

(19) 日本国特許庁(JP)

(12) 公開特許公報(A)

(11) 特許出願公開番号
特開2009-31853
(P2009-31853A)

(43) 公開日 平成21年2月12日(2009.2.12)

(51) Int.Cl.
G06F 7/58 (2006.01)
G09C 1/00 (2006.01)

F I
G06F 7/58 B
G09C 1/00 650B

テーマコード (参考)
5 J 1 0 4

審査請求 未請求 請求項の数 5 O L (全 9 頁)

(21) 出願番号	特願2007-192297 (P2007-192297)	(71) 出願人	000004204
(22) 出願日	平成19年7月24日 (2007.7.24)		日本精工株式会社
			東京都品川区大崎1丁目6番3号
		(74) 代理人	100089118
			弁理士 酒井 宏明
		(72) 発明者	久保 信広
			群馬県前橋市鳥羽町78番地 日本精工株式会社内
		Fターム(参考)	5J104 FA10 NA04

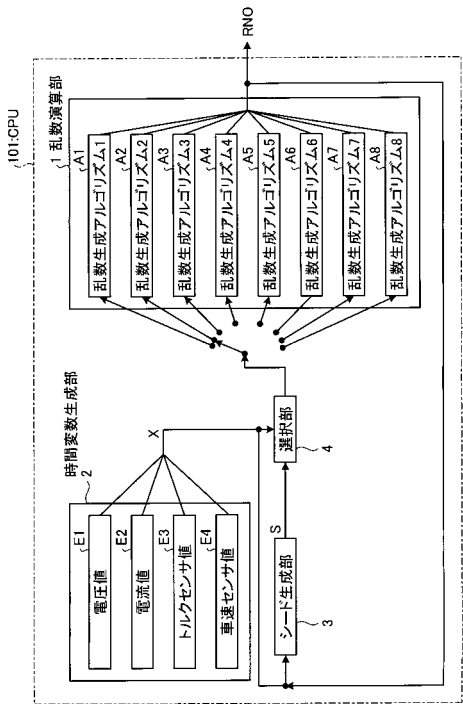
(54) 【発明の名称】 車載用擬似乱数生成装置

(57) 【要約】

【課題】 予測困難な擬似乱数を生成すること。

【解決手段】 CPU101は、シードに基づいて擬似乱数を生成する車載用擬似乱数生成装置として機能する。CPU101は、乱数演算部1と、時間変数生成部2と、シード生成部3と、選択部4とを備える。乱数演算部1は、乱数生成アルゴリズム1～乱数生成アルゴリズム8を備えている。これらは、それぞれ異なる擬似乱数演算のアルゴリズムである。選択部4は、時間の経過とともに変化するバッテリーの電圧値や電流値、パワー捨てアリング装置のトルクセンサ値等に基づいて、乱数生成アルゴリズム1～乱数生成アルゴリズム8の一つを選択し、シードSを与える。これによって、選択された乱数生成アルゴリズムが擬似乱数を生成する。

【選択図】 図3



【特許請求の範囲】

【請求項 1】

車両に搭載されて、シードに基づいて擬似乱数を生成する車載用擬似乱数生成装置において、

前記シードから擬似乱数を生成する、複数の異なる擬似乱数演算手段と、

時間の経過とともに変化する情報に基づいて、複数の異なる前記擬似乱数演算手段から一つを選択する選択手段と、

を含むことを特徴とする車載用擬似乱数生成装置。

【請求項 2】

前記情報は、前記車両に搭載される、物理量の検出手段の検出値であることを特徴とする請求項 1 に記載の車載用擬似乱数生成装置。 10

【請求項 3】

前記検出手段は、アナログ値を検出するものであることを特徴とする請求項 2 に記載の車載用擬似乱数生成装置。

【請求項 4】

選択された前記擬似乱数演算手段によって生成された擬似乱数を用いて、前記シードを生成することを特徴とする請求項 1～3 のいずれか 1 項に記載の車載用擬似乱数生成装置。

【請求項 5】

前記情報に基づいて、初回の前記シードを生成することを特徴とする請求項 1～4 のいずれか 1 項に記載の車載用擬似乱数生成装置。 20

【発明の詳細な説明】

【技術分野】

【0001】

本発明は、車両に搭載されて、擬似乱数を生成する車載用擬似乱数生成装置に関する。

【背景技術】

【0002】

シードに基づき擬似乱数を生成する擬似乱数生成方法は、例えば、通信等の分野におけるセキュリティチェック等に利用されている。また、車両においては、セキュリティを向上させるための暗号化等に擬似乱数生成方法が利用されている。例えば、特許文献 1 には、少なくとも演算処理の処理経過情報を記憶するプログラムレジスタの値に基づいて設定したシードに基づいて、擬似乱数生成演算を行う擬似乱数生成方法が開示されている。 30

【0003】

【特許文献 1】特開 2005-276113 号公報、段落番号 0014～0018、図 2

【発明の開示】

【発明が解決しようとする課題】

【0004】

しかし、特許文献 1 に開示されている技術は、擬似乱数生成演算のアルゴリズムが固定されているため、シードが変化したとしても、ある時点で擬似乱数の生成方法が判明するおそれが高い。 40

【0005】

本発明は、上記に鑑みてなされたものであって、擬似乱数を生成する方法の予測を困難にして、予測困難な擬似乱数を生成することを目的とする。

【課題を解決するための手段】

【0006】

上述した課題を解決して、本発明の目的を達成するために、本発明に係る車載用擬似乱数生成装置は、車両に搭載されて、シードに基づいて擬似乱数を生成する車載用擬似乱数生成装置において、前記シードから擬似乱数を生成する、複数の異なる擬似乱数演算手段と、時間の経過とともに変化する情報に基づいて、複数の異なる前記擬似乱数演算手段から一つを選択する選択手段と、を含むことを特徴とする。 50

【0007】

本発明の望ましい態様としては、前記情報は、前記車両に搭載される、物理量の検出手段の検出値であることが好ましい。

【0008】

本発明の望ましい態様としては、前記検出手段は、アナログ値を検出するものであることが好ましい。

【0009】

本発明の望ましい態様としては、選択された前記擬似乱数演算手段によって生成された擬似乱数を用いて、前記シードを生成することが好ましい。

【0010】

本発明の望ましい態様としては、前記情報に基づいて、初回の前記シードを生成することが好ましい。

【発明の効果】

【0011】

本発明に係る車載用擬似乱数生成装置は、擬似乱数を生成する方法の予測を困難にして、予測困難な擬似乱数を生成できる。

【発明を実施するための最良の形態】

【0012】

以下、本発明につき図面を参照しつつ詳細に説明する。なお、以下に説明する発明を実施するための最良の形態（以下実施形態という）により本発明が限定されるものではない。

【0013】

本実施形態は、車載用の擬似乱数生成装置であって、複数の異なる擬似乱数演算手段を備え、時間の経過とともに変化する情報に基づいて、複数の異なる擬似乱数演算手段のうち一つを選択して、擬似乱数を生成する点に特徴がある。

【0014】

図1は、車載通信システムの一例を示す説明図である。この車載通信システム60は、共通通信線61に複数のコンピュータを接続するバス型ネットワーク形式で構成されている。共通通信線61には、EPS（Electric Power Steering：電動パワーステアリング装置）制御装置50、エンジンコントロールユニット51、AT（Automatic Transmission）コントローラ52、ゲートウェイコンピュータ53のようなコンピュータ類や、外部機器接続用コネクタ54が接続されている。

【0015】

EPS制御装置50、エンジンコントロールユニット51、AT（Automatic Transmission）コントローラ52、ゲートウェイコンピュータ53は、共通通信線61を介して相互にデータをやり取りすることができる。また、外部機器接続用コネクタ54に診断装置やデータ書き込み装置等の外部機器を接続して、EPS制御装置50やエンジンコントロールユニット51等に記録された運転上の不具合等を診断したり、これらの制御用コンピュータプログラムを書き換えたりする。本実施形態においては、車載通信システム60の共通通信線61に接続されているEPS制御装置50、エンジンコントロールユニット51、ATコントローラ52等の機器が擬似乱数生成装置（車載用擬似乱数生成装置）を備えている。次に、EPS制御装置50を例として、本実施形態に係る擬似乱数生成装置を説明する。

【0016】

図2は、図1に示す車載通信システムに接続されるEPS制御装置のハードウェア構成を示す装置構成図である。EPS制御装置50は、図2に示すように、MCU（Micro Control Unit）100と、FET（Field Effect Transistor）ブリッドライバ回路110と、モータ駆動回路（インバータ）120と、電流検出回路130と、位置検出回路140等とを備えている。MCU100は、CPU（Central Processing Unit）101、ROM（Read Only Memory）102、RAM（Random Access Memory）103、EEPROM

(不揮発性メモリ) 104、A/D変換器105、インターフェース106、バス107等を備えている。CPU101は、ROM102に格納された各種プログラムを実行して、電動パワーステアリング装置のモータ9を制御する。

【0017】

ROM102は、CPU101が実行する各種コンピュータプログラムを格納する。具体的には、ROM102には、モータ9を制御するモータ制御処理(アシスト処理)を実行するためのモータ制御コンピュータプログラム、本実施形態に係る擬似乱数生成方法を実現するコンピュータプログラム等が格納されている。なお、以下において、コンピュータプログラムは、単にプログラムという。

【0018】

RAM103は、CPU101がプログラムを実行する場合にその作業領域として使用され、プログラムの処理過程で必要とするデータや処理結果等が記憶されるものである。EEPROM104は、EPS制御装置50の電源遮断後においても記憶内容を保持可能な不揮発性メモリであり、CPU101が、電動パワーステアリング装置の制御で使用する制御データやEEPROM104に格納される制御データのエラー発生回数等が格納される。なお、ここでは、不揮発性メモリとして、EEPROMを使用することとしたが、本実施形態においてはこれに限られるものではなく、FLASH-ROM、SDRAM等の他の不揮発性メモリを使用することにしてもよい。

【0019】

A/D変換器105は、トルクセンサ10からの操舵トルクT、車速センサ12からの車速Vc、電圧センサ14で検出されるバッテリー11の電圧Eb、電流センサ16で検出されるバッテリー11の電流Ib、電圧電流検出回路130からのモータ9の電流検出値Im、及び位置検出回路140からのモータ回転角信号θ等が入力され、これらの入力をディジタル信号に変換する。上記構成において、CPU101が、ROM102に格納された擬似乱数生成プログラムを実行することにより、擬似乱数生成装置として機能する。

【0020】

FETブリッドドライバ回路110は、MCU100から入力されるUVW各相のPWM(Pulse Width Modulation)制御信号を、各相正負の通電信号(U_p、U_n、V_p、V_n、W_p、W_n)に変換して、モータ駆動回路120に出力する。モータ駆動回路120は、一対のFETスイッチング素子からなるブリッジ回路をU相用、V相用、W相用として3相分備えており、各FETスイッチング素子には還流ダイオードが並列接続されている。このブリッジ回路には、バッテリー11から電源リレー13を介して直流電圧が印加される。各FETスイッチング素子の制御端子(ゲート端子)には、FETブリッドドライバ回路110から通電信号が入力される。

【0021】

モータ駆動回路120に印加される直流電圧は、モータ駆動回路120内のFETスイッチング素子のスイッチング動作によって3相の交流電圧に変換され、それによりモータ9が駆動される。このブリッジ回路には、シャント抵抗R1、R2が接続されている。このシャント抵抗R1、R2に電流検出回路130が接続され、これによって、モータ9の電流検出値Imを検出するようになっている。位置検出回路140は、位置センサ21に励磁電流を与えると同時に、位置センサ21からの出力信号をモータ回転角信号θとして、A/D変換器105に出力する。

【0022】

図3は、本実施形態に係る擬似乱数生成装置の機能を示す機能ブロック図である。上述したように、本実施形態では、CPU101が擬似乱数生成プログラムを実行することにより、擬似乱数生成装置として機能する。擬似乱数生成装置として機能するCPU101は、擬似乱数演算手段を複数備える乱数演算部1と、時間変数生成手段である時間変数生成部2と、シード生成手段であるシード生成部3と、選択手段である選択部4と、を含んでいる。

【0023】

10

20

30

40

50

乱数演算部 1 が備える擬似乱数演算手段は、線形合同法、混合合同法、平方採中法等の擬似乱数を生成するために用いる擬似乱数生成アルゴリズム（以下、必要に応じて乱数生成アルゴリズムという）である。本実施形態において、乱数演算部 1 は、乱数生成アルゴリズム 1（A1）～乱数生成アルゴリズム 8（A8）までの 8 個の乱数生成アルゴリズムを備える。なお、乱数演算部 1 が備える乱数生成アルゴリズムは、8 個に限定されるものではない。選択部 4 は、時間の経過とともに変化する情報（以下経時情報という）に基づいて、シード生成部によって生成される擬似乱数の種、すなわちシード S を与える乱数生成アルゴリズムを選択する。時間変数生成部 2 は、経時情報を選択部 4 に与える。

【0024】

本実施形態においては、経時情報として、トルクセンサ 10 や電圧センサ 14 等のような、物理量の検出手段によって検出されるアナログ値を用いることが好ましい。アナログ値には必ずホワイトノイズが含まれるので、アナログ値の発生パターンを予測することは極めて困難である。このため、アナログ値は、シード S を与える乱数生成アルゴリズムを選択する際に用いる情報として好ましい。本実施形態において、経時情報としては、バッテリー 11 の電圧値 E1、バッテリー 11 の電流値 E2、トルクセンサ 10 で検出されるトルクセンサ値 E3、車速センサ 12 で検出される車速センサ値 E4 といったアナログ値を用いる。そして、これらのアナログ値を、図 2 に示す MCU 100 が備える A/D 変換器 105 によってディジタル値に変換し、経時情報として用いる。

【0025】

なお、経時情報はこれらに限定されるものではなく、例えば、図 2 に示す電流検出回路 130 から出力されるモータ 9 の電流検出値 I_m や、位置検出回路から出力されるモータ回転角信号 θ を用いてもよい。また、図 2 に示す MCU 100 が、RAM 103 をリフレッシュするためのリフレッシュアジャスタを備える場合、このリフレッシュアジャスタの値を、経時情報として用いてもよい。

【0026】

図 4 は、シードを与える乱数生成アルゴリズムを選択する際の手法の一例を示す説明図である。例えば、図 4 に示すように、A/D 変換をした後における経時情報が 8 bit で表される場合、選択部 4 は、A/D 変換した後における複数の経時情報（電圧値 E1、電流値 E2、トルクセンサ値 E3、車速センサ値 E4）の総和の下位 3 bit の情報を用いて生成した時間変数 X によって、乱数演算部 1 が備える乱数生成アルゴリズム 1～乱数生成アルゴリズム 8 のうちの一つを選択する。

【0027】

3 bit は、000、001、010、011、100、101、110、111 の計 8 個の情報を有する。本実施形態に係る乱数演算部 1 は、乱数生成アルゴリズム 1～乱数生成アルゴリズム 8 の計 8 個のアルゴリズムを備える。この場合、例えば、乱数生成アルゴリズム 1～乱数生成アルゴリズム 8 に、000、001、010、011、100、101、110、111 をそれぞれの識別番号として割り当てておく。そして、時間変数生成部 2 は、A/D 変換をした後における経時情報の下位 3 bit の値から時間変数 X を生成する。選択部 4 は、時間変数生成部 2 が生成した時間変数 X を用いてシード S を与える乱数生成アルゴリズムを選択する。これによって、経時情報に基づいて、シード S を与える乱数生成アルゴリズムが選択される。

【0028】

なお、上記説明においては、経時情報を A/D 変換した後における下位 bit の情報を用いて生成した時間変数 X を用いてシード S を与えるアルゴリズムを選択したが、時間変数 X の生成に用いる情報は、下位 3 bit に限定されるものではない。しかし、下位 bit ほど、ばらつきが大きいので、その発生パターンを予測することは上位 bit を用いるよりも困難である。したがって、経時情報を A/D 変換した後における最下位の bit から所定の bit までの情報を用いて時間変数 X を生成し、これを用いてシード S を与える乱数生成アルゴリズムを選択することが好ましい。また、A/D 変換器 105 自体にも動作のばらつきが存在するため、A/D 変換後のディジタル値を用いて時間変数 X を生成す

ると、乱数生成アルゴリズムを選択する際の予測がより困難になるので、より予測が困難な擬似乱数を生成できる。

【0029】

なお、時間変数Xの生成方法は、上述したものに限定されるものではない。例えば、複数の経時情報をすべて加算又は減算し、その加算値又は減算値を乱数演算部1が備える乱数生成アルゴリズムの数nで割った余りの最下位bitから所定のbit数を選択し、時間変数Xとして用いてもよい。また、複数存在する経時情報の中から一つを選択して時間変数Xを生成してもよい。

【0030】

さらに、複数存在する経時情報の中から少なくとも二つを選択し、それらの加算値又は減算値を用いて時間変数Xを生成してもよい。複数存在する経時情報の中から少なくとも一つを選択する場合、時間変数生成部2で生成した時間変数Xに基づいて、例えば、下位3bitを用いて対応する情報を選択する等の手法により、情報を選択してもよい。このようにすれば、乱数演算部1で演算される擬似乱数がより予測困難なものになるので好ましい。

【0031】

乱数演算部1から乱数生成アルゴリズムを選択するにあたっては、時間変数生成部2で生成された時間変数Xを選択部4が取得する。この場合、乱数生成アルゴリズムの切替が煩雑にならないように、選択部4は所定の時間間隔Δtで時間変数Xを取得する。なお、時間変数生成部2が、所定の時間間隔Δtで時間変数Xを生成するとともに、生成した時間変数Xを選択部4へ出力してもよい。所定の時間間隔Δtは一定の時間としてもよいし、時間の経過とともに所定の時間間隔Δtを変更してもよい。この場合、時間変数生成部2で生成された時間変数Xを用いて所定の時間間隔Δtを変更してもよい。時間の経過とともに所定の時間間隔Δtを変更すれば、乱数演算部1で演算される擬似乱数がより予測困難なものになるので好ましい。

【0032】

選択部4は、取得した時間変数Xに基づいて乱数演算部1の乱数生成アルゴリズムを選択する。そして、選択した乱数生成アルゴリズムにシード生成部3で生成されたシードSを与える。選択された乱数演算部1の乱数生成アルゴリズムは、与えられたシードSを用いて擬似乱数RNOを生成し、出力する。乱数演算部1が生成した擬似乱数RNOは、暗号化処理やデータ転送に用いられるとともに、シード生成部3へ与えられ、シードSの生成に用いられる。

【0033】

これによって、シードSも予測は極めて困難になるので、乱数演算部1で演算される擬似乱数がより予測困難なものになり、より好ましい。なお、時間変数Xは、シード生成部3へ与えられ、初回（例えば、EPS制御装置50へ電源が投入されてから、初めて擬似乱数を生成する場合）のシードSの生成に用いられる。時間変数Xは、アナログ情報に基づいて生成されるので、規則性はほとんど存在しない。これによって、シードSの予測は極めて困難になるので、乱数演算部1で演算される擬似乱数がより予測困難なものになる。

【0034】

例えば、混合合同法は、式(1)のa、p、qに適当な数値を代入し、得られたa'の中間あたりの必要な桁数を擬似乱数RNOとして採用し、それを新たなaとして再び式(1)に代入することによって、擬似乱数RNOを得る。混合合同法において、時間変数Xを用いてシードSを生成する場合、3個の時間変数Xを数値に変換し、それぞれをa、p、qとして式(1)に与える。このa、p、qから求められるa'が、次のシードSとなる。

$$a \times p + q = a' \cdots (1)$$

ここで、混合合同法を用いる場合、aは今回のシードSとなり、a'は擬似乱数RNOであるとともに次のシードSとなる。なお、p、qは、適切な値であれば、固定値でも

10

20

30

40

50

よい。

【0035】

上述したように、本実施形態においては、図1に示す車載通信システム60の共通通信線61に接続されているEPS制御装置50、エンジンコントロールユニット51、ATコントローラ52等の機器が擬似乱数生成装置を備えている。外部機器接続用コネクタ54を介して共通通信線61上のデータをモニタすることにより、EPS制御装置50やエンジンコントロールユニット51等の制御ロジックを解析されるおそれがある。

【0036】

このため、共通通信線61に接続されている機器に本実施形態に係る擬似乱数生成装置を搭載し、この擬似乱数生成装置によって得られた擬似乱数を用いて共通通信線61上のデータの解析を困難にする。例えば、データに擬似乱数を加算したり乗算したりすることにより、データを推測しにくくする。これによって、共通通信線61に接続されるEPS制御装置50やエンジンコントロールユニット51等への不正アクセスの防止、データ書き込み防止に有効である。

【0037】

また、盗難防止機能を向上させるために、共通通信線61に接続されている機器同士が互いに認証し合ったときに、車両の走行が可能になるようなセキュリティシステムを構築した場合、本実施形態に係る擬似乱数生成装置によって生成した擬似乱数を用いて認証用のパスワードやID、あるいは暗号等を作成する。

【0038】

本実施形態に係る擬似乱数生成装置は、経時情報に基づいて、複数の異なる擬似乱数生成アルゴリズムを選択し、擬似乱数を生成する。これによって、パターン化されない幅広い質のよい擬似乱数を生成することができる。すなわち、本実施形態に係る擬似乱数生成装置は、予測の困難な擬似乱数を生成することができる。その結果、本実施形態に係る擬似乱数生成装置によって得られた擬似乱数を用いることにより、共通通信線61上のデータの解析をさらに困難にすることができ、また、セキュリティをさらに向上させることができる。

【0039】

以上、本実施形態では、経時情報に基づいて複数の異なる擬似乱数生成アルゴリズムを選択し、選択した擬似乱数生成アルゴリズムによって、擬似乱数を生成する。これによって、時間の変化とともに、擬似乱数を生成する擬似乱数生成アルゴリズムが変化するので、予測の困難な擬似乱数を生成することができる。

【0040】

また、本実施形態では、上記手法によって生成した擬似乱数を用いてシードを作成するので、シードの予測も困難になる。これによって、さらに予測の困難な擬似乱数を生成することができる。

【0041】

さらに、本実施形態においては、経時情報として、予測することが極めて困難なアナログ値を用いるので、複数の異なる擬似乱数生成アルゴリズムからいずれの擬似乱数生成アルゴリズムが選択されるかを予測することは極めて困難である。これによって、擬似乱数の予測をさらに困難なものとすることができる。

【産業上の利用可能性】

【0042】

以上のように、本発明に係る車載用擬似乱数生成装置は、車両に搭載されて擬似乱数を生成することに有用であり、特に、予測の困難な擬似乱数を生成することに適している。

【図面の簡単な説明】

【0043】

【図1】車載通信システムの一例を示す説明図である。

【図2】図1に示す車載通信システムに接続されるEPS制御装置のハードウェア構成を示す装置構成図である。

10

20

30

40

50

【図 3】 本実施形態に係る擬似乱数生成装置の機能を示す機能ブロック図である。

【図 4】 選択部がシードを与えるアルゴリズムを選択する際の手法の一例を示す説明図である。

【符号の説明】

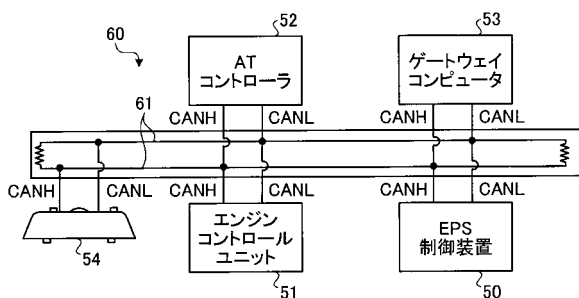
【 0 0 4 4 】

- 1 乱数演算部
- 2 時間変数生成部
- 3 シード生成部
- 4 選択部
- 10 トルクセンサ
- 11 バッテリ
- 12 車速センサ
- 14 電圧センサ
- 16 電流センサ
- 50 E P S 制御装置
- 51 エンジンコントロールユニット
- 52 コントローラ
- 53 ゲートウェイコンピュータ
- 54 外部機器接続用コネクタ
- 60 車載通信システム
- 61 共通通信線
- 100 M C U
- 101 C P U

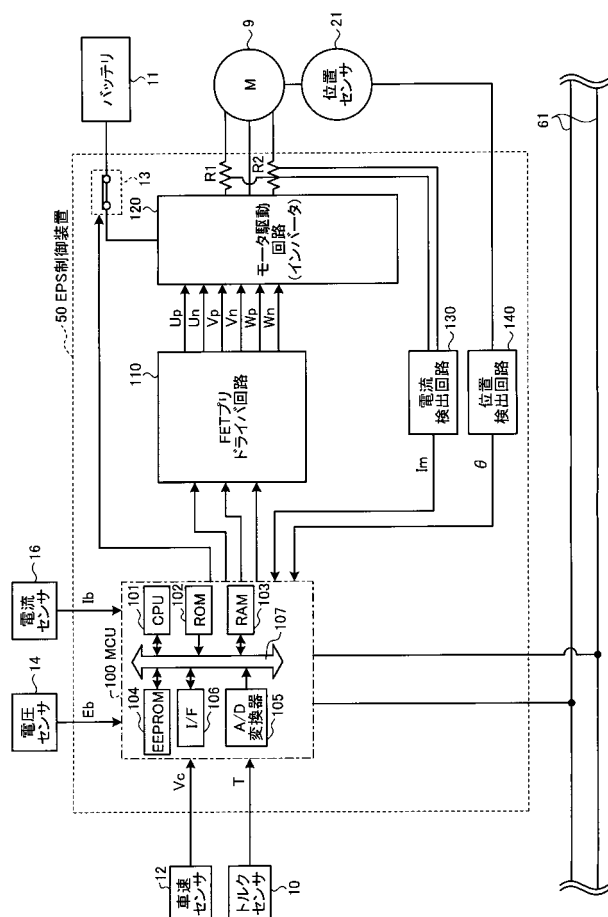
10

20

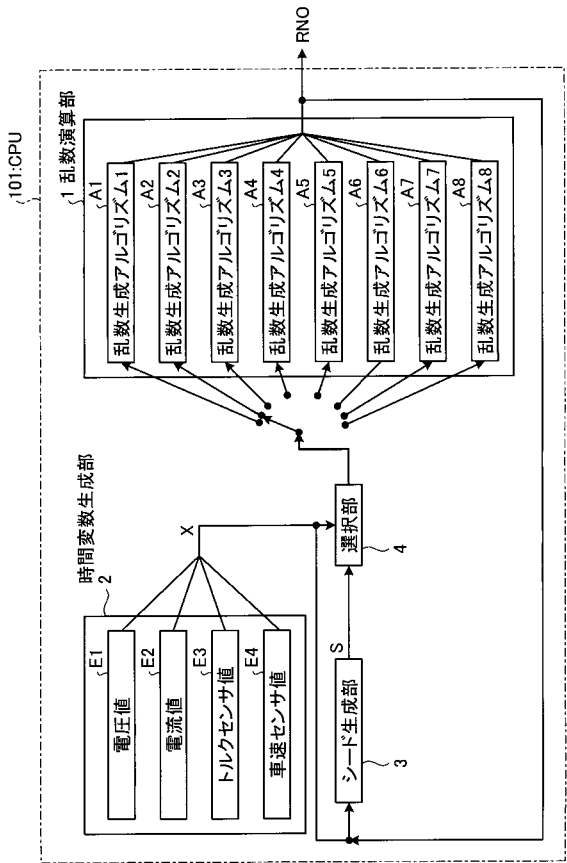
【図 1】



【図 2】



【図 3】



【図 4】

