

(19) 日本国特許庁(JP)

(12) 特 許 公 報(B2)

(11) 特許番号

特許第4131446号
(P4131446)

(45) 発行日 平成20年8月13日(2008.8.13)

(24) 登録日 平成20年6月6日(2008.6.6)

(51) Int. Cl. F I
B6OR 25/04 (2006.01) B6OR 25/04 6O2
B6OR 25/00 (2006.01) B6OR 25/04 61O
FO2N 15/00 (2006.01) B6OR 25/00 6O1
 FO2N 15/00 F

請求項の数 6 (全 16 頁)

<p>(21) 出願番号 特願2005-30040 (P2005-30040) (22) 出願日 平成17年2月7日(2005.2.7) (65) 公開番号 特開2006-213256 (P2006-213256A) (43) 公開日 平成18年8月17日(2006.8.17) 審査請求日 平成19年9月20日(2007.9.20)</p> <p>早期審査対象出願</p>	<p>(73) 特許権者 304063451 ウェブシステム企業組合 山形県山形市松栄一丁目3-8 山形県産 業創造支援センター (74) 代理人 100085589 弁理士 ▲桑▼原 史生 (72) 発明者 長瀬 幹雄 山形県山形市松栄一丁目3番8号 山形県 産業創造支援センター内 ウェブシステム 企業組合内</p> <p>審査官 大谷 謙仁</p>
---	--

最終頁に続く

(54) 【発明の名称】 エンジン始動制御システム

(57) 【特許請求の範囲】

【請求項1】

車両を運転するオペレータが所持する鍵手段と、車両に設置される第一の制御部と、車両のエンジンを始動させるためのスタータモータのマグネチックスイッチに内蔵される第二の制御部とからなり、第一の制御部は、鍵手段に記憶された特定の認証データに一意に対応付けられた認証データを記憶する第一の記憶手段と、鍵手段が挿入されたときに鍵手段に記憶された認証データと第一の記憶手段に記憶された認証データとを照合して鍵手段が正規のものであるか否かを判定する認証手段と、挿入された鍵手段が正規のものであると認証手段により判定されたときに稼動許可信号を送出する送信手段とを備え、第二の制御部は、第一の制御部の送信手段から稼動許可信号を受信する受信手段と、スタータモータを始動するための電流を通電又は遮断するモータ制御スイッチと、受信手段が稼動許可信号を受信したときにモータ制御スイッチをオンにしてスタータモータの始動を許容する始動制御手段とを備え、第一の制御部の送信手段から第二の制御部の受信手段に送信される稼動許可信号の伝送媒体として車両の車体が利用され、鍵手段に記憶される認証データは、任意桁数の数字列よりなる認証番号と、この認証番号の各桁の数字を送信してからその一つ下位の桁の数字を送信するまでの送信時間としてランダムに設定された送信時間タイミングデータとの組合せを有し、第一の制御部の第一の記憶手段に記憶される認証データが、鍵手段に記憶される認証データの認証番号と一意に対応付けられた同桁数の数字列を含む認証番号と、鍵手段に記憶される送信時間タイミングデータと一意に対応付けられた受信時間タイミングデータとの組合せを有することを特徴とするエンジン始動制御システム

ム。

【請求項 2】

第一の制御部は、さらに、外部管理サーバとの間でデータ送受信を可能にするためのデータ通信手段と、データ通信手段を通じて外部管理サーバから認証データ変更指令を受信したときに第一のメモリに記憶されている認証データを変更する認証データ変更手段とを備えることを特徴とする請求項 1 記載のエンジン始動制御システム。

【請求項 3】

エンジンのガバナに設けられた第三の制御部をさらに備え、第三の制御部は、第一の制御部の送信手段から稼動許可信号を受信する受信手段と、受信手段が稼動許可信号を受信しなくなったときにエンジンへの燃料供給を停止させるガバナ制御手段とを備えることを特徴とする請求項 2 記載のエンジン始動制御システム。

10

【請求項 4】

第一の制御部は、車両を特定する車両 ID を記憶する第二の記憶手段をさらに備えるとともに、第二の制御部は、第一の制御部の第二の記憶手段に記憶された車両 ID と一意に対応付けられた車両 ID を記憶する第三の記憶手段と、第一の制御部の第二の記憶手段に記憶された車両 ID と第三の記憶手段に記憶された車両 ID とを照合して受信手段で受信した稼動許可信号が当該車両の第一の制御部から発信されたものであるか否かを判定する車両判定手段とをさらに備え、始動制御手段は、受信した稼動許可信号が当該車両からのものであることが車両判定手段によって判定されたことを条件としてモータ制御スイッチをオンにすることを特徴とする請求項 1 乃至 3 のいずれか記載のエンジン始動制御システム

20

【請求項 5】

第一の制御部の第二の記憶手段に記憶される車両 ID が、任意桁数の数字列よりなる認証番号と、この認証番号の各桁の数字を送信してからその一つ下位の桁の数字を送信するまでの送信時間としてランダムに設定された送信時間タイミングデータとの組合せを有し、第二の制御部の第三の記憶手段に記憶される車両 ID が、第一の制御部の第二の記憶手段に記憶される車両 ID の認証番号と一意に対応付けられた同桁数の数字列を含む認証番号と、第一の制御部の第一の記憶手段に記憶される送信時間タイミングデータと一意に対応付けられた受信時間タイミングデータとの組合せを有することを特徴とする請求項 4 記載のエンジン始動制御システム。

30

【請求項 6】

車両に設置され、一定の条件が満たされたときに稼動許可信号を送出する第一の制御部と、車両のエンジンを始動させるためのスタータモータのマグネットスイッチに内蔵され、スタータモータを始動するための電流を通電又は遮断するモータ制御スイッチと、第一の制御部から稼動許可信号を受信したときにモータ制御スイッチをオンにしてスタータモータの始動を許容する始動制御手段とを備える第二の制御部とを備え、第一の制御部の送信手段から第二の制御部の受信手段に送信される稼動許可信号の送信媒体として車両の車体が利用され、第一の制御部は、車両を特定する車両 ID を記憶する第一の記憶手段を備えるとともに、第二の制御部は、第一の記憶手段に記憶された車両 ID と一意に対応付けられた車両 ID を記憶する第二の記憶手段と、第一の記憶手段に記憶された車両 ID と第二の記憶手段に記憶された車両 ID とを照合して受信した稼動許可信号が当該車両の第一の制御部から発信されたものであるか否かを判定する車両判定手段とを備え、始動制御手段は、受信した稼動許可信号が当該車両からのものであることが車両判定手段によって判定されたことを条件としてモータ制御スイッチをオンにし、且つ、第一の制御部の第一の記憶手段に記憶される車両 ID は、任意桁数の数字列よりなる認証番号と、この認証番号の各桁の数字を送信してからその一つ下位の桁の数字を送信するまでの送信時間としてランダムに設定された送信時間タイミングデータとの組合せを有し、第二の制御部の第二の記憶手段に記憶される車両 ID は、第一の制御部の第一の記憶手段に記憶される車両 ID の認証番号と一意に対応付けられた同桁数の数字列を含む認証番号と、第一の制御部の第一の記憶手段に記憶される送信時間タイミングデータと一意に対応付けられた受信時間タイ

40

50

ミングデータとの組合せを有することを特徴とするエンジン始動制御システム。

【発明の詳細な説明】

【技術分野】

【0001】

本発明はエンジン始動制御システムに関し、より詳しくは、建設機械等の車両のエンジン始動を一定条件下において不可能とする制御を行うことにより車両盗難に対する有効な防止策を与えるためのシステムに関する。

【背景技術】

【0002】

近年車両の盗難が多発しており、大きな社会問題となっている。車両盗難の多くは、イグニッションキーを持たない者がスタータモータ（セルモータ）をバッテリーと直結させる方法等によってスタータモータを回転させ、これによってエンジンを始動することによって行われている。特にブルドーザやショベルカー等の建設機械（以下、建機）にあっては、イグニッションキーも建機メーカー毎に共通の鍵を使っており、防犯意識が非常に希薄なものであった。そして、バッテリー直結等の不正な方法によってエンジンが始動されてしまうと自走移動が可能となり、不正輸出等のためにキャリアカーに積載して遠隔地に移送されてしまい、しかも、該エンジンによって駆動される油圧機構を介してアタッチメントが動作可能になるので建設作業等に不自由なく用いることができる。

【0003】

図6を参照して、従来の建機を含む車両に用いられているスタータモータの作動原理を簡単に説明すると、運転者（以下、オペレータ）がイグニッションキーによりスタータスイッチ200をSTART位置に回転させると、マグネチックスイッチ300のリリースコイル303及びシャントコイル304に電流が流れ、この電流によって生じた電磁力によりプランジャ305が左方向（図6において、以下同じ）にスライドし、シフトレバー306が引っ張られて同方向に移動する。同時に、マグネチックスイッチ300のリリースコイル303に流れた電流は、スタータモータ400のフィールドコイル401及びアーマチュアコイル402にも流れて、アーマチュアコイル402を回転させる。これにより、ピニオンギヤ404は緩く回転しながらアーマチュアシャフト406に沿って押し出されるので、ピニオンギヤ404は確実にハズミ車のリングギヤ405に噛み合う。

【0004】

このとき、左方向に移動したプランジャ305の先端に取り付けられた移動コンタクタ301が固定コンタクタ302を短絡するので、バッテリーからの主電流がマグネチックスイッチ300のB端子からM端子を通してスタータモータ400に与えられ、スタータモータ400を高速回転させ、ピニオンギヤ404とリングギヤ405の噛合を介してエンジンを始動させる。

【0005】

スタータスイッチ200をON状態に戻すと、マグネチックスイッチ300の励磁力が消失してシフトレバー306は軸に取り付けられたリターンズプリング（図示せず）の力で元の位置（図6に示す位置）に引き戻される。これによりピニオンギヤ404も元の位置に戻るため、リングギヤ405との噛合が解かれ、スタータモータ400も止まる。

【0006】

ここで、イグニッションキーがなくても、車両盗難の常套手段となっているバッテリー直結の手口を使うとスタータスイッチ200をSTART位置に回転させたと同じことになり、エンジンが始動されてしまう。

【0007】

このような事情を背景として、下記特許文献1に、遠隔地にある建機の盗難防止を図るためのシステムが提案されている。このシステムは、エンジンのスタータモータに通電するスタータモータ回路と、レバー操作に基づいて機械の油圧動作を停止させる電磁切換弁と、上記スタータモータ回路とは独立した回路として上記電磁切換弁に通電するロック制御回路とを備えた建機の盗難防止システムであって、建機に、送信局から送信された運転

10

20

30

40

50

停止信号を人工衛星を介して受信する受信装置と、この受信装置で受信した運転停止信号によって作動するリレーとを設け、このリレーの作動により上記スタータモータ回路及びロック制御回路をそれぞれ遮断するように構成したことを特徴としている（請求項1の記載を引用）。より具体的には、ガバナと油圧回路を制御対象としており、その制御にはソレノイド、つまり電磁リレー（電磁コイルを利用して機械的に接点を開閉するタイプ）を採用している。

【特許文献1】特許第3597772号公報

【0008】

この従来技術によれば、バッテリー直結によりエンジンを始動させることができたとしてもレバーロックソレノイドは励磁されないため、結果として建機の圧油操作を不可能にして建機自体の不正使用を防止することができる。また、人工衛星を利用した盗難防止システムにより建機が盗難に遭ったことが判明した時点で運転停止信号を送信すれば、エンジンの始動を不可能にすることができる。

【発明の開示】

【発明が解決しようとする課題】

【0009】

しかしながら、この従来技術は、スタータモータの不正始動を防止するための根本的な解決策を提案するものではなく、バッテリー直結の不正な手口を使えばエンジンそのものは始動できてしまう、という問題がある。加えて、そのシステム構成のうち、エンジンソレノイド、レバーロックソレノイド、リレー制御部により制御されるリレーでそれぞれ使用されているのは電磁リレーであり、且つ、それらリレーを含めた回路間配線については外観上必ずしも隠蔽される構成にはなっていない。このため、その制御部となるリレーの存在が外部から認識されてしまい、制御回路配線の短絡等の操作を行うことによる不正使用を防止することができない。

【0010】

したがって、本発明の課題は、根本的にスタータモータそのものの不正始動を防止し、且つ、その制御部や回路配線を隠蔽することができ、これによってバッテリー直結による盗難を事実上防止することができる新規なシステムを提供することにある。

【課題を解決するための手段】

【0011】

この課題を解決するため、請求項1に係る発明は、車両を運転するオペレータが所持する鍵手段と、車両に設置される第一の制御部と、車両のエンジンを始動させるためのスタータモータのマグネチックスイッチに内蔵される第二の制御部とからなり、第一の制御部は、鍵手段に記憶された特定の認証データに一意に対応付けられた認証データを記憶する第一の記憶手段と、鍵手段が挿入されたときに鍵手段に記憶された認証データと第一の記憶手段に記憶された認証データとを照合して鍵手段が正規のものであるか否かを判定する認証手段と、挿入された鍵手段が正規のものであると認証手段により判定されたときに稼動許可信号を送出する送信手段とを備え、第二の制御部は、第一の制御部の送信手段から稼動許可信号を受信する受信手段と、スタータモータを始動するための電流を通電又は遮断するモータ制御スイッチと、受信手段が稼動許可信号を受信したときにモータ制御スイッチをオンにしてスタータモータの始動を許容する始動制御手段とを備え、第一の制御部の送信手段から第二の制御部の受信手段に送信される稼動許可信号の伝送媒体として車両の車体が利用され、鍵手段に記憶される認証データは、任意桁数の数字列よりなる認証番号と、この認証番号の各桁の数字を送信してからその一つ下位の桁の数字を送信するまでの送信時間としてランダムに設定された送信時間タイミングデータとの組合せを有し、第一の制御部の第一の記憶手段に記憶される認証データが、鍵手段に記憶される認証データの認証番号と一意に対応付けられた同桁数の数字列を含む認証番号と、鍵手段に記憶される送信時間タイミングデータと一意に対応付けられた受信時間タイミングデータとの組合せを有することを特徴とするエンジン始動制御システムである。

【0013】

10

20

30

40

50

請求項 2 に係る発明は、請求項 1 記載のエンジン始動制御システムにおいて、第一の制御部は、さらに、外部管理サーバとの間でデータ送受信を可能にするためのデータ通信手段と、データ通信手段を通じて外部管理サーバから認証データ変更指令を受信したときに第一のメモリに記憶されている認証データを変更する認証データ変更手段とを備えることを特徴とする。

【 0 0 1 4 】

請求項 3 に係る発明は、請求項 2 記載のエンジン始動制御システムにおいて、エンジンのガバナに設けられた第三の制御部をさらに備え、第三の制御部は、第一の制御部の送信手段から稼動許可信号を受信する受信手段と、受信手段が稼動許可信号を受信しなくなったときにエンジンへの燃料供給を停止させるガバナ制御手段とを備えることを特徴とする。

10

【 0 0 1 5 】

請求項 4 に係る発明は、請求項 1 乃至 3 のいずれか記載のエンジン始動制御システムにおいて、第一の制御部は、車両を特定する車両 ID を記憶する第二の記憶手段をさらに備えるとともに、第二の制御部は、第一の制御部の第二の記憶手段に記憶された車両 ID と一意に対応付けられた車両 ID を記憶する第三の記憶手段と、第一の制御部の第二の記憶手段に記憶された車両 ID と第三の記憶手段に記憶された車両 ID とを照合して受信手段で受信した稼動許可信号が当該車両の第一の制御部から発信されたものであるか否かを判定する車両判定手段とをさらに備え、始動制御手段は、受信した稼動許可信号が当該車両からのものであることが車両判定手段によって判定されたことを条件としてモータ制御スイッチをオンにすることを特徴とする。

20

【 0 0 1 7 】

請求項 5 に係る発明は、請求項 4 記載のエンジン始動制御システムにおいて、第一の制御部の第二の記憶手段に記憶される車両 ID が、任意桁数の数字列よりなる認証番号と、この認証番号の各桁の数字を送信してからその一つ下位の桁の数字を送信するまでの送信時間としてランダムに設定された送信時間タイミングデータとの組合せを有し、第二の制御部の第三の記憶手段に記憶される車両 ID が、第一の制御部の第二の記憶手段に記憶される車両 ID の認証番号と一意に対応付けられた同桁数の数字列を含む認証番号と、第一の制御部の第一の記憶手段に記憶される送信時間タイミングデータと一意に対応付けられた受信時間タイミングデータとの組合せを有することを特徴とする。

【 0 0 1 8 】

請求項 6 に係る発明は、車両に設置され、一定の条件が満たされたときに稼動許可信号を送出する第一の制御部と、車両のエンジンを始動させるためのスタータモータのマグネットスイッチに内蔵され、スタータモータを始動するための電流を通電又は遮断するモータ制御スイッチと、第一の制御部から稼動許可信号を受信したときにモータ制御スイッチをオンにしてスタータモータの始動を許容する始動制御手段とを備える第二の制御部とを備え、第一の制御部の送信手段から第二の制御部の受信手段に送信される稼動許可信号の送信媒体として車両の車体が利用され、第一の制御部は、車両を特定する車両 ID を記憶する第一の記憶手段を備えるとともに、第二の制御部は、第一の記憶手段に記憶された車両 ID と一意に対応付けられた車両 ID を記憶する第二の記憶手段と、第一の記憶手段に記憶された車両 ID と第二の記憶手段に記憶された車両 ID とを照合して受信した稼動許可信号が当該車両の第一の制御部から発信されたものであるか否かを判定する車両判定手段とを備え、始動制御手段は、受信した稼動許可信号が当該車両からのものであることが車両判定手段によって判定されたことを条件としてモータ制御スイッチをオンにし、且つ、第一の制御部の第一の記憶手段に記憶される車両 ID は、任意桁数の数字列よりなる認証番号と、この認証番号の各桁の数字を送信してからその一つ下位の桁の数字を送信するまでの送信時間としてランダムに設定された送信時間タイミングデータとの組合せを有し、第二の制御部の第二の記憶手段に記憶される車両 ID は、第一の制御部の第一の記憶手段に記憶される車両 ID の認証番号と一意に対応付けられた同桁数の数字列を含む認証番号と、第一の制御部の第一の記憶手段に記憶される送信時間タイミングデータと一意に対応付けられた受信時間タイミングデータとの組合せを有することを特徴とするエンジン始動

30

40

50

制御システムである。

【発明の効果】

【0022】

請求項1に係る発明によれば、車両を運転するオペレータが所持する鍵手段に記憶される認証データと一意に対応付けられた認証データが車両に設置される第一の制御部に記憶されており、これらの認証データを照合して鍵手段が正規なものであるか否かを認証手段で判定し、正規のものであると判定したときに第二の制御部に稼動許可信号を与え、この稼動許可信号を第二の制御部が受信しない限りモータ制御スイッチがオンにならず、スタータモータの始動が許容されない構成となっているため、従来から車両盗難の手口となっているバッテリー直結によっても、エンジンが始動されてしまうことがない。また、第二の制御部は、短時間内に破壊することがきわめて困難であるスタータモータのマグネチックスイッチに内蔵されている。したがって、バッテリー直結によるエンジンの不正始動及びそれによる車両盗難に対する有効な防止策となる。さらに、車体を信号伝達手段として用いることから制御用の回路配線や端子を設ける必要が無く、隠匿性の高いシステム構成となり、車両盗難のリスクをさらに減少させることができる。さらに、鍵手段及び第一の制御部に一意に対応付けて記憶される認証データが、任意桁数の数字列よりなる任意の認証番号と、この認証番号の送受信時間としてランダムに設定された送受信タイミングデータとの組み合わせとして構成されるので、短時間で解析することが不可能であり、盗難防止効果をより高めることができる。

10

【0024】

請求項2に係る発明によれば、上記効果に加えて、第一の制御部が記憶する認証データを外部管理サーバからの変更指令によって変更することができるので、正規の鍵手段を所持する者による盗難や不正使用が発覚したときに第一の制御部が記憶する認証データを変更することによって鍵手段が記憶する認証データとの対応性を解除し、第二の制御部に対して稼動許可信号を与えないようにすることができる。

20

【0025】

請求項3に係る発明によれば、上記効果に加えて、エンジンのガバナに第三の制御部を設けて、第一の制御部から稼動許可信号を受信しなくなったときにエンジンへの燃料供給を停止させることとしているので、正規の鍵手段を所持する者による盗難や不正使用が発覚した場合に第一の制御部に記憶される認証データが鍵手段に記憶される認証データと対応しなくなったときに、直ちにエンジンを強制停止させることができる。

30

【0026】

請求項4に係る発明によれば、上記効果に加えて、車両を特定する車両IDが第一の制御部に記憶されるとともに、これと一意に対応付けられた車両IDが第二の制御部に記憶され、それらを照合することによって稼動を許可すべき車両が特定されるので、このシステムによって管理される車両が複数台近接した場所に位置している場合であっても、ある車両からの稼動許可信号によって他の車両に稼動許可が与えられることが無く、適切な車両管理が可能となる。

【0028】

請求項5に係る発明によれば、上記効果に加えて、第一の制御部及び第二の制御部に一意に対応付けて記憶される車両IDが、任意桁数の数字列よりなる任意の認証番号と、この認証番号の送受信時間としてランダムに設定された送受信タイミングデータとの組み合わせとして構成されるので、短時間で解析することが不可能であり、盗難防止効果をより高めることができる。

40

【0029】

請求項6に係る発明によれば、第二の制御部が稼動許可信号を受信しない限りモータ制御スイッチがオンにならず、スタータモータの始動が許容されない構成となっているため、従来から車両盗難の手口となっているバッテリー直結によっても、エンジンが始動されてしまうことがない。また、第二の制御部は、短時間内に破壊することがきわめて困難であるスタータモータのマグネチックスイッチに内蔵されている。したがって、バッテリー直結に

50

よるエンジンの不正始動及びそれによる車両盗難に対する有効な防止策となる。さらに、車体を信号伝達手段として用いることから制御用の回路配線や端子を設ける必要が無く、隠匿性の高いシステム構成となり、車両盗難のリスクをさらに減少させることができる。さらに、車両を特定する車両IDが第一の制御部に記憶されるとともに、これと一意に対応付けられた車両IDが第二の制御部に記憶され、それらを照合することによって稼働を許可すべき車両が特定されるので、このシステムによって管理される車両が複数台近接した場所に位置している場合であっても、ある車両からの稼働許可信号によって他の車両に稼働許可が与えられることが無く、適切な車両管理が可能となる。さらに、第一の制御部及び第二の制御部に一意に対応付けて記憶される車両IDが、任意桁数の数字列よりなる任意の認証番号と、この認証番号の送受信時間としてランダムに設定された送受信タイミングデータとの組み合わせとして構成されるので、短時間で解析することが不可能であり、盗難防止効果をより高めることができる。

10

【発明を実施するための最良の形態】

【0033】

本発明の好適な一実施形態としての建機管理システムの概略イメージである図1と、該システムの概略構成図である図2と、該システムの各手段又は処理で扱うデータを表にした図3とを参照して、以下詳述する。

【0034】

(システム構成の概要)

本システムは、大別して概略説明すると、

20

建機操縦席に設置され、オペレータが持つ後記の稼働許可認証キー20を使って正しい稼働許可番号か否かを判別する稼働許可認証手段を持ち、正しい稼働許可番号と判定した場合は後記のロック制御手段30に対して建機のロック解除指示(稼働許可信号)を発信する制御PC10と、

オペレータが制御PC10に挿入することで、制御PC10の稼働許可認証手段に対して稼働許可番号送信を行う稼働許可認証キー20(以後、メモリキーと呼ぶ)と、

建機130のスタータモータ400に付設されるマグネチックスイッチ300内に設置され、制御PC10から正当なロック解除指示を受信した場合は建機のロック解除を行うロック制御手段30(以後、SSSRと呼ぶ)と、

建機管理会社(または建機所有会社)に設置され、建機の制御PC10とのデータ通信によって、建機の位置・高度や稼働状況データ等を取得して管理し、制御PC10の稼働許可認証手段の認証用データ(錠側)の更新指示、あるいは制御PC10に建機の強制停止指示を発信することができる管理PC110と、

30

建機貸出先などの建機現場事務所に設置され、貸し出された建機の制御PC10の稼働許可認証手段の認証用データ(鍵側)をメモリキー20に書き込むクライアントPC120と、

制御PC10、メモリキー20、SSSR30が保持する認証用データをすべて一括管理し、その認証用データを管理PC110とクライアントPC120にインターネット等の通信ネットワークを経由して配布する管理センター100と、

40

から構成される。

【0035】

なお、稼働許可認証キー20としてUSB等の標準規格のポートに接続して使用する持ち歩き可能なメモリを使用するので、本システムではメモリキーと呼ぶ(ただし、メモリだけでなく制御・演算手段も含む)。また、ロック制御手段30には既知のソリッドステートリレー(Solid State Relay = SSR)を盗難防止用に新規に改良したものを使用しており、本システムではSecure SSRと呼んでいる。SSSRとはその略称である。

【0036】

本システムにおいては、建機の管理を行う上で、不正キーによる建機の稼働を防止するための稼働許可認証と、建機のロック解除指示の正当性を判定するためのロック解除指示

50

認証とを行う。

【 0 0 3 7 】

(稼働許可認証)

以下稼働許可認証について詳述する。

【 0 0 3 8 】

まず、稼働許可認証で扱うデータについて述べる。制御 P C 1 0 は稼働許可認証のための稼働許可番号・稼働許可番号受信プログラムのセット(認証データ)をメモリ 1 2 に保持している。これと対になるセット(同一の稼働許可番号と稼働許可番号送信プログラムのセット)がメモリキー 2 0 のメモリ 2 2 に保持されている。制御 P C 1 0 は、そのメモリ 1 2 に保持しているセットと対になるセットをメモリ 2 2 に保持しているメモリキー 2 0 でのみ動作可能になる。メモリキー 2 0 は、後述のように、制御 P C 1 0 の U S B 等の標準規格のポートに差し込むことによって制御 P C 1 0 から駆動電源を得て動作するものであり、市販の U S B メモリースティックとポートコネクタのみ同様の形状であって良いが、稼働許可番号及び稼働許可送信プログラムを格納する、本システムに独自の構成を有している。なお、制御 P C 1 0 のメモリ 1 2 及びメモリキー 2 0 のメモリ 2 2 に保持されたデータは、容易にコピー及びリバースエンジニアリングされないように防止機能が付けられている。

10

【 0 0 3 9 】

稼働許可認証の方式としては既知のものから任意に選択して使用することができ、特に暗証番号(稼働許可番号、数字列が一般であるが文字列であっても良い)を用いた方式を採用することができるが、本システムでは、新たに考案した認証方式として、暗証番号送信/受信プログラムが、暗証番号(稼働許可番号)だけではなく暗証番号を順に送信/受信する際のタイミングの取り方も認証の対象にしている認証方式を採用している。そのタイミングの取り方については、暗証番号の数字を一つ送信/受信した後に任意の時間間隔をおいて次の一つを送信/受信するようにしている。たとえば、送信時間間隔は、1つ目の数字を送信した後は 0 . 5 秒、2つ目の数字の後には 0 . 3 秒、3つ目の数字の後には 1 . 0 秒、. . . というようにランダムに設定され、受信時間間隔もこれと同様にする。この時間間隔は暗証番号送信/受信プログラム内に埋め込んでいる。また、1つ目の数字が送信されると同時に受信も開始し始めることで、送信と受信の開始のタイミングをとる。送信と受信のタイミングが一致し、且つ暗証番号も一致した場合のみ、認証の結果が正当なものと判定される方式であり、これを暗証番号送受信同期認証方式と呼ぶ。

20

30

【 0 0 4 0 】

この暗証番号送受信同期認証方式が採用された建機 1 3 0 を盗難するためには、特定の暗証番号とランダムに設定された時間間隔データの両方を取得しなければならない。仮にメモリキー 2 0 を不正取得した第三者にそのメモリ 2 2 に内蔵される暗証番号を知られたとしても、ランダムに設定された送信時間タイミングを解析するには長時間を要する。逆に、悪意ある者が送信時間タイミングを一致させることに成功したとしても、暗証番号を網羅して開錠を確認するためには多大な時間を要する。一例として、6桁の暗証番号(100万通りの組合せがある)において送信時間間隔を3秒程度としてすべての送受信タイミングを一致させることができたとしても、暗証番号全てを試すためには概ね一ヶ月を要することになる。すなわち、なるべく短時間内に盗難を完了させようとする盗難者側の心理を考えると、この暗証番号送受信同期認証方式は、きわめて有効な盗難防止策となる。

40

【 0 0 4 1 】

次に、稼働許可認証の手順について述べる。オペレータがメモリキー 2 0 を制御 P C 1 0 の U S B 等の標準規格のポートに差し込むと、制御 P C 1 0 からの電源供給を受けたメモリキー 2 0 の制御・演算手段 2 1 が起動してメモリ 2 2 内の稼働許可番号送信プログラムによって制御 P C 1 0 に稼働許可番号を送信し始める。同時に、制御 P C 1 0 の制御・演算手段 1 1 は、メモリ 1 2 内の稼働許可番号受信プログラムによって稼働許可認証を開始し、同プログラム内で定められた受信時間間隔で受信した番号をメモリ 1 2 内の稼働許可番号と比較してすべて一致した場合に(既述の暗証番号送受信同期認証方式のとおり)

50

、正しい稼働許可番号と判定する。

【 0 0 4 2 】

ここで、稼働許可認証データの管理について述べる。稼働許可認証データである制御 P C 1 0 の稼働許可番号・稼働許可番号受信プログラムとメモリキー 2 0 の稼働許可番号・稼働許可番号送信プログラムとのセットは、セット毎に一意なものでなければならない。つまり、稼働許可認証データは、建機 1 3 0 の操縦席等に設置される制御 P C 1 0 毎に一意なものが割り振られ、同一の建機管理会社（建機所有会社）が管理（所有）する複数の建機 1 3 0 に設置されるその制御 P C 1 0 には、すべて異なる稼働許可認証用データが組み込まれている。この一意性を保持するため、管理センター 1 0 0 がすべてのセットを一括管理する。

10

【 0 0 4 3 】

本システム運用時に建機貸出先の変更等があれば、その際に稼働許可認証データを書き換える。この書き換え処理について、制御 P C 1 0 側の書き換えとメモリキー 2 0 側の書き換えを順に説明する。

【 0 0 4 4 】

制御 P C 1 0 側（錠側）の書き換えについて述べる。建機管理会社の管理 P C 1 1 0 は、管理センター 1 0 0 に、制御 P C 用の新たな稼働許可認証データ（稼働許可番号か稼働許可受信プログラムかどちらか一方、又はその両方のセット）の発行を依頼して、発行された認証用データへの書き換え指示とその認証用データを建機の制御 P C 1 0 に発信する。制御 P C 1 0 は管理 P C 1 1 0 からデータ通信手段 1 4（たとえばデータ送受信可能な携帯電話機）を介して認証用データの書き換え指示とその認証用データを受信し、メモリ 1 2 の認証用データを書き換える。

20

【 0 0 4 5 】

メモリキー 2 0 側（鍵側）の書き換えについて述べる。建機貸出先のクライアント P C 1 2 0 は、管理センター 1 0 0 に接続して、前記の新たな稼働許可認証データである稼働許可番号・稼働許可番号送信プログラムをダウンロードして、そのクライアント P C 1 2 0 に挿入されたメモリキー 2 0 に書き込む（管理センター 1 0 0 から提供されるメモリキー 2 0 への書き込み専用プログラムを使って書き込む）。

【 0 0 4 6 】

なお、以上述べたように管理 P C 1 1 0 により建機の制御 P C 1 0 の稼働許可認証データを遠隔地から書き換えることができることを利用して、（後述の建機稼働状況管理手段等により）オペレータが建機を不正使用していることが判明した場合には、そのオペレータが持つメモリキー 2 0 の稼働許可認証データでは正しい稼働許可番号と判定できないように制御 P C 1 0 の稼働許可認証データを書き換えることにより、不正使用を阻止することが可能になる。また、稼働許可認証データのメモリキー 2 0 への書き込みを建機貸出先のクライアント P C 1 2 0 で行う構成により、たとえば建機管理会社は日本にあり、建機貸出先は海外である場合にも容易に管理可能である。

30

【 0 0 4 7 】

（ロック解除指示認証）

以下ロック解除指示認証について詳述する。

40

【 0 0 4 8 】

まず、ロック解除指示認証で扱うデータ（ロック解除指示認証データ）について述べる。S S S R 3 0 はロック解除指示認証のための認証データとなる車両 I D ・車両 I D 受信プログラムのセットをメモリ 3 2 に保持している。これと同一のロック解除指示認証データである車両 I D ・車両 I D 受信プログラムのセットが制御 P C 1 0 のメモリ 1 2 に保持されている。S S S R 3 0 は、そのメモリ 3 2 に保持しているセットと対になる（同一の）セットをメモリ 1 2 に保持している制御 P C 1 0 でのみ制御可能になる。制御 P C 1 0 と S S S R 3 0 はセットで建機に設置されるので、出荷前にメモリ 1 2 /メモリ 3 2 に車両 I D ・車両 I D 送信 / 受信プログラムを設定しておき、通常はこのままで固定され、後に変更されることはない。

50

【 0 0 4 9 】

ロック解除指示認証方式は任意であるが、本システムでは、稼働許可認証方式として採用したと略同様の暗証番号送受信同期認証方式を採用している。しかし、稼働許可認証における暗証番号である稼働許可番号はP Cの標準ポート経由で送信しているのに対して、ロック解除指示認証における暗証番号である車両I Dの送信にはP L C (Power Line Communication)を採用しており、その伝送媒体として電源のマイナスラインである車体4 0を使用している。P L Cとは一般的には電力線を使用して行われるデータ通信のことである。本システムでは、このP L C技術をリレーの制御に利用して、国内法で許容される規定のキャリア信号(このキャリア信号のみでS S S R 3 0のP L C信号受信手段3 3に対してオン信号を送信したことになる)に車両I Dの信号をミックス(畳重)して、S S S R 3 0へ車両I Dの送信を行う。

10

【 0 0 5 0 】

また、P L Cにおいて伝送媒体として車体4 0を利用しているため、S S S R 3 0の制御用配線の隠匿を可能にし、配線の短絡(バッテリー直結)等、一般的な手口となっている制御用配線を操作して不正動作させることによる盗難の防止に大きく貢献している(S e c u r e S S Rという名称を採用したのはこの所以である)。

【 0 0 5 1 】

この盗難防止効果をもたらすS S S R 3 0の制御用配線の隠匿性について補足説明する。図4 (A)に示すように通常のリレーでは制御端子部分(制御入力端子、制御出力端子)がその外観上ははっきりした形でリレ - 外部に出ているため、その制御端子部分を操作して回路製作者(装置製作者)が意図する動作と異なる不正動作させることが容易に可能である。この問題を解決するため、本発明ではP L C技術をリレーの制御に応用し、且つ、稼働許可信号の伝送媒体としてマイナスラインである車体4 0及びS S S R 3 0の金属製のケースを利用して、この金属ケースを介して入力した稼働許可信号をP L C信号受信手段で受信するようにしている(図4 (B)、図4 (C))。これにより、外観上制御端子は存在しない構成になっており、結果としてリレーの制御用配線の隠匿を可能にしているため、悪意をもって制御用回路を不正動作させることは困難である。加えて、プラスラインのノイズを避けることができるという利点も有している。図4 (C)は本システムのS S S R 3 0に対応しており、P L C信号受信手段3 3からキャリア信号に加えて車両I Dの信号も受信し、メモリ3 2内の車両I D・車両I D受信プログラム制御のデータを利用して制御・演算手段3 1でロック解除指示認証とモータ制御スイッチ3 4の制御を行う構成になっている。この構成では稼働許可信号としてキャリア信号に車両I Dを畳重したP L C信号を用いており、後述するように、ある建機に設置した本システムの制御P C 1 0から発信されたキャリア信号が他の建機に伝播して該他の建機をロック解除してしまうといった事態を防止することができるので好ましい実施形態であるが、図4 (B)のようにS S S R 3 0 'を構成することも本発明の範囲内である。このS S S R 3 0 'では、P L C信号受信手段3 3が稼働許可信号(キャリア信号のみ)を受信したときに制御手段3 1 '(本システムのS S S R 3 0における制御・演算手段3 1に相当し、同様の制御を行うもの)がロック解除指示認証を与える構成であり、車両I Dによる制御対象建機の特定制を行わないことを除いて、本システムのS S S R 3 0と同様の構成を有し同様に動作する。

20

30

40

【 0 0 5 2 】

S S S R 3 0は、制御用配線の隠匿性によって上記の利点を発揮することに加えて、マグネチックスイッチ3 0 0の内部に設置されるため、その存在を外部から確認することができず、S S S R 3 0そのものの隠匿性もきわめて高い。しかも、マグネチックスイッチ3 0 0内部を確認するためには、旋盤等の大掛かりな装置を用いてマグネチックスイッチ3 0 0を破壊しなければならず、少なくとも数時間を要する。このことは、犯罪者心理を考慮すれば、悪意を持った者によってS S S R 3 0の制御端子部分が不正動作されるリスクを実質的に回避できることを意味している。

【 0 0 5 3 】

50

さらに、ロック解除指示認証の手順について述べる。既述した稼動許可認証で正しい稼動許可番号と判定した後に、このロック解除指示認証に移行する。制御PC10の制御・演算手段11は、メモリ12内の車両ID送信プログラムによって車両IDをPLC信号送信手段13から送信し始める。同時に、PLC信号受信手段33を経由して信号を受けたSSSR30の制御・演算手段31は、メモリ32内の車両ID受信プログラムによってロック解除指示認証を開始し、同プログラム内で定められた受信時間間隔でPLC信号受信手段33から受信した番号をメモリ32内の車両IDと比較してすべて一致した場合に（既述の暗証番号送受信同期認証方式のとおり）正しい車両IDと判定し、モータ制御スイッチ34に指示を出し、建機のロック解除を行う。

【0054】

なお、稼動許可信号として車両IDを使わずにオン信号（キャリア信号）のみを送信するシステム構成も可能である（図4（B））が、複数の建機を同じ作業現場で稼動させる場合、本システムでは車体40がアンテナの役割を果たして他の建機にまで稼動許可信号が伝搬する可能性があり、結果として意図せずに他の建機にもロック解除指示を送信してしまう事態が考えられる。この事態を避けるため、つまりセットとなった制御PC10とSSSR30との間でのみロック解除を成立させるため、ロック解除指示の発信元を識別する車両IDを使うことが望ましい。

【0055】

（建機状況の取得）

本システムは、さらに建機状況を取得するための手段として、日付・時刻取得手段1、位置・高度取得手段2、傾斜センサ3及びエンジン稼動情報取得手段4を備えている。日付・時刻取得手段1としては電波時計やGPS（Global Positioning System）を利用することができる。位置・高度取得手段2としてはGPSその他の位置情報取得手段を利用することができる。傾斜センサ3は各建機130に設置され、水平に対する建機の傾斜角度を取得する。エンジン稼動情報手段4は建機130のエンジンが運転中であるか否かを判定するための情報として水温・油温等を取得する。これらの手段で取得したデータは定期的に、又は制御PC10からの指示に応じて制御PC10に送信され、受信した制御PC10においてメモリ12に保持される。

【0056】

（建機稼動条件の設定）

建機管理会社が管理する建機130を建機貸出先に対して建機稼動を許可する際には、通常、許可する稼動期間と稼動範囲を設定する。これら稼動期間及び稼動範囲等の建機稼動条件は、管理PC110によりデータ通信手段14を介して制御PC10に送信され、メモリ12に保持される。

【0057】

（建機稼動の許可・不許可）

制御PC10の制御・演算手段11は、前記建機状況取得手段、特に日付・時刻取得手段1及び位置・高度取得手段2から送信されたデータを、メモリ12に保持された上記建機稼動条件（稼動期間、稼動範囲等）と比較して稼動許可判定を行う。稼動条件内であると判定した場合には建機稼動を許可し（他の処理手段に影響を与えない）、稼動条件外であると判定した場合には建機稼動を許可しない。制御PCの動作中はこの一連の処理手順（稼動許可判定 判定に従った処理）を定期的に繰り返す。

【0058】

建機がまだ稼動していない状態で建機稼動を不許可とする判定がなされたときは、メモリキー20から暗証番号及び時間間隔のデータが送信されてきても既述の稼動許可認証処理に移行しないことで建機稼動を許可しないようにする。

【0059】

建機が稼動中に建機稼動を不許可とする判定がなされたとき、すなわち稼動を即時中止させるべき場合の処理について以下詳述する。

【0060】

10

20

30

40

50

まず、建機の動作の仕組みを述べる。建機のエンジンは油圧を作り出すための装置であり、その油圧を利用して、キャタピラ等で建機を走行（油圧 羽車を回転 キャタピラ回転）させたり、各種アタッチメントの動作（バケット操作等）をさせたりしている。建機は、自動車のようにエンジンからギヤ等で動力を直接稼働部分に伝導する仕組みではない。建機のエンジン回転を油圧に変換し、油圧を稼働各部に伝導し動作に変換する仕組みである。したがって、建機稼働が外部要因により強制停止しても、それによってエンジンが停止することはない。

【 0 0 6 1 】

建機エンジンの不正動作の阻止は、建機エンジン稼働前であれば、既述のロック制御手段 3 0 によるロック制御指示認証を介して、スタータモータ 4 0 0 を直接制御することで
10
行うことができる。エンジンが始動しなければ油圧が発生せず、建機の稼働は不可能である。しかし、上記の建機の動作の仕組みにより、建機稼働中、つまりエンジンが一旦始動した後に建機を強制停止させるためにはエンジンを直接停止させる必要がある。

【 0 0 6 2 】

本システムではエンジンを直接停止させる方法として、エンジン燃料供給部のガバナ（エンジンに供給される燃料を開閉する電磁弁）を、前記 S S S R 3 0 と同じ構成及び動作原理を持つガバナ用 S S S R（図示せず）で電子制御する方法を採用している。ガバナ用 S S S R は、S S S R 3 0 のロック解除指示認証と同様のエンジン稼働許可認証を行い、
20
そのための認証データも S S S R 3 0 のロック解除指示認証データと同じものでよい。つまり、制御 P C 1 0 の制御・演算手段 1 1 で稼働認証許可を判定したときに、キャリア信号が制御 P C 1 0 の P L C 信号送信手段 1 3 からマグネットスイッチ 3 0 0 の S S S R 3 0 とガバナ用 S S S R の両方に送信され、その後キャリア信号を継続して送信し続けることでエンジンは動作し続ける。

【 0 0 6 3 】

したがって、以上の建機の動作原理とガバナ用 S S S R の設置により、建機の稼働を中止する方法、つまりエンジンを直接停止させる方法は、制御 P C 1 0 の P L C 信号送信手段 1 3 のガバナ用 S S S R に対する稼働許可信号送信をストップさせるものである。これによって建機を強制停止させることができる。正規のメモリキ - 2 0 により制御 P C 1 0 を動作させエンジンを始動させた後に不正使用を目的として制御 P C 1 0 を取り外した場合を想定すると、ガバナ用 S S S R を設置していない場合はエンジンを停止することが
30
できないためにそのまま不正使用し続けられるが、ガバナ用 S S S R を設置している場合は制御 P C 1 0 を取り外したことにより P L C 信号送信手段 1 3 の稼働許可信号送信がストップするので建機を稼働できなくなる。つまり、ガバナ用 S S S R の設置は、エンジンを一旦始動させた後の制御 P C 1 0 取り外し行為による盗難を阻止できる、という利点がある。

【 0 0 6 4 】

また、正規のメモリキ - 2 0 が挿入された場合には稼働許可信号がマグネチックスイッチ 3 0 0 の S S S R 3 0 に送られてスタータモータ 4 0 0 及びエンジンの始動を許容するが、その後、後述のキャリアカー不正積載のような不正使用が発覚したときにも、上記と同様にして、エンジンを強制停止することができる。すなわち、この場合、管理 P C 1 1
40
0 から携帯電話機等のデータ通信手段 1 4 を介して制御 P C 1 0 に稼働許可認証データ変更指令を送ることにより、メモリ 1 2 内に記憶されている稼働許可認証データを変更又はクリアすると、制御 P C 1 0 の制御・演算手段 1 1 は稼働許可認証データの不一致により稼働許可を与えないので、ガバナ用 S S S R に対するキャリア信号がストップし、エンジンを強制停止する。

【 0 0 6 5 】

（建機状況の管理）

制御 P C 1 0 の建機状況取得手段によるデータ等を、携帯電話機等のデータ通信手段 1 4 を介して管理 P C 1 1 0 がリアルタイムに取得して管理する。管理 P C 1 1 0 は取得した建機状況を建機管理会社の管理者に報知する。管理者は、受領したデータを元に建機稼
50

動状況の把握が可能になり、たとえばエンジンの水温・油温が異常に高い状態が続いた場合には建機貸出先などの現場事務所に注意を促すことが可能になる。

【 0 0 6 6 】

(盗難防止のメカニズム)

建機の盗難には幾つかのパターンが想定されるが、大別すると、正規の稼働許可認証キー（メモリキー 20）を持たない第三者がバッテリー直結等によってエンジンを不正始動させて盗難しようとするいわゆる外部犯行のパターンと、建機管理会社の従業員等の関係者が所有する正規の稼働許可認証キーを用いて関係者自らが、又は関係者から譲り受けた正規の稼働許可認証キーを用いて悪意のある外部の人間が建機を正常な手段で稼働させて盗難しようとするいわゆる内部犯行のパターンがある。

10

【 0 0 6 7 】

外部犯行の盗難パターンに対しては、既述した稼働許可認証が有効な防止策となる。すなわち、マグネチックスイッチ 300 にロック制御手段（SSSR）30 が内蔵されている本システム（図 5 参照）によれば、万一バッテリー直結によりマグネチックスイッチ 300 の S 端子にバッテリーからの電流が流れたとしても、稼働許可認証が成立した場合にのみ制御 PC 10 から送られる稼働許可信号を受信しない限りモータ制御スイッチ 34 がオンになることがなく、マグネチックスイッチ 300 のシリーズコイル 303 及びシャントコイル 304 には電流が流れないのでプランジャ 305 を吸引するための電磁力が発生せず、したがってピニオンギヤ 404 が回転しないのでエンジンを始動させることはない。

20

【 0 0 6 8 】

しかしながら、この稼働許可認証による盗難防止策は、正規のキーを使用する内部犯行の盗難パターンに対しては有効ではない。本システムは、内部犯行の盗難パターンに対する対応策も備えている。この防止策は、外部犯行の盗難パターンに対しても二次的又は補完的な対応策として機能する。

【 0 0 6 9 】

この対応策は、建機がキャリアカーに不正積載されたことを検知した場合や建機稼働条件（稼働期間、稼働地域等）を満たさない不正使用を検知した場合等、盗難又は不正使用の可能性ありと判定したときに、メモリ 12 に記憶されている建機特定のためのデータ（稼働許可番号や車両 ID 等）と位置データをデータ通信手段 14 を介して管理 PC 110 に送信する。通報を受けた建機管理会社は、位置データに基づいて把握した建機の現在位置に急行して盗難を未然に防止し、又は不正使用を停止させることができる。また、盗難や不正使用の可能性を判定したとき、制御・演算手段 11 はメモリ 12 内の稼働許可認証データ（認証番号、受信時間間隔、受信プログラムの少なくともいずれか一つ）を変更又はクリアする。あるいは、不正積載の通報を受けた管理 PC 110 からの指令を受けてメモリ 12 内の稼働許可認証データを変更又はクリアするようにしてもよい。これにより、オペレータがメモリキー 20 を制御 PC 10 に挿入しても、既述した稼働許可認証処理において建機の稼働が許可されないため、建機の再始動はできなくなり、建機の不正使用を阻止することができる。また、不正積載された建機をキャリアカーから降ろすためにスタータモータ 400 を始動させることもできなくなるため、盗難防止にも有効である。

30

【 図面の簡単な説明 】

40

【 0 0 7 0 】

【 図 1 】 本発明の好適な一実施形態としての建機管理システムの概略ブロック図である。

【 図 2 】 このシステムの概略構成図である。

【 図 3 】 このシステムの各手段又は処理で扱うデータを表にしたものである。

【 図 4 】 このシステムにおける制御用配線の隠匿性（C）を通常のリレー（A）及び PLC 原理を単純に応用したもの（B）と対比して示す説明図である。

【 図 5 】 このシステムによるスタータモータの作動原理を説明する図である。

【 図 6 】 従来技術によるスタータモータの作動原理を説明する図である。

【 符号の説明 】

【 0 0 7 1 】

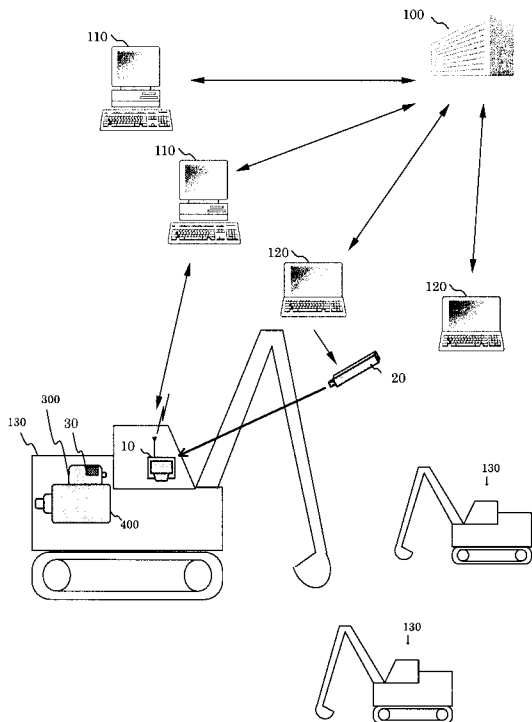
50

- 1 日付・時刻取得手段
- 2 位置・高度取得手段
- 3 傾斜センサ
- 4 エンジン稼動情報取得手段
- 10 制御PC
- 11 制御・演算手段
- 12 メモリ
- 13 PLC信号送信手段
- 14 データ通信手段
- 20 稼動許可認証キー(メモリキー)
- 21 制御・演算手段
- 22 メモリ
- 30 ロック制御手段(SSSR)
- 31 制御・演算手段
- 32 メモリ
- 33 PLC信号受信手段
- 34 モータ制御スイッチ
- 40 車体
- 100 管理センター
- 110 管理PC
- 120 クライアントPC
- 130 建機
- 200 スタータスイッチ
- 300 マグネチックスイッチ
- 400 スタータモータ

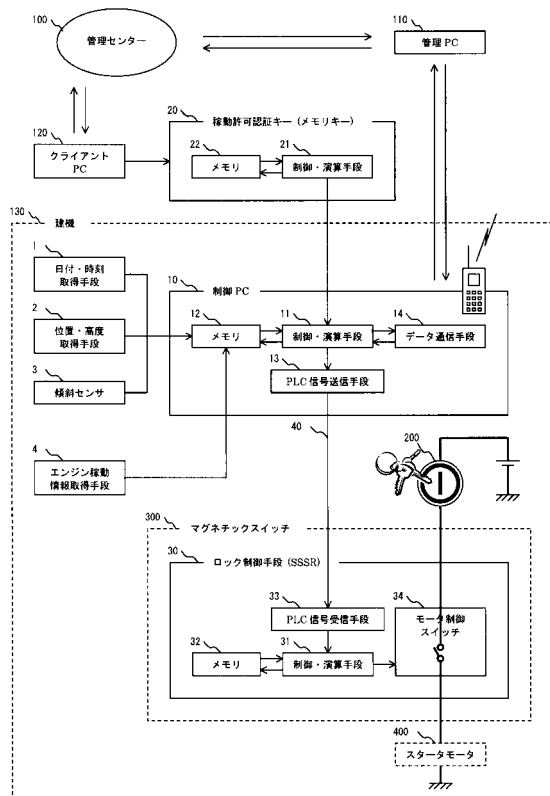
10

20

【図1】



【図2】

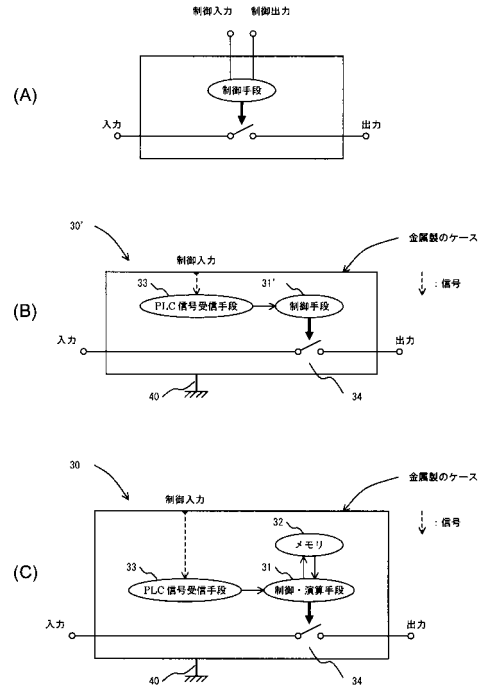


【 図 3 】

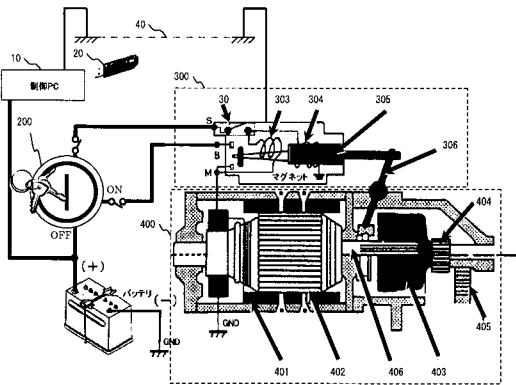
大項目	小項目	管理センター	管理PC	メモリー	制御PC	SSSR
認証	稼働許可認証	◎		○	○	
	稼働許可番号	◎		○	○	
	稼働許可番号送信プログラム 稼働許可番号受信プログラム	◎				
管理	ロック解除指示認証				●	●
	車両ID	◎			●	●
	車両ID送信プログラム 車両ID受信プログラム	◎				
	稼働状況取得		◎		○	
	白灯・緑灯 位置・高さ 車体の傾斜 エンジン稼働情報	◎ ◎ ◎ ◎			○ ○ ○ ○	
	遠隔稼働条件設定		◎		○	
	稼働期間 稼働位置範囲		◎		○	
	遠隔稼働制限				○	
	強制停止指示 遠隔稼働状況管理 (稼働状況取得時に連する)				○	

◎:すべての建機のデータを一括管理
○:書き換え可能
●:固定

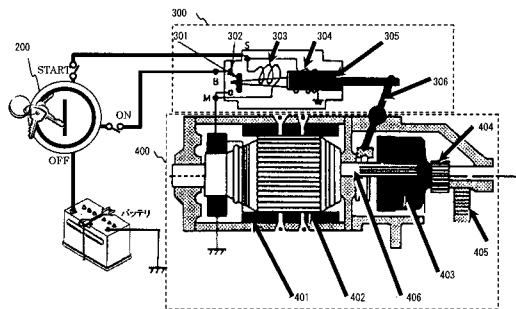
【 図 4 】



【 図 5 】



【 図 6 】



フロントページの続き

- (56)参考文献 特開平07-089355(JP,A)
特開昭64-056250(JP,A)
特開2004-051067(JP,A)
特開2002-186112(JP,A)

- (58)調査した分野(Int.Cl., DB名)
B60R 25/00-25/10