

(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号
特許第7655729号
(P7655729)

(45)発行日 令和7年4月2日(2025.4.2)

(24)登録日 令和7年3月25日(2025.3.25)

(51)国際特許分類

F I

G 0 6 F 11/36 (2025.01)

G 0 6 F 11/3698

請求項の数 3 (全10頁)

(21)出願番号	特願2021-10304(P2021-10304)	(73)特許権者	509186579 日立Astemo株式会社 茨城県ひたちなか市高場2520番地
(22)出願日	令和3年1月26日(2021.1.26)	(74)代理人	110002572 弁理士法人平木国際特許事務所
(65)公開番号	特開2022-114138(P2022-114138 A)	(72)発明者	福元 和真 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
(43)公開日	令和4年8月5日(2022.8.5)	(72)発明者	福島 悠史 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
審査請求日	令和5年11月7日(2023.11.7)	審査官	新井 則和

最終頁に続く

(54)【発明の名称】 電子制御装置のシミュレーション装置

(57)【特許請求の範囲】

【請求項1】

車両制御装置の動作を汎用計算機上で模擬するシミュレーション装置であって、
試験を実行する試験実施用汎用計算機と、
前記試験を制御する試験制御用汎用計算機と
を備え、
前記試験実施用汎用計算機は、
安全度要求の異なる複数のアプリケーションを含むアプリケーション部と、
所定の場合に、前記複数のアプリケーションの動作の1つを終了させ、他のアプリケー
ションの動作を保証する負荷制御部と、
前記複数のアプリケーションによる不正アクセスを検知し、所定の処置を実行するメモ
リ操作部と、
前記複数のアプリケーションに関する保護機能を実現する保護機能部と、
を備え、
前記試験制御用汎用計算機は、
試験のシナリオを管理するシナリオ管理部と、
前記シナリオに基づき前記試験を指示する試験指示部と、
前記指示の内容に基づき試験データを生成するデータ制御部と、
を備え、
前記試験制御用汎用計算機から任意のタイミングで前記試験データを送信し、

前記試験実施用汎用計算機にて、前記試験データに従い、前記保護機能部における前記保護機能の動作を確認し、

前記試験制御用汎用計算機は、前記指示に基づき、メモリ保護違反、データ保護違反、時間保護違反の少なくとも１つの試験指示を前記試験実施用汎用計算機へ入力し、

前記データ保護違反の試験を実施する際、

前記試験指示部は、前記データ制御部に送信データのヘッダの情報の変更の指示を出し、

前記データ制御部は、前記指示の内容に基づき前記ヘッダの内容を変更し、その変更したデータを前記試験実施用汎用計算機へ送信し、前記保護機能部の動作試験を実施する、

ことを特徴とする、車両制御装置のシミュレーション装置。

【請求項２】

前記時間保護違反の試験を実施する際、

前記データ制御部は、時間保護違反試験開始情報を、前記試験実施用汎用計算機へ送信し、

前記試験実施用汎用計算機は、前記負荷制御部にて、前記複数のアプリケーションの少なくとも１つの動作を制御して前記時間保護違反を発生させ、前記保護機能部が前記時間保護違反を検知する試験を実施する、請求項１に記載のシミュレーション装置。

【請求項３】

前記メモリ保護違反の試験を実施する際、

前記試験実施用汎用計算機は、前記メモリ操作部にて、前記複数のアプリケーションの少なくとも１つに指示し、前記メモリ保護違反を発生させ、前記保護機能部が前記メモリ保護違反を検知する試験を実施する、請求項１に記載のシミュレーション装置。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明は、自動車の電子制御装置(E C U : Electronic Control Unit)のシミュレーション装置に関する。

【背景技術】

【０００２】

自動車のE C Uのソフトウェアを開発し、その機能を検証する場合、そのソフトウェアを汎用計算機上でデバッグすることが行われている。一方、自動運転の進展などによる自動車のE C Uのソフトウェアの複雑化、大規模化に伴い、電子制御装置でソフトウェアの検証を行う場合、デバッグに多くの時間を要している。

【０００３】

また、電子制御装置でソフトウェアのデバッグを行う場合、特定の機材を使用する必要があり、且つ、デバッグ手段にも制限があるため、意図する検証が容易に行えず、検証に時間を要している。特に、異常系の試験を行う際には、電子制御装置にエラー注入してその動作の確認をする必要があるが、前述の課題のため開発に時間を要している。

【０００４】

このように、複雑、大規模化する自動運転ソフトウェアの検証を効率的に実施することが課題となっている。特許文献１では、電子制御装置内のソフトウェアのシミュレーション方法に関して提案している。具体的にこの文献は、電子制御装置内の回路素子の検証を行う際、検証を行う回路素子を汎用計算機上で模擬し、シミュレーションを実行する方法を提案している。

【０００５】

複数のセンサから出力される物体情報を統合する処理や、自車両の走行経路を推定する処理などを行う自動運転のソフトウェアを開発する際、汎用計算機でプログラムを作成した後、コンパイルし、実行ファイルを電子制御装置へ転送し、動作検証を行う。この時、電子制御装置内のメモリ情報や出力情報を確認するには、専用のデバッグツールを使用することになる。しかしながら、電子制御装置では、タイミングやメモリアクセス等への制約が多く、効率よくデバッグを進めることができない。また、前述した通り、専用のデバ

10

20

30

40

50

ッグツールを使用するため、開発費用にも影響がある。さらには、自動運転のソフトウェアの大規模、複雑化に伴い、電子制御装置でのデバッグは益々難しくなっている。

【0006】

また、ソフトウェアの異常時の動作の検証を行う際は、例えば異なる複数のCPU（Central Processing Unit）コアやプロセスの状態を定期的に観察する必要があるなど、デバッグ作業自体が複雑化しており、容易にデバッグを進めることが難しい。特に、エラー注入した異常時の動作の確認には時間を要する。

【0007】

上記特許文献1のように、電子制御装置の回路素子をシミュレートする方法は提案されているが、シミュレーション対象は回路素子に限定されている。また、このような構成では、ソフトウェアの異常状態を容易に再現することができない。

10

【先行技術文献】

【特許文献】

【0008】

【文献】特開2020-86701号公報

【発明の概要】

【発明が解決しようとする課題】

【0009】

本発明は、ソフトウェアが大規模化、複雑化した場合でも、汎用計算機上でソフトウェアの振舞いや異常時の動作の試験を実施することができ、ソフトウェアの開発効率の向上を図ることができる電子制御装置のシミュレーション装置を提供するものである。

20

【課題を解決するための手段】

【0010】

本発明に係る車両制御装置のシミュレーション装置は、車両制御装置の動作を汎用計算機上で模擬するシミュレーション装置であって、試験を実行する試験実施用汎用計算機と、前記試験を制御する試験制御用汎用計算機とを備える。前記試験実施用汎用計算機は、安全度要求の異なる複数のアプリケーションを含むアプリケーション部と、所定の場合に、前記複数のアプリケーションの動作の1つを終了させ、他のアプリケーションの動作を保証する負荷制御部と、前記複数のアプリケーションによる不正アクセスを検知し、所定の処置を実行するメモリ操作部と、前記複数のアプリケーションに関する保護機能を実現する保護機能部とを備える。前記試験制御用汎用計算機は、試験のシナリオを管理するシナリオ管理部と、前記シナリオに基づき前記試験を指示する試験指示部と、前記指示の内容に基づき試験データを生成するデータ制御部と、を備える。前記試験制御用汎用計算機から任意のタイミングで前記試験データを送信し、前記試験実施用汎用計算機にて、前記試験データに従い、前記保護機能部における前記保護機能の動作を確認する。

30

【発明の効果】

【0011】

本発明によれば、ソフトウェアが大規模化、複雑化した場合でも、汎用計算機上でソフトウェアの動作や異常時の動作の試験を実施することができ、ソフトウェアの開発効率の向上を図ることができる電子制御装置のシミュレーション装置を提供することができる。

40

【図面の簡単な説明】

【0012】

【図1】実施の形態に係る電子制御装置のシミュレーション装置を説明するブロック図である。

【図2】時間保護試験の構成の一例を表す。

【図3】時間保護試験の処理手順を示すフローチャートである。

【図4】メモリ保護試験の構成の一例を表す。

【図5】メモリ保護試験の処理手順を示すフローチャートである。

【図6】データ保護試験の構成の一例を示す。

【発明を実施するための形態】

50

【0013】

以下、添付図面を参照して本実施形態について説明する。添付図面では、機能的に同じ要素は同じ番号で表示される場合もある。なお、添付図面は本開示の原理に則った実施形態と実装例を示しているが、これらは本開示の理解のためのものであり、決して本開示を限定的に解釈するために用いられるものではない。本明細書の記述は典型的な例示に過ぎず、本開示の特許請求の範囲又は適用例を如何なる意味においても限定するものではない。

【0014】

本実施形態では、当業者が本開示を実施するのに十分詳細にその説明がなされているが、他の実装・形態も可能で、本開示の技術的思想の範囲と精神を逸脱することなく構成・構造の変更や多様な要素の置き換えが可能であることを理解する必要がある。従って、以降の記述をこれに限定して解釈してはならない。

【0015】

図1のブロック図を参照して、実施の形態に係る電子制御装置のシミュレーション装置を説明する。このシミュレーション装置は、シミュレーションを実施するための試験実施用汎用計算機100と、シミュレーションを制御するための試験制御用汎用計算機120とを備える。試験実施用汎用計算機100は、電子制御装置(Electronic Control Unit)の動作についてのシミュレーションを実行する装置であり、試験制御用汎用計算機120は、試験実施用汎用計算機100に対し動作についてのシミュレーションを実行するための各種指示を送る装置である。

【0016】

試験実施用汎用計算機100と、試験制御用汎用計算機120とは、それぞれ別々の汎用コンピュータにより構成されてもよいし、試験実施用汎用計算機100と試験制御用汎用計算機120とが1台の汎用コンピュータの中に実現されてもよい。試験実施用汎用計算機100及び試験制御用汎用計算機120は、特別な制約は無いが、CPU(Central Processing Unit)やRAM(Random Access Memory)などの記憶領域を含んで構成されているものとする。

【0017】

試験実施用汎用計算機100は、CPU模擬部101、102と、試験制御部103と、オペレーティングシステム(OS)104とを備える。

【0018】

CPU模擬部101、102は、それぞれ、電子制御装置(ECU)内の一のCPUを模擬することが可能に構成される。CPU模擬部101は、ある1つのCPUを模擬するように構成され、CPU模擬部102は、これとは別の1つのCPUを模擬するように構成される。試験実施用汎用計算機100は、複数のCPU模擬部を備えることで、複数のECU内のCPUを非同期に模擬することが可能である。図示の例は、1つの試験実施用汎用計算機100が2個のCPU模擬部101、102を備える例を示しているが、これは一例であり、これに限定されるものではない。

【0019】

電子制御装置(ECU)内のCPUは、汎用計算機上のプロセス又はスレッドとして模擬される。試験実施用汎用計算機100に搭載されるオペレーティングシステム104は、市販のオペレーティングシステムであってよい。

【0020】

試験実施用汎用計算機100は、試験制御用汎用計算機120から送信される試験指示データを通信制御部を介して受信し、解析を行うことで、実施する試験シナリオを判別する。判別された試験シナリオに基づき試験実施用汎用計算機100において試験が実施される。尚、試験制御用汎用計算機120から試験実施用汎用計算機100へデータを送信する手段は、CAN通信、Ethernet通信、シリアル通信等であってよく、特定の通信の方式には制限されない。

【0021】

各CPU模擬部(101、102)は、それぞれ、一例として、ラッパー部113、ミ

10

20

30

40

50

ドルウェア部 114、時間保護部 115、メモリ保護部 116、データ保護部 117、API部 118、アプリケーション部 119から構成される。

【0022】

ラッパー部 113は、電子制御装置と汎用計算機の差異を吸収する役割を有する。例えば、電子制御装置と汎用計算機では、使用するオペレーティングシステム（OS）のソース、システムコール、使用するドライバに差異がある。ラッパー部 113は、これらの差異を抽象化し、動作環境に応じて実行する処理の切り分けを行う。

【0023】

ミドルウェア部 114は、電子制御装置と汎用計算機で同じソースコードを用いる。ミドルウェア部 114は、試験制御用汎用計算機 120から送信される試験データを、電子制御装置と同様の処理フローで受信処理をし、その結果をデータ管理部の持つバッファへ格納する。データ管理部では、通信制御部から渡ったデータを管理し、API部 118からの指示に基づきデータの授受を行う。

10

【0024】

アプリケーション部 119は、例えば車両の周辺環境を認知する機能や、車両の認知結果に基づき自車の走行経路を計画する機能、車両の制御量を演算する機能などを備え、API部 118を介し必要な情報を取得する。また、アプリケーション部 119は、安全度要求の異なる複数のアプリケーション（例：高安全度アプリ部、低安全度アプリ部）から構成される。

【0025】

API部 118は、ミドルウェア部 114とアプリケーション部 119の間のデータの授受を仲介する。アプリケーション部 119は、API部 118を介してミドルウェア部 114とデータの受け渡しを実現する。

20

【0026】

時間保護部 115は、各アプリケーションの動作、例えばスレッドの動作が所定時間内に完了するか否かを確認する機能を有する。

【0027】

メモリ保護部 116は、各アプリケーションにおけるメモリへの不正アクセスがあるか否かを確認する機能を有する。

【0028】

データ保護部 117は、データの整合性を保証する。外部から送信されるメッセージがヘッダ情報を持つ場合、これらのヘッダ情報の内容を確認し、不正な書換えなどが無いかを確認する。不正な書換えが確認された場合、データの破棄など、事前に設定した処理を実行する。

30

【0029】

時間保護部 115、メモリ保護部 116、データ保護部 117は、複数のアプリケーションに関する保護機能を実現する保護機能部の一態様である。CPU模擬部 101、102は、時間保護部 115、メモリ保護部 116、データ保護部 117の全てを含んでもよいし、1つのみを含んでもよい。また、時間保護部 115、メモリ保護部 116、データ保護部 117以外の保護機能が設けられていてもよい。

40

【0030】

次に、試験制御部 103について説明する。試験制御部 103は、一例として、負荷制御部 111と、メモリ操作部 112とを備える。負荷制御部 111は、安全度要求が低い低安全度アプリ部が所定時間内に処理を完了できず、安全度要求が高い高安全度アプリ部の動作周期に影響を与える場合に、低安全度アプリ部を終了させ、高安全度アプリ部の動作周期を保証する。メモリ操作部 112は、各アプリケーションが本来アクセス権を与えられていないメモリ領域にアクセスした際に、不正なアクセスを検知し、不正アクセスしたアプリケーションに事前に設定した処置を実行する。

【0031】

試験制御用汎用計算機 120は、試験制御部 121と、オペレーティングシステム（O

50

S) 122とを有する。試験制御部121は、一例として、データ制御部123、試験指示部124、シナリオ管理部125とから構成され得る。オペレーティングシステム122は、試験実施用汎用計算機100のオペレーティングシステム104と異なるものであってもよい。

【0032】

試験制御部121は、シナリオ管理部125のシナリオに基づき、正常動作の指示、又は、各異常系のテストパターンを注入する。異常系の試験は、一例として、データ保護試験、時間保護試験、又はメモリ保護試験を含む。これらの試験が単独で行われても良いし、3つの試験が組み合わせた試験が行われても良い。

【0033】

データ制御部123は、試験制御部121からの指令に基づき、異常データの生成を行う。データ制御部123は、異常系の試験時に正常データのヘッダ情報を書換えて異常データを生成し、試験実施用汎用計算機100へ送信する。

【0034】

試験指示部124は、シナリオ管理部125で指定されたシナリオに従い、各種試験の指示を生成する。生成された各種指示は、オペレーティングシステム122、104により、試験実施用汎用計算機100に入力される。シナリオ管理部125は、試験実施用汎用計算機100で実行される試験のシナリオを管理する。シナリオは、事前にユーザが指定することも可能であり、動的にユーザが追加、変更することも可能である。

【0035】

図2は、時間保護部115により実行される時間保護試験の構成の一例を表す。アプリケーション部119には安全度要求の異なる複数のアプリケーション（高安全度アプリ部、低安全度アプリ部）を配置する。安全度要求が高い高安全度アプリ部200は、例えばASILアプリであり、安全度要求が低い低安全度アプリ部201は、例えばQMアプリである。この時、QMアプリに対しエラー注入を実施する。この時の処理フローを図3に示す。

【0036】

試験制御用汎用計算機120より、時間保護試験の開始の指示があった場合、シナリオ管理部125において異常シナリオが生成され（図3のステップS11）、この異常シナリオに従って、異常データがデータ制御部123において生成される。このとき、試験実施用汎用計算機100の負荷制御部111は、異常データを注入する対象である低安全度アプリ部201のスレッドの実行優先度を上げ（ステップS12）、且つ、対象の低安全度アプリ部201に対し、長期間CPUを占有する処理の実施指示を出す。これにより、低安全度アプリ部201がCPUを占有する。

【0037】

この時、時間保護部115は、予めスケジューリングされた低安全度アプリ部201の基準処理時間を、実際の処理時間と比較する。実際の処理時間は、低安全度アプリ部201の、テスト管理スレッドから供給される。低安全度アプリ部201の処理時間が基準時間を超過している場合、時間違反であると判断し（ステップS13）、時間保護部115は、事前に実装された安全機能処理を実施する。例えば、対象の低安全度アプリ部201の停止などを実行する。

【0038】

図4は、メモリ保護試験の構成の一例を表す。アプリケーション部119には安全度要求の異なるアプリケーション（高安全度アプリ部、低安全度アプリ部）を配置する。安全度要求が高い高安全度アプリ部200は、例えばASILアプリであり、安全度要求が低い低安全度アプリ部201は、例えばQMアプリである。この時、QMアプリに対しエラー注入を実施する。この時の処理フローを図5に示す。

【0039】

試験制御用汎用計算機120より、メモリ保護試験の開始指示があった際、シナリオ管理部125において異常シナリオが生成され（図5のステップS21）、この異常シナリ

10

20

30

40

50

オに従って、異常データがデータ制御部 123 において生成される。メモリアクセス違反指示を受信した低安全度アプリ部 201 は、本来アクセス許可が無いメモリ領域へアクセスする（ステップ S22）。この時、カーネルより不正なメモリアクセスに際し、アクセス違反信号 S I G S E G V が発行される（ステップ S23）。メモリ保護部 116 は、発行された信号 S I G S E G V を確認し、不正メモリアクセス違反を引き起した低安全度アプリ部 201 に対し事前に実装した保護機能を適用する。保護機能とは、例えば、対象アプリケーションのプロセスの停止処理（ステップ S24）等を含む。

【0040】

図 6 は、データ保護違反の構成の一例を表す。試験制御用汎用計算機 120 の試験指示部 124 では、シナリオ管理部 125 のシナリオに基づきデータ保護違反の試験指示をデータ制御部 123 へ出力する。データ制御部 123 では、送信するメッセージのヘッダ部を改ざん（変更）し、改ざんしたメッセージを試験実施用汎用計算機 100 へ送信する。試験実施用汎用計算機 100 のデータ保護部 117 は、受信したメッセージのヘッダ部を解析し、ヘッダ部の改ざんを検知した際は、メッセージの破棄やアプリケーション部 119 への通知など、事前に実装した保護内容を適用する。

【0041】

以上説明したように、本実施の形態のシミュレーション装置によれば、電子制御装置（ECU）のソフトウェアが大規模化、複雑化した場合でも、汎用計算機上でソフトウェアの振舞いや異常時の動作の試験を実施することができ、ソフトウェアの開発効率の向上を図ることができる。具体的には、ソフトウェアの時間保護違反、メモリ保護違反、データ保護違反などを、汎用計算機上で模擬することが容易になる。

【0042】

本発明は上記した実施例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、上記した実施例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、ある実施例の構成の一部を他の実施例の構成に置き換えることが可能であり、また、ある実施例の構成に他の実施例の構成を加えることも可能である。また、各実施例の構成の一部について、他の構成の追加・削除・置換をすることが可能である。

【符号の説明】

【0043】

100…試験実施用汎用計算機
101、102…CPU 模擬部
103…試験制御部
104…オペレーティングシステム
111…負荷制御部
112…メモリ操作部
113…ラッパー部
114…ミドルウェア部
115…時間保護部
116…メモリ保護部
117…データ保護部
118…API 部
119…アプリケーション部
120…試験制御用汎用計算機
121…試験制御部
122…オペレーティングシステム
123…データ制御部
124…試験指示部
125…シナリオ管理部
200…高安全度アプリ部

10

20

30

40

50

201…低安全度アプリ部

【図面】

【図1】

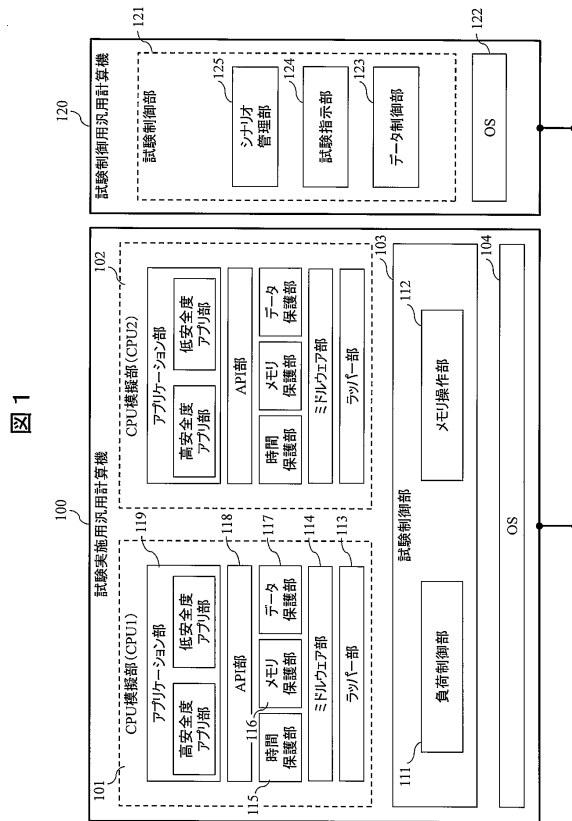
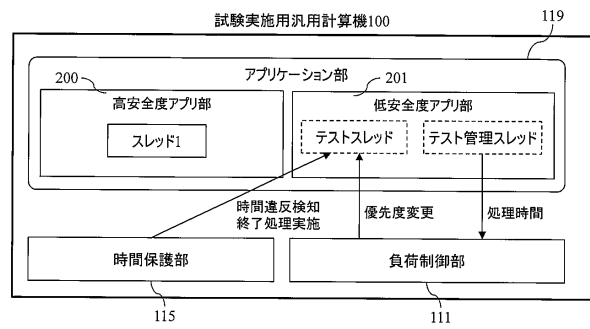


図1

【図2】

図2

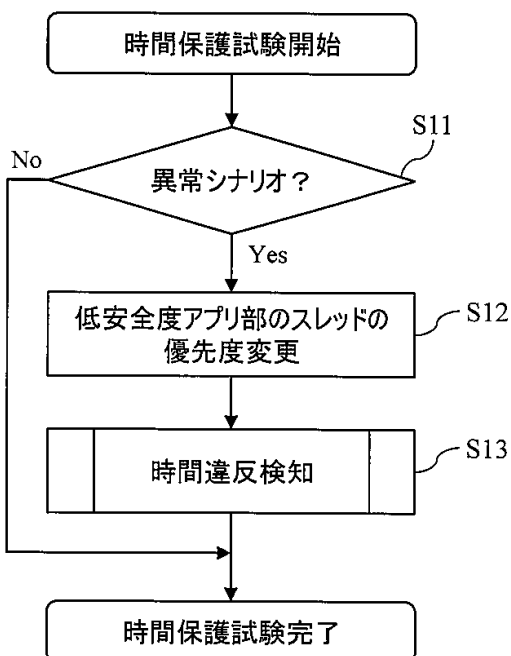


10

20

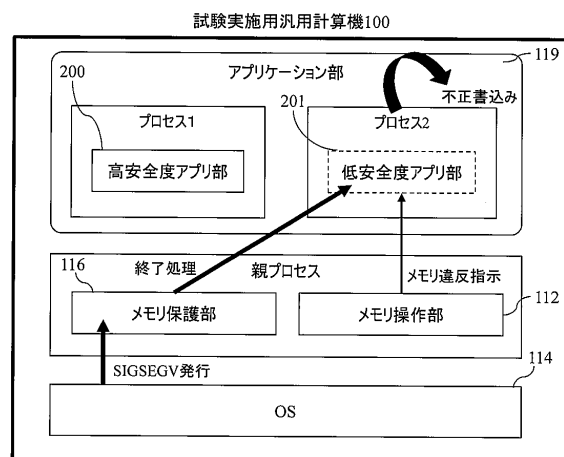
【図3】

図3



【図4】

図4

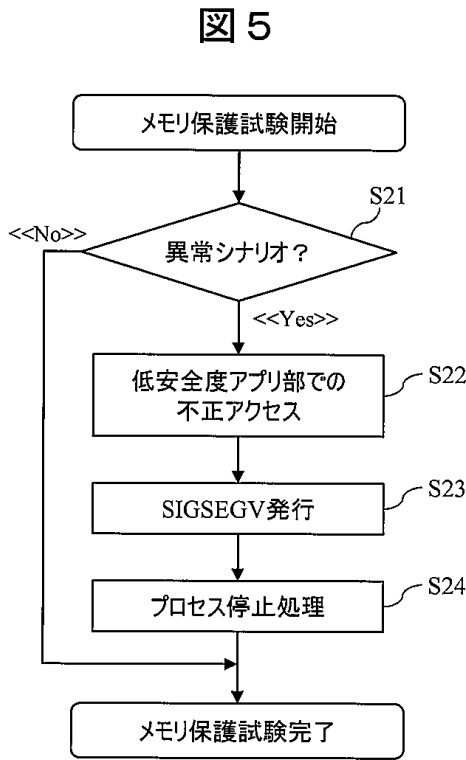


30

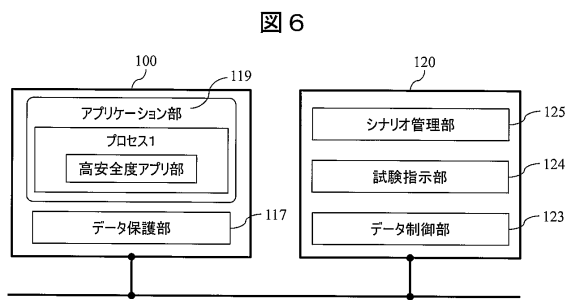
40

50

【図 5】



【図 6】



10

20

30

40

50

フロントページの続き

- (56)参考文献 特開 2019-179284 (JP, A)
国際公開第 2018/211865 (WO, A1)
特開 2011-100338 (JP, A)
特開 2019-191942 (JP, A)
- (58)調査した分野 (Int.Cl., DB名)
G06F 11/36