

(12) 特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2016 年 10 月 27 日(27.10.2016)



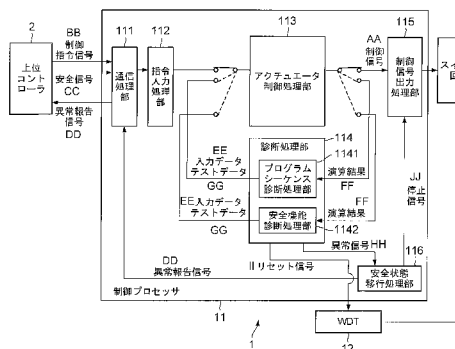
(10) 国際公開番号

WO 2016/170840 A1

- (51) 国際特許分類:
G06F 11/07 (2006.01)
- (21) 国際出願番号: PCT/JP2016/055278
- (22) 国際出願日: 2016 年 2 月 23 日(23.02.2016)
- (25) 国際出願の言語: 日本語
- (26) 国際公開の言語: 日本語
- (30) 優先権データ:
特願 2015-089082 2015 年 4 月 24 日(24.04.2015) JP
- (71) 出願人: 富士電機株式会社(FUJII ELECTRIC CO., LTD.) [JP/JP]; 〒2109530 神奈川県川崎市川崎区田辺新田 1 番 1 号 Kanagawa (JP).
- (72) 発明者: 田島 宏一(TAJIMA, Hirokazu); 〒2109530 神奈川県川崎市川崎区田辺新田 1 番 1 号 富士電機株式会社内 Kanagawa (JP). 西田 廣治(NISHIDA, Hiroji); 〒2109530 神奈川県川崎市川崎区田辺新田 1 番 1 号 富士電機株式会社内 Kanagawa (JP).
- (74) 代理人: 松本 隆(MATSUMOTO, Takashi); 〒1010024 東京都千代田区神田和泉町 1-6-1 インターナショナルビル 802 松本特許事務所内 Tokyo (JP).
- (81) 指定国 (表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.
- (84) 指定国 (表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), ユーロパ (AM, AZ, BY, KG, KZ, RU, TJ, TM), ユーロッパ (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).
- 添付公開書類:
— 国際調査報告 (条約第 21 条(3))

(54) Title: DRIVE CONTROL DEVICE

(54) 発明の名称: 駆動制御装置



(57) Abstract: Provided is a drive control device capable of maintaining a drive control system in a safe state even on the occurrence of a malfunction wherein a control processor cannot be reset in a normal manner or a malfunction which cannot be eliminated even if the control processor is reset. The control processor 11 has: an actuator control processing unit 113 for generating control signals for controlling a drive circuit 4 and an actuator 5 which are devices to be controlled; and a diagnostic processing unit 114 for performing a diagnosis of the actuator control processing unit. When the control processor 11 is operating normally, the diagnostic processing unit 114 periodically outputs a reset signal to a watchdog timer (WDT) 12. When this periodic reset signal is stopped, the WDT 12 continuously outputs a cutoff signal for cutting off the supply of the control signal from the control processor 11 to the devices to be controlled.

(57) 要約: 制御プロセッサのリセットが正常に働かなくなるような動作異常あるいは制御プロセッサのリセットを行ったとしても解消しないような動作異常が制御プロセッサに発生する場合においても、駆動制御システムを安全な状態に維持することができる駆動制御装置を提供する。制御プロセッサ 11 は、制御対象装置である駆動回路 4 およびアクチュエータ 5 のための制御信号を生成するアクチュエータ制御処理部 113 とその診断を行う診断処理部 114 を有する。診断処理部 114 は、制御プロセッサ 11 の動作が正常である場合に周期的に WDT 12 にリセット信号を出力する。WDT 12 は、この周期的なリセット信号が途絶えると、制御プロセッサ 11 から制御対象装置への制御信号の供給を遮断する遮断信号を継続的に出力する。

明 細 書

発明の名称： 駆動制御装置

技術分野

[0001] この発明は、ウォッチドッグタイマを備える駆動制御装置に関する。

背景技術

[0002] CPU (Central Processing Unit、以下「CPU」と略記) によりアクチュエータ等の制御対象装置の駆動制御を行う駆動制御システムでは、CPUの異常や故障への対策が強く求められている。そこで、CPUを監視し、CPUの異常や故障を検知する技術が種々開発されている。例えば特許文献1に開示の技術では、監視対象のCPUとは別に監視ICを設け、この監視ICがCPUのトルクモニタ部と信号異常診断部の動作状態を監視し、これらの動作異常を検知すると、マイクロコンピュータの自己監視部と協調して、フェールセーフ制御を実施する。

[0003] しかしながら、この特許文献1に開示の技術において、監視ICが検知するCPUの動作異常は、トルクモニタ部と信号異常診断部の動作異常等の特定の異常に限られる。そして、この特許文献1に開示の技術は、CPUの動作において発生し得るALU (Arithmetic Logic Unit ; 算術論理演算装置) の動作異常、データ経路の動作異常、レジスタの動作異常、内部RAMの動作異常、アドレス計算の動作異常、割り込み処理の動作異常、制御ロジックの動作異常、構成レジスタの動作異常といった広範囲の動作異常を検知して、その対応を行うことができないという問題がある。

[0004] CPUにおいて発生し得る広範囲の動作異常への対応手段として、ウォッチドッグタイマを利用した手段がある。例えば特許文献2に開示の技術では、CPUからウォッチドッグタイマに周期的にパルス信号を供給してウォッチドッグタイマをリセットする。CPUに動作異常が発生してパルス信号が所定時間供給されないと、ウォッチドッグタイマはリセット信号をCPUに

出力し、CPUにリセット処理を実行させる。また、特許文献3に開示の技術では、特許文献2と同様にウォッチドッグタイマが設けられているが、ウォッチドッグタイマは、CPUからの定期的なウォッチドッグタイマクリア信号の供給が途絶えると、CPUが正常動作していないと判断し、上位システムに対してエラー通知を送信する。

先行技術文献

特許文献

[0005] 特許文献1：特開2010-43536号公報

特許文献2：特開2003-97345号公報

特許文献3：特開2014-32558号公報

発明の概要

発明が解決しようとする課題

[0006] ところで、上述した特許文献2に開示の技術は、リセット信号が与えられても制御プロセッサであるCPUのリセット機能が正常に働かない場合への対策が講じられていない問題がある。また、上述した特許文献2に開示の技術は、制御プロセッサであるCPUのリセット機能が正常に働いたとしても、リセット後のCPUが正常な動作をする保証がないという問題がある。また、上述した特許文献2および3に開示の技術は、ウォッチドッグタイマ自体の動作が異常になった場合に、駆動制御システムを安全な状態に維持するのが困難であるという問題がある。

[0007] この発明は、以上説明した事情に鑑みてなされたものであり、その第1の目的は、制御プロセッサのリセットが正常に働かなくなるような動作異常あるいは制御プロセッサのリセットを行ったとしても解消しないような動作異常が制御プロセッサに発生する場合においても、駆動制御システムを安全な状態に維持することができる駆動制御装置を提供することにある。また、この発明の第2の目的は、ウォッチドッグタイマ自体に動作異常が発生する状況においても、駆動制御システムを安全な状態に維持することができる駆動

制御装置を提供することにある。

課題を解決するための手段

- [0008] この発明は、制御信号を生成する制御プロセッサと、前記制御プロセッサから供給されるリセット信号に応じて計時値をリセットし、このリセット後、目標計時時間の計時を完了することによって、前記制御プロセッサから制御対象装置への制御信号の供給を遮断する遮断信号を継続的に出力するウォッチドッグタイマとを具備することを特徴とする駆動制御装置を提供する。
- [0009] この発明によれば、制御プロセッサからウォッチドッグタイマへのリセット信号の供給が途絶えると、ウォッチドッグタイマは、目標計時時間の計時を完了することによって、制御対象装置への制御信号の供給を継続的に遮断する。そのため、制御プロセッサのリセットが正常に働かなくなるような動作異常あるいは制御プロセッサのリセットを行ったとしても解消しないような動作異常が制御プロセッサに発生したとしても、制御対象装置が制御プロセッサの動作異常の悪影響を受けるのを阻止し、駆動制御システムを安全な状態に維持することができる。
- [0010] 好ましい態様において、前記制御プロセッサは、当該制御プロセッサの動作の診断を行う診断手段と、前記診断手段が当該制御プロセッサの動作に異常があると診断した場合に、正常時よりも動作範囲が制限された安全状態に当該制御プロセッサを移行させる安全状態移行処理手段とを具備する。
- [0011] この態様によれば、ウォッチドッグタイマ自体の動作異常が発生し、制御プロセッサの動作異常発生時にウォッチドッグタイマが制御対象装置への制御信号の供給を遮断できなくても、制御プロセッサを安全状態に移行することができ、駆動制御システムを安全な状態に維持することができる。
- [0012] 好ましい態様において、前記診断手段は、前記目標計時時間よりも短い周期で前記診断を繰り返し、前記制御プロセッサが正常であると診断した場合に前記リセット信号を出力する。
- [0013] この態様によれば、前記診断手段が当該制御プロセッサの動作に異常があると診断した場合に、ウォッチドッグタイマが遮断信号を出力する前に、安

全状態移行手段が制御プロセッサを安全状態に移行させる。従って、制御対象装置の安全性を確保することができる。

[0014] 好ましい態様において、前記安全状態移行処理手段は、前記診断手段が前記制御プロセッサの動作の異常を診断した場合に、前記制御対象装置を正常時よりも動作範囲の制限された安全状態とする制御信号を前記制御プロセッサから出力させる。

[0015] この態様によれば、制御プロセッサの動作異常が診断された場合に、制御対象装置の動作範囲を制限することにより制御対象装置の安全性を確保することができる。

[0016] 好ましい態様においては、前記安全状態移行処理手段は、前記診断手段が前記制御プロセッサの動作の異常を診断した場合に、前記制御プロセッサからの前記制御信号の出力を停止させる。

[0017] この態様によれば、制御プロセッサの動作の異常を診断した後は、制御プロセッサの動作異常の影響が制御対象装置に及ぶのを阻止することができる。

[0018] 好ましい態様においては、前記安全状態移行処理手段は、前記診断手段が前記制御プロセッサの動作の異常を診断した場合に、前記制御対象装置の動作状態を時間経過に応じて所定の安全状態に移行させる制御信号を前記制御プロセッサから出力させる。

[0019] この態様によれば、制御プロセッサの動作の異常が診断された場合に、制御対象装置の駆動状態を時間経過に伴って徐々に安全な状態に移行させることができる。従って、制御対象装置の動作が不安定になるのを防止することができる。

[0020] 好ましい態様においては、前記制御プロセッサは、前記診断手段が前記制御プロセッサの動作の異常を診断した場合に、前記制御プロセッサの動作の異常を上位コントローラに通知する通信手段を具備する。この態様によれば、上位コントローラは制御プロセッサの動作の異常を認識することができる。

[0021] 好ましい態様においては、前記安全状態移行処理手段は、前記診断手段が前記制御プロセッサの動作の異常を診断した場合に、前記制御プロセッサをホールド状態とする。この態様によれば、制御プロセッサの動作異常が診断された場合、制御プロセッサがホールド状態とされるので、制御プロセッサの動作異常の影響が大きくなるのを防止することができる。

発明の効果

[0022] 以上説明したように、この発明によれば、制御プロセッサのリセットが正常に働かなくなるような動作異常あるいは制御プロセッサのリセットを行ったとしても解消しないような動作異常が制御プロセッサに発生したとしても、制御対象装置が制御プロセッサの動作異常の悪影響を受けるのを阻止し、駆動制御システムを安全な状態に維持することができる。

図面の簡単な説明

[0023] [図1]この発明の一実施形態による駆動制御装置 1 を含む駆動制御システムの構成を示すブロック図である。

[図2]同駆動制御装置 1 の制御プロセッサ 11 の処理内容を示すフローチャートである。

[図3]同制御プロセッサ 11 が実行する安全機能診断処理を示すフローチャートである。

[図4]同制御プロセッサ 11 の第 1 の動作例を示すタイムチャートである。

[図5]同制御プロセッサ 11 の第 2 の動作例を示すタイムチャートである。

[図6]同制御プロセッサ 11 の第 3 の動作例を示すタイムチャートである。

[図7]この発明の他の実施形態における制御プロセッサの動作例を示すタイムチャートである。

発明を実施するための形態

[0024] 以下、図面を参照しつつ、この発明の実施形態について説明する。

図 1 は、この発明の一実施形態による駆動制御装置 1 を含む駆動制御システムの構成を示すブロック図である。この駆動制御システムは、図 1 に示すように、駆動制御装置 1 と、上位コントローラ 2 と、スイッチ回路 3 と、駆

動制御装置 1 の制御対象装置である駆動回路 4 と、アクチュエータ 5 とを有する。

[0025] 上位コントローラ 2 は、例えば PLC (Programmable Logic Controller) 等の制御装置と、安全リレー等からなる安全装置とにより構成されている。この上位コントローラ 2 は、使用者による操作等に基づいて生成した制御指令信号を駆動制御装置 1 に供給する。また、上位コントローラ 2 は、駆動制御システム内において、アクチュエータ 5 への作業者の接近等の危険の発生を検知した場合あるいは非常停止ボタンの押圧操作が行われた場合等に安全信号を発生して駆動制御装置 1 に供給する。また、上位コントローラ 2 は、駆動制御装置 1 の制御プロセッサ 11 (後述) の異常を示す異常報告信号を駆動制御装置 1 から受け取り、警報の発生等、異常報告信号に対応した処理を実行する。

[0026] スイッチ回路 3 は、駆動制御装置 1 と駆動回路 4 の間に設けられている。このスイッチ回路 3 は、常時は、駆動制御装置 1 が出力する制御信号を駆動回路 4 に供給するが、駆動制御装置 1 から遮断信号が与えられることによりオフとなり、駆動制御装置 1 から駆動回路 4 への制御信号の供給を遮断する。

[0027] 駆動回路 4 は、例えばインバータの主回路であり、複数のスイッチング素子により構成されている。この駆動回路 4 は、駆動制御装置 1 から供給される制御信号に基づいてスイッチング素子をオンさせ、このスイッチング素子を介してアクチュエータ 5 に駆動電圧を供給する。アクチュエータ 5 は、例えばモータである。

[0028] 駆動制御装置 1 は、制御指令信号或いは安全信号に基づいて制御信号を生成し、スイッチ回路 3 を介して制御信号を駆動回路 4 に供給し、アクチュエータ 5 の駆動を制御する。この駆動制御装置 1 は、図 1 に示すように、制御プロセッサ 11 と、ウォッチドッグタイマ (以下、WDT と略す) 12 とを有する。WDT 12 は、一定周期のクロックのカウントを行うカウンタを有し、制御プロセッサ 11 からリセット信号の供給があると、WDT 12 はク

ロックのカウント値（すなわち、計時値）をゼロにする。また、WDT 12は、計時値が所定の目標計時時間に到達すると、スイッチ回路3に継続的に遮断信号を供給する。

[0029] 制御プロセッサ11は、上位コントローラ2から供給される制御指令信号または安全信号に基づいてアクチュエータ5を制御するための制御信号を生成する手段である。この制御プロセッサ11は、CPUコアの他、このCPUコアが実行するプログラムを記憶したROMと、CPUコアによってワークエリアとして使用されるRAMとを内蔵したCPUである。図1では、CPUコアとROMとRAMの図示は省略している。制御プロセッサ11のCPUコア（以下、説明の便宜のため、単に制御プロセッサ11という）がROM内のプログラムを実行することにより実現される機能は、図1に示す通信処理部111と、指令入力処理部112と、アクチュエータ制御処理部113と、診断処理部114と、制御信号出力処理部115と、安全状態移行処理部116とに大別することができる。

[0030] 通信処理部111は、上位コントローラ2から制御指令信号および安全信号を受信する手段である。また、通信処理部111は、安全状態移行処理部116から異常報告信号を受け取った場合に、その異常報告信号を上位コントローラ2に送信し、以後、上位コントローラ2からの制御指令信号および安全信号の受信を拒否する。ただし、上位コントローラ2が異常報告信号の内容を判断して復帰指令信号を送信した場合、通信処理部111は、この復帰指令信号を受信し、上位コントローラ2からの制御信号および安全信号の受信を再開する。指令入力処理部112は、通信処理部111が上位コントローラ2から受信した制御指令信号および安全信号をアクチュエータ制御処理部113に引き渡す手段である。アクチュエータ制御処理部113は、制御指令信号や安全信号に基づいて、アクチュエータ5を駆動制御するための制御信号を生成するための演算処理を実行する手段である。

[0031] 例えば、アクチュエータ5がモータであり、駆動回路4がモータを駆動するインバータの主回路である場合、アクチュエータ制御処理部113は、駆

動回路4の各スイッチング素子のON/OFFを制御するためのPWM (Pulse Width Modulation; パルス幅変調) 信号を生成する。その際、アクチュエータ制御処理部113は、制御指令信号や安全信号に応じて、制御信号であるPWM信号のパルス幅の増減の制御を行う。

[0032] 制御信号出力処理部115は、アクチュエータ制御処理部113によって生成される制御信号を制御プロセッサ11から出力する手段である。制御信号出力処理部115は、安全状態移行処理部116から停止信号を受け取った場合に、制御信号の出力を停止する。

[0033] 診断処理部114は、アクチュエータ制御処理部113の動作が正常であるか異常であるかを診断する手段である。図1に示すように、診断処理部114は、プログラムシーケンス診断処理部1141と、安全機能診断処理部1142とを含む。ここで、プログラムシーケンス診断処理部1141は、アクチュエータ制御処理部113の動作のうち制御指令信号に応じて制御信号の生成を行う動作が正常であるか異常であるかを診断する手段である。また、安全機能診断処理部1142は、アクチュエータ制御処理部113の動作のうち安全信号に応じて制御信号の生成を行う動作が正常であるか異常であるかを診断する手段である。

[0034] これらの診断において、プログラムシーケンス診断処理部1141および安全機能診断処理部1142は、アクチュエータ制御処理部113において使用される制御プロセッサ11のALUの異常、データ経路の異常、レジスタの異常、内部RAMの異常、アドレス計算手段の異常、割り込み処理手段の異常、制御ロジックの異常、構成レジスタの異常を検知する。

[0035] 診断処理部114は、プログラムシーケンス診断処理部1141による診断処理および安全機能診断処理部1142による診断処理を周期的に繰り返し、両診断処理においてアクチュエータ制御処理部113の動作が正常である旨の診断結果が得られた場合にリセット信号をWDT12に供給する。また、安全状態移行処理部116は、プログラムシーケンス診断処理部1141による診断処理または安全機能診断処理部1142による診断処理におい

て、アクチュエータ制御処理部 113 の動作の異常が診断された場合に、異常信号を安全状態移行処理部 116 に出力する。この異常信号は制御プロセッサ 11 が異常である旨を示す情報とその異常内容を示す情報とを含む。

[0036] 安全状態移行処理部 116 は、診断処理部 114 がアクチュエータ制御処理部 113 の動作に異常があると診断した場合に、正常時よりも動作範囲が制限された安全状態に制御プロセッサ 11 を移行させる安全状態移行処理手段として機能する。具体的には、本実施形態において安全状態とは、制御プロセッサ 11 がホールド（内部状態を遷移させない状態）し、制御信号の生成および出力を行わない状態である。安全状態移行処理部 116 は、診断処理部 114 から異常信号を受け取った場合に、制御信号出力処理部 115 に停止信号を出力するとともに、異常信号を異常報告信号として通信処理部 111 に出力し、さらに制御プロセッサ 11 をホールド状態にする。

以上が本実施形態の構成である。

[0037] 次に、本実施形態の動作について説明する。図 2 は、制御プロセッサ 11 の処理内容を示すフローチャートである。駆動制御装置 1 の電源投入等に伴って起動指令が発生すると、まず、ステップ S101 に進み、プログラムシーケンス診断処理部 1141 がプログラムシーケンス診断処理を実行する。このプログラムシーケンス診断処理は、アクチュエータ制御処理部 113 の動作のうち制御指令信号に応じて制御信号を生成する動作を診断する処理である。

[0038] 次にステップ S102 に進むと、プログラムシーケンス診断処理部 1141 は、プログラムシーケンス診断処理の診断結果についての判断を行う。アクチュエータ制御処理部 113 の動作が異常であることを診断結果が示している場合、処理はステップ S110 に進み、アクチュエータ制御処理部 113 の動作が正常であることを診断結果が示している場合、処理はステップ S103 に進む。

[0039] 次にステップ S103 に進むと、安全機能診断処理部 1142 が安全機能診断処理を実行する。この安全機能診断処理は、アクチュエータ制御処理部

１１３の動作のうち安全信号に応じて制御信号を生成する動作を診断する処理である。

[0040] 次にステップＳ１０４に進むと、安全機能診断処理部１１４２は、安全機能診断処理の診断結果についての判断を行う。アクチュエータ制御処理部１１３の動作が異常であることを診断結果が示している場合、処理はステップＳ１１０に進み、アクチュエータ制御処理部１１３の動作が正常であることを診断結果が示している場合、処理はステップＳ１０５に進む。

[0041] 次にステップＳ１０５に進むと、診断処理部１１４は、ＷＤＴ１２にリセット信号を出力し、ＷＤＴ１２の計時値をリセットさせる。次にステップＳ１０６に進むと、アクチュエータ制御処理部１１３が本来のアクチュエータ制御処理を実行する。このアクチュエータ制御処理において、アクチュエータ制御処理部１１３は、指令入力処理部１１２から制御指令信号或いは安全信号を取得し、制御指令信号や安全信号に基づいて制御信号を生成し、制御信号出力処理部１１５に供給する。

[0042] このステップＳ１０６が終了すると、処理はステップＳ１０１に戻る。以後、プログラムシーケンス診断処理（ステップＳ１０１）および安全機能診断処理（ステップＳ１０３）の両診断結果においてアクチュエータ制御処理部１１３の動作が正常である限り、ステップＳ１０１→Ｓ１０２→Ｓ１０３→Ｓ１０４→Ｓ１０５→Ｓ１０６→Ｓ１０１の順に各ステップの処理が繰り返される。

[0043] 一方、ステップＳ１０２またはＳ１０４の判断において、アクチュエータ制御処理部１１３の動作が異常であることを診断結果が示していると、処理はステップＳ１１０へ進む。このステップＳ１１０において、診断処理部１１４は、安全状態移行処理部１１６に異常信号を出力する。そして、安全状態移行処理部１１６は、異常報告信号を通信処理部１１１に出力する。これにより通信処理部１１１は、異常報告信号を上位コントローラ２に送信し、以後、上位コントローラ２からの制御指令信号および安全信号の受信を拒否する。ただし、上位コントローラ２が異常報告信号の内容を判断して復帰指

令信号を送信した場合、通信処理部 111 は、この復帰指令信号を受信し、上位コントローラ 2 からの制御信号および安全信号の受信を再開する。次にステップ S 111 に進むと、安全状態移行処理部 116 が安全状態に移行するための処理を行う。具体的には、安全状態移行処理部 116 は、停止信号を制御信号出力処理部 115 に出力する。これにより制御信号出力処理部 115 は、アクチュエータ制御処理部 113 からの制御信号の外部への出力を停止する。また、安全状態移行処理部 116 は、制御プロセッサ 11 への内部クロックを停止し、制御プロセッサ 11 をホールド状態とし、図 2 に示す処理を終了する。

[0044] 図 3 はステップ S 103 の安全機能診断処理の処理内容を示すフローチャートである。安全機能診断処理部 1142 は、この安全機能診断処理の実行を開始すると、まず、ステップ S 201 に進み、ROM から安全機能診断用の入力データを読み出して RAM に格納する。次にステップ S 202 に進むと、安全機能診断処理部 1142 は、この入力データをアクチュエータ制御処理部 113 に供給し、この入力データに基づいて演算を行わせる。次にステップ S 203 に進むと、安全機能診断処理部 1142 は、アクチュエータ制御処理部 113 の演算結果を RAM に書き込む。次にステップ S 204 に進むと、安全機能診断処理部 1142 は、ROM から安全機能診断用の入力データを再度読み出して RAM に格納する。次にステップ S 205 に進むと、安全機能診断処理部 1142 は、この入力データをアクチュエータ制御処理部 113 に再度供給し、この入力データに基づく演算を再度行わせる。次にステップ S 206 に進むと、安全機能診断処理部 1142 は、アクチュエータ制御処理部 113 の演算結果を RAM に書き込む。次にステップ S 207 に進むと、安全機能診断処理部 1142 は、ステップ S 203 において RAM に書き込んだ演算結果と、ステップ S 206 において RAM に書き込んだ演算結果とを比較し、両者が一致するか否かを診断する。

[0045] ステップ S 207 の判断結果が「NO」である場合、処理はステップ S 208 に進む。次にステップ S 208 に進むと、安全機能診断処理部 1142

は、アクチュエータ制御処理部 113 が異常であると診断し、安全機能診断処理を終了する。

[0046] 一方、ステップ S 207 の判断結果が「YES」であると、処理はステップ S 210 に進む。次にステップ S 210 に進むと、安全機能診断処理部 1142 は、安全機能診断用のテストデータを ROM から読み出し、RAM に格納する。次にステップ S 211 に進むと、安全機能診断処理部 1142 は、アクチュエータ制御処理部 113 にこのテストデータに基づく演算を行わせる。次にステップ S 212 に進むと、安全機能診断処理部 1142 は、アクチュエータ制御処理部 113 の演算結果を RAM に書き込む。次にステップ S 213 に進むと、安全機能診断処理部 1142 は、テストデータに基づく演算結果の期待値である判定値を ROM から読み出す。次にステップ S 214 に進むと、安全機能診断処理部 1142 は、ステップ S 212 において RAM に書き込んだ演算結果と、ステップ S 213 において ROM から読み出した判定値とを比較し、両者が一致するか否かを判断する。このステップ S 214 の判断結果が「NO」である場合、処理は上述したステップ S 208 に進む。一方、ステップ S 214 の診断結果が「YES」である場合、処理はステップ S 215 に進む。次にステップ S 215 に進むと、安全機能診断処理部 1142 は、アクチュエータ制御処理部 113 は正常であると診断し、安全機能診断処理を終了する。

[0047] 以上が図 2 のステップ S 103 における安全機能診断処理の内容である。ステップ S 101 のプログラムシーケンス診断処理も基本的にこの安全機能診断処理と同様である。

[0048] 図 4～図 6 は、本実施形態の動作例を示すタイムチャートである。図 4 は、前掲図 2 において、プログラムシーケンス診断処理（ステップ S 101）および安全機能診断処理（ステップ S 103）の両診断においてアクチュエータ制御処理部 113 が正常であると診断される場合の動作例を示している。この場合、制御プロセッサ 11 では、図 4 に示すように、プログラムシーケンス診断処理、安全機能診断処理およびアクチュエータ制御処理からなる

処理が周期的に繰り返される。

[0049] ここで、WD T 1 2 がリセットされてからタイムアウトになるまでの目標計時時間は、1 周期分のプログラムシーケンス診断処理、安全機能診断処理およびアクチュエータ制御処理の全所要時間よりも長い。従って、WD T 1 2 がリセットされると、その後、WD T 1 2 の計時値が目標計時時間に到達するよりも前に、プログラムシーケンス診断処理（ステップ S 1 0 1）および安全機能診断処理（ステップ S 1 0 3）の両診断においてアクチュエータ制御処理部 1 1 3 が正常であると診断され、WD T 1 2 がリセットされる。従って、WD T 1 2 がタイムアウトとなってスイッチ回路 3 が遮断されることはない。

[0050] また、プログラムシーケンス診断処理（ステップ S 1 0 1）および安全機能診断処理（ステップ S 1 0 3）の両診断においてアクチュエータ制御処理部 1 1 3 が正常であると診断される場合、診断処理部 1 1 4 は異常信号を出力せず、安全状態移行処理部 1 1 6 は停止信号を制御信号出力処理部 1 1 5 に出力しない。従って、制御信号出力処理部 1 1 5 は、アクチュエータ制御処理部 1 1 3 が生成する制御信号を出力し、スイッチ回路 3 はこの制御信号を駆動回路 4 に供給する。

[0051] 図 5 は、前掲図 2 のプログラムシーケンス診断処理（ステップ S 1 0 1）においてアクチュエータ制御処理部の動作の異常が診断され、時刻 t_1 において診断処理部 1 1 4 から異常信号が出力（図 2 のステップ S 1 1 0）される動作例を示している。この異常信号が出力されると、安全状態移行処理部 1 1 6 は、停止信号を制御信号出力処理部 1 1 5 に出力する。この結果、図 5 に示すように、制御信号出力処理部 1 1 5 は、アクチュエータ制御処理部 1 1 3 が生成する制御信号の出力を停止する。

[0052] また、本実施形態において、WD T 1 2 の目標計時時間は、プログラムシーケンス診断処理が繰り返される周期よりも長い。このため、図 5 に例示するように、時刻 t_1 より後の時刻 t_2 において、WD T 1 2 の計時値が、目標計時時間に到達し、WD T 1 2 が遮断信号をスイッチ回路 3 に出力する。

この結果、スイッチ回路 3 はオフとなる。

[0053] このように本実施形態によれば、プログラムシーケンス診断処理部 1141 が制御プロセッサ 11 の動作異常を検知した場合に、WDT 12 がスイッチ回路 3 を遮断するよりも前に、安全状態移行処理部 116 が制御信号出力処理部 115 による制御信号の出力を停止させる。安全機能診断処理部 1142 が制御プロセッサ 11 の動作異常を検知した場合も同様である。従って、例えば WDT 12 が正常に働かない状況においても制御プロセッサ 11 の誤動作の影響が制御対象装置である駆動回路 4 およびアクチュエータ 5 に及ぶのを阻止することができる。

[0054] さらに、本実施形態によれば、制御プロセッサ 11 から異常報告信号を上位コントローラ 2 に出力するので、上位コントローラ 2 が制御プロセッサ 11 の動作異常を認識し、適切な対応をとることができる。また、本実施形態によれば、制御プロセッサ 11 は、異常診断時、自らをホールド状態に移行するので、制御プロセッサ 11 の動作異常が進行するのを止め、制御プロセッサ 11 が致命的な故障に陥るのを回避することができる。

[0055] 図 6 は、前掲図 2 において、プログラムシーケンス診断処理部 1141 がプログラムシーケンス診断処理（ステップ S101）の実行を開始した後、プログラムシーケンス診断処理部 1141 の動作異常が発生し、診断処理部 114 によってリセット信号が出力されることなく、WDT 12 の計時値が時刻 t_3 において目標計時時間に到達した動作例を示している。このように本実施形態によれば、プログラムシーケンス診断処理部 1141 の動作異常が発生した場合には、WDT 12 の計時値が目標計時時間に到達し、遮断信号によりスイッチ回路 3 がオフとされ、制御プロセッサ 11 の誤動作の影響が制御対象装置である駆動回路 4 およびアクチュエータ 5 に及ぶのを阻止することができる。安全機能診断処理部 1142 の動作異常が発生した場合も同様である。

[0056] <他の実施形態>

以上、この発明の一実施形態について説明したが、この発明には他にも実

施形態が考えられる。例えば次の通りである。

- [0057] (1) 上記実施形態では、図3のステップS201～S206において、アクチュエータ制御処理部113は入力データに基づく演算を2回行い、ステップS207においてプログラムシーケンス診断処理部1141が演算結果を比較したが、演算の回数は2回に限られない。アクチュエータ制御処理部113が演算を3回以上行い、プログラムシーケンス診断処理部1141が各演算の演算結果を比較してもよい。演算の回数を増やせば制御プロセッサ11の動作異常を検知しやすくなるが、制御プロセッサ11に負荷がかかるので、制御プロセッサ11の性能に応じて適宜演算の回数を決めればよい。
- [0058] (2) 上記実施形態では、プログラムシーケンス診断処理を実行した後に安全機能診断処理を実行していたが、この順番が逆であってもよい。また、図3のステップS210～S214の処理の後にステップS201～S207の処理を実行してもよい。
- [0059] (3) 上記実施形態では、アクチュエータ制御処理部113の演算結果を判定値と比較したが、アクチュエータ制御処理部113の演算の所要時間を所定の基準時間と比較することで制御プロセッサ11の動作異常を検知してもよい。また、例えば図3の安全機能診断処理において、ステップS202の演算の所要時間とステップS205の演算の所要時間を比較し、両所要時間の差が所定の閾値を越えている場合にアクチュエータ制御処理部113の動作が異常であると診断してもよい。また、制御プロセッサ11が例えば時分割制御により複数の処理を並行して進める場合には、各処理が行われる順序を監視し、各処理の順序が所定の順序でない場合に制御プロセッサ11の動作が異常であると診断してもよい。あるいは各処理の所要時間を所定の基準時間と比較し、いずれかの処理の所要時間と基準時間との差が所定の閾値を越えた場合に制御プロセッサ11の動作が異常であると診断してもよい。あるいは処理の順序に基づく判断と処理の所要時間に基づく判断とを併用して制御プロセッサ11の動作が異常であるか否かを診断してもよい。
- [0060] (4) 上記実施形態では、診断処理部114が異常信号を安全状態移行処理

部 1 1 6 に供給すると、安全状態移行処理部 1 1 6 が停止信号を制御信号出力処理部 1 1 5 に供給し、制御信号出力処理部 1 1 5 が制御信号の供給を停止した。しかし、この場合に安全状態移行処理部 1 1 6 は、制御信号出力処理部 1 1 5 に停止信号を供給する代わりに、安全状態に対応した制御信号の生成をアクチュエータ制御処理部 1 1 3 に行わせてもよい。ここで、安全状態とは、正常時よりも動作範囲の制限されたアクチュエータ 5 の駆動状態であり、速度が制限されたアクチュエータ 5 の駆動状態やアクチュエータ 5 の停止等が安全状態に含まれる。さらに、安全状態移行処理部 1 1 6 は、異常信号の内容に応じて安全状態に対応した制御信号の生成をアクチュエータ制御部 1 1 3 に行わせてもよい。そのために、異常信号の内容とその内容に応じた安全状態もしくは安全状態の決定方法を制御プロセッサ 1 1 の ROM や RAM が予め記憶していてもよい。制御プロセッサ 1 1 の動作異常が診断された場合、安全状態移行処理部 1 1 6 は、アクチュエータ 5 をこのような安全状態にするための制御信号をアクチュエータ制御処理部 1 1 3 に生成させるのである。

[0061] あるいは制御プロセッサ 1 1 の動作異常が診断された場合、安全状態移行処理部 1 1 6 は、アクチュエータ 5 を時間経過に伴って徐々に安全状態（例えば停止状態）に移行させる制御信号をアクチュエータ制御処理部 1 1 3 に生成させてもよい。

[0062] また、安全状態移行処理部 1 1 6 は、このような安全状態に対応した制御信号の生成を行わせる指示をアクチュエータ制御処理部 1 1 3 に送った後、所定時間が経過するのを待って、停止信号を制御信号出力処理部 1 1 5 に出力することが好ましい。また、診断処理部 1 1 4 は、安全状態移行処理部 1 1 6 が停止信号を制御信号出力処理部 1 1 5 に出力するまでの間、リセット信号を WDT 1 2 に供給し続けることが好ましい。これにより、所定時間の間は、アクチュエータ制御処理部 1 1 3 が生成する安全状態に対応した制御信号が駆動回路 4 に供給され、アクチュエータ 5 が制御される。この所定時間は、予め設定した一定時間でもよいし、制御プロセッサ 1 1 の異常検出時

におけるアクチュエータ 5 の動作速度等に応じて決定してもよい。この態様によれば、アクチュエータ 5 の急停止による事故を防止できる。

[0063] (5) 上記実施形態では、プログラムシーケンス診断処理、安全機能診断処理、アクチュエータ制御処理といったタスク単位での時分割制御により、プログラムシーケンス診断処理、安全機能診断処理、アクチュエータ制御処理を並行して進めることで、制御プロセッサ 11 による制御信号の生成と並行して制御プロセッサ 11 の診断を実施した。しかし、タスク単位よりも細かい時間単位での時分割制御によりプログラムシーケンス診断処理、安全機能診断処理、アクチュエータ制御処理を並行して進めてもよい。

[0064] 図 7 はプログラムシーケンス診断処理、安全機能診断処理、アクチュエータ制御処理の時分割制御の態様を示すタイムチャートである。この例では、時間軸は、ある時間長を持った複数のタイムスロットに分割されている。図 7 に示す例では、複数のタイムスロット c の各間にタイムスロット a または b が挟まれている。制御プロセッサ 11 は、離散した複数のタイムスロット c を利用して、アクチュエータ制御処理を実行する。また、制御プロセッサ 11 は、所定個数のタイムスロット a を利用してプログラムシーケンス診断処理を実行した後、所定個数のタイムスロット b を利用して安全機能診断処理を実行し、両診断処理において制御プロセッサの動作が正常であると診断された場合に WDT 12 にリセット信号を出力する動作を周期的に繰り返す。この態様によれば、複数のアクチュエータ制御処理間の時間間隔を狭くすることができる。従って、1 周期分のプログラムシーケンス診断処理および安全機能診断処理の所要時間が長い場合に有効である。

[0065] (6) この発明は複数の CPU コアを備えたマルチコア CPU を制御プロセッサ 11 とする駆動制御装置にも勿論適用可能である。この場合において、例えば複数の CPU コアにアクチュエータ制御処理を実行させ、各 CPU コアの演算結果を比較することにより、CPU コアの動作異常の有無を診断してもよい。この場合、周期的に、各 CPU コアの動作の異常が検出されたか否かを確認し、異常が検出されなかった場合は WDT 12 にリセット信号を

出力し、異常が検出された場合は制御プロセッサ 11 を安全状態に移行させるようにすればよい。

[0066] (7) 上記実施形態では、制御プロセッサ 11 の動作を診断するための診断処理部 114 をソフトウェアにより実現したが、診断処理部 114 をハードウェアにより実現してもよい。

符号の説明

[0067] 1 ……駆動制御装置、2 ……上位コントローラ、3 ……スイッチ回路、4 ……駆動回路、5 ……アクチュエータ、11 ……制御プロセッサ、12 ……WDT、111 ……通信処理部、112 ……指令入力処理部、113 ……アクチュエータ制御処理部、114 ……診断処理部、115 ……制御信号出力処理部、116 ……安全状態移行処理部、1141 ……プログラムシーケンス診断処理部、1142 ……安全機能診断処理部。

請求の範囲

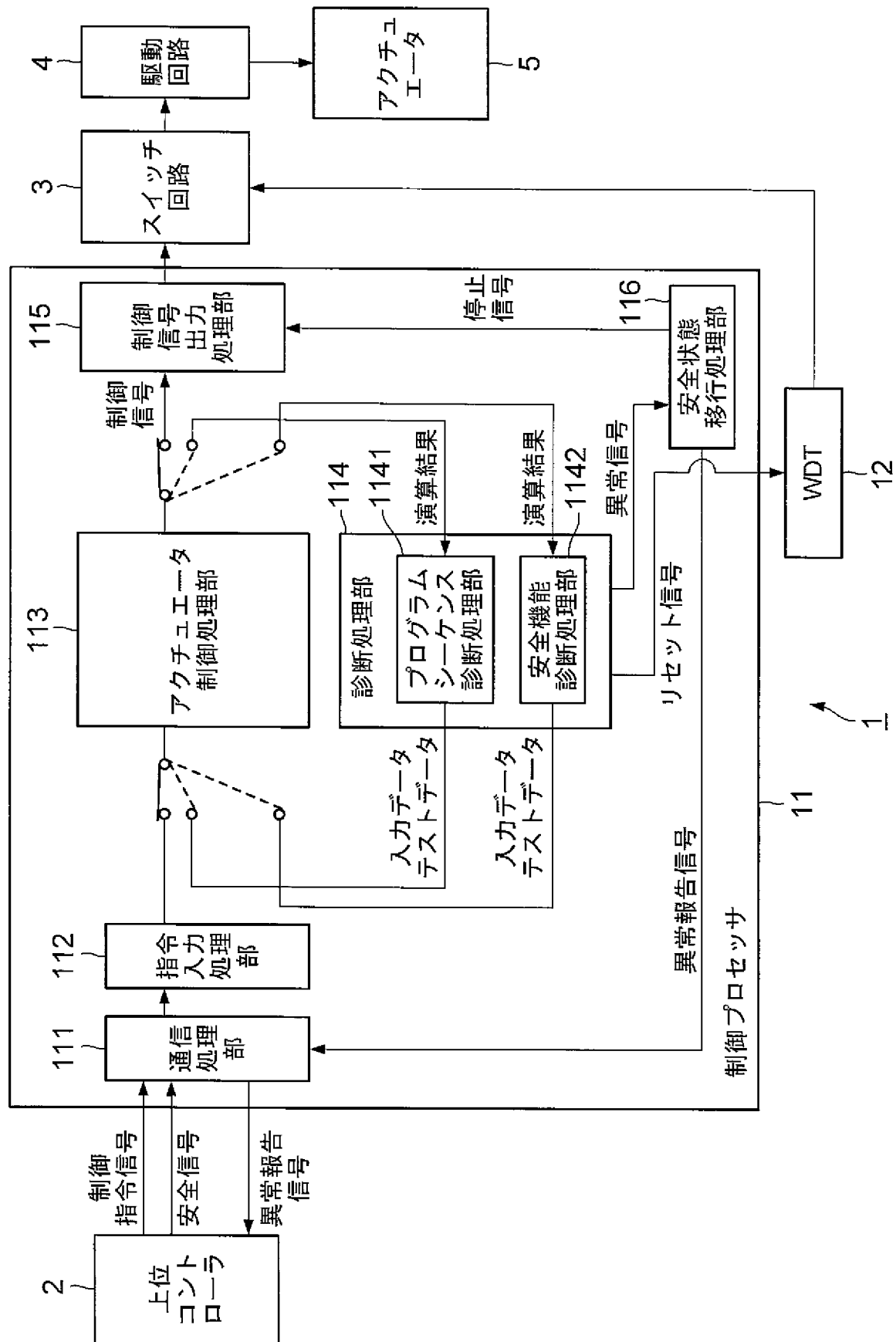
- [請求項1] 制御信号を生成する制御プロセッサと、
前記制御プロセッサから供給されるリセット信号に応じて計時値をリセットし、このリセット後、目標計時時間の計時を完了することによって、前記制御プロセッサから制御対象装置への制御信号の供給を遮断する遮断信号を継続的に出力するウォッチドッグタイマと
を具備することを特徴とする駆動制御装置。
- [請求項2] 前記制御プロセッサは、
当該制御プロセッサの動作の診断を行う診断手段と、
前記診断手段が当該制御プロセッサの動作に異常があると診断した場合に、正常時よりも動作範囲が制限された安全状態に当該制御プロセッサを移行させる安全状態移行処理手段と
を具備することを特徴とする請求項1に記載の駆動制御装置。
- [請求項3] 前記診断手段は、前記目標計時時間よりも短い周期で前記診断を繰り返し、前記制御プロセッサが正常であると診断した場合に前記リセット信号を出力することを特徴とする請求項2に記載の駆動制御装置。
- [請求項4] 前記安全状態移行処理手段は、前記診断手段が前記制御プロセッサの動作の異常を診断した場合に、前記制御対象装置を正常時よりも動作範囲の制限された安全状態とする制御信号を前記制御プロセッサから出力させることを特徴とする請求項2に記載の駆動制御装置。
- [請求項5] 前記安全状態移行処理手段は、前記診断手段が前記制御プロセッサの動作の異常を診断した場合に、前記制御プロセッサからの前記制御信号の出力を停止させることを特徴とする請求項4に記載の駆動制御装置。
- [請求項6] 前記安全状態移行処理手段は、前記診断手段が前記制御プロセッサの動作の異常を診断した場合に、前記制御対象装置の動作状態を時間経過に応じて所定の安全状態に移行させる制御信号を前記制御プロセ

ッサから出力させることを特徴とする請求項 4 に記載の駆動制御装置。
。

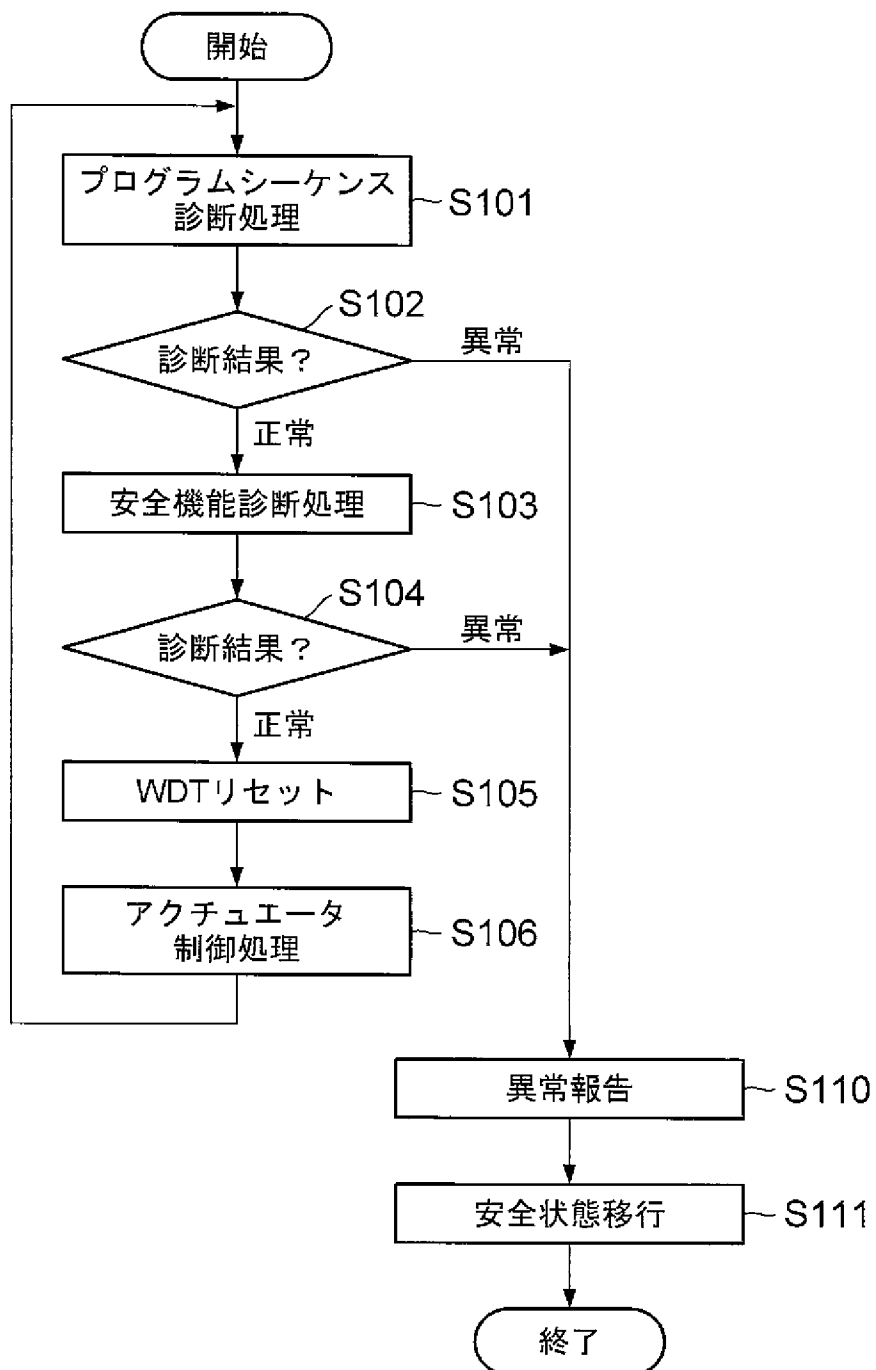
[請求項7] 前記制御プロセッサは、
 前記診断手段が前記制御プロセッサの動作の異常を診断した場合に、
 前記制御プロセッサの動作の異常を上位コントローラに通知する通
 信手段を具備することを特徴とする請求項 2 に記載の駆動制御装置。

[請求項8] 前記安全状態移行処理手段は、前記診断手段が前記制御プロセッサ
 の動作の異常を診断した場合に、前記制御プロセッサをホールド状態
 とすることを特徴とする請求項 2 に記載の駆動制御装置。

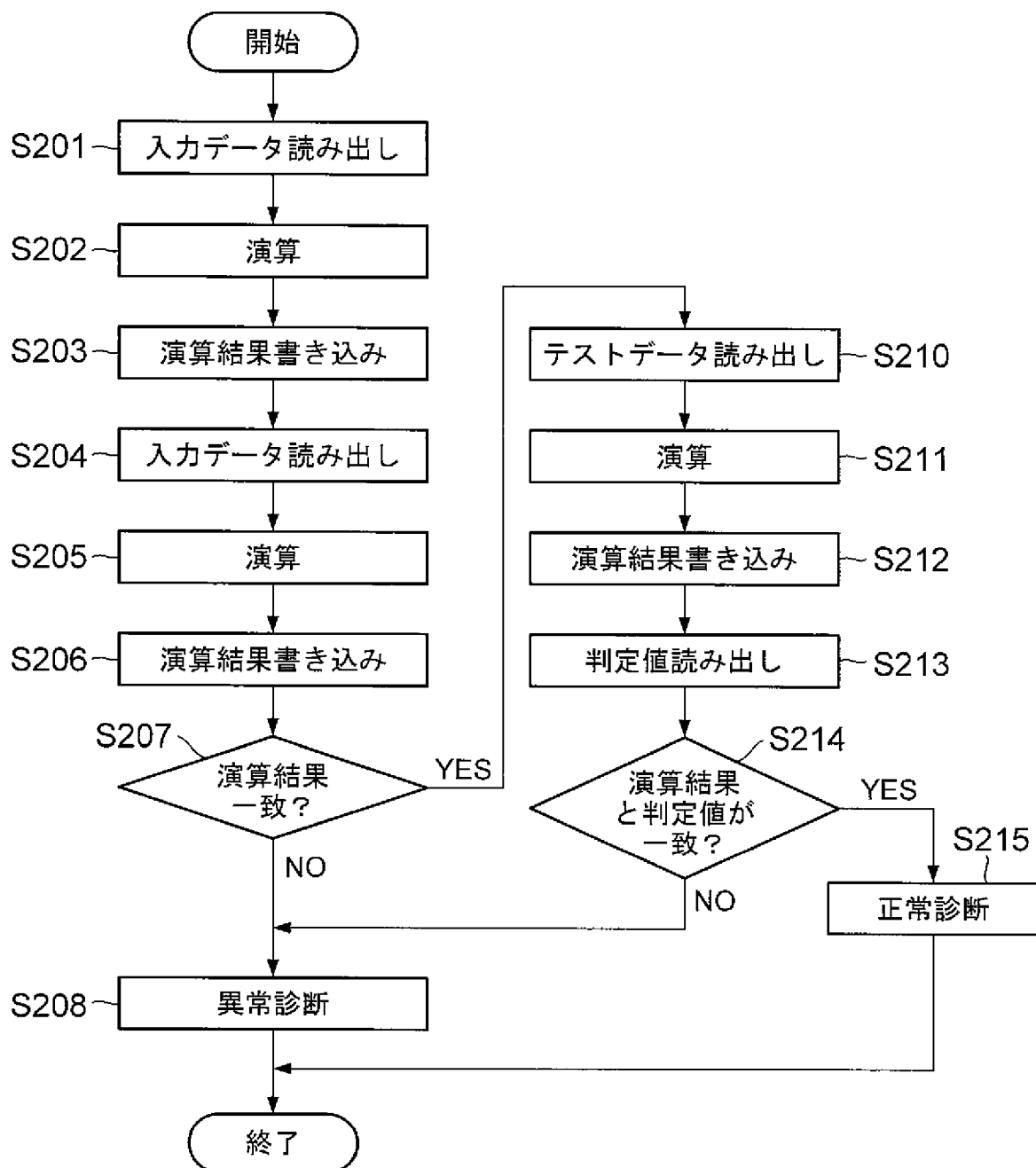
[図1]



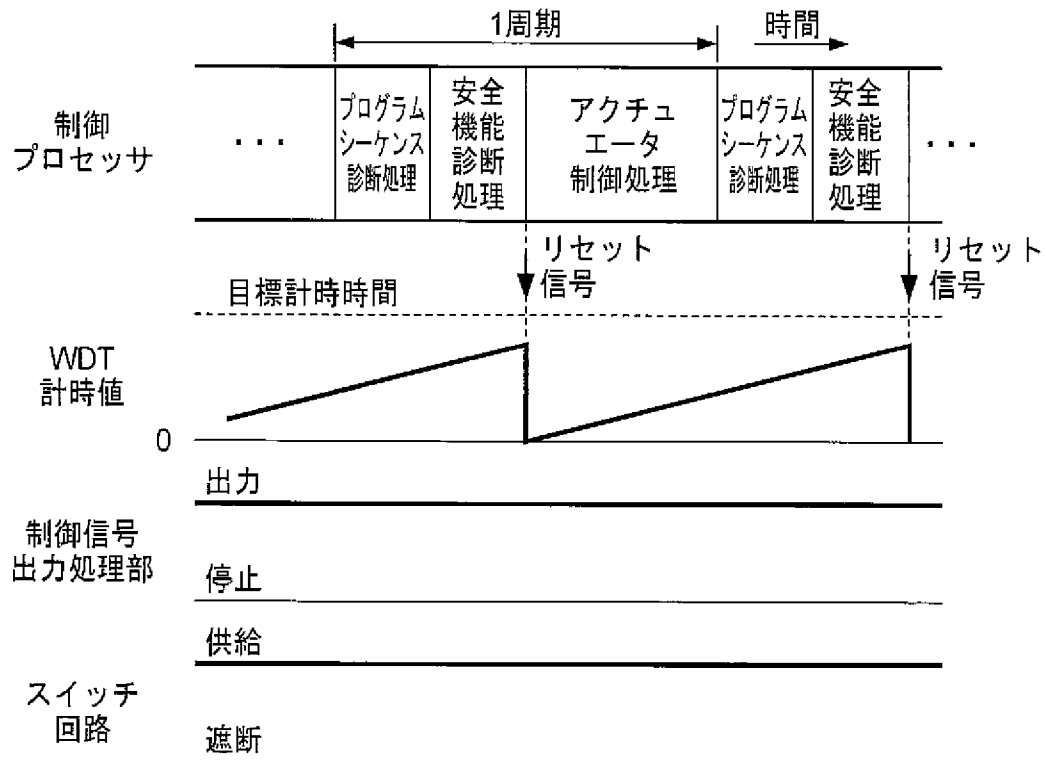
[図2]



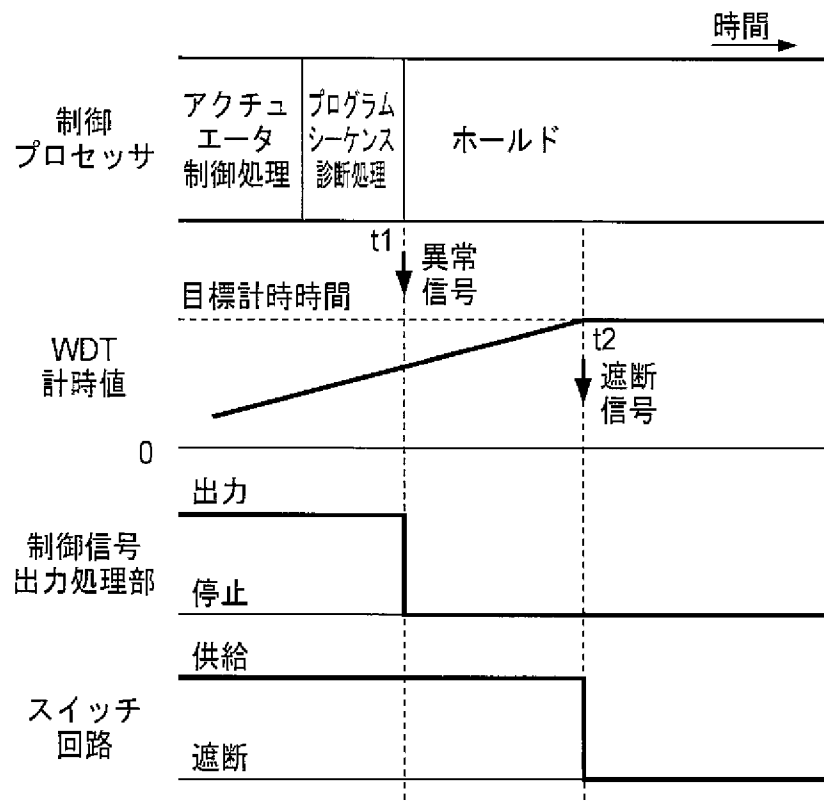
[図3]



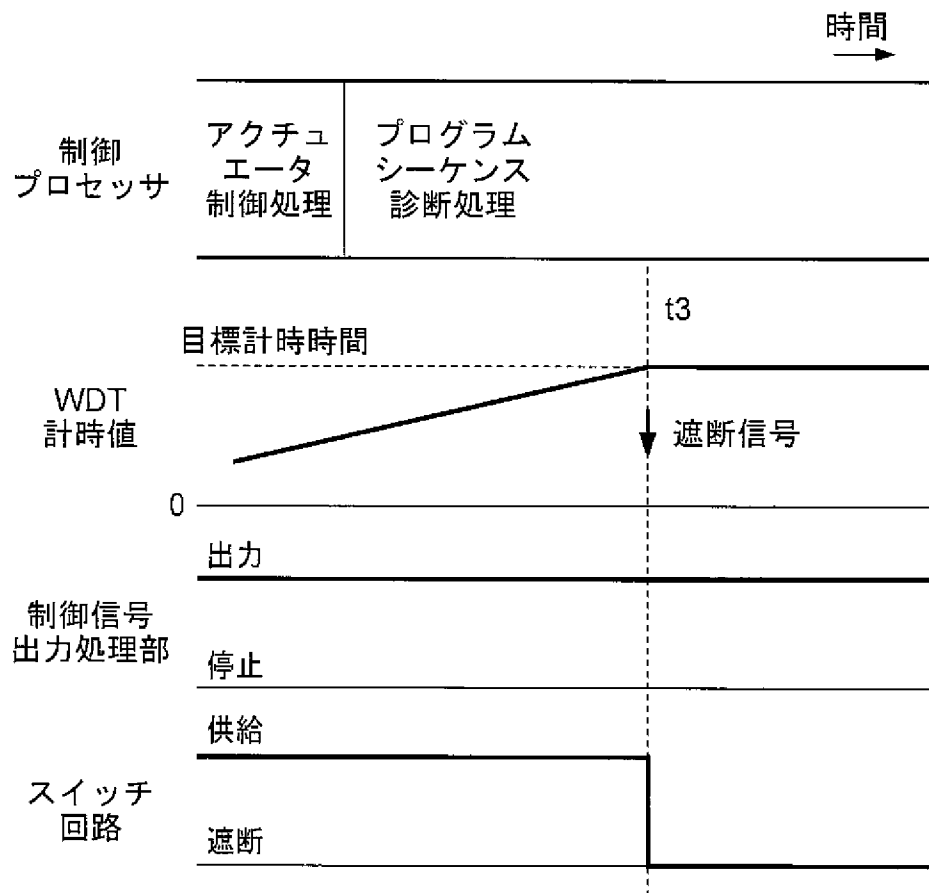
[図4]



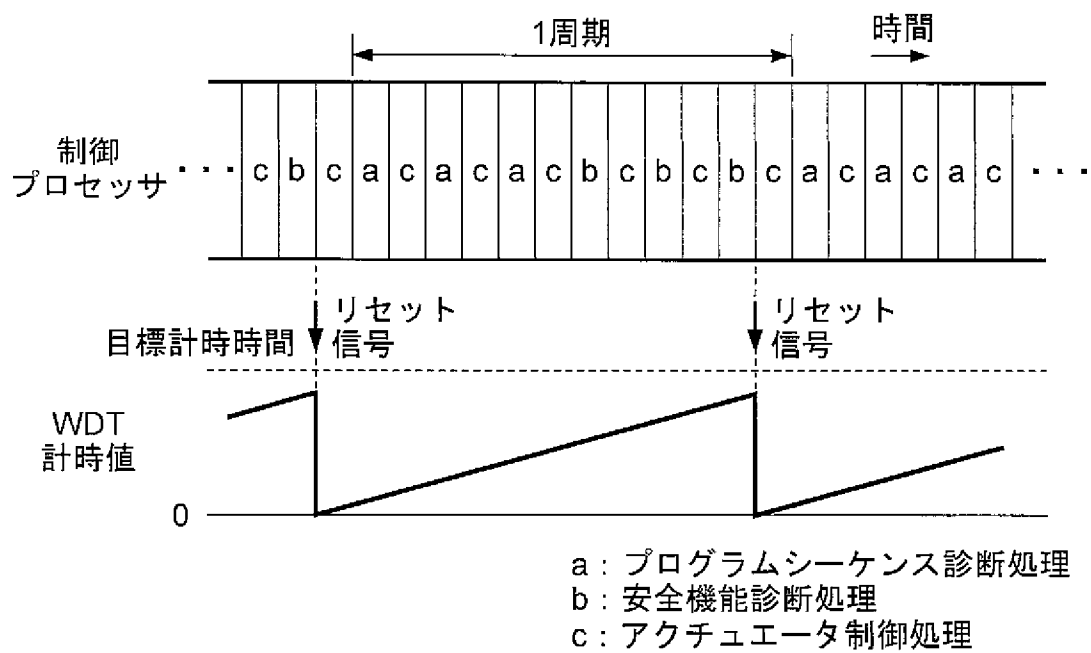
[図5]



[図6]



[図7]



INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2016/055278

A. CLASSIFICATION OF SUBJECT MATTER

G06F11/07(2006.01) i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

G06F11/07

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho	1922-1996	Jitsuyo Shinan Toroku Koho	1996-2016
Kokai Jitsuyo Shinan Koho	1971-2016	Toroku Jitsuyo Shinan Koho	1994-2016

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP 2014-048849 A (Fuji Electric Co., Ltd.), 17 March 2014 (17.03.2014), paragraphs [0011], [0042], [0084] to [0087] (Family: none)	1-8
Y	JP 11-053207 A (Koyo Seiko Co., Ltd.), 26 February 1999 (26.02.1999), paragraphs [0025] to [0027] (Family: none)	1-8
Y	JP 2002-089336 A (Nissan Motor Co., Ltd.), 27 March 2002 (27.03.2002), paragraphs [0018], [0034] (Family: none)	2-8

☒ Further documents are listed in the continuation of Box C.

☐ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search
18 May 2016 (18.05.16)

Date of mailing of the international search report
31 May 2016 (31.05.16)

Name and mailing address of the ISA/
Japan Patent Office
3-4-3, Kasumigaseki, Chiyoda-ku,
Tokyo 100-8915, Japan

Authorized officer

Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2016/055278

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP 2004-034746 A (Toyota Motor Corp.), 05 February 2004 (05.02.2004), paragraph [0011] (Family: none)	6
Y	JP 2011-061927 A (Hitachi, Ltd.), 24 March 2011 (24.03.2011), paragraphs [0073], [0078] (Family: none)	7
Y	JP 10-011408 A (Fujitsu Ltd.), 16 January 1998 (16.01.1998), paragraph [0127] (Family: none)	8

A. 発明の属する分野の分類（国際特許分類（IPC））

Int.Cl. G06F11/07(2006.01)i

B. 調査を行った分野

調査を行った最小限資料（国際特許分類（IPC））

Int.Cl. G06F11/07

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	1922-1996年
日本国公開実用新案公報	1971-2016年
日本国実用新案登録公報	1996-2016年
日本国登録実用新案公報	1994-2016年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

C. 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求項の番号
Y	JP 2014-048849 A（富士電機株式会社）2014.03.17, 段落[0011],[0042],[0084]-[0087]（ファミリーなし）	1-8
Y	JP 11-053207 A（光洋精工株式会社）1999.02.26, 段落[0025]-[0027]（ファミリーなし）	1-8
Y	JP 2002-089336 A（日産自動車株式会社）2002.03.27, 段落[0018],[0034]（ファミリーなし）	2-8

☒ C欄の続きにも文献が列挙されている。

☐ パテントファミリーに関する別紙を参照。

* 引用文献のカテゴリー

「A」特に関連のある文献ではなく、一般的技術水準を示すもの
「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
「O」口頭による開示、使用、展示等に言及する文献
「P」国際出願日前で、かつ優先権の主張の基礎となる出願

の日の後に公表された文献

「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Y」特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「&」同一パテントファミリー文献

国際調査を完了した日

18.05.2016

国際調査報告の発送日

31.05.2016

国際調査機関の名称及びあて先

日本国特許庁（ISA/J P）

郵便番号100-8915

東京都千代田区霞が関三丁目4番3号

特許庁審査官（権限のある職員）

多胡 滋

5B

3562

電話番号 03-3581-1101 内線 3545

C (続き) . 関連すると認められる文献		
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求項の番号
Y	JP 2004-034746 A (トヨタ自動車株式会社) 2004. 02. 05, 段落[0011] (ファミリーなし)	6
Y	JP 2011-061927 A (株式会社日立製作所) 2011. 03. 24, 段落[0073], [0078] (ファミリーなし)	7
Y	JP 10-011408 A (富士通株式会社) 1998. 01. 16, 段落[0127] (ファ ミリーなし)	8