

(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
2020年8月13日(13.08.2020)



(10) 国際公開番号

WO 2020/162316 A1

- (51) 国際特許分類:
G06F 12/14 (2006.01) *B60W 50/04* (2006.01)
- (21) 国際出願番号: PCT/JP2020/003411
- (22) 国際出願日: 2020年1月30日(30.01.2020)
- (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:
201941004257 2019年2月4日(04.02.2019) IN
- (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: パンチャングム キラン (PANCHANGAM Kiran); 560055 バンガロール

- マレスワラムーラジャジナガー ドクターラク
マールロード ブリゲードゲートウェイキャンパ
ス No. 26 / 1 ワールドトレードセンタ
ー 7 階ユニットナンバー S 7 0 4 日立イン
ド社内 Bangalore (IN). 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).
芹沢 一(SERIZAWA Kazuyoshi); 〒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: ポレール特許業務法人 (POLAIRE
I.P.C.); 〒1030025 東京都中央区日本橋茅場
町二丁目 1 3 番 1 1 号 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,

(54) Title: SYSTEM AND METHOD FOR HETEROGENEOUS ASYMMETRIC SYSTEMS WHICH MANAGE MIXED CRITICAL FUNCTIONALITY

(54) 発明の名称: 異種非対称システムのための混在する重要な機能を管理するためのシステムおよび方法

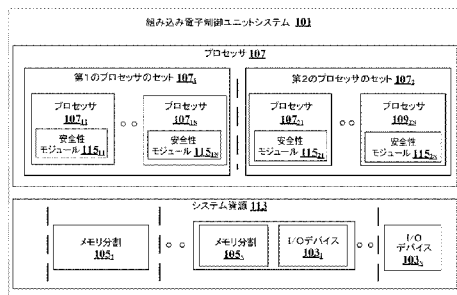


図 1b

101	Embedded electronic control unit system
103 ₁ , 103 _N	I/O device
105 ₁ , 105 _N	Memory split
107, 107 ₁₁ , 107 _{1N} , 107 ₂₁ , 107 _{2N}	Processor
107 ₁	First set of processors
107 ₂	Second set of processors
113	System resource
115 ₁₁ , 115 _{1N} , 115 ₂₁ , 115 _{2N}	Safety module

(57) Abstract: The present disclosure discloses a method and embedded electronic control unit (ECU) system for heterogeneous asymmetric systems, which manage mixed critical functionality. The embedded ECU system comprises: a split module which splits a plurality of processors into a first set of processors and a second set of processors; and an extraction module which extracts a safety setting value for the first set of processors. The safety setting value is generated during the split. The safety setting value of the first set of processors is verified on the basis of a trusted safety setting value, and the first set of processors access system resources on the basis of the result of the verification.

(57) 要約: 本開示は、異種非対称システムのための、混在する重要な機能を管理するための、方法および組み込み電子制御ユニット (ECU) システムを開示する。組み込み ECU システムは、複数のプロセッサを第 1 のプロセッサのセットと第 2 のプロセッサのセットとに分割する分割モジュールと、第 1 のプロセッサのセットの安全性設定値を抽出する抽出モジュールとを備える。安全性設定値は、分割中に生成される。第 1 のプロセッサのセットの安全性設定値は、信頼されている安全性設定値に基づいて検証され、第 1 のプロセッサのセットは、検証の結果に基づいて、システム資源にアクセスする。

CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO,
DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT,
HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH,
KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, 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,
ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG,
US, UZ, VC, VN, WS, ZA, ZM, ZW.

- (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, ST, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, RU, TJ, TM), ヨーロッパ (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).

添付公開書類:

- 一 国際調査報告 (条約第21条(3))

明 細 書

発明の名称：

異種非対称システムのための混在する重要な機能を管理するためのシステムおよび方法

技術分野

[0001] 本発明は、一般に、組み込みシステムに関し、より具体的には、限定されるものではないが、異種非対称システムのための、混在する重要な機能を管理するためのシステムおよび方法に関する。

背景技術

[0002] 近年、自動車システムにおける電子部品の使用が驚異的に増加しており、その結果、様々な機能の純機械的な実装が置き換えられている。一般に、深く組み込まれた電子制御ユニット（Electronic Control Unit、ECU）は、複雑な演算をサポートできず、複雑な演算を実行するためには、新たなECUが必要とされる場合がある。しかし、複雑な演算のための新たなECUを導入すれば、整備および製造のコストが増加する。今日、様々なECU機能を、単一のECUハードウェアに統合することができる。しかし、このような合併した単一のECUを組み合わせ実行している間に、重要度の異なるいくつかの機能が相互に干渉し、致命的なシステム障害とメモリ破壊につながる場合がある。したがって、機能安全の問題は、組み込みシステムの設計および開発においてより重要になりつつある。

[0003] 既存の組み込みシステムは、実行特権を制御するための方法を提供し、したがって、同一ハードウェア上で重要度が混在する機能の分離を提供する。特に、特権は、タスクが実行されているプロセッサに局所化されている。一般に、オペレーティングシステムは、任意の機能の特権を割り当てて管理し得る。しかし、オペレーティングシステムは、ユーザーによる変更に対して脆弱であり、それゆえ、ついには悪意のあるプログラムを実行して、システム間の妨害を引き起こす場合がある。加えて、局所化された特権は、異種ハ

ードウェア内の他のプロセッサからは認識できず、安全性違反につながる。さらに、ローカルに格納された重要なデータは、プロセッサを迂回し、ダイレクトメモリアクセス（Direct Memory Access、DMA）を介してアクセスされ得る。

[0004] 本開示のこの背景技術の節において開示される情報は、本発明の一般的な背景への理解を向上するためのものに過ぎず、この情報が、当業者に既に知られている先行技術を形成するということの、自認または何らかの形の示唆と考えるべきではない。

発明の概要

課題を解決するための手段

[0005] 一実施形態では、本開示は、異種非対称システムのための、混在する重要な機能を管理するための組み込み電子制御ユニット（ECU）システムに関する場合がある。組み込みECUシステムは、複数のプロセッサと、プロセッサに通信可能に結合されたメモリとを備えてもよく、メモリは、実行時に、組み込みECUシステムに、複数のプロセッサを第1のプロセッサのセットと第2のプロセッサのセットとに分割させて、第1のプロセッサのセットの安全性設定値を抽出させ得る、プロセッサ実行可能命令を格納する。安全性設定値は、分割中に生成される。さらに、第1のプロセッサのセットの安全性設定値は、信頼されている安全性設定値に基づいて検証される。その後、第1のプロセッサのセットは、検証の結果に基づいて、システム資源にアクセスする。

[0006] 一実施形態では、本開示は、異種非対称システムのための、混在する重要な機能を管理するための方法に関する場合がある。本方法は、複数のプロセッサを第1のプロセッサのセットと第2のプロセッサのセットとに分割して、第1のプロセッサのセットの安全性設定値を抽出することを含む。安全性設定値は、分割中に生成され、第1のプロセッサのセットの安全性設定値は、信頼されている安全性設定値に基づいて検証される。その後、第1のプロセッサのセットは、検証の結果に基づいて、システム資源にアクセスする。

[0007] 上記の概要は、例示的なものに過ぎず、決して限定的であることが意図されているものではない。上記の例示的な態様、実施形態、および特徴に加えて、さらなる態様、実施形態、および特徴が、図面および以下の詳細な説明を参照することにより明らかになるであろう。

図面の簡単な説明

[0008] 本開示に組み込まれ、かつ本開示の一部を構成する添付の図面は、例示的な実施形態を示し、図面の簡単な説明とともに、開示される原理を説明するのに役立つ。図中、参照番号の左端の数字は、その参照番号が最初に現れる図を特定する。類似の機能および構成要素を参照するために、全ての図を通して、同一の番号が使用されている。ここで、本発明の実施形態と一致する、システムおよび／または方法のいくつかの実施形態を、単なる例として、添付の図を参照して説明する。

[図1a]本開示のいくつかの実施形態による、組み込み電子制御ユニットシステムの例示的なブロック図を示す。

[図1b]本開示のいくつかの実施形態による、組み込み電子制御ユニットシステムの例示的なブロック図を示す。

[図2]本開示のいくつかの実施形態による、異種非対称システムのための、混在する重要な機能を管理するために構成された組み込みECUシステムの内部アーキテクチャを示す。

[図3a]本開示のいくつかの実施形態による、異種非対称システムのための、混在する重要な機能の管理の例示的な表現を示す。

[図3b]本開示のいくつかの実施形態による、異種非対称システムのための、混在する重要な機能の管理の例示的な表現を示す。

[図3c]本開示のいくつかの実施形態による、異種非対称システムのための、混在する重要な機能の管理の例示的な表現を示す。

[図3d]本開示のいくつかの実施形態による、異種非対称システムのための、混在する重要な機能の管理の例示的な表現を示す。

[図3e]本開示のいくつかの実施形態による、異種非対称システムのための、

混在する重要な機能の管理の例示的な表現を示す。

[図4a]本開示のいくつかの実施形態による、安全性設定の実行の例示的な表現を示す。

[図4b]本開示のいくつかの実施形態による、安全性設定の実行の例示的な表現を示す。

[図4c]本開示のいくつかの実施形態による、安全性設定の実行の例示的な表現を示す。

[図5]本開示のいくつかの実施形態による、異種非対称システムのための、混在する重要な機能を管理する方法を示す、フローチャートを示す。

[図6]本開示と一致する実施形態を実装するための、例示的なコンピュータシステム600のブロック図を示す。

[0009] 本明細書のいずれのブロック図も、本発明の原理を具現する例示的なシステムの概念図を表すことを、当業者は理解すべきである。同様に、あらゆるフローチャート、フロー図、状態遷移図、擬似コードなどは、コンピュータ読み取り可能媒体で実質的に表され得、コンピュータまたはプロセッサによって、そのようなコンピュータまたはプロセッサが明示的に示されているかどうかにかかわらず実行され得る、様々な処理を表すことが理解されよう。

発明を実施するための形態

[0010] 本文書では、「例示的」という言葉は、「例、具体例、または実例として役立つ」ことを意味するものとして本明細書で使用される。本明細書で「例示的」であるとして説明される、本発明のあらゆる実施形態または実装は、必ずしも他の実施形態よりも好適または有利であると解釈されるべきではない。

[0011] 本開示には、様々な変更および代替の形態の余地があるが、その特定の実施形態は、例として図面に示されており、以下で詳細に説明されるであろう。しかし、本開示を、開示される特定の形態に限定することは意図されておらず、反対に、本開示は、本開示の範囲内にある変更、等価、および代替のすべてに及ぶものであることが理解されるべきである。

[0012] 用語「含む（備える）（*comprises*）」、「含んでいる（備えている）（*comprising*）」、またはその他のそのあらゆる変形は、構成要素またはステップの列挙を含む構成、デバイスまたは方法が、それらの構成要素またはステップのみを含むのではなく、明示的に列挙されていないか、またはそのような構成もしくはデバイス、もしくは方法に固有の、他の構成要素もしくはステップを含み得るように、非排他的な包含に及ぶことが意図されている。言い換えると、「～を含む（備える）（*comprises*... a）」によって進行する、システムまたは装置内の1つまたは複数の要素は、システムまたは方法内の、他の要素または追加の要素の存在を、さらなる制約なしに除外するものではない。

[0013] 本開示の実施形態の以下の詳細な説明では、本明細書の一部を形成する、添付の図面を参照する。特定の実施形態がその添付の図面内で例示として示され、その特定の実施形態の中で、本開示が実施され得る。これらの実施形態は、当業者が本開示を実施できるように十分詳細に説明されており、他の実施形態が利用されてもよく、かつ本開示の範囲から逸脱することなく変更がなされてもよいことが理解されるべきである。それ故、以下の説明は、限定的な意味で考えるべきではない。

[0014] 本開示の実施形態は、異種非対称システムのための、混在する重要な機能を管理するための組み込み電子制御ユニット（ECU）システムに関する。一実施形態では、異種非対称システムは、アーキテクチャまたはマイクロアーキテクチャが相異なる、2つまたはそれより多くのプロセッサを備えるシステムを指す場合がある。一実施形態では、組み込みECUシステムは、1つまたは複数の電気システムまたはサブシステムを制御する。本開示では、組み込みECUシステムは、複数のプロセッサを備え、各プロセッサは、安全性モジュールのインスタンスを実行する。複数のプロセッサは、第1のプロセッサのセットと第2のプロセッサのセットとに分割される。一実施形態では、第1のプロセッサのセットの各プロセッサは、低信頼性プロセッサであり、第2のプロセッサのセットの各プロセッサは、高信頼性プロセッサで

ある。システム資源にアクセスするためのあらゆる要求中に、組み込みECUシステムは、第1のプロセッサのセットの安全性設定値を抽出する。抽出された第1のプロセッサのセットの安全性設定値は、ハッシュ化されて第2のプロセッサのセットに送信され、信頼されている安全性設定値に対して検証される。これにより、組み込みECUシステムは、検証に基づいて、第1のプロセッサのセットにシステム資源へのアクセスを提供する。本開示は、安全性非適合構成要素がもたらす影響による、システムの高信頼性構成要素の安全動作の妨害を抑えることにより、信頼性を高める。

[0015] 図1aおよび図1bは、本開示のいくつかの実施形態による、組み込み電子制御ユニットシステムの例示的なブロック図を示す。

[0016] 図1aに示されるように、環境は、組み込み電子制御ユニット（ECU）システム101を含む。組み込みECUシステム101は、入出力（Input/Output、I/O）インターフェース103、複数のプロセッサ107（「CPU」または「プロセッサ」、プロセッサ107という）、およびプロセッサ107によって実行可能な命令を格納するためのメモリ105、を含む。I/Oインターフェース103は、プロセッサ107と結合される。入力信号または/および出力信号は、この結合を介して通信される。当業者は、図1aが、例示的な実施形態であり、組み込みECUシステム101が、本開示で明示的に言及されていない任意の他のユニットを含み得ることを、理解するであろう。組み込みECUシステム101は、異種非対称システムのための、混在する重要な機能を管理するために使用されてもよい。一実施形態では、組み込みECUシステム101は、最高の特権レベルで、安全性モジュールのインスタンスを実行する。一実施形態では、特権レベルは、組み込みECUシステム101内でのアクセスおよび実行のための権限のレベルという場合がある。組み込みECUシステム101は、図1bに示されるようにプロセッサ107を分割する。プロセッサ107は、第1のプロセッサのセット107₁および第2のプロセッサのセット107₂として分割されてもよい。一実施形態では、第1のプロセッサのセット107₁は

、低信頼性プロセッサであってよく、第2のプロセッサのセット107₂は、高信頼性プロセッサであってよい。特に、低信頼性プロセッサは、安全性非適合プロセッサであり、高信頼性プロセッサは、安全性適合プロセッサである。一実施形態では、安全性適合プロセッサは、標準の安全度水準に基づいて、安全性非適合プロセッサよりも高く格付けされ得るプロセッサを指す場合がある。図1bに示すように、第1のプロセッサのセット107₁は、プロセッサ107₁₁、プロセッサ107₁₂、……………およびプロセッサ107_{1n}（併せて第1のプロセッサのセット107₁という）を含む。同様に、第2のプロセッサのセット107₂は、プロセッサ107₂₁、プロセッサ107₂₂、……………およびプロセッサ107_{2n}（併せて第2のプロセッサのセット107₂という）を含む。第1のプロセッサのセット107₁の各々は、それぞれ安全性モジュール115₁を含む。同様に、第2のプロセッサのセット107₂の各々は、それぞれ安全性モジュール115₂を含む。

[0017] あらゆる瞬間において、システム資源113にアクセスするための要求を受信すると、組み込みECUシステム101は、第1のプロセッサのセット107₁の安全性モジュール115₁から、安全性設定値を抽出し得る。一実施形態では、安全性設定値は、プロセッサ107の分割中に生成される。一実施形態では、第1のプロセッサのセット107₁は、分割に基づいて、第2のプロセッサのセット107₂から安全性設定値を受信し、各メモリ管理ユニット（Memory Management Unit、MMU）の安全性設定値を設定する。さらに、抽出された第1のプロセッサのセット107₁の安全性設定値は、ハッシュ化されて、プロセッサ間通信（Inter Processor Communication、IPC）技術によって第2のプロセッサのセット107₂に送信される。当業者は、本開示の範囲が、本明細書で明示的に言及されていない、安全性設定値を送信するためのあらゆる他の技術を包含し得ることを理解するであろう。さらに、第1のプロセッサのセット107₁の安全性設定値は、第2のプロセッサのセット107₂の信頼されている安全性設定値に基づいて検証される。一実施形態では、安全

性設定値は、第1のプロセッサのセット1071のアクセスを許可する範囲を含み、信頼されている安全性設定値は、複数のレベルによって分類されたアクセスを許可する範囲を含む。一実施形態では、範囲は、アプリケーションの種類に基づいて設定可能であってもよい。例えば、範囲は「0x000203~0x020304」であってもよい。一実施形態では、第1のプロセッサのセット1071の安全性設定の検証は、組み込みECUシステム101に関連付けられた、外部検証モジュール（図1bにおいて明示的には示されていない）によって実行されてよい。一実施形態では、第1のプロセッサのセット1071の安全性設定値は、組み込みECUシステム101の外部に存在する、検証モジュール（明示的には図示せず）によって実行されてもよい。別の実施形態では、組み込みECUシステム101は、第1のプロセッサのセット1071の安全性設定値を検証してもよい。第1のプロセッサのセット1071の安全性設定値は、その安全性設定値を、第2のプロセッサのセット1072の信頼されている安全性設定値と比較することにより検証される。その後、組み込みECUシステム101は、検証の結果に基づいて、システム資源113へのアクセスを、第1のプロセッサのセット1071に提供し得る。アクセスは、例えば、メモリ105の要求されたメモリ位置、メモリ位置上の書き込み可能および書き換え不能のステータスなどに関連付けられてもよい。一実施形態では、組み込みECUシステム101は、検証の結果に基づいて第1のプロセッサのセット1071にアクセスを提供するための、アクセスユニット（図において明示的には示されていない）に関連付けられてもよい。

[0018] 図2は、本開示のいくつかの実施形態による、異種非対称システムのための、混在する重要な機能を管理するために構成された組み込みECUシステムの内部アーキテクチャを示す。

[0019] 図2に示されるように、組み込みECUシステム101は、データ200、および本明細書で詳細に説明される1つまたは複数のモジュール209を含んでもよい。一実施形態では、データ200は、メモリ105内に格納さ

れてもよい。データ200は、例えば、分割データ201、安全性設定データ203、検証データ205およびその他のデータ207を含んでもよい。

[0020] 分割データ201は、プロセッサ107の、第1のプロセッサのセット107₁および第2のプロセッサのセット107₂への分割に関する詳細を含んでもよい。その詳細には、プロセッサ107に関連付けられた安全性設定値が含まれてもよい。

[0021] 安全性設定データ203は、第1のプロセッサのセット107₁から抽出された安全性設定値を含んでもよい。一実施形態では、安全性設定値は、分割中に生成されてもよい。

[0022] 検証データ205は、第1のプロセッサのセット107₁の安全性設定値を、第2のプロセッサのセット107₂の信頼されている安全性設定と比較した結果を含んでもよい。一実施形態では、検証の結果は、第1のプロセッサのセット107₁のシステム資源113へのアクセスレベルの詳細を含んでもよい。

[0023] その他のデータ207は、組み込みECUシステム101の様々な機能を実行するために1つまたは複数のモジュール209によって生成された、一時データおよび一時ファイルを含むデータを格納してもよい。

[0024] 一実施形態では、メモリ105内のデータ200は、組み込みECUシステム101のメモリ105内に存在する、1つまたは複数のモジュール211によって処理される。一実施形態では、1つまたは複数のモジュール209は、専用ユニットとして実装されてもよい。本明細書で使用されるモジュールという用語は、特定用途向け集積回路(application specific integrated circuit、ASIC)、電子回路、フィールドプログラマブルゲートアレイ(field-programmable gate array、FPGA)、プログラマブルシステムオンチップ(Programmable System-on-Chip、PSoC)、組み合わせ論理回路、および／または説明されている機能を提供するその他の適切な構成要素を指す。いくつかの実装形態では、1つま

たは複数のモジュール209は、組み込みECUシステム101の1つまたは複数の機能を実行するために、プロセッサ107に通信可能に結合されてもよい。1つまたは複数のモジュール209は、本開示で定義される機能で構成される場合、新規のハードウェアとなる。

[0025] 一実装形態では、1つまたは複数のモジュール209は、分割モジュール211、抽出モジュール213、および送信モジュール215を含んでもよいが、これらに限定されない。1つまたは複数のモジュール209は、組み込みECUシステム101の種々雑多な機能を実行するための、その他のモジュール217も含んでもよい。一実施形態では、その他のモジュール217は、検証モジュールおよびアクセスモジュールを含んでもよい。

[0026] 分割モジュール211は、プロセッサ107を、第1のプロセッサのセット107₁と第2のプロセッサのセット107₂とに仮想的に分割してもよい。一実施形態では、分割モジュール211は、プロセッサ107の各プロセッサの安全性適合に基づいて、プロセッサ107を分割してもよい。例えば、プロセッサ107の安全性非適合の各プロセッサは、第1のプロセッサのセット107₁に分割され、プロセッサ107の安全性適合の各プロセッサは、第2のプロセッサのセット107₂に分割される。一実施形態では、第1のプロセッサのセット107₁の各プロセッサは、低信頼性プロセッサであり、第2のプロセッサのセット107₂の各プロセッサは、高信頼性プロセッサである。

[0027] 第1のプロセッサのセット107₁からの、システム資源113にアクセスするための何らかの要求を受信すると、抽出モジュール213は、第1のプロセッサのセット107₁の安全性設定値を抽出し得る。さらに、第1のプロセッサのセット107₁の抽出された安全性設定値は、ハッシュ化され、インデックス付けされてもよい。

[0028] 送信モジュール215は、IPC技術によって、第1のプロセッサのセット107₁のハッシュ化された安全性設定値を、第2のプロセッサのセット107₂に送信してもよい。

[0029] 第1のプロセッサのセット107₁の安全性設定値は、組み込みECUシステム101に関連付けられた外部検証モジュールか、組み込みECUシステム101の外部に存在する検証モジュールによって、第2のプロセッサのセット107₂の信頼されている安全性設定値と比較することにより検証される。検証の結果に基づいて、第1のプロセッサのセット107₁は、システム資源113にアクセスし得る。

[0030] 図3a～図3eは、本開示のいくつかの実施形態による、異種非対称システムのための、混在する重要な機能の管理の例示的な表現を示す。

[0031] ここで図3aを参照すると、異種非対称システムのための、混在する重要な機能の管理の例示的な表現300が示されている。図3aでは、例示的な表現300は、組み込みECUシステム101を含む。組み込みECUシステム101は、低信頼性プロセッサであるプロセッサ301、および高信頼性プロセッサであるプロセッサ302を含む。当業者は、図3aが、例示的な実施形態であり、本開示が、低信頼性プロセッサと高信頼性プロセッサとの両方について、1つより多くのプロセッサも含み得ることを理解するであろう。プロセッサ301とプロセッサ302は、図3a中の点線で表されるように仮想的に分割されている。さらに、第1のプロセッサ301という第1の分割は、組み込みECUシステム101のオペレーティングシステム308から分離されている安全性モジュール303、分割用モジュール305、抽出モジュール307、ならびに更新不可能な形式の第1のアプリケーション309および更新可能な形式の第2のアプリケーション311を含む。一実施形態では、プロセッサ301内の第2のアプリケーション311は、更新されてもよい。プロセッサ302は、更新可能な形式であってはならないアプリケーション312に関連付けられている。第1のプロセッサ301は、対応するメモリ管理ユニット（MMU）内の安全性設定値を受信して設定する。プロセッサ301の設定された安全性設定値は、抽出モジュール307によって抽出され、ハッシュ化されて、IPC技術によってプロセッサ302に送信される。プロセッサ302は、プロセッサ301の安全性設定

値を、プロセッサ302の信頼されている安全性設定値で確認する、検証モジュール315を含む。したがって、第2のアプリケーション311の何らかの更新の間、如何なるDMA攻撃によっても、アクセスが許可されることはない。同様に、図3bは、フィールドプログラマブルゲートアレイ（FPGA）上に、低信頼性プロセッサとしてのプロセッサ301、および高信頼性Software317を有する、異種非対称システムのための、混在する重要な機能の管理の例示的な表現を示す。一実施形態では、いくつかの実装は、高信頼性プロセッサ／SoftwareサブシステムとしてのFPGAを含み得る。プロセッサ301の安全性設定値の検証は、専用のSoftwareである安全性検証エンジン316によって実行されてもよい。したがって、第2のアプリケーションのための何らかの更新を受信する場合、プロセッサ301の安全性設定値が検証され、そのような更新中のアクセスは、如何なるDMA攻撃によっても、許可されることはない。

[0032] 図3cは、FPGA上に、低信頼性プロセッサとしてのプロセッサ301、高信頼性プロセッサとしてのプロセッサ302、およびSoftware317を有する、混在する重要な機能を管理するための、3つのエンティティの異種サブシステムの例示的な表現を示す。プロセッサ301およびプロセッサ302は、両方とも、それぞれの安全性設定値をFPGA上のSoftware317で送信してもよい。安全性設定の検証は、FPGA上のSoftware317によって実装されてもよい。一実施形態では、FPGAは、安全性検証エンジン316の一部として実装された、安全なメモリ領域および非安全なメモリ領域を露呈してもよい。したがって、第2のアプリケーション311₁のための何らかの更新を受信する場合、プロセッサ301の安全性設定値が検証され、そのような更新中のアクセスは、如何なるDMA攻撃によっても、許可されることはない。

[0033] 同様に、図3dは、FPGA上に、低信頼性プロセッサとしてのプロセッサ301、高信頼性FPGAとしてのプロセッサ302、およびSoftware317をとまなう中間プロセッサを有する、混在する重要な機能を管理す

るための、3つのエンティティの異種サブシステムの例示的な表現を示す。プロセッサ301およびプロセッサ302は、両方とも、安全性設定値をFPGA上のSoftwareで送信してもよい。一実施形態では、Software317をとともなう中間プロセッサは、それぞれ異なるレベルの安全性分割制限を割り当て得る。FPGAは、安全性検証エンジン316の一部として実装された、安全なメモリ領域および非安全なメモリ領域を露呈してもよい。したがって、第2のアプリケーション311₁のための何らかの更新を受信する場合、プロセッサ301の安全性設定値が、安全性検証エンジン316によって検証され、そのような更新中のアクセスは、如何なるDMA攻撃によっても、許可されることはない。図3eは、安全性ミドルウェア318をとともなう低信頼性プロセッサとしてのプロセッサ301、および高信頼性プロセッサとしてのプロセッサ302を有する、混在する重要な機能を管理するための、例示的な実装を示す。一実施形態では、安全性ミドルウェア318を使用して、アプリケーション間の安全性違反を検出してもよい。安全性ミドルウェア318は、安全性違反および異常をアプリケーションレベルでフィルタリングするために配置されてもよい。一実施形態では、安全性ミドルウェア318は、カーネルの構成要素であってもよい。

[0034] 図4a、図4b、および図4cは、本開示のいくつかの実施形態による、安全性設定の実行の例示的な表現を示す。

[0035] 図4aおよび図4bは、組み込みECUシステム101における、安全性設定へのアクセス違反の報告の例示的な表現を示す。図4cは、組み込みECUシステム101における、安全性設定へのアクセス承認の報告の例示的な表現を示す。一実施形態では、第1のプロセッサのセット107₁からのメモリまたはデバイスの要求に基づいて、メモリアドレス、アクセス種別、安全ユニットID、および安全性レベルの、事前設定値が抽出されてもよい（第1のプロセッサのセット107₁の安全性設定値という）。図4aに示す最初のシナリオを検討せよ。この場合、第1のプロセッサのセット107₁に関連付けられたアプリケーションによる、安全ユニットID「0x30」、メ

モリアドレス「0x80001020」で、アクセス種別「Write (W)」の、メモリ位置にアクセスするための要求が受信される。要求を受信すると、対応するMMU設定が、設定される。MMU設定は、図4aに示す例示的な表401によって表される。組み込みECUシステム101は、要求に関連付けられた安全性設定値を、設定されたMMU設定と比較してよい。表401に示すように、要求に対応するモリアドレス「0x80001020」は、「0x80001000-0x800012FF」のモリアドレス範囲内にある。加えて、表402に示すように、安全性レベル「2」の安全ユニットID「0x30」が、初期化中に事前設定される。モリアドレス範囲「0x80001000-0x800012FF」は、安全ユニットID「0x30」のアプリケーションへの、「read」種別のみのアクセスを提供する。したがって、比較すると、組み込みECUシステム101は、第1のプロセッサのセット107₁からのアクセス要求を、違反しているとして報告し得る。要求は、「0x80001000-0x800012FF」のモリアドレス範囲について許可されていない、「write」アクセス種別へのものだからである。図4bに示す2番目のシナリオを検討せよ。この場合、第1のプロセッサのセット107₁に関連付けられたアプリケーションによる、安全ユニットID「0x34」、モリアドレス「0x80001020」で、アクセス種別「Read (R)」の、メモリ位置にアクセスするための要求が受信される。要求を受信すると、対応するMMU設定が、設定される。組み込みECUシステム101は、要求に関連付けられた安全性設定値を、設定されたMMU設定と比較してよい。表401に示すように、要求に対応するモリアドレス「0x80001020」は、「0x80001000-0x800012FF」のモリアドレス範囲内にある。しかし、モリアドレス範囲「0x80001000-0x800012FF」は、安全ユニットID「0x30」のアプリケーションへの、「read」種別のアクセスを提供する。したがって、比較すると、組み込みECUシステム101は、第1のプロセッサのセット107₁からのアクセス要求

を、違反しているとして報告し得る。安全ユニットID「0x34」は、「0x80001000-0x800012FF」のメモリアドレス範囲について許可されていないからである。一実施形態において、アクセス違反は、第1のプロセッサのセット107₁に緊急のソフトウェアリセットを発行している間に、第1のプロセッサのセット107₁へのソフトウェア割り込みを介して報告されて、OEMの設定された回復動作などを実行してもよい。表401に示すように、違反動作は、対応する動作IDにマッピングされる。許可される安全ユニットIDは、特定のアドレス範囲に関連付けられるように設定される、複数の安全ユニットID (Safety Unit ID、SUI) の機能である。システムの初期化中、安全性レベルは、複数エンティティの異種システムのユニットを区別するために使用され、SUIは、システム内の特定の処理エンティティに割り当てられた一意のIDを表す。

[0036] 同様に、図4cに示すように、要求が、第1のプロセッサのセット107₁に関連付けられたアプリケーションによって、安全ユニットID「0x30」、メモリアドレス「0x80001020」で、アクセス種別「Read (R)」の、メモリ位置にアクセスするためのものであることを検討せよ。要求を受信すると、対応するMMU設定が、設定される。組み込みECUシステム101は、要求に関連付けられた安全性設定値を、設定されたMMU設定と比較してよい。表401に示すように、要求に対応するメモリアドレス「0x80001020」は、「0x80001000-0x800012FF」のメモリアドレス範囲内にある。加えて、メモリアドレス範囲「0x80001000-0x800012FF」は、安全ユニットID「0x30」のアプリケーションへの、「read」種別のみのアクセスを提供する。したがって、比較すると、組み込みECUシステム101は、第1のプロセッサのセット107₁からのアクセス要求を、承認されるとして報告し得る。要求は、「0x80001000-0x800012FF」のメモリアドレス範囲について許可されている、「R」アクセス種別へのものだからである。

[0037] 図5は、本開示のいくつかの実施形態による、異種非対称システムのための、混在する重要な機能を管理する方法を示す、フローチャートを示す。

[0038] 図5に示すように、方法500は、異種非対称システムのための、混在する重要な機能の管理に関する1つまたは複数のブロックを含む。方法500は、コンピュータ実行可能命令の一般的な文脈で説明されてもよい。一般に、コンピュータ実行可能命令は、特定の機能を実行し、または特定の抽象データ型を実装する、ルーチン、プログラム、オブジェクト、構成要素、データ構造、手順、モジュール、および機能を含むことができる。

[0039] 方法500が記載される順序は、限定として解釈されることが意図されておらず、任意の数の記載される方法ブロックを、任意の順序で組み合わせて、本方法を実装することができる。加えて、個々のブロックは、本明細書で説明される発明の範囲から逸脱することなく、本方法から削除されてもよい。さらにまた、本方法は、任意の適切なハードウェア、ソフトウェア、ファームウェア、またはそれらの組み合わせで実装されることができる。

[0040] ブロック501で、複数のプロセッサ107は、分割モジュール211によって、第1のプロセッサのセット107₁および第2のプロセッサのセット107₂に分割される。

[0041] ブロック503で、第1のプロセッサのセット107₁の安全性設定値が、抽出モジュール213によって抽出される。安全性設定値は、分割中に生成される。第1のプロセッサのセット107₁の安全性設定値は、信頼されている安全性設定値に基づいて検証され、検証の結果に基づいて、第1のプロセッサのセット107₁は、システム資源113にアクセスする。第1のプロセッサのセット107₁の安全性設定値は、送信モジュール215によって、第2のプロセッサのセット107₂に送信される。一実施形態では、組み込みECUシステム101に関連付けられた外部検証モジュールは、第1のプロセッサのセット107₁の安全性設定値を確認してもよい。

[0042] [コンピューティングシステム]

図6は、本開示と一致する実施形態を実装するための、例示的なコンピュ

ータシステム600のブロック図を示す。一実施形態では、コンピュータシステム600は、組み込みECUシステム101を実装するために使用されてもよい。コンピュータシステム600は、中央処理装置（「CPU」または「プロセッサ」）602を含んでもよい。プロセッサ602は、異種非対称システムのための、混在する重要な機能を管理するための少なくとも1つのデータプロセッサを含んでもよい。プロセッサ602は、統合システム（バス）コントローラ、メモリ管理制御ユニット、浮動小数点ユニット、グラフィックス処理ユニット、デジタル信号処理ユニットなどの、特化した処理装置を含んでもよい。

[0043] プロセッサ602は、I/Oインターフェース601を介して、1つまたは複数の入出力（I/O）デバイス（図示せず）と通信するように配置されてもよい。I/Oインターフェース601には、限定するものではないが、オーディオ、アナログ、デジタル、monoaural、RCA、ステレオ、IEEE（登録商標）-1394、シリアルバス、ユニバーサルシリアルバス（universal serial bus、USB（登録商標））、赤外線、PS/2、BNC、同軸、コンポーネント、コンポジット、デジタルビジュアルインターフェイス（digital visual interface、DVI）、高精細度マルチメディアインターフェイス（high-definition multimedia interface、HDMI（登録商標））、RFアンテナ、S映像、VGA、IEEE（登録商標）802. n/b/g/n/x、Bluetooth（登録商標）、セルラー式（例えば、符号分割多重アクセス（code-division multiple access、CDMA）、高速パケットアクセス（high-speed packet access、HSPA+）、汎欧州デジタル移動体通信システム（global system for mobile communications、GSM（商標））、long-term evolution（LTE（商標））、WiMax（商標）など）その他などの、通信プロトコル／通信方法を採用してもよい。

[0044] I/Oインターフェース601を使用して、コンピュータシステム600は、1つまたは複数のI/Oデバイスと通信し得る。例えば、入力デバイスは、アンテナ、キーボード、マウス、ジョイスティック、（赤外線）リモコン、カメラ、カードリーダー、FAX機、 dongle、バイオメトリックリーダー、マイク、タッチスクリーン、タッチパッド、トラックボール、スタイラス、スキャナー、記憶装置、トランシーバ、ビデオデバイス／ビデオソースなどであってよい。出力デバイスは、プリンタ、FAX機、ビデオディスプレイ（例えば、ブラウン管（cathode ray tube、CRT）、液晶ディスプレイ（liquid crystal display、LCD）、発光ダイオード（light-emitting diode、LED（商標））、プラズマ、プラズマディスプレイパネル（Plasma display panel、PDP）、有機発光ダイオードディスプレイ（Organic light-emitting diode display、OLED）など）、オーディオスピーカーなどであってよい。

[0045] いくつかの実施形態では、コンピュータシステム600は、組み込みECUシステム101からなる。プロセッサ602は、ネットワークインターフェース603を介して、通信ネットワーク609と通信するように配置されてもよい。ネットワークインターフェース603は、通信ネットワーク609と通信してもよい。ネットワークインターフェース603は、直接接続、イーサネット（例えば、ツイストペア10／100／1000 Base T）、伝送制御プロトコル／インターネットプロトコル（transmission control protocol／internet protocol、TCP／IP）、トークンリング、IEEE（登録商標）802.11a／b／g／n／xなどを非限定的に含む、接続プロトコルを採用してもよい。通信ネットワーク609には、直接相互接続、ローカルエリアネットワーク（local area network、LAN）、ワイドエリアネットワーク（wide area network、WAN）、無線ネットワーク（例えば、無線アプリケーションプロトコルを使用する）、

インターネットなどが非限定的に含まれてよい。ネットワークインターフェース603は、直接接続、イーサネット（例えば、ツイストペア10/100/1000Base T）、伝送制御プロトコル/インターネットプロトコル（TCP/IP）、トークンリング、IEEE（登録商標）802.11a/b/g/n/xなどを含むがこれらに限定されない、接続プロトコルを採用してもよい。

[0046] 通信ネットワーク609には、直接相互接続、電子商取引ネットワーク、ピアツーピア（peer to peer、P2P）ネットワーク、ローカルエリアネットワーク（LAN）、ワイドエリアネットワーク（WAN）、無線ネットワーク（例えば、無線アプリケーションプロトコルを使用する）、インターネット、Wi-Fiなどが含まれるが、これらに限定されない。第1のネットワークおよび第2のネットワークは、専用ネットワークか、または共有ネットワークであり得、相互に通信するために、例えば、ハイパーテキスト転送プロトコル（Hypertext Transfer Protocol、HTTP）、伝送制御プロトコル/インターネットプロトコル（TCP/IP）、無線アプリケーションプロトコル（Wireless Application Protocol、WAP）などの種々のプロトコルを使用する、様々な種類のネットワークの関連付けを表す。さらに、第1のネットワークおよび第2のネットワークには、ルータ、ブリッジ、サーバ、コンピューティングデバイス、記憶装置などを含む、種々のネットワークデバイスが含まれてもよい。

[0047] いくつかの実施形態では、プロセッサ602は、記憶インターフェース604を介して、メモリ605（例えば、図6に示されていない、RAM、ROMなど）と通信するように配置されてもよい。記憶インターフェース604は、シリアルアドバンスドテクノロジーアタッチメント（serial advanced technology attachment、SATA（登録商標））、インテグレイティドドライブエレクトロニクス（Integrated Drive Electronics、IDE）、IEEE

E（登録商標）－1394、ユニバーサルシリアルバス（USB（登録商標））、ファイバーチャネル、小型計算機システムインターフェース（Small Computer Systems Interface、SCSI）その他などの接続プロトコルを採用して、メモリドライブ、リムーバブルディスクドライブなどを、これらに限定することなく含む、メモリ605に接続してもよい。メモリドライブは、ドラム、磁気ディスクドライブ、光磁気ドライブ、光学ドライブ、レイド（Redundant Array of Independent Discs、RAID）、ソリッドステートメモリデバイス、ソリッドステートドライブなどをさらに含んでもよい。

[0048] メモリ605は、ユーザーインターフェース606、オペレーティングシステム607などを非限定的に含む、プログラムまたはデータベースコンポーネントの集合を格納してもよい。いくつかの実施形態では、コンピュータシステム600は、本開示で説明されるように、データ、変数、レコードその他などの、ユーザー／アプリケーションデータ606を格納してもよい。そのようなデータベースは、オラクルまたはサイベースなどの、フォールトトレラントであり、スケーラブルで安全なリレーショナルデータベースとして実装されてよい。

[0049] オペレーティングシステム607は、コンピュータシステム600の資源管理および運用を容易にし得る。オペレーティングシステムの例には、APPLE MACINTOSH（登録商標）OS X、UNIX（登録商標）、UNIXライクなシステムディストリビューション（例えば、BERKELEY SOFTWARE DISTRIBUTION（商標）（BSD）、FREEBSD（商標）、NETBSD（商標）、OPENBSD（商標）など）、LINUX DISTRIBUTIONS（商標）（例えば、RED HAT（商標）、UBUNTU（商標）、KUBUNTU（商標）など）、IBM（商標）OS/2、MICROSOFT（商標）WINDOWS（商標）（XP（商標）、VISTA（商標）／7／8、10など）、APPLE（登録商標）IOS（商標）、GOOGLE（登録商標）AND

ROID（商標）、BLACKBERRY（登録商標）OSなどが非限定的に含まれる。

[0050] いくつかの実施形態では、コンピュータシステム600は、ウェブブラウザ608の格納されたプログラムコンポーネントを実装してもよい。ウェブブラウザ608は、ハイパーテキスト閲覧アプリケーション、例えば、MICROSOFT（登録商標）INTERNET EXPLORER（商標）、GOOGLE（登録商標）CHROME（商標）、MOZILLA（登録商標）FIREFOX（商標）、APPLE（登録商標）SAFARI（商標）などであってよい。安全なウェブブラウジングは、セキュアハイパーテキスト転送プロトコル（Secure Hypertext Transport Protocol、HTTPS）、セキュアソケットレイヤー（Secure Sockets Layer、SSL）、トランスポートレイヤーセキュリティ（Transport Layer Security、TLS）などを使用して提供され得る。ウェブブラウザ608は、AJAX（商標）、DHTML（商標）、ADOBE（登録商標）FLASH（商標）、JAVASCRIPT（商標）、JAVA（商標）、アプリケーションプログラミングインターフェース（Application Programming Interface、API）その他などの機能を利用してもよい。いくつかの実施形態では、コンピュータシステム600は、メールサーバーの格納されたプログラムコンポーネントを実装してもよい。メールサーバーは、Microsoft Exchangeその他などの、インターネットメールサーバーであってもよい。メールサーバーは、ASP（商標）、ACTIVEX（商標）、ANSI（商標）C++／C＃、MICROSOFT（登録商標）、.NET（商標）、CGI SCRIPTS（商標）、JAVA（商標）、JAVASCRIPT（商標）、PERL（商標）、PHP（商標）、PYTHON（商標）、WEBOBJECTS（商標）その他などの、機能を利用してもよい。メールサーバーは、インターネットメッセージアクセスプロトコル（Internet Message Ac

cess Protocol、IMAP)、メッセージングアプリケーションプログラミングインターフェース(Messaging Application Programming Interface、MAPI)、MICROSOFT(登録商標)exchange、ポストオフィスプロトコル(POP)、簡易メール転送プロトコル(Simple Mail Transfer Protocol、SMTP)その他などの、通信プロトコルを利用してよい。いくつかの実施形態では、コンピュータシステム600はメールクライアントの格納されたプログラムコンポーネントを実装してもよい。メールクライアントは、APPLE(登録商標)MAIL(商標)、MICROSOFT(登録商標)ENTOURAGE(商標)、MICROSOFT(登録商標)OUTLOOK(商標)、MOZILLA(登録商標)THUNDERBIRD(商標)その他などの、メール閲覧アプリケーションであってよい。

[0051] さらにまた、本開示と一致する実施形態を実装することにおいて、1つまたは複数のコンピュータ読み取り可能記憶媒体が、利用されてもよい。コンピュータ読み取り可能記憶媒体は、プロセッサによって読み取り可能な情報またはデータが格納され得る、任意の種類の物理メモリを指す。したがって、コンピュータ読み取り可能記憶媒体は、本明細書で説明される実施形態と一致するステップまたは段階を、プロセッサに実行させるための命令を含む、1つまたは複数のプロセッサが、実行するための命令を格納し得る。「コンピュータ読み取り可能媒体」という用語は、有形のものを含み、搬送波および一時的な信号を除外する、つまり非一時的であると理解されるべきである。例としては、ランダムアクセスメモリ(Random Access Memory、RAM)、読み出し専用メモリ(Read-Only Memory、ROM)、揮発性メモリ、不揮発性メモリ、ハードドライブ、CD ROM、DVD、フラッシュドライブ、ディスク、およびその他の知られている任意の物理記憶媒体が挙げられる。

[0052] 本開示の一実施形態は、処理能力の向上とともに機能安全基準を満たす必

要がある、自動車、工業用制御などの分野で使用されてもよい。

[0053] 本開示の実施形態は、安全性非適合システム構成要素がもたらす悪影響による、高信頼性エンティティの安全動作の妨害を抑えることにより、信頼性を高める。

[0054] 本開示の実施形態は、利用可能な構成要素の設計および開発のコストを削減する。

[0055] 本開示の一実施形態には、異種のソフトウェアおよびハードウェア構成要素の改良を強化するための、安全性ファームウェアおよび検証技術が含まれる。

[0056] 説明される動作は、ソフトウェア、ファームウェア、ハードウェア、またはそれらの任意の組み合わせを作り出すための標準的なプログラミングおよび／またはエンジニアリングの技術を用いて、方法、システムまたは製造物品として実装されてもよい。説明される動作は、「非一時的なコンピュータ読み取り可能媒体」に保持されるコードとして実装されてもよい。そこでは、プロセッサが、そのコンピュータ読み取り可能媒体からそのコードを読み取って実行し得る。プロセッサは、クエリを処理および実行できるマイクロプロセッサおよびプロセッサのうち少なくとも1つである。非一時的なコンピュータ読み取り可能媒体には、磁気記憶媒体（例えば、ハードディスクドライブ、フロッピーディスク、テープなど）、光学記憶（CD-ROM、DVD、光ディスクなど）、揮発性メモリデバイスおよび非揮発性メモリデバイス（例えば、EEPROM、ROM、PROM、RAM、DRAM、SRAM、フラッシュメモリ、ファームウェア、プログラマブルロジックなど）その他などの、媒体が含まれてもよい。さらに、非一時的なコンピュータ読み取り可能媒体には、一時的なものを除くすべてのコンピュータ読み取り可能媒体が含まれる。説明される動作を実装するコードは、さらに、ハードウェアロジック（例えば、集積回路チップ、プログラマブルゲートアレイ（Programmable Gate Array、PGA）、特定用途向け集積回路（ASIC）など）で実装されてもよい。

[0057] またさらに、説明される動作を実装するコードは、「伝送信号」で実装されてもよく、伝送信号は、空間を介して、または光ファイバ、銅線その他のなどの伝送媒体を介して伝播してもよい。コードまたはロジックがエンコードされた伝送信号には、無線信号、衛星伝送、電波、赤外線信号、Bluetoothなどが、さらに含まれてもよい。コードまたはロジックがエンコードされた伝送信号は、送信局によって送信され、受信局によって受信されることができる。伝送信号内にエンコードされたコードまたはロジックは、受信局および送信局または受信デバイスおよび送信デバイスで、デコードされて、ハードウェアまたは非一時的なコンピュータ読み取り可能媒体に格納されてもよい。「製造物品」には、コードが実装され得る、非一時的なコンピュータ読み取り可能媒体、ハードウェアロジック、および／または伝送信号が含まれる。説明される動作の実施形態を実装するコードが、エンコードされる、デバイスには、コンピュータ読み取り可能媒体またはハードウェアロジックが含まれてもよい。もちろん、当業者は、本発明の範囲から逸脱することなく、この構成に多くの変更がされ得ること、および製造物品には、当技術分野で知られている適切な情報伝達媒体が含まれてもよいことを認識するであろう。

[0058] 用語「実施形態 (an embodiment)」、「実施形態 (embodiment)」、「実施形態 (embodiments)」、「実施形態 (the embodiment)」、「実施形態 (the embodiments)」、「1つ又は複数の実施形態」、「いくつかの実施形態」、および「一実施形態」は、別途明示的に規定しない限り、「1つ又は複数の (ただし、すべてではない) 本発明の実施形態」を意味する。

[0059] 用語「含む (including)」、「含む (comprising)」、「有する (備える) (having)」およびそれらの変形は、別途明示的に規定しない限り、「含むがこれらに限定されない」を意味する。

[0060] 列挙される事項のそれら列記は、別途明示的に規定しない限り、それらの事項のいずれかまたはすべてが、相互に排他的であることを含意しない。

- [0061] 用語「a」、「an」、および「the」は、別途明示的に規定しない限り、「1つ又は複数の」を意味する。
- [0062] 互いに通信するいくつかの構成要素をとまなう実施形態の記載は、すべてのそのような構成要素が必要であることを含意しない。逆に、本発明の幅広い種々の可能な実施形態を例示するために、種々の任意の構成要素が記載されている。
- [0063] 本明細書で単一のデバイスまたは物品が説明される場合、単一のデバイス／物品の代わりに、1つより多くのデバイス／物品が、（それらが協働するかどうかにかかわらず）使用され得ることが、容易に分かるであろう。同様に、本明細書で1つより多くのデバイスまたは物品が説明される場合（それらが協働するかどうかにかかわらず）、1つより多くのデバイスもしくは物品の代わりに、単一のデバイス／物品が使用され得、または、示されている数のデバイスもしくはプログラムの代わりに、異なる数のデバイス／物品が使用され得ることが、容易に分かるであろう。デバイスの機能および／または特徴は、そのような機能／特徴を有するものとして明示的に説明されていない、1つまたは複数の他のデバイスによって代わりに具現されてもよい。したがって、本発明の他の実施形態は、デバイスそれ自体を含む必要はない。
- [0064] 図5に示される動作は、特定の順序で起きる、特定のイベントを示す。別の実施形態では、特定の動作が、異なる順序で実行され、変更され、または削除されてもよい。その上さらに、上記のロジックにステップが追加されてもよく、それでもなお、説明される実施形態に適合する。さらに、本明細書で説明される動作は、連続して起きる場合があり、または特定の動作が、並行して処理される場合がある。またさらに、動作は、単一の処理ユニットまたは分散処理ユニットによって実行されてもよい。
- [0065] 最後に、本明細書で使用される言葉は、主として読みやすさと教示的な目的のために選択されているものであり、発明を明確に記述し、または発明の範囲を定めるために選択されているものではない場合がある。それ故、本発

明の範囲は、この詳細な説明によってではなく、本明細書に基づいた出願で発行される、任意の請求項によって限定されることが、意図されている。したがって、本発明の実施形態の開示は、以下の請求項に記載される本発明の範囲を、限定することなく例示することが意図されている。

[0066] 本明細書では様々な態様および実施形態が開示されているが、他の態様および実施形態は、当業者に明らかであろう。本明細書で開示される様々な態様および実施形態は、例示を目的とするものであり、限定的であることは意図されておらず、真の範囲および精神は、以下の請求項によって示される。

符号の説明

[0067] 100…環境、101…組み込みECUシステム、103…I/Oインターフェース、105…メモリ、107…プロセッサ、107_{1N}…第1のプロセッサのセットのプロセッサ、107_{2N}…第2のプロセッサのセットのプロセッサ、113…システム資源、115_{1N}…第1のプロセッサのセットの安全性モジュール、115_{2N}…第2のプロセッサのセットの安全性モジュール、200…データ、201…分割データ、203…安全性設定データ、205…検証データ、207…その他のデータ、209…モジュール、211…分割モジュール、213…抽出モジュール、215…送信モジュール、217…その他のモジュール、301…プロセッサ、302…プロセッサ、303…安全性モジュール、305…分割用モジュール、307…抽出モジュール、309…第1のアプリケーション、311…第2のアプリケーション、312…アプリケーション、313…安全性モジュール、315…検証モジュール、316…安全性検証エンジン、317…Software、318…安全性ミドルウェア、600…コンピュータシステム、601…I/Oインターフェース、602…プロセッサ、603…ネットワークインターフェース、604…記憶インターフェース、605…メモリ、606…ユーザーインターフェース、607…オペレーティングシステム、608…ウェブブラウザ

請求の範囲

- [請求項1] 複数のプロセッサを備える組み込みE C Uシステムであって、
前記複数のプロセッサを、第1のプロセッサのセットと第2のプロセッサのセットとに分割するための分割モジュールと、
前記第1のプロセッサのセットの安全性設定値を抽出するための抽出モジュールと、を含み、
前記安全性設定値は、前記分割中に生成され、
前記第1のプロセッサのセットの前記安全性設定値は、信頼されている安全性設定値に基づいて検証され、
前記第1のプロセッサのセットは、前記検証の結果に基づいてシステム資源にアクセスする、
複数のプロセッサを備える組み込みE C Uシステム。
- [請求項2] 前記第1のプロセッサのセットは、前記分割に基づいて、前記第2のプロセッサのセットから前記安全性設定値を受信し、各メモリ管理ユニット（MMU）の前記安全性設定値を設定する、
請求項1に記載の組み込みE C Uシステム。
- [請求項3] 前記安全性設定値を前記第2のプロセッサのセットに送信するための送信モジュールを備える、
請求項1に記載の組み込みE C Uシステム。
- [請求項4] 前記第2のプロセッサのセットの前記信頼されている安全性設定値に基づいて、前記第1のプロセッサのセットの前記安全性設定値を確認するための、前記組み込みE C Uシステムの外部に存在する検証モジュールを備える、
請求項1に記載の組み込みE C Uシステム。
- [請求項5] 前記第2のプロセッサのセットの前記信頼されている安全性設定値に基づいて、前記第1のプロセッサのセットの前記安全性設定値を確認するための、前記組み込みE C Uシステムに関連付けられた外部検証モジュールを備える、

請求項 1 に記載の組み込み E C U システム。

[請求項6] 前記第 1 のプロセッサのセットは、前記安全性設定値を、前記第 2 のプロセッサのセットの前記信頼されている安全性設定値と比較することにより検証される、

請求項 1 に記載の組み込み E C U システム。

[請求項7] 前記安全性設定値は、前記第 1 のプロセッサのセットのアクセスを許可する範囲を含み、前記信頼されている安全性設定値は、複数のレベルによって分類されたアクセスを許可する範囲を含む、

請求項 1 に記載の組み込み E C U システム。

[請求項8] 前記第 1 のプロセッサのセットの各プロセッサは、低信頼性プロセッサであり、前記第 2 のプロセッサのセットの各プロセッサは、高信頼性プロセッサである、

請求項 1 に記載の組み込み E C U システム。

[請求項9] 請求項 1 に記載の組み込み E C U システムは、最高の特権レベルで、安全性モジュールのインスタンスを実行する。

[請求項10] 前記検証の結果に基づいて前記第 1 のプロセッサのセットにアクセスを提供するための、前記組み込み E C U システムに関連付けられたアクセスユニットを備える、

請求項 1 に記載の組み込み E C U システム。

[請求項11] 請求項 1 に記載の組み込み E C U システムは、前記検証の前記結果に基づいて、要求されたメモリ位置へのアクセスを前記第 1 のプロセッサのセットに提供することを含む。

[請求項12] 請求項 1 に記載の組み込み E C U システムは、前記検証の前記結果に基づいて、メモリ位置上の書き込み可能および書き換え不能のステータスについて前記第 1 のプロセッサのセットに通知することを含む。

[請求項13] 異種非対称システムのための、混在する重要な機能を管理するための方法であって、

組み込みECUシステムにより、複数のプロセッサを、第1のプロセッサのセットと第2のプロセッサのセットとに分割することと、

前記組み込みECUシステムにより、前記第1のプロセッサのセットの安全性設定値を抽出することと、を含み、

前記安全性設定値は、前記分割中に生成され、

前記第1のプロセッサのセットの前記安全性設定値は、信頼されている安全性設定値に基づいて検証され、

前記第1のプロセッサのセットは、前記検証の結果に基づいてシステム資源にアクセスする、

異種非対称システムのための、混在する重要な機能を管理するための方法。

[請求項14] 前記第1のプロセッサのセットは、前記分割に基づいて、前記第2のプロセッサのセットから前記安全性設定値を受信し、各メモリ管理ユニット(MMU)の前記安全性設定値を設定する、
請求項13に記載の方法。

[請求項15] 前記安全性設定値を前記第2のプロセッサのセットに送信すること
をさらに含む、
請求項13に記載の方法。

[請求項16] 前記第2のプロセッサのセットの前記信頼されている安全性設定値に基づいて、前記第1のプロセッサのセットの前記安全性設定値を確認するための、前記組み込みECUシステムの外部に存在する検証モジュールを備える、
請求項13に記載の方法。

[請求項17] 前記第2のプロセッサのセットの前記信頼されている安全性設定値に基づいて、前記第1のプロセッサのセットの前記安全性設定値を確認するための、前記組み込みECUシステムに関連付けられた外部検証モジュールを備える、
請求項13に記載の方法。

- [請求項18] 前記第1のプロセッサのセットの前記安全性設定値を検証することは、前記安全性設定値を、前記第2のプロセッサのセットの前記信頼されている安全性設定値と比較することを含む、
請求項13に記載の方法。
- [請求項19] 前記安全性設定値は、前記第1のプロセッサのセットのアクセスを許可する範囲を含み、前記信頼されている安全性設定値は、複数のレベルによって分類されたアクセスを許可する範囲を含む、
請求項13に記載の方法。
- [請求項20] 前記第1のプロセッサのセットの各プロセッサは、低信頼性プロセッサであり、前記第2のプロセッサのセットの各プロセッサは、高信頼性プロセッサである、
請求項13に記載の方法。
- [請求項21] 前記組み込みECUにより、最高の特権レベルで、安全性モジュールのインスタンスを実行することをさらに含む、
請求項13に記載の方法。
- [請求項22] 前記検証の前記結果に基づいて、要求されたメモリ位置への前記アクセスを前記第1のプロセッサのセットに提供することをさらに含む
請求項13に記載の方法。
- [請求項23] 前記検証の前記結果に基づいて、メモリ位置上の書き込み可能および書き換え不能のステータスについて前記第1のプロセッサのセットに通知することをさらに含む、
請求項13に記載の方法。
- [請求項24] 前記検証の結果に基づいて前記第1のプロセッサのセットにアクセスを提供するための、前記組み込みECUシステムに関連付けられたアクセスユニットを含む、
請求項13に記載の方法。

[図2]

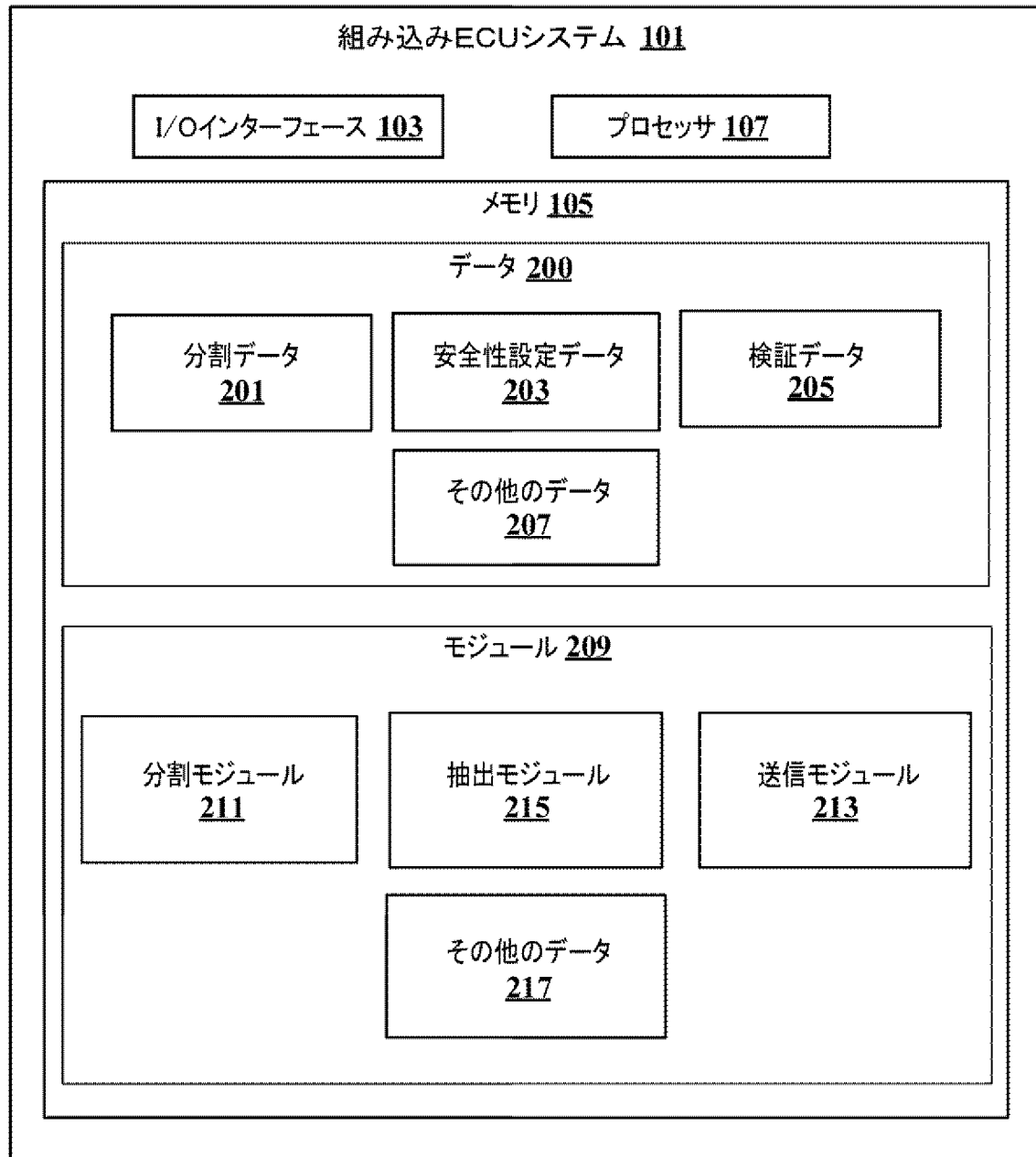


図2

[図3a]

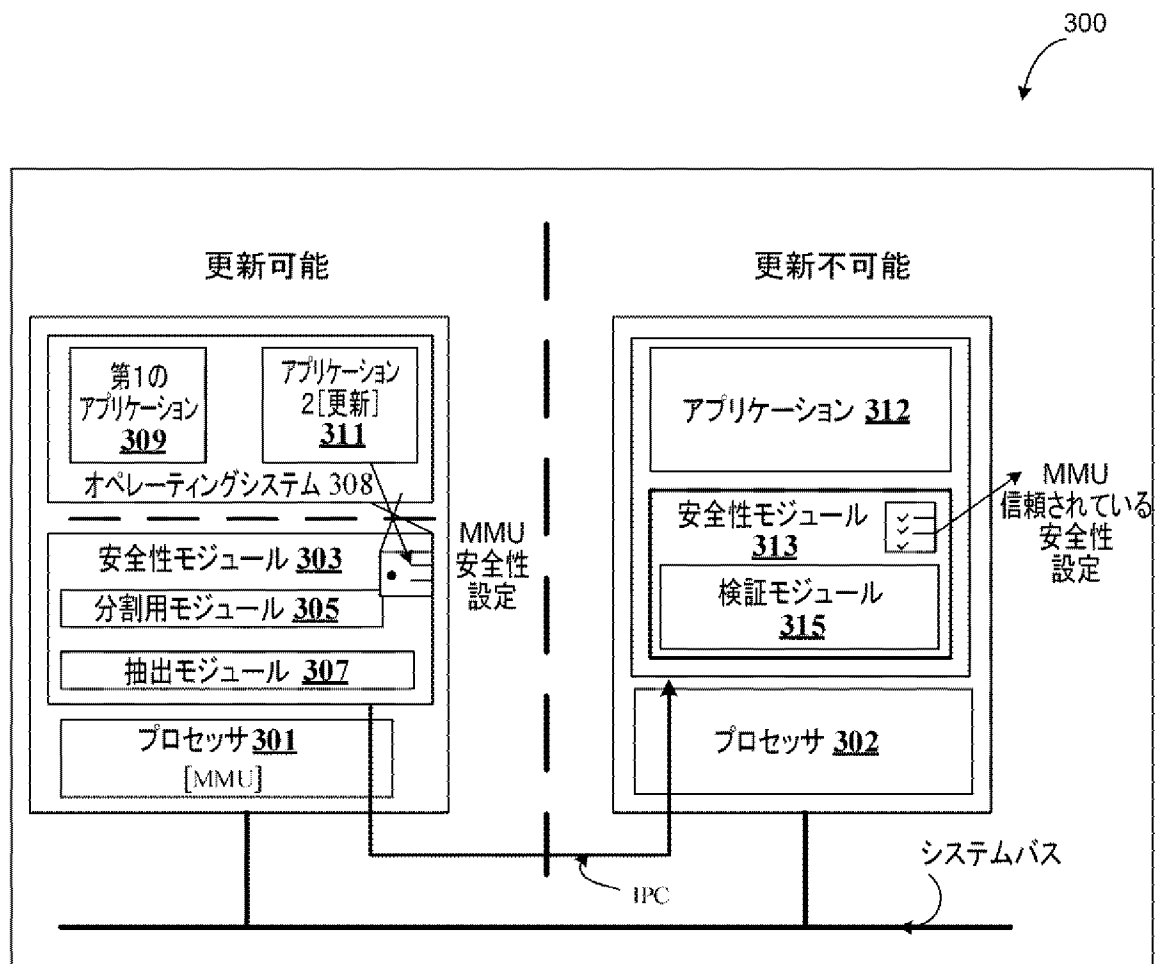


図3a

[図3b]

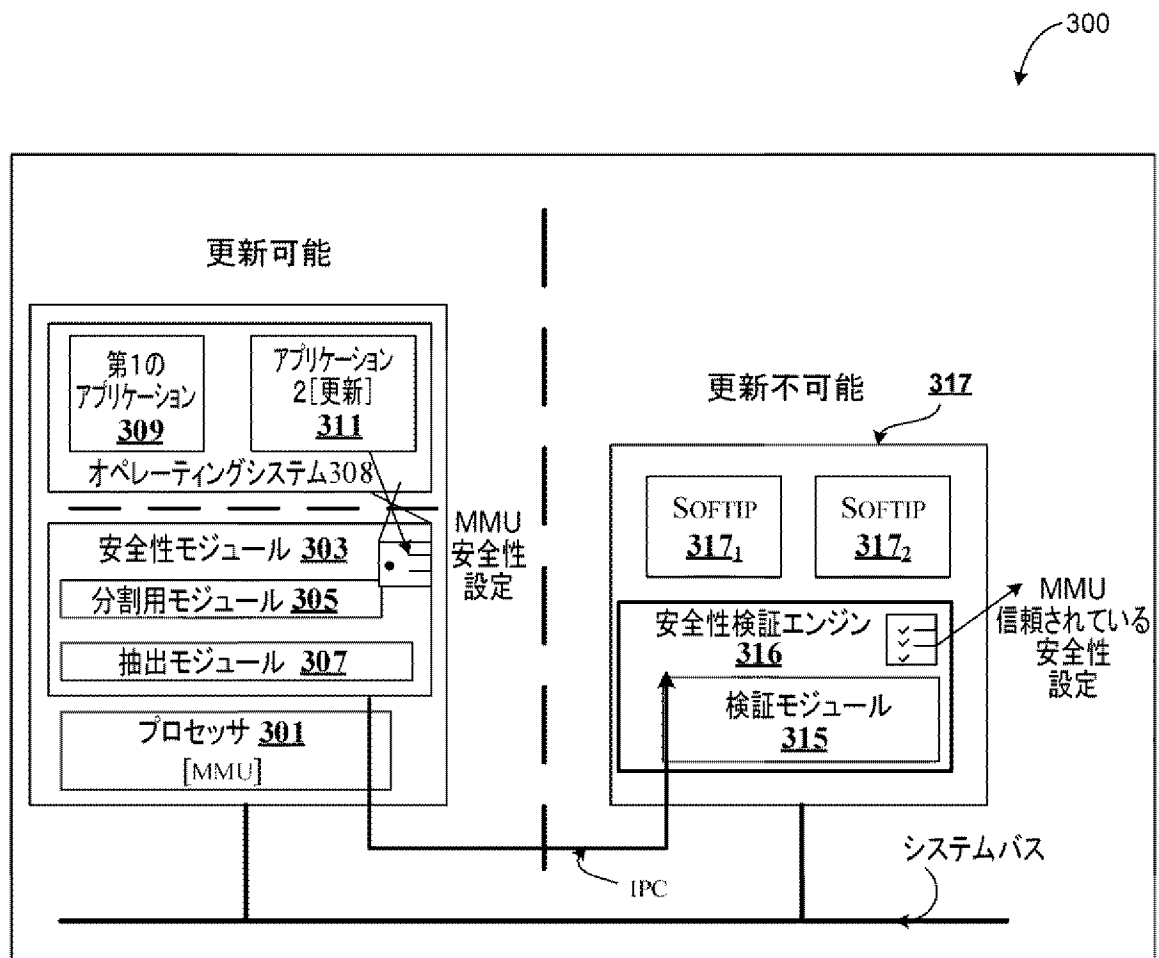


図3b

[図3c]

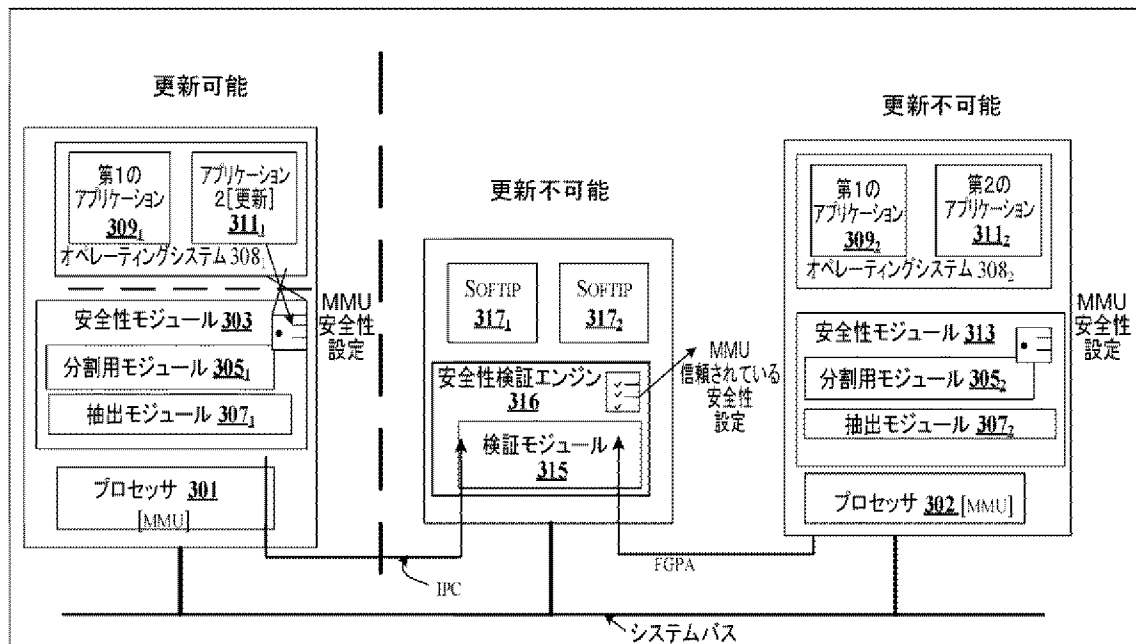


図3c

[図3d]

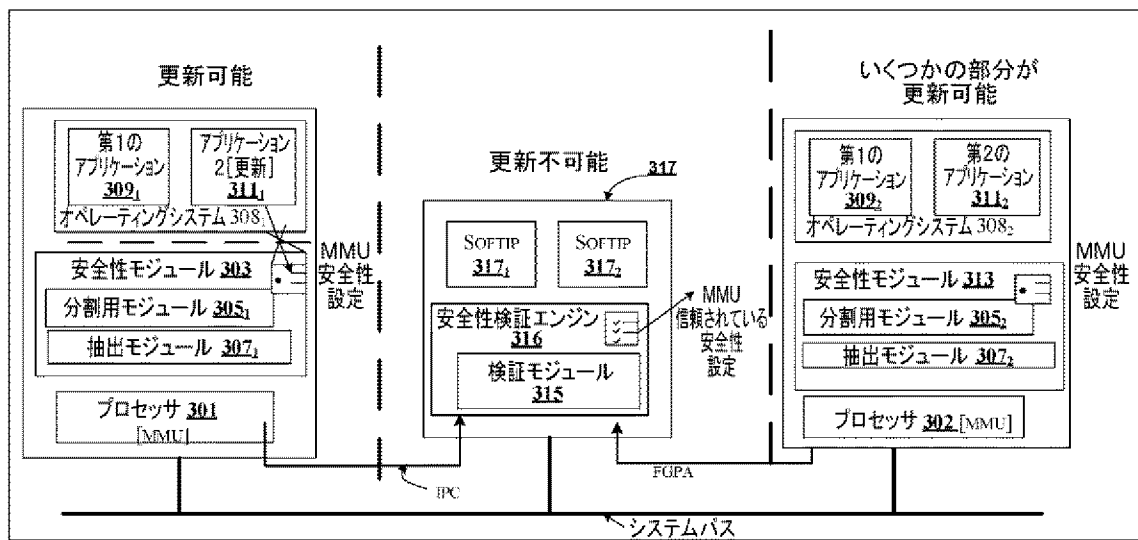


図3d

[図3e]

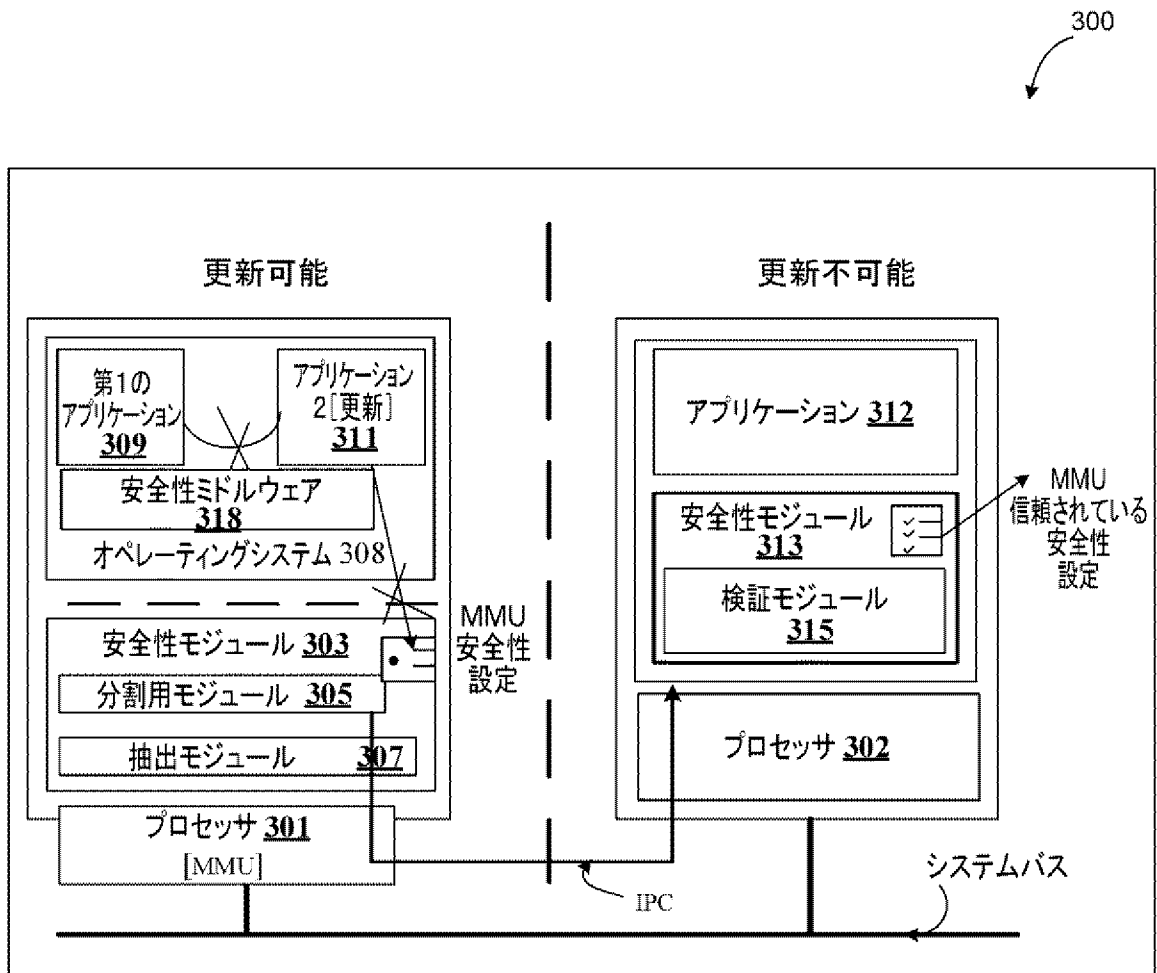


図3e

[図4a]

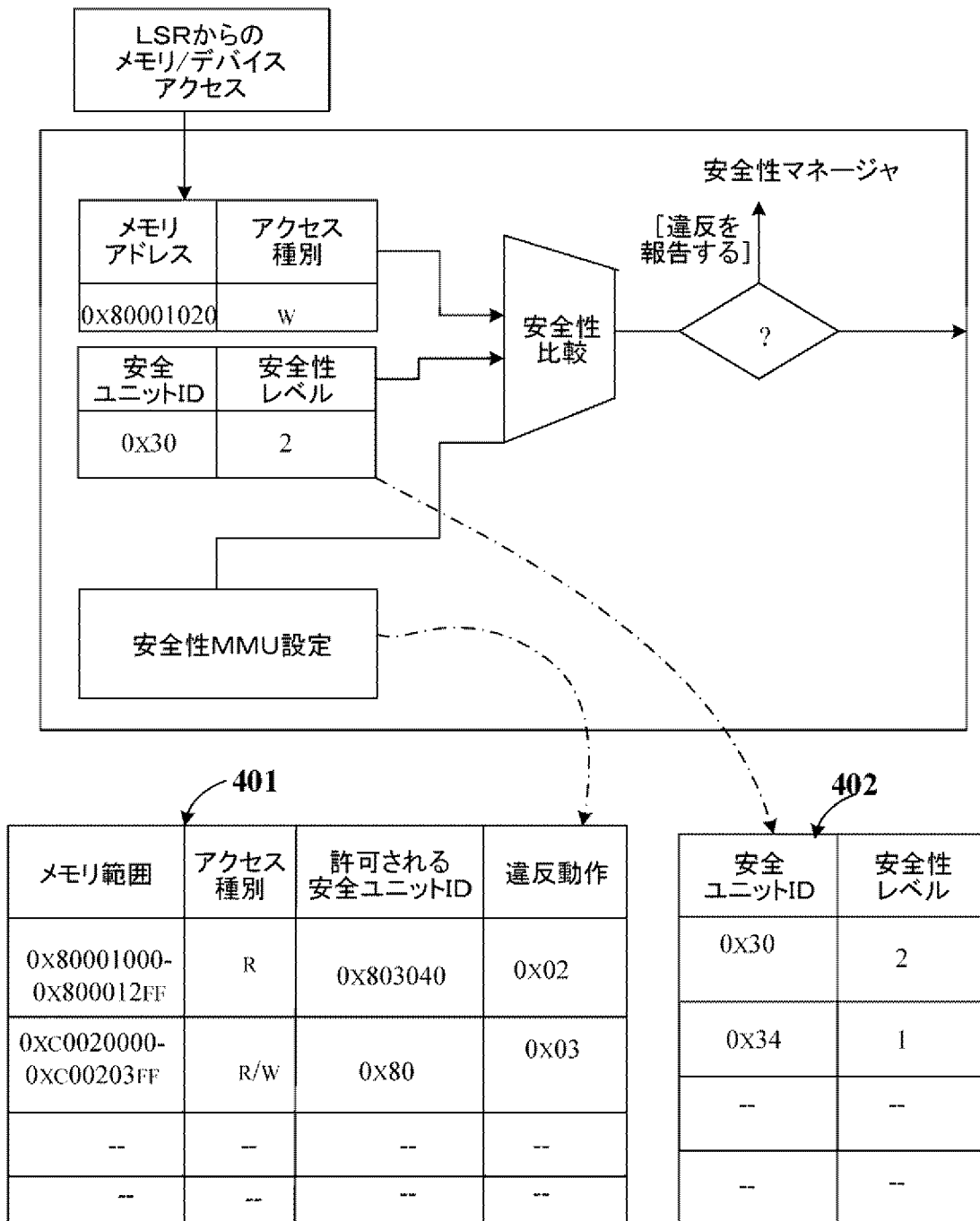


図4a

[図4b]

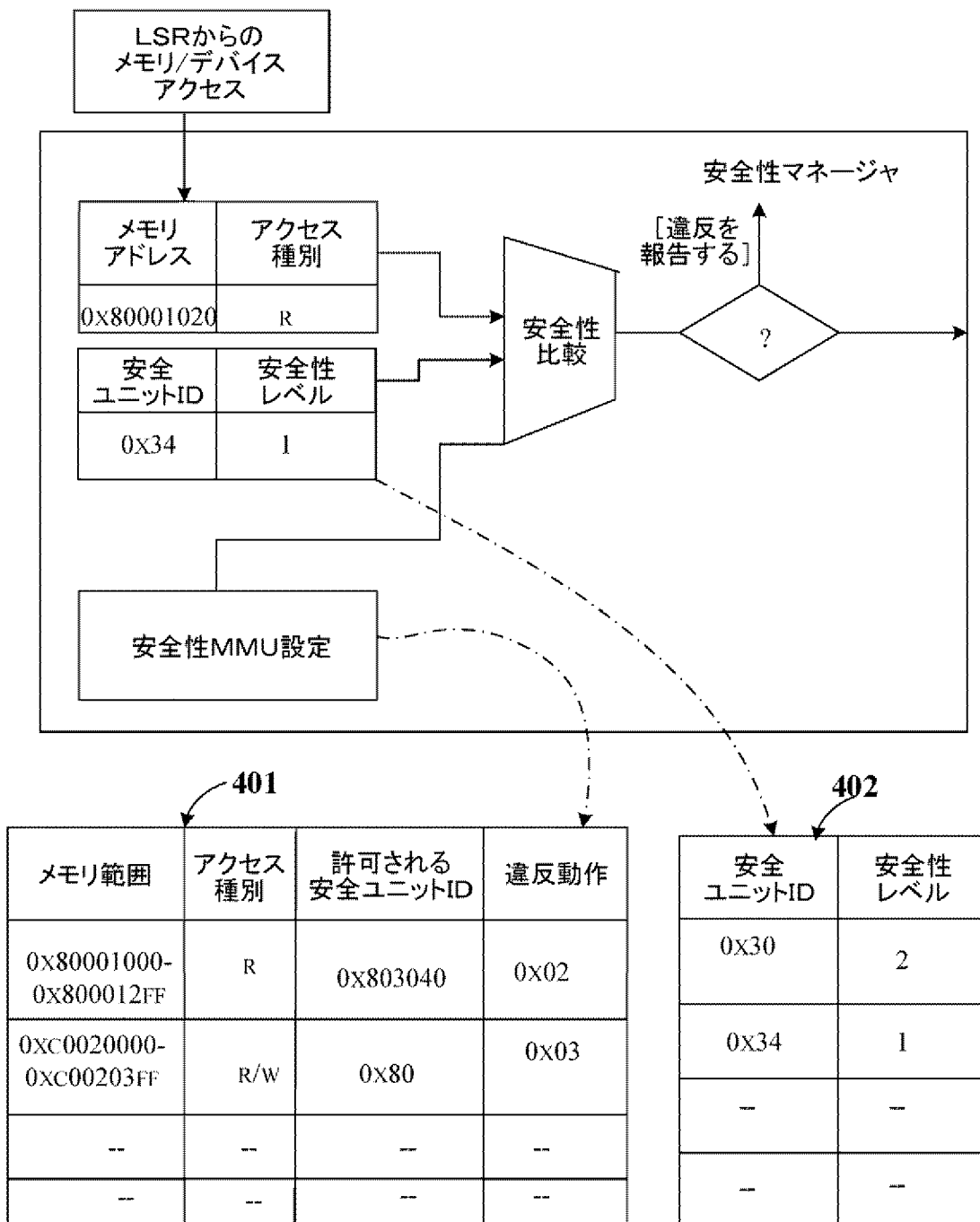


図4b

[図4c]

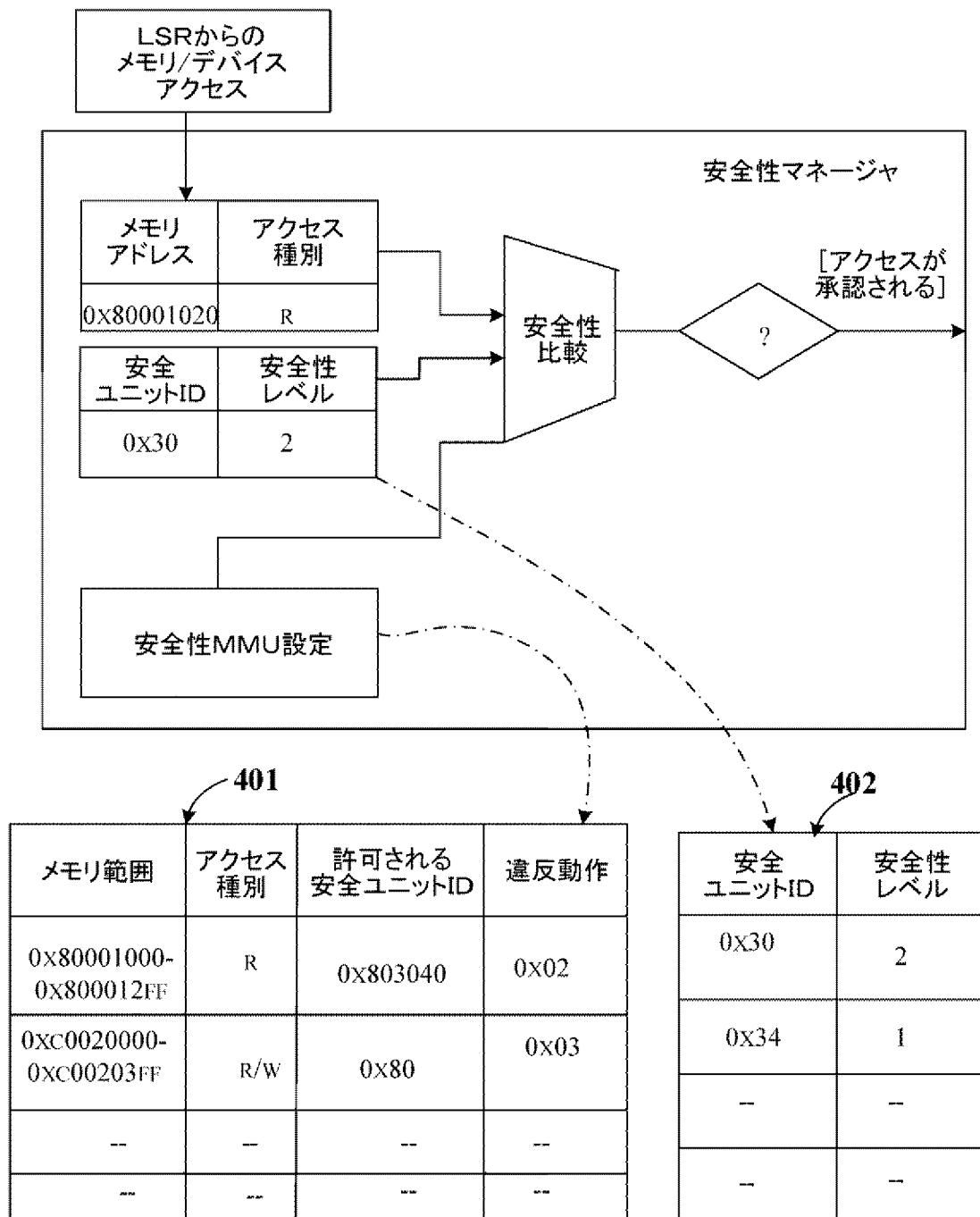


図4c

[図5]

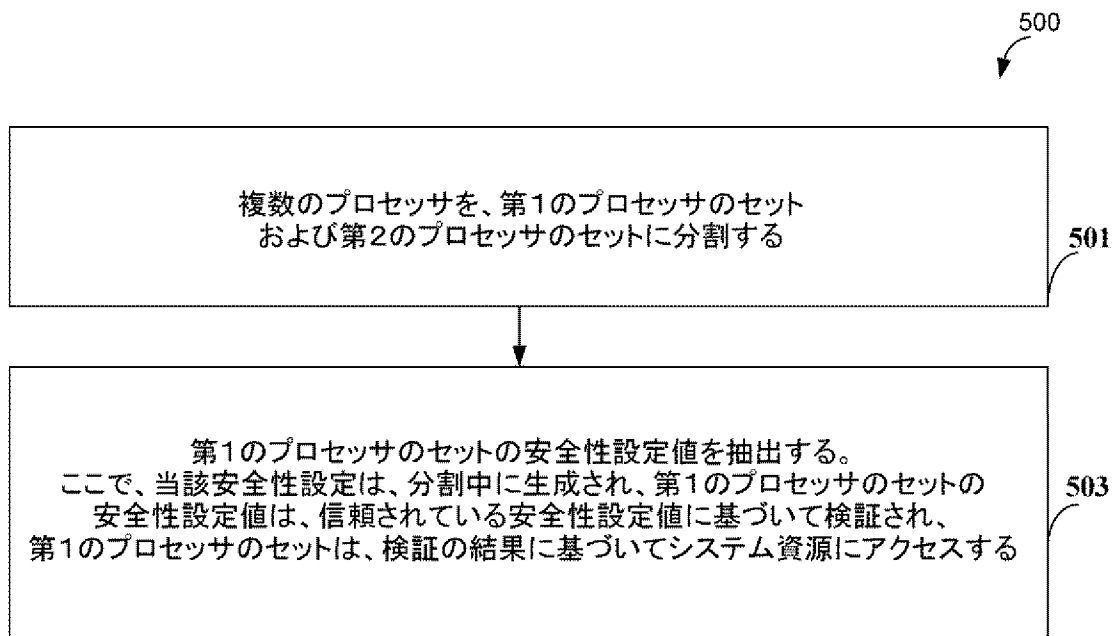


図5

[図6]

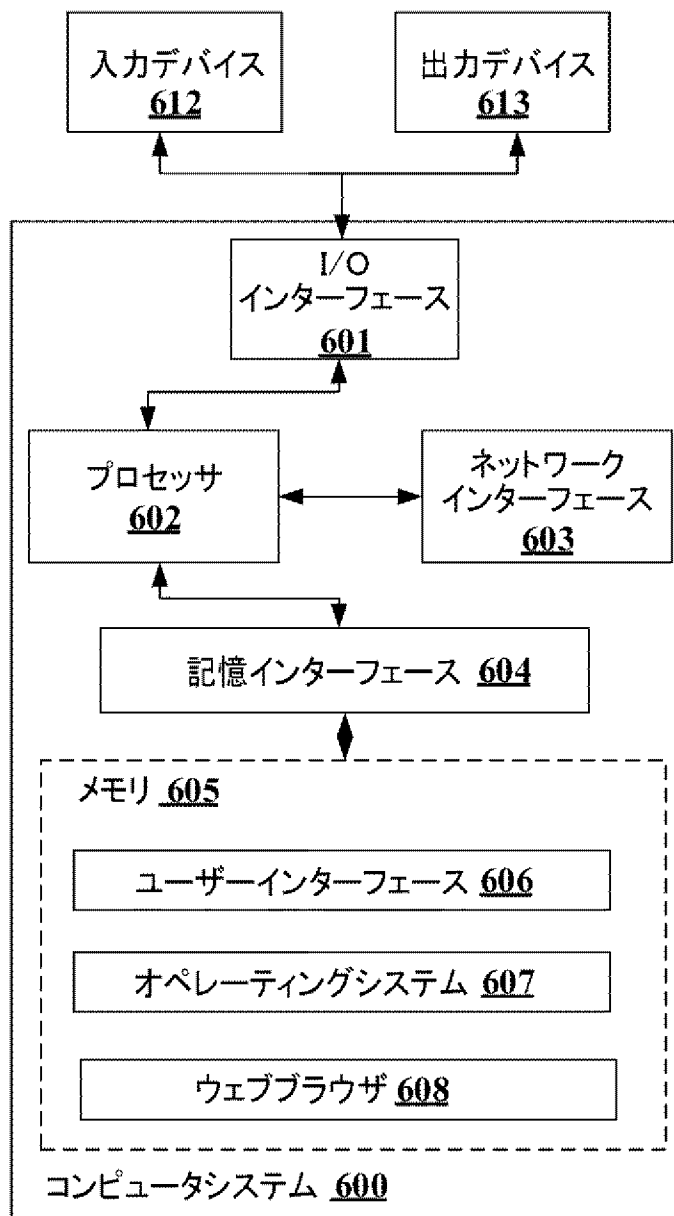


図6

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2020/003411

A. CLASSIFICATION OF SUBJECT MATTER

G06F 12/14(2006.01)i; B60W 50/04(2006.01)i
 FI: G06F12/14 510D; B60W50/04

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)

G06F12/14; B60W50/04; G06F15/167; G06F21/62

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

Published examined utility model applications of Japan	1922-1996
Published unexamined utility model applications of Japan	1971-2020
Registered utility model specifications of Japan	1996-2020
Published registered utility model applications of Japan	1994-2020

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.
A	JP 2011-70528 A (NEC CORP.) 07.04.2011 (2011-04-07)	1-24
A	WO 2017/056725 A1 (HITACHI AUTOMOTIVE SYSTEMS, LTD.) 06.04.2017 (2017-04-06)	1-24
A	DE 102018210418 A1 (DENSO CORPORATION) 17.01.2019 (2019-01-17)	1-24
A	US 2016/0259756 A1 (XILINX, INC.) 08.09.2016 (2016-09-08)	1-24



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

21 April 2020 (21.04.2020)

Date of mailing of the international search report

28 April 2020 (28.04.2020)

Name and mailing address of the ISA/

Japan Patent Office
 3-4-3, Kasumigaseki, Chiyoda-ku,
 Tokyo 100-8915, Japan

Authorized officer

Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.

PCT/JP2020/003411

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
JP 2011-70528 A	07 Apr. 2011	(Family: none)	
WO 2017/056725 A1	06 Apr. 2017	US 2018/0203823 A1	
		EP 3357761 A1	
		CN 108025685 A1	
DE 102018210418 A1	17 Jan. 2019	JP 2019-20895 A	
US 2016/0259756 A1	08 Sep. 2016	CN 105938466 A	

A. 発明の属する分野の分類（国際特許分類（IPC）） G06F 12/14(2006.01)i; B60W 50/04(2006.01)i FI: G06F12/14 510D; B60W50/04														
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）） G06F12/14; B60W50/04; G06F15/167; 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														
<table border="0"> <tr> <td>日本国実用新案公報</td> <td>1922 - 1996年</td> </tr> <tr> <td>日本国公開実用新案公報</td> <td>1971 - 2020年</td> </tr> <tr> <td>日本国実用新案登録公報</td> <td>1996 - 2020年</td> </tr> <tr> <td>日本国登録実用新案公報</td> <td>1994 - 2020年</td> </tr> </table>			日本国実用新案公報	1922 - 1996年	日本国公開実用新案公報	1971 - 2020年	日本国実用新案登録公報	1996 - 2020年	日本国登録実用新案公報	1994 - 2020年				
日本国実用新案公報	1922 - 1996年													
日本国公開実用新案公報	1971 - 2020年													
日本国実用新案登録公報	1996 - 2020年													
日本国登録実用新案公報	1994 - 2020年													
国際調査で使用了電子データベース（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												
A	JP 2011-70528 A（日本電気株式会社）07.04.2011（2011 - 04 - 07）	1-24												
A	WO 2017/056725 A1（日立オートモティブシステムズ株式会社）06.04.2017（2017 - 04 - 06）	1-24												
A	DE 102018210418 A1（DENSO CORPORATION）17.01.2019（2019 - 01 - 17）	1-24												
A	US 2016/0259756 A1（XILINX, INC.）08.09.2016（2016 - 09 - 08）	1-24												
☐ 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。														
<table border="0"> <tr> <td>* 参考文献のカテゴリー</td> <td>“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抵触するものではなく、発明の原理又は理論の理解のために引用するもの</td> </tr> <tr> <td>“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</td> <td>“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</td> </tr> <tr> <td>“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</td> <td>“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</td> </tr> <tr> <td>“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）</td> <td>“&” 同一パテントファミリー文献</td> </tr> <tr> <td>“O” 口頭による開示、使用、展示等に言及する文献</td> <td></td> </tr> <tr> <td>“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</td> <td></td> </tr> </table>			* 参考文献のカテゴリー	“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抵触するものではなく、発明の原理又は理論の理解のために引用するもの	“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	“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	“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	“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	“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）	“&” 同一パテントファミリー文献	“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	
* 参考文献のカテゴリー	“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抵触するものではなく、発明の原理又は理論の理解のために引用するもの													
“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	“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													
“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	“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													
“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）	“&” 同一パテントファミリー文献													
“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														
国際調査を完了した日 21.04.2020	国際調査報告の発送日 28.04.2020													
名称及びあて先 日本国特許庁(ISA/JP) 〒100-8915 日本国 東京都千代田区霞が関三丁目4番3号	権限のある職員（特許庁審査官） 金沢 史明 5S 4538 電話番号 03-3581-1101 内線 3546													

国際調査報告
 パテントファミリーに関する情報

国際出願番号

PCT/JP2020/003411

引用文献			公表日	パテントファミリー文献			公表日
JP	2011-70528	A	07.04.2011	(ファミリーなし)			
WO	2017/056725	A1	06.04.2017	US	2018/0203823	A1	
				EP	3357761	A1	
				CN	108025685	A1	
DE	102018210418	A1	17.01.2019	JP	2019-20895	A	
US	2016/0259756	A1	08.09.2016	CN	105938466	A	