



Hospitals Meet Security Challenges With Integrated Solutions

Providing security for hospitals involves more than the best choice of products and features—it also requires best practices. Learn how security systems such as access control, intrusion detection, and digital video surveillance can be integrated into a building automation system to protect patients, staff, property, and information.

Table of Contents

I. Executive Summary	3
II. Healthcare Security Issues Today	4
The Challenge of the Bottom Line	4
III. Moving Beyond Basic Security Technology	5
Intrusion Detection	5
Access Control	6
Video Surveillance Technologies	6
Video Analytics Help Spot Incidents	7
Integrating Intrusion Detection, Access Control, and Video Surveillance	8
IV. Benefits of Integration	9
Integrated Security Better Protects Infants	9
Control in the Event of an Emergency	10
V. Examples of TAC Customer Solutions	11
University of Chicago Hospitals	11
Moffit Cancer Center	11
VI. Conclusion	12

I. Executive Summary

Security and safety at healthcare facilities are important for both quality healthcare and public safety. Hospitals and clinics are a safe haven for those in physical or emotional need, and increasingly seen as a place of refuge in the event of a large-scale emergency such as a natural disaster or terrorist attack. For these reasons and others, more and more people use hospitals as their first source for help. Hence, it is essential that healthcare security staff not only consider facility security and safety, but also take an interest in broader public safety.

By applying best practices there are many technologies that can aid a well-trained healthcare security staff in preventing crime and managing security incidents. The key systems of security are intrusion detection, access control, emergency communications, and video surveillance. If each of these systems is purchased separately, administration and training can burden a company or property owner. Intrusion alarms occur on one system, access badges are administered in a stand-alone database, and intelligent digital video technology runs on dedicated computer equipment. Each system requires service, maintenance, administration, and training.

By integrating these separate security systems under a flexible building automation system (BAS), hospital executives realize a lower upfront investment for a considerably more powerful security solution. Installation and training occur on a single system. Operational costs like administration and maintenance are also reduced. Component devices are used in multiple ways to trigger lighting, video capture, pan-tilt-zoom, higher video resolution or frame rate, door locks, and other aspects of building control. A single system enables greater flexibility to add security components that can be easily integrated into the overall system, keeping the cost of capital expenditures low, and requiring little additional training.

An independent study by Strategic ICT Consulting of a 145,000 square foot building shows a system installation cost saving of 24% for an integrated BAS versus separate systems. And after installation, operations and life-cycle savings continue. Project analysis by Teng & Associates shows that training is reduced 33%, IT administration is reduced 82%, and the cost for changes, upgrades, and additions to an integrated system are reduced by 32%. These operational figures are based on experience and measurement, and clearly demonstrate the value of an integrated BAS.

Finally, this paper will show several examples where TAC has effectively applied building automation products and related services to provide effective integrated security for its customers.

II. Healthcare Security Issues Today

Hospital security departments and staff are especially challenged to provide safe environments for employees, patients and visitors. Hospitals, by their nature, are designed to be open and accessible to the public, which means street crime and other dangers can easily enter through hospital doors if not properly protected. A Justice Department study reveals that hospital emergency departments across the country treat more than 1.3 million people a year for injuries caused by violent attacks, which can escalate and continue within the hospital itself after the initial incident. According to Bureau of Labor Statistics data for 1993, workers in the health care field experienced the highest incidence of assault injuries. One study found that 82 percent of nurses surveyed had been assaulted on the job, 56 percent had been assaulted in the year prior to the survey, and many assaults go unreported¹. The same study shows that the greatest number of assaults (25%) occurred in emergency departments. Medical equipment, supplies, and controlled substances can also be targets of theft; and hospital patients, visitors, and staff can become victims of purse snatchings and muggings. Large, urban hospitals often serve as many as 1,000 visitors in a single day, in addition to hundreds of patients. This all adds to the ongoing staffing issues facing so many of our hospitals today.

A survey conducted by the American Society for Industrial Security (ASIS) determined that effective security has become a part of the everyday operations of many healthcare organizations, regardless of size, location, or type of hospital. Security issues and concerns are identified and addressed daily by senior and middle management. Top-ranked security concerns are shown below.

Security and Safety Priorities	Areas Ranked for Greatest Risk of Crime
1. Patients	1. Infant Units
2. Employees	2. Pediatric Units
3. Visitors	3. Pharmacy
4. Vendors	4. Psychiatric Units

THE CHALLENGE OF THE BOTTOM LINE

Even as administrators are actively addressing safety issues, hospital executives are challenged by stringent budget demands where shrinking margins can impact investment in security technology (see Figure 1). Hospitals must serve the uninsured public and spend money implementing systems and procedures that allow them to conform to government regulations, such as the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the requirements of The Joint Commission on Accreditation of Healthcare Organizations (JCAHO) and Centers for Medicare and Medicaid Services (CMS). In a competitive market, hospitals also face the private healthcare practices of nearby clinics and independent doctor consortiums, which can siphon away high-margin services such as minor surgeries, ultrasound, MRI and CT scan, and recruit staff to a more secure and safe environment. And on the revenue side there is additional pressure from the Diagnosis Related Group (DRG) reimbursement schedule, which regulates how healthcare providers can charge for services.

In this financial environment, it is essential that healthcare institutions seek to proactively and continually reduce operating costs and limit liabilities. Many hospitals are turning to technology to help make the security programs more productive and effective. New integrated solutions for security, facility and data management enable healthcare institutions to both reduce costs and improve the safety at their facilities.

¹ Erickson and Williams-Evans study, 2000

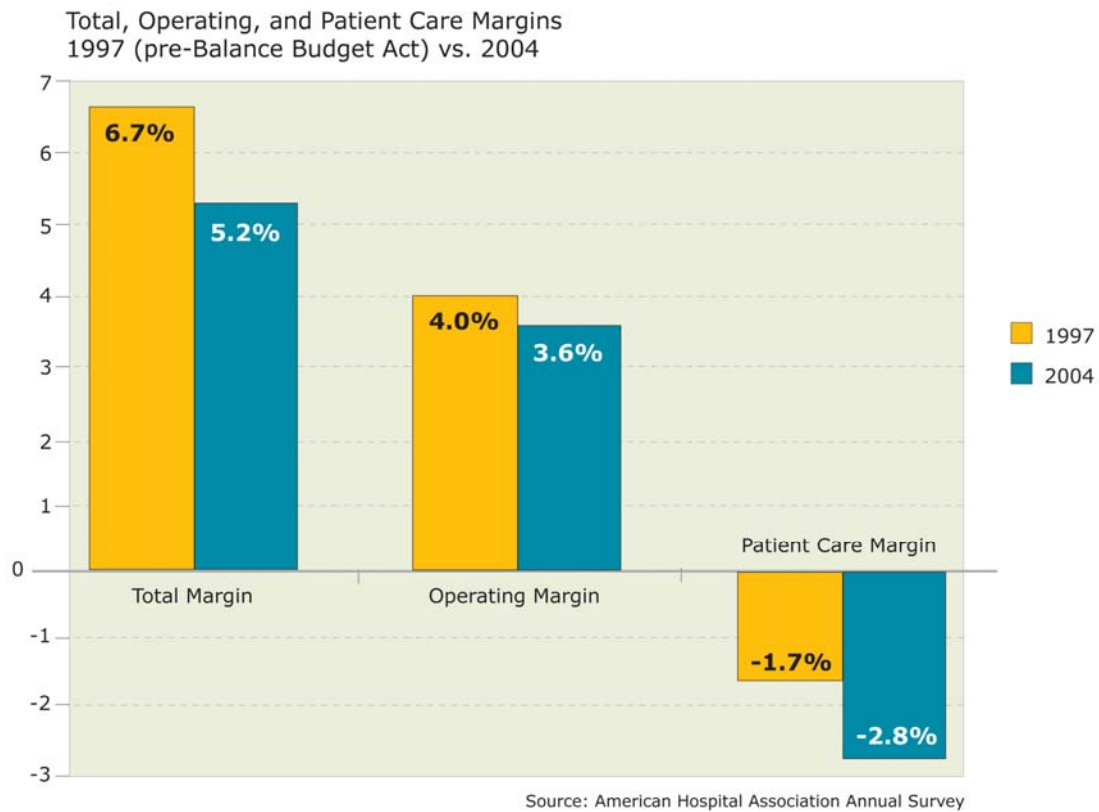


Figure 1

III. Moving Beyond Basic Security Technology

Regardless of the size of the healthcare facility, its location or the level of security risks that need to be addressed, there are essential components of an electronic security system. These include **intrusion detection, access control and visitor management system, and video surveillance**. These three systems, in the hands of competent and capable security staff, apply technology effectively to reduce crime and protect people and property. We will examine each system individually, and then in combinations to demonstrate how integrating security into the building automation system leverages these systems in multiple ways, increasing security and reducing operating and training costs.

INTRUSION DETECTION

Simple intrusion detection is probably the most familiar concept of security to most people. Intrusion detection involves the use of door or window contacts, glass contacts, or motion sensors, in combination with some type of audible alarm that sounds when a person has forced entry into a building or room. An alert is sent to the police or security station to notify authorities of the time and location of the incident. Security officers respond in person to evaluate the situation.

This method of incident response can be adequate for detecting an event and quickly getting to the scene. But the effectiveness of the response at the scene and subsequent prosecution is dependent on several things: the proximity of security personnel to the incident; whether witnesses were present; the number of people involved; the seriousness of the incident, and other factors. Furthermore, with simple intrusion detection, there is little in place that would deter people from committing a crime in the first place.

More information would be helpful, such as captured details of the situation that could lead to proper response and identification of perpetrators, thereby reducing the likelihood that a similar incident would occur again. Door and window contacts, motion sensors, and other devices already in use for alarming can be put to better use to help gather this information by triggering other parts of an integrated security system.

ACCESS CONTROL

Access control is the means by which people are granted or denied access to restricted areas, such as clinics, operating rooms, labs, and parking garages. One of the largest security challenges hospitals face is how to secure a space that is intended to be not only a public environment, but also an inviting one. This means that a balance between permissiveness and control is needed, not just using technology, but as part of the healthcare facility's culture of security. For example, a hospital may have a sophisticated access control system with picture badges issued to every employee, and card readers, electrified locks, and cameras protecting every door. But a courteous employee can defeat all of these security measures by holding a door open for a "tailgating" perpetrator. A good access control system can detect this, and issue an alarm to the security staff when it happens. Access control could be used to manage non employees—both vendors and visitors—using a "visitor management system". It can also assist with after hours access to areas of the hospital restricting and controlling certain egresses. Also, a single card could be used both for access to the parking garages and hospitals, making it easier of the staff and physicians.

With public, patient and staff needs in mind, how does management begin to evaluate the many types of access control systems that are available? Furthermore, in a growing and changing healthcare environment, what is the best kind of access control to meet future needs?

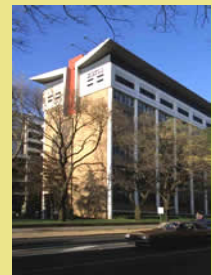
When used as a stand-alone system, card readers and other electronic access devices offer a cost-effective and flexible way for a hospital to control who has access to the various parts of the building, with the system recording who has gone where, and when. The sequence of operations is for the access device to trigger the door lock, entry is granted, and the event is recorded by the central system. But if a device can trigger the lock, why not use this inherent ability to trigger other security devices as well? As a stand-alone system, access control does its job, but does not fully leverage the connected sensors for broader security objectives.

VIDEO SURVEILLANCE TECHNOLOGIES

Video surveillance has evolved significantly in the last several years. Older video systems needed banks of video tape for continuous recording, and required manual administration to swap tapes periodically during the day. Record keeping was prone to errors and finding specific incidents on tape was time-consuming. **Digital Video Recorders (DVRs)** made significant advances in features and functions, taking advantage of fast computer processors and high density storage media to digitize, compress and record video from analog cameras. Newer cameras today have embedded processors that enable video to be compressed within the device and transmitted real-time over IP networks to **Network Video Recorders (NVRs)** that centrally manage video feeds from many IP cameras.

DVRs and NVRs have many advantages over older analog recording technology. Streaming video can be continuously recorded and discarded in cycles of days, weeks, or months if no security incidents occur. If an incident does occur, disk indexing and time-stamping make it simple to find video from a given date and time. In addition, because the video is digitized, it can be exported and distributed via email or backed up on CD, DVD, or other digital media using common computer backup programs that are widely available.

A major university of medicine on the U.S. east coast has increased expenditures for security from a \$100,000 investment in 1993 to more than \$2 million today. One reason for the increase is that the university has upgraded its CCTV system to digital video recorders with Ethernet capability and added 75 cameras. This enabled the security staff to record, monitor, play and view surveillance activity simultaneously with digital day/night pan-tilt-zoom cameras stationed throughout the university's campuses spread across five cities. The integrated surveillance and access-control systems allow officials to call up instant live video and recordings of alarm conditions and system activity. Using a single system that ties all of its properties together, the university has improved security while still making its campuses accessible to the more than 18,000 students, researchers, teachers, patients and employees.



Digital video surveillance is cost-effective and sold by many vendors in a highly price-competitive market. If purchased as a separate system to meet the needs of a security plan or upgrade, a DVR or NVR may be adequate for immediate surveillance objectives. But if this digital video recorder is integrated with an organization's access control and intrusion detection system (as part of the broader building automation system), the user improves surveillance and reduces the need for additional security personnel.

Integrated with access control, video verification, for example, allows a user to see live video as well as the cardholder's picture when a given access card is presented at a reader. The security staff can verify that the person presenting the badge is the actual cardholder. Another example of video verification effectiveness occurs in identifying individuals who are "tailgating" as noted earlier, when one person swipes their badge and gains access to the facility and another person follows them in without presenting their badge. The integrated system allows organizations to visually identify, verify and capture security breaches at access points.


VIDEO ANALYTICS HELP SPOT INCIDENTS

The advent of **video analytics** brings additional flexibility and increased productivity of security staff that monitor many cameras or for a non-manned time it can send out alerts to other staff members using mobile devices to respond where needed. Video analytics is a technology applied in software that examines the video camera's field of view for patterns of movement that match real-life events, such as falling, fence climbing, lurking, and trip-lines. Video analytics provides a means by which the user can focus only on what is truly important, managing surveillance by exception events rather than trying to observe all events.

A DVR or NVR can be configured to only display a camera's video if a specific event or alarm occurs. At a hospital for example, foot traffic in the evening past a closed pharmacy may be considered normal. But lurking



Video analytics software tracks people or objects, and can alarm on types of behavior



near the pharmacy door may be an indication that a break-in is about to happen. Video analytics can tell the difference. And additional alarms can be generated if video analytics detect more people in the video frame, which may indicate another level of security threat is occurring.

Another example of applied video analytics is a fence climbing alarm. Security staff may know that it is common for people to walk along the outside of a fence, horizontally across the field of view. They are not interested in this, as it poses no threat. Yet if someone were to begin to climb the fence, vertical motion across the field of view would trigger an alarm and transfer video to the security user's alert workstation.

These are examples of how expanded use of video surveillance technology can increase security at healthcare facilities without requiring an increase in security personnel.

INTEGRATING INTRUSION DETECTION, ACCESS CONTROL, AND VIDEO SURVEILLANCE

Today's access control and video surveillance systems can work together in an integrated BAS to provide a holistic solution for healthcare organizations, keeping intruders out of secure areas, limiting access to infant and pediatric wards, and remotely monitoring critical areas to reduce the risk of crime and security incidents. This is why more and more hospitals are increasing their use of CCTV as part of their overall security plan. Using an integrated system, security staff at a central monitoring station can view live images from surveillance cameras, control pan-tilt-zoom cameras, or search for video clips stored on digital video recorders (DVRs). When an alarm is triggered by intrusion or an invalid access card, the BAS can command the DVR to begin recording, display live video from a linked camera at the location, map the alarm location, and send an e-mail to an administrator all at the same moment.

CCTV cameras are an important surveillance component at vulnerable areas of a hospital, such as entrances, parking garages, pharmacies, and nurse stations. When a duress alarm is activated at one of these locations, cameras can be activated to survey the scene and monitor the emergency, and security personnel can quickly evaluate their response.

Asset protection is also becoming a high priority for hospitals. The hospital needs to track everything from PCs to wheelchairs, to PDAs and phones—not just for the value of the item but also for the data that could be located on it. They are more and more looking to RFID (Radio Frequency Identification) and tagging technologies to assist in this. This system works in conjunction with video and access control to document the movement of assets.

IV. Benefits of Integration

For hospital administrators and security staff, integrating various systems in the hospital offers numerous advantages. Foremost, integration provides for reduced installation and operating costs because it eliminates component redundancy and allows staff to streamline operations. Furthermore, it reduces training and empowers system operators by allowing them to perform their duties more efficiently. Integration can simplify the operation and control of complex hospital systems, while enhancing security at the same time.

Benefits of Integrating the Security System with the BAS

- ✓ A site-wide single-seat interface enables one person to be trained on multiple security systems.
- ✓ Security components become multi-use. A motion sensor can be used for lighting control during occupied hours, and intrusion detection during unoccupied hours.
- ✓ During design, flexibility, efficiency, and economy provide room for additional security expansion or integration at the lowest cost.
- ✓ Better response to occupant needs, offering patients and staff greater security and peace of mind.
- ✓ More information put to effective use, which gives hospital security staff solid ground to stand on for prosecution and proof of loss. CCTV records also aid law enforcement authorities in finding criminals.
- ✓ Vendor independence, allowing the customer to choose among best-of-class security products.
- ✓ Single-source responsibility, whereby one integrator is held accountable for the entire security system.

INTEGRATED SECURITY BETTER PROTECTS INFANTS

Administrators at all hospitals are concerned about infant abductions, and securing infants is certainly a priority, both for safety and public relations reasons. All told, 123 newborns have been abducted from hospitals since 1997. "Infant Tagging," as it is often called, is a high-tech infant protection program designed to prevent baby abductions from maternity units and nurseries. Typically, a small round button-like tag attached to a band is placed around an infant's ankle or wrist soon after birth. Each tag is actually a miniature RF device that works in conjunction with the access control system and automatic door locks. An alarm sounds when a tag approaches or goes through a door. An active monitoring system reports where the tag is at all times by sending a signal to the central monitoring center at the hospital.



With the system, the baby's parents or authorized hospital personnel can carry the baby freely throughout a designated area without generating an alarm. However, if an infant is brought near an exit door, or if the ankle band is tampered with, an alarm is generated and all doors leaving the area are automatically locked (in coordination with fire safety). An integrated system can also link infant handling to access cardholders,

activate CCTV cameras, lock stairwell doors, and control elevators. Integrated systems will also immediately display the identification of the baby and a map locating the exit door through which the baby was taken.

CONTROL IN THE EVENT OF AN EMERGENCY

At a major specialty hospital in the Northeastern United States, the BAS plays a key role in the facility's emergency shutdown procedure. A plan was put in place to protect against a potential biological attack. In the event of a bio-terrorist incident, the BAS operator will press the emergency shutdown button on the workstation screen. The system will immediately signal a critical alarm, page all maintenance personnel, and shut down the hospital's air handling systems and outside air dampers. These BAS measures ensure airborne agents are not spread further throughout the building.



Emergency rooms can be especially vulnerable, particularly at urban hospitals. Gang violence and domestic conflicts are among the problems that may enter the hospital along with a patient. This is why hospitals need the ability to restrict access to the emergency department (ED). A lockdown keeps people in the ED from further penetrating the hospital, while a lockout secures the ED entrance to keep threatening people from entering. Cameras and intercoms can be utilized as well to keep security staff fully apprised of the situation and ensure best practices are followed.

Integration Improves the Bottom Line		
<p>In an independent case study involving a 145,313 square-foot building with 1,500 occupants, a research team examined the installation costs of the components of a <i>non-integrated</i> BAS versus that of an integrated BAS.</p> <p>Systems integrated:</p> <ul style="list-style-type: none"> • Lighting Controls • Building Controls • Security • Fire and Life Safety • Metering and Monitoring • Structured Cabling 	\$2,464,693	<i>non-integrated</i> BAS
	<u>\$1,868,166</u>	<u>integrated</u> BAS
	\$596,527	difference = savings
<p>As the results show, the cost-savings were significant – over 24 percent. Findings also show that an integrated approach offers a broad range of commercial and technical benefits, including a single vendor point of contact, efficient project management, easier equipment deployment and investment protection for future upgrades.</p>		
<p>Source: Strategic ICT Consulting, April 2005</p>		

V. Examples of TAC Customer Solutions

TAC provides comprehensive, effective, and innovative building automation solutions for hundreds of healthcare facilities worldwide. Below are some examples of TAC's security solutions, and the benefits gained by the property owner.



University of Chicago Hospitals

University of Chicago Hospitals is one of the top rated healthcare institutions in the United States. With more than 1,000 beds, this academic medical center admits approximately 31,000 patients from all parts of the world and treats more than 500,000 outpatients annually, including 80,000 emergency room visits. Covering more than five city blocks, UCH employs over 4,700 employees. Providing a safe environment for both staff and patients presents a special security challenge for the Hospital's Security Department.

At one time, UCH had six different security vendors, a wide variety of security equipment, 26 different forms of authorized IDs, and had no centralized security control. A security solution from TAC provides an innovative approach to total security integration. The system controls access to over 640 doors and to the parking garage, providing full integration with the hospital's HVAC, lighting, CCTV, paging, intercom, critical life point monitoring, fire alarms, elevators, e-mail, and infant tagging systems. The TAC system also handles more than 715 unique alarms and 233 unique system schedules, stores more than 24,000 personnel records, and processes approximately 130,000 transactions per day.

Patients and employees alike can rest assured they will be secure when they come through the doors at UCH, a hospital on the forefront of medicine and leading the way in security technology.



Moffitt Cancer Center

The Moffitt Cancer Center in Tampa is the only hospital in Florida designated by the National Cancer Institute as a comprehensive cancer center. Moffitt has 162 beds and serves more than 4,500 inpatients and 100,000 outpatients yearly. The Center's campus contains nine buildings, including the Moffitt Research Center, a 101,352 square-foot facility dedicated to cancer research.

Exemplifying technology on the cutting edge, Moffitt Cancer Center chose a TAC facility management system to control and secure its facilities. The TAC system at Moffitt provides not just HVAC control, but security management, fuel tank monitoring, parking control, and integration with a Digital CCTV system.

Currently, 110 card readers control access into the Cancer Center after hours and in high-security areas 24/7. There are more than 200 digital CCTV cameras throughout the facilities, including several in an 800-car parking garage. The Moffitt security staff is able to monitor any camera from any workstation on the Center's LAN. There are currently 24 web client viewing stations spread throughout the buildings.

Administrators at Moffitt selected the TAC system to manage their systems more efficiently and utilize their full-time employees more effectively. TAC allows them to do both.

VI. Conclusion

Patients have high expectations for quality healthcare today. State-of-the-art facilities, safety and security are of primary concern. In order to meet rising expectations within this cost-sensitive market, hospitals must invest wisely in their facilities as a strategic asset to serve patients, attract qualified doctors and nurses, and serve the greater public. Fortunately, new building management solutions are able to increase security at healthcare facilities while also maximizing energy efficiency and performance. This leads to a reduction in operating costs and enables resources saved to be reallocated within the budget to new programs for patient services.

Technology must work effectively as a tool for well-trained security staff. When evaluating intrusion detection, card access control, and video surveillance systems, require that your vendors show how integration of these security functions can increase security and minimize the training and burden to security personnel. Ask that they show how integration with the facility's building automation system could provide further efficiencies of operations.

TAC is a leading expert in integrated security systems, with customers in 75 countries and more than 500 offices around the world. As a company of Schneider Electric, TAC brings the resources of a 17.3 billion euro parent company with 120,000 employees to help meet the requirements of any security or control need. To learn more about how TAC can help you achieve your business goals in the healthcare market, visit www.tac.com or call 1-866-TAC-INFO.