U.D.C. 681.323.022:681.5]-192

計算機制御システムの計画と高信頼化

System Planning and System Reliability of Computer Control

宅間　豊*　*Takuma Yutaka*
井原廣一*　*Ihara Hirokazu*
井手寿之*　*Ide Jushi*
三森定道**　*Mitsumori Sadamichi*

計算機制御システムは，一般の計算機システムあるいは制御システムと異なった手順で建設されるが，その基本となるところは，高信頼性をもったシステムを作りあげることである。

信頼性は，システム建設のあらゆる段階でシステムに組み込まれるが，それを可能にするのは，建設過程の高信頼性でもある。本稿では，システム開発技法と，信頼性向上の方法についてハードウェア，ソフトウェア，オペレーション及びこれらを統合するシステムについて述べる。HIDIC 80システムは，従来のシステム建設で得た経験を反映して新しく開発したもので，24時間無保守で稼動率の目標を99.95%としている。

1 緒　言

計算機制御システムの導入は，ますます多方面にわたり，しかも高級な制御を行なうようになっている。当初，非常に限定された範囲，あるいは機能を対象としてシステムが構成され，たとえこのシステムが故障しても一応何らかの代替方法で制御が行なわれ，プラントの停止とか災害の発生を防ぐことができた。しかし，制御用計算機技術がソフト，ハード両面より急速な進歩を遂げるにつれて，制御システムに対する期待は増大し，より大きな範囲に対してより複雑な機能を果たすことになってきた。制御システムの不稼動は，思いがけぬ災害や巨額の失費を招くことになるので，システム自体の信頼性はますます重要なものとなっている。システム自体の信頼性は，システム建設途上で順次細心の注意を払い組み込まれるもので，これを可能にするのは，信頼度の高い建設体制，あるいは管理体制であるということも言えよう。また，システムの大規模化に伴ってオペレータとのインタフェースが複雑になるので，システムの信頼性を考える場合，人間の信頼性についても十分意を用いなくてはならなくなってきた。信頼性あるシステムを開発するシステム技法がいろいろ提案されているが，以下，実際の適用例について述べる。

2 システム計画

システム開発の手順[1),2)]としては，**図1**に示すような四つのステップが提案されており，各ステップに対するシステム技法としては，プロセス制御などを中心として開発されたモデリング，シミュレーション，最適化，適応化などがある。その一例として，計算機制御システムの計画に用いられる評価設計項目を**表1**に示す。これは，計算機システムの構成，ソフトウェア構成を決める処理効率，各リソース利用率スループット，ターン アラウンド タイム，レスポンス タイムなど[3)]を各フェーズで予測し，決定するためのものである。

他の技法としては，関連図，樹木図，クラスタ分析，デルタ チャート(作業分解チャート)などあるが，いずれも図形表

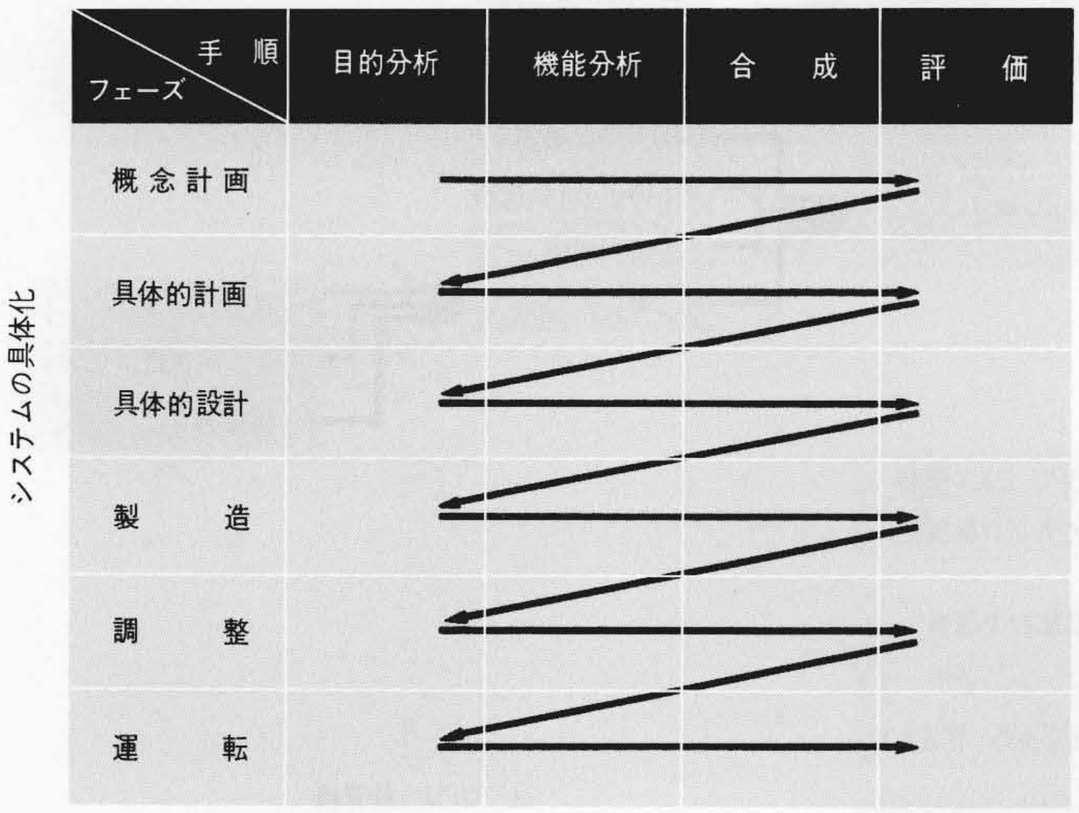


図1　システム開発のフェーズと手順　矢印の方向に段階的に作業が進められる。

表1　計算機システム評価設計項目　計算機の構成，ソフトウェアの構成を，未確定データから開発が進むにつれて確定させるためのシミュレータの一種である。

フェーズ	目　的	検討項目	検討結果
概念計画、具体的計画	1. 必要コア メモリ容量決定 2. 必要バルク メモリ容量決定 3. 大まかなオーバレイ決定 4. 大まかな応答時間算出	1. タスク数 2. 処理時間 3. 処理レベル 4. 起動周期 5. 起動方法 6. コア ブロック数* 7. 許容応答時間*	1. タスクの配置 2. 常駐，非常駐 3. 起動タイミング 4. 応答時間 (平均，最大，最小) 5. コア メモリ容量 6. タスク退避エリア
具体的設計、製造、調整	1. メモリ配置決定 2. 起動タイミングの決定 3. 応答時間の算出	注：*は入力しなくてもよい。	

* 日立製作所大みか工場　** 日立製作所システム開発研究所　工学博士

示によって，明確に目的や機能，あるいは作業の関連を示し，誤りなく効果的なシステムの完成を目指したものである。**図2**に，ダムの制御に対する関連図の一部を示す。

制御システムとして，特に重要な信頼性についての技法としては，部品あるいは機器レベルから故障モードを推定するFMEA(Failure Mode Effect Analysis)，FMECA(Failure Mode Effect Criticality Analysis)及び致命的な故障を出発点にしてそれが発生する原因を解析するFTA(Failure Tree Analysis)などがある。**図3**に交通制御システムの路上装置についてのFTAの一部分を掲げる。

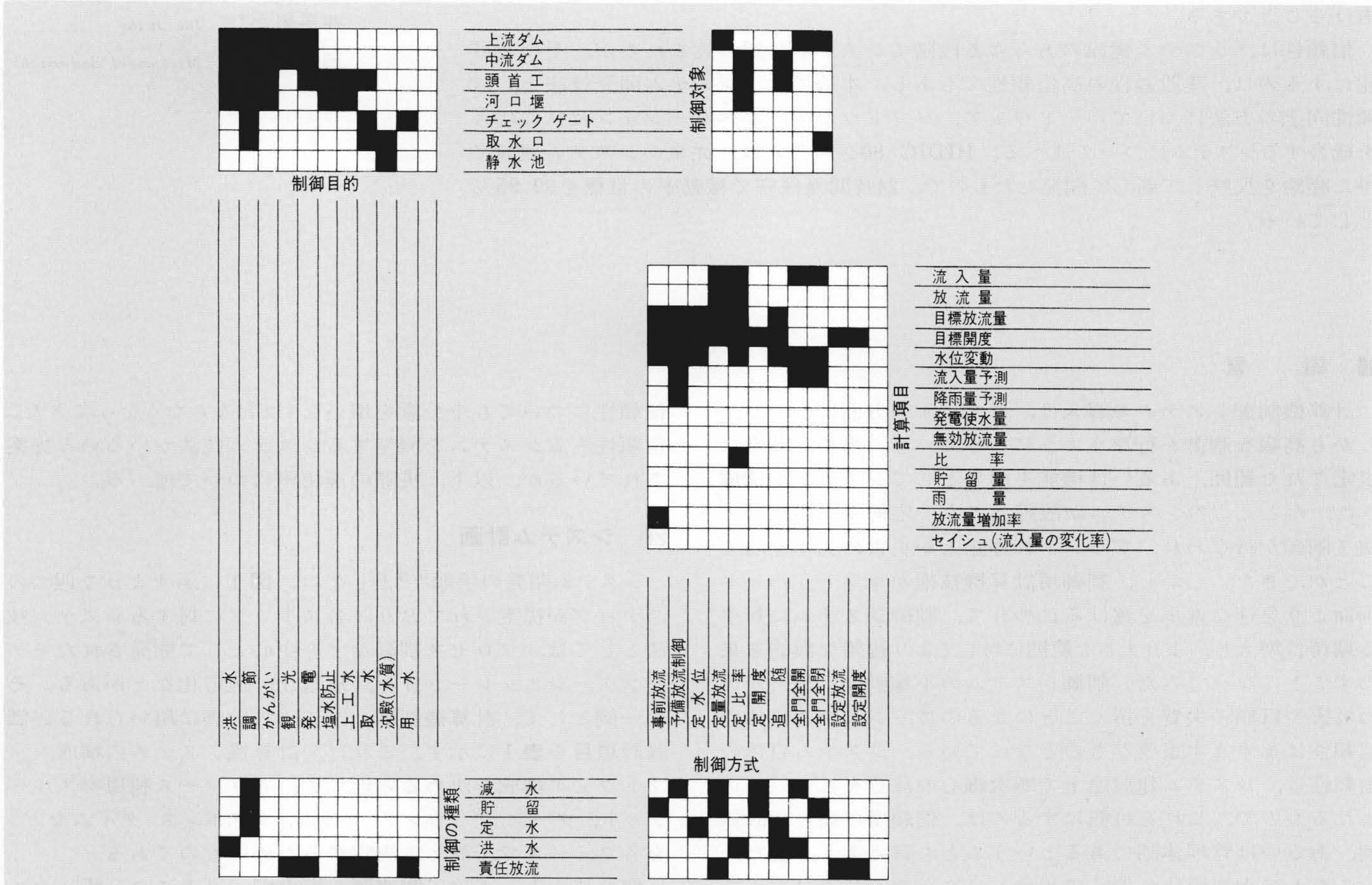


図2　ダム制御の関連図　　ダム制御の関連を示した図の一部である。

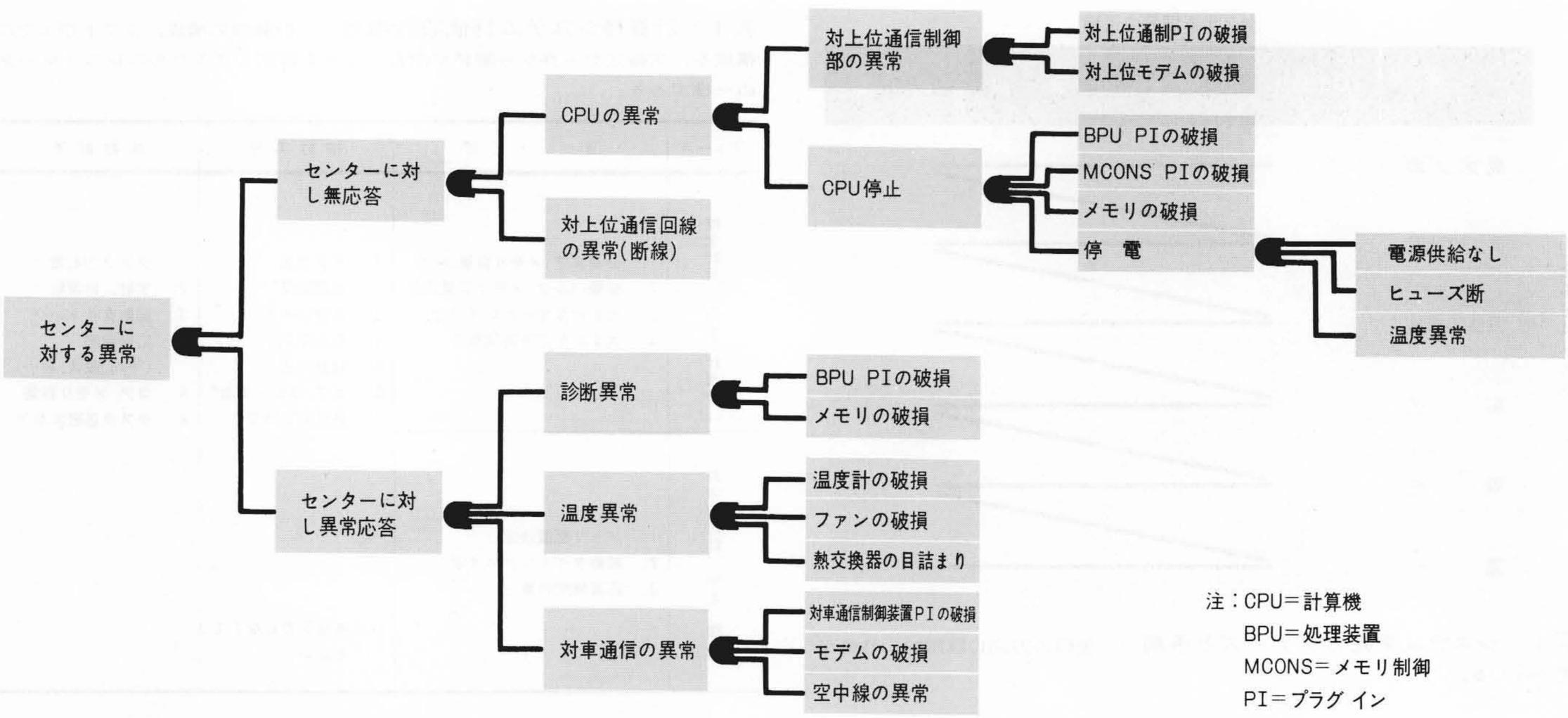


図3　交通制御システムに対するFTA(Failure Tree Analysis)の一例　　交通制御システムの路上器でのFTAの一部を示す。

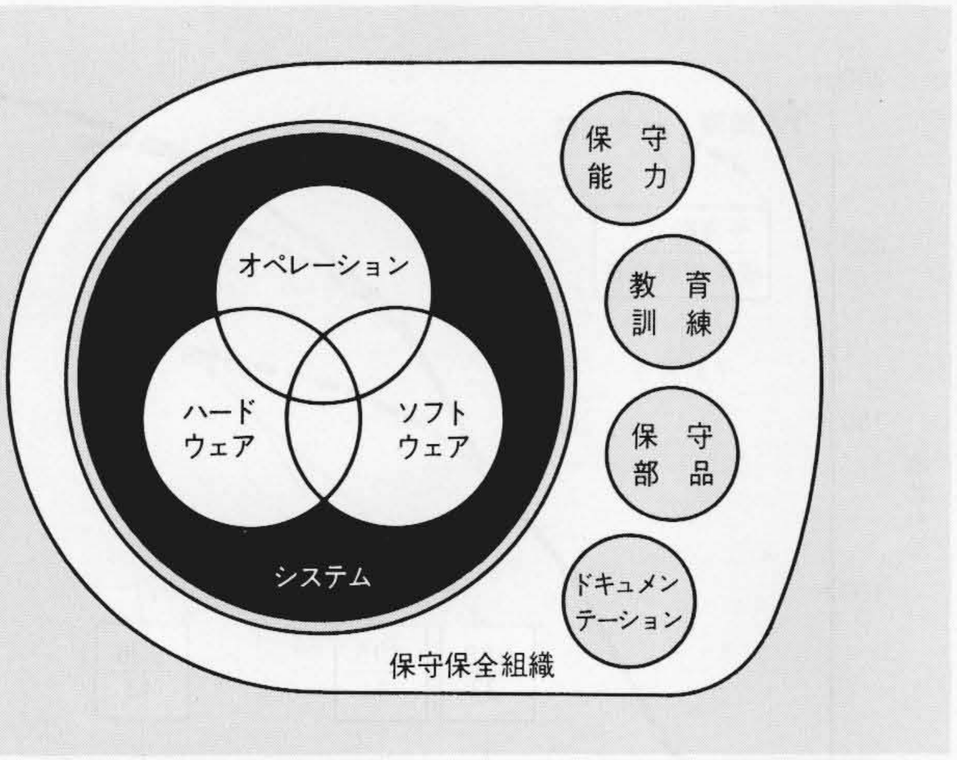


図4　システムの信頼性要素　システムの信頼性は上図のような要素の総合として決まる。

3　システムの信頼性

システムの信頼性は，**図4**に示すように三つの基本的構成要素から成るものと考えると，これらの要素を協調させあるいは補間して，より高い信頼性を得るシステム技術があり，同時にシステムの信頼性を長期間安定して支えるものとしてユーザー，メーカーの保守保全組織がある。

計算機制御システムの信頼性は，制御対象を安全に連続して操業することであり，一度，計算機システムがダウンした際には迅速に復旧できることにより表わされる。しかし，制御対象により，信頼性の重点の置き方が異なっており，計算機制御システムとしての信頼性向上策も異なってくる。

3.1　ソフトウェアに関する対策[4]

ソフトウェアの品質を完全にしておけば，ハードウェアのような劣化現象による故障はあり得ないが，複雑多岐にわたるプログラム ルートをすべてチェックすることはプロジェクト建設の限られた時間内ではなかなか困難である。したがって，プログラマが思考しやすい言語とデータをそろえること，効率よくプログラムをランさせ，バグ追求の手掛かりをできるだけ多く得ること，及びテスト データの着脱が容易にできる手段をもつことが結局はプログラム ミスを減少させることになる。すなわち，プログラミング言語と，プログラム デバッグ システムの高級化，充実が信頼性を高めることになる。またプログラムの標準化，再使用も重要である。

設計時，制御対称の分析調査が十分でなく，ソフトウェアが対応できぬ場合がある。すなわち，処理範囲を逸脱した場合，あるいは論理誤りに類するものである。これに対する有効な対応策は特にないのが現状で，このような場合少なくともシステムとしてフェイルセイフの状態にし，操作員に指示を求めるようにする。

3.2　ハードウェアに関する対策[5]

部品実装レベルに対する対策としては，

(1)　部品メーカーの品質管理レベルの監視，温度ショックなどのスクリーニングによる高信頼度部品の確保
(2)　高集積度部品の採用で部品の点数の減少
(3)　高密度実装によるコネクタの減少とコンパクト化
(4)　電力，電圧及び電流容量のディレーティング使用
(5)　電圧，温度，時間などの動作余裕の確保
(6)　論理カードの樹脂コーティングによる耐環境性の強化
(7)　高温長時間バーン インに基づくエージングによる初期不良の除外
(8)　タイプライタなどの機構部品に対する適切な予防保守などが適用されている。

内部から発生するノイズによる誤動作は，原因がなかなか判明せずやっかいなものである。アース方式，インピーダンス マッチング，スパイクの除去，信号ループ面積の極小化などの対策を採る。

環境によるストレスもハードウェアに敏感に影響する。計算機室は比較的良好な環境下にあるが，操作室設置あるいは現場設置の機器については特に塵埃，振動，電気ノイズなど，解決困難な場合が多い。

3.3　オペレーションに関する対策

システムが複雑になると，操作員の介入なしで全自動化することは，ハードウェア，ソフトウェア上の制約があって困難である。オペレータがシステムの総合的判断を行ない，計算機制御システムは，判断データを提供し指示を受けて制御する。ここに人間のミスが入る余地がある。インタフェースが複雑になりすぎると，勘違いによるミスを起こし，また操作能力を超えてしまい制御対象の変化に対応できなくなる。このため，ソフトウェア，ハードウェアとのインタフェースはできるだけ単純化し，ミスの発生を防ぎ，ミスの発生に際しては，合理性チェックあるいはウォッチ ドック タイマによるチェックで，人間をチェックする。ソフトウェア，ハードウェアの信頼性が向上して事故の発生頻度が少なくなった段階で一たび事故が発生すると迅速に対応できなくなるので，一定の周期で教育訓練を行なうことが望ましい。

3.4　システムに関する対策[6]

以上述べたように，ソフトウェア，ハードウェア及びオペレーションでそれぞれ高信頼化の施策を行なうが，そこには

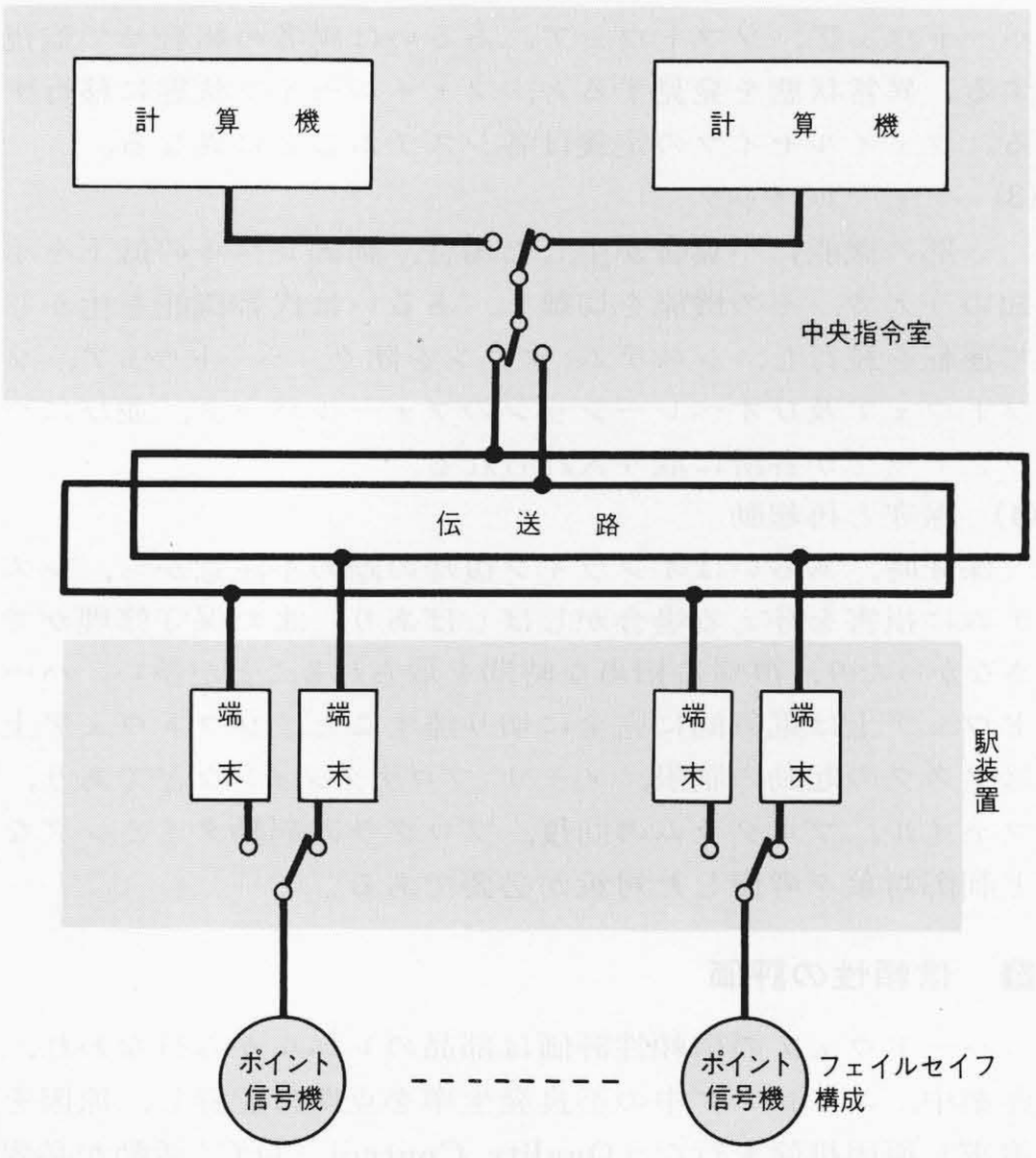
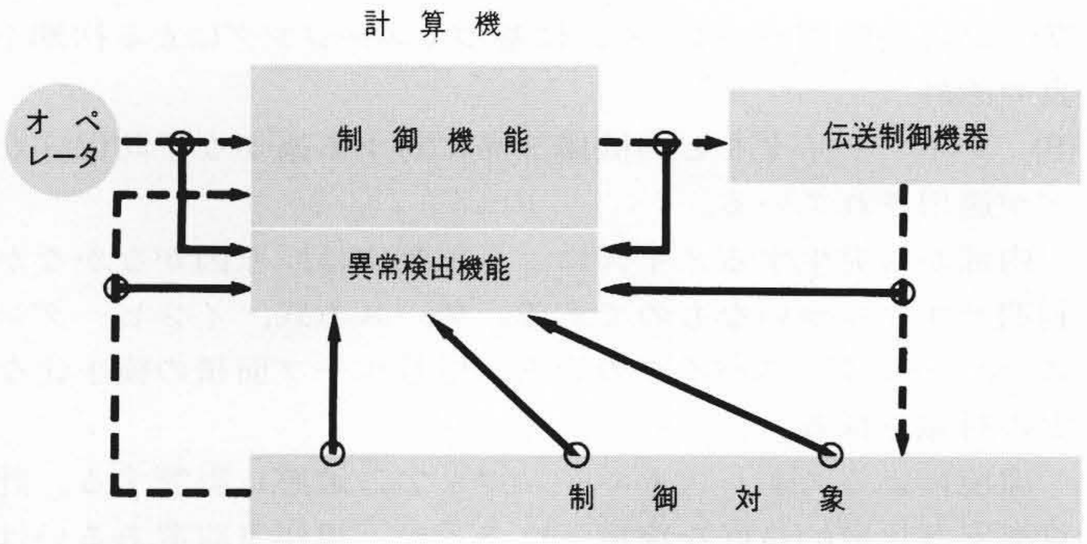


図5　二重化したシステム構成　一重系システム，階層システム，二重系システムなど，システムの重要性により，いろいろな構成をとるが，上図はシステムのすべてを二重化した鉄道システムの例である。



注：点線＝制御ルート
　　実線＝チェック ルート

図 6　異常検出ポイント　システムの異常検出は，上図のように制御ルートに従って幾重にも行なう。

限度がある。しかし，これらをすべて有機的に組み合わせて，より高信頼化することが可能である。また，システム特有の条件も折り込まれるのがシステム的高信頼技術である。

(1)　システム構成

システムの構成を階層化したり多重化して，システムの一部が故障した場合でも，システムの基本的な機能を失わずに制御を続行する方法を採る。**図 5** に示すシステム構成は，すべての部分を二重系にしたもので，このようなシステムでは，切換え時間，情報の連続，制御の連続，異常系の切離し，異常系の保守など，高度な利用技術とともにコア メモリの自動コピー，磁気ドラムの二重書き，通電時でのパッケージ着脱などの機能も電子計算機に要求されてくる。

(2)　異常検知とフェイルセイフ

システム レベルでの異常検知としては，**図 6** に示すように操作員，あるいは制御入力データ，計算機出力，制御装置出力のチェック，制御対象が異常な動作をしていないかのチェックなどであり，チェック点での合理性，あるいは応答性をハードウェア，ソフトウェア，あるいは両者の組合せで監視する。異常状態を発見すると，フェイルセイフ状態に移行する。フェイルセイフの定義は各システムごとに異なる。

(3)　フォールバック

一部の機能に不具合が生じた場合，制御レベルの低下を承知のうえで，その機能を切離し，あるいは代替機能を生かして運転を続行し，システム ダウンを防ぐ。ハードウェア，ソフトウェア及びオペレーションのフォールバック，並びにバックアップが各所に取り入れられる。

(4)　保守と再起動

保守時，あるいはオンライン復帰の際の不注意から，システムに損害を与える場合がしばしばあり，また保守修理ができなかったり，復帰に相当な時間を取られることが多い。ハードウェア上は電気的に完全に切り離すこと，ソフトウェア上はタスクの起動の制限，メモリ プロテクションなどであり，ファイル，プログラムの回復，プログラム起動タイミングなど制御対象を考慮した対策が必要である。

4　信頼性の評価

ハードウェアの信頼性評価は部品のレベルから行なわれ，作業中，エージング中の不良発生率を克明に記録し，原因を追求し原因排除を行なうQuality Control（ＱＣ）活動が必要である。ソフトウェアの評価は，ドキュメント検査及びバグ発生予測手法を用いて行なう。この予測は，ロジスティック，

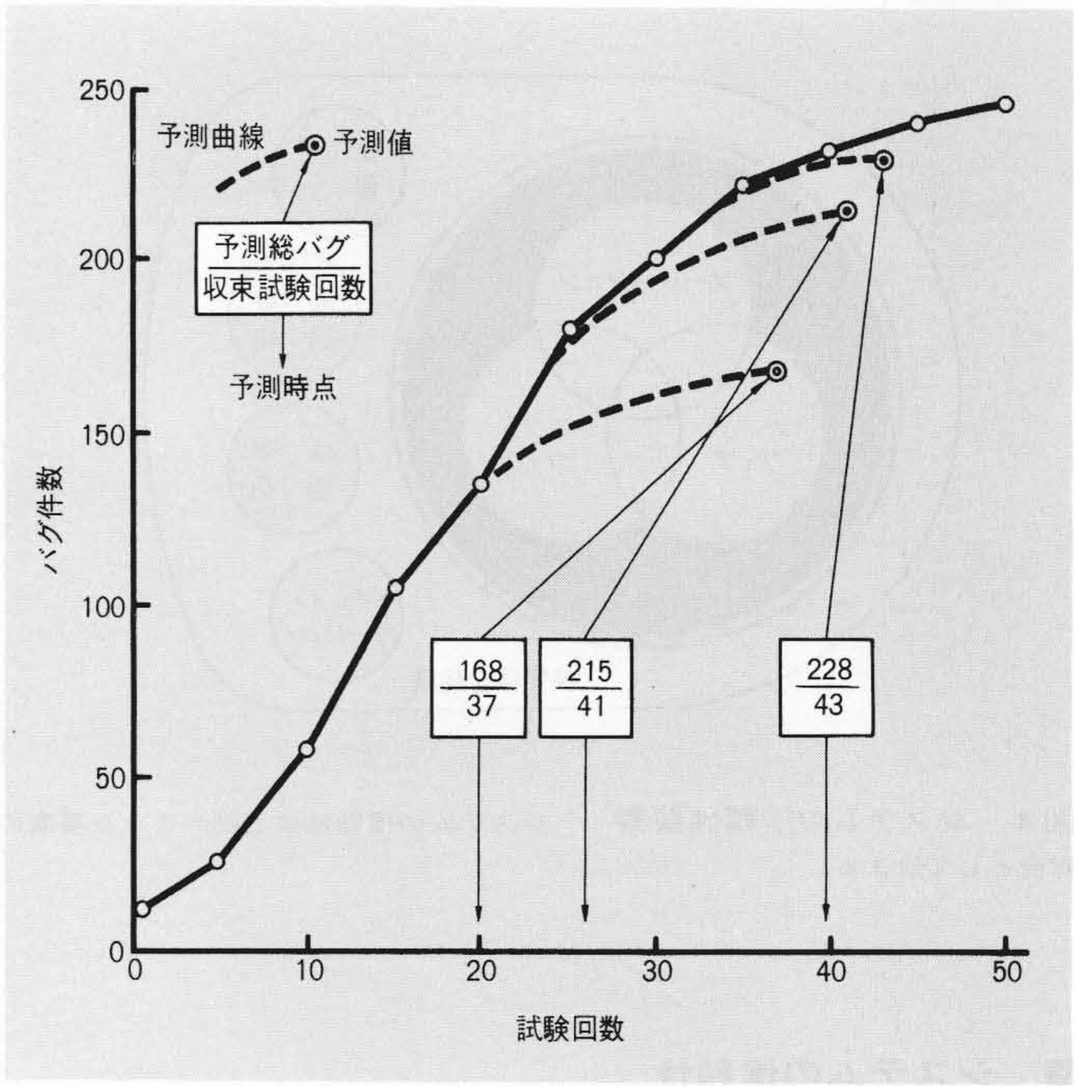


図 7　ロジスティック曲線予測例　新幹線運転管理システム（COMTRAC）の現地試験でのプログラム バグ発生予測を，ロジスティック関数で計算し実績と対比したものである。

ゴンペルツ，修正指数関数を用いて行なうもので，残存バグ数，デバッグ終了時期などの指針を与えるものである。**図 7** はロジスティック曲線によって予測した例を示したもので，終局に近づくほど予測が正確になる。

システムの信頼性は，どこまでシステム内外の異常事態に対応できるかにかかっているが，最後のとりでとしてはフェイルセイフ性にある。システムの余裕は，信頼性に大きな影響を与えるが，計算機内の負荷率の実測，プログラムの追跡が容易にできる機能が必要である。制御システムとしては無保守24時間運転で99.95%以上の稼動率を維持することが望まれる。

5　結　　言

我が国での計算機制御は歴史も既に10年以上を数えるに至り，ハードウェア，ソフトウェアの発展とともにますます広い分野に適用されている。アプリケーション特有の技術，あるいは計算機制御システム共通の技術も高度化深度化され，ハードウェア，ソフトウェアにフィードバックされている。HIDIC 80システムは，このような顧客ニーズを具現したものであり，ますます計算機制御の発展に寄与するものと思われる。

参考文献

1)　三浦：「システム計画」，電学誌，**92**，1104（昭47-11）
2)　A.D.Hall：IEEE Trans, G-SSC 5，2，156（1969）
3)　山本：「コンピュータシステムの評価」，bit，**5**，1208（昭48-11）
4)　Ogdin：Design of Reliable Software：Datamation July '72
5)　森田ほか：「計算機制御システムの信頼度向上策」，日立評論，**56**，375（昭49-4）
6)　喜田：「計算機システムの高信頼化手法」，信学誌**56**，58（昭48-1）