

(11) 特許出願公開番号

特開2017-103677

(P2017-103677A)

(43) 公開日 平成29年6月8日(2017.6.8)

(51) Int. Cl.	F I	テーマコード (参考)
H04L 12/66 (2006.01)	H04L 12/66	B 5H220
G06F 21/55 (2013.01)	G06F 21/55	5K030
G05B 19/042 (2006.01)	G05B 19/042	

審査請求 未請求 請求項の数 11 O L (全 20 頁)

(21) 出願番号 特願2015-236784 (P2015-236784)
(22) 出願日 平成27年12月3日 (2015. 12. 3)

(71) 出願人 000003078
株式会社東芝
東京都港区芝浦一丁目1番1号

(74) 代理人 110002147
特許業務法人酒井国際特許事務所

(72) 発明者 丸地 俊也
東京都港区芝浦一丁目1番1号 株式会社
東芝内

(72) 発明者 中谷 博司
東京都港区芝浦一丁目1番1号 株式会社
東芝内

(72) 発明者 竹原 潤
東京都港区芝浦一丁目1番1号 株式会社
東芝内

[最終頁に続く](#)

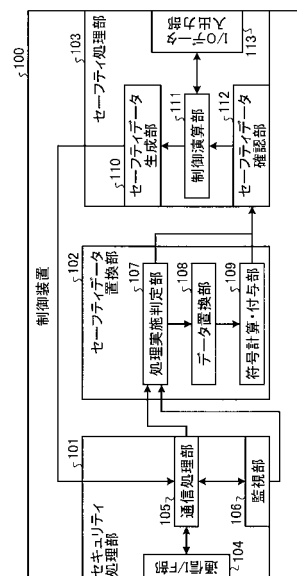
(54) 【発明の名称】 制御装置

(57) 【要約】

【課題】制御装置におけるセキュリティ機能とセーフティ機能の両立を実現し、当該制御装置を含むシステム全体のアベイラビリティの低減を回避する。

【解決手段】実施形態の制御装置は、セキュリティ処理部と、セーフティデータ置換部と、セーフティ処理部を備える。セキュリティ処理部にて、サービス不能攻撃を監視する。セーフティデータ置換部は、セキュリティ処理部によりサービス不能攻撃が検出された場合に、セキュリティ処理部から受信した通信フレームに含まれる所定のデータを健全であるとされる値に置換する。セーフティ処理部は、セーフティデータ置換部から受信した通信フレームの所定のデータから当該通信フレームの健全性を確認し、その健全性が確認された場合に、当該通信フレームのデータを基に配下の装置を制御するための制御値を配下の装置へ出力する。

【選択図】 図1



【特許請求の範囲】

【請求項 1】

通信フレームの入出力を行う通信インタフェース部と、
前記通信フレームの送受信に係る統計情報を管理する通信処理部と、
前記統計情報を基にサービス不能攻撃を監視する監視部と、
を有するセキュリティ処理部と、
前記監視部によりサービス不能攻撃が検出された場合に、受信した通信フレームに含まれる所定のデータに対する置換処理を実施すると判定する処理実施判定部と、
前記処理実施判定部で置換処理を実施すると判定された場合に、前記セキュリティ処理部から受信した通信フレームの前記所定のデータを健全であるとされる値に置換するデータ置換部と、
前記置換がなされた通信フレームの誤り検出符号を再計算し付与する符号計算・付与部と、
を有するセーフティデータ置換部と、
前記セーフティデータ置換部から受信した通信フレームの前記所定のデータから当該通信フレームの健全性を確認するセーフティデータ確認部と、
前記セーフティデータ確認部により前記セーフティデータ置換部から受信した通信フレームの健全性が確認された場合に、当該通信フレームのデータを基に配下の装置を制御するための制御値を算出する制御演算部と、
前記配下の装置へ前記制御値を出力し、配下の装置からのデータを入力する I / O データ入出力部と、
を有するセーフティ処理部と
を具備する制御装置。

【請求項 2】

前記処理実施判定部は、前記監視部によりサービス不能攻撃が検出されていない場合、受信した通信フレームを前記セーフティ処理部に転送する、請求項 1 に記載の制御装置。

【請求項 3】

前記セキュリティ処理部と前記セーフティデータ置換部との間に接続され、送受信する通信フレームに対する暗号化および復号の処理を施す暗号化／復号部を、さらに具備する請求項 1 または請求項 2 に記載の制御装置。

【請求項 4】

前記セーフティ処理部は、通信フレーム毎に変化するセーフティヘッダを含むセーフティデータを生成するセーフティデータ生成部をさらに有し、配下の装置からの入力データに対し前記セーフティデータを生成し、生成したセーフティデータを含む通信フレームを前記セキュリティ処理部を介して出力する請求項 1 から請求項 3 のいずれか 1 項に記載の制御装置。

【請求項 5】

前記監視部は、前記統計情報として前記通信フレームの受信数を監視し、該受信数が一定時間内に予め規定された値を超えた場合は、前記通信処理部に通信フレームの新規受信を禁止させ、前記セーフティデータ置換部の前記処理実施判定部に受信禁止信号を送信し、

前記処理実施判定部は、前記受信禁止信号を受信した場合に、置換処理を実施すると判定し、

前記データ置換部は、前回、前記セーフティデータ置換部から前記セーフティ処理部に送信した通信フレーム中の前記セーフティヘッダを、今回値と前回値の差分が許容範囲内となるようインクリメントした値に置換し、前記符号計算・付与部は、置換後の通信フレームを元に再度誤り検出符号を計算し付与した通信フレームを、前記セーフティ処理部へ送信する

請求項 4 に記載の制御装置。

【請求項 6】

10

20

30

40

50

前記データ置換部は、前記監視部からの受信禁止信号の解除を検出すると、前記データ置換部は、新規受信した通信フレーム内の前記セーフティヘッダの今回値と、前記セーフティデータ置換部から前記セーフティ処理部へ送信した通信フレームに含まれる前記セーフティヘッダの前回値との差分が許容範囲内となるよう置換する請求項４に記載の制御装置。

【請求項７】

前記処理実施判定部が、前記受信禁止信号の解除を検出すると、前記データ置換部は、新規受信した通信フレームの前記セーフティヘッダと前回置換した前記セーフティヘッダとの差分を演算し、その差分を新規受信した通信フレーム内の前記セーフティヘッダに加減算することにより、前記今回値と前記前回値との差分が前記許容範囲内となるよう置換する請求項６に記載の制御装置。

10

【請求項８】

前記セーフティデータ置換部は、前記監視部によりサービス不能攻撃が一度検出された後は、前記サービス不能攻撃の有無によらず継続して前記セキュリティ処理部から受信した通信フレーム内の前記所定のデータを、前記データ置換部および前記符号計算・付与部により更新することを特徴とする請求項１から請求項３のいずれか１項に記載の制御装置。

【請求項９】

サービス不能攻撃の継続時間に対する許容値を外部から前記処理実施判定部に入力することを可能とした請求項１から請求項８のいずれか１項に記載の制御装置。

20

【請求項１０】

サービス不能攻撃の継続時間が前記許容値を超えた場合、前記処理実施判定部は、ユーザ側装置に警告を伝達することを可能とした請求項９に記載の制御装置。

【請求項１１】

サービス不能攻撃の継続時間が前記許容値を超えた場合、前記セーフティデータ置換部は、前記データ置換部および前記符号計算・付与部による前記所定のデータの更新をせずに、前回出力した通信フレームを前記セーフティ処理部へ転送する請求項９または１０に記載の制御装置。

【発明の詳細な説明】

【技術分野】

30

【０００１】

本発明の実施形態は、制御装置に関する。

【背景技術】

【０００２】

従来より、プラント等を制御する制御システムは、社会基盤、産業基盤を支えるため２４時間３６５日の連続運転できることが最重要要件とされている。このような制御システムは、悪意ある第三者からの攻撃等により稼働が阻害された場合、社会的な影響が非常に大きい。従来の制御システムはクローズドシステムで構成され、外部ネットワークと接続されていないため、悪意ある第三者からの攻撃等の脅威は殆ど意識されてこなかった。

【先行技術文献】

40

【特許文献】

【０００３】

【特許文献１】特開２０１３－１９６０５８号公報

【特許文献２】特開２０１２－０４３２３０号公報

【発明の概要】

【発明が解決しようとする課題】

【０００４】

しかしながら、近年、制御システムに汎用ＯＳが採用されるようになり、外部ネットワークからのリモートコントロールができるようになるなど、システムの構成・使用状況に変化が生じてきている。そのため、制御システムで従来から求められている安全性（以下

50

セーフティと称す) と、セキュリティとを両立した制御システムが望まれている。

【0005】

本発明が解決しようとする課題は、制御装置におけるセキュリティ機能とセーフティ機能の両立を実現し、両機能をもたせた当該制御装置が制御するシステムのアベイラビリティの低減を回避することができる制御装置を提供することである。

【課題を解決するための手段】

【0006】

実施形態の制御装置は、セキュリティ処理部と、セーフティデータ置換部と、セーフティ処理部を備える。セキュリティ処理部は、通信フレームの入出力を行う通信インタフェース部と、通信フレームの送受信に係る統計情報を管理する通信処理部と統計情報を基にサービス不能攻撃を監視する監視部と、を有する。セーフティデータ置換部は、監視部によりサービス不能攻撃が検出された場合に、受信した通信フレームに含まれる所定のデータに対する置換処理を実施すると判定する処理実施判定部と処理実施判定部で置換処理を実施すると判定された場合に、セキュリティ処理部から受信した通信フレームの所定のデータを健全であるとされる値に置換するデータ置換部と置換がなされた通信フレームの誤り検出符号を再計算し付与する符号計算・付与部とを有する。セーフティ処理部は、セーフティデータ置換部から受信した通信フレームの所定のデータから当該通信フレームの健全性を確認するセーフティデータ確認部と、セーフティデータ確認部によりセーフティデータ置換部から受信した通信フレームの健全性が確認された場合に、当該通信フレームのデータを基に配下の装置を制御するための制御値を算出する制御演算部と、配下の装置へ制御値を出力し、配下の装置からのデータを入力するI/Oデータ入出力部と、を有する。

10

20

【図面の簡単な説明】

【0007】

【図1】図1は、第1の実施形態にかかる制御装置の構成を示すブロック図である。

【図2】図2は、第1の実施形態における監視部の動作フローを示すフローチャートである。

【図3】図3は、第1の実施形態におけるセーフティデータ置換部の動作フロー（通常処理）を示すフローチャートである。

【図4】図4は、第1の実施形態におけるフレームフォーマットの一例を示す図である。

30

【図5】図5は、第1の実施形態におけるセーフティ処理部の動作フローを示すフローチャートである。

【図6】図6は、第1の実施形態におけるサービス不能攻撃が収束した場合のセーフティデータ置換部の動作フローを示すフローチャートである。

【図7】図7は、第1の実施形態にかかる制御装置の、セキュリティ処理部、セーフティデータ置換部、およびセーフティ処理部間のデータの流れおよび動作を示す図である。

【図8】図8は、第2の実施形態にかかる制御装置の構成を示すブロック図である。

【図9A】図9Aは、第2の実施形態におけるフレームフォーマットの一例を示す図である。

【図9B】図9Bは、第2の実施形態における認証データベースのデータ構造の一例を示す図である。

40

【図10】図10は、第3の実施形態におけるセーフティデータ置換部の動作フロー（通常処理）を示すフローチャートである。

【図11】図11は、第3の実施形態にかかる制御装置の、セキュリティ処理部、セーフティデータ置換部、およびセーフティ処理部間のデータの流れおよび動作を示す図である。

【図12】図12は、第4の実施形態にかかる制御装置およびユーザ端末の構成を示すブロック図である。

【図13】図13は、第4の実施形態にかかる制御装置およびユーザ端末の構成（他の例）を示すブロック図である。

50

【図 1 4】図 1 4 は、第 4 の実施形態におけるセーフティデータ置換部の動作フローを示すフローチャートである。

【図 1 5】図 1 5 は、第 4 の実施形態にかかる制御装置の、セキュリティ処理部、セーフティデータ置換部、およびセーフティ処理部間のデータの流れおよび動作を示す図である。

【発明を実施するための形態】

【0008】

(概要)

プラント等を制御する制御システムにおけるセーフティ機能とセキュリティ機能に関して、以下が知られている。

【0009】

セーフティの観点では、IEC 61508「電気・電子・プログラマブル電子安全関連系の機能安全」が定められている。セーフティ機能を実現する代表的な手法の一つとして、ブラックチャネル通信と呼ばれる手法が確立されている。これは、送信側で通信フレーム（以下、フレームと記す）内に時刻情報やシーケンス番号など、フレーム毎に変化する値や、CRC (Cyclic Redundancy Check) などの誤り検出符号を付与し、受信側でそれらの情報の健全性を確認する手法である。上記フレーム毎に変化する値が一定の値から変化しない異常や、フレームの大幅な損失時など許容値以上の変化が生じる異常を、受信側で検出し、システムが安全側に遷移するようにする。

【0010】

一方、セキュリティの観点では、標準化規格の策定や評価・認証機関の整備等、制御システムセキュリティのための取り組みが本格化しつつあり、保護機能や開発プロセスを定めた IEC 国際標準規格 (IEC 62443) が策定中である。セキュリティにおける代表的な攻撃手法としてパケット (フレーム) を攻撃対象に大量に送信し、通信障害を生じさせる DoS (Denial of Service) 攻撃と呼ばれる攻撃手法が存在する。本攻撃への対応方法としては、例えば、受信したフレームの数を監視し、その数が一定値以上の値になった場合には DoS 攻撃を受けているとみなして受信を禁止し、DoS 攻撃検出後は、一定間隔で受信したフレームの数を監視し、その数が閾値を下回った場合に DoS 攻撃が収束したと判断して受信を許可する DoS 攻撃対策がある。

【0011】

しかしながら、上記のようなセーフティのためのブラックチャネル通信機能とセキュリティのための DoS 攻撃対策機能とを共に制御装置に実装した場合、以下の問題が生じる。

【0012】

DoS 攻撃対策機能により DoS 攻撃を検出し、フレームの受信を禁止する場合、DoS 攻撃が収束するまでの間フレームは受信されない。このため、DoS 攻撃の収束後、新たにフレームを受信したとき、受信したフレームに含まれるタイムスタンプやシーケンス番号の値の変化が許容範囲外となると、セーフティ機能により、システムが安全停止してしまう。つまり、制御装置にセーフティ機能とセキュリティ機能である DoS 攻撃対策機能を共存させた場合、DoS 攻撃対策機能によりシステムのアベイラビリティが損なわれてしまう。

【0013】

以下に説明する諸実施形態にかかる制御装置は、前段のセキュリティ機能を有する機能部と後段のセーフティ機能を有する機能部との間に、DoS 攻撃等のサービス不能攻撃時にブラックチャネル通信におけるタイムスタンプやシーケンス番号の付け替え (置換)、誤り検出符号の再計算および付与をすることにより、セーフティ機能によってシステムが自動的に安全停止しないようにする機能部を設けている。これにより、以下に説明する制御装置は、セキュリティ機能とセーフティ機能の両立を実現し、当該制御装置が制御するシステムのアベイラビリティの低減を回避する。

【0014】

10

20

30

40

50

(第1の実施形態)

はじめに、第1の実施形態にかかる制御装置について図1を用いて説明する。図1は、第1の実施形態にかかる制御装置の構成を示すブロック図である。

【0015】

図1に示す制御装置100は、図示しない配下の装置を制御するとともに、上位装置に対して制御状態の通知等をする装置であり、セキュリティ処理部101、セーフティデータ置換部102、およびセーフティ処理部103の3つのブロックから構成される。これらは同一のハードウェア部品上に構成されてもよいし、別々のハードウェア部品上に構成されてもよい。

【0016】

セキュリティ処理部101は、イーサネット（登録商標）等によるネットワークを介しフレームを送受信するためのインタフェースとなる通信I/F部104と、この通信I/F部104に接続され、受信したフレームを処理する通信処理部105と、通信処理部105に接続され、当該制御装置100におけるフレーム受信状況を監視する監視部106とを備える。

【0017】

通信I/F部104は、上位装置などネットワーク上の他の装置からのフレームを受信し、通信処理部105へ受信したフレームを転送する。また、通信I/F部104は、通信処理部105からのデータ（フレーム）を上位装置などネットワーク上の他の装置に送信する。

【0018】

通信処理部105は、フレーム受信状況としてのフレーム受信数（受信したフレームの数）など、統計情報を管理する。また、通信処理部105は、監視部106により受信が許可されている場合、通信I/F部104からのフレームをセーフティデータ置換部102へ転送し、監視部106により受信が禁止されている場合、通信I/F部104からのフレームを破棄する。また、通信処理部105は、セーフティ処理部103からのフレームを通信I/F部104へ転送する。

【0019】

監視部106は、上記のように通信処理部105で管理されるフレーム受信状況を監視し、フレームの受信の禁止／許可にかかる制御を行う。この監視部106の詳細については、後述する。

【0020】

セーフティデータ置換部102は、セキュリティ処理部101の後段に接続される。このセーフティデータ置換部102は、前述の通信処理部105および監視部106からの情報（後述）が入力される処理実施判定部107と、処理実施判定部107に接続され、受信したフレームに含まれる健全性確認データ（所定のデータ）のセーフティヘッダの置換（後述）を行うデータ置換部108と、データ置換部108に接続され、健全性確認データに含まれる誤り検出符号（または誤り訂正符号）を、セーフティヘッダが置換されたフレームについて再計算しあらためて付与する符号計算・付与部109とを備える。

【0021】

セーフティ処理部103は、セーフティデータ置換部102の後段に接続される。このセーフティ処理部103は、フレーム毎に変化する値をもつセーフティヘッダ、および誤り検出符号からなる安全性確認データを含むセーフティデータを生成しフレームに付与するセーフティデータ生成部110と、セーフティデータ置換部102からのデータの安全性を確認し、安全性が確認されたデータを制御演算部111へ転送するセーフティデータ確認部112と、セーフティデータ確認部112に接続され、図示しない配下の装置からのデータを処理しセーフティデータ生成部110に出力し、セーフティデータ確認部112からのデータを基に配下の装置に対する制御データ（制御値）を演算する制御演算部111と、制御演算部111からの制御データを配下の装置へ出力するとともに、配下の装置からのデータを制御演算部111へ出力するI/Oデータ入出力部113とを備える。

10

20

30

40

50

なお、配下の装置から I / O データ入出力部 1 1 3 へ入力されたデータは、制御演算部 1 1 1 およびセーフティデータ生成部 1 1 0 を介し、セーフティデータ置換部 1 0 2 を経由することなく通信処理部 1 0 5 へ転送され、通信 I / F 部 1 0 4 を介して上位装置などへ送信される。

【0022】

次に、上記構成による監視部 1 0 6 の動作の詳細について図 2 を用いて説明する。図 2 は、監視部 1 0 6 の動作フローを示すフローチャートである。

【0023】

監視部 1 0 6 は、定周期で通信処理部 1 0 5 が管理しているフレーム受信数を含む統計情報を取得し、この統計情報に含まれるフレーム受信数からその前回値と今回値の差分を計算し、規定時間内に受信したフレームの数（規定時間受信数）を算出する（S 1 0 1）。

10

【0024】

この算出値（規定時間受信数）が規定値（閾値）以上の場合（S 1 0 2 で Y e s）、サービス不能攻撃とみなし、監視部 1 0 6 は、通信処理部 1 0 5 に受信を停止するよう指令を出し（受信停止処理：S 1 0 3）、さらに、セーフティデータ置換部 1 0 2 の処理実施判定部 1 0 7 に受信禁止中信号 O N を伝達する（S 1 0 4）。一方、上記算出値（規定時間受信数）が規定値（閾値）未満の場合（S 1 0 2 で N o）、監視部 1 0 6 は、通信処理部 1 0 5 に受信を許可する指令を出し（受信許可処理：S 1 0 5）、セーフティデータ置換部 1 0 2 の処理実施判定部 1 0 7 に受信禁止中信号 O F F を伝達する（S 1 0 6）。

20

【0025】

このように、本実施形態では、セキュリティ処理部 1 0 1 により、D o S 攻撃に代表されるサービス不能攻撃のような予め規定された許容値を超えた数のフレームを受信した場合には、強制的に受信を拒否する。そして、規定時間内に受信したフレームの数が規定値未満に収まった場合、監視部 1 0 6 は、サービス不能攻撃が収束したと判定し通信処理部 1 0 5 に再び受信を許可する。許可を受けた通信処理部 1 0 5 は、受信したフレームをセーフティデータ置換部 1 0 2 の処理実施判定部 1 0 7 に転送し、監視部 1 0 6 は、受信禁止中信号 O F F を処理実施判定部 1 0 7 に伝達する。以上の処理を定周期で繰り返す。

【0026】

次に、セーフティデータ置換部 1 0 2 の動作（通常処理）について図 3 を用いて説明する。図 3 は、セーフティデータ置換部 1 0 2 の通常処理における動作フローを示すフローチャートである。

30

【0027】

セーフティデータ置換部 1 0 2 の処理実施判定部 1 0 7 は、受信禁止中信号の O N / O F F を判断し、O F F の場合（S 2 0 1 で N o）、セキュリティ処理部 1 0 1 から受信したフレームがあると（S 2 0 6 で Y e s）、このフレームをそのままセーフティ処理部 1 0 3 へ転送し（S 2 0 7）、無い場合は（S 2 0 6 で N o）、S 2 0 1 に戻る。

【0028】

一方、受信禁止中信号が O N の場合は（S 2 0 1 で Y e s）、処理実施判定部 1 0 7 は、セーフティデータ置換部 1 0 2 からセーフティ処理部 1 0 3 へ前回送信したフレーム（前回出力フレーム）を採用し、この前回出力フレームをデータ置換部 1 0 8 に転送する（S 2 0 2）。

40

【0029】

データ置換部 1 0 8 は、この前回出力フレームについて、そのセーフティヘッダを更新する置換（後述）を行う（S 2 0 3）。

【0030】

ここで、図 4 に、フレームフォーマットの一例を示す。同図に示すように、1 つのフレームは、宛先アドレスと、送信元アドレスと、データのタイプを示すデータ識別情報と、データ本体とフレームの健全性を確認するための健全性確認データとからなるセーフティデータとを含んで構成される。健全性確認データ内には、シーケンス番号やタイムスタン

50

プなど、フレーム毎に変化する値を含むセキュリティヘッダと、誤り検出符号（図4の例では、CRC）とが含まれる。なお、健全性確認データには、上記のシーケンス番号、タイムスタンプ、誤り検出符号のいずれかを含めるようにしてもよいし、全てを含めるようにしてもよい。

【0031】

データ置換部108は、図4に示したフレームに含まれる健全性確認データ内のシーケンス番号、タイムスタンプなどのセーフティヘッダを、後段のセーフティ処理部103においてセーフティヘッダの値の変化が許容範囲内と判断されるように別の値に置換する。置換する方法は、セーフティヘッダの前回値のインクリメントでもよいし、n倍などの算術計算に基づくものでもよい。

10

【0032】

その後、符号計算・付与部109が、置換後のフレームを用いてこのフレームに対する誤り検出符号を再計算し、算出した符号を新しい誤り検出符号として上記置換後のフレームにあらためて付与し（S204）、セーフティ処理部103へ送信する（S205）。

【0033】

次に、セーフティ処理部103の動作について図5を用いて説明する。図5は、セーフティ処理部103の動作フローを示すフローチャートである。

【0034】

セーフティ処理部103では、セーフティデータ置換部102からフレームを受信すると、セーフティデータ確認部112が、受信したフレーム内の健全性確認データに含まれるセーフティヘッダ（シーケンス番号やタイムスタンプ）が前回値から更新されているか否かを確認し、更新されていなければエラーと判断し（S301でNo）、制御演算部111がシステムを安全停止させるための安全停止処理へ遷移する（S305）。そうでなければ、セーフティデータ確認部112は、処理をS302へ移行する。

20

【0035】

S302では、セーフティデータ確認部112によりセーフティヘッダの今回値と前回値との差分が許容値Xを超えているか否かを確認し、超えていることが確認できた場合もエラーと判断し（S302でNo）、制御演算部111が安全停止処理へ遷移する（S305）。

【0036】

一方、セーフティデータ確認部112によりセーフティヘッダの今回値と前回値との差分が許容値以下（正常範囲内）と確認された場合（S302でYes）、制御演算部111は、セーフティデータ置換部102から転送されてきたフレームのデータを採用し、配下の装置であるI/O（入力装置／出力装置）を制御するための制御値を演算し（制御値演算：S303）、この制御値をI/Oデータ入出力部113に出力させる（I/O出力：S304）。

30

【0037】

なお、本制御装置100によるシステムのアベイラビリティを、より考慮する構成として、上記許容値に加えリトライ回数を設けるようにしてもよい。この場合、セーフティデータ確認部112が上記のようにエラーと判定した場合にはそのときのフレームのデータを採用せずに前回セーフティ処理部103へ送信したフレームのデータを採用するとともに、エラー回数を保持するようにする。そして、セーフティデータ確認部112がリトライ回数分連続してエラーが生じたことを検出した場合に異常とみなし、制御演算部111に安全停止処理へ移行させることにより、上記のように許容値を超えると直ちに安全停止処理へ移行するよりも、システムのアベイラビリティが保たれる。

40

【0038】

次に、サービス不能攻撃が収束した場合のセーフティデータ置換部102の動作について図6を用いて説明する。図6は、サービス不能攻撃が収束した場合のセーフティデータ置換部102の動作フローを示すフローチャートである。

【0039】

50

サービス不能攻撃中は先述のとおり、セーフティデータ置換部102が健全性確認データを置換したフレームを生成し、セーフティ処理部103へ伝送する。その後サービス不能攻撃が収束した際に、そのときのセーフティデータ置換部102がもつ健全性確認データと、新しく受信したフレームの健全性確認データの値に乖離が生じた場合、セーフティ処理部103により受信フレームが異常と判断されることが懸念される。

【0040】

こうした事態を避けるために、セーフティデータ置換部102の処理実施判定部107は、受信禁止中信号がONからOFFに変化したのを検出すると(S401)、前回、セーフティデータ置換部102からセーフティ処理部103へ送信したフレームのセーフティヘッダ(現セーフティヘッダ)をデータ置換部108から取得し(S402)、新規受信したフレームのセーフティヘッダ(新規受信セーフティヘッダ)を抽出する(S403)。そして、処理実施判定部107は、新規受信セーフティヘッダのデータ(例えば、シーケンス番号)と現セーフティヘッダのデータとの差分を算出する(S404)。その後、処理実施判定部107は、この差分の大小関係により、処理を分岐させる。

10

【0041】

現セーフティヘッダの値(現出力値)より新規受信セーフティヘッダの値(新規受信値)の方が大きい場合で(S405でYes)上記差分が許容値以下のとき(S406でYes)、処理実施判定部107は、新規受信値を採用することとし新規受信フレームをそのままセーフティ処理部103に転送し(S407)、その後セーフティデータ置換部102は、図3を用いて前述した通常処理へと遷移する(S411)。

20

【0042】

一方、上記差分が許容値を超えていた場合は(S406でNo)、処理実施判定部107が、新規受信値と現出力値との差分を許容値で除算して算出される値を出力回数Iとして計算する(ただし、小数点以下切り捨て)(S408)。そして、その出力回数I分、データ置換部108でセーフティヘッダの現出力値に許容値を順次加算することによりインクリメントしたセーフティヘッダを生成し、生成したセーフティヘッダを元のセーフティヘッダと置換するとともに、符号計算・付与部109が誤り検出符号を再計算し付与して、これらの置換処理(更新)を施したフレーム(置換後フレーム)を順にセーフティ処理部103へ送信し(S409)、その後セーフティデータ置換部102は、図3を用いて前述した通常処理へと遷移する(S411)。

30

【0043】

他方、セーフティヘッダの現出力値よりも新規受信値の方が小さいまたは同じ場合は(S405でNo)、セーフティヘッダがとりうる最大値からセーフティヘッダの現出力値と新規受信値との差分を引いた値を許容値で除算して算出される値を出力回数Iとして計算する(ただし、小数点以下切り捨て)(S410)。そして、その出力回数I分、データ置換部108でセーフティヘッダの現出力値に許容値を順次加算することによりインクリメントしたセーフティヘッダを生成し、生成したセーフティヘッダを元のセーフティヘッダと置換するとともに、符号計算・付与部109が誤り検出符号を再計算し付与して、これらの置換処理を施したフレーム(置換後フレーム)を順にセーフティ処理部へ送信し(S411)、その後セーフティデータ置換部102は、図3を用いて前述した通常処理へと遷移する(S411)。

40

【0044】

現出力値より新規受信値の方が大きい場合で、新規受信値と現出力値の差分が許容値以下のケースの具体例として、例えば、許容値が256、シーケンス番号の現出力値が100、新規受信フレームのシーケンス番号が101の場合、上記差分は許容範囲内であるので、処理実施判定部107は、そのまま新規受信フレームを出力する。

【0045】

一方、現出力値より新規受信値の方が大きい場合で、新規受信値と現出力値の差分が許容値を超えるケースの具体例として、例えば、許容値が256、データ置換部108が現在出力しているシーケンス番号が100、新規受信フレームのシーケンス番号が3000

50

の場合、上記差分は許容範囲外となる。このときの出力回数 I は、

$$I = (3000 - 100) / 256 = 11.3 > 11$$

となり、セーフティデータ置換部 102 は、内部で許容値 256 分を順次インクリメントしたセーフティヘッダをもつフレームを 11 回、順にセキュリティ処理部 101 へ送信することとなる。つまり、本処理が完了した際のシーケンス番号は、

$$100 + 11 \times 256 = 2916$$

となる。これにより、シーケンス番号 3000 の次のフレームを受信しても、上記差分は、

$$3000 - 2916 = 84 \leq 256$$

となり、後段のセーフティ処理部はエラーを検出しない。本処理はシーケンス番号だけでなく、タイムスタンプなど他の健全性確認データについても同様の処理を行う。なお、新規受信値が現出力値以下となる場合も、同様の結果となる。

【0046】

上述したセキュリティ処理部 101、セーフティデータ置換部 102、およびセーフティ処理部 103 間のデータの流れおよび動作を図 7 に示す。

【0047】

同図に示すように、セーフティデータ置換部 102 は、通常時には、健全性確認データに対する置換処理を行わずにセーフティ処理部 103 へ受信したフレーム (data1) をそのまま送信する。その後、Dos 攻撃等のサービス不能攻撃により、セキュリティ処理部 101 から受信禁止中信号 ON を受信すると、セーフティデータ置換部 102 は健全性確認データに対する置換処理を実施し、置換後のフレーム (data2-1、data2-2) をセーフティ処理部 103 へ送信する。その後、セーフティデータ置換部 102 は、受信禁止中信号の OFF を検出すると、検出直後のセーフティヘッダの現出力値に対して、上述のようにセーフティ処理部 103 への出力回数 I 分内部で置換処理を施しフレーム (data2-n) をセーフティ処理部 103 へ順に送信した後、図 3 を用いて前述した通常処理へと遷移し、新規受信したフレーム (data k) をそのままセーフティ処理部 103 へ転送する。

【0048】

以上説明したように、本実施形態の制御装置 100 では、セキュリティ処理部 101 によるサービス不能攻撃からの保護機能が働いてもそれによるセーフティ処理部 103 の安全停止処理を避ける処理を行う装置をセーフティ処理部 103 の前段に備えることにより、安全性を担保するため変更を加えることが好ましくないセーフティ処理部 103 側に変更を加えずに、セキュリティとセーフティの両機能を実現し、セーフティ機能と、サービス不能攻撃に対処するセキュリティ機能とを共存させた場合のシステムのアベイラビリティの低減を抑制することが可能となる。

【0049】

(第 2 の実施形態)

次に、第 1 の実施形態よりもセキュアなシステム構成とした第 2 の実施形態にかかる制御装置について図 8 を用いて説明する。図 8 は、第 2 の実施形態にかかる制御装置の構成を示すブロック図である。なお、構成については前述の第 1 の実施形態と重複する部分については同一の符号を用い説明は省略する。

【0050】

本実施形態の制御装置 100 は、図 8 に示すように、先述した図 1 に示した第 1 の実施形態の基本構成にセキュリティ認証部 200 を追加した構成となっている。このセキュリティ認証部 200 は、暗号化／復号部 201、認証機能部 202、および認証データベース (認証 DB) 203 を備えている。本実施形態では、送受信するフレームのセーフティデータ部に、正常に復号できたか否かの判定を行うための特定のデータと、認証用のデータ (ID およびパスワード) からなるセキュリティヘッダが含まれる (図 9A)。

【0051】

暗号化／復号部 201 は、フレームの送受信の際のデータ暗号化／複合を行う機能部で

10

20

30

40

50

あり、暗号化／復号の方式は共通鍵や、秘密鍵方式などシステム共通の暗号化方式や通信セッション単位で固有の暗号化方式などを用いて行う。また、暗号化／復号部 201 は、受信したフレーム内の復号対象のデータ（例えば、セーフティデータ）を所定の鍵を用いて復号し、この復号対象のデータ内の特定データが正常に読み取れれば復号成功として復号したデータを含むフレームを後段に転送し、上記特定データが正常に読み取れない場合は復号失敗として受信フレームを破棄する。

【0052】

また、暗号化／復号部 201 は、受信したフレームの暗号化されたセーフティデータが正常に復号できた場合でも認証機能部 202 により、図 9 B に示すような送信元アドレス（図 9 B では IP アドレス）、ID およびパスワードを含む認証用データを記憶する認証 DB 203 を参照し、そのデータの送信元が正当な ID とパスワードを送信しているか否かを判定する認証を行う。そして、認証機能部 202 は、認証が成功した場合は受信したフレームを後段に転送し、認証が失敗した場合は受信したフレームを破棄する。本構成により、正しく暗号化されていないデータや認証が失敗した受信フレームはセーフティ処理部 103 の前段で破棄されるため、よりセキュアな制御が可能になる。なお、図 9 B に示すように認証 DB 203 に認証済み判定項目を設け、認証に成功した場合は、認証済み判定として「済」を設定し、「済」の場合は、同一の送信元から受信するフレームの認証を省略することもできる。

【0053】

（第 3 の実施形態）

次に、第 3 の実施形態にかかる制御装置について、図面を参照して説明する。なお、構成については第 1 の実施形態で述べた図 1 を元に説明をする。なお、第 1 の実施形態と重複する部分についての詳細な説明は省略する。

【0054】

本実施形態におけるセキュリティ処理部 101 は、先述した第 1 の実施形態のものと同様であり、図 2 に示した監視処理フローに基づいてサービス不能攻撃を検出し、セーフティデータ置換部 102 に受信禁止信号を伝達する。

【0055】

本実施形態におけるセーフティデータ置換部 102 は、先述した第 1 の実施形態のものがサービス不能攻撃を検出している間およびその直後のみ健全性確認データを置換する処理を行っていたのに対し、本実施形態では、セーフティデータ置換部 102 は一度サービス不能攻撃を受けた後は、サービス不能攻撃の検出有無に関わらず、健全性確認データについては継続して置換処理を施す。以下に、セーフティデータ置換部 102 の処理について図 10 を用いて説明する。図 10 は、セーフティデータ置換部 102 の動作フローを示すフローチャートである。

【0056】

本実施形態では、受信禁止中信号が ON の場合（S501 で Yes）、つまりサービス不能攻撃を受けているとき、第 1 の実施形態と同様に、処理実施判定部 107 が、前回、セーフティデータ置換部 102 からセーフティ処理部 103 に送信したフレーム（前回出力フレーム）を採用し（S502）、データ置換部 108 がそのセーフティヘッダを置換し（S503）、さらに符号計算・付与部 109 が再計算した誤り検出符号を付与して（S504）、これらの置換処理を施した置換後のフレームをセーフティ処理部 103 に送信する（S505）。また、受信禁止中信号が一度 ON となった場合、処理実施判定部 107 は、受信禁止中信号が ON となったことを記憶する。

【0057】

一方、受信禁止中信号が OFF の場合（S501 で No）でセキュリティ処理部 101 から受信したフレームがあると（S506 で Yes）、処理実施判定部 107 は、過去に受信禁止中信号が ON になったか否かを判定する（S507）。もし過去に一度もサービス不能攻撃を受けていない場合（S507 で No）、処理実施判定部 107 は、受信したフレームをそのままセーフティ処理部 103 へ転送する（S513）。セキュリティ処理

部 1 0 1 から受信したフレームが無い場合は (S 5 0 6 で N o) 、 S 5 0 1 に戻る。

【 0 0 5 8 】

また、過去に一度でもサービス不能攻撃を受けた場合は (S 5 0 7 で Y e s) 、さらに受信フレームがあるか確認し、あれば (S 5 0 8 で Y e s) 、処理実施判定部 1 0 7 は、図 3 に示すような受信フレームに含まれている誤り検出符号 (C R C) を用いてデータの健全性を確認する (S 5 0 9) 。この確認で誤りが検出されれば (S 5 0 9 で N o) 、処理実施判定部 1 0 7 は受信フレームを破棄する (S 5 1 3) 。そうでなければ (S 5 0 9 で Y e s) 、データ置換部 1 0 8 がセーフティヘッダの置換を行い (S 5 1 0) 、符号計算・付与部 1 0 9 が誤り検出符号を再計算し付与し (S 5 1 1) 、置換後のフレームをセーフティ処理部 1 0 3 へ送信する (S 5 1 2) 。なお、S 5 1 2 および S 5 1 3 の後、な

10

【 0 0 5 9 】

データ置換部 1 0 8 が S 5 0 9 でセーフティヘッダ (例えば、シーケンス番号) を更新する際のインクリメント値は、サービス不能攻撃から復帰した際のセーフティデータ置換部 1 0 2 からセキュリティ処理部 1 0 1 へ送信したフレームのセーフティヘッダの前回値と新たに受信したフレームのセーフティヘッダの値との差分を用いる。

【 0 0 6 0 】

例えば、サービス不能攻撃中にシーケンス番号が 2 0 0 までインクリメントされ、次に受信したシーケンス番号が 1 9 0 だった場合、上記差分値は、

$$200 - 190 = 10、$$

20

となる。つまり次回出力する新規受信フレームからはシーケンス番号を $10 + 1 = 11$ だけインクリメントすることにより、置換後フレーム内のシーケンス番号は

$$190 + 11 = 201 > 200 \text{ (前回値)}、$$

となり、置換後のフレームを受けるセーフティ処理部 1 0 3 は正常に動作を継続することが可能となる。逆に、新規に受信したフレーム内のシーケンス番号が 2 3 0 と、前回値の 2 0 0 よりも進んでいた場合、上記差分値は、

$$200 - 230 = -30、$$

となる。つまり、次回出力する新規受信フレームからはシーケンス番号を $-30 + 1 = -29$ だけインクリメント (2 9 デクリメント) することにより、置換後フレーム内のシーケンス番号は、

30

$$230 - 29 = 201 > 200 \text{ (前回値)}、$$

となって、この場合もセーフティ処理部 1 0 3 は正常に動作を継続することが可能になる。本処理はシーケンス番号に対してだけでなく、タイムスタンプなど他の健全性確認データに対しても同様の処理を行う。

【 0 0 6 1 】

後段のセーフティ処理部 1 0 3 の動作は、第 1 の実施形態において先述したとおりである。

【 0 0 6 2 】

なお、本実施形態においてもシステムのアベイラビリティを、より考慮する構成として、許容値としてリトライ回数を設けるようにしてもよい。この場合、セーフティデータ確認部 1 1 2 が上記のようにエラーと判定した場合にそのフレームのデータを採用せず、前回セーフティ処理部 1 0 3 へ送信したフレームのデータを採用するとともに、エラー回数を保持するようにする。そして、そのエラー回数がリトライ回数分連続してエラーが生じた場合にセーフティデータ確認部 1 1 2 が異常とみなし、制御演算部 1 1 1 に安全停止処理へ移行させることにより、先述のように許容値を超えると直ちに安全停止処理へ移行するよりも、システムのアベイラビリティが保たれる。

40

【 0 0 6 3 】

図 1 1 に、本実施形態にかかる制御装置 1 0 0 の、セキュリティ処理部 1 0 1 、セーフティデータ置換部 1 0 2 、およびセーフティ処理部 1 0 3 間のデータの流れおよび動作を示す。

50

【0064】

図11に示すように、通常時は、受信したフレーム（data1）をそのままセーフティ処理部103まで転送し、サービス不能攻撃中（受信禁止中信号ON）は、セーフティデータ置換部102は、前回、セーフティ処理部103へ送信したフレーム（data2）を採用し、その健全性確認データを置換したフレーム（data2-1、data2-2）を生成し、セーフティ処理部103へ送信する。また、セーフティデータ置換部102は、サービス不能攻撃が収まった後も、新規受信したフレーム内の健全性確認データを置換し続け、置換後のフレーム（data k-3、data L-4）を後段のセーフティ処理部103へ転送する。

【0065】

本実施形態によれば、第1の実施形態の効果に加え、サービス不能攻撃の収束を検出した後も継続して健全性確認データの置換処理を行うことにより、第1の実施形態において図6を用いて説明したような、ある出力回数分置換処理を施したフレームをセーフティ処理部103へ送信するといった処理が不要となり、セーフティデータ置換部102の処理を簡素化した制御装置100を提供できる。

【0066】

また、第2の実施形態として前述した図8に示したセキュリティ認証部200を含む、よりセキュアな構成を採用することも可能である。この構成をとった場合、暗号化機能および認証機能により正当なフレームのみがセーフティデータ置換部102へ伝送されることになり、セキュリティ機能がより向上する。

【0067】

（第4の実施形態）

次に、第4の実施形態にかかる制御装置について、図12および図13を用いて説明する。図12および図13は、本実施形態にかかる制御装置100およびユーザ端末の構成を示すブロック図である。なお、構成については前述の諸実施形態と重複する部分については同一の符号を用い説明は省略する。

【0068】

本実施形態では、制御装置100の外部に許容時間入力部301とアラーム表示部302を具備したユーザ端末（ユーザ側装置）300を設け、許容時間入力部301とアラーム表示部302をそれぞれセーフティデータ置換部102の処理実施判定部107に接続する。なお、制御装置100とユーザ端末300との接続手段は、図12に示すような専用の接続線に限らず、図13に示すような上位装置等に接続するための制御用通信路（ネットワーク）を用いた構成としてもよい。また、ユーザ端末300は、キーボードやマウス等の入力装置、液晶モニタ等の表示装置、および、処理実施判定部107に接続するためのインタフェースを備えた、PCなどの汎用的な情報処理装置でもよいし、専用に構成されたハードウェアでもよい。PCなどの汎用的な情報処理装置を用いる場合、当該情報処理装置にインストールされた制御プログラムと当該情報処理装置のハードウェアとが協働することにより、上記許容時間入力部301とアラーム表示部302の機能を実現する。

【0069】

次に、本実施形態にかかる制御装置100と、当該制御装置100に接続するユーザ端末300の動作について図14を用いて説明する。図14は、第4の実施形態におけるセーフティデータ置換部102の動作フローを示すフローチャートである。

【0070】

以下では、ユーザ端末300内の許容時間入力部301から処理実施判定部107へ、サービス不能攻撃に対する許容時間が設定されているものとする。

【0071】

処理実施判定部107は、受信禁止中信号がOFFの場合（S601でNo）、セキュリティ処理部101から受信したフレームがあると（S610でYes）、この受信したフレームをセーフティ処理部103へそのまま転送し（S611）、無い場合は（S61

10

20

30

40

50

0でNo)、処理をS601に戻す。一方、受信禁止中信号がONの場合(S601でYes)、サービス不能攻撃が生じている時間(継続時間)を計測する(S602)。

【0072】

そして、サービス不能攻撃の継続時間が設定された許容時間(許容値)内であれば(S603でYes)、処理実施判定部107は、セーフティデータ置換部102からセーフティ処理部103へ前回送信したフレーム(前回出力フレーム)を採用し、この前回出力フレームをデータ置換部108に転送する(S604)。

【0073】

そして、第1の実施形態で前述したように、データ置換部108による前回出力フレームのセーフティヘッダの置換を行い(S605)、符号計算・付与部109による誤り検出符号の再計算および付与を行って(S606)、セーフティ処理部103へ置換後のフレームを送信する(S607)。

【0074】

一方、サービス不能攻撃が設定された許容時間を超えた場合(S603でNo)、処理実施判定部107は、ユーザ端末300に警告を通知する(S608)。ユーザ端末300への警告の通知は、上記の制御装置100とユーザ端末300との接続手段(専用の接続線または制御用通信路(ネットワーク))を介して行うが、制御用通信路の場合は、サービス不能攻撃中は半二重通信では警告が通知できなくなるため、通信I/F部104は全二重通信により警告を通知する機能を備える。

【0075】

処理実施判定部107がユーザ端末300への警告を通知した後、セーフティデータ置換部102は、前回、セーフティ処理部103へ送信したフレームの健全性確認データをデータ置換部108および符号計算・付与部109にて更新することなく、そのフレームをそのままセーフティ処理部103へ送信する(S609)。システムのアベイラビリティの観点から、セーフティ処理部103のエラー判定がn回連続検出で安全停止する仕様になっていた場合、セーフティデータ置換部102は、n回連続で前回値をもつ健全性確認データを含むフレームをセーフティ処理部103へ送信する。セーフティ処理部103は図5に示した動作フローに基づき動作し、セーフティデータ確認部112が健全性確認データが更新されていないことを検出すると、制御演算部111が安全停止処理へと遷移する。

【0076】

図15に、本実施形態にかかる制御装置100の、セキュリティ処理部101、セーフティデータ置換部102、およびセーフティ処理部103間のデータ(フレーム)の流れおよび動作を示す。

【0077】

同図に示すように、通常時、および、受信禁止中信号ONでその後の経過時間が許容時間内の場合、図7を用いて前述したデータの流れとなるが、経過時間が許容時間を過ぎると(許容時間OVER)、その後、経過時間が許容時間を過ぎる直前のフレーム(data2-2)を連続して(繰り返して)セーフティ処理部103へ送信している。その結果、セーフティ処理部103で安全停止処理へ遷移しシステムは安全停止することとなる。

【0078】

本実施形態では、以上のようにして、サービス不能攻撃が発生し、許容時間内まではデータ置換部108が前述の健全性確認データの置換を行い、符号計算・付与部109が誤り検出符号を再計算し付与したフレームを生成し、セーフティ処理部103へ転送するが、許容時間を超えた場合、セーフティデータ置換部102は、データ置換部108および符号計算・付与部109による置換処理を停止し、同一のフレームをセーフティ処理部103に転送することにより、システムを安全停止させる。

【0079】

本実施形態によれば、安全停止処理に遷移する前に上記のようにユーザに対してシステムが安全停止する旨の警告を通知することで、ユーザによる対処の機会を提供することが

10

20

30

40

50

でき、また、ユーザが許容時間を任意に設定可能としたことで、制御対象プラントごとに異なる制御応答許容時間に合わせて、サービス不能攻撃に伴う安全停止処理へ遷移するかどうかの判定時間をユーザが調整することが可能となる。

【0080】

また、本実施形態においても、第2の実施形態として前述した図8に示したセキュリティ認証部200を含む、よりセキュアな構成を採用することが可能である。この構成をとった場合、暗号化機能および認証機能により正当なフレームのみがセーフティデータ置換部102へ伝送されることになり、セキュリティ機能がより向上する。

【0081】

以上説明したとおり、第1から第4の実施形態によれば、制御装置におけるセキュリティ機能とセーフティ機能の両立を実現し、当該制御装置を含むシステム全体のアベイラビリティの低減を回避することができる。

10

【0082】

本発明のいくつかの実施形態を説明したが、これらの実施形態は、例として提示したものであり、発明の範囲を限定することは意図していない。これら新規な実施形態は、その他の様々な形態で実施されることが可能であり、発明の要旨を逸脱しない範囲で、種々の省略、置き換え、変更を行うことができる。これら実施形態やその変形は、発明の範囲や要旨に含まれるとともに、特許請求の範囲に記載された発明とその均等の範囲に含まれる。

【符号の説明】

20

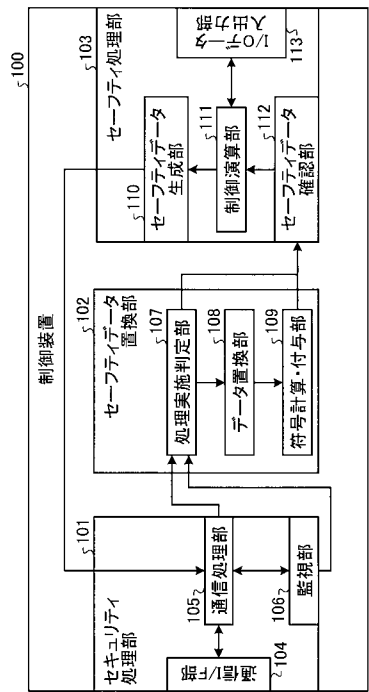
【0083】

- 100 制御装置
- 101 セキュリティ処理部
- 102 セーフティデータ置換部
- 103 セーフティ処理部
- 104 通信I/F部
- 105 通信処理部
- 106 監視部
- 107 処理実施判定部
- 108 データ置換部
- 109 符号計算・付与部
- 110 セーフティデータ生成部
- 111 制御演算部
- 112 セーフティデータ確認部
- 113 I/Oデータ入出力部
- 200 セキュリティ認証部
- 201 暗号化／復号部
- 202 認証機能部
- 203 認証DB
- 300 ユーザ端末
- 301 許容時間入力部
- 302 アラーム表示部

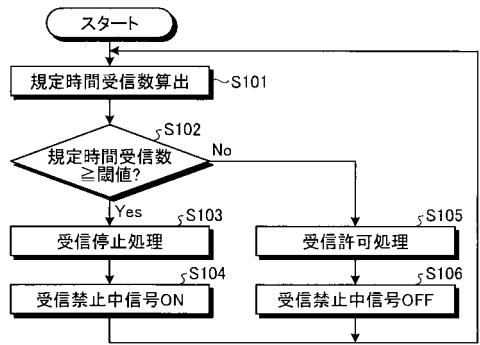
30

40

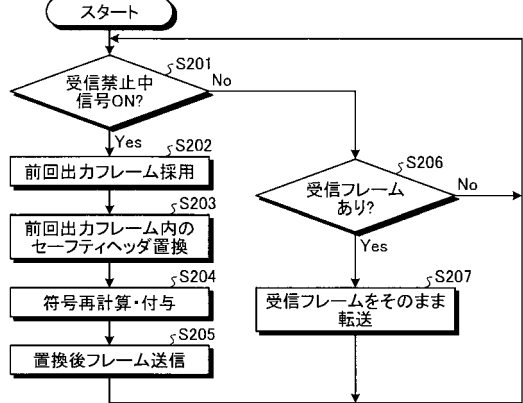
【図 1】



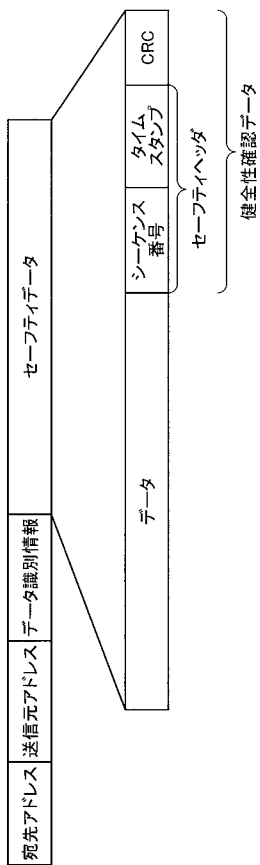
【図 2】



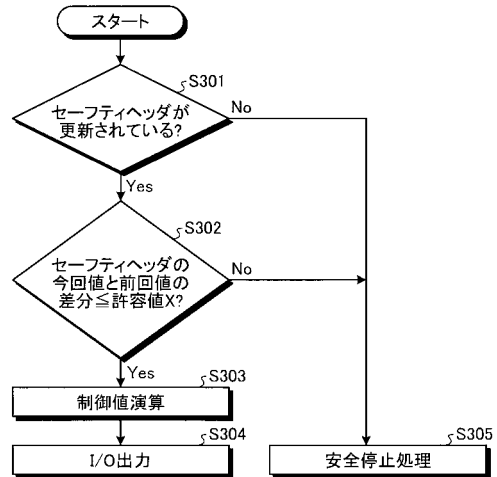
【図 3】



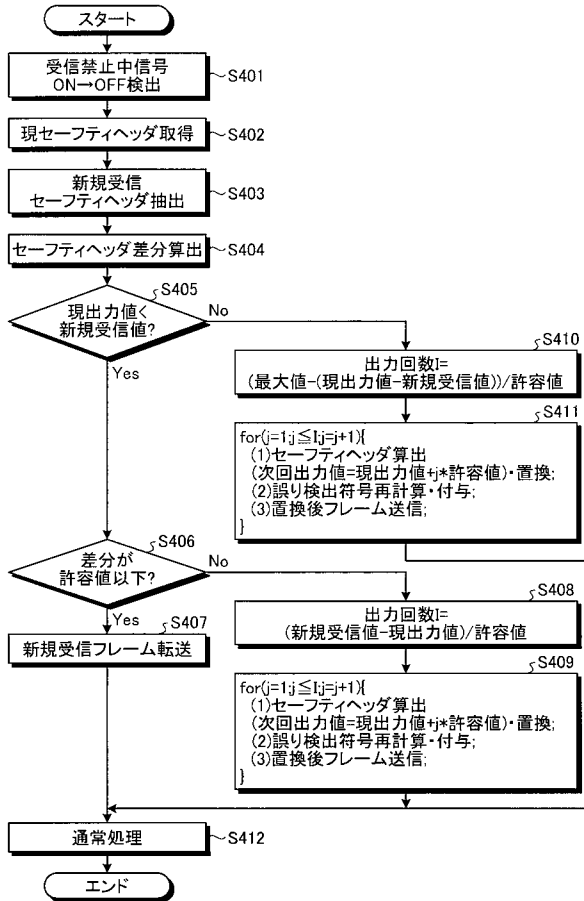
【図 4】



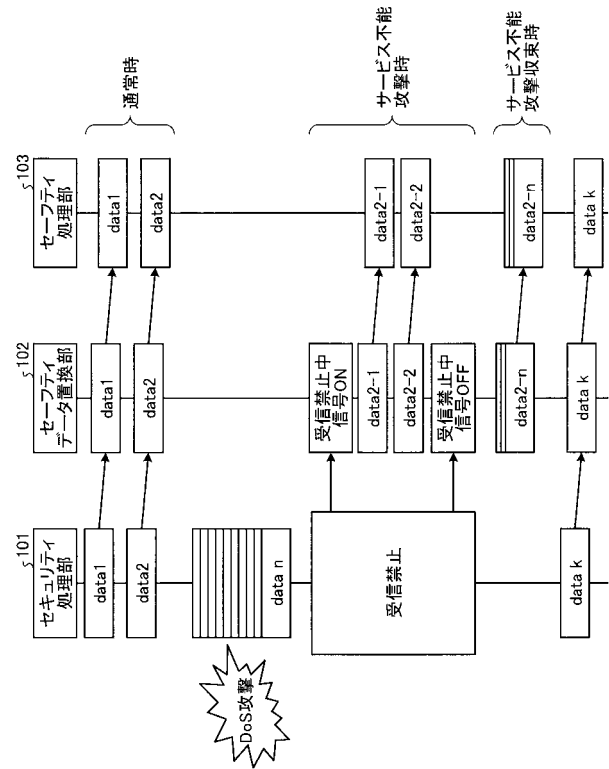
【図 5】



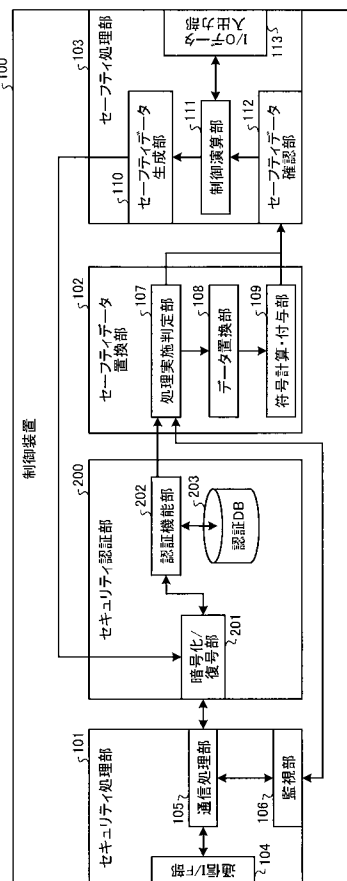
【図 6】



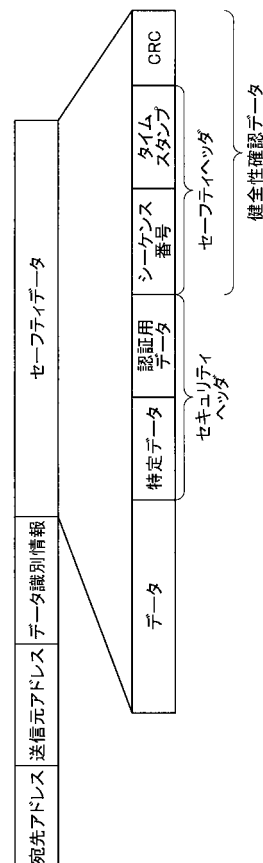
【図 7】



【図 8】



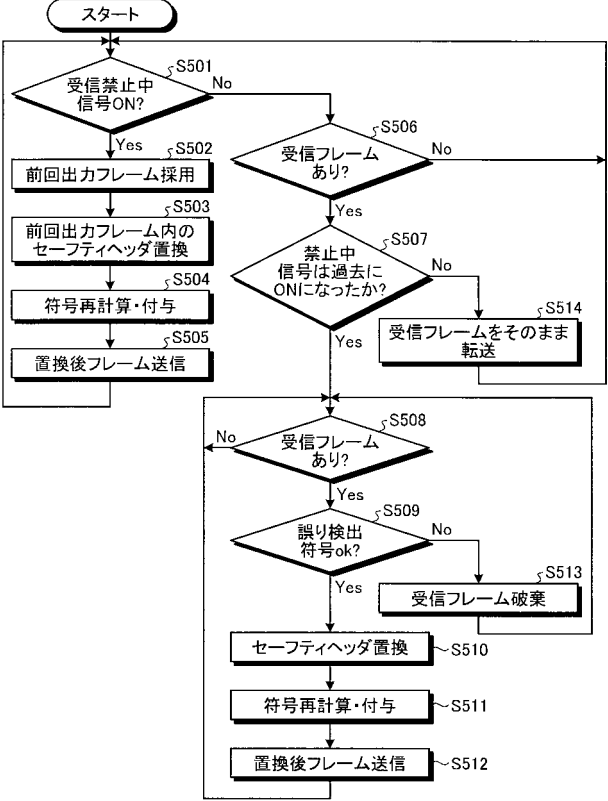
【図 9 A】



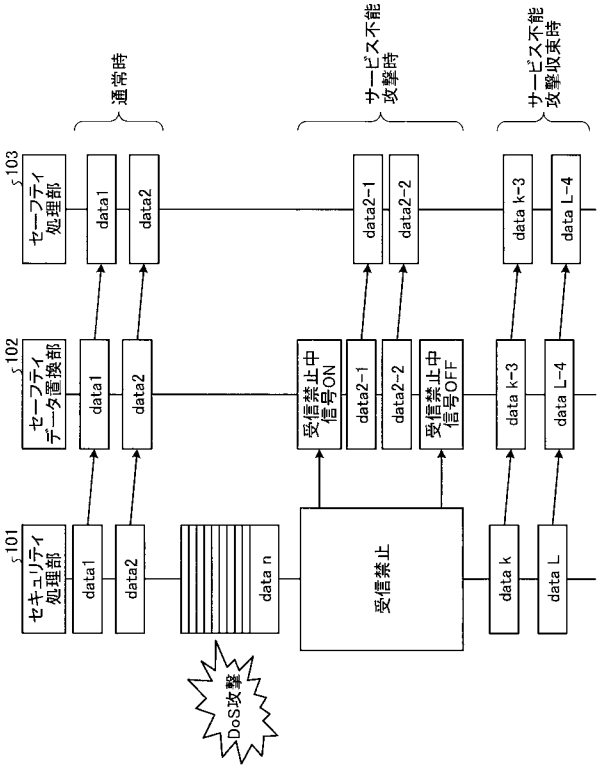
【図 9 B】

IPアドレス	ID	パスワード	認証済み判定
192.168.1.10	ID1	Pass1	未
192.168.1.52	ID2	PWD2	済
192.168.1.77	ID3	Password3	未
192.168.1.88	ID4	Pwd4	未
192.168.1.95	ID5	Pw5	済

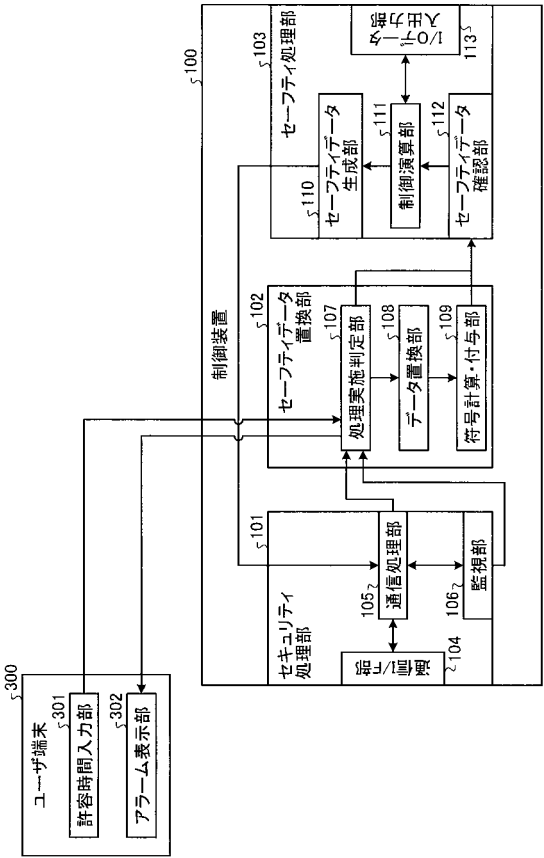
【図 1 0】



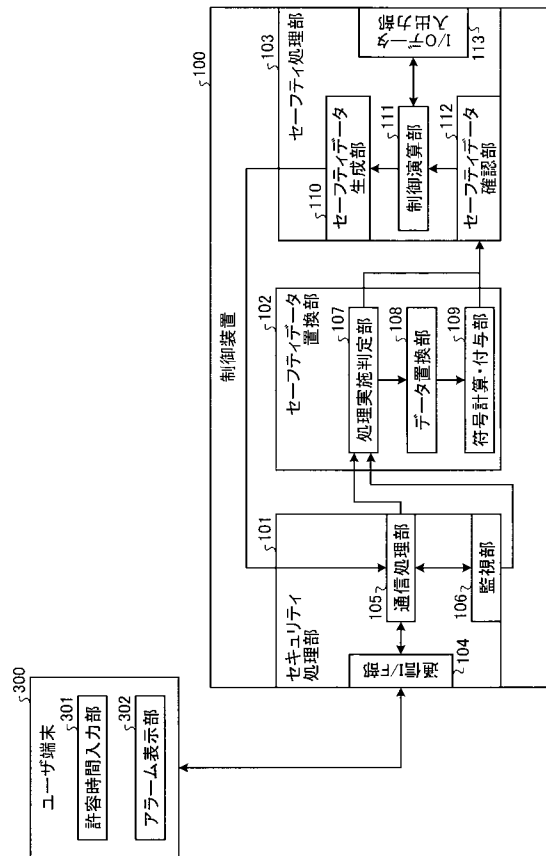
【図 1 1】



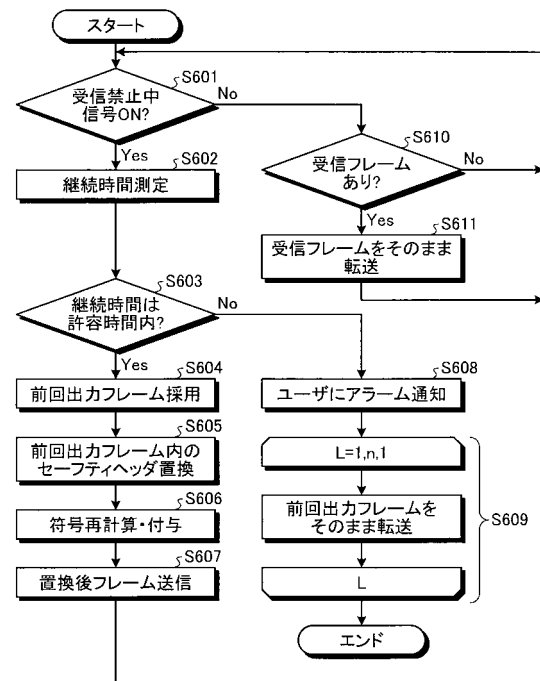
【図 1 2】



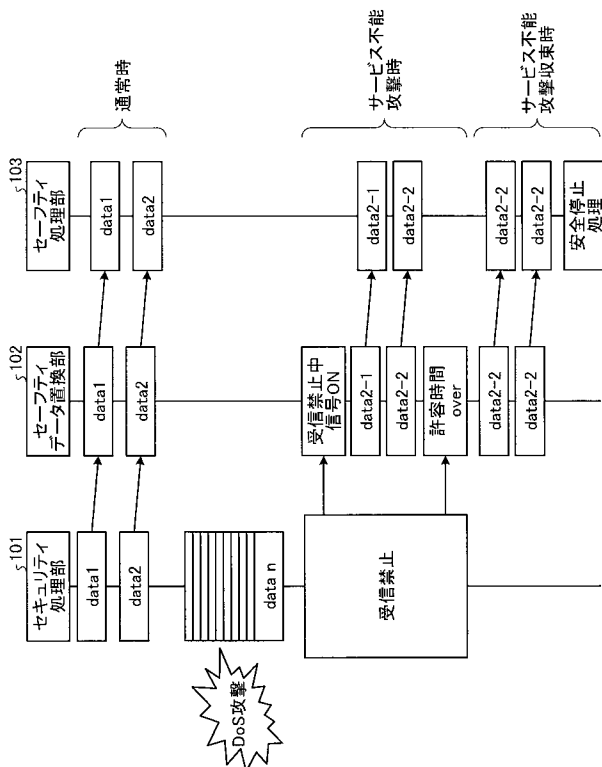
【図 13】



【図 14】



【図 15】



フロントページの続き

(72)発明者 吉川 正臣
東京都港区芝浦一丁目1番1号 株式会社東芝内
(72)発明者 大西 直哉
東京都港区芝浦一丁目1番1号 株式会社東芝内
(72)発明者 高仲 徹
東京都港区芝浦一丁目1番1号 株式会社東芝内
Fターム(参考) 5H220 AA01 BB09 CC06 CX01 JJ12 JJ28
5K030 GA15 HA08 HD03 JA11 LE11