PSB
(Process Safety Beacon)
2018 年 12 月号
の内容に対応

SCE・Net の 安全談話室(No.150)

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：共通原因による故障

（PSB 翻訳担当：澤　寛、三平忠宏）

司会：　今月号のテーマは Common Cause Failure 共通原因故障です。二件の事故事例が挙げられていますが、最初にこの記事を読んでの感想や内容について補完するコメントがありましたらお願いします。

金原：　バックアップ機能を過信すると大変な事態が生じるという教訓と共に、その保護をどこ迄考えておくかという意味で難しい課題であると考えます。この空港の発着数の実績を調べてみると、2015 年は約 88 万回で、単純に計算にすると1日に 2400 回、滑走路が5本あるので1時間あたりに 20 回／本となります。今回の事故発生は繁忙期の昼間でしたので、おそらく平均の 2 倍位にはなるでしょうから、各滑走路で1時間に約 40 回も離発着をしていることになります。通常でも円滑に運営できる体制に感心するとともに、その状況下で突然停電したにも関わらず航空機事故が発生しなかったことから、しっかりした緊急時の対応力を備えていたと考えます。

竹内：　アメリカのハブ空港というと私はシカゴのオヘア国際空港を何度か使ったことがありましたが、アトランタ国際空港の方が規模は大きいと初めて知りました。オヘア空港の規模もかなりのものでしたからアトランタ空港の規模もそれを超える巨大空港ということですね。

牛山：　昔のアトランタ空港しか知りませんが、国内線は 5 つのコンコースを直線的なトラムが往復して繋いでいてトランジットがし易く、大きな空港にかかわらず非常に機能的だという印象がありました。それだけに一旦停電で機能が失われると、逆に代替手段を講じるのが難しいのかもしれませんね。

金原：　いくつか事故を経験していますが、システムが想定通り機能せず、組織が訓練通り動かなかったことが多くありました。今回、冷静に対応できていたのは、緊急時の対応訓練の成果と思いますし、システム面でも異状なく作動できたことも航空機事故ゼロになった要因と考えます。

飯濱：　電気会社からの給電がなくなっても、バッテリーによるバックアップで管理が出来るはずで、30 分程度は管制を正常に維持できたのではないでしょうか。着陸中の飛行機はそのまま着陸させるにしても、着陸していない飛行機は引き返させるなど、管制官の仕事はしっかりできるはずです。

竹内：　管制官側からみて一番困るのは、停電が起きた時にそれが僅かな時間なのか、長くなるのかが分からないことだと思います。それが長いと分かっていたら、離陸を待っている人たちを飛行機から下ろすことを考えるでしょうし、直ぐに復帰すると分かっていれば待機させようと判断ができますが、そのもとになる情報がすぐに入手できるとは限らないということです。このケースでは機内に長時間待機させられた人たちがいたとのことですから、情報がなかったものと思われます。

澤：　サブステーションがあって二系統の電源供給があるはずなのに、停電後に何故両方が駄目になったのか理解できない人もいるでしょうね。

竹内：　そういうことが実際にどうなっているか、電源の二系統がどういう状態になっているのか分かるようになっているとよいのですが。例えば一系統が駄目になって、もう一系統へ切り替えが上手く行かないということもあり得ますので、情報がなければ「直ぐに復帰するだろう」という気になるかもしれません。

山岡：　先日の北海道・胆振地震の道内全面停電で、千歳空港も停電しましたが、その時の対応が、飛行機の発着の停止指示など直ちに適切に出来てよかったという印象を受けました。日頃の安全確保に対する意識や訓練などがうまく機能していたのでしょうか。

竹内：　あれは原因が地震よるということが管制官も分っていたので、割合とスムースに行ったのではないでしょうか。それと比べるとこのアトランタのケースは、どこで何が起きてどう対応するか、管制官が判断するのは難しかったと思います。

山岡：　先ほど竹内さんから停電が直ぐに復帰するのか、長く続くかという話がありましたが、同じようなことで当社のプラントの例で全面停電後の処置でトラブルがありました。運転担当者は停電が長くなると判断したのですが、3 分もしないうちに復帰したのです。全面停止作業中からの急な復帰を行うことになって、プラントの操

業開始後3年ということでこのような事象の経験が少なかったために、対応を間違えて大きなトラブルになりました。全面停止の作業を続けてしていればよかったとの感想が述べられていました。このトラブルを契機に、停電のみ、停電とスチームストップ、スチームのみのストップのそれぞれについて潜在危険を洗い出して対応を決め、緊急訓練のテーマに加えました。

三平: 安全に全面停止の操作をやった後に、再立ち上げをすべきだったということでしょうね。しかし現場としては何とかしてすぐに復旧させたかったということで、現場実務の経験者としてその気持ちはよく分かります。

金原: やはり日頃から、いかにしっかりと訓練されているかということと、システムの設計思想があらゆるケースについて考えられ、かつ日頃のメンテナンスが十分にされていることによって、その機能が発揮されることが大事で、それにより的確な対応ができると考えます。

澤: 全面停電のような緊急事態でプラントが停止した時に、元に戻すのにどのくらいの時間と金が掛かるのかを把握する、リカバリープランというものは出来そうで出来ていませんが、これは大事なことだと思います。

司会: 二番目の事例にパイパーアルファプラットホームの事故があります。消火ポンプのマニュアル設定の背景など細部の内容をどなたかに補完していただき、さらに追加のコメントがありましたらお願いします。

牛山: パイパーアルファの事故は、メンテの際ポンプレリーフ弁が取り外したままであるのを確認せず、ポンプを起動したことによる火災爆発事故ですが、火災が発生した際、その日は別に消火ポンプのメンテナンスのため潜水夫が吸水口周辺に潜って作業しており、消火ポンプを自動起動すると吸い込まれる危険があるため、マニュアル起動に切り替えていました。この起動用スイッチのある場所が火災発生場所に近く、人がアクセスできなかったため、消火用ポンプが起動できないという不幸が重なったものです。

金原: 私のいた工場では、プラントに冷却水を送るポンプから枝取りし、消火用水配管に接続しています。そこで何らかの原因でポンプの圧力が低下した場合には消火水専用のポンプが起動し、ブースターの役割を持って供給しています。そのポンプは自動起動ですし、さらに作動不良や停電時に備えて、ディーゼルポンプをバックアップとして保有しています。

三平: 私のところでは小型ポンプで工場の消火用水ライン全体を充圧しておき、どこかで火災発生等による消火栓が使用されて圧力が下がると、ディーゼル駆動の大型消火用水ポンプが自動起動するようになっています。消火用ポンプは停電時でも対応できる必要があり、以前は電気モーター駆動のものとディーゼル機を併設していましたが、現在は設備をシンプルにして定期的な点検とテスト運転を行っています。法改正で消防車用には消火用水ラインとは別に工場内に給水ラインと給水栓を敷設しています。無尽蔵にある海水を使うようになっていて、公設消防車も自社のものも問題はありませんが、実際に使うと放水先のプラントにいろいろと問題が起こるので、訓練では普通の消火用水を使っています。

司会: 共通原因故障とは、共通の根本原因により複数のシステム・機器が同時に故障する事象で、日本での典型例としては福島第一原子力発電所の津波による安全設備の機能喪失があります。この原発事故やその他の事故事例から共通原因故障を考察しての議論、コメントをお願いします。

三平: 福島第一原子力発電所では、通常電源設備の機器類と緊急用ディーゼル発電機がほとんど同じ高さにありましたので、地震後に襲来した津波により動力、制御、通信などの根幹となる電源が冠水により機能を喪失してしまいました。原子炉の冷却ができず、さらに非常用炉心冷却システムも使えず、炉心損傷事故を引き起こしました。

金原: バックアップといっても「通常の状態を維持する機能」と「最悪の事態を避ける機能」があると考えます。福島の原発事故については、後者の機能による保護をどこまで考えていたかが、現在裁判で問われていると考えます。危険度と頻度をマトリックスにした解析方法がありますが、それに(被害額÷投資額)のような指標を織り込んだ三次元マトリックスで考える必要があると思います。原発の例は極端なので、そんな簡単なことでは判断できないと考えますが、化学プラントでは、そのような評価指標で考えて経営判断する必要があると考えます。冒頭に示した二つあるバックアップレベルのいずれが必要かはケースバイケースによると考えます。

飯濱: バックアップと言っても二重化して通常の状態を維持するものと、もう一つはプロテクションエリアで防護するものがあります。後者は化学プラントの重大事故を防止するためのもので、基本は通常状態、その次は多少

温度や圧力が上がっても防護するようにしています。その上にさらにいくつもの階層があって一気に事故にならないように防護しています。

竹内： 要するに防護層がいくつもあって、一つの事象でそれが全部だめになることがないようにと考えるのがLOPA(Layer of protection analysis)における独立防護層の考え方です。

金原： いずれにしてもバックアップを考え、実施するには投資が必要です。その判断基準として経済指標を考える必要があると考えます。

竹内： 経済指標を入れるとなると、このビジネスでどのくらいの収益が上がるかとか秤にかけて、どれだけ投資できるからやろうとか、あるいは膨大な投資がいるから止めとこうとかと、いうところまで行ってしまうのではないでしょうか。

飯濱： 当社の場合を言わせてもらうと、ハザード系のチームは経済的なことを考えないで、検討して上へ上げます。その後金勘定して提案が受け入れられれば、工場長の権限で実行できます。より大きなものは経営者の責任による判断になりますが、定量的に表せないと経営判断もできません。

金原： 特に発生確率は小さいが、発生した場合の損害額が莫大な事故になる可能性のある案件が、その対象になります。言われる通り定量的に把握できないと経営者は判断できないので、具体的に実行するのは難しいと考えますが費用対効果を明確にする必要があると考えます。

竹内： 想定される被害額などを経営者に報告することが必要です。これくらい投資することで被害を小さく出来るという報告ならば投資額との比較で判断できます。また発生頻度がどうなのか、被害額がすごく大きくても頻度がずっと小さければ、それはリスクを取ることにしようと経営者が判断できます。チームが判断するのではなく、資料を提供することで、後はマネージメントが法規制を満足する範囲で判断するわけです。

金原： 経営者へ上げる前に絞り込み、ふるい分けが必要で、沢山提出して、自分では選べないので選んでくださいというのは、経営者としても判断しかねると考えます。

竹内： 工場長にはいくらまでとか権限移譲されている金額の範囲があり、その範囲であれば工場長の判断で実行でき、その額を超える場合は、上へ上げて経営者の判断になるのが一般的かと思います。

金原： 各社とも、職責に応じた設備投資の決裁権限が定められていて、その決裁金額の範囲内で出てきた案件に対して可否判断をすると考えます。私も決裁権限の大小いずれも経験しましたが、優先順位の篩い分けの為の費用対効果で悩みました。

司会： ご自身が関わっていたプロセスプラントで、実際に経験した共通原因故障によるトラブルや事故、あるいは同様なことを見聞した事例がありましたらコメントをお願いします。

金原： バックアップ機能が作動しなかった例を本号にも記載のあった停電で紹介します。停電時にはバックアップ電源により、緊急照明が点灯します。さらにDCSは無停電電源装置が作動して、短時間の画面監視ができます。重要な回転機器にはディーゼル発電機が自動的に起動　して送電し、回転を維持することができます。DCSでは、プラントの増設時に無停電電源装置のバックアップに入れていなかったために、停電時に監視できなかったことがあります。変更時によくラインチェックすることが必要です。またディーゼル発電機は点検時に手動切り替えとするので、点検後に自動への再切換えを忘れた為に、停電時に働かなかったことがありました。確実に戻すように指導する必要があります。

今出： 機器の点検後の自動への復帰忘れは、起こりやすいエラーのひとつですね。 それが非常用やバックアップ用ですと気づきにくいということもあります。 勤めていた事業所では消火ポンプやバックアップのディーゼルエンジンの点検後は消火配管の圧力を下げて消火ポンプの作動を確認した状態で、電源を落としディーゼルエンジンに切り替わることを確認して点検終了ということにしていました。

飯濱： 私も金原さんと全く同じ経験をしたことがあります。事業所の自家発電が停止した後に、本来の電力会社からの買電に切り替わりませんでした。その時にバックアップ用のディーゼル発電機が自動起動しませんでした。点検作業をした後に切り替えスイッチを点検モードから自動切換えモードに切り替えるのを忘れていたためです。

澤： 香港のオフィスビルであったことですが、エレベーターをシングルからダブルへ取り替えた際に、モーターのサイズが大きくなって電源容量が 5 倍になりました。電源スイッチ関係は元のままにしていたために、運転時に焼き付いてしまい、従業員がエレベーター内に閉じ込められるという事態が起きました。

山本: 2017 年 2 月に埼玉県三芳町にある大規模倉庫が火災を起こし、12 日間消えなかった事故がありました。鎮火に時間を要したのは、倉庫内に設備した防火シャッターの約 6 割が機能しなかったことが原因です。この中に火災で多くの防火シャッターの電気系統がショートして、防火シャッターが機能しなかったことが挙げられています。国交省からは、電気系統の耐火性向上や一つの防火区画で火災が発生しても、その火災が他の防火区画の防火システムに影響しないような対策の基準を見直す(平成 31 年 4 月 1 日)告示が公布されました。

司会: 電気、スチーム等のユーティリティ設備は、共通原因故障を引き起こしやすいと思います。その具体的な事例や防止のために実際のプロセスプラントで、どのように対応しているかコメントをお願いします。

金原: 私のいた工場でも電力会社からの給電は本号と同じように地下抗を通しておりました。ただし電気ケーブルは単独の地下抗で、その他のユーティリティは別の地下抗を使っていました。 したがって幹線での火災がなければ問題ないのですが、例えば被覆材の劣化等によって蓄熱し、自然発火した場合は、予備の給電線も含めてダメージを受ける可能性は否定できません。日頃の点検や定期的な交換が大切です。

牛山: 電源を別々の電源系から引くいわゆる 2 系統受電は、私も樹脂工場やコークス工場などで経験がありますが、これは一つの電源系が何らかの原因で停電となっても切り替えによって設備運転を継続できるように考慮したものです。このため実際には電源を受ける受電盤以降は、機器への配電盤など共通となっているわけです。このような、共通部分でトラブルが起こるとバックアップができなくなりどうしようもなくなります。ここが安全上の盲点になっていると思います。

澤: ケーブルの火災からのプロテクションをどのようにしていましたか。例えばコントロールルームの入り口などでの扱いです。万一燃えたらどのように延焼防止を図っていたでしょうか。

牛山: 私のところでは、ケーブルラックや配線溝を何mおきかに延焼防止剤を塗布防護するようにして、万一燃えた時はその部分を取り替えるようにしていました。

三平: 消防法の電気設備に対する諸規則では、電気室などが該当する変電設備等の位置、構造、管理の中で、区画をダクト、電線管、ケーブル等が貫通する場合は、当該部分に不燃材料を十分に充填する等延焼防止上の有効な措置を講ずることとあります。以前は何もしていませんでしたが、法の改正で厳しくなって当社の最近の工事で追加した配線敷設で実施したと聞きました。

飯濱: 可燃性液体の入る原料タンク脇に消火ポンプ用の電源ケーブルが敷設されていて、コンクリートのカバーを付けて火災から防護するように設計してありましたが、塩害によりそのカバーがひどく腐食されてしまいました。

渋谷: 予備電源を別の建物に入れるなど実際にやっているのでしょうか。

牛山: 実態としてそこまではやっていませんでしたね。予備電源を別に置いても、その先で一緒になるのが通常でした。今回の事故例を教訓として、非常時でも絶対に稼働させなければならない機器は別電源による予備機を別途設置する必要があるということでしょう。設計時点でこれらの基本的な考え方を明確にしておく必要がありそうです。

山本: 電気以外のユーティリティでも同じ考え方が重要ですね。重合設備のプラントでは冷却水のユーティリティなどがそうです。一般的には、設備が入っている建屋毎に一系統または数系統の冷却水配管から枝分けして、各重合装置に冷却水を送っていると思いますが、その一系統が故障を起こすと建屋内の複数の重合装置に影響を及ぼしてしまいます。したがって、重要なユーティリティでは一系統が故障しても他の系統でバックアップできるようなシステムにしておくことや、ポンプなどの機器にはスタンバイなどをおくとかを考えなくてはいけませんね。

司会: 共通原因故障について他のご意見がありましたらお願いします。

金原: 本号で紹介のあった温度計のチェックのミスに関連して私がいた工場ではpH 計や液面計は校正していますが、温度計は校正しておりません。温度計は挙動がおかしいとすぐに分かる計器であり、また重要機器の場合は複数付いているために他の計器で異常を発見できます。さらに物質収支やエネルギー収支に基づき IT を使った異常監視システムもあり、測定異常はベテランでなくても判別できるようになってきています。

三平: 共通原因故障の事例として反応器の緊急停止用の温度計をダブルで使うケースが記載されていますが、実際にはどうでしょうか。常識的には警報器でより低い温度のアラームを発して、早く必要な処置を取るわけで

す。心配ならばアラームを H と HH の二段にすればよい。緊急用温度計のダブル化をこの事例に取り上げるのは無理があると思いました。

金原： 以前の号で申し上げましたが、教育の不十分な人によるグリースなどの注油ミスで大きな事故を起こす可能性があります。注油を委託するにしても、新人だけにやらせるのではなく、ベテランが付き添い、きちっと指導して間違いなくできる技量に到達したことを確認した上で、一本立ちさせる必要があります。また油種の間違いを防止するために、重要ポンプには使用油のシールを貼り付ける等の工夫がいります。

竹内： 共通原因故障と言うと設備異常に目が行きがちですが、元々は Failure ですので、失敗も含まれます。事故を FTA で分析していると最終的に色々な失敗が同じ原因で発生していることがしばしばあります。典型的な共通原因は教育不足で、同じ設備で次々と異なる作業員が過ちを犯して事故に繋がるケースです。安全文化と一言で片付けてしまわれがちですが、文化が悪いと言ったのでは何をどう正すべきかが分からないでしょう。安全教育と従業員の主体性が大切です。

司会： 今月のテーマは共通原因故障で、空港での火災による電源事故例などからバックアップ機能、対策費の投資判断、経験した類似トラブル事例、消火用ポンプと施設、電気設備の防火対策など広い範囲で議論が進められて、多くのコメントが寄せられました。人が関係することからあらためて教育の重要性が指摘されました。諸分野で参考にしていただければと思います。長時間のご討議をありがとうございました。

キーワード ： 共通原因故障(失敗)、バックアップ機能、停電、バイパーアルファ、消火ポンプ、
ディーゼル駆動ポンプ、被害額、 投資額、 経営者判断、 独立防護層、防火シャッター

【談話室メンバー】

飯濱 慶、今出善久、牛山 啓、金原 聖、小谷卓也、齋藤興司、澤 寛、澁谷 徹、竹内 亮、中村喜久男、松井悦郎、三平忠宏、山岡龍介、山本一己

以 上