システムの事故の定性的表現と その信頼性解析[†]

鬼沢 武久*

システムの事故の経過を定性的に表現することは比較的容易である。本論文では、その定性的表現をもとにシステムの信頼性解析を行うには、次の点からファジィ理論の応用が必要であることを述べる。

- 1) 定性的表現には多くのあいまいな語句が含まれる。
- 2) 特にシステムが複雑、大規模になると、機器の故障やヒューマン・エラーがシステムの事故に関係してくるかどうか明確に表現できない場合がある。
- 3) 機器の故障やヒューマン・エラーについて細かく分析していくと解析がむずかしくなる。そのためマクロ的に扱うことが必要であるが、このマクロ的な扱いにもあいまいさが関係してくる。

本論文ではまた、信頼性解析を行うために必要な AND 演算、OR 演算、従属性の演算の他に、機器の故障やオペレータのエラーなど、事象の不都合がシステムの事故につながる可能性などを考慮したあいまいさの演算、また、こういった事象の不都合自体はシステムの事故に直接つながらないが、別の事象の不都合に影響し、システムの事故に関係してくる場合の演算についても述べる。

最後に、オペレータがバルブなどを操作して高压原料の流量を増やす作業についての解析例を示す。

キーワード：システムの信頼性、事故の定性的表現、機器の故障、ヒューマン・エラー、
failure possibility

1. はじめに

従来、機器の信頼性解析では故障率、人間の信頼性解析では過誤率を用いた確率論的手法がとられてきた¹⁾²⁾。しかし確率論的手法をとるにしても以下のような問題点がある。

- ① 故障率、過誤率を推定するには非常に多くのデータが必要である。しかし信頼性解析で扱う事象はごくまれにしか起こらないものであり、起こったとしても公表されないこともあり、実際問題として多くのデータを集めるのは困難な場合が多い。データ不足の場合には、類似した機器や分野

からのデータを参考にして、専門家の工学的判断をもとに基本故障率、基本過誤率を推定している。

- ② 機器の信頼性、人間の信頼性は、例えば機器が置かれている環境、オペレータの作業環境、ストレス・レベルなど多くの要因の影響を受ける。これらの要因の影響を考慮するために基本故障率、基本過誤率に、ある倍率をかけるなど修正をほどこしている。しかし倍率の選択など、この修正も専門家の工学的判断をもとにして行われている。

- ③ 安全基準が明確に確立されてないために、解析結果の判定に専門家の工学的判断が必要になってくる。

このように信頼性の概念には専門家の工学的判断が入り込んでいることがわかる。①の観点からファジィ確率の概念を使って解析する方法が提案されている³⁾⁴⁾⁵⁾。しかしファジィ確率を用いるにし

[†] Qualitative Expression of System Accident and Analysis of System Reliability
Takehisa ONISAWA

* 熊本大学 工学部 共通講座数学教室
Kumamoto University, Faculty of Engineering

でも②③の問題の他に、次の④の問題もある。

④システム全体の信頼性を解析するには機器の信頼性だけでなく、人間の信頼性も考慮しなくてはならない。しかし故障率はその単位が[1/年]などで表されるように、単位時間当りの故障の発生率という形で定義されている¹⁾。一方過誤率は、

$$\frac{\text{ある対象作業でエラーが生じた回数}}{\text{その対象作業でエラーが生じ得る機会の回数}}$$

と定義されている²⁾。このように両者は、その定義からそれぞれ異質のものであり、両者を一緒に扱うのには問題がある。

そこで筆者らは、機器、人間の信頼性を[0, 1]上のファジィ集合である failure possibility, error possibility で表現し、解析する方法⁽⁶⁾⁽⁷⁾⁽⁸⁾、また②に関してはファジィ推論を使って failure possibility, error possibility を導出する方法⁹⁾を提案し、信頼性に影響を及ぼす要因を考慮した信頼性解析を行う¹⁰⁾⁽¹¹⁾などファジィ理論を応用してきた。

本論文では、上述した①から④の他に、事故にいたる経過を定量的に表現するよりは定性的に表現したほうが比較的容易であるとの観点から信頼性解析を考える。そして事故の経過の定性的表現をもとに信頼性解析を行うには、やはりファジィ理論の応用が必要であることを述べるとともに、その手法についても述べる。

Fig. 1 プラントの概略図

2. 信頼性に関する定性的表現とあいまいさ

2.1 事故の経過の定性的表現

Fig.1 にプラントの簡単な図を示す。いま高圧原料が一定流量で容器に流れ込んで安定した反応をしている。そしてバルブを調節して原料の流量を所定流量に増やすようにオペレータが指示を受けたとする。ただし、所定流量より多い(圧力が高い)とこのシステムは暴走する可能性があり、また逆に、所定流量より少ない(圧力が低い)とシステムは停止してしまう可能性がある。オペレータの作業手順は次のようになっている。

1) オペレータは流量計(FIC 指示部)を見ながら流量指示調節器(FIC 操作部)を通して流量調節弁(FCV)を開いて所定の弁開度に保つ。

2) バルブ A の所へ行き、圧力計(PG)を見ながらバルブ A を開き所定の圧力に保つ。

1)2)の両方の作業で所定の弁開度、圧力に保てないとシステムは異常になる可能性がある。この一連の作業で、機器の故障、オペレータのエラーについて定性的に表現すると次のようになる。

(I) FIC 操作部の操作エラーがあるか、または FIC 操作部に故障があるか、または FCV に故障があると作業 1)の失敗につながる**可能性がある**。また、FS, FIC 指示部の故障は FIC 指示部の読み取りエラーに**非常に影響を与え**、FIC 指示部の読み取りエラーは FIC 操作部の操作エラーに**影響を与える**。

(II) バルブ A の操作エラーがあるか、またはバルブ A に故障があると作業 2)の失敗につながる**可能性がある**。また、PG の故障は PG の読み取りエラーに**非常に影響を与え**、このエラーはバルブ A の操作エラーに**影響を与える**。

(III) 作業 1)の失敗と作業 2)の失敗が高圧原料の流量を増やす作業全体の失敗につながる。ただし作業 1)と作業 2)は一連の作業ゆえ、作業 1)の失敗は作業 2)の失敗にやや**影響を与える**。

(IV) 上記の他に以下のことも考慮する必要がある。オペレータは自分が犯したエラーや機器の故障に

気がつき、作業をやり直すこともある。したがって、機器の故障、作業エラーが**直接事故に結びつくとは限らない**。しかし逆に、オペレータはやり直しの際に**別のエラーを犯す可能性もある**。

機器の故障、オペレータのエラーについて定性的に表現することは比較的容易であるが、この定性的表現にはあいまいな語句が多く含まれていることがわかる。また機器の故障、ヒューマン・エラー間の影響(従属)の度合も明確には表現しきれない。システムが複雑、大規模になると機器の故障、エラーがシステムの事故に直接関係してくるかもあいまいになる。さらに人間のとり行動を細かく分析していくと解析上困難な場合が生じてくる。このように大規模・複雑なマン・マシン・システムの信頼性解析ではマクロに分析していく必要がある¹²⁾¹³⁾。しかし、このマクロ的な扱いにはあいまいさが非常に関係してくる。

上記の定性的表現をツリー状に描くと Fig.2 のようになる。なお事象番号とその内容の対応を Table 1 に示す。

基本事象の起こりやすさは、1. で述べた①の観点からあいまいな表現になり、また従属の度合や、機器の故障、ヒューマン・エラーがシステムの事故につながる程度もあいまいな表現になることから、このツリーはファジィ・フォールト・ツリーになる³⁾⁴⁾⁵⁾¹²⁾。この図では、従属の程度、事故につながる程度のあいまいな表現を $R(i)$ ($i=1, 2, \dots, 19$) で表現している。この図を簡単に説明すると次のようになる。FIC の操作エラーを 1

Table 1 事象番号とその内容

事象番号	内 容
3-4	Failure of the Valve A
4-2	Error of Controlling the FIC
4-3	Failure of the FIC(Controllor)
4-4	Failure of the FCV
4-6	Error of Controlling the Valve A
5-2	Error of Reading the FIC
5-3	Failure of the PG
5-4	Error of Reading thd PG
6-1	Failure of the FS
6-2	Failure of the FIC(Indicator)

Fig. 2 ファジィ・フォールト・ツリー

つのサブシステム(A)でのエラー, FIC(操作部)とFCVの故障を1つのサブシステム(B)の故障ととらえ, これらのエラー, 故障が作業1)の失敗に $R(4)$, $R(5)$ の程度に関連している。一方, バルブAの操作エラーを1つのサブシステム(C)でのエラー, バルブAの故障を1つのサブシステム(D)の故障ととらえ, これらのエラー, 故障が作業2)の失敗に $R(6)$, $R(7)$ の程度に関連している。そして, 作業1)の失敗と作業2)の失敗が, 高圧原料の流量を増やす作業全体の失敗にそれぞれ $R(1)$, $R(2)$ の程度に関連しているが, 作業1)の失敗が作業2)の失敗に $R(3)$ の程度で影響している。

2.2 信頼性に影響を与える要因と信頼性との関係の定性的表現

機器や人間の信頼性は多くの要因の影響を受ける。しかし両者の関係は必要十分の関係とは限らず, 明確に表現できるものではない。しかしマクロ的にながめ, 両者の関係を定性的に表現することは比較的容易である。例えば, 機器の信頼性に影響を与える要因として, 「機器が置かれている環境」「保守点検の質」「稼働時間」, 人間の信頼性に影響を与える要因として, 「作業環境」「オペレータの熟練度」「マン・マシン・インタフェースの質」「オペレータの心理的ストレス・レベル」を考えると, 両者の関係は次のように表現できる。

機器が置かれている環境(EE)

環境が良ければ, 機器の信頼性は高い。

環境が悪ければ, 機器の信頼性は低い。

保守点検の質(EM)

保守点検の質が良ければ, 機器の信頼性は高い。

保守点検の質が悪ければ, 機器の信頼性は低い。

稼働時間(ET)

稼働時間が短ければ, 機器の信頼性は高い。

稼働時間が長ければ, 機器の信頼性は低い。

作業環境(HE)

作業環境が良ければ, 人間の信頼性は高い。

作業環境が悪ければ, 人間の信頼性は低い。

マン・マシン・インタフェースの質(HI)

インタフェースの質が良ければ, 人間の信頼性は高い。

インタフェースの質が悪ければ, 人間の信頼性は低い。

オペレータの熟練度(HC)

熟練度が高ければ, 人間の信頼性は高い。

熟練度が低ければ, 人間の信頼性は低い。

オペレータの心理的ストレス・レベル(HS)

ストレス・レベルが高ければ, 人間の信頼性は低い。

ストレス・レベルが適度であれば, 人間の信頼性は高い。

ストレス・レベルが低ければ, 人間の信頼性はやや低い。

信頼性と要因との関係を表した定性的表現にもあいまいな語句が多く含まれていることがわかる。

なお, 要因の信頼性に与える影響の大きさによっては, 「非常に」などの修飾語をつけて表現することもできる。例えば, マン・マシン・インタフェースの質が人間の信頼性に与える影響の大きさが大きいと判断されれば,

インタフェースの質が良ければ, 人間の信頼性は非常に高い。

インタフェースの質が悪ければ, 人間の信頼性は非常に低い。

のように表現できる。

この定性的表現に含まれるあいまいさはファジィネスに根ざすものであり, 定性的表現をもとにして信頼性を解析するにはファジィ理論の応用が必要である。そこで次節では, 解析にあたって必要な従来の方法⁶⁾⁻¹¹⁾の他に, 新しく導入する考えについても述べる。

3. 信頼性の表現と解析

3.1 Failure Possibility

機器, 人間の信頼性を $[0, 1]$ 上のファジィ集合

$$F(x) = \frac{1}{1 + 20 \times |x - x_0|^m} \quad (1)$$

で表現し、機器の場合 failure possibility, 人間の
場合 error possibility と呼ぶ。ただし、 x_0 は(1)式
が表すファジィ集合のグレードを1にするパラ
メータであり、 m はあいまいさを表すパラメータ
である。 $x \leq x_0$ のとき $m = m_L$, $x \geq x_0$ のとき $m = m_U$
と表す。これらのパラメータは以下のようにし
て求める。

(I) パラメータ x_0 の推定

故障率, 過誤率は通常, $[P_L, P_M, P_U]$ のように
三項組で与えられている。 P_M は基本故障率, 基本
過誤率の最良の推定値, P_L はその下限値, P_U はそ
の上限値である。パラメータ x_0 は, P_M と信頼性に
影響を与える要因の評価をもとにして推定する。

2.2 で述べた信頼性と要因の関係の定性的表現を
Fig.3 のようにファジィ集合で表現する。図中の
 x^* は,

$$x^* = f(P_M) \\ = \frac{1}{1 + (K \times \log(1/P_M))^3} \quad (2)$$

である。ただし、 $P_M \neq 0$, $P_M = 0$ のとき, $x^* = 0$ と
する。 $K (\geq 0)$ をパラメータとして(2)式を図示す
ると Fig.4 のようになる¹⁴⁾。この図からわかるよ
うに, K が大きくなるにつれて, 同じ P_M でも x^*
の値は小さくなり, 楽観的に評価していることにな
る。パラメータ K は主観的な安全基準を表して

Fig. 3 信頼性と各要因との関係

Fig. 4 いろいろな K に対する x^* と P_M との対応

おり、これをもとにして基本故障率，基本過誤率を評価していることになる¹⁴⁾。Fig.3 で、矢印の左側はそれぞれの要因の評価のファジィ集合(「良い」「悪い」など)，矢印の右側は信頼性の評価(「高い」「低い」など)を(1)式のパラメータ x_0 に置き換えて表現したファジィ集合である。各要因の評価 x_{ij} が与えられたとき、 x_0 を以下の手順で求める。矢印の左側のファジィ集合を表すメンバーシップ関数を g_{ij} ，右側のファジィ集合を表すメンバーシップ関数を h_{ij} とする。

- i) $w_{ij} = g_{ij}(x_{ij})$ なる w_{ij} を求める。
- ii) $w_{ij} = h_{ij}(x_{ij})$ なる x_{ij} を求める。
- iii) 重み付き平均を求める。

$$x_0 = \frac{\sum_{i,j} w_{ij} \times x_{ij}}{\sum_{i,j} w_{ij}} \quad (3)$$

この手順で x_0 を求めると、Fig.3 で表したファジィ集合は次のような意味を持つ。

機器の場合

- 1) 各要因の評価が最良の場合 x_0 は 0 に、最悪の場合 x_0 は 1 になる。
- 2) 各要因の評価が普通(0.5)の場合 x_0 は x^* になる。
- 3) 各要因の評価が普通くらいの場合、要因の評価が少し変化しても x_0 に与える影響は少ないが、各要因の評価が良いか悪い場合は、要因の評価の変化が x_0 の変化に大きく影響を与える。

オペレータの場合

- 1) 各要因の評価が最良の場合 x_0 は x^* に、最悪の

場合 x_0 は 1 になる。人間の場合、信頼性に影響を与える要因をどんなに良くしても、信頼性には限度があることを示している。

2) ストレス・レベルと信頼性との関係を表しているファジィ集合で x' は

$$x' = \frac{1+x^*}{2} \quad (4)$$

である。これはストレス・レベルが低いと信頼性は下がるが、ストレス・レベルが高いときほどではなく、文献 15) では基本過誤率を 2 倍にしていることを参考にしている。

3) 人間には、作業条件が少し悪くても作業能率を著しく低下させないくらいの柔軟性があるとの配慮から、メンバーシップ関数の形を決めている。

このように求めた x_0 は、故障率，過誤率，信頼性に影響を与える要因などの主観的評価をもとにした信頼度を表している。

(II) パラメータ m の決定

パラメータ m は三項組 $[P_L, P_M, P_U]$ をもとに決める。文献 16) によると故障率とその定性的表現の対応を 10^{-3} : improbable, 10^{-4} : very improbable, 10^{-5} : extremely improbable, 10^{-5} より小: excluded as far as one can judge next to impossible, 0: impossible, としている。本論文では、故障率，過誤率に対応させて定性的表現をせずに、故障率，過誤率を(2)式で評価した x^* に対応させて定性的表現をする。定性的表現は文献 16) より細かく分けて Table 2 のようにし、クラス分けをする。Table 2 には、各クラスでの x^* の

Table 2 x^* のクラス分けとその定性的表現

クラス	x^* の範囲	定性的表現	x^* の代表値とそれに対応する P_M
C_1	1.0	Certain	—
C_2	0.9-1.0	Most Probable	0.95(7.5-2*, 1.8-1)**
C_3	0.7-0.9	Quite Probable	0.8(1.3-2, 5.5-2)
C_4	0.5-0.7	Probable	0.6(2.4-3, 1.8-2)
C_5	0.3-0.5	Rather Improbable	0.4(3.7-4, 5.1-3)
C_6	0.2-0.3	Improbable	0.25(4.7-5, 1.3-3)
C_7	0.1-0.2	Highly Improbable	0.15(4.5-6, 2.7-4)
C_8	0.05-0.1	Extremely Improbable	0.075(1.2-7, 2.4-5)
C_9	0.0-0.05	Excluded as far as one can judge next to impossible	0.025(6.7-11, 1.7-7)
C_{10}	0.0	Impossible	—

* 7.5×10^{-2} と読む。

** 括弧内の値は、各クラスの代表値に対応する故障率、あるいは過誤率を示す。前者の値は、 K が1/3のときの、後者の値は、 K が1/2のときの故障率、あるいは過誤率である。

代表値とそれに対応する P_M の値も、2種類の安全基準の場合について示してある。なお、 x^* の代表値は各クラスの x^* の範囲の中間値としている。この表からわかるように、主観的な安全基準 K によって、同じ値の故障率、過誤率でも対応する定性的表現が異なっている。

i) $k_L = P_M / P_L$, $k_U = P_U / P_M$ とし、 m_L を決めるときには k_L を使い、 m_U を決めるときには k_U を使う。以後 k_L もしくは k_U を k と表す。

ii) 不確実性の4つの範囲を $k \leq 3$, $3 < k \leq 5$, $5 < k \leq 10$, $10 < k$ のように定める。これは Table 3¹⁵⁾ を参考にしている。

Table 3

過誤率の不確実性の範囲の一般的なガイドライン

過誤率	下限値	上限値
$0.01 < P_M$	$P_M/5$	$2 \times P_M \sim 5 \times P_M$
$0.001 < P_M < 0.01$	$P_M/3$	$3 \times P_M$
$P_M < 0.001$	$P_M/10$	$10 \times P_M$

iii) クラス C_5 で、 $k \leq 3$ に対して $m=2$, $3 < k \leq 5$ に対して $m=2.5$, $5 < k \leq 10$ に対して $m=3$, $10 < k$ に対して $m=3.5$ のように定める。

クラス C_n で x^* の代表値を x_n^* とする。またクラ

ス C_n の failure possibility, あるいは error possibility を F_n , $F_n(x_n^*)=1$ とする。

iv) $x_n^* = f(P_{Mn})$ なる P_{Mn} を求める。

v) m_U を決めるときには $x_n = f(P_{Mn} \times 10)$ とし、各クラス同じ $k (=k_U)$ の範囲で

$$F_n(x_n) = F_5(x_5) \quad (n=2, 3, \dots, 9) \quad (5)$$

が成り立つような m を m_U とする。

vi) m_L を決めるときには $x_n = f(P_{Mn}/10)$ とし、各クラス同じ $k (=k_L)$ の範囲で(5)式が成り立つような m を m_L とする。

(5)式は、failure possibility, あるいは error possibility における x_n のグレードが各クラス同じ k の範囲で等しくなるように m を決めることを示している。各クラスでの m の値は、クラス C_5 の同じ k の範囲であらかじめ決められた値を基準にして決められている。

$K = 1 / \log(1/5 \times 10^{-3})$ のときの m の値を Table 4 に示す。さらにオペレータの場合には、Table 3 を参考にしてアンダーラインを引いた値を使う。ただし、 $k > 10$ の範囲の値は、過誤率が非常にあいまいであると評価された場合に使う。

Table 4 パラメータ m

クラス	$k \leq 3$	$3 < k \leq 5$	$5 < k \leq 10$	$10 < k$
$C_2 m_U$	2.7	<u>3.3</u>	4.0	<u>4.7</u>
m_L	2.7	<u>3.3</u>	4.0	<u>4.7</u>
$C_3 m_U$	1.3	<u>1.7</u>	2.0	<u>2.3</u>
m_L	3.1	<u>3.8</u>	4.6	<u>5.4</u>
$C_4 m_U$	<u>1.9</u>	2.4	2.9	<u>3.4</u>
m_L	<u>2.6</u>	3.3	3.9	<u>4.6</u>
$C_5 m_U$	<u>2.0</u>	2.5	3.0	<u>3.5</u>
m_L	<u>2.0</u>	2.5	3.0	<u>3.5</u>
$C_6 m_U$	1.6	1.9	<u>2.3</u>	<u>2.7</u>
m_L	1.5	1.9	<u>2.3</u>	<u>2.7</u>
$C_7 m_U$	1.1	1.4	<u>1.7</u>	<u>1.9</u>
m_L	1.2	1.5	<u>1.8</u>	<u>2.1</u>
$C_8 m_U$	0.8	1.0	<u>1.1</u>	<u>1.3</u>
m_L	0.9	1.1	<u>1.4</u>	<u>1.6</u>
$C_9 m_U$	0.5	0.6	<u>0.7</u>	<u>0.9</u>
m_L	0.7	0.8	<u>1.0</u>	<u>1.2</u>

クラス C_1, C_{10} は次のように定義される。

$$F_1(x) = \begin{cases} 1, & x=1 \\ 0, & x \neq 1 \end{cases} \quad (6)$$

$$F_{10}(x) = \begin{cases} 0, & x \neq 0 \\ 1, & x=0 \end{cases}$$

パラメータ x_0, m の求めかたからわかるように、故障率、過誤率、信頼性に影響を与える要因などを評価して(1)式が表すファジィ集合を求めているため、信頼性の観点からすると、failure possibility, error possibility は一緒に扱うことができる。本論文では両者まとめて扱うため、ファジィ集合(1)を failure possibility と呼ぶことにする。解析でこのファジィ集合を使うのは、1. で述べた①の観点の他に、手元にある事故に関する情報、あるいは合理的に収集できる情報から評価できるのは、そのような事故が起こる可能性だけである¹⁷⁾という観点にも立っている。(1)式で特に $F(0)$ は、機器は絶対に故障しない、あるいはオペレータは絶対にエラーしない可能性の度合を、 $F(1)$ は、機器は確実に故障する、あるいはオペレータは確実にエラーする可能性の度合を表している

と解釈できる。

3.2 信頼性解析

Fig.2 で示したようなファジィ・フォールト・ツリーを解析するには、failure possibility の AND 演算, OR 演算, 従属性の演算の他に、機器の故障やオペレータのエラーが事故につながる可能性を考慮したあいまいさの処理が必要となる。また、機器の故障自体はシステムの事故に直接つながらないが、オペレータが故障に気がつかずにこの機器を使って作業する場合、機器の故障が結果的にオペレータのエラーに影響を与えて、システムの事故に関係してくる場合がある。ただし、オペレータは機器が故障していなくてもエラーする可能性はある。この場合の処理についても考慮しなくてはならない。以下、機器の故障、オペレータのエラーを事象と呼ぶことにする。

1) AND 演算

2つの事象が互いに独立で、2つの事象が起こると事故となるとき、その failure possibility を次式と拡張原理¹⁸⁾を使って求める。

$$H(x, y) = \frac{1}{1 + \{((1-x)/x)^{1/3} + ((1-y)/y)^{1/3}\}^3} \quad (7)$$

ただし、 $0 < x, y \leq 1$ で $H(0, y) = H(x, 0) = 0$ 。関数 H は故障率、過誤率の and 演算と対応がつく。事象 A, B の故障率、あるいは過誤率をそれぞれ P_{MA}, P_{MB} とすると、

$$f(P_{MA} \times P_{MB}) = H(f(P_{MA}), f(P_{MB})) \quad (8)$$

が成り立つ。ただし(2)式の K は同じ値、つまり、 P_{MA}, P_{MB} を同じ基準で評価するとする。

2) OR 演算

2つの事象が互いに独立で、少なくとも1つの事象が起こると事故となるとき、その failure possibility は次式と拡張原理を使って求める。

$$G(x, y) = \frac{\{(x/(1-x))^3 + (y/(1-y))^3\}^{1/3}}{1 + \{(x/(1-x))^3 + (y/(1-y))^3\}^{1/3}} \quad (9)$$

ただし, $0 \leq x, y < 1$ で $G(1, y) = G(x, 1) = 1$ 。

関数 G は故障率, 過誤率の or 演算と完全な対応はつかないが, 近似的な対応はつく。

$$f(P_{MA} + P_{MB} - P_{MA} \times P_{MB}) \cong G(f(P_{MA}), f(P_{MB})) \quad (10)$$

ただしこの場合も, (2)式で P_{MA}, P_{MB} を同じ基準で評価するとする。

3) 従属性の演算

(I) 事象 A と事象 B が起こったとき事故となるが, 事象 A が起こると事象 B が起こりやすくなる場合を考える。つまり, 事象 A と事象 B が独立とは考えられない場合である。フォールト・ツリーで表すと Fig.5(a)に相当する。一方, Fig.5(b)に示すような場合は考えない。なぜならこの場合, 事象 A が起きてしまえば, 従属性の有無にかかわらずシステムとしては機能しなくなるため, 従属性を考えても意味がないからである。

Fig. 5 従属性 I

事象 A, B の failure possibility をそれぞれ F_{MA}, F_{MB} , 従属性の程度を R とする。

i) 事象 A の発生が事象 B に影響する場合のシステム全体の failure possibility F_B' を「 F_A AND R 」で求める。

$$F_B' = H(F_A, R) \quad (11)$$

ii) 事象 A の発生が事象 B に影響しない場合のシステム全体の failure possibility は以下のようにして求める。従属性が完全従属でないかぎり, 事象 A の発生がいつも事象 B に影響するとは限らない。事象 A の failure possibility のうち事象 B に影響しない分は,

$$F_A = G(F_A', F_B') \quad (12)$$

の F_A' と考えることができる。つまり, 事象 A (F_A) は事象 B に影響するか (F_B'), しないか (F_A') である。この場合のシステム全体の failure possibility は

$$F' = H(F_A', F_B) \quad (13)$$

で求められる。つまり F' は, 事象 B に影響せずに事象 A が発生し (F_A'), かつ事象 A の発生の影響を受けずに事象 B が発生する (F_B) 場合を考えていることを意味している。

iii) i) と ii) を合わせた全体の failure possibility は

$$F = G(F', F_B') \quad (14)$$

で求められる。つまり F は, 事象 A の影響を受けて事象 B が発生する (F_B') か, 事象 A の影響を受けずに事象 B が発生する (F') 場合を考えていることを意味している。

上記の考えを故障率, 過誤率を使った場合と対応させてみる。上記 i), ii) はお互いに排他的と考えられるので, 従属性を考えた全体の故障率, 過誤率は

$$\begin{aligned} P_M &= P_{MA} \times R(B|A) \\ &\quad + P_{MA} \times (1 - R(B|A)) \times P_{MB} \\ &= P_{MA} \times R(B|A) + (P_{MA} - P_{MA} \times R(B|A)) \\ &\quad \times P_{MB} \end{aligned} \quad (15)$$

で与えられる。ここで P_{MA}, P_{MB} は事象 A, B の故障率, あるいは過誤率であり, $R(B|A)$ は事象 A が発生したときに事象 B が発生する割合である。(15)式の第一項目は(11)式に, (15)式の第二項目のカッコ内は(12)式に, (15)式の第二項目全体は(13)式に, (15)式全体は(14)式にそれぞれ対応している。

(II) (I)の場合と違って, 事象 A が発生しても事故に直接つながらないが, 事象 B に影響し, 事象 B が発生しやすくなり, 事象 B が発生したとき

に事故につながる場合を考える。ただし、事象 A が発生しなくても事象 B が発生すれば事故となる。例えば、ある機器を使用しながら作業をする場合、使用機器に故障が起こってもシステムの事故に直接影響しないが、その機器を使用しながら作業を行うため、オペレータはエラーしやすくなる。一方、機器が故障していなくてもオペレータはその作業でエラーする可能性はある。このときの failure possibility は、

$$F = G(F_A', F_B) \quad (16)$$

で求める。ただし、 $F_A' = H(F_A, R)$ である。この考えは、事象 A の発生が R の程度で事象 B に影響するため、この部分を事象 B の failure possibility に OR 演算の意味で加算しようとするものである。したがって(16)式の F は、事象 A の従属性を考えた事象 B の failure possibility である。

なお、これらの従属性の演算も拡張原理を使って計算する。

4) その他のあいまいさの処理

2. で述べたように、機器の故障やオペレータのエラーが直接事故に結びつくとはかぎらない。また、人間は自分の犯したエラーに気がついてやり直すことがある。しかしそのやり直しの際に別なエラーをする可能性もある。しかしこれらを細かく分析していったら解析すると困難な場合が多い。そこでマクロ的に処理する必要がある。このマクロ的な扱いにもあいまいさが関連してくる。

事象の failure possibility を F 、機器の故障やオペレータのエラーが事故に結びつく可能性、やり直しの際に別なエラーをする可能性を表すファジィ集合を R とすると、これらの可能性を考慮した failure possibility を「 F AND R 」で求める。つまり $H(F, R)$ を拡張原理を用いて求めることにする。例えば、完全に事故に結びつかない、あるいはエラーは完全にリカバーできると評価されれば、 $H(F, R)$ は 0 になる。逆に完全に事故に結びつく、エラーには全く気がつかないと評価されれば、 $H(F, R)$ は F となる。

4. 評価

4.1 Failure Possibility の評価

事故に関する定性的表現をもとに解析して得られた failure possibility F を次の観点から評価する。 F の α -カットを $F(\alpha) = (x_1(\alpha), x_2(\alpha))$ とする。

(I) F の最大グレードを与える x_0

$$J_1 = x_0 \quad (17)$$

(II) 故障、エラー、事故の潜在性

J_2 を以下のように定義する。

$$J_2 = \frac{\int_0^\beta (x_2(\alpha) - 0.5) \alpha d\alpha}{\int_0^1 (1 - 0.5) \alpha d\alpha} \quad (18)$$

ただし $x_2(\beta) = 0.5$ である。

J_2 は $J_1 < 0.5$ のとき評価する。failure possibility の $x_2(\alpha) \geq 0.5 (\alpha \in [0, \beta])$ の部分が評価されているため、 J_2 は故障、エラー、事故の潜在性を表していると解釈できる。 J_2 が大きいと、たとえ J_1 が小さくとも事故などの潜在性が大きいといえる。

(III) failure possibility のあいまいさ

J_3 を以下のように定義する。

$$J_3 = \frac{\int_0^1 (x_2(\alpha) - x_0) \alpha d\alpha}{\int_0^1 (1 - x_0) \alpha d\alpha} \quad (19)$$

ただし $x_2(\alpha) \geq x_0 (\alpha \in [0, 1])$ 。

J_3 は failure possibility のあいまいさを評価している。従って J_3 が大きいと、 J_1 は確信を持って評価できないことになる。

(IV) 相対的潜在性と相対的あいまいさ

J_2' 、 J_3' を以下のように定義する。

$$J_2' = \frac{\int_0^\beta (x_2(\alpha) - 0.5) \alpha d\alpha}{\int_0^{\beta'} (x_{s2}(\alpha) - 0.5) \alpha d\alpha} \quad (20)$$

ただし $x_{s2}(\beta') = 0.5$ 。

$$J_3' = \frac{\int_0^1 (x_2(\alpha) - x_0) \alpha d\alpha}{\int_0^1 (x_{s2}(\alpha) - x_0) \alpha d\alpha} \quad (21)$$

(20) (21) 式の分母は、 $J_1 = x_0$ が属するクラスの標

準の failure possibility F_s についてである。標準の failure possibility とは (1) 式のメンバーシップ関数で $x_0 = J_1$ であり, m_L, m_U の値は, x_0 が属するクラスで $3 < k \leq 5$ のときの m の値である。 F_s の α -カットを $F_s(\alpha) = (x_{s1}(\alpha), x_{s2}(\alpha))$ とする。(20) (21) 式は, x_0 が属するクラスの中での相対的な評価を表している。これらの評価を図で示すと Fig.6 のようになる。

Fig. 6 Failure Possibility の評価

Fig.6(a) は, J_1, J_2, J_3 についてであり, Fig.6(b) は, J_2', J_3' についてである。 J_2, J_3, J_2', J_3' は, それぞれハンチングした部分の重み付き面積比を考えている。

4.2 要因の重要性の評価

フォールト・ツリーの各基本事象の発生が, 頂上事象の発生にどれだけ影響しているかをみる概念として構造重要度¹⁹⁾がある。文献 20) では, 基本事象がファジィ事象として定義された場合の構造重要度として, ファジィ積分を使った fuzzy importance が提案されている。

本論文では, 2.2 で述べた要因の評価が, ファジィ・フォールト・ツリーの頂上事象の failure possibility に与える影響を評価するために, 要因の重要性を考える。この評価は, 信頼性向上のためにどの要因を改善したらよいかを選択するのに重要である。いま $S(F)$ を

$$S(F) = \int_0^1 (x_1(\alpha) + x_2(\alpha)) \alpha d\alpha \quad (22)$$

のように定義する。ただし $F(\alpha) = (x_1(\alpha), x_2(\alpha))$ は, failure possibility F の α -カットである。この $S(F)$ を使って

$$J_4(l_i) = \frac{S(F_l + \Delta F_{li}) - S(F_l)}{S(F_l + \Delta F_{li}) - S(F_l)} \quad (23)$$

を定義する。ただし, F_l はファジィ・フォールト・ツリーの頂上事象の failure possibility, F_l は l 番目の基本事象の failure possibility である。 ΔF_{li} は, l 番目の基本事象の i 番目の要因の評価を変えたときの failure possibility の変化分であり, ΔF_{li} の変化による頂上事象の failure possibility の変化分を ΔF_{li} とする。(23) 式は感度解析を意味しており²¹⁾, $J_4(l_i)$ が大きければ, それだけ l 番目の事象の i 番目の要因の重要性が大きいことになる。したがって, $J_4(l_i)$ が大きく, l 番目の事象の i 番目の要因の評価が低ければ, この要因を改善する必要がある。また, $J_4(l_i)$ が大きく, l 番目の事象の i 番目の要因の評価が高ければ, この要因の状態を維持し, 常に監視する必要がある。

5. 解析例

Fig.2 のフォールト・ツリーを解析する。解析の際に必要な情報は, 故障率, 過誤率, 安全基準, 各要因と信頼性との関係, 各要因の評価値である。

Table 5 故障率,あるいは過誤率,各要因の評価値とパラメータ K と m

機器の故障

事象番号	故障率 P_L, P_M, P_U	要因の評価値 x_{EE}, x_{EM}, x_{ET}	K	m_U, m_L
<u>3-4</u>	1-3, 5-3, 1-2*	0.3, <u>0.5</u> , 0.3	$1/\log(1/P_3)$	2.5, 2.0
<u>4-3</u>	2-2, 3.57-2, 5-2	0.4, <u>0.5</u> , 0.3	$1/\log(1/P_1)$	2.0, 2.0
<u>4-4</u>	8-4, 5.782-3, 2-2	0.3, <u>0.5</u> , 0.3	$1/\log(1/P_3)$	1.7, 4.6
5-3	1-1, 1-2, 3-2	0.3, 0.5, 0.2	$1/\log(1/P_2)$	3.0, 2.0
<u>6-1</u>	8-4, 1.752-3, 1-2	0.3, <u>0.5</u> , 0.2	$1/\log(1/P_4)$	3.1, 2.5
6-2	2-2, 4.06-2, 6-2	0.4, 0.5, 0.3	$1/\log(1/P_1)$	2.0, 2.0

ヒューマン・エラー

事象番号	過誤率 P_L, P_M, P_U	要因の評価値 $x_{HE}, x_{HI}, x_{HC}, x_{HS}$	K	m_U, m_L
4-2	1-4, 5-4, 1-3	0.8, 0.8, 0.8, 0.4	$1/\log(1/P_3)$	2.0, 3.5
4-6	1-4, 5-4, 1-3	0.8, -, 0.8, 0.4	$1/\log(1/P_4)$	2.0, 3.5
<u>5-2</u>	1-3, 3-3, 1-2	<u>0.8</u> , <u>0.8</u> , 0.8, 0.4	$1/\log(1/P_3)$	3.5, 2.0
<u>5-4</u>	1-3, 3-3, 1-2	<u>0.8</u> , <u>0.8</u> , 0.8, 0.4	$1/\log(1/P_3)$	3.5, 2.0

* 1×10^{-2} と読む。 $P_1 = 5 \times 10^{-2}$, $P_2 = 10^{-2}$, $P_3 = 5 \times 10^{-3}$, $P_4 = 10^{-3}$.

ここで使う故障率, 過誤率, 安全基準, 各要因の評価値を Table 5 に示す。なおこの表には, 参考のために m_U, m_L を示してある。また, 要因と信頼性との関係を表す定性的表現は 2.2 で述べたものと同じとし, その定量的表現は Fig.3 を使うものとする。また, 従属性の程度, 機器, オペレータのエラーが事故につながる可能性については, Fig.2 の各 $R(i)$ と Fig.7 に示したファジィ集合との対応を Table 6 に示す。Fig.7 に示したファジィ集合を用いることの効果を従属性の場合について説明する。Fig.8(a) に示したフォールト・ツリーを, 事象 A, B の failure possibility (F_A, F_B) を Fig.8(b) として, 完全従属 (R_1), 非常に高い従属 (R_2), 高い従属 (R_3), 中程度の従属 (R_4), 低い従属 (R_5), そして従属性のない場合についてそれぞれ解析した結果を Fig.8(c) に示す。従属性の程度が低くなるにつれて, failure possibility のグレードが 1 となる x_0 の値は小さくなり, また, 完全従属から高い従属までは, $x \leq x_0$ の部分での failure possibility のふくらみが大きくなっていることが

Fig. 7 従属性や事故につながる可能性を表したファジィ集合のメンバーシップ関数

Table 6 Fig.2の $R(i)$ と Fig.7の R_j の対応

$R(i)$	R_j	$R(i)$	R_j
$R(1)$	R_1	$R(11)$	R_1
$R(2)$	R_1	$R(12)$	R_3
$R(3)$	R_5	$R(13)$	R_1
$R(4)$	R_3	$R(14)$	R_2
$R(5)$	R_2	$R(15)$	R_1
$R(6)$	R_3	$R(16)$	R_2
$R(7)$	R_2	$R(17)$	R_1
$R(8)$	R_3	$R(18)$	R_1
$R(9)$	R_1	$R(19)$	R_1
$R(10)$	R_1		

わかる。逆に従属性が高いほど、 $x \geq x_0$ の部分の failure possibility が、完全従属の場合の failure possibility に一致する部分が多いことがわかる。

Fig.9 に Fig.2 のツリーを解析した結果を示す。

$J_1 = 0.146$ でクラス C_7 (highly improbable) に属し、潜在性(J_2)、あいまいさ(J_3)も比較的小さく、良い信頼性を示している。この状態で重要性の大きい要因を選択する。選択された要因は、Table 5 の事象でアンダーラインを引いた事象の要因である。事象(3-4)(4-3)(4-4)の要因は、これらの事象が比較的 OR 結合で作業の失敗につながっているため選択されている。また、事象(4-2)に影響を与える事象(4-1)に OR 結合でつながっている事象(5-2)が選択されている。一方、事象(5-2)に影響を与える事象(6-1)(6-2)のうち、事象(6-1)が選択されている。この事象が選択されたのは、事象(6-2)と比べて事象(6-1)の方が、信頼性評価が低く、failure possibility のあいまいさも大きく、事象(5-1)の failure possibility はほとんど事象(6-1)の failure possibility で決まるためである。事象(5-4)に影響を与える事象(5-3)が選択されずに事象(5-4)が選択されているのも同じ理由である。

選択された事象のうち機器に関しては(事象(3-4)(4-3)(4-4)(6-1))、評価値が1番低い環境条件は容易に変えられないため、2番目に低い保守点検を厳重に行うとして、その評価値を高く(0.8)する。一方、オペレータに関しては(事象(5-2)(5-4))、作業環境、インタフェースをさらに改良するとして、その評価値を最良(1)にする。その結果を Fig.10 に示す。それぞれの評価値($J_1, J_2, J_3, J_2', J_3'$)が小さくなり、改良されていることがわかる。

6. おわりに

本論文では、

- ① システムの事故にいたる経過を定性的に表現することは比較的容易であり、これをもとにした信頼性解析を考える必要があること
- ② しかし、システムの事故にいたる経過を定性的

Fig. 8 従属性 I についての例

Fig. 9 解析結果 I

Fig. 10 解析結果 II

に表現するとあいまいな語句が多く使われること
 ③ 機器の故障やヒューマン・エラーについて細かく分析するよりはマクロ的に扱うことが必要であり、そこにもあいまいさが関係してくること

④ 故障やヒューマン・エラーのマクロ的な見方や事故の定性的表現をもとに信頼性を解析していくにはファジィ理論の応用が必要であること

を述べた。そしてさらに本論文では、故障やヒューマン・エラーについての定性的表現をもとに信頼性を解析するにあたって以下の点を新たに導入した。

I. 機器の故障やオペレータのエラーが必ずしもシステムの事故につながるとは限らないこと、またオペレータは自分が犯したエラーに気がついてやり直しをする可能性もあることなどのあいまいさの処理。

II. 機器の故障やオペレータのエラー自体はシステムの事故に直接つながらないが、これらの不都合が別の機器の故障やオペレータのエラーに影響を与えて、システムの事故に関係してくる場合の従属性。しかも、後者は前者に影響を受けずに発生することもあり、そのときもシステムの事故につながる可能性がある場合である。

今後の課題としては、本論文で述べた内容を中心とした信頼性評価システムを構築することが考えられる。このシステムへの入力としては、故障率、過誤率などの数値や、定性的表現に含まれるあいまいな表現を受け入れるようにすることが必要である。

参 考 文 献

- 1) 塩見弘：故障解析と診断，日科技連，1979.
- 2) 林喜男：人間信頼性工学 — 人間エラーの防止技術，海文堂，1984.
- 3) 野間圭介，田中英夫，浅居喜代治：ファジィ確率を用いる欠陥関連樹木法について，人間工学，Vol.7, No.6, 291-297, 1981.
- 4) H.Tanaka, L.T.Fan, F.S.Lai and K.Toguchi : Fault-Tree Analysis by Fuzzy Probability, IEEE Trans. on Reliability, Vol. R-32, No. 5, 453-457, 1983.
- 5) F.S.Lai, S.Shenoi and L.T.Fan : Fuzzy Fault Tree Analysis : Theory and Application in : A. Kandel and E.Avni, Eds., Engineering Risk and Hazard Assessment, Vol. 1, CRC Press, 113-137, 1988.
- 6) 鬼沢武久，菅野道夫：あいまい論理を用いた故障解析，計測自動制御学会論文集，Vol. 20, No. 6, 498-505, 1984.
- 7) T.Onisawa : An Approach to Human Reliability in Man-Machine Systems Using Error Possibility, Fuzzy Sets and Systems, Vol. 27, No. 2, 89-103, 1988.
- 8) T.Onisawa and Y.Nishiwaki : Fuzzy Human Reliability Analysis on the Chernobyl Accident, Fuzzy Sets and Systems, Vol. 28, No. 2, 115-127, 1988.
- 9) 鬼沢武久：ファジィ推論を用いた人間の信頼性評価，計測自動制御学会論文集，Vol. 24, No. 12, 1312-1319, 1988.
- 10) T.Onisawa : Reliability Assessment of Man-Machine System Considering Many Factors, Proc. of Int. Workshop on Fuzzy System Applications, 91-92, Iizuka, August 1988.
- 11) T.Onisawa : An Application of Fuzzy Theory in Human Reliability Analysis Considering Performance Shaping Factors, Proc. of the 4th Symposium on Human Interface, 227-234, Tokyo, November 1988.
- 12) 和田裕明，寺野寿郎：Fuzzy Fault Tree Analysis とその応用，第一回知識工学シンポジウム資料，75-80，東京，3月，1983.
- 13) 寺野寿郎，浅居喜代治，菅野道夫共編：応用ファジィシステム入門，オーム社，1989.
- 14) T.Onisawa : Reliability Estimation from Various Subjective Standpoints, Preprints of 2nd IFSA Congress, Vol. 2, 793-796, Tokyo, July 1987.
- 15) A.D.Swain and H.E.Guttmann : Handbook of Human Reliability with Emphasis on Nuclear Power Plant Applications, NUREG/CR-1278 (2nd draft), 1980.
- 16) 山田太三郎：TMI 事象と WASH-1400，原子力工業，Vol. 26, No. 5, 67-72, 1980.
- 17) K.J.Schmucker : Fuzzy Sets, Natural Language Computations, and Risk Analysis, Computer Science Press, 1984.

- 18) D.Dubois and H.Prade : Fuzzy Sets and Systems; Theory and Applications, Academic Press, 1980.
- 19) 総合安全工学研究所編 : FTA 安全工学, 日刊工業新聞社, 1979.
- 20) H.Furuta and N.Shiraishi : Fuzzy Importance in Fault Tree Analysis, Fuzzy Sets and Systems, Vol. 12, No. 3, 205-213, 1984.
- 21) T.Onisawa : Sensitivity Analysis in Fuzzy Reliability Analysis, Proc. of the 1988 Korean

Automatic Control Conference, Vol. 2, 764-769, Seoul, October 1988.

(1989年 7月13日 受付)

(1989年12月26日再受付)

[問い合わせ先]

〒860 熊本市黒髪 2-39-1

熊本大学 工学部 共通講座数学教室

鬼沢 武久

TEL : 096-344-2111 (内)3582

FAX : 096-345-6423

著 者 紹 介

鬼沢 武久 (おにさわ たけひさ)

熊本大学 工学部 共通講座数学教室

昭和50年 3月東京工業大学工学部制御工学科卒業。昭和52年 3月同大学大学院理工学研究科修士課程制御工学専攻修了。同年 4月東京工業大学大学院総合理工学研究科システム科学専攻助手, 昭和61年10月熊本大学工学部講師, 平成元年 3月同大学工学部助教授。ファジィ理論とその応用に関する研究に従事。現在は信頼性解析への応用に関心がある。昭和62年日本人間工学会から橋本賞受賞。国際ファジィシステム学会, 計測自動制御学会, 日本人間工学会, 電子情報通信学会などの会員。工学博士。