CHAPTER 1

Introduction

It is estimated that there are 337 highway tunnels and 211 transit tunnels in the United States [Ref. 1]. These tunnels move thousands of people and tons of cargo daily. Many of these tunnel facilities are located at key "choke points" in the nation's transportation network. As with other components of the transportation infrastructure, tunnels are susceptible to a range of hazards and threats.

Tunnels can face disruption from either the occurrence of hazards (i.e., unintentional, accidental events) or the successful conduct of threats (i.e., intentional acts). Hazards can be human- or equipment-related (e.g., motor vehicle collisions and resulting fire) or natural (e.g., flooding and earthquakes). Relatively new tunnels have allowances for natural disasters incorporated into their design and construction. The allowances are based on the best engineering practices. Although older tunnels may lack some features that are commonplace in modern design and construction, the older tunnels may still be quite serviceable. Whether old or new, some tunnels may be impregnable to natural disaster because of their location, but still vulnerable to incidents.

Threats resulting in intentional disruption can include terrorist attacks such as those that occurred on September 11, 2001. While tunnels and transportation facilities were not the primary targets of those attacks, there were certainly numerous secondary effects on the transportation system. Tunnels make tempting targets because (a) they are important to the economic viability of surrounding communities, especially when they are used to transport goods; (b) many people are present at predictable times; and (c) the enclosed environment further compounds the potential for casualties from the effects of confined blast events, collapse, and flooding. Transit tunnels, in particular, are easily reached from open, accessible environments (i.e., stations); as a result, these tunnels are viewed as high-risk, high-damage potential targets. Examples of intentional, harmful aggression against transit tunnel environments and users are the 1995 sarin gas attack in Tokyo, the 2003 arson fire in Daegu, and the 2004 bombing in Moscow. The traveling public relies on the security and safety of transportation tunnels on a daily basis. It is essential that steps be taken to protect these important assets.

From a policy perspective, tunnel managers have two significant concerns. First, tunnels serve important day-to-day transportation functions, often providing nonredundant network connections. Second, owners must plan for effective use of the tunnels to transport people and goods as emergency relief in the event of severe emergencies occurring elsewhere. For example, an approaching hurricane in a coastal area may necessitate use of a highway tunnel for mass evacuation if it is deemed safe to do so. Alternatively, as on September 11, the initial closing of the transit and highway tunnels leading out of Manhattan required thousands of people to walk across outbound bridges. Even less catastrophic events, such as traffic accidents or train derailments, may have rippling effects in other parts of the transportation system. Moreover, extreme events will invariably impact multiple modes and other local, state, or national resources.

Because tunnels are expensive to build and operate, the existence of a tunnel usually indicates that no feasible alternatives existed; thus, no alternate routing or means of transport in the event of disrupted operation is likely to exist. In recognition of tunnels' vital roles and their exposure to harmful disruption, transportation tunnel security and safety issues have become part of the national security dialogue.

This report provides tunnel owners and operators with guidelines for protecting their tunnels to minimize the damage potential from extreme events so that, if damaged, the tunnels may be returned to full functionality in relatively short periods.

The report focuses on three kinds of transportation tunnels: highway, rail, and transit. Rail (which includes both passenger and freight) and transit tunnels are separate categories. Rail tunnels are typically larger and can carry greater loads than transit tunnels. Transit lines are typically in urban areas, with smaller and shorter cars, slower speeds, shorter distances, and higher occupancies than passenger rail lines.

1.1 Audience

The anticipated audience for these guidelines includes the following:

- Tunnel authorities or asset owners,
- State and local transportation departments and agencies responsible for tunnel operation and maintenance,
- Enforcement personnel and first responders responsible for tunnel safety and security, and
- Tunnel design consultants.

1.2 Basic Definitions

The basic concepts of risk management involve the relationships among (a) the nature of the threat or hazard that can cause damage to a susceptible asset, (b) the asset's operational and physical vulnerabilities to attack and/or failure, and (c) the damage potential (consisting of the loss of use of that asset and the loss of benefit of that asset to users).

Understanding relevant terminology is critical for all-hazards risk management and countermeasure strategy development. Most important is the distinction between hazards, which are unintentional, and threats, which are intentional. Neither of these terms implies a probability or likelihood that the event will materialize unless the terms are modified with explicit probability descriptors. The following definitions are used in this report:

- **Hazard—**The potential *unintentional* condition or event capable of disrupting or negatively impacting an asset, such as fire, power loss, or equipment breakdown. Hazards are usually associated with natural events and safety and are often measured in terms of the frequency and magnitude of the event. Hazards can also include degradation of structural integrity.
- **Threat—**The potential *intentional* act capable of disrupting or negatively impacting an asset. In other words, threats are deliberate attempts of a person or group to achieve various criminal or terrorist ends that may involve loss of life, loss of function, loss of visibility, and other objectives.

  Threats are distinct from hazards because they are not acts of nature, accidents, or organic happenstances for which tunnels are normally designed. Rather, threats are typically characterized as acts of intrusion; placement of explosive devices; and/or chemical, biological, or radiological attacks. In the case of terrorism, a threat consists of a scenario that combines a weapon, a host (i.e., an aggressor), a delivery mode, and tactics (i.e., a path of approach, the use of stealth or force, and the actual target of weapon placement). While hazards are associated with safety, threats are associated with security.
- **Target/Asset—**Persons, facilities, activities, or physical systems that have value to the owner or to society as a whole.
- **Damage Potential—**The potential for negative effects—including immediate and long-term damage or loss, whether tangible or intangible—resulting from an unintentional event or an attack on an asset. Mission-related damage potential (i.e., impacts that are critical to the owner's transportation institutional mission, including destruction or damage causing loss or reduction of functionality) is of special importance, together with injury or loss of life, as well as impacts on quality of life and morale. Damage potential grows as a function of an asset's criticality. However, a critical asset may be damaged without a total loss of functionality.
- **Vulnerability—**A weakness in asset design or operations that can be exploited by a threat or hazard to produce negative consequences, or damage. Specific threats and hazards therefore relate to different vulnerabilities.

It should be noted that the specific quantitative relationship among the variables in the risk equation depends on how the various factors are developed and expressed. For example, damage potential and vulnerability of assets can be judged on a relative scale with upper and lower bounds or through analytical models that assess asset criticality in terms of potential casualties, economic impacts, or physical or operational vulnerabilities. However, the probability of a threat or hazard materializing to trigger the consequences may be difficult to estimate in more than qualitative or relative terms.

1.3 Methodology

Vulnerability and damage potential have been ranked on relative scales and analyzed to develop priorities for countermeasures.

1.4 Assumptions

This report was prepared using the collective knowledge and experience of the authors. Common sense was used to avoid unnecessary duplication of effort; further exploration of common topics encountered by a tunnel owner or operator; and improbable hazard and threat situations, damage potential, and countermeasures.

The single most significant assumption made during this research effort is that guidelines that cover the range of "routine" hazards to tunnel safety—such as equipment breakdowns, derailments, utility disruptions, minor criminal acts, and medical emergencies—already exist. The experience of tunnel operators in handling these minor incidents is already

addressed in handbooks, manuals, and industry standards that are readily available. Wherever possible, references to these materials are noted in the text. The addition of security-related threats—from both major criminal acts and terrorism—then becomes an important extension to an "all-hazards" approach to tunnel security.

The research did not address nuclear threats, common natural or weather hazards, or inspection or maintenance issues.

Additional assumptions include the following:

- The physical aspects of the tunnel (i.e., structural aspects, geotechnical aspects, and water levels) are known before the tunnel owner or operator uses this guide.
- Before implementing any of the countermeasures recommended herein, the tunnel owner or operator will conduct a full engineering assessment that takes into account facility-specific conditions.