Backgrounder: The PSIA Recording and Content Management Specification

The Benefits

- The PSIA Recording and Content Management (RaCM) specification, combined with the PSIA IP Media Device spec, enables Digital Video Recorders (DVRs), Network Video Recorders (NVRs) and Video Management Systems (VMS) from different manufacturers to easily interoperate with each other and to control the different devices (e.g., cameras and encoders) in a video surveillance network.

- The PSIA RaCM specification gives DVRs, NVRs and VMS a common language; the PSIA IP Media Device specification does the same for IP-based surveillance cameras and encoders. When all these devices can "speak" to each other, video data recorded by one or more vendors' cameras can be saved to NVRs from one or more company, and can be viewed and managed by yet another vendor's VMS or a physical security information management system (PSIM). The VMS and PSIM systems can also control cameras at the network's edges.

- The PSIA RaCM spec standardizes how systems tag video data, such as a motion-triggered event, making it easier for security users to quickly search and retrieve data. Through the RaCM specification, an alarm or event in one system can be automatically communicated to and trigger actions in other systems, increasing the value of surveillance networks.

- The specifications enables integrators and end users to focus on selecting the best cameras, recorders and management systems without spending money and time writing software interfaces to ensure these devices will communicate. Devices compliant with the PSIA IP Media Device and RaCM specs are designed to work together "out of the box."

- Manufacturers can focus on product features and functions instead of communications and interoperability issues because these have been solved by the PSIA's RaCM and IP Media Device specs. Today, VMS and camera vendors put intense resources into solving these challenges.

Practical Application: Gaining Interoperability Across a Video Surveillance Network

Most video surveillance networks include a mix of IP cameras and legacy analog cameras, encoders and recorders from many different manufacturers. Very large networks may even have more than one VMS controlling different network segments. In most cases, application programming interfaces (APIs) or custom code is necessary to enable IP cameras at the edge of the network to interact with an NVR or VMS. APIs are generally unique for each camera vendor; code may be required for a specialized camera not supported by the VMS. Each time camera firmware is upgraded, APIs and custom interfaces may also need to be updated.

All of these connections are standardized and streamlined in a video surveillance network compliant with the PSIA's IP Media Device and RaCM specifications. The equipment becomes plug-and-play compatible, enabling security users to focus on functionality, not interfaces.

For example, users can enable a "motion detected" event captured by a camera and NVR in one segment of the network to be an event trigger in a VMS and/or PSIM system, even though all the devices and systems come from different manufacturers. Security users could then directly control the camera from the VMS.

Practical Application: Video/Multimedia Content Management

IP video cameras can generate vast quantities of image data, yet usually only a few seconds or minutes of footage are needed to trigger alerts in other systems or to aid in a forensic investigation. Searching the data from one camera is already a significant challenge; during a security event, users may also need to quickly locate and review data from additional devices from different vendors.

The PSIA RaCM spec simplifies and speeds up searches like these because it standardizes how video devices describe or "tag" events and provides a common language for recording, managing, searching and retrieving video/multimedia data. Knowing how all video events are tagged enables end users to quickly filter out irrelevant data.

Users can combine these capabilities with other PSIA-compliant systems to gain still more utility from surveillance networks. Because all PSIA-compliant systems understand "events" in a common language, events captured by cameras can be used to create triggers in other systems, including access control. So motion at a door could close a lock, launch a second camera view, collect data from a sensor, etc.

Specification Basics

- The PSIA specifications make plug-and-play interoperability possible for systems, applications and devices across and beyond the security ecosystem. All PSIA-compliant systems and devices, from cameras to physical security information management systems, have a common way to describe alarms, events, actions, etc.

- Because all the systems "express" themselves in a common way, it's easy for the integrator or end user to set up "if-then" triggers in the rules engines usually built into security systems and applications.