

(12) 特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2020年3月12日(12.03.2020)



(10) 国際公開番号

WO 2020/049698 A1

(51) 国際特許分類:
H04L 1/00 (2006.01)

(21) 国際出願番号: PCT/JP2018/033097

(22) 国際出願日: 2018年9月6日(06.09.2018)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(71) 出願人: 三菱電機株式会社(MITSUBISHI ELECTRIC CORPORATION) [JP/JP]; 〒1008310 東京都千代田区丸の内二丁目7番3号 Tokyo (JP).

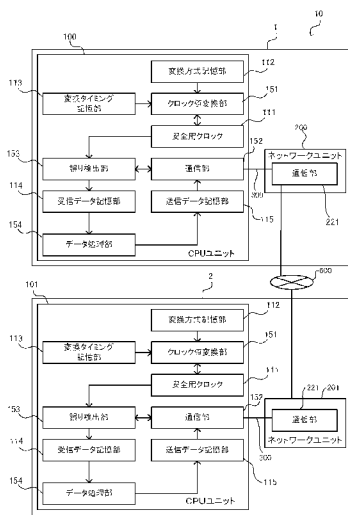
(72) 発明者: 伊藤 直輝(ITO Naoki); 〒1008310 東京都千代田区丸の内二丁目7番3号 三菱電機株式会社内 Tokyo (JP).

(74) 代理人: 木村 満(KIMURA Mitsuru); 〒1010054 東京都千代田区神田錦町二丁目7番地 協販ビル2階 Tokyo (JP).

(81) 指定国(表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(54) Title: COMMUNICATION SYSTEM, COMMUNICATION DEVICE, METHOD, AND PROGRAM

(54) 発明の名称: 通信システム、通信装置、方法及びプログラム



100, 101 CPU unit
111 Safety clock
112 Conversion scheme storage part
113 Conversion timing storage part
114 Reception data storage unit
115 Transmission data storage unit
151 Clock value conversion part
152, 221 Communication part
153 Error detection part
154 Data processing part
200, 201 Network unit

(57) Abstract: A clock value conversion part (151) of a CPU unit (100) replaces the carry counter value of a safety clock (111) of the CPU unit (100) and disperses the value of the carry counter. The CPU unit (100) transmits a frame including a timestamp value and a first error detection code generated from the timestamp value and the carry counter value to a CPU unit (101). A clock value conversion part (151) of the CPU unit (101) disperses the carry counter value of a safety clock (111) of the CPU unit (101) the same way as does the CPU unit (100). An error detection part (153) of the CPU unit (101) determines whether a second error detection code generated from the received timestamp value and the carry counter value of the safety clock (111) of the CPU unit (101) satisfies a condition set for the first error detection code.

(57) 要約: CPUユニット(100)のクロック値変換部(151)は、CPUユニット(100)の安全用クロック(111)のキャリアカウンタの値を置き換えて、キャリアカウンタが取る値を分散させる。CPUユニット(100)は、タイムスタンプの値と、タイムスタンプの値とキャリアカウンタの値とから生成された第1誤り検出符号と、を含むフレームをCPUユニット(101)に送信する。CPUユニット(101)のクロック値変換部(151)は、CPUユニット(100)と同様に、CPUユニット(101)の安全用クロック(111)のキャリアカウンタの値を分散させる。CPUユニット(101)の誤り検出部(153)は、受信したタイムスタンプの値とCPUユニット(101)の安全用クロック(111)のキャリアカウンタの値とから生成した第2誤り検出符号が、第1誤り検出符号に対して設定された条件を満たすか否かを判別する。

(84) 指定国(表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, RU, TJ, TM), ヨーロッパ (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

添付公開書類:

一 国際調査報告 (条約第21条(3))

明 細 書

発明の名称：通信システム、通信装置、方法及びプログラム

技術分野

[0001] 本発明は、通信システム、通信装置、方法及びプログラムに関する。

背景技術

[0002] ファクトリーオートメーションの分野では、機能安全の観点から通信の信頼性を高めることが要望されている。ここで、機能安全とは、安全を確保する機能を導入して、実現される許容可能なレベルの安全のことである。

[0003] 通信の信頼性の向上のためリアルタイム性が要望されている。工場内の装置間では、安全制御に関する情報が送受信される。安全制御に関する情報は、例えば、非常停止スイッチが押されたことの通知、非常停止のため電源遮断の指示等を含む。このような安全制御に関する情報は、遅延することなく宛先の装置に到達する必要がある。

[0004] データの遅延を検出するため、例えば、工場内の装置が、送信時刻を示す時間情報を付加したデータを他の装置に送信する。データを受信した他の装置は、受信した時間情報から、そのデータが適正な時間内に届いたものであるかを判別する。特許文献1には、送信側の通信装置が時間情報を付与したデータを送信し、受信側の通信装置が、受信した時間情報と受信側の通信装置が有するクロックが示す時間情報とを比較することが記載されている。

[0005] ここで、従来のクロックは、例えば、設定された時間毎にクロック信号を発生するクロック発生回路と、クロック発生回路が出力したクロック信号の数をカウントするカウンタとを含む。図4 Aに従来のカウンタの構成の一例を示す。図示する例では、カウンタは、クロック信号の数を数えるカウンタであるタイムスタンプ11と、タイムスタンプが桁あふれすると加算されるキャリーカウンタ12とを含む。クロックは時間を計時する機能を備えたものであることから、タイムスタンプ11とキャリーカウンタ12の値は順次加算される。タイムスタンプ11とキャリーカウンタ12の初期値には、ゼ

口、現在の日付等がセットされていた。

[0006] また、通信の信頼性の向上のためデータが正確に伝送されることが要望されている。伝送路上においては、符号化されたデータの一部が欠落する、符号化されたデータの一部の0と1とが反転する、といった符号誤りが発生する場合がある。上述のような安全制御に関するデータが伝送されているときに符号誤りが発生した場合、受信側の装置には本来のデータとは異なる誤ったデータが伝送され、受信側の装置が予期しない動作をすることも想定される。このため、安全制御に関する情報を正確に伝送することが安全の確保に繋がる。

[0007] 機能安全に関する基準であるIEC 61784-3では、定義された安全の目標水準毎に、許容される残存エラー率について定義されている。残存エラーとは、通信装置が受信データに対して、伝送路上で発生した符号の誤りを検出するために誤り検出を行っても、見逃されてしまうエラーをいう。IEC 61784-3では、残存エラーが発生する確率を示す残存エラー率の算出方法が定められている。機能安全を実現するために、残存エラー率を抑えることが望ましいといえる。しかし、残存エラーは、誤り検出を行ったとしても見逃されてしまうエラーであり、このようなエラーの検出率を上げることは容易ではない。

[0008] また、上述のIEC 61784-3では、残存エラー率の算出に、送信されるデータにおいて頻繁に出現する値の出現確率を使用することが規定されている。言い換えると、特定の値が出現する頻度が高い場合、その値の出現確率を残存エラー率の算出に採用しなければならない。この場合、高い出現確率を使用するため、残存エラー率が高くなってしまう。

[0009] 上述のように、送信されるデータに時間情報を付加する場合、時間情報についても符号の誤りが発生する可能性があるので、時間情報も誤り検出の対象となる。従来、クロックのタイムスタンプ11は、十分に長い時間をカウントすることができるように設定されている。タイムスタンプ11がごく短い期間で桁あふれしてしまうと、データの伝送中にタイムスタンプ11が桁

あふれすることがある。その結果、送信時に付加されたタイムスタンプの値と、受信時のタイムスタンプの値とが同じとなるといった事態が発生するおそれがある。よって、タイムスタンプ11が桁あふれすることはあまりない。仮にタイムスタンプ11の値が桁あふれした場合でも、再度タイムスタンプ11が桁あふれするまでには、長い時間がかかるため、キャリーカウンタ12の値が加算される頻度はきわめて低いといえる。

[0010] この結果、キャリーカウンタ12の値は初期値のまま、あるいは初期値付近の値を取ることが多いと言える。言い換えると、キャリーカウンタ12の値として、初期値付近の値が出現する確率が高いと言える。

先行技術文献

特許文献

[0011] 特許文献1：特開2003-298563号公報

発明の概要

発明が解決しようとする課題

[0012] 図5Aに示すように、キャリーカウンタ12の初期値としてゼロを設定した場合、キャリーカウンタ12の値としてゼロ近傍の値が出現する確率が高くなる。この場合、キャリーカウンタ12の値としてゼロが出現する確率を残存エラー率の算出に使用することになる。また、図5Bに示すように、キャリーカウンタ12の初期値として現在の日付を設定した場合、キャリーカウンタ12の値として、初期値として設定した日付近傍の値が出現する確率が高くなる。この場合、キャリーカウンタ12の値として設定された日付が出現する確率を残存エラー率の算出に使用することになる。このように、従来のクロックのキャリーカウンタ12では、特定の値の出現頻度が高くなるため、高い出現確率を残存エラー率の算出に使用せざるを得ず、残存エラー率を下げることは難しかった。

[0013] 本発明は上記実情に鑑みてなされたものであり、残存エラー率を下げるため、クロックのカウンタの値の出現頻度を分散させることを目的とする。

課題を解決するための手段

[0014] 上記目的を達成するため、本発明の通信システムでは、第1通信装置と第2通信装置とが相互に通信する。第1通信装置の第1計時手段は、時間経過をカウントする第1カウンタと、前記第1カウンタの桁あふれをカウントする第2カウンタとを備える。第1通信装置の第1データ変換手段は、予め設定されたタイミングで、予め設定された方式を使用して生成した値で、第2カウンタの値を置き換えて、第2カウンタが取る値を分散させる。第1通信装置の第1誤り検出手段は、第1カウンタの値と、第2カウンタの値とから第1誤り検出符号を生成する。第1通信装置の第1通信手段は、第2通信装置へ宛てたデータに第1カウンタの値と第1誤り検出符号とを付加したフレームを生成し、生成したフレームを前記第2通信装置に送信する。第2通信装置の第2計時手段は、時間経過をカウントする第3カウンタと、第3カウンタの桁あふれをカウントする第4カウンタとを備える。第2通信装置の第2データ変換手段は、設定されたタイミングで、設定された方式を使用して生成した値で、第4カウンタの値を置き換えて、前記第4カウンタが取る値を分散させる。第2通信装置の第2通信手段は、第1通信装置からフレームを受信する。第2通信装置の第2誤り検出手段は、フレームに含まれる第1カウンタの値と、第2計時手段の第4カウンタの値と、から第2誤り検出符号を生成し、生成した第2誤り検出符号が、フレームに含まれる第1誤り検出符号に対して設定された条件を満たすか否かを判別する。

発明の効果

[0015] 本発明の通信システムの第1通信装置は、設定されたタイミングで、設定された方式を使用して生成した値で、第1カウンタの桁あふれをカウントする第2カウンタの値を置き換えて、第2カウンタが取る値を分散させる。第2通信装置は、第1通信装置と同様に、設定されたタイミングで、設定された方式を使用して生成した値で、第3カウンタの桁あふれをカウントする第4カウンタの値を置き換えて、第4カウンタが取る値を分散させる。このような構成を備えることで、クロックのカウンタの値の出現頻度を分散させる

ことができる。

図面の簡単な説明

- [0016] [図1]実施の形態1に係る通信システムのハードウェア構成を示すブロック図
- [図2]実施の形態1に係る通信システムの機能ブロック図
- [図3]実施の形態1に係る安全用クロックの構成を示す図
- [図4A]従来の安全用クロックがカウントされる様子を示す図
- [図4B]従来の安全用クロックのタイムスタンプの桁あふれの様子を示す図
- [図5A]従来の安全用クロックのキャリーカウンタの初期値が0の場合において、キャリーカウンタの値とその出現確率との関係を示す図
- [図5B]キャリーカウンタの初期値にカレンダーが示す日を設定した場合において、キャリーカウンタの値とその出現確率との関係を示す図
- [図6]実施の形態1に係る安全用クロックのビットシフトによるデータ変換の方式を示す図
- [図7]実施の形態1に係る安全用クロックが桁あふれする様子を示す図
- [図8]実施の形態1に係るCRCの生成の方法を示す図
- [図9]実施の形態1に係る誤り検出の方法を示す図
- [図10]実施の形態1に係るデータ変換処理のフローチャート
- [図11]実施の形態2に係る安全用クロックの構成を示す図
- [図12]実施の形態2に係る安全用クロックが桁あふれする様子を示す図
- [図13]実施の形態2に係る安全用クロックのビットシフトによるデータ変換の方式を示す図
- [図14]実施の形態3に係る通信システムの構成を示す図
- [図15]実施の形態3に係る管理情報に格納されるデータの例を示す図
- [図16]実施の形態3に係るデータ変換処理のフローチャート
- [図17]実施の形態4に係る通信システムの構成を示す図
- [図18]実施の形態4に係る変換データ格納部に格納されるデータの一例を示す図

発明を実施するための形態

[0017] 以下、本発明の実施の形態に係る通信システム 10 について、図面を参照しつつ詳細に説明する。

[0018] (実施の形態 1)

図 1 に示すように、実施の形態 1 に係る通信システム 10 において、プログラマブルロジックコントローラ 1 とプログラマブルロジックコントローラ 2 とが、ネットワーク 600 を介して通信する。プログラマブルロジックコントローラ 1、2 は、例えば、生産システム、制御システム等において稼動する検出器、被制御機器を制御する。被制御機器は、産業用ロボット用のアクチュエータとサーボモータとを含む。プログラマブルロジックコントローラ 1 は、第 1 通信装置の一例であり、プログラマブルロジックコントローラ 2 は、第 2 通信装置の一例である。また、プログラマブルロジックコントローラ 1 は、他の通信装置の一例であり、プログラマブルロジックコントローラ 2 は、通信装置の一例である。また、プログラマブルロジックコントローラ 1 は、第 1 のコンピュータの一例であり、プログラマブルロジックコントローラ 2 は、第 2 のコンピュータの一例である。

[0019] プログラマブルロジックコントローラ 1 は、CPU ユニット 100 と、ネットワークユニット 200 とを有する。CPU ユニット 100 とネットワークユニット 200 は、不図示の電源ユニットとともに、ベースユニットに装着され、電源ユニットから供給された電源によって動作する。CPU ユニット 100 とネットワークユニット 200 とは共有バス 300 によって接続されており、共有バス 300 を介して相互に通信する。CPU ユニット 100 は、プログラマブルロジックコントローラ 1 全体を制御する。ネットワークユニット 200 は、CPU ユニット 100 の制御の下、他のネットワークユニット、検出器、被制御機器等と通信する。

[0020] プログラマブルロジックコントローラ 2 は、CPU ユニット 101 と、ネットワークユニット 201 とを含む。以下、プログラマブルロジックコントローラ 1 を例に説明を行うが、プログラマブルロジックコントローラ 2 もプログラマブルロジックコントローラ 1 と同様の構成を備える。

[0021] 実施の形態 1 において、プログラマブルロジックコントローラ 1 とプログラマブルロジックコントローラ 2 とは、機能安全に対応した通信を行うものとする。具体的には、プログラマブルロジックコントローラ 1 及び 2 は、受信したデータが期待された時間内に到達していないと判別すると、受信したデータに含まれるコマンドを無効とみなして、受信したデータを破棄する。このため、CPU ユニット 100 及び 101 は相互に同期して動作する計時装置であるクロックをそれぞれ備える。CPU ユニット 100 及び 101 が備えるクロックについては後述する。

[0022] 図 1 に示すように、CPU ユニット 100 はハードウェア構成として、各種データを記憶する記憶装置 110 と、ネットワークユニット 200 と共有バス 300 を介して通信を行う通信 I/F (Interface) 回路 120 と、CPU ユニット 100 全体を制御する演算装置 130 と、を有する。記憶装置 110 と、通信 I/F 回路 120 と、はいずれも内部バス 190 を介して演算装置 130 に接続されており、演算装置 130 と通信する。以下、CPU ユニット 100 を例に説明するが、プログラマブルロジックコントローラ 2 の CPU ユニット 101 も同様の構成を備えるものとする。

[0023] 記憶装置 110 は、揮発性メモリと不揮発性メモリとを含み、プログラムと各種データとを記憶する。また、記憶装置 110 は、演算装置 130 のワークメモリとして用いられる。また、記憶装置 110 は、演算装置 130 が実行することにより、後述のデータ変換処理と誤り検出処理を実現するためのプログラム 001 を記憶する。

[0024] 通信 I/F 回路 120 は、演算装置 130 の制御の下、共有バス 300 を介してネットワークユニット 200 とデータの送受信を行う。通信 I/F 回路 120 は、演算装置 130 が出力したデータを共有バス 300 を介してネットワークユニット 200 に送信する。通信 I/F 回路 120 がネットワークユニット 200 に送信するデータは、例えば、プログラマブルロジックコントローラ 1 の CPU ユニット 100 がプログラマブルロジックコントローラ 2 の CPU ユニット 101 に送信するコマンドを含む。また、通信 I/F

回路１２０は、ネットワークユニット２００から共有バス３００を介して受信したデータを演算装置１３０に出力する。通信Ｉ／Ｆ回路１２０がネットワークユニット２００から受信したデータは、例えば、プログラマブルロジックコントローラ２のＣＰＵユニット１０１がプログラマブルロジックコントローラ１のＣＰＵユニット１００に送信したコマンドを含む。

[0025] 演算装置１３０は、ＣＰＵ（Central Processing Unit）を含む。演算装置１３０は、記憶装置１１０に記憶されている各種プログラムを実行して、ＣＰＵユニット１００の各種機能を実現する。

[0026] ネットワークユニット２００はハードウェア構成として、各種データを記憶する記憶装置２１０と、通信のための通信Ｉ／Ｆ回路２２０と、ネットワークユニット２００全体を制御する演算装置２３０と、を有する。記憶装置２１０と、通信Ｉ／Ｆ回路２２０とは、いずれも内部バス２９０を介して演算装置２３０に接続されており、演算装置２３０と通信する。ネットワークユニット２００を例に説明するが、プログラマブルロジックコントローラ２のネットワークユニット２０１も同様の構成を備えるものとする。

[0027] 記憶装置２１０は、揮発性メモリと不揮発性メモリとを含み、演算装置２３０が、ネットワークユニット２００の各種機能を実現するために実行するプログラムと各種データとを記憶する。また、記憶装置２１０は、ＣＰＵユニット１００とネットワークユニット２０１とから受信したデータを一時的に記憶する。通信Ｉ／Ｆ回路２２０は、共有バス３００を介してＣＰＵユニット１００とデータの送受信を行う。また、通信Ｉ／Ｆ回路２２０は、ＣＰＵユニット１００から供給されたデータを、ネットワークユニット２０１にネットワーク６００を介して送信する。通信Ｉ／Ｆ回路２２０は、ネットワークユニット２０１からネットワーク６００を介して受信したデータをＣＰＵユニット１００に供給する。演算装置２３０は、ＣＰＵを含む。演算装置２３０は、記憶装置２１０に記憶されているプログラムを実行してネットワークユニット２００の各種機能を実現する。

[0028] 図２に示すように、ＣＰＵユニット１００は、機能的には、機能安全の観

点から設けられた安全用クロック１１１と、安全用クロック１１１のカウンタの値の変換方式を記憶する変換方式記憶部１１２と、安全用クロック１１１のカウンタの値の変換タイミングを記憶する変換タイミング記憶部１１３と、プログラマブルロジックコントローラ２から受信したデータを記憶する受信データ記憶部１１４と、プログラマブルロジックコントローラ２に宛てたデータを記憶する送信データ記憶部１１５と、安全用クロック１１１のカウンタの値を変換するクロック値変換部１５１と、他の通信装置とやり取りするデータを生成する通信部１５２と、送受信データの誤り検出を行う誤り検出部１５３と、各種のデータ処理を行うデータ処理部１５４とを含む。

[0029] CPUユニット１００の変換方式記憶部１１２と変換タイミング記憶部１１３とは第１記憶手段の一例である。CPUユニット１００のクロック値変換部１５１は第１データ変換手段の一例である。CPUユニット１００の通信部１５２は第１通信手段の一例である。CPUユニット１００の誤り検出部１５３は第１誤り検出手段の一例である。

[0030] 安全用クロック１１１は、設定された期間毎にクロックを発生するクロック発生回路と、クロック信号の発生回数をカウントするカウンタとを有した計時装置である。図３に示すように、安全用クロック１１１は、タイムスタンプ１１１１とキャリーカウンタ１１１２との２つのカウンタを備える。タイムスタンプ１１１１は、不図示のクロック発生回路が出力したクロック信号の数を数える。キャリーカウンタ１１１２は、タイムスタンプ１１１１が桁あふれすると加算される。図示する例では、タイムスタンプ１１１１がカウントした数は、下位１６ビットに格納される。キャリーカウンタ１１１２がカウントした数は、上位３２ビットに格納される。

[0031] タイムスタンプ１１１１は十分に長い時間をカウントすることができるよう設計されているものとする。タイムスタンプ１１１１が十分に長い時間をカウントすることができるため、タイムスタンプ１１１１が桁あふれることはほとんどない。この結果、キャリーカウンタ１１１２の値は初期値から変わることがほとんどなく、キャリーカウンタ１１１２の取る値は偏ったも

のとなってしまう。このため、実施の形態1においては、キャリアカウンタ1112の値を、決められたタイミングで、決められた方式で変換して、キャリアカウンタ1112の取る値を分散する。

[0032] キャリアカウンタ1112の値は、タイムスタンプ1111が桁あふれすると加算されるものの、キャリアカウンタ1112の値は決められたタイミングで変換されるため、キャリアカウンタ1112の値は、厳密にはタイムスタンプ1111が桁あふれした回数を示すものではない。キャリアカウンタ1112の値の変換については後述する。安全用クロック111は、図1に示す記憶装置110と、演算装置130とにより実現される。

[0033] 図2に示すCPUユニット100の安全用クロック111は第1計時手段の一例である。CPUユニット100の安全用クロックのタイムスタンプ1111は第1カウンタの一例である。CPUユニット100の安全用クロック111のキャリアカウンタ1112は第2カウンタの一例である。

[0034] CPUユニット101の安全用クロック111も、CPUユニット100の安全用クロック111と同様の構成を備える。CPUユニット101の安全用クロック111の不図示のクロック発生回路は、CPUユニット100の安全用クロック111のクロック発生回路と同じタイミングでクロックを発生する。また、CPUユニット101の安全用クロック111のタイムスタンプ1111及びキャリアカウンタ1112の初期値は、CPUユニット100の安全用クロック111のタイムスタンプ1111及びキャリアカウンタ1112の初期値と同じである。さらに、CPUユニット101においても、CPUユニット100と同様に、キャリアカウンタ1112の値を、決められたタイミングで、決められた方式で変換して、キャリアカウンタ1112の取る値を分散する。このように、CPUユニット101の安全用クロック111のタイムスタンプ1111及びキャリアカウンタ1112の値は、CPUユニット100の安全用クロック111のタイムスタンプ1111及びキャリアカウンタ1112の値と常に同じとなるように制御されている。

[0035] CPUユニット101の安全用クロック111は第2計時手段の一例である。CPUユニット101の安全用クロック111のタイムスタンプ1111は第3カウンタの一例である。CPUユニット101の安全用クロック111のキャリーカウンタ1112は第4カウンタの一例である。

[0036] まず、比較のため、図4A、図4Bを参照して、従来の安全用クロックのカウンタの方式を説明する。なお、安全用クロックのタイムスタンプ11とキャリーカウンタ12のそれぞれの初期値は「0」とであると仮定して説明を行う。タイムスタンプ11と安全用クロックのキャリーカウンタ12の初期値は、例えば、プログラマブルロジックコントローラ1及び2の管理者により設定される。

[0037] 従来は、図4Aに示すように、下位16ビットのタイムスタンプ11の値が、設定された期間毎に加算されていく。図4Bに示すように、タイムスタンプ11の値がカウント可能な上限値を超える、即ち桁あふれすると、キャリーカウンタ12の値が加算され、タイムスタンプ11の値は、初期値の0に戻る。タイムスタンプ11の値が順次加算され、再び、タイムスタンプ11の値が桁あふれすると、キャリーカウンタ12の値が加算される。このように、従来は、キャリーカウンタ12の値は、タイムスタンプ11の値の桁あふれ回数を示していた。なお、図4A、図4Bにおけるキャリーカウンタ12の値とタイムスタンプ11の値とは、16進で示している。以降同様である。

[0038] あるいは、プログラマブルロジックコントローラ1及び2の管理者が、キャリーカウンタ1112の初期値に、「0」ではなく、カレンダーが示す日を示す値を設定する場合もある。例えば、初期値が「4月10日」を示す値であるとする。この場合も、設定された期間毎にタイムスタンプ1111の値が加算され、タイムスタンプ11の値が桁あふれしたときに、キャリーカウンタ12が加算される。

[0039] ここで、タイムスタンプ11は十分に長い時間をカウントすることができるよう設計されていることから、タイムスタンプ11の桁あふれが発生する

ことはあまりないと考えられる。この結果、キャリアカウンタ 1 2 の値は初期値のまま、あるいは初期値付近の値を取ることが多いと言える。言い換えると、キャリアカウンタ 1 2 の値として、初期値付近の値が出現する確率が高いと言える。

[0040] 図 5 A に示すように、キャリアカウンタ 1 2 の初期値としてゼロを設定した場合、キャリアカウンタ 1 2 の値としてゼロ近傍の値が出現する頻度が高くなる。また、キャリアカウンタ 1 2 が加算される頻度が低いこと、さらに、例えば、装置の再起動により、タイムスタンプ 1 1 及びキャリアカウンタ 1 2 の値がリセットされることもあることから、実運用上においてはキャリアカウンタ 1 2 が取り得る値は限られている。図 5 B に示すように、キャリアカウンタ 1 2 の初期値として現在の日付を設定した場合、キャリアカウンタ 1 2 の値として、初期値として設定された日付近傍の値が出現する頻度が高くなる。このように、キャリアカウンタ 1 2 の初期値を「0」に設定した場合でも、あるいは初期値をカレンダーが示す日に設定した場合でも、図 5 A、図 5 B に示すように、キャリアカウンタ 1 2 が取る値は偏ってしまう。

[0041] 上記の実情に鑑みて、実施の形態 1 に係る CPU ユニット 1 0 0 は、設定されたタイミングで安全用クロック 1 1 1 のキャリアカウンタ 1 1 1 2 の値を示すビットをシフトし、キャリアカウンタ 1 1 1 2 の値を変換する。設定されたタイミングでビットシフトを行うことにより、キャリアカウンタ 1 1 1 2 の値は変換前とは異なる値に変わる。CPU ユニット 1 0 0 は、ビットシフトによりキャリアカウンタ 1 1 1 2 の値を変換するので、キャリアカウンタ 1 1 1 2 の値は順次加算されるわけではない。この結果、キャリアカウンタ 1 1 1 2 が取る値を分散することができる。タイムスタンプ 1 1 1 1 の値については、従来通り、設定された初期値から、設定された期間毎に順次加算される。タイムスタンプ 1 1 1 1 の値が桁あふれすると、キャリアカウンタ 1 1 1 2 の値は、ビットシフトによる変換が行われた後であれば、変換後の値から加算される。また、タイムスタンプ 1 1 1 1 の値が桁あふれした時点で、ビットシフトによる変換が行われていなければ、設定された初期値

から加算される。キャリアカウンタ 1112 の値の変換の具体的な方法は後述する。

[0042] 図 2 に示す変換方式記憶部 112 には、安全用クロック 111 のキャリアカウンタ 1112 の値を変換する方式を示すデータを記憶する。例えば、プログラマブルロジックコントローラ 1 及び 2 の管理者が、変換方式記憶部 112 に安全用クロック 111 のキャリアカウンタ 1112 の値を変換する方式を示すデータを予め格納する。変換方式記憶部 112 は、記憶装置 110 により実現される。実施の形態 1 においては、前述のように、安全用クロック 111 のキャリアカウンタ 1112 の値の変換はビットシフトにより行われる。このため、変換方式記憶部 112 は、キャリアカウンタ 1112 のうち、変換の対象となるビットを特定する情報と、シフトする方向を示す情報と、シフトするビット数を示す情報とを記憶する。

[0043] 例えば、図 6 に示すように、安全用クロック 111 のキャリアカウンタ 1112 の値の初期値にカレンダーの日付である「04月01日」がセットされているものとする。具体的には、「0」、「4」、「0」、「1」のそれぞれの 1 桁の 10 進値が 8 桁の 2 進値に変換された値がカウンタにセットされる。変換方式記憶部 112 には、変換方式として「上位 24 ビットを、右に、8 ビット単位で循環シフトさせる」と記憶されているものとする。この場合、上位 24 ビットが、8 ビット単位で右に循環シフトされると、キャリアカウンタ 1112 の上位 24 ビットが並べ換えられる。

[0044] 例えば、図 7 に示す状態で、タイムスタンプ 1111 に桁あふれが生じると、キャリアカウンタ 1112 が加算される。

[0045] 変換タイミング記憶部 113 は、安全用クロック 111 のキャリアカウンタ 1112 の値を変換するタイミングを示すデータを記憶する。例えば、プログラマブルロジックコントローラ 1 及び 2 の管理者が、変換タイミング記憶部 113 に安全用クロック 111 のキャリアカウンタ 1112 の値を変換するタイミングを示すデータを予め格納する。変換タイミング記憶部 113 は、図 1 に示す記憶装置 110 により実現される。図 2 に示す変換タイミン

グ記憶部 113 が記憶するタイミングは、タイムスタンプ 1111 の値が加算される設定されたタイミングとは独立したタイミングである。

[0046] キャリーカウンタ 1112 の値を変換するタイミングは、例えば、1 ミリ秒毎といったものであってもよいし、あるいは、安全用クロック 111 のタイムスタンプ 1111 が決められた回数だけカウントした場合としてもよい。また、あるいは、変換の実行タイミングは、安全用クロック 111 が桁あふれした場合としてもよい。あるいは、変換の実行タイミングは、安全用クロック 111 の設定されたビットの値が変化した場合としてもよい。なお、実施の形態 1 においては、安全用クロック 111 のカウンタの値の偏りをなくすことを目的としているため、キャリーカウンタ 1112 の値を変換する間隔は短く設定されていることが望ましい。

[0047] 受信データ記憶部 114 は、ネットワークユニット 200 がネットワークユニット 201 から受信したデータであって、後述の誤り検出部 153 が検査して誤りがないと判別したデータを格納する。ネットワークユニット 200 がネットワークユニット 201 から受信したデータは、例えば、プログラマブルロジックコントローラ 2 からプログラマブルロジックコントローラ 1 に宛てたコマンドを含む。受信データ記憶部 114 は、図 1 に示す記憶装置 110 により実現される。図 2 に示す受信データ記憶部 114 に格納されたデータは、後述のデータ処理部 154 によって適宜処理される。

[0048] 送信データ記憶部 115 は、プログラマブルロジックコントローラ 2 に宛てて送信されるデータを格納する。送信データ記憶部 115 は、図 1 に示す記憶装置 110 により実現される。図 2 に示す送信データ記憶部 115 には、後述のデータ処理部 154 が、送信用のデータを書き込む。

[0049] クロック値変換部 151 は、変換タイミング記憶部 113 が記憶するタイミングで、変換方式記憶部 112 が記憶する方式で、安全用クロック 111 のキャリーカウンタ 1112 の値を変換する。クロック値変換部 151 の機能は図 1 に示す演算装置 130 がプログラム 001 を実行することにより実現される。

[0050] 通信部 152 は、プログラマブルロジックコントローラ 2 に宛てて送信する送信フレームを生成する。送信フレームは、ヘッダ部と、データ部と、誤り検出符号とを含む。ヘッダ部は宛先情報を含む。データ部は、送信データ記憶部 115 に格納されているプログラマブルロジックコントローラ 2 に宛てたデータと安全用クロック 111 のタイムスタンプ 1111 の値とを含む。誤り検出符号は、後述の誤り検出部 153 により生成される。通信部 152 は、生成した送信フレームを共有バス 300 を介してネットワークユニット 200 に送信する。通信部 152 は共有バス 300 を介してネットワークユニット 200 からデータを受信する。ネットワークユニット 200 から供給されるデータは、ネットワークユニット 200 がプログラマブルロジックコントローラ 2 のネットワークユニット 201 から受信したデータである。通信部 152 は、図 1 に示す通信 I/F 回路 120 と演算装置 130 とにより実現される。

[0051] 図 2 に示す誤り検出部 153 は、プログラマブルロジックコントローラ 2 に宛てて送信される送信フレームに付加する CRC (Cyclic Redundancy Check) を生成する。誤り検出部 153 は、プログラマブルロジックコントローラ 2 から受信した受信フレームに付加されている CRC を使用した誤り検出を行う。実施の形態においては、誤り検出部 153 は、伝送路上でデータが破損したか否かの誤りチェックを、CRC を使用して行うものとする。誤り検出部 153 の機能は、図 1 に示す演算装置 130 がプログラム 001 を実行することにより実現される。

[0052] 具体的には、図 2 に示す誤り検出部 153 は、ネットワークユニット 200 がネットワークユニット 201 に送信する送信フレームに付加する誤り検出符号として CRC を算出する。実施の形態 1 においては、図 8 に示すように、誤り検出部 153 は、送信データ記憶部 115 に格納されているプログラマブルロジックコントローラ 2 に宛てたデータと、安全用クロック 111 のタイムスタンプ 1111 の値及びキャリーカウンタ 1112 の値から CRC を生成する。誤り検出部 153 は、生成した CRC を通信部 152 に出力

する。以下、送信側が生成したCRCをCRC__sと称することがある。送信側が生成したCRC__sは第1誤り検出符号の一例である。

[0053] また、誤り検出部153は、図9に示すように、ネットワークユニット200がネットワークユニット201から受信した受信フレームに付加されたCRC__sが、受信フレームから算出したCRCと一致するかを判別する。上述のように、送信側では、送信用のデータと、安全用クロック111のタイムスタンプ1111の値及びキャリアカウンタ1112の値からCRC__sが生成されている。このため、誤り検出部153は、通信部152が受信した受信フレームのデータ部に含まれているデータと、データ部に含まれているタイムスタンプ1111の値と、自身の安全用クロック111のキャリアカウンタ1112の値と、からCRCを生成する。以下、受信側が生成したCRCをCRC__rと称することがある。誤り検出部153は、生成したCRC__rと、受信フレームに含まれるCRC__sとが一致するか否かを判別する。受信側が生成したCRC__rは第2誤り検出符号の一例である。

[0054] CRC__rと、CRC__sとが一致しない場合、誤り検出部153は、当該受信フレームを破棄する。当該受信フレームのデータが壊れているからである。

[0055] また、CRC__rと、CRC__sとが一致する場合、誤り検出部153は、受信データのデータ部に含まれるタイムスタンプ1111の値が、自身の安全用クロック111のタイムスタンプ1111が示す現在時刻より指定された時間を遡った値であるか否かを判別する。具体的には、誤り検出部153は、受信データに含まれるタイムスタンプ1111の値に指定されたオフセット時間を加算した時刻が、自身の安全用クロック111が示す現在時刻以前であるか否かを判別する。これは、受信データが、期待された時間内に到達したか否かを判別するためである。

[0056] 誤り検出部153は、受信データに含まれるタイムスタンプ1111の値に指定されたオフセット時間を加算した時刻が、自身の安全用クロック111が示す現在時刻以前であると判別すると、受信フレームのデータを受信デ

ータ記憶部 114 に格納する。

[0057] 一方、誤り検出部 153 は、受信データに含まれるタイムスタンプ 1111 の値に指定されたオフセット時間を加算した時刻が、自身の安全用クロック 111 が示す現在時刻以降であると、当該受信フレームを破棄する。当該受信フレームが期待された時間内に到達していないからである。

[0058] データ処理部 154 は、プログラマブルロジックコントローラ 2 に宛てたデータを送信データ記憶部 115 に格納する。データ処理部 154 は、プログラマブルロジックコントローラ 2 宛てのデータとして、例えば、プログラマブルロジックコントローラ 2 に接続された制御対象機器に対するコマンドを送信データ記憶部 115 に格納する。また、データ処理部 154 は、受信データ記憶部 114 に格納されたデータに適宜処理を行う。例えば、データ処理部 154 に格納されたデータがプログラマブルロジックコントローラ 2 で収集された検査データである場合、データ処理部 154 は、検査データの統計処理を行う。データ処理部 154 は、図 1 に示す演算装置 130 により実現される。

[0059] 図 2 に示すプログラマブルロジックコントローラ 2 の CPU ユニット 101 は、CPU ユニット 100 と同様の構成を有するものとする。

[0060] プログラマブルロジックコントローラ 1 の CPU ユニット 100 と、プログラマブルロジックコントローラ 2 の CPU ユニット 101 と、においては、安全用クロック 111 の値が一致する必要がある。このため、CPU ユニット 101 の変換方式記憶部 112 には、CPU ユニット 100 の変換方式記憶部 112 と同様の変換方式に関するデータが格納されている。例えば、プログラマブルロジックコントローラ 1 及び 2 の管理者が、CPU ユニット 101 の変換方式記憶部 112 に、CPU ユニット 100 の変換方式記憶部 112 と同様の変換方式に関するデータを格納する。CPU ユニット 101 の変換タイミング記憶部 113 には、CPU ユニット 100 の変換タイミング記憶部 113 と同様の変換のタイミングに関する情報が格納されている。よって、プログラマブルロジックコントローラ 2 の CPU ユニット 101 に

においても、プログラマブルロジックコントローラ1のCPUユニット100と、同じタイミングで、同じ方式で、安全用クロック111のキャリアカウンタの値が変換される。この結果、CPUユニット100の安全用クロック111の値と、CPUユニット101の安全用クロック111の値とは常に一致したものとなる。CPUユニット100及び101はそれぞれビットシフトにより自身の安全用クロック111のキャリアカウンタ1112の値を変換する。よって、CPUユニット100及び101それぞれのキャリアカウンタ1112の値は順次加算されるわけではない。この結果、キャリアカウンタ1112が取る値を分散することができる。なお、プログラマブルロジックコントローラ1の安全用クロック111と、プログラマブルロジックコントローラ2の安全用クロック111とには、同じ値の初期値が設定される必要がある。

[0061] CPUユニット101の変換方式記憶部112と変換タイミング記憶部113とは第2記憶手段の一例である。CPUユニット101のクロック値変換部151は第2データ変換手段の一例である。CPUユニット101の通信部152は第2通信手段の一例である。CPUユニット101の誤り検出部153は第2誤り検出手段の一例である。

[0062] ネットワークユニット200は、機能的には、CPUユニット100と共有バス通信を行い、ネットワークユニット201と通信する通信部221を含む。

[0063] 通信部221は、共有バス300を介して、CPUユニット100とデータの送受信を行う。さらに、通信部221は、ネットワーク600を介して、ネットワークユニット201と通信する。例えば、通信部221は、共有バス300を介して、CPUユニット100からプログラマブルロジックコントローラ2に宛てたデータを受信する。通信部221は、受信した当該データを、ネットワーク600を介してネットワークユニット201に送信する。また、通信部221は、ネットワーク600を介して、ネットワークユニット201からデータを受信する。通信部221は、受信した当該データ

を共有バス300を介してCPUユニット100に送信する。通信部221は、図1に示す記憶装置210と通信I/F回路220と演算装置230とにより実現される。

[0064] ネットワーク600は、例えば、イーサネット（登録商標）といった規格のLAN（Local Area Network）である。

[0065] 次に、図2に示すクロック値変換部151が行う変換処理を説明する。図10に示すように、クロック値変換部151は、変換タイミング記憶部113に記憶された変換を実行されたタイミングであるか否かを判別する（ステップS11）。変換を実行するタイミングであると判別すると（ステップS11；Yes）、クロック値変換部151は、クロック値の変換を実行する（ステップS12）。

[0066] 変換方式記憶部112に、変換方式として「上位24ビットを、右に、8ビット単位で循環シフトさせる」と記憶されていると仮定する。この場合、クロック値変換部151は、図6に示すように、安全用クロック111のカウンタの値の上位24ビットを、8ビット単位に右に循環シフトする。従って、安全用クロック111のキャリーカウンタ1112の値が変換後の値に書き換えられる。図10に示すように、クロック値変換部151は、再び、ステップS11の処理に進む。

[0067] 一方、ステップS11で変換を実行するタイミングでないと判別すると（ステップS11；No）、クロック値変換部151は、実行のタイミングが来るまで待機する。

[0068] また、CPUユニット101においては、CPUユニット100と同じタイミングで同様の方法で安全用クロック111のキャリーカウンタ1112の値を変換している。このため、CPUユニット100の安全用クロック111のキャリーカウンタ1112の値と、CPUユニット101の安全用クロック111のキャリーカウンタ1112の値とは、同じように、分散されることになる。

[0069] 以上が実施の形態1に係る構成である。実施の形態1では、安全用クロッ

ク 1 1 1 が有するカウンタのうちキャリーカウンタ 1 1 1 2 の値をビットシフトした値で置き換えた。安全用クロック 1 1 1 のカウンタの設定された範囲の値を変換することで、安全用クロック 1 1 1 のカウンタの値の出現頻度を分散させることができる。しかし、安全用クロック 1 1 1 のカウンタの値は別の方法で変換してもよい。

[0070] (実施の形態 2)

実施の形態 2 における安全用クロックの値の変換は、あらかじめ設定された生成方法で生成した乱数で、安全用クロック 1 1 1 のカウンタの値を置き換えることによって行う。以下、実施の形態 1 と異なる点を中心に説明を行う。

[0071] 図 2 に示す安全用クロック 1 1 1 は、実施の形態 1 と同様に、設定された期間毎にクロックを発生するクロック発生回路と、クロック信号の発生の回数をカウントするカウンタとを有する。図 1 1 に示すように、実施の形態 2 に係る安全用クロック 1 1 1 は、タイムスタンプ 1 1 1 1 とキャリーカウンタ 1 1 1 2 との 2 つのカウンタを備える。タイムスタンプ 1 1 1 1 は、不図示のクロック発生回路が出力したクロック信号の数を数える。キャリーカウンタ 1 1 1 2 は、タイムスタンプ 1 1 1 1 の桁あふれをカウントする。さらに、安全用クロック 1 1 1 は、設定されたタイミングで値が書き換えられる領域であるスクランブル領域 1 1 1 3 を有する。図 1 1 に、実施の形態 2 における安全用クロック 1 1 1 のカウンタが保持するビット列の構成を示す。下位 1 6 ビットがタイムスタンプ 1 1 1 1 の領域として割り当てられている点は、図 3 に示す実施の形態 1 と同様である。上位 3 2 ビットのうち、8 ビットはキャリーカウンタ 1 1 1 2 の領域として割り当てられている。上位ビット 3 2 ビットのうちの残りの 2 4 ビットは、スクランブル領域 1 1 1 3 として割り当てられている。実施の形態 2 においては、決められたタイミングで、スクランブル領域 1 1 1 3 の値が生成された乱数の値で置き換えられる。

[0072] 実施の形態 1 とは、キャリーカウンタ 1 1 1 2 の割り当てビット数は異な

るものの、図 1 2 に示すように、タイムスタンプ 1 1 1 1 が桁あふれすると、キャリーカウンタ 1 1 1 2 の値が加算される。

[0073] 図 2 に示す変換方式記憶部 1 1 2 には、図 1 1 に示すスクランブル領域 1 1 1 3 のうち変換の対象とする範囲と、乱数生成アルゴリズムと、乱数生成のためのシードと、が定義されている。例えば、変換方式記憶部 1 1 2 に、対象範囲が上位 2 4 ビットであり、乱数生成アルゴリズムとして「アルゴリズム 2 0 0 0」を使用し、シードとして「シード 3 0 0 0」を使用することが定義されているとする。この場合、生成した乱数で指定された範囲を置き換えると、例えば、図 1 3 のように、安全用クロック 1 1 1 のスクランブル領域 1 1 1 3 の値が変換される。

[0074] CPU ユニット 1 0 0 及び 1 0 1 のそれぞれの安全用クロック 1 1 1 のカウンタの値を一致させなくてはならない。このため、図 2 に示す変換方式記憶部 1 1 2 に格納される乱数生成アルゴリズムは、CPU ユニット 1 0 0 及び 1 0 1 が、同じシードを使用した場合に同じ値を得ることができるアルゴリズムである必要がある。

[0075] さらに、実施の形態 2 においては、安全用クロック 1 1 1 のカウンタの値の偏りをなくすことを目的としているため、生成した乱数を 0 と 1 とを含むビット列にした場合の、0 と 1 の出現率が均等となり、乱数生成アルゴリズムの評価テストをパスした乱数生成アルゴリズムを選定することが望ましい。

[0076] 変換タイミング記憶部 1 1 3 には、図 1 1 に示す安全用クロック 1 1 1 のスクランブル領域 1 1 1 3 の指定された範囲の値を変換するタイミングが記憶されている。

[0077] クロック値変換部 1 5 1 は、変換タイミング記憶部 1 1 3 が記憶するタイミングで、変換方式記憶部 1 1 2 において指定されている乱数生成アルゴリズムとシードとから乱数を生成する。クロック値変換部 1 5 1 は、スクランブル領域 1 1 1 3 において、変換方式記憶部 1 1 2 において指定された範囲の値を、生成した乱数を示す 0 と 1 とを含むビット列で置き換える。このよ

うにして、安全用クロック 1 1 1 のスクランブル領域 1 1 1 3 の値が変換される。よって、実施の形態 2 においても、安全用クロック 1 1 1 のキャリアカウンタ 1 1 1 2 が取る値を分散させることができる。実施の形態 2 におけるクロック値変換部 1 5 1 の変換のフローは、図 1 0 に示す実施の形態 1 と同様である。

[0078] また、乱数生成アルゴリズムによっては初期化処理が必要なものもある。変換方式記憶部 1 1 2 で指定された乱数生成アルゴリズムが初期化処理を必要とする場合、クロック値変換部 1 5 1 は、変換タイミング記憶部 1 1 3 で指定されたタイミングより前に初期化処理を行っておく。

[0079] (実施の形態 3)

実施の形態 1 のビットシフトより、実施の形態 2 の乱数生成の方が、安全用クロック 1 1 1 の偏りの抑制には効果があるが、乱数生成を使用した変換の方法を採用することは、CPU ユニット 1 0 0 及び 1 0 1 にとって処理の負荷が高い。処理の負荷の観点から、CPU ユニット 1 0 0 及び 1 0 1 の処理性能に応じて、ビットシフトを使用した変換の方法を採用する方が好ましいこともある。このように、複数の CPU ユニットそれぞれが、個々の性能に応じて、ビットシフトあるいは乱数生成による変換方式を採用することが望ましい場合もある。

[0080] また、実施の形態 1、2 では、CPU ユニット 1 0 0 及び 1 0 1 がそれぞれ、安全用クロック 1 1 1 のカウンタの値を変換する方式を変換方式記憶部 1 1 2 に、変換のタイミングを変換タイミング記憶部 1 1 3 に記憶している。しかし、CPU ユニット 1 0 0 の数が多くなれば、管理者が各 CPU ユニット 1 0 0 に変換の方式と変換タイミングとを設定する必要があり、手間がかかる。

[0081] このため、実施の形態 3 では、安全用クロックのカウンタの値の変換について管理する側の通信装置と、安全用クロックのカウンタの値の変換について管理される側の通信装置と、をあらかじめ決め、管理する側の通信装置が、管理される側の通信装置に、安全用クロックの値の変換方式及び変換タイ

ミングを通知するものとする。

[0082] 図14に実施の形態3に係る通信システム50の構成を示す。プログラマブルロジックコントローラ1は、管理する側の通信装置である。プログラマブルロジックコントローラ3及び4は、管理される側の通信装置である。プログラマブルロジックコントローラ1、3及び4は、ネットワーク600を介して相互に通信可能である。以下実施の形態1、2と異なる点を中心に説明する。

[0083] 実施の形態3において、プログラマブルロジックコントローラ1のCPUユニット100は、プログラマブルロジックコントローラ3との通信に使用する安全用クロック111と、プログラマブルロジックコントローラ4との通信に使用する安全用クロック116とを有する。

[0084] 安全用クロック111は図3に示す構成を備え、安全用クロック116は図11に示す構成を備えるものとする。CPUユニット100は、安全用クロック111の値をビットシフトにより変換し、安全用クロック116の値を乱数で置き換えて変換するものとする。

[0085] また、実施の形態3において、CPUユニット100は、実施の形態1及び2における変換方式記憶部112及び変換タイミング記憶部113の代わりに、管理情報117を備える。管理情報117は、管理する側のプログラマブルロジックコントローラ1が、管理される側のプログラマブルロジックコントローラ3及び4に通知する安全用クロックの値の変換方式及び変換タイミングを示す情報を格納する。図15に示すように、管理情報117は、管理対象のプログラマブルロジックコントローラを識別する情報と、管理対象が有する安全用クロックを識別する情報と、安全用クロックの値を変換する変換方式を示す情報と、変換タイミングを示す情報と、を定義する。

ここで、安全用クロック111と、後述のプログラマブルロジックコントローラ3のCPUユニット102が有する安全用クロック111aとは、同じ値を取る必要がある。安全用クロック116と、後述のプログラマブルロジックコントローラ4のCPUユニット103が有する安全用クロック11

6 a とは、同じ値を取る必要がある。このため、管理情報 117 には、プログラマブルロジックコントローラ 3 の安全用クロック 111 a について、安全用クロック 111 と同様の変換方式及び変換タイミングを示す情報が格納されている。管理情報 117 には、プログラマブルロジックコントローラ 4 の安全用クロック 116 a について、安全用クロック 116 と同様の変換方式及び変換タイミングを示す情報が格納されている。なお、CPU ユニット 100 は、安全用クロック 111 と安全用クロック 111 a とが対応し、安全用クロック 116 と安全用クロック 116 a とが対応することを示す情報を予め記憶しているものとする。管理情報 117 は図 1 に示す記憶装置 110 により実現される。管理情報 117 は第 1 記憶手段の一例である。

[0086] 図 14 に示すクロック値変換部 151 は、管理情報 117 に定義された変換方式と変換タイミングとに従って、安全用クロック 111 及び 116 の値を変換する。

[0087] さらに、クロック値変換部 151 は、管理情報 117 が示す管理対象のプログラマブルロジックコントローラに、管理情報 117 に定義された変換方式と変換のタイミングとを通知する。クロック値変換部 151 は、管理対象毎の定義された変換方式と変換のタイミングとを示す情報を通信部 152 に出力する。従って、通信部 152 は、データ変換指示であることを示す特定のコマンドと、変換方式と変換タイミングとを示す情報とを含むフレームを生成して、生成したフレームをネットワークユニット 200 に送信する。ネットワークユニット 200 は、CPU ユニット 100 から供給されたフレームをネットワークユニット 202 及び 203 に送信する。クロック値変換部 151 は通知手段の一例である。

[0088] プログラマブルロジックコントローラ 1 の一方の管理対象であるプログラマブルロジックコントローラ 3 の CPU ユニット 102 は、安全用クロック 111 a を有している。安全用クロック 111 a は、安全用クロック 111 と同様に、図 3 に示す構成を備えるものとする。安全用クロック 111 a は、CPU ユニット 100 の安全用クロック 111 と同じ値を取るよう制御さ

れる。

[0089] また、CPUユニット102においては、クロック値変換部151aは、安全用クロック111aの値を、CPUユニット100から通知された変換方式と変換のタイミングとで変換する。通信部152aは、ネットワークユニット202がネットワークユニット200から特定のコマンドを含むフレームを受信した場合、そのフレームに含まれる変換方式と変換のタイミングとを示す情報を、クロック値変換部151aに供給する。CPUユニット102は、実施の形態1のCPUユニット100及び101が有している変換方式記憶部112及び変換タイミング記憶部113を有していない。

[0090] プログラマブルロジックコントローラ1の他方の管理対象であるプログラマブルロジックコントローラ4のCPUユニット103は、安全用クロック116aを有している。

安全用クロック116aは、安全用クロック116と同様に、図11に示す構成を備えるものとする。安全用クロック116aは、CPUユニット100の安全用クロック116と同じ値を取るよう制御される。CPUユニット103のクロック値変換部151a、通信部152aの構成は、CPUユニット102と同様である。CPUユニット103は、CPUユニット102と同様に、実施の形態1に係る変換方式記憶部112及び変換タイミング記憶部113を有していない。

[0091] なお、CPUユニット102及び103について、実施の形態1及び2のCPUユニット100及び101と同様の符号を付した構成について、実施の形態3で特に言及しない構成については、実施の形態1、2とほぼ同様であるものとする。

[0092] 上記構成を有するCPUユニット100と102と103とは、図16に示すように、データ変換の処理を行う。

[0093] まず、CPUユニット100におけるデータ変換の処理を説明する。CPUユニット100は管理する側であるので（ステップS21；Yes）、CPUユニット102、103に対して、管理情報117にそれぞれ定義され

た変換方式と変換タイミングとを通知する（ステップS 2 2）。CPUユニット1 0 2、1 0 3から、変換が可能である旨の応答があれば、変換の方式と変換タイミングとが確定したと判別して（ステップS 2 3；Y e s）、次のステップの処理を行う。ステップS 2 4において、CPUユニット1 0 0は変換を実行するタイミングであると判別すると（ステップS 2 4；Y e s）、CPUユニット1 0 2、1 0 3に割り当てられた安全用クロック1 1 1、1 1 6の値の変換処理を実行する（ステップS 2 5）。以上が、CPUユニット1 0 0の処理である。なお、ステップS 2 3において、CPUユニット1 0 0は、CPUユニット1 0 2、1 0 3のうち、変換が可能である旨の応答があったいずれか、あるいは両方のための安全用クロックの値の変換処理を行う。一方、ステップS 2 3において、CPUユニット1 0 2、1 0 3から、変換が可能である旨の応答がない場合、あるいは、変換が不可能である旨の応答があった場合、CPUユニット1 0 0は、変換の方式と変換タイミングとが確定していないと判別して（ステップS 2 3；N o）、再びステップS 2 1の処理に戻る。

[0094] また、管理される側の一方のCPUユニット1 0 2におけるデータ変換の処理を説明する。CPUユニット1 0 2は管理する側ではないので（ステップS 2 1；N o）、データ変換方式と変換タイミングをCPUユニット1 0 0から受信したか否かを判別する（ステップS 2 6）。受信した場合（ステップS 2 6；Y e s）、CPUユニット1 0 2は、変換処理が可能であるか否かを判別し、判別した結果をCPUユニット1 0 0に通知する（ステップS 2 7）。例えば、指定される変換の間隔が短いため処理負荷の面から処理を行うことができない、乱数生成のアルゴリズムのプログラムを有していない、といった場合には、変換処理が不可能であると判別する。一方、変換処理が可能であると判別した場合、変換の方式と変換タイミングとが確定したことになるので（ステップS 2 3；Y e s）、CPUユニット1 0 2は、ステップS 2 4以降の処理を行い、安全用クロック1 1 1 aの値の変換を行う。管理される側の他方のCPUユニット1 0 3もCPUユニット1 0 2と同

様の処理を行う。

[0095] (実施の形態4)

実施の形態3では、CPUユニット100が2つの安全用クロック111及び116を有する。ここで、安全用クロック111及び116は、データが期待された時間内に到着したかの判別にも使用されるため、高い精度で計時できることが要求される。このため、CPUユニット100が安全用クロック111及び116用にそれぞれ高精度の計時用素子を備える必要があり、コストがかさむ。

[0096] 実施の形態4では、管理する側の通信装置であるCPUユニット100が1つの安全用クロック111だけを有し、管理対象のCPUユニット102及び103のそれぞれの安全用クロックのデータ変換を管理する構成を説明する。

[0097] 実施の形態3と異なり、図17に示すように、実施の形態4に係るCPUユニット100は、1つの安全用クロック111のみを有する。実施の形態4においても、CPUユニット100は、図15に示す管理情報117を備えるものとする。

[0098] クロック値変換部151は、図15に示す管理情報117が記憶するタイミングと変換方式で、安全用クロック111の値を変換した値を求め、求めた値を変換データ格納部118に格納する。CPUユニット100は、CPUユニット102及び103を管理するため、それぞれの安全用クロックのためのデータ変換を行った値を変換データ格納部118に保存する。変換データ格納部118には、CPUユニット102の安全用クロック111aの値と同じ値と、CPUユニット103の安全用クロック116aの値と同じ値とが保持されることになる。

[0099] 具体的には、クロック値変換部151は、CPUユニット102の安全用クロック111aの変換タイミングと同じタイミングで、安全用クロック111aの変換方式と同じ変換方式を使用して安全用クロック111の値を変換した値を求める。クロック値変換部151は、図18に示すように、求め

た値を管理対象及び管理対象が有する安全用クロックを識別する情報とともに変換データ格納部 118 に格納する。CPU ユニット 102 においても、CPU ユニット 100 と同じ変換タイミングとで、同じ変換方式を使用して安全用クロック 111a の値を変換している。このため、変換データ格納部 118 に格納されている値は、CPU ユニット 102 の安全用クロック 111a の値と一致する。

[0100] また、クロック値変換部 151 は、CPU ユニット 103 の安全用クロック 116a の変換タイミングと同じタイミングで、安全用クロック 116a の変換方式と同じ変換方式を使用して安全用クロック 111 の値を変換した値を求め、求めた値を変換データ格納部 118 に格納する。CPU ユニット 103 は CPU ユニット 100 と同じ変換タイミングで、同じ変換方式を使用して安全用クロック 116a の値を変換している。このため、変換データ格納部 118 に格納された値は、CPU ユニット 103 の安全用クロック 116a の値と一致する。

[0101] プログラマブルロジックコントローラ 3、4 との通信の際には、誤り検出部 153 は、安全用クロック 111 のキャリーカウンタ 1112 の値ではなく、変換データ格納部 118 に格納された、相手先に対応づけられた変換後のキャリーカウンタ 1112 の値を使用して CRC の生成、誤り検出を行う。以上が実施の形態 4 に係る構成である。

[0102] 以上説明したように、実施の形態 1～4 においては、CPU ユニット 100 の安全用クロックの指定された範囲の値と、CPU ユニット 100 の通信先の CPU ユニット 101、102、103 の安全用クロックの指定された範囲の値と、を同じタイミングで、同じ方法で別の値に置き換える。従って、置き換え後の安全用クロックの値を一致させつつ、安全用クロックの値の偏りを低減することができる。よって、安全用クロックの値が誤り検出の対象となる場合に残存エラー率を下げることができる。

[0103] 実施の形態 1 においては、キャリーカウンタ 1112 の値を置き換えるためビットシフトを使用する。このため、CPU ユニット 100 に負荷をかけ

ず、残存エラー率を低減することが可能である。

[0104] 実施の形態2においては、生成した乱数でキャリアカウンタ1112の値を置き換えるため、ビットシフトによる方法に比べ、安全用クロック111の値をより分散させることができる。よって、残存エラー率の低減に高い効果を奏する。

[0105] 実施の形態3においては、データ変換処理方式および実行タイミングを通信で共有することにより、個々の通信装置への設定を行う必要がない。また、マスタとスレーブのそれぞれの処理性能に応じて適したデータ変換処理方式を選択することができる。例えば、処理性能の低い通信装置との通信においては、処理負荷が高い乱数の生成ではなく、ビットシフトの方法を採用することができる。このようにして、既存の通信装置にも、上述した実施の形態に係る構成を採用することができる。

[0106] 実施の形態4では、キャリアカウンタの値を直接書き換えないため、安全用クロックの値は、例えば、カレンダーデータ通りの時間を示している。このため、安全用クロックの値を、ある通信装置からデータが期待時間内に他の通信装置に到着しているかを確認するといった、他の用途でも使用することができるようになる。また、マスタは、安全用クロックのため、高精度な計時素子を1つだけ有すればよいので、安全用クロックを複数有する場合に比べ、コストを抑えることができる。

[0107] 実施の形態1～4において、プログラマブルロジックコントローラ1～4が相互に通信を行う例を説明したが、これに限られない。例えば、プログラマブルロジックコントローラ1だけがデータを送信する機能を備え、プログラマブルロジックコントローラ2～4は、データを受信するだけの構成であってもよい。この場合、送信側のプログラマブルロジックコントローラ1は、誤り検出符号を生成し、誤り検出符号と自身の安全用クロックのタイムスタンプとを含むフレームを他のプログラマブルロジックコントローラに送信する。受信側のプログラマブルロジックコントローラ2～4は、プログラマブルロジックコントローラ1から受信したタイムスタンプと自身の安全用クロ

ックのキャリアカウンタとから誤り検出符号を生成し、生成した誤り検出符号とプログラマブルロジックコントローラ 1 から受信した誤り検出符号とが一致するか否かを判別すればよい。

[0108] 上記の実施の形態 1 ～ 4 においては、CPU ユニットが安全用クロックを有し、安全用クロックの値を変換する処理を行う例を説明したが、CPU ユニットではなく、ネットワークユニットが上述した変換処理を行うように構成してもよい。

[0109] 上記のデータ変換処理に係るプログラムを記録する記録媒体としては、磁気ディスク、光ディスク、光磁気ディスク、フラッシュメモリ、半導体メモリ、磁気テープを含むコンピュータ読取可能な記録媒体を使用することができる。

[0110] 本発明は、広義の精神と範囲を逸脱することなく、様々な実施形態及び変形が可能とされるものである。また、上述した実施形態は、本発明を説明するためのものであり、本発明の範囲を限定するものではない。つまり、本発明の範囲は、実施形態ではなく、請求の範囲によって示される。そして、請求の範囲内及びそれと同等の発明の意義の範囲内で施される様々な変形が、本発明の範囲内とみなされる。

符号の説明

[0111] 001 プログラム、1, 2, 3, 4 プログラマブルロジックコントローラ、10, 50 通信システム、11, 1111 タイムスタンプ、12, 1112 キャリアカウンタ、100, 101, 102, 103 CPU ユニット、110, 210 記憶装置、111, 111a, 116, 116a 安全用クロック、112 変換方式記憶部、113 変換タイミング記憶部、114 受信データ記憶部、115 送信データ記憶部、117 管理情報、118 変換データ格納部、120, 220 通信 I/F 回路、130, 230 演算装置、151, 151a クロック値変換部、152, 152a, 221 通信部、154 データ処理部、153 誤り検出部、190, 290 内部バス、200, 201, 202, 203 ネットワーク

ユニット、３００ 共有バス、６００ ネットワーク、１１１３ ス克蘭
ブル領域、２０００ アルゴリズム、３０００ シード

請求の範囲

- [請求項1] 第1通信装置と第2通信装置とが相互に通信する通信システムであって、
- 前記第1通信装置は、
- 時間経過をカウントする第1カウンタと、前記第1カウンタの桁あふれをカウントする第2カウンタとを備える第1計時手段と、
- 予め設定されたタイミングで、予め設定された方式を使用して生成した値で、前記第2カウンタの値を置き換えて、前記第2カウンタが取る値を分散させる第1データ変換手段と、
- 前記第1カウンタの値と、前記第2カウンタの値とから第1誤り検出符号を生成する第1誤り検出手段と、
- 前記第2通信装置へ宛てたデータに前記第1カウンタの値と前記第1誤り検出符号とを付加したフレームを生成し、生成した前記フレームを前記第2通信装置に送信する第1通信手段と、
- を有し、
- 前記第2通信装置は、
- 時間経過をカウントする第3カウンタと、前記第3カウンタの桁あふれをカウントする第4カウンタとを備える第2計時手段と、
- 前記設定されたタイミングで、前記設定された方式を使用して生成した値で、前記第4カウンタの値を置き換えて、前記第4カウンタが取る値を分散させる第2データ変換手段と、
- 前記第1通信装置から前記フレームを受信する第2通信手段と、
- 前記フレームに含まれる前記第1カウンタの値と、前記第2計時手段の前記第4カウンタの値と、から第2誤り検出符号を生成し、生成した前記第2誤り検出符号が、前記フレームに含まれる前記第1誤り検出符号に対して設定された条件を満たすか否かを判別する第2誤り検出手段と、
- を有する、

通信システム。

[請求項2] 前記第2カウンタの初期値と前記第4カウンタの初期値とは同じである、

請求項1に記載の通信システム。

[請求項3] 前記第1データ変換手段は、前記第2カウンタの値の指定された範囲の値を、指定された方向に、指定されたビット数だけシフトさせた値で置き換え、

前記第2データ変換手段は、前記第1データ変換手段と同一の方法で、前記第4カウンタの値の置き換えを行う、

請求項1又は2に記載の通信システム。

[請求項4] 前記第1データ変換手段は、前記第2カウンタの値の指定された範囲の値を、指定された生成方法で生成した乱数で、置き換え、

前記第2データ変換手段は、前記第1データ変換手段と同一の方法で、前記第4カウンタの値の置き換えを行う、

請求項1又は2に記載の通信システム。

[請求項5] 前記第1通信装置の前記第1誤り検出手段は、前記第2通信装置へ宛てた前記データと、前記第1カウンタの値と、前記第2カウンタの値とから前記第1誤り検出符号を生成し、

前記第2通信装置の前記第2誤り検出手段は、前記フレームに含まれる前記第2通信装置へ宛てた前記データと、前記フレームに含まれる前記第1カウンタの値と、前記第2計時手段の前記第4カウンタの値と、から前記第2誤り検出符号を生成する、

請求項1から4のいずれか1項に記載の通信システム。

[請求項6] 前記第2誤り検出手段は、生成した前記第2誤り検出符号が、前記フレームに含まれる前記第1誤り検出符号に対して設定された条件を満たさないと判別すると、前記フレームを破棄する、

請求項1から5のいずれか1項に記載の通信システム。

[請求項7] 前記第2誤り検出手段は、生成した前記第2誤り検出符号が、前記

フレームに含まれる前記第 1 誤り検出符号と一致するか否かを判別する、

請求項 1 から 6 のいずれか 1 項に記載の通信システム。

[請求項 8] 前記第 2 誤り検出手段は、前記第 3 カウンタの値が示す時刻と、前記フレームに含まれる前記第 1 カウンタの値が示す時刻と、から前記フレームが設定された時間内に前記第 2 通信装置に到達したか否かを判別し、前記フレームが設定された時間内に前記第 2 通信装置に到達していないと判別すると、前記フレームを破棄する、

請求項 1 から 7 のいずれか 1 項に記載の通信システム。

[請求項 9] 前記第 1 通信装置は、

前記設定されたタイミングを示す情報と、前記設定された方式を示す情報とを記憶する第 1 記憶手段、

を有し、

前記第 2 通信装置は、

前記設定されたタイミングを示す情報と、前記設定された方式を示す情報とを記憶する第 2 記憶手段、

を有する、

請求項 1 から 8 のいずれか 1 項に記載の通信システム。

[請求項 10] 前記第 1 通信装置は、

前記設定されたタイミングを示す情報と、前記設定された方式を示す情報とを記憶する第 1 記憶手段と、

前記第 2 通信装置に、前記第 1 記憶手段に格納した情報を提供する通知手段と、

を有する、

請求項 1 から 8 のいずれか 1 項に記載の通信システム。

[請求項 11] 他の通信装置と通信する通信装置であって、

前記他の通信装置は、時間経過をカウントする第 1 カウンタと、前記第 1 カウンタの桁あふれをカウントする第 2 カウンタとを備えてお

り、予め設定されたタイミングで、予め設定された方式を使用して生成した値で、前記第2カウンタの値を置き換えて、前記第2カウンタが取る値を分散させ、前記第1カウンタの値と、前記第2カウンタの値とから第1誤り検出符号を生成し、前記通信装置へ宛てたデータに前記第1カウンタの値と前記第1誤り検出符号とを付加したフレームを生成し、生成した前記フレームを前記通信装置に送信し、

前記通信装置は、

時間経過をカウントする第3カウンタと、前記第3カウンタの桁あふれをカウントする第4カウンタとを備える第2計時手段と、

前記設定されたタイミングで、前記設定された方式を使用して生成した値で、前記第4カウンタの値を置き換えて、前記第4カウンタが取る値を分散させる第2データ変換手段と、

前記他の通信装置から前記フレームを受信する第2通信手段と、

前記フレームに含まれる前記第1カウンタの値と、前記第2計時手段の前記第4カウンタの値と、から第2誤り検出符号を生成し、生成した前記第2誤り検出符号が、前記フレームに含まれる前記第1誤り検出符号に対して設定された条件を満たすか否かを判別する第2誤り検出手段と、

を有する、

通信装置。

[請求項12]

第1通信装置と第2通信装置とが相互に通信する方法であって、

前記第1通信装置が、時間経過をカウントする第1カウンタと、前記第1カウンタの桁あふれをカウントする第2カウンタとを備える第1計時手段を有し、

前記第2通信装置が、時間経過をカウントする第3カウンタと、前記第3カウンタの桁あふれをカウントする第4カウンタとを備える第2計時手段を有し、

前記第1通信装置が、予め設定された方法で、前記第2カウンタが

取る値を分散させるステップと、

前記第1通信装置が、前記第1カウンタの値と、前記第2カウンタの値とから第1誤り検出符号を生成するステップと、

前記第1通信装置が、前記第2通信装置へ宛てたデータに前記第1カウンタの値と前記第1誤り検出符号とを付加したフレームを生成し、生成した前記フレームを前記第2通信装置に送信するステップと、

前記第2通信装置が、前記第1通信装置と同じ方法で、前記第4カウンタが取る値を分散させるステップと、

前記第2通信装置が、前記第1通信装置から前記フレームを受信するステップと、

前記第2通信装置が、前記フレームに含まれる前記第1カウンタの値と、前記第2計時手段の前記第4カウンタの値と、から第2誤り検出符号を生成し、生成した前記第2誤り検出符号が、前記フレームに含まれる前記第1誤り検出符号に対して設定された条件を満たすか否かを判別するステップと、

を含む方法。

[請求項13]

第1のコンピュータと第2のコンピュータとが相互に通信する通信システムにおいて、

前記第1のコンピュータに、時間経過をカウントする第1カウンタと、前記第1カウンタの桁あふれをカウントする第2カウンタとを備える第1計時手段を実現させ、

前記第1のコンピュータに、予め設定された方法で前記第2カウンタの値を分散させ、

前記第1のコンピュータに、前記第1カウンタの値と、前記第2カウンタの値とから第1誤り検出符号を生成させ、前記第2のコンピュータへ宛てたデータに前記第1カウンタの値と前記第1誤り検出符号とを付加したフレームを生成させ、前記フレームを前記第2のコンピュータに送信させ、

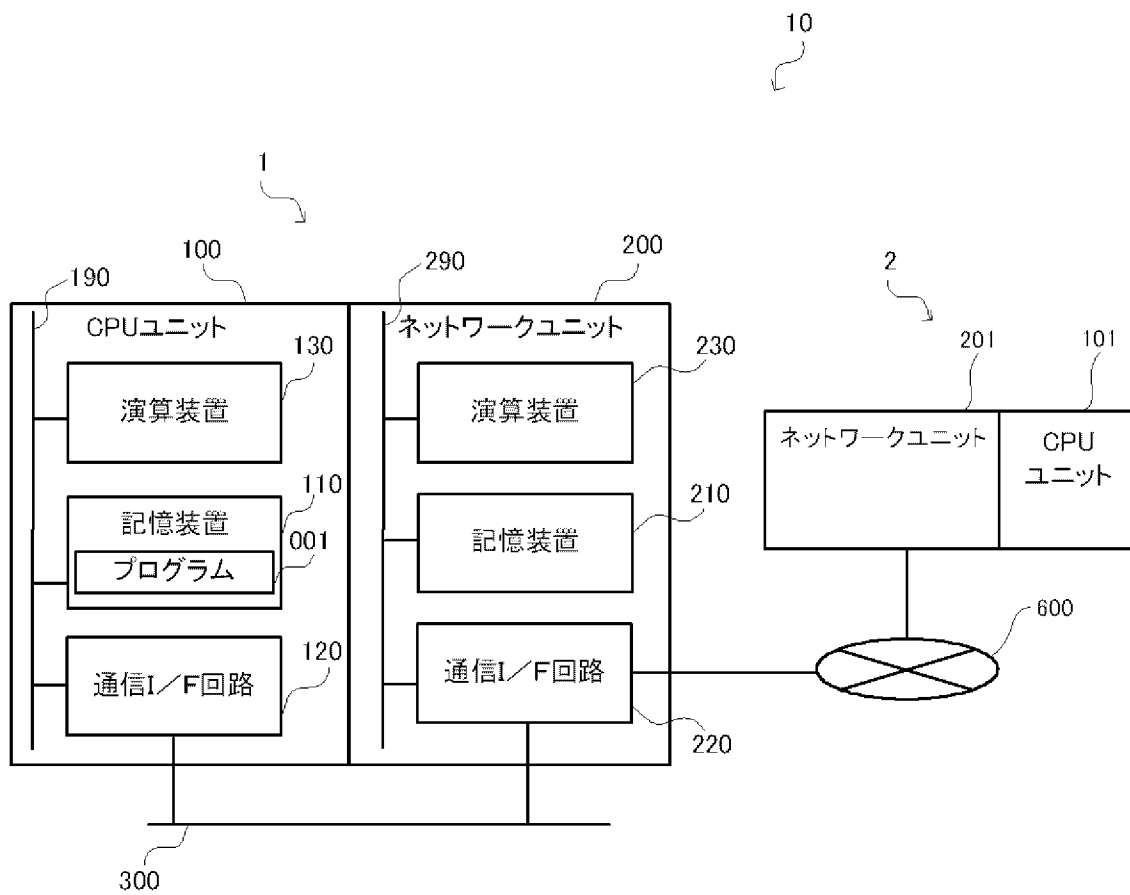
前記第2のコンピュータに、時間経過をカウントする第3カウンタと、前記第3カウンタの桁あふれをカウントする第4カウンタとを備える第2計時手段を実現させ、

前記第2のコンピュータに、前記第1のコンピュータと同じ方法で前記第4カウンタの値を分散させ、

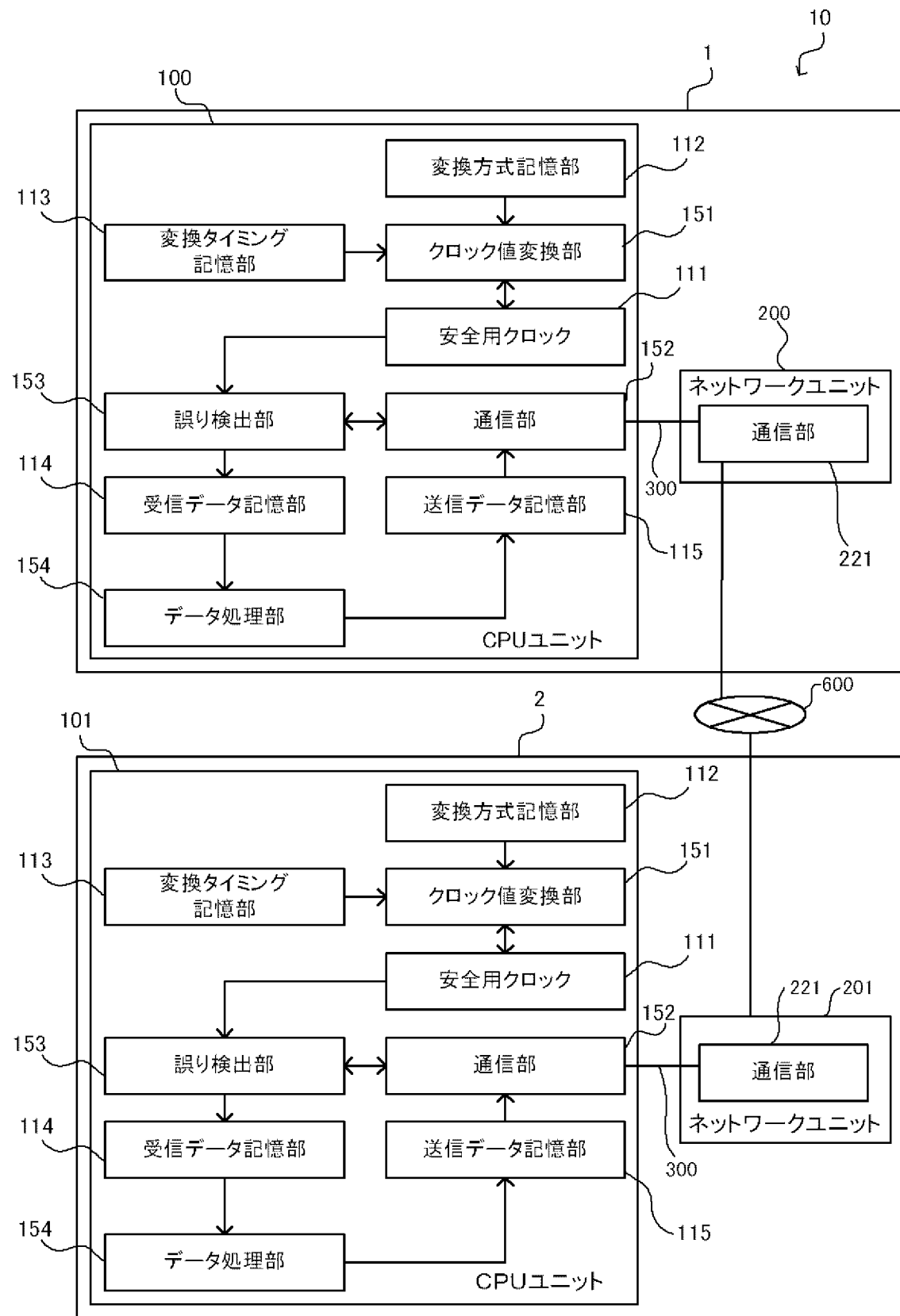
前記第2のコンピュータに、前記第1のコンピュータから送信された前記フレームに含まれる前記第1カウンタの値と、前記第2計時手段の前記第4カウンタの値と、から第2誤り検出符号を生成させ、前記第2誤り検出符号が前記フレームに含まれる前記第1誤り検出符号に対して設定された条件を満たすか否かを判別させる、

プログラム。

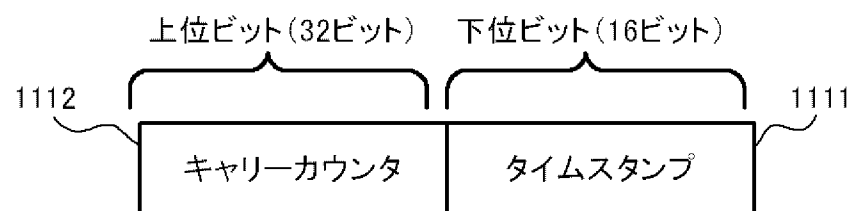
[図1]

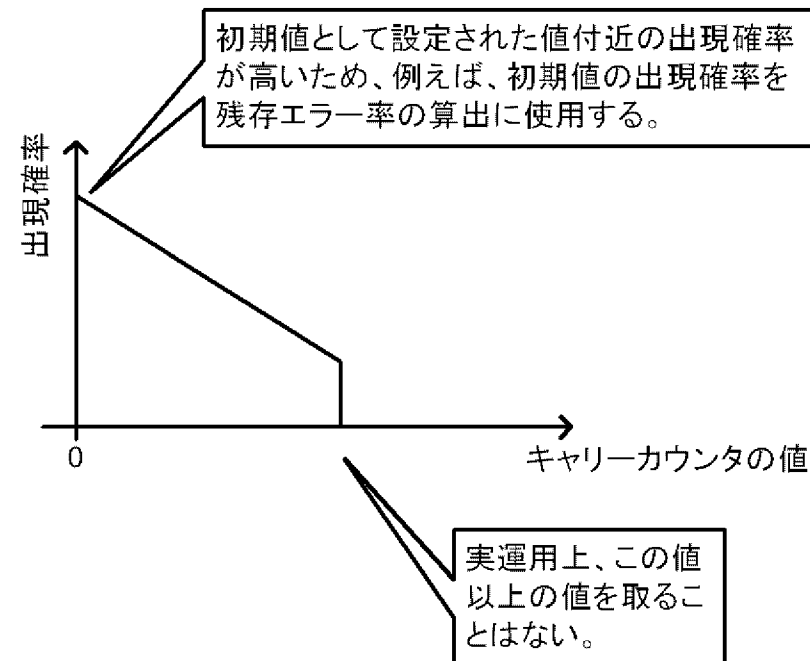
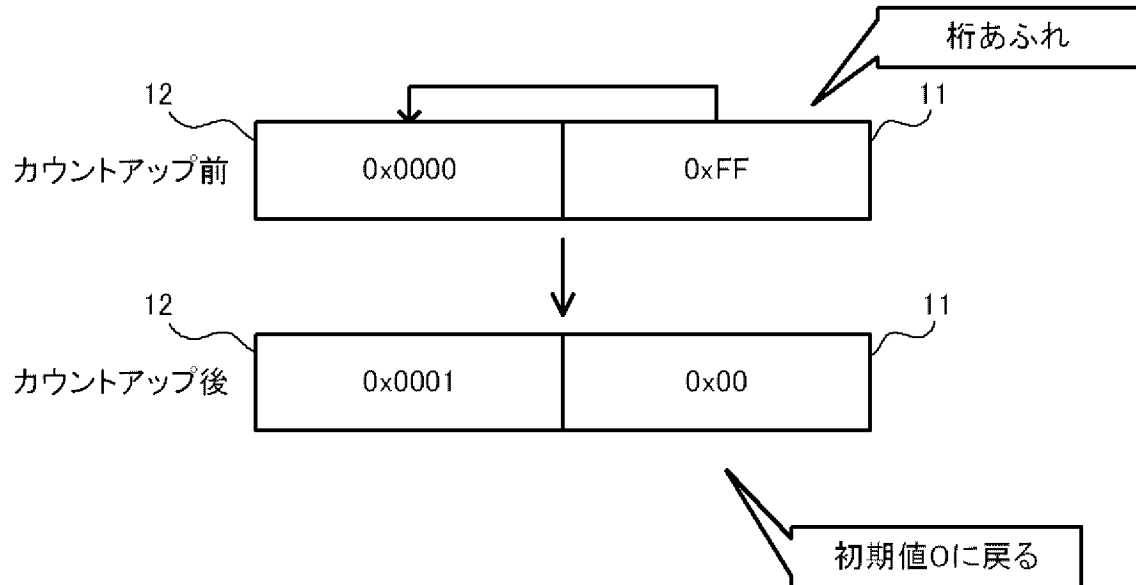
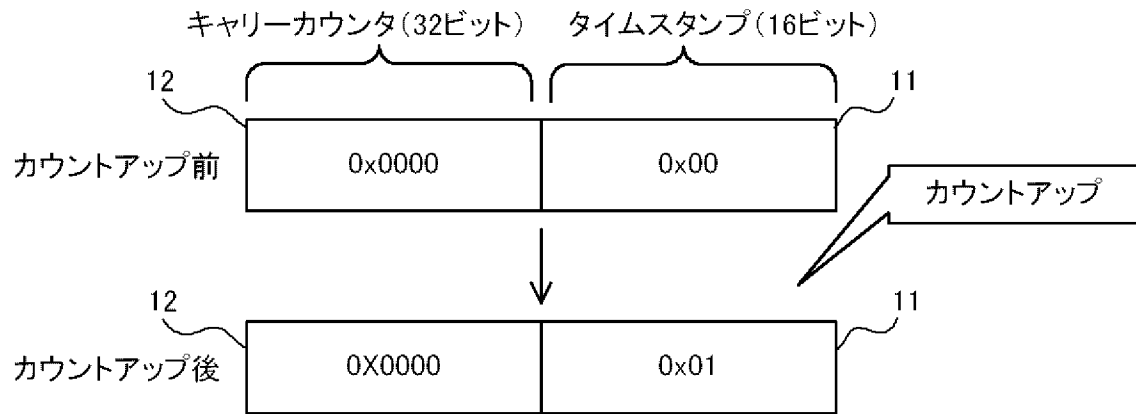


[図2]

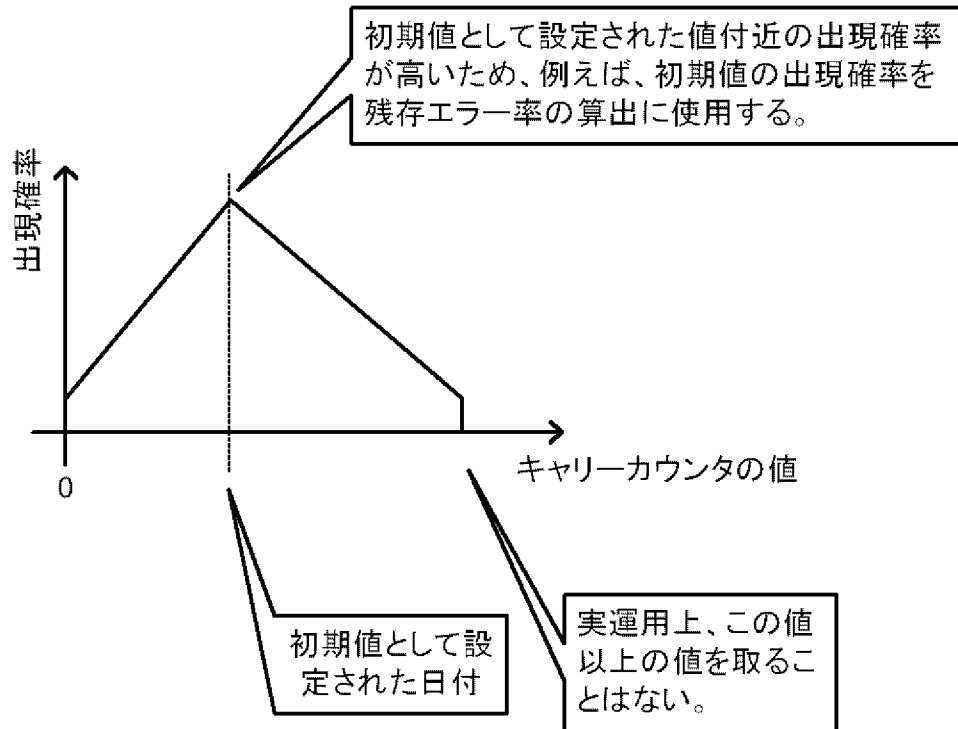


[図3]

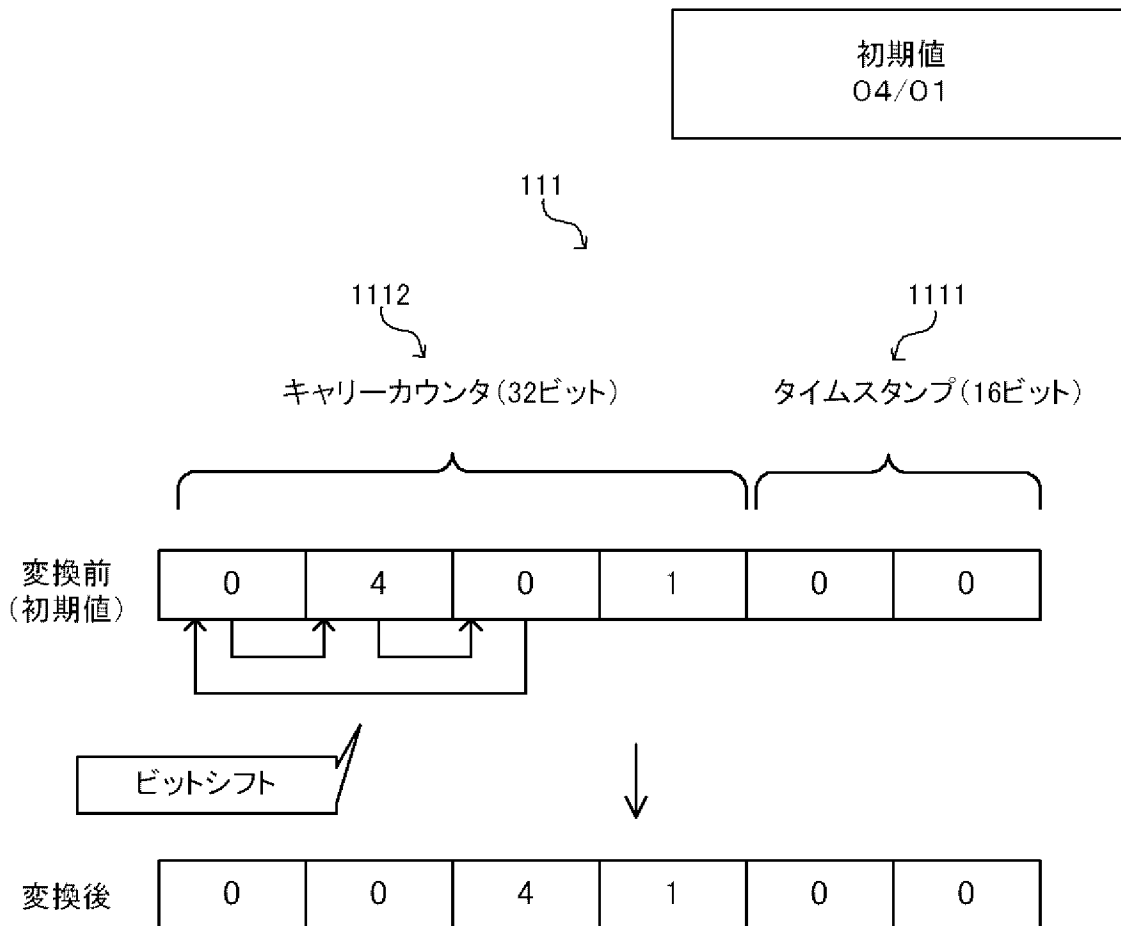




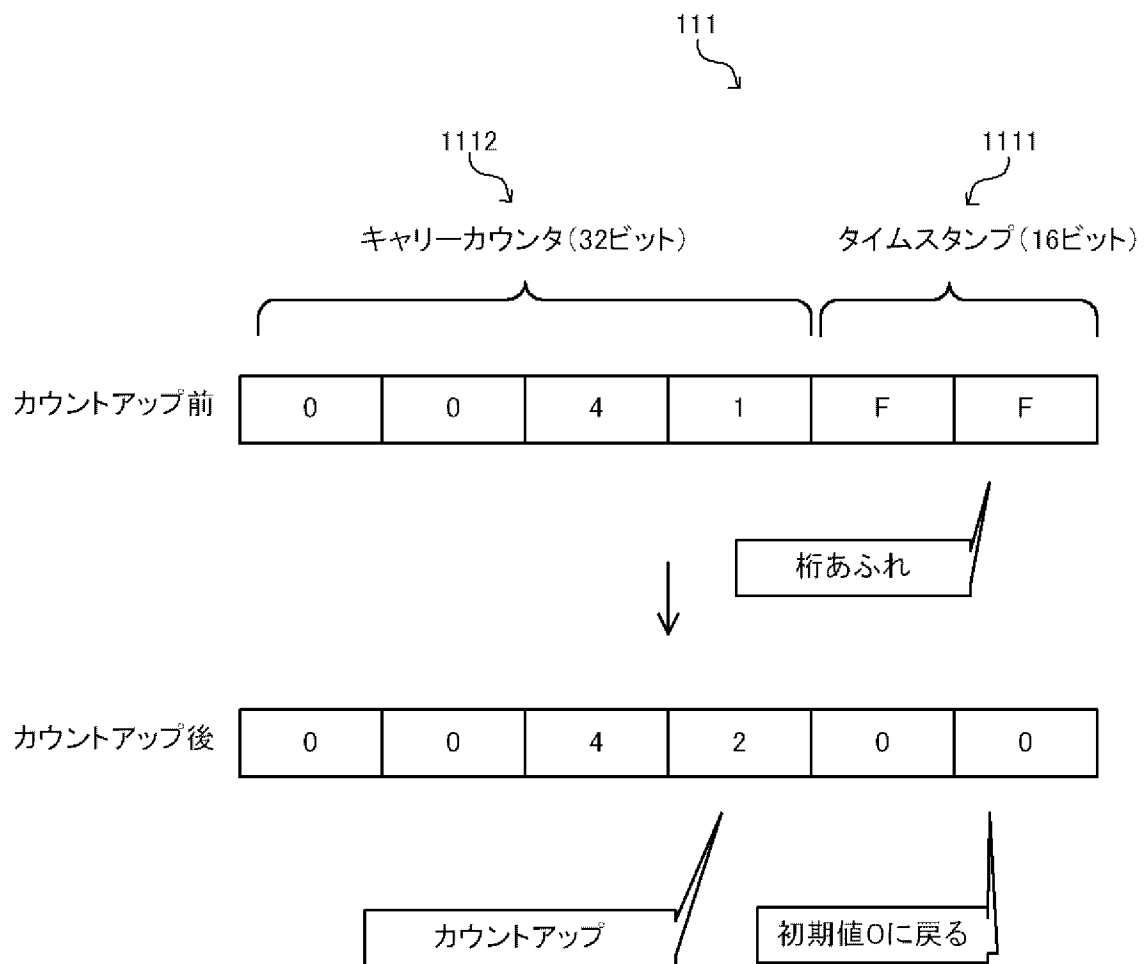
[図5B]



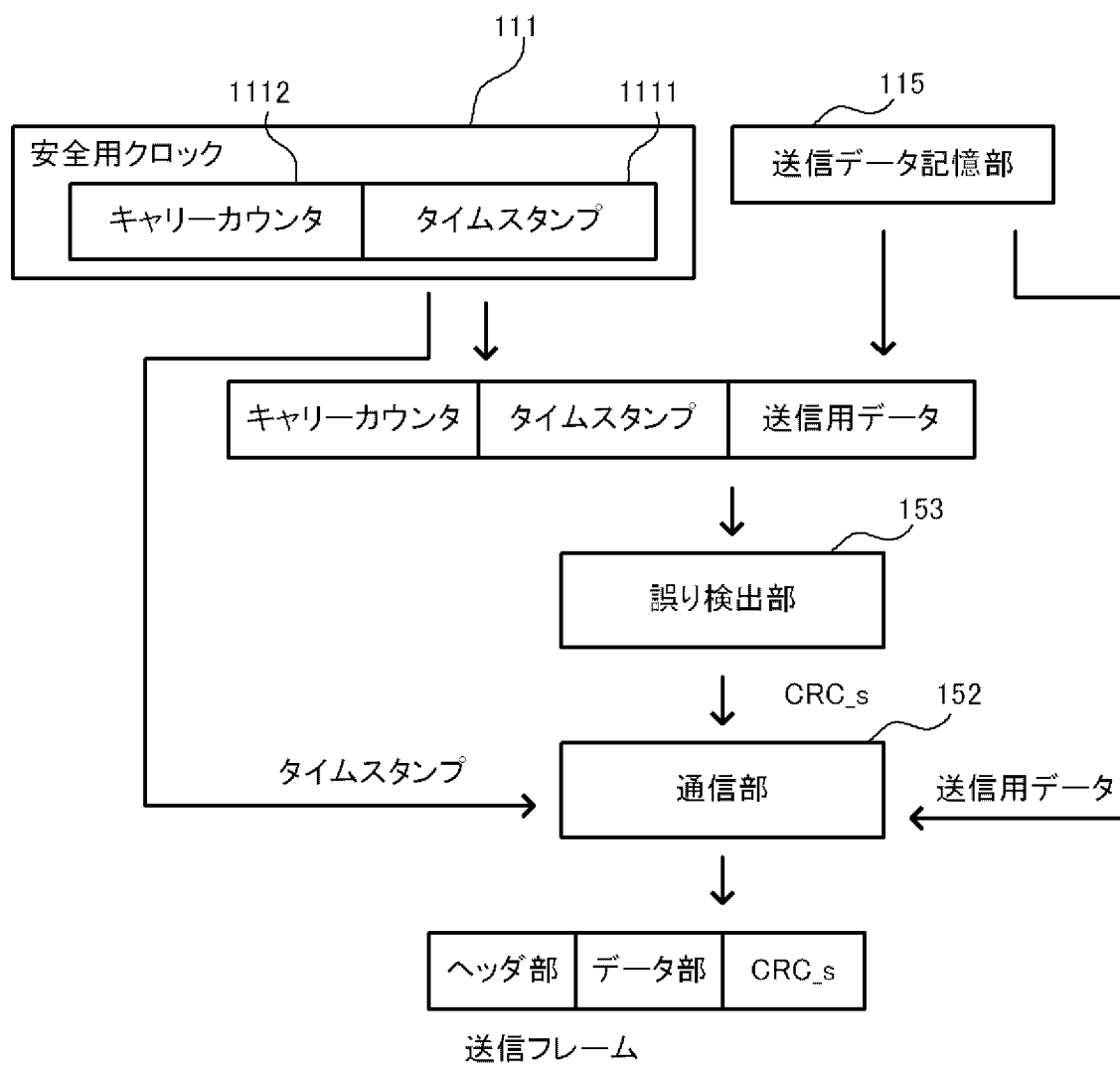
[図6]



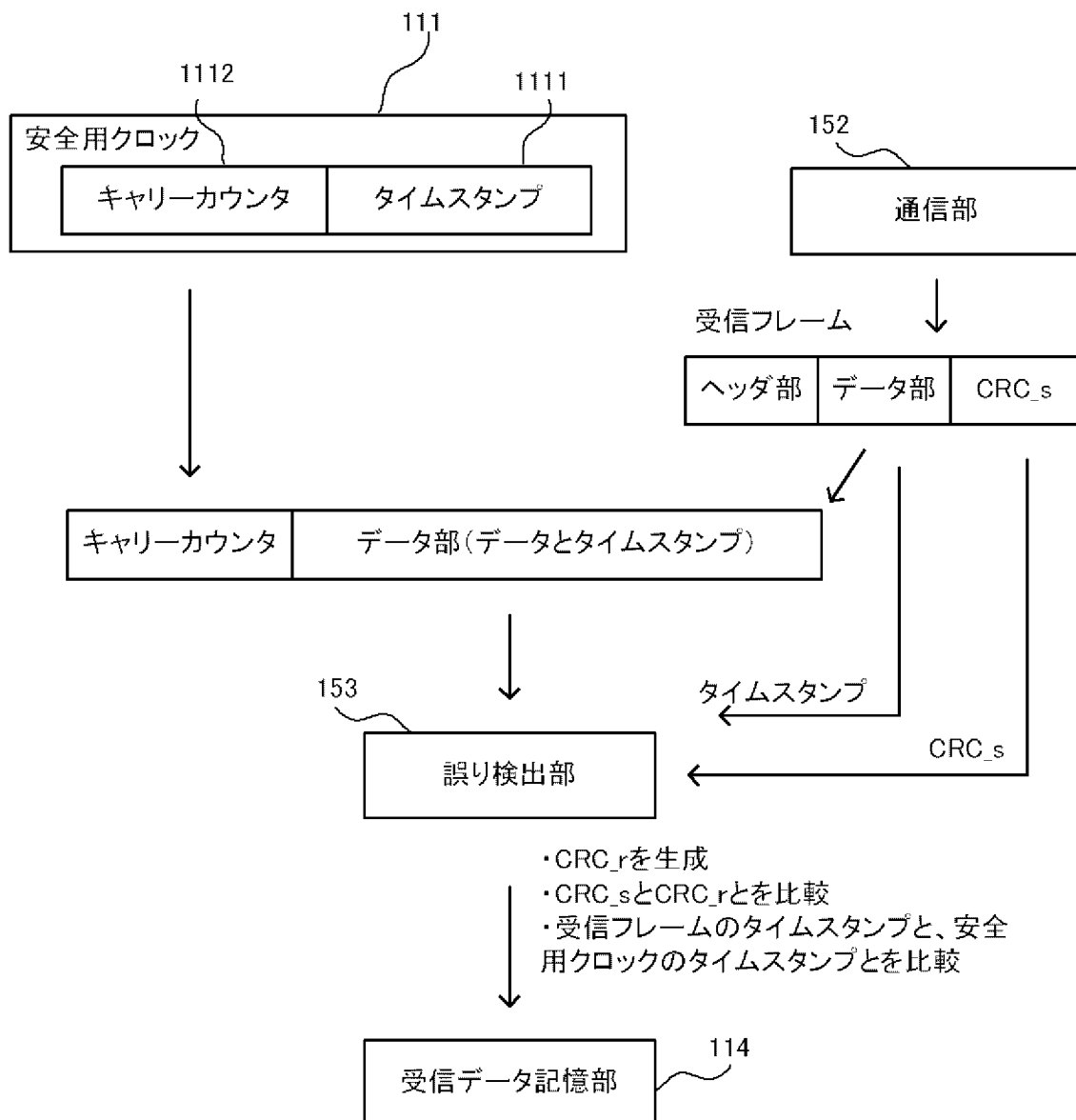
[図7]



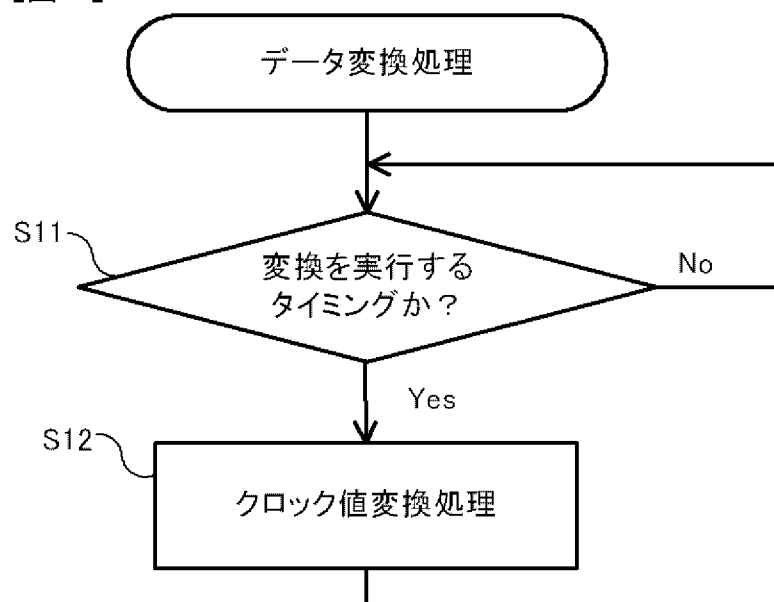
[図8]



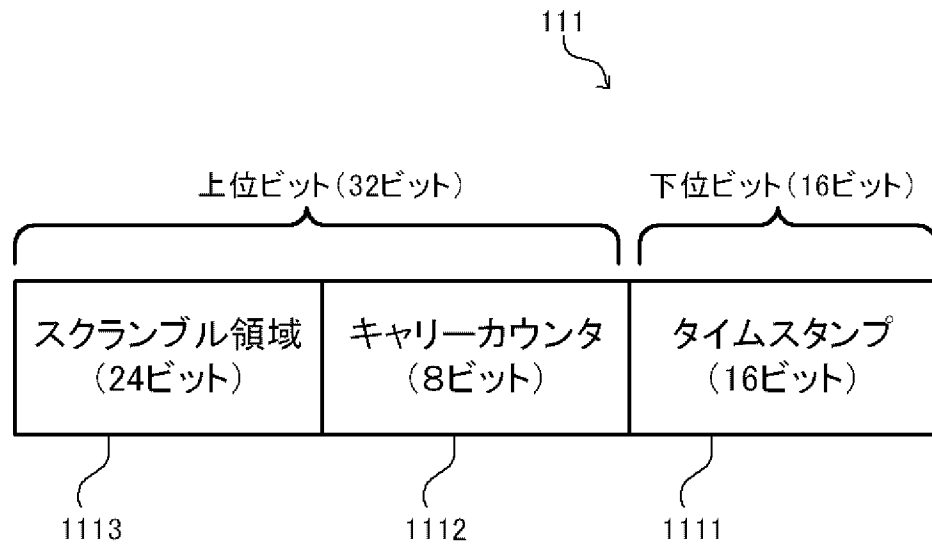
[図9]



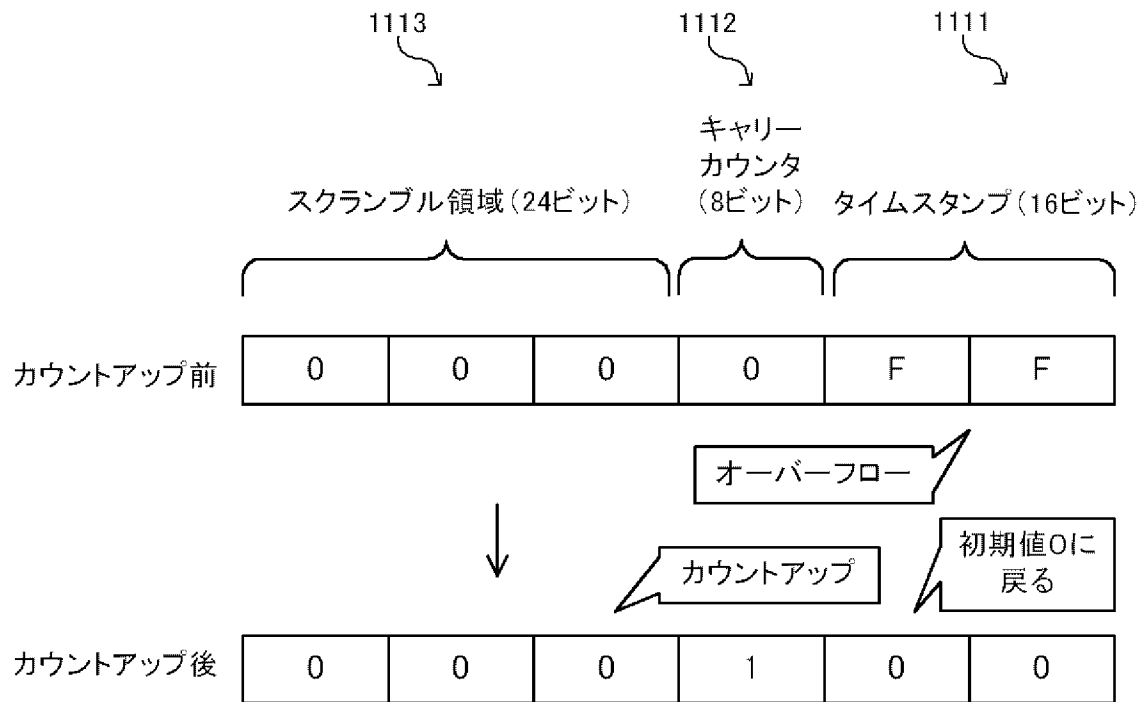
[図10]



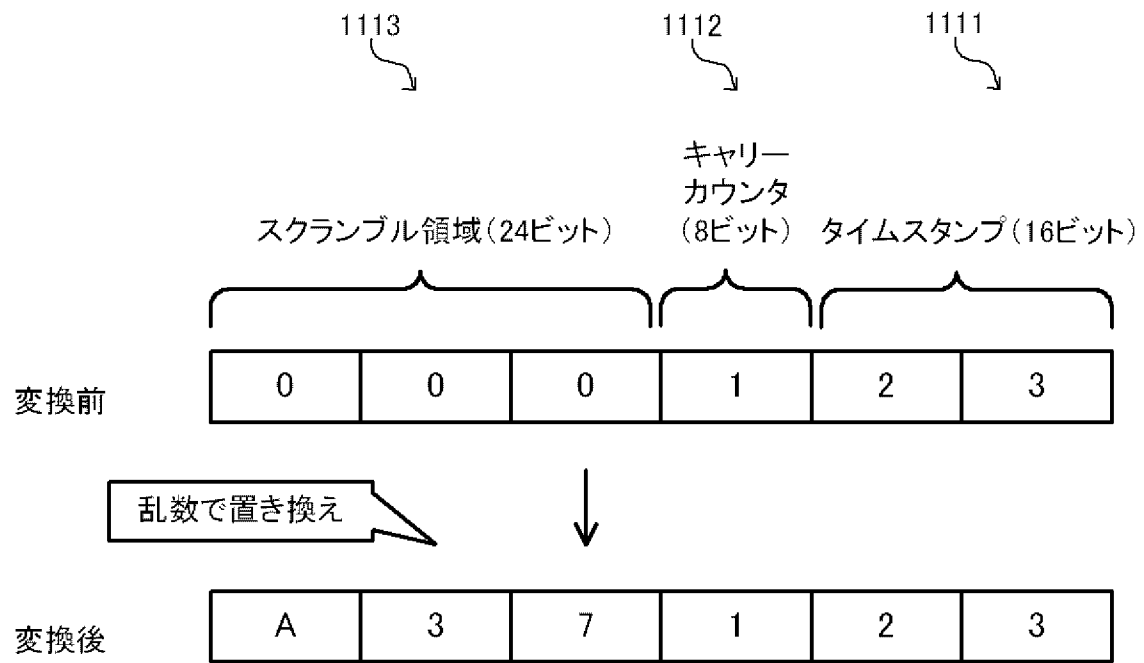
[図11]



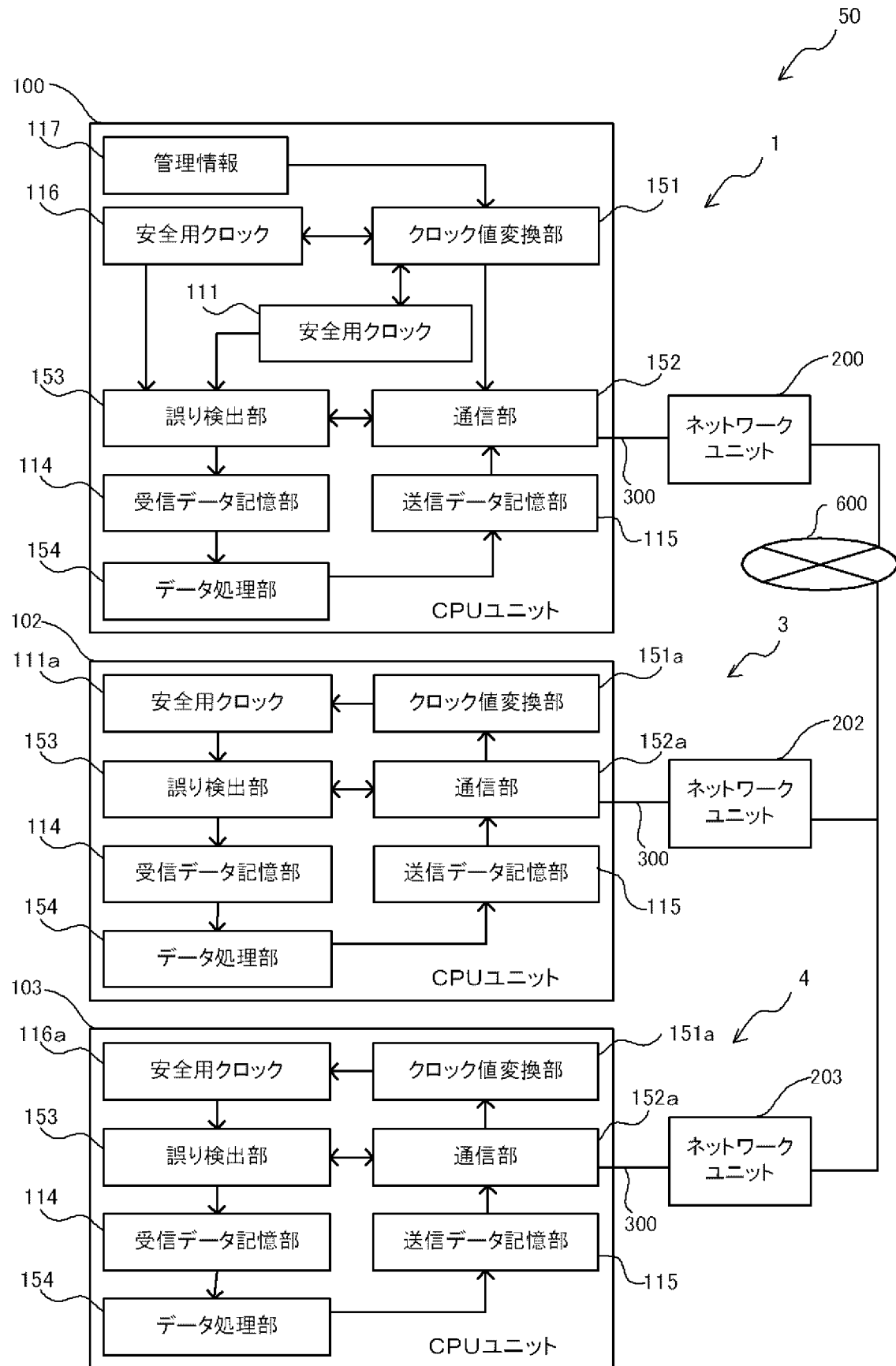
[図12]



[図13]



[図14]



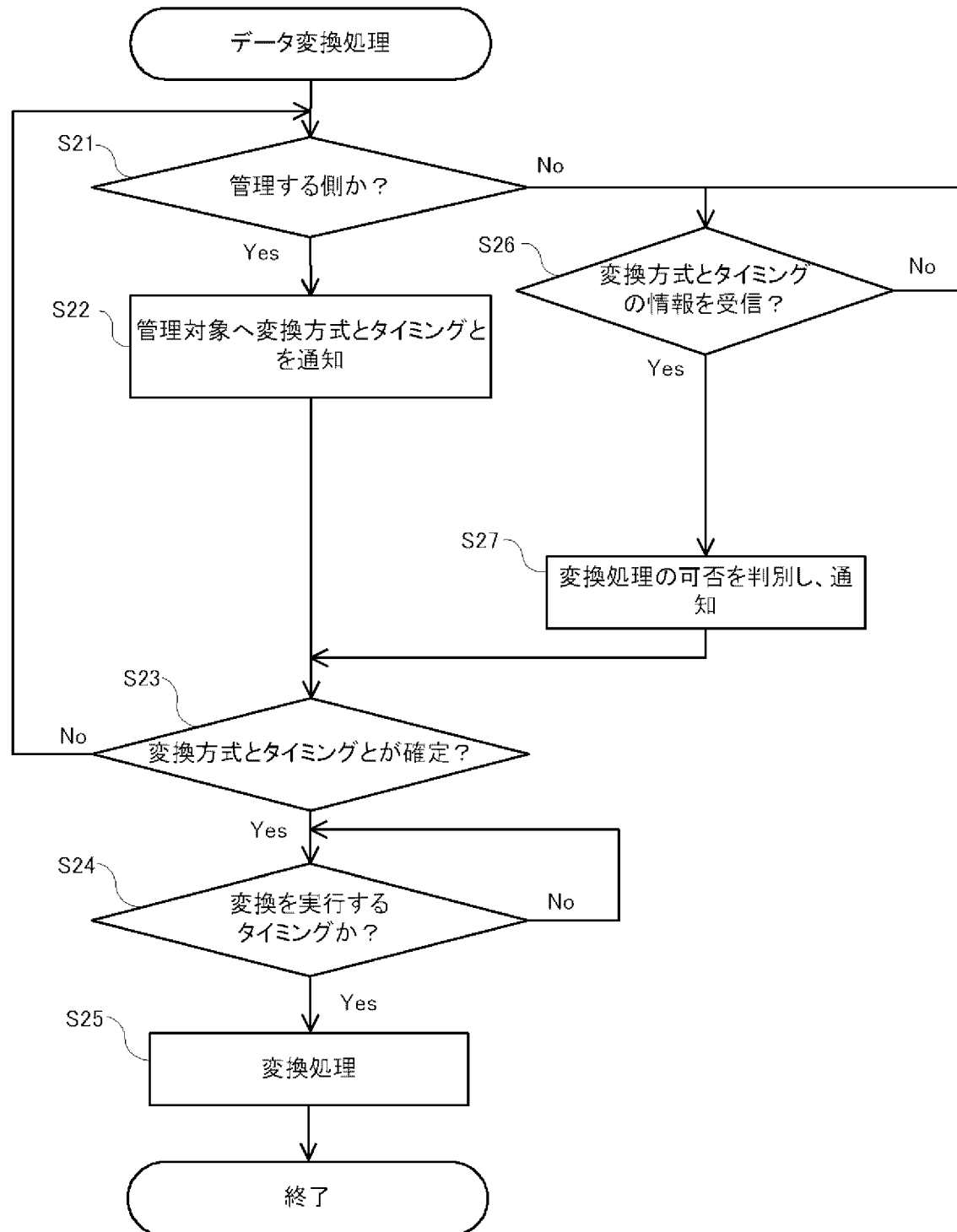
117

[図15]

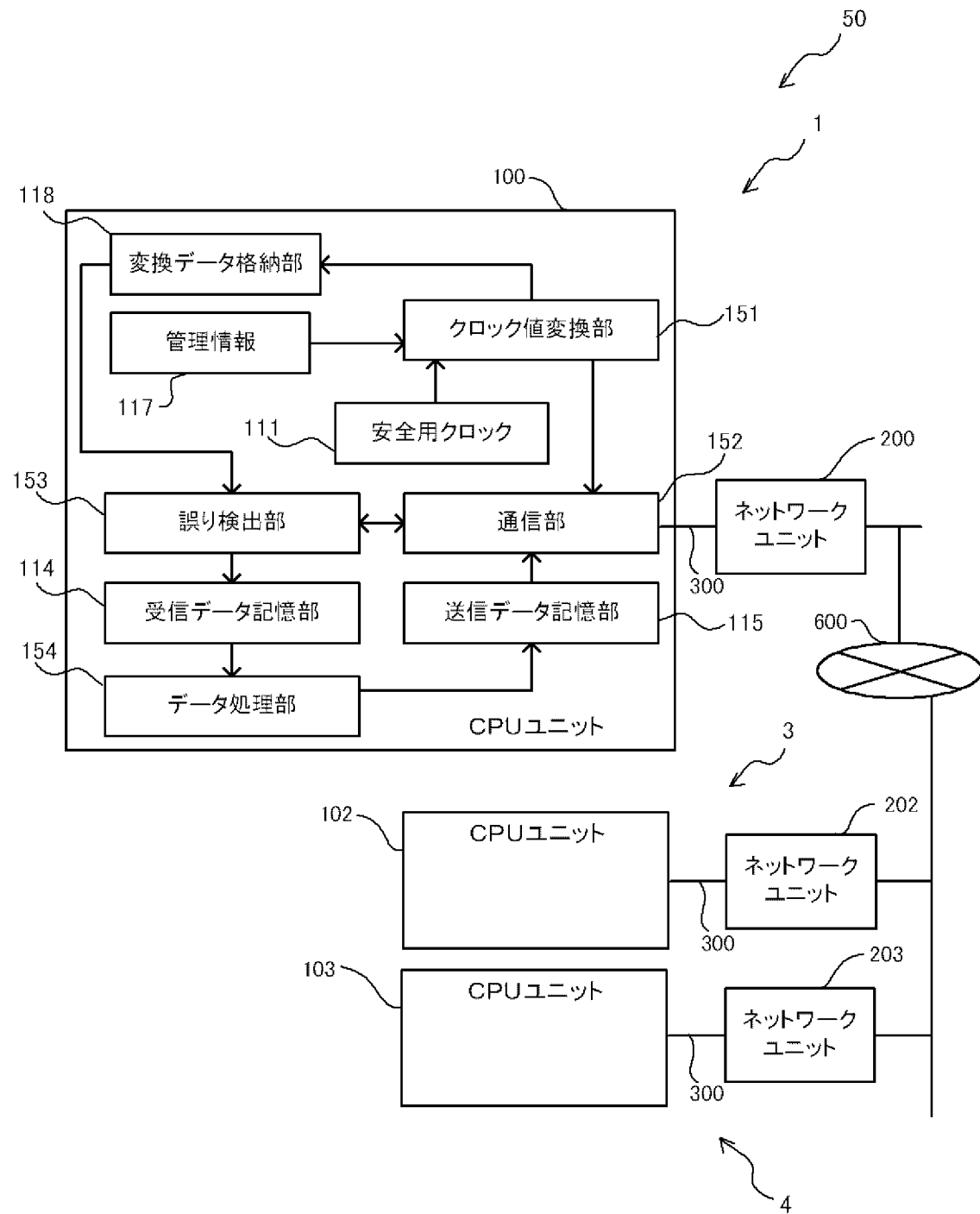
管理情報

管理対象	安全用クロック	変換方式	変換タイミング
プログラマブル ロジックコントローラ3	安全用クロック111a	ビットシフト; 上位24ビットを、右に、8ビット 単位で循環シフトする。	2ミリ秒毎
プログラマブル ロジックコントローラ4	安全用クロック116a	乱数生成: アルゴリズム2000、 シード3000Y	1ミリ秒毎

[図16]



[図17]



[図18]

118

管理対象	安全用クロック	変換後の キャリーカウンタの値
プログラマブルロジック コントローラ3	安全用クロック111a	XXXX
プログラマブルロジック コントローラ4	安全用クロック116a	XXXX

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2018/033097

A. CLASSIFICATION OF SUBJECT MATTER

Int. Cl. H04L1/00 (2006.01) i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

Int. Cl. H04L1/00

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

Published examined utility model applications of Japan 1922-1996

Published unexamined utility model applications of Japan 1971-2018

Registered utility model specifications of Japan 1996-2018

Published registered utility model applications of Japan 1994-2018

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	五十嵐俊介, CC-Link IE フィールド安全通信技術, 三菱電機技報, 25 April 2011, vol. 85, no. 4, pp. 37-40, ISSN 0369-2302, in particular, Sections 2-3 (IGARASHI, Shunsuke. CC-Link IE Field Safety Telecommunication Technology. Mitsubishi Denki Gihō.)	1-13
A	US 2016/0218946 A1 (BECKHOFF AUTOMATION GMBH & CO. KG) 28 June 2016, abstract, paragraphs [0040], [0046] & WO 2016/059100 A1 & DE 102014114883 A1	1-13
A	US 2004/0008681 A1 (GOVINDARAJAN, Priya) 15 January 2004, paragraphs [0037], [0038] (Family: none)	1-13

☐

Further documents are listed in the continuation of Box C.

☐

See patent family annex.

* Special categories of cited documents:

“A” document defining the general state of the art which is not considered to be of particular relevance

“E” earlier application or patent but published on or after the international filing date

“L” document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

“O” document referring to an oral disclosure, use, exhibition or other means

“P” document published prior to the international filing date but later than the priority date claimed

“T” later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

“X” document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

“Y” document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

“&” document member of the same patent family

Date of the actual completion of the international search
19.10.2018Date of mailing of the international search report
06.11.2018Name and mailing address of the ISA/
Japan Patent Office
3-4-3, Kasumigaseki, Chiyoda-ku,
Tokyo 100-8915, Japan

Authorized officer

Telephone No.

A. 発明の属する分野の分類 (国際特許分類 (IPC))

Int.Cl. H04L1/00 (2006.01) i

B. 調査を行った分野

調査を行った最小限資料 (国際特許分類 (IPC))

Int.Cl. H04L1/00

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	1922-1996年
日本国公開実用新案公報	1971-2018年
日本国実用新案登録公報	1996-2018年
日本国登録実用新案公報	1994-2018年

国際調査で使用した電子データベース (データベースの名称、調査に使用した用語)

C. 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求項の番号
A	五十嵐 俊介, CC-Link IE フィールド安全通信技術, 三菱電機技報, 2011.04.25, 第85巻, 第4号, p.37~40, ISSN 0369-2302, 特に第2節~第3節 (IGARASHI, Shunsuke, CC-Link IE Field Safety Telecommunication Technology)	1-13
A	US 2016/0218946 A1 (BECKHOFF AUTOMATION GMBH & CO. KG) 2016.06.28, 要約, 段落[0040], [0046] & WO 2016/059100 A1 & DE 10 2014 114883 A1	1-13

C欄の続きにも文献が列挙されている。

パテントファミリーに関する別紙を参照。

* 引用文献のカテゴリー

「A」 特に関連のある文献ではなく、一般的技術水準を示すもの
「E」 国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「L」 優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献 (理由を付す)
「O」 口頭による開示、使用、展示等に言及する文献
「P」 国際出願日前で、かつ優先権の主張の基礎となる出願

の日の後に公表された文献

「T」 国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「X」 特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Y」 特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「&」 同一パテントファミリー文献

国際調査を完了した日

19.10.2018

国際調査報告の発送日

06.11.2018

国際調査機関の名称及びあて先

日本国特許庁 (ISA/J P)

郵便番号 100-8915

東京都千代田区霞が関三丁目4番3号

特許庁審査官 (権限のある職員)

川口 貴裕

5 K

3055

電話番号 03-3581-1101 内線 3556

C (続き) . 関連すると認められる文献		
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求項の番号
A	US 2004/0008681 A1 (GOVINDARAJAN, Priya) 2004.01.15, 段落[0037]～[0038] (ファミリー無し)	1-13