(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 916 385**

(51) Int. CI.:

B66B 1/34 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **21.09.2018 E 18195966 (9)**

(97) Fecha y número de publicación de la concesión europea: **18.05.2022 EP 3626664**

(54) Título: **Método y grupo de ascensores configurados para establecer una comunicación de datos segura entre una pluralidad de controladores en cada uno de una pluralidad de ascensores del grupo de ascensores**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
30.06.2022

(73) Titular/es:

INVENTIO AG (100.0%)
Seestrasse 55
6052 Hergiswil, CH

(72) Inventor/es:

COLOMBANO, CLAUDIO

(74) Agente/Representante:

ELZABURU, S.L.P

DESCRIPCIÓN

Método y grupo de ascensores configurados para establecer una comunicación de datos segura entre una pluralidad de controladores en cada uno de una pluralidad de ascensores del grupo de ascensores

La presente invención se refiere a un método para establecer una comunicación de datos segura entre una pluralidad de controladores en cada uno de la pluralidad de ascensores de un grupo de ascensores. Además, la presente invención se refiere a un grupo de ascensores que comprende controladores configurados para ejecutar o controlar dicho método y a un producto de programa informático configurado para ejecutar o controlar dicho método, así como a un medio legible por ordenador que comprende dicho producto de programa informático almacenado en él.

En edificios grandes, puede preverse una pluralidad de ascensores que forman un grupo de ascensores para transportar multitudes de pasajeros entre varios pisos del edificio. Allí, se requiere logística sustantiva para compartir adecuadamente las capacidades de transporte de la pluralidad de ascensores. En consecuencia, mientras que en los ascensores individuales se prevén controladores para controlar los movimientos de una cabina de ascensor en este ascensor único, en la pluralidad de ascensores dichos controladores en cada uno de los ascensores necesitan comunicarse entre sí. Por ejemplo, dicha comunicación puede ser necesaria para funcionalidades como el envío de cabinas de ascensores dentro del grupo de ascensores o para realizar servicios de emergencia en todo el grupo crítico. En particular, la información sobre pisos de destino actuales, llamadas de cabina, ocupación de cabina, llamadas prioritarias, etc. y potencialmente sobre cualquier mal funcionamiento en cada uno de los ascensores o sobre emergencias puede tener que compartirse con los otros ascensores del grupo de ascensores de manera que se pueda maximizar la seguridad y/o eficiencia del grupo de ascensores. Por ejemplo, la capacidad de transporte global del grupo de ascensores puede maximizarse organizando los viajes en ascensor de manera inteligente.

Sin embargo, la comunicación entre los controladores de varios ascensores puede verse comprometida. Por ejemplo, las personas no autorizadas pueden piratear la comunicación entre los ascensores y luego pueden manipular las operaciones de los ascensores. Por ejemplo, una forma posible de adquirir acceso no autorizado a una red de comunicación de un grupo de ascensores puede ser pinchar en un sistema de comunicación que utiliza cada ascensor para comunicarse con sus pares. Específicamente, una interfaz utilizada para la comunicación de datos entre varios controladores de ascensores en un grupo de ascensores puede ser particularmente sensible, ya que es la red troncal principal que utilizan estos controladores para realizar básicamente cualquier operación, incluidos los comandos de bajo nivel a una periferia física o la interferencia con los servicios de emergencia. Por su naturaleza y sus requisitos de eficiencia, dicha red troncal de comunicaciones es generalmente de plena confianza una vez autentificada, es decir, no aplica ninguna restricción y el acceso a ella implica plena autorización para todas sus funcionalidades.

Convencionalmente, el cifrado proporcionado en los documentos EP 1535874 A1 y US 20150280910 A1 puede utilizarse para establecer una comunicación de datos segura entre los controladores de un grupo de ascensores.

Sin embargo, en los anteriores sistemas de ascensores, la implementación de dicho cifrado puede requerir, o bien una gestión compleja de las claves de cifrado, o bien puede ser vulnerable a pérdidas de seguridad debidas, p. ej., a pérdida o publicación de claves de cifrado.

En consecuencia, puede existir la necesidad de un método para establecer una comunicación de datos segura entre los controladores de una pluralidad de ascensores de un grupo de ascensores que, por un lado, pueda proporcionar una seguridad de comunicación de datos superior y que, por otro lado, pueda implementarse fácilmente y a bajo costo. De manera similar, puede existir la necesidad de un grupo de ascensores que comprenda controladores configurados para implementar o controlar dicho método, así como un producto de programa informático configurado para ejecutar o controlar dicho método y un medio legible por ordenador que comprenda dicho producto de programa informático almacenado en él.

Tales necesidades pueden satisfacerse con el objeto de las reivindicaciones independientes. Las realizaciones ventajosas se definen en las reivindicaciones dependientes, así como en la siguiente memoria descriptiva.

De acuerdo con un primer aspecto de la presente invención, se propone un método para establecer una comunicación de datos segura entre una pluralidad de controladores en cada uno de una pluralidad de ascensores de un grupo de ascensores. En él, la pluralidad de ascensores se ha instalado inicialmente sin que se haya establecido ningún cifrado en la comunicación de datos entre sus controladores. De acuerdo con el método, antes de poner en marcha el grupo de ascensores, se ejecuta una etapa de establecimiento de cifrado para establecer el cifrado de datos en futuras comunicaciones de datos entre la pluralidad de controladores. La etapa de establecer el cifrado comprende al menos las siguientes etapas, preferiblemente en el orden indicado: Primero, se inicia una generación de un par de claves de cifrado aleatorias en cada uno de los controladores del grupo de ascensores al recibir un comando de "preparar seguridad". El par de claves de cifrado comprende una clave privada y una clave pública. Luego, cada uno de los controladores almacena su clave privada generada en un área protegida en un sistema de archivos. Además, cada uno de los controladores anuncia su identidad y su clave pública a los controladores de todos los demás ascensores del grupo de ascensores. Luego, cada uno de los controladores almacena las claves públicas obtenidas tras el anuncio de los otros controladores en el grupo de ascensores. Posteriormente, la etapa de establecimiento del cifrado finaliza al transcurrir un período de tiempo predeterminado desde el inicio de la etapa de establecimiento del cifrado o al ocurrir

un evento de finalización. Después de finalizar la etapa de establecimiento del cifrado, no se acepta la obtención ni el almacenamiento de claves públicas adicionales en cada uno de los controladores y la futura comunicación de datos entre la pluralidad de controladores se establece mediante el cifrado de un paquete de comunicación de datos por parte de un controlador de envío utilizando la clave de cifrado pública de un controlador de recepción y descifrado del paquete de comunicación de datos al recibirlo en el controlador de recepción utilizando la clave privada almacenada en el controlador de recepción.

Según un segundo aspecto de la invención, se propone un grupo de ascensores que comprende una pluralidad de ascensores. En él, cada ascensor tiene un controlador, estando configurados los controladores bien para ejecutar, o bien para controlar un método según una realización del primer aspecto de la invención.

Según un tercer aspecto de la invención, se propone un producto de programa informático. El producto de programa informático comprende instrucciones legibles por ordenador que, cuando las ejecuta un procesador de un controlador en un ascensor de un grupo de ascensores, instruyen al controlador para ejecutar o controlar el método según una realización del primer aspecto de la invención.

Según un cuarto aspecto de la invención, se propone un medio legible por ordenador, comprendiendo el medio legible por ordenador un producto de programa informático según una realización del tercer aspecto de la invención almacenado en el mismo.

Las ideas subyacentes a las realizaciones de la presente invención pueden interpretarse como basadas, entre otras cosas y sin restringir el alcance de la invención, en las siguientes observaciones y reconocimientos.

Como ya se indicó brevemente en la parte introductoria, los controladores de ascensores que son miembros del grupo de ascensores generalmente necesitan comunicarse entre sí y tal comunicación puede ser vulnerable a piratería y/o manipulaciones no autorizadas.

Una forma tradicional de protegerse contra tales amenazas puede ser el uso de cifrado en la comunicación de datos entre los varios controladores.

Por ejemplo, el cifrado que aplica claves asimétricas puede proporcionar un alto nivel de seguridad en las comunicaciones. Un par de claves asimétricas generalmente comprende una clave pública que puede distribuirse a los socios de comunicación y una clave privada que debe mantenerse en secreto. Allí, la clave pública de un destinatario puede ser utilizada por un socio de comunicación para cifrar los datos antes de enviarlos al destinatario. La clave privada puede entonces ser utilizada por el destinatario para descifrar dichos datos cifrados al recibirlos.

Usando dicho cifrado, cada participante en una comunicación de datos en una red es identificado y autorizado de manera única por su par de claves. Por lo tanto, es crucial que nunca se revele la clave secreta de un determinado miembro autorizado de la red. Si se compromete una clave secreta, entonces es virtualmente posible hacerse pasar por un miembro autorizado de la red para realizar accesos no autorizados y manipulaciones de los otros miembros.

Una forma muy sencilla de implementar tareas de cifrado puede ser definir un solo par de claves generalmente para todos los ascensores de, por ejemplo, una determinada línea de productos o versión de ascensores. La clave secreta puede almacenarse, por ejemplo, en un área protegida de un sistema operativo de un controlador de ascensor. La clave pública es, en tal escenario, la misma para todos los controladores y, por lo tanto, es conocida a priori por cada uno de los miembros comunicantes de un grupo de ascensores.

Este enfoque simple puede permitir generar solo una imagen ejecutable de un software de controlador que luego puede implementarse en todas partes sin requisitos de configuración adicionales relacionados con la seguridad en el campo o en el momento de la producción. En otras palabras, en tal escenario, cada controlador podría comunicarse con cualquier otro controlador de este tipo o versión de controladores, independientemente de su ubicación, ya que todos los controladores comparten el mismo par de claves de cifrado. Aparentemente, tal enfoque puede proporcionar ventajas logísticas.

Sin embargo, si bien este enfoque puede ser simple, puede sufrir de una fiabilidad insuficiente. Por ejemplo, en caso de que una clave privada se vea comprometida en uno de los controladores, entonces todos los controladores de una determinada línea o versión de producto se verán comprometidos, ya que todos comparten las mismas claves.

En un enfoque alternativo, se pueden generar pares de claves de cifrado individuales para cada uno de una multiplicidad de controladores en múltiples ascensores. Dichos pares de claves individuales pueden generarse durante la fabricación de los ascensores y las claves públicas de dichos pares de claves pueden tener que distribuirse a continuación a todos los socios de comunicación. Sin embargo, generar y distribuir tal multiplicidad de claves individuales implica una gestión de claves compleja.

Por un lado, debe evitarse una fiabilidad insuficiente en un enfoque de cifrado. Por otro lado, también debe evitarse la generación y gestión de un gran número de pares de claves ya durante la fabricación de los ascensores y la compleja logística de gestión de claves resultante.

Por lo tanto, resumido brevemente, el enfoque propuesto en la presente memoria descriptiva pretende proporcionar un mecanismo que crea claves de cifrado de forma dinámica y las almacena durante el tiempo de puesta en marcha, es decir, después de la fabricación e instalación de un grupo de ascensores. Por un lado, dicha generación dinámica de pares de claves permite evitar el problema de fiabilidad mencionado anteriormente de tener claves compartidas globalmente, ya que se genera dinámicamente un par de claves individual para cada controlador en un ascensor que es miembro de un grupo de ascensores. En consecuencia, cuando un solo controlador se ve comprometido y se revela su clave privada, la comunicación de datos con otros controladores que utilizan otros pares de claves no se ve afectada. Por otro lado, el enfoque propuesto en la presente memoria descriptiva puede proporcionar ventajas similares a las descritas anteriormente con respecto al enfoque simple que proporciona solo un par de claves para todos los controladores, es decir, generalmente se puede evitar la configuración y gestión adicionales de múltiples claves en un momento de producción del ascensor.

En el enfoque descrito en la presente memoria descriptiva, se puede fabricar e instalar una pluralidad de ascensores que forman un grupo de ascensores sin que inicialmente se establezca ningún cifrado en la comunicación de datos entre los controladores de estos ascensores. En consecuencia, durante esta primera fase, todos los controladores de este grupo de ascensores pueden comunicarse entre sí. En particular, no se requiere verificación de autorización entre los controladores que se comunican. Por lo tanto, el trabajo de instalación y preparación para la puesta en marcha del grupo de ascensores puede simplificarse significativamente.

Sin embargo, antes de poner en marcha el grupo de ascensores, es decir, antes de entregar el grupo de ascensores a un cliente y poner en marcha el funcionamiento normal del grupo de ascensores en un edificio con servicios, debe ejecutarse la llamada etapa de establecimiento de cifrado. En dicha etapa de establecimiento de cifrado, los controladores en el grupo de ascensores se modifican y configuran específicamente de manera que cualquier comunicación de datos posterior pueda usar cifrado asimétrico y, por lo tanto, pueda ser seguro.

Específicamente, la etapa de establecimiento del cifrado comienza iniciando una generación de pares de claves de cifrado aleatorias. Dicha generación de pares de claves se inicia al recibir el llamado comando "preparar seguridad", es decir, un comando que indica que se establecerá una comunicación de datos segura para el futuro.

Por ejemplo, el comando "preparar seguridad" puede ser generado por un técnico utilizando una interfaz hombre-máquina (HMI) de usuario. El técnico puede haber realizado previamente tareas de puesta en marcha final, incluyendo por ejemplo tareas de instalación y/o tareas de configuración, para el grupo de ascensores. Dichas tareas de puesta en marcha generalmente tienen que completarse antes de entregar el grupo de ascensores a un cliente y comenzar su funcionamiento normal. Al completar dichas tareas de puesta en marcha, el técnico puede entonces generar el comando "preparar seguridad" utilizando, por ejemplo, un panel de mantenimiento que incluye una HMI. Para tal fin, el técnico normalmente tiene que estar ubicado dentro de un área restringida del grupo de ascensores, es decir, por ejemplo, dentro de un cuarto de máquinas de uno de los ascensores. Como el acceso a tal área restringida está limitado a técnicos autorizados, se puede suponer que la generación del técnico del comando "preparar seguridad" autoriza el inicio de la etapa de establecimiento de cifrado.

Alternativamente, el comando "preparar seguridad" puede generarse de otras formas. Por ejemplo, dicho comando puede enviarse a través de una red. En consecuencia, es posible que dicho comando se genere, p. ej., en un centro de control remoto de ascensores y luego se transmite hacia los controladores en el grupo de ascensores. Sin embargo, preferiblemente, se debe requerir autorización para preparar el comando "preparar seguridad". En otras palabras, por lo general, se deben implementar medidas de seguridad para garantizar que el comando "preparar seguridad" pueda ser generado y enviado exclusivamente por una persona o instancia autorizada.

Al recibir el comando "preparar seguridad", cada uno de los controladores de los ascensores del grupo de ascensores empieza a generar un par de claves de cifrado aleatorias. Dicho par de claves comprende una clave pública individual para cifrar datos y una clave privada individual asociada para descifrar posteriormente los datos. La generación de claves debe ser "aleatoria", es decir, las claves se generarán de forma aleatoria o al menos cuasi-aleatoria. Esto significa que cada controlador debe generar su par de claves de forma no determinista. Cada controlador puede comprender una fuente de entropía para generar dicho par de claves aleatorias.

Al haber generado su par de claves, cada uno de los controladores almacena su clave privada generada en un área protegida en un sistema de archivos. En otras palabras, la clave privada que debe mantenerse en secreto puede almacenarse en el controlador en un área de una memoria que está específicamente protegida contra accesos o manipulaciones no autorizados. Por ejemplo, el área protegida del sistema de archivos puede hacerse segura mediante un cortafuegos o medios técnicos similares. En consecuencia, las claves privadas no pueden verse comprometidas y solo pueden ser accesibles por el controlador que haya generado esta clave privada durante la etapa de establecimiento del cifrado.

Además, al haber generado su par de claves, cada uno de los controladores anuncia su identidad y su clave pública a los controladores de todos los demás ascensores del grupo de ascensores. En otras palabras, mientras mantiene en secreto su clave privada, un controlador distribuye su clave pública a todos los socios de comunicación, es decir, a todos los demás controladores de ascensores en el grupo de ascensores con los que se requerirá el intercambio de datos durante la operación posterior del grupo de ascensores. Junto con la clave pública, el controlador también

anuncia su identidad. En consecuencia, los controladores de los otros ascensores reciben tanto la clave pública como la información sobre la identidad del controlador que ha anunciado esta clave pública, de manera que ambas partes de la información pueden asociarse entre sí. Las claves públicas y/o la información sobre la identidad del controlador pueden distribuirse entre los controladores de ascensor a través de una red. Tales redes pueden ser cableadas o inalámbricas.

Al recibir las claves públicas anunciadas, cada uno de los controladores almacena las claves públicas obtenidas de los otros controladores del grupo de ascensores. En otras palabras, cada uno de los controladores del grupo de ascensores recibe claves públicas de todos los demás controladores del grupo de ascensores y las almacena, por ejemplo, en un sistema de archivos. Estos sistemas de archivos no necesariamente tienen que estar protegidos. Además, también se puede almacenar información sobre la identidad del controlador que anuncia una de las claves públicas. En consecuencia, en futuras comunicaciones de datos, un controlador de ascensor que desee enviar datos a otro controlador de ascensor puede determinar la clave pública que se utilizará para el cifrado de datos basándose en la identidad del otro controlador de ascensor.

Para evitar manipulaciones o usos indebidos, se debe finalizar la etapa de establecimiento del cifrado, es decir, se debe finalizar la fase en la que los controladores de ascensores deben obtener claves públicas de otros controladores de ascensores del grupo de ascensores. De lo contrario, si dicha fase continuara, por ejemplo, un manipulador podría ingresar a la red de datos entre los controladores de ascensores y enviar su propia clave pública a los miembros del grupo de ascensores de modo que, posteriormente, los controladores de ascensores de este grupo de ascensores empezarían a comunicarse con este manipulador no autorizado.

En general, la etapa de establecimiento de cifrado se puede finalizar de dos maneras:

En una primera alternativa, la etapa de establecimiento de cifrado puede finalizar automáticamente después de un período de tiempo predeterminado desde que ha transcurrido el inicio del paso de establecimiento de cifrado. Tal período de tiempo predeterminado puede ser lo suficientemente largo para completar un intercambio de claves entre todos los controladores del grupo de ascensores. Por ejemplo, el período de tiempo predeterminado debería ser superior a 10 ms, preferiblemente superior a 0,1 s o superior a 0,5 s. Sin embargo, el período de tiempo predeterminado debe ser lo suficientemente corto para reducir cualquier riesgo de uso indebido o manipulación. Por ejemplo, el período de tiempo predeterminado puede ser inferior a una hora, preferentemente inferior a 1 min o inferior a 10 s o incluso inferior a 1 s.

En una segunda alternativa, la etapa de establecimiento del cifrado puede finalizarse al ocurrir un evento de finalización específico. Dicho evento de finalización puede ser generado, por ejemplo, por un técnico o por cualquier medio técnico que verifique las condiciones dentro del grupo de ascensores.

Por ejemplo, el evento de finalización puede ser la introducción de un comando "seguro" introducido por un técnico autorizado, indicando dicho comando "seguro" que se ha completado con éxito un proceso de reconocimiento que incluye el intercambio de claves públicas entre todos los controladores.

En otras palabras, el técnico puede observar y verificar las condiciones dentro del grupo de ascensores y luego puede decidir si se debe finalizar la etapa de establecimiento de cifrado. Por ejemplo, el técnico puede comprobar las indicaciones de estado en uno, varios o todos los controladores del grupo de ascensores, informando tales indicaciones de estado, por ejemplo, sobre un número de claves públicas recibidas desde otros controladores de ascensores. En consecuencia, el técnico puede determinar si todas las claves públicas se han intercambiado satisfactoriamente entre los miembros del grupo de ascensores. Habiendo hecho tal determinación, el técnico puede ingresar el comando "seguro".

Por ejemplo, dicho comando puede introducirse a través de una HMI incluida en uno de los ascensores del grupo de ascensores. En caso de que la HMI se proporcione en un área restringida a la que solo puede tener acceso el personal autorizado, la autorización del técnico ya está dada por el hecho de que el técnico puede acceder a la HMI. En caso de que no se proporcione dicha restricción local, solo se puede aceptar introducir el comando "seguro" si un usuario ha mostrado previamente su autorización, por ejemplo, durante un proceso de autentificación.

Al finalizar la etapa de establecimiento de cifrado solo después de que el técnico autorizado haya introducido un comando "seguro", en lugar de finalizar automáticamente la etapa de establecimiento de cifrado después de un tiempo predeterminado, el técnico puede verificar personalmente si el proceso de negociación entre los controladores del ascensor se ha completado con éxito. Solo si este es el caso, el técnico introducirá el comando "seguro" para finalizar la etapa de establecimiento del cifrado.

Una vez finalizada la etapa de establecimiento del cifrado, ninguno de los controladores del grupo de ascensores puede obtener ni almacenar más claves públicas. Además, la futura comunicación de datos entre los controladores que son miembros del grupo de ascensores solo se habilitará al cifrar un paquete de comunicación de datos por parte de un controlador emisor utilizando la clave de cifrado pública de un controlador receptor. El controlador receptor puede entonces descifrar el paquete de comunicación de datos cifrados al recibirlo utilizando su clave privada.

En general, por un lado, las realizaciones del método propuesto pueden permitir una instalación y puesta en marcha simples de los ascensores de un grupo de ascensores ya que, durante dicho período de instalación y puesta en marcha, los ascensores pueden comunicarse sin restricciones. Por otro lado, las manipulaciones de la comunicación de datos entre los controladores en el grupo de ascensores pueden evitarse durante el funcionamiento normal del grupo de ascensores, ya que toda la comunicación de datos está cifrada y, por lo tanto, es segura después de haber generado dinámicamente pares de claves de cifrado y de haber intercambiado las claves públicas de estos pares de claves durante la etapa de establecimiento del cifrado. Además, no se requiere una compleja logística global de gestión de claves para, p. ej., miles de ascensores, ya que los pares de claves de cifrado para cada ascensor individual no se generan durante la fabricación del ascensor, sino que se generan dinámicamente solo para cada uno de un número relativamente pequeño de ascensores incluidos en el grupo de ascensores y luego se anunciarán directamente a todos los demás ascensores en este grupo de ascensores formando futuros socios de comunicación.

En un grupo de ascensores según una realización del segundo aspecto de la invención, cada ascensor tiene un controlador que está configurado para ejecutar o controlar una realización del método propuesto. Para tal fin, el controlador puede comprender un procesador para procesar datos, una memoria para almacenar datos y una interfaz de datos para intercambiar datos con dispositivos externos, tal como con otros controladores de ascensores. El controlador puede ser programable.

Un producto de programa informático según una realización del tercer aspecto de la invención comprende instrucciones legibles por ordenador que, cuando las ejecuta el procesador de un controlador de ascensor, instruyen al controlador para que ejecute o controle una realización del método propuesto. El producto de programa informático puede programarse en cualquier lenguaje informático.

El producto de programa informático puede almacenarse en un medio legible por ordenador, tal como una memoria flash, un CD, un DVD, una ROM, una PROM, una EPROM, etc. Alternativamente, el producto de programa informático puede almacenarse en otro ordenador o servidor o en una nube de datos y puede descargarse, por ejemplo, a través de una red tal como Internet.

Cabe señalar que las posibles características y ventajas de las realizaciones de la invención se describen en la presente memoria descriptiva en parte con respecto a un método para establecer una comunicación de datos segura entre una pluralidad de controladores en un grupo de ascensores y en parte con respecto a un grupo de ascensores en el que los controladores están configurados para implementar dicho método. Un experto en la técnica reconocerá que las características pueden transferirse adecuadamente de una realización a otra y las características pueden modificarse, adaptarse, combinarse y/o reemplazarse, etc., para llegar a otras realizaciones de la invención.

A continuación, se describirán realizaciones ventajosas de la invención con referencia a los dibujos adjuntos. Sin embargo, ni los dibujos ni la descripción se interpretarán como limitantes de la invención.

La figura 1 muestra un grupo de ascensores que comprende una pluralidad de ascensores, cada uno de los cuales tiene un controlador, según una realización de la presente invención.

La figura 2 muestra un diagrama de flujo para visualizar las etapas de un método según una realización de la presente invención.

La figura 1 muestra un grupo 1 de ascensores que comprende una pluralidad de ascensores 3. Cada ascensor 3 comprende un controlador 5. Los controladores 5 de todos los ascensores 3 del grupo 1 de ascensores se comunican entre sí a través de una red 7 de comunicación de datos. Cada uno de los controladores 5 controla una operación de un motor 9 de accionamiento respectivo para desplazar una cabina 11 de ascensor. Como se muestra esquemática y ejemplarmente para el ascensor 3 más a la izquierda, el controlador 5 puede estar conectado a una interfaz 17 hombre-máquina. Tanto el controlador 5 como la interfaz 17 hombre-máquina puede encerrarse en un cuarto 13 de máquinas a la que sólo puede tener acceso personal autorizado, tal como un técnico autorizado 15.

El diagrama de flujo que se muestra en la Fig. 2 comprende varias etapas (1) a (10). Algunas de estas etapas se relacionan con acciones preparatorias antes de establecer la comunicación segura de datos en un grupo de ascensores, mientras que otras etapas (4) - (10) se relacionan con las etapas del método para establecer la comunicación segura de datos durante una etapa (19) de establecimiento de cifrado según una realización del método inventivo.

En una primera etapa (1), varios controladores para varios ascensores de un grupo de ascensores se envían al campo sin que exista ninguna disposición de seguridad. Por lo tanto, no hay verificación de autorización entre los controladores cuando intentan establecer comunicación entre ellos.

En una segunda etapa (2), normalmente se instalan los ascensores del grupo de ascensores. Además, durante esta fase, no existen disposiciones de seguridad y, de nuevo, no existe verificación de autorización que también pueda interferir con el proceso de instalación y aceptación.

En una tercera etapa (3), un técnico realiza tareas de puesta en marcha final antes de entregar el sistema de ascensores a un cliente. Antes de hacer eso, el técnico verifica que el grupo de ascensores sea completamente funcional y esté conectado.

En una etapa siguiente (4), el técnico emite un comando "Preparar seguridad", a través de una interfaz de usuario, para comenzar la etapa de establecimiento de cifrado e iniciar la generación automática de pares de claves en todos los controladores de ascensores.

Posteriormente, en la etapa (5), cada controlador genera un par de claves aleatorias que se utilizarán para la autentificación y autorización. Las fuentes de entropía deben estar disponibles para generar suficientes claves aleatorias.

En una etapa siguiente (6), cada controlador almacena su clave privada secreta en un área protegida del sistema de archivos y se anuncia a sí mismo y su clave pública a todos los miembros del grupo de ascensores.

Luego, en la etapa (7), cada controlador almacena las claves públicas de cada uno de los demás miembros del grupo de ascensores con los que se comunica. Esto se utilizará para autentificar a los pares en la red de ascensores.

En la etapa (8), los ascensores realizan un reconocimiento para validar la finalización del procedimiento, p. ej., mostrando en una interfaz de usuario los miembros cuya clave pública se ha adquirido con éxito.

En la etapa (9), cuando todos los ascensores confirmen una adquisición correcta de las claves públicas de todos los demás miembros, el técnico seleccionará y emitirá, a través de una interfaz de usuario, un comando de "Seguridad".

Finalmente, en la etapa (10), cada uno de los controladores confirma el comando de "Seguridad" en su respectiva interfaz de usuario, y se consolida la seguridad dentro de la comunicación de datos del grupo. A partir de este momento, todos los controladores utilizarán el material de clave nuevo y aleatorio generado para realizar una comunicación segura con todos los demás miembros del grupo de ascensores.

Finalmente, para evitar cualquier mala interpretación, se debe tener en cuenta que esta invención se centrará principalmente en garantizar la seguridad de la comunicación de datos mediante la aplicación de claves dinámicas en un grupo de controladores que se supone fijo e inalterable en un determinado edificio. Su objetivo principal es fortalecer una red troncal de comunicación crítica de alto rendimiento y tráfico intensivo preferiblemente continua las 24 horas del día, los 7 días de la semana entre dichos controladores (también conocida como middleware).

Finalmente, cabe señalar que el término "que comprende" no excluye otros elementos o etapas y el "un" “una” o “uno” no excluye una pluralidad. También se pueden combinar elementos descritos en asociación con diferentes realizaciones. También debe tenerse en cuenta que los signos de referencia en las reivindicaciones no deben interpretarse como una limitación del alcance de las reivindicaciones.

Lista de signos de referencia

1 grupo de ascensores

3 ascensor

5 controlador

7 red

9 motor de accionamiento

11 cabina de ascensor

13 cuarto de máquinas

15 técnico

17 interfaz hombre-máquina

19 etapa de establecimiento de cifrado

REIVINDICACIONES

1. Método para establecer una comunicación de datos segura entre una pluralidad de controladores (5) en cada uno de una pluralidad de ascensores (3) de un grupo (1) de ascensores,

en el que la pluralidad de ascensores (3) se ha instalado inicialmente sin que se haya establecido ningún cifrado en la comunicación de datos entre sus controladores (5),

en el que antes de poner en marcha el grupo (1) de ascensores, se ejecuta una etapa (19) de establecimiento de cifrado para establecer el cifrado de datos en futuras comunicaciones de datos entre la pluralidad de controladores (5), comprendiendo la etapa (19) de establecimiento de cifrado :

- iniciar, al recibir un comando de "preparar seguridad", la generación de un par de claves de cifrado aleatorias en cada uno de los controladores (5) del grupo (1) de ascensores, comprendiendo el par de claves de cifrado una clave privada y una clave pública;

- almacenando cada uno de los controladores (5) su clave privada generada en un área protegida en un sistema de archivos y anunciando su identidad y su clave pública a los controladores (5) de todos los demás ascensores (3) del grupo (1) de ascensores;

- almacenando cada uno de los controladores (5) las claves públicas obtenidas tras anunciando desde de los otros controladores (5) en el grupo (1) de ascensores;

- finalizar la etapa (19) de establecimiento de cifrado al transcurrir un periodo de tiempo predeterminado desde el inicio de la etapa de establecimiento de cifrado y la ocurrencia de un evento de finalización;

en el que, después de finalizar la etapa (19) de establecimiento de cifrado, no se acepta la obtención ni el almacenamiento de claves públicas adicionales en cada uno de los controladores (5) y la futura comunicación de datos entre la pluralidad de controladores (5) se establece mediante el cifrado de un paquete de comunicación de datos. por un controlador emisor (5) utilizando la clave de cifrado pública de un controlador receptor (5) y descifrando el paquete de comunicación de datos al recibirlo en el controlador receptor (5) utilizando la clave privada almacenada en el controlador receptor (5).

2. Método de la reivindicación 1, en el que el período de tiempo predeterminado es inferior a una hora.

3. Método según la reivindicación 1, en el que el evento de finalización es la introducción de un comando de "seguridad" introducido por un técnico autorizado que indica que se ha completado con éxito un proceso de reconocimiento que incluye el intercambio de claves públicas entre todos los controladores (5).

4. Método según una de las reivindicaciones anteriores, en el que para preparar el comando "preparar seguridad", se requiere autorización.

5. Método según una de las reivindicaciones anteriores, en el que el comando "preparar seguridad" lo prepara un técnico (15) introduciendo un comando en una interfaz (17) hombre-máquina ubicada en un cuarto (13) de máquinas de uno de los ascensores (3).

6. Grupo (1) de ascensores que comprende una pluralidad de ascensores (3), teniendo cada ascensor (3) un controlador (5), estando configurados los controladores (5) para bien ejecutar o bien controlar un método según una de las reivindicaciones 1 a 5.

7. Producto de programa informático que comprende instrucciones legibles por ordenador que, cuando las realiza un procesador de un controlador (5) en un ascensor (3) de un grupo (1) de ascensores, instruyen al controlador (5) para que ejecute y controle el método según una de las reivindicaciones 1 a 5.

8. Medio legible por ordenador que comprende un producto de programa informático según la reivindicación 7 almacenado en el mismo.

Fig. 1

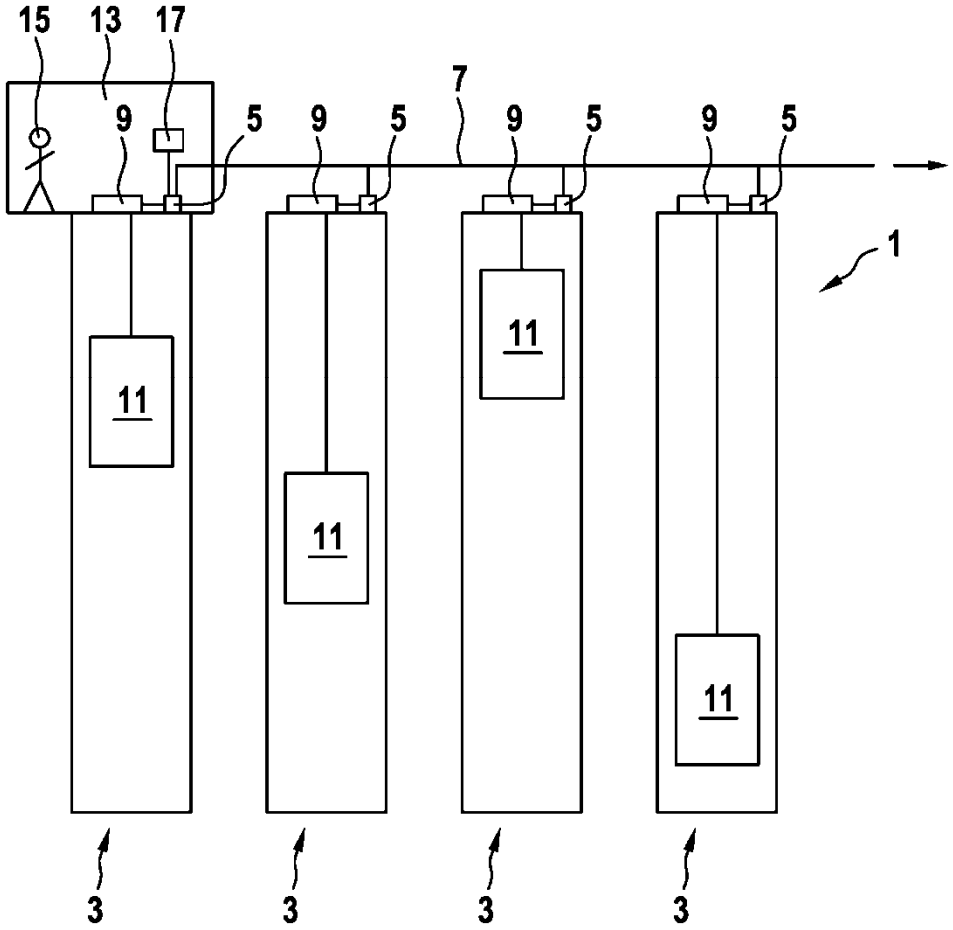

Fig. 2