(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第6571602号
(P6571602)
(45)発行日　令和1年9月4日(2019.9.4)　(24)登録日　令和1年8月16日(2019.8.16)

(51)Int.Cl.　　F I
G06F 8/658 (2018.01)　　G06F 8/658
B60R 16/02 (2006.01)　　B60R 16/02 660U

請求項の数 6　(全 18 頁)

(21)出願番号　特願2016-145945(P2016-145945)
(22)出願日　平成28年7月26日(2016.7.26)
(65)公開番号　特開2018-18186(P2018-18186A)
(43)公開日　平成30年2月1日(2018.2.1)
審査請求日　平成30年7月26日(2018.7.26)

(73)特許権者　509186579
日立オートモティブシステムズ株式会社
茨城県ひたちなか市高場２５２０番地
(74)代理人　100091096
弁理士　平木　祐輔
(74)代理人　100118773
弁理士　藤田　節
(74)代理人　100102576
弁理士　渡辺　敏章
(72)発明者　中原　章晴
茨城県ひたちなか市高場２５２０番地　日立オートモティブシステムズ株式会社内
(72)発明者　黒澤　憲一
茨城県ひたちなか市高場２５２０番地　日立オートモティブシステムズ株式会社内
最終頁に続く

(54)【発明の名称】車両制御装置、車載ネットワークシステム

(57)【特許請求の範囲】
【請求項１】
車両の動作を制御する処理を実装した制御プログラムを格納する不揮発メモリ、
前記制御プログラムを実行する演算部、
を備え、
前記不揮発メモリは、現在実行すべき現行版制御プログラムを格納する第１記憶領域と、前記現行版制御プログラムの更新版である更新版制御プログラムを格納する第２記憶領域とを有し、
前記演算部は、前記更新版制御プログラムと前記現行版制御プログラムとの間の差分を表す差分データ、もしくは前記更新版制御プログラムを圧縮した圧縮データを用いて前記更新版制御プログラムを復元して前記第２記憶領域に格納し、または前記更新版制御プログラムそのものを取得して前記第２記憶領域に格納し、
前記不揮発メモリはさらに、前記第２記憶領域から前記第１記憶領域へ前記更新版制御プログラムをコピー完了したか否かを表す管理データを格納し、
前記演算部は、前記第２記憶領域から前記第１記憶領域に対して前記更新版制御プログラムをコピーするとともに、コピー完了した旨を示す完了フラグを前記管理データに書き込み、
前記演算部は、前記管理データが前記完了フラグを表している場合は、前記第１記憶領域に対して前記更新版制御プログラムが正常に書き込まれているか否かをチェックし、
前記演算部は、前記第１記憶領域に対して前記更新版制御プログラムが正常に書き込ま

れている場合は、前記第１記憶領域が正常である旨を示す正常フラグを前記管理データに書き込み、
前記演算部は、前記第１記憶領域に対して前記更新版制御プログラムが正常に書き込まれていない場合は、前記第１記憶領域が正常である旨を示す正常フラグを前記管理データに書き込みせず、
前記演算部は、前記第１記憶領域が格納している制御プログラムを実行し、前記第２記憶領域が格納している制御プログラムは前記正常フラグの内容によらず実行しない
ことを特徴とする車両制御装置。
【請求項２】
前記演算部は、前記第２記憶領域に対して前記更新版制御プログラムを正常に書込完了した場合は、コピー未実施である旨を示す未実施フラグを前記管理データに書き込み、
前記演算部は、前記管理データが前記未実施フラグを表している場合は、前記第２記憶領域に対して前記更新版制御プログラムが正常に書き込まれているか否かをチェックし、
前記演算部は、前記第２記憶領域に対して前記更新版制御プログラムが正常に書き込まれている場合は、前記第２記憶領域から前記第１記憶領域に対して前記更新版制御プログラムをコピーするとともに、前記完了フラグを前記管理データに書き込み、
前記演算部は、前記第２記憶領域に対して前記更新版制御プログラムが正常に書き込まれていない場合は、前記更新版制御プログラムのコピーを行わず、かつ前記完了フラグを前記管理データに書き込みしない
ことを特徴とする請求項１記載の車両制御装置。
【請求項３】
請求項１記載の車両制御装置、
前記車両制御装置と接続された車載ネットワーク、
前記車両制御装置が前記車載ネットワークを介して他装置と通信する際に通信データを中継するゲートウェイ装置、
を有し、
前記ゲートウェイ装置は、前記車両制御装置に対して、前記差分データ、前記圧縮データ、または前記更新版制御プログラムのうちいずれかを送信する
ことを特徴とする車載ネットワークシステム。
【請求項４】
前記ゲートウェイ装置は、前記更新版制御プログラムを前記第２記憶領域に対して正常に書き込み完了したか否かを確認するよう要求する第１正当性チェックリクエストを、前記車両制御装置に対して送信し、
前記車両制御装置は、前記第１正当性チェックリクエストを受け取ると、前記第２記憶領域の妥当性をチェックするとともに、その結果を前記第１正当性チェックリクエストに対する返信として前記ゲートウェイ装置に対して送信する
ことを特徴とする請求項３記載の車載ネットワークシステム。
【請求項５】
前記ゲートウェイ装置は、前記更新版制御プログラムを前記第１記憶領域に対して正常にコピー完了したか否かを確認するよう要求する第２正当性チェックリクエストを、前記車両制御装置に対して送信し、
前記車両制御装置は、前記第２正当性チェックリクエストを受け取ると、前記第１記憶領域の妥当性をチェックするとともに、その結果を前記第２正当性チェックリクエストに対する返信として前記ゲートウェイ装置に対して送信する
ことを特徴とする請求項３記載の車載ネットワークシステム。
【請求項６】
前記ゲートウェイ装置は、前記車両制御装置が前記更新版制御プログラムを前記第２記憶領域から前記第１記憶領域へコピーする処理が中断したことを検出すると、前記第２正当性チェックリクエストを前記車両制御装置に対して再送信する
ことを特徴とする請求項５記載の車載ネットワークシステム。

【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、車両制御装置に関するものである。
【背景技術】
【０００２】
車両制御装置は、車両を制御する動作を実装した制御プログラムを実行する演算装置（例えばマイクロコンピュータ）、制御プログラムを格納するＦｌａｓｈＲＯＭ（Ｒｅａｄ Ｏｎｌｙ Ｍｅｍｏｒｙ）などの記憶装置を備える。制御プログラムの更新は、従来は、車両を販売店に持ち込み、専門の整備員がプログラム書込装置を車両に接続して実施することが多かった。しかし、クルマがインターネットに常時接続する、いわゆる「コネクティッド・ビークル」の急速な普及により、カーナビゲーションシステムにおける機能追加や地図データの更新にとどまらず、車両の制御プログラムについても、無線を介してユーザ自身の手で更新を実行させることが想定されるようになってきた。
【０００３】
その一方で、このようなシーンにおいて、万一プログラムの書込み処理中に何らかの要因（通信の途絶、ハードウェア異常発生など）で更新が失敗してしまった場合には、新バージョンはもちろんのこと、旧バージョンのソフトウェアも使用不能あるいは機能不全を来たすこととなり、最悪の場合、車両を動かせなくなることが想定される。また、ユーザ自身に更新を実行させる場合、プログラム更新によって車両が使用できなくなる期間を如何に低減するかは、利便性の観点から非常に重要となる。
【０００４】
下記特許文献１は、制御プログラムの現行バージョンを格納する主格納エリアと、更新バージョンを格納する副格納エリアとをＦｌａｓｈＲＯＭに設け、プログラム更新の際、そのエリアを交互に使用することにより、万一更新バージョンプログラムの書き込みに失敗しても、旧バージョンは引き続き使用可能としている。また同文献は、プログラム更新時間を短縮する手段として、全ての制御用ソフトウェアが共通に作動休止している期間を特定する手段を設け、その特定された共通休止作動期間にプログラム書換処理を実施することとしている。これにより、プログラム書換のために車両が使用できなくなる期間を低減ないし排除可能としている。
【０００５】
下記非特許文献１は、プログラムを差分更新する手法について記載している。同文献はＢｌｏｃｋ－Ｍｏｖｅアルゴリズムという手法を提案している。同アルゴリズムにより差分データに基づき更新版プログラムを復元することができる。
【先行技術文献】
【特許文献】
【０００６】
【特許文献１】特開２００６－３０１９６０号公報
【非特許文献】
【０００７】
【非特許文献１】Ｗａｌｔｅｒ Ｆ．Ｔｉｃｈｙ，「Ｔｈｅ Ｓｔｒｉｎｇ－ｔｏ－Ｓｔｒｉｎｇ Ｃｏｒｒｅｃｔｉｏｎ Ｐｒｏｂｒｅｍ ｗｉｔｈ Ｂｌｏｃｋ Ｍｏｖｅｓ」，ＡＣＭ Ｔｒａｎｓａｃｔｉｏｎｓ ｏｎ Ｃｏｍｐｕｔｅｒ Ｓｙｓｔｅｍｓ，ＡＣＭ（Ａｓｓｏｃｉａｔｉｏｎ ｆｏｒ Ｃｏｍｐｕｔｉｎｇ Ｍａｃｈｉｎｅｒｙ），１９８４年１１月，第２巻，第４号，ｐ．３０９－３２１
【発明の概要】
【発明が解決しようとする課題】
【０００８】
非特許文献１記載の技術は、プログラムを更新するために要する時間を短縮することができると考えられるので、特にユーザ自身がプログラム更新作業を実施する際には、ユー

ザ負担を抑える観点から有用である。ただし同技術を用いるに際して、差分データに基づき更新版プログラムを生成するプロセスが中断されるなどのエラーが生じると、上述のような課題が生じる。この課題は、更新データが圧縮されている場合や更新版プログラムそのものを配信する場合においても共通する。そこで例えば特許文献１記載の技術などを用いて、かかる課題を回避することが考えられる。

【０００９】

しかし特許文献１記載の技術は、常に動作しているような車両制御装置（エンジンの制御装置など）については休止作動期間を特定することができないので、プログラム書換のタイミングを特定することが困難であるという課題が想定される。

【００１０】

本発明は、上記のような課題に鑑みてなされたものであり、差分更新などの更新技術を採用した場合において、プログラム書換によって車両が動作できなくなる事態に至る可能性を抑制することができる手法を提供することを目的とする。

【課題を解決するための手段】

【００１１】

本発明に係る車両制御装置は、第１記憶領域と第２記憶領域を備え、差分データなどの更新データを受け取ってこれに基づき更新版制御プログラムを復元するとともに、更新版制御プログラムを書き込んだ記憶領域を示す更新データにその書き込み先を記録する。

【発明の効果】

【００１２】

本発明に係る車両制御装置は、第１記憶領域と第２記憶領域を備えているので、万一更新版制御プログラムの書き込みに失敗したとしても、更新前の制御プログラムをそのまま用いて制御を継続することができる。また差分更新などの手法によって、更新処理を短縮することができる。

【図面の簡単な説明】

【００１３】

【図１】実施形態１に係る更新システムの構成図である。

【図２】車両１が備える車載ネットワークシステムの構成図である。

【図３】車両制御装置１１の構成図である。

【図４】管理データ１１２３の構成を示す図である。

【図５】車両制御装置１１が制御プログラムを更新する手順を説明するシーケンス例である。

【図６】書換プログラム１１２２が更新シーケンスを実施する手順を説明するフローチャートである。

【図７】ゲートウェイ１２が車両制御装置１１に対して送信するリプログラミング命令のメッセージＭ７００の構成例である。

【図８】ステップＳ６０３の詳細を説明するフローチャートである。

【図９】車両制御装置１１が差分更新を実施する際の処理フローを説明する図である。

【図１０】車両制御装置１１がゲートウェイ１２から正当性チェックコマンドを受信した際の書換プログラム１１２２の動作を説明するフローチャートである。

【図１１】起動プログラム１１２１の動作を説明するフローチャートである。

【図１２】実施形態２に係る車両制御装置１１の構成図である。

【図１３】実施形態２における管理データ１１２３の構成を示す図である。

【図１４】実施形態２に係る車両制御装置１１が制御プログラムを更新する手順を説明するシーケンス例である。

【図１５】実施形態２に係る車両制御装置１１が差分更新を実施する際の処理フローを説明する図である。

【図１６】車両制御装置１１がゲートウェイ１２から正当性チェックコマンドを受信した際の書換プログラム１１２２の動作を説明するフローチャートである。

【図１７】コピー状態フラグ１１２３４の状態遷移を示す図である。

【発明を実施するための形態】
【００１４】
＜実施の形態１＞
図１は、本発明の実施形態１に係る更新システムの構成図である。更新システムは、車両１、サーバ２、インターネット回線３、無線基地局４を備える。車両１は、インターネット回線３および無線基地局４を介し、無線通信によりサーバ２と接続し、相互に通信する。無線通信は、例えば、３Ｇ／ＬＴＥなどの公衆回線による携帯電話網やＷｉＦｉなどの回線を用いて実現される。サーバ２は、車両１が実行する制御プログラムの更新版である更新版制御プログラムを、車両１に対して配信する。車両１が搭載している車両制御装置は、その更新版制御プログラムを書き込む。
【００１５】
図２は、車両１が備える車載ネットワークシステムの構成図である。車両制御装置１１は、車両１の動作を制御する制御プログラムを実行する装置であり、車載ネットワーク１３（例えばＣＡＮ（Ｃａｒ　Ａｒｅａ　Ｎｅｔｗｏｒｋ））を介してゲートウェイ１２（プログラム書込装置）と接続されている。車両制御装置１１は、ゲートウェイ１２を介して他の車両制御装置と通信することができる。
【００１６】
ゲートウェイ１２は、車両制御装置１１に対して制御プログラムを更新するよう指示するプログラム書込装置としての役割も有する。ゲートウェイ１２は、サーバ２から更新データＤ１３を受け取り、車両制御装置１１に対して制御プログラムの更新命令（リプログラミング命令）と更新データＤ１３を送信する。
【００１７】
ゲートウェイ１２は、演算部１２１、ＦｌａｓｈＲＯＭ（Ｒｅａｄ　Ｏｎｌｙ　Ｍｅｍｏｒｙ）１２２、ＳＲＡＭ（Ｓｔａｔｉｃ　Ｒａｎｄｏｍ　Ａｃｃｅｓｓ　Ｍｅｍｏｒｙ）１２３、通信装置１２４（例えばＣＡＮトランシーバ）を備える。演算部１２１は、ゲートウェイ１２が備える制御プログラムを実行することにより、車載ネットワーク上の車両制御装置やサーバ２との間で通信する。ゲートウェイ１２は、サーバ２から受信した更新データＤ１３をＦｌａｓｈＲＯＭ１２２に一時格納する。
【００１８】
図３は、車両制御装置１１の構成図である。車両制御装置１１は、演算部１１１、ＦｌａｓｈＲＯＭ１１２、ＳＲＡＭ１１３、ＤＲＡＭ（Ｄｙｎａｍｉｃ　Ｒａｎｄｏｍ　Ａｃｃｅｓｓ　Ｍｅｍｏｒｙ）１１４、通信装置１１５（例えばＣＡＮトランシーバ）を備える。
【００１９】
演算部１１１は、ＦｌａｓｈＲＯＭ１１２が格納している制御プログラムを実行する、例えばマイクロコンピュータなどの演算装置である。以下では記載の便宜上、各プログラムを動作主体として説明する場合があるが、実際にこれらプログラムを実行するのは演算部１１１である。
【００２０】
ＦｌａｓｈＲＯＭ１１２は、起動プログラム１１２１、書換プログラム１１２２、復元プログラム１１２６、管理データ１１２３を格納している。ＦｌａｓｈＲＯＭ１１２は、第１エリア１１２４と第２エリア１１２５を有する。第１エリア１１２４と第２エリア１１２５は、制御プログラムまたは更新版制御プログラムを格納する記憶領域である。
【００２１】
起動プログラム１１２１は、車両制御装置１１が通常モードで起動したとき演算部１１１が初めに実行するプログラムである。書換プログラム１１２２は、ゲートウェイ１２からの指示にしたがって、第１エリア１１２４または第２エリア１１２５が格納している制御プログラムを更新版制御プログラムに書き換える。本実施形態１においては、第１エリア１１２４が制御プログラムの現行プログラムＤ１１を格納し、第２エリア１１２５は空あるいは旧バージョンが格納されているものとする。復元プログラム１１２６および管理

データ１１２３については後述する。
【００２２】
車両制御装置１１は、例えば差分更新によって現行プログラムＤ１１を更新する。差分更新は、更新前後の制御プログラム間の差分を抽出し、これを用いてプログラムを更新する技術であり、プログラム更新時間を短縮することができる。差分更新の具体的な手法は例えば非特許文献１に記載されている。復元プログラム１１２６は、ゲートウェイ１２から受信した更新データＤ１３に基づき更新版制御プログラムを復元する。書換プログラム１１２２は、復元された更新版制御プログラムを第１エリア１１２４または第２エリア１１２５に対して書き込む。
【００２３】
更新データＤ１３は、現行プログラムＤ１１と更新版制御プログラムとの間の差分を抽出した差分データであってもよいし、これに代えて更新版制御プログラムを圧縮した圧縮データであってもよい。あるいは更新版制御プログラムそのものであってもよい。
【００２４】
図４は、管理データ１１２３の構成を示す図である。管理データ１１２３は、現行バージョン格納エリア番号１１２３１、第１エリアアドレスオフセット値１１２３２、第２エリアアドレスオフセット値１１２３３を保持する。
【００２５】
現行バージョン格納エリア番号１１２３１は、第１エリア１１２４と第２エリア１１２５のいずれが制御プログラムの現行バージョンを格納しているかを示すフラグである。第１エリアアドレスオフセット値１１２３２は、後述する更新命令が指定する書込先アドレスから第１エリア１１２４までの相対アドレスを指定する。第２エリアアドレスオフセット値１１２３３は、同様に第２エリア１１２５までの相対アドレスを指定する。
【００２６】
図５は、車両制御装置１１が制御プログラムを更新する手順を説明するシーケンス例である。以下図５にしたがって、実施形態１における更新シーケンスについて説明する。
【００２７】
ゲートウェイ１２は、制御プログラムの更新を開始すると、車両制御装置１１に対してモード遷移の命令を発行し、車両制御装置１１を通常モードからリプログラミングモードに遷移させる。
【００２８】
ゲートウェイ１２は、車両制御装置１１に対して、書込先エリアに格納されている古い制御プログラムのデータを消去するよう指示する。書換プログラム１１２２はその指示にしたがってＦｌａｓｈＲＯＭ１１２内のデータを消去し、完了するとその旨を応答する。書込先エリアは管理データ１１２３の記述にしたがって特定することができる（図３においては第２エリア１１２５を消去する）。
【００２９】
ゲートウェイ１２は、車両制御装置１１に対して、書込先エリアに更新版制御プログラムを書き込むよう命令する。書換プログラム１１２２は、ゲートウェイ１２からの指示にしたがって更新版制御プログラムを書き込む（図３においては第２エリア１１２５へ書き込む）。書込処理については後述する。書換プログラム１１２２は、ゲートウェイ１２に対して書込完了を応答する。
【００３０】
ゲートウェイ１２は、車両制御装置１１に対して、書き込んだデータの正当性をチェックするよう指示する。車両制御装置１１は、書き込んだ更新版制御プログラムの正当性をチェックする。正当性が確認されると、書換プログラム１１２２はその旨を応答するとともに、管理データ１１２３の現行バージョン格納エリア番号１１２３１を更新し、リプログラミングモードを終了して通常モードへ遷移する。
【００３１】
図６は、書換プログラム１１２２が更新シーケンスを実施する手順を説明するフローチ

ャートである。以下図６の各ステップについて説明する。
【００３２】
（図６：ステップＳ６００～Ｓ６０１）
演算部１１１は、ゲートウェイ１２からリプログラミング命令を受け取ると、本フローチャートを開始して書換プログラム１１２２を起動する（Ｓ６００）。演算部１１１は、リプログラミングモードに遷移する（Ｓ６０１）。
【００３３】
（図６：ステップＳ６０２～Ｓ６０４）
書換プログラム１１２２は、書込先エリアのデータを消去する（Ｓ６０２）。書換プログラム１１２２は、図５で説明した手順にしたがって更新データＤ１３をゲートウェイ１２から受け取り、復元プログラム１１２６を用いて更新版制御プログラムを復元し、復元した更新版制御プログラムを書込先エリア（図３においては第２エリア１１２５）へ書き込む（Ｓ６０３）。書換プログラム１１２２は、書き込んだ更新版制御プログラムの正当性をチェックする（Ｓ６０４）。
【００３４】
（図６：ステップＳ６０５）
書換プログラム１１２２は、Ｓ６０４における正当性チェックの判定結果をもって、更新版制御プログラムが正常に書き込み終了したか否かを判断する。正常終了した場合は、更新版制御プログラムが書き込まれたエリア（図３においては第２エリア１１２５）の番号を管理データ１１２３に書き込む。更新版制御プログラムの書き込みに失敗した場合は、管理データ１１２３を更新せず、現行バージョンを格納しているエリア番号がそのまま残った状態となる（図３においては第１エリア１１２４）。
【００３５】
（図６：ステップＳ６０５：補足）
本ステップにより、演算部１１１が制御プログラムを次回起動する際、起動プログラム１１２１は、管理データ１１２３を参照するだけで、正常に更新された制御プログラムを確実に起動することができる。さらには、更新版制御プログラムの書き込みに失敗した場合であっても、現行バージョンを引き続き実行することができる。
【００３６】
（図６：ステップＳ６０６）
以上の処理により更新シーケンスが完了し、演算部１１１は通常モードへ遷移する。
【００３７】
図７は、ゲートウェイ１２が車両制御装置１１に対して送信するリプログラミング命令のメッセージＭ７００の構成例である。メッセージＭ７００は、コマンドＭ７０１、データ種別７０２、書込データサイズＭ７０３、書込先エリア先頭アドレスＭ７０４、書込データＭ７０５を有する。
【００３８】
コマンドＭ７０１は、本メッセージがリプログラミング命令であることを示す。データ種別Ｍ７０２は、更新データが圧縮データ／差分データ／更新版制御プログラムそのもののうちいずれであるかを示す。書込データＭ７０５は更新データである。書込データサイズＭ７０３はそのサイズである。書込先エリア先頭アドレスＭ７０４は、更新版制御プログラムを書き込む記憶領域の先頭アドレスである。ただしゲートウェイ１２は、車両制御装置１１内部において第１エリア１１２４と第２エリア１１２５のいずれに対して更新版制御プログラムが書き込まれるのかを知らないので、あらかじめ定められたアドレスをＭ７０４として指定することになる。実際の書込先アドレスは、管理データ１１２３が記述している各オフセットにしたがって書換プログラム１１２２が定める。
【００３９】
図８は、ステップＳ６０３の詳細を説明するフローチャートである。以下図８の各ステップについて説明する。
【００４０】

（図８：ステップＳ８００）
書換プログラム１１２２は、ゲートウェイ１２から更新プログラム書込要求メッセージを受信すると、本フローチャートを開始する。図５においては、「更新プログラム書込」が同メッセージに対応する。
【００４１】
（図８：ステップＳ８０１）
書換プログラム１１２２は、管理データ１１２３の現行バージョン格納エリア番号１１２３１に基づき、書込先エリアアドレスを算出するためのオフセット値を取得する。図３においては、書込先エリアは第２エリア１１２５であるので、第２エリアアドレスオフセット値１１２３３を取得する。
【００４２】
（図８：ステップＳ８０２）
書換プログラム１１２２は、受信した書込先エリア先頭アドレスＭ７０４と取得した第２エリアアドレスオフセット値１１２３３から、書込先エリアである第２エリア１１２５のアドレスを算出する。例えばＭ７０４を基準としてさらに第２エリアアドレスオフセット値１１２３３だけアドレスをオフセットすることにより、第２エリア１１２５の先頭アドレスを求めることができる。
【００４３】
（図８：ステップＳ８０３）
書換プログラム１１２２は、データ種別Ｍ７０２に基づき、書込データが圧縮データなのか、差分データなのか、更新版制御プログラムそのものなのか判断する。データ種別Ｍ７０２が差分データであればステップＳ８０４へ進み、圧縮データであればステップＳ８０６へ進み、更新版制御プログラムそのものであればステップＳ８０７へスキップする。
【００４４】
（図８：ステップＳ８０４～Ｓ８０５）
書換プログラム１１２２は、現行プログラムＤ１１が格納されるアドレスを算出し（Ｓ８０４）、受信した差分データと現行プログラムＤ１１を復元プログラム１１２６へ入力して、更新版制御プログラムを復元する（Ｓ８０５）。現行プログラムＤ１１のアドレスは、受信した書込先エリア先頭アドレスＭ７０４と現行プログラムＤ１１が格納されている格納エリアのアドレスオフセット値（図３においては第１エリアアドレスオフセット値１１２３２）から求めることができる。
【００４５】
（図８：ステップＳ８０６）
書換プログラム１１２２は、受信した圧縮データを復元プログラム１１２６へ入力して更新版制御プログラムを伸張する。
【００４６】
（図８：ステップＳ８０７）
書換プログラム１１２２は、復元した更新版制御プログラムを、Ｓ８０２で求めたＦｌａｓｈＲＯＭ１１２の書込先エリアの先頭アドレスから書込データサイズＭ７０３分書き込み、本フローチャートを終了する。データ種別Ｍ７０２が更新版制御プログラムそのものである場合は、復元処理は必要ないので、受け取った更新版制御プログラムをそのまま格納先エリアへ書き込めばよい。
【００４７】
図９は、車両制御装置１１が差分更新を実施する際の処理フローを説明する図である。以下図９を用いて、差分更新の動作を説明する。
【００４８】
書換プログラム１１２２は、ゲートウェイ１２から更新プログラム書込み要求メッセージを受信すると、ＳＲＡＭ１１３上の受信バッファ１１３１に更新データＤ１３を一時的に格納する。復元プログラム１１２６は、更新データＤ１３と、ＦｌａｓｈＲＯＭ１１２上の第１エリア１１２４に格納される現行プログラムＤ１１から、更新版制御プログラム

を復元バッファ１１３２に復元する。本図には記載しないが、復元プログラム１１２６は、現行プログラムと新プログラムの差分を抽出した差分データを復元する機能と、更新プログラムを入力として生成した圧縮データを伸張する機能を持つ。書換プログラム１１２２は、復元バッファ１１３２上の新プログラムＤ１２を、書込先エリア（ここでは第２エリア１１２５）に書き込む。

【００４９】

図１０は、車両制御装置１１がゲートウェイ１２から正当性チェックコマンドを受信した際の書換プログラム１１２２の動作を説明するフローチャートである。以下図１０の各ステップについて説明する。

【００５０】

（図１０：ステップＳ１０００）

書換プログラム１１２２は、ゲートウェイ１２からデータの正当性チェックコマンドを受信すると本フローチャートを開始する。図５においては、「データの正当性チェック」が同コマンドに対応する。

【００５１】

（図１０：ステップＳ１００１～Ｓ１００３）

書換プログラム１１２２は、管理データ１１２３の現行バージョン格納エリア番号１１２３１に基づき、更新版制御プログラムをいずれのエリアに対して書き込むべきかを判断する（Ｓ１００１）。書換プログラム１１２２は、書き込まれた更新版制御プログラムのデータに誤りがないか（更新データが正しく書き込まれたか）を検証する（Ｓ１００２またはＳ１００３）。具体的には、ＣＲＣ（Ｃｙｃｌｉｃ　Ｒｅｄｕｎｄａｎｃｙ　Ｃｈｅｃｋ）やハッシュ値を用いた妥当性チェックによってこれを実施できる。

【００５２】

（図１０：ステップＳ１００４～Ｓ１００７）

書換プログラム１１２２は、上述の妥当性チェックの結果を判断する（Ｓ１００４またはＳ１００６）。妥当性チェックの結果が正常である場合は、現行プログラム格納エリア番号１１２３１を書込先エリア番号に更新する（Ｓ１００５またはＳ１００７）。妥当性チェックの結果が異常である場合は、管理データ１１２３を更新することなく本フローチャートを終了する。

【００５３】

（図１０：ステップＳ１００４～Ｓ１００７：補足）

制御プログラムが正常に更新されなかった場合は、現行プログラム格納エリア番号１１２３１を更新しないので、正常に格納されなかった制御プログラムを次回起動させないようにすることができる。

【００５４】

図１１は、起動プログラム１１２１の動作を説明するフローチャートである。以下図１１の各ステップについて説明する。

【００５５】

（図１１：ステップＳ１１００）

演算部１１１は、例えば割込信号などによってイグニッションがＯＮされた旨を検知すると、本フローチャートを開始して起動プログラム１１２１を起動する。

【００５６】

（図１１：ステップＳ１１０１～Ｓ１１０３）

起動プログラム１１２１は、管理データ１１２３の現行バージョン格納エリア番号１１２３１を取得し、第１エリア１１２４と第２エリア１１２５のいずれが現行バージョンエリアであるかを判断する（Ｓ１１０１）。起動プログラム１１２１は、そのエリアに格納されている制御プログラムを実行する（Ｓ１１０２またはＳ１１０３）。

【００５７】

（図１１：ステップＳ１１０１～Ｓ１１０３：補足）

なお、実施形態１においては、制御プログラムが第１エリア１１２４と第２エリア１１

２５のいずれかに格納されるが、プログラム起動時、ＲＡＭの固定エリアに展開してから実行されるので、実行プログラムを第１エリア用・第２エリア用それぞれ作成する必要はない。

【００５８】

＜実施の形態１：まとめ＞

本実施形態１に係る車両制御装置１１は、ＦｌａｓｈＲＯＭ１１２内に第１エリア１１２４と第２エリア１１２５を設け、差分データなどの更新データをいずれかのエリアに対して書き込むとともに、現行バージョン格納エリア番号１１２３１をその書込先エリア番号に更新する。これにより、更新処理にともなってユーザが車両を使用できない時間を低減するとともに、更新データの書き込みが失敗しても制御を継続することができる。

【００５９】

＜実施の形態２＞

図１２は、本発明の実施形態２に係る車両制御装置１１の構成図である。本実施形態２においては、第１エリア１１２４（実行エリア）は実行する制御プログラムを格納するためのみに使用され、第２エリア１１２５（副エリア）は制御プログラムの更新時において更新版制御プログラムを書き込むためのみに使用される。本実施形態２においては、ＦｌａｓｈＲＯＭ１１２が格納している制御プログラムをＦｌａｓｈＲＯＭ１１２上で実行するので、更新データを展開するためのＤＲＡＭは必ずしも必要ない。その他構成は実施形態１と同様であるので、以下では第１エリア１１２４と第２エリア１１２５の用途に関連する差異点を中心に説明する。

【００６０】

図１３は、本実施形態２における管理データ１１２３の構成を示す図である。本実施形態２における管理データ１１２３は、現行バージョン格納エリア番号１１２３１、コピー状態フラグ１１２３４を格納する。

【００６１】

本実施形態２においては、常に第１エリア１１２４が制御プログラムを実行するために使用されるので、現行バージョン格納エリア番号１１２３１は常に「第１エリア」を示す値を保持する。コピー状態フラグ１１２３４は、第２エリア１１２５に書き込まれた更新版制御プログラムを第１エリア１１２４にコピーする際に、コピー処理の状態を示すフラグを保持する。

【００６２】

図１４は、本実施形態２に係る車両制御装置１１が制御プログラムを更新する手順を説明するシーケンス例である。以下図１４にしたがって、本実施形態２における更新シーケンスについて説明する。

【００６３】

ゲートウェイ１２は、制御プログラムの更新を開始すると、車両制御装置１１に対してモード遷移の命令を発行し、車両制御装置１１を通常モードからリプログラミングモードに遷移させる。

【００６４】

ゲートウェイ１２は、車両制御装置１１に対して、書込先エリアに格納されている古い制御プログラムのデータを消去するよう指示する。書換プログラム１１２２はその指示にしたがってＦｌａｓｈＲＯＭ１１２上のデータを消去し、完了するとその旨を応答する。

【００６５】

ゲートウェイ１２は、車両制御装置１１に対して、第２エリア１１２５に更新版制御プログラムを書き込むよう命令する。書換プログラム１１２２は、ゲートウェイ１２からの指示にしたがって更新版制御プログラムを書き込む。書込処理については実施形態１と同様である。書換プログラム１１２２は、ゲートウェイ１２に対して書込完了を応答する。

【００６６】

ゲートウェイ１２は、車両制御装置１１に対して、書き込んだデータの正当性をチェックするよう指示する。本実施形態２においては、更新版制御プログラムを第２エリア１１

２５に対して正常に書込完了したことを確認する正当性チェックコマンドａと、その更新版制御プログラムを第１エリア１１２４に対して正常にコピー完了したことを確認する正当性チェックコマンドｂを、それぞれ送信する。車両制御装置１１は、これらコマンドにしたがって正当性をチェックしてその結果を応答する。応答が完了するとリプログラミングモードを終了して通常モードへ遷移する。

【００６７】

書換プログラム１１２２は、例えば更新版制御プログラムを第２エリア１１２５から第１エリア１１２４に対してコピーする処理が中断された場合は、その旨をゲートウェイ１２に対して通知することもできる。この場合ゲートウェイ１２は、正当性チェックコマンドｂを改めて送信し、車両制御装置１１は後述の図１６にしたがってチェックを改めて実施してもよい。

【００６８】

図１５は、本実施形態２に係る車両制御装置１１が差分更新を実施する際の処理フローを説明する図である。以下図１５を用いて、本実施形態２における差分更新の動作を説明する。

【００６９】

書換プログラム１１２２は、ゲートウェイ１２から更新プログラム書込み要求メッセージを受信すると、ＳＲＡＭ１１３上の受信バッファ１１３１に更新データＤ１３を一時的に格納する。復元プログラム１１２６は、更新データＤ１３と、ＦｌａｓｈＲＯＭ１１２上の第１エリア１１２４に格納される現行プログラムＤ１１から、更新版制御プログラム（新プログラムＤ１２）を復元バッファ１１３２に復元する。書換プログラム１１２２は、復元された新プログラムＤ１２を、ＦｌａｓｈＲＯＭ１１２の第２エリア（副エリア）１１２５に書き込む。新プログラムの書込み終了後、書換プログラム１１２２は、ゲートウェイ１２からの指示にしたがって、第２エリア１１２５から第１エリア１１２４へ新プログラムＤ１２をコピーする。

【００７０】

図１６は、車両制御装置１１がゲートウェイ１２から正当性チェックコマンドを受信した際の書換プログラム１１２２の動作を説明するフローチャートである。前提として、新プログラムＤ１２の書込終了時に、書換プログラム１１２２はコピー状態フラグ１１２３４に「未実施」を格納した状態となっているものとする。以下図１６の各ステップについて説明する。

【００７１】

（図１６：ステップＳ１６００）

書換プログラム１１２２は、ゲートウェイ１２からデータの正当性チェックコマンドを受信すると本フローチャートを開始する。図１４においては、「データの正当性チェックａ」「データの正当性チェックｂ」が同コマンドに対応する。

【００７２】

（図１６：ステップＳ１６０１）

書換プログラム１１２２は、最初にコピー状態フラグ１１２３４をチェックする。コピー状態フラグ１１２３４の状態遷移については図１７で改めて説明する。コピー状態フラグ１１２３４が「実行エリア正常」であれば本フローチャートを終了する。コピー状態フラグ１１２３４が「未実施」であればステップＳ１６０２へ進む。コピー状態フラグ１１２３４が「コピー完了」であればステップＳ１６０７へ進む。

【００７３】

（図１６：ステップＳ１６０２～Ｓ１６０３）

書換プログラム１１２２は、第２エリア１１２５に書込まれた更新版制御プログラムの妥当性をチェックする（Ｓ１６０２）。妥当性チェックの結果が正常である場合はステップＳ１６０４へ進み、異常であれば本フローチャートを終了する（Ｓ１６０３）。

【００７４】

（図１６：ステップＳ１６０４～Ｓ１６０６）

書換プログラム１１２２は、第１エリア１１２４のデータを消去する（Ｓ１６０４）。消去が終了したら、第２エリア１１２５から第１エリア１１２４に更新版制御プログラムをコピーする（Ｓ１６０５）。書換プログラム１１２２は、コピー状態フラグ１１２３４に「コピー完了」を格納する。

【００７５】

（図１６：ステップＳ１６０７～Ｓ１６０９）

書換プログラム１１２２は、第１エリア１１２４に書き込まれた制御プログラムの妥当性をチェックする（Ｓ１６０７）。妥当性チェックの結果が正常である場合はコピー状態フラグ１１２３４に「実行エリア正常」を格納し（Ｓ１６０９）、異常である場合は本フローチャートを終了する（Ｓ１６０８）。

【００７６】

（図１６：補足）

本フローチャートによれば、コピー状態フラグ１１２３４を用いて第２エリア１１２５から第１エリア１１２４へのコピーを制御することができる。万一、何らかの要因でコピー中に処理が中断した場合であっても、コピー状態フラグ１１２３４を参照することにより中断時の状態からコピーをリトライすることもできる。

【００７７】

図１７は、コピー状態フラグ１１２３４の状態遷移を示す図である。書換プログラム１１２２は、コピー状態フラグ１１２３４が「未実施」であるとき正当性チェックコマンドａを受信すると、ステップＳ１６０２～Ｓ１６０６を通じてコピー状態フラグ１１２３４に「コピー完了」を格納する。さらに正当性チェックコマンドｂを受信すると、ステップＳ１６０７～Ｓ１６０８を通じてコピー状態フラグ１１２３４に「実行エリア正常」を格納する。制御プログラムをさらに更新した場合、コピー状態フラグ１１２３４に「未実施」を格納する。

【００７８】

＜実施の形態２：まとめ＞

本実施形態２に係る車両制御装置１１は、実施形態１と同様に更新処理にともなってユーザが車両を使用できない時間を低減することができる。なお、本実施形態２のように制御プログラムの実行エリアを固定化（本実施例では、第１エリア１１２４）することで、実行プログラムは、それ用のみ作成すればよく、第１エリアと第２エリアいずれかに格納された状態で実行する場合にくらべ、制御プログラムの出荷前検査を２重に検証する必要がない。

【００７９】

＜本発明の変形例について＞

本発明は上記実施形態に限定されるものではなく、様々な変形例が含まれる。例えば、上記した実施形態は本発明を分かりやすく説明するために詳細に説明したものであり、必ずしも説明した全ての構成を備えるものに限定されるものではない。また、ある実施形態の構成の一部を他の実施形態の構成に置き換える事が可能であり、また、ある実施形態の構成に他の実施形態の構成を加えることも可能である。また、各実施形態の構成の一部について他の構成の追加・削除・置換をすることができる。

【００８０】

実施形態１～２においては、制御プログラムを格納するエリアの例としてＦｌａｓｈＲＯＭ１１２を挙げたが、その他の不揮発性記憶装置を用いてもよい。

【００８１】

実施形態１～２においては、ＦｌａｓｈＲＯＭ１１２が第１エリア１１２４と第２エリア１１２５に分かれている構成例を説明したが、同様の構成を２つの記憶装置によって実現することもできる。また記憶領域（または記憶装置）を３つ以上設け、実施形態１～２と同様の構成を実現することもできる。この場合は例えば各記憶領域（または記憶装置）に対して順番に制御プログラムを格納することになる。

【００８２】

管理データ１１２３は、現行バージョン格納エリア番号１１２３１を保存する構成を説明したが、書込先のエリア番号を保存する構成であってもよい。

【００８３】

更新シーケンスにおいては、制御プログラムの最新版を書き込むのが通常であるが、諸事情によってはダウンバージョンした制御プログラムで更新する可能性もある。この場合、制御プログラムの更新版とはそのダウンバージョンした制御プログラムである。すなわち制御プログラムの更新版とは、直前の更新シーケンスによって書き込まれた制御プログラムのことを指す。

【００８４】

上記各構成、機能、処理部、処理手段等は、それらの一部を、例えば集積回路で設計する等によりハードウェアで実現してもよい。また、上記の各構成、機能等は、プロセッサがそれぞれの機能を実現するプログラムを解釈し、実行することによりソフトウェアで実現してもよい。各機能を実現するプログラム、テーブル、ファイル等の情報は、メモリ、ハードディスク、ＳＳＤ（Ｓｏｌｉｄ　Ｓｔａｔｅ　Ｄｒｉｖｅ）等の記録装置、ＩＣカード、ＳＤカード、ＤＶＤ等の記録媒体に格納することができる。

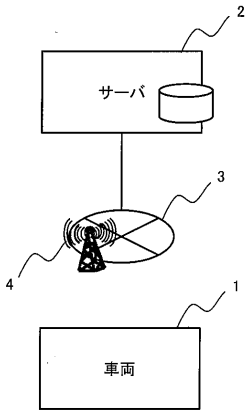
【符号の説明】

【００８５】

１：車両
２：サーバ
３：インターネット回線
４：無線基地局
１１：車両制御装置
１１２１：起動プログラム
１１２２：書換プログラム
１１２３：管理データ
１１２４：第１エリア
１１２５：第２エリア
１１２６：復元プログラム
１２：ゲートウェイ
１３：車載ネットワーク
Ｄ１１：現行プログラム
Ｄ１２：新プログラム
Ｄ１３：更新データ

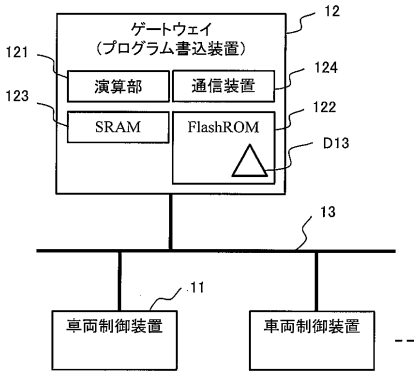
【図１】

図1



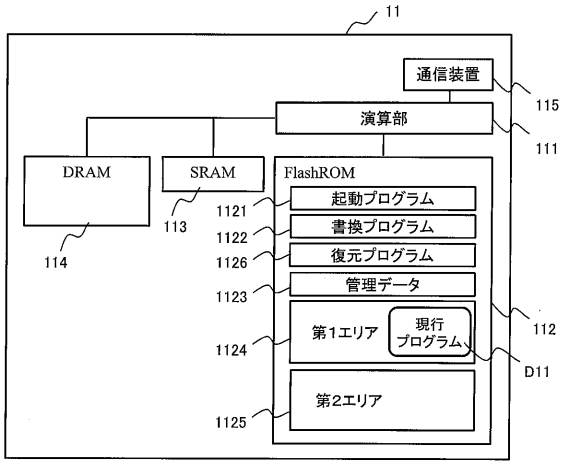
【図２】

図2



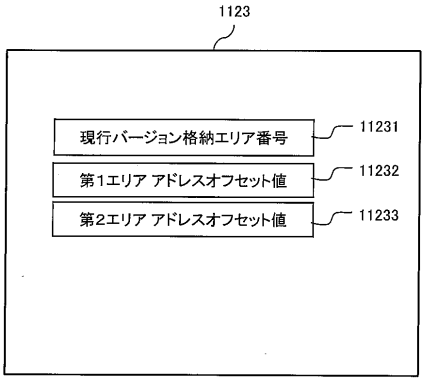
【図３】

図3



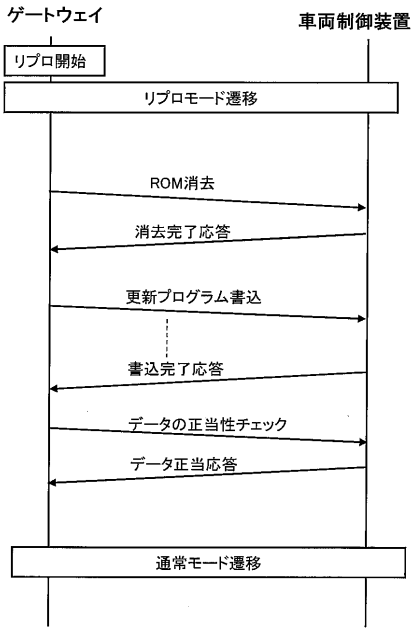
【図４】

図4



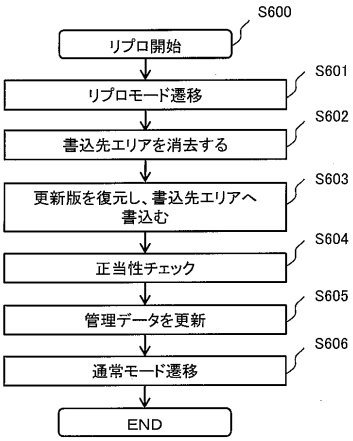
【図５】

図5



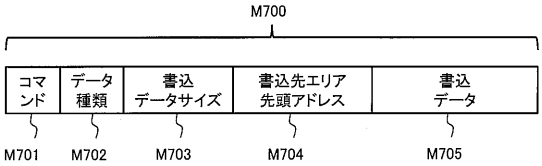
【図６】

図6



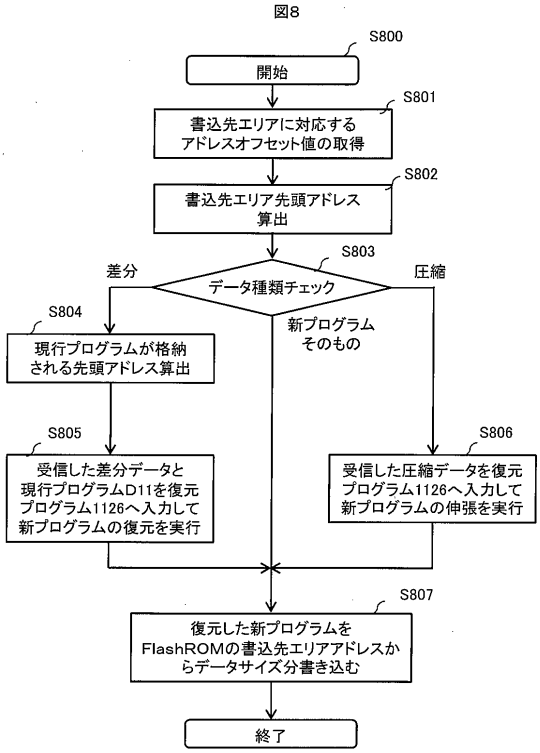
【図７】

図7



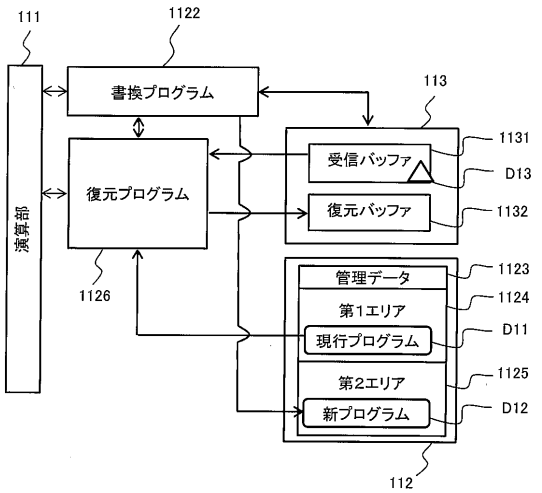
【図８】

図8



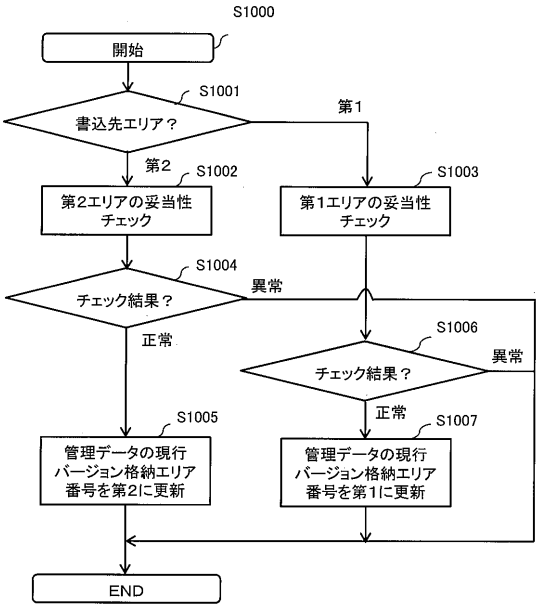
【図９】

図9



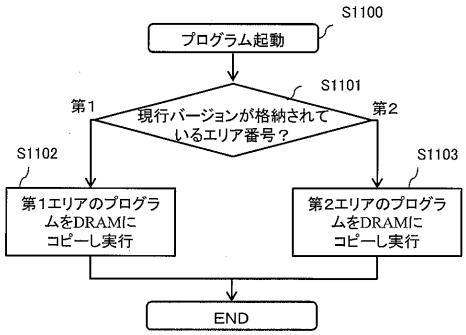
【図１０】

図10



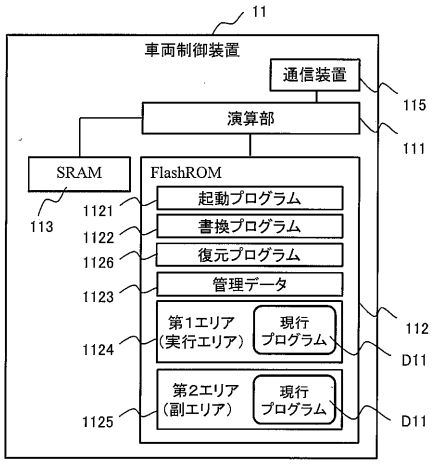
【図１１】

図11



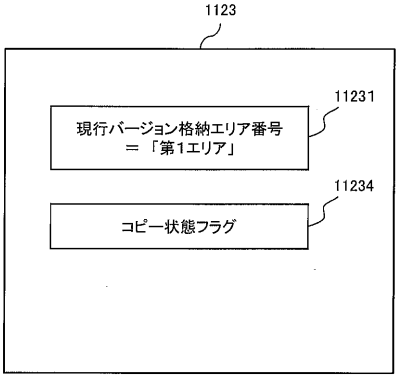
【図１２】

図12



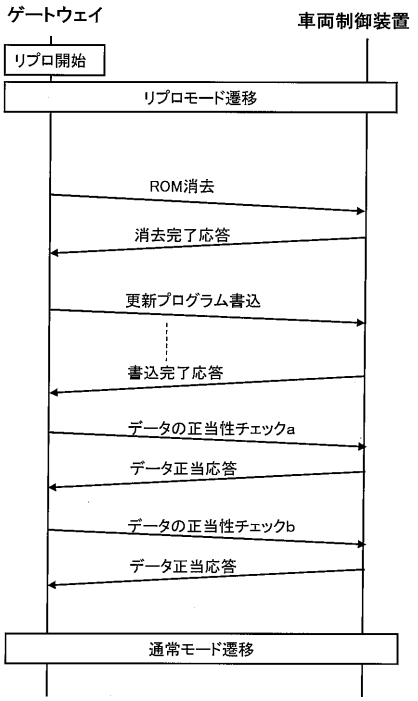
【図１３】

図13



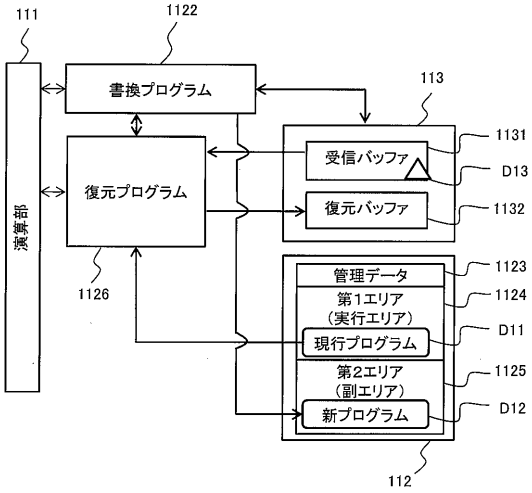
【図１４】

図14



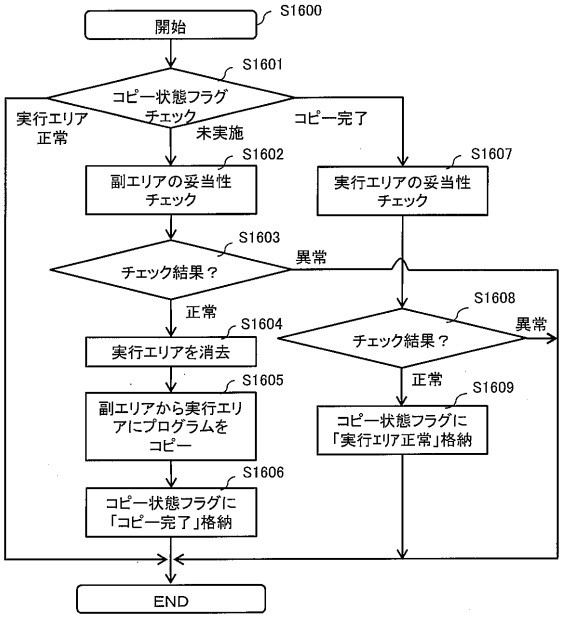
【図１５】

図15



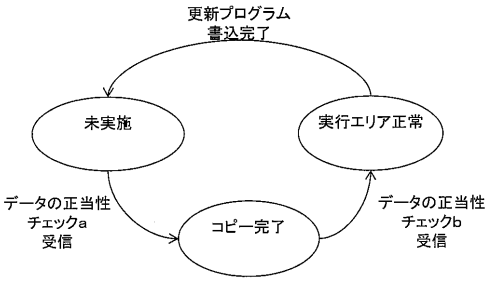
【図１６】

図16



【図１７】

図17



フロントページの続き

(72)発明者　荒木　肇
茨城県ひたちなか市高場２５２０番地　日立オートモティブシステムズ株式会社内

審査官　今城　朋彬

(56)参考文献　国際公開第２０１６／０４７３１２（WO，Ａ１）
特開２０１１－０７６３７０（ＪＰ，Ａ）
特開平１０－２６９０７８（ＪＰ，Ａ）
特開２００９－２７１７３７（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　　８／６５
Ｂ６０Ｒ　１６／０２