独立防御層の確率論的リスク評価

凌 元 錦*・鈴木 和 彦**・幸 田 武 久***

Probabilistic Risk Assessment on Independent Protection Layer

Yuanjin LING*, Kazuhiko SUZUKI** and Takehisa KOHDA***

In chemical and nuclear power plants, the safety policies have been established according to the consideration of independent protection layer (IPL). This paper studies risk reduction using the IPL consisting of n layers. For general failure distribution function of plant and IPL, we proposed a general algorithm to estimate the expected numbers of normal trips and accidents caused by IPL failure. The results of this algorithm gave agreement with those had been concluded by Markov analysis in the case of exponential distribution. Moreover, the expected numbers of normal trips and accidents are derived analytically when $n \leq 3$. Furthermore, we provided a new quantification method for assessing the risk reduction by the use of IPL. The method is illustrated through application to the risk assessment of nitrobenzene synthesis batch plant.

Key Words: independent protection layer, expected number of failures, normal trip, hazard, risk

1. 緒 言

化学プラントは、従来から多重防御の安全設計思想に基づいて安全対策が講じられてきた。これは多重の独立した防御層により安全を確保しようとするもので、独立防御層 (Independent Protection Layer: IPL)^{1), 2)} と呼ばれる。Fig. 1 は IPL の概念図である。IPL には、プロセス本質安全設計 (IPL₁)、基本プロセス制御警報システム/運転員による監視 (IPL₂)、クリティカルアラーム/運転員の介入 (IPL₃)、安全計装システム (IPL₄)、安全弁による物理的防護 (IPL₅)、防液堤による物理的防護 (IPL₆)、プラント内緊急対応計画 (IPL₇)、地域防災計画 (IPL₈) の 8 つの防御層がある。これらの防御層はお互いに独立であり、仮に内側の防御層が損なわれても、その外側の防御層が機能して、事故を未然に防止したり、その拡大を防ぐようになっている。このような独立防御の考え方は原子力プラントにおける深層防護や現代の IT 社会における住基ネットのセキュリティ対策と同様なものである。

Fig. 1 Independent Protection Layer (IPL)

IPL は、その構成要素と機能によって工学的 IPL (IPL₁~IPL₆) と組織的 IPL (IPL₇, IPL₈) に分類され则认为される。本研究は工学的 IPL のみを考察の対象とする。これまで、IPL によるリスク低減効果を評価するとき、フォールトツリー解析 (Fault Tree Analysis: FTA) やイベントツリー解析 (Event Tree Analysis: ETA) による定量的評価、または LOPA (Layer of Protection Analysis)^{2), 3)} による半定量的解析が行われてきた。しかし、これらの解析結果が時間に対する平均的なものであり、使用時間経過によってリスク低減効果がどのように変化するかが明らかにされていない。実際のシステム運用を考えると、たとえば定期点検周期や部品取替周期などの変更によりシステムの運用状態

* (株) 普遍学国際研究所 東京都台東区池之端 2-7-17

** 岡山大学工学部システム工学科 岡山市津島中 3-1-1

*** 京都大学大学院工学研究科 京都市左京区吉田本町

* International Institute of Universality, 2-7-17 Ikenohata, Taito-ku, Tokyo

** Department of System Engineering, Faculty of Engineering, Okayama University, 3-1-1 Tsushima-naka, Okayama

*** Graduate School of Engineering, Kyoto University, Yoshida-Honmachi, Sakyo-ku, Kyoto

(Received February 3, 2005)

(Revised August 29, 2005)

が変化することである。システムライフサイクルのすべての状態に対して安全性を評価するときには、それぞれの状態の時間的变化を考慮する必要がある。さらに、時間的変動を考慮した評価値は必ずしも時間平均の確率による評価値に抑えられているわけではない⁴⁾。しかし、これについていままです十分な考察がなされていない。

本研究は、一般化した n 層の工学的 IPL を考察の対象としてモデル化する。プラントと各 IPL の故障時間分布は一般的な分布関数で与えられる場合に、プラントの正常トリップの期待回数および事故発生確率の一般的な計算プロセスおよび数値計算方法を示し、本手法は指数分布の場合のマルコフ解析により得られた結果と一致することを確かめる。また、防御層数 $n \leq 3$ 、プラントおよび各防御層の故障時間が指数分布に従う場合に、正常トリップの期待回数および事故発生確率の解析解を求める。さらに、IPL によるリスク低減の時間的変動を評価するためのモデルを示し、プラントと各 IPL の故障時間分布はワイブル分布に従う場合に、本モデルをニトロベンゼン合成バッチプラントのリスク評価に適用し、結果を考察する。

2章で問題を記述し、3章で一般分布での表現、数値計算方法および $n = 3$ の場合の解析を述べ、4章で指数分布の場合のマルコフモデルによる解析、5章でリスクの定式化および応用例を示す。

2. 問題の記述

2.1 モデル

n 層の IPL をもつシステムを考える。ライフサイクルで時間計画保全（予防保全）と緊急保全（事後保全）をとともに考えるシステムの振る舞いはつぎのようになる。所定の時間間隔に到達した際に予防保全が行なわれる。一方、定期保全到達前に、プラントの異常時に IPL の正常作動によってプラントを安全に停止させると緊急保全が行なわれる。この場合、プラントの状態は正常 (S) または故障 (F)、IPL 全体の状態は正常状態 (S_i) または IPL のすべての層が故障した状態 (F) のいずれかである (S_i は、 $i-1$ 層までの IPL がすべて故障したが、第 i 層 IPL が正常、 $i+1$ 層以後の各 IPL が正常または故障のいずれかであることを意味する。 $i = 1, 2, \dots, n$)。プラントの状態 $X \in (S, F)$ と IPL の状態 $Y \in (S_i, F)$ との組合せによって、システムはつぎのような状態 (X, Y) に分類される。各状態の推移を Fig. 2 に示す。

状態 (S, S_1) または (S, F): プラントは正常に運転する状態。

状態 (F, S_i) ($i = 1, 2, \dots, n$): 第 i 層 IPL の防御による正常トリップ状態、つまりプラントは故障が発生したが、第 i 層 IPL の正常作動によってプラントを安全に停止する状態。

状態 (F, F): 事故発生状態、つまり IPL のすべての層が故障した状態で、プラントは異常が発生して事故が起こ

Fig. 2 Transition diagram of system

る状態。

正常トリップ状態 (F, S_i) ($i = 1, 2, \dots, n$) が起こると、直ちに緊急保全が行なわれて状態 (S, S_1) に戻る。ただし、緊急保全はプラントだけでなく、IPL のすべての層をチェックして保全する。状態 (F, F) は、事故（たとえば爆発事故）の発生を表わす。このとき、プラントのライフサイクルが終結する。状態 (S, F) は所定の時間間隔に到達した際に予防保全が行なわれて状態 (S, S_1) に戻る。

2.2 仮定

以下の議論において、つぎのような仮定を前提とする。

- (1) プラントおよび各 IPL の故障は統計的に独立である。
- (2) IPL が正常であれば作動要求への対応が必ず成功する。
- (3) プラントが正常な状態で IPL は故障しても発見されない。その故障はそのまま潜在している。
- (4) 正常トリップが起こると、直ちに緊急保全が行なわれる。緊急保全はプラントだけでなく、IPL のすべての層をチェックして保全する。
- (5) 保全は瞬時に完了、かつプラントおよび IPL の各層は新品同様の状態に戻る。

2.3 記号の定義

Fig. 2 を参照し、つぎのように記号を定義する。

n	IPL の数
$G(t)$	プラントの故障時間分布関数
ν	プラントの故障率
m_0	$G(t)$ がワイブル分布の場合の形状パラメータ
η_0	$G(t)$ がワイブル分布の場合の尺度パラメータ
$F_i(t)$	第 i 層 IPL の故障時間分布関数
$R_i(t)$	第 i 層 IPL の信頼度関数, $R_i(t) = 1 - F_i(t)$
λ_i	第 i 層 IPL の故障率
m_i	$F_i(t)$ がワイブル分布の場合の形状パラメータ
η_i	$F_i(t)$ がワイブル分布の場合の尺度パラメータ
T	システムの定期保全間隔

- $P_i(t)$ 正常トリップ状態 (F, S_i) ($i = 1, 2, \dots, n$) が時刻 t まで初めて発生する確率
- $P_0(t)$ 事故状態 (F, F) が時刻 t まで初めて発生する確率
- $p_i(t)$ $P_i(t)$ の密度関数
- $\tilde{f}(s)$ 関数 $f(t)$ のラプラス変換
- $W_i(t)$ 時刻 t まで、第 i 層 IPL の防御による正常トリップの期待回数 ($i = 1, 2, \dots, n$)
- $W_0(t)$ 時刻 t に事故が発生する確率
- $w_i(t)$ $W_i(t)$ の密度関数 ($i = 0, 1, \dots, n$)
- c_0 事故により生じる損害の大きさ
- $RI(t)$ リスク

3. 一般分布での表現と数値計算

本章では、プラントと各 IPL の故障時間分布は一般的な分布関数で与えられる場合に、プラントの正常トリップ期待回数および事故発生確率の一般的な計算方法を示す。

3.1 一般計算式の導出

Fig. 2 を参照し、システムは時刻 $t = 0$ で状態 (S, S_1) から運転を開始し、 $[0, T]$ の間でそれぞれの正常トリップ状態 (F, S_i) ($i = 1, 2, \dots, n$) が何回か発生し、直ちに緊急保全により瞬時に状態 (S, S_1) に戻る。そこで、時刻 t まで、 $w_i(t)$, $W_i(t)$ についてつぎのような積分式が成立つ^{5), 6)}。

$$w_i(t) = p_i(t) + \int_0^t p_i(t-\tau) \sum_{j=1}^n w_j(\tau) d\tau \quad (1)$$

$$W_i(t) = \int_0^t w_i(\tau) d\tau \quad (2)$$

ただし、 $i = 0, 1, \dots, n$ 。また、状態 (F, F) で事故が発生したが、修理が行なわれないので、 $W_0(t)$ は時刻 t に事故が発生する確率となる。

(1), (2) をラプラス変換すれば次式となる。

$$\tilde{w}_i(s) = \tilde{p}_i(s) \left\{ 1 + \sum_{j=1}^n \tilde{w}_j(s) \right\} \quad (3)$$

よって、

$$\tilde{w}_i(s) = \frac{\tilde{p}_i(s)}{1 - \sum_{j=1}^n \tilde{p}_j(s)} \quad (4)$$

$$\tilde{W}_i(s) = \frac{1}{s} \tilde{w}_i(s) \quad (5)$$

が得られる。 $W_i(t)$ は (5) 式をラプラス逆変換することで求められる。

3.2 $\tilde{p}_i(s)$ の計算

プラントおよび各 IPL の故障時間分布は一般分布に従う場合を考える。このとき、状態 (F, S_i) ($i = 1, 2, \dots, n$) が時刻 t まで初めて発生する確率 $P_i(t)$ は、 $i-1$ 層までの IPL がすべて故障かつ第 i 層 IPL が正常である状態で、プラントの故障が発生する確率となる。ところで、

(a) $i-1$ 層までの IPL が時刻 t まですべて故障した確率：

$$Q_i(t) = \prod_{j=1}^{i-1} F_j(t), \text{ ただし, } i=1 \text{ の場合, } Q_1 = 1$$

(b) 第 i 層の IPL が時刻 t まで正常である確率： $R_i(t)$

(c) プラントが時刻 t と $t+dt$ の間で故障する確率：

$$dG(t) = G'(t)dt$$

となるから、 $P_i(t)$ は次式で表わすことができる。

$$P_i(t) = \int_0^t Q_i(\tau) R_i(\tau) dG(\tau), \quad i = 1, 2, \dots, n \quad (6)$$

また、状態 (F, F) が時刻 t まで初めて発生する確率 $P_0(t)$ は、 n 層までの IPL がすべて故障した状態で、プラントの故障が発生する確率となる。したがって、

$$P_0(t) = \int_0^t \prod_{j=1}^n F_j(\tau) dG(\tau) \quad (7)$$

(6) 式と (7) 式は、 $P_i(t)$ の密度関数 $p_i(t)$ を用いて次式で表わすことができる。

$$P_i(t) = \int_0^t p_i(\tau) d\tau, \quad i = 0, 1, \dots, n \quad (8)$$

よって、

$$\begin{cases} p_0(t) = G'(t) \prod_{j=1}^n F_j(t) \\ p_1(t) = G'(t) R_1(t) \\ p_i(t) = G'(t) R_i(t) \prod_{j=1}^{i-1} F_j(t), \quad i = 2, 3, \dots, n \end{cases} \quad (9)$$

となる。

$p_i(t)$ をラプラス変換すると、 $\tilde{p}_i(s)$ が得られる。一般的に、 n が大きい場合、(5) 式をラプラス逆変換することで $W_i(t)$ を解析的に求めることは困難であるので、離散的数値解析手法に頼らざるを得ない。以下、数値計算方法および $n \leq 3$ の場合の解析解を示す。

3.3 数値計算

まず、たたみ込み積分の近似方法を示す。たたみ込み積分方程式 $y(t) = \int_0^t g(t-\tau)x(\tau)d\tau$ に対して、 $t = h\Delta t$ とすれば次式で離散近似することができる。

$$y(h\Delta t) = \Delta t \sum_{k=0}^{h-1} g(h\Delta t - k\Delta t)x(k\Delta t) \quad (10)$$

ただし、 $y(0) = 0$, $h = 1, 2, \dots$

したがって、 $t = h\Delta t$ とし、(10) 式を用いて (1) 式の微分方程式を離散近似すると、Table 1 のような近似解が得られる。

(2) 式より、 $W_i(t)$ の数値解は、

$$W_i(h\Delta t) = \Delta t \sum_{k=0}^h w_i(k\Delta t) \quad (11)$$

となる。ただし、 $h = 0, 1, 2, \dots$

Table 1 Approximate value of $w_i(t)$

h	$w_i(h\Delta t)$
0	0
1	$p_i(\Delta t)$
2	$p_i(2\Delta t) + \Delta t \cdot p_i(\Delta t) \sum_{j=1}^n w_j(\Delta t)$
3	$p_i(3\Delta t) + \Delta t \left\{ p_i(2\Delta t) \sum_{j=1}^n w_j(\Delta t) + p_i(\Delta t) \sum_{j=1}^n w_j(2\Delta t) \right\}$
$\vdots$	$\vdots$
h	$p_i(h\Delta t) + \Delta t \sum_{k=0}^{h-1} \left\{ p_i(h\Delta t - k\Delta t) \sum_{j=1}^n w_j(k\Delta t) \right\}$

3.4 $n=3$ の場合の解析

ここで、プラントおよび各 IPL の故障時間はそれぞれ指数分布: $G(t) = 1 - e^{-\nu t}$, $F_1(t) = 1 - e^{-\lambda_1 t}$, $F_2(t) = 1 - e^{-\lambda_2 t}$, $F_3(t) = 1 - e^{-\lambda_3 t}$ とする. このとき, 事故発生確率および正常トリップの期待回数のラプラス変換を求める. さらに, 各 IPL の故障率が同じの場合の解析解を示す.

(9) 式より,

$$p_0(t) = \nu e^{-\nu t} (1 - e^{-\lambda_1 t}) (1 - e^{-\lambda_2 t}) (1 - e^{-\lambda_3 t}) \quad (12)$$

$$p_1(t) = \nu e^{-(\lambda_1 + \nu)t} \quad (13)$$

$$p_2(t) = \nu \{ e^{-(\lambda_2 + \nu)t} - e^{-(\lambda_1 + \lambda_2 + \nu)t} \} \quad (14)$$

$$p_3(t) = \nu e^{-\nu t} e^{-\lambda_3 t} (1 - e^{-\lambda_1 t}) (1 - e^{-\lambda_2 t}) \quad (15)$$

が得られる.

(12) ~ (15) 式をラプラス変換し整理すると,

$$\tilde{p}_0(s) = \frac{\lambda_1 \lambda_2 \lambda_3 \nu A}{rr_0 r_1 r_2 r_3 r_{12} r_{13} r_{23}} \quad (16)$$

$$\tilde{p}_1(s) = \frac{\nu}{r_1} \quad (17)$$

$$\tilde{p}_2(s) = \frac{\lambda_1 \nu}{r_2 r_{12}} \quad (18)$$

$$\tilde{p}_3(s) = \frac{\lambda_1 \lambda_2 \nu (r + r_3)}{rr_3 r_{13} r_{23}} \quad (19)$$

が得られる. ただし, $r_0 = s + \nu$, $r_1 = s + \lambda_1 + \nu$, $r_2 = s + \lambda_2 + \nu$, $r_3 = s + \lambda_3 + \nu$, $r_{12} = s + \lambda_1 + \lambda_2 + \nu$, $r_{13} = s + \lambda_1 + \lambda_3 + \nu$, $r_{23} = s + \lambda_2 + \lambda_3 + \nu$, $r = s + \lambda_1 + \lambda_2 + \lambda_3 + \nu$, $A = r_1 r_2 r_{12} (r_{13} + r_{23}) + r_1 r_3 r_{13} (r_{12} + r_{23}) + r_2 r_3 r_{23} (r_{12} + r_{13})$.

また, (16) ~ (19) 式に対して, $\lambda_3 \rightarrow \infty$ の場合, 防御層数 $n=2$ となり, さらに $\lambda_2 \rightarrow \infty$ とすると防御層数が 1 つしかない場合となる. $n=1 \sim 3$ に対応するそれぞれ $\tilde{p}_i(s)$ の結果は Table 2 に示す.

Table 2 と (4) 式より,

$$\tilde{w}_0(s) = \frac{\tilde{p}_0(s)}{1 - \sum_{i=1}^3 \tilde{p}_i(s)} = \frac{\lambda_1 \lambda_2 \lambda_3 \nu A}{r_0 B} \quad (20)$$

Table 2 $\tilde{p}_i(s)$ when $n=1 \sim 3$

i	$n=1$	$n=2$	$n=3$
0	$\frac{\lambda_1 \nu}{r_0 r_1}$	$\frac{\lambda_1 \lambda_2 \nu (r_1 + r_2)}{r_0 r_1 r_2 r_{12}}$	$\frac{\lambda_1 \lambda_2 \lambda_3 \nu A}{rr_0 r_1 r_2 r_3 r_{12} r_{13} r_{23}}$
1	$\frac{r_1}{r_1}$	$\frac{r_1}{r_1}$	$\frac{r_1}{r_1}$
2	-	$\frac{\lambda_1 \nu}{r_2 r_{12}}$	$\frac{\lambda_1 \nu}{r_2 r_{12}}$
3	-	-	$\frac{\lambda_1 \lambda_2 \nu (r + r_3)}{rr_3 r_{13} r_{23}}$

が得られる. ただし, $B = rr_1 r_2 r_3 r_{12} r_{13} r_{23} - \nu \{ rr_2 r_3 r_{12} r_{13} r_{23} + \lambda_1 rr_1 r_3 r_{13} r_{23} + \lambda_1 \lambda_2 (r + r_3) r_1 r_2 r_{12} \}$. (20) 式を (5) 式に代入すると,

$$\tilde{W}_0(s) = \frac{\lambda_1 \lambda_2 \lambda_3 \nu A}{sr_0 B} \quad (21)$$

となる. $\tilde{W}_0(s)$ は事故発生の確率 $W_0(t)$ のラプラス変換である.

同様に, 第 i 層 IPL ($i=1, 2, 3$) の防御による正常トリップの期待回数のラプラス変換は,

$$\tilde{W}_1(s) = \frac{\nu rr_2 r_3 r_{12} r_{13} r_{23}}{sB} \quad (22)$$

$$\tilde{W}_2(s) = \frac{\lambda_1 \nu rr_1 r_3 r_{13} r_{23}}{sB} \quad (23)$$

$$\tilde{W}_3(s) = \frac{\lambda_1 \lambda_2 \nu (r + r_3) r_1 r_2 r_{12}}{sB} \quad (24)$$

となる. ところが, (21) ~ (24) 式をラプラス逆変換することによる解析解を得ることは困難である. ここで, 各防御層の故障率が同じ, つまり $\lambda_1 = \lambda_2 = \lambda_3 = \lambda$ の場合の解析解を示す.

$\lambda_1 = \lambda_2 = \lambda_3 = \lambda$ の場合, (16) ~ (19) 式より,

$$\tilde{p}_0(s) = \frac{6\lambda^3 \nu}{(s + \nu)(s + \lambda + \nu)(s + 2\lambda + \nu)(s + 3\lambda + \nu)} \quad (25)$$

$$\tilde{p}_1(s) = \frac{\nu}{s + \lambda + \nu} \quad (26)$$

$$\tilde{p}_2(s) = \frac{\lambda \nu}{(s + \lambda + \nu)(s + 2\lambda + \nu)} \quad (27)$$

$$\tilde{p}_3(s) = \frac{2\lambda^2 \nu}{(s + \lambda + \nu)(s + 2\lambda + \nu)(s + 3\lambda + \nu)} \quad (28)$$

が得られる. よって,

$$1 - \sum_{i=1}^3 \tilde{p}_i(s) = \frac{s^3 + as^2 + bs + c}{(s + \lambda + \nu)(s + 2\lambda + \nu)(s + 3\lambda + \nu)} \quad (29)$$

となる. ただし, $a = 2(3\lambda + \nu)$, $b = (3\lambda + \nu)^2 + 2\lambda^2$, $c = 6\lambda^3$.

(25) ~ (29) 式を (4) 式に代入すると, $\tilde{w}_i(s)$ が得られる. さらに (5) 式より, $\tilde{W}_i(s)$ が求められる. 結果はつぎのとおりである.

$$\tilde{W}_0(s) = \frac{6\lambda^3 \nu}{s(s + \nu)(s^3 + as^2 + bs + c)} \quad (30)$$

$$\tilde{W}_1(s) = \frac{\nu(s^2 + a_1 s + a_0)}{s(s^3 + as^2 + bs + c)} \quad (31)$$

$$\bar{W}_2(s) = \frac{\lambda\nu(s+b_0)}{s(s^3+as^2+bs+c)} \quad (32)$$

$$\bar{W}_3(s) = \frac{2\lambda^2\nu}{s(s^3+as^2+bs+c)} \quad (33)$$

ただし, $a_0 = (2\lambda+\nu)(3\lambda+\nu)$, $a_1 = 5\lambda+2\nu$, $b_0 = 3\lambda+\nu$.

(30) ~ (33) 式をラプラス逆変換することにより得られる解析解は次式の 3 次方程式の性質に依存する.

$$s^3 + as^2 + bs + c = 0 \quad (34)$$

(34) 式の方程式について,

$$p = -\frac{a^2}{3} + b = -\frac{3\lambda^2 + 6\lambda\nu + \nu^2}{3} \quad (35)$$

$$q = 2\left(\frac{a}{3}\right)^3 - \frac{ab}{3} + c \\ = -\frac{2}{27}(45\lambda^2 + 9\lambda\nu + \nu^2)\nu \quad (36)$$

$$\Delta = -\left\{\left(\frac{p}{3}\right)^3 + \left(\frac{q}{2}\right)^2\right\} \quad (37)$$

と置くと, (34) 式の 3 次方程式の実数解は p と Δ の値の符号 (正か負か 0 か) で決まる. (35) 式より常に $p < 0$ であるので, (34) 式の方程式の実数解について, つぎの 3 つのケースを考えればよい⁷⁾.

(1) ケース A: $p < 0$, $\Delta > 0$

このとき, (34) 式がつぎのような 3 つの実数解をもつ.

$$\begin{cases} x_1 = r \cos \left\{ \frac{1}{3} \arccos \left(\frac{3q}{rp} \right) \right\} - \frac{a}{3} \\ x_2 = r \cos \left\{ \frac{2\pi}{3} + \frac{1}{3} \arccos \left(\frac{3q}{rp} \right) \right\} - \frac{a}{3} \\ x_3 = r \cos \left\{ \frac{2\pi}{3} - \frac{1}{3} \arccos \left(\frac{3q}{rp} \right) \right\} - \frac{a}{3} \end{cases} \quad (38)$$

ただし, $a = 2(3\lambda+\nu)$, $r = \sqrt{-4p/3}$.

$s_1 = -x_1$, $s_2 = -x_2$, $s_3 = -x_3$ と置くと,

$$\bar{W}_0(s) = \frac{6\lambda^3\nu}{s(s+\nu)(s+s_1)(s+s_2)(s+s_3)} \quad (39)$$

$$\bar{W}_1(s) = \frac{\nu(s^2+a_1s+a_0)}{s(s+s_1)(s+s_2)(s+s_3)} \quad (40)$$

$$\bar{W}_2(s) = \frac{\lambda\nu(s+b_0)}{s(s+s_1)(s+s_2)(s+s_3)} \quad (41)$$

$$\bar{W}_3(s) = \frac{2\lambda^2\nu}{s(s+s_1)(s+s_2)(s+s_3)} \quad (42)$$

が得られる.

(2) ケース B: $p < 0$, $\Delta < 0$

このとき, (34) 式がつぎのような 1 つの実数解 x_1 をもつ.

$$x_1 = \sqrt[3]{-\frac{q}{2} + \sqrt{-\Delta}} + \sqrt[3]{-\frac{q}{2} - \sqrt{-\Delta}} - \frac{a}{3} \quad (43)$$

$s_1 = -x_1$ と置くと,

$$\bar{W}_0(s) = \frac{6\lambda^3\nu}{s(s+\nu)(s+s_1)\{(s+d)^2+\omega^2\}} \quad (44)$$

$$\bar{W}_1(s) = \frac{\nu(s^2+a_1s+a_0)}{s(s+s_1)\{(s+d)^2+\omega^2\}} \quad (45)$$

$$\bar{W}_2(s) = \frac{\lambda\nu(s+b_0)}{s(s+s_1)\{(s+d)^2+\omega^2\}} \quad (46)$$

$$\bar{W}_3(s) = \frac{2\lambda^2\nu}{s(s+s_1)\{(s+d)^2+\omega^2\}} \quad (47)$$

が得られる. ただし, $d = (a-s_1)/2$, $\omega = \sqrt{(c-s_1d^2)/s_1}$

(3) ケース C: $p < 0$, $\Delta = 0$

このとき, (34) 式がつぎのような 2 重実数解をもつ.

$$\begin{cases} x_1 = -\sqrt[3]{4q} - \frac{a}{3} \\ x_2 = x_3 = \sqrt[3]{\frac{q}{2}} - \frac{a}{3} \end{cases} \quad (48)$$

$s_1 = -x_1$, $s_2 = -x_2 = -x_3$ と置くと,

$$\bar{W}_0(s) = \frac{6\lambda^3\nu}{s(s+\nu)(s+s_1)(s+s_2)^2} \quad (49)$$

$$\bar{W}_1(s) = \frac{\nu(s^2+a_1s+a_0)}{s(s+s_1)(s+s_2)^2} \quad (50)$$

$$\bar{W}_2(s) = \frac{\lambda\nu(s+b_0)}{s(s+s_1)(s+s_2)^2} \quad (51)$$

$$\bar{W}_3(s) = \frac{2\lambda^2\nu}{s(s+s_1)(s+s_2)^2} \quad (52)$$

が得られる.

付録 A のラプラス変換表を利用して (39) ~ (52) 式をラプラス逆変換すると, $W_i(t)$ ($i = 0, 1, 2, 3$) の解析解が得られる.

3.5 $n = 1, 2$ の場合の解析解

$n = 2$ の場合, Table 2 および (4) 式, (5) 式より,

$$\bar{W}_0(s) = \frac{2\lambda_1\lambda_2\nu(s+d_0)}{s(s+\nu)(s^3+as^2+bs+c)} \quad (53)$$

$$\bar{W}_1(s) = \frac{\nu(s^2+a_1s+a_0)}{s(s^3+as^2+bs+c)} \quad (54)$$

$$\bar{W}_2(s) = \frac{\lambda_1\nu(s+b_0)}{s(s^3+as^2+bs+c)} \quad (55)$$

が得られる. ただし, $a = 2(\lambda_1+\lambda_2+\nu)$, $b = (\lambda_1+\lambda_2+\nu)^2 + \lambda_1\lambda_2$, $c = \lambda_1\lambda_2(\lambda_1+\lambda_2+2\nu)$, $a_0 = (\lambda_1+\lambda_2+\nu)(\lambda_2+\nu)$, $a_1 = \lambda_1 + 2\lambda_2 + 2\nu$, $b_0 = \lambda_1 + \nu$, $d_0 = (\lambda_1+\lambda_2)/2 + \nu$.

$n = 3$ の場合と同様な計算プロセスで $W_i(t)$ ($i = 0, 1, 2$) の解析解が得られる.

$n = 1$ の場合,

$$W_0(t) = \begin{cases} 1 - (1+\nu t)e^{-\nu t} & \text{if } \lambda_1 = \nu \\ 1 + \frac{1}{\lambda_1 - \nu} (\nu e^{-\lambda_1 t} - \lambda_1 e^{-\nu t}) & \text{if } \lambda_1 \neq \nu \end{cases} \quad (56)$$

$$W_1(t) = \frac{\nu}{\lambda_1} (1 - e^{-\lambda_1 t}) \quad (57)$$

が簡単に得られる.

4. マルコフモデルによる解析

本章では, 防御層数 $n = 3$, しかもプラントと各 IPL の故障時間が指数分布関数: $G(t) = 1 - e^{-\nu t}$, $F_1(t) = 1 - e^{-\lambda_1 t}$, $F_2(t) = 1 - e^{-\lambda_2 t}$, $F_3(t) = 1 - e^{-\lambda_3 t}$ で与えられる場合に, マルコフモデルを用いてプラントの事故発生確率を求める. また, 本手法により求められる事故発生確率は第 3.4 節に

Fig. 3 Markov transition diagram, when $n = 3$

一般的な計算方法を用いて得られた結果と一致することを確かめる。

定期保全間隔 $[0, T]$ の間に各状態の推移を Fig. 3 に示す。Fig. 3 では、横線の下側の文字列について、S はプラントが正常な状態、F は事故が起る状態、 i ($i = 1, 2, 3$) は第 i 層の IPL が正常であることを意味する。また、横線の上側の i ($i = 0, 1, \dots, 8$) は状態の識別子意味する。システムが状態 0 からスタートし、保全が瞬時に完了するので、状態 i ($i = 1, 2, \dots, 7$) で正常トリップが起ると直ちに状態 0 に戻る。状態 8 は事故が発生するから、保全せずにプラントのライフサイクルが終結する。時刻 t で各状態 i に存在する確率を $U_i(t)$ とすると、つぎの微分方程式が成立する。

$$\begin{cases} U_0'(t) = -(\lambda_1 + \lambda_2 + \lambda_3)U_0(t) + \nu\{U_1(t) + U_2(t) + U_3(t) + U_4(t) + U_5(t) + U_6(t)\} \\ U_1'(t) = -(\lambda_2 + \lambda_3 + \nu)U_1(t) + \lambda_1 U_0(t) \\ U_2'(t) = -(\lambda_1 + \lambda_3 + \nu)U_2(t) + \lambda_2 U_0(t) \\ U_3'(t) = -(\lambda_1 + \lambda_2 + \nu)U_3(t) + \lambda_3 U_0(t) \\ U_4'(t) = -(\lambda_3 + \nu)U_4(t) + \lambda_2 U_1(t) + \lambda_1 U_2(t) \\ U_5'(t) = -(\lambda_2 + \nu)U_5(t) + \lambda_3 U_1(t) + \lambda_1 U_3(t) \\ U_6'(t) = -(\lambda_1 + \nu)U_6(t) + \lambda_3 U_2(t) + \lambda_2 U_3(t) \\ U_7'(t) = -\nu U_7(t) + \lambda_3 U_4(t) + \lambda_2 U_5(t) + \lambda_1 U_6(t) \\ U_8'(t) = \nu U_7(t) \end{cases} \quad (58)$$

初期条件 $U_0(0) = 1$, $U_i(0) = 0$ ($i = 1, 2, \dots, 8$) とし、(58) 式をラプラス変換すると、

$$\begin{cases} s\tilde{U}_0(s) = 1 - (\lambda_1 + \lambda_2 + \lambda_3)\tilde{U}_0(s) + \nu\{\tilde{U}_1(s) + \tilde{U}_2(s) + \tilde{U}_3(s) + \tilde{U}_4(s) + \tilde{U}_5(s) + \tilde{U}_6(s)\} \\ s\tilde{U}_1(s) = -(\lambda_2 + \lambda_3 + \nu)\tilde{U}_1(s) + \lambda_1 \tilde{U}_0(s) \\ s\tilde{U}_2(s) = -(\lambda_1 + \lambda_3 + \nu)\tilde{U}_2(s) + \lambda_2 \tilde{U}_0(s) \\ s\tilde{U}_3(s) = -(\lambda_1 + \lambda_2 + \nu)\tilde{U}_3(s) + \lambda_3 \tilde{U}_0(s) \\ s\tilde{U}_4(s) = -(\lambda_3 + \nu)\tilde{U}_4(s) + \lambda_2 \tilde{U}_1(s) + \lambda_1 \tilde{U}_2(s) \\ s\tilde{U}_5(s) = -(\lambda_2 + \nu)\tilde{U}_5(s) + \lambda_3 \tilde{U}_1(s) + \lambda_1 \tilde{U}_3(s) \\ s\tilde{U}_6(s) = -(\lambda_1 + \nu)\tilde{U}_6(s) + \lambda_3 \tilde{U}_2(s) + \lambda_2 \tilde{U}_3(s) \\ s\tilde{U}_7(s) = -\nu \tilde{U}_7(s) + \lambda_3 \tilde{U}_4(s) + \lambda_2 \tilde{U}_5(s) + \lambda_1 \tilde{U}_6(s) \\ s\tilde{U}_8(s) = \nu \tilde{U}_7(s) \end{cases} \quad (59)$$

となる。

(59) 式を解くと、事故発生確率 $U_8(t)$ のラプラス変換 $\tilde{U}_8(s)$ は、

$$\tilde{U}_8(s) = \frac{\lambda_1 \lambda_2 \lambda_3 \nu A}{s r_0 B} \quad (60)$$

となる。ただし、 $r_0 = s + \nu$, $r_1 = s + \lambda_1 + \nu$, $r_2 = s + \lambda_2 + \nu$, $r_3 = s + \lambda_3 + \nu$, $r_{12} = s + \lambda_1 + \lambda_2 + \nu$, $r_{13} = s + \lambda_1 + \lambda_3 + \nu$, $r_{23} = s + \lambda_2 + \lambda_3 + \nu$, $r = s + \lambda_1 + \lambda_2 + \lambda_3 + \nu$, $A = r_1 r_2 r_{12}(r_{13} + r_{23}) + r_1 r_3 r_{13}(r_{12} + r_{23}) + r_2 r_3 r_{23}(r_{12} + r_{13})$, $B = r r_1 r_2 r_3 r_{12} r_{13} r_{23} - \nu\{r r_2 r_3 r_{12} r_{13} r_{23} + \lambda_1 r r_1 r_3 r_{13} r_{23} + \lambda_1 \lambda_2 (r + r_3) r_1 r_2 r_{12}\}$ 。

(21) 式より、 $\tilde{U}_8(s) = \tilde{W}_0(s)$ となる。すなわち、事故発生確率は、第 3.4 節での一般的な計算方法を用いて得られた結果と一致する。

5. リスク

5.1 リスクの定式化

プラントにおいて IPL を備えることにより潜在的な危険を未然に防ぐとする。プラントは異常が起こる場合、仮に内側の防御層が損なわれても、その外側の防御層が機能して、事故を未然に防止したり、その拡大を防ぐようになっている。しかし、プラントの異常時にすべての防御層がその機能を果たさない場合、重大な事故（たとえば爆発事故）が発生する恐れがある。ここで、プラントの事故発生確率 $W_0(t)$ と事故により生じる被害の大きさ c_0 との積はリスク $RI(t)$ としてつぎのように定義する。

$$RI(t) = c_0 W_0(t) \quad (61)$$

5.2 応用例

実際のプラントの応用例として、Fig. 4 に示すベンゼンのニトロ化のためのバッチプラント⁸⁾を取り上げる。これは実験用のプラントであるが、規模の点を除けば実用バッチプラントに近いものである。ここで、このバッチプロセスにおける反応の暴走に起因する反応器爆発事故のリスクを評価する。

プラントは反応器、原料タンク TK-A（混酸用）および TK-B（ベンゼン用）、加熱装置、冷却系、製品デカンタ、攪拌機、水槽、安全装置などから構成される。ニトロベンゼン合成のためには、混酸（硝酸と硫酸）とベンゼンを反応器内で反応させる。

Fig. 4 のニトロベンゼン合成バッチプラントでは、暴走反応に起因する事故を防ぐための安全対策として、冷却系 (IPL₁)、インターロック (IPL₂)、自動放出機構 (IPL₃)、過圧防護用の破裂板式安全装置 (IPL₄) の 4 つの独立防御層が設けられることとする。ここで、送液ポンプの異常による混酸の送液速度が高すぎると、化学反応による発熱の大量発生により反応器内の温度が上昇するから反応器爆発事故が発生するまでという事故シナリオを想定する。このとき、IPL の作動は以下のとおりである。

Fig. 4 A process flow diagram for a batch reactor

Fig. 5 $RI(t)$ vs. t when $m = 0.1 \sim 2.0$

- (1) 反応器内の温度は設定値より高くなると、冷却系が作動し設定温度まで冷却する。
- (2) (1) が失敗する場合、インターロックが作動し、送液ポンプや攪拌機を停止することにより温度や圧力の上昇を抑制する。
- (3) (2) の対処が失敗する場合、自動放出機構により、反応器の内容物を水を張った水槽に落として反応を停止させる。
- (4) (3) の自動放出機構の故障など原因で放出できない場合、過圧保護板の破裂により反応器内の圧力が減圧する。

(1) から (4) までの対応がすべて失敗する場合、反応器内の温度の上昇によって圧力も上昇し、最終的に反応器が爆発する。ここで、プラントの異常発生（例えば送液ポンプの異常）および各 IPL の故障時間はワイブル分布： $G(t) = 1 - e^{-\left(\frac{t}{\eta_0}\right)^{m_0}}$, $F_i(t) = 1 - e^{-\left(\frac{t}{\eta_i}\right)^{m_i}}$ ($i = 1, 2, 3, 4$)

Table 3 Value of risk ($RI(t)$), when $t = 1 \sim 5$ (yr)

	m	t (yr)				
		1	2	3	4	5
$RI(t)$	0.1	102.07	137.17	161.16	179.85	195.36
	0.5	23.82	81.55	157.16	241.94	330.98
	1.0	1.65	26.03	104.79	244.25	427.80
	1.5	0.09	7.85	72.26	256.55	543.84
	2.0	0.01	2.22	49.79	270.27	654.84

に従う。また、簡単化のため、形状パラメータ $m_i = m$ ($i = 0, 1, \dots, 4$) とする。ワイブル分布は形状パラメータ m の値によって、時間に対して故障率が 3 つのパターン：減少型 (DFR, $0 < m < 1$)、一定型 (CFR, $m = 1$)、増加型 (IFR, $m > 1$) になっている。各パラメータはつぎのような値をとるとする。

$$\eta_0 = 3.25 \text{ (yr)}, \eta_1 = 3.58 \text{ (yr)}, \eta_2 = 3.73 \text{ (yr)}, \\ \eta_3 = 4.12 \text{ (yr)}, \eta_4 = 3.88 \text{ (yr)}, c_0 = 10000.$$

このとき、数値計算より、 m の値に対応するリスク $RI(t)$ が時間経過による変化のようすを Fig. 5 に示す。また、時刻 $t = 1 \sim 5$ (yr), 1 年ずつ増加するとき、 m の値に対応する $RI(t)$ の値を Table 3 に示す。この数値例から、プラントのリスクは使用時間経過にともなって大きくなる。また、初期段階でのリスクは IFR 分布より DFR 分布のほうが大きい。使用時間が長くなると IFR 分布のほうがリスクが大きくなる。なお、IFR 分布の場合、使用時間が長くなるとリスクが急激に増加することがわかる。なぜならば、IFR は使用時間経過にともない次第に故障しやすくなり、一方、DFR は故障しにくくなるという性質があるからである。

6. 結 言

本研究は、 n 層の工学的 IPL をもつシステムを考察の対象とし、プラントと各 IPL の故障時間分布は一般分布の場合、プラントの正常トリップおよび事故発生確率の一般的な計算プロセスおよび数値計算方法を示した。本手法は、システムのモデル化が簡単であり、指数分布の場合のマルコフモデルを用いて得られた結果と一致することを確認した。また、防御層数 $n \leq 3$, プラントおよび各防御層の故障時間が指数分布に従う場合、正常トリップの期待回数および事故発生確率の解析解を求めた。さらに、IPL によるリスク低減の時間的変動を評価するためのモデルを示し、プラントと各 IPL の故障時間分布はワイブル分布関数で与えられる場合に、本手法をニトロベンゼン合成バッチプラントのリスク評価に適用し、その結果を考察した。

ところで、緒言に述べたように、Fig. 1 での IPL₂, IPL₃ はオペレーターの介入が必要である。このような IPL については、プラントの異常時に、オペレーターの誤操作など、いわゆるヒューマンエラーの問題がよく起こる。また、マイクロプロセッサ技術の急速な発展にともなって自己診断機能が組み込まれた電子式の IPL がよく利用されているが、故障検出率の影響を考慮する必要がある。なお、IPL の故障に

は、安全側故障、危険側故障や共通原因故障など複数の故障モードがある。これらは今後の課題として考えられる。

参考文献

- 1) AIChE/CCPS: Guidelines for Safe Automation of Chemical Processes, Center for Chemical Process Safety (1993)
- 2) AIChE/CCPS: Layer of Protection Analysis: Simplified Process Risk Assessment (2001)
- 3) A.M. Dowell III: Layer of protection analysis for determining safety integrity level; ISA Transaction, **37**-3, 155/165 (1998)
- 4) 幸田, 井上: 危険と安全の確率論的評価, 計測と制御, **35**-8, 575/580 (1996)
- 5) H. Kumamoto, H. Ohtsuka and K. Inoue: Expected Number of Failures Caused by Protective System, IEEE Trans. on Reliability, **31**-2, 219/221 (1982)
- 6) 凌, 鈴木, 幸田: 自己診断機能を持つ安全保護系の数理モデル, 計測自動制御学会論文集, **41**-3, 259/267 (2005)
- 7) 上野: 代数入門, 岩波書店 (2004)
- 8) 林 年宏: 20 リットル反応容器による反応暴走実験, 安全工学, **28**-5, 324/329 (1989)
- 9) 加藤, 菊地: ラプラス変換関数表, 日刊工業新聞社 (1968)

《付 録》

A. ラプラス変換表

Table A.1 Laplace Transform Table

Function	Laplace Transform
$\frac{1}{abcd} - \frac{1}{a(b-a)(c-a)(d-a)}e^{-at} - \frac{1}{b(a-b)(c-b)(d-b)}e^{-bt}$ $- \frac{1}{c(a-c)(b-c)(d-c)}e^{-ct} - \frac{1}{d(a-d)(b-d)(c-d)}e^{-dt}$	$\frac{1}{s(s+a)(s+b)(s+c)(s+d)}$
$\frac{a_0}{bcd} - \frac{b^2 - a_1b + a_0}{b(c-b)(d-b)}e^{-bt} - \frac{c^2 - a_1c + a_0}{c(b-c)(d-c)}e^{-ct} - \frac{d^2 - a_1d + a_0}{d(b-d)(c-d)}e^{-dt}$	$\frac{s^2 + a_1s + a_0}{s(s+b)(s+c)(s+d)}$
$\frac{1}{ab^2} - \frac{1}{a(a-b)^2}e^{-at} - \left\{ \frac{1}{b(a-b)} + \frac{a-2b}{b^2(a-b)^2} \right\} e^{-bt}$	$\frac{1}{s(s+a)(s+b)^2}$
$\frac{1}{abc^2} + \frac{1}{a(a-b)(c-a)^2}e^{-at} + \frac{1}{b(b-a)(c-b)^2}e^{-bt}$ $+ \left\{ \frac{1}{c(c-b)(a-c)}t - \frac{(c-b)(c-a) + c(2c-b-a)}{c^2(c-b)^2(c-a)^2} \right\} e^{-ct}$	$\frac{1}{s(s+a)(s+b)(s+c)^2}$
$\frac{a}{bc^2} + \frac{b-a}{b(c-b)^2}e^{-bt} + \left\{ \frac{a-c}{c(c-b)}t - \frac{c^2 - a(2c-b)}{c^2(c-b)^2} \right\} e^{-ct}$	$\frac{s+a}{s(s+b)(s+c)^2}$
$\frac{a_0}{bc^2} - \frac{b^2 - a_1b + a_0}{b(b-c)^2}e^{-bt} - \frac{c^2 - a_1c + a_0}{c(c-b)}te^{-ct} + \frac{a_0(2c-b) - c^2(a_1-b)}{c^2(b-c)^2}e^{-ct}$	$\frac{s^2 + a_1s + a_0}{s(s+b)(s+c)^2}$
$\frac{1}{b(a^2 + \omega^2)} - \frac{1}{b\{(a-b)^2 + \omega^2\}}e^{-bt} + \frac{\{a(a-b) - \omega^2\}\sin(\omega t) + \omega(2a-b)\cos(\omega t)}{\omega(a^2 + \omega^2)\{(a-b)^2 + \omega^2\}}e^{-at}$	$\frac{1}{s(s+b)\{(s+a)^2 + \omega^2\}}$
$\frac{1}{bc(a^2 + \omega^2)} \left\{ 1 - \frac{a\sin(\omega t) + \omega\cos(\omega t)}{\omega}e^{-at} \right\}$ $+ \frac{1}{b(b-c)\{(a-b)^2 + \omega^2\}} \left\{ e^{-bt} - \frac{1}{\omega}[(a-b)\sin(\omega t) + \omega\cos(\omega t)]e^{-at} \right\}$ $+ \frac{1}{c(c-b)\{(a-c)^2 + \omega^2\}} \left\{ e^{-ct} - \frac{1}{\omega}[(a-c)\sin(\omega t) + \omega\cos(\omega t)]e^{-at} \right\}$	$\frac{1}{s(s+b)(s+c)\{(s+a)^2 + \omega^2\}}$
$\frac{a_0}{b(a^2 + \omega^2)} \left\{ 1 - \frac{a\sin(\omega t) + \omega\cos(\omega t)}{\omega}e^{-at} \right\}$ $+ \frac{b-a_0}{b[(a-b)^2 + \omega^2]} \left\{ e^{-bt} - \frac{1}{\omega}[(a-b)\sin(\omega t) + \omega\cos(\omega t)]e^{-at} \right\}$	$\frac{s+a_0}{s(s+b)\{(s+a)^2 + \omega^2\}}$
$\frac{1}{\omega}e^{-at}\sin(\omega t) + \frac{a_0}{b(a^2 + \omega^2)} \left\{ 1 - \frac{a\sin(\omega t) + \omega\cos(\omega t)}{\omega}e^{-at} \right\}$ $- \frac{b^2 - a_1b + a_0}{b[(a-b)^2 + \omega^2]} \left\{ e^{-bt} - \frac{1}{\omega}[(a-b)\sin(\omega t) + \omega\cos(\omega t)]e^{-at} \right\}$	$\frac{s^2 + a_1s + a_0}{s(s+b)\{(s+a)^2 + \omega^2\}}$

[著 者 紹 介]

凌 元 錦 (正会員)

2005年岡山大学大学院自然科学研究科博士後期課程修了。同年岡山大学工学部客員研究員、同年7月(株)普遍学国際研究所研究員、現在に至る。主にシステムの信頼性・安全性の研究に従事。工学博士。

鈴木 和 彦 (正会員)

1976年九州工業大学制御工学科卒業, 77年林原(株)入社。86年岡山大学工学部助手, 93年同助教授, 98年同教授。主にシステムの信頼性, 安全性解析の研究に従事。システム制御情報学会, 化学工学会, 安全工学協会などの会員。工学博士。

幸 田 武 久 (正会員)

1983年京都大学大学院工学研究科(博士課程)修了, 同年通産省工業技術院機械技術研究所入所, 88年京都大学工学部助手, 91年同助教授, 94年改組により京都大学大学院助教授, 現在に至る。主にシステムの信頼性, 安全性に関する研究に従事。IEEE, 安全工学協会などの会員。工学博士。