

(19) 日本国特許庁 (JP)

(12) 特 許 公 報 (B2)

(11) 特許番号

特許第6417407号
(P6417407)

(45) 発行日 平成30年11月7日 (2018. 11. 7)

(24) 登録日 平成30年10月12日 (2018. 10. 12)

(51) Int. Cl.	F I
HO 4 L 9/32 (2006. 01)	HO 4 L 9/00 6 7 5 A
GO 6 F 21/44 (2013. 01)	HO 4 L 9/00 6 7 3 B
HO 4 L 9/36 (2006. 01)	GO 6 F 21/44
	HO 4 L 9/00 6 8 5

請求項の数 14 (全 52 頁)

(21) 出願番号	特願2016-517804 (P2016-517804)	(73) 特許権者	514136668
(86) (22) 出願日	平成27年4月21日 (2015. 4. 21)		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/JP2015/002161		パティ コーポレーション オブ アメリ
(87) 国際公開番号	W02015/170451		カ
(87) 国際公開日	平成27年11月12日 (2015. 11. 12)		Panasonic Intellectual
審査請求日	平成29年11月9日 (2017. 11. 9)		Property Corporation of America
(31) 優先権主張番号	61/990, 360		アメリカ合衆国 90503 カリフォル
(32) 優先日	平成26年5月8日 (2014. 5. 8)		ニア州, トーランス, スイート 200,
(33) 優先権主張国	米国 (US)		マリナー アベニュー 20000
(31) 優先権主張番号	特願2015-32206 (P2015-32206)	(74) 代理人	100109210
(32) 優先日	平成27年2月20日 (2015. 2. 20)		弁理士 新居 広守
(33) 優先権主張国	日本国 (JP)	(74) 代理人	100137235
			弁理士 寺谷 英作

最終頁に続く

(54) 【発明の名称】 車載ネットワークシステム、電子制御ユニット及び不正検知方法

(57) 【特許請求の範囲】

【請求項 1】

CAN (Controller Area Network) プロトコルに従ってバスを介して通信する複数の電子制御ユニットを備える車載ネットワークシステムにおいて用いられる不正検知方法であって、

前記バス上で送信されたデータフレームを受信する受信ステップと、

前記受信ステップで送信周期に係る所定ルールに適合しないデータフレームが受信され、かつ、前記車載ネットワークシステムを搭載する車両の状態が所定の状態である場合に限り、当該データフレーム中の特定識別子を検証する検証ステップとを含み、

前記検証ステップで、前記特定識別子についての前記検証が成功したときには、当該データフレームを正当なデータフレームとして検知し、

前記検証ステップで、前記特定識別子についての前記検証が失敗したときには、当該データフレームを不正なデータフレームとして検知する

不正検知方法。

【請求項 2】

前記特定識別子は、前記データフレームのデータフィールド内の所定位置に配置され当該データフレームの内容を反映するメッセージ認証コードであり、

前記検証ステップでは、前記所定ルールに適合しない前記データフレーム中の前記所定位置のデータが前記メッセージ認証コードであるか否かを当該データフレームの内容に基づき判別する所定処理手順により、前記検証が行われる

10

20

請求項 1 記載の不正検知方法。

【請求項 3】

前記特定識別子は、前記データフレームのデータフィールド内の所定位置に配置される所定値であり、

前記検証ステップでは、前記所定ルールに適合しない前記データフレーム中の前記所定位置のデータの値が前記所定値と同一であるか否かを判別することにより前記検証が行われる

請求項 1 記載の不正検知方法。

【請求項 4】

前記特定識別子は、前記データフレームのデータフィールド内の所定位置に配置されるカウンタ値であり、

前記検証ステップでは、前記所定ルールに適合しない前記データフレーム中の前記所定位置のデータの値が、前記受信ステップで前記所定ルールに適合しないデータフレームが受信された回数を反映した前記カウンタ値と同一であるか否かを判別することにより前記検証が行われる

請求項 1 記載の不正検知方法。

【請求項 5】

前記受信ステップでのデータフレームの受信は繰り返し行われ、

前記特定識別子は、前記データフレームのデータフィールド内の所定位置に配置される、所定演算の結果値であり、

前記検証ステップでは、前記受信ステップで受信された前記所定ルールに適合しない前記データフレーム中の前記所定位置のデータの値が、前記受信ステップで前回受信された前記特定識別子を含むデータフレーム中の当該特定識別子に基づいて前記所定演算を行った結果として得られる結果値と、同一であるか否かを判別することにより前記検証が行われる

請求項 1 記載の不正検知方法。

【請求項 6】

前記受信ステップで前記所定ルールに適合するデータフレームが受信された場合には当該データフレームを正当なデータフレームとして検知する

請求項 1 記載の不正検知方法。

【請求項 7】

CAN (Controller Area Network) プロトコルに従ってバスを介して通信する複数の電子制御ユニットを備える車載ネットワークシステムにおいて不正検知の対象となるデータフレームを送信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を搭載する車両の状態が所定の状態である場合に、送信周期に係る所定ルールに適合しないデータフレームを送信するときに限って、当該データフレーム中に特定識別子を付与する付与ステップと、

前記付与ステップで付与された特定識別子を含み前記所定ルールに適合しないデータフレームを前記バスにより送信する送信ステップとを含む

不正検知方法。

【請求項 8】

前記付与ステップでは、前記データフレームのデータフィールド内の所定位置に、前記特定識別子として当該データフレームの内容を反映するメッセージ認証コードを配置することにより前記特定識別子の前記付与が行われる

請求項 7 記載の不正検知方法。

【請求項 9】

前記付与ステップでは、前記データフレームのデータフィールド内の所定位置に、前記特定識別子として所定値を配置することにより前記特定識別子の前記付与が行われる

請求項 7 記載の不正検知方法。

【請求項 10】

前記付与ステップでは、前記データフレームのデータフィールド内の所定位置に、前記送信ステップで前記所定ルールに適合しないデータフレームが送信された回数を反映したカウンタ値を前記特定識別子として配置することにより前記特定識別子の前記付与が行われる

請求項7記載の不正検知方法。

【請求項11】

前記所定ルールに適合しないデータフレームについての前記送信ステップでの送信及び前記付与ステップでの特定識別子の付与は繰り返行われ、

前記付与ステップでは、前記送信ステップでのデータフレームの送信に際して当該データフレームのデータフィールド内の所定位置に、前記送信ステップで前回送信された前記所定ルールに適合しないデータフレームに付与した特定識別子に基づいて所定演算を行った結果として得られる値を、特定識別子として配置することにより前記特定識別子の前記付与が行われる

請求項7記載の不正検知方法。

【請求項12】

CAN (Controller Area Network) プロトコルに従ってバスを介して通信する複数の電子制御ユニットを備える車載ネットワークシステムであって、

前記車載ネットワークシステムを搭載する車両の状態が所定の状態である場合に、送信周期に係る所定ルールに適合しないデータフレームを送信するときに限って当該データフレーム中に特定識別子を付与する付与部と、前記付与部で付与された特定識別子を含み前記所定ルールに適合しないデータフレームを前記バスにより送信する送信部とを有する第1電子制御ユニットと、

前記バス上で送信されたデータフレームを受信する受信部と、前記受信部により前記所定ルールに適合しないデータフレームが受信され、かつ、前記車載ネットワークシステムを搭載する車両の状態が所定の状態である場合に限って、当該データフレーム中の特定識別子を検証する検証部とを有し、前記検証部は、前記特定識別子についての前記検証が成功したときには、当該データフレームを正当なデータフレームとして検知し、前記特定識別子についての前記検証が失敗したときには、当該データフレームを不正なデータフレームとして検知する第2電子制御ユニットとを備える

車載ネットワークシステム。

【請求項13】

CAN (Controller Area Network) プロトコルに従ってバスを介して通信する電子制御ユニットであって、

前記電子制御ユニットを含む車載ネットワークシステムを搭載する車両の状態が所定の状態である場合に、送信周期に係る所定ルールに適合しないデータフレームを送信するときに限って当該データフレーム中に特定識別子を付与する付与部と、

前記付与部で付与された特定識別子を含み前記所定ルールに適合しないデータフレームを前記バスにより送信する送信部とを備える

電子制御ユニット。

【請求項14】

CAN (Controller Area Network) プロトコルに従ってバスを介して通信する電子制御ユニットであって、

前記バス上で送信されたデータフレームを受信する受信部と、

前記受信部により送信周期に係る所定ルールに適合しないデータフレームが受信され、かつ、前記電子制御ユニットを含む車載ネットワークシステムを搭載する車両の状態が所定の状態である場合に限って、当該データフレーム中の特定識別子を検証する検証部とを備え、前記検証部は、前記特定識別子についての前記検証が成功したときには、当該データフレームを正当なデータフレームとして検知し、前記特定識別子についての前記検証が失敗したときには、当該データフレームを不正なデータフレームとして検知する

電子制御ユニット。

【発明の詳細な説明】

【技術分野】

【0001】

本開示は、電子制御ユニットが通信を行う車載ネットワークにおいて送信された不正なフレームを検知する技術に関する。

【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（E C U : Electronic Control Unit）と呼ばれる装置が多数配置されている。これらのE C Uをつなぐ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一つに、I S O 1 1 8 9 8 - 1で規定されているC A N（Controller Area Network）という規格が存在する（「非特許文献1」参照）。

10

【0003】

C A Nでは、通信路は2本のバスで構成され、バスに接続されているE C Uはノードと呼ばれる。バスに接続されている各ノードは、フレームと呼ばれるメッセージを送受信する。フレームを送信する送信ノードは、2本のバスに電圧をかけ、バス間で電位差を発生させることによって、レセシブと呼ばれる「1」の値と、ドミナントと呼ばれる「0」の値を送信する。複数の送信ノードが全く同一のタイミングで、レセシブとドミナントを送信した場合は、ドミナントが優先されて送信される。受信ノードは、受け取ったフレームのフォーマットに異常がある場合には、エラーフレームと呼ばれるフレームを送信する。エラーフレームとは、ドミナントを6 b i t連続して送信することで、送信ノードや他の受信ノードにフレームの異常を通知するものである。

20

【0004】

またC A Nでは送信先や送信元を指す識別子は存在せず、送信ノードはフレーム毎にメッセージI Dと呼ばれるI Dを付けて送信し（つまりバスに信号を送出し）、各受信ノードは予め定められたメッセージI Dのみを受信する（つまりバスから信号を読み取る）。また、C S M A / C A（Carrier Sense Multiple Access/Collision Avoidance）方式を採用しており、複数ノードの同時送信時にはメッセージI Dによる調停が行われ、メッセージI Dの値が小さいフレームが優先的に送信される。

【0005】

30

車載ネットワークにおいて不正なノードがバスに接続され、不正なノードが不正にデータフレームを送信した場合に、C A Nでは送信元の識別子が存在しないことから、不正なデータフレームが送信されていることを受信ノードは検知できない。

【0006】

そこで従来、E C Uが周期的にデータフレームを送信するという特徴を用いて、正常な周期から逸脱するようなデータフレームの送信を不正なデータフレームであると検知する技術が提案されている（「非特許文献2」参照）。またデータフレームが正規のE C Uから送信されていることを示すために、メッセージ認証コード（M A C : Message Authentication Code）の技術を用いた不正検知方法が提案されている（「非特許文献3」参照）。

40

【先行技術文献】

【非特許文献】

【0007】

【非特許文献1】“C A N S p e c i f i c a t i o n 2 . 0 P a r t A”、[online]、C A N i n A u t o m a t i o n (C i A)、[平成26年11月14日検索]、インターネット（URL：<http://www.can-cia.org/fileadmin/cia/specifications/CAN20A.pdf>）

【非特許文献2】大塚敏史、石郷岡祐、“既存E C Uを変更不要な車載L A N向け侵入検知手法”、情報処理学会研究報告、組込みシステム研究会、2013-EMB-28（6

50

）、p. 1-5

【非特許文献3】D. K. Nilsson、U. E. Larson、E. Jonsson、
“Efficient In-Vehicle Delayed Data Authentication Based on Compound Message Authentication Codes”、Vehicular Technology Conference、2008-Fall、p. 1-5

【非特許文献4】RFC2104 HMAC: Keyed-Hashing for Message Authentication

【発明の概要】

【発明が解決しようとする課題】

10

【0008】

しかしながら、非特許文献2の技術では、ECUが周期的にデータフレームを送信するのに加えて、イベントをトリガに非周期的にデータフレーム（以下、非周期的に送信されるデータフレームを「イベントドリブンデータフレーム」と称する。）を送信することもある場合には、正当なイベントドリブンデータフレームを不正なデータフレームと誤検知してしまう。また、送信する全てのデータフレームにMACを付加する方法では、MACの付加及び検証に要する処理負荷が大きい。

【0009】

そこで、本開示は、CANプロトコル等に従って通信する車載ネットワークシステムにおいて、バス上に不正なメッセージの送信が行われたことを効率的かつ適切に検知する電子制御ユニット（ECU）を提供する。また、本開示は、不正なメッセージを効率的かつ適切に検知するための不正検知方法、及び、ECUを備える車載ネットワークシステムを提供する。

20

【課題を解決するための手段】

【0010】

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、CAN（Controller Area Network）プロトコルに従ってバスを介して通信する複数の電子制御ユニットを備える車載ネットワークシステムにおいて用いられる不正検知方法であって、前記バス上で送信されたデータフレームを受信する受信ステップと、前記受信ステップで送信周期に係る所定ルールに適合しないデータフレームが受信され、かつ、前記車載ネットワークシステムを搭載する車両の状態が所定の状態である場合に限って、当該データフレーム中の特定識別子を検証する検証ステップとを含み、前記検証ステップで、前記特定識別子についての前記検証が成功したときには、当該データフレームを正当なデータフレームとして検知し、前記検証ステップで、前記特定識別子についての前記検証が失敗したときには、当該データフレームを不正なデータフレームとして検知する不正検知方法である。

30

【0011】

また本開示の一態様に係る不正検知方法は、CAN（Controller Area Network）プロトコルに従ってバスを介して通信する複数の電子制御ユニットを備える車載ネットワークシステムにおいて不正検知の対象となるデータフレームを送信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を搭載する車両の状態が所定の状態である場合に、送信周期に係る所定ルールに適合しないデータフレームの送信するときに限って、当該データフレーム中に特定識別子を付与する付与ステップと、前記付与ステップで付与された特定識別子を含み前記所定ルールに適合しないデータフレームを前記バスにより送信する送信ステップとを含む不正検知方法である。

40

【0012】

また、上記課題を解決するために本開示の一態様に係る車載ネットワークシステムは、CAN（Controller Area Network）プロトコルに従ってバスを介して通信する複数の電子制御ユニットを備える車載ネットワークシステムであって、前記車載ネットワークシステムを搭載する車両の状態が所定の状態である場合に、送信周期に係る所定ルールに適合しないデータフレームの送信するときに限って当該データフレーム中に特定識別子を付与

50

する付与部と、前記付与部で付与された特定識別子を含み前記所定ルールに適合しないデータフレームを前記バスにより送信する送信部とを有する第1電子制御ユニットと、前記バス上で送信されたデータフレームを受信する受信部と、前記受信部により前記所定ルールに適合しないデータフレームが受信され、かつ、前記車載ネットワークシステムを搭載する車両の状態が所定の状態である場合に限り、当該データフレーム中の特定識別子を検証する検証部とを有し、前記検証部は、前記特定識別子についての前記検証が成功したときには、当該データフレームを正当なデータフレームとして検知し、前記特定識別子についての前記検証が失敗したときには、当該データフレームを不正なデータフレームとして検知する第2電子制御ユニットとを備える車載ネットワークシステムである。

【0013】

10

また、上記課題を解決するために本開示の一態様に係る電子制御ユニット（ECU）は、CAN（Controller Area Network）プロトコルに従ってバスを介して通信する電子制御ユニットであって、前記電子制御ユニットを含む車載ネットワークシステムを搭載する車両の状態が所定の状態である場合に、送信周期に係る所定ルールに適合しないデータフレームの送信に際して当該データフレーム中に特定識別子を付与する付与部と、前記付与部で付与された特定識別子を含み前記所定ルールに適合しないデータフレームを前記バスにより送信する送信部とを備える電子制御ユニットである。

【0014】

また本開示の一態様に係る電子制御ユニット（ECU）は、CAN（Controller Area Network）プロトコルに従ってバスを介して通信する電子制御ユニットであって、前記バス上で送信されたデータフレームを受信する受信部と、前記受信部により送信周期に係る所定ルールに適合しないデータフレームが受信され、かつ、前記電子制御ユニットを含む車載ネットワークシステムを搭載する車両の状態が所定の状態である場合に限り、当該データフレーム中の特定識別子を検証する検証部とを備え、前記検証部は、前記特定識別子についての前記検証が成功したときには、当該データフレームを正当なデータフレームとして検知し、前記特定識別子についての前記検証が失敗したときには、当該データフレームを不正なデータフレームとして検知する電子制御ユニットである。

20

【発明の効果】

【0015】

本開示によれば、車載ネットワークシステムでバスに不正なノードが接続されて不正なデータフレームが送信された場合に効率的かつ適切にその検知が可能となる。

30

【図面の簡単な説明】

【0016】

【図1】実施の形態1に係る車載ネットワークシステムの全体構成を示す図である。

【図2】CANプロトコルで規定されるデータフレームのフォーマットを示す図である。

【図3】実施の形態1に係る車載ネットワークシステムで用いられるデータフィールドフォーマットの一例を示す図である。

【図4】実施の形態1に係るECUの構成図である。

【図5】実施の形態1に係るデータフレーム生成ルールの一例を示す図である。

【図6】実施の形態1に係る周期ルール情報の一例を示す図である。

40

【図7】実施の形態1に係るデータフレームの前回受信時刻を示す情報を列挙したリストの一例を示す図である。

【図8】実施の形態1に係るデータフレームの送受信の流れを示す図である。

【図9】実施の形態1に係るデータフレームの送信処理を示すフローチャートである。

【図10】実施の形態1に係るデータフレームの受信処理を示すフローチャートである。

【図11】実施の形態2に係る車載ネットワークシステムの全体構成を示す図である。

【図12】実施の形態2に係る車載ネットワークシステムで用いられるデータフィールドフォーマットの一例を示す図である。

【図13】実施の形態2に係るECUの構成図である。

【図14】実施の形態2に係るデータフレーム生成ルール及び送信イベントカウンタの一

50

例を示す図である。

【図 1 5】実施の形態 2 に係るデータフレームの前回受信時刻及び受信イベントカウンタを列挙したリストの一例を示す図である。

【図 1 6】実施の形態 2 に係るデータフレームの送信処理を示すフローチャートである。

【図 1 7】実施の形態 2 に係るデータフレームの受信処理を示すフローチャートである。

【図 1 8】実施の形態 3 に係る車載ネットワークシステムの全体構成を示す図である。

【図 1 9】実施の形態 3 に係る車載ネットワークシステムで用いられるデータフィールドフォーマットの一例を示す図である。

【図 2 0】実施の形態 3 に係る ECU の構成図である。

【図 2 1】実施の形態 3 に係るデータフレーム生成ルールの一例を示す図である。

10

【図 2 2】実施の形態 3 に係る周期ルール情報の一例を示す図である。

【図 2 3】実施の形態 3 に係るデータフレームの送信処理を示すフローチャートである。

【図 2 4】実施の形態 3 に係るデータフレームの受信処理を示すフローチャートである。

【図 2 5】実施の形態 4 に係る車載ネットワークシステムの全体構成を示す図である。

【図 2 6】実施の形態 4 に係る ECU の構成図である。

【図 2 7】実施の形態 4 に係るデータフレーム生成ルールの一例を示す図である。

【図 2 8】実施の形態 4 に係る周期ルール情報の一例を示す図である。

【図 2 9】実施の形態 4 に係る車状態保持部に保持された車両の状態の一例を示す図である。

【図 3 0】実施の形態 4 に係るデータフレームの送信処理を示すフローチャートである。

20

【図 3 1】実施の形態 4 に係るデータフレームの受信処理を示すフローチャートである。

【図 3 2】実施の形態 4 に係る車両の状態を示すデータフレームの送信処理を示すフローチャートである。

【図 3 3】実施の形態 4 に係るデータフレームの受信処理の変形例を示すフローチャートである。

【発明を実施するための形態】

【0017】

本開示の一態様に係る不正検知方法は、CAN (Controller Area Network) プロトコルに従ってバスを介して通信する複数の電子制御ユニットを備える車載ネットワークシステムにおいて用いられる不正検知方法であって、前記バス上で送信されたデータフレームを受信する受信ステップと、前記受信ステップで送信周期に係る所定ルールに適合しないデータフレームが受信され、かつ、前記車載ネットワークシステムを搭載する車両の状態が所定の状態である場合に限って、当該データフレーム中の特定識別子を検証する検証ステップとを含み、前記検証ステップで、前記特定識別子についての前記検証が成功したときには、当該データフレームを正当なデータフレームとして検知し、前記検証ステップで、前記特定識別子についての前記検証が失敗したときには、当該データフレームを不正なデータフレームとして検知する不正検知方法である。ここで、送信周期に係る所定ルールは、予め定められたルールであり、例えば同一 ID を有するデータフレームの送信周期（前回送信時刻から今回送信時刻までの時間差）についての条件である。不正検知方法において検証は不正なデータフレームの検知のために行われるものであり、データフレームについて検証に成功した場合には、そのデータフレームは不正と検知されない。これにより、送信周期が条件を満たさないデータフレームつまりイベントドリブンデータフレームが受信された場合において所定ルールに基づく正当性の判断はできないが特定識別子の検証により正当性の判断が可能になる。このため、所定ルールを満たさないため不正であると誤検知することが防止され、不正なデータフレーム（メッセージ）を適切に検知することが可能となる。また、この所定ルールに適合しないデータフレームについての特定識別子の検証により不正なメッセージは検知可能となるため、全てのデータフレームについて特定識別子を含ませてその検証をする必要がなく、効率的な不正の検知が可能となる。なお、効率的な不正の検知は、車載ネットワークシステムの電力消費の抑制に繋がる。所定の状態は、例えば、不正なデータフレームがバス上に流れている場合に検知されるべき必要

30

40

50

性が、所定の状態以外の状態よりも高いと想定される状態である。これにより、例えば不正検知の必要性が高いとき等といった車両が所定の状態である場合に効率的に検証を行うことが可能となる。また、データフレームを受信するECUにとっては、例えば不正検知の必要性が高いとき等の所定の状態である場合に限って効率的に検証を行うことが可能となる。

【0018】

また、前記特定識別子は、前記データフレームのデータフィールド内の所定位置に配置され当該データフレームの内容を反映するメッセージ認証コードであり、前記検証ステップでは、前記所定ルールに適合しない前記データフレーム中の前記所定位置のデータが前記メッセージ認証コードであるか否かを当該データフレームの内容に基づき判別する所定処理手順により、前記検証が行われることとしても良い。これにより、送信周期に係る所定ルール及び検証の所定処理手順を知らない不正なECU（例えば車載ネットワークシステムの正規な構成要素であるECU以外のECU）にとって、検証に成功するように特定識別子を含むデータフレームを送信することが比較的困難となり得る。

10

【0019】

また、前記特定識別子は、前記データフレームのデータフィールド内の所定位置に配置される所定値であり、前記検証ステップでは、前記所定ルールに適合しない前記データフレーム中の前記所定位置のデータの値が前記所定値と同一であるか否かを判別することにより前記検証が行われることとしても良い。ここで、特定識別子は1ビットでも複数ビットで構成されても良い。これにより、所定値と比較するのみという比較的負荷の少ない処理手順で不正検知のための検証を行うことができるようになる。

20

【0020】

また、前記特定識別子は、前記データフレームのデータフィールド内の所定位置に配置されるカウンタ値であり、前記検証ステップでは、前記所定ルールに適合しない前記データフレーム中の前記所定位置のデータの値が、前記受信ステップで前記所定ルールに適合しないデータフレームが受信された回数を反映した前記カウンタ値と同一であるか否かを判別することにより前記検証が行われることとしても良い。これにより、特定識別子がデータフレームの送受信に応じて変動し得るカウンタ値となるため、不正なECUにとって、検証に成功するように特定識別子を含むデータフレームを送信することが比較的困難となり得る。

30

【0021】

また、前記受信ステップでのデータフレームの受信は繰り返し行われ、前記特定識別子は、前記データフレームのデータフィールド内の所定位置に配置される、所定演算の結果値であり、前記検証ステップでは、前記受信ステップで受信された前記所定ルールに適合しない前記データフレーム中の前記所定位置のデータの値が、前記受信ステップで前回受信された前記特定識別子を含むデータフレーム中の当該特定識別子に基づいて前記所定演算を行った結果として得られる結果値と、同一であるか否かを判別することにより前記検証が行われることとしても良い。所定演算は、例えば、送信周期に係る所定ルールに適合しない（非周期的な）データフレームを送受信する正当な送信側と受信側とで共通して行われる演算（関数）であり、入力値に基づいて出力値（結果値）が導出される。送信側と受信側で前回の非周期的なデータフレームが送信されたときの特定識別子である所定演算の結果値をそれぞれ記憶していれば、送信側が前回の特定識別子を入力とした所定演算（関数）の出力値（結果値）を次の非周期的なデータフレームに設定して送信し、受信側では受信したデータフレームに、前回の特定識別子を入力とした所定演算の結果値と同一の値が含まれていることを検証することができる。これにより、不正なECUにとって、検証に成功するように特定識別子を含むデータフレームを送信することが比較的困難となり得る。

40

【0022】

また、前記検証ステップでは、前記受信したデータフレームが、前記所定ルールに適合するか否かを判定し、前記受信したデータフレームが前記所定ルールに適合しないと判定

50

された場合に、前記車両の状態が前記所定の状態であるか否かを判定し、前記車両の状態が前記所定の状態であると判定された場合に、前記特定識別子についての前記検証を行っても良い。また、前記受信ステップで前記所定ルールに適合するデータフレームが受信された場合には当該データフレームを正当なデータフレームとして検知することとしても良い。また、前記検証ステップで、前記受信ステップで前記所定ルールに適合しないデータフレームが受信され、かつ、前記車載ネットワークシステムを搭載する車両の状態が前記所定の状態でない場合は、当該データフレームを正当なデータフレームとして検知することとしても良い。また、前記検証ステップで、前記受信ステップで前記所定ルールに適合しないデータフレームが受信され、かつ、前記車載ネットワークシステムを搭載する車両の状態が前記所定の状態でない場合は、当該データフレームを不正なデータフレームとして検知することとしても良い。不正なデータフレームとして検知された場合の取り扱いは車載ネットワークシステムにおいて定めておくことができ、取り扱いとしては、例えば、データフレームを破棄すること（データフレームの内容に基づいて車両の制御を行わないこと等）、ログとして記録すること、車両の動作モードを変更すること等が挙げられる。

【0023】

また本開示の一態様に係る不正検知方法は、CAN（Controller Area Network）プロトコルに従ってバスを介して通信する複数の電子制御ユニットを備える車載ネットワークシステムにおいて不正検知の対象となるデータフレームを送信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を搭載する車両の状態が所定の状態である場合に、送信周期に係る所定ルールに適合しないデータフレームの送信するときに限って、当該データフレーム中に特定識別子を付与する付与ステップと、前記付与ステップで付与された特定識別子を含み前記所定ルールに適合しないデータフレームを前記バスにより送信する送信ステップとを含む不正検知方法である。これにより、データフレームの受信側において所定ルールに適合しなくても当該データフレーム中に特定識別子が含まれていることを検証することで不正なデータフレームか否かの検知が可能となるように、車載ネットワークシステムを正規に構成する送信側のECUでは特定識別子を含めた、所定ルールに適合しないデータフレームを送信する。このため、付与ステップと送信ステップとにより適切な不正検知が実現される。また、データフレームを受信するECUにとっては、例えば不正検知の必要性が高いとき等の所定の状態である場合に限って効率的に検証を行うことが可能となる。

【0024】

また、前記付与ステップでは、前記データフレームのデータフィールド内の所定位置に、前記特定識別子として当該データフレームの内容を反映するメッセージ認証コードを配置することにより前記特定識別子の前記付与が行われることとしても良い。これにより、送信周期に係る所定ルール及びメッセージ認証コードを知らない不正なECU（例えば車載ネットワークシステムの正規な構成要素であるECU以外のECU）にとって、検証に成功するように特定識別子を含むデータフレームを送信することが比較的困難となり得る。

【0025】

また、前記付与ステップでは、前記データフレームのデータフィールド内の所定位置に、前記特定識別子として所定値を配置することにより前記特定識別子の前記付与が行われることとしても良い。これにより、データフレームを受信するECUにおいては所定値と比較するのみという比較的負荷の少ない処理手順で不正検知のための検証を行うことができるようになる。

【0026】

また、前記付与ステップでは、前記データフレームのデータフィールド内の所定位置に、前記送信ステップで前記所定ルールに適合しないデータフレームが送信された回数を反映したカウンタ値を前記特定識別子として配置することにより前記特定識別子の前記付与が行われることとしても良い。これにより、特定識別子がデータフレームの送信に応じて変動し得るカウンタ値となるため、不正なECUにとって、検証に成功するように特定識

別子を含むデータフレームを送信することが比較的困難となり得る。

【0027】

また、前記所定ルールに適合しないデータフレームについての前記送信ステップでの送信及び前記付与ステップでの特定識別子の付与は繰り返し行われ、前記付与ステップでは、前記送信ステップでのデータフレームの送信に際して当該データフレームのデータフィールド内の所定位置に、前記送信ステップで前回送信された前記所定ルールに適合しないデータフレームに付与した特定識別子に基づいて所定演算を行った結果として得られる値を、特定識別子として配置することにより前記特定識別子の前記付与が行われることとしても良い。これにより、不正なECUにとって、検証に成功するように特定識別子を含むデータフレームを送信することが比較的困難となり得る。

10

【0028】

また、前記送信ステップでは更に、前記所定ルールに適合するデータフレームの送信を行い、前記付与ステップでは、前記車載ネットワークシステムを搭載する車両の状態が所定の状態である場合に前記送信ステップで前記所定ルールに適合しないデータフレームを送信するときに限って、当該データフレーム中に特定識別子の前記付与が行われることとしても良い。所定の状態は、例えば、不正なデータフレームがバス上に流れている場合に検知されるべき必要性が、所定の状態以外の状態よりも高いと想定される状態である。これにより、データフレームを受信するECUにとっては、例えば不正検知の必要性が高いとき等の所定の状態である場合に限って効率的に検証を行うことが可能となる。

20

【0029】

また、上記課題を解決するために本開示の一態様に係る車載ネットワークシステムは、CAN (Controller Area Network) プロトコルに従ってバスを介して通信する複数の電子制御ユニットを備える車載ネットワークシステムであって、前記車載ネットワークシステムを搭載する車両の状態が所定の状態である場合に、送信周期に係る所定ルールに適合しないデータフレームの送信するときに限って当該データフレーム中に特定識別子を付与する付与部と、前記付与部で付与された特定識別子を含み前記所定ルールに適合しないデータフレームを前記バスにより送信する送信部とを有する第1電子制御ユニットと、前記バス上で送信されたデータフレームを受信する受信部と、前記受信部により前記所定ルールに適合しないデータフレームが受信され、かつ、前記車載ネットワークシステムを搭載する車両の状態が所定の状態である場合に限って、当該データフレーム中の特定識別子を
検証する検証部とを有し、前記検証部は、前記特定識別子についての前記検証が成功したときには、当該データフレームを正当なデータフレームとして検知し、前記特定識別子についての前記検証が失敗したときには、当該データフレームを不正なデータフレームとして検知する第2電子制御ユニットとを備える車載ネットワークシステムである。これにより、送信周期が条件を満たさないデータフレームつまりイベントドリブンデータフレームが受信された場合において所定ルールに基づく正当性の判断はできないが特定識別子の検証により正当性の判断が可能になる。このため、所定ルールを満たさないため不正であると誤検知することが防止され、不正なデータフレーム (メッセージ) を適切に検知することが可能となる。所定の状態は、例えば、不正なデータフレームがバス上に流れている場合に検知されるべき必要性が、所定の状態以外の状態よりも高いと想定される状態である。これにより、例えば不正検知の必要性が高いとき等といった車両が所定の状態である場合に効率的に検証を行うことが可能となる。また、データフレームを受信するECUにとっては、例えば不正検知の必要性が高いとき等の所定の状態である場合に限って効率的に検証を行うことが可能となる。

30

40

【0030】

また、上記課題を解決するために本開示の一態様に係る電子制御ユニット (ECU) は、CAN (Controller Area Network) プロトコルに従ってバスを介して通信する電子制御ユニットであって、前記電子制御ユニットを含む車載ネットワークシステムを搭載する車両の状態が所定の状態である場合に、送信周期に係る所定ルールに適合しないデータフレームの送信に際して当該データフレーム中に特定識別子を付与する付与部と、前記付与

50

部で付与された特定識別子を含み前記所定ルールに適合しないデータフレームを前記バスにより送信する送信部とを備える電子制御ユニットである。これにより、送信周期が条件を満たさないデータフレームつまりイベントドリブンデータフレームを送信する場合に、不正であると誤検知されないようにデータフレームを送信することが可能となる。所定の状態は、例えば、不正なデータフレームがバス上に流れている場合に検知されるべき必要性が、所定の状態以外の状態よりも高いと想定される状態である。これにより、例えば不正検知の必要性が高いとき等といった車両が所定の状態である場合に効率的に検証を行うことが可能となる。

【0031】

また本開示の一態様に係る電子制御ユニット（ECU）は、CAN（Controller Area Network）プロトコルに従ってバスを介して通信する電子制御ユニットであって、前記バス上で送信されたデータフレームを受信する受信部と、前記受信部により送信周期に係る所定ルールに適合しないデータフレームが受信され、かつ、前記電子制御ユニットを含む車載ネットワークシステムを搭載する車両の状態が所定の状態である場合に限り、当該データフレーム中の特定識別子を検証する検証部とを備え、前記検証部は、前記特定識別子についての前記検証が成功したときには、当該データフレームを正当なデータフレームとして検知し、前記特定識別子についての前記検証が失敗したときには、当該データフレームを不正なデータフレームとして検知する電子制御ユニットである。これにより、送信周期が条件を満たさないデータフレームつまりイベントドリブンデータフレームが受信された場合において所定ルールに基づく正当性の判断はできないが特定識別子の検証により正当性の判断が可能になる。このため、所定ルールを満たさないため不正であると誤検知することが防止され、不正なデータフレームを適切に検知することが可能となる。所定の状態は、例えば、不正なデータフレームがバス上に流れている場合に検知されるべき必要性が、所定の状態以外の状態よりも高いと想定される状態である。これにより、例えば不正検知の必要性が高いとき等といった車両が所定の状態である場合に効率的に検証を行うことが可能となる。また、データフレームを受信するECUにとっては、例えば不正検知の必要性が高いとき等の所定の状態である場合に限り効率的に検証を行うことが可能となる。

【0032】

なお、これらの全般的又は具体的な態様は、システム、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で読み取り可能なCD-ROM等の記録媒体で実現されても良く、システム、方法、集積回路、コンピュータプログラム又は記録媒体の任意な組み合わせで実現されても良い。

【0033】

以下、実施の形態に係る車載ネットワークシステム、ECU等について、図面を参照しながら説明する。ここで示す実施の形態は、いずれも本開示の一具体例を示すものである。従って、以下の実施の形態で示される数値、形状、材料、構成要素、構成要素の配置及び接続形態、並びに、ステップ（工程）及びステップの順序等は、一例であって本開示を限定するものではない。以下の実施の形態における構成要素のうち、独立請求項に記載されていない構成要素については、任意に付加可能な構成要素である。また、各図は、模式図であり、必ずしも厳密に図示されたものではない。

【0034】

（実施の形態1）

以下、本開示の実施の形態として、データフレームを送受信するECU100aとECU100bとの間で、周期的に送信されるデータフレームに加えて非周期的なイベントドリブンデータフレームが送信され得る前提の下で、不正なデータフレームが送信されたことを適切に検知するための不正検知方法を実現する車載ネットワークシステム10について図面を用いて説明する。

【0035】

[1. 1 車載ネットワークシステム10の全体構成]

図1は、実施の形態1に係る車載ネットワークシステム10の全体構成を示す図である。車載ネットワークシステム10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一例であり、制御装置、センサ等の各種機器が搭載された自動車におけるネットワーク通信システムである。車載ネットワークシステム10は、各種機器に接続されたECU100a、100b、及び、各ECUをつなぐバス200を含んで構成される。なお、図1では省略しているものの、車載ネットワークシステム10にはECU100a、100b以外にもいくつものECUが含まれ得るが、ここでは、便宜上ECU100a、100bに注目して説明を行う。ECUは、例えば、プロセッサ（マイクロプロセッサ）、メモリ等のデジタル回路、アナログ回路、通信回路等を含む装置である。メモリは、ROM、RAM等であり、プロセッサにより実行される制御プログラム（コンピュータプログラム）を記憶することができる。例えばプロセッサが、制御プログラム（コンピュータプログラム）に従って動作することにより、ECUは各種機能を実現することになる。なお、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、プロセッサに対する指令を示す命令コードが複数個組み合わされて構成されたものである。以下、バス200には不正なデータフレームを送信する不正なECUが接続されている可能性があることを前提として説明する。

【0036】

ECU100aは、1つ以上のセンサを含む機器の一例としてのパワーウィンドウスイッチ110に接続されている。ECU100aは、パワーウィンドウスイッチ110の状態を示す情報を含むデータフレームを周期的にバス200に送信する。さらにパワーウィンドウスイッチ110の状態が変化した時にもパワーウィンドウスイッチ110の状態を示す情報（つまりセンサ値を示す情報）を含むデータフレームをバス200に送信する。従って、ECU100aは、一定の送信周期でデータフレームの送信を繰り返す他に、パワーウィンドウスイッチ110の状態の変化時がその送信周期と一致しないときに非周期的なイベントドリブンデータフレームをバス200に送信することになる。またECU100aは、ECU100bからバス200上に送信されてバス200に流れるデータフレームを受信し、例えばECU100aが送信したデータフレームが正しく受信されていること等を確認する。

【0037】

ECU100bは、パワーウィンドウ120に接続されており、ECU100aから送信されバス200に流れているデータフレームを受信し、そのデータフレームに含まれるパワーウィンドウスイッチ110の状態に応じて、パワーウィンドウ120の開閉の制御を行う。またパワーウィンドウ120の開閉の制御状態に応じたデータフレームを周期的にバス200に送信する。この車載ネットワークシステム10においてはCANプロトコルに従って各ECUがフレームの授受を行う。各ECUは、受信したデータフレームが不正なデータフレームであるか否かを判断する機能を有している。

【0038】

[1. 2 データフレームフォーマット]

以下、CANプロトコルに従ったネットワークで用いられるフレームの1つであるデータフレームについて説明する。

【0039】

図2は、CANプロトコルで規定されるデータフレームのフォーマットを示す図である。同図には、CANプロトコルで規定される標準IDフォーマットにおけるデータフレームを示している。データフレームは、SOF（Start Of Frame）、IDフィールド、RTR（Remote Transmission Request）、IDE（Identifier Extension）、予約ビット「r」、DLC（Data Length Code）、データフィールド、CRC（Cyclic Redundancy Check）シーケンス、CRCデリミタ「DEL」、ACK（Acknowledgement）スロット、ACKデリミタ「DEL」、及び、EOF（End Of Frame）の各フィールドで構成される。

【0040】

SOFは、1bitのドミナントで構成される。バスがアイドルの状態はレセシブにな

10

20

30

40

50

っており、SOFによりドミナントへ変更することでフレームの送信開始を通知する。

【0041】

IDフィールドは、11bitで構成される、データの種別を示す値であるID（メッセージID）を格納するフィールドである。複数のノードが同時に送信を開始した場合、このIDフィールドで通信調停を行うために、IDが小さい値を持つフレームが高い優先度となるよう設計されている。

【0042】

RTTは、データフレームとリモートフレームとを識別するための値であり、データフレームにおいてはドミナント1bitで構成される。

【0043】

IDEと「r」とは、両方ドミナント1bitで構成される。

【0044】

DLは、4bitで構成され、データフィールドの長さを示す値である。なお、IDE、「r」及びDLを合わせてコントロールフィールドと称する。

【0045】

データフィールドは、最大64bitで構成される送信するデータの内容を示す値である。8bit毎に長さを調整できる。送られるデータの仕様については、CANプロトコルで規定されておらず、車載ネットワークシステム10において定められる。従って、車種、製造者（製造メーカ）等に依存した仕様となる。

【0046】

CRCシーケンスは、15bitで構成される。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送信値より算出される。

【0047】

CRCデリミタは、1bitのレセシブで構成されるCRCシーケンスの終了を表す区切り記号である。なお、CRCシーケンス及びCRCデリミタを合わせてCRCフィールドと称する。

【0048】

ACKスロットは、1bitで構成される。送信ノードはACKスロットをレセシブにして送信を行う。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ACKスロットをドミナントとして送信する。レセシブよりドミナントが優先されるため、送信後にACKスロットがドミナントであれば、送信ノードは、いずれかの受信ノードが受信に成功していることを確認できる。

【0049】

ACKデリミタは、1bitのレセシブで構成されるACKの終了を表す区切り記号である。

【0050】

EOFは、7bitのレセシブで構成されており、データフレームの終了を示す。

【0051】

[1.3 データフィールドフォーマット]

以下、車載ネットワークシステム10で用いられるデータフレームにおけるデータフィールドについて説明する。

【0052】

図3は、車載ネットワークシステムで用いられるデータフィールドフォーマットの一例を示す図である。同図に示すように、データフィールドの最上位ビット「I」（先頭の1ビット）は、このデータフィールドを含むデータフレームが、イベントドリブンデータフレームであるか否かを識別するための識別フラグ（「イベントドリブン識別フラグ」と称する。）である。イベントドリブン識別フラグIは、周期的に送信されるデータフレームにおいては0がセットされ、イベントドリブンデータフレームにおいては1がセットされる。イベントドリブン識別フラグIに後続するデータ領域には、ECUが機器等から取得したセンサ値を示すデータ（ECU100aが送信するデータフレームにおいては例えば

10

20

30

40

50

パワーウィンドウスイッチ１１０の状態を示す値等）が含まれる。図３の例では最上位ビットをイベントドリブン識別フラグＩとしているが、イベントドリブン識別フラグＩを、データフィールド内における最下位ビット等の任意の箇所に設けても良い。

【００５３】

[１．４ ＥＣＵ１００ａの構成]

図４は、ＥＣＵ１００ａの構成図である。ＥＣＵ１００ａは、データフレーム送受信部１０１と、データフレーム生成部１０２と、データフレーム生成ルール保持部１０３と、不正データフレーム判断部１０４と、受信データフレーム周期保持部１０５と、データフレーム受信履歴保持部１０６と、データフレーム処理部１０７と、タイマ１０８と、センサ値取得部１０９とを含んで構成される。これらの各構成要素は、機能的な構成要素であり、その各機能は、ＥＣＵ１００ａにおける通信回路、メモリに格納された制御プログラムを実行するプロセッサ或いはデジタル回路等により実現される。なお、ＥＣＵ１００ｂもＥＣＵ１００ａと基本的に同様の構成を備える。但し、データフレーム生成ルール保持部１０３及び受信データフレーム周期保持部１０５及びデータフレーム受信履歴保持部１０６の各保持内容はＥＣＵ毎に異なる内容となり得る。また、データフレーム処理部１０７の処理内容は、ＥＣＵ毎に異なる。

【００５４】

データフレーム送受信部１０１は、バス２００に流れるデータフレームを受信し、ＣＡＮプロトコルに従ってデータフレームを解釈する。受信したデータフレームにおけるＩＤフィールドの内容であるＩＤ（メッセージＩＤ）が、自機（ＥＣＵ１００ａ）が受信するように予め定められているメッセージＩＤである場合は、データフレームの内容を不正データフレーム判断部１０４へ通知する。また、データフレーム送受信部１０１は、データフレーム生成部１０２から通知されたデータフレームをＣＡＮプロトコルに従ってバス２００へ送信する。

【００５５】

データフレーム生成部１０２は、データフレーム生成ルール保持部１０３に格納されたデータフレーム生成ルールに従い、データフレームを生成し、データフレーム送受信部１０１に通知する。データフレーム生成部１０２は、タイマ１０８から現在時刻を取得する。更にデータフレーム生成部１０２は、ＥＣＵ１００ａに接続された機器（パワーウィンドウスイッチ１１０）に関するデータ（センサ値）をセンサ値取得部１０９から取得する。ＥＣＵ１００ａからデータフレームを周期的に送信すべく、データフレーム生成部１０２は、現在時刻とデータフレーム生成ルール保持部１０３に格納される送信周期とによって、データフレームを生成するタイミングを決定し、データフレームの生成を周期的に行う。なお、データフレーム生成部１０２によりデータフレームが生成されると、そのデータフレームはデータフレーム送受信部１０１に通知され、データフレーム送受信部１０１はそのデータフレームの送信を行う。更に、データフレーム生成部１０２は、センサ値取得部１０９から取得されるセンサ値に変化があった時が、前述した周期的なタイミングとは異なる時である場合（例えば周期的なタイミングの許容範囲を示すマージンの範囲外である場合）には、イベントドリブンデータフレームの生成を行う。即ち、データフレーム生成部１０２は、送信周期を示すデータフレーム生成ルールに適合しないタイミングでデータフレームの送信をする際においてデータフレーム中にイベントドリブン識別フラグという特定識別子を付与したデータフレームを生成する、言わば付与部として働く。センサ値取得部１０９はセンサ（パワーウィンドウスイッチ１１０）からセンサ値に変更があった場合及び変更がない場合に随時センサ値を取得する方式で動作しても、センサ値に変更があった場合にのみセンサから供給されるセンサ値を取得する方式で動作しても良い。データフレーム生成部１０２は、センサ値取得部１０９が最後にセンサから取得したセンサ値をデータフィールドに格納したデータフレームを周期的に生成する他、前回のセンサ値から変化があったセンサ値を含むイベントドリブンデータフレームを生成することになる。なお、周期的にデータフレームを生成するタイミングにおいては、前回のセンサ値から変化がなく同じセンサ値を含むデータフレームを生成する可能性と、前回のセンサ値から

変化があったセンサ値を含むデータフレームを生成する可能性とがある。また、その周期的なタイミングではないタイミングで生成されるイベントドリブンデータフレームは、前回のセンサ値から変化があったセンサ値を含むデータフレームである。従って、データフレーム送受信部101によりECU100aからバス200に、周期的にデータフレームが送信され、更に、非周期的にイベントドリブンデータフレームが送信される。即ち、データフレーム送受信部101は、バス200上で送信されたデータフレームを受信する受信部としての機能の他に、特定識別子を含み送信周期を示すデータフレーム生成ルールに適合しないデータフレームであるイベントドリブンデータフレームをバス200により他のECUに送信する、言わば送信部としての機能等を含む。

【0056】

データフレーム生成ルール保持部103は、メモリ等の記憶媒体で実現され、データフレーム生成ルールとして、自機（ECU100a）が送信するメッセージID毎に周期的にデータフレームを送信するための送信周期を格納している。図5は、データフレーム生成ルール保持部103に格納されたデータフレーム生成ルールの一例を示す図である。ここでは、ECU100aは、パワーウィンドウスイッチ110の状態を示すデータフレーム等、複数種類のデータフレーム（種類毎にメッセージIDで識別されるデータフレーム）を送信するものとする。図5の例は、ECU100aから周期的に送信されるメッセージIDが0x100のデータフレームの送信周期は、50msであり、メッセージIDが0x200のデータフレームの送信周期は、100msであり、メッセージIDが0x300のデータフレームの送信周期は、300msであることを示している。

【0057】

不正データフレーム判断部104は、受信したデータフレームが正当なデータフレームであるか（不正なデータフレームでないか）否かについて判断する。即ち、不正データフレーム判断部104は、データフレーム送受信部101から通知されたデータフレームについて、受信データフレーム周期保持部105の周期ルール情報（後述）を参照して、メッセージID毎に予め定められた送信周期の条件を満たすか否かを確認し、送信周期の条件を満たす場合には正規のECUから送信されたデータフレーム（正当なデータフレーム）であると判断する。また、送信周期の条件を満たさないデータフレームであっても、イベントドリブンデータフレームであるか否かを識別するためのイベントドリブン識別フラグを確認し、イベントドリブンデータフレームであると識別された場合には正規ECUから送信されたデータフレーム（正当なデータフレーム）であると判断する。即ち、不正データフレーム判断部104は、送信周期を示すデータフレーム生成ルールに呼応した周期ルール情報（後述）に適合しないデータフレームがデータフレーム送受信部101により受信された場合に、そのデータフレーム中のイベントドリブン識別フラグという特定識別子を検証する、言わば検証部としての機能を有する。不正データフレーム判断部104は、受信したデータフレームが予め定められた送信周期の条件を満たさず、かつ、イベントドリブン識別フラグによってイベントドリブンデータフレームであると確認されない場合（つまり特定識別子の検証に失敗した場合）には、受信したデータフレームを不正なデータフレームであると判断する。不正データフレーム判断部104は、正当なデータフレームであると判断した場合には、データフレーム処理部107にそのデータフレームの処理を行わせ、不正なデータフレームであると判断した場合には、そのデータフレームを破棄する（つまりそのデータフレームについてデータフレーム処理部107に処理させない）。また、不正データフレーム判断部104は、送信周期の条件を満たすデータフレームを受信した場合に、受信時刻をデータフレーム受信履歴保持部106に前回受信時刻（後述）として記録する。

【0058】

受信データフレーム周期保持部105は、メモリ等の記憶媒体で実現され、周期ルール情報を保持する。この周期ルール情報は、自機（ECU100a）が受信するデータフレームのメッセージID毎に、予め定められた送信周期と、データフレームの受信間隔について、送信周期の条件が満たされる（つまり正当な送信周期に合致する）と判断されるた

10

20

30

40

50

めの許容範囲を示すマージンとを対応付けた情報である。データフレームの受信側の ECU の受信データフレーム周期保持部 105 に保持される周期ルール情報における送信周期は、そのデータフレームの送信側の ECU のデータフレーム生成ルール保持部 103 に保持されるデータフレーム生成ルールにおける送信周期に呼応する。図 6 は、ECU 100a から送信されたデータフレームを受信する ECU 100b における受信データフレーム周期保持部 105 に格納された周期ルール情報の一例を示す図である。同図の例では、メッセージ ID が 0x100 のデータフレームの送信周期が 50ms、メッセージ ID が 0x200 のデータフレームの送信周期が 100ms、メッセージ ID が 0x300 のデータフレームの送信周期が 70ms であることを示している。同図の例では、マージンは、どのメッセージ ID についても 1ms である。このマージンが 1ms であるため、メッセージ ID が 0x100 のデータフレームについて送信周期が 49ms 以上 51ms 以下の範囲であれば、ECU 100b における不正データフレーム判断部 104 は、送信周期の条件が満たされると判断することになる。

10

【0059】

データフレーム受信履歴保持部 106 は、メモリ等の記憶媒体で実現され、自機 (ECU 100a) が正常に受信 (つまり正当なデータフレームとして受信) した周期的なデータフレームについてメッセージ ID 毎に、周期的に受信した最終時刻である前回受信時刻を対応付けてなるリストを保持している。図 7 は、正当なデータフレームとして受信した周期的なデータフレームのメッセージ ID 毎に、データフレームの前回受信時刻を示す情報を列挙したリストの一例を示している。同図の例は、ECU 100b におけるデータフレーム受信履歴保持部 106 が保持するリストの例である。この例では、メッセージ ID が 0x100 であるデータフレームを周期的に受信した最終時刻 (前回受信時刻) は 200ms、メッセージ ID が 0x200 であるデータフレームを周期的に受信した前回受信時刻は 220ms、メッセージ ID が 0x300 であるデータフレームを周期的に受信した前回受信時刻は 230ms であることを示している。

20

【0060】

データフレーム処理部 107 は、不正データフレーム判断部 104 により正当なデータフレームであると判断されたデータフレームについて、そのデータフレームに応じて ECU 毎に予め定められた処理を行う。例えば、パワーウィンドウスイッチ 110 の状態を示すデータフレームを送信した ECU 100a では、ECU 100b からパワーウィンドウ 120 の開閉の制御状態に応じたデータフレームを受信して、パワーウィンドウ 120 が適切に反応しているかを確認する処理、適切に反応していない場合にアラーム音を鳴らす処理或いは他の ECU に異常を通知する処理等を行う。

30

【0061】

タイマ 108 は、計時機構であり、例えば車両のエンジン始動時或いはバッテリーからの電力供給開始時等において 0 にリセットされ、その時点から経過した時刻を、データフレーム生成部 102 及び不正データフレーム判断部 104 に通知する。タイマ 108 により、データフレーム生成部 102 は、データフレームを一定の送信周期で周期的に送信でき、不正データフレーム判断部 104 は、受信したデータフレームの受信周期が予め定められた送信周期の条件を満たすか否かを判断することができるようになる。

40

【0062】

センサ値取得部 109 は、自機 (ECU 100a) が接続している機器 (パワーウィンドウスイッチ 110) の状態を示すセンサ値を取得し、データフレーム生成部 102 に周期的に通知し、更にセンサの値が変化した時にもセンサ値をデータフレーム生成部 102 に通知する。

【0063】

[1.5 データフレームの送受信]

以下、図 8 ~ 図 10 を用いて、バス 200 を介した ECU 間でのデータフレームの送受信について説明する。

【0064】

50

図8は、ECU100aをデータフレームの送信側とし、ECU100bをデータフレームの受信側としたときのデータフレームの送受信の流れを示す図である。

【0065】

図8に示す期間Tは、周期的に送信されるデータフレームの送信周期である。この期間Tは、送信側であるECU100aのデータフレーム生成ルール保持部103が保持するデータフレーム生成ルールにおける送信周期である。また、期間Tは、受信側であるECU100bの受信データフレーム周期保持部105が保持する周期ルール情報における送信周期と一致すると想定される。ECU100aは、周期的にデータフレームを送信する。ECU100aは、その周期的な送信に加えて、接続されたパワーウィンドウスイッチ110の状態の変化のタイミングがその周期的な送信タイミングと一致しない場合に、その状態の変化のタイミングで、イベントドリブンデータフレームを送信する。

10

【0066】

車載ネットワークシステム10においては、不正なECUがバス200に接続された不正なデータフレームを送信した場合に、ECU100aが送信した正当なデータフレームと区別できる。即ち、ECU100bにより不正なデータフレームと正当なデータフレームとは判別される。この判別には、上述した周期的に送信されるデータフレームについて周期ルール情報（送信周期に係る条件）が用いられ、また、その送信周期に係る条件を満たさないイベントドリブンデータフレームについてはデータフィールド中のイベントドリブン識別フラグという特定識別子が用いられる。

【0067】

20

図9は、ECU100aにおけるデータフレームの送信処理を示すフローチャートである。

【0068】

ECU100aは、データフレーム生成ルールにおける送信周期に従った送信タイミング（前回の送信から送信周期が経過したタイミング）、或いは、センサ値取得部109からのセンサ値が変化したタイミングで、データフレームの生成が必要となり、図9の送信処理を開始する。送信処理においては、まず、ECU100aは、送信するデータフレームがイベントドリブンデータフレームか周期的なデータフレームかを判断する（ステップS1101）。

【0069】

30

ECU100aは、ステップS1101において、送信するデータフレームが、データフレーム生成ルールにおける送信周期に従っていないイベントドリブンデータフレームであると判断した場合は、生成するデータフレームのデータフィールドのイベントドリブン識別フラグI（図3参照）に、イベントドリブンデータフレームであることを示す1をセットする（ステップS1102）。

【0070】

ECU100aは、ステップS1101において、送信するデータフレームが、データフレーム生成ルールにおける送信周期に従う周期的なデータフレームであると判断した場合（イベントドリブンデータフレームでないと判断した場合は、生成するデータフレームのデータフィールドのイベントドリブン識別フラグI（図3参照）に、イベントドリブンデータフレームでないことを示す0をセットする（ステップS1103）。

40

【0071】

ECU100aは、ステップS1102又はS1103での処理を終えると、データフィールドのデータ領域にはセンサ値取得部109から取得した最新のセンサ値をセットして、送信するデータフレームを生成し、バス200へと送信する（ステップS1104）。これにより、バス200上にデータフレームが流れ、ECU100bに受信されるようになる。

【0072】

図10は、ECU100bにおけるデータフレームの受信処理を示すフローチャートである。

50

【0073】

ECU100bは、バス200上に現れるデータフレームを受信する（ステップS1201）。なお、ECU100bは、自機が受信すべきメッセージIDを含まないデータフレームであればそのデータフレームを破棄して処理を終了する。自機が受信すべきメッセージIDを含むデータフレームを受信した場合に、ECU100bは、その受信が、保持している周期ルール情報で規定された送信周期範囲内か否かを判断する（ステップS1202）。なお、ECU100bの不正データフレーム判断部104は、受信したデータフレームの受信間隔（つまり送信周期）が規定の送信周期の範囲内であるか否か（つまり周期ルール情報で定められた送信周期の条件を満たすか否か）を、タイマ108、受信データフレーム周期保持部105及びデータフレーム受信履歴保持部106から得られる情報に基づいて判断する。なお、規定の送信周期の範囲内とは、前回受信時刻と今回受信したデータフレームの受信時刻の差分（受信間隔）が、受信したデータフレームのメッセージIDに対応して定められた送信周期からマージンを引いた値以上であり、かつ、その送信周期にマージンを加えた値以下である場合を意味する。

10

【0074】

ステップS1202において、データフレームの受信間隔が送信周期の範囲内である場合には、送信周期の条件が満たされたことになり、ECU100bは、データフレーム受信履歴保持部106が保持するリストに、受信したデータフレームのメッセージIDに対応付けて、前回受信時刻として、そのデータフレームの受信時刻を記録（つまり前回受信時刻を更新）する（ステップS1204）。そして、ステップS1204での処理に続いて、ECU100bの不正データフレーム判断部104により、受信したデータフレームが正当なデータフレームであると判断され（ステップS1205）、データフレーム処理部107によりそのデータフレームに対応した処理がなされる。

20

【0075】

また、ステップS1202において、データフレームの前回受信時刻と今回受信時刻の差分が送信周期の範囲内でない場合には、ECU100bは、データフレームのデータフィールドのイベントドリブン識別フラグIが1であるか否かを判別する（ステップS1203）。イベントドリブン識別フラグIが1である場合には、ECU100bの不正データフレーム判断部104は、受信したデータフレームが正当なデータフレームであると判断し（ステップS1205）、データフレーム処理部107によりそのデータフレームに対応した処理がなされる。

30

【0076】

また、ステップS1203において、データフレームのデータフィールドのイベントドリブン識別フラグIが1でないと判別した場合には、ECU100bは、受信したデータフレームが不正なデータフレームであると判断してデータフレームを破棄する（ステップS1206）。従って、ECU100bは、不正なECUにより送信された不正なデータフレームを処理しない。

【0077】

なお、ステップS1202において、データフレームの受信間隔（つまり送信周期）が規定の送信周期の範囲内か否かを判断するに際して、初回等といった前回受信時刻が保存されていない場合においては、受信したデータフレームをイベントドリブンデータフレームと扱い、イベントドリブン識別フラグIが正しいときにそのデータフレームの受信時刻を前回受信時刻として記録してからステップS1205の処理を行うことができる。この場合、送信側のECUでは初回等の周期的な送信の起点においてはイベントドリブンデータフレームを送信する。また、各ECUが例えばスリープ状態等に入ってデータフレームの周期的な送信を休止する期間がある場合には、その後の周期的な送信の再開時にデータフレームをイベントドリブンデータフレームとして送信することとしても良い。この場合には、受信側のECUでは前回受信時刻から一定時間以上の間、送信側のECUがスリープ状態に入って周期的な送信が途切れた場合に、前回受信時刻を無効にして次回を初回と扱い、受信したデータフレームをイベントドリブンデータフレームと扱い、その正当性を

40

50

判断することができる。

【0078】

ここでは、ECU100aがデータフレームを送信してECU100bがデータフレームを受信する例を示したが、ECU100bがデータフレームを送信してECU100aがデータフレームを受信する場合においても同様の処理がなされる。即ち、ECU100bも図9に示すものと同様の送信処理を実行し得るし、ECU100aも図10に示すものと同様の受信処理を実行し得る。

【0079】

[1.6 実施の形態1の効果]

実施の形態1では、周期的に送信されるデータフレームに加えて、非周期的に送信されるイベントドリブンデータフレームが存在する場合でも、イベントドリブンデータフレーム内に特定識別子を含めることによって、正当なデータフレームか否かを区別可能にする車載ネットワークシステム10を示した。即ち、車載ネットワークシステム10では、送信周期の条件により正当なデータフレームであるか否かを判別し、送信周期の条件によっては判別ができない場合に限って特定識別子により正当なデータフレームであるか否かを判別するようにしている。不正なECUがデータフレームを送信する場合には、送信周期の条件を満たさない可能性が高く、特に特定識別子を付与しないため、このデータフレームを受信したECUによって不正なデータフレームであると判断されるようになる。なお、イベントドリブンデータフレームではないデータフレーム（つまり周期的に送信されるデータフレーム）においては、データフィールドにイベントドリブン識別フラグIを含めずにデータフィールドに、ECUが機器等から取得したセンサ値を示すデータだけを含ませることとしても良い。このようにすれば、正規のECUが周期的に送信するデータフレームには、特定識別子を設ける必要がないため例えばデータフィールドを最大限に有効活用できる。

【0080】

(実施の形態2)

以下、本開示の別の実施の形態として、データフレームを送受信するECU2100aとECU2100bとの間で、周期的に送信されるデータフレームに加えて非周期的なイベントドリブンデータフレームが送信され得る前提の下で、不正なデータフレームが送信されたことを適切に検知するための不正検知方法を実現する車載ネットワークシステム11について図面を用いて説明する。

【0081】

[2.1 車載ネットワークシステム11の全体構成]

図11は、実施の形態2に係る車載ネットワークシステム11の全体構成を示す図である。車載ネットワークシステム11は、実施の形態1で示した車載ネットワークシステム10の一部を変形したものであり、制御装置、センサ等の各種機器が搭載された自動車におけるネットワーク通信システムである。車載ネットワークシステム11は、各種機器に接続されたECU2100a、2100b、及び、各ECUをつなぐバス200を含んで構成される。車載ネットワークシステム11の構成要素のうち、実施の形態1で示した車載ネットワークシステム10と同様の機能を有する構成要素は、同じ符号を付して説明を省略する。ECUは、例えば、プロセッサ（マイクロプロセッサ）、メモリ等のデジタル回路、アナログ回路、通信回路等を含む装置である。以下、バス200には不正なデータフレームを送信する不正なECUが接続されている可能性があることを前提として説明する。

【0082】

ECU2100aは、実施の形態1で示したECU100aの一部を変形したものであり、パワーウィンドウスイッチ110に接続されている。ECU2100aは、パワーウィンドウスイッチ110の状態を示す情報を含むデータフレームを周期的にバス200に送信する。さらにパワーウィンドウスイッチ110の状態が変化した時にもパワーウィンドウスイッチ110の状態を示す情報（つまりセンサ値を示す情報）を含むデータフレー

ムをバス200に送信する。従って、ECU2100aは、一定の送信周期でデータフレームの送信を繰り返す他に、パワーウィンドウスイッチ110の状態の変化時がその送信周期と一致しないときに非周期的なイベントドリブンデータフレームをバス200に送信することになる。またECU2100aは、ECU2100bからバス200上に送信されてバス200に流れるデータフレームを受信し、例えばECU2100aが送信したデータフレームが正しく受信されていること等を確認する。

【0083】

ECU2100bは、実施の形態1で示したECU100bの一部を変形したものであり、パワーウィンドウ120に接続されている。ECU2100bは、ECU2100aから送信されバス200に流れているデータフレームを受信し、そのデータフレームに含まれるパワーウィンドウスイッチ110の状態に応じて、パワーウィンドウ120の開閉の制御を行う。またパワーウィンドウ120の開閉の制御状態に応じたデータフレームを周期的にバス200に送信する。この車載ネットワークシステム11においてはCANプロトコルに従って各ECUがフレームの授受を行う。各ECUは、受信したデータフレームが不正なデータフレームであるか否かを判断する機能を有している。

【0084】

[2.2 データフィールドフォーマット]

以下、車載ネットワークシステム11で用いられるデータフレームにおけるデータフィールドについて説明する。

【0085】

図12は、車載ネットワークシステム11で用いられるデータフィールドフォーマットの一例を示す図である。同図に示すように、データフィールドの上位8ビット「I」（先頭の8ビット）は、イベントドリブンデータフレームを送信する度に増加するカウンタ（「イベントカウンタ」と称する。）である。イベントカウンタIの値は、周期的なデータフレームの送信時には変化せず、同じメッセージIDのイベントドリブンデータフレームを1回送信する度に値が1増加（インクリメント）する。なお、例外的にイベントカウンタIの値が最大値（8ビットの最大値）になっている場合にイベントカウンタを1増加すると最小値になる。イベントカウンタIは、データフレームの受信側において正当なイベントドリブンデータフレームであるか否かを識別するための特定識別子として働く。イベントカウンタIに後続するデータ領域にはECUが機器等から取得したセンサ値を示すデータ（ECU2100aが送信するデータフレームにおいては例えばパワーウィンドウスイッチ110の状態を示す値等）が含まれる。図12の例では上位8ビットをイベントカウンタIとしているが、イベントカウンタIを、データフィールド内における下位8ビット等の任意の箇所に設けても良い。また、イベントカウンタIの長さを8ビットとしているが、必ずしも8ビットである必要はなく、任意の長さにしても良い。

【0086】

[2.3 ECU2100aの構成]

図13は、ECU2100aの構成図である。ECU2100aは、データフレーム送受信部101と、データフレーム生成部2102と、データフレーム生成ルール保持部2103と、不正データフレーム判断部2104と、受信データフレーム周期保持部105と、データフレーム受信履歴保持部2106と、データフレーム処理部107と、タイマ108と、センサ値取得部109とを含んで構成される。ECU2100aの構成要素のうち、実施の形態1で示したECU100aと同様の機能を有する構成要素は、同じ符号を付して説明を省略する。これらの各構成要素は、機能的な構成要素であり、その各機能は、ECU2100aにおける通信回路、メモリに格納された制御プログラムを実行するプロセッサ或いはデジタル回路等により実現される。なお、ECU2100bもECU2100aと基本的に同様の構成を備える。但し、データフレーム生成ルール保持部2103、受信データフレーム周期保持部105及びデータフレーム受信履歴保持部2106の各保持内容はECU毎に異なる内容となり得る。また、データフレーム処理部107の処理内容は、ECU毎に異なる。

【0087】

データフレーム生成部2102は、データフレーム生成ルール保持部2103に格納されたデータフレーム生成ルールに従い、データフレームを生成し、データフレーム送受信部101に送信する。データフレーム生成部2102は、タイマ108から現在時刻を取得する。更にデータフレーム生成部2102は、ECU2100aに接続された機器（パワーウィンドウスイッチ110）に関するデータ（センサ値）をセンサ値取得部109から取得する。ECU2100aからデータフレームを周期的に送信すべく、データフレーム生成部2102は、現在時刻とデータフレーム生成ルール保持部2103に格納される送信周期とによって、データフレームを生成するタイミングを決定し、データフレームの生成を周期的に行う。なお、データフレーム生成部2102によりデータフレームが生成されると、そのデータフレームはデータフレーム送受信部101に通知され、データフレーム送受信部101はそのデータフレームの送信を行う。更に、データフレーム生成部2102は、センサ値取得部109から取得されるセンサ値に変化があった時が、周期的なタイミングとは異なる時である場合には、イベントドリブンデータフレームの生成を行う。従って、データフレーム送受信部101によりECU2100aからバス200に、周期的にデータフレームが送信され、更に、非周期的にイベントドリブンデータフレームが送信される。データフレーム生成部2102は、周期的に送信するデータフレーム及びイベントドリブンデータフレームのデータフィールドに、イベントカウンタIとして、データフレーム生成ルール保持部2103に格納されている、メッセージID毎の送信イベントカウンタの値を含ませる。なお、データフレーム生成部2102は、イベントドリブンデータフレームを生成する場合には、データフレームの生成前にデータフレーム生成ルール保持部2103に格納されている送信イベントカウンタの値を1増加（インクリメント）する。データフレーム生成部2102も実施の形態1で示したデータフレーム生成部102と同様に、送信周期を示すデータフレーム生成ルールに適合しないタイミングでデータフレームの送信をする際においてデータフレーム中にイベントカウンタという特定識別子を付与したデータフレームを生成する付与部としての機能を有する。

【0088】

データフレーム生成ルール保持部2103は、メモリ等の記憶媒体で実現され、データフレーム生成ルールとしてECU2100aが送信するメッセージID毎に周期的にデータフレームを送信するための送信周期を格納しており、更に、データフレーム生成ルールに、送信したイベントドリブンデータフレームの回数を示す送信イベントカウンタを付与している。この送信イベントカウンタは、データフレームを送信する際に、データフィールドのイベントカウンタに設定する値として用いられる。データフレーム生成部2102がイベントドリブンデータフレームの送信時に、送信イベントカウンタを1増加し、その送信イベントカウンタの値をデータフィールド内のイベントカウンタIとして用いる。図14は、データフレーム生成ルール保持部2103に格納されたデータフレーム生成ルール及び送信イベントカウンタの一例を示す図である。ここでは、ECU2100aは、パワーウィンドウスイッチ110の状態を示すデータフレーム等、複数種類のデータフレーム（種類毎にメッセージIDで識別されるデータフレーム）を送信するものとする。図14の例では、ECU2100aから周期的に送信されるメッセージIDが0x100のデータフレームについては、送信周期が50msであり送信イベントカウンタが現在15（例えばイベントドリブンデータフレームを15回送信した状態を示す値）であり、メッセージIDが0x200のデータフレームについては、送信周期が100msであり送信イベントカウンタが現在0（例えば未だイベントドリブンデータフレームを送信していない状態を示す値）であり、メッセージIDが0x300のデータフレームについては、送信周期が300msであり送信イベントカウンタが現在5であることを示している。

【0089】

不正データフレーム判断部2104は、受信したデータフレームが正当なデータフレームであるか（不正なデータフレームでないか）否かについて判断する。即ち、不正データフレーム判断部2104は、受信データフレーム周期保持部105の周期ルール情報を参

照して、メッセージ I D 毎に予め定められた送信周期の条件を満たすか否かを確認し、送信周期の条件を満たす場合には正規の ECU から送信されたデータフレーム（正当なデータフレーム）であると判断する。また、送信周期の条件を満たさないデータフレームであっても、データフレーム受信履歴保持部 2106 に格納されている受信イベントカウンタの値と受信したデータフレームに含まれるイベントカウンタ I の値とを比較して確認し、イベントカウンタ I の値が正当なイベントドリブンデータフレームに期待される値であると判定された場合には、正規 ECU から送信されたイベントドリブンデータフレーム（正当なデータフレーム）であると判断する。即ち、不正データフレーム判断部 2104 は、実施の形態 1 で示した不正データフレーム判断部 104 と同様に、送信周期を示すデータフレーム生成ルールに呼応した周期ルール情報に適合しないデータフレームがデータフレーム送受信部 101 により受信された場合に、そのデータフレーム中のイベントカウンタという特定識別子を検証する検証部としての機能を有する。受信したデータフレームに含まれるイベントカウンタ I の値が、受信イベントカウンタの値を 1 増加させた値と一致する場合には、正当なイベントドリブンデータフレームに期待される値であり、正当なデータフレームであると判断される。不正データフレーム判断部 2104 は、受信したデータフレームが予め定められた送信周期の条件を満たさず、かつ、イベントカウンタ I により正当なイベントドリブンデータフレームであると判定されない場合には、受信したデータフレームを不正なデータフレームであると判断する。不正データフレーム判断部 2104 は、正当なデータフレームであると判断した場合には、データフレーム処理部 107 にそのデータフレームの処理を行わせ、不正なデータフレームであると判断した場合には、そのデータフレームを破棄する（つまりそのデータフレームについてデータフレーム処理部 107 に処理させない）。また、不正データフレーム判断部 2104 は、送信周期の条件を満たすデータフレームを受信した場合に、受信時刻をデータフレーム受信履歴保持部 2106 に前回受信時刻として記録する。

【0090】

データフレーム受信履歴保持部 2106 は、メモリ等の記憶媒体で実現され、自機（ECU 2100a）が正常に受信（つまり正当なデータフレームとして受信）した周期的なデータフレームについてメッセージ I D 毎に、周期的に受信した最終時刻である前回受信時刻を対応付けてなるリストを保持しており、このリストには更に正当に受信したイベントドリブンデータフレームの受信回数である受信イベントカウンタがメッセージ I D 毎に付与されている。図 15 は、正当なデータフレームとして受信した周期的なデータフレームのメッセージ I D 毎に、データフレームの前回受信時刻及び受信イベントカウンタを列挙したリストの一例を示している。同図の例は、ECU 2100b におけるデータフレーム受信履歴保持部 2106 が保持するリストの例である。この例では、メッセージ I D が 0x100 であるデータフレームを周期的に受信した最終時刻（前回受信時刻）は 200ms でありメッセージ I D が 0x100 のイベントドリブンデータフレームに対応する受信イベントカウンタが現在 15（例えばイベントドリブンデータフレームを 15 回受信した状態を示す値）であり、メッセージ I D が 0x200 であるデータフレームを周期的に受信した前回受信時刻は 220ms であり受信イベントカウンタが現在 0（例えば未だイベントドリブンデータフレームを受信していない状態を示す値）であり、メッセージ I D が 0x300 であるデータフレームを周期的に受信した前回受信時刻は 230ms であり受信イベントカウンタが現在 5であることを示している。

【0091】

〔2.4 ECU 2100a におけるデータフレームの送信処理〕

以下、ECU 2100a がデータフレームをバス 200 に送信し、ECU 2100b がデータフレームをバス 200 から受信する例を想定して、ECU 2100a におけるデータフレームの送信処理を説明する。

【0092】

図 16 は、ECU 2100a におけるデータフレームの送信処理を示すフローチャートである。

【0093】

ECU2100aは、データフレーム生成ルールにおける送信周期に従った送信タイミング（前回の送信から送信周期が経過したタイミング）、或いは、センサ値取得部109からのセンサ値が変化したタイミングで、データフレームの生成が必要となり、図16の送信処理を開始する。送信処理においては、まず、ECU2100aは、送信するデータフレームがイベントドリブンデータフレームか周期的なデータフレームかを判断する（ステップS2101）。

【0094】

ECU2100aは、ステップS2101において、送信するデータフレームが、データフレーム生成ルールにおける送信周期に従っていないイベントドリブンデータフレームであると判断した場合は、データフレーム生成ルール保持部2103に格納されている送信イベントカウンタの値を1増加（インクリメント）する（ステップS2102）。また、ECU2100aは、ステップS2101において、送信するデータフレームが、データフレーム生成ルールにおける送信周期に従う周期的なデータフレームであると判断した場合（イベントドリブンデータフレームでないと判断した場合）には、ステップS2102での送信イベントカウンタの値の増加をスキップする。

【0095】

ECU2100aは、ステップS2102での処理を終えた場合、及び、ステップS2102での処理をスキップした場合に、データフィールドのイベントカウンタIに送信イベントカウンタの値をセットし、データフィールドのデータ領域にはセンサ値取得部109から取得した最新のセンサ値をセットして、送信するデータフレームを生成し、バス200へと送信する（ステップS2103）。これにより、バス200上にデータフレームが流れ、ECU2100bに受信されるようになる。

【0096】

なお、ECU2100bも図16に示すものと同様の送信処理を実行し得る。

【0097】

[2.5 ECU2100bにおけるデータフレームの受信処理]

以下、ECU2100aがデータフレームをバス200に送信し、ECU2100bがデータフレームをバス200から受信する例を想定して、ECU2100bにおけるデータフレームの受信処理を説明する。

【0098】

図17は、ECU2100bにおけるデータフレームの受信処理を示すフローチャートである。

【0099】

ECU2100bは、バス200上に現れるデータフレームを受信する（ステップS2201）。なお、ECU2100bは、自機が受信すべきメッセージIDを含まないデータフレームであればそのデータフレームを破棄して処理を終了する。自機が受信すべきメッセージIDを含むデータフレームを受信した場合に、ECU2100bは、その受信が、保持している周期ルール情報で規定された送信周期範囲内か否かを判断する（ステップS2202）。なお、ECU2100bの不正データフレーム判断部2104は、受信したデータフレームの受信間隔（つまり送信周期）が規定の送信周期の範囲内であるか否か（つまり周期ルール情報で定められた送信周期の条件を満たすか否か）を、タイマ108、受信データフレーム周期保持部105及びデータフレーム受信履歴保持部106から得られる情報に基づいて判断する。即ち、不正データフレーム判断部2104は、前回受信時刻と今回受信したデータフレームの受信時刻の差分（受信間隔）が、受信したデータフレームのメッセージIDに対応して定められた送信周期からマージンを引いた値以上であり、かつ、その送信周期にマージンを加えた値以下であるか否かを判断する。

【0100】

ステップS2202において、データフレームの受信間隔が送信周期の範囲内である場合には、送信周期の条件が満たされたことになり、ECU2100bは、データフレーム

10

20

30

40

50

受信履歴保持部2106が保持するリストに、受信したデータフレームのメッセージIDに対応付けて、前回受信時刻として、そのデータフレームの受信時刻を記録（つまり前回受信時刻を更新）する（ステップS2204）。そして、ステップS2204での処理に続いて、ECU2100bの不正データフレーム判断部2104により、受信したデータフレームが正当なデータフレームであると判断され（ステップS2206）、データフレーム処理部107によりそのデータフレームに対応した処理がなされる。

【0101】

また、ステップS2202において、データフレームの前回受信時刻と今回受信時刻の差分が送信周期の範囲内でない場合には、ECU2100bは、データフレームのデータフィールドのイベントカウンタIが、データフレーム受信履歴保持部2106に格納された受信イベントカウンタの値を1増加させた値と一致するか否かを判定する（ステップS2203）。一致する場合には、ECU2100bでは受信イベントカウンタの値を1増加（インクリメント）させる（ステップS2205）。続いてECU2100bの不正データフレーム判断部2104は、受信したデータフレームが正当なデータフレームであると判断し（ステップS2206）、データフレーム処理部107によりそのデータフレームに対応した処理がなされる。

10

【0102】

ステップS2203において一致しないと判定した場合には、ECU2100bは、受信したデータフレームが不正なデータフレームであると判断してデータフレームを破棄する（ステップS2207）。従って、ECU2100bは、不正なECUにより送信された不正なデータフレームを処理しない。

20

【0103】

なお、ステップS2202において、データフレームの受信間隔（つまり送信周期）が規定の送信周期の範囲内か否かを判断するに際して、初回等といった前回受信時刻が保存されていない場合においては、受信したデータフレームをイベントドリブンデータフレームと扱い、イベントカウンタが正しいときに受信イベントカウンタを1増加した後にそのデータフレームの受信時刻を前回受信時刻として記録してからステップS2206の処理を行うことができる。この場合、送信側のECUでは初回等の周期的な送信の起点においてはイベントドリブンデータフレームを送信する。また、各ECUが例えばスリープ状態等に入ってデータフレームの周期的な送信を休止する期間がある場合には、その後の周期的な送信の再開時にデータフレームをイベントドリブンデータフレームとして送信することとしても良い。この場合には、受信側のECUでは前回受信時刻から一定時間以上の間、送信側のECUがスリープ状態に入ると周期的な送信が途切れた場合に、前回受信時刻を無効にして次回を初回と扱い、受信したデータフレームをイベントドリブンデータフレームと扱い、その正当性を判断することができる。

30

【0104】

また、ECU2100aも図17に示すものと同様の受信処理を実行し得る。

【0105】

〔2.6 実施の形態2の効果〕

実施の形態2では、周期的に送信されるデータフレームに加えて、非周期的に送信されるイベントドリブンデータフレームが存在する場合でも、イベントドリブンデータフレーム内に特定識別子（つまりイベントカウンタ）を含めることによって、正当なデータフレームか否かを区別可能にする車載ネットワークシステム11を示した。即ち、車載ネットワークシステム11では、送信周期の条件により正当なデータフレームであるか否かを判別し、送信周期の条件によっては判別ができない場合に限り特定識別子により正当なデータフレームであるか否かを判別するようにしている。イベントカウンタは、固定値ではないため、不正なECUがイベントカウンタと同じ値をデータフレームに付与し難い。不正なECUがデータフレームを送信する場合には、送信周期の条件を満たさない可能性が高く、正しくイベントカウンタをセットすることは容易ではないため、このデータフレームを受信したECUによって不正なデータフレームであると判断されるようになる。なお

40

50

、イベントドリブンデータフレームではないデータフレーム（つまり周期的に送信されるデータフレーム）においては、データフィールドにイベントカウンタ I を含めずにデータフィールドに、ECU が機器等から取得したセンサ値を示すデータだけを含ませることとしても良い。このようにすれば、正規の ECU が周期的に送信するデータフレームには、特定識別子を設ける必要がないため例えばデータフィールドを最大限に有効活用できる。

【0106】

（実施の形態 3）

以下、本開示の別の実施の形態として、データフレームを送受信する ECU 3100a と ECU 3100b との間に、周期的に送信されるデータフレームに加えて非周期的なイベントドリブンデータフレームが送信され得る前提の下で、不正なデータフレームが送信されたことを適切に検知するための不正検知方法を実現する車載ネットワークシステム 12 について図面を用いて説明する。

【0107】

〔3. 1 車載ネットワークシステム 12 の全体構成〕

図 18 は、実施の形態 3 に係る車載ネットワークシステム 12 の全体構成を示す図である。車載ネットワークシステム 12 は、実施の形態 1 で示した車載ネットワークシステム 10 の一部を変形したものであり、制御装置、センサ等の各種機器が搭載された自動車におけるネットワーク通信システムである。車載ネットワークシステム 12 は、各種機器に接続された ECU 3100a、3100b、及び、各 ECU をつなぐバス 200 を含んで構成される。車載ネットワークシステム 12 の構成要素のうち、実施の形態 1 で示した車載ネットワークシステム 10 と同様の機能を有する構成要素は、同じ符号を付して説明を省略する。ECU は、例えば、プロセッサ（マイクロプロセッサ）、メモリ等のデジタル回路、アナログ回路、通信回路等を含む装置である。以下、バス 200 には不正なデータフレームを送信する不正な ECU が接続されている可能性があることを前提として説明する。

【0108】

ECU 3100a は、実施の形態 1 で示した ECU 100a の一部を変形したものであり、パワーウィンドウスイッチ 110 に接続されている。ECU 3100a は、パワーウィンドウスイッチ 110 の状態を示す情報を含むデータフレームを周期的にバス 200 に送信する。さらにパワーウィンドウスイッチ 110 の状態が変化した時にもパワーウィンドウスイッチ 110 の状態を示す情報（つまりセンサ値を示す情報）を含むデータフレームをバス 200 に送信する。従って、ECU 3100a は、一定の送信周期でデータフレームの送信を繰り返す他に、パワーウィンドウスイッチ 110 の状態の変化時がその送信周期と一致しないときに非周期的なイベントドリブンデータフレームをバス 200 に送信することになる。また ECU 3100a は、ECU 3100b からバス 200 上に送信されてバス 200 に流れるデータフレームを受信し、例えば ECU 3100a が送信したデータフレームが正しく受信されていること等を確認する。

【0109】

ECU 3100b は、実施の形態 1 で示した ECU 100b の一部を変形したものであり、パワーウィンドウ 120 に接続されている。ECU 3100b は、ECU 3100a から送信されバス 200 に流れているデータフレームを受信し、そのデータフレームに含まれるパワーウィンドウスイッチ 110 の状態に応じて、パワーウィンドウ 120 の開閉の制御を行う。またパワーウィンドウ 120 の開閉の制御状態に応じたデータフレームを周期的にバス 200 に送信する。この車載ネットワークシステム 12 においては CAN プロトコルに従って各 ECU がフレームの授受を行う。各 ECU は、受信したデータフレームが不正なデータフレームであるか否かを判断する機能を有している。

【0110】

〔3. 2 データフィールドフォーマット〕

以下、車載ネットワークシステム 12 で用いられるデータフレームにおけるデータフィールドについて説明する。

【0111】

図19は、車載ネットワークシステム12で用いられるデータフィールドフォーマットの一例を示す図である。同図の例は、イベントドリブンデータフレームの場合の一例であり、データフィールドの下位16ビット「I」（後尾の16ビット）は、メッセージ認証コード（MAC：Message Authentication Code）を格納するMACフィールドIである。イベントドリブンデータフレームについてのデータフィールドにMACフィールドIを含むか否か、並びに、MACフィールドIを含む場合にはMACフィールドIの位置及び長さについて、データフレーム生成ルール保持部3103に格納されているデータフレーム生成ルール内のイベントドリブンデータフレームフォーマット（後述）で規定される。イベントドリブンデータフレームを生成して送信する場合には、MACフィールドIにデータフレーム生成ルール保持部3103に格納されているイベントドリブンデータフレームフォーマットに従ってMACをセットする。MACは、イベントドリブンデータフレームが正当であることを識別する特定識別子として機能する。周期的なデータフレームを生成して送信する場合には、データフィールド内にMACを格納する必要はなく、MACの代わりに固定値を含めても良いが、特にMAC及びその代替データを含まずデータフィールド全域をデータ領域として活用して良い。ここでは、周期的なデータフレームにはMACは格納されず、イベントドリブンデータフレームにはMACが格納されることとして説明を続ける。データフィールドのMACフィールドI以外の領域であるデータ領域（図19参照）には、ECUが機器等から取得したセンサ値を示すデータ（ECU3100aが送信するデータフレームにおいては例えばパワーウィンドウスイッチ110の状態を示す値等）が含まれる。図19の例では下位16ビットをMACフィールドIとしているが、イベントドリブンデータフレームフォーマットで規定すれば、上位ビット等、任意の箇所にMACフィールドを含めても良い。また、MACのサイズを16ビット以外にしても良い。

【0112】

[3.3 ECU3100aの構成]

図20は、ECU3100aの構成図である。ECU3100aは、データフレーム送受信部101と、データフレーム生成部3102と、データフレーム生成ルール保持部3103と、不正データフレーム判断部3104と、受信データフレーム周期保持部3105と、データフレーム受信履歴保持部106と、データフレーム処理部107と、タイマ108と、センサ値取得部109と、MAC生成部3110と、MAC鍵保持部3111と、カウンタ保持部3112とを含んで構成される。ECU3100aの構成要素のうち、実施の形態1で示したECU100aと同様の機能を有する構成要素は、同じ符号を付して説明を省略する。これらの各構成要素は、機能的な構成要素であり、その各機能は、ECU3100aにおける通信回路、メモリに格納された制御プログラムを実行するプロセッサ或いはデジタル回路等により実現される。なお、ECU3100bもECU3100aと基本的に同様の構成を備える。但し、データフレーム生成ルール保持部3103、受信データフレーム周期保持部3105及びデータフレーム受信履歴保持部106の各保持内容はECU毎に異なる内容となり得る。また、データフレーム処理部107の処理内容は、ECU毎に異なる。

【0113】

データフレーム生成部3102は、データフレーム生成ルール保持部3103に格納されたデータフレーム生成ルールに従い、データフレームを生成し、データフレーム送受信部101に送信する。データフレーム生成部3102は、タイマ108から現在時刻を取得する。更にデータフレーム生成部3102は、ECU3100aに接続された機器（パワーウィンドウスイッチ110）に関するデータ（センサ値）をセンサ値取得部109から取得する。ECU3100aからデータフレームを周期的に送信すべく、データフレーム生成部3102は、現在時刻とデータフレーム生成ルール保持部3103に格納される送信周期とによって、データフレームを生成するタイミングを決定し、データフレームの生成を周期的に行う。なお、データフレーム生成部3102によりデータフレームが生成

されると、そのデータフレームはデータフレーム送受信部101に通知され、データフレーム送受信部101はそのデータフレームの送信を行う。更に、データフレーム生成部3102は、センサ値取得部109から取得されるセンサ値に変化があった時が、周期的なタイミングとは異なる時である場合には、イベントドリブンデータフレームの生成を行う。イベントドリブンデータフレームを生成する際には、データフレーム生成部3102は、データフレーム生成ルール保持部3103に格納されているメッセージID毎のデータフレーム生成ルールのイベントドリブンデータフレームフォーマットに従ってMACをデータフレームに含める。このMACは、MAC生成部3110に、生成するデータフレームのメッセージID及びデータフィールドのデータ領域に格納するデータ（センサ値）を通知することによってMAC生成部3110から得られる値を、イベントドリブンデータフレームフォーマットで規定されるデータ長（ビット長）となるように切り捨てたものである。データフレーム生成部3102によるデータフレームの生成の結果として、データフレーム送受信部101によりECU3100aからバス200に、周期的にデータフレームが送信され、更に、非周期的にイベントドリブンデータフレームが送信される。データフレーム生成部3102も実施の形態1で示したデータフレーム生成部102と同様に、送信周期を示すデータフレーム生成ルールに適合しないタイミングでデータフレームの送信をする際においてデータフレーム中にMACという特定識別子を付与したデータフレームを生成する付与部としての機能を有する。

10

【0114】

データフレーム生成ルール保持部3103は、メモリ等の記憶媒体で実現され、データフレーム生成ルールとしてECU3100aが送信するメッセージID毎に周期的にデータフレームを送信するための送信周期と、MACの格納位置、データ長等を示すイベントドリブンデータフレームフォーマットとを格納している。図21は、データフレーム生成ルール保持部3103に格納されたデータフレーム生成ルールの一例を示している。ここでは、ECU3100aは、パワーウィンドウスイッチ110の状態を示すデータフレーム等、複数種類のデータフレーム（種類毎にメッセージIDで識別されるデータフレーム）を送信するものとする。図21の例では、ECU3100aから周期的に送信されるメッセージIDが0x100のデータフレームについては、送信周期が50msであり、この送信周期に従わずイベントドリブンデータフレームとして送信する場合にはデータフィールドの下位16ビットにMACを格納する必要があることを示している。また、メッセージIDが0x200のデータフレームについては、送信周期が100msであり、メッセージIDが0x200のイベントドリブンデータフレームは送信されないことを示している。また、ECU3100aから周期的に送信されるメッセージIDが0x300のデータフレームについては、送信周期が70msであり、この送信周期に従わずイベントドリブンデータフレームとして送信する場合にはデータフィールドの下位16ビットにMACを格納する必要があることを示している。

20

30

【0115】

不正データフレーム判断部3104は、受信したデータフレームが正当なデータフレームであるか（不正なデータフレームでないか）否かについて判断する。即ち、不正データフレーム判断部3104は、受信データフレーム周期保持部3105の周期ルール情報を参照して、メッセージID毎に予め定められた送信周期の条件を満たすか否かを確認し、送信周期の条件を満たす場合には正規のECUから送信されたデータフレーム（正当なデータフレーム）であると判断する。また、送信周期の条件を満たさないデータフレームであっても、データフィールドに正当なMACが含まれていることが検証された場合には、正当なデータフレームであると判断される。MACの検証は、データフレームのメッセージID及びデータフィールドのデータ領域の内容をMAC生成部3110に通知することによってMAC生成部3110から得られる値と、データフィールド内のMACフィールドIの内容とが、一致するか否かを判別することで行われ、一致した場合に検証に成功する。即ち、不正データフレーム判断部3104は、実施の形態1で示した不正データフレーム判断部104と同様に、送信周期を示すデータフレーム生成ルールに呼応した周期ル

40

50

ール情報に適合しないデータフレームがデータフレーム送受信部101により受信された場合に、そのデータフレーム中のMACという特定識別子を検証する検証部としての機能を有する。不正データフレーム判断部3104は、受信したデータフレームが予め定められた送信周期の条件を満たさず、かつ、MACの検証により正当なイベントドリブンデータフレームであると判定されない場合には、受信したデータフレームを不正なデータフレームであると判断する。不正データフレーム判断部2104は、正当なデータフレームであると判断した場合には、データフレーム処理部107にそのデータフレームの処理を行わせ、不正なデータフレームであると判断した場合には、そのデータフレームを破棄する（つまりそのデータフレームについてデータフレーム処理部107に処理させない）。また、不正データフレーム判断部3104は、送信周期の条件を満たすデータフレームを受信した場合に、受信時刻をデータフレーム受信履歴保持部106に前回受信時刻として記録する。

10

【0116】

受信データフレーム周期保持部3105は、メモリ等の記憶媒体で実現され、周期ルール情報を保持する。この周期ルール情報は、自機（ECU3100a）が受信するデータフレームのメッセージID毎に、予め定められた送信周期と、データフレームの受信間隔について、送信周期の条件が満たされる（つまり正当な送信周期に合致する）と判断されるための許容範囲を示すマージンとを対応付けた情報である。周期ルール情報には、更に、送信周期の条件を満たさないイベントドリブンデータフレームのデータフィールド内に格納されるMACの格納位置、データ長等を示すイベントドリブンデータフレームフォーマットが含まれる。このイベントドリブンデータフレームフォーマットは、不正データフレーム判断部3104が、イベントドリブンデータフレームについての正当性を検証（つまりMACを検証）する際に用いられる。なお、データフレームの受信側のECUの受信データフレーム周期保持部3105に保持される周期ルール情報における送信周期は、そのデータフレームの送信側のECUのデータフレーム生成ルール保持部3103に保持されるデータフレーム生成ルールにおける送信周期に呼応する。また、データフレームの受信側のECUの受信データフレーム周期保持部3105に保持される周期ルール情報におけるイベントドリブンデータフレームフォーマットは、そのデータフレームの送信側のECUのデータフレーム生成ルール保持部3103に保持されるデータフレーム生成ルールにおけるイベントドリブンデータフレームフォーマットに呼応する。図22は、ECU3100aから送信されたデータフレームを受信するECU3100bにおける受信データフレーム周期保持部3105に格納された周期ルール情報の一例を示す図である。同図の例では、メッセージIDが0x100のデータフレームの送信周期が50ms、メッセージIDが0x200のデータフレームの送信周期が100ms、メッセージIDが0x300のデータフレームの送信周期が70msであることを示している。同図の例では、マージンは、どのメッセージIDについても1msである。このマージンが1msであるため、メッセージIDが0x100のデータフレームについて送信周期が49ms以上51ms以下の範囲であれば、ECU3100bにおける不正データフレーム判断部3104は、送信周期の条件が満たされると判断することになる。また、図22の例でのイベントドリブンデータフレームフォーマットについては、メッセージIDが0x100及び0x300のイベントドリブンデータフレームは、データフィールドの下位16ビットにMACが付与されていることを示しており、メッセージIDが0x200のイベントドリブンデータフレームは送信されないことを示している。

20

30

40

【0117】

MAC生成部3110は、不正データフレーム判断部3104或いはデータフレーム生成部3102から通知されたデータフレームの内容（メッセージID及びデータフィールドのデータ領域のデータ）に基づいて、MACを生成してMACの値を通知元に与える。即ち、MAC生成部3110は、通知されたメッセージIDと、データフィールドのデータ領域のデータ値と、カウンタ保持部3112に格納されている、通知されたメッセージIDに対応するカウンタ値とを連結したものに対して、MAC鍵保持部3111に格納さ

50

れている通知されたメッセージIDに対応するMAC鍵を用いてHMAC（非特許文献4）の演算を行うことによりMACを生成して、通知元にMACの値を返す。

【0118】

MAC鍵保持部3111は、メモリ等の記憶媒体で実現され、自機（ECU3100a）が送信するデータフレームのメッセージID毎にMAC生成に用いられる暗号鍵を格納しており、更に、自機（ECU3100a）が受信するデータフレームのメッセージID毎にMAC生成に用いられる暗号鍵を格納している。

【0119】

カウンタ保持部3112は、メモリ等の記憶媒体を含んで実現され、自機（ECU3100a）が送信するデータフレームのメッセージID毎に対応して送信カウンタと、自機（ECU3100a）が受信するデータフレームのメッセージID毎に対応して受信カウンタとを保持する。データフレーム生成部3102からの通知を受けてMAC生成部3110にMACが生成される度に、対応するメッセージIDの送信カウンタが1増加（インクリメント）される。また、不正データフレーム判断部3104が、受信したデータフレームが不正でないと判断し、データフレーム処理部107にそのデータフレームが通知される都度、対応するメッセージIDの受信カウンタが1増加（インクリメント）される。これにより、メッセージID毎のイベントドリブンデータフレームの送信側のECUが保持する送信カウンタと受信側のECUが保持する受信カウンタとが同じ値となるよう同期する。MAC生成部3110は、データフレームの送信のためのMACの生成の際には送信カウンタを用いてMACを生成し、受信したデータフレームの検証のためのMACの生成の際には受信カウンタを用いてMACを生成する。

【0120】

[3.4 ECU3100aにおけるデータフレームの送信処理]

以下、ECU3100aがデータフレームをバス200に送信し、ECU3100bがデータフレームをバス200から受信する例を想定して、ECU3100aにおけるデータフレームの送信処理を説明する。

【0121】

図23は、ECU3100aにおけるデータフレームの送信処理を示すフローチャートである。

【0122】

ECU3100aは、データフレーム生成ルールにおける送信周期に従った送信タイミング（前回の送信から送信周期が経過したタイミング）、或いは、センサ値取得部109からのセンサ値が変化したタイミングで、データフレームの生成が必要となり、図23の送信処理を開始する。送信処理においては、まず、ECU3100aは、送信するデータフレームがイベントドリブンデータフレームか周期的なデータフレームかを判断する（ステップS3101）。

【0123】

ECU3100aは、ステップS3101において、送信するデータフレームが、データフレーム生成ルールにおける送信周期に従っていないイベントドリブンデータフレームであると判断した場合には、イベントドリブンデータフレームフォーマットに従って、生成するデータフレームのデータフィールドのMACフィールドIに、MACを付与する（ステップS3102）。

【0124】

ECU3100aは、ステップS3101において、送信するデータフレームが、データフレーム生成ルールにおける送信周期に従う周期的なデータフレームであると判断した場合（イベントドリブンデータフレームでないと判断した場合）には、ステップS3102での処理をスキップする。

【0125】

ECU3100aは、ステップS3102の後、或いはステップS3102での処理をスキップした後に、データフィールドのデータ領域にセンサ値取得部109から取得した

最新のセンサ値をセットして、送信するデータフレームを生成し、バス200へと送信する（ステップS3103）。これにより、バス200上にデータフレームが流れ、ECU3100bに受信されるようになる。

【0126】

なお、ECU3100bも図23に示すものと同様の送信処理を実行し得る。

【0127】

〔3.5 ECU3100bにおけるデータフレームの受信処理〕

以下、ECU3100aがデータフレームをバス200に送信し、ECU3100bがデータフレームをバス200から受信する例を想定して、ECU3100bにおけるデータフレームの受信処理を説明する。

10

【0128】

図24は、ECU3100bにおけるデータフレームの受信処理を示すフローチャートである。

【0129】

ECU3100bは、バス200上に現れるデータフレームを受信する（ステップS3201）。なお、ECU3100bは、自機が受信すべきメッセージIDを含まないデータフレームであればそのデータフレームを破棄して処理を終了する。自機が受信すべきメッセージIDを含むデータフレームを受信した場合に、ECU3100bは、その受信が、保持している周期ルール情報で規定された送信周期範囲内か否かを判断する（ステップS3202）。なお、ECU3100bの不正データフレーム判断部3104は、受信したデータフレームの受信間隔（つまり送信周期）が規定の送信周期の範囲内であるか否か（つまり周期ルール情報で定められた送信周期の条件を満たすか否か）を、タイマ108、受信データフレーム周期保持部3105及びデータフレーム受信履歴保持部106から得られる情報に基づいて判断する。即ち、不正データフレーム判断部3104は、前回受信時刻と今回受信したデータフレームの受信時刻の差分（受信間隔）が、受信したデータフレームのメッセージIDに対応して定められた送信周期からマージンを引いた値以上であり、かつ、その送信周期にマージンを加えた値以下であるか否かを判断する。

20

【0130】

ステップS3202において、データフレームの受信間隔が送信周期の範囲内である場合には、送信周期の条件が満たされたことになり、ECU3100bは、データフレーム受信履歴保持部106が保持するリストに、受信したデータフレームのメッセージIDに対応付けて、前回受信時刻として、そのデータフレームの受信時刻を記録（つまり前回受信時刻を更新）する（ステップS3204）。そして、ステップS3204での処理に続いて、ECU3100bの不正データフレーム判断部3104により、受信したデータフレームが正当なデータフレームであると判断され（ステップS3205）、データフレーム処理部107によりそのデータフレームに対応した処理がなされる。

30

【0131】

また、ステップS3202において、データフレームの前回受信時刻と今回受信時刻の差分が送信周期の範囲内でない場合には、ECU3100bは、受信データフレーム周期保持部3105に格納されているイベントドリブンデータフレームフォーマットに従ってデータフレームのデータフィールドをMACフィールドIとデータ領域とに分けて、データ領域及びメッセージIDから算出されるMACと、MACフィールドに含まれるMACとを比較することで、データフレームの正当性（MACが正しいこと）を検証する（ステップS3203）。算出されるMACとMACフィールドに含まれるMACとが一致すればMACの検証（つまりMACの正当性の検証）に成功し、受信したデータフレームが正当なデータフレームであると判断され（ステップS3205）、データフレーム処理部107によりそのデータフレームに対応した処理がなされる。

40

【0132】

ステップS3203において、算出されるMACとMACフィールドに含まれるMACとが一致しない場合（MACの検証に成功しない場合）には、ECU3100bは、受信

50

したデータフレームが不正なデータフレームであると判断してデータフレームを破棄する（ステップS 3 2 0 6）。従って、E C U 3 1 0 0 bは、不正なE C Uにより送信された不正なデータフレームを処理しない。

【0 1 3 3】

なお、ステップS 3 2 0 2において、データフレームの受信間隔（つまり送信周期）が規定の送信周期の範囲内か否かを判断するに際して、初回等といった前回受信時刻が保存されていない場合においては、受信したデータフレームをイベントドリブンデータフレームと扱い、M A Cの検証に成功したときにそのデータフレームの受信時刻を前回受信時刻として記録してからステップS 3 2 0 5の処理を行うことができる。この場合、送信側のE C Uでは初回等の周期的な送信の起点においては例外的にイベントドリブンデータフレームを送信する。また、各E C Uが例えばスリープ状態等に入ってデータフレームの周期的な送信を休止する期間がある場合には、その後の周期的な送信の再開時にデータフレームをイベントドリブンデータフレームとして送信することとしても良い。この場合には、受信側のE C Uでは前回受信時刻から一定時間以上の間、送信側のE C Uがスリープ状態に入って周期的な送信が途切れた場合に、前回受信時刻を無効にして次回を初回と扱い、受信したデータフレームをイベントドリブンデータフレームと扱い、その正当性を判断することができる。

10

【0 1 3 4】

また、E C U 3 1 0 0 aも図2 4に示すものと同様の受信処理を実行し得る。

【0 1 3 5】

20

〔3. 6 実施の形態3の効果〕

実施の形態3では、周期的に送信されるデータフレームに加えて、非周期的に送信されるイベントドリブンデータフレームが存在する場合でも、イベントドリブンデータフレーム内に特定識別子としてのM A Cを含めることによって、正当なイベントドリブンデータフレームであることを検証可能にする車載ネットワークシステム1 2を示した。即ち、車載ネットワークシステム1 2では、送信周期の条件により正当なデータフレームであるか否かを判別し、送信周期の条件によっては判別ができない場合に限り特定識別子により正当なデータフレームであるか否かを判別（つまり検証）するようにしている。これにより、送信周期の条件を満たさない正当なイベントドリブンデータフレームが不正なものとして誤検知されることが防止される。また、不正なE C Uがデータフレームを送信する場合には、送信周期の条件を満たさない可能性が高く、正しくM A Cを付与できないため、このデータフレームを受信したE C Uによって不正なデータフレームであると判断されるようになる。なお、イベントドリブンデータフレームではないデータフレーム（つまり周期的に送信されるデータフレーム）においては、データフィールドにM A Cを含める必要がないため、例えばデータフィールドを最大限に有効活用できる。

30

【0 1 3 6】

（実施の形態4）

以下、本開示の別の実施の形態として、データフレームを送受信するE C U 4 1 0 0 aとE C U 4 1 0 0 bとの間で、周期的に送信されるデータフレームに加えて非周期的なイベントドリブンデータフレームが送信され得る前提の下で、車両の状態を踏まえて、不正なデータフレームが送信されたことを適切に検知するための不正検知方法を実現する車載ネットワークシステム1 3について図面を用いて説明する。なお、車載ネットワークシステム1 3は、実施の形態1で示した車載ネットワークシステム1 0及び実施の形態3で示した車載ネットワークシステム1 2の一部を変形したものであり、車載ネットワークシステム1 3で用いられるデータフレームにおけるデータフィールドのフォーマットは、実施の形態3で示したものと同様である。

40

【0 1 3 7】

〔4. 1 車載ネットワークシステム1 3の全体構成〕

図2 5は、実施の形態4に係る車載ネットワークシステム1 3の全体構成を示す図である。車載ネットワークシステム1 3は、制御装置、センサ等の各種機器が搭載された自動

50

車におけるネットワーク通信システムである。車載ネットワークシステム13は、各種機器に接続されたECU4100a~4100c、及び、各ECUをつなぐバス200を含んで構成される。車載ネットワークシステム13の構成要素のうち、前述した車載ネットワークシステム10等と同様の機能を有する構成要素は、同じ符号を付して説明を省略する。ECUは、例えば、プロセッサ（マイクロプロセッサ）、メモリ等のデジタル回路、アナログ回路、通信回路等を含む装置である。以下、バス200には不正なデータフレームを送信する不正なECUが接続されている可能性があることを前提として説明する。

【0138】

ECU4100cは、ギア4130に接続されており、ギア4130の状態に応じて、車両の状態を判定し、バス200に車両の状態を示すデータフレームを送信する。ギア4130から判定される車両の状態は、例えば、走行中、駐車中等の各状態である。

【0139】

ECU4100aは、実施の形態1で示したECU100aの一部を変形したものであり、パワーウィンドウスイッチ110に接続されている。ECU4100aは、パワーウィンドウスイッチ110の状態を示す情報を含むデータフレームを周期的にバス200に送信する。さらにパワーウィンドウスイッチ110の状態が変化した時にもパワーウィンドウスイッチ110の状態を示す情報（つまりセンサ値を示す情報）を含むデータフレームをバス200に送信する。従って、ECU4100aは、一定の送信周期でデータフレームの送信を繰り返す他に、パワーウィンドウスイッチ110の状態の変化時がその送信周期と一致しないときに非周期的なイベントドリブンデータフレームをバス200に送信することになる。またECU4100aは、ECU4100bからバス200上に送信されてバス200に流れるデータフレームを受信し、例えばECU4100aが送信したデータフレームが正しく受信されていること等を確認する。また、ECU4100aは、ECU4100cが送信した車両の状態を示すデータフレームを受信し、車両の状態を把握し得る。

【0140】

ECU4100bは、実施の形態1で示したECU100bの一部を変形したものであり、パワーウィンドウ120に接続されている。ECU4100bは、ECU4100aから送信されバス200に流れているデータフレームを受信し、そのデータフレームに含まれるパワーウィンドウスイッチ110の状態に応じて、パワーウィンドウ120の開閉の制御を行う。またパワーウィンドウ120の開閉の制御状態に応じたデータフレームを周期的にバス200に送信する。また、ECU4100bは、ECU4100cが送信した車両の状態を示すデータフレームを受信し、車両の状態を把握し得る。この車載ネットワークシステム13においてはCANプロトコルに従って各ECUがフレームの授受を行う。各ECUは、受信したデータフレームが不正なデータフレームであるか否かを判断する機能を有している。

【0141】

[4.2 ECU4100aの構成]

図26は、ECU4100aの構成図である。ECU4100aは、データフレーム送受信部101と、データフレーム生成部4102と、データフレーム生成ルール保持部4103と、不正データフレーム判断部4104と、受信データフレーム周期保持部4105と、データフレーム受信履歴保持部106と、データフレーム処理部107と、タイマ108と、センサ値取得部109と、MAC生成部3110と、MAC鍵保持部3111と、カウンタ保持部3112とを含んで構成される。ECU4100aの構成要素のうち、実施の形態1で示したECU100a或いは実施の形態3で示したECU3100aと同様の機能を有する構成要素は、同じ符号を付して説明を省略する。これらの各構成要素は、機能的な構成要素であり、その各機能は、ECU4100aにおける通信回路、メモリに格納された制御プログラムを実行するプロセッサ或いはデジタル回路等により実現される。なお、ECU4100b及びECU4100cもECU4100aと基本的に同様の構成を備える。但し、データフレーム生成ルール保持部4103、受信データフレーム

周期保持部 4 1 0 5 及びデータフレーム受信履歴保持部 1 0 6 の各保持内容は E C U 毎に異なる内容となり得る。また、データフレーム処理部 1 0 7 の処理内容は、E C U 毎に異なる。

【0 1 4 2】

データフレーム生成部 4 1 0 2 は、データフレーム生成ルール保持部 4 1 0 3 に格納されたデータフレーム生成ルールに従い、データフレームを生成し、データフレーム送受信部 1 0 1 に送信する。データフレーム生成部 4 1 0 2 は、タイマ 1 0 8 から現在時刻を取得する。更にデータフレーム生成部 4 1 0 2 は、E C U 4 1 0 0 a に接続された機器（パワーウィンドウスイッチ 1 1 0）に関するデータ（センサ値）をセンサ値取得部 1 0 9 から取得する。E C U 4 1 0 0 a からデータフレームを周期的に送信すべく、データフレーム生成部 4 1 0 2 は、現在時刻とデータフレーム生成ルール保持部 4 1 0 3 に格納される送信周期とによって、データフレームを生成するタイミングを決定し、データフレームの生成を周期的に行う。なお、データフレーム生成部 4 1 0 2 によりデータフレームが生成されると、そのデータフレームはデータフレーム送受信部 1 0 1 に通知され、データフレーム送受信部 1 0 1 はそのデータフレームの送信を行う。更に、データフレーム生成部 4 1 0 2 は、センサ値取得部 1 0 9 から取得されるセンサ値に変化があった時が、周期的なタイミングとは異なる時である場合には、イベントドリブンデータフレームの生成を行う。イベントドリブンデータフレームを生成する際には、データフレーム生成部 4 1 0 2 は、データフレーム生成ルール保持部 4 1 0 3 に格納されているメッセージ I D 毎のデータフレーム生成ルールの M A C 付与条件（後述）に基づいて M A C をイベントドリブンデータフレームに含めるか否かを判断し、M A C を含めると判断した場合にはイベントドリブンデータフレームフォーマットに従って M A C をデータフレームに含める。M A C は、実施の形態 3 で説明したものと同様である。即ち、データフレーム生成部 4 1 0 2 も実施の形態 3 で示したデータフレーム生成部 3 1 0 2 と同様に、送信周期を示すデータフレーム生成ルールに適合しないタイミングでデータフレームの送信をする際においてデータフレーム中に M A C という特定識別子を付与したデータフレームを生成する付与部としての機能を有する。データフレーム生成部 4 1 0 2 によるデータフレームの生成の結果として、データフレーム送受信部 1 0 1 により E C U 3 1 0 0 a からバス 2 0 0 に、周期的にデータフレームが送信され、更に、非周期的にイベントドリブンデータフレームが送信される。また、データフレーム生成部 4 1 0 2 は、E C U 4 1 0 0 a が送信を行う初回等（例えばエンジン始動時或いはその前、スリープ状態からの復帰時等）の周期的な送信の起点においてはデータフレームをイベントドリブンデータフレームの形式にして送信する。周期的な送信の起点においてイベントドリブンデータフレームではない周期的なデータフレームとしてしまうと、受信側で送信周期の条件に係る判断ができないからである。なお、初回等においてはイベントドリブンデータフレームに M A C を含めることにしても良い。

【0 1 4 3】

データフレーム生成ルール保持部 4 1 0 3 は、メモリ等の記憶媒体で実現され、データフレーム生成ルールとして E C U 4 1 0 0 a が送信するメッセージ I D 毎に周期的にデータフレームを送信するための送信周期と、M A C の格納位置、データ長等を示すイベントドリブンデータフレームフォーマットと、イベントドリブンデータフレームに M A C を付与する条件である M A C 付与条件とを格納している。M A C 付与条件は、車両の状態がどのような場合に M A C を付与すべきかについて定めている。図 2 7 は、データフレーム生成ルール保持部 4 1 0 3 に格納されたデータフレーム生成ルールの一例を示している。ここでは、E C U 4 1 0 0 a は、パワーウィンドウスイッチ 1 1 0 の状態を示すデータフレーム等、複数種類のデータフレーム（種類毎にメッセージ I D で識別されるデータフレーム）を送信するものとする。図 2 7 の例では、E C U 4 1 0 0 a から周期的に送信されるメッセージ I D が 0 x 1 0 0 のデータフレームについては、送信周期が 5 0 m s であり、この送信周期に従わずイベントドリブンデータフレームとして送信する場合には、車両の状態が走行中であるときに限って M A C を付与し、M A C を付与する際にはデータフィールドの下位 1 6 ビットに M A C を格納する必要があることを示している。また、メッセー

10

20

30

40

50

ジ I D が 0 x 2 0 0 のデータフレームについては、送信周期が 1 0 0 m s であり、メッセージ I D が 0 x 2 0 0 のイベントドリブンデータフレームは送信されないことを示している。また、E C U 4 1 0 0 a から周期的に送信されるメッセージ I D が 0 x 3 0 0 のデータフレームについては、送信周期が 7 0 m s であり、この送信周期に従わずイベントドリブンデータフレームとして送信する場合には、車両の状態が走行中であるとき及び駐車中であるときに M A C を付与し、M A C を付与する際にはデータフィールドの下位 1 6 ビットに M A C を格納する必要があることを示している。

【 0 1 4 4 】

不正データフレーム判断部 4 1 0 4 は、受信したデータフレームが正当なデータフレームであるか（不正なデータフレームでないか）否かについて判断する。即ち、不正データ
10
フレーム判断部 4 1 0 4 は、受信データフレーム周期保持部 4 1 0 5 の周期ルール情報を参照して、メッセージ I D 毎に予め定められた送信周期の条件を満たすか否かを確認し、送信周期の条件を満たす場合には正規の E C U から送信されたデータフレーム（正当なデータフレーム）であると判断する。また、不正データフレーム判断部 4 1 0 4 は、送信周期の条件を満たさないデータフレームであっても、車状態保持部 4 1 1 3 に格納されている車両の状態が受信データフレーム周期保持部 4 1 0 5 に格納されている M A C 付与イベントドリブンデータフレーム受信条件を満たす場合には、イベントドリブンデータフレームフォーマットに従ってデータフレームに M A C が含まれていることを検証することで不正なデータフレームか否かを判断する。M A C 付与イベントドリブンデータフレーム受信条件は、車両の状態がどのような場合に M A C が付与されたイベントドリブンデータフレームを受信するかを示す条件である。不正データフレーム判断部 4 1 0 4 は、車両の状態が M A C 付与イベントドリブンデータフレーム受信条件を満たす場合においてデータフィールド内の M A C の検証に成功すれば、受信したデータフレームが正当であると判断し、検証に失敗すれば、受信したデータフレームが不正なデータフレームであると判断する。即ち、不正データフレーム判断部 4 1 0 4 は、実施の形態 3 で示した不正データフレーム判断部 3 1 0 4 と同様に、送信周期を示すデータフレーム生成ルールに呼応した周期ルール情報に適合しないデータフレームがデータフレーム送受信部 1 0 1 により受信された場合に、そのデータフレーム中の M A C という特定識別子を検証する検証部としての機能を有する。M A C の検証は、データフレームのメッセージ I D 及びデータフィールドのデータ領域の内容を M A C 生成部 3 1 1 0 に通知することによって M A C 生成部 3 1 1 0 から
20
30
得られる値と、データフィールド内の M A C フィールド I の内容とが、一致するか否かを判別することで行われ、一致した場合に検証に成功する。不正データフレーム判断部 4 1 0 4 は、受信したデータフレームが予め定められた送信周期の条件を満たさず、かつ、車両の状態が M A C 付与イベントドリブンデータフレーム受信条件を満たさない場合には、M A C の検証を行わないでイベントドリブンデータフレームを正当なデータフレームであると判断する。つまり、イベントドリブンデータフレームについて、車両の状態が M A C 付与イベントドリブンデータフレーム受信条件を満たす場合には M A C を検証し、その他の場合には検証を省略している。但し、周期的な送信の初回等において送信側がイベントドリブンデータフレームに M A C を含めることにする場合には、対応した M A C の検証を受信側で行うと良い。なお、不正データフレーム判断部 4 1 0 4 は、送信周期の条件を満たすデータフレームを受信した場合に、受信時刻をデータフレーム受信履歴保持部 1 0 6 に前回受信時刻として記録する。不正データフレーム判断部 4 1 0 4 は、受信したデータフレームが正当なデータフレームであると判断した場合には、データフレーム処理部 1 0 7 にそのデータフレームの処理を行わせ、不正なデータフレームであると判断した場合には、そのデータフレームを破棄する（つまりそのデータフレームについてデータフレーム処理部 1 0 7 に処理させない）。

【 0 1 4 5 】

受信データフレーム周期保持部 4 1 0 5 は、メモリ等の記憶媒体で実現され、周期ルール情報を保持する。この周期ルール情報は、自機（E C U 4 1 0 0 a）が受信するデータフレームのメッセージ I D 毎に、予め定められた送信周期と、データフレームの受信間隔
40
50

について、送信周期の条件が満たされる（つまり正当な送信周期に合致する）と判断されるための許容範囲を示すマージンとを対応付けた情報である。周期ルール情報には、更に、送信周期の条件を満たさないイベントドリブンデータフレームのデータフィールド内に格納されるMACの格納位置、データ長等を示すイベントドリブンデータフレームフォーマットとMAC付与イベントドリブンデータフレーム受信条件とが含まれる。イベントドリブンデータフレームフォーマットは、不正データフレーム判断部4104が、イベントドリブンデータフレームについての正当性を検証（つまりMACを検証）する際に用いられる。また、MAC付与イベントドリブンデータフレーム受信条件は、車両の状態に係る条件であり、車両の状態がどの状態であればイベントドリブンデータフレームについてMACを検証すべきかを示す。なお、データフレームの受信側のECUの受信データフレーム周期保持部4105に保持される周期ルール情報における送信周期は、そのデータフレームの送信側のECUのデータフレーム生成ルール保持部4103に保持されるデータフレーム生成ルールにおける送信周期に呼応する。また、データフレームの受信側のECUの受信データフレーム周期保持部4105に保持される周期ルール情報におけるイベントドリブンデータフレームフォーマットは、そのデータフレームの送信側のECUのデータフレーム生成ルール保持部4103に保持されるデータフレーム生成ルールにおけるイベントドリブンデータフレームフォーマットに呼応する。また、データフレームの受信側のECUの受信データフレーム周期保持部4105に保持される周期ルール情報におけるMAC付与イベントドリブンデータフレーム受信条件は、そのデータフレームの送信側のECUのデータフレーム生成ルール保持部4103に保持されるデータフレーム生成ルールにおけるMAC付与条件に呼応する。図28は、ECU4100aから送信されたデータフレームを受信するECU4100bにおける受信データフレーム周期保持部4105に格納された周期ルール情報の一例を示す図である。同図の例では、メッセージIDが0x100のデータフレームの送信周期が50ms、メッセージIDが0x200のデータフレームの送信周期が100ms、メッセージIDが0x300のデータフレームの送信周期が70msであることを示している。同図の例では、マージンは、どのメッセージIDについても1msである。このマージンが1msであるため、メッセージIDが0x100のデータフレームについて送信周期が49ms以上51ms以下の範囲であれば、ECU4100bにおける不正データフレーム判断部4104は、送信周期の条件が満たされると判断することになる。また、図28の例でのイベントドリブンデータフレームフォーマットについては、メッセージIDが0x100及び0x300のイベントドリブンデータフレームは、データフィールドの下位16ビットにMACが付与されていることを示しており、メッセージIDが0x200のイベントドリブンデータフレームは送信されないことを示している。また、図28の例でのMAC付与イベントドリブンデータフレーム受信条件については、メッセージIDが0x100のイベントドリブンデータフレームは車両の状態が走行中であるときにMACの検証が必要であることを示し、メッセージIDが0x200のイベントドリブンデータフレームは送信されないためMACの検証が不要であることを示し、メッセージIDが0x300のイベントドリブンデータフレームは車両の状態が走行中及び駐車中のいずれかの状態であるときにMACの検証が必要であることを示している。

【0146】

車状態保持部4113は、メモリ等の記憶媒体で実現され、車両の状態を示す値が格納される。図29に車状態保持部4113に格納された車両の状態の一例を示している。この例では車両の状態が、走行中であることを示している。車状態保持部4113における車両の状態は、ECU4100cから送信されるデータフレーム（車両の状態を示すデータフレーム）が受信され、正当なデータフレームであると判断された場合に、データフレーム処理部107により、そのデータフレームの内容に応じて格納（更新）がなされる。

【0147】

[4.3 ECU4100aにおけるデータフレームの送信処理]

以下、ECU4100aがデータフレームをバス200に送信し、ECU4100bが

10

20

30

40

50

データフレームをバス200から受信する例を想定して、ECU4100aにおけるデータフレームの送信処理を説明する。

【0148】

図30は、ECU4100aにおけるデータフレームの送信処理を示すフローチャートである。

【0149】

ECU4100aは、データフレーム生成ルールにおける送信周期に従った送信タイミング（前回の送信から送信周期が経過したタイミング）、或いは、センサ値取得部109からのセンサ値が変化したタイミングで、データフレームの生成が必要となり、図30の送信処理を開始する。送信処理においては、まず、ECU4100aは、送信するデータフレームがイベントドリブンデータフレームか周期的なデータフレームかを判断する（ステップS4101）。

10

【0150】

ECU4100aは、ステップS4101において送信するデータフレームがデータフレーム生成ルールにおける送信周期に従っていないイベントドリブンデータフレームであると判断した場合には、ECU4100cからのデータフレームに対応して車状態保持部4113に格納された車両の状態がデータフレーム生成ルールのMAC付与条件を満たすか否かを判断する（ステップS4102）。例えば、MAC付与条件が、走行中及び駐車中のいずれかを示し、ECU4100aからのデータフレームで示された車両の状態（車状態保持部4113の車両の状態）が走行中を示す場合には、車両の状態がMAC付与条件を満たすと判断される。

20

【0151】

ECU4100aは、ステップS4102において、車両の状態がMAC付与条件を満たすと判断した場合には、データフレーム生成ルールのイベントドリブンデータフレームフォーマットに従って、生成するデータフレームのデータフィールドのMACフィールドに、MACを付与する（ステップS4103）。

【0152】

ECU4100aは、ステップS4101において、送信するデータフレームが、データフレーム生成ルールにおける送信周期に従う周期的なデータフレームであると判断した場合（イベントドリブンデータフレームでないと判断した場合）には、ステップS4102、S4103での処理をスキップする。また、ECU4100aは、ステップS4102において、車両の状態がMAC付与条件を満たさないと判断した場合には、ステップS4103での処理をスキップする。

30

【0153】

ECU4100aは、ステップS4103の後、或いはステップS4103での処理をスキップした後に、データフィールドのデータ領域にセンサ値取得部109から取得した最新のセンサ値をセットして、送信するデータフレームを生成し、バス200へと送信する（ステップS4104）。これにより、バス200上にデータフレームが流れ、ECU4100bに受信されるようになる。

【0154】

なお、ECU4100bも図30に示すものと同様の送信処理を実行し得る。

40

【0155】

[4.4 ECU4100bにおけるデータフレームの受信処理]

以下、ECU4100aがデータフレームをバス200に送信し、ECU4100bがデータフレームをバス200から受信する例を想定して、ECU4100bにおけるデータフレームの受信処理を説明する。

【0156】

図31は、ECU4100bにおけるデータフレームの受信処理を示すフローチャートである。

【0157】

50

ECU4100bは、バス200上に現れるデータフレームを受信する（ステップS4201）。なお、ECU4100bは、自機が受信すべきメッセージIDを含まないデータフレームであればそのデータフレームを破棄して処理を終了する。自機が受信すべきメッセージIDを含むデータフレームを受信した場合に、ECU4100bは、その受信が、保持している周期ルール情報で規定された送信周期範囲内か否かを判断する（ステップS4202）。なお、ECU4100bの不正データフレーム判断部4104は、受信したデータフレームの受信間隔（つまり送信周期）が規定の送信周期の範囲内であるか否か（つまり周期ルール情報で定められた送信周期の条件を満たすか否か）を、タイマ108、受信データフレーム周期保持部4105及びデータフレーム受信履歴保持部106から得られる情報に基づいて判断する。即ち、不正データフレーム判断部4104は、前回受信時刻と今回受信したデータフレームの受信時刻の差分（受信間隔）が、受信したデータフレームのメッセージIDに対応して定められた送信周期からマージンを引いた値以上であり、かつ、その送信周期にマージンを加えた値以下であるか否かを判断する。

10

【0158】

ステップS4202において、データフレームの受信間隔が送信周期の範囲内である場合には、送信周期の条件が満たされたことになり、ECU4100bは、データフレーム受信履歴保持部106が保持するリストに、受信したデータフレームのメッセージIDに対応付けて、前回受信時刻として、そのデータフレームの受信時刻を記録（つまり前回受信時刻を更新）する（ステップS4204）。そして、ステップS4204での処理に続いて、ECU4100bの不正データフレーム判断部4104により、受信したデータフレームが正当なデータフレームであると判断され（ステップS4206）、データフレーム処理部107によりそのデータフレームに対応した処理がなされる。

20

【0159】

また、ステップS4202において、データフレームの前回受信時刻と今回受信時刻の差分が送信周期の範囲内でない場合には、ECU4100bは、車両の状態がMAC付与イベントドリブンデータフレーム受信条件を満たすか否かを判断する（ステップS4203）。即ち、ECU4100bは、ECU4100cからのデータフレームに対応して車状態保持部4113に格納された車両の状態が、MAC付与イベントドリブンデータフレーム受信条件を満たすか否かを判断する。

【0160】

ステップS4203において、車両の状態がMAC付与イベントドリブンデータフレーム受信条件を満たすと判断した場合には、ECU4100bは、受信データフレーム周期保持部4105に格納されているイベントドリブンデータフレームフォーマットに従ってデータフレームのデータフィールドをMACフィールドIとデータ領域とに分けて、データ領域及びメッセージIDから算出されるMACと、MACフィールドに含まれるMACとを比較することで、データフレームの正当性（MACが正しいこと）を検証する（ステップS4205）。算出されるMACとMACフィールドに含まれるMACとが一致すればMACの検証（つまりMACの正当性の検証）に成功し、受信したデータフレームが正当なデータフレームであると判断され（ステップS4206）、データフレーム処理部107によりそのデータフレームに対応した処理がなされる。

30

40

【0161】

ステップS4205において、算出されるMACとMACフィールドに含まれるMACとが一致しない場合（MACの検証に成功しない場合）には、ECU4100bは、受信したデータフレームが不正なデータフレームであると判断してデータフレームを破棄する（ステップS4207）。従って、ECU4100bは、不正なECUにより送信された不正なデータフレームを処理しない。

【0162】

また、ステップS4203において車両の状態がMAC付与イベントドリブンデータフレーム受信条件を満たさないと判断した場合には、ECU4100bは、受信したデータフレームが正当なデータフレームである判断し（ステップS4206）、データフレーム

50

処理部107によりそのデータフレームに対応した処理を行う。

【0163】

なお、ステップS4202において、データフレームの受信間隔（つまり送信周期）が規定の送信周期の範囲内か否かを判断するに際して、初回等といった前回受信時刻が保存されていない場合においては、受信したデータフレームをイベントドリブンデータフレームと扱い、MACの検証に成功したときにそのデータフレームの受信時刻を前回受信時刻として記録してからステップS4206の処理を行うことができる。この場合、送信側のECUでは初回等の周期的な送信の起点においては例外的にMACを付与したイベントドリブンデータフレームを送信する。また、各ECUが例えばスリープ状態等に入ってからデータフレームの周期的な送信を休止する期間がある場合には、その後の周期的な送信の再開時にデータフレームをイベントドリブンデータフレームとして送信することとしても良い。この場合には、受信側のECUでは前回受信時刻から一定時間以上の間、送信側のECUがスリープ状態に入ってから周期的な送信が途切れた場合に、前回受信時刻を無効にして次回を初回と扱い、受信したデータフレームをイベントドリブンデータフレームと扱い、その正当性を判断することができる。

10

【0164】

また、ECU4100aも図31に示すものと同様の受信処理を実行し得る。

【0165】

[4.5 ECU4100cにおける車両の状態を示すデータフレームの送信処理]

以下、ECU4100cが車両の状態を取得して車両の状態を示すデータフレームをバス200に送信する送信処理を説明する。

20

【0166】

図32は、ECU4100cにおける車両の状態を示すデータフレームの送信処理を示すフローチャートである。同図に示す処理は、ECU4100cにより繰り返し実行される。

【0167】

ECU4100cは、接続されているギア4130の状態をセンサから取得する（ステップS4301）。

【0168】

ECU4100cは、取得したギア4130の状態が前回取得した状態から変化したか否かを判断し（ステップS4302）、ギア4130の状態が変化した場合には、予め定められているギア4130の状態（例えば、ギアポジションについてパーキング、1速、2速等）と車両の状態（走行中、駐車中等）との対応関係に基づいて、車両の状態を特定してその車両の状態をデータフィールドの内容として含ませたデータフレームを生成し、イベントドリブンデータフレームとしてバス200へと送信する（ステップS4303）。

30

【0169】

なお、ECU4100cは、イベントドリブンデータフレームにはMACを付与して送信しても良く、この場合には、ECU4100a及びECU4100bは、バス200から受信したイベントドリブンデータフレームのMACを検証して、検証に成功した場合に限って車両の状態を取得して車状態保持部4113に格納することになる。

40

【0170】

[4.6 ECU4100bにおけるデータフレームの受信処理の変形例]

上述したデータフレームの受信処理（図31参照）においては、ステップS4203において車両の状態がMAC付与イベントドリブンデータフレーム受信条件を満たさない場合には、受信したデータフレームを正当であると判断することとしたが、車両の状態がMAC付与イベントドリブンデータフレーム受信条件を満たさない場合には、受信したデータフレームを不正なデータフレームであると判断して破棄するように変形しても良い。以下、受信処理の変形例について示す。

【0171】

50

図33は、ECU4100bにおけるデータフレームの受信処理の変形例を示すフローチャートである。

【0172】

ECU4100bは、バス200上に現れるデータフレームを受信する（ステップS4401）。ECU4100bは、自機が受信すべきメッセージIDを含むデータフレームを受信した場合に、その受信が、保持している周期ルール情報で規定された送信周期範囲内か否かを判断する（ステップS4402）。ステップS4402において、データフレームの受信間隔が送信周期の範囲内である場合には、ECU4100bは、データフレーム受信履歴保持部106が保持するリストに、受信したデータフレームのメッセージIDに対応付けて、前回受信時刻として、そのデータフレームの受信時刻を記録する（ステップS4404）。そして、ステップS4404での処理に続いて、ECU4100bの不正データフレーム判断部4104により、受信したデータフレームが正当なデータフレームであると判断され（ステップS4406）、データフレーム処理部107によりそのデータフレームに対応した処理がなされる。

10

【0173】

また、ステップS4402においてデータフレームの受信が規定された送信周期範囲内でないと判断した場合には、ECU4100bは、車両の状態がMAC付与イベントドリブンデータフレーム受信条件を満たすか否かを判断する（ステップS4403）。

【0174】

ステップS4403において、車両の状態がMAC付与イベントドリブンデータフレーム受信条件を満たすと判断した場合には、ECU4100bは、受信データフレーム周期保持部4105に格納されているイベントドリブンデータフレームフォーマットに基づいてデータ領域及びメッセージIDから算出されるMACと、MACフィールドに含まれるMACとを比較することで、データフレームの正当性（MACが正しいこと）を検証する（ステップS4405）。MACが正しいことを検証した場合にはECU4100bは、受信したデータフレームを正当なデータフレームであると判断し（ステップS4406）、データフレーム処理部107によりそのデータフレームに対応した処理を行う。

20

【0175】

ステップS4403において車両の状態がMAC付与イベントドリブンデータフレーム受信条件を満たさないと判断した場合、及び、ステップS4405においてMACが正しいことの検証に成功しない場合には、ECU4100bは、受信したデータフレームが不正なデータフレームであると判断してデータフレームを破棄する（ステップS4407）。従って、ECU4100bは、不正なECUにより送信された不正なデータフレームを処理しない。

30

【0176】

〔4.7 実施の形態4の効果〕

実施の形態4では、周期的に送信されるデータフレームに加えて、非周期的に送信されるイベントドリブンデータフレームが存在する場合でも、イベントドリブンデータフレーム内に特定識別子としてのMACを含めることによって、正当なイベントドリブンデータフレームであることを検証可能にする車載ネットワークシステム13を示した。即ち、車載ネットワークシステム13では、送信周期の条件により正当なデータフレームであるか否かを判別し、送信周期の条件によっては判別ができない場合に限って特定識別子により正当なデータフレームであるか否かを判別（つまり検証）するようにしている。これにより、送信周期の条件を満たさない正当なイベントドリブンデータフレームが不正なものとして誤検知されることが防止される。また、不正なECUがデータフレームを送信する場合には、送信周期の条件を満たさない可能性が高く、正しくMACを付与できないため、このデータフレームを受信したECUによって不正なデータフレームであると判断されるようになる。またイベントドリブンデータフレームについても、車両の状態に応じてMACを付与及び検証するか否かを切り替えることによって、効率的に不正なデータフレームの検知が可能となる。

40

50

【0177】

(他の実施の形態等)

以上のように、本開示に係る技術の例示として実施の形態1～4を説明した。しかしながら、本開示に係る技術は、これに限定されず、適宜、変更、置き換え、付加、省略等を行った実施の形態にも適用可能である。例えば、以下のような変形例も本開示の一実施態様に含まれる。

【0178】

(1) 上記実施の形態では、イベントドリブンデータフレームを送信するECUがイベントドリブンデータフレームにイベントドリブン識別フラグ、イベントカウンタ、或いは、所定演算の結果値であるMACという特定識別子を付与し、イベントドリブンデータフレームを受信するECUで特定識別子を検証する例を示したが、特定識別子は例示した以外の形式の情報であっても良い。特定識別子の検証は、例えば、データフレームの所定位置における所定データ長のデータ値が、固定値又は所定演算により導出される値と一致するか否かを検査し、一致すれば検証に成功したと扱い、一致しなければ検証に失敗したと扱う処理手順等である。なお、上記実施の形態ではデータフレームを受信するECUが、データフレームが送信周期に係るルール(条件)に適合しないイベントドリブンデータフレームであると判断した後に特定識別子の検証を行う例を示したが、データフレーム中の特定識別子の検証を、送信周期のルールに適合するか否かの判断より前に、或いは、その判断と同時に、行っても良い。

【0179】

(2) 上記実施の形態では、メッセージIDとデータ値とカウンタ値とに基づく演算によりMACを生成(計算)しているが、データフレームの一部の内容を反映して(つまり一部の内容に基づいて)MACを生成すれば良く、データ値のみからMACを生成することとしても良い。またカウンタ値のみからMACを生成することとしても良い。データフレームを受信するECUにおけるMACの検証方式は、データフレームを送信するECUがデータフレームにMACを付与する方式に対応したものであれば良い。また、MACを付与するデータフレームにおいてはデータフィールド内にデータ値及びMACの他に、一部又は全てのカウンタ値を含めても良い。また、上記実施の形態では、MAC算出のアルゴリズムをHMACとしているが、これCBC-MAC(Cipher Block Chaining Message Authentication Code)、CMAC(Cipher-based MAC)であっても良い。また、MAC計算に用いられるパディングについては、ゼロパディング、ISO10126、PKCS#1、PKCS#5、PKCS#7、その他、ブロックのデータサイズが計算に必要なとなるパディングの方式であれば何でも良い。

【0180】

(3) 上記実施の形態では、車両の状態として走行中及び駐車中という2つの状態について説明したが、停車中、高速走行中、低速走行中、バック中、エンジン停止等の各種状態を区別し、各種状態のうち、イベントドリブンデータフレームにMACを付与及び検証すべき条件としての車両の状態を定めても良い。例えば、不正なECUにより不正なデータフレームがバス上に送信された場合に不正であることを検知する必要性が比較的高いタイミングに対応するように、MACを付与及び検証すべき条件としての車両の状態を定めること等が有用となり得る。また、車両の状態は、必ずしもギア4130の状態に基づいて判断する必要はなく、車両内のいずれかのECUがいずれかの機器から取得したセンサ値等を含むデータフレームを送信し、他のECUがそのデータフレームを受信することによって車両の状態を判断することとしても良い。例えば、走行速度に関する情報等を示すデータフレームをECU間で送受信することで、そのデータフレームを受信した各ECUがそのデータフレームに基づいて車両の状態として高速走行中であること等を判断できるようにしても良い。このため、例えば車両の状態示すデータフレームを送信するECU4100cが必ずしもギア4130に接続されている必要はない。受信したデータフレームに基づいて各ECUが同様に車両の状態を判断すれば、あるECUが、MAC付与が必要な車両の状態である場合にMACを付与してデータフレームを送信すると、受信側の

E C Uはその車両の状態に基づいてM A Cの検証が必要であることを認識して検証を行い得る。

【0181】

(4) 上記実施の形態では、イベントドリブンデータフレームを識別するための特定識別子としてイベントドリブン識別フラグ、イベントカウンタ、M A Cを用いる例について、それぞれ説明したが、イベントドリブン識別フラグ、イベントカウンタ及びM A Cの2つ以上を組み合わせて用いることとしても良い。例えば、データフレームを受信したE C Uが、イベントドリブン識別フラグによってイベントドリブンデータフレームであることを判断してから、M A Cによってデータフレームの正当性を検証することとしても良い。なお、イベントドリブンデータフレームでないデータフレームについては特定識別子を付与しても構わないが、付与する必要はない。

10

【0182】

(5) 上記実施の形態では、各E C Uはデータフレームを送信することとしたが、車載ネットワークシステムは、データフレームを受信するのみでデータフレームを送信しないE C Uを含んでいても良い。また逆に、車載ネットワークシステムは、データフレームを送信するのみで、データフレームを受信しないE C Uを含んでいても良い。また、各E C Uは必ずしも周期的なデータフレームの送信をしなくても良く、車載ネットワークシステムは、イベントドリブンデータフレームのみを送信するE C Uを含んでいても良い。

【0183】

(6) 上記実施の形態では、E C Uがパワーウィンドウスイッチ或いはパワーウィンドウに接続されている構成を例示したが、E C Uは、パワーウィンドウスイッチ及びパワーウィンドウに限らず、その他の機器に接続されても良く、その機器の制御、その機器からの状態の取得等を行っても良い。

20

【0184】

(7) 上記実施の形態では、E C Uは不正なデータフレームを検知した場合に、データフレームを破棄することとしたが、必ずしも破棄する必要はなく、不正なデータフレームを検知した場合に例えば不正を検知したことを知らせるデータフレームを送信しても良く、また例えばその送信するデータフレームには不正なデータフレームに関する情報を含めても良い。また、不正なデータフレームを検知した場合に、例えば、ログとして記録すること、或いは、車両の動作モードをより安全性を高める状態等に変更すること等の処理を行っても良い。

30

【0185】

(8) 上記実施の形態では、イベントドリブンデータフレームの送信毎、及び、受信毎に各E C Uの該当の送信カウンタ或いは受信カウンタが1増加（インクリメント）されることとしたが、これらのカウンタの値に対する演算は、1増加には限定されない。これらのカウンタの値に対する演算は、データフレームの送信側と受信側で同様の計算ができ、送信カウンタと受信カウンタとが同期するような演算であれば良い。例えば、前回の演算結果を入力値として予め定められたアルゴリズムに基づいて特定された出力値を演算結果とする演算等である。即ち、E C Uは、イベントドリブンデータフレームに前回送信の際に付与したカウンタ等の特定識別子（つまり前回の演算結果）に基づいて、所定の演算を行った結果として得られる値を、次に送信するイベントドリブンデータフレームに特定識別子として含ませることとしても良い。

40

【0186】

(9) 上記実施の形態で示したデータフレーム生成ルール及び周期ルール情報は、一例であり、例示した値と異なる値にしても良い。また、データフレーム生成ルール或いは周期ルール情報は、各E C Uの出荷時に設定されても良いし、車載ネットワークシステムが搭載される車体の出荷時に設定されても良い。また、データフレーム生成ルール或いは周期ルール情報は、外部との通信に基づいて設定されても、各種記録媒体等を用いて設定されても、ツール類等によって設定されても良い。

【0187】

50

(10) 上記実施の形態では、各 ECU が不正なデータフレームを検知する機能を有する例を示したが、その機能を 1 台以上の特定の ECU のみが有することとしても良い。例えば車載ネットワークシステムが複数のバスそれぞれに接続された ECU 群で構成されることとした場合において各バスを繋ぐゲートウェイとしての ECU にのみ不正なデータフレームを検知する機能を含ませても良い。また、例えば車載ネットワークシステムが、自動車のインパネ（インストルメントパネル）等に設けられて運転者に視認されるための情報を表示する液晶ディスプレイ（LCD：liquid crystal display）等の表示装置、運転者の操作を受け付ける入力手段等を備える一種の ECU であるヘッドユニットを含む場合において、ヘッドユニットにのみ不正なデータフレームを検知する機能を含ませても良い。また、車載ネットワークシステムが、上述の不正なデータフレームを検知する機能を有し、バスを監視して不正なデータフレームを検知した場合にその旨を示すデータフレームの送信等を行う 1 台以上の特定の ECU を含むこととしても良い。

10

【0188】

(11) 上記実施の形態では、MAC 鍵をメッセージ ID 毎に 1 つ保持している例を示したが、ECU 毎に 1 つ保持することとしても良い。また、全ての ECU が同じ MAC 鍵を保持している必要はない。また、同一のバスに接続された各 ECU は、共通の MAC 鍵を保持していても良い。

【0189】

(12) 上記実施の形態では、送信カウンタ或いは受信カウンタを送信或いは受信するデータフレームのメッセージ ID 毎に 1 つ保持しているが、複数のメッセージ ID に対して 1 つ保持することとしても良い。また、同一のバス上を流れる全てのデータフレームに対して、同じカウンタを使用しても良い。

20

【0190】

(13) 上記の実施の形態における、不正データフレーム判断部は CAN コントローラと呼ばれるハードウェア、または、CAN コントローラと接続して動作するマイコン上で動作するファームウェアに実装しても良い。また、MAC 鍵保持部、カウンタ保持部、受信データフレーム周期保持部、データフレーム受信履歴保持部は、CAN コントローラと呼ばれるハードウェアのレジスタ、または、CAN コントローラと接続して動作するマイコン上で動作するファームウェアに格納されていても良い。

【0191】

30

(14) 上記実施の形態では、CAN プロトコルにおけるデータフレームを標準 ID フォーマットで記述しているが、拡張 ID フォーマットであっても良い。拡張 ID フォーマットの場合には、標準 ID フォーマットにおける ID 位置のベース ID と、拡張 ID とを合わせて 29 ビットで ID（メッセージ ID）を表すので、この 29 ビットの ID を上述の実施の形態における ID（メッセージ ID）と扱えば良い。

【0192】

(15) 上記実施の形態で示した CAN プロトコルは、TT CAN（Time-Triggered CAN）、CAN FD（CAN with Flexible Data Rate）等の派生的なプロトコルをも包含する広義の意味を有するものであっても良い。

【0193】

40

(16) 上記実施の形態における各 ECU は、例えば、プロセッサ、メモリ等のデジタル回路、アナログ回路、通信回路等を含む装置であることとしたが、ハードディスク装置、ディスプレイ、キーボード、マウス等の他のハードウェア構成要素を含んでいても良い。また、メモリに記憶された制御プログラムがプロセッサにより実行されてソフトウェア的に機能を実現する代わりに、専用のハードウェア（デジタル回路等）によりその機能を実現することとしても良い。

【0194】

(17) 上記実施の形態における各装置（ECU 等）を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良い。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

50

製造された超多機能 L S I であり、具体的には、マイクロプロセッサ、ROM、RAM等を含んで構成されるコンピュータシステムである。前記 RAM には、コンピュータプログラムが記録されている。前記マイクロプロセッサが、前記コンピュータプログラムに従って動作することにより、システム L S I は、その機能を達成する。また、上記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 チップ化されても良い。また、ここでは、システム L S I としたが、集積度の違いにより、I C、L S I、スーパー L S I、ウルトラ L S I と呼称されることもある。また、集積回路化の手法は L S I 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良い。L S I 製造後に、プログラムすることが可能な F P G A (Field Programmable Gate Array) や、L S I 内部の回路セルの接続や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良い。さらには、半導体技術の進歩又は派生する別技術により L S I 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良い。バイオ技術の適用等が可能性としてあり得る。

【0195】

(18) 上記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 I C 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良い。前記 I C カードまたは前記モジュールは、マイクロプロセッサ、ROM、RAM等から構成されるコンピュータシステムである。前記 I C カードまたは前記モジュールは、上記の超多機能 L S I を含むとしても良い。マイクロプロセッサが、コンピュータプログラムに従って動作することにより、前記 I C 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 I C 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良い。

【0196】

(19) 本開示の一態様としては、上記に示す不正検知方法であるとしても良い。また、こ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良いし、前記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良い。また、本開示の一態様としては、前記コンピュータプログラムまたは前記デジタル信号をコンピュータで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)、半導体メモリ等に記録したものとしても良い。また、これらの記録媒体に記録されている前記デジタル信号であるとしても良い。また、本開示の一態様としては、前記コンピュータプログラムまたは前記デジタル信号を、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良い。また、本開示の一態様としては、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、前記メモリは、上記コンピュータプログラムを記録しており、前記マイクロプロセッサは、前記コンピュータプログラムに従って動作するとしても良い。また、前記プログラムまたは前記デジタル信号を前記記録媒体に記録して移送することにより、または前記プログラムまたは前記デジタル信号を前記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としても良い。

【0197】

(20) 上記実施の形態及び上記変形例で示した各構成要素及び機能を任意に組み合わせることで実現される形態も本開示の範囲に含まれる。

【産業上の利用可能性】

【0198】

本開示は、車載ネットワークシステムにおいて不正な E C U によりバス上に不正なメッセージの送信が行われたことを効率的かつ適切に検知するために利用可能である。

【符号の説明】

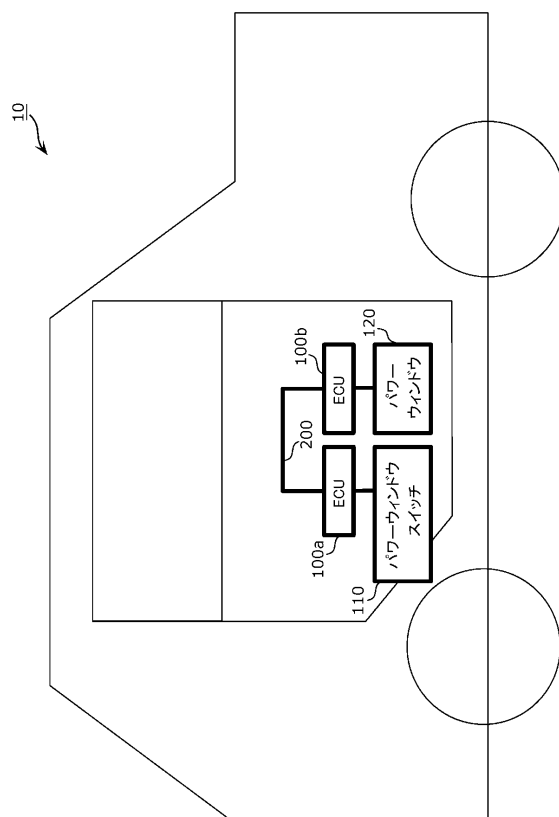
【0199】

10, 11, 12, 13 車載ネットワークシステム
100a, 100b, 2100a, 2100b, 3100a, 3100b, 4100a, 4100b, 4100c 電子制御ユニット (E C U)

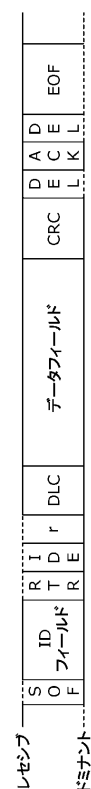
- 101 データフレーム送受信部
- 102, 2102, 3102, 4102 データフレーム生成部
- 103, 2103, 3103, 4103 データフレーム生成ルール保持部
- 104, 2104, 3104, 4104 不正データフレーム判断部
- 105, 3105, 4105 受信データフレーム周期保持部
- 106, 2106 データフレーム受信履歴保持部
- 107 データフレーム処理部
- 108 タイマ
- 109 センサ値取得部
- 110 パワーウィンドウスイッチ
- 120 パワーウィンドウ
- 200 バス
- 3110 MAC生成部
- 3111 MAC鍵保持部
- 3112 カウンタ保持部
- 4113 車状態保持部
- 4130 ギア

10

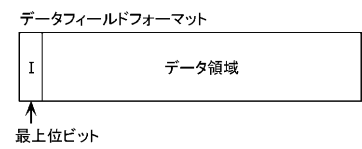
【図1】



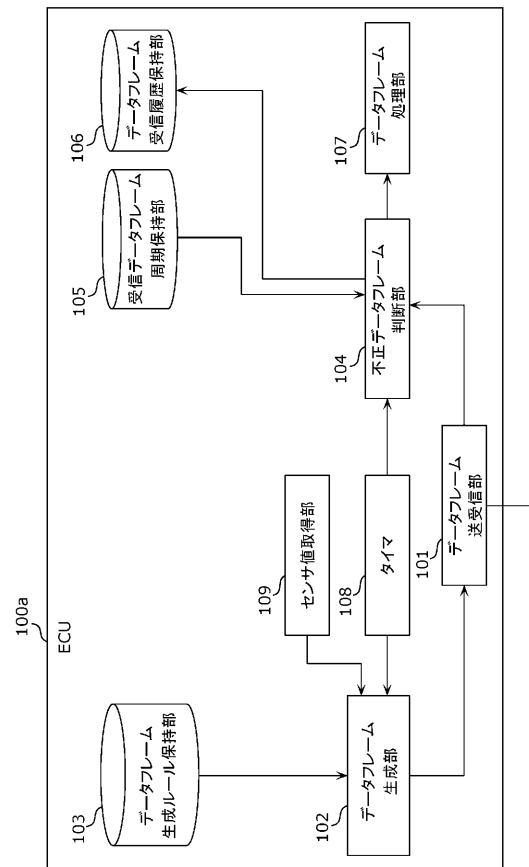
【図2】



【図 3】



【図 4】



【図 5】

データフレーム生成ルール

ID	送信周期
0x100	50
0x200	100
0x300	70
...	...

【図 7】

受信履歴リスト

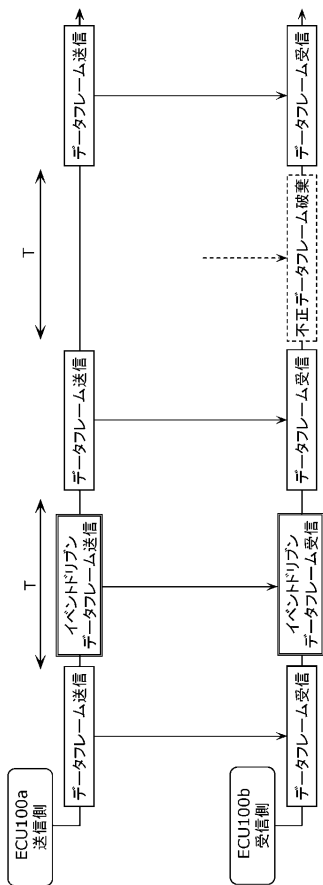
ID	前回受信時刻
0x100	200
0x200	220
0x300	230
...	...

【図 6】

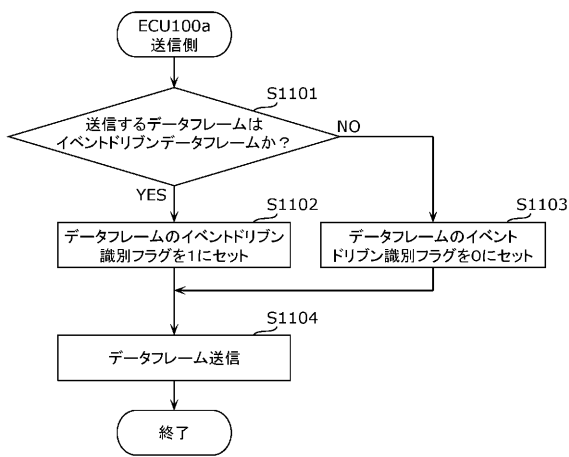
周期ルール情報

ID	送信周期	マージン
0x100	50	1
0x200	100	1
0x300	70	1
....		

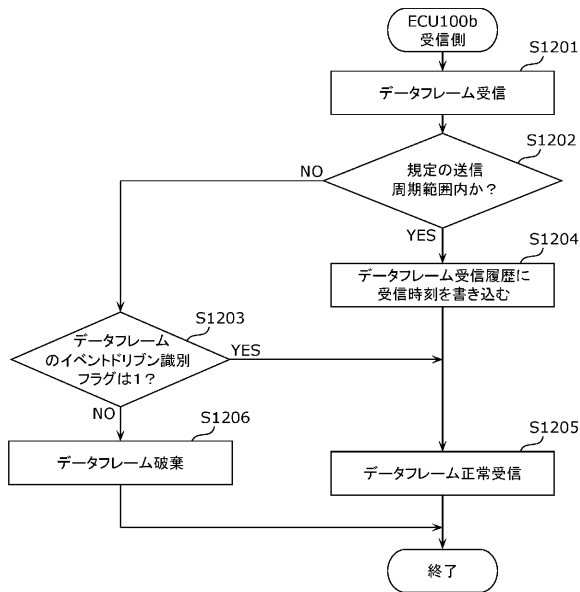
【図 8】



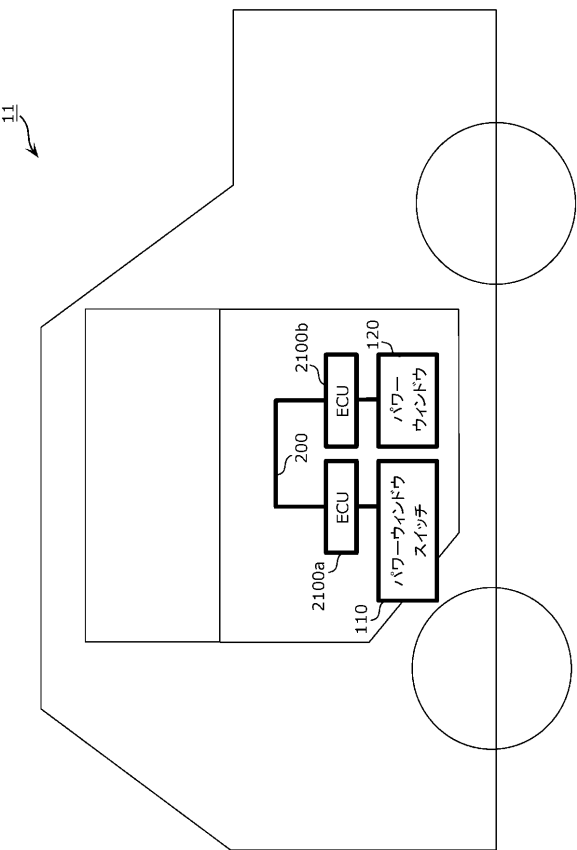
【図 9】



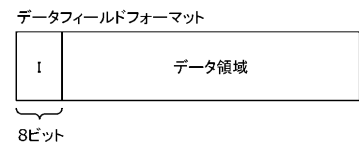
【図 10】



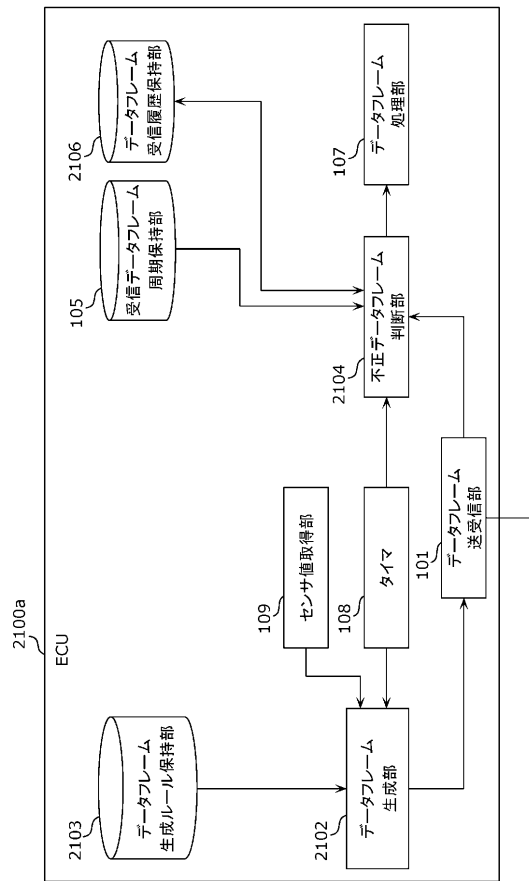
【図 11】



【図 1 2】



【図 1 3】

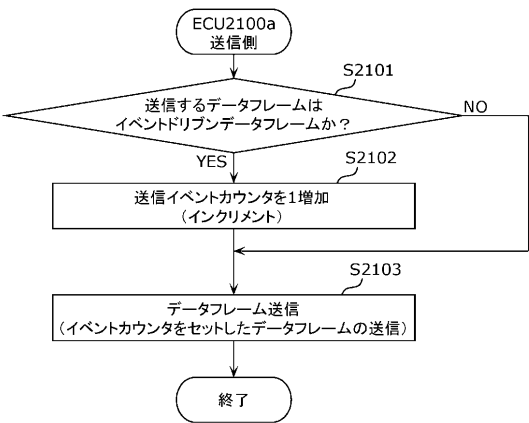


【図 1 4】

データフレーム生成ルール

ID	送信周期	送信イベントカウンタ
0x100	50	15
0x200	100	0
0x300	70	5
...	...	...

【図 1 6】

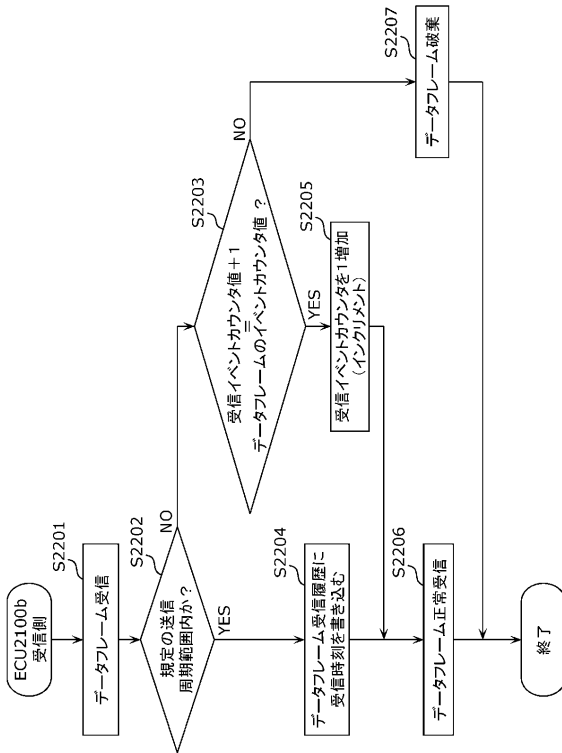


【図 1 5】

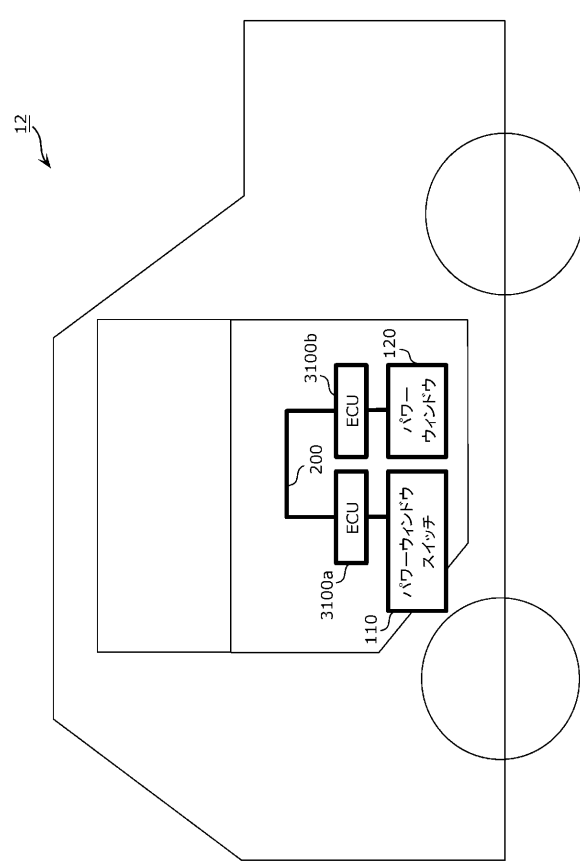
周期ルール情報

ID	前回受信時刻	受信イベントカウンタ
0x100	200	15
0x200	220	0
0x300	230	5
...	...	...

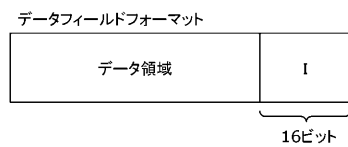
【図 17】



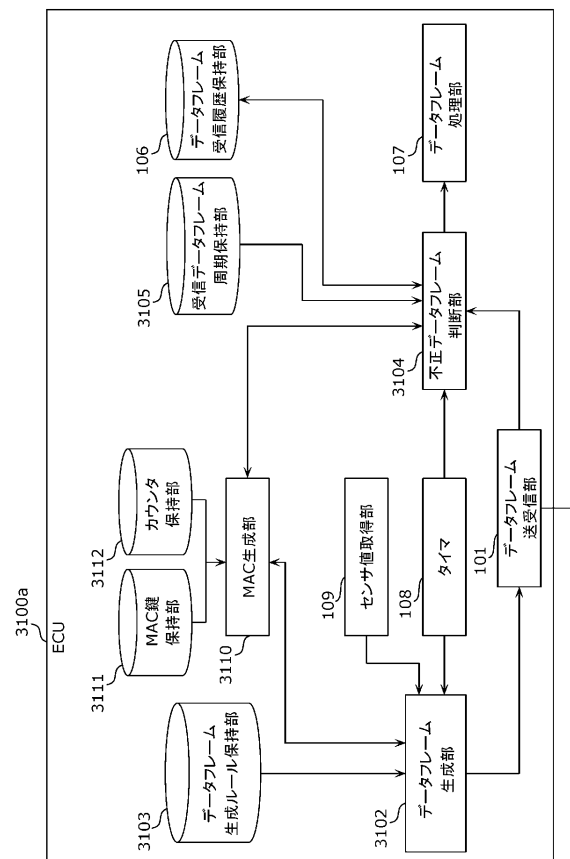
【図 18】



【図 19】



【図 20】



【図 2 1】

データフレーム生成ルール

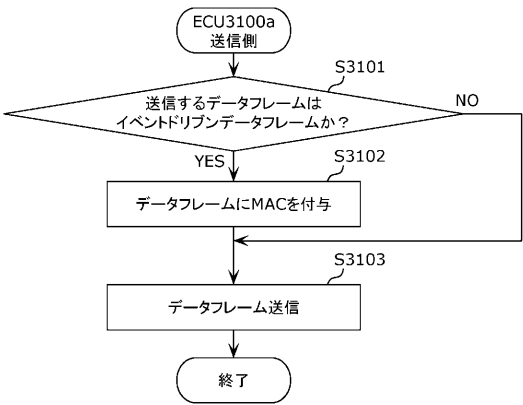
ID	送信周期	イベントドリブンデータ フレームフォーマット
0x100	50	下位16ビットMAC
0x200	100	イベントドリブンデータ フレームなし
0x300	70	下位16ビットMAC
...	...	...

【図 2 2】

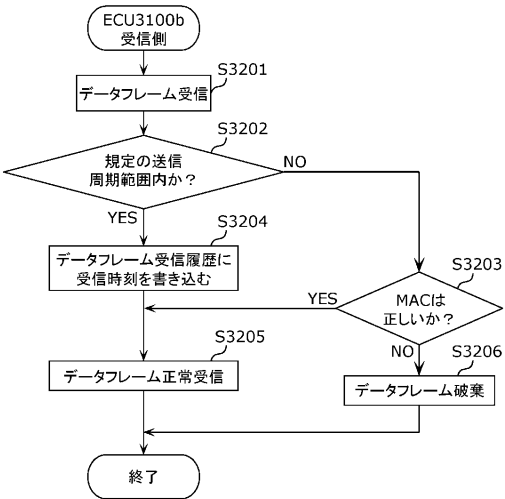
周期ルール情報

ID	送信周期	マージン	イベントドリブンデータ フレームフォーマット
0x100	50	1	下位16ビットMAC
0x200	100	1	イベントドリブンデータ フレームなし
0x300	70	1	下位16ビットMAC
...	...	...	...

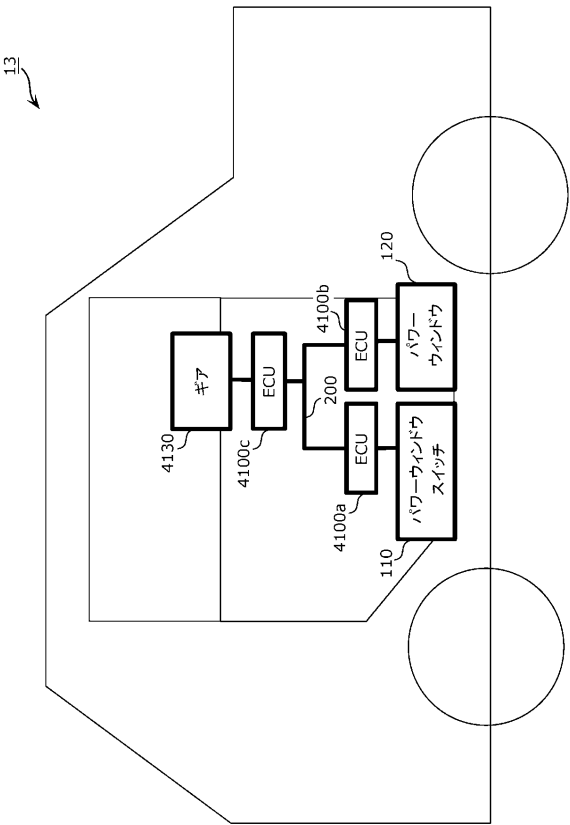
【図 2 3】



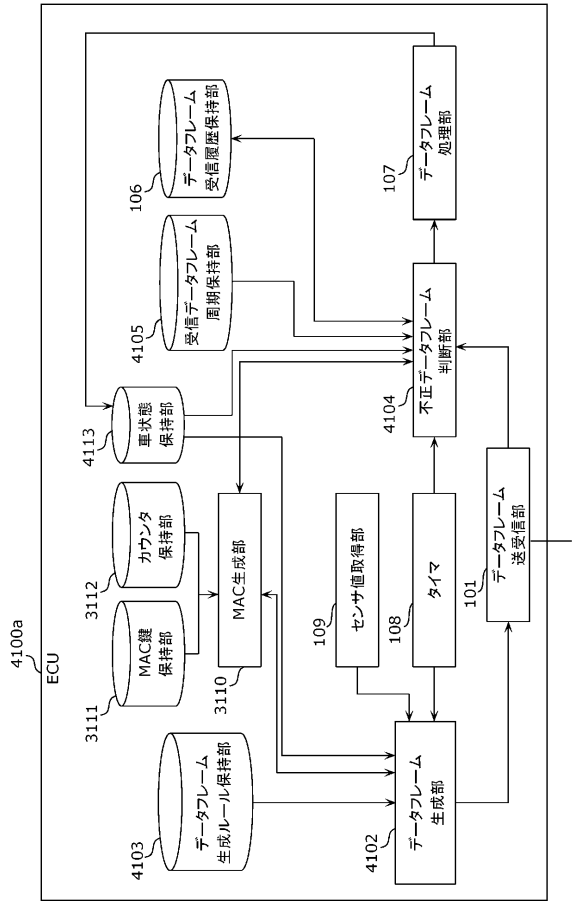
【図 2 4】



【図 2 5】



【図 2 6】



【図 2 8】

周期ルール情報				
ID	送信周期	マージン	イベントドリブンデータフレームフォーマット	MAC付与イベントドリブンデータフレーム受信条件
0x100	50	1	下位16ビットMAC	走行中
0x200	100	1	イベントドリブンデータフレームなし	なし
0x300	70	1	下位16ビットMAC	走行中、駐車中
...	...	...	...	...

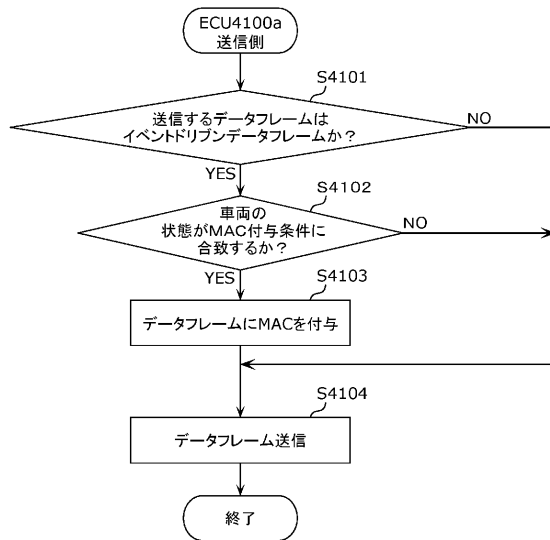
【図 2 7】

データフレーム生成ルール			
ID	送信周期	イベントドリブンデータフレームフォーマット	MAC付与条件
0x100	50	下位16ビットMAC付与	走行中
0x200	100	イベントドリブンデータフレームなし	なし
0x300	70	下位16ビットMAC付与	走行中、駐車中
...	...	...	...

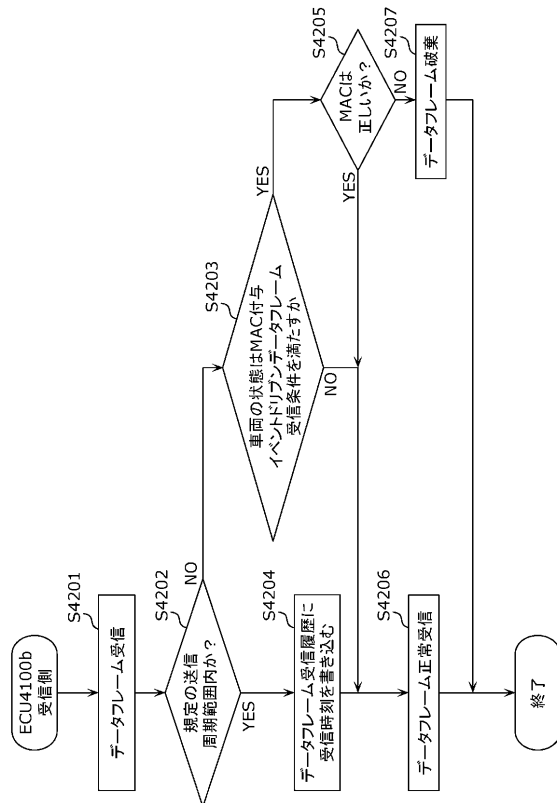
【図 2 9】

車両の状態
走行中

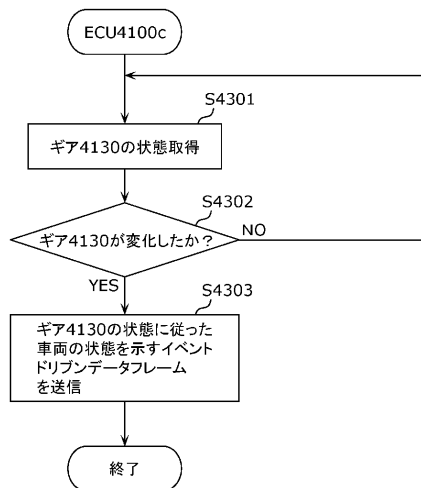
【図 30】



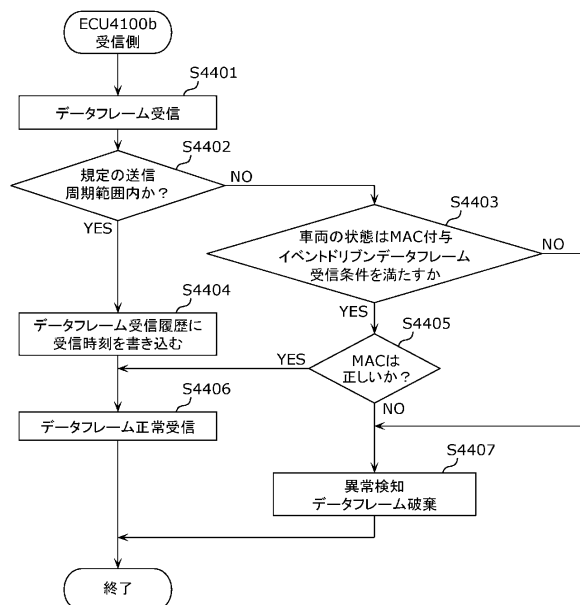
【図 31】



【図 32】



【図 33】



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 岸川 剛
大阪府門真市大字門真1006番地 パナソニック株式会社内
- (72)発明者 松島 秀樹
大阪府門真市大字門真1006番地 パナソニック株式会社内
- (72)発明者 芳賀 智之
大阪府門真市大字門真1006番地 パナソニック株式会社内
- (72)発明者 前田 学
大阪府門真市大字門真1006番地 パナソニック株式会社内
- (72)発明者 海上 勇二
大阪府門真市大字門真1006番地 パナソニック株式会社内
- (72)発明者 氏家 良浩
大阪府門真市大字門真1006番地 パナソニック株式会社内

審査官 金木 陽一

- (56)参考文献 特開2013-065689 (JP, A)
特開2013-017140 (JP, A)
MUTER, M. et al., A structured approach to anomaly detection for in-vehicle networks, Proceedings of 2010 Sixth International Conference on Information Assurance and Security (IAS), IEEE [online], 2010年, pp. 92-98, [retrieved on 2015-06-24.] Retrieved from the Internet, URL, <https://doi.org/10.1109/ISIAS.2010.5604050>

- (58)調査した分野(Int.Cl., DB名)
- | | |
|------|-------|
| H04L | 9/32 |
| G06F | 21/44 |
| H04L | 9/36 |