Critical Infrastructures (CI)
- Incapacity or destruction of systems and assets that would have a debilitating impact on [1]:
  - Security
  - National economic security
  - National public health or safety
  - or any combination of those matters.

Risk analysis and Criticality analysis
- Impact is assessed under various terms, such as consequences, criticality, or vitality, and expressed with various criteria or factors [2].
- Criticality assessment has a more broad scope than risk assessment.
- Captures the external, societal impacts.

Risk analysis vs. criticality analysis

<table>
<thead>
<tr>
<th>Risk Analysis</th>
<th>Criticality Analysis</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aim</td>
<td>Organization</td>
</tr>
<tr>
<td>Scope</td>
<td>Internal assets</td>
</tr>
<tr>
<td>Impact Type</td>
<td>Organization-centric</td>
</tr>
<tr>
<td>Threats</td>
<td>System</td>
</tr>
<tr>
<td>Vulnerabilities</td>
<td>System</td>
</tr>
<tr>
<td>Impact Scale</td>
<td>Variable</td>
</tr>
</tbody>
</table>

Criticality in large-scale environments
- Structured, multi-layer Criticality Assessment methodology [3] that takes into consideration the operator, the sector and the intra-sector layer.

Layer 1: Operator risk assessment:
- Evaluate possible impacts within the scope of the examined organization.
- A CI may consider both inside and outside threats.

Layer 2: Sector risk assessment:
- Cumulative impacts from the realization of various threats.
- Dependencies with other sectors are examined.

Layer 3: Intra-sector/National criticality assessment:
- New form of risk assessment is required: criticality assessment.
- Impacts external to a specific CI, i.e. social/societal impacts, sector-wide impacts or impacts to people/citizens.

Criticality
- Total Impact for every applicable combination of a component, an incident-threat and a resulting effect to an infrastructure [4].

\[ \text{Criticality}_I = \sum_{c, th, e} \text{Impact}_I(c, th, e) \]

Risk Assessment for interdependent CIs
- Improved methodology based on [3] for developing [4]:
  - Assesses Societal impact of an infrastructure or a sector.
  - Assesses Overall infrastructure risk, taking into account interdependencies.
  - Assesses Risk in three layers: the infrastructure level, the sector level and, finally, the national/intra-sector level.
- Considers 1st-order dependencies and cannot assess complex chain effects.

Risk assessment of multi-order dependencies
- Proposed methodology [5] for multi-order dependencies:
  1. Identify the initiating event.
  2. Identify interdependencies and perform qualitative analysis.
  3. Perform semi-quantitative assessment of the scenario.
  4. Perform detailed quantitative analysis of interdependencies (optional).
  5. Evaluate risk and measures to reduce interdependencies.
  6. Perform cost/benefit analysis (optional).

Cascading Effects
- First-order outgoing risks in Operator level and societal risk.
- Dependency Risk Table summarizes dependencies [6] of each CI to others.
- Dependencies visualized through graphs.

Table 1. CI interdependencies

<table>
<thead>
<tr>
<th>Sector</th>
<th>Physical</th>
<th>Cyber/Informational</th>
<th>Geographic</th>
<th>Logical</th>
<th>Social</th>
</tr>
</thead>
<tbody>
<tr>
<td>C1</td>
<td>State of a CI depends upon the material output</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>C2</td>
<td>State of a CI depends on information transmitted</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>C3</td>
<td>State of a CI depends on an environmental event on another CI</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>C4</td>
<td>State of a CI depends upon another CI via a nonphysical, cyber, or geographic connection</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>C5</td>
<td>State of a CI is affected by the spreading of disorder</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Conclusions
- The method of analyzing cascading effects [7] provides an efficient way to evaluate whether common-cause failures can propagate to infrastructures that are not directly affected by an examined common-cause threat.
- Assessment of likelihood, impact and risk is using five-item Likert scales [5].
  - Results from relevant approaches are incorporated in the assessment.
  - Risk assessment of n-order dependency requires computational resources if nodes of the dependency graph increase significantly.
  - Dependencies examined on a normal mode of operation. Different analysis is required when examining stress, crisis or restoration modes of operation.
- Critical infrastructure protection methods have a severe positive impact on the protection of several security-critical applications. [9-12].
- Critical infrastructure protection fits well and builds upon our Laboratory record on information security.

References