

TARA User Guide

Table of content

Introduction	3
Step-by-Step-Guide	3
Creating a new TARA file	3
Add a new row (empty rating)	5
TARA layout as per SAE J3061	5
TARA layout as per ISO 21434	5
Deleting rows (rating)	6
Creating threats and link them to TARA	7
Creating threats directly in the TARA	7
Creating threats in security goal view	8
Linking threats to ATA	8
Creating assets	10
Creating an asset in the system modeler	10
Creating Assets directly in the TARA	11
Defining potential vehicle threats	12
Defining Potential vehicle threats without a choice list	12
Selecting potential vehicle threats from predefined choice lists	12
Defining hazards	14
Defining Hazards without a catalog	14
Defining hazards with a catalog	15
Evaluation of the security level	17
Creating security goals	18
Creating Security goals directly in the TARA	18
Creating security goals in Security Goal view	19
The User Interface	20
TARA Editor [1]	20
TARA explanation	20
Context Menu of TARA	21
Overview and PSS View [2]	23
Security Goal view [3]	23
Model Explorer / Catalogs / Object lists [5]	23
Model Explorer	23
Catalogs	24

Introduction

Threat Analysis and Risk Assessment (TARA) is a methodology to identify threat scenarios, rate the feasibility of an attack as well as the impact of related damage scenarios and to assess the risk and residual risk of the identified threat scenarios. The TARA consists of several components or steps as described in corresponding guidelines and norms.

SOX supports the following guidelines and norms:

- SAE J3061 (SAE)
- ISO/SAE 21434 (ISO)

You can work with different variants and operation statuses.

Step-by-Step-Guide

The following sections guide you through the creation of a TARA step by step.

Creating a new TARA file

Precondition: A SOX project was created, and the workbench perspective is active.

1. Go to the Repository view and right-click on the TARA folder in the project.

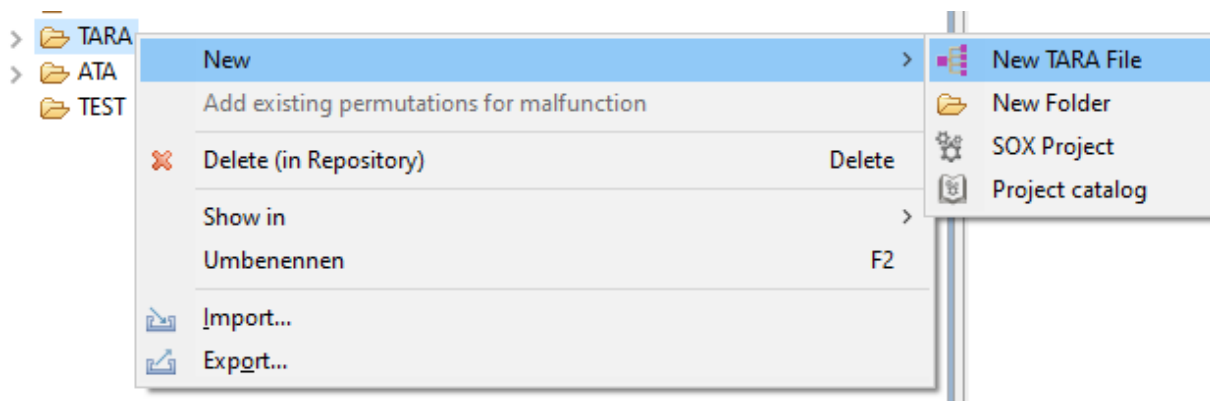


fig. 1 New TARA file context menu.

2. Choose New > New **TARA File**.
 - The "New TARA file" dialog opens.

New TARA file

Please fill in all mandatory fields

Target folder: Projects/Test Projects/Security Project 1/TARA 3 Browse...

Filename: 4

Norm: J3061_SAE 5

Profile: J3061 (Standard) 6

Description: 7

Objective: 7

Foundation: 7

8 Finish Cancel

fig. 2 New TARA file dialog.

3. Click on **Browse...** and choose TARA as target folder.
4. Enter a filename for the TARA file.
5. Choose the security norm you want to create your TARA according to.
6. Choose the security profile.

► The profile determines how impact level and threat level respective impact rating and attack feasibility are combined to the security level (SAE J30619) respective risk value (ISO 21434).

► **SAE J3061:** The standard security profile is implemented in SOX.

► **ISO 21434:** Select one of the profiles symmetric (standard), asymmetric and low risk.

7. The fields "Description", "Objective" and "Foundation" are optional and can be used for detailed descriptions of the TARA document.
8. Click on **Finish**.

→ A TARA file will be created and added to the TARA folder.

Add a new row (empty rating)

To fill the TARA a new row needs to be added.

TARA layout as per SAE J3061

Precondition: A TARA file was created and is active.

	BID	Status	Priority	Threat			Hazard		Impact Level			
				Asset	Threat Category	Security Attribute	Potential vehicle	Potential worst	Safety	Financial	Operational	Privacy and
1	TRA6	Unrated	★									

fig. 3 TARA editor tool bar - add new row

Add a new row (empty rating) by clicking the plus icon at the TARA editor tool bar.

TARA layout as per ISO 21434

Precondition: A TARA file was created and is active.

Ratings (ISO 21434 (Standard))

type filter text

☐ Regular expressions
 ☐ Automatically set state "rated/unrated"

Drag column to group

	BID	Status	Priority	Threat		Impact Level				Justification	IL sum	Impact Level (IL)	Threat Scenario
				Asset	Cyber Security	Safety	Financial	Operational	Privacy and				
1	TRAS	Unrated	★										

fig. 4 TARA editor tool bar - add new row

Add a new row for impact rating (empty) by clicking the plus icon at the TARA editor tool bar.

- The new row appears in blue color (impact rating). Here you can add or create assets, set the cybersecurity property, and rate the impact of associated damage scenario.

By clicking the icon for “add threat scenario / attack path” a new row for defining a threat (threat scenario) and rating the related attack feasibility or defining individual attack path is added depending on type of cell that is active.

- If a blue cell is active (impact rating) the added row appears in green color (attack feasibility rating, see fig. 5). Here you can add or create threats and rate the attack feasibility.
- If a green cell is active (attack feasibility rating) the added row appears in red color (attack path, see fig. 6). Here you can add or create attack paths and rate the attack feasibility individually for each attack path associated with a threat scenario.

	BID	Status	Priority	Threat		Impact Level				Justification	IL sum	Impact Level (IL)	Threat Scenario	Description
				Asset	Cyber Security	Safety	Financial	Operational	Privacy and					
1	TRA30	Unrated	★	Asset 1 [->1 0->1]	Confidentiality									
2	TRA31	Unrated	★	Asset 1 [->1 0->1]	Confidentiality									

fig. 5 TARA editor tool bar - add new (green) row for attack feasibility rating

Ratings (ISO 21434 (Standard))

type filter text ☐ Regular expressions ☐ Automatically set state "rated/unrated"

Drag column to group

	BID	Status	Priority	Threat		Impact Level				Justification	IL sum	Impact Level (IL)	Threat Scenario	Description
				Asset	Cyber Security	Safety	Financial	Operational	Privacy and					
1	TRA30	Unrated	★	Asset 1 [->1 0->]	Confidentiality									
2	TRA31	Unrated	★	Asset 1 [->1 0->]	Confidentiality								[TH2] Threat 2 [V1]	
3	TRA32	Unrated	★	Asset 1 [->1 0->]	Confidentiality									

fig. 6 TARA editor tool bar - add new (red) row for individual attack paths

Deleting rows (rating)

When a row or rating should be deleted, the created threat, asset and security goal will still be available for further usage.

Precondition: A TARA file was created containing at least one row (rating).

Ratings (ISO 21434 (Standard))

type filter text ☐ Regular expressions ☐ Automatically set state "rated/unrated"

Drag column to group

	BID	Status	Priority	Threat		Impact Level				Justification	IL sum	Impact Level (IL)	Threat Scenario
				Asset	Cyber Security	Safety	Financial	Operational	Privacy and				
1	TRAS	Unrated	★	Asset 1 [->1 0->]	Confidentiality	Moderate	Negligible	Major	Moderate		21	Medium	

fig. 7 TARA editor tool bar - deleting a row (rating)

1. Select the rating, that should be deleted.
2. Select the red cross button, to delete the rating.

Creating threats and link them to TARA

Threats can be created either directly in the TARA or in the security goal view.

Note: The layout depends on the norm selected (J3061 or ISO 21434) but the procedure is the same. If ISO 21434 is selected a row for attack feasibility rating needs to be added first (see section *TARA layout as per ISO 21434* on page 3).

Precondition: A TARA file was created and is active.

Creating threats directly in the TARA

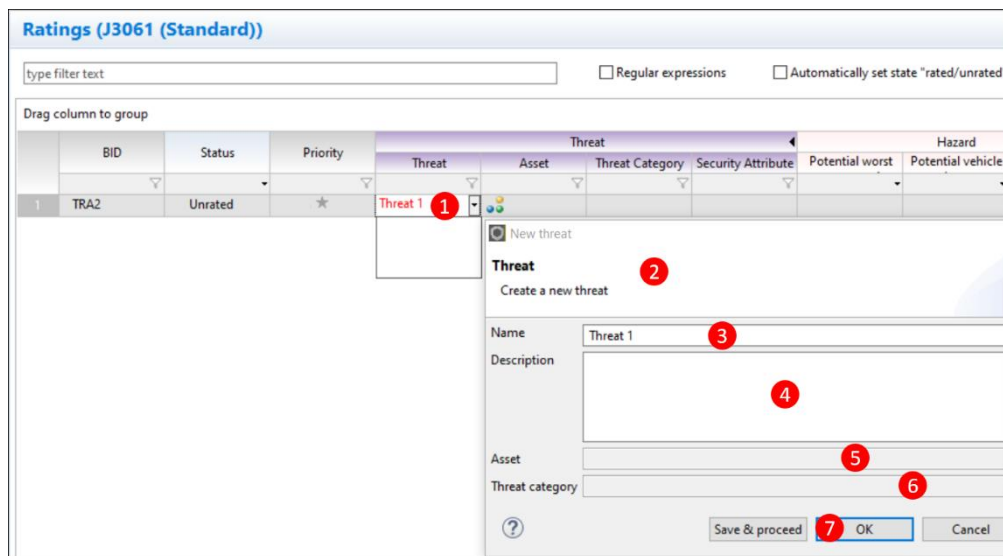


fig. 8 Defining Threats in TARA

1. Double click on a cell in column "Threat" and fill in the name of the threat.
 - Confirm the name of the threat with **Return** or with a click on a free space in the TARA.
2. The "New Threat" dialog appears.
3. The name of the threat is automatically filled in.
4. Add a description (optionally)
5. Choose an asset (if possible)
 - If assets were identified before (e.g. in the System Modeler) than choose an asset.
 - If there are no assets identified before, leave it open.
6. Select a threat category (regarding to STRIDE)
7. Confirm the threat by clicking on "OK".
 - A threat was created with a Threat ID. The threat is shown in the security goal view under the security goal "orphaned threats" because there is no security goal that is connected with the threat.

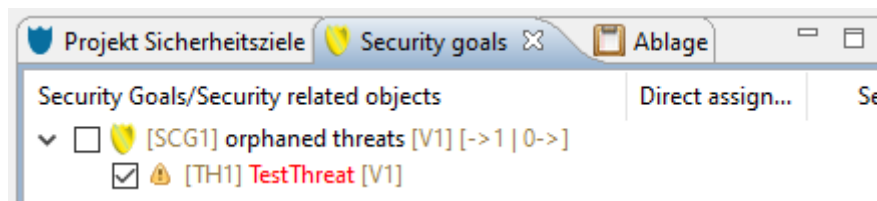


fig. 9 Threat assignment to Security Goal "orphaned threats"

Creating threats in security goal view

The following steps are explaining how to create a threat in the security goal view.

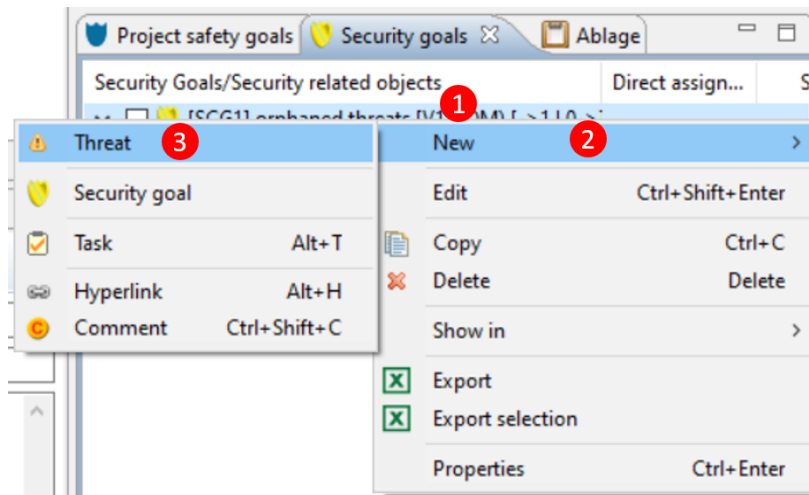


fig. 10 Defining Threat in Security Goal view

1. Right Click on the security goal
 2. Select "New"
 3. Select "Threat"
- The "New Threat" dialog from fig. 8 appears. Fill in the fields to create the threat.
 - Now the threat can be selected in the TARA in the column "Threat".

Linking threats to ATA

An attack tree analysis can be used to derive the attack feasibility of a threat more precisely. A new ATA document can be directly created from threat in TARA.

Precondition: A TARA was created containing at least one new threat.

1. Right-click on the threat.

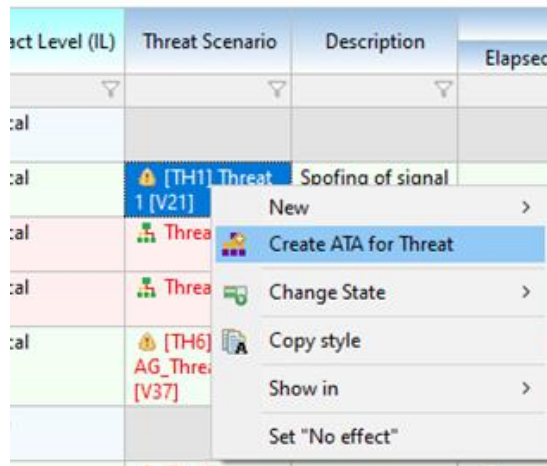


fig. 11 Create new ATA file from threat in TARA

2. Choose "Create ATA for Threat"

► The "New ATA file" Dialog opens.

3. Click on **Browse...** to choose ATA as target folder.
4. Enter a filename for the ATA File.
5. The field "Description" is optional and can be used for detailed descriptions of the ATA document.
6. The security norm is defined by TARA.
7. The security profile is defined by TARA.
8. The threat / threat scenario is filled automatically.
9. New threat / threat scenario is filled automatically.
10. Click on **Finish**.

→ An ATA File was created and added to the Repository.

New ATA file

Target folder: Projects/Test Projects/Security Project **3** Browse...

Filename: Threat 1 **4**

Description: **5**

Norm: ISO_21434 **6**

Profile: Standard **7**

Threat/Threat Scenario: [TH1] Threat Threat 1 [V21] **8**

New Threat/Threat Scenario Name: Threat 1 **9**

10 Finish Cancel

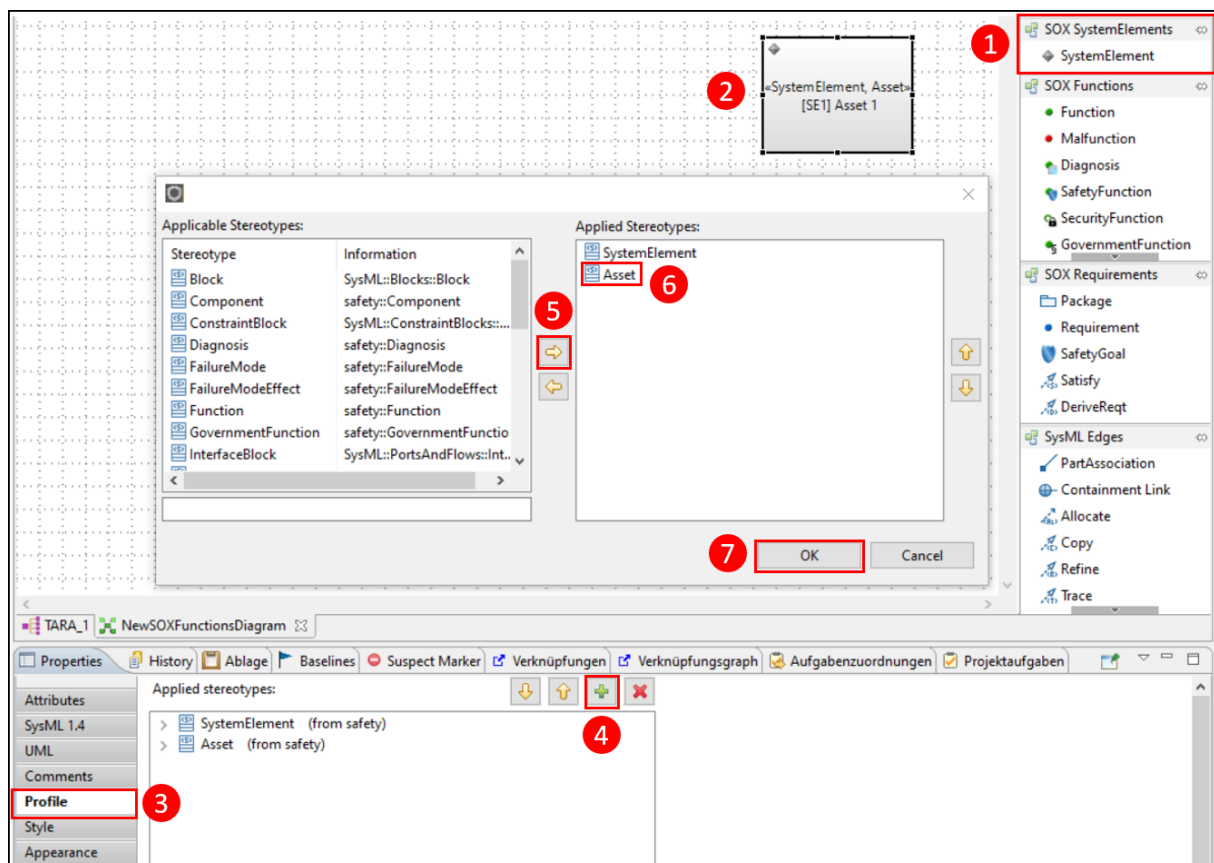
fig. 12 New ATA file dialog

Creating assets

SOX supports two types of assets, primary and secondary (supportive) assets, where primary assets are of higher order. Assets can be defined either in the system modeler or directly in the TARA.

Creating an asset in the system modeler

Precondition: A TARA file was created and is active.



1. Create an element in the UML/SysML modelling base (SOX Functions Diagram).
2. Enter a name for the created element.
3. In the properties view select **Profile** showing all stereotypes assigned to the element.

► The stereotype "Asset" needs to be assigned to the element.

4. Click on the plus icon and select stereotype "Asset" in the listing of **Applicable Stereotypes** on the left.
5. Move the stereotype "Asset" to the listing of **Applied Stereotypes** on the right by clicking the right arrow.
6. The stereotype "Asset" was moved to the right.
7. Confirm with **OK**.

► Now the element has two stereotypes, "SystemElement" and "Asset". In SOX elements having stereotype "Asset" and at least one additional stereotype are defined as secondary assets.

► In order to create a primary asset move all other stereotypes to the left in step 5 or remove them in the **Profile** tab in the properties view by clicking the remove icon.

Elements having stereotype “Asset” can be selected in the TARA in column “Asset” to define threats.

Creating Assets directly in the TARA

Precondition: A TARA file was created and is active.

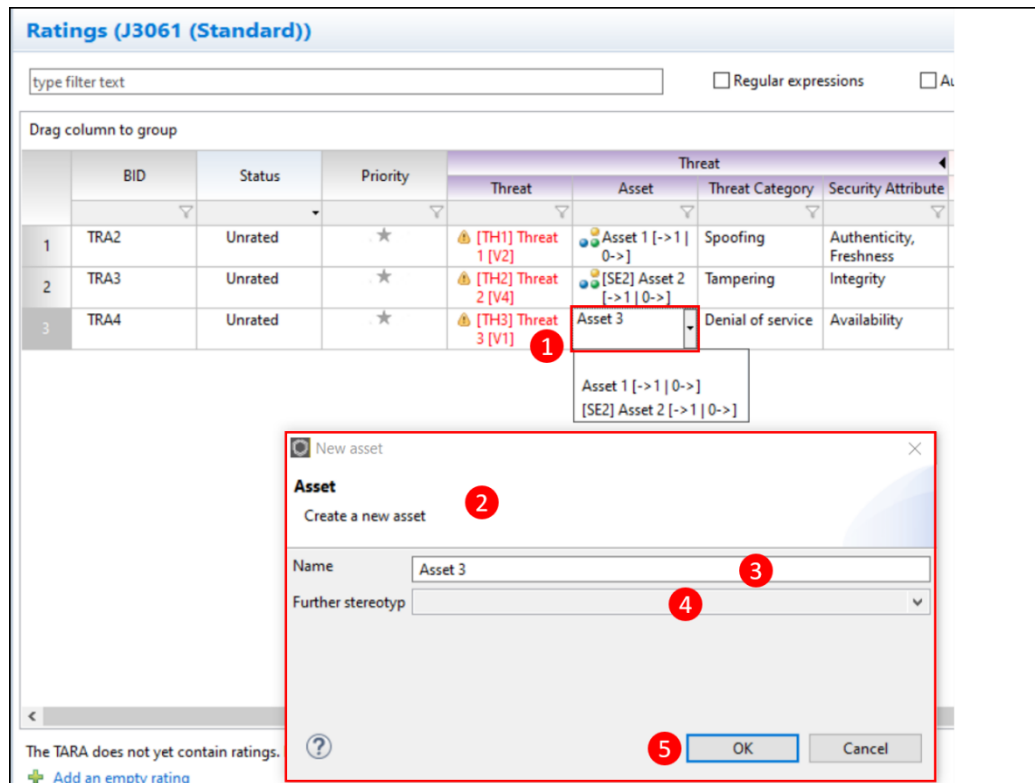


fig. 13 TARA editor tool bar add empty rating

1. Double click on an empty cell in column “Asset” and fill in the name of the asset.
 - Confirm the name of the asset with **Return** or with a click on a free space in the TARA.
2. The “New Asset” dialog appears.
3. The name of the asset is automatically filled in.
4. Add a further stereotype (optionally).
5. Confirm with **OK**.

► An asset was created. The Asset is shown in the PSS View, in the Model Explorer and the Repository View.

► The asset is automatically connected with the Threat.

► The asset is of type primary if no further stereotypes are added in step 4. Otherwise, it is a secondary asset.

Defining potential vehicle threats

SOX provides catalogs which contain standard values for the situation parameters. But you also can define individually catalogs and values. Read the chapter Customized Choice Lists for more information.

Precondition: Threats were created.

Potential vehicle threats can be defined either with or without choice lists.

Defining Potential vehicle threats without a choice list

By defining potential vehicle threats without a choice list, the threats can just be used in the SOX project, where the potential vehicle threats were created.

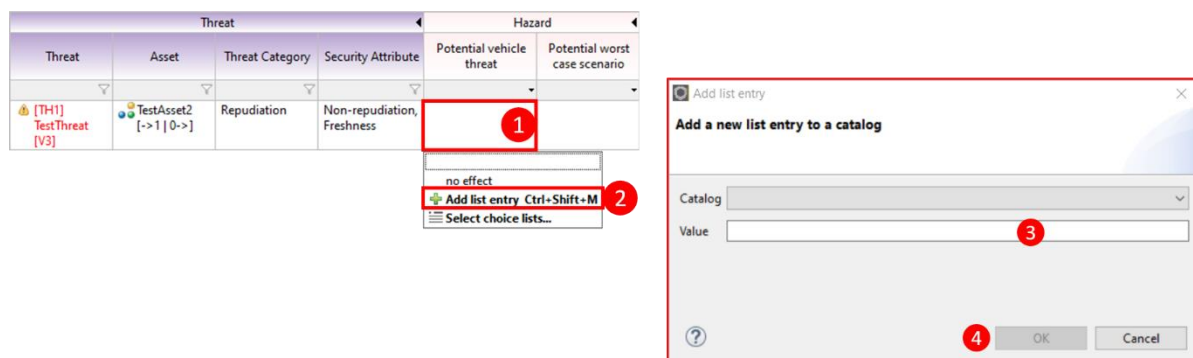


fig. 14 Defining potential vehicle threats not with a Choice List

1. Double click in the potential vehicle threat cell
2. Select "Add list entry" or use the shortcut
 - When you don't have a safety related threat (e.g. when the attacker just want private data), just select "no effect"
3. Fill in the potential vehicle threat in the value box
4. Confirm the potential vehicle threat with "OK"

Selecting potential vehicle threats from predefined choice lists

Choice lists are special kinds of catalog. By defining potential vehicle threats within such a catalog, the potential vehicle threats can be used across multiple SOX projects.

Different kinds of potential vehicle threats can be grouped within different catalogs. By selecting specific catalogs only specific potential vehicle threats are shown.

1. Double Click in the "potential vehicle threat" cell.
2. Select "Select choice lists..."
3. The "Choice list selection" dialog appears.
 - When there are already created choice lists, select them and confirm with "OK".
4. Select "Add new catalog"
5. Select the Target folder of the Choice List (with Browse...)
6. Enter the name of the Choice List
7. Enter a Description (optionally)
8. Confirm the choice with "Finish".

- Select the new created choice list and confirm with "OK".
- 9. Select the plus icon to add new potential vehicle threats to the created choice list.
- 10. Add the name of the potential vehicle threat.
- 11. If more potential vehicle threats should be created, select "OK and next".
- 12. When no more potential vehicle threats should be created, confirm with "OK".
- Go back to the TARA to select the new created potential vehicle threats.
- To create new potential vehicle threats in the TARA for the choice list, select "Add list entry".

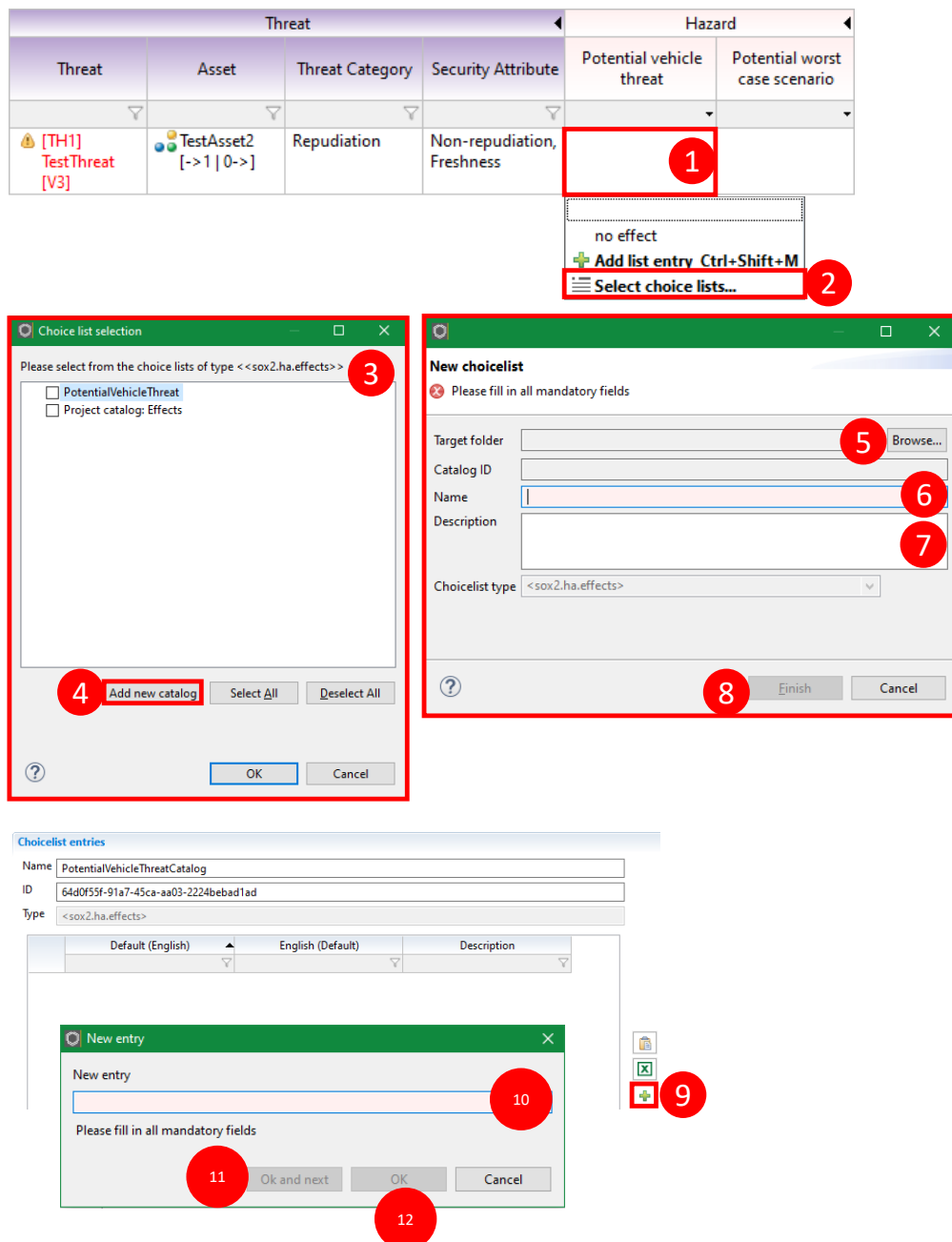


fig. 15 Defining potential vehicle threats with Choice Lists

Defining hazards

SOX provides catalogs which contain standard values for the situation parameters. But you also can define individually catalogs and values. Read the chapter Customized Choice Lists for more information.

Precondition: Threats were created.

Hazards can be defined either with or without catalogs.

Defining Hazards without a catalog

By defining potential vehicle threats without a Choice List, the threats can just be used in the SOX project, where the potential vehicle threats were created.

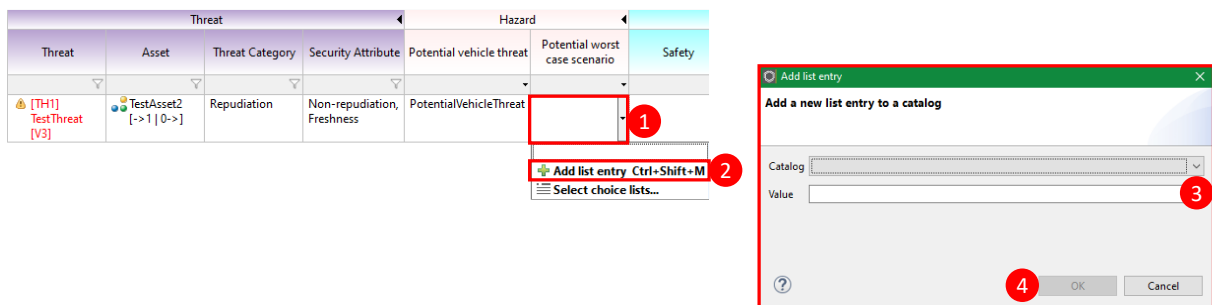


fig. 16 Defining Hazards not with a catalog

1. Double Click in the Hazard cell
2. Select "Add list entry" or use the shortcut
 - When you don't have a safety related threat (e.g. when the attacker just want private data), don't entry a value to the cell and leave it unfilled.
3. Fill in the Hazard in the value box
4. Confirm the Hazard with "OK"

Defining hazards with a catalog

By defining Hazards with a catalog, the Hazards need to be defined one time and can be used across multiple SOX projects and in the HARA. Hazards, that were defined in the HARA, can be used in the TARA as well by activating the catalog and selecting the needed Hazards.

Different kinds of hazards can be grouped within different catalogs. By selecting specific catalogs only specific hazards are shown.

1. Double Click in the "potential vehicle threat" cell
2. Select "Select choice lists..."
3. The "Choice list selection" dialog appears
 - ▶ When they are already created catalogs, select them and confirm with "OK"
4. Select "Add new catalog"
5. Select the target folder of the catalog (with "Browse")
6. Enter the name of the catalog
7. Enter a description (optionally)
8. Confirm the choice with "Finish"
- ▶ Select the new created catalog and confirm with "OK"
9. Select the Hazard icon to add new Hazards to the created catalog
10. Add the name of the Hazard
11. Add a Description
12. If more Hazards should be created, select "OK and next"
13. When no more Hazards should be created, confirm with "OK"
- ▶ Go back to the TARA to select the new created Hazards
- ▶ To create new Hazards in the TARA for the catalog, select "Add list entry"

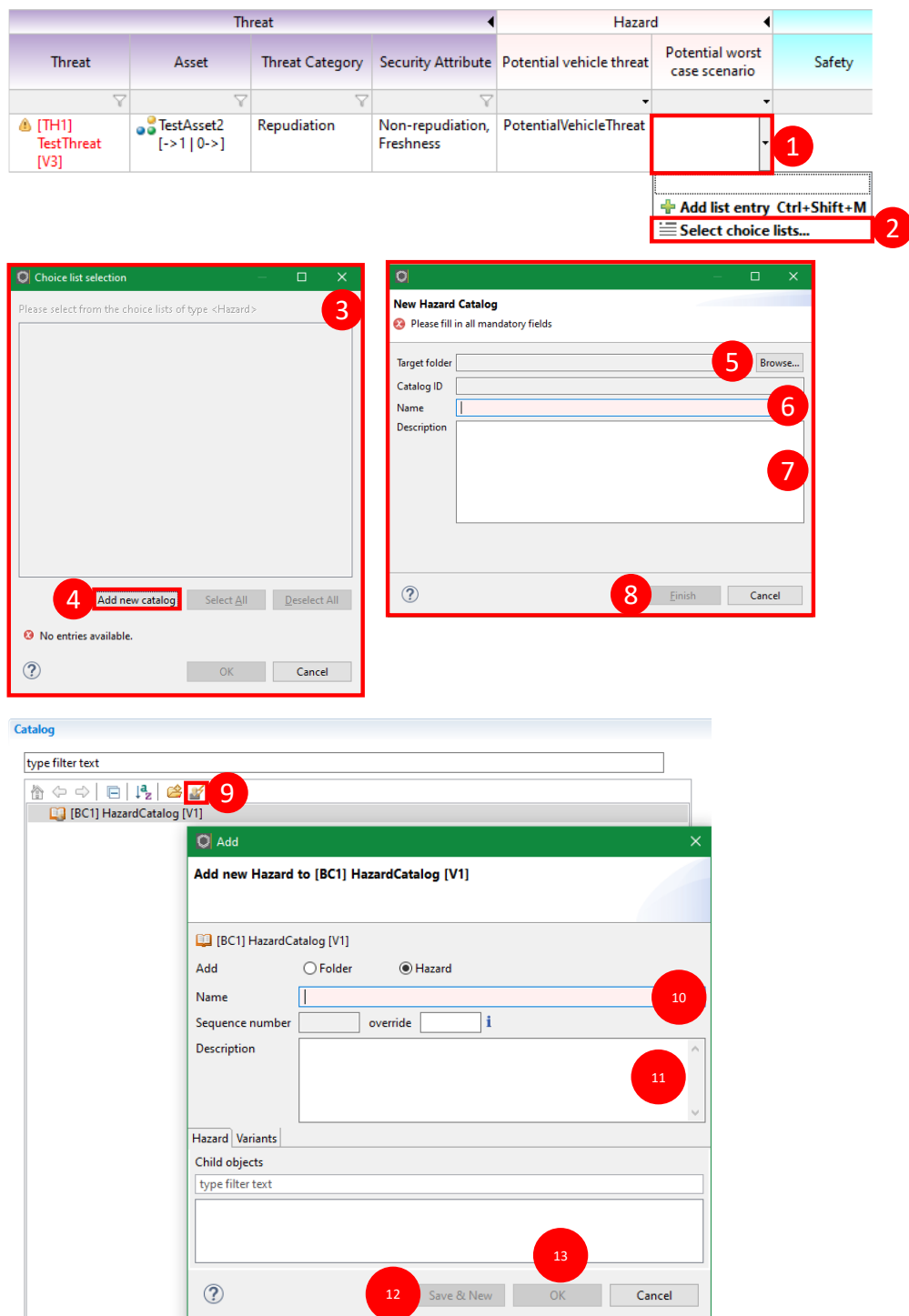


fig. 17 Defining Hazards with Catalogs

Note

The Hazards are shown in the PSS View. To reuse Hazards in other SOX projects, you need to create a Hazard Catalog in the Public folder (Choice-List). Then just add the catalog in the TARA.

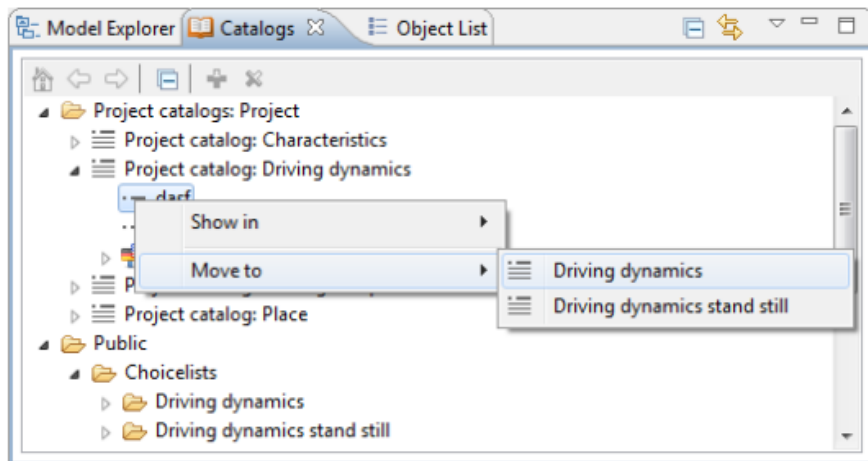


fig. 18 Context menu Move to.

Evaluation of the security level

Once the threats for the relevant assets are identified, the next step is to rank the threats.

The impact of a threat is given by the impact level parameter (Impact Level (IL)). It is determined by the ratings in each threat category, i.e. Safety, Financial, Operational and Privacy and Legislation.

Similarly, the Threat Level (TL) (SAE J3061) or attack feasibility rating (ISO 21434) is determined by the rating of the corresponding parameters. In case of SAE J3061 that is Expertise, Knowledge about TOE, Window of Opportunity, and Equipment, whereas for ISO 21434 the parameters are elapsed time, specialist expertise, knowledge of the item or component, window of opportunity and equipment.

To set / edit the rating of a parameter double-click into a cell and select a rating from drop-down list.

Impact Level and Threat Level Rating according to **SAE J3061** are shown in the figures below. For ISO 21434 the procedure is basically the same.

Impact Level				Description	IL sum	Impact Level (IL)
Safety	Financial	Operational	Privacy and Legislation			
No impact	No impact	No impact	No impact			
Low	Low	Low	Low			
Medium	Medium	Medium	Medium			
High	High	High	High			

Enter text

OK Cancel

fig. 19 Impact Level rating parameters and text entry for description

Threat Level				Description	TL sum	Threat Level (TL)
Expertise	Knowledge about TOE	Window of Opportunity	Equipment			
Layman	Public	Critical	Standard			
Proficient	Restricted	High	Specialized			
Expert	Sensitive	Medium	Bespoke			
Multiple experts	Critical	Low	Multiple bespoke			

Enter text

OK Cancel

fig. 20 Values for threat level parameters and text entry for description

Creating security goals

Security goals can be created either directly in the TARA and in the security goal View.

Precondition: Threat was created and the security level was calculated (values of parameter of Impact and Threat/Attack Feasibility Rating were selected).

Creating Security goals directly in the TARA

The following steps are explaining how to create a Security goal directly in the TARA.

New security goal

New security goal

Name

SecurityGoal

Secure State

Norm

ISO_21434

Security level

QM

Name

Secure State

Safet...

Norm

Save & proceed

OK

Cancel

Security

Security level

Security goal

Secure state

ISOLOW

SecurityGoal

[SCG1] orphaned threats [V1] [-> 1 | 0]

fig. 21 Creating security goals directly in the TARA

1. Double Click on the security goal cell and fill in the name of the security goal
 - Confirm the name of the security goal with Shortcut Ctrl + Return or with a click on a free space in the TARA
2. The "New security goal" dialog appears

3. The name of the security goal is automatically filled in
 4. Add a Secure State
 - The Norm is automatically filled in and is according to the Norm of the TARA
 - The security level is set per Default on QM because it will inherit the security level from the Rating automatically
 5. Confirm the security goal by clicking on "OK"
- A security goal was created with a security goal ID. The security goal is shown in the Security Goal view and the Threat that is connected in the Rating with the security goal. The security level is been inherited from the Rating of the Threat in the TARA.
- The Threat moves automatically to the security goal after connecting the security goal to the Rating

Security Goals/Security related objects	Security level	Secure State
<input type="checkbox"/> [SCG1] orphaned threats [V2] [->1 0->]	QM	
<input checked="" type="checkbox"/> [SCG2] SecurityGoal [V1] [->1 0->]	ISOLOW	TestSecureState
<input checked="" type="checkbox"/> [TH1] TestThreat [V4]		

fig. 22 Security goal in Security Goal view after creating security goal in TARA

Creating security goals in Security Goal view

The following steps are explaining how to create a Threat in the Security Goal view.

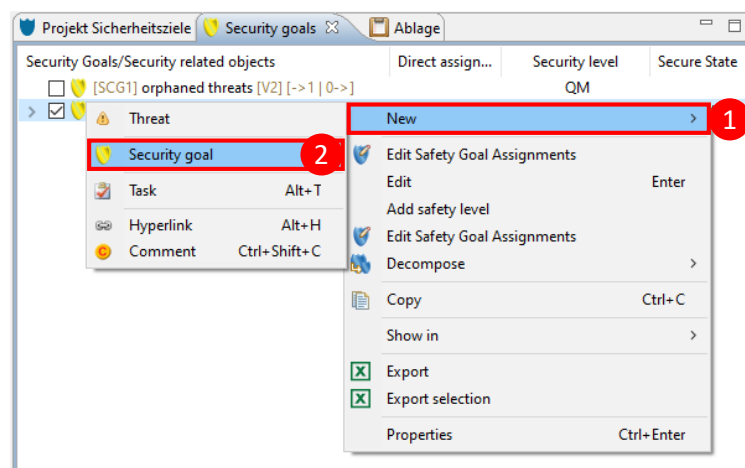


fig. 23 Defining Threat in Security Goal view

1. Right Click in the Security Goal view
 2. Select "New"
 3. Select "Security Goal"
- The "New security goal" dialog from fig. 21 appears. Fill in the fields to create the security goal.
- If several security goal should be created, select instead of "OK" "Save & proceed".
- The security goal can be chosen in the TARA in the column "Security Goal".

The User Interface

Below you see all the standard view in the TARA perspective. Remember that you can always (re-) open views by going to the menu bar and clicking **Window > Show View**. You can also arrange the views with drag & drop.

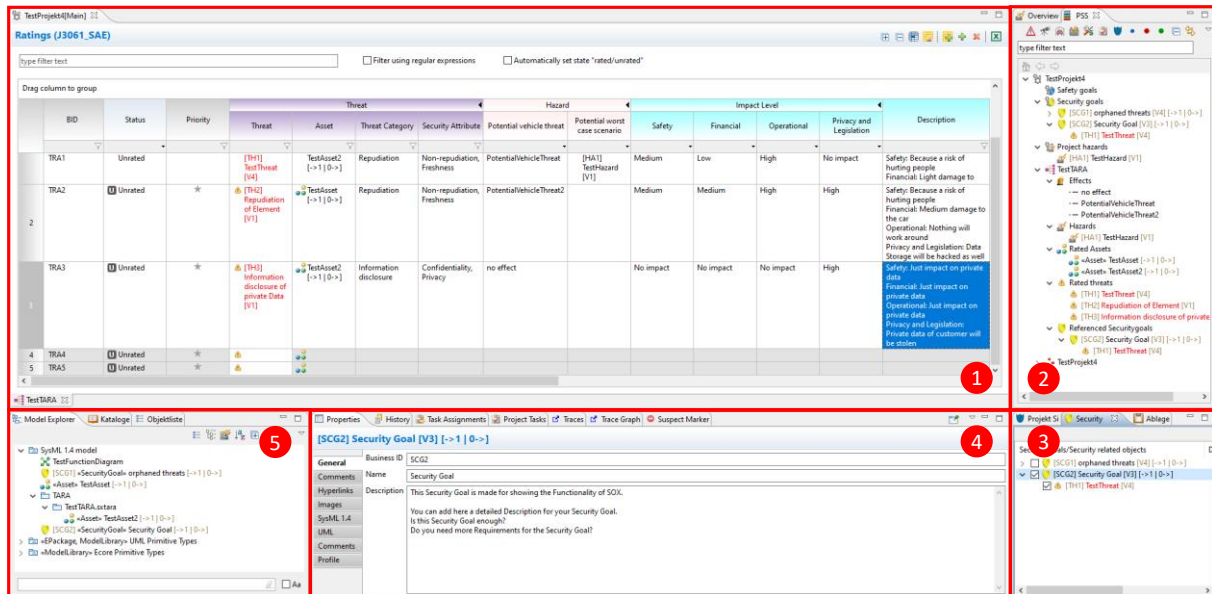


fig. 24 The User interface of the TARA module

[1] TARA Editor

[2] Overview/PSS

[3] Security Goals View

[4] Properties / History / Task Adjustments / Project tasks / Traces / Trace Graph / Suspect Marker

[5] Model Explorer / Catalogs / Object lists

TARA Editor [1]

TARA explanation

*for TARA according to SAE J3061

** for TARA according to ISO/SAE 21434

*** for TARA according to SAE J3061 and ISO 21434

*** There is a prioritization of each line in the "Priority" column (It is just for the User):

- 1 star (low)
- 2 stars (medium)
- 3 stars (high priority).

*** In the TARA editor the whole TARA is shown.

*** Threats must be defined. Threats are a combination of Assets and the Threat Category. Currently STRIDE Threat Categories are available.

** The Damage Scenario must be determined. The Damage Scenario is an association between potential vehicle threats and the Hazards. The assessment of the Damage Scenario is carried out through the Impact Level.

** The Threat Scenario must be determined. The assessment of the Threat Scenario is carried out through the Attack Feasibility Rating.

*** The security goal must be defined. The security goal is determined as the inverse of a Threat. The security goal can be created directly in the correct cell. Add security goals and then their Secure State will be shown as well. The Threat will be automatically moved to the security goal in the Security Goal view.

Context Menu of TARA

The context menu of the TARA shows a couple of functions.

Precondition: TARA was created, Threats and Assets were defined



fig. 25 Context menu in the TARA editor

New

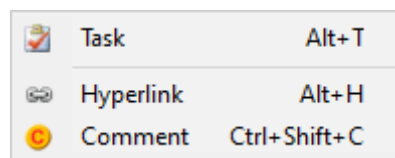


fig. 26 Context menu "New"

When clicking at "New" in the context menu of the TARA, tasks, hyperlinks and comments can be added.

Edit

With Edit the cell can be edited.

Change State

With Change State the state of the rating can be switched. It shows the current state of the rating. The default state machine rules is shown in fig. 27. The order and the selection of the states can be individualized as well.

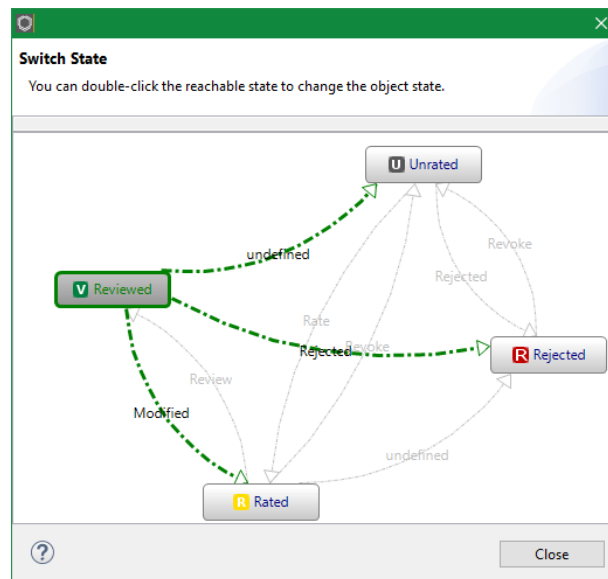


fig. 27 Default state machine rules

Show in

With show in, the diagrams, where e.g. the assets are shown, can be selected and the assets will be shown directly in the diagrams e.g. a FMEA.

No effect

With no effect the potential vehicle threat status will be switched to “no effect” and the rating of the Impact and Threat/Attack Feasibility Level will be deleted.

Drag column to group

Same values of the columns can be displayed in groups. For this drag a column [2] and drop it to the corner upper left [1].

The screenshot shows the TARA editor interface with a table of ratings. The table has columns for BID, Status, Priority, Threat, Asset, Threat Category, Security Attribute, Potential vehicle threat, Potential worst case scenario, Safety, Financial, Operational, Privacy and Legislation, and Description. The rows are grouped by BID, with groups 1, 2, 3, 4, and 5. The first column (BID) is highlighted in grey. The second column (Status) is highlighted in red. The third column (Priority) is highlighted in blue. The fourth column (Threat) is highlighted in green. The fifth column (Asset) is highlighted in yellow. The sixth column (Threat Category) is highlighted in orange. The seventh column (Security Attribute) is highlighted in purple. The eighth column (Potential vehicle threat) is highlighted in pink. The ninth column (Potential worst case scenario) is highlighted in light blue. The tenth column (Safety) is highlighted in light green. The eleventh column (Financial) is highlighted in light yellow. The twelfth column (Operational) is highlighted in light orange. The thirteenth column (Privacy and Legislation) is highlighted in light purple. The fourteenth column (Description) is highlighted in light blue.

fig. 28 TARA editor with grouped column

Greyed rows with the corresponding group names, displayed at the first column, will appear. They contain the corresponding ratings in a tree structure [3]. According to this groups can be expanded and collapsed. Further columns can be added to the groups' selection [1]. To ungroup, right-click on a group selection [1] and select ungroup by.

Overview and PSS View [2]

The Overview View is a part of the PSS View. The PSS View shows the whole Project Elements whereas the Overview View show only the elements implemented in the TARA. The Overview View of the TARA shows the same Categories like the Repository View of the TARA:

- Effects
- Hazards
- Rated Assets
- Rated Threats
- Referenced security goals

Security Goal view [3]

The Security Goal view shows:

- Threats without an allocated security goal
 - These Threats are shown in security goal “orphaned Threats”
- Security goal with no threats
- Security goal allocated with threats from rating
- Security goal with created threats (not to mix up with threats from rating)
- If security goal is assigned in a Threat

Note

A security goal can be allocated with multiple Threats but only one Threat can be allocated with one security goal

Model Explorer / Catalogs / Object lists [5]

Model Explorer

The Model Explorer shows every element and connection, that was defined. If elements encapsulated within each other, like a block has multiple parts in it, like in a standard Internal Block Diagram, than the overall Element is shown and you can click on the arrows on the left site of the element, to see the encapsulated elements. When elements are created in methods, like the TARA, there are folders with the methods names that inherits the created elements.

The Model Explorer shows:

- Folder of Methods
- Diagrams
- Security goals
- Elements (e.g. Assets and Systemelements)(Stereotypes)
- Functions
- Malfunctions
- Connection between Elements

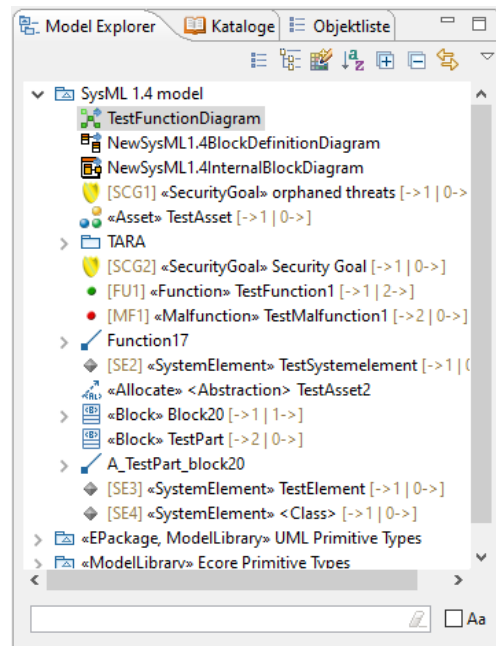


fig. 29 Model Explorer

Catalogs

There are three types of catalogs:

- Project catalogs
 - ▶ Specific catalogs for the SOX Project
- Public catalogs
 - ▶ Editable catalogs and catalogs, which were created in the SOX Project
 - ▶ These catalogs can be used in every SOX Project in a Repository
- System catalogs
 - ▶ These catalogs are not editable in SOX
 - ▶ They are just editable by downloading them and manipulating them with an Editor and importing them again