U.D.C. 62-192:〔681.51:681.323.022〕

計算機制御システムの信頼度向上策

Advancement of Reliability of Computer Control Systems

Computer control is being applied at an increasing rate in almost every industrial field, with a result that, the requirements for their reliability have become severe. The article describes Hitachi's design philosophy concerning Hitachi Control Computer series referring to the high reliability technique for computer control systems from the stand point of hardware, software and system engineering.

森田和夫* *Kazuo Morita*
桑原　洋* *Hiroshi Kvwahara*
川崎　淳** *Jun Kawasaki*
川本幸雄*** *Yukio Kawamoto*
三森定道**** *Sadamichi Mitsumori*

1 緒　言

計算機制御システムは，制御対象であるプラントと直結しており，1日24時間休みなく稼動させることが普通である。また，いったん故障で停止するとプラントに与える損害はいうに及ばず，しばしば危険を伴うことすらある。このような厳しい環境条件の下でオンライン リアルタル性が要求されるため，計算機制御システムは本質的に高信頼であらねばならない。

ところが，計算機制御システムの機能が高度化するに伴いその信頼性を損なう要因も増し，システム機能と信頼度とのバランシングが問題となってきている。

計算機制御システムに発生するおもな障害は**図1**のように分類できる。このように多様な障害要因さらにはハードウェアで発生した障害がソフトウェアに波及し，データやプログラムを破壊してシステム全体が停止するという複合障害までを考慮すると計算機制御システムの高信頼化に対する技術的な解決はけっして容易ではない。一方，顧客の立場からすれば，計算機制御システムにおける障害は，それが制御用計算機本体の故障であろうと，入出力装置の一部の故障であろうと，ソフトウェア不備によるものであろうと，さらにはオペレータの誤操作であろうとも，ひとたびシステムダウンに結びついてしまえば，システムが使えないという点では同じである。

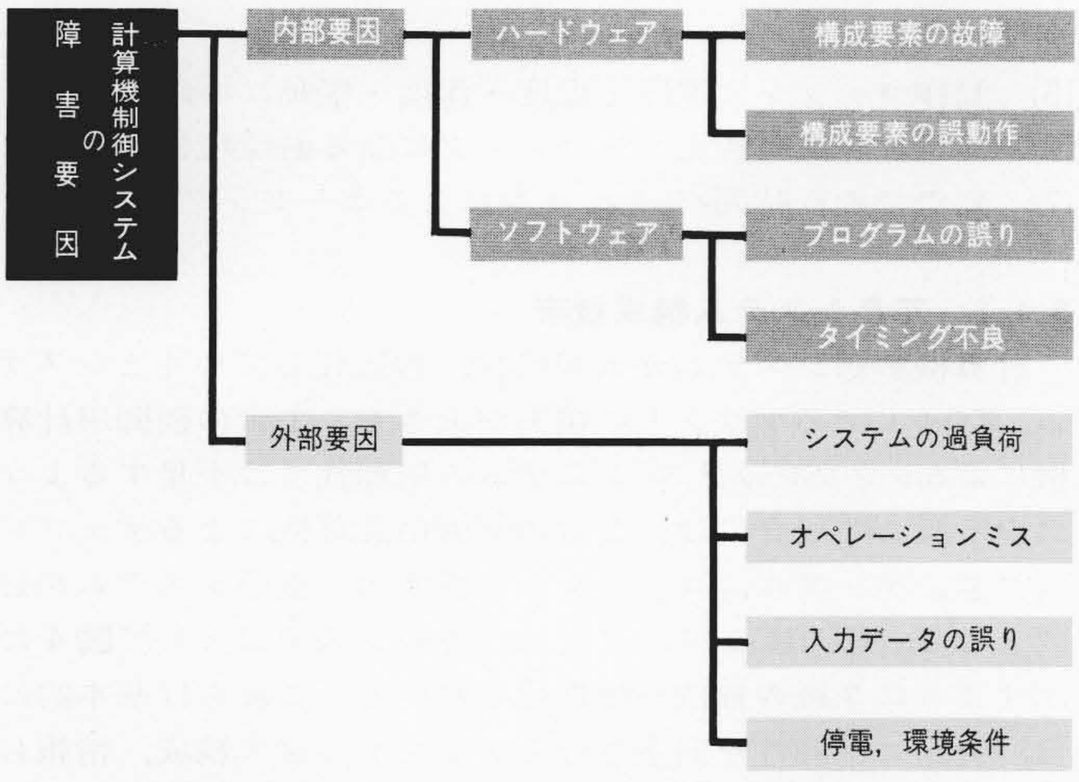

図1　計算機制御システムの障害要因　計算機制御システムの障害要因は多岐にわたっている。

Fig. 1 Type of Fault in Computer Control System

この意味で計算機制御システムの信頼度としては，まず第一にプラント操業の安全性を保証すること，すなわち，まちがった制御出力によってプラントに損害を与えぬことが大事であり，第二は，プラントの連続操業を保証すること，換言するとプラント操業の全面停止を回避すること，第三には，万一システムダウンに至ったときにはダウンからの迅速な復旧，すなわち，プラント操業停止による損失を最小にすることが重要となる。

これら3種のニーズに対する高信頼化技術は，単にハードウェアの高信頼化技術にとどまらず，ハードウェア，ソフトウェアおよびシステム エンジニアリング三者の協調によって解決すべき技術である。

以下，計算機制御システムの高信頼化に対する基本的な考え方とハードウェア，ソフトウェアおよびシステム エンジニアリング上の高信頼化技術について述べる。

2 計算機制御システムの信頼性

単に計算機制御システムの信頼性といっても，その意味する範囲はきわめて広い。たとえば一般の装置と同様に，計算機制御システムの信頼性もアップタイムとダウンタイムの比，すなわち，システムの稼動率のような寿命の信頼性で評価する場合もある。しかし，交通制御システムや高度のプラント直接制御（ＤＤＣ）の場合には，システム故障時の誤った出力により制御対象に損害を与えないことがより重要である。これは制御情報の信頼性であり，一般にフェイルセーフといわれる機能である。

2.1 システムの信頼性

単一機能の装置の場合には，装置が与えられた使命時間の間で，その機能を果たす確率をもって信頼性の評価尺度としているが，計算機制御システムでは，使用時間を一義的に定めることができないため，稼動率（**Availability**）とか平均故障間隔（以下，ＭＴＢＦと略す）といったシステムの信頼性をとらえたパラメータで評価せざるを得ない。また計算機制御が高度化すれば，その果たすべき機能も多岐にわたり，ハードウェア，ソフトウェアの構成も複雑となる。したがって，システムの一部の障害でシステム全体を停止させることなく障害が修復されるまでの間，システム機能を低下させながら運転を続行することが必要となる。これは一般にフェイルソフトといわれる機能であり，フェイルソフト性を考慮すれば，システムの信頼性尺度としての稼動率，ＭＴＢＦはシステムの機能ごとに定義されねばならない。

* 日立製作所大みか工場　** 日立製作所中央研究所　*** 日立製作所日立研究所　**** 日立製作所システム開発研究所 工学博士

また制御内容が複雑化するにつれて，システムダウン後のシステム復帰に要する時間（以下，ＭＴＴＳＲと略す）は単にハードウェアの修復時間（以下，ＭＴＴＲと略す）では済まなくなり，極端な場合にはＭＴＴＲの数十倍を要するケースも少なくない。このＭＴＴＳＲとＭＴＴＲの関係は，ハードウェア システムが回復してから，ソフトウェアが制御に必要なプラントの状況（パラメータ）を完全に把握するまでの時間で決まり，**図2**に示すように，制御対象プラントの時定数などの性格に依存する。プラントのデータ ロギングのような比較的単純なシステムのＭＴＴＳＲはＭＴＴＲにほぼ等しくなり，システムの寿命信頼度のおもな関心はＭＴＴＲの減少によるシステム稼動率の向上であろう。しかしながら，鉄鋼のＤＤＣの例のように，0.1秒程度のハードウェアのダウンが1時間に及ぶシステムのダウンとなるケースではＭＴＴＲよりもＭＴＢＦを重視する必要がある。

システム寿命の高信頼化技術としては，先に述べたフェイルソフト技術のほかにも，ハードウェアの固有信頼度を向上する技術として，高信頼度部品の選択，部品定格のディレーティング，部品およびシステムのエージング，さらにはデュアル，デュプレックスなどの冗長構成技術があり，ＭＴＴＲを短縮する技術としてオンライン テスト機能，トラブル シューティング技法，プログラムのオンライン トレース技法などが開発されている。

2.2　制御情報に関する信頼性

交通信号機は，故障時にはその出力が赤信号となるように作られており，万一の場合にも安全な処置がとられている。これが寿命の信頼性とは異なる情報の信頼性，換言するとフェイルセイフ性である。どのような装置といえども常にフェイルセイフに故障するということは不可能であり，これも確率的に評価されねばならない。交通信号機のような専用装置では，安全側出力（赤信号）を一義的に定めておけるが，タイムシェアリングに多様な処理を行なう計算機では安全側出力を一義的に定めることはできない。ところが，プラントとの情報の受け渡しを行なうプロセス入出力装置の各出力デバイスは専用機能となっているため，異常時に出力を安全側に固定することも可能である。したがって，計算機制御システム障害時のフェイルセイフ性とは誤り情報を出力する前に，自己の障害を外部システムまたはオペレータに知らせて，外部の専用システムまたはオペレータによって出力を安全側に固定してもらうように動作することといえる。

制御情報に関する高信頼化技術としては，システム障害の検出機能が重要であり，次の4種の技術に分類できる。

(1)　ハードウェアによるハードウェア障害の検出
(2)　ソフトウェアによるハードウェア障害の検出
(3)　ハードウェアによるソフトウェア障害の検出
(4)　ソフトウェアによるソフトウェア障害の検出

ところが，フェイルセイフ能力を高めるために障害検出能力を必要以上に強化すると，システム寿命の信頼性を損なうことになる。
このために，障害の検出とともに，処理の再試行が重要となってくる。

3　HIDICシリーズの信頼度向上策

日立製作所の制御用計算機HIDICシリーズでは，以上に述べたようにシステムとしての信頼性にその重点を置き，ハードウェア，ソフトウェアの両面から総合的手法により高いシステム信頼性を実現している。**図3**はHIDIC計算機制御システムの信頼度向上技術をまとめたものであるが，以下にハードウェア，ソフトウェアの高信頼化技術について述べる。

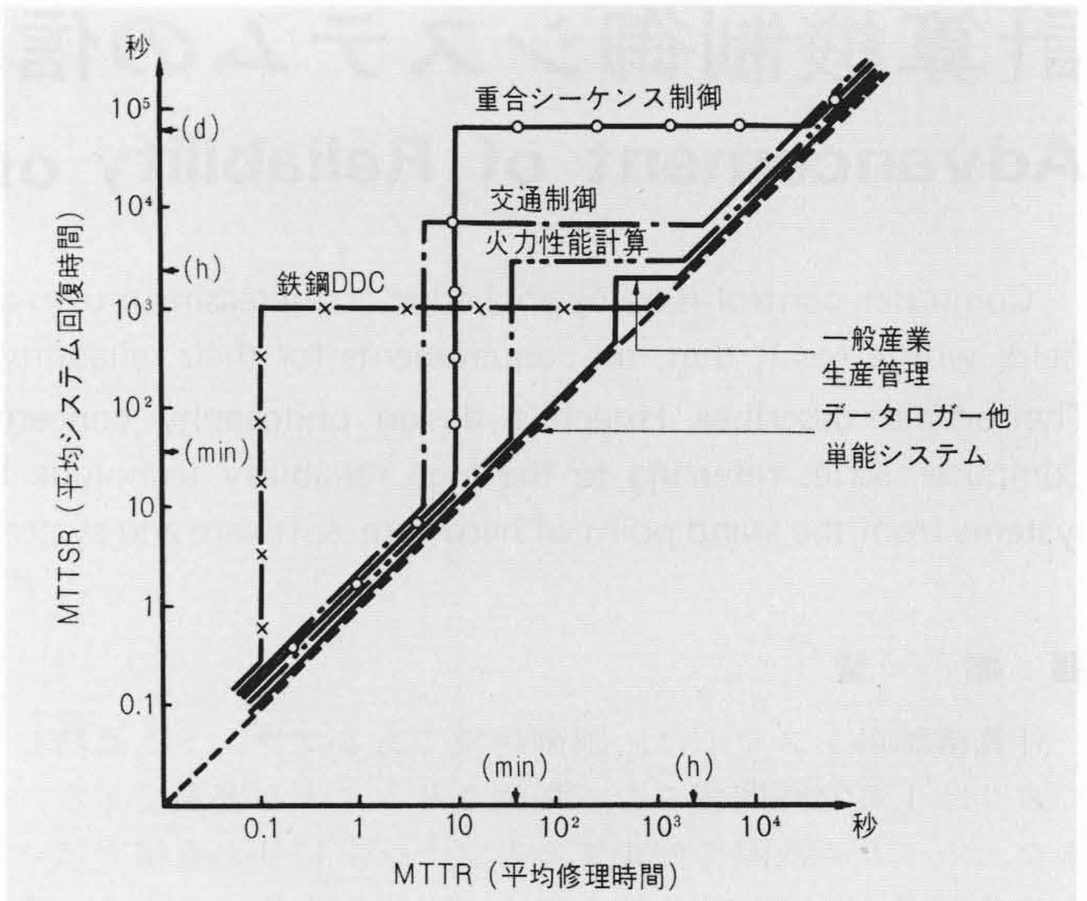

図2　ＭＴＴＲとＭＴＴＳＲの関係　ＭＴＴＲがＭＴＴＳＲに及ぼす影響は制御対象プラントの時定数などの性格により異なる。

Fig. 2　Influence of MTTR to MTTSR

3.1　ハードウェアシステムの高信頼化技術

ハードウェアの高信頼化のアプローチには，装置の固有信頼度を向上する部品・実装技術，冗長システム構成技術とシステム動作の信頼度を向上する誤り検出技術および保守技術をサポートするエラー表示・凍結技術がある。

3.1.1　部品・実装レベルの高信頼化

HIDICシリーズでのおもな信頼度向上策は下記のとおりである。

(1)　高信頼度部品の確保―部品メーカーの品質管理レベルの監視，温度ショックによるスクリーニングの実施
(2)　高集積度部品の採用による部品点数の減少
(3)　高密度実装による接触点数の減少および小形コンパクト化
(4)　部品定格（電力・電圧・電流の容量）のディレーティング使用
(5)　動作マージン（電圧・温度・湿度・振動）の確保
(6)　論理カードの樹脂コーティングによる耐環境性の向上
(7)　高温での長時間バーン インによるエージングの実施

3.1.2　冗長システム構成技術

計算機制御システムが大規模化，複雑化してゆくとシステム ダウンによるプラントの損失が大きく，1台の制御用計算機によるシンプレックス システムの信頼性では不足するようになる。この場合には，2台の制御用計算機によるデュプレックス，デュアル，ロードシェア構成の二重系システムが必要となる。HIDICシリーズでは二重系システムとして**図4**に示すように7種の構成を標準化している。これらは基本的には，寿命の信頼性を向上させるデュプレックス構成，情報および寿命の信頼性を向上させるデュアル構成，さらにはシステムの過負荷による障害を解決するロードシェア構成の3種に分類できる。**図5**は3種の二重系構成の基本形を示すものである。

以下，デュアル構成の例で二重化システムの信頼性について考察する。

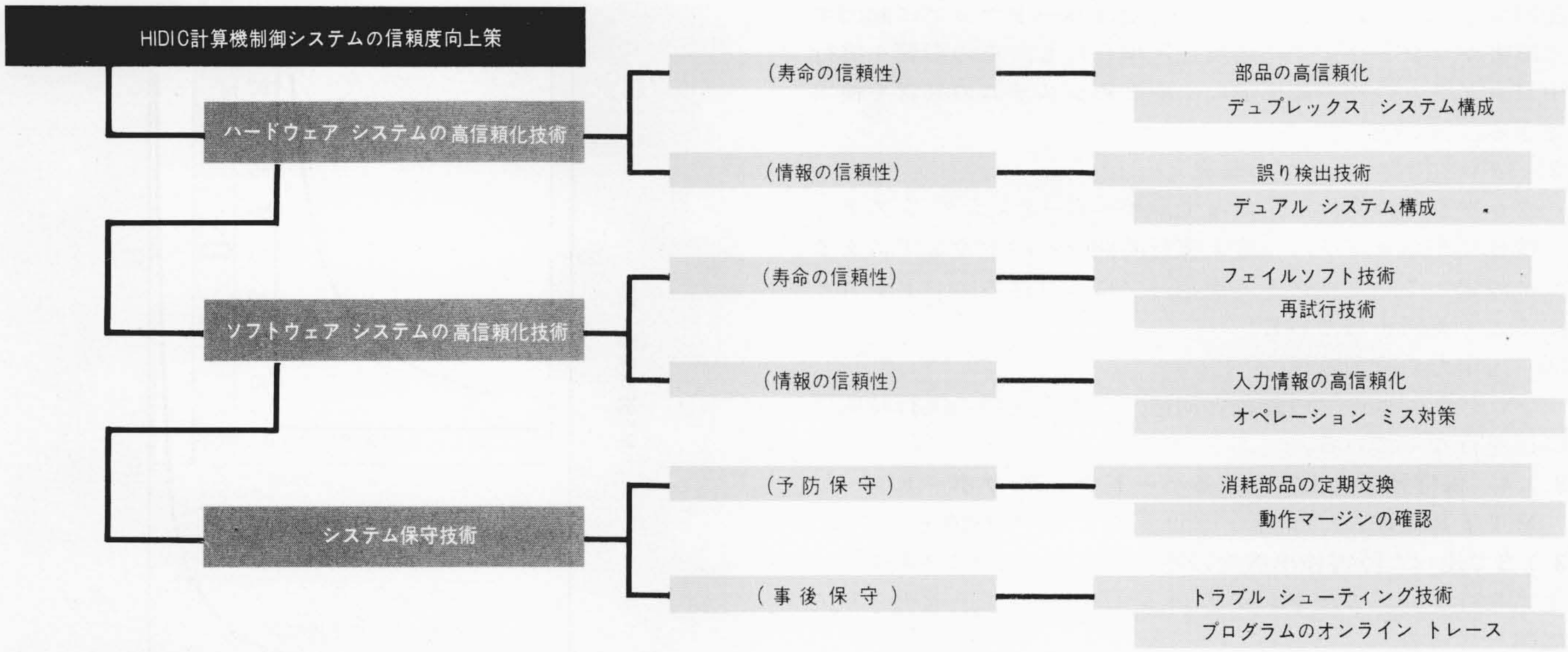

図3　HIDIC計算制御システムの高信頼化技法　HIDICシリーズではハードウェア，ソフトウェアの両面から総合的手法によりシステムの高信頼化を図っている。

Fig. 3　Advanced Technique for Improved Reliability of HIDIC Series

デュアル システムでは2台の計算機が同じオンラインの処理を実行し，その結果を照合して制御出力を行なう。この出力の照合のために，相互の動きの同期をとりながら処理を進める必要があり，処理性の低下を招くが，制御情報の信頼性は保証されることになる。ただし，実用上の問題としては，計算機が処理するすべての仕事を両系で平行処理する必要はなく，情報の信頼性を必要とする一部の重要な仕事に限って平行処理することにより，いくぶんか処理性の低下を防ぐことができる。次にデュアル システムの寿命信頼性について考えよう。デュアル システムではどちらかの系に障害が発生した場合でも，正常系がシンプレックス システムとしてオンライン運転を続行し，かつ障害系は片系運転中に修理され，再びデュアル運転を再開することができる。

このため，デュアル システムのＭＴＢＦはシンプレックス システムのＭＴＢＦの数十ないし数百倍という信頼性が期待できるといわれている。しかしこれは，障害の発見と障害系の切離しが完全に誤りなく行なえる場合にいえることであって，障害発生時に誤って正常系をオンラインから切り離してしまったら，シンプレックス システムの信頼性よりも劣る結果となってしまうであろう。障害系の切離しが α％の確率で正常に行なわれると仮定した場合のデュアル システムのＭＴＢＦの改善度を**図6**に示した。同図により，デュアル構成技術の要点はハードウェア，ソフトウェアの障害検出能力を充実し，αを高めることであることがわかる。HIDICシリーズのデュアル システムのαの値は，0.96以上であることを実験（強制障害実験）的に確かめている（すなわち，デュアル システムのＭＴＢＦは，シンプレックス システムの12倍以上）。

3.1.3　誤り検出技術

HIDICシリーズの誤り検出・修正の技術はハードウェアとソフトウェアの協調のもとで，相互扶助的に行なっている点が特色であり，その誤り検出体系の一例は**図7**に示すとおりである。以下，おもな障害検出技法について述べる。

(1)　メモリ プロテクト方式

実行中の一つのプログラムに対して主記憶装置上の二つのエリアのみを解放し，その他のエリアには書込みを禁止する方式である。すなわち，書込みを許している二つのエリアに対してその上下限値を保持するレジスタR_{1U}，R_{1L}，R_{2U}，R_{2L}を設け，書込みが行なわれようとするとき，そのアドレスAが$(R_{1L}) \leqq A \leqq (R_{1U})$，$(R_{2L}) \leqq A \leqq (R_{2U})$のいずれかの不等式を満足していることをハードウェアでチェックする。このチェックがＯＫのときのみ命令が実行され，それ以外はプログラム エラー割込を起こす。この機能により，ソフトウェアに

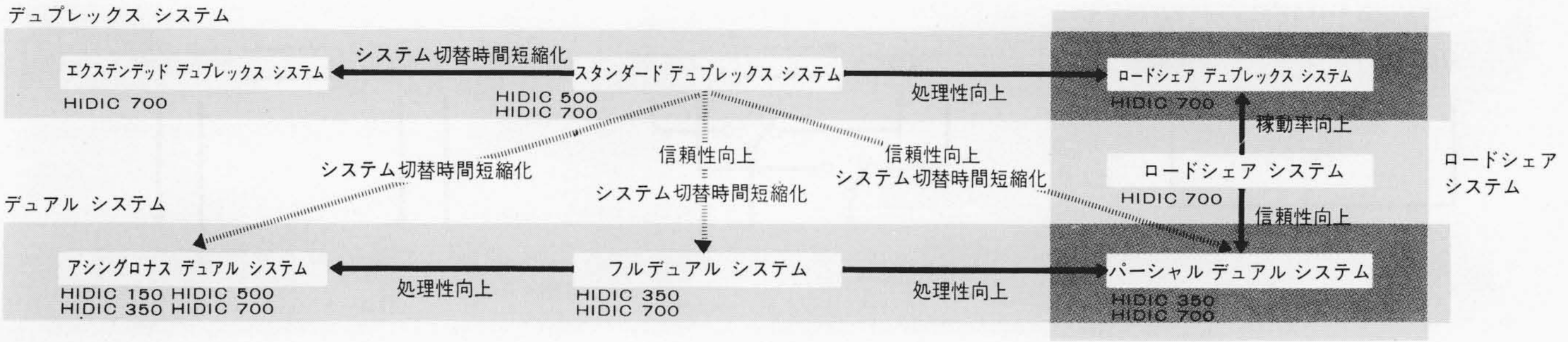

図4　二重系システムの相互関係　HIDICシリーズでは，経済性を加味しHIDIC 350ではデュアルを，順次大形になるに従いデュプレックス，ロードシェアをもサポートするようにした。

Fig. 4　Co-relation of Two Computer Systems

起因する障害が発生した場合，またはハードウェアに起因する障害がソフトウェアに波及した場合にも，その影響を実行中プログラムのみの最小限にくいとめシステムの異常を検出できる。

(2)　プログラム ループの監視

プログラムの実行に先だって，オペレーティング システム（ＯＳ）がプログラムの最大実行時間をハードウェアのタイマに設定して，プログラムがループに入り込みエンドレスとなることを防止している。

(3)　入出力の障害監視

プログラム ループの監視と同様，入出力装置の実行時間の監視を行なっている。

3.1.4　保守性の向上に対するハードウェア サポート

ＭＴＴＲ短縮のためのハードウェア サポート機能としては，**3.1.3**で述べた障害検出機能以外にも下記のようなきめ細かい手当を行ない，これをトラブル シューティング手順書として展開している。

(1)　状態表示機能

(a)　発光ダイオードによるレジスタ，ステータスおよびタイミングの表示

(b)　論理カード上の主要コントロール フリップフロップの表示

(2)　障害状態凍結機能

障害発生時の主要レジスタ，タイミングおよびステータス（障害検出コード）を保持するもの

(3)　I/O装置切離し機構（Trunk-Expander）

障害を起こしたI/Oを中央処理装置トランク（CPU TK）から切り離し，個別保守を可能とする機構

3.2　ソフトウェアシステムの高信頼化技術

ソフトウェアによるシステム高信頼化のアプローチには，ハードウェアの信頼性を補うフェイルソフト技法および再試行技法，情報の信頼性を高める入出力情報の高信頼化技法，さらにはオペレーション ミス対策，保守性サポートなどがある。

3.2.1　フェイルソフト技法

ハードウェアの信頼性を100%にすることは不可能であり，冗長構成による高信頼化は高価につくことが多い。したがって，ハードウェアの障害がシステムの本質的な機能を損なうものでないかぎり，その障害により遂行不可能となるシステム機能の一部を停止し，計算機制御システムの運転を続行する本技法はシステム寿命の高信頼化技術として有効である。

本技法適用にあたっては，停止してもよい機能を安全に停止することが重要となる。ここでいう安全とは「他の機能へ悪影響を与えずに」ということである。

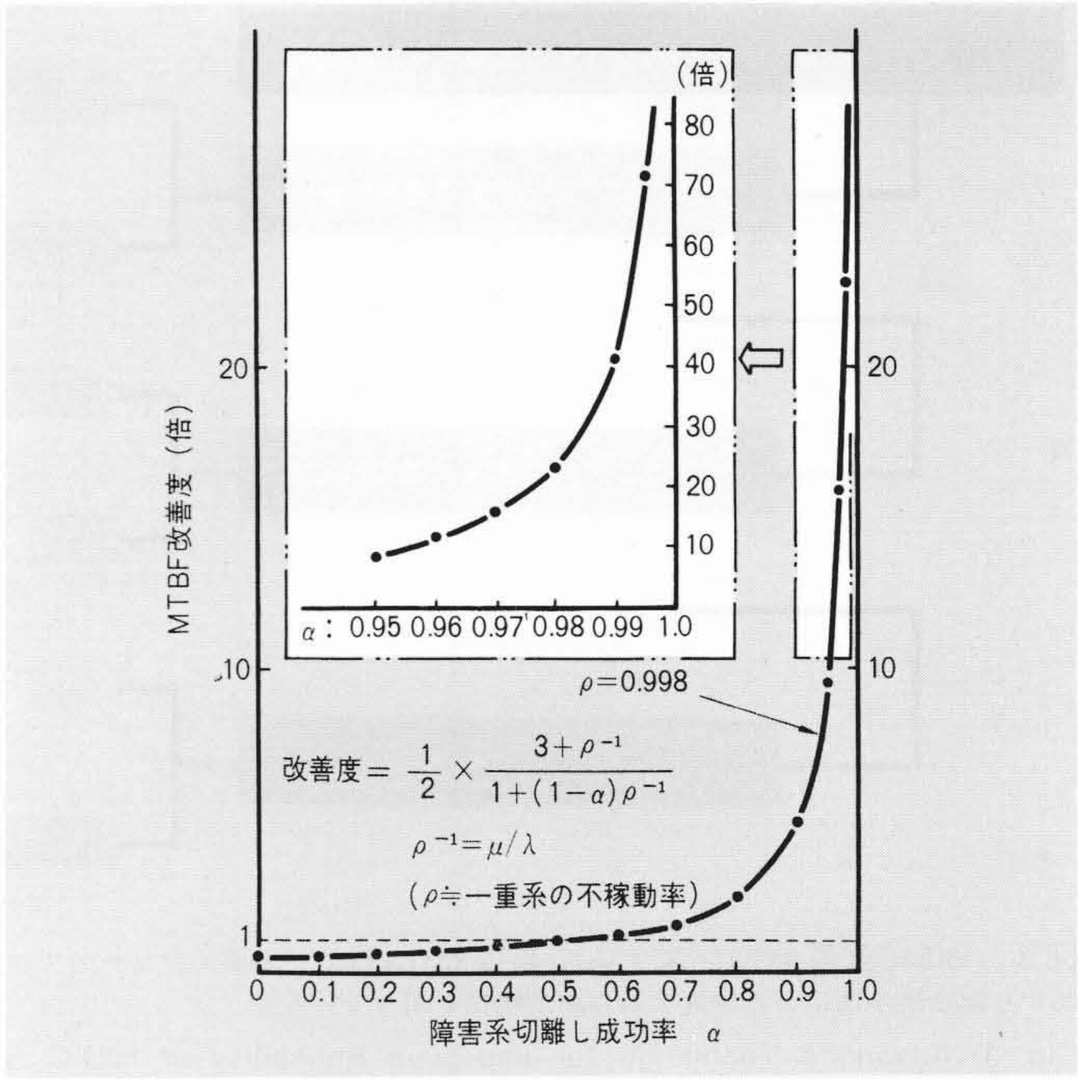

図６　デュアル システムのMTBF改善度　MTBFの改善度は障害系切離し成功率 α に大幅に依存する。

Fig. 6　MTBF of Dual System

フェイルソフト処理にはシステム機能の低下の程度に応じて以下の三つのレベルが考えられる。

(1)　レベル１：該当機能を全く停止してしまうもの。

(2)　レベル２：該当機能は見かけ上停止するが，ハードウェアが復元したときにその間で見かけ上失った情報の一部またはすべてを復元できるようにするもの。

(3)　レベル３：該当機能は停止しても，それに代わる代替機能を用意するもの。

ここでこの三つのレベルについて具体例を図示する。**図８**(a)はオペレータ リクエスト タイプライタとアラーム タイプライタをもつシステムを示すものである。両タイプライタのハードウェア仕様，印字様式は類似しているので同じデータ バッファを共有しているものとする。いまアラーム タイプライタが故障したとして，これを上記レベル１～３で実現すると**図８**(b)に示すようになる。レベル１では出力プログラムのみならず，印字処理プログラムも停止する必要があり，レベル２ではバッファのオーバフロー対策を必要とし，レベル３では切換のための論理をあらかじめ用意しておかねばな

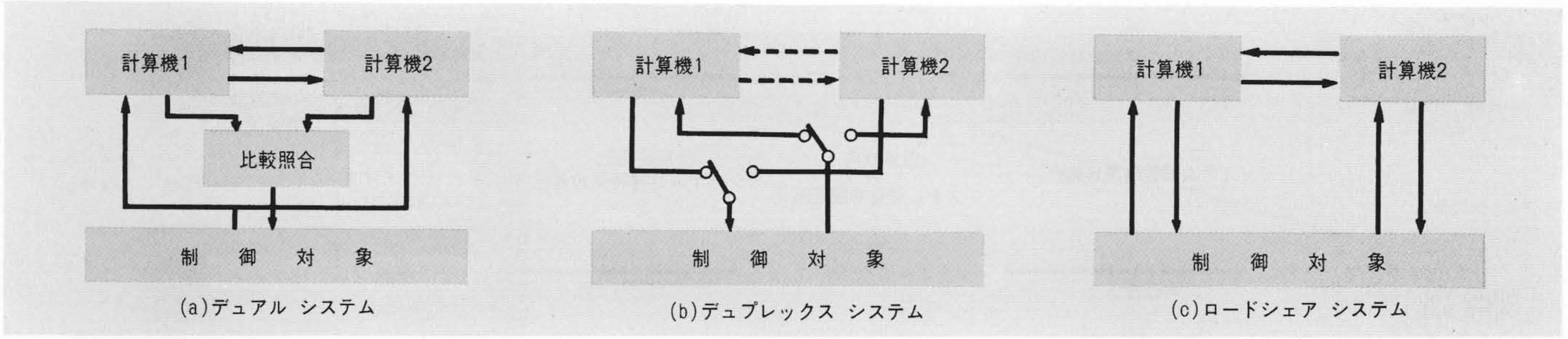

図５　二重系構成の基本形　二重系構成には，信頼性の向上を目的とするデュアル，デュプレックス，処理性の向上が目的のロードシェアシステムの３基本形がある。

Fig. 5　Typical Configuration of Two Computer Systems

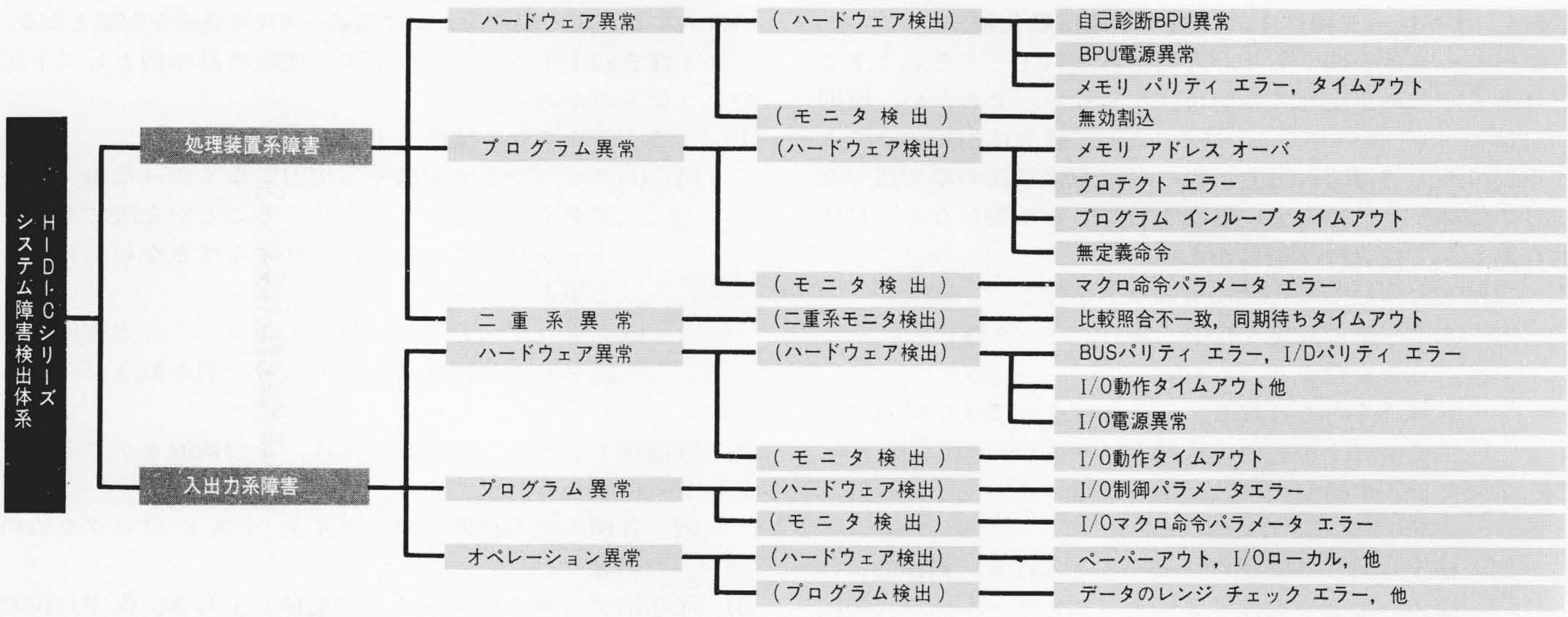

図7　HIDICシリーズの障害検出体系　HIDIC シリーズの障害検出はハードウェアとソフトウェアの協調のもとで相互扶助的に行なっている。

Fig. 7 Fault Detecting System of HIDIC Computer Control System

らない。なおレベル1の場合には，その機能はあきらめるのであるから，必然的に故障部分の局所化を可能なかぎり追求することが重要である。フェイルソフト技法の対象となる範囲は，ハードウェアの機器構成，機器レイアウト，機器間の結合方式からプログラムの組み方，故障時処置のマニュアルにまで及び，全般的にきめの細かい配慮が必要であり，信頼性向上のための総合的システム エンジニアリングとして個々のアプリケーションに対して十分な考慮を払っている。

3.2.2　再試行（Retry）技法

ハードウェアのエラーには瞬時的なものと永久的なものとがある。瞬時的エラーは再試行により救済することができるので，エラーを検知した場合，エラーの種類に応じて一定回数の再試行を行ない，エラーのシステムへの波及を防ぐことができる。本技法の対象としては，中央処理装置，入出力装置，記憶装置など計算機制御システムのほとんどすべての資源があげられる。

3.2.3　入出力情報の高信頼化技法

計算機制御システムを機能的にみると，それはデータの加工装置であるといえる。したがって，正しい意味のある出力情報を出すためには，システムへの入力信号（情報）の正しさは絶対不可欠なものである。入出力信号の高信頼技法の具体例としては次のようなものがある。

(1)　一つの入力信号の判定のために，複数個の同種入力を使用する。

例：(a)しゃ断器の入／切の状態を判定するために投入で閉，切で閉の二組の接点信号を取り論理判断を行なって，それによりしゃ断器の動作状態を知る。

(b)前出の温度測定における2 out of 3論理判断

(2)　入力信号の確からしさの判定を他の入力信号，または論理判断により行なうこと（Varification）。

例：(a)温度を測定するのに，そのものの圧力または全体系の熱平衡からその確からしさを確認する。

(b)トラッキングを行なう場合，位置検出信号に対して前後の状況，時間的考察よりその信ぴょう性を確認する。

(3)　一つの入力信号の判定のため，その入力信号のもつ特性によってテストし，その信ぴょう性を確認するもの。

例：入力値のレンジ チェック，変化幅のチェック

(4)　出力値の値の範囲を確認する。

例：DDC制御において1回の出力値の幅を監視する。

(5)　出力値の時系列的妥当性を確認する。

例：シーケンス制御において，出力を出す以前にその前の工程の重要な項目がすでに終了していることを再確認する。

図8　フェイル ソフト処理の例　フェイル ソフト技法には三つのレベルがある。

Fig. 8 3 Levels of Fail Soft Operation

3.2.4　オペレータ操作ミスに対する高信頼化技法

オペレータは人間であり，人間である以上ミスを起こすことはあらかじめ予定しておかねばならない。そのため，原則的にはオペレーション ミスはミスとして確実に拒絶することが重要であり，**3.2.3**入出力情報の高信頼化技法の項で述べた信号の信ぴょう性を十分に確認することが重要になる。具体的な例としては次の諸項目がある。

(1)　操作入力に対して合理性チェックを行なう。

例：(a)データの設定を行なう場合，データのレンジ チェックを行なう。

(b)操作を行なう場合，それを行なってよい時点であるかどうかを他の状況とにらみ合わせて判断する。

(2)　重要な操作に対しては，二重，三重にオペレータに確認する。

例：操作に対して確認のフェーズを入れる。具体的には操作→確認→実行の3ステップをオペレータに強制する。

図9はオペレータが複数の操作ボタンを同時に押した場合を想定し，これの対策を行なったフローを示すものである。ここでは点線部がその対策であるが，もしこれがないと，たとえばA，B二つのリクエストに相当するボタンを二つ同時に押してリクエストした場合，プログラムの中でリクエスト語を1ビットずつ左へシフトしてリクエスト ビットの判定をしているところから，必然的にAが実行されBは無視される。Aが本来の目的の場合にはこれでよいが，そうでない場合，特にAがなんらかの重要なデータの加工を行なうとか，Aの実行に時間がかかる場合には，システムとして大きな悪影響を受けることになる。またもし，リクエストに相当するボタンを押さないで，なんらかの理由でこのプログラムが動かされると，「15回？」の部分がなくてはダイナミック ストップになりかねない。このように通常ではあり得ない外乱に対して十分に対応し得るようプログラムを作っておくことが重要である。

3.2.5　システム保守性の向上に対するソフトウェア サポート

システム保守性の向上，すなわちMTTSRの短縮も，システムの高信頼化技術として欠かせぬ事項である。この場合重要なことは，故障部分を迅速にうまく停止させ，かつ修復を敏速に行なって事前に機能を確認し，その後にオンラインへ投入する一連の動作をいかにスムーズにできるかが鍵となる。

保守性を向上するソフトウェアの機能の具体例として下記のようなものがある。

(1)　うまく停止させる機能をもたせる。

例：(a)タイプライタが故障し出力しなくなった場合，まずタイプライタを停止させることが先決である。うっかりしていると，これすらできないシステムを組んでしまう。

(b)アナログ入力信号に対して1点ごとに走査停止機能をもたせ，異常な入力信号が引き続きシステムに入ってこないようにする。

(2)　修復後オンラインに入れる前に，その機能をテストするシステム機能をもたせておく。

例：各種入出力機器のオンライン テスト プログラムの用意

(3)　保守用データをオンラインで集積しておき，保守に役だたせる。

例：(a)直流アンプ，A/D変換器のドリフト値の集積（数年の期間）

(b)再試行により異常回復した場合の試行回数の累積

(c)入出力機器の動作回数の累積（保守インターバルの決定）

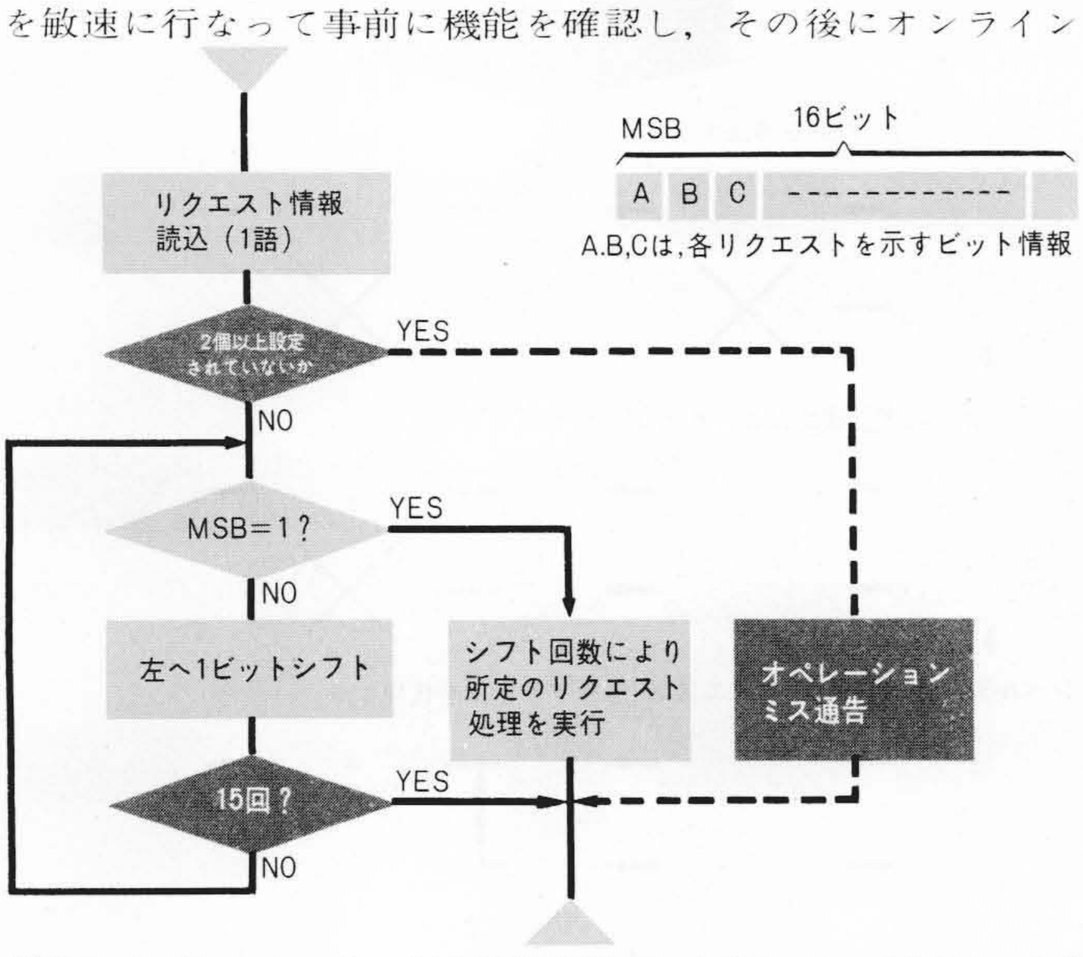

図9　オペレーション ミス対策の例　　オペレーターの操作ミスを前提に，合理性チェック機能を組み込んでおく必要がある。

Fig. 9　An Example of Protection Against Mis-Operation

3.2.6　ドキュメントの正確さの確保

システムは人間が使用するものである。それは正常状態においても，異常状態においてでも同様である。システムをうまく使用するには，その使用法，事故時の処置方法について十分に熟知し，トレーニングされていることが必要である。多くの場合，これは書き物，すなわちドキュメントとして残される。ここにドキュメントの重要さが出てくる。整然とドキュメントされていないものが，他人へ長期間（システムの寿命の間）にわたって正確に伝承されることは期待すべくもない。したがって，ドキュメントがシステムの信頼性（取扱い上の信頼性）に及ぼす影響は大きく，ドキュメントが製品の一つとして厳格な検査の対象となっている理由もここにある。

4　結　　言

以上，HIDICシリーズ計算機制御システムの高信頼性を支えているハードウェア技術とソフトウェア技法について論述したが，今後計算機制御システムの適用分野はますます拡大し，信頼性に関する要求も厳しさの度を増すものと思われる。われわれは，これに対処するため，HIDICシリーズのハードウェアの固有信頼度の向上はもちろんのこと，保守技術，ソフトウェアおよびシステム エンジニアリング技術のバランスを重視した高信頼化技術を制御用計算機システムの大きな特質の一つとして確立してゆく所存である。

終わりにあたって，平素種々ご指導，ご教示を賜わっているユーザー各位に対し深く謝意を表わす次第である。

参考文献

(1)　三森ほか：「高信頼度化二重系計算機システム」電学誌Vol. 92-C, No. 1, (Jan, 1972)

(2)　喜田ほか：「HIDIC 700二重系計算機システム」電学全大，985（昭-47）

(3)　神内ほか：「HIDIC 700システムにおける高信頼化手法」電学全大，986（昭-47）

(4)　森田ほか：「日立制御用計算機HIDICシリーズ」日立評論**55**，509（昭48-5）