働く人の安全と健康，中央災害防止協会，Vol.5, No.10, pp.82 —8４, 2004-10 より

ISO12100（JIS B 9700）
－機械類の安全性－について（4）
本質的安全設計

平田機構（株）木下博文（社）日本機械工業連合会　宮崎浩一，
明治大学理工学部　向殿政男

１．　機械安全における本質的安全設計の考え方

機械安全における本質的安全設計とは，安全を設計の段階から配慮することであり，最も本質的な安全の確保の方法である．それには、大きく二つの考え方がある。

（１）危険源が存在しないように設計する、　又は危険源が存在してもそれによる危害の度合が小さくなるように設計すること。

（２）危険源と人間とができるだけ接触しないようにすること。

上記（１）は，災害の発生要因を取り除く方法であり，（２）は危険なところに行かなければ怪我をしないという，考え方としては単純な方法である。

さて、労働災害は不安全状態と不安全行動が重なって起きるが、本質的な安全化の為には、まず不安全状態を無くすことが大前提である。設備や働く環境を安全な状態（不安全状態を取り除くこと）にすること。それには、具体的には、設備の「フールプルーフ化」と「フェールセーフ化」が必要である。これらの内容は次のようになる。

■フールプルーフ

人間が誤って不適切な操作を行なっても危険を生じない、あるいは、正常な動作を妨害されないこと。

さまざまな状況でどのような誤りを犯す可能性があるかを考えることが必要となる。

”安全インタロック”はこの特性を実現するためのものであると考えられる。

■フェールセーフ

部品やシステムなどの故障が確実に安全側のものとなること、あるいは、少なくともほぼ確実に安全側のものとなる。すなわち、危険側の故障の可能性が極めて低いことを意味する。

また、国際電気標準では「特定の障害モードが圧倒的に安全側であるようなアイテムの設計特性」(IEC61508 第 4 部)と定義している。つまり、「安全側(例、機械が止まる側)に故障する」ことを意味する。

労働災害は人が努力しても、安全技術レベルに合わせて必ず起こる。いわゆる、労働災害を防ぐのは技術の問題であり、人の対策よりも技術的な方策として本質的安全設計が重要である。

２．ISO12100 における本質的安全設計

国際安全規格 ISO12100(機械類の安全性―基本概念，設計のための一般原則）では、「第１部：基本用語，方法論」において、リスク低減のための方法論として包括的なリスク低減戦略が述べられている。

これは、３ステップメソッドと呼ばれていて、

（１）本質的安全設計によるリスクの低減

（２）安全防護によるリスクの低減

（３）使用上の情報によるリスクの低減

という順番で行うことが明記されている。

本質的安全設計方策は３ステップメソッドの最初であり、ISO12100 において最も重要なリスク低減方策と位置づけられていることは，前号でも紹介したが，その内容について以下に紹介する。

３．本質的安全設計のポイント

設計の工夫をすることにより、「安全防護策」等の追加防護を行うことなく、リスク低減を行うことであり，「設計の段階から、安全を考慮しなければならない」こと意味し、

（１）設計上の各種処置方法を適切に選択し、できる限り多くの危険源の生成を防止し、低減すること。

（２）作業員が危険区域内に介入する必要性を低減することにより、人の危険源への暴露を制限すること。

この２つに大別されることはすでに紹介したが，本質安全設計のポイントは、起こったことへの対応＝「対策」ではなく、起こりえることへの対応、つまり、「方策」であるといえる。

（１）の内容としては，幾何学的及び物理的要素に関する配慮，機械設計に関する一般的技術知識の考慮，機械的結合の安全原則，人間工学原則の遵守，制御システム設計上の安全原則，安全機能故障の確率の最小化，空圧／油圧設備の危険源防止，電気的危険源の防止などであり，以降，特に重要なポイントである「人間工学の遵守」と「制御システムの本質的安全設計」の二つについて紹介する。

４．人間工学原則の遵守

人間は間違えるものであり、疲れれば注意力が落ちるものでミスは避けられない。しかし、設計の段階からこのことを考えておけば、回避できる可能性が向上する。

厚生労働省指針である、「機械の包括的な安全基準に関する指針」には以下のようなことを掲載している。

労働者の身体的負担の軽減、誤操作等の発生の抑止等を図るため、

（１）人間工学に基づく配慮を次に定めるところにより行うこと。

労働者の身体の大きさ等に応じて機械を調節できるようにし、作業姿勢及び作業動作を労働者に大きな負担のないものとすること。

（２）機械の作動の周期及び作業の頻度については、労働者に大きな負担を与えないものとすること。

（３）通常の作業環境の照度では十分でないときは、照明設備を設けることにより作業に必要な照度を確保すること。

が規定されている。この内容は ISO12100 でも要求される内容であり，より詳細に規定されている。

５．制御システムへの本質的設計方策の適用

制御システムの設計に誤りや不適切な部分があったり、構成部品に故障が発生したり動力源が変動･故障したりすると、

（１）意図しない･予期しない機械の起動

（２）無制御状態の速度変化

（３）運動部分の停止不能

（４）加工物等の落下や放出

（５）安全装置の機能停止

などが生じて、危害が人間に及ぶ可能性がある。

これらを防止するための制御設計上の安全原則としては主として

（６）機械起動･停止の論理的原則

（７）動力遮断後の再起動防止

（８）非対称故障モード要素の使用

（９）重要構成部分の二重化

（10）自動監視の使用

（11）プロセッサ採用上の注意事項

（12）手動制御装置に関する安全原則

(13）制御･運転モードの取り扱いの留意事項

等々が規定されており，さらに詳細は ISO13849“ 機械類の安全性－制御システムの安全関連部 ” や ISO14118 “ 機械類の安全性－予期しない起動の防止 ” などで規定されている。

＜参考文献＞

・ISO12100(2003)，機械類の安全性－基本概念、設計のための一般原則

・TR B 0008(1999)，機械類の安全性－基本概念，設計のための一般原則―第１部：基本用語，方法論

・TR B 0009(1999)，機械類の安全性－基本概念，設計のための一般原則―第２部：技術原則，仕様

・ISO「機械安全」国際規格，向殿政男（監修）日本機械工業連合会（編）(1999)，日刊工

業新聞社
・国際化時代の機械システム安全技術，向殿政男(監修)(2000)，安全技術応用研究会(編)(2000)，日刊工業新聞社
・JIS B 9702（2000)，機械類の安全性－リスクアセスメントの原則