

1 群 (信号・システム) - 12 編 (信頼性理論)

2 章 システムの信頼性評価技法

(執筆者: 田村信幸) [2009 年 6 月 受領]

概要

日本工業規格 (JIS) の信頼性用語によると、システムとは「所定の任務を達成するために選定され、配列され、互いに連携して動作する一連のアイテム (ハードウェア、ソフトウェア、人間要素) の組合せ」と定義されている。システムを企画・設計・製造・使用する際には、その信頼性を適切な方法で評価し、何らかの対策を講じることによって信頼性を高め、システムの効率的・効果的運用を心掛けることが必要である。信頼性をどのように評価するかは、上記のようなシステムのフェーズのほか、統計的なデータを含めた利用可能な情報、故障や異常発生に伴う損失・損害の大きさ、更には評価に伴うコストや労力といった環境など様々な要因を考慮しなければならない。

ここで基本となるのは、ブロックダイアグラムを用いて構成要素間の故障 (あるいは異常) の相互関係、及び各構成要素とシステムの機能的関係を把握することである。そして次に、修理系であればシステムの性能を表す基本的な指標である信頼度、非修理系であればアベイラビリティを求める。更に、これらの評価尺度を用いて、FTA・FMEA・ETA を使用することによって実際にシステムの信頼性を向上させるために必要となる対策を構築し、これによりどのような効果があるかを明らかにすることが重要である。

【本章の構成】

本章ではブロックダイアグラムと基本的なシステムの評価法 (2-1 節)、非修理系の評価を行う際に用いられる指標であるアベイラビリティ導出に必要なマルコフ解析 (2-2 節)、そして、実際に信頼性を高めるための対策を構築するうえで有用な FTA・FMEA・ETA (2-3 節) に関して、基本的な考え方と各評価技法の使用法、及び使用例について述べる。

1 群 - 12 編 - 2 章

2-1 ブロックダイアグラム

(執筆者：田村信幸)[2009年6月受領]

本節では、複数の構成要素(部品など)からなる機器や装置を総称してシステムと呼ぶ。また、構成要素をユニットと呼び、ユニットが故障しても修理や取替えなどによりその機能が回復することはないものとする。このとき、システムとユニット間の信頼性の関係を探るには、あるユニットの故障がほかのユニットの故障を引き起こすかどうかというユニット間の故障の相互関係、及びユニットの故障がシステムの故障となるかといったユニットとシステムの機能的、構造的関係を事前に知っておく必要がある。ここでは特に各ユニット間の故障は互いに独立であり、各ユニットの信頼度は時間によらず一定であると仮定する。

システムとユニットの機能的、構造的関係を示す図をブロックダイアグラム(block diagram)と呼ぶ。システムをブロックダイアグラムで表現するには直列系と並列系の概念が重要である。

2-1-1 直列系と並列系

直列系(series system)とは、システムを構成するどのユニットが故障してもシステムそのものが故障となるシステムである。 n 個のユニットから構成される直列系のブロックダイアグラムは図2・1のようになる。

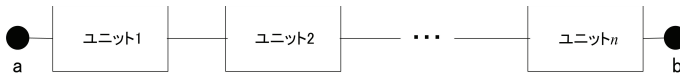


図2・1 直列系のブロックダイアグラム

ユニット i ($i = 1, \dots, n$) の信頼度を R_i とする。信頼度とは、機器や装置、部品などのアイテムが定められた期間、故障することなくその機能を果たす確率である。直列系が機能するのはすべてのユニットが機能しているときのみである。各ユニットの故障は互いに独立であるため、直列系の信頼度 R_s は式(2・1)のように各ユニットの信頼度の積として表される。

$$R_s = R_1 \times R_2 \times \dots \times R_n = \prod_{i=1}^n R_i. \quad (2 \cdot 1)$$

各ユニットの信頼度は常に $0 \leq R_i \leq 1$ を満たすことから、式(2・1)より直列系の信頼度はユニットの信頼度よりも必ず低くなること、そして、直列系の信頼度はユニット数の単調非増加関数になることが分かる。よって、直列系の信頼度を上げるには、信頼度の最も低いユニットを見つけ、その信頼度を高くするような対策を施すことが必要である。

これに対し、ユニットすべてが故障したときのみシステム故障となるようなものを並列系と呼び、図2・2のようなブロックダイアグラムで表される。並列系の信頼度を R_p とする。各ユニットの不信頼度は $1 - R_i$ ($i = 1, \dots, n$) であるため、並列系の信頼度 R_p は

$$R_p = 1 - \prod_{i=1}^n (1 - R_i) \quad (2.2)$$

で与えられる．直列系と異なり，並列系の信頼度はユニット数の単調非減少関数となる．また，並列系の信頼度を高くするためには，直列系の場合とは逆に信頼度の最も高いユニットを改善しなければならない．

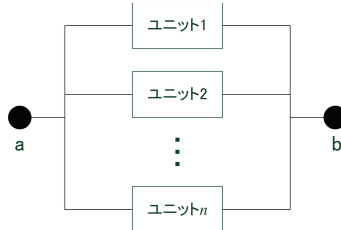


図 2.2 並列系のブロックダイアグラム

ブロックダイアグラムを作成するには，ユニットの故障が即システム故障に繋がるものを直列に，そして，あるユニットが故障しても別のユニットが動作していれば故障を防げるようなものを並列に配置する．ユニット数が多い複雑なシステムの場合，システムを幾つかのサブシステムに分解して直列と並列の組合せと見なせるようにするとブロックダイアグラムを作成しやすい．しかし，現実にはそのような単純な構造になっていないシステムが存在する．

2-1-2 パスセットとカットセット

直列と並列の組合せと見なすことができない一般的なシステムの場合，システムの機能的，構造的関係を把握しやすい等価な構造のシステムに変形する．この際に必要となる概念がパスセットとカットセットである．なお，本節の内容は構造関数に基づいて議論されることもある¹⁾が，ここでは触れない．

直列系の信頼度を求める際には，直列系が正常に動作するためのユニットの組合せを考えた．このようにシステムが動作可能なユニットの組合せをパス (path)，そして，すべてのパスの集まりをパスセット (path set) と呼ぶ．図 2.1 の直列系のパスセットは $\{1, 2, \dots, n\}$ のみである．パスの中でどのユニットが故障しても動作できなくなるようなパスをミニマルパス (minimal path)，すべてのミニマルパスの集まりをミニマルパスセット (minimal path set) と呼ぶ．直列系ではパスセットとミニマルパスセットが一致する．

一方，並列系の信頼度の算出には並列系が故障となるユニットの組合せを考えた．このようにシステムが故障となるユニットの組合せをカット (cut)，そして，すべてのカットの集まりをカットセット (cut set) と呼ぶ．並列系のカットセットは $\{1, 2, \dots, n\}$ だけである．カットセットの中でどのユニットが動作可能となってもシステムが動作するようなカットをミニマルカット (minimal cut)，すべてのミニマルカットの集まりをミニマルカットセット (minimal cut set) と呼ぶ．並列系の場合はカットセットとミニマルカットセットが一致する．

各ミニマルパスに含まれるユニットを直列に，そして，すべてのミニマルパスを並列に配

置すると等価なシステムに変形できる．カットセットを用いる場合には，各ミニマルカットに含まれるユニットを並列に，そして，すべてのミニマルカットを直列に配置すればよい．この結果を用いると信頼度も容易に算出できる．

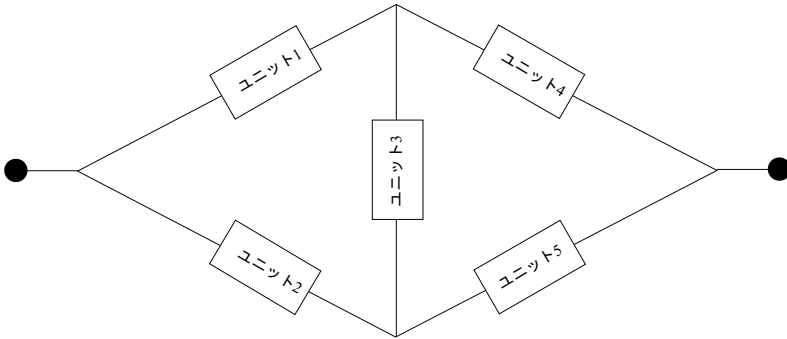


図 2.3 ブリッジシステム

例として図 2.3 のようなブリッジ構造のシステムの信頼度をミニマルパスとミニマルカットを用いて求める．図より $\{1, 3, 5\}$ のユニットが動作していればシステムは動作するが，一つでも故障するとシステムは故障となる．よって，このユニットの組合せはミニマルパスとなる．同様に， $\{1, 4\}$ ， $\{2, 5\}$ ， $\{2, 3, 4\}$ もミニマルパスとなるため，これら四つの要素の集まりがミニマルパスセットである．よって，ブリッジシステムの信頼度 R_B は

$$R_B = 1 - (1 - R_1 R_4)(1 - R_2 R_5)(1 - R_1 R_3 R_5)(1 - R_2 R_3 R_4) \quad (2.3)$$

となる．一方，ユニット 2 と 4 が動作していても $\{1, 3, 5\}$ のユニットが故障していると必ずシステム故障となるが，いずれか一つのユニットが動作可能とであればシステムも動作するためミニマルカットである．同様に $\{2, 3, 4\}$ ， $\{1, 2\}$ ， $\{4, 5\}$ もミニマルカットとなるので，ユニット i の不信頼度を $F_i = 1 - R_i$ とおくと，

$$R_B = (1 - F_1 F_3 F_5)(1 - F_2 F_3 F_4)(1 - F_1 F_2)(1 - F_4 F_5) \quad (2.4)$$

より信頼度が得られる．式を整理すると式 (2.3) と式 (2.4) の結果が一致することを確認できる．

上記の手順以外に分解法や包除原理と呼ばれる方法でも信頼度を求めることができるが，いずれもユニット数の増加に伴って信頼度の正確な算出が難しくなる．そのような場合には，近似値として信頼度の上下限を用いることがある．特にユニット間の故障発生にある非独立性の仮定を導入すると，より簡単に信頼度の上下限を計算できることが知られている²⁾．

参考文献

- 1) 真壁肇・宮村鐵夫・鈴木和幸，“信頼性モデルの統計解析，” pp.201-215，共立出版，1989．
- 2) 三根久・河合一，“信頼性・保全性の数理，” pp.90-121，朝倉書店，1982．

1 群 - 12 編 - 2 章

2-2 マルコフ解析

(執筆者: 田村信幸) [2009 年 6 月受領]

本章 2-1 節ではシステムを構成するユニットが故障してもその機能が回復しない場合に着目した。しかし、多くのシステムは、ユニットの故障あるいは異常が発生すると修理や取替えを行うことによりその機能を回復させ、システムを使用し続ける。このとき、システムをどの程度効率良く使用しているかを把握することが必要である。本節ではこのような保身を伴うシステムに対する信頼性解析のための 1 手法であるマルコフ解析について説明する。

2-2-1 マルコフ連鎖

時間の推移に従って確率法則が定まり、時点 t におけるその確率法則が確率変数 $X(t)$ で表されるとき、確率変数の集まり $\{X(t); t \geq 0\}$ を確率過程という。マルコフ解析とは、マルコフ連鎖と呼ばれる確率過程を用いてシステムの性能や特性を評価することである。確率過程は時間 t と取り得る値 $X(t)$ (通常状態と呼ばれる) がそれぞれ離散か連続かで数学的な取扱いが異なるが、信頼性評価においては連続時間、離散状態の確率過程を想定すれば十分であることが多い。 $0 \leq t_1 < t_2 \cdots < t_n < t$ に対し、

$$P\{X(t) = x | X(t_1) = x_1, X(t_2) = x_2, \dots, X(t_n) = x_n\} = P\{X(t) = x | X(t_n) = x_n\} \quad (2.5)$$

ならば、確率過程 $\{X(t), t \geq 0\}$ は連続時間マルコフ連鎖と呼ばれる。これは将来の確率法則 $X(t)$ が過去の履歴 $X(t_1), X(t_2), \dots, X(t_n)$ に関係なく、現在の状態 $X(t_n)$ だけに依存して決まることを表しており、このような性質をマルコフ性という。ある任意の $s \geq 0, t \geq 0$ に対し、

$$P_{ij}(t) = P\{X(t+s) = j | X(s) = i\} \quad (2.6)$$

は推移確率と呼ばれる。推移確率は時間 s に依存するとしても良いが、解析が難しくなるためここでは式 (2.6) である場合を考える。このとき、マルコフ連鎖は定常な推移確率をもつという。

2-2-2 解析手順

マルコフ解析は代表的な信頼性特性値であるアベイラビリティを求めるために行う。アベイラビリティには、ある時点 t でシステムが動作状態にある確率を表す瞬時アベイラビリティと長時間システムを使用したときの単位時間当たりの動作時間の期待値を表す定常アベイラビリティ (JIS2000 年版では漸近アベイラビリティと呼んでいる) の二つがよく用いられる。

時点 t での瞬時アベイラビリティを $A(t)$ 、定常アベイラビリティを A としたとき、

$$\lim_{t \rightarrow \infty} A(t) = A$$

という関係がある。したがって、瞬時アベイラビリティから定常アベイラビリティを求めることができる。

マルコフ解析の一般的な手順は以下のようなものである。

1. システムの状態を定義する .
2. 状態推移図を作成する .
3. 微分方程式または線形連立方程式を立てこれを解く .
4. 得られた解からアベイラビリティなどの信頼性特性値を求める .

上記のシステムの状態は 2-2-1 節で説明した確率過程の状態と同じものを指す . システムの状態はどのユニットが動作あるいは故障 (修理中または修理待ち) しているかという点を考慮して定義する . 状態推移図とは , ユニットの故障発生や修復作業完了によって状態が変化する様子を図示したものである .

特に以下の条件を満たしていると解析を行ううえで都合が良い .

- 各ユニットの一連の寿命時間及び修復時間が共に独立な指数分布に従う .
- 異なるユニット間の寿命時間及び修復時間が独立である .
- 各ユニットの寿命時間と修復時間が独立である .

これらの条件を満たしていなくてもマルコフ解析は可能であるが , その場合には状態の定義が複雑で , かつ解くべき方程式も難しくなり , 解析的に解を得ることが不可能であることも少なくない .

2-2-3 解析例

(1) 直列系のアベイラビリティ

ここでは修理施設が 1 箇所である 2 ユニットの直列系に対する解析例を示す . 直列系は以下の条件を満たすものとする .

1. 二つのユニットの寿命時間と修復時間は互いに独立な指数分布に従う .
2. ユニットの故障率は λ , 修復率は μ である .
3. 故障したユニットは直ちに修理施設で修理が行われる . この際 , 修理施設への移動時間は無視できる .
4. 修理が完了したら直ちに動作を再開する .

このとき

状態 0 : 二つのユニットが動作している

状態 1 : どちらか一方のユニットが故障し修理中である

と定義する . 直列系は一つのユニットが故障したらシステムは動作しない . また , 一方のユニットが修理されているときもう一方のユニットは動作しない . よって , 二つのユニットが故障している状態を考える必要はない . ここで状態 0 では 2 台のユニットが同時に動作しているため , 故障率は 2λ である . 一方 , 状態 1 では 1 台のユニットが修理中で , その修復率が

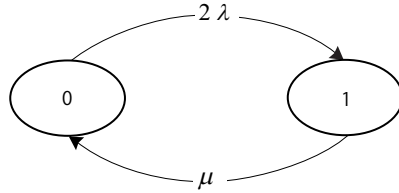


図 2・4 直列系の状態推移図

μ である．これらのことを考慮すると，図 2・4 のような状態推移図を描くことができる．時点 t で状態が j ($j = 0, 1$) である確率を $p_j(t)$ と置くと，以下のような微分方程式が得られる．

$$p'_0(t) = -2\lambda p_0(t) + \mu p_1(t), \quad (2\cdot7)$$

$$p'_1(t) = 2\lambda p_0(t) - \mu p_1(t). \quad (2\cdot8)$$

上の方程式はラプラス変換などを用いれば容易に解くことができる．直列系の瞬時アベイラビリティを $A_s(t)$ ，定常アベイラビリティを A_s とおく．直列系は二つのユニットが両方とも動作しているときのみシステムも動作するため，瞬時アベイラビリティは $p_0(t)$ そのものである．よって，

$$A_s(t) = \frac{\mu}{2\lambda + \mu} + \frac{\lambda}{2\lambda + \mu} \exp[-(2\lambda + \mu)t]. \quad (2\cdot9)$$

となり，定常アベイラビリティは瞬時アベイラビリティの極限であるため，

$$A_s = \frac{\mu}{2\lambda + \mu} = \frac{1}{2\rho + 1} \quad \left(\rho \equiv \frac{\lambda}{\mu} \right) \quad (2\cdot10)$$

で表される．

(2) 並列系のアベイラビリティ

次に並列系のアベイラビリティを求める．基本的な仮定は直列系の場合と同じである．状態を

状態 0 : 二つのユニットが共に動作している

状態 1 : 一方のユニットのみ動作し，もう一方は故障のため修理中である

状態 2 : 二つのユニットが共に故障している

と定義すると，状態推移図は図 2・5 のように描ける．状態が j である確率を $p_j(t)$ とすると，微分方程式は

$$p'_0(t) = -2\lambda p_0(t) + \mu p_1(t), \quad (2\cdot11)$$

$$p'_1(t) = 2\lambda p_0(t) - (\lambda + \mu)p_1(t) + \mu p_2(t), \quad (2\cdot12)$$

$$p'_2(t) = \lambda p_1(t) + \mu p_2(t) \quad (2\cdot13)$$

となる．並列系の瞬時アベイラビリティを $A_p(t)$ ，定常アベイラビリティを A_p とおく．ユニットが 1 台でも動作していればシステムは動作可能なので，瞬時アベイラビリティは以下のよ

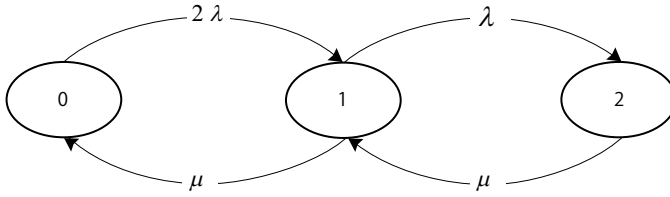


図 2・5 並列系の状態推移図

うになる .

$$\begin{aligned}
 A_p(t) &= p_0(t) + p_2(t) \\
 &= \frac{2\lambda\mu + \mu^2}{2\lambda^2 + 2\lambda\mu + \mu^2} + \frac{2\lambda^2}{(2\lambda^2 + 2\lambda\mu + \mu^2)\sqrt{\lambda^2 + 4\lambda\mu}} (s_1 \exp[s_2 t] - s_2 \exp[s_1 t]).
 \end{aligned}
 \tag{2・14}$$

ただし ,

$$s_1 = \frac{-(3\lambda + 2\mu) + \sqrt{\lambda^2 + 4\lambda\mu}}{2}, \quad s_2 = \frac{-(3\lambda + 2\mu) - \sqrt{\lambda^2 + 4\lambda\mu}}{2}$$

である . このとき , 定常アベイラビリティは

$$A_p = \frac{\mu^2 + 2\lambda\mu}{2\lambda^2 + 2\lambda\mu + \mu^2} = \frac{1 + 2\rho}{2\rho^2 + 2\rho + 1} \quad \left(\rho \equiv \frac{\lambda}{\mu} \right)
 \tag{2・15}$$

となる .

2-2-4 そのほかのシステムの解析

信頼度の場合と異なり , アベイラビリティは直列系と並列系の算出方法のみでは求めることができない . 基本的にはシステムの特性を考慮して状態を定義したうえで方程式を立て , それを解くことによってアベイラビリティを求めることになるが , ユニット数が増えると解析的に解を得ることが難しくなることもある . また , ここでは寿命時間や修復時間が指数分布に従うなどの条件の下で解析を行ったが , 指数分布以外の場合は状態の定義や解の導出が難しくなることが少なくない . 様々なシステムに対するアベイラビリティの導出法については市田¹⁾や三根ら²⁾の文献で触れている . なお , 通常ユニット数の多いシステムや指数分布以外の分布の仮定が必要なケースなどマルコフ解析が容易でない状況では , シミュレーションなどの数値計算に頼ることになる .

参考文献

- 1) 市田嵩 , “改訂 保全性工学入門,” 日科技連 , pp.157-224 , 1976 .
- 2) 三根久 , 河合一 , “信頼性・保全性の数理,” 朝倉書店 , pp.124-153 , 1982 .

1 群 - 12 編 - 2 章

2-3 FMEA・FTA・ETA

(執筆者：高久 清)[2009年6月受領]

2-3-1 概要

システムの信頼設計には、二つの側面がある。第一の側面は、高信頼性システムを実現するための設計である。この設計手法には、信頼度予測、寿命予測、ディレーティング、冗長設計などがある。第二の側面は、システムに潜在している故障または事故の因果関係を解析し、それを防止するための設計である。この設計手法には、FTA (Fault Tree Analysis, 故障の木解析), FMEA (Failure Mode and Effects Analysis, 故障モード影響解析), ETA (Event Tree Analysis, 事象の木解析), フェイルセーフ, フールプルーフ設計などがある。ここでは、第二の側面である FTA, FMEA 及び ETA について説明する。FTA 及び FMEA は、システムの故障または事故の因果関係をシステムの階層に沿って解析する手法である¹⁾⁻⁵⁾。図 2・6 に、両者の解析方法を対比して示す。ETA は、システムの故障または事故に至る時間的な経過及び人為的な判断の成功不成功を解析する手法である。その概要を図 2・7 に示す。いずれの手法もディペンダビリティ管理^{6,7)}の重要作業項目であり、システムの設計段階で適用しシステムの潜在的故障または事故を把握し、対策を立てることに利用する。

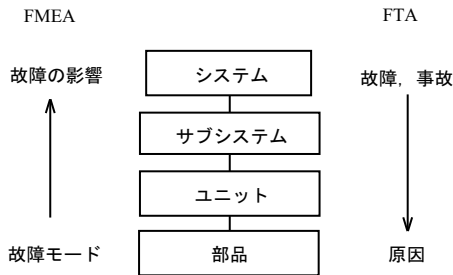


図 2・6 システムの階層と FMEA, FTA の解析方法

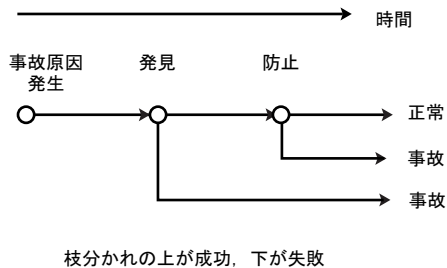


図 2・7 ETA の概要

2-3-2 FTA

(1) 概要

FTA は、1960 年代、米国で大陸間弾道ミサイルの爆発事故を契機として、その安全性を解析する手法として開発された。その後、宇宙開発、原子力、化学プラントの安全性解析で活用され、更に一般システムの故障解析、安全性解析及び事故解析に活用されるようになった。1985 年には、国際規格 (IEC 60812, Ed.1)⁸⁾ が制定され、国際的に共通の手法となった。

FTA では、システムを階層的にとらえ、システムの故障または事故の因果関係を階層に沿って樹形図 (FT 図) に展開する。樹形図の枝分かれの部分には、因果関係の論理構造を示すための論理記号を挿入する。発生原因の確率が分かれば、定量的な解析ができる。システムの重大事故 (爆発、火災、人身事故など) に関する解析は、安全性解析として位置づけられる。

(2) 解析手順

次の手順で解析する。

- (a) トップ事象を選定する。
- (b) システムを階層的 (サブシステム, ユニット, 部品などの階層) にとらえる。
- (c) トップ事象を発生させる第一次階層の故障をあげ、樹形図に展開する。
- (d) 上記の枝分かれ部分に論理記号を記入する。
- (e) 第一次階層の原因となる第二次階層の故障をあげ、樹形図に展開する。
- (f) (d) と同様に、枝分かれ部分に論理記号を記入する。
- (g) 第三次階層, 第四次階層と細分化し、最終階層 (基本事象) まで樹形図に展開する。
- (h) FT 図に基づいて、定性的解析または定量的解析を行い、重要な発生経路を明確にする。
- (i) 重要な発生経路を改善する。

ここで、トップ事象とは、システムの故障または重大事故であり、基本事象は、これ以上細分化できない事象、または、改善の対象とする事象である。FT 図を作成するとき、信頼性ブロック図を参考にすると便利である。この場合、信頼性ブロック図の直列モデルは OR ゲート、並列モデルは AND ゲートに対応させる。

FT 図には、ハードウェアの故障のほか、ヒューマンエラーまたは故障の原因となる環境条件などを記入することができる。

定性的な解析では、最小カット集合を求め、信頼性または安全性の改善対象とする。基本事象の発生確率が既知なら、定量的な解析ができる。トップ事象の発生確率、最小カット集合及びその確率を求める。最小カット集合の確率を確率重要度という。

(3) 事象記号及び論理記号

FT 図は、事象記号及び論理記号を用いて表す。表 2・1 に事象記号及び論理記号を示す。事象記号の中には、故障事象または事故を記入する。論理記号は、枝分かれの部分に挿入する。主要な論理記号は、OR 及び AND であるが、多数決論理など特殊な論理を使用する場合は、論理記号を定義すればよい。







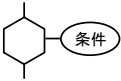
(4) 確率計算

OR ゲートの確率計算は、次式で求める。

$$Pr(A \text{ or } B) = Pr(A) + Pr(B) - Pr(A) \cdot Pr(B) \quad (2 \cdot 16)$$

ここで、A 及び B は、故障事象であり、Pr(・) は、・の発生確率である。通常、故障確率は

表 2・1 事象記号と論理記号の種類

分類	記号	名称	説明
事象記号		故障事象	故障事象記入, 一番上がトップ事象
		基本事象	これ以上分解できない要素
		未展開事象	このレベルで解析を中止または別途解析
		通常事象	通常存在する事象で, 故障事象ではない
論理記号		OR ゲート	下位事象のいずれかが存在すると, 上位事象が発生する
		AND ゲート	下位事象がすべて存在すると, 上位事象が発生する
		条件付ゲート	下位事象と条件が存在すると, 上位事象が発生する

非常に小さいので式 (2・16) 右辺の第 3 項の積の項は, 無視してもよい. AND ゲートの確率計算は, 次式で求める.

$$Pr(A \text{ and } B) = Pr(A) \cdot Pr(B) \quad (2 \cdot 17)$$



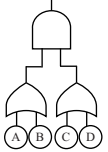
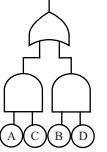
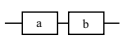

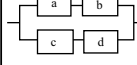
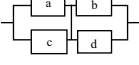
条件付ゲートは, AND ゲートと同じ公式である.

(5) 最小カット集合

最小カット集合とは, システムの正常及び故障の状態を, すべての基本事象の正常及び故障の組合せで表したとき, トップ事象を発生させるための必要最小限の組合せ (集合) である. 最小カット集合は, 複数存在しうる. その場合の FT 図は, 最小カット集合の OR ゲートで表される. したがって, トップ事象の確率は, 最小カット集合の確率の和で近似できる. 最小カットセットを構成する基本事象は, AND ゲートで表せる. 最小カット集合の発生確率は, その集合内の基本要素の発生確率の積である.

最小カット集合の求め方は, トップ事象の発生確率を求める式を基本事象の記号で表し, 論理演算 (ブール代数) で整理したとき, OR で分離されている項として求める. 表 2・2 に, FT 図, 信頼性ブロック図, 最小カット集合及びトップ事象の確率計算の例を示す.

表 2・2 FT 図の例

FT 図				
信頼性ブロック図				
最小カット集合	A, B	AB	AC, AD, BC, BD	AC, BD
トップ事象の確率	A+B	AB	AC+AD+BC+BD	AC+BD

- 注 1. 英小文字は、基本要素の名称、英大文字は故障事象を示す。
 2. トップ事象の確率は、英大文字に故障事象の故障確率の値を代入する。
 3. OR ゲートがある場合のトップ事象の確率は、近似解である。

(6) 信頼性改善の優先順序

信頼性の改善のために着目すべき事象は、最小カット集合を構成する基本事象である。最小カット集合が複数存在するときは、確率重要度が大きい最小カット集合を優先する。最小カット集合内の基本事象の優先順序は、いずれの基本事象を改善しても確率的な改善効果は同等であるから、改善が容易なものを優先する。

一方、次のような考えで改善の優先順序を決める場合がある。一つは、「最後の頼みの綱」となる要素の改善を優先する。例えば、自動操縦要素と手動操縦要素とが冗長系の場合、「最後の頼みの綱」となる手動操縦要素を頑強にする方法である。他の方法は、故障確率の大きい要素を改善する方法である。例えば、ある要素が故障すると、その要素の負荷を残りの要素で分担することになり、残りの要素の故障確率が増加するような場合である。

(7) 構造重要度とその問題点

基本事象の故障確率が未知の場合、基本事象の構造重要度を評価する。構造重要度は、基本事象の正常、故障のすべての組合せを考え、着目する基本事象が故障したとき、システムが正常から故障になる状態の数を評価する方法である。着目する基本事象の構造重要度は、次式で求める。

$$Y = (A - B) / (2^{N-1}) \quad (2 \cdot 18)$$

ここで、Y：着目する基本事象の構造重要度

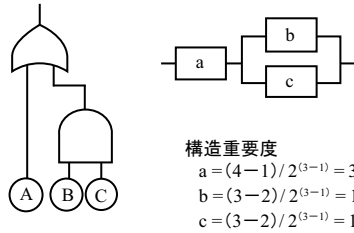
A：その基本事象が故障のとき、システムが故障である基本状態の組合せの数

B：その基本事象が正常のとき、システムが故障である基本状態の組合せの数

N：基本事象の数

である。

図 2・8 に OR ゲートと AND ゲートがある場合の構造重要度を示す．ここで，正常及び故障の組合せの数は，表 2・3 に示す真理表から求めることができる．



英小文字は，要素の名称，英大文字は，要素の故障事象を示す。

図 2・8 FT 図，信頼性ブロック図及び構造重要度

表 2・3 図 2・8 の真理表

a	b	c	T
0	0	0	0
0	0	1	0
0	1	0	0
0	1	1	1
1	0	0	1
1	0	1	1
1	1	0	1
1	1	1	1

注) 0 は，正常，1 は，故障，T は，トップ事象を示す。

構造重要度の評価で注意すべきことは，確率重要度とのかい離である．構造重要度は，正常な状態の組合せの数と故障の状態の組合せの数の差を問題とするので，確率的に見ると，それぞれの状態を同等として評価していることになる．ところが，各要素の故障確率は極めて小さいことが普通であるから，システムの正常と故障の状態の確率は，組合せの状態によって大きな差がある．例えば，図 2・8 について両者の評価の違いを考察する．構造重要度は，a が $3/4$ ，b 及び c は，それぞれ $1/4$ である．一方，確率重要度について考察すると，次のようになる．ここで，a の故障確率を 0.01，b の故障確率を 0.05 と仮定する．b は，a より 5 倍故障しやすい．そこで，この部分を冗長にする．冗長にすると，この部分の故障確率は， 2.5×10^{-3} となる．この回路の最小カット集合は，A，BC である．確率重要度は，a が 0.01，bc が 2.5×10^{-3} である．このように，確率重要度と構造重要度では，評価の方法及びその値に大きな差がある．この例では，ここの要素の故障確率または重要度を評価した結果に基づいて冗長構造を採用したのであるから，改めて構造重要度を評価する意味はない．

一般に，故障確率で比較することが实际的である．基本事象の故障確率が未知の場合は，概数値でもよいから値を仮定して，確率重要度で評価することが望ましい．

(8) ネットワークの FTA

図 2・9 に示すネットワーク (ブリッジ) 回路の FTA を説明する。まず、基本要素のなかで接続要素の数が多い e に注目する。 e が故障の場合、この部分は開いた回路となる。この場合の故障確率は、 $E \cdot (A + B) \cdot (C + D)$ となる。ここで、英大文字は、要素の故障確率、+ 記号は OR、 \cdot 記号は AND を示す。次に、 e が正常の場合、この部分は短絡した回路となる。この場合の故障確率は、 $(1 - E) \cdot (A \cdot C + B \cdot D)$ となる。結局、この回路の故障確率は、両者の和となる。OR ゲートの演算部分を、式 (2・17) の近似式を用いて整理すると、両者の和は、 $AC + BD + ADE + BCE$ となる。最小カット集合は、+ 記号で分離された集合として求める。信頼性改善の優先順序は、最小カット集合の確率重要度の大きい順である。

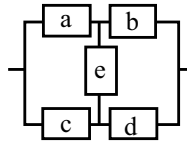


図 2・9 ブリッジ回路

2-3-3 FMEA

FMEA は、システムを構成する構成要素のすべての故障モードをあげ、その故障モードが発生したときの影響を総合的に評価し、影響が重要な故障モードを抽出し、それを信頼性の改善対象とする手法である。1990 年には、国際規格 (IEC 61025, Ed.1)⁹⁾ が制定され、国際的に共通の手法となっている。

FMEA の解析は、表にまとめる。表 2・4 に FMEA シートの例を示す。表には、システムの構成要素の様々な故障モードを記入する。構成要素は、改善対象となる信頼性の改善対象とするレベルでとらえ、部品レベルでもユニットレベルでもよい。例えば、構成要素を部品レベルでとらえると、その基本的な故障モードは、電気部品の場合、短絡、開放、マイナス側ドリフト及びプラス側ドリフトである。機械要素の場合、破壊、摩耗、疲労、腐食、ゆるみなどである。次に、それぞれの故障モードの影響を評価する。故障モードの影響の評価は、次に示すようないくつかの側面で行う。

- (a) 故障モードの発生頻度
- (b) 影響の重要性
- (c) 兆候検出の難易度または対策の余裕度など

表 2・4 FMEA ワークシートの例

要素名	故障モード	想定原因	影 響		評 価 (1)		相 対 リ ス ク	評 価 (2)	危 険 優 先 度	対 策 優 先 度
			サブシステム	システム	a. 影響度	b. 発生頻度				
警報回路	出力なし	断線	警報表示なし	停止	6	4	24	7	168	D

注 対策優先度は、危険優先度で分類する：A(1000・751)、B(750・501)、C(500・251)、D(250・0)

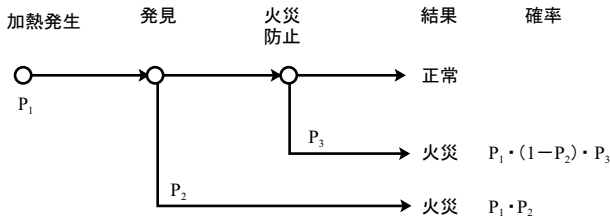
これらの評価には、相対的な評点を与える。評点は 10 段階（点）とし、大きい数字ほど重要な故障とする。例えば、故障モードの発生頻度が 10 点なら頻繁に発生するもの、1 点ならほとんど発生しないものとする。また、影響の重要性が 10 点なら基本機能が喪失し、かつ、人身事故を伴うような重大な影響があるもの、1 点なら軽微な機能低下でほとんど影響がないものとする。検出の難易度についても同様である。

総合的な重要性の評価は、二段階で評価する。第一段階は、(a) と (b) の評点の積である。この値は、相対的なリスクを表す。第二段階は、第一段階の値と (c) の評点の積の値で評価する。この値は、危険優先度 (RPN, risk priority number)⁹⁾ と呼ばれる。改善の優先順序は、いずれの場合も、評価値の大きいものからである。これらの結果から、相対的に重要な故障モードを抽出し、それに対して信頼性向上の対策を立てる。

なお、評点を 10 段階とし、かつ、その積で評価するのは、重要性の差を拡大して評価するためである。相対評価であるから、詳細な分類が困難な場合、5 段階にしてもよい。また、故障モードの評点は、それぞれの発生確率が既知ならその値を用いてもよい。この場合は、FMECA (Failure Mode, Effects and Criticality Analysis, 故障モード影響致命度解析) という。

2-3-4 ETA

ETA は、システム故障が事故に至る過程を解析する手法である。原因の発生から事故に至る一連のシーケンスを、発見または防止の失敗成功の枝分かれで解析する手法である。枝分かれが判断（決定）の分かれ道となることから、決定の木 (Decision tree analysis) ともいわれる。図 2・10 に ETA の例を示す。結果の事象の確率は、経過した枝分かれの確率の積になる。最終的に、火災の発生確率は、結果の事象が火災となる場合の確率の和で求める。



$$\text{火災発生確率} = P_1 \cdot P_2 + P_1 \cdot P_3 - P_1 \cdot P_2 \cdot P_3$$

P_1 : 発熱発生確率, P_2 及び P_3 : 失敗の確率.

図 2・10 ETA の例

参考文献

- 1) 鈴木順二郎, 牧野鉄治, 石坂茂樹, “FMEA/FTA 実施法,” 日科技連出版社, 1982.
- 2) 塩見弘, 島岡淳, 石山敬幸, “FMEA/FT 活用,” 日科技連出版社, 1983.
- 3) 小野寺勝重, “実施 FMEA 手法,” 日科技連出版社, 1998.
- 4) 同上, “実施 FTA 手法,” 日科技連出版社, 2000.
- 5) 同上, “FMEA 手法と実践事例,” 日科技連出版社, 2006.
- 6) IEC 60300-2, “Dependability management-Part 2: Dependability program element and tasks,” 1995.

- 7) JIS C 5750-2, “ディペンダビリティ管理, 第 2 部: ディペンダビリティプログラム要素及びタスク,” 6) の国際一致 JIS, 2000 .
- 8) IEC 61025. Ed.2, “Analysis technique for system reliability - Procedure for fault tree analysis (FTA),” 2006 .
- 9) IEC 60812 Ed.2, “Analysis technique for system reliability - Procedure for failure mode and effects analysis (FMEA),” 2006 .