論文紹介

原理原則に基づく化学プラントの安全化に関する考察

木　村　　真
（昭和電工株式会社 CSR 部 環境安全室）

1　はじめに

平成23年後半から平成24年に化学工場の大きな事故が多発したが、その際、再発防止対策や横展開が実施されたことに加えて、安全文化の構築や現場力の維持・向上が対策として挙げられたことは特徴的であった。これらの事故を他山の石とすべきなのは当然であるし、安全文化や現場力が今後大切になって来るのではないかと感じるのも確かである。しかし、我々事業者が確信を持って化学プラントの安全化を進めるためには、実施する施策が適切であるという論理的な根拠が必要である。

機械安全の分野では、杉本，蓬原，向殿[1)2)]によって「安全確認の原理」が確立されており、これに基づき木村（筆者）、田中、福田、杉本[3)]が、化学プラントを含む設備・機械において安全なシステムを構成する上での原則として「多段安全制御構造原則」を示すと共にインターロックを解除して行うような高いリスクの保守作業等の実施体制の原則を示した。

本論文では、「化学プラントにおける安全化の方向性」を安全の制御という視点から安全の原理原則に基づいて検討するものとし、まず「安全確認の原理」および「多段安全制御構造原則」を適用した設備・機械の安全の全体構造のモデルとして「浮き橋を自転車で渡るモデル（氷上浮橋モデル）」を提示し、そのモデルが示唆する方向性を整理する。次に、氷上浮橋モデルの安全制御にかかわる部分を設備と人の信頼性の違いを考慮して「スイスチーズモデル」に書き換え、そのモデルが示唆する方向性を整理する。さらに、人の作業ミスが直接事故につながるようなプラント保守作業について検討し、プラント保守作業における安全制御構造を提案する。

2　安全の全体構造

2．1　安全制御構造原則

機械・設備における制御による安全は、**図1**に示す多段安全制御構造[3)]とすることが原則である。実運用されている機械・設備には、設計された「安全に運転を継続できる範囲」（以下「安全範囲」という。）が存在している。そこには、本来の目的を達成しようとする制御（以下「目的制御」という。）がある。しかし制御である限りそこには制御の限界が存在する。このため、制御対象が外乱等により変動して安全範囲から逸脱しようとするとき、自動的にあるいは人の介入などにより目的制御が安全範囲内に留まるように調整する制御（以下「調整制御」という。）が存在する。この調整制御にもまた制御の限界があるため、さらに制御が乱れて安全範囲から

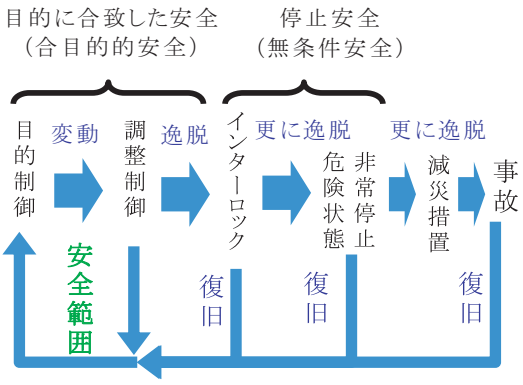

図1　多段安全制御構造原則

逸脱しようとすることをインターロックが検知し、目的制御の継続を放棄して停止させる。インターロックもまた制御の範疇であることからこれにも限界があり、更に逸脱する場合もある。その際は人が手動による非常停止等の手段によって運転を停止させることになる。もし、これにも失敗すると減災措置を経て事故・災害と発展する。このような制御の限界を補うように多段に制御される構造を多段安全制御構造という。

安全範囲の中で実施される調整制御は、本来の装置や設備を導入した目的に合致した安全であり「合目的的安全」という。また、インターロック以降の安全は、目的達成を放棄して装置や設備を停止させる安全であり「無条件安全」という[(4)]。

なお、この多段安全制御構造原則は、機械・設備のような物理的に存在する物に限らず、プラントの運転や保守作業にも適用すべき普遍的な原則である。この場合の「安全範囲」は、運転管理マニュアルや作業手順書あるいは文書化されていない作業手順（以下「非文書化作業手順」という。）となり、「調整制御」は作業者がマニュアル、手順書、非文書化作業手順から逸脱しないようにすることを意味する。

2．2　氷上浮橋モデル

危険物の製造、機械加工、列車の運行などの行為は、生身の人の能力を超えるエネルギーを持つものを制御して目的を効率よく達成するためのものであり、そのエネルギーが人の意思に反して解放されたり人に降りかかったりした場合には事故や災害になる。言い換えれば、我々は危険を伴う行為(目的を達成するための行為)を事故や災害を起こさずに実行したいのである。このために機械・設備に多段安全制御構造を構築しているが、機械・設備、安全範囲および安全制御構造の関係を表すモデルとして浮き橋を自転車で渡るモデル（氷上浮橋モデル）を

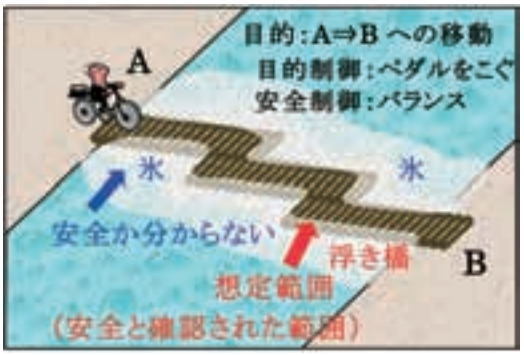

図 2　氷上浮橋モデル

図 2 に示す。ここでは、自転車の運転手（作業者）が A 点から B 点へ移動することを目的として運転（作業）を行うものとしている。目的達成のためには、まず事故や災害を起こさずに目的を達成できる安全範囲が存在しなければならない。それが浮橋（安全範囲）である。この浮橋は、雨、風等の環境や利用者の荷重等の前提条件（想定範囲）から強度や通路幅が設計され、施工される（安全範囲の構築）。また、この浮橋は老朽化に対応して継続的に維持管理される（安全範囲の維持管理）。一方、自転車の運転手（作業者）は、自転車（道具・工具等）を使用して、前進するためにペダルを踏み（目的制御）、同時に浮橋（安全範囲）から落ちないようにバランスをとる（調整制御）。さらに、何らかの理由によりバランスを崩して浮橋から出そうになったとき、出てしまう前にブレーキを掛けて停止する（インターロック）。氷は、安全範囲のあいまいさを表すと共に、浮橋から出たとしても必ずしも水に転落する訳ではないことを表現している。これは、化学プラントや機械・設備においてインターロックの条件を逸脱しても必ずしも事故が発生するという訳ではないことを氷で表現したものである。

2．3　浮橋モデルが示す化学プラント安全化の方向

浮橋モデルにおいて水の中に転落するという

事故・災害が発生する原因は、二つに大別することができる。ひとつは、浮橋の渡り難さや欠陥に起因するものである。化学プラントの設計に起因するものとしては、設備の設計震度は適切だったが配管系の設計震度が低い、津波を想定していない、計装機器は単一故障しか考慮していない、ユーティリティの供給は必ずバックアップされる、暴走反応は未然に防げることを前提とするなどの最悪想定の配慮不足が考えられる。また、化学プラントの維持管理に起因する欠陥もあり、設備の長期未点検箇所の存在、寿命予測が全面腐食を前提として局部腐食の考慮不足などが考えられる。

プラントの運転や保守作業という視点では、作業が複雑で微妙な操作が要求され難易度が高い、人にとって非常に大きな力を要求される、作業姿勢が悪い、計器類が見難い、作業が文書化されていないために作業のルールがあいまいで統一されていない、プロセスが改造されたときに運転マニュアルが改訂されなかったなどが考えられる。

いくら制御が正常であっても制御が安全と信じている安全範囲とマッチしていなければ事故が発生するということを意味する。よって、化学プラントの安全化の方向は、次が考えられる。

（安全化方向－１）安全範囲の拡大：設備設計における最悪想定の見直し、作業の容易化等。

（安全化方向－２）安全範囲の信頼性の向上：保守管理の技術力の向上、点検網羅性の確保。非文書化作業の文書化等。

もうひとつの事故原因は、本論文の視点である制御側に起因するもの、すなわち制御の失敗による安全範囲からの逸脱である。例えば、設備に備わる制御が外乱に耐えきれなかった、制御装置の故障など、制御の限界によって逸脱する、人の作業であれば、操作手順を誤ってしまった、マニュアル通りに実施しなかった、故意にルール違反をした、気を失ってしまった、アラームを見落としたなどのヒューマンエラーがある。安全範囲がしっかりしていても、制御の限界によって事故が発生することを意味する。この制御の信頼性向上の方法については後述することとし、ここでは安全確認の原理に基づく安全制御の基本を述べるにとどめる。

安全確認の原理とは、「安全は、その安全状態を確認して改めて「安全」と認められる。安全が確かめられないときに危険とみなす。」というもので、化学プラントを運転して良い条件とは、「安全範囲に入っていることが確認されていること」であって、安全範囲に入っていることが確認できなくなった場合にはそれを危険とみなして運転を停止する、という運転が、安全確認の原理に基づく運転である。安全の範囲（機械・設備の想定範囲や運転マニュアル・作業手順書の想定範囲）からの逸脱が必ずしも水中に転落（事故災害の発生）する事態にはならない。このため、生産継続のために氷上を運転して危機を切り抜けるという行動を起こしがちである。たとえば、プラントがインターロックによって止まろうとしているのに、それを解除してマニュアル運転で立て直して運転を継続しようとする、あるいは重要な安全装置が故障してプラントが乱れているのに、それを無効化して運転を継続しようとする、といった行為である。これらの行動は安全の原理原則から外れており、確実な安全は到底望めない。我々がより確実な安全を目指すのであれば、安全確認の原理を徹底することが必要であるため、次を安全化方向－３とする。

（安全化方向－３）安全確認の原理に基づく運転の徹底：安全範囲を外れたら運転停止を徹底。

3　スイスチーズモデルによる検討

3．1　スイスチーズモデルのプラント調整制御への適用

安全の概念モデルとして「スイスチーズモデル」は非常に有名であるが、その使われ方に決まりがあるわけではない。そこで本論文では、多段安全制御構造のうちの調整制御の部分を設備と人の信頼性の違いを考慮して適用する。**図3**にそのスイスチーズモデルを示す。まず、チーズがカバーする範囲を安全範囲とする。すなわち、どれだけのリスクを想定して設備が設計されているかをチーズの大きさに対応させ、安全範囲からの逸脱は左にあるリスクが右側に抜けてしまうことで表現した。なお、人の調整制御がカバーしている範囲は安全範囲全体であるが、そのうちの一部は設備の調整制御によってもカバーされている。この設備による調整制御と人による調整制御が重なっている部分は、製品を製造することを目的とする目的制御および安全範囲に留まるように調整制御が設備の自動制御によってなされ、一方運転者（作業者）は、設備による調整制御の性能や信頼性（以下単に「信頼性」という。）に限界があるので、化学プラントが安全範囲に留まるように設備の制御を補助する。例えば、自動制御していた流量

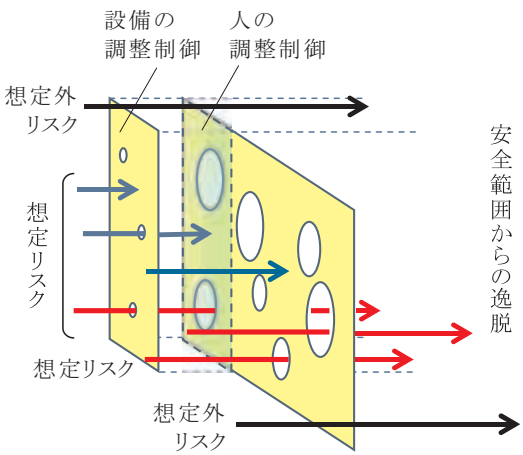

図3　プラントの調整制御のスイスチーズモデル

が乱れた時に制御弁をマニュアルモードに切り替えて運転する、自動制御に使用していた温度計が故障したときに自動制御を止めて人が熱源流量を操作するような制御構成を指し、制御が乱れた時に一時的に人が大きく操作して乱れを抑え、また自動制御に戻すという行為など、自動制御の限界による乱れを自動制御に代わって制御する場合である。

また設備による調整制御がなく、人による調整制御のみが行われる部分とは、あらかじめ人が実施するように設計された部分を指す。大きく分けて2種類あり、一つ目は自動化されていないプラントのスタートアップやシャットダウン、アラームに対する処置などのプラントの状況に影響を与える作業、そしてもう一つが手動バルブを操作して行うサンプリング、運転中のフィルター清掃、プラントの一部を停止して行う保守作業など（以下「プラント保守作業」という。）の設備がその作業を異常と検出しないように、言い換えれば運転に影響を与えないように行われる作業がある。

次に穴の大きさは、信頼性の違いを表現し、設備は人に比較して信頼性が高いため穴が小さく、人は機械・設備に比べて信頼性が低いため穴が大きい。そして、黒色の矢印は、想定範囲外のリスクが安全範囲からの逸脱として顕現した状況を示し、赤色の矢印は、想定していたリスクであるが調整制御の信頼性の限界によりチーズをすり抜けて安全範囲を逸脱した状況を示し、青色の矢印は、調整制御により安全範囲に留めることができたリスクを示す。

3．2　スイスチーズモデルが示す化学プラント安全化の方向

一般的なスイスチーズモデルでは、二つの計器の故障と人のエラーが同時に発生したために起きた事故を「3層のチーズの穴をすり抜けた事故。」と表現する場合がある。しかし、前項で提案したスイスチーズモデルは、この「二つの

計器の故障と人のエラーの同時発生」という事象を設計で想定していたのであればチーズの穴をすり抜けた事故、想定していなかったのであればチーズがカバーする範囲（安全範囲）の外のリスクが顕現した事故と捉え、原因の所在が信頼性にあるのか、設計における想定条件設定にあるのかを区別できるようになっている。信頼性は穴の大きさで表現しているが、その信頼性を上げるための方法については後述するものとして、**図 4** にはそれ以外の安全化の方向性を示す。**図 3** で示したリスクの矢印の中に安全範囲から逸脱したリスクとして 5 本の矢印があり、**図 4** ではその内の 3 本を安全範囲から逸脱しないように変えているが、安全化の方向は次の 2 つである。A および B は、前述の安全範囲の拡大であり、安全化方向－ 1 に相当する。そして C が、新たな安全化の方向である。

（安全化方向－ 4）自動化による技術伝承の推進：人による制御の技術を自動化によって伝承。（人から人への技術伝承の最少化）

これは人が実施している調整制御の自動化、すなわち手動制御を自動制御にするという方向性である。人が実施している制御や作業は、人から人へ技術伝承されなければならない部分である。もちろん作業手順書やマニュアルが整備されるが、書面に書ききれない部分の技術が伝

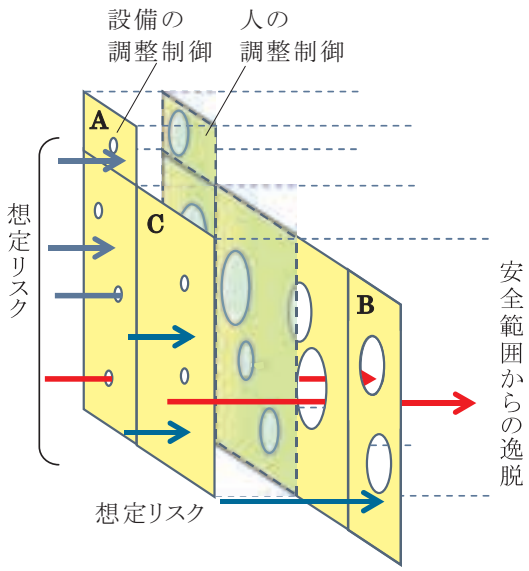

図 4　プラントの調整制御の安全化の方法

承する上での課題となる。手動制御を自動制御にするということは、伝承すべき技術を設備化して伝承するということであって、忘れ去られることのない伝承方法である。なお、ある一定の操作手順しか実施できないようにするなどのフールプルーフも手動制御の設備化の一種と考えてよい。

ここで、どのような手動制御を自動制御にしていくかが問題となるが、自動化の効果をエラー発生率で検討する。**表 1**[(5)]は、人のエラー発生率を意識フェーズ毎に整理したものであるが、ここでは代表的な値として、正常・リラッ

表 1　人の意識フェーズとエラー発生率[(5)]

フェーズ	意識のモード	生理的状態	エラー発生率
O	無意識、失神	睡眠	1.0
I	意識ぼけ	疲労、居眠り	0.1以上
II	正常、リラックスした状態	休息時、定例作業時	0.01～0.00001
III	正常、明晰な状態	積極活動時	0.000001以下
IV	興奮状態	慌てている時、パニック時	0.1以上

クスした状態のエラー発生率を0.0001、興奮状態のエラー発生率を0.1、設備のエラー発生率を0.0000001、設備の能力の限界を補う人のエラー発生率を興奮状態と仮定して0.1、全制御の内で自動化されている比率を *Raut*、手動制御のリラックス状態の比率を *Rrel*、手動制御の興奮状態の比率を *Rexi*（ただし、*Raut* + *Rrel* + *Rexi* = 1）とすると、設備全体としてのエラー発生率 *ERall* は、次のように表される。

$$ERall = Raut \times 0.0000001 \times 0.1 + Rrel \times 0.0001 + Rexi \times 0.1 \quad ①$$

ここで、リラックス状態で行われる手動制御を自動化して、全体の自動化率を１％引き上げると考えた時、設備全体としてのエラー発生率 *ERall* は次のように表される。

$$ERall = (Raut + 0.01) \times 0.0000001 \times 0.1 + (Rrel - 0.01) \times 0.0001 + Rexi \times 0.1 \quad ②$$

また、興奮状態で行われる手動制御を自動化して、全体の自動化率を１％引き上げると考えた時、設備全体としてのエラー発生率 *ERall* は次のように表される。

$$ERall = (Raut + 0.01) \times 0.0000001 \times 0.1 + Rrel \times 0.0001 + (Rexi - 0.01) \times 0.1 \quad ③$$

式②と③の差異は0.000999の一定値であり、自動化がどれだけ進んでいたとしてもリラックス状態で手動制御を行っている作業を自動化するよりも興奮状態で手動制御を行っている部分を自動化する方がエラー発生率の低下が1000倍大きい。この倍率は興奮状態と正常・リラックスした状態のエラー発生率の比であるため、エラー発生率の仮定により異なる値になるが、大きな倍率になることに変わりはない。興奮状態で手動制御を行っている部分の代表的なものとしては、プラントが乱れて多量のアラームが同時発生したとき、重要アラームが鳴った時の処置、緊急シャットダウンが発生した際に大至急実施しなければならない後処置などが考えられるが、こういった部分を優先的に自動化するべきである。よって、安全化方向－４を効果的に実現するために次も方向性として必要である。

（安全化方向－４’）人の作業の自動化は、興奮状態で行う作業の自動化を優先

３．３　インターロックおよび非常停止

設備による「インターロック」とその限界を補う人による「手動非常停止」の関係は、前項の設備による調整制御と人による調整制御の関係と同じであり、安全化の方向性も同じである。しかし、人によってのみ安全制御が行われる部分は、人の能力の限界によって失敗したときにそれを補ってくれるものがない場合がある。前述のとおり、人による安全制御はプラントに影響を与えるものと与えないように行われるものがあるが、人による安全制御がプラントに影響を与える場合、例えば手動によるプラントのスタートアップ操作など、人の行った失敗によってプラントの自動シャットダウン条件に至った場合は、その機能によりシャットダウンが実施されることになる。その一方で、プラント保守作業など、プラントに影響を与えないように実施される作業は、その作業が作業手順書やマニュアルから逸脱しそうになることを設備が検知することができないため、操作のミスが危険物の漏えいなどの事故に直結する場合が多い。これに対しては、人の調整制御の信頼性を向上させるとともに減災措置をインターロックの代替としなければならない。その方法は第４項で示す。

4　調整制御・インターロックの信頼性向上

4．1　設備による調整制御とインターロックの信頼性向上

スイスチーズモデルの設備部分における穴は、装置の故障によるもののほか、外乱に対する能力の限界などによるものである。これらの対応としては､装置そのものの信頼性向上の他、冗長化、モデルを使用した高度な制御など確立した技術があるため、それらの採用を推進する必要がある。現在のプラントの制御は相当に信頼性が上がっていると思われ、新たな安全化の方向とする必要がないものと思われる。むしろ、安全化方向－１の安全範囲の拡大として何処を設備化するが重要であると考える。

4．2　人による調整制御の信頼性向上

人の信頼性というものは、一時的に信頼性が上がることがあっても恒常的に信頼性が２倍に上がるようなことがないことは誰もが知ることであり、それを考慮した対応が必要である。その一つの方法が既に述べた手動制御の自動化であるが、ここでは、操作のミスが危険物の漏えいなどの事故に直結するプラント保守作業について自動化に拠らない対策を検討する。

機械の場合、挟まれ・巻き込まれ防止対策として、機械の可動領域に人が進入すると機械が停止するインターロックが組み込まれるが、その機械のインターロックを解除して機械を作動させるリスクの高い保守作業がある。このような、高リスク保守作業であっても安全に作業を継続できる安全範囲が存在し、それが作業要領書や手順書等に記された作業方法である。機械と人が連携・協調して動き、連続的に保守作業を継続することができればよいが、安全範囲から逸脱してしまって事故が発生する。人の行動が機械と同等に正確であれば事故はほとんど発生しないであろう。しかし、人はミスをする、ルールを忘れる、良かれと思ってルール違反をする、これらが原因である。安全に保守作業を実施するためには、安全制御構造原則に基づいて「調整制御」と「インターロック」機能を適用するべきである。すなわち、**図５**に示すように実際に作業を実施する人の他に、「作業手順書から逸脱しないように介助する機能を果たす人（調整制御介助者）」、「手順書から逸脱しようとしたときに作業の停止命令を出す人（安全確認実施者）」の二人が必要である[(3)]。ここで G_M, G_Hは、それぞれ機械側および人側のインターロックを表す論理演算要素であり、N_Mおよび

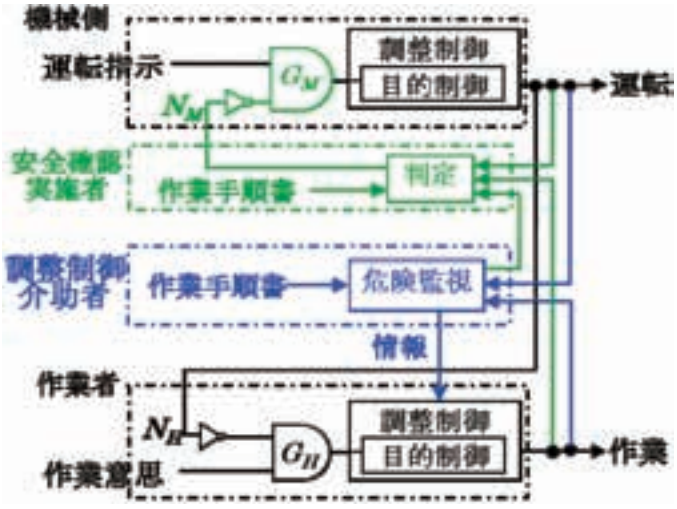

図５　機械保守作業の制御構造原則

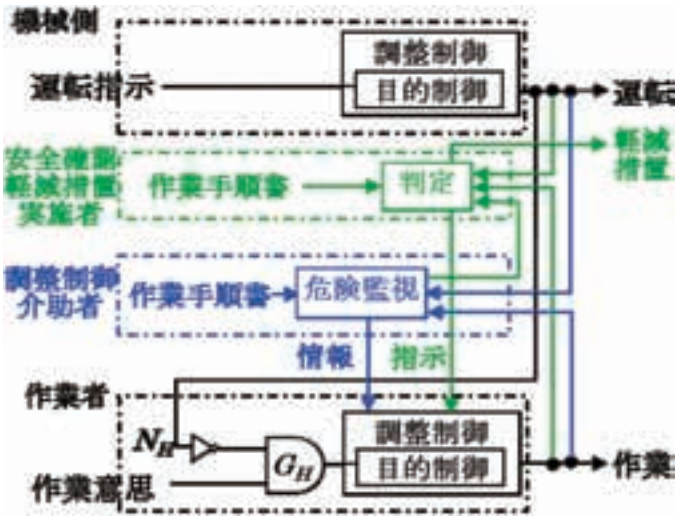

図 6　プラント保守作業の制御構造原則

N_Hは否定要素を示している。

ここで検討するプラント保守作業は、プラント停止操作が事故の未然防止に時間的に間に合わない場合や既にプラントが停止しているが危険物や可燃性ガスが存在している状況での作業であり、作業者のミスが直接危険物の漏洩を引き起こしてしまうような作業である。この場合の安全確認実施者は、プラントを停止しても効果がないことから作業者の行っている作業が安全範囲から逸脱する前に作業停止を指示して止めさせる機能を担わなければならない。また、安全確認実施者の停止指示によってもリスクが下がらない場合、すなわち作業停止の指示が事故の未然防止に間に合わない場合は、安全制御構造原則にのっとり危険物等の漏えいやその後の着火に対して即座に減災処置（着火防止措置や消火作業）を行える体制をとって作業することを原則としなければならない。この制御構造を**図 6** に示す。

プラントの保守作業についても、安全の原理原則に基づいた体制をとることが今後の安全化の方向性の一つである。

（安全化方向－５）プラント保守作業の信頼性向上：安全制御構造原則に基づくプラント保守作業

5　おわりに

安全の原理原則から導かれた化学プラントの安全化の方向性を**表 2** に整理する。一般的に言われている安全化の方向性と同じものも含まれているが、安全化方向－３、４、５については安全の原理原則から導かれる特徴的な方向性である。

まず、安全確認の原理に基づく運転を実施すること。これが大前提となる。最近の事故で現場力の維持・向上が対策として挙げられていることが特徴であることを冒頭に述べたが、現場力の維持・向上の施策が安全確認の原理に反することに向けられてはならない。むしろ、安全範囲の拡大や自動化の推進の中で現場力の維持・向上を目指すべきである。安全確認の原理から外れたことをやっていたのでは、確実な安全は到底望めないことを改めて強調しておきたい。

事業者はこれを踏まえて化学プラントの安全化のために設備の改善を実施する必要があるが、どの部分に投資して安全範囲を拡大するべ

表 2　化学プラントにおける安全化の方向性

No.	安全化の方向
－ 1	安全範囲の拡大：設備設計における最悪想定の見直し、作業の容易化等。
－ 2	安全範囲の信頼性の向上：保守管理の技術力の向上、点検網羅性の確保。非文書化作業の文書化等。
－ 3	安全確認の原理に基づく運転の徹底：安全範囲を外れたら運転停止を徹底。
－ 4	自動化による技術伝承の推進：人による制御の技術を自動化によって伝承。（人から人への技術伝承の最少化）。効果的な自動化のためには、興奮状態で行う作業の自動化を優先。
－ 5	プラント保守作業の信頼性向上：安全制御構造原則に基づくプラント保守作業。

きかを検討するのが事業者の課題となる。手動制御の自動制御化については「興奮状態で行う作業の自動化を優先」という方向を導いたものの、最悪想定の見直しや想定条件の抜けを見出すことには貢献しない。現在、事業者は事故事例を水平展開するほか HAZOP や FMEA などの解析手法を使ってリスクアセスメントを実施して安全化を進めようとしているが、これらの解析手法は1950年代から1960年代に開発された手法であり、解析の肝となる部分を人に依存している手法である。その当時のプラントにおいては有効に機能したからこそ世界中に広まったものだが、最近発生した化学プラントの事故を見ても、複雑化した現代のプラントにおいて現在の社会から求められている安全レベルに見合った結果を出すことは極めて難しくなっていると思われる。化学プラントの安全化を効果的に実現するためにも、新しい解析手法の開発が望まれる。

また、自動化できないプラントの保守作業については、三つの機能を担う作業者による多段安全制御構造の体制での作業を提案しているが、ロケットや人工衛星関係の作業では既にこのような制御構造がとられている。あらゆる保守作業を三人以上の体制で実施することは、一般の産業では到底実現できないであろう。しかし、結果的に二人作業あるいは一人作業になるとしても、この三人による安全制御構造から人数を減らしてよい根拠を明確にするリスクアセスメント（リスクを上げるためのアセスメント）を実施することで、安全性の向上が期待できる。

本論文では、機械安全の分野で培われた安全の原理原則を化学プラントに適用して安全化の方向を検討したが、このような検討はまだ始まったばかりであり、検討を深めることで新たな発見が期待できる。最近の事故の対策として挙げられている安全文化は、倫理的な文化だけではなく、安全を論理的に考える文化も必要であると考える。今後、より多くの研究者によって論理的な検討がなされることを期待したい。

参考文献

(1) 杉本旭，蓬原弘一，向殿政男，安全作業システムの原理とその論理的構造，電気学会論文誌 D，Vol. 107-D, No.9 (1987), pp. 1092-1098

(2) 杉本旭，蓬原弘一，安全の原理，日本機械学会論文集 C 編，Vol. 56, No.530 (1990), pp. 75-83

(3) 木村真，田中慎也，福田隆文，杉本旭，機械の安全制御構造とその保守作業への適用に関する考察，日本機械学会論文集 C 編，Vol. 77, No. 775 (2011), pp. 1090-1098

(4) 杉本旭，粂川壮一 他，安全確認型安全の基本構造［安全（確認）型構造の条件について］，日本機械学会論文集 C 編，Vol. 54, No. 505 (1987), pp. 2284-2292

(5) 橋本邦衛，安全人間工学，中央労働災害防止協会 1984