(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2016-200948
(P2016-200948A)
(43)公開日　平成28年12月1日(2016.12.1)

(51)Int.Cl.		F I			テーマコード（参考）
G06F 21/44	(2013.01)	G06F	21/44		
G06F 21/62	(2013.01)	G06F	21/62	３１８	
G06F 21/12	(2013.01)	G06F	21/12	３１０	

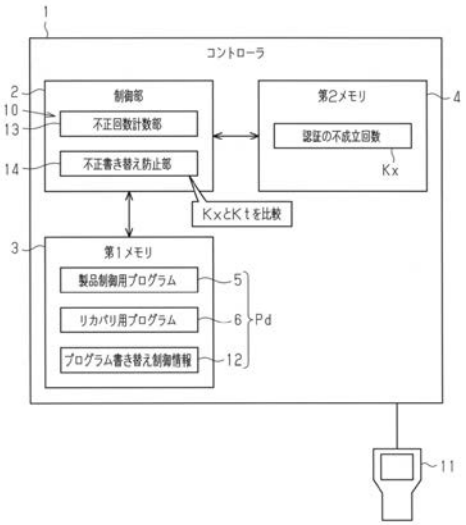
審査請求 未請求　請求項の数 5　ＯＬ　（全 8 頁）

(21)出願番号　特願2015-80131(P2015-80131)
(22)出願日　平成27年4月9日(2015.4.9)

(71)出願人　000003551
株式会社東海理化電機製作所
愛知県丹羽郡大口町豊田三丁目２６０番地
(74)代理人　100105957
弁理士　恩田　誠
(74)代理人　100068755
弁理士　恩田　博宣
(72)発明者　八木　英樹
愛知県丹羽郡大口町豊田三丁目２６０番地
株式会社東海理化電機製作所内

(54)【発明の名称】プログラム不正書き替え防止装置

(57)【要約】
【課題】プログラムデータの不正書き替えを生じ難くすることができるプログラム不正書き替え防止装置を提供する。
【解決手段】ツール１１からコントローラ１にアクセスしてプログラム書き替えを行うとき、不正回数計数部１３は、ツール１１とコントローラ１との間に課される認証（本例はチャレンジレスポンス認証）の不成立回数Ｋｘを計数する。不正書き替え防止部１４は、不成立回数Ｋｘが規定値Ｋｔ以上となったことを確認すると、コントローラ１の第１メモリ３に書き込まれているプログラムデータＰｄの書き替えを制限又は禁止する処置を実行する。
【選択図】図１



【特許請求の範囲】
【請求項１】
コントローラのメモリに書き込まれたプログラムが不正に書き替えられるのを防止するプログラム不正書き替え防止装置において、
ツールから入力するプログラム書き替え要求を基に前記コントローラ及びツールの間で認証が実行されるにあたり、繰り返された当該認証において、該認証が不正となった回数を計数する不正回数計数部と、
前記認証が不正となった回数が規定値以上となったとき、前記メモリのプログラムの書き替えを制限又は禁止する不正書き替え防止部と
を備えたことを特徴とするプログラム不正書き替え防止装置。
【請求項２】
前記認証は、チャレンジレスポンス認証である
ことを特徴とする請求項１に記載のプログラム不正書き替え防止装置。
【請求項３】
前記コントローラは、前記プログラムの書き込み先となる第１メモリと、前記認証が不正となった回数を書き込む第２メモリとを備え、
前記不正回数計数部は、前記認証が不正となった回数を前記第２メモリに逐次書き込んでいくことにより、当該回数を計数する
ことを特徴とする請求項１又は２に記載のプログラム不正書き替え防止装置。
【請求項４】
前記不正書き替え防止部は、前記認証が不正となった回数が規定値以上となったとき、前記ツールに対して、通信不可の旨を通知する処理、又は返信を返さない処理を実行する
ことを特徴とする請求項１～３のうちいずれか一項に記載のプログラム不正書き替え防止装置。
【請求項５】
前記コントローラのメモリは、通常の作動時に使用される製品制御用プログラムが書き込まれ、
前記不正書き替え防止部は、前記認証が不正となった回数が規定値以上となったとき、前記メモリに書き込まれている前記製品制御用プログラムを消去して、リカバリ動作を実行する
ことを特徴とする請求項１～３のうちいずれか一項に記載のプログラム不正書き替え防止装置。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、コントローラに書き込まれたプログラムデータの不正書き替えを防止するプログラム不正書き替え防止装置に関する。
【背景技術】
【０００２】
従来、コントローラのメモリに書き込まれたプログラムデータの不正書き替えを防止するプログラム不正書き替え防止装置が周知である（特許文献１等参照）。コントローラのプログラムデータを書き替える一例としては、例えばツールを使用する形式がある。この場合、例えばツールとコントローラとの間で認証が実施され、この認証が成立すれば、ツールによるプログラムデータの書き替えが許可される。
【先行技術文献】
【特許文献】
【０００３】
【特許文献１】特開２０１４－８８０６２号公報
【発明の概要】
【発明が解決しようとする課題】

【０００４】
ところで、第三者が不正なツールを使用して、コントローラのプログラムデータを書き替えようと試みる場合も想定される。ツールとコントローラとの間の認証としてチャレンジレスポンス認証を採用している場合、例えば疑似乱数を何度も繰り返して相手側に送信することにより、不正に認証を成立させてしまう行為が考えられる。よって、このような不正なプログラムデータの書き替え行為に対する対策が必要とされていた。
【０００５】
本発明の目的は、プログラムデータの不正書き替えを生じ難くすることができるプログラム不正書き替え防止装置を提供することにある。
【課題を解決するための手段】
【０００６】
前記問題点を解決するプログラム不正書き替え防止装置は、コントローラのメモリに書き込まれたプログラムが不正に書き替えられるのを防止する構成において、ツールから入力するプログラム書き替え要求を基に前記コントローラ及びツールの間で認証が実行されるにあたり、繰り返された当該認証において、該認証が不正となった回数を計数する不正回数計数部と、前記認証が不正となった回数が規定値以上となったとき、前記メモリのプログラムの書き替えを制限又は禁止する不正書き替え防止部とを備えた。
【０００７】
本構成によれば、ツールとコントローラとの間で実行される認証の不成立回数を計数し、不成立回数が規定値以上となったときには、コントローラのメモリに書き込まれているプログラムの書き替えを制限又は禁止する処置を実行する。このため、仮に不正なツールを用いて認証を何度も行って当該認証を不正に成立させようとする行為に対して、認証の不成立回数が規定値以上となった時点で、この不正行為を終了させることが可能となる。よって、プログラムデータの不正書き替えを生じ難くすることが可能となる。
【０００８】
前記プログラム不正書き替え防止装置において、前記認証は、チャレンジレスポンス認証であることが好ましい。この構成によれば、第三者によりツールを通じてチャレンジレスポンスの弱点をつくような不正行為をされても、認証の不成立回数が規定値以上となったときにプログラムの書き替えが制限又は停止される。よって、２者間の認証にチャレンジレスポンス認証を使用したとしても、プログラムの不正書き替えを生じ難くすることが可能となる。
【０００９】
前記プログラム不正書き替え防止装置において、前記コントローラは、前記プログラムの書き込み先となる第１メモリと、前記認証が不正となった回数を書き込む第２メモリとを備え、前記不正回数計数部は、前記認証が不正となった回数を前記第２メモリに逐次書き込んでいくことにより、当該回数を計数することが好ましい。この構成によれば、プログラムの書き込み箇所と不成立回数の書き込み箇所とをそれぞれ別としたので、各情報を管理し易くすることが可能となる。
【００１０】
前記プログラム不正書き替え防止装置において、前記不正書き替え防止部は、前記認証が不正となった回数が規定値以上となったとき、前記ツールに対して、通信不可の旨を通知する処理、又は返信を返さない処理を実行することが好ましい。この構成によれば、認証の不成立回数が規定値以上となったときには、ツールに通信不可の旨を通知する、又はツールに返信を返さないという簡素な処理により、第三者によるツールを用いたプログラムの不正書き替えに対する処置を講ずることが可能となる。
【００１１】
前記プログラム不正書き替え防止装置において、前記コントローラのメモリは、通常の作動時に使用される製品制御用プログラムが書き込まれ、前記不正書き替え防止部は、前記認証が不正となった回数が規定値以上となったとき、前記メモリに書き込まれている前記製品制御用プログラムを消去して、リカバリ動作を実行することが好ましい。この構成

によれば、認証の不成立回数が規定値以上となったときには、コントローラにリカバリ動作を実行させるので、リカバリ後、第三者が所持するようなツール（不正ツール）ではプログラム書き替えを実行することができなくなる。よって、プログラム不正書き替えの防止に一層有利となる。

【発明の効果】

【００１２】

本発明によれば、プログラムデータの不正書き替えを生じ難くすることができる。

【図面の簡単な説明】

【００１３】

【図１】一実施形態のプログラム不正書き替え防止装置の構成図。

【図２】ツール及びコントローラの間で実行される認証のシーケンス図。

【図３】認証が不正と判定されたときの処置の一例を示すシーケンス図。

【図４】認証が不正と判定されたときの他の処置の一例を示す説明図。

【発明を実施するための形態】

【００１４】

以下、プログラム不正書き替え防止装置の一実施形態を図１～図４に従って説明する。

図１に示すように、コントローラ１は、例えばＥＣＵ（Electronic Control Unit）からなる。コントローラ１は、コントローラ１の作動を制御する制御部２と、コントローラ１の作動時に実行されるプログラムデータＰｄが書き込まれた第１メモリ３と、プログラムデータＰｄによってのみ書き込み及び読み出しが可能な第２メモリ４とを備える。第１メモリ３及び第２メモリ４は、例えば不揮発性メモリからなり、第１メモリ３がプログラムＲＯＭ（Read Only Memory）からなり、第２メモリ４がデータフラッシュからなることが好ましい。

【００１５】

第１メモリ３には、コントローラ１を通常時において作動させる際に実行される製品制御用プログラム５と、コントローラ１をリカバリ動作（初期化）するときに実行されるリカバリ用プログラム６とが書き込み保存されている。制御部２は、製品制御用プログラム５を実行することにより、コントローラ１における演算や、他のＥＣＵとのデータ通信などを実行する。また、制御部２は、例えばコントローラ１においてリカバリを開始する要件が揃ったときや、外部からリカバリ要求等の指令を受け付けたとき、リカバリ用プログラム６を実行することにより、コントローラ１を初期化する。

【００１６】

コントローラ１は、プログラムデータＰｄの不正書き替えを防止するプログラム不正書き替え防止機能（プログラム不正書き替え防止装置１０）を備える。ところで、コントローラ１のプログラムデータＰｄを書き替えるにあたっては、コントローラ１との間でチャレンジレスポンス認証が成立することが課されている。チャレンジレスポンス認証は、相手側に疑似乱数であるチャレンジコードを送信して演算させ、その演算結果であるレスポンスコードを取得して、これの正否を確認する認証である。本例のプログラム不正書き替え防止装置１０は、例えばコントローラ１に接続された外部のツール１１からの不正なプログラム書き替え行為に対して、プログラムデータＰｄが意図に不正に書き替えられてしまうことに対する対策として設けられている。本例が想定するプログラム不正書き替え行為は、例えばプログラムデータＰｄの連続的な書き替え攻撃である。

【００１７】

プログラム不正書き替え防止装置１０は、プログラム不正書き替え防止装置１０を実現するにあたってのソフトウェアとなるプログラム書き替え制御情報１２を備える。プログラム書き替え制御情報１２は、第１メモリ３に書き込み保存されている。本例のプログラム書き替え制御情報１２は、チャレンジレスポンス認証の不成立となる回数（不成立回数Ｋｘ）を計数し、その回数が規定値Ｋｔ以上となったときに、プログラム不正書き替え行為に対する処置を実行することを実現するソフトウェアである。

【００１８】

プログラム不正書き替え防止装置１０は、チャレンジレスポンス認証の不成立回数を計数する不正回数計数部１３を備える。不正回数計数部１３は、制御部２がプログラム書き替え制御情報１２を実行することにより、制御部２に機能的に生成される。不正回数計数部１３は、ツール１１から入力するプログラム書き替え要求を基にコントローラ１及びツール１１の間で認証（本例はチャレンジレスポンス認証）が実行されるにあたり、連続的に繰り返された認証が不成立となった回数（不成立回数Ｋｘ）を計数する。不正回数計数部１３は、認証の不成立回数Ｋｘを第２メモリ４に書き込み、回数が増える度に、これを逐次更新する。

【００１９】

プログラム不正書き替え防止装置１０は、不成立回数Ｋｘが規定値Ｋｔ以上となったときにプログラムデータＰｄの書き替えを制限又は禁止する不正書き替え防止部１４を備える。不正書き替え防止部１４は、制御部２がプログラム書き替え制御情報１２を実行することにより、制御部２に機能的に生成される。プログラムデータＰｄの書き替えの制限又は禁止の処理としては、例えばチャレンジレスポンス認証において相手に通信不可を通知することや、通信自体を実施しない（途中で停止する）などがある。また、これ以外としては、コントローラ１のリカバリ動作がある。

【００２０】

次に、図２～図４を用いて、プログラム不正書き替え防止装置１０の動作を説明する。

図２に示すように、ステップ１０１において、ツール１１は、プログラム書き替えの実行をコントローラ１に要求するプログラム書き替え要求Ｓａをコントローラ１に出力する。プログラム書き替え要求Ｓａは、チャレンジレスポンス認証に必要な認証情報Ｓｂの送信をコントローラ１に要求する認証情報出力要求であることが好ましい。この場合、プログラム書き替え要求Ｓａは、例えばチャレンジレスポンス認証に必要な暗号鍵（共通鍵）と、認証の度に毎回異なる値をとる乱数値（チャレンジコード）とを、コントローラ１に送信させる要求であることが好ましい。

【００２１】

ステップ１０２において、コントローラ１は、ツール１１からプログラム書き替え要求（認証情報出力要求）Ｓａを受信すると、認証情報Ｓｂをツール１１に送信する。認証情報Ｓｂは、チャレンジレスポンス認証用の暗号鍵（共通鍵）と、送信の度に値が毎回変更される乱数値（チャレンジコード）とを含む情報であることが好ましい。

【００２２】

ステップ１０３において、ツール１１は、コントローラ１から受信した認証情報Ｓｂを基に、チャレンジレスポンス認証の演算結果である鍵値（レスポンスコード）Ｓｃを演算する。本例の場合、ツール１１は、コントローラ１から取得した乱数及び暗号鍵を、ツール１１に登録されたアルゴリズム（関数）に通すことにより、演算を実行する。

【００２３】

ステップ１０４において、ツール１１は、演算した鍵値（レスポンスコード）Ｓｃをコントローラ１に送信する。

ステップ１０５において、コントローラ１は、ツール１１から鍵値（レスポンスコード）Ｓｃを受信すると、自らも同様に演算した鍵値（レスポンスコード）と比較することにより、認証を実行する。コントローラ１は、これら鍵値Ｓｃが一致することを確認すると、チャレンジレスポンス認証を成立とし、逆に一致しなければ、チャレンジレスポンス認証を不成立とする。このとき、不正回数計数部１３は、認証（チャレンジレスポンス認証）が成立しないことを確認すると、例えば第２メモリ４のカウンタを「１」、更新するなどして、認証の不成立回数Ｋｘを計数する。

【００２４】

ステップ１０６において、コントローラ１は、鍵値Ｓｃの認証結果Ｓｄをツール１１に通知する。すなわち、コントローラ１は、チャレンジレスポンス認証が成立すれば、認証成立の旨の通知Ｓｄをツール１１に出力し、チャレンジレスポンス認証が不成立であれば、認証不成立の旨の通知Ｓｄをツール１１に出力する。

【００２５】
ステップ１０７において、ツール１１は、コントローラ１から取得した鍵値の認証結果Ｓｄを基に、認証が成立したか否かを確認する。すなわち、認証成立の旨の通知Ｓｄを受け付ければ、チャレンジレスポンス認証が成立したと判断し、認証不成立の旨の通知Ｓｄを受け付ければ、チャレンジレスポンス認証が不成立であると判断する。
【００２６】
ところで、悪意をもった第三者がツール（不正ツール）１１を通じてコントローラ１との認証（チャレンジレスポンス認証）をすり抜けようとした場合には、疑似乱数を都度生成することによってチャレンジレスポンス認証が繰り返し実行される。このとき、ツール１１が不正ツールであれば認証が成立しないので、不成立回数Ｋｘの計数値が「１」ずつ、カウントアップされていく。不正書き替え防止部１４は、不成立回数Ｋｘが規定値Ｋｔ以上となったことを確認すると、プログラム不正書き替えに対する処置を実行する。
【００２７】
図３に、プログラム不正書き替えに対する処置の一例を図示する。同図の例（１）に示されるように、不正書き替え防止部１４は、プログラム書き替え行為が不正であると判定したとき、いま通信中のツール１１に対して、通信不可の通知を実施する。また、これ以外の動作としては、同図の例（２）に示されるように、不正書き替え防止部１４は、プログラム書き替え行為が不正であると判定されたとき、ツール１１に返信自体を実施しない（応答を返さない）ようにしてもよい。いずれの処置を実施するにせよ、ツール１１との通信が途中で強制終了されるので、プログラムデータＰｄが不正に書き替えられてしまうことがない。
【００２８】
図４に、プログラム不正書き替えに対する処置の他の例を図示する。同図に示されるように、不正書き替え防止部１４は、プログラム書き替え行為が不正であると判定したとき、第１メモリ３に書き込まれている製品制御用プログラム５を消去し、リカバリ用プログラム６を実行することによって、リカバリ動作を実行してもよい。こうすれば、コントローラ１が初期化されてツール１１との通信は不可となるので、プログラムデータＰｄが不正に書き替えられずに済む。
【００２９】
本実施形態の構成によれば、以下に記載の効果を得ることができる。
（１）ツール１１からコントローラ１にアクセスしてプログラム書き替えを行うとき、ツール１１とコントローラ１との間に課される認証（本例はチャレンジレスポンス認証）の不成立回数Ｋｘを計数し、不成立回数Ｋｘが規定値Ｋｔ以上となったときには、コントローラ１の第１メモリ３に書き込まれているプログラムデータＰｄの書き替えを制限又は禁止する処置を実行する。このため、仮に不正なツール１１を用いて認証を何度も行って当該認証を不正に成立させようとする行為に対して、認証の不成立回数Ｋｘが規定値Ｋｔ以上となった時点で、この不正行為を終了させることが可能となる。よって、コントローラ１のプログラムデータＰｄの不正書き替えを生じ難くすることができる。
【００３０】
（２）コントローラ１のプログラムデータＰｄをツール１１により書き替えるときに課される認証は、チャレンジレスポンス認証である。ところで、チャレンジレスポンス認証には、乱数が偏ってしまう傾向があり、ツール１１からコントローラ１にアクセスしたとき、この点をつき、認証をすり抜けようと試みられることも想定される。しかし、本例の場合は、認証の不成立回数Ｋｘが規定値Ｋｔ以上となったときには、プログラム書き替えを制限するので、チャレンジレスポンス認証の弱点をつくような不正行為をされても、これに対処することができる。
【００３１】
（３）コントローラ１は、プログラムデータＰｄの書き込み先となる第１メモリ３と、認証の不成立回数Ｋｘを書き込む第２メモリ４とを備える。よって、本例の場合、プログラムの書き込み箇所と、認証の不成立回数Ｋｘの書き込み箇所とを、それぞれ別としたの

で、各情報を管理し易くすることができる。

【００３２】

（４）認証の不成立回数Ｋｘが規定値Ｋｔ以上となったときの処置は、ツール１１に対して通信不可の旨を通知する処理、又はツール１１に返信を返さない処理とした。このため、ツール１１からコントローラ１にプログラム書き替えの不正な攻撃があったときには、ツール１１に通信不可の旨の通知を行う、またはツール１１に応答しないという簡素な処理により、第三者によるツール１１を用いたプログラムの不正書き替えに対する処置を講ずることができる。

【００３３】

（５）認証の不成立回数Ｋｘが規定値Ｋｔ以上となったときの処置は、コントローラ１のリカバリ動作とした。これにより、リカバリ後は、第三者が所持するようなツール（不正なツール）１１ではプログラム書き替えを実行することができなくなる。よって、プログラム不正書き替えの防止に一層有利となる。

【００３４】

なお、実施形態はこれまでに述べた構成に限らず、以下の態様に変更してもよい。

・一般的に、コントローラ１の第１メモリ３には、コントローラ１を作動させるにあたって逐次登録されていく設定情報が書き込まれる。設定情報は、例えばアプリケーションの一種である。この場合、認証の不成立回数Ｋｘが規定値Ｋｔ以上となってプログラム書き替え行為が不正と判定されたときに、コントローラ１の第１メモリ３に書き込まれた設定情報を削除するようにしてもよい。このようにしても、コントローラ１から設定情報が削除された時点で通常通りの作動ができなくなるので、ツール１１と通信を実行することができなくなる。よって、第三者によるツール１１を通じてのプログラム不正書き替えを生じ難くすることができる。

【００３５】

・認証の不成立回数Ｋｘをクリア（リセット）するのは、どのタイミングでもよい。すなわち、不成立回数Ｋｘは、１機会の不正攻撃に対する計数値でもよいし、または複数機会に亘っての積算値でもよい。

【００３６】

・ツール１１を用いてプログラム書き替えを行うときに両者の間に課す認証は、チャレンジレスポンス認証に限らず、相手側の正否を確認できるものであれば、種々の態様に変更可能である。

【００３７】

・第１メモリ３と第２メモリ４とを１つのメモリにまとめてもよい。

・認証の不成立回数Ｋｘが規定値Ｋｔ以上となったときに実施する処置は、プログラム書き替えを制限又は禁止する処理であれば、種々の態様に変更可能である。

【００３８】

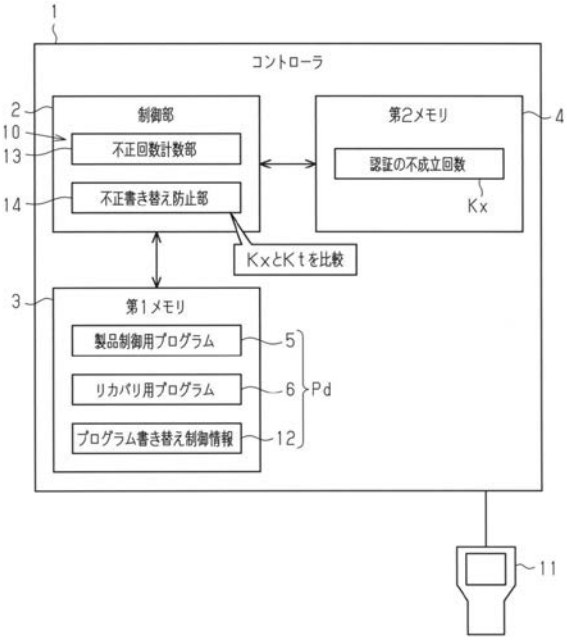
・本例のコントローラ１は、種々の装置や機器に適用可能である。

【符号の説明】

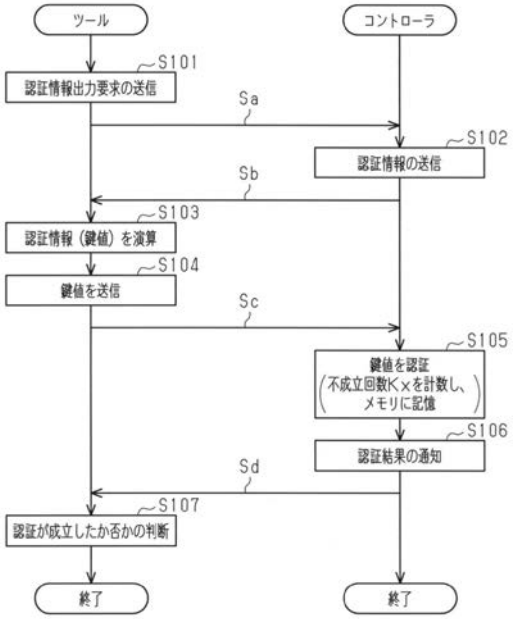
【００３９】

１…コントローラ、３…メモリ（第１メモリ）、５…製品制御用プログラム、６…リカバリ用プログラム、１０…プログラム不正書き替え防止装置、１１…ツール、１３…不正回数計数部、１４…不正書き替え防止部、Ｐｄ…プログラム（プログラムデータ）、Ｓａ…プログラム書き替え要求、Ｋｘ…不成立回数、Ｋｔ…規定値。

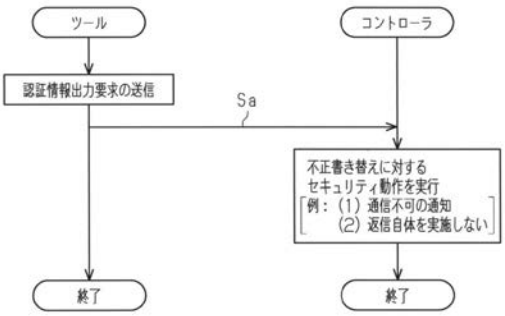
【図１】


1
コントローラ
2
制御部
10
13
不正回数計数部
14
不正書き替え防止部
第2メモリ
4
認証の不成立回数
Kx
KxとKtを比較
3
第1メモリ
製品制御用プログラム
5
リカバリ用プログラム
6
Pd
プログラム書き替え制御情報
12
11

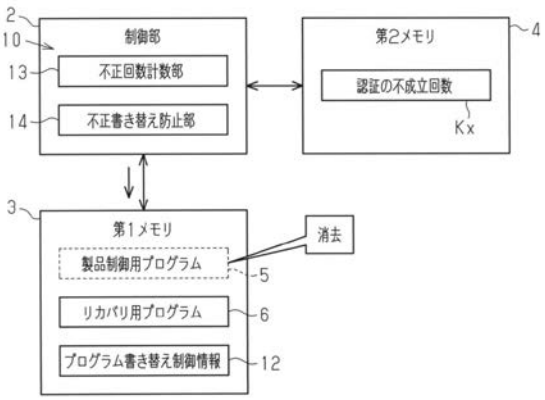
【図２】


ツール
コントローラ
S101
認証情報出力要求の送信
Sa
S102
認証情報の送信
Sb
S103
認証情報（鍵値）を演算
S104
鍵値を送信
Sc
S105
鍵値を認証
（不成立回数Kxを計数し、メモリに記憶）
S106
認証結果の通知
Sd
S107
認証が成立したか否かの判断
終了
終了

【図３】


ツール
コントローラ
認証情報出力要求の送信
Sa
不正書き替えに対する
セキュリティ動作を実行
例：（1）通信不可の通知
（2）返信自体を実施しない
終了
終了

【図４】


2
10
制御部
13
不正回数計数部
14
不正書き替え防止部
第2メモリ
4
認証の不成立回数
Kx
3
第1メモリ
消去
製品制御用プログラム
5
リカバリ用プログラム
6
プログラム書き替え制御情報
12