(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第4993249号
(P4993249)
(45)発行日　平成24年8月8日(2012.8.8)　(24)登録日　平成24年5月18日(2012.5.18)

(51)Int.Cl.　F I
*G06F 9/48 (2006.01)*　G06F 9/46 315Z

請求項の数 3 (全 30 頁)

(21)出願番号　特願2005-305195(P2005-305195)
(22)出願日　平成17年10月20日(2005.10.20)
(65)公開番号　特開2006-134318(P2006-134318A)
(43)公開日　平成18年5月25日(2006.5.25)
審査請求日　平成20年10月16日(2008.10.16)
(31)優先権主張番号　10/970,570
(32)優先日　平成16年10月21日(2004.10.21)
(33)優先権主張国　米国(US)

(73)特許権者　390041542
ゼネラル・エレクトリック・カンパニイ
アメリカ合衆国、ニューヨーク州、スケネクタデイ、リバーロード、１番
(74)代理人　100137545
弁理士　荒川　聡志
(74)代理人　100105588
弁理士　小倉　博
(74)代理人　100129779
弁理士　黒川　俊久
(72)発明者　グレゴリー・スコット・ドロバ
アメリカ合衆国、カリフォルニア州、サン・ノゼ、ナンバー１３０７、アルマデン・ロード、１７７６番

最終頁に続く

(54)【発明の名称】計測システムおよび制御システム向けのイベントベースのオペレーティングシステム、方法、および装置

(57)【特許請求の範囲】
【請求項１】
ノンプリエンプティブなオペレーティングシステムを備えたコントローラ（１２）をプロセッサにより操作する方法であって、前記方法は、
前記プロセッサにより、クロック間で、センサー（４２）、スイッチ（５６）、実行中のプログラムの命令、あるいはその組み合わせからの、複数のイベントのうちの１つのイベントが、非アクティブなイベント（３０２）、アクティブなイベント（３０８）、保留中のイベント（３０６）、実行中のイベント（３１０）、または、待機中のイベント（３０４）であることを示すとともに、非アクティブなイベント（３０２）、アクティブなイベント（３０８）、保留中のイベント（３０６）、実行中のイベント（３１０）、および、待機中のイベント（３０４）を含む前記イベントの１つまたは複数を開始する１つまたは複数の信号を受信する工程と、
前記プロセッサにより、前記１つまたは複数の信号を受信する工程の直後のクロックまたはその後に、前記受信した信号に従ってイベントのエントリを更新し、クロック時に前記オペレーティングシステムのシャドウセマフォを更新して、前記シャドウセマフォを用いて開始期限を過ぎたイベントの優先順位を付け直す工程であって、前記エントリには、前記保留中のイベントの残り時間、前記アクティブなイベントの開始期限経過時間、各イベントの優先順位、前記複数のイベント中のイベントが非アクティブ、待機、保留、アクティブ、実行中のいずれであるかの表示を含む、工程と、
前記プロセッサにより、前記保留中のイベント（３０６）が開始期限が到来したかどう

かを判断し、前記開始期限が到来したイベントを保留中のイベント（３０６）からアクティブなイベント（３０８）に変更する工程と、
前記プロセッサにより、最も優先順位の高い、前記保留からアクティブに変更されたイベントを実行中のプログラムに通知する工程と、
を含み、
開始期限を過ぎたイベントの優先順位を付け直す工程は、前記プロセッサにより、前記実行中のプログラムにまだ通知していない開始期限を過ぎたアクティブなイベント（３０８）の前記優先順位を上げる工程を含む、
方法。
【請求項２】
ノンプリエンプティブなオペレーティングシステムを備え、プロセッサにより実行可能な命令が記録されたコンピュータ可読記録媒体であって、前記命令は、プロセッサにより、
クロック間で、センサー（４２）、スイッチ（５６）、実行中のプログラムの命令、あるいはその組み合わせからの、複数のイベントのうちの１つのイベントが、非アクティブなイベント（３０２）、アクティブなイベント（３０８）、保留中のイベント（３０６）、実行中のイベント（３１０）、または、待機中のイベント（３０４）であることを示すとともに、非アクティブなイベント（３０２）、アクティブなイベント（３０８）、保留中のイベント（３０６）、実行中のイベント（３１０）、および、待機中のイベント（３０４）を含む前記イベントの１つまたは複数を開始する１つまたは複数の信号を受信し、
前記１つまたは複数の信号の受信の直後のクロックまたはその後に、前記受信した信号に従ってイベントのエントリを更新し、クロック時に前記オペレーティングシステムのシャドウセマフォを更新して、前記シャドウセマフォを用いて開始期限を過ぎたイベントの優先順位を付け直し、この際、前記エントリは、前記保留中のイベントの残り時間、前記アクティブなイベントの開始期限経過時間、各イベントの優先順位、前記複数のイベント中のイベントが非アクティブ、待機、保留、アクティブ、実行中のいずれであるかの表示を含み、
前記保留中のイベント（３０６）が開始期限が到来したかどうかを判断し、前記開始期限が到来したイベントを保留中のイベント（３０６）からアクティブなイベント（３０８）に変更し、
最も優先順位の高い、前記保留からアクティブに変更されたイベントを実行中のプログラムに通知する
命令であり、この際、
開始期限を過ぎたイベントの優先順位の付け直しは、前記プロセッサにより、前記実行中のプログラムにまだ通知していない開始期限を過ぎたアクティブなイベント（３０８）の前記優先順位を上げることを含む、
コンピュータ可読記録媒体。
【請求項３】
プロセッサと、ノンプリエンプティブなオペレーティングシステムと前記プロセッサにより実行可能な命令が記録されたメモリとを備えたコントローラであって、前記コントローラは、
クロック間で、センサー（４２）、スイッチ（５６）、実行中のプログラムの命令、あるいはその組み合わせからの、複数のイベントのうちの１つのイベントが、非アクティブなイベント（３０２）、アクティブなイベント（３０８）、保留中のイベント（３０６）、実行中のイベント（３１０）、または、待機中のイベント（３０４）であることを示すとともに、非アクティブなイベント（３０２）、アクティブなイベント（３０８）、保留中のイベント（３０６）、実行中のイベント（３１０）、および、待機中のイベント（３０４）を含む前記イベントの１つまたは複数を開始する１つまたは複数の信号を受信し、
前記１つまたは複数の信号の受信の直後のクロックまたはその後に、前記受信した信号に従ってイベントのエントリを更新し、クロック時に前記オペレーティングシステムのシ

ャドウセマフォを更新して、前記シャドウセマフォを用いて開始期限を過ぎたイベントの優先順位を付け直し、この際、前記エントリは、前記保留中のイベントの残り時間、前記アクティブなイベントの開始期限経過時間、各イベントの優先順位、前記複数のイベント中のイベントが非アクティブ、待機、保留、アクティブ、実行中のいずれであるかの表示を含み、

前記保留中のイベント（３０６）が開始期限が到来したかどうかを判断し、前記開始期限が到来したイベントを保留中のイベント（３０６）からアクティブなイベント（３０８）に変更し、

最も優先順位の高い、前記保留からアクティブに変更されたイベントを実行中のプログラムに通知し、

この際、

開始期限を過ぎたイベントの優先順位の付け直しは、前記プロセッサにより、前記実行中のプログラムにまだ通知していない開始期限を過ぎたアクティブなイベント（３０８）の前記優先順位を上げることを含む、

コントローラ。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明は、一般的にはコンピュータオペレーティングシステムに関し、より具体的には計測システムおよび制御システムにおいて高度なタイミング機能提供するためのコンピュータオペレーティングシステムに関する。

【背景技術】

【０００２】

原子力発電所向けのホウ酸水注入系（ＳＬＣ：Ｓｔａｎｄｂｙ　Ｌｉｑｕｉｄ　Ｃｏｎｔｒｏｌ）の論理プロセッサは、複数のさまざまなイベントに迅速に反応する必要があり、結果として発電所内の複数のさまざまなシステムのパラメータを監視する必要がある。こうしたパラメータには、頻繁かつ／または定期的に変化するものがある一方で、特定の設備で発生してはならないきわめてまれなイベントに応答した場合にのみ変化するものもある。論理プロセッサのイベントおよびその状態変化のコンテキストを検出し、間接費の導入を一定限度に抑えるために、マイクロプロセッサ用のオペレーティングシステム（ＯＳ：Ｏｐｅｒａｔｉｎｇ　Ｓｙｓｔｅｍ）を採用することができる。いくつかの構成において、ＳＬＣには多くの同期タイマー（たとえば、８個の同期タイマー）が必要であり、１つのマイクロコントローラでは対応できない場合がある。

【特許文献１】米国特許６，７７５，７２８号公報

【発明の開示】

【発明が解決しようとする課題】

【０００３】

タスク指向のＯＳには、少なくともいくつかの周知の核計測分析および制御（ＮＵＭＡＣ：Ｎｕｃｌｅａｒ　Ｍｅａｓｕｒｅｍｅｎｔ　Ａｎａｌｙｓｉｓ　ａｎｄ　Ｃｏｎｔｒｏｌ）機器が使用されている。このＯＳでは、すべてのタスクをラウンドロビン方式で実行する必要がある。この種のＯＳを適用すると、間接費がかかり、特定の機能が必要ないのに実行される。しかし、各タイマーのカウンタとしてグローバルなスタティック変数を作成することで、複数のタイミングイベントを監視できる。このような変数は、システムクロックを使用してセットし、カウンタの値を増減できる。この限られた数のタイマーを使用して複数のタイミングイベントを監視する方法は、非常に単純であるが、記述するコードの量を増大し、コードのメンテナンスコストを増大する傾向がある。さらに、グローバル変数を使用することでインターフェイスの設計が複雑になり、さまざまなモジュールの操作の相互依存性が必要以上に高くなる。

【課題を解決するための手段】

【０００４】

したがって、本発明のいくつかの構成では、複数のタイマーを備えるコントローラを操作し、これを使用してタイマーの数より多い複数のイベントを制御する方法を提供する。本方法には、クロックチック（ｃｌｏｃｋ　ｔｉｃｋｓ）間で、１つまたは複数の時間指定（ｔｉｍｅｄ）イベントを開始するセンサー、スイッチ、実行中のプログラム、あるいはその組み合わせからの１つまたは複数の信号を受信する工程が含まれる。本方法には、１つまたは複数の信号を受信した直後のクロックチックの後に、受信した信号（１つまたは複数）に従ってイベント制御ブロック内のエントリを更新する工程がさらに含まれる。エントリには、保留イベントの残り時間、アクティブイベントの期限経過時間、および各イベントの優先順位が含まれる。本方法には、保留イベント（１つまたは複数）がタイムアウトしたかどうかを判断する工程と、タイムアウトしたイベントがある場合にそれを開始する工程と、開始した最も優先順位の高いイベントについて通知する信号を実行中のプログラムに送信する工程がさらに含まれる。

【０００５】

本発明の別のいくつかの態様において、プロセッサに対してさまざまな機能の実行を指示するように構成された命令を含むノンプリエンプティブ（ｎｏｎ－ｐｒｅｅｍｐｔｉｖｅ）なオペレーティングシステムが記録された機械可読媒体またはメモリが提供される。このような機能には、クロックチック間で、１つまたは複数の時間指定イベントを開始するセンサー、スイッチ、実行中のプログラム、あるいはその組み合わせからの１つまたは複数の信号を受信する機能が含まれる。こうした機能には、１つまたは複数の信号を受信した直後のクロックチックまたはその後に、受信した信号（１つまたは複数）に従ってイベント制御ブロック内のエントリを更新する機能がさらに含まれる。ただし、エントリには保留イベントの残り時間、アクティブイベントの期限経過時間、および各イベントの優先順位が含まれる。本機能には、保留イベント（１つまたは複数）がタイムアウトしたかどうかを判断する機能と、タイムアウトしたイベントがある場合にそれを開始する機能と、開始した最も優先順位の高いイベントについて通知する信号を実行中のプログラムに送信する機能がさらに含まれる。

【０００６】

本発明のさらに別の態様において、本発明は複数のタイマーを備えるプロセッサと、プロセッサに対する命令を格納するメモリとを備えるコントローラを提供する。本コントローラには、クロックチック間で、１つまたは複数の時間指定イベントを開始するセンサー、スイッチ、実行中のプログラム、あるいはその組み合わせからの１つまたは複数の信号を受信するように構成されている。本コントローラは、１つまたは複数の信号を受信した直後のクロックチックまたはその後に、受信した信号（１つまたは複数）に従ってイベント制御ブロック内のエントリを更新するようにさらに構成されている。こうしたエントリには、保留イベントの残り時間、アクティブイベントの期限経過時間、および各イベントの優先順位が含まれる。本コントローラは、保留イベント（１つまたは複数）がタイムアウトしたかどうかを判断し、タイムアウトしたイベントがある場合にそれを開始し、開始した最も優先順位の高いイベントについて通知する信号を実行中のプログラムに送信するようにさらに構成されている。

【０００７】

したがって、本発明の構成は、１つまたは複数の物理的なタイマーを備えるコントローラを使用して、工業プラント内のイベントのように複雑なイベントのタイミングを提供するのが有利であることが認識されよう。ただし、物理的なタイマーの数は時間指定イベントの数より少ない。

【発明を実施するための最良の形態】

【０００８】

本発明の構成は、時間指定イベント（原子力発電所を含む工業プラント内で発生するものなど）の高度な制御を可能にする。本発明のいくつかの構成による技術的な効果には、使用可能なハードウェアタイマーの数より多い複数のイベントのタイミングを制御することと、時間指定イベントが特定の時間内に確実に発生することがある。

いくつかの構成では、工業プロセスにおける安全制御として使用するのに適したマイクロコントローラアーキテクチャが提供される。このアーキテクチャは多くの工業プロセスに適しているが、特に原子力に関する機器および制御システムには最適である。たとえば、このマイクロコントローラアーキテクチャは核計測分析および制御（ＮＵＭＡＣ）モジュール、高圧炉心注水系（ＨＰＣＦ：Ｈｉｇｈ　Ｐｒｅｓｓｕｒｅ　Ｃｏｒｅ　Ｆｌｏｏｄｅｒ）制御モジュール、出力論理ユニット（ＯＬＵ：Ｏｕｔｐｕｔ　Ｌｏｇｉｃ　Ｕｎｉｔ）モジュール、ホウ酸注入系（ＳＬＣ）モジュールでの使用に適している。こうしたモジュールは、本発明の構成を採用する一連のマイクロコントローラベースのシャーシである。さまざまな構成において、このような機器はモジュール形式をとっており、さらにリレー、ファイバ／光通信リンク、入力コンタクトカード（ｉｎｐｕｔ　ｃｏｎｔａｃｔ　ｃａｒｄｓ）、またはマイクロコントローラ、ファームウェア、カスタムロジック（ＣＰＬＤ）、ＥＰＲＯＭ、ＮＶＲＡＭ、ＲＡＭ、およびさまざまなＩＣを含む論理ボード（マザーボード）に直接または間接的に挿入できるその他の入力／出力（Ｉ／Ｏ）カードを追加することで拡張できる。本発明のいくつかの構成では、同類のモジュールを交換できるように、取り外し可能なすべてのモジュールを標準化している。いくつかの構成において、外部接続やインターフェイスはメンテナンスしやすいように機器のパネル背面に配置される。本発明のさまざまな構成から得られる技術的な効果には、特に担当者が監視を行うことによるアナログの安全システムの自動化、容易に拡張できる操作、コンポーネントの標準化による利便性がある。

【０００９】

本発明のマイクロプロセッサアーキテクチャを利用した機器は、幅４８．２６ｃｍ（１９インチ）の業務用のラックに収納できるように設計でき、標準の高さを１３．３３５ｃｍ（５．２５インチ）にできる。本発明のいくつかの構成では、冗長電源（２つの電源）を使用して、マイクロプロセッサアーキテクチャを利用した機器のフェイルセーフで堅牢な電気的なニーズを満たしている。いくつかの構成では、マイクロコントローラファームウェアにおいて特定のアプリケーションのセルフテストと監視の方法が提供される。いくつかの構成では、マイクロコントローラサブシステムロジックは、ＣＰＬＤサブシステムに含まれるロジックから独立して動作し、一方のサブシステムに破局的な（ｃａｔａｓｔｒｏｐｈｉｃ）障害が発生した場合に他方が機能するように、マイクロコントローラとＣＰＬＤとのインターフェイスが提供される。本発明の構成を複数の機器で利用すると、一貫したユーザーインターフェイスとフィードバック（「ルックアンドフィール」）が得られる。各機器は、たとえばキーロックスイッチを使用してフロントパネルを固定することもできる。本発明のいくつかの構成では、押しボタン、ＬＥＤ、および／または英数字ディスプレイも提供される。新しい機器は、顧客に固有の要件や技術的な要件を満たすように拡張できる。たとえば、特定の通信プロトコル（ＭＩＬ－ＳＴＤ－１５５３、ＲＳ－２３２など）、特定の電圧と電流（１２ＶＤＣ、２４ＶＤＣ、１２０ＶＡＣなど）を処理するように設計されたリレー、さまざまな波長（８５０ｎｍ、１３００ｎｍなど）の光データを送信および受信するように設計された光ファイバカードに適応できるデバイスは、本発明のさまざまな構成で利用できる。

【００１０】

本発明のいくつかの構成において、機器はたとえば４８．２６ｃｍ（１９インチ）の標準的な機器ラックにラックマウント方式で取り付けることができる。たとえば、本発明のいくつかの構成において、機器のシャーシは、幅４８．２６ｃｍ（１９インチ）、高さ１３．３３５ｃｍ（５．２５インチ）、奥行き３０．４８ｃｍ～３５．５６ｃｍ（１２～１４インチ）である。各機器のシャーシには、機器の該当するアプリケーションに応じて、前面パネルディスプレイ、デュアル冗長電源、論理カード、Ｉ／Ｏカードを収納できる。同類のモジュールは電気的にも機械的にも機器間で交換可能であり、交換しても補正は必要ない。

【００１１】

本発明のいくつかの構成において、図１を参照すると、論理カード１０は機器のロジッ

クと制御、外部システム（論理カード１０を含む機器の外部のシステム）へのステータス通信、およびオペレータ用のディスプレイおよびキーボード制御を提供している。論理カード１０のいくつかの構成には、以下のコンポーネントが含まれる。

【００１２】

マイクロコントローラ

マイクロコントローラ１２を使用すると、高速の計算と迅速な入力／出力操作を処理できる。適切なマイクロコントローラの例には、８７Ｃ１９６ＫＤマイクロコントローラ、すなわちＩｎｔｅｌ　Ｃｏｒｐｏｒａｔｉｏｎ，Ｓａｎｔａ　Ｃｌａｒａ，ＣＡから入手可能な１６ビットＣＨＭＯＳプロセッサがある。本発明の構成に利用できるこのマイクロコントローラの機能には、２０　ＭＨｚのクロック、１　ＫＢレジスタＲＡＭ、前二重シリアルポート、５つの８ビットＩ／Ｏポート、４個の内蔵１６ビットタイマー、および入力ＭＵＸを伴う１０ビットＡ／Ｄコンバータが含まれる。

【００１３】

論理カードの機能上の操作は、マイクロコントローラ１２で監視する。マイクロコントローラ１２は、監視に利用できる非同期のシリアルステータスメッセージを送信し、キーボードとディスプレイの制御を可能にし、デジタルＩ／Ｏラインを監視する。こうした機能に加えて、マイクロコントローラは電源と外部のセンサー電圧を監視し、メモリの整合性を確認することで、起動およびオンラインのセルフテストを実行する。送信された通信メッセージは、ループバックしてセルフテストで確認できる。

【００１４】

マイクロコントローラスーパーバイザ

マイクロプロセッサスーパーバイザロジックには、冗長電源１６および１８から供給される論理カード１０およびＩ／Ｏモジュール３４の＋５　ＶＤＣ電力を監視し、電圧が＋４．５０～４．６０　ＶＤＣの場合にマイクロコントローラ１２をリセットする電源監視回路１４が含まれる。このリセットにより、ＣＰＬＤコントローラロジック４６も初期状態に戻る。マイクロプロセッサスーパーバイザロジックの要素として、電圧＋５　ＶＤＣという基準線源（ｒｅｆｅｒｅｎｃｅ　ｓｏｕｒｃｅ）２０とリセット／電源投入回路２２も提供される。

【００１５】

マイクロコントローラ１２の他に１つまたは複数の結合プログラム可能論理回路（ＣＰＬＤ：Ｃｏｍｐｌｅｘ　Ｐｒｏｇｒａｍｍａｂｌｅ　Ｌｏｇｉｃ　Ｄｅｖｉｃｅ）４６が提供され、制御と復号を実行し、かつ／または機能ロジックを提供する。

【００１６】

制御および復号ハードウェア

本発明のいくつかの構成において、制御および復号ハードウェアは、次の１つまたは複数を提供するように構成された結合プログラム可能論理回路（ＣＰＬＤ）４６を含むまたはそれから基本的に構成される。

１．　ＥＰＲＯＭ　２６やＲＡＭ　２８、およびメモリをマップするすべてのＩ／Ｏ機能のアドレス復号

２．　さまざまな論理ステータスレジスタのアドレス復号

３．　周辺装置に低速でアクセスすることによるマイクロコントローラ１２の待ち状態のジェネレータ制御（たとえば、読み出しまたは書き込みアクセスのいくつかの構成では、前面パネルＬＥＤディスプレイ３０には３つの待ち状態が必要である）。

【００１７】

機能ロジックインターフェイスハードウェア

本発明のいくつかの構成において、機能ロジックインターフェイスハードウェアは、次の少なくとも１つを提供するように構成された結合プログラム可能論理回路（ＣＰＬＤ）を含むまたはそれから基本的に構成される。

１．　さまざまな分周器（ｆｒｅｑｕｅｎｃｙ　ｄｉｖｉｄｅｒｓ）

２．　トリップステータスとＩ／Ｏを監視し、トリップコマンドとその他の制御コマン

ドを生成できる機能ロジック
３．　さまざまな通信プロトコルのサポートロジック
４．　外部インターフェイスカード３４とその他のグルーロジック（ｇｌｕｅ　ｌｏｇｉｃ）のサポート
【００１８】
論理カード１０の構成は複数のＣＰＬＤ　４６（たとえば、いくつかの構成では１枚のカードに最大３個）に対応しており、ＣＰＬＤは容易に修理、交換、再構成できるようにソケットが付いている。したがって、制御および復号ハードウェアと機能ロジックインターフェイスハードウェアは、唯一のＣＰＬＤ内の配置、２つの別々のＣＰＬＤ上の配置、あるいは２つ以上のＣＰＬＤにまたがった配置などが可能である。本発明では、一方で制御および復号ハードウェアと機能ロジックインターフェイスハードウェア、他方で個々のＣＰＬＤが１対１に対応する必要はない。
【００１９】
入力保護とアナログ参照
制御カード上の入力ライン、＋５　ＶＤＣ、＋５ＶＤＣ前面パネル、＋５ＶＤＣ光ファイバ、＋５ＶＤＣリレーカードＡ　＆　Ｂ、＋２４　ＶＤＣ、＋４８　ＶＤＣは、温度限流器（ｔｈｅｒｍａｌ　ｃｕｒｒｅｎｔ　ｌｉｍｉｔｉｎｇ　ｄｅｖｉｃｅｓ）（図１で個別には図示せず）を自動的にリセットすることで保護される。電流が限界に達して限流器が加熱されると、過電流の状態がなくなるまで回路が開く。入力ラインは、セルフテスト中に電源監視回路１４を使用してマイクロコントローラ１２で監視される。このテストの各測定の結果を組み合わせて、前面パネルに表示された電源障害ＬＥＤ（ＬＥＤ　３０に含まれる）を制御する。いくつかの構成において、電源電圧は論理カード１０を備える機器の背面パネルのテストポイントで測定できる。
マイクロコントローラ１２のＡ／Ｄコンバータで必要な＋５　ＶＤＣ参照２０は、＋２４ＶＤＣ入力から生成され、不足電圧／過電圧検出回路によって監視される。
【００２０】
ＥＰＲＯＭおよびＲＡＭメモリ
いくつかの構成では、不揮発性プログラムストレージとしてＥＰＲＯＭ　２６が提供される。この目的で、３２　ＫＢ　ＥＰＲＯＭを提供してもよい。いくつかの構成では、コントローラ１２用の高速読み出し／書き込みメモリとしてスタティックＲＡＭ　２８、たとえば８　ＫＢスタティックＲＡＭが提供される。
【００２１】
不揮発性ＲＡＭ
いくつかの構成では、電力が供給されなくなっても失われてはならないアプリケーションパラメータを記憶するために、不揮発性ＲＡＭ　３８（２Ｋｘ８ビット強誘電性ＲＡＭなど）が提供される。こうしたパラメータはカード１０を利用するアプリケーションに依存するが、不揮発性ＲＡＭ　３８に格納できるアプリケーションパラメータの部分的なリストには、セルフテストのエラーコードと回数、較正パラメータなどを含めてもよい。いくつかの構成において、ＲＡＭ　３８は電力消費が低く、耐久性がきわめて高いシリアルデバイスである。
【００２２】
光ファイバインターフェイスカード
光ファイバインターフェイスカード４０は、光信号と電気信号との変換を行う。本発明のいくつかの構成において、各カードは６つの物理チャネルを備えている。こうしたチャネルは、カード１０のアプリケーションに基づいて、送信、受信、あるいは双方向通信に利用できる。たとえば、各チャネルは最大感度（ｐｅａｋ　ｓｅｎｓｉｔｉｖｉｔｙ）の波長が８５０ｎｍの光ファイバ信号で動作するが、いくつかの構成では別の波長（たとえば１３００ｎｍ）を使用している。いくつかの構成において、光送信機と光受信機は標準のＳＴタイプの光コネクタに接続する。
【００２３】

リレーＩ／Ｏカード

多くのアプリケーションでは、１つまたは複数のリレーＩ／Ｏカード４２が提供される。Ｉ／Ｏカード４２には、たとえば機械的なラッチリレー（ｌａｔｃｈｉｎｇ　ｒｅｌａｙｓ）、ノンラッチリレー、コンタクトクロージャ（ｃｏｎｔａｃｔ　ｃｌｏｓｕｒｅ）感知回路、またはそれらの任意の組み合わせを含めてもよい。各Ｉ／Ｏカード４２は、論理カード１０と制御の対象となる他のデバイスとのインターフェイス　バッファとして構成される（論理カード１０の視点からは「外部の世界」として映る）。シャーシに入る高電圧信号は、標準のＴＴＬレベルに変換される。標準のＴＴＬレベルの信号は、多くのインスタンスでこうしたカードに送信され、外部システムで使用するはるかに高い電圧に切り替えられる。

【００２４】

光ファイバインターフェイスカード４０とリレーＩ／Ｏカード４２は、外部システム（たとえば、限定はされないが、バルブ、ポンプ、その他の機器）を制御かつ／または感知でき、監視できる。一方では、外部のシステムと論理カード１０上のコンポーネントとの電気的絶縁を提供する。このように、論理カード１０は外部システムまたは安全機器と外部システムとの通信ラインの電気的障害が原因となって発生する問題に左右されにくい。いくつかの構成では、インターフェイスハードウェア３２が提供され、マイクロコントローラ１２および／またはＣＰＬＤ　４６と機器内にある任意のインターフェイスカード３４とをインターフェイスする。

【００２５】

外部ロジックを使用するかＣＰＬＤを使用するかに関わらず、本発明のいくつかの構成では、最大４枚のＩ／Ｏカード３４、前面パネルディスプレイ３０、および／または４４、ＥＰＲＯＭ　２６、ＲＡＭ　２８、および１～３個のＣＰＬＤ　４６へのインターフェイスを提供するバスを採用している。適切なバス構成の一部を図２に示す。この構成には、特に、アドレスバス（ＡＤＲ　ＢＵＳ）とデータバス（ＤＡＴＡ　ＢＵＳ）が含まれており、本明細書では集合的にアドレス／データバス（ＡＤＤＲ／ＤＡＴＡ　ＢＵＳ）と呼ぶこともある。バス構造によって信号を搬送することで、コンポーネントの相互の対話、メモリおよびＩ／Ｏデータ転送、直接メモリアクセス、その他の機能を実行できる。バス構造は、マスターデバイス５０がバスとスレーブデバイス（たとえばスレーブデバイス５２）を制御する「マスタースレーブ」構成の変形であり、アドレスを復号すると同時に、マスターデバイスが発行するコマンドに従って動作する。

【００２６】

いくつかの構成では、８ＸＣ１９６ＫＤデバイス（Ｉｎｔｅｌ　Ｃｏｒｐｏｒａｔｉｏｎ，Ｓａｎｔａ　Ｃｌａｒａ，ＣＡから入手できる）がバスマスター５０として動作する。バスマスターは、アドレスラッチイネーブル（ＡＬＥ：Ａｄｄｒｅｓｓ　Ｌａｔｃｈ　Ｅｎａｂｌｅ）信号を外部ラッチに送信し、アドレス／データバスからのアドレスを多重分離する。この信号は外部メモリ（たとえばＲＡＭ　２８やＥＰＲＯＭ　２６）で使用され、下位の８つのアドレス信号を復号する。その他の周辺装置は、ＣＰＬＤ　４６と１つまたは複数のオクタルバスドライバ４８の組み合わせによって処理され、制御される。ＣＰＬＤ　４６は、上位の８つのアドレスラインを復号し、適切なオクタルバスＢＵＳドライバ４８に対してＥＮＡＢＬＥＤ信号を発行することで、下位の８つのアドレスラインを使用して周辺装置を処理できる。バスを介して転送された信号は、実行する機能に基づいて複数のクラスにグループ分けできるこうしたクラスには、制御信号、アドレスおよび抑止信号、データ信号がある。

【００２７】

監視機能

本発明のいくつかの構成は、セルフテストステータスおよび報告の機能を提供し、高度な監視機能をサポートする。いくつかの構成において、電源電圧は論理カード１０を備える機器の背面パネルで測定できる。たとえば、マイクロコントローラ１２で動作するソフトウェアまたはファームウェアによって、バス状態の過不足の電圧をテストし、報告する

。いくつかの構成において、監視の対象となる各電源の電圧は、パネル背面からＤＶＭで直接測定できる。

【００２８】

本発明のさまざまな構成において、マイクロコントローラ１２とＣＰＬＤ　４６は２つの別々のサブシステムとして並列に実行される。安全関連のロジックやグルーロジックをＣＰＬＤに適切に分割することで、いずれか１つのサブシステムに発生した破局的な障害が他のいずれかのサブシステムに必ずしも影響を及ぼさない。たとえば、マイクロコントローラ１２で使用するアドレス／データラッチのセット、マルチプレクサ、デマルチプレクサ、割り込みコントローラ（ｉｎｔｅｒｒｕｐｔ　ｃｏｎｔｒｏｌｌｅｒｓ）は第１のＣＰＬＤ　４６内でプログラミングしてもよい。別のＣＰＬＤ　４６（または一連のＣＰＬＤ）は、論理カード１０を含む機器の機能を実装するようにプログラミングしてもよい。マイクロコントローラ１２で使用する数百個のレジスタやアドレスデコーダ（ａｄｄｒｅｓｓ　ｄｅｃｏｄｅｒｓ）を追加してもよい（ＣＰＬＤ　４６の物理的な限界まで）。論理カード１０を含む機器の動作を定義するＣＰＬＤ　４６は、今後のプラントのアプリケーションに合わせて調整できる。たとえば、Ｉ／Ｏライン、タイマー、波形発生器（ｗａｖｅｆｏｒｍ　ｇｅｎｅｒａｔｏｒｓ）、さまざまなステートマシンを追加してもよい。マイクロコントローラ１２のグルーロジック（ＣＰＬＤ　４６内または他の場所）により、マイクロコントローラロジックサブシステム１２とＣＰＬＤロジックサブシステム４６とのバッファリングが可能になる。このような構成では、バッファリングＣＰＬＤ　４６が正常に動作している限り、マイクロコントローラ１２内のロジックの破局的な障害は機器の論理カード１０の性能には影響を及ぼさない。こうした分割によって、機器の論理カード１０は動作でき、安全上の分類の異なる他の機器にインターフェイスできる。たとえば、ＣＰＬＤ　４６はその動作が人命を左右する安全に関連する機能を実行できる。ＥＰＲＯＭ　２６および／またはＲＡＭ　２８内にマイクロコントローラ１２に対して人命を危険にさらす安全以外の機能を実行するように命令するソフトウェアまたはファームウェアを配置できる。あるいは、ＣＰＬＤ　４６は安全関連以外の機能を実行してもよい。ＥＰＲＯＭ　２６および／またはＲＡＭ　２８と組み合わせて安全関連の機能を実行してもよい。ＣＰＬＤ　４６とマイクロコントローラ１２は、選択された機能を協調的に実行するように構成してもよい。前面パネルインディケータ３０および／または４４は論理カード１０で制御されており、論理カード１０で監視かつ／または制御する外部システムに関する情報（たとえば、バルブやポンプの状態、または機器への入力を提供する外部センサー）をユーザーに提供する。

【００２９】

前述のように、論理カード１０はさまざまなタイプの機器（たとえば、ＯＬＵ、ＳＬＣ、ＨＰＣＦ）で利用できるが、特に原子力発電所内にある複数の安全システムに適している。たとえば、原子炉容器（ｒｅａｃｔｏｒ　ｖｅｓｓｅｌ）を備える原子力発電所内のホウ酸注入系（ＳＬＣ）の１つの構成では、４つのスクラム失敗イベント（ＡＴＷＳ：Ｔｒａｎｓｉｅｎｔ　Ｗｉｔｈｏｕｔ　Ｓｃｒａｍ）論理ユニットの少なくとも２つによって、またはオペレータが起動したキースイッチによってコマンドが発行された場合に、原子炉容器にホウ素溶液が注入される。注入のプロセスは、ロッドの動作を制御しなくても原子炉を全出力から臨界前（ｓｕｂ－ｃｒｉｔｉｃａｌ）の状態にするのに十分である。いくつかの構成において、ＳＬＣシステムは２つの冗長ＳＬＣ論理ユニットコントローラを備えており、安全区分１と２に配置する。図３を参照すると、ＳＬＣ論理プロセッサ１００として構成された論理カード１０をＳＬＣシステムで使用し、自動または手動で起動する。起動すると、ＳＬＣ論理プロセッサ１００は必要なバルブとポンプを自動的に制御し、原子炉を全出力から臨界前の状態にする。ＳＬＣ論理プロセッサ１００はハードウェアベースとソフトウェアベースのロジック（マイクロコントローラ１２とＣＰＬＤ　４６）を協調的に使用して、ＳＬＣ論理プロセッサ１００のステータスを監視かつ報告し、監視機能を自動化するための制御機能とソフトウェアを実現する。ＳＬＣ論理プロセッサ１００内の論理カード１０はモジュール方式で設計されており、機器の障害に関する通知を

オペレータに自動送信するように構成できる。いくつかの構成では、セルフテストソフトウェアおよびハードウェアの機能が提供され、モジュールレベルで障害を特定できる。したがって、モジュールを交換することでＳＬＣ論理プロセッサ１００のさまざまな構成を迅速に修復できる（たとえば３０分以内）。

【００３０】

ＳＬＣ論理プロセッサ１００はＮＵＭＡＣファミリのメンバーであり、論理カード１０（ＣＰＬＤ　４６を含む）、マイクロコントローラ１２、ソフトウェア／ファームウェアプログラミングを含んでいる。いくつかの実施形態は、ＳＬＣ注入の中央制御室パネル（Ｍａｉｎ　Ｃｏｎｔｒｏｌ　Ｒｏｏｍ　Ｐａｎｅｌ）から送信される手動の起動／停止信号を処理して「深層防護（Ｄｅｆｅｎｓｅ　ｉｎ　Ｄｅｐｔｈ）」を実現し、このシステムの多様性の要件を満足するように構成されている。いくつかの構成では、さらに前面パネル（図４を参照）に機器のセルフテストとステータス診断が表示され、Ｒｅａｃｔｏｒ　Ｔｒｉｐ　ａｎｄ　Ｉｓｏｌａｔｉｏｎ　Ｆｕｎｃｔｉｏｎ（ＲＴＩＦ）Ｃｏｍｍｕｎｉｃａｔｉｏｎｓ　Ｉｎｔｅｒｆａｃｅ　Ｍｏｄｕｌｅ（ＣＩＭ）に送信される。いくつかの構成において、安全に関連する機能は、ハードワイヤード（ｈａｒｄｗｉｒｅｄ）（ＣＰＬＤ　４６）とＳＬＣ論理プロセッサ１００内のソフトウェアロジックで協調的に実行される。ソフトウェアはこうした機能をセルフテスト診断で監視し、光ファイバモジュール４０を経由してステータスメッセージをＣＩＭに送信する。また、ソフトウェアはシャーシの前面パネル５４のＬＥＤ　３０と英数字ディスプレイ４４を制御し、前面パネルの押しボタンとキーロックスイッチ５６に直ちに反応する。いくつかの構成において、ハードワイヤード／ＳＬＣ論理プロセッサのソフトウェアによる協調的な機能には、中央制御室パネル（ＭＣＲＰ）上の２４のコンタクト入力モジュール（Ｃｏｎｔａｃｔ　Ｉｎｐｕｔ　Ｍｏｄｕｌｅ）４２を介してＭＣＲＰから信号を受信する機能、ソリッドステートリレーを介してインディケータライトを制御する機能、さらにラッチリレー制御モジュール（Ｌａｔｃｈｉｎｇ　Ｒｅｌａｙ　Ｃｏｎｔｒｏｌ　Ｍｏｄｕｌｅ）４２を介してポンプとバルブを制御する機能が含まれる。

【００３１】

コンタクト入力モジュール４２（たとえば、いくつかの構成では２４のコンタクト入力モジュール）はＭＣＲＰにインターフェイスし、オペレータはさまざまなスイッチや押しボタンを使用してＳＬＣ論理プロセッサ１００を制御できる。また、コンタクト入力モジュール４２はポンプ、バルブ、スイッチギアからステータス信号を受信する。

【００３２】

本発明のいくつかの構成において、光ファイバモジュール４０には少なくとも１つの送信機が含まれる。光ファイバモジュール４０は、ＳＬＣ論理プロセッサ１００とＲｅａｃｔｏｒ　Ｔｒｉｐ　ａｎｄ　Ｉｓｏｌａｔｉｏｎ　Ｆｕｎｃｔｉｏｎ（ＲＴＩＦ）Ｃｏｍｍｕｎｉｃａｔｉｏｎ　Ｉｎｔｅｒｆａｃｅ　Ｍｏｄｕｌｅ（ＣＩＭ）との通信リンクを提供する。

【００３３】

いくつかの構成において、図４を参照すると、ＳＬＣ前面パネル５４アセンブリはオペレータとＳＬＣ論理プロセッサとのローカルインターフェイスを提供する。ＳＬＣ前面パネルアセンブリには、オペレータがセルフテストを開始し、ＳＬＣ論理プロセッサとホウ素注入系のステータスを監視するための押しボタンとキーロックスイッチ５６が含まれる。前面パネルのＬＥＤ　３０とディスプレイ４４は、ＡＴＷＳ信号、バイパス信号、アナログトリップモジュール（ＡＴＭ：Ａｎａｌｏｇ　Ｔｒｉｐ　Ｍｏｄｕｌｅ）信号、中央制御室パネル（ＭＣＲＰ）信号、リレー、セルフテストの結果、およびＳＬＣ論理プロセッサの動作モードを示している。

【００３４】

本発明のいくつかの構成において、２つのラッチリレーモジュール４２はそれぞれ１２個の機械的ラッチリレーと２つのソリッドステートリレー（ｓｏｌｉｄ－ｓｔａｔｅ　ｒｅｌａｙｓ）を備えている。ラッチリレーコンタクト（ｌａｔｃｈｉｎｇ　ｒｅｌａｙ

ｃｏｎｔａｃｔｓ）を使用してポンプの起動と停止、およびバルブの開閉機能を制御する。ソリッドステートリレーを使用して、ＭＣＲＰ上に配置されたインディケータライトを操作する。

【００３５】

ＳＬＣ論理プロセッサカード１０は、ＳＬＣ論理プロセッサのロジックによる処理、監視、通信の各機能を提供する。このモジュールには、マイクロコントローラ１２、メモリ３８、２６、２８、ＣＰＬＤ　４６、およびインターフェイスロジックが含まれる。このモジュールは、入力モジュール３４からのＭＣＲＰ信号のステータスを表す信号を受信し、ホウ素タンクレベル信号を受信する。さらに、ノンラッチ（Ｎｏｎ－Ｌａｔｃｈｉｎｇ）リレーモジュール４２上のリレーを制御し、光ファイバモジュール４０のインターフェイスしてＲＴＩＦ　ＣＩＭにメッセージを送信する。マイクロコントローラスーパーバイザは、電源１６および／または１８からの入力電圧が範囲外の場合にリセット信号を生成する電源監視回路１４の形で提供される。いくつかの構成において、監視回路１４はさらにＣＰＬＤ　４６ロジックをリセットして初期状態に戻す。ウォッチドッグタイマー５８は、あらかじめ指定した時間（たとえば１．１２秒）内にマイクロコントローラがストロボ信号を送信できなかった場合にタイムアウトする。いくつかの構成において、ウォッチドッグタイマー５８はマスク不可能な割り込み（ＮＭＩ：ｎｏｎ－ｍａｓｋａｂｌｅ　ｉｎｔｅｒｒｕｐｔ）に電気的に接続するので、ウォッチドッグタイマー５８がタイムアウトすると、マイクロコントローラ１２へのＮＭＩが生成され、ウォームリブートが行われる。ただし、ウォッチドッグタイマーによってＣＰＬＤ　４６はリセットされない。

【００３６】

いくつかの構成において、ＣＰＬＤ　４６は複雑な５６０個のマクロセル（ｍａｃｒｏ－ｃｅｌｌ）のプログラム可能な論理デバイス（ＰＬＤ：Ｐｒｏｇｒａｍｍａｂｌｅ　Ｌｏｇｉｃ　Ｄｅｖｉｃｅｓ）を備えており、ａ）　ＥＰＲＯＭ　２６およびＲＡＭ　２８メモリデバイスとメモリにマップされたすべてのＩ／Ｏ機能のアドレス復号、ｂ）　低速の周辺装置にアクセスするためのマイクロコントローラ１２の待ち状態（いくつかの構成において、前面パネルＬＥＤディスプレイ３０と２４枚のコンタクト入力カードには、読み出しアクセスと書き込みアクセスのための２つの待ち状態が必要である）、ｃ）　マイクロコントローラ１２が入力信号のステータス、出力制御、ＰＬＤ改訂、リレーのステータスにアクセスするためのアドレス指定可能なポートとレジスタ、ｄ）　リレードライバコンポーネントにインターフェイスする５つの出力ポート、ｅ）　前面パネルディスプレイカードにインターフェイスする１つの出力ポート、ｆ）　１２ＭＨｚ～１ＭＨｚのクロックジェネレータ、ｇ）　ＳＬＣ論理プロセッサの　１）　ＡＴＭトリップステータスとコンタクト入力スイッチステータスの監視、２）　コンタクト入力の処理、３）　ポンプとバルブの制御コマンド生成のすべての機能ロジックを提供するように構成されている。

【００３７】

電流が限界に達して温度限流器が加熱されると、限流器が自動的にリセットされ、過電流の状態がなくなるまで回路が開くことで、ＳＬＣ論理モジュールの入力ラインが保護される。

【００３８】

いくつかの構成において、３２　ＫＢ　ＥＰＲＯＭ　２６はソフトウェアを格納する不揮発性のストレージを提供する。いくつかの構成において、すべてのソフトウェアはファームウェアとして不揮発性メモリに格納されるので、ソフトウェアの変更はＥＰＲＯＭの交換によって実行される。いくつかの構成において、８　ＫＢのスタティックＲＡＭ　２８はマイクロコントローラ１２から要求される高速の読み出し／書き込みメモリを提供する。いくつかの構成で提供される不揮発性の２Ｋｘ８強誘電性ＲＡＭ　３８は、電力が供給されなくなっても失われてはならないアプリケーションパラメータの記憶場所を提供する。このＲＡＭは電力消費が低く、耐久性がきわめて高いシリアルデバイスである。マイクロコントローラのポート１を介した４線のシリアルインターフェイスによって、メモリデバイス内の任意のバイトにアクセスできる。ＮＶＲＡＭ　３８に格納する変数の例には

、１） コールドブートカウンタ、２） ウォームブートカウンタ、３） ウォッチドッグカウンタ、４） 電源電圧の測定値と設定値、５） エラーコード、６） セルフテストステータスがあるが、これらに限定はされない。

【００３９】

ＬＥＤ ６０は、論理カード１０自体の上に配置され、テストおよび／または障害を示している。また、必要に応じて電圧とタイミングを観測するさまざまなテストポイントと監視ポイントが提供される。

【００４０】

ＳＬＣ論理プロセッサ１００は、シャーシ背面にあるコネクタを介して光ファイバ出力などのさまざまな電気信号にインターフェイスする論理カード１０を備えている。電気的入力には、中央制御室パネルやさまざまなポンプ、流量計、圧力トランスデューサ（ｔｒａｎｓｄｕｃｅｒｓ）上のコンタクトクロージャ（ｃｏｎｔａｃｔ ｃｌｏｓｕｒｅｓ）が含まれる。シャーシの前面パネルにも、複数の電気的コンタクト入力が配置されている。こうした入力には、押しボタンやキーロックスイッチ５６が含まれる。

【００４１】

イベントベースオペレーティングシステム（ＥＢＯＳ）

いくつかの構成において、原子力発電所向けのホウ酸注入系（ＳＬＣ）はＩｎｔｅｌ Ｃｏｒｐｏｒａｔｉｏｎ，Ｓａｎｔａ Ｃｌａｒａ，ＣＡから入手できるＩＮＴＥＬ（登録商標）８７Ｃ１９６ＫＤマイクロコントローラ１２を使用している。論理プロセッサカード１０は、さらに８ ＫＢのランダムアクセスメモリ（ＲＡＭ：Ｒａｎｄｏｍ Ａｃｃｅｓｓ Ｍｅｍｏｒｙ）２８、３２ ＫＢの外付けの電気的にプログラム可能な読み出し専用メモリ（ＥＰＲＯＭ：Ｅｌｅｃｔｒｉｃａｌｌｙ Ｐｒｏｇｒａｍｍａｂｌｅ Ｒｅａｄ Ｏｎｌｙ Ｍｅｍｏｒｙ）２６、および２ ＫＢの不揮発性メモリＮＶＲＡＭ ３８が含まれる。「ＫＤ」バージョンのマイクロコントローラ１２には、さらに１０２４バイトの内蔵ＲＡＭと３２ ＫＢの１度のみ書き込み可能な読み出し専用メモリ（ＲＯＭ：Ｒｅａｄ Ｏｎｌｙ Ｍｅｍｏｒｙ）が含まれる。ただし、これらは本発明のいくつかの構成では使用されない。本発明のいくつかの構成において、ノンプリエンプティブなイベントベースのオペレーティングシステム（ＥＢＯＳ）が提供される。これは、特にこうしたハードウェアアーキテクチャおよび原子力発電所内のＳＬＣシステムに適している。ただし、本発明のＥＢＯＳ構成は、ＳＬＣシステムにも原子力発電所での利用にも限定はされず、特定のタイプのマイクロコントローラ、マイクロプロセッサ、コンピュータ、論理カードのいずれにも限定はされない。

【００４２】

マイクロコントローラ１２は、高速の計算と迅速な入力／出力（Ｉ／Ｏ）操作を行う１６ビットのＣＨＭＯＳデバイスである。

【００４３】

８７Ｃ１９６ＫＤマイクロコントローラ１２は、さまざまな方法で構成できる２つの別々の内蔵タイマーを提供する。本発明のいくつかの構成では、多くのタイマー（たとえば８個以上の同期タイマー）を提供する。多くのハードウェア（たとえば外付けのタイマー）を提供しないように、本発明のいくつかの構成では、限られた数のハードウェアタイマー（たとえばマイクロソフトコントローラ１２の２つのタイマー）を使用して多くのタイマーがあるように見せかけるＥＢＯＳを提供する。このように、本発明のいくつかの構成では、ＥＢＯＳと適切なアプリケーションソフトウェアを提供し、時間指定イベントより少ない数のタイマーで複数の時間指定イベントを検出し、追跡する。中央のタイミング（ｔｉｍｉｎｇ）機能が提供され、本明細書では個別の「チック」を提供するシステムクロックと呼ぶ。本発明のいくつかの構成では、唯一のタイマーを使用して中央のタイミング機能を提供し、すべてのタイミング機能が唯一のポイントから制御され、監視され、更新されるので、決定性（ｄｅｔｅｒｍｉｎｉｓｍ）のレベルが向上する。

【００４４】

本発明のいくつかの構成では、スケジューラとシステムクロックの両方を提供し、タイ

ミングイベントを管理する。スケジューラを使用することでイベントベースのオペレーティングシステム（ＥＢＯＳ）の抽象化とカプセル化が進み、結果として実装に必要なコードの量が減少するとともに、モジュール性が向上し、ソフトウェアメンテナンスコストが削減される。いくつかの構成では、さらにコンテキストスイッチャ（ｃｏｎｔｅｘｔ　ｓｗｉｔｃｈｅｒ）が提供される。実行ループにおいて、コンテキストスイッチャはたとえば１つまたは複数のＣＡＳＥ文またはＩＦ、ＥＬＳＥ文の組み合わせを含むソフトウェアモジュールを備えていてもよい。（ＣＡＳＥ文とＩＦ、ＥＬＳＥ文の組み合わせは、ＣおよびＣ＋＋プログラミング言語のコードである。他の言語の相当する文も使用できることは、コンピュータプログラミング技術者には言うまでもない。本明細書と添付の特許請求の範囲に記載するこのＣまたはＣ＋＋に固有の表現は、本発明と請求項をＣまたはＣ＋＋プログラミング言語を使用する構成またはこれを含む構成に限定するものと理解してはならない。）コンテキストスイッチャは実行機能のプリエンプション（ｐｒｅｅｍｐｔ）を行い、プリエンプションを行った機能を正確に復元するために必要なオーバーヘッドを提供する。しかし、本発明のいくつかの構成では、こうしたプリエンプションが提供されず、それに伴う複雑性は回避される。代わりに、コンテキストスイッチャは抽象化とカプセル化を使用したブランチアクティビティ（ｂｒａｎｃｈｉｎｇ　ａｃｔｉｖｉｔｙ）を呼び出す。

【００４５】

いくつかの構成ではセマフォが提供され、これを使用してアトミックな（ａｔｏｍｉｃ）操作を保護する。たとえば、いくつかの構成において唯一のセマフォ構造が提供され、ＥＢＯＳでイベントが発生したがイベントの厳密な特性がわからない場合に、残っているアプリケーションソフトウェアについて通知する。このように、機能をモジュール化でき、ＳＬＣの安全性と堅牢性を維持できる。

【００４６】

ＥＢＯＳイベントは、スケジューラの外付けハードウェア割り込みの結果として、または入力レジスタがポーリングするときに発生する。いくつかの構成において、スケジューラは割り込みを生成するハードウェアタイマーでも定義される。本発明のいくつかの構成で使用する８ＸＣ１９６ＫＤマイクロコントローラは、ハードウェアイベント割り込みを処理するように構成されているが、本発明の多くの構成では割り込みの使用を制限または限定している。８ＸＣ１９６ＫＤマイクロコントローラは、周辺装置ステータスタイマー（ＰＳＴ：Ｐｅｒｉｐｈｅｒａｌ　Ｓｔａｔｕｓ　Ｔｉｍｅｒｓ）、パルス幅変調（ＰＷＭ：Ｐｕｌｓｅ　Ｗｉｄｔｈ　Ｍｏｄｕｌａｔｏｒｓ）、高速Ｉ／Ｏ（ＨＳＩＯ：Ｈｉｇｈ　Ｓｐｅｅｄ　Ｉ／Ｏ）を含む１８種類の割り込みを提供する。ただし、本発明のいくつかの構成では、使用する割り込みを制限している。たとえば、割り込みをタイマー割り込み（システムクロックとスケジューラで使用する）、押しボタンイベントをキャプチャする外部割り込み、送信（ＴＸ）割り込み（マイクロコントローラのＴＸポートにデータを送信する）、マスク不可能な割り込み（ＮＭＩ、ウォッチドッグタイマーで使用する）に制限してもよい。

表Ｉは割り込みと、８ＸＣ１９６ＫＤマイクロコントローラが提供する優先順位のリストである。本発明のいくつかの構成ではこのすべてを利用できる。

【００４７】

表Ｉ

【表１】
【表1】

| 優先順位 | 割り込み名 | 割り込みアプリケーションステータス |
|---|---|---|
| 0 | タイマーオーバーフロー割り込み | 無効 |
| 1 | Ａ／Ｄ変換完了割り込み | 無効 |
| 2 | ＨＳＩデータ利用可能割り込み | 無効 |
| 3 | ＨＳＯ割り込み | 無効 |
| 4 | ＨＳＩ．０ピン割り込み | 無効 |
| 5 | タイマー割り込み | 無効 |
| 6 | シリアルポート割り込み | 無効 |
| 7 | 外部割り込み | 有効（診断モードで押しボタンのみ） |
| 8 | 送信割り込み | 有効 |
| 9 | 受信割り込み | 標準モードで無効、ＩＮＯＰセルフテストで有効 |
| １０ | ＨＳＩ　ｆｉｆｏ　４割り込み | 無効 |
| １１ | タイマー２キャプチャ割り込み | 無効 |
| １２ | タイマー２オーバーフロー割り込み | 有効（システムクロック） |
| １３ | 外部割り込み１ | 無効 |
| １４ | ＨＳＩ　ｆｉｆｏ　ｆｕｌ１割り込み | 無効 |
| １５ | ＮＭＩ | 有効（無効化できない） |
| Ｎ／Ａ | ソフトウェアトラップ | エラー処理の場合は有効 |
| Ｎ／Ａ | 実装されていないＯｐＣｏｄｅ | エラー処理の場合は有効 |

【００４８】

割り込みを使用することで決定性が向上し、マイクロコントローラのハードウェア割り込みの優先順位スキーマに従ってＥＢＯＳイベントに優先順位が割り当てられる。８ＸＣ１９６ＫＤ上の割り込みは、優先順位に従って処理される。番号が大きい割り込みほど処理の優先順位が高い。ＳＬＣのいくつかの構成では、ＮＭＩ、ソフトウェアタイマーのオーバーフロー、ＴＸデータ、最後に外付けハードウェア割り込みの順に処理される。ソフトウェアトラップと実装されないＯｐコード割り込みには優先順位を割り当てていない。いくつかの構成では、一般的なタイマー割り込みの代わりにタイマー２オーバーフロー割り込みを使用することで、システムクロックとその機能の優先順位を上げ、システムクロックが押しボタン、データ送信、入力イベントのポーリングより優先されることを保証している。このような構成では、ＮＭＩ（ウォッチドッグで使用する）はタイマー２オーバーフロー割り込みより優先される唯一のイベントである。

【００４９】

本発明のいくつかの構成において、ＥＢＯＳで処理できる各イベントに優先順位が割り当てられるので、いったんスケジュールされたイベントがアクティブになると、優先順位の最も高いイベントがスケジューラで処理される。ＳＬＣアプリケーションの１つの構成で使用するためにローカライズされたイベントを、優先順位に従って表ＩＩにリストアップする。イベントには、安全機能と応答時間に従って優先順位が割り当てられる。この特定の構成では、ダブルワード（ＤＷＯＲＤ）セマフォを使用しているので、ＤＷＯＲＤの３２ビット中の３１ビットがさまざまなイベントと優先順位に対応する割り込みとは異なり、低い優先順位の数値を割り当てられたイベントが最初に実行される。こうしたイベントは特定のＳＬＣアプリケーション構成に関連するが、他の多くのイベントドリブン型システムで発生するイベントについても同様の優先順位のリストを作成できる。したがって

、本発明の構成がＳＬＣアプリケーションでの使用のみに限定されないことは言うまでもない。

【００５０】

表ＩＩ

【００５１】

【表２－１】

【表２－１】

| 優先順位 | イベント名 | イベントの説明 |
|---|---|---|
| １． | ＦＵＮＣＴＩＯＮ＿ＴＩＭＥ＿ＯＵＴ | 機能にかかる時間が長すぎる。 |
| ２． | ＳＭ＿ＩＮＰＵＴ＿ＣＨＡＮＧＥ | ステートマシンの入力が変更された。 |
| ３． | ＭＯＤＥ＿ＣＨＡＮＧＥ | 機器のモードが変更された。 |
| ４． | ＳＥＬＦ＿ＴＥＳＴ | セルフテストのステータスが変更された。 |
| ５． | ＡＴＷＳ＿ＰＲＥＳＥＮＴ | 有効なＡＴＷＳ緩和（Ｍｉｔｉｇａｔｉｏｎ）イベントパルスを０．５秒間生成し、次のパルスまでのすべての入力を無視する。 |
| ６． | ＦＬＡＳＨ＿ＬＡＭＰＳ | ０．５秒が経過し、ランプが点滅すると、ランプの状態がオンの場合にオフになり、オフの場合はオンになる。 |
| ７． | ＩＮＪ＿ＣＯＭＰＬＥＴＥ | 注入完了信号を実際の信号の期限が切れてから２．５秒間保持する。 |
| ８． | ＴＸ＿ＭＥＳＳＡＧＥ | 最後のメッセージ送信から０．５秒が経過した。 |
| ９． | ＭＢＶ５＿ＯＶＥＲＬＯＡＤ＿ＢＹＰＡＳＳ | ＭＢＶ５過負荷バイパス（Ｏｖｅｒｌｏａｄ　Ｂｙｐａｓｓ）信号がバイパス信号のない状態で２．５秒間要求された。 |
| １０． | ＭＢＶ１＿ＯＶＥＲＬＯＡＤ＿ＢＹＰＡＳＳ | ＭＢＶ１過負荷バイパス信号がバイパス信号のない状態で２．５秒間要求された。 |
| １１． | ＰＵＭＰ＿ＳＴＡＲＴ＿ＴＲＩＰ | ポンプ起動信号が２．５秒間要求された。 |
| １２． | ＰＵＭＰ＿ＯＮ＿ＳＩＧＮＡＬ | ポンプ停止信号を受信してからポンプが２．５秒間動作している（停止しようとしたが実際には動作している）。 |
| １３． | ＰＵＭＰ＿ＲＵＮ＿Ｗ＿ＡＴＷＳ | ＡＴＷ自動起動（Ｉｎｉｔｉａｔｅ　Ａｕｔｏ　Ｓｔａｒｔ）信号とポンプ稼働（Ｐｕｍｐ　Ｒｕｎｎｉｎｇ）信号が２．５秒間存在している。 |
| １４． | ＢＲＥＡＫＥＲ＿ＮＯＴ＿ＳＥＴ | ブレーカーが設定されない状態で蓄積エネルギー（ｓｔｏｒｅｄ　ｅｎｅｒｇｙ）信号が２．５秒間存在している。 |
| １５． | ＭＢＶ５＿２＿５＿ＳＥＣ＿ＥＶＥＮＴ | ２．５秒の遅延の間にバルブが動作（開くまたは閉じる）を開始するか、あるいは動作を開始しない場合に信号が設定され、保持される。 |

【００５２】

【表２－２】
【表２－２】

| | | |
|---|---|---|
| １６． | ＭＢＶ５＿ＶＬＶ＿ＳＴＲＯＫ＿ＥＶＥＮＴ | ３１．５秒の遅延の間にバルブが開閉を終了するか、あるいは動終了しない場合に信号が設定され、保持される。 |
| １７． | ＭＢＶ１＿２＿５＿ＳＥＣ＿ＥＶＥＮＴ | ２．５秒の遅延の間にバルブが動作（開くまたは閉じる）を開始するか、あるいは動作を開始しない場合に信号が設定され、保持される。 |
| １８． | ＭＢＶ１＿ＶＬＶ＿ＳＴＲＯＫＥ＿ＥＶＥＮＴ | １０１．５秒の遅延の間にバルブが開閉を終了するか、あるいは動終了しない場合に信号が設定され、保持される。 |
| １９． | ＬＡＭＰ＿ＴＥＳＴ＿ＥＶＥＮＴ | ランプテストイベントの継続をスケジュールし、ランプテスト機能がＣＰＵを独占できないようにする。 |
| ２０． | ＨＥＸ＿ＤＵＭＰ | ５秒の遅延の間にオペレータが適切なキーシーケンスを入力し、機器はＨＥＸダンプモードに入る。 |
| ２１． | ＭＥＭＯＲＹ＿ＲＥＳＥＴ＿ＥＶＥＮＴ | メモリリセットイベントをスケジュールする（押しボタンを押すのと同様に） |
| ２２． | ＦＩＶＥ＿ＳＥＣ＿ＥＶＥＮＴ | セルフテスト全体の表示や１行のディスプレイを更新する場合など、５秒以上かかるイベントの場合に、完了時期をスケジュールして通知し、合間に他のタスクを実行する。 |
| ２３． | ＳＴＥＰ＿ＤＩＳＰＬＡＹ＿ＥＶＥＮＴ | ステップディスプレイイベントをスケジュールする（押しボタンを押すのと同様に） |
| ２４． | ＷＤＴ＿ＴＥＳＴ | ウォッチドッグタイマーをテストするのに１．１２秒が経過した。 |
| ２５． | ＳＴＡＲＴ＿ＳＥＬＦ＿ＴＥＳＴ | セルフテスト開始イベントをスケジュールする（押しボタンを押すのと同様に） |
| ２６． | ＵＰＤＡＴＥ＿ＮＶＲＡＭ＿ＥＶＥＮＴ | ＮＶＲＡＭ内の情報を更新するための１分のイベント |
| ２７． | ＩＮＶＡＬＩＤ＿ＥＶＥＮＴ | 常に一覧の最後のイベント。 |
| ２８－３１ | Ｎ／Ａ | このＳＬＣアプリケーション構成の例では使用しない。 |

【００５３】
実行ループは、イベントをビットマップする唯一のセマフォを追跡する。イベントを処理するには、機能を実行する必要がある。本明細書で説明する例示的な構成では、スケジューラのイベントハンドラがＬＳＢからＭＳＢの順にイベントを１度に１つずつ処理する（ＤＷＯＲＤセマフォで指定する）。０のイベントが最も優先順位が高い。本発明のいくつかの構成では、複数のイベントのどれを実行するかを決定するときにレイテンシー（ｌａｔｅｎｃｙ）を考慮する。より具体的には、特定のスケジュールされたイベントが他のスケジュールされたイベントより短い時間で実行を終了でき、２つのイベントはそれ以外の優先順位が等しい場合に、時間が短い方が優先される。両方のイベントの絶対的なタイマーレイテンシーが同じでも、イベント全体のレイテンシーはイベントのレイテンシーにそのイベントに関連するすべてのイベントを実行する時間を加えたものである。１つのイベントが別のイベントの後にスケジュールされた場合は、２つのレイテンシーが発生し、

レイテンシーのパーセンテージは直ちに実行するようにスケジュールされたイベントの倍になる。ただし、２つのレイテンシーが発生する長期のイベントは、１つのレイテンシーが発生する短期のイベントより実行時間に対するレイテンシーのパーセンテージとしては低くなる可能性がある。したがって、本発明のいくつかの構成では、短期のイベントは優先順位の同じ長期のイベントより前にスケジュールされる。

【００５４】

さらに、本発明のいくつかの構成では、安全に関連しない機能には最も低い優先順位が割り当てられる。たとえば、ランプテストイベントは１クロックチックの最長時間、最悪の場合、５０ミリ秒のチックで実行できるので、クロックチックの直後にランプテストボタンを押した場合はランプテストが１００ミリ秒にわたって実行されている可能性がある。オペレータがランプテストボタンを押した状態で１チックを過ぎると、ランプテストが再スケジュールされる。ＳＬＣに優先順位の高いイベントが続けざまに発生すると、ランプテスト機能（またはその他の優先順位の低い安全に関連しない機能）は特定の期間は実行できない。ただし、本発明のいくつかの構成では、すべての機能を６ミリ秒以内に実行できるように構成されているので、こうした状況が発生する可能性は低い。

【００５５】

いくつかの構成では、グローバルフラグセマフォを使用して一部の機能またはイベントの実行を許可または拒否できる。すべてのイベントが実行される可能性があること、そして優先順位の高いイベントはＣＰＵ　１２を独占しないことを保証するために、イベントがＡＣＴＩＶＥになるクロックチックごとに、「Ｔｉｍｅ　Ａｃｔｉｖｅ」ＥＣＢエントリが増分される。いくつかの構成では、２６のイベントが同時にスケジュールされた場合に、１チックの間にどのイベントにも実行されるチャンスが与えられる。このような構成では、１つのイベントが実行されずに２６チックを経過すると、シャドウセマフォマスク（ｓｈａｄｏｗ　ｓｅｍａｐｈｏｒｅ　ｍａｓｋ）によってこのイベントに優先順位が割り当てられ、次にこのイベントが実行される。

【００５６】

本発明のいくつかの構成では、指定されたセマフォ、システムクロック、スケジュールアップデータ（ｓｃｈｅｄｕｌｅ　ｕｐｄａｔｅｒ）を使用した決定性が保証される。スケジューラとセマフォを組み合わせて使用することで、予想以上に時間のかかるイベントを監視する。スケジューラでセマフォを使用すると、システム障害、プリエンプション、後続のシステムのウォームスタートが発生する。これらはすべてオペレータの注意を促す異常な状態を発生し、望ましい決定性の結果をもたらす。

【００５７】

さまざまなイベントハンドラ、押しボタン、タイミング、ステートマシンが連携することで、実行中のステートマシンに１つの処理状態から別の処理状態へのコンテキストの切り替えが発生する。コンテキストの切り替えが発生するまで、ステートマシンは実行ループによってセルフテストモードで無限にループする。３つのイベントハンドラを使用して、動作中にマシンに発生するさまざまなタイプのイベントを処理する。

【００５８】

より具体的には、図５を参照すると、本発明のいくつかの構成では、流れ図２００によって２２２で表現される実行ループを提供する。このループの技術的な効果は、たとえば工場の運転中に発生するイベントのタイミング調整とスケジューリングである。ポイント２０２、２０４、２０６、２０８は、イベントハンドラ起動の原因となるイベントとしてラベル付けされた開始ポイントを表す。終了ポイントは２９０、２９２、２９４で示されている。押しボタンイベントは、押しボタンイベントハンドラ２１０でほとんど排他的に処理される。このハンドラは、いくつかの構成において押しボタンを押すことで発生する外部イベントによってのみ起動するランプテスト機能２１２は、ＣＰＵを独占できないので、５０ミリ秒または１クロック「チック」のランプテスト機能２１２は保留になり、他のイベントが処理される。したがって、ランプテスト機能２１２のスケジュール自体が再実行され、次にタイマー／スケジューライベントハンドラ２１８がこのスケジュールを処

理する。システムクロックは、スケジュール更新ハンドラ２１４を使用して、５０ミリ秒間隔でスケジューリングイベントが発生していないかをチェックする。ユーザーがモードを変更した場合、または入力ステータスの変更が検出された場合は、ステートマシンイベントハンドラ２１６が起動する。診断モードでは押しボタンイベントが直ちに処理され、完了するとコンテキストはスイッチによって中断されていた機能に戻る。タイマーイベントとステートマシンイベントが発生すると、一般にステートマシンが変更される。この場合は、ステートマシン更新ハンドラ２２０が呼び出され、完了するとコンテキストは実行ループの２９４に戻る。２２２で、ＣＩＭへのステータス送信イベントがスケジュールされる。ＴＸイベントが発生すると、送信バッファにデータが入り、２２４で別の送信機能が生成されてメッセージが送信される。メッセージの送信が完了すると、コンテキストは実行ループの最後の状態でもある２９４に直ちに返される。本発明のさまざまな構成において、その他のイベントハンドラ（ステップディスプレイハンドラ２２６、トリップメモリリセットハンドラ２２８、セルフテスト開始ハンドラ２３０、メモリ１６進表示（ｍｅｍｏｒｙ　ｈｅｘ　ｄｉｓｐｌａｙ）ハンドラ２３２、ランプ点滅設定（ｓｅｔ　ｆｌａｓｈｉｎｇ　ｌａｍｐ）ハンドラ２３４など）が提供される。一部のイベントは、スケジュールイベント削除ハンドラ２３６で処理された後にスケジュールから削除される。

【００５９】

任意のイベントをスケジュールできるが、通常はタイミングイベントのみがスケジュールされる。「Ｖａｌｖｅ　ｆａｉｌｅｄ　ｔｏ　ｍｏｖｅ（バルブが動かない）」などのアラームは、最初の信号から少し時間が経過してからキャプチャされる。イベントがスケジュールされると、タイマーが起動する。ステートマシンが変化した場合（たとえばバルブ移動信号がアサートされた場合）は、変化が発生したときにイベントがスケジュールから削除される。それ以外の場合は、イベントが発生し、ステートマシンの更新とそれに関連する後続のアラームが発生する。

【００６０】

いくつかの構成では、図６の状態図３００を参照すると、イベントの状態は５つの状態、すなわち非アクティブ３０２、待機３０４、保留３０６、アクティブ３０８、実行３１０のいずれかである。イベントがスケジュールされた場合に、実行時間は希望のタイミング要件を満たすためのクロックチック数の計算値として設定される。チックを刻むたびに、実行時間が減少する。実行時間がゼロになると、以下で説明するスケジューラの状態に関する動作で指定するように状態が変化する。レイテンシー、アクティブな時間、実行された時間もスケジュールアップデータによってクロックサイクルごとに増加または減少する。

【００６１】

ＥＢＯＳスケジューラは、スケジューライベント制御ブロック（ＥＣＢ：Ｅｖｅｎｔ　Ｃｏｎｔｒｏｌ　Ｂｌｏｃｋ）データ構造を使用する。イベントごとに、ＥＣＢへのエントリがある。たとえば、いくつかの構成において、ＥＣＢは以下の構造をとるが、これに限定はされない。

```
typedef struct scheduler_ecb
{
EVENT_STATE event_state;
WORD wait_time;
WORD execution_time;
BYTE time_executed;
WORD time_active;
} ECB;
```

【００６２】

スケジュールされた各イベントは、状態図３００に示す状態に対応する非アクティブ、アクティブ、保留、実行、待機のいずれかの状態が可能である。クロックサイクルまたはクロックチックごとに、次に示す特定のイベントの状態に基づいて、ＥＣＢが走査され、

更新される
・非アクティブなイベントは、スケジューラで特に注目する必要のないイベントである。
・アクティブなイベントは、実行される順番を待っているアクティブなイベントである。アクティブイベントが実行されないチックごとに、ｔｉｍｅ＿ａｃｔｉｖｅ Ｅｃｂエントリが増分される。
・保留中のイベントは、実行できるまで特定の時間を必要とするイベントであり、スケジュールアップデータはクロックチックごとにＥＣＢ内の「ｔｉｍｅ ｔｏ ｅｘｅｃｕｔｅ」ワードから１を減算する。「ｔｉｍｅ ｔｏ ｅｘｅｃｕｔｅ」がゼロになると、状態はアクティブに変化する。
・実行中のイベントの状態は、一部のアプリケーションでは機能開始時に設定され、機能終了時に解除される。他のアプリケーションでは、実行中の状態を使用してプログラムアプリケーションにタイマーの特定の実装（たとえばパルスタイマーか遅延タイマーか）に関する信号を送る。機能の開始と終了を制御する場合は、イベントを１度に１つずつ実行する必要があり、イベント実行中のサイクルごとに、ＥＣＢ「ｅｘｅｃｕｔｉｏｎ ｔｉｍｅ」が増分される。ｅｘｅｃｕｔｉｏｎ ｔｉｍｅはイベントが実行を許可される時間（ハードコードされた値）と比較できる。時間指定イベントのタイプを通知する場合は、状態の変化を使用してアプリケーションまたは実行ループステートマシンおよび論理パスの変化を通知できる。
・待機中のイベントは、実行されたが再び実行されるまでに特定のレイテンシーが必要である。この値は、イベントの実行が完了したときに設定され、「ｔｉｍｅ ｔｏ ｅｘｅｃｕｔｅ」と同様にチックごとにカウントダウンされる。イベントがスケジュールされ、レイテンシーが保留の時間を超えると、両方がカウントダウンされ、保留の時間がゼロになると、直ちに状態がアクティブになる。それ以外の場合は保留中になり、残り時間がカウントダウンされる。０ＸＦＦＦＦｈの値は減少しないので、この値が変わらない限り、イベントは永久に待機する。

【００６３】
本発明のいくつかの構成において、システムクロックは約５０ミリ秒ごとに１チックを刻む。チックごとに、スケジュールされたイベントがないか、イベント制御ブロック（ＥＣＢ）がチェックされる。イベントがある場合は、現在の機能を完了できるか、「タイムアウト」とタグ付けされるかに関わらず、プリエンプションが行われる。通常は、機能を完了でき、制御は実行ループに戻る。実行ループは、スケジューリングセマフォを受け取り、機能を呼び出してステートマシンを更新する。
【００６４】
本発明のいくつかの構成において、外部のウォッチドッグタイマーは１．１２秒後にタイムアウトし、正常な状態では１．００秒以内にリセットされる。ウォッチドッグは、システムクロックＩＳＲからリセットされる。これで、ウォッチドッグタスクも実行される。システムクロックＩＳＲは５０ミリ秒ごとに起動するので、５０ミリ秒以内にはリセットできない。標準モードのセルフテスト機能は、実行ループによって実行され、さまざまな機能を備えている。一般に、標準モードの各機能は５０ミリ秒以内に実行されるので、コンテキストスイッチャがより優先順位の高い機能に変わる前に、唯一のチックが終了する。本発明のいくつかの構成では、他の多くの機能が６ミリ秒以内に実行される。
【００６５】
６．１　データストアとデータ構造
【００６６】
ＥＢＯＳは、セマフォを使用してイベントがスケジュールされたかどうかを検知するとともに、グローバルに知られている必要のある特定の機能について通知する。セマフォは、２つのグループ、すなわちスケジュールされたイベントとシステムフラグに分類される。イベントセマフォは、スケジュールされたイベントが現在アクティブであり、実行を待機していることを示す。システムフラグセマフォは、特定のアトミックな機能の実行を許

可するかどうかを制御する。こうしたセマフォは、特定のアプリケーションで使用するようにカスタマイズできる。ＳＬＣアプリケーションのいくつかの構成については、こうしたセマフォの仕様が図７、図８及び図９に示されている。

【００６７】

イベントベースのマイクロＯＳを使用すると、ほんのわずかなＣＰＵオーバーヘッドで、堅牢な機能を提供し、複数のタイミングイベントを同時に追跡できる。

【００６８】

特許請求の範囲で使用する「コントローラ」という用語は、特に指定のない限り、その範囲内には、オペレーティングシステムが動作することができるマイクロコントローラ、マイクロプロセッサ、ＣＰＵ、コンピュータ、または他の同様のデバイスを含むものとすることが認識されよう。コントローラは、オペレーティングシステムを使用して、センサー、タイマー、および／またはスイッチを使用するプログラムを実行し、時間および／または制御イベントを検出できることを目的としている。コントローラには、マイクロコントローラ、およびメモリに使用するエレクトロニクスを含めてもよいがこれに限定はされない。外部信号インターフェイスをコントローラに統合してもよいが、それに限定はされない。

【００６９】

また、特許請求の範囲で使用する「プロセッサ」という用語には、特に指定のない限り、マイクロコントローラ、マイクロプロセッサ、あるいはＣＰＵを含めてもよいことが理解されよう。また、ＥＢＯＳは不揮発性メモリとしても揮発性メモリとしても提供できる（前述のＳＬＣモジュール、プロセッサ、マイクロコントローラ、ＣＰＵなどで提供されるものなど）。いくつかの構成において、ＥＢＯＳは磁気、光学、または他のタイプの媒体として提供できる。こうした構成では、磁気、光学、または他のタイプの読み取り装置が提供される。たとえば、ＥＢＯＳは不揮発性または揮発性のメモリ内の命令としても、ＣＤ－ＲＯＭ、ＤＶＤ、ＣＤ－ＲＷ、ＤＶＤ－ＲＷ、ＤＶＤ＋ＲＷ、フロッピー（登録商標）ディスク、ハードディスク、あるいは紙テープとしても提供できる。さらに、プロセッサへの命令は複数の異なるメモリユニットおよび／または媒体にわたって任意にまたは意図的に分割できるので、メモリおよび／または媒体の組み合わせを使用してもよい。したがって、特に指定のない限り、何かすることを「プロセッサに対して指示するように構成された命令を含むノンプリエンプティブなオペレーティングシステムが記録された機械可読媒体またはメモリには、これらの命令が記録された複数の機械可読媒体またはメモリ（すべて同じタイプである必要はない）が含まれるものと理解されたい。

【００７０】

本発明のさまざまな実施形態について説明してきたが、本発明の精神と範囲を逸脱しない限りの変更が可能なことは、当業者には言うまでもない。なお、特許請求の範囲に記載された符号は、理解容易のためであってなんら発明の技術的範囲を実施例に限縮するものではない。

【図面の簡単な説明】

【００７１】

【図１】本発明による論理カードのさまざまな構成を示すブロック図である。

【図２】図１に示す論理カードに適したバス構成の１つを示す概略図である。

【図３】図１に示す論理カード構成を備える安全制御機器（この場合は、ホウ酸注入系［ＳＬＣ］の論理プロセッサ）を示すブロック図である。

【図４】図３に示す機器構成の前面パネルを示す実体図である。

【図５】本発明のいくつかの構成による実行ループ構成を示す流れ図である。

【図６】図５に示す実行ループを実行する間に本発明のいくつかの構成で発生する可能性のあるイベントの状態を示す状態図である。

【図７】本発明のいくつかの構成で使用するイベントセマフォを示す図である。

【図８】本発明のいくつかの構成で使用するイベントセマフォを示す図である。

【図９】本発明のいくつかの構成で使用するフラグセマフォを示す図である。

【図１】

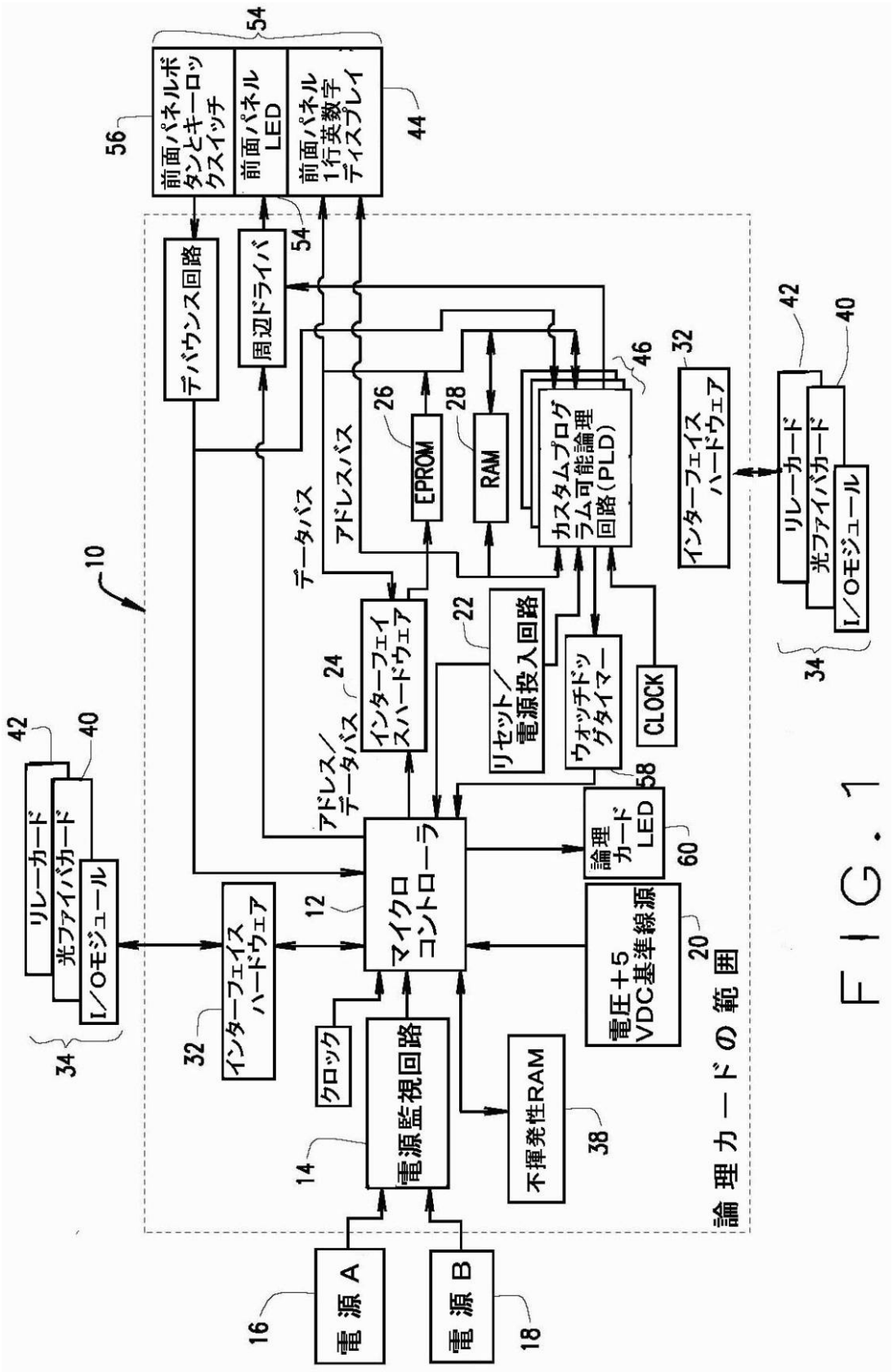
前面パネルボタンとキーロックスイッチ
前面パネルLED
前面パネル1行英数字ディスプレイ
54
56
44
デバウンス回路
周辺ドライバ
データバス
アドレスバス
EPROM
RAM
カスタムプログラム可能論理回路(PLD)
インターフェイスハードウェア
リセット／電源投入回路
ウォッチドッグタイマー
CLOCK
アドレス／データバス
マイクロコントローラ
論理カードLED
電圧＋5 VDC基準線源
クロック
電源監視回路
不揮発性RAM
電源A
電源B
リレーカード
光ファイバカード
I／Oモジュール
10
12
14
16
18
20
22
24
26
28
32
34
38
40
42
46
58
60
論理カードの範囲

FIG. 1

【図２】

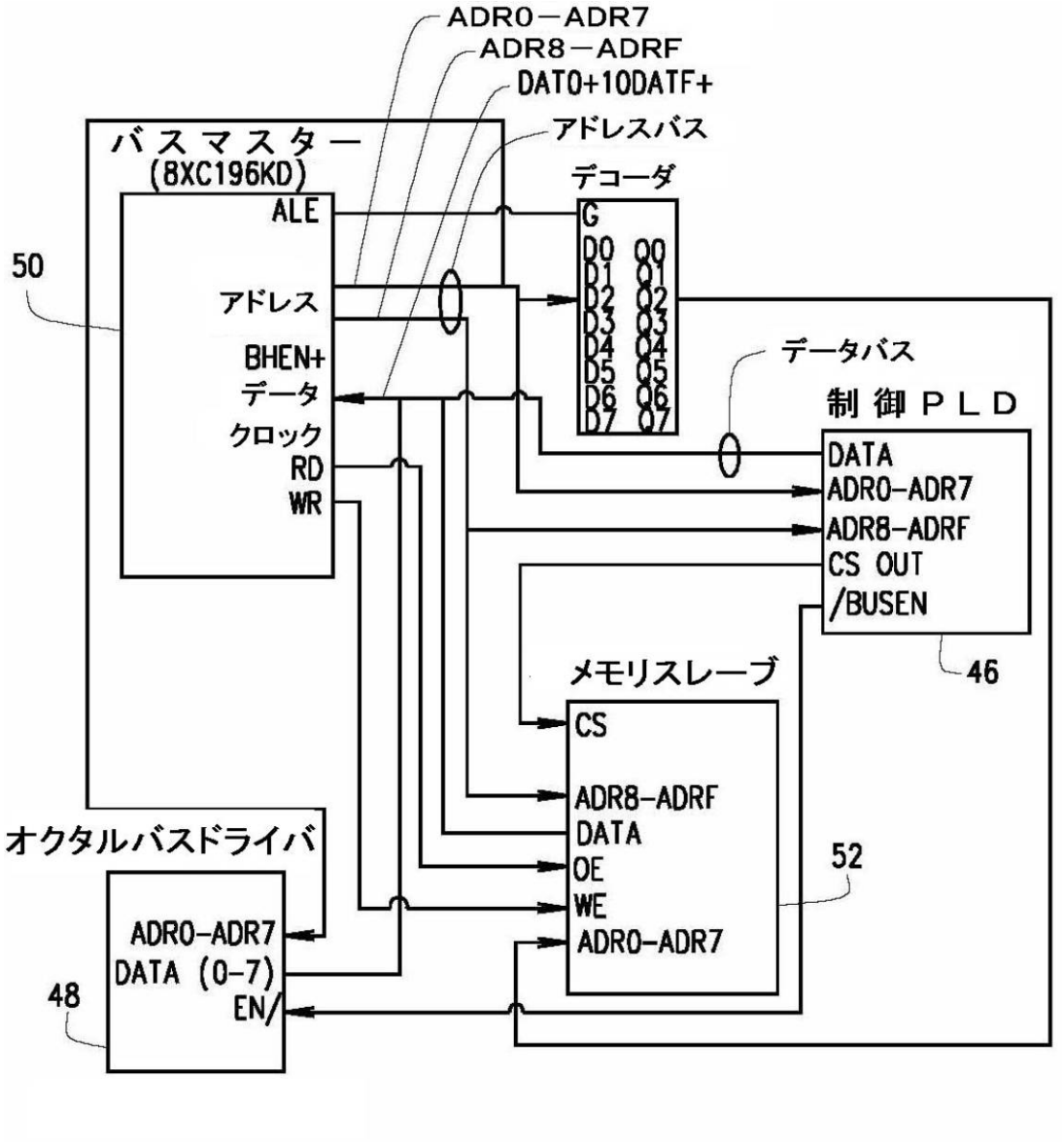
ADR0－ADR7
ADR8－ADRF
DAT0+10DATF+
アドレスバス
バスマスター
(8XC196KD)
ALE
アドレス
BHEN+
データ
クロック
RD
WR
50
デコーダ
G
D0 Q0
D1 Q1
D2 Q2
D3 Q3
D4 Q4
D5 Q5
D6 Q6
D7 Q7
データバス
制御ＰＬＤ
DATA
ADR0-ADR7
ADR8-ADRF
CS OUT
/BUSEN
46
メモリスレーブ
CS
ADR8-ADRF
DATA
OE
WE
ADR0-ADR7
52
オクタルバスドライバ
ADR0-ADR7
DATA (0-7)
EN/
48

FIG.2

【図３】

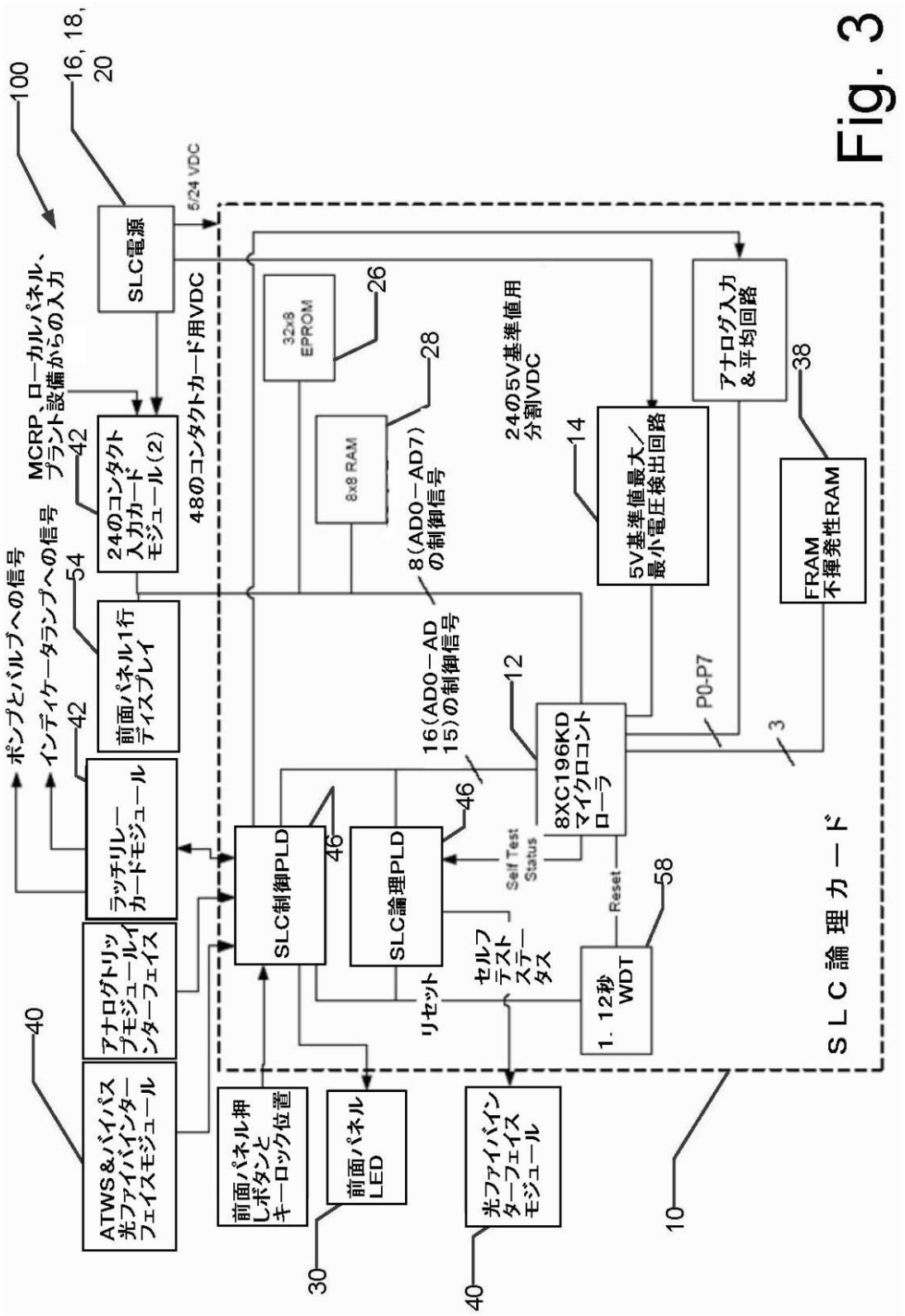
Fig. 3
100
16, 18, 20
SLC電源
5/24 VDC
48のコンタクトカード用VDC
MCRP、ローカルパネル、プラント設備からの入力
インディケータランプへの信号
ポンプとバルブへの信号
24のコンタクト入力カードモジュール(2)
42
前面パネル1行ディスプレイ
54
ラッチリレーカードモジュール
アナログトリップモジュールインターフェイス
ATWS&バイパス光ファイバインターフェイスモジュール
40
SLC制御PLD
SLC論理PLD
46
32x8 EPROM
26
8x8 RAM
28
8(AD0−AD7)の制御信号
16(AD0−AD15)の制御信号
12
24の5V基準値用分割VDC
14
5V基準値最大／最小電圧検出回路
アナログ入力&平均回路
38
FRAM不揮発性RAM
8XC196KDマイクロコントローラ
P0-P7
3
Self Test Status
Reset
1. 12秒WDT
58
リセット
セルフテストステータス
前面パネル押しボタンとキーロック位置
前面パネルLED
30
光ファイバインターフェイスモジュール
SLC論理カード
10

【図４】

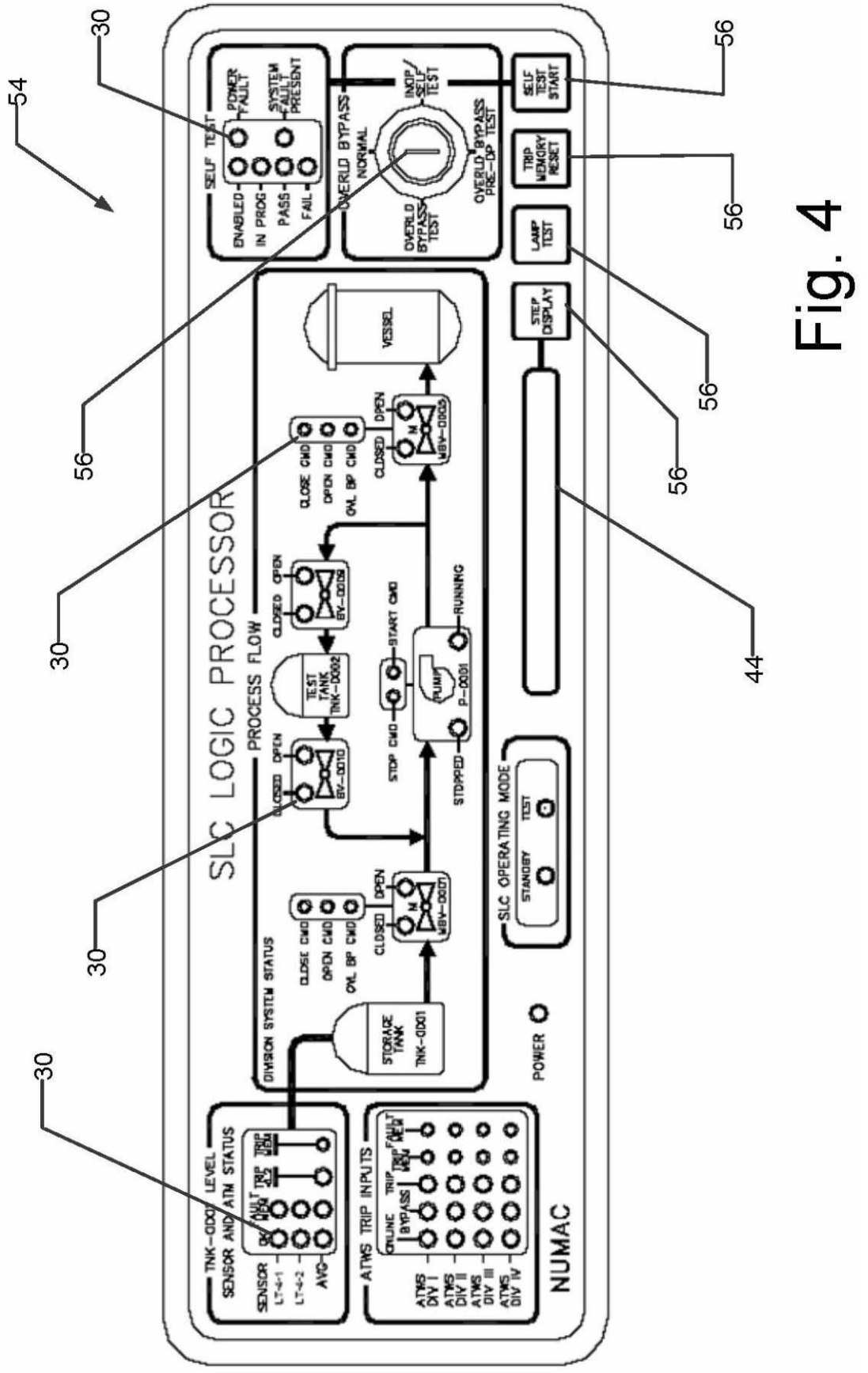
54
30
56
SELF TEST
ENABLED
IN PROG
PASS
FAIL
POWER FAULT
SYSTEM FAULT PRESENT
OVERLD BYPASS
NORMAL
OVERLD BYPASS TEST
OVERLD BYPASS PRE-DP TEST
INOP/ SELF TEST
SELF TEST START
TRIP MEMORY RESET
LAMP TEST
STEP DISPLAY
SLC LOGIC PROCESSOR
PROCESS FLOW
VESSEL
CLOSE CMD
OPEN CMD
OVL BP CMD
CLOSED
OPEN
MBV-0005
BV-0010
TEST TANK TNK-0002
START CMD
STOP CMD
PUMP
P-0001
RUNNING
STOPPED
MBV-0001
STORAGE TANK TNK-0001
DIVISION SYSTEM STATUS
SLC OPERATING MODE
STANDBY
TEST
POWER
TNK-0001 LEVEL
SENSOR AND ATM STATUS
SENSOR
LT-1
LT-2
AVG
ATWS TRIP INPUTS
ONLINE BYPASS
TRIP
FAULT
ATWS DIV I
ATWS DIV II
ATWS DIV III
ATWS DIV IV
NUMAC
44

Fig. 4

【図５】

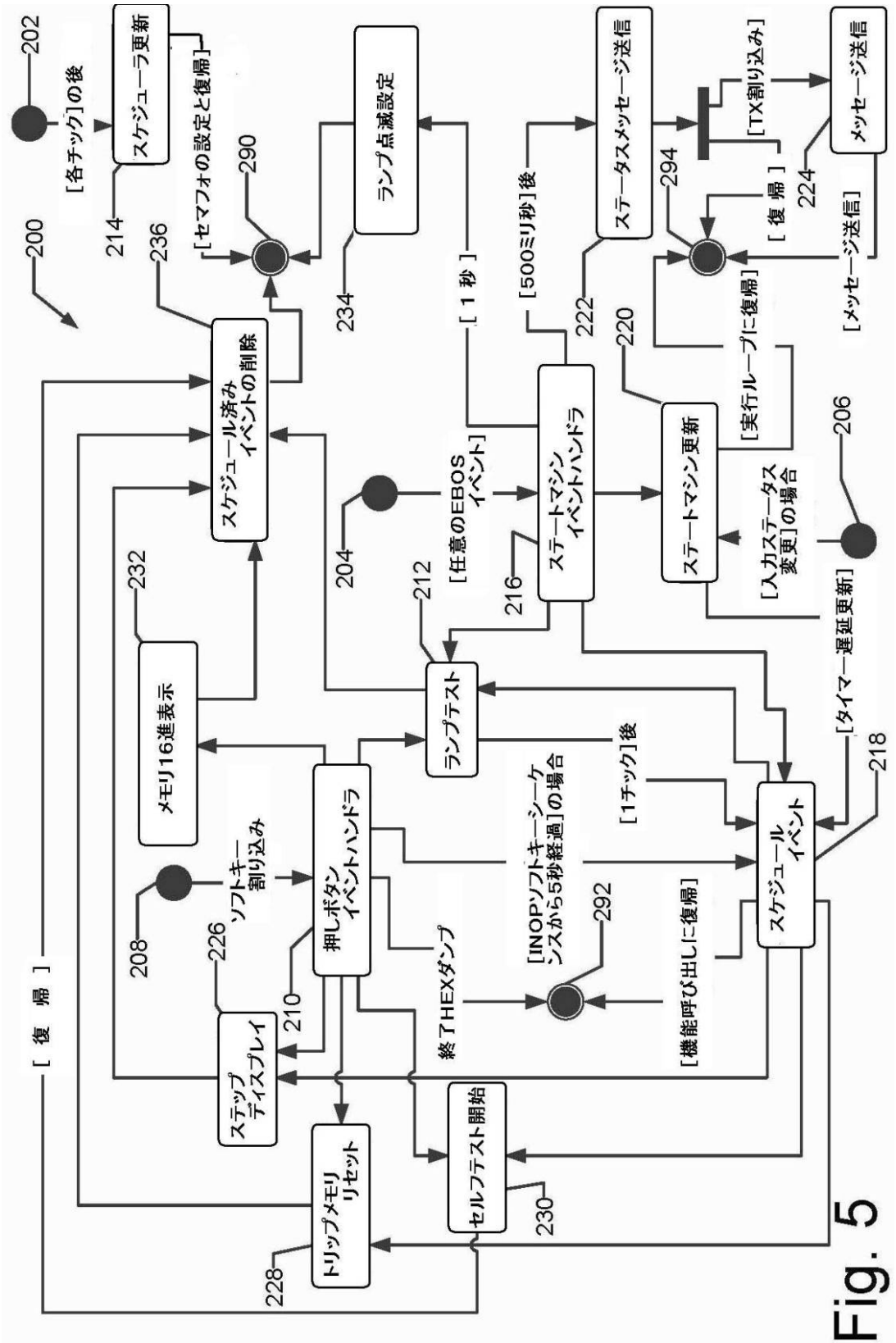
200
202
[各チック]の後
スケジューラ更新
214
236
[セマフォの設定と復帰]
290
ランプ点滅設定
234
[１秒]
[500ミリ秒]後
ステータスメッセージ送信
222
294
[TX割り込み]
メッセージ送信
224
[復帰]
[メッセージ送信]
スケジュール済みイベントの削除
232
204
[任意のEBOSイベント]
ステートマシンイベントハンドラ
220
ステートマシン更新
[実行ループに復帰]
206
[入力ステータス変更]の場合
[タイマー遅延更新]
メモリ16進表示
ランプテスト
212
216
[1チック]後
218
ソフトキー割り込み
208
226
押しボタンイベントハンドラ
[INOPソフトキーシーケンスから5秒経過]の場合
292
スケジュールイベント
終了HEXダンプ
[機能呼び出しに復帰]
210
ステップディスプレイ
トリップメモリリセット
セルフテスト開始
230
228
[復帰]

Fig. 5

【図６】

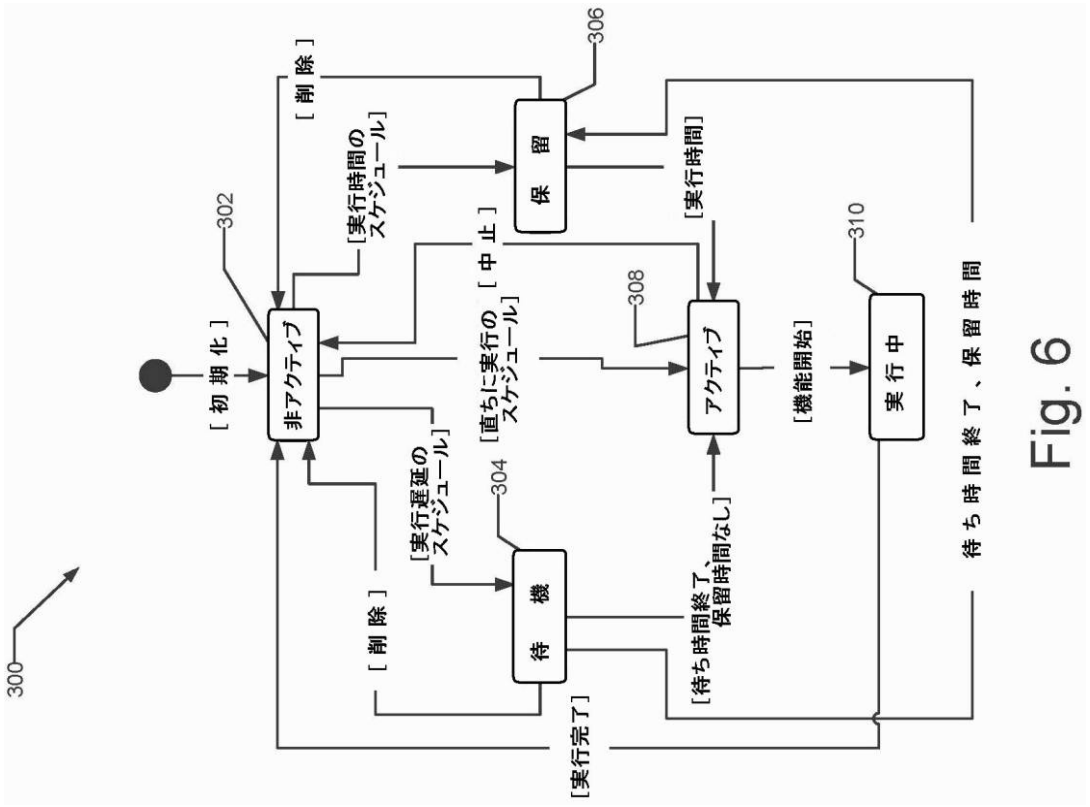
300
302
304
306
308
310
[初期化]
非アクティブ
[削除]
[実行時間のスケジュール]
保留
[中止]
[直ちに実行のスケジュール]
[実行遅延のスケジュール]
[削除]
待機
[実行時間]
アクティブ
[機能開始]
実行中
[待ち時間終了、保留時間なし]
[実行完了]
待ち時間終了、保留時間

Fig. 6

【図７】

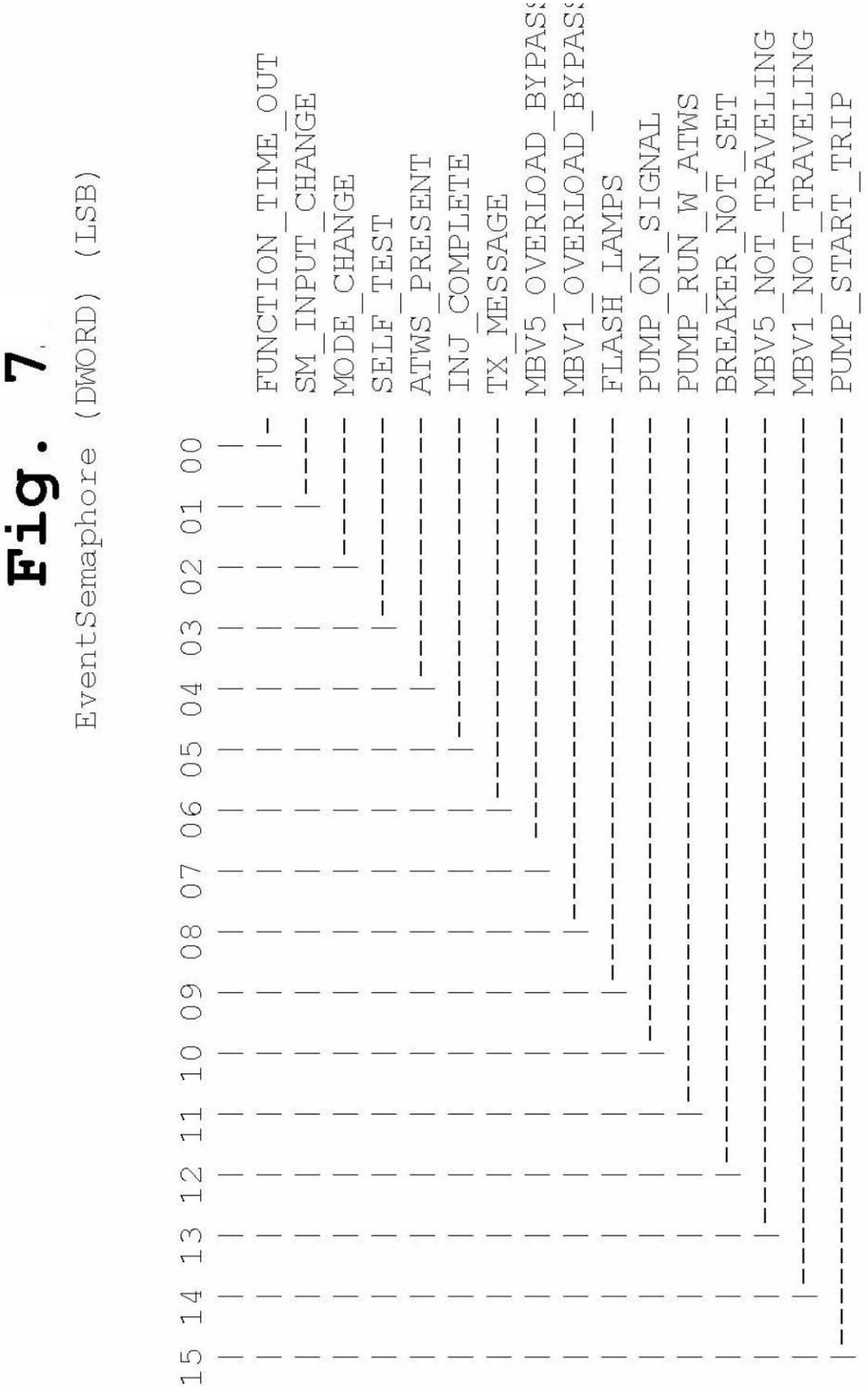
Fig. 7
EventSemaphore (DWORD) (LSB)
15 14 13 12 11 10 09 08 07 06 05 04 03 02 01 00
FUNCTION_TIME_OUT
SM_INPUT_CHANGE
MODE_CHANGE
SELF_TEST
ATWS_PRESENT
INJ_COMPLETE
TX_MESSAGE
MBV5_OVERLOAD_BYPAS
MBV1_OVERLOAD_BYPAS
FLASH_LAMPS
PUMP_ON_SIGNAL
PUMP_RUN_W_ATWS
BREAKER_NOT_SET
MBV5_NOT_TRAVELING
MBV1_NOT_TRAVELING
PUMP_START_TRIP

【図８】

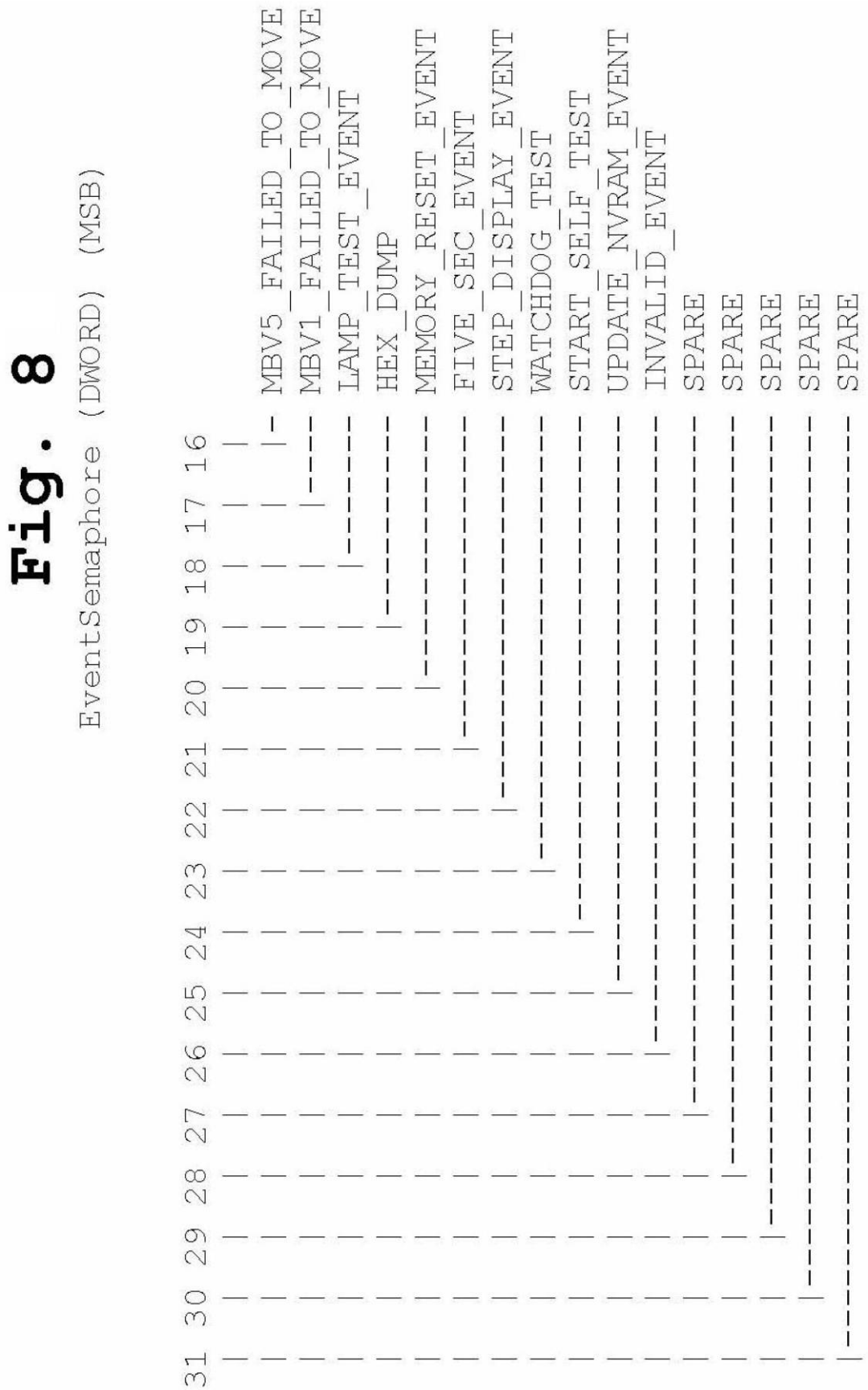
Fig. 8
EventSemaphore (DWORD) (MSB)
31 30 29 28 27 26 25 24 23 22 21 20 19 18 17 16
MBV5_FAILED_TO_MOVE
MBV1_FAILED_TO_MOVE
LAMP_TEST_EVENT
HEX_DUMP
MEMORY_RESET_EVENT
FIVE_SEC_EVENT
STEP_DISPLAY_EVENT
WATCHDOG_TEST
START_SELF_TEST
UPDATE_NVRAM_EVENT
INVALID_EVENT
SPARE
SPARE
SPARE
SPARE
SPARE
SPARE

【図９】

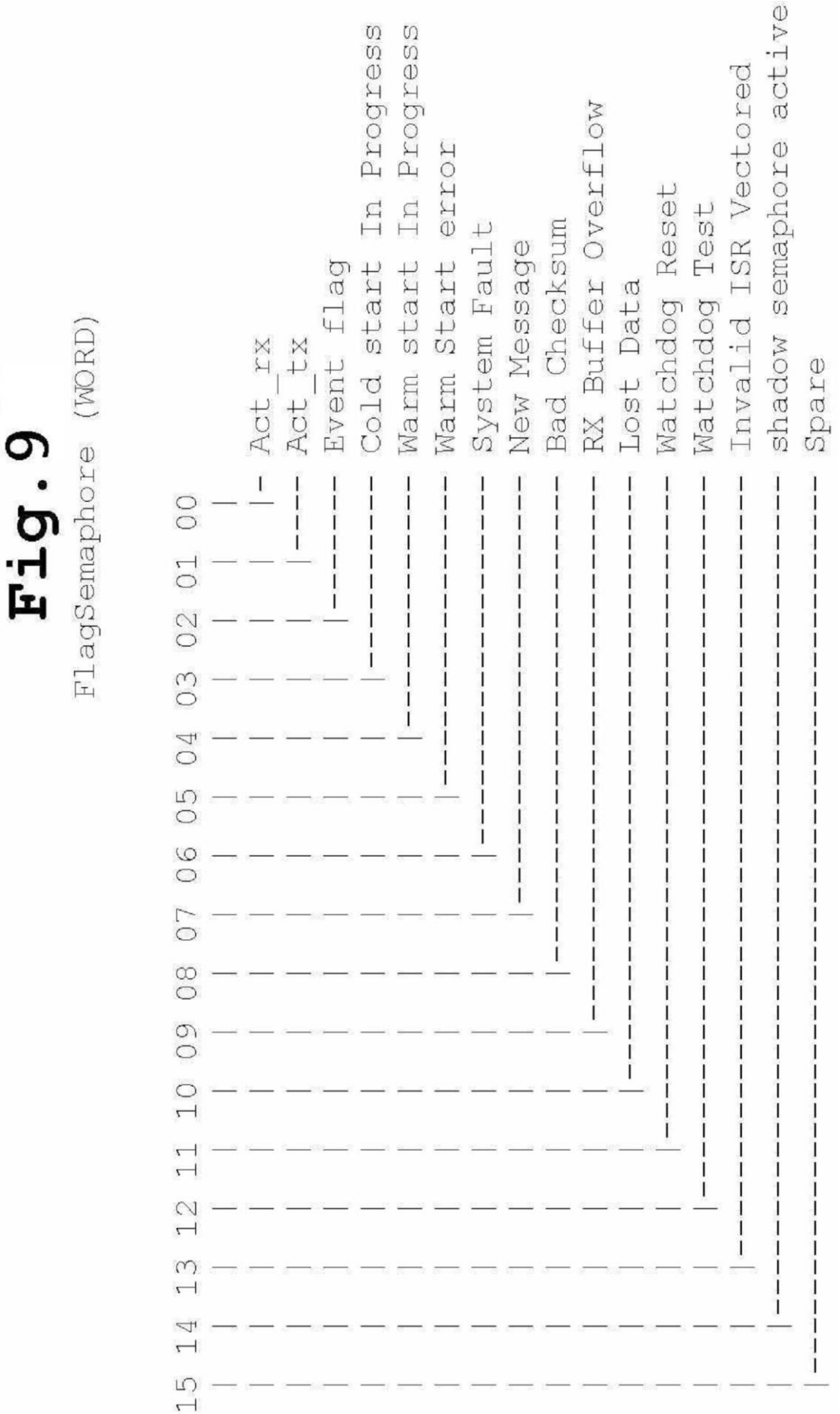
Fig.9
FlagSemaphore (WORD)
15 14 13 12 11 10 09 08 07 06 05 04 03 02 01 00
Act_rx
Act_tx
Event flag
Cold start In Progress
Warm start In Progress
Warm Start error
System Fault
New Message
Bad Checksum
RX Buffer Overflow
Lost Data
Watchdog Reset
Watchdog Test
Invalid ISR Vectored
shadow semaphore active
Spare

フロントページの続き

審査官　井上　宏一

(56)参考文献　特開２０００－２５９４２９（ＪＰ，Ａ）
特開２０００－１４８５１３（ＪＰ，Ａ）
特開平０２－１５６３３６（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　　９／４６　－９／５４