What are Cyber-Physical Security Systems?

A CoSN Member Resource
October 2018

In the wake of school shootings, bullying, natural disasters, and other threats, districts are increasingly turning toward technological systems to enhance the safety of their campuses. These technological systems, know as Cyber-Physical Security Systems (CPSS), bridge the physical and the digital environments. CPSS equipment can range from entryway cameras, automatic locks, and intercoms to facial recognition software and biometric readers. These systems can be integrated to form an advanced security platform capable of automatic threat detection and facility lock-down; remote video observation through web-enabled camera systems; and enhanced communication with district personnel, students, community, and first responders. The impact of these technologies on physical facilities, network infrastructure, and district procedures and policies and must be considered as part of a larger, holistic school security approach.

Cyber-Physical Security Systems Equipment

There are many tools, products, and resources used by school districts in support of CPSS. Combining CPSS with well-considered policies and procedures can help create comprehensive security solutions. However, state and local laws may restrict the use of some security technologies; door barriers, for example, may not comply with local fire codes, or facial recognition software might conflict with state privacy laws.

Access Control is the selective restriction of access to places or other resources. Access control can be accomplished by using a human resource (such as a security guard), mechanical means (such as locks and gates) or a technological solution (such as swiping an ID card). Examples of access control solutions include:

- **Locks, Gates, and Vestibules.** Experts recommend that schools campuses be closed during the school day with only one entrance point. Office personnel may clear outsiders to enter through a secure vestibule, which may be built of bullet-proof glass or enhanced with a shatter-proofing film.
- **Metal Detectors.** Some schools use metal detectors to prevent students, staff, or visitors from bringing guns or other weapons onto the school campus.
- **Door Barriers.** These retrofit security devices turn the classroom door into a barricade to help prevent an attacker from gaining access. Although effective, these products may conflict with local fire codes.
- **Entry Cards.** Entry cards can be used with or without embedded technology. ID cards provide a visual indication of whether or not an individual is authorized to be on a school campus. Some school systems issue ID cards to students, faculty and staff. Visitors may receive guest badges or adhesive stickers. Smart ID cards include a chip that can be used together with a reader to identify student locations during an emergency or allow school staff to unlock doors. Biometric readers such as fingerprint scanners can be used for the same purposes.
- **Access Software.** Specialized software, often used in school offices or other campus entry points, can track visitor histories, print temporary badges, and check databases for registered sex offenders. **Facial Recognition software** can be used to prevent unapproved individuals from entering a building, match visitors against criminal databases, or help ensure that students board the correct bus. However, this software is in its infancy and concerns have been raised about accuracy and student privacy. Along the same lines, object recognition technology can be used to identify weapons or other prohibited objects. **Central Lockdown Capability** consists of integrated security systems that can automatically trigger a school lockdown when a panic button is activated, an alarm goes off, or a gunshot is detected.

Surveillance. Video cameras can deter crime, identify campus visitors, and provide real-time information during an active threat situation. Passive Monitoring refers to recorded data that is analyzed at a later time, usually as part of an event investigation. Active Monitoring involves personnel watching a live video feed. Some districts have agreements with law enforcement to provide real-time video feed access during a security incident.

Communications Equipment and Platforms. Wired and wireless communication technologies, such as intercom systems, local alarm annunciators, phone systems, and two-way radios are used by school officials and emergency personnel during emergencies. Enhanced 911 (E911) and other location based communications identify the location from which calls or messages are sent. Attendance and Check-In Apps can be used to track student presence on campus and allow school staff to account for students during an emergency incident.

Sensors and Alarms can be used to notify personnel on and off campus that an emergency is taking place. Mapping and verification solutions can help personnel the exact location of the emergency and provide audio and/or video input officials determine the nature of the threat.

- **Duress Alarms (panic buttons)** are wired or wireless devices that can be used to notify school officials and emergency personnel about an emergency. Some devices also transmit the sender's identity in addition to location. **Door and Window Sensors** can send alerts or trigger alarms when doors and windows have been breached. **Gunshot Detectors** can identify the location and caliber of a gunshot. They can be integrated with comprehensive security systems which can alert authorities, point cameras at the impacted area, and lock doors.
- **Robots** that integrate a number of security features, including facial and object recognition and streaming video, can serve as the eyes and ears for emergency responders.
- **Lighting** should be considered to provide safe passage in an emergency and improve overall campus security. In addition to highlighting emergency exit routes, lighting can be used for communications, such as allowing law enforcement to identify locations that have been cleared during a security incident.

Fogging and Pepper Spray Systems create a smokescreen or deploy chemical aversives and are often put in vestibules. However, these run the risk of hampering responder operations and can be compromised or misused.

Cyber-Physical Security Systems equipment can play an important role in enhancing the security of school campuses. However, they must not be deployed in isolation. CPSS technologies are only as effective as the overall security plans, processes and procedures they support. CPSS should be implemented as part of a larger, coordinated school safety strategy that takes into account the impact on school networks, IT staff, security personnel, students, faculty, and staff.

For more detailed information on school emergency planning, see the U.S. Department of Education's Readiness and Emergency Management for Schools (REMS) Technical Assistance Website.

CyberSecurity
for the digital district • a CoSN leadership initiative

CoSN is grateful to the following sponsors for their support of the Cybersecurity Initiative:
CDW G . Cisco . ENA . Fortinet . iboss . Microsoft

CoSN
LEADING EDUCATION INNOVATION