

VIDEO & INTERACTIVE ALARM VERIFICATION WHITE PAPER

By: Steven D. Bayrd, Manager of Systems & Engineering, Premier Security, Inc., 1-800-320-2527

As technology expands throughout all aspects of daily life, it is only natural that it should be used to overcome problems that have had few solutions in the past. One of the problem areas in the use of **intrusion, robbery and medical emergency** alarm systems has been the lack of information available to first responders. Law enforcement in particular has had to contend with a large rate of **false alarms** from intrusion (burglary) alarm systems, both commercial and residential. Additionally, when responding to immediate, life-threatening events such as **robberies in progress**, police often have no detail of what the situation is within the location upon arrival.

In response to false alarms to which police must respond, at (it is claimed by law enforcement) a cost to tax-payers both in dollars and efficiency, some law enforcement agencies are adopting a **“no response unless verified”** approach. For instance, a recent policy adopted by the **Los Angeles Police Commission** (but temporarily placed on hold by the city council) states that officers will not respond except to an alarm call “that includes a visual monitoring of potential criminal activity or a person reporting an open door, broken window or activity consistent with a burglary.” **In the case of robbery or so-called duress alarms, officers will respond; however, an ideal situation would allow police to view the interior and/or exterior of the location to ascertain the gravity of the situation and formulate the best response.** This would greatly assist in the protection of life and property. There seems to be a very real trend amongst local and county governments to attempt to adopt similar “non-response unless verified” policies. The Los Angeles policy is of particular interest in that 20 percent of alarm owners/users create 100 percent of the false alarms. It is clearly unwise to penalize the 80 percent of responsible alarm users for the problems caused by the 20 percent who are false alarm generators.

In the past, efforts have been made by alarm monitoring stations to verify alarms through multiple calls to the location and responsible parties. Additionally, some systems were used that monitored audio microphones at the location during alarm situations. Both methods provided some help but often the person at the monitoring station was placed in the difficult situation of subjectively trying to decide whether an actual crime was in progress.

The most recent, and most promising method of alarm verification is through the use of cameras and optional voice communication equipment at the alarmed premises. This is called Video Verification. As **communication and networking technologies** have overcome many obstacles that made video image transmission slow and cumbersome, a new industry developed to exploit the increases in bandwidth now commonly available. This can also include two-way voice communication with the monitoring station to hear, see and in certain cases speak to the persons at the premises.

The security and alarm industries are taking full advantage of this expanded capability to address the problem of alarm verification. From image capture during alarms to network cameras to digital recorders with remote viewing to streaming video over networks and the internet, virtually any location can be monitored from anywhere by authorized personnel for a number of uses. While for this study we address video alarm verification, many other uses of such systems exist. **A video monitoring system can be an exceptional management tool** for employee training, internal loss prevention, employee safety, as a replacement for costly guard services and reduction of insurance premiums as well as evidence insurance and/or worker’s compensation claim cases.

Most often in commercial, institutional and industrial facilities, there are already cameras in use in a closed circuit television system (CCTV). These **existing cameras can generally be used for video**

verification with the addition of transmission equipment. To enhance the system where needed, additional cameras can be added and **on-site or remote digital recording can store the images for later review or evidence use**. Most systems include **password protection** to eliminate unauthorized access or lock-outs that allow viewing only during alarm events. These measures address **privacy issues** that naturally occur in virtually every installation, especially in residential applications.

While most video verification is conducted by alarm monitoring centers and security companies, an unusual but seemingly successful video verification system has been enacted by the Seal Beach (California) Police Department. In their systems, selected commercial and institutional business have sent live video from the monitored location to determine if a crime is in progress. So far, several banks and retail chain stores are participating. It is highly unlikely that this service will be extended to residential users due to the cost of the service and also the volume of alarm activity in the residential alarm market. A more likely scenario for **most municipalities will be a requirement for video alarm verification through traditional alarm monitoring centers**, who will then forward the information and images to police when a crime is detected.

The available technology is impressive and ranges from systems that automatically send still-frame pictures of the scene to the alarm monitoring center, to streaming video solutions that can be directed to wired and wireless networks and the internet. As this technology expands and municipalities and counties move to a verified response only policy, it is essential that business, residential and institutional security alarm system users **seek qualified video verification providers** that are keeping up with this rapidly expanding market. The lines between the Security industry and the Information Technology (IT) industry are blurring rapidly. As new developments in technology bring better video verification solutions to market, end users will need the help of security providers and system integrators that are trained and aware of the latest technologies.

In conclusion, whether your local authorities are requiring visual alarm verification before response or not, the trend to verify will continue. Planning for this eventuality and implementing video verification will not only place the user in a position for priority law enforcement response, but will also gain the availability of excellent management tools for themselves.