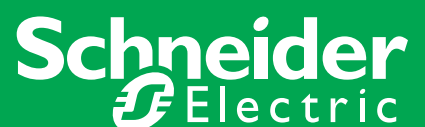


Creating Safe Campuses with Integrated Security Solutions

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

September 2006 / White Paper

Make the most of your energy



Summary

I. Executive Summary	3
II. Campus Security Issues Today	4
III. Moving Beyond Basic Security Technology	5
Intrusion Detection	5
Access Control	5
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 and Lighting Control	9
Convergence: The Future is Here	10
V. Examples of TAC Customer Solutions	11
The Georgia Institute of Technology	11
The University of Wales	11
VI. Conclusion	12

I. Executive Summary

Campus security and safety are important issues at universities today. Providing students nationwide with a safe environment in which to learn, and keeping students, parents and employees well informed about campus security are goals that have been voiced by many groups. These goals were advanced in 1990 by the Clery Act, which requires all colleges and universities that participate in federal financial aid programs to keep and disclose information about crime on and near their respective campuses.

Theft on campus, property crime and information security are major concerns today. Universities invest millions of dollars in security technology with the intention of increasing security, protecting students and staff, and solving security issues. This technology includes burglar alarms, fire protection systems, video surveillance, access control systems, and intrusion detection devices. Technology, in the hands of competent and capable security officers, can reduce crime, cut material losses, and keep people safe. But keeping security staff trained on separate, stand-alone systems can be challenging, and must be addressed as part of broader campus security objectives.

The key systems of security are intrusion detection, access control, and video surveillance. If each of these systems is purchased separately, administration and training can burden a university's resources. 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), university management realizes 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. Campus Security Issues Today

The safety of students, staff and visitors on college and university campuses is the responsibility of security officers who must pay close attention to the places where people spend most of their time, such as residence halls, classrooms, lecture halls and offices. But campuses consist of more than these buildings. A school might be home to sensitive research projects that require restricted access and closer scrutiny. A campus also might have other facilities that warrant special vigilance: laboratories with valuable data, libraries with rare volumes, museums with valuable and historically significant artifacts, and walls and corridors dotted with athletic trophies, paintings or sculptures.

Furthermore, college and university campuses are home to thousands of students 24 hours a day. As residential and work communities alike, campuses are dynamic environments with constant activity. As a result, an effective campus security program must address the protection of students, faculty, staff, and the safeguarding of campus property and facilities from damage or loss.

According to figures from the United States Department of Education, crime continues to be a problem at public and private colleges and universities (see figure 1). In 2003, the latest year for which statistics are available, there were more than 40,000 burglaries; 8,000 aggravated assaults;

3,700 sexual assaults (including more than 1,800 occurring in residence halls); and more than 1,300 arsons (almost half occurring in residence halls). There were also nearly 1,200 arrests for illegal weapons possession on campuses in 2003.

In such an environment, security remains a critical concern for administrators. Colleges and universities are spending money on a variety of technology and equipment to increase campus safety and protect property. This includes burglar alarms, fire protection systems, digital video recorder (DVR) surveillance and video cameras, security lighting, access control, sensors and detectors, and badging/ID card systems.

But are these investments the best way to increase security? These separate systems each address a different security need, and require training and familiarity to be most effective. A system that integrates the functions of many security devices into a single system significantly reduces capital expenditures and lowers facility operating costs because component devices are used in multiple ways and security officers can be trained on one system rather than many. Through integration, the whole security system becomes greater than the sum of its separate parts. And security staff becomes more effective on the job.

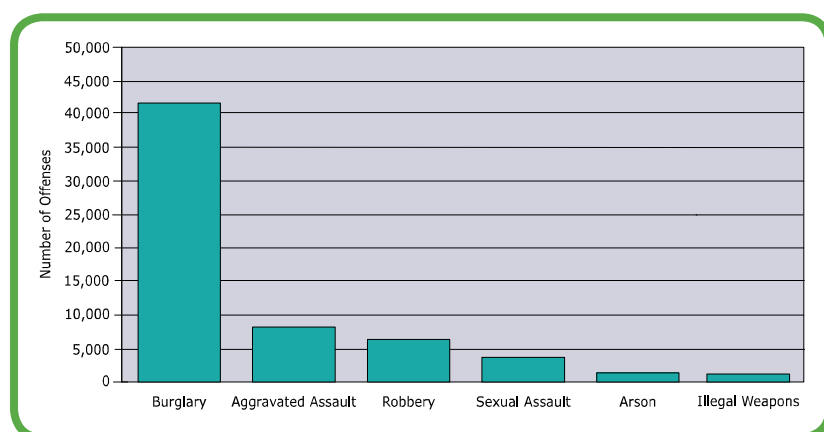


Figure 1:
2003 US Statistics at
Colleges and Universities¹

¹ Reported to the U.S. Department of Education. Figures from more than 6,000 public and private non-profit, and private for-profit institutions offering post-secondary educational programs

III. Moving Beyond Basic Security Technology

Regardless of the size of the campus, 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 **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 on campus. 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 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 the security system.

Access control

Access control is the means by which people are granted or denied access to restricted areas, such as residence halls, labs, parking garages, and fee-for-service areas like cafeterias or laundry. Colleges and universities are unique with respect to access control because the needs of the community vary widely depending on who needs to go where. There are day students, night students, athletes, faculty, staff, and other personnel with dissimilar requirements for security and building access. Some people on campus require varying degrees of temporary access privileges, and others need permanent access.

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

A flexible form of access control uses cards with magnetic card readers, proximity readers, barcodes, or smart cards with embedded microprocessors. Card access control at colleges and universities is common today, and there are a variety of systems with different levels of sophistication. There are many advantages to card access control. Students can be coded with access to specific areas depending on their academic major, seniority, class enrollment, team participation, or any number of factors. Individual privileges can expire on a given date if desired. And access can be granted or denied at any time based on the student's status. Cards can also be used as debit cards for meal-plans and other

university fee-based services. In areas where tighter security is required, management can install keypads, keypad/card combinations, or biometric devices that can scan fingerprints or handprints.

When used as a stand-alone system, card readers and other electronic access devices offer a cost-effective and flexible way for a university to control who has access to the various parts of campus, 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 decade. 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.

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," or 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 who monitor many cameras. 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 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 university for example, foot traffic on a sidewalk near a residence hall may be deemed normal, and not trip an alarm according to video analytics assessment. However, stepping off the



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

sidewalk and crossing left-to-right across the field of view to a window may trigger an alarm. Additional alarms can be escalated if video analytics detect loitering near the window, or someone climbing a fence.

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



A university serving 20,000 students on five campuses sought an integrated BAS that would allow the school to decrease operating costs, increase security for students and faculty, and allow for remote monitoring of each campus from a central location. The resulting system controls and monitors a wide variety of different building functions, such as access control events and logs, ventilation, day and nighttime energy use, chillers and boilers, and air quality. Even though there are five campus locations, they are all centrally monitored from an off-campus office.

A series of unobtrusive security measures are in place that ensure student safety and prevent campus crime or unlawful trespassing, without interfering with university life. Three of the campuses have a state-of-the-art contactless smartcard-based access control system that is linked via the university's existing IT Ethernet.

The TAC system controls over 160 doors and can handle 20,000 unique users. The system also integrates with other security systems, such as CCTV and intrusion alarms. The BAS controls all aspects of security and daily indoor environmental operations via constant readings from 3,500 control points. Via the university Ethernet, data passes from one building to another and allows system access from any site.

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 on college and university campuses. Keeping intruders off campus, limiting access to facilities that house expensive equipment, and remotely monitoring secluded areas to reduce the risk of crime. This is why more and more campuses now rely on CCTV as part of their overall security solution. 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 another part of the BAS, it 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 component of campus emergency call boxes. When a student contacts security via one of these stations, lights and cameras can be activated to survey the scene to observe the emergency, and officers can intervene to thwart an attack. Cameras are also useful for adding extra protection in remote areas, such as parking lots and garages on campus, especially late at night.



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, 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 maintaining a discrete and unobtrusive surveillance presence for more than 18,000 students, researchers, teachers, patients and employees.

IV. Benefits of Integration

For colleges and universities with diverse populations and building types spread over large areas, integrating various building systems offers numerous advantages. Foremost, integration provides for reduced installation and operating costs because it eliminates component redundancy and allows customers to streamline operations. Furthermore, it reduces training and empowers system operators by allowing them to perform their duties more efficiently. Colleges and universities

are also vulnerable to lawsuits alleging negligence in providing security, especially if there are uneven or inconsistent levels of security for buildings with similar purposes or design. Integration allows for uniform monitoring and control across a campus and demonstrates that an institution has applied appropriate security strategies at all its buildings. Lastly, enhanced safety, security and comfort create a more positive learning environment where faculty can teach and students can learn.

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 and more flexible response to campus needs, offering students and staff greater security and peace of mind.
- More information put to effective use, which gives university 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 university customer to choose among best-of-class security products.
- Laundry facilities and kitchens can consume 10-15% of the building's energy, increasing the need to more closely monitor hours of peak demand from these sources.
- Single-source responsibility, whereby one integrator is held accountable for all the components of the security system.

Integrated security and lighting control

By way of example, consider the benefits of simply installing a lighting control system versus integrating it with security. In a university laboratory facility, the lighting controls will enable the operator to maintain comfortable lighting levels and use presets to control the lighting. This ensures the lights are only on when and where they are needed, saving energy and related costs. If, however, there is a security

breach late at night, without integration, personnel will need to locate switches and issue commands to the control system to switch on lights in the affected area. If the lighting controls are integrated, the scenario after the security breach is much different. The lights are automatically switched on in the area where the security breach is reported, and CCTV cameras are activated to record the emergency. The operator has a single console to assess the situation and to ensure the appropriate reaction from the fire department or police.

With an integrated security and BAS, it is possible for a university's facility staff to control entire buildings from one workstation via a networked computer. From this single browser interface, operators can manage diverse building functions, such as environmental control, access control, video surveillance and alarm and event monitoring.

Building staff can view live or recorded video, open or lock a door, grant access to service technicians for emergency situations and handle visitor management. These tasks can be accomplished onsite or remotely at any time, whether during business hours, at nights or on weekends.

Integration Improves the Bottom Line

In an independent case study involving a 145,313 square-foot office building with 1,500 occupants, a research team examined the installation costs of the components of a non-integrated BAS versus that of an integrated BAS.

Systems integrated:

- Lighting Controls
- Building Controls
- Security
- Fire and Life Safety
- Metering and Monitoring
- Structured Cabling

\$2,464,693	non-integrated BAS
<u>\$1,868,166</u>	<u>integrated BAS</u>
\$596,527	difference = savings

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.

Source: Strategic ICT Consulting, April 2005

Convergence: the future is here

Today, most colleges and universities have high-speed computer networks and sophisticated and secure IT infrastructure. The campus network supports administrative servers, Internet access, multimedia file sharing, collaborative online communities, class registration, and many other computing resources. This type of infrastructure positions the institution to leverage the best that integrated BASs have to offer by sharing the campus-wide network for security and facilities management as well.

As a single integrated system, security and facilities management allows many building functions to be viewed within a single, common interface.

All hardware, even video, alarm and printing equipment, can work seamlessly within its framework. Entering security and facility data just once, and having the framework synchronize with existing hardware and software automatically, is common on many campuses. An integrated system reduces the overall hardware and software requirements. This leads to fewer training issues, lowers training costs, and allows staff to work more efficiently trending building performance and troubleshooting building alarms. All of these benefits result in decreasing the burden on tightly controlled higher education budgets, freeing more money to go directly to educational programs.

VI. Examples of TAC Customer Solutions

TAC provides comprehensive, effective, and innovative building automation solutions for hundreds of college and university campuses

worldwide. Below are some examples of TAC's security solutions, and the benefits gained by the institutions.



The Georgia Institute of Technology

The Georgia Institute of Technology is a renowned education and research institution situated in downtown Atlanta. The 350-acre urban campus contains 160 buildings and 20,000 students. Over the years, various departments installed several types of keyless entry systems in more than two dozen buildings. There was no compatibility or integration between systems, and service and maintenance were difficult.

Solution

Georgia Tech turned to a TAC partner to install a system that integrated access control, security management, alarm monitoring and CCTV. Operating over the campus' existing LAN, the system offers distributed network operations. A single agency provides campus-wide centralized system security and database management, while the individual academic departments maintain decentralized operation and control. Each department assigns access to its facilities for students and staff and sets door lock/unlock schedules.

Gains

The University now issues one multi-purpose card to the faculty, staff, and students for both access control and for campus retail operations, such as food service and the bookstore. The ID card has both a magnetic stripe and bar code, so it is used as an access control card, a library card, meal card, and debit card. Another card includes a chip that only allows designated individuals access to sensitive areas on campus requiring more stringent security.



The University of Wales, Swansea, U.K.

The University of Wales, in Swansea, is one of the UK's top 50 universities, according to the Financial Times. More than 10,000 students and 2,000 staff study or work on its campus of 20 buildings. There are also five off-campus buildings and the new Wales National Pool.

Solution

Previously, on-site access control consisted of various stand-alone systems using several different access cards. The university decided to revamp the entire access infrastructure and move to a single, comprehensive security and management control system.

TAC provides a system capable of monitoring and controlling a wide range of electrical and mechanical subsystems, in addition to security. This flexibility gives university staff a unifying control system that feeds all data to a central database for easy operation, data storage and report generation. TAC integrated its solution with existing legacy systems using hybrid smart cards, an affordable solution that did not compromise security. The system controls all card-based services, such as vending, printing and copying, use one card that functions over the university's IP network for easier and faster management.

Gains

The university now uses security staff more efficiently because training and operation occurs on a single system. And costs were kept low by integrating the legacy card system.

VIII. Conclusion

Students have high expectations when they select a college or university. They require a quality education and campus experience at a reasonable cost. State-of-the-art facilities, safety and security are of primary concern. In order to meet rising expectations within this cost-sensitive market, colleges and universities must invest wisely in their facilities as a strategic asset to recruit students and attract faculty and staff. Fortunately, new building management solutions are able to increase campus security 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 students.

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 campus building automation system could provide further efficiencies of operations.

Schneider Electric

One High Street,
North Andover, MA 01845 USA
Telephone: +1 978 975 9600
Fax: +1 978 975 9674
www.schneider-electric.com/buildings

All brand names, trademarks and registered trademarks are the property of their respective owners. Information contained within this document is subject to change without notice.

On October 1st, 2009, TAC became the Buildings Business of its parent company Schneider Electric. This document reflects the visual identity of Schneider Electric, however there remains references to TAC as a corporate brand in the body copy. As each document is updated, the body copy will be changed to reflect appropriate corporate brand changes.