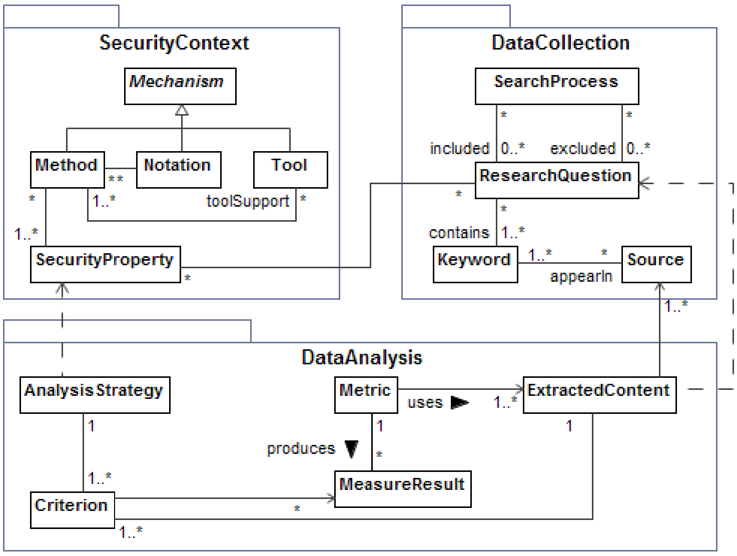
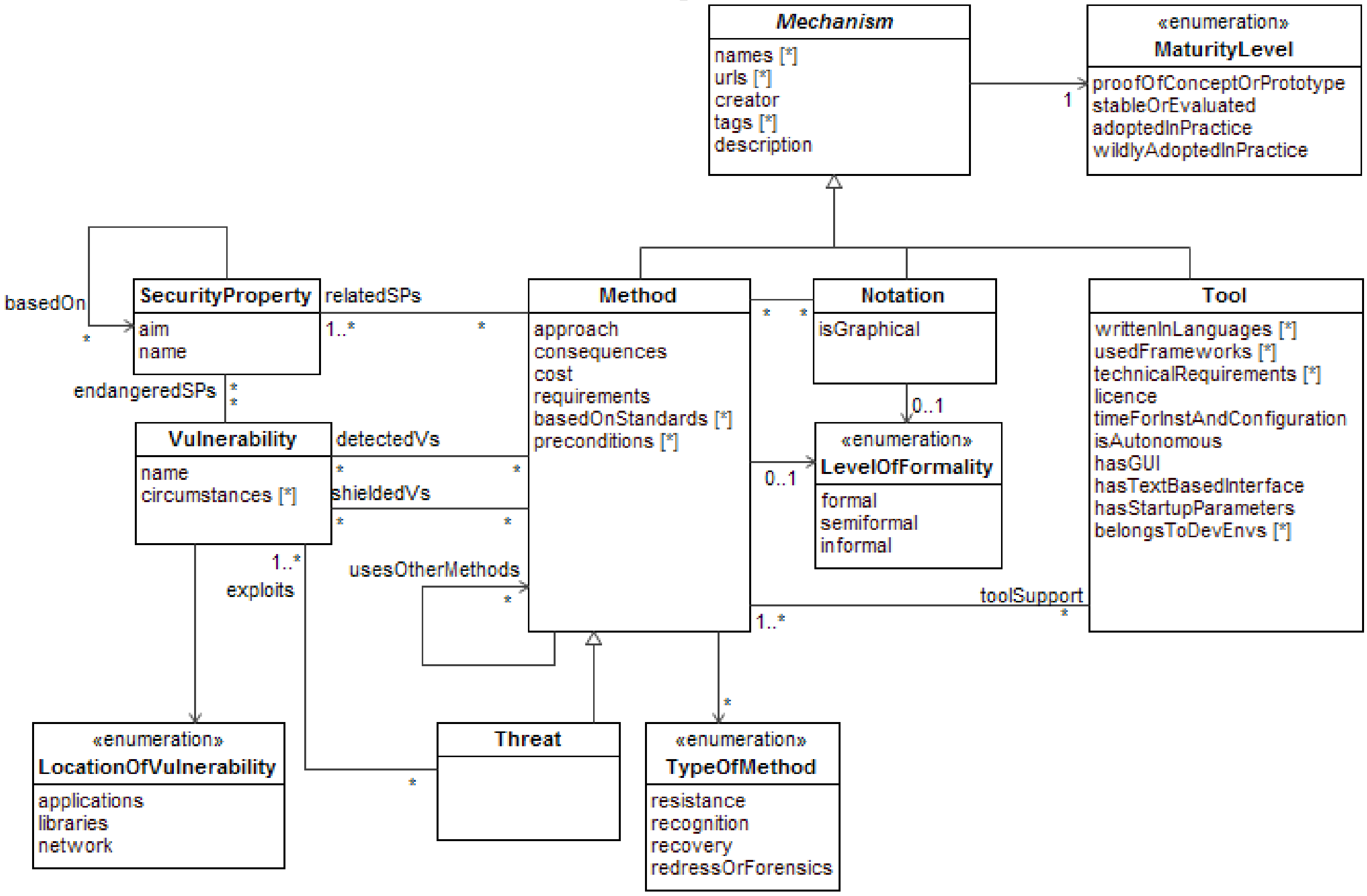
Security Engineering Method and Tool Evaluation

Our **aim** is to provide an approach for the evaluation of methods and tools for the engineering of secure software systems. In our approach we do not only distinguish methods and tools, but also notations. For an evaluation and comparison approach we need to define (1) the process of how to conduct a comparison and (2) the structure used to collect security-related data and metrics to analyze it. Therefore, we define a conceptual framework that comprises these three aspects: Security Context, Data Collection and Analysis. We depict the concepts and their relationships as a model, so that we can instantiate concrete methods, tools and notations.



Additionally, we will compare other approaches with our framework in order to further adapt or extend it with the objective to make it more general.

The **basic structure** of our model of the `Security Context` is as follows:

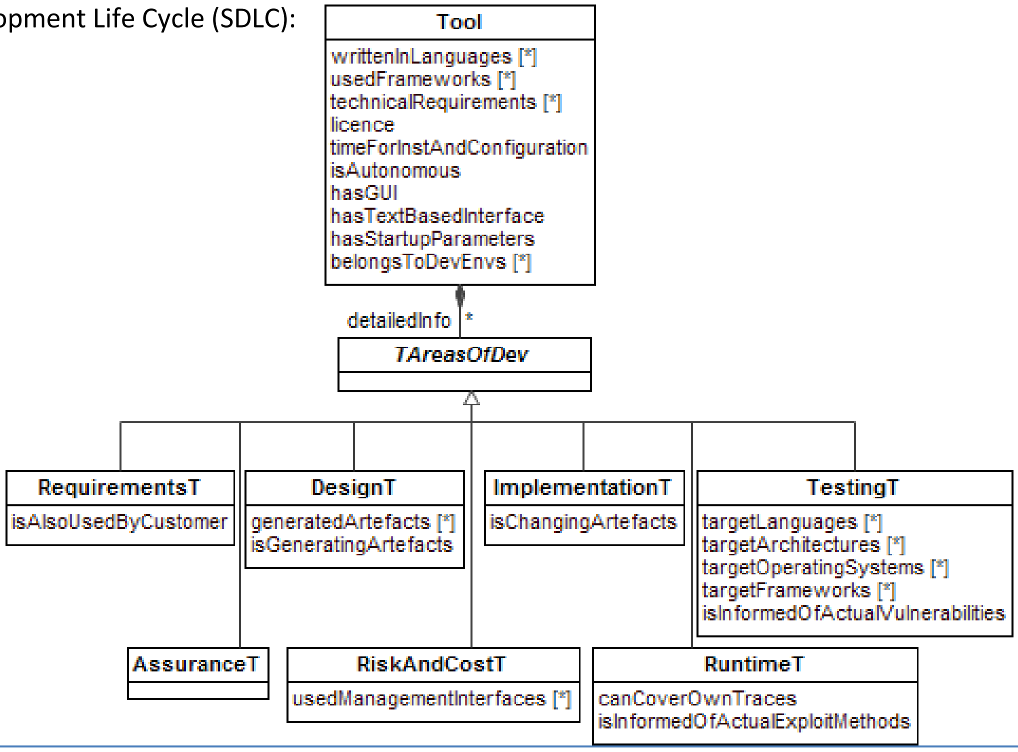


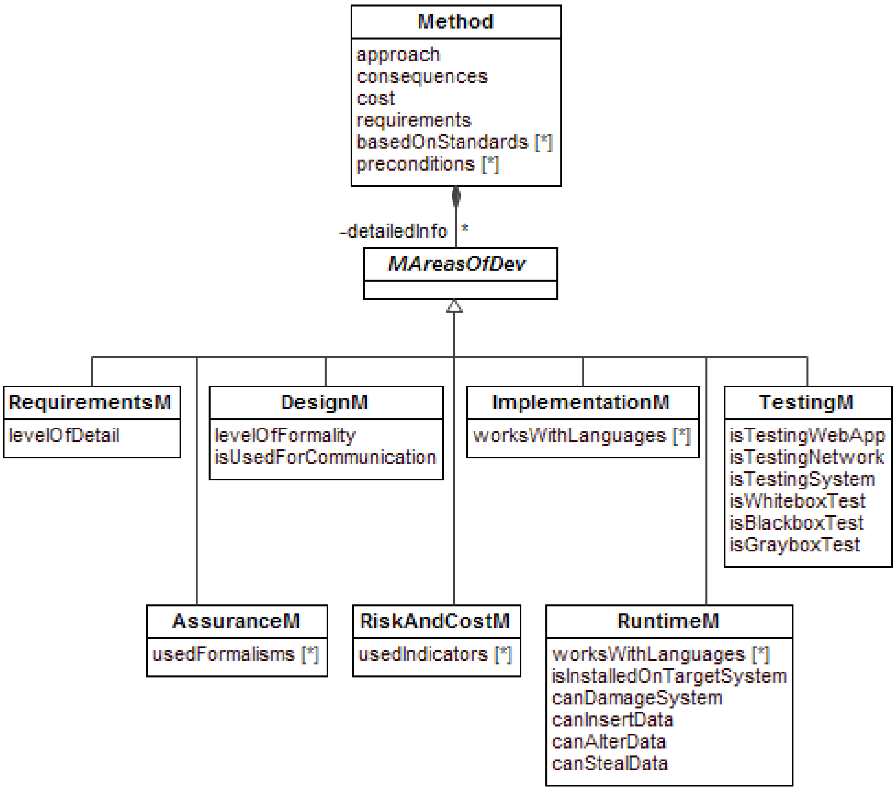
The classes `Method`, `Notation` and `Tool` are depicted in the center. They inherit general attributes, as e.g., names and URLs, from the abstract class `Mechanism` (we are still looking for a better name to replace “mechanism”, suggestions are welcome!). A tool can support methods and a notation can be used for several methods.

Security features are shown on the left hand side:

- A `Security Property` can be, e.g., authorization, authentication, integrity, etc. Several security properties can be enforced or attacked by a method.
- A `Vulnerability` can endanger security properties. Examples are XSS, SQL Injection, Buffer or Overflows, etc.
- A `Threat` can exploit vulnerabilities. Threats are kind of methods which are vicious.

In the following diagrams, the classes **`Tool` and `Method` are refined** according to their usage in the Software Development Life Cycle (SDLC):





Questions and Suggestions

1. Name:

   Partner:

2. Areas of security you are working in?

3. Can **methods** from your area be represented using our model?

   Provide examples of methods.

   Are concepts or relationships missing? Which?

4. Can **tools** from your area be represented using our model?

   Provide examples for tools.

   Are concepts or relationships missing? Which?

5. Can **notations** from your area be represented using our model?

   Provide examples of notations.

   Are concepts or relationships missing? Which?

7. Would you use our structure to evaluate tool, methods or notations in your area?
   If not, what would your approach look like?

   If yes, where do you see its strengths?

8. Can you suggest related work (esp. for managing tool and method portfolios for the area you are working in or general approaches to compare with our approach)?

9. General comments or improvements?