設計自動化49－6
(1989.10.25)

多重化によるフェールセーフ設計

Design of Fail-Safe Systems by Redundancy Technique

中島　恭一
Kyoichi　NAKASHIMA

姫路工業大学
Himeji Institute of Technology

あらまし　本報告では，システムを多重使用することによりフェールセーフ特性を改善する可能性について理論的検討を行う．先ず，同じ要求出力であっても入力によって出力誤りの発生確率が異なる多値出力システムについて，期待損失を最小にする多重化方式はk-out-of-n冗長であることを証明し，多重化により期待損失が小さくなるための条件を明らかにする．次に，それを利用して危険側出力誤り率を最小にする多重化方式や危険側出力誤り率の減少が保障されるための条件について議論し，voterの故障が無視できない場合の考察も行う．また，出力誤り率が一定値以下という条件下で危険側出力誤り率を最小にする多重化方式も検討する．得られた結果は多重化によりフェールセーフ特性を改善する際の有力な指針を与える．

Abstract　The paper considers on the possibility of improving fail-safe characteristics through the use of redundancy. For systems in which the probability that an incorrect output is observed differs with input values, we adopt the redundant use of n copies of identical systems which we call the n-redundant systems. First, it is proved that the n-redundant system that minimizes the expected loss is a k-out-of-n redundant system under the condition that the voter functions perfectly, and a necessary condition for reducing the expected loss by the redundant use is clarified. Next, the paper discusses the redundancy technique for minimizing the probability of dangerous errors and presents some necessary conditions for reducing its probability.

1．はじめに

システムの大規模化，自動化に伴い，その故障や異常の発生は生命や財産を脅かす事故を引き起こすことになりかねないため，故障や異常が発生しても安全側の出力を保障するフェールセーフ化を計ることが重要になっている。特に，自動化，エレクトロニクス化に伴いシステムには各種の制御装置，監視装置，防護装置が取り付けられているが，こうした装置の誤動作が危険側に働かないようにすることが必要であろう。鉄道信号，航空機，原子炉制御などではかなり古くからフェールセーフ設計がとられている[1]し，産業用ロボットなどのいわゆるメカトロ機械の安全確認作業システム[2]のフェールセーフ化も計られている．

フェールセーフシステムを構成するには非対称誤り素子の実現が不可欠となる[3]が，そのような素子として重力場や永久磁石などの外力を利用したものや半導体を利用した演算素子[4]や論理回路[5][6]なども考案されている．しかし，完全な（危険側に誤る確率が0である）非対称誤り特性を実現することが困難であり，又実現できたとしてもそれらを使ってフェールセーフシステムを構成するためには種々の制約があることも多い．

例えば，各種の監視装置，防護装置，安全装置などは多くの場合，異常や安全を監視するセンサー部，センサー部からの信号を処理する回路部，回路部の判断

により駆動装置を動かす動作部から構成される．これらのシステムのフェールセーフ化を計る場合，信号（情報）伝達のあらゆる過程で非対称誤り特性を持つユネイト性を保持される必要があるが，それらの過程全てに非対称誤り特性を実現することは困難である．特に，センサーや駆動装置の中に使われるメカニカルな部品のフェールセーフ化がネックになる場合が多い．また，プラントの状態診断システムや防護システム，各種制御システムなど要求に応じて複数個の可能な出力のいずれかを発する多値出力システムとしてモデル化されるシステムでは，要求出力が変わると危険側出力も変わることが多く，その場合のフェールセーフ化はますます困難となる．従って，完全なフェールセーフシステムを構成できなかったとしても，危険側に誤る確率ができるだけ小さいシステムを構成することが必要となる．本論文では，そのための手段として多重化を用いてフェールセーフ特性の改善を計ることを考える．

我々は２値出力システムを包含する多値出力システムの最適多重化方式に関し考察してきた[7]-[9]が，本論文では先ず，同じ要求出力であっても入力によって出力誤りの発生確率が異なる場合について，期待損失を最小にする冗長方式はk-out-of-n冗長であることを証明し，多重化により期待損失が小さくなるための条件を示す．これは，文献（７）－（９）の結果の拡張，一般化であり，以下のフェールセーフ特性の改善の考察にも重要な役割を果たす．次に，危険側出力誤り率を最小にする多重化方式や危険側出力誤り率の減少が保障されるための条件について議論する．更に，voterの故障が無視できない場合の考察も行う．また，危険側出力誤り率を小さくすることだけを考えると安全側出力誤り率が大きくなる場合もあり，両方の出力誤りを合わせた出力誤り率が一定値以下という条件下で危険側出力誤り率を最小にする多重化方式も検討する．

２．m値出力システムと危険側出力誤り

要求に応じて出力yが$\Gamma_S=\{0, 1, \cdots, m-1\}$のm個のいずれかの値を発するm値出力システムSを考える．システムSはℓ個の入力$x_1, x_2, \cdots, x_\ell$をもち，入力x_i（$i=1, 2, \cdots, \ell$）は$\Gamma_i=\{0, 1, \cdots, \beta_i-1\}$の$\beta_i$個のいずれかの値を取る．

$X\equiv(x_1, x_2, \cdots x_\ell)$，$\Gamma_I\equiv\overset{\ell}{\underset{i=1}{\times}}\Gamma_i$とすると，システムSは入力Xに対して離散関数ｆ（Ｘ）（写像ｆ：$\Gamma_I\rightarrow\Gamma_S$）の値に等しい要求出力ｒを出力するように設計されている．従って，入力Xに対し実際の観測出力ｙが要求出力ｒ（＝ｆ（Ｘ））に等しければシステムは正常である．しかし，システムの故障や異常の発生によりｒとは異なる出力が観測される出力誤りが生じる可能性がある．

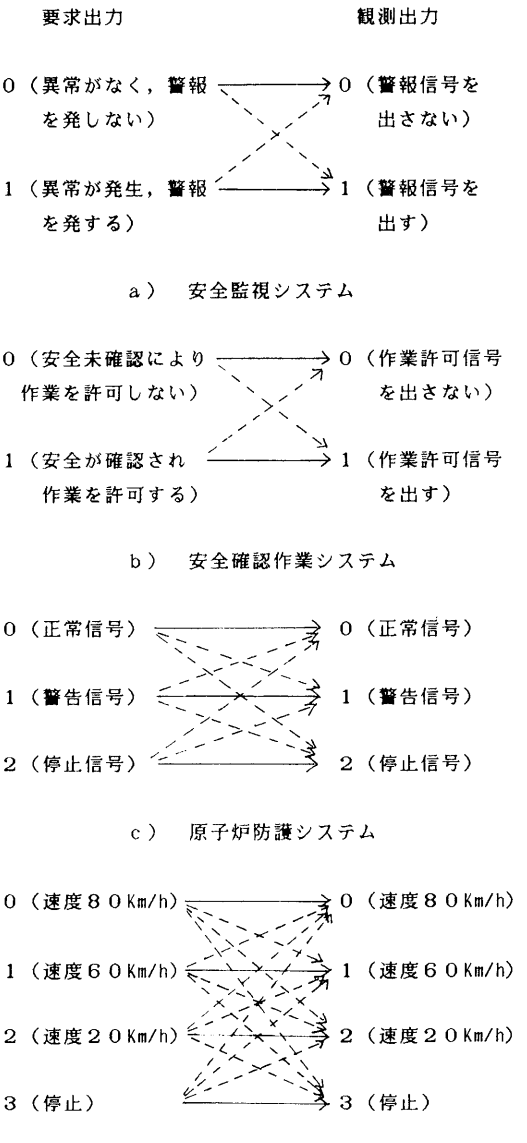


図１　多値出力システムの例

２値出力システムの例としては自動火災警報装置などの安全監視システム[11]（図１－ａ）やロボットなどの安全確認作業システム（図１－ｂ）がある．原子炉などの各種プラントにおいて，プラント内の状態により正常信号，停止信号だけでなく，異常の程度に応じた警告信号を発する防護システムは３値出力システムの例である（図１－ｃ）．流量，温度，圧力，速度などの物理量をｍ個のレベルに制御する制御システムはｍ値出力システムの例である（図１－ｄ）．

ｍ値出力システムについて，次の記号を定義する．

$p_{x,y}$：入力Ｘに対し，観測出力がｙである確率．

$$\sum_{y \in \Gamma_S} p_{x,y} = 1 \quad \text{for} \quad X \in \Gamma_I .$$

$$P_{L(x,y)} \equiv \sum_{\delta=0}^{y} p_{x,\delta} , \quad P_{U(x,y)} \equiv \sum_{\delta=y}^{m-1} p_{x,\delta} \qquad (1)$$

α_x：入力Ｘの発生確率．$\sum_{X \in \Gamma_I} \alpha_x = 1$．

$w_{r,y}$：要求出力ｒに対し，観測出力がｙであるときの損失．

システムの期待損失W_1は次式で与えられる．

$$W_1 = \sum_{X \in \Gamma_I} \sum_{y \in \Gamma_S} \alpha_x w_{r(x),y} p_{x,y} \qquad (2)$$

要求出力ｒに対し，観測出力ｙに出力誤りが生じたとき（$y \neq r$），それが危険側出力誤り（D-error）であれば$\delta_{r,y}=1$，安全側出力誤り（S-error）であれば$\delta_{r,y}=0$とする（但し，$\delta_{r,r}=0$とする）．そのとき，

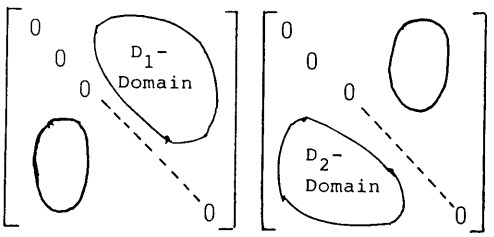
Δ：ｒ行ｙ列（(r,y)－要素）が$\delta_{r,y}$である行列を定義する．行列Δの中で$\delta_{r,y}=1$である(r,y)－要素から成る領域を危険側誤り領域又はＤ領域と呼ぶ．Ｄ領域のうち対角要素に関して右上側の部分（$y > r$の部分）の領域をD_1領域，左下側の部分（$y < r$の部分）の領域をD_2領域と呼ぶ．システムのＤ領域がD_1領域又はD_2領域のいずれかのみから構成されるならば片側危険システム，Ｄ領域がD_1領域とD_2領域の両方から構成されるならば両側危険システムという（図２参照）．

例えば，図１－ｃの原子炉防護システムの場合，要求出力１（警告）に対し観測出力が０（正常）のとき及び要求出力２（停止）に対し観測出力が０又は１のとき危険側出力誤りであるとすると，システムはD_2領域のみから成る片側危険システムである．

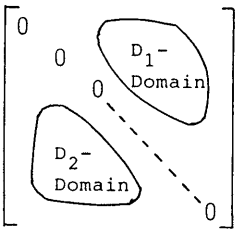
単一システムの危険側出力誤り率PD_1は

$$PD_1 = \sum_{X \in \Gamma_I} \sum_{y \in \Gamma_S} \alpha_x \delta_{r(x),y} p_{x,y} \qquad (3)$$

で与えられ，PD_1は危険側出力誤りに対し$w_{r,y}=1$，安全側出力誤り及び正常出力に対し$w_{r,y}=0$としたときの期待損失W_1に等しい．



（ａ）　片側危険システム



（ｂ）　両側危険システム

図２　行列ΔのＤ領域によるシステムの分類

３．期待損失を最小にする多重化方式と期待損失減少の条件

３．１．ｍ値出力システムの多重化

$p_{x,y}$（$X \in \Gamma_I$，$y \in \Gamma_S$）の値が同じであるｍ値出力システムS_1，S_2，…，S_n（$n \geq 2$）を冗長使用したｎ重化システム（以下ｎ－冗長システムと呼ぶ）において，その出力ｙはｎ個のシステムの出力y_1，y_2，…，y_nよりvoterを通して決定される．ｙはy_1，y_2，…，y_nの多値論理関数

$$y = \phi (y_1, y_2, \cdots, y_n) \qquad (4)$$

として表され，この関数をｎ－冗長システムの構造関数と呼ぶ．

ｎ－冗長システムに対し，文献（９）と同様に次の仮定をする．

１．ｎ個のｍ値出力システムの出力誤りの発生は統計的に独立である．

２．voterは論理和∨，論理積・のみを使って構成できる．即ち構造関数$\phi (y_1, y_2, \cdots, y_n)$は変数$y_1$，$y_2$，…，$y_n$と二つの演算子∨，・のみを使って表現できる．

３．出力ｙの決定に関与しない出力y_1，y_2，…，

y_nは存在しない．

4．voterは完全に動作する．即ちvoterによる出力誤りは生じない．

n－冗長システムに対し次の記号を定義する．

$p^{(n)}_{x,y}$：入力Xに対し，観測出力がyである確率．

$$\sum_{y\in\Gamma_s} p^{(n)}_{x,y} = 1 \quad \text{for} \quad X\in\Gamma_I .$$

$$P^{(n)}_{L(x,y)} \equiv \sum_{\delta=0}^{y} p^{(n)}_{x,\delta},\quad P^{(n)}_{U(x,y)} \equiv \sum_{\delta=y}^{m-1} p^{(n)}_{x,\delta} \qquad (5)$$

次の関係が成り立つ．

$$\left.\begin{aligned} P_{U(x,y)} &= 1-P_{L(x,y-1)} \\ P^{(n)}_{U(x,y)} &= 1-P^{(n)}_{L(x,y-1)} \end{aligned}\right\} \qquad (6)$$

$$(0\leqq y\leqq m-1)$$

2状態システムの構造関数$z=\phi(z_1, z_2, \cdots, z_n)$に対する信頼度関数を$R(p_1, p_2, \cdots, p_n)$，$p_1=p_2=\cdots=p_n=p$のとき$h(p)\equiv R(p, p, \cdots, p)$とする．但し，$p_i\equiv P_r\{z_i=1\}$，$i=1, 2, \cdots, n$である．このとき，次の関係が成り立つ．

$$\left.\begin{aligned} P^{(n)}_{U(x,y)} &= h(P_{U(x,y)}) \\ P^{(n)}_{L(x,y)} &= 1-h(1-P_{L(x,y)}) \end{aligned}\right\} \qquad (7)$$

$$\begin{aligned} p^{(n)}_{x,y} &= h(P_{U(x,y)})-h(P_{U(x,y+1)}) \\ &= h(1-P_{L(x,y-1)}) \\ &\quad -h(1-P_{L(x,y)}) \end{aligned} \qquad (8)$$

$$(X\in\Gamma_I,\ 0\leqq y\leqq m-1)$$

$\{y_1, y_2, \cdots, y_n\}$を$y_{(1)}\geqq y_{(2)}\geqq\cdots\geqq y_{(n)}$のように値の減少する順序に並べ変えたとき，n－冗長システムの観測出力を$y=y_{(k)}$により決める場合，このシステムはk-out-of-n冗長（$1\leqq k\leqq n$）であるという．$k=1$ならば$y=\max_r\{y_r\}$となり並列冗長，$k=n$ならば$y=\min_r\{y_r\}$となり直列冗長であるという．k-out-of-n冗長システムの構造関数は，2値k-out-of-n冗長システムの構造関数の変数を多値変数に変えることにより得られる．

2値k-out-of-n冗長システムの信頼度関数

$$h_{k,n}(p) \equiv \sum_{a=k}^{n} \binom{n}{a} p^a (1-p)^{n-a} \qquad (9)$$

を使って，k-out-of-n冗長システムに対して式（7）（8）と同様な次の関係が得られる．

$$\left.\begin{aligned} P^{(n)}_{U(x,y)} &= h_{k,n}(P_{U(x,y)}) \\ P^{(n)}_{L(x,y)} &= 1-h_{k,n}(1-P_{L(x,y)}) \end{aligned}\right\} \qquad (10)$$

$$\begin{aligned} p^{(n)}_{x,y} &= h_{k,n}(P_{U(x,y)})-h_{k,n}(P_{U(x,y+1)}) \\ &= h_{k,n}(1-P_{L(x,y-1)}) \\ &\quad -h_{k,n}(1-P_{L(x,y)}) \end{aligned} \qquad (11)$$

$$(X\in\Gamma_I,\ 0\leqq y\leqq m-1)$$

次式が成立することが証明されている[10]．

$$h(p) = \sum_{k=1}^{n} a_k h_{k,n}(p) \qquad (12)$$

但し，

$$a_k\geqq 0,\ k=1, 2, \cdots, n \text{ かつ } \sum_{k=1}^{n} a_k = 1 .$$

3．2．期待損失を最小にする多重化方式

n－冗長システムの期待損失W_nは次式で与えられる．

$$\begin{aligned} W_n &= \sum_{X\in\Gamma_I}\sum_{y\in\Gamma_S} \alpha_X w_{f(x),y} p^{(n)}_{x,y} \\ &= \sum_{X\in\Gamma_I}\sum_{y\in\Gamma_S} \alpha_X w_{f(x),y}\{h(P_{U(x,y)}) \\ &\quad -h(P_{U(x,y+1)})\} \end{aligned} \qquad (13)$$

同様に，k-out-of-n冗長システムの期待損失$W_{k,n}$は

$$\begin{aligned} W_{k,n} &= \sum_{X\in\Gamma_I}\sum_{y\in\Gamma_S} \alpha_X w_{f(x),y}\{h_{k,n}(P_{U(x,y)}) \\ &\quad -h_{k,n}(P_{U(x,y+1)})\} \end{aligned} \qquad (14)$$

［性質1］期待損失W_nを最小にするn－冗長システムはk-out-of-n冗長システムである．

（証明）式（12）を式（13）に代入すると，

$$\begin{aligned} W_n &= \sum_{X\in\Gamma_I}\sum_{y\in\Gamma_S} \alpha_X \sum_{k=1}^{n} a_k w_{f(x),y} \\ &\quad \{h_{k,n}(P_{U(x,y)})-h_{k,n}(P_{U(x,y+1)})\} \\ &= \sum_{k=1}^{n} a_k \Big[\sum_{X\in\Gamma_I}\sum_{y\in\Gamma_S} \alpha_X w_{f(x),y} \\ &\quad \{h_{k,n}(P_{U(x,y)})-h_{k,n}(P_{U(x,y+1)})\}\Big] \\ &= \sum_{k=1}^{n} a_k W_{k,n} \geqq \min_k W_{k,n} \end{aligned} \qquad (15)$$

$W_{k,n}$を最小にするkの値をk^*とすれば，$W_{k^*,n}$がW_nの最小値となる．（証明終）

性質1よりW_nを最小にするn－冗長システムは，n個のk-out-of-n冗長システム（$1\leqq k\leqq n$）の$W_{k,n}$の中から最小の$W_{k^*,n}$を選べばよい．

入力$X\in\Gamma_I$に対し観測出力が要求どうりのf（X）である確率$p_{f(x),f(x)}$は1／2より大きいと考えてよい．従って，次の仮定をする．

（1）入力Xのとき，$y<f(X)$について$P_{L(x,y)}<1/2$及び$P_{U(x,y+1)}>1/2$である．

（2）入力Xのとき，$y>f(X)$について$P_{U(x,y)}<1/2$及び$P_{L(x,y-1)}>1/2$である．

このとき，つぎの性質が成り立つ．

［性質2］（ｉ）$y<r$について$w_{r,y}\geqq 0$，$y\geqq r$について$w_{r,y}=0$が全ての$r\in\Gamma_S$に対して成り立つならば，$k^*=1$（並列冗長）である．

（ｉｉ）$y\leqq r$について$w_{r,y}=0$，$y>r$について$w_{r,y}\geqq 0$が全ての$r\in\Gamma_S$に対して成り立つならば，$k^*=n$（直列冗長）である．

（証明）式（９）より

$$\frac{dh_{k,n}(p)}{dp}=\beta_{k,n}\left(\frac{p}{1-p}\right)^{k-1}(1-p)^{n-1} \qquad (16)$$

但し，

$$\beta_{k,n}\equiv\frac{n!}{(k-1)!\,(n-k)!}$$

で，$\beta_{1,n}=\beta_{n,n}=n=\min_k \beta_{k,n}$ が成り立つ．

$1>p>1/2$のとき$\frac{p}{1-p}>1$だから$\frac{dh_{k,n}(p)}{dp}$はｋ＝１のとき最小であり，$0\leqq p<1/2$のとき$\frac{p}{1-p}<1$だから$\frac{dh_{k,n}(p)}{dp}$はｋ＝ｎのとき最小である．

（ｉ）この場合，

$$W_{k,n}=\sum_{X\in\Gamma_1}\sum_{y\in\Gamma_S}(y<f(X))^{\alpha_X w_{f(X),y}}\{h_{k,n}(P_{U(X,y)})-h_{k,n}(P_{U(X,y+1)})\}$$

となり，仮定より$P_{U(X,y)}\geqq P_{U(X,y+1)}>1/2$だから｛｝内はｋ＝１のとき最小となる．

（ｉｉ）この場合，

$$W_{k,n}=\sum_{X\in\Gamma_1}\sum_{y\in\Gamma_S}(y>f(X))^{\alpha_X w_{f(X),y}}\{h_{k,n}(P_{U(X,y)})-h_{k,n}(P_{U(X,y+1)})\}$$

となり，仮定より$P_{U(X,y+1)}\leqq P_{U(X,y)}<1/2$だから｛｝内はｋ＝１のとき最小となる．　（証明終）

３．３．期待損失が減少するための条件

次に，多重化により期待損失の減少が保障されるための条件について考察する．

ｎ－冗長システムの構造関数φより生成される２値論理関数$z=\phi(z_1,z_2,\cdots,z_n)$を，その論理和形（sum-of-products form）及び論理積形（product-of-sums form）に関する次の条件により分ける．

（Ⅰ）論理和形が次数（変数の数）１の積項を含まず，かつ論理積形が次数１の和項を含まない．

（Ⅱ）論理和形が次数１の積項を含む．

（Ⅲ）論理積形が次数１の和項を含む．

例えば，k-out-of-n冗長（$2\leqq k\leqq n-1$）は条件Ⅰを，1-out-of-n冗長（並列冗長）は条件Ⅱを，n-out-of-n冗長（直列冗長）は条件Ⅲを満足する．

［性質3］（１）条件Ⅰを満足するとき，$h'(p_1)=h'(p_2)=1$であるp_1，p_2（$0<p_1<p_2<1$）が存在し，$0\leqq p<p_1$及び$p_2<p\leqq 1$では$0\leqq h'(p)<1$である．（２）条件Ⅱを満足するとき，$h'(p_2)=1$であるp_2（$0<p_2<1$）が存在し，$p_2<p\leqq 1$では$0\leqq h'(p)<1$である．（３）条件Ⅲを満足するとき，$h'(p_1)=1$であるp_1（$0<p_1<1$）が存在し，$0\leqq p<p_1$では$0\leqq h'(p)<1$である．但し，$h'(a)\equiv\left.\frac{dh(p)}{dp}\right|_{p=a}$．

（証明）それぞれの場合について次のことが成り立つ[12]ことより明らかである．（１）$h(p)$は$0\leqq p\leqq 1$でＳ字形関数（S-shaped function）となり$h'(0)=h'(1)=0$が成り立つ．（２）$h'(0)>1$，$h'(1)=0$が成り立つ．（３）$h'(0)=0$，$h'(1)>1$が成り立つ．　（証明終）

k-out-of-n冗長システム（$2\leqq n\leqq 5$）のp_1，p_2の値を表１に示す．なお，$2\leqq k\leqq n-1$に対し，$h_{k,n}(p)=p$（$0<p<1$）を満足するｐの値$\rho_{k,n}$が求められており[13]，$0<p<\rho_{k,n}$では$h_{k,n}(p)<p$，$\rho_{k,n}<p<1$では$h_{k,n}(p)>p$となる（$p_1<\rho_{k,n}<p_2$が成立）．k-out-of-n冗長システム（$2\leqq n\leqq 5$）の$\rho_{k,n}$の値も表１に示す．

表１　k-out-of-n冗長システムのp_1（上段），p_2（下段）と$\rho_{k,n}$（中段）

n＼k	1	2	3	4	5
2		0.5000			
	0.5000				
3		0.2112	0.6934		
		0.500			
	0.3066	0.7888			
4		0.1037	0.3612	0.7071	
		0.232	0.768		
	0.2929	0.6388	0.8963		
5		0.06025	0.2403	0.4495	0.7248
		0.131	0.500	0.869	
	0.2752	0.5505	0.7597	0.93975	

次の性質はｎ－冗長システムの$p_{x,y}^{(n)}$が単一システムの$p_{x,y}$よりも小さくなるための条件を与える．

［性質4］n－冗長システムの構造関数φが条件Ⅰを満足するとき，入力Xに対し$0<P_{U(x,y)}<p_1$または$p_2<P_{U(x,y+1)}<1$が成り立つならば$p^{(n)}_{x,y}<p_{x,y}$である．また，条件Ⅱ（または条件Ⅲ）を満足するとき，入力Xに対し$p_2<P_{U(x,y+1)}<1$（または$0<P_{U(x,y)}<p_1$）が成り立つならば$p^{(n)}_{x,y}<p_{x,y}$である．但し，$p_{x,y}\neq 0$とする．

（証明）$p_{x,y}\neq 0$より$P_{U(x,y)}\neq P_{U(x,y+1)}$．いずれの場合も，性質3より$P_{U(x,y+1)}\leqq p\leqq P_{U(x,y)}$で$0\leqq h'(p)<1$が成り立つ．従って，$p^{(n)}_{x,y}=h(P_{U(x,y)})-h(P_{U(x,y+1)})<P_{U(x,y)}-P_{U(x,y+1)}=p_{x,y}$が成り立つ．　（証明終）

n重化による$p_{x,y}$の減少率$I_{x,y}$を

$$I_{x,y}\equiv\frac{p^{(n)}_{x,y}}{p_{x,y}}=\frac{h(P_{U(x,y)})-h(P_{U(x,y+1)})}{P_{U(x,y)}-P_{U(x,y+1)}}\qquad(17)$$

より定義すると，$0\leqq p<p_1$では$h'(p)$はpに関し単調増加，$p_2<p\leqq 1$では単調減少だから，

（1）$0<P_{U(x,y)}<p_1$のとき，$I_{x,y}$は$P_{U(x,y)}$が小さいほど小さくなり，

（2）$p_2<P_{U(x,y+1)}<1$のとき，$I_{x,y}$は$P_{U(x,y+1)}$が大きいほど（即ち，$P_{L(x,y)}$が小さいほど）小さくなる．

性質4を使って，多重化により期待損失が小さくなるための条件を求めることができる．

［性質5］$y\neq r$について$w_{r,y}\geqq w_{r,r}$が全ての$r\in\Gamma_s$に対して成り立つと仮定する．全ての入力Xに対し，出力yが$y<f(X)$のとき$P_{U(x,y+1)}>p_2$，$y>f(X)$のとき$P_{U(x,y)}<p_1$の関係が少なくとも1つのk-out-of-n冗長システム（$2\leqq k\leqq n-1$）について成り立つとき，$W_{k\cdot,n}<W_1$である．但し，全ての（X，y）の組（$y\neq f(X)$）に対し$p_{x,y}=0$又は$w_{f(x),y}=w_{f(x),f(x)}$が成立することはないとする．

（証明）k-out-of-n冗長システムに対し

$$W_{k,n}=\sum_{X\in\Gamma_1}\alpha_x w_{f(x),f(x)}+\sum_{X\in\Gamma_1}\sum_{\substack{y\in\Gamma_s\\(y\neq f(X))}}\alpha_x(w_{f(x),y}-w_{f(x),f(x)})\,p^{(n)}_{x,y}$$

上の関係が成り立つとき条件Ⅰを満足するから，性質4より$p_{x,y}\neq 0$ならば$p^{(n)}_{x,y}<p_{x,y}$だから，$W_{k,n}<W_1$が成立する．$W_{k\cdot,n}\leqq W_{k,n}$より，$W_{k\cdot,n}<W_1$が得られる．　（証明終）

観測出力が要求どうりに得られる確率$p_{x,f(x)}$（$X\in\Gamma_1$）は1に近いから，通常は性質5の関係が成立するとみてよい．

4．危険側出力誤り率の改善

4．1．危険側出力誤り率を最小にする多重化方式

n－冗長システムの危険側出力誤り率PD_nは

$$PD_n=\sum_{X\in\Gamma_1}\sum_{y\in\Gamma_s}\alpha_x\delta_{f(x),y}\,p^{(n)}_{x,y}\qquad(18)$$

で与えられ，PD_nは危険側出力誤りに対し$w_{r,y}=1$，安全側出力誤り及び正常出力に対し$w_{r,y}=0$としたときの期待損失W_nに等しい．

従って，性質1，2は危険側出力誤り率に対し次のように言い替えることができる．

［性質1′］危険側出力誤り率PD_nを最小にするn－冗長システムはk-out-of-n冗長システムである．

即ち，PD_nを最小にするn－冗長システムは，n個のk-out-of-n冗長システム（$1\leqq k\leqq n$）の$PD_{k,n}$の中から最小の$PD_{k\cdot,n}$を選べばよい．

［性質2′］（i）D_2領域のみから成る片側危険n－冗長システムでは，並列冗長システムがPD_nを最小にする．

（ii）D_1領域のみから成る片側危険n－冗長システムでは，直列冗長システムがPD_nを最小にする．

4．2．危険側出力誤り率が減少するための条件

同様に，性質5は次のように言い替えることができ，これは多重化により危険側出力誤り率が小さくできるための条件を与える．

［性質5′］全ての入力Xに対し，出力yが$\delta_{f(x),y}=1$でかつ$y<f(X)$のとき$P_{U(x,y+1)}>p_2$，$\delta_{f(x),y}=1$でかつ$y>f(X)$のとき$P_{U(x,y)}<p_1$の関係が少なくとも1つのk-out-of-n冗長システム（$2\leqq k\leqq n-1$）について成り立つとき，$PD_{k\cdot,n}<PD_1$である．

特に，要求出力rに対し，観測出力yが$r<y<S(r)$のとき安全側出力誤りで$S(r)\leqq y\leqq m-1$のとき危険側出力誤りになるようにD_1領域が，$0\leqq y\leqq T(r)$のとき危険側出力誤りで$T(r)<y<r$のとき安全側出力誤りになるようにD_2領域が構成される場合，次の性質6のように条件は緩和される．

［性質6］全ての入力Xに対し，$P_{U(x,S(f(x)))}<\rho_{k,n}$，$P_{U(x,T(f(x))+1)}>\rho_{k,n}$の関係が少なくとも1つのk-out-of-n冗長システム（$2\leqq k\leqq n-1$）について成り立つとき，$PD_{k\cdot,n}<PD_1$である．

（証明）このとき

$$PD_1 = \sum_{X \in \Gamma_1} \alpha_X \left(1 - P_{U(X,T(f(X))+1)} + P_{U(X,S(f(X)))}\right)$$

$$PD_{k,n} = \sum_{X \in \Gamma_1} \alpha_X \left(1 - h_{k,n}\left(P_{U(X,T(f(X))+1)}\right) + h_{k,n}\left(P_{U(X,S(f(X)))}\right)\right)$$

$h_{k,n}(P_{U(X,S(f(X)))}) < P_{U(X,S(f(X)))}$,

$h_{k,n}(P_{U(X,T(f(X))+1)}) > P_{U(X,T(f(X))+1)}$だから

$PD_{k,n} < PD_1$が成り立つ．$PD_{k^*,n} \leqq PD_{k,n}$だから

$PD_{k^*,n} < PD_1$である．　（証明終）

4．3．ｖｏｔｅｒの故障に関する考察

これまでは，ｎ－冗長システムのvoterによる出力誤りは生じないとの仮定の下で考察してきたが，ここではこの仮定を緩和してvoterによる出力誤りも考慮する場合の検討を行う．

Voterへの入力$Y=(y_1, y_2, \cdots, y_n)$に対して出力が$y$である確率を$p^{v}_{Y,y}$とすると危険側出力誤り率$PD'_n$は

$$PD'_n = \sum_{X \in \Gamma_1} \sum_{y_1 \in \Gamma_S} \sum_{y_2 \in \Gamma_S} \cdots \sum_{y_n \in \Gamma_S} \sum_{y \in \Gamma_S} \alpha_X \times \delta_{f(X),y}\, p_{X,y1}\, p_{X,y2} \cdots p_{X,yn}\, p^{v}_{Y,y} \quad (19)$$

となり$p^{v}_{Y,y}$がvoterの種類により異なるため簡単な式は得られない．

次の記号を定義する．

PD^1_n：voterが正常であっても危険側出力誤りが生じており，実際の観測出力も危険側出力である確率．

PD^2_n：voterが正常であれば危険側出力誤りが生じていたが，実際の観測出力が正常または安全側出力である確率．

PD^v_n：voterが正常であれば正しい出力または安全側出力を出していたが，voterの故障により危険側出力誤りが生じる確率．

$PD_n = PD^1_n + PD^2_n$，$PD^2_n \ll PD^1_n$より

$$PD'_n = PD^1_n + PD^v_n = PD_n - PD^2_n + PD^v_n \simeq PD_n + PD^v_n \quad (20)$$

のような近似を得る．多重化により$PD_n \ll PD_1$が実現したとしても，$PD'_n \ll PD_1$であるためには

$$PD^v_n \ll PD_1 \quad (21)$$

が成り立つことが条件になる．PD_nを最小にするk-out-of-n冗長を実現するvoterが（２１）式の条件を満たせばよいが，そうでない場合は

（１）k-out-of-n冗長よりも回路構成が簡単で（２１）式の条件を満たす他のvoterを探す，

（２）voterのフェールセーフ特性を改善する，

などの対策が必要となるが，フェールセーフな多数決演算回路を構成する研究[14]も見られる．

5．出力誤り率の制約下で危険側出力誤り率を最小にする多重化方式

信頼度関数ｈ（ｐ）を持つｎ－冗長システムを採用した場合，期待損失W_nは式（１４）より

$$W_n = \sum_{k=1}^{n} a_k W_{k,n} \quad (22)$$

で与えられる．ｎ－冗長システムの出力誤り率E_nは出力誤りに対し$w_{r,y}=1$，正常出力に対し$w_{r,r}=0$としたときの期待損失W_nに等しいから，

$$E_n = \sum_{k=1}^{n} a_k E_{k,n} \quad (23)$$

が成り立つ．同様に，危険側出力誤り率PD_nに対しても次式が成り立つ．

$$PD_n = \sum_{k=1}^{n} a_k PD_{k,n} \quad (24)$$

但し，$E_{k,n}$，$PD_{k,n}$はk-out-of-n冗長システムの出力誤り率，危険側出力誤り率である．

出力誤り率はフォールトトレランスを表す特性量の一つ，危険側出力誤り率はフェールセーフ性を表す特性量の一つと考えられるが，PD_nが最小な冗長システムがE_nも最小にするとは限らず，またPD_nが小さな冗長システムはE_nも小さいとも限らない．PD_nが小さいが逆にE_nが大きくなる冗長システムも多く，例えば片側危険システムで並列冗長や直列冗長を使用する場合はｈ（ｐ）がＳ字形関数にならないためにその様な傾向が見られる．従って，出力誤り率が一定値以下の制約の下で，危険側出力誤り率を最小にする多重化方式を求める問題が生じる．

［性質７］　制約条件$E_n \leqq E$（一定）の下でPD_nを最小にするｎ－冗長システムは次により求められる．

（ｉ）性質１′によりPD_nを最小にするk^*-out-of-n冗長システムに対し$E_{k^*,n} \leqq E$を満足すれば，このシステムが求めるものである．

（ｉｉ）$E_{k^*,n} > E$の場合．$\Omega_1 = \{k \mid E_{k,n} \leqq E\}$，$\Omega_2 = \{k \mid E_{k,n} > E\}$とする．

$$\frac{PD_{k1,n} - PD_{k2,n}}{E_{k2,n} - E_{k1,n}} = \max_{k \in \Omega_2}\left(\frac{PD_{k1,n} - PD_{k,n}}{E_{k,n} - E_{k1,n}}\right) = \min_{k \in \Omega_1}\left(\frac{PD_{k,n} - PD_{k2,n}}{E_{k2,n} - E_{k,n}}\right) \quad (25)$$

を満足する$k_1 \in \Omega_1$, $k_2 \in \Omega_2$を求める．このとき

$$a^*_{k1} = \frac{E_{k2,n} - E}{E_{k2,n} - E_{k1,n}} \qquad a^*_{k2} = \frac{E - E_{k1,n}}{E_{k2,n} - E_{k1,n}} \tag{26}$$

として，$a^*_{k1} PD_{k1,n} + a^*_{k2} PD_{k2,n}$が$PD_n$の最小値となる（$a^*_{k1} + a^*_{k2} = 1$，$a^*_{k1} E_{k1,n} + a^*_{k2} E_{k2,n} = E$を満足する）．即ち，$PD_n$を最小にするn－冗長システムは，確率$a^*_{k1}$で$k_1$-out-of-n冗長をとり確率$a^*_{k2}$で$k_2$-out-of-n冗長をとる冗長方式である．

（証明）（ｉ）は自明．（ｉｉ）b_k≡式（２５）の第２式の（）内，c_k≡式（２５）の第３式の（）内，とすると，$b_{k2} = c_{k1}$＝式（２５）の第１式，となる．また，$\Omega \equiv \Omega_1 \cup \Omega_2 = \{1, 2, \ldots, n\}$とする．

$$\begin{aligned} & a^*_{k1} PD_{k1,n} + a^*_{k2} PD_{k2,n} \\ &= (1 - a^*_{k2}) PD_{k1,n} + a^*_{k2} PD_{k2,n} \\ &= PD_{k1,n} - a^*_{k2} (PD_{k1,n} - PD_{k2,n}) \\ &= PD_{k1,n} - a^*_{k2} b_{k2} (E_{k2,n} - E_{k1,n}) \\ &= PD_{k1,n} - b_{k2} (E - E_{k1,n}) \end{aligned} \tag{27}$$

$\sum_{k \in \Omega} a_k E_{k,n} \leqq E$のとき，$\sum_{k \in \Omega} a_k PD_{k,n} \geqq a^*_{k1} PD_{k1,n} + a^*_{k2} PD_{k2,n}$を示せばよい．

$$\begin{aligned} & \sum_{k \in \Omega} a_k PD_{k,n} \\ &= \sum_{k \in \Omega_1} a_k PD_{k,n} + \sum_{k \in \Omega_2} a_k PD_{k,n} \\ &= \sum_{k \in \Omega_1} a_k \{PD_{k2,n} + c_k (E_{k2,n} - E_{k,n})\} \\ &\quad + \sum_{k \in \Omega_2} a_k \{PD_{k1,n} - b_k (E_{k.n} - E_{k1,n})\} \\ &\geqq \sum_{k \in \Omega_1} a_k \{PD_{k2,n} + b_{k2} (E_{k2,n} - E_{k,n})\} \\ &\quad + \sum_{k \in \Omega_2} a_k \{PD_{k1,n} - b_{k2} (E_{k,n} - E_{k1,n})\} \\ &= \left(\sum_{k \in \Omega_1} a_k\right) (PD_{k2,n} + b_{k2} E_{k2,n}) \\ &\quad + \left(\sum_{k \in \Omega_2} a_k\right) (PD_{k1,n} + b_{k2} E_{k1,n}) \\ &\quad - b_{k2} \sum_{k \in \Omega} a_k E_{k,n} \\ &\geqq PD_{k1,n} + b_{k2} E_{k1,n} - b_{k2} E \\ &= a^*_{k1} PD_{k1,n} + a^*_{k2} PD_{k2,n} \end{aligned} \tag{28}$$

（式（２７）より．$PD_{k2,n} + b_{k2} E_{k2,n} = PD_{k1,n} + b_{k2} E_{k1,n}$に注意．）　（証明終）

信頼度関数が$h(p) = a^*_{k1} h_{k1,n}(p) + a^*_{k2} h_{k2,n}(p)$であるようなvoterを構成できればよいが，できない場合はk_1-out-of-n voterとk_2-out-of-n voterを$a^*_{k1} : a^*_{k2}$の割合で使用することが必要になる．実際的には，この信頼度関数に近い構造を持ち，$E_n \leqq E$を満足するようなvoterを探すことになろう．

なお，危険側出力誤り率が一定値以下の制約の下で，出力誤り率を最小にする多重化方式を求める問題の解も同様に得ることができる．

６．むすび

多値出力システムとしてモデル化できるシステムのフェールセーフ特性を改善する一つの方法として，その多重化をはかることの有効性を検討した．voterの故障確率が十分小さければ，k-out-of-n冗長方式が危険側出力誤り率を最小にし，かつその出力誤り率は単一システムよりも小さくなることが保障される．しかし，voterの故障が無視できない場合は，voterのフェールセーフ化を計ることが必要になる．また，出力誤り率が一定値以下の制約の下で，危険側出力誤り率を最小にする多重化方式を求めた．

参考文献

(1) 信学会昭４９全国大会シンポジウム：“フェイルセイフと信頼性・安全性”，講演論文集文冊１，S13-1～9（1974）.

(2) 杉本，蓬原：“ロボットにおける安全確認作業システムの構成”，情報処理，29，2，pp.107-113（1988）.

(3) 三根，古賀：“フェール・セーフ・システムの構成理論について”，電学誌，95，9，pp.801-808（1975）.

(4) 土屋：“フェイルセイフ論理方式の研究”，電気試験所研究報告，695（1969）.

(5) 水上，古賀：“半導体によるフェイルセイフ論理回路の一実現法”，信学論（Ｄ），J65-D，12，pp.1550-1557（1982）.

(6) 蓬原：“非対称誤り素子によるフェイルセイフ論理回路の一構成法”，電学論（Ｃ），104，2，pp.29-34（1984）.

(7) 中島，大和：“期待損失を最小にする多値出力システムの多重化方式”，信学論（Ｄ），J69-D，11，pp.1565-1571（1986-11）.

(8) K. Nakashima and K. Yamato:“On optimal redundancy of multivalue-output systems”, IEEE Trans. Reliab., R-36, 2, pp.216-221 (1987).

(9) 中島，喜田，大和：“出力誤り率を最小にする多重化方式”，信学論（Ｄ），J72-D，6，pp.507-515（1989-06）.

(10) M.J. Phillips:“k-out-of-n:G systems are preferable”, IEEE Trans. Reliab., R-29, 2, pp.166-169 (1980).

(11) 幸田，井上，熊本，高見：“二つの故障モードをもつ安全監視システムの最適論理構造”，計測自動制御学会論文集，17,9，pp.908-913（1981-12）.

(12) J.D. Esary and F. Proschan:“The reliability of coherent systems”, in Redundancy Technique for Computing Systems (eds. R.H. Wilcox and W.C. Mann), Spartan Books, pp.47-61 (1962).

(13) Z.W. Birnbaum, J.D. Esary and S.C. Saunders :“Multi-component systems and structures and their reliability”, Technometrics, 3, 1, pp.55-77(Feb. 1961)

(14) K. Futsuhara and M. Mukaidono:“Application of window comparator to majority operation, Proc. 19th Int. Symp. on Multiple-Valued Logic, Guangzhou, China, pp.114-121 (1989).