(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 681 822**

(51) Int. CI.:

***G05B 9/02*** (2006.01)
***B61L 19/06*** (2006.01)
***B61L 21/04*** (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **28.11.2013 E 13194789 (7)**

(97) Fecha y número de publicación de la concesión europea: **04.07.2018 EP 2879008**

(54) Título: **Método para manejar un comando crítico de seguridad en una red informática**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
**17.09.2018**

(73) Titular/es:

**THALES MANAGEMENT & SERVICES DEUTSCHLAND GMBH (100.0%)**
**Thalesplatz 1**
**71254 Ditzingen, DE**

(72) Inventor/es:

**MÜLLER, FRANK**

(74) Agente/Representante:

**ISERN JARA, Nuria**

## DESCRIPCIÓN

Método para manejar un comando crítico de seguridad en una red informática

Antecedentes de la invención

La invención se refiere a un método para manejar un comando crítico de seguridad en una red informática.

Un método de este tipo se conoce a partir del documento DE 10 2006 029 851 A1.

Una orden crítica de seguridad según la invención es una orden relativa a la ejecución de un proceso crítico de seguridad en un elemento de un sistema crítico de seguridad (por ejemplo, al interruptor de emergencia los puntos de una vía férrea), donde la "seguridad" está relacionada con la revelación de fallo, es decir, cuanto mayor es la revelación de fallo, mayor es la categoría de seguridad. La expresión "seguro" se utiliza en el contexto de la exclusión de salidas peligrosas del sistema, mientras que la expresión "asegurado" significa que se evita el impacto no deseado del medio ambiente en el sistema.

El documento DE 44 32 419 A1 describe un método para manejar comandos críticos de seguridad de un ordenador seguro EKIR de un enclavamiento a un ordenador de área segura. El EKIR crea un número aleatorio y lo transmite al ordenador del área. Para autorizar un comando, el usuario debe ingresar el número aleatorio que se envía a EKIR, donde se compara la entrada y el número aleatorio original.

El documento DE 10 2010 015 285 A1 divulga un método para confirmar un estado seguro de un sistema crítico de seguridad (sistema de señalización ferroviaria), en el que se envían códigos de activación al usuario que no pueden leerse en máquina. El usuario debe ingresar el código de activación manualmente.

Las soluciones conocidas para manejar comandos críticos de seguridad se basan normalmente en un procedimiento de comando crítico, en el que el operador debe confirmar que se lleva a cabo una transacción activando al menos un botón de confirmación como se describe en el documento DE 10 2006 029 851 A1, o TAN - Procedimientos conocidos de http://en.wikipedia.org/wiki/Transaction authentication_number. Para autorizar la ejecución de un comando de seguridad crítica, el operador debe ingresar manualmente una TAN, que sin embargo requiere mucho tiempo y es complicada. Dichos procedimientos TAN también son sensibles en caso de fallos del operador.

En un entorno cerrado, la implementación de dicho procedimiento TAN debe garantizar la independencia de dos canales de procesamiento dentro del terminal de operador no seguro: un primer canal para recibir el TAN del sistema seguro y mostrarlo al operador, un segundo canal para recibir el TAN ingresado del operador y transferir el TAN ingresado al sistema seguro. Dentro de un entorno abierto, debe garantizarse adicionalmente que no comprometan las transmisiones dentro del primer y segundo canal. Por lo tanto, los sistemas conocidos usan transmisión encriptada. También para el procedimiento de comando crítico se debe garantizar la independencia del procesamiento de la entrada replicada dentro del terminal operador y la independencia de la transmisión de la entrada replicada al ordenador seguro. Sin embargo, esto requiere propiedades dedicadas a ambos puntos finales de la comunicación, en particular, ambos puntos finales deben ser validados y evaluados.

Objeto de la invención

Por lo tanto, un objeto de la invención es proporcionar un método simplificado para manejar un comando crítico para la seguridad en una red informática con requisitos reducidos en cuanto a hardware y software.

Descripción de la invención

Este objetivo se consigue mediante un método de acuerdo con la reivindicación 1 y un uso de una red informática de acuerdo con la reivindicación 10 que comprende medios adaptados para implementar el método de la invención.

El método de la invención puede llevarse a cabo en una red informática con un ordenador seguro y un terminal de operador no seguro, el comando relativo a una transacción en un elemento. De acuerdo con la invención, el método comprende:

- transferencia del comando desde el terminal de operador no seguro al ordenador seguro;
- generación de un TAN, identificando el TAN el comando;
- generación de un primer código ejecutable y un segundo código ejecutable por el ordenador seguro, el segundo código que contiene el TAN, el primer código capaz de mostrar una consulta en un dispositivo de visualización del terminal operador no seguro y el segundo código que es capaz de permitir la ejecución de la transacción;

- encriptación de los códigos por el ordenador seguro;

- transmisión de los códigos encriptados al terminal de operador no seguro;

- desencriptado de los códigos por el terminal de operador no seguro;

- ejecución del primer código en el terminal de operador no seguro, mediante el cual se muestra una consulta al operador con una invitación para confirmar la consulta, es decir, para confirmar si el comando crítico debe ejecutarse o anularse;

- en caso de una confirmación por parte del operador, se ejecuta el segundo código y el TAN se transfiere a el ordenador seguro.

Un terminal de operador "no seguro" es un terminal de operador que no cumple con SIL 2, en particular que no cumple con ningún nivel de integridad de seguridad. Las únicas funcionalidades que son obligatorias para el terminal de operador no seguro son las siguientes: Poder enviar y recibir mensajes desde/hacia el ordenador seguro; ser capaz de identificar mensajes que contienen códigos encriptados; ser capaz de desencriptar dichos mensajes y ofrecer una plataforma para ejecutar el código desencriptado. El terminal de operador no seguro no necesita tener ninguna funcionalidad, que esté relacionada con el procesamiento correcto del procedimiento de confirmación. Un "ordenador seguro" es un ordenador que cumple SIL 2 o mejor, preferiblemente SIL 4.

La metodología del método de la invención se basa en la transmisión de códigos ejecutables encriptados, que permite el uso de un terminal de operador no seguro. El método de la invención permite la transferencia segura de TAN desde un sistema seguro a un terminal de operador no seguro y hacia atrás mientras se usa el mismo canal de transmisión. Solo un punto final (incluido el código que debe transmitirse y que debe ejecutarse mediante el terminal de operador no seguro) de la comunicación debe tener propiedades dedicadas que necesiten validación y evaluación. Las propiedades dedicadas se refieren en particular a canales de procesamiento independientes, en los que la independencia tiene que darse no solo para la transmisión sino también para el procesamiento, lo que significa que el punto final correspondiente debe cumplir con SIL $\geqq$ 0. De acuerdo con la presente invención, esto solo se requiere para el ordenador seguro, pero no para la terminal del operador (a diferencia de los métodos del estado de la técnica) en los que se ejecutan los códigos.

De acuerdo con la invención, el comando es introducido por un operador en el terminal de operador no seguro. El comando crítico de seguridad se transfiere luego a un sistema seguro para su ejecución. Para garantizar que el comando recibido no se vea comprometido por un dispositivo no seguro o una transmisión no segura y no asegurada, el sistema seguro genera códigos ejecutables que se encriptan y transfieren al terminal de operador no seguro, lo que contribuye a un seguro transmisión.

El TAN es generado preferiblemente por el ordenador seguro e identifica la transacción que se llevará a cabo (por ejemplo, el punto de conmutación A a la posición X).

Preferiblemente, el TAN comprende una contraseña de un solo uso (OTP). El encriptado de los códigos, en particular del segundo código que comprende el TAN, se puede hacer mediante un encriptado de almohadilla de una sola vez. Debido al encriptado de los códigos por el terminal de operador no seguro, se garantiza un funcionamiento instantáneo correcto del terminal de operador no seguro para ejecutar el código.

El primer código ejecutable hace que el operador no seguro muestre una consulta en un dispositivo de visualización según las instrucciones codificadas que ha recibido el ordenador seguro. La consulta solicita al operador la confirmación de si el comando crítico debe ejecutarse o anularse y devuelve un mensaje de confirmación basado en el TAN a través del segundo código ejecutable.

El desencriptado del segundo código se lleva a cabo preferentemente después de la confirmación por el operador para reducir el tiempo entre el desencriptado y la transmisión del TAN, lo que hace que el ordenador seguro ejecute la transacción crítica de seguridad.

El procedimiento de encriptado y desencriptado está alineado entre el ordenador seguro y el terminal de operador no seguro. Las claves apropiadas se intercambian antes del encriptado. Además, el entorno de ejecución para el primer código y el segundo código (tipo binario usado, bibliotecas externas usadas) debe estar alineado entre el ordenador seguro y el terminal de operador no seguro. Preferiblemente, se usa un código de byte de Java.

El método de la invención permite un reemplazo del procedimiento de comando crítico complejo conocido a partir del estado de la técnica, que exige un terminal de operador seguro. Desde la perspectiva de un operador, el procedimiento de comando crítico se simplifica, ya que no se exige duplicación de entrada. Sin embargo, es posible realizar un comportamiento conocido por el procedimiento de comando crítico por clic de tiempo supervisado en dos botones. Desde la perspectiva de un proveedor, la necesidad de tener un terminal de operador seguro

desaparecerá, es decir, ni el hardware ni el software del terminal no seguro deben cumplir con las exigencias del nivel de integridad de seguridad (SIL). No se requieren más actividades de evaluación (validación, caso de seguridad, informe de evaluación) para el terminal del operador. Por lo tanto, el terminal del operador puede estar hecho de hardware y software COTS (comercialmente disponible para la venta) que ofrece costes seguros.

El método de la invención permite el procesamiento paralelo/concurrente de comandos críticos. Al usar el método de la invención, no es necesario proporcionar canales independientes para la transmisión de los códigos, es decir, se puede usar un único terminal de operador no seguro canalizado. Además de proporcionar el encriptado y el TAN, los canales de comunicación entre el terminal operador y el ordenador seguro ya no requieren redes cerradas.

Variantes preferidas

Mediante la ejecución del primer código, una variante preferida del método de la invención muestra una ventana en el dispositivo de visualización, mostrando la ventana un reflejo del comando y al menos dos botones para confirmación y anulación de la transacción, respectivamente. La visualización de la consulta en el terminal de operador no seguro puede ser textual o gráfica. Alternativamente o, además, la pantalla y/o la confirmación pueden ser acústicas. En caso de que se realice un procedimiento de comando crítico mediante el método de la invención, se requieren más de dos botones. El segundo código se divide en el número correspondiente (correspondiente al número de botones) de los subcódigos, el primer subcódigo es la devolución de llamada para el primer botón para activar el segundo botón.

Se prefiere que la ventana muestre además información sobre el estado del elemento (por ejemplo, "el punto A está en la posición Y") y/o el estado del entorno del elemento (por ejemplo, "la sección de seguimiento relacionada está ocupada") en el que se realizará la transacción. La información de estado ayuda al operador a decidir si la transacción sugerida es acrítica o peligrosa bajo las circunstancias dadas.

En una variante ventajosa del método de la invención, el segundo código contiene una función de devolución de llamada para el primer código, la función de devolución de llamada transfiere el TAN.

Para evitar la ejecución repetida o retardada de la transacción, el TAN está equipado preferiblemente con una restricción de tiempo. En caso de que el TAN no se transmita dentro de un intervalo de tiempo predeterminado o antes de un límite de tiempo predeterminado, la transacción no se ejecuta a pesar de un TAN correcto.

En una variante especial, el primer código y el segundo código se incorporan en un archivo de programa.

Alternativamente, el primer código y el segundo código son archivos de programa separados. Al proporcionar los códigos como archivos de programa separados, el tiempo entre la ejecución del primer código y el segundo puede elegirse más tiempo en comparación con ambos códigos que forman parte de un único programa, por ejemplo, varios minutos. En este caso para el procesamiento simultáneo/paralelo de los comandos críticos, el primer código y el segundo código de un comando específico se vinculan entre sí para identificar los códigos correspondientes a dicho comando especificado. Esto se puede hacer proporcionando a cada código una característica de identificación, por ejemplo, una clave o una suma de verificación o un TAN adicional que se utiliza para el encriptado y/o la asignación del segundo código. Por ejemplo, el primer código se puede proporcionar con una clave para el desencriptado del segundo código. Alternativamente, el primer código puede proporcionarse con una clave que se compara con el segundo código.

Preferiblemente, el segundo código se desencripta inmediatamente antes de ejecutar el segundo código. Por lo tanto, la encriptación exitosa aumenta la confianza en el funcionamiento correcto del terminal de operador no seguro.

Para minimizar la interacción del operador, la confirmación del operador se puede llevar a cabo por medio de una técnica de un clic.

El método de la invención se puede usar ventajosamente para transacciones relacionadas con el transporte ferroviario u otros vehículos guiados.

La presente invención también se refiere al uso de un sistema de red informática que comprende un ordenador seguro y un terminal de operador no seguro para procedimientos de operación seguros de un nivel predeterminado de integridad de seguridad, en particular para el transporte ferroviario, en el que el ordenador seguro y el terminal de operador no seguro está conectado entre sí para transmitir mensajes, en el que el terminal de operador no seguro comprende un dispositivo de visualización y está configurado para identificar un código encriptado, para desencriptar el código encriptado y para visualizar una consulta en el dispositivo de visualización, en el que el ordenador seguro cumple con la categoría de seguridad predeterminada y el terminal de operador no seguro no cumple con la categoría de seguridad predeterminada.

El método de la invención se usa preferiblemente para sistemas técnicos para los que se aplica IEC 61508, o

normas derivadas de IEC 61508, o estándares similares, donde se necesita interacción humana para servicios seguros.

Preferiblemente, la categoría de sistema de transmisión predeterminado es de categoría 1, 2 o 3 según EN50159:2010.

El método de la invención puede usarse para la gestión del tráfico y la operación segura de sistemas de señalización, sistemas de control de rutas, sistemas de control de trenes y sistemas de enclavamiento. La "operación segura" resume el proceso de transmisión segura de comandos críticos para su ejecución. Una "transmisión segura" se refiere a un siguiente proceso de votación, que permite una revelación de fallos dentro del proceso solo con los medios de los componentes de la red informática utilizada para el método inventivo.

La base de la invención es la ejecución de un código extraño (código generado por el ordenador seguro) en un terminal de operador no seguro, en el que el código se prepara en un sistema seguro solo para ese fin y se protege mediante el uso de métodos criptográficos. De acuerdo con la invención, se completa con el ordenador seguro para controlar los mecanismos de seguridad que se aplican para el procedimiento de operación segura. Por lo tanto, se proporciona la independencia funcional del mecanismo de seguridad para las funciones par debidas por el terminal de operador no seguro.

Se pueden extraer ventajas adicionales de la descripción y el dibujo adjunto. Las características mencionadas anteriormente y a continuación se pueden usar de acuerdo con la invención individual o colectivamente en cualquier combinación. Las realizaciones mencionadas no deben entenderse como una enumeración exhaustiva, sino que tienen un carácter ejemplar para la descripción de la invención.

Dibujos

La invención se muestra en los dibujos.

La figura 1 muestra las etapas del método básico del método de la invención.

La figura 2 muestra un diagrama de flujo detallado de una variante preferida del método de la invención, en el que las etapas están relacionadas con los compuestos por medio de los cuales se llevan a cabo las etapas.

El método de la invención comprende las etapas que se muestran en la figura 1. Un comando crítico de seguridad $f_i(e_k)$ se transmite desde un terminal de operador no seguro a un ordenador seguro, donde fi denota una función (por ejemplo, f1: cambia un punto a X) y ek denota el elemento sobre el cual se llevará la función fuera (por ejemplo, e1: punto A)". El ordenador seguro genera un primer código A y un segundo código B, en el que el segundo código B incluye un TAN T. Los códigos A, B se encriptan y transmiten al terminal de operador no seguro, donde se ejecuta el primer código A, lo que resulta al mostrar una consulta al operador. Dependiendo de la entrada del operador en respuesta a la consulta, el segundo código B se ejecuta o anula.

En contraste con los métodos del estado de la técnica, los códigos A, B se ejecutan como "códigos extranjeros", es decir, los códigos A, B se generan en el ordenador seguro y están sujetos a los requisitos de seguridad del ordenador seguro, pero están ejecutado en el terminal de operador no seguro que no es responsable de la corrección de los códigos y la integridad de seguridad, que depende del ordenador seguro. La "integridad de seguridad" en particular se refiere a la correlación del primer código A y el segundo código B, la calidad OTP de TAN T y la exactitud de los códigos A, B. Se puede verificar el funcionamiento correcto del terminal de operador no seguro o falsificado por el encriptado correcto de los códigos A y B en el terminal de operador no seguro.

La figura 2 muestra una secuencia detallada de las etapas de una variante preferida del método de la invención, en la que las etapas del método se asignan al componente en el que se llevan a cabo las etapas. Primero, el comando crítico de seguridad $f_i(e_k)$ es ingresado por un operador en el terminal de operador no seguro (etapa 1) antes de la transferencia del terminal de operador no seguro a un ordenador seguro (etapa 2). Antes de ejecutar el comando $f_i(e_k)$, se debe garantizar que el comando crítico de seguridad recibido $f_i(e_k)$ sea correcto y no se vea comprometido (modificado). A menudo se debe garantizar, además, que el elemento ek esté en el estado correcto s para realizar la función fi. El primer código A generado por el ordenador seguro (etapa 3) presenta una ventana que contiene un reflejo del comando crítico recibido $f_i(e_k)$ y dos botones para confirmar, respectivamente, anular la operación. Además, la ventana también puede contener información sobre un estado s del elemento ek y/o un estado del entorno (no se muestra). El segundo código B generado por el ordenador seguro (etapa 5) contiene una función de devolución de llamada para el primer código A. La función de devolución de llamada transfiere un TAN T, que también ha sido generado por el ordenador seguro (por ejemplo, como contraseña de un solo uso) siendo opcionalmente equipado con una restricción de tiempo (etapa 4). El TAN T identifica de forma segura el comando crítico $f_i(e_k)$ para la ejecución. Como el código A y el código B se han generado en el sistema seguro, existe una independencia funcional de los códigos A, B y los datos y códigos A, B propiedad de/ubicados en el terminal de

operador no seguro. Ambos, el código A y el código B son encriptados por el ordenador seguro (etapa 6) y transferidos al terminal de operador no seguro (etapa 7).

En el terminal de operador no seguro, el primer código A se desencripta y se ejecuta (etapa 8). Al ejecutar el primer código A, se muestra la ventana al operador (etapa 9). El operador ahora vota si el comando crítico de seguridad $f_i(e_k)$debe ejecutarse o anularse (etapa 10) y en consecuencia envía una confirmación o un rechazo al terminal operador no seguro (etapa 11), por ejemplo, mediante una operación de un clic en un botón de "aceptar" o "anular". Para los códigos de confirmación de operador de un clic, A y B se preparan de manera tal que se previene la ejecución involuntaria del segundo código B (por ejemplo, debido a un mal funcionamiento del terminal de operador no seguro). Por lo tanto, en el caso de una operación del ratón, el evento clic se acepta solo si el ratón se mueve solo dentro de la ventana del código A justo antes de este clic. Esto es supervisado por el código A, respectivamente, el código B. En el caso de las pantallas táctiles, se utilizan y supervisan gestos definidos equivalentes.

En caso de que el operador confirme que ejecuta el comando crítico de seguridad solicitado $f_i(e_k)$, el segundo código desencriptado B es ejecutado por el terminal de operador no seguro (etapa 12) y el TAN T se transferirá a el ordenador seguro (etapa 13). El terminal de operador no seguro realiza una desencriptación del segundo código B antes o después de la confirmación del operador (no se muestra). El ordenador seguro finalmente puede votar sobre la corrección del TAN recibido (etapa 14) y ejecutar el comando crítico en caso de una votación positiva (etapa 15).

La operación segura de acuerdo con la invención todavía está basada en TAN. Pero la participación del operador en ese conocido procedimiento TAN puede reducirse al mínimo: confirmación con un clic.

La invención presentada supone una infraestructura criptográfica tanto en el terminal de operador no seguro como en el sistema seguro. La operación segura de la invención a través del terminal de operador no seguro utilizando métodos criptográficos garantiza una interacción minimizada del usuario y una independencia incorporada del procesamiento de información entrante y saliente, aunque usando un solo operador terminal no seguro y una única transmisión canalizada, donde "seguro" está relacionado con la revelación de fallos

Con el método de la invención, se pueden detectar y tratar una variedad de modos de fallo, algunos de los cuales se describen a continuación:

> En caso de un retraso significativo o una supresión entre las etapas 1 y 8, la etapa 8 será demasiado tarde o no se ejecutará, lo cual es revelado obviamente por el operador.

El operador revela cualquier corrupción o desvío durante las etapas 1 y 2 (por ejemplo, un comando modificado) votando si el comando mostrado debe ejecutarse o anularse (etapa 10).

Una inserción de una transmisión de un comando (etapa 2) también se revelará durante la etapa 9.

Cualquier desviación durante la transmisión de los códigos A, B (etapa 7) se revela para el falso receptor durante el desencriptado del código A (etapa 8), ya que no es posible el desencriptado exitoso y durante la votación (etapa 9) debido a la supresión para el lado correcto del receptor.

Cualquier ejecución involuntaria del código A (en la etapa 8) se revela por las propiedades del código A (reflejo del comando crítico) durante la votación (etapa 10).

Cualquier transmisión involuntaria de TAN T (etapa 13) se puede evitar mediante las propiedades del código B, en particular mediante las propiedades de TAN T, que se pueden generar como OTP dedicado a la solicitud "Realizar $f_i(e_k)$" (etapa 4).

Cualquier retraso o supresión significativa durante la transmisión del TAN T (etapa 13) se revela por la reacción faltante o retardada del sistema seguro en las etapas 14 y 15.

Cualquier inserción o corrupción o desvío durante la transmisión del TAN T (etapa 13) se revela durante la votación (etapa 14).

Lista de números de referencia

A primer código
B segundo código
T TAN
fi función
ek elemento
$f_i(e_k)$ comando crítico de seguridad
s estado del elemento

**REIVINDICACIONES**

1. Método para manejar un comando crítico de seguridad ($f_i(e_k)$) en una red informática con un ordenador seguro y un terminal de operador no seguro, el comando relativo a una transacción en un elemento (ek), el método comprende:

- transferencia del comando ($f_i(e_k)$) del terminal de operador no seguro al ordenador seguro;
- generación de un TAN (T), identificando el TAN (T) el comando; estando el método caracterizado además por
- generación de un primer código ejecutable (A) y un segundo código ejecutable (B) por el ordenador seguro, el segundo código (B) que contiene el TAN (T), el primer código (A) que es capaz de mostrar una consulta en un dispositivo de visualización del terminal de operador no seguro y el segundo código (B) que es capaz de permitir la ejecución de la transacción;
- encriptado de los códigos (A, B) por el ordenador seguro;
- transmisión de los códigos encriptados (A, B) al terminal de operador no seguro;
- desencriptado de los códigos (A, B) por el terminal de operador no seguro;
- ejecución del primer código (A) en el terminal de operador no seguro. mediante el cual se muestra una consulta al operador con una invitación para confirmar si el comando crítico debe ejecutarse o anularse;
- en caso de una confirmación por parte del operador, se ejecuta el segundo código (B) y el TAN (T) se transfiere a el ordenador seguro.

2. Método de acuerdo con la reivindicación 1, caracterizado por que mediante la ejecución del primer código (A) se visualiza una ventana en el dispositivo de visualización, mostrando la ventana un reflejo del comando y al menos dos botones para confirmación y anulación de la transacción, respectivamente.

3. Método de acuerdo con la reivindicación 2, caracterizado por que la ventana muestra además información sobre el (los) estado(s) del elemento (ek) y/o el estado del entorno del elemento (ek) sobre el que se va a realizar la transacción.

4. Método de acuerdo con una de las reivindicaciones anteriores, caracterizado por que el segundo código (B) contiene una función de devolución de llamada para el primer código (A), la función de devolución de llamada transfiere el TAN (T).

5. Método de acuerdo con una de las reivindicaciones anteriores, caracterizado por que el TAN (T) está equipado con una restricción de tiempo.

6. Método de acuerdo con una de las reivindicaciones 1 a 5, caracterizado por que el primer código (A) y el segundo código (B) se incorporan en un archivo de programa.

7. Método de acuerdo con las reivindicaciones 1 a 5, caracterizado por que el primer código (A) y el segundo código (B) son archivos de programa separados.

8. Método de acuerdo con una de las reivindicaciones anteriores, caracterizado por que la confirmación del operador se lleva a cabo mediante una técnica de un clic.

9. Método de acuerdo con una de las reivindicaciones anteriores, caracterizado por que el método se usa para transacciones relacionadas con el transporte ferroviario u otros vehículos guiados.

10. Uso de un sistema de red informática que comprende medios adaptados para implementar el método de una de las reivindicaciones anteriores.

11. Uso según la reivindicación 10, caracterizado por que se proporciona un ordenador seguro y un terminal de operador no seguro para procedimientos de operación seguros de un nivel predeterminado de integridad de seguridad, en particular para el transporte ferroviario, en el que el ordenador seguro y el terminal de operador no seguro están conectadas entre sí para transmitir mensajes, en el que el terminal de operador no seguro comprende un dispositivo de visualización y está configurado para identificar un código encriptado (A, B), para desencriptar el código encriptado (A, B) y para visualizar una consulta en el dispositivo de visualización
en el que el ordenador seguro cumple con la categoría de seguridad predeterminada y el terminal de operador no seguro no cumple con la categoría de seguridad predeterminada.

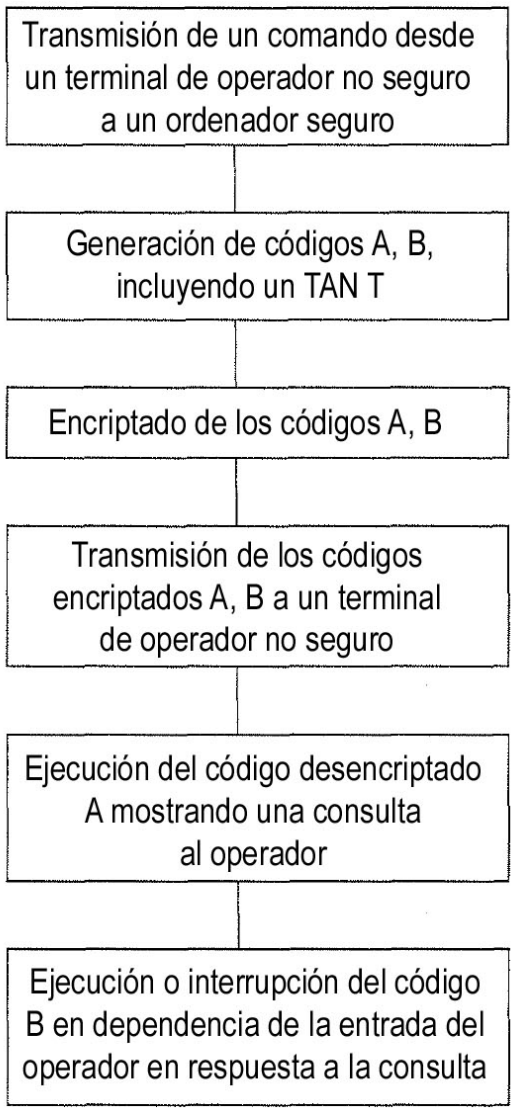
Transmisión de un comando desde un terminal de operador no seguro a un ordenador seguro
Generación de códigos A, B, incluyendo un TAN T
Encriptado de los códigos A, B
Transmisión de los códigos encriptados A, B a un terminal de operador no seguro
Ejecución del código desencriptado A mostrando una consulta al operador
Ejecución o interrupción del código B en dependencia de la entrada del operador en respuesta a la consulta

Fig. 1

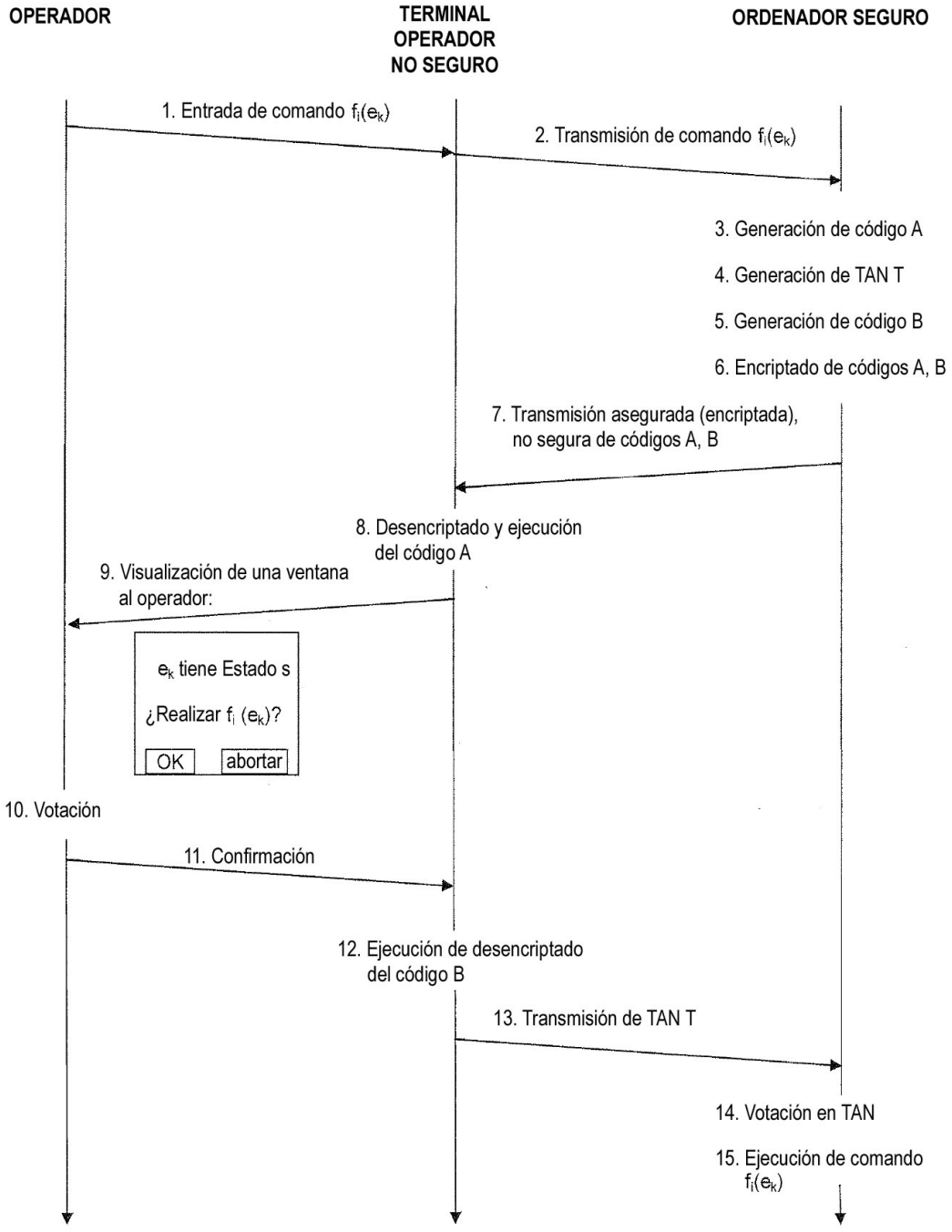
OPERADOR
TERMINAL OPERADOR NO SEGURO
ORDENADOR SEGURO
1. Entrada de comando $f_i(e_k)$
2. Transmisión de comando $f_i(e_k)$
3. Generación de código A
4. Generación de TAN T
5. Generación de código B
6. Encriptado de códigos A, B
7. Transmisión asegurada (encriptada), no segura de códigos A, B
8. Desencriptado y ejecución del código A
9. Visualización de una ventana al operador:
$e_k$ tiene Estado s
¿Realizar $f_i$ ($e_k$)?
OK
abortar
10. Votación
11. Confirmación
12. Ejecución de desencriptado del código B
13. Transmisión de TAN T
14. Votación en TAN
15. Ejecución de comando $f_i(e_k)$

Fig. 2