

(19) 日本国特許庁(JP)

(12) 特 許 公 報(B2)

(11) 特許番号

特許第4613019号  
(P4613019)

(45) 発行日 平成23年1月12日(2011.1.12)

(24) 登録日 平成22年10月22日(2010.10.22)

|                   |              |                  |            |      |  |
|-------------------|--------------|------------------|------------|------|--|
| (51) Int.Cl.      |              | F I              |            |      |  |
| <b>G06F 11/30</b> | <b>11/30</b> | <b>(2006.01)</b> | G06F 11/30 | 305D |  |
| <b>G06F 11/16</b> | <b>11/16</b> | <b>(2006.01)</b> | G06F 11/30 | F    |  |
|                   |              |                  | G06F 11/30 | 310K |  |
|                   |              |                  | G06F 11/16 | 310C |  |

請求項の数 1 (全 9 頁)

|           |                               |           |                             |
|-----------|-------------------------------|-----------|-----------------------------|
| (21) 出願番号 | 特願2004-55735 (P2004-55735)    | (73) 特許権者 | 000006013                   |
| (22) 出願日  | 平成16年3月1日(2004.3.1)           |           | 三菱電機株式会社                    |
| (65) 公開番号 | 特開2005-250524 (P2005-250524A) |           | 東京都千代田区丸の内二丁目7番3号           |
| (43) 公開日  | 平成17年9月15日(2005.9.15)         | (74) 代理人  | 100094916                   |
| 審査請求日     | 平成18年10月13日(2006.10.13)       |           | 弁理士 村上 啓吾                   |
| 前置審査      |                               | (74) 代理人  | 100073759                   |
|           |                               |           | 弁理士 大岩 増雄                   |
|           |                               | (74) 代理人  | 100093562                   |
|           |                               |           | 弁理士 児玉 俊英                   |
|           |                               | (74) 代理人  | 100088199                   |
|           |                               |           | 弁理士 竹中 考生                   |
|           |                               | (72) 発明者  | 得田 和治                       |
|           |                               |           | 東京都千代田区丸の内二丁目2番3号 三菱電機株式会社内 |

最終頁に続く

(54) 【発明の名称】 コンピュータシステム

(57) 【特許請求の範囲】

【請求項1】

コンピュータとその動作を監視するウォッチドッグタイマ回路とを備え、かつ、上記ウォッチドッグタイマ回路から上記コンピュータに対してCPUリセット信号を出力した回数を記憶するWDT動作記憶部を設けるとともに、上記コンピュータは、起動時に上記WDT動作記憶部の内容を確認し、上記ウォッチドッグタイマ回路からCPUリセット信号が一度も出力されていない場合にはこのウォッチドッグタイマ回路に対してタイマリセット信号の供給を停止し、これに応じて上記ウォッチドッグタイマ回路からCPUリセット信号が出力されない場合には、当該ウォッチドッグタイマ回路に異常が生じているものと判断してCPUはその時点でプログラムの実行を停止する一方、上記ウォッチドッグタイマ回路に対するタイマリセット信号の供給停止に応じて当該ウォッチドッグタイマ回路からCPUリセット信号が出力された場合には、そのCPUリセット信号の出力回数を上記WDT動作記憶部に記憶するとともに、当該CPUリセット信号によってコンピュータがリセットされ、このリセット後にコンピュータが上記WDT動作記憶部の内容を確認した際に、上記ウォッチドッグタイマ回路からCPUリセット信号が一度でも出力されていると判断された場合には、上記ウォッチドッグタイマ回路およびコンピュータを含むシステムが健全なものとして、コンピュータは所定の制御プログラムの実行を開始するコンピュータシステムにおいて、上記コンピュータシステムが二重化されており、かつ、上記各コンピュータは、自己の診断完了を相手側に通知する通信手段と、この通信手段で通知された相手側の診断完了のタイミングと自己の診断完了のタイミングとを比較して両タイミング

の差が所定時間以内でない場合にはシステム異常と判断する判断手段と、を備えることを特徴とするコンピュータシステム。

【発明の詳細な説明】

【技術分野】

【0001】

本発明は、コンピュータとその動作を監視するウォッチドッグタイマ回路とを備えたコンピュータシステムに関するものである。

【背景技術】

【0002】

コンピュータシステムにおいては、コンピュータの制御プログラムの誤動作等によって例えば予め定められた時間内に処理が終了しないなどの異常が生じた場合には制御プログラムの実行を停止する必要がある。このため、従来より、コンピュータの動作を監視するウォッチドッグタイマ回路（以下、WDT回路と表記する）を設けている（例えば、特許文献1参照）。

【0003】

図5はこのような従来のコンピュータシステムの構成図である。

ここで、コンピュータ（本例ではマイクロコンピュータ）1は、制御プログラムが正常に実行されている場合には、予め設定されている所定の周期 $T_0$ でタイマリセット信号を出力してWDT回路2をリセットする。このため、WDT回路2からはコンピュータ1に対してCPUリセット信号が出力されない。

【0004】

一方、コンピュータ1は、制御プログラムの実行中に何らかの異常を検出すると、WDT回路2に対してタイマリセット信号の供給を停止する。WDT回路2は、このタイマリセット信号が所定の周期 $T_0$ で供給されなくなるとタイムアップして、コンピュータ1に対してCPUリセット信号を出力する。コンピュータ1はWDT回路2からのCPUリセット信号が入力されたときには、プログラムに割り込みを発生させてCPU内の各種レジスタやI/Oポートのデータをクリアして初期状態に戻す。なお、上記の所定周期 $T_0$ は、コンピュータ1の制御プログラムの異常検出のステップが所定回数繰り返されるのに要する時間以上の時間となるように予め定められている。

【0005】

【特許文献1】特許第2695775号公報

【発明の開示】

【発明が解決しようとする課題】

【0006】

ところで、例えば、鉄道車両用の自動列車制御装置や航空管制等などに使用されるコンピュータシステムにおいては、安全性確保の観点から、常にフェイルセーフが要求される。

【0007】

図5に示した従来のコンピュータシステムにおいては、コンピュータ1に対してWDT回路2を設けることでコンピュータの動作を監視できる利点があるものの、WDT回路2自身に異常が生じた場合にはこれに対処することができず、上記のフェイルセーフの要求に十分に応えることができない。

【0008】

すなわち、図5に示した従来構成のコンピュータシステムの場合には、システム起動時に既にWDT回路2が故障していてもコンピュータ1自体はそのことを認識することができず、制御プログラムを実行することができる。つまり、WDT回路2の異常が潜在化してしまう。このため、その後、コンピュータ1が制御プログラムを実行中に異常が生じたためにタイマリセット信号の出力を停止してもWDT回路2からはCPUリセット信号が出力されないため、コンピュータ1はリセットされずに異常動作をそのまま継続するなどの不具合を生じる。

10

20

30

40

50

## 【0009】

本発明は、上記の課題を解決するためになされたもので、WDT回路の潜在異常を早期にかつ確実に検出できるようにして、フェイルセーフの要求に十分に 대응することができるコンピュータシステムを提供することを目的とする。

## 【課題を解決するための手段】

## 【0010】

上記の目的を達成するために、コンピュータとその動作を監視するウォッチドッグタイマ回路とを備えたコンピュータシステムにおいて、次の構成を採用している。

## 【0011】

すなわち、本発明では、コンピュータとその動作を監視するウォッチドッグタイマ回路とを備え、かつ、上記ウォッチドッグタイマ回路から上記コンピュータに対してCPUリセット信号を出力した回数を記憶するWDT動作記憶部を設けるとともに、上記コンピュータは、起動時に上記WDT動作記憶部の内容を確認し、上記ウォッチドッグタイマ回路からCPUリセット信号が一度も出力されていない場合にはこのウォッチドッグタイマ回路に対してタイマリセット信号の供給を停止し、これに応じて上記ウォッチドッグタイマ回路からCPUリセット信号が出力されない場合には、当該ウォッチドッグタイマ回路に異常が生じているものと判断してCPUはその時点でプログラムの実行を停止する一方、上記ウォッチドッグタイマ回路に対するタイマリセット信号の供給停止に応じて当該ウォッチドッグタイマ回路からCPUリセット信号が出力された場合には、そのCPUリセット信号の出力回数を上記WDT動作記憶部に記憶するとともに、当該CPUリセット信号によってコンピュータがリセットされ、このリセット後にコンピュータが上記WDT動作記憶部の内容を確認した際に、上記ウォッチドッグタイマ回路からCPUリセット信号が一度も出力されていると判断された場合には、上記ウォッチドッグタイマ回路およびコンピュータを含むシステムが健全なものとして、コンピュータは所定の制御プログラムの実行を開始するコンピュータシステムにおいて、上記コンピュータシステムが二重化されており、かつ、上記各コンピュータは、自己の診断完了を相手側に通知する通信手段と、この通信手段で通知された相手側の診断完了のタイミングと自己の診断完了のタイミングとを比較して両タイミングの差が所定時間以内でない場合にはシステム異常と判断する判断手段と、を備えることを特徴としている。

## 【0012】

また、本発明では、上記のコンピュータシステムが二重化されている場合において、各コンピュータには、上記各コンピュータは自己の診断完了を相手側に通知する通信手段と、この通信手段で通知された相手側の診断完了のタイミングと自己の診断完了のタイミングとを比較して両タイミングの差が所定時間以内でない場合にはシステム異常と判断する判断手段とが設けられている。

## 【発明の効果】

## 【0013】

本発明のコンピュータシステムは、コンピュータがWDT動作記憶回路に記憶されている情報に基づいてWDT回路を診断し、WDT回路が健全であるとコンピュータがリセットされた後に制御プログラムの実行を開始するので、WDT回路の潜在異常の有無を早期に検出することができるとともに、フェイルセーフの要求に十分に 대응することができる。そして、制御プログラムの実行中はWDT回路が健全である可能性が高いことから、コンピュータが異常動作したときには、確実にコンピュータにリセットをかけることができるので、この点でもフェイルセーフの要求に十分に 대응することが可能となる。これに加えて、コンピュータシステムが二重化されている場合において、各WDT回路の異常の有無のみならず、コンピュータ相互間で診断完了のタイミングを比較することによってWDT動作記憶回路の異常の有無も検知することができ、これにより、異常検知の確率が高くなり、診断機能が失われるのを確実に防止でき、さらに一層コンピュータシステム全体の信頼性を向上させることができる。

## 【0014】

また、本発明では、上記のコンピュータシステムが二重化されている場合において、WDT回路の異常の有無のみならず、コンピュータ相互間でコンピュータの診断完了のタイミングを比較することによってWDT動作記憶回路の異常の有無も検知できるため、異常検知の確率が高くなる。このため、診断機能が失われるのを確実に防止でき、さらにコンピュータシステム全体の信頼性を向上させることができる。

【発明を実施するための最良の形態】

【0015】

実施の形態1.

図1は本発明の実施の形態1におけるコンピュータシステムの構成図であり、図5に示した従来技術と対応する構成部分には同一の符号を付す。

10

【0016】

この実施の形態1のコンピュータシステムは、マイクロコンピュータ(以下、単にコンピュータという)1と、その動作を監視するWDT回路2とを備えるとともに、WDT動作記憶部3が設けられている。

【0017】

このWDT動作記憶部3は、WDT回路2からコンピュータ1に対して出力されるCPUリセット信号の出力回数を記憶するもので、例えばカウンタやメモリ等が適用される。そして、このWDT動作記憶部3の記憶内容は、コンピュータシステムの電源が切られない限りそのまま保持されるようになっている。

20

【0018】

一方、コンピュータ1は、WDT動作記憶部3に対してアクセスできるようになっており、所定の制御プログラムの実行を開始する前にWDT動作記憶部3の内容を確認し、WDT回路2からCPUリセット信号が一度も出力されていない場合にはこのWDT回路2に対してタイマリセット信号の供給を停止して当該回路2の診断を行うように構成されている。

【0019】

次に、上記構成を備えたコンピュータシステムの動作について、図2に示すフローチャートを参照して説明する。なお、図中、符号Sは各ステップを意味する。

【0020】

このコンピュータシステムに電源が投入されると、コンピュータ1は、各種の初期設定をしながらWDT回路2に対して所定周期T0でタイマリセット信号を出力する(ステップ1)。コンピュータ1は、初期設定が終了すると、所定の制御プログラムの実行を開始する前にWDT動作記憶部3に対してアクセスしてその記憶内容を確認し(ステップ2)、WDT回路2に対する診断を実施したか否かを判断する(ステップ3)。

30

【0021】

すなわち、WDT動作記憶部3は、WDT回路2からCPUリセット信号が出力されるたびにその出力回数Nをカウントして記憶するので、いま、その出力回数N=0の場合、WDT回路2からはCPUリセット信号が一度も出力されていないことが分かる。そこで、この場合には、コンピュータ1は、WDT回路2が正常に動作するか否かを確認するために、WDT回路2に対してタイマリセット信号の供給を停止する(ステップ4)。

40

【0022】

その際、WDT回路2が故障などによる異常が生じている場合には、WDT回路2に対するタイマリセット信号の供給を停止しても、WDT回路2からはCPUリセット信号が出力されない。このため、コンピュータ1はその時点でプログラム処理動作を停止する。これにより、WDT回路2に異常があることが分かる。

【0023】

一方、WDT回路2が正常な場合、ステップ4でコンピュータ1からタイマリセット信号の供給が停止されるとタイムアップしてCPUリセット信号を出力する。これにより、コンピュータ1はこのCPUリセット信号によってリセットされて再びステップ1の最初の状態に戻り、初期設定処理から順に実施していくとともに、WDT動作記憶部3にはC

50

P Uリセット信号の出力回数  $N = 1$  が格納される。

【 0 0 2 4 】

引き続き、コンピュータ 1 は、W D T 動作記憶部 3 の記憶内容を確認し (ステップ 2 )、次に W D T 回路 2 の診断を実施したか否かを判断するが (ステップ 3 )、このとき、W D T 動作記憶部 3 の記憶内容は既に  $N = 1$  になっているので、診断実施済みであることが分かる。このため、この段階で初めてコンピュータ 1 は所定の制御プログラムの実行を開始する (ステップ 5 )。

【 0 0 2 5 】

なお、ステップ 5 以降のコンピュータ 1 の動作は、従来の場合と同様であって、制御プログラムが正常に実行されている場合には所定の周期  $T_0$  でタイマリセット信号を出力して W D T 回路 2 をリセットする。また、制御プログラムを実行中に異常が生じた場合、コンピュータ 1 はタイマリセット信号の出力を停止するので、W D T 回路 2 からは C P U リセット信号が出力されてコンピュータ 1 がリセットされる。

【 0 0 2 6 】

このように、この実施の形態 1 のコンピュータシステムにおいては、コンピュータ 1 が W D T 動作記憶回路 3 に記憶されている情報に基づいて W D T 回路 2 を診断した後に制御プログラムの実行を開始するので、W D T 回路 2 の潜在異常を早期に診断することができる。そして、制御プログラムの実行中は W D T 回路 2 が健全である可能性が高いことから、コンピュータ 1 が異常動作したときには、確実にコンピュータ 1 にリセットをかけることができる。このため、コンピュータ 1 の異常動作が継続するのを確実に防止でき、フェイルセーフの要求に十分に答えることが可能となる。

【 0 0 2 7 】

実施の形態 2 .

図 3 は本発明の実施の形態 2 におけるコンピュータシステムの構成図である。

【 0 0 2 8 】

この実施の形態 2 におけるコンピュータシステムは、図 1 と同じ構成をもつコンピュータシステムを 2 系列配置した、いわゆる二重化されたコンピュータシステムである。したがって、各系列 A , B のコンピュータシステムは、コンピュータ 1 a , 1 b と、その動作を監視する W D T 回路 2 a , 2 b と、W D T 動作記憶部 3 a , 3 b とを備えている。

【 0 0 2 9 】

そして、通常、各系列 A , B のコンピュータ 1 a , 1 b は互いに同期をとりながら並列動作しており、例えば、一方の系列 A のコンピュータシステムが故障したときには、他方の系列 B のコンピュータシステムがバックアップすることでフェイルセーフ動作を確保できるようにしている。

【 0 0 3 0 】

また、この実施の形態 2 において、各系列 A , B のコンピュータ 1 a , 1 b は、診断完了を相手側に通知する通信手段 5 a , 5 b と、通信手段 5 a , 5 b により通知された相手側の診断完了のタイミングと自己の診断完了のタイミングとを比較して両タイミングの差が所定時間  $T$  以内でない場合にはシステム異常と判断する判断手段 6 a , 6 b とを備えている。

【 0 0 3 1 】

次に、上記構成を備えたコンピュータシステムの動作について、図 4 に示すフローチャートを参照して説明する。なお、図中、符号 S は各ステップを意味する。

【 0 0 3 2 】

各系列 A , B のコンピュータシステムにおいて、電源が投入されてから、W D T 回路 2 a , 2 b の診断を一回実施して、診断実施済みと判断するまでの動作 (図 4 のステップ 1 ~ ステップ 4 ) は、実施の形態 1 の場合と同じである。したがって、ここでは詳しい説明は省略する。

【 0 0 3 3 】

前述のごとく、各系列 A , B のコンピュータ 1 a , 1 b は互いに同期をとりながら並列

10

20

30

40

50

動作しており、各系列 A , B のコンピュータ 1 a , 1 b の通信手段 5 a , 5 b は、自己の W D T 回路 2 a , 2 b の診断が完了すると、その診断完了の情報を相手側に通知する（ステップ 7）。すなわち、一方の系列 A のコンピュータ 1 a の通信手段 5 a は、自己の W D T 回路 2 a の診断が完了すると、その診断完了の情報を相手側の通信手段 5 b に通知する。同様に、他方の系列 B のコンピュータ 1 b の通信手段 5 b は、自己の W D T 回路 2 b の診断が完了すると、その診断完了の情報を相手側の通信手段 5 a に通知する。

【 0 0 3 4 】

したがって、各系列 A , B のコンピュータ 1 a , 1 b の判断手段 6 a , 6 b は、相手側と自己との両 W D T 回路 2 a , 2 b の診断完了のタイミングを比較する。そして、両タイミングの差が所定時間  $T$  以内に収まっているか否かを判断する（ステップ 8）。

10

【 0 0 3 5 】

ここで、例えば他方の系列 B における W D T 動作記憶部 3 b が故障するなどして、常に  $N = 1$  をコンピュータ 1 b に出力するような異常が生じた場合、その系列 B のコンピュータ 1 b は、実際は W D T 回路 2 b の診断が未実施であるにもかかわらず診断完了済みと誤判断するため、相手側のコンピュータ 1 a に対して診断完了の情報を出力しない。このため、相手側の W D T 回路 2 b の診断完了のタイミングと自己の W D T 回路 2 a の診断完了のタイミングとの差が所定時間  $T$  を越えることになる。これにより、コンピュータ 1 の判断手段 6 a は、システム全体に何らかの異常が発生しているものと判断して制御プログラムの実行を停止する（ステップ 9）。また、故障である旨を外部に報知する。このことは、一方の系列 A における W D T 動作記憶部 3 a が故障するなどの異常が生じた場合も同じである。

20

【 0 0 3 6 】

一方、両系列 A , B のコンピュータシステムが共に正常な場合には、ほぼ同じタイミングで W D T 回路 2 a , 2 b の診断が完了するので、両系列 A , B の診断終了のタイミングが所定時間  $T$  以内に収まることになる。この段階で初めて各コンピュータ 1 a , 1 b は所定の制御プログラムの実行を開始する（ステップ 10）。

【 0 0 3 7 】

なお、ステップ 10 以降のコンピュータ 1 a , 1 b の動作は、従来の場合と同様であって、各コンピュータ 1 a , 1 b は制御プログラムが正常に実行されている場合には所定の周期  $T_0$  でタイマリセット信号を出力して W D T 回路 2 a , 2 b をリセットする。また、制御プログラムを実行中に異常が生じた場合には、コンピュータ 1 a , 1 b はタイマリセット信号の出力を停止するので、W D T 回路 2 a , 2 b からは C P U リセット信号が出力されてコンピュータ 1 a , 1 b がリセットされる。

30

【 0 0 3 8 】

このように、この実施の形態 2 では、コンピュータシステムが二重化されている場合において、各 W D T 回路 2 a , 2 b の異常の有無のみならず、コンピュータ 1 a , 1 b 相互間で診断完了のタイミングを比較することによって W D T 動作記憶回路 3 a , 3 b の異常の有無も検知することができる。これにより、異常検知の確率が高くなり、診断機能が失われるのを確実に防止でき、さらにコンピュータシステム全体の信頼性を向上させることができる。

40

【 0 0 3 9 】

なお、本発明は、フェイルセーフが要求される分野のコンピュータシステムについて広く適用することが可能である。なお、この場合に使用されるコンピュータとしてはマイクロコンピュータに限らず、ミニコンピュータなどの他の種類のコンピュータであってもよい。

【 図面の簡単な説明 】

【 0 0 4 0 】

【 図 1 】 本発明の実施の形態 1 におけるコンピュータシステムの構成図である。

【 図 2 】 図 1 のコンピュータシステムにおける動作説明に供するフローチャートである。

【 図 3 】 本発明の実施の形態 2 におけるコンピュータシステムの構成図である。

50

【図4】図3のコンピュータシステムにおける動作説明に供するフローチャートである。

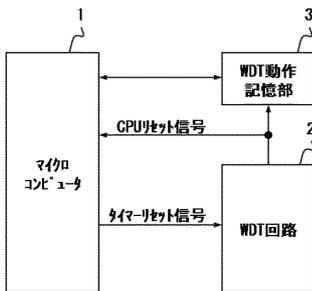
【図5】従来のコンピュータシステムの構成図である。

【符号の説明】

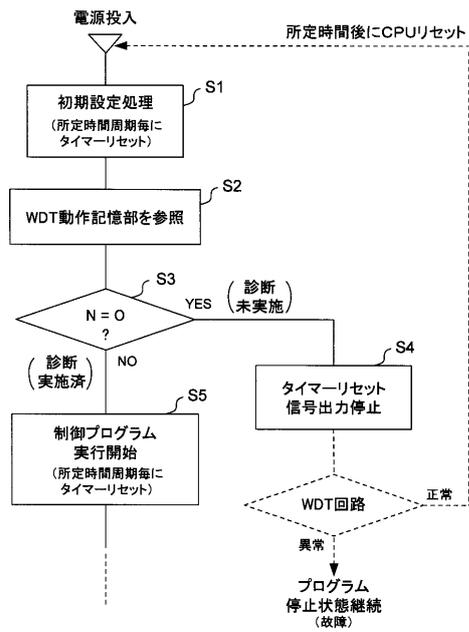
【0041】

- 1, 1a, 1b マイクロコンピュータ(コンピュータ)、
- 2, 2a, 2b WDT回路(ウォッチドッグタイマ回路)、
- 3, 3a, 3b WDT動作記憶部、5a, 5b 通信手段、6a, 6b 判断手段。

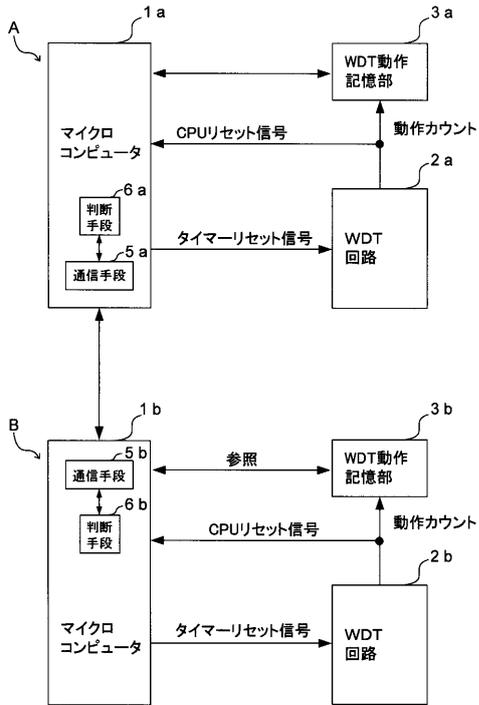
【図1】



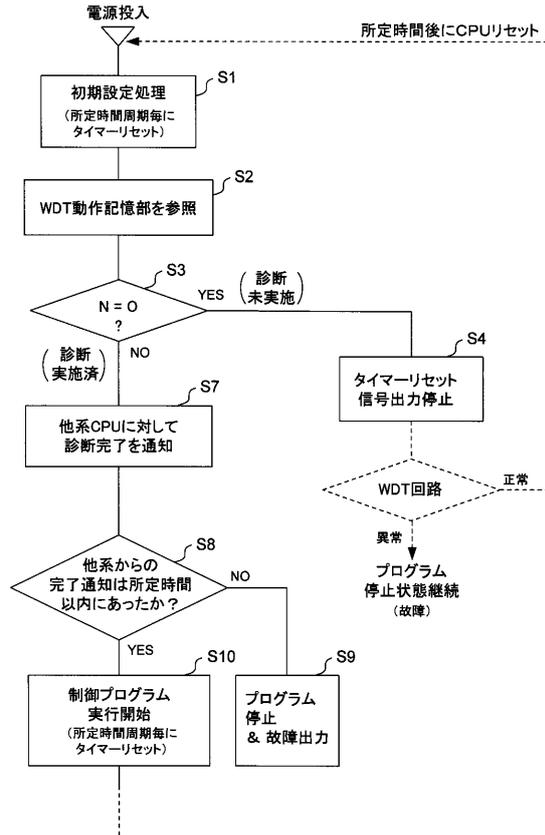
【図2】



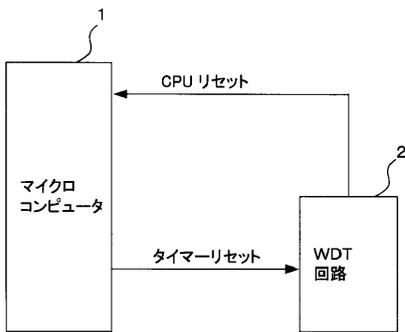
【図3】



【図4】



【図5】



---

フロントページの続き

(72)発明者 伊藤 努

東京都千代田区九段北一丁目13番5号 三菱電機エンジニアリング株式会社内

審査官 坂庭 剛史

(56)参考文献 特開平09-311797(JP,A)

特開昭61-023202(JP,A)

特開平10-171501(JP,A)

特開昭54-056740(JP,A)

実開平06-081039(JP,U)

特開平08-263455(JP,A)

特開平02-306362(JP,A)

(58)調査した分野(Int.Cl., DB名)

G06F 11/30

G06F 11/16