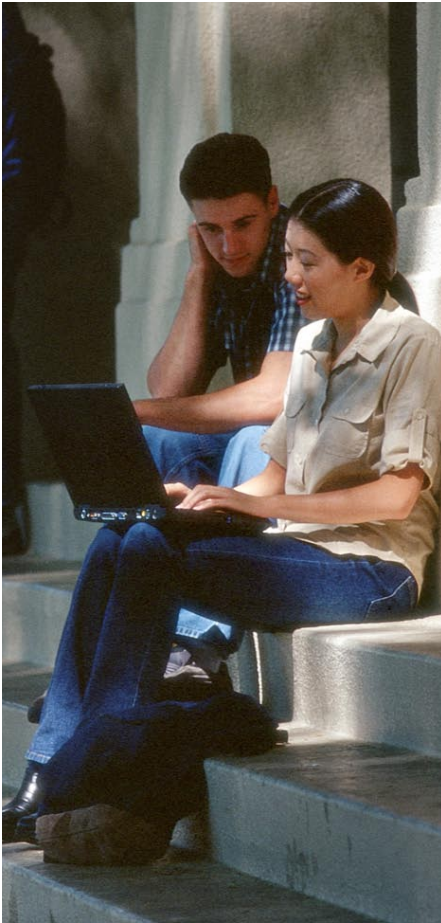


The Convergence of Physical Safety and Information Technology on Higher-Education Campuses



Abstract

Higher-education campus safety organizations are effectively using processes and technology to protect students, faculty, staff, and visitors. Nonviolent crimes such as burglary, auto theft, and arson decreased year over year from 2003 to 2005, and the violent crime rate declined 54 percent from 1995 to 2002.* But efforts to improve campus safety never cease because manmade and natural disasters can come at any time. For this reason, campus safety organizations continually strive to improve event detection, notification of affected students and staff, and response.

Campus safety organizations are making progress by deploying advanced communications systems, building management systems, and access controls. These become even more effective if they work together rather than in isolation. On most campuses today, motion sensors, notification systems, and video surveillance cameras are connected to separate networks. Therefore, if a motion sensor reveals activity in a secured area, a human operator has to notice the activity and then manually initiate the appropriate response, such as alerting security personnel or cueing a video surveillance camera. The need for human intervention can delay response, wasting critical time in a crisis situation. What's more, separate networks increase costs.

Higher-education institutions are taking the next step to increase campus safety by converging their physical safety systems with information technology (IT) systems. When campus safety monitoring and communications systems are connected to campus wired and wireless IP networks, the safety systems can be centrally monitored and set up to automatically execute actions based on campus safety policies. For example, a fire alarm in the chemistry building can trigger a policy to call 911, notify campus security on any communications device, activate a nearby video surveillance camera, and send text messages to students' mobile phones that classes in that building are cancelled.

This paper, intended for campus police, administrators, facilities personnel, and IT personnel, explains how the convergence of physical safety systems and campus wired and wireless networks can enhance campus safety.

Roles for Physical Safety on Higher-Education Campuses

Higher-education campus safety plans usually focus on the following goals:

- Prevention: Denying the means and ability to plan, act, or acquire materials intended to cause harm or interfere with normal operations
- Deterrence: Using governance, operations, and technology to create active and visible countermeasures to dissuade unlawful or disruptive actions

**Campus Violence White Paper*, American College Health Association, Feb 2005

- Detection: Providing immediate notification when unlawful or other prohibitive acts are occurring
- Response: Enhancing incident management processes by activating preplanned notifications or escalation policies to halt or mitigate unlawful, disruptive, or prohibited actions

Meeting these goals has traditionally required collaboration between campus administration, campus and community police, and the facilities organization. Increasingly, the campus IT group is also becoming involved (Table 1).

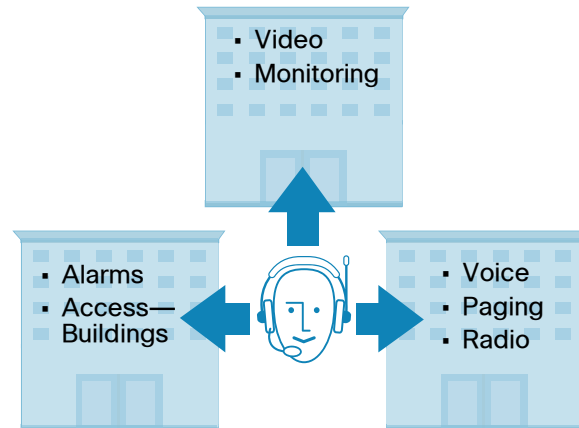
Table 1 Campus Safety Roles

Administration	Campus and Community Police	Facilities	Campus IT
<ul style="list-style-type: none"> • Provide a safe environment for students and staff • Support campus personnel with budget and resources 	<ul style="list-style-type: none"> • Deploy effective methods to prevent, deter, detect, and respond to safety incidents • Develop safety plans and train with first responders • Establish processes and communication systems to respond appropriately • Keep unauthorized visitors off campus 	<ul style="list-style-type: none"> • Develop and maintain safe buildings and grounds • Ensure that all facilities support diverse security needs across campuses • Understand and use cost-effective ways to enhance campus safety • Deploy systems to enhance safety and reduce destruction to property 	<ul style="list-style-type: none"> • Use technology to enhance safety • Protect physical safety systems as well as campus networks from unauthorized use • Provide safe network access for the entire campus population

Value of Converging Physical Safety Systems and IT

In most campuses, the communications systems, building systems, and monitoring systems currently operate over their own networks (Figure 1). Therefore, individual campus-safety systems cannot communicate with each other directly. Instead, a human operator needs to use one system to detect an event and another to take action, such as sending e-mails or sending a page to affected areas of campus.

Figure 1 Today's Physical Safety Systems Do Not Interoperate



For example, consider a university responding to an armed robbery that occurred in a storefront near campus dormitories. Here is the sequence of typical responses:

1. Local police notify campus administration and campus police by phone and radio.
2. Administration notifies the dorm resident advisors by phone or e-mail.
3. Resident advisors physically walk to the building entrances to lock down the building and then knock on students' doors to notify them of the lock down.
4. Most students are not sure why the lock down occurred, and rumors begin to circulate across campus, as students send each other text messages. Concerned parents call the dean's office and local police.
5. When the situation is resolved, local police again notify campus administration.
6. The administration again notifies resident advisors that the lock down has ended.
7. Resident advisors unlock the building.
8. Students in other parts of campus find out from their friends that the situation has been resolved.

The manual communication processes outlined here result in delays and confusion. And if the event had involved a toxic leak in a chemistry building rather than a lock down, students who were already on their way to campus might never receive the e-mail cancelling class, which would both compromise their safety and creating unnecessary traffic near the incident scene.

What if it were possible for all systems used for campus safety—building access, communications, and monitoring—to interact over the same network, automatically activating each other when needed to accelerate response time? In fact, higher-education campuses around the world are converging their physical safety and IT systems today to enhance campus safety.

New Role for IT in Campus Safety

Examples of the convergence of physical safety systems and IT include:

- **Newer physical security technology:** Today's access controls, badge readers, video surveillance cameras, and sensors are designed to operate over IP networks instead of single-purpose networks. In addition, safety organizations and IT groups on many campuses are establishing a relationship with the IT department to help configure new security systems, many of which are managed using a Web interface.
- **Growing acknowledgement that information security is part of campus safety:** Campus safety organizations protect people; facilities organizations protect physical assets; and IT organizations protect information assets. It makes sense for the organizations to come together for collaborative planning.
- **Network access control:** Campus IT groups have the technology to authenticate users and provide each one with the appropriate access privileges to buildings, systems, and networks to prevent unauthorized access. IT groups can also create a log of all user actions, such as entering buildings or deactivating security systems, for later review if an incident occurs.
- **Standards:** Industry groups are establishing interoperability standards for physical security systems and IP networks, simplifying integration.

Campus Safety Enhancements Made Possible by the Campus Network

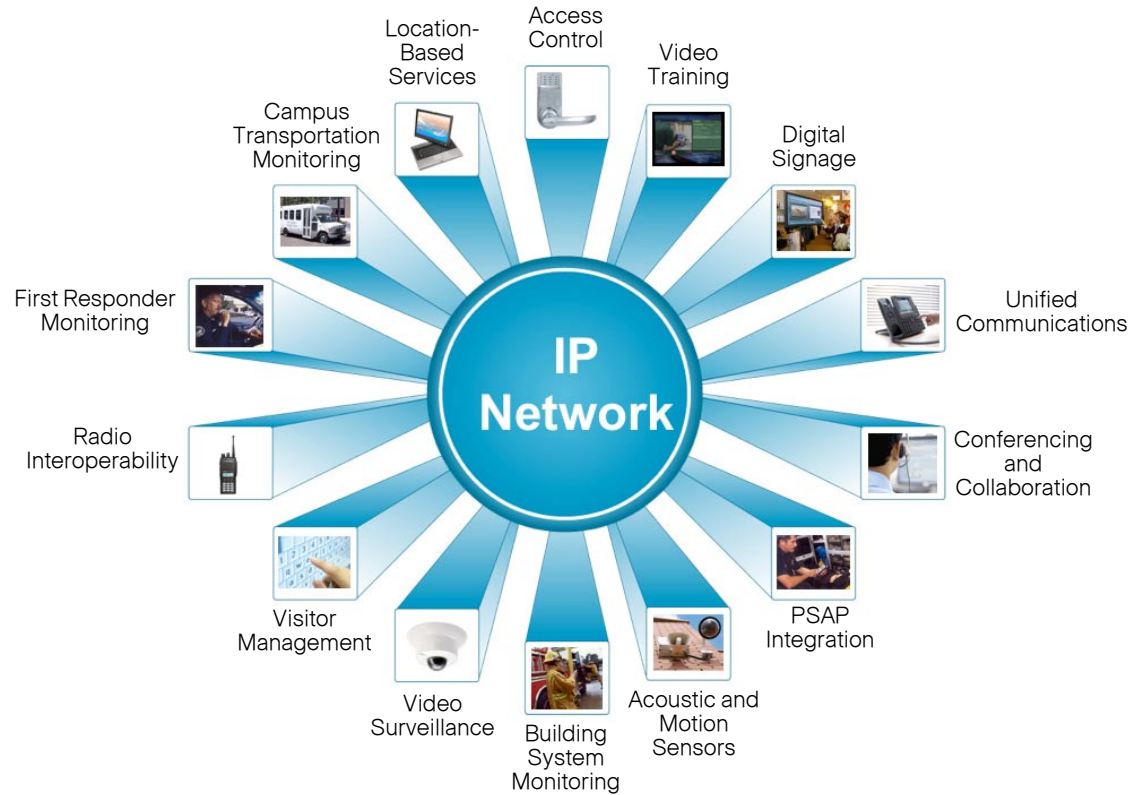
By connecting existing campus safety systems and communications systems to the IP network, colleges and universities can automate notification and response to reduce the time to respond effectively to safety events. For example, in the event of the dorm lock down described earlier, the response is faster:

1. Local police notify the university.
2. An administrator or campus police officer clicks a few buttons to activate a predefined policy to automatically send a voicemail and text message to resident advisors and students. The text message contains a link to a Webpage with more information and a phone number for students and parents with questions.
3. A message regarding the situation is displayed on digital signs across campus.
4. The campus security department remotely locks down the buildings using network-connected access controls, and unlocks them when the alert situation is over.

If the situation had involved a toxic leak and the fire department needed to evacuate dorms or nearby neighborhoods, the central dispatch could send a reverse 911 notification to the people affected, provide detailed evacuation information to the local police department, and notify schools within the evacuation area.

Following are some of the other ways that the convergence of physical safety systems and IP networks is enhancing campus safety. Colleges and universities can adopt these applications in any combination and order (Figure 2).

Figure 2 Campus Safety Services that Take Advantage of the Network



Video Surveillance

Use of video surveillance cameras helps campus security personnel deter, detect, and respond to safety incidents. Connecting surveillance cameras to the existing IP network avoids the cost of installing and maintaining a separate video network. It also gives the campus the flexibility to deploy cameras in any campus location with a wired or wireless network connection, with no incremental cost other than for the camera. Campus police, local police, and campus administrators can monitor the video from any Web browser, even from home. Grant Joint Union School High School District in Sacramento, California, deployed Cisco® Video Surveillance Manager to reduce break-ins and vandalism and prevent safety and liability issues (such as children entering the swimming pool area after school hours). District personnel can now use any Web browser to simultaneously view live video and high-quality images from all 13 high school and junior high campuses and parking lots as well as other facilities.

Higher-education institutions can also use IP-connected video surveillance cameras with video analytics software that can recognize suspicious activity, such as the presence of a person in a prohibited area. When an event is detected, the system automatically triggers the appropriate response based on campus policy, such as sounding an alarm or notifying administrators, campus police, or local police.

Cisco Unified Communications Systems and Alerting

Cisco Unified IP phones in classrooms and offices provide one-touch access to security and emergency services. Moraine Valley Community College in Palos Hills, Illinois, uses CiscoEmergency Responder to identify the exact location of people who call 911 from campus. The college also uses a solution from Cisco partner SchoolMessenger to alert staff and students within minutes of an incident and also to support daily administrative needs. Brandeis University in Waltham, Massachusetts, and East Carolina University in Greenville, North Carolina, use InformaCast software from Cisco partner Berbee to send pages to the entire campus or selected areas through the built-in speakers of Cisco Unified IP phones and other speakers across campus. The University of West Virginia in Morgantown, West Virginia, uses CiscoUnified Communications Manager to comply with Homeland Security requirements by recording all call detail information, including their origin and duration. At Cristo Rey Jesuit High School in Minneapolis, Minnesota, teachers press one button on their classroom Cisco Unified IP phone to summon security personnel. Soon the same button will also initiate streaming of video from in-classroom video cameras to the security department, providing the situational awareness needed to plan an appropriate response.

Conferencing and Collaboration

Conferencing and collaboration solutions from Cisco enable campus administrators, safety personnel, and other decision-making parties to collaborate with voice, video, and Web to share disaster recovery plans, maps, URLs, and more. For example, the Broward County School District in Florida uses its CiscoUnified MeetingPlace server to coordinate command, control, and recovery efforts after hurricanes and other disasters. During the 2004 hurricane season, the school district made the Cisco Unified MeetingPlace system available to the National Guard and Florida State Emergency Operations Center.

Communications Interoperability

Today, campus organizations that use different types of radio systems cannot communicate directly with each other or with local public safety agencies. Communicating through a dispatcher takes time and does not scale well for disaster situations. Cisco IP Interoperability and Collaboration System (IPICS) enables communications interoperability among different organizations and agencies using various push-to-talk radio devices, IP phones, and PCs or laptops using Cisco software. Operations personnel can click a button to activate pre-defined notification policies and talk groups for different types of events, such as weather-related emergencies or dangerous campus visitors. Bryant University in Smithfield, Rhode Island is using Cisco IPICS to facilitate collaboration between its safety, campus management, and residence-life departments as well as local public safety agencies. Another university uses Cisco IPICS to make it easier for campus police to communicate with local first responders and each other. Dispatchers previously had to use dozens of different interfaces, including radio, telephone, and different databases. With Cisco IPICS, they can access many of the tools from a single interface, simplifying training and improving response times.

Public Safety Answering Points

During critical events, public safety answering points (PSAPs) become the central point of command and control. And yet many campuses either do not have a PSAP or have one with limited capability. For example, traditional public branch exchange (PBX) systems can quickly become overwhelmed by high call volume so that callers receive busy signals. Cisco Unified Communications solutions, which connect to the campus IP network instead of the public switched telephone network (PSTN), scale easily to handle higher call volumes. They also enable campus organizations to communicate about the emergency using video, maps, floor plans, and databases in addition to voice. Safety personnel gain a common operating picture and greater situational awareness, which helps them plan a more effective response.

Desktop Video Training

Campus safety organizations can use their IP network to deliver video-based training for students, faculty, and staff about campus safety plans, safety resources, responses, chemical or OSHA regulations, and more. Cisco Digital Media Manager makes it easy for safety personnel without a technology background to create, publish, and distribute videos.

Digital Signage

By connecting digital signage to the IP network in high-traffic areas, campus police or administrators can efficiently disseminate text, images, and video information about campus safety events to students, faculty, and staff. Digital signage at the entrance to parking areas, for example, can warn students not to enter certain areas of campus. Safety personnel create and distribute the safety information using Cisco Digital Media Manager, the same easy-to-use software used for desktop video training.

Location Services

With an indoor or outdoor Cisco wireless network, campus police, facilities, and other departments can pinpoint the location of wireless laptops and smartphones as well as lab equipment and other moveable assets equipped with radio frequency ID (RFID) tags. The same solution can track visitors who are given RFID badges, alerting appropriate personnel when equipment or visitors exit a designated area. Location services help to reduce equipment loss and improve inventory management.

Campus Transportation Monitoring

By using sensors to transmit information from campus shuttles and buses, campus transportation groups can monitor vehicles' location and status and view and record video monitoring feeds. If the system detects the opening of an emergency exit or excessive speed, for example, it can be programmed to automatically send an alert to campus or local police.

Visitor Management Systems

Today, signing in campus visitors is a manual process. A staff member asks visitors to sign a paper log and then issues the visitor an ID badge. Network-based visitor-tracking systems automatically capture an image of visitors and their identification, making it unnecessary for a staff person to always be at the desk. These systems can also check the visitor's name against databases of wanted persons and flagged lists created by campus safety, and more. When integrated with Cisco Unified Communications solutions, visitor-tracking systems enable visitors to click a button on an IP phone to request an escort to designated areas such as dormitories or access the information desk.

Access Control

IP-based access controls integrate with door and window locks so that the safety organization can monitor and remotely control who enters and exits buildings, dormitories, libraries, and other campus areas. The ability to remotely monitor building entry reduces personnel requirements, enables personnel to remotely lock down area to isolate a safety incident, and can reduce unauthorized access to campus buildings. The system also produces accurate logs for incident reporting.

Building System Monitoring

By integrating building-system monitoring with the network, facilities personnel can remotely monitor alarms, climate control, and other building systems, enabling earlier incident detection. Response is faster when the system is set up to automatically notify nearby maintenance personnel. Connecting building systems to the IP network also reduces costs by eliminating the need for separate wiring systems.

Acoustic and Motion Sensors

When acoustic and motion sensors are connected to the network, campus police or facilities can monitor them centrally, from any location with a network connection. In addition, the IT department can work with campus security to set up policy-based actions. Examples include automatically responding to a motion sensor in an off-limits area by notifying appropriate personnel or cueing a video surveillance camera to begin transmitting video of the area back to the command center.

Benefits Summary: Converged Safety Systems and Information Technology

Table 2 summarizes the improvements to campus safety when communications systems, building systems, and access controls can work together over the IP network.

Table 2 Enhancements to Campus Safety from the IP Network

	When Safety Systems Operate on Their Own Networks	When Safety Systems Are Converged on the IP Network
Notifications and actions	Serially, prolonging response	In parallel, accelerating response
Relationship between communications systems and decision-support systems	Disconnected: a human needs to first notice unusual situation and then manually contact the appropriate personnel	Connected: monitoring and communications systems can work with each other to trigger policy-based responses
Amount of human intervention required	Higher	Lower

Network Security: A New Part of Campus Safety

Newer physical security solutions are connected to the IT infrastructure, making it important for campuses to protect the network from attacks, infection, and unauthorized access. Advanced IP networks have the security features to provide this assurance by:

- Authenticating users and giving them appropriate access based on their role
- Monitoring and even stopping application behavior that appears suspicious
- Automatically responding to specified network events according to policy

Policy-based controls give campus security groups the flexibility to respond immediately and appropriately to suspicious behavior. For example, if someone trying to enter a building swipes an access card three times without success, the system can automatically page campus security and dispatch them to the building.

Why Cisco?

Colleges and universities around the world are choosing Cisco solutions for enhanced campus safety because Cisco:

- Provides a unified voice, video, and data network that serves as a solid foundation for advanced safety services
- Enables educational institutions to get more from their existing network investment by adopting advanced physical safety services and tools for collaboration
- Designs safety solutions for education that take advantage of network security features for authenticating and segmenting users, monitoring rogue behavior, and implementing policy-based responses

- Continually invests in physical safety and security technologies that fit smoothly into the Cisco network architecture as plug-in services
- Collaborates with other technology providers to provide additional capabilities to meet customer requirements for a comprehensive, converged network solution
- Has extensive expertise with IP and physical security convergence. Cisco's own network has more than 2700 analog cameras and 6500 badge readers deployed across more than 400 global locations, all monitored from a central location
- Has an open architecture that supports existing safety system investments and provides a path to the future. Cisco systems evolve and scale as new safety technologies emerge

Conclusion

The convergence of campus safety systems and campus IT groups is helping higher-education institutions better protect students, faculty, and staff and collaborate with local safety agencies. Deploying IP-based systems for communications, building systems, and access controls helps to:

- Provide more capabilities for preventing, deterring, detecting, and responding to incidents
- Improve response times for campus security and first responders
- Accelerate notification of students, faculty, staff, and the surrounding community during safety incidents
- Improve operational efficiency of existing physical security systems and resources
- Reduce network and personnel costs

For More Information

Visit: www.cisco.com/go/campussafety



Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Europe Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: +31 0 800 020 0791
Fax: +31 0 20 357 1100

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

CCVP, the Cisco logo, and Welcome to the Human Network are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, Catalyst, CCDA, CCDP, CCIE, CCIIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, IQ Expertise, the IQ logo, IQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0711R)