

明 細 書

発明の名称： 検証処理装置、検証処理方法及びプログラム

技術分野

[0001] 本発明は、検証処理装置、検証処理方法及びプログラムに関する。

本願は、2018年11月1日に日本に出願された特願2018-206518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] 特許文献1には、モデル検査を用いて、データ処理システムの動作ロジックの網羅的検証を行うことが記載されている。

先行技術文献

特許文献

[0003] 特許文献1：特開2008-071135号公報

発明の概要

発明が解決しようとする課題

[0004] 例えば、モデル検査でリレー回路の動作ロジックを検証する場合、当該リレー回路の基本動作ロジックを検証するだけでは不十分であり、当該リレー回路に含まれる信号線や回路素子に不具合が発生し得ることを加味して検証を行う必要がある。

[0005] 信号線や回路素子の不具合（例えば、信号線の混触、断線、回路素子の故障）はリレー回路の基本動作ロジックによらず同時多発的かつ非同期的に発生し得ることを考慮すると、モデル検査においては、基本動作中に起こり得る状態遷移に加え、基本動作中の各状態から発生し得る不具合の全ての組み合わせを網羅的に検証する必要がある。

[0006] しかしながら、そうした場合、リレー回路に含まれる各信号線及び各回路素子で生じた複数の不具合の組み合わせを含む反例が出力されたとしても、当該不具合の組み合わせの中には、不安全事故に至ったことに必ずしも寄与しない（クリティカルでない）不具合が含まれている可能性がある。

[0007] つまり、モデル検査は、BDD (Binary Decision Diagram) などにより、検査対象モデルが取り得る全状態を論理式で表現することにより、不安全事故に至る条件（パターン）を網羅的に検査するものであり、その不安全事故に至った過程においては、必ずしもクリティカルでない状態遷移をも含み得る。そのため、不安全事故に関してクリティカルでない不具合をも含み得る反例について反例解釈を行わざるを得ず、モデル検査の反例解釈の作業に要する負担が大きかった。

[0008] 本発明の少なくとも一実施形態は、モデル検査の反例解釈の作業に要する負担を軽減可能な検証処理装置、検証処理方法及びプログラムを提供することを目的とする。

課題を解決するための手段

[0009] 本発明の第1の態様によれば、検証処理装置は、検査対象モデルに対してモデル検査を実施する処理部と、前記モデル検査の結果に基づき、不安全事故に至る過程で状態が変化した要素の中から一つの要素を選択する選択部と、を備える。前記処理部は、更に、前記一つの要素を除外してなる検査対象モデルに対して再度のモデル検査を実施する。

[0010] 本発明の第2の態様によれば、前記処理部は、前記再度のモデル検査で前記不安全事故に至らなかった場合に、前記一つの要素を前記検査対象モデルに戻し、前記一つの要素とは異なる要素を前記検査対象モデルから除外してなる検査対象モデルに対して再度のモデル検査を実施する。

[0011] 本発明の第3の態様によれば、前記処理部は、前記再度のモデル検査で前記不安全事故に至った場合に、前記一つの要素を前記検査対象モデルに戻すことなく、前記一つの要素とは異なる要素を前記検査対象モデルから除外してなる検査対象モデルに対して再度のモデル検査を実施する。

[0012] 本発明の第4の態様によれば、前記処理部は、前記検査対象モデルに対する最初のモデル検査において特定された、不安全事故に至るまでの遷移ステップ数以下の範囲で、前記再度のモデル検査を実施する。

[0013] 本発明の第5の態様によれば、上述の検証処理装置は、前記再度のモデル

検査の結果に基づいて抽出された要素から不安全事故の定義に含まれる要素までの最短パスを特定する特定部を更に備える。

[0014] 本発明の第6の態様によれば、上述の検証処理装置は、要素ごとに規定された不具合発生確率に基づいて、前記検査対象モデルが初期状態から不安全事故に至る確率を演算する演算部を更に備える。

[0015] 本発明の第7の態様によれば、前記選択部は、前記確率が所定の判定閾値を下回る場合、前記モデル検査の結果に基づき前記一つの要素を選択する処理を省略する。

[0016] 本発明の第7の態様によれば、検証処理方法は、検査対象モデルに対してモデル検査を実施するステップと、前記モデル検査の結果に基づき、不安全事故に至る過程で状態が変化した要素の中から一つの要素を選択するステップと、前記一つの要素を除外してなる検査対象モデルに対して再度のモデル検査を実施するステップと、を有する。

[0017] 本発明の第8の態様によれば、プログラムは、検証処理装置のコンピュータに、検査対象モデルに対してモデル検査を実施するステップと、前記モデル検査の結果に基づき、不安全事故に至る過程で状態が変化した要素の中から一つの要素を選択するステップと、前記一つの要素を除外してなる検査対象モデルに対して再度のモデル検査を実施するステップと、を実行させる。

発明の効果

[0018] 上述の発明の各態様によれば、モデル検査の反例解釈の作業に要する負担を軽減することができる。

図面の簡単な説明

[0019] [図1]第1の実施形態に係る検証処理装置の構成を示す図である。

[図2]第1の実施形態に係る検証処理装置のCPUの機能構成を示す図である。

[図3]第1の実施形態に係る検査対象モデルの例を示す図である。

[図4]第1の実施形態に係る検証処理装置の処理フローを示す図である。

[図5]第1の実施形態に係る検証処理装置の動作を詳細に説明するための図で

ある。

[図6]第1の実施形態に係る検証処理装置の動作を詳細に説明するための図である。

[図7]第2の実施形態に係る検証処理装置のCPUの機能構成を示す図である。

[図8]第2の実施形態に係る特定部の動作を詳細に説明するための図である。

[図9]第2の実施形態に係る特定部の動作を詳細に説明するための図である。

[図10]第3の実施形態に係る検証処理装置のCPUの機能構成を示す図である。

[図11]第3の実施形態に係る演算部の動作を詳細に説明するための図である。

[図12]第3の実施形態に係る演算部の動作を詳細に説明するための図である。

発明を実施するための形態

[0020] <第1の実施形態>

以下、第1の実施形態に係る検証処理装置について、図1～図6を参照しながら説明する。

[0021] (検証処理装置の構成)

図1は、第1の実施形態に係る検証処理装置の構成を示す図である。

図2は、第1の実施形態に係る検証処理装置のCPUの機能構成を示す図である。

[0022] 図1に示すように、検証処理装置1は、CPU10と、メモリ11と、ディスプレイ12と、入力デバイス13と、ストレージ14とを備え、一般的なコンピュータとして構成されている。

[0023] メモリ11は、いわゆる主記憶装置であって、CPU10がプログラムに基づいて動作するための命令及びデータが展開される。

[0024] ディスプレイ12は、情報を視認可能に表示する表示デバイスであって、例えば、液晶ディスプレイや有機ELディスプレイなどであってよい。

- [0025] 入力デバイス 13 は、検証処理装置 1 の使用者の操作を受け付ける入力デバイスであって、例えば、一般的なマウス、キーボード、タッチセンサなどであってよい。
- [0026] ストレージ 14 は、いわゆる補助記憶装置であって、例えば、HDD (Hard Disk Drive)、SSD (Solid State Drive) 等であってよい。ストレージ 14 には、例えば、検査対象とするリレー回路を示す検査対象モデルMODなどが記録される。
- [0027] CPU 10 は、検証処理装置 1 の動作全体の制御を司るプロセッサである。本実施形態に係るCPU 10 は、図 2 に示すように、処理部 100、選択部 101 及び再構築部 102 としての機能を発揮する。
- [0028] 処理部 100 は、検査対象モデルMODに対してモデル検査を実施する。ここで実施されるモデル検査とは、BDD (Binary Decision Diagram) などにより検査対象モデルが取り得る全状態を論理式で表現することで、不安全事故に至る条件 (パターン) を網羅的に検査するものである。本実施形態において実施されるモデル検査のアルゴリズムは、一般によく知られているものであってよい。
- 検査対象モデルMODとは、検査対象とするシステム (例えば、鉄道の保安システム) の動作ロジックが規定された情報であり、モデル検査では、ここで規定された動作ロジックにしたがって、システムの網羅的な動作検証が実施される。
- また、不安全事故とは、検査対象とするシステムがいかなる場合であっても遷移してはならない状態として定義される状態である。例えば、鉄道の保安システムにおいては、“車両の自動運転制御中に非常ブレーキが効かない”状態、“車両が踏切を走行しているにもかかわらず遮断機が下りていない”状態などが不安全事故として定義される。
- [0029] 選択部 101 は、処理部 100 によって実施されたモデル検査の結果に基づき、不安全事故に至る過程で状態が変化した要素の中から一つの要素を選択する。「要素」とは、検査対象モデルMODの動作ロジック及び状態を規

定する最小単位であって、例えば、保安システムのリレー回路に実装されている信号線や回路素子などである。後述するように、「要素」には、現実のリレー回路に実装されている信号線や回路素子の動作そのものを模擬するものの他、不具合発生時におけるリレー回路の動作を模擬するために規定された仮想の素子をも含む。

[0030] 再構築部102は、本実施形態で実施されるモデル検査の過程において、所定の条件に従い、検査対象モデルMODを再構築する。

[0031] (検査対象モデルの例)

図3は、第1の実施形態に係る検査対象モデルの例を示す図である。

図3に示す検査対象モデルMODは、鉄道の保安システムを構成するリレー回路の動作ロジックを模擬する。

図3に示す配線V及び配線Gは、それぞれ、電源線及び接地線（グラウンド）である。また、要素A1、A2、・・・はリレースイッチであり、通電に応じてOFF状態またはON状態に遷移する（ $0(FALSE) = OFF / 1(TRUE) = ON$ ）。また、要素X1、X2、・・・は、マニュアルスイッチであり、人の操作によってOFF状態またはON状態に遷移する（ $0 = OFF / 1 = ON$ ）。

要素E1、E2、・・・は、各信号線で発生し得る不具合（断線及び混触）を再現するために規定された仮想素子である。例えば、配線V（電源線）と要素X1（マニュアルスイッチ）とを結ぶ信号線上には、要素E1が規定されている。この要素E1は、当該信号線における不具合の一つとして“断線の発生”を再現する（ $0 = 断線 / 1 = 非断線$ ）。また、要素X1と要素X2（マニュアルスイッチ）とを結ぶ信号線上には、2つの要素E2、E3が規定されている。このうち、要素E2は、当該信号線における“断線の発生”を再現し（ $0 = 断線 / 1 = 非断線$ ）、要素E3は、当該信号線における“電源線との混触の発生”を再現する（ $0 = 非混触 / 1 = 混触$ ）。同様に、要素X2と要素A1（リレースイッチ）とを結ぶ信号線上には、2つの要素E4、E5が規定されている。このうち、要素E4は、当該信号線における“断

線の発生”を再現し（0＝断線／1＝非断線）、要素E 5は、当該信号線における“電源線との混触の発生”を再現する（0＝非混触／1＝混触）。

[0032] 実際の検査対象モデルMODは、論理式（言語）によって記述される。例えば、要素A 1（リレースイッチ）に関しては、マニュアルスイッチX 1、X 2の他、各信号線に生じ得る不具合（断線、混触）を加味して、式（1）のように記述される。

[0033]
$$A 1 = (E 1 \& X 1 \& E 2 \& X 2 \& E 4) \text{ or } (E 3 \& X 2 \& E 4) \text{ or } (E 5) \cdots (1)$$

[0034] 他の要素についても同様の論理式によって記述される。

[0035] なお、式（1）は、要素A 1（リレースイッチ）自身に不具合が発生していない場合における要素A 1の状態遷移を規定するものである。現実には、要素A 1自身にも不具合が発生する可能性があるため、検査対象モデルMODは、要素A 1が式（1）の論理式にかかわらずOFF状態又はON状態に遷移する遷移パターンをも含む。他の要素A 2、A 3、・・・等についても同様である。

また、マニュアルスイッチである要素X 1、X 2、・・・は、人の操作に従って状態遷移する要素であるため、モデル検査においては、不具合の発生を規定する要素E 1、E 2、・・・と同様に、あらゆるタイミングで同時多発的かつ非同期的な状態遷移が起こり得るものとして規定される。

[0036] （検証処理装置の処理フロー）

図4は、第1の実施形態に係る検証処理装置の処理フローを示す図である。

図5及び図6は、第1の実施形態に係る検証処理装置の動作を詳細に説明するための図である。

図4に示す処理フローは、検査対象モデルMODに対するモデル検査の一連の処理の流れを示している。

[0037] まず、CPU 10の処理部100は、検査対象モデルMODに対して通常モデル検査を行う（ステップS 01）。ステップS 01にて実施されるモデ

ル検査について、図5に示す状態遷移図を用いて説明する。

図5に示す複数の状態 ST_x は、それぞれ、図3で示した検査対象モデルMODの状態を示している。検査対象モデルMODの各状態は、当該検査対象モデルMODに含まれる要素 A_1 、 A_2 、 $\dots$ 、 X_1 、 X_2 、 $\dots$ 、 E_1 、 E_2 、 $\dots$ の各々の状態(0/1)の組み合わせで規定される。このうち、状態 ST_1 は検査対象モデルMOD(即ち、保安システム)の初期状態である。処理部100は、検査対象モデルMODで規定される論理式(式(1)参照)にしたがい、不安全事故(状態 ST_2)から初期状態(状態 ST_1)に到達する状態遷移が存在するかを網羅的に検証する。不安全事故(状態 ST_2)は、例えば、検査対象モデルMODに含まれる他の要素 S_1 、 T_1 、 U_1 についての論理式($S_1 \& T_1 \& U_1 = TRUE$)を含む状態として規定される。

[0038] 不安全事故(状態 ST_2)から初期状態(状態 ST_1)に到達するパス(条件)が存在する場合、処理部100は、当該不安全事故に到達した過程において不具合が発生した要素をリストアップし、不具合リストを作成する(ステップS02)。ステップS02にて作成される不具合リストの例を図6に示す。

[0039] 処理部100は、初期状態(状態 ST_1)から無作為に状態遷移を繰り返した結果、不安全事故(状態 ST_2)に至った場合に、当該不安全事故に至った過程において状態が変化した要素(つまり、不具合が発生した要素)をリストアップする。そして、処理部100は、図6に示すような不具合リストLを作成する。

[0040] 図6に例示される不具合リストでは、状態 ST_1 から状態 ST_2 までの各遷移ステップで状態遷移が発生した要素の一覧と、各要素が何ステップ目になどのような値に遷移したかが示される。例えば、図6に示す不具合リストLには、初期状態から第6ステップ目の状態遷移で不安全事故($S_1 \& T_1 \& U_1 = TRUE$)に至ったことが示されている。また、不具合リストLによれば、要素 X_1 は、不安全事故に至る過程において、4ステップ目に $FALSE$

SEからTRUEに遷移し、5ステップ目にTRUEからFALSEに遷移したことが読み取れる。

[0041] しかしながら、ステップS02で示される不具合リストLは、無作為な状態遷移を繰り返した結果、初期状態から不安全事故（S1 & T1 & U1 = TRUE）に行きつく過程においてたまたま状態遷移が起こった要素をリストアップしたものにすぎない。したがって、不具合リストLにリストアップされた各要素には、不安全事故に至ったことに直接的に寄与していない要素が含まれることが推察される。そこで、本実施形態に係る検証処理装置1は、更に、以下のステップS03～ステップS08の処理を実行する。

[0042] 具体的には、CPU10の選択部101は、リストアップされた要素のうちの一つを選択する（ステップS03）。簡単な例として、不具合リストLにリストアップされた要素が（E1、E2、E3、X1、X2）の5つであった場合、選択部101は、例えば、そのうちの一つとして要素E1を選択する。

[0043] 次に、CPU10の再構築部102は、検査対象モデルMODから、ステップS03で選択された要素を除いたモデルを作成（再構築）する（ステップS04）。以下、ステップS04で作成されたモデルを「再構築モデル」とも記載する。例えば、ステップS03で要素E1が選択されたとき、再構築部102は、もともとの検査対象モデルMODから要素E1を除外した再構築モデルを作成する。

[0044] 次に、処理部100は、ステップS04で作成された再構築モデルに対し、再度のモデル検査を実施する（ステップS05）。上記の例では、この再構築モデルには要素E1が含まれていない。したがって、ステップS05で実施されるモデル検査では、配線V（電源線、図3参照）と要素X1（マニュアルスイッチ、図3参照）とを結ぶ信号線上における“断線の発生”は考慮されない。

[0045] 処理部100は、ステップS05で再度実施されたモデル検査の結果を出力し、最初のモデル検査（ステップS01）にて発生した不安全事故と同一

の不安全事象（ $S1 \& T1 \& U1 = TRUE$ ）が発生するか否かを判定する（ステップS06）。

同一の不安全事象が発生しなかった場合（ステップS06；NO）、ステップS03で選択された要素が除外された結果、不安全事象が発生しなくなったのであるから、当該除外された要素は、不安全事象の発生に寄与する、クリティカルな要素であるといえる。したがって、この場合、再構築部102は、ステップS03で選択された要素を検査対象モデルMODに戻す（ステップS07）。

他方、同一の不安全事象が発生した場合（ステップS06；YES）、ステップS03で選択された要素が除外されたにもかかわらず、依然として不安全事象が発生したのであるから、当該除外された要素は、不安全事象の発生には寄与しない（クリティカルではない）要素といえる。このような要素は、反例解釈の際には除外されていることが望ましいから、再構築部102は、ステップS03で選択された要素を検査対象モデルMODに戻すことなく次のステップに移行する。

[0046] 次に、選択部101は、ステップS02の不具合リストLでリストアップされた全ての要素を選択したか否かを判定する（ステップS08）。全ての要素が選択されていない場合（ステップS08；NO）、選択部101はステップS03に戻り、前回のステップS03とは異なる要素を一つ選択する。そして、再構築部102及び処理部100は、ステップS04～ステップS07の処理を繰り返す。

全ての要素が選択されていた場合（ステップS08；YES）、選択部101は、不具合リストLにリストアップされた要素のうち、検査対象モデルMODに残った要素を出力する（ステップS09）。

[0047] 例えば、ステップS02の不具合リストLにリストアップされた要素（E1、E2、E3、X1、X2）のうち、ステップS03からステップS08までの処理を経て、要素（E1、E2、X1）がクリティカルな要素ではなく除外されたとすると、残った要素（E3、X2）がステップS09で出力

される。

[0048] （作用、効果）

以上の通り、第1の実施形態に係る検証処理装置1は、検査対象モデルMODに対してモデル検査を実施する処理部100と、モデル検査の結果に基づき、不安全事故に至る過程で状態が変化した要素の中から一つの要素を選択する選択部101と、を備える。そして、処理部100は、選択部101によって選択された一つの要素を除外してなる検査対象モデル（再構築モデル）に対して再度のモデル検査を実施する。

このようにすることで、モデル検査で示された複数の要素（不具合）のうち、不安全事故の直接的な要因となる不具合のみを抽出することができる（図4のステップS09参照）。したがって、検査対象モデルMODの検証者は、不安全事故の発生に寄与するクリティカルな要素のみを含む反例について反例解釈を行えばよいので、反例解釈の作業負担を軽減することができる。

[0049] また、第1の実施形態に係る処理部100は、再度のモデル検査で不安全事故に至らなかった場合に、選択された一つの要素を検査対象モデルMODに戻し、当該一つの要素とは異なる要素を検査対象モデルMODから除外してなる検査対象モデルに対して再度のモデル検査を実施する。

また、処理部100は、再度のモデル検査で不安全事故に至った場合に、選択された一つの要素を検査対象モデルMODに戻すことなく、当該一つの要素とは異なる要素を検査対象モデルMODから除外してなる検査対象モデルに対して再度のモデル検査を実施する。

このようにすることで、最初の不具合リストLでリストアップされた要素（不具合）の候補のうち、不安全事故に関してクリティカルな要素のみを抽出する作業を自動化することができるので、検証者の負担を一層軽減することができる。

[0050] （第1の実施形態の変形例）

以上、第1の実施形態に係る検証処理装置1について詳細に説明したが、

検証処理装置 1 の具体的な態様は、上述のものに限定されることはなく、要旨を逸脱しない範囲内において種々の設計変更等を加えることは可能である。例えば、第 1 の実施形態の変形例に係る処理部 100 は、更に、以下の機能を有してもよい。

[0051] 第 1 の実施形態の変形例に係る処理部 100 は、検査対象モデル MOD に対する最初のモデル検査（図 4 のステップ S01）において特定された、不安全事故に至るまでの遷移ステップ数以下の範囲で、再度のモデル検査（図 4 のステップ S05）を実施する。

例えば、図 6 に示す不具合リスト L の例では、最初のモデル検査の結果、検査対象モデル MOD は 6 回の状態遷移（遷移ステップ数 = 6）を経て不安全事故（ $S1 \ \& \ T1 \ \& \ U1 = TRUE$ ）に至ることが判明している。なお、最初のモデル検査では、不安全事故に至るあらゆる状態遷移の可能性を網羅する目的で、遷移ステップ数に特段の上限を設けることなく実施される。

ここで、要素数が削減された検査対象モデル MOD に対する再度のモデル検査（図 4 のステップ S05）において不安全事故に至るまでの遷移ステップ数が、要素数を削減する前の検査対象モデル MOD に対するモデル検査（図 4 のステップ S01）において不安全事故に至るまでの遷移ステップ数よりも大きくなることはない。そこで、図 4 のステップ S05 で実施される再度のモデル検査においては、図 4 のステップ S01 で実施されたモデル検査で判明した遷移ステップ数を上限として定めたいえで、実施するようにしてもよい。このようにすることで、検査対象モデル MOD に対する 2 回目以降のモデル検査で検証される遷移ステップ数に制限がかかるため、2 回目以降のモデル検査に要する処理負荷、処理時間を低減することができる。

[0052] <第 2 の実施形態>

次に、第 2 の実施形態に係る検証処理装置について、図 7 ～図 9 を参照しながら説明する。

[0053] （検証処理装置の構成）

図 7 は、第 2 の実施形態に係る検証処理装置の CPU の機能構成を示す図

である。

図 7 に示すように、第 2 の実施形態に係る CPU 10 は、更に、特定部 103 としての機能を発揮する。

特定部 103 は、再度のモデル検査の結果に基づいて抽出された要素（図 4 のステップ S09 参照）から不安全事故の定義に含まれる要素までの最短パスを特定する。

特定部 103 による処理は、例えば、図 4 に示す一連の処理の完了後、自動的に実行される態様であってよい。

[0054] （最短パス特定部の処理）

図 8 ～図 9 は、第 2 の実施形態に係る最短パス特定部の動作を詳細に説明するための図である。

[0055] 図 4 に示す処理フローの結果、不安全事故に至るクリティカルな要素として要素（E3、X2）が抽出されたとする（図 4 のステップ S09）。この場合、最短パス特定部 103 は、続いて、図 8 に示すように、抽出された要素 E3、X2 のそれぞれで起きた状態遷移（不具合）が、不安全事故の定義に含まれる各要素（要素 S1、T1、U1）のそれぞれに状態遷移を起こさせるまでの最短パスを特定する。

[0056] より具体的に説明すると、図 9 に示すように、検査対象モデル MOD を規定するロジックシート（論理式の集合）を参照して上述の最短パスを特定する。ここで、図 9 は、要素 X2 で起きた状態遷移が要素 S1 に状態遷移を起こさせるまでの最短パスを特定する処理の例を示している。

図 9 に示すように、まず、最短パス特定部 103 は、ロジックシートを参照し、右辺に要素 X2 を含む論理式を特定する。ここで特定された論理式 LC1、LC2 によれば、要素 X2 の状態遷移の影響を受ける要素として、要素 B1 及び要素 B3 が特定される（ステップ S11）。

次に、最短パス特定部 103 は、ロジックシートを参照し、右辺に要素 B1 を含む論理式を特定する（ステップ S12）。ここで特定された論理式 LC3 によれば、要素 B1 の状態遷移の影響を受ける要素として、要素 C1 が

特定される（ステップS 1 3）。同様に、最短パス特定部1 0 3は、ロジックシートを参照し、右辺に要素B 3を含む論理式を特定する（ステップS 1 4）。ここで特定された論理式L C 3によれば、要素B 3の状態遷移の影響を受ける要素として、ステップS 1 3で特定した要素と同一の要素C 1が特定される（ステップS 1 5）。

最短パス特定部1 0 3は、以上のステップS 1 1からステップS 1 5までの処理を、要素S 1に到達するまで繰り返し実行する。これにより、要素X 2から要素S 1までの最短パスが特定される。

同様に、最短パス特定部1 0 3は、要素X 2から要素T 1までの最短パス、要素X 2から要素U 1までの最短パス、要素E 3から要素S 1までの最短パス、要素E 3から要素T 1までの最短パス、及び、要素E 3から要素U 1までの最短パスを特定する。

[0057] （作用、効果）

以上の通り、第2の実施形態に係る検証処理装置1によれば、不安全事故を引き起こすクリティカルな不具合（要素）から実際に不安全事故に至るまでの最短パスを自動的に特定することができる。また、第1の実施形態で得られる効果により、最短パス特定部1 0 3によって特定される最短パスはいずれも不安全事故に直結する最短パス（クリティカルパス）のみとなり、不安全事故の発生に寄与しない要素からの最短パスは含まれない。これにより、検証者は、最短パス特定部1 0 3によって特定されたクリティカルパスについて対策を検討すればよいので、反例検証に要する作業負担を一層軽減することができる。

[0058] 第2の実施形態の変形例に係る検証処理装置1は、更に、リレー回路で発生した不具合が上記クリティカルパスを伝搬する様子を、別途用意された回路図（図3参照）上でアニメーション表示する機能を有していてもよい。これにより、検証者は、不安全事故が発生する過程をより直感的に理解することができる。

[0059] <第3の実施形態>

次に、第3の実施形態に係る検証処理装置について、図10～図12を参照しながら説明する。

[0060] (検証処理装置の構成)

図10は、第3の実施形態に係る検証処理装置のCPUの機能構成を示す図である。図10に示すように、第3の実施形態に係るCPU10は、更に、演算部104としての機能を発揮する。

演算部104は、要素X1、X2、・・・E1、E2、・・・A1、A2、・・・ごとに事前に規定された不具合発生確率 λ に基づいて、検査対象モデルMODが初期状態から不安全事故に至る確率（到達確率）を演算する。不具合発生確率 λ は、単位時間（例えば1時間以内）に各要素で不具合が発生する確率である。このような不具合発生確率 λ は、過去の運用実績やシミュレーションなどによって、要素別に事前に特定されているものとする。

[0061] (演算部の処理)

図11～図12は、第3の実施形態に係る演算部の動作を詳細に説明するための図である。

図11は、検査対象モデルMODの要素別に規定される故障モデルの例を示している。図11は、信号線で起こる不具合の一つである“混触の発生”を示す故障モデルである。図11に示す故障モデルによれば、信号線は、混触が発生していない状態（False）から「 $1 - \lambda$ 」の確率で同状態（False）に留まり、「 λ 」の確率で混触が発生した状態（True）に遷移する。そして、いったん混触が発生した後は、常に（1の確率で）同状態（True）に留まり続ける。なお、図示を省略するが、信号線における“断線の発生”についても個別に故障モデルが規定される。また、マニュアルスイッチである要素X1についての故障モデル、及び、リレースイッチである要素A1についての故障モデル等も同様に規定されている。

[0062] 図12は、演算部104の処理を具体的に説明するための図である。本実施形態に係る演算部104は、処理部100によって作成された不具合リストL（図6）が作成された後（図4のステップS02の後）、当該不具合リ

ストLに示される不安全事故の発生に至る確率を演算する。

具体的には、演算部104は、不具合リストLに示される1回目の状態遷移が起きる確率（状態遷移確率 λ_1 ）を演算する。ここで、演算部104は、1回目の状態遷移で変化した要素の故障モデルを用いて状態遷移確率 λ_1 を演算する（図11参照）。同様に、演算部104は、不具合リストLに示される2回目の状態遷移が起きる確率（状態遷移確率 λ_2 ）を演算する。ここで、演算部104は、2回目の状態遷移で変化した要素の故障モデルを用いて状態遷移確率 λ_2 を演算する。以下、同様にして、不安全事故（状態ST2）に至るまでの各状態遷移確率 λ_3 、 λ_4 、 $\dots$ 、 λ_6 を演算する。そして、演算部104は、不具合リストLで示された状態遷移が起こり得る確率、即ち、初期状態（状態ST1）から不安全事故（状態ST2）に至る確率（ $\lambda_1 \times \lambda_2 \times \dots \times \lambda_6$ ）を演算する。

[0063] （作用、効果）

以上の通り、第3の実施形態に係る検証処理装置1は、要素ごとに規定された不具合発生確率 λ に基づいて、検査対象モデルMODが初期状態から不安全事故に至る確率を演算する演算部104を更に備える。

これにより、検査対象モデルMODに対する最初のモデル検査（図4のステップS01）の結果として不具合リストLが作成された場合に、その不安全事故に至るすべての確率の総和を求めることができる。そして、その確率に応じて、反例解釈及び対策の優先度を適切に定めることができる。例えば、図4のステップS02で作成された不具合リストに示される状態遷移の発生確率が極めて低い場合（所定の判定閾値に満たない場合）には、図4のステップS03以降の処理を省略し、直ちに別の不具合リストLについての絞り込みや反例検証に移行するという判断を下すことができる。

以上より、検査対象モデルMODの反例解釈の作業について、一層の効率化を図ることができる。

[0064] 上述の第1～第3の実施形態において、上述したCPU10の各種処理の過程は、プログラムの形式でコンピュータ読み取り可能な記録媒体に記憶さ

れており、このプログラムをコンピュータが読み出して実行することによって上記各種処理が行われる。また、コンピュータ読み取り可能な記録媒体とは、磁気ディスク、光磁気ディスク、CD-ROM、DVD-ROM、半導体メモリ等をいう。また、このコンピュータプログラムを通信回線によってコンピュータに配信し、この配信を受けたコンピュータが当該プログラムを実行するようにしてもよい。

[0065] 上記プログラムは、上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。更に、上述した機能をコンピュータシステムにすでに記録されているプログラムとの組み合わせで実現できるもの、いわゆる差分ファイル（差分プログラム）であってもよい。

[0066] 以上のとおり、本発明に係るいくつかの実施形態を説明したが、これら全ての実施形態は、例として提示したものであり、発明の範囲を限定することを意図していない。これらの実施形態は、その他の様々な形態で実施されることが可能であり、発明の要旨を逸脱しない範囲で種々の省略、置き換え、変更を行うことができる。これらの実施形態及びその変形は、発明の範囲や要旨に含まれると同様に、特許請求の範囲に記載された発明とその均等の範囲に含まれる。

産業上の利用可能性

[0067] 本発明の各態様によれば、モデル検査の反例解釈の作業に要する負担を軽減することができる。

符号の説明

[0068] 1 検証処理装置

10 CPU

100 処理部

101 選択部

102 再構築部

103 特定部

104 演算部

1 1 メモリ

1 2 ディスプレイ

1 3 入力デバイス

1 4 ストレージ

MOD 検査対象モデル

L 不具合リスト

請求の範囲

- [請求項1] 検査対象モデルに対してモデル検査を実施する処理部と、
前記モデル検査の結果に基づき、不安全事故に至る過程で状態が変化した要素の中から一つの要素を選択する選択部と、
を備え、
前記処理部は、更に、前記一つの要素を除外してなる検査対象モデルに対して再度のモデル検査を実施する
検証処理装置。
- [請求項2] 前記処理部は、
前記再度のモデル検査で前記不安全事故に至らなかった場合に、前記一つの要素を前記検査対象モデルに戻し、前記一つの要素とは異なる要素を前記検査対象モデルから除外してなる検査対象モデルに対して再度のモデル検査を実施する
請求項1に記載の検証処理装置。
- [請求項3] 前記処理部は、
前記再度のモデル検査で前記不安全事故に至った場合に、前記一つの要素を前記検査対象モデルに戻すことなく、前記一つの要素とは異なる要素を前記検査対象モデルから除外してなる検査対象モデルに対して再度のモデル検査を実施する
請求項2に記載の検証処理装置。
- [請求項4] 前記処理部は、
前記検査対象モデルに対する最初のモデル検査において特定された、不安全事故に至るまでの遷移ステップ数以下の範囲で、前記再度のモデル検査を実施する
請求項1から請求項3のいずれか一項に記載の検証処理装置。
- [請求項5] 前記再度のモデル検査の結果に基づいて抽出された要素から不安全事故の定義に含まれる要素までの最短パスを特定する特定部を更に備える

請求項 1 から請求項 4 のいずれか一項に記載の検証処理装置。

[請求項6] 要素ごとに規定された不具合発生確率に基づいて、前記検査対象モデルが初期状態から不安全事故に至る確率を演算する演算部を更に備える

請求項 1 から請求項 5 のいずれか一項に記載の検証処理装置。

[請求項7] 前記選択部は、前記確率が所定の判定閾値を下回る場合、前記モデル検査の結果に基づき前記一つの要素を選択する処理を省略する

請求項 6 に記載の検証処理装置。

[請求項8] 検査対象モデルに対してモデル検査を実施するステップと、
前記モデル検査の結果に基づき、不安全事故に至る過程で状態が変化した要素の中から一つの要素を選択するステップと、
前記一つの要素を除外してなる検査対象モデルに対して再度のモデル検査を実施するステップと、
を有する検証処理方法。

[請求項9] 検証処理装置のコンピュータに、
検査対象モデルに対してモデル検査を実施するステップと、
前記モデル検査の結果に基づき、不安全事故に至る過程で状態が変化した要素の中から一つの要素を選択するステップと、
前記一つの要素を除外してなる検査対象モデルに対して再度のモデル検査を実施するステップと、
を実行させるプログラム。