

(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
2016 年 2 月 4 日(04.02.2016)



(10) 国際公開番号

WO 2016/017560 A1

- (51) 国際特許分類:
G06F 11/36 (2006.01) G06F 11/28 (2006.01)
- (21) 国際出願番号: PCT/JP2015/071185
- (22) 国際出願日: 2015 年 7 月 27 日(27.07.2015)
- (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 2014-153420 2014 年 7 月 29 日(29.07.2014) 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: 成沢 文雄(NARISAWA Fumio); 〒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). 松原 正裕(MATSUBARA Masahiro); 〒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). 西 昌能(NISHI Masataka); 〒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). 蛭名 朋仁(EBINA Tomohito); 〒3128503 茨城県ひたちなか市高場 2 5 2 0 番地 日立オートモティブシステムズ株式会社内 Ibaraki (JP).

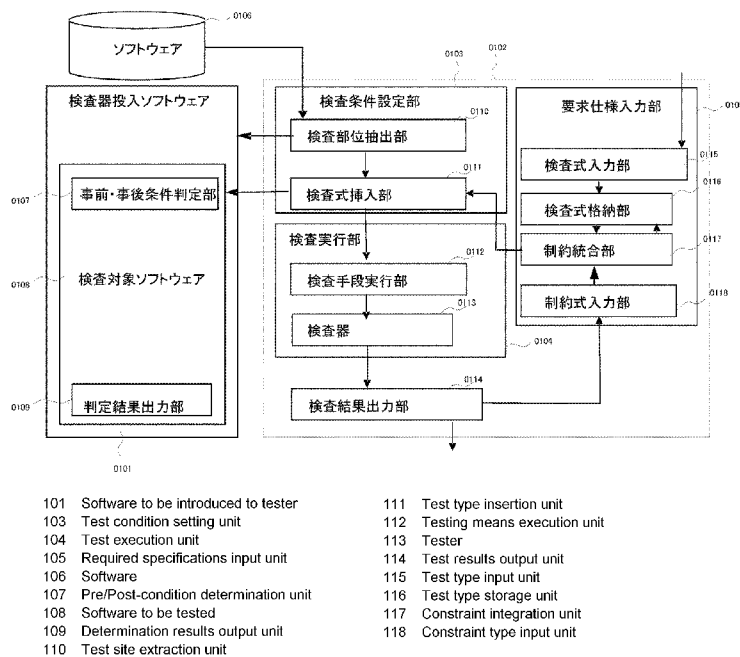
- (74) 代理人: 井上 学, 外(INOUE Manabu et al.); 〒1008220 東京都千代田区丸の内一丁目 6 番 1 号 株式会社日立製作所内 Tokyo (JP).
- (81) 指定国 (表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, KE, KG, KN, KP, KR, 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, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, 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), ユーロパ (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))

(54) Title: SOFTWARE VALIDATION SYSTEM AND CONTROLLER

(54) 発明の名称: ソフトウェア検証システムおよび制御装置



(57) Abstract: The purpose of the present invention is to divide large-scale software into small portions and perform validation on each portion, and to combine the results over an entire system. The scope of validation is restricted by proceeding with validation while integrating the validation results of each portion, enabling thorough validation of large-scale software. In order to achieve this purpose, the present invention comprises: a test type input unit for inputting required specifications, which serve as test conditions for software to be tested, as a first test type; a test execution unit for extracting, via a test point extraction unit, the software to be validated for each of a plurality of test unit points, inserting the test type for test objects via a test type insertion unit, and performing thorough testing of the software to be tested; a test results output unit for outputting test results; an input unit for inputting the test results as a second constraint expression; and an integration unit for integrating a first constraint expression and the second constraint expression.

(57) 要約:

[続葉有]

WO 2016/017560 A1



本発明の目的は、大きなソフトウェアを小さな部分に分けて部分毎に検証し、その結果をシステム全体で組み合わせることを目的とし、部分毎の検証結果を統合しながら検証を進めることで検証範囲を限定し、規模の大きなソフトウェアへの網羅的検証を可能とすることである。前記目的を実現するために、検査対象ソフトウェアの検査条件である要求仕様を第一の検査式として入力する検査式入力部と、検査部位抽出部により検証対象ソフトウェアを検査単位の部位毎に抽出し、検査式挿入部により検査対象に対し検査式を挿入し、前記検査対象ソフトウェアの網羅的検査を行う検査実行部と検査結果を出力する検査結果出力部と、検査結果を第二の制約式として入力する入力部と第一の制約式と第二の制約式を統合する統合部を備えることを特徴とする。

明 細 書

発明の名称： ソフトウェア検証システムおよび制御装置

技術分野

[0001] 本発明は、ソフトウェアを検証する検証システムおよびそのソフトウェアを搭載した制御装置に関する。

背景技術

[0002] 自動車エンジン制御などの制御装置として、中央演算装置、ROM、RAM、入出力信号処理装置などを内蔵したマイクロコントローラ(以下マイコンと表記)が用いられている。マイコンが実行するソフトウェアは制御対象が目的とする制御動作を行うように、一般的には制御処理を行うアプリケーションプログラムと入出力を行うデバイスドライバやオペレーティングシステム(OS)などによって構成されている(例えば、特許文献1参照)。

[0003] このような制御装置は、車両の制御を行うことで車両乗員の安全性に直接係る制御を行うことから、高い安全性を要求されている(例えば、特許文献2参照)。また、近年制御の高度化と規模の増大に伴い、安全に関わるシステムが第三者から見ても必要とされる高い安全性を満足する開発を行うためには、開発工程のうち検証工程において網羅率のより高い検証を求められており、安全に関わらないシステムと比べて、大きな開発工数を要することが課題となっている。

[0004] 網羅的な検証を可能とする技術として、形式検証技術と呼ばれる技術が近年注目されている。形式検証技術は網羅的な検証が可能となる。

先行技術文献

特許文献

[0005] 特許文献1：特許第3460593号公報

特許文献2：特開2002-14839号公報

非特許文献

[0006] 非特許文献1：Edmund Clarke著 ANSI-C Bounded Model Checker User Manual

2006

非特許文献2 : frama-c Value Analysis <http://frama-c.com/download/frama-c-value-analysis.pdf>

非特許文献3 : Pascal Cuoq他著, Frama-C: A Software Analysis Perspective, in LNCS7504 Software Engineering and Formal Methods, p233

非特許文献4 : Jeffrey E.F. Friedl著, 詳説 正規表現, オライリージャパン
発明の概要

発明が解決しようとする課題

- [0007] 形式検証技術によれば網羅的な検証が可能となるものの、検証対象ソフトウェア規模が増大すると、検証に要する計算時間やメモリ、やディスクなどの計算資源が指数関数的に増大するため検証がし切れなくなるという、状態爆発と呼ばれる問題がある。このため、現実には用いられるソフトウェア全体を一度に検証することは現実的には実現できない。
- [0008] 大規模で形式検証適用が困難なソフトウェアを検証するためには、ソフトウェアを小さな検証単位に分割することと、探索範囲となる検証すべき条件を可能な限り限定することが有効である。
- [0009] このため本発明の目的は、大きなソフトウェアを小さな部分に分けて部分毎に検証し、その結果をシステム全体で組み合わせ、部分毎の検証結果を統合しながら検証を進めることにある。
- [0010] また、本発明の他の目的は、検証対象ソフトウェアに存在する条件だけでなく、設計情報としての条件を検証条件に与えることで検証範囲を限定し規模の大きなソフトウェアへの網羅的検証を可能とすることにある。

課題を解決するための手段

- [0011] 前記目的を実現するために、本発明のソフトウェア検証システムは、入出力に依存関係のある複数の機能を備えた制御プログラムのソースコードを入力し、前記制御プログラムを検証する検査実行部と、前記ソースコードを前記複数の機能単位で複数の検査部位に分割し抽出する検査部位抽出部と、前記複数の検査部位のうち一の検査部位に関する検査結果出力に基づき、連続

する次の検査部位の検査範囲を規定する第1の制約式を作成する第1の制約式作成部と、を備え、前記第1の制約式に基づいて前記複数の検査部位を順に検査することを特徴とする。

発明の効果

[0012] 上記構成にてソフトウェア検証装置を作成すると、大規模なソフトウェアを小さな単位で分割しながら、ひとつの検証部位の検証結果と設計者が与えた検証条件を次の検証部位に適用していくことにより、状態爆発を抑制しながら大規模なソフトウェアの検証が可能となる。

図面の簡単な説明

[0013] [図1]システムの構成を示した図である。
[図2]装置の構成を示した図である。
[図3]制御装置の構成を示した図である。
[図4]検査式挿入の実行手順を示した図である。
[図5]検査器投入ソフトウェアを示した図である。
[図6]制約式統合の実行手順を示した図である。
[図7]検査式情報を示した図である。
[図8]検査手段実行部、検査器、および検査結果を示した図である。
[図9]検査式出力パターンを示した図である。

発明を実施するための形態

[0014] 以下、図面を参照しながら本発明の実施形態について説明する。

実施例 1

[0015] (ハードウェア構成)

図1は本発明の実施形態のソフトウェア検証システムの構成を示す構成図である。検査装置（検査ツール）0102はソフトウェア0106を全体を検査することを目的としている。ここでいう検査とは、ソフトウェア0106のソースコードに挿入された検査式で定義される検証範囲内において、ソースコードが取り得る状態を網羅的に探索し、所望の状態になることを検証することをいう

。

[0016] ソフトウェア0106は、例えば図3で後述するような、自動車を制御するコントロールユニットに搭載される制御ソフトウェアである。検査条件設定部0103では、まず検査部位抽出部0110により0106から検査対象ソフトウェア0108を一定の検査単位でソフトウェア部品として抽出し、次に検査式挿入部0111により検査式を挿入する。

[0017] 前記検査式は0108中で所定の処理を行う処理部の実行前または実行後に、事前事後条件判定部0107と、判定結果を出力する判定結果出力部0109として挿入する。上述した自動車を制御する制御ソフトウェアの例では、処理部（所定の入力値に対して出力値を演算する処理等）の実行前に、センサ値などの入力値の取り得る値（検証範囲）が事前条件として挿入される。また、事前条件で指定された入力値に対する処理部の出力値の取り得る値（設計値等）が事後条件として挿入される。

[0018] 次に検査実行部0104は検査手段実行部0112により、前記検査式を挿入した前記ソフトウェア部品を検査器投入ソフトウェア0101として検査器0113を用いて網羅的に検証する。

[0019] 検査結果出力部0114は検査器0113から得た検査結果をユーザ或いは出力装置に出力するとともに、要求仕様入力部0105に出力する。

[0020] 要求仕様入力部0105は前記検査結果を制約式入力部0118を用いて第一の制約式として入力する。また検査式入力部0105はユーザから入力した検査式を前記検査式保持部0116に第2の制約式として保持する。制約統合部0117は前記第1の制約式と前記第2の制約式を統合し検査式挿入部に出力する。

[0021] なお、前記検査単位とはソフトウェアを構成する構成要素を示しており、C言語のひとつの関数が前記単位の一例であるが、その他の粒度に設定することも可能であり、この例に特定されるものではない。

[0022] 図2は本発明を実現するためのシステム構成図である。計算機の演算装置などからなる処理装置301と、ディスク装置やメモリ装置からなる記憶装置302と、モニタ、キーボード、ネットワーク、プリンタなどからなる入出力装置3

03から構成される。処理装置301には、前記検査部位抽出部305、検査式挿入部306、検査手段起動部307、検査結果出力部308、検査式入力部309、制約統合部310、検査式入力部311が配置される。記憶装置には前記、ソフトウェア0106を格納するプログラムコード312、前記検査式保持部313、検査結果格納部314、検査対象ソフトウェア315が配置される。

[0023] 図3は本発明の対象とする制御システムのひとつである自動車エンジン制御システムの構成を示すものである。

[0024] コントロールユニット301はマイクロコントローラ 302 (CPU)、信号入力回路309、アクチュエータ駆動回路 312、通信回路 311 から構成され、センサ1 311、 センサ2 316から信号入力回路309を介して得た外界の情報に基づき、駆動回路310を介してアクチュエータ314を駆動することで制御を行う。また、一部の信号については通信回路311を介して通信線217から得た他の制御装置316からの入出力を用いて制御処理を行う。

[0025] 前記マイクロコントローラ302は、入力回路 303、演算装置 304、揮発性読み書きメモリ305(RAM)、読み出し専用メモリ306(ROM)、割込み制御装置 307、メモリ保護装置 308、出力回路 309、通信制御装置 310、から構成される。

[0026] ソフトウェア0106は読み出し専用メモリ306に格納され、マイクロコントローラ302によって実行され、所定の制御処理を行う。

[0027] (ソフトウェアの処理詳細)

図4aに示すのが、検査部位抽出部の動作である。検査部位抽出部はプログラムコード格納部312からソフトウェア0106のプログラムコードの特定部位を抽出し部分的なプログラム構成要素を出力する部分である。まず抽出を開始する点である抽出始点を検索401し、次に抽出の終点を検索402する。始点から終点到相当するプログラムコードを検査部位として切り出し403、検査式生成部を呼出し404、検査部位として抽出したプログラムコード中に検査式を挿入する。全ての対象モジュールを抽出し終えたか否かを判定405し、全ての対象の抽出を終了していれば動作を終了405する。

[0028] 図4bに示すのが検査式生成部の動作である。検査式生成部は、プログラムコードあるいはプログラムコードの一分を入力し、検査式を挿入したプログラムコードを出力する部分である。検査式格納部313から条件式パターンをそれぞれ入力し、検査式情報を作成し制約統合部310へ格納することが目的である。処理が開始406されると、検査式格納部313から検査式を読み込み407、プログラムコード格納部312からプログラムコードを一行ずつ入力する407。読み込んだ部位が検査式を挿入すべき位置か判定する409。挿入部位に該当する場合には、検査式を抽出し410、検査式を生成する411。対象モジュールの読み込みが終端に達しているか判定し412、終端に達していれば終了413し、対象モジュール全体への検査式挿入判定と挿入が完了するまで繰り返す。

[0029] 図5に示すのが検査器が検査する対象とする検査器投入ソフトウェア0101の例である。検査対象となる検査対象ソフトウェア0108の例が、図5(a)の関数501とその処理内容503、ならびに図5(b)関数505とその処理内容507である。502が事前・事後条件判定部0107の例であり、507によると、符号なし2バイト長の変数"ETH" はソースコードの情報のみからは、0以上65535以下の値を取り得る、と判断できるが、さらに設計上の情報を与えたことにより、0以上50以下の値のみを取り得る、という前提条件を課することができる。

[0030] このように変数の取り得る値を限定することにより、検証時の探索範囲を削減することができ、前述の状態爆発を避けることが可能となる。同様に変数 "WTP" は0以上150以下の範囲であることを示している。504は関数501の処理内容503を実行後に満たすべき条件を記述した事前・事後条件判定部0107の例である。実行後に変数SINJWが0以上150以下の範囲であることを検査条件として示している。

[0031] 506は関数505に対する事前・事後条件判定部0107の例であり、502に加えて変数"SINJW"が0以上150以下であるという条件が追加されている。これは、504で検証した関数501の事後条件を関数505の事前条件として追加したものであり、関数501と関数505が、その呼出し元関数509から前後順に呼び出されている情報を用いることにより、関数501の次に続く関数505の条件を、関数501の

検証結果と事前の設計情報である事前条件502を統合した条件として、制約統合部0117により統合された場合の例である。連続する検査対象の検査結果と設計情報として与えた条件を統合することにより、検査範囲をより限定できる。508は事前・事後条件判定部0107および判定結果出力部0109の例であり、検査を行い違反が見付かった場合にはその情報を出力する。この判定および結果出力は検証時に処理装置301上で実行し入出力装置303から結果を出力する実施形態と、制御装置301上のROM306に搭載するソフトウェアとして実装し、301上で実施し結果を通信線316を介し診断端末314あるいは制御装置315に出力する実施形態がある。自動車等の制御ソフトウェアでは、ある関数の出力結果を用いて続く関数が演算処理を行い、複数の関数が連続して処理を行って機器を制御する場合が多い。本発明では、このように入出力値に依存関係のある連続した関数において、前の関数の検証結果を続く関数の制約式として用いることにより、個々の関数の検証範囲を抑えつつも制御ソフトウェア全体を網羅的に検証することが出来る。

[0032] 図6は制約統合部0117の処理手順である。検査対象ソフトウェアの検査式挿入位置に関する情報を入力する601。挿入位置に関する情報とは、ソフトウェアのソースコードを含むファイル名や行番号、関数などのモジュール名、その実行前、実行後などの具体的な位置を示す情報である。次に検査式格納部0116から第1の検査式を入力する602。次に制約式入力部0118から第2の検査式を入力する603。第2の検査式は、要求仕様入力部0105に入力された制御仕様等に基づいて設定されている。制御仕様としては、例えば自動車の制御ソフトウェアの場合、車両の取り得る状態遷移、車両の外界情報設定値、所定の車載機器が所定の条件で取るべき仕様等である。次に602、603によって入力した各々の検査式について検査式の種別を判定し604、この種別に基づき検査式同士の結合条件を決定する605。最後に605で決定した結合条件を表す条件結合子を用いて検査式を連結し、統合した制約式として出力する606。

[0033] 図7は、検査式格納部0116に格納される検査式情報の例である。0705から0708まで4つの検査式情報の例を示している。各検査式情報は、起動条件0701、

条件種別0702、結合子0703、0704条件の項目を含む。起動条件0701は、どのような条件で検査を行うかを定めたものであり、0705の例では指定した関数“INJWCALC”の実行前であることを指定した例である。この他に常に検査する“always” 0706、0707指定したファイル“module1.c”の指定した行番号“110”のようなファイル位置の指定 0701 を行う。条件種別0702は、その検査式が常に成り立つ“hold” 0705、0706、0707、あるいはその条件が成立してはならないという安全条件“do not hold” 0708、を指定する。結合子0703は、複数の検査式を連結する際には何らかの論理演算子で結合する必要があるが、それらの条件には、常に成立すべき仕様や、その条件に陥ってはならない安全仕様などがあり、これらを統合し接続するためには個別に異なるため、これを指定するためのものである。条件0704は、各検査式情報が示す具体的な条件である。

[0034] 図8は検査器0113から出力された検査結果の出力例である。図8(a)801は検査器0113として、非特許文献1に記載のCBMCを利用した場合の検証器の起動および検証結果の例である。801は検証器を起動するコマンドである。803は検証器の出力であり、検証すべき項目が全て正しい結果であったことが得られたことを示している。

[0035] 図8(a)804は検証器に検証した項目を明示的に表示させた出力結果である。0805はその検証項目の一例であり、そのうちの0805は変数“SINJW”と変数“rinjw”の加算結果の値が0以上65535以下であることが証明されたことが出力されている。

[0036] 図8(b)は、0808の検査器投入ソフトウェア0101の例を、非特許文献2、非特許文献3に示す検証器である“frama-c”で検証した際の出力例である。

[0037] 検証の結果変数“INJW”の取り得る値が0~10であることが示された様子を示している。

[0038] これらの検査器の出力は検査結果出力部0114により検証支援装置の画面やプリンタなどの入出力装置303から表示させる。また、この出力はつぎの検査単位の検査条件として制約式入力部0118から入力し、制約統合部0117として

統合することで、より限定された検査範囲での検査を可能とし、検証時間の短縮や、同一検証環境の計算機資源においてより多くのソフトウェアの検証を可能とすることができる。

[0039] また、検査器の出力に代えて、コントロールユニット301によって、ソフトウェア0106を実行した時に、ソフトウェア0106に記述された検査式の検査結果をRAM305に保持するようにしてもよい。これにより、車両の運転中に実行された処理結果を機能単位で保持または出力出来て、エラーが生じた際の原因特定に役立てることが出来る。

[0040] 図9は検査式挿入部011の処理フロー図4のステップ411、検査式生成の工程で使用する出力文字列を具体的に記載した例である。挿入する文字列は検査器0113の仕様に依存するため、適切な検査式となる文字列への変換が必要である。図9 901は前記CBMCに適した検査式文字列の生成パターンを示しており、正規表現を用いた記載例である。固定部前半902と可変部903、固定部後半904を指定し、条件を可変部903に埋め込むことにより実際に選択した検査器0113に対応した検査式記述を出力できる。このような正規表現を用いた固定文字列と可変文字列の組み合わせは非特許文献4に示されている。

[0041] (実施例による効果)

これにより、検証時の検証対象ソフトウェアを入出力値に依存関係のある複数の機能単位で分割し、探索範囲である検証条件を限定することが可能となり、より大規模なソフトウェアに対し、網羅的検証が可能となる。

符号の説明

[0042] 0102・・・検査装置、0103・・・検査条件設定部、0104・・・検査実行部、0105・・・要求仕様入力部、0106・・・ソフトウェア、0108・・・検査対象ソフトウェア

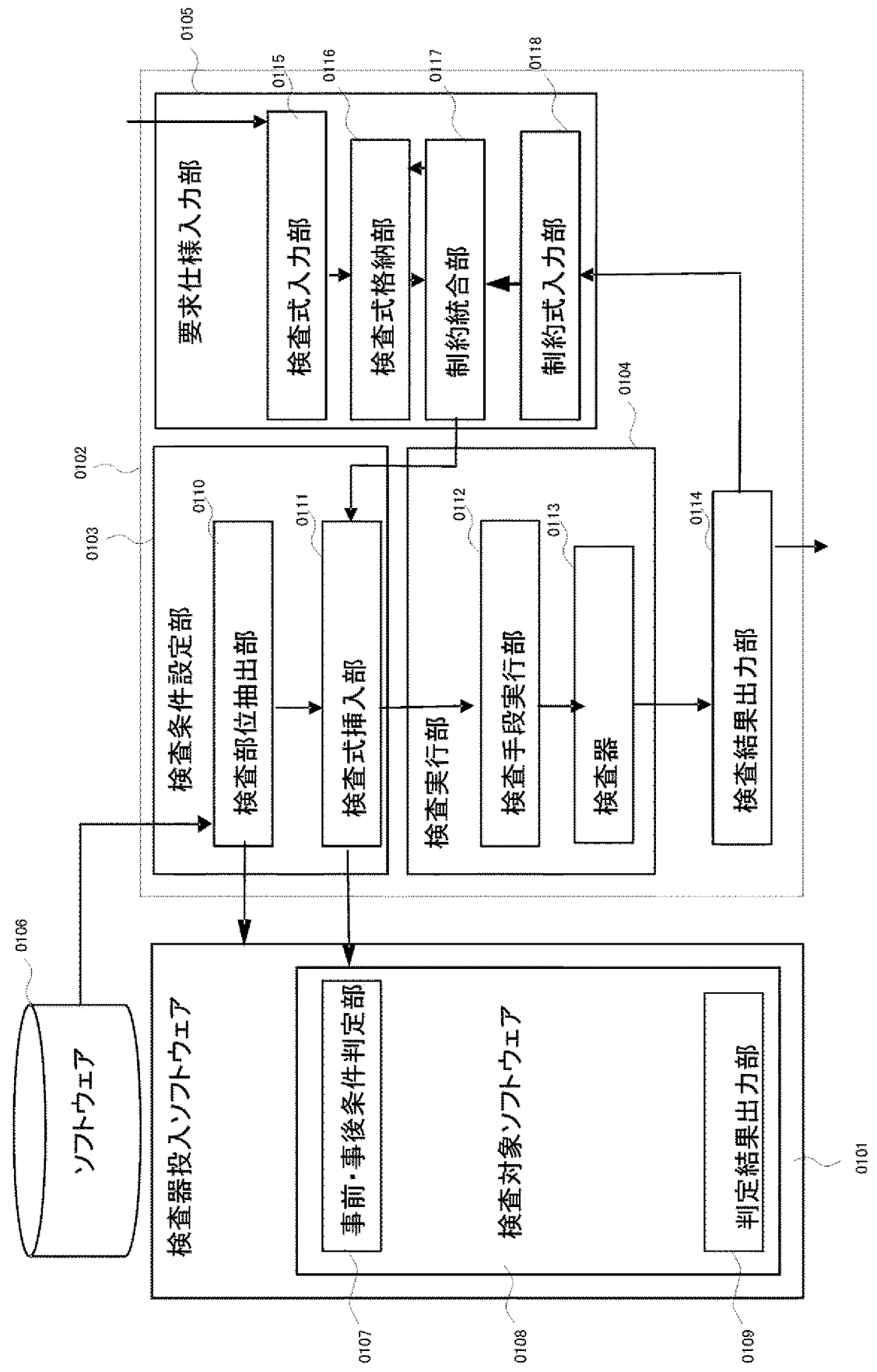
請求の範囲

- [請求項1] 入出力に依存関係のある複数の機能を備えた制御プログラムのソースコードを入力し、前記制御プログラムを検証する検査実行部と、
前記ソースコードを前記複数の機能単位で複数の検査部位に分割し抽出する検査部位抽出部と、
前記複数の検査部位のうちの検査部位に関する検査結果出力に基づき、連続する次の検査部位の検査範囲を規定する第1の制約式を作成する第1の制約式作成部と、を備え、
前記第1の制約式に基づいて前記複数の検査部位を順に検査することを特徴とするソフトウェア検証システム
- [請求項2] 請求項1に記載のソフトウェア検証システムにおいて、
制御対象機器の取り得る状態遷移、制御対象機器の外界情報設定値、制御仕様の少なくとも1つに基づいて、検査部位の検査範囲を規定する第2の制約式を作成する第2の制約式作成部を備え、
第1の制約式と第2の制約式とに基づいて前記複数の検査部位を順に検査することを特徴とするソフトウェア検証システム。
- [請求項3] 請求項2に記載のソフトウェア検証システムであって、
前記検査部位抽出手段はC言語で記述されたソフトウェアのソースコードを対象とし、関数を単位として抽出することを特徴とするソフトウェア検証システム。
- [請求項4] 請求項2に記載のソフトウェア検証システムであって、
検査対象処理記述と事前条件と事後条件のうち少なくともひとつを入力として、前記複数の検査部位を順に検査することを特徴とするソフトウェア検証システム
- [請求項5] 請求項2に記載のソフトウェア検証システムであって、
前記第1の制約式と前記第2の制約式を統合する制約式統合部を備えることを特徴とするソフトウェア検証システム。
- [請求項6] センサおよびアクチュエータに接続され、

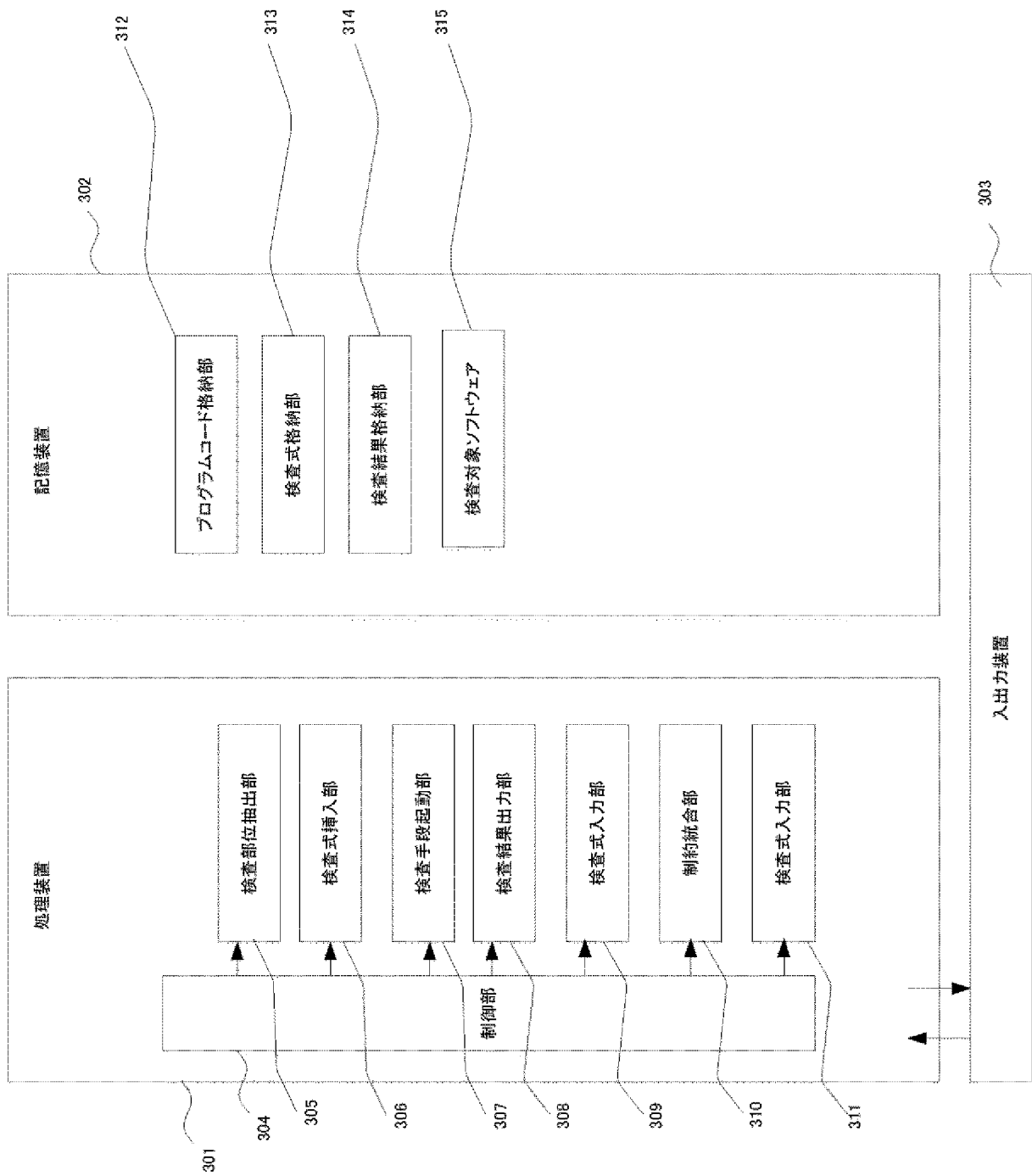
前記センサの入力をもとに制御演算を行いアクチュエータへ出力する制御装置において、

請求項 1 に記載の制御ソフトウェアを実行し、前記検査式による検査結果を保持または出力する制御装置。

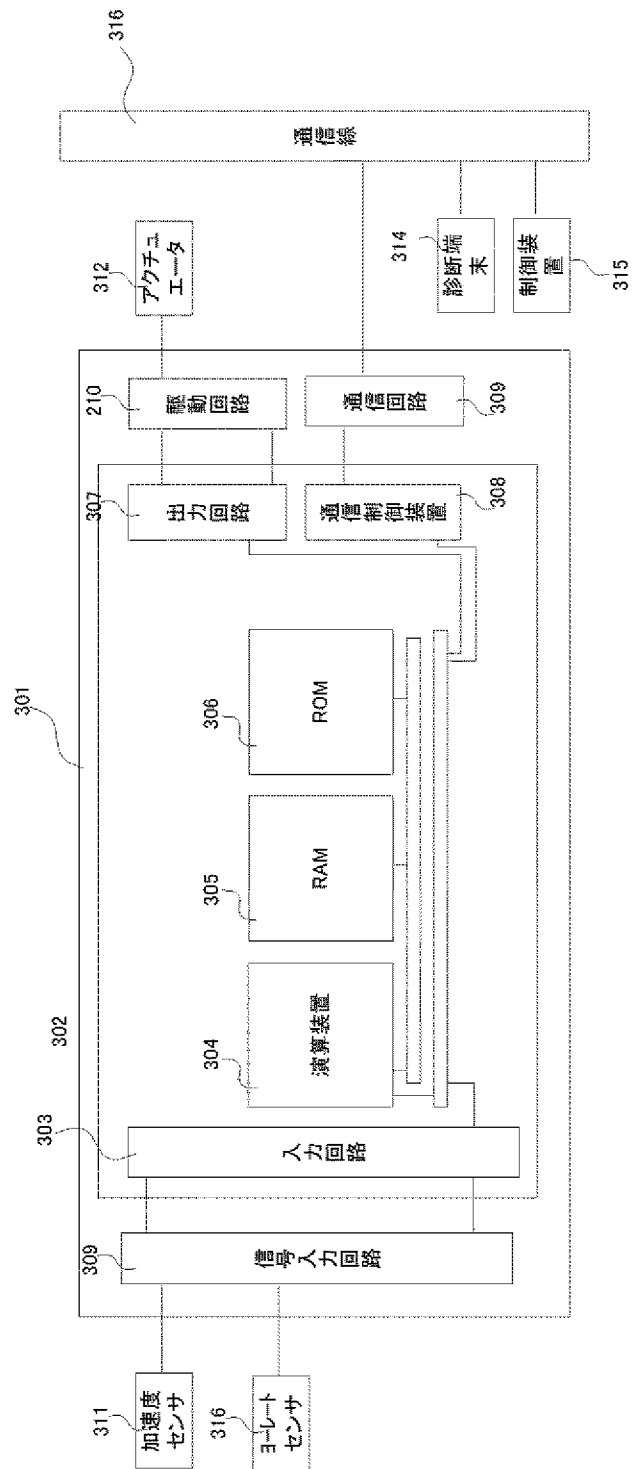
[図1]



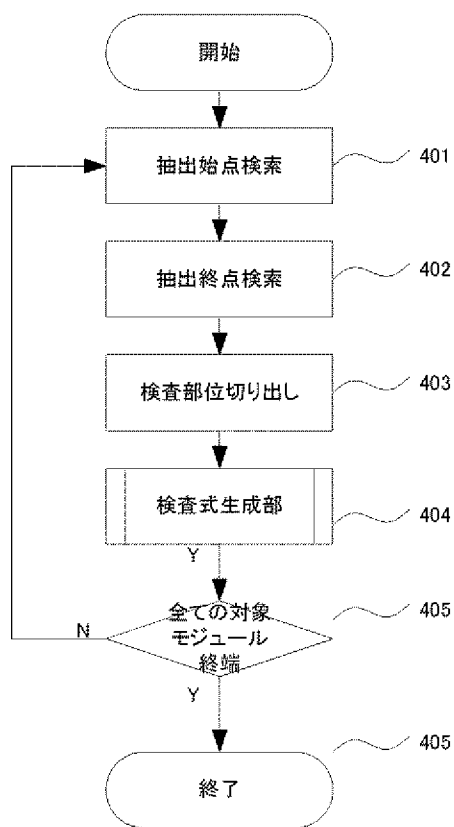
[図2]



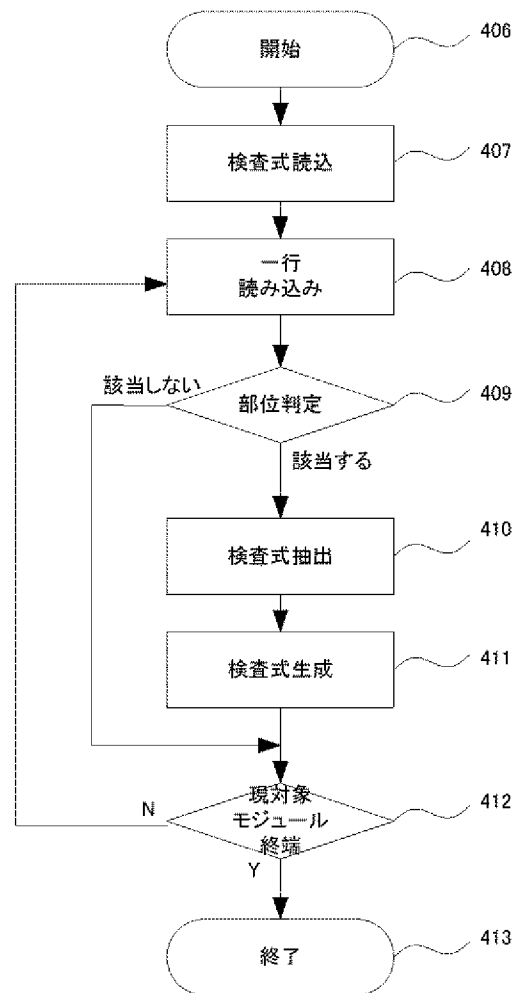
[図3]



[図4]



(a) 検査部位抽出部



(b) 検査式生成部

[5]

```

509
void ctrltask(void){
    :
    :
    InjSCalc();
    InjRCalc();
    :
    :
}

```

図 5(c)

```

801 void InjSCalc(void){
      unsigned short sinjw;
      /* INPUT: ETH, WTP */
802   _OPROVER_assume( 0<= ETH && ETH <= 50);
      _OPROVER_assume( 20<= WTP && WTP <= 120);
803   sinjw = QUADCALC (INJSM, ETH, WTP);
      SINJW = sinjw;
804   assert( 0<= SINJW && SINJW <= 150);
}

```

図 5(a)

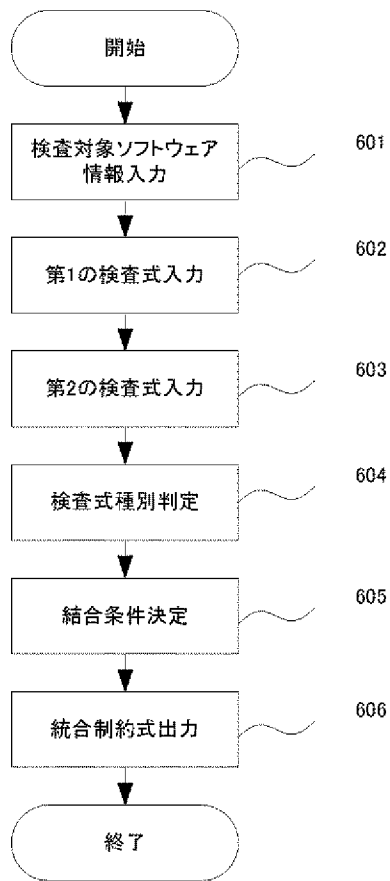
```

505 void InjRCalc(void){
      unsigned short rinjw;
806   _OPROVER_assume( 0<= ETH && ETH <= 50);
      _OPROVER_assume( 20<= WTP && WTP <= 120);
      _OPROVER_assume( 0<= SINJW && SINJW <= 150);
807   if(EMOD == RUN){
      rinjw = QUADCALC(INJNM, ETH, WTP);
      }else if(EMOD == START){
      rinjw = LINCALC (INJSM, ETH);
      }else if(EMOD == WTERR){
      rinjw = LINCALC (INJWEM, ETH);
      }else{
      rinjw = INJWDF;
      }
      INJW = SINJW + rinjw;
808   runtime_assert( 0<= INJW && INJW <= 200,
      &log[id], "INJWLMT:%d, TIMER: %d",
      INJW, timer);
}

```

図 5(b)

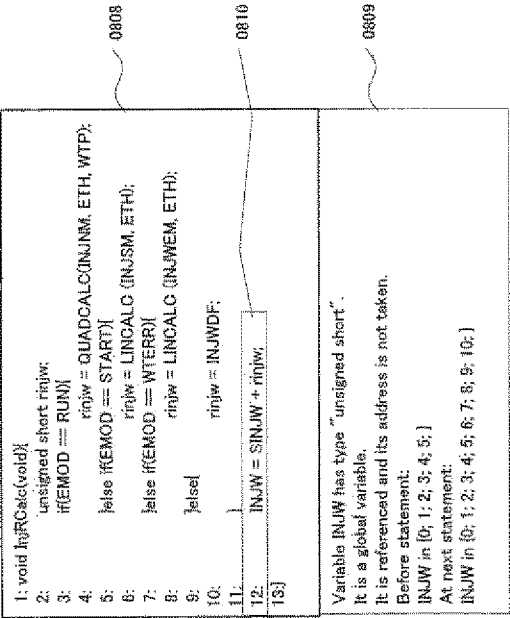
[図6]



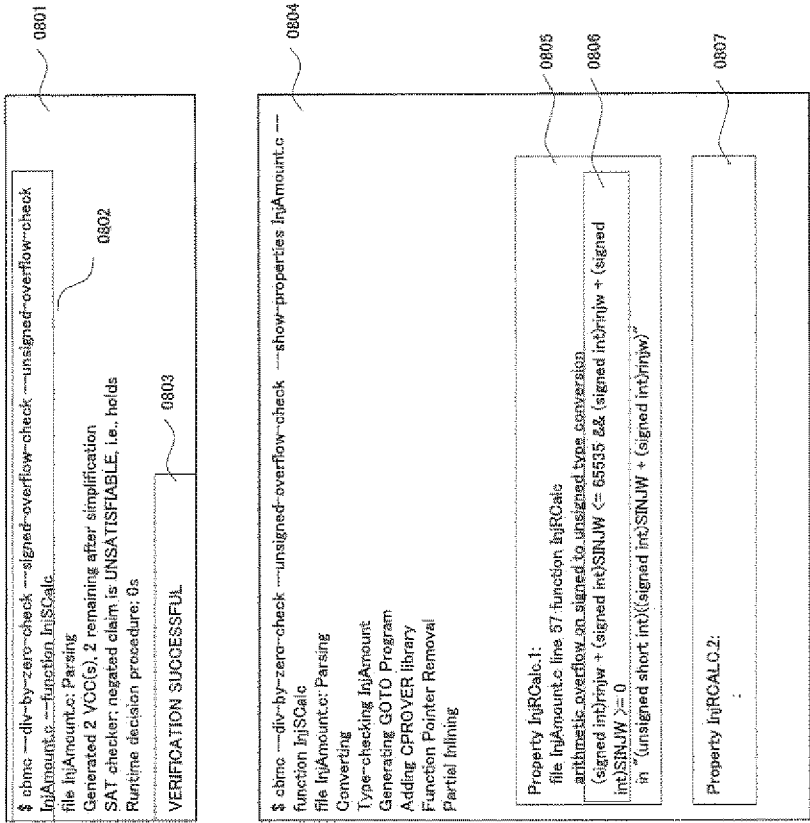
[図7]

起動条件	条件種別	結合子	条件
Pre: function: INJWCALC()	hold	&&	0 <= INJW && INJW <= 50
always	hold		EMOD==RUN && 0 <= INJW && INJW <= 255
always	hold		EMOD==START && 0 <= INJW && INJW <= 64
file: module1.c lineno: 110	do not hold	&& !(¥1)	(HWFAIL = 1) && (SYSSTAT== NORMAL)
:	:	:	:

[8]



8(b)



8(a)

[図9]

検査式固定部1	条件式	検査式固定部2
"_CPROVER_assert(" + \$condexp	+	");"

902 903 904 901

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2015/071185

A. CLASSIFICATION OF SUBJECT MATTER

G06F11/36(2006.01) i, G06F11/28(2006.01) i

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)

G06F11/36, G06F11/28

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

Jitsuyo Shinan Koho	1922-1996	Jitsuyo Shinan Toroku Koho	1996-2015
Kokai Jitsuyo Shinan Koho	1971-2015	Toroku Jitsuyo Shinan Koho	1994-2015

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 2010-218148 A (Toshiba Corp.), 30 September 2010 (30.09.2010), paragraphs [0015] to [0096]; fig. 1 to 7 & US 2010/0235818 A1 paragraphs [0049] to [0137]; fig. 1 to 7	1-6
A	WO 2011/052030 A1 (Toshiba Corp.), 05 May 2011 (05.05.2011), entire text; all drawings & US 2012/0266133 A1 entire text; all drawings	1-6

☐ 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
05 November 2015 (05.11.15)

Date of mailing of the international search report
17 November 2015 (17.11.15)

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

Authorized officer

Telephone No.

A. 発明の属する分野の分類（国際特許分類（I P C））

Int.Cl. G06F11/36(2006.01)i, G06F11/28(2006.01)i

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（I P C））

Int.Cl. G06F11/36, G06F11/28

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

日本国実用新案公報	1 9 2 2 - 1 9 9 6 年
日本国公開実用新案公報	1 9 7 1 - 2 0 1 5 年
日本国実用新案登録公報	1 9 9 6 - 2 0 1 5 年
日本国登録実用新案公報	1 9 9 4 - 2 0 1 5 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 2010-218148 A（株式会社東芝）2010.09.30, 段落 [0015] - [0096]、図1-7 & US 2010/0235818 A1, 段落[0049]-[0137], 図1-7	1-6
A	WO 2011/052030 A1（株式会社 東芝）2011.05.05, 全文、全図 & US 2012/0266133 A1, 全文、全図	1-6

☐ 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。

* 引用文献のカテゴリー

「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

「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

「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）

「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

「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矛盾するものではなく、発明の原理又は理論の理解のために引用するもの

「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

「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

「&」同一パテントファミリー文献

国際調査を完了した日

0 5 . 1 1 . 2 0 1 5

国際調査報告の発送日

1 7 . 1 1 . 2 0 1 5

国際調査機関の名称及びあて先

日本国特許庁（I S A / J P）

郵便番号100-8915

東京都千代田区霞が関三丁目4番3号

特許庁審査官（権限のある職員）

衣川 裕史

5 B

9 5 5 7

電話番号 03-3581-1101 内線 3545