(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 397 926**

(51) Int. CI.:

G05B 19/18 (2006.01)
G06F 9/455 (2006.01)
G05B 19/414 (2006.01)
G05B 19/418 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **21.06.2008 E 08784246 (4)**

(97) Fecha y número de publicación de la concesión europea: **24.10.2012 EP 2162805**

(54) Título: **Dispositivo para controlar una máquina así como sistema de telecomunicaciones**

(30) Prioridad:

29.06.2007 DE 102007030396

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
12.03.2013

(73) Titular/es:

TRUMPF WERKZEUGMASCHINEN GMBH + CO. KG (100.0%)
JOHANN-MAUS-STRASSE 2
71254 DITZINGEN, DE

(72) Inventor/es:

BAUER, KLAUS

(74) Agente/Representante:

ISERN JARA, Nuria

DESCRIPCIÓN

Dispositivo para controlar una máquina así como sistema de telecomunicaciones

La invención se refiere a un dispositivo de control de máquina herramienta según el preámbulo de la reivindicación 1 así como a un sistema para la telecomunicación entre un ordenador o portal de servicio y el dispositivo de control de máquina herramienta. En el marco de la invención, por una máquina herramienta se entiende también un aparato láser.

Un dispositivo de control de máquina herramienta de este tipo se dio a conocer, por ejemplo, por el documento EP 1 715 395 A.

El sistema conocido por el documento EP 1 715 395 A para la telecomunicación entre un PC de servicio y un control de máquina comprende al menos un ordenador central; que está protegido mediante un cortafuegos y que presenta varios ordenadores virtuales ejecutables adyacentes, que están configurados en cada caso para el mismo tipo o tipos diferentes de conexiones de comunicación con controles de máquina, pudiendo conectarse el PC de servicio con el ordenador central a través de una conexión y pudiendo conectarse el ordenador central con un control de máquina a través del ordenador virtual que está configurado para la conexión de comunicación asociada a este control de máquina.

La orientación global de los fabricantes de máquinas herramienta y láseres actuales con clientes y operadores de máquina en todo el mundo hace necesario poder ofrecer un mantenimiento, diagnóstico de errores, actualización de software y dado el caso también una reparación de las máquinas herramienta y láseres suministrados (a continuación agrupadas bajo el término “máquinas”) no sólo directamente *in situ*, sino también por acceso remoto (teleservicio). Para los fabricantes de máquinas herramienta y láseres no hay alternativa comercial alguna al mantenimiento remoto. No obstante, los operadores de instalaciones de producción modernas se ven afectados, ya que sus instalaciones han sido colapsadas en el pasado por virus o troyanos infiltrados. Dado que la interconexión en red de instalaciones de producción industrial aumenta constantemente y con la interconexión en red también aumenta el potencial de riesgo, los clientes, sobre todo las grandes empresas, ya han puesto freno a soluciones de mantenimiento remotas no seguras y han formulado amplios requisitos de seguridad. Para fabricantes de máquinas herramienta y láseres tiene una consecuencia fatal, ya que, si cada cliente formula sus propios estándares de seguridad para el acceso remoto, se producen “innumerables” variantes, que van desde el tipo de marcación (módem, ISDN, Internet, GSM, UMTS) pasando por diferentes normas VPN para la conexión de datos hasta una pluralidad de escáneres de virus y cortafuegos prescritos.

Para poder aprovechar las posibilidades del teleservicio, es necesaria una conexión segura, fiable y sin perturbaciones. Mientras que para ello, hasta ahora, habitualmente tenía lugar una marcación directa desde un ordenador de servicio a través de un módem analógico o una conexión RDSI, aumenta la demanda de una técnica de comunicación más moderna, la denominada *virtual private network*. Una *virtual private network* (VPN) (es decir, red privada virtual) es una red informática, que sirve para el transporte de datos privados de una red pública, en particular Internet, cifrándose habitualmente la conexión a través de la red pública. Mediante el cifrado se genera una red que sólo es accesible con las direcciones y contraseñas correctas, de modo que sólo usuarios autorizados pueden comunicarse entre sí. La VPN posibilita por tanto una transmisión segura a través de una red no segura. Internet se ofrece como medio central para el teleservicio también en el entorno de la técnica de automatización. Los sistemas de cortafuegos y VPN ayudan a hacer que el uso de Internet sea seguro. Además de la seguridad claramente mejorada, las conexiones de mantenimiento remoto basadas en IP (Internet Protocol) ofrecen un ancho de banda esencialmente superior a la conexión por módem convencional. Pueden transmitirse muchos datos, incluso para la transmisión de información de vídeo, por ejemplo en sistemas de monitorización distribuidos, en banda ancha a través de Internet.

Sobre todo las grandes empresas desarrollan sus pasarelas de cortafuegos hacia portales VPN, a través de los cuales los fabricantes de máquinas herramienta y láseres obtienen acceso remoto a máquinas herramienta y láseres suministrados. Asociado a ello, se exige a los fabricantes de máquinas herramienta y láseres que eliminen sus accesos RDSI y módems locales instalados en las máquinas herramienta y láseres. Además, algunas empresas definen entretanto especificaciones de acceso, que no están normalizadas. Además de VPN se utilizan también otros procedimientos de autenticación, como por ejemplo ID de llamante, claves previamente compartidas, contraseñas de un solo uso o SecureID, o hardware especial.

Un acceso remoto a través de VPN plantea elevados requisitos en cuanto a la infraestructura y seguridad. Es especialmente problemático el hecho de que el acceso remoto a través de VPN depende de la técnica utilizada por el operador de la máquina. Una solución universal sencilla en el lado del fabricante de máquinas herramienta y láseres se ve dificultada por la circunstancia de que, hasta ahora, no es posible utilizar diferente software de cliente VPN (por ejemplo cliente VPN de CISCO y cliente VPN de Checkpoint) al mismo tiempo dentro de un sistema operativo, es decir por ejemplo al mismo tiempo en el ordenador de servicio de un trabajador de servicio. En función de la solución VPN utilizada por el operador de la máquina son necesarios un cliente VPN diferente y por tanto un ordenador independiente. Surgen problemas similares si el operador de la máquina exige además otras especificaciones de acceso y tecnologías de marcación, por ejemplo RAS a través de ISDN o a través de módem.

Surgen otros problemas si datos (de acceso) sensibles del operador de la máquina están almacenados localmente en ordenadores de servicio de los trabajadores de servicio. Estos datos simplemente no están protegidos suficientemente frente a ataques desde Internet o en caso de robo de un ordenador de servicio.

Los ciclos de vida de producto de componentes de hardware utilizados en ordenadores de gestión para el control de máquinas son por lo general claramente más cortos que los ciclos de vida de producto de las máquinas y el software utilizado (por ejemplo software de gestión de máquina). La disponibilidad limitada de componentes de hardware lleva durante el ciclo de vida de un tipo de máquina a una pluralidad de variantes del hardware del ordenador de gestión utilizado. Estas distintas variantes de hardware deben tenerse en cuenta en las actualizaciones del software de gestión de máquina y soportarse por el software. Por regla general, una modificación de hardware supone una modificación de hardware (por ejemplo, el controlador). Como consecuencia, los desarrolladores de software deben realizar un esfuerzo extremadamente alto para que todas las variantes de hardware utilizadas se soporten también en el software. Deben efectuarse una y otra vez modificaciones más grandes, porque determinados controladores para un nuevo hardware sólo se soportan todavía en sistemas operativos actuales. Por lo general es necesario entonces una actualización del sistema operativo. Debido a las dependencias de los diferentes componentes de software de una máquina se llega una y otra vez a un cambio forzoso de otros componentes (por ejemplo hardware y software NCK), en caso de que en el caso de una pieza de repuesto no esté disponible ningún hardware compatible. Otro problema consiste en que los sistemas de cifrado modernos a menudo sólo funcionan con sistemas operativos actuales y no pueden utilizarse con sistemas operativos más antiguos como Windows 3.11. Para mantener la seguridad al nivel más actualizado, es necesario entonces instalar un sistema operativo actual en el ordenador de gestión.

Por el documento DE 102 12 151 A1 se conoce un procedimiento para aplicaciones críticas en cuanto a seguridad en máquinas, aparatos y/o instalaciones, comprendiendo el procedimiento las siguientes etapas:

- recibir datos desde el proceso crítico en cuanto a seguridad:
- invocar un programa de aplicación para procesar los datos recibidos en al menos dos entornos de procesamiento;
- emitir los datos procesados;

posibilitando los al menos dos entornos de procesamiento una invocación y/o ejecución con diversidad de tiempo y/o diversidad de datos de un programa de aplicación.

Partiendo del documento EP 1 715 395 A, el objetivo de la presente invención es proporcionar un control de máquina herramienta, en el que puedan realizarse modificaciones en la conexión de comunicación de manera flexible y, en cualquier caso, sin influir en el software de gestión de máquina.

Este objetivo se soluciona según la invención mediante un dispositivo de control de máquina herramienta con las características de la reivindicación 1. Preferiblemente, al menos algunos de los ordenadores virtuales presentan diferentes sistemas operativos.

Los ordenadores virtuales, abreviado VM por *virtual machine*, se ejecutan en un entorno encapsulado bajo el control de un programa de virtualización. Entre los programas de virtualización conocidos se encuentran, a modo de ejemplo, VMware Server, VMware Workstation, Microsoft Virtual Server y Microsoft Virtual PC. Con la virtualización es posible por un lado aislar varios ordenadores virtuales con sistemas operativos heterogéneos, y por otro lado implementarlos unos junto a otros en la misma máquina física. Cada ordenador virtual dispone de un conjunto de hardware virtual propio, como por ejemplo memoria RAM, CPU, NIC, etc., sobre el que pueden cargarse el sistema operativo y las aplicaciones. El ordenador físico real en el que se ejecutan los ordenadores virtuales, se designará ordenador anfitrión. Un ordenador virtual se denomina huésped y el sistema operativo correspondiente se denomina sistema operativo huésped.

Un ordenador virtual actúa como un ordenador plenamente válido: ni el sistema operativo huésped, ni aplicaciones o usuarios notan diferencia alguna con un ordenador físico y también en LAN puede aparecer un ordenador virtual como un ordenador plenamente válido con una dirección IP y MAC propia. Los ordenadores virtuales están completamente aislados del ordenador anfitrión y de otros ordenadores virtuales. Los ordenadores virtuales sólo pueden comunicarse por tanto entre sí, tal como sería el caso igualmente entre ordenadores separados, por ejemplo a través de conexiones de red. En caso de avería de un ordenador virtual, los demás ordenadores virtuales y el ordenador anfitrión no se ven afectados por ello. Los datos no pueden desviarse a otros ordenadores virtuales, y las aplicaciones sólo pueden comunicarse entre sí a través de conexiones de red configuradas. Debido al aislamiento mutuo de los ordenadores virtuales unos respecto a otros y respecto al ordenador anfitrión pueden ejecutarse diferentes sistemas operativos en paralelo e independientemente sobre el mismo hardware.

Tras la instalación del ordenador virtual, el disco duro virtual todavía está vacío. Al igual que en un ordenador físico debe instalarse en primer lugar un sistema operativo. El ordenador virtual arranca el sistema operativo huésped desde el CD de instalación físico o desde una imagen ISO. La rutina de configuración instala el sistema operativo huésped de la manera habitual y copia todos los archivos de sistema en el disco duro virtual, sin saber que sólo es

un archivo en algún lugar en el disco duro del ordenador anfitrión. El reconocimiento de hardware reconoce todos los aparatos emulados, como si fueran reales. A continuación se instalan los *Service-Packs* y parches así como herramientas necesarias y el software de aplicación necesario en el huésped.

Según la invención, para evitar problemas de compatibilidad en el ordenador de control tras un cambio de hardware necesario, el software de gestión de máquina se ejecuta en un ordenador virtual. Puede prescindirse de adaptaciones y modificaciones costosas en el software de gestión de máquina, ya que el software de gestión de máquina se ejecuta además con su antiguo sistema operativo. Las dependencias del software de gestión de máquina respecto de las generaciones de hardware durante la vida útil de producto de la máquina pueden dominarse mediante el uso de hardware virtualizado. El software (por ejemplo software de gestión de máquina) se instala y gestiona dentro de un ordenador virtualizado. El sistema operativo del ordenador anfitrión (sistema operativo maestro) sólo se usa sobre el hardware físico, para proporcionar los entornos de hardware virtuales. En el caso de una pieza de recambio puede utilizarse prácticamente cualquier hardware sobre el que pueda utilizarse en ejecución el entrono virtual. No es necesaria una adaptación de la aplicación de software (por ejemplo MMC) ejecutada dentro del entorno virtual, ya que el entorno de tiempo de ejecución (sistema operativo, memoria, número de procesadores, infraestructura como por ejemplo tarjetas de red, tarjetas gráficas,...) no se modifica desde el punto de vista de la aplicación de software ejecutada. Mediante una ejecución paralela de varios entornos virtuales sobre un hardware físicamente proporcionado pueden ahorrarse además costes.

Según la invención pueden realizarse además diferentes aplicaciones, como software de gestión de máquina así como cifrado y conexión a Internet, a través de ordenadores virtuales separados. Mediante el uso de ordenadores virtuales o de hardware virtualizado con un sistema operativo independiente pueden evitarse dependencias mutuas y efectos secundarios (consecuencias negativas). En lugar de efectuar, como hasta ahora, el cifrado de la conexión de Internet del ordenador de control a través de un módulo separado, según la invención se realiza la conexión de comunicación global no dentro del sistema operativo principal del ordenador de control, sino dentro de un hardware virtualizado con un sistema operativo independiente.

La invención se refiere, en un aspecto adicional, también a un sistema para la telecomunicación entre un ordenador o portal de servicio y el dispositivo de control de máquina herramienta tal como se describió anteriormente.

Un sistema de telecomunicación entre un ordenador de servicio y un control de máquina para un acceso remoto seguro a la máquina se conoce por ejemplo por el documento EP 1 715 395 A. Este sistema de telecomunicación conocido comprende un ordenador central protegido por un cortafuegos con varios ordenadores virtuales y una base de datos, que tiene almacenados todos los datos (técnica de marcación, contraseñas, solución VPN) acerca de clientes y máquinas. En el ordenador central están instalados varios ordenadores virtuales, que presentan diferentes sistemas operativos y software de aplicaciones (como programas de protección frente a virus). Para cada cliente y cada control de máquina hay un ordenador virtual especialmente configurado, a través del cual se establece la conexión desde el ordenador central al control de máquina. El ordenador central determina con ayuda de los datos almacenados en la base de datos la conexión asociada y el ordenador virtual asociado y establece la conexión con el control de máquina a través de Internet. El ordenador de servicio no está conectado directamente con la máquina, sino que la conexión se produce a través del ordenador central protegido. La conexión entre el ordenador de servicio y el ordenador central así como la conexión entre el ordenador central y el control de máquina se producen a través de Internet, respectivamente a través de una conexión VPN protegida.

Otras ventajas y configuraciones ventajosas del objeto de la invención pueden deducirse de la descripción, el dibujo y las reivindicaciones. Igualmente, las características anteriormente mencionadas y que se explicarán adicionalmente aún pueden usarse según la invención en cada caso de manera individual por sí solas o varias en cualquier combinación. La forma de realización mostrada y descrita no ha de entenderse como enumeración excluyente, sino que tiene más bien un carácter a modo de ejemplo para ilustrar la invención.

Los dibujos muestran:

La figura 1, esquemáticamente la construcción básica de un dispositivo para controlar una máquina con un ordenador de control configurado como ordenador de gestión;

La figura 2, esquemáticamente la construcción básica del ordenador de gestión virtualizado según la invención de la figura 1;

La figura 3, esquemáticamente la construcción básica del sistema de telecomunicación según la invención entre el ordenador de gestión mostrado en la figura 2 y un ordenador o portal de servicio, y

La figura 4, el sistema de telecomunicación de la figura 3, estando conectado el ordenador de gestión a la intranet del operador de la máquina y el ordenador de servicio a la intranet del fabricante de la máquina.

El dispositivo 1 mostrado en la figura 1 para controlar una máquina 2 comprende un ordenador de control configurado en este caso como ordenador 3 de gestión, que está conectado con la máquina 2 y con un servidor 4. En el ordenador 3 de gestión están instalados un software de gestión de máquina y un software tal como PC-Anywhere, a través del que tiene lugar un acceso remoto a la máquina 2, y dado el caso otras aplicaciones. Los

programas NC para una orden de trabajo ya no se crean manualmente sino con ayuda de sistemas 5 de programación. El sistema 5 de programación está instalado en el ordenador 3 de gestión de la máquina 2 o en uno o varios ordenadores 6 (Notebook, Tower-PC) en la red de IT. El programador deposita el programa NC terminado en una base de datos 7 en el servidor 4. El operario de la máquina puede acceder a la base de datos 7 del servidor 4 e invocar el programa NC directamente al ordenador 3 de gestión. La transferencia de datos del programa NC también puede realizarse a través de un medio de almacenamiento tal como un disquete, un CD-ROM o un lápiz USB. El sistema 5 de programación convierte las estrategias que el programador ha seleccionado. Establece el orden de mecanizado, fija puntos de corte, redondea esquinas puntiagudas y completa pequeños *loopings*. Para que la calidad de mecanizado sea correcta, el programa NC suministra al control 1 de máquina valores adecuados para los parámetros de mecanizado, como por ejemplo potencia de láser y velocidad de avance. Estos valores están almacenados en tablas 8 de tecnología. Las tablas 8 de tecnología son memorias de conocimiento, que contienen valores seguros para el proceso para todos los parámetros de mecanizado. Se aplican para cada tipo de material y espesor de material, teniendo en cuenta también el tipo de láser, el tamaño de contorno y distancias focales ópticas. Cada tabla 8 de tecnología tiene un número y está depositada en el control 1 de máquina, es decir en el ordenador 3 de gestión. Puede mantenerse y actualizarse de manera centralizada y está disponible para toda orden de trabajo. En el programa NC no aparecen valores para los parámetros de mecanizado, sino el número de la tabla 8 de tecnología, en la que están almacenados los valores adecuados. Durante el mecanizado, el control 1 de máquina recurre a las tablas 8 de tecnología. Lo que aparece en el programa NC, lo convierte el control 1 de máquina en la realidad, controla los movimientos de los ejes de máquina y regula la potencia de láser y la alimentación de gas.

En la figura 2 se muestra esquemáticamente la construcción del ordenador 3 de gestión de la máquina 2 (máquina herramienta o láser), en el que se ejecutan el software de gestión de máquina y dado el caso otro software de aplicaciones. El ordenador 3 de gestión está configurado como ordenador 9 anfitrión con dos ordenadores 10a, 10b virtuales y presenta una tarjeta 11 de red para la conexión a un ordenador 12 de servicio o a un portal 13 de servicio.

Los ordenadores 10a, 10b virtuales se ejecutan en un entorno encapsulado en el ordenador 3 de gestión bajo el control de un software de virtualización, que está instalado en el ordenador 9 anfitrión. El ordenador 9 anfitrión se ejecuta con un sistema operativo anfitrión (por ejemplo Windows Vista o Linux). Un ordenador 10a virtual, designado en la figura 2 como VM1, se ejecuta con un primer sistema operativo, por ejemplo Windows XP(e), y en él están instaladas todas las aplicaciones relacionadas con la conexión de comunicación del ordenador 9 anfitrión, por tanto en particular la conexión a Internet (navegador de Internet) y el cifrado de Internet (software VPN). El otro ordenador virtual, designado en la figura 2 como VM2, se ejecuta con un segundo sistema operativo, por ejemplo Windows NT4.0, y en él está instalado el software de gestión de máquina. Además, la máquina 4b virtual presenta también un almacén de datos, por ejemplo para las tablas 8 de tecnología y para datos acerca de herramientas existentes de la máquina. Asimismo el sistema 5 de programación para crear programas NC puede implementarse como ordenador virtual.

Para el caso en el que un componente de hardware del ordenador 3 de gestión deba reemplazarse por otro componente de hardware no compatible, se prepara en primer lugar un archivo de seguridad del ordenador 10b virtual. Puesto que el ordenador 10b virtual no representa otra cosa que un archivo en el disco duro del ordenador 9 anfitrión, el archivo de seguridad es una copia del archivo, que se almacena en el servidor 4 de la red de IT o en un medio de almacenamiento tal como un disquete, un CD-ROM o un lápiz USB. Una vez reemplazado el componente de hardware, se instalan en el ordenador 9 anfitrión en primer lugar el sistema operativo anfitrión, que puede ser idéntico o diferente del sistema operativo anfitrión previamente instalado, y a continuación el software de virtualización. Una vez instalado el ordenador 10b virtual a través del software de virtualización, tiene lugar la instalación del sistema operativo huésped y del software de aplicaciones (software de gestión de máquina etc.) mediante la copia del archivo de seguridad. No es necesaria ninguna nueva instalación del sistema operativo huésped y del software de aplicaciones.

El sistema 20 mostrado en la figura 3 sirve para la telecomunicación entre el ordenador 3 de gestión de la máquina 2 construido tal como se describió anteriormente y el ordenador 12 de servicio o el portal 13 de servicio, para posibilitar un mantenimiento, diagnóstico de errores, actualización de software y, dado el caso, una reparación de la máquina 2 por acceso remoto.

El sistema 20 comprende al menos un ordenador 21 central, que está protegido mediante un cortafuegos 22 hacia el exterior y presenta varios ordenadores 23 virtuales ejecutables adyacentes. Estos ordenadores 23 virtuales individuales, tal como se explica en más detalle más adelante, están configurados en cada caso para el mismo tipo o tipos diferentes de conexiones 24 con ordenadores 3 de gestión. El ordenador 12 de servicio de un trabajador de servicio está conectado con el ordenador 21 central a través de una conexión 25, que permite en particular sólo la transmisión de información de píxel, movimientos de ratón y teclado. El ordenador 21 central está conectado con el ordenador 3 de gestión de la máquina 2 a través del ordenador 23 virtual que está configurado para la conexión 24 asociada a esta máquina 2. La asociación de máquinas 2 con sus ordenadores 3 de gestión con sus respectivas conexiones 24 está almacenada en una base de datos 26 del ordenador 21 central. Los ordenadores 23 virtuales del ordenador 21 central presentan diferentes sistemas operativos con diferentes programas de aplicaciones, que establecen la conexión 24 entre el ordenador 21 central y los diferentes ordenadores 3 de gestión. El ordenador 3 de gestión presenta varios ordenadores 10a, 10b virtuales, que pueden comunicarse entre sí a través de una tarjeta de red virtual. En el ordenador 10a virtual están instaladas todas las aplicaciones que se refieren a la conexión del

ordenador 3 de gestión con el mundo exterior, tal como cifrado y conexión de Internet. La conexión 25 entre el ordenador 12 de servicio y el ordenador 21 central así como la conexión 24 entre el ordenador 21 central y el respectivo ordenador 3 de gestión tienen lugar a través de Internet 27, y concretamente en cada caso a través de una conexión VPN. El ordenador 21 central junto con el cortafuegos 22 forma el portal 13 de servicio.

Para un acceso remoto al ordenador 3 de gestión de la máquina 2, un trabajador de servicio establece en primer lugar la conexión 25 entre su ordenador 12 de servicio y el ordenador 21 central protegido por el cortafuegos 22. El trabajador de servicio se autoriza en el ordenador 21 central y selecciona el cliente y la máquina 2 pertinentes. Todas las especificaciones individuales (contraseñas) del cliente están almacenadas de manera centralizada en la base de datos 26. Gracias a los datos almacenados en la base de datos 26, el ordenador 21 central determina la conexión 24 asociada a la máquina 2 y selecciona el ordenador 23 virtual configurado para esa conexión 24, para su conexión con el ordenador 3 de gestión e inicia este ordenador 23 virtual. A través de la conexión 24, el trabajador de servicio lleva a cabo funciones del ordenador 3 de gestión y/o intercambia archivos entre el ordenador 3 de gestión y el ordenador 21 central, no estando conectado el ordenador 3 de gestión de una máquina 2 situada en las instalaciones del cliente directamente con el ordenador 12 de servicio, sino sólo a través del ordenador 21 central protegido. El sistema 20 de telecomunicación posibilita que varios trabajadores de servicio se conecten al mismo tiempo con sus ordenadores 12 de servicio a través del ordenador 21 central con el ordenador 3 de gestión de la máquina 2. Según la situación problemática pueden conectarse trabajadores de servicio o especialistas desde distintos lugares a través del ordenador 21 central con el ordenador 3 de gestión.

Por motivos de seguridad, un acceso remoto a la máquina 2 sólo tiene lugar por un trabajador de servicio con el consentimiento del operador de la máquina. Para ello está instalada una aplicación correspondiente en el ordenador 3 de gestión, que debe aplicarse por el operador de la máquina. El ordenador 21 central dirige una solicitud al control de máquina y espera a que el operador de la máquina active la máquina 2 para el acceso remoto. Alternativamente, también es posible que el trabajador de servicio pida por teléfono la activación al operador de la máquina. Si el operador de la máquina ha activado el acceso remoto a la máquina 2, el ordenador 21 central establece en primer lugar la conexión 24 con el ordenador 10a virtual. Los ordenadores 10a, 10b virtuales y el ordenador 9 anfitrión están conectados entre sí mediante tarjetas de red físicas y virtuales. El trabajador de servicio puede acceder a través del ordenador 10a virtual, que actúa como encaminador, al ordenador 9 anfitrión y al otro ordenador 10b virtual. A través de la conexión 24 el trabajador de servicio realiza funciones del ordenador 3 de gestión y/o intercambia archivos entre el ordenador 3 de gestión y el ordenador 21 central. El trabajador de servicio puede actualizar por ejemplo el software de gestión de máquina y/o las tablas 8 de tecnología en el ordenador 10b virtual. El ordenador 3 de gestión de una máquina 2 situada en las instalaciones del cliente no está conectado directamente con el ordenador 12 de servicio, sino sólo a través del ordenador 21 central protegido.

Tal como se indica con la línea discontinua en la figura 3, también es posible una conexión 28 directa entre el ordenador 3 de gestión y el ordenador 12 de servicio a través de Internet 27, debiendo estar esta conexión 28 directa protegida entonces mediante correspondientes sistemas de seguridad.

En la figura 4, el ordenador 21 central está conectado a través del cortafuegos 22 a la Intranet (red doméstica) 29 del fabricante de la máquina, que está conectada a través de otro cortafuegos 30 con Internet 27. Además, el ordenador 3 de gestión está conectado a la Intranet (red doméstica) 31 del operador de la máquina, que está conectada igualmente con Internet 27. El ordenador 21 central es un área LAN protegida (VLAN), que está separada a través del cortafuegos 22 de la Intranet 29 del fabricante de la máquina. Sólo determinadas personas tienen acceso a la estructura detrás del cortafuegos 22. El ordenador 12 de servicio está conectado o bien directamente a través de la Intranet 29 del fabricante de la máquina o bien a través de Internet 27 con el ordenador 21 central. Tal como se indica con la línea discontinua en la figura 4, también en este caso es posible una conexión 28 directa entre el ordenador 3 de gestión y el ordenador 12 de servicio a través de Internet 27, debiendo estar esta conexión 28 directa protegida entonces mediante correspondientes sistemas de seguridad.

REIVINDICACIONES

1.- Dispositivo (1) para controlar una máquina herramienta (2) con un control de máquina en forma de un ordenador (3) de control, en el que se opera un software de gestión de máquina, **caracterizado,**

porque el control de máquina presenta un primer ordenador (10a) virtual y un segundo ordenador (10b) virtual,

porque el primer ordenador (10a) virtual se opera con un primer sistema operativo y el segundo ordenador (10b) virtual con un segundo sistema operativo,

porque en el primer ordenador virtual (10a) está instalada una conexión a Internet, y

porque en el segundo ordenador (10b) virtual está instalado un software de gestión de máquina.

2.- Dispositivo de control de máquina herramienta según la reivindicación 1, **caracterizado porque** los ordenadores (10a, 10b) virtuales primero y segundo presentan diferentes sistemas operativos.

3.- Dispositivo de control de máquina herramienta según la reivindicación 1 ó 2, **caracterizado porque** los ordenadores (10a, 10b) virtuales primero y segundo se comunican entre sí a través de una tarjeta de red virtual.

4.- Dispositivo de control de máquina herramienta según una de las reivindicaciones anteriores, **caracterizado porque** el ordenador (3) de control está configurado como ordenador (9) anfitrión con dos ordenadores (10a, 10b) virtuales y los ordenadores (10a, 10b) virtuales y el ordenador (9) anfitrión están conectados entre sí mediante tarjetas de red físicas y virtuales.

5.- Dispositivo de control de máquina herramienta según una de las reivindicaciones anteriores, **caracterizado porque** el ordenador (3) de control está equipado como ordenador (9) anfitrión con los dos ordenadores (10a, 10b) virtuales y presenta una tarjeta (11) de red para la conexión a un ordenador (12) de servicio o a un portal (13) de servicio.

6.- Sistema (20) para la telecomunicación entre un ordenador (12) de servicio o un portal (13) de servicio y un dispositivo (1) de control de máquina herramienta que presenta un control de máquina en forma de un ordenador (3) de control según una de las reivindicaciones anteriores, incluyendo el sistema el dispositivo de control de máquina herramienta, realizándose la conexión (24, 25, 28) de comunicación a través de Internet (27), en particular a través de una conexión VPN.

7.- Sistema según la reivindicación 6, **caracterizado porque** la conexión (24, 25) de comunicación entre el ordenador (12) de servicio o portal (13) de servicio y el control de máquina se realiza a través de al menos un ordenador (21) central, que está protegido mediante un cortafuegos (22) y presenta varios ordenadores (23) virtuales ejecutables adyacentes, que están configurados en cada caso para el mismo tipo o tipos diferentes de conexiones (24, 25) de comunicación con controles de máquina, pudiendo conectarse el ordenador (12) de servicio con el ordenador central (21) a través de una conexión (25) de Internet y pudiendo conectarse el ordenador (21) central con un control de máquina a través del ordenador (23) virtual que está configurado para la conexión (24) de comunicación asociada a este control de máquina, a través de una conexión (24) de Internet.

8.- Sistema según la reivindicación 6, **caracterizado porque** la conexión de comunicación (24, 25) entre el ordenador (12) de servicio o portal (13) de servicio y el control de máquina se realiza directamente a través de Internet (27).

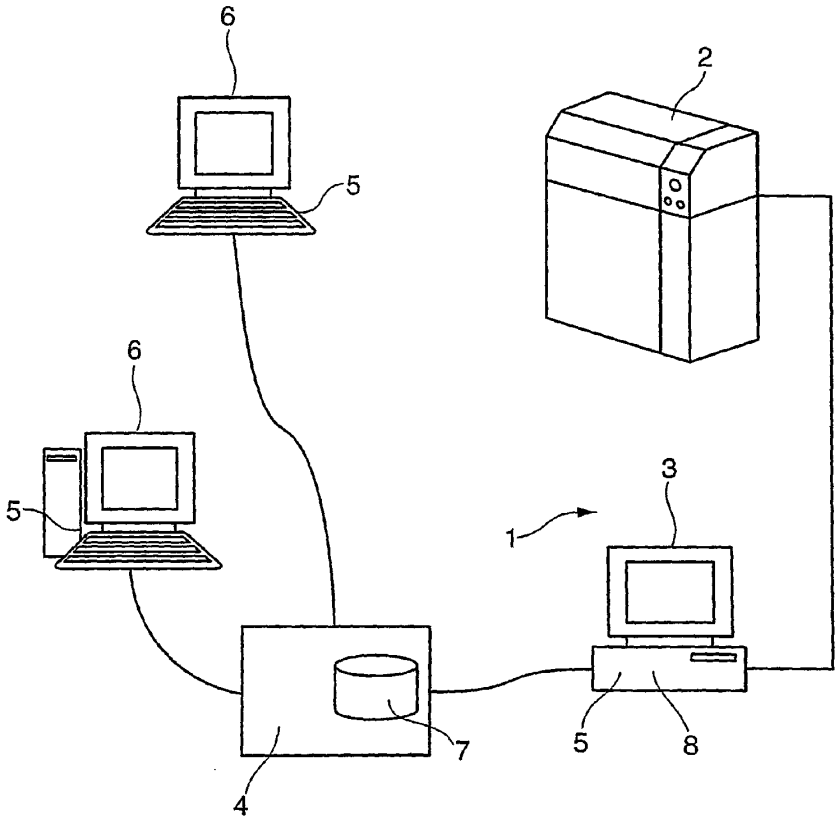

Fig. 1

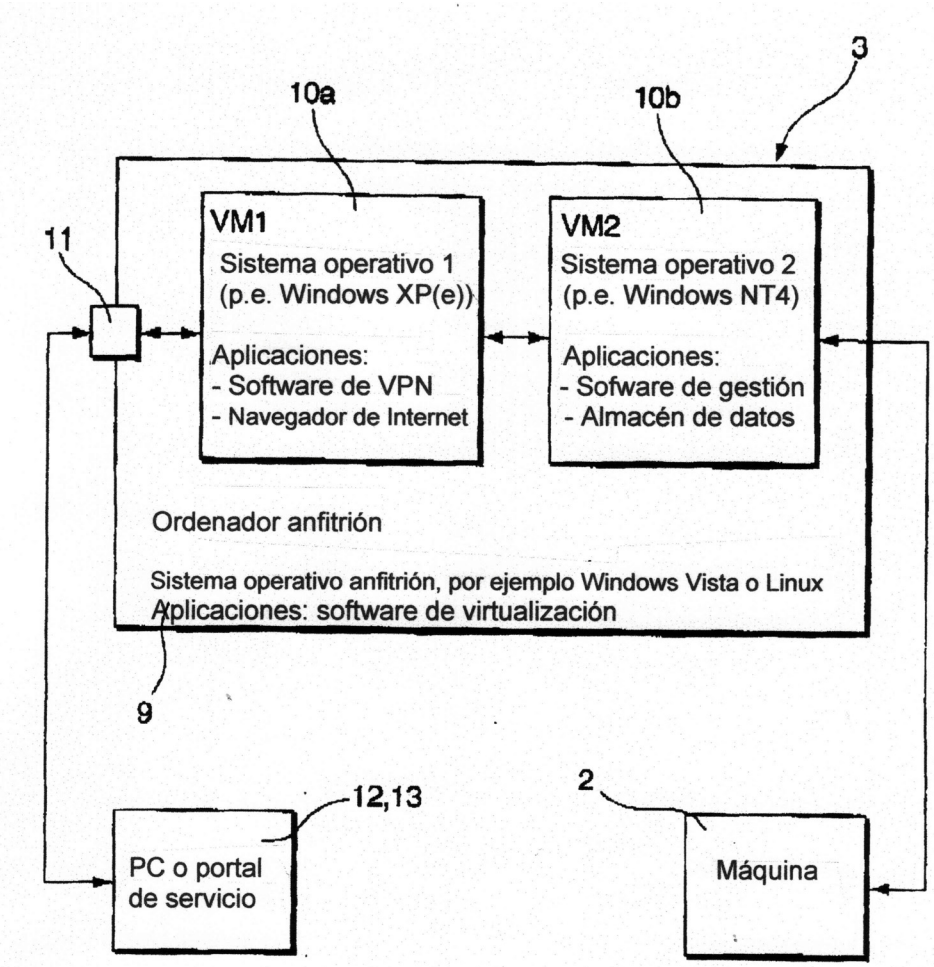
3
10a
10b
11
VM1
Sistema operativo 1
(p.e. Windows XP(e))
Aplicaciones:
- Software de VPN
- Navegador de Internet
VM2
Sistema operativo 2
(p.e. Windows NT4)
Aplicaciones:
- Sofware de gestión
- Almacén de datos
Ordenador anfitrión
Sistema operativo anfitrión, por ejemplo Windows Vista o Linux
Aplicaciones: software de virtualización
9
12,13
PC o portal
de servicio
2
Máquina

Fig. 2

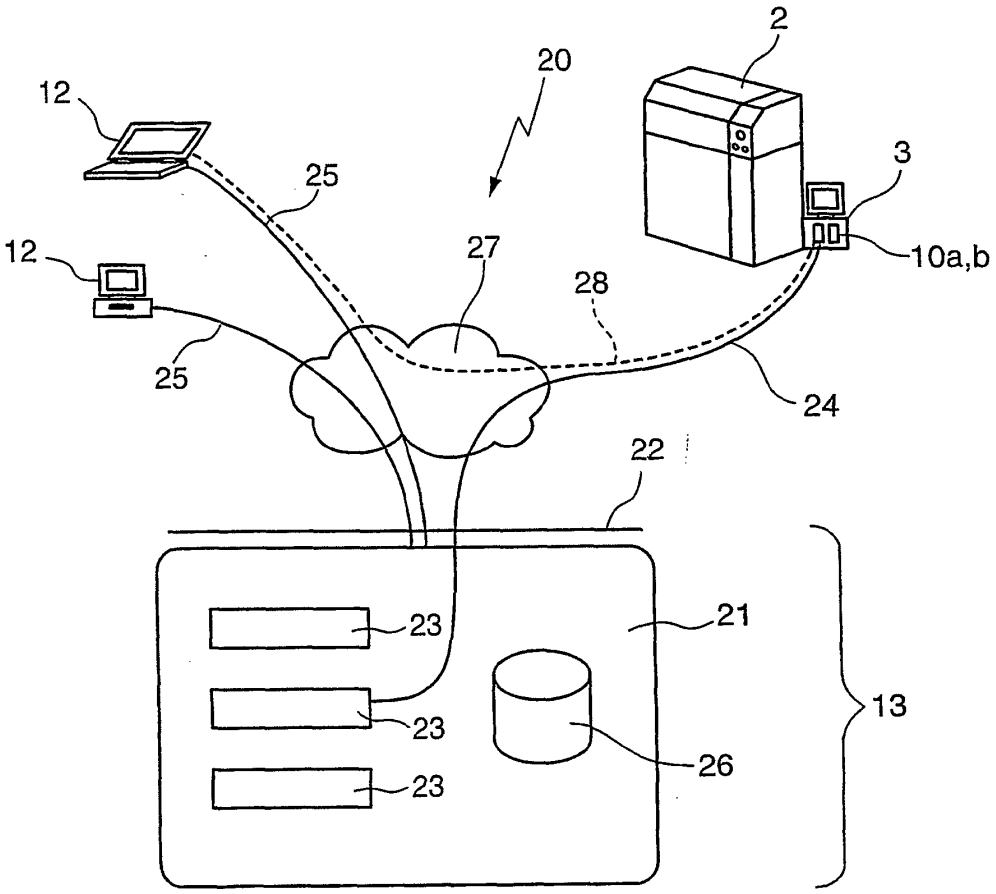

Fig. 3

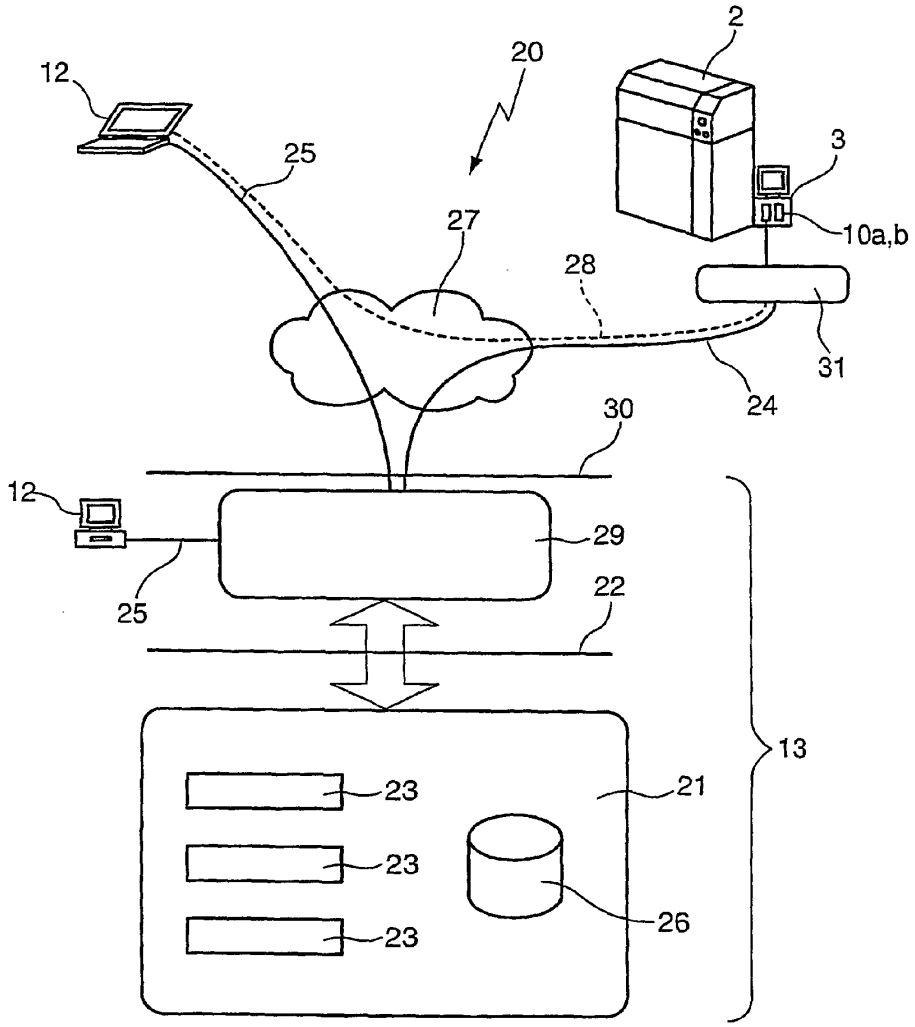

Fig. 4