PSB (Process Safety Beacon) 2016 年 3 月号 の内容に対応	SCE・Net の 安全談話室 (No.117) http://www.sce-net.jp/anzen.html	化学工学会 SCE・Net 安全研究会作成 （編集担当：三平忠宏 ）

今月のテーマ：安全装置それとも制御機器？

（PSB 翻訳担当：中村喜久男、三平忠宏、竹内　亮、小谷卓也（纏め））

司会：　今月の記事は、本来安全装置として使うべきものを制御用に使うという、大変危険で問題のある内容を取り上げています。まずこの記事を読んでの感想や意見をお聞かせください。

山岡：　制御装置と安全装置は目的も機能も異なるものとして扱っていますので、一般にはこのようなことは考えられないのですが、アメリカでは一緒に使うことが普通のこととして行われているのでしょうか。あるいはテーマとして取り上げるベース、素地があるのでしょうか。

竹内：　しっかりと安全管理を行っている日本の会社では考えられない事故かも知れませんが、安全対策があるが故に油断してしまうケースは少なくありません。例えば、書類の間違いを複数の人でチェックすることにすると、一人一人は真剣にチェックしなくなる傾向があります。何かに頼って自分が楽をしようとすることは、我々日本人にもあることだと思います。

山岡：　確かに、計器の見過ごし、警報の無視、他との並行作業などをして、必要な制御がなされずに安全装置作動に至ってしまうことはありますね。このようなことをしないことと、運転の管理をしていることをしっかりと意識することが大事です。

澤：　制御装置（BPCS-Basic Process Control System）と高次の Protection Layer(防護層) を混同してはいけないという話の趣旨は分かります。LOPA分析でも低次の Protection layer としてBPCSを挙げていますし、それに近いコントロールは一般的です。この点をはっきりさせるには、必ず HA(High Alarm)と HHA(High High Alarm)の両方をつけて、HA はプロセスコントロール用、HHA は緊急停止用であることを理解してその使い分けを正しく理解させて、それぞれのアラームに対するオペレーター対応の仕方を明確にすべきことなのだと思います。

蒸気機関車の話にしても本来ボイラーが炊き上がったこと知らせる警報が必要なのを安全弁が吹くシューという音をその警報代わりに使っていたと思われます。またコントロールとしては、圧力を逃がすことを圧力コントロールとせずに火力のコントロールで温度コントロールとすべきであるのを、圧力逃がしでボイラー内圧をコントロールするという使い方が根本的な間違いのもとであると思います。でも昔のようにたくさんの計装機器をつけることをしなかった頃は、安全装置を制御機器に使うことも一般的であった可能性は大いにあると思います。

小谷：　プロセス安全の先駆者 Trever Kletz 教授の名が出て来たので、業績を簡単に紹介します。彼はユダヤ系ロシア移民出身で 1944 年に Liverpool 大学卒業後 ICI に研究員として入社しました。各種プラントのマネージャーとして経験を積み、1968 年に初代の Technical Safety Advisor に就任しました。ICI 社が公表した Hazard and Operability Study (HAZOP)初版作成での中心人物として知られています。1982 年に引退後も著作や講演などで inherent safety(本質安全)の概念を世界的に高めた功績等を評価され、Royal Society of Chemistry(英)、Institution of Chemical Engineers(英)、AIChE の三つの学会で Fellow に推挙されていました。また、教授が逝去されたときは,US CSB の会長が、それを悼むステートメントを出すなど世界的に評価の高い人物でした。

そのステートメントには、彼の言葉として「長い間事故の大半は human error によるとされているが、事実ではあるかもしれないが大して役には立たない。落下事故は重力によると言うようなものだ」と言っていたそうです。

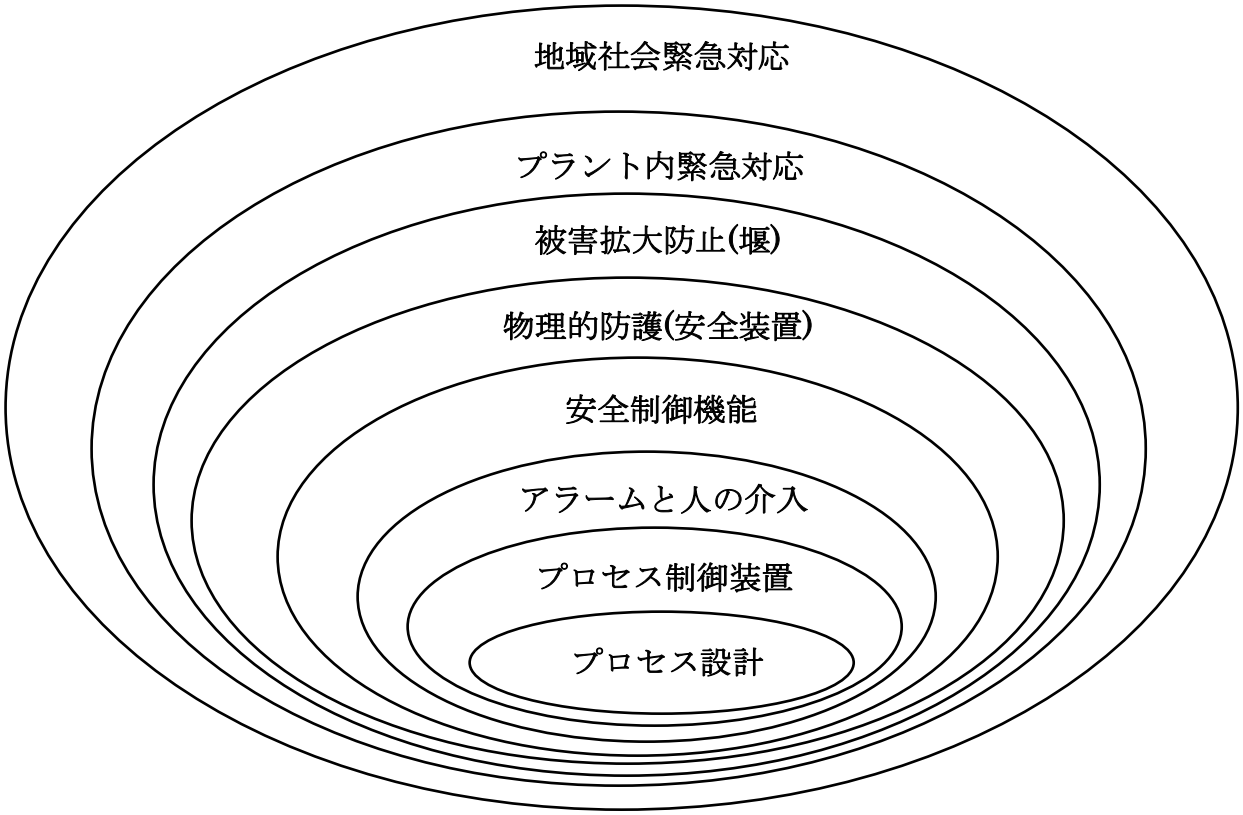
司会：　今月の記事の中に「第二防護層という言葉が出てきて、ここは分かりにくいですね。言葉の簡単な解説も欲しいですが、皆さんの会社ではこれに相当することをどのようにされていましたか。

牛山：　スイスチーズモデルが割合分かり易い例かもしれません。スイスチーズは所々孔（欠陥）があいていますが、チーズ片（防護層）を何枚も重ねると孔が重なることがなくなり、危険に対する防護ができることになりま

す。簡単な例では機器が漏れに対する第1防護設備で、タンクの防油堤やプラント周囲の防液堤が第2防護設備になります。

竹内: 先程、澤さんの発言にもありましたが、LOPA(Layer of Protection Analysis)というハザード分析の手法があります。米国では PSM(Process Safety Management)が OSHA によって義務化されているので、化学関係の会社では多くの人が LOPA を知っています。従って米国人は Layer of Protection (防護層)には違和感がないでしょうが、日本ではあまり馴染みがないと思います。その意味で、この PSB は訳し辛かったですね。因みに LOPA をしっかりと行っていれば、福島第一原発の事故は防ぐことが出来たと思います。

澤: CCPS の発行している Layer of Protection Analysis という本の12ページの2．1図に可能性のある事故に対する防護層（Layers of defense against a possible accident）として LOPA(Layer of protection analysis)の基本的概念として以下のような図が載っております。



2.1 図 CCPS Layer of Protection Analysis より

このように LOPA では、事故防止のために基本的な本質安全設計から最終的は地域防災体制の整備まで、多くの防護層に守られてプロセスの安全が図られているという考え方をします。この考え方では、基本的なプロセスコントロールも保護層であり、より深層の保護層という考え方ができます。また基本的なプロセスコントロール系は2番目の保護層、そのコントロール系の入力を使ってハイレベルアラームを吹鳴しオペレーターに行動を求めるのが3番目の防護層、さらに安全弁は第五番目の保護層となっています。そのようなわけで Primary protection layer を主保護層と翻訳せずに一次保護層、Secondary protection layer を二次保護層と翻訳すれば、LOPA 的解析のスイスチーズモデルの第一保護層、第二保護層といった考え方で解析できると考えられます。

中村: 保護層という言葉についてですが、2002 年 3 月号の Beacon には、次のことが書かれており、参考になります。①“保護層”のどれも機能しなかった為に起きた事故。（アラームが間違っているとの思い込み。圧力制御システムの機能停止。放出ラインのフレームアレスター目詰まり。その結果がタンク屋根の破壊。） ②保護層とは何か。（運転員によるモニタリング、作業手順、アラーム、インターロック、規格圧力の機器、リリーフ弁/バキューム弁。大抵の損傷は複数の保護層の不具合より起こる。） ③保護層の観点で、装置を保護す

るためにすること。（アラームの異常はすぐに修理。シフト業務の最初に全アラームの状態チェックと理解。圧力/真空リリーフ弁を確実にテストするメンテナンスシステム。ベントラインは詰まらないようにクリーニングを十分に。非日常操作では保護層は特に重要。）

竹内： なるほど、「アラームと人の介入」「安全制御機能」「物理的防護」の防護層が機能せずに事故が起きたのですね。

司会： この記事ではボイラーの圧力制御に緊急脱圧用安全弁を使用した例と、タンクからのオーバーフロー防止用の緊急停止計器を受け入れの通常制御に使用した例が挙げられています。極端な事例のようにも思いますが、似たようなことでトラブルや事故・災害を起こした経験や見聞がありましたらお聞かせください。

竹内： タンクからのオーバーフローの事故は前回のプエルトリコの場合も、バンスフィールドの場合も緊急遮断装置が安全装置として設置してあったのに機能せず、事故になっています。最終的には安全装置があるから大丈夫だろうという気持ちで運転していた可能性があると思います。

澤： 私が、ダウケミカルで使用していたプロセスコントロールシステムは2台のコンピューターが同時に作動しているDDCで、もちろんセンサー等は一個が共有されているものでとても完全なDUELシステムではありませんでした。しかしプロセスコントロールプログラムを作成する場合は、ほとんどの測定点に対してむろんフィードバック・コントロールはさせていましたし、アラームはH(High)とHH(High High)をつけ、警報の音色も変えて、対応に仕方も変えるように指導しました。ボイラーの圧力制御は本来熱量の制御をすべきで（燃料が無駄ですから）、緊急脱圧用安全弁を圧力コントロールに使用することは設計思想が間違っていることであり、タンクのオーバーフロー防止にはたとえ同一計器の信号を使ったとしても、コントロール用とは別に H、HH のアラームを発報させ、異なった対処を要求するようにプログラムすべきです。

司会： プロセス制御でよく使われているのは圧力、温度、レベルなどですが、これらの ON-OFF 制御で計器が故障した際に逸脱してトラブルが起こります。また連続制御の計器でも同様なことがあり得ます。通常は警報による検知やインターロックによる停止でトラブルや事故を防ぐように設計すると思いますが、それでも特殊なケースとして問題を起こしたことはないでしょうか。

澤： 電源が完全に停止した場合は制御系もダメになります。そのことを防止するためには補助電源を使って重要計装を動かすことですが、それも長時間経過することでダメになります。東日本大震災の時の東京電力福島原子力発電所の事故がそのような例ではないでしょうか？

山岡： 計器の誤作動のため、重要な機器にインターロックが作動したことがあり、それを機会に運転や安全管理上の重要な計器には、2 out of 3 の冗長システムを入れました。 安全設備については、通常は使われませんが、常時、必要な時に働くよう、定期的に腐食や欠陥の有無などの目視点検や作動テストなど実施することが大事です。また、生産能力を増強するときなど、安全設備の能力もチェックする必要があります。

司会： 安全装置を制御機器に使うというのは、日本ではあまり例がないと思われるので、このような代替の例ではなく、個々の安全装置、制御機器が原因でトラブルや事故・災害の経験や見聞がありましたらお聞かせください。制御機器の例は多いと思いますので、大きなものや特殊なものをお願いします。

三平： VCM(塩ビモノマー)をタンカー輸送で受け入れた初期には船側にポンプがなく、中間タンクのガスを圧縮してタンカー気相部を加圧して液モノマーを荷揚げしていました。揚がって来た液は同じ中間タンクに受け入れ、LIC 制御で別の貯蔵タンクへ送るようにしていました。この LIC のディスプレッサー型発信器が故障して、液モノマーがオーバーフローして圧縮機に流入するという大きなトラブルを経験しました。

入社して間もないーオペレーターの時期で、レシプロ圧縮機が大音響で振動しているのを必死に停止しました。荷揚げだけの短時間の使用というためか、この制御系にはアラームもインターロックも付いていませんでした。後日いろいろなプラントのプロセス設計に関わるようになり、アラームやインターロックをしっかり考えるようになった原点のトラブルです。

澤： 安全装置を制御機器に使うというわけではありませんが、制御面から見ると一つの検出端からフィードバック・コントロールの測定端、アラームの入力に使うことは一般に実施することだと思うので、日本であまり例がないと思うという意見には同意しかねます。電源、検出端、コントロール系、出力をすべて別にした近年の厳

密なSISシステムなどが一般的でない頃のプロセスコントロールでは、プロセスインプットをコントロール、警報、インターロック、シーケンシングなどいろいろな目的に使っていました。またこのような系をすべてのコントロールにつけることは非常に高価となりますので、その必要性はプロセスの危険度で選択することになると思います。

竹内: LOPA の考え方では、一つの検出端から取ったコントロール、警報、インターロックなどは防護層としては一つとしてしか数えられないことになっています。複数の防護をしたつもりでも、一つの検出端の故障で全ての防護機能が失われるのであれば防護層として一階層でしかないという考え方です。

司会: 安全装置の管理基準や作業員への教育について、実施する際に注意していたことをお聞かせください。

竹内: 安全装置が故障していてはいざという時に事故を防止出来ないので、その検査や調整は極めて重要です。一般の機器のメンテナンスとは異なるレベルの保守計画が必要でした。

澤: 近年はプロセスコントロールが進んですべてが自動運転されるようになると、すべて計器任せで何も考えない運転員や技術者が増えて、計器が狂った時にどのように対応するかわからない場合があるように思います。そういう事態に備えて原理、原則を理解することと、すべての計装について定期的な検査と作動確認を行うことが重要であることを教育しておりました。

車の自動停止装置の搭載が一般的になってきている現在、万一自動運転が正常に作動しなくなった時に、運転者がどのように異常であるかを判断し、緊急停止をどのようにできるか、また安全な状態まで持って行って停止できるか、理解されているか不安に思うこの頃です。

司会: 今月は安全装置と制御機器についての PSB の記事からの議論で、多くのコメントをいただきました。第二防護層という言葉から日本ではあまり馴染みのない LOPA についての詳しい解説があり、プロセス制御と安全についても踏み込んだ議論が行われました。これを契機にハザード分析や PSM など米国流の安全対策への理解が進むことを期待します。長時間のご討議をありがとうございました。

（キーワード） 安全装置、制御機器、プロセスコントロール、防護層、スイスチーズモデル、LOPA 、インターロック

【談話室メンバー】

井内 謙輔　牛山　啓、加治 久継、小谷 卓也、齋藤 興司、澤 寛、澁谷　徹、竹内　亮、
中村 喜久男、長安 敏夫、日置 敬、松井 悦郎、三平 忠宏、山岡 龍介、山本 一己、渡辺 紘一

以 上