグレータの責任が定めら

れている．これら統合生産システムにおいては，とりわけ作業領域が広くなり，複数の制御盤により個々の機械が起動される為，人が防護柵内に存在していない事を確認の上起動する事，或いは低速モードで機械が運転される事が安全の条件とされる．
それには，確実な電源遮断，人の出入りの管理，防護柵がある際はその内部が閉鎖空間となる為，そこからの緊急脱出の手段等，電源管理と人の出入り管理が重要となる．

２．２．要素技術による解決

２．２．１．止める（止まる）安全

多くの生産システムは機械の統合システムであり，機械の設計，設置，試運転，保全，改造等の段階で危険源の適切な処理が要求される．とりわけ，機械設備の変更管理及び繰り返しのリスクアセスメントの実施が怠った場合には，危険源が顕在化し，重大事故の要因となる場合が多々ある．

安全に設計された機械を使用者側で設置する際に，調整作業が必要となる，不具合品が製造された際にそれを除去する必要がある，製品が搬送される際に荷崩れが起きればそれを補正する事が求められる，プレス等は金型交換が必要とされる，大きなロールの清掃は電源遮断の状態では可能でない場合がある．

機械安全が求める隔離と停止の原則はここでは通用しない為，機械運転者の使い勝手を配慮した上で，**電源遮断と再起動のフローを明確に**し，その都度安全な状態が保持される事がリスクアセスメントで要求されてくる．

先ず，機械システムを包囲する固定ガード（**防護柵**等）があり，これらについては ISO14120 等の規格で定められた安全距離や防護柵の強度に配慮が必要となる（図 2．参照）．

図 2．防護柵と統合生産システム

防護柵の出入り口の扉については，インターロックスイッチで監視する必要が有り，リスクの度合いにより電磁ロック有り・無し，場合により防爆対応等の選択が必要となる．

扉を開けるとインターロックスイッチにより，内部機械の電源は遮断され安全な状態になる（①ISO 12100-2, 5.5.4 遮断及びエネルギー消散に関する方策）が，この状態で防護柵の内部に誰が，或いは何名の人が入り，再起動の際に，全員退出した事を確認する事が求められる．

この手段として，例えば南京錠等によるロックアウト・タグアウトシステムが挙げられる．インターロックスイッチが開の状態，すなわち電源遮断の状態で第三者が扉を閉めて機械の再起動防止の為にスイッチをロック（①同上，5.5.4 項）する．

しかしながら，これらの作業は人が行うために，万が一機械作業者が防護柵から退出し，出入り口の近くに置き忘れた工具等を取りに戻る際，その距離が数メート　ルであれば心理的にロックをせずに中に入ってしまう事が合理的に予見可能となる．もしその工具が，機械の影にあり第三者が扉を閉めて機械を再起動すると，中に閉じ込められてしまう．閉鎖空間においては内部から脱出可能性を持たす事が求められており，その為には緊急脱出ハンドル，ボタン等が要求される（②ISO 12100-2, 5.5.3　補足された人の脱出及び救助のための方策）．

これら ISO 12100 で要求される電源遮断，ロック，緊急脱出の**3 つの機能をひとつした安全ドアハンドルシステム**が存在する（図 3．参照）．これは従来のプラグシステムの代替えとして誕生したもので，とりわけ自動車の生産システムにおいて多用されている．

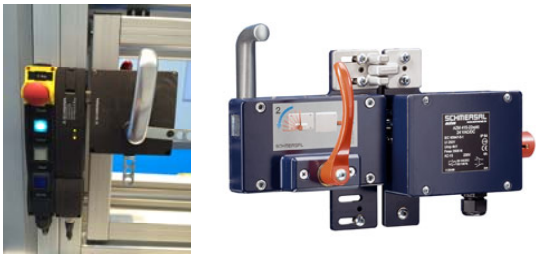

図 3．ドアハンドルシステム(Schmersal 製)

惰性回転がある機械等では，図 4．に示されている**キートランスファー（トラップドキー）・システム**により，同一キーにより異なる場所での機械の電源遮断と再起動を遅延時間の管理を含め，簡単に実施する事も可能である．これには電気が不要の為，安全スイッチと遅延回路付きの安全回路が必要無く大変経済的な解決策となる．

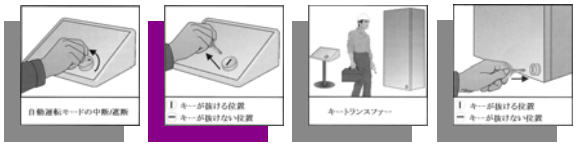

図 4．キートランスファー・システム

２．２．２．止めない安全

これらは，基本的に電源遮断に関わる方策であるが，他方で危険状態であっても電源遮断せずに危険状態で

人が作業できる環境を設定する可能性がある．

ー本質安全設計

回転機の回転数が制限され，それによりもたらされる速度やトルクが，充分に回避可能な場合．或いはロボット等でも人と衝突しても重大な危害を及ぼすに至らない程エネルギーが制限されている場合で，図 5. にある様に AUTOMATICA 2014 で出店された KUKA の LBR，Universal Robot 等の例がある．

欧米では産業用ロボットの安全に関わる ISO 10218 の関連規格が整備されつつあり，とりわけ製造用人とロボットの協働につき小型ロボットが複数上市されてきている．これらは Collaborateive Robot という表現で，ドイツでは IFA，Fraunhofer，アメリカの RIA 等が積極的に推進している．

ここで，機械設計者が **ISO 13849 の PLd** に準拠した制御設計を実施するに留めるか，或いは **IEC 61508 の SIL** に準拠した設計を実施するかにより，設計並びに認証作業の負荷が大きく事なってくる．

図 5. AUTOMATICA 2014 での協働ロボット

ー安全ドライブシステム(IEC 61800-5-2)

これは機能安全規格により速度監視，制限を行い安全な減速，静止，不意な機動の防止等をドライブ制御に具備したものである．これにより，バーチャルフェンス等の構築は可能となるものの，個別アプリケーション毎の安全パラメータ設計が必要とされ，適用が必ずしも安易にゆかない事がある．同様に，これによりロボットの暴走は監視できるものの，作業領域に人が侵入する事は別途安全なセンサにより監視される必要が有り，この分野での要素技術の開発は未だ最適化されていない．

前述の，工作機械の軸速度監視等はこの安全ドライブシステムの規格の適用により達成可能である．しかしながら，現実としては自働・手動の運転モード切替により非定常作業を実施している事が殆どである．そして，機械の安全設計が，使用者の使い勝手の観点から充分に配慮されていない場合には，機械の安全装置が無効化され，折角機械設計者が施した安全設計は無用の長物と化し，危険源が顕在化し重大事故に繋がるという悪循環に陥ってしまう．

フィールドのセンサレベル並びにドライブシステムの安全関連信号の処理は，システムが大きくなればなる程，**機能安全規格対応の安全通信**の必要性が高まってくる．この際，たとえば統合システムのどこかで短絡によりシステムダウンした際には，MTTR の観点から，その故障が何処で発生したかを直ぐに診断できるシステムか否かが重要となってくる．IEC 61311-9 で定められた通信プロトコールはこの点が配慮されてきている．

PLC の標準化を推進する PLC open では，従来の PLC 言語の標準化を超え，言語を XML で記述する事，そして安全・ドライブシステム・通信の標準化を一体化して推進している．これらの標準化が推進される事により安全の確保と同時にエンジニアリングコストの削減が見込まれている．図 6. ～図 8. 参照．

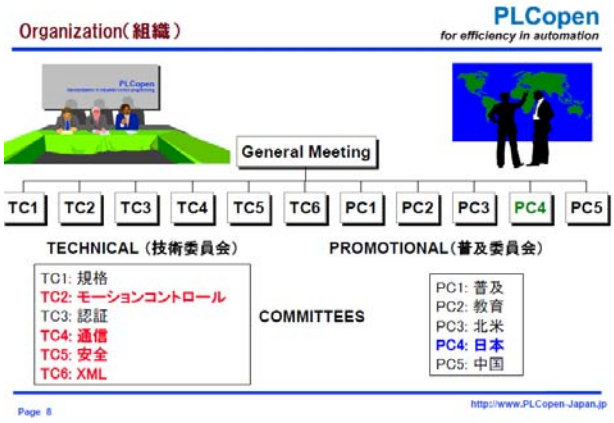

図 6．PLCopen の組織

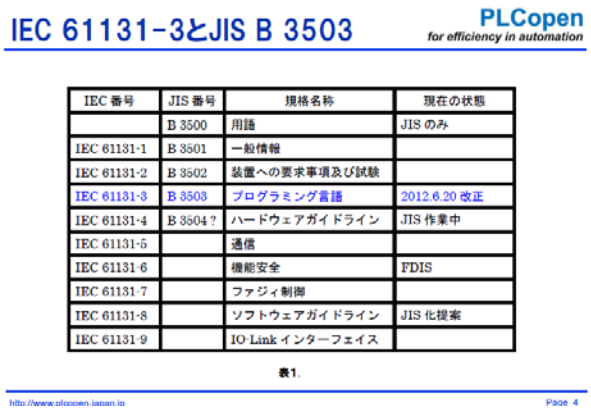

図 7. IEC61131 関連規格

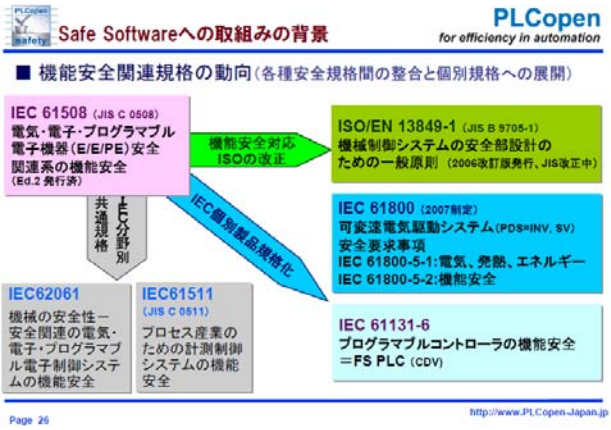

図 8. PLCopen の安全への取組み(ULR 公開資料)

３．労働安全概念への回帰

機械安全の隔離と停止の原則の可能性と限界をこれまで観察して来たが，機械の非定常運転・作業については，いくら個別機械が安全であっても，その操作と手順を正しく行わないと，リスクが顕在化してしまう．それ故，個別機械の残留リスク及び複合機械システムの際の電源管理の手順が労働安全の観点からとりわけ重要となってくる．

ドイツ工作機械組合（VDW）は，**マシニングセンタ**の従来のモード 1−3 に対し，**モード 4 の概念**を導入しようと働きかけをしている．すなわち，生産を維持するために人と機械の協働が要望される際に，他に技術的な可能性がなく，機械使用者がそれを求めた際には，機械設計者と機械使用者が念書を交わし，適切な安全教育を受けた作業者がその作業を実施するという事で，欧州機械指令が禁じている人と機械の協働を例外的に認めようとしているものである．従来機械安全は危険源へアプローチする事により，従来の人にアプローチする労働安全の限界を越えようとした．ここでは，機械安全概念の限界から，それを乗越える為に**労働安全への回帰**がうながされている事が着目に値する．

４．まとめ

機械関係の ISO と電気関係の IEC 等の国際規格により体系化された機械安全の概念と方法論は，人への危害を回避するために基本的に隔離と停止の原則からなりたっており，これらは基本的に機械設計者を対象としている為に，可能性とともに限界がある事を考察した．機械は単独でなく，複合システムとして使用される事が多く，その**システムのライフサイクル**での**リスク管理及び全ライフサイクルに亘る変更管理**(change management)が重要とされる．

事故は自動運転中には発生せずに，非定常運転・作業において顕在化する．それ故，停止した機械システムへの介入とそれに伴う電源管理の手順が労働安全の観点から適正管理されないと，リスクが顕在化してしまう．

とめない安全は，非定常作業において必須要件となる為，その実施方法は機械設計者が機械使用者の立場を踏まえてリスクヘッジする必要がある．それ故，止める（止まる）安全と止まらない安全は機械設計者，システムインテグレータ，機械使用者らが一体となり取組む課題であり，これらの最適化には未だ多くの課題が残されている．

更には，機械安全の流れの中でソフトウェアを含む制御システムの規格が進化してきており，機械関係が定めた ISO 13849(Performance Level: PL) に対し電気関係が定めた IEC 61508(Safety Integrated Level: SIL)更にそれを機械設計者用に組替えた IEC 62061(SIL)そして，現在この両者統合して **IEC/ISO 17305** を策定する事が協議されている．

この流れは，安全機器メーカや認証団体にとっては有利であるが，機械設計者や機械使用者にとっては，これまでの機械安全規格の体系化をさらに難解化する事にもつながり，**全体像がつかみにくくなっている**．又，この安全制御を理解するにあたっては，実際には機械安全そのものの基本的理解が必要とされる為，設計者負担は増大するという別の問題が発生する．

機械設計者や機械使用者への利便性を考えた際には，本来容易で，**究極の顧客満足度**を備えた安全要素技術が求められる時期に来ているとも言えるだろう．

同様に工業立国である日本から国際規格，とりわけ安全関係への発信がかなり少なく，技術者は世界が決めたルールの中で技術を競う事を強いられている．それ故，如何にして安全**規格を日本から発信**し，日本のものづくりが培った知恵を安全という人類共通の財産へ組込んでゆくかが今後の課題として残る．

最後に，欧州の場合機械指令により機械設計者は設計し流通する機械は安全であることを自己宣言する事が義務付けられているが，日本では該当する法の強制力はないものの，リスクアセスメント及びリスク低減の実施につき罰則が伴わないものの関連法規は以下の通り存在するため，事故発生時の説明責任として事業者は認識並びに対応が求められる事となっている；

労働安全衛生法第 28 条の 2：(2006 年 4 月)

実質的にリスクアセスメント及びリスク低減の実施

労働安全衛生規則第 24 の 13：(2012 年 4 月)

事業者は機械設計者から残留リスクの提示請求可能

参考文献

ISO 1210:2010(JIS B 9700:2013),，機械類の安全性　設計のための一般原則，リスクアセスメント及びリスク低減