

(19) 日本国特許庁(JP)

(12) 公表特許公報(A)

(11) 特許出願公表番号

特表2007-507016

(P2007-507016A)

(43) 公表日 平成19年3月22日(2007.3.22)

(51) Int. Cl.

G06F 11/00 (2006.01)

F I

G06F 9/06 630A

テーマコード (参考)

5B176

審査請求 有 予備審査請求 未請求 (全 22 頁)

(21) 出願番号 特願2006-515278 (P2006-515278)
 (86) (22) 出願日 平成16年6月24日 (2004.6.24)
 (85) 翻訳文提出日 平成17年12月22日 (2005.12.22)
 (86) 国際出願番号 PCT/DE2004/001326
 (87) 国際公開番号 W02005/004160
 (87) 国際公開日 平成17年1月13日 (2005.1.13)
 (31) 優先権主張番号 10328241.6
 (32) 優先日 平成15年6月24日 (2003.6.24)
 (33) 優先権主張国 ドイツ (DE)

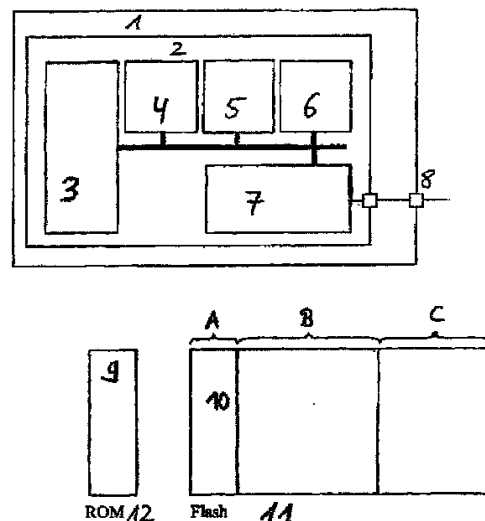
(71) 出願人 501125231
 ローベルト ボッシュ ゲゼルシャフト
 ミット ベシュレンクテル ハフツング
 ドイツ連邦共和国 70442 シュトゥ
 ットガルト ポストファッハ 30 02
 20
 (74) 代理人 100095957
 弁理士 亀谷 美明
 (74) 代理人 100096389
 弁理士 金本 哲男
 (74) 代理人 100101557
 弁理士 萩原 康司
 (72) 発明者 ツラウカ, トーマス
 ドイツ連邦共和国 70376 シュトゥ
 ットガルト エルベシュトラーセ 45
 最終頁に続く

(54) 【発明の名称】 シリアルインターフェイスを介したフラッシュプログラミングによる電子制御装置のソフトウェアアップデート方法およびこれに対応する状態自動装置

(57) 【要約】

本発明は、シリアルインターフェイスを介して制御装置の複数のセグメントを有するフラッシュメモリをフラッシュプログラミングすることによって、制御装置のソフトウェアアップデートを実施する方法に関するものである。この場合、フラッシュプログラムに課すべき要請が決定され、ソフトウェアの状態と移行を定義する状態自動装置によってフラッシュプログラミングのシーケンスが具現化されて、状態自動装置の各状態と各移行の可用性要請、安全性要請および信頼性要請が検査される。さらに、本発明は、対応する状態自動装置と可用性要請、安全性要請および信頼性要請を自動的に検査するためのコンピュータプログラムに関する。

【選択図】 図1



【特許請求の範囲】**【請求項 1】**

シリアルのインターフェイスを介して制御装置の複数のセグメントを有するフラッシュメモリをフラッシュプログラミングする、制御装置のソフトウェアアップデート方法であって、少なくとも次のステップ、

a) 前記フラッシュプログラミングに課すべき要請を決定し；

b) ソフトウェアの状態と移行を定義する状態自動装置によって前記フラッシュプログラミングのシーケンスを決定し；

c) 前記状態自動装置の各状態および各移行の可用性要請、安全性要請および信頼性要請を検査する；

を含むことを特徴とする、制御装置のソフトウェアアップデート方法。

10

【請求項 2】

前記制御装置の前記ソフトウェアのため、

特に「初期状態」、「正規状態」および「ソフトウェアアップデート」からなる種々の駆動状態と、前記駆動状態間の移行と、移行条件と、
について特定されることを特徴とする、請求項 1 に記載の制御装置のソフトウェアアップデート方法。

【請求項 3】

前記制御装置の前記ソフトウェアの、前記フラッシュプログラミングのために重要なメモリブロックは、プログラミング可能な前記メモリブロックとプログラミング不可能な前記メモリブロックに分割され、

これに応じて、新たにプログラミングする前記ソフトウェアのコンポーネントが、前記メモリブロックに対応づけられることを特徴とする、請求項 1 または 2 に記載の制御装置のソフトウェアアップデート方法。

20

【請求項 4】

前記ソフトウェアの前記メモリブロックは、それぞれ前記制御装置のメモリに対応づけられ、

特にプログラミング可能な前記メモリブロックは、前記フラッシュメモリの少なくとも 1 つのセグメントに対応づけられ、あるいは、プログラム不可能な前記メモリブロックは、前記制御装置の ROM に対応づけられることを特徴とする、請求項 3 に記載の制御装置のソフトウェアアップデート方法。

30

【請求項 5】

前記制御装置の前記フラッシュメモリの前記セグメント内には、前記フラッシュプログラミングを実施するために必要なソフトウェア機能を準備するブートブロック、プログラム状態およびデータ状態が格納され、

前記制御装置の前記 ROM 内には、前記フラッシュプログラミングを実施するために必要なソフトウェア機能を準備するスタートアップブロックが格納されることを特徴とする、請求項 1 ~ 4 のいずれかに記載の制御装置のソフトウェアアップデート方法。

【請求項 6】

前記フラッシュプログラミングの安全要請、信頼性要請および可用性要請が特定されることを特徴とする、請求項 1 ~ 5 のいずれかに記載の制御装置のソフトウェアアップデート方法。

40

【請求項 7】

前記状態自動装置によってフラッシュプログラミングを実施する場合に、「ソフトウェアアップデート」の駆動状態において、とることの可能なサブ状態、前記サブ状態間の移行および移行条件が特定されることを特徴とする、請求項 2 ~ 6 のいずれかに記載の制御装置のソフトウェアアップデート方法。

【請求項 8】

制御装置のソフトウェアアップデートをフラッシュプログラミングによって実施するための状態自動装置であって：

50

前記ソフトウェアアップデートを実施する際に取り得ることの可能な、前記制御装置のソフトウェアにおけるすべてのサブ状態と、前記サブ状態間の移行と、移行条件とが定義され、

前記ソフトウェアアップデートの実施の間に障害が発生した場合に、前記障害が発生する前に最後に有効であった状態、あるいはエラーのない状態における情報を、永続的に失われることのないように格納することを特徴とする、状態自動装置。

【請求項 9】

前記サブ状態は、「中断/エラー報告」状態と、「終了/成功報告」状態とからなり、認証およびシグニチャテストのためのサブ状態と、フラッシュメモリのセグメントの消去およびプログラミングのためのサブ状態とについて具現化されていることを特徴とする、請求項 8 に記載の状態自動装置。 10

【請求項 10】

プログラムコードエレメントからなるコンピュータプログラムであって、前記コンピュータプログラムによって、前記プログラムコードエレメントがコンピュータ上またはコンピュータシステム上で実施される場合に、自動的に、請求項 8 または 9 に記載の状態自動装置の各状態と各移行の予め定められた可用性要請、安全要請および信頼性要請がテストされることを特徴とする、コンピュータプログラム。

【請求項 11】

フラッシュプログラミングを実施するために必要なソフトウェア機能を準備する、フラッシュメモリの第 1 のセグメント（フラッシュセグメント A）に格納されているブートブロックのフラッシュプログラミング方法であって、 20

少なくとも以下のステップ、

a) 新しくプログラミングする古いブートブロックを、第 2 のメモリ（RAM）の空領域へコピーし；

b) 前記第 2 のメモリ（RAM）内の前記古いブートブロックをアクティブにし、かつ前記フラッシュメモリ内の前記古いブートブロックを非アクティブにし；

c) 新しいブートブロックを、前記フラッシュメモリの第 2 のセグメント（フラッシュセグメント C）内に一時的に格納し；

d) 前記第 2 のセグメント（フラッシュセグメント C）を前記第 1 のセグメント（フラッシュセグメント A）へコピーすることにより、前記新しいブートブロックをプログラミングし； 30

e) 前記第 1 のセグメント（フラッシュセグメント A）内の前記新しいブートブロックをアクティブにして、前記第 2 のメモリ（RAM）内の前記古いブートブロックを非アクティブにする、

を含むことを特徴とする、ブートブロックのフラッシュプログラミング方法。

【請求項 12】

ブートブロックは、前記フラッシュメモリ内において、前記フラッシュプログラミングの新規スタートのために有効なブートブロックとして常にマーキングされることを特徴とする、請求項 11 に記載のブートブロックのフラッシュプログラミング方法。 40

【発明の詳細な説明】

【技術分野】

【0001】

本発明は、シリアルインターフェイスを介してフラッシュプログラミングにより電子制御装置のソフトウェアアップデートを実施する方法に関する。

【背景技術】

【0002】

電子制御装置において、プログラム状態およびデータ状態のためのメモリ技術としていわゆるフラッシュを使用することが増加している。このメモリ技術は、シリアルインターフェイスを介して制御装置の該当するフラッシュメモリに新規プログラミングすることに 50

よって制御装置のソフトウェアアップデートを可能にする。この場合、シリアルインターフェイスは、例えば車両の中央のオフボード診断インターフェイスであり、これを介していわゆるフラッシュプログラミングツールによって、車両の電子制御装置のフラッシュメモリに新しくプログラミングされる。したがって、該当する電子制御装置を車両から取り外すことなくソフトウェアアップデートが可能であるので、制御装置を交換または取り外す場合と比較して著しいコスト削減をもたらす。上述した種類のフラッシュプログラミングの場合、特に車両のサービス、かつ安全上重要な電子制御装置の領域において、高い安全性および信頼性の要請を満たされなければならない。

【 0 0 0 3 】

現在使用されているフラッシュテクノロジーによれば、フラッシュメモリのフラッシュ領域全体を消去し、あるいは新しくプログラミングすることだけができる。ここで、フラッシュメモリの、物理的に関連し合う、閉成された消去またはプログラミング可能な最小のメモリユニットは、セグメントと称される。したがって、フラッシュプログラミングにおいては、フラッシュセグメントの消去とプログラミングのステップが区別される。このとき、さらに、同じフラッシュモジュールの他のセグメントが新たにプログラミングされる間に、同時にフラッシュセグメントからプログラムを実施することはできないことに注意しなければならない。したがって、フラッシュモジュールのためのプログラミングシーケンスを制御するためのプログラム部分は、フラッシュプログラミングを実施する間少なくとも一時的に、他のメモリモジュール、または他のフラッシュモジュールあるいは制御装置の R A M (R a n d o m A c c e s s M e m o r y) の空き領域に待避させなければならない。

【 0 0 0 4 】

オフボード診断インターフェイスの伝送パワーは制限されているため、電子制御装置のフラッシュメモリが大きい場合には、フラッシュプログラミング時間が非常に長くなる。したがって、製造およびサービスの分野において、フラッシュプログラミング時間を短縮する要請がしばしば生じる。

【 0 0 0 5 】

さらに、フラッシュプログラミングにおいて、責任の理由から常に、許可されていないフラッシュプログラミングまたは操作されたプログラム状態またはデータ状態によるフラッシュプログラミングができる限り阻止されるように、注意しなければならない。結局、いわゆるオフボード診断インターフェイスを介してのフラッシュプログラミングは、常に比較的長いタイムスパンを要求できることに、注意が必要である。この場合、場合によって発生する障害によるプログラミングシーケンスの中断が、常に考慮される。この種の障害としては、例えば車両またはフラッシュプログラミングツールの電圧供給障害、ネットワーク内の他の制御装置による許容されない反応、プログラミングを要する電子制御装置とそのために使用されるフラッシュプログラミングツールとの間の通信接続の中断あるいは操作エラー等がある。また、誤ってなされた認証およびシグニチャテストも、フラッシュプログラミングの中断をもたらすことがある。したがって、常にフラッシュプログラミングの可用性または即座に新規スタートができる保証が必要である。

【 発明の開示 】

【 発明の効果 】

【 0 0 0 6 】

本発明に基づく請求項 1 に記載の方法と請求項 8 に記載の状態自動装置が効果的である。また、他の利点および好適な実施形態については、従属請求項に記載されている。

【 0 0 0 7 】

請求項 1 によれば、シリアルインターフェイスを介して制御装置の複数のセグメントを有するフラッシュメモリをフラッシュプログラミングすることによって、制御装置のソフトウェアアップデートを実施する方法が提供される。かかる方法の第 1 のステップにおいて、フラッシュプログラミングに課すべき要請が決定されるので、フラッシュプログラミングのシーケンスが、制御装置のソフトウェアの状態と移行を定義する状態自動装置によ

って特定される。最終的に、状態自動装置の各状態と各移行の可用性、安全性および信頼性の要請が検査される。

【 0 0 0 8 】

好ましくは、フラッシュプログラミングに課すべき要請を定める場合に、まず、制御装置のソフトウェアが種々の駆動状態に特定される。このとき、種々の駆動状態は、好ましくは、「初期状態」、「正規状態」および「ソフトウェアアップデート」の状態に区別される。さらに、上述した駆動状態間の移行と移行条件が定義される。本方法の他の好ましい実施形態においては、制御装置のソフトウェアの、フラッシュプログラミングのために重要なメモリブロックが、プログラミング可能なメモリブロックとプログラミング不可能なメモリブロックに分割されて、それに応じてソフトウェアの新しくプログラミングすべきコンポーネントが制御ブロックに対応づけられる。さらに好ましくは、ソフトウェアのメモリブロックがそれぞれ制御装置のメモリに、特にプログラミング可能なメモリブロックがフラッシュメモリのセグメントに、またはプログラミング不可能なメモリブロックが電子制御装置のROM (Read - Only - Memory) に対応づけられる。オフボード診断インターフェイスの伝送パワーが制限されているため、フラッシュメモリが大きい場合には、極めて長いフラッシュプログラミング時間をもたらされる。

10

【 0 0 0 9 】

したがって、フラッシュプログラミング時間を短縮することが望ましく、例えば、新しくプログラミングが必要なフラッシュセグメントを減少させることによって可能である。これは、好ましくは、個々のソフトウェア機能のフラッシュプログラミングによって、あるいは電子制御装置のプログラム状態とデータ状態について別々にフラッシュプログラミングすることによって達成される。この場合、しばしば、プログラム状態は制御装置製造時にすでにプログラミングされ、データ状態は後に、例えば車両の製造の最後にそれぞれの車両固有にプログラミングされる。これに基づいて、本発明に基づく方法の他の好ましい実施形態においては、それぞれ制御装置のフラッシュメモリのセグメント内に、いわゆるブートブロック、プログラム状態およびデータ状態が格納される。これは、種々のソフトウェア機能およびプログラム状態とデータ状態が異なるフラッシュセグメントに格納されることを意味している。

20

【 0 0 1 0 】

この場合、フラッシュプログラミングの間にオフボード診断インターフェイスを介して制御装置とフラッシュプログラミングツールとの間で通信するために必要な、制御装置のすべてのプログラム部分は、対応するフラッシュプログラミングルーチン、いわゆるフラッシュローダーと共に、電子制御装置のROM内あるいは他のフラッシュセグメント内に格納されなければならない。制御装置とフラッシュプログラミングツールの間の通信に必要なプログラム部分は、プログラミング可能な部分とプログラミング不可能な部分に分割される。すなわち、以下でスタートアップブロックと称される、ROM内に格納されるベース範囲と、以下でブートブロックと称される、フラッシュに格納されるベース範囲とに分割される。スタートアップブロックとブートブロックは、共に、オフボード診断インターフェイスを介してフラッシュプログラミングするために必要な制御装置のマイクロコントローラのソフトウェア機能を提供する。

30

40

【 0 0 1 1 】

スタートアップブロックとブートブロックに分割することは、種々の理由から重要である。すなわち、ブートブロック自体が上述したようにフラッシュメモリに格納される場合に、新しくプログラミングすることができる。さらに、ブートブロック内に、フラッシュプログラミングの実際のステータスが失われないように格納されるので、例えばフラッシュプログラミングが中断された後に、再セットアップが可能である。これに対して、セットアップブロックの変更できないベース機能と、電子制御装置のハードウェアバリエーションのための識別子は、制御装置に設けられた、安価で新しくプログラミングすることのできないROMに格納することができる。本発明によれば、さらに、プログラム状態とデータ状態がそれぞれフラッシュメモリの他のセグメントに格納される。

50

【 0 0 1 2 】

本発明に基づく方法の他の好ましい実施形態においては、フラッシュプログラミングの安全性、信頼性および可用性についての要請が具現化される。制御装置のマイクロコントローラの駆動状態が「ソフトウェアアップデート」へ移行することは、フラッシュメモリツールによって促される。例えば、エンジン制御装置の場合に、走行プログラムの終了と「ソフトウェアアップデート」の駆動状態への移行の前に実施されなければならないエンジン停止状態チェック等、場合によっては必要な蓋然性チェックの他に、製造およびサービスに使用する場合には、他の安全措置が必要である。したがって、例えば責任の理由から、許可されていないフラッシュプログラミングまたは操作されたプログラム状態あるいはデータ状態によるフラッシュプログラミングをできる限り阻止することが必要である。少なくとも上述したようなフラッシュプログラミングを認識し、かつ立証できなければならない。

【 0 0 1 3 】

したがって、フラッシュプログラミングアクセスは、通常2つの異なる暗号化方法を行うことにより、安全性が確保される。第1の暗号化方法は認証であって、本来のアクセス権限の検査に相当し、蓋然性チェックの後に実施される。この場合、デジタルキーを用いて、フラッシュプログラミングツールのユーザが、そもそもソフトウェアアップデートを実施する権限を有しているか否かについてチェックされる。第2の暗号化方法は、いわゆるシグニチャチェックである。この場合、新しくプログラミングするプログラム状態またはデータ状態のデータ一貫性についてチェックされる。

【 0 0 1 4 】

シグニチャチェックでは、フラッシュプログラミングツールによって他のデジタルキーを用いて、新たにプログラミングするプログラム状態またはデータ状態が制御装置ハードウェアに適しているか、そして新たにプログラミングするプログラム状態またはデータ状態が、例えば車両メーカーによりサービス機構へ引き渡された後に、許容できない操作をされていないかについてチェックする。上述した検査が成功して終了した後に初めて、フラッシュメモリの該当するセグメントの消去とプログラミングが許可される。このプログラミングの許可は、上述したブートブロックによって行われる。

【 0 0 1 5 】

フラッシュプログラミングの安全性および信頼性要求を具現化する場合に、フラッシュプログラミングの後に、プログラミングの間のエラーを認識することができるようにするために、実際にフラッシュメモリへプログラミングされたプログラム状態とデータ状態に基づく制御装置のマイクロコントローラのシグニチャが考慮されることにも、注意しなければならない。シグニチャチェックが成功した後、考慮されたシグニチャ自体はフラッシュメモリに格納される。このために特別なメモリ構造、いわゆるプログラム状態ロジスティックとデータ状態ロジスティックがプログラム状態およびデータ状態の一部としてフラッシュメモリに格納される。シグニチャチェックが成功した後のみ、ブートブロックは、例えば走行プログラムのような、新しいプログラムの活性化を許可する。

【 0 0 1 6 】

さらに、本発明に基づく方法において、好ましくはフラッシュプログラミングの可用性要請も具現化される。オフボード診断インターフェイスを介してのフラッシュプログラミングは、上述した最適化措置にもかかわらず比較的長いタイムスパンを要求することが可能であるため、一般に、障害によるプログラムシーケンスの中断について常に考慮されなければならない。このような障害としては、例えば車両またはフラッシュプログラミングツールの電圧供給障害、ネットワーク内の他の障害装置による許容できない反応、電子制御装置と電子制御装置に使用されるフラッシュプログラミングツールとの間の通信接続の中断または操作エラー等がある。誤ってなされた認証やシグニチャチェックも、通常、フラッシュプログラミングを中断させる要因となる。したがって、フラッシュプログラミングのシーケンス設計においては、考えられるすべての状況の下でフラッシュプログラミングの可用性を保証することが重要である。

【 0 0 1 7 】

例えば、すべての状況において中断した後に、いつでもプログラムシーケンスが新規にスタートさせることができることについて保証されていることを意味している。このため、本発明に基づく方法の他の好ましい実施形態においては、状態自動装置によってフラッシュプログラムを実施する場合に、「ソフトウェアアップデート」の駆動状態においてとることの可能なサブ状態、サブ状態間の移行および移行条件が具現化される。このとき、サブ状態としては、サブ状態「中断/エラー報告」または「終了/成功報告」等がある。さらに好ましくは、認証およびシグニチャチェックのためのサブ状態およびフラッシュメモリのセグメントの消去とプログラミングのためのサブ状態も具現化することができる。さらに、ブートブロックの待避とフラッシュプログラミングのためのサブ状態の具現化も行うことが望ましい。上述したサブ状態間の移行とこれに対応する移行条件の具現化は、本発明において同様に行われる。

【 0 0 1 8 】

さらに、本発明は、プログラムコードエレメントからなるコンピュータプログラムを含んでいる。このコンピュータプログラムによってコンピュータ上またはコンピュータシステム上でプログラムコードエレメントを実施する場合、自動的に、上述した状態自動装置の各状態および各移行の予め定義された可用性、安全性および信頼性の要求について検査される。

【 0 0 1 9 】

そして、本発明は、上述したブートブロックをフラッシュプログラミングする方法に関する。例えば、フラッシュプログラミングを実施するために必要なソフトウェア機能性を準備する、ブートブロックのフラッシュプログラミングを実施する方法が提供される。この場合、ブートブロックは、フラッシュメモリの第1のセグメント内に格納されている。第1のステップにおいて、新しくプログラミングされる古いブートブロックが、空RAM領域へコピーされる。すなわち、まだアクティブな古いブートブロックをフラッシュプログラミングの間に制御装置の他のメモリモジュール内へ待避させなければならず、ブートブロックがリロケーション可能であることを意味している。

【 0 0 2 0 】

その後、第2のステップにおいて、RAM内の古いブートブロックが活性化されて、フラッシュメモリ（ここでブートブロックは第1のセグメント内に格納されている）内では非活性化される。さらに、新しいブートブロックがフラッシュメモリの第2のセグメントに一時的に格納される。このとき、かかるステップは、フラッシュメモリの第2のセグメントの消去、フラッシュメモリの第2のセグメントへの新しいブートブロックのプログラミング、およびフラッシュメモリの第2のセグメント内の新しいブートブロックのためのシグニチャチェックを含む。この処理ステップの間に処理が中断した場合には、その後、フラッシュメモリの第1のセグメント内における古い、有効なブートブロックによって、フラッシュプログラミングを新しく開始することができる。

【 0 0 2 1 】

本発明に基づく方法の他のステップにおいて、フラッシュメモリの第2のセグメントをフラッシュメモリの第1のセグメント内へコピーすることによって、最終的に新しいブートブロックがプログラミングされる。この場合、かかるステップは、第1のフラッシュセグメントの消去、第2のフラッシュセグメントを第1のフラッシュセグメントへコピーすることによる第1のフラッシュセグメントへの新しいブートブロックのプログラミング、および第1のフラッシュセグメント内の新しいブートブロックのためのシグニチャチェックを含む。この処理ステップの間に処理が中断した場合には、その後、第2のフラッシュセグメント内の新しい、有効なブートブロックによって、フラッシュプログラミングを新しく開始することができる。好ましくは、フラッシュメモリ内では常に、ブートブロックは、フラッシュプログラミングの新規スタートのために有効なブートブロックとしてマーキングされる。この場合にこの有効なマーキング自体が、フラッシュメモリ内に失われないうように格納されなければならず、かかる情報によって再セットアップすることが可能で

ある。

【 0 0 2 2 】

その後、本発明に基づく方法の最終ステップにおいて、フラッシュメモリの第1のセグメント内の新しいブートブロックが活性化されて、同時にRAM内の古いブートブロックが非活性化される。

【発明を実施するための最良の形態】

【 0 0 2 3 】

本発明の他の利点および好ましい実施形態を、図を用いて詳細に説明する。

【 0 0 2 4 】

図1には、フラッシュプログラミングによって制御装置のソフトウェアアップデートを実施するための制御装置における、ソフトウェアのメモリブロックの対応づけが示されている。図1に示すように、制御装置1は、マイクロコントローラ2を有する。マイクロコントローラ2は、マイクロプロセッサ3と3つの異なるメモリ、すなわちROM (Read - Only - Memory) 4、フラッシュメモリ5およびRAM (Random Access Memory) 6を有する。さらに、制御装置1は、オフボード診断インターフェイス8に結合するためのシリアルインターフェイス7を有しており、オフボード診断インターフェイスを介してフラッシュプログラミングツールを接続することができる。

【 0 0 2 5 】

図1の下部には、制御装置1のソフトウェアの、フラッシュプログラミングにとって重要なメモリブロックのメモリ割当てが示されている。メモリブロックは、プログラミング可能なメモリブロックとプログラミング不可能なメモリブロックとに分割されており、これに応じてソフトウェアの新たにプログラミングするコンポーネントが、メモリブロックに対応づけられている。マイクロコントローラ2のプログラム部分は、フラッシュプログラミングの間オフボード診断インターフェイス8を介してマイクロコントローラ2とフラッシュプログラミングツールの間で通信するために必要な、いわゆるスタートアップブロック9といわゆるブートブロック10に分割されている。スタートアップブロック9とブートブロック10は、一緒になって、オフボード診断インターフェイス8を介してのフラッシュプログラミングのために必要なマイクロコントローラ2のソフトウェア機能を提供する。

【 0 0 2 6 】

スタートアップブロック9とブートブロック10に分割することは、種々の理由から重要である。すなわち、図1の場合において、フラッシュメモリ11のセグメントAに格納されているブートブロック10自体は、新たにプログラミングすることができる。さらにブートブロック10は、フラッシュプログラミングの実際のステータスが失われないように格納されることができるので、例えば処理が中断した場合にも、その後再セットアップが可能である。これに対してスタートアップブロック9の、変更不可のベース機能は、コスト的に好ましい、新たにプログラミングできないROM 12に格納することができる。フラッシュメモリの他のセグメントについては、フラッシュセグメントBには、プログラム状態が格納され、フラッシュセグメントCにはデータ状態が格納されている。

【 0 0 2 7 】

図2には、フラッシュプログラミングを実施する場合の安全要請の仕様として、フラッシュプログラミングツール13と制御装置のマイクロコントローラ2との間の通信の可能なシーケンスが示されている。「ソフトウェアアップデート」の駆動状態へ移行する前に実施されなければならない、フラッシュプログラミングツール13の側からの送信とマイクロコントローラ2の返信とによって実施される蓋然性チェック14の後に、本来のアクセス権限に関するチェックが実施される。このアクセス権限に関するチェックのステップが、認証15である。この場合、デジタルキーを用いて、フラッシュプログラミングツール13のユーザがソフトウェアアップデートを行う権限を有しているか否かについて調べられる。

【 0 0 2 8 】

10

20

30

40

50

次いで、他の検査ステップ 16 において、新たにプログラミングするプログラム状態またはデータ状態のデータ一貫性について検査される。この検査ステップは、シグニチャテストとも称される。ここでは、フラッシュプログラミングツール 13 によって他のデジタルキーを用いて新たにプログラミングするプログラム状態またはデータ状態が制御装置ハードウェアに合っているか、そして新たにプログラミングするプログラム状態またはデータ状態がその引渡し元から許容されない操作をされていないか、について調べられる。この検査において成功して終了した後にはじめて、ステップ 17 においてフラッシュセグメントが消去され、次にステップ 18 において、対応するフラッシュセグメントがプログラミングされる。

【0029】

10

フラッシュプログラミングの後に、プログラミングの間のエラーを認識することができるようになるために、マイクロコントローラ 2 によって実際にフラッシュメモリ内にプログラミングされたプログラム状態とデータ状態に基づいてシグニチャが計算される。シグニチャテスト 19 が成功した後に、この計算されたシグニチャテスト自体がフラッシュメモリに格納される。このため、特別なメモリ構造、いわゆるプログラムおよびデータ状態ロジスティックがプログラムおよびデータ状態の一部として、フラッシュメモリに格納される。シグニチャテスト 19 が成功した後にだけ、ブートブロックは、例えば走行プログラムのような、新しいプログラムを活性化する。

【0030】

図 3 は、プログラム状態およびデータ状態をフラッシュプログラミングする場合のブートブロックの状態と移行を概略的に示している。まず、ステップ 20 において、オフボード診断インターフェイスを介してフラッシュプログラミングツールとマイクロコントローラとを結合する際に、制御装置が識別されて、マイクロコントローラの「ソフトウェアアップデート」の駆動状態への移行が開始される。このとき、ステップ 21 において、エラーが認識された場合には、すぐにプログラミングプロセスが中断され、同時にエラー報告 F が出力される。次いで、他のステップ 22 において、結合されているフラッシュプログラミングツールのユーザの認証が行われる。ここでも、ステップ 23 においてエラーが認識された場合には、処理が中断され、エラー報告 F が出力される。これに続いて、シグニチャテスト 24 が行われ、ハードウェア - / プログラム状態 - / データ状態ロジスティックについてのデータ一貫性のテストを行う。シグニチャテスト 24 においてエラー 25 認識された場合には、ここでも、処理が中断され、信号化されたエラー報告 F が出力される。

20

30

【0031】

このステップを実施した後に、プログラム状態が格納されているフラッシュセグメントの消去 26 が行われ、続いてステップ 27 において、新しいプログラム状態がプログラミングされて、新しいプログラム状態のためのシグニチャテスト 28 が実施される。ステップ 26、27、28 と同じステップが、ステップ 29、30、31 においてデータ状態のフラッシュプログラミングに関して行われる。プログラム状態またはデータ状態についてのシグニチャテストにおいて、エラーが認識された場合には、ここでも処理が中断され、エラー報告 F が出力される。これに対してエラーが認識されない場合には、ステップ 32 において、リセット処理により「初期状態」の駆動状態へのマイクロコントローラの移行が行われる。

40

【0032】

図 4 は、ブートブロックのフラッシュプログラミングにおける処理ステップを示している。まず、アクティブなブートブロック "A" をフラッシュプログラミングの間、マイクロコントローラの他のメモリモジュールへ待避させなければならない。このため、ブートブロック "A" は、リロケーション可能でなければならない。これは、例えば、ブートブロック "A" を、フラッシュプログラミングの間、空 RAM 領域へコピーすることによって行うことができる。

【0033】

50

次に、ブートブロック " A " を R A M から実施する。このとき、ブートブロックのフラッシュプログラミングが誤って行われた後でも、プログラムシーケンスを新規にスタートがさせることが可能でなければならない。処理が中断した場合、その後可用性を維持するためには、エラーのないブートブロックで十分である。処理の第 1 のステップにおいて、古いブートブロック " A " が、空 R A M 領域へコピーされる。第 2 のステップにおいては、R A M 内の古いブートブロックが活性化され（これがマーキング " A " によって見分けられるようにされている）、フラッシュメモリ内で非活性化される。新しいブートブロックが、フラッシュセグメント C 内にバッファされる。このとき、フラッシュセグメント C が消去されて、新しいブートブロックがフラッシュセグメント C 内へプログラミングされて、フラッシュセグメント C 内の新しいブートブロックについてシグニチャテストが実施される。この処理ステップの間に処理が中断した場合には、その後、フラッシュセグメント A 内の有効な古いブートブロックによってフラッシュプログラミングを新たに開始することができる。

10

【 0 0 3 4 】

第 3 のステップにおいて、新しいブートブロックがプログラミングされる。このプログラミングは、フラッシュセグメント C をフラッシュセグメント A へコピーした後に行われる。このステップは、フラッシュセグメント A の消去、フラッシュセグメント C を A へコピーすることによる、フラッシュセグメント A における新しいブートブロックのプログラミング、およびフラッシュセグメント A 内の新しいブートブロックのシグニチャテストを有する。この処理ステップの間に処理が中断した場合には、その後、フラッシュセグメント C 内の有効な新しいブートブロックによってフラッシュプログラミングを新たにスタートさせることができる。フラッシュメモリ内のそれぞれ有効なブートブロックは、マーキングされなければならない、この有効なマーキング自体が、失われないようにフラッシュメモリ内に格納される。このため、かかる情報によって再セットアップが可能である。

20

【図面の簡単な説明】

【 0 0 3 5 】

【図 1】本発明方法の実施形態に基づく、制御装置のフラッシュプログラミングのために重要なメモリブロックの仕様を概略的に示している。

【図 2】本発明方法の他の実施形態に基づく、安全要請および安全措置の仕様を概略的に示している。

30

【図 3】電子制御装置のプログラム状態およびデータ状態をフラッシュプログラミングする場合のブートブロックの状態と移行を概略的に示している。

【図 4】ブートブロックのフラッシュプログラミングを実施するための、本発明に基づく方法の実施形態のシーケンスを概略的に示している。

【 図 1 】

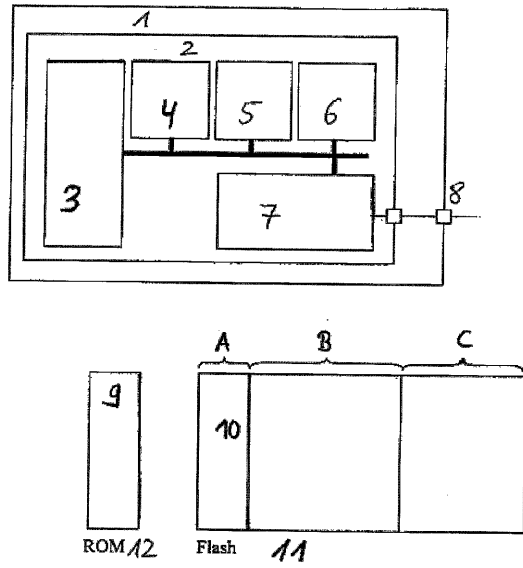


Figure 1

【 図 2 】

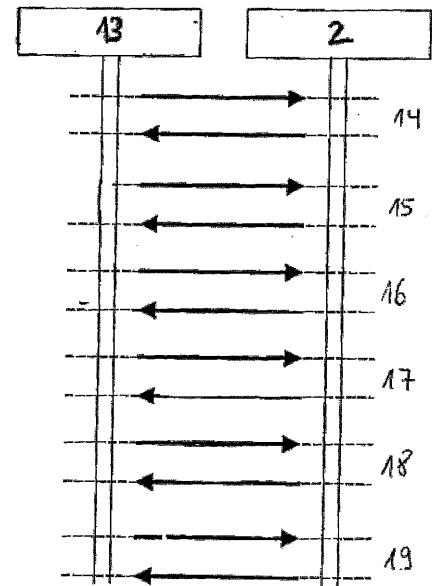


Figure 2

【 図 3 】

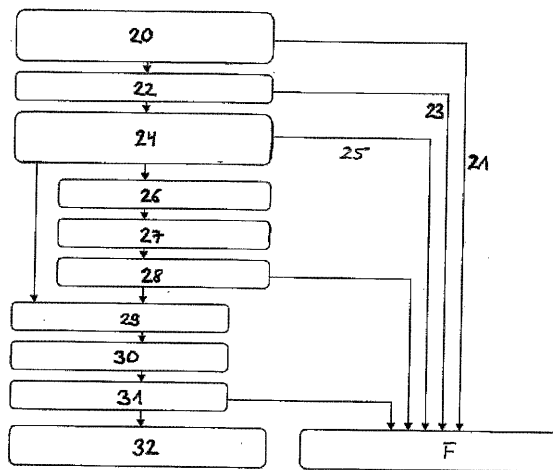


Figure 3

【 図 4 】

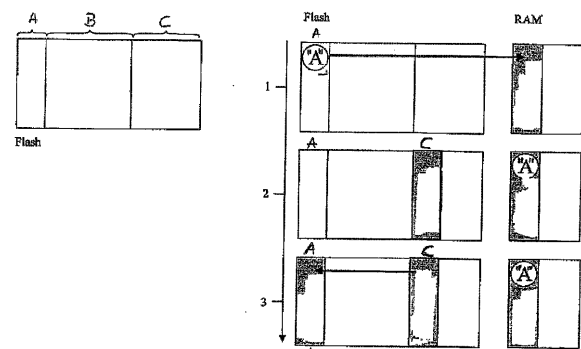


Figure 4

【国際調査報告】

60600550089 		INTERNATIONAL SEARCH REPORT		International Application No. PCT/DE2004/001326	
A. CLASSIFICATION OF SUBJECT MATTER G06F9/445					
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) G06F G11C					
Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched					
Electronic data base consulted during the international search (name of data base and, where practical, search terms used) EPO-Internal, WPI Data, PAJ, INSPEC, IBM-TDB					
C. DOCUMENTS CONSIDERED TO BE RELEVANT					
Category *	Citation of document, with indication, where appropriate, of the relevant passages				Relevant to claim No.
Y	US 2003/041182 A1 (MARTWICK ANDREW W) 27 February 2003 (2003-02-27) abstract paragraph [0014] - paragraph [0040]; figures 1-4				1-10
Y	ROLAND C. BACKHOUSE: "Program construction and verification" 1986, PRENTICE-HALL, INC., UPPER SADDLE RIVER, NJ, USA 6 902873, XP002332801 page 5, line 1 - page 11, line 39				1-10
A	EP 1 260 907 A (SIEMENS SCHWEIZ AG) 27 November 2002 (2002-11-27) abstract paragraph [0009] - paragraph [0024]; figure 1				1-10
----- -/--					
☒ Further documents are listed in the continuation of box C. ☒ Patent family members are listed in 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 document 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 "Z" document member of the same patent family					
Date of the actual completion of the international search 21 June 2005			Date of mailing of the international search report 23. 12. 2005		
Name and mailing address of the ISA European Patent Office, P.B. 5818 Patentaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 851 epo nl, Fax: (+31-70) 340-3016			Authorized officer Wierzejewski, P 01. 5. 2006		

Form PCT/ISA/210 (second sheet) (January 2004)

2

INTERNATIONAL SEARCH REPORT

International Application No.

PCT/DE2004/001326

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 5 701 492 A (WADSWORTH ET AL) 23 December 1997 (1997-12-23) abstract column 2, line 17 - column 3, line 56; figures 4-6b column 8, line 15 - column 9, line 53 claims 1-14	1-10
A	----- EP 1 120 709 A (NEC CORPORATION) 1 August 2001 (2001-08-01) abstract paragraph [0030] - paragraph [0047] paragraph [0066] - paragraph [0105] -----	1-10

2

INTERNATIONAL SEARCH REPORT

International application No.

PCT/DE2004/001326**Box I** Observations where certain claims were found unsearchable (Continuation of item 1 of first sheet)

This international search report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:
2. ☐ Claims Nos.:
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:
3. ☐ Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box II Observations where unity of invention is lacking (Continuation of item 2 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

SEE SUPPLEMENTAL SHEET

1. ☐ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.
2. ☐ As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.
3. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:
4. ☒ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

1-10

Remark on Protest☐

The additional search fees were accompanied by the applicant's protest.

☐

No protest accompanied the payment of additional search fees.

4

INTERNATIONAL SEARCH REPORT

International application No.
PCT/DE2004/001326

The International Searching Authority has found that the international application contains multiple (groups of) inventions, as follows:

1. Claims: 1-10

Method for updating software of an electronic control device by flash programming via a corresponding finite state machine.

2. Claims: 11-12

Method for updating software of an electronic control device by flash programming with intermediate storage of software.

5

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No

PCT/DE2004/001326

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2003041182 A1	27-02-2003	US 2004163081 A1	19-08-2004
EP 1260907 A	27-11-2002	NONE	
US 5701492 A	23-12-1997	NONE	
EP 1120709 A	01-08-2001	JP 2001209543 A	03-08-2001
		US 2002002652 A1	03-01-2002

6

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen

PCT/DE2004/001326

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES G06F9/445		
Nach der Internationalen Patentklassifikation (IPK) oder nach der nationalen Klassifikation und der IPK		
B. RECHERCHIERTE GEBIETE		
Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole) G06F G11C		
Recherchierte aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen		
Während der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe) EPO-Internal, WPI Data, PAJ, INSPEC, IBM-TDB		
C. ALS WESENTLICH ANGESEHENE UNTERLAGEN		
Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
Y	US 2003/041182 A1 (MARTWICK ANDREW W) 27. Februar 2003 (2003-02-27) Zusammenfassung Absatz [0014] - Absatz [0040]; Abbildungen 1-4	1-10
Y	ROLAND C. BACKHOUSE: "Program construction and verification" 1986, PRENTICE-HALL, INC., UPPER SADDLE RIVER, NJ, USA 6 902873, XP002332801 Seite 5, Zeile 1 - Seite 11, Zeile 39	1-10
A	EP 1 260 907 A (SIEMENS SCHWEIZ AG) 27. November 2002 (2002-11-27) Zusammenfassung Absatz [0009] - Absatz [0024]; Abbildung 1	1-10
-/-		
☒ Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen ☒ Siehe Anhang Patentfamilie		
* Besondere Kategorien von angegebenen Veröffentlichungen : "A" Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist "E" Älteres Dokument, das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist "L" Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt) "O" Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht "P" Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist "T" Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist "X" Veröffentlichung von besonderer Bedeutung: die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden "Y" Veröffentlichung von besonderer Bedeutung: die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren anderen Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist "Z" Veröffentlichung, die Mitglied derselben Patentfamilie ist		
Datum des Abschlusses der internationalen Recherche		Absenddatum des internationalen Recherchenberichts
21. Juni 2005		23. 12. 2005
Name und Postanschrift der Internationalen Recherchenbehörde Europäisches Patentamt, P.B. 5818 Patentaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3018		Bevollmächtigter Bediensteter Wierzejewski, P

Formblatt PCT/ISA210 (Blatt 2) (Januar 2004)

7

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen
PCT/DE2004/001326

C.(Fortsetzung) ALS WESENTLICH ANGESEHENE UNTERLAGEN		
Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
A	US 5 701 492 A (WADSWORTH ET AL) 23. Dezember 1997 (1997-12-23) Zusammenfassung Spalte 2, Zeile 17 - Spalte 3, Zeile 56; Abbildungen 4-6b Spalte 8, Zeile 15 - Spalte 9, Zeile 53 Ansprüche 1-14 -----	1-10
A	EP 1 120 709 A (NEC CORPORATION) 1. August 2001 (2001-08-01) Zusammenfassung Absatz [0030] - Absatz [0047] Absatz [0066] - Absatz [0105] -----	1-10

8

INTERNATIONALER RECHERCHENBERICHT

internationales Aktenzeichen
PCT/DE2004/001326

Feld II Bemerkungen zu den Ansprüchen, die sich als nicht recherchierbar erwiesen haben (Fortsetzung von Punkt 2 auf Blatt 1)

Gemäß Artikel 17(2)a) wurde aus folgenden Gründen für bestimmte Ansprüche kein Recherchenbericht erstellt:

1. ☐ Ansprüche Nr. _____
weil sie sich auf Gegenstände beziehen, zu deren Recherche die Behörde nicht verpflichtet ist, nämlich _____
2. ☐ Ansprüche Nr. _____
weil sie sich auf Teile der internationalen Anmeldung beziehen, die den vorgeschriebenen Anforderungen so wenig entsprechen, daß eine sinnvolle internationale Recherche nicht durchgeführt werden kann, nämlich _____
3. ☐ Ansprüche Nr. _____
weil es sich dabei um abhängige Ansprüche handelt, die nicht entsprechend Satz 2 und 3 der Regel 6.4 a) abgefaßt sind.

Feld III Bemerkungen bei mangelnder Einheitlichkeit der Erfindung (Fortsetzung von Punkt 3 auf Blatt 1)

Die internationale Recherchenbehörde hat festgestellt, daß diese internationale Anmeldung mehrere Erfindungen enthält:

siehe Zusatzblatt

1. ☐ Da der Anmelder alle erforderlichen zusätzlichen Recherchegebühren rechtzeitig entrichtet hat, erstreckt sich dieser internationale Recherchenbericht auf alle recherchierbaren Ansprüche.
2. ☐ Da für alle recherchierbaren Ansprüche die Recherche ohne einen Arbeitsaufwand durchgeführt werden konnte, der eine zusätzliche Recherchegebühr gerechtfertigt hätte, hat die Behörde nicht zur Zahlung einer solchen Gebühr aufgefordert.
3. ☐ Da der Anmelder nur einige der erforderlichen zusätzlichen Recherchegebühren rechtzeitig entrichtet hat, erstreckt sich dieser internationale Recherchenbericht nur auf die Ansprüche, für die Gebühren entrichtet worden sind, nämlich auf die Ansprüche Nr. _____
4. ☒ Der Anmelder hat die erforderlichen zusätzlichen Recherchegebühren nicht rechtzeitig entrichtet. Der internationale Recherchenbericht beschränkt sich daher auf die in den Ansprüchen zuerst erwähnte Erfindung; diese ist in folgenden Ansprüchen erfaßt:
1-10

Bemerkungen hinsichtlich eines Widerspruchs

- ☐ Die zusätzlichen Gebühren wurden vom Anmelder unter Widerspruch gezahlt.
- ☐ Die Zahlung zusätzlicher Recherchegebühren erfolgte ohne Widerspruch.

Internationales Aktenzeichen PCT/ DE2004/ 001326

WEITERE ANGABEN

PCT/ISA/ 210

Die internationale Recherchenbehörde hat festgestellt, dass diese internationale Anmeldung mehrere (Gruppen von) Erfindungen enthält, nämlich:

1. Ansprüche: 1-10

Verfahren zur Durchführung eines Software-Updates eines elektronischen Steuergerätes durch eine Flash-Programmierung über ein entsprechender Zustandsautomat

2. Ansprüche: 11-12

Verfahren zur Durchführung eines Software-Updates eines elektronischen Steuergerätes durch eine Flash-Programmierung mit Software Zwischenablegung

10,

INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Nationales Aktenzeichen

PCT/DE2004/001326

Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
US 2003041182 A1	27-02-2003	US 2004163081 A1	19-08-2004
EP 1260907 A	27-11-2002	KEINE	
US 5701492 A	23-12-1997	KEINE	
EP 1120709 A	01-08-2001	JP 2001209543 A	03-08-2001
		US 2002002652 A1	03-01-2002

フロントページの続き

(81)指定国 AP(BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), EA(AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), EP(AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OA(BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG), AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW

(72)発明者 ショイフェレ, イェルク

ドイツ連邦共和国 7 4 3 9 1 エルリッヒハイム シュメルバッハヴェーク 1 1

Fターム(参考) 5B176 EB01 EB03