This task describes the design and execution of a SMS to answer the following:

- What attributes of the studied systems make them both modular and open?
- What security concerns have been presented in the literature for modular open systems?
- What attack vectors have been presented in the literature for modular open systems?
- What security patterns have been proposed in the literature to address the attack vectors in modular open systems?

**DATA & ANALYSIS**

<table>
<thead>
<tr>
<th>Database</th>
<th>Initial Hits</th>
<th>Number of Papers Selected by Full Text Review</th>
</tr>
</thead>
<tbody>
<tr>
<td>IEEE</td>
<td>212</td>
<td>8</td>
</tr>
<tr>
<td>SPIE</td>
<td>234</td>
<td>4</td>
</tr>
<tr>
<td>Science Direct</td>
<td>1038</td>
<td>0</td>
</tr>
<tr>
<td>Scopus</td>
<td>486</td>
<td>5</td>
</tr>
<tr>
<td>Springer Link</td>
<td>2558</td>
<td>2</td>
</tr>
<tr>
<td>Snowballt</td>
<td>14</td>
<td>2</td>
</tr>
</tbody>
</table>

**RESEARCH TASK / OVERVIEW**

- **Attributes of the modular open systems were tabulated. Excerpt:**
  - A Systematic Mapping Study (SMS) of Systems Security Engineering for Modular Open Systems

**METHODOLOGY**

- Map security and attack vectors identified in this literature mapping. Understand the protection gap of unmitigated attack vectors
- Understand how to handle modules form distinct security provenances
- Propose mitigations and security patterns for supply chain attack vectors
- Applications of security patterns for trusted/untrusted module boundaries, and security provenance boundaries
- Maintaining the integrity of the system when operating
- Securely integrating components into the system

**CONTACTS / REFERENCES**


**GOALS & OBJECTIVES**

- The objectives of this research are:
  - To understand the security concerns of modular open systems.
  - To identify attack vectors that could pose a threat to modular open systems.
  - To identify security patterns that will mitigate the identified attacks.

**DATA & ANALYSIS**

- A total of 78 security patterns were identified
- Categorized using Risk Management Framework (RMF) control families

**DATA & ANALYSIS**

- Security Patterns in the top three control families were further categorized:
  - System and Communication Protection, System and Information Integrity, System and Services Acquisition

**DATA & ANALYSIS**

- Security Patterns Categorized using RMF control families

**DATA & ANALYSIS**

- System and Communication Protection
  - Authorization, Assessment, and Authorization
  - Configuration Management
  - Physical Security
  - Access Control

**DATA & ANALYSIS**

- System and Information Integrity
  - Identification and Authentication
  - Access Controls
  - Media Protection

**DATA & ANALYSIS**

- System and Services Acquisition
  - Information Integrity, System and Privacy
  - Information Integrity, System and Protection, System and Communication