

(19) 日本国特許庁(JP)

(12) 特 許 公 報(B2)

(11) 特許番号

特許第4433006号
(P4433006)

(45) 発行日 平成22年3月17日(2010.3.17)

(24) 登録日 平成22年1月8日(2010.1.8)

(51) Int. Cl. F I
G06F 11/30 (2006.01) G06F 11/30 F
 G06F 11/30 305H

請求項の数 6 (全 19 頁)

(21) 出願番号	特願2007-176544 (P2007-176544)	(73) 特許権者	000004260 株式会社デンソー
(22) 出願日	平成19年7月4日(2007.7.4)		愛知県刈谷市昭和町1丁目1番地
(65) 公開番号	特開2009-15590 (P2009-15590A)	(74) 代理人	100106149 弁理士 矢作 和行
(43) 公開日	平成21年1月22日(2009.1.22)	(74) 代理人	100121991 弁理士 野々部 泰平
審査請求日	平成21年1月8日(2009.1.8)	(72) 発明者	柴田 健志 愛知県刈谷市昭和町1丁目1番地 株式会 社デンソー内
		(72) 発明者	井原 博之 愛知県刈谷市昭和町1丁目1番地 株式会 社デンソー内
		審査官	多胡 滋

最終頁に続く

(54) 【発明の名称】 マルチコアの異常監視装置

(57) 【特許請求の範囲】

【請求項1】

複数のプロセッサコア及びこれら複数のプロセッサコア間を接続する第1通信路が1つのパッケージに集積され、

前記複数のプロセッサコアは、演算処理部と、主にこの演算処理部によって使用される一時記憶部と、前記演算処理部が前記一時記憶部にアクセス可能にこれら演算処理部及び一時記憶部を接続する第2通信路とをそれぞれ所有し、

前記複数のプロセッサコアのうちの少なくとも2つのプロセッサコアは、自身以外のプロセッサコアの動作状態を監視する監視側コア、及び、この監視側コアによって動作状態が監視される被監視側コアに割り当てられ、

前記被監視側コアは、当該被監視側コア所有の一時記憶部に対し、当該被監視用コア所有の前記第2通信路を介してアクセスして、所定時間毎に第1書込操作を実行し、

前記監視側コアは、前記被監視側コアによる第1書込操作の結果を前記第1通信路を介して監視しつつ、当該監視側コア所有の一時記憶部に対し、当該監視側コア所有の前記第2通信路を介してアクセスして、前記第1書込操作の結果に対応する第2書込操作を前記所定時間毎に実行するとともに、当該監視側コア所有の一時記憶部に書き込まれたこの第2書込操作の結果に基づく所定の判定条件が成立するとき、前記被監視側コアの動作状態が異常である旨を判定するマルチコアの異常監視装置であって、

前記監視側コアは、アドレス情報記憶部及びアクセス判定部を有する第1保護手段を、前記第1通信路と当該監視側コア所有の一時記憶部との接続部に所有しており、

10

20

前記第1保護手段の前記アドレス情報記憶部には、当該監視側コアの演算処理部によって設定された前記監視側コア所有の一時記憶部のアドレス情報及びこのアドレスへのアクセス禁止態様があらかじめ記憶され、

前記第1保護手段の前記アクセス判定部は、前記監視側コア以外のプロセッサコアが前記第1通信路を介してアクセスしようとするアドレス及びそのアクセス態様が、前記第1保護手段の前記アドレス情報記憶部に記憶されたアドレス情報及びアクセス禁止態様に、それぞれ一致するか否かを判定し、

前記第1保護手段は、当該第1保護手段の前記アクセス判定部によって一致する旨が判定されるとき、前記監視側コア以外のプロセッサコアが前記第1通信路を介して前記監視側コア所有の一時記憶部へアクセスすることを遮断することを特徴とする、マルチコアの異常監視装置。

10

【請求項2】

前記被監視側コアは、アドレス情報記憶部及びアクセス判定部を有する第2保護手段を、当該被監視側コア所有の演算処理部と前記第1通信路との接続部に所有しており、

前記第2保護手段の前記アドレス情報記憶部には、当該被監視側コアの演算処理部によって設定された前記監視側コア所有の一時記憶部のアドレス情報及びこのアドレスへのアクセス禁止態様があらかじめ記憶され、

前記第2保護手段の前記アクセス判定部は、当該被監視側コアが前記第1通信路を介してアクセスしようとするアドレス及びそのアクセス態様が、前記第2保護手段の前記アドレス情報記憶部に記憶されたアドレス情報及びアクセス禁止態様に、それぞれ一致するか否かを判定し、

20

前記第2保護手段は、当該第2保護手段の前記アクセス判定部によって一致する旨が判定されるとき、前記被監視側コアが前記第1通信路を介して前記監視側コア所有の一時記憶部へアクセスすることを遮断することを特徴とする、請求項1に記載のマルチコアの異常監視装置。

【請求項3】

前記第1保護手段は、動作時に、前記監視側コア所有の一時記憶部にアクセスしようとした、前記監視側コア以外のプロセッサコアの動作状態にかかる情報を前記監視側コアに通知する通知手段をさらに備え、

前記監視側コアは、前記通知手段によって通知された前記情報に基づいて前記監視側コア以外のプロセッサコアの動作状態の異常の程度を判断し、前記被監視側コアの復帰処理をこの異常の程度に応じて実行することを特徴とする、請求項1または2に記載のマルチコアの異常監視装置。

30

【請求項4】

前記第1書込操作は、前記被監視側コアが、前記被監視側コア所有の一時記憶部に対し、所定値及びこの所定値の反転値を所定時間毎に交互に書き込む操作である、請求項1～3のいずれか一項に記載のマルチコアの異常監視装置。

【請求項5】

前記第2書込操作は、前記監視側コアが、前記監視側コア所有の一時記憶部に対し、前記第1書込操作が連続して正しく実行されない回数を書き込む操作である、請求項1～4のいずれか一項に記載のマルチコアの異常監視装置。

40

【請求項6】

当該マルチコアの異常監視装置は、制御対象を制御するための最終制御値を算出する制御装置に適用され、

前記監視側コアは、前記制御対象が有する各種センサのセンサ出力値に基づき、前記制御対象の制御を持続可能とする基本制御値を算出する基本制御値算出処理と、所定のデフォルト値に基づいて、前記基本制御値算出処理を通じて算出された基本制御値を最終制御値に補正する第1補正処理とを実行し、

前記被監視側コアは、前記センサ出力値に基づいて、前記基本制御値算出処理を通じて算出された基本制御値を最終制御値に補正する第2補正処理を実行し、

50

当該装置は、前記被監視側コアの動作状態が正常である旨判定されるとき、前記第2補正処理を通じて補正された最終制御値に基づき前記制御対象を制御し、前記被監視側コアの動作状態が異常である旨判定されるとき、フェイルセーフとして、前記第1補正処理を通じて補正された最終制御値に基づき前記制御対象を制御することを特徴とする、請求項1～5のいずれか一項に記載のマルチコアの異常監視装置。

【発明の詳細な説明】

【技術分野】

【0001】

この発明は、複数のプロセッサコアが1つのパッケージに集積されたマルチコアの異常監視装置に関する。

10

【背景技術】

【0002】

一般に、マイクロプロセッサ(CPU)は、命令発行器や演算器等が組み合わされて1つの部品として動作するプロセッサコアを、1つのパッケージに1つのみ有している。そして、そうしたCPUを複数用いるマルチプロセッサ構成のECUを用い、例えば自動車等の各種制御が実行されている。こうしたマルチプロセッサ構成のECUでは、該ECUを構成する複数のCPUが、監視元(監視する側：以下、メイン側と記載)あるいは監視対象(監視される側：以下、サブ側と記載)に割り当てられており、メイン側CPUはサブ側CPUの動作状態を監視している。

【0003】

20

詳しくは、例えば、サブ側CPUは、所定のポート出力値を所定時間毎に反転し、メイン側CPUは、所定のポート出力値をモニタする。ここで、所定のポート出力値が反転しなかったり異なる値になったりすることが連続して所定回数生じると、メイン側CPUは、サブ側CPUの動作状態が異常であると判断する。サブ側CPUの動作状態が異常であると判断すると、メイン側CPUは、例えばサブ側CPUが算出した値を予め定められたデフォルト値に置換するなど、フェイルセーフを実行する。

【0004】

こうした一般的な技術を、複数のプロセッサコアを1つのパッケージに有するマルチコア構成のECUに対してそのまま適用しようとする、次のような課題が生じる。すなわち、マルチコア構成のECUでは、該ECUを構成する複数のプロセッサコア間で共有する例えばRAMやレジスタ等のリソース(資源)を1つのパッケージ内に備えており、各プロセッサコアはこの共有リソースにアクセスすることが可能である。そのため、サブ側コアの動作状態が異常であるとき、上記所定回数をカウントするためにメイン側コアが使用していた共有RAMの領域に、サブ側コアがアクセスしてしまい、その内容を書き換えてしまうことがある。このように共有RAMの内容が書き換えられると、共有RAMに記憶保持された内容に基づきサブ側コアの動作状態を判断しているため、メイン側コアはサブ側コアの動作状態を正確に判断することができなくなってしまう。ひいては、上記フェイルセーフを適切に実行することが難しくなってしまう。

30

【0005】

そこで従来、例えば特許文献1に記載の技術では、各プロセッサコアと共有RAMとの間に書き込み禁止領域指定手段を備え、この書き込み禁止領域指定手段を通じて、プロセッサコアが当該プロセッサコア専用の領域以外の領域に書き込もうとするとき、その書込を無効にしていた。

40

【特許文献1】特開平7-200503号公報

【発明の開示】

【発明が解決しようとする課題】

【0006】

上記従来技術では、共有RAMの各プロセッサコアが使用する領域をそれぞれ専用化することができるため、例えば上記サブ側コアの動作状態が異常であったとしても、上記メイン側コアが使用していた共有RAMのメイン側コアの専用領域に記憶保持されていた内

50

容を、サブ側コアが書き換えてしまうようなことは生じにくくなる。

【0007】

しかしながら、サブ側コアの異常動作状態がさらに深刻になると、例えば、サブ側コアは、上記書込禁止領域指定手段に記憶されている書込禁止領域を書き換えてしまい、上記メイン側コアが使用していた共有RAMのメイン側コアの専用領域を、書込禁止領域の指定から外してしまうことも考えられる。こうなると、メイン側コアの専用領域に記憶されていた内容がサブ側コアによって書き換えられてしまうことも起こり得る。そして、メイン側コアは、サブ側コアの動作状態を正確に判断することができなくなり、ひいては、上記フェイルセーフを適切に実行することがやはり難しくなってしまう。

【0008】

本発明は、こうした実情に鑑みてなされたものであって、その目的は、各コアの動作状態をより正確に判定することのできるマルチコアの異常監視装置を提供することにある。

【課題を解決するための手段】

【0009】

こうした目的を達成するため、請求項1に記載の発明では、複数のプロセッサコア及びこれら複数のプロセッサコア間を接続する第1通信路が1つのパッケージに集積され、前記複数のプロセッサコアは、演算処理部と、主にこの演算処理部によって使用される一時記憶部と、前記演算処理部が前記一時記憶部にアクセス可能にこれら演算処理部及び一時記憶部を接続する第2通信路とをそれぞれ所有し、前記複数のプロセッサコアのうち少なくとも2つのプロセッサコアは、自身以外のプロセッサコアの動作状態を監視する監視側コア、及び、この監視側コアによって動作状態が監視される被監視側コアに割り当てられ、前記被監視側コアは、当該被監視側コア所有の一時記憶部に対し、当該被監視用コア所有の前記第2通信路を介してアクセスして、所定時間毎に第1書込操作を実行し、前記監視側コアは、前記被監視側コアによる第1書込操作の結果を前記第1通信路を介して監視しつつ、当該監視側コア所有の一時記憶部に対し、当該監視側コア所有の前記第2通信路を介してアクセスして、前記第1書込操作の結果に対応する第2書込操作を前記所定時間毎に実行するとともに、当該監視側コア所有の一時記憶部に書き込まれたこの第2書込操作の結果に基づく所定の判定条件が成立するとき、前記被監視側コアの動作状態が異常である旨を判定するマルチコアの異常監視装置であって、前記監視側コアは、アドレス情報記憶部及びアクセス判定部を有する第1保護手段を、前記第1通信路と当該監視側コア所有の一時記憶部との接続部に所有しており、前記第1保護手段の前記アドレス情報記憶部には、当該監視側コアの演算処理部によって設定された前記監視側コア所有の一時記憶部のアドレス情報及びこのアドレスへのアクセス禁止態様があらかじめ記憶され、前記第1保護手段の前記アクセス判定部は、前記監視側コア以外のプロセッサコアが前記第1通信路を介してアクセスしようとするアドレス及びそのアクセス態様が、前記第1保護手段の前記アドレス情報記憶部に記憶されたアドレス情報及びアクセス禁止態様に、それぞれ一致するか否かを判定し、前記第1保護手段は、当該第1保護手段の前記アクセス判定部によって一致する旨が判定されるとき、前記監視側コア以外のプロセッサコアが前記第1通信路を介して前記監視側コア所有の一時記憶部へアクセスすることを遮断することとした。

【0010】

マルチコアの異常監視装置としてのこのような構成では、まず、被監視側コアは、被監視側コア所有の一時記憶部に第2通信路を介してアクセスし、所定時間毎に第1書込操作を実行する。一方、監視側コアは、そうした被監視側コアによる第1書込操作の結果を第1通信路を介して監視しつつ、監視側コア所有の一時記憶部に第2通信路を介してアクセスし、第1書込操作の結果に対応する第2書込操作を所定時間毎に実行する。そして、監視側コアは、この第2書込操作の結果に基づく所定の判定条件が成立するとき、被監視側コアの動作状態が異常である旨を判定する。

【0011】

ここで、例えば監視側コア以外のプロセッサコアの1つ(ここでは被監視側コア)の動

10

20

30

40

50

作状態が異常となり、被監視側コアが監視側コア所有の一時記憶部に異常アクセスして、第1書込操作を含む操作をこの一時記憶部に実行しようとすることがある。このとき、第1保護手段を構成するアクセス判定部は、被監視側コアが第1通信路を介してアクセスしようとするアドレス及びそのアクセス態様が、第1保護手段を構成するアドレス情報記憶部に記憶されたアドレス及びアクセス禁止態様に、それぞれ一致するか否かを判定する。ここで、被監視側コアが第1通信路を介してアクセスしようとするアドレスは、監視側コア所有の一時記憶部のアドレスであり、アドレス情報記憶部に記憶されたアドレスに一致する。また、そうしたアクセス態様は、第1書込操作を含む操作、すなわち書き込みアクセスであり、アドレス情報記憶部に記憶されたアクセス禁止態様は、通常、書き込みアクセスであるため、これらは一致する。したがって、第1保護手段を構成するアクセス判定部を通じて、一致する旨が判定され、被監視側コアによる監視側コア所有の一時記憶部への異常アクセスは第1保護手段によって遮断されることになる。そのため、監視側所有の一時記憶部に対し第1書込操作を含む操作が実行されることはなくなる。

10

【0012】

しかも、被監視側コアの異常動作状態が背景技術の欄に記載したほどに深刻になったところで、第1保護手段を構成するアドレス情報記憶部に上記アドレス情報及び上記アクセス態様を記憶するのは、深刻な異常動作状態にある被監視側コアの演算処理部ではなく、正常な動作状態にある監視側コアの演算処理部である。そのため、第1保護手段を構成するアドレス情報記憶部に記憶されるアドレスは、間違いなく、監視側コアが所有する一時記憶部のアドレスとなり、第1保護手段を構成するアドレス情報記憶部に記憶されるアクセス禁止態様は、間違いなく、書き込みアクセスとなる。そして、被監視側コアによる監視側コア所有の一時記憶部への異常アクセスは、第1保護手段を構成するアクセス判定部によって確実に遮断され、監視側コア所有の一時記憶部に記憶されているデータが書き換えられるようなことはなくなる。したがって、監視側コアは、上記判定条件を正確に判定することができ、被監視側コアの動作状態を正確に判断することができるようになる。そしてひいては、各コアの動作状態をより正確に判断することができるようになる。

20

【0013】

上記請求項1に記載の構成において、請求項2に記載の発明では、前記被監視側コアは、アドレス情報記憶部及びアクセス判定部を有する第2保護手段を、当該被監視側コア所有の演算処理部と前記第1通信路との接続部に所有しており、前記第2保護手段の前記アドレス情報記憶部には、当該被監視側コアの演算処理部によって設定された前記監視側コア所有の一時記憶部のアドレス情報及びこのアドレスへのアクセス禁止態様があらかじめ記憶され、前記第2保護手段の前記アクセス判定部は、当該被監視側コアが前記第1通信路を介してアクセスしようとするアドレス及びそのアクセス態様が、前記第2保護手段の前記アドレス情報記憶部に記憶されたアドレス情報及びアクセス禁止態様に、それぞれ一致するか否かを判定し、前記第2保護手段は、当該第2保護手段の前記アクセス判定部によって一致する旨が判定されるとき、前記被監視側コアが前記第1通信路を介して前記監視側コア所有の一時記憶部へアクセスすることを遮断することとした。

30

【0014】

ここで、例えば監視側コア以外のプロセッサコアの1つ(ここでは被監視側コア)の動作状態が異常となり、被監視側コアが監視側コア所有の一時記憶部に異常アクセスして、第1書込操作を含む操作をこの一時記憶部に実行しようとすることがある。このとき、第2保護手段を構成するアクセス判定部は、被監視側コアが第1通信路を介してアクセスしようとするアドレス及びそのアクセス態様が、第2保護手段を構成するアドレス情報記憶部に記憶されたアドレス及びアクセス禁止態様に、それぞれ一致するか否かを判定する。ここで、被監視側コアが第1通信路を介してアクセスしようとするアドレスは監視側コア所有の一時記憶部のアドレスであり、第2保護手段を構成するアドレス情報記憶部に記憶されたアドレスに一致する。また、そうしたアクセス態様は、第1書込操作を含む操作、すなわち書き込みであり、第2保護手段を構成するアドレス情報記憶部に記憶されたアクセス禁止態様は、通常、書き込みアクセスであるため、これらは一致する。したがって、

40

50

第2保護手段を構成するアクセス判定部を通じて、一致する旨が判定され、被監視側コアによる監視側コア所有の一時記憶部への異常アクセスは第2保護手段によって遮断される。そのため、監視側所有の一時記憶部に対し第1書込操作を含む操作が実行されることは抑制される。

【0015】

ただし、被監視側コアの異常動作状態が背景技術の欄に記載したほどに深刻になると、第2保護手段を構成するアドレス情報記憶部に上記アドレス情報及び上記アクセス態様を記憶するのは、深刻な異常動作状態にある被監視側コアの演算処理部であるため、第2保護手段を構成するアドレス情報記憶部に記憶されるアドレスは、間違いなく、監視側コアが所有する一時記憶部のアドレスであるとは言えなくなり、第2保護手段を構成するアドレス情報記憶部に記憶されるアクセス禁止態様も、間違いなく、書き込みアクセスであるとは言えなくなってしまう。そのため、被監視側コアによる監視側コア所有の一時記憶部への異常アクセスが、第2保護手段を構成するアクセス判定部によって遮断されることなく、監視側コア所有の一時記憶部に記憶されているデータが書き換えようとするこも起こり得る。

10

【0016】

しかしながら、上記請求項2に記載の構成は、上記請求項1に記載の構成と併用されることが前提である。そのため、第2保護手段にて遮断されなかった異常アクセスは、上記第1保護手段にて確実に遮断される。このように、上記第1及び第2保護手段を併用する上記請求項2に記載の構成によれば、監視側コア所有の一時記憶部の、被監視側コアによる異常アクセスに対する堅牢性が高められ、監視側コアは、上記判定条件をより正確に判定することができ、被監視側コアの動作状態をより正確に判断することができるようになる。

20

【0017】

こうした構成において、例えば請求項3に記載の発明のように、前記第1保護手段は、動作時に、前記監視側コア所有の一時記憶部にアクセスしようとした、前記監視側コア以外のプロセッサコアの動作状態にかかる情報を前記監視側コアに通知する通知手段をさらに備え、前記監視側コアは、前記通知手段によって通知された前記情報に基づいて前記監視側コア以外のプロセッサコアの動作状態の異常の程度を判断し、前記被監視側コアの復帰処理をこの異常の程度に応じて実行することとしてもよい。これにより、監視側コア以外のプロセッサコアの動作状態が異常であるか否かの2値的な判定に留まらず、その異常の程度を判断することができるため、各コアの動作状態をさらに正確に判断することができるようになる。

30

【0018】

また、こうした構成において、前記第1書込操作としては、例えば請求項4に記載の発明のように、前記被監視側コアが、前記被監視側コア所有の一時記憶部に対し、所定値及びこの所定値の反転値を所定時間毎に交互に書き込む操作を採用することとしてもよい。さらに、前記第2書込操作としては、例えば請求項5に記載の発明のように、前記監視側コアが、前記監視側コア所有の一時記憶部に対し、前記第1書込操作が連続して正しく実行されない回数を書き込む操作を採用することとしてもよい。このような簡素な構成によっても、各コアの動作状態が異常であるか否かを判定することができるようになる。

40

【0019】

上記請求項1～5のいずれかに記載の構成において、例えば請求項6に記載の発明のように、当該マルチコアの異常監視装置は、制御対象を制御するための最終制御値を算出する制御装置に適用され、前記監視側コアは、前記制御対象が有する各種センサのセンサ出力値に基づき、前記制御対象の制御を持続可能とする基本制御値を算出する基本制御値算出処理と、所定のデフォルト値に基づいて、前記基本制御値算出処理を通じて算出された基本制御値を最終制御値に補正する第1補正処理とを実行し、前記被監視側コアは、前記センサ出力値に基づいて、前記基本制御値算出処理を通じて算出された基本制御値を最終制御値に補正する第2補正処理を実行し、当該装置は、前記被監視側コアの動作状態が正

50

常である旨判定されるとき、前記第2補正処理を通じて補正された最終制御値に基づき前記制御対象を制御し、前記被監視側コアの動作状態が異常である旨判定されるとき、フェイルセーフとして、前記第1補正処理を通じて補正された最終制御値に基づき前記制御対象を制御することが望ましい。

【発明を実施するための最良の形態】

【0020】

(第1の実施の形態)

以下、本発明に係るマルチコアの異常監視装置の第1の実施の形態について、図1～図6を参照して説明する。なお、図1及び図6は、本実施の形態の構成例及び動作例をそれぞれ示す模式図であり、図2及び図3は、本実施の形態で実行される異常監視判断処理及び被監視用処理について、その処理手順をそれぞれ示すフローチャートである。また、図4及び図5は、本実施の形態で実行される出口保護手段及び入口保護手段の初期設定処理について、その処理手順をそれぞれ示すフローチャートである。

10

【0021】

これら図1～図6に示されるように、また、以下に詳述するように、本実施の形態のマルチコアの異常監視装置は、例えば2つのプロセッサコア及びこれらプロセッサ間を接続する第1通信路が1つのパッケージに集積された、いわゆるデュアルコアによって構成されており、例えば自動車の燃焼室に燃料を噴射供給する燃料噴射制御装置に適用されている。

【0022】

20

はじめに、図1を参照して、本実施の形態の構成について説明する。同図1に示すように、デュアルコアの異常監視装置1は、基本的に、被監視側コア10bの動作状態を監視する監視側コア10aと、該監視側コア10aによってその動作状態が監視される被監視側コア10bと、これら両コア10a及び10bが後述する各種処理及び各種制御を実行するために必要な情報を送受信可能に接続する第1通信路(例えばバス等)60とをパッケージ100に備えている。なお、本実施の形態では、パッケージ100はプロセッサコアを2つ有しており、説明の便宜上、図1の左方に位置するプロセッサコアを監視側コアに、図1の右方に位置するプロセッサコアを被監視側コアにそれぞれ割り当てているが、これらプロセッサコアの役割を逆に割り当てることとしてもよく、互いに互いを監視するように役割を割り当てることとしてもよい。

30

【0023】

ここで、監視側コア10aは、基本的に、後述の異常監視判断処理を実行するCPU(演算処理部)20aと、このCPU20aによって主に使用されるRAM30aと、CPU20aがRAM30aにアクセス可能にこれらを接続する第2通信路70aとを所有している。同様に、被監視側コア10bも、基本的に、後述する被監視用処理を実行するCPU(演算処理部)20bと、このCPU20bによって主に使用されるRAM30bと、CPU20bがRAM30bにアクセス可能にこれらを接続する第2通信路70bとを所有している。

【0024】

RAM30aは、監視側コア10aによって所有され、主に使用されるものの、被監視側コア10bによっても第1通信路60を介することで使用される。同様に、RAM30bは、被監視側コア10bによって所有され、主に使用されているものの、監視側コア10aによっても第1通信路60を介することで使用される。

40

【0025】

ただし、監視側コア10a及び被監視側コア10bはそれぞれ、RAM30a及び30bの全領域を使用(書き込み及び読み込み)することができるわけではない。図1に示すように、RAM30aには、第2通信路70aを介して監視側コア10aのみが書き込み及び読み込みをすることができ、第1通信路60を介したところで被監視側コア10bは読み込みをすることさえできない、カウント用RAM領域31aが、プログラム(ソフトウェア)上、設定されている。同様に、図1に示すように、RAM30bには、第2通信

50

路 70b を介して被監視側コア 10b のみが書き込み及び読み込みをすることができ、第 1 通信路 60 を介したところで監視側コア 10a は読み込むことしかできない、被監視用 RAM 領域 31b が、プログラム (ソフトウェア) 上、設定されている。

【0026】

詳しくは、被監視用 RAM 領域 31b は、監視側コア 10a によって、以下のように使用される。

【0027】

図 2 に示すように、CPU 20b は、まず、ステップ S20 の処理として、被監視用 RAM 領域 31b に一時記憶されている値を第 2 通信路 70b を介して読み込み、続くステップ S22 の処理として、被監視用 RAM 領域 31b に読み込んだ値の反転値を第 2 通信路 70b を介して書き込む。こうした一連の処理 (ステップ S20 及び S22) を所定時間毎に実行する。なお、本実施の形態では、被監視用 RAM 領域 31b に一時記憶されている初期値として、例えば 16 進数「\$55」を採用している (したがって、その反転値は 16 進数「\$AA」となる)。そのため、CPU 20b の動作状態が正常であるとき、被監視用処理が正常に実行されるため、被監視用 RAM 領域 31b には、16 進数「\$55」及び「\$AA」が所定時間毎に反転して一時記憶されることとなる。ちなみに、CPU 20a は、後述するように、この被監視用 RAM 領域 31b に一時記憶されているデータを読み込み、この読み込んだデータに基づいて CPU 20b の動作状態の判断を実行する。

【0028】

また、カウント用 RAM 領域 31a は、監視側コア 10a (正確には CPU 20a) によって、以下のように使用される。

【0029】

図 3 に示すように、CPU 20a は、まず、ステップ S30 の処理として、被監視用 RAM 領域 31b に一時記憶されている値を第 1 通信路 60 を介して読み込み (モニタリング)、続くステップ S31 の判断処理として、読み込んだ値に異常があるか無いかを判断する。すなわち、CPU 20a は、読み込んだ値が上記所定値とその反転値との間で所定時間毎に反転されているか否かについて判断する。ここで、先のステップ S31 の判断処理において、読み込んだ値が上記所定値とその反転値との間で所定時間毎に反転されているとき (ステップ S31 の判断処理で「NO」)、CPU 20b による上記被監視用処理 (図 2) は正しく実行されていることを意味する。そのため、CPU 20a は、CPU 20b の動作状態は正常であると判断し、続くステップ S32 の処理として、カウント用 RAM 領域 31a に一時記憶されている異常回数カウント値を第 2 通信路 70a を介して零にクリアした上で、異常監視判断処理を一旦終了する。

【0030】

一方、先のステップ S31 の判断処理において、読み込んだ値が所定時間毎に反転されていないとき、あるいは、読み込んだ値が上記所定値及びその反転値以外の値になっているとき (ステップ S31 の判断処理で「Yes」)、CPU 20b による上記被監視用処理 (図 2) が正しく実行されていないことを意味する。そのため、CPU 20a は、CPU 20b の動作状態が異常である可能性が高いと判断し、続くステップ S33 の処理として、カウント用 RAM 領域 31a に一時記憶されている異常回数カウント値を第 2 通信路 70a を介してインクリメントする。

【0031】

そして、CPU 20a は、続くステップ S34 の判断処理として、異常回数カウント値が判定値に到達したか否かを判断する。ここで、異常回数カウント値が判定値に到達しないとき (ステップ S34 の判断処理において「NO」)、CPU 20b の動作状態が正常に復帰する可能性もあるため、CPU 20b の動作状態が異常である旨の判定をただちにすることなく、異常監視判定処理を一旦終了する。しかしながら、異常回数カウント値が判定値に到達するとき (ステップ S34 の判断処理において「YES」)、CPU 20b の動作状態が正常に復帰する可能性は極めて低いため、CPU 20b の動作状態が異常で

10

20

30

40

50

ある旨を判定し、続くステップS35の処理として、後述のフェイルセーフ処理を実行する。監視側コア10a(正確にはCPU20a)は、こうした一連の異常監視判断処理(ステップS30~S35)を所定時間毎に実行する。

【0032】

しかしながら、上記CPU20a及び20bの実行プログラムが、上記RAM30a及び30bを上述の態様をもって使用するようプログラムされていても、また、そうしたプログラムがたとえ正しいものであったとしても、実際には、例えばノイズに起因して、あるいは、被監視側であるCPU20bの動作状態が異常となると、CPU20bがカウント用RAM領域31aに第1通信路60を介してアクセスし、該カウント用RAM領域31aに一時記憶されているデータを書き換えてしまうことがある。このようにカウント用RAM領域31aに一時記憶されているデータが書き換えられてしまうと、CPU20aは、カウント用RAM領域31aに一時記憶されているデータに基づきCPU20bの動作状態を判断しているため、CPU20bの動作状態を正確に判断することができなくなってしまう。そして、ひいては、後述するフェイルセーフ処理(先のステップS35の処理)を適切に実行することが難しくなってしまう。

10

【0033】

そこで、本実施の形態では、先の図1に示すように、被監視側コア10bは、第1通信路60とCPU20bとの接続部、並びに、第2通信路70bとCPU20bとの接続部に、出口保護部(第2保護手段)40bを所有することとし、監視側コア10aは、第1通信路60とCPU20aとの接続部、並びに、第2通信路70aとCPU20aとの接続部に、出口保護部40aを所有することとした。すなわち、CPU20bは、出口保護部40bを介さなければ、RAM30a(特に、カウント用RAM領域31a)あるいはRAM30b(特に、被監視用RAM領域31b)にアクセスすることができず、同様に、CPU20aは、出口保護部40aを介さなければ、RAM30a(特に、カウント用RAM領域31a)あるいはRAM30b(特に、被監視用RAM領域31b)にアクセスすることはできない。このように、出口保護部40a及び40bを介在させることで、上述のようにCPU20bの動作状態が異常となっても、カウント用RAM領域31a及び被監視用RAM領域31bを、上記態様にて、CPU20a及び20bに使用させようとしている。

20

【0034】

以下、こうした出口保護部40a及び40bについて詳述する。先の図1に示されるように、出口保護部40aは、例えば小規模なマイコンによって構成され、アクセス判定部41a及びアドレス情報記憶部42aを有しており、同様に、出口保護部40bは、例えば小規模なマイコンによって構成され、アクセス判定部41b及びアドレス情報記憶部42bを有している。

30

【0035】

CPU20aは、先の図3に示した異常監視判断処理の実行前に、図4(a)に示す出口保護部40aの初期設定処理を実行する。CPU20aは、まず、ステップS40aの処理として、カウント用RAM領域31a及び被監視用RAM領域31bのアドレスをアドレス情報記憶部42aに記憶させる。CPU20aは、次に、ステップS42aの処理として、そうした記憶済みの各アドレスを対象に、「書き込みまで許可する」及び「読み込みのみ許可する」旨の設定をそれぞれ行う。同様に、CPU20bは、先の図2に示した被監視用処理の実行前に、図4(b)に示す出口保護部40bの初期設定処理を実行する。CPU20bは、まず、ステップS40bの処理として、カウント用RAM領域31a及び被監視用RAM領域31bのアドレスをアドレス情報記憶部42bに記憶させる。CPU20bは、次に、ステップS42bの処理として、そうした記憶済みの各アドレスを対象に、「一切のアクセスを禁止する」及び「書き込みまで許可する」旨の設定をそれぞれ行う。

40

【0036】

ここで、CPU20a及び20bによる、カウント用RAM領域31a及び被監視用R

50

A M領域 3 1 b への、上記アクセス禁止態様を採用する理由を説明する。

【 0 0 3 7 】

そもそも、C P U 2 0 b の動作状態について C P U 2 0 a が判断するにあたり、C P U 2 0 b がカウント用 R A M 領域 3 1 a を第 1 通信路 6 0 を介して読み込んだり書き込んだりする必要はない。また、C P U 2 0 b の動作状態について C P U 2 0 a が判断するにあたり、C P U 2 0 b は被監視用 R A M 領域 3 1 b に対して上記所定値及び上記反転値を書き込む必要がある。

【 0 0 3 8 】

そのため、C P U 2 0 b から出口保護部 4 0 b に対し、R A M 3 0 a あるいは 3 0 b へのアクセスが要求されると、まず、アクセス判定部 4 1 b は、要求先のアドレスが、(アドレス情報記憶部 4 2 b に一時記憶しておいた) 上記カウント用 R A M 領域 3 1 a あるいは被監視用 R A M 領域 3 1 b のアドレスに一致するか否かを判定する。ここで、要求先のアドレスが上記アドレスに一致しないとき、アクセス判定部 4 1 b は、C P U 2 0 b によるアクセス要求を許可する。

10

【 0 0 3 9 】

一方、要求先のアドレスが上記アドレスに一致するとき、アクセス判定部 4 1 b は、さらに、C P U 2 0 b によるアクセス要求が読み込み要求であるか書き込み要求であるかを判別する。そして、アクセス判定部 4 1 b は、C P U 2 0 b によるアクセス要求が、カウント用 R A M 領域 3 1 a の読み込み要求、あるいは、カウント用 R A M 領域 3 1 a への書き込み要求であるとき、これら一切を遮断することとしている。また、C P U 2 0 b によるアクセス要求が、被監視用 R A M 領域 3 1 b の読み込み要求、あるいは、被監視用 R A M 領域 3 1 b への書き込み要求であるとき、これらを受け入れることとしている。

20

【 0 0 4 0 】

このように、C P U 2 0 b は、カウント用 R A M 領域 3 1 a にアクセスして、一時記憶されているデータを読み込むことも、データを書き換えることもできなくなる。したがって、当該デュアルコアの異常監視装置 1 では、被監視側コア 1 0 b が出口保護部 4 0 b を所有するため、カウント用 R A M 領域 3 1 a に一時記憶されるデータは破壊されにくくなる。

【 0 0 4 1 】

一方、C P U 2 0 a は、C P U 2 0 b の動作状態について判断を行う目的で、被監視用 R A M 領域 3 1 b を読み込む必要がある。また、C P U 2 0 b の動作状態について C P U 2 0 a が判断するにあたり、C P U 2 0 a はカウント用 R A M 領域 3 1 a に異常回数カウント値を書き込む必要がある。

30

【 0 0 4 2 】

そのため、C P U 2 0 a から出口保護部 4 0 a に対し、R A M 3 0 a あるいは 3 0 b へのアクセスが要求されると、まず、アクセス判定部 4 1 a は、要求先のアドレスが、(アドレス情報記憶部 4 2 a に一時記憶しておいた) 上記カウント用 R A M 領域 3 1 a あるいは被監視用 R A M 領域 3 1 b のアドレスに一致するか否かを判定する。ここで、要求先のアドレスが上記アドレスに一致しないとき、アクセス判定部 4 1 a は、C P U 2 0 a によるアクセス要求を許可する。

40

【 0 0 4 3 】

一方、要求先のアドレスが上記アドレスに一致するとき、アクセス判定部 4 1 a は、さらに、C P U 2 0 a によるアクセス要求が読み込み要求であるか書き込み要求であるかを判別する。そして、アクセス判定部 4 1 a は、C P U 2 0 a によるアクセス要求が、カウント用 R A M 領域 3 1 a の読み込み要求、あるいは、カウント用 R A M 領域 3 1 a への書き込み要求であるとき、これらを受け入れることとしている。また、C P U 2 0 a によるアクセス要求が、被監視用 R A M 領域 3 1 b の読み込み要求であるとき、これらを受け入れることとしている。しかしながら、C P U 2 0 a によるアクセス要求が、被監視用 R A M 領域 3 1 b への書き込み要求であるとき、これを遮断することとしている。

【 0 0 4 4 】

50

このように、CPU 20 aは、被監視用RAM領域31 bにアクセスして、一時記憶されているデータを読み込むことはできるものの、データを書き換えることはできなくなる。したがって、当該デュアルコアの異常監視装置1では、監視側コア10 aが出口保護部40 aを所有するため、被監視用RAM領域31 bに一時記憶されるデータは破壊されにくくなる。

【0045】

ところで、先の図4(b)に示したように、また、既述したように、CPU 20 bは、カウント用RAM領域31 a及び被監視用RAM領域31 bのアドレスをアドレス情報記憶部42 bに記憶させるとともに、そうしたアドレスの各別に、「一切のアクセスを禁止する」及び「書き込みまで許可する」旨の設定をそれぞれ行っている。

10

【0046】

そのため、CPU 20 bの異常動作状態が深刻になると、例えばCPU 20 bが、出口保護部40 bの上記保護機能を解除してしまうことがある。具体的には、CPU 20 bが、出口保護部40 bの初期設定処理(図4(b)参照)において、カウント用RAM領域31 a及び被監視用RAM領域31 bのアドレスとは異なるアドレスをアドレス情報記憶部42 bに記憶させてしまったり、そうしたアドレスの各別に、上記アクセス許可態様とは異なる許可態様の設定を行ってしまったりすることがある。そして、CPU 20 bから出口保護部40 bに対し、そもそも出力されるはずのない、カウント用RAM領域31 aへの書き込み要求が出力されても(異常アクセス)、出口保護部40 bはそうした異常アクセスを遮断することができず、カウント用RAM領域31 aに一時記憶されていたデータがCPU 20 bによって書き換えられる、すなわち、破壊されてしまうことも起こり得る。そして、CPU 20 aは、CPU 20 bの動作状態を正確に判断することができなくなり、ひいては、後述のフェイルセーフ処理を適切に実行することが難しくなってしまう。

20

【0047】

そこで、本実施の形態では、先の図1に示すように、監視側コア10 aは、第1通信路60とRAM 30 aとの接続部に、入口保護部(第1保護手段)50 aを所有することとし、被監視側コア10 bは、第1通信路60とRAM 30 bとの接続部に、入口保護部50 bを所有することとした。すなわち、CPU 20 bは、出口保護部40 bのみならず、入口保護部50 aを介さなければ、RAM 30 a(特に、カウント用RAM領域31 a)にアクセスすることができず、同様に、CPU 20 aは、出口保護部40 aのみならず、入口保護部50 bを介さなければ、RAM 30 b(特に、被監視用RAM領域31 b)にアクセスすることはできない。このように、入口保護部50 a及び50 bを介在させることで、カウント用RAM領域31 a及び被監視用RAM領域31 bを、CPU 20 a及び20 bに、上記態様にて確実に使用させようとしている。

30

【0048】

以下、こうした入口保護部50 a及び50 bについて詳述する。先の図1に示されるように、入口保護部50 aは、例えば小規模なマイコンによって構成され、アクセス判定部51 a及びアドレス情報記憶部52 aを有しており、同様に、入口保護部50 bは、例えば小規模なマイコンによって構成され、アクセス判定部51 b及びアドレス情報記憶部52 bを有している。

40

【0049】

CPU 20 aは、先の図3に示した異常監視判断処理の実行前に、先の図4(a)に示した出口保護部40 aの初期設定処理に加え、図5(a)に示す入口保護部50 aの初期設定処理も実行する。CPU 20 aは、まず、ステップS50 aの処理として、カウント用RAM領域31 aのアドレスをアドレス情報記憶部52 aに記憶させる。CPU 20 aは、次に、ステップS52 aの処理として、そうした記憶済みアドレスを対象に、「一切のアクセスを禁止する」旨の設定を行う。同様に、CPU 20 bは、先の図2に示した被監視用処理の実行前に、先の図4(b)に示した出口保護部40 bの初期設定処理に加え、図5(b)に示す入口保護部50 bの初期設定処理を実行する。CPU 20 bは、まず

50

、ステップS50bの処理として、被監視用RAM領域31bのアドレスをアドレス情報記憶部52bに記憶させる。CPU20bは、次に、ステップS52bの処理として、そうした記憶済みアドレスを対象に、「読み込みのみ許可する」旨の設定を行う。

【0050】

ここで、CPU20aによるカウント用RAM領域31aへの上記アクセス許可態様、並びに、CPU20bによる被監視用RAM領域31bへの上記アクセス許可態様を採用する理由を説明する。

【0051】

既述したように、そもそも、CPU20bの動作状態についてCPU20aが判断するにあたり、CPU20bがカウント用RAM領域31aを読み込んだり書き込んだりする必要はない。そのため、出口保護部40bの保護機能を突破して、入口保護部50aに対しCPU20bからRAM30a（特に、カウント用RAM領域31a）へアクセスが要求されると、アクセス判定部51aは、要求先のアドレスが、（アドレス情報記憶部52aに一時記憶しておいた）上記カウント用RAM領域31aのアドレスに一致するか否かを判定する。ここで、要求先のアドレスが上記アドレスに一致しないとき、アクセス判定部51aは、CPU20bによるアクセス要求を許可する。一方、要求先のアドレスが上記アドレスに一致するとき、アクセス判定部51aは、CPU20bによるアクセス要求が読み込み要求であるか書き込み要求であるかを問わず、これら一切を遮断することとしている。

【0052】

このように、たとえ、CPU20bの動作異常状態が深刻になり、出口保護部40bの保護機能を突破し、カウント用RAM領域31aへアクセスしようとしても（異常アクセス）、この異常アクセスは、入口保護部50aによって遮断されるため、カウント用RAM領域31aに一時記憶されているデータを読み込むことも、書き換えることもできなくなる。したがって、当該デュアルコアの異常監視装置1では、監視側コア10aが入口保護部50aを所有するため、カウント用RAM領域31aに一時記憶されるデータは破壊されなくなる。

【0053】

また、CPU20aは、CPU20bの動作状態について判断を行う目的で、被監視用RAM領域31bを読み込む必要がある。そのため、出口保護部40aの保護機能を（正常に）通過して、入口保護部50bに対しCPU20aからRAM30b（特に、被監視用RAM領域31b）へアクセスが要求されると、アクセス判定部51bは、要求先のアドレスが、（アドレス情報記憶部52aに一時記憶しておいた）上記被監視用RAM領域31bのアドレスに一致するか否かを判定する。ここで、要求先のアドレスが上記アドレスに一致しないとき、アクセス判定部51bは、CPU20aによるアクセス要求を許可する。

【0054】

一方、要求先のアドレスが上記アドレスに一致するとき、アクセス判定部51bは、さらに、CPU20aによるアクセス要求が読み込み要求であるか書き込み要求であるかを判別する。そして、アクセス判定部51bは、CPU20aによるアクセス要求が、被監視用RAM領域31bの読み込み要求であるとき、これを受け入れるものの、CPU20aによるアクセス要求が、被監視用RAM領域31bへの書き込み要求であるとき、これを遮断することとしている。

【0055】

このように、CPU20aは、被監視用RAM領域31bにアクセスして、一時記憶されているデータを読み込むことはできるものの、データを書き換えることはできなくなる。したがって、当該デュアルコアの異常監視装置1では、監視側コア10aが出口保護部40aを所有するため、被監視用RAM領域31bに一時記憶されるデータは破壊されにくくなる。

【0056】

10

20

30

40

50

入口保護部50aは、CPU20bと同一の被監視側コア10bに所有されているわけではなく、動作状態が正常であるCPU20aと同一の監視側コア10aに所有されている。そのため、たとえCPU20bの異常動作状態が深刻になったとしても、CPU20bは、入口保護部50aの保護機能を解除することができない。詳しくは、入口保護部50aの保護機能は、アドレス情報記憶部52aに一時記憶されたアドレス情報と、そのアドレスを対象としたアクセス許可態様に基づくことにより成立する。そうした入口保護部50aの初期設定処理は、CPU20aによってのみ行うことができ、プログラム上も、物理的にも、CPU20bは行うことができない。そのため、たとえCPU20bの異常動作状態が深刻になったとしても、入口保護部50aの保護機能を解除することはできない。したがって、CPU20bは、出口保護部40bの保護機能を突破することができたとしても、入口保護部50aの保護機能を突破してカウント用RAM領域31aにアクセスし、一時記憶されているデータを読み込んだり、データを書き込んだりすることはできなくなる。

10

【0057】

以上のように構成されたデュアルコアの異常監視装置1の動作例を図6を参照しつつ説明する。

【0058】

被監視側コア10b（正確にはCPU20b）の動作状態が異常であるとき、図6に矢印にて異常アクセスAc21及びAc22として示すように、CPU20bはカウント用RAM領域31aに異常アクセスしようとする。しかしながら、CPU20bの異常動作状態が軽度であり、出口保護部40bの保護機能は解除されていないため、CPU20bがカウント用RAM領域31aに異常アクセスしようとしても、そうした異常アクセスAc21及びAc22は、出口保護部40bを突破することはできない。したがって、カウント用RAM領域31aに一時記憶されるデータは保護されることになる。

20

【0059】

また、被監視側コア10b（正確にはCPU20b）の異常動作状態が深刻になると、図6に矢印にて異常アクセスAc23として示すように、CPU20bはカウント用RAM領域31aに異常アクセスしようとする。このとき、CPU20bの異常動作状態が深刻であり、出口保護部40bの保護機能は解除されてしまうため、異常アクセスAc23は出口保護部40bの保護機能を突破してしまう。しかしながら、たとえCPU20bの異常動作状態が深刻であっても、同一の監視側コア10aに所有されていない入口保護部50aの保護機能を解除することはできないため、異常アクセスAc23は、入口保護部50aにて遮断されることになる。したがって、カウント用RAM領域31aに一時記憶されるデータは保護されることになる。

30

【0060】

このように、カウント用RAM領域31aに一時記憶されているデータは、出口保護部40b及び入口保護部50aにて保護されているため、CPU20aはCPU20bの動作状態の判断を正確に判断することができるようになる。

【0061】

また、こうしたデュアルコアの異常監視装置1は、既述したように、例えば自動車の燃焼室に燃料を噴射供給する燃料噴射制御装置（ECU）に適用されている。

40

【0062】

自動車の運転制御においては、一般に、ECUを構成する複数のプロセッサコアの一部の動作状態が異常となった場合であっても、フェイルセーフとして、少なくとも退避走行ができなければならない。そのため、例えば燃料噴射制御は、以下に説明するように実行されている。

【0063】

ECUを構成する複数のプロセッサコアの動作状態が正常であるときにあっては、例えばエンジンの燃焼室に吸入される空気量等に基づいて、自動車の運転を持続可能な量である基本燃料噴射量を算出するとともに、例えば水温センサにて検出される水温等のパラメ

50

ータに基づき補正係数を算出し、この補正係数を用いて基本燃料噴射量を最終燃料噴射量に補正する。そして、インジェクタの駆動制御を通じて最終燃料噴射量の燃料を燃焼室に噴射供給している。

【0064】

一方、ECUを構成する複数のプロセッサコアの一部の動作状態が異常であるときには、上記フェイルセーフとして、上記パラメータに基づき算出された補正係数を用いるのではなく、この補正係数を所定のデフォルト値に置き換え、このデフォルト値を用いて上記基本燃料噴射量を最終燃料噴射量に補正する。そして、インジェクタの駆動制御を通じて最終燃料噴射量の燃料を燃焼室に噴射供給している。

【0065】

そして、本実施の形態では、監視側コア10a（正確にはCPU20a）が、上記基本燃料噴射量（基本制御値）を算出する基本燃料噴射量算出処理（基本制御値算出処理）、及び、所定のデフォルト値を補正係数として用いて基本燃料噴射量を最終燃料噴射量（最終制御値）に補正する第1補正処理、並びに、上記インジェクタの駆動制御を通じた最終燃料噴射量の燃料噴射供給を実行するようにしている。また、被監視側コア10b（正確にはCPU20b）が、各種センサのセンサ出力値に基づき算出した補正係数を用いて上記基本燃料噴射量を最終燃料噴射量に補正する第2補正処理を実行するようにしている。

【0066】

これにより、当該燃料噴射装置は、CPU20bの動作状態が異常である旨CPU20aによって判定されるとき、フェイルセーフとして、所定のデフォルト値が補正係数として用いられ基本燃料噴射量が補正された最終燃料噴射量の燃料を、インジェクタの駆動制御を通じて燃焼室に噴射供給することで、搭載された自動車の退避走行を確実に実行することができるようになる。

【0067】

（第2の実施の形態）

次に、本発明に係るマルチコアの異常監視装置の第2の実施の形態について、図7を参照して説明する。なお、図7は、本実施の形態の別の構成例を示す模式図である。

【0068】

同図7に示すように、本実施の形態も、先の図1～図6に示した第1の実施の形態に準じた構成となっている。すなわち、本実施の形態は、例えば2つのプロセッサコア及びこれらプロセッサ間を接続する第1通信路が1つのパッケージに集積された、いわゆるデュアルコアによって構成されており、例えば自動車の燃焼室に燃料を噴射供給する燃料噴射制御装置に適用されている。

【0069】

ただし、本実施の形態のデュアルコアの異常監視装置1aでは、図7に示すように、また、以下に詳述するように、入口保護部50aは、CPU20bによる異常アクセスAc23を遮断する際、この異常アクセスAc23に係る情報をCPU20aに通知する通知部53aを備えるとともに、CPU20aは、通知部53aによって通知された情報に基づいてCPU20bの異常動作状態の程度を判断し、CPU20bの復帰処理をこの異常動作状態の程度に応じて実行する。

【0070】

詳しくは、図7に異常アクセスAc23として示すように、CPU20bが出口保護部40bの保護機能を突破してカウント用RAM領域31aに異常アクセスしようとする、入口保護部50a（正確にはアクセス判定部51a）は、この異常アクセスAc23を既述したように遮断する。そして、アクセス判定部51aは、例えばいずれのプロセッサコアからRAM30aのどの領域にアクセスが試みられたか等、異常アクセスAc23の発生状況に係る情報を取得し、取得した情報を通知部53aに伝達する。通知部53aは、図7に通知Ac3として示すように、この伝達された情報をCPU20aに通知する。

【0071】

こうした情報の通知を受けたCPU20aは、図7に復帰処理22として示すように、

10

20

30

40

50

まず、異常アクセス A c 2 3 の発生状況に係る情報に基づいて、例えば「出口保護部 4 0 b に瞬時的な誤作動が生じた」、「C P U 2 0 b の動作状態が異常である」、「C P U 2 0 b の異常動作状態が深刻であり、カウント用 R A M 領域 3 1 a への異常アクセスを乱発している」等々、C P U 2 0 b の異常動作状態の程度を判断する。そして、C P U 2 0 a は、復帰処理 2 2 として、判断した C P U 2 0 b の異常動作状態の程度に応じて、例えば「出口保護部 4 0 b の再設定」、「C P U 2 0 b のリセット」、「当該装置全体のリセット」等の復帰処理を実行する。

【 0 0 7 2 】

以上説明したデュアルコアの異常監視装置 1 a によれば、C P U 2 0 b の動作状態が異常であるか正常であるかといった 2 値的な判定に留まらず、C P U 2 0 b の異常動作状態の程度を判断することができ、その程度に応じた復帰処理を実行することができるようになる。そしてひいては、例えば、C P U 2 0 b の異常動作状態が軽度であって C P U 2 0 b のリセットを実行すれば十分であるにもかかわらず、当該装置全体をリセットしてしまうといったことを未然に防ぐことができるようになるため、当該装置をより効率的に作動させることができるようになる。

【 0 0 7 3 】

なお、上記第 2 の実施の形態では、入口保護部 5 0 a は、既述の保護機能に加え、通知機能を有していた（すなわち、通知部 5 3 a は入口保護部 5 0 a の構成要素であった）が、これに限らない。他に例えば、通知部 5 3 a を入口保護部 5 0 a の構成要素から分離し、入口保護部 5 0 a とは別に、監視側コア 1 0 a が所有することとしてもよい。

【 0 0 7 4 】

（他の実施の形態）

なお、本発明に係るマルチコアの異常監視装置は、上記第 1 及び第 2 の実施の形態で示した構成に限定されるものではなく、本発明の趣旨を逸脱しない範囲において、種々に変形して実施することが可能である。すなわち、上記各実施の形態を適宜変更した例えば次の形態として実施することもできる。

【 0 0 7 5 】

上記各実施の形態では、被監視用処理（図 2 参照）として、C P U 2 0 b は、被監視用 R A M 領域 3 1 b に一時記憶されている値を第 2 通信路 7 0 b を介して読み込み、この読み込んだ値の反転値を第 2 通信路 7 0 b を介して書き込むこととしていたが、これに限らない。他に例えば、C P U 2 0 b は、被監視用 R A M 領域 3 1 b に一時記憶されている値を第 2 通信路 7 0 b を介して読み込み、この読み込んだ値に所定数を加えた積算値を第 2 通信路 7 0 b を介して書き込む（カウントアップ）こととしてもよい。要は、C P U 2 0 a が C P U 2 0 b の動作状態を監視するにあたり、C P U 2 0 b の動作状態が正しく反映される操作であれば、任意である。

【 0 0 7 6 】

上記各実施の形態では、そうした C P U 2 0 b による操作結果を一時記憶するための被監視用 R A M 領域 3 1 b を被監視側コア 1 0 b の所有としていたが、これに限らず、監視側コア 1 0 a が被監視用 R A M 領域 3 1 b を所有する、すなわち、R A M 3 0 a 内に被監視用 R A M 領域 3 1 b を設定することとしてもよい。この場合、例えば、C P U 2 0 b が R A M 3 0 a に設定された被監視用 R A M 領域に C P U 2 0 a を介することなくアクセスする、いわゆる D M A (D i r e c t M e m o r y A c c e s s) 方式を採用することができる。要は、C P U 2 0 b による操作結果を C P U 2 0 a によって監視することができれば、被監視用 R A M 領域 3 1 b の所在は任意である。

【 0 0 7 7 】

上記各実施の形態では、異常監視判断処理（図 3 参照）として、被監視用 R A M 領域 3 1 b に一時記憶されているデータに基づき C P U 2 0 b の動作状態を判断し、動作状態が異常であると判断された回数である異常回数カウント値が判定値に到達するとき、C P U 2 0 b の動作状態が異常である旨の（最終的な）判定を行うこととしたが、判定値については任意である。例えば、動作状態が異常であると一度でも判断されたら、ただちに、C

10

20

30

40

50

P U 2 0 b の動作状態が異常である旨の最終的な判定を行う（すなわち、判定値が「1」）こととしてもよい。

【0078】

上記各実施の形態では、デュアルコアの異常監視装置1及び1aは、出口保護部40a及び40b並びに入口保護部50a及び50bの双方を備えていたが、これに限らず、出口保護部40a及び40bを割愛した構成としてもよい。

【0079】

上記各実施の形態では、デュアルコアの異常監視装置1及び1aを自動車の燃焼室に燃料を噴射供給する燃料噴射制御装置に適用し、上記基本燃料噴射量算出処理、及び、上記第1補正処理、並びに、上記インジェクタの駆動制御を通じての最終燃料噴射量の燃料噴射供給を、監視側コア10aに実行させ、上記第2補正処理を、被監視側コア10bに実行させることとしていたが、これに限らない。要は、当該マルチコアの異常監視装置を、任意の制御対象を制御するための最終制御値を算出する制御装置に適用し、監視側コアに、制御対象が有する各種センサのセンサ出力値に基づき、制御対象の制御を持続可能とする基本制御値を算出する基本制御値算出処理と、所定のデフォルト値に基づいて、基本制御値算出処理を通じて算出された基本制御値を最終制御値に補正する第1補正処理とを実行させるとともに、被監視側コアに、センサ出力値に基づいて、基本制御値算出処理を通じて算出された基本制御値を最終制御値に補正する第2補正処理を実行させればよい。これにより、当該装置は、被監視側コアの動作状態が異常である旨監視側コアによって判定されたとき、フェイルセーフとして、第1補正処理を通じて補正された最終制御値に基づき制御対象を制御することができるようになる。

【0080】

上記各実施の形態では、2つのプロセッサコアが1つのパッケージに集積された、いわゆるデュアルコアによって構成していたが、プロセッサコアの個数は任意である。プロセッサコアの数が多数になるほど、上記出口保護手段及び入口保護手段による保護機能による効果が高まり、好適である。すなわち、1つのプロセッサコアの動作状態が異常となり、これが起因して、あるプロセッサコアの動作状態が異常となったことを契機として、他のプロセッサコアの動作状態が次々に異常となる連鎖を生じにくくすることができるようになる。

【図面の簡単な説明】

【0081】

【図1】本発明に係るマルチコアの異常監視装置の第1の実施の形態について、その構成例を示す模式図。

【図2】同第1の実施の形態の被監視用処理について、その処理手順の一例を示すフローチャート。

【図3】同第1の実施の形態の異常監視判断処理について、その処理手順の一例を示すフローチャート。

【図4】(a)及び(b)は、同第1の実施の形態を構成する出口保護部40a及び40bの初期設定処理について、その処理手順の一例をそれぞれ示すフローチャート。

【図5】(a)及び(b)は、同第1の実施の形態を構成する入口保護部50a及び50bの初期設定処理について、その処理手順の一例をそれぞれ示すフローチャート。

【図6】同第1の実施の形態について、その動作例を示す模式図。

【図7】本発明に係るマルチコアの異常監視装置の第2の実施の形態について、その構成例を示す模式図。

【符号の説明】

【0082】

1...デュアルコアの異常監視装置、10a...監視側コア、10b...被監視側コア、20a、20b...CPU(演算処理部)、21a...異常監視判断処理、21b...被監視用処理、22...復帰処理、30a、30b...RAM(一時記憶部)、31a...カウント用RAM領域、31b...被監視用RAM領域、40a、40b...出口保護部(第2保護手段)、41

10

20

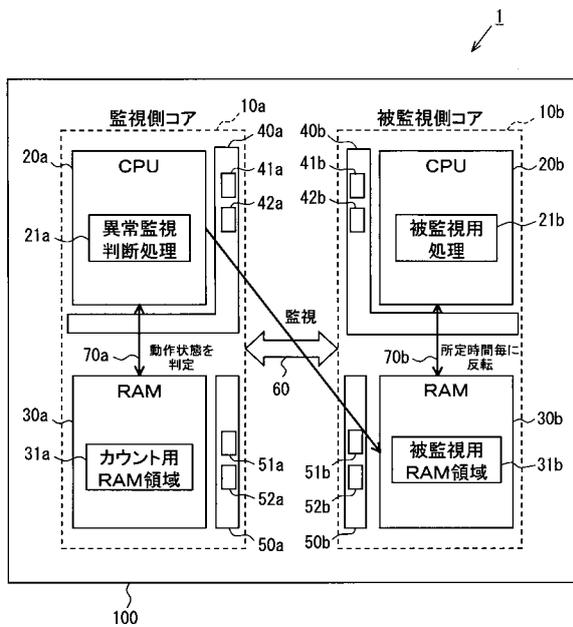
30

40

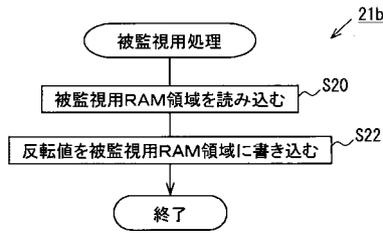
50

a、41b...アクセス判定部、42a、42b...アドレス情報記憶部、50a、50b...
 入口保護部（第1保護手段）、51a、51b...アクセス判定部、52a、52b...アド
 レス情報記憶部、53...通知部、60...第1通信路、70a、70b...第2通信路、10
 0...チップ、Ac21~Ac23...異常アクセス、Ac3...通知。

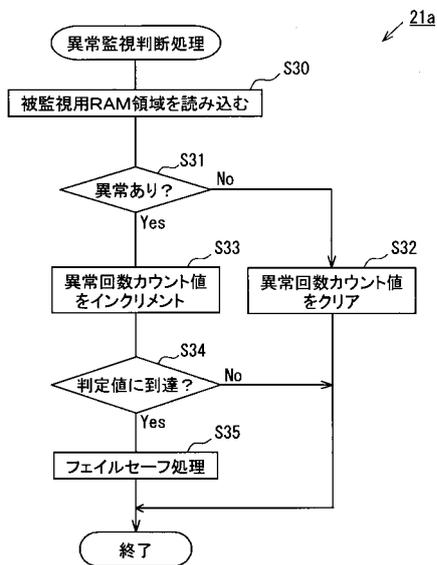
【図1】



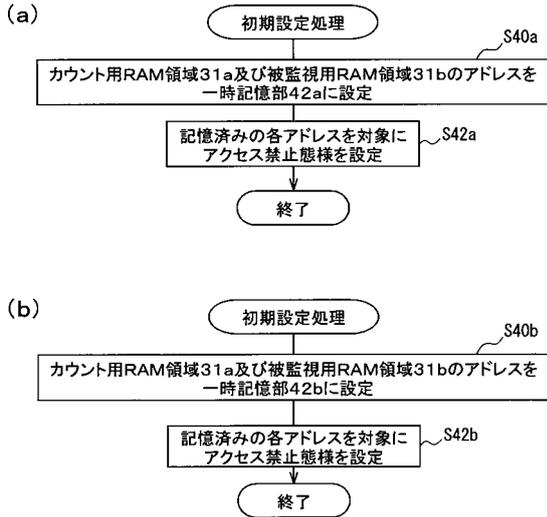
【図2】



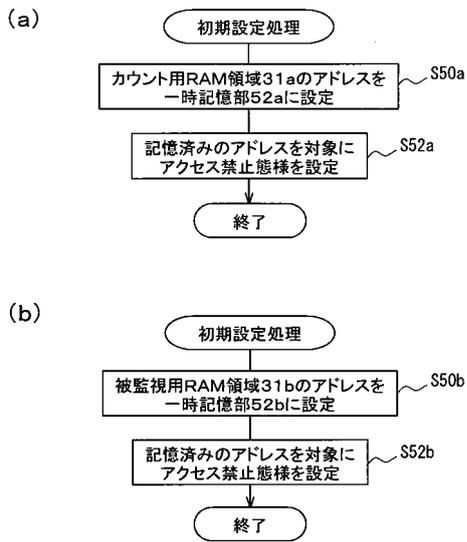
【図3】



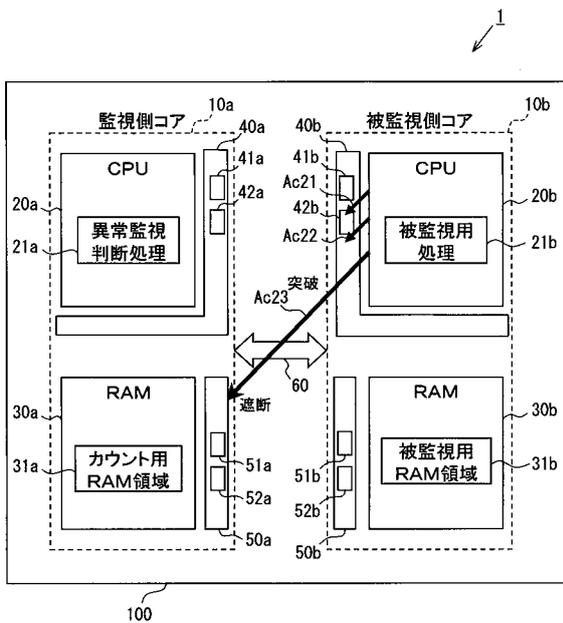
【図4】



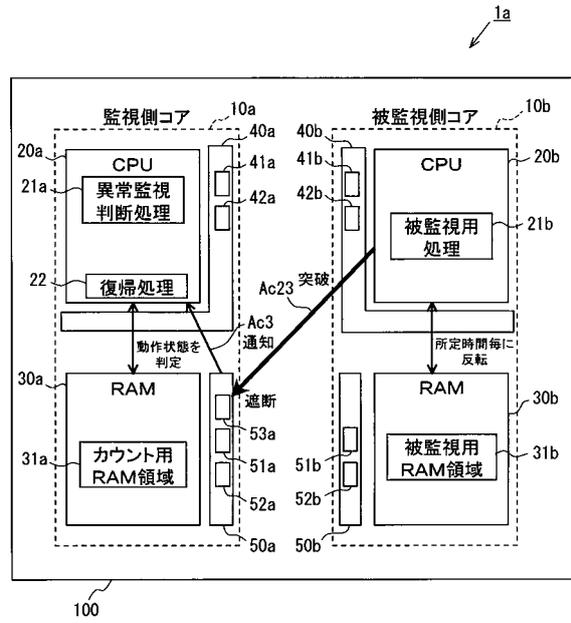
【図5】



【図6】



【図7】



フロントページの続き

(56)参考文献 特開平05-241905 (J P , A)
特開2001-331376 (J P , A)
特開2002-132743 (J P , A)
特開2003-099293 (J P , A)

(58)調査した分野(Int.Cl. , D B 名)
G 0 6 F 1 1 / 3 0