解　説

# コンピュータを用いたフェイルセイフなシステム†

奥　村　幾　正††

## 1. まえがき

近年，コンピュータシステムの進展は目覚しく，現代社会の種々な分野に適用されている．特に交通，原子炉の制御など，装置の故障が直接人命にかかわるシステムでは単に高信頼化ばかりでなく，安全性の観点からも十分満足するシステムが要求される．

一方安全性の面では，鉄道信号の分野で古くから芽生えてきた「装置が故障した場合，安全側に動作する」いわゆる「フェイルセイフ」(fail safe) の概念が見直され[1]，コンピュータを用いたフェイルセイフなシステムの開発が叫ばれている．本文では最初にこれらフェイルセイフの考え方を明らかにし，次に主として鉄道信号システムに適用すべく開発中のコンピュータを用いた種々のフェイルセイフなシステム構成法を紹介し，今後の展望をなす．

## 2. フェイルセイフなシステムの構成例

### 2.1 広義のフェイルセイフ

システムとか機器がどこか具合が悪くなっても，安全側に動作するというフェイルセイフなシステムの構成法は安全性設計上，最も本質的な考え方とされ，安全性を要する多くの分野で使用されている．しかし，各適用分野ごとにシステムの使命が異なるところから，それに応じて「安全側の状態」がそれぞれ異なり，同一の「フェイルセイフ」と呼ばれる技術も多様化し，種々な解釈がなされ，広い意味を有している．これらを広義のフェイルセイフと呼び，最初にこれら広義のフェイルセイフの構成とその特徴を紹介する．

#### 2.1.1 原子炉のフェイルセイフ

原子炉は安全確保のため，緊急事態が発生した場合，核反応を減少させ，炉を停止させることが至上命令となっている．そのため，原子炉の制御を司る制御棒の駆動にフェイルセイフ設計がなされている．すなわち，制御棒の駆動は炉心から重力に逆らって引き抜く時は反応度は増加し，重力に応じて炉心に挿入する時は減少，炉停止の方向である．したがって緊急炉停止の場合は重力によって制御棒は落下し，炉は確実に停止する．また電源喪失事故に対しても制御棒を接着している電磁石の励磁が切れて，制御棒が落下するよう構成されている[2]．

このように原子炉の制御棒の駆動方式は装置の故障時に安全側に確実に停止するよう構成されており，この手法は後述する鉄道信号の構成例と同一な概念と考えられ，いわゆる狭義のフェイルセイフ（後述する）の典型的な構成例といえる．

#### 2.1.2 航空機のフェイルセイフ

旅客輸送用航空機の機体構造設計に際し，使われているフェイルセイフとは「構造物のなかの一部分の主要構造要素が疲労により破壊した時，そのままの状態で飛行を続けても，機体全体としては飛行特性が害われないように致命的な全体破壊や変形をしないように構造を設計すること」をいう[3]．

フェイルセイフを考察するとき，何が安全側であるかは対象によって異なってくる．航空機の例は前述の原子炉や後述する鉄道信号の場合とまったく逆に現れる．すなわち，航空機の安全側は「飛行を継続すること」と考えられるので，故障が発生しても機能を停止させることができず，「機能維持」を図ることが安全側となる．よってその技術・手法は多重化の概念を基礎として構成される．

#### 2.1.3 エレベータのフェイルセイフ

超高層ビルなどに使われている高速エレベータでは，安全な昇降速度を超えたとき，緊急に停止するための安全装置を有している．しかし，この安全装置は非常時の最後の手段であるため，「通常の制御回路の故障により速度が速くなったとき，速度を落すためのバックアップ回路を設けること」が義務づけられており，これをフェイルセイフと呼んでいる[4]．

---

† Fail-safe System Using Computers by Ikumasa OKUMURA (Railway Technical Research Institute, J. N. R.).

†† 日本国有鉄道鉄道技術研究所信号研究室

**2.1.4　道路交通管制システムのフェイルセイフ**

広域の道路交通信号を計算機制御するシステムではまた別の意味にフェイルセイフが使われている．このシステムは複数のコンピュータが階層構成となっていて，上位のコンピュータで広域制御を行っているが，この上位コンピュータが故障した場合，下位のコンピュータに制御を移し，各道路ごとの系統制御を実施する．これを1次フェイルセイフという．また下位のコンピュータや回線が故障すると，各交差点の制御器が動作し，単独制御を実施する．これを2次フェイルセイフという[5]．

このように機器の故障時にシステムの機能は低下してもそれをダウンさせない手法を「フェイルソフト」と称するが，機能を停止させると危険な状態に至るシステムでは，こうしたフェイルソフト手法をもフェイルセイフな設計と称している．

**2.1.5　プラント関連のフェイルセイフ**

石油化学プラントなどのフェイルセイフは「機械，設備に異常，故障等がおきたとき，必ず安全な方向，すなわち運転停止の方向に向かうよう設計されていること」をいう[6]が，これらのシステムでは多くの場合，何ごとも変化なく，運転を維持しておく方が安全といわれ，一斉に停止することはかえって危険をまねき，複雑な場合になると，安全側がいずれか一方に固定できないという特性を有している．

**2.1.6　医用電子機器のフェイルセイフ**

最近，医用電子機器が発達し，患者に直接電極をつける機器等が使用されている．これら医用電子機器の安全側は人体に漏れ電流を与えないよう構成することといわれ，危険要因をできるだけ除去するよう構成する手法をフェイルセイフと呼んでいる．

**2.1.7　コンシューマ機器のフェイルセイフ**

家庭電化製品などいわゆるコンシューマ機器に対してもフェイルセイフが使われている．この場合には，消費者は技術的に無知であるという前提のもとに，誤って使用しても安全で，失敗のないシステムを作る，いわゆる「フールプルーフ」機構をフェイルセイフということが多い．

**2.1.8　その他のフェイルセイフ**

自動車を運転する際に安全ベルトをしめることもフェイルセイフといわれ，そのほか軍事システム（アメリカの戦略空軍）におけるフェイルセイフシステム[7]，計算機制御システムにおけるフェイルセイフ[8]などがあり，非常に多くの分野で広い意味に使われている．

**2.1.9　広義のフェイルセイフのまとめ**

以上に示すように一般のフェイルセイフは非常に広い意味をもっている．ここで各分野のフェイルセイフについて特徴的な安全側の状態を考えてみると，図-1に示すようにまとめられる．そしてそれぞれに使われている安全性技術・手法は同じ 図-1 に示すように8分類からなる手法に関連づけられる．すなわち，広義のフェイルセイフは一般に良く知られている安全性向上のための技術・手法の全般にわたり，広範な技術の総称と考えられる．しかしフェイルセイフをこのように広く解釈すると，フェイルセイフ技術・手法の真の意義をあいまいにさせる恐れがあるため，本文では，もう少し厳密な，狭い意味のフェイルセイフな構成法について以下に考察する．

**2.2　狭義のフェイルセイフ**（鉄道信号におけるフェイルセイフ構成例）

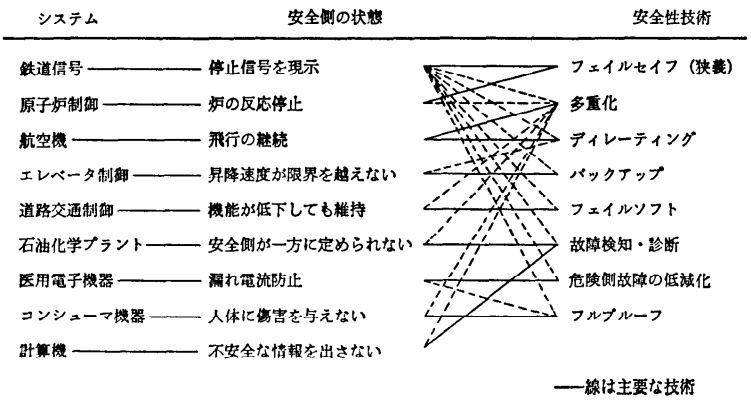


**図-1**　種々な分野におけるフェイルセイフの関連図

狭義のフェイルセイフの厳密な定義に関しては後に構成理論の項で述べることにして，最初に実用面のフェイルセイフ構成例を述べる．

狭義のフェイルセイフ技術の代表的な例は何といっても鉄道信号のシステムであろう．鉄道信号システムでは，進行信号であれば，列車は進行しうるから，停止信号を出すべきときに，誤って進行信号を出したなら，列車は衝突したり，大事故に至る危険がある．逆に進行信

号を出すべきときに，機器の故障により停止信号を出しても，列車は停車するだけで危険はない．したがって，鉄道信号機器は故障が発生した場合，停止信号が出されるように構成され，それが安全側を示すことになる．このような考え方をもとにして，鉄道信号の分野では独特なフェイルセイフ技術が早くから芽生え，経験的に確立されてきた．そこには過去に経験した事故を二度と繰り返さないようにする多くの教訓が結集され，確立されている．

### 2.2.1 電磁リレーによるフェイルセイフ構成例

鉄道信号のフェイルセイフの代表例は重力利用による電磁リレーに見られる．この種のリレーにおいて電気回路が構成され，リレーの電磁石が励磁されると，その電磁吸引力は重力に抗して働き，動作接点を構成させる．したがって復旧接点を安全側に，動作接点を非安全側の信号に割り当てれば（たとえば，復旧接点で停止信号を，動作接点で進行信号を点灯する構成とすれば），電気回路，コイルなどの断線障害が発生しても，リレーは重力によって確実に復旧し，安全側（停止信号）になる．近年のリレーは復旧力に「接点ばね」を利用したものが多くあるが，フェイルセイフ構成の考え方は重力利用のものと変らない．

以上のように障害時の故障モードが一方に限られ，その発生確率が非対称となるような素子を「非対称誤り素子」と称する．鉄道信号設備は非対称誤り素子を利用して，その安全性を確保しているといえる．なお，安全側の故障モードを「許容故障状態」という．

### 2.2.2 電子的な回路のフェイルセイフ構成例

電子回路がフェイルセイフであるためには，回路を構成する各部品の故障状態を検討し，その影響について考慮しなければならない．特に半導体の導通故障，断線故障に対しても安全側に動作することが必要である．このため現在，信号機器に最も多く使われているフェイルセイフ構成法は，交流回路を利用するもので，最終出力として前述の信号用リレーを駆動する方式である．**図-2** にリレー駆動回路のフェイルセイフ構成例を示す．

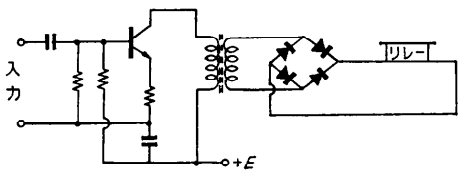


**図-2** リレー駆動回路におけるフェイルセイフ構成例

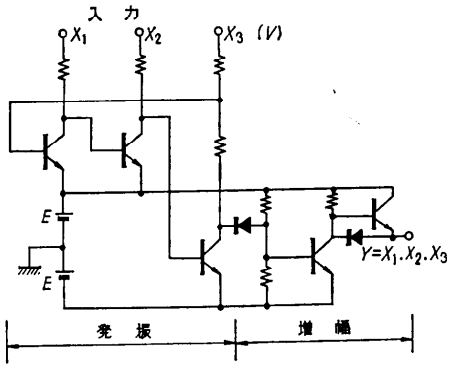


**図-3** しきい値発振形フェイルセイフ論理回路の構成例

図に示すように増幅回路により交流入力を増幅し，トランスを介して得られた出力を整流し，信号用リレーを駆動する．この回路において，たとえばトランジスタが導通故障をおこしても，トランスの2次側には出力が現れず，リレーは復旧し，安全側となる．現在の鉄道信号分野では，電子信号といわれるATC(自動列車制御装置）といえども，最終出力はこのような回路により信号用リレーを用いてフェイルセイフを確保している．

### 2.2.3 電子的なフェイルセイフ論理素子の構成例

一般の半導体理論回路は故障モードが真理値0または1のいずれに誤るか判らず，いわゆる非対称誤り素子ではないから，そのままの形でフェイルセイフを要するシステムに用いることはできない．そこで，信号用リレーに代る電子的な非対称誤り素子の開発が試みられている．

**図-3** は電総研の土屋氏らによって提案された抵抗と半導体によるしきい値発振形のフェイルセイフ論理素子の構成例である[9]．図-3のように3個のトランジスタを接続して，帰還すると，すべての入力電圧が $V$ （$V>E$）なるときのみ発振する．この回路の抵抗，トランジスタの故障および入力電圧が $E$（$B$電圧）より低下したときは発振することはなく，この発振出力を増幅し，整流し，次段の入力として用いることにより非対称誤り形の論理回路が構成できる．またこれを薄膜集積回路で構成した例もあり[10]，実用性の高い素子として後述する電子連動装置にも一部使用している．

### 2.3 新幹線運転管理システムにおけるフェイルセイフ構成例

鉄道信号設備も近年，大規模化し，コンピュータの導入が必要となってきた．そこで昭和47年より新幹

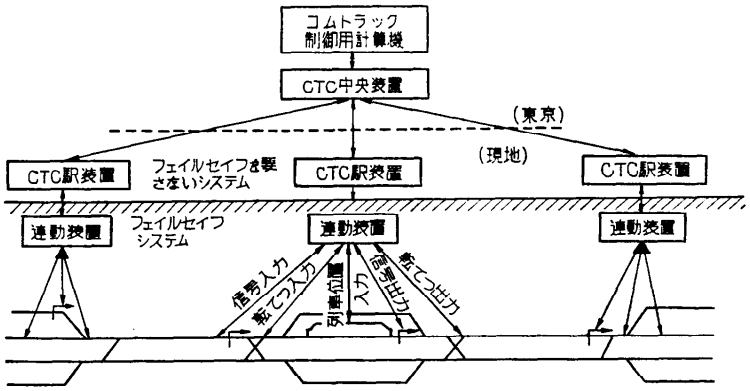


図-4　新幹線運転管理システムのフェイルセイフ構成例

線全線の全列車の運転状況の監視と，全信号機（ATC進路）の制御をコンピュータで行うコムトラック（Computer aided traffic control）運転管理システムが実用化された．このシステムをフェイルセイフ構成の観点から眺めると，図-4 に示すように階層構造として構成され，直接制御に関与する機器のみをフェイルセイフ構成としている．このため，上層のコンピュータや CTC と呼ばれる伝送装置はフェイルセイフを要さず，コンピュータは単にスーパバイズする機能をもてばよく，誤制御やシステムダウンが発生しても，列車運転の安全性を犯すことはない．このシステムの安全性は各駅ごとに設置されている連動装置（駅構内の信号機や転てつ器に一定の連動関係を与えて制御し，列車の進路を安全に構成する装置）によって確保されている．現在この連動装置には，前述した電磁リレーを使用した装置が一般に使用されているが，これにコンピュータを利用したシステム（これを電子連動という）を開発することが世界各国の鉄道における当面の課題であり，これがフェイルセイフを要するためにコンピュータを用いたフェイルセイフなシステムの開発が必要となるに至っている．

## 3. フェイルセイフシステム構成理論

フェイルセイフシステムの理論的な研究は，鉄道信号機器にエレクトロニクスを導入する研究に端を発し[11]，1965 年ごろより国内はもとより，諸外国においてもディジタルシステムを中心に多くの研究成果が発表されている[12)~18)]．これらの理論は，種々な立場から研究されており，これらを大別すると，前述した「非対称誤り素子」を要する理論と，要しない理論に区別される．ここでは先に前者の理論の概要を述べる．

### 3.1 フェイルセイフの定義

「ある論理系において故障が生じても，誤り出力があらかじめ決められた安全側の出力に限られるとき，その論理系はフェイルセイフである」と定義されている[15]．すなわち，システムの正常時 $\lambda$ の出力集合を $Z_n$，正常時の出力関数を $Z(x,\lambda)$（$x$ は入力ベクトルを示す），安全側の出力集合を $Z_s$，故障 $f$ が生じたときの出力関数を $Z(x,f)$ とすると，入力 $x$，故障 $f$ に対して，

$$Z(x,f)\neq Z(x,\lambda)\Rightarrow Z(x,f)\in Z_s$$

ならば，このシステムはフェイルセイフであるという．

ここでいろいろの立場の理論があり，$Z_n$ と $Z_s$ は $Z_n\cap Z_s=\phi$ であるものと，そうでないものがあり，その素子の性質によりさらに 2 値論理，3 値論理などに類別される．

### 3.2 2値フェイルセイフ論理系

2 値フェイルセイフ論理系は非対称誤り素子の性質から，単一方向誤りの理論と双方向誤りの理論に類別される．前者は前述の信号用リレーのように誤りの方向が一方で，復旧側だけの素子を利用して構成される理論で，後者は 0 または 1 に誤る 2 種類の素子を利用できる場合の理論である．

非対称誤り素子を構成する立場からは一般に前者のものが多く考えられている．その理由は 0 または 1 に誤る双方向誤り素子を開発するには，リレーにたとえると，故障時に復旧側に誤るもののほか，動作側にも誤る素子を作る必要が生じ，構成し難いためである．したがって現在開発されている素子は単一方向誤りに関するものが多く，フェライトコア論理，磁気増幅器などが発表されている[16]．一方，双方向誤り素子としてはパラメトロン[12]によるものがあるほかは，対称誤り形の素子（一般の半導体素子）を直並列に接続し，非対称誤り特性を付与するもののみである[14]．

一方，構成理論の立場からは，双方向非対称誤りの理論が一般的である．詳細は文献 15) 等を参照されたい．

### 3.3 3値フェイルセイフ論理系

2値論理によるフェイルセイフ系の最大の悩みは，$Z_n \cap Z_s \neq \phi$ で，正常時の出力集合と故障時の安全側の出力集合が区別できないことである．すなわち $Z_n = \{0, 1\}$，$Z_s = \{0\}$，または $\{1\}$ となるからである．そこで，3値フェイルセイフ論理系はこれを区別すべく $Z_n = \{0, 1\}$，$Z_s = \{s\}$ とし，$Z_n \cap Z_s = \phi$ としたもので，正常なる値0，1のほかに故障状態 $s$ を付加し，3値としたものである．

3値フェイルセイフ論理系では $s$ の値の性質に基づき，C形[9]と $\phi$ 形[15]の2形式が発表されている．また3値論理系用の素子としては **2.2.1**（3）で前述したしきい値発振形素子[9]，薄膜磁性線による素子[17]などが発表されている．

### 3.4 セルフチェッキングシステム構成理論

前述までの理論はいずれも非対称誤り素子を必要とするが，一般の素子を利用してフェイルセイフとする理論が発表されている．これらの理論は当初，東工大の当麻氏らが，「対称誤り素子によるフェイルセイフ」として発表されたものであるが[18]，これに対して，最近では，IBM のCarter 氏らが名づけた「セルフチェッキングシステム」という用語が一般化している[19),20)]．

セルフチェッキングシステムとは「回路の出力を監視し，回路内の故障を自己チェックする方式」をいい，出力に何らかの冗長コードを採用し，出力コードを監視するチェッカによって故障を検知するもので，このチェッカもセルフチェッキングの必要がある．

これらセルフチェッキングシステムの簡単な例は，出力として $(s_0, s_1)$ の二重化を図り，この出力が（0，1），（1，0）のときは正常動作，（0，0），（1，1）のときは故障であることを示すように回路構成を行うもので，この例では 1 out of 2コードであるが，より一般的には $k$ out of $n$ コードを用いてセルフチェッキング回路が構成できる[21]．その理論的な研究も多く，その中から代表的な「フォルトセキュア」という用語の定義を文献22),23)から紹介する．

「故障によっても，誤りのコード出力を絶対に出さない回路をフォルトセキュア（fault secure）という」．すなわち回路に故障が生じても，その出力は正しいコードか，またはある一定内のコード空間にあるとき，これをフォルトセキュアであるという．

このようにフォルトセキュアと **3.1** で前述したフェイルセイフの定義は非常に類似した概念といえ，コンピュータを用いたフェイルセイフなシステム構成法の有効な手段となり得る．

## 4. コンピュータを用いたフェイルセイフなシステムの構成

フェイルセイフの理論的な研究は前述の通り，多くの報告文が発表され，すでに成熟期を過ぎているといわれているが，実際的な応用面の研究，特にコンピュータシステムとしてまとめられたものは少ない．しかしながら，理論面にて多くの立場の研究があるように，応用面でも種々なアプローチが考えられ，大別して次の3方式が挙げられる．

（1） フェイルセイフな論理素子を用いた特殊コンピュータ方式

（2） セルフチェッキングコンピュータ方式

（3） 外部に誤り検知回路を有した汎用コンピュータ方式

以下にこれらの諸方式を紹介する．

### 4.1 特殊なハードウェアによる構成

この方式はフェイルセイフなハードウェア，すなわち，前述した非対称誤り素子を用いてコンピュータの回路自体をフェイルセイフに構成するもので，狭義のフェイルセイフコンピュータといえる．この方式の具体的な構成例としては筆者らによって1966年に開発された鉄道信号用の第1期電子連動システムが挙げられる[25),26)]．

この第1期電子連動システムでは，非対称誤り素子としてフェイルセイフ形のパラメトロンを使用している．一般のパラメトロンと異なる点はフェイルセイフ定数（論理値 “0” または “1”）が与えられ，素子に故障が生じたとき，与えられた定数に誤るので，故障時に “0” に誤る素子と “1” に誤る素子という双対な許容故障状態を有するものが実現でき，**図-5** に示すように，一方の系は論理値 “0” を，他方の系は

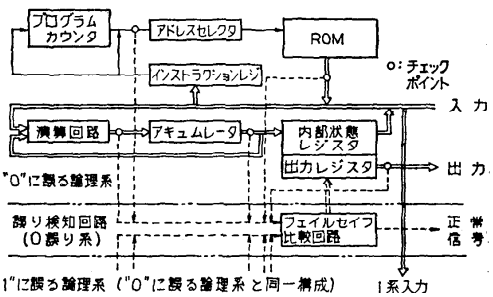


**図-5** 特殊なハードウェアによるフェイルセイフコンピュータの機能構成図

論理値“1”を許容故障状態とする「同一論理双対故障形二重系」により誤り検知を確実化し得る．すなわち，この二重システムが故障すると，その論理値は一方の系が“0”に，他方の系が“1”にそれぞれ故障するから，両系が同時に故障しても論理値は不一致をきたし，確実に故障を検出し得る．

誤り検知回路は“0”を許容故障状態とする基本論理回路により「同値検出回路」を構成すれば良く，この検知回路自体が故障しても“0”に縮退故障し，これが不一致信号を意味するので，フェイルセイフを満足する．

この方式は有効な非対称誤り素子の開発にかかっており，単一方向のみの非対称誤り素子が得られるならば，論理を双対構成とする「双対論理同一故障形二重系」システムが構成できる．目的は異なるが電気試験所（現電総研）の初期のリレー形計算機 ETL MARK II 計算機[27]はこの双対論理同一故障形二重系で構成されており，有効な電子素子が得られたなら参考となる構成法であろう．

### 4.2 セルフチェッキング回路による構成

前節で論じた構成法は非対称誤り素子を前提にしているが，この構成法は一般の対称誤り形の素子を用いて構成できるので，自由度は大きい．理論的な研究の概要は前述した通りであるが，実際的な応用面の研究はまだ少なく，今後に期待されるところである．ここではコンピュータの演算ユニットに対して部分セルフチェッキングを行う構成例を紹介する．

セルフチェッキング回路はコード出力を監視し，自動的に故障を検出したり，出力を防護しようとするもので，多くのコードが研究されている．一般に演算回路には情報ビット(I)とチェックビット (Cp) が分かれている Separable コードが使われており，Wakerly 氏はコンピュータの演算ユニット (ALU) が論理演算を行うときのみ，すなわち，Secure な入力モードのときのみ，セルフチェッキングを行う構成法を提案している[24]．

**図-6** にこの部分セルフチェッキング回路の構成図を示す．図-6 に示すように回路は Secure モード $(C_0, C_1)=(0, 1)$ のときのみ，チェッカでセルフチェックし，Secure モードでないときには，スイッチ回路によりチェックビットジェネレータからの出力自体をチェッカに入力し，常にチェッカ出力が良好になるように構成した手法である．この方式は完全なチェック法とはいえず，また故障を即座に検出できない欠点を

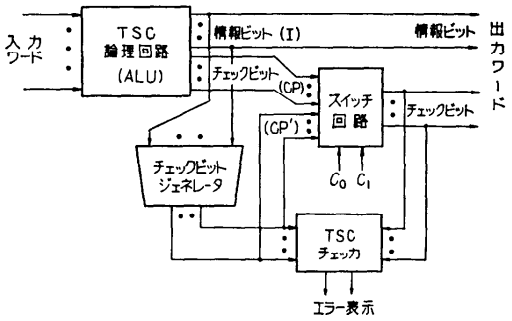


**図-6** 部分セルフチェッキング回路構成例

有するが，やがては Secure モードとなり，その時点で故障検出されるので，実用性の高い手法といえる．なお応用例として示された ALU は4ビット演算用の MSI チップから成る情報ビット16，チェックビット4で構成された演算回路である．

またベル研の Gay 氏らは信頼性の観点からこの Secure モードによる最適なチェック周期を求める手法を提案している[28]．

### 4.3 汎用コンピュータを用いる構成

この構成法は一般に使用されている汎用コンピュータ(ミニコンまたはマイコン)を冗長構成し，その外部に誤り検知回路を設け，これによりシステムとして，フェイルセイフを満足させようとするもので，誤り検知回路に非対称誤り素子を用いるのが一般的である．この汎用コンピュータの冗長系の構成法として大別して次の3方式が提案されている．

(1) ソフトウェア二重化（単一ハードウェア）方式
(2) 二重系方式
(3) 2 out of 3系方式

**4.3.1 ソフトウェア二重化方式**（単一ハードウェア方式）

この方式の代表例は，スウェーデン国鉄とエリクソン社で開発し，スウェーデンのイエテボリ駅の連動装置として実用化されたシステムが挙げられる[29]．**図-7** にそのハードウェア構成を示す．

このシステムは中央の4台の計算機，2台のインタフェース機器，および多数のコンセントレータ（現場機器と情報の授受を行う端末の集線装置）から構成されている．計算機は階層構成され，連動用計算機は2台のミニコン（エリクソン製 UAC 1610）から成るが，単一系として稼動し，一台は待機予備系である．

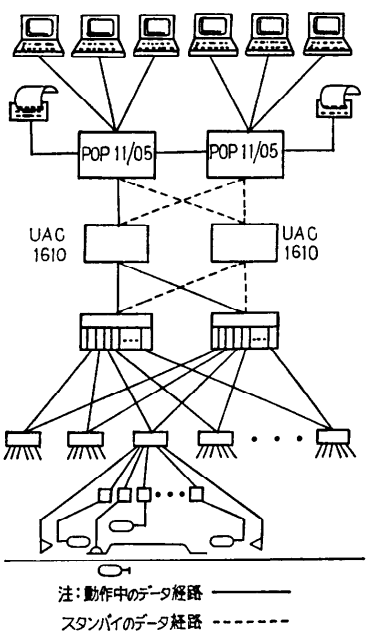


図-7 エリクソン方式電子連動システムのハードウェア構成図

この単一系には，A，Bと称する2組の独立したプログラムが実装され，同一の処理を2組のプログラムで二重化処理を行う．それぞれの制御出力は，2台のインタフェース機器と伝送ラインを介して，個別に同一のコンセントレータに出力される．コンセントレータでは，2組のプログラムで処理され，出力された制御指令を比較し，一致している場合に現場機器を実制御するもので，コンセントレータの比較回路，および出力回路には信号用の電磁リレーを使用し，フェイルセイフを確保している．

この方式の特徴はソフトウェアの二重化により，処理装置のハードウェアを単一系で構成でき，コスト低減を図れることにある．2組のソフトウェアは独立に作業する2組のプログラムにより別個に作成され，プログラムバグに基づく制御誤りを防止している．

#### 4.3.2 二重系方式

ハードウェアを二重化する方式は最も一般的で多くの構成法があるが，ここでは西ドイツのジーメンス社にて開発された「安全マイクロコンピュータシステム(SIMIS) Sichere Mikrocomputersystem」を紹介する[30]．図-8 に SIMIS の構成図を示す．

このシステムは同一のクロックパルスで同期して制御される2つのマイクロコンピュータと，それぞれのバスの情報を比較する比較器から構成されている．比較器は両系のバスの情報が一致しているときのみ，クロックパルスを通過させる機能を有する．

クロックパルス発生器は，2台のマイクロコンピュータにクロックパルスを送出する前に，照合用パルスを比較器に送出する．これにより両系のバスの情報が一致していることを照合し，一致を示すクロックパルスが比較器から返送されてくるのを受信した後，制御パルスを2台のマイクロコンピュータに送出するよう構成されている．したがって，情報に不一致が発生した場合は制御用のクロックパルスが送出されず，マイクロコンピュータは停止し，出力信号変換器が出力を安全側に固定し，フェイルセイフを満足する構成である．

このシステムは西ドイツ連邦鉄道で車内信号用制御装置として機関車に搭載し，試験が続けられており，連動装置への適用も検討されている．

#### 4.3.3 2 out of 3 系方式

前述の二重系による方式はフェイルセイフの観点か

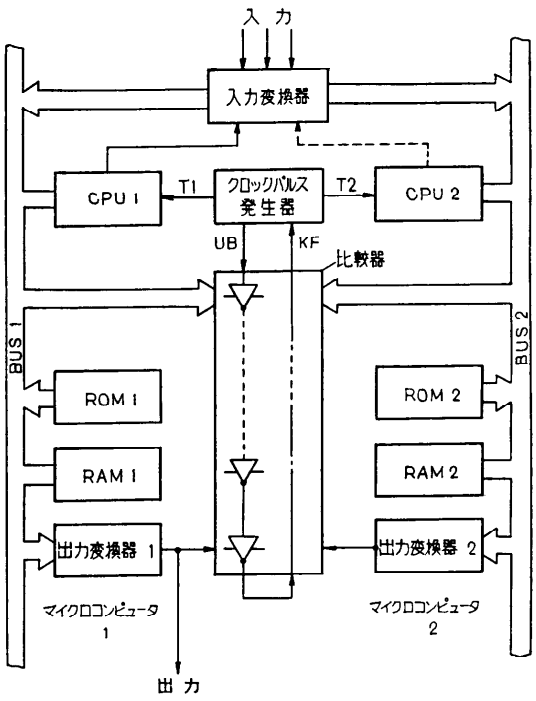


図-8 SIMIS マイクロコンピュータの構成図

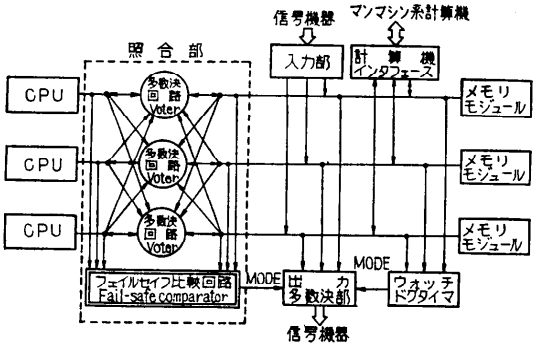


図-9 バスレベル同期式高安全性コンピュータ

ら満足するものであっても，実用的には信頼性の観点から，さらに待機系を設ける必要が生じ，結果として四重化せねばならなくなり，経済的な問題が生ずる．そこで 2 out of 3 系が有効と考えられる．2 out of 3 系構成としては，イギリス国鉄[31]と筆者ら日本国鉄の構成例が挙げられる．以下に筆者らが開発中の第2期電子連動用高安全性計算機の構成について述べる[32),33)]．図-9 にそのハードウェア構成図を示す．

この計算機は内部に多数決回路と故障検出回路を有し，常に3台のマイクロプロセッサのバス情報を照合しつつ動作するものである．すなわち，マイクロプロセッサのバスに双方向の多数決回路を挿入し，多数決回路を通してマイクロプロセッサはメモリや入出力回路と接続されており，同一のクロックにより3台のマイクロプロセッサの情報が常に多数決され，バスレベルで同期して動作する構成である．またこの多数決回路も三重化され，これら多数決回路の入出力情報を比較する故障検出回路を有し，多数決回路の故障も含め，不良系の判定を行い，故障が検出された場合，その系の切り離しを行い，二重系運転で稼動することができる．また不良系の保全も可能である．さらにこのシステムの制御出力回路には前述したしきい値発振形の非対称誤り素子による回路[10]を使用し，最終的な出力情報のフェイルセイフ化を図っている．

なおこの電子連動システムは，マイクロプロセッサとしてインテル社の 8085 を使用し， ROM 32 KB, RAM 8 KB を有し，56年3月より上越線石打駅の連動装置（106 進路）としてフィールドテストを実施中である．

### 4.4 ソフトウェア上の配慮

コンピュータを用いたフェイルセイフなシステムではソフトウェアの欠陥によるシステムの誤動作が致命的な事故に結びつく．そのため，ソフトウェア構成上の特段の配慮が必要である．しかしフェイルセイフなソフトウェア構成法といった定式化された手法が確立されているわけではないので，ここでは筆者らが電子連動システムで検討した手法[34)]を紹介する．

高安全性を要するソフトウェア開発上で配慮すべき事項は大別して，高信頼ソフトウェアの開発とハードを含めたシステムの高信頼化をサポートするソフトウェアの開発とが挙げられる．前者はさらに誤りのないソフトウェア (Software correctness) の作成と誤りに対して強靭性を有するソフトウェア (robustness) の作成が必要であり，後者は主に故障診断機能とその異常処理とからなる．一方ソフトウェアはプログラム構造とデータ構造の両者を検討する必要があり，連動装置としての特性から，プログラムは各駅共通なものとして汎用化をはかり，その正しさを検証するよう構成し，各駅ごとに異なる条件は経路図等の入力により自動的に作成されたデータを ROM に焼きつけるように構成した．

誤りのないソフトウェアを実現する手法としては，文書化による仕様の徹底，プログラムを処理単位に分割したモジュール構成の採用，モジュールテストから総合テストまでの綿密なテストとテストの容易性の追求を行った．

次に強靭性を有するソフトウェアを開発するため，線路図を示すファイルのダブルリンク化，定周期起動による常時スキャンニング処理方式の採用，安全側の状態割付けと容易に安全側状態へ遷移できる非対称処理の採用等を行った．

またシステムの高信頼化をサポートするソフトウェアとして，監視タイマによる安全情報出力，アイドル時の RAM 故障診断，特殊 RAM 領域での3系一致によるデータ保護等を実施した．

## 5. 今後の展望

コンピュータを用いたフェイルセイフなシステムの構成法について，その基本的な考え方や鉄道信号を主とした各国の構成例などを紹介してきた．これらを眺めると，種々な方式があり，まさに百花繚乱の感がある．しかしいずれの方式が今後発展していくかはなかなか予測し難い問題である．これには2つの理由が考えられよう．1つは各国の技術的背景，環境，安全性に対する考え方，法規などがそれぞれ異なると考えられ，将来的にも各国の実情やシステムに即した方式が

採用されるものと予想される．ほかの1つはこれらを実現させる技術がまだ急速な進歩の過程にあることである．マイコンを初めとする電子素子の集積化の技術がますます進歩するにつれ，素子自体で高信頼な，高安全なものが低価格で市販されるものと予想され，システム構成上の考え方も変化してくるものと考えられる．

また素子ばかりでなく，たとえ一部の素子が故障しても，機能は停止せず，保全性も容易なシステムの構成法が近年活発に研究されてきた．これらをフォルトトレラントコンピューティング (fault-tolerant computing) 技術といい[20]，ミサイルや原子炉の制御用にこのような機能を持ったコンピュータが市販される動向にあり，今後に期待されるところである．

最後にこうしたシステムで最も重要な安全性の解析，評価に対する技術動向として，従来経験的に伝承されてきた安全性技術に対して，システム工学的に組織的に危険な要因を見い出し，それを除去する手法が米軍を中心に開発されてきた．こうした解析手法の進展とともに，システムの安全性を適確に評価することが必要となろう．

## 参考文献


1) 奥村：鉄道信号におけるフェイルセイフ，昭49電子通信学会全国大会，S13-5.
2) 川口他：原子炉におけるフェイルセイフ，同上，S13-8.
3) 島：旅客輸送用航空機のフェイルセイフ，同上，S13-7.
4) 宮尾他：高速エレベータのフェイルセイフと安全性，同上，S13-6.
5) 猪瀬：道路交通制御，信学誌，Vol. 54, No. 11, p. 1598 (Nov. 1971).
6) 機械安全化・無公害化委員会：安全計装システムの指針，計量管理協会 (1975).
7) J. レイモンド：フェイルセイフとペンタゴン，朝日ジャーナル (1963年1月13日).
8) 三森他：高信頼度化二重系計算機システム，電学論 (C)，Vol. 92-C, No. 1 (Jan. 1972).
9) 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，No. 695 (Jan. 1969).
10) 森谷他：薄膜集積化フェールセーフ論理素子，日本信号技報，Vol. 2, No. 3, p. 9 (July 1978).
11) 川西他：信号設備にエレクトロニクス導入の研究報告書，信号保安協会 (Mar. 1965).
12) 渡辺他：パラメトロンによる準フェイルセイフ論理系，信学会電算研資 (Dec. 1965).
13) 駒宮他：フェイルセイフ論理回路概要，昭41電四連大，No. 1986.
14) Mine, H. and Koga, Y.: Basic properties and a construction method for fail-safe logic system, IEEE, Vol. EC-16, No. 6, p. 282 (1967).
15) 平山他：Fail Safe 論理系の構成理論，信学論 (C)，Vol. 52-C, No. 1, p. 33 (Jan. 1969).
16) 奥村：フェイルセイフ論理系における磁気素子，応用磁気137委員会シンポ，p. 57 (Jan. 1970).
17) 川西他：磁性線を用いたフェイルセイフ論理素子，信学会磁気応用研資，NM 43-23 (1969).
18) 当麻他：対称誤りを考慮したフェイルセイフの構成法，信学論(D)，Vol. 55-D, No. 3 (Mar. 1972).
19) 奥村：セルフチェッキング回路の話題，昭53連大 No. 201, p. 6.
20) 当麻，南谷：フォールトトレラントシステム，信学誌，Vol. 63, No. 10, p. 1031 (1980).
21) Tohma, Y., et al.: Realization of Fail-Safe Sequential Machines by Using a $k$ out of $n$ Code, IEEE, Vol. C-20, No. 11 (1971).
22) Anderson, D. A. and Metze, G.: Design of totally self-checking check circuits for $m$ out of $n$ codes, IEEE, Vol. C-22, No. 3, p. 263 (1973).
23) Carter, W. C., et al.: Cost effectiveness of self checking computer design, in Proc. FTCS-7, p. 117 (1977).
24) Wakerly, J. F.: Partially self-checking circuits and their use in performing logical operations, IEEE, Vol. C-23, No. 7 (1974).
25) 奥村：鉄道信号用連動装置のハードウェアに関するフェイルセイフ構成法，電学論(C) Vol. 50-C, No. 6, p. 131 (June 1975).
26) 奥村：フェイルセイフを要する鉄道信号用連動装置のプログラム構成法，同上，Vol. 49-C, No. 29 (1974).
27) 駒宮他：Theory and structure of the au-to-ma-tic Relay computer E. T. L. Mark II, 電気試験所研究報告，No. 556 (1956).
28) Gay, F. A.: Reliability of partially self-checking circuit, in proc. FTCS-7, p. 135 (1977).
29) Sterner, B. J.: Computerised interlocking system, Railway Engineer International, p. 29 (Nov., Dec. 1978).
30) Strelow, H. and Uebel, H.: Das Sichere Mikrocomputersystem SIMIS, Signal und Draht, Vol. 70, No. 4 (1978).
31) Cribbens, A. H., et al.: An experimental application of microprocessors to railway signalling, Electronics & power (Mar. 1978).
32) 中村他：信号保安装置用高安全性計算機の開発，昭55信学全大，No. 2368.
33) Kawakubo, K., Nakamura, H. and Okumura, I.: The architecture of a fail-safe and fault-tolerant computer for railway signalling device, in proc. FTCS-10 (1980).
34) Okumura, I., Watanabe, T. and Kawakubo, K.: The software structure of a fail-safe and fault-tolerant computer for railway signalling device, in proc. FTCS-11 (1981).


(昭和56年5月20日受付)