

Fail-Safe 論理系の構成について

津野義頼

(早稲田大学大学院)

第1章 序言

システムの大型化, 複雑化に伴い, システム内に障害が発生しても常に安全側に落着く, いわゆる "Fail-Safe" システムの重要性が高まってきた。

本稿は, このような "Fail-Safe" システムの構成に関する筆者らの最近の研究結果をまとめたものである。

本章では, "Fail-Safe" の基本的概念を明らかにし, 各種の Fail-Safe 論理系を定義する。

次に, このような Fail-Safe 論理系研究の発端と目的, "0" ["1"] 形 Fail-Safe 論理系の構成を論ずる。(第2章)

第3章においては, "0" ["1"] 形 Fail-Safe 論理系を有する問題の解決策として筆者らが提唱する "Ⅱ" 形 Fail-Safe 論理系について, (Ⅰ) 多値論理(システム)に占める位置 (Ⅱ) 多値論理からみた諸性質等の検討を行う。

最後に新しい2重系, 交番論理系について考察する。(第4章)

1. 1. "Fail-Safe" の概念

一般に、システムの安全性は人的な要素を無視し得ないのであるが、ここでは当面の問題として純粹に工学的な立場から論ずることとする。このとき、"Fail-Safe" という概念はいつに定義されるであろうか。

"Fail", "Safe" のいずれにも概念の広がりも存在するから、統一的解釈を与えることは難しい。現実には "Fail-Safe" と称されているシステムを参考にして、広義 "Fail-Safe" を次のような概念を包含するものとして定義するのが妥当と思われる。

(i) 狭義信頼性 (Reliability)

部分システムの "Fail" が全システムの "Fail" (特に論理的、機能的障害、故障) とはならない。(能力の低下はしない。)

(ii) 狭義 Fail-Safe

ある部分システムの "Fail" が全システムの機能的障害、故障状態を招く。それらにのみ "安全側の許容障害、故障状態" と指定されるものに限られる。

(iii) Fail-Soft (Graceful Degradation)

部分システムの "Fail" によって全システムの能力(能率、効率)の低下となる。システム全体の機能的障害、故障とはならない。(機能的障害、故障も局部的。)

(N) Fool-Proof (Fail-Proof)

特に人間-機械システムにおいて、人間工学的な観点から、人間が操作する機械の取扱い誤りやレトリ、誤って取扱って危険を及ぼすようにする。

このように、広義“Fail-Safe”なる概念はさらに幾つかに細分されるが、それらけ互いに重なり合う場合も少なくない。本稿では狭義“Fail-Safe”について考察する。

1. 2 Fail-Safe 論理系

前節で述べた Fail-Safe の概念を論理システム（論理系）に適用するとき、狭義 Fail-Safe 論理系を次のように定義される。

Fail-Safe 論理系は、“その部分論理系に障害が生起するとき、予め指定された論理動作（安全側の故障状態に入る（例えげ、許容出力がゼロ、誤りとみなされ出力があるいは予め定められた安全側許容誤り出力を発生する）論理系”である。

このとき、予め指定される論理動作（安全側故障状態、安全側の許容誤り出力）の設定の仕方により各種の Fail-Safe 論理系を定義されるのである。以下の各章参照。

第2章 “0”[“1”] 形 Fail-Safe 論理系

2. 1 “0”[“1”] 形 Fail-Safe 論理系

論理系の Fail-Safe 性に際して対象とする故障を次のように限定しておく。論理系に生ずる障害(故障)は、その部分論理系 m 、

(I) 機能障害(誤り論理動作)と見るもの

(II) 機能障害(誤り論理動作)とみなすもの

に類別される m 、“論理”の立場から前章にについてのみ考察するものとする。更に、論理システムの構造を考慮し、特にその議論を簡単にすゝる為、以後、特に基本論理(回路)の stuck (固定)故障のみ取扱うものとする。

従つて、その部分論理系は“0”固定故障~~あり~~/+“1”固定故障の生じ~~る~~予想される2値(“0”、“1”)論理系では“0”[“1”] 形 Fail-Safe 論理系 m 以下の~~よう~~に定義される。

[定義 2. 1] 安全側の許容誤り出力は $1 \rightarrow 0$ 形(“0”形) [$0 \rightarrow 1$ 形(“1”形)] であるとする。その構成部品は“0”固定~~あり~~/+“1”固定故障~~を~~発生するとき、論理系 m 許容出力即ち、論理的に正しい出力あるいは“0”[“1”]形誤り(故障)出力を有するが、この論理系は“0”[“1”] 形 Fail-Safe (論理系) であるという。

換言すれば、与えられた論理関数 $f(X)$ を実現する論理系 S_f が "0" ("1") 形 Fail-Safe であるというのとは、

S_f は可能に全ての故障 E_i について

$$\text{条件 I. } 0 \subseteq F_{E_i}(X) \subseteq f(X)$$

$$(\text{条件 II. } 1 \supseteq F_{E_i}(X) \supseteq f(X))$$

と成ることを要する。但し、故障論理関数 $F_{E_i}(X)$ は故障 E_i が生起する際の論理系の出力論理関数である。

このように論理系で次のような結果が得られてゐる。

〔定理 2.1〕 論理関数 $f(X)$ を実行する非冗長論理系は同一桌上に "0" 固定故障と "1" 固定故障の両方が生起可能であるとき Fail-Safe とはなり得ない。

〔定理 2.2〕 所与の論理関数

$$f(X) = f(q_1(X), q_2(X), \dots, q_i(X), \dots)$$

を実行する論理系 S_f 中、その部分論理関数 $q_i(X)$ の " α " 固定故障 ($\alpha = 0$ or 1) と等価な故障 E_α をもつとき、この論理系中故障 E_α に対して "Fail-Safe" である場合には、 $f(X)$ は $q_i(X)$ によってunate であり得る。

"0" ("1") 形 Fail-Safe 論理系は、その構成を論ずるとき次のように分類するのが実用的である。

[定義 2.2] “0” (“1”) 形 Fail-Safe 論理系に於て、
 特定の入力誤り (故障) について条件 I (条件 II) が
 成立するとき、その論理系は “Strongly” “0” (“1”) 形 Fail-Safe で
 あるといい、それらの入力を “許容誤り入力” あるいは “
 “Fail-Safe 入力” と呼ぶ。この “許容誤り入力” (“Fail-Safe”
 入力”) をもつ論理系は “Weakly” “0” (“1”) 形 Fail-Safe 論理系
 と称される。

[定理 2.3] 基本論理回路は (i) Strongly (ii) Weakly
 “0” (“1”) 形 Fail-Safe であるための必要十分条件は、

その出力論理関数は (i)unate であり、(ii)unate でなく
 かつ、可能に出力故障は “0” (“1”) 固定故障である。

2.2. 交番則の適用による “0” (“1”) 形 Fail-Safe 論理系の 構成

[定義 2.3] “許容誤り出力割当に準ずる交番則”

“許容誤り出力割当に準ずる交番則” (“交番則”) は、与えられ
 た論理関数 $f(x)$ を実行する Strongly (Weakly) “ α ” 形 Fail-Safe
 論理系実現の為に、構成要素である各基本論理回路に許容
 される誤り出力の形 (type) を割当てる規則で、“各定論理を
 含む基本論理回路” に準じて α , $\bar{\alpha}$ は許容誤り出力状態を

交替的に割り当てられるものである。ここで“否定論理を含む基本論理回路”は、その出力論理関数 $f(X_i)$ が入力変数 X_i に関与して負であるものを意味する。 $\alpha = 0$ or 1

[定理 2.4] 与えられた論理関数 $f(X)$ を実行する論理系は (i) Strongly, (ii) Weakly “ α ” 形 Fail-Safe である α の必要十分条件は、

(i) 交番則により矛盾なく割り当てられた許容誤り出力 “ α_j ” を有する Strongly “ α_j ” 形 Fail-Safe 基本論理回路: $f_j(X)$ から構成される,

(ii) error-free 入力という仮定のもとで交番則を適用するとき矛盾なく割り当てられた許容誤り出力 “ α_k ” (“ α_l ”) を有する Weakly “ α_k ” 形 Fail-Safe 基本論理回路 $f_k(X)$ (または Strongly “ α_l ” 形 Fail-Safe 基本論理回路 $f_l(X)$) から構成される

ことである。 $\alpha, \alpha_j, \alpha_k, \alpha_l = 0$ or 1

尚、一般に Strongly Fail-Safe 論理系の場合、同一入力変数について複数個の基本回路から2種の許容誤り入力それぞれに要請されるとき、系は Pseudo-Strongly Fail-Safe であるということになる。(non-unate 論理関数は Pseudo-Strongly Fail-Safe あるいは Weakly Fail-Safe 論理系として実行される。)

第3章 “互”形 Fail-Safe 論理系

3.1 “互”形 Fail-Safe 論理系

前章で述べた “0” (“1”) 形 Fail-Safe 論理系は

(i) “0” (“1”) 形出力誤り許容される,

(ii) 部分論理系は “0” 固定故障/または “1” 固定故障の生起可能,

という前提に立つものであるから次の問題を含んでいる。

問題1. “0” (“1”) 形 Fail-Safe 論理系に於いてはその出力 “0” (“1”) の正誤を決定不能。そのため、故障検査が困難。

問題2. 任意の論理回路を “0” (“1”) 形 Fail-Safe 論理系として実現しようとするとき、実現する物理系で理想的なものとしてみえらるゝと困難な場合もある。

問題3. 論理系に生ずる障害で “0” 固定故障/または “1” 固定故障を特定し得ないことがある。

問題4. システムは誤せられず目的に達するためには論理動作の判定が未定または中止となり、誤り状態であることと証明可能”は許容されるが、誤って “0”, “1” の出力を発生すること許されない場合を考慮される。

以上の点を考慮して筆者は、障害発生時の出力誤り “0”, “1” に等しくなる “互” 形故障論理系, “互” 形誤り出力を許容誤り出力とする “互” 形 Fail-Safe 論理系を提唱した。

[定義 3.1] 正常動作時の論理系の“0”状態(出力, 真理値)と“1”状態(出力, 真理値)と disjoint である状態(出力, 真理値); “ $\square$ ”に固定するものや“ $\square$ ”形故障(“ $\square$ ”固定故障)という。正常動作状態(出力, 真理値)集合 $\Sigma = \{“0”, “1”\}$ で表わすとき,

$$\Sigma \cap \square = \emptyset \text{ (空)}$$

である。

ある2値(“0”, “1”)論理系 $f(X) = f(X_1, X_2, \dots, X_n)$ の構成要素に生起可能な故障(誤り)は“ $\square$ ”形故障のみであるとき, 系は“ $\square$ ”形故障(基本)論理系であるといわれ, 以下のよう定義化される。

I. 正常動作状態

$$f({}^{(k)}X_{i_1}, {}^{(k)}X_{i_2}, \dots, {}^{(k)}X_{i_r}, {}^{(l)}X_{j_1}, {}^{(l)}X_{j_2}, \dots, {}^{(l)}X_{j_s})$$

$$(f({}^{(k)}X_{(i,r)}, {}^{(l)}X_{(j,s)})) \text{ と略記する}$$

$$\triangleq \{\Sigma\} = \{“0”, “1”\}$$

$$\text{但し, } X_{(i,r)} \cup X_{(j,s)} = X, X_{(i,r)} \cap X_{(j,s)} = \emptyset \text{ (空)}$$

かつ r -組 $(X_{i_1}, X_{i_2}, \dots, X_{i_r})$, $(X_{i_k} = 0 \text{ or } 1)$ の k 番目の組合わせ, s -組 $(X_{j_1}, X_{j_2}, \dots, X_{j_s})$, $(X_{j_l} = 0 \text{ or } 1)$ の l 番目の組合わせを表現する。

II. 故障動作状態

(i) “ $\square$ ”形入力故障の場合 変数 X_i は“ $\square$ ”状態に固

定する故障 $\{ \text{⑤} \} X_i$ とすれば、一般に “⑤” 形入力故障は

$$f \{ {}^{(k)}X_{i_1}, {}^{(k)}X_{i_2}, \dots, {}^{(k)}X_{i_r}, {}^{(\text{⑤})}X_{j_1}, {}^{(\text{⑤})}X_{j_2}, \dots, {}^{(\text{⑤})}X_{j_s} \}$$

$$(f \{ {}^{(k)}X_{(i,r)}, {}^{(\text{⑤})}X_{(j,s)} \}) \text{ と略記}$$

と表わされる。

(a) “⑤” 形入力故障に対応する、ある i, i' について

$$f \{ {}^{(k)}X_{(i,r)}, {}^{(k)}X_{(j',s)} \} \neq f \{ {}^{(k)}X_{(i,r)}, {}^{(k)}X_{(j,s)} \}$$

$$\text{であるとき, } f \{ {}^{(k)}X_{(i,r)}, {}^{(\text{⑤})}X_{(j,s)} \} \equiv \{ \text{⑤} \}$$

(b) “⑤” 形入力故障に対応する、全ての i, i' について

$$f \{ {}^{(k)}X_{(i,r)}, {}^{(k)}X_{(j',s)} \} = f \{ {}^{(k)}X_{(i,r)}, {}^{(k)}X_{(j,s)} \}$$

$$\text{であるとき, } f \{ {}^{(k)}X_{(i,r)}, {}^{(\text{⑤})}X_{(j,s)} \} \equiv \{ \text{㊥} \} \text{ or } \{ \text{⑤} \}$$

(㊥/⑤ で表す)

(ii) “⑤” 形出力故障の場合 論理系自体の出力故障は入

力とは無関係に “⑤” 形誤り出力となる。

$$\{ \text{⑤} \} f \{ {}^{(k)}X_{(i,r)}, {}^{(k)}X_{(j',s)} \} = \{ \text{⑤} \} f \{ {}^{(k)}X_{(i,r)}, {}^{(\text{⑤})}X_{(j,s)} \}$$

$$\equiv \{ \text{⑤} \}$$

この定義において、条件 II. (i), (b) における任意性 π 論理系
の情報曖昧さの程度を規定する。例えば、ここで

$$f \{ {}^{(k)}X_{(i,r)}, {}^{(\text{⑤})}X_{(j,s)} \} \equiv \text{㊥} \{ \text{⑤} \}$$

とすれば、系 π の情報曖昧さは最小 [最大] となる。(このとき、

“㊥” (“㊥”) 形故障論理系という。)

従って、一般の“重”形故障論理系は、それらの論理系を両極限として定義されるのである。

〔定義 3. 2〕 安全側にある許容誤り出力を“重”形（ $0 \rightarrow$ “重”形 かつ/または $1 \rightarrow$ “重”形）であるとする。このとき、ある論理系に生起する、いかなる障害に対しても安全側の許容出力をとるならば、即ち、可能に誤り出力を“重”形誤り出力に限られるならば、系は“重”形 Fail-Safe 論理系であるという。

（尚、最小〔最大〕情報意味を有する“重”形 Fail-Safe 論理系は“重_m”〔“重_M”〕形 Fail-Safe であるという。）

このとき、『“重”形故障（基本）論理系を構成要素とする論理系は、“重”形 Fail-Safe 論理系である。』但し、論理系への入力は論理的に誤りにならない、あるいは“重”形誤り（故障）に限定されるものとする。

3. 2 3レベル（0, ϕ , 1）“重”形 Fail-Safe 論理系
前項で“重”形故障論理系の構造と“重”形 Fail-Safe 論理系の存在可能性について述べてきたが、以下の節では実際の物理系との対応を考慮しながら具体的に検討を行う。特に、3レベル：0, ϕ , 1 をもつ（Single Rail）論理系と Double

Rail 論理系について考察する。(ここで、 ϕ は故障状態(出力, 真理値)を表わすものとする。)

A. “ Φ ”形故障 (“ Φ ”形 Fail-Safe) 基本論理回路

3レベル: 0, ϕ または 1 をもち, 2 値 (“0”, “1”) 論理系に以下の “ Φ ”形故障 (Fail-Safe) 基本論理回路により構成される。但し, 正常状態(真理値): $\Psi \triangleq \{0, 1\}$

$$\text{故障状態(真理値)}: \Phi \triangleq \{\phi\}$$

ここで 2 変数論理関数の場合について述べた n 変数論理関数回路への拡張も同様に与えられる。

1) “ Φ ” (“ ϕ ”) 形故障 (Fail-Safe) 論理和回路: $\phi \vee$

2 変数 “ ϕ ” 形故障 (Fail-Safe) 論理和回路: $\phi \vee$ は,

図 3. 1. (a) に示す真理値表により規定されるものである。

表中の $1/\phi$ は対応の出力を “1” とする “ ϕ ” である: ϕ を意味するもので、(但し, $1/\phi$ は、一般には、それ n 占める座標の座標である), そのいずれをとる n 論理系の情報意味を規定する。すぐわかるように、表中の全ての $1/\phi$ について

$$1/\phi \triangleq 1[\phi] \text{ とするとき, 最小[最大]情報意味の論理系 } \phi_m \vee [\phi_u \vee]$$

となる。

“ ϕ ” 形故障 (誤り) 入力に対応する, 論理回路: $\phi \vee$ の出力の中で “ ϕ ” は誤りである n , “1” は論理的に正しい出力

力である。

以上、基本論理回路の故障状態として入力の“重”(“ ϕ ”)形故障のみ扱っているが、これは次の仮定に基づいている。

仮定 1. 部分論理系の出力故障は“重”形故障に限られる。

仮定 2. ある部分論理系の“重”形出力故障は次の部分論理系への入力“重”形故障(誤り)と等価である。

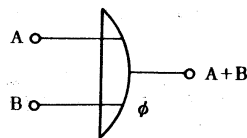
これらの仮定は後述の論理回路についても成立するものである。

2) “重”(“ ϕ ”)形故障(Fail-Safe)論理棒回路: $\phi \wedge$

$\phi \wedge$ は $\phi \vee$ と双対的な性質をもつ。図 3. 1. (b) 参照。

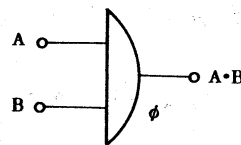
3) “重”(“ ϕ ”)形故障(Fail-Safe)論理否定回路: ϕN

図 3. 1. (c) の真理値表により規定される。



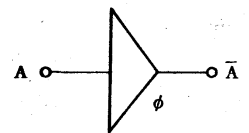
B \ A	0	ϕ	1
0	0	ϕ	1
ϕ	ϕ	ϕ	$1/\phi$
1	1	$1/\phi$	1

(a) $\phi \vee$



B \ A	0	ϕ	1
0	0	$0/\phi$	0
ϕ	$0/\phi$	ϕ	ϕ
1	0	ϕ	1

(b) $\phi \wedge$



A	$\bar{A}$
0	1
ϕ	ϕ
1	0

(c) ϕN

図 3. 1. “重”(“ ϕ ”)形 Fail-Safe 基本論理回路

β. 基本論理回路: $\phi_V, \phi_\wedge, \phi_N$ により 3レベル “重” 形 Fail-Safe 論理系の構成

『任意に与えられた論理関数 $f(X)$ は, Δ で定義した基本論理回路: $\phi_V, \phi_\wedge, \phi_N$ により “重” 形 Fail-Safe 論理系として実現される。』

3. 3. 多値論理からみた “重” 形 Fail-Safe 論理系の構成

Δ. 多値論理に占める “重” 形 Fail-Safe 論理系の位置

従来の多値論理研究において主として完全性について論じられてゐる。このため “重” 形 Fail-Safe 論理系も一種の多値論理系であるから,

(i) M 値 ($M = |\{\text{真}\}| + |\{\text{重}\}|$) 論理と 2 値 ($2 = |\{\text{真}\}|$)

論理に縮退して用い, 残りの真理値には實際の意味のある論理値として使われる情報以外の情報, 即ち “重” 形故障発生という情報を与える,

(ii) M 値論理として完全でないう M 2 値論理として完全である

ことを活用してゐる点に特徴がある。

このように, 一般に完全でないう M 値論理 (系) を完全とする N 値論理 (系) に縮退させて用いることにより付加的な情報を加へることもでき, 逆に N 値論理 (系) を M 値論理 (系) に拡張

張する ことにより、その構造を見やすくすることと期待されるから、このように多値論理の見方は重要と思われる。

B. Kleene の 3 値論理と " ϕ_m " 形 Fail-Safe 論理系

S. C. Kleene が提唱した 3 値論理システムは、 χ の one-to-one 対応を考えると、" Φ " 形 (" ϕ_m " 形) Fail-Safe 論理系の構造を調べるのに適していることとなる。

	" ϕ_m " 形 Fail-Safe 論理系	Kleene 論理
真理値	$\Psi = \{0, 1\}$	I, II
	$\Phi = \{\phi\}$	III
順序付け	$0 < \phi < 1$	I < II < III
基本演算	$\phi_m \vee (X, Y)$	加法 + : $X + Y = \text{Max}(X, Y)$
	$\phi_m \wedge (X, Y)$	乗法 $\cdot$: $X \cdot Y = \text{Min}(X, Y)$
	$\phi_m N(X)$	否定 - : $\bar{X} = \text{IV} - X$

定義域 $L_1 = \{I, II, III\}$ で定義される 3 値 Kleene 論理系の基本演算 (論理) : $+$, $\cdot$, $-$ を定数または変数 ($X_1, X_2, \dots, X_n$) に繰り返し適用することにより得られる論理関数, 3 値 Kleene 論理関数を $f_K(X)$ で表わすこととなる。この 3 値 Kleene 論理関数 $f_K(X)$ は定義域を $L_2 = \{I, II\}$ に制限すれば, 2 値 (I, II) Boole 論理関数 $f_B(X)$ を生成する。換言すれば, 上述の対応を考えると, " ϕ_m " 形 Fail-Safe

基本論理回路からなる論理系の論理動作は、入力“重” (“ ϕ ”) 形故障 (誤り) を含めて 3 値 Kleene 論理により記述されるのである。

Kleene 論理の基本的性質

冪等律, 交換律, 結合律, 吸収律, 分配律, 一重否定および de Morgan の法則; $\overline{X + Y} = \overline{X} \cdot \overline{Y}$
 $\overline{X \cdot Y} = \overline{X} + \overline{Y}$

の成立するものは 2 値の Boole 代数と同様である。但し、次の性質に注意せよ。

$$(i) \quad X \cdot Y + X \cdot \overline{Y} \subseteq X$$

$$(X + Y) \cdot (X + \overline{Y}) \supseteq X$$

$$(ii) \quad q_{k1} = X_i^\alpha \cdot X_j^\beta \cdot X_k^\gamma, \quad q_{k2} = X_i^\alpha \cdot X_j^\beta \cdot X_k^\gamma$$

$$q_{k3} = X_i^\alpha \cdot X_j^\beta \cdot X_k^\gamma, \quad q_{k4} = X_i^\alpha \cdot X_j^\beta \cdot X_k^\gamma$$

$$\begin{aligned} \text{ゆえ} \quad \sum_{i=1}^4 q_{ki} &\subseteq X_j^\beta \cdot X_k^\gamma + X_i^\alpha \cdot X_k^\gamma \\ &\subseteq X_j^\beta \cdot X_k^\gamma + X_i^\alpha \cdot X_k^\gamma + X_j^\alpha \cdot X_j^\beta \\ &(\triangleq f_k^*(X_i, X_j, X_k)) \end{aligned}$$

$$\text{但し, } \alpha, \beta, \gamma = 0 \text{ or } 1, \quad X^0(X^1) = \overline{X} \quad (X)$$

$$X_i, X_j, X_k = \{I, III\} \text{ に対し, } \sum_{i=1}^4 q_{ki} = f_k^*(X_i, X_j, X_k)$$

$$\sum_{i=1}^4 q_{ki} = I \text{ に対し, } f_k^*(X_i, X_j, X_k) = I$$

構形式で述べた性質 (ii) に対する結果も構形式について得られる。

このように 3 値 Kleene 論理の性質を活用することにより、
 “ Φ ” (“ ϕ ”) 形 Fail-Safe 論理系 (ある意味で) 最適な構成法
 が得られる。(C. 参照)

C. “ ϕ_m ” 形 Fail-Safe 論理系の最適構成法

与えられた論理関数 $f(X)$ を前章の “ ϕ_m ” 形 Fail-Safe 基本
 論理回路: $\phi_m V$, $\phi_m \wedge$, $\phi_m N$ にとり実現する際、論理系の入
 力 “ ϕ ” 形故障 (誤り) に対して最小情報意味をもつ構成
 がある。(この手法は M. Yoeli, E. B. Eichelberger による hazard
 free network 構成法と全く同様に考えられるものであるから
 詳細は省略する。)

“全ての主項の和で表わされ α 2 値論理関数 $f_B^*(X)$ の α
 2 値論理: 論理和 (OR), 論理積 (AND), 論理否定 (NOT)
 をそれぞれ $\phi_m V$, $\phi_m \wedge$, $\phi_m N$ で実現する論理系は
 “ Φ_m ” (“ ϕ_m ”) 形 Fail-Safe である。”

一般に, “ ϕ_m ” 形 Fail-Safe 基本論理回路: $\phi_m V$, $\phi_m \wedge$,
 $\phi_m N$ により f なる論理系は, “ ϕ_m ” 形 Fail-Safe 性によって保
 てらる。従って, 上に提案された構成法はその点から尤も

味深い。

D. " ϕ_m " 形 Fail-Safe 論理系の 実値論理実現

" ϕ_m " 形 Fail-Safe 論理系の論理動作を記述する 3 値 (0, ϕ , 1) 論理関数の導出を行う。その実値実現を試みる。
このように一般 3 値論理関数には、単一実値素子で実現される範囲に限られており、多実値素子構成の論議も容易で無い。
そこで、任意の論理関数を冗長入力の単入に作り対称化する。このことのできる事実を利用すること等により、対称論理関数として実現する方法を考えられる。

3. 4. "五" 形 Fail-Safe Double Rail 論理系

前述のように、3 レベル (0, ϕ , 1) "五" (" ϕ ") 形 Fail-Safe 論理系の構成は、基本論理回路: ϕ_V , $\phi_\wedge$, ϕ_N の存在という仮定に立つのであるが、 ϕ_N の物理的実現は不能 (困難) な場合も予想される。

筆者らが提唱した "Double Rail" 論理系の概念は、この難点を避けることのできる点で、故障検出などにおいて多くの利点を有していることも示される。

Double Rail 論理系は J. Von Neumann の "Double Line Trick" を応用したもので、2 つの信号線 (線路) によりなる。この論

理系は、論理変数 X_i へ $m(X_i, \gamma_i)$ のように対の信号 (符号)
) : 大文字 X_i と小文字 γ_i の組み合わせで表す。

真理値 “0” と 符号 (0, 1)

真理値 “1” と 符号 (1, 0)

なる対応のもとで所定の論理 (率数) を実行するものである。

残りの 2-tuple は故障 (誤り) を表す。

3 レベル (0, ϕ , 1) を有する Double Rail 2値 “0”

(0, 1), “1” (1, 0) } 論理系として、図. 3. 2 に示

する基本論理回路:

“ ϕ ” 形 Fail-Safe Double Rail 論理和回路: ϕV_d

“ ϕ ” 形 Fail-Safe Double Rail 論理積回路: $\phi \wedge_d$

“ ϕ ” 形 Fail-Safe Double Rail 論理否定回路: ϕN_d

からなるものを考える。

これらの基本論理回路は、

$\Pi \triangleq \{ \text{“0”} (0, 1), \text{“1”} (1, 0) \}$

$\Phi \triangleq \{ (0, \phi), (\phi, 0), (\phi, \phi) \}$

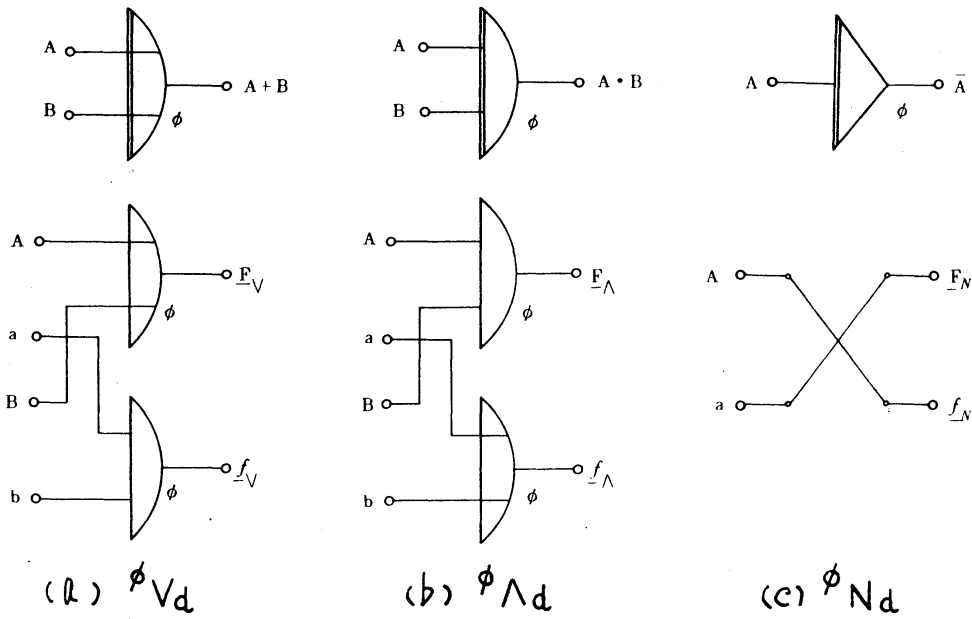
$(\phi, 1), (1, \phi) \}$

とするとき, “ Φ ” 形故障論理系 “ Φ ” 形 Fail-Safe 論理

系であることがわかる。

表. 3. 1. $\phi V_d, \phi N_d$ の真理値表

表. 3. 2. $\phi V_d, \phi N_d$ の誤り出力表



☒ 3. 2 $\phi V_d, \phi \Lambda_d, \phi N_d$ の構成

表 3. 1 $\phi V_d, \phi N_d$ の真値表

(a) ϕV_d

A	B		0				1				
	Aa	Bb	0 0	0 ϕ	0 1	ϕ 0	$\phi \phi$	ϕ 1	1 0	1 ϕ	1 1
0	0 0	0 0	0 $\frac{0}{\phi}$	0 0	ϕ 0	$\phi \frac{0}{\phi}$	ϕ 0	1 0	1 $\frac{0}{\phi}$	1 0	
	0 ϕ	0 $\frac{0}{\phi}$	0 ϕ	0 ϕ	$\phi \frac{0}{\phi}$	$\phi \phi$	$\phi \phi$	1 $\frac{0}{\phi}$	1 ϕ	1 ϕ	
	0 1	0 0	0 ϕ	0 1	ϕ 0	ϕ 0	ϕ 1	1 0	1 ϕ	1 1	
	ϕ 0	ϕ 0	$\phi \frac{0}{\phi}$	ϕ 0	ϕ 0	$\phi \frac{0}{\phi}$	ϕ 0	$\frac{1}{\phi}$ 0	$\frac{1}{\phi}$ $\frac{0}{\phi}$	$\frac{1}{\phi}$ 0	
	ϕ 0	$\phi \frac{0}{\phi}$	$\phi \phi$	$\phi \phi$	$\phi \frac{0}{\phi}$	$\phi \phi$	$\phi \phi$	$\frac{1}{\phi}$ $\frac{0}{\phi}$	$\frac{1}{\phi}$ ϕ	$\frac{1}{\phi}$ ϕ	
	ϕ 1	ϕ 0	$\phi \phi$	ϕ 1	ϕ 0	$\phi \phi$	ϕ 1	$\frac{1}{\phi}$ 0	$\frac{1}{\phi}$ ϕ	$\frac{1}{\phi}$ 1	
	1 0	1 0	1 $\frac{0}{\phi}$	1 0	$\frac{1}{\phi}$ 0	$\frac{1}{\phi}$ $\frac{0}{\phi}$	$\frac{1}{\phi}$ 0	1 0	1 $\frac{0}{\phi}$	1 0	
1	1 ϕ	1 $\frac{0}{\phi}$	1 ϕ	1 ϕ	$\frac{1}{\phi}$ $\frac{0}{\phi}$	$\frac{1}{\phi}$ ϕ	$\frac{1}{\phi}$ ϕ	1 $\frac{0}{\phi}$	1 ϕ	1 ϕ	
	1 1	1 0	1 ϕ	1 1	$\frac{1}{\phi}$ 0	$\frac{1}{\phi}$ ϕ	$\frac{1}{\phi}$ 1	1 0	1 ϕ	1 1	

(b) ϕN_d

A	Aa	$\bar{A}a$
0	0 0	0 0
	0 ϕ	ϕ 0
	0 1	1 0
	ϕ 0	0 ϕ
	$\phi \phi$	$\phi \phi$
1	ϕ 1	1 ϕ
	1 0	0 1
	1 ϕ	ϕ 1
	1 1	1 1

表 3.2 誤り出力表

(a) ϕV_d

" ϕ " failure input	Output
$(0\phi)^d (00)^d (\phi\phi)$	$(0\phi)^d (00)^d (\phi\phi)$
$(\phi 1)^d (1\phi)^d$	$(\phi 1)^d (1\phi)^d (10)^{\odot}$
$(00)^* (11)^*$	

(b) ϕN_d

" ϕ " failure input	Output
$(0\phi)^d (00)^d (\phi\phi)$	$(0\phi)^d (00)^d (\phi\phi)$
$(\phi 1)^d (1\phi)^d$	$(\phi 1)^d (1\phi)^d$
$(00)^* (11)^*$	

3. 5. " Φ_0 " (" Φ_1 ") 形 Fail-Safe Double Rail 論理系基本論理回路: ϕV , $\phi \wedge$ からなる " Φ " 形 Fail-SafeDouble Rail 論理系の概念は第2章で述べた " 0 " (" 1 ") 形Fail-Safe 基本論理回路: $0V$, $0\wedge$ [$1V$, $1\wedge$] により構

成される Double Rail 論理系に拡張される。

論理回路: ϕV から $\phi \wedge$ をそれぞれ論理回路: $0V$ から $0\wedge$ [$1V$ から $1\wedge$] で置換えることにより実現される Double Rail 論理和回路, 論理積回路を ϕV_d , $\phi \wedge_d$ [ϕV_d , $\phi \wedge_d$] で表す。論理回路: ϕN_d [ϕN_d] は ϕN_d と全く同じもの, 即ち, 2つの信号線を単純に交叉させたものとする。

よって,

$$\Phi = \{ "0" (0, 1), "1" (1, 0) \}$$

$$\Phi_0 = \{ (0, 0) \}$$

$$\Phi = \{ "0" (0, 1), "1" (1, 0) \}$$

$$\{ \Phi = \{ (1, 1) \} \}$$

であるとする。このような論理回路: $\phi_0 V_d, \phi_0 \wedge_d, \phi_0 N_d$
 $\{ \phi_1 V_d, \phi_1 \wedge_d, \phi_1 N_d \}$ は "Φ" 形故障, Fail-Safe 論理系
 である。

従って, これらの基本論理回路を用いて, 任意の論理関数 $f(X)$ は "Φ₀" ["Φ₁"] 形 Fail-Safe Double Rail 論理系として実現される。

第4章 交番論理系

最後に、Double Rail 論理系（第3章）において空宙に置いて冗長性を時空領域に拡張して“交番論理系”について簡単に述べる。

論理系の高信頼度化のため冗長性を導入する多重化（2重化）法は古くから知られている技法であるが、実用的効果として

(i) 部分論理系の故障はシステム・ダウンとされず、所定の使命が遂行される

(ii) 故障検査（検出、診断）容易な機構（構造）を与えることが考えられる。従来、主として前者の観点から論議が行われてきたが、後者は2次的なものとも行われてきた。また、論理系の処理速度より安全性を重要視され、第2の特長を適用する多次2重化を積極的に採用するところも望まれても、それに伴う費用の増大がもたらがれがいたことも少なかった。

従って、ハードウェアの増加をできる限り小さくし、（少なくとも単純な2重化系より低costで）、2重化論理系の特徴を活かすという要請を生じてくる。この要請に応えるものとして次のように“交番論理系”を提唱される。

4. 1 交番論理系

交番論理系は, 1つの論理変数 (真理値) を2つの交番的 (相補的) 情報の時空的系列からなる 2-tuple で表現し, かつ, 通常の論理系と同様, 所与の論理動作を行うものである。

本稿では, 真理値 "0" $\longleftrightarrow$ 交番情報 (0, 1)

真理値 "1" $\longleftrightarrow$ 交番情報 (1, 0)

変数 X $\longleftrightarrow$ 交番情報 $(X, \bar{X})$

なる対応付けを考える。

一般に論理変数 $f(X)$ を実行する交番論理系は, 入力変数 X に対応する交番入力 (変数), $(X, \bar{X})$ を印加するとき, $f(X)$ に対応する交番出力 $f_f \equiv (f_f^A(X), f_f^B(\bar{X}))$;

$$(i) f_f^A(X) = \overline{f_f^B(\bar{X})}$$

$$(ii) f(X) = \alpha \Rightarrow (f_f^A(X), f_f^B(\bar{X})) = (\alpha, \bar{\alpha})$$

とすることも考えられるが,

$$f_f^A(X) = f(X), \quad f_f^B(\bar{X}) = f^D(\bar{X})$$

とするのが最も自然であろう。

時 q の非交番的信息からなる 2-tuple は,

$$\bar{\Omega} \equiv \{ "0" (0, 1), "1" (1, 0) \}$$

と disjoint な " Ω " 形故障 (誤 q) を表示する。

$$\Omega \equiv \{ (0, 0), (1, 1) \}$$

4. 2 交番論理系の構成

△. 基本交番論理系に於ける構成

(i) 交番論理和回路 $V_{\oplus} = (V, \wedge)$

$$\text{論理和数} : f_V(X_1, X_2) = X_1 + X_2$$

$$\text{交番出力数} : f_V^A(X_1, X_2) = X_1 + X_2$$

$$f_V^B(\bar{X}_1, \bar{X}_2) = \bar{X}_1 \cdot \bar{X}_2$$

(ii) 交番論理積回路 $\wedge_{\oplus} = (\wedge, V)$ (iii) 交番論理否定回路 $N_{\oplus} = (N, N)$ or 信号交換作って、基本交番論理回路: $V_{\oplus}[\wedge_{\oplus}]$ かつ $V \times \wedge[\wedge \times V]$

の機能は交番的に進行するものといえる。可変真値真値論理系の真値を適当に選定するといふより実現される。

自己反対論理数である論理否定の場合には、通常の否定回路に交番入力 $(X, \bar{X})$ を印加すると交番論理系を実現される。すなわち、交番論理否定は2つの交番的(相補的)信号を時直的に入れ換えるものと考えられるから、その手段を許される物理系を用いるならば簡単に構成となる。

このとき、与えられた論理数 $f(X)$ の交番論理系 $f(X)$ を実行する通常の論理和、論理積、論理否定回路からなる論理系に於いて各論理回路を交番論理回路で置換えるといふより構成される。

基本交番論理回路の故障検出:

基本交番論理回路に於ける2種類の故障;

(i) 真理値固定故障 ----- 交番論理回路の出力 Y 入力 X と

無関係に $(0, 0)$ または $(1, 1)$ に固定する。

(ii) 機能固定故障 ----- 交番論理回路, $V_{\oplus}$, $\wedge_{\oplus}$ において

その機能を論理和, 論理積の一方に固定する。

を予想される。

一般に, 交番論理系の故障検査は出力端に於ける誤り信号

$(0, 0)$ または $(1, 1)$ の検出 (“重”形故障検査) に

よってのみ行うものとすれば,

“基本交番論理回路; $V_{\oplus}$, $\wedge_{\oplus}$, $N_{\oplus}$ で構成される任意の

交番論理系において, 一つの基本論理回路が故障するとき,

系の出力は論理的に正しい交番出力または“重”形故障検査

可能の出力である。”

3. 自己双対論理率族と交番論理系

所与の論理率族 $f(X)$ が自己双対であるとき, その $f(X)$

を実現する通常の論理系に交番入力 $(X, \bar{X})$ を印加する。

とにより所望の交番出力 f_f が得られる。

よって, n 変数自己双対論理率族は完全系をなす得る。

から, “任意の n 変数論理率族は高々1個の冗長入力により自

己双対化可能”であることが利用される。(この構成では

単なる 2 重系構成に 1, 2, 3, 4 の基本論理回路で実現される論理関数の例を得られる。))

“所与の自己双対論理関数 $f(x)$ を実行する交番論理系：
 $f_f(x, \bar{x}) = (f_f^A(x), f_f^B(\bar{x})) = (f(x), \bar{f}(\bar{x}))$
 において故障の生起する部位 (gate) の部分論理関数を $g(x)$ とする。このとき、 $f(x)$ が $g(x)$ について正相関系であるならば、 $g(x)$ の “0” 相関 “1” への固定と等価な故障による出力誤りは (α, α) に限られる。” ($\alpha = 0$ or 1)

4. 3. 交番論理系の Fail-Safe 性

空間的 2 重論理系である Double Rail 論理系で考察されるものとアナログカルに

$$\Psi = \{ "0" (0, 1), "1" (1, 0) \}$$

$$\Phi_\alpha = \{ (\alpha, \alpha) \} \quad \alpha = 0 \text{ and/or } 1$$

とする。ことにより “ Φ_α ” 形 Fail-Safe 交番論理系を定義するのが妥当と思われる。即ち、“ある交番論理系に生起する全ての障害に対して可能な誤り出力 $\{(\alpha, \alpha)\}$ に限られるとき、系は “ Φ_α ” 形 Fail-Safe 交番論理系である” という。これは前節の “ Φ_α ” 形故障検出可能性と同値であるから、基本交番論理回路は 2 値的 (双方向, 対称) 故障を予想されるとき、その交番論理系の出力成分関数 f_f^A と f_f^B のいずれか

が error-free である限りにおいて " Φ_α " 形 Fail-Safe 性を保
存されるのである。

このように " Φ_α " 形 Fail-Safe 性をとり確保するのもとする
ために、一方回 (非対称) 誤り基本論理回路の存在を仮定す
る場合についても、前述の結果から容易に推察されよう。

以上、筆者らが行ってきた Fail-Safe 論理系構成に関する
研究をまとめ、多値論理の応用例として興味深い性質を含
まれていることについて述べてきた。

最後に同席から御指導いただき、本学の早山博教授に米、感
謝する。Fail-Safe 論理系に準じて終始適切な御助言をい
ただく国際電気研究所後援昭治博士に米謝する。また、交番論
理系について、その多くが国際電気研究所山本英雄氏にお
っていることを付記し、同席に感謝の意を表します。

文 献

- [1] 渡辺, 高橋: "フェイルセーフ形論理系の構成法"
信学全 72 (1965-11)
- [2] 渡辺, 浦野: "パラメトリック準 Fail-Safe 論理系"
信学電算研 50 (1966-12)
- [3] 渡辺, 浦野: "Fail-Safe 論理系" 信学誌 50
2 p.p. 290-291 (1967-02)
- [4] 浦野, 平山, 渡辺: "φ型 Fail Safe 論理系" 信学
オートマトン研 A 67-41 (1967-11)
- [5] 平山, 渡辺, 浦野: "Fail-Safe 論理系の構成理論"
信学論誌 52-C 1 p.p. 33-40 (1969-01)
- [6] 浦野, 平山: "互型 Fail-Safe 論理系の構成" 信学
電算研 EC 68-34 (1969-01)
- [7] 向殿, 土屋, 駒宮: "C形フェイルセーフ論理回路
の数学的構造について" (1), (2) 信学電算研
EC 67-30 (1968-02), EC 68-6 (1968-05)
- [8] 橋本, 都倉, 嵩: "非対称誤り素子によるフェイル
セーフ論理回路と2重化論理" 信学誌 50 4
p.p. 680-687 (1967-04)
- [9] Mine, Koga: "Basic Properties and a Construction
Method for Fail-Safe Logical Systems"

I.E.E.E. Trans. on EC EC-16 3 pp.282-289

(1967-06)

- [10] 三根, 高田: "非対称故障論理回路を用いた多重の一構成法" 信学十-トマトノ研彙 (1967-09)
- [11] 中道: "フェイルセーフ論理回路とその無接点継電器系への応用" 制御工学 13 2 (1969-02)
- [12] 山本, 渡辺, 津野: "交番論理系とその故障検出への応用": 信学電算研彙 EC 69-15 (1967-07)