

(12) 特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2020年9月3日(03.09.2020)



(10) 国際公開番号

WO 2020/175060 A1

(51) 国際特許分類:
G05B 23/02 (2006.01)

(21) 国際出願番号: PCT/JP2020/004324

(22) 国際出願日: 2020年2月5日(05.02.2020)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(30) 優先権データ:
特願 2019-034227 2019年2月27日(27.02.2019) JP

(71) 出願人: 日立オートモティブシステムズ株式会社(HITACHI AUTOMOTIVE SYSTEMS, LTD.) [JP/JP]; 〒3128503 茨城県ひたちなか市高場 2 5 2 0 番地 Ibaraki (JP).

(72) 発明者: 竹下 若菜 (TAKESHITA, Wakana); 〒1008280 東京都千代田区丸の内一丁目 6 番 6 号 株式会社日立製作所内 Tokyo (JP).
池田 貴広 (IKEDA, Takahiro); 〒1008280 東京都千代田区丸の内一丁目 6 番 6 号 株式会社日立製作所内 Tokyo (JP).

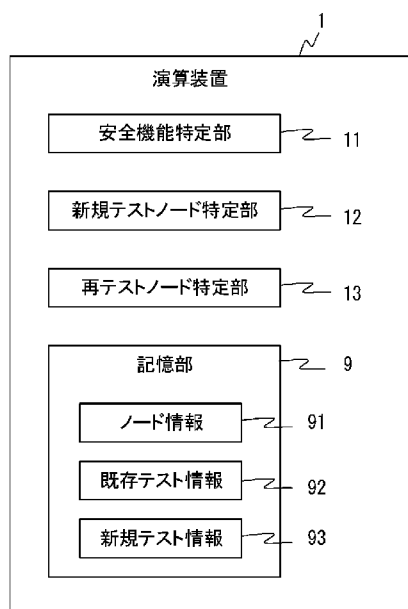
(74) 代理人: 特許業務法人サンネクスト国際特許事務所(SUNNEXT INTERNATIONAL PATENT OFFICE); 〒1400002 東京都品川区東品川二丁目 3 番 1 2 号 シーフォートスクエア センタービルディング 1 6 階 Tokyo (JP).

(81) 指定国(表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH,

(54) Title: COMPUTATION DEVICE AND RECORDING MEDIUM

(54) 発明の名称: 演算装置、記録媒体

【図2】



- 1 Computation device
- 9 Storage unit
- 11 Safety function specifying unit
- 12 New test node specifying unit
- 13 Re-test node specifying unit
- 91 Node information
- 92 Existing test information
- 93 New test information

(57) Abstract: A computation device is provided with: a storage unit for storing, for a fault tree having a plurality of nodes, at least one of the plurality of nodes being related to a safety function, a configuration of the fault tree before a change, a configuration of the fault tree after the change, and information indicating a node tested in a past for each safety function; a safety function specifying unit for specifying, on the basis of information relating to the change of the fault tree, a safety function affected by the change; a re-test node specifying unit for specifying, on the basis of the configuration

CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO,
DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT,
HN, HR, HU, ID, IL, IN, IR, IS, JO, KE, KG, KH,
KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY,
MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ,
NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT,
QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL,
ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG,
US, UZ, VC, VN, WS, ZA, ZM, ZW.

- (84) 指定国(表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, RU, TJ, TM), ヨーロッパ (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

添付公開書類:

- 国際調査報告 (条約第21条(3))

of the fault tree after the change and the node tested in the past, a re-test node, which is a node for testing again the safety function specified by the specifying unit, the node being tested in the past; and a new test node specifying unit for specifying, on the basis of the configuration of the fault tree after the change and the node tested in the past, a new test node, which is a node to be tested newly.

(57) 要約: 演算装置は、複数のノードを有し、複数のノードのうち少なくとも1つのノードは安全機能と関連付けられている故障木について、変更前の故障木の構成、変更後の故障木の構成、および安全機能ごとに過去にテストされたノードを示す情報を格納する記憶部と、故障木の変更に関する情報に基づき変更の影響を受ける安全機能を特定する安全機能特定部と、変更後の故障木の構成および過去にテストされたノードに基づき、特定部により特定された安全機能を再度テストするためのノードであって、過去にテストされたノードである再テストノードを特定する再テストノード特定部と、変更後の故障木の構成および過去にテストされたノードに基づき、新たにテスト対象となるノードである新規テストノードを特定する新規テストノード特定部とを備える。

明 細 書

発明の名称： 演算装置、記録媒体

技術分野

[0001] 本発明は、演算装置、および記録媒体に関する。

背景技術

[0002] 近年、自動車、建設機械、鉄道などの分野において機能安全開発が取り入れられつつある。機能安全とは、製品に安全機能をつけることにより、事故に至るリスクを許容できるレベルまで軽減するという安全性の考え方である。機能安全はISOやIECによって規格化されており、人命に関わる製品において規格準拠が開発要件として求められることが増えてきた。

[0003] 機能安全開発においては、発生する可能性のある事故およびその要因の識別が必須である。事故およびその要因の識別には、リスク分析手法が使われる。リスク分析手法には、発生する可能性のある事故を入力としてそれに至る要因を識別するトップダウン分析手法と、システム内に起こりうる故障を入力としてそれが引き起こす事故を識別するボトムアップ分析手法がある。機能安全開発では通常、トップダウン分析手法とボトムアップ分析手法の両方を組み合わせて使う。代表的なトップダウン分析手法は故障木分析（FTA: Fault Tree Analysis）である。代表的なボトムアップ分析手法はFMEA（Failure Mode and Effect Analysis）である。

[0004] 故障木について、故障木の生成を自動化する手法が存在する。特許文献1にはHAZOPワークシートからハザード発生シナリオに関する情報を抽出して加工し、該情報を起因事象、中間事象、防御手段、ハザード及び影響度という項目に記録し、かつ影響度をキーとして降順ソートしたハザード一覧を作成するためのハザード一覧作成手段と、前記ハザード一覧に記録された対象となるハザードに対して、起因事象ごとに、防御手段があるかどうかを考慮せずに起因事象から、トップ事象となるハザードまでの事象間の因果関係を論理構造として構築し、その事象間の因果関係の論理構造について、防

御手段がある場合の事象に対して、該事象と、その防御手段機能失敗事象をANDゲートで結合し、その防御手段機能失敗事象に対して、防御手段の種類に応じて、予め登録された防御機能失敗に関する基本事象をORゲートで結合し、そのORゲートを防御手段機能失敗事象と結び、前記対象となるハザードに複数の異なる起因事象がある場合、各起因事象に対応する事象間の因果関係の論理構造に存在する同じ中間事象を同定し、該中間事象を発生させる複数の原因事象（下位）をORゲートで結合し、そのORゲートを該中間事象と結び、前記対象となるハザードに関する事象と事象との間の因果関係の論理構造をフォールト・ツリーで表記することによって、ハザードをトップ事象としたフォールト・ツリーを作成し、該フォールト・ツリーをグラフィックで表現するためのフォールト・ツリー作成手段と、前記フォールト・ツリーにおける起因事象と基本事象に、予め登録された故障発生頻度を与えることで、対象となるハザードの発生頻度を算出するためのハザード発生頻度算出手段と、を備えることを特徴とするプロセスリスクアセスメント支援装置が開示されている。

[0005] 機能安全開発において、設計に変更があった場合には、変更の影響範囲の特定とその変更が安全性に対して影響するか否かを特定することが必須である。そのため、設計変更時には必ずリスク分析結果の修正および更新が行われる。リスク分析の更新が製品に及ぼす影響も同様に分析しなければならず、影響が及ぶと思われる部分は再試験を実施する必要がある。

[0006] 再設計時あるいは設計変更時を想定すると、当初の設計に対して変更が行われると、機能安全開発ではリスク分析の再検討および変更に伴う修正が行われる。さらに、変更が及ぼす影響を解析し、影響する箇所は再試験および再検証を実施する必要がある。再試験および再検証が必要な箇所は次のように特定される。まず、リスク分析と要求との間のトレーサビリティ情報を元に、変更箇所が影響する要求や機能を特定する。次に、要求や機能からトレーサビリティで紐付けられたテストケースを取得し、再試験が必要か判断し、必要であるならば再試験を実施する。大規模なシステムあるいは複雑なシ

ステムの場合、再試験が必要なテストケースの検討および実施には多大な工数がかかる。

先行技術文献

特許文献

[0007] 特許文献1：日本国特開2012-98820号公報

発明の概要

発明が解決しようとする課題

[0008] 特許文献1に記載されている発明では、故障木の変更に伴い全テストケースの検討が必要である。

課題を解決するための手段

[0009] 本発明の第1の態様による演算装置は、複数のノードを有し、前記複数のノードのうち少なくとも1つのノードは安全機能と関連付けられている故障木について、変更前の前記故障木の構成、変更後の前記故障木の構成、および前記安全機能ごとに過去にテストされた前記ノードを示す情報を格納する記憶部と、前記故障木の変更にに関する情報に基づき前記変更の影響を受ける前記安全機能を特定する安全機能特定部と、前記変更後の前記故障木の構成および過去にテストされた前記ノードに基づき、前記安全機能特定部により特定された前記安全機能を再度テストするための前記ノードであって、過去にテストされた前記ノードである再テストノードを特定する再テストノード特定部と、前記変更後の前記故障木の構成および過去にテストされた前記ノードに基づき、新たにテスト対象となるノードである新規テストノードを特定する新規テストノード特定部とを備える。

本発明の第2の態様による記録媒体は、複数のノードを有し、前記複数のノードのうち少なくとも1つのノードは安全機能と関連付けられている故障木について、変更前の前記故障木の構成、変更後の前記故障木の構成、および前記安全機能ごとに過去にテストされた前記ノードを示す情報を格納する記憶部を備えるコンピュータに、前記故障木の変更にに関する情報に基づき前

記変更の影響を受ける前記安全機能を特定することと、前記変更後の前記故障木の構成および過去にテストされた前記ノードに基づき、前記特定された前記安全機能を再度テストするための前記ノードであって、過去にテストされた前記ノードである再テストノードを特定することと、前記変更後の前記故障木の構成および過去にテストされた前記ノードに基づき、新たにテスト対象となるノードである新規テストノードを特定することとを実行させるためのプログラムが記録され、コンピュータ読み取り可能である。

発明の効果

[0010] 本発明によれば、故障木の変更に伴う必要なテストケースの数を削減できる。

図面の簡単な説明

[0011] [図1]演算装置 1 のハードウェア構成図

[図2]演算装置 1 の機能構成図

[図3]ノード情報 9 1 の一例を示す図

[図4]故障木の変更前後の一例を示す図

[図5]既存テスト情報 9 2 の一例を示す図

[図6]新規テスト情報 9 3 の一例を示す図

[図7]第 1 の実施の形態における演算装置 1 の全体処理を示すフローチャート

[図8]新規テストノード特定部 1 2 の処理を示すフローチャート

[図9]新規中核処理を示すフローチャート

[図10]再テストノード特定部 1 3 の処理を示すフローチャート

[図11]再テスト中核処理を示すフローチャート

[図12]カウント数と対象ノードリストの一例を示す図

[図13]決定処理を示すフローチャート

[図14]変形例 2 においてプログラムを外部から読み込む様子を示す図

[図15]第 2 の実施の形態における既存テスト情報 9 2 A の一例を示す図

[図16]第 2 の実施の形態における演算装置 1 A の全体処理を示すフローチャート

発明を実施するための形態

[0012] 一第 1 の実施の形態一

以下、図 1 ～図 1 3 を参照して、演算装置の第 1 の実施の形態を説明する。本実施の形態では、故障テストとして故障挿入テストを行う。故障挿入テストとは、故障事象を発生させ、安全機能が正常に作動することを試すテストである。

[0013] (ハードウェア構成)

図 1 は、本発明に係る演算装置 1 のハードウェア構成図である。演算装置 1 は、中央演算処理装置である CPU 2 と、不揮発性で読み出し専用の ROM 3 と、揮発性で読み書き可能な RAM 4 と、外部と情報を授受するインタフェース 8 と、不揮発性で読み書き可能な記憶部 9 とを備える。ROM 3 にはあらかじめプログラムが格納されている。CPU 2 は、ROM 3 に格納されているプログラムを RAM 4 に展開して実行することで後述する機能を実現する。

[0014] インタフェース 8 は、通信により外部と情報を授受する通信インタフェース、または物理メディアを読み込み可能なインタフェースである。通信インタフェースとはたとえば、IEEE 802. 3 に対応する有線通信モジュール、または無線 LAN や 4 G などに対応する無線通信モジュールである。記憶部 9 はたとえばハードディスクドライブやフラッシュメモリである。記憶部 9 には後述する情報があらかじめ格納される。ただし記憶部 9 に格納される情報は、インタフェース 8 を介して外部から入力されてもよい。

[0015] (機能構成)

図 2 は、演算装置 1 の機能構成図である。ただし図 2 には記憶部 9 に格納される情報も示している。演算装置 1 はその機能として、安全機能特定部 1 1 と、新規テストノード特定部 1 2 と、再テストノード特定部 1 3 とを備える。これらの機能は、CPU 2 が ROM 3 に格納されるプログラムを実行することにより実現される。記憶部 9 には、ノード情報 9 1 と、既存テスト情報 9 2 と、新規テスト情報 9 3 とが格納される。

- [0016] 安全機能特定部 1 1、新規テストノード特定部 1 2、および再テストノード特定部 1 3 は、記憶部 9 に格納されているノード情報 9 1、および既存テスト情報 9 2 を対象として演算を行い、新規テスト情報 9 3 を作成する。すなわち図 2 では記憶部 9 には、ノード情報 9 1、既存テスト情報 9 2、および新規テスト情報 9 3 が格納されているが、このうちノード情報 9 1 と既存テスト情報 9 2 があらかじめ作成されている情報であり、新規テスト情報 9 3 は新たに作成される情報である。
- [0017] 安全機能特定部 1 1 は、故障木の変更に関する情報に基づき変更の影響を受ける安全機能を特定する。新規テストノード特定部 1 2 は、安全機能特定部 1 1 により特定された安全機能を再度テストするためのノードであって、過去にテストされたノードである再テストノードを特定する。新規テストノード特定部 1 2 は、変更後の故障木の構成および過去にテストされたノードに基づき、新規テストノードを特定する。再テストノード特定部 1 3 は、新たにテスト対象となるノードである新規テストノードを特定する。再テストノード特定部 1 3 は、変更後の故障木の構成および過去にテストされたノードに基づき、再テストノードを特定する。
- [0018] 故障木は、故障事象や異常事象、セキュリティリスク事象など、リスク事象から構成される木構造である。また、その他のリスク分析手法で生成される木構造も故障木に含む。すなわち故障木は、リスク事象を表現するノードから構成される木構造であればよい。故障木は事象を表す複数のノードから構成される。
- [0019] ノード情報 9 1 には、故障木を構成する各ノードの情報が格納される。ノードの情報とは、ノードごとの故障木における位置を特定可能な情報である。本実施の形態では、ノード情報 9 1 にはさらに、各ノードが対応する安全機能の識別子も格納される。ノード情報 9 1 は人間が作成してもよいし、既知の自動処理により作成してもよい。既存テスト情報 9 2 は、人間が作成してもよいし、既知の自動処理により作成してもよいし、演算装置 1 が過去に作成したものであってもよい。

[0020] すなわち次のように新規テスト情報 9 3 が既存テスト情報 9 2 として扱われてもよい。たとえばまずノード情報 9 1 が更新され、演算装置 1 が新規テスト情報 9 3 を作成する。そして、作成した新規テスト情報 9 3 に記載のテストが実行され、さらにノード情報 9 1 が再度更新された場合を想定する。この場合に演算装置 1 は、従前に作成した新規テスト情報 9 3 を既存テスト情報 9 2 として扱い、改めて新規テスト情報 9 3 を作成してもよい。

[0021] 既存テスト情報 9 2 には、過去に実行されたテストの内容が記載される。既存テスト情報 9 2 と新規テスト情報 9 3 に格納される情報は同種である。既存テスト情報 9 2 と新規テスト情報 9 3 は同一の記載フォーマットを採用してもよいし、記載フォーマットが異なってもよい。

[0022] (ノード情報)

図 3 は、記憶部 9 に格納されるノード情報 9 1 の一例を示す図である。ただし図 3 はノード情報 9 1 の例示に過ぎず、情報の格納は表形式に限定されない。ノード情報 9 1 は複数のレコードから構成され、各レコードは、ノード ID、上位ゲート ID、下位ゲート ID、安全機能 ID、および新旧のフィールドを有する。各レコードにはノード ID のフィールドに格納される情報により特定されるノード（以下、「対象ノード」と呼ぶ）に関する情報が格納される。なお図 3 に示す例ではゲートの種類が記載されていないが、図 3 にゲートの種類の情報が含まれてもよいし、ゲートの種類を示す情報のみが記憶部 9 に別途含まれてもよい。

[0023] 「ノード ID」のフィールドには、対象ノードを識別する識別子が格納される。「上位ゲート ID」のフィールドには、対象ノードの上位のゲートを識別する識別子が格納される。ただし上位のゲートが存在しない場合には、存在しないことを示す記号、たとえば「-」が格納される。「下位ゲート ID」のフィールドには、対象ノードの下位のゲートを識別する識別子が格納される。ただし下位のゲートが存在しない場合には、存在しないことを示す記号、たとえば「-」が格納される。

[0024] 「安全機能 ID」のフィールドには、対象ノードの事象に対する安全機能

を識別する識別子が格納される。ただし対象ノードの事象に対する安全機能が存在しない場合はその旨を示す記号、たとえば「－」が格納される。また「安全機能 I D」のフィールドには、対象ノードの事象に対する安全機能を識別する識別子の代わりに、対象ノードの事象に対する安全要求、安全要件、および設計情報のいずれかの識別子が格納されてもよい。

[0025] 「新旧」のフィールドには、対象ノードが既存のものであるか、それとも変更により追加削除されたものであるかを示す情報が格納される。図 3 に示す例では変更により 3 つのノードが追加されたことが示されている。ただし「新旧」のフィールドは必須の構成ではなく、変更の前後でそれぞれノード情報 9 1 が存在する場合には「新旧」のフィールドが備えられなくてもよい。

[0026] (故障木の例)

図 4 は、故障木の変更前後の一例を示す図であり、前述の図 3 に対応する。厳密には図 4 は、図 3 に示す故障木の構成のみを視覚的に示した図である。図 4 に示す故障木は、N 1 0 1 から N 1 1 3 までの全 1 3 個のノードと、G 1 1 から G 1 6 までの全 6 個のゲートとから構成される。ゲート N 1 0 1 が最上位のノードであり、図示下方向にあるほど下位のノードである。図 4 では、変更前の故障木の構成を実線で示し、変更により追加された故障木の構成を破線で示す。すなわち図 4 に示す例の変更ではいずれにノードも削除されていない。ゲートは AND ゲートと OR ゲートの 2 種類が含まれ、図 4 に示す例ではその形状によりゲートの種類を示している。図 4 に示す例ではゲート G 1 3 のみが AND ゲートであり、それ以外の 5 つのゲートは OR ゲートである。

[0027] 上位のノードは、ゲートによって下位のノードと接続される。OR ゲートは、下位ノードの事象のうちどれか 1 つでも発生すれば上位ノードの事象が発生することを意味する。AND ゲート 2 0 3 は、下位ノードの事象の全てが発生した際に、上位ノードの事象が発生することを意味する。たとえばゲート G 1 1 は OR ゲートなので、ノード N 1 0 2 およびノード N 1 0 3 のい

いずれかの事象が発生すればノードN101の事象が発生する。以下では、下位にゲートを有しないノードを「末端ノード」と呼び、末端ノード以外のノードを「非末端ノード」と呼ぶ。図4に示す例では、ノードN104、N106、N108、N109、N110、N112、N113が末端ノードである。

[0028] また以下では、ゲートを挟んで上下関係にあるノード同士を「一段上位のノード」と呼ぶ。たとえば図4に示す例において、ノードN110の一段上位のノードはノードN107である。

[0029] 図4に示す例では、変更によりゲートG13の下にノードN111、ゲートG16、ノードN112、およびノードN113が追加されている。ゲートG13がANDノードであることは変更がない。変更前は、ノードN106およびノードN107の両方の事象が発生するとノードN103の事象が発生していたが、変更後はこれら2つの事象に加えてノードN111の事象が発生しなければ、ノードN103の事象が発生しない。

[0030] (既存テスト情報)

図5は、既存テスト情報92の一例を示す図であり、前述の図3に対応する。既存テスト情報92は複数のレコードから構成される。既存テスト情報92の各レコードは、テストケースID、安全機能ID、および故障挿入箇所のフィールドを有する。各レコードには「テストケースID」のフィールドに格納される情報により特定されるテストケース（以下、「対象テストケース」と呼ぶ）に関する情報が格納される。

[0031] 「テストケースID」のフィールドには、対象テストケースを識別する識別子が格納される。「安全機能ID」のフィールドには、対象テストケースにおいてテストされる安全機能を識別する識別子が格納される。「故障挿入箇所」のフィールドには、対象テストケースにおいて発生させる故障事象に対応するノードの識別子が格納される。

[0032] 図5の最初のレコードに示す例では、IDが「TC1」であるテストケースでは、安全機能IDが「SF1」である安全機能のテストが行われること

が示されている。さらにそのテストケースでは、ノードN104およびノードN108に対応する故障事象が発生させられることが示されている。

[0033] (新規テスト情報)

図6は、新規テスト情報93の一例を示す図であり、前述の図3に対応する。新規テスト情報93の構成は既存テスト情報92と同一なので説明を省略する。

[0034] (フローチャート)

以下、図7～図13を参照して演算装置1の動作を説明する。また以下のフローチャートの説明では、図3や図4などに示した例を参照して具体的な動作を補足説明する。

[0035] (フローチャート 全体処理)

図7は、第1の実施の形態における演算装置1の全体処理を示すフローチャートである。演算装置1は、インタフェース8を介して外部から既存の故障木に対する構成の変更を受信すると、図7に示す処理を開始する。ただし予め記憶部9に新旧の故障木の構成、および既存テスト情報92が格納された状態で、外部から処理開始の指令を受けた場合に図7に示す処理を開始してもよい。図7に示す処理が開始される時点で、記憶部9にはノード情報91および既存テスト情報92が格納されている。

[0036] なお以下に説明するフローチャートでは、故障木を構成する全ノードについて「通過フラグ」を個別に設定し演算に利用する。通過フラグとは、真偽の2値をとる変数であり以下に説明するフローチャート中でのみ利用される。通過フラグの情報は、RAM4に格納される。

[0037] 演算装置1の安全機能特定部11はまず、ノード情報91を参照して、故障木の構成の変更が影響する安全機能を特定する(S701)。影響する安全機能とは、変更が行われた箇所から最上位のノードに向かって順番に辿った際に通過する全てのノードに紐付けられた安全機能である。図4に示す例では、追加された故障木から最上位のノードに向かって辿ると、ノードN103とノードN101が存在する。そして、ノードN101は安全機能ID

を有さずノードN103のみが安全機能ID「SF2」を有するので、S701では「SF2」が特定される。

[0038] 次に演算装置1は、記憶部106の既存テスト情報92を参照し、故障挿入箇所を設定されているノードを特定する。図5に示す例では、故障挿入箇所を設定されているノードとして、ノードN104、ノードN106、ノードN108、およびノードN109が特定される。

[0039] 次に演算装置1は、S701において特定した全ての安全機能を順番に「対象安全機能」として選択し、S703とS708との間に存在する処理、すなわちS704～S707を実行する。たとえばS701において特定した安全機能がSF7とSF8である場合は、まずは対象安全機能をSF7としてS704～S707を実行し、次に対象安全機能をSF8としてS704～S707を実行する。図3に示す例ではS701において特定される安全機能はSF2のみなのでS704～S707は1回のみ実行される。

[0040] S704～S707の処理は次のとおりである。まず、全ノードの通過フラグに偽を設定する(S704)。次に、新規テストノード特定部12が、新規にテストすべきノード、すなわち新規テストノードを特定する(S705)。S705の詳細は図8を参照して後に説明する。次に、再テストノード特定部13が、過去にテストしたノードの中から再試験を実施すべきノード、すなわち再テストノードを特定する(S706)。S706の詳細は図10を参照して後に説明する。

[0041] そして演算装置1は、S705とS706で特定されたノードを故障挿入箇所とするテストケースを作成する(S707)。S707の具体的な動作は後述する。以上がS704～S707の処理内容である。最後に演算装置1は、S707で作成したテストケースを出力して(S709)、図7に示す処理を終了する。

[0042] (フローチャート 新規テストノード特定部)

図8は、新規テストノード特定部12の処理を示すフローチャートであり、図7のS705の詳細を示すフローチャートである。まず新規テストノード

ド特定部12は、故障木における変更に係る最上位ノードを特定する（S801）。図3や図4に示す例では、ノードN111～N113およびゲートG16が追加されたので、変更に係る最上位ノードはノードN111である。仮にノードN111～N113だけでなくノードN108も変更により追加されていた場合には、S801ではノードN108およびノードN111が特定される。

[0043] 次に新規テストノード特定部12は、S801において特定した全ての最上位ノードを対象ノードとしてS803およびS804の処理を実行する。S803では新規テストノード特定部12は、新規テストの対象となるノードを特定する新規中核処理を実行する。S803の詳細は図9を参照して後述する。S804では新規テストノード特定部12は、S803において出力されるリストを記録する。新規テストノード特定部12は、S801において特定した全ての最上位ノードを対象にS803およびS804の処理が完了すると、S804において記録したリストを出力して（S806）、図8に示す処理を終了する。なおS806において出力したリストは、図7のS707において利用される。

[0044] （フローチャート 新規中核処理）

図9は、新規中核処理を示すフローチャートであり、図8のS803の詳細を示すフローチャートである。図9に示す処理では、図8のS801において特定したノードが「対象ノード」に設定されて実行される。新規テストノード特定部12はまず、対象ノードの通過フラグを「真」に設定する。次に新規テストノード特定部12は対象ノードが末端ノードであるか否かを判断する（S902）。前述のとおり、末端ノードは下位にゲートを有しないノードである。新規テストノード特定部12は、対象ノードが末端ノードであると判断する場合は、対象ノードのみを要素とするリストを作成して出力し（S903）、図9に示す処理を終了する。新規テストノード特定部12は、対象ノードが末端ノードではないと判断する場合はS906に進む。

[0045] S906では新規テストノード特定部12は、対象ノードの下位ゲートは

ANDゲートであるか否かを判断し、下位ゲートがANDゲートであると判断する場合はS 9 1 1に進み、下位ゲートがORゲートであると判断する場合はS 9 2 1に進む。新規テストノード特定部 1 2は、S 9 1 1～S 9 1 3において、対象ノードよりも下位の全ノードを順番に「ループ対象」としてS 9 1 2の処理を実行する。たとえば図3に示す例においてノードN 1 0 2が処理対象の場合には、たとえばノードN 1 0 4をループ対象としてS 9 1 2を実行し、次にノードN 1 0 5をループ対象としてS 9 1 2を実行し、最後にノードN 1 0 8をループ対象としてS 9 1 2を実行する。

[0046] S 9 1 2では新規テストノード特定部 1 2は、ループ対象を対象ノードとして図9に示す新規中核処理を実行する。すなわちS 9 1 2は再帰呼び出しである。たとえば前述の例においてノードN 1 0 4をループ対象としてS 9 1 2を実行すると、ノードN 1 0 4を対象ノードとして図9に示す新規中核処理が実行される。新規テストノード特定部 1 2は、対象ノードの全ての下位ノードをループ対象としてS 9 1 2を実行するとS 9 1 4に進む。

[0047] S 9 1 4では新規テストノード特定部 1 2はS 9 1 2の処理により出力されるリストを組み合わせたリストを作成する。たとえば前述のとおり、対象ノードがN 1 0 2の場合にはループ対象はノードN 1 0 4、N 1 0 5、およびN 1 0 8である。この3つのそれぞれが対象ノードとして新規中核処理を実行すると出力されるリストはN 1 0 2、N 1 0 4、およびN 1 0 8である。そのためS 9 1 4ではこれらを組み合わせたリストとしてN 1 0 2、N 1 0 4、N 1 0 8、{N 1 0 2、N 1 0 4}、{N 1 0 2、N 1 0 8}、{N 1 0 4、N 1 0 8}、{N 1 0 2、N 1 0 4、N 1 0 8}が作成される。ただしここでは、1つのリストに複数の要素が含まれる場合は波括弧を使って1つのリストの範囲を明示している。続くS 9 1 5では新規テストノード特定部 1 2は、S 9 1 4において作成したリストを出力して図9に示す処理を終了する。

[0048] 新規テストノード特定部 1 2は、S 9 2 1～S 9 2 4において、対象ノードよりも下位の全ノードを順番に「ループ対象」としてS 9 2 2およびS 9

23の処理を実行する。たとえば図3に示す例においてノードN102が処理対象の場合には、ノードN104、N105、N108をループ対象としてS922とS923を実行する。S922では新規テストノード特定部12は、ループ対象を対象ノードとして図9に示す新規中核処理を実行する。すなわちS922は再帰呼び出しである。S923では新規テストノード特定部12は、S922の処理により出力されるリストを出力する。新規テストノード特定部12は、対象ノードの全ての下位ノードをループ対象としてS922およびS923を実行すると図9に示す処理を終了する。

[0049] S911～S915で実行される処理と、S921～S924で実行される処理は似ているが細部が異なる。すなわちS911～S915では、再帰処理によりS912で新規中核処理を実行して出力されたリストをそのまま出力するのではなく、組み合わせて出力する。その一方でS921～S924では、再帰処理によりS922で新規中核処理を実行して出力されたリストをそのまま出力する。

[0050] 実際にはS906の判断が存在するので、同一の対象ノードがS911～S915とS921～S924の両方を実行することはないが、説明のためにあえて記載すると、対象ノードが同一であってもS911～S915とS921～S924では、呼び出し元である図8のS803において出力されるリストが次のように異なる。すなわちS911～S915ではN102、N104、N108、{N102、N104}、{N102、N108}、{N104、N108}、{N102、N104、N108}が出力され、S921～S924ではN102、N104、およびN108が出力される。

[0051] (フローチャート 再テストノード特定部)

図10は、再テストノード特定部13の処理を示すフローチャートであり、図7のS706の詳細を示すフローチャートである。なお図10に示す処理は、S1001～S1006により構成されるが、S1003を除いて、図8に示すS801～S806の処理にそれぞれ対応する。ここではS10

03の処理だけを説明する。S1003では再テストノード特定部13は、再テストの対象となるノードを特定する再テスト中核処理を実行する。S1003の詳細は図11を参照して後述する。

[0052] 図11は、再テスト中核処理を示すフローチャートであり、図11のS1003の詳細を示すフローチャートである。図11に示す処理では、図10のS1001において特定したノードが「対象ノード」に設定されて実行される。図11ではまず再テストノード特定部13は、対象ノードが故障木の最上位ノードであるか否かを判断する（S1011）。再テストノード特定部13は、対象ノードが最上位ノードであると判断する場合は、図9に示す処理を終了し、対象ノードが最上位ノードではないと判断する場合はS1012に進む。

[0053] S1012では再テストノード特定部13は、対象ノードの上位ゲートはANDゲートであるか否かを判断し、上位ゲートがANDゲートであると判断する場合はS1021に進み、上位ゲートがORゲートであると判断する場合はS1013に進む。S1013では再テストノード特定部13は、対象ノードの一段上位のノードの通過フラグを真に設定してS1014に進む。たとえば対象ノードが図3に示すノードN107の場合に、S1013ではノードN103の通過フラグが真に設定される。

[0054] S1014では再テストノード特定部13は、対象ノードの1段上位のノードの安全機能IDは対象安全機能、すなわち図7のS701において特定した安全機能の1つであって、1つずつ順番に選択された安全機能と一致するか否かを判断する。再テストノード特定部13は、対象ノードの1段上位のノードの安全機能IDが対象安全機能と一致すると判断する場合は図11に示す処理を終了する。再テストノード特定部13は、対象ノードの1段上位のノードの安全機能IDが対象安全機能と一致しないと判断する場合は、対象ノードを現在の対象ノードの1段上位のノードに変更してS1012に戻る。

[0055] たとえば対象ノードが図3に示すノードN107の場合に、S1013で

はノードN103の安全機能IDが対象安全機能と一致するか否かが判断される。ノードN103の安全機能IDは図3の例によればSF2なので、対象安全機能がSF2であれば肯定判断される。仮に対象ノードの1段上位のノードが安全機能IDを有しない場合は、対象安全機能がどのような値であってもS1013では否定判断がされる。

[0056] 再テストノード特定部13は、S1021～S1030において、対象ノードの上位ゲートであるANDゲート以下の全ノードを順番に「ループノード」としてS1022～S1029の処理を実行する。S1022では再テストノード特定部13は、ループノードの通過フラグが偽であるか否かを判断し、ループノードの通過フラグが偽であると判断する場合はS1023に進み、ループノードの通過フラグが偽ではない、すなわち真であると判断する場合はS1030に進む。S1023では再テストノード特定部13は、ループノードの通過フラグを真に設定してS1024に進む。

[0057] S1024では再テストノード特定部13は、ループノードはテスト済であるか否か、すなわち既存テスト情報92のいずれかのテストケースにおいて故障挿入箇所を設定されているか否かを判断する。再テストノード特定部13は、ループノードが既存テスト情報92のいずれかのテストケースにおいて故障挿入箇所を設定されていると判断する場合はS1025に進む。再テストノード特定部13は、ループノードが既存テスト情報92のいずれかのテストケースにおいても、故障挿入箇所を設定されていないと判断する場合はS1026に進む。

[0058] S1025では再テストノード特定部13は、ループノードをテスト対象に選択してS1029に進む。S1026では再テストノード特定部13は、ループノードの下位ゲートはANDゲートであるか否かを判断する。再テストノード特定部13は、ループノードの下位ゲートはANDゲートであると判断する場合はS1030に進み、ループノードの下位ゲートはANDゲートではない、すなわちORゲートであると判断する場合はS1027に進む。

[0059] S 1 0 2 7では再テストノード特定部 1 3は、ループノードの下位ゲートであるORゲート以下の全ノードを順番に評価ノードとして図 1 3に示す決定処理を実行する。たとえば図 3に示す例においてループノードがノード N 1 0 7の場合に、ノード N 1 0 7の下位ゲートはゲート G 1 5なので、ノード N 1 0 9とノード N 1 1 0が順番に評価ノードとして図 1 3に示す決定処理が実行される。詳しくは後述するが、この決定処理では、カウント数と対象ノードリストが出力される。続く S 1 0 2 8では再テストノード特定部 1 3は、S 1 0 2 7において実行した決定処理において最小のカウント数である対象ノードリストをテスト対象に選択し、S 1 0 2 9に進む。

[0060] 図 1 2は、カウント数と対象ノードリストの一例を示す図である。仮に S 1 0 2 7においてORゲート以下のノードが全部で4つあり、それぞれの出力が図 1 2に示すものである場合に S 1 0 2 9ではカウント数が最小である 1 行目の対象ノードリスト、すなわちノード N 2 0 1がテスト対象に選択される。

[0061] S 1 0 2 9では再テストノード特定部 1 3は、テスト対象を1つのリストとして出力する。再テストノード特定部 1 3は、対象ノードの上位ゲートであるANDゲート以下の全ノードをループノードとして S 1 0 2 2～S 1 0 2 9の処理を実行すると、図 1 1に示す処理を終了する。

[0062] (フローチャート 決定処理)

図 1 3は、決定処理を示すフローチャートであり、図 1 1の S 1 0 2 7の詳細を示すフローチャートである。再テストノード特定部 1 3はまず、カウント数をゼロに、対象ノードリストをNULL、すなわち空白状態に初期化する(S 1 1 0 1)。次に再テストノード特定部 1 3は、評価ノードはテスト済みであるか否か、すなわち既存テスト情報 9 2のいずれかのテストケースにおいて故障挿入箇所を設定されているか否かを判断する。再テストノード特定部 1 3は、評価ノードが既存テスト情報 9 2のいずれかのテストケースにおいて故障挿入箇所を設定されていると判断する場合は S 1 1 0 3に進む。再テストノード特定部 1 3は、評価ノードが既存テスト情報 9 2のい

れかのテストケースにおいても、故障挿入箇所に設定されていないと判断する場合はS 1 1 0 4に進む。

[0063] S 1 1 0 3では再テストノード特定部13は、カウント数に「1」、対象ノードリストに評価ノードを設定してS 1 1 3 1に進む。S 1 1 3 1では再テストノード特定部13は、設定されたカウント数と対象ノードリストを出力して図13に示す処理を終了する。

[0064] S 1 1 0 4では再テストノード特定部13は、評価ノードの下位ゲートはANDゲートであるか否かを判断し、下位ゲートがANDゲートであると判断する場合はS 1 1 1 1に進み、下位ゲートがORゲートであると判断する場合はS 1 1 2 1に進む。

[0065] 再テストノード特定部13は、S 1 1 1 1～S 1 1 1 4において、評価ノードよりも下位の全ノードを順番に「ループ対象」としてS 1 1 1 2の処理を実行する。S 1 1 1 2では再テストノード特定部13は、ループ対象を評価ノードとして図13に示す決定処理を実行する。すなわちS 1 1 1 2は再帰呼び出しである。続くS 1 1 1 3では再テストノード特定部13は、S 1 1 1 2を実行することにより出力されるカウント数と対象ノードリストを一時的に記録する。再テストノード特定部13は、評価ノードの全ての下位ノードをループ対象としてS 1 1 1 2およびS 1 1 1 3を実行するとS 1 1 1 5に進む。

[0066] S 1 1 1 5では再テストノード特定部13は、カウント数をS 1 1 1 3において記録したカウント数の総計に設定し、対象ノードリストをS 1 1 1 3において記録した全てのノードリストに設定してS 1 1 3 1に進む。S 1 1 1 3において記録したカウント数と対象ノードリストが図12に示すものの場合に、S 1 1 1 5ではカウント数は1、2、2、3の総計である「8」に設定され、対象ノードリストは、ノードN 2 0 1～N 2 0 8に設定される。

[0067] 再テストノード特定部13は、S 1 1 2 1～S 1 1 2 4において、評価ノードよりも下位の全ノードを順番に「ループ対象」としてS 1 1 2 2の処理を実行する。S 1 1 2 2では再テストノード特定部13は、ループ対象を評

価ノードとして図 1 3 に示す決定処理を実行する。すなわち S 1 1 2 2 は再帰呼び出しである。続く S 1 1 2 3 では再テストノード特定部 1 3 は、S 1 1 2 2 を実行することにより出力されるカウント数と対象ノードリストを一時的に記録する。再テストノード特定部 1 3 は、評価ノードの全ての下位ノードをループ対象として S 1 1 2 2 および S 1 1 2 3 を実行すると S 1 1 2 5 に進む。

[0068] S 1 1 2 5 では再テストノード特定部 1 3 は、カウント数を S 1 1 1 3 において記録したカウント数の最小値に設定し、対象ノードリストを最初のカウント数に対応するノードリストに設定して S 1 1 3 1 に進む。なお最小のカウント数が複数存在する場合には、対象ノードリストに設定するノードリストは、最小のカウント数に対応するノードリストのいずれでもよい。テストの演算量を減らすために最小のカウント数を選択しているので、対象ノードとしていずれを選択してもテストの演算量には影響がないからである。

[0069] S 1 1 2 5 の具体例を説明する。S 1 1 2 3 において記録したカウント数と対象ノードリストが図 1 2 に示すものの場合に、S 1 1 2 5 では最小のカウント数である「1」に設定し、対象ノードリストはカウント数が「1」であるノード N 2 0 1 に設定する。以上が図 1 3 に示す処理の説明である。

[0070] 上述した第 1 の実施の形態によれば、次の作用効果が得られる。

(1) 演算装置 1 は、複数のノードを有し、複数のノードのうち少なくとも 1 つのノードは安全機能と関連付けられている故障木について、変更前の故障木の構成、変更後の故障木の構成、および安全機能ごとに過去にテストされたノードを示すノード情報 9 1 を格納する記憶部 9 と、故障木の変更に關する情報に基づき変更の影響を受ける安全機能を特定する安全機能特定部 1 1 と、変更後の故障木の構成および過去にテストされたノードに基づき、再テストノードを特定する再テストノード特定部 1 3 と、変更後の故障木の構成および過去にテストされたノードに基づき、新規テストノードを特定する新規テストノード特定部 1 2 とを備える。そのため、故障木の変更に伴う必要なテストケースの数を削減できる。

- [0071] (2) 安全機能特定部 11 は、変更により追加されたノードから故障木の最上位のノードまで辿った際に通過する全てのノードのそれぞれに関連付けられる安全機能を、変更の影響を受ける安全機能として特定する。
- [0072] (3) 再テストノード特定部 13 は、変更により追加されたノードのうち最上位のノードを対象ノードとし、対象ノードが変更による変更後の故障木における最上位のノードである場合は再テストノードへの追加を行わない（図 11 の S1011 : YES）。
- [0073] (4) 再テストノード特定部 13 は、対象ノードに接続される上位のゲートが AND ゲートの場合は、当該 AND ゲートに接続するそれぞれのノードの事象が発生するように、当該 AND ゲート以下のノードであって過去にテストされたノードを再テストノードに追加する（図 11 の S1012 : YES、S1021 ~ S1030）。
- [0074] (5) 新規テストノード特定部 12 は、変更により追加されたノードのうち最上位のノードを対象ノードとし、対象ノードが下位のノードを有しない場合は対象ノードを新規テストノードに追加し（図 9 の S902 : YES、S903）、対象ノードが下位のノードを有する場合は対象ノードを新規テストノードに追加しない（S902 : NO、S906 以降）。
- [0075] (6) 新規テストノード特定部 12 は、対象ノードが下位のノードを有する場合であって、対象ノードに接続される下位ゲートが AND ゲートの場合は、当該 AND ゲートに接続される全てのノードの事象が発生するように AND ゲート以下のノードを新規テストノードに追加する（S906 : YES、S911 ~ S915）。対象ノードが下位のノードを有する場合であって、対象ノードに接続される下位ゲートが OR ゲートの場合は、当該 OR ゲートに接続されるいずれか 1 つのノードの事象が発生するように当該 OR ゲート以下のノードを新規テストノードに追加する（S906 : NO、S921 ~ S924）。
- [0076] (変形例 1)

上述した第 1 の実施の形態では、故障木を構成するノードおよびゲートの

情報がノード情報 91 に格納され、さらに各ノードが対応する安全機能の識別子もノード情報 91 に格納された。しかしノード情報 91 にゲートの情報を含めず、ゲートの情報を個別に記憶部 9 に格納してもよい。また安全機能の情報もノード情報 91 に含めなくてもよい。

[0077] (変形例 2)

演算装置 1 を動作させるためのプログラムは、予め ROM に格納されていなくてもよく、次のように外部から読み込まれてもよい。図 14 は、プログラムを外部から読み込む様子を示す図である。演算装置 1 に対するプログラムの供給は、プログラムを格納した CD-ROM などの記録媒体 904 を演算装置 1 にセットして行ってもよいし、ネットワークなどの通信回線 901 を経由する方法で演算装置 1 へ読み込ませてもよい。通信回線 901 を経由する場合は、当該通信回線に接続されたサーバー 902 のストレージ装置 903 などにプログラムを格納しておく。

[0078] サーバー 902 はストレージ装置 903 を使用してプログラムの情報を読み出し、通信回線 901 を介して演算装置 1 に送信する。すなわち、プログラムをデータ信号として搬送波を介して、通信回線 901 を介して送信する。このように、演算装置 1 を動作させるためのプログラムは、記録媒体やデータ信号（搬送波）などの種々の形態のコンピュータ読み込み可能なコンピュータプログラム製品として供給できる。

[0079] (変形例 3)

演算装置 1 は、CPU 2、ROM 3、および RAM 4 の組み合わせの代わりに書き換え可能な論理回路である FPGA (Field Programmable Gate Array) や特定用途向け集積回路である ASIC (Application Specific Integrated Circuit) により実現されてもよい。また演算装置 1 は、CPU 2、ROM 3、および RAM 4 の組み合わせの代わりに、異なる構成の組み合わせ、たとえば CPU、ROM、RAM と FPGA の組み合わせにより実現されてもよい。

[0080] 一第 2 の実施の形態一

図 1 5 ～図 1 6 を参照して、演算装置の第 2 の実施の形態を説明する。以下の説明では、第 1 の実施の形態と同じ構成要素には同じ符号を付して相違点を主に説明する。特に説明しない点については、第 1 の実施の形態と同じである。本実施の形態では、故障木の構成に変更があった場合に、故障挿入テスト以外のテストについて、新規にテストが必要な箇所を特定するとともに、テスト済みの部分については回帰テスト対象となるテストケースを特定する。第 1 の実施の形態と同じ構成には同じ番号を付与して説明を省略する。本実施の形態では、故障挿入テストだけではなく開発中に実施されたテスト、たとえば、総合テスト、結合テスト、単体テストなども実施する。

[0081] (構成)

第 2 の実施の形態における演算装置 1 A のハードウェア構成は、第 1 の実施の形態と同様なので説明を省略する。第 2 の実施の形態における演算装置 1 A の動作が第 1 の実施の形態と一部のみ異なる。また本実施の形態では記憶部 9 には、既存テスト情報 9 2 および新規テスト情報 9 3 の代わりに既存テスト情報 9 2 A および新規テスト情報 9 3 A が格納される。

[0082] 本実施の形態における既存テスト情報 9 2 A は、第 1 の実施の形態における既存テスト情報 9 2 の情報に加えてテスト種別の情報が格納される。新規テスト情報 9 3 A の構成も同様である。

[0083] 図 1 5 は第 2 の実施の形態における既存テスト情報 9 2 A の一例を示す図である。既存テスト情報 9 2 A の各レコードは、第 1 の実施の形態における既存テスト情報 9 2 のフィールドに加えてテスト種別のフィールドを有する。またテストの種別が故障挿入テストに限定されないため、「故障挿入箇所」のフィールドが「対象ノード」に改称される。

[0084] 図 1 6 は第 2 の実施の形態における演算装置 1 A の全体処理を示すフローチャートである。図 1 6 は、第 1 の実施の形態における図 7 から S 7 0 7 を削除して S 1 5 0 7 および S 1 5 0 8 を追加したものである。ここでは追加した S 1 5 0 7 および S 1 5 0 8 のみ説明する。S 1 5 0 7 では、演算装置 1 A は、S 7 0 5 および S 7 0 6 で特定されたノードについて新規テストノ

ード特定部 1 2 A を参照してそのノードがテスト対象となったテストケースを選択する。この際に、そのノードがテスト対象となった全てのテストケースを選択してもよいし、テスト種別を限定してもよい。

[0085] たとえば S 7 0 5 および S 7 0 6 で特定されたノードが N 3 0 1 であり、既存テスト情報 9 2 A が図 1 5 に示すものの場合に、次のテストケースが選択される。すなわち、ノード N 3 0 1 はテストケース T C 1 1 および T C 1 2 の両方において対象ノードとなっているので、テストケース T C 1 1 および T C 1 2 の両方のテストケースが選択される。ただしあらかじめオペレータなどがテスト種別を結合テストに限定していた場合には、テストケース T C 1 1 のみが選択される。

[0086] 次に演算装置 1 A は、S 1 5 0 8 において、S 7 0 5 で特定されたノードから新規にテストケースを作成すべきノードを特定する。なお特定されたすべてのノードのうち、ノード情報にテストケースが設定されていないノードは、すべてテストケースを作成するノードとなる。また、新規のテストケースのテスト種別は特に限定されないが、たとえば故障挿入テストとすることができ。以上の処理によって、回帰テスト対象のテストケースの特定、および、新規テスト対象のノードの特定が可能である。

[0087] （第 2 の実施の形態の変形例）

第 2 の実施の形態において、既存テスト情報 9 2 A にテストケース I D を記録する代わりに検証 I D を記録してもよい。テストケース I D は試験内容を特定するための識別番号であったが、検証 I D は過去の検証活動における試験の結果や検証記録を特定するための識別番号である。この場合は、過去に検証が行われたノードのうち、再検証が必要なノードを特定すること、および、新規に検証が必要なノードを特定することも可能である。検証 I D を使用する場合のノードの特定方法はテストケースを作成すべきノードの特定の方法と同様であり、参照すべき情報が異なる。すなわち、リストを作成することにより再検証が必要なノードを特定する。

[0088] なお、本発明は上記した実施例に限定されるものではなく、様々な変形例

を含む。例えば、上記した実施例は本発明を分かりやすく説明するために詳細に説明したものであり、必ずしも説明した全ての構成を備えるものに限定されるものではない。また、ある実施例の構成の一部を他の実施例の構成に置き換えることが可能であり、また、ある実施例の構成に他の実施例の構成を加えることも可能である。また、各実施例の構成の一部について、他の構成の追加・削除・置換をすることが可能である。

[0089] 上述した各実施の形態および変形例は、それぞれ組み合わせてもよい。上記では、種々の実施の形態および変形例を説明したが、本発明はこれらの内容に限定されるものではない。本発明の技術的思想の範囲内で考えられるその他の態様も本発明の範囲内に含まれる。

[0090] 次の優先権基礎出願の開示内容は引用文としてここに組み込まれる。

日本国特許出願 2019-34227（2019年2月27日出願）

符号の説明

[0091] 1…演算装置

9…記憶部

11…安全機能特定部

12…新規テストノード特定部

13…再テストノード特定部

請求の範囲

- [請求項1] 複数のノードを有し、前記複数のノードのうち少なくとも1つのノードは安全機能と関連付けられている故障木について、変更前の前記故障木の構成、変更後の前記故障木の構成、および前記安全機能ごとに過去にテストされた前記ノードを示す情報を格納する記憶部と、
- 前記故障木の変更に関する情報に基づき前記変更の影響を受ける前記安全機能を特定する安全機能特定部と、
- 前記変更後の前記故障木の構成および過去にテストされた前記ノードに基づき、前記安全機能特定部により特定された前記安全機能を再度テストするための前記ノードであって、過去にテストされた前記ノードである再テストノードを特定する再テストノード特定部と、
- 前記変更後の前記故障木の構成および過去にテストされた前記ノードに基づき、新たにテスト対象となるノードである新規テストノードを特定する新規テストノード特定部とを備える演算装置。
- [請求項2] 請求項1に記載の演算装置において、
- 前記安全機能特定部は、前記変更により追加された前記ノードから前記故障木の最上位の前記ノードまで辿った際に通過する全ての前記ノードのそれぞれに関連付けられる安全機能を、前記変更の影響を受ける安全機能として特定する演算装置。
- [請求項3] 請求項1に記載の演算装置において、
- 前記再テストノード特定部は、前記変更により追加された前記ノードのうち最上位のノードを対象ノードとし、前記対象ノードが前記変更による変更後の前記故障木における最上位の前記ノードである場合は前記再テストノードへの追加を行わない演算装置。
- [請求項4] 請求項3に記載の演算装置において、
- 前記再テストノード特定部は、前記対象ノードに接続される上位のゲートがANDゲートの場合は、当該ANDゲートに接続するそれぞれの前記ノードの事象が発生するように、当該ANDゲート以下の前

記ノードであって過去にテストされたノードを前記再テストノードに追加する演算装置。

[請求項5] 請求項1に記載の演算装置において、

前記新規テストノード特定部は、前記変更により追加された前記ノードのうち最上位のノードを対象ノードとし、前記対象ノードが下位の前記ノードを有しない場合は前記対象ノードを前記新規テストノードに追加し、前記対象ノードが下位の前記ノードを有する場合は前記対象ノードを前記新規テストノードに追加しない演算装置。

[請求項6] 請求項5に記載の演算装置において、

前記新規テストノード特定部は、

前記対象ノードが下位の前記ノードを有する場合であって、前記対象ノードに接続される下位ゲートがANDゲートの場合は、当該ANDゲートに接続される全ての前記ノードの事象が発生するように前記ANDゲート以下の前記ノードを前記新規テストノードに追加し、

前記対象ノードが下位の前記ノードを有する場合であって、前記対象ノードに接続される下位ゲートがORゲートの場合は、当該ORゲートに接続されるいずれか1つの前記ノードの事象が発生するように当該ORゲート以下の前記ノードを前記新規テストノードに追加する演算装置。

[請求項7] 複数のノードを有し、前記複数のノードのうち少なくとも1つのノードは安全機能と関連付けられている故障木について、変更前の前記故障木の構成、変更後の前記故障木の構成、および前記安全機能ごとに過去にテストされた前記ノードを示す情報を格納する記憶部を備えるコンピュータに、

前記故障木の変更に関する情報に基づき前記変更の影響を受ける前記安全機能を特定することと、

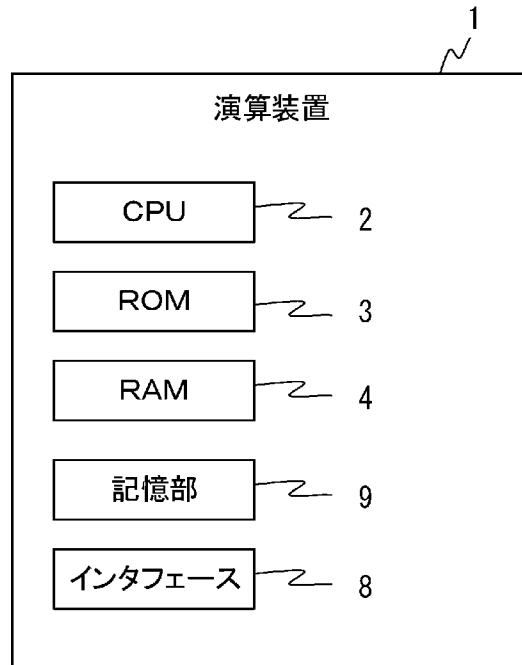
前記変更後の前記故障木の構成および過去にテストされた前記ノードに基づき、前記特定された前記安全機能を再度テストするための前

記ノードであって、過去にテストされた前記ノードである再テストノードを特定することと、

前記変更後の前記故障木の構成および過去にテストされた前記ノードに基づき、新たにテスト対象となるノードである新規テストノードを特定することとを実行させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体。

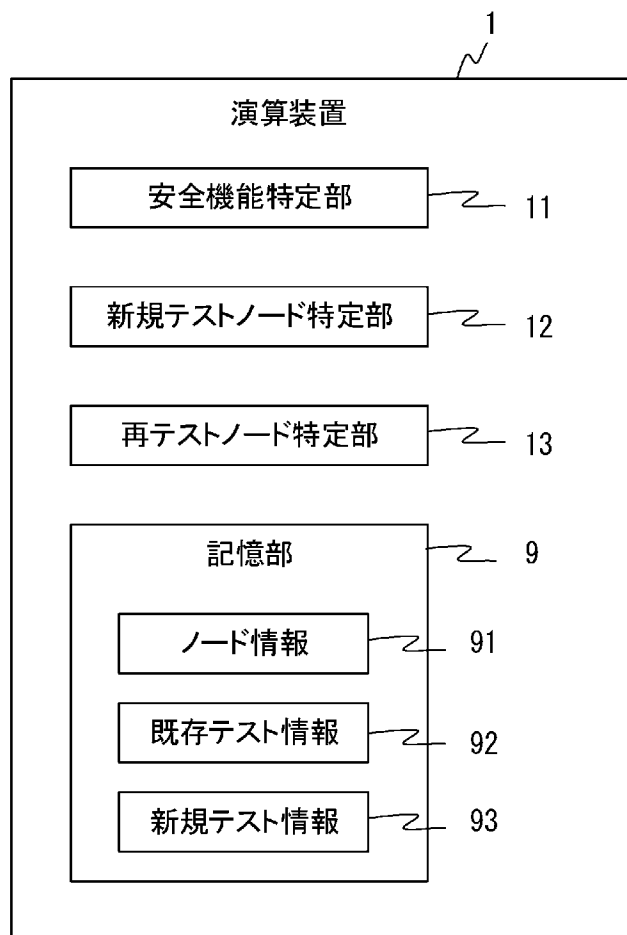
[図1]

【図1】



[図2]

【図2】



[図3]

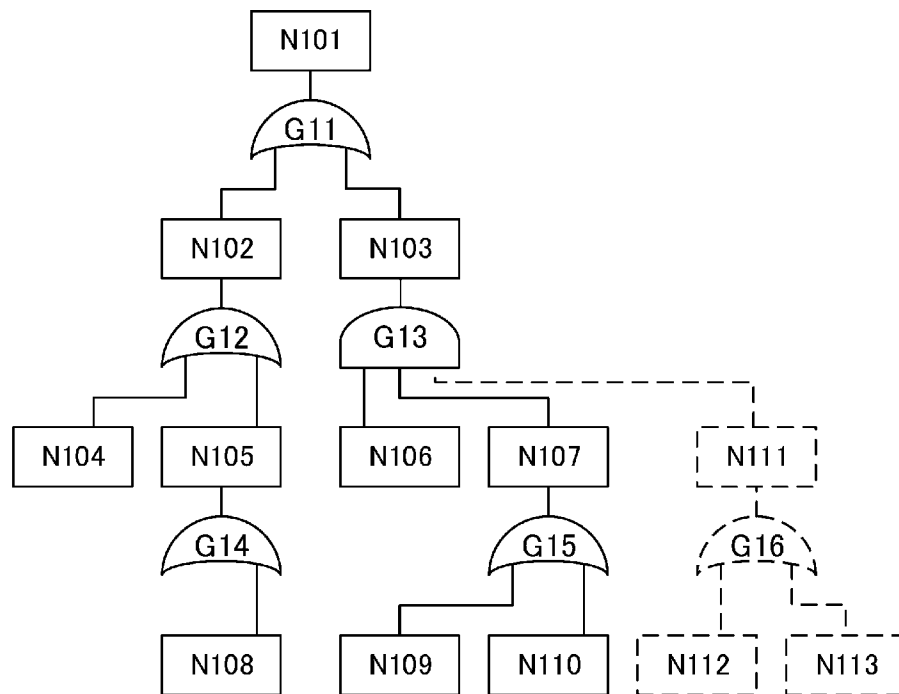
【図3】

91

ノード情報				
ノードID	上位 ゲートID	下位 ゲートID	安全機能 ID	新旧
N101	－	G11	－	既存
N102	G11	G12	SF1	既存
N103	G11	G13	SF2	既存
N104	G12	－	－	既存
N105	G12	G14	－	既存
N106	G13	－	－	既存
N107	G13	G15	－	既存
N108	G14	－	－	既存
N109	G15	－	－	既存
N110	G15	－	－	既存
N111	G13	G16	－	追加
N112	G16	－	－	追加
N113	G16	－	－	追加

[図4]

【図4】



[図5]

【図5】

92
~

既存テスト構成		
テストケースID	安全機能ID	故障挿入箇所
TC1	SF1	N104, N108
TC2	SF2	N106, N109

[図6]

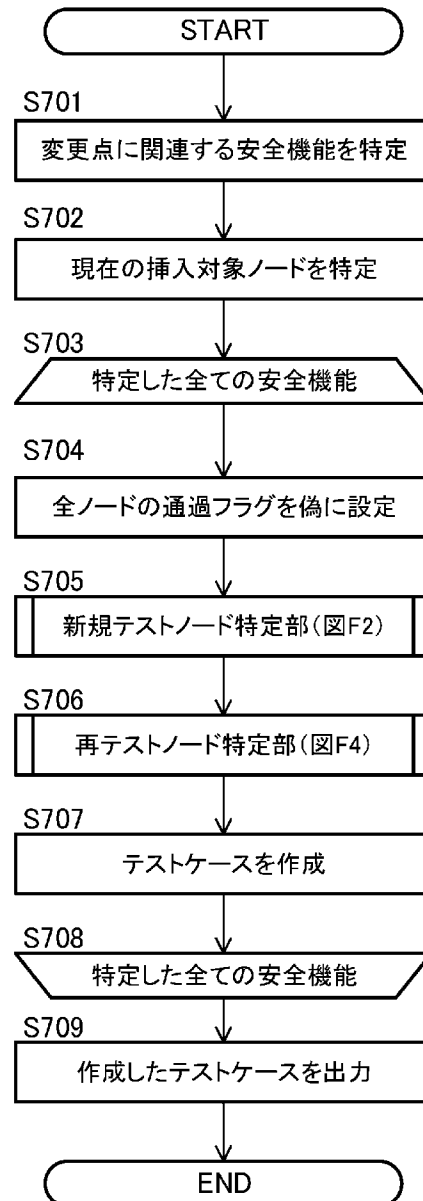
【図6】

93
~

修正後テスト構成		
テストケースID	安全機能ID	故障挿入箇所
TC1	SF1	N104, N108
TC2	SF2	N106, N109, N112

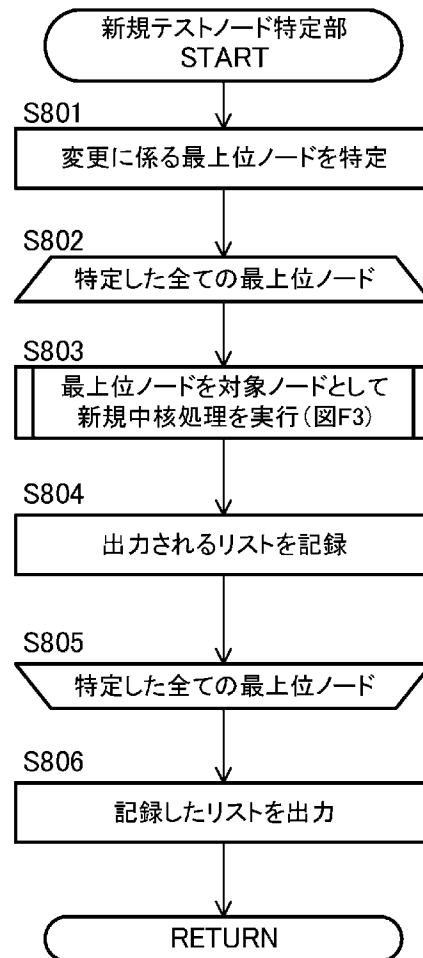
[図7]

【図7】



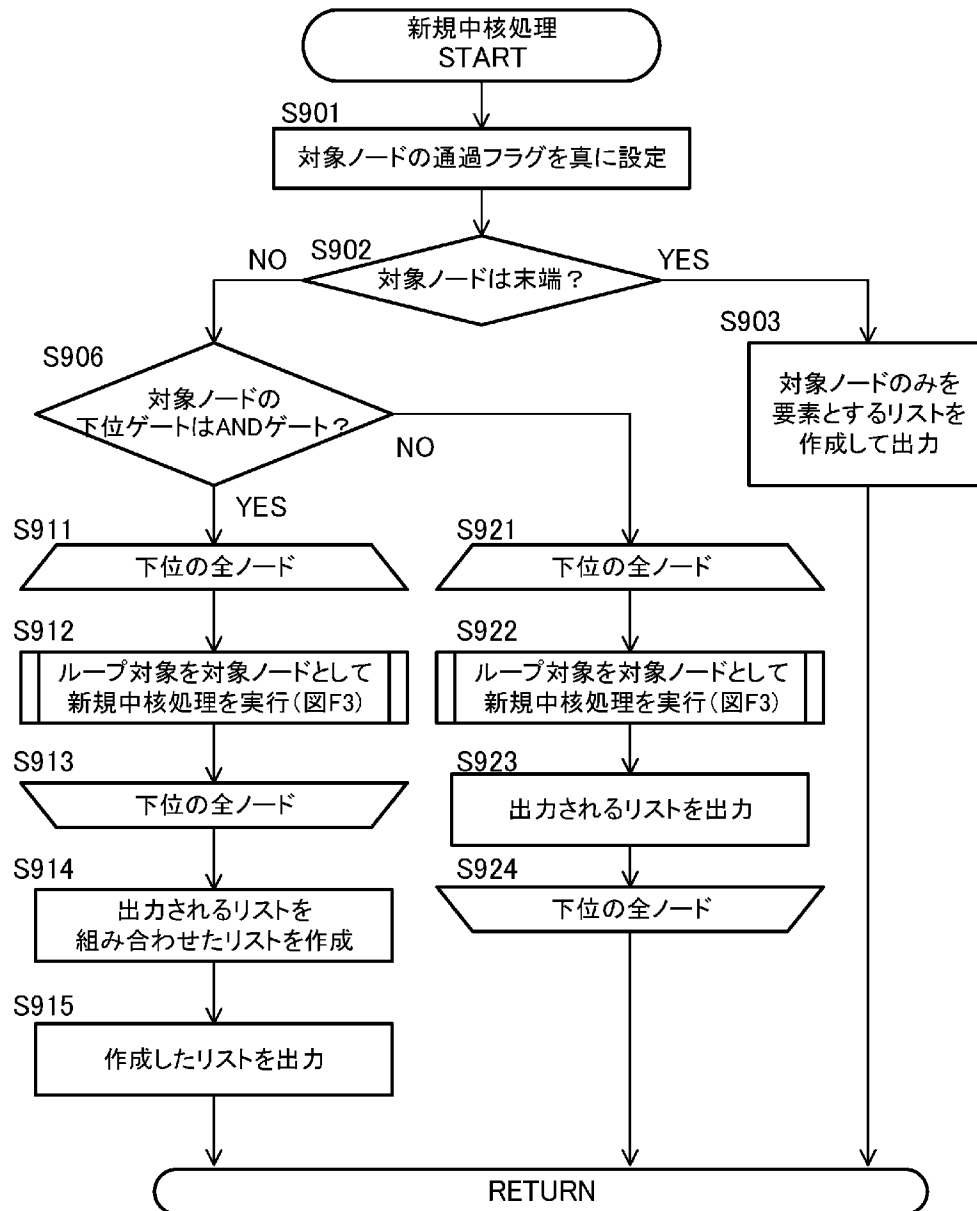
[図8]

【図8】



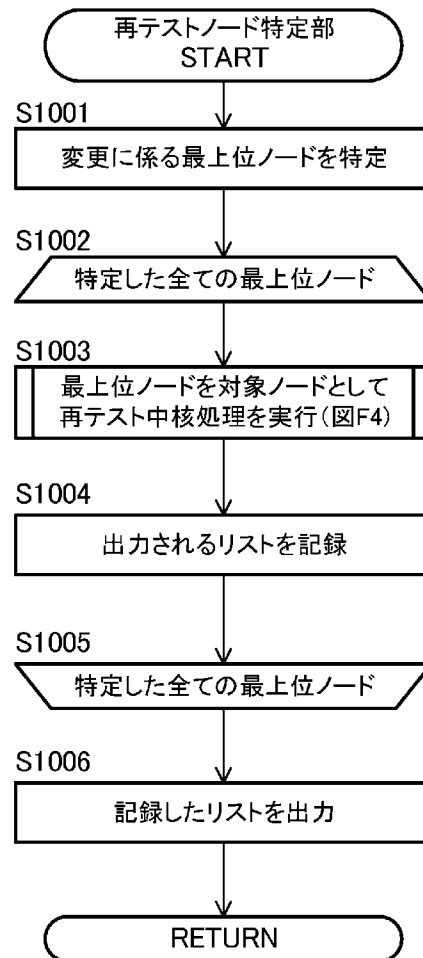
[図9]

【図9】



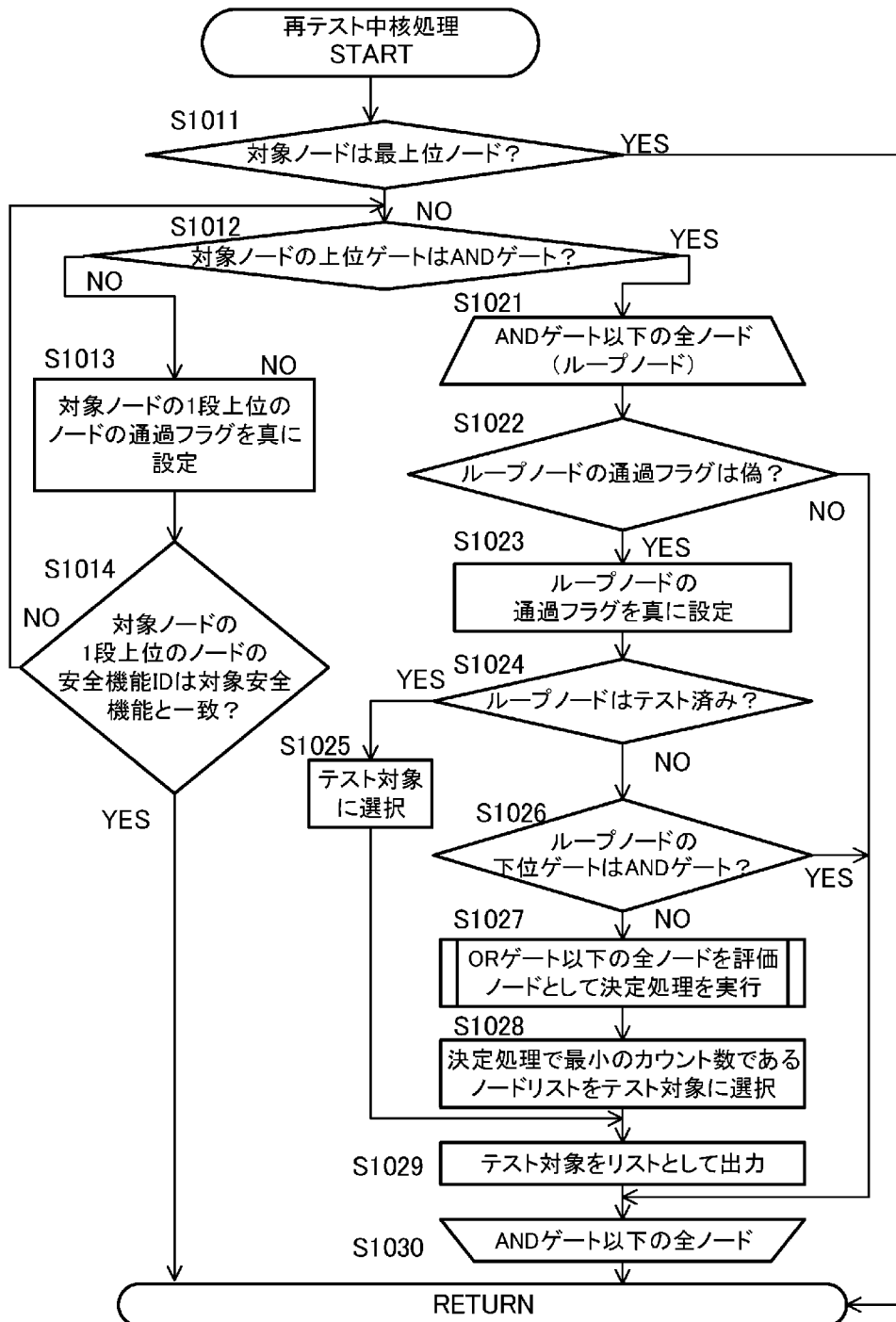
[図10]

【図10】



[図11]

【図11】



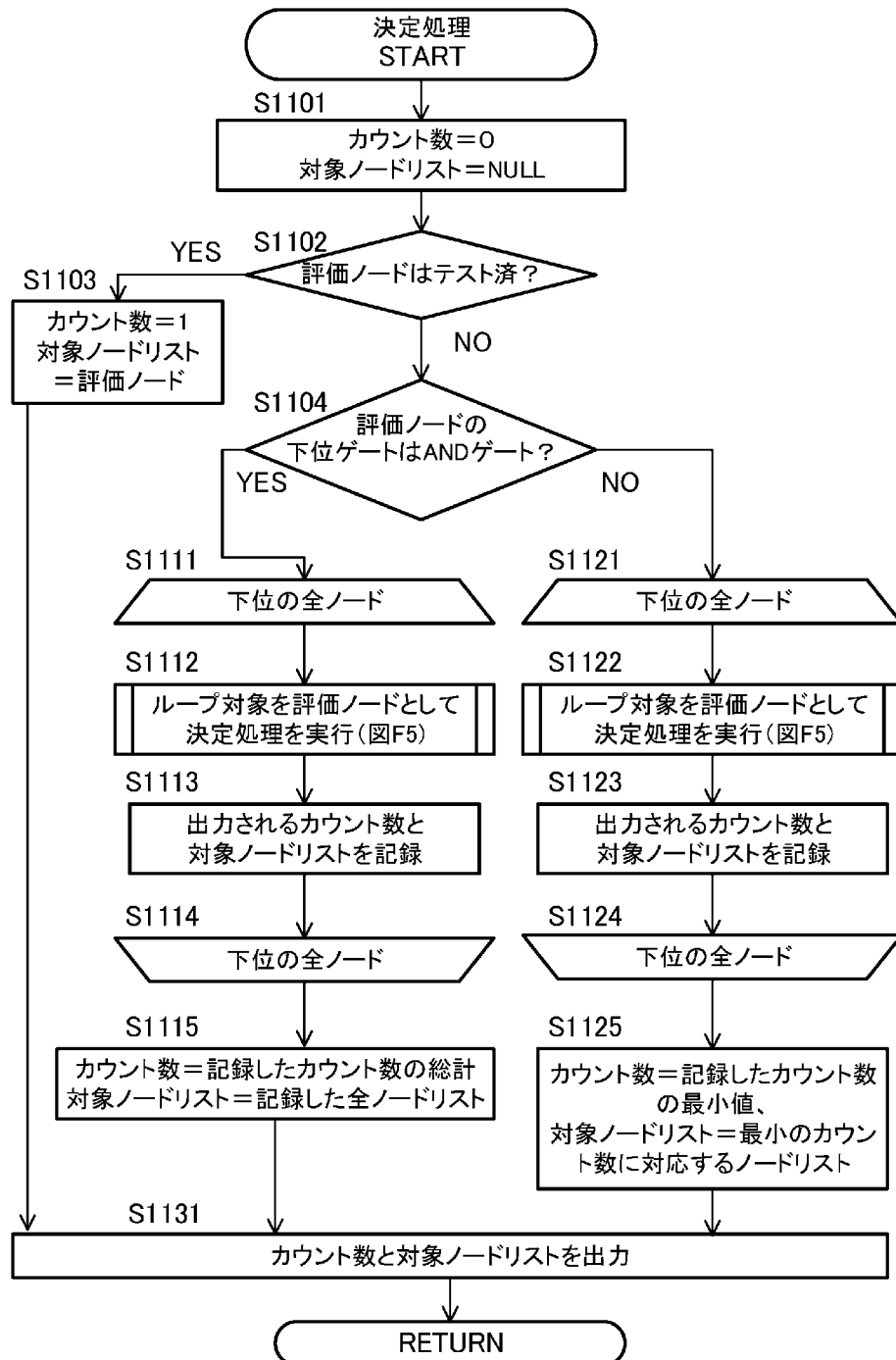
[図12]

【図12】

カウント数	対象ノードリスト
1	N201
2	N202, N203
2	N204, N205
3	N206, N207, N208

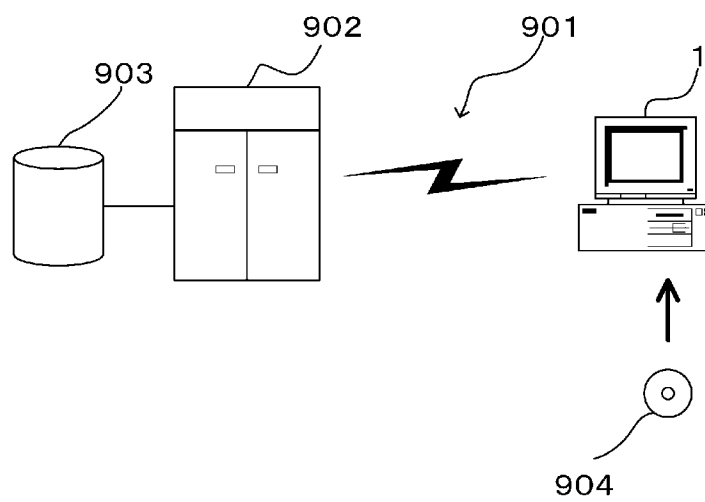
[図13]

【図13】



[図14]

【図14】



[図15]

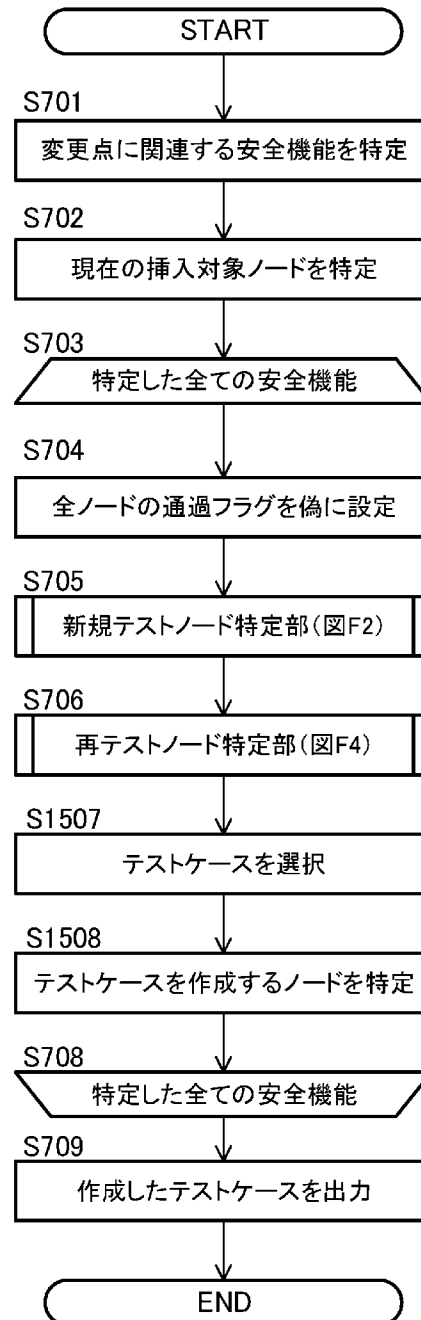
【図15】

92A

既存テスト構成			
テストケースID	テスト種別	安全機能ID	対象ノード
TC11	結合	SF1	N301, N302
TC12	故障挿入	SF2	N301, N303, N309

[図16]

【図16】



INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2020/004324

A. CLASSIFICATION OF SUBJECT MATTER

G05B 23/02 (2006.01) i

FI: G05B23/02 T; G05B23/02 301Y; G05B23/02 302Y

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

G05B23/02

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Published examined utility model applications of Japan	1922-1996
Published unexamined utility model applications of Japan	1971-2020
Registered utility model specifications of Japan	1996-2020
Published registered utility model applications of Japan	1994-2020

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP 6-222922 A (SANKYO SEIKI MFG CO., LTD.) 12.08.1994 (1994-08-12) paragraphs [0019], [0035]	1-7
A	JP 2003-228485 A (KAWASAKI HEAVY INDUSTRIES, LTD.) 15.08.2003 (2003-08-15) paragraph [0014]	1-7

☐ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* Special categories of cited documents:

“A” document defining the general state of the art which is not considered to be of particular relevance

“E” earlier application or patent but published on or after the international filing date

“L” document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

“O” document referring to an oral disclosure, use, exhibition or other means

“P” document published prior to the international filing date but later than the priority date claimed

“T” later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

“X” document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

“Y” document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

“&” document member of the same patent family

Date of the actual completion of the international search
24 March 2020 (24.03.2020)

Date of mailing of the international search report
31 March 2020 (31.03.2020)

Name and mailing address of the ISA/
Japan Patent Office
3-4-3, Kasumigaseki, Chiyoda-ku,
Tokyo 100-8915, Japan

Authorized officer

Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.

PCT/JP2020/004324

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
JP 6-222922 A	12 Aug. 1994	(Family: none)	
JP 2003-228485 A	15 Aug. 2003	(Family: none)	

A. 発明の属する分野の分類（国際特許分類（IPC）） G05B 23/02(2006.01)i FI: G05B23/02 T; G05B23/02 301Y; G05B23/02 302Y														
B. 調査を行った分野														
調査を行った最小限資料（国際特許分類（IPC）） G05B23/02														
最小限資料以外の資料で調査を行った分野に含まれるもの <table border="0"> <tr> <td>日本国実用新案公報</td> <td>1922 - 1996年</td> </tr> <tr> <td>日本国公開実用新案公報</td> <td>1971 - 2020年</td> </tr> <tr> <td>日本国実用新案登録公報</td> <td>1996 - 2020年</td> </tr> <tr> <td>日本国登録実用新案公報</td> <td>1994 - 2020年</td> </tr> </table>			日本国実用新案公報	1922 - 1996年	日本国公開実用新案公報	1971 - 2020年	日本国実用新案登録公報	1996 - 2020年	日本国登録実用新案公報	1994 - 2020年				
日本国実用新案公報	1922 - 1996年													
日本国公開実用新案公報	1971 - 2020年													
日本国実用新案登録公報	1996 - 2020年													
日本国登録実用新案公報	1994 - 2020年													
国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）														
C. 関連すると認められる文献														
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求項の番号												
A	JP 6-222922 A（株式会社三協精機製作所）12.08.1994（1994 - 08 - 12） [0019], [0035]	1-7												
A	JP 2003-228485 A（川崎重工業株式会社）15.08.2003（2003 - 08 - 15） [0014]	1-7												
☐ C欄の続きにも文献が列挙されている。 ☒ パテントファミリーに関する別紙を参照。														
<table border="0"> <tr> <td>* 引用文献のカテゴリー</td> <td>“T” 国際出願日又は優先日後に公表された文献であって出願と抵触するものではなく、発明の原理又は理論の理解のために引用するもの</td> </tr> <tr> <td>“A” 特に関連のある文献ではなく、一般的技術水準を示すもの</td> <td>“X” 特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの</td> </tr> <tr> <td>“E” 国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの</td> <td>“Y” 特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの</td> </tr> <tr> <td>“L” 優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）</td> <td>“&” 同一パテントファミリー文献</td> </tr> <tr> <td>“O” 口頭による開示、使用、展示等に言及する文献</td> <td></td> </tr> <tr> <td>“P” 国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献</td> <td></td> </tr> </table>			* 引用文献のカテゴリー	“T” 国際出願日又は優先日後に公表された文献であって出願と抵触するものではなく、発明の原理又は理論の理解のために引用するもの	“A” 特に関連のある文献ではなく、一般的技術水準を示すもの	“X” 特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの	“E” 国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの	“Y” 特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの	“L” 優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）	“&” 同一パテントファミリー文献	“O” 口頭による開示、使用、展示等に言及する文献		“P” 国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献	
* 引用文献のカテゴリー	“T” 国際出願日又は優先日後に公表された文献であって出願と抵触するものではなく、発明の原理又は理論の理解のために引用するもの													
“A” 特に関連のある文献ではなく、一般的技術水準を示すもの	“X” 特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの													
“E” 国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの	“Y” 特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの													
“L” 優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）	“&” 同一パテントファミリー文献													
“O” 口頭による開示、使用、展示等に言及する文献														
“P” 国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献														
国際調査を完了した日 24.03.2020	国際調査報告の発送日 31.03.2020													
名称及びあて先 日本国特許庁(ISA/JP) 〒100-8915 日本国 東京都千代田区霞が関三丁目4番3号	権限のある職員（特許庁審査官） 牧 初 3U 9064 電話番号 03-3581-1101 内線 3364													

国際調査報告
パテントファミリーに関する情報

国際出願番号

PCT/JP2020/004324

引用文献			公表日	パテントファミリー文献	公表日
JP	6-222922	A	12.08.1994	(ファミリーなし)	
JP	2003-228485	A	15.08.2003	(ファミリーなし)	