Quantitative Security Risk Assessment and Management for Railway Transportation Infrastructures

presented by

Francesco Flammini

Ansaldo STS Italy - Business Innovation Unit
University Federico II of Naples - Department of Computer and Systems Engineering
• Railway and Subway transportation systems are exposed to threats ranging from vandalism to terrorism
• CIP life-cycle:
Risk Analysis

• Risk Analysis
  - Qualitative
  - Quantitative

• Iterative steps
  - Risk Assessment
  - Risk Mitigation

• Main objective of traditional (qualitative) approaches
  - Evaluation of most relevant vulnerabilities

• Advantages of quantitative approaches
  - More precise results
  - Support the design of protection mechanism
  - Evaluation of the return on investment
Quantitative Definition of Risk

\[ R = P \cdot V \cdot D \]

- \( P \): threat frequency [events / year]
- \( D \): expected damage [€]
- \( V \): system vulnerability w.r.t threat (adimensional)

\[ P(success \mid \text{threat}) \]

Therefore, the Risk can be expressed in [€ / year] (monetary loss)
Effect of Protection Mechanisms

• Protection mechanisms are able to reduce the risk by having three main effects:
  - Protective, aimed at the reduction of $V$
  - Deterrent, aimed at the reduction of $P$
  - Rationalizing, aimed at the reduction of $D$

• In the assumption that:
  - Threat $T$ belongs to category $C$
  - Threat $T$ happens in (or passes through) site $S$
  - Protection $M$ is installed in site $S$
  - Protection $M$ is effective on threat category $C$

then it can be stated that $M$ protects against $T$
Extensive Risk Formula

\[ R_T = \sum_i R_i \cdot \prod_j (1 - E_{Pji} \cdot COV_j) \cdot (1 - E_{Dji} \cdot COV_j) \cdot (1 - E_{Rji} \cdot COV_j) \]

- \( R_T \) is the total mitigated risk
- \( R_i \) is the initial risk associated to threat \( i \)
- \( E_{Pji} \) is an estimate of the protective effect of mechanism \( j \) on threat \( i \)
- \( E_{Dji} \) is an estimate of the deterrent effect of mechanism \( j \) on threat \( i \)
- \( E_{Rji} \) is an estimate of the rationalizing effect of mechanism \( j \) on threat \( i \)
- \( COV_j \) is a measure of the coverage of mechanism \( j \) (e.g. percentage of the physical area or perimeter of the site)
Return on investment

\[ EB = \text{risk reduction} - \text{total investment in security} = (R_T - \sum_{i} R_i) - \sum_{j} C_j \]

- \( EB \) is the Expected Benefit, which can be positive or negative
- \( C_j \) is the cost of the protection mechanism \( j \), obtained considering all the significant costs (acquisition, installation, management, maintenance, etc.)
The Q-RA tool: software architecture

- Languages / technologies employed in design and implementation of the tool:
  - UML, MySQL, JSP, Apache Tomcat
### Example application

#### PROTECTION MECHANISMS

<table>
<thead>
<tr>
<th>PROT. ID</th>
<th>COUNTERMEASURE DESCRIPTION</th>
<th>ACQ. COST [k$]</th>
<th>MANAG. COST [k$/YR]</th>
<th>SITE</th>
<th>COV</th>
<th>THREAT CATEGORIES</th>
<th>$E_r$</th>
<th>$E_p$</th>
<th>$E_e$</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>ALARMED FENCE</td>
<td>10</td>
<td>1</td>
<td>STATION EXT. STATION INT. (NIGHT)</td>
<td>0.9</td>
<td>VANDALISM, THEFT, P. SABOTAGE</td>
<td>0.9</td>
<td>0.3</td>
<td>0.2</td>
</tr>
<tr>
<td>2</td>
<td>VOLUMETRIC DETECTOR</td>
<td>5</td>
<td>1</td>
<td>TECH. ROOM</td>
<td>1</td>
<td>THEFT</td>
<td>0.8</td>
<td>0.6</td>
<td>0.2</td>
</tr>
<tr>
<td>3</td>
<td>VIDEO-SURVEILLANCE (INTERNAL)</td>
<td>150</td>
<td>20</td>
<td>HALL, PLATFORM</td>
<td>0.95</td>
<td>VANDALISM, THEFT, SABOTAGE, TERRORISM EXPLOSION, TERRORISM CHEM</td>
<td>0.4</td>
<td>0.6</td>
<td>0.3</td>
</tr>
<tr>
<td>4</td>
<td>CHEM. DETECTOR</td>
<td>50</td>
<td>2</td>
<td>PLATFORM</td>
<td>0.9</td>
<td>TERRORISM CHEM</td>
<td>0.6</td>
<td>0.2</td>
<td>0.4</td>
</tr>
<tr>
<td>5</td>
<td>INTRUSION DETECTION SYSTEM</td>
<td>1</td>
<td>0.5</td>
<td>TLC SERVER</td>
<td>1</td>
<td>L. SABOTAGE</td>
<td>0.9</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>6</td>
<td>EXPLOSIVE DETECTOR</td>
<td>50</td>
<td>2</td>
<td>STATION INT. (*)</td>
<td>1</td>
<td>SABOTAGE, TERRORISM EXPLOSION</td>
<td>0.8</td>
<td>0.4</td>
<td>0.1</td>
</tr>
</tbody>
</table>

(*) detectors are physically installed near tunnels, but the protection is effective on the whole station interval.

---

#### THREATS

<table>
<thead>
<tr>
<th>THREAT ID</th>
<th>THREAT DESCRIPTION</th>
<th>THREAT CATEGORY</th>
<th>SITE</th>
<th>EST. P [#/YEAR]</th>
<th>EST. VNT [k$]</th>
<th>EXP. ASSET D [k$]</th>
<th>EXP. SERVICE D [k$]</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>GRAFFITI</td>
<td>VANDALISM</td>
<td>STATION EXT.</td>
<td>60</td>
<td>0.9</td>
<td>0.5</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>THEFT OF PCs</td>
<td>THEFT</td>
<td>TECH. ROOM</td>
<td>4</td>
<td>0.8</td>
<td>8</td>
<td>6</td>
</tr>
<tr>
<td>3</td>
<td>GLASS BREAK</td>
<td>VANDALISM</td>
<td>STATION EXT.</td>
<td>12</td>
<td>1</td>
<td>0.5</td>
<td>0</td>
</tr>
<tr>
<td>4</td>
<td>BOMBING</td>
<td>TERRORISM EXPLOSION</td>
<td>PLATFORM</td>
<td>0.01</td>
<td>1</td>
<td>600</td>
<td>300</td>
</tr>
<tr>
<td>5</td>
<td>HACKING</td>
<td>SABOTAGE</td>
<td>TLC SERVER</td>
<td>2</td>
<td>0.8</td>
<td>0</td>
<td>10</td>
</tr>
<tr>
<td>6</td>
<td>GAS ATTACK</td>
<td>TERRORISM CHEM.</td>
<td>PLATFORM</td>
<td>0.01</td>
<td>1</td>
<td>10</td>
<td>150</td>
</tr>
<tr>
<td>7</td>
<td>FURNITURE DAMAGE</td>
<td>VANDALISM</td>
<td>HALL</td>
<td>70</td>
<td>1</td>
<td>0.1</td>
<td>0</td>
</tr>
<tr>
<td>8</td>
<td>INFRASTRUCT. DAMAGE</td>
<td>SABOTAGE</td>
<td>PLATFORM</td>
<td>4</td>
<td>0.9</td>
<td>5</td>
<td>0</td>
</tr>
</tbody>
</table>
Q-RA GUI: example inputs and outputs
Conclusions & future works

• A methodology and a tool for the quantitative risk analysis have been developed which allow to compute the return on investment of security protection mechanism.

• The tool has been designed and experimented for the physical protection of rail-based mass transit systems; however, it is suited to logical threats and other classes of critical infrastructures.

• The automation provided by the tool also eases the analysis of parametric sensitivity in order to assess how error distributions in the input values affect the overall results.

• For attacks involving persons (injury or kill), a quantification of consequences, though possible, is not generally accepted. Therefore, qualitative approaches can be applied separately to such classes of threats. Q-RA is also intended for the integration of qualitative analysis by means of associative tables.

• It is possible to extend the tool with functionalities of cost/benefit optimization (e.g. by genetic algorithms), considering limited budget constraints. In such a way, the optimal set of protection mechanism minimizing the risk can be automatically determined.

• The evaluation of parameters involved in the risk formula can be performed by adopting model-based approaches. See:
  …later, during the poster session.
Thank you for your kind attention.

Any questions?