Security Analyst 21.3

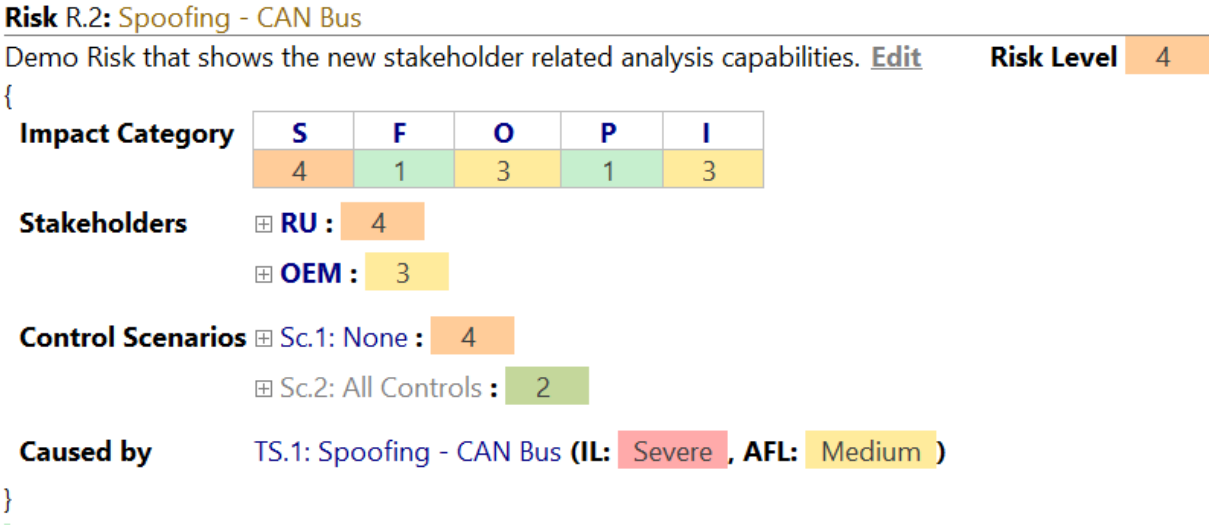
Release Notes

Stakeholder Analysis per Risk

It is now possible to do Stakeholder centric analyses for each risk element.
Each Risk contains the following new or updated sections:

Impact Category

This section shows the Risk Level with respect to each Impact Category that you have in use and allows quick analyses regarding potential Impacts. The example below shows that the main Impact is driven by the Safety category.



Stakeholders

This section allows analyses with respect to the Stakeholders. There is one section per defined Stakeholder. You can see the overall Risk Level for each Stakeholder and expand the view to see the Risk for the related Stakeholder per Impact Category and Control Scenario.

The example below shows the overall Risk Level 4 for the Road User. The detailed table shows that we have Control Scenario Sc.1 active (bold black text) and that the Risk is driven by Safety. In addition, you may see that with Control Scenario Sc. 2 the Risk Level was already reduced to 2.

RU : 4

	S	F	O	P	I	All
Sc.1	4	1	3	1	none	4
Sc.2	2	1	1	1	none	2

Control Scenarios

Like the Stakeholders overview, you can find the Risk Level per Control Scenario in this section. Optionally, you may have a look at the details per Control Scenario and find the Impact per Category and Stakeholder.

The example below shows the overall Risk Level 4 for Control Scenario Sc. 1. When extending the details, we can see that the Risk originates from the Road User while for the OEM the Risk is at Level 3.

Sc.1: None : 4

	S	F	O	P	I	All
RU	4	1	3	1	none	4
OEM	none	none	none	none	3	3

Stakeholders in Attack Path Analysis

In addition to the additional Stakeholder information per Risk you may now also find the Risk per Impact Category and Stakeholder in the following elements:

- Controls
- Attack Steps / Threat Scenarios
- Security Objectives

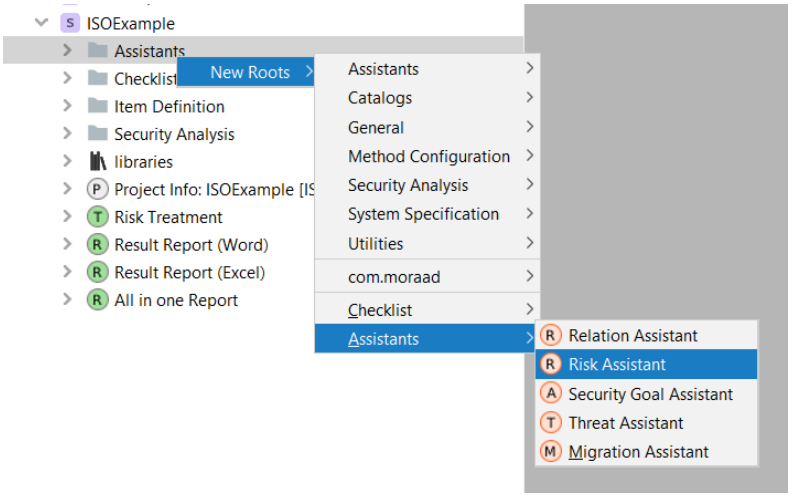
Risk Level 4

	S	F	O	P	I	All
RU	4	1	3	1	none	4
OEM	none	none	none	none	3	3
ALL	4	1	3	1	3	4

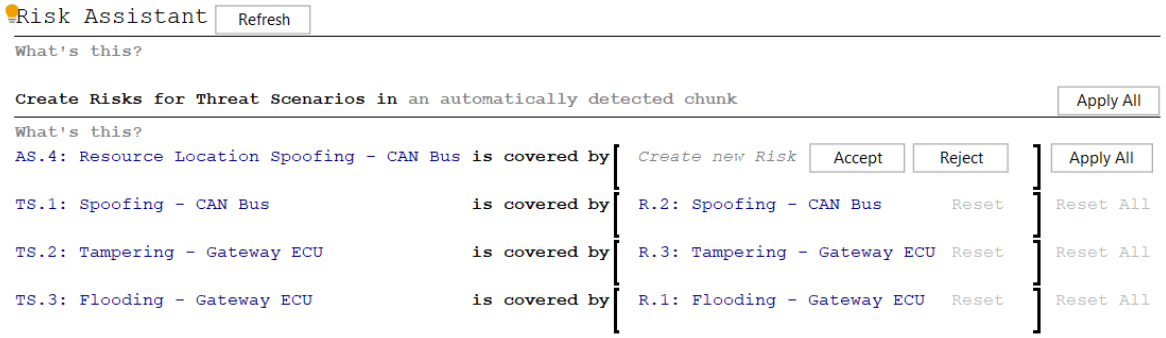
Risk Assistant

You may now create a Risk Assistant that allows you to create a Risk for each Threat Scenario. After having modeled some Threat Scenarios and Security Objectives with their corresponding Damage Scenarios, you might want to have a Risk created for each Threat

Scenario. Some Risks may cover multiple Threat Scenarios, but in general, creating one for each is a good start. For that, just right-click on the *Assistants* folder and under “New Roots > Assistants”, select “Risk Assistant”, as follows:



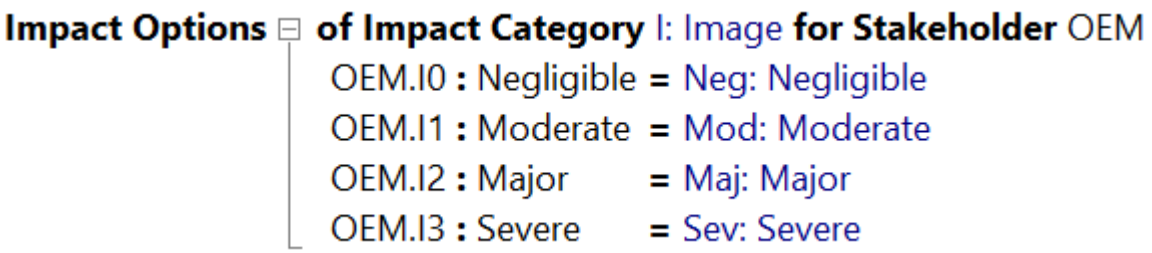
The new chunk is now tracking which Threat Scenarios are covered by which Risk. If a Threat Scenario is not covered, it suggests creating a new Risk.



By clicking “Apply All” on top, you may kick start your Risk identification phase and have a Risk created for each Threat Scenario.

Automatic Impact Option Generation

Impact Options are now auto generated with a consistent pattern including the relevant Stakeholder, the short name of the Impact Category and an index based on the related Impact Level. The names are still customizable in case you prefer your own custom Impact Options.



CAL support

Support for *Cybersecurity-Assurance-Level* (CAL) was added to Security Objectives and System Elements (Components, Data, Channels, Dataflows, Functions). It is visible in the respective inspectors (Open with *ALT+2* or *Right-Click→ Inspect Node*). An additional column was added to the respective Report items. By default, no CAL is set. Note that it does not affect calculation.

ISO/SAE 21434 Terminology

- Aligned terms with final ISO/SAE 21434 in the user guide
- Aligned terms with final ISO/SAE 21434 in tutorial
- Updated feasibility model to be consistent with final ISO/SAE 21434

Improved Assistants

- Improved performance for Asset Identification and Threat Assistant
- Assistants are no longer in beta state
- Renamed “SUD” to “TOE” (Target of Evaluation)
- Sort Risks in Risk Treatment by name
- “RemoveAllDamage” term can be customized via terminology profile

Various fixes and improvements

- Xsam
    - abort import, if the type of a reference does not match the expected type
    - name-based references now may contain slashes in the name

Open initiative for an exchange format

You might already know our exchange format XSAM. Starting from this, we are launching an initiative to form an open community which aims at establishing a cross-vendor, cross-tool XML-based format for eXchanging Security Analysis Models. We call it openxsam.io and recently talked about it at ASRG. If you are interested in joining the initiative, please contact us at security-analyst@itemis.de.

Additionally, we still have the knowledge base at https://www.security-analyst.org about general security analysis processes and norms.

Version Mapping

The following table can be used to determine the Security Analyst version based of the internal plugin version “com.moraad.core” that is stored in the .msd file of every solution:

```
<language slang="l:2bca1aa3-c113-4542-8ac2-2a6a30636981:
com.moraad.core" version="<com-moraad-core-version>" />
```

com.moraad.core version	Security Analyst version
74	21.3
73	21.2
72	21.1.1
71	21.1
64	20.4
63	20.3.1
61	20.3
59	20.2.1
58	20.2
55	20.1.1
54	20.2.1
49	19.4.1
48	19.4
46	19.3.1
44	19.3
41	19.2
37	2.5.1