SecTro2

USER MANUAL FOR “SECTRO2” V2.0

Updated on: 20/10/2013

Viktoras Malinauskas

Contents

Introduction

"SecTro2" is a CASE tool, which allows system modelling using Secure Tropos methodology. Besides standard modelling activities it also aids developer in validating created models and running various analyses against them. "SecTro2" supports generating graphical images as well as producing Word® and PDF reports of the created models and their features. This document introduces the tool by showing the most useful features and their usage.

Installation

System requirements

- Windows® XP, 7 or 8 (32/64bit)
- Pentium III or equivalent processor (Pentium 4 or equivalent processor recommended)
- 350 MB of free hard disk drive (HDD) space for the installation and "SecTro2" database
- At least 512 MB of free memory (RAM) (1024 MB recommended)

Detailed installation instructions are available at http://securetropos.org/sectro2-tool/downloads/.

Running the tool

After the successful installation of the "SecTro2" it can be launched from the Windows® start menu: **Programs – SecTro2 Modelling Toolkit (Standalone) – SecTro2 Modelling Toolkit.**

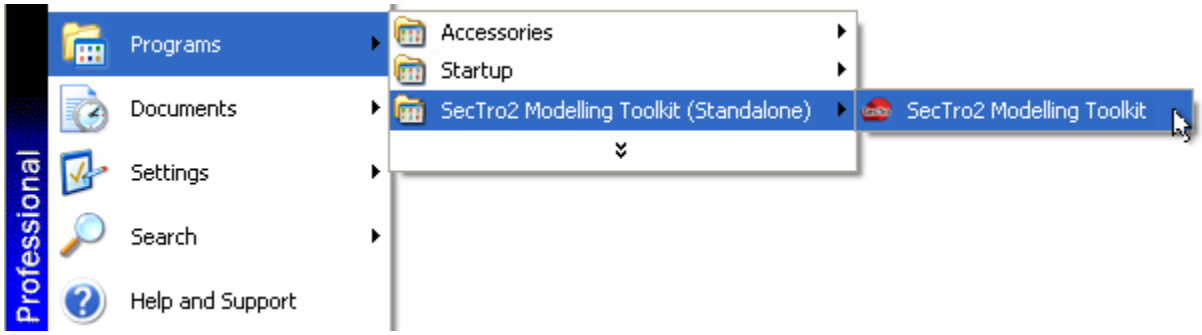

Figure 1. Launching "SecTro2" in Windows® XP.

Introduction to the Graphical User Interface (GUI)

The “SecTro2” graphical user interface comprises of the six main parts:

1. Main menu
2. Component bar
3. Quick-access toolbar
4. Model explorer
5. Modelling toolbar
6. Modelling area

The main menu

The main menu is located on the top right of the application window (Figure 2). It contains mostly used functions, such as creating new model, saving model, exiting the application, renaming the modelling object, etc. The contents of the main menu depends on the component which is currently active. The separation of functions allows easy and quick access to the functions related to the currently performed activity in the tool.

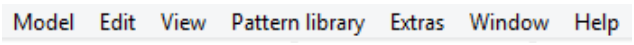

Figure 2. The main menu in the modelling component.

Component bar

The component bar contains buttons, which allow switching between various components of the tool (Figure 3). Each component is a separate section of the tool, which has its own purpose. The “SecTro2” features three components:

1. Modelling component – this component is designated for modelling activities, e.g. manipulating models and performing modelling;
2. Analysis component – represents the interface for running various analyses against the created models;
3. Import/export component – this component has functions to import and export models. Some of the use cases include model sharing or model backup. The import/export component also provides access to the model reports generation facility.

Figure 3. The component bar contains buttons for component switching.

Quick-access toolbar

The quick-access toolbar is a toolbar strip which holds the most necessary functions just one mouse click away. Its contents is dependent on the currently active component in the same way the main menu does.

The quick access toolbar in the modelling component provides access to the model manipulation features (Figure 4). Amongst the most common functions, such as create, open, save and print the model it provides access to view switching buttons for the currently active model (far left on the image).

View switching buttons represent views:

- **O** – **O**rganisational View;
- **SR** – **S**ecurity **R**equirements View;
- **SC** – **S**ecurity **C**omponents View;
- **SA** – **S**ecurity **A**ttacks View;
- **CA** – **C**loud **A**nalysis View.

Figure 4. Quick-access toolbar in the modelling component.

The analysis component has a radically different quick-access toolbar (Figure 5). It provides access to only two functions: analysis window (green tick mark) and queries/report window.

Figure 5. Quick-access toolbar in the analysis component.

The quick-access toolbar in the import/export component (Figure 6) provides three buttons (from left to right in the Figure 6):

- ADL Import – import models from an ADL file;
- ADL Export – export models to the ADL file;
- Report generation – perform report generation to a Word® or PDF file.

Figure 6. Quick-access toolbar in the import/export component.

Model explorer

Model explorer is what its name implies – it is a section in the tool's GUI which provides the means for model manipulation and organisation (Figure 7).

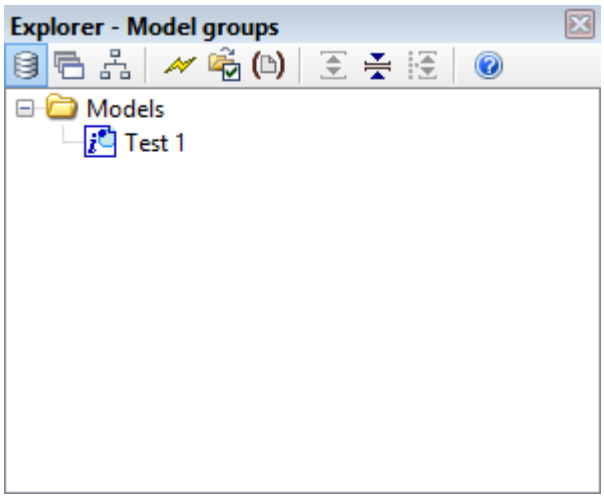

Figure 7. Model explorer with one test model named "Test 1".

Model explorer allows organising models into groups and subgroups of models. Model group is represented as an entry with a yellow folder icon and can be useful to manage projects. For example, if a project has several models, it would make sense to create a model group representing the project and put the models inside of it. An example of such structure is shown in the Figure 8.

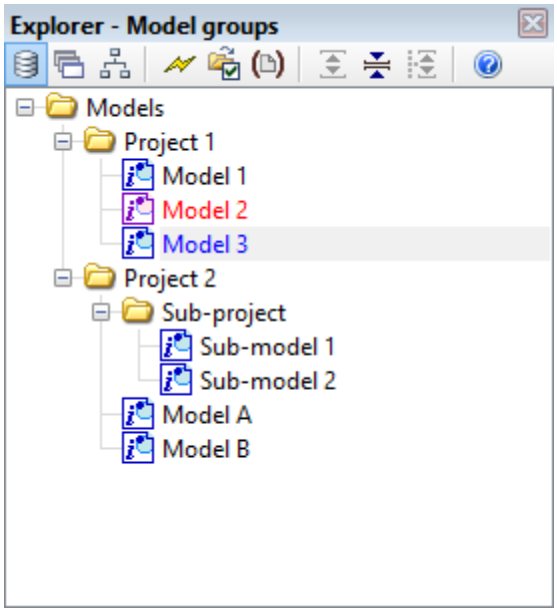

Figure 8. An example of projects' structure.

Another useful feature the model explorer has is showing which models are currently open and which ones are currently open and modified. Looking at the Figure 8, we can see that *Model 3* is open (model name is in blue colour), while *Model 2* is open and modified, but not saved yet (model name is in red colour). This feature is particularly useful if there are many models created and displayed in the model explorer.

Modelling toolbar

The modelling toolbar contains concepts, which are used to design the model (Figure 9). The concepts include both instance concepts (e.g. actor, resource, plan, etc.) as well as relational concepts (e.g. dependency link, means-end link, etc.); instance concepts being above the relational concepts in the modelling toolbar. The selection of concepts depends on the currently activated view and the concepts are active only in the modelling component.

Figure 9. Modelling toolbar showing concepts for the Cloud Analysis View.

Modelling area

The modelling area is a surface where the models are designed by creating various objects and relationships between them (Figure 10). It shows currently activated view which means that the same surface is used to create a single model.

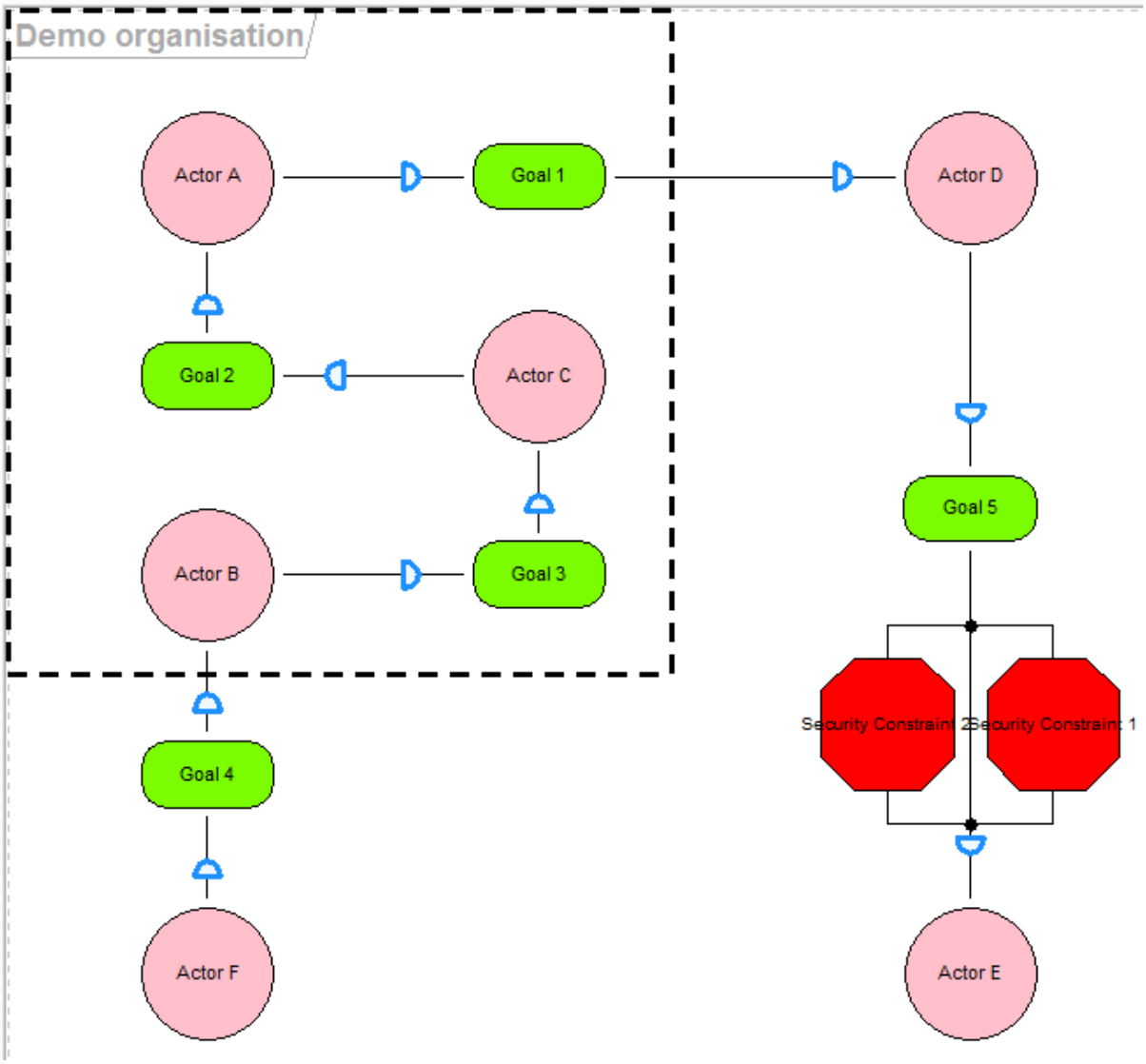

Figure 10. Modelling area showing the Organisational View.

“SecTro2” validates the models against the Secure Tropos metamodel rules. Validation is performed in two ways: during a modelling action (e.g. creating a new object or relationship on the modelling area) or running cardinality check analysis manually. When the validation fails during the modelling action the tool will produce an error message similar to the one shown in the Figure 11, and the modelling action will be cancelled. In the more complex cases it might be required to run the validation manually. The manual validation is called cardinality check and it can be run from the analysis component. Check “Running analysis against the model” section for steps how to achieve that.

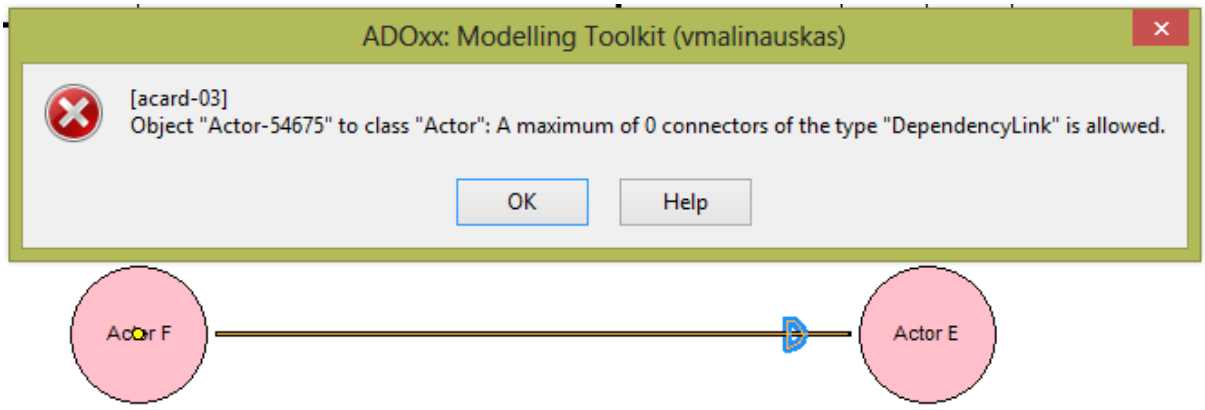

Figure 11. Creating a dependency link between two actors produces the error message.

Creating a Security Model

A Security Model can be created in the following two ways:

- Using model groups explorer (Figure 12)
- Using the main menu (Figure 13).

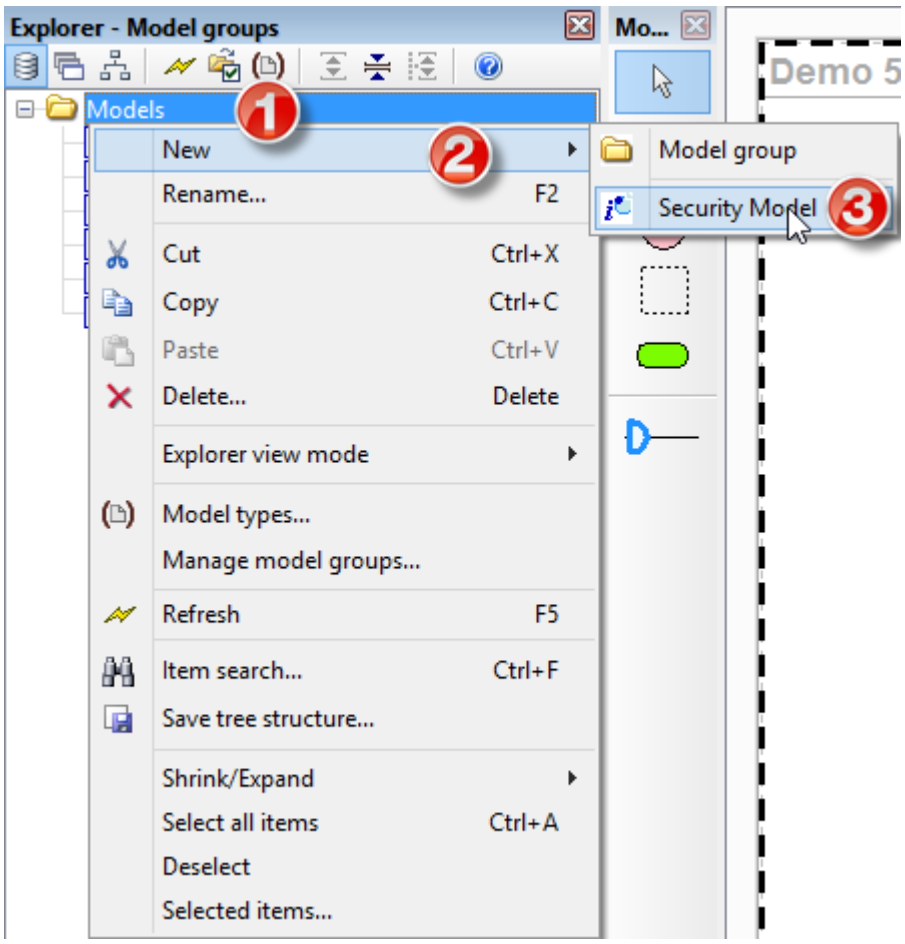

Figure 12. Right mouse button click on the model group will open the context menu, which allows creating models and model groups.

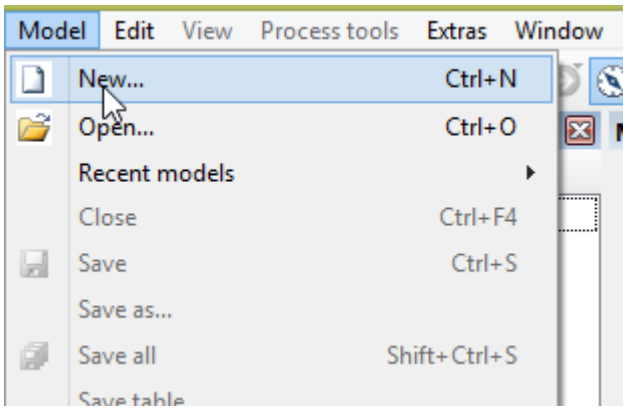

Figure 13. Creating new model using the main menu.

Model preparation

The “SecTro2” prepares new models based on the user preferences. Two important actions the tool performs are:

- Asking the user whether the Organisational View should be created for the new model;
- Creating a System Actor on the Security Requirements View.

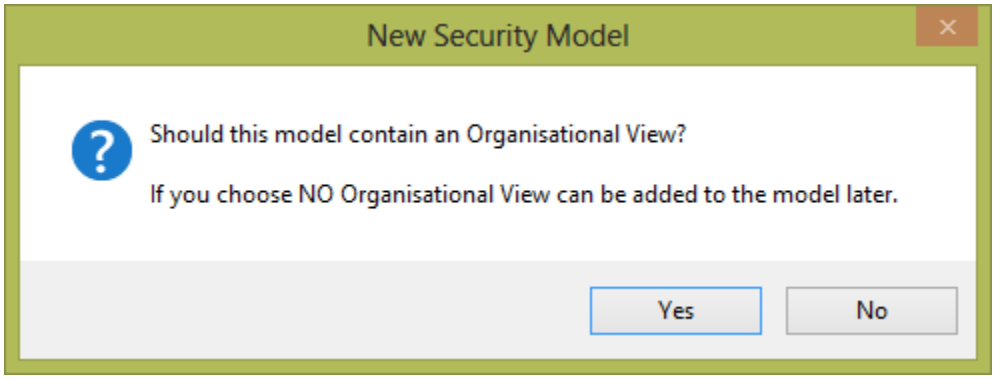

Figure 14. User is asked whether the Organisational View should be created.

The Figure 14 shows the query box presented to the user when a new model is being created. If the model will contain an organisational analysis then pressing “Yes” will create the Organisational View, but first will ask to name the organisation. On the other hand, if “No” is selected, the Organisational View will not be created for the model at question. The Organisational View for the model can be created later by going to the main menu “Edit” item and selecting “Create Organisational View” (Figure 15).

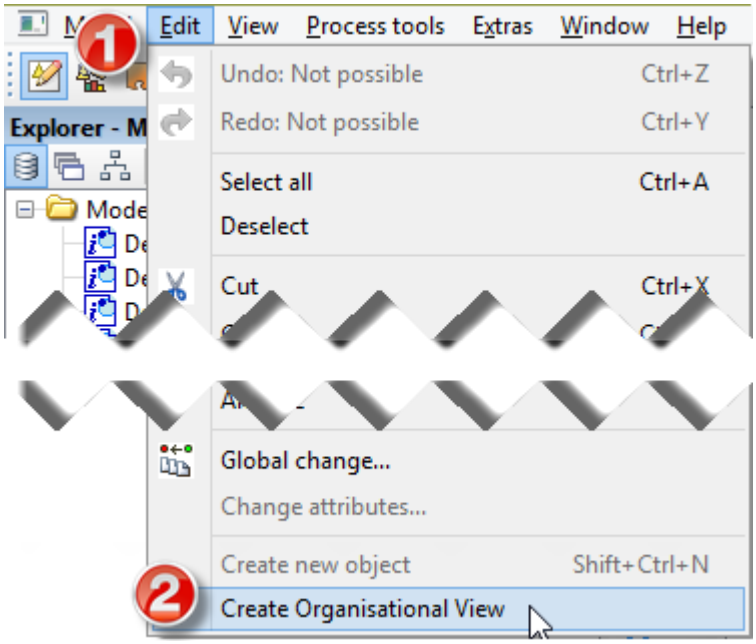

Figure 15. Organisational View can be created later if a model is missing one.

Model and model objects' specifics

The "SecTro2" supports the development of models by introducing model views' synchronisation. Some objects on the specific views indicate the state of the object or view synchronisation.

Model attributes

Each model have several attributes, which are used in the report generation as described in p.24 - Generating model reports. Model attributes' values can be changed by right clicking on the model as selecting "Model attributes" (Figure 16).

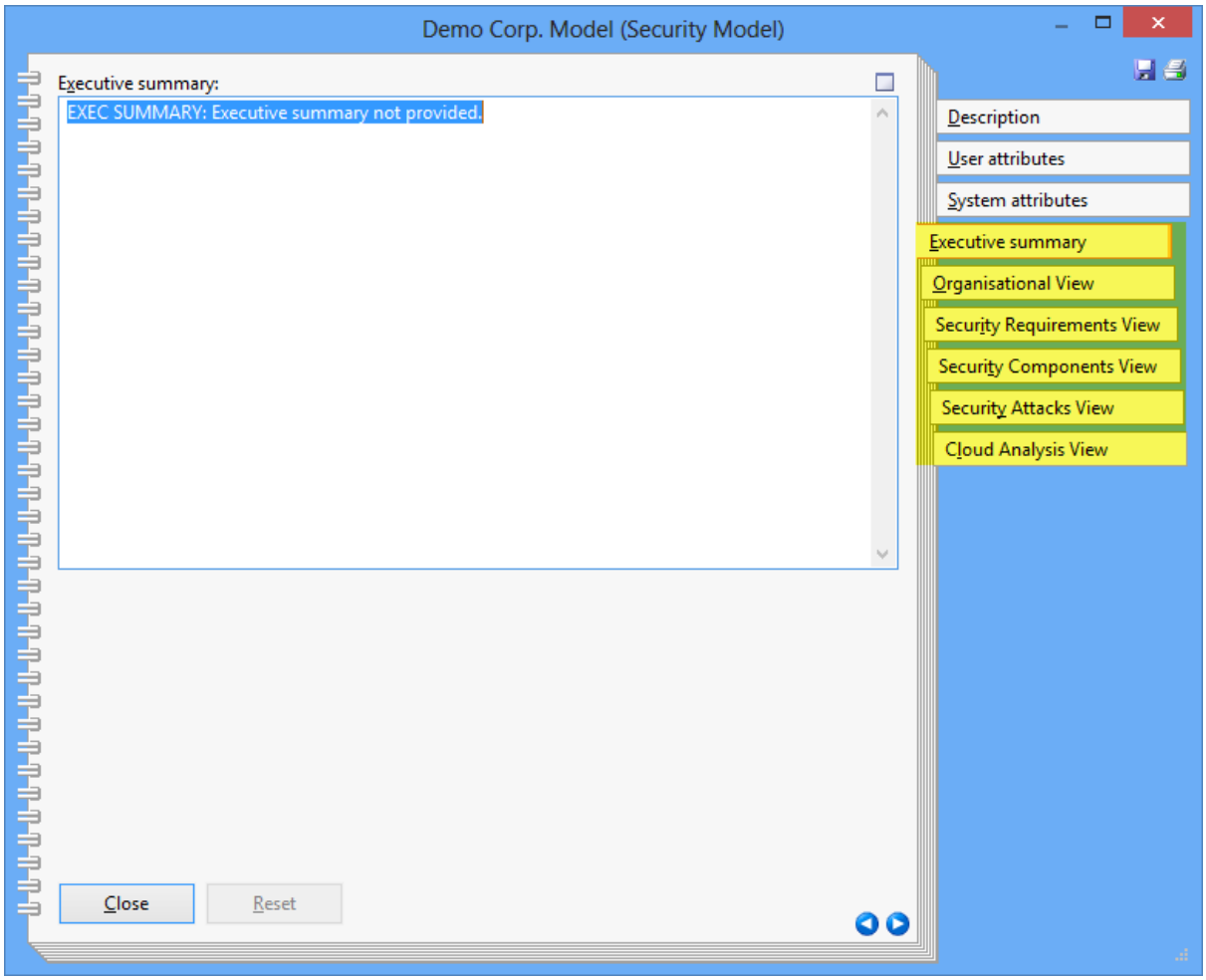

Figure 16. Model attributes window.

Attributes in sections, highlighted in yellow, will be included in the generated model's report. Each attribute can specify textual information related to the model and specific views. This is the best place to insert descriptions and explanations why some views are empty or not created (in case of the Organisational View), for example.

Goal delegation

Goals on the Organisational View can be synchronised to any of the actors on the Security Requirements View. The goal can be delegated to the System Actor, any of the existing actors on the Security Requirements View, a new actor on the Security Requirements View or the dependee from the dependency relationship can be transferred from the Organisational View to the Security Requirements View. The options for the target actor can are shown in the Figure 17.

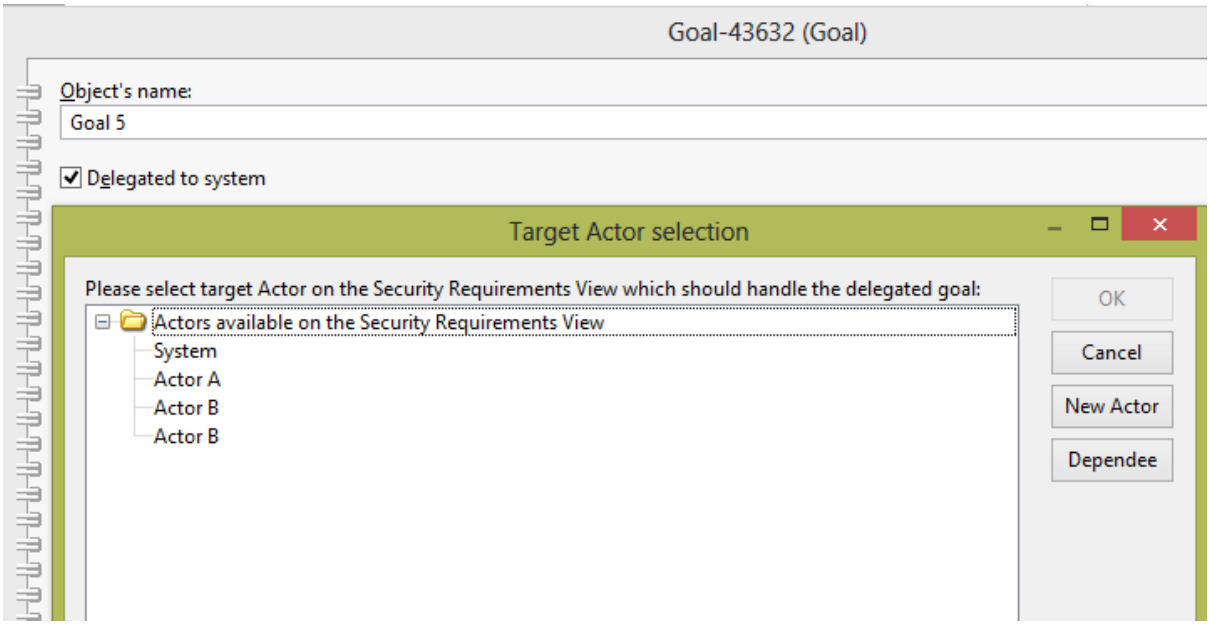

Figure 17. Target actor selection window shown upon the delegation of a goal.

In the case a goal is delegated to the dependee, the dependee will be mirrored from the Organisational View to the Security Requirements View. These two actors will be linked and synchronised – their names and several other attributes will be synchronised removing the burden from the developer to keep track of changes on various views.

Despite which option for a target actor is selected the goal in question will be mirrored on the Security Requirements View. Similar to the dependee synchronisation mentioned above, both goals on the Organisational View and the Security Requirements View will be synchronised. The goal on the Organisational View will receive a visual indicator showing that it has been delegated; this is shown in the Figure 18.

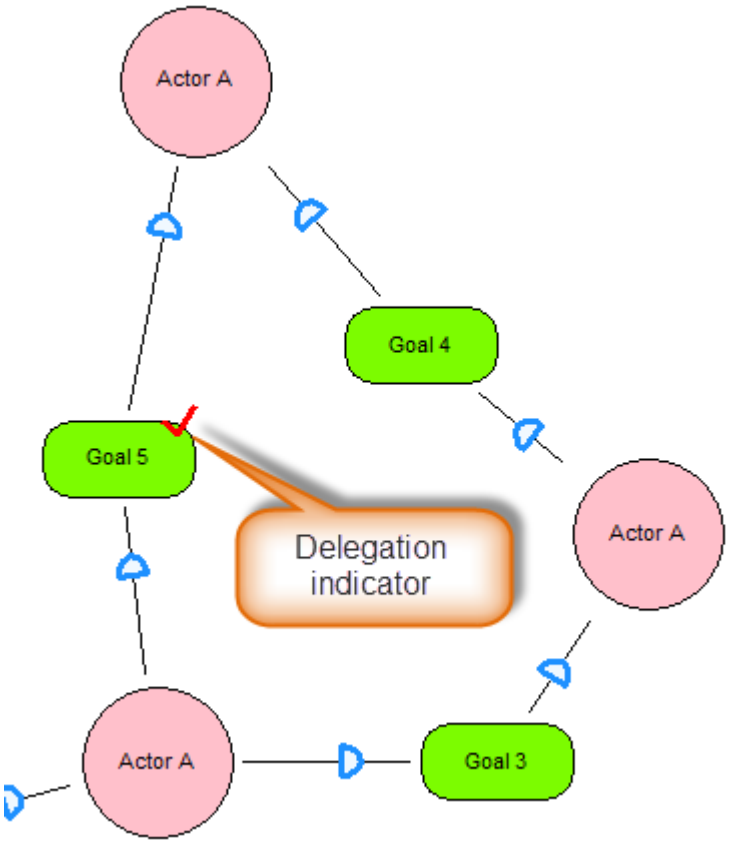

Figure 18. Goal 5 has been delegated to the Security Requirements View and its synchronisation is enabled.

Synchronisation of the Security Requirements View.

Two views are accessible only from the Security Requirements View: the Security Components View and the Security Attacks View. These two views are specific to the linked Security Mechanism and Threat objects, thus each Security Mechanism allows creating a different Security Components View and each Threat allows creating a different Security Attacks View. As both the Security Components View and the Security Attacks View are specific to the object they are linked to, it is convenient to call them as *sub-views* instead of full views. For example, if the "Threat A" is linked to a Security Attacks View, we can say that "Threat A" as a sub-view of the Security Attacks View.

Security Mechanism and Threat objects on the Security Requirements View have hotspots, which function in two ways:

1. Creates a sub-view related to the object, and
2. Opens the linked sub-view if it already has been created.

Examples of the hotspot visual appearance can be seen in the Figure 19 and Figure 20. A yellow hotspot indicates that the object has no sub-view associated, whereas a green hotspot with a red circle inside of it indicates the presence of the sub-view.

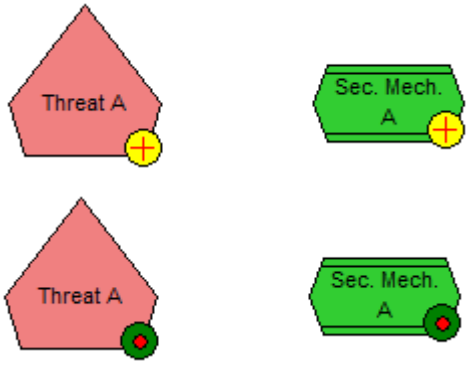

Figure 19. Object indicators showing the presence of a sub-view.

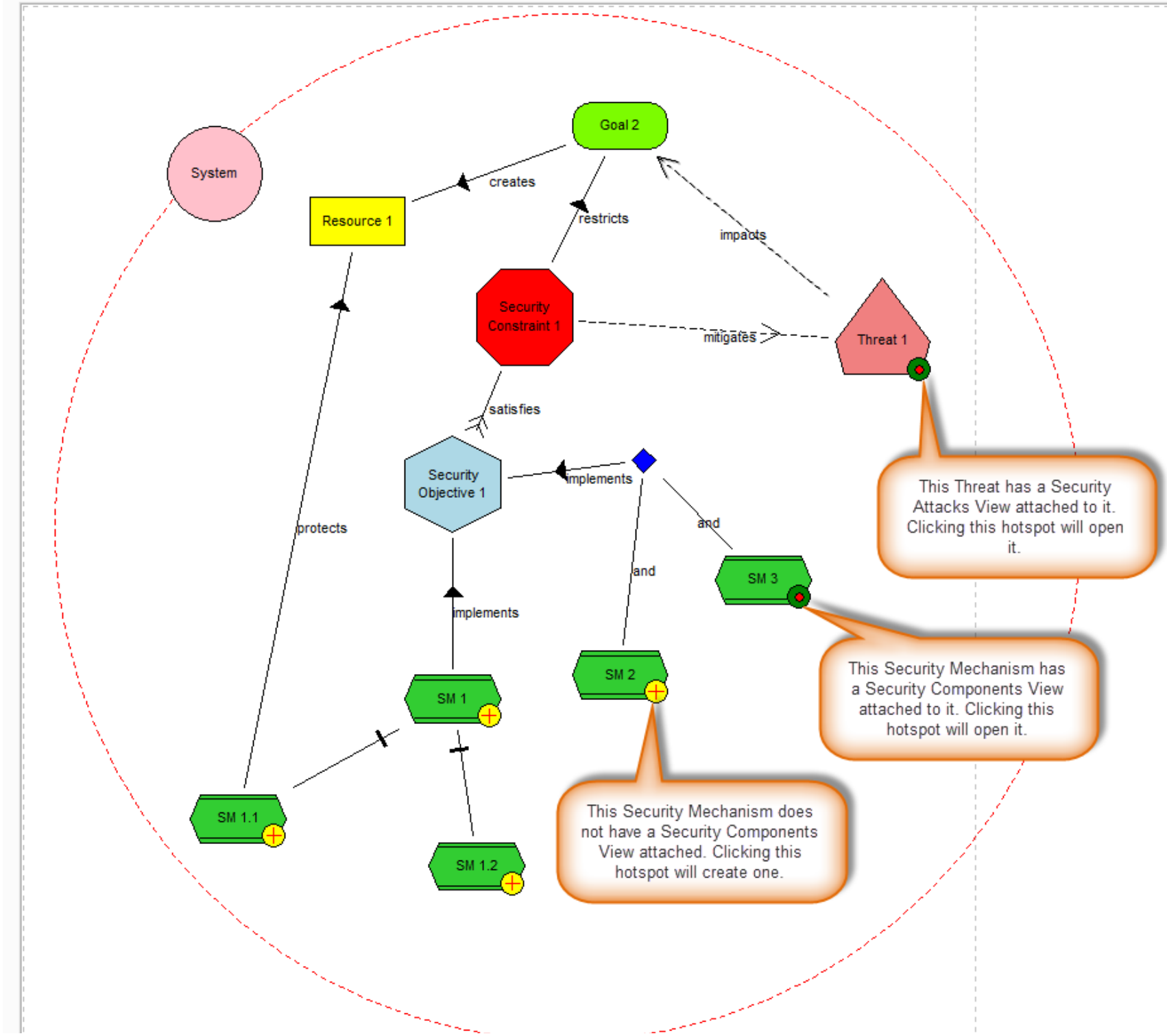

Figure 20. Demonstration of the Security Requirements View and Security Mechanisms'/Threats' hotspots.

Running analysis against the model

Cardinality check

A cardinality check is a validation of the model against the Secure Tropos metamodel rules. It checks if the objects and relationships on the model are correctly designed and shows an error message if inconsistencies were found.

The cardinality check function can be accessed in the analysis component using the main menu as shown in the Figure 21.

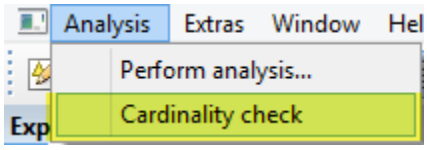

Figure 21. Cardinality check can be accessed from the main menu in the analysis component.

Analysis methods

The "SecTro2" allows running several analysis methods against the created models. To access the analysis functions the analysis component has to be activated as shown in the Figure 22.

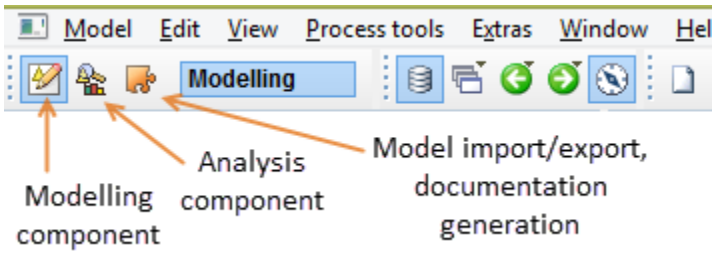

Figure 22. Modelling, analysis and import/export components.

Analysis methods invocation window can be accessed in the analysis component using the main menu as well as the toolbar button as displayed in the Figure 23.

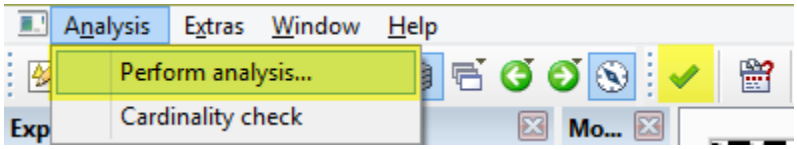

Figure 23. Access to the analysis methods invocation window.

Currently there are 7 analysis methods:

1. **Default object names** – checks the objects on the model for default names. For example, actor object with a name “Actor-1234” would not pass the analysis.
2. **Dangling objects** – this analysis checks the model for incomplete relationships. For example, dangling objects analysis will show a dependency relationship if there is a depender and dependum, but no dependee.
3. **Redundant objects** – checks for objects with no relationships. It considers objects without any modelling relationships as well as synchronisation relationships. For example, if a goal on the Organisational View is delegated to the system, but it does not have any modelling relationships, the analysis will consider such goal as having a synchronisation relationship and it will be excluded from the analysis results.
4. **Duplicate name analysis** – this analysis checks if any of the objects on a single view have the same name. The name checks are performed across the same type objects. For example, two actors with names “Actor A” on the Organisational View will not pass the analysis, but actor and goal with the same name will be excluded from the analysis results.
5. **Security Constraints analysis** – checks if security constraints on the Security Requirements View are satisfied. If a security constraint is satisfied by at least one security objective, then the analysis checks if the security objective is implemented by at least one security mechanism.
6. **Threat mitigation analysis** – this analysis checks if the attacks, thus threats, are mitigated on each of the Security Attacks Views.
7. **Cloud provider selection analysis** – analyses the Cloud Analysis View and shows the cloud provider, which has the highest satisfiability value.

Analysis methods invocation window is shown in the Figure 24. Each analysis method is denoted with . Several analysis methods can be selected from the analysis methods invocation window by clicking on them while a keyboard CONTROL key is pressed.

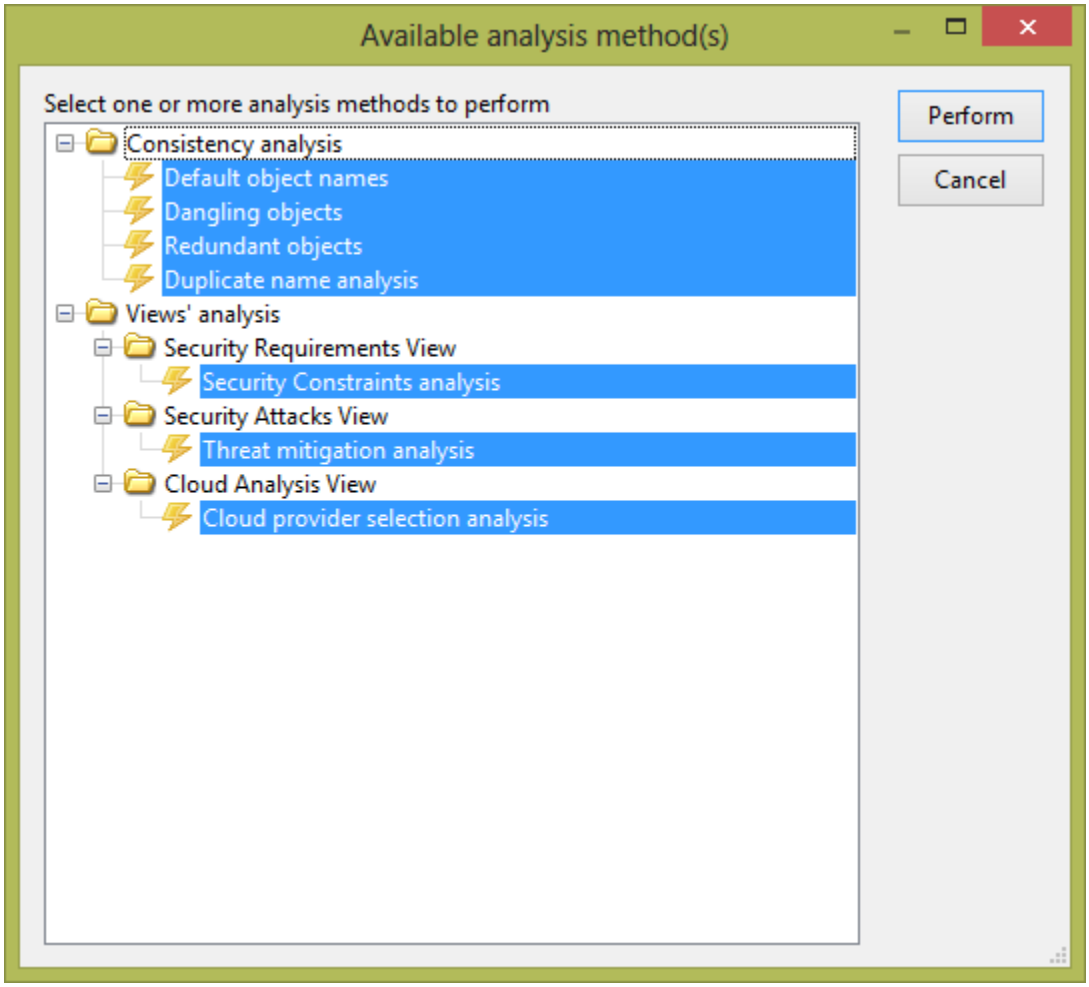

Figure 24. Analysis methods invocation window.

After running the analysis the analysis results window will be shown. Similarly to the analysis invocation window, analysis methods which were run will be denoted with and child items under each method will contain problems found in the model. An example of the analysis results window can be seen in the Figure 25.

If analysis results need further inspection referring to the model, then these can be transferred to the window which does not block the interactions with the model. To achieve that all required analysis methods (with) from the analysis results window have to be selected and after pressing “OK” a small window will appear at the bottom of the tool, similar to the one in the Figure 26.

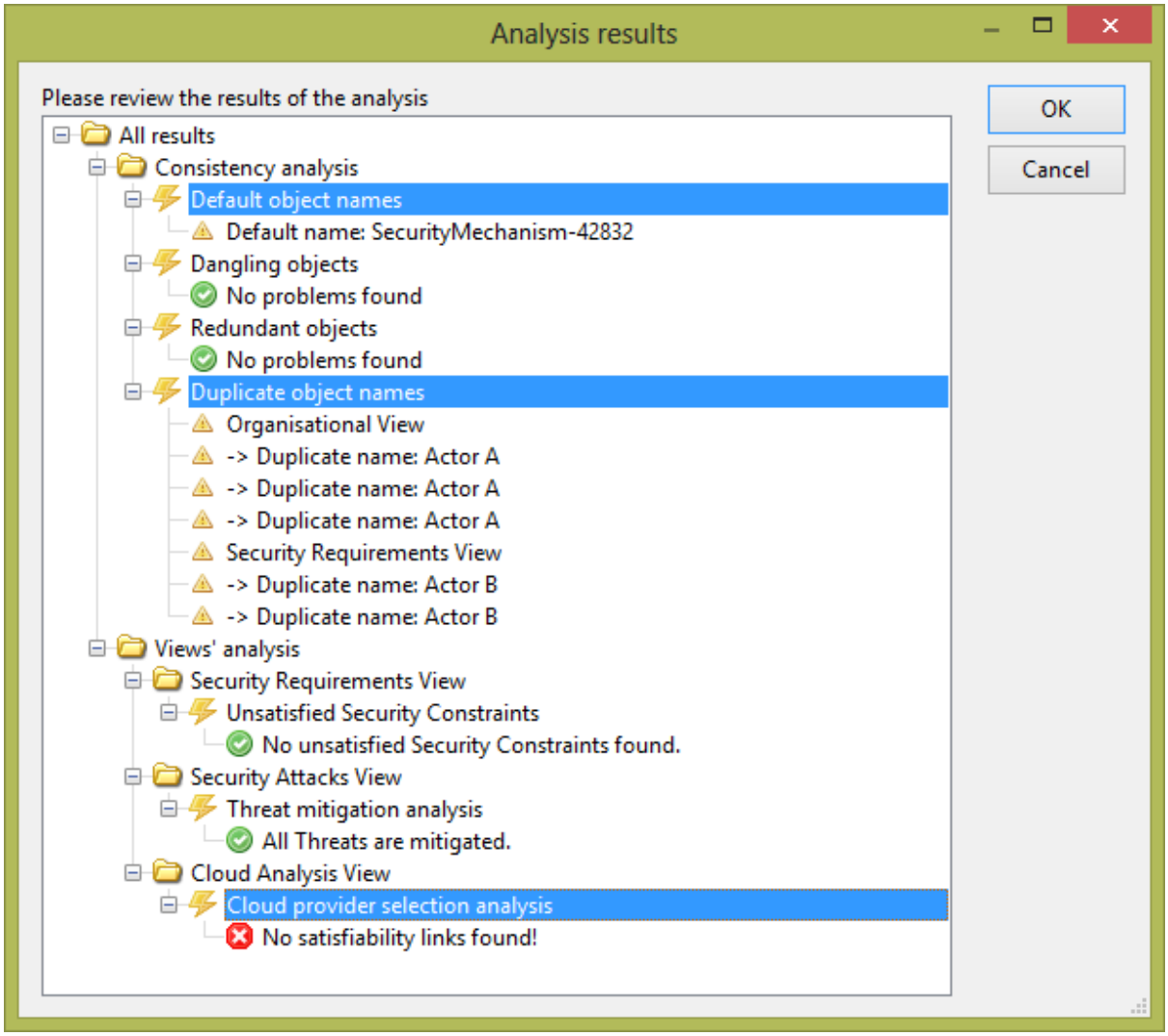

Figure 25. Analysis results window with three analysis methods selected.

Analysis results (24/04/2013 19:48:33)

- Default object names:
  * Default name: SecurityMechanism-42832
- Duplicate object names:
  * Organisational View
  * -> Duplicate name: Actor A
  * -> Duplicate name: Actor A
  * -> Duplicate name: Actor A
  * Security Requirements View
  * -> Duplicate name: Actor B
  * -> Duplicate name: Actor B
- Cloud provider selection analysis:
  * No satisfiability links found!

Figure 26. Analysis results transferred to the separate window for further the inspection of the results against the model.

The Design Pattern Library (DPL)

The Design Pattern Library (DPL) is the add-on for the "SecTro2", introduced in the version 2.0 of the tool. The DPL allows capturing modelling structures on the model and saving them for latter reuse. Such mechanism enables various experts to capture their knowledge and transfer it to the developer of the system. The main features of the DPL are:

- The design patterns are modelled in the "SecTro2" using the same concepts available to developer so no extra tools are required;
- Saved design patterns are associated with a number of attributes which describe each individual pattern or group of patterns;
- Saved design patterns can be selectively exported as a "well-formed" XML (E**x**tensible **M**arkup **L**anguage) file which can be imported into DPL by other team members and developers. This XML file also can be used in other tools supporting such functionality;
- The database, which holds saved design patterns, is a single file database, located in user's Documents folder. This file can be easily saved elsewhere for backup purposed and then restored back to user's Documents folder.

The DPL functionality can be accessed from the main menu when the modelling component is active. Main menu contains three sub-menus for DPL utilisation as shown in the Figure 27.

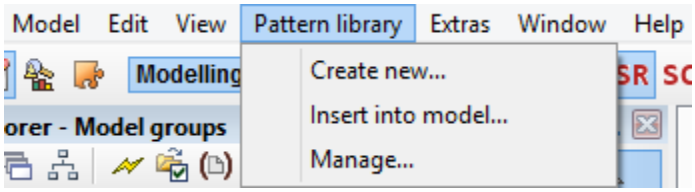

Figure 27. The main menu and sub-menus for the DPL.

Creating a design pattern

Creating a new design pattern involves selecting one or more modelling object and required relationships on the currently active model and selecting "Create new…" sub-menu. The "Create new pattern" window will open allowing to enter various attributes' values describing the design pattern, its purpose and reasoning (Figure 28).

The attributes of each design pattern are separated into three groups:

1. **General**. Contains design pattern's name, author, context and a static graphical image how the pattern looks like.
2. **Problem and Solution**. Two attributes – "Problems and Forces" and "Solution" – allow describing the problem(s) the design pattern is supposed to tackle, while "Solution" describes how the design pattern solves the problem at hand.
3. **Rationale**. Rationale's "Benefits" and "Liabilities" attributes describe the upsides and downsides of the design pattern. The "Related patterns" section allows selecting related patterns, which are to cover all downsides this pattern might have.

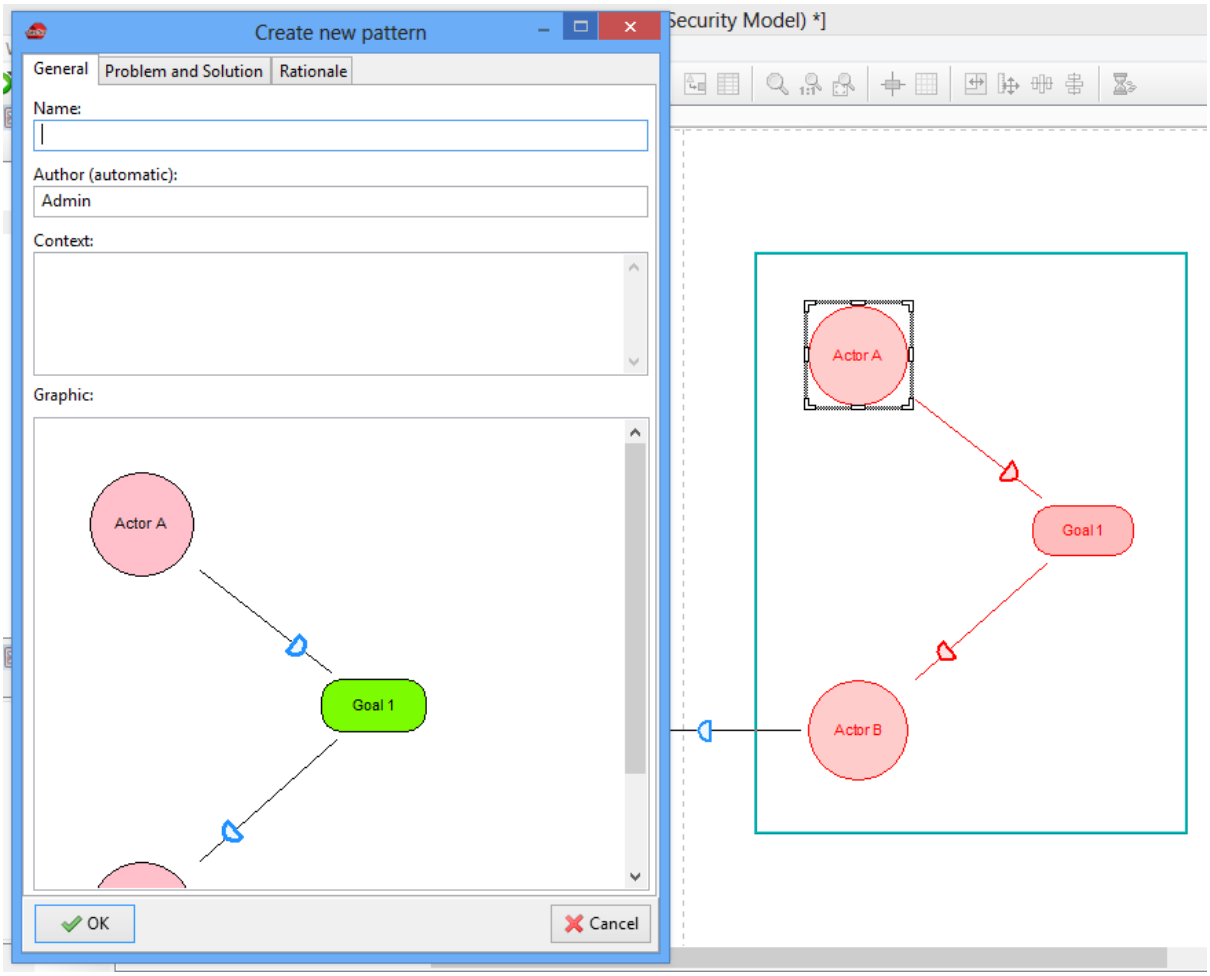

Figure 28. Creating a new design pattern from selected modelling objects and relationships.

Inserting saved design patterns

Inserting design patterns into a model requires the desired model to be opened first. Then selecting "Insert into model…" sub-menu (Figure 27) a design pattern selection window will open (Figure 29).

Depending on the type of saved design patterns, some of them will be greyed our as shown in the Figure 29. During the creation of each of the design patterns, a view to which they belong to is assigned to it automatically. Therefore the design pattern selection window will recognise the currently active view and allow inserting design patterns which only belongs to this view. Taking Figure 29 as an example, the Cloud Analysis View has to be activated for the "Agency guard" pattern to be inserted into the model.

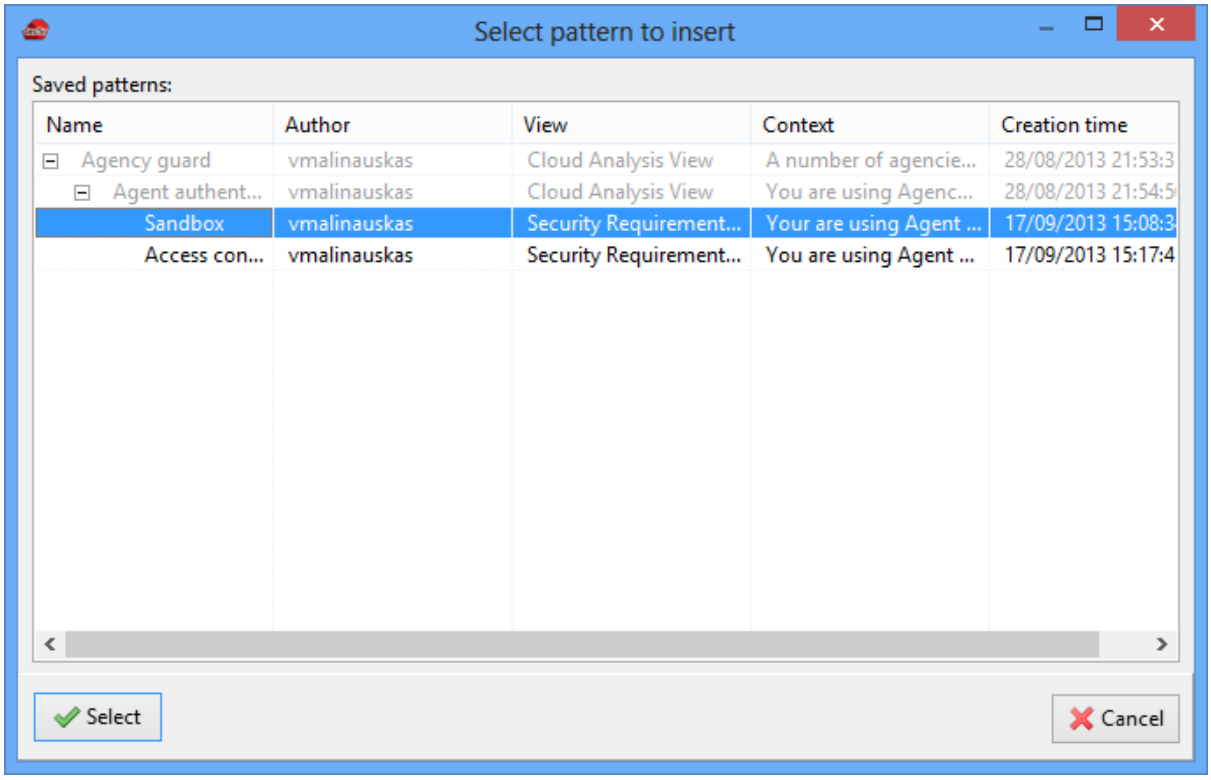

Figure 29. Design pattern selection window.

Managing the Design Pattern Library

The DPL management window is shown in the Figure 30. Here the saved design patterns can be managed using GUI elements provided. Several of the GUI elements have hotkeys, allowing to execute actions using only the keyboard.

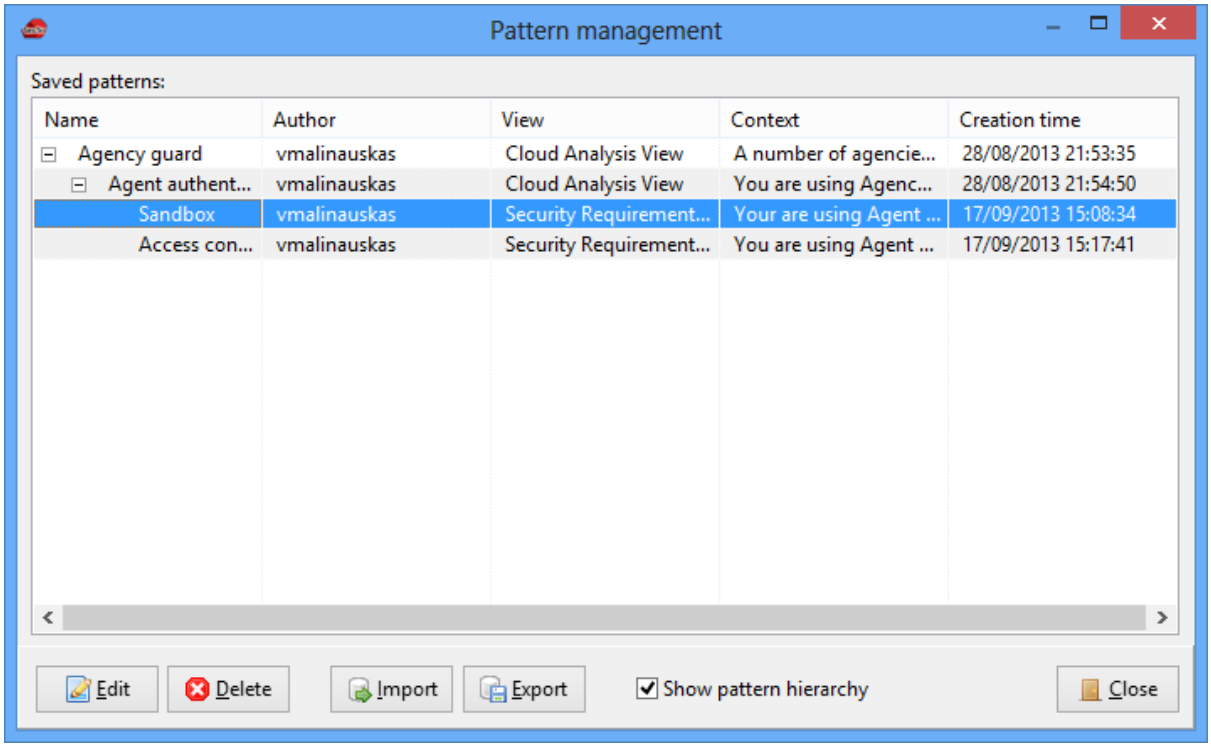

Figure 30. The DPL management window.

GUI elements, hotkeys and their functionality is:

- **"Edit" button (or pressing ENTER on the keyboard)** – open the design pattern editing window, where various design pattern's attributes can be changed;
- **"Delete" button (or pressing DELETE on the keyboard)** – removes the currently selected design pattern from the library;
- **"Import" button** – allows importing design patterns from XML file;
- **"Export" button** – allows exporting design patterns to XML file for easy sharing;
- **"Show pattern hierarchy" checkbox** – enables/disables hierarchical design pattern view. The hierarchy is extracted from the "Related patterns" attribute.

The DPL management window also has a context menu, accessible by clicking the right mouse button on any of the saved design patterns (Figure 31). The context menu contains actions, which can be used when more advanced management functionality is required.

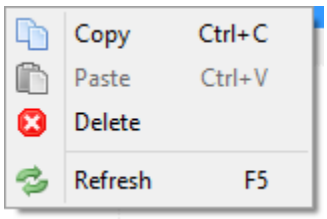

Figure 31. The DPL context menu.

- **"Copy" (or pressing CONTROL + C on the keyboard)** – copies the selected design pattern into the clipboard. The copied design pattern stays in the clipboard even if the "SecTro2" is closed.
- **"Paste" (or pressing CONTROL + V on the keyboard)** – pastes the copied pattern from the clipboard into the DPL. This essentially allows creating a duplicate design pattern in the DPL without recreating it from scratch.
- **"Delete"** – deletes the selected design pattern.
- **"Refresh" (or pressing F5 on the keyboard)** – refreshes the DPL by reloading all patterns from the database.

Customised model export (XSLT)

The customised model export functionality allows exporting models in the XML format, but changing the final result to suit different scenarios. The final XML file is produced by transforming it according to the XSLT transformations provided to the “SecTro2”.

The customised model export functionality can be accessed in the Import/Export component. The main menu “Model” contains sub-menu for running the export, removing XSLT plugins and adding new ones (Figure 32).

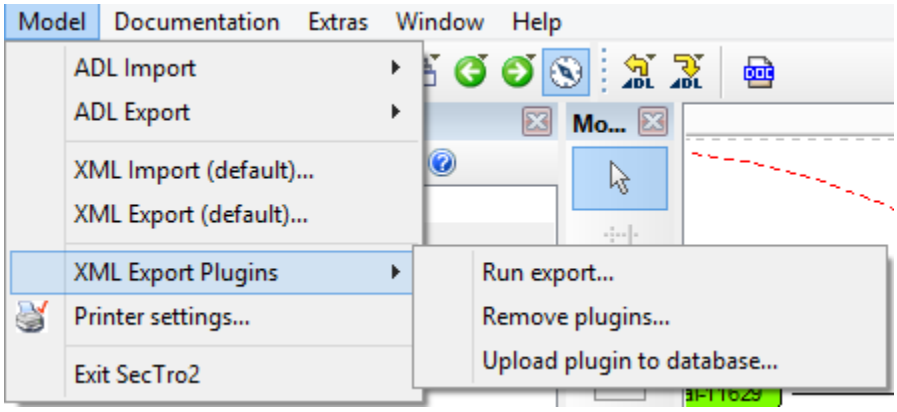

Figure 32. Customised model export menus.

The mentioned model export functionality is based on the user provided XSLT transformation files. Such files are considered being XML export plugins, which can be uploaded and removed to/from the “SecTro2” database.

Typical customised model export workflow:

Figure 33. Customised XML model export workflow.

The “SecTro2” installation by default has only one customised model export plugin called “Barebones”. This plugin exports model separating modelling objects and relationships to views they belong to. More plugins can be acquired from the official “SecTro2” website http://securetropos.org/sectro2-tool/. New plugins are uploaded to the “SecTro2” database by selecting “Upload plugin to database…” menu as illustrated in the Figure 32.

Generating model reports

The following steps are required to generate model reports as a Word® or PDF document.

1. A model has to be opened before the report generation takes place. The currently opened model will be used for the report.
2. The report generation facility is located in the import/export component. The button in the Figure 34 opens the report options window.

Figure 34. Report generation button is located in the import/export component's quick-access toolbar.

3. The report options window will open (Figure 35). Several options can be specified which will reflect on the generated report:
    - **Report title** – title of the report. This can be useful is several reports are generated for the same project, but, for example, running different sets of analysis.
    - **Project** – specified the title of the project.
    - **Developer** – name of the developer. Instead of specifying the person who generated the report it can be organisation or department responsible for system's documentation.
    - **Format** – "SecTro2" version 2.0 allows generating two type of reports - Word® or PDF (**P**ortable **D**ocument **F**ormat). The structure of the report will be the same despite the selected format, but if the report is will be opened on other operating systems than Microsoft® Windows® then PDF format is advisable.

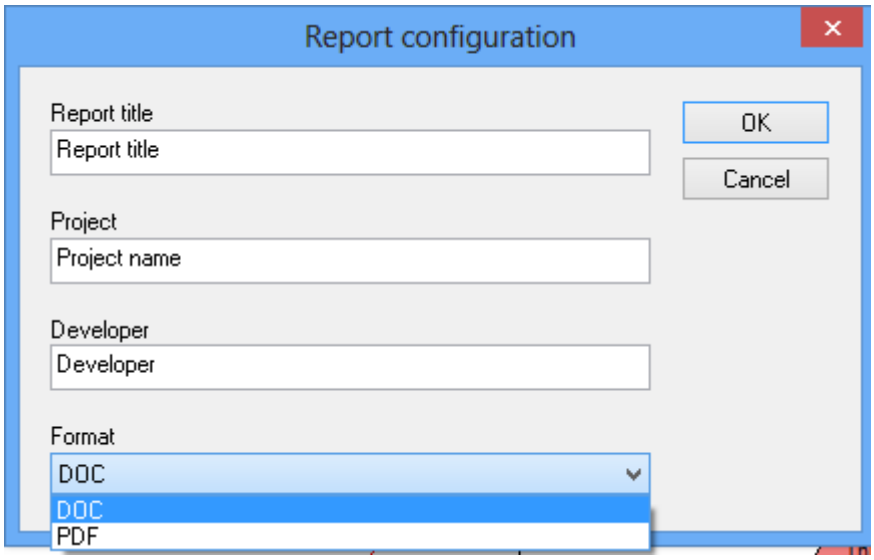

Figure 35. Report options window.

4. After specifying all options in the report options window (Figure 35) the save dialogue will open (Figure 36). **Note:** to generate a report an empty directory has to be selected at this step. The report generation process creates several intermediate files required for the final Word® or PDF generation, which are removed at the completion of the process. To avoid any important files removed from the user's computer, an empty folder has to be created and specified as the report destination.

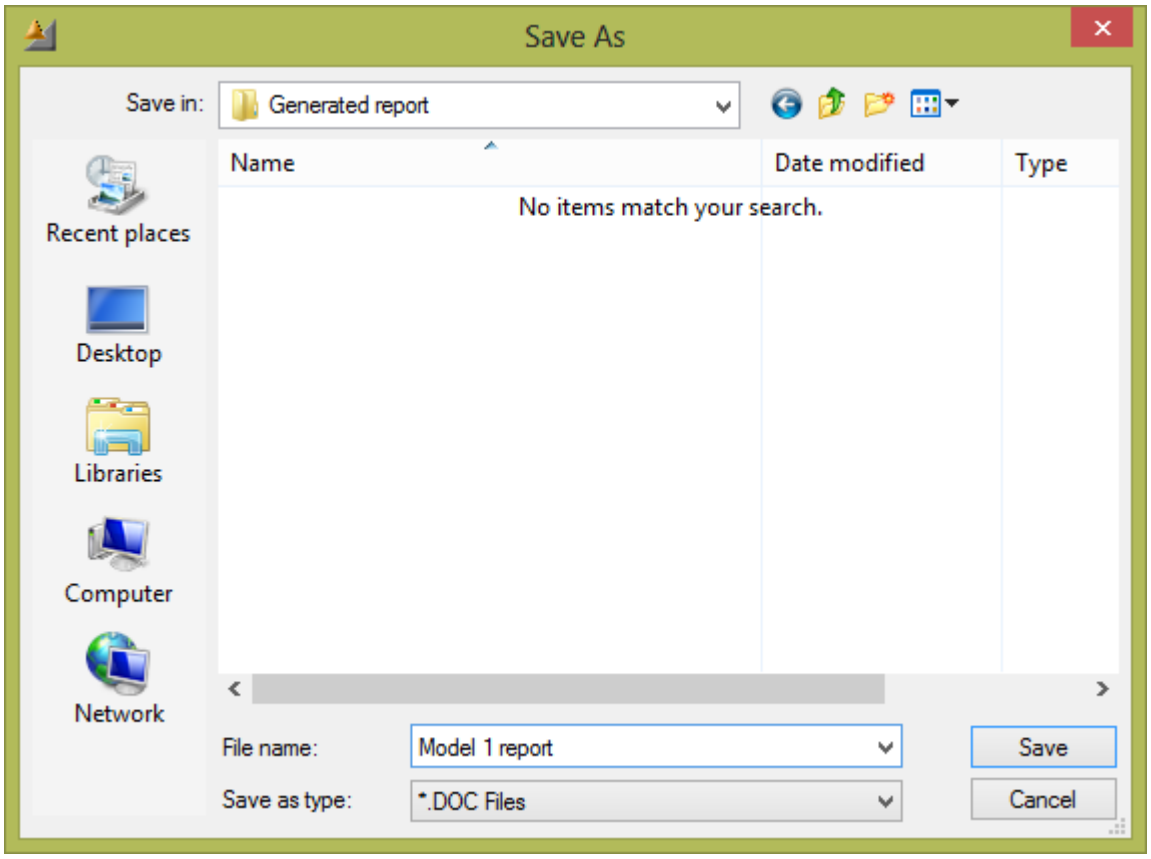

Figure 36. Save file dialogue.

5. Selecting save will start a report generation process which will take varying time depending on the size of the model being reported.