特集
これだけは身に付けておきたい
機械設計の新常識

Part 2

新規システムの開発には社会的な責任も生じる

1　安全問題と企業イメージ

事故が発生する度に国が関与してくる。本来，装置製造は安全問題も含めて，民間に任されているのではないかという疑念が頭をよぎる。これは，国家が主導して製品に許認可を与えてきた歴史的経緯があるからかもしれない（電気製品，機械部品，計量機器など）。経済産業省では，実製品に携わる工業会を組織し，製品規格の制定などを指導してきている。また，製品の許認可に関してもJIS 指定工場を定め，そこからの出荷製品については，品質に確証を与えるものであるとしている。Part1 で述べた工場審査はその 1 例でもある。農林水産省，国交省なども同様な指導形態をとっている。

筆者は，かつて大型車両の衝突実験を担当していたが，その新聞報道に関連して，担当省から呼び出しを受けたことがある。議論の中で，強く言われた言葉が今でも耳に焼き付いている。「行政としては安全であると認めたからこそ，世の中に出すことを許可している。公害を出さないと認めたからこそ，世の中に出すことを許可している。そうでなければ許可はしない」。しかし，「事故は多発しているではないか」という指摘に対しては，「それは，利用者，使用者に責任がある」。これは声を荒立てて言われた言葉である。

確かに，誤発進などに関連して車両装置の構造，機能に欠陥があったのではと利用者側から訴えられる事案は後を絶たない。しかし，利用者側からの立件・証明は難しく，裁判では敗訴となる場合がほとんどである。結果的には利用者側に責任があったとみなされる。利用者側にとっては，国・企業が一体となっているという印象は拭い去れない。しかし，勝訴したとはいえ，裁判に至ったということは，企業イメージに大ダメージを受ける。そのため，企業側は，欠陥を早々とつかみ，リコールを申請する。製品を世に出すまでには，技術者は必死になって，良き製品を出すことに勤める。TQC（Total quality control）　や TPM（Total plant maintenance）といった運動などを通して生産管理，品質管理，在庫管理などを徹底し，品質保証

された製品を供給することに邁進してきた。同時に，万一の事態に対して，利用者・使用者への教育を徹底してきた。そのような背景もあって，事故が生じた時は，利用者・使用者も諦めて，裁判に至ることも少なかった。このようにして，日本的な，安全に対する神話が根付いてきた。

しかし，製品にまつわる欧米の裁判事例（規模，金額など）は，日本人にとっては驚くほどのものが多かった。言いがかりとしか受け止められないという声も聞こえるほどである。PL 法など各種の法整備が急がれたわけである。これは製造者の責任を明確にさせるためのものであった。

このような事情もあって，2015 年 3 月号で述べたように国際安全規格の導入などが急がれているわけである。

2　リスクアセスメント

従前は，安全性に対して，以下に示すような指標が使用されてきた。

安全率：機械部品に関する安全性を図る指標である。材料の基準強さに対する機械部品の予期される強度との比率で示される。確率的な値となる。

故障率：機械部品を複数組み合わせて構築されるシステムの安全性を図る指標である。製造時よりある時間経過した時点で残存しているシステムの総数に対して，その時点で故障すると予期されるシステムの数との比率で示される。

これらの指標は，機械部品やシステムそのものの安全性に関わるものである。これに対して，国際安全規格は人間への安全性に論及するものである。この場合は，Safety integrity という指標を用いる。人の安全を保障するのに，最後の手段として非常停止を使用するような機械では integrity が極端に低いと評価される。機械が正常に機能している，あるいは機能するように見えていながら，実際には機能していない状態も integrity が低いと評価される。スリーマイル島での原発のように，熱交換器が危険な運転状態のまま放置されるようなことが生じる場合も Integrity が低いと評価される。Integrity が高いとは，そのような可能性が低い場合をいう。以上のようなことからもわかるように，Integrity は常時その動作の正常性が要求される場合，正常であるかのごとくに振る舞いながら，実際的には異常状態に陥っている 1 時間当りの確率。あるいは，異常状態になってからそのことを知らせる信号を出力するまでの時間で評価される。IEC61508 では，安全装置の安全度水準（SIL：Safety Integrity Level）を**表 1** に示したような 4 段階の数値目標で示している。

ここで，安全度水準を決定するためには**図 2** に示したようなイベントツリーによって事故シナリオを定量的な値で評価することになる。傷害の程度 S と危険事象の発生頻度/継続時間 F，危険回避の可能性 P の 3 要素を組み合わせて評価を行う。矢印で示したように，事故を回避できるかあるいは事故発生の影響を十分に低減できるときのみ $P1$ で，それ以外の場合は $P2$ である。上記の分析結果に対して危険性のカテゴリ I～V が割り当てられる。この I～V に対するシステムとしての挙動としては，**表 2** に示したカテゴリ B，1～4 のようになる。そして，それに対する対応策は**表 3** に示したようにすべきとしている。このことを勘案して，図 2 中には要求される基準を満足しているかどうかをわかりやすくするため，○，⊗，◎が示されている。⊗の左側に入るようなカテゴリではリスクに対して安全対策が不十分であり，右側に入るようなカテゴリでは，安全対策の性能が過剰であることを示している。

今，一例として**図 3** のような装置について考えてみる。安全コントローラは，圧力異常を圧力セ

表 1　安全度水準：E/E / PE 安全関連系に割り当てられる安全機能に対する目標機能失敗尺度

SIL	低頻度作動要求モード運用（注 1）	高頻度作動要求又は連続モード運用（注 2）
4	10^{-5} 以上 10^{-4} 未満	10^{-9} 以上 10^{-8} 未満
3	10^{-4} 以上 10^{-3} 未満	10^{-8} 以上 10^{-7} 未満
2	10^{-3} 以上 10^{-2} 未満	10^{-7} 以上 10^{-6} 未満
1	10^{-2} 以上 10^{-1} 未満	10^{-6} 以上 10^{-5} 未満

（注 1）作動要求当たりの設計上の機能失敗平均確率
（注 2）単位時間当たりの危険側故障確率［1/時間］