(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
2014 年 3 月 20 日(20.03.2014)

WIPO | PCT

(10) 国際公開番号
WO 2014/041596 A1

(51) 国際特許分類:
G05B 19/05 (2006.01) *G05B 9/03* (2006.01)

(21) 国際出願番号: PCT/JP2012/073179

(22) 国際出願日: 2012 年 9 月 11 日(11.09.2012)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(71) 出願人 (米国を除く全ての指定国について): 三菱電機株式会社 (Mitsubishi Electric Corporation) [JP/JP]; 〒1008310 東京都千代田区丸の内二丁目７番３号 Tokyo (JP).

(72) 発明者; および

(75) 発明者/出願人 (米国についてのみ): 神余 浩夫 (KANAMARU, Hiroo) [—/JP]; 〒1008310 東京都千代田区丸の内二丁目７番３号 三菱電機株式会社内 Tokyo (JP). 浅野 義智 (ASANO, Yoshitomo) [—/JP]; 〒1008310 東京都千代田区丸の内二丁目７番３号 三菱電機株式会社内 Tokyo (JP). 谷藤圭一 (YATO, Keiichi) [—/JP]; 〒1008310 東京都千代田区丸の内二丁目７番３号 三菱電機株式会社内 Tokyo (JP).

(74) 代理人: 酒井 宏明 (SAKAI, Hiroaki); 〒1006020 東京都千代田区霞が関三丁目２番５号 霞が関ビルディング 酒井国際特許事務所 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, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, 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, 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, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, RU, TJ, TM), ヨーロッパ (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, ML, MR, NE, SN, TD, TG).

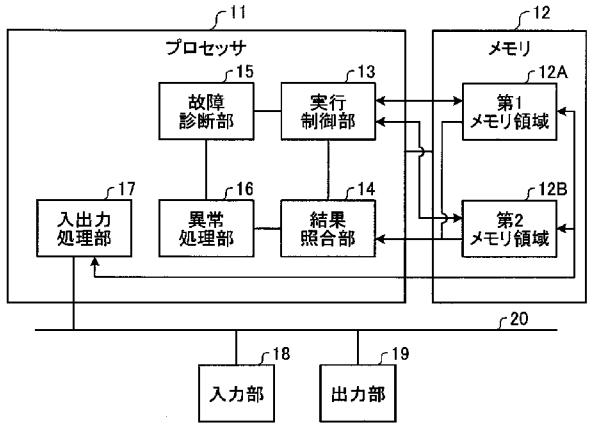
添付公開書類:

— 国際調査報告（条約第 21 条(3)）

(54) **Title**: SAFETY CONTROLLER

(54) 発明の名称 : 安全コントローラ

[図1]



11 Processor
12 Memory
12A First memory region
12B Second memory region
13 Execution controller
14 Result comparison unit
15 Fault diagnosis unit
16 Abnormality processor
17 Input/output processor
18 Input unit
19 Output unit

(57) **Abstract**: This invention has a processor (11) and a memory (12). The memory has a first memory region (12A), and a second memory region (12B) having a different address from that of the first memory region. The processor has: an execution controller (13) for executing a first process procedure including program processing of input data written into the first memory region, and a second process procedure including program processing of input data written into the second memory region and addition of redundancy code to output data written into the second memory region; a result comparison unit (14) for performing a comparison between output data to which the redundancy code has been added in the first process procedure and output data to which the redundancy code has been added in the second process procedure; a fault diagnosis unit (15) for diagnosing the presence or absence of a fault in the processor or the memory; and an abnormality processor (16) for discontinuing the outputting of the output data when an abnormality is detected in any one of the redundancy test, the comparison performed by the result comparison unit, and the diagnosis performed by the fault diagnosis unit.

(57) 要約:

[続葉有]

WO 2014/041596 A1

プロセッサ（１１）およびメモリ（１２）を有し、メモリは、第１メモリ領域（１２Ａ）と、第１メモリ領域とは異なるアドレスの第２メモリ領域（１２Ｂ）を有し、プロセッサは、第１メモリ領域に書き込まれた入力データのプログラム処理を含む第１処理過程と、第２メモリ領域に書き込まれた入力データのプログラム処理、および第２メモリ領域に書き込まれた出力データへの冗長符号の付与と、を含む第２処理過程と、を実行する実行制御部（１３）と、第１処理過程における冗長符号の付与を経た出力データ、および第２処理過程における冗長符号の付与を経た出力データを照合する結果照合部（１４）と、プロセッサおよびメモリの故障の有無を診断する故障診断部（１５）と、冗長検査、結果照合部における照合および故障診断部における診断の少なくともいずれかにおいて異常が検出された場合に、出力データの出力を停止させる異常処理部(１６)と、を有する。

明　細　書

発明の名称 ： 安全コントローラ

技術分野

[0001] 本発明は、安全コントローラ、特に、信頼性の高い制御動作を保障するための内部診断を実施する安全コントローラに関する。

背景技術

[0002] 安全制御のための安全コントローラは、例えば、機能安全に関する国際規格であるIEC61508にしたがって、プロセッサやメモリにおける回路の永続的な故障であるハードウェア故障と、一時的な故障であるソフトウェア故障との両方を検出可能であることが求められている。

[0003] 安全コントローラの内部診断については、例えば、２つのプロセッサの演算結果を照合して相互診断する手法や、１つのプロセッサにて同じ演算処理を２回実行して処理結果を比較する手法が知られている。例えば、特許文献１には、１つのプロセッサが同じ演算処理を２回実行した結果を別々のメモリに書き込む方法が開示されている。

先行技術文献

特許文献

[0004] 特許文献1：特開昭５９－１９４２０４号公報

発明の概要

発明が解決しようとする課題

[0005] 特許文献１に記載の構成によると、２つのメモリからの出力は、二重化されたデマルチプレクサとフリップフロップ回路とを用いて一重化される。プロセッサで演算処理を２回実行した結果の照合は、二重化されたハードウェア回路により実現される。この二重化された回路構成を採用する場合、一重の入出力回路からなる一般的な構成に比べて、冗長な回路構成が必要となる分、安全コントローラが複雑かつ高コストとなることが問題となる。

[0006] 本発明は、上記に鑑みてなされたものであって、一重の回路構成として簡

易かつ低コストを実現し、ハードウェア故障およびソフトウェア故障の両方を検出可能とする安全コントローラを得ることを目的とする。

課題を解決するための手段

[0007] 上述した課題を解決し、目的を達成するために、本発明は、入力データのプログラム処理を実施するプロセッサと、前記プロセッサへ入力される前記入力データ、および前記プログラム処理の結果である出力データを保持するメモリと、を有し、前記メモリは、第１メモリ領域と、前記第１メモリ領域とは異なるアドレスの第２メモリ領域と、のそれぞれに、前記入力データおよび前記出力データを保持可能であって、前記プロセッサは、前記第１メモリ領域に書き込まれた前記入力データの前記プログラム処理と、前記プログラム処理の結果として前記第１メモリ領域に書き込まれた前記出力データへの冗長符号の付与と、を含む第１処理過程と、前記第２メモリ領域に書き込まれた前記入力データの前記プログラム処理と、前記プログラム処理の結果として前記第２メモリ領域に書き込まれた前記出力データへの冗長符号の付与と、を含む第２処理過程と、を実行する実行制御部と、前記第１処理過程における前記冗長符号の付与を経た前記出力データと、前記第２処理過程における前記冗長符号の付与を経た前記出力データとを照合する結果照合部と、前記プロセッサおよび前記メモリの故障の有無を診断する故障診断部と、前記入力データおよび前記出力データの冗長検査、前記結果照合部における照合、および前記故障診断部における診断の少なくともいずれかにおいて異常が検出された場合に、前記出力データの出力を停止させる異常処理部と、を有することを特徴とする。

発明の効果

[0008] 本発明にかかる安全コントローラは、プロセッサおよびメモリを含む一重の回路構成を備える。実行制御部は、第１メモリ領域から読み出した入力データ、および第２メモリ領域から読み出した入力データに対し、それぞれプログラム処理を実行する。結果照合部は、双方の入力データについてのプログラム処理の結果を照合することで、ソフトウェア故障を検出する。故障診

断部は、プロセッサおよびメモリにおけるハードウェア故障を検出する。これにより、安全コントローラは、一重の回路構成として簡易かつ低コストを実現し、ハードウェア故障およびソフトウェア故障の両方を検出できるという効果を奏する。

図面の簡単な説明

[0009] [図1]図１は、本発明の実施の形態１にかかる安全コントローラの構成を示すブロック図である。

[図2]図２は、安全コントローラの動作手順を示すフローチャートである（その１）。

[図3]図３は、安全コントローラの動作手順を示すフローチャートである（その２）。

[図4]図４は、本発明の実施の形態２にかかる安全コントローラの動作手順を示すフローチャートである（その１）。

[図5]図５は、本発明の実施の形態２にかかる安全コントローラの動作手順を示すフローチャートである（その２）。

発明を実施するための形態

[0010] 以下に、本発明にかかる安全コントローラの実施の形態を図面に基づいて詳細に説明する。なお、この実施の形態によりこの発明が限定されるものではない。

[0011] 実施の形態１．

図１は、本発明の実施の形態１にかかる安全コントローラの構成を示すブロック図である。安全コントローラは、プロセッサ１１、メモリ１２、入力部１８および出力部１９を有する。プロセッサ１１、入力部１８および出力部１９は、バス２０を介して互いに接続されている。

[0012] 入力部１８は、安全コントローラへの入力データの入力を受け付ける。プロセッサ１１は、入力部１８へ入力された入力データのプログラム処理を実施する。メモリ１２は、プロセッサ１１へ入力される入力データ、およびプログラム処理の結果である出力データを保持する。出力部１９は、安全コン

トローラから外部へ出力データを出力する。

[0013] メモリ１２は、互いに独立した第１メモリ領域１２Ａおよび第２メモリ領域１２Ｂを有する。第２メモリ領域１２Ｂは、第１メモリ領域１２Ａとはアドレスが異なる。第１メモリ領域１２Ａおよび第２メモリ領域１２Ｂは、いずれも入力データおよび出力データを保持可能とされている。

[0014] プロセッサ１１は、実行制御部１３、結果照合部１４、故障診断部１５、異常処理部１６および入出力処理部１７を有する。実行制御部１３は、第１メモリ領域１２Ａに書き込まれた入力データについての第１処理過程と、第２メモリ領域１２Ｂに書き込まれた入力データについての第２処理過程とを実行する。結果照合部１４は、第１処理過程において第１メモリ領域１２Ａに書き込まれた出力データと、第２処理過程において第２メモリ領域１２Ｂに書き込まれた出力データとを照合する。

[0015] 故障診断部１５は、プロセッサ１１およびメモリ１２の故障の有無を診断する。異常処理部１６は、入力データおよび出力データの冗長検査、結果照合部１４における照合、および故障診断部１５における診断の少なくともいずれかにおいて異常が検出された場合に、出力データの出力を停止させる。

[0016] 入出力処理部１７は、入力部１８と第１メモリ領域１２Ａおよび第２メモリ領域１２Ｂとの間の入力データの転送と、出力部１９と第１メモリ領域１２Ａおよび第２メモリ領域１２Ｂとの間の出力データの転送とを行う。

[0017] 図２および図３は、安全コントローラの動作手順を示すフローチャートである。入力部１８は、入力された入力データに冗長符号を付与する。入出力処理部１７は、冗長符号が付与された入力データを入力部１８から読み込む。入出力処理部１７は、読み込んだ入力データを第１メモリ領域１２Ａおよび第２メモリ領域１２Ｂに書き込む（ステップＳ１）。

[0018] 実行制御部１３は、第１メモリ領域１２Ａへ書き込まれた入力データ（第１入力データ）に付随する冗長符号をチェックする（ステップＳ２）。冗長符号は、例えばＣＲＣ（Cyclic Redundancy Checking）とする。

[0019] かかる冗長検査において異常が検出された場合（ステップＳ３、Ｙｅｓ）

、異常処理部１６は、安全コントローラの動作を停止させる（ステップＳ１８）。一方、ステップＳ２の冗長検査により異常が無いことを確認すると（ステップＳ３、Ｎｏ）、実行制御部１３は、第１入力データのプログラム処理を実行する（ステップＳ４）。プログラムは、例えばユーザにより作成されたアプリケーションプログラムとする。実行制御部１３は、プログラム処理において、第１入力データと、第１メモリ領域１２Ａが保持する自己保存データとを用いる。

[0020] 実行制御部１３は、ステップＳ４における処理結果である出力データ（第１出力データ）を、第１メモリ領域１２Ａに書き込む（ステップＳ５）。実行制御部１３は、第１メモリ領域１２Ａが保持する自己保存データを、ステップＳ４における処理結果に応じて書き換える。

[0021] 実行制御部１３は、第１メモリ領域１２Ａへ書き込まれた第１出力データに冗長符号を付与する（ステップＳ６）。冗長符号は、例えばＣＲＣとする。ステップＳ２からステップＳ６は、第１メモリ領域１２Ａに書き込まれた第１入力データについての第１処理過程に相当する。

[0022] 次に、実行制御部１３は、第２メモリ領域１２Ｂへ書き込まれた入力データ（第２入力データ）に付随する冗長符号をチェックする（ステップＳ７）。冗長符号は、例えばＣＲＣとする。かかる冗長検査において異常が検出された場合（ステップＳ８、Ｙｅｓ）、異常処理部１６は、安全コントローラの動作を停止させる（ステップＳ１８）。一方、ステップＳ７の冗長検査により異常が無いことを確認すると（ステップＳ８、Ｎｏ）、実行制御部１３は、第２入力データのプログラム処理を実行する（ステップＳ９）。

[0023] 第１メモリ領域１２Ａおよび第２メモリ領域１２Ｂは、オフセットアドレスが異なる以外は、メモリマップは同一である。実行制御部１３は、第２入力データに対しては、ステップＳ４における第１入力データの処理のときとは異なるオフセットアドレスとして、同じプログラムを実行する。実行制御部１３は、プログラム処理において、第２入力データと、第２メモリ領域１２Ｂが保持する自己保存データとを用いる。

[0024] 実行制御部１３は、ステップＳ９における処理結果である出力データ（第２出力データ）を、第２メモリ領域１２Ｂに書き込む（ステップＳ１０）。実行制御部１３は、第２メモリ領域１２Ｂが保持する自己保存データを、ステップＳ９における処理結果に応じて書き換える。

[0025] 実行制御部１３は、第２メモリ領域１２Ｂへ書き込まれた第２出力データに冗長符号を付与する（ステップＳ１１）。冗長符号は、例えばＣＲＣとする。ステップＳ７からステップＳ１１は、第２メモリ領域１２Ｂに書き込まれた第２入力データについての第２処理過程に相当する。

[0026] 次に、結果照合部１４は、ステップＳ６における冗長符号の付与を経た第１出力データと、ステップＳ１１における冗長符号の付与を経た第２出力データとを比較照合する（ステップＳ１２）。結果照合部１４は、第１および第２出力データに加えて、値が変更される可能性のある自己保存データを、比較照合の範囲に含めることとしても良い。

[0027] 結果照合部１４での照合において異常が検出された場合（ステップＳ１３、Ｙｅｓ）、異常処理部１６は、安全コントローラの動作を停止させる（ステップＳ１８）。一方、結果照合部１４での照合に異常が無いことを確認すると（ステップＳ１３、Ｎｏ）、入出力処理部１７は、第１メモリ領域１２Ａから第１出力データを読み出し、第１出力データを出力部１９に書き込む。

[0028] 出力部１９は、入出力処理部１７によって書き込まれた第１出力データに付随する冗長符号をチェックする（ステップＳ１４）。かかる冗長検査において異常が検出された場合（ステップＳ１５、Ｙｅｓ）、異常処理部１６は、出力部１９による第１出力データの出力を停止させる（ステップＳ１８）。一方、ステップＳ１４の冗長検査により異常が無いことを確認すると（ステップＳ１５、Ｎｏ）、出力部１９は、第１出力データを出力する。

[0029] 次に、故障診断部１５は、プロセッサ１１およびメモリ１２の故障の有無を診断する（ステップＳ１６）。故障診断部１５は、プロセッサ１１のＡＬＵ（Arithmetic and Logic Unit）に対し、テストパターンを使用して診

断を行う。テストパターンとしては、ＡＬＵのレジスタの各ビットが独立してＯＮ／ＯＦＦできることを確認可能であるものを選択する。

[0030] 例えば、和算を行うＡＬＵの場合、演算対象となる２つのレジスタの各ビット（０，０），（０，１），（１，０），（１，１）の確認と、下位ビットからのキャリー演算を実施する。さらに、隣接しているメモリビット間にショートが無いことを確認するために、テストパターンとしては、隣接ビットが異なる結果となるもの（０ｘ５５５５および０ｘＡＡＡＡ）を選択する。

[0031] 故障診断部１５は、第１メモリ領域１２Ａおよび第２メモリ領域１２Ｂの指定されたアドレスに対し、互いに異なるテストパターンの書き込みおよび読み出しを行う。第１メモリ領域１２Ａおよび第２メモリ領域１２Ｂは、互いに異なるオフセットアドレスと、同じメモリマップとを持つ。同じテストパターンでは、オフセットアドレスラインが固着する故障があっても、第１メモリ領域１２Ａおよび第２メモリ領域１２Ｂの同じアドレスに同じ値が書き込まれることとなり、正確な故障診断が困難となる。故障診断部１５は、第１メモリ領域１２Ａおよび第２メモリ領域１２Ｂの指定されたアドレスに予め異なる値を書き込み、読み出された値と書き込み時の値とを比較することで、アドレスラインの故障を診断する。

[0032] プロセッサ１１およびメモリ１２の故障診断において異常が検出された場合（ステップＳ１７、Ｙｅｓ）、すなわちプロセッサ１１およびメモリ１２の少なくともいずれかに故障があった場合、異常処理部１６は、安全コントローラの動作を停止させる（ステップＳ１８）。

[0033] 一方、プロセッサ１１およびメモリ１２の故障診断により異常が無いこと、すなわちプロセッサ１１およびメモリ１２のいずれにも故障が無いことを確認すると（ステップＳ１７、Ｎｏ）、安全コントローラは、ステップＳ１に戻って、安全制御のための動作を継続する。

[0034] 安全コントローラは、入力データおよび出力データの冗長検査、結果照合部１４における照合、および故障診断部１５における診断の少なくともいず

れかにおいて異常が検出された場合、ステップＳ１８における動作の停止により、無為の無限ループ状態となる。これにより、安全コントローラは、異常を検出した時点で、出力データの出力を停止させる。

[0035] 安全コントローラは、プロセッサ１１およびメモリ１２のいずれかにソフトウェア故障が発生した場合、結果照合部１４による照合結果から、故障の発生を検出することができる。なお、安全コントローラは、ソフトウェア故障があった場合に、動作を停止させる以外に、所定の処置を施した上で動作を継続することとしても良い。

[0036] ソフトウェア故障は、ソフトウェア処理におけるある周期にて検出されても、次周期以降には解消されることがあり得る。安全コントローラは、例えば、故障が検出された周期の直前の周期における出力データを当該周期に適用することで、エラー扱いとせず次周期以降の処理を継続することとしても良い。安全コントローラは、所定回数の周期にて連続して故障を検出した場合に、動作を停止させることとしても良い。

[0037] 安全コントローラは、プロセッサ１１およびメモリ１２のいずれかにハードウェア故障が発生した場合、故障診断部１５による診断結果から、故障の発生を検出することができる。ハードウェア故障は、ソフトウェア処理のある周期にて検出されれば、次周期以降も解消されないこととなる。このため、安全コントローラは、ハードウェア故障を検出した場合、直ちに動作を停止させる。

[0038] 安全コントローラは、プロセッサ１１、メモリ１２、入力部１８および出力部１９からなる一重の回路構成を採用する。安全コントローラは、二重化されたハードウェア構造を採用しなくても、ハードウェア故障およびソフトウェア故障の両方を検出することができる。安全コントローラは、一重の回路構成として簡易かつ低コストを実現できる。

[0039] 実施の形態２．

図４および図５は、本発明の実施の形態２にかかる安全コントローラの動作手順を示すフローチャートである。本実施の形態にかかる安全コントロー

ラは、実施の形態１にかかる安全コントローラ（図１参照）と同様の構成を備える。本実施の形態における動作手順のうちステップＳ１からステップＳ９の手順は、実施の形態１における動作手順のステップＳ１からＳ９（図２参照）と同様である。

[0040] 実行制御部１３は、ステップＳ９における処理結果である出力データ（第２出力データ）を、ビット反転させる（ステップＳ２０）。実行制御部１３は、ビット反転を経た第２出力データを、第２メモリ領域１２Ｂに書き込む（ステップＳ１０）。また、実行制御部１３は、第２メモリ領域１２Ｂが保持する自己保存データを、ステップＳ９における処理結果に応じて書き換えるとともに、ビット反転させる。

[0041] 実行制御部１３は、第２メモリ領域１２Ｂへ書き込まれた第２出力データに冗長符号を付与する（ステップＳ１１）。冗長符号は、例えばＣＲＣとする。ステップＳ７からステップＳ１１は、第２メモリ領域１２Ｂに書き込まれた第２入力データについての第２処理過程に相当する。

[0042] 次に、結果照合部１４は、ステップＳ６における冗長符号の付与を経た第１出力データと、ステップＳ１１における冗長符号の付与を経た第２出力データとを比較照合する（ステップＳ１２）。ステップＳ１２において、結果照合部１４は、互いの排他論理和を求める手法により、第１出力データと第２出力データとを照合する。その後ステップＳ１３からステップＳ１５の動作手順は、実施の形態１におけるステップＳ１３からステップＳ１５の動作手順と同様である。

[0043] ステップＳ１４の冗長検査により異常が無いことを確認すると（ステップＳ１５、Ｎｏ）、出力部１９は、第１出力データを出力する。次に、故障診断部１５は、プロセッサ１１の故障の有無を診断する（ステップＳ２１）。第１メモリ領域１２Ａが保持する第１出力データに対し、第２メモリ領域１２Ｂが保持する第２出力データは、ステップＳ２０におけるビット反転を経ている。アドレスラインの故障は、第１出力データと第２出力データとを比較照合することで検出できる。よって、実施の形態２では、故障診断部１５

によるメモリ１２の故障診断は不要となる。

[0044] ステップＳ１７およびステップＳ１８の動作手順は、実施の形態１におけるステップＳ１７およびステップＳ１８の動作手順と同様である。実施の形態２にかかる安全コントローラは、実施の形態１と同様に、一重の回路構成として簡易かつ低コストを実現し、ハードウェア故障およびソフトウェア故障の両方を検出することができる。

[0045] 実施の形態３．

実施の形態３にかかる安全コントローラは、実施の形態１にかかる安全コントローラ（図１参照）と同様の構成を備える。本実施の形態にかかる安全コントローラの動作手順は、実施の形態２にかかる安全コントローラの動作手順（図４および図５参照）のうちステップＳ２０において、ビット反転に代えて、補数への変換を行う。ここで、本実施の形態の動作手順を、図４および図５のフローチャートを参照して説明する。

[0046] 実行制御部１３は、ステップＳ９における処理結果である出力データ（第２出力データ）を、補数へ変換する。実行制御部１３は、補数への変換を経た第２出力データを、第２メモリ領域１２Ｂに書き込む（ステップＳ１０）。また、実行制御部１３は、第２メモリ領域１２Ｂが保持する自己保存データを、ステップＳ９における処理結果に応じて書き換えるとともに、補数に変換する。

[0047] 結果照合部１４は、ステップＳ６における冗長符号の付与を経た第１出力データと、ステップＳ１１における冗長符号の付与を経た第２出力データとを比較照合する（ステップＳ１２）。ステップＳ１２において、結果照合部１４は、互いの和がゼロであるか否かにより、第１出力データと第２出力データとを照合する。その後の動作手順は、実施の形態２におけるステップＳ１３からステップＳ１８の動作手順と同様である。

[0048] 実施の形態３では、実施の形態２と同様、第１メモリ領域１２Ａに書き込まれる第１出力データと第２メモリ領域１２Ｂに書き込まれる第２出力データとは異なる値である。アドレスラインの故障は、第１出力データと第２出

力データとを比較照合することで検出できる。よって、実施の形態３では、故障診断部１５によるメモリ１２の故障診断は不要となる。

[0049] 実施の形態３にかかる安全コントローラは、実施の形態１および２と同様に、一重の回路構成として簡易かつ低コストを実現し、ハードウェア故障およびソフトウェア故障の両方を検出することができる。

[0050] 実施の形態４.

実施の形態４にかかる安全コントローラは、実施の形態１にかかる安全コントローラ（図１参照）と同様の構成を備える。本実施の形態にかかる安全コントローラの動作手順は、実施の形態２にかかる安全コントローラの動作手順（図４および図５参照）のうちステップＳ２０において、ビット反転に代えて、エンディアンを逆転させる変換を行う。ここで、本実施の形態の動作手順を、図４および図５のフローチャートを参照して説明する。

[0051] 実行制御部１３は、ステップＳ９における処理結果である出力データ（第２出力データ）について、例えば１６ビットデータの上位ビットおよび下位ビットを逆にする変換を行う。実行制御部１３は、エンディアンの逆転を経た第２出力データを、第２メモリ領域１２Ｂに書き込む（ステップＳ１０）。また、実行制御部１３は、第２メモリ領域１２Ｂが保持する自己保存データを、ステップＳ９における処理結果に応じて書き換えるとともに、エンディアンを逆転させる。

[0052] 結果照合部１４は、ステップＳ６における冗長符号の付与を経た第１出力データと、ステップＳ１１における冗長符号の付与を経た第２出力データとを比較照合する（ステップＳ１２）。その際、結果照合部１４は、第２メモリ領域１２Ｂが保持する第２出力データを、エンディアンを逆転させて読み出す。結果照合部１４は、第１出力データと、エンディアンの逆転を経た第２出力データとを照合する。その後の動作手順は、実施の形態２におけるステップＳ１３からステップＳ１８の動作手順と同様である。

[0053] 実施の形態４では、実施の形態２および３と同様、第１メモリ領域１２Ａに書き込まれる第１出力データと第２メモリ領域１２Ｂに書き込まれる第２

出力データとは異なる値である。アドレスラインの故障は、第１出力データと第２出力データとを比較照合することで検出できる。よって、実施の形態４では、故障診断部１５によるメモリ１２の故障診断は不要となる。

[0054] 実施の形態４にかかる安全コントローラは、実施の形態１から３と同様に、一重の回路構成として簡易かつ低コストを実現し、ハードウェア故障およびソフトウェア故障の両方を検出することができる。

[0055] 実施の形態４にかかる安全コントローラは、ステップＳ４における処理結果である出力データ（第１出力データ）についてエンディアンを逆転させることとしても良い。結果照合部１４は、比較照合の際に、第１メモリ領域１２Ａが保持する第１出力データ、および第２メモリ領域１２Ｂが保持する第２出力データのいずれについて、エンディアンを逆転させて読み出すこととしても良い。

[0056] 実施の形態５.

実施の形態５にかかる安全コントローラは、実施の形態１にかかる安全コントローラ（図１参照）と同様の構成を備える。本実施の形態にかかる安全コントローラの動作手順は、実施の形態１にかかる安全コントローラの動作手順（図２および図３参照）と同様である。ここで、本実施の形態の動作手順を、図２および図３のフローチャートを参照して説明する。

[0057] 第１入力データのプログラム処理（ステップＳ４）において、実行制御部１３は、１６ビット向けのコンパイラとして生成されたプログラムを使用する。一方、第２入力データのプログラム処理（ステップＳ９）において、実行制御部１３は、３２ビット向けのコンパイラとして生成されたプログラムを使用する。

[0058] コントローラが扱うデータのほとんどは、１６ビットデータである。実行制御部１３は、ステップＳ４において、１６ビットである第１入力データをレジスタにロードし、１６ビット命令を実行する。実行制御部１３は、処理結果である１６ビットの第１出力データを第１メモリ領域１２Ａに書き込む（ステップＳ５）。

[0059] また、プロセッサ１１は、ステップＳ９において、１６ビットである第２入力データをレジスタにロードし、３２ビット命令を実行する。実行制御部１３は、処理結果である１６ビットの第２出力データを第２メモリ領域１２Ｂに書き込む（ステップＳ１０）。

[0060] 実施の形態５では、第１入力データおよび第２入力データに対して実行する命令が互いに異なる。結果照合部１４は、第１出力データと第２出力データとの比較照合により、プロセッサ１１のソフトウェア故障およびハードウェア故障を検出することができる。よって、実施の形態５では、故障診断部１５によるプロセッサ１１の故障診断は不要となる。

[0061] 実施の形態５にかかる安全コントローラは、実施の形態１から４と同様に、一重の回路構成として簡易かつ低コストを実現し、ハードウェア故障およびソフトウェア故障の両方を検出することができる。

産業上の利用可能性

[0062] 本発明の安全コントローラは、機械や設備の安全制御を担う安全コントローラとして有用である。

符号の説明

[0063] １１　プロセッサ、１２　メモリ、１２Ａ　第１メモリ領域、１２Ｂ　第２メモリ領域、１３　実行制御部、１４　結果照合部、１５　故障診断部、１６　異常処理部、１７　入出力処理部、１８　入力部、１９　出力部、２０　バス。

請求の範囲

［請求項1］ 入力データのプログラム処理を実施するプロセッサと、

前記プロセッサへ入力される前記入力データ、および前記プログラム処理の結果である出力データを保持するメモリと、を有し、

前記メモリは、第１メモリ領域と、前記第１メモリ領域とは異なるアドレスの第２メモリ領域と、のそれぞれに、前記入力データおよび前記出力データを保持可能であって、

前記プロセッサは、

前記第１メモリ領域に書き込まれた前記入力データの前記プログラム処理と、前記プログラム処理の結果として前記第１メモリ領域に書き込まれた前記出力データへの冗長符号の付与と、を含む第１処理過程と、前記第２メモリ領域に書き込まれた前記入力データの前記プログラム処理と、前記プログラム処理の結果として前記第２メモリ領域に書き込まれた前記出力データへの冗長符号の付与と、を含む第２処理過程と、を実行する実行制御部と、

前記第１処理過程における前記冗長符号の付与を経た前記出力データと、前記第２処理過程における前記冗長符号の付与を経た前記出力データとを照合する結果照合部と、

前記プロセッサおよび前記メモリの故障の有無を診断する故障診断部と、

前記入力データおよび前記出力データの冗長検査、前記結果照合部における照合、および前記故障診断部における診断の少なくともいずれかにおいて異常が検出された場合に、前記出力データの出力を停止させる異常処理部と、を有することを特徴とする安全コントローラ。

［請求項2］ 前記実行制御部は、前記第２処理過程において、ビット反転させた前記出力データを前記第２メモリ領域に書き込み、

前記結果照合部は、前記第１メモリ領域から読み出した前記出力データと、前記第２メモリ領域から読み出した前記出力データとを、互

いの排他論理和により照合することを特徴とする請求項１に記載の安全コントローラ。

［請求項3］ 前記実行制御部は、前記第２処理過程において、補数への変換を経た前記出力データを前記第２メモリ領域に書き込み、

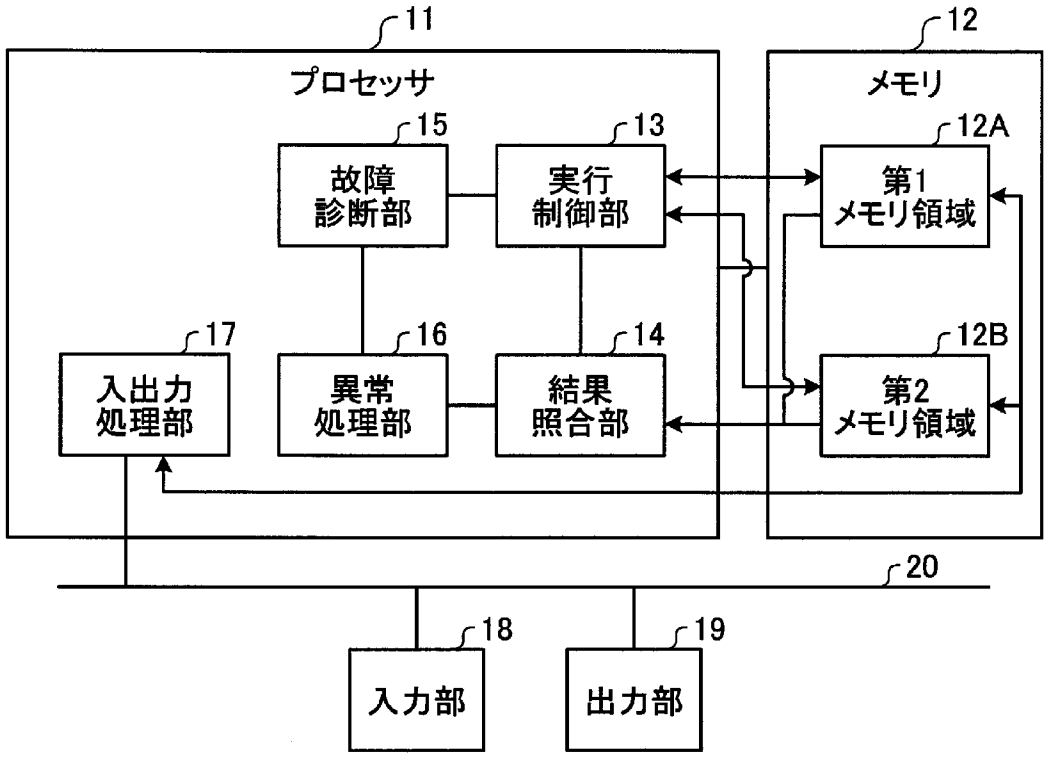
前記結果照合部は、前記第１メモリ領域から読み出した前記出力データと、前記第２メモリ領域から読み出した前記出力データとを、互いの和により照合することを特徴とする請求項１に記載の安全コントローラ。

［請求項4］ 前記実行制御部は、前記第１メモリ領域に書き込む前記出力データと前記第２メモリ領域に書き込む前記出力データとのうちの一方について、エンディアンを逆転させ、

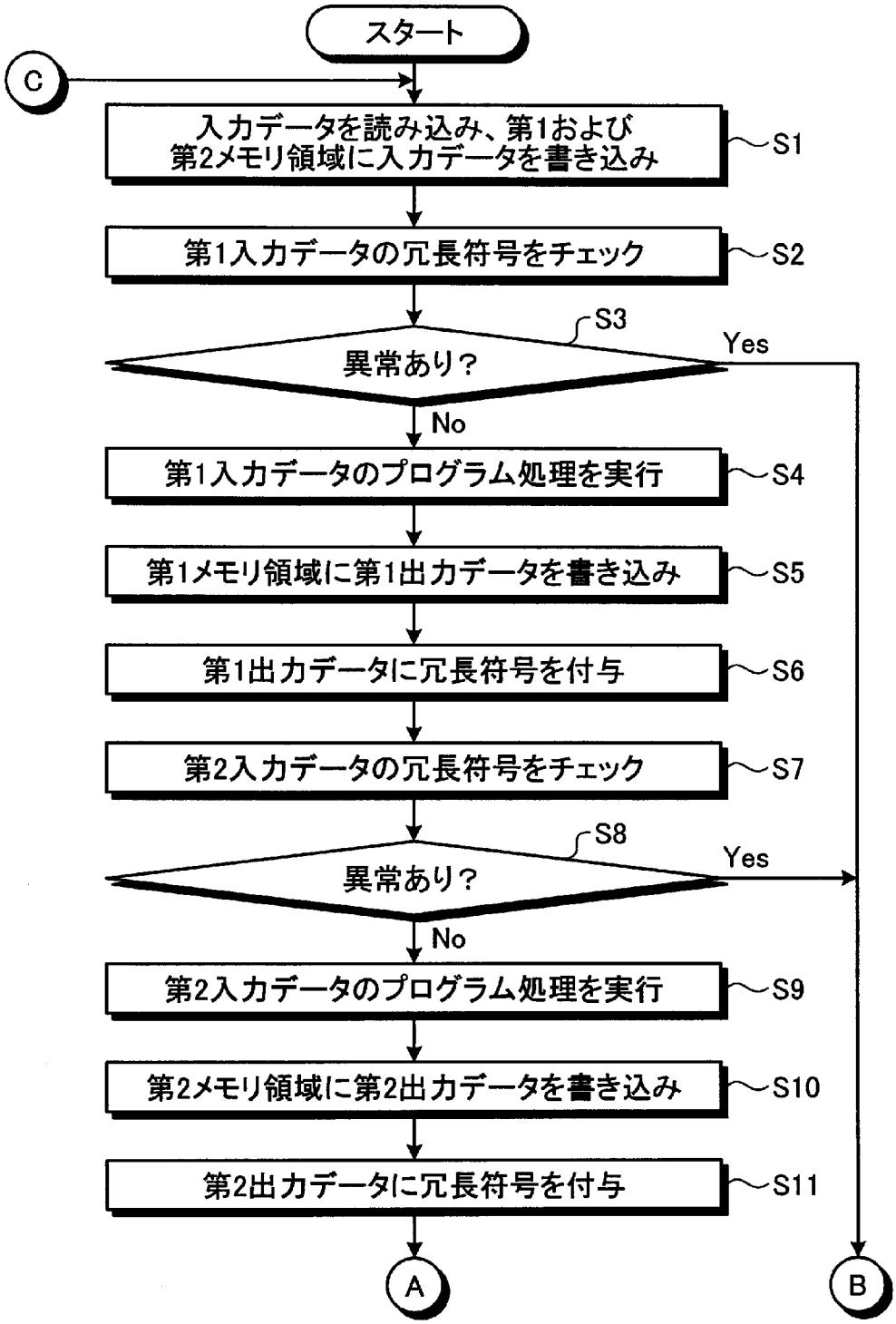
前記結果照合部は、前記第１メモリ領域から読み出した前記出力データと前記第２メモリ領域から読み出した前記出力データとのうちの一方についてエンディアンを逆転させて、照合することを特徴とする請求項１に記載の安全コントローラ。

［請求項5］ 前記実行制御部は、前記第１メモリ領域から読み出した前記入力データの前記プログラム処理において、１６ビット向けのコンパイラとして生成されたプログラムを使用し、かつ、前記第２メモリ領域から読み出した前記入力データの前記プログラム処理において、３２ビット向けのコンパイラとして生成されたプログラムを使用することを特徴とする請求項１に記載の安全コントローラ。

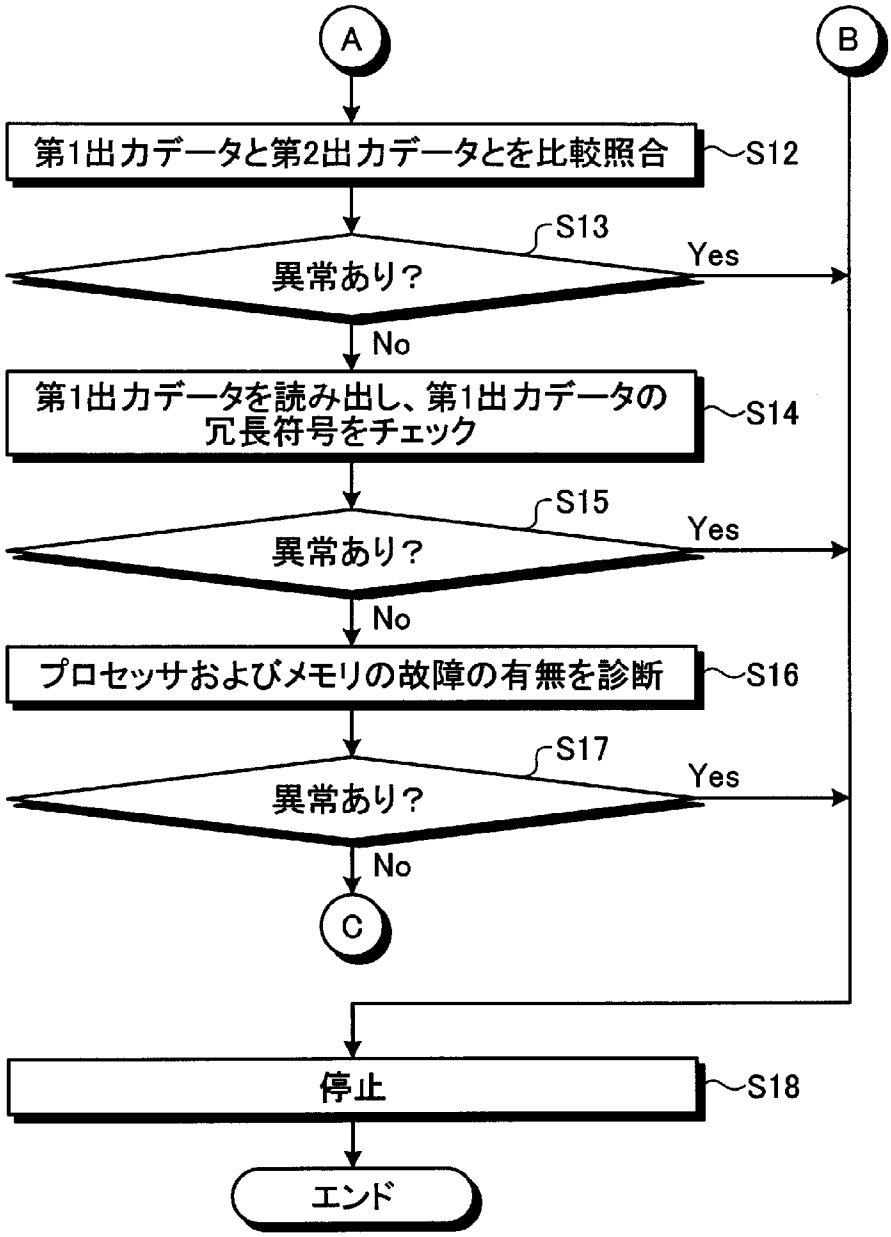
[図1]


11
プロセッサ
12
メモリ
15
故障
診断部
13
実行
制御部
12A
第1
メモリ領域
17
入出力
処理部
16
異常
処理部
14
結果
照合部
12B
第2
メモリ領域
20
18
入力部
19
出力部

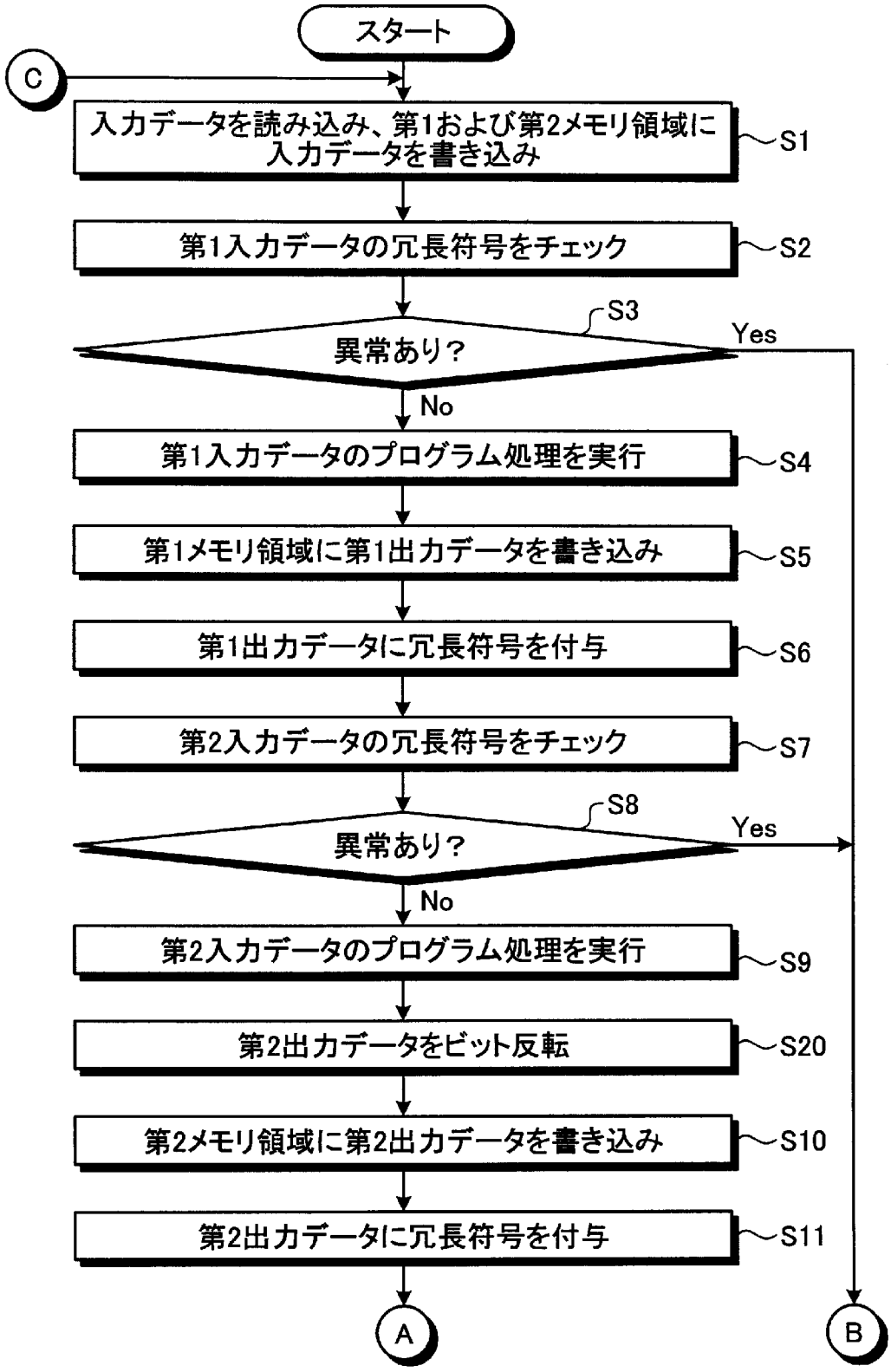
[図2]


スタート
C
入力データを読み込み、第1および第2メモリ領域に入力データを書き込み
S1
第1入力データの冗長符号をチェック
S2
S3
異常あり？
Yes
No
第1入力データのプログラム処理を実行
S4
第1メモリ領域に第1出力データを書き込み
S5
第1出力データに冗長符号を付与
S6
第2入力データの冗長符号をチェック
S7
S8
異常あり？
Yes
No
第2入力データのプログラム処理を実行
S9
第2メモリ領域に第2出力データを書き込み
S10
第2出力データに冗長符号を付与
S11
A
B

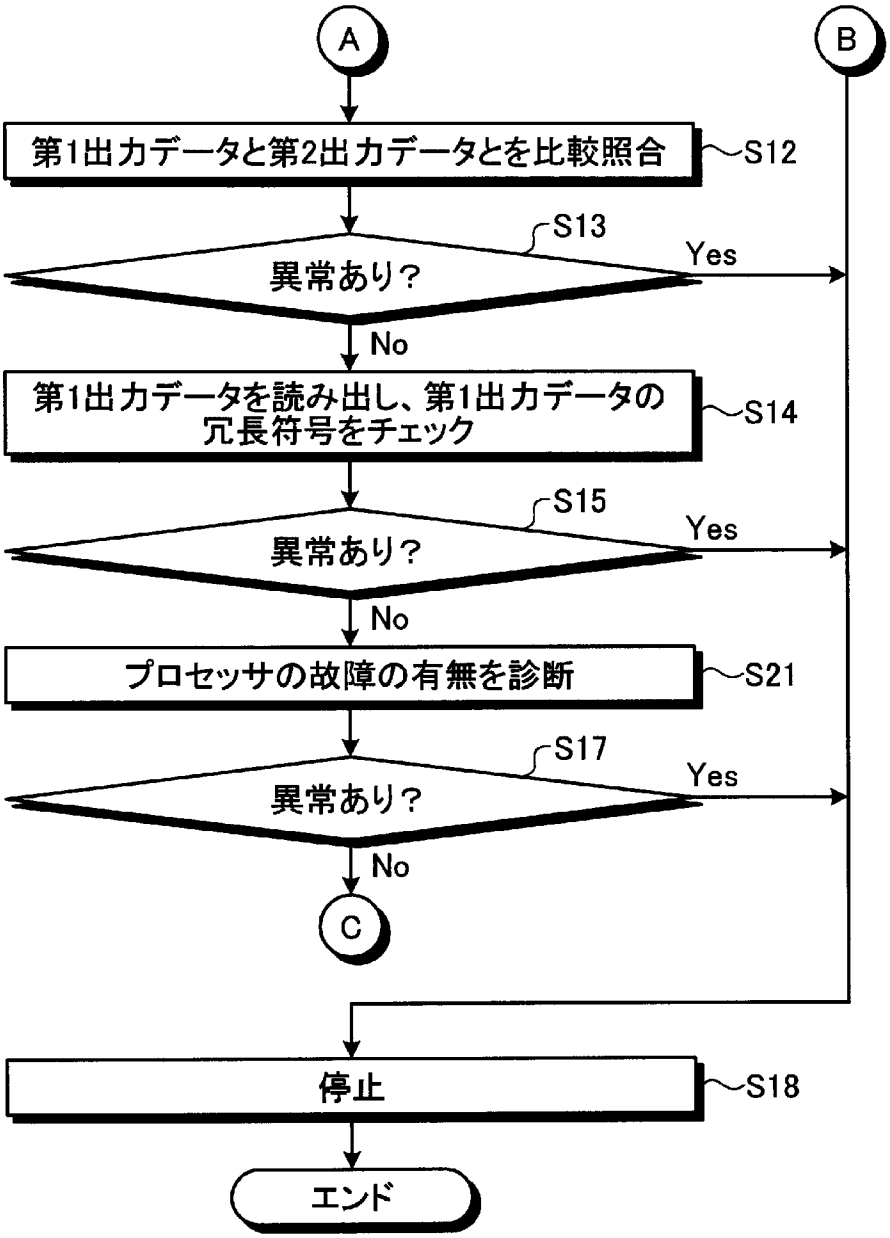
[図3]


A
B
第1出力データと第2出力データとを比較照合
S12
S13
異常あり？
Yes
No
第1出力データを読み出し、第1出力データの冗長符号をチェック
S14
S15
異常あり？
Yes
No
プロセッサおよびメモリの故障の有無を診断
S16
S17
異常あり？
Yes
No
C
停止
S18
エンド

[図4]


スタート
C
入力データを読み込み、第1および第2メモリ領域に入力データを書き込み
S1
第1入力データの冗長符号をチェック
S2
S3
異常あり？
Yes
No
第1入力データのプログラム処理を実行
S4
第1メモリ領域に第1出力データを書き込み
S5
第1出力データに冗長符号を付与
S6
第2入力データの冗長符号をチェック
S7
S8
異常あり？
Yes
No
第2入力データのプログラム処理を実行
S9
第2出力データをビット反転
S20
第2メモリ領域に第2出力データを書き込み
S10
第2出力データに冗長符号を付与
S11
A
B

[図5]


A
B
第1出力データと第2出力データとを比較照合
S12
S13
異常あり？
Yes
No
第1出力データを読み出し、第1出力データの冗長符号をチェック
S14
S15
異常あり？
Yes
No
プロセッサの故障の有無を診断
S21
S17
異常あり？
Yes
No
C
停止
S18
エンド

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2012/073179

A. CLASSIFICATION OF SUBJECT MATTER
G05B19/05(2006.01)i, *G05B9/03*(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)
G05B19/05, G05B9/03

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	1996-2012
Kokai Jitsuyo Shinan Koho	1971-2012	Toroku Jitsuyo Shinan Koho	1994-2012

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.
A	JP 2010-262432 A (Mitsubishi Electric Corp.), 18 November 2010 (18.11.2010), entire text; all drawings (Family: none)	1-5
A	JP 2-8911 A (Matsushita Electric Works, Ltd.), 12 January 1990 (12.01.1990), entire text; all drawings (Family: none)	1-5
A	JP 2000-148216 A (Mitsubishi Electric Corp.), 26 May 2000 (26.05.2000), entire text; all drawings (Family: none)	1-5

☐ 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	Date of mailing of the international search report
02 October, 2012 (02.10.12)	16 October, 2012 (16.10.12)
Name and mailing address of the ISA/ Japanese Patent Office Facsimile No.	Authorized officer Telephone No.

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ２０１２／０７３１７９

Ａ．　発明の属する分野の分類（国際特許分類（ＩＰＣ））

Int.Cl.　G05B19/05(2006.01)i, G05B9/03(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.　G05B19/05, G05B9/03

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	１９７１－２０１２年
日本国実用新案登録公報	１９９６－２０１２年
日本国登録実用新案公報	１９９４－２０１２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
A	JP 2010-262432 A（三菱電機株式会社）2010.11.18, 全文全図（ファミリーなし）	１－５
A	JP 2-8911 A（松下電工株式会社）1990.01.12, 全文全図（ファミリーなし）	１－５
A	JP 2000-148216 A（三菱電機株式会社）2000.05.26, 全文全図（ファミリーなし）	１－５

☐　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 ０２．１０．２０１２	国際調査報告の発送日 １６．１０．２０１２
国際調査機関の名称及びあて先 日本国特許庁（ＩＳＡ／ＪＰ） 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）　３Ｕ　４１３５ 川東　孝至 電話番号　０３－３５８１－１１０１　内線　３３２４