共通の故障率と修復率をもつ順序依存形故障論理の定量化* (解析解の導出と FTA への適用について)

龍 偉^{*1}, 佐藤 吉 信^{*2}

Sequential Failure Logic Characterized with Common Failure and Repair Rates (Derivation of Analytical Solutions and Its Application to FTA)

Wei LONG and Yoshinobu SATO^{*3}

^{*3} Tokyo Univ. of Mercantile Marine, 2-1-6 Etchujima, Koto-ku, Tokyo, 135-8533, Japan

New international safety standards, ISO 12100 and International Electrotechnical Commission (IEC) 61508, are based on the concept of risk reduction to an acceptable level. The standards require increasing our capacities for risk management. Fault tree analysis (FTA) is a well-known and widely accepted method for risk analyses. Sequential failure logic (SFL) is essential for the application of FTA to risk analyses of, for example, space satellite systems and safety-related systems for product liability prevention. Algorithm for quantification of SFL has been proposed in the form of multiple integration. The present paper proposes analytical solutions of the multiple integration, given that basic events are characterized with common failure and repair rates. This makes it possible to estimate analytically the probability that an output from a minimal-cut priority-AND structure is in a failed state at time t and the statistically expected number of failures of the output per unit time at time t . Moreover, it is demonstrated how to analyze fault trees with SFL in order to estimate the statistically expected number of occurrences of the top event by use of the algorithms.

Key Words: Safety Engineering, Risk Analysis, Reliability Engineering, Systems Engineering, Sequential Failure Logic, Priority-AND Gates, FTA (Fault Tree Analysis)

1. 緒 言

最近の経済活動のグローバル化に伴い、品質管理規格 ISO 9000 シリーズにみられるように、個々の製品のみならずプラントなど生産システムのライフサイクル管理に対する国際標準化の作業が急ピッチで進められている。特に安全の分野では、安全に関する共通の基本的見解に基づいて規格を作成することにより、異なる規格間に高度な整合性を付与するため、ISO/International Electrotechnical Commission(IEC)ガイド 51「安全の見方と考え方—規格に安全の見解を取り入れるための指針」⁽¹⁾等が作成されている。これらの指針に基づいて、工作機械など機械類の安全を設計および運用上で確保するための ISO 12100「機械設備の安全性」⁽²⁾、電子技術を用いた安全関連系に適用する IEC 61508「電気・電子・プログラマブル電子安全関連系の機能安全」⁽³⁾などの規格が発刊あるいは策定されつつある。

わが国の国際整合化政策の一環として、JIS 規格を

ISO/IEC などの国際規格に整合させる作業がこの数年間において急ピッチで進められた。この結果、平成 10 年度の作業として、安全と密接な関係にあるディペンダビリティ用語の JIS Z 8115 が IEC 50(191)を中心とした整合化により改訂された。また、安全に関するものでは IEC 61508 等の翻訳 JIS 化が実施され、JIS C 0508 シリーズとして発行されることになっている。今後、それらの規格は産業界に大きな影響を与えることが予想される。

最近の安全規格のいずれにおいても、安全は受容できないリスクから免れていること⁽¹⁾という基本的概念に基づいて要求事項が展開されている。ここで、リスクは危害発生蓋然性と危害の厳しさの組合せ⁽¹⁾と定義される。このため、事故の予防という観点から、システムの事前安全計画は；1)設計や運用等に先だってシステムあるいは機器のリスクを解析し、2)これを許容リスクと比較して、改善の必要がある場合には、3)リスク軽減措置を策定し、4)リスク軽減措置がとられた後に残存するリスクを推定し、5)残存リスクと許容リスクとを比較検討して、さらにリスク軽減が必要であるかを決定する；という手順になる。このような国際標準の普及により、リスク解析に関する方法論の研究はこれまで以上に重要な意味をもつことになる

* 原稿受付 1999 年 5 月 7 日。

^{*1} 東京商船大学大学院 (〒135-8533 東京都江東区越中島 2-1-6)。

^{*2} 正員、東京商船大学大学院海洋情報システム工学専攻。
E-mail: yoshi@ipc.tosho-u.ac.jp

う。

リスク解析手法の一つである Fault Tree Analysis (FTA) は、多くの機器やシステムに適用され、多数の研究成果が公表されている^{(4)~(6)}。FTA において、任意に展開された Fault Tree (FT) がその頂上事象とそのすべての最小カット AND 構造を OR ゲートで結合した FT と等価になることはよく知られている。ここで、最小カット AND 構造とは、ある最小カット集合を構成するすべての入力事象(基本事象)とその出力事象とを AND ゲートで結合したものである⁽⁵⁾。この性質を利用して、リスク解析のための FTA は：1) システムと潜在危険生成機構の理解に基づく FT の展開、2) 当該 FT からの最小カット集合の抽出、3) 最小カット AND 構造の定量化、4) FT 全体すなわち頂上事象の定量化などを実施する；という手順になるのが一般的である。ここで、定量化とは、入力事象、出力事象、頂上事象をそれらの生起確率などにより数量化することを意味する。

通常の最小カット AND 構造では、入力事象がすべて生起すると出力事象が生起する。しかし、実際の故障論理においては、その条件だけではなく、出力事象の生起が入力事象の発生順序にも依存するいわば最小カット優先 AND 構造なるものを考慮しなければならない場合がある。ここで、「生起」は事象が生じている状態、「発生」は事象が非生起から生起に移行する状態変化をそれぞれ意味する。故障の発生が指数分布に従う主電源、予備電源およびそれらの切り替え器からなる電源供給系がこのような故障論理の最初の事例として論じられた⁽⁷⁾。また、人間-ロボット系において、故障の発生と修復が指数分布でモデル化される順序依存形の故障論理が示された⁽⁸⁾。最近では、リスク解析における順序依存形の故障論理の必要性と具体例が人工衛星打ち上げシステムの故障解析⁽⁹⁾、電気掃除機の製品安全設計⁽¹⁰⁾ などにおいて示されている。さらに、文献⁽¹¹⁾ では、リスク軽減のための安全関連系への要求事項である安全度水準が順序依存形故障論理によってモデル化され論じられている。それらの報告は、リスク解析のための FTA における順序依存形故障論理の重要性が増大してきたことを示唆している。

文献⁽⁸⁾ では、順序依存形故障論理のアルゴリズム、すなわち入力事象の生起が互いに統計的に独立で、それらの生起が指数分布でモデル化できる場合に、出力事象の時刻 t での生起確率 $Q^*(t)$ および単位時間あたりの発生回数の統計的期待値 $\omega^*(t)$ が提案されている。さらに、 $Q^*(t)$ と $\omega^*(t)$ との定常状態での解析解および故障率が修復率に対して相対的に無視できる

程度に小さい場合での近似的解析解が得られている。しかし、非定常状態での解析解は得られていない。また、提案されたアルゴリズムは、単一の最小カット優先 AND 構造を定量化するためのもので、FTA 全体への適用方法が詳細には検討されていない。そこで、本論文では n 個の入力事象 $1, 2, \dots, n$ が共通の故障率と修復率を持つ場合での $Q^*(t)$ と $\omega^*(t)$ との非定常状態での解析解を求める。さらに、順序依存形故障論理のアルゴリズムを実際の FTA に適用する方法を事例的に示す。

用語の定義

n ：入力事象の数

$\mathbf{x}$ ： n 個の異なる入力事象 $1, 2, \dots, n$ が $x_1, x_2, \dots, x_n$ の順序で発生し、結果的に全ての入力事象が同時に生起することを表す入力事象の順序ベクトル $[x_1, x_2, \dots, x_n]$

X ： $n!$ 個存在する発生順序ベクトル $\mathbf{x}$ の集合

X_i ：出力事象を生起させる発生順序ベクトル $\mathbf{x}$ の集合

m ：出力事象を生起させる発生順序ベクトル $\mathbf{x}$ の数

λ ：発生率 (1/hr)

μ ：修復率 (1/hr)

$Q^*(t)$ ：入力事象もしくは出力事象が時刻 t で生起している確率、ただし $Q(0)=0$

$\omega^*(t)$ ：入力事象もしくは出力事象の時刻 t での単位時間あたりの発生回数の統計的期待値

t, τ_i, ξ_i ：時間およびそのパラメータ

2. 順序依存形故障論理のアルゴリズム

一般的に、最小カット集合を構成する n 個の入力事象に対し、次の仮定を置く。

(1) おのおのの入力事象 $1, 2, \dots, n$ は、統計的に相互に独立して生起する。

(2) 入力事象 $i(i=1, 2, \dots, n)$ は、定数発生率 λ_{x_i} および修復率 μ_{x_i} をもつ指数分布でモデル化され、 $t=0$ では非生起である。

(3) おのおのの入力事象が微小時間 $[t, t+\Delta t]$ で 2 回以上発生する確率を $o(\Delta t)$ とする。

n 個の入力事象をもつ順序依存形故障論理では、 $Q^*(t)$ と $\omega^*(t)$ はそれぞれ次のように与えられる⁽⁸⁾。

$$Q^*(t) = \sum_{\mathbf{x} \in X_i} \int_{\tau_0}^t \int_{\tau_1}^t \cdots \int_{\tau_{n-1}}^t f_{x_1}(\tau_1) f_{x_2}(\tau_2) \cdots f_{x_n}(\tau_n) d\tau_n d\tau_{n-1} \cdots d\tau_1 \cdots \quad (1)$$

$$\omega^*(t) = \sum_{\mathbf{x} \in X_i} \omega_{x_n}(t) \int_{\tau_0}^t \int_{\tau_1}^t \cdots \int_{\tau_{n-2}}^t f_{x_1}(\tau_1) f_{x_2}(\tau_2) \cdots$$

$$f_{x_{n-1}}(\tau_{n-1})d\tau_{n-1}d\tau_{n-2}\cdots d\tau_1 \cdots \cdots (2)$$

ここで,

$$\omega_{x_n}(t) = \left(\frac{\lambda_{x_n}}{\lambda_{x_n} + \mu_{x_n}} \right) [\mu_{x_n} + \lambda_{x_n} e^{-(\lambda_{x_n} + \mu_{x_n})t}] \cdots (3)$$

$$f_{x_i}(\tau_i) = \left(\frac{\lambda_{x_i}}{\lambda_{x_i} + \mu_{x_i}} \right) [\mu_{x_i} + \lambda_{x_i} e^{-(\lambda_{x_i} + \mu_{x_i})\tau_i}] e^{-\mu_{x_i}(t - \tau_i)} \cdots \cdots (4)$$

3. 共通の故障率と修復率からなる入力事象における解析解

厳密な意味でまったく等しい故障率と等しい修復率をもつ工業製品群を製造することは不可能であるが, ある信頼度を目標として設計及び製造され, 適切な運用条件で使用する製品群は, ある範囲の統計的誤差で近似的に等しい(共通の)故障率と共通の修復率もつものとして扱われている場合が多い。

例えば, 上に述べた意味で共通の故障率と修復率をもつ電源 A, B およびそれらの切り替え器 C からなる以下のようなシステムの設計・製造を考えることができる。ここで, 電源のうち少なくとも一つが機能すればシステムは機能するものとし, 通常は A から電力が供給される。A が故障すると, C が瞬時に電源を B に切り替えて, システムは電力を供給する。A と C が故障する場合では, A が先に故障し, その後, C が故障しても, システムは機能する。逆に, C が先に故障し, B に切り替えができなくなり, その後 A が故障するとシステムは故障状態になる。

次に, 上と同じように共通の故障率と修復率をもつ製品として設計・製造される電源 A, B およびそれらの切り替え器 C, D からなるシステムを考える。電源のうち少なくとも一つが正常であればシステムは機能するものとする。通常は, A から電力が供給される。A が故障すると, C は瞬時に電源を B に切り替えて, 電力を供給する。このとき, C が故障状態にある場合では, D が C に代って A から B に切り替えて電力を供給する。ここで, A, C および D が故障状態になる場合を考えると, 6 通りの故障発生順序が存在する。このうち, C → D → A と D → C → A の故障発生順序では, システムは故障する。しかしながら, 他の故障発生順序 A → C → D, A → D → C, C → A → D および D → A → C では, システムは故障状態にならない。

現在のところ, システムの故障が要素の故障状態だけでなくそれらの発生順序にも依存する順序依存形故障論理の出力事象の統計量を推定するための式(1), (2)の一般解を求めることは困難である。しかし, 上述の例のような特別な場合を想定して, 入力事象が共

通の故障率($\lambda_{x_1} = \lambda_{x_2} = \cdots = \lambda_{x_n} = \lambda$)と共通の修復率($\mu_{x_1} = \mu_{x_2} = \cdots = \mu_{x_n} = \mu$)をもつ場合の出力事象の統計的期待値を推定する解析解を求めることは興味のあることであり, システムの統計量の時間的変動を考察する上で有用であろう。

ここで, 出力事象を発生させる発生順序ベクトル $\mathbf{x}$ の集合 X_1 が m 個の発生順序ベクトルをもつと仮定しても一般性は失われない。入力事象が共通の故障率と修復率をもつので, いずれの発生順序ベクトルによる出力事象の生起確率も等しくなる。したがって, 式(2)は次のように書き換えることができる。

$$\begin{aligned} \omega^*(t) &= m\omega_{x_n}(t) \int_{\tau_0}^t \int_{\tau_1}^t \int_{\tau_2}^t \cdots \int_{\tau_{n-2}}^t f_{x_1}(\tau_1) f_{x_2}(\tau_2) \cdots \\ &\quad f(\tau_{n-1}) d\tau_{n-1} d\tau_{n-2} \cdots d\tau_1 \\ &= m\omega_n(t) \int_{\tau_0}^t \int_{\tau_1}^t \int_{\tau_2}^t \cdots \int_{\tau_{n-2}}^t f_1(\tau_1) f_2(\tau_2) \cdots \\ &\quad f_{n-1}(\tau_{n-1}) d\tau_{n-1} d\tau_{n-2} \cdots d\tau_1 (n \geq 2, \tau_0 \equiv 0) \cdots (5) \end{aligned}$$

ここで,

$$\omega_n(t) = \left(\frac{\lambda}{\lambda + \mu} \right) [\mu + \lambda e^{-(\lambda + \mu)t}] \cdots \cdots (6)$$

$$f_i(\tau_i) = \left(\frac{\lambda}{\lambda + \mu} \right) [\mu e^{\mu(\tau_i - t)} + \lambda e^{-(\lambda + \mu)\tau_i}] \cdots \cdots (7)$$

式(5)を解くために, 次の定理が必要である。

[定理]

$$\begin{aligned} &\int_{\xi_n}^t \int_{\xi_{n-1}}^t \cdots \int_{\xi_1}^t f_{k-1}(\xi_{k-1}) f_{k-2}(\xi_{k-2}) \cdots \\ &\quad f_0(\xi_0) d\xi_{k-1} d\xi_{k-2} \cdots d\xi_0 \\ &= \frac{1}{k!} \left(\frac{\lambda}{\lambda + \mu} \right)^k [\varphi(\xi_k)]^k \cdots \cdots (8) \end{aligned}$$

ここで,

$$f_i(\xi_i) = \left(\frac{\lambda}{\lambda + \mu} \right) [\mu e^{\mu(\xi_i - t)} + \lambda e^{-(\lambda + \mu)\xi_i}] \cdots \cdots (9)$$

$$\varphi(\xi_k) = 1 - e^{-(\lambda + \mu)t} - [e^{\mu(\xi_k - t)} - e^{-(\lambda + \mu)\xi_k}] \cdots \cdots (10)$$

[証明] 数学的帰納法を用いて証明する。まず, $k=1$ の場合,

$$\begin{aligned} &\int_{\xi_1}^t f_0(\xi_0) d\xi_0 \\ &= \int_{\xi_1}^t \left(\frac{\lambda}{\lambda + \mu} \right) [\mu e^{\mu(\xi_0 - t)} + \lambda e^{-(\lambda + \mu)\xi_0}] d\xi_0 \\ &= \left(\frac{\lambda}{\lambda + \mu} \right) \{1 - e^{-(\lambda + \mu)t} - [e^{\mu(\xi_1 - t)} - e^{-(\lambda + \mu)\xi_1}]\} \\ &= \left(\frac{\lambda}{\lambda + \mu} \right) \varphi(\xi_1) \cdots \cdots (11) \end{aligned}$$

ここで,

$$\varphi(\xi_1) = 1 - e^{-(\lambda + \mu)t} - [e^{\mu(\xi_1 - t)} - e^{-(\lambda + \mu)\xi_1}] \cdots \cdots (12)$$

次に $k \geq 2$ の場合, 次式が成立するものとする。

$$\int_{\xi_{k-1}}^t \int_{\xi_{k-2}}^t \cdots \int_{\xi_1}^t f_{k-2}(\xi_{k-2}) f_{k-3}(\xi_{k-3}) \cdots$$

$$\begin{aligned}
& f_0(\xi_0) d\xi_{k-2} d\xi_{k-3} \cdots d\xi_0 \\
&= \frac{1}{(k-1)!} \left(\frac{\lambda}{\lambda+\mu} \right)^{k-1} \{1 - e^{-(\lambda+\mu)t} \\
&\quad - [e^{\mu(\xi_{k-1}-t)} - e^{-(\lambda\xi_{k-1}+\mu t)}]\}^{k-1} \\
&= \frac{1}{(k-1)!} \left(\frac{\lambda}{\lambda+\mu} \right)^{k-1} [\varphi(\xi_{k-1})]^{k-1} \cdots \cdots (13)
\end{aligned}$$

すると,

$$\begin{aligned}
& \int_{\xi_k}^t \int_{\xi_{k-1}}^t \cdots \int_{\xi_1}^t f_{k-1}(\xi_{k-1}) f_{k-2}(\xi_{k-2}) \cdots \\
& f_0(\xi_0) d\xi_{k-1} d\xi_{k-2} \cdots d\xi_0 \\
&= \int_{\xi_k}^t \frac{1}{(k-1)!} \left(\frac{\lambda}{\lambda+\mu} \right)^{k-1} \\
& \times [\varphi(\xi_{k-1})]^{k-1} f_{k-1}(\xi_{k-1}) d\xi_{k-1} \\
&= \int_{\xi_k}^t \frac{1}{(k-1)!} \left(\frac{\lambda}{\lambda+\mu} \right)^{k-1} \\
& \times [\varphi(\xi_{k-1})]^{k-1} \left(\frac{\lambda}{\lambda+\mu} \right) [\mu e^{\mu(\xi_{k-1}-t)} \\
& + \lambda e^{-(\lambda\xi_{k-1}+\mu t)}] d\xi_{k-1} \\
&= \frac{1}{(k-1)!} \left(\frac{\lambda}{\lambda+\mu} \right)^k \int_0^{\varphi(\xi_k)} [\varphi(\xi_{k-1})]^{k-1} d\varphi(\xi_{k-1}) \\
&= \frac{1}{k!} \left(\frac{\lambda}{\lambda+\mu} \right)^k [\varphi(\xi_k)]^k \cdots \cdots (14)
\end{aligned}$$

以上により証明が終了した。

定理において, $k=n-1$ ならば, 次の関係式が得られる。

$$\begin{aligned}
& \int_{\xi_{n-1}}^t \int_{\xi_{n-2}}^t \cdots \int_{\xi_1}^t f_{n-2}(\xi_{n-2}) f_{n-3}(\xi_{n-3}) \cdots \\
& f_0(\xi_0) d\xi_{n-2} d\xi_{n-3} \cdots d\xi_0 \\
&= \frac{1}{(n-1)!} \left(\frac{\lambda}{\lambda+\mu} \right)^{n-1} [\varphi(\xi_{n-1})]^{n-1} \cdots \cdots (15)
\end{aligned}$$

さらに, $\xi_{n-1}=t_0, \xi_{n-2}=t_1, \cdots, \xi_{n-(i+1)}=t_i, \cdots, \xi_0=t_{n-1}$ において, 上式に代入すると,

$$\begin{aligned}
& \int_{t_0}^t \int_{t_1}^t \cdots \int_{t_{n-2}}^t f_1(t_1) f_2(t_2) \cdots f_{n-1}(t_{n-1}) dt_1 dt_2 \cdots dt_{n-1} \\
&= \frac{1}{(n-1)!} \left(\frac{\lambda}{\lambda+\mu} \right)^{n-1} [\varphi(t_0)]^{n-1} \cdots \cdots (16)
\end{aligned}$$

式(5)と(16)より,

$$\begin{aligned}
\omega^*(t) &= m\omega_n(t) \int_{t_0}^t \int_{t_1}^t \cdots \int_{t_{n-2}}^t f_1(t_1) f_2(t_2) \cdots \\
& f_{n-1}(t_{n-1}) dt_{n-1} dt_{n-2} \cdots dt_1 \\
&= m\omega_n(t) \frac{1}{(n-1)!} \left(\frac{\lambda}{\lambda+\mu} \right)^{n-1} [\varphi(t_0)]^{n-1} \\
&= \frac{m}{(n-1)!} \left(\frac{\lambda}{\lambda+\mu} \right)^n [\mu + \lambda e^{-(\lambda+\mu)t}] [\varphi(t_0)]^{n-1} \\
&\cdots \cdots (17)
\end{aligned}$$

ここで, $t_0=0$ であるので上式は次のように書き換えることができる。

$$\begin{aligned}
\omega^*(t) &= \frac{m}{(n-1)!} \left(\frac{\lambda}{\lambda+\mu} \right)^n [\mu + \lambda e^{-(\lambda+\mu)t}] \\
& \times [1 - e^{-(\lambda+\mu)t}]^{n-1} \cdots \cdots (18)
\end{aligned}$$

同様にして,

$$Q^*(t) = \frac{m}{n!} \left(\frac{\lambda}{\lambda+\mu} \right)^n [1 - e^{-(\lambda+\mu)t}]^n \cdots \cdots (19)$$

4. 順序依存形故障論理の FTA への適用

本章では, 順序依存形故障論理のアルゴリズムから, FT の頂上事象すなわち危険事象の単位時間当りの発生回数の統計的期待値, および時刻 0 から t までの発生回数の統計的期待値を推定する方法について例示する。

FT の頂上事象の統計量を推定するために最小カット集合を用いる場合, 厳密には集合の包含・排除原理 (inclusion-exclusion principle) によって, 推定値の上限・下限値などを評価する必要がある。Kinetic Tree Theory (KITT) において, 任意の数の最小カット集合をもち, おのおの最小カット集合が任意の数の基本事象をもつ場合での一般的な解法が提示されている。

しかしながら, 優先 AND ゲートを含む FT において, 上述と同様の方法で頂上事象を評価する事例についての論文発表は今のところ見当たらない。本論文では, この点を考慮し, 優先 AND ゲートをもつ FT では, 通常の FT の場合と比べてどのような点に, どのように注意して包含・排除原理による解析を行うべきかを例示する。なお, 一般化された FT で優先 AND ゲートを持つ場合の一般的解法を導出することはたいへん重要である。しかし, これはかなり複雑な問題になることが予想され, 今後の検討課題とする。

4.1 順序依存形故障論理をもつ FT 図 1 は, あるシステムの故障論理を FT を用いて表現したものである。この FT は, 5 個の基本事象 (すなわち入力事象) 1, 2, ..., 5 をもち, 図中 2 箇所に優先 AND ゲートで示された順序依存形故障論理が存在する。ここで, 入力事象は, その生起が指数分布に従い, 互いに統計的に独立であり, 共通の故障率と修復率をもつと仮定する。

Fig. 1 FT with Sequential Failure Logic

FT から最小カット集合 $\{1, 2, 3, 5\}$ および $\{1, 2, 4, 5\}$ が容易に得られる。しかし、順序依存形故障論理を表す FT の優先 AND ゲートから、頂上事象が発生するためには入力事象 1 は 2 よりも先に発生しなければならない、また入力事象 2 は 3, 4 および 5 のいずれよりも先に発生しなければならない。FT は、この入力事象の発生順序の条件を考慮すると、出力事象 $i-j$ ($i, j=1, 2$) をもつ優先 AND ゲートを使用した最小カット優先 AND 構造を用いて図 2 のように等価的に表現できる。

4.2 頂上事象の定量化 ここで、事象および記号を以下のように定める。

事象

E_{top} : 微小時間 $[t, t+\Delta t]$ で頂上事象が発生する

A_{i-j} : 微小時間 $[t, t+\Delta t]$ で出力事象 $i-j$ ($i, j=1, 2$) が発生する

B_{i-j} : 時刻 t で出力事象 $i-j$ ($i, j=1, 2$) が生起している

$\bar{B}_{i-j}$: 時刻 t で出力事象 $i-j$ ($i, j=1, 2$) が生起していない

$C_{[a,b,c,d,e]}$: 入力事象が時刻 t までに a, b, c, d の順序で発生し、すべて生起している時に微小時間 $[t, t+\Delta t]$ で入力事象 e が発生する

$A \equiv A_{1-1} \cup A_{1-2} \cup A_{2-1} \cup A_{2-2}$

$B \equiv B_{1-1} \cup B_{1-2} \cup B_{2-1} \cup B_{2-2}$

$\bar{B} \equiv \bar{B}_{1-1} \cap \bar{B}_{1-2} \cap \bar{B}_{2-1} \cap \bar{B}_{2-2}$

記号

$Q_{a-b-c-d}(t)$: 入力事象が a, b, c, d の順序で発生して、時刻 t ですべて生起している確率

$\omega_{i-j}(t)$: 出力事象 $i-j$ の時刻 t における単位時間あたりの発生回数の統計的期待値

$\omega_{top}(t)$: 頂上事象の時刻 t における単位時間あたりの発生回数の統計的期待値

頂上事象が微小時間 $[t, t+\Delta t]$ で発生する確率は、

$$Pr\{E_{top}\} = \omega_{top}(t)\Delta t + o(\Delta t) \quad (20)$$

と書ける⁽⁸⁾。

ここで、 $E_{top} = A \cap \bar{B}$ であるから、次式が成立する。

$$Pr\{E_{top}\} = Pr\{A\} - Pr\{A \cap B\} \quad (21)$$

上式の右辺第 1 項、 $Pr\{A\} = Pr\{A_{1-1} \cup A_{1-2} \cup A_{2-1} \cup A_{2-2}\}$ を集合の包含・排除原理(inclusion-exclusion principle)を用いて展開する。図 2 において、出力 1-1 と 2-1 の組合せは、例えば入力事象が 1, 2, 3, 4 の順序で発生した後、入力事象 5 が微小時間で発生することができるので、同時に生起することができる。出力 1-2 と 2-2 の組合せにおいて微小時間で入力事象 3 と 4 が同時に発生する確率は、出力 1-1 と 2-1 とにおいて入力事象 5 のみが微小時間で発生する場合よりも高次の微小項となるので省略できる。それ以外の出力事象の組合せでは、順序が排反になるので、同時に生起することはない。すると、式(21)の右辺第 1 項は、

$$Pr\{A\} = \sum_{i,j=1}^2 Pr\{A_{i-j}\} - Pr\{A_{1-1} \cap A_{2-1}\} \quad (22)$$

と表現することができる。これは、さらに次のように書き換えることができる。

$$\begin{aligned} Pr\{A\} &= \sum_{i,j=1}^2 Pr\{A_{i-j}\} - Pr\{C_{[1,2,3,4,5]} \cup C_{[1,2,4,3,5]}\} \\ &= \sum_{i,j=1}^2 [\omega_{i-j}(t)\Delta t + o(\Delta t)] \\ &\quad - [Q_{1-2-3-4}(t) + Q_{1-2-4-3}(t)][\omega_5(t)\Delta t + o(\Delta t)] \end{aligned} \quad (23)$$

共通の故障率と修復率をもつ入力事象に対して、式(23)は

$$Pr\{A\} = 4[\omega_{i-j}(t)\Delta t + o(\Delta t)] - 2Q_{a-b-c-d}(t)[\omega(t)\Delta t + o(\Delta t)] \quad (24)$$

となる。ここで、 $\omega(t)$ 、 $\omega_{i-j}(t)$ および $Q_{a-b-c-d}(t)$ は、式(18)、(19)において、 $m=1$ 、 $n=4$ として、次式により与えられる。

$$\omega(t) = \left(\frac{\lambda}{\lambda + \mu}\right) [\mu + \lambda e^{-(\lambda + \mu)t}] \quad (25)$$

$$\omega_{i-j}(t) = \frac{1}{3!} \left(\frac{\lambda}{\lambda + \mu}\right)^4 [\mu + \lambda e^{-(\lambda + \mu)t}] [1 - e^{-(\lambda + \mu)t}]^3 \quad (26)$$

Fig. 2 Equivalent expression of FT given in Fig. 1

$$Q_{a-b-c-d}(t) = \frac{1}{4!} \left(\frac{\lambda}{\lambda + \mu} \right)^4 [1 - e^{-(\lambda + \mu)t}]^4 \dots (27)$$

次に、時刻 t において、ある出力事象が生起しているとき、他の出力事象が微小時間 $[t, t + \Delta t]$ で発生することもある。例えば、入力事象が 1-2-3-5 の順序で発生したため出力事象 1-1 が生起しているとき、入力事象が 1-2-5-4 の順序で発生することにより出力事象 2-2 が生起することが可能である。このようなことを考慮すると、式 (21) 右辺第 2 項は、

$$\begin{aligned} Pr\{A \cap B\} &= Pr\{C_{[1,2,3,5,4]} + Pr\{C_{[1,2,5,3,4]} \\ &+ Pr\{C_{[1,2,4,5,3]} + Pr\{C_{[1,2,5,4,3]}\} \\ &= 4Q_{a-b-c-d}(t)[\omega(t)\Delta t + o(\Delta t)] \dots (28) \end{aligned}$$

となる。式 (20)～(28) から、次式を得る。

$$\begin{aligned} \omega_{top}(t) &= \lim_{\Delta t \rightarrow 0} \frac{Pr\{E_{top}\}}{\Delta t} \\ &= \frac{4}{3!} \left(\frac{\lambda}{\lambda + \mu} \right)^4 [\mu + \lambda e^{-(\lambda + \mu)t}] [1 - e^{-(\lambda + \mu)t}]^3 \\ &\quad - \frac{6}{4!} \left(\frac{\lambda}{\lambda + \mu} \right)^5 [\mu + \lambda e^{-(\lambda + \mu)t}] [1 - e^{-(\lambda + \mu)t}]^4 \\ &\quad \dots (29) \end{aligned}$$

時刻 0 から t までの頂上事象の発生回数の統計的期待値 $W^*(0, t)$ は、 $\omega_{top}(t)$ を 0 から t まで時間積分して、次のように与えられる。

$$\begin{aligned} W^*(0, t) &= -\frac{\lambda^5}{240(\lambda + \mu)^6} [-12\lambda e^{-5(\lambda + \mu)t} \\ &\quad + 15(4\lambda - \mu)e^{-4(\lambda + \mu)t} + 40(-3\lambda + 2\mu)e^{-3(\lambda + \mu)t} \\ &\quad + 60(2\lambda - 3\mu)e^{-2(\lambda + \mu)t} + 60(-\lambda + 4\mu)e^{-(\lambda + \mu)t} \\ &\quad + 60\mu(\lambda + \mu)t] + \frac{\lambda^4}{18(\lambda + \mu)^5} [3\lambda e^{-4(\lambda + \mu)t} \\ &\quad + 40(-3\lambda + \mu)e^{-3(\lambda + \mu)t} + 18(\lambda - \mu)e^{-2(\lambda + \mu)t} \\ &\quad + 12(-\lambda + 3\mu)e^{-(\lambda + \mu)t} + 12\mu(\lambda + \mu)t] \\ &\quad - \frac{\lambda^4}{720(\lambda + \mu)^5} (-84\lambda^2 + 385\lambda\mu + 880\mu^2) \dots (30) \end{aligned}$$

4.3 考察 式 (29) 右辺第 1 項は出力事象が単位時間当たりに発生する回数の統計的期待値を単純に合計したものである。第 2 項は、ある出力事象が生起しているときに他の出力事象が発生するまたは二つ以上の出力事象が同時に発生する回数の単位時間当たりの統計的期待値を合計したものである。これより、次のことがいえる。

(1) 修理系では、しばしば、 $\lambda/\mu \ll 1$ 、すなわち修復時間が平均故障発生間隔に比べて十分に短い。そのような場合、右辺第 1 項と比べると第 2 項は無視できるので、 $\omega_{top}(t)$ を近似的に第 1 項のみから求めてもよい。

(2) 非修理系では、 $\mu = 0$ なので、第 2 項は必ずし

も無視できず、 $\omega_{top}(t)$ は第 1 項と第 2 項を考慮して推定すべきである。

5. 結 論

最近の安全に関する国際規格の動向とそれらの JIS 化の影響により、システムの事前安全計画におけるリスク解析の必要性がますます高まってきている。代表的なリスク解析手法の FTA については、これまでに多数の研究結果が報告されている。それらの中で、順序依存形故障論理のアルゴリズムは、多重積分の形式で与えられている。本論文では、最小カット集合が n 個の基本事象からなる順序依存形故障論理を扱っている。基本事象が共通の故障率と修復率をもつ場合における多重積分の一般解を導出することができた。また、順序依存形故障論理アルゴリズムは、単一の最小カット優先 AND ゲートを定量化するためのものであるが、このアルゴリズムを用いて FT の頂上事象の生起確率および発生回数の統計的期待値等をどのように推定するかについて事例を用いて示した。さらに、この定量化の結果から若干の考察を行った。

文 献

- (1) ISO/IEC Guide 51, *Safety aspects-Guidelines for their inclusion in standards*, (1998), ISO/IEC.
- (2) Draft ISO 12100-1, *Safety of machinery-Basic concepts, general principles for design*, Part 1 (1998), ISO.
- (3) IEC 61508, *Functional safety of electrical/electronic/programmable electronic safety-related systems*, Part 1-General requirements, (1998), IEC.
- (4) Lee, W. S., Grosh, D. L., Tillman, F. A. and Lie, C. H., Fault tree analysis, methods, and applications-a review, *IEEE Trans. Reliability*, 34-3 (1985), 194-203.
- (5) Henley, E. J. and Kumamoto, H., *Probabilistic Risk Assessment*, (1993), 44-152, IEEE Press Inc.
- (6) Modarres, M., *Reliability and Risk Analysis*, (1993), 142-154, Marcel Dekker Inc.
- (7) Fussell, J. B., Aber, E. F. and Rahl, R. G., On the quantitative analysis of priority-AND failure logic, *IEEE Trans. Reliability*, 25-5 (1976), 324-326.
- (8) 佐藤吉信・井上紘一・熊本博光, 人間-ロボット系の安全性評価(第 3 報), 機論, 52-475, C (1986), 1110-1117.
- (9) Ngom, L., Cabarbaye, A. and Barpm, C., Taking into account of dependency relations in the Monte Carlo's simulation of non-coherent fault trees, *Proc. 4th Probabilistic Safety Assessment Management*, (1998-9), 2067-2072.
- (10) Scibata, Y. and Sato, Y., A case study of risk analysis for product liability prevention, *Proc. 4th Probabilistic Safety Assessment Management*, (1998-9), 82-86.
- (11) 加藤栄一・佐藤吉信・堀籠教夫, 機能安全規格における安全度水準モデルについて, 電子情報通信学会 A 論文誌, J 82-2 (1999), 247-255.