

氏 名	かの 鹿 股 昭 雄
授 与 学 位	工 学 博 士
学位授与年月日	昭和 60 年 1 月 9 日
学位授与の根拠法規	学位規則第 5 条第 2 項
最 終 学 歴	昭和 43 年 3 月 東北大学工学部電子工学科卒業
学位論文題目	マイクロコンピュータの高信頼化システム構成とその 信頼度評価に関する研究
論文審査委員	東北大学教授 樋口 龍雄 東北大学教授 重井 芳治 東北大学教授 高木 相 東北大学助教授 亀山 充隆

論 文 内 容 要 旨

第 1 章 緒 言

近年のマイクロコンピュータの利用は、通常の使用条件に比べ雑音などの厳しい環境で用いられる場合が多く、かつ、その故障が経済的にも人命の上からも極めて重大な影響を引き起こす分野に及んでいる。

このような厳しい環境中でマイクロコンピュータの高信頼化を計る手段として、間欠的な故障による内部状態の異常を自動的に回復する多重化冗長構成がこれまでに提案されている。しかし、実装の高密度化が進むにつれてその影響が問題となるモジュール間の同時故障相関に関しては、これまでほとんど検討されていない。また、これまでの研究の多くは、既存のマイクロプロセッサを多重化したものであり、内部状態の異常の検出やその回復処理が必ずしも迅速には行われておらず、故障の潜在によるシステムダウンの危険性が無視できない。このため、多重化されたモジュール間の同時故障への対策を考慮した上で、プロセッサ内部のアーキテクチャも含めた高信頼化システムの構成法を考察する必要がある。

本研究は、以上のような背景のもとに、多重化冗長システムの高信頼化を計るには、『瞬時回復性』と『耐同時故障性』の実現が特に重要であることに着目し、この 2 つの基本概念に基づいた統一した設計思想のもとに、一貫してシステムの構成や評価を行っている。その結果、故障の検出と回復をマイクロプログラムレベルで行い、かつ、インパルス性雑音に対する耐同時故障性を有する

マイクロコンピュータシステムの構成法を提案している。さらに、その信頼性を解析的に評価するとともに試作システムを用いて実験的にその効果を明らかにしている。

第2章 マイクロコンピュータの高信頼化に関する基礎的考察

本章では、マイクロコンピュータの高信頼化に関する基礎的な考察を行い、瞬時回復性と耐同時故障性を実現するには、マイクロコンピュータを3つの機能モジュール、すなわち、レジスタ・演算部、マイクロプログラム制御部、および主記憶部に分割し、各モジュールの特徴に応じ、レジスタ・演算部には3相クロック同期式3重化冗長を、後者2つには相補的論理・2重化冗長技法を適用することが優れていることを明らかにしている。

第3章 3相クロック同期式3重化冗長技法

本章では、レジスタ・演算部に適用した故障回復機能を有する3重化冗長構成とその信頼度評価について考察を行っている。

異常なレジスタを参照した時点で故障を検出し、直ちに多数決の結果を用いて1レジスタにつき1マイクロ命令で内部状態を回復できる瞬時回復性を備えた構成を提案している。図1にレジスタ・演算部とマイクロプログラム制御部の基本構成を示す。

次に、数学的なモデルに基づいて解析した結果、非冗長な構成に対する提案システムの信頼度の改善度は、3重化されたモジュール間の同時故障率に反比例すること、また、同時故障相関の少ない条件のもとでは、信頼度の改善度が故障の検出および回復に要する時間にはほぼ反比例することを明らかにしている。

従来提案されているマイクロプロセッサレベルでの冗長システムでは、メモリあるいはI/Oポートに異常なデータが出力されるまで検出が待たされ、その間故障が潜在するのに対して、提案する構成ではレジスタを参照するマイクロ命令の周期で検査が行われるため、大幅に信頼度を向上することができる。さらに、インパルス性雑音に対する耐同時故障性を実現するため3重化された各レジスタ・演算部に対して3相クロックパルスで同期をとる時間的な冗長方式を新たに提案している。

また、通常の冗長システムでは問題となる照合検査回路の故障率は、提案する3重化レジスタ・演算部の信頼度

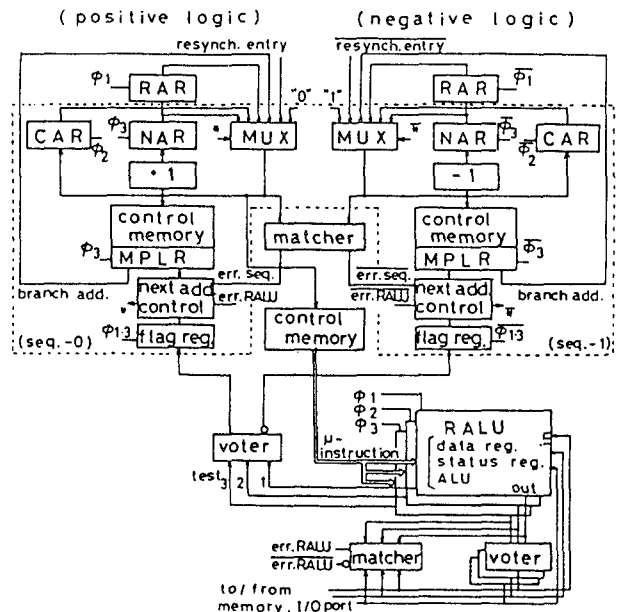


図1 マイクロプログラム制御部とレジスタ・演算部の構成

にほとんど影響を与えないことを明らかにしている。

第4章 相補的論理・2重化冗長技法

本章では、マイクロプログラム制御部と主記憶部に適用している故障回復機能を有する2重化冗長構成とその信頼度評価について考察を行っている。

マイクロプログラム制御部はコンピュータの制御の中心となる部分であることから、図1に示すように1個のバックアップレジスタ(CAR)を含む極めて単純なハードウェアに基づいた自己回復形の構成を提案している。マイクロプログラムのアドレスの異常を2重系の不一致で検出すると、直ちに1サイクル前のアドレスを用いて、1マイクロ命令でロールバックを行い、瞬時回復性を実現している。

数学的なモデルによる解析の結果、信頼度と安全度はともに2重系の照合検査では検出できない同時故障に大きく影響を受けることを明らかにしている。ここで、安全度は、少なくともそのシステムが暴走しない確率として定義される尺度である。

本研究では、正論理系と負論理系で並列に動作している半導体素子がインパルス性雑音によって異なる影響を受け易いことに着目し、同時故障相関の強い環境でも内部状態の異常を効率良く検出する手段として相補的論理・2重化冗長構成を提案している。この方式は、時間的冗長の効果が期待できないメモリ内のデータに対する同時故障対策としても有効と考え、主記憶部にも適用している。相補的論理・2重化冗長の効果は、6章で実験的に明らかにされている。

一方、主記憶部においては、読み出しサイクルごとに照合検査を行い、異常の場合には、誤り検出符号を用いて故障モジュールを特定し、レジスタ・演算部の多数決機能を利用して容易に回復できる構成を提案している。また、6章で行った故障実験で数多く観測された一方向性多重故障に対して、高い検出能力をもつ新たな変形剰余検査符号(MRCC-II)を提案している。

第5章 マイクロコンピュータの高信頼化システム構成

本章では、3章と4章で提案した冗長技法を機能モジュールごとに有機的に適用した高信頼化マイクロコンピュータシステムの構成法と各機能モジュール間の従属故障の影響について考察している。

まず、各機能モジュール間のインタフェースとファームウェアの構成を示し、自己回復形のマイクロプログラム制御部を中心とする階層的な構造のもとで、内部状態の異常を迅速に回復できることを明らかにして

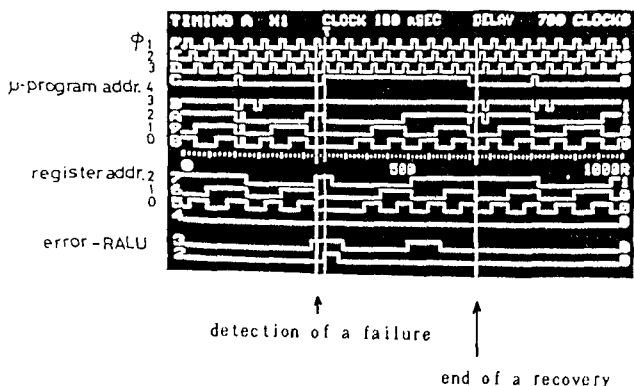


図2 3重化レジスタ・演算部の故障回復のシーケンス

いる。レジスタ・演算部の回復処理は、使用レジスタの個数と同じ数のマイクロ命令で、一方主記憶部の場合は8マイクロ命令で完了できることを示している。図2に8個のレジスタを使用したレジスタ・演算部の故障回復のシーケンスを示す。

次に、システム全体の高信頼化を計るには、瞬時回復性と耐同時故障性に加えて、機能モジュール間の『耐従属故障性』の実現が重要であることを数学的なモデルに基づいて示し、本研究で提案する機能モジュールごとの冗長システムがその性質をも十分に満たしていることを明らかにしている。

第6章 故障実験と信頼度・安全度評価

提案する冗長技法の効果を現実的な雑音環境のもとで定量的に評価するため、試作した機能モジュールの直流電源線に高電圧パルスを重畳させて故障実験を行った。図3は実験装置の外観を示す写真である。

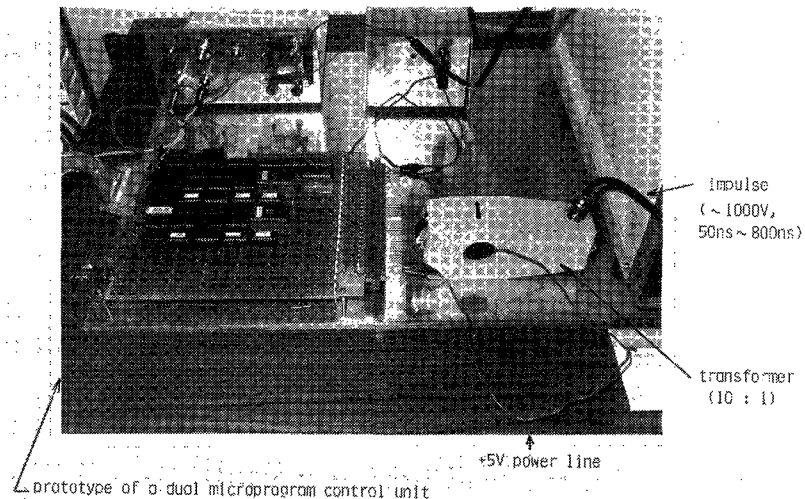


図3 電源雑音環境実験装置の外観

実験の結果は次の通りである。(1)3相クロック同期式は、通常の単相クロック同期式に比べて、同時故障を約1/4～1/10に軽減できた。(2)通常の2重系では、同時故障関連のため照合による故障検出率が30%～80%であったのに対して、相補的論理・2重化では100%検出できる実験結果を得た。(3)新たに提案した誤り検出符号(MRCC-II)の誤り検出率は0.9程度の高い値を示した。一方、パリティ検査符号や従来の変形剰余検査符号の検出率は、同じ環境でそれぞれ0.5、0.7程度であった。

さらに、各機能モジュールの信頼度、安全度を評価し、提案システムが高信頼度、高安全度を達成する上で優れていることを明らかにしている。

また、本章では、試作した冗長システムに論理的な縮退故障を擬似不規則信号に従って強制的に注入し、故障回復の動作や耐故障性の範囲の確認、および信頼度を実験的に求めることができる評

価システムを提案している。これを3重化レジスタ・演算部に適用し、解析的に求めた信頼度とほぼ一致することを示し、その有用性を明らかにしている。

第7章 結 言

以上、2章から6章にわたり『瞬時回復性』と『耐同時故障性』の実現がマイクロコンピュータの高信頼化を計る上で特に重要であることを明らかにし、この2つの基本概念に基づいた冗長技法を提案し、高信頼化システムの構成法について考察を行った。さらに、提案するシステムの信頼度、安全度を解析的に評価するとともに、試作した機能モジュールを用いて故障実験を行い、従来の冗長構成に比べて信頼度と安全度を大幅に向上できることを示した。なお、半導体素子の信頼性データは、ほとんど公表されておらず、測定の基準すら定まっていないのが現状であり、本故障実験は、本研究で対象としているような冗長システムに対する実験的評価法の一つの基準を与えるものと考えられる。

審査結果の要旨

最近マイクロコンピュータは、電磁環境が厳しく、その故障が重大な影響を及ぼす分野にも、使用されるようになってきた。それに伴い、冗長性を利用したフォールトトレラント技法の導入が要求されるようになり、特に同時故障相関の強い環境においても、高い信頼度を得る技法の開発が望まれていた。

著者は、マイクロコンピュータの高信頼化を達成する上で、間欠故障に対する、耐同時故障性と瞬時回復性を備えることが重要であることに着目し、新しい高信頼化システム構成法を提案し実現すると共に、信頼度評価を行い、その有用性を実証した。本論文はその成果をまとめたもので、全文7章よりなる。

第1章は緒言である。

第2章では、マイクロコンピュータの多重化冗長システムの基本モデルを与えて、その解析を行い、耐同時故障性と瞬時回復性の実現が、高信頼化を図る上で特に重要であることを明らかにしている。

第3章では、レジスタ・演算部に異常があるとき、マイクロ命令レベルで検出・回復が可能で、耐同時故障性にも優れている3相クロック同期方式を提案し、レジスタ・演算部の構成法を与えると共に、数学的モデルに基づく信頼度の解析、およびシミュレーションにより、本構成法の有効性を確かめている。

第4章では、同時故障相関の強い環境でも、マイクロプログラム制御部と、主記憶部の故障検出能力が十分有効に機能する、相補的論理に基づく新しい2重化冗長構成法を提案し、その信頼度を求めている。また、多重故障に対し、検出率の極めて高い誤り検出符号を考案している。これらは有用な成果である。

第5章では、前章までの成果に基づき、耐同時故障と瞬時回復性を備えた、マイクロコンピュータの高信頼化システム構成法を確立すると共に、システム全体の信頼度を検討することにより、本構成法がシステム構成上重要な、機能モジュール間の耐従属故障性の点でも、優れていることを確認している。

第6章では、被試験システムとしてのプロトタイプに雑音を印加し、その動作状態を監視・制御する信頼度評価システムを試作し、詳細に実験を行った結果、プロトタイプの信頼度が通常の冗長化方式に比べて、約1桁向上することを実証している。また、本評価システムを利用して、従来必ずしも明確にされていなかった、同時故障発生の機構を解明しているが、これは貴重な成果である。

第7章は結言である。

以上要するに本論文は、同時故障相関の強い環境における、マイクロコンピュータの新しい高信頼化システム構成と、その信頼度評価を与えると共に、高信頼化システム構成上基礎となる、多くの有用な知見を加えたもので、電子工学および情報工学の発展に寄与するところが少なくない。

よって、本論文は工学博士の学位論文として合格と認める。