

**UNIVERSIDAD DEL CEMA
Buenos Aires
Argentina**

Serie
DOCUMENTOS DE TRABAJO

Área: Ingeniería Informática

SISTEMAS VMS Y PSIM

Gastón A. Addati

**Julio 2014
Nro. 539**

**www.cema.edu.ar/publicaciones/doc_trabajo.html
UCEMA: Av. Córdoba 374, C1054AAP Buenos Aires, Argentina
ISSN 1668-4575 (impreso), ISSN 1668-4583 (en línea)
Editor: Jorge M. Streb; asistente editorial: Valeria Dowding <jae@cema.edu.ar>**

Sistemas VMS y PSIM

Gastón A. Addati

“Las opiniones y/o comentarios que pudieran generarse en este trabajo, son de exclusiva responsabilidad de su autor, y no necesariamente expresan la posición de la Universidad del CEMA”

ABSTRACT

Las Organizaciones que requieren disponer de sistemas de control y seguridad basado en video cámaras, demandan día a día mayores funcionalidades soportadas sobre todo con las nuevas tecnologías y desarrollos de software. La Informática y la Electrónica aportan muchos de los nuevos beneficios que día a día se ven reflejados como nuevos desafíos a superar entre las diferentes compañías que desarrollan e investigan nuevos productos basadas en innovadoras funcionalidades.

Se sabe que si una persona mira de manera fija un pantalla durante varios minutos, escenas o puntos importantes no son percibidos y tal como se vió en documentos de trabajo anteriores, los sistemas VMS (Video Management Systems) han logrado optimizar muchos de estos procesos, automatizando actividades que antes dependían de un operador. Algunos ejemplos de automatización de estos procesos, son los que se enmarcan dentro de las “Analíticas de Video” que incluso varios fabricantes ya integran dentro de los procesadores y del software de las cámaras IP que producen.

Surge entonces, una nueva necesidad: ¿Cómo se integran otros sistemas existentes en una organización (sistemas eléctricos, electrónicos, mecánicos, de rayos laser, infrarrojos, etc..)? ¿Cómo puede gestionarse de manera centralizada e integral todos estos dispositivos, incluyendo a las cámaras IP?. ¿Cómo se pueden gestionar y automatizar eventos para ciertos procesos predefinidos y basados en estos sistemas

integrales de la organización?. La respuesta a todos estos interrogantes y más, la tienen los Sistemas PSIM. **“Physical Security Information Management”**.

INDICE

ABSTRACT	1
INDICE	2
¿Qué son los Sistemas VMS: Video Management Systems?	3
¿Cómo es la interfaz gráfica de un Sistema VMS?	5
¿Qué es un Sistema PSIM – “Physical Security Information Management”?	8
¿Qué beneficios puede aportar PSIM a la organización?	11
¿Cómo se integra un sistema PSIM en la Organización?	12
Conclusiones Finales.....	14
Bibliografía Consultada	16

¿Qué son los Sistemas VMS: Video Management Systems?

Son sistemas de información que tienen la particularidad de correr en cualquier tipo de hardware, integrar una gran cantidad de dispositivos IP's o dispositivos analógicos, y gestionar los flujos de video y los eventos que ingresan al sistema, para poder hacer con ellos, las acciones que un administrador u operador dispongan.

Un VMS es un software que permite, entre otras cosas, disponer de una plataforma abierta (es decir, que no se encuentra ligada estrechamente a ningún fabricante de hardware, tal como ocurre con los DVRs).¹

Como software abierto, es posible utilizarlos para visualizar las imágenes en tiempo real de cualquier tipo de dispositivo (y no necesariamente de un solo fabricante), para visualizar las grabaciones (el historial de grabaciones), para acceder las imágenes en tiempo real o desde archivo a través de internet, pero sobre todo, están pensados para hacer mucho más fácil el trabajo de los operadores, permitiendo configurar y parametrizar ciertas automatizaciones, como pueden ser alarmas, mapas, interacción con relés o bien integrarse con otros sistemas ya existentes de una organización.

Y por supuesto, lo que caracteriza a estos sistemas VMS es la posibilidad de utilizar las Analíticas de Video para optimizar el uso del sistema.

Existen en el mercado una gran cantidad de marcas y/o fabricantes de software que se dedican exclusivamente a este tipo de sistemas. Entre ellos, y los más importantes a nivel mundial son:

- AxxonSoft
- Milestone
- ISS
- Lenel
- iPronet

¹ Para más información respecto de lo que son los Sistemas DVR y sus características, puede consultar el documento de trabajo Nro 529 "Analíticas de Video IP" en el siguiente Link:
<http://ideas.repec.org/p/cem/doctra/529.html>

A continuación, mencionaremos algunas ventajas en la utilización de sistemas VMS:

- **Más flexibilidad en la escalabilidad del hardware:** Normalmente los NVR y DVR's sólo ofrecen unas pocas posibilidades de configuraciones y, a menudo tienen restricciones en la forma en que se pueden ampliar estos sistemas. Por el contrario, mediante el uso VMS se pueden cambiar o agregar componentes o hardware integrando diferentes fabricantes y marcas.
- **Los VMS no están “atados” al hardware:** Por lo general, cuando se usan los NVRs o DVRs, existen serios problemas si se desea actualizar o reemplazar el hardware. En caso de tener mayor demanda de video cámaras, Siempre se termina en la misma solución; adquiriendo cámaras y nuevos NVRs o DVRs, lo que incrementa sustancialmente los costos, el lugar físico del centro de cómputos, la energía, los riesgos de falla, etc.. Cuando se tiene en cuenta el crecimiento a futuro de los sistemas VMS y se invierte inicialmente en el hardware necesario es mucho más económico y sencillo el tratamiento de la escalabilidad (o el crecimiento) ya que solo sería necesario invertir en las licencias adicionales de software que se requieran y eventualmente, como es lógico en nuevas cámaras IP, que no necesariamente tendrían que ser de una única marca o modelo (la importancia de disponer de una plataforma abierta).
- **Menor costo del hardware:** Es posible adquirir licencias de software VMS y un hardware equivalente al de un NVR por un precio más bajo que comprar el NVR. Esta no es una regla universal y dependerá desde luego, de las características del sistema y de la marca y/o del producto que se esté evaluando.
- **Mejores características:** Por lo general, los sistemas VMS cuentan con funciones más avanzadas que los NVRs, como video análisis específicos, balanceo de cargas, auto backup, integración con terceros, Funcionalidades adicionales, como Detección de rostros, patentes de vehículos, entre otros.

Extraído de: <http://www.tecnoseguro.com/analisis/cctv/sistemas-de-grabacion-de-cctv-ip-cual-es-el-mejor-nvr-o-vms.html> con algunas modificaciones del autor.

¿Cómo es la interfaz gráfica de un Sistema VMS?

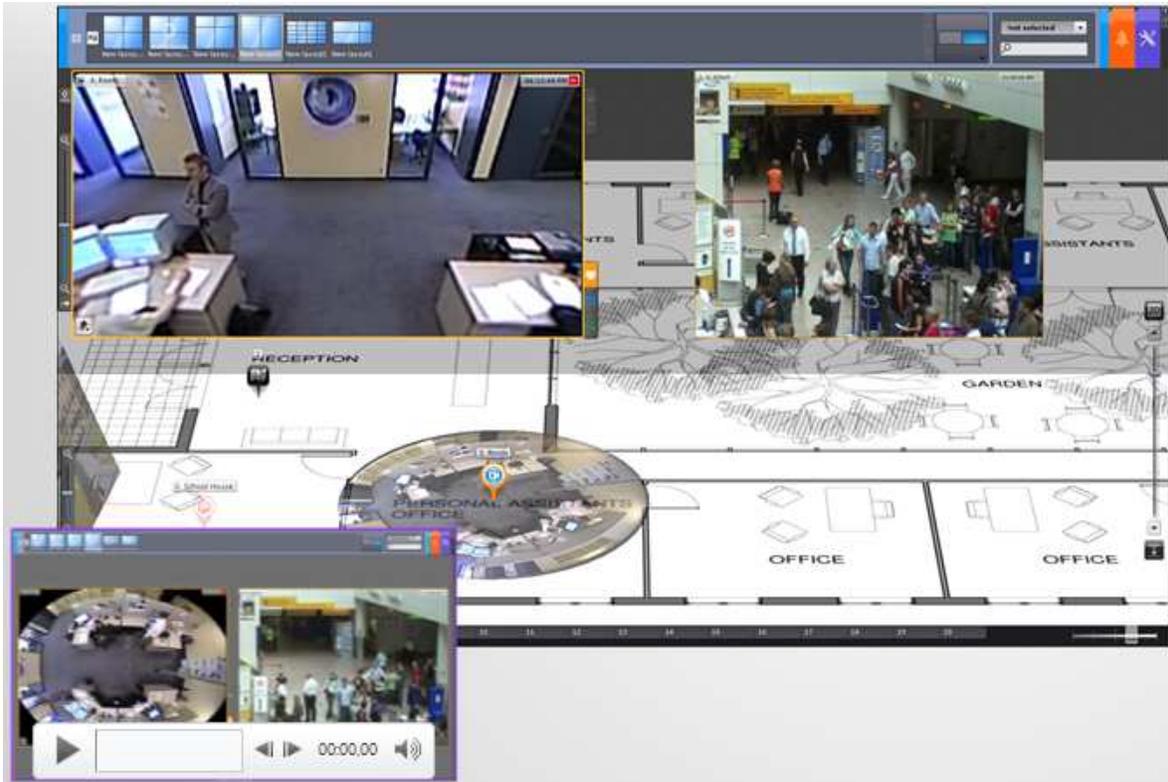


Imagen extraída del sitio oficial de AxxonSoft:

http://www.axxonsoft.com/sp/products/axxon_next/interface

Son en general, muy prácticas, intuitivas, y flexibles, ya que permiten entre otras cosas acomodar la pantalla según las necesidades o gusto personal de cada operador. Admite diferentes formatos y distribución de cámaras en pantalla.

Permiten fácilmente localizar cámaras, sectores y alarmas en tiempo real, mediante la implementación de mapas en 3D, lo que facilita y agiliza las acciones del personal, ante eventos programados y no programados.



Pantalla del software AxonNext 3.5, donde puede visualizarse un mapa de la organización, y navegarlo en modo inmersión²

Si la organización tuviera sitios dispersos y estos estuvieran siendo monitoreados con un sistema VMS, podrían integrarse con Google Maps, para una mejor localización de las cámaras sobre un mapa:

² El modo Inmersión, se refiere a la funcionalidad específica que incluyen las cámaras del tipo “Ojo de Pez” o “FishEye”, la cual dispone de una visión de 360°.



*Ejemplo de Integración de software VMS con Google Maps. * extraído del sitio oficial de AxxonSoft.*

Como puede observarse, los sistemas VMS (Video Management Systems) son potentes desarrollos de software, que poseen gran escalabilidad, y funcionalidad avanzada, fácil interacción con el usuario que opera el sistema, y sobre todo, gestionan eventos que provienen de dispositivos IP's o analógicos que se encuentran integrados al sistema. Los Sistemas VMS gestionan los eventos, y los utilizan para realizar acciones específicas con ellos. Esas acciones específicas abarcan desde enviar un simple email, hasta capturar fotos y activar o desactivar relés.

La fortaleza de los sistemas VMS de última generación, son la aplicación de analíticas de video, que están orientadas a resolver y mejorar procesos específicos del negocio o de la seguridad, y que sin la ayuda del software, sería muy costoso y laborioso de encontrar, e incluso de visualizar.

¿Qué es un Sistema PSIM – “Physical Security Information Management”?

En el abstract quedaron planteadas algunas preguntas: ¿Cómo se integran otros sistemas existentes en una organización (sistemas eléctricos, electrónicos, mecánicos, de rayos laser, infrarrojos, etc..? ¿Cómo puede gestionarse de manera centralizada e integral todos estos dispositivos, incluyendo a las cámaras IP?. ¿Cómo se Pueden gestionar y automatizar eventos para ciertos procesos predefinidos y basados en estos sistemas integrales de la organización?, Y afirmamos que la respuesta a todos estos interrogantes la tienen los Sistemas PSIM. **“Physical Security Information Management”**.

Los Sistemas PSIM, son sistemas basados en software informático que se utiliza para implementar tecnologías o plataformas abiertas de hardware y software, con el objetivo de centralizar, consolidar, y automatizar la gestión integral de eventos relacionados con la seguridad física de una organización.

Surgen entonces nuevos interrogantes. ¿Cuáles serían los eventos o dispositivos que forman parte de la seguridad física de una organización?.

No existe una definición formal, pero podemos realizar una aproximación.

Algunos de los elementos o sistemas que forman parte de la seguridad física de las organizaciones son:

- Sistemas anti incendios.
- Sistemas de extinción de incendios.
- Sistemas de cercos perimetrales (en todas sus combinaciones: Barreras infrarrojas, cable microfónico, etc.)
- Sistemas de control de acceso, en cualquier variante (por biometría, RFID, etc)
- Sistemas de control de temperatura y humedad
- Sistemas de protección eléctrica
- Entre otros, también el CCTV

Por lo general cada uno de estos sub-sistemas, dentro de una organización funciona de forma aislada. Cada fabricante desarrolla sus propios productos, que pueden ser utilizados por su propio software, lo que hace que se requiera de una infraestructura

tecnológica para cada uno de estos sistemas (servidores, Almacenamiento, Impresoras, Racks, cableados específicos, etc.).

Seguramente la pregunta que se hará el lector en este punto es: ¿Cómo hace entonces una organización para gestionar de manera correcta cada uno de estos sistemas, si todos ellos funcionan en forma aislada, y más aún, si cada uno de ellos necesita especialistas (recursos humanos técnicamente capacitados y hasta certificados) para ser operados?.

Esa respuesta, hasta hace algunos años no tenía una solución válida. Es decir, cada empresa, debía manejar (e incluso al día de hoy muchas lo siguen haciendo) en forma independiente a cada uno de estos sistemas de seguridad física. Especialistas en las distintas áreas, o bien contratos de alto valor económico eran y son necesarios para una correcta gestión de incidentes o eventos que cada sistema puede emitir y para un efectivo mantenimiento y accionar de cada uno de ellos.

Sistemas que funcionan en forma descentralizada, sin interconexión entre otros sistemas, y muchas veces sin un efectivo mantenimiento preventivo, complican a los gerentes responsables de las áreas de seguridad física y patrimonial, ya que la información de cada sistema para la toma de decisiones, no es fácil de obtener y centralizar.

El advenimiento de los sistemas PSIM ha resuelto de manera integral todos estos problemas, y ha logrado consolidar la información en una única plataforma de gestión desde donde los operadores, ahora pueden tener acceso en tiempo real, a las cámaras de CCTV, a los sensores infrarrojos, a los sensores de los cercos perimetrales, entre otras opciones. Es más, la automatización de eventos puede llegar al punto de programar al sistema, por ejemplo, que ante la activación del cerco perimetral, en un punto específico de la cerca, una cámara, tipo domo PTZ, pueda dirigirse automáticamente a la zona en alerta, para que el operador visualice en tiempo real lo que sucede.

La posibilidad de activar o desactivar un relé mediante un click, de tener información centralizada en la pantalla sobre la temperatura y humedad del cuarto de máquinas, de activar o desactivar una barrera infrarroja o bien de encender una luz exterior, con los sistemas PSIM es una tarea muy simple de hacer, y además, permite registrar cada una de la acciones realizadas por los operadores, brindando una especie de “bitácora” o “log de auditoría”, con cada uno de los eventos y acciones que se realizaron sobre el sistema.

Un sistema PSIM completo debe proporcionar 5 facilidades clave:³

1. **Recolección:** mediante un software independiente de los dispositivos que recoja datos de distintos elementos o sistemas de seguridad.

2. **Análisis:** el sistema debe analizar y correlacionar datos, eventos y alarmas para identificar claramente la situación real y establecer los niveles de prioridad adecuados.

3. **Verificación:** el software PSIM tiene que mostrar la información relevante de forma rápida y amigable a los operadores, para que estos puedan verificar la situación real con precisión.

4. **Resolución:** el sistema debe proporcionar procedimientos operativos con instrucciones paso a paso, basados en buenas prácticas y políticas de la organización y que permitan resolver de forma eficaz las diversas las situaciones que se puedan presentar.

5. **Informes:** el software PSIM, además de analizar la información y registrar los pasos ejecutados, debe generar informes de conformidad que faciliten la depuración, mejora de procedimientos, formación y, en caso necesario, un análisis de profundidad.

³ Extraído de: <http://www.alava-ing.es/seguridad/productos/physical-security-information-management---psim/>

¿Qué beneficios puede aportar PSIM a la organización?

Los beneficios son múltiples. Pero alguno de ellos los podemos resumir de la siguiente forma:

Beneficios Operativos:

- Información centralizada de todos los sistemas de seguridad física
- Información en tiempo real, con acciones predeterminadas para eventos conocidos y desconocidos.
- Independencia de los operadores de los sistemas, porque ya no necesitan realizar acciones en forma manual
- Elimina la necesidad de disponer de varios sistemas, monitores, y accesorios. Todo está centralizado, por ejemplo en un Video Wall⁴
- Automatiza la detección y resolución de alarmas.
- Identifica los “Verdaderos y Falsos” de las situaciones, permitiendo trabajar sobre lo que es prioritario.

Beneficios Tecnológicos:

- Soporte integración con los dispositivos más importantes y utilizados del mercado.
- Soporte integración con tecnologías analógicas y digitales.
- Reduce los gastos de IT, por la consolidación de la infraestructura.
- Mejora los tiempos de respuesta, ante eventos no deseados, debido a la centralización de la información en un único punto, y sobre todo por la capacidad de programar acciones automáticas ante eventos previstos.

⁴ Video Wall es una forma de visualizar imágenes, utilizando para ello, varios monitores, por ejemplo LEDs, en forma horizontal y/o vertical. Estos monitores o televisores interconectados, permiten unir la imagen de forma tal que se aumente el tamaño de visualización, como si hubiera un único monitor o TV de mayor tamaño.

¿Cómo se integra un sistema PSIM en la Organización?

Posiblemente resulte difícil de visualizar la explicación de todo lo que anteriormente se describió, por eso, la siguiente imagen que fue extraída de internet, representa una clara visión de cómo todos los diferentes subsistemas pueden estar interconectados mediante un software PSIM.

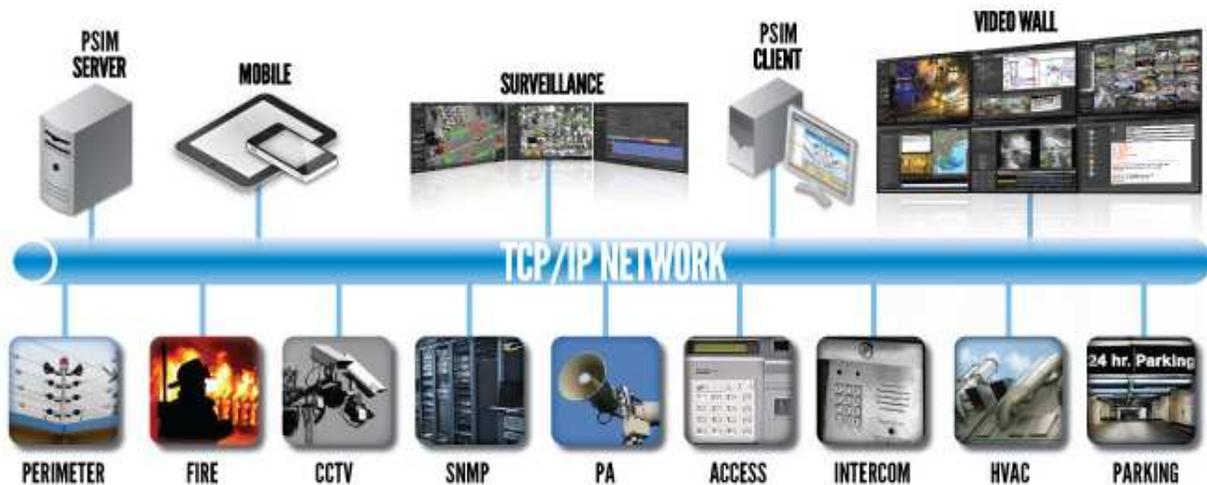


Imagen extraída del sitio web: <http://www.aventuracctv.com/psim/>

La parte fundamental del sistema PSIM, además de la correcta elección del software, y su capacidad de integración con otros productos, sin dudas es la red TCP/IP, ya que a través de la red de datos, todos los sistemas y dispositivos establecerán una conexión para poder operar.

La red de datos, debe tener las características propias de una red confiable, para poder permitir la transmisión de toda la información necesaria de manera segura y fiable.

Es muy común que en los sistemas donde conviven cámaras IP, Sistemas de Control de Accesos, y otros softwares o dispositivos, la implementación de redes de esta naturaleza se realice con Fibra Óptica y a velocidades superiores al Gigabit/Seg. Por supuesto, la implementación de VLANs para este tipo de sistema es un requisito fundamental e indispensable para un adecuado funcionamiento.

El dimensionamiento de la red, y cómo debe diseñarse, sobre todo si hay cámaras grabando en alta resolución es un paso muy delicado que requiere planeación previa.

Lo mismo ocurre con los servidores y con el almacenamiento (storage). Cualquier error en el dimensionamiento de la infraestructura tecnológica, puede tener consecuencias graves en el funcionamiento del sistema PSIM. Por ejemplo, un diseño incorrecto de la red de datos puede traer aparejado problemas serios en la medida que se incorporan cámaras nuevas para el sistema de CCTV, y es una falla frecuente, notar que el sistema funciona lento, congela las imágenes e incluso la pérdida de video puede ser constante, como consecuencia de una mala "Ingeniería de la solución".

Se sugiere en todos los casos, antes de la instalación o implementación de un sistema PSIM, generar contacto con firmas especializadas, de trayectoria y con experiencia comprobable en el diseño, implementación y puesta en marcha de soluciones de esta magnitud.

Conclusiones Finales

Seguramente habrá lectores que se estarán preguntando, luego de leer este documento, que tipo de sistema conviene implementar en la organización. ¿Conviene un VMS? o conviene un PSIM?.

En realidad, la conveniencia estará dada por la necesidad que la organización tenga en la actualidad y “hacia el futuro”.

Si la organización necesita únicamente de un sistema de video cámaras, que sea escalable, y eventualmente requiere interactuar con otros dispositivos tales como controles de acceso y/o sistemas perimetrales, puede que una única implementación con un Software tipo VMS alcance y sea suficiente, siempre y cuando el software permita que los dispositivos se vean interconectados entre sí (en la jerga a esa práctica se la conoce como INTEGRACION). Siempre que los dispositivos a visualizar y/o controlar, estén integrados con el software VMS, no habrá problemas, y en el mercado hoy pueden encontrarse soluciones VMS de bajo costo que integran miles de dispositivos y tecnologías.

En cambio, cuando la organización es más grande estructuralmente, y cuando en ella coexisten diversos y varios tipos de sistemas de seguridad física, sin dudas, el tipo de software que conviene elegir es aquel que esté destinado a cumplir con esa función. En este caso un software PSIM sería el indicado.

En párrafos anteriores, mencionaba la frase “Hacia el Futuro”. Esto no es una cuestión menor. Está relacionado directamente con la estrategia de las TIC's⁵ que el CIO de la organización deberá contemplar.

Puede que la organización se esté formando, y que en un lapso muy corto de tiempo, sólo necesite, por ejemplo, utilizar video cámaras, pero puede que en los planes de 3(tres) a 5(cinco) años (por dar un ejemplo), la organización decida implementar nuevos sistemas de seguridad física.

Si este fuera el caso, entonces, conviene implementar un sistema PSIM desde los inicios, el que luego, con el tiempo, puede ir creciendo en forma escalonada, o en forma modular para integrar nuevas tecnologías y productos de seguridad de la compañía. En este caso, un correcto diseño de la solución, con visión a futuro, permitirá ahorrar costos, optimizar infraestructura, y crecer rápidamente sin necesidad de hacer grandes cambios estructurales.

⁵ TIC's se refiere a las Tecnologías de la Información y Telecomunicaciones.

Para finalizar, vale aclarar nuevamente que sea cual fuera la elección del software que se implementará en la organización (VMS o PSIM), es altamente recomendable que el grupo de Analistas junto con el CIO, realicen un estudio técnico profundo, sobre la tecnología que se desea implementar, y de las potenciales empresas que lo podrían implementar, con el fin de asegurar que los requisitos técnicos y del negocio, son alcanzables y realizables.

Bibliografía Consultada

http://www.axxonsoft.com/products/axxon_next/

<http://www.cctvforum.com/>

<http://www.seguritecna.es/seguridad-privada/seguridad-electronica/analisis-de-video-para-la-proteccion-perimetral-y-grandes-areas>

<http://www.lenel.com/case-studies>

<http://www.lenel.com/video-management>

<http://www.milestonesys.com/Software/XProtect-IP-Video-Surveillance/XProtect-Open-Platform/>

http://www.axxonsoft.com/integrated_security_solutions/pos/functions.php

<http://www.axxonsoft.com>

<http://www.cnlsoftware.com/images/Whitepapers-Reports/White-Paper-CNL-Software-Why-Should-I-Be-Interested-MWP-501-0212.pdf>

<http://www.cnlsoftware.com/ipsecuritycenter/white-papers-reports>

<http://www.csoonline.com/article/2126002/metrics-budgets/physical-security-information-management--psim---the-basics.html>

<http://www.alava-ing.es/seguridad/productos/physical-security-information-management--psim/>

<http://www.digitalavmagazine.com/2012/09/20/axxonsoft-integra-el-escaner-laser-redscan-de-optex-en-la-psim-axxon-intellect/>