CHAPTER 1

INTRODUCTION

Security is an expectation of surface transportation users. Tools like intelligent transportation systems (ITS), which provide services such as surveillance, control, communication, and information collection and dissemination in real time, can support safeguards against threats. This chapter introduces the concepts of security within the context of ITS, then concludes with a description of the anticipated audience and scope of this book.

1.1 CONCEPT OF SECURITY

The world is full of natural and man-made risks, often characterized in terms of their likelihood of occurrence and their subsequent impacts to both life and property. Natural events, such as floods, hurricanes, tornados, and earthquakes, as well as involuntary events, such as machine or system malfunctions, can be quantified in terms of probability of occurrence and severity of their impacts. Similarly, human-induced events, such as deliberate attacks or errors, can cause similarly devastating affects. These deliberate or unintentional acts also can be expressed in terms of risks of their occurring and possible impacts of these events once they occur. Table 1.1 shows similarities and dissimilarities between deliberate threats, such as terrorist attacks and natural disasters such as hurricanes.

The perception of security has far-reaching effects. A secure environment provides an atmosphere where innovations and economic growth flourishes. Even the perception of security can benefit society and improve social and economical fabrics of life through new investments.
Several factors contribute to the perception of security. One such factor is a possible in-place system that can identify threats before they occur. This forward-thinking concept is most desirable, but often it is the most difficult to accomplish. Therefore, having an appropriate response plan for any deliberate attack is also important for an overall security plan. This plan may include coordination between first responders, resource sharing, providing immediate care to those most affected, and evacuating those most at risk. Thus, security planning against deliberate threats encompasses different facets of tasks between multiple agencies involved in different activities, whose coordination is a must for identifying and managing any security threats.

Conversely, a security breach, resulting in either man-made or natural catastrophes, both impedes innovation and stifles economic creativity and the vitality of areas affected by such events. Within a very short time—in a matter of days, in fact—the sense of security shared in the public’s collective perception, which has evolved over a long period, is shattered. In addition to public loss of confidence in security measures, the loss of human life, injuries, and, the economic costs of a terrorist attack on any region are overwhelming. A study conducted by the RAND Corporation reported that the initial costs of a terrorist attack involving a nuclear event near the port of Long Beach, California, could exceed $1 trillion. (Meade and Molander 2006). These staggering costs, which would cause untold harm to the U.S. and global economies, would be driven by demands for a massive medical response to such a disaster, subsequent insurance claims, compensation for lost jobs, and economic devastation to the greater Los Angeles area, not to mention the overwhelming cost of evacuation and reconstruction, including radioactive cleanup. Table 1.2 shows the wide range of terrorist threats and their possible impacts on infrastructure and other targets.

### Table 1.1 Possible Similarities and Dissimilarities of Terrorist Attacks with Natural Disasters

<table>
<thead>
<tr>
<th>Similarities</th>
<th>Dissimilarities</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mass casualties</td>
<td>Caused by people on purpose</td>
</tr>
<tr>
<td>Damage to infrastructure</td>
<td>May target specific security vulnerabilities</td>
</tr>
<tr>
<td>Occur with or without warning</td>
<td>Affected areas will be treated as crime scenes</td>
</tr>
<tr>
<td>Evacuation or displacement of citizens</td>
<td>May not be immediately recognizable as terrorist events</td>
</tr>
<tr>
<td></td>
<td>May not be single events</td>
</tr>
<tr>
<td></td>
<td>Place responders at higher risk</td>
</tr>
<tr>
<td></td>
<td>May result in widespread contamination of critical equipment and facilities</td>
</tr>
<tr>
<td></td>
<td>May expand geometrically in scope</td>
</tr>
<tr>
<td></td>
<td>May cause strong public reaction</td>
</tr>
</tbody>
</table>

*Source: Parsons Brinckerhoff and Science Applications International Corporation, 2002.*
<table>
<thead>
<tr>
<th>Weapons of Mass Destruction</th>
<th>Possible Distinguishing Signs</th>
</tr>
</thead>
</table>
| Conventional explosives (detonation of military-type or commercial bombs, such as fuel oil–fertilizer, etc.) | - Explosions  
- Casualties  
- Various types of localized blast damage up to structural collapse  
- Exposure to dust and hazardous building materials (e.g., asbestos)  
- May be used to spread harmful radiological or chemical materials |
| Chemical (dispersion of pesticides, mustard gas, chlorine gas, cyanide, tear gas, etc.)      | - Initial unexplained deaths and illnesses  
- Effects mostly localized to release site but may be distributed farther by wind and contamination  
- Area may be marked by unusual clouds, haze, mist, odors, tastes, droplets, etc. |
| Biological (dispersion of viruses, bacteria, toxins, fungi, etc.)                          | - Initial unexplained deaths and illnesses, possibly beginning a day or more after an incident  
- Immediate effects mostly localized to release area, but distribution may be expanded through human transmittal  
- Possible persistence in environment  
- Possible geographic contamination |
| Radiological (dispersion of radioactive material by nonnuclear explosion or pressurized gas) | - Unexplained deaths and illnesses  
- Effects mostly localized to release but may be some distribution via wind and other means beyond release site  
- Persistence in environment  
- Geographic contamination  
- Conventional explosives used for dispersal may cause additional effects and explosions |
| Nuclear (nuclear detonation with radioactive fallout)                                      | - Large-scale infrastructure destruction  
- Extensive radioactive fallout  
- Long-term persistence in environment  
- Geographic contamination  
- Radioactive poisoning of foodstuffs, water sources, and long-term illnesses |
| Novel concepts (unusual delivery systems—aircraft, boats; combinations of weapons and attack modes; unexpected targets with secondary consequences) | - Unknown |

*Source: Parsons Brinckerhoff and Science Applications International Corporation, 2002.*
Table 1.3 outlines the major topics concerning infrastructure security and related issues. Although this table was developed for bridge and tunnel security by the Blue Ribbon Panel on Bridge and Tunnel Security, it can apply to other transportation infrastructure. The table provides important considerations for infrastructure security in six different phases: policy, planning, design and engineering, operations and management, information security, response, and recovery.

1.2 TRANSPORTATION AND SECURITY

Transportation has always been strongly tied to economic development and sustainability; and regional, national or international economies have come to depend increasingly on efficient and secure transportation systems. Transportation systems connect vital regional economic components (e.g., businesses and employee housing) to ensure that employees can use these systems to get to work while also ensuring that businesses can use them to provide and receive various supporting services and/or supplies. Nationally, the U.S. system of interstate roadways plays an indispensable role in economic vitality, connecting the goods of one region with the demands of another. Interstate travel also plays
a significant role in national defense; indeed, our system of interstate highways was built with just this purpose in mind. The overriding objective of the Eisenhower Interstate Highway System in the United States, begun in the 1950s, was the strategic, efficient, and quick movement of troops, weapons, and supplies in time of war. While successful in scope, it is interesting to note that the major benefit of the Interstate Highway System has been one of commerce rather than for the military, becoming the great enabler of moving goods and people efficiently via surface transportation.

Transport services are provided through air (including space), water, and surface vehicles. Airplanes and ships mainly accommodate air and water travel, respectively, whereas railroads, private automobiles, commercial trucks, and public transit comprise the surface transportation system. Many times these different transportation modes serve independent travels, and these modes often complement each other in serving overlapping travel requirements. For example, delivering cargo from Paris, France to Santa Fe, New Mexico, United States, necessitates that goods be freighted through a complex web of surface, water, and in some cases air travel to reach their destination. These transportation choices are not simply relegated to the movement and reception of cargo. Residents around Seattle, Washington, may use private automobiles, public transit, or ferry transportation to commute to work. Similar complementary services exist within modes; travelers in the Boston area may use either private automobile or the Massachusetts Bay Transit Authority light rail to reach their destinations.

There have been numerous terrorist attacks on such large-scale transportation systems. The September 11, 2001, terrorist attacks by means of the U.S. airline industry revealed the risks of the transportation system being used as a weapon. We realized that not just aircraft but surface transportation systems (trucks, containers, transit cars, barges) and the bridges and tunnels that facilitate their use could be weaponized (Kulash 2002). Critical transportation infrastructures, such as bridges, tunnels, and intermodal facilities, were seen to be particularly vulnerable to terrorist attacks. Other bombings—coordinated bombings in 2004 against the commuter train system of Madrid, Spain, which killed 191 people and wounded 2,050, and the July 7, 2005, bombings against London’s public transport system, in which 52 commuters were killed and 700 were injured—illustrate these vulnerabilities (U.S. Department of State 2004).

Since 2000, terrorist attacks on transportation systems worldwide have more than doubled as compared to the previous decade, with attacks being conducted against smaller targets and in smaller cities. (U.S. Department of State 2004). Security incidents can have an impact on the transportation system. For example, the September 11 terrorist attacks in the United States affected all modes of transportation for the entire region and the I-95 corridor and necessitated significant road repair. Threats near a transportation facility can result in closures or travel restrictions (Federal Highway Administration 2004). In the United States, the Federal Highway Administration (FHWA) is
supporting the development of new technologies and training programs to assist regional and state transportation agencies in upgrading operational tools and processes for providing enhanced security (Federal Highway Administration 2008). The focus of this effort related to ITS includes:

- Model emergency scenarios
- Integrate ITS with State Emergency Operations Centers,
- Implement voice and data interoperability between transportation and public safety agencies
- Train transportation agency personnel in Incident Command/Unified Command (ICS/UC). ICS/UC is a tool, jointly developed by stakeholder agencies called the National Response Team (NRT) to protect the public against threats from land, air and water by efficiently responding and managing emergency events. NRT includes stakeholder agencies such as U.S. Department of Commerce, U.S. Department of Defense, and U.S. Department of Transportation (NRT 2008).
- Apply ITS to support and improve homeland security efforts.

These efforts, along with state and local planning, are improving the future security landscape of the United States. Both developing and developed nations have initiated their own transportation security strategies.

In the United States, transportation security is an integral part of homeland security. In fact, transportation is listed as one of the 17 critical infrastructure sectors in the strategies for homeland security (Office of Homeland Security 2005). Because most of the European initiatives parallel efforts in the United States, many opportunities exist for international collaboration through communications and information sharing. This sharing is expected to result in efficient management of international security efforts to minimize security threats worldwide, which is an increasingly important task.

1.3 SECURITY IN THE ITS CONTEXT

This book focuses on the ability of intelligent transportation systems to improve security. ITS systems combine traffic engineering, computer technologies, and communications systems that complement and integrate these services provided by various agencies to improve traffic flow and safety in the surface transportation system (Chowdhury and Sadek 2003). The surface transportation system includes roads, bike paths and pedestrian corridors, mass transit systems, and railroads. Surface transportation infrastructure includes the fixed assets of the surface transportation system, such as highways and streets, train stations, public transit terminals, and bridges (U.S. General Accounting Office 2004). Although the concept of intelligent vehicle highway systems, which was later renamed ITS, was introduced in the 1980s, it has recently received much
attention and has proceeded through several evolutionary milestones. Today ITS is a recognized field of research in the transportation community that provides a viable means to help meet future transportation demands. The systems are also increasingly viewed as alternatives to additional road infrastructure construction to meet future travel demands. ITS applications primarily focus on the surface transportation infrastructure, but they also are applicable to air and water transportation systems (e.g., airports and seaports) that have the potential to be interdependent.

Through government-sponsored field evaluations in which ITS was shown to minimize crashes while reducing travel times, the collective transportation community has come to see the inherent value of such systems. Studies conducted by the U.S. Department of Transportation (DOT) determined that the deployment of ITS in major U.S. metropolitan areas resulted in considerable savings in travel time, an increase in safety, improvement in air quality, higher customer satisfaction, and lower fuel consumption (U.S. DOT 2005). These applications, encompassing various areas, are briefly described next along with some primary security risks.

- **Arterial management systems.** Arterial management systems include computer and sensor systems to control traffic flow on arterial roadways based on demand. Because operating agencies often control such systems from remote locations, they are vulnerable to unauthorized usage. For example, depending on the signal preemption security settings, individuals have been able to acquire devices that cause unintended signal preemption.

- **Freeway management systems.** A freeway management system includes such functions as surveillance, control, guidance, warning, and information dissemination (FHWA, Freeway Management Handbook, 2003). These functions, provided in limited-access highways to improve traffic flow, are also vulnerable to security disruptions, which can be potentially catastrophic during mass evacuations.

- **Incident management systems.** Incident management systems are used to reduce the impact of unusual or abnormal occurrences, such as crashes, stalled vehicles, work zone lane closures, or special events. Such systems potentially can minimize the duration of an incident, minimize the risks of secondary crashes, and support re-routing traffic. Any disruption to the incident management system can accentuate the response to incidents.

- **Transit management systems.** Transit management systems are designed to improve the efficiency, security, and safety of public transit, including subways, light rail and buses. The public expects that these systems provide a safe and secure environment. Location identification technologies, operations software, real-time information, and electronic fare payment are some of the primary tools used to improve the efficiency, safety, and security of the transit systems. Knowing the real-time location
of the transit system elements and having transit drivers communicate with the dispatch and operations center ensures that the transit system is alerted of potential incidents on routes, so that drivers can take alternate routes. By implementing video and sensor surveillance in the transit terminals and area outside the vehicles, security of the system can be enhanced.

• Electronic toll collection (ETC). ETC systems permit automatic toll payment, where motorists need not stop to pay tolls. Vehicle-mounted units record payments from individual motorists, lessening toll plaza backups of vehicles and permitting more efficient and safer travel. Similar to ETC technology, security-related detection and surveillance devices in automated toll booths and at critical locations are also under development for monitoring suspicious activities.

• Regional multimodal traveler information systems. Multimodal traveler information systems provide travel-related information for use in highway, transit, ferry, and airway systems. The fusion of historical and current data makes it possible to create real-time information that can be passed on to travelers to rerout and avoid an incident scene, thus increasing safety and efficiency. Providing similar information on evacuation routes, routes to avoid, emergency transit services, and the transportation situation during emergencies can be valuable during and after an emergency event.

Field evaluations have been mostly positive regarding the effectiveness of these applications. This positive experience has been the major motivating factor for widespread deployment of ITS. Previous studies and field evaluations found positive gains in safety by implementing various ITS services. It is expected that the deployment of ITS will increase nationwide, expanding new opportunities to improve the transportation infrastructure and its associated regional and national security concerns.

Because using ITS to improve security can simultaneously attain other mobility and safety objectives, ITS can prove to be an efficient endeavor for both public and private agencies. Integrating ITS with other non-transportation infrastructure, such as surveillance cameras for businesses, can further mitigate safety and security risks. Large trucks carrying unauthorized hazardous materials are of major concern. The technology that can be applied to scan and check the carrier credentials and truck contents from a roadway checkpoint while the truck is in transit is a potentially beneficial way to improve security. In addition, ITS can minimize the impact after a security breach has occurred through the use of preestablished routes for evacuating people during emergencies. In both cases, providing motorists with real-time traffic assignment based on the traffic demands on designated routes and alternate evacuation routes can minimize the impact of any security breach within the infrastructure of the U.S. surface transportation system.
The primary benefits of ITS, including efficiency, safety, and security, are illustrated in Figure 1.1. Also shown are the security-related services provided by ITS, which potentially can prevent the tampering of both highway and transit infrastructures, including surveillance of traffic conducted through sensors, videos, and freeway service patrols. In addition, the use of ITS to regularly monitor commercial vehicles can support constant surveillance to prevent their use as terrorist weapons. Moreover, because ITS can minimize the impacts of highway incidents through traffic control and management at and near the incident-impacted area, the same concepts and technologies, such as use of dynamic message signs to inform motorists, the use of lane access control signs, and gates, can be used adjacent to the site of a terrorist attack to reroute traffic and track the location of vehicles carrying hazardous material close to the crisis area.

Additionally, ITS can help first responders and subsequent public safety assets dispatched by various law enforcement or rescue agencies increase their effectiveness by maintaining secure communications links. ITS can also support evacuation by providing information and control regarding lane reversal. Through ITS deployment in one or more of these areas—detection, surveillance, control, information, and coordination—some of the surface transportation safety and security risks can be minimized.

![Figure 1.1 ITS Functions and Security.](image-url)
The security-related services presented in Figure 1.1 may also provide “safety” and “efficiency” benefits; which means that investment of ITS and any other transportation infrastructure to strengthen security is likely to provide benefits in other areas as well. For example, ITS-related security features for bridges over navigable waterways, such as surveillance systems, will also support traffic management during a crash or evacuations due to natural or man-made emergencies, thus supporting safer and efficient traffic operations. Other security measures on bridges, such as lighting and pier strengthening, will contribute to its overall safety. Similarly, having an integrated and interoperable communication system between different stakeholder agencies for accelerated security response will benefit non-security related emergency events, such as supporting hurricane or flood related evacuations of at-risk population from an affected region (Parsons Brinckerhoff and Science Applications International Corporation, 2002). The multiple non-security related benefits that may be derived from a transportation security investment will make it more cost-effective and thus more justifiable.

1.4 SCOPE AND AUDIENCE OF THE BOOK

The focus of this book is on the infrastructure-based transportation technology that will contribute to the regional and national security against deliberate attacks on the transportation system. Although the book concentrates on technology related to the surface transportation infrastructure, modes of transport, such as personal transportation, public transit, and freight, are presented in terms of their relationship with the surface transportation infrastructure as identified in the National ITS Architecture (RITA, National ITS Architecture 6.0) including the Security Document (RITA, National ITS Architecture Security Document). This book discusses different objective measures to identify and quantify risks and develop mitigating measures using ITS while concentrating on different vulnerable links in transportation where ITS can contribute to security.

This book is intended to serve as a reference for transportation engineers, planners, and service providers in the public and private sectors involved in transportation or infrastructure security and will be useful to personnel involved in homeland security. It is also designed to serve as a college textbook for a graduate-level course or as a supplement to an undergraduate course. This book covers theories behind many risk analysis tools and provides real-world examples of transportation security plans and implementation guidelines of these plans. It concentrates on infrastructure planning and the system architecture that binds it with various surface transportation modes: personal vehicle, public transit (paratransit, buses, ferries, and rail), and commercial vehicle operations.

The surface transportation system faces the challenges of meeting the demand of increasing congestion with increased risks in safety and security
breach. We need to educate and train our future transportation professionals to meet these challenges. As ITS is expected to be a dominant element of future transportation systems, transportation professionals should know how to minimize the greatest risks to surface transportation systems through an understanding of security. By presenting academic background as well as project-oriented examples, this book provides fundamental knowledge to prepare professionals and students to improve the safety and security of transportation systems. Review questions are available at the end of each chapter in addition to exercises to help the reader apply the material.

1.5 CONTENT AND ORGANIZATION

The initial chapters of this book discuss how ITS can contribute to security, followed by approaches on using ITS for security and concluding with issues and opportunities to providing security through ITS and concepts of security. This book is organized into ten chapters:

- Chapter 1 introduced the concept of security and its contributions to positive social and economic growth. This chapter also discussed transportation security and how ITS can contribute to it. Additionally, the scope of this book and intended audience are also identified.

- Chapter 2 presents the case for having a comprehensive security framework for surface transportation infrastructure to minimize the risk of occurrence of a deliberate attack and to minimize impact after such an event has occurred. The chapter presents several case studies from around the world on transportation security programs.

- Chapter 3 introduces how the systems engineering approach of the National ITS Architecture can facilitate effective and systematic deployment of transportation technologies. This chapter focuses on the security aspects of the National ITS Architecture and presents examples of how these tools have been applied.

- Chapter 4 presents the process for identifying infrastructure security risks and associated factors with example problems and solutions. This will be the foundation for identifying the qualitative and quantitative relationship between risk and associated factors using state-of-the-art tools as presented in Chapter 5.

- Chapter 5 illustrates different concepts of risk modeling, including the data requirements and assumptions. In addition to detailing processes for evaluating the threats, this chapter discusses potential measures for mitigating these threats.

- Chapter 6 explains the fundamentals of computer network security as it pertains to ITS. It provides a background on the elements of computer network security followed by a general approach to securing these
networks. The objective of this chapter is to prepare the reader for Chapter 7 which is entitled Securing ITS.

- Chapter 7 discusses how ITS itself can be protected from deliberate attacks. The chapter presents different areas of ITS that need security considerations: information security, personnel security, and operational security. The chapter also discusses how security programs could be built on safety initiatives.

- Chapter 8 discusses the relationship between ITS security areas and other modes of transportation. It presents a framework of how ITS security areas can contribute to the security of air, maritime, rail, and military transportation.

- Chapter 9 presents the process for developing an integrated program in surface transportation security using ITS. This chapter also discusses how security can be integrated into the transportation planning and asset management processes.

- Chapter 10 discusses the issues and challenges for implementing security programs in the surface transportation system and discusses practical ways to meet these challenges.

REFERENCES


REVIEW QUESTIONS

1. Differentiate between natural hazards and terrorist threats in terms of protection and impacts.
2. Why is the perception of security so important for a society?
3. Provide a summary of attacks on transportation infrastructure around the world and their impacts.
4. Provide two scenarios where transportation security concerns will impact a highway engineer.
5. What is ITS? How can risks to our transportation system be minimized with ITS infrastructure?
6. Identify the stakeholders who are responsible for providing transportation security in your region and their roles in this capacity.


