E/E/PE 安全関連系のプルーフテスト実施間隔に関する一考察

On Proof-Testing Intervals for E/E/PE Safety-Related System

関西大学・総合情報学部　井上 真二
鳥取大学・大学院工学研究科　山田　茂

Shinji Inoue (Faculty of Informatics, Kansai University)
Shigeru Yamada (Graduate School of Engineering, Tottori University)

1　はじめに

システムに求められる安全性を機能的側面から確保する概念として機能安全がある．近年では，この機能安全を電気・電子・プログラマブル電子（E/E/PE）安全関連系と呼ばれるシステムが全体システムの安全性を担う場面が増えている．この状況を踏まえ，2000 年に E/E/PE 安全関連系に関する国際基本機能安全規格 IEC 61508 [1]（第 1 版）が発行されると共に，各産業分野におけるグループ安全規格も発行されている．基本的に，E/E/PE 安全関連系は，非制御装置（EUC）と EUC 制御系（BCS）から構成されるメインシステムに対して付加的に取り付けれるシステムであり，このメインシステムが安全機能の遂行に失敗した場合，待機中の E/E/PE 安全関連系に対し作動要求が発せられ，E/E/PE 安全関連系が作動することによって，所定の安全性を最終的に確保する仕組みで作動する．したがって，E/E/PE 安全関連系の安全性評価を行うには，E/E/PE 安全関連系そのものの状態だけでなく，E/E/PE 安全関連系への作動要求頻度に注意を払う必要がある．

IEC 61508 では，E/E/PE 安全関連系の安全性評価手法に関して，安全度水準（SIL）をはじめとする一定の指針を与えており，上記の点を踏まえながら，運用時における作動要求頻度に基づいた目標機能失敗尺度をそれぞれ定義している．また，E/E/PE 安全関連系の内部構造や作動要求頻度などを考慮しながら，当該規格上では厳密に議論されていない状況を想定した安全性評価手法に関する議論も行われている [2,3,7]．これらを含め E/E/PE 安全関連系に対する安全性評価において，プルーフテスト実施間隔はその評価結果に大きく影響を与える要因として知られている．プルーフテストは，E/E/PE 安全関連系に対する一種の定期的な保全活動であり，特に，運用時において頻繁に実施される自己診断では検出できないフォールト，いわゆる DU（dangerous undetected）フォールトの検知および修復に主軸を置く．このプルーフテストは，設計時における安全性能を維持し，DU 故障もしくは DU フォールトに起因する危害事象の発生を未然に防ぐ重要な保全活動であり，このプルーフテストの実施間隔を短くすれば，運用時における所定の安全性を維持できることが期待される．しかし，一方で，保全活動に必要なコストの発生とシステム全体の可用性の低下を招くため，所定の安全性を満足することを意識しつつも，これらの保全コストや危害事象の発生を想定したリスク（危害リスク）を考慮した経済的な保全活動の実施が求められる．

本研究では，上述の背景に基づいて，E/E/PE 安全関連系の状態と作動要求発生事象との双方の不確実性を考慮しつつ，保全コストと危害リスクとのトレードオフ関係に基づいた最適プルーフテスト実施間隔を導くための手法について議論する．また，信頼性数理における保全性理論を活用しながら，E/E/PE 安全関連系に対する保全実施により発生するコストと危害事象発生確率とその影響を考慮した危害リスクに基づいて，経済的に視点から最適な保全実施を実現を支援するための最適方策を解析的に示す．

2　E/E/PE 安全関連系の運用パターン

保全コストと危害リスクを考慮した期待費用を求めるにあたり，危害事象発生論理 [3, 6] に基づいて，E/E/PE 安全関連系の運用時に想定される運用パターンを整理する．前述した E/E/PE 安全関連系とメインシステムの構造上の関係から，一般的に，危害事象は，フォールト状態（安全機能を喪失している状態）において E/E/PE 安全関連系への作動要求が行われることで危害事象が発生する「フォールト・作動要求論理」と，作動要求状態において危険側故障が発生し危害事象が発生する「作動要求状態・危険側故障論

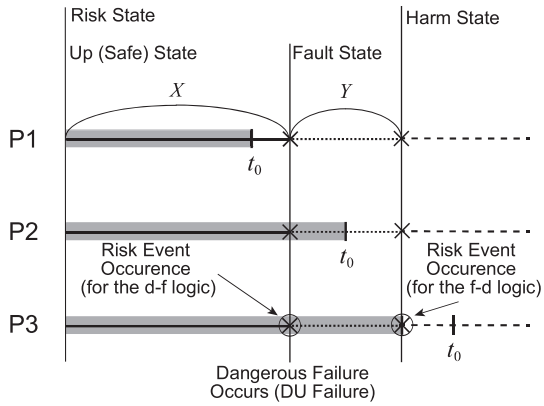

図 1： 想定する運用パターン.

理」の互いに排反する事象によって生起する．また，危険側故障についても，高い頻度で実施される自己診断機能によって検出される DD（dangerous detected）故障と，この自己診断機能では検出されずプルーフテストによってのみ検出できる DU 故障がある．

いま，DD フォールトは，自己診断機能によって検知され，完全にその原因が修復され即座に安全な状態へ推移するものと仮定する．このとき，運用時において想定される E/E/PE 安全関連系に対して，プルーフテストもしくは危害事象のどちらか一方が生起するまでの期間を 1 サイクルとして，その運用パターンは，上述した危害事象発生論理に基づいて，次の 3 つのパターンが考えられる：

P1 リスク・アップ状態にてプルーフテストが実施される．

P2 DU 故障発生後，リスク・ダウン状態においてプルーフテストが実施される．

P3 プルーフテスト実施前に危害事象（リスク事象）が生起する．

ここで，リスク・アップ状態とは，E/E/PE 安全関連系は正常に稼働しており，作動要求時も含め，システム全体として危害状態に至らない状態を表す．一方，リスク・ダウン状態とは，DU 故障発生によって E/E/PE 安全関連系はフォールト状態にあるが，作動要求状態ではないため，危害事象は生起せず，システム全体として危害状態でない状態を表す．また，**P3** に関して，危害事象は前述の通り，DU 故障発生直後にリスク事象が発生するパターン（作動要求状態・危険側故障論理）と，DU 故障発生後に作動要求事象が生起することでリスク事象が発生するパターン（フォールト・作動要求論理）が想定されるが，プルーフテスト実施前にリスク事象が生起するパターンとして，本研究では,「フォールト・作動要求論理」に対応した状況のみを考慮している．

ここで，$X(>0)$ および $Y(\geq 0)$ を，それぞれ，リスク・アップ状態から開始され DU 故障が発生するまでの時間，および，DU 故障発生から E/E/PE 安全関連系へ作動要求事象が生起するまでの時間を表す確率変数とする．さらに，連なる確率変数 X および Y は，それぞれ独立な分布関数 $F_X(x)$（確率密度関数 $f_X(x)$）および $G_Y(y)$（確率密度関数 $g_Y(y)$）に従うとする．図 1 に，プルーフテスト実施時刻を t_0 とおき，運用時に想定される E/E/PE 安全関連系の運用パターンを示す.

3 単位時間あたりの期待費用

本研究では，1 サイクルを，運用開始時からプルーフテストの実施もしくはリスク事象発生のどちらかが先に起きるまでの時間間隔とする．図 1 に示した運用パターンに基づいて，**P1** の発生確率は，

$$\Pr\{X > t_0\} = \bar{F}_X(t_0), \tag{1}$$

と与えられる．ここで，$\bar{F}_X(x) \equiv 1 - F_X(x)$ である．また，**P2** および **P3** の発生確率も，それぞれ，

$$\int_0^{t_0} \Pr\{Y > t_0 - x \mid X = x\} dF_X(x) = \int_0^{t_0} \bar{G}_Y(t_0 - x) dF_X(x), \tag{2}$$

および

$$\Pr\{X + Y \le t_0\} \equiv H_{X+Y}(t_0) = \int_0^{t_0} G_Y(t_0 - x) dF_X(x). \tag{3}$$

と求められる．

いま，c_1 をリスク・アップ状態におけるプルーフテストの実施に係るコスト，c_2 をリスク・ダウン状態におけるプルーフテスト実施，DU フォールト修復，およびその他の保全に係るコスト，ならびに c_3 を危害事象発生時の危害コストとおく．このとき，P1，P2，および P3 がそれぞれ排反であるため，1 サイクル当たりの期待費用 $Q(t_0)$ は，

$$\begin{aligned} Q(t_0) &= c_1 \bar{F}_X(t_0) + c_2 \int_0^{t_0} \bar{G}_Y(t_0 - x) dF_X(x) + c_3 \int_0^{t_0} G_Y(t_0 - x) dF_X(x) \\ &= c_3 - (c_3 - c_1)\bar{F}_X(t_0) - (c_3 - c_2) \int_0^{t_0} \bar{G}_Y(t_0 - x) dF_X(x), \end{aligned} \tag{4}$$

と与えられる．また，1 サイクル当たりの期待時間 $S(t_0)$ は，各運用パターンでの期待時間の和として与えられ，

$$\begin{aligned} S(t_0) &= \int_{t_0}^{\infty} t_0 dF_X(x) + t_0 \int_0^{t_0} \bar{G}_Y(t_0 - x) dF_X(x) + \int_0^{t_0} t dH_{X+Y}(t) \\ &= t_0 \bar{F}_X(t_0) + t_0 F_X(t_0) - t_0 \int_0^{t_0} G_Y(t_0 - x) dF_X(x) - t_0 \bar{H}_{X+Y}(t_0) + \int_0^{t_0} \bar{H}_{X+Y}(t) dt \\ &= \int_0^{t_0} \bar{H}_{X+Y}(t) dt. \end{aligned} \tag{5}$$

と求められる．E/E/PE 安全関連系における DU 故障発生事象や安全関連系への作動要求発生事象は時間的な不確実性を伴うため，このサイクルを繰り返した場合を想定する．この場合，定常状態における単位時間当たり期待費用 $C(t_0)$ は，基本再生定理 [5] に基づいて，

$$C(t_0) = \frac{Q(t_0)}{S(t_0)}, \tag{6}$$

と与えられる．

4　最適プルーフテスト実施方策の導出

式 (6) を最小にする t_0 を最適プルーフテスト実施間隔として議論する．最適プルーフテスト実施間隔を得るための必要条件として，式 (6) を t_0 について微分して 0 とおくと，最終的に，

$$\begin{aligned} &\frac{c_2 - c_1}{c_3 - c_2} \left\{ r_X(t_0) \frac{\bar{F}_X(t_0)}{\bar{H}_{X+Y}(t_0)} \int_0^{t_0} \bar{H}_{X+Y}(t) dt - F_X(t_0) \right\} \\ &\qquad + r_{X+Y}(t_0) \int_0^{t_0} \bar{H}_{X+Y}(t) dt - H_{X+Y}(t_0) = \frac{c_1}{c_3 - c_2}, \end{aligned} \tag{7}$$

と整理される．ここで，$r_X(t_0)$ および $r_{X+Y}(t_0)$ は，それぞれ，X および $X + Y$ に関する時刻 t_0 でのハザードレートを表す．安全関連系を取り扱う場合，特に，危害事象発生の危害コストは，それ以前に実施された保全コストよりも極めて高いことが容易に想像できる．そこで，式 (7) において，$c_1 \approx c_2 \ll c_3$ の場合を考えると，$(c_2 - c_1)/(c_3 - c_2) \approx 0$ となり，式 (7) は，$c_0 = c_1 \approx c_2$ として，

$$r_{X+Y}(t_0) \int_0^{t_0} \bar{H}_{X+Y}(t) dt - H_{X+Y}(t_0) = \frac{c_0}{c_3 - c_0}, \tag{8}$$

のように改められる．式 (8) は,（リスク事象発生率）×（リスク事象発生までの平均時間） −（リスク事象発生確率)=（危害コスト比）の構造であり，本質的に，いわゆる信頼性理論の取替方策において最適時刻を求めるための基本型構造 [4] に従っている．ここで，式 (8) における左辺を $s(t_0)$ とおくと，

$$\frac{ds(t_0)}{dt_0} = \frac{dr_{X+Y}(t_0)}{dt_0} \int_0^{t_0} \bar{H}_{X+Y}(t)dt. \tag{9}$$

と求められ，$r_{X+Y}(t_0)$ と $s(t_0)$ の単調性は互いに一致することがわかる．

いま，$H_{X+Y}(t)$ が IFR（increasing failure rate）で平均が $1/\mu$ の一般分布に従うものと仮定すると，$dr_{X+Y}(t)/dt > 0$ となる．このとき，$s(0) = 0$ かつ $s(\infty) = r_{X+Y}(\infty)/\mu - 1 > c_0/(c_3 - c_0)$，すなわち，

$$r_{X+Y}(\infty) > \frac{\mu c_3}{c_3 - c_0}, \tag{10}$$

ならば，$s(0) < c_0/(c_3 - c_0) < s(\infty)$ であるため，式 (8) を満たす有限で唯一の解 $t_0{=}t_0^*$ が存在することになる．一方，$s(\infty) = r_{X+Y}(\infty)/\mu - 1 \le c_0/(c_3 - c_0)$，すなわち，

$$r_{X+Y}(\infty) \le \frac{\mu c_3}{c_3 - c_0)}, \tag{11}$$

であれば，式 (6) に示した単位時間当たりの期待費用 $C(t_0)$ は，t_0 に関して単調減少する関数となり，$t_0^* \to \infty$ となる．つまり，この場合，保全コストや危害リスクの観点から，運用期間中のプルーフテストの実施を含め DU 故障に対する保全活動は実施せず，リスク事象発生時に修復もしくは取替を行うべきとの指針を与える．ところで，$c_0 = c_1 \approx c_2 \ll c_3$ のとき，式 (6) は，

$$C(t_0) = \frac{c_3 + (c_0 - c_3)\bar{H}_{X+Y}(t_0)}{\int_0^{t_0} \bar{H}_{X+Y}(t)dt}, \tag{12}$$

と求められる．したがって，$c_3 \le c_0$ のとき，$C(t_0)$ は t_0 について単調減少関数となり，$t_0^* = \infty$ となる．また，式 (12) より，プルーフテストを実施しないときの $C(t_0)$ は，$\lim_{t_0\to\infty} C(t_0) = \mu c_3$ となる．さらに，最適解 t_0^* が存在するときの $C(t_0^*)$ は，式 (8) より，

$$\int_0^{t_0^*} \bar{H}_{X+Y}(t)dt = \frac{c_0 + (c_3 - c_0)H(t_0^*)}{(c_3 - c_0)r_{X+Y}(t_0^*)} \tag{13}$$

であるため，これを式 (12) に代入することで，最終的に，

$$C(t_0^*) = (c_3 - c_0)r_{X+Y}(t_0^*), \tag{14}$$

と求められる．以上の議論を，最適プルーフテスト実施方策として次のようにまとめる：

【最適プルーフテスト実施方策】

$H_{X+Y}(t)$ は，平均 $1/\mu$ で，連続かつ単調増加関数であるハザードレート $r_{X+Y}(t)$（狭義の IFR 型）をもつ確率分布関数であり，$c_0 \ll c_3$ と仮定する．

(i) $r_{X+Y}(\infty) > \mu c_3/(c_3 - c_0)$ ならば，式 (8) を満たす有限かつ唯一の解 $t_0^*(0 < t_0^* < \infty)$ が存在して，そのとき，単位時間当たりの期待費用は，式 (14) で与えられる．

(ii) $r_{X+Y}(\infty) \le \mu c_3/(c_3 - c_0)$ ならば，$t_0^* = \infty$ となり，運用期間中のプルーフテストの実施を含め DU 故障に対する保全活動は実施せず，リスク事象発生時に修復もしくは取替を行えばよい．

5　数値例

本研究において導出した最適プルーフテスト実施方策の数値例を与える．安全関連系の安全性評価においては，その故障発生現象を表すハザードレートが一定の場合を想定した議論が一般的であるため，リスク・アップ状態から開始され DU 故障が発生までの時間については指数分布を仮定する．また，作動要求が運用時間に応じて変化するような状況はほとんど想定されないため，確率変数 X および Y が，それぞれ

$$F_X(t) = 1 - \exp[-\lambda_0 t], \tag{15}$$

$$G_Y(t) = 1 - \exp[-\lambda_0 t], \tag{16}$$

表 1： 推定された最適プルーフテスト実施間隔.

λ_D	1.0×10^{-5}	1.0×10^{-6}	1.0×10^{-7}	1.0×10^{-8}
DC		0.6		
c_3/c_0		t_0^* (年)		
1.0×10^{6}	4.0398×10^{-2}	4.0398×10^{-1}	4.0398	40.398
1.0×10^{7}	1.2767×10^{-2}	1.2767×10^{-1}	1.2767	12.767
1.0×10^{8}	4.0363×10^{-3}	4.0364×10^{-2}	4.0366×10^{-1}	4.0363
DC		0.9		
1.0×10^{6}	1.6159×10^{-1}	1.6159	16.159	161.59
1.0×10^{7}	5.10666×10^{-2}	5.10669×10^{-1}	5.10669	51.066
1.0×10^{8}	1.6145×10^{-2}	1.6146×10^{-1}	1.6146	16.146
DC		0.99		
1.0×10^{6}	1.6159	16.159	161.59	1615.93
1.0×10^{7}	5.1067×10^{-1}	5.1067	51.066	510.67
1.0×10^{8}	1.6146×10^{-1}	1.6146	16.146	161.45

に従う場合を考える．ここで，$\lambda_0(>0)$ は DU 故障率もしくは作動要求率を表わす．特に，DU 故障率 λ_0 については，E/E/PE 安全関連系に対する所与の危険側故障率 λ_D から自己診断率 DC を用いて，$\lambda_0=(1-\mathrm{DC})\lambda_D$ として与えられる．また，この場合，DU 故障率が作動要求率と同じとなる状況を想定しているが，特に，低頻度作動要求モード上においては，あり得ない条件設定ではないものと考える．式 (15) および式 (16) から，導出した最適プルーフテスト実施方策における $H_{X+Y}(t)$ は，

$$H_{X+Y}(t)\equiv\Pr\{X+Y\le t\}=\int_0^t G_Y(t-x)dF_X(x)$$
$$=1-(1+\lambda_0 t)\exp[-\lambda_0 t], \tag{17}$$

となり，2 次のガンマ分布に従うことがわかる．したがって，

$$\int_0^{t_0}\bar{H}_{X+Y}(t)dt=\frac{2}{\lambda_0}(1-e^{-\lambda_0 t_0})-t_0e^{-\lambda_0 t_0}, \tag{18}$$

および，

$$r_{X+Y}(t)=\frac{\lambda_0^2 t}{1+\lambda_0 t}, \tag{19}$$

がそれぞれ得られ，最適プルーフテスト実施方策における μ は，

$$\frac{1}{\mu}\equiv\int_0^{\infty}\bar{H}_{X+Y}(t)dt=\frac{2}{\lambda_0}, \tag{20}$$

より，$\mu=\lambda_0/2$ を得る．これより，有限な t_0^* が存在する条件は，前述した議論から，

$$r_{X+Y}(\infty)=\lambda_0>\frac{\mu c_3}{c_3-c_0}. \tag{21}$$

すなわち，

$$c_3>2c_0, \tag{22}$$

と与えられる．

表 1 に，導出した最適プルーフテスト実施方策に基づいて推定した最適プルーフテスト実施間隔を表す．表 1 では，IEC61508 で規定された DC に関する規格しきい値に従い，0.6，0.9，0.99 の場合について，それぞれ，SIL のしきい値に基づいて与えた危険側故障率 λ_D および危害コスト比 c_3/c_0 に沿って最適プルーフテスト実施間隔を推定した．表 1 に示した推定結果から，危険側故障率 λ_D が減少するにつれて，また，

自己診断率 DC が増加するにつれて，危害事象発生確率は低下するため，最適プルーフテスト実施間隔は一定のコスト比において長くなることがわかる．一方，一定の危険側故障率および自己診断率において，最適プルーフテスト実施間隔はコスト比が増大するについて短くなることもわかる．つまり，たとえ高い安全性を達成しているとしても，危害事象発生時の危害コストが保全コストに対して非常に大きくなるにつれて，そのリスクを回避すべく，最適プルーフテスト実施間隔は短く推定されることがわかる．また，通常，プルーフテスト実施間隔は半年から 2 年程度であると言われているが [6]，高い安全性を有しつつもコスト比が非常に大きい場合，その周辺で最適プルーフテスト実施間隔が推定される場合も散見された．

6　おわりに

本研究では，DU フォールトの検出および修復に主眼におく保全活動であるプルーフテストの最適実施間隔を決定する問題を定義すると共に，E/E/PE 安全関連系における保全コストと危害事象発生時のリスクに応じながら，最適なプルーフテスト実施間隔を導くための最適方策を求めた．具体的には，E/E/PE 安全関連系における危害事象発生論理および E/E/PE 安全関連系への作動要求率に基づいて，危害事象発生もしくはプルーフテスト実施までの運用パターンを列挙しつつ，各運用パターンにおける 1 サイクル当たりの期待コストおよび期待時間を導出し，単位時間当たりの期待費用を最小化するプルーフテスト実施間隔を解析的に議論した．また，導出した最適プルーフテスト実施方策に対する適用例では，一定の条件下において，E/E/PE 安全関連系の危険側故障発生率，自己診断率，および作動要求率を与えながら，危害コスト比に応じて最適なプルーフテスト実施間隔が推定できることを示した．今回の議論は，E/E/PE 安全関連系の状態およびそれへの作動要求に関する不確実性に基づいて，保全コストや危害リスクに対して合理的な保全実施計画の策定を支援するための一つの理論的手法として期待される．今後は，より現実的な状況を想定しながら，今回導出した最適プルーフテスト実施方策に対する数値実験を網羅的に行い，これから得られる知見や顕在化する問題を整理を反映しつつ,「作動要求状態・危険側故障論理」にも対応したモデルの改良など今回議論した手法の改良も必要である．

参考文献

[1] IEC 61508: Functional safety of electrical/electronic/programmable electronic safety-related systems, Edition 2.0, 2010.

[2] E. Kato and Y. Sato, “Safety integrity levels model for IEC 61508 —examination of modes of operation —,” *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, Vol. E83-A, No. 5, pp. 863–865, 2000.

[3] Y. Misumi and Y. Sato, “Estimation of average hazardous-event-frequency for allocation of safety-integrity levels,” *Reliability Engineering and System Safety*, Vol. 66, No. 2, pp. 135–144, 1999.

[4] T. Nakagawa, *Maintenance Theory of Reliability*. Springer-Verlag, 2005.

[5] S. Osaki, *Applied Stochastic System Modeling*. Springer-Verlag, Berlin, Heidelberg, 1992.

[6] 佐藤吉信,「機能安全の基礎」，日本規格協会，東京，2014.

[7] I. Yoshimura and Y. Sato, “Safety achieved by the safe failure fraction (SFF) in IEC 61508,” *IEEE Transactions on Reliability*, Vol. 57, No. 4, pp. 662–669, 2008.