Applied Coursework

Technology for Homeland Security Course Paper

Author:
Ash Chatterjee
Cohort 0701/0702

Lead Instructor:
Richard Bergin

“The Nation’s Homeland Security Educator”
Learn more about the CHDS Master’s Degree Program:
Website: www.chds.us
Email: chdsmaap@nps.edu
Phone: 831-656-3829
Background  Closed Circuit Television (CCTV)\textsuperscript{1} systems are increasingly used for perimeter protection of large facilities, for monitoring critical/ sensitive areas, retail shops, banks, government establishments and for a range of applications too numerous to list. It is important to note however, that CCTVs are most effective for intercepting an intruder or terrorist, when used as part of an automated security management system, rather than when used in isolation. For example, CCTVs may be used as part of a system along with intrusion detectors, barriers, access control measures, alarms, archiving and event retrieval systems, along with non-technological operational security measures carried out by trained security personnel. A systems approach is preferred because each measure has its limitations when it comes to intercepting a terrorist. Complex, multi-camera CCTV systems can carry out image processing, object recognition and scene analysis. The output from the system is presented in an integrated display at the Operations Control Center (SCC/ OCC) on large monitors to assist the watchstander. The starting point for any CCTV system however is the camera. The camera creates the picture that will be transmitted to the OCC.

This research paper seeks to achieve a better understanding of the application of CCTV systems, and their underlying technologies. This would be helpful for security practitioners in government, and owners of infrastructure, for understanding and making judicious investments in security technologies, CCTVs in this instance. DHS’s role in helping to develop and implement security technologies, and the underlying plans and directives are described below, with reference to the transportation sector.

\textsuperscript{1} As its name implies Closed Circuit Television circuits are closed, unlike broadcast television where any receiver that is correctly tuned can pick up the signal from the airwaves.
HSPD-7 for Critical Infrastructure Identification, Prioritization, and Protection [1] states that a Sector-Specific Agency is a federal agency responsible for critical infrastructure protection activities in a sector. Of the 17 infrastructure sectors, TSA is the Sector Specific Agency for the transportation sector. Most U.S. infrastructure is owned by the private sector; TSA assists them with their infrastructure protection efforts. The National Strategy for Homeland Security and HSPD-7 guided the development of the National Infrastructure Protection Plan (NIPP) [4]. The NIPP, in turn, guided the development of TSA’s Transportation Systems Sector Security Plan (TSSP) [5]. The Plans describe the process for developing and implementing protective security measures, for which technology and R&D are key enablers.

In the technology area, DHS/ Science and Technology Directorate (S&T) carries out near and long term research for all areas of homeland security on behalf of other DHS agencies, such as TSA, each of whom have different technology needs depending on their sector of responsibility. TSA establishes the technology needs for securing the transportation sector, and S&T conducts the necessary R&D, using the national laboratories. TSA also provides the coordination between the private sector who use the technology, and DHS/ S&T. Occasionally S&T and TSA conduct trials for screening technology with the private sector to test and evaluate how well the technologies can be integrated with operations, and the ability of technological products to withstand the rigors of the operating environment (dust, vibration, heat and other ambient conditions). TSA’s prior R&D expertise lay in developing screening technologies for the Aviation mode, and the expertise resided in its Transportation Security Laboratory in Atlantic City, NJ. The laboratory has since been transferred to S&T under a re-organization.

An understanding of technology by government agencies is necessary for it to fulfill its technology-related responsibilities, which include:

- Developing and implementing R&D policies and plans.
• Developing voluntary security standards and guidance, both for protection and response. Standards/ guidance may be developed for process, operations, or be technical in nature. Examples are guidelines developed by TSA for airport planning, design and construction [2], and the RTCA standards for airport security and access control systems [3]. These contain standards/ guidelines for CCTV systems. TSA also works with other organizations to develop security standards.

• TSA, with DHS/ Grants & Training, and the Department of Transportation (DOT), provide infrastructure protection grants to industry, for surface transportation security. There are several areas for which grants are provided, the implementation of security technologies being one.

• TSA’s surface transportation inspectors provide assistance to transit agencies to improve their security plans and practices, including technology applications. TSA’s shares smart practices or new technologies among transit agencies.

Multiple Benefits of CCTV

CCTV applications are too numerous to list. It is widely used to protect against terrorism, enhance public safety, control crime and anti-social behavior in public places, and enforce traffic regulations. CCTVs with intelligence can detect speeding cars, and locate and read their tag numbers. CCTV recordings have primarily been used for conducting investigations after terrorism, crime or safety incidents have taken place. Sophisticated recording, playback and search capabilities provide audit capability and present evidence in legal proceedings. Recorded images can be enhanced offline to make it easier to identify criminals involved in a crime. For example, recordings from CCTVs enabled investigators to quickly identify the suicide bombers who attacked the London Underground in 2005. Modern cameras are smaller in size making them unobtrusive to criminals and terrorists, along with visible dummy cameras placed for
deterrence. CCTVs have gained popularity in security in airports, mass transit and rail, ports, chemical and nuclear plants, water purification plants, fuel storage plants, food processing plants, and dams.

**Implementation Issues**

Privacy is an implementation issue for CCTVs, although they are now being increasingly socially accepted in a post 9/11 world. CCTVs are now commonly used at airports, subway stations and shopping areas (to control shoplifting). Random searches of carry-on bags, and testing carry-ons using portable explosives trace detectors are being used in several subway stations in the U.S., particularly during high threat periods and during nationally significant events or political conventions. Initially there was pushback from civil liberties groups that these may be violations of privacy; however these are gradually being accepted by the public. The posting of signage warning the public that they may be subject to search, as well as the process of random selection has helped alleviate privacy concerns. Accuracy of the detectors and minimization of false alarms is another key factor that has helped gain public acceptance.

Issues regarding chain of custody and evidence preservation need to be addressed. When video recordings are used as evidence in court proceedings, it is necessary to ensure the feasibility of an independent and authenticated audit [9]. Use of efficient image compression methods to reduce data transmission and storage needs, may be questioned before being admitted as evidence [9].

Where videos are transmitted over the internet, they need to be protected from cyber attacks, and password protected for access by authorized levels of security personnel. Perhaps what is most important is that the internet itself may not function, similar to the overload of cell phone circuits, during a 9/11 like emergency. This would require a back up system, such as fiber optic transmission lines.
Defining System Requirements The first step in installing a CCTV system is to develop system requirements, which depend on site specific characteristics, and the capabilities desired. An important consideration is whether or not the system will integrate with an access control system.

A site survey should be conducted to define the design and operational requirements for a system. Functional requirements include determining the areas requiring surveillance (perimeters, parking lots, approaches to buildings, ingress/ egress points, waterfront access areas). A vulnerability assessment of the facility may be used as a guide for determining areas requiring coverage, as well as locations containing high value materials and classified information. For example, the vast expanse of railroad tracks is not monitored, but CCTV cameras are set up in strategic locations, such as bridges, tunnel entrances, and inside passenger stations. Types of cameras employed in rail typically include visible light, Infra red (IR) and thermal imaging with overlapping coverage. Thermal imaging cameras require a temperature difference of at least $\frac{1}{2}$ degree F to produce the necessary contrast in an image. Generally the cameras are remotely operated and monitored with local or rail police responding to incidents. CCTVs at airports are used for three major tasks: perimeter surveillance, exterior and interior surveillance of the terminal and its critical areas. It is used as part of a layered intrusion detection system. Long range, exterior monitoring CCTV systems use thermal imaging cameras and day/ night 360 degree Pan, Tilt, Zoom (PTZ) cameras, to provide coverage of the perimeter, access roads and flight lines. The cameras assist in detecting intrusions by providing a video record to assess and document alarms from other intrusion detection systems, and to assist in response. They cannot recognize the identity of an intruder.
The intermediate layer of the CCTV system monitors the parking areas, the exterior of the terminal building and flight line access ways. Inside the terminal, passenger areas and loading gate areas are monitored by CCTV.

**Operational Considerations** Operation in actual weather and ambient conditions should be tested. The range of detection should be specified and tested. Cameras can be more robust than some types of other intrusion detector sensors in locations where passenger and freight rail operate because of ambient noise, vibration, and dust that can adversely affect sensor performance. Light levels, natural and artificial, affect camera selection. For example, cameras at exterior locations require automatic aperture adjustments, while internal cameras require backlight adjustment.

**Scalability** In the fast evolving field of technology, it is easy for a CCTV installation to become technologically obsolete; consequently a flexible architecture is needed for the system to be compatible with other system security developments mass transit systems are planning to address future threats. This addresses the need to accommodate additional cameras, software or increased memory and recording capabilities. Budget limitations often require capital projects to be implemented in stages; therefore technology upgrades may be planned in stages.

**Cost** Life cycle costs should be used in cost estimates when acquiring new CCTV systems, including maintenance and personnel costs. The cost of re-design and temperature control of the expanded Central Monitoring Station should be considered at the outset. The cost of initial and continuing personnel training should be included.

**Reliability & Maintainability** Since reliability of new systems is hard to estimate, it is useful to run trial programs on site, bench test or confer with managers of facilities with advanced systems. The degree to which the system can be operated and maintained without continued vendor support should be considered.
Advanced CCTV Technologies

Newer CCTVs are built with digital components. Since any information can be reduced to digital bits, digitized CCTV systems can be integrated with other information handling systems. CCTVs can be blended into a facility’s intrusion detection access control and other systems, so that information from all devices can be displayed to security personnel on the same screens, images and maps. Multi-media presentations can be prepared that merge video with radar, sonar, intrusion detection alarms, satellite mapping, and imaging to create integrated visual situation images. [6]. CCTV built to IP standards can transmit via the internet. Wireless and satellite telephony and miniaturized, portable communicators allow security personnel to monitor CCTV systems from anywhere in the world. Receiving video from a camera to a cell phone is currently possible if the phone can connect to the internet, but live video over cellular devices is likely soon. Today cellular phones include PDAs, cameras, access to the internet, and color screens [6].

Video Motion Detection (VMD)/Automated Video Surveillance (AVS)

Multiplexer systems (see figure below) can alarm the security monitoring station whenever it detects movement in its field of vision. A multiplexer can receive an analog signal and then digitize it, and often contains embedded software that can perform analytical tasks on a video signal, such as video motion detection [6]. Before transmitting the video data to other components it can convert the signal back to analog for display or recording.

Since personnel cannot attentively monitor a large number of video screens, the monitoring process has been automated. Basic VMD products allow security personnel to set up grid lines on the image, so that the software will alert them to movement across the lines. Personnel could then switch to the appropriate monitor or video feed. Earlier products would generate nuisance alarms from normal movements (wind, birds, bugs). Software has since been
developed to learn what was normal about a scene, distinguish between human, mechanized, animal, insect and bird movement. The software can also detect movement in designated directions, distinguish between normal and aberrant passenger flow patterns, and provide other movement-related capabilities. While motion detection was the first step, software now can identify loitering, detect objects left behind or removed from a scene. These intelligent features have high potential for use in high density passenger flow applications such as mass transit rail stations and airports.

Software can also track moving objects and hand over tracked objects from one camera to another. Cameras increasingly incorporate analysis capabilities, leaving the more demanding analytical tasks to the main server. Single function products can detect and read license plates, and are suitable in areas of controlled environments and routine activities, such as highway toll booths. Some products can work with GPS systems to direct response teams more accurately. CCTVs are increasingly capable of blending input from various types of cameras and other sensors.

**The National Capital Region Rail Pilot Project** is an application of advanced CCTV technology [7]. It involves installation of a seven mile remotely viewable video buffer zone surveillance system along the railroad owned by CSX freight rail company, in Washington DC. The design includes state-of-the-art surveillance, chemical detection and processing equipment, and radiation monitoring to test the concept of detecting levels above background from trains traveling at speeds up to 15 mph. It will include the following:

**Virtual Fence** – 200 fixed cameras and 30 pan/tilt/zoom (PTZ) high resolution, color, day/night cameras and 65 RFID active scanners covering the seven mile stretch of CSX railroad extending north from the intersection of the George Washington Parkway and route 233 to the northern shore of the Anacostia Bridge. The cameras will completely cover the buffer zone and
use video as a tool for detection and identification of unauthorized personnel and interlopers in concert with the Friend or Foe Detection System (FFDS). Fixed cameras will be installed at 750 foot intervals, and the PTZ cameras will be installed in 1,500 foot intervals. High intensity lights will provide proper lighting. The system uses Duos Technologies rvspro™ digital video recorders and Praesidium™ intelligent video software [7].

**Virtual Gates** – Two virtual gates will serve as advanced checkpoints for inbound rail traffic and include (a) train presence sensors, (b) high resolution, PTZ cameras, (c) chemical sensors, (d) radiation detection devices and a dedicated rvspro™ to control live streaming video and I/O data [7].

**Command and Control** – All data (live streaming video, alarms, sensor detections will be processed in dedicated 16 X 20 head end. The data will be delivered to a state-of-the-art Command and Control (C&C) center via secure internet circuits to the CSX Police at their headquarters in Jacksonville, Fl as well as multiple government agencies. The system is unmanned until alarm notification is automatically transmitted and an instantaneous email notification arrives to police and operators. The C&C will have three 40 inch LCD monitors, three dedicated operator PC (intel P4 processor) work stations [7].

The architecture of an intelligent CCTV video system is shown in the Figure below.
Video Server: The server is a remote, programmable digital video recorder, multiplexer, and transmission sever in one. The server can be accessed from virtually anywhere using industry standard TCP/IP protocol, and can be interfaced with local and wide area network nodes, PDA’s and most TCP/IP devices. Video can be sent and cameras controlled from the server across wireless networks and via the internet. Intelligent software is integrated into the server to provide defined automated intelligent video capabilities (detecting moving objects, objects left behind or removed from a scene, loitering activity etc) [8]. The server includes features such as:

- **Alarm/Alert**: Alarms from motion detection or rule based alerts will alert a designated remote camera and transmit live video from the alarmed camera.

- Motion detection can be configured independently for each camera.
- Provides online remote viewing of live video with password control, security features and user management.

- **Playback features:** Allows remote playback of recorded video. Intelligent search functions for recorded video. Maintains a history log of alarmed events.

- Software allowing control of PTZ cameras.

**Geo-spatial visualization:** Large scale installations include a graphic representation of the security zones, presented in an interactive, browser-based electronic map. The intelligent software can be combined with additional intelligent mapping software that can visualize the type and location of a suspected security breach.

**Sensors:** Sensors, controls and logic can be added to provide early indication of fire in a rail tunnel. Temperature data and alarms can be integrated into the Graphic User Interface.

**Strategy for CCTV applications in Mass Transit & limitations**

The use of CCTVs gained popularity in mass transit security after the terrorist bombings of the London Underground in 2005. Although the cameras assisted investigators to identify the suicide bombers involved, they were not effective in preventing the bombing. The cameras could not detect the explosives that were hidden in the backpacks of the terrorists. While CCTV cameras are effective for intrusion detection at entrances of tunnels and remote areas where human presence would be suspicious or unusual, it is a greater challenge to detect a terrorist in a rush hour crowd entering a mass transit rail station. With a much greater and rapid throughput of passengers, mass transit presents a greater challenge compared to the slower process of screening at airports where checkpoints allow the time needed for detection, and interdiction to take place. Cameras with sophisticated intelligence are required to detect a suspicious package or a person moving in a direction that would be suspicious, in time to prevent a terrorist from attacking.
Greater assurance of security may be obtained by using a strategy of layered defense, using several, orthogonal\(^2\) technologies combined with operational measures. Such a layered strategy is envisioned for future trials by TSA with a mass transit system. The goal to detect and prevent (interdict) an attack by a suicide bomber using Improvised Explosive Devices (IED) or IEDs in leave-behind packages, involving detection of explosives hidden under clothing or in a carry-on bag.

Detection of liquid (peroxide-based) explosives, and components of home-made explosives are harder to detect using cameras; consequently the use of combinations of (orthogonal) technologies, and operational means, constituting a layered defense, is more effective. The outermost layer around a metro/rail station should use the least invasive standoff technology that screen the largest number of passengers in the least time. CCTV with intelligent software may be useful for detecting suspicious passenger behaviour. Infra-red cameras may be used for night vision, as well as for detecting concealed weapons. CCTV cameras may also be used to monitor parking lots. During high DHS HSAS (Homeland Security Advisory Systems) alert conditions, truck/van mounted (mobile) Backscatter X-ray machines may be used to inspect parked cars, and passenger drop-off areas.

The middle layer can use standoff-capable, remote MilliMeter Wave (MMW) screening technology for detecting IEDs or weapons hidden under clothing or in carry-on bags, and alert security personnel using portable communication devices. CCTV cameras could use facial recognition software to identify a known terrorist, and alert security. However this would be a complex process requiring automated access to existing terrorist databases, and assumes that the suspect is included in an existing database. Plainclothes security personnel trained in suspicious

\(^2\) Orthogonal: Use of two or more detection methods based on independent technologies (principles) to reduce the probability of a false reading.
behavior detection would monitor incoming passengers for suspicious behavior. Suspect passengers may then be subject to secondary screening and questioning. The technology for automated detection of terrorist intent using CCTV camera systems is under development, and not mature for deployment [10].

The innermost security layer at the turnstiles may be protected by trace particle explosive detectors incorporated into ticket slots at turnstiles and ticket vending machines. Canine units are popularly used for explosives detection and deterrence. Canines are considered a useful and reliable supplement to technology, especially while intelligent CCTV software is still being refined and developed.

Terrorists are adaptable, and can defeat installed technologies, if they are not deployed as a combination of technologies providing greater flexibility and coverage for the security system as a whole. A layered defense would make it more difficult for a terrorist to break through all the protective layers in a single attempt. However layers of technological defense come with a high cost, and the combination of technologies should be optimized to ensure that the costs incurred are commensurate with the reduction in risk. This concept is addressed in infrastructure protection plans [5,6]

Intelligent software for use with CCTVs are developing rapidly, and more innovations in this field are forthcoming.

References


8. National Capital Region Rail Pilot project
   http://www.epsilonsystems.com/div_security_techNCRRPP.cfm
