日本学術振興会
プロセスシステム工学第１４３委員会
平成１８年度 第５回研究会議事録

１．日　時：　平成１９年２月９日（金）１３：１０～１７：００

２．場　所：　東京　弘済会館　（東京都千代田区麹町５－１）

３．出席者：４９名（順不同，敬称略）
委員長：長谷部伸治（京都大学）
委　員：大杉　健（ジャパンエナジー），轡　義則（住友化学），小西信彰（横河電機），篠原和太郎（東芝），鈴木　剛（東洋エンジニアリング），高田晴夫（三菱化学エンジニアリング），山田　明（三井化学），柘植義文（九州大学），野田　賢（奈良先端科学技術大学院大学），橋本芳宏（名古屋工業大学），渕野哲郎（東京工業大学），山下善之（東北大学），加納　学（京都大学），伊藤利昭，梅田富雄（青山学院大学），北島禎二（東京農工大学），小木曽公尚（奈良先端科学技術大学院大学），島田行恭（労働安全衛生総合研究所），武田和宏（静岡大学），殿村　修（京都大学），橋爪　進（名古屋大学），濵口孝司（名古屋工業大学），Hossam A. GABBAR（岡山大学），松本秀行（東京工業大学），矢嶌智之（名古屋大学），山本重彦（工学院大学），吉田雅俊（東北大学），大田原健太郎（クレハエンジニアリング），栗原久光（出光興産），小崎恭寿男（日揮），坂本英幸（代理：高野雅一，横河電機），重政　隆（東芝三菱電機産業システム），薄　豊文（代理：長崎一成，ジャパンエナジー），中川明浩（日産化学工業），西野由高（日立製作所），馬場一嘉（代理：安藤隆彦，ダイセル化学工業），濱村光利（代理：橘田洋一，東洋エンジニアリング），一津屋茂（三井化学），藤田宗宏（三井化学），丸山　亨（新日本石油化学），村礒　肇（代理：土井浩司，住友化学），森　正美（オムロン），米田　稔（三菱化学），関　宏也（東京工業大学），赤井　創（横河電機），石川良雄（日揮），青山貴征（三菱化学エンジニアリング），布野俊彦（日立ハイテクトレーディング）

４．研究会

テーマ：「安全設計と安全計装」

（司会：柘植義文 委員，高田晴夫 委員）

１）「独立防御階層設計に基づく安全ライフサイクルの実現」
≪講演者≫　労働安全衛生総合研究所　島田行恭 氏　（資料#1）
[概要]プロセス安全解析，独立防御層設計，安全計装設計に基づく安全ライフサイクルの実現と，プロセス安全管理システムのあり方について述べられた。

＜質疑応答＞

伊　藤：アラームやインターロックの設定値をどうやって決めていくのか？危険が進展するスピードとその危険を安全サイドにもっていく処理スピードの時間的兼ね合いから決まると思うが，そのような研究はどのような状況か？（例えば，水素防爆のためのガス検知機の濃度は随分低く，それは水素が危険に進展するスピードが非常に速いという根拠から）

島　田：難しい。防爆指針などについては，実験ベースで研究している様であるが。

米　田：本講演で話された内容は合理的で設計するときに役立つと思う。許容されるリスクというのは何で決まるか，現状は許容されるリスクになっていないのか，といった話についてどのように考えているのか？

渕　野：伊藤委員の質問こそ，この研究会で議論したい内容である。また，米田委員の質問に関連する，リスクを測れるような状態で設計されているのか，という点もこの会で議論したい 。

2）「安全計装システムの規格と適合システム紹介」

≪講演者≫　横河電機　赤井創 氏　（資料#2）

[概要] 安全計装システムが規範とする国際規格 IEC61508 の思想およびその概説と，それに適合する安全計装システムの設計骨子を紹介された。

＜質疑応答＞

北　島：安全度水準（SIL）について，許容リスクの判断はどう行うのか？

赤　井：ベンダー側としての回答になるが，許容リスクをどう捉えるかについては社会が決め手になると思う。現状のリスクを定量化するのは簡単なことではない。

石　川：海外ＰＪの事例として，IEC61508，つまり，リスクグラフに基づく SIL の決定方法を私の講演の中で紹介する。それは，人的な被害，環境の被害，生産の被害の３つのファクターでアセスメントしている。私の講演の中で，SIL の決定方法がどのくらい環境に影響するか等について説明したい。

GABBAR：SIL と PFD の話について，設計時に MTTR を考慮するだけで十分なのか？オペレータ用 HMI 上でのアラーム表示について，安全コントローラと全アラームの違いは？事例は？

赤　井：SIL は定義として与えられる。PFD 計算時，MTTR だけではなく故障率を掛けている点がポイントである。PFD はいざというときに働かない確率であるから，危険外故障に着目したときの unavailability である。それから，アラーム表示の変更は可能である。現状，２分割表示のみである。また，アラームの種類については，プロセスアラームと機器（故障）アラームがある。

3）「安全計装設計の最新動向と進め方」

≪講演者≫　日揮　石川良雄 氏　（資料#3）

[概要] エンジニアリング企業における安全計装設計の進め方を安全計装の事例を紹介しながら，安全計装の最新動向と現状の課題について述べられた。

＜質疑応答＞

伊　藤：メンテナンスバイパスあるいはフルストロークテストでは，メンテナンス周期は短くなって PFD は低くなる一方，不安全な状態を作り出していることになるように思う。どうなっているのか？　2oo3 や 2oo1 は危険なときに作動しない確率を減らすことになるのだと思うが，そういった考え方は式に考慮されているのか？

石　川：シャットダウンシステムに入っている発信器の故障と交換において，冗長化されていない場合に外してもよいのか，バイパスによって運転を続行すべきか，といった考え方はユーザによって異なる。定量的な考え方（捉え方）の仕組みがあれば教えてもらいたい。例えばあるループの SIL 1 なら SIL 1 に合った計装ループで十分であり，その際，発信器の数を定量的に捉えるために PFD の計算をするということでよいのではないか。

長谷部：SIL 検証のところで，PFD 計算の自動化は行われているのか？

石　川：計算プログラムが存在する。インターネット経由の計算も可能。

野　田：アラームマネージメントシステム設計において SIL に相当する定量的指標はあるか？

石　川：ないと思う。

4）「HAZchart 手法による安全計装設計手法の事例」

≪講演者≫　三菱化学エンジニアリング　青山貴征 氏　（資料#4）

[概要] 危険事象の発生確率とその危険事象の回避の失敗確率から最終事象の発生確率を定量的に計算することで安全性を評価する手法を用いた事例を紹介し，安全計装規格を利用した評価の考え方について述べられた。

＜質疑応答＞

重　政：分解炉の増強時，既設への影響はあったのか？

青　山：インターロックとしては単独のシステムである。冷媒で繋がっているということはない。既設を改めて評価すると，今まで見えてなかったものが見えてくる，リスクを把握して運転していたものが見えてくる，といったことがある。既設のレビューをしっかり実施し，設備投資を行って改善するという取り組みを行っている。

関　　：インターロックの仕組みが複雑になって，安全にシャットダウンはできるのか？

青　山：Emergency shutdown は安全だと思っていないし，十分な検討ができていない。

伊　藤：常時励磁・非励磁のどちらがよいのか？オーダーとしてどのくらい差が生じるのか？

青　山：基本的には常時励磁。

石　川：電磁弁などの場合，励磁と非励磁の故障率は約１桁異なる。

加　納：トップダウン決定の実際はどうなのか？

青　山：実体としては，プロジェクトから目標を皆で話して決める。

米　田：トップダウンの意味は，社会的な許容リスクをきちんと考えてやっているということをトップが判断するということである。

長谷部：機器の故障率は年月が経つと変わってくると思うが，その点を考慮しているのか？

青　山：現状考慮していない。

布　野：ハンドブックによって数値の桁が異なっている場合があるが，実際どう取り扱っているのか？　また，ユーザ間でデータの共有化はできないか？

青　山：数値のバラツキは確かにある。メンテナンスの故障率の履歴データに基づいてリーズナブルな数値かどうか判断している。データの共有化は必要だと思うし，それに賛同する。

柘　植：石川氏の結果と青山氏の結果を比較したことはあるか？石川氏の結果よりも低い方に出てくる印象を抱いたのだが。

青　山：リスクグラフでの評価はしていない。両者の結果は同じになるはずだろう。

鈴　木：青山氏の方法では，リスク評価時に HAZOP のようなものを行った後，フォールトツリーへ繋げていくが，その中にはオペレータの仕事も，普通の運転でリカバーできる確率も含まれていると思う。一方，石川氏の方法では，そういう影響は HAZOP で検討されていて SIL スタディの中では十分に見込まれていないのではないだろうか。

石　川：本来，SIL スタディは不必要な安全係数を入れないために行うものである。

渕　野：恐らく，リスクグラフの元になっている CCPS の論文では，IPL 防御層が何枚加わった上で SIL をデザインするかよってパラメータを変更するようになっていたはずだ。フォールバックできるかできないかについての考えは同じレベルだと思う。
SIL をデザインする際，IPL 2 や 3 をデザインして始めて IPL 4 が設計できるはずである。アラームが設計されて，重要アラームが設計される（オペレータインターベンションが入る）。オペレータはアラームを聞いて，原因特定を行い，アクションを起こしてフォールバックできる，というロジックがあるかどうかで，IPL が何枚あるから SIL はこれでよい，という論理が通るかどうかが決まると解釈している。今回の研究会を通して問題点等の抽出ができたと思うので，143 委員会の WS へと展開していければと思う。

配布資料：

#1：独立防御階層設計に基づく安全ライフサイクルの実現

#2：安全計装システムの規格と適合システム紹介

#3：安全計装設計の最新動向と進め方

#4：HAZchart 手法による安全計装設計手法の事例　　以上