

1 ARIS Business Architect with RASEN Plugin

General information	
Name	ARIS Business Architect + RASEN Plugin
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, 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_alfabet/bpa/overview/default.asp
Technical information	
Download site	Download site of the RASEN Model Extension https://project.sintef.no/eRoomReq/Files/ikt2/RASEN/0_48ae6/Y3-SAG%20Tool%20Deliverable%20RASEN.zip
OS	Web-based solution, server installation supports 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	An in-depth description exists at the ARIS Community: http://www.ariscommunity.com/users/frankwerner/2015-07-16-innovative-modeling-approach-security-testing-networked-systems

1.1 Presentation

The ARIS Business Architect (ABA) is proprietary software from Software AG. A screenshot of the ABA with the different modeling aspects 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.

¹ <http://cwe.mitre.org>

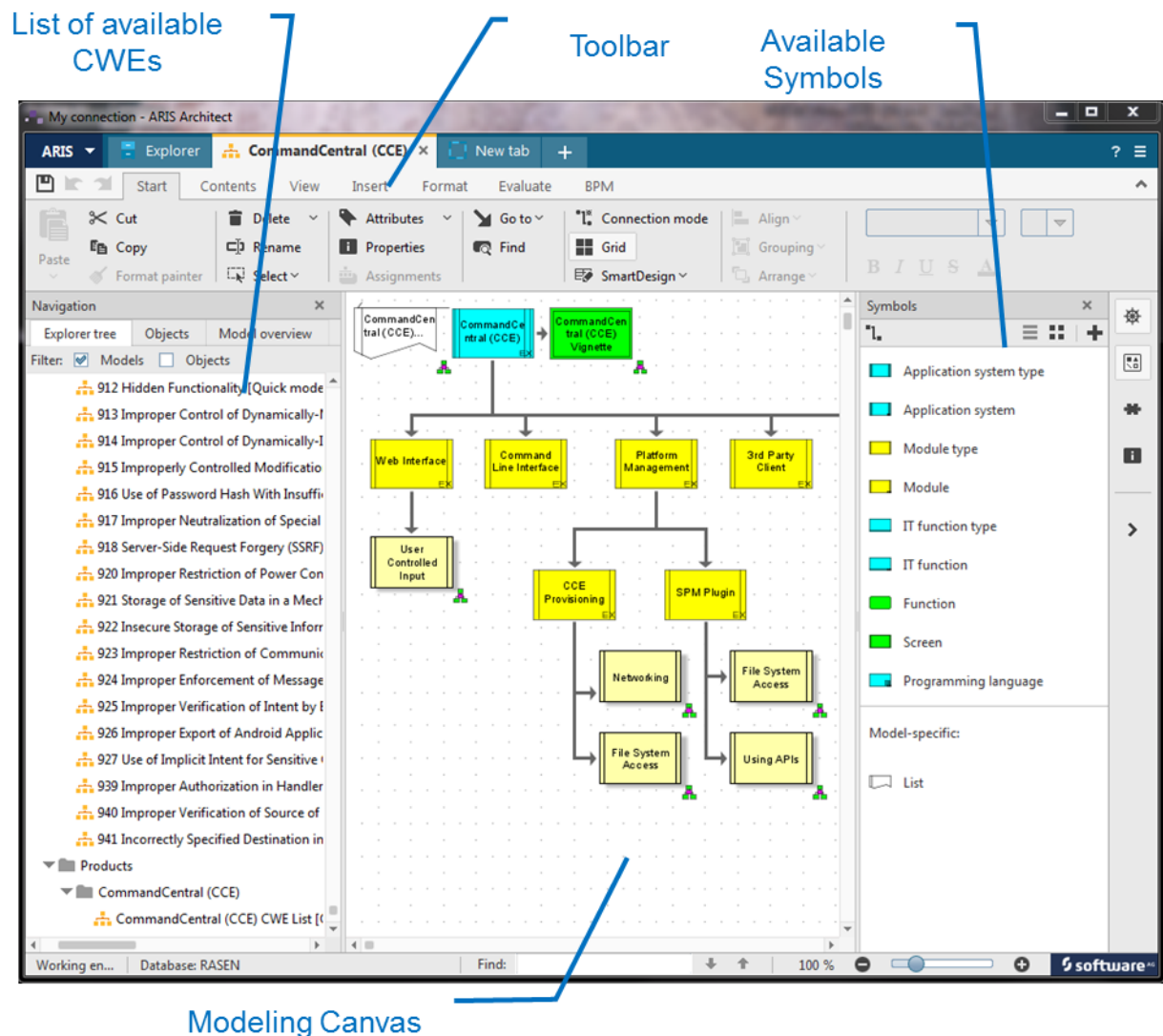


Figure 1 – Screenshot of the Security Risk Assessment in RASEN model

1.2 Installation Guidelines

An individual installation program can be started using the provided Setup.exe which is guiding the user 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 RASEN artefacts from a ZIP file which contains the base package, consisting of the reports, the definition of necessary modeling elements, the macro, a preliminary set of already defined CWEs, and a predefined set of generic component types previously generated.

1.3 User Guide

The Product Model builds the base of the proposed modelling approach. The respective product is modelled as the root entry of the model; the corresponding components are modelled as child entries (cf. Figure 4). An exemplary RASEN model of the Command Central Component is shown in the figure below, providing a full detailed description of the Software AG's product, the CCE Vignette, the component tree and the final CWSS scoring.

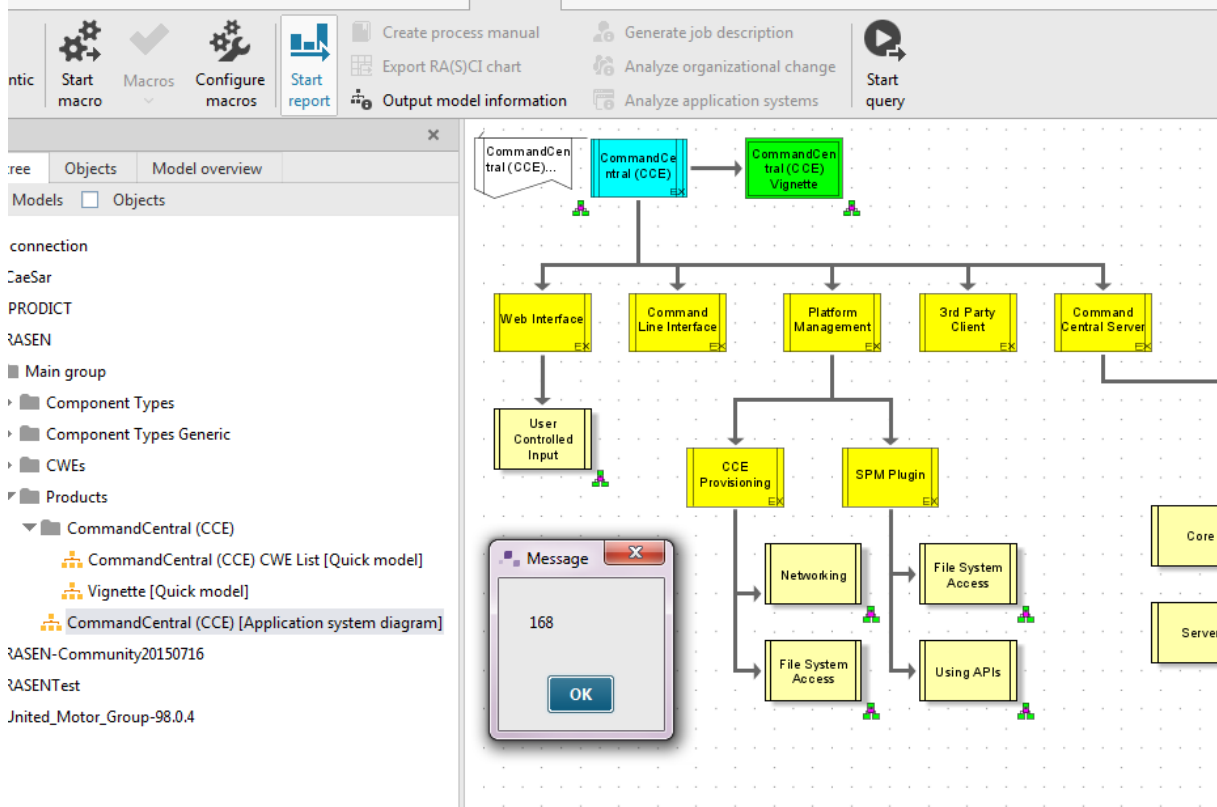


Figure 4 – The final product model with the resulting CWSS Score (CCE Score 168)

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 were deleted from the property list. A CWE Model contains all relevant information as the ID, name and technical impacts about one CWE from the CWE database. The technical impacts were mapped to 8 technical impacts to fit the vignette schema and later on used for score computations. A clipping of the vignette is shown in the figure below.

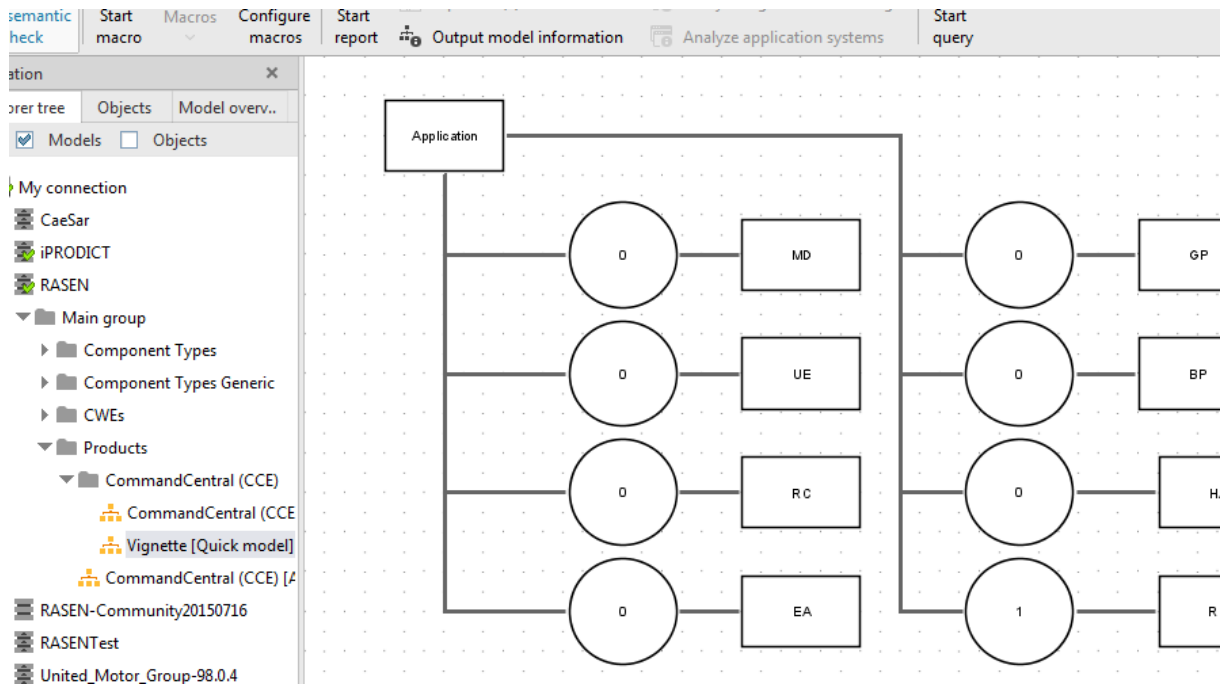


Figure 2 – The Product’s Vignette containing information about the deployment scenario

The most frequently used components are defined as generic components which can be used as a kind of library to quickly instantiate a new product with components and accelerate the modelling effort. As shown in the figure below, each Generic Component Type consists of a set of assigned CWEs and the assignment follows best practices.

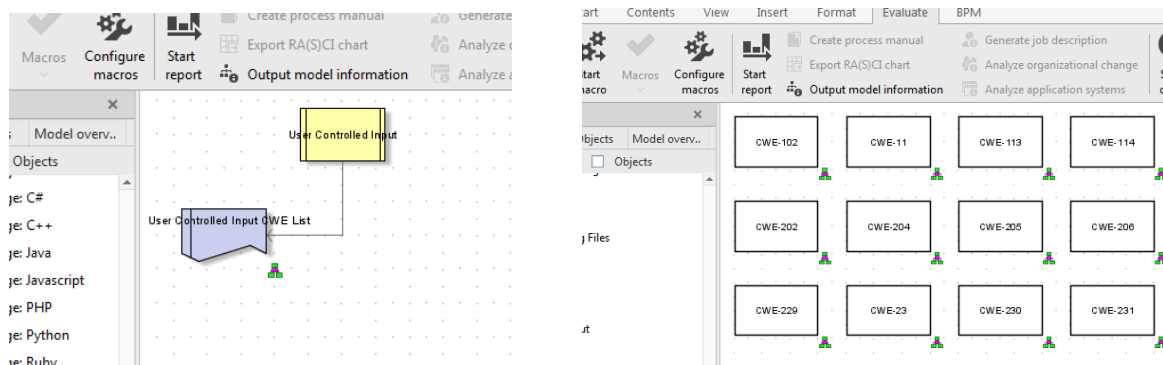


Figure 3 – ARIS Security Risk Assessment: the left the associated CWE list for the generic “Authentication” type; right: Clipping of CWEs linked to the “Authentication” type

The following functionality is implemented as either Reports (run on the ARIS server) or as Marcos (executed in the ARIS client):

- New Product – A wizard which supports the creation all necessary templates and directory for the security risk assessment of a new product
- New Component Type – A Wizard to support the creation of defining user-specific component types
- Import CWE Database --.Import and update the ARIS RASEN CWE database with inputs obtained from the MITRE CWE database

- Import Component Types – Import the set of generic component types from an external file or database
- Union Components – Compute the aggregation of all components
- Evaluate: The functionality which computes from the lower level aggregated and the vignette the CWSS score of the modeled product

An exemplary RASEN model of the Comment Central Component is shown in the figure below, providing a full detailed description of the Software AG's product, the CCE Vignette, the component tree and the final CWSS scoring.

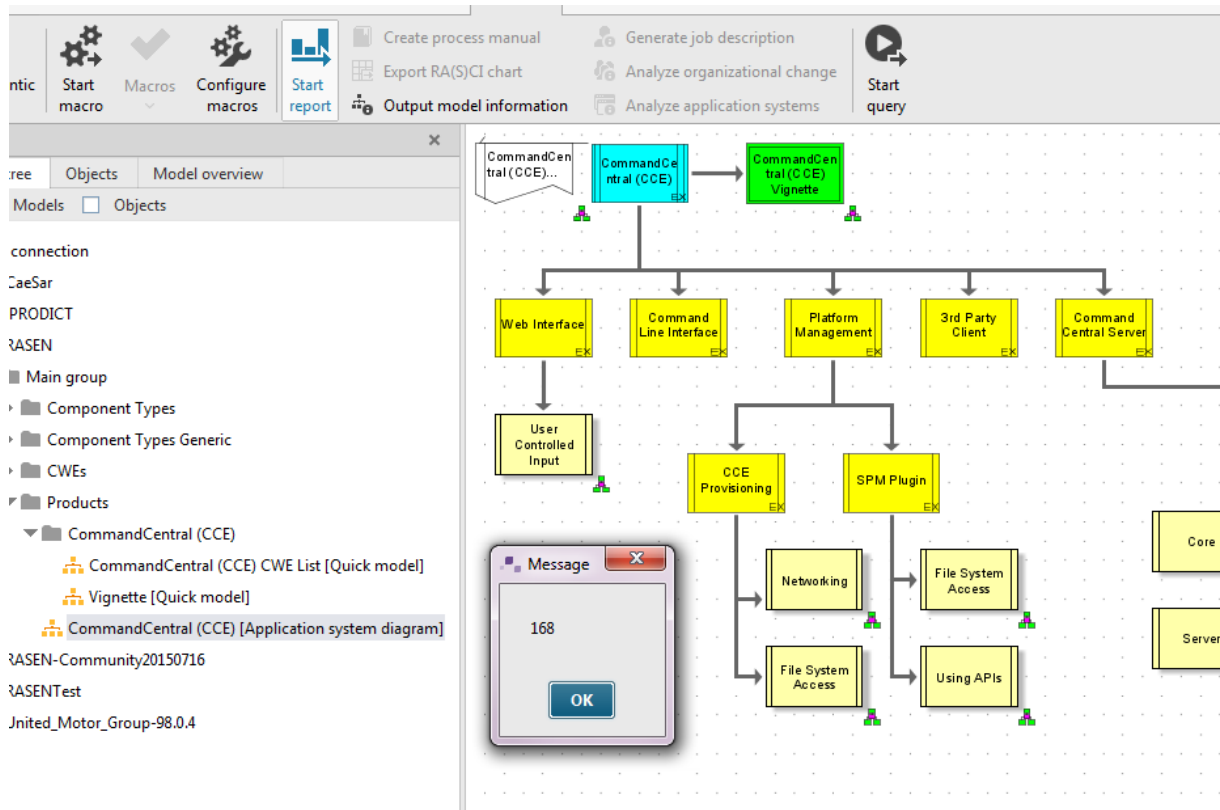


Figure 4 – The final product model with the resulting CWSS Score (CCE Score 168)