(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 368 670**

(51) Int. CI.:
G05B 19/042 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **08803303 .0**
(96) Fecha de presentación: **28.08.2008**
(97) Número de publicación de la solicitud: **2193406**
(97) Fecha de publicación de la solicitud: **09.06.2010**

(54) Título: **PROCEDIMIENTO PARA EL CONTROL DEL ACCESO A UNA INSTALACIÓN DE AUTOMATIZACIÓN.**

(30) Prioridad:
25.09.2007 DE 102007045772

(45) Fecha de publicación de la mención BOPI:
21.11.2011

(45) Fecha de la publicación del folleto de la patente:
21.11.2011

(73) Titular/es:
SIEMENS AKTIENGESELLSCHAFT
WITTELSBACHERPLATZ 2
80333 MÜNCHEN, DE

(72) Inventor/es:
FALK, Rainer;
KOHLMAYER, Florian y
KÖPF, Andreas

(74) Agente: **Zuazo Araluze, Alexander**

Aviso: En el plazo de nueve meses a contar desde la fecha de publicación en el Boletín europeo de patentes, de la mención de concesión de la patente europea, cualquier persona podrá oponerse ante la Oficina Europea de Patentes a la patente concedida. La oposición deberá formularse por escrito y estar motivada; sólo se considerará como formulada una vez que se haya realizado el pago de la tasa de oposición (art. 99.1 del Convenio sobre concesión de Patentes Europeas).

DESCRIPCIÓN

Procedimiento para el control del acceso a una instalación de automatización

Con la introducción de la técnica de la información (IT) en la automatización y con la creciente integración con entornos de oficina, aumenta también la necesidad de soluciones de seguridad para entornos de automatización. El control de accesos es entonces una funcionalidad de seguridad esencial, mediante la que se fija e impone quién puede realizar qué operaciones. Así puede fijarse por ejemplo qué accesos puede realizar el personal de operación para operar y observar un proceso o una fabricación o bien un proceso continuo o de fabricación.

Tres columnas principales de la seguridad en la IT son la confidencialidad, la integridad y la disponibilidad. Referido a entornos de oficina típicos, la mayoría de las veces juega el papel principal la confidencialidad y la integridad de los datos. En el entorno de automatización es no obstante más importante la disponibilidad que la confidencialidad de los datos. Usualmente no suele tratarse al respecto de datos muy secretos, sino principalmente de la transmisión de órdenes de control y de estado a través de la red.

Debido al entorno de aplicación, deben tenerse en cuenta allí condiciones marginales especiales. Así por ejemplo en un entorno de automatización en técnica de procesos continuos no debe detenerse de forma así de simple un proceso de fabricación/en la industria de procesos un proceso físico, como por ejemplo el calentamiento y la agitación de un adhesivo en un caso de emergencia de seguridad en el control de la instalación. Igualmente a la inversa no debe de impedirse en un caso de emergencia, por ejemplo en un sobrecalentamiento del adhesivo, una intervención por parte del personal de servicio mediante medidas de seguridad de IT. Unos derechos de acceso estrictamente implantados, tal como es deseable desde el punto de vista de la seguridad de la IT, no deben dar lugar a que en un tal caso de emergencia las intervenciones manuales necesarias se impidan o se dificulten innecesariamente.

Un control de accesos basado en roles (RBAC; Role Based Access Control) es ya conocido. En la práctica se entiende bajo ello a menudo solamente una administración de derechos de acceso basada en roles. Entonces se definen grupos en función de las tareas que se presentan. Se asignan derechos de acceso a distintos grupos. Los distintos colaboradores se asignan a los grupos correspondientes a sus tareas y reciben así los derechos de acceso necesarios para su tarea.

Considerado desde el punto de vista teórico, RBAC significa que un determinado colaborador asume en distintos momentos distintas tareas y correspondientemente en distintos instantes asume distintos roles. Si entre varios instantes varían las tareas del colaborador, ejecuta el mismo para ello en cada caso un cambio de rol, para recibir los derechos de acceso asociados al rol asumido en cada momento.

Por el documento EP 1621 944 A2 se conoce un procedimiento para el control del acceso a una instalación de automatización en el que los derechos de acceso prescritos por el control de accesos dependen del estado de funcionamiento de la instalación de automatización.

Por Covington y colab. "Securing Context-Aware Applications Using Environment Roles" (asegurar aplicaciones sensibles al contexto utilizando roles del entorno", actas del 6º simposio ACM de modelos y tecnologías de control de accesos, Chantilly, Virginia, Estados Unidos, págs. 10-20, 2001, ISBN:1-58113-350-2 se conoce además un control de accesos basado en el contexto en la atención y vigilancia de personas mayores en el hogar, en el que los derechos de acceso dependen de una información de contexto denominada también información de entorno. Esta información de contexto se refiere a la hora del día, el día de la semana, el lugar de estancia o el estado actual de una secuencia de trabajo. Los derechos de acceso están asignados a determinados roles de entorno. Los distintos roles de entorno pueden ser activados por informaciones de contexto. Una activación de un rol de entorno puede activar automáticamente una acción. Así por ejemplo cuando hay una activación del rol de entorno "vulneración" se establece automáticamente una llamada de emergencia.

Puede considerarse como tarea de la invención proporcionar un control de accesos mejor adaptado a un entorno de automatización.

La tarea se soluciona según la invención mediante las características de la reivindicación 1.

Un procedimiento correspondiente a la invención para el control de accesos en una instalación de automatización prevé que los derechos de acceso prescritos por el control de accesos dependan del estado de servicio de la instalación de automatización, otorgándose al menos en un caso de emergencia, independientemente de los derechos de acceso en funcionamiento normal, derechos de acceso más amplios que los del funcionamiento normal.

Al otorgarse al menos en casos de emergencia un acceso de emergencia con derechos de acceso ampliados, se posibilita una operación rápida y flexible, que no se ve impedida o dificultada innecesariamente por medidas de seguridad de IT.

La invención tiene ventajas respecto al estado de la técnica en particular dado que para el servicio regular operativo de la instalación de automatización pueden establecerse derechos de acceso restrictivos según las necesidades del funcionamiento regular. Para estados de servicio especiales, en particular en un caso de emergencia, se otorgan derechos de acceso correspondientemente ampliados.

Se definen básicamente roles que corresponden a los diferentes estados de servicio de una instalación de automatización. No se realiza a libre elección un cambio de roles como en el RBAC, sino que los derechos de acceso dependen del estado de servicio. En funcionamiento normal se logra un gran nivel de seguridad y pueden establecerse derechos de acceso restrictivos, ya que sólo en un estado de servicio especial, como por ejemplo en trabajos de mantenimiento o en un caso de emergencia, se otorgan derechos de acceso ampliados, que son entonces necesarios. Esto puede considerarse también como un cierto modo de funcionalidad override (invalidación), en el que en determinadas circunstancias el control de los derechos de acceso puede ponerse fuera de servicio.

Además se simplifica la gestión de los derechos de acceso, ya que sólo tienen que fijarse de manera exacta y estricta los derechos de acceso para el funcionamiento normal. En situaciones especiales se otorgan derechos de acceso ampliados bajo la hipótesis de que el personal cualificado y de confianza que realiza la operación y el mantenimiento no abusa bajo tales circunstancias de los derechos de acceso. Esta confianza está basada en que de todos modos existe una elevada responsabilidad del personal de operación y mantenimiento, ya que el mismo debe realizar tareas de mantenimiento, como por ejemplo cambio de herramientas o calibración o bien una parada controlada de un proceso continuo, que no está automatizado o no por completo.

Una configuración ventajosa de la invención prevé que para detectar el estado de servicio se vigile la instalación de automatización. La vigilancia puede realizarse mediante sensores adecuados o mediante personal de operación y mantenimiento.

Preferiblemente se activa automáticamente un caso de emergencia tan pronto como determinadas magnitudes de proceso de la instalación de automatización sobrepasan valores límite prescritos. Igualmente puede pensarse en activar manualmente un caso de emergencia mediante el personal de operación y vigilancia.

Una configuración ventajosa de la invención prevé que los derechos de acceso se fijen estrictamente para el funcionamiento normal, para evitar operaciones incorrectas y accesos no autorizados.

Otra configuración ventajosa de la invención prevé que los derechos de acceso se determinen para el funcionamiento normal basados en roles.

Otra configuración ventajosa de la invención prevé que para el funcionamiento normal, para lograr derechos de acceso y/o para lograr derechos de acceso adicionales y/u otros derechos de acceso, se realice una identificación de la persona que accede o bien una autentificación por ejemplo mediante un protocolo log-in (de acceso). El protocolo log-in puede tener cualquier configuración, por ejemplo introduciendo el nombre del usuario y/o la palabra de paso, mediante un token (validador) de autentificación, como por ejemplo mediante una tarjeta de chip o inalámbricamente, o mediante una huella dactilar o cualquier otra identificación biométrica.

Una configuración ventajosa adicional de la invención prevé que al presentarse un caso de emergencia se active una alarma, para dar automáticamente la alarma y activar medidas de emergencia, por ejemplo para que las fuerzas de intervención puedan confirmar el caso de emergencia.

Una configuración especialmente ventajosa de la invención prevé que al menos durante un caso de emergencia o bien en un caso de servicio para el que estén otorgados derechos de acceso ampliados, las acciones y accesos llevados a cabo por el personal de operación y mantenimiento sean registradas por ejemplo por una cámara de video y/o protocolizados por ejemplo en un servidor de logging o acceso. Los derechos de acceso pueden así sobrepasarse caso necesario, en cierta medida según deseo. Pero esto queda patente tanto mediante el registro y protocolización de los accesos llevados a cabo como también mediante la activación de la vigilancia de video y puede comprobarse así posteriormente si esto tuvo lugar efectivamente sobre una base justificada.

Una configuración ventajosa de la invención prevé que al menos en un caso de emergencia esté previsto un modo especial de seguridad para casos de emergencia, en el que los duros y estrictos controles y otorgación de derechos de acceso previstos para el funcionamiento normal sean sustituidos por medidas más suaves, que no obstante posteriormente puedan evaluarse o bien se evalúen. La sustitución de duras medidas de seguridad vigentes durante el funcionamiento normal por medidas de seguridad más suaves en un caso de emergencia posibilita que pueda llevar a cabo todas las medidas necesarias el personal de operación y vigilancia, evitándose no obstante un abuso, ya que el hecho de la activación del caso de emergencia, así como las acciones realizadas y los accesos realizados, pueden reproducirse posteriormente.

Preferiblemente incluyen las medidas más suaves el otorgamiento de derechos de acceso ampliados y/o dado el caso una desactivación del control y otorgamiento de derechos de acceso, permitiéndose así todas las operaciones y accesos.

Alternativamente puede pensarse en que las medidas más suaves incluyan una renuncia a una autentificación, por ejemplo mediante log-in, con lo que cualquier persona puede utilizar un equipo de operación y vigilancia que controla la instalación de automatización.

Para la evaluación posterior de las medidas más suaves, se realiza preferiblemente un registro y protocolización de los accesos llevados a cabo. Esto puede realizarse sobre el propio equipo de operación y vigilancia o sobre un servidor de logging previsto expresamente para ello, por ejemplo alojado en una sala resistente a la emergencia, por ejemplo segura frente al fuego y/o a la explosión.

Para la evaluación posterior de las medidas más suaves puede realizarse por ejemplo una activación de una vigilancia de video o bien una activación de un registro de video, para detectar así en base al material de video registrado quién ha activado el modo de seguridad de emergencia y quién ha realizado qué accesos o bien acciones.

Preferiblemente incluye el modo de seguridad para casos de emergencia varios escalones con distintos derechos de acceso, que pueden activarse o bien se activan paso a paso. Puesto que eventualmente ya son suficientes derechos de acceso mínimamente aumentados para protegerse prácticamente como primera ayuda del peor caso en una emergencia, incluye el modo de seguridad para casos de emergencia preferiblemente varios escalones. Éstos pueden activarse paso a paso. En un primer escalón de activación para casos de emergencia pueden por ejemplo otorgarse sólo los derechos más necesarios, para por ejemplo demorar un caso de emergencia inminente y poder iniciar contramedidas sencillas. En el caso de que se necesiten medidas más amplias para impedir el caso de emergencia, entonces debe activarse también adicionalmente un segundo escalón de activación de casos de emergencia, que otorga un acceso más amplio, por ejemplo ilimitado. Por ejemplo puede pensarse en que entonces también puedan realizarse modificaciones de configuración duraderas. La activación de un tal segundo escalón de activación para casos de emergencia puede entonces estar protegida de forma más costosa que el primer escalón de activación para casos de emergencia. Así puede pensarse por ejemplo en activar el primer escalón de activación para casos de emergencia mediante un clic de ratón en el nivel de usuario del equipo de operación y vigilancia y el segundo escalón de activación para casos de emergencia sólo mediante un interruptor de seguridad físico, que por ejemplo sólo puede accionarse tras romper un cristal de protección.

La activación del modo de seguridad para casos de emergencia puede realizarse manualmente, por ejemplo accionando un pulsador especial sobre un nivel de operación gráfica. Para impedir la activación del modo de seguridad para casos de emergencia por comodidad durante el servicio regular operativo, está previsto para ello un pulsador especial sobre un nivel de operación gráfico, mediante cuyo accionamiento se realiza un cambio manual al modo de seguridad de emergencia. Entonces puede ser accesible el cambio manual en el modo de seguridad para casos de emergencia a todos los colaboradores, o sólo a determinados colaboradores autentificados, por ejemplo sólo al o a los supervisores.

Alternativamente puede realizarse una activación manual del modo de seguridad para casos de emergencia accionando un interruptor de seguridad físico. Un tal interruptor de seguridad físico puede ser por ejemplo un interruptor de llave, o un pulsador con cristal de ruptura, tal como se conoce por ejemplo en los avisadores de incendio, o bien dos interruptores alejados espacialmente, que deben ser accionados preferiblemente por al menos dos personas a la vez. En este último caso pueden estar alojados ambos interruptores en la instalación de automatización, pero a una distancia tal que no puedan ser accionados por una sola persona a la vez. Ambos interruptores pueden estar dispuestos separados espacialmente también tal que un interruptor esté alojado por ejemplo en la propia instalación de automatización y el segundo interruptor en una central de seguridad alejada.

El interruptor físico puede estar acoplado con un botón para incendios o de alarma, con lo que cuando se acciona adicionalmente se emite una alarma, por ejemplo a los bomberos de la fábrica.

Además puede pensarse en que se realice una activación manual del modo de seguridad para casos de emergencia mediante un protocolo log-in especial, por ejemplo la introducción de una palabra de paso especial para casos de emergencia o la utilización de un token (validador) especial de autentificación para casos de emergencia, como por ejemplo una tarjeta de chip para casos de emergencia.

La activación del modo de seguridad para casos de emergencia se realiza preferiblemente de forma automática en función del estado de servicio de la instalación de automatización. Para ello se vigilan determinados parámetros de la instalación de automatización y se decide, por ejemplo de forma automática mediante comparación con valores límite prescritos para estos parámetros, si existe un estado de servicio normal o un caso de emergencia. En instalaciones de automatización de procesos continuos pueden medirse por ejemplo la presión y la temperatura mediante sensores adecuados, dispuestos preferiblemente de forma redundante, vigilándose de forma automática mediante comparación con valores límites fijados, como por ejemplo una temperatura máxima admisible, una presión máxima admisible, una

temperatura mínima, una presión mínima y determinándose si los valores de medida para la presión y la temperatura en la instalación de automatización se encuentran cuando se realiza un determinado proceso continuo dentro de una determinada zona de funcionamiento admisible, es decir, si existe un caso de servicio normal o no, es decir, un caso de emergencia. Alternativamente puede también vigilarse la velocidad de giro del motor y compararse con valores de consigna fijados.

El modo de seguridad para casos de emergencia puede permanecer tras la activación hasta que se desactiva de nuevo manualmente, por ejemplo accionando un interruptor o de forma similar.

Alternativamente puede pensarse en que el modo de seguridad para casos de emergencia se desactive de nuevo de forma automática tras su activación después de un espacio de tiempo predeterminado.

Igualmente puede desactivarse automáticamente el modo de seguridad para casos de emergencia tras la activación una vez finalizado el caso de emergencia, por ejemplo cuando los valores de medida captados por sensores se encuentren de nuevo dentro de una zona de servicio admisible.

Además puede pensarse en que el modo de seguridad para casos de emergencia sólo permanezca activo mientras que se accione o se mantenga activado el correspondiente interruptor de activación o similar.

La invención se describirá a continuación en base a un ejemplo de ejecución representado en el dibujo. Se muestra en:

figura 1 una representación esquemática de una instalación de automatización.

Una instalación de automatización 01 representada en la figura 1 incluye un agitador 02 que es accionado por un motor 03. El agitador 02 agita una sustancia en un recipiente 04. En el recipiente 04 se encuentra un calentador 05 y un sensor de temperatura 06, estando ambos unidos con un ordenador de procesos 07. Las tuberías para transportar la sustancia hacia y desde el recipiente 04 no se representan. El ordenador de procesos 07 está conectado a un equipo de operación y vigilancia 08. El equipo de operación y vigilancia 08 está conectado a un interruptor de emergencia 09, una cámara de video 10 así como un servidor de logging 11. El personal de operación y mantenimiento 12 vigila y controla el proceso continuo de agitación de la sustancia en el recipiente 04 mediante el equipo de operación y vigilancia 08. En el caso de un incidente o de una emergencia, acciona el personal de operación y mantenimiento 12 el interruptor de emergencia 09, a continuación de lo cual el personal de operación y mantenimiento 12 recibe derechos de acceso ilimitados y con ello acceso ilimitado. No obstante, a la vez son registradas las acciones emprendidas por el personal de operación y mantenimiento 12 y los accesos por la videocámara 10 y se protocolizan en el servidor de logging 11.

En el marco de la invención se realiza para el funcionamiento regular de una instalación de automatización con un equipo de operación y vigilancia un estricto control de accesos, en el que debe autentificarse el personal de operación, por ejemplo mediante un log-in y sólo pueden realizar accesos al equipo de operación y vigilancia que además estén permitidos en base a una política de control de accesos definida. El objeto es entonces menos lograr una elevada confidencialidad de los datos de automatización trasmitidos que más bien evitar operaciones incorrectas y accesos no autorizados. El protocolo de log-in puede estar configurado de cualquier forma, por ejemplo mediante introducción del número de usuario y/o la palabra de paso, mediante un token o validador de automatización, como por ejemplo mediante una tarjeta de chip, o inalámbricamente, o mediante una huella dactilar u otra cualquier identificación biométrica.

Para poder reaccionar de manera adecuada en casos de emergencia, que naturalmente pueden incluir aspectos imprevisibles, son necesarios allí derechos de acceso ampliados. En el marco de la invención se otorgan en casos de emergencia derechos de acceso ampliados. Es posible así un manejo rápido y flexible, que no se ve impedido o innecesariamente estorbado por medidas de seguridad de IT.

Para ello está previsto un modo de seguridad especial para casos de emergencia/una configuración especial de seguridad para casos de emergencia.

Entonces se sustituye el control de accesos previsto para el funcionamiento normal o bien servicio regular por medidas más suaves, que no obstante pueden evaluarse a posteriori:

- Otorgamiento de derechos de acceso ampliados y/o dado el caso desactivación del control de accesos, con lo que se permiten todos los accesos.
- Renuncia a la autentificación por ejemplo mediante log-in, con lo que cualquiera puede utilizar el equipo de operación y vigilancia.
- Registro y protocolización de los accesos realizados, el llamado logging. Esto puede realizarse sobre el propio equipo de operación y vigilancia o sobre un servidor de logging previsto especialmente al respecto, por ejemplo alojado en una sala resistente a las emergencias, por ejemplo segura frente a incendios y/o segura frente a explosiones.

- Activación de una vigilancia de video o bien activación de un registro de video, para detectar así en base al material de video registrado quién ha activado el modo de seguridad para casos de emergencia y quién ha realizado qué accesos o bien acciones.
- Activación de una alarma, para que las fuerzas de intervención puedan confirmar el caso de emergencia.

La sustitución de estrictas medidas de seguridad válidas durante el funcionamiento normal por medidas de seguridad más suaves en un caso de emergencia, posibilita que el personal de operación y vigilancia pueda tomar todas las medidas necesarias. No obstante, se impide un abuso, ya que el hecho de la activación del caso de emergencia, así como las acciones emprendidas y los accesos realizados, pueden reproducirse a posteriori.

Los derechos de acceso pueden así sobrepasarse caso necesario, en determinada medida según deseo. No obstante esto queda detectado, tanto mediante el registro y protocolización de los accesos realizados, como también mediante la activación de una vigilancia de video y puede comprobarse así a posteriori si esto se realizó efectivamente sobre una base justificada.

Puesto que eventualmente ya son suficientes unos derechos de acceso mínimamente superiores para poder impedir, prácticamente como primera ayuda, lo peor que pueda suceder en un caso de emergencia, puede incluir el modo de seguridad en caso de emergencia varios escalones. Éstos pueden activarse paso a paso. En un primer escalón de activación para casos de emergencia pueden por ejemplo otorgarse sólo los derechos muy necesarios, para por ejemplo retardar un caso de emergencia inminente e iniciar contramedidas sencillas. En el caso de que sean necesarias medidas más amplias para impedir el caso de emergencia, debe activarse a continuación una segunda etapa de activación para casos de emergencia, que otorga un acceso más amplio, por ejemplo ilimitado. Por ejemplo puede pensarse en que entonces se realicen también modificaciones de configuración duraderas. La activación de un tal segundo escalón de activación para casos de emergencia puede entonces estar protegida de manera más costosa que el primer escalón de activación para casos de emergencia. Así puede pensarse por ejemplo en que el primer escalón de activación para casos de emergencia pueda activarse mediante un clic de ratón en el nivel de usuario del equipo de operación y vigilancia y el segundo escalón de activación para casos de emergencia sólo mediante un interruptor de seguridad físico, que por ejemplo sólo pueda accionarse tras romper un cristal de protección.

El cambio al modo de seguridad para casos de emergencia puede realizarse de distintas formas. Al respecto es importante que el significado especial quede claro y por lo tanto se evite una activación por comodidad durante el funcionamiento operativo regular.

Una primera variante que asegura que se evita una activación del modo de seguridad para casos de emergencia por comodidad durante el funcionamiento operativo regular puede lograrse por ejemplo en base a un pulsador especial sobre un nivel de operación gráfica, mediante cuya activación se realiza un cambio manual al modo de seguridad para casos de emergencia. Entonces puede ser accesible el cambio manual al modo de seguridad para casos de emergencia para todos los colaboradores o sólo para determinados colaboradores autentificados, por ejemplo sólo para el o los supervisores.

Una segunda variante que asegura que se evita una activación del modo de seguridad para casos de emergencia por comodidad durante el funcionamiento operativo regular, es la utilización de un interruptor de seguridad físico para activar el modo de seguridad para casos de emergencia. Un tal interruptor de seguridad físico puede ser por ejemplo un interruptor de llave, o un pulsador con cristal de ruptura, tal como se conoce por ejemplo en los avisadores de incendio, o bien dos interruptores alejados espacialmente, que deben ser accionados por al menos dos personas preferiblemente a la vez. En este último caso pueden estar alojados ambos interruptores en la instalación de automatización, pero a una distancia tal que no puedan ser accionados por una sola persona a la vez. Ambos interruptores pueden también estar dispuestos separados espacialmente tal que un interruptor esté alojado por ejemplo en la propia instalación de automatización y el segundo interruptor en una central de seguridad alejada. Los interruptores de seguridad físicos descritos pueden estar acoplados con un auténtico botón para incendios o alarmas, con lo que cuando se acciona se emite adicionalmente una alarma, por ejemplo para los bomberos de la fábrica.

Una tercera variante que asegura que se evita una activación del modo de seguridad para casos de emergencia por comodidad durante el funcionamiento operativo regular prevé un protocolo de log-in especial, por ejemplo la introducción de una palabra de paso especial para casos de emergencia o la utilización de un token de autentificación especial para casos de emergencia, como por ejemplo una tarjeta de chip para casos de emergencia.

Una cuarta variante que asegura que se evita una activación del modo de seguridad para casos de emergencia por comodidad durante el funcionamiento operativo regular, depende automáticamente del estado de servicio de la instalación de automatización. Para ello se vigilan determinados parámetros de la instalación de automatización y se decide de forma automática, por ejemplo comparando con valores límites prescritos para estos parámetros, si existe un estado de servicio normal o un caso de emergencia. En instalaciones de automatización de procesos continuos pueden medirse por ejemplo la presión y la temperatura mediante sensores adecuados, dispuestos preferiblemente de forma redundante, vigilándose y mediante comparación con valores límites fijados, como por ejemplo una temperatura máxima admisible, una presión máxima admisible, una temperatura mínima, una presión mínima, de forma automática y

determinándose si los valores de medida para la presión y la temperatura en la instalación de automatización se encuentran cuando se realiza un determinado proceso continuo dentro de una zona de servicio determinada admisible, es decir, si existe un caso de servicio normal o no, es decir, un caso de emergencia.

El modo de seguridad para casos de emergencia bien permanece tras la activación de forma permanente hasta que se desactiva el mismo manualmente, por ejemplo accionando un interruptor o similar, o bien se desactiva de nuevo automáticamente tras un determinado espacio de tiempo prescrito. El modo de seguridad para casos de emergencia puede también desactivarse tras desaparecer el caso de emergencia de forma automática, por ejemplo cuando los valores de medida captados por sensores se encuentren de nuevo dentro de la zona de servicio admisible. Como posibilidad adicional puede pensarse en que el modo de seguridad para casos de emergencia sólo permanezca activado hasta que se accione o permanezca activado el correspondiente interruptor de activación o similar.

REIVINDICACIONES

1. Procedimiento para el control de accesos a una instalación de automatización, en el que los derechos de acceso prescritos por el control de acceso dependen del estado de servicio de la instalación de automatización (01),
caracterizado porque al menos en un caso de emergencia, independientemente de los derechos de acceso en funcionamiento normal, se otorgan derechos de acceso ampliados.

2. Procedimiento según la reivindicación 1,
caracterizado porque para captar el estado de servicio se vigila la instalación de automatización (01).

3. Procedimiento según la reivindicación 2,
caracterizado porque la vigilancia se realiza automáticamente mediante sensores adecuados (06).

4. Procedimiento según la reivindicación 2,
caracterizado porque la vigilancia se realiza mediante un personal de operación y mantenimiento (12).

5. Procedimiento según una de las reivindicaciones precedentes,
caracterizado porque se activa automáticamente un caso de emergencia tan pronto como determinadas magnitudes de proceso de la instalación de automatización (01) sobrepasan los valores límite prescritos.

6. Procedimiento según una de las reivindicaciones 1 a 4,
caracterizado porque el caso de emergencia se activa manualmente.

7. Procedimiento según una de las reivindicaciones precedentes,
caracterizado porque los derechos de acceso se fijan de manera estricta en caso normal, para evitar operaciones incorrectas y accesos no autorizados.

8. Procedimiento según una de las reivindicaciones precedentes,
caracterizado porque los derechos de acceso se fijan en funcionamiento normal basados en roles.

9. Procedimiento según una de las reivindicaciones precedentes,
caracterizado porque en funcionamiento normal, para lograr derechos de acceso y/o para lograr derechos de acceso adicionales y/u otros derechos de acceso, se realiza una identificación de la persona que accede o bien una autentificación.

10. Procedimiento según una de las reivindicaciones precedentes,
caracterizado porque al presentarse un caso de emergencia se activa una alarma para dar automáticamente la alarma y activar medidas de emergencia.

11. Procedimiento según una de las reivindicaciones precedentes,
caracterizado porque al menos en un caso de emergencia se registran y/o protocolizan las acciones y accesos realizados por un personal de operación y mantenimiento (12).

12. Procedimiento según una de las reivindicaciones precedentes,
caracterizado porque al menos en un caso de emergencia está previsto un modo de seguridad especial para casos de emergencia, en el que se sustituyen el duro control y otorgamiento de derechos de acceso previsto para el funcionamiento normal por medidas más suaves, que pueden evaluarse o bien se evalúan a posteriori.

13. Procedimiento según la reivindicación 12,
caracterizado porque las medidas más suaves incluyen el otorgamiento de derechos de acceso ampliados y/o una desactivación del control y otorgamiento de derechos de acceso, con lo que se permiten todas las operaciones y accesos.

14. Procedimiento según la reivindicación 12,
caracterizado porque las medidas de seguridad más suaves incluyen la renuncia a una autentificación, con lo que cualquier persona puede utilizar un equipo de operación y vigilancia (08) que controla la instalación de automatización (01).

15. Procedimiento según la reivindicación 12, 13 ó 14,
caracterizado porque para la posterior evaluación de las medidas más suaves se realiza un registro y protocolización de los accesos realizados.

16. Procedimiento según una de las reivindicaciones 12 a 15,
caracterizado porque para la evaluación a posteriori de las medidas más suaves se realiza una activación de una vigilancia por video (10) o bien una activación de un registro de video.

17. Procedimiento según una de las reivindicaciones 12 a 16,
caracterizado porque el modo de seguridad para casos de emergencia incluye varios escalones con distintos derechos de acceso, que pueden activarse o bien que se activan paso a paso.

18. Procedimiento según una de las reivindicaciones 12 a 17,
caracterizado porque la activación del modo de seguridad para casos de emergencia se realiza manualmente.

19. Procedimiento según la reivindicación 18,
caracterizado porque la activación del modo de seguridad para casos de emergencia se realiza activando un pulsador especial sobre un nivel de operación gráfico.

20. Procedimiento según la reivindicación 18,
caracterizado porque la activación del modo de seguridad para casos de emergencia se realiza accionando un interruptor de seguridad físico (09).

21. Procedimiento según la reivindicación 20,
caracterizado porque el interruptor físico (09) está acoplado con un botón para incendios o alarma.

22. Procedimiento según la reivindicación 18,
caracterizado porque la activación del modo de seguridad para casos de emergencia se realiza mediante un protocolo de log-in especial.

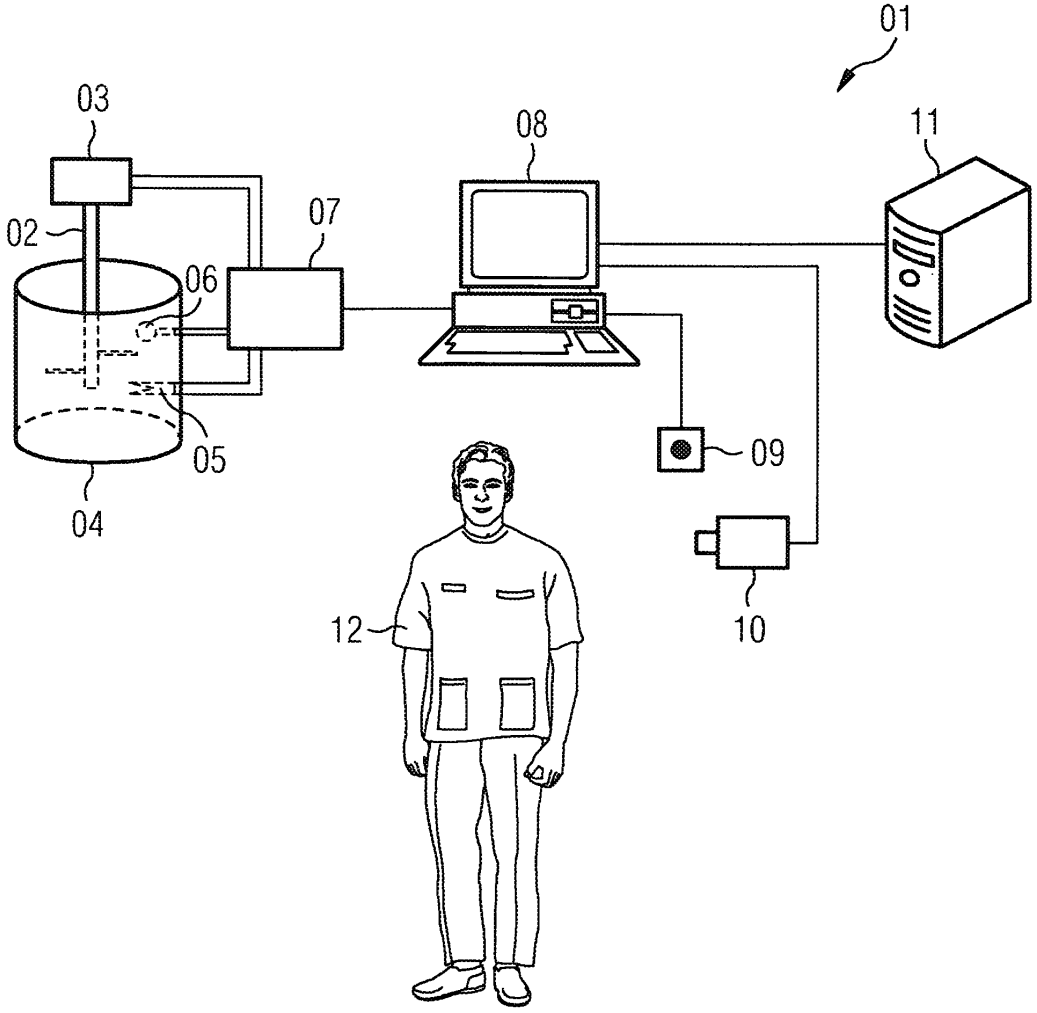
23. Procedimiento según una de las reivindicaciones 12 a 17,
caracterizado porque la activación del modo de seguridad para casos de emergencia se realiza automáticamente en función del estado de servicio de la instalación de automatización (01).

24. Procedimiento según una de las reivindicaciones 12 a 23,
caracterizado porque el modo de seguridad para casos de emergencia permanece tras la activación hasta que el mismo es desactivado manualmente.

25. Procedimiento según una de las reivindicaciones 12 a 23,
caracterizado porque el modo de seguridad para casos de emergencia se desactiva automáticamente tras la ctivación una vez transcurrido un espacio de tiempo predeterminado.

26. Procedimiento según una de las reivindicaciones 12 a 23,
caracterizado porque el modo de seguridad para casos de emergencia se desactiva automáticamente tras la activación tras desaparecer el caso de emergencia.

27. Procedimiento según una de las reivindicaciones 12 a 23,
caracterizado porque el modo de seguridad para casos de emergencia sólo permanece activado mientras se accione el correspondiente interruptor de activación (09).


01
03
08
11
02
07
06
05
04
09
10
12