(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 372 415**

(51) Int. CI.:
G06Q 10/00 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **06703077 .5**
(96) Fecha de presentación: **18.01.2006**
(97) Número de publicación de la solicitud: **1851698**
(97) Fecha de publicación de la solicitud: **07.11.2007**

(54) Título: **SISTEMA DE MONITORIZACIÓN Y GESTIÓN DE ACCESO, MÉTODO Y PRODUCTO INFORMÁTICO CORRESPONDIENTES.**

(30) Prioridad:
27.01.2005 IT TO20050047

(45) Fecha de publicación de la mención BOPI:
19.01.2012

(45) Fecha de la publicación del folleto de la patente:
19.01.2012

(73) Titular/es:
MICRONTEL S.P.A.
REGIONE PESCARITO, VIA UMBRÍA 13
10099 SAN MAURO TORINESE, IT

(72) Inventor/es:
ALIVERTI, Adriano y
MIGLIASSO, Giuseppe

(74) Agente: **Curell Aguilá, Marcelino**

DESCRIPCIÓN

Sistema de monitorización y gestión de acceso, método y producto informático correspondientes.

Campo de la invención

La presente invención se refiere a técnicas de monitorización y gestión de acceso, y se ha desarrollado prestando atención específica a posibles aplicaciones en procedimientos de control de acceso relacionados con sistemas de comprobación de presencia y de control horario, que comprenden en particular controles de paso. No obstante, el alcance de la invención se extiende a cualquier sistema de registro y señalización de eventos, en los que existan las condiciones que se describen posteriormente.

Descripción de los antecedentes de la técnica

Los sistemas de control de acceso se usan, en general, para controlar el acceso de personal a lugares de trabajo, por ejemplo, a través de aparatos de impresión, y/o a áreas restringidas. El sistema de control de acceso debe conceder y registrar el acceso para las personas autorizadas, y denegar el acceso a personas no autorizadas.

Por ejemplo, el documento US 2004/0093309 se refiere a un sistema de gestión de tiques de entrada electrónicos que incluye un organizador de eventos para planificar un evento, un vendedor de tiques de entrada electrónicos para distribuir información de tiques de entrada electrónicos que autentica el derecho a asistir al evento, un chip de almacenamiento de información para almacenar la información de los tiques de entrada electrónicos, y un centro de plataforma de tiques de entrada electrónicos para gestionar la distribución de la información de tiques de entrada electrónicos. Se toma una determinación sobre si al usuario se le permite entrar en el recinto del evento según la integridad de la información de evento almacenada en un chip de almacenamiento de información.

Por ejemplo, la patente US nº 6.363.351 da a conocer un sistema que concede, a abonados autorizados, acceso a los eventos seleccionados de entre eventos recreativos en varios recintos recreativos. Preferentemente, el sistema comprende una estación de procesado central y una pluralidad de controladores de puntos de acceso. Cada uno de los controladores de puntos de acceso lee un identificador de abonado presentado por el abonado que asiste al evento recreativo respectivo, y confirma que el abonado que asiste al evento recreativo respectivo dispone de autorización basándose en el identificador de abonado.

Por ejemplo, el documento WO 02/065358 se refiere a un sistema para comprar e imprimir un tique de entrada por medio de Internet. En el lugar del evento se lee un identificador, por ejemplo, un código de barras, incorporado al tique de entrada, y el mismo se usa para comprobar la validez del tique de entrada. El sistema incluye un servidor local dispuesto en el lugar del evento, hacia el cual una copia de la base de datos está dispuesta para ser transferida desde el servidor, y los lectores de identificadores y los identificadores de validez están conectados a dicho servidor local.

Por ejemplo, el documento WO 01/84504 da a conocer un sistema y un método para proporcionar admisión o acceso, sin tiques de entrada físicos en papel, a eventos en recintos. El sistema incluye software para comprar la admisión o el acceso a eventos proporcionando una tarjeta de crédito/débito a un sitio de reservas en Internet. A continuación, el número de la tarjeta de crédito se almacena en una base de datos de admisiones. Seguidamente, el consumidor va al recinto apropiado y pasa su tarjeta de crédito/débito a través de un lector en la entrada del recinto o del medio de transporte. Si se halla una autorización correspondiente a la tarjeta de crédito/débito que se ha pasado por el lector, se permite que el consumidor pase a través de la entrada y hacia el recinto o vehículo de transporte. Por ejemplo, el documento WO 01/63466 describe un navegador web que tiene marcos ocultos para transferir eventos y recibir actualizaciones de páginas. Para mejorar el rendimiento, se emiten por flujo continuo múltiples actualizaciones en un único marco en forma de una sola respuesta HTTP activa. En un aspecto de la invención, en cada actualización se incluye cierto código de guión de instrucciones que se ejecuta dinámicamente después de que se reciba la actualización, transfiriéndose el control a una rutina de actualización, y proporcionándose de este modo un multiplexado en tiempo real a través de una única respuesta HTTP.

Los últimos sistemas de control de acceso comprenden una pluralidad de controles de entrada, por ejemplo, dispositivos situados en varios puntos de acceso en una empresa o fábrica, que están integrados en o asociados a terminales, así como conectados entre sí y a un centro de monitorización por medio de redes de comunicación. A través de dichas redes de comunicación se intercambia información referente a eventos representativos del acceso. Esta información se usa para comprobaciones que conllevan comparaciones con y alteraciones en información contenida en bases de datos implementadas en ordenadores que también están asociados a las redes de comunicación. Tal como se ha dicho, se dispone también de centros de monitorización provistos de terminales asociados a la red con el fin de permitir que los operadores monitoricen y comprueben eventos relacionados con el acceso.

Para garantizar el cumplimiento de normas de seguridad estrictas, dichos sistemas de monitorización y control de acceso requieren que la detección y el control de los eventos que se producen sucesivamente en los diferentes

nodos de la red de acceso se realicen con la mayor similitud posible al tiempo real. No obstante, este objetivo de monitorización en tiempo real es complicado de lograr en una arquitectura de red, especialmente sin usar equipos de hardware altamente especializados o dedicados y protocolos de gestión de software.

Objetivo y breve descripción de la invención

La presente invención pretende resolver el problema antes descrito y propone una solución que permite llevar a cabo una monitorización en tiempo real a través de equipos de hardware no especializados o no dedicados y protocolos de gestión de software.

Según la presente invención, este objetivo se alcanza por medio de un sistema que incorpora las características de las reivindicaciones adjuntas, las cuales forman parte de las enseñanzas técnicas de la invención.

La presente invención se refiere también a un método correspondiente, así como a un producto informático que se puede implementar en la memoria de por lo menos un ordenador y que comprende partes de código de software con el fin de ejecutar el método anterior. En este marco, la referencia a dicho producto informático debe entenderse como una referencia a 3 medios legibles por ordenador que contienen instrucciones para controlar un sistema de ordenador con el fin de coordinar la implementación del método según la invención. La referencia a “por lo menos un ordenador” está destinada a resaltar la posibilidad de implementar la presente invención de una manera distribuida y/o modular.

Breve descripción de los dibujos

A continuación, se describirá la invención a título de ejemplo no limitativo en referencia a los dibujos adjuntos, en los cuales:

- la Fig. 1 muestra una arquitectura de un sistema de monitorización y gestión de acceso según la invención;

- la Fig. 2 muestra una pantalla procesada por el producto informático que implementa el método según la invención, y que representa una situación de monitorización en relación con una entrada;

- la Fig. 3 muestra una pantalla procesada por el producto informático que implementa el método según la invención, y que representa una situación de monitorización en relación con una pluralidad de entradas;

- la Fig. 4 muestra una pantalla procesada por el producto informático que implementa el método según la invención, y que muestra la identidad de las personas que están presentes en el interior de una cierta área monitorizada;

- la Fig. 5 muestra una pantalla procesada por el producto informático que implementa el método según la invención, y que representa la ubicación de una pluralidad de terminales de acceso.

Descripción detallada de ejemplos de formas de realización de la invención

En pocas palabras, la invención propone un sistema de monitorización y gestión de acceso y un método de monitorización correspondiente que asocian un conjunto de terminales de acceso a través de una red de comunicaciones, y que monitorizan, a través de uno o más terminales de monitorización remotos, eventos que se producen en dichos terminales de acceso. Para la monitorización se utiliza un servidor de aplicaciones, el cual se comunica por interfaz, por un lado, con la red de comunicaciones de los terminales de acceso y, por otro lado, con los terminales de monitorización remotos a través de una red de tipo Internet. El servidor de aplicaciones, según un aspecto de la invención, comprende un módulo sinóptico para publicar eventos en los terminales de monitorización remotos, el cual intercambia información con un módulo de gestión de tiempo real, y una base de datos para eventos SCADA (Control de Supervisión y Adquisición de Datos). El módulo de gestión de tiempo real está dedicado a la gestión rápida de las transacciones con los terminales de acceso y la base de datos. El sistema se completa con un módulo de paso que intercambia información con dicho módulo de gestión de tiempo real y dicha base de datos en lo que respecta a la gestión de eventos de datos personales.

La Fig. 1 ilustra un diagrama básico de una arquitectura de un sistema de monitorización y gestión de accesos, designado en su conjunto como 100.

Este sistema 100 comprende un sistema de acceso 400, que comprende una pluralidad de terminales de acceso 401. Dichos terminales de acceso 401 son dispositivos empotrados privativos, de bajo coste, que tienen un tamaño compacto y un diseño particularmente elegante. Los terminales de acceso 401 están equipados también con una pluralidad de interfaces que les permiten conectarse fácilmente tanto a la red de comunicaciones 700 como a dispositivos de identificación auxiliares externos, opcionales.

Los terminales de acceso 401 comprenden entradas 420 relacionadas con señales que provienen principalmente de pasos de comprobación, aunque posiblemente también de sensores de puertas o alarmas tecnológicas de diversos

tipos. Los terminales de acceso 401 comprenden también salidas 430 relacionadas con señales para gestionar el paso y, por otra parte, con señales de alarma y órdenes anti-intrusión. En una versión preferida, los terminales de acceso 401 son terminales Karpos Kompact que recopilan, comprueban y transmiten información referente a la detección de presencia de personal, datos de producción y control de acceso.

El sistema de acceso 400 tiene sus terminales de acceso 401 conectados a una red de comunicaciones 700 a través de un protocolo cifrado multi-plataforma privativo denominado MicronNet.

Un servidor de aplicaciones 200, es decir, un ordenador anfitrión que proporciona servicios de procesado a usuarios o nodos para el acceso remoto, está conectado a dicha red de comunicaciones 700. Dicho servidor de aplicaciones 200 está conectado también a una red intranet 600. De forma más general, dicha red 600 está configurada como una red de tipo Internet, es decir, una red de ordenadores que usa el protocolo TCP/IP.

Una pluralidad de terminales de usuario 500, en particular ordenadores personales equipados con programas de navegación que se ajustan al Protocolo de Internet, o navegadores de Internet, está asociada a la red intranet 600.

Dicho servidor de aplicaciones 200 comprende un módulo de servicios de Internet 210, que, a su vez, incluye un primer módulo de gestión de acceso 230 para permitir la actualización de datos personales, intervalos de tiempo, perfiles en una base de datos 310 a través de los terminales de usuario 500, y un módulo sinóptico 240. El servidor de aplicaciones 200 comprende también un módulo de gestión de tiempo real 220, que está comunicado por interfaz con la red de comunicaciones 700.

El módulo de gestión de acceso 230 envía e intercambia eventos de datos personales hacia/con el módulo de gestión de tiempo real 220 a través de una línea 232, mientras que el módulo sinóptico 240 intercambia eventos SCADA con el mismo módulo de gestión de tiempo real 220 a través de una línea 242. Los módulos del servidor de aplicaciones 200 se implementan preferentemente usando tecnología del tipo Microsoft NET.

El módulo de gestión de acceso 230 se comunica por interfaz en este caso con la red de Internet 600 a través de una conexión 630, que permite que los terminales de usuario 500 lean, modifiquen y fijen datos personales en un servidor de base de datos 300.

Además de gestionar perfiles de acceso de entrada, el módulo de gestión de acceso 230 tiene un recurso de informes de gran alcance de tal manera que permite el análisis de todas las condiciones de tránsito que se hayan producido.

De hecho, el sistema de monitorización y gestión de acceso 100 está equipado también con un servidor de base de datos 300 que contiene la base de datos 310 de los eventos. Dicho servidor de base de datos 300, a través de una serie de conexiones 223, 233, 243, intercambia señales referentes a eventos y valores de configuración, según se detalla posteriormente, con el servidor de aplicaciones 200, respectivamente con el módulo de gestión de acceso 230 a través de una línea 233, con el módulo sinóptico 240 a través de una línea 243, y con el módulo de gestión de tiempo real 220 a través de una línea 223.

El módulo sinóptico 240 permite la obtención de una sinopsis del estado del sistema en relación con eventos que se producen en los terminales de acceso 401, publicándose dicha sinopsis en la red intranet 600 a través de una conexión 640, y permite en particular:

- monitorizar situaciones relacionadas con el sistema (alarmas, estados de puertas, etcétera), según se muestra en la Fig. 2, que ilustra una pantalla procesada por el producto informático que implementa el método según la invención, y que representa la situación de monitorización en un paso de control;

- monitorizar fallos de conexión de los terminales de acceso 401, según se muestra en la Fig. 3, que ilustra una pantalla procesada por el producto informático y que representa la situación de monitorización en una pluralidad de pasos de control;

- monitorizar las personas que están presentes en las áreas de seguridad controladas mediante el uso de la función denominada *"Anti-PassBack"* (función que impide de nuevo acceso sin haber salido previamente), es decir, control y registro tanto de entradas como de salidas que se producen en el área de seguridad, según se muestra en la Fig. 4, que ilustra una pantalla procesada por el producto informático y que representa la identidad de una pluralidad de personas que están presentes dentro de una cierta área monitorizada;

- gestionar la activación/desactivación de tránsito a través de las entradas;

- visualizar en mapas los sitios en los que están ubicados los terminales de acceso 401, según se muestra en la Fig. 5. La herramienta cartográfica tiene su propia navegación y proporciona movimientos de X-Y y funciones de zoom; cuando se visualizan los mapas, los terminales de acceso 401 se pueden representar con diferentes efectos cromáticos dependiendo de si existen o no condiciones de alarma.

Para monitorizar un evento de alarma, indicado con E en la Fig. 1, dicho módulo sinóptico 240 lleva a cabo el siguiente procedimiento:

- el terminal de acceso 401 adquiere, a través de la entrada 420, un evento de alarma E referente a una conexión digital periférica;

- este evento de alarma E se transfiere al módulo de gestión de tiempo real 220 a través de la red de comunicaciones 700;

- el módulo de gestión de tiempo real 220 realiza una etapa de escritura del evento de alarma E en la base de datos 310 a través de la línea 223 y, simultáneamente, encamina, a través de la línea 242, un paquete de UDP (Protocolo de Datagrama de Usuario) referente al evento de alarma E, interceptado automáticamente por el módulo sinóptico 240; dicho protocolo UDP difiere con respecto al protocolo TCP en el que el paquete se puede encaminar a cualquiera perteneciente a una cierta familia de escucha y en que no requiere el envío de una respuesta de confirmación al emisor;

- el módulo sinóptico 240 realiza una operación de parada o consulta, del evento de alarma E en la base de datos 310, recuperando de este modo información vinculada EA y almacenándola en una memoria caché del lado del servidor 245, o memoria temporal, a la espera de su publicación.

Como ejemplo adicional, para monitorizar las personas que están presentes en las áreas de seguridad controladas en cuanto a *"Anti-PassBack"*, dicho módulo sinóptico lleva a cabo el siguiente procedimiento:

- el terminal de acceso 401 adquiere un evento de control horario;

- este evento de control horario se transfiere al módulo de gestión de tiempo real 220 a través de la red de comunicaciones 700;

- el módulo de gestión de tiempo real 220 ejecuta una etapa de escritura del evento de control horario en la base de datos 310 a través de la línea 223 y, simultáneamente, encamina, a través de la línea 242, un paquete de UDP (Protocolo de Datagrama de Usuario) referente al evento de control horario, interceptado automáticamente por el módulo sinóptico 240;

- el módulo sinóptico 240 ejecuta una consulta del evento de entrada de control horario en la base de datos 310, recuperando de este modo toda la información vinculada y almacenándola en una memoria caché del lado del servidor 245, a la espera de su publicación.

De modo similar, dicho módulo sinóptico 240 lleva a cabo el siguiente procedimiento para efectuar la monitorización de fallos de conexión de los terminales de acceso 401:

- el módulo de gestión de tiempo real 220 recibe un evento de conexión/desconexión desde el sistema que controla el protocolo de la red de comunicaciones 700;

- el módulo de gestión de tiempo real 220 ejecuta una etapa de escritura del evento de conexión/desconexión en la base de datos 310 a través de la línea 223 y, simultáneamente, encamina, a través de la línea 242, un paquete de UDP (Protocolo de Datagrama de Usuario) referente al evento de conexión/desconexión interceptado automáticamente por el módulo sinóptico 240;

- el módulo sinóptico 240 ejecuta una consulta del evento de conexión/desconexión en la base de datos 310, recuperando así toda la información vinculada y almacenándola en su memoria caché del lado del servidor 245, a la espera de su publicación.

El sistema de monitorización y gestión de acceso 100 a continuación lleva a cabo el siguiente procedimiento para controlar la activación/desactivación del tránsito en los pasos individuales:

- el módulo sinóptico 240 recibe el evento de activación/desactivación, que se fija a través del navegador de Internet de uno de los terminales de usuario 500;

- a continuación, dicho módulo sinóptico 240 ejecuta una operación de escritura en la base de datos 310 de la información de fijación relacionada, o configuración, del paso, y envía un evento de establecimiento al módulo de gestión de tiempo real 220 a través de la línea 242, que es un *socket* TCP para eventos SCADA;

- el módulo de gestión de tiempo real 220 ejecuta una consulta del evento en la base de datos 310 para recuperar la información de configuración del paso y da salida, hacia el terminal de acceso pertinente 401, a un paquete

adecuado a la red de comunicaciones 700 y que contiene la nueva información de funcionamiento del paso referido;

- el terminal de acceso 401 se ajusta automáticamente a la nueva configuración.

El procedimiento para publicar los eventos en páginas de monitorización en los terminales de usuario 500 se produce de la manera siguiente:

- la memoria caché del lado del servidor 245 del módulo sinóptico 240 es exclusiva para páginas de monitorización del mismo tipo; se hace que este recurso esté disponible simultáneamente para todos los usuarios conectados al módulo sinóptico 240. Esta medida optimiza las prestaciones del sistema cuando se refrescan las páginas de monitorización, ya que la parte de la memoria es unívoca.

- la publicación de la información almacenada en la memoria caché 245 tiene lugar a través del módulo de servicios de Internet 210 en el lado del servidor de aplicaciones 200 y, a través de los navegadores de Internet, en el lado del terminal de usuario 500.

El código de software HTML y Javascript publicado por solicitud del usuario, que se reenvía a través del navegador de Internet en el terminal de usuario 500, está estructurado de tal manera que permite la visualización de las páginas hacia el usuario sin ningún efecto de refresco perturbador, gracias a las siguientes características:

- toda la información sujeta a cambio y visualizada de forma clara consta de variables en el lado del navegador;

- la página visualizada en el terminal de usuario 500 contiene un marco oculto que recibe, a través de un refresco cíclico y automático, la información que ha cambiado en la memoria caché del lado del servidor 245 del módulo sinóptico 240; en dicho marco oculto, se inserta un código de Javascript que es capaz de procesar la información recibida desde la memoria caché del lado del servidor 245; el marco oculto se refresca de manera automática y cíclica;

- en cada evento de refresco, toda la información recibida se actualiza en las variables publicadas de forma clara en la página del usuario.

El módulo de gestión de tiempo real 220 gestiona:

- la conexión desde y hacia los terminales de acceso 400, usando el protocolo, preferentemente el protocolo privativo MicronNet, de la red de comunicaciones 700;

- la conexión desde y hacia las aplicaciones del servidor (módulo 230 y 240) (protocolos TCP/UDP);

- todos los eventos del sistema de monitorización y gestión de acceso 100, actualizando la base de datos 310.

El módulo de gestión de tiempo real 220 también se puede conectar a otros sistemas externos, no mostrados, usando los protocolos TCP/IP y/o UDP.

Para la publicación web, tanto el módulo de gestión de acceso 230 como el módulo sinóptico 240 usan únicamente el código fuente Html y Javascript; por lo tanto, en los terminales 500 no se instala localmente ningún módulo de software que sea externo al navegador, y no se requiere la presencia de la Máquina Virtual de Java. De este modo, los terminales 500 llevan a cabo la actividad de monitorización únicamente usando la configuración del navegador para leer código fuente Html y Javascript.

Los anteriores módulos de software web se pueden considerar como no invasivos con respecto a las configuraciones de software de los terminales de usuario 500; su ejecución no actualiza ningún módulo de software local en los terminales de usuario 500 y no requiere la carga de ningún código Java, ActiveX o enchufable (*plug-in*) de ningún tipo.

El módulo de gestión de acceso 230 puede dar salida a informes en los siguientes formatos normalizados: “PDF” de Adobe, “DOC” de Microsoft Word y “TXT ASCII” con caracteres delimitadores de campo. El módulo de gestión de tiempo real 220 se construye como un servicio de sistema que se activa cuando se pone en marcha el servidor de aplicaciones 200.

El módulo de gestión de tiempo real 220 puede recibir eventos de actualización de datos personales también desde módulos opcionales de importación de datos personales conectados a sistemas externos de gestión de recursos humanos.

El módulo de gestión de tiempo real 220 puede construir archivos ASCII de tipo transferencia para dichos sistemas externos de gestión de recursos humanos.

De forma ventajosa, el sistema antes descrito de monitorización y gestión de acceso usa un servidor de aplicaciones que comprende un módulo de gestión de tiempo real y un módulo sinóptico para publicar, a través de una red del Protocolo de Internet, eventos transmitidos por los terminales de acceso hacia dicho módulo de gestión de tiempo real por medio de una red local. Esto garantiza la rapidez necesaria y permite una señalización oportuna para o una visualización en los terminales de usuario en los que tiene lugar la monitorización.

Según otro aspecto ventajoso del sistema de acuerdo con la invención, el uso de un servidor de aplicaciones que es compatible con redes de Internet/Intranet permite usar, como terminales de usuario, ordenadores comerciales equipados con un navegador de Internet. Este equipo de hardware y software de bajo coste está fácilmente disponible en el mercado y, dada la generalización de las interfaces de navegador, el personal habitualmente no necesita que se le entrene en particular para usar los programas. En el lado del usuario, el sistema según la invención aparece como una aplicación que es completamente del tipo Malla Multimedia Mundial.

También de forma ventajosa, se usan procedimientos de presentación visual y refresco que están adaptados para obtener una rapidez particular de visualización y refresco. En este marco, la introducción de un módulo sinóptico con una única memoria caché permite lograr un rendimiento de refresco óptimo para todos los terminales de usuario conectados a dicho módulo sinóptico.

Por lo tanto, sin perjuicio de los principios de la invención, los detalles y las formas de las realizaciones pueden variar incluso significativamente en comparación con los descritos e ilustrados en la presente memoria a título de ejemplo no limitativo, sin apartarse, por ello, del alcance de la invención, según se define en las siguientes reivindicaciones.

REIVINDICACIONES

1. Sistema de monitorización y gestión de acceso, que comprende por lo menos un conjunto de terminales de acceso (400) asociados a una primera red de comunicaciones (700), y un servidor de aplicaciones (200) que también está asociado a dicha primera red de comunicaciones (700) para intercambiar información, comprendiendo dicho servidor de aplicaciones (200):

- un módulo de gestión de tiempo real (220) configurado para intercambiar información de eventos (E) con dicho conjunto de terminales de acceso (400) a través de dicha primera red de comunicaciones (700);

- un módulo sinóptico (240) configurado para recibir (242) dicha información de eventos (E) desde dicho módulo de gestión de tiempo real (220) y para publicar (640) dicha información de eventos (E) por lo menos en un terminal de usuario de monitorización (500) a través de una red de tipo Internet (600),

caracterizado porque dicho módulo sinóptico (240) comprende una memoria temporal (245) para almacenar temporalmente la información de eventos, siendo accesible la memoria temporal (245) por dicho por lo menos un terminal de usuario de monitorización (500) para la publicación y siendo exclusiva para páginas de monitorización de un mismo tipo, enviando dicho módulo sinóptico (240) un código de publicación a petición de dicho por lo menos un terminal de usuario (500), implementando dicho código de publicación las siguientes operaciones:

- asignar toda la información sujeta a cambio y visualizada de forma clara, a variables asociadas a un navegador de dicho por lo menos un terminal de usuario de monitorización (500);

- proporcionar, en una página visualizada en dicho por lo menos un terminal de usuario de monitorización (500), un marco oculto que recibe, a través de un refresco cíclico y automático, la información que ha cambiado en la memoria temporal (245), comprendiendo dicho marco oculto unas partes de código adaptadas para procesar la información recibida desde la memoria temporal (245) y para refrescar dicho marco oculto de manera automática y cíclica;

- actualizar, en cada evento de refresco, toda la información recibida en dichas variables asociadas a dicho navegador de dicho por lo menos un terminal de usuario de monitorización (500) y publicada de forma clara.

2. Sistema según la reivindicación 1, caracterizado porque dicho código de publicación comprende solamente código HTML o Javascript, y porque dicho código se interpreta para la publicación por parte de dicho navegador de dicho por lo menos un terminal de usuario (500).

3. Sistema según la reivindicación 1 ó 2, caracterizado porque dicho sistema de gestión de eventos (200) está asociado (223, 233, 243) a un sistema de base de datos (300) y porque dicho módulo sinóptico (240) está configurado para acceder a una base de datos de eventos (310) en dicho sistema de base de datos (300), para escribir dicha información de eventos (E) recibida desde el módulo de gestión de tiempo real (220) en la base de datos de eventos (310) y para recuperar información (EA) vinculada a dicha información de eventos (E) para su publicación en dicho por lo menos un terminal de usuario de monitorización (500).

4. Sistema según la reivindicación 3, caracterizado porque dicho sistema de gestión comprende también un módulo de gestión de acceso (230) configurado para intercambiar (630, 232, 233) información de datos personales con dicho por lo menos un terminal de usuario de monitorización (500), dicho módulo de gestión de tiempo real (220) y dicho sistema de base de datos (300).

5. Sistema según una o más de las reivindicaciones 1 a 4, caracterizado porque dicha información de eventos (E) intercambiada entre dicho módulo sinóptico (240) y dicho módulo de gestión de tiempo real (230) es del tipo SCADA (Control de Supervisión y Adquisición de Datos).

6. Sistema según una o más de las reivindicaciones 1 a 5, caracterizado porque dicho módulo sinóptico (240) está configurado para llevar a cabo una o más de las siguientes operaciones:

- monitorizar situaciones relacionadas con el sistema;

- monitorizar fallos de conexión de los terminales de acceso (401);

- monitorizar las personas que están presentes en áreas de seguridad controladas mediante el uso de la funcionalidad *Anti-PassBack;*

- gestionar la activación/desactivación del tránsito a través de entradas controladas por dichos terminales de acceso (401).

7. Sistema según una o más de las reivindicaciones 1 a 6, caracterizado porque dicho módulo de gestión de tiempo real (220) está configurado para gestionar:

- una conexión bidireccional con dichos terminales de acceso (400) usando el protocolo de dicha primera red de comunicaciones (700);

- una conexión (232) con dicho módulo de gestión de acceso (230) según un protocolo TCP;

- una conexión (242) con dicho módulo sinóptico según protocolos TCP/UDP;

- eventos de dicho sistema de monitorización y gestión de acceso (100) a través de operaciones para actualizar dicha base de datos (310).

8. Sistema según una o más reivindicaciones anteriores, caracterizado porque dicho módulo de gestión de tiempo real (220) está conectado por lo menos a un sistema externo de gestión de recursos humanos para transferir eventos de actualización de datos personales.

9. Método para monitorización y gestión de accesos en un sistema que comprende por lo menos un conjunto de terminales de acceso (400) y por lo menos un terminal de usuario de monitorización (500), según el cual se transmite información de eventos (E) referente a eventos que se producen en dichos terminales de acceso (500), a través de una primera red de comunicaciones (700) asociada a dicho por lo menos un conjunto de terminales de acceso (400) y a través de un servidor de aplicaciones (200) asociado a dicha primera red de comunicaciones (700) y a dicho por lo menos un terminal de usuario de monitorización (500), en el que dicho servidor de aplicaciones (200) implementa:

- un procedimiento de gestión de tiempo real (220) según el cual se intercambia información de eventos (E) con dicho conjunto de terminales de acceso (400) a través de dicha primera red de comunicaciones (700);

- un procedimiento sinóptico (240) para recibir (242) dicha información de eventos (E) desde dicho procedimiento de gestión de tiempo real (220) y para publicar (640) dicha información de eventos (E) en dicho por lo menos un terminal de usuario de monitorización (500) a través de una red de protocolo de tipo Internet (600), caracterizado porque dicho procedimiento sinóptico (240) comprende una memoria temporal (245) para almacenar temporalmente la información de eventos, siendo accesible la memoria temporal (245) por dicho por lo menos un terminal de usuario de monitorización (500) para la publicación y siendo exclusiva para páginas de monitorización de un mismo tipo, enviando dicho módulo sinóptico (240) un código de publicación por solicitud de dicho por lo menos un terminal de usuario de monitorización (500), implementando dicho código de publicación las siguientes operaciones:

- asignar toda la información sujeta a cambio y visualizada de forma clara, a variables asociadas a un navegador de dicho por lo menos un terminal de usuario de monitorización (500);

- proporcionar, en una página visualizada en dicho por lo menos un terminal de usuario de monitorización (500), un marco oculto que recibe, a través de un refresco cíclico y automático, la información que ha cambiado en la memoria temporal (245), comprendiendo dicho marco oculto partes de código adaptadas para procesar la información recibida desde la memoria temporal (245) y para refrescar dicho marco oculto de manera automática y cíclica;

- actualizar, en cada evento de refresco, toda la información recibida en dichas variables asociadas a dicho navegador de dicho por lo menos un terminal de usuario de monitorización (500) y publicada de forma clara.

10. Método según la reivindicación 9, caracterizado porque dicho código de publicación comprende solamente código HTML o Javascript, y porque dicho código se interpreta para la publicación por parte de dicho navegador de dicho por lo menos un terminal de usuario de monitorización (500).

11. Método según la reivindicación 9 ó 10, caracterizado porque comprende una operación para asociar una base de datos (300) a dicho servidor de aplicaciones (200) y porque dicho procedimiento sinóptico (240) tiene acceso a dicha base de datos de eventos (310) en dicha base de datos (300), escribe dicha información de eventos (E) recibida desde el procedimiento de gestión de tiempo real (220) en dicha base de datos de eventos (310), y recupera información (EA) vinculada a dicha información de eventos (E) para su publicación en dicho por lo menos un terminal de usuario de monitorización (500).

12. Método según la reivindicación 11, caracterizado porque dicho servidor de aplicaciones (200) implementa también un procedimiento de gestión de acceso (230) para intercambiar (630, 232, 233) información de datos personales con dicho por lo menos un terminal de usuario de monitorización (500), dicho procedimiento de gestión de tiempo real (220) y dicha base de datos (300).

13. Método según una o más de las reivindicaciones 9 a 12, caracterizado porque dicho módulo de gestión de acceso (230) es capaz de generar archivos de informes, constituidos particularmente en los formatos “DOC”, “PDF” y “TXT ASCII”, referentes a dicha información de eventos (E).

14. Método según una o más de las reivindicaciones 9 a 13, caracterizado porque dicha información de eventos (E) intercambiada entre dichos procedimiento sinóptico (240) y procedimiento de gestión de tiempo real (220) es del tipo SCADA.

15. Método según una o más de las reivindicaciones 9 a 14, caracterizado porque dicho procedimiento sinóptico (240) comprende una o más de las siguientes operaciones:

- monitorizar situaciones relacionadas con el sistema;

- monitorizar fallos de conexión de los terminales de acceso (401);

- monitorizar las personas que están presentes en áreas de seguridad controladas mediante el uso de la funcionalidad *Anti-PassBack*;

- gestionar la activación/desactivación del tránsito a través de entradas controladas por dichos terminales de acceso (400).

16. Método según una o más de las reivindicaciones 9 a 15, caracterizado porque dichas situaciones relacionadas con el sistema y dichos terminales de acceso (401) se visualizan en una pantalla y se representan con diferentes efectos cromáticos dependiendo de si existen o no condiciones de alarma.

17. Método según una o más de las reivindicaciones 9 a 16, caracterizado porque dicho procedimiento de gestión de tiempo real (220) gestiona:

- una conexión bidireccional con dichos terminales de acceso (400) usando el protocolo de dicha primera red de comunicaciones (700);

- una conexión (232) con dicho procedimiento de gestión de acceso (230) según el protocolo TCP;

- una conexión (242) con dicho procedimiento sinóptico (240) según los protocolos TCP/UDP;

- eventos de dicho sistema de monitorización y gestión de acceso (100) a través de operaciones de actualización de dicha base de datos (310).

18. Método según una de las reivindicaciones 9 a 17, caracterizado porque monitoriza dichos eventos por medio de las siguientes operaciones:

- adquirir un evento de alarma y/o de control horario y/o de conexión/desconexión en el terminal de acceso (401) a través de una entrada (420) relacionada con una conexión digital periférica;

- transferir dicho evento de alarma y/o de control horario y/o de conexión/desconexión hacia dicho procedimiento de gestión de tiempo real (220) a través de dicha primera red de comunicaciones (700);

- por medio de dicho procedimiento de gestión de tiempo real (220), escribir el evento de alarma y/o de control horario y/o de conexión/desconexión en la base de datos (310) y, al mismo tiempo, encaminar, a través de la conexión (242) hacia dicho procedimiento sinóptico (240), un paquete UDP (Protocolo de Datagrama de Usuario) relacionado con el evento de alarma y/o de control horario y/o de conexión/desconexión interceptado automáticamente por el procedimiento sinóptico (240);

- dicho procedimiento sinóptico (240) comprende también operaciones para consultar el evento de alarma y/o de control horario y/o de conexión/desconexión en la base de datos (310), recuperar dicha información vinculada (EA), y almacenar (245) dicha información vinculada (AE) temporalmente a la espera de una operación de publicación a través de la red de Internet (600).

19. Método según la reivindicación 15, caracterizado porque dicha operación para gestionar la activación/desactivación de tránsito a través de entradas controladas por dichos terminales de acceso (401) comprende a su vez las siguientes operaciones:

- enviar al procedimiento sinóptico (240) un evento de activación/desactivación fijado a través de dicho por lo menos un terminal de usuario de monitorización (500);

- por medio de dicho procedimiento sinóptico (240), escribir en la base de datos (310) información de configuración relacionada del terminal de acceso (401) y enviar un evento de configuración al procedimiento de gestión de tiempo real (220);

- consultar el evento en la base de datos (310) en el procedimiento de gestión de tiempo real (220) para recuperar dicha información de configuración y para dar salida hacia el terminal de acceso (401) a un paquete apto para la red de comunicaciones (700) y que contiene información de funcionamiento para el terminal.

20. Producto informático que se puede cargar en la memoria de por lo menos un ordenador y que comprende partes de código de software para ejecutar el método según cualquiera de las reivindicaciones 9 a 19.

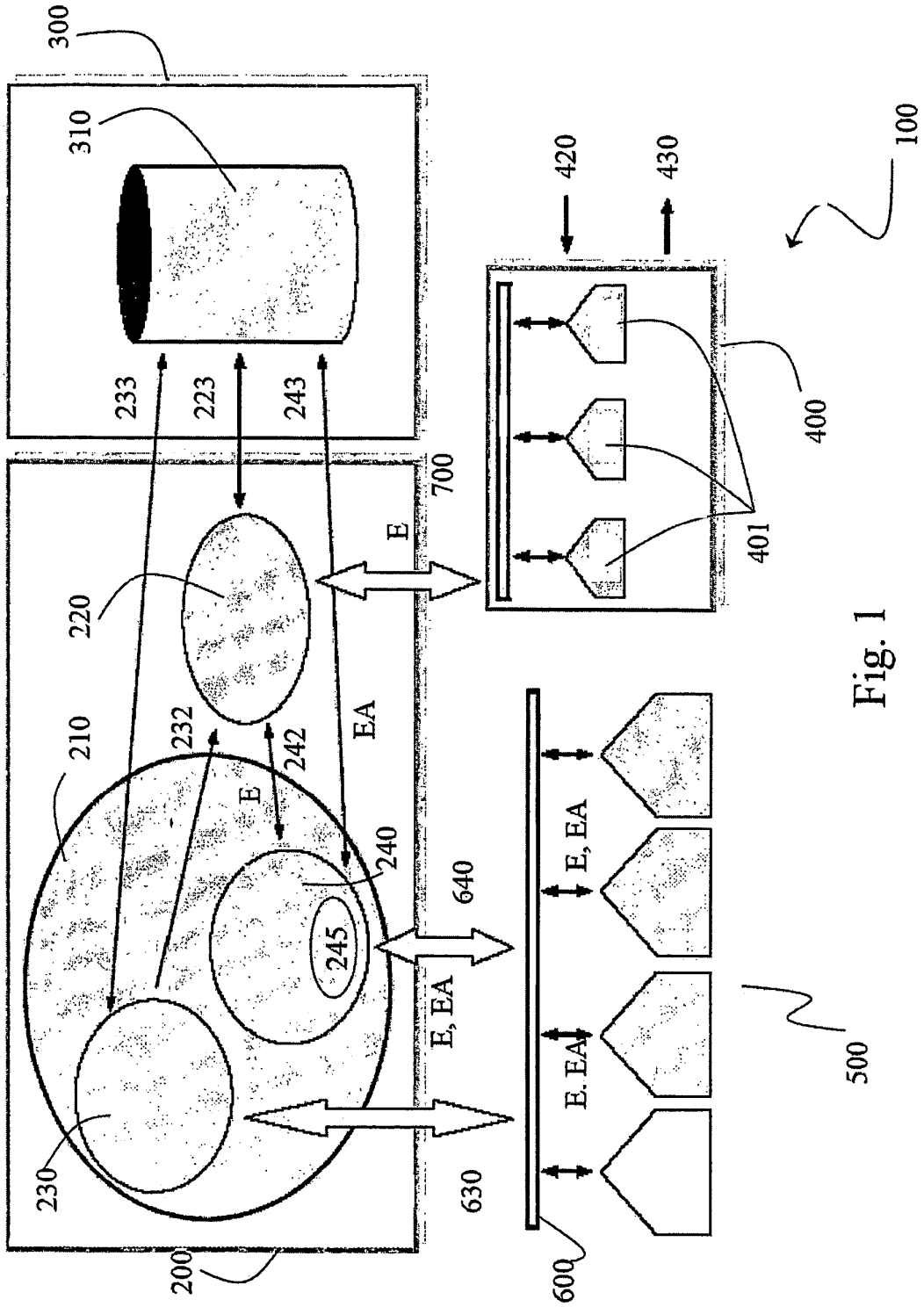
300
310
233
223
243
700
E
220
210
232
242
EA
E
240
245
640
E, EA
230
630
E, EA
E, EA
600
200
420
430
100
400
401
500

Fig. 1

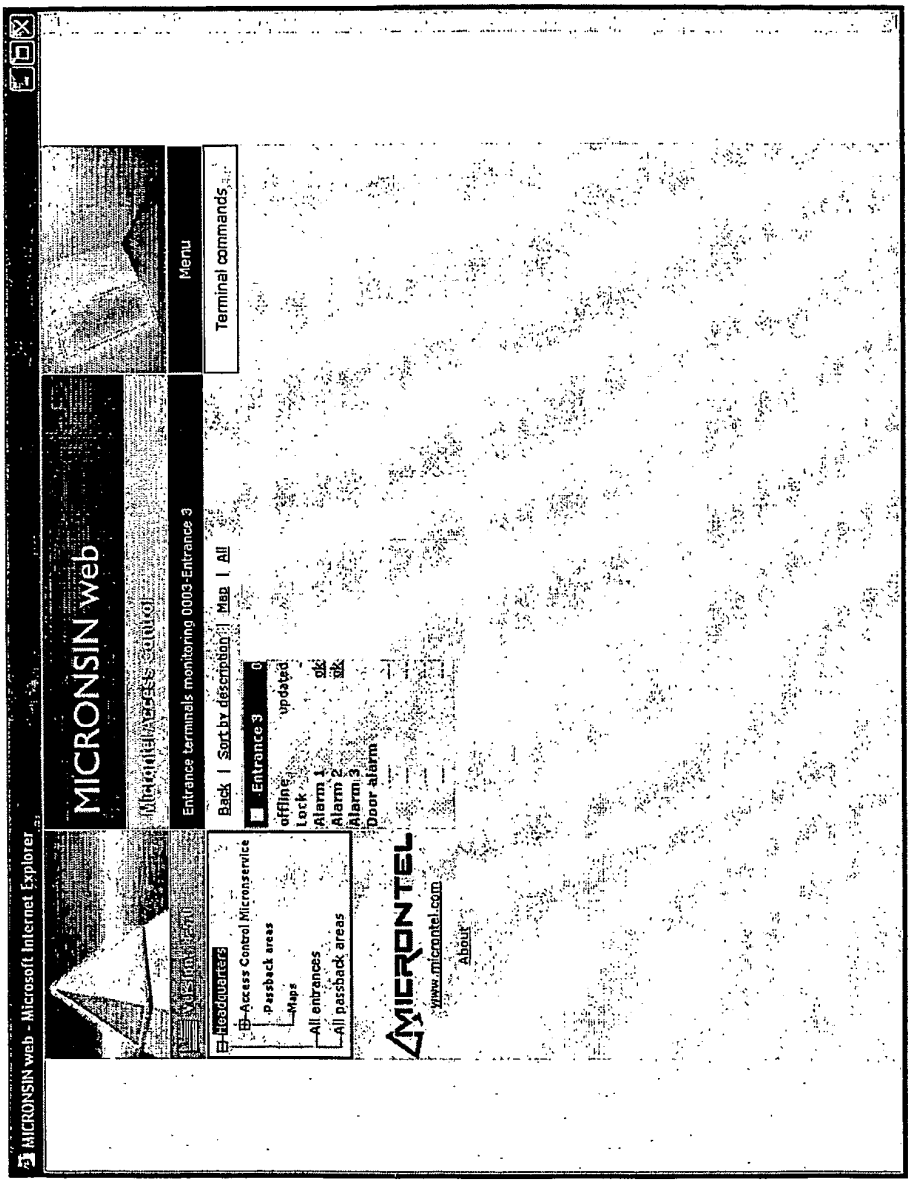
MICRONSIN - Microsoft Internet Explorer
MICRONSIN web
Menu
Terminal commands
Entrance terminals monitoring 0003-Entrance 3
Back | Sort by description | Map | All
Entrance 3
offline
updated
Lock
Alarm 1
Alarm 2
Alarm 3
Door alarm
Headquarters
Access Control Microneservice
Passback areas
Maps
All entrances
All passback areas
MICRONTEL
www.microntel.com
About

Fig. 2

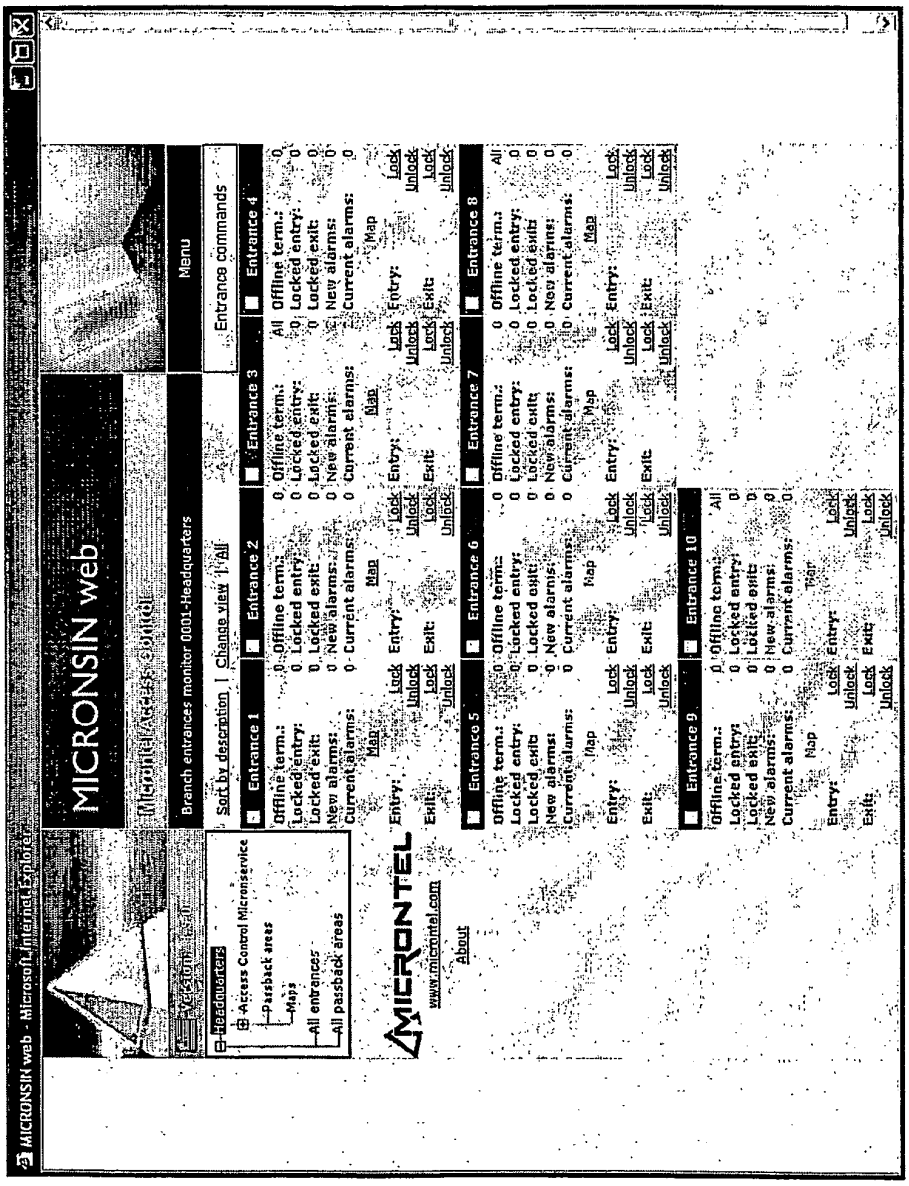
MICRONSIN web - Microsoft Internet Explorer
MICRONSIN web
Micronsin Access Control
Menu
Branch entrances monitor 0001-Headquarters
Sort by description | Change view | All
Entrance commands
Headquarters
Access Control Microniservice
Passback areas
Maps
All entrances
All passback areas
Entrance 1
Entrance 2
Entrance 3
Entrance 4
Entrance 5
Entrance 6
Entrance 7
Entrance 8
Entrance 9
Entrance 10
Offline term.:
Locked entry:
Locked exit:
New alarms:
Current alarms:
Map
Entry:
Exit:
Lock
Unlock
MICRONTEL
www.microntel.com
About

Fig. 3

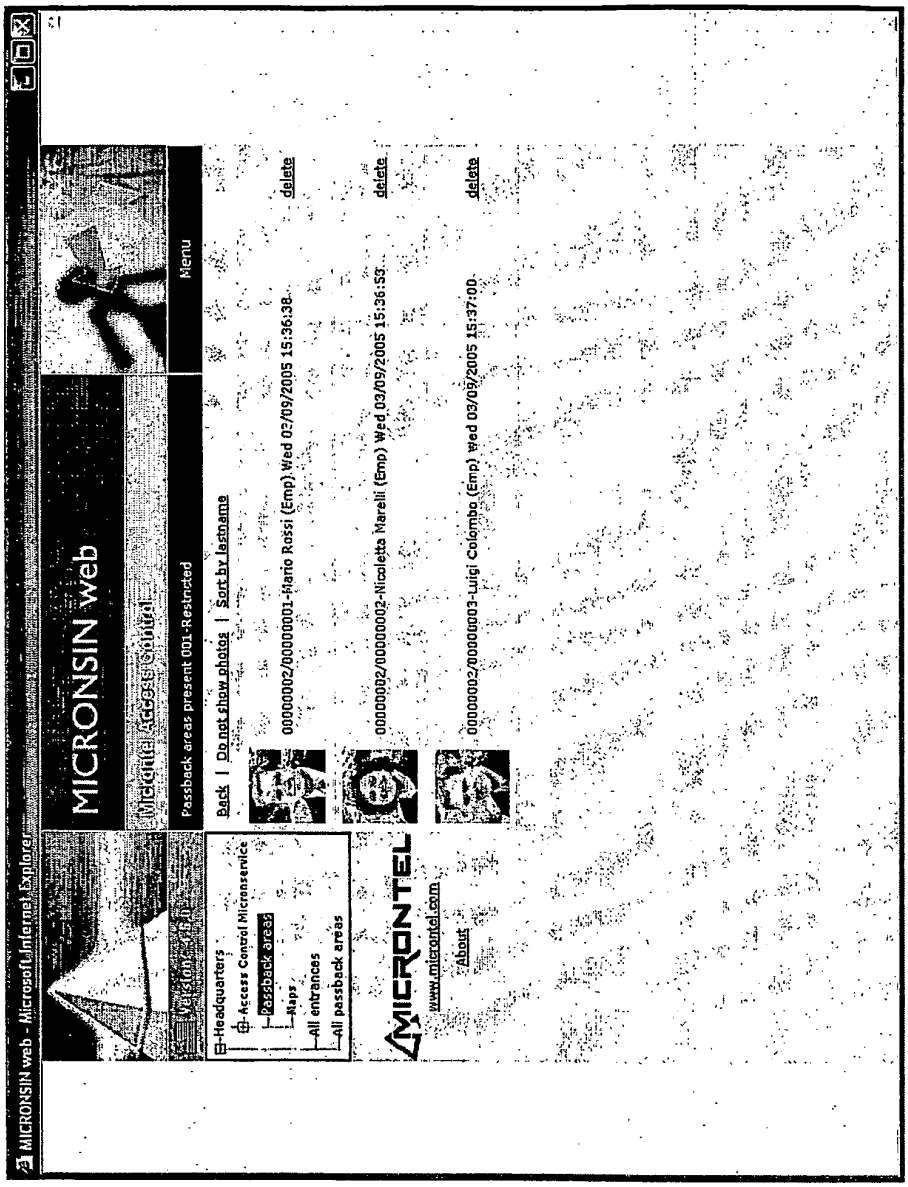
MICRONSIN web - Microsoft Internet Explorer
MICRONSIN web
Menu
Passback areas present 001-Restricted
Back | Do not show photos | Sort by lastname
Headquarters
Access Control Micronservice
Passback areas
Maps
All entrances
All passback areas
00000002/00000001-Mario Rossi (Emp) Wed 02/09/2005 15:36:38
delete
00000002/00000002-Nicoletta Marelli (Emp) Wed 03/09/2005 15:36:53
delete
00000002/00000003-Luigi Colombo (Emp) Wed 03/09/2005 15:37:00
delete
MICRONTEL
www.micronlel.com
About

Fig. 4

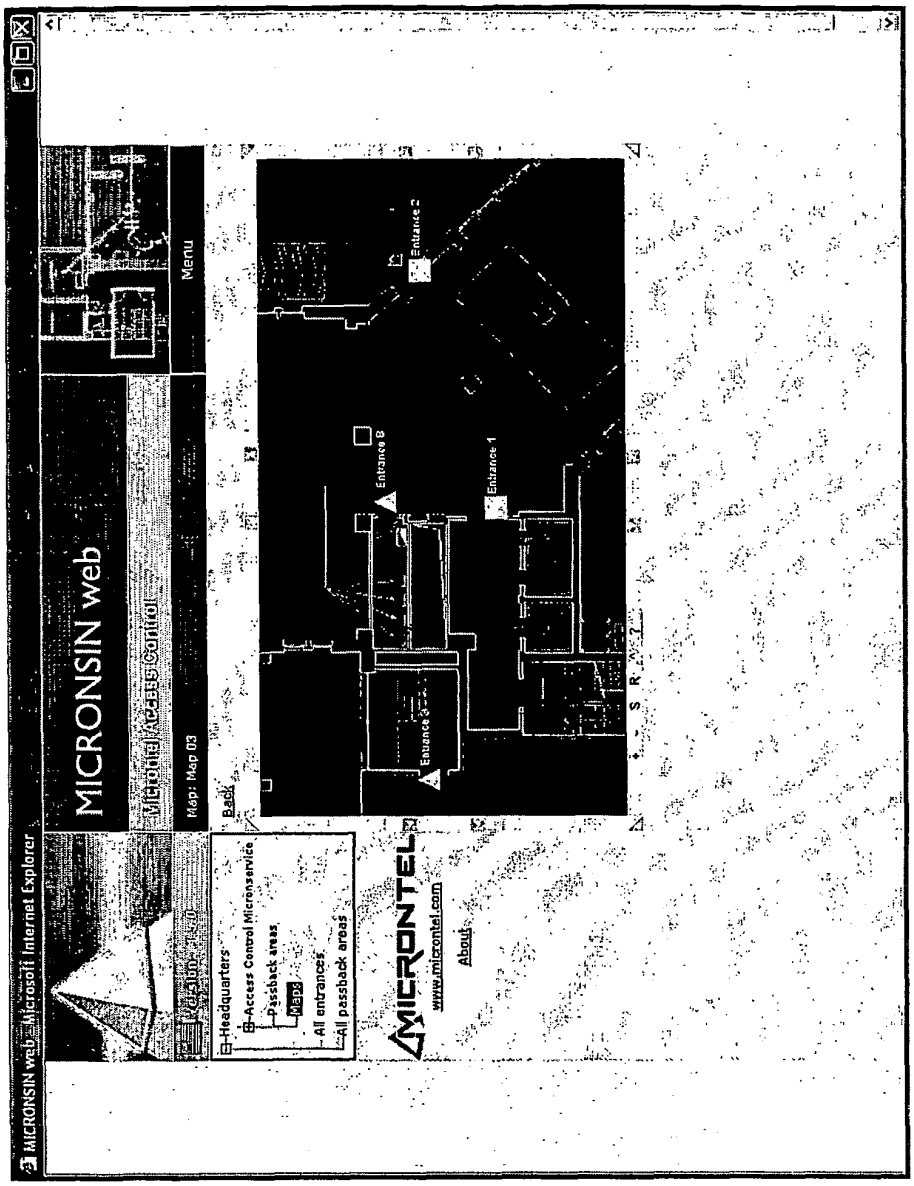
MICRONSIN web - Microsoft Internet Explorer
MICRONSIN web
Menu
Map: Map 03
Back
Headquarters
Access Control Microservice
Passback areas
Maps
All entrances
All passback areas
MICRONTEL
www.microntel.com
About
Entrance 2
Entrance 3
Entrance 1
S
R
A
T

Fig. 5