

Market View: Government Facilities

Enhancing the Protection of Critical Government Facilities

The Challenge

Government facilities, both federal and local, are prime targets for terrorists. A strike against any government facility whether it were a general use office building, special use military facility, embassy, courthouse, national laboratory or other would be a strong statement by terrorists. Government facilities must also be prepared for non-terrorism related acts of violence and natural disasters. In many cases, government facilities are not yet where they need to be to manage various security threats. Improving conditions at these facilities to protect vital buildings, systems, employees, and the public against disasters, acts of violence, and terrorism is of critical importance. Enhanced protection requires a comprehensive approach encompassing perimeter security, access control, video surveillance and communications. However, it is the ability to use the information provided by the various security systems and respond readily and appropriately to potential threats that will make the difference in the event of a disaster.

Protecting the Perimeter

The facility perimeter is the first point of potential security breach and, therefore, the first place to strengthen security measures. Depending on the facility, the perimeter may be entered through authorized access points (e.g. front door, parking lot) on foot, by vehicle, or both. Caution must also be taken to ensure the perimeter is not breached through unauthorized access points (e.g. over a fence).



Sufficient illumination around the perimeter fence is a critical first method of defence. It not only acts as a deterrent, but also ensures that activities are able to be seen clearly by cameras surrounding the area, particularly at night. Infrared (IR) illumination is another tactic that can be used. While still allowing cameras to clearly capture images at night, potential perpetrators are not alerted to the fact that they are being watched. A standard electronic fence can be enhanced with additional sensors like motion detection to further harden the facility.

Vehicle entrances should be equipped with barriers, access control, cameras with video analytics (e.g. licence plate recognition) and communications (e.g. intercom). To be most effective a guard needs to be at the entrance to verbally and visually inspect vehicles entering the premises.

Guards should also be present at pedestrian entrances to evaluate visitors as they pass through security measures like metal detectors.

Turnstiles can also provide an effective way to manage the intake and flow of people into a facility.

Protecting the Building

Once inside, video surveillance and access control are among the most important security measures. Effective access control can take on a variety of forms (e.g. cards, biometrics) and ensures that unauthorized individuals are not able to enter areas holding sensitive information. Burglar alarms are an added layer that protect against unauthorized access during off hours.

Video surveillance allows for live monitoring either on or off premise depending on security protocols. Recorded video is also imperative for investigating events in the case of a situation.

The installation of intercoms throughout the facility and a quality public address (PA) system significantly enhances communications throughout the building which becomes of utmost importance during an emergency.

Actionable Intelligence

The installation of multiple systems, sensors and devices as described above produces a wealth of information. Being able to harness the information and use it in an

intelligent and timely manner in the case of security situations in a separate challenge and one that must be considered carefully.

Bringing the information from all systems (e.g. video, access control, burglar alarm, fence sensors, metal detectors, etc.) into one central location goes a long way in consolidating information for the operator. Providing operators all relevant risk information within a central system, helps to create fast, intelligent event response by reducing the risk and time associated with gathering and interpreting data from individual systems.

Additionally, being able to guide operator actions with well planned response workflows through the same central system removes manual decision-making requirements from the operators, reducing the risk associated with human error in high pressure, emergency situations.

The Platform for Actionable Intelligence

Command and Control Center (3C)

3C is a common management platform providing government facilities with a customizable and scalable solution to converge physical security subsystems into one easy-to-manage system. Its

ability to integrate and manage third-party systems suits the needs of critical government facilities by consolidating a vast amount of information from various sources and presenting it a way that will draw an operator's attention to the most critical information.

3C is an intuitive system comprised of four modules; an event management and response module, a mapping module, a video management module, and an intercom management module.

Event Management and Response

The event management and response module displays notification of an alarm indicating alarm type, description and priority. Alarms can be generated by any integrated subsystem. The associated predefined procedure for responding to the particular alarm also appears on this screen to guide the operator through the required response actions.

Mapping

The multi-level mapping module is designed to respond to alarms (i.e. fire alarm) from the event management system, instantly 'popping up' a map with an alarm icon to indicate the location of the alarm. The operator also has visual representation of nearby cameras and can double click to display for fast alarm verification.

Video Management

The Video Management Module allows operators to view both live and recorded video from multiple sources like analogue cameras, IP cameras and digital video recorders from any vendor.

Video Analytics

The Video Management Module seamlessly integrates with video analytics to detect elements such as motion detection, directional movement, left baggage or people counting.

Digital Video Storage System

The Digital Video Storage System is an advanced storage and filing system that allows audio and video from multiple sources and multiple compressions to be easily queried and viewed. It also employs a unique video authentication tool that will detect video tampering of any image.

Intercom Management System

The Intercom Management System is a standards-based VoIP Intercom solution. The Intercom Management System integrates voice, image and data into one cohesive solution allowing for the ability to communicate across vast distances over the network.