

(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
2019年10月31日(31.10.2019)



(10) 国際公開番号

WO 2019/207697 A1

(51) 国際特許分類:
H04L 1/00 (2006.01)

(21) 国際出願番号: PCT/JP2018/016884

(22) 国際出願日: 2018年4月25日(25.04.2018)

(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:宮▲崎▼ 清人(MIYAZAKI, Kiyohito); 〒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).

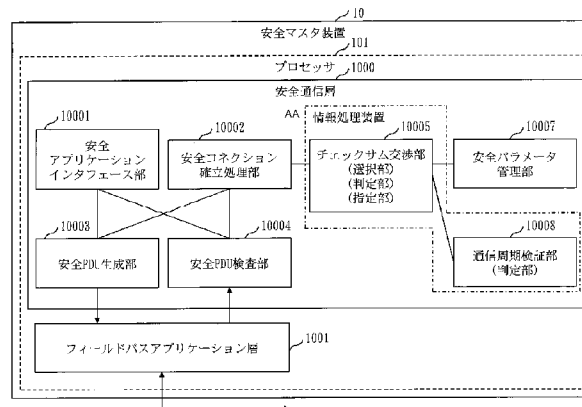
伊藤 直輝(ITO, Naoki); 〒1008310 東京都千代田区丸の内二丁目7番3号 三菱電機株式会社内 Tokyo (JP).

(74) 代理人: 溝井 国際特許業務法人(MIZOI INTERNATIONAL PATENT FIRM); 〒2470056 神奈川県鎌倉市大船二丁目17番10号3階 Kanagawa (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,

(54) **Title:** INFORMATION PROCESSING DEVICE, INFORMATION PROCESSING METHOD, AND INFORMATION PROCESSING PROGRAM

(54) 発明の名称: 情報処理装置、情報処理方法及び情報処理プログラム



10 Safety master device
101 Processor
1000 Safety communication layer
1001 Fieldbus application layer
10001 Safety application interface unit
10002 Safety connection establishment processing unit
10003 Safety PDU generating unit
10004 Safety PDU checking unit
10005 Checksum negotiating unit
(Selection unit)
(Determination unit)
(Specification unit)
10007 Safety parameter managing unit
10008 Communication period verifying unit
(Determination unit)
AA Information processing device

(57) **Abstract:** A checksum negotiating unit (10005) selects, from a plurality of polynomials a candidate for a generator polynomial used for communication between a safety master device (10) and a safety slave device (20), as a candidate polynomial. A communication period verifying unit (10008) determines whether a calculation using the candidate polynomial is completed in each of the safety master device (10) and the safety slave device (20) by a prescribed deadline. The communication period verifying unit (10008) specifies the candidate polynomial as a generator polynomial when the

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.

- (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)）

calculation using the candidate polynomial is determined to be completed in each of the safety master device (10) and the safety slave device (20) by the deadline.

(57) 要約：チェックサム交渉部（10005）は、安全マスタ装置（10）と安全スレーブ装置（20）との間の通信で用いられる生成多項式の候補を複数の多項式の中から候補多項式として選択する。通信周期検証部（10008）は、候補多項式を用いた計算が安全マスタ装置（10）及び安全スレーブ装置（20）の各々で規定の期限までに完了するか否かを判定する。通信周期検証部（10008）は、候補多項式を用いた計算が安全マスタ装置（10）及び安全スレーブ装置（20）の各々で期限までに完了すると判定された場合に、候補多項式を生成多項式に指定する。

明 細 書

発明の名称：

情報処理装置、情報処理方法及び情報処理プログラム

技術分野

[0001] 本発明は、生成多項式の指定に関する。

背景技術

[0002] IEC (International Electrotechnical Commission) 61784-3に基づく安全通信では、伝送路で生じるビットエラーなどに対する安全PDU (Protocol Data Unit) の完全性を、安全度水準に基づく要求値未満にする必要がある。完全性を確保するための代表的な安全対策として、CRC (Cyclic Redundancy Check) などのチェックサムが広く利用されている。

CRC計算は一般的に処理量が大きいため、一般的な通信ではハードウェアにより行われるが、安全通信ではソフトウェアにより行われるケースが多い。CRC計算がハードウェアにより行われるケースでは、IEC 61508に基づくハードウェアの診断が必要であるため、処理負荷が増大する。この処理負荷の増大を避けるために、安全通信ではCRC計算がソフトウェアで行われることが多い。

CRCには、CRC-16やCRC-32のように次数の異なる複数のバリエーションがある。一般に次数の大きいCRC多項式ほどエラーの検出能力が高く、低い残存エラーレートを達成できるが、一方で計算量（時間または空間）が大きくなってしまう。

こうした計算量の問題は、計算リソースが潤沢な機器では問題になりにくい。が、計算リソースが限られ、かつ、規定時間内に処理を完了しなければならない組み込み機器では問題となる。

[0003] 特許文献1の技術では、与えられたデータ長及びデータ種別に対して、未

検出誤り率を最小とするようなCRC生成多項式が選択される。

このために、特許文献1の技術では、生成多項式の最大及び最小ハミング距離をあらゆる符号長に対して求めるステップと、送受信するデータのデータ長及びデータ種別に応じて、最小ハミング距離が最大となる生成多項式を選択するステップとが存在する。

先行技術文献

特許文献

[0004] 特許文献1：特開2009-171539号公報

発明の概要

発明が解決しようとする課題

[0005] 特許文献1の技術では、未検出誤り率の最小化のみが考慮されている。このため、計算リソースが限られた条件下では、安全通信において求められる安全応答時間内に必要な処理を完了することができないという課題がある。なお、安全応答時間は、例えば安全センサなどでの検知が発生してから、制御対象のアクチュエータなどを安全状態に遷移させるまでの時間である。安全応答時間の要求値は、システム構成を踏まえて決定される。また、安全応答時間の構成要素の一つに安全通信周期がある。

一般的に、CRC多項式の未検出誤り率を低くするためには、次数の大きい多項式が必要である。次数の大きい多項式が用いられると、CRC算出に必要な計算量が大きくなり、安全通信周期の制約を満たしにくくなる。そこで、マージンをもって小さめに設定されている安全通信周期を、マージンの範囲内で大きく設定することが考えられる。しかし、この方法では通信エラーによって安全PDUが規定時間内に送受信されない確率が増す。このため、システムが必要以上に安全状態に遷移してしまい、システムの可用性が低下してしまう問題が生じる。

[0006] 本発明は、このような事情に鑑み、計算リソースが限られた条件下でも規定の期限までに計算を完了させることができる多項式を指定することができ

る構成を得ることを主な目的とする。

課題を解決するための手段

[0007] 本発明に係る情報処理装置は、

マスタ装置とスレーブ装置との間の通信で用いられる生成多項式の候補を複数の多項式の中から候補多項式として選択する選択部と、

前記候補多項式を用いた計算が前記マスタ装置及び前記スレーブ装置の各々で規定の期限までに完了するか否かを判定する判定部と、

前記候補多項式を用いた計算が前記マスタ装置及び前記スレーブ装置の各々で前記期限までに完了すると前記判定部により判定された場合に、前記候補多項式を前記生成多項式に指定する指定部とを有する。

発明の効果

[0008] 本発明によれば、計算リソースが限られた条件下でも規定の期限までに計算を完了させることができる多項式を指定することができる。

図面の簡単な説明

[0009] [図1]実施の形態1に係る安全通信システムの構成例を示す図。

[図2]実施の形態1に係る安全マスタ装置のハードウェア構成例を示す図。

[図3]実施の形態1に係る安全スレーブ装置のハードウェア構成例を示す図。

[図4]実施の形態1に係る安全マスタ装置の機能構成例を示す図。

[図5]実施の形態1に係る安全スレーブ装置の機能構成例を示す図。

[図6]実施の形態1に係る安全コネクションを確立する処理を示すフローチャート。

[図7]実施の形態1に係る安全コネクションを確立する処理を示すフローチャート。

[図8]実施の形態1に係る安全コネクションを確立する処理を示すフローチャート。

[図9]実施の形態1に係るCRC多項式テーブルの例を示す図。

[図10]実施の形態2に係る安全コネクションを確立する処理を示すフローチャート。

[図11]実施の形態2に係る計算能力情報の例を示す図。

[図12]実施の形態3に係るCRC多項式テーブルの例を示す図。

[図13]実施の形態4に係る情報処理装置のハードウェア構成例を示す図。

[図14]実施の形態4に係る情報処理装置の機能構成例を示す図。

[図15]実施の形態4に係る情報処理装置の動作例を示すフローチャート。

発明を実施するための形態

[0010] 以下、本発明の実施の形態について、図を用いて説明する。以下の実施の形態の説明及び図面において、同一の符号を付したものは、同一の部分又は相当する部分を示す。

[0011] 実施の形態1.

概要

本実施の形態では、安全通信に必要なCRC計算の処理量の削減を、安価な組込み機器で実現可能する構成を説明する。具体的には、本実施の形態では、規格で要求される残存エラーレートと、システムに要求される安全通信周期とを両立できる最適なCRC多項式の選択を、計算リソースが限られているマイクロコンピュータで実現できる構成を説明する。

[0012] 安全規格で要求される残存エラーレートについては、国際規格であるIEC 61784-3において、下記によって定まる残存エラーレートが、目標とする安全度水準ごとに定められた要求値未満となることが求められている（括弧内に各値と残存エラーレートとの関係を示す）。

- ・安全PDUのサイズ n （サイズ n が小さいほど残存エラーレートは低い）

- ・安全PDUの時間あたり送信レート v （送信レート v が小さいほど残存エラーレートは低い）

- ・ビットエラー検出に使用するチェックサム生成用多項式の最小ハミング距離 h_d （最小ハミング距離 h_d が大きいほど残存エラーレートは低い）

- ・想定する伝送路のビットエラー率 P_e 。（ビットエラー率 P_e が小さいほど残存エラーレートは低い）

[0013] 安全通信周期は、許容される応答時間に基づいて設定される。システムに要求される安全応答時間から、許容される応答時間が定まる。そして、許容される応答時間に基づいて、ユーザが安全通信周期を設定する。安全通信では、規定の時間（以下、 t_r と呼ぶ）内に破損のない正常な安全PDUが受信されなければ、機器を停止させるといった安全状態に遷移する。ビットエラー等により頻繁に安全状態に遷移することを避けるために、 t_r 内に複数の安全PDUを受信するよう、安全通信周期 T_{safety} にマージンを持たせ、安全通信周期 T_{safety} として、 t_r よりも数倍小さい値を設定することが多い。

[0014] 本実施の形態では、伝送路の性能に応じて、システムの可用性を損なわない範囲で、安全通信周期を延長する。安全通信周期を延長するか否かの基準となる式の例を以下に記載する。

以下の式は、規定の時間 t_r 内に1以上の安全PDUが送信されること（式1）と、安全PDUの異常による安全停止の発生レートが要求値を下回らないこと（式2）を表す。

本実施の形態では、以下の2つの式の両方を満たす範囲で、安全通信周期が緩和（延長）される。

[0015] [数1]

$$T_{safety} < t_r \quad \cdots \text{ (式1)}$$

$$P_{fault}^{\left\lceil \frac{T_{safety}}{t_r} \right\rceil} \times v < R_{fault} \quad \cdots \text{ (式2)}$$

- [0016] ・ T_{safety} : 安全通信周期
 ・ t_r : 正常な安全PDUの受信間隔の要求値
 ・ P_{fault} : 安全PDUに発生する異常の発生確率

・ γ : 安全 P D U 送信レート

・ $R_{f a u l t}$: 安全 P D U の異常による安全停止発生レートの要求値

[0017] ***構成の説明***

図 1 は、本実施の形態に係る安全通信システムの構成例を示す。

本実施の形態に係る安全通信システムは、1 つまたは複数の安全マスタ装置 1 0 と、1 つまたは複数の安全スレーブ装置 2 0 と、安全マスタ装置 1 0 と安全スレーブ装置 2 0 とを接続するネットワーク 3 0 から構成される。

安全マスタ装置 1 0 と安全スレーブ装置 2 0 とが、1 対 1 の安全コネクション（安全通信に用いる論理的なコネクション）を作成し、安全通信を行う。安全マスタ装置 1 0 と安全スレーブ装置 2 0 は、それぞれ、例えば組込み機器である。

安全マスタ装置 1 0 は、安全スレーブ装置 2 0 を管理する。

安全スレーブ装置 2 0 は、例えば、安全センサに接続されている。また、安全スレーブ装置 2 0 は、例えば、アクチュエータを制御する。

安全スレーブ装置 2 0 は、安全通信において安全センサのセンサ値を安全マスタ装置 1 0 に通知する。また、安全マスタ装置 1 0 は、例えば、安全センサのセンサ値に基づき、安全通信においてアクチュエータの制御値を安全スレーブ装置 2 0 に通知する。そして、安全スレーブ装置 2 0 は、安全マスタ装置 1 0 から通知された制御値を用いてアクチュエータを制御する。以上の処理手順が安全応答時間内に完了している必要がある。

図 1 では、1 対の安全マスタ装置 1 0 と安全スレーブ装置 2 0 が示されているが、前述のように、安全通信システムに含まれる安全マスタ装置 1 0 と安全スレーブ装置 2 0 の数は、図 1 の例に限定されない。

安全マスタ装置 1 0 は、マスタ装置に相当する。また、安全スレーブ装置 2 0 に相当する。

[0018] 図 2 は、安全マスタ装置 1 0 のハードウェア構成例を示す。

安全マスタ装置 1 0 は、プロセッサ 1 0 1、メモリ 1 0 2、フィールド通信インタフェース 1 0 4 及びこれらを接続するバス 1 0 5 を備える。

安全マスタ装置１０は、コンピュータである。

プロセッサ１０１は、メモリ１０２上に展開された通信処理プログラムである安全通信層を実行することで、バス１０５およびフィールド通信インタフェース１０４を介して、対向する安全スレーブ装置２０と安全通信を行う。

[0019] 図３は、安全スレーブ装置２０のハードウェア構成例を示す。

安全スレーブ装置２０は、プロセッサ２０１、メモリ２０２、入出力インタフェース２０３、フィールド通信インタフェース２０４及びこれらを接続するバス２０５を備える。

安全スレーブ装置２０は、コンピュータである。

プロセッサ２０１は、メモリ２０２上に展開された通信処理プログラムである安全通信層を実行することで、バス２０５およびフィールド通信インタフェース２０４を介して、対向する安全マスタ装置１０と安全通信を行う。

図３に示すように、安全スレーブ装置２０は、デバイス制御を行うための入出力インタフェース２０３を備える。例えば、安全スレーブ装置２０は、入出力インタフェース２０３を介してアクチュエータを制御する。

[0020] 図４は、安全マスタ装置１０の機能構成例を示す。

[0021] 安全マスタ装置１０は、安全通信層１０００とフィールドバスアプリケーション層１００１で構成される。

安全通信層１０００とフィールドバスアプリケーション層１００１はプログラムで実現される。

[0022] 安全通信層１０００は、フィールドバスアプリケーション層１００１を介して、対向する安全スレーブ装置２０の後述する安全通信層２０００と通信する。

[0023] 安全通信層１０００には、安全アプリケーションインタフェース部１０００１、安全コネクション確立処理部１０００２、安全ＰＤＵ生成部１０００３、安全ＰＤＵ検査部１０００４、チェックサム交渉部１０００５、安全パラメータ管理部１０００７及び通信周期検証部１０００８が含まれる。

チェックサム交渉部 10005、通信周期検証部 10008 以外の要素は、一般的な安全通信で用いられる要素と同様である。

より具体的には、安全 PDU 生成部 10003 は、安全アプリケーションインタフェース部 10001 又は安全コネクション確立処理部 10002 からの要求に応じて、安全 PDU を生成する。

安全 PDU 検査部 10004 は、安全アプリケーションインタフェース部 10001 又は安全コネクション確立処理部 10002 宛ての安全 PDU をフィールドバスアプリケーション層 1001 を介して受信し、受信した安全 PDU を検査する。

安全アプリケーションインタフェース部 10001 は、送受信する安全 PDU をユーザアプリケーションに受け渡しする。

安全コネクション確立処理部 10002 は、安全コネクションが切断された状態から、あらかじめ決められた通信シーケンスで、安全スレーブ装置 20 の後述する安全通信層 2000 との間で安全コネクションを確立する処理を行う。

安全パラメータ管理部 10007 は、安全マスタ装置 10 及び安全スレーブ装置 20 の、安全通信に使用する安全パラメータを保管する。安全マスタ装置 10 の安全パラメータとしては、少なくとも下記が必要である。

- (1) システムとしての安全度水準の要求値
- (2) 安全スレーブ装置 20 ごとの下記の値：
 - (A) 安全通信周期（安全 PDU 送信レートから逆算可能）
 - (B) 安全データサイズ
 - (C) 使用すべき多項式の識別情報
 - (D) 伝送路のビットエラー率（特に証明済みの値がある場合のみ）

[0024] チェックサム交渉部 10005 は、安全コネクションを確立する処理において、安全通信に使用する CRC 多項式、送信間隔および安全 PDU の構造等を、対向する安全スレーブ装置 20 の安全通信層 2000 との間で調整し、決定する。

また、チェックサム交渉部 10005 は、安全マスタ装置 10 と安全スレーブ装置 20 との間の通信で用いられる生成多項式の候補を複数の CRC 多項式の中から選択する。より具体的には、チェックサム交渉部 10005 は、複数の CRC 多項式の中から次数が最大の CRC 多項式を選択する。以降、チェックサム交渉部 10005 により選択される CRC 多項式を仮選択多項式と呼ぶ。仮選択多項式は、候補多項式に相当する。

また、チェックサム交渉部 10005 は、仮選択多項式を用いた計算が安全マスタ装置 10 及び安全スレーブ装置 20 の各々で安全通信周期内に完了すると判定された場合に、仮選択多項式を安全マスタ装置 10 と安全スレーブ装置 20 との通信で用いる生成多項式に指定する。

チェックサム交渉部 10005 は、選択部、判定部及び指定部に相当する。また、チェックサム交渉部 10005 により行われる処理は選択処理、判定処理及び指定処理に相当する。

チェックサム交渉部 10005 の動作の詳細は後述する。

[0025] 通信周期検証部 10008 は、チェックサム交渉部 10005 からの指示により、チェックサム交渉部 10005 が選択した仮選択多項式を用いての安全 PDU の生成処理及び検査処理が、安全パラメータにて規定された安全通信周期内に完了するか否かの検証を行う。つまり、通信周期検証部 10008 は、仮選択多項式を用いた計算が安全マスタ装置 10 で規定の期限（安全通信周期の終期）までに完了するか否かを判定する。なお、上記の安全 PDU の生成処理とは、CRC の生成を含む、安全スレーブ装置 20 に送信する安全 PDU を生成する処理である。上記の安全 PDU の検査処理とは、安全スレーブ装置 20 から受信した安全 PDU に対する CRC による検査を行う処理である。

通信周期検証部 10008 は、実際の処理動作を模擬して処理時間を計測して、仮選択多項式を用いての安全 PDU の生成処理及び検査処理が安全通信周期内に完了するか否かの検証を行うことができる。また、通信周期検証部 10008 は、事前に定量化した算出式を用いて、仮選択多項式を用いて

の安全PDUの生成処理及び検査処理が安全通信周期内に完了するか否かの検証を行うことができる。

検証の方法として様々な方法が考えられるが、本実施の形態では、通信周期検証部10008は、既存技術を適用して検証を行うものとし、検証方法の詳細は説明しない。

また、通信周期検証部10008は、チェックサム交渉部10005及び後述する安全スレーブ装置20の通信周期検証部20008とともに、判定部に相当する。また、通信周期検証部10008により行われる処理は、チェックサム交渉部10005により行われる処理及び後述する安全スレーブ装置20の通信周期検証部20008により行われる処理とともに、判定処理に相当する。

[0026] 図4では、プロセッサ101が安全通信層1000及びフィールドバスアプリケーション層1001の機能を実現するプログラムを実行している状態を模式的に表している。

また、本実施の形態では、チェックサム交渉部10005、通信周期検証部10008と、安全スレーブ装置20の通信周期検証部20008とが、本願の情報処理装置を構成する。

[0027] 図5は、安全スレーブ装置20の機能構成例を示す。

[0028] 安全スレーブ装置20は、安全通信層2000とフィールドバスアプリケーション層2001で構成される。

安全通信層2000とフィールドバスアプリケーション層2001はプログラムで実現される。

[0029] 安全通信層2000は、フィールドバスアプリケーション層2001を介して、対向する安全マスタ装置10の安全通信層1000と通信する。

[0030] 安全通信層2000には、安全アプリケーションインタフェース部20001、安全コネクション確立処理部20002、安全PDU生成部20003、安全PDU検査部20004、チェックサム交渉部20005、安全パラメータ管理部20007及び通信周期検証部20008が含まれる。

安全通信層 2000 の構成は、安全通信層 1000 と同様である。

安全コネクション確立処理部 20002 及びチェックサム交渉部 20005 は、安全マスタ装置 10 に対向して通信を行うため、安全コネクション確立処理部 10002 及びチェックサム交渉部 10005 とは処理の流れが異なる。

安全通信層 2000 と安全通信層 1000 における、これら以外の差分を以下に記載する。

安全パラメータ管理部 20007 は、安全スレーブ装置 20 に必要な安全パラメータを保持する。

安全パラメータ管理部 20007 が保持する安全パラメータは以下の通りである。

(1) 安全マスタ装置 10 についての下記の値：

- (A) 安全通信周期（安全 PDU 送信レートから逆算可能）
- (B) 安全データサイズ
- (C) 使用すべき多項式の識別情報

通信周期検証部 20008 は、チェックサム交渉部 20005 からの指示により、チェックサム交渉部 10005 が選択した仮選択多項式を用いての安全 PDU の生成処理及び検査処理が、安全パラメータにて規定された安全通信周期内に完了するか否かの検証を行う。つまり、通信周期検証部 20008 は、選択された仮選択多項式を用いた計算が安全スレーブ装置 20 で規定の期限（安全通信周期の終期）までに完了するか否かを判定する。なお、上記の安全 PDU の生成処理とは、CRC の生成を含む、安全マスタ装置 10 に送信する安全 PDU を生成する処理である。上記の安全 PDU の検査処理とは、安全マスタ装置 10 から受信した PDU に対する CRC による検査を行う処理である。

安全スレーブ装置 20 は、一般的に作成する安全コネクション数が少ないため安全通信による負荷は小さいが、計算リソースも限られているため、上記の検証が必要である。

また、チェックサム交渉部 10005 で選択された仮選択多項式が安全スレーブ装置 20 ではサポートされていない可能性もある。このため、通信周期検証部 20008 は、安全通信周期についての検証を行う前に、仮選択多項式が安全スレーブ装置 20 でサポートされているか否かを検証する。

安全通信周期についての検証の方法については、安全マスタ装置 10 の通信周期検証部 10008 と同様に、既存手法を適用するものとして、詳細は説明しない。

前述したように、通信周期検証部 20008 は、チェックサム交渉部 10005 及び通信周期検証部 10008 とともに、判定部に相当する。また、通信周期検証部 20008 により行われる処理は、チェックサム交渉部 10005 により行われる処理及び通信周期検証部 10008 により行われる処理とともに、判定処理に相当する。

[0031] ***動作の説明***

図 6、図 7 及び図 8 は、本実施の形態に係る安全コネクションを確立する処理を示すフローチャートである。

図 6、図 7 及び図 8 に示す処理は、本願の情報処理方法及び情報処理プログラムの処理に相当する。

[0032] ステップ S001 において、安全コネクションの確立を主導する安全マスタ装置 10 のチェックサム交渉部 10005 が、安全パラメータをもとに、CRC 多項式の候補を仮選択する。

安全マスタ装置 10 では、例えば、図 9 に示す CRC 多項式テーブルにおいて、複数の CRC 多項式を管理している。図 9 の CRC 多項式テーブルでは、CRC 多項式ごとに、次数、最小ハミング距離及び分布係数が示される。図 9 の CRC 多項式テーブルを用いることにより、特定のフレーム長及びビットエラー率の条件下で残存エラー率が算出することができる。

チェックサム交渉部 10005 は、ステップ S001 において、例えば、残存エラーレートにマージンをもたせるため、最大の次数の CRC 多項式を選択することが考えられる。

[0033] ステップS 0 0 2では、通信周期検証部1 0 0 0 8が、仮選択多項式を用いたCRC計算が安全マスタ装置1 0において安全通信周期内に完了するか否かを検証する。

このとき、通信周期検証部1 0 0 0 8は、安全マスタ装置1 0として実行すべき処理全体を考慮して、チェックサムの生成を含む当該安全コネクションの安全PDUの生成処理及び検査処理が、設定された安全通信周期内に完了するか否かを検証する。

前述したように、通信周期検証部1 0 0 0 8は、安全マスタ装置1 0の全体としての処理を考慮して生成された算出式を用いて当該検証を行うことができる。また、通信周期検証部1 0 0 0 8は、シミュレーションを行って当該検証を行うこともできる。更に、通信周期検証部1 0 0 0 8は、実際の処理動作を模擬して処理時間を計測して当該検証を行うこともできる。通信周期検証部1 0 0 0 8は、既存のいずれかの検証方法を用いて当該検証を行うことができる。

[0034] 仮選択多項式を用いたCRC計算が安全通信周期内に完了する場合（ステップS 0 0 3でYES）は、処理はステップS 0 0 4に遷移する。一方、仮選択多項式を用いたCRC計算が安全通信周期内に完了しない場合（ステップS 0 0 3でNO）は、処理はステップS 0 0 8に遷移する。

[0035] ステップS 0 0 4では、チェックサム交渉部1 0 0 0 5が、仮選択多項式を使用可能か否かについて、安全コネクションを作成する対向する安全スレーブ装置2 0と交渉する。

具体的には、チェックサム交渉部1 0 0 0 5が、仮選択多項式の識別情報を含むメッセージを、安全スレーブ装置2 0へ送信する。

ステップS 0 0 4は、安全マスタ装置1 0と安全コネクションを確立する全ての安全スレーブ装置2 0について行われる。

[0036] 安全スレーブ装置2 0では、チェックサム交渉部2 0 0 0 5がメッセージを受信する。そして、チェックサム交渉部2 0 0 0 5は、通信周期検証部2 0 0 0 8に仮選択多項式の検証を指示する。

通信周期検証部 20008 は、チェックサム交渉部 20005 の指示に従い、仮選択多項式の検証を行う。具体的には、通信周期検証部 20008 は、安全スレーブ装置 20 が仮選択多項式を用いた CRC 算出をサポートしているか否かを検証する。

安全スレーブ装置 20 が仮選択多項式を用いた CRC 算出をサポートしている場合は、通信周期検証部 20008 は、仮選択多項式を用いての安全 PDU の生成処理及び検査処理が、安全スレーブ装置 20 において安全通信周期内に完了するか否かを、他の処理の影響も考慮して検証する。

チェックサム交渉部 20005 は、上記の 2 つの検証の両方で問題がなければ、安全マスタ装置 10 に「合意」の旨の応答メッセージを送信する。一方、上記の 2 つの検証のうちの少なくともいずれか一方で問題があれば、チェックサム交渉部 20005 は、安全マスタ装置 10 に「合意不成立」の旨の応答メッセージを送信する。

[0037] ステップ S005 では、チェックサム交渉部 10005 は、安全スレーブ装置 20 からの応答メッセージを確認し、全ての安全コネクションについて「合意」の旨の応答メッセージを受信している場合（ステップ S005 で YES）は、処理がステップ S006 に遷移する。一方、「合意不成立」の旨の応答メッセージを受信している場合（ステップ S005 で NO）は、処理がステップ S008 に遷移する。

[0038] ステップ S006 では、チェックサム交渉部 10005 が、仮選択多項式を、安全マスタ装置 10 と全ての安全スレーブ装置 20 との通信で用いる生成多項式に指定する。

そして、チェックサム交渉部 10005 は、全ての安全スレーブ装置 20 のチェックサム交渉部 20005 に、生成多項式として指定した仮選定多項式を安全通信に用いることを通知するメッセージを送信する。

[0039] ステップ S007 では、安全マスタ装置 10 の安全コネクション確立処理部 1002 及び安全スレーブ装置 20 の安全コネクション確立処理部 2002 が安全コネクションを確立し、以後、ステップ S006 で指定された生成

多項式を用いた安全通信が行われる。

[0040] 下記のステップS008～S010は、仮選択多項式を用いたCRC計算が安全通信周期内に完了できないと判明した場合に、仮選択多項式の変更を検討するフェーズである。

[0041] ステップS008では、チェックサム交渉部10005が、当該仮選択多項式よりも次数の小さいCRC多項式の適用時における、安全コネクションごとの残存エラーレート $\Lambda_{sc}(P_e)$ を算出する。チェックサム交渉部10005は、安全通信の国際規格で規定された算出方法を使って残存エラーレート $\Lambda_{sc}(P_e)$ を算出する。本実施の形態では、残存エラーレート $\Lambda_{sc}(P_e)$ の具体的な算出方法の説明は省略する。チェックサム交渉部10005は、算出に必要な安全通信周期、ビットエラー率などの値に、安全パラメータの値を使用する。

なお、ステップS008及び以降のステップで、新たな仮選択多項式及び正式な生成多項式は、全ての安全コネクションで同じである必要はない。

[0042] ステップS009では、チェックサム交渉部10005は、上記のステップS008で得られた残存エラーレート $\Lambda_{sc}(P_e)$ が要求値を満たすか否かを判定する。本実施の形態では、この要求値は、安全通信の国際規格で規定された要求値である。このため、本実施の形態では、要求値の具体的な値には言及しない。

残存エラーレート $\Lambda_{sc}(P_e)$ が要求値を満たす場合（ステップS009でYES）、つまり、次数の小さいCRC多項式に変更しても安全度水準の要求値を満たす場合は、処理がステップS010へ遷移する。一方、残存エラーレート $\Lambda_{sc}(P_e)$ が要求値を満たさない場合（ステップS009でNO）は、処理がS011へ遷移する。

[0043] ステップS010では、チェックサム交渉部10005は、現在の仮選択多項式よりも次数が小さく、かつ残存エラーレート $\Lambda_{sc}(P_e)$ の値が要求値を満たすCRC多項式を、新たな仮選択多項式として選択する。

その後、新たな仮選択多項式に対してステップS002以降の処理が行わ

れる。つまり、新たな仮選択多項式を用いた計算が安全マスタ装置 10 及び安全スレーブ装置 20 の各々で安全通信周期内に完了するか否かが検証される。

[0044] 下記のステップ S011～S013 は、安全通信周期の延長を検討するフェーズである。

具体的には、仮選択多項式を用いた計算が安全通信周期内に完了しない場合（ステップ S003 で NO）、または、いずれかの安全スレーブ装置 20 から「合意不成立」との応答メッセージを受信した場合（ステップ S005 で NO）であって、残存エラーレート $\Lambda_{sc}(P_e)$ が要求値を満たす次数が小さい CRC 多項式が存在しない場合（ステップ S009 で NO）に、ステップ S011～S013 において、安全通信周期の延長が検討される。

[0045] ステップ S011 では、チェックサム交渉部 10005 が、安全接続ごとに、安全通信周期を延長できるか否かを判定する。つまり、チェックサム交渉部 10005 は、仮に安全接続の安全通信周期を延長しても、必要な安全応答時間、可用性を維持できるか否かを判定する。

チェックサム交渉部 10005 は、具体的には、前述の（式 1）及び（式 2）を適用して、安全通信周期の延長が可能であるか否かを判定する。

[0046] 安全通信周期を延長できる安全接続がある場合（ステップ S011 で YES）は、処理が S012 へ遷移する。一方、安全通信周期を延長できる安全接続がない場合（ステップ S011 で NO）は、処理が S014 へ遷移する。

[0047] ステップ S012 では、チェックサム交渉部 10005 が、安全通信周期の延長可能な割合のマージンが最大である安全接続を選択する。

[0048] ステップ S013 では、チェックサム交渉部 10005 が、ステップ S012 で選択した安全接続について、安全通信周期の延長又はデータフレームの分割を実施する。

チェックサム交渉部 10005 は、前述の（式 1）、（式 2）の範囲で安全通信周期を延長することができる。

チェックサム交渉部 10005 は、ステップ S012 で選択された安全コネクションの現在の仮選択多項式を新たな仮選択多項式として選択する。そして、当該新たな仮選択多項式について延長された安全通信周期を用いてステップ S002 以降の処理が行われる。つまり、新たな仮選択多項式を用いた計算が安全マスタ装置 10 及び安全スレーブ装置 20 の各々で、延長された安全通信周期内に完了するか否かが検証される。

また、データフレームを分割することで計算時間が短縮される。つまり、チェックサム交渉部 10005 は、データフレームの分割により、個々のデータフレームのフレーム長を短くし、分割により得られた分割データフレームの全てが通信先に到着するまでの実質的な間隔を長くする。これにより、次数の小さい CRC 多項式を使用することが可能になり、計算時間を短縮することができる。

チェックサム交渉部 10005 は、ステップ S012 で選択された安全コネクションの現在の仮選択多項式を新たな仮選択多項式として選択する。そして、分割データフレームに対して当該新たな仮選択多項式が用いられてステップ S002 以降の処理が行われる。つまり、分割データフレームに対する新たな仮選択多項式を用いた計算が安全マスタ装置 10 及び安全スレーブ装置 20 の各々で安全通信周期内に完了するか否かが検証される。

[0049] ステップ S014 では、安全マスタ装置 10 又は安全スレーブ装置 20 の処理性能上、実現不可能な安全通信設定がなされていることが判明する。このため、チェックサム交渉部 10005 は、安全コネクションの確立ができないと判定し、その旨を安全マスタ装置 10 のユーザに通知する。

[0050] ***実施の形態の効果の説明***

以上、本実施の形態では、仮選択多項式を用いた計算が安全マスタ装置 10 及び安全スレーブ装置 20 の各々で安全通信周期内に完了するか否かが判定される。そして、仮選択多項式を用いた計算が安全マスタ装置 10 及び安全スレーブ装置 20 の各々で安全通信周期内に完了する場合に、仮選択多項式が生成多項式に指定される。このため、本実施の形態によれば、計算リソ

ースが限られた条件下でも安全通信周期内にCRC計算を完了させることができる生成多項式を指定することができる。

[0051] 実施の形態2.

実施の形態1では、安全マスタ装置10が安全スレーブ装置20に仮選択多項式を用いた計算が安全通信周期内に完了するか否かを判定させて、生成多項式を指定している。

本実施の形態では、安全マスタ装置10が仮選択多項式を用いた計算が安全スレーブ装置20で安全通信周期内に完了するか否かを判定する例を説明する。より具体的には、本実施の形態では、安全マスタ装置10が安全スレーブ装置20から、安全スレーブ装置20の計算能力に関する情報（以下、計算能力情報）を取得し、安全スレーブ装置20の計算能力情報に基づいて、安全スレーブ装置20で仮選択多項式を用いた計算が安全通信周期内に完了するか否かを判定する。

[0052] ***構成の説明***

本実施の形態に係る安全通信システムの構成例は図1に示す通りである。

また、本実施の形態に係る安全マスタ装置10のハードウェア構成例は図2に示す通りである。

また、本実施の形態に係る安全スレーブ装置20のハードウェア構成例は図3に示す通りである。

また、本実施の形態に係る安全マスタ装置10の機能構成例は図4に示す通りである。

また、本実施の形態に係る安全スレーブ装置20の機能構成例は図5に示す通りである。

なお、実施の形態1では、チェックサム交渉部10005、通信周期検証部10008及び通信周期検証部20008が判定部に相当していたが、本実施の形態では、チェックサム交渉部10005及び通信周期検証部10008のみが判定部に相当する。また、実施の形態1では、チェックサム交渉部10005、通信周期検証部10008及び通信周期検証部20008が

情報処理装置を構成するとしていたが、本実施の形態では、チェックサム交渉部 10005 及び通信周期検証部 10008 が情報処理装置を構成する。

[0053] ***動作の説明***

本実施の形態に係る安全コネクションを確立する処理は、図 10 に示す通りである。図 10 において、図 6 と同じ符号の処理は図 6 に示すものと同じである。以下では、主に実施の形態 1 との差分を説明する。以下で説明していない事項は、実施の形態 1 と同じである。

図 10 に示す処理は、本願の情報処理方法及び情報処理プログラムの処理に相当する。

[0054] ステップ S021 では、安全マスタ装置 10 のチェックサム交渉部 10005 が、安全通信を行う全ての安全スレーブ装置 20 に対して、CRC 多項式ごとの計算能力情報の送信を要求する。

各安全スレーブ装置 20 のチェックサム交渉部 20005 は、通信周期検証部 20008 に計算能力情報の生成を指示する。通信周期検証部 20008 は、計算能力情報を生成し、生成した計算能力情報を安全マスタ装置 10 に送信する。計算能力情報は、各 CRC 多項式を適用した場合に安全スレーブ装置 20 が実現可能な通信周期を表す情報である。図 11 は、計算能力情報の例を示す。計算能力は、安全スレーブ装置 20 が安全通信システムにおいて実行すべき処理に応じて変動するため、図 11 に示す「実現可能な通信周期」は必ずしも固定値ではない。

[0055] ステップ S022 では、安全マスタ装置 10 のチェックサム交渉部 10005 が、安全スレーブ装置 20 から計算能力情報を受信する。

[0056] ステップ S001 では、チェックサム交渉部 10005 が、CRC 多項式の候補を仮選択する。チェックサム交渉部 10005 は、実施の形態 1 と同様に、例えば、最大の次数の CRC 多項式を選択する。

[0057] ステップ S002 では、実施の形態 1 と同様に、通信周期検証部 10008 が、仮選択多項式を用いた CRC 計算が安全マスタ装置 10 において安全通信周期内に完了するか否かを検証する。

[0058] 仮選択多項式を用いたCRC計算が安全通信周期内に完了する場合（ステップS003でYES）は、処理はステップS023に遷移する。一方、仮選択多項式を用いたCRC計算が安全通信周期内に完了しない場合（ステップS003でNO）は、処理はステップS008に遷移する。ステップS008以降の処理は実施の形態1で説明した通りなので、説明を省略する。

[0059] ステップS023では、通信周期検証部10008が、ステップS022で受信した計算能力情報に基づき、仮選択多項式を用いたCRC計算が安全スレーブ装置20において安全通信周期内に完了するか否かを検証する。

ステップS023は、安全マスタ装置10と安全コネクションを確立する全ての安全スレーブ装置20について行われる。

[0060] 仮選択多項式を用いたCRC計算が安全通信周期内に完了する場合（ステップS0024でYES）は、処理はステップS006に遷移する。一方、仮選択多項式を用いたCRC計算が安全通信周期内に完了しない場合（ステップS024でNO）は、処理はステップS008に遷移する。ステップS006以降の処理及びステップS008以降の処理は実施の形態1で説明した通りなので、説明を省略する。

[0061] ***実施の形態の効果の説明***

本実施の形態では、安全マスタ装置10が、安全スレーブ装置20でのCRC計算が安全通信周期内に完了するか否かを検証する。つまり、安全スレーブ装置20の計算リソースを用いることなく、安全スレーブ装置20でのCRC計算が安全通信周期内に完了するか否かの検証が行われる。このため、本実施の形態によれば、安全スレーブ装置20の計算リソースが限られていても、安全通信周期内にCRC計算を完了させることができる生成多項式を指定することができる。

[0062] 実施の形態3.

実施の形態1及び実施の形態2では、安全マスタ装置10では、図9のCRC多項式テーブルに示すように、単一のCRC多項式が仮選択多項式の選択肢として管理されている。

本実施の形態では、図 12 の CRC 多項式テーブルに示すように、複数の CRC 多項式の組合せを、仮選択多項式の選択肢として管理する。つまり、本実施の形態では、1 つの安全 PDU に異なる複数のチェックサムを付与する。

安全通信層 1000 が動作するハードウェア及び安全通信層 2000 が動作するハードウェアが多重化されている場合は、チェックサムを並列に算出することができる。このため、次数の大きい CRC 多項式で生成した 1 つのチェックサムを安全 PDU に付与するよりも、次数の小さい CRC 多項式で生成した複数個のチェックサムを安全 PDU に付与することが望ましいと考えられる。つまり、次数の小さい CRC 多項式で生成した複数個のチェックサムを安全 PDU に付与する場合は、次数の大きい CRC 多項式で生成した 1 つのチェックサムを安全 PDU に付与する場合と同等の残存エラーレートを担保しつつ計算時間を短縮することができる。そこで、図 12 のように CRC 多項式テーブルを拡張して、仮選択多項式の選択肢を増やすことが考えられる。

[0063] 実施の形態 4.

実施の形態 1 では、安全マスタ装置 10 が安全コネクションの確立時に図 6～図 8 に示す処理を行って、生成多項式を指定する。

しかしながら、図 6～図 8 に示す処理の結果は、安全通信システムの構成、安全パラメータ及びネットワーク 30 の条件に変化が無ければ、毎回同じ結果になる。従って、安全通信システムの構成、安全パラメータ及びネットワーク 30 の条件に対して、図 6～図 8 に示す処理を行って安全コネクションごとに生成多項式を予め指定しておけば、安全コネクションの確立の度に図 6～図 8 に示す処理を繰り返す必要はない。

本実施の形態では、安全マスタ装置 10 とは異なる情報処理装置が、図 6～図 8 に示す処理を行って生成多項式を予め指定する例を説明する。

そして、情報処理装置が、指定した生成多項式を安全マスタ装置 10 に通知する。安全マスタ装置 10 は、情報処理装置から通知された生成多項式を

安全通信に適用する。

[0064] ***構成の説明***

図13は、本実施の形態に係る情報処理装置50のハードウェア構成例を示す。

情報処理装置50は、プロセッサ501、メモリ502、通信インタフェース503及びこれらを接続するバス504を備える。

情報処理装置50は、コンピュータである。

プロセッサ501は、メモリ102上に展開された、後述する選択部5001、判定部5002及び指定部50003を実行する。

選択部5001、判定部5002及び指定部50003は、例えば、プログラムで実現される。

通信インタフェース503は、指定された生成多項式を安全マスタ装置10に通知する。

[0065] 図14は、情報処理装置50の機能構成例を示す。

[0066] 情報処理装置50は、選択部5001、判定部5002及び指定部5003で構成される。

図14では、プロセッサ501が選択部5001、判定部5002及び指定部50003の機能を実現するプログラムを実行している状態を模式的に表している。

[0067] 選択部5001は、安全マスタ装置10と安全スレーブ装置20との間の通信で用いられる生成多項式の候補を複数のCRC多項式の中から選択する。本実施の形態でも、選択部5001により選択されたCRC多項式を仮選択多項式という。

選択部5001により行われる処理は、選択処理に相当する。

[0068] 判定部5002は、仮選択多項式を用いた計算が安全マスタ装置10及び安全スレーブ装置20の各々で安全通信周期内に完了するか否かを判定する。

判定部5002は、例えば、図11に示す計算能力情報を安全マスタ装置

１０及び各安全スレーブ装置２０について保持している。そして、判定部５００２は、計算能力情報を用いて、仮選択多項式を用いた計算が安全マスタ装置１０及び安全スレーブ装置２０の各々で安全通信周期内に完了するか否かを判定する。

判定部５００２により行われる処理は、判定処理に相当する。

[0069] 指定部５００３は、仮選択多項式を用いた計算が安全マスタ装置１０及び安全スレーブ装置２０の各々で安全通信周期までに完了すると判定部５００２により判定された場合に、仮選択多項式を生成多項式に指定する。

また、指定部５００３は、通信インタフェース５０３を介して、指定した生成多項式を安全マスタ装置１０に通知する。

指定部５００３により行われる処理は、指定処理に相当する。

[0070] ***動作の説明***

図１５は、本実施の形態に係る情報処理装置５００の動作例を示す。

図１５に示す処理は、本願の情報処理方法及び情報処理プログラムの処理に相当する。

[0071] ステップＳ０４１では、選択部５００１が、ＣＲＣ多項式の候補を仮選択する。選択部５００１は、実施の形態１のステップＳ００１と同様に、例えば、最大の次数のＣＲＣ多項式を選択する。

[0072] ステップＳ０４２では、判定部５００２が、安全マスタ装置１０についての計算能力情報に基づき、仮選択多項式を用いたＣＲＣ計算が安全マスタ装置１０において安全通信周期内に完了するか否かを検証する。

[0073] 仮選択多項式を用いたＣＲＣ計算が安全マスタ装置１０において安全通信周期内に完了する場合（ステップＳ０４３でＹＥＳ）は、処理はステップＳ０４４に遷移する。一方、仮選択多項式を用いたＣＲＣ計算が安全通信周期内に完了しない場合（ステップＳ０４３でＮＯ）は、処理は図７のステップＳ００８に遷移する。

[0074] ステップＳ０４４では、判定部５００２が、安全スレーブ装置２０についての計算能力情報に基づき、仮選択多項式を用いたＣＲＣ計算が安全スレー

ブ装置 20 において安全通信周期内に完了するか否かを検証する。

ステップ S 0 4 4 は、安全マスタ装置 10 と安全コネクションを確立する全ての安全スレーブ装置 20 について行われる。

[0075] 仮選択多項式を用いた CRC 計算が全ての安全スレーブ装置 20 において安全通信周期内に完了する場合（ステップ S 0 0 4 5 で YES）は、処理はステップ S 0 4 6 に遷移する。一方、いずれかの安全スレーブ装置 20 にて仮選択多項式を用いた CRC 計算が安全通信周期内に完了しない場合（ステップ S 0 4 5 で NO）は、処理は図 7 のステップ S 0 0 8 に遷移する。

[0076] ステップ S 0 4 6 では、指定部 5 0 0 3 が、仮選択多項式を、安全マスタ装置 10 と全ての安全スレーブ装置 20 との通信で用いる生成多項式に指定する。

そして、指定部 5 0 0 3 は、ステップ S 0 4 7 において、安全マスタ装置 10 に、指定した生成多項式を通知するメッセージを送信する。

[0077] 本実施の形態では、図 7 のステップ S 0 0 8 において、判定部 5 0 0 2 が、当該仮選択多項式よりも次数の小さい CRC 多項式の適用時における、安全コネクションごとの残存エラーレート $\Lambda_{sc}(P_e)$ を算出する。指定部 5 0 0 3 は、安全通信の国際規格で規定された算出方法を使って残存エラーレート $\Lambda_{sc}(P_e)$ を算出する。本実施の形態では、残存エラーレート $\Lambda_{sc}(P_e)$ の具体的な算出方法の説明は省略する。指定部 5 0 0 3 は、算出に必要な安全通信周期、ビットエラー率などの値は、安全パラメータの値を使用する。

なお、ステップ S 0 0 8 及び以降のステップで、新たな仮選択多項式及び正式な生成多項式は、全ての安全コネクションで同じである必要はない。

[0078] ステップ S 0 0 9 では、判定部 5 0 0 2 は、上記のステップ S 0 0 8 で得られた残存エラーレート $\Lambda_{sc}(P_e)$ が要求値を満たすか否かを判定する。本実施の形態では、この要求値は、安全通信の国際規格で規定された要求値である。このため、本実施の形態では、要求値の具体的な値には言及しない。

残存エラーレート $\Lambda_{sc}(P_e)$ が要求値を満たす場合（ステップ S 0 0 9 で

YES)、つまり、次数の小さいCRC多項式に変更しても安全度水準の要求値を満たす場合は、処理がステップS010へ遷移する。一方、残存エラーレート $\Lambda_{sc}(P_e)$ が要求値を満たさない場合(ステップS009でNO)は、処理がS011へ遷移する。

[0079] ステップS010では、判定部5002は、現在の仮選択多項式よりも次数が小さく、かつ残存エラーレート $\Lambda_{sc}(P_e)$ の値が要求値を満たすCRC多項式を、新たな仮選択多項式として選択する。

その後、新たな仮選択多項式に対してステップS042以降の処理が行われる。つまり、新たな仮選択多項式を用いた計算が安全マスタ装置10及び安全スレーブ装置20の各々で安全通信周期内に完了するか否かが検証される。

[0080] 仮選択多項式を用いた計算が安全通信周期内に完了しない場合(ステップS043でNO)、または、いずれかの安全スレーブ装置20から「合意不成立」との応答メッセージを受信した場合(ステップS045でNO)であって、残存エラーレート $\Lambda_{sc}(P_e)$ が要求値を満たすCRC多項式が存在しない場合(ステップS009でNO)に、ステップS011~S013において、安全通信周期の延長が検討される。

[0081] ステップS011では、判定部5002が、安全コネクションごとに、安全通信周期を延長できるか否かを判定する。つまり、判定部5002は、仮に安全コネクションの安全通信周期を延長しても、必要な安全応答時間、可用性を維持できるか否かを判定する。

判定部5002は、具体的には、前述の(式1)及び(式2)を適用して、安全通信周期の延長が可能であるか否かを判定する。

[0082] 安全通信周期を延長できる安全コネクションがある場合(ステップS011でYES)は、処理がS012へ遷移する。一方、安全通信周期を延長できる安全コネクションがない場合(ステップS011でNO)は、処理がS014へ遷移する。

[0083] ステップS012では、判定部5002が、安全通信周期の延長可能な割

合のマージンが最大である安全コネクションを選択する。

[0084] ステップS 0 1 3では、判定部5 0 0 2が、ステップS 0 1 2で選択した安全コネクションについて、安全通信周期の延長又はデータフレームの分割を実施する。

判定部5 0 0 2は、前述の（式1）、（式2）の範囲で安全通信周期を延長することができる。

判定部5 0 0 2は、ステップS 0 1 2で選択された安全コネクションの現在の仮選択多項式を新たな仮選択多項式として選択する。そして、当該新たな仮選択多項式について延長された安全通信周期を用いてステップS 0 0 2以降の処理が行われる。つまり、新たな仮選択多項式を用いた計算が安全マスタ装置1 0及び安全スレーブ装置2 0の各々で、延長された安全通信周期内に完了するか否かが検証される。

また、データフレームを分割することで計算時間が短縮される。つまり、判定部5 0 0 2は、データフレームの分割により、個々のデータフレームのフレーム長を短くし、分割により得られた分割データフレームの全てが通信先に到着するまでの実質的な間隔を長くする。これにより、次数の小さいC R C多項式を使用することが可能になり、計算時間を短縮することができる。

判定部5 0 0 2は、ステップS 0 1 2で選択された安全コネクションの現在の仮選択多項式を新たな仮選択多項式として選択する。そして、分割データフレームに対して当該新たな仮選択多項式が用いられてステップS 0 0 2以降の処理が行われる。つまり、分割データフレームに対する新たな仮選択多項式を用いた計算が安全マスタ装置1 0及び安全スレーブ装置2 0の各々で安全通信周期内に完了するか否かが検証される。

[0085] ステップS 0 1 4では、安全マスタ装置1 0又は安全スレーブ装置2 0の処理性能上、実現不可能な安全通信設定がなされていることが判明する。このため、判定部5 0 0 2は、安全コネクションの確立ができないと判定し、その旨を安全マスタ装置1 0に通知する。

[0086] ***実施の形態の効果の説明***

本実施の形態では、情報処理装置50が、安全マスタ装置10及び安全スレーブ装置20でのCRC計算が安全通信周期内に完了するか否かを検証する。つまり、安全マスタ装置10及び安全スレーブ装置20の計算リソースを用いることなく、安全マスタ装置10及び安全スレーブ装置20でのCRC計算が安全通信周期内に完了するか否かの検証が行われる。このため、本実施の形態によれば、安全マスタ装置10及び安全スレーブ装置20の計算リソースが限られていても、安全通信周期内にCRC計算を完了させることができる生成多項式を指定することができる。

[0087] 以上、本発明の実施の形態について説明したが、これらの実施の形態のうち、2つ以上を組み合わせる実施しても構わない。

あるいは、これらの実施の形態のうち、1つを部分的に実施しても構わない。

あるいは、これらの実施の形態のうち、2つ以上を部分的に組み合わせる実施しても構わない。

なお、本発明は、これらの実施の形態に限定されるものではなく、必要に応じて種々の変更が可能である。

[0088] ***ハードウェア構成の説明***

最後に、安全マスタ装置10、安全スレーブ装置20及び情報処理装置50のハードウェア構成の補足説明を行う。

プロセッサ101、プロセッサ201及びプロセッサ501は、プロセッシングを行うIC(Integrated Circuit)である。

プロセッサ101、プロセッサ201及びプロセッサ501は、CPU(Central Processing Unit)、DSP(Digital Signal Processor)等である。

メモリ102、メモリ202及びメモリ502は、RAM(Random Access Memory)、ROM(Read Only Memory)、フラッシュメモリ、HDD(Hard Disk Drive)等

である。

フィールド通信インタフェース104、フィールド通信インタフェース204及び通信インタフェース503は、データの通信処理を実行する電子回路である。

フィールド通信インタフェース104、フィールド通信インタフェース204及び通信インタフェース503は、例えば、通信チップ又はNIC (Network Interface Card) である。

[0089] また、メモリ102には、OS (Operating System) も記憶されている。

そして、OSの少なくとも一部がプロセッサ101により実行される。

プロセッサ101はOSの少なくとも一部を実行しながら、安全通信層1000及びフィールドバスアプリケーション層1001の機能を実現するプログラムを実行する。

プロセッサ101がOSを実行することで、タスク管理、メモリ管理、ファイル管理、通信制御等が行われる。

また、安全通信層1000及びフィールドバスアプリケーション層1001の処理の結果を示す情報、データ、信号値及び変数値の少なくともいずれかが、メモリ102、プロセッサ101内のレジスタ及びキャッシュメモリの少なくともいずれかに記憶される。

また、安全通信層1000及びフィールドバスアプリケーション層1001の機能を実現するプログラムは、磁気ディスク、フレキシブルディスク、光ディスク、コンパクトディスク、ブルーレイ（登録商標）ディスク、DVD等の可搬記録媒体に格納されていてもよい。

[0090] また、メモリ202にも、OSが記憶されている。

そして、OSの少なくとも一部がプロセッサ201により実行される。

プロセッサ201はOSの少なくとも一部を実行しながら、安全通信層2000及びフィールドバスアプリケーション層2001の機能を実現するプログラムを実行する。

プロセッサ201がOSを実行することで、タスク管理、メモリ管理、ファイル管理、通信制御等が行われる。

また、安全通信層2000及びフィールドバスアプリケーション層2001の処理の結果を示す情報、データ、信号値及び変数値の少なくともいずれかが、メモリ202、プロセッサ201内のレジスタ及びキャッシュメモリの少なくともいずれかに記憶される。

また、安全通信層2000及びフィールドバスアプリケーション層2001の機能を実現するプログラムは、磁気ディスク、フレキシブルディスク、光ディスク、コンパクトディスク、ブルーレイ（登録商標）ディスク、DVD等の可搬記録媒体に格納されていてもよい。

[0091] また、メモリ502にも、OSが記憶されている。

そして、OSの少なくとも一部がプロセッサ501により実行される。

プロセッサ501はOSの少なくとも一部を実行しながら、選択部5001、判定部5002及び指定部5003の機能を実現するプログラムを実行する。

プロセッサ501がOSを実行することで、タスク管理、メモリ管理、ファイル管理、通信制御等が行われる。

また、選択部5001、判定部5002及び指定部5003の処理の結果を示す情報、データ、信号値及び変数値の少なくともいずれかが、メモリ502、プロセッサ501内のレジスタ及びキャッシュメモリの少なくともいずれかに記憶される。

また、選択部5001、判定部5002及び指定部5003の機能を実現するプログラムは、磁気ディスク、フレキシブルディスク、光ディスク、コンパクトディスク、ブルーレイ（登録商標）ディスク、DVD等の可搬記録媒体に格納されていてもよい。

[0092] また、安全マスタ装置10、安全スレーブ装置20及び情報処理装置50は、処理回路により実現されてもよい。処理回路は、例えば、ロジックIC (Integrated Circuit)、GA (Gate Array

)、ASIC (Application Specific Integrated Circuit)、FPGA (Field-Programmable Gate Array) である。

なお、本明細書では、プロセッサと、メモリと、プロセッサとメモリの組合せと、処理回路との上位概念を、「プロセッシングサーキットリー」という。

つまり、プロセッサと、メモリと、プロセッサとメモリの組合せと、処理回路とは、それぞれ「プロセッシングサーキットリー」の具体例である。

符号の説明

[0093] 10 安全マスタ装置、20 安全スレーブ装置、30 ネットワーク、50 情報処理装置、101 プロセッサ、102 メモリ、104 フィールド通信インタフェース、105 バス、201 プロセッサ、202 メモリ、203 入出力インタフェース、204 フィールド通信インタフェース、205 バス、501 プロセッサ、502 メモリ、503 通信インタフェース、504 バス、1000 安全通信層、1001 フィールドバスアプリケーション層、10001 安全アプリケーションインタフェース部、10002 安全コネクション確立処理部、10003 安全PDU生成部、10004 安全PDU検査部、10005 チェックサム交渉部、10007 安全パラメータ管理部、10008 通信周期検証部、2000 安全通信層、2001 フィールドバスアプリケーション層、20001 安全アプリケーションインタフェース部、20002 安全コネクション確立処理部、20003 安全PDU生成部、20004 安全PDU検査部、20005 チェックサム交渉部、20007 安全パラメータ管理部、20008 通信周期検証部、5001 選択部、5002 判定部、5003 指定部。

請求の範囲

- [請求項1] マスタ装置とスレーブ装置との間の通信で用いられる生成多項式の候補を複数の多項式の中から候補多項式として選択する選択部と、
- 前記候補多項式を用いた計算が前記マスタ装置及び前記スレーブ装置の各々で規定の期限までに完了するか否かを判定する判定部と、
- 前記候補多項式を用いた計算が前記マスタ装置及び前記スレーブ装置の各々で前記期限までに完了すると前記判定部により判定された場合に、前記候補多項式を前記生成多項式に指定する指定部とを有する情報処理装置。
- [請求項2] 前記選択部は、
- 前記複数の多項式の中から次数が最大の多項式を前記候補多項式として選択し、
- 前記候補多項式を用いた計算が前記マスタ装置及び前記スレーブ装置のいずれかで前記期限までに完了しないと前記判定部により判定された場合に、前記候補多項式よりも次数が小さい多項式を新たな候補多項式として選択し、
- 前記判定部は、
- 前記新たな候補多項式を用いた計算が前記マスタ装置及び前記スレーブ装置の各々で前記期限までに完了するか否かを判定する請求項1に記載の情報処理装置。
- [請求項3] 前記選択部は、
- 前記候補多項式よりも次数が小さく、残存エラーレートが要求値を満たす多項式を前記新たな候補多項式として選択する請求項2に記載の情報処理装置。
- [請求項4] 前記選択部は、
- いずれの多項式を用いた計算も前記マスタ装置及び前記スレーブ装置のいずれかで前記期限までに完了しないと前記判定部により判定された場合に、前記複数の多項式の中で前記期限よりも長い期限である

延長期限を用いることができる多項式を新たな候補多項式として選択し、

前記判定部は、

前記新たな候補多項式を用いた計算が前記マスタ装置及び前記スレーブ装置の各々で前記延長期限までに完了するか否かを判定する請求項 2 に記載の情報処理装置。

[請求項5]

前記選択部は、

いずれの多項式を用いた計算も前記マスタ装置及び前記スレーブ装置の各々で前記期限までに完了しないと前記判定部により判定された場合に、前記複数の多項式の中で前記期限よりも長い期限である延長期限を用いることができる多項式を新たな候補多項式として選択し、

前記判定部は、

規定のデータフレームを分割した分割データフレームに対する前記新たな候補多項式を用いた計算が前記マスタ装置及び前記スレーブ装置の各々で前記期限までに完了するか否かを判定する請求項 2 に記載の情報処理装置。

[請求項6]

前記判定部は、

前記候補多項式を用いた計算が前記マスタ装置及び前記スレーブ装置の各々で、前記マスタ装置及び前記スレーブ装置との間で行われる安全通信の安全通信周期内に完了するか否かを判定し、

前記指定部は、

前記候補多項式を用いた計算が前記マスタ装置及び前記スレーブ装置の各々で前記安全通信周期内に完了すると前記判定部により判定された場合に、前記候補多項式を前記生成多項式に指定する請求項 1 に記載の情報処理装置。

[請求項7]

前記複数の多項式には、2 以上の多項式の組合せが含まれる請求項 1 に記載の情報処理装置。

[請求項8]

前記情報処理装置が、前記マスタ装置である請求項 1 に記載の情報

処理装置。

[請求項9] 前記情報処理装置が、前記マスタ装置及び前記スレーブ装置である請求項1に記載の情報処理装置。

[請求項10] 前記情報処理装置が、前記マスタ装置及び前記スレーブ装置とは異なるコンピュータである請求項1に記載の情報処理装置。

[請求項11] コンピュータが、マスタ装置とスレーブ装置との間の通信で用いられる生成多項式の候補を複数の多項式の中から候補多項式として選択し、

前記コンピュータが、前記候補多項式を用いた計算が前記マスタ装置及び前記スレーブ装置の各々で規定の期限までに完了するか否かを判定し、

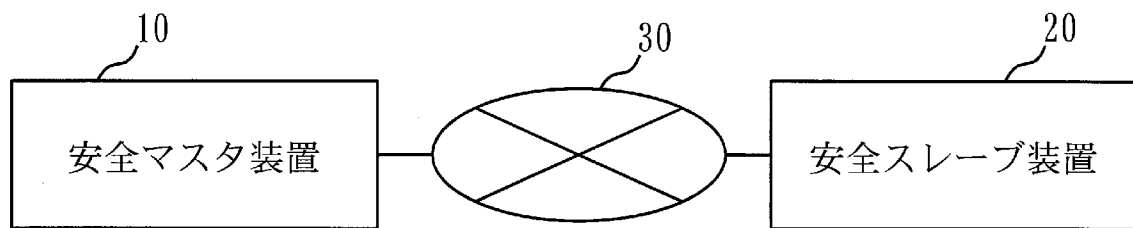
前記候補多項式を用いた計算が前記マスタ装置及び前記スレーブ装置の各々で前記期限までに完了すると判定された場合に、前記コンピュータが、前記候補多項式を前記生成多項式に指定する情報処理方法。

[請求項12] マスタ装置とスレーブ装置との間の通信で用いられる生成多項式の候補を複数の多項式の中から候補多項式として選択する選択処理と、

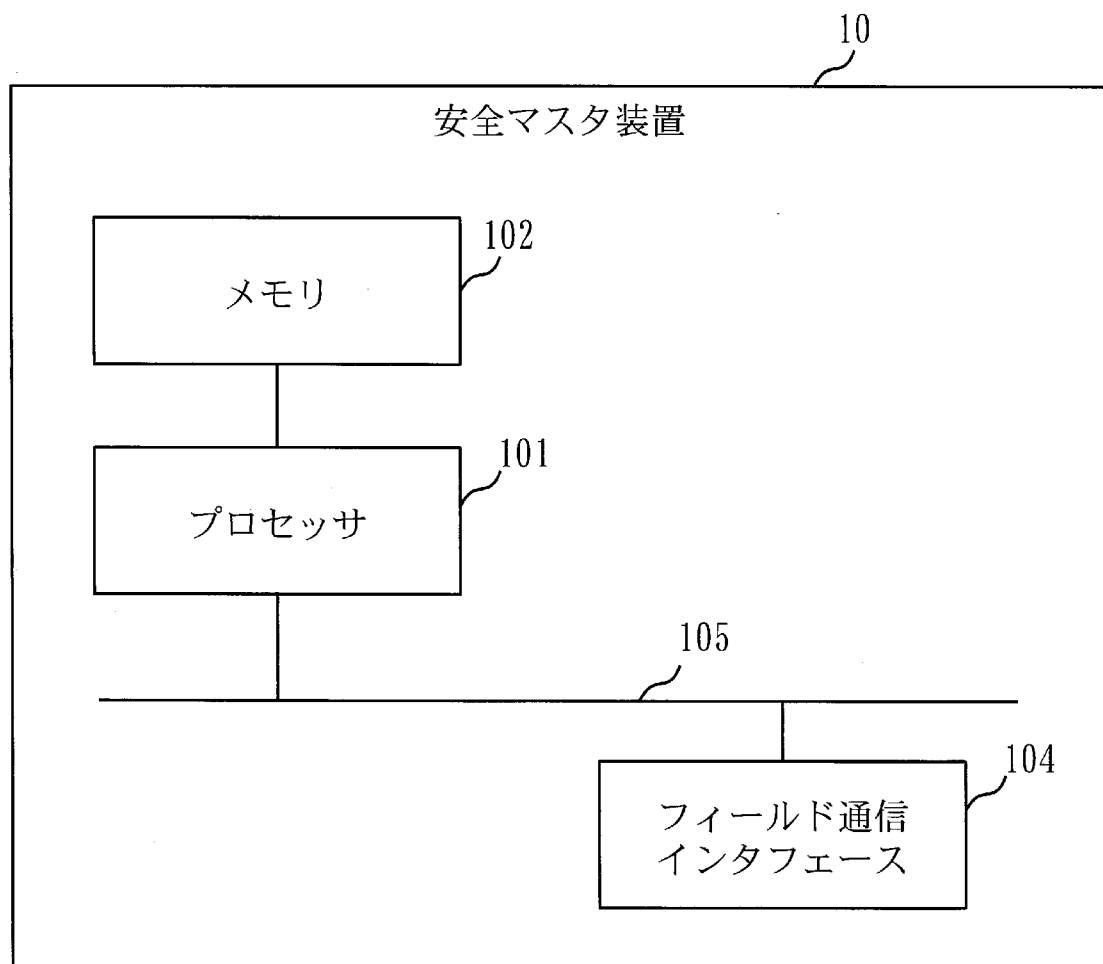
前記候補多項式を用いた計算が前記マスタ装置及び前記スレーブ装置の各々で規定の期限までに完了するか否かを判定する判定処理と、

前記候補多項式を用いた計算が前記マスタ装置及び前記スレーブ装置の各々で前記期限までに完了すると前記判定処理により判定された場合に、前記候補多項式を前記生成多項式に指定する指定処理とをコンピュータに実行させる情報処理プログラム。

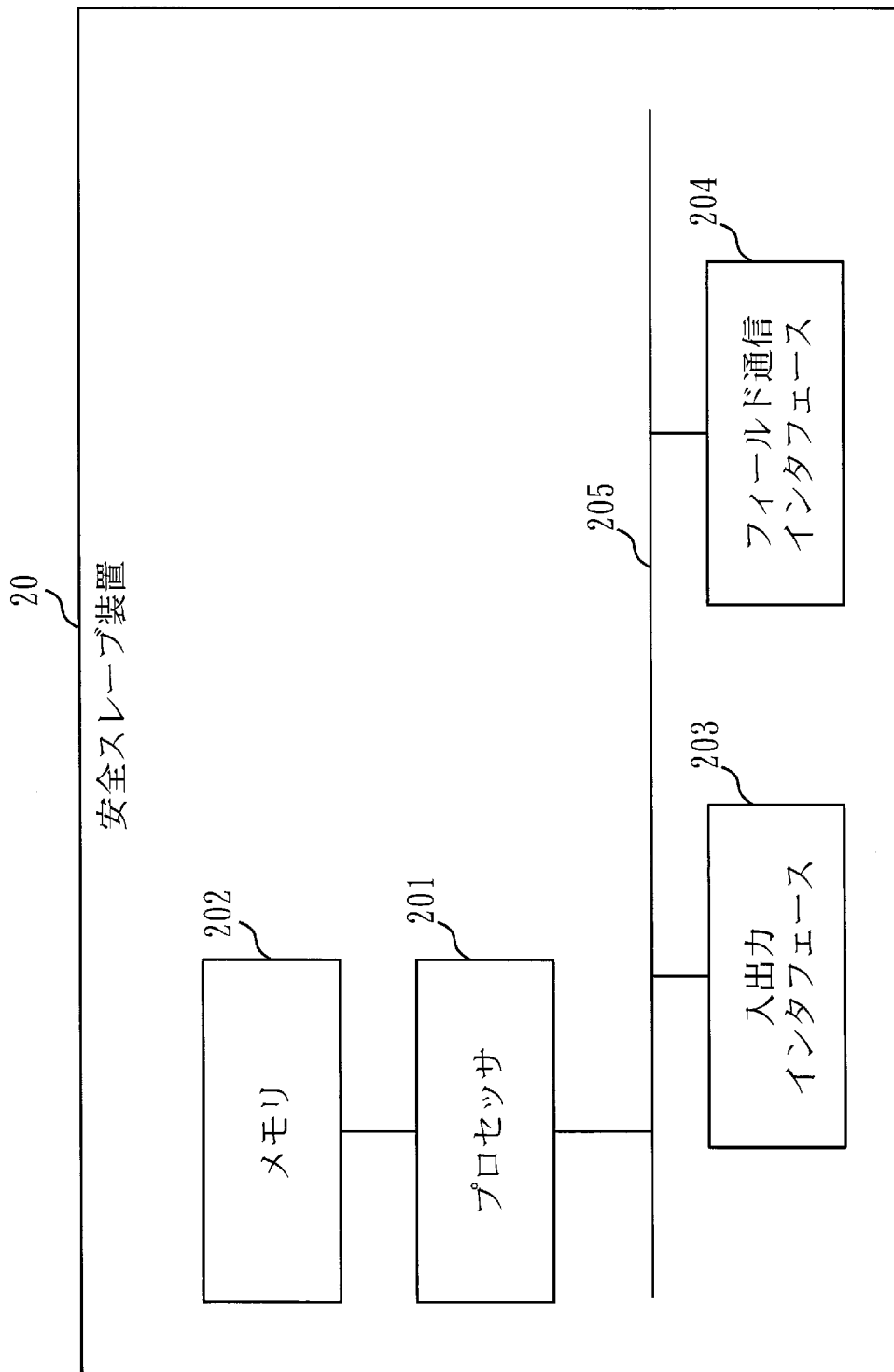
[図1]



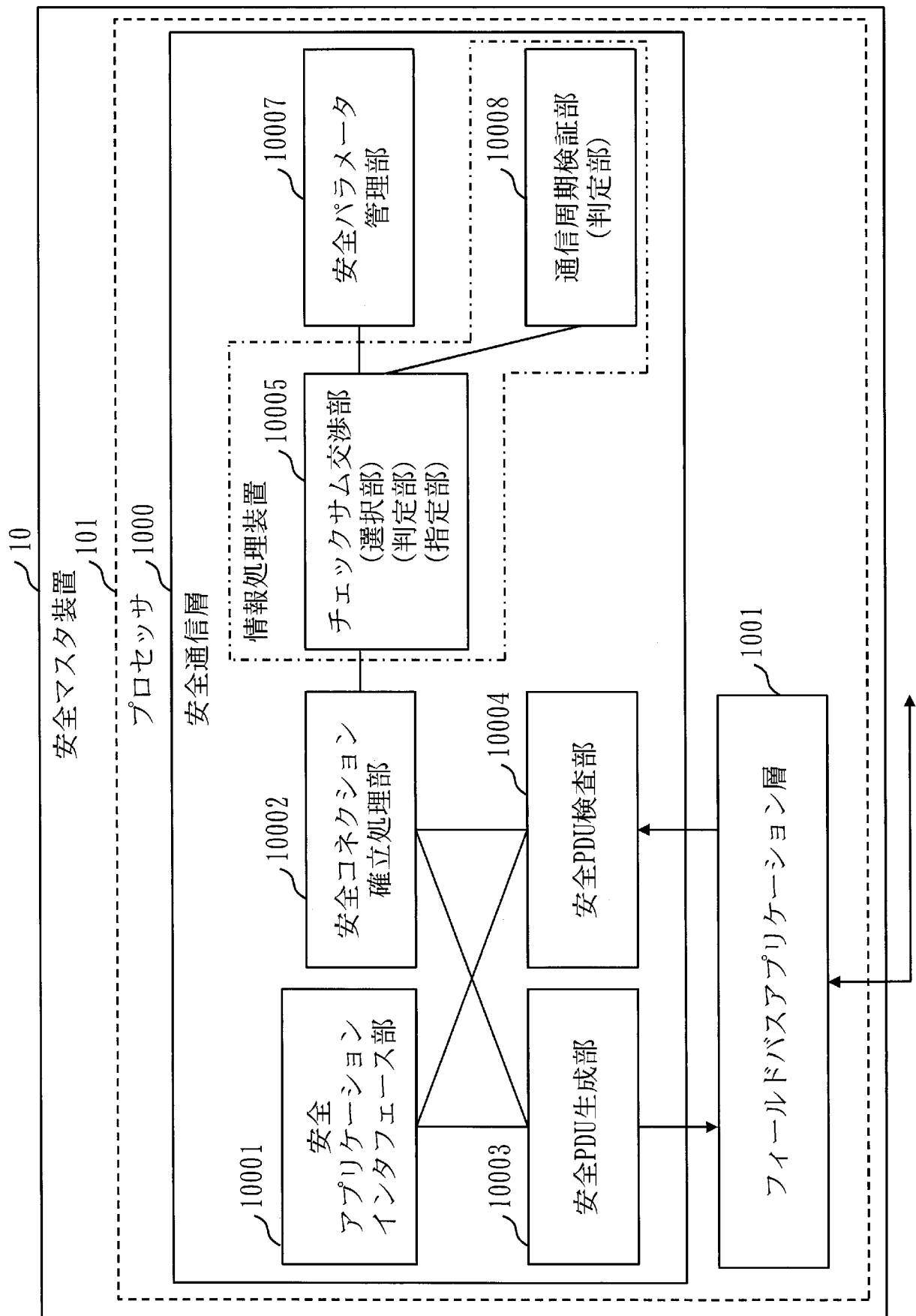
[図2]



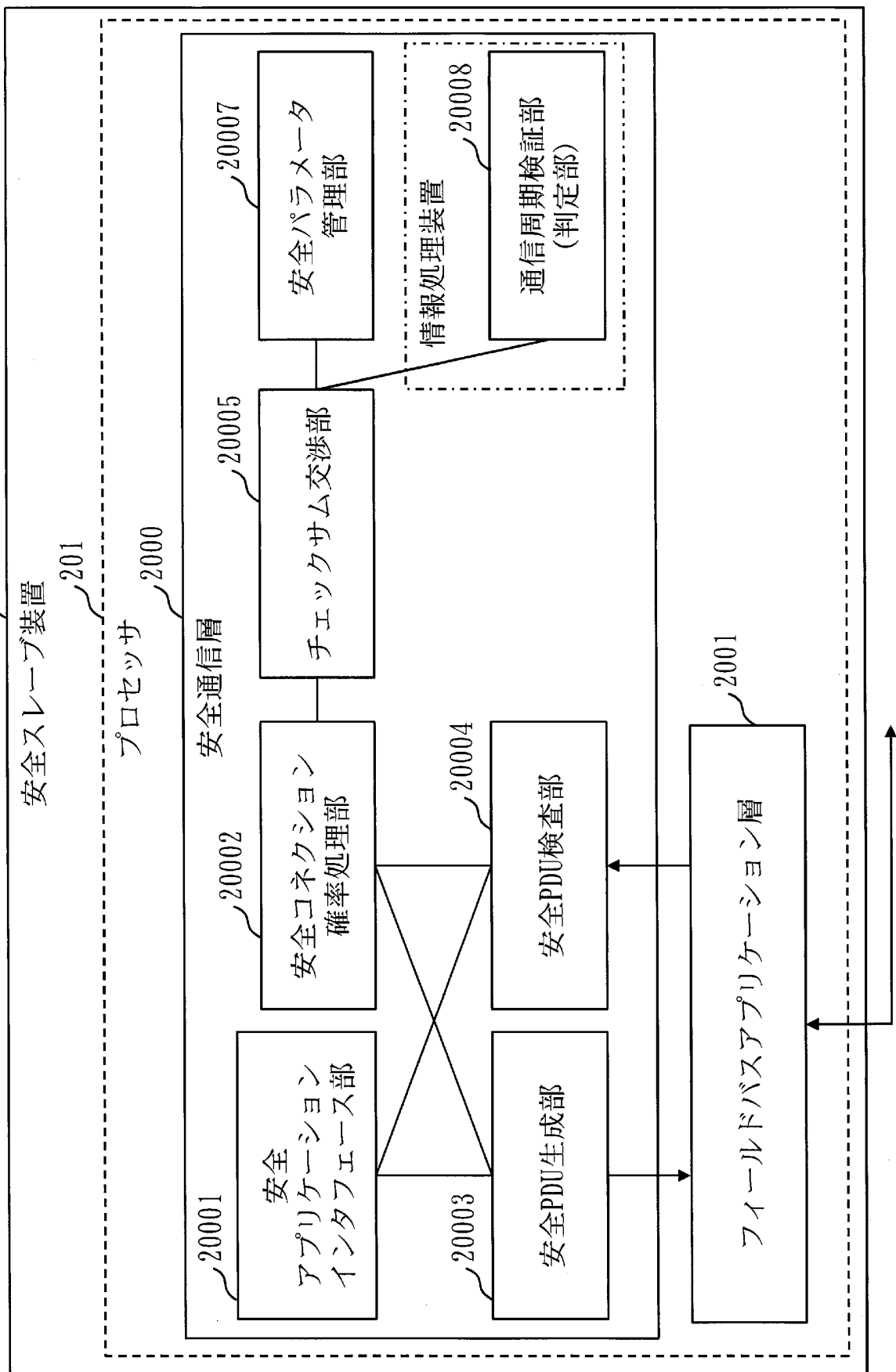
[図3]



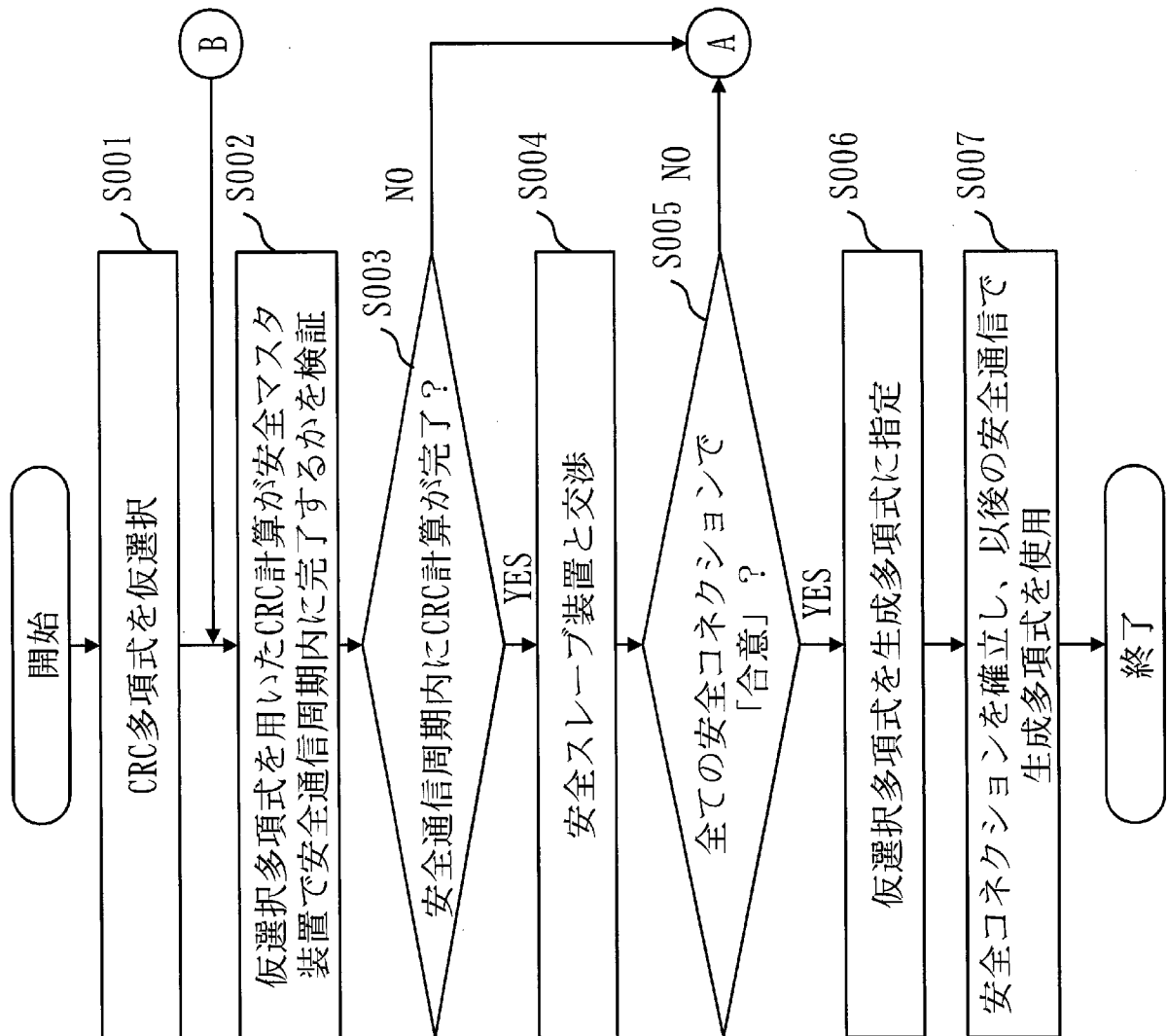
[図4]



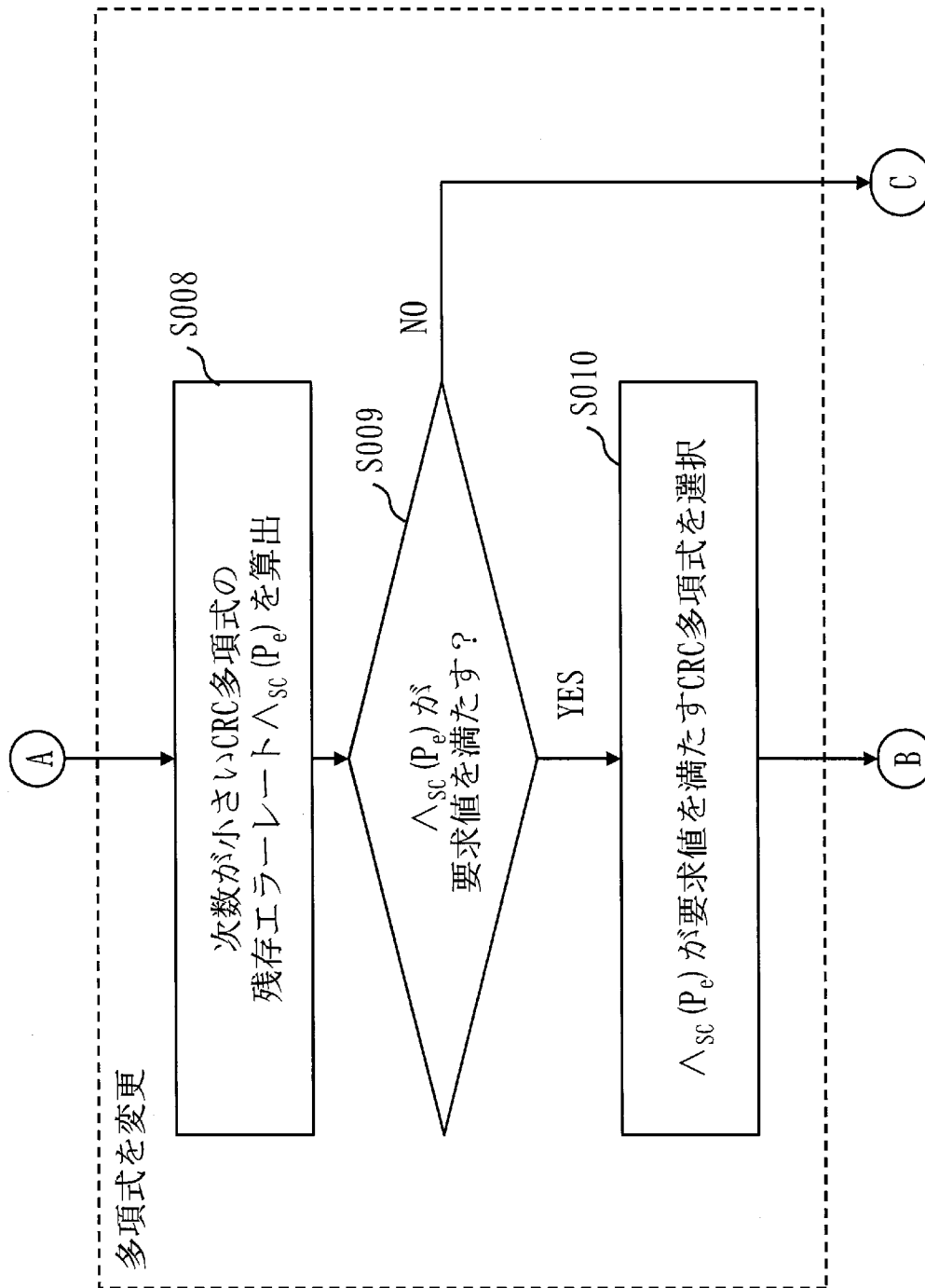
[図5]



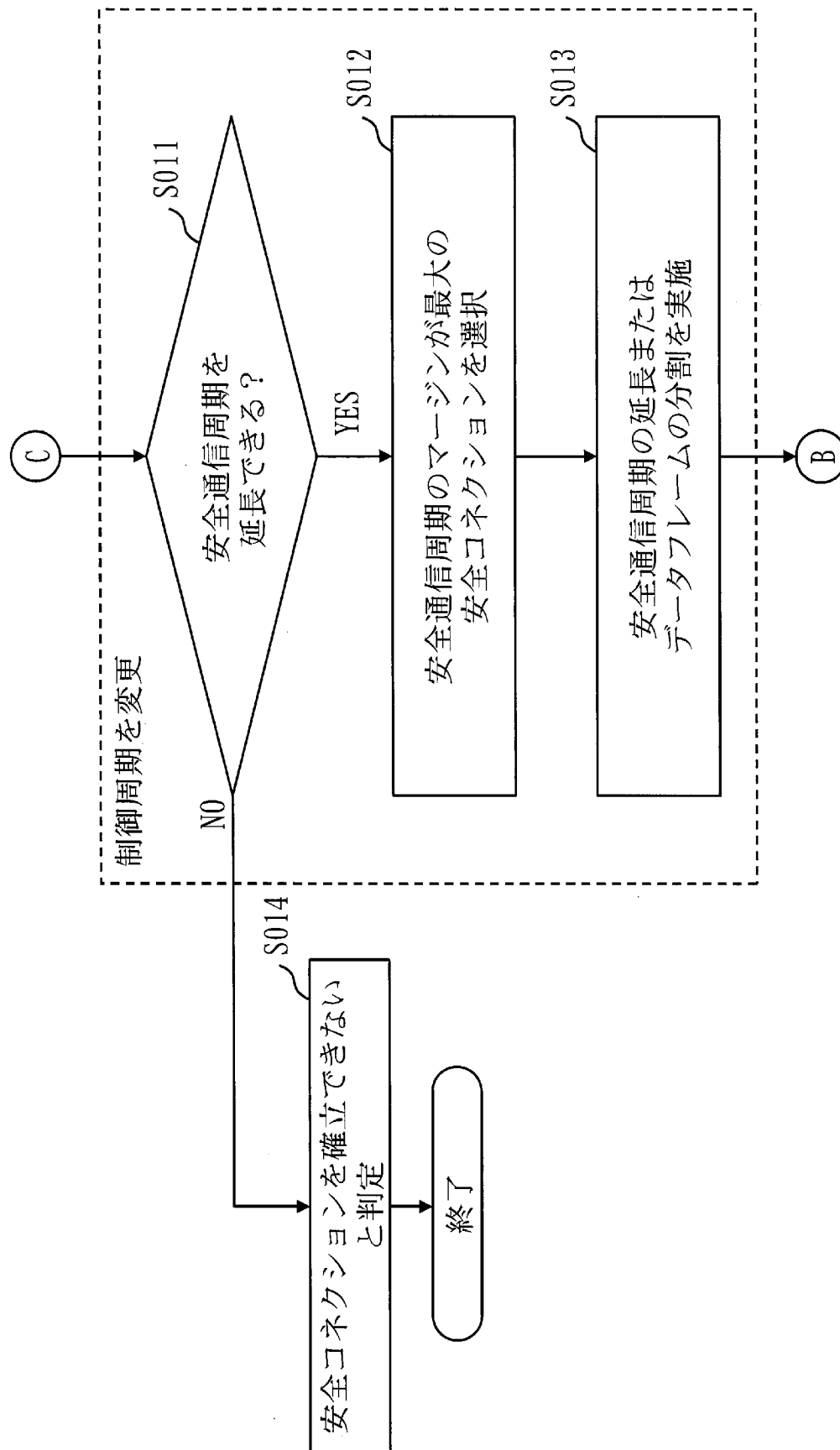
[図6]



[図7]



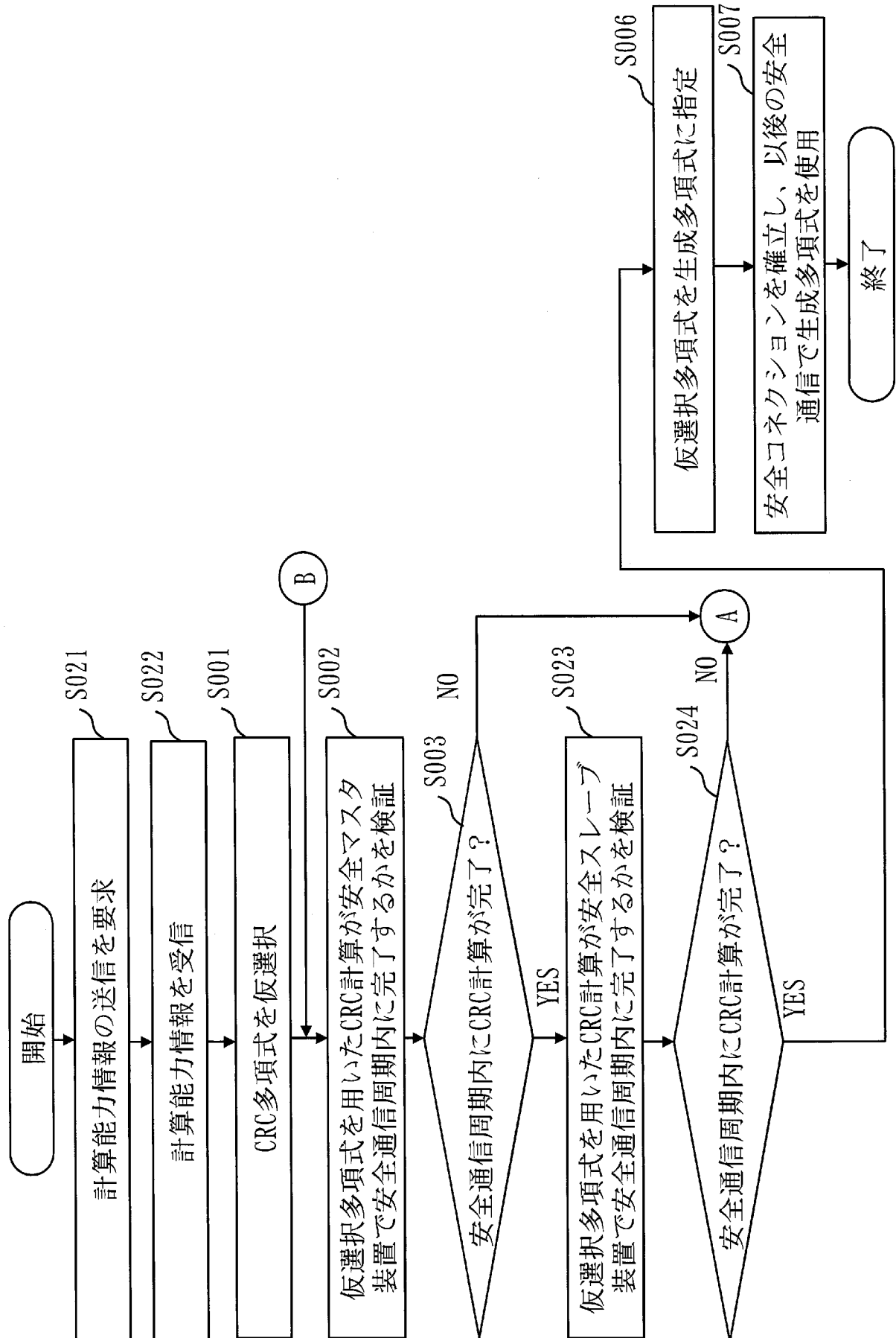
[図8]



[図9]

番号	次数	多項式	最小ハミング距離	分布係数 A_i
1	CRC-8	...	...	...
2	CRC-16	...	...	...
3	CRC-24	...	...	...
4	CRC-32	...	...	...

[図10]



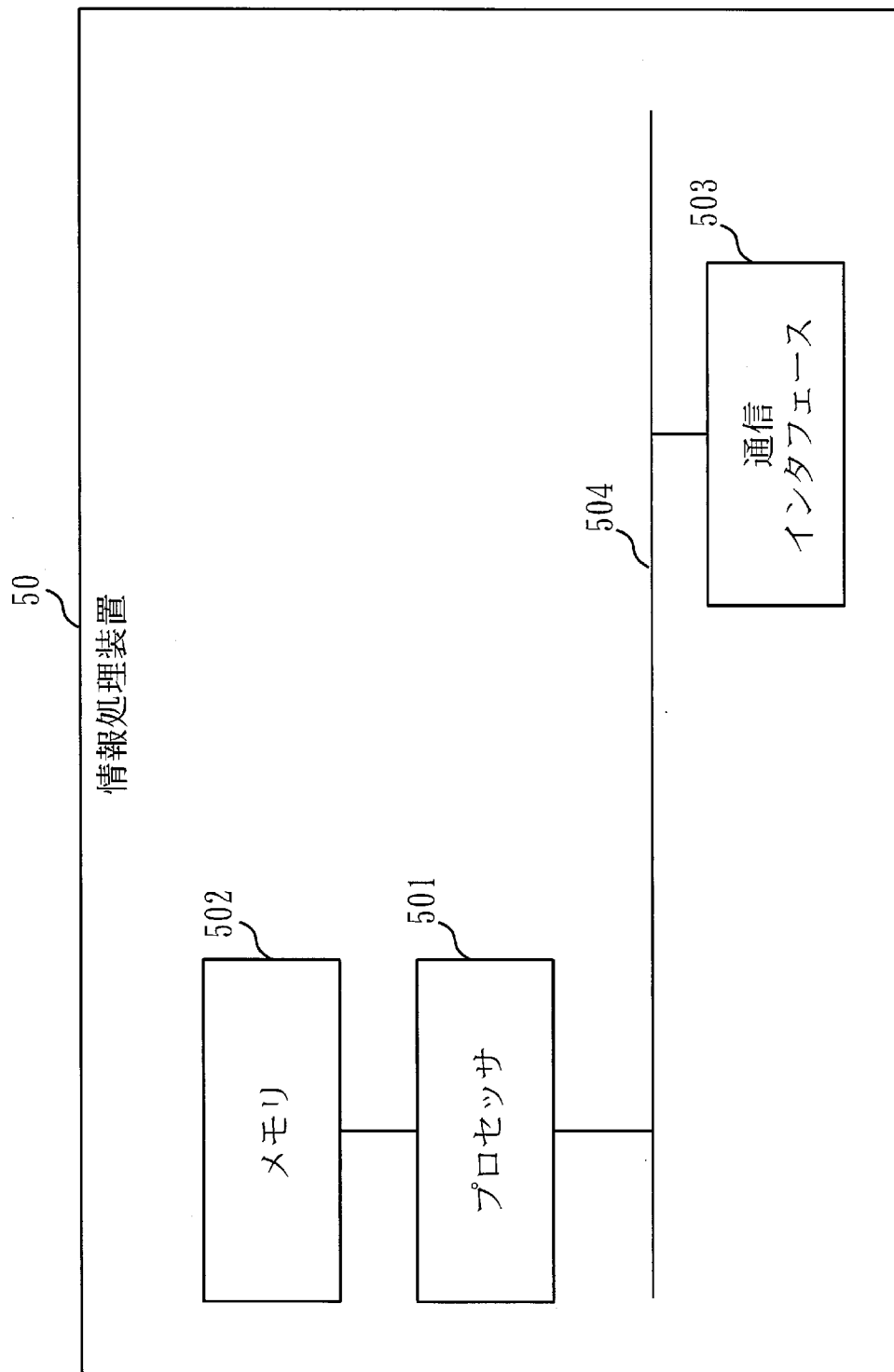
[図11]

CRC多項式	実現可能な通信周期
CRC-8	3.0 ms
CRC-16	3.5 ms
CRC-24	4.5 ms
CRC-32	× (未対応)

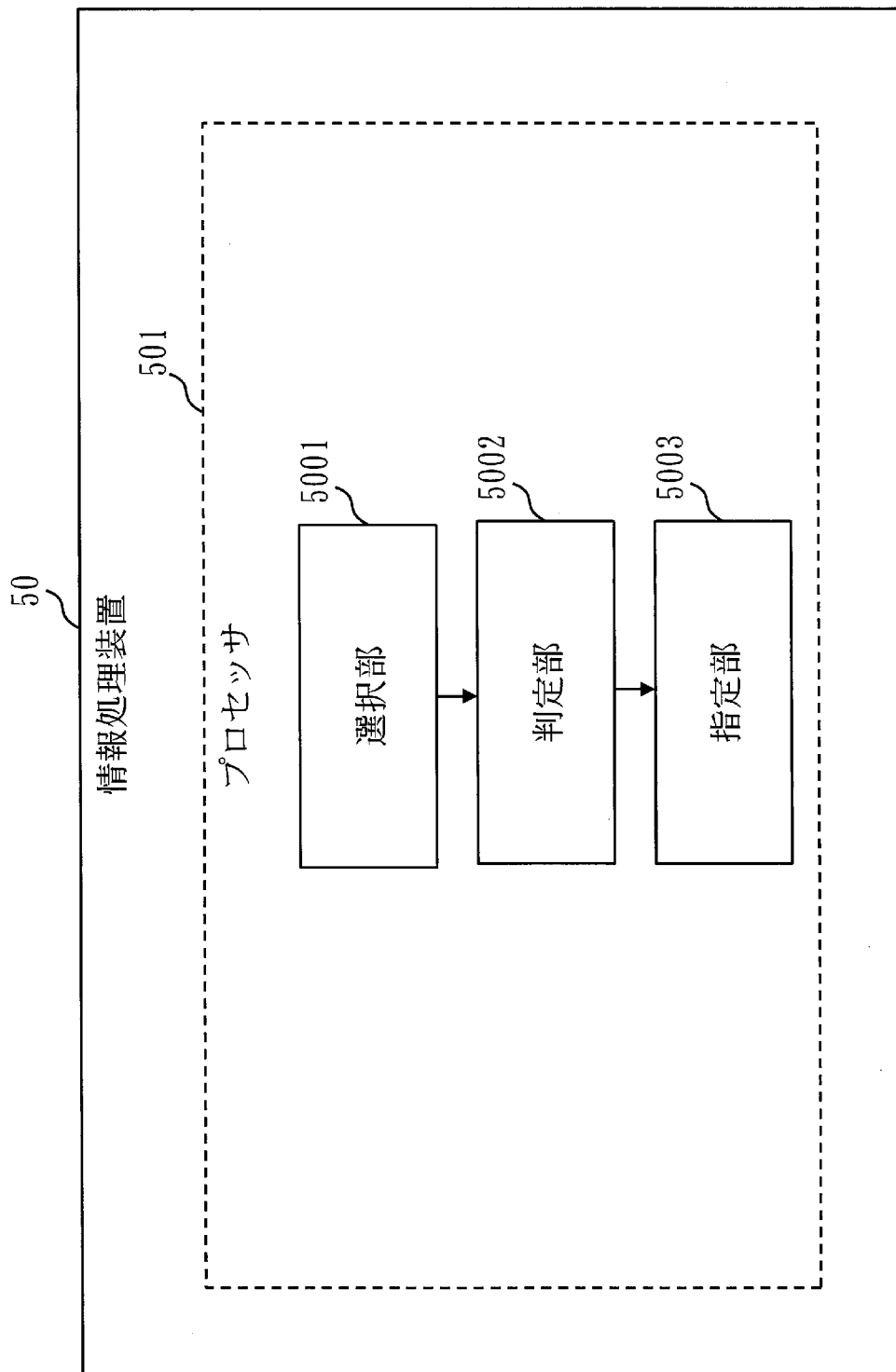
[図12]

番号	次数	多項式	最小ハミング距離	分布係数 A_i
1	CRC-8	...	...	...
2	CRC-8 (A) + CRC-8 (B)	...	...	...
3	CRC-16	...	...	...
4	CRC-16 (A) + CRC-16 (B)	...	...	...
5	CRC-24	...	...	...
6	CRC-32	...	...	...

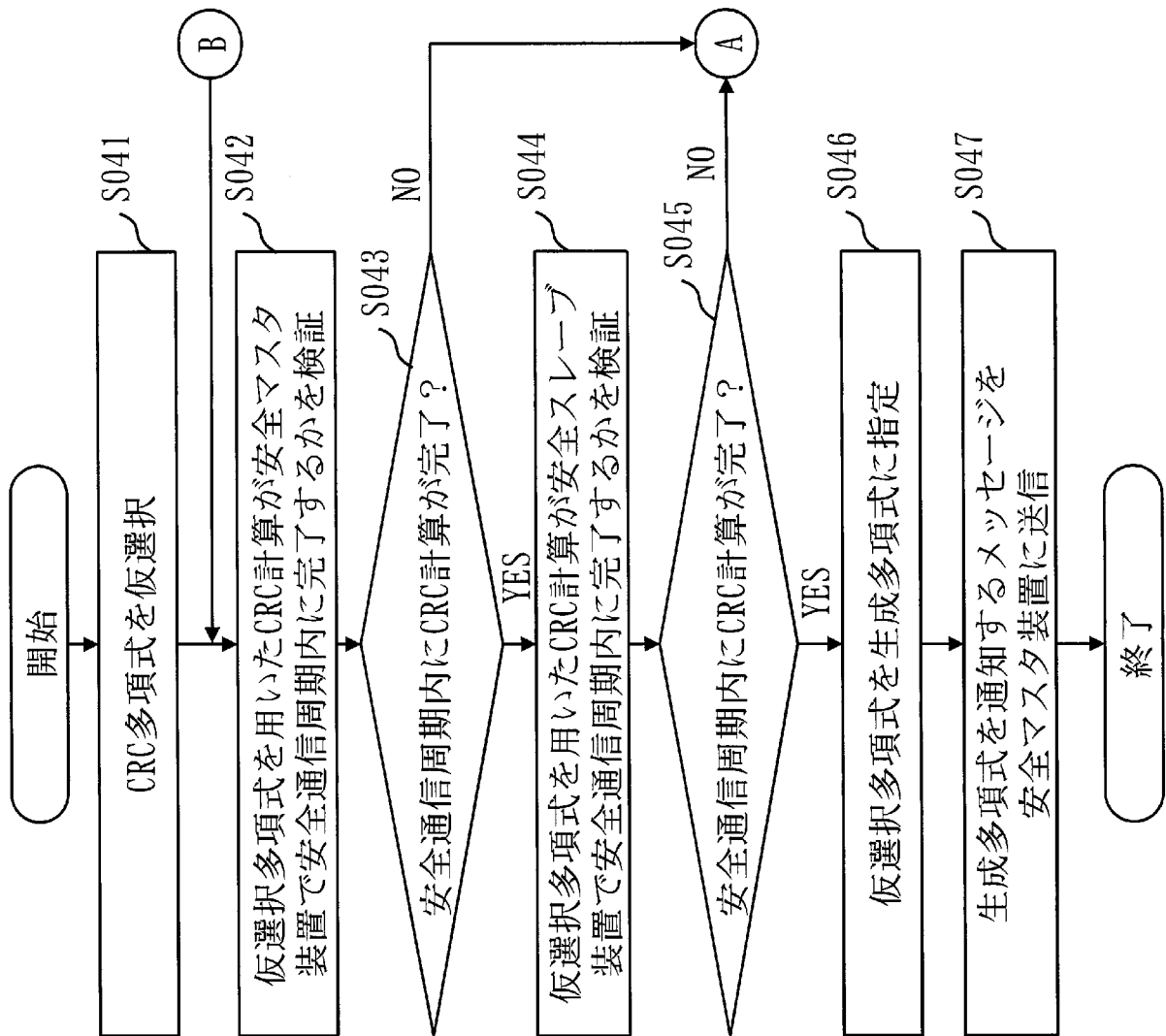
[図13]



[図14]



[図15]



INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2018/016884

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	JP 2010-206394 A (MITSUBISHI ELECTRIC CORP.) 16 September 2010 (Family: none)	1-12
A	WO 2017/212547 A1 (MITSUBISHI ELECTRIC CORP.) 14 December 2017 & TW 201743208 A	1-12
A	JP 2010-124260 A (NEC ENGINEERING LTD.) 03 June 2010 (Family: none)	1-12
A	JP 2016-218867 A (YASKAWA ELECTRIC CORP.) 22 December 2016 & US 2016/0344429 A1	1-12

☒ 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
04.07.2018

Date of mailing of the international search report
17.07.2018

Name and mailing address of the ISA/
Japan Patent Office
3-4-3, Kasumigaseki, Chiyoda-ku,
Tokyo 100-8915, Japan

Authorized officer

Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2018/016884

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	久場亮平他, 機能安全通信における安全データサイズ拡張方式の評価, 電子情報通信学会 2014 年総合大会講演論文集 情報・システム 1, March 2014, p. 121, D-10-2, non-official translation (KUBA, Ryohei et al. Evaluation of Secure Data Size Expansion Method for Function Safety Communication. Proceedings of the 2014 IEICE General Conference: Information/Systems 1)	1-12

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	JP 2010-206394 A（三菱電機株式会社）2010.09.16,（ファミリーなし）	1-12
A	WO 2017/212547 A1（三菱電機株式会社）2017.12.14, & TW 201743208 A	1-12
A	JP 2010-124260 A（NECエンジニアリング株式会社）2010.06.03,（ファミリーなし）	1-12

☒ 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

04.07.2018

国際調査報告の発送日

17.07.2018

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）

谷岡 佳彦

5 K

3 4 6 3

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	JP 2016-218867 A (株式会社安川電機) 2016.12.22, & US 2016/0344429 A1	1-12
A	久場 亮平 他, 機能安全通信における安全データサイズ拡張方式の評価, 電子情報通信学会 2014 年総合大会講演論文集 情報・システム 1, 2014.03, p.121, D-10-2	1-12