

Remote Surveillance

from the Ground Up

Factors to consider about your remote monitoring project before you even reach the design stage.

By Rebecca Jew and Jay Wallace



A video entry system provides security for a remote parking deck.

Many technological advancements have been made in the past few years in the CCTV systems market: the introduction of the digital video recorder, digital cameras, CCTV motion detection, video servers, video over IP and more. CCTV has developed into an integral part of security systems and operations. It has grown in capabilities, affordability and quality.

At the same time, new threats, budgetary constraints and staffing limitations have changed organizations' expectations of CCTV. Companies and businesses with multiple sites or campus environments now find it

necessary to consolidate their security operations into one central location. As the security director or CSO of a company, you may struggle with a common dilemma: how to recognize, among the wealth of technologies, the right solutions for remote surveillance at your facility, and how to combine them to create a successful system.

Carefully examining each aspect of the surveillance system and then examining the system as a whole can give you perspective on the nature of a comprehensive and time-surviv-



able system. Often, applying multiple technologies can prove a cost-effective benefit to system design.

Bandwidth

Bandwidth use is a critical factor for remote video surveillance. Each component of the system will affect the bandwidth needed for communication at remote locations.

Cameras and Views. What type of camera will you need? Will it have to monitor a sales counter at a 24-hour convenience store, a person exiting the building through a remote door, or an entire retail sales floor? What is the ambient light level of the area? Will you require incident detection? How detailed will the images need to be—do you need to read license plate numbers or identify drivers? Of course, larger images, higher resolutions and advanced features will likely mean more data to be transmitted.

Storage. How much online retrieval will you need? What is the backup plan? Will the cameras be recorded

Wachovia Bank Standardizes on March Networks Digital Video Systems and Software

Wachovia Bank N.A. has chosen March Networks™ DVRs and Enterprise Management Suite software as the standard digital video surveillance system for Wachovia's retail banking facilities and international corporate offices. Wachovia selected the products, as well as the Banking Assistant software module, after a thorough product evaluation process conducted by its physical security and IT teams.

"The DVRs are engineered to perform as networked security devices and are well-suited to the high reliability demands of large implementations such as ours at Wachovia," said David Smith, vice president and leader of Security Systems and Equipment with Wachovia Bank.

A phased deployment of the Linux-based DVRs and software was started in early 2005 and entails integration with the bank's access control systems and alarm monitoring center. The Banking Assistant software module links digital video with synchronized ATM and teller transaction data to support the bank's loss management and corporate fraud investigations teams in expediting dispute resolution and investigations.

The Enterprise Management Suite provides the multi-site DVRs with consistent programming and configuration in all retail banking locations. The software's centralized management capabilities provide the bank's security services group with centralized control and access to video across all of Wachovia's locations. Additionally, the software supports remote diagnostics, user authentication and automated system health notification of the IP-networked DVR installation.

full time, or just upon incident? What recording rate (frames per second) will you require?

Transmission. Will the data from the remote sites and buildings be transmitted via the existing company WAN or a separate network? How much data will be transmitted from any given location?

Preparing for Expansion

Another area you must address

at the onset of design is the future expansion of the surveillance system. A comprehensive system must anticipate future growth within the original infrastructure design. How many manageable systems have evolved into rats' nests with piecemeal equipment, making maintenance and operation almost impossible?

To avoid this fate, first brainstorm an ideal system. Envision a system that will fulfill the anticipated needs

and growth for the next five to 10 years. Define the capabilities of the central site, and then do the same for each remote location or building. For example, one location may be unstaffed with just a fence gate and door, while another may be a building with many employees, entrances and a parking lot.

Developing and applying templates for the various types of location will help define the size of the system. Specify the areas of responsibility and define resources. Next, go back and define realistically what can and will be done in the immediate future.

Maintenance Concerns

Another area that is often overlooked is the ownership and maintenance responsibility of the video equipment and software connected to the company network. Too often there are no clearly defined roles in this area between the IT and the security departments. To avoid problems, set up roles and responsibilities at the onset of design, and be sure all parties agree upon them.

One option is for the IT department to supply, set up and support all network-related devices, such as workstations, servers and mass storage devices. IT could also perform the back-up functions, since they typically perform these functions for other departments. A security technician could service and maintain all security-related devices, such as cameras and switchers. The security technician would also be responsible for video applications that run on the workstations and other network equipment.

An arrangement such as this defines clear areas of responsibility for each department, eliminating future conflicts over maintenance.

Transmission Considerations

With the advent of IP video devices and equipment, systems no longer have to be wired point-to-point from remote device to the head end. The system may now be looked at as any other data network with the same infrastructure devices, capabilities and limitations. Video over IP is now coming into its own, easing some of the old pitfalls and addressing issues by providing better video compression and other pro-

programmable features to reduce network traffic. Additional features and technological advances allow better user interfaces and better integration with access control and intrusion detection systems than before.

Review the infrastructure needed to transmit video and control to and from remote locations and buildings. Large companies typically have some type of network infrastructure in place already. If no network connectivity exists between locations, consider alternatives. Among the options are dial-up, Web-based and wireless transmission. You could also create a stand-alone video network. Each option has limitations that must be understood.

- Dial-up is slow and generally has poor frame rate and resolution.
- DSL helps but is good only for a few cameras.
- DSL may not be readily available everywhere.
- Web-based systems have limitations similar to dial-up and are at the mercy of Internet traffic loads.
- Wireless can offer much improved resolution and frame rate but is usually limited by distance, unless you have access to television station-type feeds.
- Creating, installing and maintaining a new network can be expensive.

This is the ideal time to bring in the IT department. Include them as part of the project team in decisions, recommendations, design and implementation. By involving IT as part of the process at the onset, you allow them to take on some ownership of the system. They can provide valuable input into the transmission design, which will go a long way to make the entire process easier.

Ask the IT department if it is possible use the corporate network for video transmission. Is there extra bandwidth? Can more bandwidth be added? Which remote sites have connectivity? Ask for an IT network connectivity diagram. The diagram will show whether there is network

connectivity to one, some, all or none of your remote locations. Ask for the long-term growth plans for the IT network. Using all the information gathered, you



can paint a clear picture of exactly what is needed at each location and what exists at each location to support the system.

One advantage of an IP-based surveillance network is that expansions and additions are relatively easy. Each remote location can be designed as its own sub-network; a location can function on its own for recording purposes. If the rest of the network goes down, the location will continue to function and record, providing redundancy and survivability for the system. Once the network is back online, full access to all recorded events and online control will be available. This configuration allows video storage and control to be distributed throughout the network. Several buildings can be online backup locations for each other, sharing storage and control.

Video Management

At night, the remote sites could download each day's recordings to a central video server or SAN for intermediate storage. The recorded video would be available for access by others connected anywhere on the network.

One archiving method is to record all video locally. When an incident occurs, the local system creates the



video segment and notifies the local and central site security personnel of the incident. The equipment at each remote location can be programmed to site- and camera-specific actions. Event priorities can be programmed locally and remotely to assist personnel in handling the condition.

By displaying only critical incidents at the central location, the system frees the network from becoming tied up with video data transmission. Since each remote site would be recording all cameras locally, a large amount of data would be transmitted to the recording device at the site. This may be too much for the remote site network to accommodate; therefore, analog cameras and wiring may be the most cost-effective way to wire the remote site, using video over IP for transmission to the central site.

For large surveillance installations with many cameras, the speed of the network becomes more important to the overall performance of the data and video system equipment. There are 10GB systems available for this purpose, but the initial outlay of equipment could be expensive. A balanced approach with the proper mix of IP and analog cameras will satisfy the operational objectives of the system while controlling cost. **ST&D**

Rebecca Jew and Jay Wallace are security consultants based in Sako & Associates' Washington, DC, office. They may be reached by phone at 703-641-4600 or by e-mail (jwallace@rjagroup.com or rjew@rjagroup.com).