

(19) 日本国特許庁(JP)

(12) 特許公報(B2)

(11) 特許番号

特許第6598288号
(P6598288)

(45) 発行日 令和1年10月30日(2019.10.30)

(24) 登録日 令和1年10月11日(2019.10.11)

| | | | | | |
|--------------|-------|-----------|------|-------|------|
| (51) Int.Cl. | | F I | | | |
| HO4L | 12/28 | (2006.01) | HO4L | 12/28 | 200M |
| GO5B | 23/02 | (2006.01) | GO5B | 23/02 | V |
| HO4L | 12/46 | (2006.01) | HO4L | 12/46 | 200S |
| HO4Q | 9/00 | (2006.01) | HO4Q | 9/00 | 301B |

請求項の数 4 (全 17 頁)

| | | | |
|-----------|-------------------------------|-----------|-------------------------------------|
| (21) 出願番号 | 特願2015-36148 (P2015-36148) | (73) 特許権者 | 304021277 |
| (22) 出願日 | 平成27年2月26日(2015.2.26) | | 国立大学法人 名古屋工業大学 |
| (65) 公開番号 | 特開2016-158194 (P2016-158194A) | | 愛知県名古屋市昭和区御器所町字木市29番 |
| (43) 公開日 | 平成28年9月1日(2016.9.1) | (72) 発明者 | 越島 一郎 |
| 審査請求日 | 平成30年2月23日(2018.2.23) | | 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) 【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)の通信を傍受するLAN分岐装置(73)を有し、
 前記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)の通信を傍受するフィールドバス分岐装置(83)を有し、

10

20

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、

10

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、

20

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)。

30

【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安全性を向上させる技術に関する。

40

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

50

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ンネルスイッチ装置、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。

10

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。

20

【0006】

図7の従来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。

30

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。

40

【0007】

図8は従来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

50

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。

10

【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

20

【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。

30

【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)の通信を傍受する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)の通信を傍受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

40

50

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

10

20

30

40

50

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

10

【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。

20

【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。

30

【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35、ワークステーション36、OPCデータサーバ37、データベースサーバ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。

40

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。

50

【 0 0 1 8 】

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

10

【 0 0 1 9 】

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

20

【 0 0 2 0 】

(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。

30

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。

【 0 0 2 1 】

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

40

50

している。

また監視手段 7 2 1 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 7 2 2 が働きネットワーク構成変更手段 7 1 2 に構成を変更する命令を出す。

正常時切替手段 7 2 2 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 7 1 2 に送る。

インシデントが発生した場合には、監視手段 7 2 1 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 7 2 3 が働きネットワーク構成変更手段 7 1 2 に構成を変更する命令を出す。

異常時切替判定手段 7 2 3 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 7 1 2 に送る。LAN 分岐装置 7 3 はローカルコントローラ 5 4 と LAN 切り替え装置 7 1 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しており、ローカルコントローラ 5 4 の通信を傍受しローカルコントローラ群監視装置 7 2 に情報を送る。

【 0 0 2 2 】

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 8 1 1 によって複数のローカルコントローラ 5 4 と複数のフィールド機器 6 1 が接続される。これによりローカルコントローラ 5 4 から指定のフィールド機器 6 1 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 8 1 のネットワーク構成変更手段 8 1 2 によってフィールド機器 6 1 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 8 1 2 1 と自動変更プログラム 8 1 2 2 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している。変更を自動で行うためにフィールド機器監視装置 8 2 はフィールドバス分岐装置 8 3 と監視手段 8 2 1 によりローカルコントローラ 5 4 とフィールド機器 6 1 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 8 1 2 2 に命令を出す。

また監視手段 8 2 1 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 8 2 2 が働きネットワーク構成変更手段 8 1 2 に構成を変更する命令を出す。

正常時切替手段 8 2 2 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 8 1 2 に送る。

インシデントが発生した場合には、監視手段 8 2 1 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 8 2 3 が働きネットワーク構成変更手段 7 1 2 に構成を変更する命令を出す。

異常時切替判定手段 8 2 3 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 8 1 2 に送る。

フィールドバス分岐装置 8 3 はローカルコントローラ 5 4 とフィールド機器 6 1 の間のフィールドバス 6 2 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しており、フィールドバス 6 2 を流れる情報を傍受しフィールド機器監視装置 8 2 に情報を送る。

【 0 0 2 3 】

ローカルコントローラ群監視装置 7 2 の監視手段 7 2 1 およびフィールド機器監視装置 8 2 における監視手段 8 2 1 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

10

20

30

40

50

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。

10

監視手段 7 2 1、8 2 1 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 7 2 1、8 2 1 において、それぞれ異なる。

【 0 0 2 4 】

（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。

20

S 2 0 0 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。S 2 0 1 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。S 2 0 2 でオペレーターは S C A D A を操作して O P C サーバを經由してフィールド機器の設定値を入力する。S 2 0 3 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。

S 2 0 4 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。S 2 0 5 ではローカルコントローラ群監視装置 7 2 の監視手段 7 2 1 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 S 2 0 6 へ（S 2 0 5 : Y E S）、検知されなかった場合 S 2 1 4 へ進む（S 2 0 5 : N O）。異常状態か否かの判断は、監視手段 7 2 1 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。S 2 0 6 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。S 2 0 7 ではローカルコントローラ群監視装置 7 2 によって検知された異常状態が異常時切替判定手段 7 2 3 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 S 2 0 8 へ（S 2 0 7 : Y E S）、合致しなかった場合 S 2 1 1 へ進む（S 2 0 7 : N O）。S 2 0 8 でローカルコントローラ群監視装置 7 2 の異常時切替判定手段 7 2 3 が L A N 切り替え装置の自動変更プログラム 7 1 2 2 を動かす命令を送る。S 2 0 9 で L A N 切り替え装置の自動変更プログラム 7 1 2 2 がインシデントに応じて実行され L A N 切り替え手段 7 1 1 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。S 2 1 0 で警告表示手段 7 2 4 がオペレーターに異常を検知し自動変更プログラム 7 1 2 2 によって構成が変更されたことを表示して知らせる。S 2 1 1 で警告表示手段 7 2 4 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。S 2 1 2 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 S 2 1 3 に移行（S 2 1 2 : Y E S）、必要でなければ S 2 1 4 に移行する（S 2 1 2 : N O）。S 2 1 3 ではオペレーターは構成の変更を必要と判断したため L A N 切り替え装置の手動変更プログラム 7 1 2 1 を実行し L A N 切り替え手段 7 1 1 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。S 2 1 4 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。

30

40

50

次に、S 2 1 4 ではフィールド機器監視装置 8 2 の監視手段 8 2 1 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 S 2 1 5 へ (S 2 1 4 : Y E S)、検知されなかった場合 S 2 2 3 へ進む (S 2 1 4 : N O)。異常状態か否かの判断は、監視手段 8 2 1 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。S 2 1 5 では警告表示手段 8 2 4 が監視手段 8 2 1 によって検知された異常をオペレーターに告げる。S 2 1 6 では監視装置 8 2 によって検知された異常状態が異常時切替判定手段 8 2 3 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 S 2 1 7 へ (S 2 1 6 : Y E S)、合致しなかった場合 S 2 2 0 へ進む (S 2 1 6 : N O)。S 2 1 7 で監視装置 8 2 の異常時切替判定手段 8 2 3 がフィールドバス切り替え装置 8 1 の自動変更プログラム 8 1 2 2 を動かす命令を送る。S 2 1 8 でフィールドバス切り替え装置 8 1 の自動変更プログラム 8 1 2 2 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 8 1 1 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。S 2 1 9 で警告表示手段 8 2 4 がオペレーターに異常を検知し自動変更プログラム 8 1 2 2 によって構成が変更されたことを表示して知らせる。S 2 2 0 で警告表示手段 8 2 4 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。S 2 2 1 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 S 2 2 2 に移行 (S 2 2 1 : Y E S)、必要でなければ S 2 2 3 に移行する (S 2 2 1 : N O)。S 2 2 2 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 8 1 2 1 を実行しフィールドバス切り替え手段 8 1 1 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。S 2 2 3 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。

10

20

【 0 0 2 5 】

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 7 1 2 2、8 1 2 2 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 7 1 2 1、8 1 2 1 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 7 1 2 1、8 1 2 1 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。

30

【 0 0 2 6 】

(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。

【 0 0 2 7 】

L A N 切り替え装置 7 1 のネットワーク構成変更手段 7 1 2 によって、ローカルコントローラ 5 4 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 S C A D A のみ、ハッカーによって侵入された端末が O P C サーバのみなど) S C A D A や O P C サーバ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。

40

【 0 0 2 8 】

L A N 分岐装置 7 3 とフィールドバス分岐装置 8 3 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 7 2 またはフィールド機器監視装置 8 2 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

50

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、

10

20

30

40

50

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に不正な命令を送った。LAN分岐装置73によって傍受された不正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

10

20

30

40

50

ーバー、ローカルコントローラ 5 4 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 S C A D A を操作して、フィールド機器 6 1 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 6 1 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

10

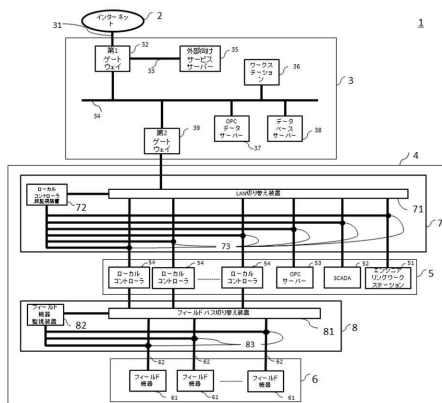
【符号の説明】

【 0 0 3 4 】

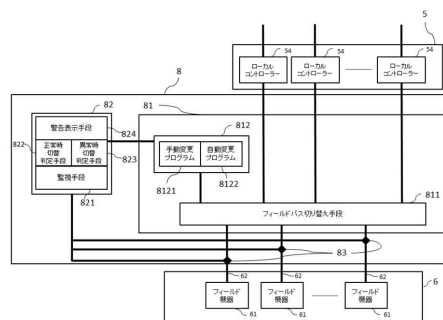
| | | |
|---------|-------------------|----|
| 1 | プラントシステム | |
| 2 | インターネット | |
| 3 | I T 系システム | |
| 4 | 制御系システム | |
| 5 | ローカルコントローラ群 | |
| 6 | フィールド機器群 | |
| 7 | L A N 切り替えシステム | 20 |
| 8 | フィールドバス切り替えシステム | |
| 9 | 正常時状態遷移表 | |
| 3 1 | 外部ネットワーク | |
| 3 2 | 第 1 ゲートウェイ | |
| 3 3 | 非武装地帯 | |
| 3 4 | 内部ネットワーク | |
| 3 5 | 外部向けサービスサーバー | |
| 3 6 | ワークステーション | |
| 3 7 | O P C データサーバー | |
| 3 8 | データベースサーバー | 30 |
| 3 9 | 第 2 ゲートウェイ | |
| 5 1 | エンジニアリングワークステーション | |
| 5 2 | S C A D A | |
| 5 3 | O P C サーバー | |
| 5 4 | ローカルコントローラ | |
| 6 1 | フィールド機器 | |
| 6 2 | フィールドバス | |
| 7 1 | L A N 切り替え装置 | |
| 7 2 | ローカルコントローラ群監視装置 | |
| 7 3 | L A N 分岐装置 | 40 |
| 8 1 | フィールドバス切り替え装置 | |
| 8 2 | フィールド機器監視装置 | |
| 8 3 | フィールドバス分岐装置 | |
| 7 1 1 | L A N 切り替え手段 | |
| 7 1 2 | ネットワーク構成変更手段 | |
| 7 1 2 1 | 手動変更プログラム | |
| 7 1 2 2 | 自動変更プログラム | |
| 7 2 1 | 監視手段 | |
| 7 2 2 | 正常時判定手段 | |
| 7 2 3 | 異常時判定手段 | 50 |

- 7 2 4 警告表示手段
- 8 1 1 フィールドバス切り替え手段
- 8 1 2 ネットワーク構成変更手段
- 8 1 2 1 手動変更プログラム
- 8 1 2 2 自動変更プログラム
- 8 2 1 監視手段
- 8 2 2 正常時判定手段
- 8 2 3 異常時判定手段
- 8 2 4 警告表示手段

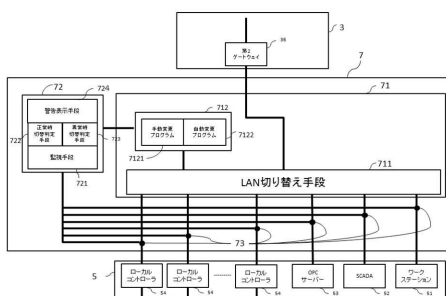
【図1】



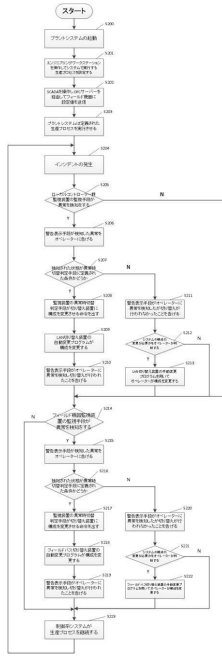
【図3】



【図2】



【図4】

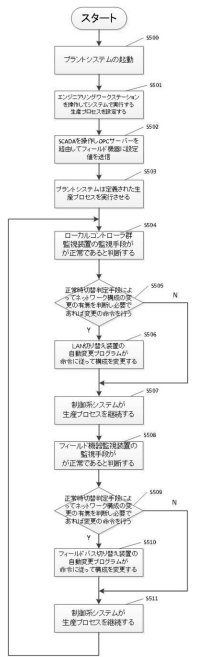


【図5】

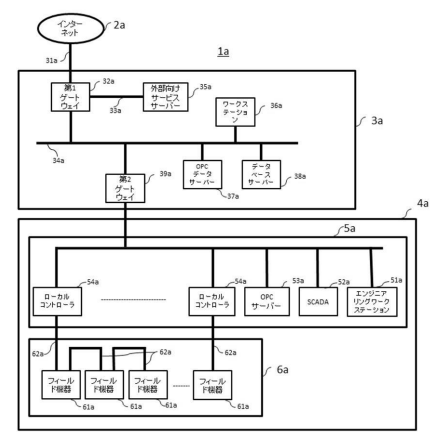
9

| 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 |

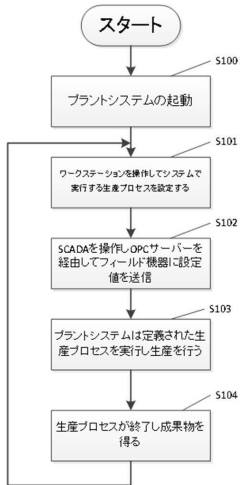
【図6】



【図7】



【図 8】



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

審査官 大石 博見

- (56)参考文献 特開2006-092166(JP,A)
特表平07-503345(JP,A)

- (58)調査した分野(Int.Cl., DB名)
- | | |
|------|-------|
| H04L | 12/28 |
| G05B | 23/02 |
| H04L | 12/46 |
| H04Q | 9/00 |