

(19) 日本国特許庁(JP)

(12) 特 許 公 報(B1)

(11) 特許番号

特許第6527647号
(P6527647)

(45) 発行日 令和1年6月5日(2019.6.5)

(24) 登録日 令和1年5月17日(2019.5.17)

(51) Int.Cl. F I
H O 4 L 12/28 (2006.01) H O 4 L 12/28 2 0 0 Z

請求項の数 4 (全 30 頁)

(21) 出願番号	特願2019-516260 (P2019-516260)	(73) 特許権者	514136668
(86) (22) 出願日	平成30年12月4日 (2018.12.4)		パナソニック インテレクチュアル プロ
(86) 国際出願番号	PCT/JP2018/044568		パティ コーポレーション オブ アメリ
審査請求日	平成31年3月25日 (2019.3.25)		カ
(31) 優先権主張番号	特願2018-64431 (P2018-64431)		Panasonic Intellectual
(32) 優先日	平成30年3月29日 (2018.3.29)		ual Property Corpor
(33) 優先権主張国	日本国(JP)		ation of America
早期審査対象出願			アメリカ合衆国 90503 カリフォル
			ニア州, トーランス, スイート 200,
			マリナー アベニュー 20000
		(74) 代理人	100109210
			弁理士 新居 広守
		(74) 代理人	100137235
			弁理士 寺谷 英作
最終頁に続く			

(54) 【発明の名称】 不正検知方法、不正検知装置及びプログラム

(57) 【特許請求の範囲】

【請求項 1】

車載ネットワークにおける異常なメッセージを検知する不正検知方法であって、
前記車載ネットワークに、繰り返し送出されたメッセージの周期が異常であるか否かを
判定する周期異常判定ステップと、
前記メッセージが前記車載ネットワークに送出された際に調停が発生していたか否かを
検出する調停検出ステップと、
前記メッセージの周期が異常であり、前記メッセージが前記車載ネットワークに送出さ
れた際に調停が発生していなかった場合、前記メッセージを異常なメッセージと判定する
メッセージ判定ステップとを含む、
不正検知方法。

【請求項 2】

前記調停検出ステップでは、前記メッセージが、前記メッセージを受信する周期の正常
範囲内の時刻に受信された他のメッセージから連続して受信された 1 つ以上のメッセージ
に含まれる場合、調停が発生したと判定する

請求項 1 に記載の不正検知方法。

【請求項 3】

車載ネットワークにおける異常なメッセージを検知する不正検知装置であって、
1 個以上のプロセッサと、
記憶部と、を含み、

前記１個以上のプロセッサは、前記記憶部を用いて、

前記車載ネットワークに、繰り返し送出されたメッセージの周期が異常であるか否かを判定する周期異常判定ステップと、

前記メッセージが前記車載ネットワークに送出された際に調停が発生していたか否かを検出する調停検出ステップと、

前記メッセージの周期が異常であり、前記メッセージが前記車載ネットワークに送出された際に調停が発生していなかった場合、前記メッセージを異常なメッセージと判定するメッセージ判定ステップとを行う

不正検知装置。

【請求項４】

コンピュータに請求項１に記載の不正検知方法を実行させるためのプログラム。

【発明の詳細な説明】

【技術分野】

【０００１】

本開示は、車載ネットワークにおける異常なメッセージを検知する不正検知方法等に関する。

【背景技術】

【０００２】

近年、自動車の中のシステムには、電子制御ユニット（ＥＣＵ：Electronic Control Unit）と呼ばれる装置が多数配置されている。これらのＥＣＵをつなぐ通信ネットワークは車載ネットワークと呼ばれる。車載ネットワークには、多数の通信規格が存在する。その中でも最も主流な車載ネットワークの規格の一つに、Controller Area Network（CAN）がある。

【０００３】

CANの規格に拠るネットワーク（CANネットワーク）では、通信路（バス）は２本のケーブルで構成され、バスに接続されているＥＣＵはノードとも呼ばれる。バスに接続されている各ノードは、フレーム又はメッセージと呼ばれる単位でデータを送受信する。またCANでは、データの送信先又は送信元を示す識別子は用いられない。

【０００４】

フレームを送信するノード（送信ノード）は、メッセージ毎にメッセージの種類を示すメッセージIDと呼ばれるIDを付けてメッセージを送信、つまりバスに信号を送出する。メッセージを受信するノード（受信ノード）は、予め決められたメッセージIDを含むメッセージのみ受信、つまりバスから信号を読み取る。同一IDのメッセージは、一定の周期で送信される。

【０００５】

上述の通り、自動車の中のシステムに多数配置されているＥＣＵは、それぞれがCANネットワークに接続され、様々なメッセージを互いにやりとりしながら動作している。

【０００６】

ここで、CANネットワークの外部と通信機能を持つＥＣＵが、外部から不正にアクセスされること等により、何者かに不正に制御され、CANネットワークに対して異常なメッセージ（攻撃メッセージ）を送信することが起こり得る。このような何者かに不正に制御されたＥＣＵ（不正ＥＣＵ）は、例えば他のＥＣＵになりすまして異常なメッセージを送信し、車両を不正に制御することが可能となる。このような、いわゆるなりすまし攻撃を検知するための方法が、例えば、特許文献１に開示されている。

【先行技術文献】

【特許文献】

【０００７】

【特許文献１】国際公開第２０１４／１１５４５５号

【発明の概要】

【発明が解決しようとする課題】

10

20

30

40

50

【 0 0 0 8 】

しかしながら、特許文献 1 に開示されている方法では、C A N ネットワークバス上の送信周期の乱れにより正常なメッセージの送信周期が長くなった場合に、正しい判断ができないという課題がある。

【 0 0 0 9 】

本開示は、上記課題を解決するもので、バスに送出された個々のメッセージが異常なメッセージであるか否かを判定する不正検知方法、不正検知装置等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】

【 0 0 1 0 】

10

上記課題を解決するために、本開示の一態様に係る不正検知方法は、車載ネットワークシステムにおける異常なメッセージを検知する不正検知方法であって、前記車載ネットワークシステムに、繰り返し送出されたメッセージの周期が異常であるか否かを判定する周期異常判定ステップと、前記メッセージが前記車載ネットワークシステムに送出された際に調停が発生していたか否かを検出する調停検出ステップと、前記メッセージの周期が異常であり、前記メッセージが前記車載ネットワークシステムに送出された際に調停が発生していなかった場合、前記メッセージを異常なメッセージと判定するメッセージ判定ステップとを含む。

【 0 0 1 1 】

20

なお、これらの包括的または具体的な態様は、システム、装置、方法、集積回路、コンピュータプログラム又はコンピュータ読み取り可能な C D - R O M などの非一時的な記録媒体で実現されてもよく、システム、装置、方法、集積回路、コンピュータプログラム及び記録媒体の任意な組み合わせで実現されてもよい。

【発明の効果】

【 0 0 1 2 】

本開示の一態様に係る不正検知方法等によれば、バスに送出された個別のメッセージが異常なメッセージであるか否かを判定することができる。

【図面の簡単な説明】

【 0 0 1 3 】

【図 1】図 1 は、実施の形態 1 における車載ネットワークシステムの全体構成を示すブロック図である。

30

【図 2】図 2 は、実施の形態 1 における C A N プロトコルのメッセージ（データフレーム）のフォーマットを示す図である。

【図 3】図 3 は、実施の形態 1 における車載ネットワークシステムに含まれるゲートウェイの構成を示すブロック図である。

【図 4】図 4 は、実施の形態 1 における受信 I D リストの一例を示す図である。

【図 5】図 5 は、実施の形態 1 における転送ルールの一列を示す図である。

【図 6】図 6 は、実施の形態 1 における不正検知処理機能群の一例を示すブロック図である。

【図 7 A】図 7 A は、実施の形態 1 における調停発生時のメッセージの受信パターンを示す図である。

40

【図 7 B】図 7 B は、実施の形態 1 における調停発生時のメッセージの受信パターンを示す別の図である。

【図 8】図 8 は、実施の形態 1 における不正検知処理機能群の別の一例を示すブロック図である。

【図 9】図 9 は、実施の形態 1 における車載ネットワークシステムに含まれる E C U の一例を示すブロック図である。

【図 1 0】図 1 0 は、実施の形態 1 における不正検知処理の一例を示すフローチャートである。

【図 1 1】図 1 1 は、実施の形態 1 における転送処理の一例を示すフローチャートである

50

。

【図 1 2】図 1 2 は、実施の形態 2 における不正検知処理機能群の一例を示すブロック図である。

【図 1 3】図 1 3 は、実施の形態 2 における不正検知処理の一例を示すフローチャートである。

【図 1 4】図 1 4 は、変形例における不正検知処理機能群の一例を示す図である。

【図 1 5】図 1 5 は、変形例における不正検知処理機能群の一例を示す図である。

【図 1 6】図 1 6 は、変形例における ECU の一例を示すブロック図である。

【図 1 7】図 1 7 は、変形例における ECU の一例を示すブロック図である。

【図 1 8】図 1 8 は、変形例における ECU の一例を示すブロック図である。

10

【発明を実施するための形態】

【0014】

（本開示の基礎になった知見）

CAN ネットワーク上に、多くの ECU が接続されている場合、それぞれの ECU が独立してメッセージを送信しようとする、メッセージの送信タイミングが同じになる可能性が高くなる。

【0015】

その場合は、CAN ネットワークには、「調停」と呼ばれる機能があり、ID の小さいメッセージが優先的に送信され、ID の大きなメッセージは、送信を待つことになる。そうすると、メッセージを送信する送信タイミングにずれが生じるため、メッセージの送信間隔に応じて正常なメッセージか異常なメッセージかを判定する機能が誤作動し、正常なメッセージを異常なメッセージであると判定する可能性が生じる。

20

【0016】

そこで、本開示の一態様に係る不正検知方法は、記憶部を含む情報処理システムで実行される、車載ネットワークシステムにおける異常なメッセージを検知する不正検知方法であって、前記車載ネットワークシステムに、繰り返し送出されたメッセージの周期が異常であるか否かを判定する周期異常判定ステップと、前記メッセージが前記車載ネットワークシステムに送出された際に調停が発生していたか否かを検出する調停検出ステップと、前記メッセージの周期が異常であり、前記メッセージが前記車載ネットワークシステムに送出された際に調停が発生していなかった場合、前記メッセージを異常なメッセージと判定するメッセージ判定ステップとを含む。

30

【0017】

これにより、車載ネットワークシステムに送出されたメッセージに調停などによって送信遅れが生じた場合に、受信したメッセージが、正常なメッセージか否かを適切に判定できる。その結果、個々のメッセージが異常なメッセージであるか否かの判定は、より高い精度で実行される。

【0018】

また例えば、前記周期異常判定ステップで周期を判定する際に周期の起点となる時刻を前記メッセージの受け付け時刻または、受け付け予定時刻に決定する周期起点決定ステップとを含み、前記周期異常検知ステップでは、前記周期起点決定ステップで決定された起点を用いて周期を判定してもよい。

40

【0019】

これにより、調停が発生した際のメッセージ送信方法が複数ある場合においても、メッセージの受信時刻に現れる特徴に基づいて正常なメッセージであるか否かを判断することで、より高い精度で異常なメッセージを判定できる。

【0020】

また、例えば、前記メッセージの送信タイプを判定する送信タイプ判定ステップを含み、前記周期起点決定ステップでは、送信タイプに応じて前記メッセージの受付時刻または受け付け予定時刻に決定してもよい。

【0021】

50

これにより、車載ネットワークに送出されたメッセージの送信タイプに応じた、調停検出を行うことができる。

【 0 0 2 2 】

また、例えば、前記調停検出ステップでは、前記メッセージが、前記メッセージを受信する周期の正常範囲内の時刻に受信された他のメッセージから連続して受信された 1 つ以上のメッセージに含まれる場合、調停が発生したと判定してもよい。

【 0 0 2 3 】

これにより、調停などによってメッセージの送信遅れが生じた場合でも、受信したメッセージが正常なメッセージか否かを適切に判定できる。

【 0 0 2 4 】

また、本開示の一態様に係る不正検知装置は、車載ネットワークシステムにおける異常なメッセージを検知する不正検知装置であって、1 個以上のプロセッサと、記憶部と、を含み、前記記憶部を用いて、前記 1 個以上のプロセッサは、前記車載ネットワークシステムに送出されたメッセージの周期が異常であるか否かを判定する周期異常判定ステップと、前記メッセージが前記車載ネットワークシステムに送出された際に調停が発生していたかどうかを検出する調停検出ステップと、前記メッセージの周期が異常であり、前記メッセージが前記車載ネットワークシステムに送出された際に調停が発生していた場合、前記メッセージを正常なメッセージと判定する周期判定ステップとを行う。

【 0 0 2 5 】

これにより、車載ネットワークシステムに送出されたメッセージが調停などにより送信遅れが生じても、正常なメッセージか否かを適切に判定できる。その結果、個々のメッセージが異常なメッセージであるか否かの判定も、より高い精度で実行される。

【 0 0 2 6 】

また、本開示の一態様に係るプログラムは、上記の不正検知装置において、前記 1 個以上のプロセッサに上記の不正検知方法のいずれかを実施させるためのプログラムである。

【 0 0 2 7 】

これにより、車載ネットワークシステムに送出されたメッセージに調停などによって送信遅れが生じても、正常なメッセージか否かを適切に判定できる。その結果、個々のメッセージが異常なメッセージであるか否かの判定も、より高い精度で実行される。

【 0 0 2 8 】

以下、実施の形態について図面を参照しながら具体的に説明する。

【 0 0 2 9 】

なお、以下で説明する実施の形態は、いずれも包括的または具体的な例を示すものである。以下の実施の形態で示される数値、形状、材料、構成要素、構成要素の配置および接続形態、ステップ、ステップの順序などは一例であり、本開示を限定する趣旨ではない。以下の実施の形態における構成要素のうち、最上位概念を示す独立請求項に記載されていない構成要素は、任意で含まれる構成要素として説明されるものである。

【 0 0 3 0 】

(実施の形態 1)

[1 . 概要]

本実施の形態では、車載ネットワークシステムにおいて、送信されているメッセージが異常なメッセージであるか否かの判定がなされる場合について図面を参照しながら説明する。なお、ここで、異常なメッセージは、基本的に、不正なメッセージである。

【 0 0 3 1 】

[1 . 1 車載ネットワークシステムの全体構成]

図 1 は、本実施の形態における車載ネットワークシステム 10 の全体構成を示すブロック図である。

【 0 0 3 2 】

図 1 において、車載ネットワークシステム 10 は、CAN ネットワークで構成され、E C U 1 0 0 a、E C U 1 0 0 b、E C U 1 0 0 c、及び E C U 1 0 0 d と、バス 2 0 0 a

10

20

30

40

50

及びバス200bと、ゲートウェイ300とを含む。

【0033】

以下では、ECU100a、ECU100b、ECU100c、ECU100dを、集合的にECU100とする場合がある。又、ECU100a、ECU100b、ECU100c、ECU100dのいずれかを指して、ECU100として説明する場合がある。

【0034】

また、以下では、バス200a、バス200b集合的にバス200とする場合がある。又、バス200a及びバス200bのいずれか一方を指して、バス200とする場合がある。

【0035】

ECU100aはエンジン101に接続され、ECU100bはブレーキ102に接続される。また、ECU100cはドア開閉センサ103に接続され、ECU100dはウィンドウ開閉センサ104に接続されている。

【0036】

ECU100は、接続されている機器の状態を取得し、取得した状態を表すメッセージを周期的にバス200に送出する。例えばECU100aは、エンジン101の回転数を取得し、この回転数を表すデータ値を含むメッセージに所定のIDを付けてバス200に送出する。

【0037】

また、各ECU100は、他のECU100が送信したメッセージをバス200から読み出し、メッセージに付されたIDに応じて選択的に受信する。この選択的な受信については後述する。

【0038】

ゲートウェイ300は、ECU100a及びECU100bが接続されているバス200aと、ECU100c及びECU100dが接続されているバス200bとを接続している。ゲートウェイ300は一方のバスから受信したメッセージを、もう一方のバスに転送する機能を持つ。ゲートウェイ300もまた、CANネットワーク上ではひとつのノードである。

【0039】

なお、車載ネットワークシステム10は、メッセージが異常なメッセージであるか否かの判定をする不正通信検知システム等が適用可能な対象を説明するための例であり、その適用対象は車載ネットワークシステム10に限定されない。LAN(Local Area Network)等を用いた各種ネットワークシステム又は分散データベース等に適用されてもよい。

【0040】

[1.2 メッセージのデータフォーマット]

図2は、CANプロトコルのメッセージ(データフレーム)のフォーマットを示す図である。ここではCANプロトコルにおける標準IDフォーマットにおけるメッセージを示している。

【0041】

メッセージは、Start Of Frame(SOF)と、IDフィールド、Remote Transmission Request(RTR)、IDE(Identifier Extension)、予約ビット(r)、データレングスコード(DLC)、データフィールド、CRC(Cyclic Redundancy Check)シーケンス、CRCデリミタ(図中、左のDEL)と、ACK(Acknowledgement)スロットと、ACKデリミタ(図中、右のDEL)と、EOF(End Of Frame)から構成される。

【0042】

SOFは、1ビットのドミナントである。ドミナントは、優性の意である。ドミナントは、データの伝達にデジタル方式が用いられるCANネットワークにおいて、“0”の値

10

20

30

40

50

を送信するようにバスを構成する2本のケーブルに電圧がかけられた状態、または送信されるこの“0”の値のことである。これに対し、“バスを構成する2本のケーブルに1”の値を送信するように電圧がかけられた状態、または送信されるこの“1”の値のことはレセシブと呼ばれる。レセシブは、劣勢の意である。2つのノードからバスに同時に“0”の値と“1”の値とが送信された場合には、“0”の値が優先される。アイドル時のバスはレセシブの状態である。各ECU100は、バス200の状態をレセシブからドミナントへ変化させることでメッセージの送信を開始し、他のECU100はこの変化を読み取って同期する。図2において、メッセージを構成するドミナント又はレセシブを示す線が実線である部分は、ドミナント又はレセシブの各値を取り得ることを示す。SOFはドミナントの状態で固定されているため、ドミナントの線は実線であり、レセシブの線は破線である。

10

【0043】

IDとは、メッセージが含むデータの種別を示す11bitの値である。またCANでは、複数のノードが同時に送信を開始したメッセージ間での通信調停において、IDの値がより小さいメッセージがより高い優先度となるよう設計されている。

【0044】

RTRとは、フレームがメッセージ(データフレーム)であることを示す1bitのドミナントである。

【0045】

IDEとは、それぞれ1bitのドミナントである。

20

【0046】

DLCは、続くデータフィールドの長さを示す4bitの値である。

【0047】

データフィールドは、送信されるデータの内容を示す値であり、最大64bit長で、8bit単位で長さを調整できる。送られるデータのこの部分への割り当てに関する仕様は、車種又は製造者に依存する。

【0048】

CRCシーケンスは、SOF、IDフィールド、コントロールフィールド、データフィールドの送信値より算出される15bitの値である。

【0049】

CRCデリミタは1bitのレセシブ固定の、CRCシーケンスの終了を表す区切り記号である。受信ノードは、受信したメッセージのSOF、IDフィールド、コントロールフィールド、及びデータフィールドの値から算出した結果をCRCシーケンスの値と比較することで異常の有無を判断する。

30

【0050】

ACKスロットは1bit長で、送信ノードはこの部分でレセシブを送信する。受信ノードはCRCシーケンスまで正常に受信ができていれば確認応答としてドミナントを送信する。ドミナントが優先されるため、1メッセージの通信がCRCシーケンスまで正常に行われていれば、ACKスロットの送信中のバス200はドミナントである。

【0051】

ACKデリミタは1bitのレセシブに固定されており、ACKスロットの終了を表す区切り記号である。

40

【0052】

EOFは7bitのレセシブに固定されており、メッセージの終了を示す。

【0053】

[1.3 ゲートウェイの構成]

図3は、本実施の形態における車載ネットワークシステム10に含まれるゲートウェイ300の構成を示すブロック図である。図3において、ゲートウェイ300は、フレーム送受信部310と、フレーム解釈部320と、受信ID判定部330と、受信IDリスト保持部340と、フレーム処理部350と、転送ルール保持部360と、不正検知処理機

50

能群 370 と、フレーム生成部 380 とを備える。

【0054】

なお、これらの構成は機能を示す構成であり、ゲートウェイ 300 は、例えばプロセッサで実現される処理部、半導体メモリ等で実現される記憶部、入出力ポートで実現される入出力部等を備える情報処理装置として提供される。

【0055】

上記の機能を示す構成は、記憶部に保持されるプログラムを処理部により読み出し、実行し、記憶部へ所定のデータを記録することで実現される。若しくは、記憶部へ所定のデータを記録することの代わりに、入出力部を介してデータの送受信を実行することでこれらの構成が実現されてもよい。又は、上記の機能を示す構成は、これらの組み合わせで実現されてもよい。

10

【0056】

フレーム送受信部 310 は、バス 200 a、200 b のそれぞれに対して、CAN のプロトコルに従ったメッセージを送受信する。

【0057】

より具体的には、フレーム送受信部 310 は、バス 200 に送出されたメッセージを 1 bit ずつ読み出し、読み出したメッセージをフレーム解釈部 320 に転送する。

【0058】

また、フレーム送受信部 310 は、フレーム生成部 380 より送信されたバス情報に応じて、メッセージをバス 200 a 及び 200 b に 1 bit ずつ送出する。

20

【0059】

フレーム送受信部 310 は、バス 200 a から受信したメッセージをバス 200 b に送信し、バス 200 b から受信したメッセージをバス 200 a に送信することでバス 200 間でのメッセージの転送を実行する。

【0060】

フレーム解釈部 320 は、フレーム送受信部 310 よりメッセージの値を受け取り、CAN プロトコルにおける各フィールドにマッピングして、受信したメッセージの解釈を行う。フレーム解釈部 320 は、ID フィールドの値と解釈した一連の値を、受信 ID 判定部 330 へ転送する。

【0061】

30

フレーム解釈部 320 はさらに、受信 ID 判定部 330 から通知される判定結果に応じて、メッセージの ID フィールドの値及び ID フィールド以降に現れるデータフィールドをフレーム処理部 350 へ転送するか、メッセージの受信を中止するかを決定する。

【0062】

また、フレーム解釈部 320 は、受信したメッセージが CAN プロトコルに則っていないメッセージと判断した場合は、エラーフレームを送信するようにフレーム生成部 380 へ要求する。

【0063】

エラーフレームは、CAN ネットワーク上でエラーが発生した場合に、ノードから送信される、上述のメッセージとは異なる、CAN プロトコルで規定される所定のフォーマットのフレームである。エラーフレームがバスに送出されると、そのネットワークでのメッセージの送信は中断される。

40

【0064】

また、フレーム解釈部 320 は、他のノードが送信したエラーフレームを受信したと解釈した場合、読み取り中のメッセージを破棄する。

【0065】

受信 ID 判定部 330 は、フレーム解釈部 320 から ID フィールドの値を受け取り、受信 ID リスト保持部 340 が保持しているメッセージ ID のリストに従い、読み出したメッセージを受信するか否かの判定を行う。受信 ID 判定部 330 は、この判定の結果をフレーム解釈部 320 へ通知する。

50

【 0 0 6 6 】

受信ＩＤリスト保持部３４０は、ゲートウェイ３００が受信するメッセージＩＤのリスト（受信ＩＤリスト）を保持する。図４は、本実施の形態における受信ＩＤリストの一例を示す図である。図４における受信ＩＤリストの詳細は、後述する。

【 0 0 6 7 】

フレーム処理部３５０は、転送ルール保持部３６０が保持するデータ転送に関するルールに従って、受信したメッセージのＩＤに応じて転送先となるバス２００を決定し、転送先となるバス２００と、フレーム解釈部３２０より通知されたメッセージＩＤと、転送するデータとをフレーム生成部３８０へ通知する。

【 0 0 6 8 】

またフレーム処理部３５０は、フレーム解釈部３２０より受け取ったメッセージを不正検知処理機能群３７０へ送り、不正検知処理機能群３７０に対して、そのメッセージが、異常なメッセージであるか否かの判定を行うように要求する。不正検知処理機能群３７０において異常なメッセージであると判定されたメッセージを、フレーム処理部３５０は転送しない。

【 0 0 6 9 】

転送ルール保持部３６０は、各バス２００のデータ転送に関するルール（以下、転送ルールともいう）を保持する。図５は、本実施の形態における転送ルールの一例を示す図である。図５における転送ルールの詳細は、後述する。

【 0 0 7 0 】

不正検知処理機能群３７０は、受信中のメッセージが異常なメッセージであるか否かを判定する機能群である。不正検知処理機能群３７０に含まれる機能構成の詳細は後述する。

【 0 0 7 1 】

フレーム生成部３８０は、フレーム解釈部３２０からのエラーフレーム送信の要求に従い、エラーフレームを生成し、フレーム送受信部３１０にエラーフレームを送出させる。

【 0 0 7 2 】

またフレーム生成部３８０は、フレーム処理部３５０より受け取ったメッセージＩＤ及びデータを使ってメッセージフレームを生成し、バス情報とともに、フレーム送受信部３１０にメッセージフレームを送出する。

【 0 0 7 3 】

〔 １．４ 受信ＩＤリスト 〕

図４は、本実施の形態における受信ＩＤリストの一例を示す図である。受信ＩＤリストは、ゲートウェイ３００が受信して処理するメッセージのメッセージＩＤのリストである。

【 0 0 7 4 】

図４において、受信ＩＤリストは、各行にメッセージのＩＤが格納されている。図４の受信ＩＤリストは、メッセージＩＤが、「１」、「２」、「３」及び「４」であり、ゲートウェイ３００は、これらのメッセージＩＤのメッセージを受信する。ゲートウェイ３００は、受信ＩＤリストに含まれないメッセージＩＤのメッセージの受信を中止する。

【 0 0 7 5 】

なお、ＩＤの値及び受信ＩＤリストに含まれるＩＤの個数は説明のための一例であり、ゲートウェイ３００で用いられる受信ＩＤリストの構成をこれに限定するものではない。

【 0 0 7 6 】

〔 １．５ 転送ルール 〕

図５は、本実施の形態における転送ルールの一例を示す図である。図５において、転送ルールは、各行にメッセージの転送元のバスと転送先のバス、及び転送対象のメッセージＩＤの組み合わせが格納されている。

【 0 0 7 7 】

具体的には、転送ルールの１行目は、転送元「バス２００ a」、転送先「バス２００ b

10

20

30

40

50

」、ID「*」であり、ゲートウェイ300は、バス200aから受信するメッセージを、IDが何であってもバス200bに転送する、というルールである。転送ルールの2行目は、転送元「バス200b」、転送先「バス200a」、ID「3」であり、ゲートウェイ300は、バス200bから受信するメッセージは、IDが「3」のメッセージであればバス200aに転送する、というルールである。

【0078】

[1.6 不正検知処理機能群の構成]

図6は、本実施の形態におけるゲートウェイ300が備える不正検知処理機能群370の一例を示すブロック図である。図6において、不正検知処理機能群370は、周期判定部371と、ルール判定情報保持部372と、調停検出部373と、受信メッセージ情報保持部374とを含む。

10

【0079】

なお、これらの構成は機能を示す構成であり、ゲートウェイ300において記憶部に保持されるプログラムを処理部により読み出し、実行し、記憶部へ所定のデータを保持する。若しくは、記憶部へ所定のデータを記録することの代わりに、入出力部を介してデータの送受信を実行することでこれらの構成が実現されてもよい。又は、これらの構成は、上記の組み合わせで実現されてもよい。

【0080】

周期判定部371は、同じIDを持つメッセージごとに、メッセージを受信した周期（経過時間）が正常と判定できる範囲内に収まっているかどうかを判定する。

20

【0081】

周期判定部371は、フレーム処理部350から受信したメッセージからメッセージのIDを取得し、そのIDに関連した周期を判定するために必要な情報を取得する。具体的には、ルール、前回受信時刻、をルール判定情報保持部372から取得する。

【0082】

周期判定部371は、現在のメッセージを受信した時刻と、ルール判定情報保持部372から取得した前回受信時刻との差を求め、その差の値（経過時間）が、ルール判定情報保持部372から取得したルールで示される範囲内に含まれるかどうかを判定する。

【0083】

周期判定部371は、上記経過時間がルールで示される範囲内に含まれる場合はOKと判定し、上記経過時間がルールで示される範囲から外れる場合はNGと判定する。

30

【0084】

ここで、ルールは、同じIDのメッセージを前回受信してからの経過時間の上限と下限の情報であってもよい。また、ルールは、基準となる経過時間の値と、基準となる時間からのOKと判定される範囲の幅の情報であってもよい。

【0085】

また、周期判定部371における判定は、メッセージを受信した時刻と、前回受信時刻との差が、ルールで示される範囲内に含まれるか否かの判定をするとしたが、これに限定されない。例えば、周期判定部371は、前回受信時刻にルールで示される経過時間の範囲を足すことで、期待する受信時刻の範囲を求め、今回受信したメッセージの受信時刻が、その期待する受信時刻の範囲内に含まれるか否かを判定してもよい。

40

【0086】

また、周期判定部371は、調停検出部373に、メッセージを受信した際に調停が発生していたかどうかを問い合わせる。周期判定部371は、調停検出部373から調停が発生していたか否かを示す情報と、調停が発生していた場合は、その発生している調停の開始時刻を取得する。

【0087】

周期判定部371は、NGと判定した場合において、調停が発生していた場合、調停の開始時刻が上記ルールで示される範囲の上限より早い場合、すなわち、値が小さい場合には、判定をOKに変更する。また、調停が発生していなかった場合には、判定をNGのま

50

まで変更しない。

【 0 0 8 8 】

なお、周期判定部 3 7 1 は、メッセージを受信するたびに調停検出部 3 7 3 へ調停が発生していたか否かを問い合わせてもよい。また、ルール判定情報保持部 3 7 2 から取得したルールに対する判定が N G の場合にのみ、調停検出部 3 7 3 へ調停が発生していたか否かを問い合わせてもよい。

【 0 0 8 9 】

周期判定部 3 7 1 が、ルール判定情報保持部 3 7 2 から取得したルールに対する判定が N G の時のみ調停検出部 3 7 3 へ調停が発生していたか否かを問い合わせる場合は、周期判定部 3 7 1 は、メッセージを受信するたびに、メッセージの受信時刻を調停検出部 3 7 3 へ通知するか、受信メッセージ情報保持部 3 7 4 へ受信時刻を保存する。

10

【 0 0 9 0 】

また、周期判定部 3 7 1 は、調停検出部 3 7 3 において調停が発生していた場合、メッセージの受信時刻が基準となる経過時間の値より小さい場合に、判定を O K に変更してもよい。

【 0 0 9 1 】

また、周期判定部 3 7 1 は、判定が O K の場合に、その時に受信したメッセージの受信時刻を、ルール判定情報保持部 3 7 2 へ通知する。

【 0 0 9 2 】

ルール判定情報保持部 3 7 2 は、周期判定部 3 7 1 が使用するルールとメッセージに含まれる I D ごとのメッセージの受信時刻を保持する。ルールは、同じ I D のメッセージを前回受信してからの経過時間の上限と下限の情報であってもよい。また、基準となる経過時間の値と、基準となる経過時間の値からの O K と判定される範囲の幅を示す情報であってもよい。

20

【 0 0 9 3 】

調停検出部 3 7 3 は、周期判定部 3 7 1 からの問合せに応じて、そのメッセージを受信したときに、調停が発生していたか否かを検出する。図 7 A、図 7 B は、本実施の形態における調停発生時のメッセージの受信パターンを示す図である。図 7 A、図 7 B において、三角の記号は、1 つのメッセージを示し、横軸は時間を示しており、T 1、T 2 はメッセージを受信する予定の時刻を示している。 α は、ルール判定情報保持部 3 7 2 から取得したルールに対する判定が O K となる範囲の幅を示している。

30

【 0 0 9 4 】

図 7 A、図 7 B において、例えば、時刻 $(T 1 - \alpha)$ は、周期判定部 3 7 1 が時刻 T 1 において O K と判定する下限値であり、時刻 $(T 1 + \alpha)$ は、周期判定部 3 7 1 が時刻 T 1 において O K と判定する上限値である。

【 0 0 9 5 】

また、メッセージ M 1、メッセージ M 3 は、周期判定部 3 7 1 が時刻 T 1 に受信すると予想していたメッセージであり、メッセージ M 2、メッセージ M 4 は、調停が開始されたメッセージである。調停検出部 3 7 3 は、メッセージ M 2 又はメッセージ M 4 の受信時刻を、調停の開始時刻として、周期判定部 3 7 1 へ通知する。

40

【 0 0 9 6 】

調停検出部 3 7 3 は、予め決められた時間間隔以下でメッセージを受信した際に、調停が発生していたと判定する。例えば、図 7 A では、メッセージ M 2 からメッセージ M 1 までメッセージが連続して送信されているため、メッセージ M 2 からメッセージ M 1 まで調停が発生していたと判定する。図 7 B では、メッセージ M 4 と、メッセージ M 4 の前の時刻 T 1 に受信したメッセージ M 5 の時間間隔が広い場合、メッセージ M 4 から調停が発生したと判定する。

【 0 0 9 7 】

図 6 において、調停検出部 3 7 3 は、周期判定部 3 7 1 からメッセージの受信時刻を受け取り、受信メッセージ情報保持部 3 7 4 に格納されている、前回メッセージの受信時刻

50

を取得し、調停が発生したか否かを判定する。調停検出部 373 は、調停が発生していると判定した場合、受信メッセージ情報保持部 374 から調停が発生しているか否かを示す情報である調停発生状態情報を取得する。取得した調停発生状態情報が、調停が発生していないことを示す場合、調停検出部 373 は、調停発生開始時刻としてメッセージの受信時刻を受信メッセージ情報保持部 374 で保持する。また、調停検出部 373 は、前回のメッセージの受信時刻として、今回のメッセージの受信時刻を受信メッセージ情報保持部 374 で保持し、調停発生状態情報を受信メッセージ情報保持部 374 で保持する。

【0098】

また、調停検出部 373 は、周期判定部 371 から調停が発生しているかどうかの問い合わせがあった場合に、メッセージの受信時刻から、調停が発生しているかどうかを判定する。そして、調停が発生していた場合には、受信メッセージ情報保持部 374 から調停発生開始時刻を取得し、調停が発生している判定結果と一緒に、周期判定部 371 へ通知する。一方、調停検出部 373 は、調停が発生していなかった場合には、調停が発生していない旨を示す判定結果のみを通知する。

【0099】

なお、調停検出部 373 は、調停が発生していなかった場合には、調停が発生していない旨を示す判定結果のみを通知するとしたが、これに限定するものではない。例えば、調停検出部 373 は、判定結果と一緒に調停発生開始時刻を示す値を通知してもよいし、前回の調停発生時の調停発生開始時刻を通知してもよい。

【0100】

受信メッセージ情報保持部 374 は、調停検出部 373 が使用する前回のメッセージの受信時刻と、調停発生状態情報、調停発生開始時刻を保持する。

【0101】

なお、不正検知処理機能群 370 は、周期判定を行う機能群として説明したが、これに限定されない。図 8 は、本実施の形態における不正検知処理機能群 370 の別の一例を示す図であり、不正検知処理機能群 370 の変形例を示している。図 8 において、不正検知処理機能群 370 a は、6 種類の判定機能を含んでいる。具体的には、判定機能として、メッセージの ID フィールドをチェックする機能である ID 判定機能、メッセージのデータ長をチェックする機能であるデータ長判定機能、メッセージが送信される周期（時間間隔）をチェックする機能である送信周期判定機能、メッセージが送信される頻度をチェックする機能である送信頻度判定機能、メッセージのデータフィールドの値（データ値）をチェックする機能であるデータ値判定機能を含み、さらに、これらの判定機能の判定結果、送信周期、頻度、データ値、又はデータ値の変化量などに基づいて車両の状態を認識し、車両状態をチェックする機能である車両状態判定機能を含む。さらに不正検知処理機能群 370 a は、受信したメッセージが異常なメッセージであるか否かを、これらの判定機能による判定結果から総合的に判定する総合判定機能を含む。総合判定機能の結果が、不正検知処理機能群 370 a による不正の検知の結果となる。

【0102】

なお、図 6 における不正検知処理機能群 370 の周期判定部 371 と、ルール判定情報保持部 372 と、調停検出部 373 と、受信メッセージ情報保持部 374 とは、図 8 における不正検知処理機能群 370 a の、送信周期判定機能に組み込まれていてもよい。

【0103】

なお、これらの構成は機能を示す構成であり、ゲートウェイ 300 において記憶部に保持されるプログラムを処理部により読み出し、実行し、記憶部へ所定のデータを格納、若しくは入出力部を介してデータの送受信を実行することによって実現される。又は、これらの構成は、上記の組み合わせで実現されてもよい。

【0104】

[1.7 ECU の構成]

図 9 は、本実施の形態における車載ネットワークシステム 10 に含まれる ECU 100 の一例を示すブロック図である。図 9 において、ECU 100 は、フレーム送受信部 11

10

20

30

40

50

0と、フレーム解釈部120と、受信ID判定部130と、受信IDリスト保持部140と、フレーム処理部150と、データ取得部170と、フレーム生成部180とを備える。

【0105】

なお、これらの構成は機能を示す構成であり、ECU100は、例えばプロセッサで実現される処理部、半導体メモリ等で実現される記憶部、入出力ポートで実現される入出力部等を備える情報処理装置として提供される。

【0106】

上記の機能を示す構成は、記憶部に保持されるプログラムを処理部により読み出し、実行し、記憶部へ所定のデータを保持し、若しくは入出力部を介してデータの送受信を実行することで実現される。又は、これらの構成は、上記の組み合わせで実現されてもよい。

【0107】

フレーム送受信部110は、バス200に対して、CANのプロトコルに従ったメッセージを送受信する。

【0108】

より具体的には、フレーム送受信部110は、バス200に送出されたメッセージを1bitずつ読み出し、読み出したメッセージをフレーム解釈部120に転送する。

【0109】

また、フレーム送受信部110は、フレーム生成部180より通知を受けたメッセージをバス200に送出する。

【0110】

フレーム解釈部120は、フレーム送受信部110よりメッセージの値を受け取り、CANプロトコルにおける各フィールドにマッピングするようにしてメッセージの解釈を行う。フレーム解釈部120は、IDフィールドと解釈した一連の値を、受信ID判定部130へ転送する。

【0111】

フレーム解釈部120はさらに、受信ID判定部130から通知される判定結果に応じて、メッセージのIDフィールドの値及びIDフィールド以降に現れるデータフィールドをフレーム処理部150へ転送するか、メッセージの受信を中止するかを決定する。

【0112】

また、フレーム解釈部120は、受信したメッセージが、CANプロトコルに則っていないメッセージであると判断した場合は、エラーフレームを送信するようにフレーム生成部180へ要求する。

【0113】

また、フレーム解釈部120は、他のノードが送信したエラーフレームを受信したと判断した場合、読取中のメッセージを破棄する。

【0114】

受信ID判定部130は、フレーム解釈部120からIDフィールドの値を受け取る。そして、受信IDリスト保持部140が保持しているメッセージIDのリストに従い、読み出したメッセージを受信するか否かの判定を行う。受信ID判定部130は、この判定の結果をフレーム解釈部120へ通知する。

【0115】

受信IDリスト保持部140は、ECU100が受信する受信IDリストを保持する。受信IDリストは、図4と同様の形式であるため、ここではその説明を省略する。

【0116】

フレーム処理部150は、受信したメッセージのデータに応じた処理を行う。処理の内容は、ECU100ごとに異なる。

【0117】

例えば、ECU100aでは、自動車の時速が30kmを超えているときに、ドアが開いていることを示すメッセージを受信すると、アラーム音を鳴らすための処理を実行する

10

20

30

40

50

。ECU100cは、ブレーキがかかっていないことを示すメッセージを受信しているときにドアが開くと、アラーム音を鳴らすための処理を実行する。

【0118】

これらの処理は、説明のために一例として挙げているだけであり、ECU100は上記以外の処理を実行してもよい。このような処理を実行するために送出するフレームを、フレーム処理部150はフレーム生成部180に生成させる。

【0119】

データ取得部170は、ECU100に接続されている機器の状態を示すデータ又はセンサによる計測値等を示す出力データを取得し、フレーム生成部180に転送する。

【0120】

フレーム生成部180は、フレーム解釈部120からのエラーフレーム送信の要求に従い、エラーフレームを構成してフレーム送受信部110へ送る。

【0121】

またフレーム生成部180は、データ取得部170より受け取ったデータの値に対して予め定められたメッセージIDを付けてメッセージフレームを構成し、フレーム送受信部110へ送る。

【0122】

[1.8 不正検知処理]

図10は、本実施の形態における不正検知処理の一例を示すフローチャートである。

【0123】

まず、不正検知処理機能群370の周期判定部371は、フレーム処理部350からメッセージを受け取る(ステップS1001)。

【0124】

周期判定部371では、受け取ったメッセージが、同じIDを持つメッセージに対して、メッセージを受信した周期(経過時間)が正常と判定できる範囲内に収まっているかどうかを判定する(ステップS1002)。

【0125】

周期判定部371は、受信したメッセージが正常と判定できる範囲内に収まっていない場合(ステップS1003でYesの場合)、ステップS1004へ進む。周期判定部371は、受信したメッセージが正常と判定できる範囲内に収まっている場合(ステップS1003でNoの場合)、ステップS1007へ進む。

【0126】

ステップS1003で周期判定部371が受信したメッセージが正常と判定できる範囲内に収まっていないと判定した場合(ステップS1003でYesの場合)、調停検出部373は、メッセージ受信時に調停が発生していたか否かの検出を行う(ステップS1004)。

【0127】

調停検出部373は、メッセージ受信時に調停が発生していた場合(ステップS1005でYesの場合)、ステップS1007へ進む。調停検出部373は、メッセージ受信時に調停が発生していなかった場合(ステップS1005でNoの場合)、ステップS1006へ進む。

【0128】

ステップS1005で、調停検出部373において調停が発生していると検出した場合(ステップS1005でNoの場合)、周期判定部371は、受信したメッセージが正常なメッセージではない、すなわち、異常なメッセージであると判定する(ステップS1006)。その後、不正検知処理機能群370での不正検知処理を終了する。

【0129】

ステップS1003で、周期判定部371が受信したメッセージが正常と判定できる範囲内に収まっていると判定した場合(ステップS1003でNoの場合)又は、ステップS1005で、調停検出部373がメッセージ受信時に調停が発生したと検出した場合(

10

20

30

40

50

ステップS 1 0 0 5でY e sの場合)、周期判定部3 7 1は、受信したメッセージが正常なメッセージであると判定する(ステップS 1 0 0 7)。その後、不正検知処理機能群3 7 0での不正検知処理を終了する。

【0 1 3 0】

[1 . 9 転送処理]

図1 1は、本実施の形態における転送処理の一例を示すフローチャートである。ゲートウェイ3 0 0が行う転送処理は、転送の方向によらず実質的に共通であるため、ゲートウェイ3 0 0がバス2 0 0 aから受信したメッセージをバス2 0 0 bへ転送する場合を例に説明する。

【0 1 3 1】

まず、フレーム送受信部3 1 0は、バス2 0 0 aからメッセージを読み出す(ステップS 1 1 0 1)。フレーム送受信部3 1 0は、読み出したメッセージの各フィールドのデータをフレーム解釈部3 2 0へ通知する。

【0 1 3 2】

次に、フレーム解釈部3 2 0は、受信ID判定部3 3 0と連携して、読み出したメッセージのIDフィールドの値(メッセージID)から、受信して処理する対象のメッセージであるか否かを判定する(ステップS 1 1 0 2)。フレーム解釈部3 2 0が処理する対象のメッセージではないと判定した場合(ステップS 1 1 0 2でN oの場合)、当該メッセージの転送は行われない。

【0 1 3 3】

フレーム解釈部3 2 0は、ステップS 1 1 0 2で、受信して処理する対象のメッセージであると判断した場合には(ステップS 1 1 0 2でY e sの場合)、フレーム処理部3 5 0へメッセージ内の各フィールドの値を転送する。その後、フレーム処理部3 5 0は、転送ルール保持部3 6 0に保持される転送ルールに従って、転送先のバスを決定する(ステップS 1 1 0 3)。

【0 1 3 4】

フレーム処理部3 5 0は、フレーム解釈部3 2 0から受け取ったメッセージ内の各フィールドの値を不正検知処理機能群3 7 0へ通知し、異常なメッセージであるか否かの判定を要求する。不正検知処理機能群3 7 0は、通知されたメッセージの各フィールドの値から、通知されたメッセージが異常なメッセージであるか否かを判定し、その判定の結果をフレーム処理部3 5 0へ通知する(ステップS 1 1 0 4)。

【0 1 3 5】

ステップS 1 1 0 4で不正検知処理機能群3 7 0が、メッセージは異常なメッセージであると判定した場合(ステップS 1 1 0 5でY e sの場合)、そのメッセージの転送は行われない。

【0 1 3 6】

ステップS 1 1 0 4で不正検知処理機能群3 7 0が、メッセージは異常なメッセージではなく正常なメッセージであると判定した場合(ステップS 1 1 0 5でN oの場合)、フレーム処理部3 5 0は、そのメッセージをステップS 1 1 0 3で決定した転送先のバスに、転送しようフレーム生成部3 8 0へ要求する。

【0 1 3 7】

フレーム生成部3 8 0は、フレーム処理部3 5 0からの要求を受けて、指定された転送先が受信しようメッセージを生成し、このメッセージをフレーム送受信部3 1 0に送出させる(ステップS 1 1 0 6)。

【0 1 3 8】

なお、上記の例では、受信したメッセージの転送先の決定(ステップS 1 1 0 3)の後にこのメッセージが異常なメッセージであるかの判定(ステップS 1 1 0 4)がなされているが、これに限定されない。受信したメッセージが異常なメッセージであるかの判定の後にこのメッセージの転送先の決定がなされてもよい。また、受信したメッセージの転送先の決定と異常なメッセージであるかの判定が並行して行われてもよい。

10

20

30

40

50

【 0 1 3 9 】

[1 . 1 0 効果]

本実施の形態では、不正検知処理機能群 3 7 0 は、車載ネットワークシステムのネットワークを流れるメッセージを監視し、メッセージが所定の周期より遅れて受信された場合、調停によって遅れたのかどうかを判定することで、異常なメッセージであるか否かを判定する。これにより従来の不正検知の技術で用いられていたような、例えば所定の周期より短い時間間隔でメッセージを受信したときに、不正が発生したと判断する技術では、正常なメッセージであるか異常なメッセージであるかの判定が困難であったメッセージに関しても、より高い精度で異常なメッセージであるか否かを判定することが可能になる。その結果、車載ネットワークシステムの安全性が高められる。

10

【 0 1 4 0 】

(実施の形態 2)

[2 . 概要]

実施の形態 2 では、実施の形態 1 の不正検知処理機能群 3 7 0 の代わりに、不正検知処理機能群 3 7 0 b が用いられる。不正検知処理機能群 3 7 0 b において周期判定部が、ルール判定情報保持部へ通知するメッセージの受信時刻の決定に、調停検出部 3 7 3 の検出結果を利用する。このような不正検知処理機能群 3 7 0 b は、実施の形態 1 で説明した図 3 における不正検知処理機能群 3 7 0 に代えてゲートウェイ 3 0 0 に含まれ得る。

【 0 1 4 1 】

なお、この不正検知処理機能群 3 7 0 b を含むゲートウェイ、及びこのゲートウェイを備える車載ネットワークシステムは実施の形態 1 と基本的に共通のため、その構成についての説明を省略する。

20

【 0 1 4 2 】

[2 . 1 不正検知処理機能群の構成]

図 1 2 は、本実施の形態における不正検知処理機能群 3 7 0 b を示すブロック図である。図 1 2 において、図 6 と同じ構成要素については同じ符号を用い、説明を省略する。また、同じ構成の一部については、図示を省略する。以下、不正検知処理機能群 3 7 0 b について、不正検知処理機能群 3 7 0 との差異点を中心に説明する。

【 0 1 4 3 】

不正検知処理機能群 3 7 0 b は、実施の形態 1 における不正検知処理機能群 3 7 0 の構成に加え、周期起点決定部 3 7 5 と、送信タイプ判定部 3 7 6 を含む。また、不正検知処理機能群 3 7 0 b は、周期判定部 3 7 1 に代えて周期判定部 3 7 1 b を含む。

30

【 0 1 4 4 】

これらの構成は機能を示す構成であり、ゲートウェイ 3 0 0 において記憶部に保持されるプログラムを処理部により読み出し、実行し、記憶部へ所定のデータを保持する。若しくは、記憶部へ所定のデータを記録することの代わりに、入出力部を介してデータの送受信を実行することで実現される。又は、これらの構成は上記の組み合わせで実現される。

【 0 1 4 5 】

周期起点決定部 3 7 5 は、周期判定部 3 7 1 b がメッセージを受信した周期（経過時間）が正常と判断できる範囲内に収まっているかどうかを判定するときに、経過時間を算出するための起点として利用する「前回受信時刻」の値を決定する。周期起点決定部 3 7 5 は、周期判定部 3 7 1 b からの問合せを受け、経過時間を算出するための起点として利用する「前回受信時刻」の値を決定し、周期判定部 3 7 1 b へ通知する。

40

【 0 1 4 6 】

周期起点決定部 3 7 5 は、受信したメッセージの ID を送信タイプ判定部 3 7 6 へ通知し、送信タイプの判定を依頼する。周期起点決定部 3 7 5 は、送信タイプ判定部 3 7 6 が判定した結果に応じて、「前回受信時刻」の値を決定する。

【 0 1 4 7 】

例えば、メッセージの受信時刻（今回受信時刻）を「前回受信時刻」の値とする送信タイプ（A タイプ）と、メッセージを受信する予定だった時刻（受信予定時刻）、つまり、

50

前回受信時刻に、ルールとして保持している基準となる経過時間を足した値を「前回受信時刻」の値とする送信タイプ（Ｂタイプ）とがあるとする。

【 0 1 4 8 】

この時、周期起点決定部 3 7 5 は、送信タイプ判定部 3 7 6 が送信タイプをＡタイプと判定したときは、今回受信時刻を「前回受信時刻」として周期判定部 3 7 1 b へ通知する。また、周期起点決定部 3 7 5 は、送信タイプ判定部 3 7 6 が送信タイプをＢタイプと判定したときには、受信予定時刻を「前回受信時刻」として周期判定部 3 7 1 b へ通知する。

【 0 1 4 9 】

また、周期起点決定部 3 7 5 は、周期判定部 3 7 1 b から受信したメッセージと共に、そのメッセージを受信した際に調停が発生していたかどうかの情報も取得し、調停が発生していたかどうかで、起点となる時刻を決定してもよい。

10

【 0 1 5 0 】

例えば、そのメッセージを受信した際に調停が発生していなかった場合には、周期起点決定部 3 7 5 は常に今回受信時刻を「前回受信時刻」として周期判定部 3 7 1 b へ通知する。そして、そのメッセージを受信した際に調停が発生していた場合にのみ、周期起点決定部 3 7 5 は送信タイプ判定部 3 7 6 へ送信タイプの判定を依頼し、得られた送信タイプによって起点となる時刻を上述した方法等で決定してもよい。

【 0 1 5 1 】

送信タイプ判定部 3 7 6 は、周期起点決定部 3 7 5 からの問合せに応じて、受信したメッセージのＩＤから、送信タイプを判定し、周期起点決定部 3 7 5 へ通知する。

20

【 0 1 5 2 】

送信タイプの判定は、例えば、送信タイプ判定部 3 7 6 が、ＩＤとそのＩＤの送信タイプの組が記載されたテーブルを事前に保持しておき、周期起点決定部 3 7 5 からの問合せに応じて、事前に保持しておいたテーブルから、受信したメッセージのＩＤに対応した送信タイプを判定する。

【 0 1 5 3 】

周期判定部 3 7 1 b は、実施の形態 1 における周期判定部 3 7 1 と同様の処理を行い、受信したメッセージが最終的に正常なメッセージであると判定した際に、ルール判定情報保持部 3 7 2 に保持を依頼する前回受信時刻の決定を、周期起点決定部 3 7 5 へ依頼する。つまり、周期判定部 3 7 1 b は、周期起点決定部 3 7 5 が通知してきた前回受信時刻を、ルール判定情報保持部 3 7 2 へ通知し、保持を依頼する。

30

【 0 1 5 4 】

なお、周期起点決定部 3 7 5 は、メッセージを受信した際に調停が発生していたかどうかの情報を、周期判定部 3 7 1 b から取得するとしたが、これに限定されない。例えば、周期起点決定部 3 7 5 が直接、調停検出部 3 7 3 からメッセージを受信した際に調停が発生していたかどうかの情報を取得してもよい。

【 0 1 5 5 】

[2 . 2 不正検知処理]

図 1 3 は、本実施の形態における不正検知処理の一例を示すフローチャートである。図 1 0 と共通のステップについては、図 1 3 において同じ参照符号を用いて示し、一部説明を省略する。

40

【 0 1 5 6 】

まず、不正検知処理機能群 3 7 0 b の周期判定部 3 7 1 b は、フレーム処理部 3 5 0 からメッセージを受け取る（ステップ S 1 0 0 1 ）。

【 0 1 5 7 】

ステップ S 1 0 0 2 からステップ S 1 0 0 7 までの処理は、図 1 0 と共通であるため、説明を省略する。

【 0 1 5 8 】

周期判定部 3 7 1 は、ステップ S 1 0 0 7 で受信したメッセージが正常なメッセージで

50

あると判定すると、周期起点決定部 375 へ、前回受信時刻の決定を依頼する。周期判定部 371b は、周期起点決定部 375 が通知してきた前回受信時刻を、ルール判定情報保持部 372 へ通知し、ルール判定情報保持部 372 が保持する前回受信時刻を更新する (S1008)。その後、不正検知処理機能群 370b での不正検知処理は終了する。

【0159】

[2.3 効果]

本実施の形態では、不正検知処理機能群 370b での不正検知処理において、周期判定部 371 がメッセージを受信した周期 (経過時間) が正常と判断できる範囲内に収まっているかどうかを判定する際に利用する「前回受信時刻」の値を、送信タイプ又は、調停が発生していたかどうかにより柔軟に決定する。これにより、従来起こりえた、ID ごとに送信方法が異なる場合又は、調停が発生した際の送信タイミングのズレにより周期検知が正しくできない場合でも、より高い精度で異常なメッセージであるか否かの判定をすることができる。その結果、車載ネットワークシステムの安全性が高められる。

【0160】

[3. その他の変形例]

本開示は、上記で説明した各実施の形態に限定されない。本開示の趣旨を逸脱しない限り、当業者が思いつく各種変形を実施の形態に施したもの、及び異なる実施の形態における構成要素を組み合わせて構築される形態も、本開示の範囲内に含まれる。例えば以下のような変形例も本開示に含まれる。

【0161】

(1) 上記の実施の形態 2 では、不正検知処理機能群 370b は、周期判定部 371b と、ルール判定情報保持部 372 と、調停検出部 373 と、受信メッセージ情報保持部 374 と、周期起点決定部 375 と、送信タイプ判定部 376 とを備えると説明したが、これに限定されない。

【0162】

図 14 は、変形例における不正検知処理機能群の一例を示す図である。図 14 に示すように、不正検知処理機能群 370c は、周期判定部 371c と、ルール判定情報保持部 372 と、調停検出部 373 と、受信メッセージ情報保持部 374 と、周期起点決定部 375c と、送信タイプ判定部 376c と、周期タイプ学習部 377 と、周期タイプ保持部 378 とを備える。

【0163】

周期タイプ学習部 377 は、周期判定部 371c から受信した情報を元に、ID ごとの周期タイプを判定する。判定方法としては、例えば、周期タイプ学習部 377 は、ID ごとに受信したメッセージの受信時刻を記録 (蓄積) していき、一定数の受信時刻が蓄積できたタイミングで、ID ごとにそれぞれの受信時刻の一つ前の受信時刻との差 (経過時間) を求める。

【0164】

周期タイプ学習部 377 は、その受信時刻の差が、ID ごとに決められている経過時間の基準値と比較したときに、(1) 基準値と同程度か、(2) 基準値より短いか、(3) 基準値より長いかを判定する。

【0165】

ここで、基準値と同程度か否かの判定には、予め決められたしきい値 (上限用と下限用) を用いる。周期タイプ学習部 377 は、基準値から下限用のしきい値を引いた値から、基準値に上限用のしきい値を足した値の間に、経過時間が含まれる場合に、「基準値と同程度」と判定し、経過時間が、基準値から下限用のしきい値を引いた値より小さい場合に、「基準値より短い」と判定し、経過時間が、基準値に上限用のしきい値を足した値より大きい場合に、「基準値より長い」と判定する。

【0166】

周期タイプ学習部 377 は、判定した結果 (1. 基準値と同程度か、2. 基準値より短い、3. 基準値より長い) の数を ID と一緒に周期タイプ保持部 378 へ通知する。

【 0 1 6 7 】

周期タイプ保持部 3 7 8 は、周期タイプ学習部 3 7 7 から通知された周期タイプの判定結果を保持し、送信タイプ判定部 3 7 6 からの問合せに応じて、周期タイプを通知する。周期タイプ保持部 3 7 8 は、周期タイプ学習部 3 7 7 からの通知を受けた際に、既に通知された I D と同じ I D の判定結果を保持していた場合、新たに通知された判定結果で上書きしてもよいし、既に保持していた値に足した値で更新してもよい。

【 0 1 6 8 】

周期判定部 3 7 1 c は、受信したメッセージのうち、最終的に O K と判定したメッセージに関する情報を、周期タイプ学習部 3 7 7 へ通知する。

【 0 1 6 9 】

送信タイプ判定部 3 7 6 c は、周期起点決定部 3 7 5 c から送信タイプの判定を依頼された際に、依頼された I D に関連する受信タイミングごとの経過時間と経過時間の基準値とを比較した結果を周期タイプ保持部 3 7 8 より取得する。送信タイプ判定部 3 7 6 は、(2) 基準値より短いと判定した数が、(3) 基準値より長いと判定した数より少なかった場合、送信タイプが A タイプであると判定し、(2) 基準値より短いと判定した数と、(3) 基準値より長いと判定した数とが、ほぼ同じ数であった場合に、送信タイプが B タイプであると判定し、それ以外の場合は、送信タイプが判定できないと判定する。(2) 基準値より短いと判定した数が (3) 基準値より長いと判定した数より少ないとの判定は、判定した数そのものが予め決められた数以上の差があるかどうかで判定してもよいし、判定した数の比が予め決められた値より小さいかどうかで判定してもよい。(1) 基準値と同じぐらいか、(2) 基準値より短いか、(3) 基準値より長いかのそれぞれの割合を求め、その割合が予め決められた値以上の差があるかどうかで判定してもよい。(2) 基準値より短いと判定した数と、(3) 基準値より長いと判定した数とが、ほぼ同じ数との判定は、判定した数そのものが予め決められた数以内の差に収まっているかどうか判定してもよいし、判定した数の比が予め決められた値より大きい、または予め決められた範囲に収まっているかどうかで判定してもよい。(1) 基準値と同じぐらいか、(2) 基準値より短いか、(3) 基準値より長いかのそれぞれの割合を求め、その割合が予め決められた値以内の差に収まっているかどうかで判定してもよい。

【 0 1 7 0 】

送信タイプ判定部 3 7 6 c は、周期起点決定部 3 7 5 c からの要求に応じて、判定した結果を通知する。送信タイプ判定部 3 7 6 c は、送信タイプが判定できなかった場合には、予め決められたタイプを周期起点決定部 3 7 5 c へ通知する。

【 0 1 7 1 】

なお、周期タイプ学習部 3 7 7 は、I D ごとに受信したメッセージの受信時刻を記録していき、一定数の受信時刻が蓄積できたタイミングで、I D ごとにそれぞれの受信時刻の一つ前の受信時刻との差(経過時間)を求めるとしたが、これに限定されるものではない。

【 0 1 7 2 】

例えば、周期タイプ学習部 3 7 7 は、車両が工場から出荷される前に、周期タイプを学習する時間を設け、その間に受信したメッセージの受信時刻を蓄積し、I D ごとにそれぞれの受信時刻の一つ前の受信時刻との差(経過時間)を求めてもよい。

【 0 1 7 3 】

さらに、周期タイプ学習部 3 7 7 は、工場出荷後から受信時刻を蓄積し、一定数、または、一定時間、受信時刻を蓄積したタイミングで、I D ごとにそれぞれの受信時刻の一つ前の受信時刻との差(経過時間)を求めてもよい。

【 0 1 7 4 】

また、周期タイプ学習部 3 7 7 は、車両外部の機器からメッセージの受信時刻を蓄積するように指示を受け、受信時刻を蓄積し、外部の機器から蓄積停止の指示を受けるまで一定数、または、一定時間、受信時刻を蓄積したタイミングで、I D ごとにそれぞれの受信時刻の一つ前の受信時刻との差(経過時間)を求めてもよい。

【 0 1 7 5 】

また、周期タイプ学習部 3 7 7 は、メッセージを受信するたびに受信時刻を記録し、一定数、または、一定時間の受信時刻が蓄積できた後は、メッセージを受信するごとに、受信時刻の一つ前の受信時刻との差（経過時間）を求めてもよい。

【 0 1 7 6 】

なお、周期タイプ学習部 3 7 7 は、受信時刻を記録し、あるタイミングで I D ごとにそれぞれの受信時刻の一つ前の受信時刻との差（経過時間）を求めるとしたが、これに限定されるものではない。例えば、周期タイプ学習部 3 7 7 は、メッセージを受信するごとに、前のメッセージの受信時刻との差（経過時間）を求め、経過時間を記録（蓄積）し、最新の受信時刻を記録してもよい。

10

【 0 1 7 7 】

なお、基準値と同じぐらいかどうかの判定には、予め決められたしきい値（上限用と下限用）を用いるとしたが、これに限定されるものではない。例えば、1つのしきい値を用いて、下限も上限も同じ値を用いてもよいし、基準値としきい値という組み合わせではなく、下限値と上限値の2つの値を用いてもよい。

【 0 1 7 8 】

なお、周期タイプ学習部 3 7 7 は、判定した結果（（1）基準値と同じぐらいか、（2）基準値より短いか、（3）基準値より長いか）の数を周期タイプ保持部 3 7 8 へ通知するとしたが、これに限定されるものではない。例えば、割合を通知してもよいし、周期タイプ保持部 3 7 8 へ既に保持されている値があれば、その値に、今回の値を足した数を通知してもよい。

20

【 0 1 7 9 】

これにより、送信タイプを事前に設定することなく、自動的に送信タイプを判定することが可能となる。更に、修理などで E C U が交換された場合にも、自動的に送信タイプを判定することが可能となる。その結果、更なる不正検知精度の向上又は、処理コスト、製造コストを低減することが可能となる。

【 0 1 8 0 】

（2）上記の実施の形態 2 では、不正検知処理機能群 3 7 0 b は、周期判定部 3 7 1 b と、ルール判定情報保持部 3 7 2 と、調停検出部 3 7 3 と、受信メッセージ情報保持部 3 7 4 と、周期起点決定部 3 7 5 と、送信タイプ判定部 3 7 6 とを備えると説明したが、これに限定されない。

30

【 0 1 8 1 】

図 1 5 は、変形例における不正検知処理機能群の一例を示す図である。図 1 5 に示すように、不正検知処理機能群 3 7 0 d は、周期判定部 3 7 1 b と、ルール判定情報保持部 3 7 2 と、調停検出部 3 7 3 と、受信メッセージ情報保持部 3 7 4 と、周期起点決定部 3 7 5 d とを備える。

【 0 1 8 2 】

周期起点決定部 3 7 5 d は、メッセージの受信時に調停が発生していたかどうかで、周期の起点を決定する。例えば、調停が発生していなかった場合には、周期起点決定部 3 7 5 d は今回受信時刻を「前回受信時刻」として周期判定部 3 7 1 b へ通知し、調停が発生していた場合には、周期起点決定部 3 7 5 d は受信予定時刻を「前回受信時刻」として周期判定部 3 7 1 b へ通知する。

40

【 0 1 8 3 】

なお、周期起点決定部 3 7 5 d は、今回受信時刻を「前回受信時刻」とするか、受信予定時刻を「前回受信時刻」とするかを周期判定部 3 7 1 b へ通知するとしたが、これに限定されるものではない。

【 0 1 8 4 】

例えば、周期起点決定部 3 7 5 d は、調停が発生した1回目は今回受信時刻を「前回受信時刻」として、その後、調停が連続して発生する度に、予め決められた時間又は予め決められた割合で、受信予定時刻へ近づけた時刻を「前回受信時刻」として周期判定部 3 7

50

1 bへ通知してもよい。また、調停が発生した1回目から受信予定時刻へ近づけた時刻を「前回受信時刻」として周期判定部371bへ通知してもよい。

【0185】

また、周期起点決定部375dは、それぞれのIDごとに事前に、どれだけ今回受信時刻から受信予定時刻へ近づけた時刻を「前回受信時刻」として周期判定部371bへ通知するかを、例えば、歪度(Skewness)又は尖度(Kurtosis)などの統計的な数値を用いて算出しておき、その事前に算出しておいた値分、今回受信時刻から受信予定時刻へ近づけた時刻を「前回受信時刻」として周期判定部371bへ通知してもよい。

【0186】

また、歪度又は尖度だけでなく、中央値又は平均値、最頻値などから求まる値又は、標準偏差などの値を使用して、どれだけ今回受信時刻から受信予定時刻へ近づけた時刻を「前回受信時刻」とするかを決定してもよい。この時、それぞれの値を個別に利用してもよいし、いくつかの値から計算した値を用いてもよい。また、周期タイプ学習部377により、これらを学習してもよい。

【0187】

これにより、前回時刻を二者択一で決定するよりも、柔軟に決定することが出来るため、より検知精度を向上させることが出来る。

【0188】

(3) 上記各実施の形態では、ECU100は、フレーム送受信部110と、フレーム解釈部120と、受信ID判定部130と、受信IDリスト保持部140と、フレーム処理部150と、データ取得部170と、フレーム生成部180とを備えると説明したが、本開示における車載ネットワークシステムが備えるECU100の構成はこれに限定されるものではない。

【0189】

図16は、変形例におけるECUの一例を示すブロック図である。図16に示すECU100eは、さらに不正検知処理機能群370を備える。この場合、異常なメッセージであるか否かの判定を、フレーム処理部150が不正検知処理機能群370へ要求してもよいし、フレーム解釈部120が要求してもよい。

【0190】

図17は、変形例におけるECUの一例を示すブロック図である。図17に示すECU100fは、フレーム送受信部110と、フレーム解釈部120と、フレーム生成部180とで構成される。この場合、フレーム解釈部120は、例えばIDによらず全てのメッセージを受信し、全てのメッセージについて不正検知処理機能群370へ異常なメッセージであるかどうかの判定を依頼してもよい。

【0191】

また、ECU100fは、図17の構成に加えて、受信ID判定部130と、受信IDリスト保持部140とを備え、受信IDリスト保持部が保持する受信IDリストに記載されたメッセージIDを持つメッセージのみを受信し、そのメッセージに関して、不正検知処理機能群370へ異常なメッセージであるか否かの判定を依頼してもよい。なお、不正検知処理機能群370は、上述の370a~370dのいずれに代えられてもよい。

【0192】

これにより、ゲートウェイだけでなく、ECU100でも、バスに送信されているメッセージが異常なメッセージであるか否かを判定できる。その結果、例えば車載ネットワークシステムにおける不正検知のための仕組の冗長性が向上し、より高度に安全が確保される。

【0193】

図18は、変形例におけるECUの一例を示すブロック図である。図18に示すECU100gは、バス200へ送信するデータを他の接続機器又は外部等から取得する送信データ取得部171を備えてもよい。ECU100gが備える不正検知処理機能群370e

10

20

30

40

50

は、送信データ取得部 171 から受信したデータが異常なメッセージであるか否かについても判定し、異常なメッセージではないと判定した場合のみ、フレーム生成部 180 へメッセージの送信を依頼してもよい。なお、不正検知処理機能群 370 e の構成は、不正検知処理機能群 370、370 a、370 b、370 c、370 d のいずれかの構成と共通であってもよい。

【0194】

これにより、例えば、カーナビゲーションと一緒に利用される ECU 100 f が、乗っ取られたカーナビゲーションから異常なメッセージが送信されるような場合において、そのメッセージのネットワークへの拡散を抑制することができる。または、車外から送り込みが試みられる異常なメッセージの車載ネットワークシステム内部への侵入を抑制することができる。

10

【0195】

(4) 上記各実施の形態では、不正の検知に応じたアクションとして、受信したメッセージを転送しない例を示したが、これに限定されない。例えば、上述の不正検知処理機能群を備えるゲートウェイ又は ECU 100 は、メッセージの受信中に不正検知処理を行い、異常なメッセージであると判定した時点で、エラーフレームを送信することで、ネットワークから受信中のメッセージを無効化してもよい。

【0196】

これにより、異常なメッセージが見つかったバスに接続された他の ECU 100 が異常なメッセージを受信することを防止することができる。同様のアクションは、転送しないメッセージに対しても適用できる。

20

【0197】

また、上述の不正検知処理機能群を備えるゲートウェイ 300 又は ECU 100 はさらに、不正の発生のユーザ若しくは外部のサーバ等への通知、不正の発生のログへの記録、又は車両のフェールセーフモードへの移行を実行してもよい。

【0198】

これにより、不正検知後の柔軟な対応が可能となる。また異常なメッセージと判定した複数のメッセージをデータの 1 以上の系列として扱い、各系列について、データの値又は受信間隔の集合を不正なラベルとして学習してもよい。

【0199】

30

(5) 上記各実施の形態では、標準フォーマットの ID における例を示したが、拡張フォーマットの ID であってもよい。

【0200】

(6) 上記各実施の形態では、メッセージは平文で送信される例を示したが、暗号化されていてもよい。またメッセージにメッセージ認証コードを含んでいてもよい。

【0201】

(7) 上記実施の形態では、正常モデルと、受信ログとを平文で保持している例を示したが、これらを暗号化して保持していてもよい。

【0202】

(8) 上記の実施の形態では、CAN プロトコルに従って通信するネットワーク通信システムの例として車載ネットワークを示した。本開示に係る技術は、車載ネットワークでの利用に限定されるものではなく、ロボット、産業機器等のネットワークその他、車載ネットワーク以外の CAN プロトコルに従って通信するネットワーク通信システムに利用してもよい。

40

【0203】

また、車載ネットワークシステム 10 として CAN プロトコルを用いていたが、これに限るものではない。例えば、CAN - FD (CAN with Flexible Data Rate)、FlexRay、Ethernet、LIN (Local Interconnect Network)、MOST (Media Oriented Systems Transport) などを用いてもよい。あるいはこれらのネットワーク

50

をサブネットワークとして、組み合わせたネットワークであってもよい。

【0204】

(9) 上記の実施の形態における各装置は、具体的には、マイクロプロセッサ、ROM (Read Only Memory)、RAM (Random Access Memory)、ハードディスクユニット、ディスプレイユニット、キーボード、マウスなどから構成されるコンピュータシステムである。RAMまたはハードディスクユニットには、コンピュータプログラムが記録されている。マイクロプロセッサが、コンピュータプログラムにしたがって動作することにより、各装置は、その機能を達成する。ここでコンピュータプログラムは、所定の機能を達成するために、コンピュータに対する指令を示す命令コードが複数個組み合わせられて構成されたものである。

10

【0205】

(10) 上記の実施の形態における各装置は、構成する構成要素の一部または全部は、1個のシステムLSI (Large Scale Integration: 大規模集積回路) から構成されているとしてもよい。システムLSIは、複数の構成部を1個のチップ上に集積して製造された超多機能LSIであり、具体的には、マイクロプロセッサ、ROM、RAMなどを含んで構成されるコンピュータシステムである。RAMには、コンピュータプログラムが記録されている。マイクロプロセッサが、コンピュータプログラムにしたがって動作することにより、システムLSIは、その機能を達成する。

【0206】

また、上記の各装置を構成する構成要素の各部は、個別に1チップ化されていても良いし、一部又はすべてを含むように1チップ化されてもよい。

20

【0207】

また、ここでは、システムLSIとしたが、集積度の違いにより、IC (Integrated Circuit)、LSI、スーパーLSI、ウルトラLSIと呼称されることもある。また、集積回路化の手法はLSIに限るものではなく、専用回路又は汎用プロセッサで実現してもよい。LSI製造後に、プログラムすることが可能なFPGA (Field Programmable Gate Array) 又は、LSI内部の回路セルの接続又は設定を再構成可能なりコンフィギュラブル・プロセッサを利用してもよい。

【0208】

さらには、半導体技術の進歩又は派生する別技術によりLSIに置き換わる集積回路化の技術が登場すれば、当然、その技術を用いて機能ブロックの集積化を行ってもよい。バイオ技術の適用等が可能性としてありえる。

30

【0209】

(11) 上記の各装置を構成する構成要素の一部または全部は、各装置に脱着可能なICカードまたは単体のモジュールから構成されているとしてもよい。ICカードまたはモジュールは、マイクロプロセッサ、ROM、RAMなどから構成されるコンピュータシステムである。ICカードまたはモジュールは、上記の超多機能LSIを含むとしてもよい。マイクロプロセッサが、コンピュータプログラムにしたがって動作することにより、ICカードまたは前記モジュールは、その機能を達成する。このICカードまたはこのモジュールは、耐タンパ性を有するとしてもよい。

40

【0210】

(12) 本開示は、上記に示す方法であるとしてもよい。また、これらの方法をコンピュータにより実現するコンピュータプログラムであるとしてもよいし、コンピュータプログラムからなるデジタル信号であるとしてもよい。

【0211】

また、本開示は、コンピュータプログラムまたはデジタル信号をコンピュータ読み取り可能な記録媒体、例えば、フレキシブルディスク、ハードディスク、CD-ROM、MO、DVD、DVD-ROM、DVD-RAM、BD (Blu-ray (登録商標) Disc)、半導体メモリなどに記録したものとしてもよい。また、これらの記録媒体に記録されているデジタル信号であるとしてもよい。

50

【 0 2 1 2 】

また、本開示は、コンピュータプログラムまたはデジタル信号を、電気通信回線、無線または有線通信回線、インターネットを代表とするネットワーク、データ放送等を経由して伝送するものとしてもよい。

【 0 2 1 3 】

また、本開示は、マイクロプロセッサとメモリを備えたコンピュータシステムであって、メモリは、上記コンピュータプログラムを記録しており、マイクロプロセッサは、コンピュータプログラムにしたがって動作するものとしてもよい。

【 0 2 1 4 】

また、プログラムまたはデジタル信号を記録媒体に記録して移送することにより、またはプログラムまたはデジタル信号を、ネットワーク等を経由して移送することにより、独立した他のコンピュータシステムにより実施するものとしてもよい。

【 0 2 1 5 】

(1 3) 上記実施の形態及び上記変形例をそれぞれ組み合わせるものとしてもよい。

【 0 2 1 6 】

以上、一つ又は複数の態様に係る車載ネットワークにおける、異常なメッセージによる不正制御を目的とする不正通信検知の基準として用いられるメッセージの決定のための技術について実施の形態及びその変形例に基づいて説明した。これらの各実施の形態及びその変形例では、車載ネットワークシステムに接続されて通信するゲートウェイ若しくは ECU、又はこれらとサーバコンピュータとの組み合わせによって不正通信検知の基準として用いられるメッセージが決定される。このような不正通信検知を実行する、1個以上のプロセッサ及び記憶部を含むシステムを、本開示では不正通信検知基準決定システムと呼ぶ。したがって、不正通信検知基準決定システムは車載ネットワークシステムに接続される1台のゲートウェイのように1個の装置によって実現されるものも、このようなゲートウェイと ECU との組み合わせ、又はゲートウェイ若しくは ECU と遠隔にあるサーバコンピュータとの組み合わせのように複数個の装置によって実現されるものも含む。

【 0 2 1 7 】

また、この技術は、上記各実施の形態又はその変形例において、各構成要素が実行する処理のステップの一部又は全部を含む方法として、又は不正通信検知基準決定システムのプロセッサに実行されて、不正通信検知基準決定システムがこの方法を実施させるためのプログラムとしても実現可能である。

【 0 2 1 8 】

また、上記実施の形態又はその変形例において、特定の構成要素が実行する処理を特定の構成要素の代わりに別の構成要素が実行してもよい。また、複数の処理の順序が変更されてもよいし、複数の処理が並行して実行されてもよい。

【産業上の利用可能性】

【 0 2 1 9 】

本開示にかかる車載ネットワークシステム等に適用可能である。

【符号の説明】

【 0 2 2 0 】

1 0 車載ネットワークシステム

1 0 0、1 0 0 a、1 0 0 b、1 0 0 c、1 0 0 d、1 0 0 e、1 0 0 f、1 0 0 g

ECU

1 0 1 エンジン

1 0 2 ブレーキ

1 0 3 ドア開閉センサ

1 0 4 ウィンドウ開閉センサ

1 1 0 フレーム送受信部

1 2 0 フレーム解釈部

1 3 0 受信 ID 判定部

10

20

30

40

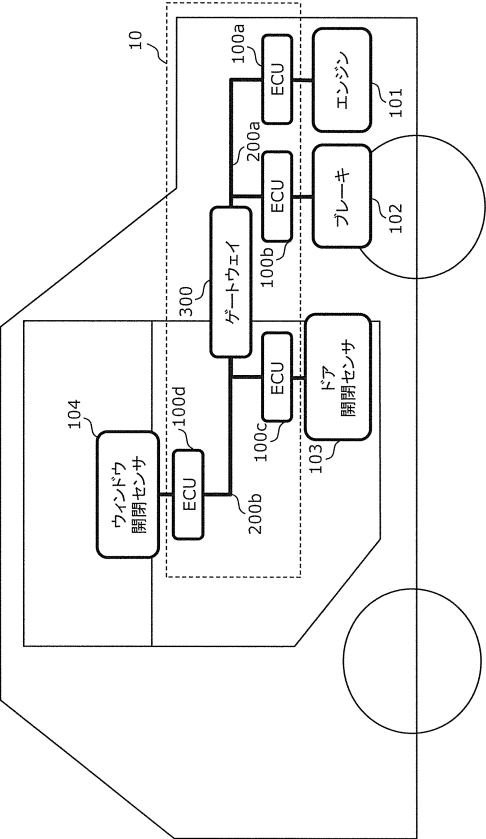
50

140	受信IDリスト保持部	
150	フレーム処理部	
170	データ取得部	
171	送信データ取得部	
180、380	フレーム生成部	
200、200a、200b	バス	
300	ゲートウェイ	
310	フレーム送受信部	
320	フレーム解釈部	
330	受信ID判定部	10
340	受信IDリスト保持部	
350	フレーム処理部	
360	転送ルール保持部	
370、370a、370b、370c、370d、370e	不正検知処理機能群	
371、371b、371c	周期判定部	
372	ルール判定情報保持部	
373	調停検出部	
374	受信メッセージ情報保持部	
375、375c、375d	周期起点決定部	
376、376c	送信タイプ判定部	20
377	周期タイプ学習部	
378	周期タイプ保持部	

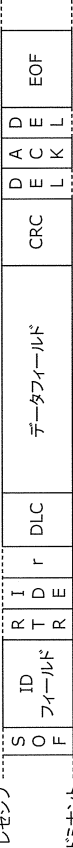
【要約】

車載ネットワークに、繰り返し送出されたメッセージの周期が異常であるか否かを判定する周期異常判定ステップ（S1002）と、メッセージが車載ネットワークに送出された際に調停が発生していたか否かを検出する調停検出ステップ（S1004）と、メッセージの周期が異常であり、メッセージが車載ネットワークに送出された際に調停が発生していなかった場合、メッセージを異常なメッセージと判定するメッセージ判定ステップ（S1006）を含む。

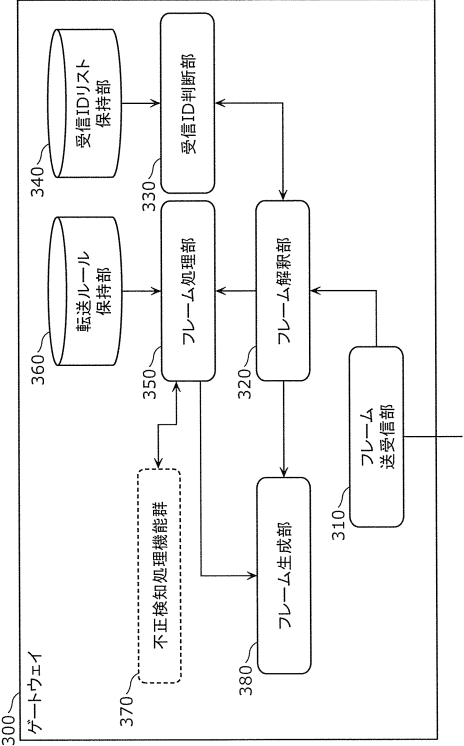
【図 1】



【図 2】



【図 3】



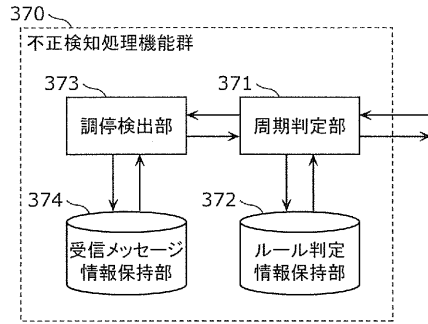
【図 4】

受信IDリスト
1
2
3
4

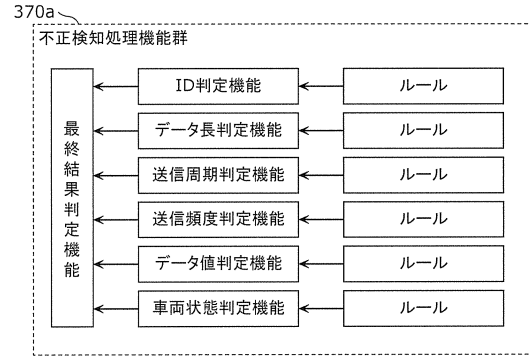
【図 5】

転送元	転送先	ID
バス200a	バス200b	*
バス200b	バス200a	3

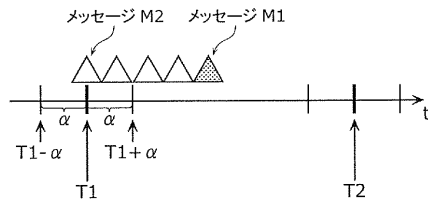
【図 6】



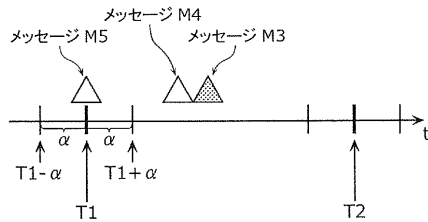
【図 8】



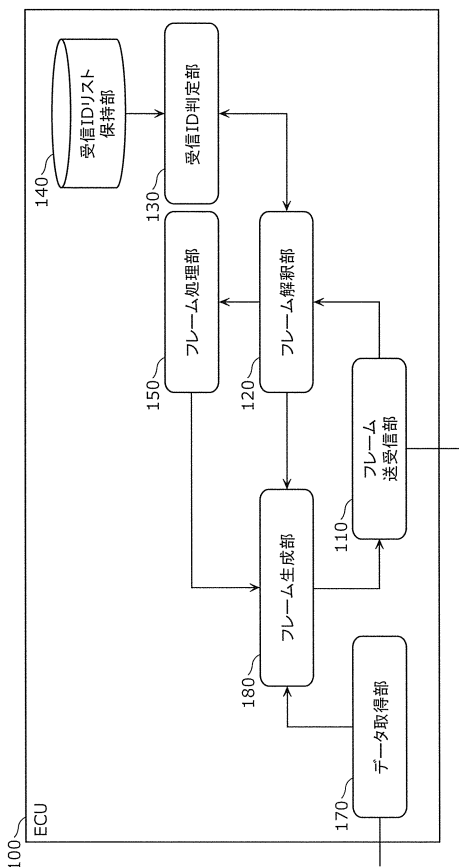
【図 7 A】



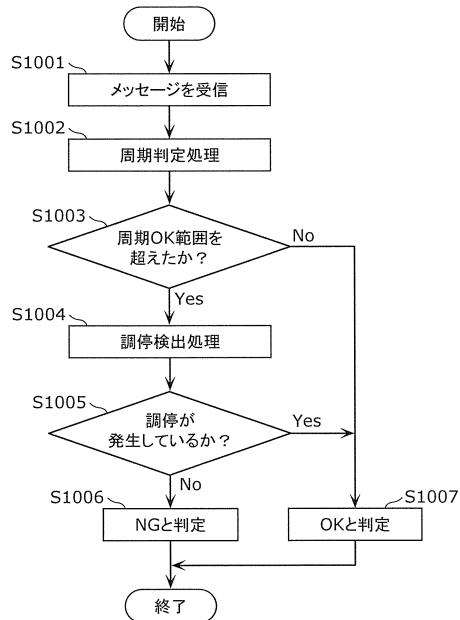
【図 7 B】



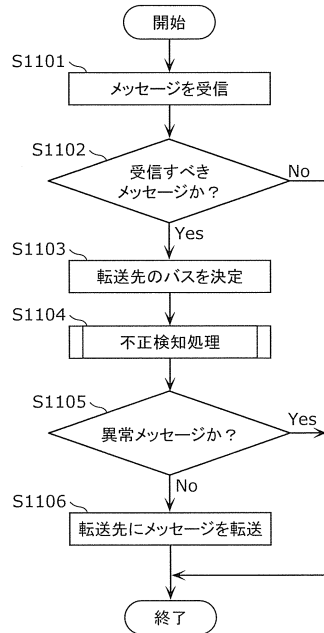
【図 9】



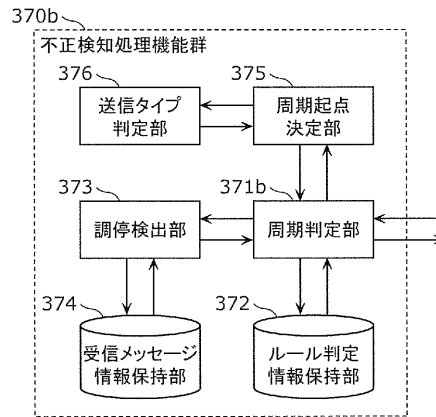
【図 10】



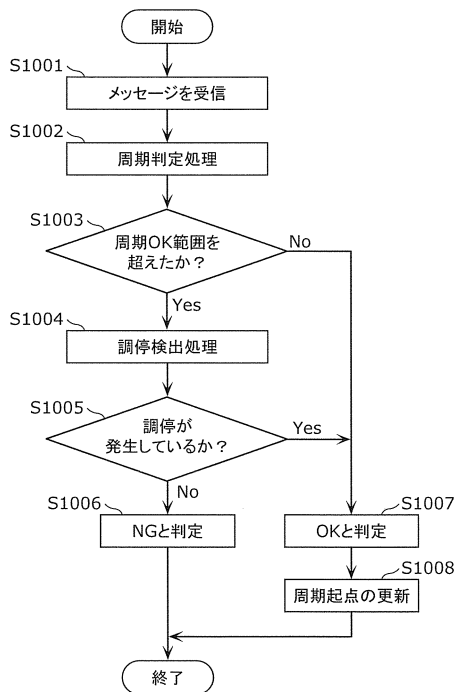
【図 1 1】



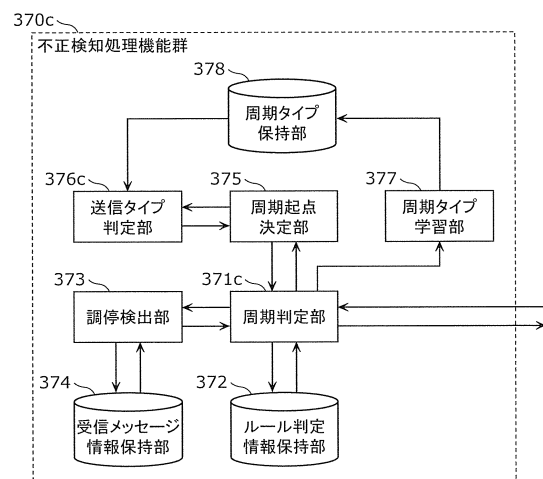
【図 1 2】



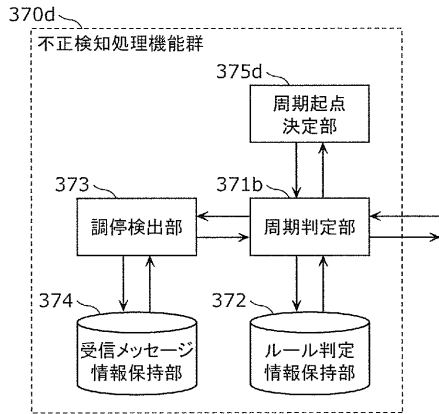
【図 1 3】



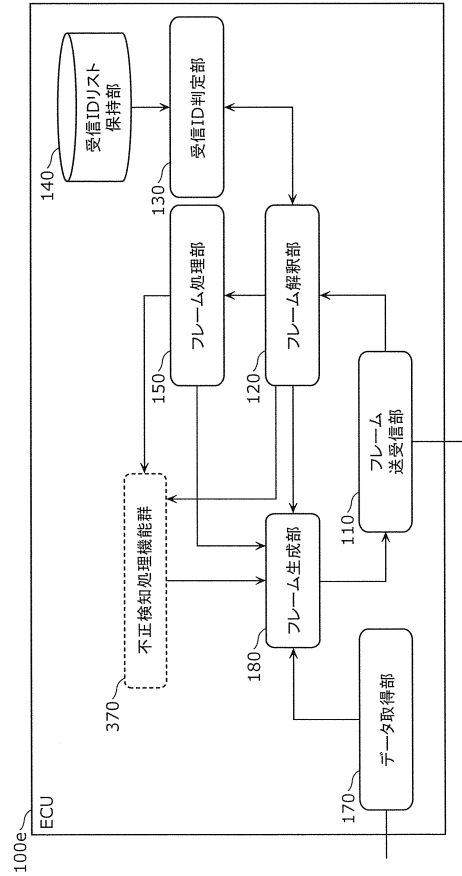
【図 1 4】



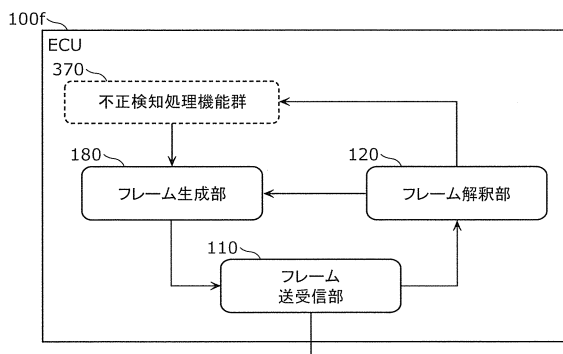
【 図 1 5 】



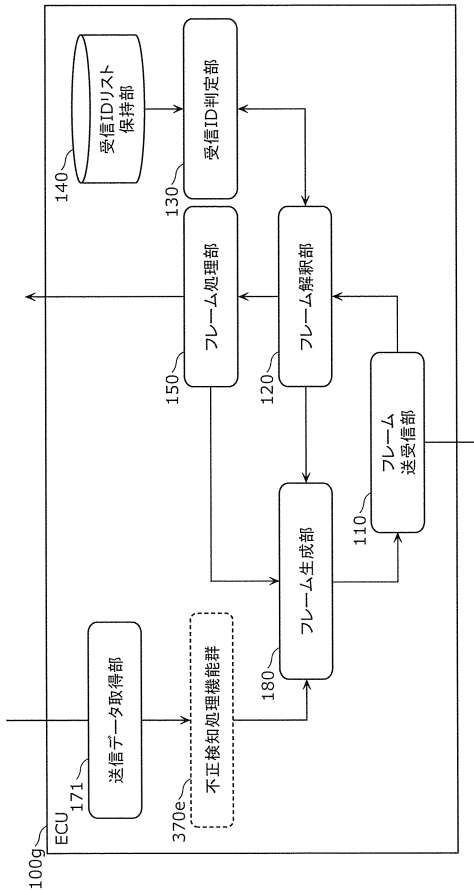
【 図 1 6 】



【 図 1 7 】



【 図 1 8 】



フロントページの続き

(74)代理人 100131417

弁理士 道坂 伸一

(72)発明者 前田 学

日本国大阪府門真市大字門真 1 0 0 6 番地 パナソニック株式会社内

(72)発明者 岸川 剛

日本国大阪府門真市大字門真 1 0 0 6 番地 パナソニック株式会社内

(72)発明者 国宗 大介

日本国京都府長岡京市神足焼町 1 番地 パナソニックデバイスシステムテクノ株式会社内

審査官 松崎 孝大

(56)参考文献 国際公開第 2 0 1 3 / 0 9 4 0 7 2 (W O , A 1)

特開 2 0 1 4 - 1 4 6 8 6 8 (J P , A)

特開 2 0 1 6 - 1 3 4 9 1 3 (J P , A)

国際公開第 2 0 1 7 / 1 5 4 8 2 8 (W O , A 1)

国際公開第 2 0 1 8 / 0 5 1 6 0 7 (W O , A 1)

(58)調査した分野(Int.Cl. , D B 名)

H 0 4 L 1 2 / 2 8