CHAPTER 6

System Integration

6.1 Introduction

The seemingly disparate safety and security countermeasures identified in Chapter 5 may be incorporated into an integrated system. This approach uses a system methodology to improve tunnel safety and security.

6.2 System Safety and Security

System safety and security is the systematic application of engineering, technology, and management tools to identify, analyze, and control hazards and threats within operational, budget, and time constraints. It encompasses all of the integral factors that make up a tunnel system:

- People—tunnel operating and maintenance personnel, the public, emergency responders, and vendors.
- Operating procedures—routine operating procedures, emergency procedures due to a security or safety incident, and measures implemented due to a particular hazard or threat.
- Engineering and technology systems and controls—communication systems, ventilation systems, intrusion detectors, lighting, fencing, and so forth.
- Physical aspects of the tunnel structure.

Each of these elements, independently, provides some degree of safety and security. However, when combined, they significantly improve safety and security. Tunnel operation and maintenance personnel, for example, can be trained to recognize and report suspicious behavior in and around a transportation tunnel. Fences and barriers define areas where unauthorized personnel are not permitted. Lighting aids in the observation of activity. When these disparate systems are integrated, the likelihood of deterring and detecting a security incident is greatly increased. An effective safety and security system can be developed when one understands the interrelationships of these systems and integrates them so that they operate as a whole.

6.2.1 People

Tunnel Personnel

Training of tunnel operation and maintenance personnel is an important and integral component of ensuring tunnel safety and security. Tunnel personnel can be a key element to deterring, detecting, and responding to a safety or security incident. Tunnel personnel should be trained to recognize suspicious packages, activity, and behavior and to react accordingly. They must also be taught how to respond to an actual safety or security incident. In order to carry out these responsibilities, tunnel personnel must have a basic understanding of their role as the eyes and ears of tunnel operations and of their responsibility for safety and security. They should be trained to recognize things that are out of the ordinary and to identify suspicious actions that might constitute pre-attack activity. In particular, their instruction should include the difference between unattended packages and suspicious packages, as well as what constitutes a suspicious security event. When all unattended packages and unwarranted activity are deemed “suspicious,” unnecessary disruption of the tunnel system occurs. Tunnel personnel should also have a clear understanding of the proper procedures for reporting and responding to an event.

Specific technical training should be afforded to central control personnel or others who are responsible for activating emergency systems, such as ventilation and fire suppression systems (i.e., dry standpipes), or de-energizing traction power systems in rail transportation tunnels.

Lastly, tunnel personnel training should include coordination with the many agencies and departments that may be necessary during the management of a tunnel security incident, such as police, fire and rescue departments, emergency medical services, and other forms of technical assistance. This training should include the following:

- An overview of the incident command system (ICS),
- Coordination with emergency responders, and
- Evacuation protocols.

Emergency Responders

Tunnels can be viewed as inherently hazardous. Vehicular and train traffic, traction power in rail tunnels, and the confined nature of the space all challenge and impact emergency response capability. Tunnel operators should develop formal training programs for emergency responders. The training should consist of the following:

- Inherent hazards—vehicular traffic, rail traffic, and traction power (rail systems only).
- Right-of-way safety.
- Tunnel life safety systems—ventilation, fire detection, fire suppression and hydrants, points of egress, and rescue areas.
- Communication systems—capabilities and limitations and emergency telephone locations.
- Training aids—checklists, facility diagrams, and so forth.

The Public

The public can play an important role in reporting suspicious packages and activities. A public security awareness campaign can be designed to heighten the security awareness of the public. The public should be encouraged to be aware of their surroundings and to look for suspicious or unusual activity. The campaign should emphasize the following:

- What to look for,
- How to report the information and
- What tunnel emergency elements are available (exits, evacuation procedures, fire extinguisher locations, emergency telephone locations, and so forth).

The FTA's Transit Watch program is an example of a public security outreach program.

6.2.2 Operating Procedures

An effective response to any safety or security incident includes predetermined response procedures for both tunnel operators and emergency response personnel. The foundation for the procedures is an emergency plan that establishes the policies and guidelines for the procedures. The procedures are typically jointly developed by tunnel operation departments, tunnel safety/security departments, and emergency responders (including fire and police). These procedures serve as guidance during the response to a safety or security incident and include specific actions that are to take place by tunnel operation and maintenance personnel, central control staff, and other tunnel staff. The procedures should include the following:

- Reporting protocol;
- Facts to be collected and evaluated;
- Verification protocol;
- Protection of the scene;
- Limiting vehicular and train traffic;
- Right-of-way safety;
- Vehicle safety (transit, rail vehicles, and special vehicles);
- Removal and restoration of traction power;
- Activation of emergency systems, including ventilation and dry standpipe system;
- Assistance in rescue and evacuation operations;
- Deployment of roving patrols;
- Posting of guards;
- Hazardous materials restrictions;
- Background investigations of employees and vendors;
- Inspections of vehicles, cargo, and persons;
- Bomb-sniffing dogs;
- Credentialing; and
- Command protocol.

The cornerstone of the procedures is the sharing of information and responsibilities between emergency responders (fire, law enforcement, and emergency medical services) and the tunnel owners and operators. When designing programs to respond to safety and security incidents, understanding the activities to be performed is essential. These activities must take place in advance of developing specific response protocol.

An interorganizational memorandum of understanding or agreement (MOU or MOA) is the basis for acknowledging what resources each organization will provide during a response.

6.2.3 Engineering and Technological Systems and Controls

Engineering Systems and Controls

Fire protection, fire detection, ventilation systems, lighting, fencing, and barriers are among the engineering controls that support tunnel safety and security. These measures provide access control for deterring an attack, assist in the detection of intruders, and limit the damage potential of an incident due to fire or toxic gases and substances.

Technological Systems and Controls

Technology systems and controls encompass a wide range of measures, including, but not limited to, access control systems (identification card readers, intrusion detection systems, CCTV, communication systems, and C/B/R detectors). Each of the systems should be evaluated to determine what is suitable for the particular application. In order to make this determination, it will be necessary to know the operational aspects of the security system and how the security system will be used. Consequently, successful deployment of a technology requires the development of a needs assessment, desired performance characteristics, and training of staff to operate and maintain the technology. The technology will be based on the hazard or threat assessment. Study of the technologies currently available determines current capabilities.

Table 72 illustrates how the various countermeasures deter, detect, and respond to a hazard or threat.

6.2.4 Physical Aspects of the Tunnel Structure

Physical aspects of the tunnel structure include length, cross section, portal locations, cross-passage locations, and other points of access. Physical hardening of the tunnel structure minimizes the damage potential of a hazard or threat and helps to maintain the structural integrity. See Section 5.4 for more detailed information.

6.3 Security System Integration

Integrated security measures can deter a potential security incident by making it more difficult to execute, increase the likelihood of detection, minimize the damage potential of an incident, and aid in response and recovery efforts. As an example, the use of intrusion technology can assist in both the deterrence and detection of an intruder, thereby perhaps preventing a terrorist attack or simply the destruction or vandalism of property. Roving patrols and guards coupled with a detection system can be used to monitor unauthorized access into a tunnel and its associated facilities.

An integrated security system design must take into consideration the physical aspects of the operating environment, the performance capability of the systems, and the personnel requirements for operation and maintenance. As previously discussed, an integrated security system consists of

- People,
- Operating procedures,
- Engineering and technology systems and controls, and
- Physical aspects of the tunnel structure.

Table 72. How countermeasures deter, detect, and respond to hazards and threats.

Deterrence	Detection	Response
• Operational Tactics – Roving patrols – Bomb-sniffing dogs – Background checks of employees and contractors – Background checks of facility vendors – Access control – Credentialing and identification card system – Guards at entry points – Intelligence – Hazardous material restriction – Inspections • Technology – CCTV – Intrusion detectors – System integration • Engineering – Blast design – Elimination of hidden corners, alcoves, and shelves – Open, unimpeded lines of sight – Lighting – Locked facility doors	• Operational Tactics – Intelligence – Security awareness training of operating and maintenance personnel – Roving patrols – Guards at entry points – Bombing-sniffing dogs – Identification card system – Inspections • Technology – Intrusion detectors – Identification card readers – Chemical/biological/radiological detectors – Seismic/stress detectors – Mobile monitoring – Explosive detectors – System integration • Engineering – Fire detection	• Operational Tactics – Command and control (multi-tenant) – Evacuation protocol – Information sharing – Tunnel ventilation – Portable fire extinguishers • Technology – CCTV system – Communication – Chemical/biological/radiological monitoring – Explosive detectors – Interface with traffic monitoring – System integration • Engineering – Fire protection – Lighting – Ventilation

Before a system can be integrated, adequate resources should be allocated to planning, defining the system requirements, and implementing the design stages of the project. An assessment must be carried out to determine the capability of the existing system, the present requirements, and possible future requirements. Some of the major considerations are as follows:

- **System codes and standards—**Appropriate standards should be used to ensure that each of the systems is capable of being assembled into an integrated system. These standards should address system components, including communication protocols, communication interfaces, data dictionaries, and message sets.

  Designing to standards such as Synchronous Optical Network (SONET), Asynchronous Transfer Mode (ATM), and Ethernet allows operability between manufacturers. Future system requirements are always difficult to predict, and an upgrade path for computer and communication systems should always be available. For instance, in order to accommodate future upgrades as improved technology becomes available, one may specify standard rack-mounted and blade servers as well as a SONET platform, which is scaleable from OC 48 to OC 192 by upgrade of the optics. Other applicable standards are available from the Electronics Industries Association (EIA), the International Electrotechnical Commission (IEC), the American National Standards Institute (ANSI), the Institute of Electrical and Electronics Engineers (IEEE), and others.

  Individual code requirements should also be assessed. For example, integration of a fire alarm system must take into account the requirements of *NFPA 72: National Fire Alarm Code*, as well as the requirements of *UL Standard 827: Standard for Safety for Central-Station Alarm Services*.
- **Device compatibility—**A primary decision in the design phase is determining which interfaces need to communicate with each other and whether these interfaces are human or electronic. Interoperability of the security devices needs to be considered to ensure functional compatibility.

  An integrated system has many advantages, including a common operator interface for individual MEC systems, common alarms, and a real-time database. An integrated system offers the flexibility to view and control the individual systems from different locations and to export data to external agencies. However, integrating systems is expensive, especially for older systems. Therefore, before integration is undertaken, one should carefully evaluate the potential cost of integration as well as budget limitations.
- **Data communication—**Data communication must be considered when integrating different systems.

  A typical system upgrade might accommodate a planned increase in communication bandwidth and data requirements along with a phased migration of MEC systems to the integrated system. For instance, allowances might be made for the future integration of a new digital CCTV system.

  Assessment must be an ongoing exercise. For example, if voice-over IP (VoIP) communications are to be added to an Ethernet local area network (LAN), then an assessment should be made to determine if the response time of an emergency system on the same LAN is still acceptable.

  Traditional safety-related systems have well-defined safety boundaries that can be assessed for availability and integrity. When a system is integrated, the influence of other MEC systems can blur the safety boundaries and degrade the safety system. It is important to ensure that this does not happen. The damage potential of the integrated system failing should also be assessed for each case. As an example, a tunnel ventilation system does not usually have a default fail-safe running condition, and a supervisory command must be received to set the mode of operation (i.e., supply or exhaust) to properly drive the smoke and heat away from escaping passengers.
- **Integrated legacy systems—**When introducing new technologies into an existing system, compatibility must be considered. If possible, consideration should be given to introducing an interface rather than changing the existing architecture.

  When interfacing to a legacy (i.e., existing) communication system, the hardware interface is typically relatively straightforward. The more complicated issue tends to be the software. If a software driver is not available for the system writing, a new driver for the communication protocol can range from trivial to extremely difficult and expensive. It is very important for the owner or operator to give guidance on how to accurately specify this work so that a system integrator can assess the degree of difficulty before bidding the job. There are also costs associated with maintenance and support of the third-party communication software.

The following are typical steps for developing an integration strategy:

1. Identify proposed locations for the operational control center and backup secondary control center. Size requirements can be considered after the system assessment is carried out.
2. Establish a communication backbone, taking into consideration
   - Bandwidth requirements (this is covered in more detail below);
   - Technology choices (i.e., SONET, ATM, and Ethernet); and
   - Physical structure, redundancy, and diverse routing of fiber links.

3. For each individual system, identify performance criteria, functionality requirements, code requirements, and level of security (safety-critical, safety-related, and so forth). Also identify fall-back requirements.
4. Determine whether or not each individual system can be integrated. For example, the video channels to be taken back to the control center and the real-time performance requirements will determine the bandwidth of a CCTV system. It must be determined if this bandwidth can be accommodated on the communication backbone.
5. Determine the level of integration that can be achieved within the budget.
6. Assess the worst case (i.e., maximum) bandwidth that includes all possible commands necessary during an incident (equipment control, multiple alarms, traffic monitoring and control, frequent VoIP communications, and so forth).
7. Evaluate the computer architecture, including the following:
   - Client server,
   - Peer-to-peer architecture,
   - Redundancy issues,
   - Expansion capability,
   - Real-time performance, and
   - Database requirements.
8. Choose an off-the-shelf or custom-made supervisory control and data acquisition (SCADA) software design based on the desired performance level and budget.
9. For each system, determine system integration options, levels of interoperability, and whether migration paths can be achieved with the integrated system.
10. Conduct a phased replacement program of the obsolete systems.
11. Design the operations control center theater, including desks and the video wall.
12. Determine the power supply requirements, including the uninterrupted power supply with backup generators.
13. Ensure that devices are hardened or concealed to guard against tampering and vandalism. Network access and data communications should be secured by firewalls, password protection, encryption, and authentication.
14. Perform testing and simulation to ensure the functionality of the system.

6.4 Information Sharing

The aforementioned guidelines are particularly critical for transportation tunnels. Because it is not uncommon for transportation tunnels to cross municipal or governmental boundaries, these tunnels may have multiple users or tenants. Response to an emergency incident typically requires close coordination among the multiple users, including law enforcement, fire departments, and emergency medical services from the responding jurisdictions. The tunnel operating authority or agency has the primary responsibility for emergency management planning and initiation of an immediate response to incidents. However, a coordinated response among all entities involved is critical to minimizing the damage potential of the incident or event. It stands to reason that integration of tunnel systems, such as CCTV systems, is warranted. It is desirable to track suspects or events that move from one jurisdictional boundary to another within the tunnel environment. Without a coordinated and integrated system, such tracking is not possible.

Tunnel tenants and users should have emergency response plans for their respective operations that address emergency response coordination. The tunnel owners and operators must ensure that all stakeholders—including tenants; emergency response agencies at the local, state, and federal levels; and municipal or governmental jurisdictions, as appropriate—are actively involved in the development of an all-hazards emergency response plan that outlines roles and responsibilities, coordinates efforts, and integrates each tenant user.

6.5 Conclusions

System safety and security are the systematic application of engineering, technology, and management tools to identify, analyze, and control hazards and threats within operational, budget, and time constraints. Systems encompass all of the integral factors that make up a tunnel, including people, operating procedures, engineering and technology systems and controls, and the physical aspects of the tunnel structure. Each of these elements independently provides some degree of safety and security. However, when combined, they significantly improve safety and security.