◇特集：安全・安心◇

安全工学の現状

松岡　猛＊

1．はじめに

安全工学とは文字通り解釈すると安全を確保するための工学の学問分野ということができる。

その場合の「安全」には、人間との係りが必ず条件となっている。例えば、人跡未踏の大平原で河川の氾濫があったとしても直接安全にはかかわってこない。一方、人間生活にかかわる事象は非常に多岐に亘っている。生産活動、交通、住居、自然現象、レジャー活動、医療等々とある。これらの場での状況を考える必要があり、通常「安全」はどんな危険も存在しないという否定形で表され具体的に指定できないため、「リスク」を経由して考えられている。良く考えてみるとこれらの活動の場ではリスクが必ず存在するため、「リスクが受け入れ可能な状態」が「安全」ということになる。それ故、「絶対安全」は存在しないことが現在では広く認知されて来ている。

これら各場面において安全を確保するための技術は、それぞれ個別的な技術となる場合が多い。しかし、各分野の安全の技術や考え方を整理し構造化することで、安全の知識をよりいっそう明確にできる。安全確保のための普遍的な考え方、技術をもとに学問分野を構築しているのが安全工学といえる。

バルブを日頃取り扱っている読者にとっては「安全」という語から、機器・部品の機能劣化、故障、誤動作をいかに抑えるかということがすぐ頭に浮かぶことと思う。これらの不具合の発生の程度を正しく評価し、機器の信頼度を上げることが安全確保に直結する。しかし、単一の機器でなく複数の機器で特定の機能・目的を持ったシステムが作られている時には単一機器の故障では安全が損なわれない設計となっている場合が多くある。逆に、システム動作が高度・複雑化されており構成機器には何ら故障・不具合が発生しなくても、設計者の意図を超えた動作状況により事故を引き起こす場合も発生している。

＊宇都宮大学

本論では、工学システムを対象とした安全確保／安全性評価のための工学技術について説明していく。

2．確率論的安全評価と決定論的安全評価

「1．はじめに」で述べた様に、安全はリスクを経由して考えられている。それ故、近年確率論的安全評価（PSA：Probabilistic Safety Assessment）という考え方が導入されてきている。

従来の立場は、決定論的方法と言われ、安全確保のための工夫がどの様に機能するかを解析し、安全が確保されていることを確認する方法と言える。使用経験の蓄積により安全性が判断され、安全確保のための様々な工夫が積み上げられていくことになる。

しかし、完全・無欠な工学システムというものは存在しないという立場からは何重にも整備された安全確保の設備でも次々に機能しなくなる多重故障を評価しなくてはならない。システムを構成する機器の故障・破損、システムを取りまく状況の発生を確率的な事象と捉え、システムにとり不都合な事態（事故）が発生する確率を定量的に評価するのが確率論的安全評価である。

ここで、確率論的な事象の捉え方を単一の機器・構造物について説明する。図1は、ある機器・構造物の耐力（Ls）とそれに加えられる外力・荷重の強さ（Ld）の関係を模式的に示したものである。こ

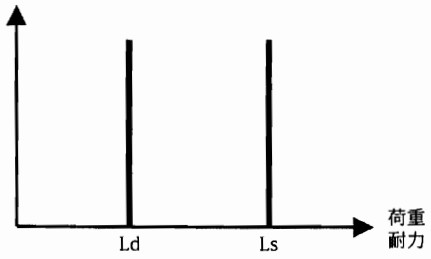

図1　荷重と耐力の関係

こで、外力・荷重とは機器等の故障・破損形態に対応した種々のストレス、例えば衝撃力、荷重、圧力、振動、高温環境、腐食環境…等を総称している。それ故、耐力はそれらに対抗し得る強度・性質等を総称したものである。図1では、耐力も荷重も明確な値が判明しており、耐力が荷重を上回っている。この様な場合に機器・構造物の故障・破損は絶対に発生しないと判断するのが決定論的な方法である。実際には、決定論的な方法においても荷重は定まった値を取るのではなく、条件により種々の値を取り得るので安全係数というものを2.0～5.0～7.0と設定し、想定される最大荷重の2～5～7倍の大きさを耐力として設計する事が通常実施されている。これにより設計された機器・構造物の故障・破損は発生せず安全は確保できると判断する。

しかし、実際に製作された機器等には製造過程における品質のばらつきが避けられない。これを考慮すると図2のLsに示す耐力の分布が考えられる。一方荷重にもLdの分布があるがこの図に示す様に二つの分布が十分分離している場合には、機器の故障・破損は発生せず安全は確保できると判断できる。決定論的な判定においてもLs、Ldの分布を認めていないわけではない。分布が存在するからこそ安全係数を設定するのであり、Ls、Ldが十分距離を置いて存在しかつ、その距離に比較して分布の巾が狭ければ図1に近いという暗黙の了解のもとに安全性を評価している。

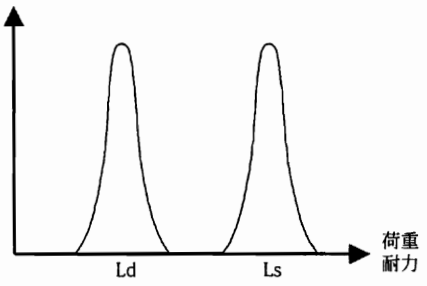

図2　荷重と耐力に分布がある場合

これに対し、荷重の性質、物質の性質、製作コストの制約、分布巾に関する情報・知識の欠如等によりLs、Ldの分離が十分に達成できず図3のように重なり部分が生じてしまう事が避けられない場合に確率論的な評価が必要となってくる。荷重が耐力を

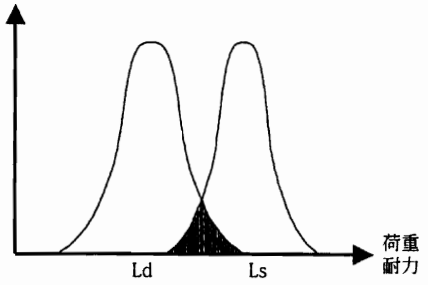

図3　荷重と耐力の重なり

上回る場合に故障・破損が発生するので、その発生確率を評価する。安全が十分確保されているかどうかは故障発生確率値が判定値・基準値に比較して小であるかどうかによって判断される。

この様に考えると、確率論的な方法では従来明確には意識していなかった確率的な分布をはっきりとした形で取り扱い、より深いレベルの検討を行っていると言える。それにより決定論的な方法では無視していた様な故障・破損の可能性までも定量的に評価するとともに、逆に故障・破損が必然で従来採用されていなかった技術も、その事象を定量的に評価し、安全対策における検討対象として扱う事も実施している。

確率論的安全評価では、被害発生の可能性の程度を明らかにする。そのための種々の解析方法が開発され使用されてきている。以下の各章においてそれらの説明を行なう。

3．システムの分析

安全解析の第一歩は解析対象の工学システムに起こり得る不具合・故障・事故を調べ上げることである。そのために良く用いられるのがFMEA（Failure Modes and Effects Analysis：故障モード及び影響評価法）[1]である。機器の故障モードとその故障が他の機器、系統に及ぼす影響を抜け落ちなく徹底的に調べる方法である。各機器についてその本来の機能、故障モード、故障のメカニズム、系への影響、故障の検出方法等の項目を徹底的に調べ表の形にまとめる。FMEAの結果できる表の一例を表1に示す。大規模システムの場合は100ページ以上にも亘る表となる。これは定性的な解析方法であり、従来の決定論的解析においても多く実施されてきている。単独では定量的解析とはならず、後述するフォール

表1　FMEA ワークシートの一例

システム名称		エスカレーター			システム・ブロック線図		エスカレーターの安全性評価ページ 12 参照			
日付		2010 年 1 月 1 日			検討／修正／最終確認		MY			
解析者氏名		MY								
装置名	機器名	機能	故障モード	故障の原因	故障の影響		故障検出	是正処置	故障影響の重大性	備考
					局部的影響	最終的影響				
欄干	移動手すり	踏段と同一方向に同一速度で移動する。	動作不良	手すりの摩耗、表面に水や油等が付着	手すりがスリップ	正常運行不可	動きに異常	部品取替え、清掃	大きな影響	ただし、乗客が大勢乗っているときに発生した場合は大事故のおそれありなので「危険な影響」～「破滅的影響」
	内側板	踏段側面のパネル。	破損	劣化	影響なし	影響なし	目視	部品取替え	小さな影響	正しい乗り方であれば影響はない
	デッキボード	進行方向に連続した細長い板状の化粧材。	破損	劣化	影響なし	影響なし	目視	部品取替え	小さな影響	正しい乗り方であれば影響はない
	スカートガード	踏段とわずかな距離を保っている。	破損	劣化	影響なし	影響なし	目視	部品取替え	小さな影響	乗り方によっては、挟み込みが起こりやすくなるので「危険な影響」
駆動装置	制御盤	駆動機に電力を供給し、運転・停止の指示を出している。	動作不良	基盤の破損、結線不良、劣化	駆動機に電力が供給されない	運行不能	移動停止	修理、取替え	大きな影響	
	駆動機	駆動チェーンを介して、エスカレーターを駆動させている。	停止	電動機の故障、減速機の故障	運動停止	運行停止	移動停止	修理、取替え	大きな影響	
	駆動チェーン	電動機と直結して、その動力をスプロケットに伝えている。	チェーンの伸び	チェーンの劣化、過剰な負荷	不安定な動作	運行停止	移動停止	部品取替え	大きな影響	ただし、安全装置が故障していた場合は大事故の恐れありなので「危険な影響」～「破滅的影響」
			チェーンの破断	チェーンの劣化、過剰な負荷	運動停止	運行停止	移動停止	部品取替え	大きな影響	ただし、安全装置が故障していた場合は大事故の恐れありなので「危険な影響」～「破滅的影響」

ト・ツリー解析や、イベントツリー解析における起因事象の選定に先立つ予備的な解析として実施されている。

同様な解析法に FMECA（Failure Modes Effects and Criticality Analysis）[2]がある。各故障がシステム運用に及ぼす影響を明らかにし、安全性に致命的となる単一の故障個所を決定し、故障影響の致命度と発生確率により各故障に順位をつけるもので、一種の定量的解析になっている。

FMEA に類似した方法として HAZOP（Hazard Operability：ハザード及び運転可能性解析）[3]がある。これは 1970 年代はじめにイギリスの ICI 社で開発された定性的危険度評価手法である。化学プラント等の流体、物流、信号、情報の流れや行動、作業手順のシーケンスの異常に着目して、想定される通常状態からのズレ（異常）を見出し、FMEA と同様な表を作成し、異常のもととなっている原因とシステムへの影響、対策をまとめる。

HAZOP と FMEA の違いは単方向であるか双方向であるかという点にある。FMEA は、部品の故障から出発してシステムへの影響を調べるという一方向型である。HAZOP はシステム内の状態量のズレ(異常）から出発して、ズレの原因の方へさかのぼるとともに、システムへの影響波及（結果）へと双方向に解析を進める手法である。

解析対象のシステムの論理的なつながりをモデル化して表現する方法として信頼性ブロックダイアグラム[4]がある。これは構成機器あるいは機器の集合（サブシステム）まで分解してそれらをブロックで表現し、系の動作経路に従ってブロック間の関係を結んだ図形式の表現である。図 4 は信頼性ブロックダイアグラムの簡単な例であり、ユニット B,C,D が一群となり、それと並列にユニット A が置かれている。同一ユニット E が 3 個存在し、2 out of 3 系

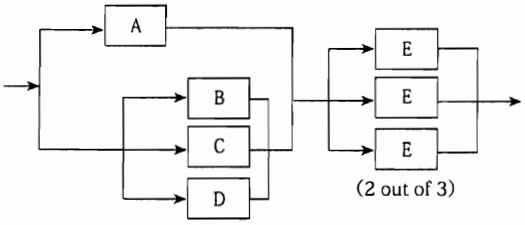

図4　信頼性ブロックダイアグラムの一例

を構成しておりユニットA、B、C、Dと直列に配置されている。この表現自体は定性的な分析といえるが、各ユニットの動作・故障確率値等を基に系全体の信頼度を別途計算することが可能となる。

4．システムの評価

確率論的安全評価では、前章の方法により分析したシステムを定量的に評価する必要がある。そのために主としてイベント・ツリー（Event Tree）解析手法[5]とフォールト・ツリー（Fault Tree）解析手法[6]の組み合わせが多く用いられる。

大規模システムが高度な安全防護系を備えている場合は、突然事故が発生するわけではなく、何か発端となる不具合が発生し、偶発的な故障の重なりにより事故に至る。この状況を定量的に評価するために開発されたのがイベント・ツリー解析である。

図5に示す様なツリー構造を持ったのがイベント・ツリーである。左端に起因事象（発端となる不具合）が置かれ、順次各種安全防護系／安全系統を表す見出し（ヘディング）が上部に書かれている。各ヘディングにおける機能の成否に対応して事故のシーケンスが上下に分岐して行く。この様にして、論理的に起こり得る全ての事故シーケンスを同定することができる。

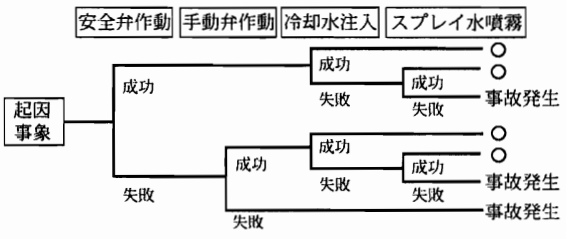

図5　イベント・ツリーの一例

これにより、システム中の安全防護系の異常・故障の様々な組み合せを体系的に評価することが可能となる。システムが大規模となると事故シーケンス数は何百～何万となる。

このイベント・ツリーにより得られる各事故シーケンスを定量的に評価するためには、起因事象の発生頻度と各ヘディングの機能の成否に対応したシステムの成功／失敗確率を求める必要がある。ヘディング機能の失敗確率値を求めるためにシステム信頼性解析が用いられ、その一種であるフォールト・ツリー（FT）解析が多く用いられている。

FTはシステムの故障を構成機器の故障に分解して分析する解析手法で、図6に示す様なツリー構造を持っている事からフォールト・ツリー（故障木）と呼ばれている。

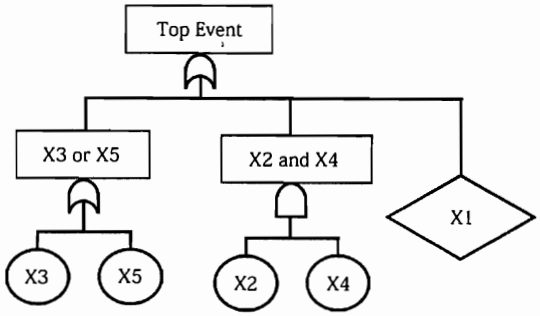

図6　フォールト・ツリーの一例

フォールト・ツリー解析手法は、航空機産業界における40年以上の経験及び1975年のラスムッセン報告[7]以来の原子力産業界における使用経験がある。

フォールト・ツリー（FT）は複数の機器から構成されたシステムに起こる望ましくない事象（頂上事象）をそれぞれの機器の故障、誤動作等のAND、ORの様な単純な論理関係で結合して表現したものである。

頂上事象を分解する場合、第一段階ではできるだけ一般的な分類に基づき分解する。分類された事象は通常長方形で囲まれた中間事象として表現され、より具体的・詳細な事象の組み合わせより成り立っている事を意味している。

さらに、中間事象をより具体的・基本的な事象により分解していくと、各枝の末端で円により表現された基事象か、ダイアモンド形で表現された未分解事象にたどり着く。基事象は故障、破損、誤動作等の基本的事象で物理モデル、統計データ等から発生

確率のデータが入手可能か、推定が容易な事象である。

FTが大規模、複雑なものとなると手計算で定量評価をすることは不可能となるため、種々の計算プログラムが開発され[8]、それぞれの目的に応じて使用されている。

FT解析ではある特定の時刻におけるシステムの故障確率を算出することは可能であるが、時間推移によるシステムの信頼度変化、動的な挙動を示すシステムの解析は不可能である。そのため、GO-FLOW手法[9]のようなシステム信頼性解析手法が開発されている。

GO-FLOW手法は成功確率を追うシステム信頼性解析手法であり、解析対象を構成する機器の故障、動作を事前に用意されている標準オペレータを用いモデル化する。それらの機器間の結合関係は信号線を用いて表現する。その際、AND、OR、NOT等の論理的結合を表現する論理オペレータも用意されている。解析対象システムのモデル化の結果、GO-FLOWチャートと呼ばれる、信号線とオペレータから構成される図が作成される（図7）。

オペレータの動作・故障に対して動作／故障確率をデータとして与え、オペレータの定義に基づき信号を処理していくことにより、最終的に系の動作／不動作確率を求めることができる。

GO-FLOW手法は時間経過にともなう信頼度の推移、要求されるシステム動作成功基準が変化する場合、補修による機器故障の復旧の効果、システム動作状況が機器状態・プロセス状態等により変化する動的システムの解析等の種々の解析が容易に実施できるという優れた特長を持っている。

この他に、マルコフ過程を応用したマルコフ解析[10]、ベイズ理論を組み込んだベイジアン・ネットワーク[11]、ペトリ・ネット解析[12]、確率過程とプラント状態シミュレーションを組み合わせたDYLAM[13]等、それぞれ特徴を持ったシステム信頼性解析手法が開発されている。

5．安全設計

前章までの分析・評価方法により、システム中で脆弱な部分を定量的に明らかにすることができる。安全性の向上には構成機器の信頼度の向上がまず考えられるが、成熟した製品ではそれは既に限界に達している。システム構成を改善することにより効果的に安全性を高める事が可能な場合があり、種々の設計方法が採用されている。これらの主要な考え方を以下項目別に説明する。

5－1　冗長性（Redundancy）

2重あるいは多重に同一の働きをする機器を備えておき、システム全体の信頼性を増加させる手法

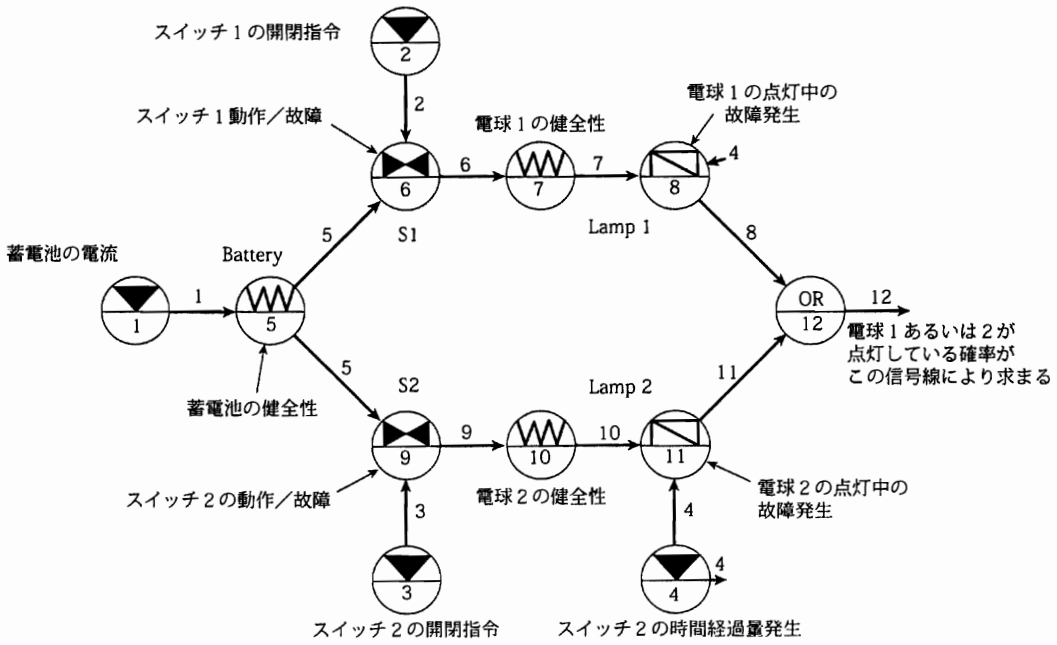

図7　GO-FLOWチャートの一例

を冗長性という。部品の一つが故障したとしても他の部品によって機能を確保できるようにするなどして、故障を予め考慮したシステム構成がなされているものを「冗長系」と呼ぶ。例えば2重の冗長系では、単一の部品の故障確率が0.03であっても、システムの機能は0.0009の確率でしか失われない極めて信頼度の高いシステムを作ることができる。

5－2　フェイルセーフ設計（Fail safe）

機械は不可避的に故障が発生するということを念頭に置き、故障が発生した場合にも、常に安全が保たれる様にする設計思想。例えば、鉄道における列車検出システムでは、万一システム中の機器故障、信号伝達線の断線等で検出信号が得られなくなった時、列車が存在すると判断するようになっており、列車の衝突が防げるようになっている。

5－3 フールプルーフ設計（Foolproof）

専門的な知識をもたない者が誤った用法で事故を引き起こさないようにする設計思想を指す。自動車ドアのロック解除には2段階の操作を必要とし、幼児が走行中誤って開くことの無い様に設計してあるのもフールプルーフの一例。このように、仕組みを理解していない者や知識を持たない者が操作した場合に機能しない仕組みに設計すること。

5－4　フォールトトレラント設計
（Fault tolerant）

システムの一部に問題が生じても全体が機能停止するということなく動作し続ける（一部機能でも）ように設計すること。冗長性採用により実現ができるが、他の設計方法でも実現可能。トレーラーで、多数あるタイヤの一本がパンクしても走行できるような設計もこの一例。

5－5　デッドマン装置

列車運転中に運転士の意識喪失などの異常事態が発生した場合に、自動的に列車を停止させる運転保安装置。これは、運転中に運転士が常に保持していなければならない装置部品を置くことにより実現している。船舶には一定時間操作をしないと警報を発し、居眠りを防止する装置が設置されているものもある。

5－6　安全率

2項でも述べた様に、破壊される最小の負荷と、安全に利用できる最大の負荷との比（前者÷後者）のこと。応力（荷重･強度）のほか、トルク、電圧、曝露量などさまざまな負荷に対し使われる。

安全率は安全係数とも言う。類似の語にマージン（margin）がある、これは、安全率から1を引いた余裕部分を意味する。

「耐荷重量:100 kgf（安全率 2.5）」と言った場合、安全に使用出来るのは100kgfまでであり、250 kgfで確実に壊れる（あるいは計算上壊れると予想される）という意味である。

例えばエレベーターのかごを吊るすロープなどは安全率を10以上とすることが建築基準法によって定められている。人間が摂取する薬品に対しては、100倍等の特段厳しい安全係数が用いられる。逆に、航空宇宙工学では、安全係数が1.15～1.25倍と極めて低く取られている。これは安全のための設備や余裕が、そのまま機体重量に直結し、経済性の悪化につながるためである。徹底した品質管理で安全確保を行っている。

6．人間信頼性解析

工学システムでは運転員（人間）が関与し操作するのが普通である。安全を評価する場合には、人間と機械システムをトータルなシステムとして捉え、人間の誤操作や逆に人間による機械部分の故障の修復・誤作動のバックアップも考慮する必要がある。

それ故、人間の信頼性解析が安全性評価においては重要な仕事となってくる。しかし、人間は機械システムとは異なり種々の複雑な性質を持っている。感覚器官からの入力を基に判断し、システムへフィードバック的動作を行う。また、不十分、互いに矛盾する、あるいは多義性のある情報が与えられた時でも何らかの判断を実施する事が可能である。正しい判断・操作をする確率は訓練の程度、手順書の良否に大きく依存している。余裕時間が長いほど通常正しい判断・操作を実施する事ができる。さらに、人間の置かれた状態によっても動作の成功確率は種々異なってくる。

人間信頼性解析（Human Reliability Analysis；HRA）とは、安全評価を実施する上で、ある状況において人間がとるべき行動から逸脱する確率を評価する作業のことで、これにより人間の信頼度を推定する。HRAにおいては、まずシステムの信頼度に

影響を与える人間行動を同定する。人間は要求された動作を正しく実行できないことの他に、本題とは無関係な事を突然してしまう事もある。人間行動の全ての可能性を予測する事は不可能である。そこで、システムの信頼度に影響を及ぼす可能性の大きな人間行動を取り上げ、主要なものについて調べていかざるを得ない。

人間行動に対しての確率値を推定するのは難しい作業で、不確実さが大きなものとなる。通常、大きな不確実さ幅を取り、真値がその中に確実に収まるようにしている。また、人間行動に影響を与える要因を考慮する必要がある。この要因を Performance Shaping Factor（PSF）という。PSF には外部的なものと、人間自身が持っている内部的な要因がある。

外部的なものには、作業環境、設備の設計条件、手順書の形式、口頭による指示のあり方等がある。これには心理的な要因及び物理的な要因がある。内部的なものには、個々人の特性・技量、動機、行動が評価されるかどうかがある。

HRA の初期の手法では、人間はシステムを構成する部品とされ、要求された通り「人間部品」が機能するか否かを評価することが関心事となる。その様な第一世代の HRA のなかでは THERP 手法[14]が有名である。これは一般的なタスクに対する過誤率を与え、それに対して PSF を用い、解析対象とする特定の状況下における過誤率を求める手順である。

HRA のより進んだ手法では、人間を単なる部品としてではなく、「主体性をもって自ら判断する生身の存在」として扱う。その中の CREAM 手法[15]は、人間行動の因果関係をあらかじめ類型化して用意しておき、それを活用し、解析対象で抽出されたヒューマンエラーの背後要因の連鎖を詳細に調べあげる方法である。

そのほかに、人間行動を、スキルベース、ルールベース、知識ベースの３種類の階層構造に分解して考えるラスムッセンのラダーモデル[16]、人間と機械・ソフト・環境との接点部分にヒューマンエラーの要因があるとする SHELL モデル[17]、m-SHELL モデル[18]等が人間信頼性解析において使用されている。

7．おわりに

現在、安全工学の分野で行なわれている、主としてシステム工学的なアプローチについて述べた。確率論的な考え方がかなり普及してきており、関連する分析方法、評価方法としても多くのものが存在している事がお分かり頂けたことと思う。また、安全対策のための設計法の考え方、人間信頼性評価の必要性も紹介させて頂いた。本論が、バルブ工業会会員の皆様が、今後一層安全について取り組んでいく際の参考になれば幸いである。

＜参考文献＞

1）熊本博光：「モダン信頼性工学」，2.7節，コロナ社，2005年
2）MIL-STD-1629A：“Military Standard Procedures for Performing a Failure Mode, Effects and Criticality Analysis”, 1980年
3）British Standard BS: IEC61882:2002 “Hazard and operability studies （HAZOP studies）-Application Guide”
4）熊本博光：「モダン信頼性工学」，5.1節，コロナ社，2005年
5）U.S.Nuclear Regulatory Commission：“An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants, Appendix I Accident definitions and use of event tree”, WASH-1400, NUREG-75/014, 1975年
6）U.S.Nuclear Regulatory Commission：“An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants, Appendix II Fault tree methodology”, WASH-1400, NUREG-75/014, 1975年
7）U.S.Nuclear Regulatory Commission：“An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants”, WASH-1400, NUREG-75/014, 1975年
8）IAEA-TECDOC-553：“Computer Codes for Level 1 Probabilistic Safety Assessment”, June 1990年
9）松岡　猛：「システム信頼性解析手法GO-FLOW」，配管技術，Vol.51, No.3, pp.11-16, 2009年
10）熊本博光：「モダン信頼性工学」，6.3節，コロナ社，2005年
11）繁枡算男・他：「ベイジアンネットワーク概説」，培風館，2006年
12）太田　淳・辻　孝吉：「ネット理論－ペトリネットとその解析問題－」，Fundamental Review, Vol.2, No.4, pp.56-67, 2009年
13）G. Cojazzi, P.C.Cacciabue, and P. Parisi：“DYLAM-3 A Dynamic Methodology for Reliability Analysis and Consequences Evaluation in Industrial Plants”, EUR15265EN ,1993年
14）A. D. Swain and H.E.Guttman：“Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications”, NUREG/CR-1278, 1983年
15）Erik Hollnagel：“Cognitive Reliability and Error Analysis Method CREAM”, ELSEVIER, 1998年
16）J. Rasmussen：“Skills, Rules, and Knowledge ; Signals, Signs, and Symbols, and Other Distinctions in Human Performance Models”, IEEE Trans. On SMC, Vol.SMC-13, pp.257-266, 1983年
17）H. F. Hawkins：“Human Factors in Flight”, Gower Technical Press Ltd., 1987年（黒田勲監修・石川好美監訳「ヒューマン・ファクター」，成山堂書店，1992年）
18）河野龍太郎：「医療におけるヒューマンエラー」，医学書院，2004年