Beyond One-Shot Security:

Keeping Information Systems Secure through Environment-Driven Knowledge Evolution

Thomas Ruhroth

Jens Bürger, Jan Jürjens, Kurt Schneider, Stefan Gärtner

technische universität dortmund

Leibniz Universität Hannover

Environment-driven Security Evolution

http://www.zeit.de/digital/datenschutz/2012-07/ec-karten-hack

Assumptions about Environment and Knowledge of Attacker

It is difficult to get informations out of an secure chip.

Change in Knowledge

It is difficult to get informations out of an secure chip.

Open display- and keyboard-APIs can be used to show fake dialogs.

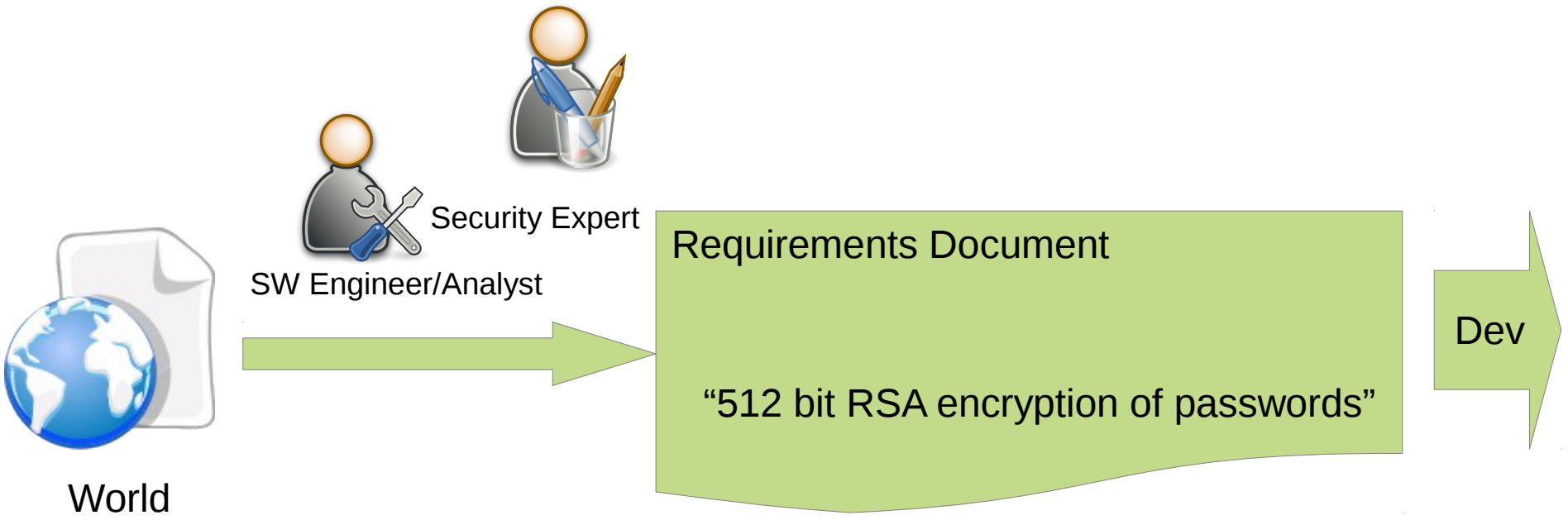
No changes in System

Use of internal and secure chips prevent the leakage of PINs

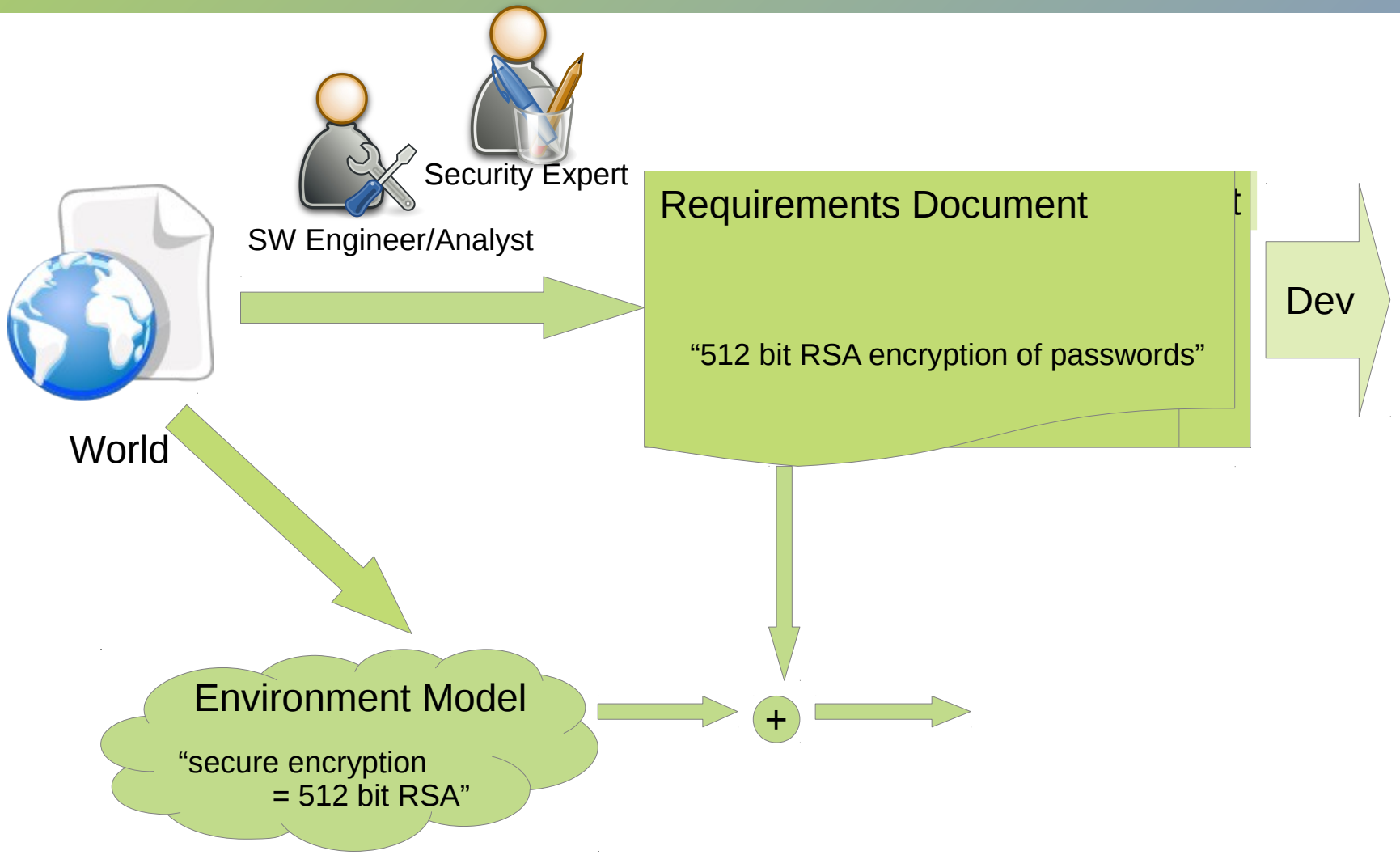
time

Attack using additional dialogs, so that the customer repeats the PIN in an insecure mode

Traditional Requirements Eng.



Environment Model



Environment Evolution

Abstract Requirements Document

"secure encryption of passwords"

Environment Model

"secure

Requirements Document

passwords"

This is general Idea

But:

We need to also change the models and the software!

Security Expert

Environment Model

"secure encryption
= **1024** bit RSA"

+

Requirements Document

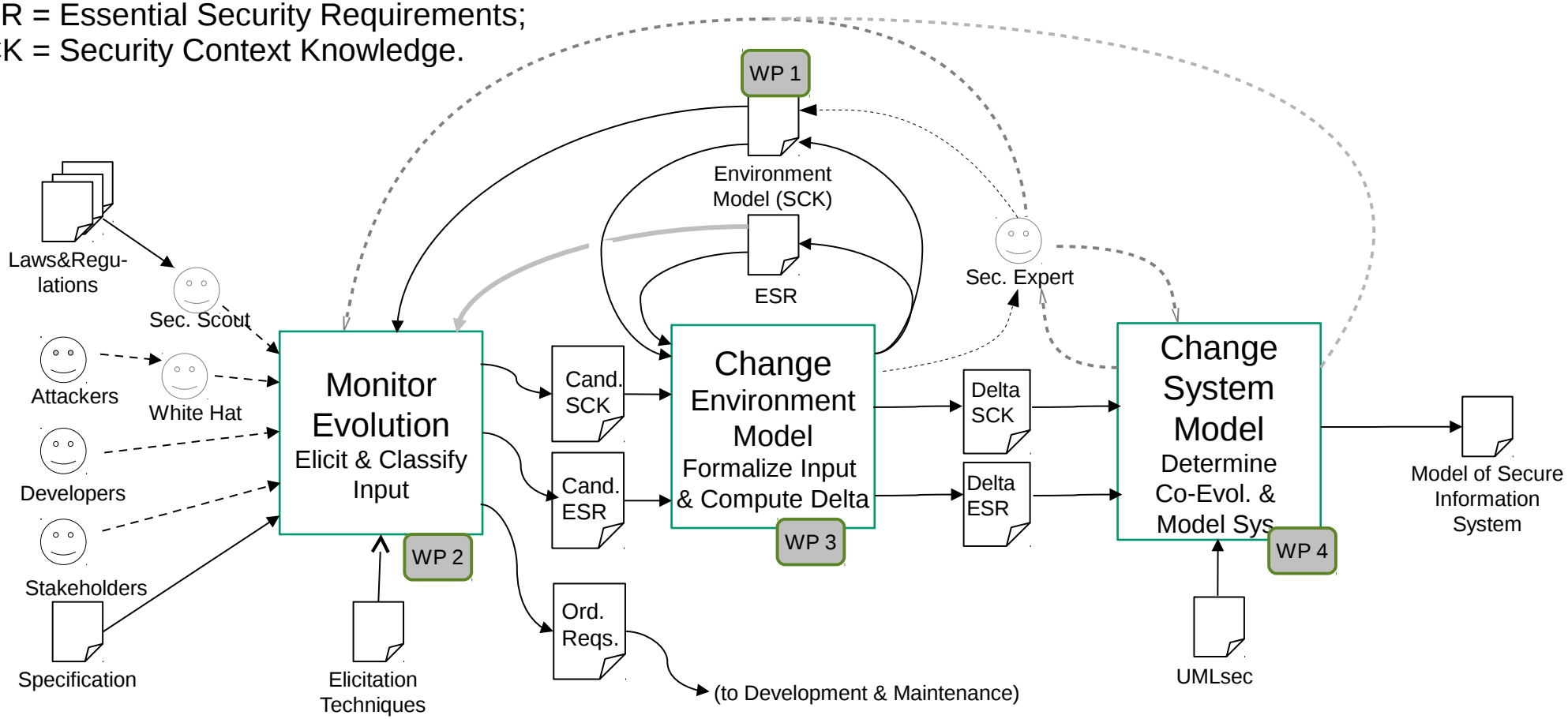
"**1024** bit RSA encryption of passwords"

technische universität
dortmund

Leibniz
Universität
Hannover

SecVolution: An Overview

ESR = Essential Security Requirements;
SCK = Security Context Knowledge.

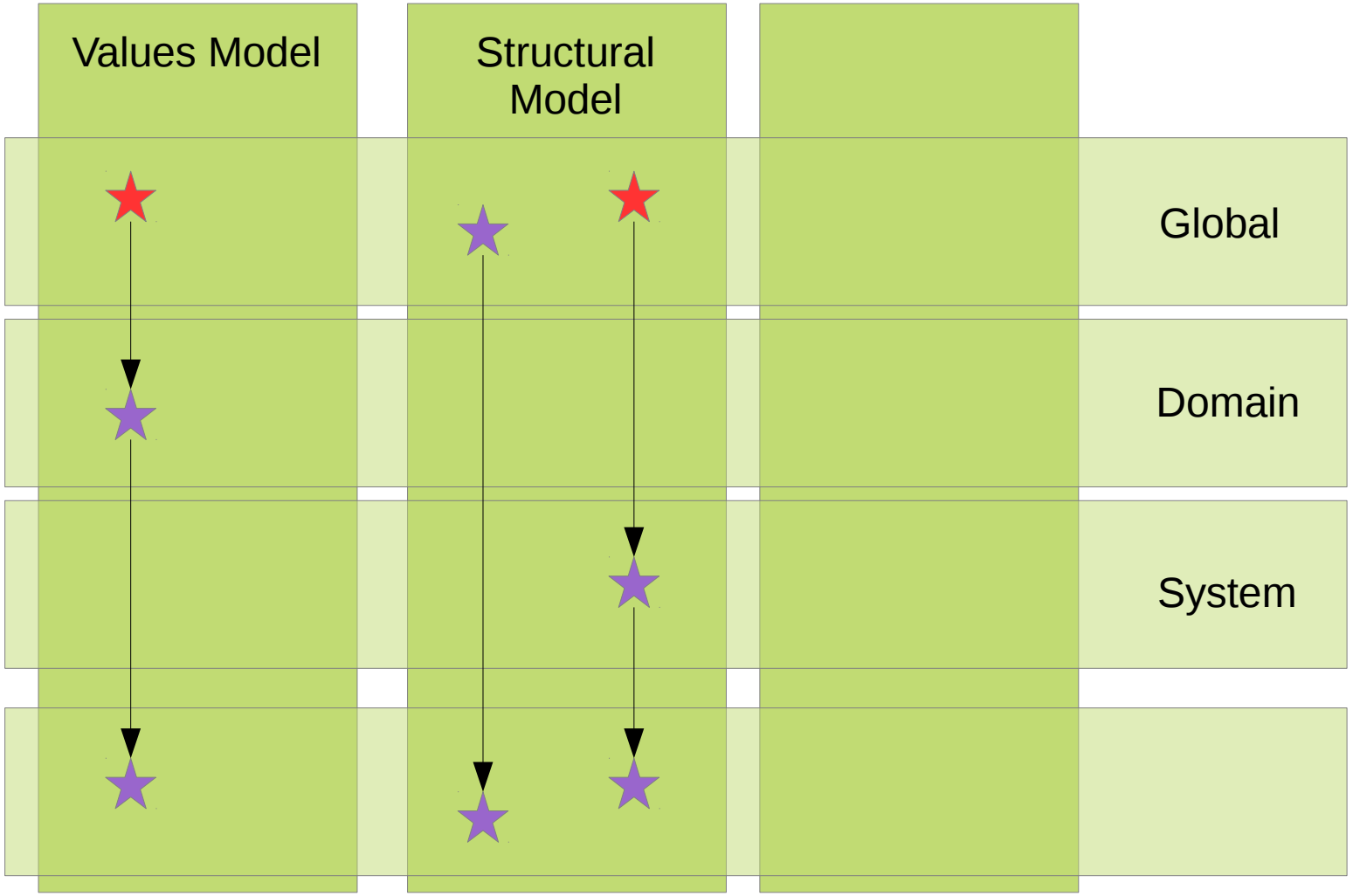


Extended scope and knwoledge sources

Heuritic Identification of relevant requirements and facts

Determine Reaction and Update UMLsec models
- *Based on Existing Model*
- *By extending Metamodel*

WP1: Environment Model



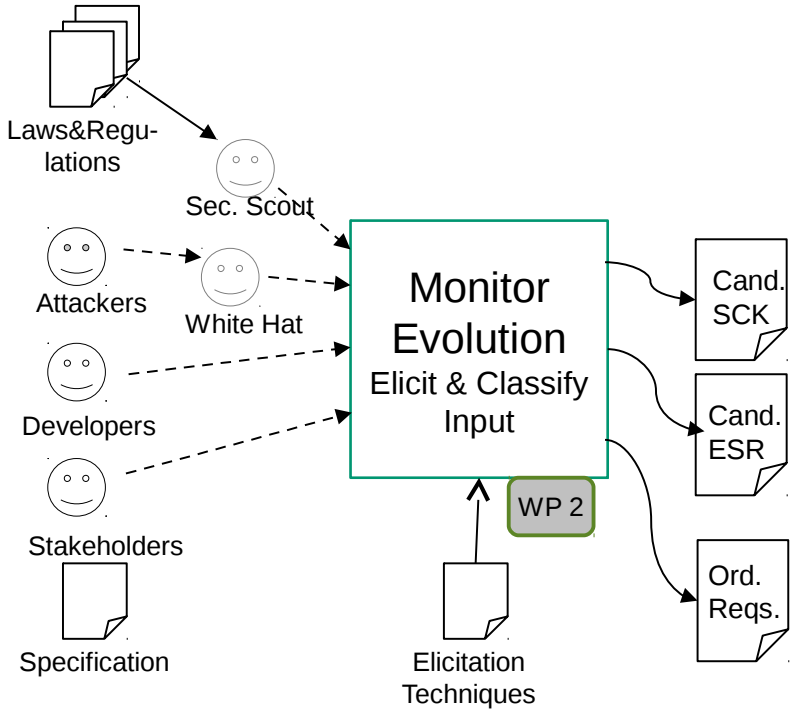
"secure encryption
= 1024 bit RSA"

Banking:

"secure encryption
= 2048 bit RSA"

"secure encryption
= 2048 bit RSA"

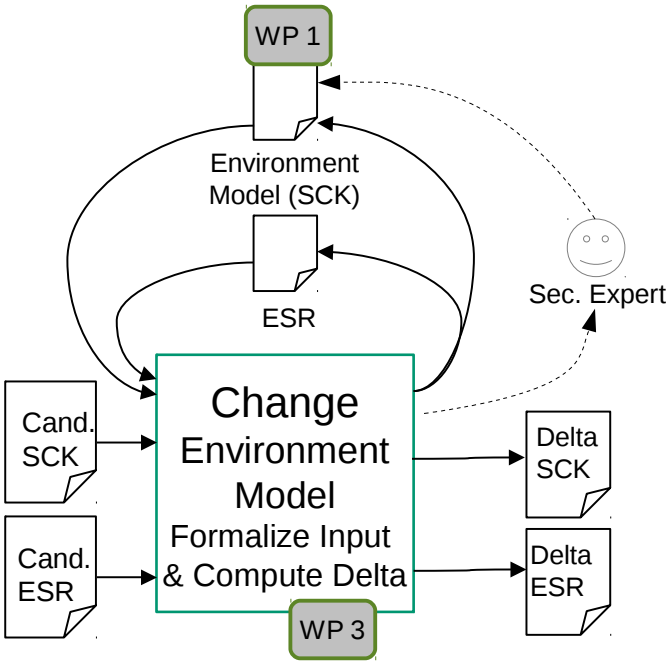
WP2: Monitor Evolution



ESR = Essential Security Requirements;
SCK = Security Context Knowledge.

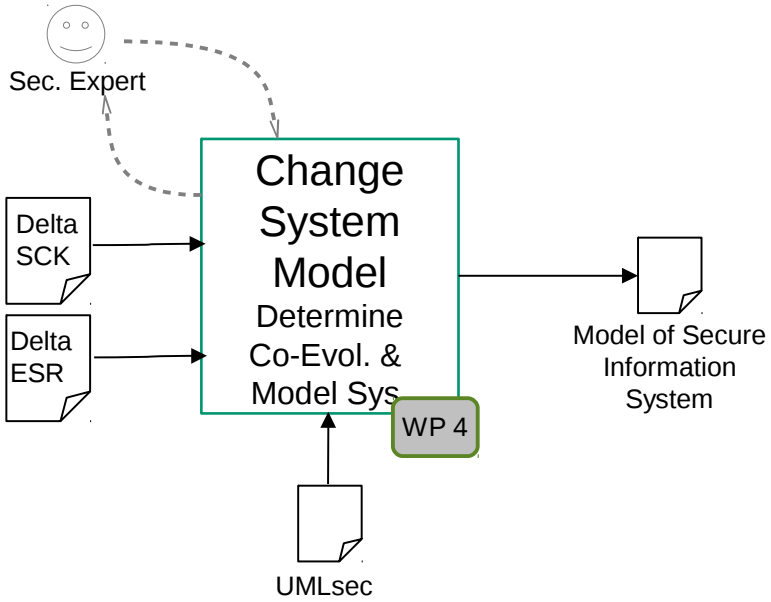
- Identification of potentially relevant knowledge sources to monitor
- Characterization of different types of knowledge and information in those sources, including an information flow overview model
- Guidance for carrying out non-automated parts of the classification, in particular when exceeding the environment model

WP 3: Change Environment Model



- Techniques and tools to formalize changes in metamodels and data
- Data model for differences between different versions of environment models
- Technique for difference computation between different versions of environment models
- Semi-automated mapping of identified potential security triggers to changes of the environment model

WP 4: Change System Model

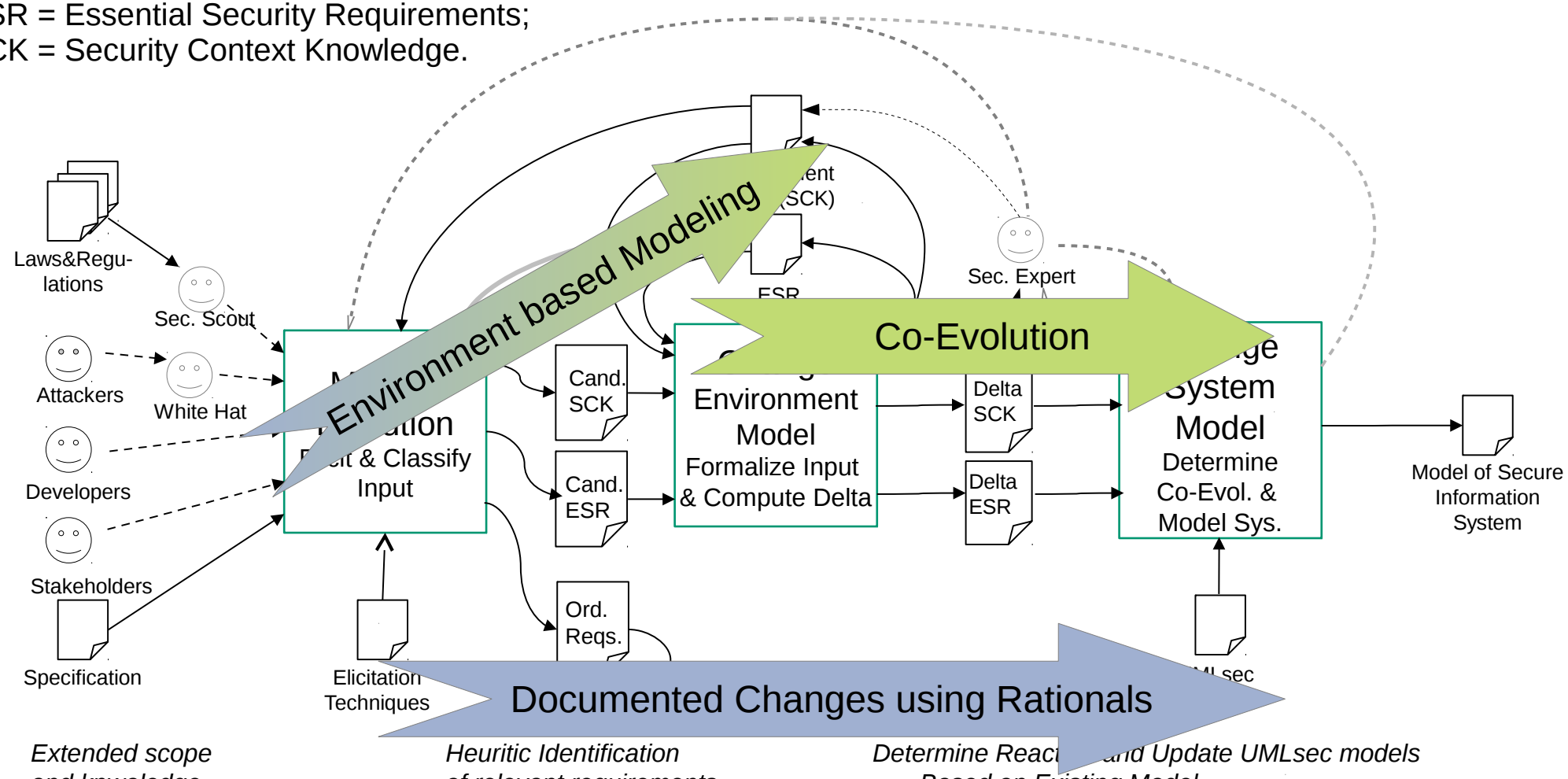


- Formalization of Evolutions and Co-Evolution
- Catalog of Environment Model Evolutions and Corresponding System Model Co-Evolutions
- Prototype for Application of Evolutions and Co-Evolutions

ESR = Essential Security Requirements;
SCK = Security Context Knowledge.

SecVolution: An Overview

ESR = Essential Security Requirements;
SCK = Security Context Knowledge.

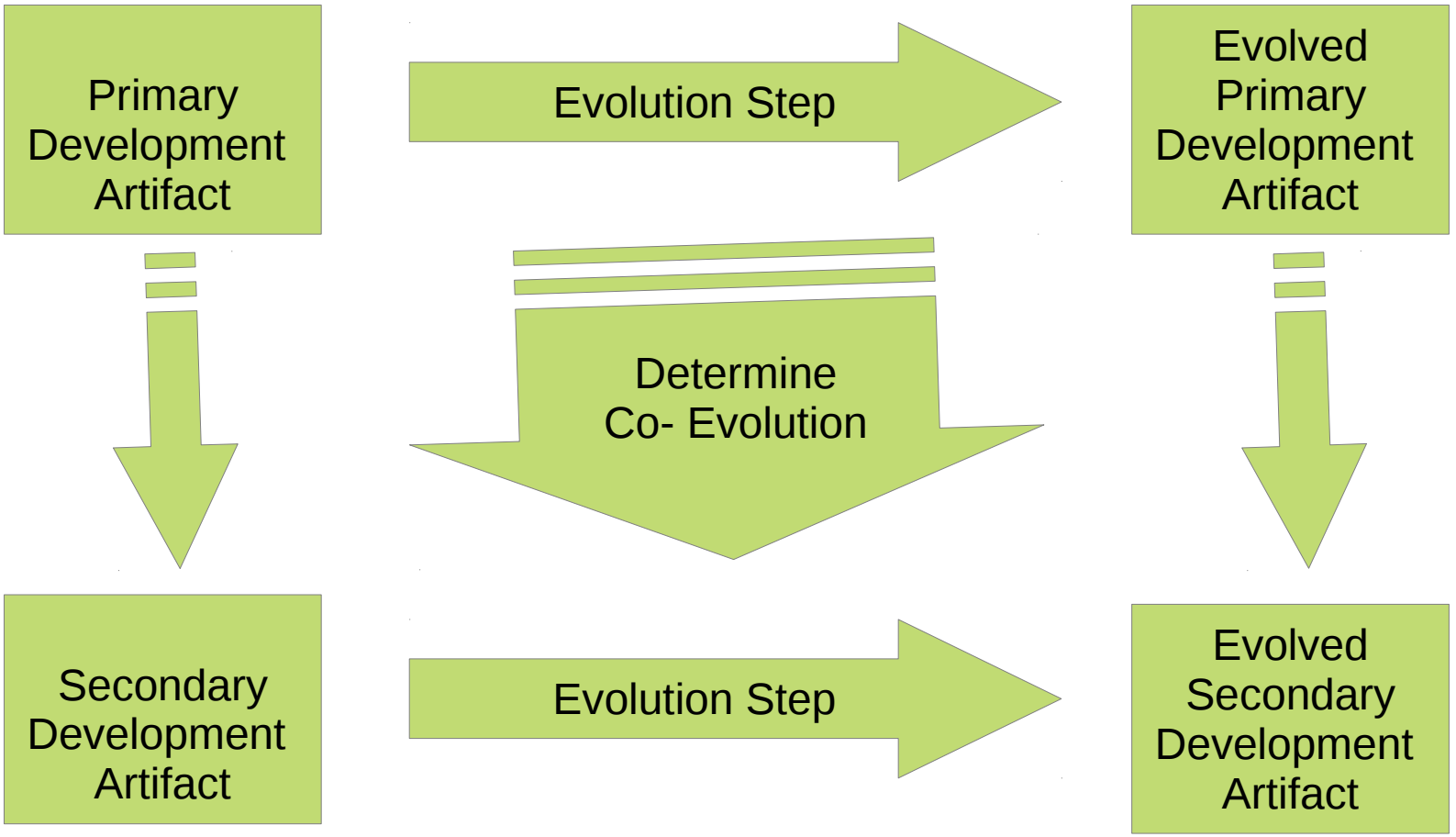


Extended scope and knwoledge sources

Heuritic Identification of relevant requirements and facts

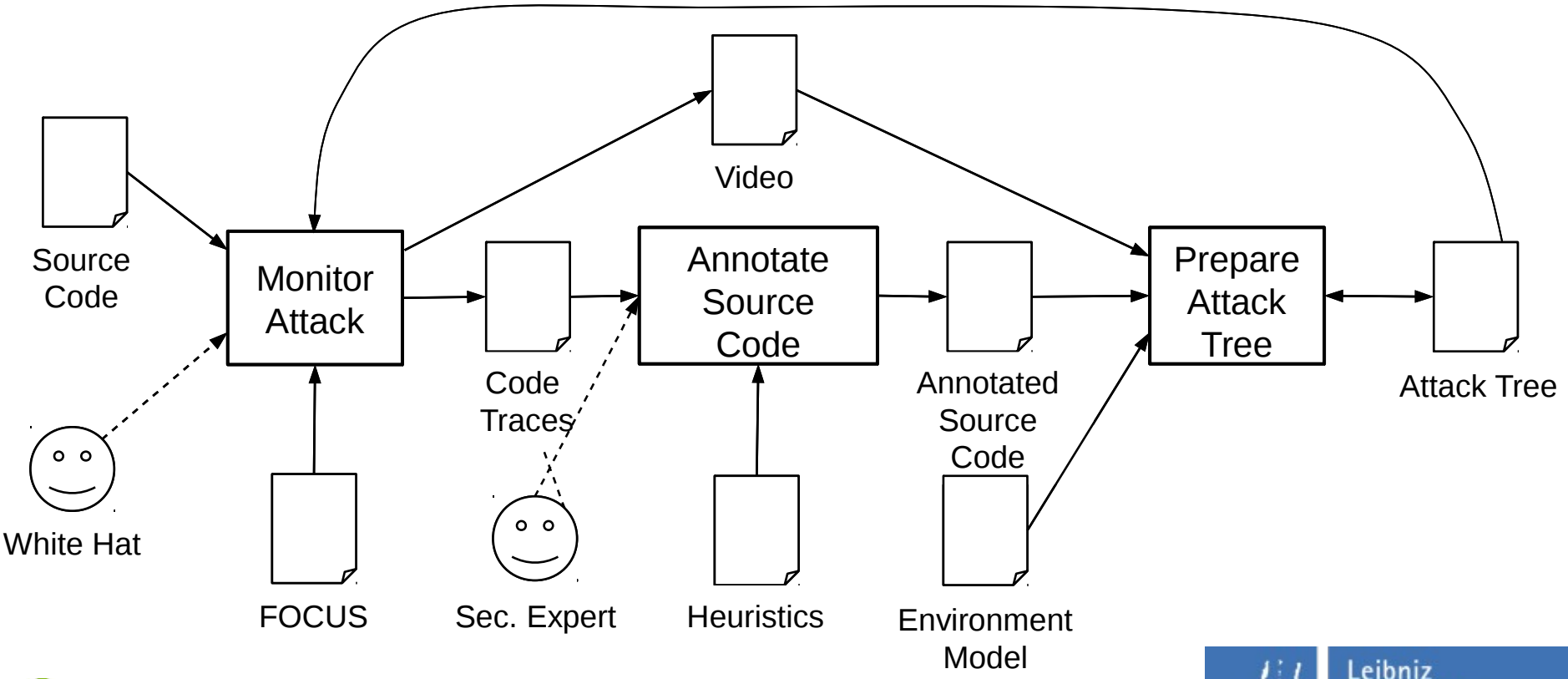
Determine React and Update UMLsec models
- *Based on Existing Model*
- *By extending Metamodel*

Co-Evolution



Rationale

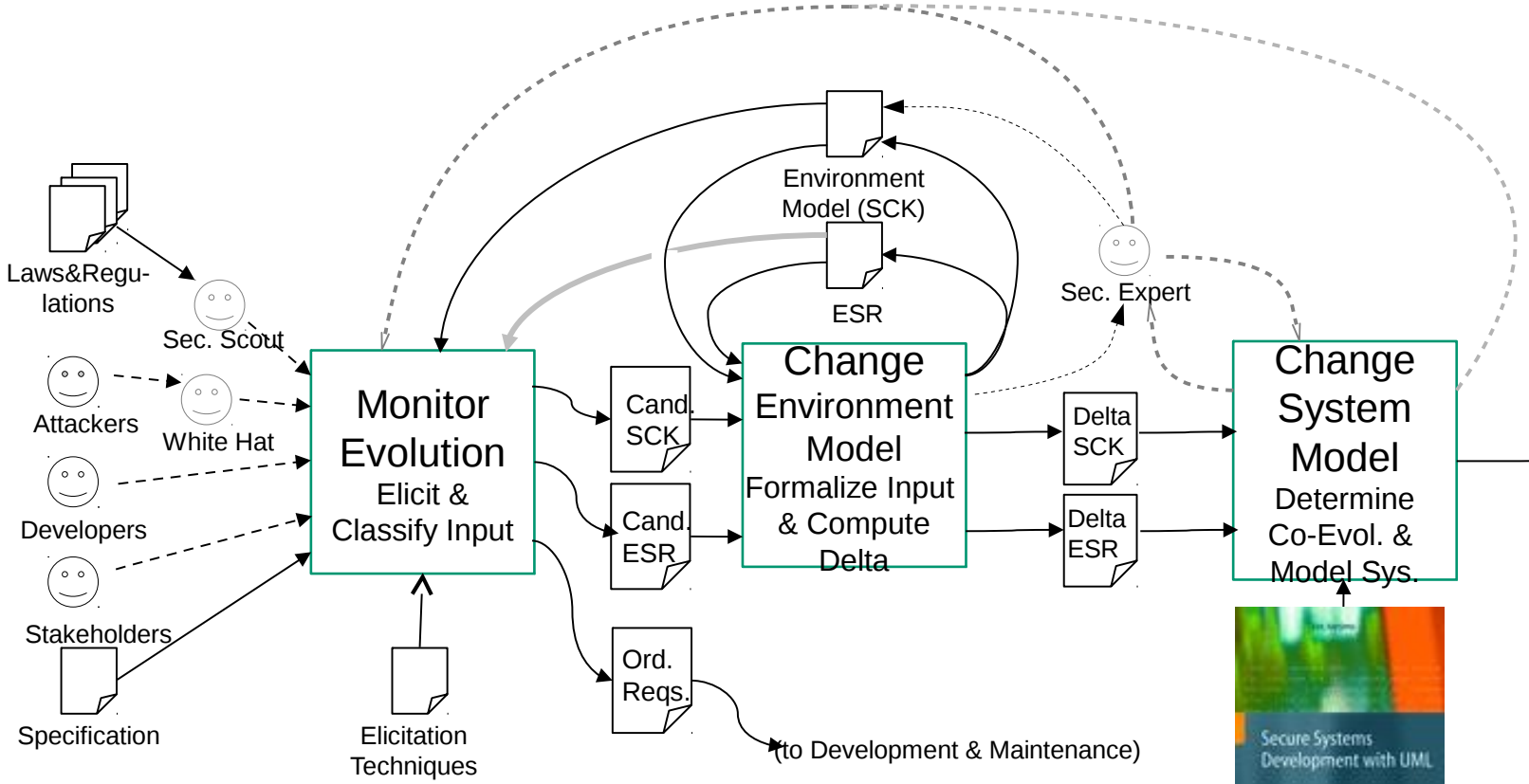
- Example: Analysis of Attacks
- Rationals as Byproduct
- Feedback: Collection of Experience



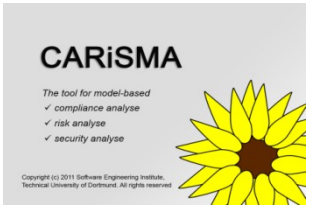
Conclusion

- Adopted Core Concepts from our preliminary work:
  - Information flow modeling
  - Reuse of experiences
  - Organizational learning
  -
- New Core Concepts:
  - Automated reaction to observed change in the environment
  - Active and lightweight elicitation as a by-product
  -

Conclusion


Laws&Regu-lations
Sec. Scout
Attackers
White Hat
Developers
Stakeholders
Specification
Monitor Evolution
Elicit & Classify Input
Elicitation Techniques
Environment Model (SCK)
ESR
Cand. SCK
Cand. ESR
Ord. Reqs.
(to Development & Maintenance)
Change Environment Model
Formalize Input & Compute Delta
Sec. Expert
Delta SCK
Delta ESR
Change System Model
Determine Co-Evol. & Model Sys.
Model of Secure Information System
HERA
JFOCUS

Secure Systems Development with UML


CARiSMA
The tool for model-based
✓ compliance analyse
✓ risk analyse
✓ security analyse

Thank You - Questions