特 集
プロセスプラントの安全，健全性とAIの活用

プロセス安全におけるHAZOPスタディとSILスタディの役割

角田 浩

The Role of HAZOP and SIL Studies in Process Safety

1. はじめに

プロセス安全に関するリスク評価手法の一つとして，定性的リスク評価手法のHazard and Operability Study（HAZOP）がある。そのHAZOPがプロセス安全の有力なツールであることが1974年に公表されて[1]，半世紀が過ぎた。1980年代半ば頃からHAZOPが欧米の化学産業で採用されるようになり，現在では世界的に化学プラントの設計・建設段階におけるリスク評価の代表的な手法として定着している。国内でも，2000年頃からHAZOPの有効性が認識され始めた[2]。

（公社）化学工学会・安全部会は，2000年12月第一回HAZOPセミナーを開催した。当初，1年に1回，3日間コースの合宿形式で始まったHAZOPセミナー（座学＋演習）は，現在では1年に2回，それぞれ2日間コースのオンラインコース（座学＋演習）で開催している。

一方，安全計装システム（Safety Instrumented System（SIS））の実装のために行うSILスタディは，世界的にはHAZOPと並んで標準的に実施すべきリスク評価のデファクトスタンダードとなっているが，国内ではHAZOPほどには認知されていない。これは，国内においてSISの実装に対する動機付けが低いことによるものと考えられる。

2. HAZOPのポイント

HAZOPはシナリオに基づく定性的リスク評価手法であり，解析チームの知見を活用して，異常の始まり（原因）から最終事象（損失）までの事象の連鎖をシナリオとして記述し，必要な安全対策が整っていることを検証する。

Hiroshi SUMIDA（正会員）
1979年　九州大学工学部造船学科卒業
現　在　レジリエント安全研究所 代表
E-mail　hiroshi.sumida@nifty.com

2025年8月31日受理

リスク評価すべき対象のプロセスシステムは，一般的に複雑であり，かつ大規模の場合もある。HAZOPでは，その複雑なシステムのリスク評価を効果的にかつ効率よく進めるために，P&IDをある特定の設計・運転意図に基づいてノードに分割し，ノード毎に解析を進める。

本稿では，HAZOPの重要ポイントである「ずれ（Deviation）」，「ずれの原因」，「システムへの影響」，「安全対策」の考え方に焦点を当てて解説する。

2.1 ずれ

HAZOPでは，意図した運転から逸脱する状況を的確に想定するために，「ずれ」という概念を用いる。「ずれ」の視点を用いて，潜在的なリスクシナリオを体系的にかつ網羅的に同定する。

あるノードにおける重要な「ずれ」に効率的に気付くために，「ずれ」を「パラメータ」と「ガイドワード」の組み合わせで表す。

「パラメータ」は，「どのような運転をしたいのか」，「何をしたいのか」という設計や運転の「意図」を表すものである。化学プラントの（プロセス）「パラメータ」は，一般的に，流量（Flow），温度（Temperature），圧力（Pressure），液面（Level），組成（Composition）（FTPLC）などで表される。FTPLCはプラントの設計・運転意図を典型的に代表するので，通常これらを用いれば，検討すべきシナリオの多くはカバーされる。さらに本来の意味を汲み取って，重要な「パラメータ」に基づいた「ずれ」を想定できると，より効率良く効果の高いHAZOPを行うことができる。

「ガイドワード」は，「ずれ」の指向性を示唆する気付きのためのキーワードであり，一般的には，No，More，Less，Reverse，As well As，Part of，Other thanが用いられる[3]。非定常操作のHAZOPでは，さらに時間・タイミングというパラメータに適用する「ガイドワード」が加わる。

パラメータとガイドワードの組み合わせのすべてが意味のある「ずれ」になるとは限らない。次頁の**表1**は，FTPLCについて一般的に有意と考えられる組み合わせの「ずれ」の例を表している。ずれの「意図しない流れ」は，「異なる方向への流れ」でもある。

著作権法により無断での転載等は禁止されています

表1　パラメータとガイドワードの組み合わせによる「ずれ」

パラメータ	ガイドワード						
	No/None	More	Less	Reverse	As well As	Part of	Other than
流れ	流れ無し	流量増	流量減	逆流	–	–	意図しない流れ
温度	–	温度高	温度低	–	–	–	–
圧力	–	圧力高	圧力低	負圧	–	–	–
液面	–	液面高	液面低	–	–	–	–
組成	–	–	–	–	組成増（汚染，混入）	組成減	異物混入

2.2　ずれの原因

HAZOPでは，一般的に単一の機器・制御機器故障または誤操作を「ずれ」の原因として，影響を検討する。これは，単一故障によって引き起こされる重大な事故事象をまず同定することが重要であるという考え方に立ち，解析を容易に行うためのものである。なお，チームの知見によって充分に起こる可能性が高いと共通認識される，あるいは過去に起こったことのある二重故障が想定される場合には，その二重故障を原因として採用することは構わない。

「ずれ」を引き起こしうる原因は，検討対象のノード内で同定することが重要である。このルールの適用は，システムへの影響を同定する際にノード外に範囲を広げて評価することと組み合わせることで，P&ID全体について漏れなくダブりなくリスクシナリオを同定する，効果の高いHAZOPを行ううえで特に重要なアプローチである。すなわち，「原因同定はノード内，影響の評価範囲はノード外を含む」という統合ルールである。

「ずれ」の原因として制御機器の故障（例：制御弁の故障全閉や全開）を想定する場合，DCS制御ループ内の最悪ケースの故障モード（非明示故障であり，自動故障検出ができない）を仮定する。この場合，当該ループのトランスミッターからの信号は誤っているために，制御弁の誤動作の結果生じるプロセスパラメータの変動をセンサーが正しく認識できず，アラームを発報できないことに留意する。

手動弁の誤操作は，原則として，定期・不定期に開閉操作をする必要のある手動弁のみを対象として「開け忘れ」，「閉め忘れ」等を想定原因とする。スタートアップ時に操作し，その後の通常運転では操作する必要のない手動弁の誤操作は，原則として想定しない。

2.3　システムへの影響

次に，下記の二つの仮定のもとに，「ずれの原因」によってシステムに起こりうる最悪の影響を同定する。

1）「ずれの原因」として仮定した，ある故障したDCS制御ループの機器以外の制御ループは正常に機能している。

2）検討対象システムに存在する安全対策（例えば，インターロック，安全弁，DCSアラームおよびアラームに基づいた運転員による対応，等）を考慮しない。すなわち，安全対策は存在しないものと仮定する。

このアプローチによって，最終事象の本質的な重大性を理解できる。この最終事象が設計条件を超える可能性がある場合には，圧力システム（機器・配管）の機能低下（封じ込め機能喪失，破損）の可能性，それに伴う化学物質の漏洩が予測され，最終的な火災・爆発・毒性影響の可能性，および死亡リスクの可能性に言及する必要がある。

DCSシステムは，ロジック・ソルバーの故障率よりも，センサーや末端の制御機器の故障率がはるかに高いことが，産業界の実績から分かっている[4]。この認識に基づいて，HAZOPにおいては，一般的に「ずれの原因」として仮定した単一故障のDCS制御ループ以外のDCSループは故障していない（すなわち，変動に応答する）と考える。

システムにおける影響を評価することは，あるDCS制御ループの故障が引き金になって起こった「ずれ」が，システムに残されている他の制御ループの応答性に任せた場合に，異なる平衡状態に落ち着くのか，あるいは配管を伝播して，または時間経過（時間的伝播）によってさらに異常拡大し，最終的にシステムにおける平衡が破綻して，健全性を損なう状態に達するかどうかを見極めることである。

影響の検討範囲は，当該検討ノードのなかに限定されず，ノードの外に及ぶこともある。

2.4　安全対策

システムへの影響を検討した後，現在すでに講じられている安全対策を同定し，その適合性および妥当性を評価する。

安全対策は，検知，防護・緩和，（運転）対応の視点で整理して評価することが重要である。

【検知】は，異常発生を早期に検出するためのものである。適切に検知できなければ，インターロックの応答も，運転員による対応も取れない。

【防護・緩和】は，発生した異常の拡大を抑制し，影響を緩和するためのものである。例えば，安全弁，インターロック，等のハードウェアによる安全対策である。

【（運転）対応】は，異常発生に際して，運転員によって取られる対応行動である。そのためには，検知によるアラー

著作権法により無断での転載等は禁止されています

ムが発報することが条件となる。アラーム発報後，異常の状況を認識し，原因を同定し，対応策を決定し，必要な措置を取るまでの時間，取った措置によって安全な状態になるまでの時間を考慮したうえで運転対応に必要な時間を見極めて，有効性を判定する必要がある。

安全対策は，ハードウェアの場合には故障（機能喪失）する可能性があるために，運転員による対応の場合にはヒューマンエラーのために，機能失敗する確率が必ず存在する。したがって，安全対策が対応すべきシナリオのリスクの程度に応じた信頼性を考慮する必要がある。

2.5　HAZOPのまとめ

HAZOPは，知見のあるメンバーがP&IDを持って集まれば，すぐに始められる。特別な解析ツールを必要としないという手軽さが，プロセス安全に寄与するHAZOPの強みである。HAZOPの手法は，方法論としては複雑ではない。むしろ，驚くほどシンプルである。シンプルであるがゆえに，リスク評価を行う際のルールを明確にし，原理・原則を忠実に守ることと，透明性を保って例外処理を行うことが，適切にHAZOPを使いこなすことに繋がる。

一般的に解析対象のシステムは複雑であり，様々な条件や制約のもとで運転されているために，原則的なHAZOPルールの適用だけでは，リスクシナリオを適切に表すことができない場合も出てくる。そのような場合には，例外処理が必要であるが，前提をどのように修正して考えたかが明確に分かるように記録することが重要である。

HAZOPを行った価値は，最終的にワークシートに記録されるシナリオの記述に集約される。したがって，上記の例外処理を含めて，ワークショップに参加していない人がワークシートを読んだ際に正しく理解できるように記録することが求められる。

HAZOPには，試験のように「これが正解である」という画一的な答えはない。ハザードを正しく同定していること，適切な安全対策による適正なリスク許容を行っていることを常に検証することが重要である。

HAZOPは使い勝手の良い有益なリスク評価手法であるが，それだけでプラントに潜在するリスクのすべてを評価できるわけではない。プラントのリスク特性を見極め，必要に応じて，他の適切な定性的または定量的リスク評価手法を活用することを考慮する必要がある。HAZOPは，それらの次に行うべきリスク評価への道標となりうる。

3.　HAZOPとSILスタディの受け持ち領域

図1は，縦軸を危害の過酷度とし，横軸を危害の発生頻度とするリスク領域において，典型的なリスク評価手法がどの範囲をカバーするのか，その受け持ち領域のイメージを示したものである。HAZOPがカバーする範囲は，広範である。SILスタディは，リスクの高い部分に対して，安全対策としてより高い信頼度を有する安全計装システムを必要とするリスクシナリオをカバーする。

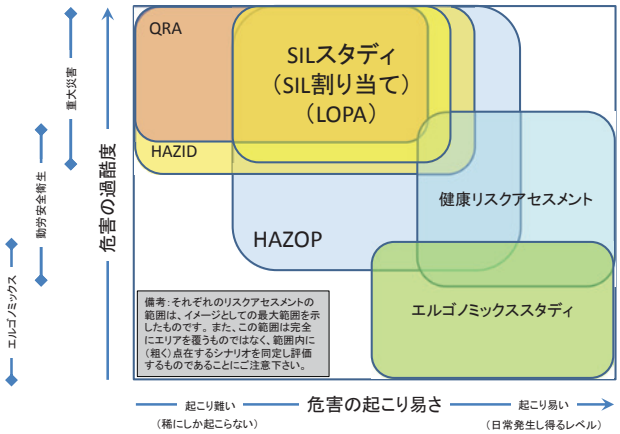


図1　リスク評価手法のカバー領域

4.　SILスタディ

（用語の定義については，末尾を参照）

SILスタディは，安全計装システムを構築するために実施される，主として「SIL割当（SIL Classification）」と「SIL検証（SIL Verification）」という二つの評価作業によって成立する複合的な検討である。

「SIL割当」は，HAZOPと同様の解析チームによるワークショップで行われるリスク評価であり，ある特定のリスクシナリオに対する固有のSIFに必要なSILを割り当てる。SIL割当に用いる手法は，規格（IEC 61511 / JIS C0511）では任意であるが，近年ではLOPA（Layers of Protection Analysis）を用いることが多い。

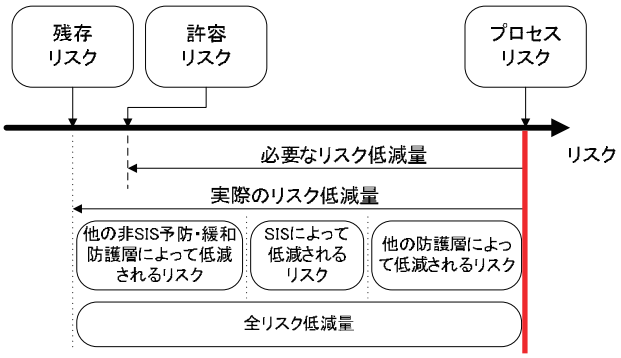
「SIL検証」は，SISがSIFに割り当てられたSILを維持できることを保証するために，ハードウェア・アーキテクチャに基づいてPFD_{avg}を計算し，機能試験の要件（試験内容および試験頻度）を決定する，特定分野専門家による解析業務である。

4.1　SIL割当

あるリスクシナリオに対する安全計装機能（SIF）に割り当てるSILは，**図2**のリスク低減の概念に基づいて，残存リスクが許容リスクを下回るように決定するものである。

SISが受け持つリスク低減の幅は，SISが具備すべき信頼度を表す。あるリスクシナリオに対して，他の独立防護層によるリスク低減が期待できず，SISが負担して低減すべきリスクの幅が大きいほど，高い信頼度のSILが必要と

著作権法により無断での転載等は禁止されています



出典：IEC61511-3, 2016, Functional Safety : Safety Instrumented Systems for the Process Industry Sector

図2　安全計装システムによるリスク低減の考え方

なる。

HAZOPで同定された安全対策はSILスタディにおける独立防護層の候補ではあるが，その安全対策が独立防護層であると認められるためには，厳格な要件（有効性，独立性，監査できること）を満足しなければならない。

4.2　SIL検証

SIFに割り当てられたSILは，次のようなSISの実装によってのみ保証される。

まず，規格要求に基づいて，要素の冗長性に関するハードウェア・フォールト・トレランス（HFT）の最少要求を検証し，割り当てられたSILに対応するSISハードウェア・アーキテクチャ案を仮決定する。次に，そのハードウェア案に基づいてPFD_{avg}を計算し，必要に応じて，要素の冗長化を行ったり，機能試験の頻度を調整したりして，割り当てられたSILを達成するためのハードウェア・アーキテクチャの最終構成，および機能試験の要件を決定する。

このように決定されたハードウェア要件は，そのSISのライフサイクルを通じて維持しなければならない。

4.3　SILスタディのまとめ

SIL割当てによってSILを決めただけでは実効性はなく，SIL検証の結果に基づいた機能をもつハードウェアをライフサイクルに渡って維持することによって初めて，SILスタディの成果が有効になる。

5.　おわりに

化学プラントの評価すべきリスクは広範に存在しうるが，その主要な範囲はHAZOPスタディがカバーできる。HAZOPを起点として，より高度なリスク評価を行うための一歩と考え，適切なリスク評価に役立ててもらいたい。

HAZOPおよびSILスタディでは，P&IDをはじめとするプラントの機密情報を取り扱い，深い専門知識と経験を必要とするため，汎用の生成AIを支援に使用することは恐らく難しい。これらのリスク評価を支援する実用的なAIシステムを構築するためには，AI開発パートナーと提携し，企業内に管理されたAIシステムを構築し，データの隔離とセキュリティを確保したうえで，機密情報であるエンジニアリング情報をAIに読み込ませ，過去のHAZOPおよびSILスタディを学習させることが必要である。

SILスタディに関する用語の定義：

SIS（安全計装システム）	Safety Instrumented Systemの頭字語であり，「エス・アイ・エス」と読む。SISは，1以上のSIFを実装する計装システムであり，センサー，ロジック・ソルバーおよび操作端（例えば，遮断弁）の組み合わせで構成される。
SIL（安全度水準）	Safety Integrity Levelの頭字語であり，「シル」と読む。SILは，SIFに対して割り当てられる信頼度であり，プロセス産業セクターでは，作動要求発生時平均失敗確率（Average Probability of Dangerous Failure on Demand）（PFD_{avg}）に基づいて3段階に区分される。
SIF（安全計装機能）	Safety Instrumented Functionの頭字語であり，「シフ」と読む。プロセス産業セクターにおけるSIFは，一般的に安全計装防護機能である。

参考文献

1）Lawley, H. G.：*Chemical Engineering Progress*, **70**(4), 105-116(1974)
2）高木 伸夫：安全工学, **44**(1), 31-36(2005)
3）Center for Chemical Process Safety(CCPS)：Guidelines for Hazard Evaluation Procedures, 3rd ed., John Wiley & Sons, inc., New Jersey, USA, 118(2008)
4）化学工学会・安全部会監訳：重大ハザードのリスクを下げるLOPA －防護層解析－, 丸善出版, 91(2022)

著作権法により無断での転載等は禁止されています