(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2017-111532
(P2017-111532A)
(43)公開日　平成29年6月22日(2017.6.22)

(51)Int.Cl.		F I			テーマコード（参考）
G06F 13/00	(2006.01)	G06F	13/00	351Z	5B089
G05B 9/02	(2006.01)	G05B	9/02	B	5H209
G06F 21/55	(2013.01)	G06F	21/55		

審査請求 未請求　請求項の数 8　ＯＬ　（全 16 頁）

(21)出願番号　特願2015-244048 (P2015-244048)
(22)出願日　平成27年12月15日 (2015.12.15)

(71)出願人　000006507
横河電機株式会社
東京都武蔵野市中町２丁目９番３２号
(74)代理人　100106909
弁理士　棚井　澄雄
(74)代理人　100146835
弁理士　佐伯　義文
(74)代理人　100167553
弁理士　高橋　久典
(74)代理人　100181124
弁理士　沖田　壮男
(72)発明者　小川　永志樹
東京都武蔵野市中町２丁目９番３２号　横河電機株式会社内

最終頁に続く

(54)【発明の名称】制御装置及び統合生産システム

(57)【要約】
【課題】安全計装システムに対する内部及び外部の少なくとも一方からのサイバー攻撃を未然に防いで安全計装システムの健全性を担保することが可能な制御装置及び統合生産システムを提供する。
【解決手段】統合生産システム１は、ネットワークＮに接続された安全計装システム３０と、統合生産システム１に対する内部及び外部の少なくとも一方からのサイバー攻撃を検知する検知装置６０と、安全計装システム３０の一部をなし、検知装置６０の検知結果に基づいて、自装置の少なくとも一部の機能を制限する対策を行う安全コントローラ３１ａ，３１ｂとを備える。
【選択図】図１

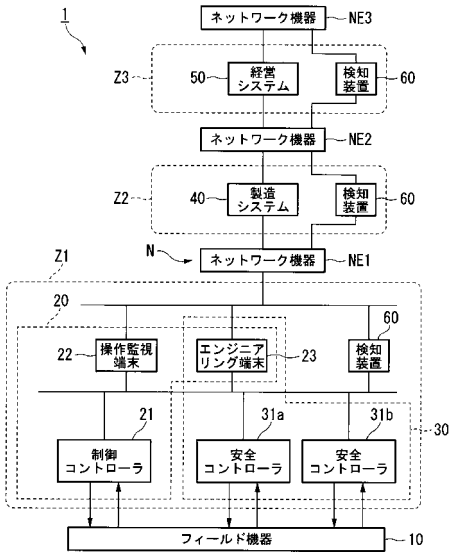

図1

【特許請求の範囲】
【請求項１】
プラントに構築された統合生産システムの制御装置において、
前記統合生産システムに対する内部及び外部の少なくとも一方からのサイバー攻撃を検知する検知手段の検知結果に基づいて、自装置の少なくとも一部の機能を制限する対策を行う防御手段を備える制御装置。
【請求項２】
前記防御手段は、前記検知手段の検知結果に基づいて前記サイバー攻撃の対象及び種別を特定し、特定した前記サイバー攻撃の対象及び種別に応じた前記対策を設定する設定手段と、
前記設定手段で設定された前記対策を実行する実行手段と、
を備える請求項１記載の制御装置。
【請求項３】
前記設定手段は、前記サイバー攻撃の対象及び種別と、前記サイバー攻撃の対象及び種別に応じて行うべき対策とが対応付けられた設定リストを用いて前記対策を設定する、請求項２記載の制御装置。
【請求項４】
前記制御装置は、前記統合生産システムに異常が生じた場合に、前記統合生産システムを安全な状態に停止させる安全計装システムの制御装置である、請求項１から請求項３の何れか一項に記載の制御装置。
【請求項５】
ネットワークに接続された安全計装システムを備える統合生産システムにおいて、
前記統合生産システムに対する内部及び外部の少なくとも一方からのサイバー攻撃を検知する検知手段と、
前記安全計装システムの一部をなす請求項１から請求項３の何れか一項に記載の制御装置と、
を備える統合生産システム。
【請求項６】
前記統合生産システムは、複数のゾーンに区分けされており、
前記検知手段は、前記ゾーン毎に設けられていて、自ゾーンに対する内部及び外部の少なくとも一方からのサイバー攻撃を検知する
請求項５記載の統合生産システム。
【請求項７】
前記制御装置の防御手段は、前記ネットワークを介して前記検知手段の検知結果を得る、請求項５又は請求項６記載の統合生産システム。
【請求項８】
前記制御装置の防御手段は、前記ネットワークとは異なる通信線を介して前記検知手段の検知結果を得る、請求項５又は請求項６記載の統合生産システム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、制御装置及び統合生産システムに関する。
【背景技術】
【０００２】
従来から、プラントや工場等（以下、これらを総称する場合には、単に「プラント」という）においては、統合生産システムが構築されており、高度な自動操業が実現されている。このような統合生産システムは、安全性を確保しつつ高度な制御を行うために、プラントで実現される工業プロセスの制御を行うプロセス制御システムである分散制御システム（ＤＣＳ：Distributed Control System）等の制御システムと、安全計装システム（ＳＩＳ：Safety Instrumented System）等の安全システムとを備える。

【０００３】
上記の分散制御システムは、フィールド機器と呼ばれる現場機器（測定器、操作器）と、これらを制御するコントローラとが通信手段を介して接続され、フィールド機器で測定された測定データをコントローラが収集し、収集した測定データに応じてコントローラがフィールド機器を操作（制御）することによって工業プロセスにおける各種の状態量の制御を行うシステムである。上記の安全計装システムは、緊急時においてプラントを確実に安全な状態に停止させることで、人身事故や環境汚染を未然に防止するとともに、高価な設備の保護を図るシステムである。この安全計装システムは、プラントに異常事態が生じた場合に、「安全を守る最後の砦」としての役割を担っている。
【０００４】
上述した統合生産システムは、外部からのサイバー攻撃を受ける可能性が考えられる。このため、統合生産システムでは、分散制御システム及び安全計装システムの各々で個別に、或いは統合生産システム全体で、サイバー攻撃を受けた場合の対策（セキュリティ対策）が施されている。例えば、外部から統合生産システムへの侵入を防ぐためのファイアウォールの設置、或いはコンピュータに対するウィルス対策ソフト（ウィルス感染を検知してウィルスの除去を行うソフト）のインストール等が行われている。尚、分散制御システム及び安全計装システムの中核をなすコントローラは、独自のオペレーティングシステムを用いることで、サイバー攻撃に対する耐性が高められている。
【０００５】
統合生産システムは、複数のゾーンに区分けされており、上述したセキュリティ対策は基本的にゾーン毎に施されている。例えば、国際標準規格ＩＳＡ－９５（ＩＥＣ／ＩＳＯ６２２６４）で規定されている階層構造に準じて構築されている統合生産システムは、階層を基準として複数のゾーンに区分けされており、上述したセキュリティ対策は階層毎に施されている。尚、以下の特許文献１，２には、制御系ネットワークのセキュリティを維持するための従来技術が開示されており、以下の特許文献３には、上述した国際標準規格ＩＳＡ－９５の階層構造に習ったツリービューを表示する従来技術が開示されている。
【先行技術文献】
【特許文献】
【０００６】
【特許文献１】特開２０００－２６７９５７号公報
【特許文献２】特開２０１０－０８１６１０号公報
【特許文献３】特開２０１３－１６１４３２号公報
【発明の概要】
【発明が解決しようとする課題】
【０００７】
ところで、上述の通り、外部からのサイバー攻撃に対するセキュリティ対策は基本的にゾーン毎に施されていることから、サイバー攻撃が行われた場合のセキュリティ対策はゾーン毎に個別に実行されることになる。このため、従来の統合生産システムでは、各ゾーンのセキュリティ対策がサイバー攻撃に対して十分でない場合には、安全計装システムが属するゾーンまでサイバー攻撃が及んでしまい、最終的な防衛策は、安全計装システムが属するゾーンで施されているセキュリティ対策に依存してしまうという問題がある。
【０００８】
また、安全計装システムは、上位のシステムとの通信は通常行わないが、分散制御システムと通信する必要がある。一方、分散制御システムには、上位システムとの通信が求められる。すると、安全計装システムも、結果として上位システムと繋がることになるため、サイバー攻撃が及んでしまう可能性が考えられるという問題がある。
【０００９】
ここで、上述の通り、各ゾーンのセキュリティ対策がサイバー攻撃に対して十分でない場合には、安全計装システムが属するゾーンまでサイバー攻撃が及んでしまい、安全計装システム（或いは、安全計装システムで用いられるプログラムの作成を行うエンジニアリ

ングステーション）の制御権が奪われる事態が生ずる虞が考えられる。また、統合生産システム内部からサイバー攻撃が行われる場合（例えば、ウィルスに感染した機器が統合生産システム内に持ち込まれた場合等）にも、安全計装システム等の制御権が奪われる事態が生ずる虞が考えられる。このような事態が生じて安全計装システムの中核をなすコントローラのプログラムが書き換えられてしまうと「安全を守る最後の砦」としての役割が失われてしまうことから、上記の事態が生じないようにする必要がある。

【００１０】

本発明は上記事情に鑑みてなされたものであり、安全計装システムに対する内部及び外部の少なくとも一方からのサイバー攻撃を未然に防いで安全計装システムの健全性を担保することが可能な制御装置及び統合生産システムを提供することを目的とする。

【課題を解決するための手段】

【００１１】

上記課題を解決するために、本発明の制御装置は、プラントに構築された統合生産システム（１、２）の制御装置（３１ａ、３１ｂ）において、前記統合生産システムに対する内部及び外部の少なくとも一方からのサイバー攻撃を検知する検知手段（６０）の検知結果に基づいて、自装置の少なくとも一部の機能を制限する対策を行う防御手段（ＤＦ）を備える。

また、本発明の制御装置は、前記防御手段が、前記検知手段の検知結果に基づいて前記サイバー攻撃の対象及び種別を特定し、特定した前記サイバー攻撃の対象及び種別に応じた前記対策を設定する設定手段（７１）と、前記設定手段で設定された前記対策を実行する実行手段（７２）と、を備える。

また、本発明の制御装置は、前記設定手段が、前記サイバー攻撃の対象及び種別と、前記サイバー攻撃の対象及び種別に応じて行うべき対策とが対応付けられた設定リスト（ＬＳ）を用いて前記対策を設定する。

また、本発明の制御装置は、前記制御装置が、前記統合生産システムに異常が生じた場合に、前記統合生産システムを安全な状態に停止させる安全計装システム（３０）の制御装置である。

本発明の統合生産システムは、ネットワーク（Ｎ）に接続された安全計装システム（３０）を備える統合生産システム（１、２）において、前記統合生産システムに対する内部及び外部の少なくとも一方からのサイバー攻撃を検知する検知手段（６０）と、前記安全計装システムの一部をなす上記の何れかに記載の制御装置（３１ａ、３１ｂ）と、を備える。

また、本発明の統合生産システムは、複数のゾーン（Ｚ１～Ｚ３）に区分けされており、前記検知手段が、前記ゾーン毎に設けられていて、自ゾーンに対する内部及び外部の少なくとも一方からのサイバー攻撃を検知する。

また、本発明の統合生産システムは、前記制御装置の防御手段が、前記ネットワークを介して前記検知手段の検知結果を得る。

また、本発明の統合生産システムは、前記制御装置の防御手段が、前記ネットワークとは異なる通信線（Ｌ１）を介して前記検知手段の検知結果を得る。

【発明の効果】

【００１２】

本発明によれば、統合生産システムに対する内部及び外部の少なくとも一方からのサイバー攻撃を検知する検知手段を設け、検知手段の検知結果に基づいて制御装置の防御手段が、自装置の少なくとも一部の機能を制限する対策を行うようにしているため、安全計装システムに対する内部及び外部の少なくとも一方からのサイバー攻撃を未然に防いで安全計装システムの健全性を担保することが可能であるという効果がある。

【図面の簡単な説明】

【００１３】

【図１】本発明の第１実施形態による統合生産システムの全体構成を示すブロック図である。

【図２】本発明の第１実施形態による制御装置の要部構成を示すブロック図である。
【図３】本発明の第１実施形態における設定リストの一例を示す図である。
【図４】本発明の第１実施形態における攻撃対象リスト及び対策リストの一例を示す図である。
【図５】本発明の第１実施形態における設定リストの他の例を示す図である。
【図６】本発明の第１実施形態における攻撃対象リスト及び対策リストの他の例を示す図である。
【図７】本発明の第１実施形態による制御装置としての安全コントローラ内の防御部の動作を示すフローチャートである。
【図８】本発明の第２実施形態による統合生産システムの全体構成を示すブロック図である。
【図９】本発明のその他の実施形態による統合生産システムを示すブロック図である。
【発明を実施するための形態】
【００１４】
以下、図面を参照して本発明の実施形態による制御装置及び統合生産システムについて詳細に説明する。
【００１５】
〔第１実施形態〕
〈統合生産システム〉
図１は、本発明の第１実施形態による統合生産システムの全体構成を示すブロック図である。図１に示す通り、本実施形態の統合生産システム１は、フィールド機器１０、分散制御システム（ＤＣＳ）２０、安全計装システム（ＳＩＳ）３０、製造システム４０、経営システム５０、及び検知装置６０（検知手段）を備えており、プラントの自動操業を行うとともにプラントの維持管理等を行う。
【００１６】
この統合生産システム１は、国際標準規格ＩＳＡ－９５（ＩＥＣ／ＩＳＯ ６２２６４）で規定されている階層構造に準じて構築されている。具体的に、統合生産システム１は、レベル２の階層に分散制御システム２０及び安全計装システム３０が属し、レベル３の階層に製造システム４０が属し、レベル４の階層に経営システム５０が属するように構築されている。これら分散制御システム２０、安全計装システム３０、製造システム４０、及び経営システム５０に加えて、検知装置６０は、ネットワーク機器ＮＥ１～ＮＥ３等によって構成されるネットワークＮを介して接続されている。
【００１７】
また、統合生産システム１は、セキュリティ対策のために、上述した階層を基準として複数のゾーンに区分けされている。具体的に、統合生産システム１は、分散制御システム２０及び安全計装システム３０がゾーンＺ１に区分けされており、製造システム４０がゾーンＺ２に区分けされており、経営システム５０がゾーンＺ３に区分けされている。
【００１８】
ここで、上記のプラントとしては、化学等の工業プラントの他、ガス田や油田等の井戸元やその周辺を管理制御するプラント、水力・火力・原子力等の発電を管理制御するプラント、太陽光や風力等の環境発電を管理制御するプラント、上下水やダム等を管理制御するプラント等がある。
【００１９】
フィールド機器１０は、プラントの現場に設置されて分散制御システム２０の制御の下で工業プロセスの制御に必要な測定や操作を行う機器である。具体的に、フィールド機器１０は、例えば圧力計や流量計や温度センサやガスセンサや振動センサ等のセンサ機器、流量制御弁や開閉弁等のバルブ機器、ファンやモータ等のアクチュエータ機器、プラント内の状況や対象物を撮影するカメラやビデオ等の撮像機器、プラント内の異音等を収集したり警報音等を発したりするマイクやスピーカ等の音響機器、各機器の位置情報を出力する位置検出機器、その他の機器である。

【００２０】
フィールド機器１０は、分散制御システム２０又は安全計装システム３０と通信を行う。例えば、フィールド機器１０は、分散制御システム２０又は安全計装システム３０との間で、ネットワークや通信バス（図示省略）を介した有線通信、或いはＩＳＡ１００．１１ａやＷｉｒｅｌｅｓｓＨＡＲＴ（登録商標）等の産業用無線通信規格に準拠した無線通信を行う。
【００２１】
分散制御システム２０は、制御コントローラ２１、操作監視端末２２、及びエンジニアリング端末２３を備えており、フィールド機器１０で測定された測定データを収集し、収集した測定データに応じてフィールド機器１０を操作（制御）することによって各種の状態量の制御を行う。尚、分散制御システム２０によって制御される状態量は、工業プロセスにおける各種の状態量であり、例えば圧力、温度、流量等である。
【００２２】
制御コントローラ２１は、分散制御システム２０の中核をなす装置であり、フィールド機器１０からの測定データの収集、フィールド機器１０に対する操作（制御）を行う。操作監視端末２２は、例えばプラントの運転員によって操作され、プラントの運転状態の監視のために用いられる装置である。エンジニアリング端末２３は、制御コントローラ２１及び操作監視端末２２で実行されるプログラムを作成するための装置である。尚、エンジニアリング端末２３は、常時ネットワークに接続されている必要はない。また、エンジニアリング端末２３は、分散制御システム２０と安全計装システム３０とで共用されるものとする。
【００２３】
安全計装システム３０は、安全コントローラ３１ａ，３１ｂ（制御装置）及びエンジニアリング端末２３を備えており、緊急時においてプラントを確実に安全な状態に停止させることで、人身事故や環境汚染を未然に防止するとともに、高価な設備の保護を図るシステムである。この安全計装システムは、プラントに異常事態が生じた場合に、「安全を守る最後の砦」としての役割を担っている。
【００２４】
安全コントローラ３１ａ，３１ｂは、安全計装システム３０の中核をなす装置であり、フィールド機器１０、或いは他の安全コントローラ（図示省略）と通信を行って必要なデータを得てプラントに異常事態が生じたか否かを判断する。また、安全コントローラ３１ａ，３１ｂは、プラントに異常事態が生じたと判断した場合に、安全制御を実現するための安全制御ロジックを実行する。エンジニアリング端末２３は、安全コントローラ３１で実行されるプログラムの作成するための装置でもある。
【００２５】
尚、本実施形態では、エンジニアリング端末２３が、分散制御システム２０と安全計装システム３０とで共用されるものとするが、分散制御システム２０及び安全計装システム３０の各々にエンジニアリング端末２３に相当する専用の端末が設けられていても良い。また、本実施形態では、安全計装システム３０に２台の安全コントローラ３１ａ，３１ｂが設けられる例について説明するが、安全計装システム３０に設けられる安全コントローラの台数は１台であっても良く、３台以上であっても良い。尚、安全コントローラ３１ａ，３１ｂの詳細については後述する。
【００２６】
製造システム４０は、プラントでの製品の製造を効率的に行うために構築されるシステムである。例えば、製造システム４０は、製造実行システム（ＭＥＳ：Manufacturing Execution System）、プラント情報管理システム（ＰＩＭＳ：Plant Information Management System）、或いは機器管理システム（ＰＡＭ：Plant Asset Management）等である。この製造システム４０として、製造実行システム、プラント情報管理システム、及び機器管理システムの何れか１つのみが構築されていても良く、何れか２つ以上が構築されていても良い。

【００２７】
経営システム５０は、企業における経営或いは営業等の業務を行うために構築されるシステムである。例えば、経営システム５０は、基幹業務システム（ＥＲＰ：Enterprise Resource Planning）等である。
【００２８】
ゾーンＺ１に区分けされた操作監視端末２２、エンジニアリング端末２３、及び検知装置６０は、ネットワーク機器ＮＥ１を介してゾーンＺ２に区分けされた製造システム４０に接続されている。ゾーンＺ２に区分けされた製造システム４０は、ネットワーク機器ＮＥ２を介してゾーンＺ３に区分けされた経営システム５０に接続されている。ゾーンＺ３に区分けされた経営システム５０は、ネットワーク機器ＮＥ３を介して不図示の他のネットワーク（例えば、インターネット）に接続されている。
【００２９】
つまり、上記のネットワーク機器ＮＥ１は、ゾーンＺ１とゾーンＺ２との間に設けられており、上記のネットワーク機器ＮＥ２は、ゾーンＺ２とゾーンＺ３との間に設けられており、上記のネットワーク機器ＮＥ３は、ゾーンＺ３と不図示の他のネットワーク（例えば、インターネット）との間に設けられている。尚、ネットワーク機器ＮＥ１～ＮＥ３は、ファイアウォール、ルータ、スイッチ等である。
【００３０】
検知装置６０は、前述したゾーンＺ１～Ｚ３毎に設けられており、自ゾーンに対する内部及び外部の少なくとも一方からのサイバー攻撃を検知する装置である。ここで、自ゾーンに対する外部からのサイバー攻撃としては、統合生産システム１への不正な侵入、統合生産システム１で用いられているプログラムの改竄、統合生産システム１で用いられるデータの詐取や破壊、統合生産システム１を機能不全に陥らせる行為、その他の行為が挙げられる。また、自ゾーンに対する内部からのサイバー攻撃としては、例えばウィルスに感染されたＵＳＢ（Universal Serial Bus）機器の持ち込み使用によって、上述のプログラムの改竄等が行われる事態が挙げられる。
【００３１】
検知装置６０は、ゾーンＺ１～Ｚ３の各々の設計思想により実装され、例えば市販のウィルス対策ソフト（ウィルス感染を検知してウィルスの除去を行うソフト）、或いは侵入検知システム等を活用することが可能である。尚、本実施形態では、理解を容易にするために、検知装置６０が「装置」として実装される例について説明するが、検知装置６０の機能がソフトウェアによって実現されていても良い。
【００３２】
ゾーンＺ１～Ｚ３の各々に設けられる検知装置６０は、ネットワークＮに接続されており、サイバー攻撃を検知した場合には、その検知結果を、ネットワークＮを介して安全コントローラ３１ａ，３１ｂに送信する。尚、本実施形態では、説明を簡単にするために、検知装置６０の検知結果が安全コントローラ３１ａ，３１ｂに送信されるとするが、安全コントローラ３１ａ，３１ｂに加えて制御コントローラ２１に送信されても良い。
【００３３】
〈制御装置〉
図２は、本発明の第１実施形態による制御装置の要部構成を示すブロック図である。尚、本実施形態による制御装置としての安全コントローラ３１ａ，３１ｂは、同様の構成である。このため、ここでは安全コントローラ３１ａについて説明し、安全コントローラ３１ｂについての説明は省略する。
【００３４】
図２に示す通り、安全コントローラ３１ａは、安全制御部ＳＣと防御部ＤＦ（制御手段）とを備える。安全制御部ＳＣは、安全コントローラ３１ａの本来の機能を実現する部分であり、外部の機器（例えば、フィールド機器１０、安全コントローラ３１ｂ等）と通信を行い、プラントに異常が生じた場合に、安全制御を実現するための安全制御ロジックを実行する。

【００３５】
防御部ＤＦは、設定部７１（設定手段）及び実行部７２（実行手段）を備えており、検知装置６０から得られる検知結果に基づいて、内部及び外部の少なくとも一方からのサイバー攻撃を防ぐためのセキュリティ対策を行う。具体的に、防御部ＤＦは、安全制御部ＳＣを制御して、安全コントローラ３１ａの機能の一部又は全部を制限する対策を行う。例えば、安全コントローラ３１ａで用いられているアプリケーションプログラムの変更を制限し、外部から入力される制御コマンドの実行を制限する制限を行う。
【００３６】
設定部７１は、検知装置６０の検知結果に基づいてサイバー攻撃の対象及び種別等を特定し、特定した内容に応じたセキュリティ対策を設定する。ここで、設定部７１は、サイバー攻撃の対象及び種別等の一覧を示す攻撃対象リストと、サイバー攻撃の対象及び種別等に応じて行うべきセキュリティ対策の一覧を示す対策リストとが対応付けられた設定リストＬＳを用いて上述のセキュリティ対策を設定する。実行部７２は、設定部７１で設定されたセキュリティ対策を実行する。尚、防御部ＤＦの機能はハードウェアによって実現されていても良く、ソフトウェアによって実現されていても良い。
【００３７】
図３は、本発明の第１実施形態における設定リストの一例を示す図である。また、図４は、本発明の第１実施形態における攻撃対象リスト及び対策リストの一例を示す図である。尚、図４（ａ）が、攻撃対象リストを示す図であり、図４（ｂ）が、対策リストを示す図である。図３，図４に示す通り、設定リストＬＳは、攻撃対象リストの「攻撃対象番号」（攻撃対象Ｎｏ．）、対策リストの「対策番号」（対策Ｎｏ．）、及び「対象機器」が対応付けられたリストである。尚、上記の「対象機器」は、セキュリティ対策が行われる対象となる機器である。
【００３８】
図４（ａ）に示す通り、攻撃対象リストは、「攻撃対象番号」（攻撃対象Ｎｏ．）、「ゾーン」、「機器」、「レベル」、及び「タイプ」が対応付けられたリストである。この攻撃対象リストは、どのゾーンのどの機器にどのような攻撃がなされたかを特定するために用いられるリストである。上記の「攻撃対象番号」は、統合生産システム１に対して行われる様々なサイバー攻撃を区別するために割り当てられる番号である。上記の「ゾーン」は、サイバー攻撃が行われたゾーンを特定するための情報である。
【００３９】
上記の「機器」は、サイバー攻撃が行われた機器を特定するための情報である。この「機器」としては、例えばパーソナルコンピュータ（ＰＣ)、コントローラ、スイッチ、ルータ、ファイアウォール等が挙げられる。上記の「レベル」は、サイバー攻撃が機器のどの部分に対して行われているかを特定するための情報である。この「レベル」としては、オペレーティングシステム（ＯＳ）、ネットワーク、ハードウェア、アプリケーションプログラム等が挙げられる。上記の「タイプ」は、サイバー攻撃の種別を特定するための情報である。この「タイプ」としては、例えばウィルス、ＤｏＳ攻撃（Denial of Service attack）等が挙げられる。
【００４０】
図４（ｂ）に示す通り、対策リストは、「対策番号」（対策Ｎｏ．）と「アクション」とが対応付けられたリストである。上記の「対策番号」は、統合生産システム１で行われる様々なセキュリティ対策を区別するために割り当てられる番号である。上記の「アクション」は、サイバー攻撃が行われた場合に、サイバー攻撃に対して行うべきセキュリティ対策を規定した情報である。この「アクション」としては、例えば安全コントローラ３１ａ，３１ｂで用いられているアプリケーションプログラムの変更の制限、同アプリケーションプログラムの変更の禁止、外部から入力される制御コマンドの実行の制限、同制御コマンドの破棄、全通信機能の停止、プラントシャットダウン等が挙げられる。
【００４１】
例えば、図３に示す設定リストＬＳの第１～４行目では、攻撃対象番号“Ａ１”～“Ａ

４”に対して、対策番号“Ｂ１”がそれぞれ対応付けられており、対象機器は対応付けられていない。このような対応付けがなされていることで、ゾーンＺ３に属する機器（ファイアウォール、スイッチ、ＰＣ）に対するサイバー攻撃が行われた場合には、安全コントローラ３１ａ，３１ｂでは、イベントログへの記録及びシステム管理者への通知のみが行われ、機能の一部又は全部を制限する対策は行われないことになる。

【００４２】

また、例えば、図３に示す設定リストＬＳの第５～７行目では、攻撃対象番号“Ａ５”～“Ａ７”に対して、対策番号“Ｂ２＆Ｂ４”がそれぞれ対応付けられ、対象機器“ＥＮＧ２３，ＣＮＴ３１ａ，３１ｂ”が対応付けられている。このような対応付けがなされていることで、ゾーンＺ２に属する機器（ファイアウォール、スイッチ、ＰＣ、コントローラ）に対するサイバー攻撃が行われた場合には、エンジニアリング端末（ＥＮＧ）２３及び安全コントローラ（ＣＮＴ）３１ａ，３１ｂにおいて、アプリケーションプログラムの変更を制限し、且つ外部から入力される制御コマンドの実行を制限する対策が行われることになる。

【００４３】

また、例えば、図３に示す設定リストＬＳの第８，１０～１２行目では、攻撃対象番号“Ａ８”，“Ａ１０”～“Ａ１２”に対して、対策番号“Ｂ３＆Ｂ５”がそれぞれ対応付けられ、対象機器“ＥＮＧ２３，ＣＮＴ３１ａ，３１ｂ”が対応付けられている。このような対応付けがなされていることで、ゾーンＺ１に属する操作監視端末（ＨＭＩ）２２、安全コントローラ（ＣＮＴ）３１ａ，３１ｂ、及び制御コントローラ２１に対するサイバー攻撃が行われた場合には、エンジニアリング端末（ＥＮＧ）２３及び安全コントローラ（ＣＮＴ）３１ａ，３１ｂにおいて、アプリケーションプログラムの変更を禁止し、且つ外部から入力される制御コマンドを破棄する対策が行われることになる。

【００４４】

また、例えば、図３に示す設定リストＬＳの第９行目では、攻撃対象番号“Ａ９”に対して、対策番号“Ｂ６”が対応付けられ、対象機器“ＥＮＧ２３，ＣＮＴ３１ａ，３１ｂ”が対応付けられている。このような対応付けがなされていることで、ゾーンＺ１に属するエンジニアリング端末（ＥＮＧ）２３に対するサイバー攻撃が行われた場合には、エンジニアリング端末（ＥＮＧ）２３及び安全コントローラ（ＣＮＴ）３１ａ，３１ｂにおいて、全通信機能を停止する対策が行われることになる。

【００４５】

図５は、本発明の第１実施形態における設定リストの他の例を示す図である。また、図６は、本発明の第１実施形態における攻撃対象リスト及び対策リストの他の例を示す図である。尚、図６（ａ）が、攻撃対象リストを示す図であり、図６（ｂ）が、対策リストを示す図である。図５に示す設定リストＬＳ、並びに図６に示す攻撃対象リスト及び対策リストは、図３，図４に示すものと比べてシンプルにしたものであり、サイバー攻撃が検知された場合に、管理者がサイバー攻撃への対応を判断するようにするものである。

【００４６】

例えば、図５に示す設定リストＬＳの第１，２行目では、攻撃対象番号“Ａ２１”，“Ａ２２”に対して、対策番号“Ｂ２１”がそれぞれ対応付けられており、対象機器は対応付けられていない。このような対応付けがなされていることで、ゾーンＺ２，Ｚ３に属する任意の機器に対するサイバー攻撃が行われた場合には、安全コントローラ３１ａ，３１ｂでは、イベントログへの記録及びシステム管理者への通知（画面表示）のみが行われ、機能の一部又は全部を制限する対策は行われないことになる。

【００４７】

また、例えば、図５に示す設定リストＬＳの第３行目では、攻撃対象番号“Ａ２３”に対して、対策番号“Ｂ２２”が対応付けられ、対象機器“ＥＮＧ２３，ＣＮＴ３１ａ，３１ｂ”が対応付けられている。このような対応付けがなされていることで、ゾーンＺ１に属する操作監視端末（ＨＭＩ）２２及び安全コントローラ（ＣＮＴ）３１ａ，３１ｂに対するサイバー攻撃が行われた場合には、エンジニアリング端末（ＥＮＧ）２３及び安全コ

ントローラ（ＣＮＴ）３１ａ，３１ｂにおいて、アプリケーションプログラムの変更を制限する対策が行われることになる。

【００４８】

また、例えば、図３に示す設定リストＬＳの第４行目では、攻撃対象番号“Ａ２４”に対して、対策番号“Ｂ２３”が対応付けられ、対象機器“ＥＮＧ２３，ＣＮＴ３１ａ，３１ｂ”が対応付けられている。このような対応付けがなされていることで、ゾーンＺ１に属するエンジニアリング端末（ＥＮＧ）２３に対するサイバー攻撃が行われた場合には、エンジニアリング端末（ＥＮＧ）２３及び安全コントローラ（ＣＮＴ）３１ａ，３１ｂにおいて、アプリケーションプログラムの変更を制限し、且つ外部から入力される制御コマンドの実行を制限する対策が行われることになる。

【００４９】

次に、上記構成における統合生産システム１の動作について説明する。尚、統合生産システム１の動作は多岐に亘るが、以下では、主に検知装置６０及び安全コントローラ３１ａ，３１ｂで行われる動作（サイバー攻撃を検知して防御する動作）について説明する。図７は、本発明の第１実施形態による制御装置としての安全コントローラ内の防御部の動作を示すフローチャートである。尚、図７に示すフローチャートの処理は、例えば予め規定された一定の周期で実行される。

【００５０】

図７に示すフローチャートの処理が開始されると、まず、検知装置６０から得られる検知結果を読み込み（ステップＳ１１）、その検知結果を解析する処理（ステップＳ１２）が安全コントローラ３１ａ，３１ｂに設けられた防御部ＤＦの設定部７１（図２参照）で行われる。次に、解析の結果に基づいて統合生産システム１に対するサイバー攻撃の有無を判断する処理が設定部７１で行われる（ステップＳ１３）。統合生産システム１に対するサイバー攻撃が無いと判断された場合（ステップＳ１３の判断結果が「ＮＯ」の場合に）には、図７に示す一連の処理が終了する。

【００５１】

これに対し、統合生産システム１に対するサイバー攻撃が有ったと判断された場合（ステップＳ１３の判断結果が「ＹＥＳ」の場合に）には、ステップＳ１２で行われた解析の結果から、サイバー攻撃の対象及び種別等を特定する処理が設定部７１で行われる（ステップＳ１４）。サイバー攻撃の対象及び種別等が特定されると、設定リストＬＳを用いて、特定された内容に応じたセキュリティ対策を設定する処理が設定部７１で行われる（ステップＳ１５）。セキュリティ対策が設定されると、設定されたセキュリティ対策を示す情報が設定部７１から実行部７２に出力され、設定部７１で設定されたセキュリティ対策を実行する処理が実行部７２で行われる（ステップＳ１６）。

【００５２】

ここで、例えばゾーンＺ３に属する経営システム５０で用いられているＰＣに対するサイバー攻撃が行われ、そのＰＣがウィルス感染したとする。すると、ゾーンＺ３に属する検知装置６０によって、ＰＣのウィルス感染が検知される。この検知結果は、安全コントローラ３１ａ，３１ｂに設けられた防御部ＤＦの設定部７１に読み込まれて（ステップＳ１１）、解析が行われる（ステップＳ１２）。すると、図７に示すステップＳ１３の判断結果が「ＹＥＳ」となり、ステップＳ１４の処理によって、サイバー攻撃によってゾーンＺ３に属するＰＣにウィルスが感染した（攻撃対象番号“Ａ４”）と特定される。

【００５３】

サイバー攻撃の対象及び種別等が特定されると、図３に示す設定リストＬＳの第４行目から攻撃対象番号“Ａ４”に対応付けられている対策番号“Ｂ１”に基づいて、安全コントローラ３１ａ，３１ｂに設けられた防御部ＤＦの設定部７１では、イベントログへの記録及びシステム管理者への通知を行うセキュリティ対策が設定される（ステップＳ１５）。そして、上記の設定部７１によって設定されたセキュリティ対策が実行部７２で行われ、イベントログへの記録及びシステム管理者への通知が実施される（ステップＳ１６）。

【００５４】

また、例えばゾーンＺ１に属するエンジニアリング端末２３に対するサイバー攻撃が行われたとする。すると、ゾーンＺ１に属する検知装置６０によって、エンジニアリング端末２３に対するサイバー攻撃が検知される。この検知結果は、安全コントローラ３１ａ，３１ｂに設けられた防御部ＤＦの設定部７１に読み込まれて（ステップＳ１１）、解析が行われる（ステップＳ１２）。すると、図７に示すステップＳ１３の判断結果が「ＹＥＳ」となり、ステップＳ１４の処理によって、サイバー攻撃によってゾーンＺ１に属するエンジニアリング端末２３に対するサイバー攻撃が行われた（攻撃対象番号“Ａ９”）と特定される。

【００５５】

サイバー攻撃の対象及び種別等が特定されると、図３に示す設定リストＬＳの第９行目から攻撃対象番号“Ａ９”に対応付けられている対策番号“Ｂ６”及び対象機器“ＥＮＧ２３，ＣＮＴ３１ａ，３１ｂ”に基づいて、エンジニアリング端末２３及び安全コントローラ３１ａ，３１ｂの全通信機能を停止するセキュリティ対策が設定される（ステップＳ１５）。そして、安全コントローラ３１ａ，３１ｂに設けられた防御部ＤＦの設定部７１によって設定されたセキュリティ対策が実行部７２で行われ、エンジニアリング端末２３及び安全コントローラ３１ａ，３１ｂの全通信機能が停止される（ステップＳ１６）。

【００５６】

以上の処理が行われることで、例えばウィルスに感染されたＵＳＢ機器がエンジニアリング端末２３で使用され、エンジニアリング端末２３がウィルスに感染したとしても、エンジニアリング端末２３及び安全コントローラ３１ａ，３１ｂは、全通信機能が停止されることになる。これにより、安全コントローラ３１ｂ，３１ｂに対するサイバー攻撃を未然に防ぐことができ、安全コントローラ３１ｂ，３１ｂの健全性を担保することができることから、「安全を守る最後の砦」としての役割が失われることはない。

【００５７】

以上の通り、本実施形態では、外部又は内部からのサイバー攻撃を検知する検知装置６０を設け、検知装置６０の検知結果に基づいて、安全コントローラ３１ａ，３１ｂ及びエンジニアリング端末２３の機能を制限する対策を行うようにしている。このため、安全コントローラ３１ｂ，３１ｂに対するサイバー攻撃を未然に防ぐことができ、安全コントローラ３１ｂ，３１ｂの健全性を担保することができる。また、サイバー攻撃の脅威に応じた対応策を設定することで、プラントを不用意に停止させることなく、サイバー攻撃を効果的に防ぐことが可能である。

【００５８】

〔第２実施形態〕

図８は、本発明の第２実施形態による統合生産システムの全体構成を示すブロック図である。尚、図８においては、図１に示す構成と同じ構成（或いは、図１に示す構成に相当する構成）には同一の符号を付してある。図８に示す通り、本実施形態の統合生産システム２は、図１に示す統合生産システム１と概ね同様の構成である。但し、本実施形態の統合生産システム２は、検知装置６０と安全コントローラ３１ａ，３１ｂとが、ネットワークＮとは異なる通信線Ｌ１（通信線）を介して接続されている点が、図１に示す統合生産システム１とは異なる。

【００５９】

通信線Ｌ１は、例えば接点信号を伝送するための伝送線、アナログ信号を伝送するための伝送線であり、検知装置６０で検知された検知結果を安全コントローラ３１ａ，３１ｂに送信するためのものである。尚、通信線Ｌ１は、検知装置６０と安全コントローラ３１ａ（或いは、安全コントローラ３１ｂ）とを１対１で接続するものであっても良く、複数の検知装置６０と安全コントローラ３１ａ，３１ｂとをネットワークの形態で接続するものであっても良い。

【００６０】

このように、通信線Ｌ１によって検知装置６０と安全コントローラ３１ａ，３１ｂとを接続するのは、外部又は内部からのサイバー攻撃をより確実に防ぐことができるようにす

るためである。つまり、サイバー攻撃がなされると、ネットワークＮを介した通信ができなくなる可能性が考えられる。仮に、ネットワークＮを介した通信ができなくなったとしても、通信線Ｌ１を介した通信が可能であれば、検知装置６０の検知結果を安全コントローラ３１ａ，３１ｂに送信することができ、検知装置６０の検知結果に応じたセキュリティ対策を安全コントローラ３１ａ，３１ｂで実施することができるため、外部又は内部からのサイバー攻撃をより確実に防ぐことができる。

【００６１】

尚、本実施形態の統合生産システム２は、検知装置６０の検知結果が通信線Ｌ１を介して安全コントローラ３１ａ，３１ｂに送信される点を除いて第１実施形態の統合生産システム１と同様である。このため、本実施形態の統合生産システム２の動作は、基本的には第１実施形態の統合生産システム１と同様であるため、ここでの詳細な説明は省略する。

【００６２】

以上の通り、本実施形態においても、第１実施形態と同様に、外部又は内部からのサイバー攻撃を検知する検知装置６０を設け、検知装置６０の検知結果に基づいて、安全コントローラ３１ａ，３１ｂ及びエンジニアリング端末２３の機能を制限する対策を行うようにしている。このため、安全コントローラ３１ｂ，３１ｂに対するサイバー攻撃を未然に防ぐことができ、安全コントローラ３１ｂ，３１ｂの健全性を担保することができる。また、サイバー攻撃の脅威に応じた対応策を設定することで、プラントを不用意に停止させることなく、サイバー攻撃を効果的に防ぐことが可能である。

【００６３】

〔その他の実施形態〕

図９は、本発明のその他の実施形態による統合生産システムを示すブロック図である。図９においては、図１，図８に示す構成と同じ構成（或いは、図１，図８に示す構成に相当する構成）には同一の符号を付してある。また、図９においては、フィールド機器１０及びネットワーク機器ＮＥ１～ＮＥ３等を省略して図示を簡略化している。

【００６４】

図９（ａ）に示す実施形態の統合生産システムは、製造システム４０と経営システム５０とが１つのゾーンＺ２０に区分けされ、そのゾーンＺ２０に１つの検知装置６０が設けられたものである。第１，第２実施形態の統合生産システム１，２は、階層を基準として複数のゾーンＺ１～Ｚ３に区分けされていたが、本実施形態のように、複数の階層が１つのゾーンに区分けされていても良い。

【００６５】

図９（ｂ）に示す実施形態の統合生産システムは、分散制御システム２０及び安全計装システム３０を複数備えるものである。この態様の統合生産システムでは、分散制御システム２０、安全計装システム３０、及び検知装置６０が１つずつゾーンＺ１１，Ｚ１２にそれぞれ区分けされている。尚、図９（ｂ）に示す態様の統合生産システムでは、例えばゾーンＺ２，Ｚ３に設けられた検知装置６０の検知結果は、ゾーンＺ１１，Ｚ１２に設けられた安全計装システム３０の安全コントローラ（図示省略）にそれぞれ入力され、ゾーンＺ１１に設けられた検知装置６０の検知結果は、ゾーンＺ１１に設けられた安全計装システム３０の安全コントローラ（図示省略）に入力され、ゾーンＺ１２に設けられた検知装置６０の検知結果は、ゾーンＺ１２に設けられた安全計装システム３０の安全コントローラ（図示省略）に入力される。

【００６６】

以上、本発明の実施形態による統合生産システムについて説明したが、本発明は上述した実施形態に制限されることなく、本発明の範囲内で自由に変更が可能である。例えば、上述した実施形態では、統合生産システムが、セキュリティ対策のために、国際標準規格ＩＳＡ－９５（ＩＥＣ／ＩＳＯ ６２２６４）で規定されている階層を基準として複数のゾーンＺ１～Ｚ３に区分けされている例について説明した。しかしながら、統合生産システムは、必ずしも上記の規格に準拠して構築されている必要はない。また、セキュリティ対策のためのゾーンは、図９に例示する通り、任意に設定することができ、統合生産シス

テムをなす構成を何れのゾーンに区分けするかも任意に設定することができる。

【００６７】

また、上述した実施形態では、理解を容易にするために、安全計装システム３０の安全コントローラ３１ｂ，３１ｂに対するサイバー攻撃を防御する例について説明した。しかしながら、安全計装システム３０に加えて、分散制御システム２０への影響を考慮して、セキュリティ対策を行うようにしても良い。このようなセキュリティ対策を行う場合には、安全計装システム３０の安全コントローラ３１ａ，３１ｂが備える防御部ＤＦと同様の構成を分散制御システム２０の制御コントローラ２１に設け、検知装置６０の検知結果が制御コントローラ２１にも入力される構成にする。そして、サイバー攻撃が行われた場合には、制御コントローラ２１が少なくとも一部の機能を制限する対策を行うようにする。

【００６８】

尚、図３，図５を用いて説明した通り、設定リストＬＳの内容は任意に設定することができるが、例えば「安全を守る最後の砦」としての役割を担っている安全計装システム３０が属するゾーンＺ１に近づくにつれて、対策のレベルが上がっていく内容に設定することが望ましい。このような内容に設定することで、プラントを不用意に停止させることなく、サイバー攻撃をより効果的に防ぐことが可能である。

【符号の説明】

【００６９】

１，２	統合生産システム
３０	安全計装システム
３１ａ，３１ｂ	安全コントローラ
６０	検知装置
７１	設定部
７２	実行部
ＤＦ	防御部
Ｌ１	通信線
ＬＳ	設定リスト
Ｎ	ネットワーク
Ｚ１～Ｚ３	ゾーン

【図１】

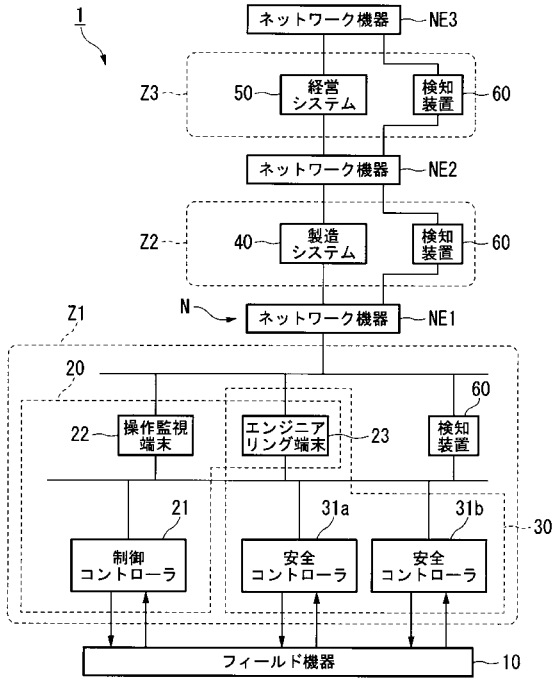

図１

【図２】

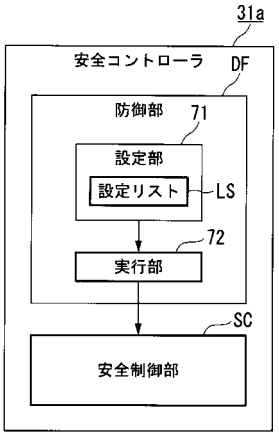

図２

【図３】

LS

攻撃対象No.	対策No.	対象機器
A1	B1	—
A2	B1	—
A3	B1	—
A4	B1	—
A5	B2&B4	ENG23, CNT31a, 31b
A6	B2&B4	ENG23, CNT31a, 31b
A7	B2&B4	ENG23, CNT31a, 31b
A8	B3&B5	ENG23, CNT31a, 31b
A9	B6	ENG23, CNT31a, 31b
A10	B3&B5	ENG23, CNT31a, 31b
A11	B3&B5	ENG23, CNT31a, 31b
A12	B3&B5	ENG23, CNT31a, 31b

図３

【図４】

(a)

攻撃対象No.	ゾーン	機器	レベル	タイプ
A1	Z3	ファイアウォール	ネットワーク	全アラーム
A2	Z3	ファイアウォール	ネットワーク	全アラーム
A3	Z3	スイッチ	ネットワーク	全アラーム
A4	Z3	PC	ALL	ウィルス ワーム
A5	Z2	ファイアウォール スイッチ	ネットワーク	全ワーニング 全アラーム
A6	Z2	スイッチ	ネットワーク	全ワーニング 全アラーム
A7	Z2	PC コントローラ	ALL	全ワーニング 全アラーム
A8	Z1	HMI22	ALL	全ワーニング 全アラーム
A9	Z1	ENG23	ALL	全ワーニング 全アラーム
A10	Z1	CNT31a	ALL	全ワーニング 全アラーム
A11	Z1	CNT31b	ALL	全ワーニング 全アラーム
A12	Z1	制御コントローラ	ALL	全ワーニング 全アラーム

(b)

対策No.	アクション
B1	イベントログに記録、システム管理者に通知
B2	アプリケーションの変更制限(二重パスワード)
B3	アプリケーションの変更禁止
B4	外部からの制御コマンド実行制限(確認ダイアログ表示)
B5	外部からの制御コマンド破棄
B6	全通信機能停止
B7	プラントシャットダウン

図４

【図５】

LS

攻撃対象No.	対策No.	対象機器
A21	B21	−
A22	B21	−
A23	B22	ENG23, CNT31a, 31b
A24	B23	ENG23, CNT31a, 31b

図5

【図６】

(a)

攻撃対象No.	ゾーン	機器	レベル	タイプ
A21	Z3	ALL	ALL	全アラーム
A22	Z2	ALL	ALL	全アラーム
A23	Z1	HMI22, CNT31a, 31b	ALL	全アラーム
A24	Z1	ENG23	ALL	全アラーム

(b)

対策No.	アクション
B21	イベントログに記録、システム管理者の管理画面にて表示可
B22	アプリケーションの変更制限(二重パスワード)
B23	アプリケーションの変更制限(二重パスワード) 外部からの制御コマンド実行制限(確認ダイアログ表示)

図6

【図７】

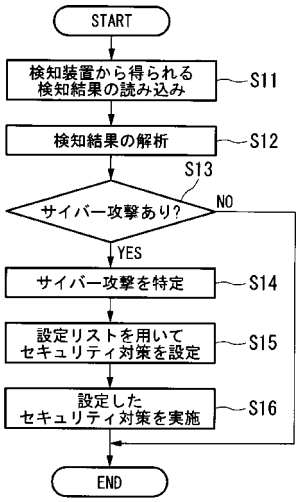

図7

【図８】

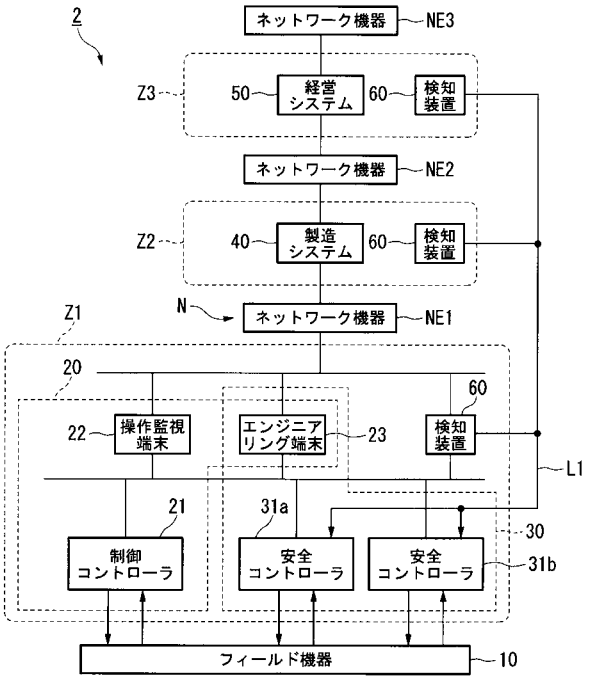

図8

【図９】

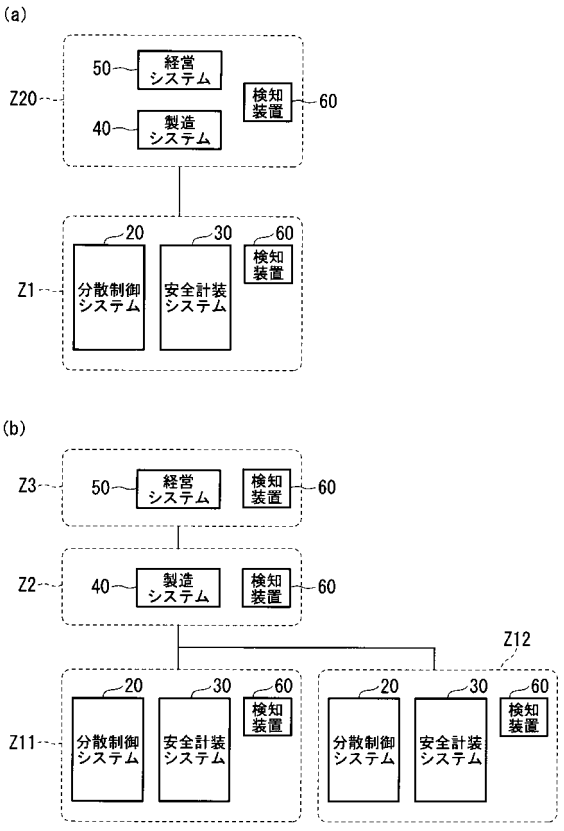

図9

フロントページの続き

(72)発明者　鈴木　和也
東京都武蔵野市中町２丁目９番３２号　横河電機株式会社内
(72)発明者　山城　靖彦
東京都武蔵野市中町２丁目９番３２号　横河電機株式会社内
(72)発明者　藤田　祥
東京都武蔵野市中町２丁目９番３２号　横河電機株式会社内
(72)発明者　長谷川　健司
東京都武蔵野市中町２丁目９番３２号　横河電機株式会社内
(72)発明者　監物　太郎
東京都武蔵野市中町２丁目９番３２号　横河電機株式会社内
(72)発明者　門脇　勇一郎
東京都武蔵野市中町２丁目９番３２号　横河電機株式会社内

Ｆターム(参考) 5B089 GA31 GA32 GB02 HA10 JB16 KA17 KB13 KC47 KC52 MC08
ME10
5H209 AA01 AA05 DD11 FF05 GG04 HH02 HH04 HH30