本質安全という概念について†

向殿 政男*

Inherent safety is an important and fundamental concept to design systems safe. The main purposes of this article are to introduce the concept of inherent safety and to clarify the relationships between inherent safety, intrinsic safety and fail safety.

After some fundamental concepts concerning safety, such as definition of safety, the order of priority of safety measures, three steps method and risk assessment, are introduced, many inherently safe design measures are listed up. At this point distinction between inherent safety and inherently safety is proposed. The relationships between inherent safety and intrinsic safety, passive safety and active safety, functional safety and inherent safety, are clarified. Finally, the relationship between inherent safety and fail safety is discussed in detail.

1. まえがき

「通路のこんなところに穴が開いている．危ないじゃないですか」．「怪我をする可能性があるので，皆に注意するように伝え，穴の前に注意書きを貼り出すことにしよう」．これは，人間の注意に基づく安全確保である．さらに，「周りを策で囲んで，人が入れないようにしよう」．これは，安全防護，安全装置に基づく安全確保である．これらに対して，「穴を埋めてしまえ」ば，事故の起こる可能性がない．これが本質安全の考え方である．同様に，家庭内での事故のトップは，常に階段による事故である．人間が注意して昇り降りするのも重要だし，手すりを付けたり，滑り止めを付けたりするハード的な方策も重要だ．しかし，二階を作らずに平屋にして階段そのものをなくしてしまえば事故は起きない．これが本来の本質安全である．

現実はこんな単純は話だけではないし，本質安全にも色々な考え方がある．また，必ずしもすべてにおいて本質安全を実現できる訳でもない．本稿では，本質安全にまつわるいくつかの考え方について紹介する．特に，本質的安全設計方策について紹介するとともに，本質安全とフェールセーフとの関係について考察する．

†平成24年5月25日 受付

*明治大学 理工学部情報科学科

連絡先：〒214-8571 神奈川県川崎市多摩区東三田1-1-1
(勤務先)

2. 安全に関するいくつかの概念[1]

まず，安全そのものに関する基本的な事項を振り返っておこう．

2.1 安全とは

安全という言葉は，通常，何となく使われているが，製品や機械設備等(以後システムと呼ぶ)の分野では，リスクという概念と危害という概念を経由して厳密に定義されている．すなわち，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)」[2]である．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」のことである．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．受け入れ不可能なよう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．設計・製造者は，受け入れ可能になるまで残留リスクを低減し，利用者はその残留したリスクの制御を委ねているということを自覚する必要がある．設計・製造者はもとより，利用者にも安全を確保する役割分担の責任がある．冒頭で紹介したように，危険なところ(以後，危険源と呼ぶ)をはじめから除去できるのであれば理想的だが，現実の安全はそう簡単ではない．

2.2 安全確保の分野と優先順位

安全学の視点[3]からは，安全の確保は大きく分けて三つの分野に分類されている．一つは，システムそのものをハード的に安全化することであり，主として設計や製造等のメーカの役割である．これは技術による安全の確保といえる．二つ目は，人間が操作・運用をして安全を確保することで，注意，訓練，教育等が重要となる．これは人間による安全の確保である．三つ目は，組織，管理，基準，社会制度等の決めたルールを守ることによるもので，これは仕組みによる安全確保といってよいであろう．それぞれ，自然科学，人文科学，社会科学に対応している．これら三つの分野が統一した理念の下に，総合的に連携して適用されない限り，適切な安全は確保されないことが指摘されている[3]．三つのうちのどの分野を優先すべきであろうか．現在の国際安全規格[2],[4]では，人間による安全確保の前に，技術による安全確保が優先されるべきであることが宣言されている．それらが正しく行われているかを，また常に改善されているかを仕組みによる安全確保により管理するという構造になっている．

2.3 技術による安全確保の手順～スリーステップメソッド～

安全の確保は，まず技術による安全確保，すなわちシステムの安全化から始まるべきことを紹介したが，システムの安全化の本質は，設計の段階で危険源を見出しておき，各危険源に対するリスクをいかに低減するかにある．設計の段階でリスク低減をする手順には実は順番があり，その最も大事な最初のステップが，本稿の主題である本質安全の方策である．この順番は次の様にスリーステップメソッドと呼ばれている．

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る．これについては4章で詳しく紹介する．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できない．そこで，残されたリスクに対しては，次に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．それでも残ったリスクに対しては，第三のステップとして，使用上の情報の提供，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策の順番，スリーステップメソッドである．第三ステップの使用上の情報は利用者に渡され，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，人間による安全の確保がなされる．まえがきで紹介した通路の穴のリスクに対する方策は，この逆の順番で記述されている．

表・1　スリーステップメソッド

(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)
(利用者側)
(4) 訓練，個人防護，管理によるリスクの低減

なお，このスリーステップメソッドで重要なことは，この順番でリスク低減策が施されなければならないことである．機能・性能・コストを重視して本質的安全設計の配慮をしないで，後で危ないところに，時には事故が起きてから，安全装置などを付けるのは間違いである．ましてや，危険なところがむき出しで，安全装置も付けないで，警告ラベルだけを貼って，ユーザの注意にすべての安全の確保を委ねてしまうのは正しくない．

2.4 リスクアセスメント

リスクアセスメントとは，事前に大きなリスクを見出しておき，ハード的にリスク低減の方策を施しておくという未然防止の考え方である．リスクアセスメントでは，まずその機械設備の使用条件を明確にしてから(使用条件の明確化)，潜在している危険なところである危険源を全部見つけ出しておく(危険源の同定)．その各々の危険源に対して，人間が近寄る可能性や事故の回避可能性等を考えて怪我をする頻度，および事故になってしまった時の怪我のひどさ，すなわちリスクの要素を明らかにする(リスクの見積り)．次のステップが，そのリスクの大きさを評価して，許容可能か否かを判定する(リスクの評価)．その結果，許容できないような大きなリスクであれば，リスクの低減策を施す(リスク低減)．施すべきリスク低減策は，前述したスリーステップメソッドに従う．以上の手順を繰り返して，許容可能なリスクしか残らないように事前に手を施しておくことがリスクアセスメントの考え方である．事故が起きてから対策を施す再発防止ではなく，事故の未然防止の方策である．

3．本質安全にまつわるいくつかの概念

3.1 本質安全とは

本質安全とは，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ことである．本質安全が設計におけるスリーステップメソッドで最も重視される理由は，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，本質安全に基づく設計は有効性が高い．基本的には，危険源を除去するかリスクを低減させるかである．リスクを低減させるには，リスクの定義に従えば各危険源に対して危害の程度を下げるか，または危害の発生の頻度を下げる必要がある．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る．危険源を無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．また，故障等が生じたら，安全装置等の他の方策を施さなくても，自然現象を用いて自ずから安全状態の落ちこむ性質を持たせることも含まれる．これは，後述するフェールセーフとも深く関連する．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(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(危害の頻度を下げる)

の二つに分類される．

3.2 本質安全と本質的安全

一般には，また本稿でもここまでは，本質安全(Inherent safety)と本質的安全(Inherently safety)とをあまり区別なく使用しているが，筆者は両者の言葉を使い分けたらどうかと考えている．例えば，上記に紹介した(1)危険源に関するリスク低減方策のうち危険源が除去されているか，危害のひどさが許容可能な程度までに下げられているときに本質安全という．一方，この本質安全を含めて，それ以外の上記の(1)と危害の頻度を下げる(2)の方策を，本質安全的な性質を有しているという意味から，本質的安全と呼ぶことを提案したい．この観点からは，いくらエネルギーを下げても，また滅多に起きないように信頼度を高くしても，もし危害が発生した時には許容できない場合には本質安全ではない．いくら頻繁に発生しても危害の大きさに問題がない場合には本質安全である．危害が大きな場合には，信頼性に基づく方策はいくら確率が小さくても本質安全の方策ではなく，本質的安全の方策である．

3.3 本質安全と固有安全

本質安全とは，上述のように，付加装置など他の力を借りないで，その装置自身の構造や物理的特性などの性質により，安全を確保する性質をいう．本質安全化の手法の典型例が，危険源を無くしてしまうこと，すなわち危険源の除去である．一方，固有安全(Intrinsic safety)という呼び方もある．その装置の固有の特性として安全を確保する性質を有していることを意味し，本質安全とほとんど同じ意味に用いられている場合が多い．しかし，分野により，固有安全という用語の方を特に用いている場合がある．例えば，防爆の分野では，爆発性雰囲気で火花が出て爆発に繋がらないように，爆発を起こすレベル以下の電気のエネルギーしか使わない機器や，電気の代りの空気や流体などを使った機器を固有安全(本質安全防爆)機器と呼んでいる．しかし，日本語の本質安全と固有安全でも，また英語の Inherent safety と Intrinsic safety でも，その区別はそう厳密ではないようである．例えば原子力の分野では，英語では Inherent safety に日本語では固有安全の言葉を当てている場合が多い．本稿では，本質安全，及び本質的安全という用語を用いることとする．

3.4 受動安全と能動安全

安全の確保には，受動安全(passive safety)という考え方と能動安全(active safety)という二つの考え方がある．受動安全とは，システムが，外部からのエネルギーや信号，操作等なしで，それ自体が有する機構で自動的に安全が確保されることをいう．このためには，システムを構成している物質の物理的性質や化学的性質に基づくか，システムに作用する重力や熱伝動

等の自然法則を利用するのが基本である．これに対して，能動安全とは，外部からのエネルギーや信号，操作等を用いて積極的に安全を確保するもので，外部からのエネルギーや信号，操作等が途絶えた場合には，安全が確保される保証はなくなる．原子炉の場合を例にとると分かりやすい．現在の原子炉の安全は，「止める」，「冷やす」，「閉じ込める」の3要素で実現されているが，これは明らかに能動安全である．何らかの手立てをもって，積極的に止め，冷やし，閉じ込めなければならないからである．現実には，これらのためには電源が必要であり，全電源喪失により，今回の福島第一原発の事故が発生した．これに対して，何もできなくなったら，自動的に「止まる」，「冷える」，「閉じこもる」構造を構築しておくことが，受動安全である．受動安全は，本質安全の基本あり，かつ後述するフェールセーフの基本となっている．本質安全にとっては，受動安全の考え方は極めて重要である．

ここでついでに，原子力の安全について，簡単に触れておこう．現実の原子炉には，多くの受動安全の考え方が導入されている．重力により制御棒が落下して核分裂が止まる(沸騰水型原子炉では，用いられていない)，蒸気圧を用いた対流による原子炉を冷却する非常用復水器等は，外部電源を必要としない受動安全である．原子力の分野では，これを固有安全とか静的安全とも呼んでいる．特に原子力で有名な固有安全は，軽水炉では，減速材の温度効果や燃料のドップラー効果で核分裂が制御されて出力が安定状態に自動的に自己制御される構造を有していることである(図・1参照)．これは，原子爆弾のように核爆発をするという危険源に関しては，原子炉は本質安全になっているという意味である．この型の原子炉では核爆発は生じないが，この状態は臨界状態であり，放射線は出続けている．放射能の放出，崩壊熱の除去，水素爆発等の危険源に関しては本質安全になっていない．従って，原子炉が本質安全(固有安全)になっているというのも，また原子炉は全く本質安全になっていないというのもどちらも正しくない．今後の原子力発電では，全面的に受動安全に基づくフェールセーフな原子炉の開発が最も望ましいと筆者は考えている．

3.5 本質安全と機能安全

システムの安全を確保する機能を，一般的に安全機能という．技術による施設設備側の安全機能の実現には，二つのやり方がある．一つは，システム自体に安全を確保する機能を本質的な性質として構造的に持たせるものであり，これにより実現される安全機能が，本稿で紹介している本質安全である．これに対して，外部から安全を確保する機能を追加するやり方がある．安全装置や安全防護策，安全監視等を付加装置として付けることで安全を確保する考え方である．安全機能のうち，外部から追加することで実現されるものを機能安全という．最近，機能安全が注目され出して来ているのは，安全のために付加する装置に，コンピュータのようなICTの技術が積極的に応用されるようになったからである．ICT技術で使われる電子機器の故障の物理的状態には不確定性が高く，またソフトウエアにバグがないことを保証することは困難であり，ここに本質安全の考え方を導入するのは難しい．従って，正しく働く確率のみで評価されることになる．最近の機能安全の手法では，安全装置の様にシステムの安全確保のために付加される部分を安全関連系と呼び，本来の機能を実現する部分(安全関連系により監視，制御される部分)を非安全関連系と呼んで二つの部分に分け，安全関連系だけは徹底的に信頼度を高く作ろうという発想に基づいている．機能安全では，コンピュータを導入して安全関連系が正しく働く確率を高くすることでシステム全体の安全を確保しようとしている．

以上の様な観点から，安全確保のやり方としては，本質安全と機能安全の二つに分けられて対比される．また，これは構造安全と確率安全，または確定的安全と確率論的安全のように対比されることもある．

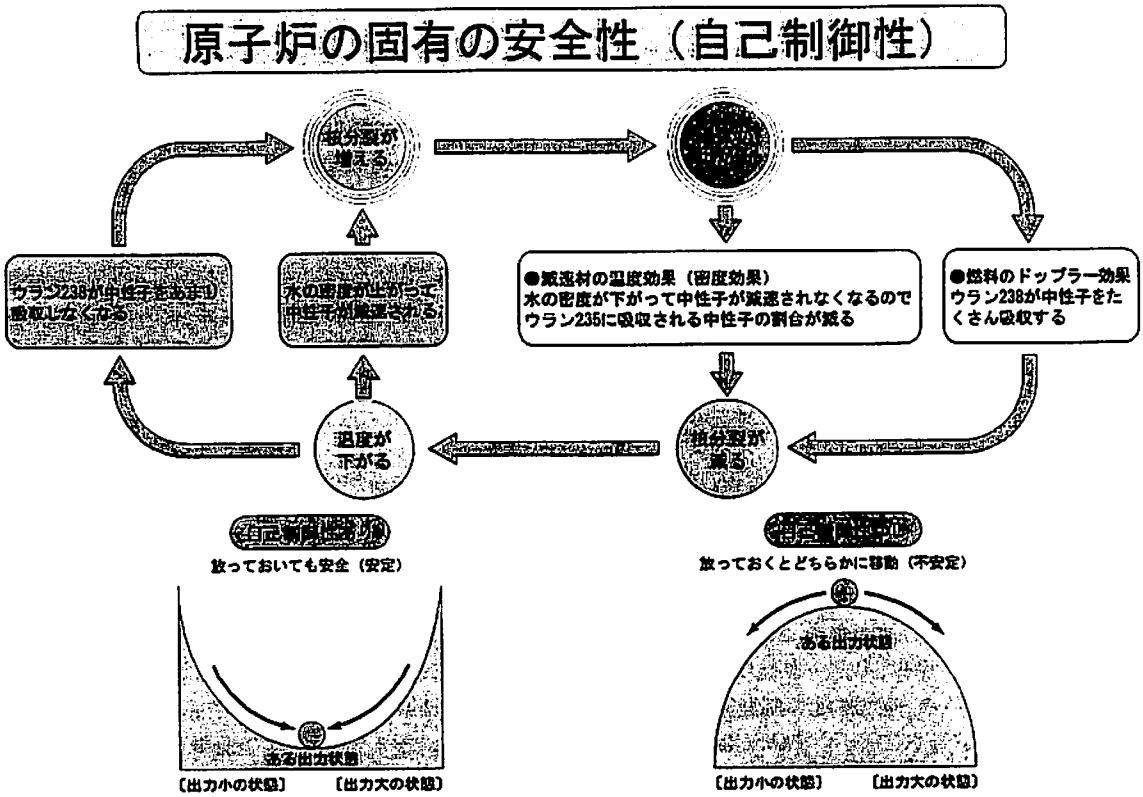
4．本質的安全設計の方策[4]

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[4]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．

「1．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．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



図・1　原子炉の固有安全性(出典：原子力・エネルギー図面集 2011)

用すること.

「4．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．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)させることをいう.

「6．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等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．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．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．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して電流が大地に流れるような方策.

「10．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．制御システムへの本質的安全設計方策の適用」とは，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および電気・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いう.

「12．安全機能の故障の確率の最小化」とは，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．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．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ことがなくなり，リスクが低減されるという考え方である．

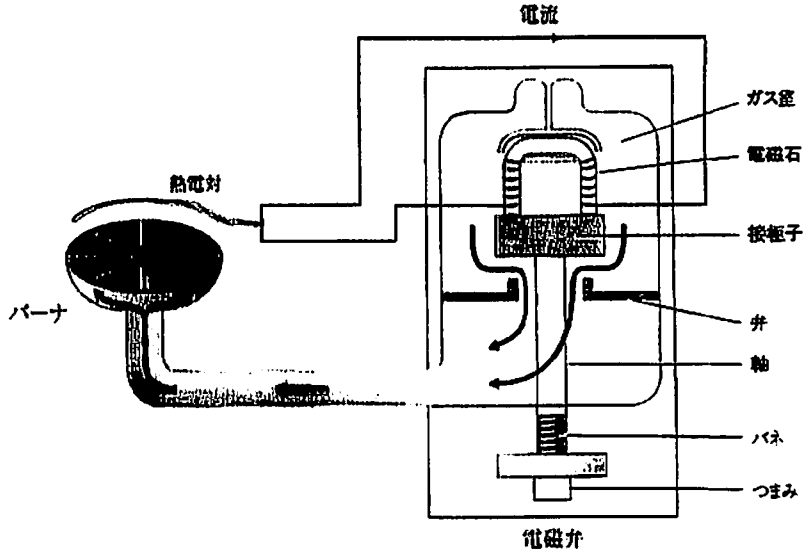
表・2　本質的安全設計の項目[4]

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

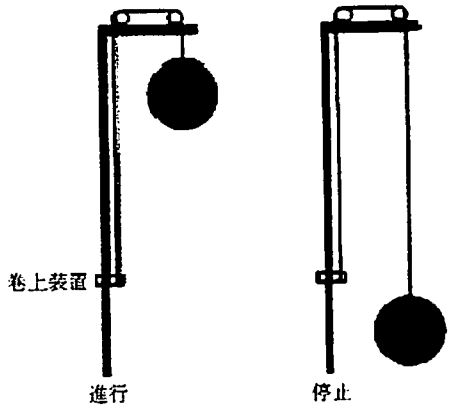
以上，ここで紹介した本質的安全設計の内容は，これまでの永い間の世界の安全技術者の経験と努力のエッセンスである．ここには，本質安全と本質的安全とが混在している．

5．本質安全とフェールセーフ

最後に，本質安全とフェールセーフの関係について触れておこう．フェールセーフ(fail safe)とは，失敗(fail)しても安全(safe)であるということである．システムの場合，失敗とは，具体的には故障に相当する．一般に，システムの部品やサブステムの故障には，システムの状態を危険側に導くものと安全側に導くものとがある．フェールセーフなシステムでは，故障の発生は認めるが安全側に導く故障しか認めないようにするというものである．この様な故障を非対称故障と呼ぶ．すなわち，非対称故障とは，故障すると必ずある決まりきった状態になり，それ以外にはならないようにすることを意味している．そんなことが可能かというと，物理現象などを利用して工夫を凝らすことで可能になる場合がある．例えば，良く出される例に踏み切りの遮断機がある．列車が来なくて，遮断機が正常に働いている時は開いているが，遮断機が故障をすると，列車が来る来ないにかかわらず，重力により自動的に遮断機は降りてしまう構造である．重力に逆らって遮断機が自然に上がるということはあり得ない．故障すると必ず閉まる方向に固定することになる．これが非対称故障であり，この場合の故障は安全



図・2　フェールセーフなガス燃焼装置[5]



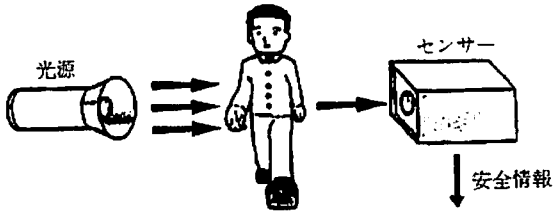
図・3　ボール信号機

側である．

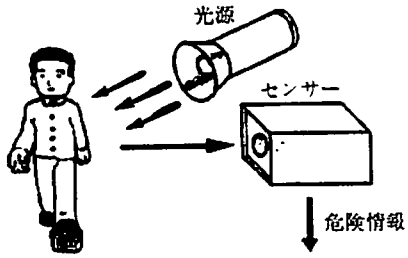
図・2にもう一つの典型的なフェールセーフの例を示す．これはガス燃焼装置の例で，バーナーに火がついて燃えている時には，その熱により熱電対で電気が発生して電流が流れ，これにより電磁石が働き接触子と書いてある蓋が持ち上げられ，ガスがガス室からバーナーへ流れる構造である．バーナーの炎が消えたりすれば電気の発生が止まり，電磁石が働かないので重力とばねによりふたが閉まってしまいガスが止まる．熱電対が故障したり電線が断線した場合も，すべて蓋が閉まる方向で，生ガスが出っぱなしという事故は発生しない．これらの故障は安全側となり，フェールセーフが実現されている．

ところで，これは本質安全と呼んでよいのであろうか．機器自体が，ガスを燃焼して熱を出すという本来の機能において，構造的に安全を確保する性質を有しているので，筆者はこれも本質安全に分類したいと考えている．このような考え方は付加設備としての安全装置等にも適用することもできる．

図・3は，ボール信号と呼ばれる昔の列車用の信号機の構造である．ボールが高い位置(ハイボール)にある時，緑の信号を表していて列車の進行を許可し，ボールが地上にある(ローボール)時には，赤信号として列車の進行をストップさせる．ボール信号機の故障とは，ロープなどが切れたりすることに相当する．この時には，ハイボール(緑信号)であっても，ボールは重力で落下してローボール(赤信号)になり，列車は進行することは出来ない．故障すると列車は止まるという安全側(赤信号)になって，迷惑を被ることはあっても，人命に係るような大事故に繋がる心配はない．逆に，ハイボールを赤信号(停止信号)に対応させると，故障すると停止信号が伝わらず，大惨事につながる可



(a) 透過型センサー（安全確認型の例）



(b) 反射型センサー（危険検出型の例）

図・4　安全確認型と危険検出型のセンサー[5]

能性がある．許可信号(緑の信号)に対してハイボールを対応させることによって，フェールセーフ(故障すると必ず安全側に固定される)が実現されている．なぜならば，ローボールが重力に逆らって故障でハイボールになることはないからである．重力がある限りこの原理は裏切られない．これが非対称故障を保証している．踏切の遮断機と同じ原理である．列車の信号機は，本来，一種の安全装置である．安全装置にフェールセーフの原理という本質安全の考え方を適用していると言える．これに対して，安全装置にフェールセーフの原理を用いないで高信頼性のみに頼って安全確保が実現されているのが機能安全である．

ここには，“許可を表す緑信号には，エネルギーの高い物理的状態を対応させなければならない”という深遠なる安全の原理が背景にある．これを私は，“ハイボールの原理”と呼んでいる[3]．ウイスキーの炭酸割りはハイボールといわれているが，お酒のハイボールと上の信号のハイボールとが，次のような逸話として結びついている．昔，英国で，駅近くの酒場のカウンターで列車待ちをしながら，ちびりちびりとウイスキーを飲んでいた英国紳士が，ハイボールを見て，急いで(ウイスキーは強いのでそのままいっきに飲むと体に良くないから)ウイスキーを炭酸で割って薄くして，そしていっきに飲んでホームに向かった．よってウイスキーの炭酸割りをハイボールという語源説である．

5.1 安全確認型と危険検出型

安全装置を用いてシステム全体をフェールセーフにするには，ハイボールの原理と共に，安全確認型という原理が重要となる．システム全体を必ずしもフェールセーフに構成出来ない場合には，センサー等を用いた安全装置でフェールセーフを実現することになる．この時，センサーや安全装置が壊れても安全側になるように設計しなければならない．そのためには，安全が確認された時だけ危険を伴う作業を許可し，確認されない時には許可しないとい安全確認型の考え方が重要となる．この時，安全を確認したことを表す安全確認信号には，エネルギーの高い状態を対応させなければならない(上記のハイボールの原理)．このことを，図・4で人が存在しない時のみロボット等の危険なシステムの稼働を許可する例で説明する．(a)は透過型センサーで人が居ないこと(安全であること)を確認して，その確認信号(エネルギーの高い状態)でロボット等の稼働を許す．人が居て光を遮った時には安全が確認されていないとして，安全確認信号がなくなる(エネルギーの低い状態)ので，ロボットの稼働を許可しない構造である．この構造だと，人がいる時だけでなく，光源やセンサーや信号線等で構成される安全装置が故障した時にも，安全確認信号が出ないので，ロボットの稼働は許可されない．安全装置の故障は安全側となり，フェールセーフが実現さる．この反対が，危険検出型であり(図・4の(b))，反射型センサーで人が居て危険であることを検出して，それを伝えてロボットの稼働を止めるという考え方である．この場合，安全装置が故障すると，危険が伝わらないので危険側の故障となる．安全確認型でないとフェールセーフは実現できない．

本質安全とフェールセーフはお互いに深く，かつ極めて重要な関係にあるが，その関係はそれほど明確ではない．例えば，上のように付加装置としての安全装置に物理現象などの用いた本質安全の考え方を採用している場合，システム全体としてフェールセーフになっているといってよいが，本質安全といってよいか否かは難しいところである．

6．あとがき

本質安全にまつわるいくつかの話題を提供することで，本質安全の概念を紹介した．本質安全，本質的安全，固有安全，受動安全，フェールセーフ等は，お互いに深い関係にあるが，その関係はそれほど明確になっているとは思われない．今後，更に整理する必要があろうが，本稿ではこれらの関係の一つの概念整理を試みたものである．

参考文献

[1] 杉原健治・向殿政男(2009)："安全設計の基本概念"，「品質」，39，〔4〕，7-15.

[2] ISO/IECガイド51(JIS B 8051 2004)「安全面一規格への導入指針」(1999)

[3] 向殿政男・北野大・他(2009)：「安全学入門～安全の確立から安心へ～」，研成社.

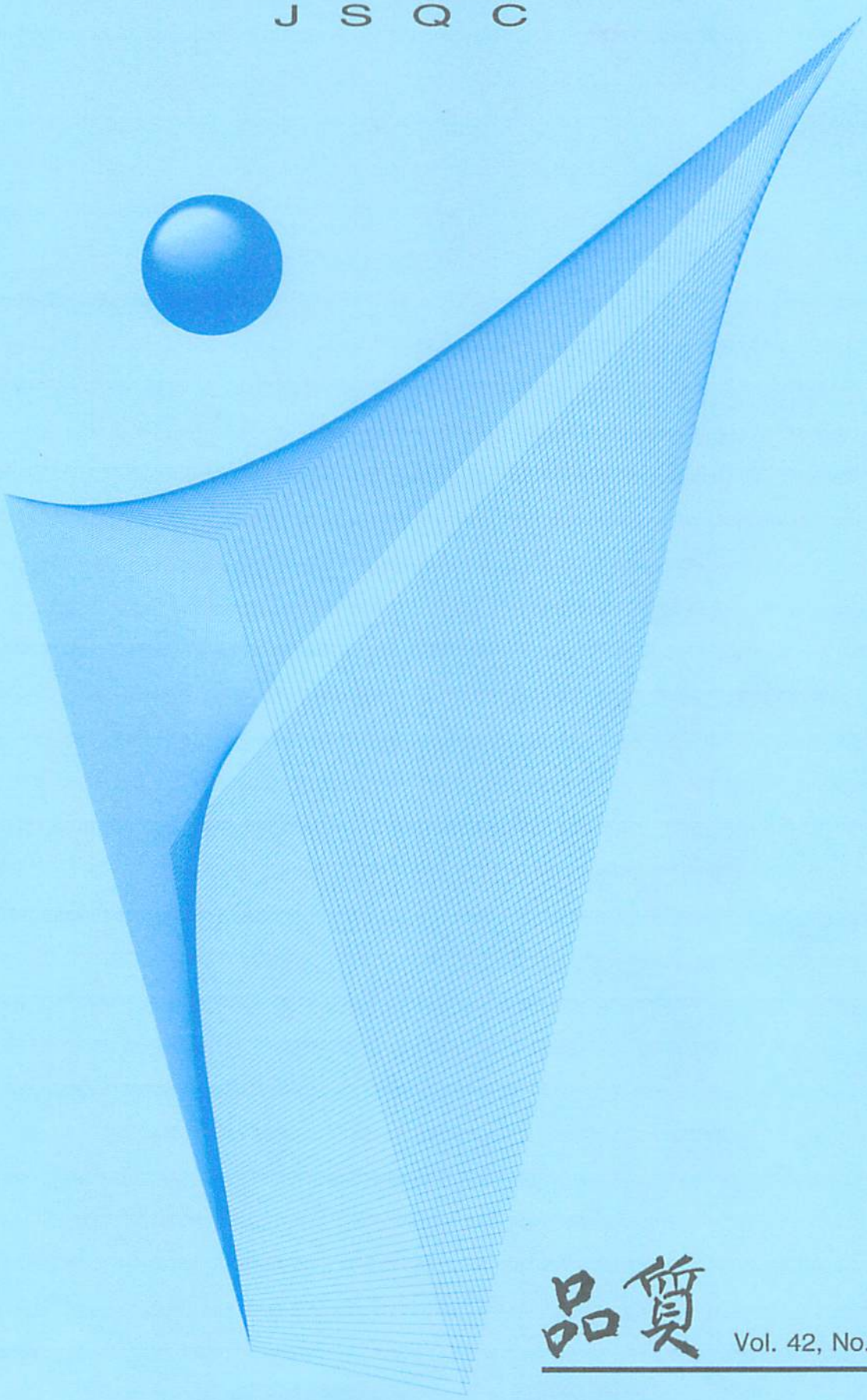
[4] ISO 12100(JIS B 97002004)「機械類の安全性一安全設計設計のための基本概念，一般原則」(2004)

[5] 柚原直弘・古川 修・稲垣敏之編(2012-7(予定))：「ヒューマンエラーとシステム設計一事例で学ぶ事故防止策」，講談社.

ISSN 0386-8230

Quality

JSQC



品質

Vol. 42, No. 3, 2012

JOURNAL OF THE JAPANESE SOCIETY FOR QUALITY CONTROL