連　載

プラントの安全性評価

第 4 回　システムの安全性解析

日本防災システム協会 副幹事長
松岡 俊介

これまで潜在危険性の特定手法として活用できる HAZOP、What-If 等 6 つの方法について述べてきた。今回は、システムの安全面における弱点の解析や、システムの機能喪失や事故・災害事象の発生頻度の推定などに用いられ、システム安全性解析手法と呼ばれる以下の方法について、それぞれの特徴、適用上の留意点等を述べる。

・フォールトツリー解析（FTA）
・イベントツリー解析（ETA）
・原因結果解析（CCA）

なお、前回紹介した故障モード・影響解析／故障モード・影響・重大性解析（FMEA/FMECA）もシステム安全性解析手法として活用されている。

フォールトツリー解析（FTA）

フォールトツリー解析（FTA）手法は、1972 年～ 1975 年、米国 M.I.T（マサチューセッツ工科大学）のラスムッセン教授の指導の下に進められた商業用原子炉の定量的リスク解析（第 3 回原稿の脚注(4)を参照）のなかで確立された確率論的リスク評価の中核的な手法として生み出され、今日では、原子力分野に限らず化学産業ほか様々な分野で活用されている。

FTA は、システムにとって望ましくない事柄、事象（トップ事象、頂上事象）を取り上げ、その原因、要因を演繹的に掘り下げて行き、根本的な原因、要因（基本事象）を特定し、それらの因果関係を論理記号（AND ゲート、OR ゲートなど）を用いてツリー状（フォールトツリーという）に表現する手法である。論理演算により因果関係を整理した後、基本事象の発生頻度や発生確率を与えることによって、トップ事象の発生頻度を求めることが出来る。

FTA で作成されるフォールトツリーの簡単な例を**図 4** に示す。火災はその 3 要素である燃料、酸素および着火源がすべて揃った時にはじめて起るが、ガソリンスタンドで車に給油している間は、燃料については給油ノズルからガソリンが燃料タンクに注がれガソリン蒸気が給油口から漂い出ており、酸素は空気としてもともと存在しているので、唯一着火源が発生すれば、給油中の車から出火することになる。

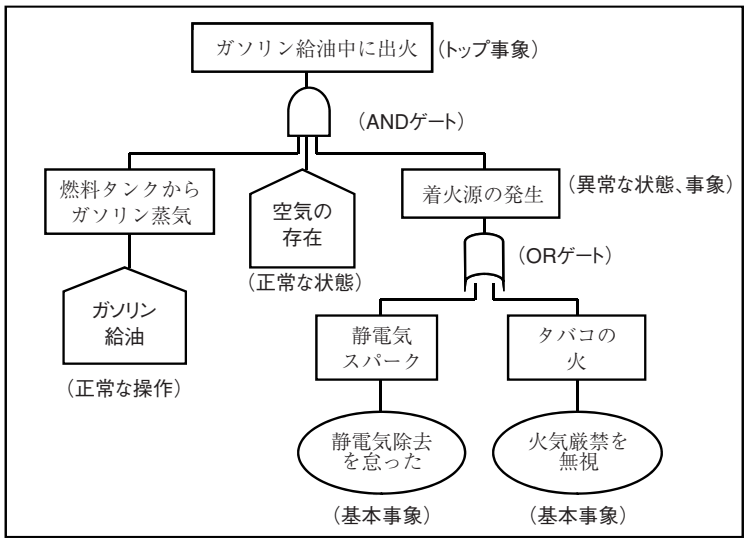


図 4　ガソリンスタンドでの給油中の火災事故のフォールトツリー

表 10　フォールトツリーの論理ゲートおよび事象記号

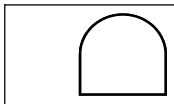
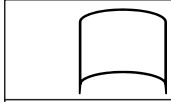
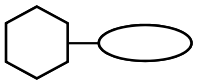
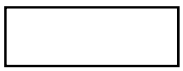
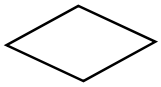
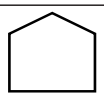
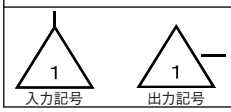
	ANDゲート	論理積。ゲートの下位にある入力事象のすべてが成立したとき、ゲートの上位の事象が出力される。
	ORゲート	論理和。ゲートの下位にある入力事象のいずれか 1 つが成立したとき、ゲートの上位の事象が出力される。
	抑制ゲート	下位の入力事象が楕円のなかに記述された条件を満足する場合のみ上位の事象が出力される。
	トップ事象 中間事象	上記の論理ゲートを用いて下位事象に展開すべきフォールト事象。枠内に事象の内容を簡潔に記述する。
	基本事象	それ以上の展開を必要としない最下位の事象。通常、発生頻度または発生確率が分かっている事象。円内に事象の内容を簡潔に記述する。
	省略事象 ダイヤモンド事象	解析の範囲外か情報の不足により意図的にそれ以上の展開を中断する事象。枠内に事象の内容を簡潔に記述する。
	外部事象 ハウス事象	境界条件として存在する事象または条件。システムの正常な状態または操作。枠内に事象の内容を簡潔に記述する。
	転移入力記号 転移出力記号	二つのフォールトツリーを連結するための記号。三角形内に数字または記号を示す。同一ツリーの繰り返しを避ける場合にも使用する。

図 4 では、着火源として給油中の人体からの静電気の放電スパークとタバコの火を取り上げ、それぞれ「(給油前の) 静電気除去を怠った」、「火気厳禁であることを無視した」という人的ミスを基本事象として特定している（厳密には静電気スパークによる着火が起るのは、人体が十分帯電しているのに静電気除去を怠ったため、ガソリンの最小着火エネルギー以上のエネルギーを放出する火花放電がガソリン蒸気の付近で発生した場合)。

このフォールトツリーから、給油前の静電気の除去および火気厳禁の不履行がトップ事象である火災の発生の直接原因であり、逆に言えばこれらの厳守が火災防止の基本的対策であることが分かる。

このフォールトツリーでは AND ゲートと OR ゲートという FTA の代表的な論理ゲートが使用されているが、その意味をほかの論理ゲートや事象記号と合わせ**表 10** に示す。

FTA は、通常以下の手順に沿って進める。

① トップ事象の定義、境界条件など前提条件の設定
② フォールトツリーの作成
③ 最小カットセット（Minimal Cut Sets）の特定
④ トップ事象の発生頻度の推定
⑤ システムの弱点箇所の特定
⑥ システムの改善案の検討

(1) トップ事象の定義、境界条件など前提条件の設定

まず、解析対象のシステムにとって避けるべき危険状態をトップ事象として設定し、「どこで（どの機器で）いつ（システムがどんな状態のとき)、何（どんな危険状態）が起った」のように明確に定義する。FTA の前に HAZOP や What-If などで潜在危険性の特定分析が行われていれば、その結果を活用する。

トップ事象とともに、システムの範囲・境界、解析の深さ、システムの初期状態、解析から除外する事象、存在する事象・条件など解析の前提条件を設定する。

(2) フォールトツリーの作成

因果関係の推論によってトップ事象を発生させる必要十分な直接的要因（フォールト事象）を第 1 次中間事象として特定する。中間事象のどれもがトップ事象の直接要因となる場合は OR ゲートを用いてトップ事象と中間事象を結び、トップ事象の発生にすべての中間事象が必要な場合は AND ゲートで結ぶ。

第 1 次中間事象のそれぞれについて、同様に必要十分な直接的要因を第 2 次中間事象として特定し、OR ゲートまたは AND ゲートで連結する。この展開作業をすべてのフォールト事象が基本事象あるいは省略事象に到達するまで続ける。

フォールト事象は、機器故障事象とシステム故障事象に分けられる。機器故障事象は一次故障（機器自体の欠陥、寿命による不調）、二次故障（設計条件を超える想定外の条件下で起こる不調）およびコマンド故障（指令元の機器の故障による誤作動）に展開し OR ゲートで結ぶ。一次故障は基本事象であり、二次故障およびコマンド故障は中間事象としてさらに一次故障まで展開する。

システム故障事象はシステムの異常状態であり（たとえば異常な圧力上昇）、その直接要因を洗い出し OR ゲートまたは AND ゲートで結ぶ。

なお、OR ゲートも AND ゲートもゲートどうしを直接結ぶことはしない。ゲートの入力事象および出力事象は、常に適切に記述されたフォールト事象とする。

(3) 最小カットセット（Minimal Cut Sets）の特定

OR ゲート（論理和）および AND ゲート（論理積）の演算によって作成されたフォールトツリーを分解すれば、すべての中間事象が消去されてトップ事象が基本事象の組み合わせの集合として表される。この基本事象の組み合わせのひとつひとつをカットセットと呼ぶ。カットセットからトップ事象の発生に関係しない（あるいはかならずしも必要ではない）基本事象を取り除いたものを最小カットセット（MCS）という。カットセット群から MCS を得るためには、以下のブール代数即を用いた論理演算を行う（A、B ：基本事象）。

① A × A ＝ A
② A ＋ A ＝ A
③ 1 ＋ A ＝ 1
④ A ＋ AB ＝ A （1 ＋ B） ＝ A

各 MCS は、トップ事象を引き起こすための最小限必要な基本事象（機器故障、誤操作および環境条件）の組み合わせであり、トップ事象の発生条件である。この MCS のリストは、後述するようにシステムの安全性評価の重要な情報となる。

(4) トップ事象の発生頻度の推定

まず、各 MCS を構成する基本事象の発生頻度または発生確率のデータを収集して MCS の発生頻度を計算する。MCS を構成する基本事象は、一つがある発生頻度をもつ起因事象であり、残りはすべてある発生確率をもつ確率的事象である。たとえば、予備機をもつポンプシステムの故障を含む MCS（主機と予備機の同時故障停止）の場合は、主機については運転中の故障停止の発生頻度を与え、予備機については要求時の不作動確率（アンアベイラビリティ）を与える。それらを乗じて MCS（主機と予備機の同時故障停止）の発生頻度を求める。すべての MCS の発生頻度を求めた後、それらを合計すればトップ事象の発生頻度が得られる。

(5) システムの弱点箇所の特定

MCS のリスト、各 MCS の発生頻度およびトップ事象の発生頻度が得られると、システムのどこに弱点があるか分析することが出来る。発生頻度の計算を行わなくとも、定性的な評価は可能である。構成基本事象数の少ない MCS は、構成基本事象数の多い MCS に比べ防護階層が薄く発生頻度が高いと推測できるからである。

発生頻度計算を行った場合は、各 MCS の発生頻度がトップ事象の発生頻度に占める比率を求める。この比率が高い MCS がそのシステムの弱点箇所を示しており、トップ事象の発生頻度が許容レベルを超えている場合は改善すべき重点対象となる。

(6) システムの改善案の検討

システムの改善案は、上記の弱点解析から容易に求めることが出来る。すなわち、構成基本事象数の少ない MCS あるいは発生頻度比率の高い MCS について追加の防護対策（冗長化など）を検討する。通常、基本事象数が 3 つまでの MCS が対象となる。4 つ以上になれば発生頻度はかなり低下すると考えてよい。発生頻度比率の高い MCS については、追加の防護対策案を検討しそれによりトップ事象の発生頻度および比率がどの程度低下するか再計算する。

以上述べてきたように、HAZOP や What-If 等による潜在危険性の特定作業を行った後、特に重要な危険事象について FTA を適用してシステムの安全性を評価すれば、より効果的な改善検討が可能になると期待できる。

イベントツリー解析（ETA）

イベントツリー解析（ETA）手法も、FTA とともに確立された確率論的リスク評価手法のひとつである。ただし、演繹的な推論アプローチの FTA とは異なり、ETA は帰納的な推論プロセスである。すなわち、引き金的な起因事象（システムの異常状態）を出発点として、システムに組み込まれたいく

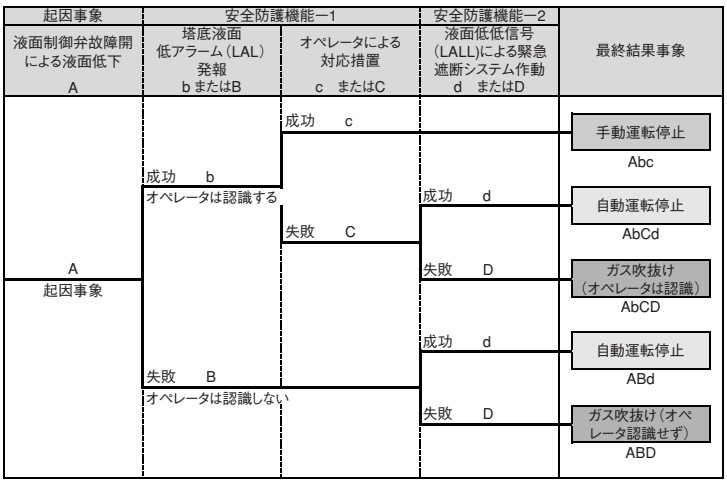


図５　蒸留塔の塔底からのガスの吹抜けのイベントツリー

つかの安全防護機能バリアの成功、失敗の分岐を経て、最終的な結果事象（事故なし、軽微な結果、重大な結果など）に到達する事故シーケンスを特定する。

例題として、高圧で操作される蒸留塔の塔底液面コントロールシステムを考える。もしこの液面制御弁が故障して閉まらなくなったら、高圧のガスが下流システムに吹き抜けて過圧によって破裂する可能性があるので、安全防護機能として液面低アラーム（LAL）および液面低低信号（LALL）による緊急遮断弁が設置されている。

このシステムにおいて「液面制御弁故障開による液面低下」を起因事象とするイベントツリーを**図５**に示す。最終結果事象として、「手動による運転停止」、「自動運転停止」、および「ガス吹抜け」の３つの事故シーケンスが特定されている。緊急遮断システムの失敗による「ガス吹抜け」が最悪の結果であるが、液面低アラーム（LAL）が正常に作動した場合、オペレータはガス吹抜けによる下流システムの破裂を回避あるいは緩和する対応の余地が残されている。液面低アラーム（LAL）が正常に作動しなかった場合、誰も気づくことなく突然下流システムの破裂に至ることになり、より重大な結果となる。

この例題のように、ETA は多重の安全防護機能をもつ複雑なシステムにおいて、ひとつの起因事象から起りうる事故シーケンスをすべて特定することが出来る。特定された各事故シーケンスの原因の解析には FTA を用いる。

ETA の手順を以下に示す。

① 起因事象および安全防護機能の特定
② イベントツリーの作成
③ 事故シーケンス MCS の特定
④ 発生頻度の推定
⑤ システムの改善案の検討

(1) 起因事象および安全防護機能の特定

起因事象は、例題に示したようなプロセス異常であり、機器の故障や誤操作が選ばれることもある。安全防護機能は、アラーム、オペレータの対応、自動運転停止システム、安全弁、緊急冷却システム、事故影響緩和システム（除害システム、封じ込めなど）などが考えられる。HAZOP や What-If が実施されていれば、特定された重大な潜在危険性とそれらに対する安全対策を対象に選定することが出来る。

(2) イベントツリーの作成

まず、ページの上方に起因事象と、関連する安全防護機能の応答を時系列的に配列する。次に最初の安全防護機能が事故の進展に関係するかどうか判断し、関係する場合は成功と失敗のパスに分岐する（成功パスを上に、失敗パスは下に）。関係しない場合は直接、次の安全防護機能に進む。すべての安全防護機能について同様の分岐を続け、最終的な結果事象を簡潔に記述する。

(3) 事故シーケンス MCS の特定

ETA の事故シーケンス MCS は、FTA と同じ方法で分析できる。上記例題の事故シーケンスについては、以下の通りとなる（カッコ内は重要度ランク）。

「手動運転停止」(I) ： A b c
「自動運転停止」(II) ： A b C d ＋ AB d
「ガス吹き抜け」(III) ： A b CD ＋ ABD

小文字の英字は成功事象であるのでこれを取り除くと FTA における MCS と同じになる（成功事象は MCS には含まない）。

(4) 発生頻度の推定

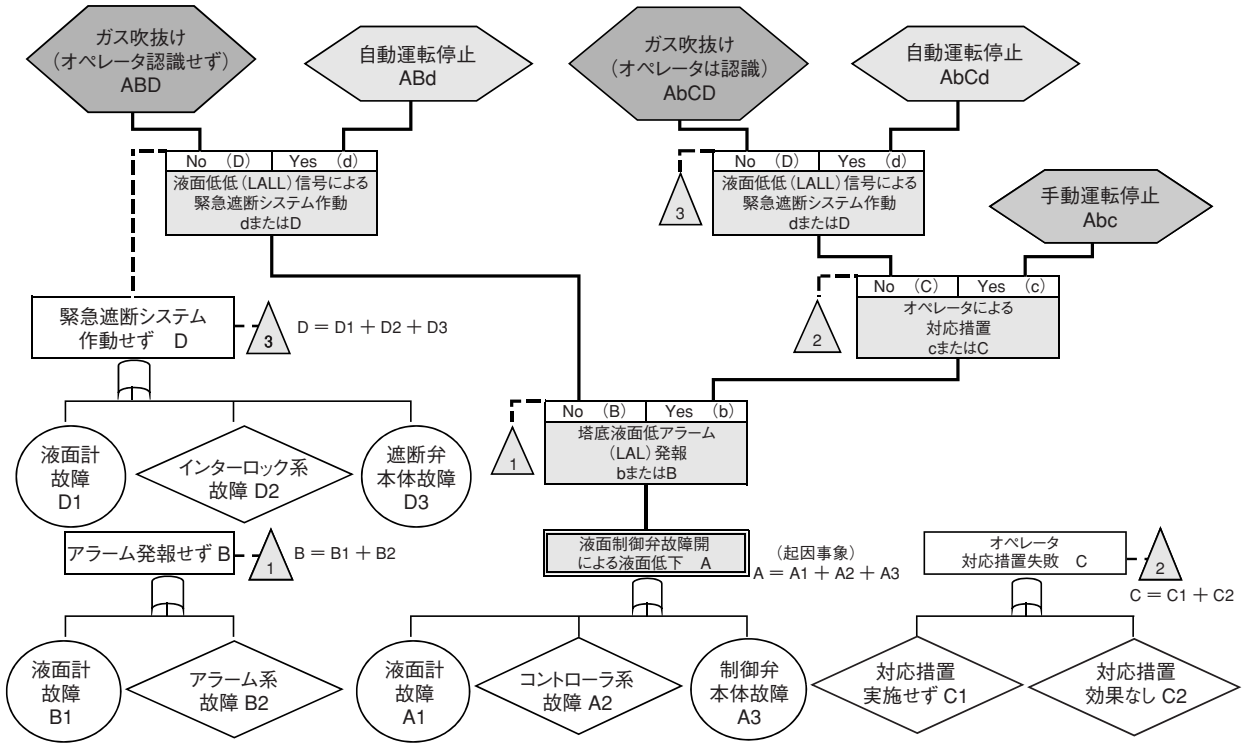
起因事象の発生頻度と安全防護機能の成功／失敗の分岐確率を設定すれば、各事故シーケンスの発生頻度を計算することが出来る。

(5) システムの改善案の検討

最も重大な事故シーケンス（例題ではガス吹抜け）の発生頻度が許容レベルを超える場合は、追加の安全防護機能案（冗長化など）を検討し、それによりイベントツリーを修正し、修正 MCS の発生頻度を再計算する。

原因結果解析（CCA）

原因結果解析（CCA）は、FTA と ETA を組み合わせた手法で、イベントツリーによって事故シーケ



（注）液面計は制御系、インターロック系およびアラーム系それぞれに専用と仮定

図 6　蒸留塔の塔底からのガス吹抜けの CCA 図

ンスを展開させながら、同時に起因事象および各安全防護機能の失敗事象をトップ事象とするフォールトツリーを作成するものである。したがって、CCA を実行すれば、すべての事故シーケンスが特定され、同時に各事故シーケンスの原因解析を行うことが出来る。フォールトツリーの部分があまり大きくなく簡単な場合にはよく用いられる。

ETA の例題として挙げた蒸留塔の塔底からのガス吹抜けについて作成した CCA 図を**図 6** に示す。起因事象（二重ボックス）からスタートして、各安全防護機能を Yes/No 付きのボックスで表示し、最終結果事象は図の上方に亀の子ボックスで表示する。ここまでは、イベントツリーを裏返しにしてヨコからタテに置き換えたのと同じであるが、CCA の特徴は、起因事象および安全防護機能の失敗事象に、それぞれをトップ事象とするフォールトツリーが連結されることである。フォールトツリーによって起因事象および安全防護機能の失敗事象は基本事象または省略事象にブレークダウンされる。これにより、各最終結果事象の事故シーケンスは、基本事象および省略事象からなる MCS で表現することが出来る（成功事象は取り除く）。そして、各 MCS に含まれる事象の数とタイプからそれぞれの重要度ランクが決定される。

CCA の手順は以下の通りである。

① 起因事象の設定（FTA で解析したトップ事象または ETA の起因事象を設定）
② 安全防護機能の特定および事故パスの展開（ETA と同じステップ）
③ 起因事象と安全防護機能の失敗事象の原因解析（FTA とおなじステップ）
④ 事故シーケンス MCS の特定と評価（最初の事故シーケンスの重要度評価は ETA と同じ。次の MCS の特定と重要度評価は FTA と同じ）
⑤ システム改善案の検討

繰り返しになるが、以上に述べた FTA、ETA および CCA は、HAZOP や What-If などによってプラントの潜在危険性を洗い出したあと、特に重要な危険性（事故事象）について適用することが薦められる。それにより事故事象の根本的な原因となる機器の故障や誤操作を特定するとともに、事故事象の最終的な結果に至るプロセスを事故シーケンスとして特定し、システムの弱点箇所の把握と改善策の検討を行うことが出来る。これらの解析、検討は、発生頻度計算を行わず定性的に実施するだけでも、一定の結果を得ることができる。