検査技術、Vol.18, No,6, pp.26-31, 日本工学出版、2013-6　より

・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・

安全確保における本質安全の役割について

向殿政男

明治大学理工学部

・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・

アブストラクト

本質安全の概念について述べる。安全の定義と安全確保のステップについて触れた後に、安全確保における安全設計の位置付け、特にその中で本質安全の果たす役割について紹介する。的という言葉が付加された本質的安全と本質安全とは異なった概念であることを提案すると共に、機能安全との関係も明確にする。最後に、本質的安全の具体的な例と考え方を国際規格に基づいて紹介をする。

・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・

１．まえがき

人類はこれまで、人間の幸せの実現のために多くの道具や機械類や設備等を作ってきた。これら人工的なシステムは、多くのベネフィット（利便性）をもたらすと共に、時には我々に危害をもたらすことがある。光のあるところには影が生ずるごとく、ベネフィットのある所、必ずリスクが存在する。ここに安全の問題が発生する。人工的なシステムにおけるリスクの典型は、システムに故障等が起こった場合と、人間が間違えて取り扱った場合に、人に危害を及ぼすことにある。従って、安全は、機械設備側が故障しないようにするか、人間が間違えないようにするのが基本となる。しかし、「機械・設備はいつかは故障して使えなくなり、人間はいつかは間違えるものである」というのは安全における大前提である。本質安全という概念は、機械類が故障しても人間が間違えても、危害が人間に及ぶのを防ぐことに関連した安全確保の考え方の一つである。

本質安全とは、素朴に考えれば、人間に危害を及ぼす危険の源（危険源と呼ぶ）をはじめからなくしてしまうという考え方である。高いところものを取る時、落ちる、または落とす危険性があるのならば、はじめからものを低いところに置いておくとか、角に当たって怪我をする可能性があるのならば、はじめから角を丸くしておくとかといった幾何学的な構造から、動くものとの衝撃で怪我をする可能性がるのならば、ゆっくりとしか動かない構造にするとか、感電の可能性があるのならば、大きな電力は使わないとかといったエネルギー的な課題まで、多くの工夫があり得る。

本稿では、本質安全の考え方について紹介をする。その前に、安全の概念と安全確保のステップについて簡単に触れておく。

２．安全の概念

「安全である」いった場合、「絶対に事故は起きないとか、危険性はゼロである」といっ

た絶対安全を意味している訳ではな。絶対安全は現実にはあり得ない。現実の安全は、リスクを通して定義され、そのシステムから受けるベネフィットを考慮して、「リスクが許容可能な状態まで低減されている時、安全であるという」というのが国際的な常識である。このことをもう少し詳しく見てみよう。

安全とは、「受け入れ不可能なリスクが存在しないこと（freedom from unacceptable risk）」[(1)]、または、「リスクが許容可能な状態に抑えられている状態」と定義されている。ここで、リスクとは「危害の発生する確率と危害のひどさの組合せ」であり、危害とは、分野により異なるが、一般的に「身体の物理的傷害、健康障害、及び財産の損害等」のことである。また、許容可能なリスク（Tolerable risk）とは、「その時代の社会の価値観に基づく所与の状況下で，受け入れられるリスク 」と定義されている。ここでの重要な視点は、通常はリスクはゼロにはならないということである。受け入れ不可能な大きなリスクがなくなった時に安全である、というだけである。このように安全といってもシステムには、常に受入れ可能なレベルの残留リスクが存在する（図１参照）。

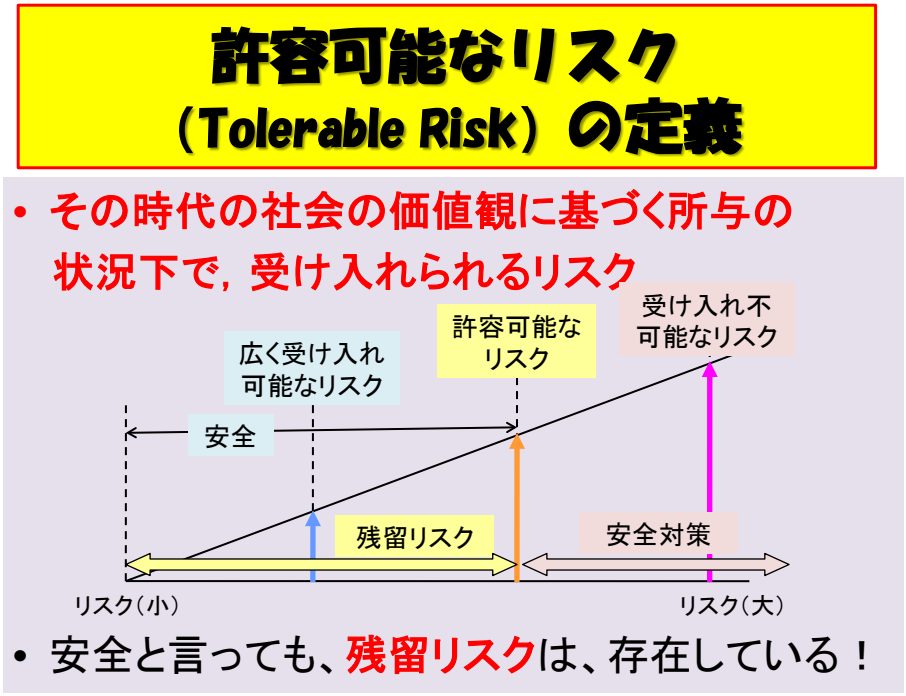

図１：許容可能なリスク

３．安全確保のステップとスリーステップメソッド

次に、人工的なシステムにおける一般的な安全の確保のステップを振り返ってみよう。図２に示すように、まず最初に、設計段階で未然防止方策を施す。予防安全である。次の実際の運用段階では、人間が注意をしながら、また保守点検や保全をしながら事故を起こさないように安全を確保する。運用安全と呼ぶことができよう。現実には、上記のように

絶対安全はあり得ないので事故の可能性は常にある。実際に事故が発生した時には、危害のひどさを下げる、拡大を防ぐ、再稼働を早める等の対策を施す。自動車や交通機関などで言えば衝突安全である。その後、事故調査が行われ、原因を追及するために、科学的、客観的な事実を物理現象はもちろんのこと、背景や組織まで含めて明らかにして、それに基づき再発防止策を提案して、各ステージにフィードバックをする。例えば、新しい安全設計基準等を設けて再度設計段階の予防安全から繰り返すことになる。

現実には、事故が起きてから安全対策を施す再発防止対策が優先されているきらいがあるのは残念であるが、上記の安全確保のステップで最も重要なことは、本来は再発防止よりは未然防止が基本であり、未然防止のためには、設計の段階から安全を組み込んでおく必要があることである。設計の段階でリスクを低減する方策には、スリーステップメソッドと呼ばれる方策が、これも世界の常識になっている（表 1)。　すなわち、第一ステップは、まず最初に、本質的安全設計を行うことであり、これが本稿の主題に関連する。一般的に、本質的安全設計ですべてのリスクを回避することは出来ないので、第二ステップとして、安全防護策や安全装置を施すことになる。　それでも残った残留リスクに対しては、第三のステップとして、利用者に使用上の情報を提供する、すなわち、警告ラベル等で表示したり、残留リスクを避けるためのマニュアルや説明書等を提供したりすることになる。これが設計者が技術として行うべきリスク低減方策の順番、スリー・ステップ・メソッドである。なお、使用上の情報が利用者に渡され、これに基づいて、はじめて利用者が個人または集団として機械や製品を注意して使うことになり、労働現場などではそのための訓練・教育等が行われ、人間により運用安全が確保がなされる。

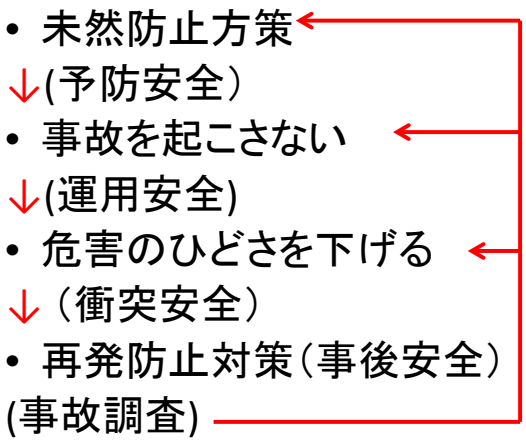

図２．安全確保のステップ

＜＜表１　設計におけるリスク低減方策～スリーステップメソッド～＞＞入る

（１）本質的安全設計によるリスクの低減
（２）安全防護策、安全装置によるリスクの低減
（３）使用上の情報の提供によるリスクの低減

（製造メーカ側）：予防安全（設計安全）
・・・・・・・・・・・・・・・・・・・・
（利用者側）：運用安全

（４）訓練、個人防護、管理によるリスクの低減

４．本質安全と本質的安全

安全の確保は、機械設備側による安全確保と人間の注意による安全確保とがある。機械設備側の安全確保は、事故が起きる前の設計段階で行われる未然防止方策を基本とする。設計の段階における未然防止方策には、機械設備自体を安全に設計する方策（これが本質的安全設計である）と他の装置を用いて機械設備の安全を確保する方策（これが安全防護策や安全装置による安全確保である）とに分けられる。上記のスリーステップメソッドは、人間による注意よりは機械設備側で設計の段階で安全を確保することを優先すべきであることを宣言している。それと共に、設計段階では、他の装置を用いて安全を確保するよりは、自分自身で安全を確保する本質的安全設計を第一とすべきことを宣言している。

ここで、本稿の主題である本質安全と上記の本質的安全の概念の違いについて、筆者なりの考え方を示しておこう。安全を実現するためには、リスクを低減する必要がある。リスクは、危害の発生確率と危害のひどさの組合せであるから、少なくとの発生確率とひどさのどちらかを下げる必要がある。発生確率の低減とひどさの低減のどちらを優先させるべきであろうか。筆者は、発生確率よりは、危害のひどさを下げることを優先すべきであると考えている。一方、上記のように設計の段階で安全方策を施すには、自分自身を安全に設計するのと、他の力を借りで安全を確保する設計とに分けられる。他の力を借りないで自分自身で安全を確保する設計のうち、本質安全設計とは、危害のひどさを低減する方策を言い、本質的安全設計とは、危害のひどさと共に（すなわち、本質安全設計を含み)、危害の発生確率も下げる方策をいう。このように、本質安全も本質的安全も他の力を借りないで自分自身で安全を確保する設計を言い、これが「本質」という言葉に託されている。

本質安全や本質的安全が、安全防護や安全装置などの他の力を借りないで、システム自体で安全を確保する方策がなぜ重要視されているのかというと、安全装置や安全防護は、故障等で機能しない場合や、時には無効化される場合があるからであり、使用上の情報は、必ずしも守られない場合がるからである。その点、本質安全や本質的安全に基づく設計は

有効性が高い。

本質的安全設計の基本は、危険源を除去するか、除き切れない場合に各危険源に対して、前述のように危害の程度を下げるか、または、危害の発生確率を下げるところにある。すなわち、

(1) 危険源の除去

(2) 危害のひどさの低減

(3) 危害の発生確率の低減

の三つに分類される。最初の二つの危険源の除去と危害のひどさの低減は、危険源そのものに対する方策であり、これが本質安全である。危険源をなくす例は冒頭でも紹介したが、道路の例でいえば，平面の交差点の代わりに立体交差にするようなことであり、毒物を使わなくて済む場合には、無毒な代替品を使うようなことである。なお、立体交差は本質安全ではないとの主張もあり得るが、交差点で横からの衝突という危険源をなくしており、本質安全の例と考えてよいだろう。ただし、立体交差点からの墜落という新しい危険源が生ずることを忘れてはならない。次に、危害の程度を下げようとするためには、例えば、危険源の持っているエネルギーを小さくするとか、スピードが出ないように設計することに相当する。三番目の危害の発生確率の低減とは、信頼性を高めて故障しないようにして危害の発生確率を下げたり、修理等のために人間が危険源に近づかなくても済むように自動運転にするといったことに相当する。以上を纏めると、本質的安全設計とは

(1) 設計上の各種処置方策を適切に選択することで，可能な限り危険源を無くすか危害の大きさを低減させること（本質安全：構造に基づき危害のひどさを小さくする)，

(2) 設計上の工夫により，可能な限り危険事象が発生しないように、また、人間が危険区域内に入る必要性を少なくすること（確率安全：危害の頻度を下げる）

の二つに分類される。

なお、危害のひどさの低減は、構造で実現するしかなく、発生確率の低減は信頼性等の確率論で評価される。従って、本質安全設計は構造安全の考え方の従い、本質的安全設計は、構造安全と共に確率安全も含んでいることになる。

設計の段階での本質的安全設計の次の第二ステップである安全防護策や安全装置等の他の装置を用いて安全を確保する方策は、何と呼ばれているのであろうか。これがいわゆる機能安全の概念である。本質安全や本質的安全と機能安全との根本的な違いは、安全設計のスリーステップメソッドにおける第一ステップの方策か第二ステップの方策かの違いにあると考えられる。

５．本質的安全設計の方策(2)

本質的安全設計に基づくリスク低減方策について国際安全規格[3]には以下のような多くの項目が述べられている（表２)。各項目について、簡単に触れておこう。

表２　本質的安全設計の項目[3]

１．幾何学的要因
２．物理的側面の考慮
３．機械設計に関する一般的技術知識の考慮
４．適切な技術の選択
５．構成品間のポジティブな機械的作用の原理の採用
６．安定性に関する規定
７．保全性に関する規定
８．人間工学原則の遵守
９．電気的危険源の防止
10．空圧及び液圧設備の危険源の防止
11．制御システムへの本質的安全設計方策の適用
12．安全機能の故障の確率の最小化
13．設備の信頼性による危険源への暴露機会の制限
14．搬入（供給）／搬出（取り出し）作業の機械化及び自動化
　　による危険源への暴露機会の制限
15．設定（段取り等）及び保全の作業位置を危険区域外とする
　　ことによる危険源への暴露機会の制限

1の幾何学的要因とは、例えば、挟まれる危険がある場合は入れないように狭く、また挟まれても抜け出せるように広く設計する、とがって刺されそうな部分は丸くする、バリはとる、人間が制御している場合には制御位置から危険なところが直接見えるように機械の形状を設計すること等。

2．物理的側面の考慮とは、作動力,運動エネルギーを小さく制限する等が相当する。

3の機械設計に関する一般的技術知識の考慮とは、機械的応力、材料とその特性、エミッション値（騒音、振動、放射等）等の一般的技術知識を適切に使用すること。

4の適切な技術の選択とは、本質安全防爆により電気設備溶剤を発火点以下で使用することや、高い騒音の場合には機械的切断の代わりに水による切断を使う等のこと。

5 の構成品間のポジティブな機械的作用の原理の採用とは、ポジティブモードでの結合（機械的構成部品が直接、または剛体要素を介して他の機械的構成部品に連動させる）をいう。

6の安定性に関する規定とは、機械自体のバランスや運転中の振動、地震等の外部からの力でなどで機械が転倒することによる危害を防止するために配慮すべき事項。

7 の保全性に関する規定とは、保全のために考慮すべき要因、例えば、接近のしやすさ、作業のし易さ、工具や人体の寸法の配慮、特殊な工具の採用等。

8 の人間工学原則の遵守とは、機械の運転、保守、清掃などをする人の身体的、精神的なストレスを低減させるために設計の段階で組み込むべき方策。

9 の電気的危険源の防止とは、人間が直接、間接に電気に触れないような工夫、触れた場合でも感電しないように電圧を安全なレベルまで抑え込むことや、低インピーダンスのアースを接地して電流が大地に流れるような方策。

10 の空気及び液圧設備の危険源の防止とは、最大定格圧力を超えない設計の工夫、動力源が無くなった場合に残圧により危害が発生しないように減圧を行う設計の工夫、等。

11 の制御システムへの本質的安全設計方策の適用は、技術的に最も内容の豊富な項目である。制御システムは、多くのセンサーや電子部品、及び電気・電子に基づく制御が使われていて、それに対して本質的安全設計を適用することを述べている。

12 の安全機能の故障の確率の最小化は、信頼性を上げることで安全機能の働く時間を長くしようとする信頼性に基づく安全性の向上策。

13 の設備の信頼性による危険源への暴露機会の制限とは、故障が発生すると修理のために保守員が危険源に近づく可能性が高くなり、危害が発生する確率が高まるので、その機会を出来るだけ少なくするには、設備の信頼性を上げる必要があることを意味している。これは、信頼性を上げることで安全性を向上させる方策である。

14 の搬入（供給）／搬出（取り出し）作業の機械化及び自動化による危険源への暴露機会の制限とは、作業を機械化し、自動化してしまえば、作業員と危険源が触れ合う機会がなくなるので、特に災害が多い部品や材料の搬入（供給)、搬出（取り出し）作業には、機械化、自動化を適用する必要があることを述べている。

最後の 15 の設定（段取り等）及び保全の作業位置を危険区域外とすることによる危険源への暴露機会の制限とは、危険源から離れた危険区域外に作業位置を定めておけば、作業員と危険源とが触れ合うなくなり、リスクが低減されるという考え方。

以上、ここで紹介した本質的安全設計の内容は、これまでの永い間の世界の安全技術者の経験と努力のエッセンスである。ここには、本質安全と本質的安全とが混在している。

６．あとがき

本稿の趣旨を要約してみると以下のようになる。安全の確保には、再発防止より未然防止を重視すべきであり、未然防止のためには、設計段階から安全を組み込んでおく必要がある。設計段階での安全の組込みでまず最初に考えなければならない最も大事なことは、安全装置などの他の機構を用いて安全を確保することを考える前に、自分自身の本体で安全が確保できる本質的安全設計の考え方を用いなければならないことである。本質的安全設計には、危害のひどさを低減させる方法と危害の発生確率を低減する方法とを含むが、前者のひどさを低減させる考え方が、本稿の趣旨である最も本質的な本質安全である。本質安全は、安全設計思想の中で最も重視すべき概念であり、安全設計に従事する設計者は、まずはじめに本質安全に基づく安全確保を試みなければならない。

最後に、安全における検査技術の役割に触れておこう。検査技術は、図 1 の安全確保のステップで言えば、第二ステップの運用安全に主として用いられるが、もちろん、設計における未然防止にも、事故後の調査にも重要な技術である。人工システムはいつか動かなくなり、最後には危険側の故障を起こして寿命を終るものも少なくない。従って、人工的なシステムを安心して使うためには、まず耐用寿命を想定して、故障、摩耗、劣化等を考慮して、定期的な保守点検、整備、交換等のメンテナンスを行うと共に、システムとして寿命を終える前に、全面的に取り換える必要がある。実は、ほとんどのシステムの安全は、メンテナンスで確保されているといってよい。特に、インフラ等の公共システムの安全確保には、我が国では、新しく設計、建設するよりもメンテナンスの方がはるかに重要になり、多くの資金の投入が必要となることは間違いない。この時に、寿命の予測、故障診断、劣化診断等に検査技術が果たす役割は本質的である。従って、検査技術、特に非破壊検査技術は、今後の安全確保の中核をなす技術になると予想される。

参考文献

（1）ISO/IEC ガイド 51(JIS B 8051 2004)安全面一規格への導入指針、1999

（2）向殿政男、本質安全という概念について、品質、Vol.42, No.3, 日本品質管理学会、2012-3

（3）ISO12100(JIS B 97002004)機械類の安全性一安全設計設計のための基本概念、一般原則、2004