(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 514 365**

(51) Int. CI.:

G06F 21/31 (2013.01)
G05B 19/042 (2006.01)
G06F 21/32 (2013.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **19.01.2012 E 12151730 (4)**

(97) Fecha y número de publicación de la concesión europea: **13.08.2014 EP 2618226**

(54) Título: **Sistema de automatización industrial y método para su protección**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
28.10.2014

(73) Titular/es:

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

(72) Inventor/es:

AKIL, YAHYA y
MÜLLER, JÖRG

(74) Agente/Representante:

CARVAJAL Y URQUIJO, Isabel

DESCRIPCIÓN

Sistema de automatización industrial y método para su protección

La presente invención hace referencia a un sistema de automatización industrial y a un método para su protección.

Los sistemas de automatización industriales comprenden una pluralidad de procesadores para controlar las máquinas, los sensores, etc. Los sistemas de automatización industriales, debido a razones de seguridad, generalmente consisten en sistemas cerrados, es decir que el acoplamiento de otros componentes (como por ejemplo máquinas, aparatos, procesadores para controlar y actualizar componentes existentes del sistema, etc.), con frecuencia se asocia por tanto a problemas vinculados a la seguridad. En los sistemas de automatización se implementan parcialmente también dispositivos de ese tipo que no respaldan los protocolos de seguridad o los protocolos de autentificación del sistema de automatización. Los dispositivos de ese tipo son potencialmente inseguros y constituyen un posible punto débil para atacantes.

Un ejemplo de un dispositivo inseguro de este tipo de un sistema de automatización es un componente con una interfaz para un dispositivo externo que debe ser conectado al sistema de automatización. El componente puede tratarse por ejemplo de un conmutador o de un puente. Sus interfaces están basadas mayormente en el protocolo Ethernet. El dispositivo que presenta la interfaz para el dispositivo externo, da manera optativa puede estar conectado mediante cableado o de forma inalámbrica con otros componente del sistema de automatización.

Otro ejemplo de dispositivos inseguros son aquellos componentes que no poseen la capacidad para respaldar protocolos de seguridad. Si a un dispositivo de esta clase se conecta mediante la interfaz otro dispositivo externo, como por ejemplo un ordenador, entonces es posible ya un acceso a todos los componentes del sistema de automatización, puesto que no se proporcionan otros mecanismos de seguridad. Debido a ello es posible para un atacante espiar por ejemplo datos de configuración y similares.

Una posibilidad para impedir un acceso no controlado a los componentes del sistema de automatización consiste en poner a disposición un puerto dedicado para un dispositivo inseguro. Puede proporcionarse una pasarela entre el dispositivo inseguro y los componentes del sistema de automatización, donde la pasarela proporciona entonces un puerto para el dispositivo inseguro. Sin embargo, ambas soluciones conducen al problema de que debe proporcionarse un puerto abierto, inseguro, al cual pueda ser conectado el dispositivo inseguro.

Para aumentar la seguridad del sistema de automatización, por la solicitud US 7,314,169 B1 se conoce el hecho de hacer producir por una unidad central un ticket de acceso u otra estructura de datos adecuada para un dispositivo a ser conectado al sistema de automatización, donde el ticket de acceso se basa al menos parcialmente en una característica de identidad de la unidad solicitante. De este modo, en un ticket de acceso a cada unidad solicitante se asocian derechos de acceso. Una desventaja de este método reside en el hecho de que se requiere una gran inversión para la administración.

Es objeto de la presente invención indicar un sistema de automatización industrial y un método para su protección, en donde pueda proporcionarse una seguridad elevada con una inversión reducida para la administración.

Estos objetos se alcanzarán a través de un sistema de automatización industrial según las características de la reivindicación 1 y a través de un método para su protección según las características de la reivindicación 8. En las reivindicaciones dependientes se indican variantes ventajosas.

La presente invención crea un sistema de automatización industrial que comprende una firma digital que se encuentra asociada a una unidad que solicita el acceso al sistema de automatización y que está basada en uno o más parámetros de una comunicación de la unidad con un componente del sistema de automatización, el cual determina la firma digital. El sistema de automatización comprende además el componente que determina la firma digital, el cual durante el funcionamiento del sistema de automatización otorga a la unidad solicitante el acceso al sistema de automatización y compara la firma digital determinada de la unidad solicitante con una firma digital almacenada.

En el método acorde a la invención para proteger el sistema de automatización industrial una firma digital se asocia a una unidad que solicita el acceso al sistema de automatización. La firma digital es determinada en base a uno o más parámetros de una comunicación de la unidad con un componente del sistema de automatización, el cual determina la firma digital. El componente que determina la firma digital compara la firma digital con una firma digital almacenada, otorgando al acceso al sistema de automatización sólo en el caso de una comparación positiva.

El componente que determina la firma digital representa una pasarela para la unidad solicitante, para la conexión al sistema de automatización industrial. Gracias a que el componente que determina la firma digital determina una firma digital de la unidad solicitante puede proporcionarse de forma sencilla una protección de acceso automatizada

con respecto al sistema de automatización. El sistema de automatización es protegido contra diferentes formas de ataque, como por ejemplo ataques activos, ataques desde dentro del sistema de automatización, spoofing (suplantación de identidad), ataques close-in (de proximidad) o ataques de tipo hijacking (secuestro de información). Un puerto abierto, al cual se encuentra comunicado o al cual puede comunicarse la unidad solicitante, tampoco puede ser utilizado para acceder a otros componentes del sistema de automatización sin que haya sido efectuada una verificación y un control previos de la unidad solicitante mediante la firma digital. En particular, a través de la invención es posible conectar al sistema de automatización también aquellas unidades solicitantes que de lo contario no presentan respaldos para protocolos autorizados.

En una primera variante conveniente del sistema de automatización acorde a la invención el componente que determina la firma digital es un nodo terminal del sistema de automatización, al cual puede conectarse la unidad solicitante para intercambiar datos mediante una interfaz predeterminada, especialmente conforme al protocolo Ethernet. El componente que determina la firma digital puede consistir por ejemplo en un puente o en un conmutador que presenta al menos una interfaz para la conexión de la unidad solicitante. En el entorno de los sistemas de automatización por lo general se recurre a conexión según Ethernet, puesto que éste se trata de un estándar muy difundido. De este modo, no sólo es posible conectar dispositivos específicos o máquinas de un sistema de automatización, sino también un procesador, el cual por ejemplo debe utilizarse para tareas de configuración o de control de otros componentes del sistema de automatización.

Según otra variante del sistema de automatización, el componente que determina la firma digital se autentifica al menos una única vez con respecto al sistema de automatización para el intercambio de datos con otros componentes del sistema de automatización. El componente que determina la firma digital representa así un componente seguro del sistema de automatización, el cual dispone de todos los protocolos y mecanismos relevantes para la seguridad. El propio componente, del modo indicado, se encarga de determinar la firma digital de la unidad solicitante y de compararla con una firma digital almacenada, para posibilitar el acceso al sistema de automatización sólo a unidades autorizadas.

En otra variante conveniente, el componente que determina la firma digital se encuentra conectado a otros componentes del sistema de automatización mediante cableado o de forma inalámbrica para el intercambio de datos. En particular en el caso de componentes conectados comunicativamente de forma inalámbrica al sistema de automatización existe el riesgo de que éstos sean utilizados de forma indebida con el fin de un ataque. Por lo tanto, en el caso de componentes de este tipo la protección de acceso propuesta representa una medida particularmente efectiva contra el uso indebido.

De acuerdo con otra variante conveniente la firma digital determinada inicialmente de una de las unidades solicitantes se encuentra almacenada en el componente o en una memoria del sistema de automatización a la cual puede acceder el componente. La comparación efectuada en el marco de la verificación se realiza de este modo entre la firma digital determinada y la firma digital almacenada en la memoria.

En particular, la firma digital almacenada se encuentra asociada a un identificador único de la unidad solicitante, en particular a una dirección MAC. La firma digital almacenada, de modo opcional, puede comprender o no la dirección MAC. En el primer caso la firma digital se encuentra asociada de forma única a una unidad solicitante determinada. Si la dirección MAC no forma parte de la firma digital, entonces la firma digital es válida para un tipo de máquina determinado o para una clase determinada de dispositivos.

En otra variante ventajosa, la firma digital está formada a partir de una cantidad parcial configurable de parámetros de una cantidad total de parámetros de la comunicación de la unidad. Cuantos más parámetros sean procesados en la firma digital, de forma tanto más unívoca y segura puede ser verificada una unidad solicitante determinada. No obstante, puede ser conveniente asignar a un administrador del sistema de automatización la selección de los parámetros en base a una cantidad total de parámetros, para considerar particularidades específicas de un sistema de automatización. Asimismo, en el caso de una cantidad parcial configurable es posible agrupar (to cluster) unidades solicitantes, por ejemplo según tipo de dispositivo, fabricante, etc.

En una variante del método acorde a la invención la unidad que determina la firma digital, al menos después del primer establecimiento de una conexión de comunicación hacia el componente solicitante, intercambia datos predeterminados o datos arbitrarios en el marco de una comunicación con el componente solicitante, determina la firma digital en base a la comunicación y almacena dicha firma digital en el componente o en una memoria del sistema de automatización a la cual puede acceder el componente.

En otra variante, después del establecimiento de una conexión de comunicación del componente solicitante hacia la unidad que determina la firma digital se determina la firma digital del componente, y se controla si dicha firma digital se encuentra almacenada, donde en el caso negativo (es decir cuando la firma digital no fue hallada en la memoria) se controla si en una interfaz de persona - máquina puede determinarse una confirmación positiva de la firma digital determinada, y sólo en el caso de una confirmación positiva tiene lugar un almacenamiento de la firma digital, así como se otorga el acceso al sistema de automatización. La determinación inicial de la firma digital es necesaria para

poder tenerla a disposición como referencia en la memoria del sistema de automatización o en el componente que determina la firma digital. Para asegurarse de que durante la determinación inicial y durante el almacenamiento no pueda realizarse ningún uso indebido se requiere de forma adicional una confirmación mediante una interfaz de persona - máquina. Una confirmación de este tipo puede efectuarse por ejemplo a través de un administrador del sistema de automatización, el cual con su entrada confirma que el componente conectado al sistema de automatización, así como a la unidad, posteriormente debe poder acceder al sistema de automatización de manera autorizada. Para ello, la interfaz de persona - máquina puede estar sometida a mecanismos de seguridad separados, como por ejemplo el ingreso de una contraseña requerida, para que el administrador pueda autentificarse con respecto al sistema de automatización.

En otra variante, la determinación de la firma digital de los componentes conectados a la unidad y la comparación con la firma digital almacenada para el componente son efectuadas por la unidad a intervalos de tiempo predeterminados y/o al presentarse determinados eventos. De este modo, la firma digital no se utiliza sólo para la verificación en la conexión inicial del componente con el sistema de automatización. En lugar de ello, a través de la determinación repetida de la firma digital y de la comparación con la firma digital almacenada puede asegurarse también durante la operación que el componente está autorizado con respecto a un acceso al sistema de automatización y que no fue intercambiado.

De manera conveniente, para determinar además la firma digital se determina una cantidad total de parámetros de la comunicación, donde la firma digital se forma a partir de una cantidad parcial configurable de parámetros de la cantidad total de parámetros de la comunicación de la unidad. Se entiende que la firma digital puede formarse también a partir de todos los parámetros, incluyendo una dirección MAC, del componente solicitante.

De manera conveniente, la cantidad total de parámetros comprende lo siguiente:

- un protocolo usado por el componente para la comunicación con la unidad;

- el puerto de la unidad utilizado por el componente para la comunicación;

- las direcciones consultadas por el componente en el marco de la comunicación;

- la longitud de la trama de datos producida por el componente;

- una duración de tiempo entre la emisión sucesiva de dos tramas de datos;

- una dirección MAC del componente solicitante.

Se entiende que, en principio, para determinar la firma digital del componente solicitante pueden emplearse todos los parámetros que caracterizan la comunicación, así como todas las propiedades de la comunicación. De todas formas, en base a la descripción precedente es evidente para un experto que para determinar la firma digital no es necesario utilizar todos los parámetros indicados, sino que una selección parcial reducida también es suficiente.

Se considera además conveniente que el componente que determina la firma digital se autentifique al menos una única vez con respecto al sistema de automatización para el intercambio de datos con otros componentes del sistema de automatización.

A continuación, la presente invención se describe en detalle mediante un ejemplo de ejecución. Las figuras muestran:

Figura 1: una representación esquemática del desarrollo de la comunicación en un sistema de automatización industrial acorde a la invención, al cual debe conectarse una unidad solicitante; y

Figura 2: una representación esquemática del desarrollo de la comunicación en el sistema de automatización industrial acorde a la invención durante el funcionamiento regular del sistema de automatización.

En el marco de la comunicación para proteger un sistema de automatización industrial, la cual se describe a continuación, esencialmente se encuentran involucrados tres componentes. Una unidad solicitante se encuentra indicada con el símbolo de referencia M. La unidad solicitante M puede consistir por ejemplo en un procesador, por ejemplo para configurar o actualizar los componente del sistema de automatización, o en una máquina o dispositivo que debe ser conectado al sistema de automatización. El símbolo de referencia EK indica un nodo terminal del sistema de automatización. El nodo terminal puede tratarse por ejemplo de un puente o un direccionador (router), al cual puede ser conectada la unidad solicitante M, preferentemente mediante una conexión Ethernet del componente terminal EK. El símbolo de referencia NW indica otros componentes del sistema de automatización, donde NW

puede representar una pluralidad de diferentes componentes individuales que pueden conectarse unos con otros de forma adecuada para el intercambio de datos. La comunicación entre el nodo terminal EK y los otros componentes del sistema de automatización, de manera opcional, puede tener lugar mediante cableado o de forma inalámbrica.

En la siguiente descripción el símbolo de referencia NW indica también la red de automatización. Esta formulación debe entenderse como un sinónimo con respecto a los componentes de la red de automatización.

En un primer paso tiene lugar una autentificación del nodo terminal EK con respecto al resto de los componentes del sistema de automatización NW. Primero el nodo terminal EK transmite una consulta de autentificación AUTH que es procesada por el sistema de automatización NW y que obtiene una respuesta de autentificación AUTH_ACC. En el marco de la autentificación, por ejemplo puede ser intercambiada una información secreta, conocida por el nodo terminal EK, de la red de automatización NW. La autentificación puede tener lugar por ejemplo en el marco de un método de desafío - respuesta (challenge-response) o mediante otros métodos de autentificación conocidos adecuados. Después de realizada la autentificación positiva, el nodo terminal EK se encuentra en condiciones de comunicarse con el sistema de automatización NW. La comunicación puede efectuarse de forma segura, por ejemplo utilizando un protocolo especial.

Asimismo, se parte del supuesto de que un dispositivo (unidad solicitante) M desea acceder, así como ingresar, al sistema de automatización NW. Del modo antes mencionado, la conexión tiene lugar mediante una conexión Ethernet del nodo terminal EK. Tan pronto como el dispositivo M se encuentra conectado al nodo terminal EK tiene lugar una comunicación entre el dispositivo M y el nodo terminal EK. En el marco de la comunicación se intercambian tramas FRM entre el dispositivo M y el nodo terminal EK. De este modo, el nodo terminal EK analiza el tipo de comunicación del dispositivo M. A modo de ejemplo, el nodo terminal EK determina con qué protocolo se comunica el dispositivo M. Se verifica además por ejemplo qué puertos son utilizados por el dispositivo M durante la comunicación con el nodo terminal EK. Es posible verificar qué direcciones son consultadas por el dispositivo M en el marco de la comunicación. Otra característica que describe la comunicación hace referencia a la longitud de la trama de datos FRM producida por el componente, así como a la duración de tiempo entre las emisiones consecutivas entre dos tramas de datos. La dirección MAC del dispositivo M es igualmente identificada por el nodo terminal EK. En base a la comunicación pueden extraerse además otros aspectos de la comunicación. A partir de todos o de una parte de estos parámetros, el nodo terminal EK forma una firma digital (B FP) que es almacenada por el nodo terminal EK (S FP). Para ello puede proporcionarse una memoria propia dentro del nodo terminal EK. Puede utilizarse igualmente una memoria del sistema de automatización NW a la cual puede acceder comunicativamente el nodo terminal EK.

Para asegurar que sólo sean almacenadas aquellas firmas digitales del dispositivo M que después deban ser autorizadas de manera efectiva, accediendo a la red del sistema de automatización NW, la autenticidad de un dispositivo M puede ser confirmada por ejemplo por un administrador del sistema de automatización. A modo de ejemplo, la conexión a ser efectuada entre el dispositivo M y el nodo terminal EK puede ser efectuada por el administrador, donde puede efectuarse una confirmación correspondiente mediante una interfaz de persona - máquina, la cual es leída por el nodo terminal EK. A este respecto se considera conveniente que el administrador del sistema de automatización NW se autentifique a su vez con relación al sistema de automatización NW o al nodo terminal EK.

Tan pronto como es almacenada una firma digital de un dispositivo M, a través del nodo terminal EK un mensaje COM_ACC se transmite al dispositivo M conectado, de manera que desde ese momento se autoriza una comunicación con el sistema de automatización NW. A continuación el dispositivo M puede intercambiar tramas de datos FRM con el sistema de automatización NW.

Al almacenar una firma digital ésta preferentemente es asignada a una dirección MAC, es decir a un identificador único del dispositivo M. La firma digital en sí misma puede por su parte comprender la dirección MAC, de manera que la firma digital sea única para cada respectivo dispositivo. Del mismo modo, la dirección MAC puede formar parte de la firma digital, de manera que una firma digital sea válida para una clase de máquina, para un determinado tipo de dispositivos y similares. Esto tiene como consecuencia que una máquina con el mismo tipo de construcción, la cual presenta propiedades de comunicación idénticas a las de aquella máquina que se encontraba conectada al nodo terminal durante la primera determinación y almacenamiento de la firma digital, pueda acceder igualmente al sistema de automatización. Por ejemplo, esto puede considerarse como ventajoso cuando, debido a un defecto, un dispositivo debe ser reemplazado por un dispositivo con el mismo tipo de construcción.

En principio se considera conveniente almacenar todos los parámetros determinados que podrían ser utilizados para formar la firma digital. Cuáles de los parámetros se utilizan después para determinar la firma digital puede ser establecido por ejemplo a través de un administrador del sistema de automatización NW o a través de un archivo de configuración predeterminado.

La figura 2 muestra el desarrollo de la comunicación después de que una firma digital ha sido almacenada para el dispositivo M. En primer lugar se efectúa nuevamente una autentificación del nodo terminal EK con respecto al

sistema de automatización NW, a través del intercambio de una consulta de autentificación AUT y de una respuesta correspondiente a través de una respuesta de autentificación AUTH_ACC. A continuación tiene lugar la comunicación antes mencionada entre el dispositivo M y el nodo terminal EK, donde a su vez se genera una firma digital (B_FP). Al continuar el desarrollo puede tener lugar una comunicación entre el dispositivo M y el sistema de automatización NW. De este modo se ejecutan repetidamente pasos sucesivos, indicados con el símbolo de referencia L, donde L hace referencia a "loop" (bucle), gracias a lo cual se realiza una repetición regular de los pasos descritos. La comunicación realizada entre el dispositivo M y el sistema de automatización NW se efectúa mediante el nodo terminal EK que actúa como pasarela. Debido a ello, al nodo EK se le brinda la posibilidad de analizar las propiedades de comunicación del dispositivo M y de determinar su firma digital (B_FP). A continuación se efectúa una comparación de la firma digital determinada con la firma digital (COMP_FP) contenida en la memoria para el dispositivo. Por ello se utiliza la dirección MAC del dispositivo M, para poder determinar la firma digital asociada desde la memoria. Si la comparación es positiva (véase el símbolo de referencia A, "ALT"), entonces la comunicación puede ser mantenida. Si durante la comparación (véase el símbolo de referencia E, "Else") se determina que la firma digital determinada no está contenida en el banco de datos de la memoria, entonces desde el nodo terminal EK se transmite un mensaje STP al dispositivo M, el cual le indica al mismo la interrupción del acceso al sistema de automatización. Tiene lugar una interrupción de la conexión de comunicación entre el dispositivo M y el sistema de automatización NW. Esto se indica con el símbolo de referencia DCT.

La verificación de la firma digital del dispositivo M y su comparación con una firma digital almacenada para la dirección MAC según el bucle L se efectúa preferentemente de forma periódica. De este modo, también durante el funcionamiento puede efectuarse la verificación de la confirmación del dispositivo M con respecto a la comunicación con el sistema de automatización.

En el marco de la transmisión del mensaje STP desde el nodo terminal EK hacia el dispositivo M puede tener lugar también una señalización de alarma, de manera que por ejemplo se puede advertir a un administrador sobre la no coincidencia de la firma digital de un dispositivo M conectado con firmas digitales almacenadas de dispositivos conocidos. Una señalización puede efectuarse en forma de un correo electrónico, de un aviso de alarma o similares.

REIVINDICACIONES

1. Sistema de automatización industrial, el cual comprende

- una firma digital que se encuentra asociada a una unidad (M) que solicita el acceso al sistema de automatización (NW) y que está basada en uno o más parámetros de una comunicación de la unidad (M) con un componente (EK) del sistema de automatización (NW), el cual determina la firma digital;

- el componente (EK) que determina la firma digital, el cual durante el funcionamiento del sistema de automatización (NW) otorga a la unidad (M) solicitante el acceso al sistema de automatización (NW) y compara la firma digital determinada de la unidad (M) solicitante con una firma digital almacenada.

2. Sistema de automatización según la reivindicación 1, donde el componente (EK) que determina la firma digital es un nodo terminal del sistema de automatización (NW), al cual puede conectarse la unidad (M) solicitante para intercambiar datos mediante una interfaz predeterminada, especialmente conforme al protocolo Ethernet.

3. Sistema de automatización según la reivindicación 1 ó 2, donde el componente (EK) que determina la firma digital se autentifica al menos una única vez con respecto al sistema de automatización (NW) para el intercambio de datos con otros componentes del sistema de automatización (NW).

4. Sistema de automatización según una de las reivindicaciones precedentes, donde el componente (EK) que determina la firma digital se encuentra conectado con otros componentes del sistema de automatización (NW) mediante cableado o de forma inalámbrica para el intercambio de datos.

5. Sistema de automatización según una de las reivindicaciones precedentes, donde la firma digital determinada inicialmente de una de las unidades (M) solicitantes se encuentra almacenada en el componente (EK) o en una memoria del sistema de automatización (NW) a la cual puede acceder el componente (EK).

6. Sistema de automatización según la reivindicación 5, donde la firma digital almacenada se encuentra asociada a un identificador único de la unidad (M) solicitante, en particular a una dirección MAC.

7. Sistema de automatización según una de las reivindicaciones precedentes, donde la firma digital está formada a partir de una cantidad parcial configurable de parámetros de una cantidad total de parámetros de la comunicación de la unidad (M).

8. Método para proteger un sistema de automatización industrial, donde

- una unidad (M) que solicita el acceso al sistema de automatización (NW) se encuentra asociada a una firma digital;

- la firma digital es determinada en base a uno o más parámetros de una comunicación de la unidad (M) con un componente (EK) del sistema de automatización (NW), el cual determina la firma digital;

- el componente (EK) que determina la firma digital compara la firma digital determinada con una firma digital almacenada, otorgando al acceso al sistema de automatización (NW) sólo en el caso de una comparación positiva.

9. Método según la reivindicación 8, donde la unidad (EK) que determina la firma digital, al menos después del primer establecimiento de una conexión de comunicación hacia el componente (M) solicitante, intercambia datos predeterminados o datos arbitrarios en el marco de una comunicación con el componente solicitante, determina la firma digital en base a la comunicación y almacena dicha firma digital en el componente (EK) o en una memoria del sistema de automatización (NW) a la cual puede acceder el componente (EK).

10. Método según la reivindicación 9 ó 10, donde después del establecimiento de una conexión de comunicación del componente (M) solicitante hacia la unidad (EK) que determina la firma digital se determina la firma digital del componente (M), y se controla si dicha firma digital se encuentra almacenada, donde en el caso negativo se controla si en una interfaz de persona - máquina puede determinarse una confirmación positiva de la firma digital determinada, y sólo en el caso de una confirmación positiva tiene lugar un almacenamiento de la firma digital, así como se otorga el acceso al sistema de automatización (NW).

11. Método según una de las reivindicaciones 8 a 10, donde la determinación de la firma digital de los componentes (M) conectados a la unidad (EK) y la comparación con la firma digital almacenada para el componente (M) son efectuadas por la unidad (EK) a intervalos de tiempo predeterminados y/o al presentarse determinados eventos.

12. Método según una de las reivindicaciones 8 a 11, donde para determinar la firma digital se determina una cantidad total de parámetros, donde la firma digital se forma a partir de una cantidad parcial configurable de parámetros de la cantidad total de parámetros de la comunicación de la unidad (M).

13. Método según la reivindicación 12, donde la cantidad total de parámetros comprende lo siguiente:

- un protocolo usado por el componente (M) para la comunicación con la unidad (EK);

- el puerto de la unidad (EK) utilizado por el componente (M) para la comunicación;

- las direcciones consultadas por el componente (M) en el marco de la comunicación;

- la longitud de la trama de datos producida por el componente (M);

- una duración de tiempo entre la emisión sucesiva de dos tramas de datos;

- una dirección MAC del componente.

14. Método según una de las reivindicaciones 8 a 13, donde el componente (EK) que determina la firma digital se autentifica al menos una única vez con respecto al sistema de automatización (NW) para el intercambio de datos con otros componentes del sistema de automatización (NW).

FIG 1

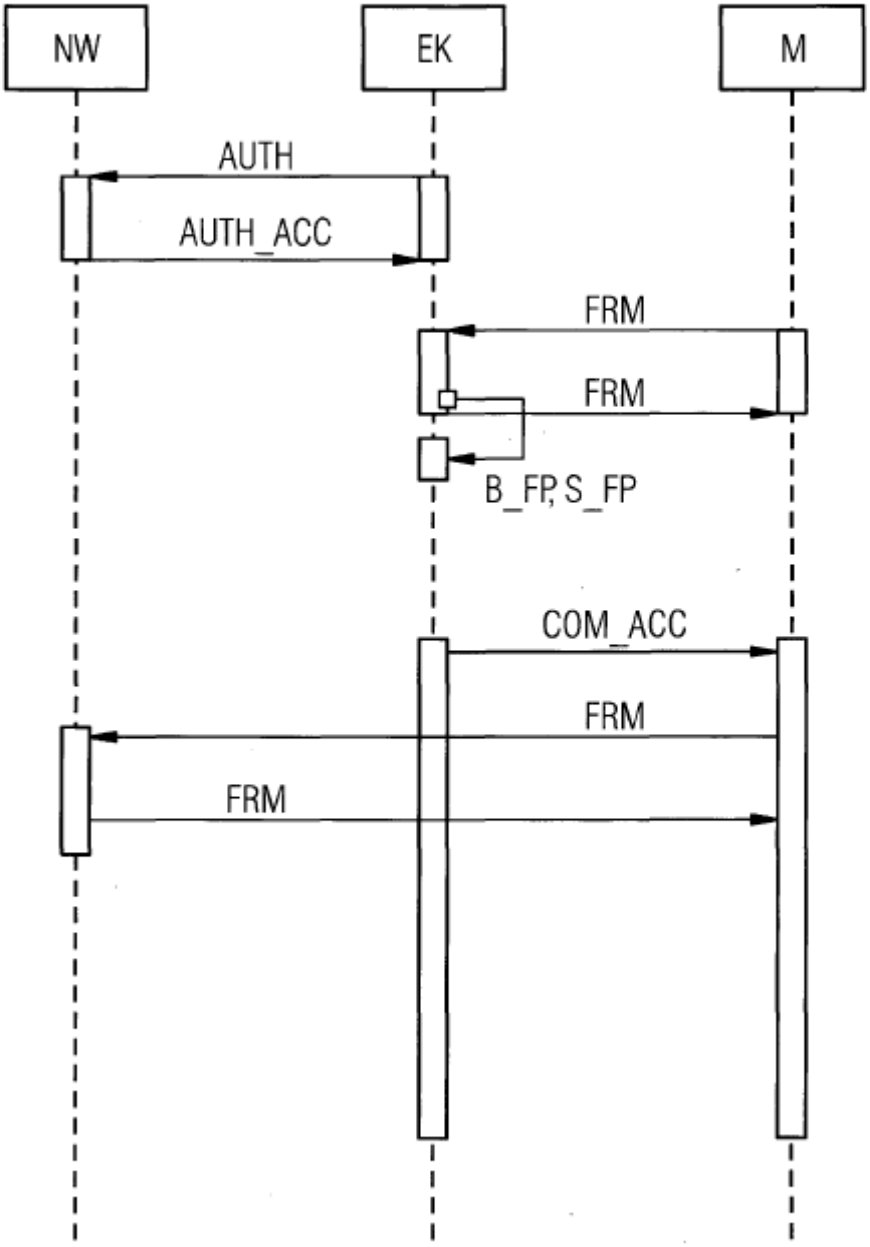
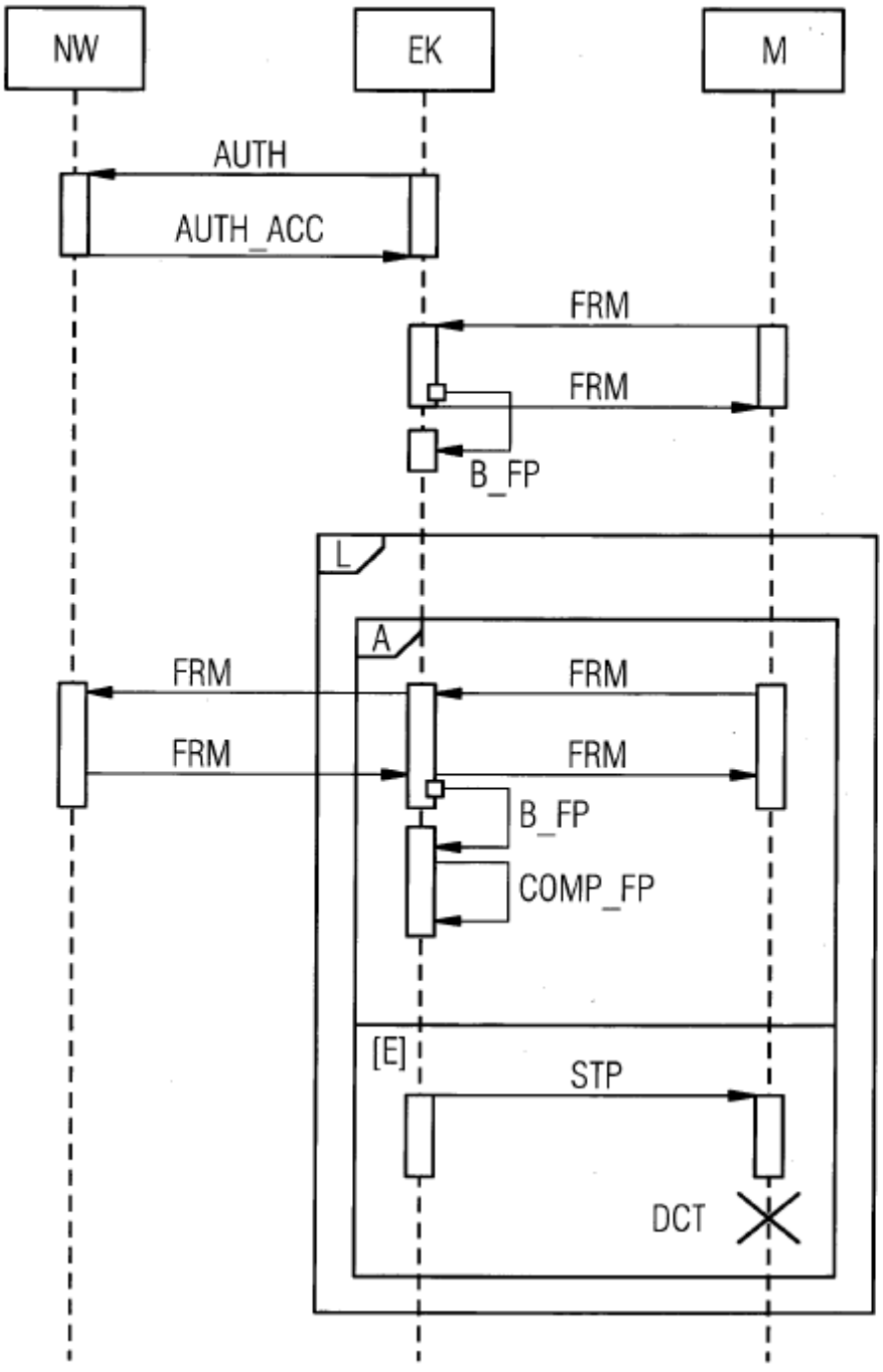


FIG 2


NW
EK
M
AUTH
AUTH_ACC
FRM
FRM
B_FP
L
A
FRM
FRM
FRM
FRM
B_FP
COMP_FP
[E]
STP
DCT