MINISTERO DELLO SVILUPPO ECONOMICO
DIREZIONE GENERALE PER LA TUTELA DELLA PROPRIETA' INDUSTRIALE
UFFICIO ITALIANO BREVETTI E MARCHI

UIBM

DOMANDA NUMERO	**101994900402660**
Data Deposito	**15/11/1994**
Data Pubblicazione	**15/05/1996**

Priorità	9313712
Nazione Priorità	FR
Data Deposito Priorità	

Sezione	Classe	Sottoclasse	Gruppo	Sottogruppo
B	62	D		

Titolo

ELABORATORE DI CONTROLLO DELL'UTILIZZAZIONE DI UN AUTOVEICOLO

D E S C R I Z I O N E

del brevetto per Invenzione Industriale

di Société d'Applications Générales d'Electricité et de Mécanique SAGEM

di nazionalità francese,

a 75783 PARIS Cédex 16 (Francia),

6 avenue d'Iéna

Inventore: BERTHET Patrick

TO 94A000915

* * *

La presente invenzione si riferisce ad un elaboratore di controllo dell'utilizzazione di un autoveicolo comprendente un insieme di organi di funzionamento, tra i quali un motore, comprendente, per la gestione del funzionamento di almeno uno degli organi funzionali, un processore, mezzi di lettura di mezzi di controllo portatili e mezzi, di ricezione di almeno un dato di controllo dei mezzi di controllo, per autorizzare il processore a gestire l'organo considerato.

Il controllo di utilizzazione di un autoveicolo consiste nel verificare che un individuo abbia le qualità giuste per guidarlo. Questa qualità può essere materializzata da una chiave meccanica che permette di sbloccare un dispositivo antifurto, ma questa chiave è facile da imitare.

E' anche conosciuto il mezzo di utilizzo di una

chiave elettronica. In questo caso, una tastiera del cruscotto del veicolo permette all'utilizzatore di inserire un codice confidenziale che, dopo verifica da parte di un circuito elettronico associato alla tastiera, è trasformata in un segnale di controllo che autorizza il funzionamento di un dispositivo di comando di un organo essenziale del veicolo, per esempio un segnale sotto forma di un dato di controllo di un elaboratore che gestisce un dispositivo di accensione delle candele del motore. Oltre alla tastiera, è anche conosciuto il mezzo di prevedere un lettore di scheda a chip, cosa che aumenta la protezione, poichè si deve disporre contemporaneamente del codice e della scheda.

Tuttavia, il dato di controllo è in generale una semplice polarità trasmessa su un filo, in modo che il dispositivo di controllo, formato dal lettore e dalla scheda a chip, è facilmente aggirabile, poichè è sufficiente disinserire il filo in uscita e applicarvi la polarità voluta perchè il calcolatore di gestione dell'organo del veicolo possa funzionare.

La presente invenzione mira a rendere inefficace ogni azione fraudolenta diretta sull'elaboratore di gestione che avrebbe lo scopo di simulare il dato di controllo proveniente da un dispositivo di controllo

di utilizzazione, a chiave elettronica, di un autoveicolo.

A questo scopo, l'invenzione si riferisce ad un elaboratore del tipo appena menzionato, caratterizzato dal fatto che i mezzi di ricezione comprendono mezzi di sbroglio, il processore essendo strutturato per trasmettere almeno un dato di autorizzazione della sua gestione dell'organo da gestire ai mezzi di controllo comprendenti mezzi di imbroglio, i mezzi di ricezione essendo strutturati per disbrogliare il detto dato, precedentemente imbrogliato dai mezzi di controllo, e confrontarlo con il dato trasmesso ai mezzi di controllo per autorizzare la gestione dell'organo gestito.

Viene così formato un circuito comprendente mezzi di controllo portatili, per esempio una scheda a chip e, quando questi non sono quelli previsti, i dati ricevuti in ritorno dall'elaboratore non corrispondono ai dati di risposta attesi, in modo che l'utilizzazione del veicolo è impossibile. In particolare, il disinnesto fraudolento del circuito di ricezione dei mezzi di lettura e il suo innesto con una polarità qualunque non può simulare il dato imbrogliato atteso.

Vantaggiosamente, i mezzi di ricezione

comprendono un generatore di sequenze pseudo-aleatorie.

L'imbroglio e il disimbroglio sono effettuati secondo queste sequenze e una eventuale simulazione di un dato imbrogliato valido è così quasi impossibile, anche in caso di osservazione preliminare, nel corso di utilizzazioni autorizzate, dei dati imbrogliati.

Vantaggiosamente sempre, sono previsti mezzi di memorizzazione di dati di identificazione del calcolatore per essere comparati a dati associati a mezzi di controllo portatili.

Si può così identificare individualmente ciascuno degli elaboratori appartenenti a una medesima sede di fabbricazione e, per esempio, trasmettere i dati di identificazione verso i mezzi di controllo perchè essi li confrontino con questi medesimi dati, immagazzinati localmente, al fine di autorizzare o no un imbroglio corretto dei dati di controllo.

Al fine di aumentare ulteriormente la difficoltà di determinazione, tramite un'osservazione dei dati scambiati, di una chiave di imbroglio che serve al generatore di sequenze pseudo-aleatorie, è preferibile che questo comprenda in ingresso un circuito di inizializzazione strutturato per forzare le uscite del generatore in uno stato determinato.

L'invenzione sarà meglio compresa con l'aiuto della descrizione che segue della forma di realizzazione preferita dell'elaboratore di controllo dell'invenzione, facendo riferimento alla figura unica del disegno annesso che è una rappresentazione per blocchi funzionali.

L'elaboratore di controllo dell'utilizzazione di un autoveicolo, con riferimento 1, è qui alloggiato in una vettura per gestirne organi di funzionamento, e in particolare l'accensione delle candele del motore 40 in questo esempio. Per organo di funzionamento, si deve comprendere qualunque organo necessario al momento dello spostamento della vettura, tipo il motore, lo sterzo, i freni, il cui funzionamento non è corretto o il cui bloccaggio impedisce l'utilizzazione della vettura.

L'elaboratore 1 comprende un processore 2, che assicura la gestione dell'accensione del motore 40 indicata in precedenza, che è collegato ad una memoria 3 che contiene un dato di autorizzazione all'utilizzo della vettura. Un bus 4 collega il processore 2 a un lettore 5 strutturato per ricevere una scheda a chip 30 e scambiare dati con essa. Un bus 6 collega il vettore 5 a un circuito di ricezione 10 del calcolatore 1, una cui uscita fornisce al processore 2

un segnale 11 di autorizzazione di gestione del motore 40. Si comprenderà che i bus 4 e 6 possono essere costituiti da un unico bus bidirezionale.

Il circuito di ricezione 10 comprende un comparatore 12 e un insieme 13 sbrogliatore di dati comprendente un comparatore 14, qui una porta logica OU esclusiva, collegata in uscita al comparatore 12 e collegata in ingresso al bus 6 oltre che ad un'uscita di un generatore 15 di sequenze cicliche pseudo-aleatorie di bits. E' anche previsto qui, un circuito 16 di inizializzazione del generatore 15 per forzarne le uscite in uno stato determinato per un numero proveniente qui dal processore 2. Il generatore 15 è un contatore a grande numero di stadi associato a porte logiche comandate dall'uscita di taluni degli stadi per applicare in allacciamento segnali su ingressi paralleli, di forzatura, di stadi precedenti e così creare un conteggio pseudo-aleatorio. Il circuito di inizializzazione 16 è, per chiarezza di esposizione, stato disegnato separatamente dal generatore 15 ma è in effetti costituito, in questo esempio, dai circuiti di ingresso parallelo, o di forzatura, di ciascuno degli stadi sopra nominati oltre che di un circuito di orologio che comanda l'attivazione di questi circuiti di ingresso

parallelo. Il comparatore 12 è anche collegato in ingresso a un memoria 17 che contiene un terzo dato associato al dato di autorizzazione contenuto nella memoria 3.

Il comparatore 12 è qui un comparatore parallelo, preceduto da un registro tampone serie/parallelo, non rappresentato, per memorizzare i bits generati dal comparatore 14, e seguito da una bilancia che memorizza il segnale 11. Il comparatore 12 potrebbe anche essere un comparatore serie, come una porta logica OU esclusiva, seguita da un registro serie/parallelo di ricezione del risultato della comparazione di ciascuno dei bits del dato sbrogliato, OU esclusivo 12 producendo, in caso di discordanza dei due bits applicati in ingresso, il passaggio temporaneo dalla sua uscita a uno stato di inibizione rilevato in seguito nel registro in uscita per mantenere o far passare il segnale 11 a uno stato che impedisce la gestione del motore 40 da parte del processore 2.

E' previsto, in questo esempio, un insieme 20 di controllo di identità del calcolare 1. L'insieme 20 comprende una memoria morta 21 contenente una parola specifica di codice di identità, particolare per l'elaboratore 1, che è applicata ad un comparatore

22, qui una porta OU esclusiva, collegata in ingresso al bus 6 e la cui uscita è memorizzata in una bilancia 23 che fornisce un segnale 24 di convalida dell'identità.. Il segnale 24 controlla il funzionamento della gestione del motore 40 da parte del processore 2, qui essendo applicato ad un ingresso di bloccaggio del generatore 15.

La scheda a chip 30 comprende un circuito 31 di imbroglio di dati, di struttura simile a quella dello sbrogliatore 13, e una memoria 32 contenente anche la parola specifica della memoria 21.

In un intento di chiarezza, i registri tampone necessari all'emissione e alla ricezione di dati oltre che i circuiti di sincronizzazione di orologio associati non sono stati rappresentati. Parimenti, il protocollo di trasmissione per determinare per esempio la posizione o l'indirizzo del circuito destinatario dei dati trasmessi e la loro natura, per esempio l'impiego di un marcatore, o gettone, è ben noto al tecnico specializzato e non è stato spiegato qui.

Sarà ora spiegato il funzionamento del calcolatore 1.

In assenza della scheda a chip 30 nel lettore 5, il segnale 11 di autorizzazione di gestione impedisce ogni gestione dell'accensione 40 da parte del

processore 2. In questo esempio, non è previsto di rilevare materialmente l'introduzione della scheda a chip 30 nel lettore 5, in modo che il dato di autorizzazione contenuto nella memoria 3 è trasmesso ciclicamente sul bus 4 tramite il processore 2, al fine di effettuare scrutamento e di rilevarne una risposta sul bus 6 in caso di presenza della scheda a chip 30. In questo caso, il circuito di imbroglio 31 della scheda a chip 30 riceve il dato di autorizzazione e gli applica una trasformazione tramite imbroglio prima di rinviarlo sotto forma imbrogliata al circuito di ricezione 10, attraverso il bus 6.

Il circuito di sbroglio 13 effettua una trasformazione supplementare sul dato imbrogliato che lo trasforma in un dato sbrogliato identico, se la scheda a chip 30 è valida, al terzo dato contenuto nella memoria 17. Così, il circuito di ricezione 10 può confrontare il dato sbrogliato con il dato di autorizzazione, trasmesso da parte del processore 2 sul bus 4, tramite il terzo dato associato al dato di autorizzazione trasmesso.

L'impiego di due trasformazioni non inverse l'una dell'altra e di una associazione, segreta, fra il dato di autorizzazione emesso (3) e il dato atteso in

ritorno (17) permette così di disporre di tre chiavi indipendenti, la cui scoperta di una sola non pregiudica il segreto delle altre due. Si noterà che il confronto del dato di autorizzazione (3) con il dato sbrogliato avrebbe potuto essere effettuato confrontando direttamente questi due dati per determinarne una differenza, comparata in seguito con una differenza prevista, memorizzata (17).

Potrebbe anche tuttavia essere stato previsto di effettuare una trasformazione di sbroglio inversa di quella di imbroglio e, in questo caso, la memoria 17 che, associata con la memoria 3, costituisce la terza chiave, sarebbe stata inutile poichè il confronto dei dati trasmesso e ricevuto in ritorno sarebbe stato una semplice ricerca di uguaglianza, tramite applicazione del contenuto della memoria 3 al comparatore 12, la differenza indicata in precedenza essendo nulla.

Il circuito di inizializzazione 16 ha lo scopo di far iniziare la sequenza ciclica pseudo-aleatoria in un punto determinato del ciclo. Questo punto è determinato da un numero, variabile da un utilizzo all'altro della scheda a chip 30. Questo numero, che inizializza anche l'imbrogliatore 31, avrebbe potuto essere generato dalla scheda a chip 30 ma è qui generatore dal processore 2 e corrisponde qui al

numero dei secondi di un circuito di base di tempo, non rappresentato, dell'elaboratore 1. Ciò avrebbe potuto essere il generatore pseudo-aleatorio 15, o un altro, che genera il numero precedente. Questo numero è trasmesso, tramite il processore 2, alla scheda a chip 30 e all'ingresso del circuito di inizializzazione 16. Così, il dato imbrogliato varia da un'utilizzazione della scheda a chip 30 alla seguente e rende così più arduo il rilevamento di un algoritmo o chiave di imbroglio/sbroglio utilizzato dai circuiti di imbroglio 31 e di sbroglio 13.

L'insieme 20 di controllo di identità riceve, tramite il bus 6, la parola specifica di codificazione della memoria 32 e la confronta con quella della memoria 21 al fine di verificare che l'elaboratore 1 sia ben accoppiato alla scheda a chip 30 voluta. Si noterà che le posizioni relative dell'insieme 20 e della memoria 32 potrebbero essere permutate, poichè tutti gli elementi di controllo sono in un circuito 2, 4, 5, 30, 6, 10 e ogni interruzione logica di questo circuito invalida il segnale 11 di autorizzazione di gestione.

Può peraltro essere previsto che un dato variabile sia incluso in, o costituisca, il dato di autorizzazione (3). Questa può essere una parola di

codice, fornita dal generatore pseudo-aleatorio 15 o un'altra cosa. Questo può anche essere un dato di sfruttamento per la gestione dell'organo 40 gestito dal processore 2, cosa che evita di prevedere di memorizzare specificamente un dato di autorizzazione e permette anche di disporre di un dato di autorizzazione variabile, cosa che accresce ulteriormente la difficoltà di rilevazione fraudolenta dell'algoritmo di imbroglio/sbroglio. In quest'ultimo caso, potrebbe essere previsto di non inibire tramite il segnale 11 la gestione del motore 40 e di trasmettere gli ordini di accensione dopo un passaggio in un circuito di controllo 40, 30, 6, 10.

Quando il dato sbrogliato non fosse corretto, la gestione dell'accensione sarebbe essa stessa non corretta e impedirebbe in pratica l'uso della vettura.

Al fine di autorizzare l'autorizzazione della vettura da parte dei possessori di schede a chip diversi dal possessore della scheda 30, può essere previsto di accedere all'elaboratore 1 con la scheda 30 poi, a partire da mezzi di ingresso di dati uomo-macchine, tipo una tastiera, collegati al calcolatore 11, memorizzare nell'elaboratore 1 l'identità (32) di un'altra scheda che permette l'utilizzazione della vettura.

Possono anche essere associati, all'identità di una o dell'altra scheda, dati che limitano l'utilizzazione della vettura, per esempio nella sua durata o nelle sue prestazioni, per esempio tramite strangolamento del motore per mezzo del processore 2.

RIVENDICAZIONI

1. - Elaboratore di controllo dell'utilizzazione di un autoveicolo comprendente un insieme di organi di funzionamento (40), tra i quali un motore, comprendente, per la gestione del funzionamento di almeno uno degli organi funzionali (40), un processore (2), mezzi di lettura (5) di mezzi di controllo portatili (30) e mezzi (10), di ricezione di almeno un dato di controllo dei mezzi di controllo (30), per autorizzare il processore (2) a gestire l'organo considerato (40), elaboratore caratterizzato dal fatto che i mezzi di ricezione (10) comprendono mezzi di sbroglio (13), il processore (2) essendo strutturato per trasmettere almeno un dato di autorizzazione (3) della sua gestione dell'organo (40) da gestire ai mezzi di controllo (30) comprendenti mezzi di imbroglio (31), i mezzi di ricezione (10) essendo strutturati per sbrogliare (13) il detto dato, precedentemente imbrogliato (31) tramite i mezzi di controllo (30), e confrontarlo (12) con il dato (3) trasmesso ai mezzi di controllo (30) dall'organo gestito (40).

2. - Elaboratore secondo la rivendicazione 1, nel quale i detti mezzi di ricezione (10) sono strutturati (12) per confrontare il detto dato sbrogliato con il

dato trasmesso da parte del processore (2) tramite un terzo dato (17) associato al dato trasmesso (3).

3. - Elaboratore secondo una delle rivendicazioni 1 e 2, nel quale i mezzi di ricezione (10) comprendono un generatore (15) di sequenze pseudo-aleatorie.

4. - Elaboratore secondo una delle rivendicazioni da 1 a 3, nel quale sono previsti mezzi (21) di memorizzazione di dati di identificazione dell'elaboratore per essere confrontati dati associati (32) nei mezzi di controllo portatili (30).

5. - Elaboratore secondo la rivendicazione 1, nel quale i mezzi di ricezione (10) comprendono una porta logica OU esclusiva (12) per procedere al confronto del dato (3) trasmesso dal processore (2) e del dato sbrogliato.

6. - Elaboratore secondo una delle rivendicazioni da 3 a 5, nel quale il generatore (15) di sequenze pseudo-aleatorie comprende in ingresso un circuito di inizializzazione (16) strutturato per forzare le uscite del generatore (15) in uno stato determinato.

7. - Elaboratore secondo una delle rivendicazioni da 1 a 6, che è strutturato per includere, nel dato di autorizzazione (3), un dato di comando del detto organo gestito (40).

8. - Elaboratore secondo una delle

rivendicazioni da 1 a 7, che è strutturato per gestire un organo di accensione (40) del motore.

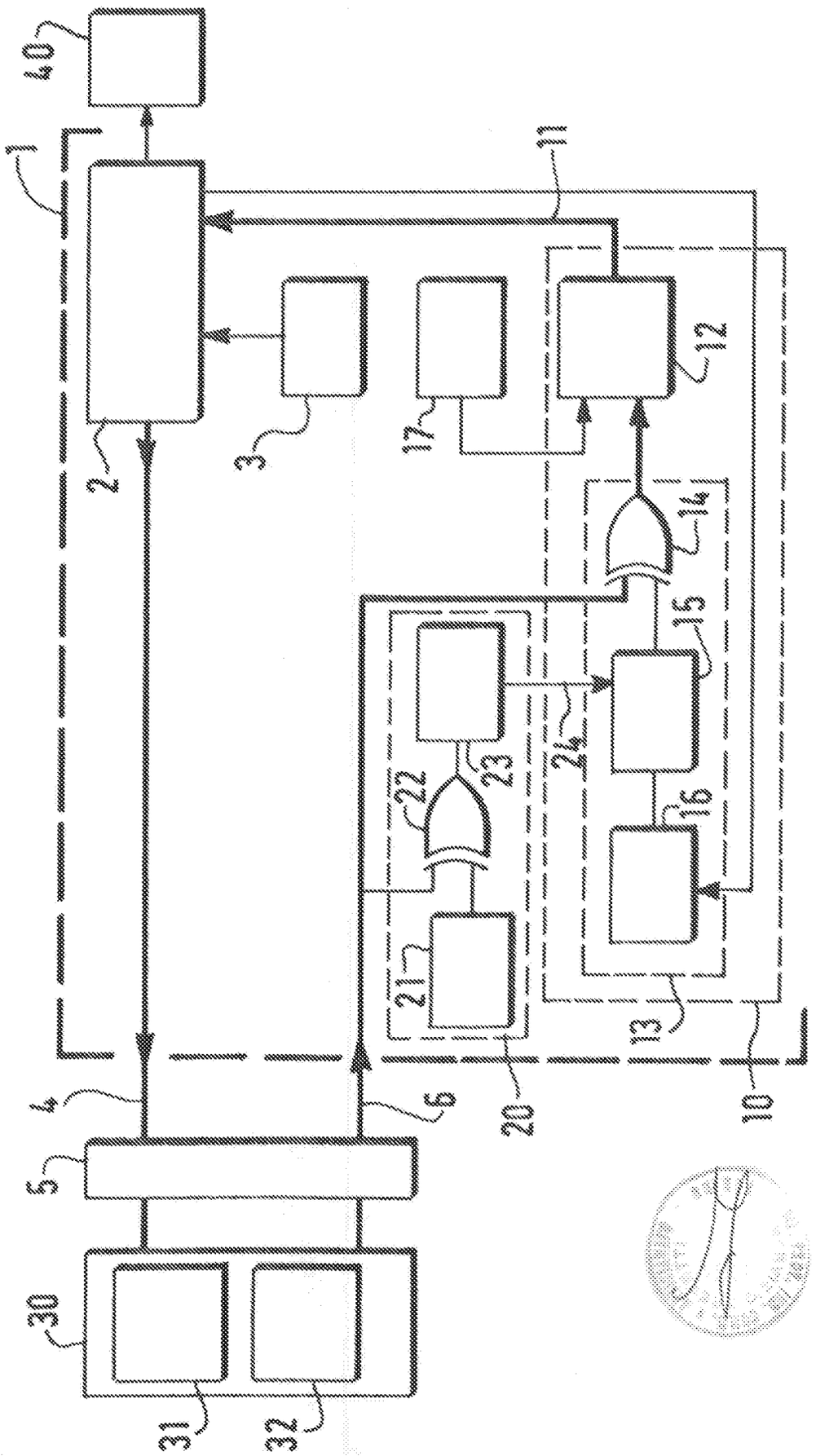
p.i.: Société d'Applications Générales d'Electricité et de Mécanique SAGEM

Luigi Franzolin

FRANZOLIN Luigi
(iscrizione Albo nr. 482)

FRANZOLIN Luigi
(iscrizione Albo nr. 482)

Caso DOS 511



p.i.: Société d'Applications Générales d'Electricité et de Mécanique SAGEM
FRANZOLIN Luigi
(iscrizione Albo nr. 482)