

明 細 書

発明の名称： 検証処理装置、ロジック生成装置及び検証処理方法

技術分野

[0001] 本発明は、検証処理装置、ロジック生成装置及び検証処理方法に関する。

本願は、2018年1月17日に日本に出願された特願2018-005995号について優先権を主張し、その内容をここに援用する。

背景技術

[0002] 従来、リレーを用いるリレー論理回路が、各種制御システムで利用されている。リレー論理回路の基本動作の検証は、回路シミュレータなどの検証処理装置で実施されており、その論理的な動作の信頼度が確保されている。ただし、リレー論理回路内の接続線等への混触や同回路を形成する素子の故障などの不具合が発生した場合の検証は、想定すべき事象が多くなることから実施が困難なことがある。

[0003] 特許文献1には、半導体LSI回路の設計において、半導体LSI回路が達成すべき機能要件の検証を行う際に、モデル検査手法に代表される形式手法を用いることが記載されている。

先行技術文献

特許文献

[0004] 特許文献1：特開2008-71135号公報

発明の概要

発明が解決しようとする課題

[0005] 上述した特許文献1によれば、その回路が達成すべき機能要件を検証することとして、平常時に達成すべき基本機能の性能検査を実施することが開示されているが、不具合事象が生じた平常時とは異なるときに安全性が確保されるのかを確認することまでの開示は無い。

この発明は、上記事情を鑑みてなされたものであり、リレーを用いるリレー論理回路において、不具合事象が生じたときの安全性を検証可能にする検

証処理装置、ロジック生成装置及び検証処理方法を提供することを目的の一つとする。

課題を解決するための手段

[0006] 上記の課題を解決するために以下の構成を採用する。

この発明の第一態様によれば、検証処理装置は、検証対象のリレー論理回路が前記リレー論理回路を形成するリレー、素子および接続線に対応する変数を変数にとり論理式で示される評価式であって、少なくとも前記リレー論理回路に不具合事象が生じた場合の前記論理式を含む評価式で示された回路ロジックモデルを取得する取得部と、前記回路ロジックモデルに基づいて、前記素子または前記接続線に不具合事象が生じた場合に前記リレーの出力の論理状態を判定する判定部とを備える。

このように構成することで、検証対象のリレー論理回路が前記リレー論理回路を形成するリレー、素子および接続線に対応する変数を変数にとり論理式で示される評価式であって、少なくとも前記リレー論理回路に不具合事象が生じた場合の前記論理式を含む評価式で示された回路ロジックモデルを取得することができる。そのため、リレー論理回路に不具合事象が生じた場合の論理式を含む評価式で示された回路ロジックモデルを取得できる。さらに、前記回路ロジックモデルに基づいて、前記素子または前記接続線に不具合事象が生じた場合に前記リレーの出力の論理状態を判定することができる。

したがって、リレーを用いるリレー論理回路において、不具合事象が生じたときの安全性を検証できる。

[0007] この発明の第二態様によれば、第一態様に係る検証処理装置において、前記論理式の変数は、前記検証対象の経路上の素子および接続線の導通状態が正論理で示され、前記不具合事象が生じた場合の前記論理式には、前記検証対象の経路上の素子を示す変数および前記検証対象の経路上の接続線を示す変数の論理積演算を示す論理式が含まれている。

このように構成することで、接続線の断線を論理式に表すことができ、接続線の断線による不具合事象が生じたときの安全性を検証できる。

[0008] この発明の第三態様によれば、第一態様に係る検証処理装置において、前記検証対象のリレー論理回路に含まれるリレーの評価式は、前記リレーの評価式の演算結果を前記リレーの変数の値にするように記述されている。

このように構成することで、素子の障害を論理式に表すことができ、素子の障害による不具合事象が生じたときの安全性を検証できる。

[0009] この発明の第四態様によれば、第三態様に係る検証処理装置において、前記論理式の変数は、前記検証対象の経路上の素子および接続線の導通状態が正論理で示され、前記リレーの評価式が、前記リレーが設けられた経路上の前記素子を示す変数および前記接続線を示す変数の論理積演算を含む第1の式と、前記リレーが設けられた経路のうち、前記経路上で短絡が生じ得る地点の素子または接続線と前記リレーとの間の経路上に存在する素子および接続線を解析対象にして前記解析対象の素子を示す変数および前記解析対象の接続線を示す変数の論理積演算を含む第2の式と、を含み、前記第1の式と前記第2の式の論理和演算を含む。

このように構成することで、素子の短絡を論理式に表すことができ、素子の短絡による不具合事象が生じたときの安全性を検証できる。

[0010] この発明の第五態様によれば、第四態様に係る検証処理装置において、前記リレーが設けられた経路が、前記リレーの制御電圧が印加される給電線から前記給電線に対する接地極までの間を接続可能に形成された経路である。

このように構成することで、給電線から前記給電線に対する接地極までの間を接続可能に形成された所定の経路の構成を論理式に表すことができ、上記の所定の経路において不具合事象が生じたときの安全性を検証できる。

[0011] この発明の第六態様によれば、第一から第五態様のいずれかに係る検証処理装置において、前記素子および接続線のそれぞれに関連付けて、当該素子または接続線の第1の端に接続される素子または接続線と、当該素子または接続線の第2の端に接続される素子または接続線とに関連するデータを格納した素子一覧表に基づいて、前記回路ロジックモデルを生成するロジック生成部をさらに備えている。

このように構成することで、上記の素子一覧表に基づいて、上記の回路ロジックモデルを生成することができ、上記の回路ロジックモデルに基づいて不具合事象が生じたときの安全性を検証できる。

- [0012] この発明の第七態様によれば、第六態様に係る検証処理装置において、前記ロジック生成部は、前記リレーの制御電圧が印加される給電線の接続点と、前記給電線に係る電源との関係を示すデータを格納する給電定義表に基づいて、前記回路ロジックモデルを生成する。

このように構成することで、上記の給電定義表から生成された回路ロジックモデルに基づいて不具合事象が生じたときの安全性を検証できる。

- [0013] この発明の第八態様によれば、ロジック生成装置は、検証対象のリレー論理回路を形成するリレー、素子および接続線を変数にとる論理式で示される評価式であって、少なくとも前記リレー論理回路に不具合事象が生じた場合の前記論理式を含む評価式で示された回路ロジックモデルを、前記素子および接続線の互いの接続関係を示す一覧表のデータに基づいて生成するロジック生成部を備える。

このように構成することで、検証対象のリレー論理回路を形成するリレー、素子および接続線を変数にとる論理式で示される評価式であって、少なくとも前記リレー論理回路に不具合事象が生じた場合の前記論理式を含む評価式で示された回路ロジックモデルを、前記素子および接続線の互いの接続関係を示す一覧表のデータに基づいて生成することにより、リレーを用いるリレー論理回路において、不具合事象が生じたときの安全性を検証可能になる。

- [0014] この発明の第九態様によれば、検証処理方法は、検証対象のリレー論理回路が前記リレー論理回路を形成するリレー、素子および接続線を変数にとる論理式で示される評価式であって、少なくとも前記リレー論理回路に不具合事象が生じた場合の前記論理式を含む評価式で示された回路ロジックモデルを取得する工程と、前記回路ロジックモデルに基づいて、前記素子または前記接続線に不具合事象が生じた場合に前記リレーの出力の論理状態を判定す

る工程とを含む。

このように構成することで、リレーを用いるリレー論理回路において、不具合事象が生じたときの安全性を検証できる。

発明の効果

[0015] 上記した検証処理装置、ロジック生成装置及び検証処理方法によれば、リレーを用いるリレー論理回路において、不具合事象が生じたときの安全性を検証できる。

図面の簡単な説明

[0016] [図1]第1の実施形態の検証処理装置の概略構成を示す構成図である。
[図2]この発明の実施形態における検証処理の手順を示すフローチャートである。
[図3]この実施形態における検証処理を説明するための図である。
[図4]図3に示した接続形態に対応する回路ロジックの一例を示す図である。
[図5]この実施形態におけるモデル検査コードの一例を説明するための図である。
[図6]第2の実施形態の検証処理装置の概略構成を示す構成図である。
[図7]この実施形態におけるより複雑なリレー論理回路の一例を示す図である。
[図8]図7に示したリレー論理回路の電源系の構成を示す給電定義表について説明するための図である。
[図9]図7に示したリレー論理回路の素子一覧表を示す図である。
[図10]この実施形態の断線診断用の論理式の生成処理のフローチャートである。
[図11]この実施形態の同一の接続点を抽出する処理について説明するための図である。
[図12]この実施形態の接続点情報の自動作成処理について説明するための図である。
[図13]この実施形態における論理式を示す図である。

発明を実施するための形態

[0017] 次に、この発明の実施形態における検証処理装置を図面に基づき説明する。

なお、以下の説明において、電氣的に接続されることを単に「接続される」ということがある。また、コンピュータプログラムのソースコードのことを単に「コード」ということがある。後述する「モデル検査コード」は、上記の「コード」の一例である。

[0018] なお、以下の実施形態における検証処理装置は、不安全事故が発生した場合の事象について、所定の検査式を用いて検査する。例えば、上記の検査式は、「リレー素子Aとリレー素子Bが共にONの場合は、必ずアラーム信号を発生させる素子CがONになること」という検査を論理演算式で定義される。このような検査の表現方法として、時相論理がある。「linear temporal logic(LTL)」「Computational Tree Logic(CTL)」などは、時相論理の一例である。また、実施形態における検証処理装置は、ロジック生成装置の一例である。

[0019] (第1の実施形態)

図1は、この実施形態の検証処理装置の概略構成を示す構成図である。

図1に示すように、この実施形態における検証処理装置1は、記憶部10と、制御部20とを備える。

[0020] 記憶部10は、評価式DB11と、評価条件DB12と、検査式DB13と、コードDB14に関するデータを格納する。

[0021] 評価式DB11には、評価対象のリレー論理回路に関する評価式に関するデータが含まれる。評価式は、検証対象のリレー論理回路を形成するリレー、素子および接続線を変数にとり論理式として形成される。この評価式には、少なくともリレー論理回路に不具合事象が生じた場合の論理式が含まれる。例えば、その論理式は、動作の解析対象のリレーごとに生成されている。

[0022] 評価条件DB12には、評価式DB11に格納された評価式を用いる解析処理を実施するに当たり、その評価条件と、その評価条件に基づいた解析の結果とに関するデータが含まれる。例えば、評価条件には、解析処理の種別

を規定するデータが含まれていてもよい。

- [0023] 例えば、解析処理の種別には、下記の種別のものが含まれる。第1の種別として、仕様により定まるリレー論理回路の基本的動作を解析するもの。第2の種別として、リレー論理回路に不具合事象が生じた場合の一例として、解析対象の経路の途中で断線が生じた場合について解析するもの。第3の種別として、リレー論理回路に不具合事象が生じた場合の一例として、解析対象の経路の途中で混触が生じた場合について解析するもの。
- [0024] 検証処理装置1における解析要求仕様として、評価条件DB12に解析処理の実行について規定することにより、上記の個々の種別の解析を単独で実施すること、又は組み合わせた解析を実施することを規定することができる。
- [0025] 検査式DB13には、評価対象のリレー論理回路に関する検査項目に対応する検査式に関するデータが含まれる。
- [0026] コードDB14には、評価式DB11に格納された評価式に関するデータに基づいて生成された評価処理用のコード（モデル検査コード）が含まれる。そのモデル検査コードには、上記の評価式その他、評価式の実行に必要とされる前提条件等のデータが格納され、それらを組み合わせた回路ロジックモデルを形成する。その具体的なモデル検査コードの例について後述する。
- [0027] 制御部20は、解析データ設定部21と、検査式設定部22と、コード生成部23と、取得部24と、解析処理部25（判定部）と、表示制御部26とを備える。
- [0028] 解析データ設定部21は、ユーザの操作により又は通信により、外部から検証処理のための解析データを取得する。例えば、解析データ設定部21は、ユーザが作成した評価式を含むデータを取得して、それを評価式DB11に格納する。
- [0029] 検査式設定部22は、ユーザの操作により又は通信により、外部から検証処理のための検査条件に関するデータを取得する。例えば、検査式設定部22は、リレー論理回路に発生する不安全事故を表現する検査式を設定して、

それを検査式DB13に格納する。

- [0030] コード生成部23は、リレー論理回路に不具合事象が生じた場合の論理式を含む評価式を評価式DB11から取得して、その評価式に対応するコード（評価式コード）を生成する。コード生成部23は、リレー論理回路に不具合事象が生じた場合の事象を検査するための検査式を検査式DB13から取得して、その検査式に対応するコード（検査式コード）を生成する。コード生成部23は、その評価式コードと検査式コードとを組み合わせ、上記の評価式に対応するモデル検査コードをコードDB14に追加する。
- [0031] 取得部24は、その評価式に対応するモデル検査コードを、コードDB14から取得する。なお、評価式に対応するモデル検査コードは、回路ロジックモデルの一例である。
- [0032] 解析処理部25は、取得部24によって取得された回路ロジックモデルに基づいた論理解析処理などを実施する。その解析処理は、モデル検査手法を用いるものである。
- [0033] より具体的には、解析処理部25は、評価条件DB12から評価条件に関するデータを取得して、その評価条件に従った検査（解析）を実施する。例えば、検査の工程には、評価条件により規定された種類の解析処理を実施する工程と、解析処理の結果と期待値とを照合する判定処理の工程が含まれる。解析処理部25は、評価条件に規定された検査項目に従って、検査項目ごとの解析処理を実施して、その解析処理の結果を所定の検査式を用いて判定した判定の結果を、検査項目に対応づけて評価条件DB12に格納する。
- [0034] 表示制御部26は、記憶部10に格納されている各種データを加工して可視化するための表示画面のデータを生成する。表示制御部26によって生成される表示画面には、回路ロジックモデルを規定する評価式を含むもの、解析処理の結果に基づいて判定の結果を含むものなどが含まれる。
- [0035] なお、上記のように形成された検証処理装置1は、例えば、リレー論理回路における不具合事象を、その動作の検証の条件に含めることにより、リレー論理回路の状態と不具合事象とを組み合わせ、状態を解析してもよい。上

記の場合には、順序回路型のリレー論理回路についての解析も可能になる。

[0036] なお、評価条件 D B 1 2 に規定する検査項目は、解析処理における検査項目に漏れが無いように、その項目を網羅的に規定するとよい。その項目を網羅的に規定する方法として、解析処理に用いる評価式中の変数の値が、検査項目ごとに互いに異なる変数の組み合わせになるように機械的に自動生成させる方法がある。上記のような方法により、網羅的に検査項目を規定することにより、状態を問わずに発生する任意の事象に対して、リレー論理回路におけるリレーの出力に不安全事故が生じないことを検証することを可能にする。

[0037] 図 2 は、この実施形態における検証処理の手順を示すフローチャートである。最初に、検証処理の概要を説明する。この実施形態では、一部の処理をユーザが実施する。

[0038] まず、ユーザは、リレー論理回路における各素子の接続関係を読み取り（ステップ S 1 1）、各素子の接続関係を整理する。

[0039] 次に、解析データ設定部 2 1 は、複数ある不具合事象の種類の中から、検査対象にする不具合事象の種類（検査対象不具合事象）を、予め定められた規則に従い順に選択する（ステップ S 1 2）。例えば、表示制御部 2 6 は、検査対象にする不具合事象の種類に対応付けられる解析処理の複数の種別を、図示しない表示部に表示させる。ユーザは、表示された解析処理の複数の種別から一又は複数の種別を選択して、選択の結果を検証処理装置 1 に登録する。解析データ設定部 2 1 は、選択の結果に対応する検証条件を、評価条件 D B 1 2 に格納させる。

[0040] 次に、ユーザは、リレー論理回路に不具合事象が生じた場合の事象を検査するための検査式に関するデータを生成して、検証処理装置 1 に登録する。これを受け、検査式設定部 2 2 は、リレー論理回路に発生する不安全事故を表現する検査式を設定して（ステップ S 1 3）、検査式 D B 1 3 に格納させる。

[0041] 次に、ユーザは、各素子の接続関係に基づいて、不具合事象を含めた論理

回路（ロジック）を示すデータを生成して（ステップS 1 4）、検証処理装置 1 に登録する。これを受け、解析データ設定部 2 1 は、ユーザによって生成された評価式のデータを記憶部 1 0 の評価式 D B 1 1 に格納させる。

[0042] 次に、コード生成部 2 3 は、評価式 D B 1 1 に格納されている評価式のデータと、検査式 D B 1 3 に格納されている検査式のデータとに基づいて、モデル検査コードを生成する（ステップS 1 5）。モデル検査コードを生成することを、図 2 において「自動コーディング」と示す。モデル検査コードとは、検証対象の論理回路に対応する評価式を含み、コンピュータが実行可能とするようにプログラムのコードに変換されたものである。後述する図 5 にそのモデル検査コードの一例を示す。

[0043] 次に、取得部 2 4 は、モデル検査コードをコード D B 1 4 から取得する。そのモデル検査コードは、リレー論理回路 2 に不具合事象が生じた場合の論理式を含む評価式で回路ロジックモデルが示されている。解析処理部 2 5 は、生成されたモデル検査コードに基づいて、検査を実行する（ステップS 1 6）。

[0044] 次に、解析処理部 2 5 は、所定の計算時間内に計算が完了していないことを判定する（ステップS 1 7）。所定の計算時間内に計算が完了していない場合には、ステップS 1 2 からの処理を繰り返す。なおその際に、検査対象にする不具合事象の種類を切替えてもよい。

[0045] 所定の計算時間内に計算が完了している場合には、表示制御部 2 6 は、その結果を表示部に表示させることにより、ユーザに判定の結果が良好なものであるかについて解釈させる（ステップS 1 8）。検証処理装置 1 は、上記の手順に従って各処理を実施した後、図に示す一連の処理を終える。

[0046] 続いて、上記の検証処理の手順の各ステップの処理の詳細について、順に説明する。

[0047] 図 3 は、この実施形態における検証処理を説明するための図である。図 3 には、リレー論理回路 2 の接続図が一例として記載されている。この図 3 に示すリレー論理回路 2 には、リレー A と、スイッチ B と、スイッチ C と、電

源部Pとが含まれる。リレーAは、図示しないコイルと接点とを備える。リレーAのコイルと、スイッチBと、スイッチCとが、記載の順に直列に接続されており、直列に接続された回路の第1端（スイッチC側の端）が電源部Pに接続され、第2端（リレーA側の端）が接地極（Ground）に接続される。

- [0048] より詳しく上記の接続を説明すると、電源部Pは、その出力端子が接続線Line111の1端に接続されている。その接続線Line111には、スイッチCの第1端が接続される。スイッチCの第2端には、接続線Line112の一端が接続される。その接続線Line112の他端には、スイッチBの第1端が接続される。スイッチBの第2端には、接続線Line113が接続される。その接続線Line113には、リレーAのコイルの第1端が接続される。リレーAのコイルの第2端には、接地極が接続される。
- [0049] リレー論理回路2を形成する各部には、各部の種類に依存する固有の不具合事象が発生することがある。その不具合事象としては、以下を想定する。
- [0050] 不具合事象が生じ得る対象として、マニュアル操作型のスイッチと、リレー素子と、電源部と、接続線と、ダイオードとについて例示する。上記の各対象に生じ得る不具合事象として、以下のものを想定する。
- [0051] マニュアル操作型のスイッチの操作には、誤操作の虞がある。マニュアル操作型のスイッチの導通状態には、ON状態とOFF状態の何れの状態も取り得るものとする。
- [0052] リレー素子には、機械的接点を有するものと、機械的接点に代えて半導体素子を有するものが有る。ここでは、機械的接点を有するリレー素子の場合を例示する。機械的接点を有するリレー素子には、リレーの接点の溶着と、リレーのコイル側への接触と混触の虞がある。それゆえ、リレーの接点の導通状態（出力状態という。）が、リレーのコイルに掛かる制御電圧に対応する論理状態（ロジックという。）に従う場合と、そのロジックに従わず、ON状態とOFF状態の何れかの状態を取り得る場合の両方の場合が想定されるものとする。上記のロジックとは、リレーの接点の出力状態の期待値になる。

[0053] 電源部には、その出力側に互いに異なる電位の混触と、電源部の出力端子に電氣的に接続される接続線の断線の虞がある。それゆえ、電源部の状態が、定格電圧などの所定の電圧を出力可能な状態（ON状態）と、上記の所定の電圧を出力できない状態（OFF状態）の何れの状態も取り得るものとする。所定の電圧を出力可能な状態（ON状態）には、所定の電流を出力できる状態を含み、所定の電圧を出力できない状態（OFF状態）には、所定の電流を出力できない状態を含むものとする。

[0054] 接続線には、混触と断線の虞がある。そこで、実施形態では、各接続線に対して、論理状態を有する仮想素子を割り付ける。

[0055] なお、図3には図示していないが、ダイオードなどの整流素子（以下、纏めてダイオードという。）には、溶着（素子損傷）による逆流の虞がある。

[0056] 図4は、図3に示した接続形態に対応する論理式（回路ロジック）の一例を示す図である。

図4（a）に、通常時の動作を規定する論理式を示す。図4（a）に示す論理式は、変数として、Aと、Bと、Cと、（Power_100V）とを含む。その論理式は、式（1）のように記述されている。

[0057] $A = B \text{ and } C \text{ and Power_100V} \quad \cdot \cdot \cdot (1)$

[0058] 式（1）における変数Aと、Bと、Cと、（Power_100V）の型（タイプ）は、それぞれ論理型である。例えば、上記の変数Aと、Bと、Cと、（Power_100V）は、それぞれリレーAと、スイッチBと、スイッチCと、電源部Pとに対応づけられている。

[0059] 上記の論理式の内、変数Aは、検証対象のリレーの出力状態を示す。また、変数Bと、Cは、検証対象の経路上の素子の状態を示す。その値は、導通状態（ON状態）が正論理の真値で示される。例えば、各変数は、「0」（偽値）と「1」（真値）の2値の何れかの値をとる。例えば、スイッチB、スイッチC等の接点を有するものが導通状態（ON状態）にある場合の変数の値を「1」に定める。

[0060] 上記の論理式の内、変数（Power_100V）は、電源部Pの出力状態を示す

。その値は、出力状態（ON状態）が正論理の真値で示される。例えば、出力状態（ON状態）にある場合の変数の値を「1」に定める。

[0061] また、式（1）において各変数を繋ぐ「and」は、論理積演算を示す演算子である。この演算式の演算が実施されると、式（1）の右辺側の演算の結果が左辺の変数に代入される。

[0062] 式（1）に示す基本動作を規定する論理式には、検証対象の経路上の素子を示す変数同士の論理積演算を示す論理式が含まれる。基本動作とは、断線、混触などの不具合事象が生じていない場合の動作のことである。

[0063] 上記の式（1）と図3の回路に対応付けると、スイッチBが導通し、スイッチCが導通し、スイッチCに制御用の電力（Power_100V）が電源部P1から供給されている場合に、リレーAのコイルに対して制御電圧が印加される。上記の式（1）は、上記の状況にある場合に、リレーAの接点が閉じて導通することをモデル化したものである。なお、上記以外の状況にある場合には、リレーAの接点が開いて導通しないことを示す。

[0064] 図4（b）と図4（c）とに、図3の回路における不具合事象を想定した論理式（回路ロジック）を示す。次に示す論理式には、少なくともリレー論理回路2に不具合事象が生じた場合の動作を示す要素が含まれる。

[0065] 図4（b）に示す不具合事象を想定した論理式は、混触を想定したものである。

回路内の各接続点（接続線）に混触が発生した場合には、本来、リレーAのコイルに電流が流れない状態にあるべき状況であっても、接続線等の混触により電位が生じたことによって、リレーAのコイルに電流が流れてしまう事象が想定される。

[0066] 前述の図3に示した一例では、接続線Line111、Line112、Line113の3つの接続線が存在する。これらの接続線に混触が生じると仮定すれば、下記する3とおりの事象が発生し得る。3通りの事象とは、接続線Line113の混触と、接続線Line112の混触と、接続線Line111の混触のことである。これらの事象についてモデル化して、次の論理式に表す。

[0067] 例えば、接続線Line113が混触した場合には、リレーAのコイルに電流が流れて作動してしまう場合がある。このような場合は、スイッチBなどの状態によらずにリレーAが作動する。これを次の式（2）に示す。

$$[0068] \quad A = \text{Line113} \quad \cdot \cdot \cdot (2)$$

[0069] また、接続線Line112が混触した場合には、スイッチBがON状態にあるとリレーAのコイルに電流が流れて作動してしまう場合がある。このような場合は、スイッチCの状態によらずにリレーAが作動する。これを次の式（3）に示す。

$$[0070] \quad A = B \text{ and Line112} \quad \cdot \cdot \cdot (3)$$

[0071] また、接続線Line111が混触した場合には、スイッチBとスイッチCの両方がON状態にあるとリレーAのコイルに電流が流れて作動してしまう場合がある。これを次の式（4）に示す。

$$[0072] \quad A = B \text{ and C and Line111} \quad \cdot \cdot \cdot (4)$$

[0073] また、上記の式（2）から式（4）の他に、式（1）に示した基本機能による条件を満たした場合に、リレーAのコイルに電流が流れる。つまり、これらの式（1）から式（4）までの何れかの条件が満たされた場合に、リレーAが作動することになる。この関係を式（5）に示す。式（5）は、式（2）から式（4）までの演算結果の論理和を算出する式である。

$$[0074] \quad A = \text{Line113 or (B and Line112) or (B and C and Line111)} \\ \text{or (B and C and Power_100V)} \quad \cdot \cdot \cdot (5)$$

[0075] 上記の論理式の内、変数Aと、Bと、Cは、上述したように検証対象のリレーと、経路上の素子の状態を示す。上記の論理式の内、変数（ Power_100V ）は、上述したように電源部Pの出力状態を示す。

上記の論理式の内、変数Line113と、Line112と、Line111は、検証対象の経路上の接続線の状態を示すものであり、混触状態（ON状態）が正論理の真値で示される。例えば、各変数は、「0」（偽値）と「1」（真値）の2値の何れかの値をとる。例えば、接続線に混触が生じた場合に、その接続線の変数の値を「1」にする。接続線に混触が生じていない場合に、その接続線の

変数の値を「0」にする。

[0076] なお上記の論理式の内、式（1）が、リレーが設けられた経路上の素子を示す変数および接続線を示す変数の論理積演算を含む第1の式の一例である。また、式（2）から式（4）が、リレーが設けられた経路のうち、その経路上で短絡（混触）が生じ得る地点の素子または接続線とリレーとの間の経路上に存在する素子および接続線を解析対象にして解析対象の素子を示す変数および前記解析対象の接続線を示す変数の論理積演算を含む第2の式の一例である。

[0077] また、式（5）において各項を繋ぐ「or」は、論理和演算を示す演算子である。この式（5）の場合も、前述の式（1）の場合と同様に、演算式の演算が実施されると、式（5）の右辺側の演算の結果が左辺の変数に代入される。

[0078] 図4（c）に、不具合事象として混触と断線を想定した回路ロジックを示す。

回路内の各接続点（接続線）に混触と断線の何れかが発生した場合には、本来、リレーAのコイルに電流が流れない状態にあるべき状況であっても、接続線等に混触が発生したことによって、リレーAのコイルに電流が流れてしまう事象が想定される。また、本来、リレーAのコイルに電流が流れる状態にあるべき状況であっても、接続線等の断線が発生したことによって、リレーAのコイルに電流が流れなくなる事象が想定される。

[0079] 前述の図3に示した一例では、接続線Line111、Line112、Line113の3つの接続線が存在する。これらの接続線に混触と断線の何れかが生じると仮定する。混触については前述したとおりである。ここでは断線について説明する。接続線に断線が生じると、下記する3とおりの事象が発生し得る。3通りの事象とは、接続線Line113の断線と、接続線Line112の断線と、接続線Line111の断線のことである。これらの事象についてモデル化して、次の論理式に表す。

[0080] 例えば、接続線Line113が混触したことにより、接続線Line113が断線して

いなければリレー A のコイルに電流が流れて作動する場合がある。このような場合は、スイッチ B の状態によらずにリレー A が作動する。これを次の式 (6) に示す。

$$[0081] \quad A = (\text{Line113 and DC_Line113}) \quad \cdot \cdot \cdot (6)$$

[0082] なお、上記の式 (6) において、変数 DC_Line113 は、接続線 Line113 の断線の有無を示す変数である。以下同様に変数「DC_Linexxx」は、接続線 Linexxx の断線の有無を示す変数である。例えば、DC_Line113 は、その接続線に断線が生じていない場合には正論理の真値 (TRUE) としての「1」を示し、断線が生じている場合には正論理の偽値としての「0」を示す。

[0083] また、接続線 Line112 が断線していない状態にあり、且つスイッチ B が ON 状態にあると、接続線 Line112 が混触したことにより、リレー A のコイルに電流が流れて作動する場合がある。このような場合は、スイッチ C の状態によらずにリレー A が作動する。これを次の式 (7) に示す。

$$[0084] \quad A = B \text{ and } (\text{Line112 and DC_Line112}) \quad \cdot \cdot \cdot (7)$$

[0085] また、接続線 Line111 が断線していない状態にあり、且つスイッチ B とスイッチ C の両方が ON 状態にあると、接続線 Line111 が混触したことにより、リレー A のコイルに電流が流れて作動する場合がある。これを次の式 (4) に示す。

$$[0086] \quad A = B \text{ and } C \text{ and } (\text{Line111 and DC_Line111}) \quad \cdot \cdot \cdot (8)$$

[0087] また、上記の式 (6) から式 (8) の他に、式 (1) に示した基本動作の条件を満たした場合に、リレー A のコイルに電流が流れる。これらの式 (1) と式 (6) から式 (8) までの何れかの条件が満たされた場合に、リレー A が作動することになる。この関係を式 (9) に示す。式 (9) は、式 (1) と、式 (6) から式 (8) までの演算結果の論理和を算出するものである。

$$[0088] \quad A = (\text{Line113 and DC_Line113}) \\ \text{or } B \text{ and } (\text{Line112 and DC_Line112}) \\ \text{or } B \text{ and } C \text{ and } (\text{Line111 and DC_Line111})$$

or (B and C and Power_100V) . . . (9)

[0089] 上記の論理式の内、変数Aと、Bと、Cと、変数 (Power_100V) と、変数Line113と、Line112と、Line111は、上述したとおりである。上記の論理式の内、変数DC_Line113と、DC_Line112と、DC_Line111は、検証対象の経路上の接続線の導通状態を示すものであり、導通状態 (ON状態) が正論理の真値で示される。例えば、各変数は、素子の場合と同様に「0」 (偽値) と「1」 (真値) の2値の何れかの値をとる。例えば、接続線Line113が導通状態 (ON状態) にある場合に、その接続線の変数の値を「1」にする。接続線Line113が断線状態 (OFF状態) にある場合に、その接続線の変数の値を「0」にする。

[0090] 以上に示したように、不具合事象が生じていない場合、混触 (不具合事象) が生じている場合、混触又は断線などの不具合事象が生じている場合の3通りの検証の事例について説明した。上記の各検証については、前述の図2におけるステップS12の処理のように、「複数ある不具合事象の種類の中から、検査対象にする不具合事象の種類 (検査対象不具合事象) を、予め定められた規則に従い順に選択」して実施するようにしてもよい。

[0091] 次に、上記の検証処理に用いる回路検証用のモデルの具体的な一例について説明する。

[0092] 図5は、この実施形態におけるモデル検査コードの一例を説明するための図である。

この図5に示すモデル検査コードは、論理検証の処理を実施するためのものである。そのモデル検査コードが示す内容によって、下記のように複数のブロックに分けることができる。

[0093] この図5に示す一例では、下記の演算処理を提供するコードが示されている。このコードは、SMV方式の検査手法に準じたものである。

[0094] 第1ブロック (第1行) : メインモジュール (main) の宣言文である。

[0095] 第2ブロック : 各変数の型式を定義するための変数宣言部である。例えば、変数Switch_Bと変数Switch_Cのそれぞれの変数の型式を論理型 (boolean) として定義する。変数Switch_Bは、スイッチBの誤操作があった場合に、不具

合事象の発生を示す論理「1」が設定されるものとして定義される。変数Switch_Cは、スイッチCの誤操作があった場合に、不具合事象の発生を示す論理「1」が設定されるものとして定義される。

- [0096] 第3ブロック：各変数の値を定義するための変数定義部である。図に示す例では、変数Line111の値を、初期値として「1」に固定する。例えば、論理「1」を「TRUE」で示す。図示していないが、論理「0」を「False」で示す。
- [0097] 第4ブロック：本モジュールの演算処理を規定する論理演算部であり、素子の状態を更新する箇所である。以下に示す演算処理は、代入文で記述されている。第4ブロックの1行目の式は、変数Relay_Cの初期値を「False」にするものである。その2行目の式は、変数Relay_Cに、次の条件による値を代入する。この式は、変数Switch_Bと、変数Switch_Cと、変数Line111との全ての変数が論理「1」である場合に、変数Power_100Vが論理「1」である場合に、変数Relay_Cを論理「1」にすることを示す。
- [0098] 第5ブロック：上記の演算処理の結果を判定するための検査式を設定する検査式部である。この例はCTLで記述されている。第5ブロックの2行目の式は、「変数ProcessXがTRUE（真値又は「1」）になった場合に、Relay_CがFALSEであることが、生じることが無い。」ことを要求仕様として規定するものである。例えば、より具体的な事例に当てはめると、緊急信号を発出しなければならない状況（ProcessX=TRUE）になった場合に、緊急信号が発信されない（Relay_C=FALSE）であることが、生じることが無い。」ことを要求仕様として規定することができる。
- [0099] 上記の実施形態によれば、例えば、回路ロジックモデルがモデル検査コードで表現され、それに対する検査式がCTLで記述されている。これにより、リレーを用いるリレー論理回路に代わる回路ロジックモデルを用いることによって、リレー論理回路内の素子または接続線に生じる不具合事象について判定部が検証することが可能になり、上記のリレー論理回路に不具合事象が生じたときの安全性を検証できる。
- [0100] 上記の回路ロジックモデルは、検証対象のリレー論理回路を形成するリレ

一、素子および接続線に対応する変数を変数にとる論理式で示される評価式であって、少なくとも前記リレー論理回路に不具合事象が生じた場合の論理式を含む評価式で示されていることにより、不具合事象が生じた場合に、不安全状態に陥る可能性の解析を可能にする。なお、不安全状態とは、検証対象のリレー論理回路の出力が安全な状態とは異なる状態のことである。例えば、この不安全状態とは、検証対象のリレー論理回路を稼働させているなかで、その出力に発生しないことが望まれる状態のことである。

[0101] (第2の実施形態)

続いて、図2と、図6から図15までの図を参照して、第2の実施形態について説明する。第1の実施形態では、論理検証用のモデルとしての論理検証コードは、ユーザによって生成されたものであったが、本実施形態の論理検証コードは、検証処理装置が生成する。

[0102] 図6は、この実施形態の検証処理装置の概略構成を示す構成図である。

図6に示すように、この実施形態における検証処理装置1Aは、記憶部10Aと、制御部20Aとを備える。

[0103] 記憶部10Aは、評価式DB11と、評価条件DB12と、検査式DB13と、コードDB14と、素子情報DB15と、信号情報DB16とを備える。

[0104] 素子情報DB15 (Dev表) には、検証処理の対象のリレー論理回路に含まれる素子と、その素子の接続関係を示す接続情報とに関する構成情報のデータが含まれる。素子情報DB15の詳細については後述する。

[0105] 信号情報DB16 (Sig表) には、検証処理の対象のリレー論理回路に電力を供給する電源系に関するデータが含まれる。後述する給電定義表は、上記の電源系に関するデータの一例である。信号情報DB16の詳細については後述する。

[0106] 制御部20Aは、解析データ設定部21Aと、コード生成部23と、取得部24と、解析処理部25と、表示制御部26と、ロジック生成部27とを備える。

- [0107] 解析データ設定部 2 1 A は、ユーザの操作により又は通信により、外部から検証処理のための解析データを取得する。例えば、解析データ設定部 2 1 A は、ユーザが作成したデータを取得して、それを素子情報 DB 1 5 と信号情報 DB 1 6 とに格納する。ユーザが作成したデータには、検証処理の対象のリレー論理回路に含まれる素子と、その素子の接続関係を示す接続情報の一覧表と、検証処理の対象のリレー論理回路に電力を供給する電源系に関するデータの一覧表などが含まれる。
- [0108] ロジック生成部 2 7 は、評価式で示された回路ロジックモデルを、前記素子および接続線の互いの接続関係を示す一覧表のデータに基づいて生成する。上記の評価式は、前述したように検証対象のリレー論理回路を形成するリレー、素子および接続線を変数にとる論理式で示されたものであり、少なくともそのリレー論理回路に不具合事象が生じた場合の論理式を含む。
- [0109] なお、コード生成部 2 3 は、ロジック生成部 2 7 が生成したロジック（評価式）をコードに変換する。なお、実施形態ではコード生成部 2 3 とロジック生成部 2 7 とを分けて説明しているが、分けずに一体のものとして形成してもよい。
- [0110] 次に、前述の図 2 を参照して、本実施形態の検証処理の概要について説明する。
- [0111] まず、ユーザは、リレー論理回路における各素子の接続関係を読み取り（ステップ S 1 1）、各素子の接続関係を示すデータを、検証処理装置 1 に登録する。これを受け、解析データ設定部 2 1 は、ユーザによって生成された各素子の接続関係を示すデータを素子情報 DB 1 5 に登録する。例えば、解析データ設定部 2 1 A は、検証処理のためのリレー論理回路の構成情報を、ユーザの操作により又は通信によってその外部の装置等から取得する。例えば、その構成情報には、リレー論理回路から抽出された素子と、その素子の接続関係を示すデータがその素子一覧表に含まれている。この場合、解析データ設定部 2 1 A は、その素子一覧表に関するデータを取得して、素子情報 DB 1 5 に追加する。さらに、解析データ設定部 2 1 A は、同様に、リレー

論理回路のリレーに電力を供給する電源系に関するデータを取得して、信号情報DB16に追加する。

[0112] 次に、解析データ設定部21は、複数ある不具合事象の種類の中から、検査対象にする不具合事象の種類（検査対象不具合事象）を、予め定められた規則に従い順に選択する（ステップS12）。例えば、表示制御部26は、検査対象にする不具合事象の種類に対応付けられる解析処理の複数の種別を、図示しない表示部に表示させる。ユーザは、表示された解析処理の複数の種別から特定の種別を選択して、選択の結果を検証処理装置1に登録する。解析データ設定部21は、その選択の結果を評価条件DB12に格納させる。

[0113] 次に、ユーザは、リレー論理回路に不具合事象が生じた場合の事象を検査するための検査式に関するデータを生成して、検証処理装置1に登録する。これを受け、検査式設定部22は、リレー論理回路に発生する不安全事故を表現する検査式を設定して（ステップS13）、検査式DB13に格納させる。

[0114] 次に、ロジック生成部27は、素子情報DB15のデータと信号情報DB16のデータとに基づいて、不具合事象を含めた論理式（ロジック）を生成する（ステップS14）。論理回路（ロジック）を示すデータの生成について後述する。

[0115] 次に、コード生成部23は、評価式DB11に格納されている評価式のデータと、検査式DB13に格納されている検査式のデータとに基づいて、モデル検査コードを生成する（ステップS15）。

[0116] 次に、解析処理部25は、コード生成部23によって生成されたモデル検査コードに基づいて、検査を実行する（ステップS16）。なお、ステップS17以降の処理は、前述の第1の実施形態における説明を参照する。

[0117] 図7は、この実施形態におけるより複雑なリレー論理回路の一例を示す図である。

この図7に示すリレー論理回路2Aには、リレーR1、R2、R3及びR4と、ダイオードDiode_121及びDiode_121と、スイッチSW_1、SW_2、SW_3、S

W_4、SW_5及びSW_6と、遮断器Breaker、C_1、C_2、R11及びR12と、電源部P 1、P 2、P 3とが含まれる。

[0118] リレーR 1、R 2、R 3及びR 4は、前述のリレーAに相当するものである。

ダイオードDiode_121及びDiode_121は、整流機能を有する半導体である。

スイッチSW_1、SW_2、SW_3、SW_4、SW_5及びSW_6は、前述のスイッチBとC等に相当するものであり、a接点型である。

[0119] 遮断器Breaker、R11及びR12は、所謂遮断器であり、b接点型である。なお、R11及びR12は、リレーの接点であってもよい。

[0120] コンタクタC_1及びC_2は、接続線間を電氣的に接続するものであり、b接点型である。

[0121] 最初に電源系について説明する。図8は、図7に示したリレー論理回路の電源系の構成を示す給電定義表について説明するための図である。図8に示す給電定義表（Sig表）は、電源部、ブレーカ、コネクタ部、接続点等の項目を含む。この給電定義表には、電源系の接続情報が示されている。例えば、給電定義表には、リレーの制御電圧が印加される給電線の接続点と、前記給電線に係る電源との関係を示すデータが格納されている。

[0122] 例えば、給電定義表における電源部の項目には、対応する電源装置の識別情報に関するデータが含まれ、ブレーカの項目には、設けられた遮断器（ブレーカ）を識別する識別情報に関するデータが含まれ、コネクタ部の項目には、上記の遮断器に接続される接続先に関するデータが含まれ、接続点の項目には、上記の遮断器と接続先とを繋ぐ配線（接続線）に関するデータが含まれる。

[0123] この給電定義表の電源部の項目に記載された電源部P 1と、電源部P 2及びP 3とは、予め定められた制御電圧を出力する電源であって、例えば定電圧源として機能するものである。例えば、電源部P 1の出力電圧は100ボルトである。電源部P 2及びP 3の出力電圧は、それぞれ4ボルトである。電源部P 2及びP 3は、例えば互いに異なる系統の電源である。電源部P 1

と、電源部 P 2 及び P 3 は、互いの出力が短絡しても各電源部の動作に影響がないように構成されている。

[0124] 電源部 P 1 の後段には、遮断器 Breaker の第 1 端子が接続され、遮断器 Breaker の第 2 端子（接続点）には、接続線 VOL_100_2 の第 1 端が接続されている。接続線 VOL_100_2 の第 2 端（コネクタ部）には、コンタクタ C_2 の第 1 端子が接続されている。コンタクタ C_2 の第 2 端子には、接続線 VOL_100_1 が接続されている。電源部 P 1 の後段には、遮断器 R11 の第 1 端子が接続され、遮断器 R11 の第 2 端子（接続点）には、接続線 Line111（図中の表記は（1 1 1））の第 1 端が接続されている。電源部 P 2 の後段には、遮断器 R10 の第 1 端子が接続され、遮断器 R10 の第 2 端子（接続点）には、接続線 Line211（図中の表記は（2 1 1））の第 1 端が接続されている。

[0125] なお、接続線の名称に「VOL_」をついているものは、このリレー論理回路における高電位が供給される接続線であり、この「VOL_」が付いた名称の接続線には、他の接続線と電氣的に接触しても混触により高電位に変化することが無いことを示す。

[0126] 例えば、リレー R1 のコイルと、スイッチ B と、スイッチ C とが、記載の順に直列に接続されており、直列に接続された回路の第 1 端が電源部 P に接続され、第 2 端が接地極（Ground）に接続される。

[0127] まず、接続点ごとに、ブレーカと電源部とを論理積演算子（&）で接続する。

次に、電源部に記載がない接続点については、同一コネクタを持つ接続点の行に記載の電源部、ブレーカ、コネクタ部を論理積演算子（&）で接続する。

[0128] 例えば、ロジック生成部 27 による上記の処理により、下記の接続点の変数について、その変数の値を決定する論理式が生成される。その式を式（10）から式（13）に示す。

[0129]
$$\text{VOL_100_1} = \text{!C_2} \ \& \ \text{Breaker} \ \& \ 100\text{VDC} \quad \dots \quad (10)$$

$$\text{VOL_100_2} = \text{Breaker} \ \& \ 100\text{V} \quad \dots \quad (11)$$

111_temp= R11 & 4V_1 . . . (12)

211_temp= R10 & 4V_2 . . . (13)

[0130] 第1の接続点の変数であるVOL_100_1の値は、コンタクトC_2と遮断器Breakerと電源部P 1 (100VDCと表記)のそれぞれに対応する変数の論理積演算の結果になる。

第2の接続点の変数であるVOL_100_2の値は、遮断器Breakerと電源部P 4 (100Vと表記)のそれぞれに対応する変数の論理積演算の結果になる。

第3の接続点の変数であるLINE111の値は、遮断器R11と電源部P 2 (4V_1と表記)のそれぞれに対応する変数の論理積演算の結果になる。

第4の接続点の変数であるLINE211の値は、遮断器R10と電源部P 3 (4V_2と表記)のそれぞれに対応する変数の論理積演算の結果になる。

[0131] コード生成部23は、上記の接続構成に関するデータを生成した後、コードDB14 (図1)に格納する。

[0132] なお、電源系以外の範囲に含まれる各素子の接続については、後述する。

[0133] 図9を参照して、図7に示したリレー論理回路の素子一覧表の一例について説明する。図9は、図7に示したリレー論理回路の素子一覧表を示す図である。この図9には、素子と素子間の接続関係のデータを格納する素子一覧表が記載されている。素子一覧表は、No、Device、コモン、b接点、a接点の項目を含む。Noの項目には、この表に格納される各素子のデータを素子ごとに組にして、その組を単位に識別可能な番号が格納されている。なお、Noの項目は省略してもよい。Deviceの項目には、リレー論理回路2Aを形成する各素子を識別するデータが格納されている。例えば、各素子を識別するデータを、リレー論理回路2Aの接続図に記載の記号、部品表の部品名等に対応付けるとよい。コモンの項目には、各素子が備える1対の端子の内の第1端を高電位側とした場合、第1端に接続されている接続線を識別するデータが格納される。b接点とa接点の項目は、各素子が平常状態で導通状態(ON状態)にあるものか遮断状態(OFF状態)にあるものかを識別するためのものである。b接点とa接点の項目には、素子が備える1対の端子の内の第

2 端に接続されている接続線を識別するデータが、b 接点の項目と a 接点の項目の何れか一方に格納される。なお、この実施形態のリレー論理回路 2 A における「コモン」とは、各リレー及び各スイッチ等が備える 1 又は複数の接点の第 1 端が、互いに共通する電位である高電位側に接続される。このような第 1 端の接続形態を共通に接続されることを意味する「コモン」接続という。この実施形態において、スイッチ又はリレー等の接点に関し「コモン」又は「コモン部」という場合は、スイッチ又はリレー等の接点の高電位側に配置されている端子（第 1 端）を示す。

[0134] この素子一覧表（Dev 表）には、素子および接続線のそれぞれを関連付けて、当該素子または接続線の第 1 の端に接続される素子または接続線と、当該素子または接続線の第 2 の端に接続される素子または接続線とに関連するデータを格納する。

[0135] 図 7 に示したリレー論理回路から、下記の情報が読み取れる。その情報はこの素子一覧表の形に整理される。素子一覧表についての説明は、前述の図 10 を参照する。

[0136] この素子一覧表は、1 から 13 までの番号がそれぞれ附された素子の情報（データ）を含む。各素子の接続関係は下記の通りである。

1 番目の素子であるリレー R1 は、第 1 端が接続線 Line113（図中の表記は「1 1 3」）に接続され、第 2 端が接地極（図中の表記は、「G_100E1」）に接続される。

2 番目の素子であるリレー R2 は、第 1 端が接続線 Line111（図中の表記は「1 1 1」）に接続され、第 2 端が接地極に接続される。

3 番目の素子であるリレー R3 は、第 1 端が接続線 Line213（図中の表記は「2 1 3」）に接続され、第 2 端が接地極に接続される。

4 番目の素子であるリレー R4 は、第 1 端が接続線 Line211（図中の表記は「2 1 1」）に接続され、第 2 端が接地極に接続される。

5 番目の素子であるスイッチ SW_1 は、第 1 端が接続線 Line112（図中の表記は「1 1 2」）に接続され、第 2 端が接続線 Line113 に接続される。

6 番目の素子であるスイッチSW_2は、第 1 端が接続線Line111に接続され、第 2 端が接続線Line112に接続される。

7 番目の素子であるダイオードDiode_121は、第 1 端がLine121（図中の表記は「1 2 1」）に接続され、第 2 端が接続線Line111に接続される。

8 番目の素子であるスイッチSW_3は、第 1 端が電源部 P 1 に接続される接続線のうち、接続線VOL_100_1に接続され、第 2 端が接続線Line121に接続される。

9 番目の素子であるスイッチSW_4は、第 1 端が接続線Line212（図中の表記は「2 1 2」）に接続され、第 2 端が接続線Line213に接続される。

10 番目の素子であるスイッチSW_5は、第 1 端が接続線Line211に接続され、第 2 端が接続線Line212に接続される。

11 番目の素子であるダイオードDiode_221は、第 1 端がLine221（図中の表記は「2 2 1」）に接続され、第 2 端が接続線Line211に接続される。

12 番目の素子であるスイッチSW_6は、第 1 端が電源部 P 1 に接続される接続線のうち、接続線VOL_100_2に接続され、第 2 端が接続線Line221に接続される。

13 番目の素子であるコンタクタC_1は、第 1 端が接続線Line111に接続され、第 2 端が接続線Line211に接続される。

[0137] 上記と同様に、リレー論理回路内の素子に関する情報を第 14 番目以降に続けて整理する。ここでは、その記載を省略する。

[0138] なお、上記の 1 番目から 13 番目各素子の内、7 番目の素子であるダイオードDiode_121と、11 番目の素子であるダイオードDiode_221と、13 番目のコンタクタC_1は、b 接点であり、上記の素子以外は、a 接点である。ここで、ダイオードを b 接点として扱うことについて説明を補足する。ダイオードは、順バイアス状態にあると電流を流すが、逆バイアス状態にあると電流を遮断する。このリレー論理回路におけるダイオードは、順バイアスされるように配置されており、ダイオードに関連する経路が導通状態になれば、ダイオードも電流を流すことから、b 接点相当のものとして扱っている。

[0139] (断線診断用の論理式の生成)

次に、図10と前述の図9とを参照して、断線診断用の経路の検索と論理式の生成について説明する。図10は、この実施形態の断線診断用の論理式の生成処理のフローチャートである。以下、断線診断用の経路のことをパスという。

[0140] まず、ロジック生成部27は、素子情報DB15の素子一覧表から特定のリレーを抽出する(ステップSA21)。例えば、ロジック生成部27は、特定のリレーを、リレーR1に決定する。

[0141] 次に、ロジック生成部27は、抽出した特定のリレーの第1端(コモン部)に接続される接続線を、素子一覧表から抽出する(ステップSA22)。例えば、リレーR1の場合には接続線Line113である。

[0142] 次に、ロジック生成部27は、その接続線から給電定義表(Sig表)に記載の接続点に到達するパスを探索する(ステップSA23)。

[0143] 次に、ロジック生成部27は、パスの終端に到達したか否かを判定する(ステップSA24)。例えば、パスの終端とは、グラウンド(G_100E1)か給電定義表(Sig表)に記載の接続点のことである。パスをたどっていく際、パスの終端に到達していない場合、すなわち抽出した接続点がグラウンド(G_100E1)か給電定義表(Sig表)に記載の接続点に到達していない場合には、ロジック生成部27は、ステップSA23からの処理を繰り返す。

[0144] パスをたどっていく際、パスの終端に到達した場合、すなわち抽出した接続点がグラウンド(G_100E1)か給電定義表(Sig表)に記載の接続点に到達した場合には、ロジック生成部27は、到達地点について判定する(ステップSA25)。

到達地点がグラウンド(G_100E1)である場合、ロジック生成部27は、抽出したパスの情報をコードDB14に追加せずに次のステップSA27に処理を進める。

[0145] 到達地点が給電定義表(Sig表)に記載の接続点である場合、ロジック生成部27は、抽出したパスの情報をコードDB14に追加する(ステップSA

26)。なお、追加するパスが、上記の特定を起点にする複数のパスの内の1つである場合には、ロジック生成部27は、他のパスの論理式と今回抽出したパスの論理式の論理和を得るように論理和演算子により接続する。

[0146] ステップSA26の処理を終えた後、又はステップSA25の判定において到達地点がグラウンド(G_100E1)であると判定した場合には、ロジック生成部27は、上記の特定のリレーを起点にする未検索のパスが残っているか否かを判定する(ステップSA27)。未検索のパスが残っている場合には、ロジック生成部27は、対象のパスを次にパスに切り替えて、ステップSA23からの処理を実施する。

[0147] 未検索のパスが残っていない場合には、ロジック生成部27は、一又は複数のパスの論理式(ロジック)を関連付けて、関連付けた論理式を評価式に編集して評価式DBに登録する。コード生成部23は、上記の処理で作成した論理式に基づいて、実行可能なコードを作成し(ステップSA28)、図に示す一連の処理を終える。

[0148] (混触診断用の論理式の自動作成)

次に、図10の手順を適用した混触診断用の論理式の自動作成について、上記の図9を参照してより具体的な事例について説明する。

[0149] ステップSA31:

まず、ロジック生成部27は、リレーR1の第1端(コモン部)に接続される接続線の変数名を次の方法で決定する。ロジック生成部27は、リレーR1の第1端(コモン部)に接続される接続線の情報を、素子情報DB15のコモン部の欄から読み取る。ロジック生成部27は、基本ロジック用の変数については、その接続線名に"DC_"を付けたものを変数名にして、その変数を論理式の変数として登録する。例えば、素子情報DB15の1行目のコモン部の欄から読み取ったデータが(113)である場合、ロジック生成部27は、そのデータの(113)に"DC_"を付けて、混触を含むロジック用の変数の変数名にする。また、ロジック生成部27は、混触を含むロジック用の変数については、その名称の変数を論理式の変数として登録する。

ロジック生成部27は、そのデータの(113)に”Line_”を付けて、基本ロジック用の変数の変数名にする。また、ロジック生成部27は、基本ロジック用の変数については、その名称の変数を論理式の変数として登録する。

これにより基本ロジックが式(14)になり、混触を含むロジックが式(15)になる。

[0150] $R1 = DC_113 \quad \dots (14)$

$R1 = Line113 \quad \dots (15)$

[0151] ステップSA32:

次に、ロジック生成部27は、リレーR1以外のデバイス(素子)でコモン、b接点又はa接点の項目が(113)であるデバイスを抽出し、これを基本ロジックに追加する。例えば、ロジック生成部27は、(SW_1)を抽出する。

これにより基本ロジックが式(16)になる。なお、ここでは、混触を含むロジックの変更はない。

[0152] $R1 = DC_113 \ \& \ SW_1 \quad \dots (16)$

[0153] ステップSA33:

次に、ロジック生成部27は、スイッチSW_1の(113)ではない方の接点の情報を読み取る。上記の場合、その接点は(112)である。読み取った文字列に”DC_”を付加して、これを基本ロジックに追加する。

なお、ロジック生成部27は、混触含むロジックとして、この時点の基本ロジックから”DC_”の文字が付加された変数を除いたロジックとその接続線を論理積演算子で接続したものを追加する。

これにより基本ロジックが式(17)になり、混触を含むロジックが式(18)になる。

[0154] $R1 = DC_113 \ \& \ SW_1 \ \& \ DC_112 \quad \dots (17)$

$R1 = SW_1 \ \& \ Line \ 112 \quad \dots (18)$

[0155] ステップSA34:

次に、ロジック生成部27は、他のデバイスでコモン、b接点又はa接点の項目が(112)であるデバイスを抽出する。

これにより基本ロジックが式(19)になる。ここでは、混触を含むロジックの変更はない。

$$R1 = DC_113 \ \& \ SW_1 \ \& \ DC_112 \ \& \ SW_2 \quad \cdots \quad (19)$$

[0156] ステップS A 3 5 :

次に、ロジック生成部27は、SW_1の(113)ではない方の接点に関する情報を読み取る。その情報が(111)である。この(111)は、給電定義表(Sig表)に含まれる接続点を示すものであるので、ロジック生成部27は、このパスの探索を終了する。

これにより基本ロジックが式(20)になり、混触を含むロジックが式(21)になる。 $R1 = DC_113 \ \& \ SW_1 \ \& \ DC_112 \ \& \ SW_2 \ \& \ Line \ 111 \quad \cdots$
(20)

$$R1 = SW_1 \ \& \ Line \ 112 \quad \cdots \quad (21)$$

[0157] (接続点情報の生成)

次に、図11と図12を参照して、接続点情報の自動作成について説明する。

図12は、この実施形態の同一の接続点を抽出する処理について説明するための図である。

[0158] 例えば、接続線Line111を接続点として規定する場合を例示して説明する。コモンの項目とb接点の項目に、接続線Line111(図中の表記は「111」)が記載されている素子が複数存在する。例えば、接続線Line111に接続されている素子は、第2番目の素子であるリレーR2、第6番目の素子であるスイッチSW_2、第7番目の素子であるダイオードDiode_121、及び第13番目の素子であるコンタクタC_1である。他の接続線についても上記と同様の方法により、抽出できる。

[0159] 図12は、この実施形態の接続点情報の自動作成処理について説明するための図である。

[0160] ステップS A 4 1 :

まず、ロジック生成部27は、その接続点(111_temp)として、評価式にお

ける基本ロジックの論理式に追加する。これにより基本ロジックが式(22)になる。

```
[0161] Line 111 = 111 temp      . . . (2 2)
```

[0162] ステップS A 4 2 :

次に、ロジック生成部 27 は、デバイスのコモン、b 接点又は a 接点の項目に、(111) が設定されているデバイスを抽出する。例えば、第 13 番目のデバイス (C_1) のコモンの項目に (111) が設定されている。デバイス (C_1) のコモン側の接続点 Line111 とは別の接続点である b 接点の項目の (211) を抽出する。ロジック生成部 27 は、このパスに関する論理式を、上記の式 (22) の基本ロジックの論理式に論理和演算子「|」を介して、追加する。これにより基本ロジックが式 (23) になる。

```
[0163] Line 111 = 111_temp
      | ( !C 1 & Line 211 )      . . . ( 2 3 )
```

[0164] ステップS A 4 3 :

次に、上記のパスの終点が接続点であるから、ロジック生成部 27 は、このパスの探索を終了する。

第13番目の素子であるコンタクトC_1は、第1端が接続線Line111に接続され、第2端が接続線Line211に接続されていることにより、上記の式(23)が得られる。

[0165] ステップS A 4 4 :

次に、ロジック生成部 27 は、上記と同様にコモン、b 接点又は a 接点の項目に、(111) が設定されている他のデバイスを抽出する。例えば、第 7 番目のデバイス(Diode_121)の b 接点の項目に (111) が設定されている。ロジック生成部 27 は、デバイス(Diode_121)の b 接点とは別の接続点であるコモンの項目の(121)を抽出する。(121)が、給電定義表 (Sig表) に格納されている接続点でない場合には、ロジック生成部 27 は、"DC_121" として基本ロジックに追加する。なお、ロジック生成部 27 は、このパスに関する論理式を、上記の式 (23) の基本ロジックの論理式に論理和演算子「|」を介し

て、追加する。これにより基本ロジックが式(24)になる。

```
[0166] Line 111 = 111 temp | ( !C 1 & Line 211 )
```

| (!Diode 121) & (DC 121) . . . (2 4)

[0167] また、ロジック生成部 27 は、上記の基本ロジックとは別に、混触を含むロジックとして、この時点での基本ロジックから“DC_”を除いたロジックとその接続線を論理積演算子で接続したロジックとして登録する。これにより混触を含むロジックが式(25)になる。

```
[0168] Line 111 = ( !Diode 121 ) & Line 121      . . . ( 2 5 )
```

「0169」ステップS A 4 5 :

次に、ロジック生成部 27 は、他のデバイスで b 接点又は a 接点の項目に、(121) が設定されているもの抽出する。例えば、第 8 番目のデバイス (SW_3) の a 接点の項目に、(121) が設定されている。ロジック生成部 27 は、デバイス (SW_3) の a 接点とは別の接続点であるコモンの項目の (VOL_100_1) を抽出する。

(VOL_100_1)が給電定義表 (Sig表) に格納されている接続点であるため、ロジック生成部 27 は、これまで抽出した基本ロジックに論理和をとるよう、(VOL_100_1)を追加する。これにより基本ロジックが式 (26) になる。

```
[0170] Line 111 = 111 temp | ( !C 1 & Line 211 )
```

```
| { ( !Diode_121 ) & ( DC_121 ) & SW_3 & VOL_100_1 }      . . .
6)
```

[0171] なお、(VOL_100_1)が給電定義表（Sig表）に格納されている接続点であるため、ロジック生成部27は、ここでこのパスの検索を終了する。このパスの混触を含むロジックへの追加は無い。

[0172] ステップS A 4 6 :

次に、ロジック生成部 27 は、他のデバイスでコモン、b 接点又は a 接点の項目に、(111) が設定されているもの抽出する。例えば、第 6 番目のデバイス (SW_2) のコモンの項目に、(111) が設定されている。ロジック生成部 27 は、デバイス (SW_2) のコモンとは別の接続点である a 接点の項目の (112)

）を抽出する。この(112)が、給電定義表（Sig表）に格納されている接続点ではないため、ロジック生成部27は、(112)を”DC_112”に変換して、これを基本ロジックの変数にする。ロジック生成部27は、このパスに関する論理式を、上記の式（25）に示す基本ロジックの論理式に論理和演算子「|」を介して追加する。これにより基本ロジックが式（27）になる。

```
[0173] Line 111 = 111_temp | ( !C_1 & Line 211 )
      | { ( !Diode_121 ) & ( DC_121 ) & SW_3 & VOL_100_1 }
      | SW_2 & DC_112 . . . ( 2 7
    )
```

[0174] ステップS A 4 7 :

また、ロジック生成部 27 は、上記により混触を含むロジックに、 (112) を変数として追加する。混触を含むロジックが式 (28) になる。

```
[0175] Line 111 = ( !Diode_121 ) & Line 121
                | ( SW 2 & 112 )          . . . ( 2 8 )
```

[0176] ステップS A 4 8 :

次に、ロジック生成部 27 は、他のデバイスでコモンの項目に、(112) が設定されているものを抽出する。例えば、第 5 番目のデバイス (SW_1) のコモンの項目に、(112) が設定されている。ロジック生成部 27 は、デバイス (SW_1) のコモンとは別の接続点である a 接点の項目の (113) を抽出する。この (113) が、給電定義表 (Sig 表) に格納されている接続点ではないため、ロジック生成部 27 は、(113) を "DC_113" に変換して、これを上記の式 (27) の基本ロジックの論理式に追加する。これにより基本ロジックが式 (29) になる。

```
[0177] Line 111 = 111_temp | ( !C_1 & Line 211 )
      | { ( !Diode_121 ) & ( DC_121 ) & SW_3 & VOL_100_1 }
      | SW 2 & DC 112 & SW 1 & DC 113          . . . ( 2 9 )
```

[0178] ステップS A 4 9 :

これにより混触を含むロジックが式 (30) になる。

[0179] Line 111 = (!Diode_121) & Line 121

| (SW_2 & Line 112)

| (SW_2 & SW_1 & Line 113) . . . (3 0)

[0180] ステップ S A 5 0 :

次に、ロジック生成部 2 7 は、他のデバイスでコモン、b 接点又は a 接点の項目に、(113)が設定されているもの抽出する。例えば、第 1 番目のデバイス (R1) のコモンの項目に、(113)が設定されている。ロジック生成部 2 7 は、デバイス (R1) のコモンとは別の接続点である a 接点の項目の(“G_100E1”)を抽出する。ロジック生成部 2 7 は、グラウンド(“G_100E1”)に到達したので、ステップ S A 4 6 から S A 4 9 までで生成した基本ロジックを改めて削除する。なお、ロジック生成部 2 7 は、混触ロジックはステップ S A 4 9 までに生成した式 (3 0) を残す。これにより基本ロジックが式 (3 1) になる。

[0181] Line 111 = 111_temp | (!C_1 & Line 211)

| { (!Diode_121) & (DC_121) & SW_3 & VOL_100_1 } . .

. (3 1)

[0182] ステップ S A 5 1 :

これにより混触を含むロジックが式 (3 2) になる。

[0183] Line 111 = (!Diode_121) & Line 121

| (SW_2 & Line 112)

| (SW_2 & SW_1 & Line 113) . . . (3 2)

[0184] なお、上記の他、第 2 番目の素子であるリレー R 2 は、第 1 端が接続線 Line 111 に接続され、第 2 端が接地極(“G_100E1”)に接続されている。このパスの場合、接続線 Line 111 にリレーを駆動するための所定の電位を与えるパスとして有効ではないことから検索の対象にしない。

[0185] 図 1 3 を参照して、上記の処理により生成される論理式の一例について説明する。図 1 5 は、この実施形態における論理式を示す図である。

[0186] 図 1 3 (a) は、リレー R 1 の論理式であり、式 (3 3) に示す論理式が

記載されている。

[0187] 図 1 3 (a) の上段の枠内の式は、接続線の断線を条件に付加した論理式であり、下段の枠内内の式が混触を条件に付加した論理式である。上段の式と下段の式は、論理和演算子により接続される。「&」は論理積演算子であり、「|」は論理和演算子である。以下、同様である。

[0188] $R1 = ((DC_113) \& SW_1 \& (DC_112) \& SW_2 \& Line111)$
 $| (Line113) | (SW_1 \& Line112) \quad \cdot \cdot \cdot ($
 $3 \ 3)$

[0189] 式 (3 3) において、(DC_113) と (DC_112) は、接続線 Line113 と Line112 に対応する変数であり、断線が生じた場合の判定を可能にするものである。「SW_1」は、スイッチ SW_1 に対応する変数であり、「SW_2」は、スイッチ SW_2 に対応する変数である。(Line111) と (Line 113) と (Line112) は、接続線 Line111 と Line112 と Line113 に対応する変数である。(Line111) については、後述する式によって定義される。

[0190] この式 (3 3) によれば、リレー R1 の出力は、接続線 Line113 と Line112 に断線が無くスイッチ SW_1 とスイッチ SW_2 が導通状態にある場合、接続線 Line113 が混触した場合、又はスイッチ SW_1 が導通状態にあって接続線 Line112 が混触した場合の何れかの場合に導通する、ことが分かる。

[0191] 図 1 3 (b) は、リレー R 2 の論理式であり、式 (3 4) に示す論理式が記載されている。

[0192] $R2 = (Line \ 111)$
 $| (!Diode_121 \& Line121) \quad \cdot \cdot \cdot (3 \ 4)$

[0193] 式 (3 4) において、(!Diode_121) は、ダイオード Diode_121 に対応する変数である。「!」印は、b 接点であることを示す。「!」が付いた変数の素子は、定常時に偽値 (「1」) をとり、所定の条件を満たす場合に、真値 (「0」) をとる。この「!」を否定の演算子と扱ってもよい。

[0194] 接続線 Line113 と Line112 に対応する変数であり、断線が生じた場合の判定を可能にするものである。「SW_1」は、スイッチ SW_1 に対応する変数であり

、「SW_2」は、スイッチSW_2に対応する変数である。

[0195] この式(34)によれば、リレーR2の出力は、接続線Line111に断線が無く且つ変数Line111の値が「1」である場合、ダイオードDiode_121が導通状態にあって且つ接続線Line121が混触した場合の何れかの場合に導通する、ことが分かる。

[0196] 図13(c)は、リレーR3の論理式であり、式(35)に示す論理式が記載されている。

[0197]
$$R3 = ((DC_213) \& SW_4 \& (DC_212) \& SW_5 \& Line\ 211) \\ | (Line213) | (SW_4 \& Line212) \quad \dots$$

(35)

[0198] この式(35)によれば、リレーR3の出力は、接続線Line213とLine212に断線が無くスイッチSW_4とスイッチSW_5が導通状態にあり且つ変数Line111の値が「1」である場合、変数Line213が混触した場合、スイッチSW_4が導通状態にあって接続線Line213が混触した場合の何れかの場合に導通する、ことが分かる。

[0199] 図13(d)は、リレーR4の論理式であり、式(36)に示す論理式が記載されている。

[0200]
$$R4 = (Line211) \\ | (!Diode_221 \& Line221) \quad \dots$$
 (36)

[0201] この式(36)によれば、リレーR4の出力は、変数Line111の値が「1」である場合、ダイオードDiode_121が導通状態にあって接続線Line221が混触した場合の何れかの場合に導通する、ことが分かる。

[0202] 図13(e)は、接続線Line111を定義する論理式であり、式(37)に示す論理式が記載されている。

[0203]
$$Line111 = Line111_temp \\ | (!C_1 \& Line211) \\ | (!C_1 \& (DC_211) \& !Diode_221 \& (DC_221) \& SW_6 \& VOL_100_2)$$

$$\begin{aligned}
 & | (!\text{Diode_121} \ \& \ (\text{DC_121}) \ \& \ \text{SW_3} \ \& \ \text{VOL_100_1}) \\
 & | (\text{SW_2} \ \& \ \text{SW_1} \ \& \ \text{Line_113}) \\
 & | (\text{SW_2} \ \& \ \text{Line112}) \\
 & | (!\text{Diode_121} \ \& \ \text{Line121}) \qquad \qquad \qquad \cdot \cdot \cdot \ (3
 \end{aligned}$$

7)

[0204] 式(37)において、変数Line111_tempは、変数Line111の現在の値を示す。
 上記の式の演算後に、演算結果の値に更新される。

[0205] この式(37)によれば、接続線Line111に対応する変数Line111の値は、
 下記の複数の何れかの場合に「1」になり導通することが分かる。

- [0206] ・変数Line111の現在の値が「1」である場合。
- ・コンタクタC_1が導通状態にあつて接続線Line211の値が「1」である場合。
 - ・コンタクタC_1が導通状態にあつて接続線Line211とLine221に断線が無く、ダイオードDiode_221とスイッチSW_6が導通状態にあつて接続線VOL_100_2の値が「1」である場合。
 - ・スイッチSW_2とSW_1が導通状態にあつて接続線Line221が混触した場合。
 - ・スイッチSW_2が導通状態にあつて接続線Line112が混触した場合。
 - ・ダイオードDiode_121が導通状態にあつて接続線Line221が混触した場合。

[0207] 図13(f)は、リレーR4の論理式であり、式(38)に示す論理式が記載されている。

[0208] $\text{Line211} = (\text{Line211_temp})$

$$\begin{aligned}
 & | (!\text{Diode_221} \ \& \ (\text{DC_221}) \ \& \ \text{SW_6} \ \& \ \text{VOL_100_2}) \\
 & | (!\text{C_1} \ \& \ \text{Line111}) \\
 & | (!\text{C_1} \ \& \ (\text{DC_111}) \ \& \ !\text{Diode_121} \ \& \ (\text{DC_121}) \ \& \ \text{SW_3} \ \& \ \text{VOL_100_1}) \\
 & \qquad \qquad | (\text{SW_5} \ \& \ \text{SW_4} \ \& \ \text{Line213}) \\
 & | (\text{SW_5} \ \& \ \text{Line212}) \\
 & | (!\text{Diode_221} \ \& \ \text{Line221}) \qquad \qquad \qquad \cdot \cdot \cdot \ (
 \end{aligned}$$

38)

- [0209] 式(38)において、変数Line211_tempは、変数Line211の現在の値を示す。上記の式の演算後に、演算結果の値に更新される。
- [0210] この式(38)によれば、接続線Line211に対応する変数Line211の値は、下記の複数の何れかの場合に「1」になり導通することが分かる。
- [0211] ・変数Line211の現在の値が「1」である場合。
- ・接続線Line211に断線が無くダイオードDiode_221とスイッチSW_6が導通状態にあって接続線VOL_100_2の値が「1」である場合。
 - ・コンタクトC_1が導通状態にあって接続線Line111とLine121とに断線が無くダイオードDiode_121とスイッチSW_3が導通状態にあって接続線VOL_100_2の値が「1」である場合。
 - ・スイッチSW_5とSW_4が導通状態にあって接続線Line213が混触した場合。
 - ・スイッチSW_5が導通状態にあって接続線Line212が混触した場合。
 - ・ダイオードDiode_221が導通状態にあって接続線Line221が混触した場合の何れかの場合。
- [0212] 上記の実施形態によれば、検証処理装置は、検証対象のリレー論理回路を形成するリレー、素子および接続線に対応する変数を変数にとり論理式で示される評価式であって、少なくとも前記リレー論理回路に不具合事象が生じた場合の前記論理式を含む評価式で示された回路ロジックモデルを取得する取得部と、前記回路ロジックモデルに基づいて、前記素子または前記接続線に不具合事象が生じた場合でも、不安全状態に至る状態組合せがあるかを判定する判定部とを備えることにより、リレー論理回路において、不具合事象が生じたときでも安全性が保証されることを検証できる。
- [0213] 上記の実施形態は、各種システムに適用可能である。各種システムの安全性要求は年々高まる傾向にある。一方で、そのシステムの制御は複雑化している。このような場合に、上記の実施形態の手法を適用することにより、不具合事象が生じた場合の検証を含めて網羅的に検証するためのモデル検査手法を適用できる。
- [0214] 特に第2の実施形態の場合、リレー論理回路の情報、例えば、モデル検査

に必要な状態遷移モデルを作成するための情報を、プログラム言語（VHDLやVerilog等の論理回路記述言語、C言語、JAVA（登録商標）など）で書かれたものとしてあらかじめ用意する必要が無い。この場合、図8と図10に示したような一覧表に基づいて、リレー論理回路の情報が、検証処理装置1Aによって生成される。

[0215] なお、前述の図1と図6は、少なくとも1つの実施形態に係るコンピュータの構成を示す概略ブロック図である。コンピュータは、図示しないプロセッサ、メインメモリ、ストレージ、インタフェースを備える。

上述の検証処理装置は、コンピュータに実装される。そして、上述した各処理部の動作は、プログラムの形式でストレージに記憶されている。プロセッサは、プログラムをストレージから読み出してメインメモリに展開し、当該プログラムに従って上記処理を実行する。また、プロセッサは、プログラムに従って、上述した各記憶部に対応する記憶領域をメインメモリに確保する。

[0216] ストレージの例としては、HDD（Hard Disk Drive）、SSD（Solid State Drive）、磁気ディスク、光磁気ディスク、CD-ROM（Compact Disc Read Only Memory）、DVD-ROM（Digital Versatile Disc Read Only Memory）、半導体メモリ等が挙げられる。ストレージは、コンピュータのバスに直接接続された内部メディアであってもよいし、インタフェースまたは通信回線を介してコンピュータに接続される外部メディアであってもよい。また、このプログラムが通信回線によってコンピュータに配信される場合、配信を受けたコンピュータが当該プログラムをメインメモリに展開し、上記処理を実行してもよい。少なくとも1つの実施形態において、ストレージは、一時的でない有形の記憶媒体である。

[0217] また、当該プログラムは、前述した機能の一部を実現するためのものであってもよい。さらに、当該プログラムは、前述した機能をストレージに既に記憶されている他のプログラムとの組み合わせで実現するもの、いわゆる差分ファイル（差分プログラム）であってもよい。

[0218] なお、この発明は上述した実施形態の構成に限られるものではなく、その要旨を逸脱しない範囲で設計変更可能である。

例えば、上述した実施形態では、コードの一例としてSMV (Symbolic Model Verifier) コードに準拠したものを示したが、これに制限されることなく、他の規格のコード又はプログラム言語を採用してもよい。

産業上の利用可能性

[0219] 上記した検証処理装置、ロジック生成装置及び検証処理方法によれば、リレーを用いるリレー論理回路において、不具合事象が生じたときの安全性を検証できる。

符号の説明

- [0220] 1、1 A 検証処理装置
- 10、10 A 記憶部
 - 11 評価式DB
 - 12 評価条件DB
 - 13 検査式DB
 - 14 コードDB
 - 15 素子情報DB
 - 16 信号情報DB
 - 20、20 A 制御部
 - 21、21 A 解析データ設定部
 - 22 検査式設定部
 - 23 コード生成部
 - 24 取得部
 - 25 解析処理部
 - 26 表示制御部
 - 27 ロジック生成部
 - 2、2 A リレー論理回路