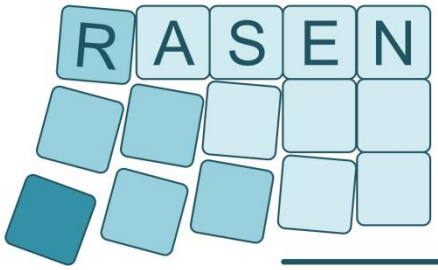


Compositional Risk Assessment and Security Testing of Networked Systems

# Deliverable D3.3.1

# Tools for Compositional Security Risk Assessment and Security Test Result Aggregation v.1

---

# Documentation and Installation Guide

| | |
|---|---|
| **Project title:** | RASEN |
| **Project number:** | 316853 |
| **Call identifier:** | FP7-ICT-2011-8 |
| **Objective:** | ICT-8-1.4 Trustworthy ICT |
| **Funding scheme:** | STREP – Small or medium scale focused research project |

| | |
|---|---|
| **Work package:** | WP3 |
| **Deliverable number:** | D3.3.1 |
| **Nature of deliverable:** | Prototype &Report |
| **Dissemination level:** | PU |
| **Internal version number:** | 1.0 |
| **Contractual delivery date:** | 2013-09-30 |
| **Actual delivery date:** | 2013-09-30 |
| **Responsible partner:** | Fraunhofer |

## Contributors

| | |
|---|---|
| Editor(s) | Bjørnar Solhaug (SINTEF) |
| Contributor(s) | Fabien Peureux (Smartesting), Martin Schneider (Fraunhofer), Fredrik Seehusen (SINTEF), Bjørnar Solhaug (SINTEF), Frank Werner (SAG) |
| Quality assuror(s) | Fabien Peureux (Smartesting), Fredrik Seehusen (SINTEF) |

## Version history

| Version | Date | Description |
|---|---|---|
| 0.1 | 13-09-11 | ToC and contents overview |
| 0.2 | 13-09-17 | Contents provided to all sections |
| 0.3 | 13-09-20 | Complete version finalized for internal review |
| 1.0 | 13-09-26 | Final version |


## Abstract

This report provides some basic information about the tools of the WP3 prototype deliverable D3.1.1 due at project month M12. The delivered tools are CORAS from SINTEF, RISKTest from Fraunhofer FOKUS, CertifyIt from Smartesting and ARIS Business Architect from Software AG.



## Keywords

Security, security risk assessment, security testing, test-based risk assessment, tool support, prototype

# Executive Summary

The overall objective of RASEN WP3 is to develop tools and techniques to support test-based and compositional security risk assessment. Deliverable D3.2.1 presents the WP3 techniques that were developed during the first year of the projects, while D5.3.1 presents the methodologies that the WP3 techniques should support. This report accompanies the D3.3.1 prototype deliverable, and gives an overview and introduction to the four tools of that deliverable.

The set of tools are as follows:

- The CORAS tool from SINTEF, supporting model-driven risk analysis
- The RISKTest tool from Fraunhofer FOKUS, which is a tool integration platform for risk-based security testing
- The CertifyIt tool from Smartesting for model-based security testing
- The ARIS Business Architect from Software AG, supporting security assessment and risk modeling of software and IT systems

# Table of contents

**TABLE OF CONTENTS** ..... **5**

**1 INTRODUCTION** ..... **6**

**2 CHARACTERISTICS OF THE IDENTIFIED WP3 TOOLS** ..... **7**

2.1 CORAS ..... 7
2.2 RISKTEST ..... 8
2.3 SMARTESTING CERTIFYIT ..... 9
2.4 ARIS BUSINESS ARCHITECT ..... 10

**3 DESCRIPTION OF THE IDENTIFIED WP3 TOOLS** ..... **11**

3.1 CORAS ..... 11
3.2 RISKTEST ..... 11
3.3 SMARTESTING CERTIFYIT ..... 12
3.4 ARIS BUSINESS ARCHITECT ..... 13
3.4.1 Presentation ..... 13
3.4.2 Installation Guidelines ..... 13
3.4.3 User Guide ..... 13
3.4.4 Features within the RASEN Project ..... 15

**4 CONCLUSION** ..... **17**

# 1 Introduction

This report is a brief documentation of and introduction to the RASEN WP3 prototype deliverable D3.3.1. The prototypes are developed to provide support for the methods and techniques that are also developed in this work package. The reader is referred to deliverable D3.2.1 for an overview of the WP3 research results after the first year of the RASEN project.

The prototypes presented in this report serve as a part of the RASEN tool-box for security risk assessment and security testing that is developed in the context of WP5. WP5 defines the common RASEN data meta-model that will be used for integrating the tools by facilitating the communication between them. An important part of the RASEN prototype development is therefore to provide support for exporting and importing data to and from the common RASEN data model.

The tools that are presented in the next two sections are CORAS, RISKTest, Smartesting CertifyIt and ARIS Business Architect. In Section 2 we give a brief overview of the main characteristics of the tools, and in Section 3 we present the tools in some more details, give installations and user guidelines, and explain the planned and current status for the development of tool features relevant in WP3. Finally, in Section 4 we conclude.

# 2 Characteristics of the Identified WP3 Tools

In this section we give an overview of the RASEN tools relevant for WP3, providing some basic general information and technical information, as well as other additional information that may be useful.

## 2.1 CORAS

| General information | |
|---|---|
| Name | CORAS tool |
| Provider | SINTEF |
| Topic addressed | Model-based risk assessment |
| Description | The tool is based on Eclipse and the GMF/EMF framework, but it is distributed as a stand-alone tool |
| License | Eclipse Public License v1.0 (http://www.eclipse.org/legal/epl-v10.html) |
| Website | http://coras.sourceforge.net |
| **Technical information** | |
| Download site | http://coras.sourceforge.net/downloads.html |
| OS | Tested on Windows; a non-tested distribution is also available for Linux |
| Technology environment | The tool needs Java |
| Other dependencies | None |
| **Additional information** | |
| Known issues/risks | None |
| Additional useful information | None |

## 2.2 RISKTest

| General information | |
|---|---|
| Name | RISKTest 0.1 as an extension to Fokus!MBT |
| Provider | Fraunhofer FOKUS |
| Topic addressed | Tool Integration Platform for Risk-Based Security Testing |
| Description | RISKTest is a tool integration platform for risk-based security testing. It consists firstly of the management of traces and other services evaluating and analyzing these. It supports exchange formats specified in D5.2.1. |
| License | RASEN project partner can obtain a license for the project duration. |
| Website | N/A |
| **Technical information** | |
| Download site | N/A |
| OS | Win, Linux and Mac |
| Technology environment | Java (1.6 and newer) 32-bit, Juno Eclipse Modelling |
| Other dependencies | Papyrus, TestingTech, ProR, CORAS, CReMa |
| **Additional information** | |
| Known issues/risks | N/A |
| Additional useful information | N/A |

## 2.3 Smartesting CertifyIt

| General information | |
|---|---|
| Name | Smartesting CertifyIt |
| Provider | Smartesting |
| Topic addressed | Model-Based Testing solution |
| Description | The tool is composed by a Rational Software Architect plugin for modeling activities, and a standalone Java application for the test generation and test case management |
| License | RASEN project partner can obtain a license for the project duration. |
| Website | www.smartesting.com |
| **Technical information** | |
| Download site | www.smartesting.com |
| OS | Win or Linux |
| Technology environment | Rational Software Architect v8.0.x and v8.5.x, EMF compliant<br>JAVA 1.6, 1.7 compliant |
| Other dependencies | N/A |
| **Additional information** | |
| Known issues/risks | N/A |
| Additional useful information | N/A |

## 2.4 ARIS Business Architect

| General information | |
|---|---|
| Name | ARIS Business Architect + RASEN Model Extension |
| Provider | Software AG |
| Topic addressed | Security Assessment and Risk Modeling of Software and IT Systems |
| Description | The model extension is based on the ARIS Business Process Analysis Platform (http://www.softwareag.com/corporate/products/aris/bpa/default.asp), a proprietary solution of Software AG and provides an interface to model risk assessment of IT security systems. |
| License | Proprietary |
| Website | http://www.softwareag.com/corporate/products/aris/bpa/architect_design/overview/default.asp |
| **Technical information** | |
| Download site | Download site of the RASEN Model Extension https://project.sintef.no/eRoomReq/Files/ikt2/RASEN/0_33361/SAG%20Prototype.zip |
| OS | Windows, Linux, (Any OS supported by the ARIS Business Architect) |
| Technology environment | None |
| Other dependencies | None |
| **Additional information** | |
| Known issues/risks | None |
| Additional useful information | None |

# 3 Description of the Identified WP3 Tools

## 3.1 CORAS

In the context of RASEN WP3, the CORAS tool will be extended and further developed to provide support for test-based and compositional security risk assessment. For a presentation of the current, official CORAS tool, the reader is referred to deliverable D4.3.1. That deliverable also gives the installation guidelines and an introductory user guide. Instead of repeating anything here from D4.3.1, we present in this section the planned features of the CORAS tool in WP3, as well as the current status of the development.

**Planned Features**

The following features are currently the planned extensions of the CORAS tool within RASEN WP3:

- Add support for importing and exporting CORAS models to models of the common RASEN data-meta model as a means for communicating with the other prototypes of the RASEN tool-box.
- Add support for updating CORAS models based on security test results. The development of this feature is broken down into the following tool development tasks:
    - Add support for the identification of new vulnerabilities with an estimate of their severity based on security test results.
    - Add support for the removal of obsolete vulnerabilities from the CORAS models based on security test results.
    - Add support for the specification of functions to aggregate values of security metrics to validate or update the current risk estimates in CORAS models. The functions should facilitate test-based risk assessment for both active testing (using security measurements) and passive testing (using security indicators).
- Add support for combining CORAS models from different CORAS projects based on the RASEN compositional proof rules.

**Current Status**

As described in more details in the report for deliverable D4.3.1, an export from the CORAS model to the current version of the RASEN data meta-model has been implemented. The function takes a CORAS project as input and produces an XML-file representing the RASEN data model as output.

The CORAS features for supporting compositional and test-based security risk assessment have yet to be developed. In order to implement such functionalities in the tool, we need to further develop the WP3 techniques that we aim to support (cf. the current status of this as reported in deliverable D3.2.1). We have started to use the CORAS tool in test-based risk assessment, but currently the risk analysts need to interpret the test results manually in order to use the data as input to the risk models.

Hence, the main tasks in further developing the CORAS tool in WP3 can be summarized as follows:

- Develop support for importing RASEN data models to the CORAS tool.
- Develop support for aggregating security test results in the CORAS tool.
- Develop support for combining risk models according to the compositional proof rules.

## 3.2 RISKTest

The RISKTest prototype is developed to support methods and techniques in both RASEN WP3 and WP4. For the presentation of the prototype, the installation guidelines and user guide, the reader is referred to the D4.3.1 documentation.

**Current Status**

- The trace management (the creation, deletion of traces) is directly integrated in each of the integrated tools. Additionally, traces are visualized in the trace explorer by a tree structure and can be used for navigation. A filter mechanism can be used to find traces.
- RISKTest allows bidirectional navigation between related elements. Trace source and target can be visualized directly within the integrated tools.
- Creating traces can be done manually or automatically, e.g. by model-based test generation services.
- The traces are defined on basis of a trace meta-model that distinguishes the individual elements that are allowed to be part of a trace and allow for distinguishing different trace types.
- The trace meta-model defines a service interface that allow for introducing services that query the trace model for information (e.g. services for coverage analysis or impact analysis).
- RISKTest is extensible. That means, it provides a well-defined interface to easily integrate other tools that are based on Java and Eclipse.

**Planned Features**

The relevant features within the RASEN project are the following:

- Support for the exchange format for RASEN Data Integration Model specified in RASEN deliverable D5.4.1
- Dashboard for security testing result aggregation
- Implementing query algorithm on basis of domain meta-models
- Advanced network hierarchical visualization of trace model

## 3.3 Smartesting CertifyIt

This section introduces the tool CertifyIt developed and provided by the company Smartesting to generate security test cases from vulnerability risk assessment, and to produce test results, which can actively contribute to identify, estimate and finally treat the risk of the tested application. The test generation features of the tool (including installation and user guide) are introduced in the deliverable D4.3.1. That is why the rest of this section only deals with the specific RASEN development dedicated to risk assessment features.

The extensions to the Smartesting tool to complement the risk picture basically consist of calculating and exporting test data and results to the risk assessment tool, which will aggregate them to provide accurate security indicators and risk metrics. Currently, the expected test data for risk assessment are the following:

- Purpose of each test case trace in terms of targeted vulnerability (risk traceability matrix) and targeted part of the application under test (organic traceability matrix).
- Executed test case traces including all performed actions with potential filled data.
- Expected effects of each action of the test traces, from the behavioral model point of view.
- Observed effects of each action of the test traces, from the execution point of view.
- Test verdict in terms of identification of test success (discovered vulnerability) and failure (absence of vulnerability), and more generally feedback when something unusual or unexpected has occurred during the trace execution.

These test data will be published from CertifyIt using dedicated extension that will take the form of Java libraries and/or Eclipse Plug-in (with dedicated API). This API will provide the data in dedicated structured output files (XML-based) to enable, ease and automate the risk assessment processing. These developments are currently starting in order to provide an integrated tool suite by the end of the second year of the RASEN project, and to make it possible to validate the relevance of the testing artifacts to complement the risk picture.

## 3.4 ARIS Business Architect

### 3.4.1 Presentation

The ARIS Business Architect (ABA) is proprietary software from Software AG. A screenshot of the ABA with the underlying RASEN model type is depicted in Figure 1. It shows on the left hand side a list of all possible Common Weakness Enumerations (CWEs)[1] which can directly be aligned to a software component. On the right hand side (cf. Symbol Box) a selection of other components can be selected and drawn into the modeling pane in the center of the screen.

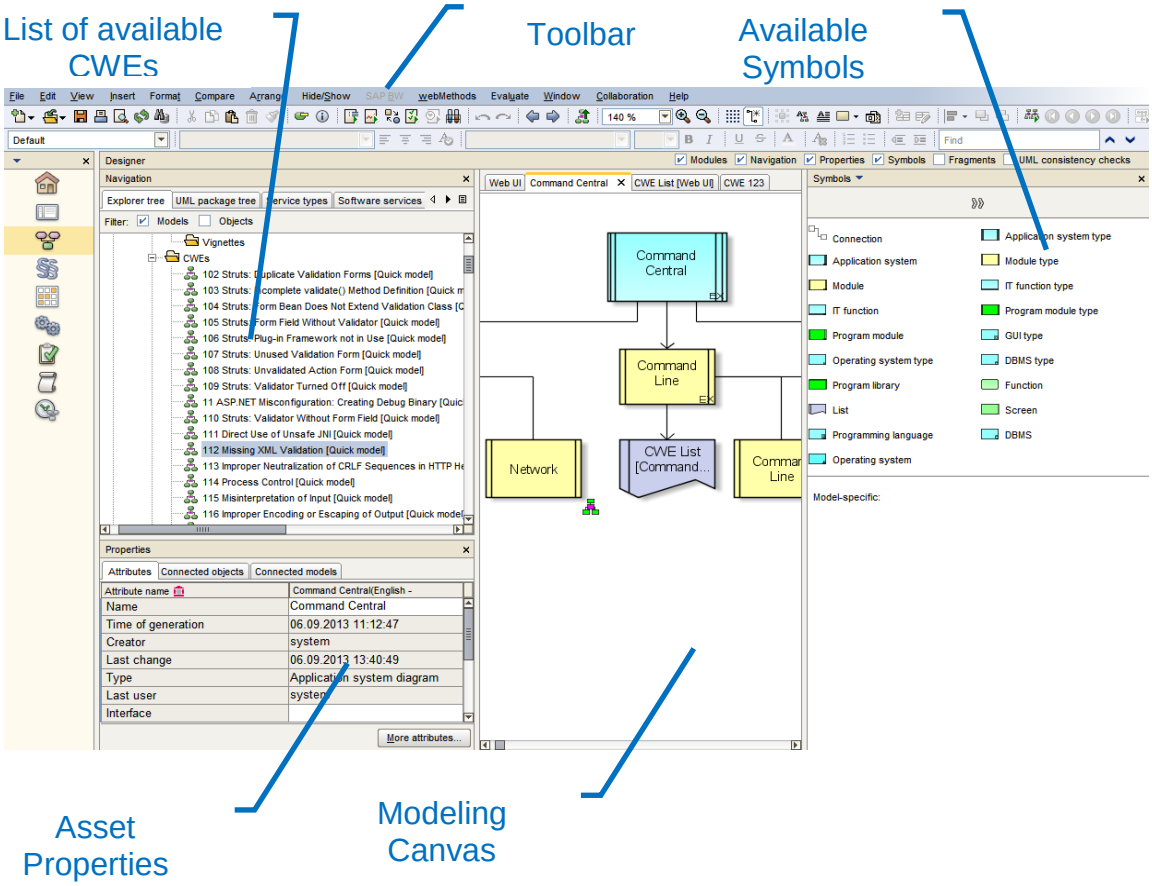


**Figure 1 – Screenshot of the Security Risk Assessment in RASEN model**

### 3.4.2 Installation Guidelines

An individual installation program can be started using the provided Setup.exe which is guiding the used through the provided setup-routine. If system files are changed during installation, you are prompted to reboot your computer after installation. In addition to that there is a detailed installation guide of how to install the ARIS Business Architect on most spread operating systems. On top of the base installation of the ARIS Business Architect, the RASEN methodology is added by importing the ZIP file which contains the base package, consisting of the reports, the definition of necessary modeling elements, the macro, and a preliminary set of already defined CWEs.

### 3.4.3 User Guide

The way how the RASEN model extension can be used is exemplified, using a model of Software AG's component called Command Central.

[1] http://cwe.mitre.org

The Product Model builds the base of the proposed modeling approach. The respective product is modeled as the root entry of the model; the corresponding components are modeled as child entries. At least one so called Component Template which specifies a special type of component is assigned to each component. Additionally a list of CWEs is assigned to the component. This list represents the union of all relevant CWE for this component which are automatically derived from the Component Template. This list can be modified in sense of deleting irrelevant CWEs or extending them according to the needs of the security expert doing the risk assessment.

The present model type represents a program under test as a set of components with their hierarchical relation. This relation is not restricted to one level but as several layers of sub-components building are feasible (subcomponents, sub-subcomponents, etc.), this can also be reflected within the model. Each component has a list of CWEs defined by the Component Template as denoted earlier. The initial content of these lists is defined by the connected *Component Types* provided as a *Risk Template.*

The product is now tested for all CWEs in its components lists. Afterwards the test results are imported into the tool and consequently all irrelevant CWEs where deleted from the property list.

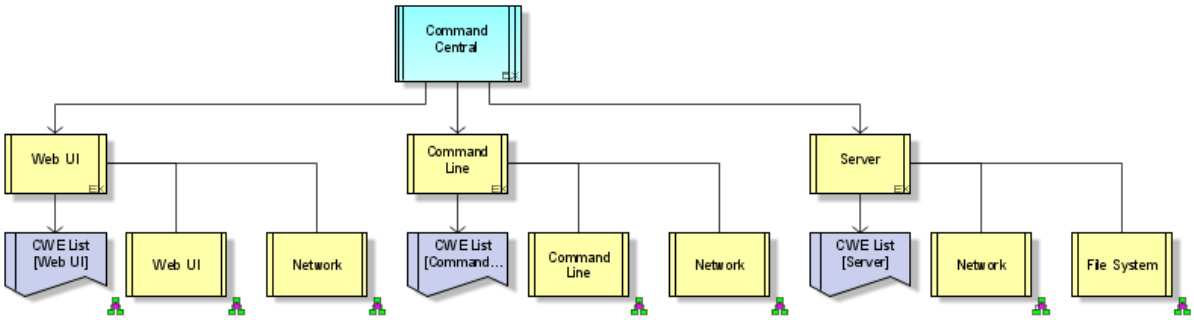


**Figure 2 – Model of the "Command Central" Product**

A Component Type Model is used to classify components. A Component Type Model consists of a pre-defined list of CWEs as well as of a pre-defined vignette. A vignette[2] or vignette scorecard is a kind of table where every entry out of 8 is assigned to a number. This vignette is used for further computations.

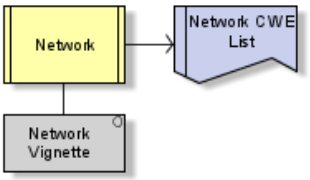


**Figure 3 – Component Type Model for the Network Component with Network Vignette and CWEs**

A CWE List is model that contains a list of references to CWE Models. CWE Lists are assigned to Component Types and Components where the lists that are assigned to component types are modifiable.

[2] http://cwe.mitre.org/cwraf/data/vignettes.html

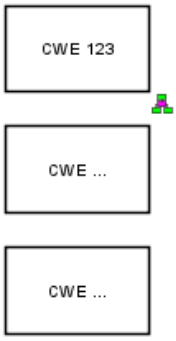


**Figure 4 – List of relevant CWEs defined by the Component Type**

A CWE Model contains all relevant information as the ID, name and technical impacts about one CWE from the CWE database. The technical impacts where mapped to 8 technical impacts to fit the vignette scorecard schema and later on used for score computations. For the example above this is displayed as an excerpt in Figure 5.

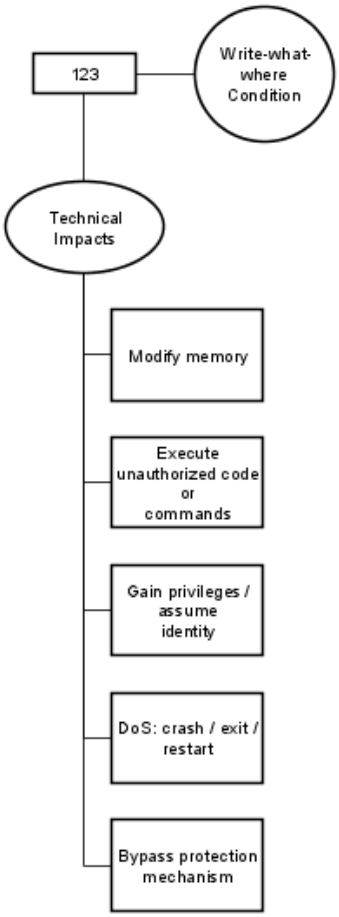


**Figure 5 – CWE consisting an ID and Technical Impacts**

### 3.4.4 Features within the RASEN Project

The results of the development within RASEN are encompassed in a new model type which provides all relevant aspects for security modeling. As a base tool the ARIS Business Architect (ABA) from Software AG is chosen.

The provided modeling approach is multi-layered starting from the product down to the components hereby forming a hierarchical structure. A security risk assessment is done for each component individually with the help of component template, containing all relevant security treads known for this type of components. A conceptual view on the modeling is provided in the following Figure 6.

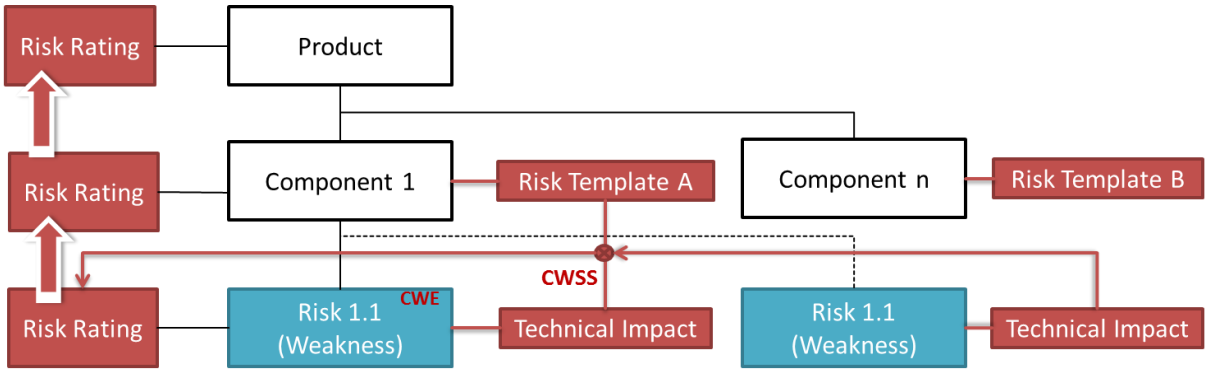


**Figure 6 – Concept of Risk Modeling Using Risk Templates**

As stated above, each Component is assigned a specific *Risk Template* describing likely risks which account for this component type. When doing the risk modeling (selection of a template and assign it to a component) one can chose from a number of already present component types defined in the system.

The proposed approach of using Risk Templates which correspond to component types relies on the concept of CWE (Common Weakness Enumeration). They provide a unified, measurable set of software weaknesses that is enabling more effective discussion, description, selection, and use of software security tools and services that can find these weaknesses in source code and operational systems as well as better understanding and management of software weaknesses related to architecture and design.

In addition to that, The Risk Templates are enriched using the concept of vignettes used to provide a shareable, formalized way to define a particular environment, the role that software plays within that environment, and an organization's priorities with respect to software security. It identifies essential resources and capabilities, as well as their importance relative to security principles such as confidentiality, integrity, and availability. For example, in an e-commerce context, 99.999% uptime may be a strong business requirement that drives the interpretation of the severity of discovered weaknesses.

This new modeling concept is illustrated, by applying it to one of Software AG's products called *Command Central*, a central monitoring and management application which interconnects all web Methods products and is used to control different servers.

# 4 Conclusion

In this report we have given an overview of the RASEN WP3 tools that are delivered as prototype deliverable D3.1.1. In context of WP3 these tools are developed to support the techniques of this work package for compositional and test-based security risk assessment. Together, the WP3 tools and techniques shall support the RASEN methodologies that are developed in WP5.

The tools presented in this deliverable are CORAS (SINTEF), RISKTest (Fraunhofer FOKUS), CertifyIt (Smartesting) and ARIS Business Architect (Software AG). In addition to give an introduction to the features and purposes of these tools, we have described the further development goals and the current status of these tools in WP3.