# Threat and Vulnerability Assessment (TVA)

A Threat and Vulnerability Assessment (TVA) for passenger rail systems considers the need to protect people and assets while minimizing exposure to crime, breaches of security, and terrorism. Effective security starts with a clear understanding of the system's vulnerabilities. Soteria takes a multidisciplinary approach to gauge the system's strengths and weaknesses in various scenarios, to provide our clients with a comprehensive and critical evaluation of their entire security framework.

We address credible threat scenarios thorough mitigations interwoven into the design process to provide an integrated approach to security risk and operations resilience. The primary mitigation categories include:

- Systems and technologies
- Site and architectural layout
- Security operations
- Protective engineering (blast, ballistic [active shooter], and vehicle ramming threats)

Soteria's TVA process is predicated on principles and experience from the transit sector throughout North America and overseas, and provides clients with:

- A quantified and prioritized analysis of the potential security threats and damage consequences
- Effective systems, operational, and architectural countermeasures to reduce security risk
- Risk-based cost-effective protective engineering mitigations to harden assets selectively where needed

**Our five-phase approach allows security risk management to be seamlessly integrated into project-wide objectives.**

## PHASE 1 – EARLY BASIS OF DESIGN DEVELOPMENT

**Data Collection and Threat and Vulnerability Identification**

- Data gathering and discussions with rail agency security personnel to identify and prioritize relevant threats, critical assets, and key vulnerabilities affecting overall security concerns.

**Basis of Design and Performance Objectives**

- Discussions with key project stakeholders to identify threat scenarios and performance objectives for critical rail system assets.
- Performance objectives determined to minimize damage to physical structures and system function while ensuring maximum system resilience. Stable structural and functional performance are obtained for a range of threats.

## PHASE 2 –RISK AND DAMAGE IMPACT ASSESSMENTS

**Field Survey and Design Review to Identify Vulnerabilities**

- Alignment survey to determine and document first-hand the potential security vulnerabilities of the system.
- Analysis of security strengths and weaknesses in system technologies and overall design through review of architectural and systems conceptual engineering drawings.

**Quantitative and Qualitative Risk Analysis Process for All Security Threats**

- Security risk analysis to define qualitative and/or quantitative risk rankings of security threats. These may include vehicle and person-borne explosives, active shooter (ballistic), vehicle ramming, arson, chemical/bio warfare, malicious pandemic spread, sabotage, crime, and any other credible system threat.
- A formalized risk process allows for protection considerations to be prioritized relative to asset criticality and damage likelihood and severity. Higher-risk assets and more likely and consequential threat scenarios are given precedence.

**Blast, Ballistic, and Vehicle Ramming Analysis**

- Preliminary engineering evaluations of credible explosive, ballistic, and vehicle ramming threats to determine the potential damage impact these may impart to system components.
- Other non-code based extreme events such as high-intensity fire and forced entry may also be evaluated.

## PHASE 3 - MITIGATION STRATEGY & PROTECTIVE ENGINEERING DEVELOPMENT

- Where risk analysis shows physical and functional losses would exceed acceptable values, design modifications, technologies, operational solutions, and structural hardening and enhancements will be suggested to strengthen system resilience and/or alter the exposure to the extreme loads.
- In the early stages of this phase, Soteria will conduct a workshop to
    - Present initial findings and preliminary proposed countermeasures.
    - Obtain stakeholder input in order to further refine recommendations.
- Our analysis will recommend mitigation in the following categories to deter, detect and delay potential system attacks:
    - *Architectural and site layout enhancements* such as CPTED to substantially reduce security risk at the outset in the overall site design and layout.
    - Implementation of *systems and technologies* such as smart surveillance, intrusion detection, access control, and thermal screening to further buy down risk to occurrence of adverse event.
    - *Operational schemes* to lower probability of successful attack.
- To mitigate potential critical damage to key assets from a successful explosive attack or other extreme-event, *structural and engineering enhancements* may be explored.
- Various combinations of the above countermeasure types are iteratively test fit to reduce system security risk to acceptable levels and formulate security design criteria. Cost vs. risk reduction is an integral part of this step. This method leads to an optimized suite of tailored mitigations that include both prescriptive and performance-based design and structural enhancements, operational mitigations, and systems-based solutions.
- Our approach looks to first and foremost leverage the already existing protective attributes that are inherent to the un-enhanced condition (code-based) and subsequently develop incremental security hardening measures to meet risk tolerance. Mitigations are then balanced with other project goals and costs are significantly reduced.

### PHASE 4 - PRESENTATION OF ASSESSMENT FINDINGS AND REPORT SUBMITTAL

- In this phase our report is presented to key stakeholders and submitted following their review and acceptance.

### PHASE 5 – FOLLOW-ON OVERSIGHT THROUGHOUT PROJECT LIFE

- Soteria will provide follow-on oversight for the certification process to verify implementation of accepted recommendations in the system's final design and construction.