(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第6918791号
(P6918791)
(45)発行日　令和3年8月11日(2021.8.11)　(24)登録日　令和3年7月27日(2021.7.27)

(51)Int.Cl.　F I
*G05B 23/02 (2006.01)*　G05B 23/02 302T

請求項の数 26 (全 40 頁)

(21)出願番号　特願2018-518521(P2018-518521)
(86)(22)出願日　平成28年10月7日(2016.10.7)
(65)公表番号　特表2018-530077(P2018-530077A)
(43)公表日　平成30年10月11日(2018.10.11)
(86)国際出願番号　PCT/US2016/056024
(87)国際公開番号　WO2017/062787
(87)国際公開日　平成29年4月13日(2017.4.13)
審査請求日　令和1年10月7日(2019.10.7)
(31)優先権主張番号　62/239,657
(32)優先日　平成27年10月9日(2015.10.9)
(33)優先権主張国・地域又は機関
米国(US)

(73)特許権者　512132022
フィッシャー－ローズマウント　システムズ，インコーポレイテッド
アメリカ合衆国　テキサス　７８６８１－７４３０　ラウンド　ロック　ウェスト　ルイス　ヘナ　ブルバード　１１００　ビルディング　１　エマーソン　プロセス　マネージメント
(74)代理人　100113608
弁理士　平川　明
(74)代理人　100138357
弁理士　矢澤　広伸

最終頁に続く

(54)【発明の名称】原因結果マトリックスの安全論理を検証するためのシステム及び方法

(57)【特許請求の範囲】
【請求項１】
プロセスプラントのプロセス制御システムの構成を決定するコンピュータ実装の方法であって、前記プロセス制御システムが、一組の機能ブロックとして実装され、前記方法が、
前記一組の機能ブロックの各々について、（ｉ）前記機能ブロックの一組の出力、（ｉｉ）前記機能ブロックの論理、及び（ｉｉｉ）前記機能ブロックの一組の入力、に基づいて、前記機能ブロック構成を決定することと、
前記機能ブロック構成に基づいて、一組の試験原因及び一組の試験結果を有する試験原因結果マトリックス（ＣＥＭ）を発生させることであって、前記一組の試験原因及び前記一組の試験結果のうちの少なくともいくつかが、試験原因－結果の対として関連される、発生させることと、
入力としての一組の原因及び出力としての一組の結果を有する要求定義ＣＥＭにアクセスすることであって、前記一組の原因の各々が、前記プロセスプラント内の条件を表し、前記一組の結果の各々が、前記プロセスプラント内で行われるべき結果を表し、前記一組の原因及び前記一組の結果のうちの少なくともいくつかが、原因－結果の対として関連され、それによって、前記対応する条件の発生に応答して前記対応する結果を起動させる、アクセスすることと、
前記試験ＣＥＭと前記要求定義ＣＥＭとを比較して、一組の不一致が存在するかどうかを判定することと、を含む、コンピュータ実装の方法。

【請求項２】
前記一組の不一致が存在するとき、前記方法が、
前記一組の不一致をユーザインターフェースに表示することをさらに含む、請求項１に記載のコンピュータ実装の方法。
【請求項３】
前記ユーザインターフェースを介して、前記一組の不一致のうちの１つの不一致の選択を受信することと、
前記不一致に対応する複数の相互に接続された前記機能ブロックのうちの１つの機能ブロックを決定することと、
決定された前記機能ブロックの指示を前記ユーザインターフェースに表示することと、
をさらに含む、請求項２に記載のコンピュータ実装の方法。
【請求項４】
前記機能ブロック構成を決定することが、
前記機能ブロックの前記一組の出力を識別することと、
前記機能ブロックの前記一組の入力を識別することと、
前記機能ブロックの、前記機能ブロックの入力を前記機能ブロックの出力に変換する前記論理を決定することと、
を含む、請求項１から３のいずれか１項に記載のコンピュータ実装の方法。
【請求項５】
前記機能ブロック構成に基づいて、前記試験原因結果マトリックス（ＣＥＭ）を発生させることが、
複数の前記機能ブロックのうち第一のものの一組の入力を識別することと、
複数の前記機能ブロックのうち第二のものの一組の出力を識別することであって、複数の前記機能ブロックのうち前記第二のものの前記一組の出力の一つは、複数の前記機能ブロックのうち前記第一のものへの入力である、識別することと、
複数の前記機能ブロックのうち前記第一および前記第二のものの論理を結合して、複数の前記機能ブロックのうち前記第二のものの１または複数の前記入力から、複数の前記機能ブロックのうち前記第一のものの１または複数の前記出力に関する論理式を決定し、結合された論理を生成することと、
前記結合された論理を使って前記試験ＣＥＭの１または複数の原因と結果の組を決定することと、
を含む、請求項１から４のいずれか１項に記載のコンピュータ実装の方法。
【請求項６】
前記一組の機能ブロックが、一組の監視ブロック及び一組の結果ブロックを含む、請求項１から５のいずれか１項に記載のコンピュータ実装の方法。
【請求項７】
前記監視ブロックおよび前記結果ブロックが相互に接続する
請求項６に記載のコンピュータ実装の方法。
【請求項８】
前記機能ブロックの前記構成を決定することが、
前記機能ブロックの前記入力を前記機能ブロックの前記出力に変換するブーリアン論理を決定することを含む、
請求項１から７のいずれか１項に記載のコンピュータ実装の方法。
【請求項９】
前記試験ＣＥＭを発生させることが、
前記試験原因－結果の対で前記試験ＣＥＭをポピュレートすることを含む、請求項１から８のいずれか１項に記載のコンピュータ実装の方法。
【請求項１０】
前記機能ブロックの前記論理は、前記機能ブロックの前記一組の入力の少なくとも１つの前記入力と、前記機能ブロックの前記一組の出力の少なくとも１つの前記出力との間の

関係を示す数値表現として実装される、
請求項１から９のいずれか１項に記載のコンピュータ実装の方法。
【請求項１１】
プロセスプラントのプロセス制御システムの構成を決定するためのシステムであって、前記プロセス制御システムが、複数の相互に接続された機能ブロックとして実装され、該システムが、
（ｉ）一組のコンピュータ実行可能命令、及び（ｉｉ）一組の入力としての原因及び一組の出力としての結果を有する要求定義ＣＥＭを記憶するように構成されたメモリであって、前記一組の原因の各々が、前記プロセスプラント内の条件を表し、前記一組の結果の各々が、前記プロセスプラント内で行われるべき結果を表し、前記一組の原因及び前記一組の結果のうちの少なくともいくつかが、原因－結果の対として関連され、それによって、１または複数の対応する原因の発生に応答して前記対応する結果を起動させる、メモリと、
前記メモリとインターフェースされたプロセッサであって、前記一組のコンピュータ実行可能命令を実行して、前記プロセッサに、
相互に接続された複数の前記機能ブロックの各々について、（ｉ）前記機能ブロックの一組の出力、（ｉｉ）前記機能ブロックの論理、及び（ｉｉｉ）前記機能ブロックの一組の入力、に基づいて、前記機能ブロックの構成を決定させ、
前記機能ブロックの構成に基づいて、一組の入力としての試験原因及び一組の出力としての試験結果を有する、相互に接続された複数の前記機能ブロックの操作を定義する試験原因結果マトリックス（ＣＥＭ）を発生させ、前記一組の試験原因及び前記一組の試験結果のうちの少なくともいくつかが、前記試験ＣＥＭ内の試験原因－結果の対として関連され、
前記要求定義ＣＥＭにアクセスさせ、
前記試験ＣＥＭと前記要求定義ＣＥＭとを比較して、一組の不一致が存在するかどうかを判定させ、
ユーザに前記一組の不一致を通知するように構成される、プロセッサと、を備える、システム。
【請求項１２】
ユーザインターフェースをさらに備え、
前記一組の不一致が存在するときに、前記プロセッサが、
前記ユーザインターフェースに、前記一組の不一致を表示させるようにさらに構成される、請求項１１に記載のシステム。
【請求項１３】
前記プロセッサが、
前記ユーザインターフェースを介して、前記一組の不一致のうちの１つの不一致の選択を受信し、
前記不一致に対応する複数の相互に接続された前記機能ブロックのうちの１つの機能ブロックを決定し、そして、
前記ユーザインターフェースに、決定された前記機能ブロックの指示を表示させるようにさらに構成される、請求項１２に記載のシステム。
【請求項１４】
前記機能ブロックの構成を決定するために、前記プロセッサが、
前記機能ブロックの前記一組の出力を識別し、
前記機能ブロックの前記一組の入力を識別し、
前記機能ブロックの、前記機能ブロックの入力を前記機能ブロックの出力に変換する前記論理を決定するように構成される、請求項１１から１３のいずれか１項に記載のシステム。
【請求項１５】
前記一組の機能ブロックが、一組の監視ブロック及び一組の結果ブロックを含む、請求

項１１から１４のいずれか１項に記載のシステム。
【請求項１６】
前記機能ブロックの前記構成を決定するために、前記プロセッサが、
前記機能ブロックの前記入力を前記機能ブロックの前記出力に変換するブーリアン論理を決定するように構成される、請求項１１から１５のいずれか１項に記載のシステム。
【請求項１７】
前記試験ＣＥＭを発生させるために、前記プロセッサが、
前記試験原因－結果の対で前記試験ＣＥＭをポピュレートするように構成される、請求項１１から１６のいずれか１項に記載のシステム。
【請求項１８】
命令を記憶する非一時的コンピュータ可読媒体であって、該命令が、機械の１つ以上のプロセッサによって実行されたときに、前記機械に、
プロセスプラントのプロセス制御システムを実装する複数の相互に接続された機能ブロックの各々について、（ｉ）前記機能ブロックの一組の出力、（ｉｉ）前記機能ブロックの論理、及び（ｉｉｉ）前記機能ブロックの一組の入力、に基づいて、前記機能ブロックの構成を決定させ、
前記機能ブロックの構成に基づいて、一組の入力としての試験原因及び一組の出力としての試験結果を有する試験原因結果マトリックス（ＣＥＭ）を発生させ、前記一組の試験原因及び前記一組の試験結果のうちの少なくともいくつかが、試験原因－結果の対として関連され、
一組の原因及び一組の結果を有する要求定義ＣＥＭにアクセスさせ、前記一組の原因の各々が、前記プロセスプラント内の条件を表し、前記一組の結果の各々が、前記プロセスプラント内で行われるべき結果を表し、前記一組の原因及び前記一組の結果のうちの少なくともいくつかが、原因－結果の対として関連され、それによって、１または複数の前記対応する原因の発生に応答して前記対応する結果を起動させ、
前記試験ＣＥＭと前記要求定義ＣＥＭとを比較して、一組の不一致が存在するかどうかを判定させ、
ユーザに前記一組の不一致を通知する、
非一時的コンピュータ可読媒体。
【請求項１９】
プロセス制御システムの安全論理を検証するコンピュータ実装の方法であって、
前記プロセス制御システムの安全制御論理にアクセスすることであって、前記安全制御論理は一組の原因と一組の結果に基づいて制御を行い、各々の前記一組の原因はプロセスプラント内の状態を表し、各々前記一組の結果は前記プロセスプラント内で実行される結果を表し、前記一組の原因と前記一組の結果の少なくとも一部が原因－結果の組として関連付けられ、それにより、1または複数の対応する前記原因の発生に応じて対応する前記結果が起動され、前記安全制御論理は複数の相互に接続された機能ブロックとして実装され、複数の相互に接続された前記機能ブロックの各々は、一組の入力、一組の出力および、前記一組の入力を前記一組の出力に関連付ける機能ブロック論理を有し、複数の前記機能ブロックのうちの1つの機能ブロックの少なくとも1つの出力は、複数の前記機能ブロックのうちの少なくとも1つの他の機能ブロックへの入力として接続され、前記原因の各々は、複数の相互に接続された前記機能ブロックの少なくとも1つへの入力であり、前記結果の各々は、複数の相互に接続された前記機能ブロックの少なくとも1つの出力である、ことと、
前記安全制御論理の複数の前記機能ブロックに基づいて、一組の試験原因及び一組の試験結果を有する試験原因結果マトリックス（ＣＥＭ）を生成することであって、前記一組の試験原因および前記一組の試験結果は、試験の原因－結果の組として関連付けられる、ことと、
前記プロセス制御システムのメモリから要求定義ＣＥＭにアクセスすることであって、前記要求定義ＣＥＭは前記プロセス制御システムの前記安全制御論理を表現する、ことと

、
前記試験ＣＥＭと要求定義ＣＥＭを比較して、一組の不一致が存在するかどうかを判定することと、
を含む、コンピュータ実装の方法。
【請求項２０】
１つまたは複数の前記機能ブロックは、１つまたは複数の監視ブロックおよび１つまたは複数の結果ブロックを含み、前記１つまたは複数の監視ブロックの各々は、第１の組の入力、第１の組の出力、および監視ブロック論理を含み、前記１つまたは複数の結果ブロックの各々が、第２の組の入力、第２の組の出力、および結果ブロック論理を含み、前記安全制御論理が少なくとも1つの監視ブロックの監視ブロック論理内と、少なくとも１つの結果ブロックの結果ブロック論理内に分散される、
請求項１９に記載のコンピュータ実装の方法。
【請求項２１】
１つまたは複数の前記監視ブロックまたは前記結果ブロックは相互に接続されている
請求項２０に記載のコンピュータ実装の方法。
【請求項２２】
前記監視ブロックまたは前記結果ブロックのうちの１つまたは複数が、階層化、入れ子、ループ、または連鎖を介して相互に接続される、
請求項２１に記載のコンピュータ実装の方法。
【請求項２３】
前記試験ＣＥＭを生成するために、１つまたは複数の相互に接続された監視または結果ブロックを通過させること、をさらに含む
請求項２２に記載のコンピュータ実装の方法。
【請求項２４】
前記試験ＣＥＭを生成するために１つまたは複数の相互に接続された監視または結果ブロックを通過させることは、
第１の監視ブロックへの第１の入力を識別することと、
前記第１の監視ブロックの前記第１の入力に論理的に結合された前記第１の監視ブロックの第１の出力を識別することと、
第１の結果ブロックへの第２の入力を識別することであって、前記第１の結果ブロックへの前記第２の入力は、前記第１の監視ブロックの第１の出力に論理的に結合されることと、
前記第１の結果ブロックの前記第２の入力に論理的に結合された前記第１の結果ブロックの第２の出力を識別することと、
前記第1の監視ブロックの前記第1の入力を前記第1の結果ブロックの前記第2の出力に関連付ける論理式を決定して、結合された論理を生成することと、
前記結合された論理を使用して、前記試験ＣＥＭの1つまたは複数の原因と結果の組を決定することと、を含む、
請求項２３に記載のコンピュータ実装の方法。
【請求項２５】
前記要求定義ＣＥＭは、プロセスプラントが必要とする安全論理の正確な表現を定義するマトリックスである、
請求項１９から２４のいずれか１項に記載のコンピュータ実装の方法。
【請求項２６】
前記一組の不一致の各々の不一致について、
前記要求定義ＣＥＭに対応する原因－効果の組とは異なる前記試験ＣＥＭの原因－効果の組に対応する、複数の前記機能ブロックのうちの１つまたは複数の機能ブロックを識別することと、
識別された前記1つまたは複数の機能ブロックを表示することと、を含む
請求項１９から２５のいずれか１項に記載のコンピュータ実装の方法。

【発明の詳細な説明】
【技術分野】
【０００１】
関連出願
本特許出願は、２０１５年１０月９日に出願された「Ａ Ｓｙｓｔｅｍ ａｎｄ Ｍｅｔｈｏｄ ｆｏｒ Ｃｏｎｆｉｇｕｒｉｎｇ Ｓｅｐａｒａｔｅｄ Ｍｏｎｉｔｏｒ ａｎｄ Ｅｆｆｅｃｔ Ｂｌｏｃｋｓ ｏｆ ａ Ｐｒｏｃｅｓｓ Ｃｏｎｔｒｏｌ Ｓｙｓｔｅｍ」という名称の米国仮特許出願第６２／２３９，６５７号の出願日に対する優先権及び利益を主張する、正規の特許出願であり、参照により明示的に本明細書に組み込まれる。
【０００２】
本開示は、一般に、プロセスプラント内のプロセス制御システムを管理することに関し、より具体的には、プロセス制御システムと関連付けられた原因結果マトリックス（ＣＥＭ）を構成すること、及び該ＣＥＭに関連する監視ブロック及び結果ブロックを作成することに関する。
【背景技術】
【０００３】
化学、石油、または他のプロセスで使用されているようなプロセス制御システムは、典型的に、アナログ、デジタル、またはアナログ／デジタルバスもしくはラインを介して、少なくとも１つのホストもしくはオペレータワークステーションに、及び１つ以上のフィールドデバイスに通信的に結合された、１つ以上のプロセスコントローラを含む。例えば、弁、弁ポジショナ、スイッチ、及びトランスミッタ（例えば、温度、圧力、及び流量センサ）であり得るフィールドデバイスは、弁の開閉、及びプロセスパラメータの測定等のプロセスプラント内の機能を行う。プロセスコントローラは、フィールドデバイスによって作成されるプロセス測定値及び／またはフィールドデバイスに関する他の情報を示す信号を受信し、この情報を使用して制御ルーチンを実装し、次いで、制御信号を発生させ、該制御信号は、バスまたはラインを通じてフィールドデバイスに送信されて、プロセスの動作を制御する。フィールドデバイス及びコントローラからの情報は、典型的に、オペレータワークステーションによって実行される１つ以上のアプリケーションが利用できるようになり、オペレータが、プロセスを構成すること、プロセスの現在の状態を見ること、プロセスの動作を修正すること等の、プロセスに関する任意の所望の機能を行うことを可能にする。
【０００４】
加えて、多くのプロセスでは、毒性化学物質の漏洩、爆発等のプラント内の深刻な危険をもたらし得る、またはつながり得る問題が生じたときに、プロセスプラント内の重大な安全関連の問題を検出して、自動的に弁を閉じる、デバイスからの電力供給を停止する、プラント内の流れを切り換える等のために、別個の安全システムが提供される。これらの安全システムは、典型的に、標準的なプロセス制御コントローラとは別の、論理ソルバーと称される１つ以上の別個のコントローラを有し、該コントローラは、プロセス制御プラント内に設置された別個のバスまたは通信ラインを介して、安全なフィールドデバイスに接続される。論理ソルバーは、安全フィールドデバイスを使用して、特定の安全スイッチまたは遮断弁の位置、プロセスにおけるオーバーフローもしくはアンダーフロー、重要な発電もしくは制御デバイスの動作、障害検出デバイスの動作等の重要なイベントと関連付けられたプロセス条件を検出し、それによって、プロセスプラント内の「イベント」を検出する。単一の条件または２つ以上の条件の同時発生であり得るイベント（典型的に、「原因」と称される）が検出されると、安全コントローラは、弁を閉じる、デバイスをオフにする、プラントのセクションからの電力供給を停止する等の、イベントの有害な性質を制限するために、いくつかのアクション（典型的に、「結果」と称される）をとる。一般に、これらのアクションまたは結果は、安全デバイスを、プロセスプラント内の深刻なまたは危険な条件を防止するように設計された、トリップまたは「安全」動作モードに切り

換えることを含む。

【０００５】

マネージャ及びエンジニア等のプロセスプラントのオペレータは、典型的に、関連する原因結果を記憶するデータベース構造を維持する。例えば、マトリックスは、複数の行及び列を有することができ、各行は、原因に対応し、各列は、結果に対応し、また、マトリックスの各セルは、特定の原因結果関係に対応する。セルは、原因及び結果それぞれの関係を示す様々なトリガーによってポピュレートすることができる。いわゆる原因結果マトリックス（ＣＥＭ）は、一般に、制御システムまたはプラントの安全設計を定義する要求文書に従って構成される。制御エンジニアは、ＣＥＭを利用して、適宜に安全設計が実装されるように制御システムをエンジニアリングすることができる。しかしながら、そのようなＣＥＭは、マトリックスの定義されたサイズによって制限され、また、しばしば、全ての所望の原因／結果データの関係を扱うのに十分な大きさではない。さらに、そのようなＣＥＭは、連鎖化、リンク化、平準化、ループ化等のより複雑／精巧な原因／結果を扱うことができない。またさらに、大きいＣＥＭは、制御論理への実装が面倒であり、したがって、実装中にエラーを起こし易い。適切に動作させるための安全システムの故障は、プラント人員側の深刻な負傷、さらには死亡に、また、潜在的に数百万ドルのプラント内の設備及び材料の破壊につながる可能性があるので、ＣＥＭにおけるエラーは深刻になり得るため、安全システムでは、正確なＣＥＭを維持することが必須である。

【発明の概要】

【０００６】

プロセスプラントのプロセス制御システムは、原因結果マトリックス（ＣＥＭ）において定義された制御論理を達成するように実装または設計することができる安全システムを有することができ、ＣＥＭは、視覚表現で表示される、プロセスプラントの安全アクションの概要である。全般的に言えば、ＣＥＭは、プロセスプラント内の様々な安全プロトコルまたはプロシージャの基本的な原因結果関係を定義する。一般に、ＣＥＭは、一組の入力と、一組の出力とを含むことができ、一組の入力の各々は、プロセスプラント内の条件を表し、一組の出力の各々は、プロセスプラント内で行われるべき結果またはアクションを表す。さらに、一組の入力及び一組の出力のうちの少なくともいくつかは、原因－結果の対として関連され、それによって、対応する結果のアクティビティが、対応する条件または原因の発生に応答する。

【０００７】

プロセス制御システムの管理者は、一組の様々な機能ブロックとしてＣＥＭを実装することができる。しかしながら、プロセスプラントの規模及び／または複雑さに応じて、所与のＣＥＭは、多数の原因、結果、及び原因－結果の対を含む場合があり、したがって、対応する大量の機能ブロックを実装することが必要になり得る。したがって、この実装は、時間がかかり、複雑で、面倒になる可能性があり、潜在的な実装エラーにつながる。説明されるシステム及び方法によれば、監視機能ブロック及び結果機能ブロックとしてＣＥＭ論理を実装するように説明される、分離されているが相互接続されている一組の機能ブロックとして、ＣＥＭをプロセス制御システム内に実装するための様々な技術が提供される。

【０００８】

１つの実施形態において、システム及び方法は、ＣＥＭ内のパターン及びグルーピングを識別することができ、また、識別したパターン及びグルーピングに従って一組の監視ブロック及び一組の結果ブロックを実装することができ、したがって、ＣＥＭの実装の複雑さを低減する。一実装例において、ＣＥＭ内のデータのグルーピング（例えば、ＣＥＭの列）は、ＣＥＭのその一部分によって定義される論理の数値表現として定義して、ＣＥＭ論理を実装するために使用される機能ブロック（例えば、監視及び結果ブロック）内にＣＥＭの論理が実装されることを理解し、検証する、簡単であまり複雑でない様態を提供することができる。またさらに、ＣＥＭ（例えば、ＣＥＭの行及び／または列）を分析し、かつ再順序付けまたは再配設して、より良好な、より論理的な、より容易に実装される、

等の、一組以上の原因結果ブロックとして実装されるＣＥＭ論理のグルーピングを提供するために、ツールを使用することができる。

【０００９】

本開示は、ＣＥＭを管理するための追加的な技術を提供する。具体的には、本明細書で説明されるシステム及び方法は、ＣＥＭがインタラクティブ機能を含むように構成するために使用することができる。例えば、構成されたＣＥＭは、ＣＥＭの原因結果関係を構成する安全プロトコルを詳述する１つ以上の文書にアクセスするリンクもしくは選択肢、プラントに実装されたときにユーザが特定の結果に関する以前の条件もしくは動作をより容易に理解することを可能にするための、ＣＥＭの１つ以上の結果の現在及び／もしくは過去の状態を表すグラフ、ならびにＣＥＭの原因結果に関連するデバイスを含むプロセスプラントの図を含むことができる。

【００１０】

加えて、ＣＥＭに含まれるしばしば大量の情報のため、エンジニアは、プロセス制御システムに含まれる任意の不一致またはエラーを識別することが困難であり得る。本明細書で提供されるシステム及び方法は、さらに、リバースエンジニアリング技術及びシステムを実装して、デバイスによって実際に実装されるＣＥＭ論理、及びプロセスプラントの制御論理（またはいくつかの実装例において、プロセス制御システム内の監視及び結果ブロック）を定義する試験ＣＥＭ、ならびに特定のプロセスプラントのための必要な安全プロトコルを自動的に作成することを可能にする。故に、本明細書で説明されるシステム及び方法は、試験ＣＥＭと既存のＣＥＭとを比較して、プラント動作の実際の構成と設計文書に詳述され得る構成との間の任意の不一致またはエラーを識別することができる。

【図面の簡単な説明】

【００１１】

下で説明される図は、開示されるシステム及び方法の様々な態様をその中に表す。各図は、開示されるシステム及び方法の特定の態様の一実施形態を表すこと、及び図の各々は、その可能な実施形態と一致することを意図することを理解されたい。さらに、可能な限り、以下の説明は、以下の図に含まれる参照番号を参照し、複数の図面において表される特徴は、一貫した参照番号で示される。

【００１２】

図面には、現在論じられている配設が示されるが、本実施形態は、示される正確な配設及び手段に限定されないことを理解されたい。

【００１３】

【図１】例示的なプロセスプラントのブロック図である。

【図２】図１に概略的に例示される例示的なワークステーションのブロック図である。

【図３】例示的な原因結果マトリックスの説明図である。

【図４】例示的な一組の監視及び結果ブロックの説明図である。

【図５】監視及び結果ブロックを実装するために使用することができる一組の機能ブロックの第１の実施例の説明図である。

【図６】監視及び結果ブロックを実装するために使用することができる一組の機能ブロックの第２の実施例の説明図である。

【図７】プロセスプラントと関連付けられた監視ブロック及び結果ブロックを構成する例示的な方法のフロー図である。

【図８】原因結果マトリックスの第２の実施例の説明図である。

【図９】別個の論理ブロックに再編成され、構成された図８の原因結果マトリックスの第２の実施例の説明図である。

【図１０】原因結果マトリックスを再編成する例示的な方法のフロー図である。

【図１１】例示的な数値表現を有する原因結果マトリックスの第２の実施例の説明図である。

【図１２】原因結果マトリックス論理の数値表現を算出する例示的な方法のフロー図である。

【図１３】原因結果マトリックスの安全論理に対応する様々なインターリンクされたユーザインターフェースの例示的な説明図である。
【図１４】図１３のインターリンクされたユーザインターフェース間をナビゲートするための例示的な方法のフローチャートである。
【図１５】試験原因結果マトリックスをリバースエンジニアリングするための例示的な方法のフローチャートである。
【図１６Ａ】監視される安全イベントを表示する例示的なユーザインターフェースの説明図である。
【図１６Ｂ】監視される安全イベントを表示する例示的なユーザインターフェースの説明図である。
【図１６Ｃ】監視される安全イベントを表示する例示的なユーザインターフェースの説明図である。
【図１６Ｄ】監視される安全イベントを表示する例示的なユーザインターフェースの説明図である。
【図１７】監視される安全イベントを表示するための例示的な方法のフローチャートである。
【図１８】許容及び時間遅延トリガーを含む例示的な原因結果マトリックスの説明図である。
【００１４】
図面は、単に例示の目的で、好ましい実施形態を表す。当業者は、本明細書で説明される本発明の原理を逸脱することなく、本明細書で例示されるシステム及び方法の代替の実施形態が用いられ得ることを、以下の議論から容易に認識するであろう。
【発明を実施するための形態】
【００１５】
図１は、１つ以上のノード１２、１６、１８、及び２０を含む、例示的なプロセスプラント１０のブロック図である。図１の例示的なプロセスプラント１０において、ノード１２及び１６の各々は、例えばＦｏｕｎｄａｔｉｏｎ　Ｆｉｅｌｄｂｕｓインターフェース、ＨＡＲＴインターフェース等とすることができる入力／出力（Ｉ／Ｏ）デバイス２４を介して、１つ以上のフィールドデバイス２２及び２３に接続されたプロセスコントローラ１２ａ、１６ａを含む。コントローラ１２ａ及び１６ａはまた、例えば、１つ以上のバス、イーサネットローカルエリアネットワーク（ＬＡＮ）等の有線ＬＡＮ、無線ＬＡＮ、ワイドエリアネットワーク（ＷＡＮ）、インターネット等を備えることができるネットワーク３０を介して、ノード１８及び２０の１つ以上のホストまたはオペレータワークステーション１８ａ及び２０ａにも結合される。コントローラノード１２、１６、ならびに該コントローラノードと関連付けられたＩ／Ｏデバイス２４及びフィールドデバイス２２、２３は、典型的に、あるときには過酷なプラント環境内の下流に位置付けられ、該プラント環境を通して分配され、オペレータワークステーションノード１８及び２０は、通常、コントローラ人員によって容易に評価することができる、制御室内または他のあまり過酷でない環境内に位置付けられる。
【００１６】
全般的に言えば、ノード１８及び２０のワークステーション１８ａ及び２０ａは、プロセスプラント１０を構成し、監視するために、ならびに／またはプロセスプラント１０のデバイス２２、２３、２４及びコントローラ１２ａ、１６ａを管理するために使用されるアプリケーションを記憶し、実行するために使用することができる。例えば、ワークステーション１８ａ及び／または２０ａは、システムナビゲータアプリケーション１５、原因結果分析器ツール１７、プロセス制御構成アプリケーション１９、及びプロセスプラント１０の安全要求を管理するために実装することができる安全構成アプリケーション２１等のツールを含むことができる。システムナビゲータアプリケーション１５は、プロセスプラントの安全要求及びデバイスに関する情報を提供する、ユーザインターフェースのインターリンクされたグループを提供するように実装することができる。原因結果分析器ツー

ルは、原因結果マトリックス（ＣＥＭ）を管理するように、及び／または既知の安全要求及び／または機能ブロックからリバースエンジニアリングすることによって原因結果マトリックスを作成するように実装することができる。さらに、プロセス制御構成アプリケーション１９及び安全構成アプリケーション２１は、ワークステーション１８ａ及び／または２０ａを通してプロセスプラントのデバイスを管理する能力をユーザに提供する。構成データベース３２は、ネットワーク３０に接続することができ、また、ノード１２、１６、１８、２０にダウンロードされ、及び／または該ノード内に記憶されたときに、プロセスプラント１０の現在の構成を記憶する、データヒストリアン及び／または構成データベースとして動作することができる。構成データベースはまた、ＣＥＭを再配設するための規則３１、及び／または数値表現３３を含むこともできる。

【００１７】

一例としてＥｍｅｒｓｏｎ　Ｐｒｏｃｅｓｓ　Ｍａｎａｇｅｍｅｎｔによって販売されるＤｅｌｔａＶ（商標）コントローラとすることができる、コントローラ１２ａ及び１６ａの各々は、いくつかの異なる、独立して実行される制御モジュールまたはブロック使用して制御ストラテジを実装するコントローラアプリケーションを記憶し、実行することができる。制御モジュールは、それぞれ、一般に機能ブロックと称されるもので構成することができ、各機能ブロックは、制御ルーチン全体の一部またはサブルーチンであり、また、（リンクと呼ばれる通信を介して）他の機能ブロックと連動して、プロセスプラント１０内のプロセス制御ループを実装するように動作する。よく知られているように、機能ブロックは、典型的に、（トランスミッタ、センサ、または他のプロセスパラメータ測定デバイス等と関連付けられた）入力機能、（ＰＩＤ、ファジー論理等の制御を行う制御ルーチン等と関連付けられた）制御機能、または（弁等の）いくつかのデバイスの動作を制御する出力機能、のうちの１つを行って、プロセスプラント１０内のいくつかの物理理的機能を行う。当然ながら、ハイブリッド及び他のタイプの機能ブロックが存在し、利用することができる。フィールドバスプロトコル及びＤｅｌｔａＶ（商標）システムプロトコルは、オブジェクト指向プログラミングプロトコルで設計され、実装された制御モジュール及び機能ブロックを使用することができるが、制御モジュールは、例えばシーケンシャル機能ブロック、ラダーロジック等の任意の所望の制御プログラミングスキームを使用して設計することができ、また、機能ブロックまたは任意の他の特定のプログラミング技術を使用して設計されることに限定されない。典型的であるように、プロセス制御ノード１２及び１６内に記憶したときの制御モジュールの構成は、ワークステーション１８ａ及び２０ａによって実行されるアプリケーションにアクセスすることができる構成データベース３２に記憶することができる。機能ブロックは、例えばコントローラ１２ａ、１６ａに記憶され、それによって実行することができ、これは典型的に、これらの機能ブロックが、標準的な４～２０ｍＡデバイス、及びＨＡＲＴデバイス等のいくつかのタイプのスマートフィールドデバイスに使用されるときに、または該デバイスと関連付けられるときに当てはまり、または該機能ブロックは、フィールドデバイス自体に記憶し、それによって実装することができ、これは、フィールドバスデバイスの場合に当てはまり得る。

【００１８】

図１に例示されるシステムにおいて、コントローラ１２ａ及び１６ａに結合されたフィールドデバイス２２及び２３は、標準的な４～２０ｍＡデバイスとすることができ、またはプロセッサ及びメモリを含む、ＨＡＲＴ、Ｐｒｏｆｉｂｕｓ、もしくはＦｏｕｎｄａｔｉｏｎフィールドバスフィールドデバイス等の、スマートフィールドデバイスとすることができる。Ｆｏｕｎｄａｔｉｏｎフィールドバスフィールドデバイス等の（図１において参照番号２３が付される）これらのデバイスのうちのいくつかは、コントローラ１２ａ及び１６ａに実装された制御ストラテジと関連付けられた、機能ブロック等のモジュールまたはサブモジュールを記憶し、実行することができる。当然ながら、フィールドデバイス２２、２３は、センサ、弁、トランスミッタ、ポジショナ等の任意のタイプのデバイスとすることができ、Ｉ／Ｏデバイス２４は、ＨＡＲＴ、Ｆｏｕｎｄａｔｉｏｎフィールドバス、Ｐｒｏｆｉｂｕｓ等の任意の所望の通信またはコントローラプロトコルに準拠する任

意のタイプのＩ／Ｏデバイスとすることができる。

【００１９】

コントローラ１２ａ及び１６ａは、それぞれ、メモリに記憶された１つ以上のプロセス制御ルーチンを実装または監督するプロセッサを含み、該プロセス制御ルーチンは、その中に記憶された、または別様にはそれと関連付けられた制御ループを含むことができる。コントローラ１２ａ及び１６ａは、フィールドデバイス２２、２３、ワークステーション１８ａ、２０ａ、及びデータベース３２と通信して、任意の所望の様式でプロセスを制御する。コントローラ１２ａ及び１６ａは、それぞれ、任意の所望の様態で制御ストラテジまたは制御ルーチンを実装するように構成することができる。

【００２０】

プロセスプラント１０はまた、プロセス制御ノード１２及び１６と統合された安全システム１４（破線で示す）も含むことができる。安全システム１４は、一般に、プロセス制御ノード１２及び１６によって提供される制御を監視し、オーバーライドして、プロセスプラント１０の適切な安全動作を最大にするために、安全計装システム（ＳＩＳ）として動作させることができる。

【００２１】

ノード１２及び１６の各々は、１つ以上の安全システム論理ソルバー５０を含むことができる。論理ソルバー５０の各々は、プロセッサ及びメモリを有するＩ／Ｏデバイスであり、また、メモリに記憶した安全論理モジュールを実行するように構成される。各論理ソルバー５０は、安全システムフィールドデバイス６０及び６２に制御信号を提供し、及び／またはそれらから信号を受信するように通信的に結合される。加えて、ノード１２及び１６の各々は、少なくとも１つのメッセージ伝達デバイス（ＭＰＤ）７０を含むことができ、該ＭＰＤは、リングまたはバス接続７４（図１にはその一部のみが例示される）を介して、他のＭＰＤ７０に通信的に結合される。安全システム論理ソルバー５０、安全システムフィールドデバイス６０及び６２、ＭＰＤ７０、ならびにバス７４は、一般に、図１の安全システム１４を構成する。

【００２２】

図１の論理ソルバー５０は、プロセッサと、メモリとを含む任意の所望のタイプの安全システム制御デバイスとすることができ、該メモリは、プロセッサに対して実行して、フィールドデバイス６０及び６２を使用する安全システム１４と関連付けられた制御機能を提供するように適合された安全論理モジュールを記憶する。当然ながら、安全フィールドデバイス６０及び６２は、上で述べたもの等の、任意の既知の、または所望の通信プロトコルに準拠する、またはそれを使用する、任意の所望のタイプのフィールドデバイスとすることができる。具体的には、フィールドデバイス６０及び６２は、因習的に別個の専用の安全関連の制御システムによって制御されるタイプの安全関連のフィールドデバイスとすることができる。図１に例示されるプロセスプラント１０において、安全フィールドデバイス６０は、ＨＡＲＴまたは４～２０ｍＡプロトコル等の専用の、またはポイントツーポイントの通信プロトコルを使用するように表されおり、一方で、安全フィールドデバイス６２は、Ｆｉｅｌｄｂｕｓプロトコル等のバス通信プロトコルを使用するように表される。安全フィールドデバイス６０は、遮断弁、遮断スイッチ等の機能等の、任意の所望の機能を行うことができる。しかしながら、安全システムフィールドデバイス６０及び６２は、他のタイプのデバイスとすることができ、また、任意の所望の有線または無線通信プロトコルを含む、論理ソルバー５０と通信する他のタイプの通信プロトコルを使用することができる。

【００２３】

ノード１２及び１６の各々において共通のバックプレーン（図示せず）を使用して、コントローラ１２ａ及び１６ａを、プロセス制御Ｉ／Ｏカード２４、安全論理ソルバー５０、及びＭＰＤ７０に通信的に結合することができる。コントローラ１２ａ及び１６ａはまた、ネットワーク３０にも通信的に結合される。コントローラ１２ａ及び１６ａ、Ｉ／Ｏデバイス２４、論理ソルバー５０、ＭＰＤ７０は、ネットワーク３０を介して、ノード１

８及び２０と通信することができる。

【００２４】

当業者によって理解されるように、ノード１２、１６のバックプレーン（図示せず）は、論理ソルバー５０が互いにローカルに通信して、これらのデバイスによって実装される安全機能を協調させること、データを互いに通信すること、及び／または他の統合機能を行うことを可能にする。同様に、ノード１６のバックプレーン（図示せず）は、論理ソルバー５０が互いにローカルに通信して、これらのデバイスによって実装される安全機能を協調させること、データを互いに通信すること、及び／または他の統合機能を行うことを可能にする。一方で、ＭＰＤ７０は、プロセスプラント１０の非常に異なる場所に配置された安全システム１４の一部分が、依然として、互いに通信して、プロセスプラント１０の異なるノードにおいて、協調させた安全動作を提供することを可能にする。具体的には、ＭＰＤ７０は、バス７４と連動して、プロセスプラント１０の異なるノード１２及び１６と関連付けられた論理ソルバー５０が、共に通信的にカスケードされて、指定された優先度に従ってプロセスプラント１０内の安全関連の機能をカスケードできるようにすることを可能にする。ＭＰＤ７０及びバス７４は、ネットワーク３０の代替となる通信リンクを安全システムに提供する。

【００２５】

代替的に、プロセスプラント１０内の異なる場所の２つ以上の安全関連の機能は、ＭＰＤ７０及び通信ライン７４の使用を通してプラント１０の別個の領域またはノード内の個々の安全フィールドデバイスまで専用のラインを引くことを必要とすることなく、インターロックまたは相互接続することができる。換言すれば、ＭＰＤ７０及びバス７４の使用は、安全エンジニアが、事実上プロセスプラント１０全体を通して分配されるが、異なる安全関連のハードウェアが必要に応じて互いに通信することを可能にするように通信的に相互接続された該ハードウェアの異なる構成要素を有する、安全システム１４を設計し、構成することを可能にする。この特徴はまた、追加的な安全論理ソルバーが必要とされたときに、または新しいプロセス制御ノードがプロセスプラント１０に加えられたときに、該追加的な安全論理ソルバーを安全システム１４に追加することを可能にするという点で、安全システム１４のスケーラビリティも提供する。論理ソルバー５０は、典型的に、１つ以上の原因結果マトリックス（ＣＥＭ）によって定義される安全論理を実装する制御論理を含むことが理解されるであろう。

【００２６】

図２は、例示的なワークステーション１８ａ（ワークステーション２０ａは、同じまたは類似のデバイスを備えることができる）の構造を概略的に例示するブロック図である。ワークステーション１８ａは、少なくとも１つのプロセッサ１００と、揮発性メモリ１０４と、不揮発性メモリ１０８とを含むことができる。揮発性メモリ１０４は、例えば、ランダムアクセスメモリ（ＲＡＭ）を含むことができる。いくつかの実施形態において、ＲＡＭは、停電が生じた場合にデータが失われないように、１つ以上のバッテリによってバックアップすることができる。不揮発性メモリ１０８は、例えば、ハードディスク、リードオンリーメモリ（ＲＯＭ）、コンパクトディスクＲＯＭ（ＣＤ－ＲＯＭ）、プログラマブルＲＯＭ（ＰＲＯＭ）、消去可能プログラマブルＲＯＭ（ＥＰＲＯＭ）、電気的消去可能プログラマブルＲＯＭ（ＥＥＰＲＯＭ）、デジタル多用途ディスク（ＤＶＤ）、フラッシュメモリ等のうちの１つ以上を含むことができる。ワークステーション１８ａはまた、ワークステーションＩ／Ｏデバイス１１２も含むことができる。プロセッサ１００、揮発性メモリ１０４、不揮発性メモリ１０８、及びワークステーションＩ／Ｏデバイス１１２は、アドレス／データバス１１６を介して相互接続することができる。ワークステーション１８ａはまた、少なくとも１つの表示デバイス１２０及び少なくとも１つのユーザ入力デバイス１２４も含むことができ、これらは、例えば、キーボード、キーパッド、マウス、トラックボール、タッチスクリーン、ライトペン等のうちの１つ以上とすることができる。いくつかの実施形態において、揮発性メモリ１０４、不揮発性メモリ１０８、及びワークステーションＩ／Ｏデバイス１１２のうちの１つ以上は、別個のバスを介してアドレ

ス／データバス１１６（図示せず）からプロセッサ１００に結合することができ、または直接プロセッサ１００に結合することができる。

【００２７】

表示デバイス１２０及びユーザ入力デバイス１２４は、ワークステーションＩ／Ｏデバイス１１２と結合される。加えて、ワークステーション１８ａは、ワークステーションＩ／Ｏデバイス１１２を介して、ネットワーク３０に結合される。ワークステーションＩ／Ｏデバイス１１２は、図２において１つのデバイスとして例示されているが、複数のデバイスを備えることができる。加えて、いくつかの実施形態において、表示デバイス１２０及びユーザ入力デバイス１２４のうちの１つ以上は、アドレス／データバス１１６に、またはプロセッサ１００に直接結合することができる。

【００２８】

以下、図１及び２を参照すると、制御ノード１２及び１６のうちの１つ以上と関連付けられたプロセス制御構成アプリケーション１９は、１つ以上のワークステーション１８ａ及び２０ａに記憶され、それらによって実行することができる。例えば、プロセス制御構成アプリケーション１９は、不揮発性メモリ１０８及び／または揮発性メモリ１０４に記憶され、プロセッサ１００によって実行することができる。しかしながら、所望であれば、このアプリケーションは、プロセスプラント１０と関連付けられた他のコンピュータに記憶され、実行することができる。全般的に言えば、プロセス制御構成アプリケーション１９は、プログラマ、制御エンジニア、または他の人員が、コントローラ１２ａ、１６ａ、Ｉ／Ｏデバイス２４、及び／またはフィールドデバイス２２、２３によって実装される制御ルーチン、制御モジュール、機能ブロック、プログラム、論理等を作成し、構成することを可能にする。これらの制御ルーチン、制御モジュール、機能ブロック、プログラム、論理等は、次いで、ネットワーク３０を介して、コントローラ１２ａ、１６ａ、Ｉ／Ｏデバイス２４、及び／またはフィールドデバイス２２、２３のうちの適切なものにダウンロードすることができる。

【００２９】

同様に、安全システム１４と関連付けられた安全システム構成アプリケーション２１は、ワークステーション１８ａ及び２０ａのうちの１つ以上に記憶され、それらによって実行することができる。例えば、安全システム構成アプリケーション２１は、不揮発性メモリ１０８及び／または揮発性メモリ１０４に記憶され、プロセッサ１００によって実行することができる。しかしながら、所望であれば、このアプリケーションは、プロセスプラント１０と関連付けられた他のコンピュータに記憶され、実行することができる。全般的に言えば、安全システム構成アプリケーションは、プログラマ、安全エンジニア、または他の人員が、論理ソルバー５０及び／またはデバイス６０、６２によって実装される安全関連の制御ルーチン、安全論理モジュール、機能ブロック、プログラム、論理等を作成し、構成することを可能にする。これらの制御ルーチン、安全モジュール、機能ブロック、プログラム、論理等は、次いで、ネットワーク３０を介して、コントローラ１２ａ、１６ａ、論理ソルバー５０、及び／またはフィールドデバイス６０、６２のうちの適切なものにダウンロードすることができる。

【００３０】

安全システムは、典型的に、国際電気標準会議（ＩＥＣ）６１１３１－３規格によって定義されたいくつかの言語のうちの１つでプログラムされ、いくつかの事例において、安全論理は、一連の相互接続された機能ブロックまたは他のルーチンで構成することができる。プログラミング言語に関係なく、開始点は、通常、制御及び／または安全アクションの要求を指定する注釈文書である。安全システムにおいて、安全要求は、安全要求仕様（ＳＲＳ）に文書化されている。下でさらに詳細に説明されるＳＲＳは、プレーンテキスト、論理図、または特性要因図（原因結果マトリックスとも呼ばれる）のいずれかによって表すことができる論理記述を提供することができる。原因結果マトリックス（ＣＥＭ）は、単純な視覚的表現で安全システムによって提供される安全アクションの概要である。したがって、ＣＥＭは、安全論理によって実装される基本的な原因結果関係を定義し、また

、安全論理を構成するためのベースである。

【００３１】

図３は、任意のタイプの表示デバイスを介して表示することができる、ＣＥＭ３００の１つの例示的な表現を例示する。具体的には、表示デバイスは、安全構成アプリケーション２１と関連付けられたユーザインターフェースの一部とすることができ、表示は、例えばワークステーション１８ａの表示デバイス１２０を介して、プログラマまたは管理者に提示することができる。従来のプロセス制御システムにおいて利用することができるＣＥＭである例示的なＣＥＭ３００は、複数の原因及び複数の結果を含む。ＣＥＭの原因は、一般に、安全要求仕様によって定義され、また、プロセスプラント１０の全体を通して、論理ソルバー５０、フィールドデバイス２２、２３、６０、及び６２等によって、またはそれらにおいて示される、測定される、または検出される条件に関連する。ＣＥＭ３００において定義される異なる原因Ｃ１、Ｃ２等は、ＣＥＭ３００の各行と関連付けられる。例えば、１つの原因は、プラントの特定の領域の温度が安全または予め定義された範囲外である、センサ示度であり得る。

【００３２】

原因に対応する条件が生じたときに、結果をトリガーすることができ、結果は、プラントで行われるべきアクションとすることができる。ＣＥＭ３００の異なる結果Ｅ１、Ｅ２等は、ＣＥＭ３００の各列について定義され、かつ該列と関連付けられる。例えば、ＣＥＭ３００の１つの結果（例えば、Ｅ３）は、弁を閉じる、アラームを鳴らす等の、プラントで行われるべき安全アクションに関連させることができる。特定の原因（例えば、Ｃ２またはＣ６）が特定の結果（Ｅ３）をトリガーしたときには、対応する原因結果の対または関係が存在する。

【００３３】

ＣＥＭ３００において、原因結果関係は、各セルにおいて「Ｘ」で示され、これは、セルの行と関連付けられた原因によって、セルの列と関連付けられた結果がトリガーされることを示す。これらの関係は、本明細書で原因－結果の対と称することができる。代替の実装例において、セルは、関連付けられた原因結果をどのように関連させることができるのかをより正確に示す、様々な「トリガー」によってポピュレートすることができる。例えば、トリガーは、原因を受信した場合に即時に結果が起動されることを示す「Ｘ」、原因を受信した場合に、時間遅延を伴って結果が起動される「Ｔ」、原因を受信した場合に結果を許容することを示す「Ｐ」、等の形態とすることができる。さらに、空白セルは、特定の原因／結果の対がマトリックスにおいて現在関連していないことを示すことができ、したがって、プラントにおいて起動し得ない（すなわち、原因の発生が、いかなる結果とのトリガー関係も有しない）。

【００３４】

例示的なＣＥＭ３００は、７×７のマトリックスであり、これは、プロセスプラントの典型的な原因結果マトリックスよりも小さくなり得るが、例示のために単純な形態で示される。例示的なＣＥＭ３００は、一組の対応するセルの各々において「Ｘ」で示される１０個の原因／結果関係を含む。例えば、原因２（Ｃ２）は、結果３、４、及び５（Ｅ３、Ｅ４、及びＥ５）にそれぞれ対応する各セルに「Ｘ」を含む。したがって、原因２（Ｃ２）の関連付けられたイベントが生じた場合、結果３、４、及び５（Ｅ３、Ｅ４、及びＥ５）のそれぞれのアクションは、プラントの安全論理モジュールによって、プロセスプラント内でトリガーすることができる。しかしながら、いくつかの実施形態において、結果３、４、及び５の各々はまた、トリガーされる前に、他の関連付けられた原因が生じることも必要とし得る。例えば、システムで使用される論理に応じて、結果４は、結果４がトリガーされる前に（すなわち、結果４が、原因２、３、４、及び５の各々について「Ｘ」を有するので）、原因２、３、４、及び／または５のうちの１つ以上を起動することを必要とし得る。したがって、ＣＥＭによって定義される論理は、「ＯＲ」論理（すなわち、結果列における任意の１つの原因の発生が、結果の開始をもたらす）に基づくことができ、または「ＡＮＤ」論理（すなわち、安全論理によって結果がトリガーされる前に、結果列

にあらゆる原因が存在しなければならない）に基づくことができる。

【００３５】

別の実施形態において、結果（結果４等）は、どの原因が生じるのかに依存する、異なる様態でトリガーすることができる。例えば、１つの関連付けられた原因が生じた場合は、結果（結果４等）を遅延してトリガーすることができ、一方で、２つ以上の関連付けられた原因が生じた場合は、結果（結果４等）を即時にトリガーすることができる。さらに、いくつかの関連付けられた原因は、自動トリガーを起動させることができ、一方で、他の原因は、結果４等の結果の遅延トリガーを起動させることができる。さらにまた、いくつかの関連付けられた原因は、他の関連付けられた原因とは独立に結果をトリガーすることができ、一方で、他の関連付けられた原因は、それらが１つ以上の他の原因と組み合わせて存在するときにのみ結果をトリガーすることができる。提供される実施例は、限定することを意図するものではなく、対応する原因結果の対によって、論理及び／または遅延の任意の組み合わせを実装することができる。

【００３６】

より詳細に論じられるように、ＣＥＭによって定義される論理は、ＣＥＭによって定義される原因結果のサブセットに実装される、多数の一組またはグループの論理に分けることができ、これらの論理の異なるサブセットは、安全論理実装の特定の機能ブロックによって実装することができる。例えば、機能ブロックは、ＣＥＭ３００に例示される選択された論理ブロック３０５及び３１０によって定義される論理を実装するために使用することができる。この事例において、論理ブロック３０５は、２つの原因入力（Ｃ２及びＣ３）を含み、また、３つの結果出力（Ｅ３、Ｅ４、及びＥ５）に対応する。この例示的な実施形態において、論理ブロック３０５及び３１０によって実装される論理のサブセットは、単に、ＣＥＭ３００のポピュレートされたセルのクラスタを認識することによって識別される。ここで、論理ブロック３０５及び３１０は、ＣＥＭ３００の４９個のセルのうちの１２個のみをカバーしている間、ＣＥＭ３００によって示される重要な情報（原因／結果関係）の大部分を含む。他の実施形態において、論理ブロック３０５及び３１０は、より大きくして、及び／または別の論理ブロックの論理を加えて、または識別して、論理ブロック３０５及び３１０に含まれていないＣＥＭ３００の残りのポピュレートされたセルを含むことができる。下でさらに詳細に論じるように、ＣＥＭは、より良好な、またはより効率的な態様で、ポピュレートされたセルをクラスタ化するように再配設し、それによって、論理ブロックを識別することを支援し、次に、機能ブロックを作成する。このクラスタ化は、所与のＣＥＭ３００の些細な課題のように見え得るが、人間が、数百（または数千）のセルを伴うＣＥＭのパターンを効率的に識別することはほとんど不可能であり得る。

【００３７】

従来のシステムにおいて、ＣＥＭは、状態機械の機能ブロックによって表され、原因が入力であり、結果が出力である。典型的に、状態機械の機能ブロックは、ＣＥＭの結果ごとに作成される。その結果、状態機械の機能ブロックは、それらの定義されたサイズによって使用が限定されず、よって、広範囲に増殖させることができる。しかしながら、従来のシステムとは異なり、本システムは、ＣＥＭを２つのタイプの機能ブロックに、すなわち、論理の複雑さを低減させ、また、複雑な、または大きいＣＥＭを実装するときに安全システム内の論理実装の最適化を高める役割を果たす、監視ブロック及び結果ブロックに組織化する。

【００３８】

より具体的には、別個の監視ブロック及び結果ブロックを使用して、対応するＣＥＭに定義される論理の任意のパターンまたはグループを実装することで、結果から原因を２つの異なるカテゴリのブロックに分けることによって、従来のシステムの欠点に対処する。一般に、監視ブロック（ＭＢ）は、原因の抽象的表現であり、結果ブロック（ＥＢ）は、結果の抽象的表現である。そのため、システムは、１つ以上の結果ブロックにリンクまたは接続された１つ以上の監視ブロックによって、大きいＣＥＭならびにその原因及び結果

を表すことができる。例えば、一組の監視ブロックの出力は、１つ以上の結果ブロックへの入力としての役割を果たすことができ、故に、各結果ブロックの入力は、１つ以上の監視ブロックからの出力として起こり得る。一実施形態において、監視ブロックの出力は、代替的に、または加えて、１つ以上の他の監視ブロックへの入力としての役割を果たすことができる。その結果、監視ブロック及び／または結果ブロックは、最適に任意の所望のＣＥＭ論理を実装するために、所望に応じて、連鎖化、入れ子化、階層化、及び／またはレベル化することができる。さらに、ＣＥＭを複数のＭＢ及びＥＢとして表す（及び実装する）ことは、安全システムのより簡単な実装及び保守を可能にし、さらに、より複雑なＣＥＭ関係を容易に表し、構成することを可能にする。

【００３９】

別個の監視ブロック及び結果ブロックを作成することには、多くの利点がある。具体的には、ＭＢ及びＥＢは、所望に応じてサイズ決定することができ、これは、よりエラーを起こし難い、より迅速でより簡単な実装につながる。また、ＣＥＭ論理を実装するためにこれらのより小さくサイズ決定されたＭＢ及びＥＢを機能ブロックとして使用する制御または安全システムは、原因の関係を透過的に表すため、より容易に試験し、トラブルシューティングする（または一般に、リバースエンジニアリングする）ことができる。さらに、大きいＣＥＭは、より管理し易いサイズの論理ブロックに分けることができる。さらにまた、複雑な原因結果関係が、別個のＭＢ及びＥＢを使用することによって、より容易に表される。例えば、階層化、ループ化、入れ子化、連鎖化等は、全て、別個の監視及び結果ブロックを使用して表すことができる。

【００４０】

図４は、一組の相互接続した監視ブロック及び結果ブロックの概略図４００である。図４の一組の監視及び結果ブロックは、図３のＣＥＭ３００に対して提供または定義される情報または論理の全てを含む（実装する）。ここで、監視ブロック４０５及び４１０は、一般に、論理ブロック３０５及び３１０の原因（Ｃ２～Ｃ５）に対応し、一方で、結果ブロック４１５及び４２０は、一般に、論理ブロック３０５及び３１０の、またはそれらと関連付けられた結果（Ｅ３、Ｅ４、Ｅ５、Ｅ６）に対応する。例えば、監視ブロック１（ＭＢ１）４０５は、ＣＥＭ３００の原因２及び原因３を入力として含む。しかしながら、ＭＢ１　４０５の出力は、（論理ブロック３０５のように）ＣＥＭ３００の結果３、４、及び５に直接対応しない。通常は直接的な原因結果関係を実装する論理ブロック３０５及び３１０の論理を実装するために作成される状態機械とは対照的に、監視ブロックは、入力（他の監視ブロックからの原因及び出力等）及び出力（他の監視ブロックまたは結果ブロックに送信することができる）を含むことができるが、結果には直接対応しない。例えば、ＭＢ１　４０５の出力は、セット４００の様々な他の監視及び結果ブロックに送信される。具体的には、監視ブロックＭＢ１（４０５）の出力４０１は、結果ブロック１（ＥＢ１）４１５に送信され、監視ブロックＭＢ１の出力４０２は、監視ブロック２（ＭＢ２）に４１０に送信され、監視ブロックＭＢ１の出力４０３は、結果ブロック２（ＥＢ２）４２０に送信される。

【００４１】

ＭＢの出力は、一般に、対応する入力に関する情報を提供する。例えば、出力４０１は、原因２に関する情報を提供する（ＭＢ１　４０５の対応するセルの「Ｘ」が、この関係を示す）。同様に、出力４０２は、原因２及び／または原因３に関する情報を提供する。例えば、出力４０２は、原因Ｃ２またはＣ３のいずれかが存在する（例えば、論理的に真である）場合に高く（論理１）になり得、または、出力４０２は、原因Ｃ２及びＣ３がどちらも存在するときにのみ高くなり得る。当然ながら、他の論理動作を原因Ｃ２及びＣ３に対して行って、専用のＯＲｉｎｇ等の出力４０２を決定することができる。類似する様態で、ＭＢ２　４１０の出力４１１は、３つの入力（ＭＢ１　４０５の出力４０２、原因４、及び原因５）に関する情報を提供する。換言すれば、出力４１１は、（原因ブロックＭＢ１の出力４０２を生成した論理によって定義される）原因２及び原因３、ならびに原因４及び原因５に関する情報を提供する。

【００４２】
以下、結果ブロック４１５及び４２０を参照すると、結果ブロック１（ＥＢ１）４１５は、２つの入力、すなわち、監視ブロックＭＢ１からの出力４０１（原因２の状態に依存する）、及び原因６（ＣＥＭ３００からの原因６に対応する）を受信する。結果ブロックＥＢ１（４１５）のみが、１つの結果、すなわち、結果３に対応する。したがって、ＣＥＭ３００のように、結果ブロックＥＢ１（４１５）は、原因２及び６を相関させて、結果ブロックＥＢ１（４１５）の出力である結果３を作成する。理解されるように、結果ブロックＥＢ１（４１５）は、任意の所望の論理を実装することができ、また、出力４０１（ここでも原因２の状態に関連する）の状態及び原因６（Ｃ６）の状態に基づいて遅延する。

【００４３】
同様に、結果ブロックＥＢ２（４２０）は、ＣＥＭ３００の結果４、５、及び６の状態を作成または定義する論理に対応し、それを実装する。結果ブロックＥＢ２（４２０）の入力を対応する監視ブロックまでさかのぼることで、ＣＥＭ３００の結果４、５、及び６の原因結果関係が、結果ブロックＥＢ２（４２０）によって達成されることが分かる。具体的には、結果ブロックＥＢ２　４２０は、監視ブロックＭＢ２に入力される原因４及び５に基づく、及び監視ブロックＭＢ１の出力４０２に基づく、出力４１１を受信する。したがって、出力４１１は、結果ブロックＥＢ２の結果４をトリガーするために使用される原因２、３、４、及び５から導出される値または状態を有する。さらに、結果ブロックＥＢ２は、原因２及び４によって論理的に定義される、及び結果５をトリガーするためにいくつかの論理表現で使用される出力４０３及び４１２を受信する。またさらに、結果ブロックＥＢ２は、原因４及び５に基づく論理値に対応する、または該論理値として定義された出力４１３を受信し、出力４１３を使用して、結果６をトリガーする。次に、図４の一組の監視及び結果ブロック４００は、図３のＣＥＭ３００に対して以前に提供または定義された関係情報（及び論理）の全てを含む。ＣＥＭ３００を一組の監視及び結果ブロック４００に分解することによって提供される利点は、この実施例では明確でないかもしれないが、該利点は、より大きいＣＥＭを分解するときに、より明らかになる。図４に表される一組の監視及び結果ブロック４００は、単に一例を意味するものであり、監視ブロック及び結果ブロックは、ＣＥＭによって定義される論理を実装するために、無数のサイズ及び構成で作成し、構成することができることに留意されたい。

【００４４】
図５は、表示デバイスによって表示することができ、また、ＣＥＭの論理またはＣＥＭの一部分を実装する一組の監視及び結果機能ブロック表現する、または表す、構成画面５００の説明図の１つの実施例である。構成画面５００は、監視及び結果ブロックと関連付けられた論理を概略的に表すこと意図する一組の監視及び結果ブロック４００とは対照的に、監視及び結果ブロックのより詳細な機能ブロックの実装例を表す。図５の実施例において、構成画面５００は、入力（原因５０８、原因マスク５１２、及び論理タイプ５０６）と、図４の監視ブロックＭＢ１（４０５）に対応する監視ブロック５０２と、図４の結果ブロックＥＢ１（４１５）に対応する結果ブロック５０４とを含む。

【００４５】
監視ブロック５０２は、２つの原因５０８、原因マスク入力５１２、及び論理タイプ５０６にそれぞれ対応する、４つの入力（ＩＮ＿Ｄ１及びＩＮ＿Ｄ２、ＩＮ＿ＭＡＳＫ及びＬＯＧＩＣ＿ＴＹＰＥ）を受信する。論理タイプ５０６は、どのようなタイプの論理が現在の一組の監視及び結果ブロックに実装されているのかを定義する。一実施形態において、論理タイプは、正または負とすることができる。正論理は、原因の全てが最初に「偽」の状態で始まり、トリップされた場合に「真」になることを示すことができる。したがって、１つ以上の原因が「真」である場合、対応する出力は、「真」であり得る。次に、対応する結果ブロックは、１つ以上の「真」の入力を受信することができ、これは、結果ブロックの状態を高めることができ、及び／または結果ブロックをトリガーすることができる。負論理は、類似し得るが、原因が最初に「真」から始まり、原因が生じた場合に、「

偽」に設定される。例示的な論理は、限定することを意図しておらず、論理タイプ５０６はまた、「ＡＮＤ」論理、「ＯＲ」論理、または監視及び結果ブロックを実装する際に有用であり得る任意の他の論理も含むことができる。

【００４６】

原因マスク入力５１２は、監視ブロック５０２によって受信される原因５０８をフィルタリングするための初期パラメータを表すことができる。監視ブロック５０２はまた、監視ブロック５０２を構成するために使用される３つの構成マスクＣＦＧ＿ＭＡＳＫ１、ＣＦＧ＿ＭＡＳＫ２、及びＣＦＧ＿ＭＡＳＫ３　５１０も含み、各マスクは、どの原因が各出力に対応するのかを表し、及びいくつかの事例では、マスクされていない入力からの出力を発生させるために使用される論理を表す。構成マスク５１０は、下でさらに詳細に説明されるように、ＣＥＭから導出される数値表現とすることができる。

【００４７】

監視ブロック５０２はまた、５つの出力（ＯＵＴ＿Ｄ１～ＯＵＴ＿Ｄ３　５１４、ＲＡＷ＿ＶＡＬ５１６、及びＭＡＳＫ＿ＶＡＬ５１８）も含み、出力５１４のうちの１つ（ＯＵＴ＿Ｄ１）は、結果ブロック５０４への入力としての役割を果たす（図４の構成において識別される）。生の値５１６は、単に、原因５０８の受信した値を出力することができ、一方で、マスクされた値５１８は、原因マスク５１２を適用した後に、原因５０８の値を出力することができる。さらに、ＯＵＴ＿Ｄ１～ＯＵＴ＿Ｄ３は、図４のＭＢ１　４０５の出力４０１～４０３に対応する。構成マスク５１０は、どの原因が各出力に対応するのかを示す。例えば、（構成マスク５１０のうちの）ＣＦＧ＿ＭＡＳＫ１は、「Ａ」に設定され、これは、（原因５０８のうちの）原因２のみが（出力５１４のうちの）ＯＵＴ＿Ｄ１に対応することを示すことができる。さらに、（構成マスク５１０のうちの）ＣＦＧ＿ＭＡＳＫ２は、「Ｂ」に設定され、これは、（原因５０８のうちの）原因２及び原因３が、（出力５１４のうちの）ＯＵＴ＿Ｄ２に対応することを示すことができる。またさらに、いくつかの事例において、構成マスク５１０は、１６進数等の数値表現とすることができ、これは、どの監視ブロックの入力が特定の監視ブロックの出力を駆動または達成するのかを表し、及び／またはブロックの入力からブロックの出力を発生させるために使用される実際の論理を表す。

【００４８】

図５に例示されるように、結果ブロック５０４は、４つの入力（ＩＮ＿Ｄ１及びＩＮ＿Ｄ２　５２０、リセット５２２、及びＬＯＧＩＣ＿ＴＹＰＥ５０６）及び２つの出力（状態５２６及びＯＵＴ＿Ｄ５２４）を含むことができる。結果ブロック５０４の入力５２０は、監視ブロック５０２の出力５１４、さらには、図３のＣＥＭ３００の原因６を含む。結果ブロック５０４の状態５２６は、結果ブロック５０４に対応するデバイスの動作状態に対応することができる。換言すれば、いかなる対応する「真」の原因も受信しなかった場合、状態５２６は、正常であり得る。しかしながら、例えば「真」の値に設定された１つ以上の原因を受信する場合、状態は、新しい状態（例えば、「警告」、「危険」、「トリガー済」）を示すように変化し得る。リセット入力５２２は、結果ブロック５０４が非正常状態であるときに必要なアクションが行われた時点で、ユーザが、結果ブロック５０４の状態を正常へ自動的にリセットすることを可能にすることができる。当然ながら、（例えば、原因の入力または監視ブロックの入力の変化状態に応じて）許可のリセット等の、他の状態変化入力も同様に、結果ブロックに提供することができる。さらに、この実施例では論理タイプ５０６が正に設定されているので、受信した入力５２０のうちの１つ以上が「真」である場合、この事例においてＣＥＭ３００の結果３に対応する出力ＯＵＴ＿Ｄは、トリガー済応答であり得る。

【００４９】

一例として、図５は、原因２及び原因３の入力が「偽」であり、かつブロック５０２及び５０４両方の論理タイプが正に設定されているときの、（ブロック５０２の）ＯＵＴ＿Ｄ１、（ブロック５０４の）ＩＮ＿Ｄ２、及びＯｕｔ＿Ｄの各々の状態を例示する。この時点で、プロセスプラントにおいて（原因５０８のうちの）原因２が起こった場合は、原

因２の状態が「偽」から「真」に変化し得る。したがって、ＭＢ１　５０２は、真として入力ＩＮ＿Ｄ１を受信する。次いで、対応する出力ＯＵＴ＿１もまた、Ｌｏｇｉｃ＿Ｔｙｐｅの入力での正論理タイプ及びＯＵＴ＿Ｄ１（出力１）の構成マスク、すなわち、ＣＦＧ＿ＭＡＳＫ１に基づいて、真に変化する。この実施例において、構成マスク５１０が適用されられた後に、ＩＮ＿Ｄ１は、出力（ＯＵＴ＿Ｄ１～ＯＵＴ＿Ｄ３）５１４の各々の値を駆動または達成する。具体的には、ＯＵＴ＿Ｄ１は、「真」に設定されているＩＮ＿Ｄ１に基づいて、「真」に設定することができる。したがって、次いで、ＥＢ１　５０４が少なくとも１つの「真」の入力（ＩＮ＿Ｄ１）を受信する。その結果、ＥＢ１　５０４の状態５２６は、「トリガー済」に変化し、結果ブロック５０４の出力５２４のＯＵＴ＿Ｄは、図４の結果３がトリガー済または「真」となることを意味する、「真」に設定される。結果的に、結果がトリガーされ、任意の対応するアクション及び／またはアラームをプロセス制御プラントにおいてオフに設定することができる。

【００５０】

図６は、表示デバイスによって表示することができ、また、監視及び結果ブロックの構成を表すことができる、構成画面６００の説明図の別の実施例である。図６の実施例は、図４からの監視ブロックＭＢ２及び結果ブロックＥＢ２に重点を置く。例示の目的で、論理タイプ６０６は、負に設定され、これは、通常状態であるときに、全ての原因が「真」であることを意味する。負論理タイプにおいて、１つ以上の入力が発生し、状態を「偽」に切り換えるときに、監視ブロックの対応する出力は、「偽」に設定することができ、これは、結果ブロックを受信し、次いで、結果を「真」に設定する結果をトリガーすることができる。

【００５１】

さらに、結果ブロックＥＢ６０４は、時間遅延入力６０８を含む。この実施例において、結果ブロック６０４の入力１（ＩＮ＿Ｄ１）は、結果ブロック６０４のＤｅｌａｙ＿Ｔｉｍｅ１の入力に「２０」が入力されたときに、出力ＯＵＴ＿Ｄを、２０秒の遅延（ＤＥＬＡＹ＿ＴＩＭＥ１）によってトリガーさせる。しかしながら、この実施例の入力２（ＩＮ＿Ｄ２）は、時間遅延（ＤＥＬＡＹ＿ＴＩＭＥ２）がゼロに設定されているので、出力（ＯＵＴ＿Ｄ）を、即時にトリガーさせることができる。この実施例は、限定することを意図しておらず、特定の結果ブロックに対して任意の数の遅延及び遅延時間を設定することができる。

【００５２】

一実施例として、原因４が生じた場合は、原因４の状態（結果的に、ＩＮ＿Ｄ２）が「偽」に変化する。図４を再び参照すると、原因４が、監視ブロック４１０の出力４１１～４１３の各々に対応する、またはそれらを達成することが分かる。したがって、この実施例において、原因４（及びＩＮ＿Ｄ２）は、監視ブロック６０２の構成マスクによって実装される論理に従って、ＭＢ２の全ての出力（ＯＵＴ＿Ｄ１～ＯＵＴ＿Ｄ３）を駆動または達成することができる。具体的には、ＭＢ２　６０２のＯＵＴ＿Ｄ１を「偽」に設定することができる。次に、ＥＢ２　６０４のＩＮ＿Ｄ２が「偽」として受信される。したがって、ＥＢ２　６０４のＩＮ＿Ｄ２に対応する時間遅延（ＤＥＬＡＹ＿ＴＩＭＥ２）がゼロの時間遅延に設定されたときには、ＥＢ２　６０４の対応する結果を即時にトリガーすることができる。一実施例として、図４のＭＢ２　４１０の出力４１１がＭＢ２　６０２のＯＵＴ＿Ｄ１に対応する場合は、これらの出力のみが、ＥＢ　６０４においてＯＵＴ＿Ｄ１として表すことができる（ＣＥＭ３００の）結果４を駆動する。したがって、この時点でＥＢ６０４のＯＵＴ＿Ｄ１をトリガーし、「真」に設定することができる。

【００５３】

図５及び６において提供される例示的な監視及び結果ブロックは、実証の目的で単純にすることを意図する。例えば、監視ブロック５０２は、図５において４つの入力及び５つの出力を有するように示されているが、他の実施形態は、監視ブロックの機能に基づいて、任意の所望の数の必要な入力及び出力を含むことができる。１つの実施形態において、入力ＩＮ＿Ｄｘ及び出力ＯＵＴ＿Ｄｘの数は、一般に、再編成されたＣＥＭの各論理ブロ

ックの入力及び出力の数に対応する。さらに、システムは、１つの監視を実装して、複数の結果ブロック及び追加的な監視ブロックを駆動または達成することができるようにマスクを構成することができる。次に、ＣＥＭは、層化、ループ化、入れ子化、連鎖化等を行うことができる複数の監視及び結果ブロックに分けることができ、これは、従来の状態機械の実装よりも大きい、プロセス制御プラントのシステムを構成するための柔軟性をシステムに提供することができる。

【００５４】

図７は、プロセスプラントと関連付けられた監視ブロック及び結果ブロックを構成する例示的な方法７００のフロー図である。方法７００は、定期的に、及び／または構成エンジニアまたは他のユーザまたは他の安全論理デザイナーによる指示または開始信号等の、トリガーイベントに応答して実装することができる。方法７００は、図１に関して論じられるプロセスプラント１０等のプロセスプラントの１つ以上の構成要素を含むことができる電子デバイス（例えば、原因結果分析器ツール１７）によって行うことができる。

【００５５】

ブロック７１０で、電子デバイスは、ＣＥＭを受信する、または別様にはそこにアクセスすることができる。特定の実施形態では、論理ブロックを識別する前に、ＣＥＭを再配設して、グループのクラスタにおけるスパース性及び他の収集情報を除去することが有益であり得る。ブロック７１５で、電子デバイスは、自動的にＣＥＭを再配設することができ、及び／またはユーザがＣＥＭを再配設することを可能にすることができる。ＣＥＭを自動的に再配設するための方法は、下でさらに詳細に論じられる。ブロック７２０で、電子デバイスは、一組の監視ブロック及び結果ブロックを識別し、作成して、ＣＥＭの論理を実装することができる。ブロック７３０で、電子デバイスは、監視及び結果ブロックを、ＣＥＭを実装する安全または制御論理を設計することができる構成または安全論理エンジニア等のユーザに表示することができる。具体的には、電子デバイスは、表示デバイスに、グラフィカルユーザインターフェース（ＧＵＩ）を表示させることができ、ＧＵＩは、第１の監視ブロック、第２の監視ブロック、及び結果ブロックを示すことができる。さらに、第１の監視ブロック、第２の監視ブロック、及び結果ブロックの各々は、第１の次元及び第２の次元を有するマトリックスで配設された複数のセルを示すことができ、第１の次元に沿った位置は、出力を示すことができ、第２の次元に沿った位置は、入力に対応することができ、よって、第１及び第２の次元に対する複数のセルの位置に基づいて、複数のセルが入力／出力対を定義することができる。

【００５６】

ブロック７４０で、電子デバイスは、監視ブロック及び結果ブロックを構成して、またはユーザが該ブロックを構成することを可能にして、ＣＥＭの論理を実装することができる。一実施形態において、電子デバイスは、ユーザが、入力デバイスを介して構成データを入力することを可能にする。別の実施形態において、電子デバイスは、ＣＥＭを構文解析することによって、構成データを自動的に判定すること、または発生させることができる。実装例によれば、電子デバイスは、第１の監視ブロックの出力のうちの１つを、第２の監視ブロックの入力のうちの１つとしての役割を果たすように構成することができ、第１の監視ブロックの出力のうちの追加的な１つ及び第２の監視ブロックの出力のうちの１つを、結果ブロックへの入力としての役割を果たすように構成することができ、ならびに／または第１の監視ブロック、第２の監視ブロック、及び結果ブロックの各々の複数のセルのうちの少なくとも１つを、それぞれのセルのそれぞれの入力／出力対と関連付けられた、及びプロセスプラントの条件に対応する、トリガーに指定することができる。

【００５７】

一実施形態において、監視ブロック及び結果ブロックを構成するために、電子デバイスは、追加的な入力／出力対を定義する追加的な複数のセルを有する少なくとも１つの追加的な監視ブロックを組み込むことができ、追加的な監視ブロックの少なくとも１つの出力を、第１の監視ブロック、第２の監視ブロック、及び結果ブロックのうちの少なくとも１つへの入力としての役割を果たすように構成することができ、また、追加的な複数のセル

のうちの少なくとも１つを、それぞれの追加的なセルのそれぞれの追加的な入力／出力対と関連付けられた、及びプロセスプラントの追加的な条件に対応する、追加的なトリガーに指定することができる。別の実施形態において、監視ブロック及び結果ブロックを構成するために、電子デバイスは、追加的な入力／出力対を定義する追加的な複数のセルを有する少なくとも１つの追加的な結果ブロックを組み込むことができ、追加的な結果ブロックの少なくとも１つの入力を、第１の監視ブロックまたは第２の監視ブロックのうちの１つの出力に対応する構成するように構成することができ、また、追加的な複数のセルのうちの少なくとも１つを、それぞれの追加的なセルのそれぞれの追加的な入力／出力対と関連付けられた、及びプロセスプラントの追加的な条件に対応する、追加的なトリガーに指定することができる。

【００５８】

加えて、一実施形態において、監視ブロック及び結果ブロックを構成するために、電子デバイスは、第１の監視ブロック及び第２の監視ブロックの各々の入力を構成することができ、第１の監視ブロック及び第２の監視ブロックのうちの少なくとも１つの入力マスクを、該入力マスクが、第１の監視ブロック及び第２の監視ブロックのうちの少なくとも１つの入力と論理的に関連付けられるように構成することができ、トリガーのうちの少なくとも１つを、関連付けられた結果を時間遅延を伴って起動させるために、時間遅延トリガーに指定することができ、ならびに／またはトリガーのうちの少なくとも１つを、許容トリガーに指定することができる。

【００５９】

ブロック７５０において、電子デバイスは、構成した監視ブロック及び結果ブロックを記憶することができる。具体的には、電子デバイスは、第１の監視ブロック、第２の監視ブロック、及び結果ブロックと関連付けられたコンピュータ可読媒体に構成データを記憶することができる。一実施形態において、電子デバイスは、第１の監視ブロック、第２の監視ブロック、及び結果ブロックの各々の複数のセルを表示デバイスにさらに表示することができ、また、それぞれの複数のセル内のそれぞれのトリガーを示すことができる。

【００６０】

当然ながら、方法７００は、任意の数の方法で共に接続された任意の数の監視及び結果ブロックを作成して、これらの相互接続した監視及び結果ブロックを使用してＣＥＭの論理を実装することができる。各監視ブロックは、任意の数のＣＥＭの原因またはその任意のサブセットを、該監視ブロックへの入力として含むことができ、また、他の監視ブロックの出力に結び付けることができ、それによって、カスケード型監視ブロックを達成することができる。さらに、任意の結果ブロックは、一組の入力から１つ以上の結果を判定することができ、また、監視ブロックの出力及び／または任意の原因の入力のいずれかを入力として受信することができる。またさらに、方法７００で、様々な監視ブロックならびに他の監視ブロック及び結果ブロックを相互接続することができ、またはユーザが該ブロックを相互接続する（すなわち、該ブロック間の接続を定義する）ことを可能にする。そのため、各監視ブロックは、原因信号（直接的な、または別の上流の監視ブロックに入力された原因信号から生じた別の中間論理信号の形態での、監視ブロックへの入力）の１つ以上に基づいて、１つ以上の中間論理条件または信号を判定する論理を含む。同様に、各結果ブロックは、該結果ブロックへの一組の入力に基づいて、１つ以上の結果信号を生成し、そのような入力は、監視ブロックの１つ以上から出力される原因信号及び／または中間論理信号である。この様態で、方法７００は、中間論理信号を、原因信号のいくつかの論理組み合わせを表す１つ以上の監視ブロックにおいて生じさせることを可能にし、また、この中間論理信号を１つ以上の結果ブロックへの入力として提供または使用することを可能にし、それによって、結果信号を作成するために結果ブロックによって実装される構成、サイズ、及び論理を簡単にする。

【００６１】

より小さいＣＥＭの場合は、方法７００のブロック７１５で、パターンを識別することによって、または関連する原因及び結果をグループ化しようとすること等によって、安全

エンジニアが、ＣＥＭを手動で再配設及び／または構成することを可能にすることができる。そのような再配設は、ユーザによって、グラフィカルユーザインターフェースを介して、手動で実装することができ、ＣＥＭの周囲の様々な行及び／または列を移動させて、または再配設して、原因結果関係（例えば、Ｘの印が付されたセル）が互いに近づくように、またはより密度の高いグルーピングを形成するように定義するセルをグループ化する。しかしながら、より大きいＣＥＭを再編成するには多数の方法があり、再編成するための最良のオプションを識別することが有益である。故に、プロセス制御システムと関連付けられたＣＥＭを動的かつ自動的に分析し、再編成する機会が存在する。

【００６２】

一実施形態において、システム（すなわち、図１のコンピュータシステム）は、一組の規則に基づいて大きいＣＥＭを自動的に再編成するために、原因結果分析器ツール１７を実装することができる。一実施形態において、規則３１は、図１の構成データベース３２に記憶することができ、ならびに／またはワークステーション１８ａ及び／もしくは２０ａのユーザインターフェースを介して受信することができる。分析器ツール１７は、ＣＥＭを分析して、一組の規則３１を考慮してＣＥＭの最適な、または最適化された構成（すなわち、ＣＥＭを再配設して、一組の監視及び結果ブロックを生成する最良の様態）を決定する。一組の規則３１は、特定のプロセスプラントの現在のニーズまたは構成に基づいて、エンジニアによって指定するか、または別様には、分析器ツール１７等のコンピュータによって自動的に発生させることができる。例えば、一組の規則３１は、この論理が実装されるべき対応する論理ソルバー５０、ＭＰＤ７０、ならびに／またはフィールドデバイス２２、２３、２４、６０、及び６２に基づいて、ＣＥＭを、特定の原因及び／または結果が共にグループ化された状態で、グループに構成するべきであることを示すことができる。さらに、一組の規則３１は、特定のパターンに基づいて、システムの効率に基づいて、及び／または他の基準に基づいて、ＣＥＭを再編成して、スパース性を除去するべきであることを示すことができる。別の実施形態において、一組の規則３１は、特定の原因及び／または結果（または原因及び／または結果のグループ）を移動させるべきではないことを示すことができる。さらに別の実施形態において、一組の規則３１は、再編成する必要がある特定の原因及び／または結果の重みを示すことができ、該重みは、異なる結果につながる多数の規則を適用しようとするときのコンフリクトを解決するために使用される。

【００６３】

一実施形態において、一組の規則３１は、ＣＥＭが、特定の数のグループ及び／または特定のサイズのグループに再編成されるべきであることを示すことができる。一組の規則３１は、グループが構成されるべき様態をさらに示すことができる。例えば、一組の規則３１は、各集団が、特定の数の、特定の最大数の、または特定の最小数の原因及び／または結果を含むべきであることを示すことができる。一実施形態において、一組の規則３１は、グループが、重複する原因及び／または結果を含むべきではないことを示すことができる。規則３１はまた、例えば、これらの原因が特定の論理ソルバーによって、もしくは特定のノードにおいて検出されるので、または結果を特定の論理ソルバーにおいて特定のノードによって実装することが必要であり得るので、特定の原因または結果を共にグループ化するべきであることを指定することもできる。いずれにしても、ＣＥＭが再編成されると、一組の規則３１は、さらに、エンジニアがＣＥＭの特定の原因及び／または結果を手動で構成することを可能にすることができる。代替の、または追加的な規則が想定されることを認識されたい。

【００６４】

一実現形態において、分析器ツールは、一組の規則３１を受信すること、または発生させることができ、該一組の規則は、プロセスプラントの特定の領域に対応する特定の原因及び／または結果のみを再編成するべきであること、またはこれらの原因及び結果を共に、またはグループとして再編成するべきであることを示す。同様に、一組の規則３１は、ＣＥＭの原因及び結果の特定のサブセットのみを再編成するべきであることを示すことが

できる。分析器ツールはまた、特定の行及び／または列を「ロックする」一組の規則３１を受信して、または発生させて、受信した行及び／または列が再編成中に移動することを防止することもできる。またさらに、分析器ツールは、一組の規則３１を受信すること、または発生させることができ、該一組の規則は、正論理（すなわち、原因が「オン」である場合に結果を起動する）に対応する原因を共にグループ化するべきであること、及び負論理（すなわち、原因が「オン」である場合に結果を起動しない）に対応する原因を共にグループ化するべきであることを示す。ＣＥＭセルにおいて定義される論理のタイプ（すなわち、実装されるべき論理のタイプ）に基づいてＣＥＭの行及び列をグループ化または再編成する他の様態も、同様に使用することができる。

【００６５】

次に、ＣＥＭの再編成は、コンピュータによって実装することができ、かつ一組の規則３１に基づくことができるマルチパート分析を必要とし得る。コンピュータは、行によって、列によって、グループによって、トリガーによって、対応する論理ソルバー５０、ＭＰＤ７０、ならびに／もしくはフィールドデバイス２２、２３、２４、６０、及び６２に基づいて、または一組の規則３１の実装に最良に適している任意の他の要素によって、ＣＥＭを分析することができる。例えば、図８は、以前の例示的な図３のＣＥＭ３００よりもかなり大きい例示的なＣＥＭ８００である。ＣＥＭ８００は、マトリックスの全体を通して散在するいくつかのポピュレートされたセルを含む。ＣＥＭ８００は、ＣＥＭ３００よりもわずかにより大きいだけであるが、一組の監視及び結果ブロックによって実装されるＣＥＭ８００の論理ブロックまたは論理グループを識別する問題が、ますます複雑であることは明白である。さらに、ＣＥＭ８００は、より大きいグルーピングから散在された、ポピュレートされたセルを含み、これは、監視及び結果ブロックを発生させるために使用される論理ブロックを効率的に選択する難しさを増加させる。増加したサイズのＣＥＭの場合、論理ブロックを手動で選択する、または定義する難しさが非常に増大する。

【００６６】

図９は、図８からのＣＥＭ８００を再編成したバージョンであるＣＥＭ９００を表す表示の１つの実施例を例示する。図９に例示されるように、ＣＥＭ９００は、３つの主グループまたは論理ブロック９０１、９０２、及び９０３を含むように構成されている。例示的な一実施形態において、論理ブロック９０１、９０２、及び９０３は、それぞれ、プロセスプラント内の特定の論理ソルバー５０に対応することができる。別の実施形態において、コンピュータは、一組の規則３１内で定義された基準に基づいて、論理ブロック９０１～９０３を識別することができる。

【００６７】

例えば、図９の論理ブロック９０１は、全てがプロセスプラント（例えば、特定の加熱セクション）の特定の物理的な場所に属する、またはプラント制御システムの同じコントローラまたは論理ソルバーによって実装される、一組の結果に対応することができる。さらに、論理ブロック９０２は、全ての原因が全ての結果に関連するグループを認識することによって、ＣＥＭからスパース性を除去する分析器ツールによって生じさせることができる。具体的には、論理ブロック９０２で、原因４～１０の各々は、結果３～５の各々と対になる。論理ブロック９０３は、負論理の原因結果関係のグループに対応することができる。例示的ＣＥＭ９００は、３つの論理ブロックを含んでいるが、ＣＥＭは、任意の数の論理ブロックに分けることができ、また、ＣＥＭを分析し、再編成するときに分析器ツール１７によって使用することができる規則３１のうちのいずれか、または任意の組み合わせまたは規則３１に、上で説明した、もしくは上で述べられていない任意の他の規則に基づくことができる。論理ブロック９０１、９０２、及び９０３は、それぞれ、図３及び４に関して上で説明したように、一組の相互接続した監視及び結果ブロックを定義して、ＣＥＭのこれらの部分の論理を実装するために使用することができる。

【００６８】

図１０は、プロセス制御システムの安全または制御論理を開発する際に使用されるＣＥＭの原因結果マトリックスを再配設し、論理ブロックを定義及び／または管理する例示的

な方法１０００のフロー図である。方法１０００は、例えば、プラントの構成中、論理のＣＥＭが変更または更新されるたび、等のときに、定期的に、及び／またはトリガーイベントに応答して、実装することができる。方法１０００は、図１に関して論じられるプロセスプラント１０等のプロセスプラントの１つ以上の構成要素を含むことができる電子デバイス（例えば、図１の分析器ツール１７）によって行うことができる。ブロック１０１０で、電子デバイスは、一組の入力及び一組の出力（すなわち、一組の原因及び一組の結果）を有する初期原因結果マトリックスにアクセスする。実施形態において、一組の入力の各々は、プロセスプラント内の条件を表すことができ、一組の出力の各々は、プロセスプラント内で行われるべき結果を表すことができる。さらに、一組の入力及び一組の出力のうちの少なくともいくつかは、原因－結果の対として関連され、それによって、対応する結果を、対応する条件の発生に応答して起動させることができる。初期原因結果マトリックス（ＣＥＭ）は、プロセス制御プラントのデータリポジトリに記憶することができ、またはプラントの新しいプロセスを構成するための電子デバイスにおいてユーザによって発生させることができる。初期ＣＥＭはまた、プロセス制御システムの外部のデータベースから受信することもできる。いくつかの実施形態において、初期ＣＥＭは、適切な証明書を有するエンジニアによってのみアクセスすることができ、したがって、初期ＣＥＭへのアクセスを許可するために、ログインまたは他のパスワードが必要であり得る。

【００６９】

電子デバイスは、初期ＣＥＭ内の一組の関連するグループの各々を定義することができる。具体的には、ブロック１０２０で、電子デバイスは、一組の関連するグループと関連付けられた一組の規則３１にアクセスすることができる。具体的には、電子デバイスは、プロセス制御システムの内部または外部のいずれかの１つ以上のデータベースを通して、一組の規則３１にアクセスすることができる。電子デバイスはまた、プロセス制御プラントのエンジニアによって提供される入力として、一組の規則３１を受信することもできる。さらに、一組の規則３１は、様々なデータベース及び／または入力を通してアクセスされる様々な規則の組み合わせとすることができる。上でさらに詳しく論じたように、一組の規則３１は、効率的かつ有効な様態でＣＥＭを再編成することを目的とすることができる。

【００７０】

１つの実施形態において、規則は、一組の出力の指定された部分が、同じ関連するグループ内でなければならないことを指定することができる。別の実施形態において、規則は、一組の入力の一部分が、ある量に達しなければならないことを指定することができる。さらなる実施形態において、規則は、一組の入力も、一組の出力も、一組の関連するグループの間で重複してはならないことを指定することができる。当然ながら、任意の他の所望の規則を使用することができる。

【００７１】

ブロック１０３０で、電子デバイスは、ＣＥＭにおいて定義された対応する原因－結果の対によって定義される一組の規則に従って、一組の出力（結果）の一部分に関連する一組の入力（原因）の一部分を識別することができる。さらに、ブロック１０４０で、電子デバイスは、対応する原因－結果の対の一部分が再配設されるように、一組の入力の一部分及び一組の出力の一部分を再配設することができる。ブロック１０４０は、この再配設を行って、上で定義されたように、一組の監視及び結果ブロックを使用して実装される１つ以上の機能ブロック論理ユニットを定義することができる。ブロック１０５０は、再配設されたＣＥＭを分析し、プロセスが完了したかどうかを判定することができ、完了していない場合は、制御をブロック１０３０に提供して、再配設されたＣＥＭに基づいて監視及び結果ブロックの作成をさらに最適化することを目指してＣＥＭを再配設するために使用される他の規則を識別することができる。さらに、ブロック１０５０は、再配設が完了したときに、図９の３つの論理グルーピング９０１、９０２、及び９０３等の、再配設されたＣＥＭ内の論理ブロックまたは論理のグループを定義することができる。

【００７２】

一実現形態において、電子デバイスは、ブロック１０５０によって定義される一組の関連するグループに従って、プロセス制御システムの１つ以上の機能ブロック論理ユニットをさらに構成することができる。加えて、または代替的に、電子デバイスは、図１１～１２に関して下でさらに詳細に論じられる、関連するグループの１６進表現を算出すること等によって、再配設された原因－結果の対に従って、一組の関連するグループの各関連するグループについて、関連するグループの、または関連するグループの一部分の数値表現を自動的に算出することができる。

【００７３】

分析器ツールがＣＥＭ９００を再編成すると、システムは、ＣＥＭ９００を別個の論理グループにさらに分けて、それらの論理グループを実装する監視及び結果ブロックを作成する際の効率をさらに改善することができる。図１１は、図９のＣＥＭ９００の追加的な表現を表す。具体的には、システムは、図９のＣＥＭ９００を分析して、一組の相互接続した監視ブロック及び結果ブロックとして機能ブロックを構成するためにシステムが使用することができる、様々な数値表現１１０１、１１０２、及び１１０３を生成することができる。一実施形態において、数値表現１１０１～１１０３は、それぞれ、再配設されたＣＥＭ９００によって定義される原因結果の対によって定義された論理関係の構成に基づいて、１６進値等の値として出力または結果を表す、または定義することができる。この数値は、論理表現として各列を表す従来のシステムとは対照的である。しかしながら、そのような従来のシステムは、論理表現を実装または理解することが難しいので、非効率的である。

【００７４】

一実施形態において、システムは、マトリックスの各セルに２つの値（例えば、オンまたはオフ、１または０等）のうちの１つを指定し、次いで、ＣＥＭの行または列の各ビットグループ（例えば、４桁の２進数）を１６進数に変換することによって、数値表現を案出することができる。例えば、図１１に例示されるように、出力１４の数値表現１１０１は、出力１４と関連付けられたセルの１６進表現（ＦＥ０８）であり、ここで、セルのＸは、バイナリの「１」として扱われ、空きセルは、バイナリの「０」として扱われる。この算出は、出力１４を４つのビットグループに分け（セル間を太線で区切り、上から下へ：１１１１、１１１０、００００、１０００の４つのビット数を形成する）、次いで、各ビットグループを１６進数に変換することによって示すことができる。この事例において、１６進数字で、Ｆ＝１１１１、Ｅ＝１１１０、０＝００００、及び８＝１０００であるので、出力１４の数値表現１１０１は、ＦＥ０８である。同じ様態で、出力５は、上から下へ、ビット００００、０１１１、１１１０、００００に分けることができるので、数値表現１１０２（０７Ｅ０）は、出力５に対応し、これは、１６進数の０７Ｅ０に翻訳する。類似する様態で、出力１７は、１６進数の００７２（数値表現１１０３）として表すことができる。例示的な数値表現は、限定することを意図しておらず、列及び／または行のうちのいくつかまたは全てが数値表現を指定することができる。さらに、数値表現は、必ずしも１６進変換である必要はなく、また、任意の他の適切な形態で作成することができる。

【００７５】

ＣＥＭ内の論理セルの特定のグルーピングについて数値表現を案出することには、多くの利点がある。具体的には、従来のシステムと比較して、列を１６進変換することは、より単純であり、表現を発生させるために追加的なゲートまたはプログラミングを必要とせず、記憶するために費やすメモリが少なく、そして、機能ブロック入力に通信するために費やす帯域幅が少ない。さらに、１６進値入力は、所望に応じてより容易にエラーを補正して、精度を確保することができ、図１５の試験マトリックスに関して下で論じられる。

【００７６】

数値表現は、システムが、安全システム構成環境の原因／結果関係を構成することをさらに可能にすることができる。具体的には、数値表現は、システムが、多数の原因及び結果の関係を定義することを可能にすることができる。さらに、数値表現は、全ての行及び

／または列全体を単一の数値に取り出すことによって、構成エラーを排除することを補助することができる。加えて、数値表現は、原因／結果関係の変化を識別し、また、ＣＥＭの変化を管理するために必要な労力をさらに低減させる、単純で効率的な方法を提供することができる。

【００７７】

例えば、数値表現は、図４～６の監視及び結果ブロック等の機能ブロックの構成マスクとして実装することができる。したがって、これらの数値表現は、監視及び／または結果ブロックの特定の結果について実装されるべき論理を実際に識別することができる。数値表現は、どの入力が各特定の出力に対応するのかを定義し、したがって、特定の出力に対応しない入力を切り離す（すなわち、マスクする）ことができる。例えば、図１１の結果１４の数値表現１１０１は、結果１４から原因６～１３の全てを切り離すことができる。換言すれば、監視ブロックは、原因１～１６の全てを受信することができるが、数値表現１１０１をマスクとして実装した場合は、単に、原因１～５及び１４～１６を結果１４に相関させる。

【００７８】

さらに、システムは、可能なセル値の範囲が２つを超えるときに（例えば、セルが、値なし、Ｘ、１Ｔ（時間遅延を示す）、Ｐ（原因の許容を示す）等の、多数の異なるトリガーを定義することができるときに）、数値表現を適合させることができる。例えば、例示的な４つの可能な交差値の範囲について、システムは、２つの１６進変換を行って、結果として生じる数値表現を発生させることができる。換言すれば、各セルの４つの可能な異なる値は、２ビット数の４つの可能な値のうちの１つとして表すことができ、これは、各セルが、図１１に示される１ビット値の代わりに、２ビット値によって定義されることを意味する。この事例において、各一組の文字列の２つの隣接するセルは、１６進数に変換することができる４ビット値を形成する。その結果、このシナリオにおける数値表現は、図１１に示される数値表現の２倍の長さになるが、ＣＥＭを実装する論理において使用される、より多い数の潜在的な論理表現を表すことができるように、より動的である。代替的に、システムは、ベース１６以外の適切なベースを使用して数値表現を算出することができ、次いで、随意に、（所望であれば）数値表現を機能ブロック（すなわち、監視及び結果ブロック）の１６進の入力値に変換することができる。

【００７９】

図１２は、ＣＥＭ内の値または要素の数値表現を作成／算出するための例示的な方法のフローチャートである。ブロック１２１０で、原因及び結果分析器ツール１７は、ＣＥＭにアクセスすることができる。例示的な一実施形態において、ＣＥＭは、継続する前に再配設することができる。ブロック１２２０で、ツール１７は、原因のサブセットを識別することができる。一実施形態において、原因のサブセットは、上で説明したように、特定の論理ブロックに属すること、及び／または一組の規則によって定義することができる。次に、ブロック１２３０で、ツール１７は、原因のサブセットの単一の次元マトリックスを定義することができる。一次元マトリックスは、ＣＥＭの特定の結果に対応することができる。次に、ブロック１２４０で、ツール１７は、一次元マトリックスの数値表現を算出することができる。上で説明したように、ツール１７は、一次元マトリックスを２進文字列及び／または多数の２進文字列に変換することができる。一実施形態において、ツールは、次いで、１つ以上の２進文字列の１６進表現または任意の他の適切な数値表現への変換に進むことができる。算出した数値表現は、数値表現３３として図１の構成データベース３２等のリポジトリに記憶することができる。

【００８０】

ブロック１２５０で、次いで、数値表現３３を使用して、一組の機能ブロック（例えば、監視及び結果ブロック）を構成することができる。例えば、上で説明したように、数値表現３３は、１つ以上の監視ブロックの構成マスクとして実装することができる。

【００８１】

本明細書で説明されるシステムの別の態様において、システムナビゲータアプリケーシ

ョンは、プロセスプラントの関連する安全情報を提供する異なるユーザインターフェース画面の間を迅速にナビゲートする能力をユーザに提供する。そのような情報は、ＣＥＭ、監視及び結果ブロック、安全文書、ならびにシステム構成表示において見つけることができる。いくつかの実施形態において、これらの異なるユーザインターフェースは、同じ安全論理の異なる視覚的表現を提供する。したがって、本発明は、インターリンクされた一組のユーザインターフェースの間をナビゲートするために、（図１の）ナビゲータツール１５を提供する。例えば、図１３は、インターリンクされた一組のユーザインターフェースの例示的な説明図１３００である。

【００８２】

いくつかの例示的なプロセスプラントにおいて、安全プロトコルは、いくつかの言語のうちの１つでプログラムされる。プログラミング言語に関係なく、安全プロトコルの開始点は、通常、プロセスプラントの制御及び／または安全アクションの要求を指定する注釈文書である。安全計装システム（ＳＩＳ）等の、他の例示的なプロセスプラントにおいて、安全要求は、安全要求仕様（ＳＲＳ）として知られている文書において文書化されている。

【００８３】

ＳＲＳに関する情報のうちの１つは、識別された安全計装機能（ＳＩＦ）のリストである。各ＳＩＦは、特定の危険から保護し、また、定義されたレベルのリスク低減を提供する。ＳＩＳは、１つ以上のＳＩＦで構成される。いくつかの実施形態において、いくつかの安全システムは、個々のＳＩＦの区別なく、ＳＩＳ構成において全てのＳＩＦを組み合わせる。さらに、いくつかの安全システムは、ＳＩＦアプローチに従って、ＳＩＦベースのＳＩＳ構成を可能にする。

【００８４】

ＳＲＳは、通常、異なるセクションを含む。セクションのうちの１つは、プレーンテキスト、論理図、または特性要因図（すなわち、原因結果マトリックス）のいずれかによって表すことができる論理記述である。上で述べたように、いくつかの安全システムは、ＳＩＳ構成内の全てのＳＩＦを組み合わせ、ＣＥＭの視覚化は、そのような実施形態を実装する際に非常に好都合であり得る。

【００８５】

１つの実施形態において、ナビゲータアプリケーション１５は、エンジニアが、ＣＥＭ内の所与の原因（及び／または結果）を選択して、選択された原因（及び／または結果）を説明する特定の文書にナビゲートすることを可能にする。例えば、原因を選択することで、ＳＲＳ内の特定のＳＩＦの説明にリダイレクトすることができる。この特徴は、エンジニアが、原因及び／または結果と関連付けられた特定の安全論理を見ることを可能にする。一実施形態において、エンジニアはまた、所与のＳＩＦと関連付けられた安全モジュール（システム構成）を選択することもでき、次いで、ＣＥＭから適切なＳＩＦを表示するユーザインターフェースにリダイレクトすることができる。さらに、エンジニアは、ＣＥＭの要素を選択して、ＣＥＭの特定の要素に関連するシステム構成強調表示デバイス、論理ブロック、機能ブロック、監視及び結果ブロック等の表示にリダイレクトすることができる。安全または制御モジュールから、ユーザはまた、ＳＲＳまたは制御いずれかの注釈に関する適切なセクションにリダイレクトすることもできる。換言すれば、現在のシステムは、エンジニアが、ＣＥＭ、ＳＲＳ、またはシステム構成のビューの間をシームレスに切り換えることを可能にすることができる。

【００８６】

例えば、エンジニアがＣＥＭ１３１０を表示する図１３のユーザインターフェースの原因及び／または結果を選択した場合は、エンジニアを、ＣＥＭの選択された原因及び／または結果に関連する特定のデバイスを含むシステム構成を示す表示画面１３２０にリダイレクトすることができる。例えば、システム構成１３２０は、ＣＥＭの選択された原因及び／または結果に関連するタンク、弁、トランスミッタ、ポンプ、パイプ、センサ等のシンボルを含むことができる。この実施例では、温度計アイコン１３２１が強調表示されて

おり、選択された原因または結果が温度センサの示度に対応することを示す。

【００８７】

さらに、ＣＥＭ１３１０またはシステム構成１３２０のいずれかから、エンジニアは、ＳＲＳ１３３０等のプロセスプラントの安全プロトコルを説明する文書にアクセスすることができる。図１３は、関連する安全プロシージャを説明するアイコン１３３１及びテキスト１３３２を含む安全要求仕様の一部分の例示的な表示１３３０を例示する。ナビゲータアプリケーション１５は、エンジニアが、表示の間をトグルすることを可能にし、以前はアクセスすることが煩雑であって情報及び洞察をエンジニアに提供する。さらに、インターフェース１３１０、１３２０、及び／または１３３０のうちの任意の１つから、ユーザは、（例えば、ＣＥＭ１３１０の）関連する選択された要素を実装する論理を含む一組の監視及び結果ブロック（または他の機能ブロックもしくは論理）を表示するユーザインターフェース１３４０にアクセスすることができる。

【００８８】

例示的な一実施形態において、エンジニアは、ＣＥＭ１３１０（またはＳＲＳ１３３０、システム構成１３２０、または監視及び結果ブロック１３４０）の要素を右クリックして、ドロップダウンメニューにアクセスすることができる。ドロップダウンメニューは、他の表示ビュー（１３１０、１３２０、１３３０、及び１３４０等）及び／または（下の図１６Ａ～Ｄに関して説明されるような）他のビューのうちの１つにアクセスする能力を含むオプションをエンジニアに提供することができる。

【００８９】

ユーザは、ＣＥＭ１３１０から（またはＣＥＭ１３１０の個々のセル、原因、または結果から）またはシステム構成１３２０から、一般バイパス原理の定義、証明試験要求等の要求仕様（ＳＲＳ１３３０）内の特定のセクション（複数可）まで、容易にナビゲートすることができる。

【００９０】

この機能は、文書の構成と設計との間を行ったり来たりするシームレスな移行を提供して、構成の検証、変化の管理、トラブルシューティング、及び証明試験を容易にする。

【００９１】

図１４は、プロセス制御システムによって制御されるプロセスプラントの安全要求仕様（ＳＲＳ）に含まれる情報へのアクセスを可能にする例示的な方法１４００のブロック図を表す。方法１４００は、サーバまたは別様には任意のタイプの電子デバイスによって容易にすることができ、サーバは、コンテンツを表示するように構成されたユーザインターフェースを備える、またはそれに接続することができる。ＳＲＳは、サーバによってアクセスすることができるメモリに記憶することができる。

【００９２】

方法１４００は、ブロック１４１０から始まり、そこで、サーバは、ＣＥＭをユーザインターフェースに表示することができる。実施形態において、（ＣＥＭ）は、一組の原因及び一組の結果を含む一組の要素を含むことができ、一組の原因の各々は、プロセスプラント内の条件を表すことができ、一組の結果の各々は、プロセスプラント内で行われるべき結果を表すことができる。さらに、一組の原因及び一組の結果のうちの少なくともいくつかは、原因－結果の対として関連され、それによって、対応する結果を、対応する条件の発生に応答して起動させることができる。

【００９３】

ブロック１４２０で、サーバは、ユーザインターフェースを介して、一組の要素のうちの１つの要素の選択を受信することができる。具体的には、サーバは、一組の原因のうちの１つの原因または一組の結果のうちの１つの結果の選択を受信することができる。選択を受信することに応答して、ブロック１４３０で、サーバは、ＳＲＳから、一組の要素のうちの１つの要素と関連付けられた一組の情報にアクセスすることができる。具体的には、サーバは、ＳＲＳから、選択された原因または選択された結果と関連付けられた一組の情報にアクセスすることができる。実施形態によれば、サーバは、ＳＲＳから、選択され

た要素と関連付けられた配管及び計装図（Ｐ＆ＩＤ）、選択された要素と関連付けられた安全計装機能（ＳＩＦ）の説明、または他の情報にアクセスすることができる。

【００９４】

ブロック１４４０で、サーバは、一組の情報をユーザインターフェースに表示することができる。一実施形態において、サーバはまた、ユーザインターフェースを介して、選択された要素と関連付けられた安全論理を表示するように構成されたアプリケーションを開始することもできる。加えて、一実施形態において、サーバは、ユーザインターフェースを介して、ユーザインターフェースに表示される一組の情報の一部分の追加的な選択を受信し、ＳＲＳから、一組の情報の一部分と関連付けられた追加的な一組の情報にアクセスし、そして、追加的な一組の情報をユーザインターフェースに表示することができる。さらに、一実施形態において、サーバは、ユーザインターフェースを介して、ユーザインターフェースに表示される一組の情報の一部分の追加的な選択を受信することができ、一組の情報の一部分は、ＣＥＭの一組の要素のうちの追加的な１つの要素に対応することができ、また、ＣＥＭ及び追加的な要素の指示をユーザインターフェースに表示することができる。

【００９５】

いくつかの実施形態において、大きいＣＥＭは、数千の原因結果の対を含み得る。結果的に、これらの大きいＣＥＭは、数百の監視ブロック、結果ブロック、及び数値表現に分けられ得る。多数のデータ構造にわたって散存する大量の情報のため、ユーザは、プロセス制御システムの安全論理が正確に実装されていることを手動で確認することが不可能であり得る。以前のプロセス制御システムは、構成したプロセス制御システムが必要な安全プロトコルを満たすことを厳格に検証するための手段が欠如していた。換言すれば、以前のシステムは、プロセスプラントの安全を管理するために実装されていたＣＥＭ及び機能ブロックの精度を試験する、いかなる様態も有していなかった。本開示は、プロセスプラントに現在実装されている安全論理を自動的に検証することができるツール（例えば、原因結果分析器ツール１７）を提供する。

【００９６】

１つの態様において、原因結果分析器ツール１７は、プロセスプラント（またはその一部分）の構成を自動的に横断して、構築したままの、または構成したままのシステムの１つ以上の試験ＣＥＭを発生させることができる。一実施形態において、ツール１７は、機能ブロック（すなわち、監視及び結果ブロック）、及びプロセスプラントの現在実装されている安全論理を表す数値表現に基づいて、リバースエンジニアリングを通して試験ＣＥＭを構築することができる。次いで、試験ＣＥＭと、要求定義ＣＥＭ（プロセスプラントによって必要とされる安全論理の正確な表現であることが知られているＣＥＭ）とを比較することができる。この比較は、不一致または他のエラーを明らかにすることができ、次いで、それをユーザに提示することができる。

【００９７】

図１５は、原因結果マトリックスの安全論理を検証するための例示的な方法のブロック図である。ブロック１５１０で、分析器ツール１７は、原因結果マトリックスの安全論理を表す１つ以上の機能ブロックの構成を決定することができる。一実施形態において、機能ブロックは、上で説明したように、入力、出力、及び数値表現を含む監視及び結果ブロックである。原因結果分析器ツール１７は、監視及び結果ブロック（ＭＥＢ）の構成を決定するために、ＭＥＢに実装される論理及び／またはＭＥＢの数値表現等のいくつかの要因を考慮しながら、ＭＥＢの入力及び出力を横断することができる。例えば、ツール１７は、上の図５及び６で説明したように、一組の監視及び結果ブロックを受信することができる。ツール１７は、結果ブロックの出力から開始し、結果ブロックの入力から入力のソース（すなわち、結果ブロックに、及び／または監視ブロックの出力に直接供給される原因）まで横断することができる。ツール１７は、次いで、数値表現に基づいて、監視ブロックの出力を監視ブロックの対応する入力まで追跡することができる。ツール１７は、各原因結果の対の各関係が識別されるまで、各結果について反復的にＭＥＳを横断する、こ

のプロセスを続けることができる。

【００９８】

ブロック１５２０で、ツール１７は、決定した構成に基づいて、試験ＣＥＭを発生させることができる。ツール１７は、監視及び結果ブロックの決定した構成に基づいて、識別した原因結果の対で試験ＣＥＭをポピュレートすることができる。試験ＣＥＭが作成されると、ツール１７は、試験ＣＥＭ３７をデータリポジトリ（図１の構成データベース３２等）に記憶することができる。試験ＣＥＭ３７は、本明細書で説明されるＣＥＭのいずれかとして実装することができる。

【００９９】

ブロック１５３０で、ツール１７は、要求定義ＣＥＭにアクセスすることができる。１つの実施形態において、要求定義ＣＥＭ３５は、データリポジトリ（図１の構成データベース３２等）に記憶することができる。他の実施形態において、ツール１７は、プロセスプラント及びＳＲＳのデバイスの現在の構成、ならびに他の安全文書に基づいて、要求定義ＣＥＭを作成することができる。一実施形態において、要求定義ＣＥＭ３５は、一組の原因及び一組の結果を含むことができ、原因結果の対の関係は、プロセスプラントの安全要求に基づく。要求定義ＣＥＭ３５は、本明細書で説明されるＣＥＭのうちのいずれかとして実装することができる。

【０１００】

ブロック１５４０で、ツール１７は、試験ＣＥＭ３７と、要求定義ＣＥＭ３５とを比較して、任意の不一致があるかどうかを判定することができる。不一致は、試験ＣＥＭ３７から要求定義ＣＥＭ３５までの原因結果の対の間の任意の違いを含むことができる。例えば、原因結果の対は、同じトリガータイプ（例えば、許容、即時、遅延）及び／または同じ論理タイプ（ＡＮＤ／ＯＲ）によって相関していない場合がある。

【０１０１】

ツール１７は、１つ以上の判定した不一致のうちのいずれかを表示することができる。一実施形態において、ツール１７は、図１３及び１６ａ～ｄにおいて説明したようなユーザインターフェースのうちのいずれかに不一致を強調表示することができる。換言すれば、ツール１７は、誤った論理がＣＥＭ、監視及び結果ブロック、ＳＲＳ文書、及び／またはシステム構成ユーザインターフェースに実装されている場所を強調表示することができる。

【０１０２】

図１３及び１４に関して上で論じた機能に加えて、プロセスプラントの１つ以上のデバイス、原因、及び／または結果の状態履歴を見ることも有益であり得る。本発明の別の態様は、プロセス制御システムの安全システムの状態を監視するためのユーザインターフェースビューを提供し、該状態は、典型的に、物理的設備及び／または安全試験結果に基づいているか、または「鍵が付され」、また、様々な原因または結果の現在及び過去の状態を示して、ＣＥＭ論理がプラントにいつ及びどのように実装されているのかを知るいくつかの能力をユーザに提供することができる。例えば、エンジニアは、設備の特定のデバイスもしくは一部、またはそのグループを表示する（図１３に関して上で論じたような）ビューを提示することができ、次いで、さらに、表示ビューに示される、監視されるデバイス／設備の各部の現在及び／または過去の安全状態、原因信号等を提示する（例えば、図１６Ａ～Ｄ）、表示ビューにアクセスするために使用することができる。加えて、または代替的に、安全エンジニアは、プラントの設備の特定の物理的デバイス／一部に対して安全試験を行うことができ、そして、結果を表示ビューに表示することができる（例えば、図１６Ａ～Ｄ）。以前のシステムは、物理的デバイス／設備の多数の異なる表示ビューにアクセスすることを必要とすることなく、または特定の診断を行って試験結果を取得しなければならないことによって、プラントの（またはプラントの所望の領域の）全体的な安全状態をエンジニアが迅速に監視し、アクセスすることを可能にしなかった。以前のシステムは、エンジニアにとって不都合であっただけでなく、緊急的な状況の間に、貴重な時間が失われ、一方で、エンジニアは、対象とする状態データを取得する、または見つける

ために、多数のビューまたは試験の実行を切り抜けなければならない。

【０１０３】

本明細書で説明されるシステム及び方法は、（特定のデバイス、設備、または試験結果ではなく）監視される安全イベントの現在の状態及び／または状態の変化の容易にアクセス可能な表示ビューを提供する。システムは、システム全体または領域全体の安全イベント／入力状態を、単一の表示ビューまたは視覚化にまとめて、経時的な安全イベントの変化を取り込み、安全表示ビュー全体の視覚化した安全イベントをデバイス／設備／試験結果にリンクする。

【０１０４】

「安全イベント」は、監視される条件の論理表現である。例示的な一実施形態において、ＣＥＭの各監視される入力（原因）は、監視される安全イベントとすることができる。加えて、各結果は、監視される安全イベントとすることができる。監視されることが所望される各安全イベントのそれぞれの状態及び／または状態のそれぞれの変化は、安全イベント視覚化ビュー上の異なるオブジェクト／アイテム／グラフィカルアイテムによって表される。例えば、各監視されるイベントは、色付きのドットによって提示することができ、異なる色によって、異なる現在の状態（例えば、赤色－不具合、青色－注意、黒色－ＯＫ）を示す。加えて、または代替的に、例えば異なる色または表現によって、現在の状態の変化を（２進数で、及び／または変化の程度によって）表すことができる。そのような状態及び／または状態の変化は、経時的に取り込み、保存することができる。実際には、表示ビューは、監視されるイベントについて、回転するスナップショットの時間を提供することができ、また、異なるレートで（例えば、２分ごとに、２０分ごとに、２時間ごとに）監視される安全イベントの異なるセクションを含むことができる。

【０１０５】

図１６Ａ～Ｄは、経時的な安全イベントの状態の変化の例示的な説明図である。図１６Ａ～Ｄにおいて、イベントＥ１は、監視される安全イベントである。経時的なＥ１の現在の安全状態は、時間軸に沿った形状のランニングラインとして表示ビュー上に表すことができ、（図１６Ａに表されるような）各形状は、異なる状態を表す。グラフ１６００において、円形は、通常の状態を表し、正方形は、警告的な状態を表し、三角形は、危険な状態を表す。代替的に、経時的なＥ１の安全状態の変化は、変化が生じた時点に基づいて表すことができる。例えば、図１６Ｂにおいて、グラフ１６１０は、「０」によって定常状態（またはいかなる状態変化もないこと）を示し、「－」によって安全状態の低下を示し、「＋」によって安全状態の上昇を示す。安全状態及びその変化は、任意のタイプの数値またはグラフィカル形態で示すことができることを認識されたい。図１６Ｃは、数字として状態を表示するグラフ１６２０を例示し、０からの負の増加は、追加的な状態の低下を表す。所望であれば、安全状態の変化の程度を表すことができる。例えば、グラフのｙ軸は、正常から外れた低下の範囲を示すことができ、経時的な安全状態は、線グラフ、または図１６Ｄのドットの棒グラフ１６３０のように見え得る。加えて、監視されるイベントのドットの色付きランニングラインの単一の線を、ある色から別の色へ緩やかにモーフィング／シェーディングして、安全状態の悪化及び／改善を示すことができる。

【０１０６】

上の実施例は、限定することを意図しておらず、数字、シンボル、色、グラフィックス、及び／または線の任意の組み合わせを表示して、エンジニアが、監視されるイベントの安全レベルを迅速に評価することを可能にすることができる。さらに、状態及び／または様々なイベントの状態の変化は、所望であれば、後処理のために記憶することができる。

【０１０７】

一実施形態では、グラフ１つ以上のグラフを、一緒に及び／または同時に表示することができる。所望の監視されるイベントのグルーピングは、例えば、プラントの領域、機能、（例えば、バッチプロセスの特定の段階中の）特定の条件または要因等によって、接近させて表示することができる。エンジニアは、表示ビューをマスクして、一見するだけで対象の特定の安全イベントを見ることができるようになり得る。

【０１０８】
さらに、視覚化は、より抽象的な安全イベントを提供することができる。上で論じたように、監視される安全イベントは、監視及び結果ブロック等の、監視されるイベントのグループの抽象化とすることができる。
【０１０９】
例えば、図５及び６を参照すると、イネーブラまたは結果ブロックＥＢ１及びＥＢ２への直接入力が、監視される安全イベントであり得、及び／または結果ブロックＥＢ１及びＥＢ２の各結果Ｅ１、Ｅ２等が、監視される安全イベントであり得る。各所望の監視されるイベントが含まれる条件または入力の各々は、その状態の変化の程度に寄与し得る。例えば、イベントをトリガーするために、監視されるイベントが４つの条件を必要とする場合、１つの条件が存在するときに、監視されるイベントの状態は、「－１」であり得、２つの条件が存在するときに、監視されるイベントの状態は、「－２」であり得、３つの条件が存在するときに、監視されるイベントの状態は、「－３」であり得、４つ全ての条件が存在するときに、状態は「Ｘ」または「トリップ済」であり得る。したがって、一例として、図１６Ａ～１６Ｄのシンボル、数字、ドット等は、結果の（または原因の）異なる可能な状態を表すことができ、または設定される原因の数、または設定する必要がある原因の総数を外れた真状態である、もしくは結果信号をトリップまたは開始するために真状態である原因の数を表すことができる。
【０１１０】
さらに、特定の安全状態または状態変化インジケータのクリックまたは他のユーザ指示は、ユーザを、対応する条件（複数可）の詳細へ自動的にリンクすることができる。上で説明したように、エンジニアは、安全イベント視覚化グラフから、ＳＲＳ、システム構成、及び／またはＣＥＭの表示にアクセスすることができる。例えば、監視されるイベントをトリップすることが必要である４つの条件の上の例を参照すると、上の例のグラフ１６２０の監視されるイベントについて安全視覚化が「－１」を示し、ユーザが「－１」をクリックした場合、「－１」の安全状態に対応する条件を生じさせる設備のデバイスまたは一部を含むシステム構成の表示ビューを表示することができる。
【０１１１】
図１７は、プロセスプラント内の安全イベントを視覚化する例示的な方法１７００のブロック図を表す。方法１７００は、サーバまたは別様には任意のタイプの電子デバイスによって容易にすることができ、サーバは、コンテンツを表示するように構成されたユーザインターフェースを備える、またはそれに接続することができる。
【０１１２】
方法１７００は、サーバが、一組の原因及び一組の結果を有するＣＥＭにアクセスする（ブロック１７１０）ときに開始することができる。実施形態において、一組の原因の各々は、プロセスプラント内の条件を表すことができ、一組の結果の各々は、プロセスプラント内で行われるべき結果を表すことができる。さらに、一組の原因及び一組の結果のうちの少なくともいくつかは、原因－結果の対として関連され、それによって、対応する結果を、対応する条件の発生に応答して起動させることができ、一組の原因及び一組の結果は、プロセスプラント内の一組の監視される安全イベントを表すことができる。
【０１１３】
サーバは、ユーザインターフェースを介して、一組の監視される安全イベントのうちの１つの監視される安全イベントの選択を受信することができる（ブロック１７２０）。さらに、サーバは、監視される安全イベントの指示及び監視される安全イベントの現在の状態をユーザインターフェースに表示することができる（ブロック１７３０）。実施形態において、サーバは、１つ以上の第１のグラフィカルオブジェクトとして現在の状態を表示することができる。
【０１１４】
サーバは、監視される安全イベントの状態の変化を検出することができる（ブロック１７４０）。一実施形態において、サーバは、期間の終了に応答して、状態の変化を検出す

ることができる。サーバはまた、状態の変化に従って、監視される安全イベントの更新された状態をユーザインターフェースに表示することもできる（ブロック１７５０）。実施形態において、サーバは、１つ以上の第１のグラフィカルオブジェクトと異なり得る１つ以上の第２のグラフィカルオブジェクトとして、更新された状態を表示することができる。さらに、実施形態において、サーバは、現在の状態と、監視される安全イベントの更新された状態との間の変化の程度を判定することができ、また、変化の程度をユーザインターフェースに表示することができる。

【０１１５】

一実施形態において、サーバは、さらに、期間の終了に応答して、監視される安全イベントの更新された状態が変化しなかったと判定することができ、また、監視される安全イベントの更新された状態をユーザインターフェースに表示することができる。加えて、または代替的に、サーバは、ユーザインターフェースを介して、監視される安全イベントの更新された状態の選択を受信することができ、監視される安全イベントは、一組の関連付けられた条件を有することができ、また、一組の関連付けられた条件の各々の条件状態をユーザインターフェースに表示することができる。加えて、または代替的に、サーバは、ユーザインターフェースを介して、監視される安全イベントの更新された状態の選択を受信することができ、監視される安全イベントは、存在する関連付けられた条件を有することができ、また、存在するべき関連付けられた条件を生じさせているプロセスプラント内のデバイスの指示をユーザインターフェースに表示することができる。

【０１１６】

加えて、または代替的に、サーバは、監視される安全イベント、監視される安全イベントの現在の状態、及び監視される安全イベントの更新された状態を表すデータをメモリに記憶することができる。さらに、加えて、または代替的に、サーバは、（ｉ）一組の監視される安全イベントのうちの追加的な１つの監視される安全イベントの追加的な指示、及び（ｉｉ）追加的な監視される安全イベントの追加的な現在の状態をユーザインターフェースに表示し、追加的な監視される安全イベントの状態の追加的な変化を検出し、また、追加的な状態の変化に従って、追加的な監視される安全イベントの追加的な更新された状態をユーザインターフェースに表示することができる。

【０１１７】

上で提供した例示的なＣＥＭは、例示の目的であることを意図する、単純な表現である。図１８は、時間遅延トリガー、許容トリガー、即時トリガー、及びリセットトリガーを含む、より複雑なＣＥＭである、例示的なＣＥＭ１８００を例示する。ＣＥＭ１８００は、現実のＣＥＭのより正確な表現である、ＣＥＭのより実質的な一実施例である。図１８に例示されるようなＣＥＭ１８００において、「Ｘ」のみを含むセルは、即時トリガーの結果を表すことができる。さらに、「Ｒ」のみでポピュレートされた任意のセルは、原因を受信した場合に、リセットするように結果がトリガーされることを表すことができる。文字「Ｔ」で始まるＣＥＭ１８００のセルは、原因が結果を直接トリガーするが、ある時間遅延を伴うことを示すことができる。時間遅延は、所定の増分に設定することができる。例えば、「Ｔ１」が１０秒の時間遅延に対応することができ、「Ｔ２」が２０秒の時間遅延に対応することができる、等である。

【０１１８】

ＣＥＭ１８００はまた、数字のみを含むセルも含み、それによって、これらのセルは「イネーブラ」に対応することができる。具体的には、セルの数字は、イネーブラが属するグループを識別し、各グループについて１つ以上のイネーブラが存在し得る。数字で始まるだけでなく、かつ他の文字も有するＣＥＭ１８００のセルは、イネーブラもトリガーされる場合に、結果のみをトリガーする関係を表すことができる。いくつかの実施形態において、対応するイネーブラ（または複数のイネーブラ）に関連するあらゆるセルは、トリガーされるべき結果について「オン」でなければならない。他の実施形態において、特定のイネーブラグループの原因の任意の組み合わせを組み合わせて、結果をトリガーすることができる。同様に、イネーブラの任意の組み合わせは、結果をトリガーすることを必要

とし得る。

【０１１９】

例えば、図１８に例示されるようなＣＥＭ１８００において、原因１８０１は、グループ１のイネーブラである。したがって、原因１８０２がトリップされる場合、対応する結果は、原因１８０１もトリップされない限り、トリガーされ得ない。この原因結果関係は、イネーブラが「オン」である場合にのみ結果がトリガーされるので、許容関係とみなされる。この実施例を続けると、セル１８０３は、原因結果関係がイネーブラグループ１に属すること、及び原因信号１８０２が高くなり、かつイネーブラ原因信号１８０１も高いまたはオンであるときに、長さＴ１に対応する時間遅延を伴って結果１８０５がトリガーされることを示す。セル１８０４は、原因結果関係が、許容であり、かつイネーブラグループ１に属すること、ならびに原因信号１８０２が有効にされ（すなわち、原因信号１８０１がオンである）かつトリップされた場合に、結果１８０６が即時にトリガーされることを示す。

【０１２０】

ＣＥＭ１８００は、上で説明した以前の方法７００、１０００、１２００、１４００、１５００、及び１７００の全てに実装することができる。さらに、ＣＥＭまたはＣＥＭの論理を実装するための本明細書で説明される監視及び結果ブロックは、例えばＣＥＭ１８００の複雑な論理機能及び相互に関係する論理機能を、または他のＣＥＭの任意の他の論理機能を実装するために使用することができる。ＣＥＭ１８００の付加的な複雑さにもかかわらず、依然として、ＣＥＭを管理する利点を適用する。さらに、例示的なＣＥＭは、限定することを意図しておらず、上で説明した方法７００、１０００、１２００、１４００、１５００、及び１７００のうちのいずれかを、安全論理をプロセスプラントに実装するために使用される原因結果マトリックスの任意の将来の実施形態と共に実装することができる。

【０１２１】

図７、１０、１２、１４、１５、及び１７の方法７００、１０００、１２００、１４００、１５００、方法１７００の各々は、ソフトウェア、ファームウェア、もしくはハードウェア、またはソフトウェア、ファームウェア、及び／もしくはハードウェアのいくつかの組み合わせによって実装することができる。加えて、図７、１０、１２、１４、１５、１７のフロー図は、ルーチンとして説明したが、これらのフロー図は、ソフトウェア、ハードウェア、ファームウェア、またはソフトウェア、ファームウェア、及び／もしくはハードウェアの組み合わせによって実装することができる。

【０１２２】

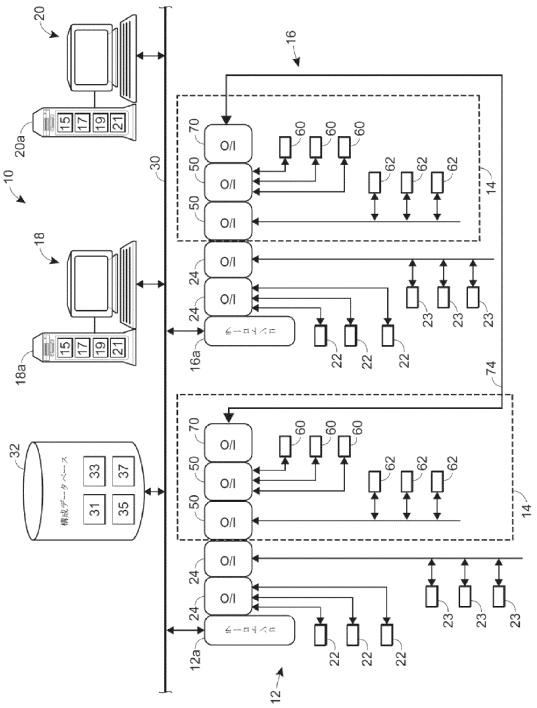
上で説明したユーザインターフェース等のユーザインターフェースの実施形態は、全体的または部分的に、例えばソフトウェアプログラムに従って構成された、プロセッサによって実装することができる。例えば、ワークステーション１８ａもしくは２０ａ、またはいくつかの他のコンピュータは、全体的または部分的に、上で説明したユーザインターフェースを実装することができる。ユーザインターフェースの実施形態を実装するためのソフトウェアプログラムは、ハードディスク、ＲＡＭ、バッテリバックアップされたＲＡＭ、ＲＯＭ、ＣＤ－ＲＯＭ、ＰＲＯＭ、ＥＰＲＯＭ、ＥＥＰＲＯＭ、ＤＶＤ、フラッシュメモリ等の有形媒体に、またはプロセッサと関連付けられたＲＡＭ等のメモリに記憶されたソフトウェアに具現化することができるが、当業者は、プログラム全体またはその一部を、代替的に、プロセッサ以外のデバイスによって実行すること、ならびに／または既知の様態でファームウェア及び／もしくは専用のハードウェアに具現化することができることを容易に認識するであろう。

【０１２３】

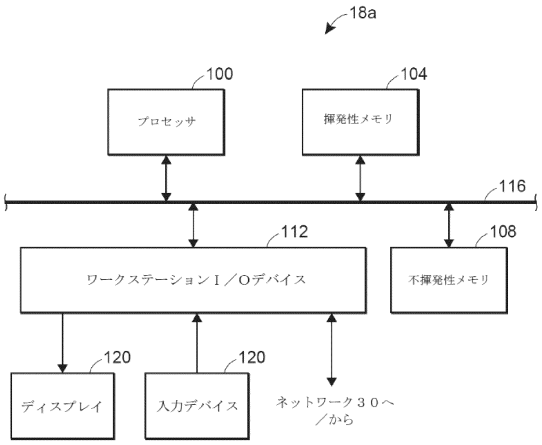
本発明は、様々な修正物及び代替の構成物が可能であるが、本発明の特定の例示的な実施形態は、図面に示され、本明細書に詳細に記載される。しかしながら、本発明を、開示される特定の形態に限定することは意図しておらず、それとは逆に、添付の特許請求の範囲によって定義されるような本開示の趣旨及び範囲の範囲内に入る全ての修正物、代替の

構成物、及び均等物を網羅することを意図することを理解されたい。

【図１】




【図２】



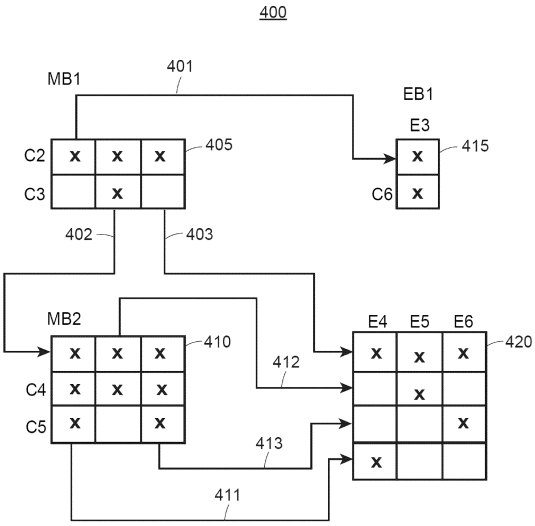
【図３】

| | 結果1 | 結果2 | 結果3 | 結果4 | 結果5 | 結果6 | 結果7 |
|---|---|---|---|---|---|---|---|
| 原因1 | | | | | | | |
| 原因2 | | | X | X | X | | |
| 原因3 | | | | X | | | |
| 原因4 | | | | X | X | X | |
| 原因5 | | | | X | | X | |
| 原因6 | | | X | | | | |
| 原因7 | | | | | | | |

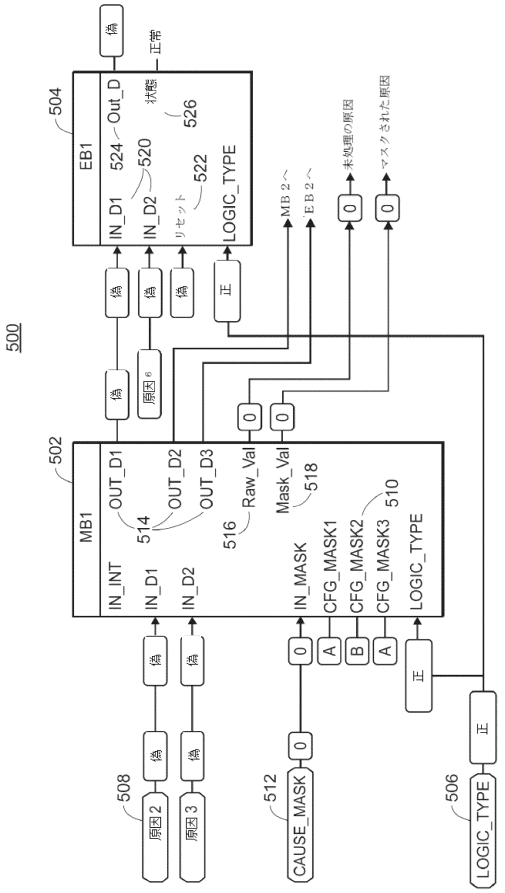
305

310

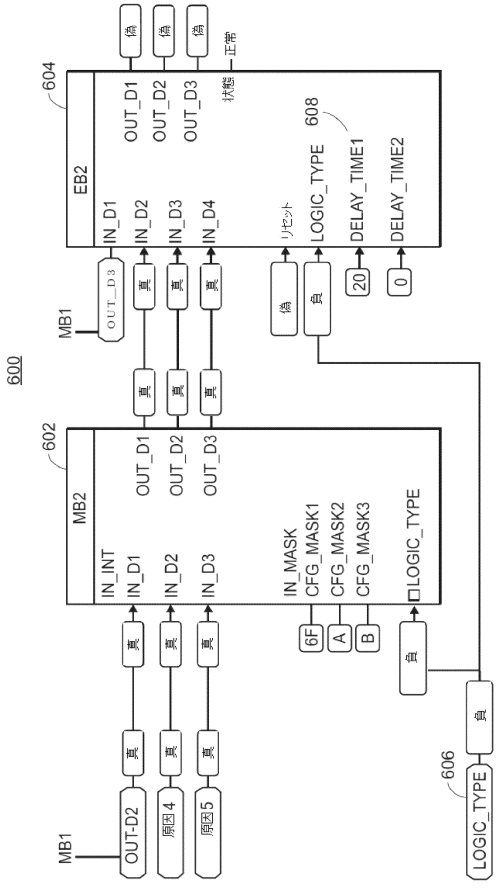
【図４】



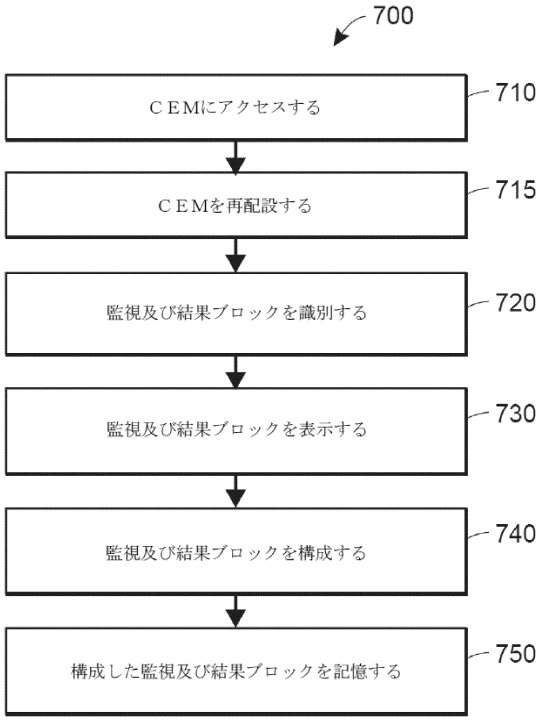

【図５】




【図６】



【図７】

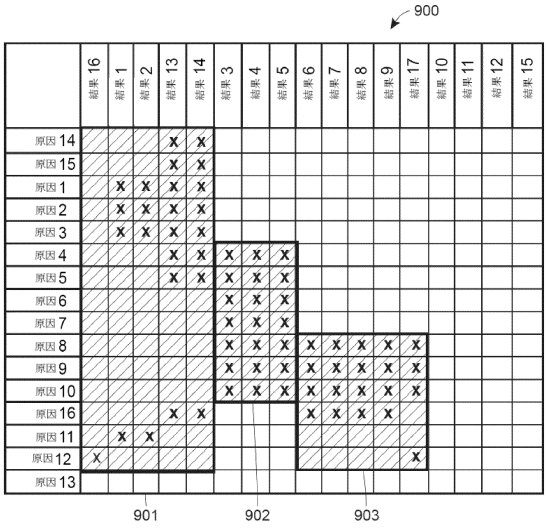



【図８】

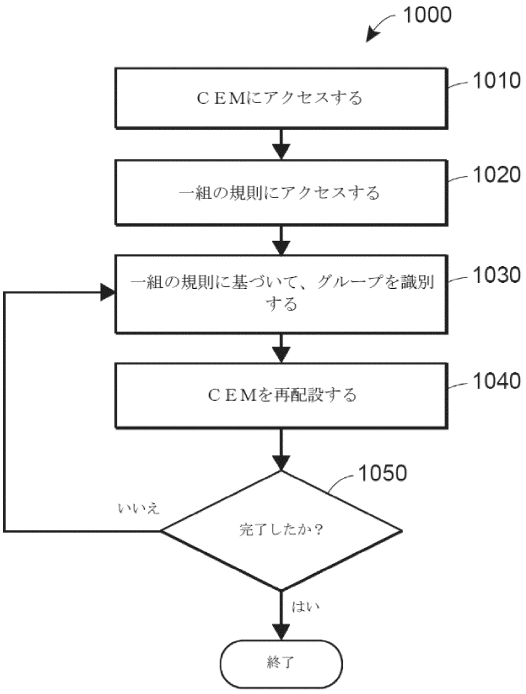
800

| | 結果1 | 結果2 | 結果3 | 結果4 | 結果5 | 結果6 | 結果7 | 結果8 | 結果9 | 結果10 | 結果11 | 結果12 | 結果13 | 結果14 | 結果15 | 結果16 | 結果17 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 原因1 | x | x | | | | | | | | | | | x | x | | | |
| 原因2 | x | x | | | | | | | | | | | x | x | | | |
| 原因3 | x | x | | | | | | | | | | | x | x | | | |
| 原因4 | | | x | x | x | | | | | | | | x | x | | | |
| 原因5 | | | x | x | x | | | | | | | | x | x | | | |
| 原因6 | | | x | x | x | | | | | | | | | | | | |
| 原因7 | | | x | x | x | | | | | | | | | | | | |
| 原因8 | | | x | x | x | x | x | x | x | | | | | | | | x |
| 原因9 | | | x | x | x | x | x | x | x | | | | | | | | x |
| 原因10 | | | x | x | x | x | x | x | x | | | | | | | | x |
| 原因11 | x | x | | | | | | | | | | | | | | | |
| 原因12 | | | | | | | | | | | | | | | | x | x |
| 原因13 | | | | | | | | | | | | | | | | | |
| 原因14 | | | | | | | | | | | | | x | x | | | |
| 原因15 | | | | | | | | | | | | | x | x | | | |
| 原因16 | | | | | | x | x | x | x | | | | x | x | | | |

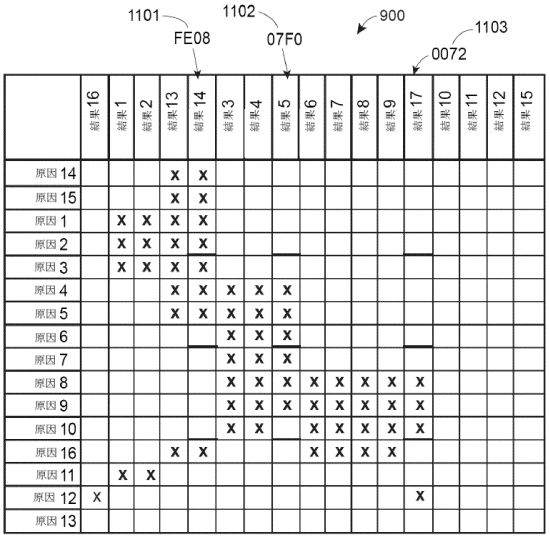
【図９】



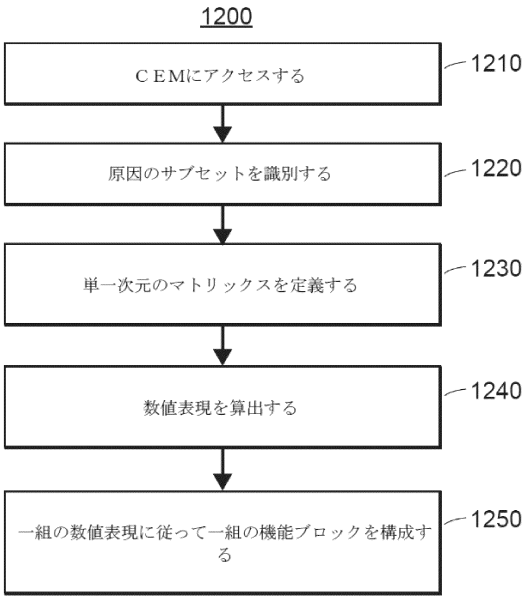

【図１０】



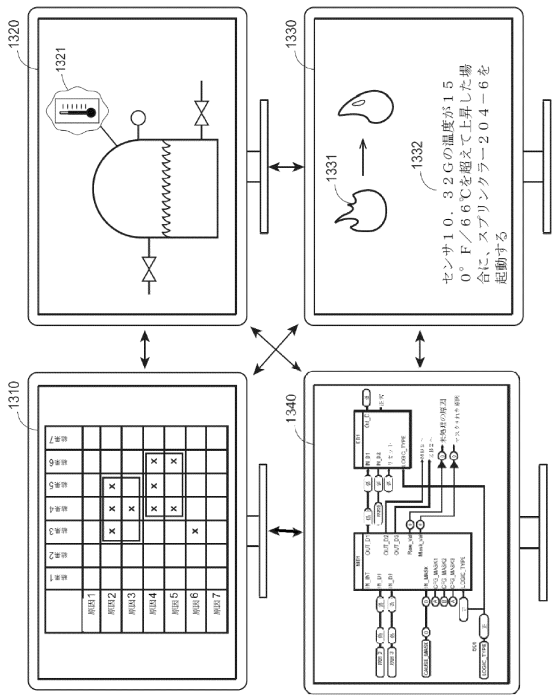
【図１１】



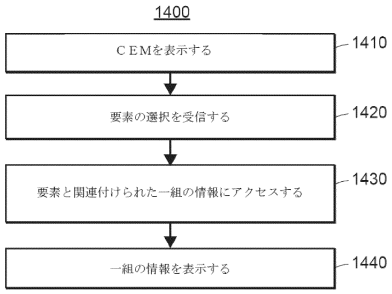

【図１２】



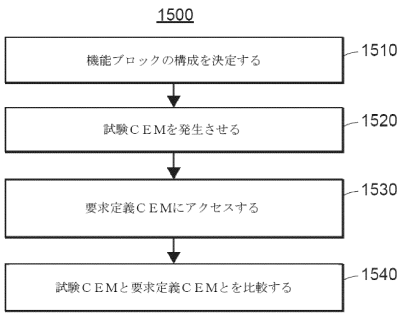

【図１３】



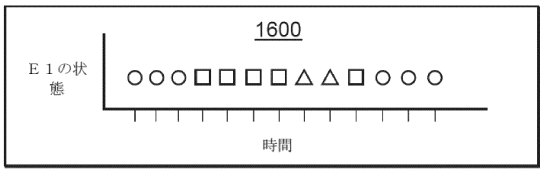

【図１４】



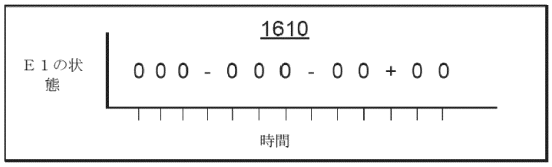

【図１５】



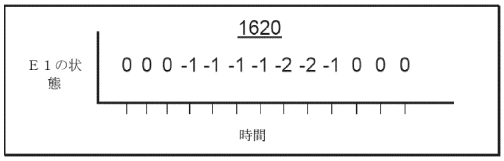
【図１６Ａ】



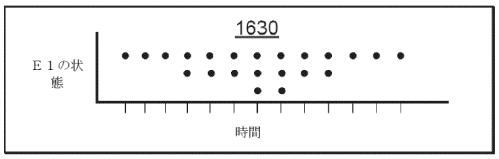

【図１６Ｂ】



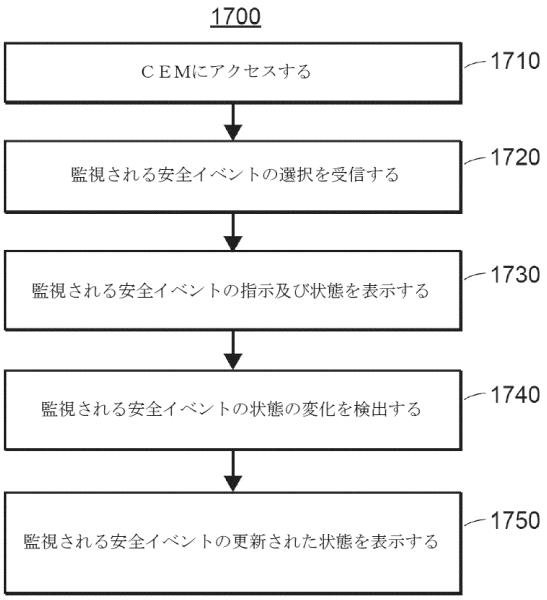

【図１６Ｃ】



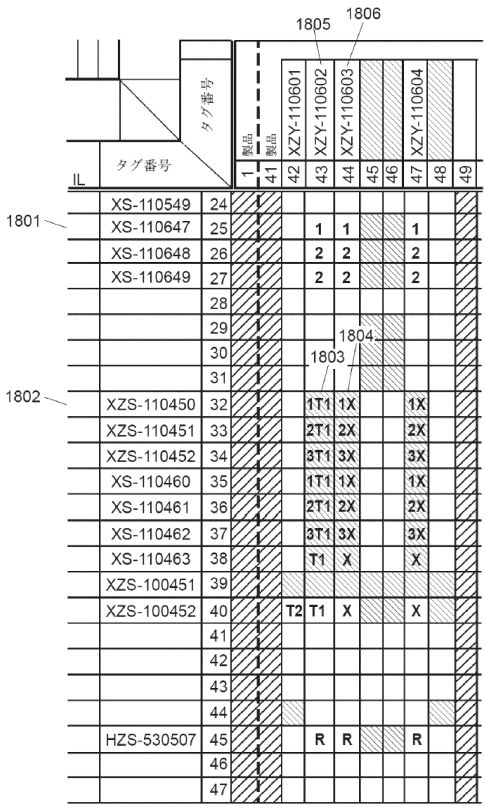

【図１６Ｄ】




【図１７】




【図１８】



フロントページの続き

(72)発明者 ロウ, ゲーリー ケー.
アメリカ合衆国 テキサス ７８６３３ ジョージタウン ミシェル コート １１０
(72)発明者 シェリフ, ゴッドフリー アール.
アメリカ合衆国 テキサス ７８７１７ オースチン ウエスト ドーマン ドライブ １６４１０

審査官 中田 善邦

(56)参考文献 米国特許第０６３６９８３６（ＵＳ，Ｂ１）
特開２００８－３１０４７９（ＪＰ，Ａ）
米国特許出願公開第２００６／０１６８１８３（ＵＳ，Ａ１）
特開２０１５－０１８５５３（ＪＰ，Ａ）
特開２０１０－１９８５６２（ＪＰ，Ａ）
米国特許出願公開第２００２／０１９８９０７（ＵＳ，Ａ１）
米国特許出願公開第２００４／０１９３２９０（ＵＳ，Ａ１）
FISCHER S.,LOHMANN S., ENGELL S., Neutral Representation, Visualization and Verification of Logic Controllers Represented by Funtion Block Diagrams, 2nd IFAC Workshop on Dependable Control of Discrete Systems DCDS'09, IFAC, ２００９年 ６月１０日, pp.40-45

(58)調査した分野(Int.Cl., ＤＢ名)
Ｇ０５Ｂ２３／００－２３／０２