(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 315 343**

(51) Int. Cl.:
H04M 11/00 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **02405270 .6**
(96) Fecha de presentación : **05.04.2002**
(97) Número de publicación de la solicitud: **1351480**
(97) Fecha de publicación de la solicitud: **08.10.2003**

(54) Título: **Métodos para el control a distancia de un sistema.**

(45) Fecha de publicación de la mención BOPI:
01.04.2009

(45) Fecha de la publicación del folleto de la patente:
01.04.2009

(73) Titular/es: **ABB Research Ltd.**
Affolternstrasse 52
8050 Zürich, CH

(72) Inventor/es: **Straub, Florian;**
Von Hoff, Thomas;
Crevatin, Mario y
Züger, Hans Peter

(74) Agente: **Ungría López, Javier**

DESCRIPCIÓN

Método para el control a distancia de un sistema.

Campo técnico

La invención se refiere al ámbito del control y/o de la regulación de sistemas situados en un sitio alejado. Se refiere a un método para el control y/o regulación a distancia de un sistema, particularmente de una instalación industrial, de acuerdo con el preámbulo de la reivindicación independiente.

Estado de la técnica

Las posibilidades de una supervisión, un control y/o una regulación a distancia son un factor cada vez más importante durante la concepción de todo tipo de sistemas, particularmente en instalaciones industriales e instalaciones de suministro, a modo de ejemplo, en los ámbitos de electricidad, agua y calor. Tales posibilidades permiten aumentos de eficacia y flexibilidad en un funcionamiento y mantenimiento de los sistemas, particularmente desde el punto de vista de prestaciones de atención al cliente y de servicios, sin embargo, también en un funcionamiento normal de sistemas más complejos, en el caso de que se requiera una intervención frecuente del personal de servicio para un funcionamiento sin problemas de los sistemas. Un aspecto de la supervisión y el control a distancia se refiere a una transmisión de una información que se refiere al sistema, a modo de ejemplo, en forma de un aviso o una alarma y una transmisión de retorno posterior de una información de orden como reacción del personal de servicio.

El documento EP 617350 describe métodos para el control a distancia de instalaciones de calefacción o de aire acondicionado así como para el autodiagnóstico con transmisión a distancia de resultados de diagnóstico. En el autodiagnóstico se detectan, procesan, codifican datos relevantes para el diagnóstico de la instalación de calefacción o de aire acondicionado por un equipo de comunicación y, después del establecimiento de una conexión de datos, se transmiten como informaciones de diagnostico a un equipo de recepción externo, donde se reciben, descodifican y finalmente se procesan, indican, imprimen y/o almacenan. Durante el control a distancia se establece en primer lugar una conexión de datos desde un equipo de órdenes externo con el equipo de comunicación y a continuación se codifica una información de orden en el equipo de orden, se transmite al equipo de comunicación, se recibe y descodifica en ese lugar y finalmente se procesa y/o ejecuta en el equipo de comunicación y/o un equipo de control y/o regulación de la instalación de calefacción o de aire acondicionado. Una transmisión de informaciones de diagnóstico y/u órdenes se puede producir por una línea directa, sin embargo, también es posible utilizar sistemas de transmisión de información convencionales existentes, por ejemplo, sistemas de telecomunicaciones de correos, teléfono, fax, radio búsqueda (Cityruf) y similares para la transmisión.

Una problemática en sistemas controlables y/o regulables a distancia es el riesgo de una intervención en el sistema por no autorizados. En el caso de que el equipo de comunicación presente una conexión con una red pública, a modo de ejemplo, un sistema de telecomunicaciones de correos, se puede establecer una conexión con el equipo de comunicación por no autorizados sin mayores dificultades. Si se conoce un protocolo para una codificación/descodificación de la información de orden, los no autorizados pueden transmitir de forma muy sencilla informaciones de órdenes al equipo de comunicación. Si las mismas se ejecutan correspondientemente por el equipo de control y/o regulación, se pueden producir fallos o incluso daños en el sistema, dependiendo del sistema, en circunstancias incluso una puesta en peligro o daño del entorno y del medio ambiente. Por lo tanto, en el documento EP 617350 se propone realizar en el equipo de comunicación antes de la propia entrada de informaciones de órdenes una autentificación de usuario. Para esto se tiene que introducir una contraseña o un número de identificación, que contengan la autorización del acceso al equipo de comunicación y, por tanto, al sistema.

Mientras que por una autentificación de usuario se puede evitar considerablemente el riesgo de un acceso por no autorizados, sin embargo, todavía permanece un determinado riesgo residual. Esto es particularmente el caso cuando los no autorizados conocen o pueden conocer la contraseña o el número de identificación.

Además de esto, los denominados ataques por piratas informáticos (hacker) representan un riesgo particular. Estos son ataques por no autorizados, que tienen como objetivo averiguar por intentos repetidos la contraseña y/o el número de identificación. Sobre todo los sistemas cuyos equipos de comunicación presentan conexiones con redes informáticas, están particularmente en riesgo en este caso, ya que el ataque del pirata informático se puede automatizar con ayuda de programas y/o guiones informáticos, de tal forma que en el intervalo de un tiempo breve se puede realizar un gran número de intentos para averiguar la contraseña y/o el número de identificación.

La invención se refiere a un método para el control y/o la regulación a distancia de aparatos de acuerdo con el documento WO 01/72012. En el método descrito se envía por el sistema por un equipo de comunicación una comunicación con un código de validación a un receptor. El receptor puede usar el código de validación para proporcionar un código de control a un mensaje al sistema. En el sistema se puede extraer el código de control del mensaje y se puede comprobar mediante el código de validación y el código de control la autenticidad del mensaje. Ya que el código de validación y el código de control sirven para la autentificación de mensajes y son independientes de las direcciones de los aparatos receptores, en el caso necesario se puede usar el mismo código de validación y código de control para aparatos diferentes.

En el documento WO 01/48722 se describe un módulo de telemetría controlable a distancia, que está diseñado como identificador y aparato de control. Si el aparato recibe un mensaje, las órdenes de control contenidas en el mismo solamente se tienen que ejecutar cuando el mensaje se envió por una persona autorizada. Para esto se comprueba si al menos una parte del número de llamada del emisor coincide con un número de llamada de autorización almacenada. Esto presupone que la red de comunicación permite la transmisión del número de llamada del emisor. La identificación de emisor se produce independientemente del mensaje que se tiene que transmitir y tampoco se puede encriptar con el mismo o independientemente del mismo. Por lo tanto, este tipo de detección de emisor y autorización ofrece solamente una medida reducida de seguridad.

En la Patente de Estados Unidos Nº 6.201.996 B1 se describen un método y un dispositivo para el control a distancia de una instalación industrial por internet. Para la seguridad del usuario se describe un acceso protegido por contraseña a la página web del equipo de comunicación, un encriptado de los datos que se tienen que transmitir por la red y una autentificación adecuada de usuario, con los que el usuario obtiene derecho de acceso a una página web reglada, por la que puede controlar a distancia la instalación. La identificación de emisor no es ningún componente integral del mensaje que se tiene que transmitir a la página web. Más bien, la autentificación de usuario, a su vez, se realiza antes de un acceso a los datos o mecanismos de control que se tienen que proteger e independientemente de los datos que se tienen que proteger o informaciones de órdenes.

En el documento EP 0 930 792 se describe un sistema y un método para la transmisión inalámbrica de datos de estado a una interfaz de aparato. Para evitar el mal uso se pueden enviar datos de identificación del emisor con el mensaje. Con este propósito se transmite, a modo de ejemplo, el número de teléfono del emisor del mensaje.

Descripción de la invención

Por lo tanto, es objetivo de la invención indicar un método para el control y la regulación a distancia de sistemas, que minimice de forma eficaz el riesgo de una manipulación por no autorizados y particularmente de ataques de piratas informáticos.

Adicionalmente es objetivo de la invención indicar un método seguro para el control y/o la regulación a distancia de un sistema, que trabaje sin la necesidad de una autentificación de usuario que se produce antes de la propia transmisión de una información de órdenes y que, por tanto, sea sencillo y eficaz.

Estos objetivos se resuelven mediante un método de acuerdo con la reivindicación 1 y la reivindicación 4. Una comunicación, que comprende una información que se refiere al sistema y un código de validación, se envía por un equipo de comunicación asignado al sistema, preferiblemente un equipo de recepción determinado de antemano. En cuanto el equipo de comunicación recibe un mensaje en un momento después del envío de la comunicación, se extrae de este mensaje de acuerdo con una regla predefinida un código de control. Mediante el código de validación y el código de control se comprueba, teniendo en cuenta la regla predefinida, un origen del mensaje, es decir, se comprueba si el mensaje procede de un receptor de la comunicación. De este modo es posible verificar mediante el código de validación y el código de control si el mensaje recibido representa una respuesta a la comunicación enviada.

El código de validación presenta una validez limitada en el tiempo y al código de validación se añade una información de validez, por la que se define la limitación en el tiempo de la validez del código de validación.

En una primera realización se añade directamente la información de validez al código de validación, se transmite el código de validación de forma encriptada y después de una desencriptación del mensaje o del código de control en el equipo de comunicación, la información de validez se vuelve a presentar en un texto comprensible.

En una segunda realización, durante un envío de la comunicación se almacena una copia del código de validación, para estar disponible para la comparación durante la posterior recepción de un mensaje, y una información de validez, por la que se define la limitación en el tiempo de la validez del código de validación, se almacena junto con el código de validación.

Solamente en los casos en los que se comprobó de forma exitosa que el mensaje procede de un receptor de la comunicación se extrae del mensaje recibido adicionalmente al código de control de acuerdo con la regla predefinida una información de órdenes y se procesa y/o ejecuta por el sistema.

En el caso de que, por el contrario, no se pudiera verificar mediante el código de validación y el código de control que el mensaje recibido representa una respuesta a la comunicación enviada, la información de órdenes no se extrae del mensaje o la información de órdenes extraídas se ignora.

Estos y otros objetivos, ventajas y características de la invención son evidentes a partir de la siguiente descripción detallada de un ejemplo de realización preferido de la invención en relación a los dibujos.

Breve descripción del dibujo

La Figura 1 muestra esquemáticamente un diagrama de bloques de un sistema controlable y/o regulable a distancia con el método de acuerdo con la invención.

Las referencias usadas en el dibujo y su significado se resumen en la lista de referencias.

Modos de realizar la invención

La Figura 1 muestra esquemáticamente un diagrama de bloques de un sistema 1, que es controlable y/o regulable a distancia por un equipo de comunicación 2, que presenta una interfaz de sistema 22 y una interfaz de red 21, y un equipo de recepción 3 según el método de acuerdo con la invención. La interfaz de red 21 dispone de al menos respectivamente un medio para e envío o la recepción de comunicaciones o mensajes.

Los datos que se refieren al sistema se almacenan y, en un caso dado, procesan en el equipo de comunicación 2, una instalación de procesamiento de datos conectada y/o una subunidad del sistema 1. Los datos pueden referirse directamente o indirectamente al sistema 1. Pueden ser, por un lado, parámetros de funcionamiento como, por ejemplo, temperaturas, presiones, cantidades de paso de sustancias, parámetros de configuración como posiciones de conmutadores o válvulas, por otro lado, también parámetros del entorno, como, a modo de ejemplo, temperaturas del entorno o similares. Se puede tratar, como en los ejemplos que se han mencionado anteriormente, de datos individuales, que se pueden expresar por un valor numérico individual, ventajosamente, sin embargo, también de conjuntos de datos complejos, pre-procesados por una subunidad del sistema. Los datos se agrupan finalmente hasta formar una información. La información puede consistir solamente en una fecha individual, puede consistir en una pluralidad de datos o ser incluso el resultado de un análisis de datos que se realizó en el equipo de comunicación 2, la instalación de procesamiento de datos conectada o el propio sistema 1.

Una comunicación, que contiene la información, se transmite al cumplir determinadas condiciones por el equipo de comunicación 2 por la interfaz de red 21 a un equipo de recepción 3. La condición para una transmisión de una comunicación es preferiblemente un error diagnosticado durante la evaluación de los datos en el sistema 1. Sin embargo, también se puede concebir que una comunicación se transmita independientemente de un estado del sistema 1, a modo de ejemplo, cuando un parámetro que se refiere indirectamente al sistema 1, como la temperatura del entorno, sobrepasa o pasa por debajo de un determinado valor umbral. En las situaciones mencionadas, la transmisión de la comunicación representa por así decirlo una alarma. Sin embargo, ventajosamente, la comunicación también se puede transmitir en una fija, en un día fijo o en fechas determinadas de antemano.

A la comunicación se añade un código de validación por el equipo de comunicación 2. Con este propósito, la información y el código de validación se agrupan de acuerdo con una primera regla de combinación. Ventajosamente, esto se produce por una conexión de información y código de validación. Si la información y el código de validación consisten en secuencias de caracteres, durante la conexión se intercalan ventajosamente signos de control o especiales predefinidos como separador.

Preferiblemente, una validez del código de validación es única y está sometida a una limitación en el tiempo. El código de validación se genera de un modo adecuado, a modo de ejemplo, por un generador de números aleatorios, de tal forma que los no autorizados no lo pueden predecir. La limitación en el tiempo y validez única dificultan una manipulación del sistema 1 por no autorizados en los casos en los que se conoce el código de validación.

El método de acuerdo con la invención continúa en cuanto el equipo de comunicación 2 recibe un mensaje por la interfaz de red 21. Después, el equipo de comunicación 2 extrae de acuerdo con una primera regla de extracción un código de control del mensaje. A continuación se comprueba un origen del mensaje recibido mediante el código de validación y del código de control. Ventajosamente se usa con este propósito un código de control que es idéntico al código de validación. La comprobación del origen se realiza entonces por una comparación del código de validación y el código de control. Para esto, durante un envío de la comunicación se tiene que almacenar una copia del código de validación para estar disponible para la comparación durante la recepción posterior de un mensaje. Una limitación en el tiempo de la validez del código de validación se posibilita en este caso ventajosamente almacenando una información de validez junto con el código de validación. Sin embargo, también se puede utilizar ventajosamente una comprobación sin conocimiento explícito del código de validación. De este modo, entre otras cosas se puede recurrir a propiedades determinadas del código de validación para la comprobación, a modo de ejemplo, la suma de sus cifras. El código de control se tiene que comprobar entonces solamente con respecto a estas propiedades, en el ejemplo, la suma de las cifras.

Además del código de control, del mensaje se extrae además de acuerdo con la primera regla de extracción una información de orden. Solamente con una comprobación exitosa mediante el código de validación y de control se transmite la información de orden por el equipo de comunicación 2 con el propósito de una ejecución por la interfaz del sistema 22 al sistema 1, en un caso dado, después de un procesamiento anterior. Preferiblemente, entre el equipo de comunicación 2 y el sistema 1 se proporciona un equipo de control, al que se proporciona la información de orden y desde donde se transmite al sistema 1. Si la comprobación no fue exitosa, la información de orden se ignora.

La primera regla de extracción preferiblemente está compuesta de tal forma que el código de control y la información de órdenes se extraen por un recorte de subzonas del mensaje.

Como se obtiene a partir de las anteriores explicaciones, un uso del método de acuerdo con la invención garantiza que solamente un receptor de la comunicación, y por tanto, del código de validación, es capaz de enviar órdenes para el control y/o la regulación a distancia del sistema 1. Para hacer esto, el receptor tiene que extraer de acuerdo con una segunda regla de extracción, que representa una inversión de la primera regla de combinación, en primer lugar el código de validación de la comunicación. A partir de las órdenes, que tiene intención de enviar, puede generar junto con el código de validación conociendo la primera regla de extracción un mensaje, del cual, el equipo de comunicación 2, después de que haya recibido este mensaje, extrae un código de control, que conduce a la comprobación exitosa del mensaje y, por tanto, a la extracción y transformación de la información de órdenes. Para esto tiene que utilizar una segunda regla de combinación que garantice esto.

En una configuración preferida adicional del método de acuerdo con la invención se extrae del mensaje de acuerdo con una tercera regla de extracción una información de emisor. En el equipo de comunicación 2 se comprueba la información de emisor y solamente en el caso de una identificación de emisor exitosa, es decir, una coincidencia de la información de emisor con los datos de emisor almacenados de usuarios autorizados, se transmite y/o procesa la información de órdenes por el equipo de comunicación 2 al sistema 1. Preferiblemente, la información de emisor contiene una contraseña secreta o un número de identificación secreto. En este caso se trata de una denominada autentificación de usuario fuerte, es decir, el emisor se autentifica como usuario autorizado porque por un lado conoce algo, de hecho, una contraseña o un número de identificación, por otro lado, posee algo, en el presente caso, el equipo de recepción 3, al que se transmitió la comunicación o la comunicación que recibió con el equipo de recepción 3. El receptor de la comunicación tiene que añadir a un mensaje que genera, la información de emisor de acuerdo con una tercera regla de combinación.

En una configuración preferida del método de acuerdo con la invención, el código de validación, el código de control y/o la información de emisor se transmiten de forma encriptada. Para esto, preferiblemente se encriptan el código de validación y/o la propia información de emisor, antes de que se añadan de acuerdo con la primera o tercera regla de combinación a la comunicación o el mensaje. Sin embargo, ventajosamente también se puede encriptar toda la comunicación y/o el mensaje. Si el equipo de comunicación 2 recibe un mensaje encriptado, el mismo se tiene que desencriptar en primer lugar. Si el código de control o la información de emisor están presentes de forma encriptada después de la extracción del mensaje, los mismos se tienen que desencriptar. Cuando el mensaje contiene una información de emisor, por una transmisión encriptada se continúa disminuyendo el riesgo de una manipulación por no autorizados, debido a que por mensajes escuchados o captados no se puede obtener sin más la información de emisor. También cuando la validez del código de validación tiene que estar sometida a una limitación en el tiempo es ventajosa una transmisión encriptada. En este caso se puede añadir una información de validez directamente al código de validación, a modo de ejemplo, por conexión. Se impide una manipulación de la información de validez por el receptor. Después de una descodificación del mensaje o del código de control en el equipo de comunicación 2, la información de validez vuelve a estar presente en un texto comprensible. Por tanto no se necesita un almacenamiento de la información de validez.

En una configuración preferida del método de acuerdo con la invención, la comunicación o el mensaje se envían o reciben mediante el servicio de mensajes cortos (SMS) por una red GSM o ISDN.

En una configuración preferida adicional del método de acuerdo con la invención, el mensaje se recibe por una red informática pública, preferiblemente, internet.

Los medios utilizados durante la realización del método de acuerdo con la invención de acuerdo con la anterior descripción como equipo de comunicación 2, interfaz de red 21, interfaz de sistema 22, equipo de recepción 3 y equipo de control se tienen que considerar elementos funcionales y no tienen que estar configurados necesariamente como unidades físicas independientes. De este modo, con el método también se puede controlar y/o regular a distancia un sistema 1, en el que el equipo de comunicación y/o el equipo de control estén integrados en el sistema 1. Ventajosamente, el equipo de comunicación 2 puede estar integrado en un ordenador electrónico, en el que también se implementa ventajosamente el equipo de control. Ventajosamente, el ordenador electrónico también sirve como instalación de procesamiento de datos durante una detección y el análisis de datos que se refieren al sistema.

El método de acuerdo con la invención también se puede utilizar ventajosamente en el control y/o la regulación a distancia de sistemas basados en ordenadores como, a modo de ejemplo, sistemas de procesamiento de datos, sistemas de transacciones financieras o sistemas de comercio.

El receptor de la comunicación generalmente será una persona. En este caso, la comunicación también puede presentarse ventajosamente en forma acústica y consistir, a modo de ejemplo, en una secuencia temporal de información y código de validación. Sin embargo, también se puede concebir que el receptor sea un aparato electrónico, que genere un mensaje con una información de órdenes adecuada automáticamente como respuesta a la comunicación y transmita el mismo de vuelta al equipo de comunicación 2.

Lista de referencias

1 Sistema

2 Equipo de comunicación

21 Interfaz de red

22 Interfaz de sistema

3 Equipo de recepción

REIVINDICACIONES

1. Método para el control y/o la regulación a distancia de al menos un sistema (1), particularmente de una instalación industrial,

- usando un equipo de comunicación (2), que está asignado al sistema (1),
- donde el equipo de comunicación (2) envía una comunicación,
- la comunicación comprende una información que se refiere al sistema (1) y un código de validación, donde la información y el código de validación se agrupan de acuerdo con una primera regla de combinación y
- por un mensaje, que recibe el equipo de comunicación (2) después del envío de la comunicación,
  - de acuerdo con una primera regla de extracción se extrae un código de control y
  - mediante el código de validación y el código de control se comprueba si el mensaje procede de un emisor de la comunicación y
  - solamente en el caso de una comprobación exitosa se extrae una información de órdenes de acuerdo con la primera regla de extracción del mensaje y se transforma por el sistema (1),

donde el código de validación presenta una validez limitada en el tiempo,

caracterizado porque

- al código de validación se añade una información de validez, por la que se define la limitación en el tiempo de la validez del código de validación,
- la información de validez se añade directamente al código de validación,
- el código de validación se transmite en forma encriptada y
- después de una desencriptación del mensaje o el código de control en el equipo de comunicación (2), la información de validez vuelve a estar presente en un texto comprensible.

2. Método de acuerdo con la reivindicación 1, **caracterizado** porque

- al código de validación se añade o antepone la información de validez.

3. Método de acuerdo con una de las reivindicaciones precedentes, **caracterizado** porque

- no se produce un almacenamiento de la información de validez en el equipo de comunicación (2).

4. Método para el control y/o la regulación a distancia de al menos un sistema (1), particularmente de una instalación industrial,

- usando un equipo de comunicación (2), que está asignado al sistema (1),
- donde el equipo de comunicación (2) envía una comunicación,
- la comunicación comprende una información que se refiere al sistema (1) y un código de validación, donde la información y el código de validación se agrupan de acuerdo con una primera regla de combinación y
- por un mensaje, que recibe el equipo de comunicación (2) después del envío de la comunicación,
  - de acuerdo con una primera regla de extracción se extrae un código de control y
  - mediante el código de validación y el código de control se comprueba si el mensaje procede de un emisor de la comunicación y
  - solamente en el caso de una comprobación exitosa se extrae una información de órdenes de acuerdo con la primera regla de extracción del mensaje y se transforma por el sistema (1),

donde el código de validación presenta una validez limitada en el tiempo,

caracterizado porque

- durante un envío de la comunicación se almacena una copia del código de validación para estar disponible para la comparación durante la posterior recepción de un mensaje y

- una información de validez, por la que se define la limitación en el tiempo de la validez del código de validación, se almacena junto con el código de validación.

5. Método de acuerdo con una de las reivindicaciones precedentes, **caracterizado** porque

- la validez del código de validación es única.

6. Método de acuerdo con una de las reivindicaciones precedentes, **caracterizado** porque

- el código de validación se genera por un generador de números aleatorios.

7. Método de acuerdo con una de las reivindicaciones precedentes, **caracterizado** porque

- el propio código de validación se encripta antes de que se añada de acuerdo con la primera regla de combinación a la comunicación o el mensaje.

8. Método de acuerdo con una de las reivindicaciones precedentes, **caracterizado** porque

- el código de control se transmite en forma encriptada.

9. Método de acuerdo con una de las reivindicaciones precedentes, **caracterizado** porque

- por el emisor de la comunicación se añade al mensaje que genera, una información de emisor de acuerdo con una tercera regla de combinación,

- del mensaje se extrae de acuerdo con una tercera regla de extracción la información de emisor,

- mediante la información de emisor y datos de emisor almacenados se identifica el emisor,

- solamente en el caso de una comprobación exitosa, de si el mensaje procede de un receptor de la comunicación, y una identificación de emisor exitosa, una información de órdenes después de la extracción del código de control y la información de emisor se transforma del mensaje por el sistema (1) y,

- en el caso de que la comprobación y/o la identificación de emisor no fuera o fueran exitosas, la información de órdenes se ignora.

10. Método de acuerdo con la reivindicación 9, **caracterizado** porque

- la información de emisor contiene una contraseña secreta o un número de identificación secreto.

11. Método de acuerdo con una de las reivindicaciones 9-10, **caracterizado** porque

- la información de emisor se transmite en forma encriptada.

12. Método de acuerdo con una de las reivindicaciones 9-11, **caracterizado** porque

- la propia información de emisor se encripta antes de que se añada de acuerdo con una tercera regla de combinación al mensaje.

13. Método de acuerdo con una de las reivindicaciones precedentes, **caracterizado** porque

- toda la comunicación y/o el mensaje se codifican.

14. Método de acuerdo con una de las reivindicaciones precedentes, **caracterizado** porque

- la comunicación y/o el mensaje se envían y/o reciben por servicio de mensajes cortos.

15. Método de acuerdo con una de las reivindicaciones precedentes, **caracterizado** porque

- el mensaje se recibe por internet.

16. Método de acuerdo con una de las reivindicaciones precedentes, **caracterizado** porque

- la transmisión de la comunicación representa una alarma, particularmente porque
- la transmisión de la comunicación está condicionada por un error diagnosticado en el sistema (1) o
- la transmisión de la comunicación, independientemente de un estado del sistema (1), está condicionada porque un parámetro que se refiere indirectamente al sistema (1), particularmente una temperatura del entorno, supera o pasa por debajo de un valor umbral.

17. Método de acuerdo con una de las reivindicaciones precedentes, **caracterizado** porque

- la comunicación se transmite en una hora fija, en un día fijo o en fechas determinadas de antemano.

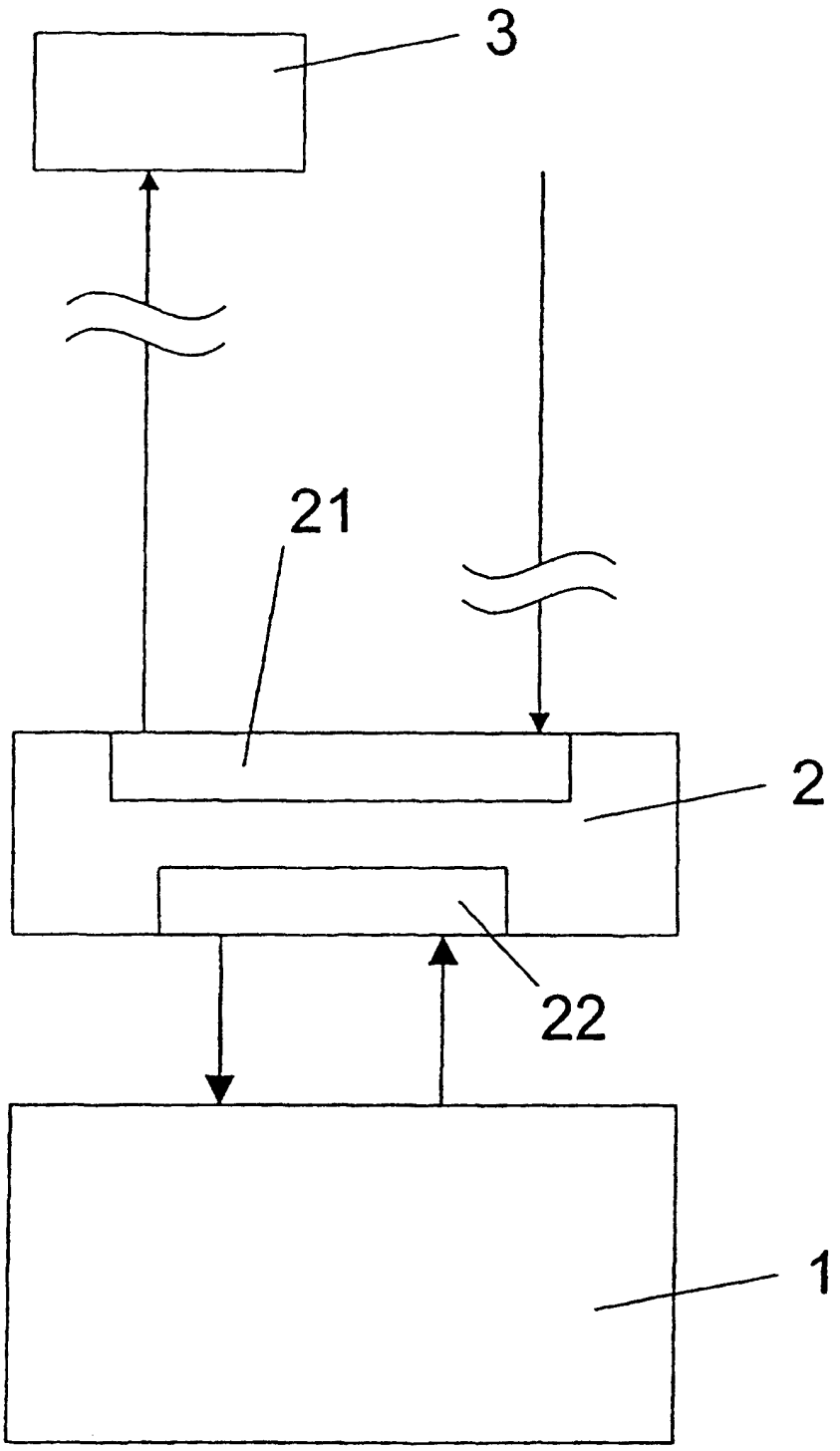

Fig. 1