(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 473 472**

(51) Int. CI.:

G05B 19/418 (2006.01)
H04L 29/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **09.07.2010 E 10007119 (0)**

(97) Fecha y número de publicación de la concesión europea: **07.05.2014 EP 2407843**

(54) Título: **Transmisión segura de datos en una red de automatización**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
07.07.2014

(73) Titular/es:

SIEMENS AKTIENGESELLSCHAFT (100.0%)
Wittelsbacherplatz 2
80333 München, DE

(72) Inventor/es:

KOPPERS, JOACHIM

(74) Agente/Representante:

CARVAJAL Y URQUIJO, Isabel

DESCRIPCIÓN

Transmisión segura de datos en una red de automatización

La invención se refiere a redes de automatización industriales, en particular a la transmisión segura de datos en una red de automatización industrial.

Una red de automatización industrial está constituida normalmente por al menos un aparato de control y al menos un grupo de construcción. El aparato de control sirve para la programación del grupo de construcción y comprende a tal fin una instancia de programada. El grupo de construcción puede ser, por ejemplo, un control de máquinas de una máquina en una línea de producción. Una red de automatización sirve para accionar máquinas o instalaciones industriales automáticamente y sin la colaboración de personas.

Por lo tanto, deben transmitirse datos desde la instancia del programa hacia el grupo de construcción, para que el aparato de control pueda programar el grupo de construcción. Estos datos se llaman datos de proyección. Cuando la transmisión de los datos de proyección desde la instancia del programa hacia el grupo de construcción debe transmitirse a prueba de escucha y protegidos contra manipulaciones, se utiliza normalmente un protocolo de transmisión seguro como HTTPS o IPSEC. Para estos protocolos de transmisión deben cumplirse determinados requerimientos de seguridad, que no pueden ser cumplidos por cualquier red de automatización o bien cualquier grupo de construcción.

Se sabe a partir del documento EP 2 159 653 A1 que para la concesión de una autorización de acceso a un objeto basado en ordenador en un sistema de automatización para un programa de control se determina un identificador y que el identificador es codificado por medio de una clave digital privada asociada a una unidad de control y de supervisión del sistema de automatización. Con la ayuda del objeto basado en ordenador se acondiciona un primer servicio y con la ayuda del programa de control se acondiciona un segundo servicio del sistema de automatización. El identificador codificado es descodificado durante la transmisión a un servicio de autentificación y es verificado a través del servicio de autentificación. El servicio de autentificación transmite, en el caso de verificación con éxito, una señal válida al menos a corto plazo al segundo servicio. La señal es transmitida en el caso de una solicitud de acceso al objeto basado en ordenador a través del programa de control hasta el primer servicio para la verificación. Se concede un acceso al objeto basado en ordenador en el caso de un resultado de verificación positivo por el programa de control.

La invención tiene el cometido de crear un procedimiento mejorado para la transmisión segura de datos en una red de automatización. Además, la invención tiene el cometido de crear un aparato de control mejorado y un grupo de construcción mejorado en una red de automatización y de crear medios de memoria mejorados para tal grupo de construcción y para tal aparato de control.

Los cometidos en los que se basa la invención se solucionan, respectivamente, con las características de las reivindicaciones independientes de la patente.

Las formas de realización de la invención se indican en las reivindicaciones dependientes de la patente.

De acuerdo con la invención se crea un procedimiento para la transmisión segura de datos en una red de automatización. La red de automatización comprende al menos una instancia de programa y al menos un grupo de construcción. La seguridad de la transmisión de los datos se garantiza independientemente del procedimiento de transmisión utilizado.

Una red de automatización puede estar configurada, por ejemplo, como red de automatización industrial. Tales redes de automatización industriales pueden estar configuradas, instaladas y/o previstas, por ejemplo, para el control y/o la regulación de instalaciones industriales (por ejemplo, instalaciones de producción, instalaciones de transporte, etc.), máquinas y/o aparatos. En particular, las redes de automatización o bien redes de automatización industriales pueden presentar protocolos de comunicación en tiempo real, (por ejemplo, Profinet, Profibus, Real-Time-Ethernet) para la comunicación al menos entre los componentes implicados en las tareas de control y/o de regulación (por ejemplo, entre las unidades de control y las instalaciones y/o máquinas a controlar). De la misma manera, está cubierta la transmisión segura de datos a través de medios de memoria.

Además, pero adicionalmente a un protocolo de comunicación en tiempo real, también puede estar previsto todavía otro protocolo de comunicación (que no tiene que ser, por ejemplo, capaz de tiempo real) en la red de automatización o bien red de automatización industrial, por ejemplo para la supervisión, instalación, reprogramación y/o re-parametrización de una o varias unidades de control en el red de automatización.

Una red de automatización puede comprender, por ejemplo, componentes de comunicación por cable y/o componentes de comunicación sin hilos. Además, una red de automatización puede comprender al menos una instalación de automatización.

Una instalación de automatización puede ser, por ejemplo, un ordenador, PC y/o controlador con tareas de control o bien con capacidades de control. En particular, una instalación de automatización puede ser, por ejemplo, una instalación de automatización industrial, que puede estar configurada, instalada y/o prevista, por ejemplo, especialmente para el control y/o regulación de instalaciones industriales. En particular, tales instalaciones de automatización o bien instalaciones de automatización industriales pueden ser capaces en tiempo real, es decir, que posibilitan un control o bien una regulación en tiempo real. A tal fin, la instalación de automatización o bien la instalación de automatización industrial puede comprender, por ejemplo un sistema operativo en tiempo real y/o al menos, entre otras cosas, un protocolo de comunicación capaz de tiempo real para la comunicación (por ejemplo, Profinet, Profibus, Real-Time-Ethernet).

Una red de automatización comprende varios sensores y actuadores. Los actuadores y sensores son controlados por al menos una instalación de control. Los actuadores, los sensores y la al meno una instalación de control intercambian datos entre sí. Para el intercambio de datos se utiliza un protocolo de automatización. La al menos una instalación de control controla los actuadores, los sensores y el intercambio de datos, de tal manera que se desarrolla un proceso de fabricación mecánica, en el que se fabrica, por ejemplo, un producto.

Una instalación de automatización industrial puede ser, por ejemplo, un control programable con memoria, un módulo o parte de un control programable con memoria, un control programable con memoria integrado en un ordenador PC así como aparatos de campo correspondientes, sensores y/o actuadores, aparatos de entrada y/o salida o similares para la conexión en un control programable con memoria o pueden comprender tales componentes.

Como protocolo de automatización en el sentido de la presente invención se entiende cualquier tipo de protocolo, que está previsto, es adecuado y/o está instalado para la comunicación con instalaciones de automatización de acuerdo con la presente descripción. Tales protocolos de automatización pueden ser, por ejemplo, el protocolo Profi-Bus (por ejemplo, de acuerdo con IEC 61158/EN50170), un protocolo prof.-Bus-DP, un protocolo Profi-Bus-PA, un protocolo Prof.-Net, un protocolo Profi-Net-IO, un protocolo según AS-Interface, un protocolo según IO-Link, un protocolo-KNK, un protocolo según una interfaz de varios puntos, (Multipoint-Interface, MPI), un protocolo para un acoplamiento de punto-a-punto (Point-to-Point, PtP), un protocolo según las especificaciones a la S7-Kommunikation (que está prevista e instalada, por ejemplo, para la comunicación de controles programables con memoria de la Firma Siemens) o también un protocolo de Ethernet Industrial, o protocolo Real-Time-Ethernet o bien otros protocolos específicos para la comunicación con aparatos de automatización. Como protocolo de automatización en el sentido de la presente invención pueden estar previstas también combinaciones discrecionales de los protocolos mencionados anteriormente.

La instancia del programa dispone de un sistema de derechos de la instancia del programa y el grupo de construcción dispone de un sistema de derechos de grupos de construcción. El procedimiento comprende las siguientes etapas. En primer lugar se autentifica un usuario de la instancia del programa. Esto se realiza a través del sistema de derechos de la instancia del programa con la ayuda de datos del usuario. Los datos del usuario pueden ser, por ejemplo, un nombre de usuario y una palabra de paso o también otros procedimientos ya conocidos para la autentificación de usuarios a través de sistemas de derechos de la instancia del programa.

El sistema de derechos de la instancia del programa es un sistema de derechos de la instancia del programa. El sistema de derechos de la instancia del programa puede autentificar, por lo tanto, por un lado, a un usuario con la ayuda de los datos del usuario y, por otro lado, puede asignar diferentes derechos a diferentes usuarios. Hay que observar que de la misma manera es posible que se concedan todos los derechos a todos los usuarios autentificados.

El sistema de derechos del grupo de construcción es u sistema de ordenador del grupo de construcción. El sistema de derechos del grupo de construcción puede autentificar de la misma manera, por un lado, aun usuario con la ayuda de los datos del usuario y puede asignar, por otro lado, diferentes derechos a diferentes usuarios. También hay que observar aquí que de la misma manera es posible que se concedan todos los derechos a todos los usuarios autentificados.

Los datos a transmitir son codificados y firmados por la instancia del programa. Por ejemplo, la instancia del programa comprende a tal fin un fichero-DLL firmado o un fichero firmado ejecutable, que está protegido de esta manera contra manipulaciones. Con preferencia, la instancia del programa está equipada para la codificación y firma de los datos con claves asimétricas. Los datos comprenden de la misma manera los datos del usuario. Los datos del usuario son transmitidos codificados y firmados, por lo tanto, junto con los datos de proyección a transmitir hacia el grupo de construcción.

En el grupo de construcción se descodifican los datos. A continuación se lleva a cabo una autentificación de la instancia del programa frente al grupo de construcción. Esto se puede realizar, por ejemplo, porque los datos han sido firmados con una clave privada asimétrica de la instancia del programa y está firma es autentificada en el grupo de construcción a través de una clave pública de la instancia del programa. La firma de los datos se verifica, por lo

tanto, en el grupo de construcción. De esta manera se asegura que no han tenido lugar manipulaciones de los datos y el grupo de construcción ha recibido los datos solamente desde una instancia del programa autorizada para el control del grupo de construcción. A través de la firma con la clave privada de la instancia del programa no es necesaria ninguna transmisión de datos desde el grupo de construcción hacia la instancia del programa, en oposición, por ejemplo al llamado procedimiento de pregunta-respuesta. La instancia del programa es autentificada, sin que deban transmitirse datos desde el grupo de construcción hacia la instancia del programa.

Los datos descodificados comprenden los datos del usuario. El usuario es autentificado con la ayuda de los datos del usuario a través del sistema de derechos del grupo de construcción. Adicionalmente, el usuario puede ser autorizado para la transmisión de datos al grupo de construcción. Por lo tanto, aquí se trata de una autorización posterior. Si se comprobase que el usuario no está autorizado para la transmisión de los datos, se desechan los datos. En otro caso, se utilizan los datos para el control del grupo de construcción. Esta etapa asegura que el usuario anunciado en la instancia del programa está autorizado para la transmisión datos al grupo de construcción. Por lo tanto, no son posibles manipulaciones de los datos y solamente son procesados en el grupo de construcción datos que han sido transmitidos por usuarios autorizados de la instancia del programa al grupo de construcción. La vía de transmisión es totalmente indiferente en este caso. Por lo tanto, se puede tratar también de un canal de transmisión inseguro. A través de la codificación de los datos, la firma de los datos y la transmisión de los datos del usuario al grupo de construcción los datos están protegidos contra cualquier manipulación y se asegura independientemente de la vía de transmisión que los datos no pueden ser interceptados o manipulados.

La seguridad especial de transmisiones de datos de acuerdo con formas de realización de la invención consiste en que los datos del usuario son transmitidos codificados con los datos de proyección desde la instancia del programa hacia el grupo de construcción y se lleva a cabo en el grupo de construcción una autentificación del usuario. Adicionalmente a la autentificación del usuario en la instancia del programa y a la firma y transmisión codificada de los datos resulta una red de automatización protegida contra manipulaciones, la cual ofrece una transmisión segura de datos independientemente de la seguridad del canal de transmisión. De acuerdo con formas de realización de la invención, en la codificación de los datos se trata de una codificación asimétrica.

De acuerdo con formas de realización de la invención, la instancia del programa y el grupo de construcción presentan, respectivamente, una clave pública asimétrica de la instancia del programa y una clave pública asimétrica del grupo de construcción. La instancia del programa presenta, además, una clave privada de la instancia del programa y el grupo de construcción presenta una clave privada del grupo de construcción. Por consiguiente, tanto para la instancia del programa como también para el grupo de construcción existe una pareja de claves, que se utiliza para firmas y codificaciones. Una pareja de claves está constituida, respectivamente, por una clave pública y una clave privada.

Los datos son codificados en la instancia del programa con la clave pública del grupo de construcción y son firmados con la clave privada de la instancia del programa. Hay que observar que los datos comprenden de la misma manera los datos del usuario. Los datos codificados y firmados transmitidos desde la instancia del programa hacia el grupo de construcción son descodificados en el grupo de construcción con la clave privada del grupo de construcción. La autentificación de la instancia de programa como emisor de los datos se realiza con la clave pública de la instancia del programa. La autentificación del usuario de la insania el programa se realiza a través de la evaluación de los datos descodificados.

De acuerdo con formas de realización de la invención, los datos codificados y firmados pueden ser registrados a través de la instancia del programa en un medio de memoria. Antes de la descodificación se leen los datos en el grupo de construcción desde el medio de memoria. El medio de memoria puede ser, por ejemplo, un medio de memoria óptico, magnético y/o digital. De la misma manera se puede tratar de un medio de memoria rotatorio. El medio de memoria puede ser, por ejemplo, un USB-Stick, una tarjeta de memoria o un disco duro. Puesto que los datos están codificados y firmados y los datos del usuario están igualmente registrados al mismo tiempo, no tiene importancia con que seguridad se realice el registro de los datos en el medio de memoria. Los datos están suficientemente protegidos frente a manipulaciones o lectura no autorizada.

Aunque los datos no se transmiten a través de la red de automatización, esta forma de realización representa igualmente un procedimiento para la transmisión segura de datos en una red de automatización. La vía de la transmisión de datos es independiente de la red de automatización.

De acuerdo con formas de realización de la invención, los datos codificados y firmados pueden ser transmitidos a través de una conexión de cable entre la instancia del programa y el grupo de construcción. En este caso, se puede tratar también de una conexión de cable insegura, puesto que los datos están suficientemente asegurados frente a manipulaciones o lectura no autorizada a través de la codificación, la firma y la transmisión simultánea de los datos del usuario.

De acuerdo con formas de realización de la invención, la transmisión de los datos se realiza a través de la conexión por cable por medio de uno de los siguientes protocolos: MPI, Profibus, Ethernet, TCP/IP, Profinet, WLAN.

De acuerdo con formas de realización de la invención, los datos comprenden una clave simétrica para transmisiones de datos codificados desde la instancia del programa hacia el grupo de construcción. Esta clave simétrica se puede utilizar para futuras transmisiones de datos. La utilización de una clave simétrica puede ser ventajosa cuando se trata, por ejemplo, de una red de automatización isocrona determinista. En tal red de automatización es importante que se procesen datos con exactitud en un instante determinado por el grupo de construcción. En este caso, una codificación y descodificación asimétrica de los datos podría durar demasiado tiempo. Por lo tanto, en este caso la clave simétrica con los datos del usuario se transmite codificada y firmada al grupo de construcción y se puede utilizar para transmisiones de datos siguientes.

De acuerdo con formas de realización de la invención, los datos comprenden otra clave privada el grupo de construcción para transmisiones de datos codificados desde la instancia del programa hacia el grupo de construcción. La otra clave privada del grupo de construcción sustituye a la clave privada anterior del grupo de construcción, de manera que en adelante se garantiza una transmisión segura de los datos. Por razones de seguridad, debería sustituirse regularmente una clave privada.

En otro aspecto, la invención se refiere a un aparato de control en una red de automatización. El aparato de control comprende una instancia del programa y la instancia del programa dispone de un sistema de derechos de la instancia del programa. El aparato de control comprende, además, medios para la autentificación de un usuario a través el sistema de derechos de la instancia del programa con la ayuda de datos del usuario para la liberación de una utilización de la instancia del programa a través el usuario, medios para la codificación y firma de datos a través de la instancia del programa, de manera que los datos comprenden los datos del usuario, y medios para la transmisión de los datos a través de un medio de transmisión.

En otro aspecto, la invención se refiere a un grupo de construcción en una red de automatización. El grupo de construcción dispone de un sistema de derechos del grupo de construcción. El grupo de construcción presenta, además, medios para la recepción de datos, medios para la descodificación de datos, medios para la autentificación de un aparato de control como emisor de los datos y medios para la autentificación de un usuario a través el sistema de derechos del grupo de construcción con la ayuda de los datos del usuario para la transmisión de datos al grupo de construcción.

Todavía en otro aspecto, la invención se refiere a un medio de memoria legible por ordenador con instrucciones, que pueden ser ejecutadas en un grupo de construcción en una red de automatización. El grupo de construcción dispone de un sistema de derechos del grupo de construcción. Durante la ejecución de las instrucciones, las instrucciones inducen al grupo de construcción a la ejecución del siguiente procedimiento. En primer lugar se reciben y descodifican los datos. A continuación se autentifica un aparato de control y un usuario es autentificado a través del sistema de derechos del grupo de construcción con la ayuda de los datos del usuario.

Por lo demás, se explican en detalle formas de realización de la invención con referencia a los dibujos. En este caso:

La figura 1 muestra una representación esquemática de una red de automatización con una instancia del programa, con un canal de transmisión y con un grupo de construcción.

La figura 2 muestra una representación esquemática de una red de automatización con una instancia del programa, un grupo de construcción, en el que la transmisión de los datos se realiza con la ayuda de un medio de memoria; y

La figura 3 muestra un diagrama de flujo de un procedimiento para la transmisión segura de datos en una red de automatización.

Los elementos de las siguientes figuras, que se corresponden entre sí, están identificados con los mismos signos de referencia.

La figura 1 es una vista esquemática de una red de automatización 100 con un aparato de control 102 y un grupo de construcción 104. El aparato de control 102 presenta una instancia del programa 106. El aparato de control 102 y el grupo de construcción 104 están conectados por medio de un canal de transmisión discrecional 108. Discrecional significa aquí que el canal de transmisión 108 puede ser también un canal de transmisión inseguro. Para una transmisión segura de los datos, no tiene importancia según la invención el canal de transmisión. El aparato de control 102 comprende una interfaz 109, con lo que el aparato de control 102 está conectado con el canal de transmisión 108 y puede transmitir datos a través del canal de transmisión 108 al grupo de construcción 104. El grupo de construcción 104 comprende una interfaz 111, con lo que el grupo de construcción 104 está conectado con el canal de transmisión 108 y puede recibir datos a través del canal de transmisión 108 desde el aparato de control 102.

La instancia del programa dispone de una clave privada de la instancia del programa 110. Además, la instancia del programa 106 dispone de una clave pública del grupo de construcción 112. El grupo de construcción 104 dispone de una clave privada del grupo de construcción 116. Además, el grupo de construcción dispone de la clave pública de la instancia del programa (no se representa aquí). Las claves públicas están disponibles, por lo tanto, para ambas

unidades. Además, cada una de las unidades dispone de la clave privada respectiva.

A clave pública del grupo de construcción en la instancia del programa 106 es utilizada para la codificación de datos antes de la transmisión desde el aparato de control 102 hacia el grupo de construcción 104. Los datos son firmados, además, con la clave privada de la instancia del programa 110 a través de la instancia del programa 106. a firma es verificada con la clave pública de la instancia del programa en el grupo de construcción 104 después de la transmisión de datos y la instancia del programa 106 es autentificada como emisor de los datos. La decodificación de los datos se realiza con la clave privada del grupo de construcción 116.

Antes de la transmisión de los datos se introducen datos del usuario 118 a través de un usuario en el aparato de control 102. En este caso, se puede tratar, por ejemplo, de datos de solicitud que están constituidos por un nombre de usuario y una palabra de paso. Los datos del usuario 118 son transmitidos a la instancia del programa 106. La instancia del programa 106 transmite los datos del usuario 118 con los datos a transmitir al grupo de construcción 104. Los datos 120 transmitidos desde la instancia del programa 106 hacia el grupo de construcción 104 comprenden, por lo tanto, los datos del usuario 118 y datos de la proyección. Los datos de la proyección son datos que sirven para el control el grupo de construcción 104 a través de la instancia del programa 106.

La figura 2 es una vista esquemática de una red de automatización 200 con un aparato de control 102 y un grupo de construcción 104. El aparato de control 102 presenta, además, una instancia del programa 106. La instancia del programa 106 dispone de una clave privada de la instancia del programa 110. Además, la instancia del programa dispone de la clave pública el grupo de construcción. El grupo de construcción 104 dispone de una clave privada el grupo de construcción 116. Además, el grupo de construcción 104 dispone de la clave pública de la instancia el programa (no se muestra). La transmisión de los datos en le red de automatización 200 desde el aparato de control 102 hacia el grupo de construcción 104 se realiza por medio de un medio de memoria 202. Este puede ser, por ejemplo, una llamada tarjeta multimedia (MMC). En primer lugar se escriben los datos en la tarjeta multimedia 202. Esto se puede realizar, por ejemplo, a través de un procesador 204 el aparato de control 102, que tiene acceso a la tarjeta multimedia 202 y puede provocar el registro de datos en la tarjeta multimedia 202. La tarjeta multimedia 202 es enchufada entonces en un lector de tarjetas (no se representa) el grupo de construcción 104, de manera que un procesador 206 el grupo de construcción 14 tiene acceso a la tarjeta multimedia 202 y puede leer los datos. La descodificación y verificación de los datos se realizan de manera similar al procedimiento ya descrito en la figura 1.

El aparato de control 102 dispone, además, de un medio de memoria 208 legible por ordenador, que registra instrucciones, que puede inducir al aparato de control a la realización del procedimiento descrito anteriormente, cuando se ejecutan las instrucciones, por ejemplo, a través del procesador 204.

El grupo de construcción 104 dispone de la misma manera de un medio de memoria 210, que registra instrucciones, que induce durante la ejecución a través del procesador 206 al grupo de construcción a la realización del procedimiento descrito anteriormente.

La figura 3 muestra un diagrama de flujo de una forma de realización de la invención. En primer lugar se autentifica en la etapa S1 un usuario a través del sistema de derechos de la instancia del programa con la ayuda de datos del usuario. Por lo tanto, se asegura que el usuario esté autorizado para la utilización de la instancia del programa. Esto se realiza, por ejemplo, con un nombre de usuario y una contraseña como datos del usuario. En una segunda etapa S2 se codifican datos a través de la instancia del programa y se firman. Los datos comprenden los datos del usuario. En la etapa S3 se transmiten los datos a través de un medio de transmisión desde la instancia del programa hacia el grupo de construcción y en la etapa S4 se descodifican en el grupo de construcción. La instancia del programa se autentifica en la etapa S5 frente al grupo de construcción como emisor de los datos y en la etapa 6 se autentifica el usuario a través del sistema de derechos del grupo de construcción con la ayuda de los datos del usuario.

Lista de signos de referencia

100 Red de automatización
102 Aparato de control
104 Grupo de construcción
106 Instancia del programa
108 Canal de transmisión
109 Interfaz
110 Clave privada de la instancia del programa
111 Interfaz
112 Clave pública el grupo de construcción
116 Clave privada del grupo de construcción
118 Datos del usuario
120 Datos
200 Red de automatización
202 Medio de memoria

204 Procesador
206 Procesador
208 Medio de memoria
210 Medio de memoria

REIVINDICACIONES

1.- Procedimiento para la transmisión segura de datos en una red de automatización (100), en el que la red de automatización comprende al menos una instancia del programa (106) y al menos un grupo de construcción (104), en el que la instancia del programa dispone de un sistema de derechos de la instancia del programa y el grupo de construcción dispone de un sistema de derechos del grupo de construcción, y en el que el procedimiento comprende la siguientes etapas:

- autentificación (S1) de un usuario a través del programa de derechos de la instancia del programa con la ayuda de datos del usuario para la liberación de una utilización de la instancia del programa a través del usuario;

- codificación (S2) y firma de datos (120) a través de la instancia del programa, en la que los datos comprenden datos del usuario;

- transmisión (S3) de los datos a través de un medio de transmisión (108; 202) desde la instancia del programa hacia el grupo de construcción;

- descodificación (S4) de los datos en el grupo de construcción;

- autentificación (S5) de la instancia del programa frente al grupo de construcción; y

- autentificación (S6) del usuario a través del sistema de derechos del grupo de construcción con la ayuda de los datos del usuario.

2.- Procedimiento de acuerdo con la reivindicación 1, en el que la codificación es una codificación asimétrica.

3.- Procedimiento de acuerdo con la reivindicación 2, en el que la instancia del programa y el grupo de construcción presentan, respectivamente, una clave pública asimétrica de la instancia del programa y una clave pública asimétrica del grupo de construcción (112), y en el que la instancia del programa presenta una clave privada de la instancia del programa (110) y el grupo de construcción presenta una clave privada del grupo de construcción (116), en el que el procedimiento comprende las siguientes etapas:

- codificación simétrica de los datos en la instancia del programa con la clave pública del grupo de construcción y firma de los datos con la clave privada de la instancia del programa;

- transmisión de los datos codificados y firmados desde la instancia del programa hacia el grupo de construcción; y

- descodificación de los datos codificados en el grupo de construcción con la clave privada del grupo de construcción y autentificación de la instancia del programa como emisor de los datos con la clave pública de la instancia del programa.

4.- Procedimiento de acuerdo con una de las reivindicaciones anteriores, en el que los datos codificados y firmados son memorizados a través de la instancia del programa en un medio de memoria (202) y son leídos antes de la descodificación en el grupo de construcción desde el medio de memoria.

5.- Procedimiento de acuerdo con una de las reivindicaciones 1 a 3, en el que los datos codificados y firmados son transmitidos a través de una conexión de cable (108) entre la instancia del programa y el grupo de construcción.

6.- Procedimiento de acuerdo con la reivindicación 5, en el que la transmisión de datos se realiza a través de la conexión por cable por medio de uno de los siguientes protocolos: MPI, PROFIBUS, Ethernet, TCP-IP, PROFINET.

7.- Procedimiento de acuerdo con la reivindicación 5, en el que la transmisión de datos se realiza a través de conexión sin hilos por medio de uno de los siguientes protocolos: Ethernet, TCP-IP, PROFINET.

8.- Procedimiento de acuerdo con una de las reivindicaciones anteriores, en el que los datos comprenden una clave simétrica para transmisiones codificadas de datos desde la instancia del programa hacia el grupo de construcción.

9.- Procedimiento de acuerdo con una de las reivindicaciones 3 a 7, en el que los datos comprenden otra clave privada de grupo de construcción y otra clave pública de la instancia el programa para transmisiones de datos codificadas desde la instancia del programa hacia el grupo de construcción.

10.- Aparato de control (102) en una red de automatización, en el que el aparato de control comprende una instancia del programa y está configurado para la realización de un procedimiento de acuerdo con una de las reivindicaciones 1 a 9, y en el que la instancia el programa dispone de un sistema de derechos de la instancia del programa, con

- medios (208) para la autentificación de un usuario a través del sistema de derechos de la instancia el programa con la ayuda de datos del usuario para la liberación de una utilización de la instancia del programa a través del usuario;

- medios (10; 112; 208) para la codificación y firma de datos a través de la instancia del programa, en el que los datos comprenden datos del usuario; y

- medios (109) para la transmisión de los datos a través de un medio de transmisión.

11.- Grupo de construcción (104) en una red de automatización, en el que el grupo de construcción dispone de un sistema de derechos el grupo de construcción y está configurado para la realización de un procedimiento de acuerdo con una de las reivindicaciones 1 a 9, con:

- medios (111) para la recepción de datos;

- medios (116; 210) para la descodificación de datos;

- medios (114; 210) para la autentificación de un aparato de control como emisor de los datos; y

- medios (210) para la autentificación de un usuario a través del sistema de derechos del grupo de construcción con la ayuda de los datos del usuario.

12.- Red de automatización que comprende un aparato de control, de acuerdo con la reivindicación 10, en el que el aparato de control está configurado para la transmisión de datos a través de un medio de transmisión desde el aparato de control hacia el grupo de construcción, y con un grupo de construcción de acuerdo con la reivindicación 11, en el que el grupo de construcción está configurado para la recepción de los datos transmitidos.

13.- Medio de memoria (206) legible por ordenador con instrucciones, que en la ejecución en un grupo de construcción en una red de automatización, en la que el grupo de construcción dispone de un sistema de derechos del grupo de construcción, inducen al grupo de construcción a la realización del siguiente procedimiento:

- recepción de datos,

- descodificación de datos,

- autentificación de un aparato de control como emisor de los datos; y

- autentificación de un usuario a través del sistema de derechos del grupo de construcción con la ayuda de los datos del usuario,

en el que el medio de memoria legible por ordenador está configurado para la realización de un procedimiento de acuerdo con una de las reivindicaciones 1 a 9.

FIG 1

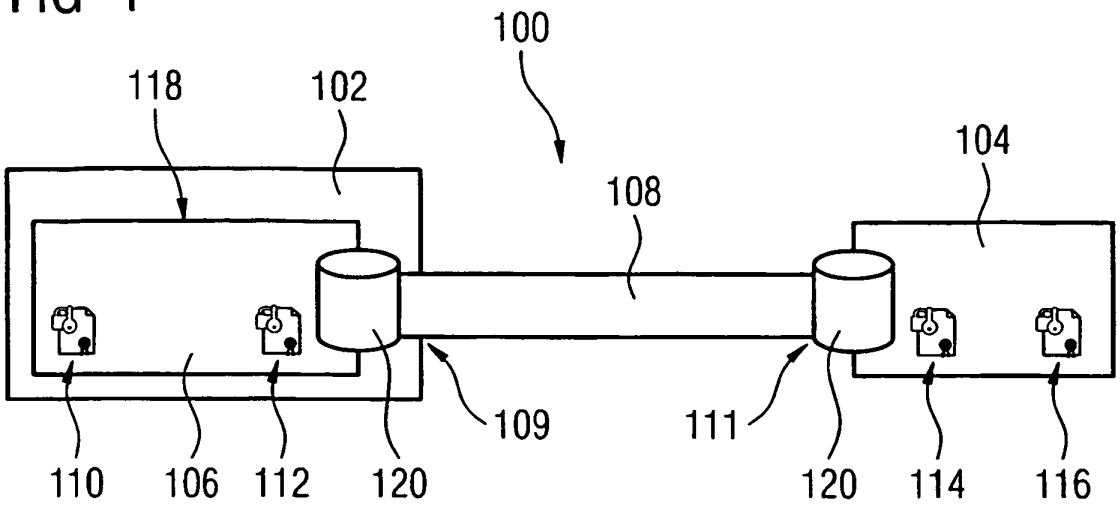
100
118
102
104
108
109
111
110
106
112
120
120
114
116

FIG 2

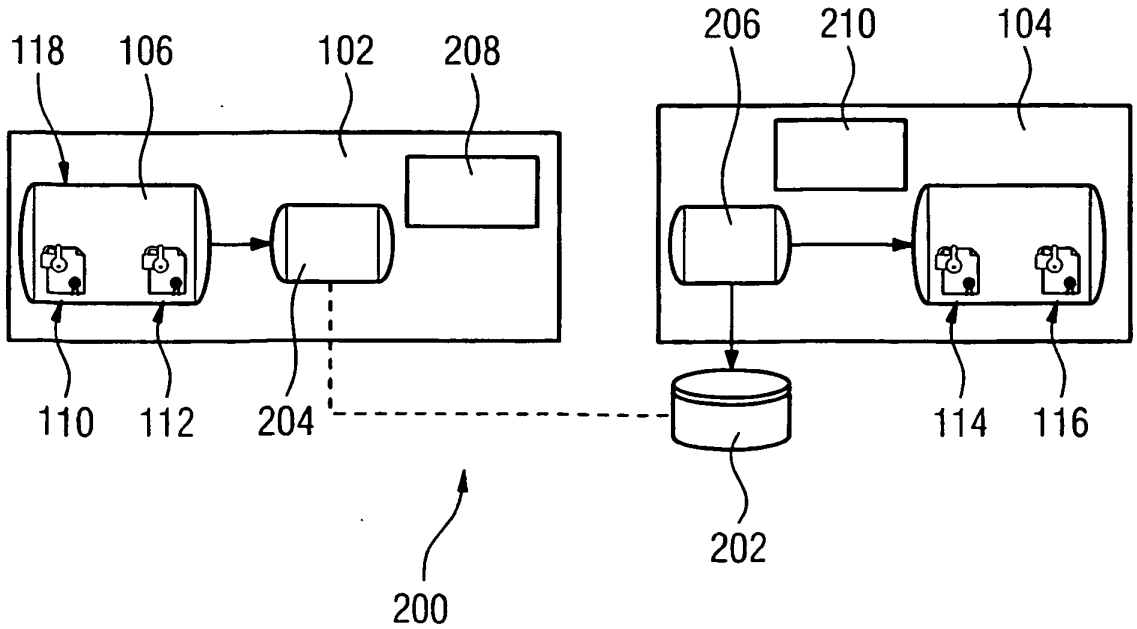
118
106
102
208
206
210
104
110
112
204
114
116
202
200

FIG 3