

(12) 特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2015 年 4 月 2 日(02.04.2015)



(10) 国際公開番号
WO 2015/045507 A1

- (51) 国際特許分類:
B60R 16/02 (2006.01) **G06F 21/62** (2013.01)
- (21) 国際出願番号: PCT/JP2014/065838
- (22) 国際出願日: 2014 年 6 月 16 日(16.06.2014)
- (25) 国際出願の言語: 日本語
- (26) 国際公開の言語: 日本語
- (30) 優先権データ:
特願 2013-202960 2013 年 9 月 30 日(30.09.2013) JP
- (71) 出願人: 日立オートモティブシステムズ株式会社 (HITACHI AUTOMOTIVE SYSTEMS, LTD.) [JP/JP]; 〒3128503 茨城県ひたちなか市高場 2 5 2 0 番地 Ibaraki (JP).
- (72) 発明者: 月舘 統宙 (TSUKIDATE Tsunamichi); 〒1008280 東京都千代田区丸の内一丁目 6 番 6 号 株式会社日立製作所内 Tokyo (JP). 成沢 文雄 (NARISAWA Fumio); 〒1008280 東京都千代田区丸

の内一丁目 6 番 6 号 株式会社日立製作所内 Tokyo (JP). 石郷岡 祐 (ISHIGOOKA Tasuku); 〒1008280 東京都千代田区丸の内一丁目 6 番 6 号 株式会社日立製作所内 Tokyo (JP). 蛭名 朋仁 (EBINA Tomohito); 〒3128503 茨城県ひたちなか市高場 2 5 2 0 番地 日立オートモティブシステムズ株式会社内 Ibaraki (JP). 川津 昌義 (KAWATSU Masayoshi); 〒3128503 茨城県ひたちなか市高場 2 5 2 0 番地 日立オートモティブシステムズ株式会社内 Ibaraki (JP).

- (74) 代理人: 井上 学, 外 (INOUE Manabu et al.); 〒1008220 東京都千代田区丸の内一丁目 6 番 1 号 株式会社日立製作所内 Tokyo (JP).
- (81) 指定国 (表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS,

[続葉有]

(54) Title: VEHICULAR CONTROL DEVICE

(54) 発明の名称: 車両用制御装置

【図8】

プログラム No.	ソフトウェア名	安全度水準	動作モード	プログラム切替ID	
1	AA QMアプリ1	QM	非特権 FFモード	3	アクセス 権限 HH
2	BB ASIL アプリ1	ASIL	非特権 FFモード	2	動作 モード II
3	CC ASIL OS	ASIL	特権モード	GG 1	動作 モード II
4	DD QM アプリ2	QM	非特権 FFモード	3	アクセス 権限 HH
5	EE ASIL アプリ2	ASIL	非特権 FFモード	2	アクセス 権限 HH
6	EE QM アプリ3	QM	非特権 FFモード	3	アクセス 権限 HH

1220061... PROGRAM NO.
1220062... SOFTWARE NAME
1220063... SAFETY LEVEL
1220064, II... OPERATION MODE
1220065... PROGRAM SWITCH ID
AA... FIRST QM APPLICATION
BB... FIRST ASIL APPLICATION
CC... SECOND QM APPLICATION
DD... SECOND ASIL APPLICATION
EE... THIRD QM APPLICATION
FF... NON-PRIVILEGE MODE
GG... PRIVILEGE MODE
HH... ACCESS RIGHT

(57) Abstract: The purpose of the present invention is to provide a vehicular control device capable of ensuring safety while suppressing process load even when a plurality of software with different safety levels are operated. The present invention is characterized by being provided with: a storage unit; a software control unit that controls operation of a plurality of software stored in the storage unit; an operation mode switch unit that switches operation mode of the software control unit between a privilege mode and a non-privilege mode; and an access right switch unit that switches access right of each software with respect to the storage unit.

(57) 要約: 本発明は、安全度水準の異なる複数のソフトウェアを動作させる場合であっても、処理負荷を抑えつつ安全性を確保することができる車両用制御装置を提供することを目的とする。本発明は、記憶部と、該記憶部に記憶される複数のソフトウェアの動作を制御するソフトウェア制御部と、前記ソフトウェア制御部の動作モードを特権モードと非特権モードとの間で切り換える動作モード切換部と、前記記憶部に対する前記各ソフトウェアのアクセス権限を切り換えるアクセス権限切換部とを備えることを特徴とする。



LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

パ (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

(84) 指定国 (表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), ユーロ
シア (AM, AZ, BY, KG, KZ, RU, TJ, TM), ヨーロッパ

添付公開書類:

— 国際調査報告 (条約第 21 条(3))

明 細 書

発明の名称：車両用制御装置

技術分野

[0001] 本発明は、車両用制御装置に関するものである。

背景技術

[0002] 近年の多くの車両制御システムは、電子化された車両制御機器を操作する ECU、すなわち電子制御装置 (Electronic Control Unit) と、複数の ECU 間の通信を可能にする車載 LAN (Local Area Network) から構成されている。

[0003] 車両制御システムは環境負荷の低減や安全要求に伴い、システムの高機能化、機能の分散化、複雑化が進んでいる。その結果、ECU のソフトウェアアーキテクチャの標準化、安全装置の電子制御化とその安全性確保の仕組みの重要性が増大している。

[0004] 例えば、カーメーカは分散させた機能毎に専用の ECU を用意するため、一つの車両制御システムに複数の ECU が混在する。標準化された車両制御装置のソフトウェアアーキテクチャを導入することで、仕様の異なる ECU を組合せて車両制御システムを構築することを容易にしている。AUTOSAR アーキテクチャでは、マイコンに依存する機能単位や、センサやアクチュエータの制御処理のアルゴリズム、設定パラメータ単位でモジュール化が行われているため、マイコンが変更となっても対象となるモジュールを修正するだけで、他のモジュールを修正することなく対応できる。

[0005] また、車両制御機器における安全装置の電子制御化にともない機能安全の仕組みが車両制御システムに導入されてきている。ここで、機能安全とはシステムに不具合が生じたときにシステムが安全側に遷移することで安全を確保する考えである。例えば自動車向け機能安全規格 ISO 26262 では、安全度水準である ASIL (Automotive Safety Integrity Level) が設けられている。

[0006] 一般的な車両制御システムは、コスト増加抑制や性能最適化の要求を満たすべく、さまざまな制御アプリケーションによって構成されており、さまざまな安全度水準のソフトウェアが混在することになる。機能安全規格 I S O 2 6 2 6 2 では安全要求が異なるソフトウェア間の干渉を防止することが求められている。具体的には、安全度水準の低い Q M のソフトウェアが暴走して、A S I L D 等の安全度水準の高いソフトウェアが格納されているメモリへアクセスし、データを破壊することを防ぐことである。従って、一般的な車両制御システムにおいて機能安全規格 I S O 2 6 2 6 2 に準拠するには、ソフトウェア間の干渉を防止する仕組みが必要となる。

[0007] このような仕組みの一例として、特許文献 1 では、安全度の異なるタスクを実行する場合には、ユーザモードとカーネルモードとの間で動作モードを切り換えることが提案されている。

先行技術文献

特許文献

[0008] 特許文献1：特開 2 0 1 2 - 2 4 7 9 7 8 号公報

発明の概要

発明が解決しようとする課題

[0009] しかし、上記従来技術では、安全度水準の異なるタスクを実行すべく動作モードを切り換える際に、負荷の大きい割り込み処理を行うものである。従って、上記従来技術では、安全性を確保できたとしても、オーバーヘッドが増加してしまうという問題がある。

[0010] そこで、本発明は、安全度水準の異なる複数のソフトウェアを動作させる場合であっても、処理負荷を抑えつつ安全性を確保することができる車両用制御装置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] 本発明は、記憶部と、該記憶部に記憶される複数のソフトウェアの動作を制御するソフトウェア制御部と、前記ソフトウェア制御部の動作モードを特

権モードと非特権モードとの間で切り換える動作モード切換部と、前記記憶部に対する前記各ソフトウェアのアクセス権限を切り換えるアクセス権限切換部とを備えることを特徴とする。

発明の効果

[0012] 本発明によれば、安全度水準の異なる複数のソフトウェアを動作させる場合であっても、処理負荷を抑えつつ安全性を確保することができる。

図面の簡単な説明

[0013] [図1]本発明の実施形態に係る車両用制御装置の構成図である。

[図2]車両用制御装置のメモリ保護領域アクセス権限設定管理テーブルの例を示す図である。

[図3]車両用制御装置のメモリ保護領域アクセス権限管理テーブルの例を示す図である。

[図4]車両用制御装置のメモリ保護領域活性状態管理テーブルの例を示す図である。

[図5]車両用制御装置のメモリ保護領域活性パターン管理テーブルの例を示す図である。

[図6]車両用制御装置の動作モード管理テーブルの例を示す図である。

[図7]車両用制御装置で動作するソフトウェアの安全度水準と動作モードの例を示す図である。

[図8]車両用制御装置のプログラム切換ID管理テーブルの例を示す図である。

[図9]車両用制御装置の前回プログラムID管理テーブルの例を示す図である。

[図10]車両用制御装置のテーブルサイズ管理テーブルの例を示す図である。

[図11]車両用制御装置の前回動作モードフラグ管理テーブルの例を示す図である。

[図12]車両用制御装置の割り込み処理用退避データ管理テーブルの例を示す図である。

[図13]車両用制御装置のソフトウェア制御部の例を示す図である。

[図14]車両用制御装置のMPU設定部の動作フローの例を示す図である。

[図15]車両用制御装置の動作モード切換部の動作フローの例を示す図である。

[図16]車両用制御装置のアクセス権限切換部の動作フローの例を示す図である。

[図17]車両用制御装置で動作するソフトウェアの安全度水準と動作モードの他の例を示す図である。

発明を実施するための形態

[0014] 図1は、本発明の実施形態に関わる車両用制御装置の構成図である。以下、車両用制御装置として、エンジンを制御する装置であるECU1を元に説明する。エンジン制御装置ECU1は演算装置(CPU)11、記憶部としてのメモリ12、入出力回路13、CANコントローラ14、スロットルセンサ15、ペダルセンサ16を備える。

[0015] 演算装置(CPU)11は、CPUコア111、メモリ保護装置(MPU)112からなる。CPUコア111は、メモリ12が記憶(格納)している複数のソフトウェア(本実施形態では「プログラム」と称することがある。)を実行するプロセッサ(Central Processing Unit)である。演算装置(CPU)11は、特権モード、非特権モードと呼ばれる動作モードを有しており、両動作モードは、割り込み処理によって切り換えることができる。なお、CPUコア111の数は1つとしているが、CPUコア111の数は複数でもかまわない。

[0016] メモリ保護装置(MPU)112は、主にメモリ12へのアクセス権限を管理する装置であり、ソフトウェアのアクセス権限を監視するアクセス権限違反監視部を備える。アクセス権限を管理するとは、メモリ12のアドレス空間に対し、任意の領域にアクセス権限を設定し、その設定を有効化、無効化することである。さらにメモリ12に対するアクセスを監視し、アクセスに異常(即ち、違反)があればCPUコア111の処理を無効又は中止して

、処理結果が反映されないようにする。同等の機能を、回路デバイスなどのハードウェアを用いて構成することもできる。また、メモリ保護装置（MPU）１１２は、メモリ１２を分割して複数の記憶領域を設定する記憶領域設定部を備えている。後述するメモリ保護領域は、この記憶領域設定部により設定される領域である。

[0017] メモリ１２はプログラム領域１２１とデータ記憶領域１２２を有する。プログラム領域１２１は、ソフトウェア制御部１１２１、アクセス権限切換部１２１２、動作モード切換部１２１３、MPU設定部１２１４を格納する。データ記憶領域１２２は後述の図２で説明するメモリアクセス権限管理テーブル１２２００１０、図３で説明するメモリ保護領域アクセス権限管理テーブル１２２００２１、図４で説明するメモリ保護領域活性状態管理テーブル１２２００３０、図５で説明するメモリ保護領域活性パターン管理テーブル１２２００４０、図６で説明する動作モード管理テーブル１２２００５０、図８で説明するプログラム切換ＩＤ管理テーブル１２２００６０、図９で説明する前回プログラムＩＤ管理テーブル１２２００７０、図１０で説明するテーブルサイズ管理テーブル１２２００８０、図１１で説明する前回動作モードフラグ管理テーブル１２２００９０、図１２で説明する割り込み処理用退避データ管理テーブル１２２００１００を格納する。

[0018] 本実施形態では、エンジン制御ＥＣＵ１の構成を機能安全規格ＩＳＯ２６２６２対応のＥＣＵアーキテクチャとしているが構成はこれに限らない。例えば、データを保存するための不揮発性メモリ（バックアップラム）や水温センサなどを備えてもよい。

[0019] エンジン制御装置１のデータ記憶領域１２２に格納されるテーブルを下記より説明する。

[0020] 図２は、メモリアクセス権限管理テーブル１２２００１０の例を示す図である。メモリアクセス権限管理テーブル１２２００１０は、MPUが管理する、メモリ１２に対するデフォルトのアクセス権限の設定情報を管理するテーブルであり、先頭アドレスフィールド１２２００１１、後尾アドレスフィ

ールド1220012、特権モード書き込みフィールド1220013、特権モード実行フィールド1220014、特権モード読み込みフィールド1220015、非特権モード書き込みフィールド1220016、非特権モード実行フィールド1220017、非特権モード読み出しフィールド1220018からなる。説明の都合上、本実施形態ではメモリ12に対するデフォルトのアクセス権限の設定情報を管理するためにメモリアクセス権限管理テーブル1220010を用いるが、これに限らない。

[0021] 先頭アドレスフィールド1220011は、メモリ保護ユニット(MPU)112が管理するメモリを示す先頭アドレスを保持する。後尾アドレスフィールド1220012は、メモリ保護ユニット(MPU)112が管理するメモリの後尾を示すアドレスを保持する。特権モード書き込みフィールド1220013は、演算装置(CPU)11が特権モード時に先頭アドレスと後尾アドレスによって指定された領域(以下、メモリ保護領域)に対し、書き込み可能か判断するための値を保持する。ここでは0か1の値を保持し、0の場合は書き込み不可とし、1の場合は書き込み可能とする。特権モード実行フィールド1220014は、演算装置(CPU)11が特権モード時にメモリ保護領域に対し、処理を実行可能か判断するための値を保持する。ここでは0か1の値を保持し、0の場合は処理の実行不可とし、1の場合は処理の実行可能とする。特権モード読み込みフィールド1220015は、演算装置(CPU)11が特権モード時にメモリ保護領域に対し、読み出し可能か判断するための値を保持する。ここでは0か1の値を保持し、0の場合は読み出し不可とし、1の場合は読み出し可能とする。非特権モード書き込みフィールド1220016は、演算装置(CPU)11が非特権モード時にメモリ保護領域に対し、書き込み可能か判断するための値を保持する。ここでは0か1の値を保持し、0の場合は書き込み不可とし、1の場合は書き込み可能とする。非特権モード実行フィールド1220017は、演算装置(CPU)11が非特権モード時にメモリ保護領域に対し、処理を実行可能か判断するための値を保持する。ここでは0か1の値を保持し、0の場

合は処理の実行不可とし、１の場合は処理の実行可能とする。非特権モード読み出しフィールド１２２００１８は、演算装置（ＣＰＵ）１１が非特権モード時にメモリ保護領域に対し、読み出し可能か判断するための値を保持する。ここでは０か１の値を保持し、０の場合は処理の実行不可とし、１の場合は処理の実行可能とする。ここで、メモリ領域１２のデフォルトのアクセス権限は、特権モードの書き込み、実行、読み出しは許可するが、非特権モードの書き込み、実行、読み出しは許可されない、としたがこれに限らない。例えば、特権モード、非特権モードにおいても書き込み、実行、読み出しを許可してもかまわない。

[0022] 図３は、メモリ保護領域アクセス権限管理テーブル１２２００２０の例を示す図である。メモリ保護領域アクセス権限設定管理テーブル１２２００２０は、ＭＰＵが管理する、メモリ１２に対するアクセス権限の設定情報を管理するテーブルであり、メモリ保護領域番号フィールド１２２００２１、先頭アドレスフィールド１２２００２２、後尾アドレスフィールド１２２００２３、特権モード書き込みフィールド１２２００２４、特権モード実行フィールド１２２００２５、特権モード読み込みフィールド１２２００２６、非特権モード書き込みフィールド書き込み１２２００２７、非特権モード実行フィールド１２２００２８、非特権モード読み出しフィールド１２２００２９からなる。説明の都合上、本実施形態ではメモリ１２に対するアクセス権限の設定情報を管理するためにメモリ保護領域アクセス権限管理テーブル１２２００２０を用いるが、これに限らない。

[0023] メモリ保護領域アクセス権限管理テーブル１２２００２０では、複数のメモリ保護領域１～４を有し、アクセス権限切換部は、各メモリ保護領域に対し、異なるアクセス権限を設定する。また、メモリ保護領域２，３は、実際には同じ領域であるが、アクセス権限切換部は、このメモリ保護領域２，３に対し、ソフトウェアの安全度に応じて異なるアクセス権限を設定する。

[0024] メモリ保護領域番号フィールド１２２００２１は、メモリ保護ユニット（ＭＰＵ）１２が管理するメモリ保護領域の領域番号を保持する。ここではメ

メモリ保護領域が設定可能な領域は合計4領域としているがこれに限らない。先頭アドレスフィールド1220022は、メモリ保護ユニット(MPU)112が管理するメモリ保護領域を示す先頭アドレスを保持する。後尾アドレスフィールド1220023は、メモリ保護ユニット(MPU)112が管理するメモリ保護領域の後尾を示すアドレスを保持する。特権モード書き込みフィールド1220024は、演算装置(CPU)11がメモリ保護領域に対し、書き込み可能か判断するための値を保持する。ここでは0か1の値を保持し、0の場合は書き込み不可とし、1の場合は書き込み可能とする。

[0025] 特権モード実行フィールド1220025、演算装置(CPU)11が特権モード時に先頭アドレスと後尾アドレスによって指定された領域に対し、処理を実行可能か判断するための値を保持する。ここでは0か1の値を保持し、0の場合は処理の実行不可とし、1の場合は処理の実行可能とする。

[0026] 特権モード読み出しフィールド1220026は、演算装置(CPU)11が特権モード時にメモリ領域に対し、読み出し可能か判断するための値を保持する。ここでは0か1の値を保持し、0の場合は読み出し不可とし、1の場合は読み出し可能とする。非特権モード書き込みフィールド1220027は、演算装置(CPU)11が非特権モード時にメモリ保護領域に対し、書き込み可能か判断するための値を保持する。ここでは0か1の値を保持し、0の場合は書き込み不可とし、1の場合は書き込み可能とする。非特権モード実行フィールド1220028は、演算装置(CPU)11が非特権モード時にメモリ保護領域に対し、処理を実行可能か判断するための値を保持する。ここでは0か1の値を保持し、0の場合は処理の実行不可とし、1の場合は処理の実行可能とする。非特権モード読み出しフィールド1220029は、演算装置(CPU)11が非特権モード時にメモリ保護領域に対し、読み出し可能か判断するための値を保持する。ここでは0か1の値を保持し、0の場合は処理の実行不可とし、1の場合は処理の実行可能とする。ここで、先頭アドレス220022と後尾アドレス220023によって範

囲指定されないメモリ12へのアクセス権限は、メモリアクセス権限管理テーブル1220010で設定されたデフォルトのアクセス権限に設定される。

[0027] 図4はメモリ保護領域活性状態管理テーブル1220030の例を示す図である。メモリ保護領域活性状態管理テーブル1220030は、メモリ保護ユニット(MPU)112がメモリ保護領域に設定したアクセス権限が有効か無効かを管理するためのテーブルであり、メモリ保護領域番号フィールド1220031、活性状態フィールド1220032からなる。

[0028] メモリ保護領域番号フィールド1220031は、メモリ保護ユニット(MPU)112が管理するメモリ保護領域の領域番号を保持する。ここではメモリ保護領域を4領域としているが、領域数はこれに限らない。

[0029] 活性状態フィールド1220032は、メモリ保護ユニット(MPU)112が管理するメモリ保護領域の活性状態の値を保持する。ここでは0か1の値を保持し、0の場合は該当するメモリ領域に設定されたアクセス権限の設定は無効となり、1の場合は該当するメモリ領域に設定されたアクセス権限の設定が有効となる。活性状態の値が0を保持した場合、該当するメモリ領域に設定されたアクセス権限は、メモリ保護領域アクセス権限管理テーブル1220010におけるデフォルトのアクセス権限である。

[0030] 図5はメモリ保護領域活性パターン管理テーブル1220040の例を示す図である。メモリ保護領域活性パターン管理テーブル1220040は、メモリ保護領域活性状態管理テーブル1220030の活性状態フィールド1220032に設定するメモリ保護領域の活性状態の設定パターンであり、メモリ保護領域番号フィールド1220041、活性パターン1フィールド1220042、活性パターン2フィールド1220043からなる。

[0031] この図5のメモリ保護領域活性パターン管理テーブル1220040にあるとおり、アクセス権限切換部は、複数のメモリ保護領域ごとに設定されるアクセス権限のパターンを活性パターン1及び活性パターン2として複数管理し、このパターンを切り換えることにより、複数のメモリ保護領域領域に

対する個別のアクセス権限を一括して切り換える。

[0032] メモリ保護領域番号フィールド1220041は、メモリ保護ユニット（MPU）112が管理するメモリ保護領域の領域番号を保持する。ここではメモリ保護領域を4領域としているが、領域数はこれに限らない。

[0033] 活性パターン1フィールド1220042は、メモリ保護領域活性状態管理テーブル1220030の活性状態フィールド1220032に設定するメモリ保護領域の活性状態の設定パターンの一つである。ここでは全メモリ領域に対して、活性状態を設定しているが、一部のメモリ領域に対してのみ活性状態を設定してもよい。活性パターン2フィールド1220043は、メモリ保護領域活性状態管理テーブル1220030の活性状態フィールド1220032に設定するメモリ保護領域の活性状態の設定パターンの一つである。ここでは全メモリ領域に対して、活性状態を設定しているが、一部のメモリ領域に対してのみ活性状態を設定してもよい。

[0034] 図6は動作モード管理テーブル1220050の例を示す図である。動作モード管理テーブル1220050は、演算装置（CPU）11の動作モードを管理するためのテーブルであり、動作モードフラグフィールド1220051からなる。

[0035] 動作モードフラグフィールド1220051は、演算装置（CPU）11の動作モードを示す値を保持する。ここでは0か1の値を保持し、0を保持するときは演算装置（CPU）11の動作モードは特権モード、1を保持するときは非特権モードを示す。

[0036] 本実施形態では、各ソフトウェアが一般的な安全度水準（ASIL、QM）による区分とは別に、動作モードによる分類によって区分されている。これを図7を用いて説明する。具体的には、各ソフトウェアは、特権モードで動作可能な特権モード動作ソフトウェア（ASIL OS）と、非特権モードで動作可能な非特権モード動作ソフトウェア（ASIL アプリ1～2、QM アプリ1～3）とに区分される。また、非特権モード動作ソフトウェアは、さらに安全度に応じて複数段階に区分されている。図7では、非特権モード

動作ソフトウェアのうち比較的安全度が高いＡＳＩＬアプリ１～２と、比較的安全度が低いＱＭアプリ１～３とに区分されている。

[0037] 安全度水準の区分に基づいて説明すると、同じＡＳＩＬであるソフトウェア（ＡＳＩＬＯＳと、ＡＳＩＬアプリ１～２）がさらに安全度に応じて複数段階に区分されており、安全度が比較的低い方のソフトウェア（ＡＳＩＬアプリ１～２）は、ＱＭアプリと同じ非特権モード動作ソフトウェアに分類されている。

[0038] これは、各ソフトウェアが安全度に応じていわば高・中・低の３段階に区分される状態とも言える。

[0039] このように、本実施形態では、ソフトウェアの分類分けが工夫されており、非特権モードで動作させるソフトウェアの範囲が、通常は特権モードで動作させることが想定される安全度水準ＡＳＩＬのソフトウェアの一部を含むように拡張されている。

[0040] そして、ソフトウェア制御部が動作させるソフトウェアを特権モード動作ソフトウェアと非特権モード動作ソフトウェアとの間で切り換える場合には、動作モード切換部が動作モードを切り換える。一方、ソフトウェア制御部が動作させるソフトウェアを同じ動作モードで動作するソフトウェア同士の間で切り換える場合には、アクセス権限切換部がソフトウェアの安全度に応じてアクセス権限を切り換える。

[0041] 図８はプログラム切換ＩＤ管理テーブル１２２００６０の例を示す図である。プログラム切換ＩＤ管理テーブル１２２００６０は、演算装置（ＣＰＵ）１１が実行するプログラムにおいて、ソフトウェア間のパーティショニングを実現するために割り当てるＩＤを管理するテーブルであり、プログラムＮｏ．フィールド１２２００６１、プログラム名フィールド１２２００６２、安全度水準フィールド１２２００６３、動作モードフィールド１２２００６４、プログラム切換フィールドＩＤ１２２００６５からなる。

[0042] プログラムＮｏ．フィールド１２２００６１は、エンジン制御ＥＣＵ１において実行されるソフトウェアに割り振られるナンバーである。

- [0043] プログラム名フィールド1220062は、エンジン制御ECU1において実行されるソフトウェアの名称である。
- [0044] 安全度水準フィールド1220063は、エンジン制御ECU1において実行されるソフトウェアに割り付けられた安全度水準である。ここで、安全度水準はASILとQMに大別され、QMが割り付けられたソフトウェアに比べASILが割り付けられたソフトウェアに対する安全度水準が高い。
- [0045] ところで、安全度水準は、ソフトウェアに異常が発生した場合にシステムに与える影響の大きさに基づいて設定されており、安全度水準が高いソフトウェアとは、動作の際に要求される安全度が高いことを意味する。
- [0046] 動作モードフィールド1220064は、該当するプログラム実行時に求められる演算装置(CPU)11の動作モードを示す。ここではOSや一部のアプリケーションに対し特権モードでの動作が割り当てられ、そのほかのアプリケーションは非特権モードで動作する。
- [0047] プログラム切換IDフィールド1220065は、前回動作したプログラムのプログラム切換IDを保持する。プログラム切換IDはASILレベルと、実行動作モードの組み合わせで一意に決定される。ここでは、ASILレベルがASIL、実行動作モードが特権モードのプログラムに対し1が割り付けられ、ASILレベルがASIL、実行動作モードが非特権モードのプログラムに対し2が割り付けられ、ASILレベルがQM、実行動作モードが非特権モードのプログラムに対し3が割り付けられるが、プログラム切換IDの設定はこれに限らない。
- [0048] 図9は前回プログラム切換ID管理テーブル1220070の例を示す図である。前回プログラム切換ID管理テーブル1220070は、前回プログラム切換IDフィールド1220071からなる。
- [0049] 前回プログラム切換IDフィールド1220071は、前回動作したプログラムのプログラム切換IDの値を保持する。
- [0050] 図10はテーブルサイズ管理テーブル1220080の例を示す図である。テーブルサイズ管理テーブル1220080は、名称フィールド1220

０８１、総数フィールド１２２００８２、プログラム個数フィールド１２２００８３、メモリ保護領域数フィールド１２２００８４からなる。

[0051] 名称フィールド１２２００８１は、テーブルサイズ管理テーブル１２２００８０で管理する対象の名称である。

[0052] 総数フィールド１２２００８２は、テーブルサイズ管理テーブル１２２００８０で管理する対象の総数を表す。

[0053] プログラム個数フィールド１２２００８３は、プログラム切替ＩＤ管理テーブル１２２００６０が管理するプログラムＩＤの最大数を示す。

[0054] メモリ保護領域数フィールド１２２００８４は、メモリ保護領域アクセス権限管理テーブル１２２００２０で管理するメモリ保護領域番号の最大数を示す。

[0055] 図１１は前回動作モードフラグ管理テーブル１２２００９０の例を示す図である。前回動作モードフラグ管理テーブル１２２００９０は、前回実行されたプログラムの演算装置（ＣＰＵ）１１の動作モードを示す値を管理するテーブルであり、前回動作モードフラグフィールド１２２００９１からなる。

[0056] 前回動作モードフラグフィールド１２２００９１は、前回実行されたプログラムの演算装置（ＣＰＵ）１１の動作モードを示す値を保持する。ここでは０か１の値を保持し、０を保持するときは前回プログラムが実行した際の演算装置（ＣＰＵ）１１の動作モードが特権モードであることを示し、１を保持するときは非特権モードを示す。

[0057] 図１２は割り込み処理用退避データ管理テーブル１２２０１００の例を示す図である。割り込み処理用退避データ管理テーブル１２２０１００は、ＯＳによる割り込み処理時に退避するデータを管理するテーブルであり、動作モードフィールド１２２０１０１、プログラムカウンタフィールド１２２０１０２からなる。

[0058] 動作モードフィールド１２２０１０１は、ＯＳの割り込み処理の直前の演算装置（ＣＰＵ）１１の動作モードを示す値を保持する。ここでは０か１

の値を保持し、0を保持するときは演算装置（CPU）11の動作モードは特権モード、1を保持するときは非特権モードを示す。

[0059] プログラムカウンタフィールド1220102は、演算装置（CPU）11がOSの割り込み処理の直前に実行したメモリのアドレスである。

[0060] 以上のテーブルが実施例1のエンジン制御ECU1の記憶領域122に格納される。

[0061] これよりエンジン制御ECU1のプログラム領域121に格納されているプログラムの動作フローについて説明する。

[0062] 図13はソフトウェア制御部1211の動作フローである。以下、図13の各ステップについて説明する。診断設定情報送信実行部1211は、iに0を代入する（S1211000）。診断設定情報確認用データ生成部1211は、iに1を加える（S1211001）。ソフトウェア制御部1211は、iがテーブルサイズ管理テーブル1220080で管理するプログラム個数の総数を超えているかを判定する（S1211002）。iがプログラム個数の総数を超えている場合には処理を終了し、超えていない場合はS1211003に進む。ソフトウェア制御部1211は、後述の図11で説明するMPU設定部1215を呼び（S1211003）。これにより実行するプログラムに応じた演算装置（CPU）11の動作モードの変更や、メモリ12に割り付けられたメモリ保護領域の活性状態を変更し、メモリ保護を実現する。ソフトウェア制御部1211は、プログラム切換ID管理テーブル1220060のiに該当するプログラムNo.のプログラムを実行し、ステップ1211001に進む（S1211004）。

[0063] 図14はMPU設定部1215の動作フローである。以下、図14の各ステップについて説明する。MPU設定部1215は、プログラム切換ID管理テーブル1220060からiと等しいプログラムNo.のプログラム切換IDを取得する（S1215000）。MPU設定部1215は、前回プログラム切換ID管理テーブル1220070から前回のプログラム切換IDを取得する（S1215001）。MPU設定部1215は、取得したプログラ

ム切換 I D と前回のプログラム切換 I D を比較し (S 1 2 1 5 0 0 2)、両者の値が等しい場合には、ステップ 1 2 1 5 0 0 6 に進み、異なる場合にはステップ 1 2 1 5 0 0 3 に進む。MP U 設定部 1 2 1 5 は、取得したプログラム切換 I D と前回のプログラム実行 I D のうち、どちらかのプログラム I D が 1 の場合には、S 1 2 1 5 0 0 4 に進み、異なる場合には S 1 2 1 5 0 0 5 に進む。MP U 設定部 1 2 1 5 は、後述の図 1 5 の動作モード切換部 1 2 1 3 を呼び、演算装置 (C P U) の動作モードを切り換える (S 1 2 1 5 0 0 4)。MP U 設定部 1 2 1 5 は、後述の図 1 3 のアクセス権限切換部 1 2 1 2 を呼び、メモリ領域の活性状態を変更し、メモリ 1 2 へのアクセス権限を切り換える (S 1 2 1 5 0 0 5)。MP U 設定部 1 2 1 5 は、前回プログラム切換 I D 管理テーブル 1 2 2 0 0 7 0 の前回のプログラム I D を今回のプログラム I D で更新し (S 1 2 1 5 0 0 6)、処理を終了する。

[0064] 図 1 5 は動作モード切換部 1 2 1 3 の動作フローである。以下、図 1 5 の各ステップについて説明する。動作モード切換部 1 2 1 3 は、動作モードフラグ管理テーブル 1 2 2 0 0 5 0 から演算装置 (C P U) 1 1 の動作モードフラグを取得する (S 1 2 1 3 0 0 0)。動作モード切換部 1 2 1 3 は、O S の割り込み処理を実施し、現在のプログラムカウンタと動作モードフラグを割り込み処理用退避データ管理テーブル 1 2 2 0 1 0 0 に退避させる (S 1 2 1 3 0 0 1)。動作モード切換部 1 2 1 3 は、割り込み処理用退避データ管理テーブル 1 2 2 0 1 0 0 から動作モードフラグを取得する (S 1 2 1 3 0 0 2)。動作モード切換部 1 2 1 3 は、取得した動作モードフラグの値を反転し、割り込み処理用退避データ管理テーブル 1 2 2 0 1 0 0 の動作モードフラグを反転した値で更新する (S 1 2 1 3 0 0 3)。動作モード切換部 1 2 1 3 は、O S による割り込み処理を終了し、割り込み処理用退避データ管理テーブル 1 2 2 0 1 0 0 から退避した動作モードフラグとプログラムカウンタを取得し (S 1 2 1 3 0 0 4)、プログラムカウンタ、動作モードフラグを更新し処理を終了する。

[0065] 図 1 6 はアクセス権限切換部 1 2 1 2 の動作フローである。以下、図 1 6

の各ステップについて説明する。アクセス権限切換部1212は、プログラム切換ID管理テーブル1220060からiに該当するプログラムNo.のプログラム切換IDを取得する(S1212000)。アクセス権限切換部1212は、前回プログラム切換ID管理テーブル1220070から前回プログラム切換IDを取得する(S1212001)。アクセス権限切換部1212は、jに0を代入する(S1212002)。アクセス権限切換部1212は、取得したプログラムIDと前回プログラムIDの組み合わせを比較し(S1212003)、組み合わせが(1, 3)または(3, 1)であればステップ1212004に、異なる場合はステップ1212007に進む。S1212003でYesの場合、アクセス権限切換部1212は、jに1を加える(S1212004)。アクセス権限切換部1212は、メモリ保護領域活性状態管理テーブル1220030のjと同じメモリ保護領域番号の活性状態を、メモリ保護領域活性パターン管理テーブル1220040のjと同じメモリ保護領域番号の活性パターン2の値に設定する(S1212005)。アクセス権限切換部1212は、テーブルサイズ管理テーブル1220080のメモリ保護領域数とjを比較し(S1212006)、メモリ領域数がjよりも小さいステップ1212006に、大きい場合にはステップ12120010に進む。S1212003でNoの場合、アクセス権限切換部1212は、jに1を加える(S1212007)。アクセス権限切換部1212は、メモリ保護領域活性状態管理テーブル1220030のjと同じメモリ保護領域番号の活性状態を、メモリ保護領域活性パターン管理テーブル1220040のjと同じメモリ保護領域番号の活性パターン1の値に設定する(S1212008)。アクセス権限切換部1212は、テーブルサイズ管理テーブル1220080のメモリ保護領域数とjを比較し(S1212009)、メモリ領域数がjよりも小さいステップ1212006に、大きい場合にはステップ12120010に進む。アクセス権限切換部1212は、前回プログラム切換ID管理テーブル1220070の前回プログラム切換IDを、取得したプログラム切換IDの値で更新す

る（S1212010）。

[0066] 次に、本実施形態の車両用制御装置で行われる動作を図8を用いて説明する。

[0067] まず、ソフトウェア制御部1211は、プログラムNo. 1として、非特権モードで動作する安全度水準QMのソフトウェア「QMアプリ1」を動作させている。そして、QMアプリ1の実行中に、ソフトウェア制御部1211は、プログラムNo. 2として、非特権モードで動作する安全度水準ASILのソフトウェア「ASILアプリ1」を動作させようとする。このとき、「QMアプリ1」と「ASILアプリ1」とは、動作モードは非特権モードで同じであるため動作モード切換部による動作モード切換は不要であるが、安全度が異なることに起因してアクセス権限が異なるため、アクセス権限切換部がアクセス権限を切り換える。ここで、安全度水準（即ち、安全度水準がASILかQMか）に基づいて動作モードを切り換える方法では、動作させるソフトウェアを「QMアプリ1」から「ASILアプリ1」に変更する時点で動作モード切換部による動作モード切換が必要となる。しかし、本実施形態では、処理負荷（オーバヘッド）の大きな動作モード切換の処理が不要であり、アクセス権限切換の処理で済むため、ソフトウェアを「QMアプリ1」から「ASILアプリ1」に変更する際の処理を高速化する。

[0068] 次に、ソフトウェア制御部1211は、プログラムNo. 3として、非特権モードで動作する安全度水準ASILのソフトウェア「ASILOS」を動作させようとする。このとき、「ASILアプリ1」と「ASILOS」とでは動作モードが異なるため、動作モード切換部が動作モードを切り換える。ここでは、処理負荷の大きな動作モード切換の処理が発生する。

[0069] 次に、ソフトウェア制御部1211は、プログラムNo. 4として、非特権モードで動作する安全度水準QMのソフトウェア「QMアプリ2」を動作させようとする。このとき、「ASILOS」と「QMアプリ2」とでは動作モードが異なるため、動作モード切換部が動作モードを切り換える。ここでも、処理負荷の大きな動作モード切換の処理が発生する。

[0070] 次に、ソフトウェア制御部1211は、プログラムNo. 5として、非特権モードで動作する安全度水準ASILのソフトウェア「ASILアプリ2」を動作させようとする。従来であれば動作モード切換部による動作モード切換が必要であったが、本実施形態では動作モード切換は不要であり、アクセス権限切換部がアクセス権限を切り換える。

[0071] 次に、ソフトウェア制御部1211は、プログラムNo. 6として、非特権モードで動作する安全度水準QMのソフトウェア「QMアプリ3」を動作させようとする。ここで、安全度水準に基づいて動作モードを切り換える方法では、作モード切換部による動作モード切換が必要であるが、本実施形態では動作モード切換は不要であり、アクセス権限切換部がアクセス権限を切り換える。

[0072] このように、動作させるソフトウェアをプログラムNo. 1から6まで順次変更する上記の例では、従来は4回必要であった動作モード切換が、本実施形態であれば2回で済む。このように、本実施形態によれば、動作するソフトウェアが順次変更されながら行われる車両制御全体としての負荷（オーバヘッド）を減少させることができる。

[0073] 一般的に、車両制御に用いられるソフトウェアは、安全度が低いものの方が安全度が高いものに比べて多い。従って、安全度の比較的低いソフトウェア間ではアクセス権限切換によるメモリ保護を採用することで、動作モード切換が必要な対象を安全度の比較的高いソフトウェアに絞ることができる。即ち、動作モード切換が必要となる安全度を引き上げることができる。従って、全体として、動作モード切換の回数を減少させることができる。

[0074] 以上のように、通常のソフトウェアアーキテクチャでは、一つのタスクに異なる安全度のソフトウェアが混在しており、異なる安全要求のソフトウェアにおいてパーティショニングを適用すると、メモリ保護ユニット（MPU）によるアクセス制限が発生する。従来手法ではアクセス権限切り換え処理は、実行中の処理の中断が伴うOSの割り込み機能によって実現されるため、既存のソフトウェアでは、メモリ保護ユニット（MPU）で管理するアク

セス権限の切り換えが頻発し、処理中断によるオーバーヘッド増加が懸念されていた。

[0075] 一方、本実施形態によれば、安全度水準の異なる複数のソフトウェアを動作させる場合であっても、処理負荷を抑えつつ安全性を確保することができる。即ち、メモリ保護装置 112 が管理するメモリ保護領域の活性状態を柔軟にコントロールすることで、同一の演算装置（CPU）11 の動作モードで異なる安全度のソフトウェア間のメモリ保護を実現することができる。また、演算装置（CPU）11 の動作モードの切換と、メモリ保護装置 112 が管理するメモリ保護領域の活性状態の設定を活用することで、OS の割り込み頻度の少ない高速なメモリアクセス権限の切換をすることができる。

[0076] なお、車両用制御装置がアクセス権限違反を検出した場合、ドライバにその旨を報知するものであっても良い。例えば、ユーザインタフェース用の車両用制御装置を含む複数の車両用制御装置が車載ネットワークを介して接続される車両制御システムを例に説明すると、いずれかの車両用制御装置がメモリアクセスの異常（即ち、違反）を検出した場合、ユーザインタフェース用の車両用制御装置に異常情報を送信し、異常情報を受信した前記ユーザインタフェース用の車両用制御装置がドライバーへの警告に関する指令を行う方法がある。

[0077] また、アクセス異常情報を記憶するバックアップメモリを車両用制御装置に設け、ソフトウェアのアクセスに権限違反があった場合には、バックアップメモリに保存するようにしてもよい。この場合には、車載ネットワークを介して解析ツールを車両用制御装置に接続し、解析ツールからメモリアクセス異常情報を要求するメッセージを送信することにより、このメッセージを受信した車両用制御装置がメモリアクセス異常情報を解析ツールに送信することで、メモリアクセス異常情報を取り出すことができる。

[0078] なお、上記実施形態においては、特権モードで動作可能なソフトウェアがASIL OS であり、非特権モード動作ソフトウェアが安全度に応じて複数段階に区分される例を説明したが、これに限定されず、特権モード動作ソフ

トウェアが安全度に応じて複数段階に区分されるものであってもよい。この場合には、同じ特権モードにおいてアクセス権限切換部がソフトウェアの安全度に応じてアクセス権限を切り換える。一例としては、図17に示すように、ASIL-OSとASIL-Cアプリが特権モード動作ソフトウェアであり、非特権モード動作ソフトウェアがASIL-Bアプリ、ASIL-Aアプリ、QMアプリである例が考えられる。

請求の範囲

- [請求項1] 記憶部と、
 該記憶部に記憶される複数のソフトウェアの動作を制御するソフトウェア制御部と、
 前記ソフトウェア制御部の動作モードを特権モードと非特権モードとの間で切り換える動作モード切換部と、
 前記記憶部に対する前記各ソフトウェアのアクセス権限を切り換えるアクセス権限切換部とを備えることを特徴とする車両用制御装置。
- [請求項2] 前記各ソフトウェアは、特権モードで動作可能な特権モード動作ソフトウェアと、非特権モードで動作可能な非特権モード動作ソフトウェアとに区分され、
 前記ソフトウェア制御部が動作させるソフトウェアを前記特権モード動作ソフトウェアと前記非特権モード動作ソフトウェアとの間で切り換える場合には、前記動作モード切換部が動作モードを切り換え、
 前記ソフトウェア制御部が動作させるソフトウェアを同じ動作モードで動作するソフトウェア同士の間で切り換える場合には、前記アクセス権限切換部が前記ソフトウェアの安全度に応じて前記アクセス権限を切り換えることを特徴とする請求項1記載の車両用制御装置。
- [請求項3] 前記非特権モード動作ソフトウェアは、安全度に応じて複数段階に区分されることを特徴とする請求項1記載の車両用制御装置。
- [請求項4] 前記ソフトウェアのアクセス権限を監視するアクセス権限違反監視部を備え、
 前記アクセス権限違反監視部がアクセス権限違反を検知すると処理を中止することを特徴とする請求項1記載の車両用制御装置。
- [請求項5] 前記ソフトウェアのアクセス権限を監視するアクセス権違反監視部を備え、
 前記アクセス権限違反監視部がアクセス権限違反を検知すると違反に関する情報を保存することを特徴とする請求項1記載の車両用制

御装置。

[請求項6] 前記記憶部を分割して複数の記憶領域を設定する記憶領域設定部を備え、

前記アクセス権限切換部は、前記複数の記憶領域に対し、異なるアクセス権限を設定することを特徴とする請求項1記載の車両用制御装置。

[請求項7] 前記記憶部を分割して複数の記憶領域を設定する記憶領域設定部を備え、

前記アクセス権限切換部は、前記複数の記憶領域の中の同じ記憶領域に対し、ソフトウェアの安全度に応じて異なるアクセス権限を設定することを特徴とする請求項1記載の車両用制御装置。

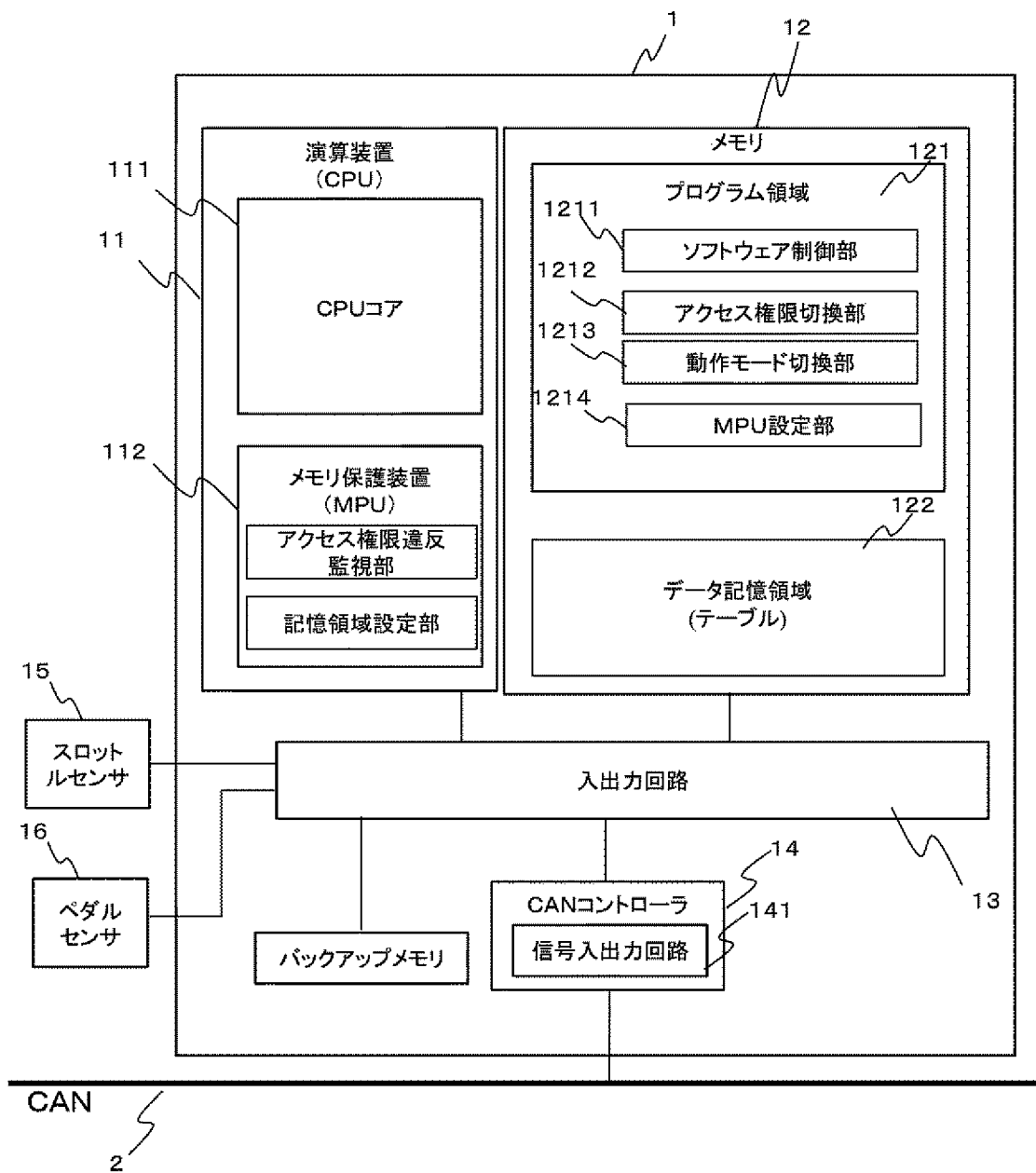
[請求項8] 前記アクセス権限切換部は、前記複数の記憶領域ごとに設定されるアクセス権限のパターンを複数管理し、

前記パターンを切り換えることにより、前記複数の記憶領域に対する個別のアクセス権限を一括して切り換えることを特徴とする請求項6記載の車両用制御装置。

[請求項9] 前記アクセス権限切換部は、前記記憶部に対して設定されるアクセス権限を、前記ソフトウェアの実行中に再設定することを特徴とする請求項1記載の車両用制御装置。

【図1】

【図1】



[図2]

【図2】

1220010		1220011		1220012					
先頭 アドレス	後尾 アドレス	特権モード アクセス権			非特権モード アクセス権				
		W	X	R	W	X	R		
0xffff	0x000	1	1	1	0	0	0		
		1220013	1220015	1220017	1220018				
		1220014	1220016						

[図3]

【図3】

1220021	1220022	1220023						
メモリ保護 領域番号	先頭 アドレス	後尾 アドレス	特権モード アクセス権			非特権モード アクセス権		
			W	X	R	W	X	R
1	0xffff	0xC00	1	1	1	0	0	1
2	0xC00	0xAFF	1	1	1	0	0	1
3	0xC00	0xAFF	1	1	1	1	1	1
4	0xAFF	0x0000	1	1	1	0	0	1
1220020			1220024	1220026	1220028	1220029		
			1220025	1220027				

[図4]

【図4】

1220030	1220031	1220032
メモリ保護 領域番号		活性状態
1		1
2		0
3		1
4		1

[図5]

【図5】

1220040	1220041	1220042	1220043
メモリ保護 領域番号	活性 パターン1	活性 パターン2	
1	1	1	
2	0	1	
3	1	0	
4	1	1	

[図6]

【図6】

1220050	1220051
動作モード フラグ	
0	

[図7]

【図7】

安全度水準	ソフトウェア	動作モード
ASIL	ASIL OS	特権モード
	ASIL アプリ1~2	非特権モード
QM	QMアプリ1~3	

[図8]

【図8】

1220060	1220061	1220062	1220063	1220064	1220065
プログラム No.	ソフトウェア名	安全度 水準	動作モード	プログラム 切替ID	
1	QMアプリ1	QM	非特権 モード	3	アクセス 権限
2	ASIL アプリ1	ASIL	非特権 モード	2	動作 モード
3	ASIL OS	ASIL	特権モード	1	動作 モード
4	QM アプリ2	QM	非特権 モード	3	アクセス 権限
5	ASIL アプリ2	ASIL	非特権 モード	2	アクセス 権限
6	QM アプリ3	QM	非特権 モード	3	アクセス 権限

[図9]

【図9】

1220070	1220071
前回プログラム 切替ID	
0	

[図10]

【図10】

1220080	1220081	1220082
1220083	1220084	
名称		総数
プログラム個数		20
メモリ保護領域数		4

[図11]

【図11】

1220090	1220091
前回動作モード フラグ	
0	

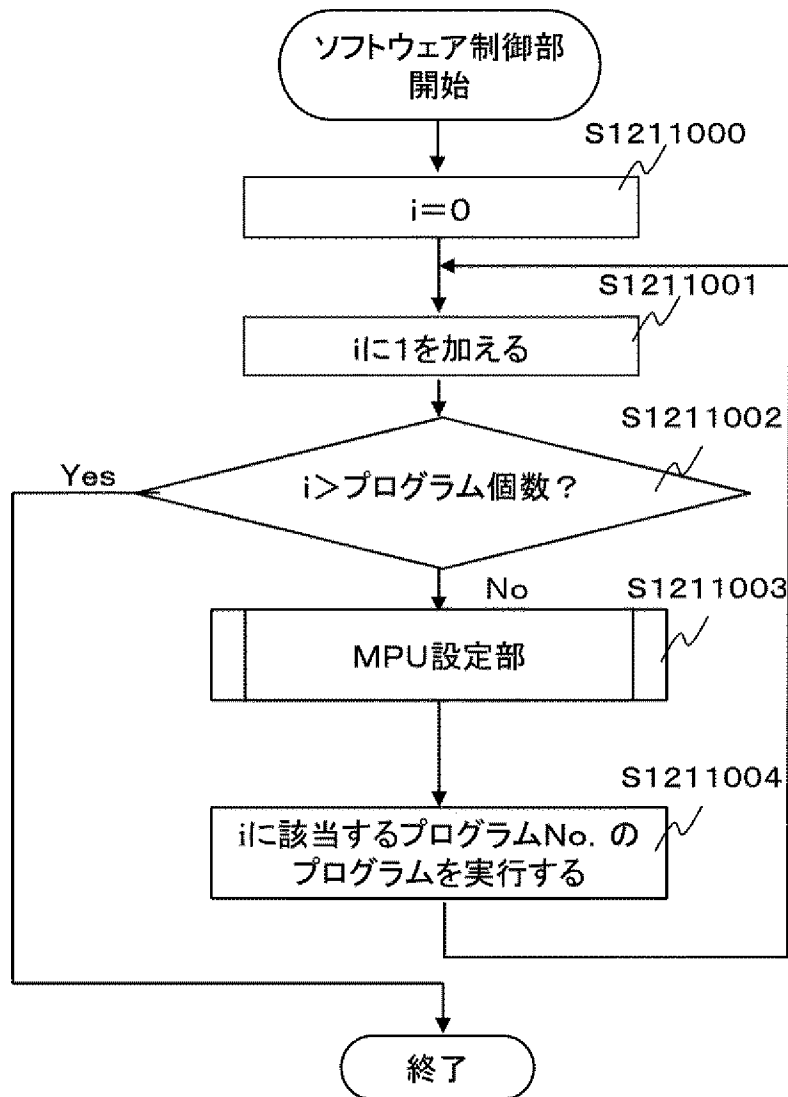
[図12]

【図12】

1220100	1220101	1220101
動作モード フラグ	プログラム カウンタ	
1	0xa133	

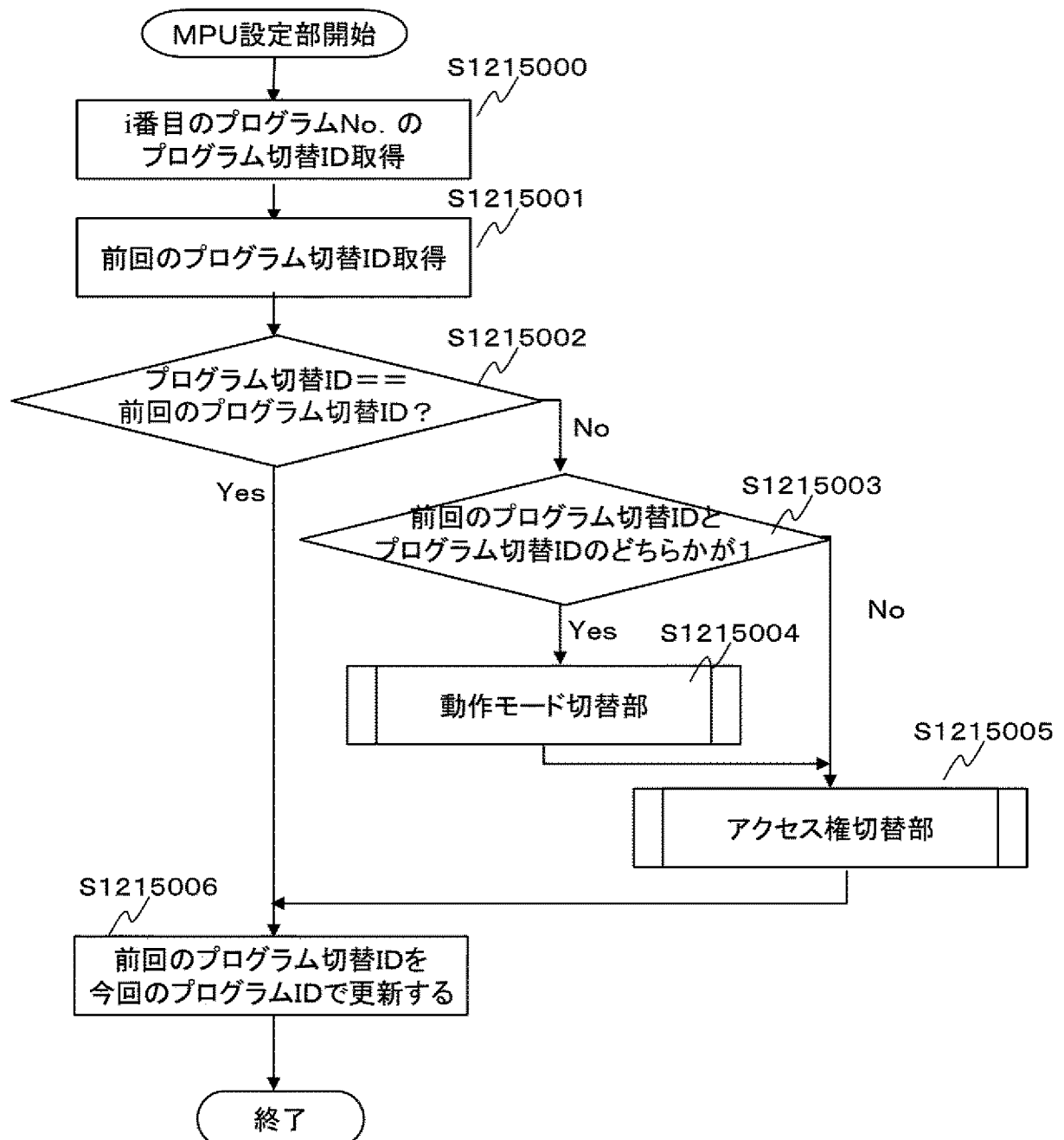
[図13]

【図13】



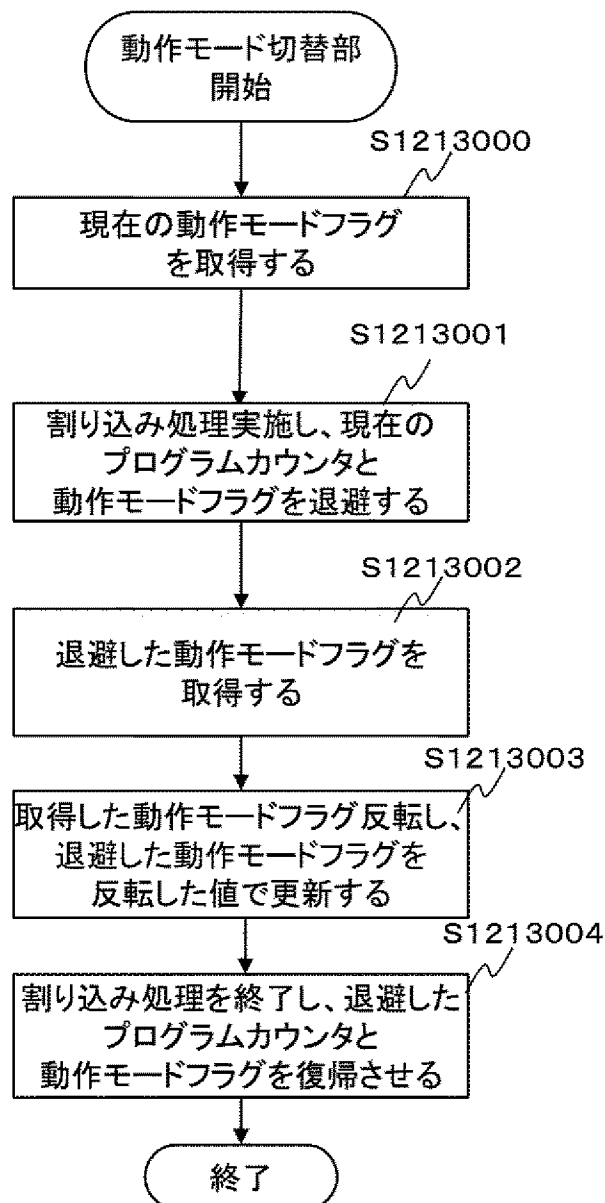
[図14]

【図14】



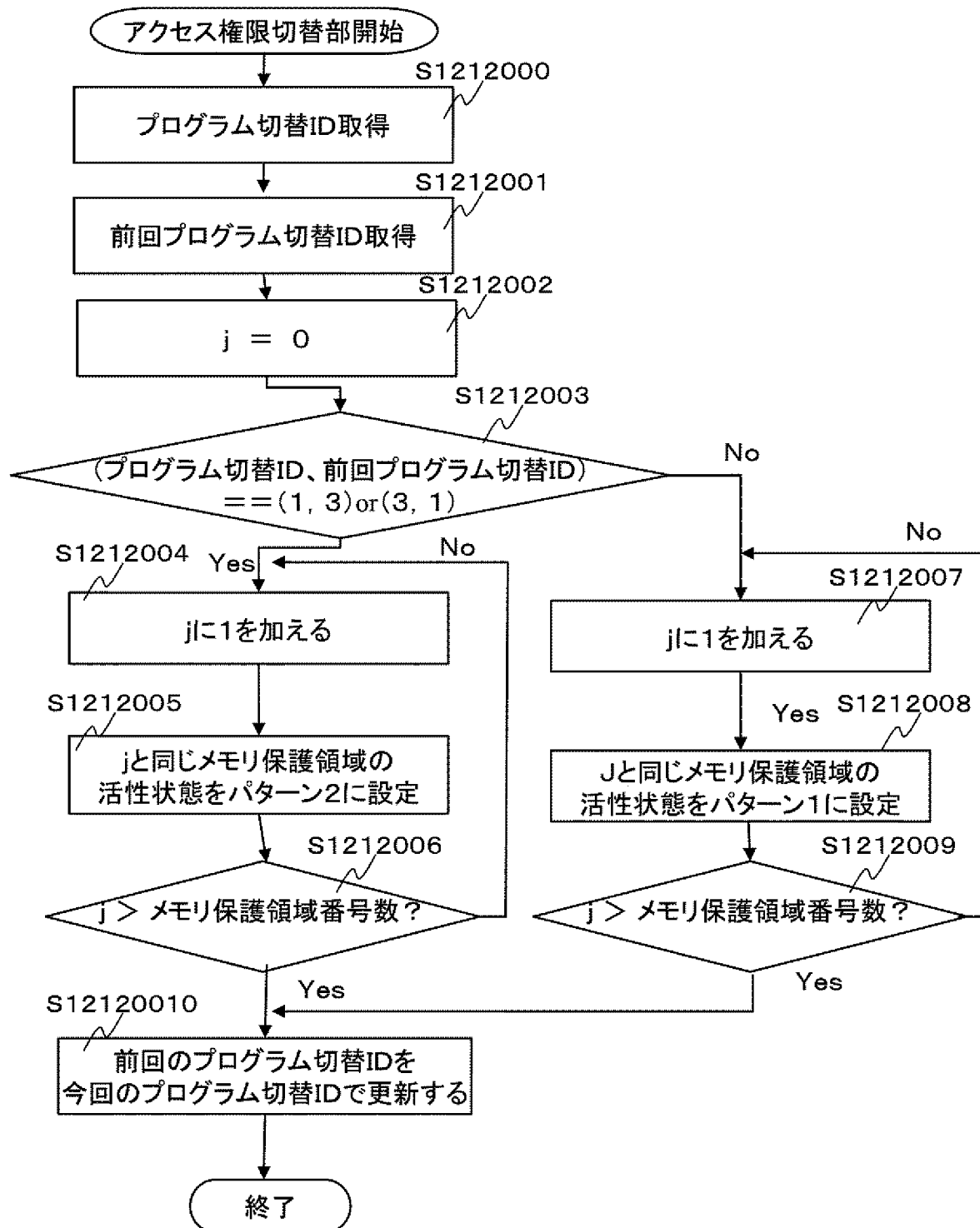
[図15]

【図15】



[図16]

【図16】



[図17]

【図17】

安全度水準		ソフトウェア	動作モード
ASIL	ASIL-D	ASIL OS	特権モード
	ASIL-C	ASIL-C アプリ	
	ASIL-B	ASIL-B アプリ	非特権モード
	ASIL-A	ASIL-A アプリ	
QM		QMアプリ	

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2014/065838

A. CLASSIFICATION OF SUBJECT MATTER

B60R16/02(2006.01) i, G06F21/62(2013.01) i

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)

B60R16/02, G06F21/62

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho	1922-1996	Jitsuyo Shinan Toroku Koho	1996-2014
Kokai Jitsuyo Shinan Koho	1971-2014	Toroku Jitsuyo Shinan Koho	1994-2014

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP 2013-161299 A (Toyota Motor Corp.), 19 August 2013 (19.08.2013), paragraphs [0012] to [0048] (Family: none)	1-9
Y	JP 2013-171467 A (Toyota Motor Corp.), 02 September 2013 (02.09.2013), paragraphs [0029], [0031], [0035], [0036], [0038] to [0055] (Family: none)	1-9
Y	JP 2007-287103 A (NEC Electronics Corp.), 01 November 2007 (01.11.2007), paragraphs [0002], [0004] & US 2007/0250675 A1 & US 2013/0132694 A1	1-9

☐ Further documents are listed in the continuation of Box C.

☐ See patent family 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 application or patent 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

"&" document member of the same patent family

Date of the actual completion of the international search
29 July, 2014 (29.07.14)

Date of mailing of the international search report
12 August, 2014 (12.08.14)

Name and mailing address of the ISA/
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

A. 発明の属する分野の分類（国際特許分類（IPC））

Int.Cl. B60R16/02(2006.01)i, G06F21/62(2013.01)i

B. 調査を行った分野

調査を行った最小限資料（国際特許分類（IPC））

Int.Cl. B60R16/02, G06F21/62

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	1922-1996年
日本国公開実用新案公報	1971-2014年
日本国実用新案登録公報	1996-2014年
日本国登録実用新案公報	1994-2014年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

C. 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求項の番号
Y	JP 2013-161299 A（トヨタ自動車株式会社）2013.08.19, 段落 0012 から 0048（ファミリーなし）	1 - 9
Y	JP 2013-171467 A（トヨタ自動車株式会社）2013.09.02, 段落 0029, 0031, 0035, 0036, 0038 から 0055（ファミリーなし）	1 - 9
Y	JP 2007-287103 A（NECエレクトロニクス株式会社）2007.11.01, 段落 0002, 0004 & US 2007/0250675 A1 & US 2013/0132694 A1	1 - 9

☐ C欄の続きにも文献が列挙されている。☐ パテントファミリーに関する別紙を参照。

* 引用文献のカテゴリー

「A」特に関連のある文献ではなく、一般的技術水準を示すもの

「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの

「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）

「O」口頭による開示、使用、展示等に言及する文献

「P」国際出願日前で、かつ優先権の主張の基礎となる出願

の日の後に公表された文献

「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの

「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの

「Y」特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの

「&」同一パテントファミリー文献

国際調査を完了した日

29.07.2014

国際調査報告の発送日

12.08.2014

国際調査機関の名称及びあて先

日本国特許庁（ISA/J P）

郵便番号100-8915

東京都千代田区霞が関三丁目4番3号

特許庁審査官（権限のある職員）

前田 浩

3D

2943

電話番号 03-3581-1101 内線 3341