ま　え　が　き

本書は安全分析、アシュアランスケース、モデルベースシステムズエンジニアリングを解説した本です。

2022 年 10 月

松野裕, 高井利憲, 岡本圭史

1 イントロダクション

この本はシステムの安全性分析および保証を解説する。近年、自動運転システムなどの人工知能を用いた複雑なシステムが実用化しつつある。しかしながらその安全性の分析や保証は従来よりも困難になりつつある。機械学習のモデルの出力

週 1 回 15 コマの授業を想定し、各コマで演習を行えるようにしている。

2 安全分析の基本手法: FTA と FMEA

2.1 未然防止の手法

障害への対応法は、応急処置、再発防止、および未然防止がある。応急処置、再発防止は発生した障害に対応する事後解析であり、リアクティブな方法（Reactive Approach）と呼ばれる。未然防止は、障害が発生してから対策を取るのではなく、計画段階や設計段階の生産の源流において、将来起こりうる障害を洗い出して、それらに対策を講じてしまうことである。潜在的な障害に対応する事前解析であり、プロアクティブな方法 (proactive approach) といわれる。未然防止の手法には、FMEA(Failure Mode and Effect Analysis), FTA(Fault Tree Analysis), ETA(Event Tree Analysis), 良品解析などがある。信頼性工学や安全性工学では良さ加減を増強するよりも、悪さ加減を減少させる方法がとられることが多い。

未然防止技術は多くある（多変量解析、品質機能展開、品質工学、実験計画法、WCA、FEM、信頼性試験、故障解析、信頼性データ解析、リスク・アセスメント、ライフサイクル・アセスメント（LCA））。本講義では、最も代表的な FTA, FMEA を扱う。

2.2 FTAとFMEA

FMEA, FTA は対象とするシステム（製品、設備、プロセスなど）の故障、不具合、欠陥などの「悪さ加減」を論理的に洗い出して、内在する問題点を発見する解析手法である。見出された問題点に対しては、実際の技術活動や管理活動を通じて対策や是正措置が取られる。

FTA と FMEA の形態を示す。図図 2.1、図図 2.2 は、工作用の洋ばさみについての FTA と FMEA である。(a) ははさみの部分と名称を示したもので、

図 2.1 FTA の形態（工作用はさみの事例）

内刃、外刃、留ねじの 3 つの部品からなる。(b) ははさみに対して実施した設計 FMEA を示す。部品の故障モードを洗い出して、システム（この場合ははさみ）への影響を表形式で解析する手法である。原因系から結果系を予測する方法と言える。(c) は、はさみで紙が切れないという結果の事象を取り上げて、

図 2.2 FMEA の形態（工作用はさみの事例）

その原因を探る FTA の一部を示す。FTA は木構造の解析手法である。主な論理ゲートは AND ゲート (論理積) と OR ゲート (論理和) である。

一般にシステムはサブシステムに、サブシステムはコンポーネントに、というように、順次、下位の構成要素に分解される。最終的にこれ以上分解できないレベルにいたる。システムとしては、階層的に分解できる構造であれば、ハードウエアでも、ソフトウエアでも、プロセスでも、あるいはそれらの複合でもよい。FMEA は下位の階層の悪さ加減が上位の階層の悪さ加減にどのように影響するかを表形式上で論理的に解析する手法である。FTA は逆に上位の階層の悪さ加減の原因となる下位の階層の悪さ加減を木構造で論理的に解析する手法である。FMEA は単一の原因が及ぼす複数の結果を網羅的に洗い出すのに優れ

た手法であるが、複数の原因によって及ぼされる結果の洗い出しは難しい。一方、FTA は複数の原因によって及ぼされる結果も表現できるが、網羅性が十分ではない。両者は相補的かつ相乗的に用いられている。

2.3　FTA(Fault Tree Analysis、故障の木解析)

FTA は、「なぜなぜ」を繰り返すことで、重大な故障やトラブルの発生要因を下方に向かって木構造として展開し、網羅した要因の中から重要な要因を抽出する。1979 年にスリーマイル島で発生した原子力事故の解析の際、マサチューセッツ工科大学教授の Rasmussen が原因の特定に使用したことでその有効性が評価され広まった手法である。

2.3.1　FT 図を読む

FT 図は、視覚的に故障に至るメカニズムが大変わかりやすく表現されている。FT 図の記号は、イベントを示す事象記号と、それらの間の因果関係を示す論理記号とに分けられる。表表 2.1 にある 4 つの記号の意味を理解できれば、ほとんどの FT 図を読むことができる。さらに、表表 2.2 のノードも用いられる。FT 図の例を図図 2.3 に示す。トップ事象である欠報の原因には「火災の検知信号が届かない」不具合と「ブザーが鳴らない」不具合とがあり、いずれか一方の原因で欠報に陥ることが示されている。さらに、その 2 つ以外に原因がないこと、あるいは他の原因は無視してよいことを示している点が重要である。この必要十分性は、熟練者でもしばしば見落とす点である。一方の AND

表 2.1　FTA で用いる基本的な記号

表 2.2　FTA で用いる便利な記号

ゲートは、すべての下位事象が同時に発生するときに上位事象が発生することを示す記号で、並列型に対応する。「火災の検知信号が届かない」事象は、冗長に設置された２つのセンサ系 A,B が同時に故障しているときのみ発生する事象となる。FTA には、

図 2.3 FT 図の例

- トップ事象と基本事象との因果関係が視覚的に示され、多様な事象間関係を把握しやすい。
- AND ゲートにより多重故障を解析できる。

などの特徴がある。

2.3.2 FT 図 の 作 成

FTA の実施は、FT 図の作成と FT 図の解析の２つのステップで構成される。ここでは作成までの手順を説明する。

1. FTA 実施の準備。対象製品を熟知する技術者と品質保証担当者を含めた 3 名から 6 名程度のメンバーで実施する。設計資料、図面、材料部品リストや想定使用状況、関連するトラブル、クレーム情報、特に不具合に関する情報を集める。
2. 解析対象の機能の理解。FTA で解析する対象製品の構造や機能について、参加者全員で十分理解する。自分の専門とする部分や分野に対象を限定することなく、周辺との関係なども理解することが重要である。
3. トップ事象の選定。信頼性や安全性を損なうような「発生することが望ましくない」トップ事象を注意深く選定する。その際、1. 明確に定義できる事象、2. 多くの下位事象の結果として発生する事象、3. 設計の中で技術的に対処できる基本事象が予想される事象、であることが望ましい。1 が最も重要な要件であり、「明確」なとは、その事象発生の有無の判断が人によって異なることはない、との意味である。例えば「エアバッグが開かない（不動作故障)」、「エアバッグが不要のときに開く（誤作動故障)」など

は、トップ事象としてふさわしい。しかし「***の満足度が低い」、「***の回転が不安定」などは、その範囲（基準値）が不明瞭であり適さない。また一見良さそうに見える「排気ガス規制の基準値を満たしていない」のような表現も避けるべきである。ガスの種類や基準値は時代と共に変化するので、「排気ガス CO の規制基準値**ppm を満たさない」などの具体的な基準値を明記する必要がある。2. は、FTA 解析はマンパワーが必要となるので、できるだけ重要なトップ事象を扱う、という意味である。3. は、設計時に、FT 図作成に関わる技術者が基本事象まで書ききることができるようにするためである。

4. トップ事象の 1 次要因への展開。トップ事象の 1 次要因を、製品の構造や機能、手順 1 で準備した情報などを基に列挙し、論理記号を用いて因果関係を明確に図示する。

   展開する方法は大きく分けて 2 つある。

   (a) 構造（信頼性ブロック図）からの作成。あるシステムが信頼性ブロック図で構造が示される場合、直列系の部分を OR ゲートに、並列型部分を AND ゲートに対応させることで、FT 図を容易に作成できる。

   (b) 機能を考えて作成。実際には、信頼性ブロック図を基に FT 図全てを作成できるケースは多くない。構成要素の機能に着目して、トップ事象の直接の原因である 1 次要因を抽出し、さらにそれらの原因である 2 次要因を抽出するという具合に、意味を考えてトップダウンに作成することになる。

   1 次要因への展開は、最も頭を悩ませるステップだが、重要な箇所であり、時間をかけるべき手順である。システムを構成するサブシステムごとに空間的に分割し、それぞれを解析するとの方針がとられることが多いが、それよりも、エネルギーの流れに注目するなど、機能的な側面から 1 次要因を分解すると、装置間の相互作用などを見失うことが少なく、効果的な木になることが多い。

5. トップ事象の 2 次要因以下への展開。展開可能な 1 次要因に関して、さ

らになぜなぜ分析を続け、2 次要因、3 次要因を列挙、基本事象または非展開事象に至るまで論理記号を用いて展開する。

例題 図図 2.4 に示されるような、2 つのセンサが並列に設置された自動照明器で、「照明が点灯しない」をトップ事象とする FT 図を作成せよ。

図 2.4 照明設備の回路図と信頼性ブロック図

手順 5 までで FT 図ができあがるが、効果的な FT 図を作成するためのコツがある。

i) 事象発生の有無が明確な表現にすること。トップ事象にかかわらず、中間事象や基本事象でも、事象発生の有無が人によりかわることのない、明確な表現にする。「**が弱い」、「**が不安定」などの表現はさけるべきである。

ii) 基本事象では、事象を一意に特定できるように表現すること。基本事象レベルでの「接点故障」などの表現は不適切であり、それらの状況により対策が異なる。基本事象では、FT 図の作成者に聞くことなく、その状況を一意に把握できる表現まで分解することが必要である。

iii) 必要で十分な要因を漏れなく列挙しながらトップダウンで作成すること。各レベルでの要因抽出時に、思いつく要因の候補をあげればよい、という発想という発想では適切な FT 図は得られない。特に OR ゲートの下位事象では、必要十分な要因を漏れなく列挙することが求められる。

iv) 横のレベルをそろえながら分解すること。自分の得意な部分になると、いきなり詳細の部位の不具合要因がならぶことがよくある。1 次、2 次、とトップダウンで作成するが、それぞれのレベルに並ぶ事象の階層を合わせることが、見やすい FT 図を作るコツである。

2.4　FT 図で定量的に解析する

FT 図を作成すると、トップ事象を発生させる要因、およびその発生経路が明らかになる。それらを基に、解析のステップに移ることができる。

手順６では、トップ事象に対して改善効果が高いことが見込まれる基本事象を抽出するために、定量的評価法または定性的評価法を適用する。定量的評価法では、トップ事象の発生確率を求め、さらに、その確率を下げるためにはどの基本事象の発生確率を下げることが効果的かを特定する。そのためには、すべての基本事象の発生確率がわかっていることが前提となる。

手順７では、手順６で抽出された重要要因について、対策事項、対策方法を決定し、担当部署を決める。そして、対策実施後のフォローアップを確実に行う。

手順 6 におけえる定量的評価法では、トップ事象の発生確率を求め、さらにその確率を下げるためにはどの基本事象の発生確率を下げることが効果的かを特定する。そのためには、すべての基本事象の発生確率がわかっていることが前提となる。

(i)　トップ事象の発生確率。トップ事象の発生確率は、基本事象の発生確率から容易に推定することができる。論理記号に着目して、次の方法で上位事象の確率を算出していく。

(a)　OR ゲート $\rightarrow$ 下位事象の発生確率の和

(b)　AND ゲート $\rightarrow$ 下位事象の発生確率の積

例えば、図図 2.5(b) で基本事象である各パソコンの故障の確率を 0.001, プリンタの故障確率を 0.0001 とする。トップ事象の発生確率を推定する場合、パソコン故障の発生確率は、AND ゲートであるから、

$$Pr = 0.001 \times 0.001 = 1.0 \times 10^{-6}$$

となり、トップ事象の発生確率は、OR ゲートで結ばれているため、

$$Pr = 1.0 \times 10^{-6} + 1.0 \times 10^{-4} = 0.000101$$

となる。以下に注意したい。

- 事象の発生確率とは不信頼度 F のことであり、故障率ではない。故障率は単位時間当たりの故障発生回数で定義されるので、OR ゲートの場合は各構成要素の故障率の和で定義できるが、AND ゲートでは面倒な計算が必要となる。
- OR ゲートでの計算方法は近似式である。
- AND ゲート、OR ゲートでの計算の独立性が仮定されている。

(ii)　同一事象の排除。FT 図においては、同一の基本事象、中間事象が 2 箇所に現れても構わない。ただし、定量的解析を行う場合、同一事象を一つにまとめた FT 図に変形してから解析を進めなければ、誤った結果を導いてしまうことに注意すべきである。同一事象が複数含まれる場合には、事象間の独立性が失われるからである。図図 2.5 では、Tree としては同値だが、トップ事象の発生確率を求める場合、同一の基本事象を一つにまとめた (b) 図を用いなければならない。より深刻な例として、2000 年 12 月の京

図 2.5　同じ意味の 2 つの FT 図

福電鉄の正面衝突事故がある。常用ブレーキも非常ブレーキも効かなかった事故であるが、通常、常用と非常用のブレーキは冗長化構造になっており、図図 2.6 の (a) の FT 図が想定される。並列の 2 つのブレーキがあるにもかかわらず同時に故障に陥る確率は、1 次要因が AND ゲートで結ばれているため、積により小さな値になることが容易に想像できる。しかしこの車両のブレーキ装置では、常用と非常用で同一のブレーキレバーの角度の違いで操作する形式であり、ブレーキ制御部は同じものを使用していた。二重化されていたのは、圧縮空気の送風装置だけである。このため (b) の FT 図でトップ事象の発生確率を算出する必要があった。

図 2.6　常用ブレーキと非常ブレーキの多重故障の解析

(iii) トップ事象に大きな影響を与える基本事象の抽出。トップ事象の発生確率が推定されると、次に、どの基本事象の発生を抑えることがトップ事象の発生確率を下げるために効果的かを知ることができる。OR ゲートの場合、トップ事象の発生確率は（重複事象がなく独立性が成立していれば）基本事象の発生確率のトータル和となるため、発生確率の最も高い基本事象から対策を講じれば良い。しかし AND ゲートが含まれると容易ではない。

2.5　FT 図で定性的に解析する

多くの場合、基本事象の発生確率を推定することは難しい。基本事象の発生確率を前提とせず、トップ事象への影響の大きな基本事象を特定するための方法として、最小カット集合を利用した方法と構造重要度を利用した方法がある。

2.5.1　最小カット集合を利用した方法

最小カット集合とは、トップ事象を発生させ得る最小の基本事象の組み合わせである。例えば図 2.7 の Tree では、$\{A, B\}, \{A, C\}$ の 2 つが最小カット集合になる。この時、最小カット集合に共通の基本事象 A が存在することから、A の発生を確実に抑えることができれば、トップ事象を回避することができる。すべての最小カット集合に共通の基本事象が存在するとは限らないが、一般には、できるだけ少ない基本事象の組み合わせで、すべての最小カット集合の発生を防止できるような組み合わせを探し出し対策を講じることで、トップ事象を防ぐことが可能となる。例えば最小カット集合が $\{A, B\}, \{B, C, D\}, \{B, E, F\}, \{D, E, F, G\}, \{G, H\}$ ならば、B と G の 2 つの事象に確実な対策を施せばトップ事象を回避することができる。最小カット集合を得るためには、FT 図の AND ゲートを積、OR ゲートを和で表し、ブール代数を用いて積で表した項の和 (加法標準形) で全体を表現できれば、それら各項が最小カット集合である。ブール代数において、0 は事象未発生、正常、1 は事象発生、故障とする。図図 2.7 では

$$T = A \cdot (B + C) = A \cdot B + A \cdot C$$

となり、$\{A, B\}$, $\{A, C\}$ の 2 つの最小カット集合が得られる。

2.5.2 構造重要度を利用した方法

構造重要度は、一つの基本事象に着目し、その事象が正規した時にトップ事象が発生する割合 (他の事象の組み合わせ増加数) を表す。図図 2.7 の例で説明する。

図 2.7 FT 図とその基本事象とトップ事象

(i) 最小カット集合を求める。$\{A, B\}, \{A, C\}$ が最小カット集合である。

(ii) 最小カット集合に基づき、基本事象とトップ事象との関係を表す真理表を作成する。$A = B = 1$(故障)、$A = C = 1$ のとき $T = 1$ とすればよい。

(iii) A に関する構造重要度 $I_S(A)$ を下記で求める。

- $X =$ 事象 A が故障時のトップ事象発生の組み合わせ数、
- $Y =$ 事象 A が正常時のトップ事象発生の組み合わせ数としたとき、

$$I_S(A) = \frac{X - Y}{2^{n-1}},$$

すなわち $I_S(A) = \dfrac{3-0}{4} = \dfrac{3}{4}$ となる。また $I_S(B) = I_S(C) = \dfrac{2-1}{4} = \dfrac{1}{4}$ となり、A の構造重要度は B,C のそれよりも 3 倍となる。よって A を重点的に対策を取れば良いといえる。すべての基本事象の構造重要度を算出することで、トップ事象の回避への寄与度を知ることができるが、この値の算出は意外と面倒である。FTA 解析用のソフトウエアでは自動的に計算され便利である。

2.6 FTA 実施上の留意点

FTA を実施する際に注意すべき点は下記の通りである。

(i) 全ての基本事象の発生確率が必要であること。

(ii) 創発故障への対応。部品間の相互作用による創発故障を見落とさないためには、１次の分解で、構造ではなく、機能に着目して分解することに注意するとよい。

(iii) 動的変化への対応。FTA は基本的に静的な解析であり、動的変化を解析しにくい。トップ事象の発生確率も動的に変化するため、一定期間後のある時点での値で評価することに限定される。

(iv) 事後解析での活用。未然防止での利用を念頭に説明してきたが、故障解析や事故解析などの事後解析では確率値を利用した解析は行わない。実際に発生している真の原因を、多数の可能性がある要因の中から絞るために FT 図を利用するものであり、最小カット集合の中から、新の発生要因を絞り込むことが可能になる。

参 考 文 献

本資料は「システムの信頼性と安全性、田中健次、朝倉書店」、「新 FMEA 技法、益田昭彦、高橋正弘、本田陽広、日科技連」を基にしている。

3 安全分析手法STAMP/STPA

4 モデルベースシステムズエンジニアリング

5 アシュアランスケース

人工知能の研究開発は加速的に進み始めている。2022 年に登場した ChatGPT は、誰でも簡単にウエブ上で質問をすることができるチャットボットであるが、その回答の詳細さと自然さに、多くの人が驚いた。また歩行者や標識を自動認識する人工知能を持つ自動運転車は、アメリカの Waymo 社や日本の Tier4 社など、多くの企業が開発競争を繰り広げており、アメリカではすでにカリフォルニア州において自動運転タクシーが実用化されている。しかしながら、チャットボットや自動認識を行う人工知能は、100%正しい出力をするわけではない。であるにも関わらず、その圧倒的な利便性から、人工知能が組み込まれたシステムが加速的に普及していくことはより確実になってきている。そのような状況おいて、我々を取り巻くシステムが安心して利用できるものなのか、改めて社会的な合意形成が必要な時期になっている。

5.1 アシュアランスケースの記述方法

アシュアランスケースは基本的にドキュメントであり、多くの場合文書形式で記述される。近年では、アシュアランスケースの主張と議論構造、およびエビデンスのつながりをモデル化したグラフィカルな記述方法も用いられている。本著では、グラフィカルな記述方法の中で、Goal Structuring Notaion (GSN) を用いる。

GSN は主に以下のノードの種類からなる。

- ゴール (Goal)：システムに対して、議論すべき命題である。例えば「システムはディペンダブルである」とか「システムは適切な安全性をみたす」などである。
- 戦略 (Strategy): ゴールが満たされることを、サブゴールに分割して詳細化するときの議論の仕方である。例えば、「システムは安全である」というゴールに対して、現時点で識別されているハザードに対処できていることによって議論したいとき、戦略ノードとして「識別されたハザードごとに場合分け」を用いると、例えばひとつのサブゴールは「システムはハザード X に対処できる」となる。
- 前提 (Context): ゴールや戦略を議論するとき、その前提となる情報である。例えば、運用環境や、システムのスコープ、あるいは「識別されたハザードのリスト」などである。
- 未達成 (Undeveloped): ゴールを保証するための十分な議論もしくはエビデンスがないことを表す。

5.2　アシュアランスケースの例

5.3　アシュアランスケース記述ステップ

5.4　基　本　演　習

6 総合演習

7 まとめ