(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2016-158194
(P2016-158194A)
(43)公開日　平成28年9月1日(2016.9.1)

(51)Int.Cl.		F I			テーマコード（参考）
H04L 12/28	(2006.01)	H04L	12/28	200M	3C223
G05B 23/02	(2006.01)	G05B	23/02	V	5K033
H04L 12/46	(2006.01)	H04L	12/46	200S	5K048
H04Q 9/00	(2006.01)	H04Q	9/00	301B	

審査請求 未請求　請求項の数 4　ＯＬ　（全 17 頁）

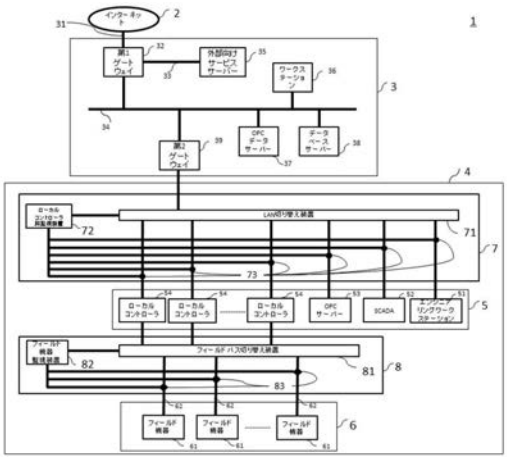
(21)出願番号　特願2015-36148(P2015-36148)
(22)出願日　平成27年2月26日(2015.2.26)

(71)出願人　304021277
国立大学法人　名古屋工業大学
愛知県名古屋市昭和区御器所町字木市２９番
(72)発明者　越島　一郎
愛知県名古屋市昭和区御器所町字木市２９番　国立大学法人名古屋工業大学内
(72)発明者　待井　航
愛知県名古屋市昭和区御器所町字木市２９番　国立大学法人名古屋工業大学内
(72)発明者　小池　正人
愛知県名古屋市昭和区御器所町字木市２９番　国立大学法人名古屋工業大学内

最終頁に続く

(54)【発明の名称】動的ゾーニングプラントシステム

(57)【要約】　（修正有）
【課題】プラントの機器のネットワーク接続を変更することによりインシデント被害の拡大の阻止と早期復旧を可能とする動的ゾーニングプラントシステムを提供する。
【解決手段】ＩＴ系システム３とローカルコントローラ群５との間に、ＬＡＮ切り替え装置７１と、ローカルコントローラ群監視装置７２と、ＬＡＮ分岐装置７３を有し、ローカルコントローラ群５のネットワークの構成を動的に変更するするＬＡＮ切り替えシステム７を備える。さらに、ローカルコントローラ群５とフィールド機器群６との間のフィールドバス６２に、フィールドバス切り替え装置８１と、フィールド機器監視装置８２と、フィールドバス分岐装置８３を有し、ローカルコントローラ群５とフィールド機器群６をつなぐネットワークの構成を動的に変更するフィールドバス切り替えシステム８を備える。
【選択図】図１



【特許請求の範囲】
【請求項１】
インターネットに繋がるＩＴ系システム（３）と、
前記ＩＴ系システム（３）に繋がるローカルコントローラ群（５）とフィールド機器群（６）を有する制御系システム（４）と、
を有する動的ゾーニングプラントシステム（１）において、
前記ＩＴ系システム（３）と前記ローカルコントローラ群（５）との間に、
前記ローカルコントローラ群（５）のネットワーク構成の変更のためのネットワークの動的変更を行う制御を行うＬＡＮ切り替え装置（７１）と、
前記ローカルコントローラ群（５）の通信の監視するローカルコントローラ群監視装置（７２）と、
前記ローカルコントローラ群（５）の通信を監視するＬＡＮ分岐装置（７３）を有し、
前記ローカルコントローラ郡（５）のネットワークの構成を動的に変更するするＬＡＮ切り替えシステム（７）と、を備え、
前記ローカルコントローラ群（５）と前記フィールド機器群（６）との間のフィールドバス（６２）に、
前記フィールド機器群（６）のネットワーク構成の変更のためのネットワークの動的変更を行う制御するフィールドバス切り替え装置（８１）と、
前記フィールド機器群（６）の通信の監視するフィールド機器監視装置（８２）と、
前記フィールド機器群（６）の通信を監視するフィールドバス分岐装置（８３）を有し、
前記ローカルコントローラ群（５）と前記フィールド機器群（６）をつなぐネットワークの構成を動的に変更するフィールドバス切り替えシステム（８）と、を備え、
プラントの動作中であってもプラントのネットワーク構成を手動もしくは自動で変更できる前記ＬＡＮ切り替えシステム（７）、または前記フィールドバス切り替えシステム（８）のいずれかを備えたことを特徴とする動的ゾーニングプラントシステム（１）。
【請求項２】
前記ＬＡＮ切り替え装置（７１）は、
前記ローカルコントローラ群（５）を接続するためのＬＡＮ切り替え手段（７１１）と、
自動でネットワーク構成を行うための自動変更プログラム（７１２２）を有するネットワーク構成変更手段（７１２）を備え、
前記ローカルコントローラ群監視装置（７２）は、
前記ＬＡＮ分岐装置（７３）が傍受した通信から、
前記ローカルコントローラ群（５）の状態を監視し、
異常発生時、
前記ネットワーク構成変更手段（７１２）に対して、
ネットワークの構成を変更の命令をすることを特徴とする請求項１に記載の動的ゾーニングプラントシステム（１）。
【請求項３】
前記フィールドバス切り替え装置（８１）は、
前記ローカルコントローラ群（５）と前記フィールド機器群（６）を接続するためのフィールドバス切り替え手段（８１１）と、
自動でネットワーク構成を行うための自動変更プログラム（８１２２）を有するネットワーク構成変更手段（８１２）を備え、
前記フィールド機器監視装置（８２）は、
前記フィールドバス分岐装置（８３）が傍受した通信から、
前記フィールド機器群（６）の状態を監視し、
異常発生時、
前記ネットワーク構成変更手段（８１２）に対して、
ネットワークの構成を変更の命令をすることを特徴とする請求項１または２に記載の動的ゾーニングプラントシステム（１）。

【請求項４】
前記ローカルコントローラ群監視装置（７２）、および前記フィールド機器監視装置（８２）は、正常時状態遷移表（９）を有し、異常判断を行っていることを特徴とする請求項１乃至３のいずれかに記載する動的ゾーニングプラントシステム（１）。

【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、プラントシステムのネットワークや接続構成を、生産プロセスを実行中であっても変更、つまりは動的な切り替えを可能にすることによりセキュリティやセーフティを向上させる技術に関する。
具体的には、現在主流のインターネットと接続されている一般的なプラントシステムは、ＩＴ系システムと制御系システムを備え、制御系はフィールドコントローラとローカルコントローラそれらの情報を監視するスーパーバイザリーシステムなどを備える。本発明は制御系システムに流れる通信を傍受することで、それらのシステムを監視し状態を把握することで、プラントシステムのネットワークや接続構成の変更を可能にする切り替え手段を有する動的ゾーニングプラントシステムに関する。システム構成の変更とはローカルコントローラやフィールド機器の接続を変更もしくは遮断することである。
【背景技術】
【０００２】
ネットワークを切り替える技術は既に存在しており、ネットワークの設定をソフトウェアで切り替える技術とネットワークのＬＡＮの接続を物理的に切り替える装置が存在する。これらの技術はセキュリティ向上やネットワークのリソースの効果的な活用のために利用されている。またこの技術を活用したシステムとして特許文献１が挙げられる。
【０００３】
特許文献１は、ネットワークに接続されたホストと、制御スイッチを備えたチャネルスイッチ装置、複数の記録媒体とロボット装置を格納したライブラリ装置からなる。ライブラリ制御システムはスイッチ装置がホストとドライブの接続の組み合わせを切り替え、さらにロボット装置が記録媒体とドライブの接続を切り替える仕組みを持つ動的ゾーニングプラントシステムが記載されている。これによりホストとドライブ装置の接続が変更可能になり、必要な時に動的にホストとドライブ装置の接続を変更することにより、複数のホストによりライブラリ装置を共有化して使用する場合に発生するデータ消失や破壊の防止などのセキュリティ向上を目的としている。
要するに最初から複数のホストによりライブラリ装置を共有化して使用する装置がありそれに対してセキュリティの向上を目的とした接続切り替え装置になる。
【０００４】
特許文献１に記載されている技術は、ネットワークを切り替える技術ではなく、システムの装置の構成を動的に切り替える技術である。またこの特許技術が対象にしているシステムはライブラリ装置になる。この特許技術の効果もセキュリティ向上と利便性にある。
【０００５】
現行のプラントのような制御系を用いたシステムはＩＴ系システムと組み合わせて構成されている。また近年では、プラントシステムは利便性や生産効率向上の観点から、外部

ネットワークへ接続されるようになってきた。しかしながら、制御系システムはセキュリティの観点を考慮して設計されておらず、セキュリティ対策が十分になされていない。その結果、ハッカーからのサイバー攻撃によってシステムをコントロールされてしまうという事例が発生している。ハッカーからのサイバー攻撃に対するセキュリティ向上策として、ゾーン分割という技術が存在する。これは制御系装置を複数のゾーンに分割し配置することでハッカーからの攻撃によって重大な事故を引き起こさせられる確率を下げ、サイバー攻撃による情報隠蔽工作を検知するためのものである。

【０００６】

図７の従来の一般的なプラントシステムの動的ゾーニングプラントシステムの構成図を示しており、この図について説明する。図７が示すようにプラントシステムは大きくＩＴ系システム３ａと制御系システム４ａに分割することができ、ＩＴ系システムは第１ゲートウェイ３２ａを通じて外部のインターネット２ａと接続されている。

ＩＴ系システム３ａにはインターネット２ａに接続される外部ネットワーク３１ａと非武装地帯に接続されるネットワーク３３ａと内部ネットワーク３４ａに接続する第１ゲートウェイ３２ａ、外部向けサービスサーバー３５ａ、ワークステーション３６ａ、ＯＰＣデータサーバー３７ａ、データベースサーバー３８ａ、内部ネットワーク３４ａと制御系システム４ａを接続する第２ゲートウェイ３９Ａがある。

さらに制御系システム４ａにはエンジニアリングワークステーション５１ａ、ＳＣＡＤＡ５２ａ、ＯＰＣサーバー５３ａ、ローカルコントローラ５４ａが存在する。これらを今回の発明ではローカルコントローラ群５ａとする。ローカルコントローラ５４ａの下位にフィールド機器６１ａがフィールドバス６２aで接続され存在し、これらをフィールド機器群６ａとする。

【０００７】

図８は従来の通常時の一般的なプラントシステムの動作のフローチャートを示しており、図８に従い、一般的なプラントシステムの動作を説明する。

Ｓ１００でオペレーターはエンジニアリングワークステーションを操作して生産プロセスを定義する。Ｓ１０１でオペレーターはプラントシステムを起動させる。Ｓ１０２でオペレーターは、ＳＣＡＤＡを操作してＯＰＣサーバーを経由してフィールド機器の設定値を入力する。Ｓ１０３でオペレーターはさきほど定義した生産プロセスを実行し、プラントシステムは生産プロセスにしたがって生産を行う。Ｓ１０４でプラントシステムは生産プロセスを完了し成果物を得る。

【０００８】

制御系はインフラや工場などに使用されており、インシデントが発生すると被害総額や被害規模が大規模になる可能性がある。過去において制御系を備えたプラントシステムはネットワークと接続されていなかったため、サイバー攻撃を受けることはないと考えられていた。その結果、十分なセキュリティ対策が施されていない、また制御系システムではオペレーションを常時継続することを最優先するため、そのオペレーションを阻害する可能性のあるＩＴ系のための既存のセキュリティ対策をそのまま適用できないという問題もある。例えば、制御系システムの代表であるプラントシステムなどは生産効率や安全性の観点から、インシデントが発生したからといって急にシステムを停止することが出来ないという問題がある。そのためＩＴ系サイドだけでなく制御系サイドでの特徴を考慮したセキュリティ対策が求められている現状がある。

【先行技術文献】

【特許文献】

【０００９】

【特許文献１】特開２００６－９２１６６

【００１０】

【非特許文献１】Industrial Network Security: Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems 2011/8/29Eric D. Knapp, Joel Thomas Langill

【発明の概要】
【発明が解決しようとする課題】
【００１１】
従来の動的ゾーニングプラントシステムは、制御系を備えたプラントシステムがセキュリティ上の脆弱性を持っており、これに対して対策を行う必要がある。またその解決策は既存のＩＴ系のセキュリティ対策ではなく制御系の特徴を踏まえたセキュリティ対策手法を提案すること。さらに制御系にインシデントが発生したとしても早期復旧や対策を行えるようにすることが本発明の解決しようとしている課題になる。
本発明は、動的ゾーニングプラントシステムであるプラントが生産プロセスを実行中であっても構成を変更させることでインシデント対応を行うことを目的とする。
【課題を解決するための手段】
【００１２】
発明１は、インターネットに繋がるＩＴ系システム（３）と、ＩＴ系システム（３）に繋がるローカルコントローラ群（５）とフィールド機器群（６）を有する制御系システム（４）と、を有する動的ゾーニングプラントシステム（１）において、ＩＴ系システム（３）とローカルコントローラ群（５）との間に、ローカルコントローラ群（５）のネットワーク構成の変更のためのネットワークの動的変更を行う制御を行うＬＡＮ切り替え装置（７１）と、ローカルコントローラ群（５）の通信の監視するローカルコントローラ群監視装置（７２）と、ローカルコントローラ群（５）の通信を監視するＬＡＮ分岐装置（７３）を有し、ローカルコントローラ郡（５）のネットワークの構成を動的に変更するするＬＡＮ切り替えシステム（７）と、を備え、ローカルコントローラ群（５）とフィールド機器群（６）との間のフィールドバス（６２）に、フィールド機器群（６）のネットワーク構成の変更のためのネットワークの動的変更を行う制御するフィールドバス切り替え装置（８１）と、フィールド機器群（６）の通信の監視するフィールド機器監視装置（８２）と、フィールド機器群（６）の通信を監視するフィールドバス分岐装置（８３）を有し、ローカルコントローラ群（５）とフィールド機器群（６）をつなぐネットワークの構成を動的に変更するフィールドバス切り替えシステム（８）と、を備え、プラントの動作中であってもプラントのネットワーク構成を手動もしくは自動で変更できるＬＡＮ切り替えシステム（７）、またはフィールドバス切り替えシステム（８）のいずれかを備えたことを特徴とする動的ゾーニングプラントシステム（１）である。
発明２は、ＬＡＮ切り替え装置（７１）は、ローカルコントローラ群（５）を接続するためのＬＡＮ切り替え手段（７１１）と、自動でネットワーク構成を行うための自動変更プログラム（７１２２）を有するネットワーク構成変更手段（７１２）を備え、ローカルコントローラ群監視装置（７２）は、ＬＡＮ分岐装置（７３）が傍受した通信から、ローカルコントローラ群（５）の状態を監視し、異常発生時、ネットワーク構成変更手段（７１２）に対して、ネットワークの構成を変更の命令をすることを特徴とする発明１に記載の動的ゾーニングプラントシステム（１）である。
発明３は、フィールドバス切り替え装置（８１）は、ローカルコントローラ群（５）とフィールド機器群（６）を接続するためのフィールドバス切り替え手段（８１１）と、自動でネットワーク構成を行うための自動変更プログラム（８１２２）を有するネットワーク構成変更手段（８１２）を備え、フィールド機器監視装置（８２）は、フィールドバス分岐装置（８３）が傍受した通信から、フィールド機器群（６）の状態を監視し、異常発生時、ネットワーク構成変更手段（８１２）に対して、ネットワークの構成を変更の命令をすることを特徴とする発明１または２に記載の動的ゾーニングプラントシステム（１）である。
発明４は、ローカルコントローラ群監視装置（７２）、およびフィールド機器監視装置（８２）は、正常時状態遷移表を有し、異常判断を行っていることを特徴とする発明１乃至３のいずれかに記載する動的ゾーニングプラントシステム（１）である。
【発明の効果】
【００１３】

発明１は、動的ゾーニングプラントシステムに、ＬＡＮ切り替えシステム（７）、またはフィールドバス切り替えシステム（８）のいずれかを有する動的ゾーニングプラントシステム（１）を提供することで、プラントシステムに、インシデントの発生、例えばハッカーからの攻撃やコンピュータウィルスの感染が発生した際、プラントシステムの構成を変更させるなどの対応をすることができる。よって、プラントシステムが稼働中の場合でも、生産を止めないで対策することが可能になる。
発明２は、ＬＡＮ切り替えシステム（７）のＬＡＮ切り替え装置（７１）は、ローカルコントローラ群（５）の状態を監視し、異常発生時、ネットワーク構成変更手段（７１２）に対して、ネットワークの構成を変更の命令をする。これは、自動変更プログラムによって自動的にローカルコントローラ群（５）の構成を変更できるようになり、インシデントの発生時にローカルコントロール群（５）の状態に合わせてネットワーク構成を変更することでインシデント対応を可能にする。よって、プラントシステムの生産プロセス実行に伴うプラントの状態変化に合わせて、制御系システムのネットワーク接続構成を変更することにより攻撃を受けにくくすることができる。
発明３は、フィールドバス切り替えシステム（８）のフィールドバス切り替え装置（８１）は、フィールド機器群（６）の状態を監視し、異常発生時、ネットワーク構成変更手段（８１２）に対して、ネットワークの構成を変更の命令をする。これは、自動変更プログラムによって自動的にフィールド機器群（６）の構成を変更できるようになり、インシデントの発生時にフィールド機器群（６）の状態に合わせてネットワーク構成を変更することでインシデント対応を可能にする。よって、プラントシステムの生産プロセス実行に伴うプラントの状態変化に合わせて、制御系システムのネットワーク接続構成を変更することにより攻撃を受けにくくすることができる。
発明４は、ローカルコントローラ群監視装置（７２）、およびフィールド機器監視装置（８２）は、正常時状態遷移表（９）を有し、異常判断を行っている。正常時状態遷移表（９）は、生産プロセス実行によりローカルコントローラとフィールド機器の状態も変化するため、時系列順のローカルコントローラとフィールド機器の状態変化を表す。ローカルコントローラ群監視装置（７２）、およびフィールド機器監視装置（８２）は、傍受した情報から把握したローカルコントローラとフィールド機器の状態と比較し、一致していれば正常、一致していなければ異常であると判断する。これにより、ローカルコントローラとフィールド機器の状態の異常を、適格に判断することができる。
以上より、本発明の動的ゾーニングプラントシステム（１）の適用は、プラントシステムに対するインシデントが発生の際の復元性の向上やプラントシステムのセーフティとセキュリティの向上効果を有する。
具体的には、プラントシステムを稼働時に、さらに何らかのインシデントが発生した場合には不正規な情報が流れるためこれを監視、発見し、状況に応じてネットワーク構成の変更を行うことで被害の拡大を阻止することが可能になる。
【００１４】
上記および特許請求の範囲における括弧内の符号は、特許請求の範囲に記載された用語と後述の実施形態に記載される当該用語を例示する具体物等との対応関係を示すものである。
【図面の簡単な説明】
【００１５】
【図１】本発明の第１実施形態に係る動的ゾーニングプラントシステム１の概要図を示す。
【図２】ＬＡＮ切り替えシステム７の構成図を示す。
【図３】フィールドバス切り替えシステム８の構成図を示す。
【図４】動的ゾーニングプラントシステム１の構成を元にしたインシデント発生時のフローチャートを示す。
【図５】ローカルコントローラ群５またはフィールド機器群６の正常時状態遷移表９を示す。

【図６】第２実施形態に係る動的ゾーニングプラントシステム１の正常時のフローチャートを示す。
【図７】従来のプラントシステムの概要図を示す。
【図８】従来の通常時の一般的なプラントシステムの動作のフローチャート示す。
【発明を実施するための形態】
【００１６】
以下図面を参照にしながら本発明の実施形態を説明する。本発明は、以下の実施形態に限定されるものではなく、発明の範囲を逸脱しない限りにおいて、変更、修正、改良を加え得るものである。
【００１７】
（第１実施形態）
図１は、本発明の第１実施形態に係る動的ゾーニングプラントシステム１の構成図を示す。図１に示すように、動的ゾーニングプラントシステムは、大きくＩＴ系システム３と制御系システム４に分割することができ、ＩＴ系システムは第１ゲートウェイを通じて外部のインターネットに接続されている。この図の構成は参考特許文献から抜粋した図８とほぼ同じ構成になっている。
ＩＴ系システム３には外部ネットワーク３１と非武装地帯３３と内部ネットワーク３４に接続する第１ゲートウェイ３２、外部向けサービスサーバー３５、ワークステーション３６、ＯＰＣデータサーバー３７、データベースサーバー３８、内部ネットワーク34と制御系ネットワークを接続する第２ゲートウェイ３９を有している。
さらに制御系システム４には一般的な制御系システムと同様にエンジニアリングワークステーション５１、ＳＣＡＤＡ５２、ＯＰＣサーバー５３、ローカルコントローラ５４、フィールド機器６１、フィールドバス６２を有している。
さらにローカルコントローラ群５の上部にＬＡＮ切り替えシステム７がある。ローカルコントローラ群５の内部にＬＡＮ切り替え装置７１と、ローカルコントローラ群監視装置７２とＬＡＮ分岐装置７３を有している。
ローカルコントローラ群５とフィールド機器群６の間のフィールドバス６２にフィールド機器監視システム８があり、フィールド機器監視システム８の内部にフィールド機器監視装置８２とフィールドバス分岐装置８３を有している。
【００１８】
図２は、第１実施形態のＬＡＮ切り替えシステム７の詳細を表した図である。ＬＡＮ切り替え装置７１は、手動変更プログラム７１２１と自動変更プログラム７１２２を備えたネットワーク構成変更手段７１２とＬＡＮ切り替え手段７１１を備えている。このＬＡＮ切り替え手段７１１によりＬＡＮ切り替え装置７１は第２ゲートウェイ３６とエンジニアリングワークステーション５１、ＳＣＡＤＡ５２、ＯＰＣサーバー５３、さらに複数のローカルコントローラ５４が接続される。ＬＡＮ切り替え装置７１に接続されたローカルコントローラ群監視装置７２は監視手段７２１と正常時切替手段７２２と異常時切替判定手段７２３を有する。ローカルコントローラ群監視装置７２はＬＡＮ分岐装置７３からの信号を受け取る。ＬＡＮ分岐装置７３はＬＡＮ切り替え装置７１とローカルコントローラ群５の間に存在する。
【００１９】
図３は、第１実施形態のフィールドバス切り替えシステム８の詳細を表した図である。フィールドバス切り替え装置８１は、手動変更プログラム８１３と自動変更プログラム８１４を備えたネットワーク構成変更手段８１２とフィールドバス切り替え手段８１１を備えている。このフィールドバス切り替え手段８１１によりフィールドバス切り替え装置８１は複数のローカルコントローラ５２と複数のフィールド機器６１が接続される。フィールドバス切り替え装置８１に接続されたフィールド機器監視装置８２は監視手段８２１と正常時切替手段８２２と異常時切替判定手段８２３を有する。フィールド機器監視装置８２はフィールドバス分岐装置６３からの信号を受け取る。フィールドバス分岐装置６３はローカルコントローラ５４とフィールド機器６１の間に存在する。

【００２０】
（機能）
図２を用いて、第１実施形態の動的ゾーニングプラントシステム１の機能について説明する。一般的なプラントシステムの機能と同様に動的ゾーニングプラントシステム１におけるＩＴ系システム３の第２ゲートウェイ３６の下位に存在する制御系システムはＳＣＡＤＡ５２を使用し、ＯＰＣサーバー５３を介して情報をローカルコントローラ５４へと送信する。ローカルコントローラ５４はその情報を基に設定されたプロセスを遂行する。
エンジニアリングワークステーション５１は生産プロセスの構築を行う機能を持ち、生産プロセスを稼働させる前に使用される。
ＩＴ系システムに存在するサーバー群は生産管理や生産計画の受注を行うためのものであり、そのため外部と情報のやりとりが必要になり、インターネットと接続される。
ローカルコントローラ５４はフィールド機器６１の制御を行い、フィールドバスを介してフィールド機器６１に接続される。
ローカルコントローラ５４は与えられた命令に従ってフィールド機器６１をコントロールし、生産プロセスを実行する。
ＬＡＮ切り替えシステムとフィールドバス切り替えシステムに関しては後述する。
【００２１】
図３を用いて、第１実施形態のＬＡＮ切り替えシステム７の機能について説明する。
ＬＡＮ切り替えシステム７はＬＡＮ切り替え手段７１１によってゲートウェイと複数のローカルコントローラ５４、ＯＰＣサーバー５３、ＳＣＡＤＡ５２、エンジニアリングワークステーション５１が接続される。ローカルコントローラ５４とＯＰＣサーバー５３、ＳＣＡＤＡ５２、エンジニアリングワークステーション５１にはアドレスが与えられており、指定の場所に情報が受け渡すことが可能になっている。ＬＡＮ切り替え装置７１のネットワーク構成変更手段７１２によってネットワーク構成を変更することが可能である。この際の変更は手動変更プログラム７１２１と自動変更プログラム７１２２によって手動もしくは自動で行うことができ、切り替えは短時間で行われプラントシステムの生産プロセスを妨げることがないようになっている。変更を自動で行うためにローカルコントローラ群監視装置７２はＬＡＮ分岐装置７３と監視手段７２１によりローカルコントローラ群５が上部でやり取りする通信を監視しローカルコントローラとフィールド機器の状態を把握している。
また監視手段７２１は監視した通信からローカルコントロール群５が正常か異常かを判断する。正常時においては、正常時切替手段７２２が働きネットワーク構成変更手段７１２に構成を変更する命令を出す。
正常時切替手段７２２にはコントローラ群５の状態に応じたプラント構成が登録されており、コントローラ群５が正常時の特定の状態の時に登録されたプラント構成へと変更させる命令をネットワーク構成変更手段７１２に送る。
インシデントが発生した場合には、監視手段７２１は監視した通信をもとに異常を発見し、必要があれば異常時切替判定手段７２３が働きネットワーク構成変更手段７１２に構成を変更する命令を出す。
異常時切替判定手段７２３にはローカルコントローラ群５の異常な状態に応じたプラント構成が登録されており、ローカルコントローラ群５が登録された異常な状態になると、これに合わせたプラント構成を変更させる命令をネットワーク構成変更手段７１２に送る。
ＬＡＮ分岐装置７３はローカルコントローラ５４とＬＡＮ切り替え装置７１の間に存在しており、アドレスを持たないためハッカーからのネットワーク解析によって自身を発見させないようになっており、ローカルコントローラ５４の通信を傍受しローカルコントローラ群監視装置７２に情報を送る。
【００２２】
図３を用いて、フィールドバス切り替えシステム８の機能について説明する。フィールドバス切り替えシステム８はフィールドバス切り替え手段８１１によって複数のローカルコントローラ５４と複数のフィールド機器６１が接続される。これによりローカルコントロ

ーラ５４から指定のフィールド機器６１に情報が受け渡すことが可能になっている。フィールドバス切り替え装置８１のネットワーク構成変更手段８１２によってフィールド機器６１の接続先は変更することが可能である。この際の変更は手動変更プログラム８１２１と自動変更プログラム８１２２によって手動もしくは自動で行うことができ、切り替えは短時間で行われプラントシステムの生産プロセスを妨げることがないようになっている。変更を自動で行うためにフィールド機器監視装置８２はフィールドバス分岐装置８３と監視手段８２１によりローカルコントローラ５４とフィールド機器６１でやりとりされる通信を監視し、各フィールド機器の状態を把握し、状態が変化したタイミングで自動変更プログラム８１２２に命令を出す。

また監視手段８２１は監視した通信からフィールド機器群６が正常か異常かを判断する。正常時においては、正常時切替手段８２２が働きネットワーク構成変更手段８１２に構成を変更する命令を出す。

正常時切替手段８２２にはフィールド機器群６の状態に応じたプラント構成が登録されており、フィールド機器群６が正常時の特定の状態の時に登録されたプラント構成へと変更させる命令をネットワーク構成変更手段８１２に送る。

インシデントが発生した場合には、監視手段８２１は監視した通信をもとに異常を発見し、必要があれば異常時切替判定手段８２３が働きネットワーク構成変更手段７１２に構成を変更する命令を出す。

異常時切替判定手段８２３にはコントローラ群５の異常な状態に応じたプラント構成が登録されており、フィールド機器群６が登録された異常な状態になると、これに合わせたプラント構成を変更させる命令をネットワーク構成変更手段８１２に送る。

フィールドバス分岐装置８３はローカルコントローラ５４とフィールド機器６１の間のフィールドバス６２に存在しており、アドレスを持たないためハッカーなどからのネットワーク解析によって自身を発見させないようになっており、フィールドバス６２を流れる情報を傍受しフィールド機器監視装置８２に情報を送る。

【００２３】

ローカルコントローラ群監視装置７２の監視手段７２１およびフィールド機器監視装置８２における監視手段８２１がどのように正常か異常かを判断する方法を説明する。一例として図５は、プラントシステムのローカルコントローラ群５とフィールド機器群６の正常時の状態遷移を表している（以下、正常時状態遷移表９）。正常時状態遷移表９の最左列が生産プロセス実行による変化するステップ番号になり、最上行はプラントシステムを構成するローカルコントローラ群５とフィールド機器群６になる。即ち、正常時状態遷移表９は、生産プロセス実行によりローカルコントローラ群５とフィールド機器群６の状態も変化するため、時系列順のローカルコントローラ群５とフィールド機器群６の状態変化が分かるようになっている。正常時状態遷移表９の図５のセルの中に記述されている０や１はローカルコントローラ群５とフィールド機器群６の状態を示している。このように正常時状態遷移表９は、プラントシステムの正常な作動状態を数値で定義する。第１実施形態は０と１で表しているが、プラントの生産プロセスや機器の仕組みなどによってはもっと多くの状態があるため、正常時状態遷移表９は、０や１以外の数値が記述されることもあり得る。

監視手段７２１、８２１では事前にこの図のような正常時状態遷移表９の情報を所持しており、傍受した情報から把握したローカルコントローラ群５とフィールド機器群６の状態と比較し、完全に一致していることを確認できた場合、正常であると判断する。また一部でも一致しないことを確認した場合、異常であると判断する。正常時状態遷移表９は、監視手段７２１、８２１において、それぞれ異なる。

【００２４】

（動作）

図４に従い、動的ゾーニングプラントシステム１のインシデント発生時の動作を説明する。

Ｓ２００でオペレーターは動的ゾーニングプラントシステム１を起動させる。Ｓ２０１で

オペレーターはエンジニアリングワークステーションを操作して生産プロセスを定義する。Ｓ２０２でオペレーターはＳＣＡＤＡを操作してＯＰＣサーバーを経由してフィールド機器の設定値を入力する。Ｓ２０３でオペレーターはさきほど定義した生産プロセスを実行し、動的ゾーニングプラントシステム１は生産プロセスにしたがって生産を行う。
Ｓ２０４ではハッカーなどのサイバー攻撃によるインシデントが発生する。Ｓ２０５ではローカルコントローラ群監視装置７２の監視手段７２１によって通信の異常を検知できたかどうかで分岐し、検知された場合Ｓ２０６へ（Ｓ２０５：ＹＥＳ）、検知されなかった場合Ｓ２１４へ進む（Ｓ２０５：ＮＯ）。異常状態か否かの判断は、監視手段７２１ではそれぞれローカルコントローラ群５に相当する正常時状態遷移表９の情報を所持しており、傍受した情報から把握したローカルコントローラ群５の状態と比較し、完全に一致していることを確認できた場合、正常であると判断する。Ｓ２０６では警告表示手段が監視手段によって検知された異常をオペレーターに告げる。Ｓ２０７ではローカルコントローラ群監視装置７２によって検知された異常状態が異常時切替判定手段７２３に定義された切り替えの条件か否かで分岐し、定義された条件に合致した場合S２０８へ（Ｓ２０７：ＹＥＳ）、合致しなかった場合Ｓ２１１へ進む（Ｓ２０７：ＮＯ）。Ｓ２０８でローカルコントローラ群監視装置７２の異常時切替判定手段７２３がＬＡＮ切り替え装置の自動変更プログラム７１２２を動かす命令を送る。Ｓ２０９でＬＡＮ切り替え装置の自動変更プログラム７１２２がインシデントに応じて実行されＬＡＮ切り替え手段７１１を用いてローカルコントローラの接続を変更し構成を変更する。Ｓ２１０で警告表示手段７２４がオペレーターに異常を検知し自動変更プログラム７１２２によって構成が変更されたことを表示して知らせる。Ｓ２１１で警告表示手段７２４がオペレーターに異常を検知したが構成が変更されなかったことを表示して知らせる。Ｓ２１２では自動的に切り替え装置が働かなかったとしても再度、オペレーターが動的ゾーニングプラントシステムの構成の変更が必要かどうかを判断し必要であると判断すればＳ２１３に移行（Ｓ２１２：ＹＥＳ）、必要でなければＳ２１４に移行する（Ｓ２１２：ＮＯ）。Ｓ２１３ではオペレーターは構成の変更を必要と判断したためＬＡＮ切り替え装置の手動変更プログラム７１２１を実行しＬＡＮ切り替え手段７１１を用いてローカルコントローラの接続５を変更し構成を変更する。Ｓ２１４ではプラントシステムは構成変更の有る無しにかかわらず定義された生産プロセスを継続する。

次に、Ｓ２１４ではフィールド機器監視装置８２の監視手段８２１によって通信の異常を検知できたかどうかで分岐し、検知された場合Ｓ２１５へ（Ｓ２１４：ＹＥＳ）、検知されなかった場合Ｓ２２３へ進む（Ｓ２１４：ＮＯ）。異常状態か否かの判断は、監視手段８２１では、それぞれフィールド機器群６に相当する正常時状態遷移表９の情報を所持しており、傍受した情報から把握したフィールド機器群６の状態と比較し、完全に一致していることを確認できた場合、正常であると判断する。Ｓ２１５では警告表示手段８２４が監視手段８２１によって検知された異常をオペレーターに告げる。Ｓ２１６では監視装置８２によって検知された異常状態が異常時切替判定手段８２３に定義された切り替えの条件か否かで分岐し、定義された条件に合致した場合S２１７へ（Ｓ２１６：ＹＥＳ）、合致しなかった場合Ｓ２２０へ進む（Ｓ２１６：ＮＯ）。Ｓ２１７で監視装置８２の異常時切替判定手段８２３がフィールドバス切り替え装置８１の自動変更プログラム８１２２を動かす命令を送る。Ｓ２１８でフィールドバス切り替え装置８１の自動変更プログラム８１２２がインシデントに応じて実行されフィールドバス切り替え手段８１１を用いてフィールド機器の接続を変更し構成を変更する。Ｓ２１９で警告表示手段８２４がオペレーターに異常を検知し自動変更プログラム８１２２によって構成が変更されたことを表示して知らせる。Ｓ２２０で警告表示手段８２４がオペレーターに異常を検知したが構成が変更されなかったことを表示して知らせる。Ｓ２２１では自動的に切り替え装置が働かなかったとしても再度、オペレーターが動的ゾーニングプラントシステムの構成の変更が必要かどうかを判断し必要であると判断すればＳ２２２に移行（Ｓ２２１：ＹＥＳ）、必要でなければＳ２２３に移行する（Ｓ２２１：ＮＯ）。Ｓ２２２ではオペレーターは構成の変更を必要と判断したためフィールドバス切り替え装置の手動変更プログラム８１２１を実

行しフィールドバス切り替え手段８１１を用いてフィールド機器群６の接続を変更し構成を変更する。Ｓ２２３ではプラントシステムは構成変更の有る無しに関わらず定義された生産プロセスを継続する。

【００２５】

以上より、インシデントが発生し異常を検出し、自動変更プログラム７１２２、８１２２が実行されない場合、オペレーターがプラントを手動変更プログラム７１２１、８１２１で変更することになる。ただし、オペレーターが手動変更プログラム７１２１、８１２１を実行できなかったとしても、プラントの生産プロセスは既に実行されている場合急には、生産を停止することはできないため生産プロセスが継続される。

【００２６】

（効果）

第１実施形態の動的ゾーニングプラントシステム１によって、インシデントが起こった際にプラントの機器のネットワーク接続を変更することにより被害の拡大の阻止と早期復旧を可能とする。

【００２７】

ＬＡＮ切り替え装置７１のネットワーク構成変更手段７１２によって、ローカルコントローラ５４の接続が変更されるとハッカーがサイバー攻撃を成功することがより困難になる。またネットワークから切り離すことにより攻撃の影響の範囲を限定することができる上に、隔離した状態でコントロールが可能になる。ハッカーのサイバー攻撃に対して早期に気付いた場合（例えば、マルウェア感染した場所がＳＣＡＤＡのみ、ハッカーによって侵入された端末がＯＰＣサーバーのみなど）ＳＣＡＤＡやＯＰＣサーバーをネットワークから切り離すことで、安全性の確立と、早期マルウェア対応やハッカーをシャットアウトすることが可能になる。これらの切り替えはプラントの生産プロセスを実行中に可能であるため、生産プロセスを止めることなくインシデント対応が可能になる。

【００２８】

ＬＡＮ分岐装置７３とフィールドバス分岐装置８３は自身のアドレスを持たずに自身の存在するネットワークに流れる情報を傍受し、ローカルコントローラ群監視装置７２またはフィールド機器監視装置８２に受け渡す。これによりハッカーからはプラントシステムのローカルコントローラ群５とフィールド機器群６を監視していることを分からないようにしながら監視することができるためＬＡＮ分岐装置７３とフィールドバス分岐装置８３は攻撃を受けることなく確実に傍受し続けることが可能になる。

【００２９】

ローカルコントローラ群監視装置７２とフィールド機器監視装置８２は、それぞれ監視手段７２１、８２１と異常時切替判定手段７２３、８２３を持ち、ＬＡＮ分岐装置７３とフィールドバス分岐装置８３により傍受した通信を、監視手段７２１、８２１に定義された情報の状態と比較することで異常を発見することが可能である。また異常時切替判定手段７２３、８２３により発見した異常に合わせた適切な命令をネットワーク切り替え手段に送ることが可能である。

【００３０】

（第２実施形態）

従来のプラントシステムでは、正常に稼働している場合、構成機器など変更の際には安全のためにプラントをいったん完全に停止させる必要があった。そのためプラント構成を変更させるためには停止から再稼働までの時間と停止したことによる生産効率の低下によるコストがかかる課題があった。第２実施形態は、プラントを停止することなく、プラントの構成を変更できるようにし、オペレーターの操作ミスやハッカーからのサイバー攻撃の予防をすることを目的とする。

【００３１】

発明１により、これを行う動的ゾーニングプラントシステム（１）を提供することができる。

また、発明５は、ＬＡＮ切り替え装置（７１）は、ローカルコントローラ群（５）を接続

するためのＬＡＮ切り替え手段（７１１）と、自動でネットワーク構成を行うための自動変更プログラム（７１２２）を有するネットワーク構成変更手段（７１２）を備え、ローカルコントローラ群監視装置（７２）は、ＬＡＮ分岐装置（７３）が傍受した通信から、前記ローカルコントローラ群（５）の状態を監視し、正常時に監視していた情報から、ローカルコントローラ群（５）の接続を変更すべきタイミングを判断し、ネットワーク構成変更手段（７１２）に対して、ネットワークの構成を変更の命令をすることを特徴とする発明１に記載の動的ゾーニングプラントシステム（１）である。
発明５は、ＬＡＮ切り替えシステム（７）のＬＡＮ切り替え装置（７１）は、ローカルコントローラ群（５）の状態を監視し、正常時、ネットワーク構成変更手段（７１２）に対して、ネットワークの構成を変更の命令をする。これは、自動変更プログラムによって自動的にローカルコントローラ群（５）の構成を変更できるようになり、インシデントが発生しておらず生産プロセスが問題なく遂行されている正常時にローカルコントロール群（５）の状態に合わせてネットワーク構成を変更することを可能にする。よって、プラントシステムの生産プロセス実行に伴うプラントの状態変化に合わせて、制御系システムのネットワーク接続構成を変更することにより、使っていない機器を切り離すなど必要性の薄い機器を変更する機能がある。よって、プラントシステムのサイバー攻撃に対する露出を最小限にする、人間による誤操作を防ぐ効果がある。
発明６は、フィールドバス切り替え装置（８１）は、ローカルコントローラ群（５）とフィールド機器群（６）を接続するためのフィールドバス切り替え手段（８１１）と、
自動でネットワーク構成を行うための自動変更プログラム（８１２２）を有するネットワーク構成変更手段（８１２）を備え、フィールド機器監視装置（８２）は、フィールドバス分岐装置（８３）が傍受した通信から、フィールド機器群（６）の状態を監視し、正常時に監視していた情報からフィールド機器群（６）の接続を変更すべきタイミングを判断し、ネットワーク構成変更手段（８１２）に対して、ネットワークの構成を変更の命令をすることを特徴とする発明１または５に記載の動的ゾーニングプラントシステム（１）である。
発明６は、フィールドバス切り替えシステム（８）のフィールドバス切り替え装置（８１）は、フィールド機器群（６）の状態を監視し、インシデントが発生しておらず生産プロセスが問題なく遂行されている正常時、ネットワーク構成変更手段（８１２）に対して、ネットワークの構成を変更の命令をする。これは、自動変更プログラムによって自動的にフィールド機器群（６）の構成を変更できるようになり、正常時にフィールド機器群（６）の状態に合わせてネットワーク構成を変更することを可能にする。よって、プラントシステムの生産プロセス実行に伴うプラントの状態変化に合わせて、制御系システムのネットワーク接続構成を変更することにより、使っていない機器を切り離すなど必要性の薄い機器を変更する機能がある。よって、プラントシステムのサイバー攻撃に対する露出を最小限にする、人間による誤操作を防ぐ効果がある。
【００３２】
図６に、第２実施形態に係る動的ゾーニングプラントシステム１正常時のフローチャートを示す。
まずＳ５００でオペレーターは動的ゾーニングプラントシステム１を起動させる。Ｓ５０１でオペレーターはエンジニアリングワークステーションを操作して生産プロセスを定義する。Ｓ５０２でオペレーターはＳＣＡＤＡを操作してＯＰＣサーバーを経由してフィールド機器群６の設定値を入力する。Ｓ５０３でオペレーターはさきほど定義した生産プロセスを実行し、動的ゾーニングプラントシステム１は生産プロセスにしたがって生産を行う。Ｓ５０４でローカルコントローラ群監視装置７２の監視手段７２１が通信を監視し、正常状態であると判断する。Ｓ５０５でローカルコントローラ群監視装置７２の正常時切替判定手段７２２によって切り替えの条件と照らし合わせネットワーク構成の変更の有無を判断し、必要であると判断すれば変更の命令を自動変更プログラム７１２２に対して行いＳ５０６に移行（Ｓ５０５：ＹＥＳ）、必要でなければＳ５０７に移行する（Ｓ５０５：ＮＯ）。Ｓ５０６でＬＡＮ切り替え装置７１の自動変更プログラム７１２２が命令に従

ってＬＡＮ切り替え手段７１１を用いてローカルコントローラ群５の接続を変更する。Ｓ５０７ではプラントシステムは構成の変更が有る無しに関わらず定義された生産プロセスを継続する。
次に、Ｓ５０８でフィールド機器監視装置８２の監視手段８２１が通信を監視し、正常状態であると判断する。Ｓ５０９でフィールド機器監視装置８２の正常時切替判定手段８２２によって切り替えの条件と照らし合わせネットワーク構成の変更の有無を判断し、必要であると判断すれば変更の命令を自動変更プログラム８１２２に対して行いＳ５１０に移行（Ｓ５０９：ＹＥＳ）、必要でなければＳ５１１に移行する（Ｓ５０９：ＮＯ）。
Ｓ５１０でフィールドバス切り替え装置８１の自動変更プログラム８１２２が命令に従ってフィールドバス切り替え手段８１１を用いてフィールド機器群６の接続を変更する。Ｓ５１１ではプラントシステムは構成の変更が有る無しに関わらず定義された生産プロセスを継続する。

【産業上の利用可能性】

【００３３】

（使用時の例１）

動的ゾーニングプラントシステム１のＩＴ系システム３の部署にハッカーが潜り込みプラントシステムを破壊するマルウェアをＯＰＣデータサーバーにアップロードした。マルウェアは通信のログなどを元にさらなるネットワーク情報を取得し、脆弱性を悪用して制御系システム内部のＳＣＡＤＡに侵入した場合の使用例である。マルウェアはＳＣＡＤＡからＯＰＣサーバーを踏み台にしてローカルコントローラ５４に不正規な命令を送った。ＬＡＮ分岐装置７３によって傍受された不正規な命令はローカルコントローラ群監視装置７２に送られ監視手段を用いて異常を発見した。この異常を元に異常時切替判定手段７２３がＬＡＮ切り替え装置７１のネットワーク構成変更手段を用いてローカルコントローラ５４を素早くネットワークから独立させた。これによりマルウェアの影響の波及を抑えることができる。

（使用時の例２）

プラントシステムに対する攻撃が何件も報告されているというシチュエーションを仮定した場合である。こういったニュースが動的ゾーニングプラントシステム１の関係者の耳に入った時点で、念のためエンジニアリングワークステーション、ＳＣＡＤＡ、ＯＰＣサーバー、ローカルコントローラ５４のアドレスや構成、ゾーン、さらにローカルコントローラ群５とフィールド機器群６の接続構成がネットワーク構成変更手段を用いて変更された。この攻撃は事前に内部の情報を取得したことで成功させるタイプの攻撃だったため、アドレス、ゾーンを変更することで攻撃対象を見失うことになり、ハッカーの思惑が外れた。これにより事前に攻撃を防ぐことができる。

（使用時の例３）

通常時においてオペレーターはＳＣＡＤＡを操作して、フィールド機器６１に設定値を送り込んだ場合である。その後の生産プロセスにおいてこのフィールド機器６１は操作を行う必要がないため、自動変更プログラムによってネットワークから切り離された。これにより、オペレーターが間違った操作をすることを防ぐことができ、またハッカーの攻撃の対象となりうる可能性を下げることができた。

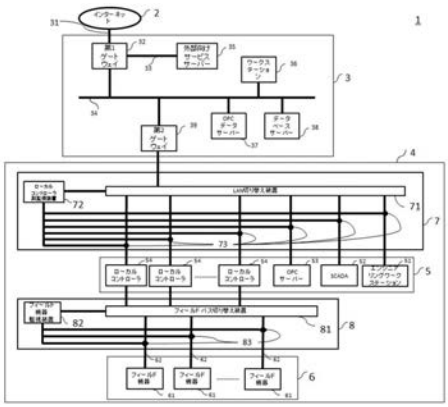
【符号の説明】

【００３４】

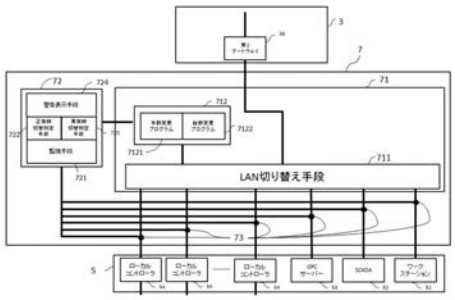
１　プラントシステム
２　インターネット
３　ＩＴ系システム
４　制御系システム
５　ローカルコントローラ群
６　フィールド機器群
７　ＬＡＮ切り替えシステム
８　フィールドバス切り替えシステム

９　　正常時状態遷移表
３１　　外部ネットワーク
３２　　第１ゲートウェイ
３３　　非武装地帯
３４　　内部ネットワーク
３５　　外部向けサービスサーバー
３６　　ワークステーション
３７　　ＯＰＣデータサーバー
３８　　データベースサーバー
３９　　第２ゲートウェイ
５１　　エンジニアリングワークステーション
５２　　ＳＣＡＤＡ
５３　　ＯＰＣサーバー
５４　　ローカルコントローラ
６１　　フィールド機器
６２　　フィールドバス
７１　　ＬＡＮ切り替え装置
７２　　ローカルコントローラ群監視装置
７３　　ＬＡＮ分岐装置
８１　　フィールドバス切り替え装置
８２　　フィールド機器監視装置
８３　　フィールドバス分岐装置
７１１　ＬＡＮ切り替え手段
７１２　ネットワーク構成変更手段
７１２１　手動変更プログラム
７１２２　自動変更プログラム
７２１　監視手段
７２２　正常時判定手段
７２３　異常時判定手段
７２４　警告表示手段
８１１　フィールドバス切り替え手段
８１２　ネットワーク構成変更手段
８１２１　手動変更プログラム
８１２２　自動変更プログラム
８２１　監視手段
８２２　正常時判定手段
８２３　異常時判定手段
８２４　警告表示手段

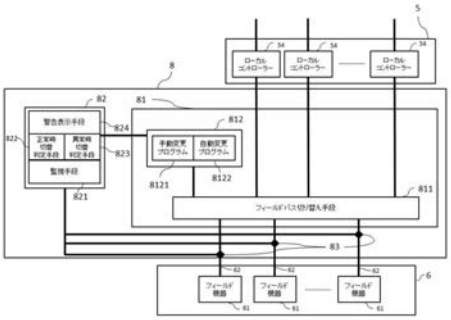
【図１】



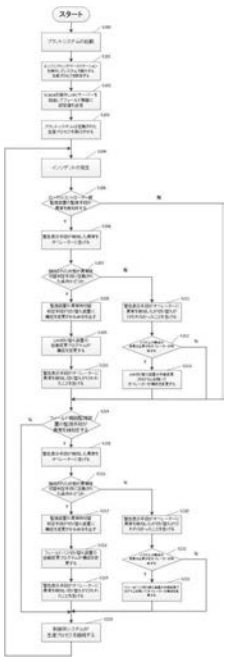
【図２】



【図３】



【図４】

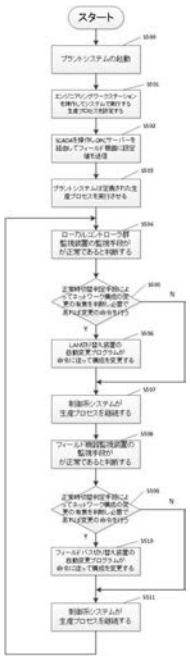


【図５】

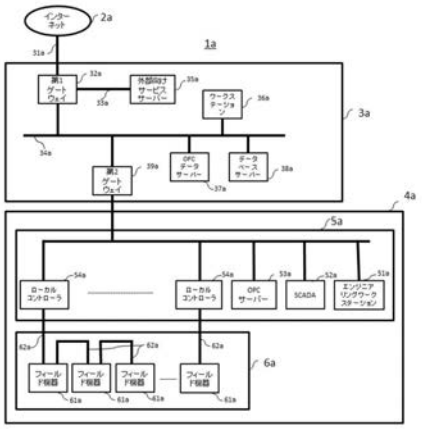
9

プラントの生産プロセスのステップ	機器1	機器2	機器3	機器4	機器5	機器6	機器7	機器8
1	0	0	0	0	0	0	0	0
2	1	1	0	0	0	1	1	1
3	1	1	0	0	0	0	0	0
4	1	1	0	0	1	0	0	0
5	0	1	0	0	1	0	1	0
6	0	1	0	0	1	0	1	0
7	0	1	0	0	1	0	1	0
8	0	1	0	0	0	0	0	0
9	0	1	0	1	0	0	0	0
10	0	1	0	1	0	0	0	0
11	1	1	0	0	0	0	0	0
12	1	1	0	0	0	0	0	0
13	1	1	1	0	0	0	0	0
14	0	1	1	0	0	1	0	0
15	0	1	1	0	0	1	0	0
16	1	1	1	0	0	1	0	1
17	1	1	0	0	0	0	0	1
18	1	1	0	0	1	0	0	1
19	0	1	0	0	1	0	1	1
20	0	1	1	0	0	0	1	1
21	0	0	1	0	0	0	1	1
22	0	0	0	0	0	0	1	0
23	0	0	0	0	0	0	1	0

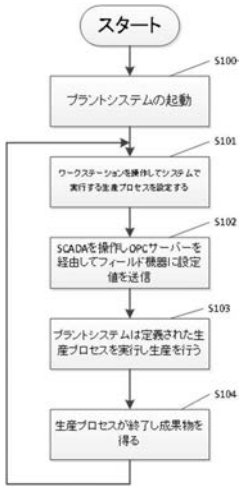
【図６】


スタート
S100
プラントシステムの起動
S101
S102
S103
S104
S105
S106
S107
S108
S109
S110
S111

【図７】


インターネット
2a
1a
31a
第1ゲートウェイ
32a
33a
外部向けサービスサーバー
35a
ワークステーション
36a
3a
34a
第2ゲートウェイ
39a
OPCデータサーバー
37a
データベースサーバー
38a
4a
5a
ローカルコントローラ
54a
ローカルコントローラ
54a
OPCサーバー
53a
SCADA
52a
エンジニアリングワークステーション
51a
62a
62a
62a
フィールド機器
61a
フィールド機器
61a
フィールド機器
61a
フィールド機器
61a
6a

【図８】


スタート
S100
プラントシステムの起動
S101
ワークステーションを操作してシステムで実行する生産プロセスを設定する
S102
SCADAを操作しOPCサーバーを経由してフィールド機器に設定値を送信
S103
プラントシステムは定義された生産プロセスを実行し生産を行う
S104
生産プロセスが終了し成果物を得る

フロントページの続き

(72)発明者　青山　友美
愛知県名古屋市昭和区御器所町字木市２９番　国立大学法人名古屋工業大学内
(72)発明者　内田　拓郎
愛知県名古屋市昭和区御器所町字木市２９番　国立大学法人名古屋工業大学内

Ｆターム(参考) 3C223 AA01 BA04 CC04 DD03 DD04 EA07 FF32 GG01 HH01
5K033 AA06 BA08 DA02 DB01 DB20 EA06 EB07 EB08
5K048 AA06 BA23 DC03 EB02