(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2017-139530
(P2017-139530A)
(43)公開日　平成29年8月10日(2017.8.10)

| (51)Int.Cl. | | | F I | | | テーマコード（参考） |
|---|---|---|---|---|---|---|
| H04L | 9/32 | (2006.01) | H04L | 9/00 | 675A | 5J104 |
| G09C | 1/00 | (2006.01) | G09C | 1/00 | 640D | 5K033 |
| H04L | 12/28 | (2006.01) | H04L | 12/28 | 200Z | |
| B60R | 16/023 | (2006.01) | B60R | 16/023 | P | |

審査請求 未請求　請求項の数 1　ＯＬ　（全 12 頁）

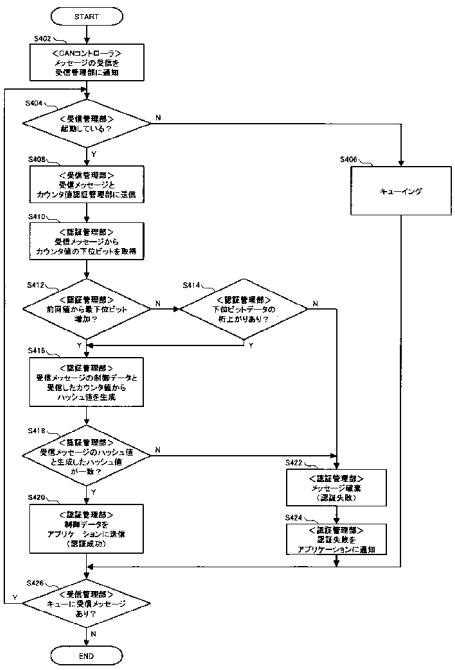
(21)出願番号　特願2016-17496(P2016-17496)
(22)出願日　平成28年2月1日(2016.2.1)

(71)出願人　000003207
トヨタ自動車株式会社
愛知県豊田市トヨタ町１番地
(74)代理人　100107766
弁理士　伊東　忠重
(74)代理人　100070150
弁理士　伊東　忠彦
(72)発明者　坂野　将秀
愛知県豊田市トヨタ町１番地　トヨタ自動車株式会社内

Ｆターム(参考)　5J104 AA08 LA01 NA11 NA38 PA07
5K033 AA05 BA06 CA07 DA13

(54)【発明の名称】通信システム

(57)【要約】　（修正有）
【課題】送信ノード或いは受信ノードにリセット等が発生し、送信ノードと受信ノードの双方で保持されるカウンタ値が異なる状況になっても、受信ノードが送信ノードから送信されるメッセージの認証を適切に行うことが可能なＣＡＮ通信システムを提供する。
【解決手段】マスタノードは、送信ノードからメッセージが送信される度に所定の規則に従いカウンタ値を更新すると共に、送信ノード及び受信ノードにカウンタ値を送信する。送信ノードは、起動後、カウンタ値をマスタノードから受信するまでの間、カウンタ値に基づく第１認証用データの生成とメインデータ及び第１認証用データの受信ノードへの送信を停止する。受信ノードは、起動後、カウンタ値をマスタノードから受信するまでの間、カウンタ値に基づく第２認証用データの生成と、送信ノードから受信する第１認証用データと第２認証用データとの比較による受信メッセージの認証を停止する。
【選択図】図６



【特許請求の範囲】
【請求項１】
マスタノード、送信ノード、及び受信ノードがバスで接続されるＣＡＮ通信システムであって、
前記マスタノードは、前記送信ノードからメッセージが送信される度に所定の規則に従いカウンタ値を更新すると共に、前記送信ノード及び前記受信ノードに前記カウンタ値を送信し、
前記送信ノードは、前記マスタノードから前記カウンタ値を受信する第１カウンタ値受信部と、前記受信ノードへの送信対象であるメインデータと前記第１カウンタ値受信部が受信したカウンタ値に基づき、第１認証用データを生成する第１生成部と、前記メインデータ及び前記第１認証用データを前記受信ノードに送信するデータ送信部と、前記送信ノードが起動してから前記第１カウンタ値受信部が前記カウンタ値を前記マスタノードから受信するまでの間、前記第１生成部及び前記データ送信部による処理を停止させる第１停止部と、を含み、
前記受信ノードは、前記送信ノードから前記メインデータ及び前記第１認証用データを受信するデータ受信部と、前記マスタノードから前記カウンタ値を受信する第２カウンタ値受信部と、前記データ受信部が受信した前記メインデータと前記第２カウンタ値受信部が受信した前記カウンタ値に基づき、第２認証用データを生成する第２生成部と、前記データ受信部が受信した前記第１認証用データと前記第２生成部が生成した前記第２認証用データの比較により、前記メインデータを含むメッセージの正当性を認証する認証部と、前記受信ノードが起動してから前記第２カウンタ値受信部が前記カウンタ値を前記マスタノードから受信するまでの間、前記第２生成部及び前記認証部による処理を停止させる第２停止部と、を含む、
ＣＡＮ通信システム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、ＣＡＮ（Controller Area Network）通信システムに関する。
【背景技術】
【０００２】
従来、メインメッセージと、メインメッセージに対応する認証用データ（例えば、ＭＡＣ：Message Authentication Code）を生成して受信ノードに送信する送信ノードと、受信したメインメッセージに対応する認証用データを生成する受信ノードを含むＣＡＮ通信システムが知られている（例えば、特許文献１等参照）。
【０００３】
特許文献１では、送信ノードと受信ノードの双方が共通するカウンタ値を記憶し、送信ノードは、メインメッセージと自身が記憶するカウンタ値に所定のアルゴリズムを適用してＭＡＣを生成して受信ノードに送信する。そして、受信ノードは、受信したメインメッセージと自身が記憶するカウンタ値に同様のアルゴリズムを適用してＭＡＣを生成して、受信したＭＡＣと比較することにより、メインメッセージの正当性を認証する。
【先行技術文献】
【特許文献】
【０００４】
【特許文献１】国際公開２０１３／０６５６８９号
【発明の概要】
【発明が解決しようとする課題】
【０００５】
しかしながら、特許文献１に開示される技術では、例えば、受信ノード或いは送信ノードが何等かの理由でリセットされると、送信ノードと受信ノードとの間で共通のカウンタ値にならない可能性がある。そのため、受信ノードは、受信メッセージの誤認証を行って

しまう可能性がある。

【０００６】

一方、送信ノードから受信ノードにカウンタ値を送信して、受信ノードは、送信ノードから受信したカウンタ値を用いて認証用データを生成することも可能である。しかしながら、例えば、車両に搭載されるＣＡＮ通信装置では、車両寿命を勘案すると、カウンタ値のデータサイズとして１２８ビット程度が必要とされるのに対して、ＣＡＮメッセージのデータフィールドは、最大８バイト（６４ビット）である。そのため、送信ノードは、フルサイズのカウンタ値を受信ノードに送信することができない可能性がある。

【０００７】

そこで、上記課題に鑑み、送信ノード或いは受信ノードにリセット等が発生し、送信ノードと受信ノードの双方で保持されるカウンタ値が異なる状況になっても、受信ノードが送信ノードから送信されるメッセージの認証を適切に行うことが可能なＣＡＮ通信システム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】

【０００８】

上記目的を達成するため、本発明の一実施態様において、

マスタノード、送信ノード、及び受信ノードがバスで接続されるＣＡＮ通信システムであって、

前記マスタノードは、前記送信ノードからメッセージが送信される度に所定の規則に従いカウンタ値を更新すると共に、前記送信ノード及び前記受信ノードに前記カウンタ値を送信し、

前記送信ノードは、前記マスタノードから前記カウンタ値を受信する第１カウンタ値受信部と、前記受信ノードへの送信対象であるメインデータと前記第１カウンタ値受信部が受信したカウンタ値に基づき、第１認証用データを生成する第１生成部と、前記メインデータ及び前記第１認証用データを前記受信ノードに送信するデータ送信部と、前記送信ノードが起動してから前記第１カウンタ値受信部が前記カウンタ値を前記マスタノードから受信するまでの間、前記第１生成部及び前記データ送信部による処理を停止させる第１停止部と、を含み、

前記受信ノードは、前記送信ノードから前記メインデータ及び前記第１認証用データを受信するデータ受信部と、前記マスタノードから前記カウンタ値を受信する第２カウンタ値受信部と、前記データ受信部が受信した前記メインデータと前記第２カウンタ値受信部が受信した前記カウンタ値に基づき、第２認証用データを生成する第２生成部と、前記データ受信部が受信した前記第１認証用データと前記第２生成部が生成した前記第２認証用データの比較により、前記メインデータを含むメッセージの正当性を認証する認証部と、前記受信ノードが起動してから前記第２カウンタ値受信部が前記カウンタ値を前記マスタノードから受信するまでの間、前記第２生成部及び前記認証部による処理を停止させる第２停止部と、を含む、

ＣＡＮ通信システムが提供される。

【０００９】

本発明の一実施態様によれば、ＣＡＮ通信装置のマスタノードは、送信ノードからメッセージが送信される度に所定の規則に従いカウンタ値を更新すると共に、送信ノード及び受信ノードにカウンタ値を送信する。そして、ＣＡＮ通信装置の送信ノードは、送信ノードが起動してから第１カウンタ値受信部がカウンタ値を受信するまでの間、第１生成部及びデータ送信部による処理を停止させる第１停止部を含む。従って、何等かの理由で送信ノードがリセットされた場合、送信ノードが再起動した後、マスタノードから最新のカウンタ値を受信するまで、カウンタ値に基づく第１認証用データの生成や、メインデータ及び第１認証用データの送信が行われない。即ち、送信ノードのリセットにより、送信ノードが保持するカウンタ値が不定値等になり、受信ノードが保持するカウンタ値と異なるような事態が発生しても、マスタノードから最新のカウンタ値を受信しない限り、カウンタ値に基づく第１認証用データの生成やメインデータ及び第１認証用データの送信が行われ

ない。そのため、送信ノードにおいて、受信ノードが保持するものと異なるカウンタ値に基づく第１認証用データが受信ノードに送信されることがなくなり、受信ノードにおける誤った第１認証用データに基づくメッセージの誤認証を抑制することができる。

【００１０】

また、受信ノードは、受信ノードが起動してから第２カウンタ値受信部がカウンタ値を受信するまでの間、第２生成部及び認証部による処理を停止させる第２停止部を含む。従って、何等かの理由で受信ノードがリセット等された場合、受信ノードが再起動した後、マスタノードから最新のカウンタ値を受信するまで、カウンタ値に基づく第２認証用データの生成や、送信ノードから受信する第１認証用データと第２認証用データとの比較によるメインデータを含むメッセージの正当性の認証が行われない。即ち、受信ノードのリセット等により、受信ノードが保持するカウンタ値が不定値等になり、送信ノードが保持するカウンタ値と異なるような事態が発生しても、マスタノードから最新のカウンタ値を受信しない限り、カウンタ値に基づく第２認証用データの生成や、送信ノードから受信する第１認証用データと第２認証用データとの比較によるメインデータを含むメッセージの正当性の認証が行われない。そのため、受信ノードにおいて、送信ノードが保持するものと異なるカウンタ値に基づく第２認証用データが生成されないようにすることができ、誤った第２認証用データに基づくメッセージの誤認証を抑制することができる。

【発明の効果】

【００１１】

送信ノード或いは受信ノードにリセット等が発生し、送信ノードと受信ノードの双方で保持されるカウンタ値が異なる状況になっても、受信ノードが送信ノードから送信されるメッセージの認証を適切に行うことが可能なＣＡＮ通信システムを提供することができる。

【図面の簡単な説明】

【００１２】

【図１】ＣＡＮ通信システムの構成の一例を概略的に示す構成図である。

【図２】ＥＣＵの構成の一例を概略的に示すブロック図である。

【図３】ＥＣＵの起動時における処理の一例を概略的に示すフローチャートである。

【図４】ＥＣＵの停止時における処理の一例を概略的に示すフローチャートである。

【図５】ＥＣＵにおけるメッセージの送信処理の一例を概略的に示すフローチャートである。

【図６】ＥＣＵにおけるメッセージの受信処理の一例を概略的に示すフローチャートである。

【発明を実施するための形態】

【００１３】

図１は、本実施形態に係るＣＡＮ通信システム（以下、単に「通信システム」と称する）１の構成の一例を概略的に示す構成図である。

【００１４】

通信システム１は、例えば、車両に搭載され、バス２に接続される複数のＥＣＵ（Electrical Control Unit）１０と、マスタＥＣＵ２０とを含む。

【００１５】

ＥＣＵ１０は、予め割り当てられた機能を実現するための各種制御処理を行う電子制御ユニットである。各ＥＣＵ１０は、バス２を通じて、他のＥＣＵ１０との間で、ＣＡＮプロトコルに基づくＣＡＮメッセージ（以下、単に「メッセージ」と称する）の送受信を行う。即ち、各ＥＣＵ１０は、通信システム１における送信ノードの一例であり、受信ノードの一例でもある。

【００１６】

マスタＥＣＵ２０は、ＥＣＵ１０（即ち、送信ノード）の何れかがバス２を通じて他のＥＣＵ１０（即ち、受信ノード）にメッセージを送信する度、即ち、ＥＣＵ１０の何れかがメッセージをバス２上に出力する度に、所定の規則に従いカウンタ値Ｃｔを更新する処

理を行う。所定の規則は、例えば、"メッセージが送信される度に、カウンタ値Ｃｔを所定値（例えば、"１"）だけインクリメントすること"や"メッセージが送信される度に、カウンタ値Ｃｔを所定値（例えば、"１"）だけデクリメントすること"等、任意であってよい。以下、カウンタ値Ｃｔは、所定の規則に従い、単調増加することを前提に説明を続ける。マスタＥＣＵ２０は、所定時間毎に、最新のカウンタ値Ｃｔをバス２に出力して、各ＥＣＵ１０に送信する。

【００１７】

尚、本実施形態におけるマスタＥＣＵ２０は、バス２に含まれるバス２ａとバス２ｂとの間で送受信されるメッセージの中継を行う機能を果たす。即ち、マスタＥＣＵ２０は、ゲートウェイ装置（ゲートウェイＥＣＵ）である。

【００１８】

次に、図２を参照して、ＥＣＵ１０の構成について説明する。

【００１９】

図２は、本実施形態に係るＥＣＵ１０の構成の一例を概略的に示すブロック図である。ＥＣＵ１０は、アプリケーション１０１、送信管理部１０２、受信管理部１０３、認証管理部１０４、メッセージボックス（ＭＢＯＸ）１０５，１０６、ＣＡＮコントローラ１０７、ＣＡＮトランシーバ１０８を含む。

【００２０】

アプリケーション１０１は、ＥＣＵ１０内のＣＰＵ（不図示）上で実行され、各ＥＣＵ１０に割り当てられる任意の機能を実現するための各種制御処理を行うプログラムである。アプリケーション１０１は、予め規定された条件等に応じて、演算結果（以下、「制御データ（受信ノードである他のＥＣＵ１０への送信対象であるメインデータの一例）」と称する）を他のＥＣＵ１０に送信するため、送信管理部１０２に送信要求を出力する。

【００２１】

送信管理部１０２は、マスタＥＣＵ２０から送信され、ＣＡＮコントローラ１０７がＣＡＮトランシーバ１０８を介してバス２から受信したカウンタ値ＣｔをＭＢＯＸ１０５から取得する。また、送信管理部１０２は、起動している間、アプリケーション１０１からの制御データを含む送信要求と、ＭＢＯＸ１０５から取得したカウンタ値Ｃｔを認証管理部１０４に送信する。一方、送信管理部１０２は、停止している間、アプリケーション１０１からの制御データを含む送信要求と、ＭＢＯＸ１０５から取得したカウンタ値Ｃｔを認証管理部１０４に送信せず、アプリケーション１０１からの送信要求をキューイング或いは破棄する。

【００２２】

尚、送信管理部１０２が"起動している"状態は、アプリケーション１０１からの制御データを含む送信要求と、ＭＢＯＸ１０５から取得したカウンタ値Ｃｔを認証管理部１０４に送信する機能が実行可能な状態になっていることを表す。即ち、ＥＣＵ１０が起動していれば、送信管理部１０２が起動していない場合でも、送信管理部１０２は、他の機能（送信要求の有無を判断する機能や送信要求をキューイング或いは破棄したりする機能等）を実行可能である。

【００２３】

受信管理部１０３は、マスタＥＣＵ２０から送信され、ＣＡＮコントローラ１０７がＣＡＮトランシーバ１０８を介してバス２から受信したカウンタ値ＣｔをＭＢＯＸ１０５から取得する。また、受信管理部１０３は、ＣＡＮコントローラ１０７がＣＡＮトランシーバ１０８を介してバス２から受信した制御データを含むメッセージ（以下、「受信メッセージ」と称する）をＭＢＯＸ１０６から取得する。また、受信管理部１０３は、起動している間、ＭＢＯＸ１０６から取得した受信メッセージと、ＭＢＯＸ１０５から取得したカウンタ値Ｃｔを認証管理部１０４に送信する。一方、受信管理部１０３は、停止している間、ＭＢＯＸ１０６から取得した受信メッセージと、ＭＢＯＸ１０５から取得したカウンタ値Ｃｔを認証管理部１０４に送信せず、受信メッセージをキューイング或いは破棄する。

【００２４】
尚、受信管理部１０３が"起動している"状態は、ＭＢＯＸ１０６から取得した受信メッセージと、ＭＢＯＸ１０５から取得したカウンタ値Ｃｔを認証管理部１０４に送信する機能が実行可能な状態になっていることを表す。即ち、ＥＣＵ１０が起動していれば、受信管理部１０３が起動していない場合でも、受信管理部１０３は、他の機能（受信メッセージの有無を判断する機能や受信メッセージをキューイング或いは破棄したりする機能等）を実行可能である。
【００２５】
ここで、図３、図４を参照して、ＥＣＵ１０の起動／停止に伴う、送信管理部１０２、受信管理部１０３の起動／停止動作について説明する。
【００２６】
図３は、ＥＣＵ１０の起動時における処理の一例を概略的に示すフローチャートである。図４は、ＥＣＵ１０の停止時における処理の一例を概略的に示すフローチャートである。図３に示すフローチャートによる処理は、起動要求（起動信号）がＥＣＵ１０に入力されると実行される。また、図４に示すフローチャートによる処理は、停止要求（停止信号）がＥＣＵ１０に入力されると実行される。
【００２７】
図３を参照するに、ステップＳ１０２にて、ＥＣＵ１０は起動する。
【００２８】
ステップＳ１０４にて、ＥＣＵ１０は、送信管理部１０２及び受信管理部１０３が停止しているか否かを判定する。ＥＣＵ１０は、送信管理部１０２及び受信管理部１０３が停止している場合、ステップＳ１０８に進み、停止していない場合、ステップＳ１０６に進む。
【００２９】
ステップＳ１０６にて、ＥＣＵ１０は、送信管理部１０２及び受信管理部１０３を停止させて、ステップＳ１０８に進む。
【００３０】
ステップＳ１０８にて、ＥＣＵ１０は、送信管理部１０２及び受信管理部１０３の初期化を行う。
【００３１】
ステップＳ１１０にて、ＥＣＵ１０は、ＥＣＵ１０の起動後、ＣＡＮコントローラ１０７がＣＡＮトランシーバ１０８を介してマスタＥＣＵ２０からカウンタ値Ｃｔを受信したか否かを判定する。ＥＣＵ１０は、マスタＥＣＵ２０からカウンタ値Ｃｔを受信している場合、ステップＳ１１２に進み、マスタＥＣＵ２０からカウンタ値Ｃｔを受信していない場合、ステップＳ１１０の処理を繰り返す。
【００３２】
ステップＳ１１２にて、ＥＣＵ１０は、送信管理部１０２及び受信管理部１０３を起動し、今回の処理を終了する。
【００３３】
また、図４を参照するに、ステップＳ２０２にて、ＥＣＵ１０は。送信管理部１０２及び受信管理部１０３を停止させる。
【００３４】
そして、ステップＳ２０４にて、ＥＣＵ１０は、停止し、今回の処理を終了する。
【００３５】
このように、送信管理部１０２及び受信管理部１０３は、ＥＣＵ１０の停止に伴い、停止し、ＥＣＵ１０の起動した後、ＣＡＮコントローラ１０７がＣＡＮトランシーバ１０８を介してマスタＥＣＵ２０から送信されたカウンタ値Ｃｔを受信すると、起動する。即ち、送信管理部１０２及び受信管理部１０３は、ＥＣＵ１０が起動してから、マスタＥＣＵ２０からのカウンタ値を受信するまで、停止している。
【００３６】

図２に戻り、認証管理部１０４は、制御データを含むメッセージ（以下、送信メッセージと称する）を他のＥＣＵ１０に送信する際、他のＥＣＵ１０で実行されるメッセージ認証のための認証用データ（以下、「第１認証用データ」と称する）を生成する。具体的には、認証管理部１０４は、送信管理部１０２から取得した制御データ及びカウンタ値Ｃｔに基づき、第１認証用データを生成する。より具体的には、認証管理部１０４は、制御データとカウンタ値Ｃｔを結合したデータに対して、所定のアルゴリズム（例えば、一方向ハッシュ関数等）を適用することにより、第１認証用データ（例えば、ハッシュ値）を生成する。以下、第１認証用データは、制御データとカウンタ値Ｃｔを結合したデータに対して、一方向ハッシュ関数を適用して生成されるハッシュ値である前提で説明を継続する。そして、認証管理部１０４は、制御データ、カウンタ値Ｃｔの下位ビットデータ（カウンタ値Ｃｔの最下位ビットから予め規定された数桁分のデータ。以下、単に「下位ビットデータ」と称する）、及び第１認証用データ（ハッシュ値）を含む送信メッセージを生成する。具体的には、認証管理部１０４は、ＣＡＮメッセージのデータフィールドの最大６４ビットのデータサイズに収まるように、制御データ、下位ビットデータ、及びハッシュ値を含む送信メッセージを生成する。

【００３７】

また、認証管理部１０４は、メッセージを他のＥＣＵ１０から受信した際、受信メッセージに含まれる下位ビットデータと、例えば、ＲＡＭ上の所定領域等に保持するカウンタ値Ｃｔの前回値（最新値の１つ前のカウンタ値Ｃｔ。以下、単に「前回値」と称する）との比較により、受信メッセージの正当性を認証する（第１認証）。具体的には、認証管理部１０４は、受信メッセージに含まれる下位ビットデータと前回値との比較により、受信メッセージに含まれる下位ビットデータが所定の規則に従っている（即ち、前回値から単調増加している）と判断した場合、第１認証を成功とする。また、認証管理部１０４は、第１認証に成功した場合、受信メッセージに含まれる第１認証用データとの比較により、受信メッセージの正当性を認証するための認証用データ（以下、「第２認証用データ」と称する）を生成する。具体的には、認証管理部１０４は、受信管理部１０３から取得した受信メッセージに含まれる制御データと、受信管理部１０３から取得したカウンタ値Ｃｔに基づき、第２認証用データを生成する。より具体的には、認証管理部１０４は、受信メッセージに含まれる制御データ及びマスタＥＣＵ２０から送信された最新のカウンタ値Ｃｔを結合したデータに対して、第１認証用データを生成する際と同様のアルゴリズム、即ち、一方向ハッシュ関数を適用することにより、第２認証用データ（ハッシュ値）を生成する。そして、認証管理部１０４は、受信メッセージに含まれる第１認証用データ（ハッシュ値）と生成した第２認証用データ（ハッシュ値）を比較し、一致する場合、受信メッセージの正当性を認証する（第２認証）。即ち、認証管理部１０４は、第１認証と第２認証の双方に成功した場合、受信メッセージの正当性を認証する。

【００３８】

ＭＢＯＸ１０５は、マスタＥＣＵ２０から送信され、ＣＡＮコントローラ１０７がＣＡＮトランシーバ１０８を介して受信するカウンタ値Ｃｔを含むメッセージを格納する記憶領域である。

【００３９】

ＭＢＯＸ１０６は、他のＥＣＵ１０から送信され、ＣＡＮコントローラ１０７がＣＡＮトランシーバ１０８を介してバス２から受信する制御データを含むメッセージ（受信メッセージ）を格納する記憶領域である。

【００４０】

ＣＡＮコントローラ１０７は、プロトコルコントローラや、ＣＰＵクロックを分周する分周器、レジスタ等を備え、ＣＡＮトランシーバ１０８を介して、バス２（バス２ａ或いはバス２ｂ）との間でメッセージを送受信する。

【００４１】

ＣＡＮトランシーバ１０８は、ＣＡＮコントローラ１０７から取得した送信メッセージを作動電圧に変換してバス２に出力する。また、ＣＡＮトランシーバ１０８は、バス２か

らメッセージを取得する際、バス２の作動電圧を読み取り、所定の電圧範囲に含まれるように整形した受信信号をＣＡＮコントローラ１０７に出力する。

【００４２】

次に、図５、図６を参照して、ＥＣＵ１０によるメッセージの送信処理及び受信処理について説明する。

【００４３】

図５は、ＥＣＵ１０におけるメッセージの送信処理の一例を概略的に示すフローチャートである。図６は、ＥＣＵ１０におけるメッセージの受信処理の一例を概略的に示すフローチャートである。図５に示すフローチャートは、ＣＰＵ上で実行されるアプリケーション１０１が送信対象である制御データを生成する度に実行される。図６に示すフローチャートは、ＣＡＮコントローラ１０７がＣＡＮトランシーバ１０８を介して他のＥＣＵ１０からの制御データを含むメッセージを受信する度に実行される。

【００４４】

図５を参照するに、ステップＳ３０２にて、アプリケーション１０１は、送信管理部１０２に制御データを含むメッセージの送信要求を送る。

【００４５】

ステップＳ３０４にて、送信管理部１０２は、起動しているか否か、即ち、アプリケーション１０１からの制御データを含む送信要求と、ＭＢＯＸ１０５から取得したカウンタ値Ｃｔを認証管理部１０４に送信する機能が実行可能な状態か否かを確認する。送信管理部１０２は、起動していない場合、ステップＳ３０６に進み、起動している場合、ステップＳ３０８に進む。

【００４６】

ステップＳ３０６にて、送信管理部１０２は、アプリケーション１０１からの送信要求をキューイングし、ステップＳ３１８に進む。

【００４７】

尚、本ステップにて、送信管理部１０２は、送信要求を破棄すると共に、その旨をアプリケーション１０１に通知してもよい。

【００４８】

一方、ステップＳ３０８にて、送信管理部１０２は、アプリケーション１０１からの制御データを含む送信要求と、ＭＢＯＸ１０５から取得したカウンタ値Ｃｔを認証管理部１０４に送信する。

【００４９】

ステップＳ３１０にて、認証管理部１０４は、送信管理部１０２から受信した制御データ及びカウンタ値Ｃｔからハッシュ値を生成する。

【００５０】

ステップＳ３１２にて、認証管理部１０４は、制御データ、下位ビットデータ、及びハッシュ値を含む送信メッセージを生成する。

【００５１】

ステップＳ３１４にて、認証管理部１０４は、作成した送信メッセージをＭＢＯＸ１０６に格納する。

【００５２】

ステップＳ３１６にて、ＣＡＮコントローラ１０７は、ＣＡＮトランシーバ１０８を介してＭＢＯＸ１０６に格納される送信メッセージをバス２に出力し、他のＥＣＵ１０に送信する。

【００５３】

ステップＳ３１８にて、送信管理部１０２は、キューに送信要求があるか否かを確認する。送信管理部１０２は、キューに送信要求がある場合、ステップＳ３０４に戻り、ステップＳ３０４～Ｓ３１８の処理を繰り返し、キューに送信要求がない場合、今回の処理を終了する。

【００５４】

また、図６を参照するに、ステップＳ４０２にて、ＣＡＮコントローラ１０７は、他のＥＣＵ１０から制御データを含むメッセージを受信した旨を受信管理部１０３に通知する。

【００５５】

ステップＳ４０４にて、受信管理部１０３は、起動しているか否か、即ち、ＭＢＯＸ１０６から取得した受信メッセージと、ＭＢＯＸ１０５から取得したカウンタ値Ｃｔを認証管理部１０４に送信する機能が実行可能な状態になっているか否かを確認する。受信管理部１０３は、起動していない場合、ステップＳ４０６に進み、起動している場合、ステップＳ４０８に進む。

【００５６】

ステップＳ４０６にて、受信管理部１０３は、受信メッセージをキューイングし、ステップＳ４２６に進む。

【００５７】

尚、本ステップにて、受信管理部１０３は、受信メッセージを破棄すると共に、その旨をアプリケーション１０１に通知してもよい。

【００５８】

一方、ステップＳ４０８にて、受信管理部１０３は、ＭＢＯＸ１０６から取得した受信メッセージと、ＭＢＯＸ１０５から取得したカウンタ値Ｃｔを認証管理部１０４に送る。

【００５９】

ステップＳ４１０にて、認証管理部１０４は、受信メッセージから下位ビットデータを取得する。

【００６０】

ステップＳ４１２にて、認証管理部１０４は、下位ビットデータと前回値の比較を行い、下位ビットデータの最下位ビットが前回値から増加しているか否かを確認する。認証管理部１０４は、最下位ビットが前回値から増加していない場合、ステップＳ４１４に進み、最下位ビットが前回値から増加している場合、カウンタ値Ｃｔが所定の規則に従い単調増加している、即ち、第１認証の成功と判断し、ステップＳ４１６に進む。

【００６１】

ステップＳ４１４にて、認証管理部１０４は、下位ビットデータの桁上がりがあるか否かを確認する。認証管理部１０４は、下位ビットデータの桁上がりがある場合、カウンタ値Ｃｔが所定の規則に従い単調増加している、即ち、第１認証の成功と判断し、ステップＳ４１６に進み、下位ビットデータの桁上がりがない場合、第１認証の失敗と判断し、ステップＳ４２２に進む。

【００６２】

尚、ＥＣＵ１０にリセットが発生し、前回値が保持されていない場合、認証管理部１０４は、ＭＢＯＸ１０５から取得した最新のカウンタ値Ｃｔから所定の規則に従い、前回値を生成し、生成した前回値を用いて、ステップＳ４１２、Ｓ４１４の処理を実行する。

【００６３】

ステップＳ４１６にて、認証管理部１０４は、受信管理部１０３から取得した受信メッセージに含まれる制御データと、受信管理部１０３から取得したカウンタ値Ｃｔからハッシュ値を生成する。

【００６４】

ステップＳ４１８にて、認証管理部１０４は、受信メッセージから取得したハッシュ値と、ステップＳ４１６で生成したハッシュ値を比較し、一致するか否かを判定する。認証管理部１０４は、一致する場合、第２認証の成功と判断し、ステップＳ４２０に進み、一致しない場合、第２認証の失敗と判断し、ステップＳ４２２に進む。

【００６５】

ステップＳ４２０にて、認証管理部１０４は、受信メッセージの正当性を認証し、受信メッセージに含まれる制御データをアプリケーション１０１に送る（認証成功）。

【００６６】

一方、ステップＳ４２２にて、認証管理部１０４は、受信メッセージの正当性を認証せず（認証失敗）、受信メッセージを破棄し、ステップＳ４２４に進む。

【００６７】

そして、ステップＳ４２４にて、認証管理部１０４は、受信メッセージの認証失敗をアプリケーション１０１に通知する。

【００６８】

ステップＳ４２６にて、受信管理部１０３は、キューに受信メッセージがあるか否かを確認する。受信管理部１０３は、キューに受信メッセージがある場合、ステップＳ４０４に戻り、ステップＳ４０４～Ｓ４２６の処理を繰り返し、キューに受信メッセージがない場合、今回の処理を終了する。

【００６９】

尚、本実施形態では、第１認証と第２認証の双方により、受信メッセージの正当性の認証を試みるが、第２認証だけで受信メッセージの正当性の認証を行ってもよい。

【００７０】

このように、本実施形態では、マスタＥＣＵ２０は、各ＥＣＵ１０からメッセージが送信される度に所定の規則に従いカウンタ値を更新すると共に、各ＥＣＵ１０にカウンタ値を送信する。そして、送信管理部１０２は、ＥＣＵ１０が起動してからカウンタ値をマスタＥＣＵ２０から受信するまでの間、アプリケーション１０１からの制御データを含む送信要求と、ＭＢＯＸ１０５から取得したカウンタ値Ｃｔを認証管理部１０４に送信する機能を停止する。換言すれば、送信管理部１０２は、認証管理部１０４による処理（即ち、カウンタ値Ｃｔに基づく第１認証用データを生成すると共に、制御データ、下位ビットデータ、及び第１認証用データを含む送信メッセージを生成する処理）及びＣＡＮコントローラ１０７による処理（即ち、制御データを含む送信メッセージを他のＥＣＵ１０に送信する処理）を停止させる。従って、何等かの理由でＥＣＵ１０がリセットされた場合、ＥＣＵ１０が再起動した後、マスタＥＣＵ２０から最新のカウンタ値Ｃｔを受信するまで、カウンタ値Ｃｔに基づく第１認証用データの生成や、制御データ、下位ビットデータ、及び第１認証用データを含む送信メッセージの送信が行われない。即ち、ＥＣＵ１０（送信ノード）のリセットにより、当該ＥＣＵ１０が保持するカウンタ値が不定値等になり、他のＥＣＵ１０（受信ノード）が保持するカウンタ値と異なるような事態が発生しても、マスタＥＣＵ２０から最新のカウンタ値を受信しない限り、カウンタ値Ｃｔに基づく第１認証用データの送信や制御データ、下位ビットデータ、及び第１認証用データを含む送信メッセージの送信が行われない。そのため、当該ＥＣＵ１０において、他のＥＣＵ１０が保持するものと異なるカウンタ値に基づく下位ビットデータや第１認証用データが他のＥＣＵ１０に送信されることがなくなり、他のＥＣＵ１０における誤った下位ビットデータや第１認証用データに基づく受信メッセージの誤認証を抑制することができる。

【００７１】

また、受信管理部１０３は、ＥＣＵ１０が起動してからカウンタ値をマスタＥＣＵ２０から受信するまでの間、ＭＢＯＸ１０６から取得した受信メッセージと、ＭＢＯＸ１０５から取得したカウンタ値Ｃｔを認証管理部１０４に送信する機能を停止する。換言すれば、受信管理部１０３は、ＥＣＵ１０が起動してからカウンタ値をマスタＥＣＵ２０から受信するまでの間、認証管理部１０４による処理（即ち、カウンタ値Ｃｔに基づく第２認証用データを生成すると共に、第１認証及び第２認証による受信メッセージの正当性を認証する処理）を停止させる。従って、何等かの理由でＥＣＵ１０がリセット等された場合、当該ＥＣＵ１０が再起動した後、マスタＥＣＵ２０から最新のカウンタ値を受信するまで、カウンタ値Ｃｔに基づく第２認証用データの生成や、下位ビットデータ及び第２認証用データに基づく制御データを含む受信メッセージの正当性の認証が行われない。即ち、ＥＣＵ１０（受信ノード）のリセット等により、当該ＥＣＵ１０が保持するカウンタ値が不定値等になり、他のＥＣＵ１０（送信ノード）が保持するカウンタ値と異なるような事態が発生しても、マスタＥＣＵ２０から最新のカウンタ値を受信しない限り、カウンタ値Ｃｔに基づく第２認証用データの生成や、下位ビットデータ及び第２認証用データに基づく

制御データを含む受信メッセージの正当性の認証が行われない。そのため、当該ＥＣＵ１０において、他のＥＣＵ１０が保持するものと異なるカウンタ値に基づく第２認証用データが生成されないようにすることができると共に、誤った下位ビットデータ及び第２認証用データに基づく受信メッセージの正当性の認証（第１認証及び第２認証）が行われることがなくなり、当該ＥＣＵ１０における受信メッセージの誤認証を抑制することができる。

【００７２】

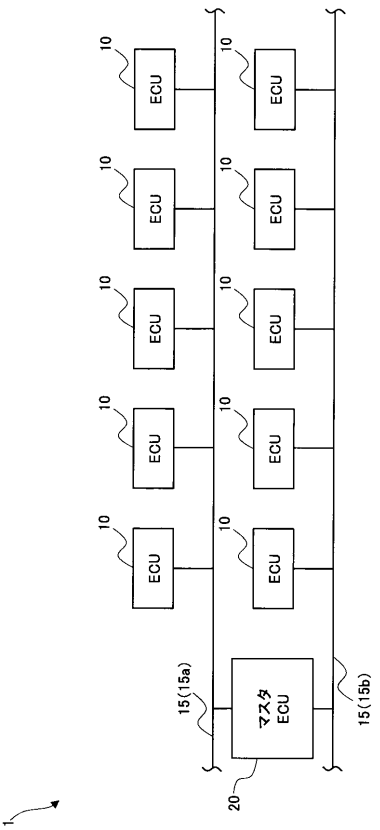
以上、本発明を実施するための形態について詳述したが、本発明はかかる特定の実施形態に限定されるものではなく、特許請求の範囲に記載された本発明の要旨の範囲内において、種々の変形・変更が可能である。

【符号の説明】

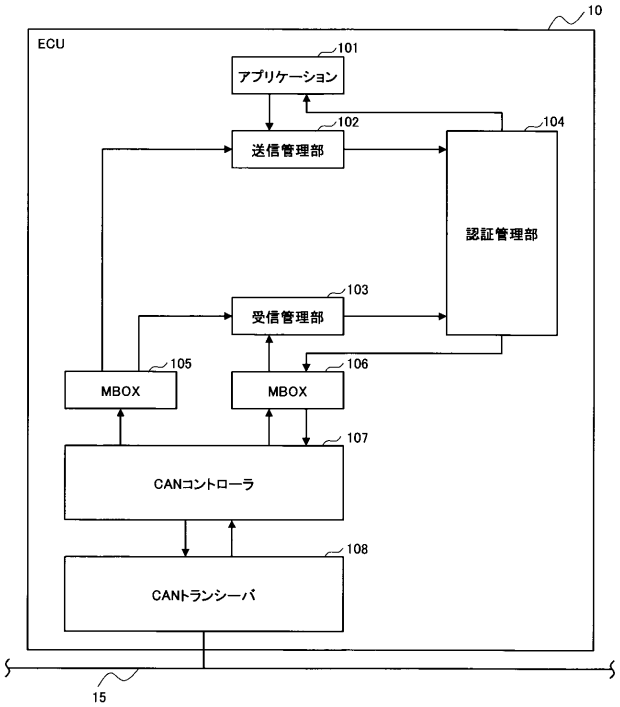
【００７３】

１　ＣＡＮ通信システム
２，２ａ，２ｂ　バス
１０　ＥＣＵ（送信ノード、受信ノード）
２０　マスタＥＣＵ（マスタノード）
１０１　アプリケーション
１０２　送信管理部（第１停止部）
１０３　受信管理部（第２停止部）
１０４　認証管理部（第１生成部、第２生成部、認証部）
１０５，１０６　メッセージボックス
１０７　ＣＡＮコントローラ（データ送信部、第１カウンタ値受信部、データ受信部、第２カウンタ値受信部）
１０８　ＣＡＮトランシーバ

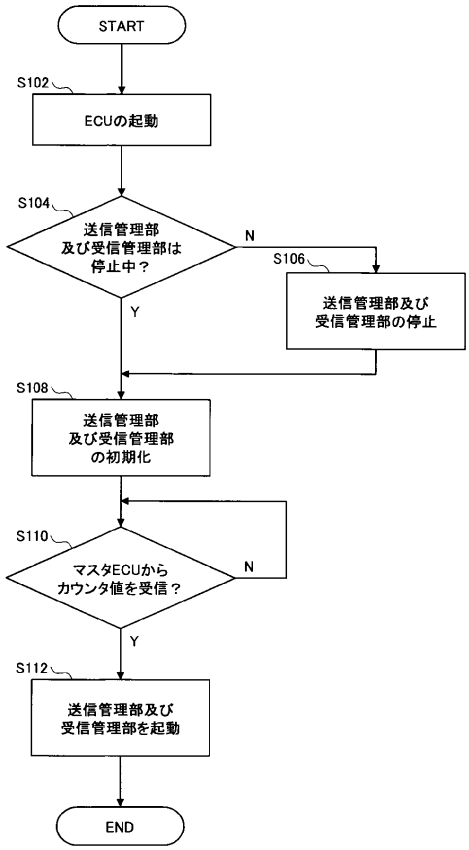
【図１】



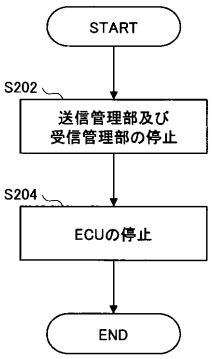

【図２】



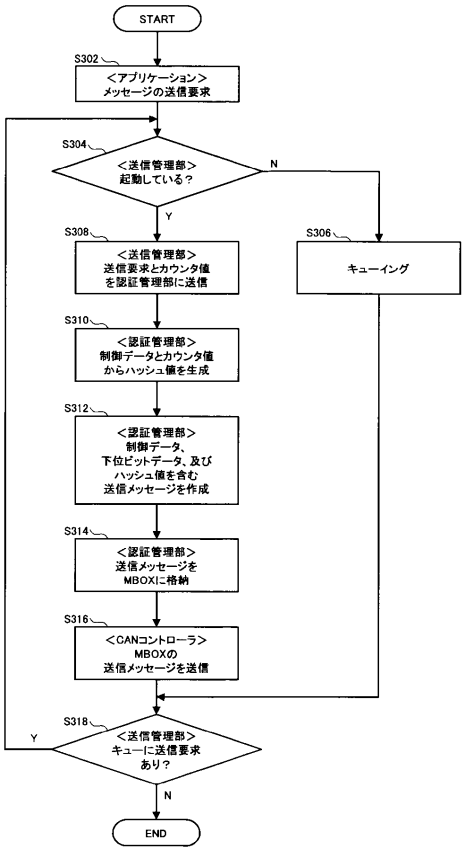
【図３】


START
S102
ECUの起動
S104
送信管理部
及び受信管理部は
停止中？
N
S106
送信管理部及び
受信管理部の停止
Y
S108
送信管理部
及び受信管理部
の初期化
S110
マスタECUから
カウンタ値を受信？
N
Y
S112
送信管理部及び
受信管理部を起動
END

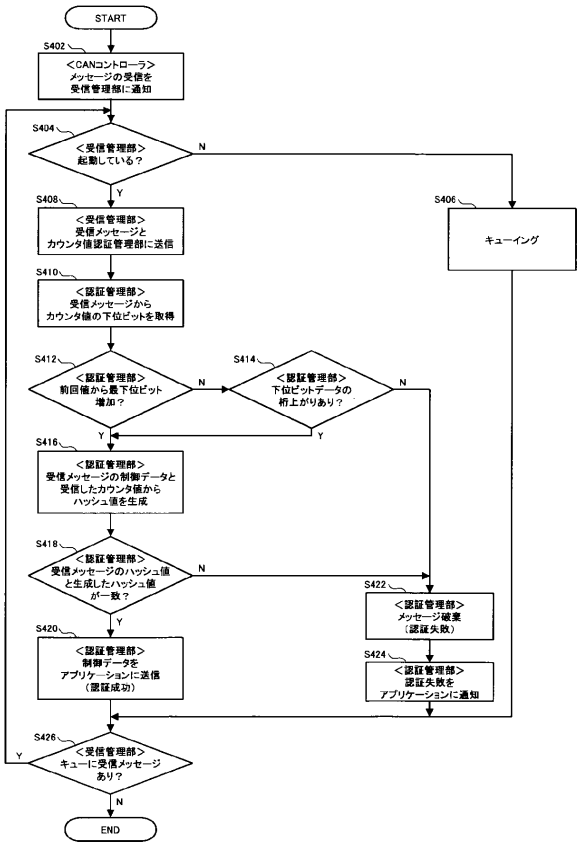
【図４】


START
S202
送信管理部及び
受信管理部の停止
S204
ECUの停止
END

【図５】


START
S302
＜アプリケーション＞
メッセージの送信要求
S304
＜送信管理部＞
起動している？
N
Y
S306
キューイング
S308
＜送信管理部＞
送信要求とカウンタ値
を認証管理部に送信
S310
＜認証管理部＞
制御データとカウンタ値
からハッシュ値を生成
S312
＜認証管理部＞
制御データ、
下位ビットデータ、及び
ハッシュ値を含む
送信メッセージを作成
S314
＜認証管理部＞
送信メッセージを
MBOXに格納
S316
＜CANコントローラ＞
MBOXの
送信メッセージを送信
S318
＜送信管理部＞
キューに送信要求
あり？
Y
N
END

【図６】


START
S402
＜CANコントローラ＞
メッセージの受信を
受信管理部に通知
S404
＜受信管理部＞
起動している？
N
Y
S406
キューイング
S408
＜受信管理部＞
受信メッセージと
カウンタ値認証管理部に送信
S410
＜認証管理部＞
受信メッセージから
カウンタ値の下位ビットを取得
S412
＜認証管理部＞
前回値から最下位ビット
増加？
N
S414
＜認証管理部＞
下位ビットデータの
桁上がりあり？
N
Y
Y
S416
＜認証管理部＞
受信メッセージの制御データと
受信したカウンタ値から
ハッシュ値を生成
S418
＜認証管理部＞
受信メッセージのハッシュ値
と生成したハッシュ値
が一致？
N
Y
S420
＜認証管理部＞
制御データを
アプリケーションに送信
（認証成功）
S422
＜認証管理部＞
メッセージ破棄
（認証失敗）
S424
＜認証管理部＞
認証失敗を
アプリケーションに通知
S426
＜受信管理部＞
キューに受信メッセージ
あり？
Y
N
END