D5.4.A Framework for Integrated Documentation of System and Assessment Results

Mass Soldal Lund, Fredrik Seehusen, Bjørnar Solhaug, Ketil Stølen (SIN)

Document information

Document Number	D5.4.A
Document Title	Framework for integrated documentation of system and assessment results
Version	1.0
Status	Final
Work Package	WP 5
Deliverable Type	Appendix to D5.4 prototype
Contractual Date of Delivery	N/A
Actual Date of Delivery	
Responsible Unit	SIN
Contributors	SIN
Keyword List	
Dissemination level	PU+LIC

Document change record

Version	Date	Status	Author (Unit)	Description
0.1	22.11.10	Draft	Fredrik Seehusen, Bjørnar Solhaug, Ketil Stølen (SIN)	First draft
0.2	24.11.10	Draft	Fredrik Seehusen (SIN)	Second draft
0.3	06.01.11	Draft	Fredrik Seehusen (SIN)	Added screenshots
1.0	11.01.11	Final	Bjørnar Solhaug (SIN)	Polishing and finalization

Executive Summary

Deliverable D5.4 is a prototype risk assessment tool. The objective of developing the prototype is to provide tool support and automation or semi-automation for tasks and activities that are conducted during the risk assessment process of changing systems. The prototype is therefore closely aligned with the method for the risk assessment of changing and evolving systems that is presented in deliverable D5.3.

The risk assessment method for changing systems is in turn based on several risk assessment techniques and artifacts that are developed in WP5 for supporting and facilitating specific tasks of the risk assessment process. The main of these latter artifacts is the language for the modeling and documentation of changing risks. The modeling language for changing risks is presented in D5.2 and is further developed in D5.3. In fact, an overall guiding principle for the WP5 research and development tasks is the understanding of the risk assessment method, the risk modeling language and the prototype tool as three tightly interwoven cornerstones of a general approach to the risk assessment of changing and evolving systems.

The prototype tool consists of three main editors:

- The diagram editor, which can be used to create and edit diagrams with notation for expressing changing risks
- The indexing editor, which can be used to index system models that describe the target of analysis
- The mapping editor, which can be used to create mapping rules between the risk diagrams and the (indexed) target of analysis

The tool hence supports the task of risk identification and risk documentation, the task of tracing changes from the target system to the risk models, as well as the task of identifying, assessing and documenting changes to the risks.

Index

1 Introduction

This document presents the prototype tool of SecureChange deliverable D5.4 by describing its main functionality and its main purposes in the setting of risk assessment of changing and evolving systems. The objective of developing the prototype is to provide tool support and automation or semi-automation for tasks and activities that are conducted during the risk assessment process of changing systems. The prototype is therefore closely aligned with the method for the risk assessment of changing and evolving systems that is presented in SecureChange deliverable D5.3.

The risk assessment method for changing systems is in turn based on several risk assessment techniques and artifacts that are developed for supporting and facilitating specific tasks of the risk assessment process. In SecureChange WP5, the main artifact that is developed to support the risk assessment method is the language for the modeling and documentation of changing risks. The modeling language for changing risks is presented in D5.2 and is further developed in D5.3. In fact, an overall guiding principle for the WP5 research and development tasks is the understanding of the risk assessment method, the risk modeling language and the prototype tool as three tightly interwoven cornerstones of a general approach to the risk assessment of changing and evolving systems.

In addition to the risk modeling language, the risk assessment process is supported by techniques for the identification of changing risks, techniques for the estimation and evaluation of changing risks, as well as techniques for tracing changes from the target system to the risk models. These techniques are based on the risk modeling artifacts that are developed in WP5. In the development of the prototypes in WP5, both D5.4 and the subsequent D5.5, we aim at providing tool support for all of these techniques, for some of them automatic or semi-automatic support. In this document we focus on D5.4, but we also discuss tool support in the more general context of WP5.

The approach of the research tasks of WP5 is to develop and deliver artifacts for risk assessment of changing systems that are general in the sense that they can be instantiated by several specific approaches to risk assessment. Such an instantiation is in D5.3 made in CORAS [2] to demonstrate and explain the more general approach of WP5 by a specific instance. The instantiation results in the generalization of the CORAS approach to the setting of the risk assessment of changing and evolving systems. The instantiation thereby offers the CORAS risk assessment process, risk assessment techniques and risk modeling language for change. In the development of prototype tools we implement the artifacts in the CORAS instantiation.

The rest of the document is structured as follows. In Section 2 we present the overall objectives of the WP5 prototypes. In Section 3 we present the main functionality of the D5.4 prototype. In Section 4 we conclude.

2 Objectives

The overall objective of the prototype is to support the various tasks of the CORAS risk assessment process. A core part of the risk assessment of changing systems is the identification and modeling of changing risks. This is usually conducted in workshops of structured brainstorming involving personnel of various backgrounds and different expert insight into the system that is the subject of the analysis, i.e. into the target of analysis. During the risk identification, the findings and the results are documented on-the-fly using the CORAS language. In such a setting, it is important that the results can be quickly and efficiently documented such that the participants can pass their opinions between them, and also such that the diagrams can be made on-the-fly without interrupting the flow of the discussion. The tool support should facilitate efficient modeling of easily understandable diagrams while ensuring that the diagrams are syntactically correct.

In the risk assessment of changing and evolving systems, a main challenge is to maintain a correct understanding of the risk picture while the system is changing. Maintaining the correct understanding means that the validity of the risk models must be ensured after the occurrence of system changes. For efficient identification of the potential impact of system changes on the risk picture, we have in WP5 introduced techniques for traceability between the target system and the risk models. In the setting of the risk identification workshops, the tasks of which include the identification and modeling of changing risks, there should be tool support for the identification and documentation of the relationships between the target system and the risk models.

According to the ISO 31000 standard on risk management [1], the risk analysis process consists of the five activities of context establishment, risk identification, risk estimation, risk evaluation and risk treatment. The three activities in the middle constitute what is referred to as risk assessment. The CORAS process is aligned with these overall activities, and in the risk assessment method for changing systems presented in D5.3 there are modeling and analysis techniques to facilitate each of the various activities. An objective of the prototype development is to provide tool support for all of the modeling and analysis tasks.

The risk models and other diagrams that are made during the risk assessment process serve not only as a basis for the risk assessment tasks; they are also used as part of the final documentation and reporting of the risk assessment results. When using a diagram editing tool for making the various models and diagrams, the results should therefore be of a format that is adequate for reporting.

3 Main Functionality of Tool

The tool consists for three main editors

- *The CORAS diagram editor*, which can be used to create and edit CORAS diagrams with notation for expressing change
- *The indexing editor*, which can be used to index system models that describe the target of analysis.
- *The mapping editor,* which can be used to create mapping rules between the CORAS diagrams and the (indexed) target of analysis, i.e. to create the trace model.

3.1 The CORAS diagram editor

3.1.1Purpose

The purpose of the CORAS diagram editor is to support the creation and editing of CORAS diagrams that document a risk analysis of a changing system. In addition to supporting the specification of common risk analysis notions such as threat, vulnerability, unwanted incident, etc., the tool also supports a notion of change:

1. Every element of a CORAS diagram may be in one of three modes that indicate whether the diagram element is applicable only before, only after, of both before and after a change in the target of analysis.
2. The CORAS diagram editor also has a construct which can be used to relate a given element of the CORAS diagram to an (indexed) part of the target of analysis. The purpose of this construct is to help the user analyze which parts of the CORAS diagram will be affected when the target of analysis is changed

.

3.1.2 Functionality

A screenshot of the CORAS diagram editor is given in Figure 1. As indicated in the figure, the editor has six main parts:

- A *pull-down menu* that offers standard functions such as open, save, copy, cut, paste, undo and print.
- A *tool-bar* that offers easy access to the standard functions of the pull-down menu.
- A *palette* that contains the model elements and relations for drawing the diagrams.

- A *drawing area* or canvas for drawing the diagrams.
- A *properties window* that lists the properties of a selected element, and that can be used to edit the values of the properties.
- An *outline* that presents a project and its diagrams as a tree.

Except for the pull-down menu and the tool bar, all parts of the tool can be closed or hidden.

In the prototype tool, a project is a collection of diagrams, and each diagram must belong to a project. A project must therefore be created before any diagrams are created.

The outline contains a tree representation of the project. The diagrams of the project are listed at the first level, and under each diagram all the diagram elements are listed. When a new element is created in the drawing area, it is automatically added to the tree under the correct diagram.

The drawing area is the part of the prototype tool where the diagrams are made by inserting, editing, annotating and deleting elements. This is also where likelihoods and consequences are inserted to diagrams as part of the risk estimation, and it is also where risk levels are inserted as part of the risk evaluation.

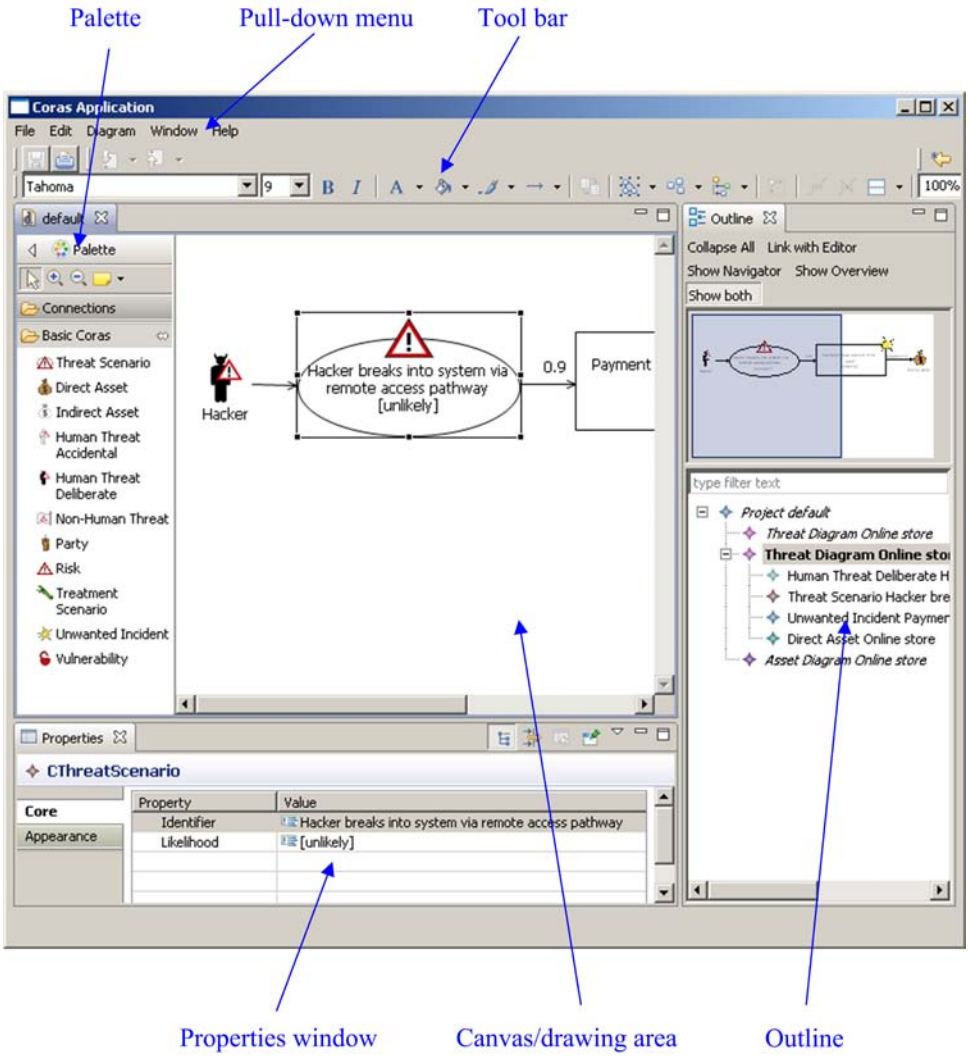

Figure 1 Prototype screenshot

Each element of a CORAS diagram may be in one of three modes to indicate whether the element should apply before, after, or before and after the target of analysis has changed. To set the mode of an element, the element is right-clicked and “Set mode” is selected in the appearing pull-down menu. A dialog will then appear, allowing one of three modes to be selected. The mode of a given element is in expressed graphically as illustrated in Figure 2. The figure on the left hand side (in grey) is in mode “before”, the middle figure (in color) is in mode “after”, while the right most figure (two-layered) is in mode “before-after”.

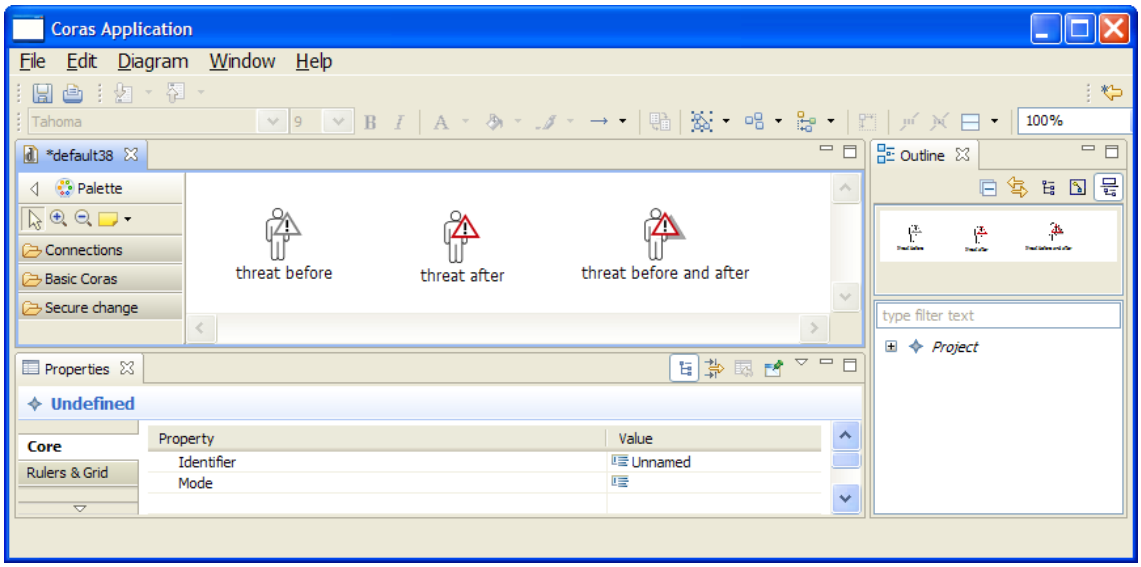

Figure 2 Visualization of change modes

The CORAS diagram editor supports a construct called *target segment* to help visualize to which parts of the target of analysis a given CORAS element is related. This construct may be attached to any CORAS diagram element. Given that the relationship between the target of analysis and the CORAS diagram elements have been specified in the mapping editor (as described in Section 3.3), the target segment will automatically be populated with text that indicates which parts of the target of analysis the CORAS element that the target segment is attached to is related to.

In Figure 3, we have illustrated a CORAS diagram that includes the target segment construct. Both the boxes labeled “Radar” and “Sector team, Task T1, A/C monitoring” are target segment constructs. The latter construct is attached to the threat scenario “Monitoring of A/C in the sector fails”, thereby indicating that this threat scenario may be affected if changes are made in the parts of the target of analysis related to Sector team, Task T1, or A/C monitoring. More precisely, Sector team, Task T1, and A/C monitoring are *tags* that are use to group mapping rules which relate elements in the target of analysis to elements in the CORAS diagram. These tags must be defined in the mapping editor (described in Section 3.3).

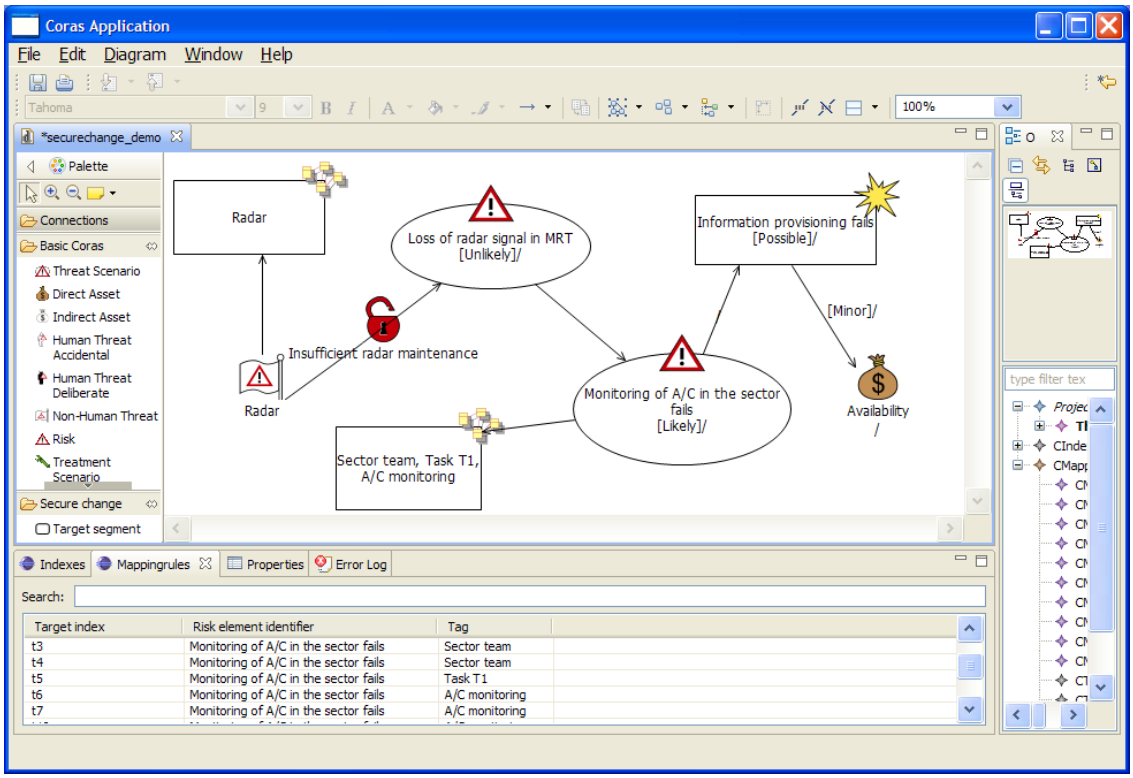

Figure 3 Graphical representation of the mapping rules attached to a CORAS element

3.2 The indexing editor

3.2.1Purpose

The purpose of the indexing tool is to provide a way of referring to parts of the target of analysis that should be related to the elements of the CORAS diagram. In particular, the indexing editor allows the user to index parts of the target of analysis. These indexes can then be used when defining the mapping rules that relate CORAS diagram elements to parts of the target of analysis, i.e. when making the trace model.

3.2.2Functionality

The indexing editor is illustrated in Figure 4. The editor is basically a table consisting of the following columns:

- **ID:** The unique identifier of the index
- **Name:** The name of the part of the target of analysis which is referred to by the index.
- **Category:** The type of the part of the target of analysis (actor, scenario, or event)

- **Description:** A description of the indexed part of the target of analysis.
- **Mode:** Specifies whether the part of the target of analysis belongs to the initial system (before), the changed system (after), or both (before-after).

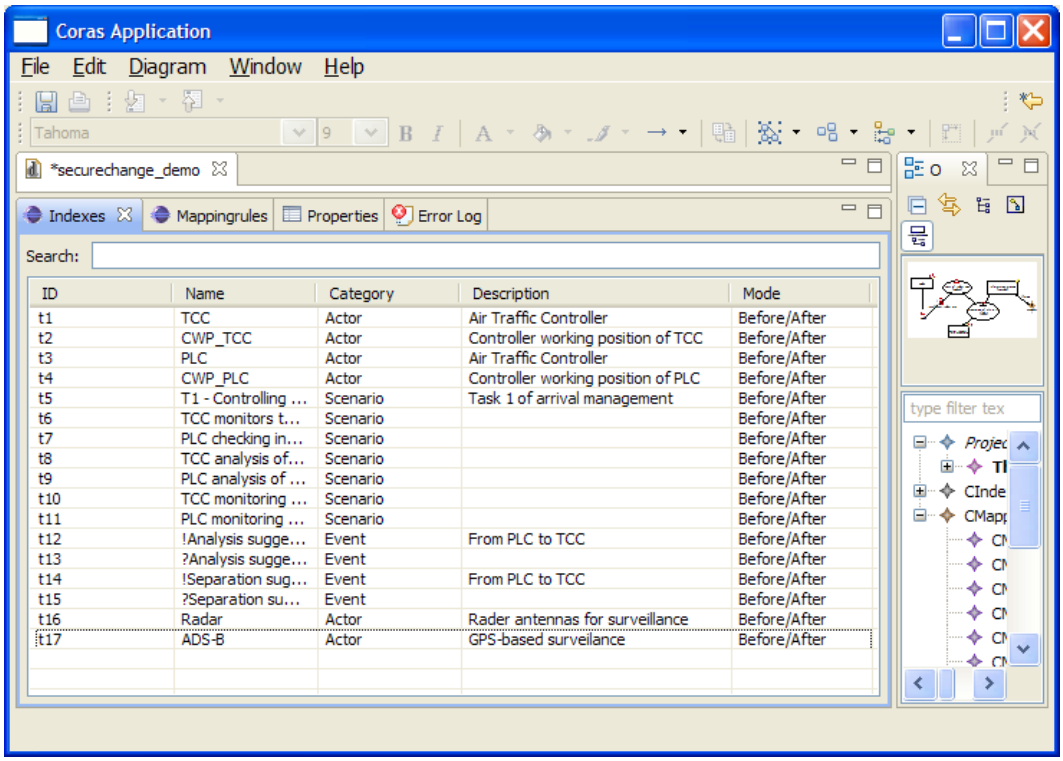

Figure 4 Illustration of the indexing editor

In order to add a row to the indexing table, simply right-click the table and select “add index” in the appearing pull-down menu. A dialog will then appear, allowing the required row entries to be filled in.

3.3 The mapping editor

3.3.1Purpose

The purpose of the mapping editor is to support the specification of the relationship between the CORAS diagram elements and the (indexed) parts of the target of analysis.

3.3.2Functionality

The mapping editor enables the user to specify a list of *mapping rules* that relate CORAS diagram elements to (indexed) parts of the target of analysis. Each mapping rule has the following ingredients:

- **Target index**: References the indexed part of the target of analysis to which the mapping rule applies
- **Risk element identifier**: References the CORAS diagram element to which the mapping rule applies.
- **Tag**: Reference to a tag which provides a means of categorizing mapping rules into groups.

A screenshot of the mapping editor is given in Figure 5. Here we see that the mapping rules are presented in a table which can be edited to create new mapping rules or change existing mapping rules.

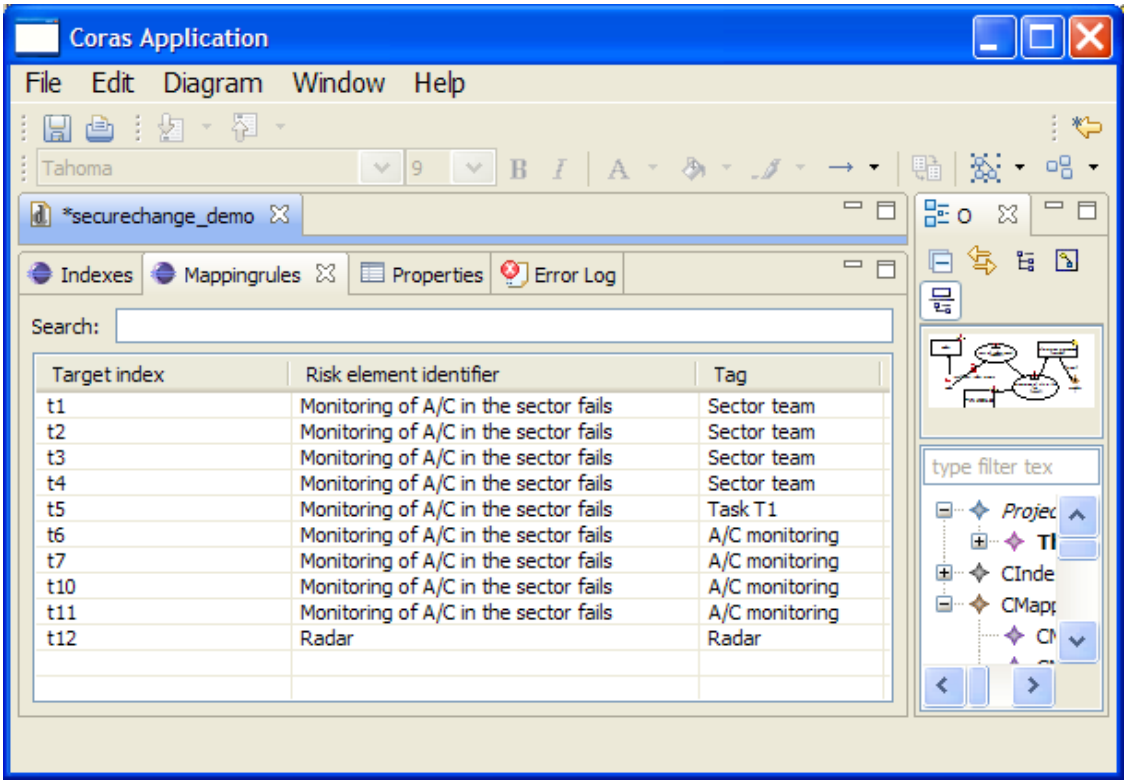

Figure 5 Illustration of the mapping editor

4 Conclusion

The overall objective of WP5 is to develop an approach to risk assessment of changing and evolving systems. The three main kinds of artifacts that are delivered for this purpose are a method for risk assessment of changing systems, languages for the modeling of changing risks, and prototype tools to support the former two. The risk modeling languages are tightly interwoven with the risk assessment method, and the prototype tools are designed to support and facilitate the use of the modeling languages during the various activities of the risk assessment tasks.

In this document we have presented and explained the main functionality and purposes of the SecureChange prototype deliverable D5.4. A main purpose of the tool is to enable efficient on-the-fly modeling while ensuring that the diagrams that are made are clearly presented, easily understandable and syntactically correct.

When addressing changing and evolving systems, there are certain challenges for which specific support should be provided. One such challenge is to enable the explicit modeling and assessment of risks as changing risks. The assessment method provides guidelines for how to identify and evaluate risks of changing systems, and the modeling languages provides support for modeling changing risks. The prototype tool in turn supports both by providing a means for efficient modeling and documentation of changing risks.

A further challenge is to enable the tracing of changes from the system to the risk models, in order to understand the potential impact of changes and how changes may propagate. The assessment method provides guidelines for how to handle the traceability of changes, and specific techniques for making the trace model is provided. The prototype tool supports handling the traceability by providing means for specifying and documenting the trace model, and for visualizing the relations between the system and the risk models in an intuitive way.

References

[1] International Organization for Standardization: ISO 31000 Risk management – Principles and guidelines, 2009.

[2] Lund, M. S., Solhaug, B., Stølen, K., ”Model-Driven Risk Analysis – The CORAS Approach”, Springer, 2010.