

(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号
特許第7589657号
(P7589657)

(45)発行日 令和6年11月26日(2024.11.26)

(24)登録日 令和6年11月18日(2024.11.18)

(51)国際特許分類

F I

G 0 6 F 8/654(2018.01)

G 0 6 F 8/654

G 0 6 F 21/64 (2013.01)

G 0 6 F 21/64

G 0 9 C 1/00 (2006.01)

G 0 9 C 1/00 6 1 0 A

請求項の数 7 (全15頁)

(21)出願番号	特願2021-121135(P2021-121135)	(73)特許権者	000004260
(22)出願日	令和3年7月23日(2021.7.23)		株式会社デンソー
(65)公開番号	特開2023-16643(P2023-16643A)		愛知県刈谷市昭和町1丁目1番地
(43)公開日	令和5年2月2日(2023.2.2)	(74)代理人	
審査請求日	令和6年1月9日(2024.1.9)		矢作 和行
		(74)代理人	100121991
			弁理士 野々部 泰平
		(74)代理人	100145595
			弁理士 久保 貴則
		(72)発明者	浅井 健史
			愛知県刈谷市昭和町1丁目1番地 株式
			会社デンソー内
		審査官	児玉 崇晶

最終頁に続く

(54)【発明の名称】 電子制御装置

(57)【特許請求の範囲】
【請求項1】

制御プログラム（111）が書き込まれるプログラム領域（101）、前記制御プログラムに固有の固有認証子（112）が書き込まれる固有認証子領域（102）、および前記制御プログラムの書換えが完了した際に、前記制御プログラムの書換えが完了したか否かを検証するための検証計算から得られ、前記制御プログラムの書換えが完了している場合には前記固有認証子と所定の対応関係を有する検証情報（113）が書き込まれる検証情報領域（103）を含む書換領域（100）を有する記憶部（10）と、
前記記憶部に書き込まれた情報を演算する演算部（50）と、を備え、
前記演算部は、前記書換領域の書換えを行う書換部（S20～S60）、および起動時に前記書換領域の書換えが完了しているか否かを判定する判定部（S100～S130）を有し、
前記書換部は、前記書換領域を消去するものであって、前記検証情報を初めに消去する消去部（S20）と、
前記消去部が消去を行った後に、書換用の前記制御プログラムを前記プログラム領域に書き込むとともに、前記固有認証子を前記固有認証子領域に書き込む書込部（S30）と、
前記書込部が書込みを行った後に、前記検証計算を行う検証部（S40）と、
前記検証部によって得られた前記検証情報を前記検証情報領域に書き込む検証情報書込部（S60）と、を有し、
前記判定部は、前記固有認証子領域に記憶された値と、前記検証情報領域に記憶された

値と、が所定の対応関係を有する場合には、前記書換領域の書換えが完了していると判定し、所定の対応関係を有さない場合には、前記書換領域の書換えが完了していないと判定する、電子制御装置。

【請求項 2】

前記判定部によって前記書換領域の書換えが完了していると判定された場合には、書き換えられた前記制御プログラムを起動させ、前記書換領域の書換えが完了していないと判定された場合には、前記制御プログラムの書換えを開始させる起動制御部（S 1 2 0、S 1 3 0）を備える、請求項 1 に記載の電子制御装置。

【請求項 3】

前記制御プログラムは、分割して M 個（M は 2 以上の整数）のブロックが得られるものであり、

前記検証計算には、各ブロックを 1 番目のブロックから順番に用いて暗号化するものであり、N 番目（N は 1 以上の整数、 $M \geq N$ ）のブロックについて暗号化された暗号文によって N + 1 番目のブロックを暗号化する暗号利用モードが用いられており、

前記検証情報とは、あらかじめ定められた L 番目（L は 2 以上の整数、 $M > L$ ）のブロックについての暗号文（1 1 3 a）であり、

前記判定部は、起動時に、前記 L 番目のブロックについての暗号文を用いた暗号化から前記検証計算を再度行うことで、1 番目から M 番目のブロックまでの暗号化を行い、前記 M 番目のブロックの暗号文を再検証認証子として演算する再検証部（S 1 0 0）を有し、

前記所定の対応関係とは、前記再検証認証子の値と、前記固有認証子の値と、が一致する関係である、請求項 2 に記載の電子制御装置。

【請求項 4】

前記 L 番目とは、M が偶数の場合、 $L \leq M / 2$ であり、M が奇数の場合、 $L \leq (M + 1) / 2$ である、請求項 3 に記載の電子制御装置。

【請求項 5】

前記 L 番目とは、M が偶数の場合、 $L > M / 2$ であり、M が奇数の場合、 $L > (M + 1) / 2$ である、請求項 3 に記載の電子制御装置。

【請求項 6】

前記検証計算には、前記制御プログラムを分割して得られる M 個（M は 2 以上の整数）のブロックのうち、N 番目（N は 1 以上の整数、 $M \geq N$ ）のブロックについて暗号化された暗号文によって N + 1 番目のブロックを暗号化する暗号利用モードが用いられており、

前記検証情報とは、前記検証計算の結果である検証認証子（1 1 3 b）であり、

前記所定の対応関係とは、前記検証認証子の値と、前記固有認証子の値と、が一致する関係である、請求項 2 に記載の電子制御装置。

【請求項 7】

書換用の前記制御プログラム、および前記固有認証子は、外部の書換ツール（6 0）から送信され、

前記 L 番目とは、前記書換ツールから指定された番号である、請求項 3 に記載の電子制御装置。

【発明の詳細な説明】

【技術分野】

【0 0 0 1】

本開示は、制御プログラムの書換完了判定を行う電子制御装置に関する。

【背景技術】

【0 0 0 2】

特許文献 1 には、制御プログラムに従う動作をする電子制御装置が記載されている。電子制御装置は、制御プログラムの書換え時に、制御プログラムの書換えの進行段階を示す値をメモリ内に記憶している。

【先行技術文献】

【特許文献】

【０００３】

【文献】特許第５３４９１０４号公報

【発明の概要】

【発明が解決しようとする課題】

【０００４】

上述した電子制御装置は、制御プログラムの書換えの進行段階に応じて、進行段階を示す値の消去および書込みを行う必要がある。よって、進行段階を示す値の消去および書込みは、制御プログラムの書換えの最中に行われる。さらに、書換用の制御プログラムと進行段階を示す値とでは、メモリへの書込みおよび消去のタイミングが異なる。このため、電子制御装置は、書換えの進行段階を示す値を記憶させる場合、制御プログラムが書き込まれたプログラム領域とは別に、進行段階に応じた値を書き込む段階記憶領域をメモリに有しなければならない。また、メモリは、段階記憶領域として、データの消去単位分の領域が必要になる。

10

【０００５】

ところで、メモリには、データの書込単位よりも、データの消去単位のほうが大きなものがある。また、進行段階を示す値は、制御プログラムの書換えの進行段階に応じた値であるため、データの書込み単位程度のサイズとなる。

【０００６】

このため、電子制御装置は、データの消去単位よりも小さなサイズの、進行段階に応じた値を記憶しておくためだけに、データの消去単位分の段階記憶領域が必要となる。よって、メモリの使用効率が低下する虞がある。

20

【０００７】

このような事情に鑑み、本開示の目的は、制御プログラムの書換えが完了しているか否かを判定でき、かつメモリの使用効率を向上できる電子制御装置を提供することである。

【課題を解決するための手段】

【０００８】

その目的を達成するための本開示の一態様における電子制御装置は、制御プログラム（１１１）が書き込まれるプログラム領域（１０１）、制御プログラムに固有の固有認証子（１１２）が書き込まれる固有認証子領域（１０２）、および制御プログラムの書換えが完了した際に、制御プログラムの書換えが完了したか否かを検証するための検証計算から得られ、制御プログラムの書換えが完了している場合には固有認証子と所定の対応関係を有する検証情報（１１３）が書き込まれる検証情報領域（１０３）を含む書換領域（１００）を有する記憶部（１０）と、

30

記憶部に書き込まれた情報を演算する演算部（５０）と、を備え、

演算部は、書換領域の書換えを行う書換部（Ｓ２０～Ｓ６０）、および起動時に書換領域の書換えが完了しているか否かを判定する判定部（Ｓ１００～Ｓ１３０）を有し、

書換部は、書換領域を消去するものであって、検証情報を初めに消去する消去部（Ｓ２０）と、

消去部が消去を行った後に、書換用の制御プログラムをプログラム領域に書き込むとともに、固有認証子を固有認証子領域に書き込む書込部（Ｓ３０）と、

40

書込部が書込みを行った後に、検証計算を行う検証部（Ｓ４０）と、

検証部によって得られた検証情報を検証情報領域に書き込む検証情報書込部（Ｓ６０）と、を有し、

判定部は、固有認証子領域に記憶された値と、検証情報領域に記憶された値と、が所定の対応関係を有する場合には、書換領域の書換えが完了していると判定し、所定の対応関係を有さない場合には、書換領域の書換えが完了していないと判定する、電子制御装置である。

【０００９】

本開示における電子制御装置において、消去部は、書換前の制御プログラム、固有認証子、および検証情報のうち、検証情報を初めに消去する。このため、消去部の処理が開始

50

されていれば、たとえ書換前の固有認証子が消去される前に書換領域の書換えが中断した場合でも、書換前の検証情報は消去されている。すなわち、固有認証子領域には書換前の固有認証子の値が記憶されており、検証情報領域には消去後の値が記憶されている。よって、固有認証子領域に記憶された値と、検証情報領域に記憶された値と、は所定の対応関係を有さない。そのため、判定部は、制御プログラムの書換えが完了していないと判定できる。

【0010】

さらに、検証部は、書込部が書込みを行った後に検証計算を行い、検証情報書込部は、該検証計算によって得られた検証情報を、検証情報領域へと書き込む。すなわち、書込部が書込みを行っている際に、検証情報書込部は動作しない。このため、制御プログラムおよび検証情報は同じ書換領域に記憶することができる。

10

【0011】

よって、電子制御装置は、書換領域とは別で制御プログラムの書換えの進行段階を書き込む領域を有さなくとも、書換えが完了しているか否かを判定できる。言い換えれば、記憶部は、書換えの進行段階を示す値だけを書き込むために、データの消去単位分の領域を有する必要がない。このため、本開示における電子制御装置は、記憶部のうち、書換領域以外の領域を、効率的に使用できる。

【図面の簡単な説明】

【0012】

【図1】第1実施形態における電子制御装置の構成を説明するブロック図である。

20

【図2】図1の電子制御装置による書換領域の書換処理を説明するフローチャートである。

【図3】図1の電子制御装置による検証計算処理を説明するフローチャートである。

【図4】図1の電子制御装置による起動時の書換完了判定処理を説明するフローチャートである。

【図5】第4実施形態における電子制御装置の構成を説明するブロック図である。

【図6】図5の電子制御装置による起動時の書換完了判定処理を説明するフローチャートである。

【図7】第5実施形態における電子制御装置による書換領域の書換処理を説明するフローチャートである。

【発明を実施するための形態】

30

【0013】

以下、本開示の複数の実施形態を図面に基づいて説明する。なお、各実施形態において対応する構成要素には同一の符号を付すことにより、重複する説明を省略する場合がある。各実施形態において構成の一部分のみを説明している場合、当該構成の他の部分については、先行して説明した他の実施形態の構成を適用することができる。また、各実施形態の説明において明示している構成の組み合わせばかりではなく、特に組み合わせに支障が生じなければ、明示していなくても複数の実施形態の構成同士を部分的に組み合わせることができる。そして、複数の実施形態および変形例に記述された構成同士の明示されていない組み合わせも、以下の説明によって開示されているものとする。

【0014】

40

(第1実施形態)

1. 電子制御装置1の構成

本実施形態における電子制御装置1の構成について、図1～図3を用いて説明する。本実施形態における電子制御装置1は、例えば、車両に搭載され、車両内の各種システムの制御を行う車載制御装置に適用することができる。各種システムは、エンジン、ハンドル、ブレーキ等の走行系システムなどがあげられる。また、各種システムは、メータ、パワーウィンドウ等のボデー系システムや、ナビゲーション装置などの情報系システムがあげられる。

【0015】

なお、電子制御装置1は、ECU (Electronic Control Unit)

50

とも称することができる。また、本開示は、車載制御装置に限定されず、車両とは異なる装置の制御を行うものであってもよい。

【0016】

電子制御装置1は、記憶部、演算部、RAM30(Random Access Memory)、電源40を有する。ここで、本実施形態において、記憶部とは、ROM10(Read Only Memory)に相当し、演算部とは、CPU50(Central Processing Unit)に相当する。よって以下においては、記憶部のことをROM10、演算部のことをCPU50、と記載する。

【0017】

図1に示すごとく、電子制御装置1は、書換ツール60と接続可能に構成されている。書換ツール60は、電子制御装置1が配置された車両の外部に設けられている。書換ツール60は、後ほど説明する、書換用の制御プログラム111を送信するための装置である。

【0018】

ROM10は、記憶されている情報を読み出すことができるメモリである。ROM10は、書換領域100と、リプログラムソフト領域200と、を有する。書換領域100には、ECUソフトが書き込まれている。ECUソフトは、電子制御装置1を動作させるソフトウェアである。リプログラムソフト領域200には、リプログラムソフトが書き込まれている。リプログラムソフトは、ECUソフトの書換え、すなわちリプログラミングを行うソフトウェアである。

【0019】

書換領域100は、プログラム領域101、固有認証子領域102、および検証情報領域103を有する。プログラム領域101には、制御プログラム111が書き込まれる。固有認証子領域102には、制御プログラム111の固有の認証子である固有認証子112が書き込まれる。検証情報領域103には、検証情報113が書き込まれる。ここで、制御プログラム111とは、電子制御装置1による車両内の各種システムの制御に必要なプログラムである。また、検証情報113は、制御プログラム111の書換えが完了したか否かを検証するための検証計算から得られる。検証情報113は、制御プログラム111の書換えが完了した場合には固有認証子112と所定の対応関係を有する。制御プログラム111の書換えの完了とは、制御プログラム111の書換えが、異常や改ざんなく終了することを示す。

【0020】

本実施形態における検証計算は、CBC(Cipher Block Chaining)モードと呼ばれる暗号利用モードを用いる。CBCモードは、制御プログラム111を分割して得られるM個(Mは2以上の整数)のブロックのうち、N番目(Nは1以上の整数、 $M \geq N$)のブロックについて暗号化された暗号文によってN+1番目のブロックを暗号化する、暗号利用モードである。

【0021】

固有認証子112とは、M番目、すなわち最後のブロックについて暗号化された暗号文である。ここで、上述したように、M番目のブロックは、M-1番目のブロックの暗号文を用いて暗号化される。すなわち、M番目のブロックについての暗号文は、それ以前のすべてのブロックに依存する。

【0022】

また、本実施形態において、検証情報113は、あらかじめ定められたL番目(Lは2以上の整数、 $M > L$)のブロックについて暗号化された暗号文である。以下において、L番目のブロックについて暗号化された暗号文は、L番目の暗号文113aと省略して記載する。

【0023】

リプログラムソフト領域200には、リプログラムソフトを構成するプログラムとして、書換機能220、起動制御機能230、認証機能240、通信機能250、および判定機能260が書き込まれている。書換機能220は、消去機能221、書込機能222、検証機能

10

20

30

40

50

２２３、および検証情報書込機能２２４を有する。判定機能２６０は、再検証機能２６１、一致判定機能２６２、および完了判定機能２６３を有する。

【００２４】

ＣＰＵ５０は、ＲＯＭ１０に記憶されているリプログラムソフトやＥＣＵソフトに含まれる各プログラムを読み出し、これらの各プログラムに従って、処理を実行する。また、ＣＰＵ５０は、処理結果を一時的にＲＡＭ３０に記憶しつつ、処理を実行する。これによって、リプログラムソフトを実行する際には、ＣＰＵ５０は、リプログラムソフトが有する各機能に基づいた処理を実行することになる。一方、ＥＣＵソフトを実行する際には、ＣＰＵ５０は、制御プログラム１１１に基づき、車両内の各種システムの制御を実行することになる。

【００２５】

ＲＡＭ３０は、処理結果の一例として、Ｎ＋１番目のブロックの暗号化に必要なＮ番目の暗号文が一時的に記憶される。Ｎ＋１番目のブロックの暗号化が終われば、Ｎ番目の暗号文はＮ＋１番目の暗号文に上書きされる。ただし、検証計算に用いるＬ番目の暗号文１１３ａは、検証計算が完了し、ＲＯＭ１０内の検証情報領域１０３に退避されるまで、Ｌ＋１番目の暗号文に上書きされることなくＲＡＭ３０に記憶されている。

【００２６】

電源４０は、電子制御装置１内の各部品に、電力を供給する。

【００２７】

２．電子制御装置１による演算処理

上述した構成を備えた電子制御装置１による、各種演算処理について、図２～図４を用いて説明する。

【００２８】

２．１．書換領域１００の書換処理

まず、図２を用いて、書換処理について説明する。

【００２９】

電子制御装置１は、車両の外部に配置された書換ツール６０から、信号を受信することで、書換処理を開始する。具体的には、ＣＰＵ５０が通信機能２５０を読み出し、実行する。これによって、ＣＰＵ５０は書換ツール６０と通信し、書換処理を開始する。書換処理は、書換領域１００の書換えを行う処理である。また、制御プログラム１１１の書換えを行う処理ともいえる。さらに、ＥＣＵソフトの書換えを行う処理ともいえる。

【００３０】

Ｓ１０は、認証部である。Ｓ１０では、ＣＰＵ５０が認証機能２４０を読み出し、実行する。つまり、ＣＰＵ５０は、通信対象の書換ツールが、正規の書換ツール６０であるか否かを認証する。これによって、ＣＰＵ５０は、非正規の書換ツールから送信されたプログラムで、制御プログラム１１１の書き換えを行うことを抑制できる。

【００３１】

Ｓ２０～Ｓ６０は書換部である。Ｓ２０～Ｓ６０では、ＣＰＵ５０が書換機能２２０を読み出し実行する。これによって、ＣＰＵ５０は、書換領域１００の書換を行う。書換部の処理について、具体的に説明する。

【００３２】

Ｓ２０は、消去部である。Ｓ２０では、ＣＰＵ５０が消去機能２２１を読み出し、実行する。これによって、ＣＰＵ５０は、ＲＯＭ１０の書換領域１００に記憶されている情報を消去単位ごとに、順番に消去する。この結果、ＲＯＭ１０は、プログラム領域１０１に書き込まれた書換前の制御プログラム１１１、固有認証子領域１０２に書き込まれた書換前の固有認証子１１２、および検証情報領域１０３に書き込まれた書換前の検証情報１１３が消去される。ここで、検証情報１１３は、制御プログラム１１１、固有認証子１１２、および検証情報１１３のうち初めに消去される。

【００３３】

Ｓ３０は、書込部である。Ｓ３０では、ＣＰＵ５０が書込機能２２２を読み出し、実行する。これによって、ＣＰＵ５０は、Ｓ２０で消去が行われたプログラム領域１０１に対

10

20

30

40

50

して、書換用の制御プログラム 111 を書き込む。また、CPU 50 は、S 20 で消去が行われた固有認証子領域 102 に対して、書換用の固有認証子 112 を書き込む。

【0034】

S 40 および S 50 は検証部である。S 40 では、CPU 50 が検証機能 223 を読み出し、実行する。これによって、CPU 50 は、検証計算を行う。S 40 の検証計算に関しては、後ほど詳しく説明する。

【0035】

S 50 では、CPU 50 が検証機能 223 を読み出し、実行する。これによって、書換領域 100 の書換えが完了したか否かを検証する。具体的には、CPU 50 は、固有認証子 112 の値と、検証計算の結果である検証認証子 113 b の値と、を比較する。CPU 50 は、これらの値が一致するか否かによって、書換えが完了したか否かを検証する。固有認証子 112 の値と検証認証子 113 b の値とが一致した場合は、S 60 へと移行する。固有認証子 112 の値と検証認証子 113 b の値とが一致しなかった場合は、S 70 へと移行する。

【0036】

S 60 は、検証情報書込部である。S 60 では、CPU 50 が検証情報書込機能 224 を読み出し、実行する。これによって、CPU 50 は、RAM 30 に記憶された L 番目の暗号文 113 a を、検証情報 113 として検証情報領域 103 に書き込む。ここで、L 番目の暗号文 113 a は、制御プログラム 111、固有認証子 112、L 番目の暗号文 113 a のうち初めに消去されるよう、書換領域 100 に配置される。CPU 50 は、L 番目の暗号文 113 a を検証情報領域 103 に書き込むと、書換処理を終了する。

【0037】

S 70 では、CPU 50 は、書換処理が異常終了したものとみなし書換ツール 60 に失敗を通知して、書換処理を終了する。なお、CPU 50 は、書換ツール 60 から参照可能なように、異常フラグを立てて、書換処理を終了してもよい。

【0038】

ここで、S 40 の検証計算処理について、図 3 を用いて説明する。前述の通り、本実施形態における電子制御装置 1 は、検証計算に CBC モードを用いている。CPU 50 は、検証機能 223 を読み出すことで検証計算を開始する。S 200 は、1 番目のブロックから処理を開始することを示す。

【0039】

S 210 では、CPU 50 は、ブロック番号 N が総ブロック数 M 以下であれば、S 220 に移行し、そうでなければ検証計算を終了する。

【0040】

S 220 では、CPU 50 は、 $N \geq 2$ の場合は、 $N - 1$ 番目の暗号文を用いて、N 番目のブロックの暗号化を行う。また、CPU 50 は、 $N = 1$ の場合は、暗号文の代わりに初期化ベクトルを用いて、N 番目のブロックの暗号化を行う。

【0041】

S 230 では、CPU 50 は、検証計算の対象を $N + 1$ 番目のブロックへと移行する。CPU 50 は、 $N > M$ となるまで、S 210 ~ S 230 の処理を繰り返す。 $N > M$ となると、CPU 50 は、検証計算処理を終了する。ここで、 $N = M$ となったとき、すなわち、検証計算が正常に完了した場合、S 220 で最後に演算された M 番目のブロックについての暗号文が、検証計算の結果である検証認証子 113 b となる。

【0042】

2. 2. 起動時の書換完了判定処理

次に、図 4 を用いて、書換完了判定処理について説明する。電子制御装置 1 は、起動時に、図 4 に示すフローチャートを開始する。書換完了判定処理は、書換領域 100 の書換えが完了しているかを判定する処理である。また、書換完了判定処理は、制御プログラム 111 の書換えが完了しているかを判定する処理ともいえる。さらに、書換完了判定処理は、制御プログラム 111 が、正常に実行可能な状態であるかを判定する処理ともいえる。

10

20

30

40

50

【0043】

S100～S120は、判定部である。S100～S120では、CPU50が判定機能260を読み出し、実行する。これによって、CPU50は、固有認証子領域102に記憶された値と、検証情報領域103に記憶された値と、を比較する。CPU50は、前述した2つの値が所定の対応関係を有する場合、書換領域100の書換えが完了していると判定する。また、CPU50は、前述した2つの値が所定の対応関係を有さない場合、書換えが完了していないと判定する。判定部における各処理について具体的に説明する。

【0044】

S100は再検証部である。S100では、CPU50が再検証機能261を読み出し、実行する。これによって、CPU50は、検証情報領域103に記憶された値を用いて、再度、上述した検証計算を行う。本実施形態においては、L番目の暗号文113aが検証情報113として、検証情報領域103に記憶されている。よってS100では、CPU50はL番目の暗号文113aをもとに、L+1番目からM番目のブロックについて暗号化を行う。CPU50は、この検証計算の結果であるM番目の暗号文を、再検証認証子として演算する。つまり、CPU50は、1番目からM番目のブロックについての暗号化を再度行うことはしない。CPU50は、L+1番目からM番目のブロックについて暗号化を行うことで、1番目からM番目のブロックについて暗号化を行う。

10

【0045】

S110は一致判定部である。S110では、CPU50が一致判定機能262を読み出し、実行する。これによって、CPU50は、固有認証子領域102に記憶された値と、検証情報領域103に記憶された値と、が所定の対応関係を有するか否かを判定する。ここで、本実施形態において、所定の対応関係とは、固有認証子領域102に記憶された固有認証子112の値と、検証情報領域103に記憶されたL番目の暗号文113aをもとに演算された再検証認証子の値と、が一致する関係を示す。

20

【0046】

ここで、固有認証子112の値と再検証認証子の値とが一致関係を有する場合とは、以下の状態を示す。すなわち、制御プログラム111の書換えが正常に完了している。その上で、書換えから起動までの間に、制御プログラム111が故障していない状態である。

【0047】

一方、固有認証子112の値と再検証認証子の値とが一致関係を有さない場合とは、以下の状態を示す。1つは、上述した書換処理が完了していないため、検証情報領域103にL番目の暗号文113aが記憶されていない状態である。もう1つは、書換処理は完了しているが、完了から起動時の書換完了判定までの間に、制御プログラム111のうち、L+1番目以降のブロックが、故障してしまった状態である。言い換えれば、書換後の制御プログラム111が故障し、異常を有する状態である。

30

【0048】

固有認証子112の値と再検証認証子の値とが一致関係を有する場合、CPU50は、S120へと移行する。CPU50は、一致関係を有する場合、書換領域100の書換えが完了していると判定して、S120へ進むともいえる。一方、一致関係を有さない場合、CPU50は、S130へと移行する。CPU50は、一致関係を有さない場合、書換領域100の書換えが完了していないと判定して、S130へ進むともいえる。なお、一致関係を有さない場合は、制御プログラム111の書換え途中や、制御プログラム111が壊れているとみなすことができる。

40

【0049】

S120は、起動制御部である。S120では、CPU50が起動制御機能230を読み出し実行する。つまり、CPU50は、書換後の制御プログラム111を実行する。CPU50は、制御プログラム111を実行することで、車両内の各種システムの制御を行う。

【0050】

一方、S130では、CPU50は、起動制御機能230および書換機能220を読み

50

出し実行する。つまり、CPU50は、リプログラムソフトを起動する。CPU50は、書換えが完了していない書換領域100に対し、前述した書換処理を再度行う。また、CPU50は、リプログラムソフトを起動して、書換ツール60からの書換え指示を待つともいえる。

【0051】

なお、本開示は、S110でNO判定の場合、S130と異なる処理を行ってもよい。例えば、電子制御装置1は、自らをリセットしてもよいし、そのほかの異常系の処理を行ってもよい。

【0052】

本実施形態における電子制御装置1の効果について説明する。

【0053】

S20では、CPU50は、書換前の制御プログラム111、固有認証子112、および検証情報113のうち、検証情報113を初めに消去する。このため、S20での処理が開始されていれば、たとえ書換前の固有認証子112が消去される前に書換領域100の書換えが中断した場合でも、書換前の検証情報113は消去されている。すなわち、固有認証子領域102には書換前の固有認証子112の値が記憶されており、検証情報領域103には消去後の値が記憶されている。よって、固有認証子領域102に記憶された値と、検証情報領域103に記憶された値と、は所定の対応関係を有さない。このため、CPU50は、制御プログラム111の書換えが完了していないと判定できる。

【0054】

さらに、CPU50は、S30で書換用の制御プログラム111および固有認証子112の書込みを行う。その後、CPU50は、S50で、書換えが完了したか否かを検証するための検証計算を行う。また、S60では、CPU50は、該検証計算によって得られた検証情報113を、検証情報領域103へと書き込む。すなわち、書換用の制御プログラム111、および固有認証子112の書込みが行われている際には、検証情報113は書き込まれない。このため、電子制御装置1は、制御プログラム111および検証情報113を同じ書換領域100に記憶することができる。

【0055】

よって、電子制御装置1は、制御プログラム111の書換の進行段階を書き込む領域を、書換領域100とは別で有さなくとも、書換えが完了しているか否かを判定できる。言い換えれば、ROM10は、書換の進行段階を示す値だけを書き込むために、データの消去単位分の領域を有する必要がない。このため、電子制御装置1は、ROM10のうち、書換領域100以外の領域を、効率的に使用できる。

【0056】

また、S110において一致関係を有すると判定された場合、S120では、CPU50は、制御プログラム111を起動する。一方、一致関係を有しないと判定された場合、S130では、上述した書換処理を再度行う。このため、電子制御装置1は、書換えが完了していない、不完全な制御プログラム111が起動することを防止できる。すなわち、電子制御装置1は、不完全な制御プログラム111の起動により誤作動がおこることを防止できる。

【0057】

また、本実施形態においては、S100では、CPU50は、検証情報113としてL番目の暗号文113aを用いる。具体的には、S100では、CPU50は、L番目の暗号文113aを用いて検証計算を再度行い、再検証認証子を演算する。よって、CPU50は、起動時の書換完了判定において、制御プログラム111のうち、1番目のブロックから検証計算を行う必要がない。すなわち、電子制御装置1は、起動時の書換完了判定にかかる時間を抑制できる。

【0058】

また、CPU50は、起動時にL+1番目以降のブロックについて再度検証計算を行う。このため、制御プログラム111のうちL+1番目以降のブロックが、宇宙線や改ざんといった要因によって故障した場合に、判定部は制御プログラム111の書換えが完了し

10

20

30

40

50

ていないと判定することができる。言い換えれば、判定部、書換処理から起動時の書換完了判定処理までの間に、 $L + 1$ 番目以降のブロックが故障した場合でも、この故障を検出できるともいえる。よって、電子制御装置 1 は、異常を有する制御プログラム 1 1 1 が起動することを抑制できる。

【0059】

(第2実施形態)

本実施形態における電子制御装置 1 について説明する。第1実施形態と同様の構成、処理、作用、効果、については、説明を省略する。

【0060】

本実施形態は、ブロック番号 L の定義が第1実施形態と異なる。本実施形態においては、ブロック番号 L とは、2 以上の整数、かつ $M \geq L$ であるとともに、 M が偶数の場合、 $L \leq M/2$ であり、 M が奇数の場合、 $L \leq (M + 1)/2$ である。

【0061】

本実施形態における、電子制御装置 1 の効果を説明する。電子制御装置 1 の起動時、 $S100$ において、 $CPU50$ は、 M が偶数の場合、 $L \leq M/2$ である L 番目の暗号文 1 1 3 a を用いて再度検証計算を行う。一方、 M が奇数の場合、 $S100$ において、 $CPU50$ は、 $L \leq (M + 1)/2$ である、 L 番目の暗号文 1 1 3 a を用いて再度検証計算を行う。すなわち、 $CPU50$ は、 M 個のブロックのうち、前半に位置するブロックの暗号文を用いて検証計算を行う。この結果、 $CPU50$ は、再検証認証子の演算に際して、後半に位置するブロックの暗号化を必ず行う。よって、 M 個のうち後半に位置するブロックの暗号文を用いて検証計算を行う場合と比べ、起動時に検証計算が行われるブロック数は多い。このため、書換処理から起動時の書換完了判定処理までの間に起こる制御プログラム 1 1 1 の故障について、前半に位置するブロックの暗号文を用いたほうが、故障の検出確率は高くなる。このため、電子制御装置 1 は、異常を有する制御プログラム 1 1 1 が起動することをより一層抑制できる

【0062】

(第3実施形態)

本実施形態における電子制御装置 1 について説明する。第1実施形態と同様の構成、処理、作用、効果、については、説明を省略する。

【0063】

本実施形態は、ブロック番号 L の定義が第1実施形態と異なる。本実施形態においては、ブロック番号 L とは、2 以上の整数、かつ $M \geq L$ であるとともに、 M が偶数の場合、 $L > M/2$ であり、 M が奇数の場合、 $L > (M + 1)/2$ である。

【0064】

本実施形態における電子制御装置 1 の効果を説明する。電子制御装置 1 の起動時、 $S100$ において、 $CPU50$ は、 M が偶数の場合、 $L > M/2$ である L 番目の暗号文 1 1 3 a を用いて再度検証計算を行う。一方、 M が奇数の場合、 $CPU50$ は、 $L > (M + 1)/2$ である L 番目の暗号文 1 1 3 a を用いて再度検証計算を行う。すなわち、 $CPU50$ は、 M 個のうち後半に位置するブロックの暗号文を用いて検証計算を行う。よって、 M 個のうち前半に位置するブロックの暗号文を用いて検証計算を行う場合と比べ、電子制御装置 1 の起動時、 $S100$ において検証計算が行われるブロック数は少ない。言い換えれば、 $S100$ において、 $CPU50$ が行う計算量はより少ない。このため、電子制御装置 1 は、起動時の書換完了判定処理にかかる時間を短縮できる。

【0065】

(第4実施形態)

本実施形態における電子制御装置 1 について、図5、および図6を用いて説明する。第1実施形態と同様の構成、処理、作用、効果、については、説明を省略する。なお、図6は、 $S100$ を有しない点が図4と異なる。

【0066】

本実施形態は、検証情報 1 1 3 が第1実施形態と異なる。本実施形態では、図5に示す

ごとく、検証認証子 1 1 3 b を検証情報 1 1 3 として用いる。また、検証認証子 1 1 3 b を用いるため、CPU 5 0 は、電子制御装置 1 の起動時の書換完了判定処理において、再検証機能 2 6 1 を読み出して、再検証認証子を演算する必要がない。すなわち、リプログラムソフトは、再検証機能 2 6 1 を有さない。

【0 0 6 7】

書換完了判定処理について、図 6 を用いて説明する。S 1 1 0 は一致判定部である。S 1 1 0 では、CPU 5 0 が一致判定機能 2 6 2 を読み出し、実行する。これによって、CPU 5 0 は、固有認証子領域 1 0 2 に記憶された値と、検証情報領域 1 0 3 に記憶された値と、が所定の対応関係を有するか否かを判定する。ここで、本実施形態において、所定の対応関係とは、固有認証子領域 1 0 2 に記憶された固有認証子 1 1 2 の値と、検証情報領域 1 0 3 に記憶された検証認証子 1 1 3 b の値と、が一致する関係を示す。

10

【0 0 6 8】

CPU 5 0 は、固有認証子 1 1 2 の値と検証認証子 1 1 3 b の値とが一致するか否かを判定する。一致関係を有する場合、CPU 5 0 は、S 1 2 0 へと移行する。また、一致関係を有さない場合、CPU 5 0 は、S 1 3 0 へと移行する。

【0 0 6 9】

本実施形態における電子制御装置 1 の効果について説明する。電子制御装置 1 の起動時、S 1 0 0 では、CPU 5 0 は、固有認証子 1 1 2 の値と検証認証子 1 1 3 b の値とが一致すれば、書換領域 1 0 0 の書換えが完了していると判定する。すなわち、CPU 5 0 は、起動時の書換完了判定において、再度検証計算を行う必要がない。よって、電子制御装置 1 は、起動時の書換完了判定にかかる時間を短縮することができる。

20

【0 0 7 0】

(第 5 実施形態)

本実施形態における電子制御装置 1 について図 7 を用いて説明する。第 1 実施形態と同様の構成、処理、作用、効果、については、説明を省略する。

【0 0 7 1】

本実施形態は、検証情報 1 1 3 として用いる暗号文のブロック番号 L の決め方が第 1 実施形態と異なる。本実施形態では、ブロック番号 L とは、書換ツール 6 0 から指定された値である。

【0 0 7 2】

次に、図 7 を用いて電子制御装置 1 の書換処理について説明する。電子制御装置 1 は、書換ツール 6 0 から、書換用の制御プログラム 1 1 1、該制御プログラム 1 1 1 の固有認証子 1 1 2、およびブロック番号 L を受信することで、書換処理を開始する。

30

【0 0 7 3】

S 1 0 は、認証部である。S 1 0 では、CPU 5 0 が認証機能 2 4 0 を読み出し、実行する。つまり、CPU 5 0 は、通信対象の書換ツールが、正規の書換ツール 6 0 であるか否かを認証する。なお、本実施形態では、ステップ S 6 0 において、検証情報に加えて、ブロック番号 L を記憶しておく。この場合、CPU 5 0 は、ステップ S 1 0 0 の前にブロック番号 L を読み出す。CPU 5 0 は、ブロック番号 L を読み出した後にステップ S 1 0 0 を実行する。

40

【0 0 7 4】

本実施形態において、ブロック番号 L とは、書換ツール 6 0 から指定された値である。言い換えれば、電子制御装置 1 は、書換ツール 6 0 の指定によって、検証情報 1 1 3 として用いる暗号文のブロック番号を変更できる。このため、電子制御装置 1 は、書換用の制御プログラム 1 1 1 に合わせて、検証情報 1 1 3 として用いる暗号文について、何番目のブロックを用いるかを変更できる。

【0 0 7 5】

よって、例えば制御プログラム 1 1 1 の容量が大きい場合、S 1 0 0 において、CPU 5 0 は、後半に位置するブロックの暗号文を検証情報 1 1 3 として用いて演算を行う。この結果、起動時の書換完了判定処理にかかる時間を短くすることができる。このように、

50

電子制御装置 1 は、制御プログラム 1 1 1 の容量等の性質に合わせて、CPU 5 0 が行う検証計算の計算量を少なくする、といった検証計算の計算量の調整が可能となる

【0 0 7 6】

(他の実施形態)

以上、本開示の実施形態を説明したが、本開示は上述の実施形態に限定されるものではなく、次の実施形態も本開示の技術的範囲に含まれ、さらに、下記以外にも要旨を逸脱しない範囲内で種々変更して実施することができる。

【0 0 7 7】

第 1 実施形態において、検証情報 1 1 3 は、制御プログラム 1 1 1、固有認証子 1 1 2、検証情報 1 1 3 のうち初めに消去されるよう、書換領域 1 0 0 に配置されているが、本開示はこれに限るものではない。検証情報 1 1 3 の一部が、CPU 5 0 に初めに消去されるよう、書換領域 1 0 0 に配置されていればよい。

【符号の説明】

【0 0 7 8】

電子制御装置… 1

1 0 記憶部、 1 0 0 書換領域、 1 0 1 プログラム領域、 1 0 2 固有認証子領域、 1 0 3 検証情報領域、 1 1 1 制御プログラム、 1 1 2 固有認証子、 1 1 3 検証情報、 1 1 3 a L 番目のブロックについての暗号文、 1 1 3 b 検証認証子、 5 0 演算部、 6 0 書換ツール

10

20

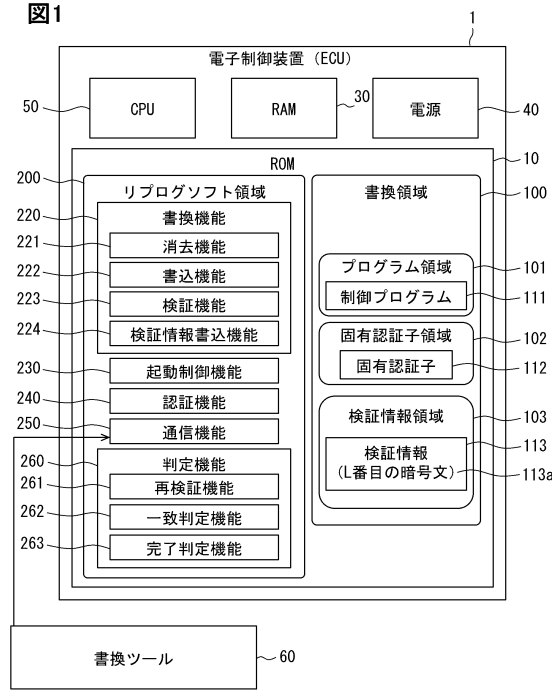
30

40

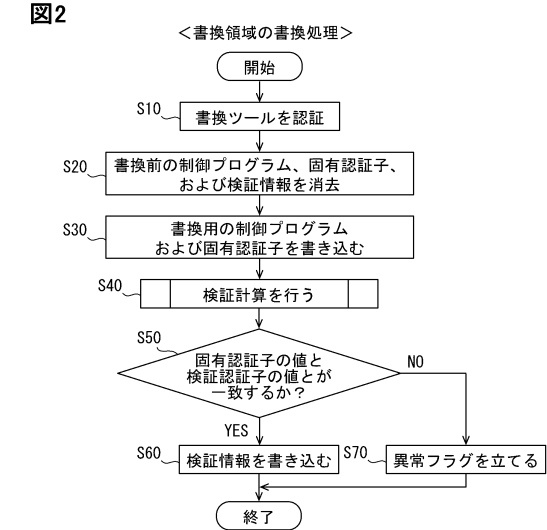
50

【図面】

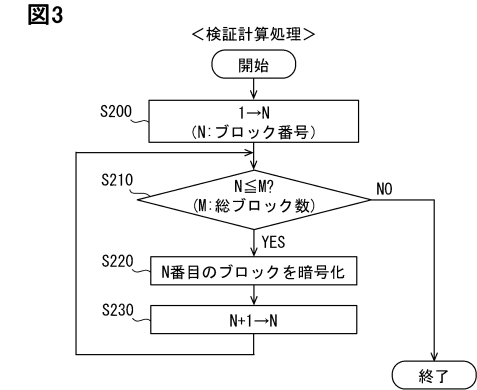
【図 1】



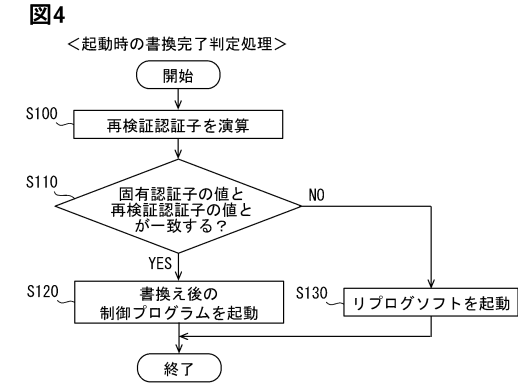
【図 2】



【図 3】



【図 4】



10

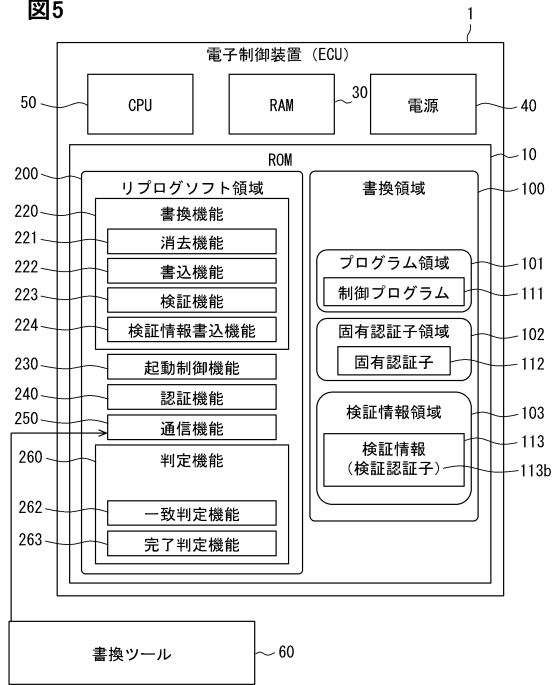
20

30

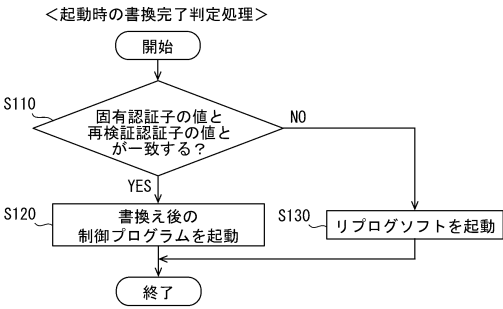
40

50

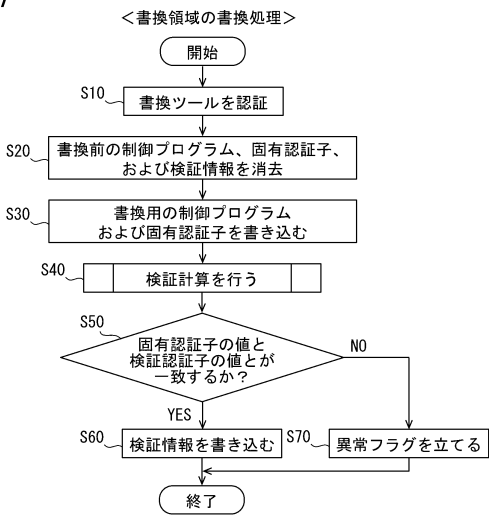
【図 5】
図5



【図 6】
図6



【図 7】
図7



フロントページの続き

- (56)参考文献 特開 2 0 0 4 - 3 1 0 2 1 6 (J P , A)
国際公開第 2 0 1 5 / 0 6 8 2 2 0 (W O , A 1)
特開 2 0 0 8 - 1 1 7 4 0 4 (J P , A)
- (58)調査した分野 (Int.Cl., D B 名)
- | | |
|---------|-----------|
| G 0 6 F | 8 / 6 5 4 |
| G 0 6 F | 2 1 / 6 4 |
| G 0 6 F | 2 1 / 4 4 |
| G 0 9 C | 1 / 0 0 |