ETAS ESCRYPT CycurRISK V2.31.10

User Guide

www.etas.com

Copyright

ESCRYPT CycurRISK V2.31.10 I User Guide R01 EN I 07.2026

Contents

1 Introduction

1.1 Intended Use

CycurRISK is used to generate and manage Threat Analysis and Risk Assessments (TARA) according to ISO/SAE 21434. It is designed to uncover and evaluate the potential attack surfaces in your automotive systems.

CycurRISK is not intended for the following:

- Use in productive or field operation phase
- Use in a vehicle that is meant for productive or field operation
- Use as part of a life support system
- Use as part of a medical application
- Use in applications in which misuse can lead to injury or damage

1.2 Target Group

This user guide addresses cybersecurity engineers working in the fields of automotive and embedded systems.

1.3 Classification of Safety Messages

Safety messages warn of dangers that can lead to personal injury or damage to property:

DANGER

DANGER indicates a hazardous situation that, if not avoided, will result in death or serious injury.

WARNING

WARNING indicates a hazardous situation that, if not avoided, could result in death or serious injury.

CAUTION

CAUTION indicates a hazardous situation that, if not avoided, could result in minor or moderate injury.

NOTICE

NOTICE indicates a situation that, if not avoided, could result in damage to physical property.

ATTENTION

ATTENTION indicates a situation that, if not avoided, could result in damage to digital property like data loss, data corruption and system vulnerability.

1.4 Safety Information

Refer to the following safety instructions and the technical documentation available to download from the ETAS website www.etas.com. Keep the information provided in a safe place.

Failure to comply with the safety instructions may lead to the risk of damage to life and limb or property. The ETAS Group and its representatives shall not be liable for any damage or injury caused by improper operation or use of the product.

Only use the product if you have read and understood the information concerning safe operation and have the required qualifications and training for this product. If you have questions about safe operation, contact ETAS:

- Technical Support: www.etas.com/hotlines
- ETAS contact partners by region: www.etas.com/contact

The product is only approved for the applications described in the technical documentation. When using and operating this product, all applicable regulations and laws must be observed.

ETAS products made available as beta versions or prototypes of firmware, hardware and/or software are to be used exclusively for testing and evaluation purposes. These products may not have sufficient technical documentation and not fulfill all requirements regarding quality and accuracy for market-released series products. The product performance may therefore differ from the product description. Only use the product under controlled testing and evaluation conditions. Do not use data and results from beta versions without prior and separate verification and validation and do not share them with third parties.

Before starting up the product, check whether there is a Known Issue Report (KIR) for that product version: www.etas.com/kir (password: KETASIR). Note the information given in the report.

Program codes or program control sequences that are created or changed via ETAS products, as well as all types of data obtained through the use of ETAS products, must be checked for their reliability and suitability prior to use or distribution. Only use these codes or sequences in public areas (e.g., in road traffic) if you have ensured that the application and product settings are safe through testing in selfcontained and designated testing environments and circuits.

This ETAS product allows you to influence safety-relevant systems or data (e.g. in motor vehicles, vehicle components and test benches). In the event of a malfunction or a hazardous situation, it must be possible to put the system into a safe state (e.g., emergency stop or emergency operation).

1.5 Data Protection

If the product contains functions that process personal data, legal requirements of data protection and data privacy laws shall be complied with by the customer. As the data controller, the customer usually designs subsequent processing. Therefore, he must check if the protective measures are sufficient.

1.6 Data and Information Security

To securely handle data in the context of this product, see the next sections about data and storage locations as well as technical and organizational measures.

1.6.1 Data and Storage Locations

The following sections give information about data and their respective storage locations for various use cases.

1.6.1.1 License Management

When using the ETAS License Manager in combination with user-based licenses that are managed on the FNP license server within the customer's network, the following data are stored for license management purposes:

Data

- Communication data: IP address
- User data: Windows user ID

Storage location

- FNP license server log files on the customer network

When using the ETAS License Manager in combination with host-based licenses that are provided as FNE machine-based licenses, the following data are stored for license management purposes:

Data

- Activation data: Activation ID
  - Used only for license activation, but not continuously during license usage

Storage location

- FNE trusted storage

  C:\ProgramData\ETAS\FlexNet\fne\license\ts

1.6.2 Technical and Organizational Measures

We recommend that your IT department takes appropriate technical and organizational measures, such as classic theft protection and access protection to hardware and software.

2 About CycurRISK

2.1 Introduction

CycurRISK is a TARA software tool that helps you uncover and evaluate potential attack surfaces in automotive systems and architectures at an early stage.

It allows you to systematically identify and analyze threats via attack feasibility (based on attack potential) using attack trees. Damage scenarios are used to assess the impact on road users and your business.

Thus, this TARA software tool enables you to prioritize risks and countermeasures and to create a security concept that complies with the requirements of security engineering processes, and ISO/SAE 21434.

Fig. 2-1: ESCRYPT CycurRISK logo

The main features of CycurRISK are as follows:

- Workflow-oriented guidance
- User-friendly GUI
- Direct comparison of initial and residual risks
- Automatic management summary
- Integrated attack tree editor
- Support of attack potential method with automatic attack potential computation
- Dedicated mode for TARA reuse
- Sophisticated functionality for variant handling to create and compare TARAs for numerous product variants in one project
- Models and analyses of hierarchical systems of features and com-

ponents

- Collaboration on TARA projects on locally hosted servers
- Review functionality

CycurRISK highlights are as follows:

- Widely used solution with professional maintenance, support, and frequent updates.
- Compliant with the requirements of ISO/SAE 21434.
- Fully configurable report templates and methodologies.
- Tool classification according to ISO 26262 available and tool qualification for all use cases for TCL 2/3 performed.

2.2 Restrictions

2.2.1 Parallel Installation

CycurRISK V2.31.10 cannot be installed in parallel with a lower or higher version of CycurRISK on the same PC. If any version of CycurRISK is installed in your PC, uninstall it before installing CycurRISK V2.31.10.

2.2.2 Compatibility to Earlier Releases

TARA versions created in CycurRISK V1.x or V2.x.x can be opened and edited with CycurRISK V2.31.10. However, the TARA versions saved in CycurRISK V2.31.10 cannot be opened in CycurRISK's previous versions.

3 Installation

3.1 System Requirements

This section describes the required hardware and software components to install and run CycurRISK. Along with these prerequisites, it is necessary to have a valid license(s) as described in the section Licensing.

3.1.1 General

The following system requirements are necessary to install and run CycurRISK.

- Operating System (OS): Windows 11 (64-bit) (Recommended)
- Use the OS and Keyboard in English (US).

3.2 Installing

3.2.1 Preparation

Check the Delivery Package to ensure that it contains all the deliverables. Make sure that your system corresponds to the system requirements. Depending on the OS and network connection, you must ensure you have the necessary user privileges.

3.2.2 Delivery Package

You can download the CycurRISK package from the Internet using the given ETAS Download Center link https://www.etas.com/en/products/download_center.php, which includes:

- CycurRISK installer
- This user guide
- Server
- Server manual
- Methodology.mdd
- DocumentationLinks.json
- Report templates (LaTeX and HTML)

3.2.3 User Privileges

You must have administrator rights to perform the following operations:

- Installation of CycurRISK
- Uninstallation of CycurRISK

> **Note**
>
> If administrator rights are not available, contact your system administrator.

3.2.4 Installing CycurRISK

To install CycurRISK from the Internet

1. Go to link https://www.etas.com/en/products/download_center.php.
2. Download and save **.zip** file.
3. Unzip the downloaded file and run the **.exe** file.
   The "Welcome to CycurRISK 2.31.10 Setup" dialog box is displayed.

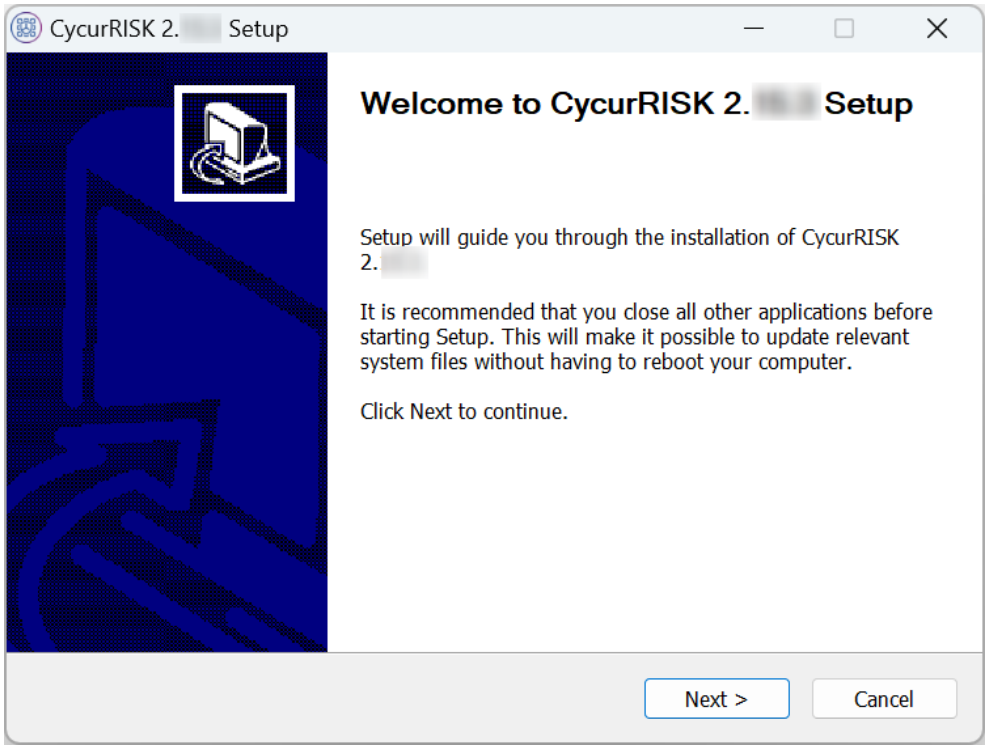


Fig. 3-1: Welcome window

4. Click **Next >** to continue.
   The "ETAS Safety Advice" dialog box is displayed.

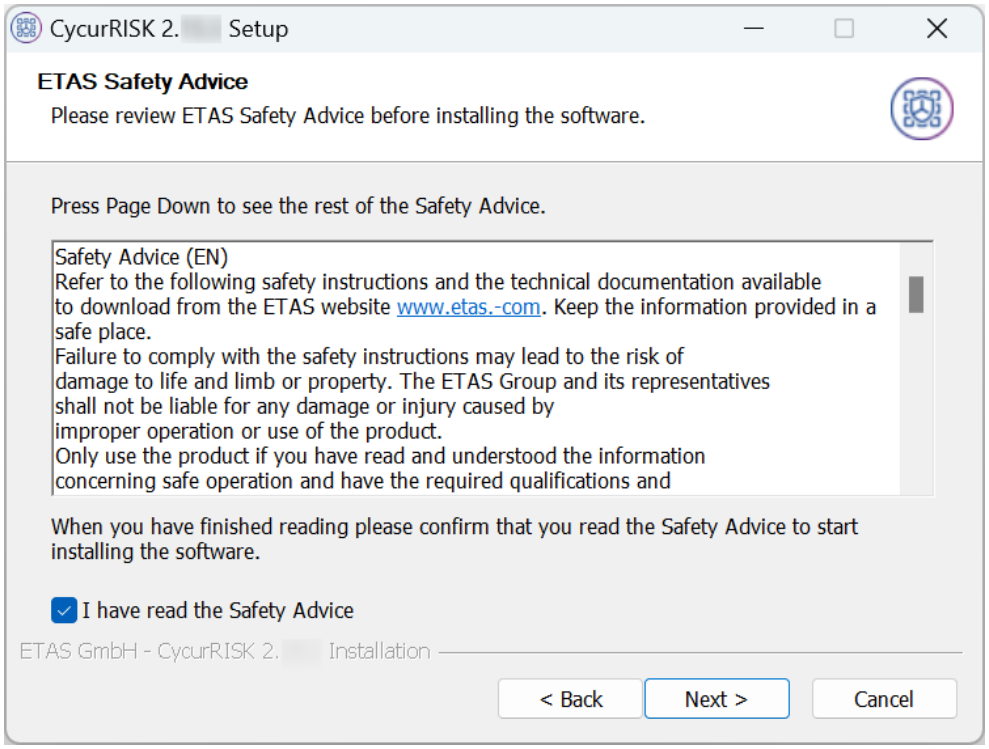


Fig. 3-2: The ETAS Safety Advice dialog box

5. Review and confirm the safety advice before installing the software. Click **Next ›** to continue.
   The "Choose Install Location" dialog box is displayed.

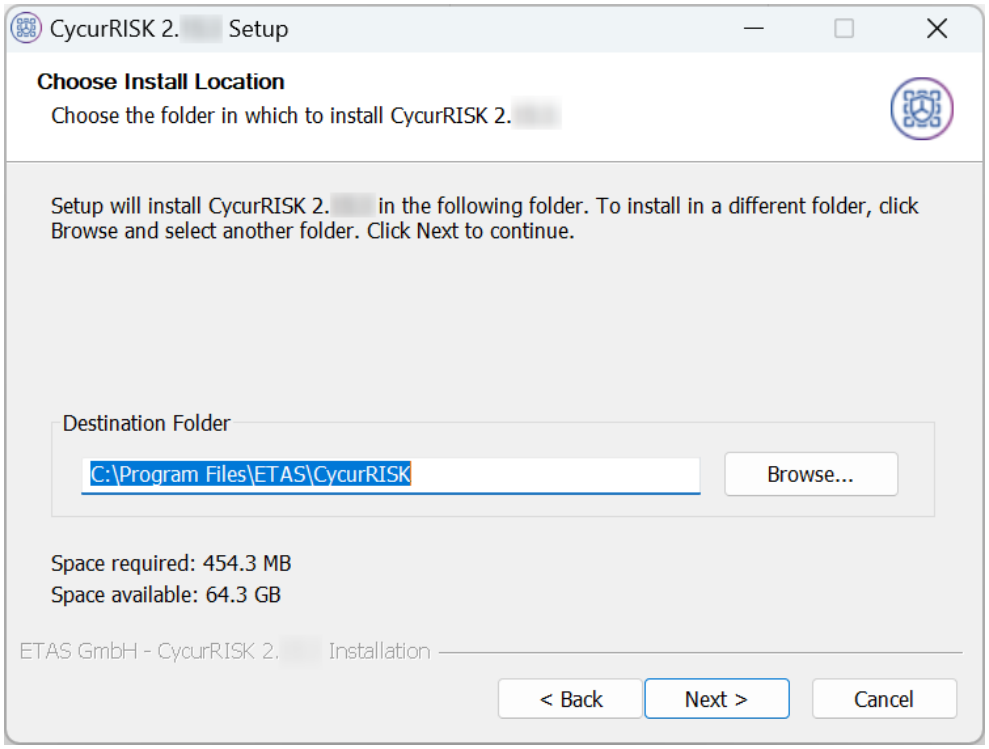


Fig. 3-3: The Choose Install Location dialog box

6. By default, C:\Program Files\ETAS\CycurRISK folder will be created for installation. Specify the installation path or click **Browse...** to select the different folder to install CycurRISK.
7. Click **Next >** to proceed with further installation steps.
   The "Choose Start Menu Folder" dialog box is displayed to create the CycurRISK V2.31.10 shortcuts.

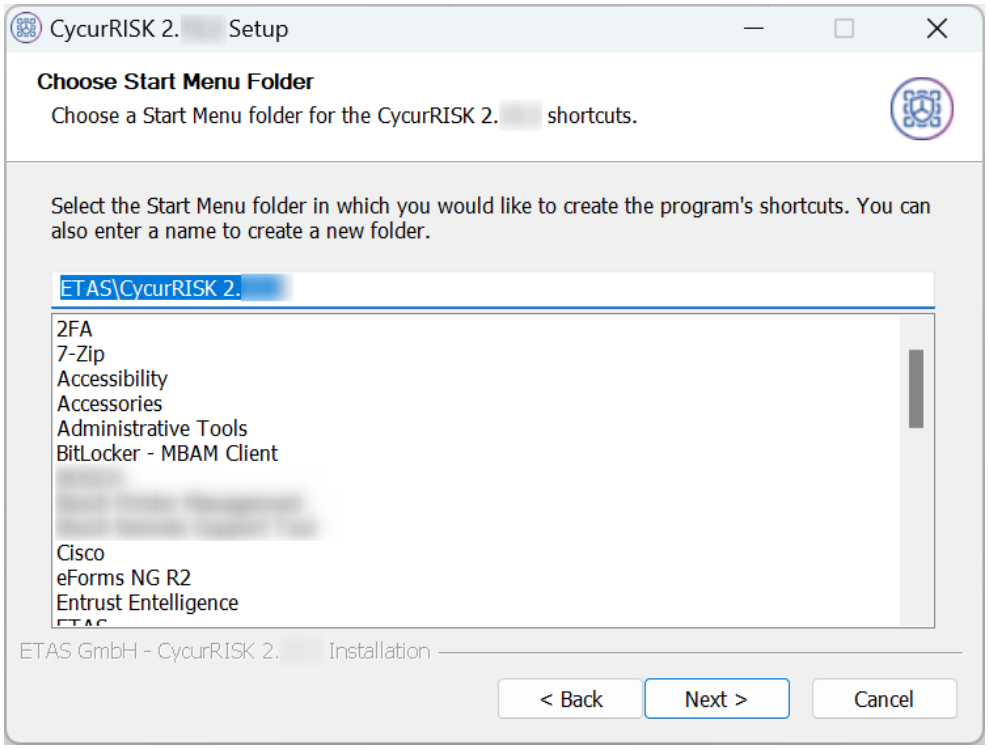


Fig. 3-4: The Choose Start Menu Folder dialog box

8. Click **Next >** to continue.
   The installation process is initiated. The "Installation Complete" dialog box is displayed after the completion of the installation process.

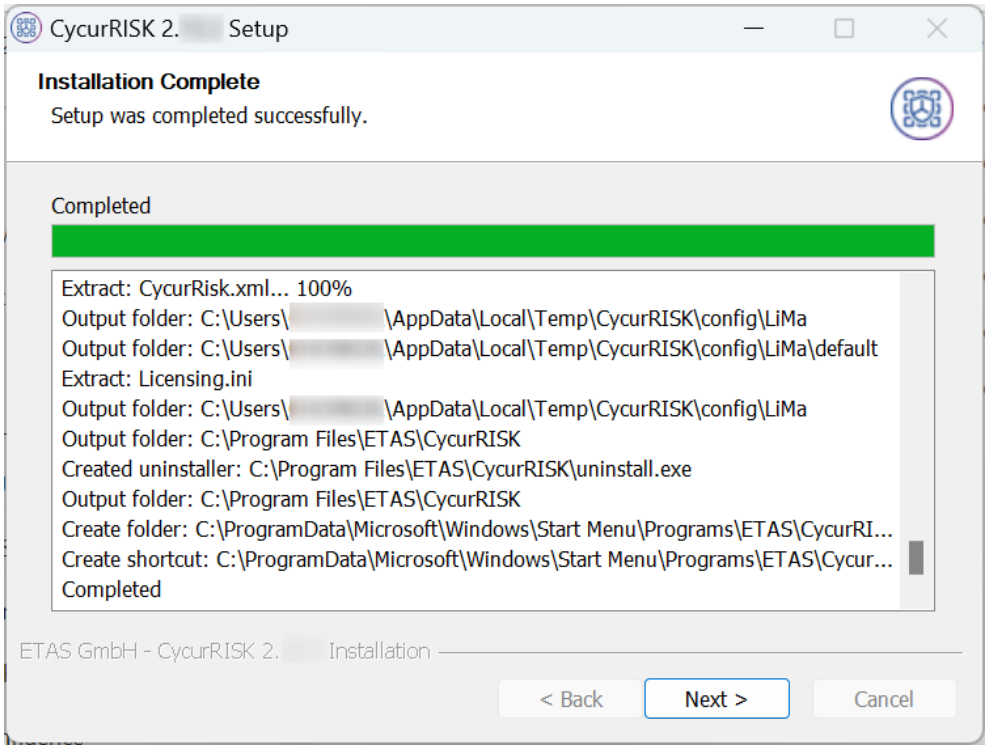


Fig. 3-5: The Installation Complete dialog box

> **Note**
>
> A progress indicator shows the progress of installation.

9. Click **Next >** to continue.
   The "Check Latex Installation" dialog box is displayed.

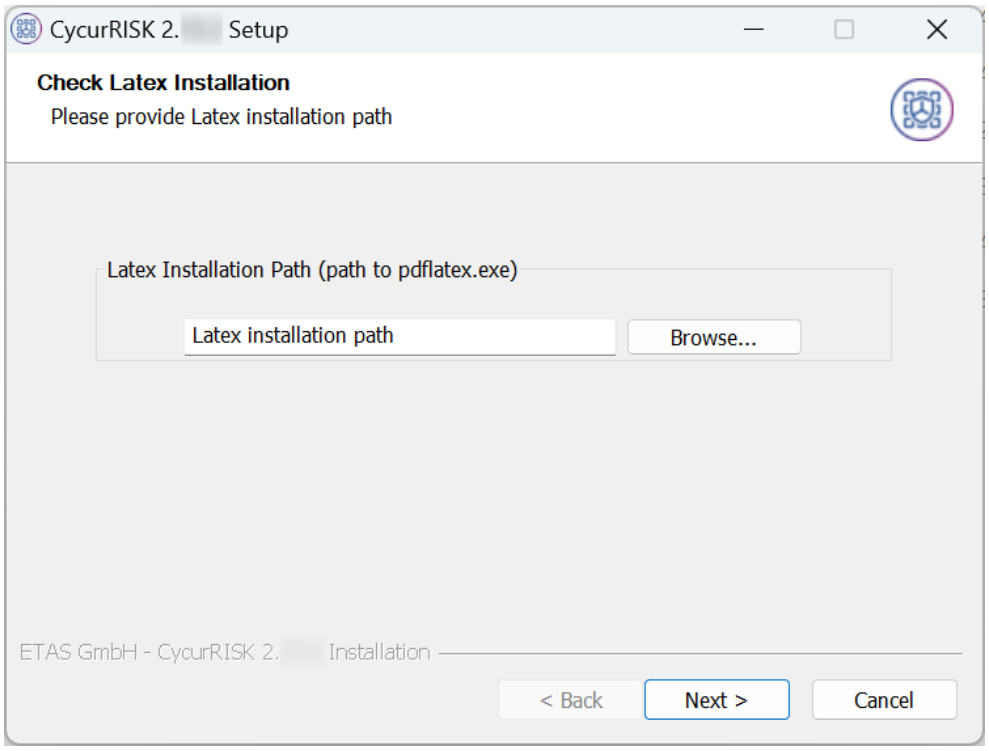


Fig. 3-6: The Check Latex Installation dialog box

> **Note**
>
> The CycurRISK delivery package does not contain the latex installer. You must install it from another source.

10. Specify the latex installation path or click **Browse...** to select the latex installation path.
11. Click **Next >** to continue.
    The "Completing CycurRISK 2.31.10 Setup" dialog box is displayed.

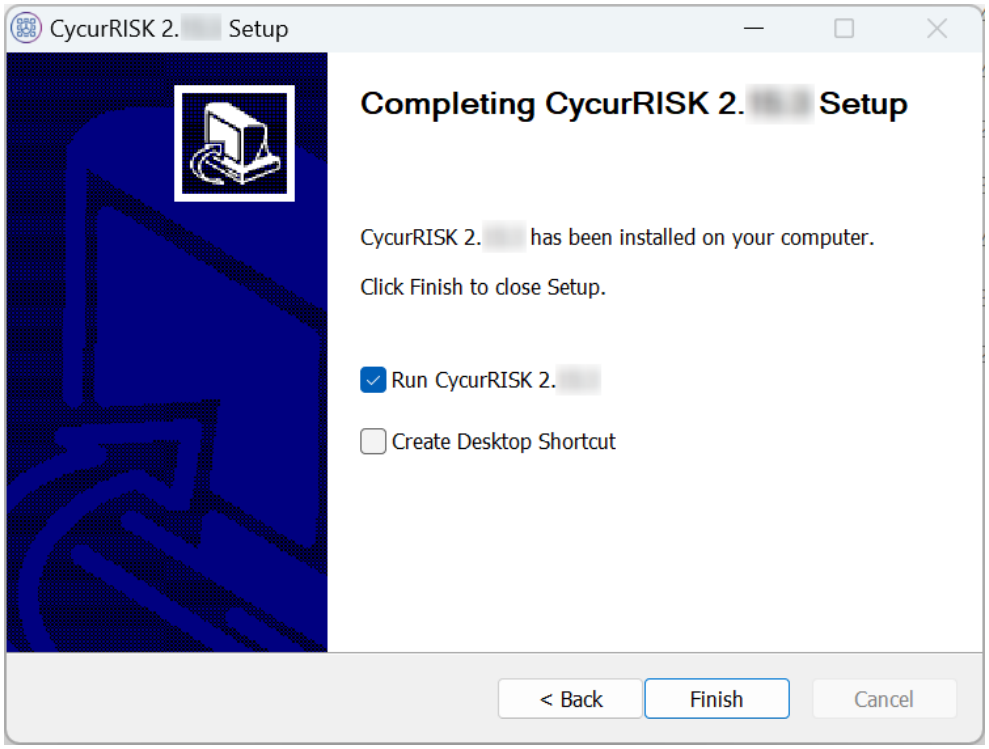


Fig. 3-7: The Completing CycurRISK 2.31.10 Setup dialog box

12. Click **Finish** to complete the installation.

⇨ CycurRISK is installed in the selected location. This will automatically delete the previous versions of the software and old user configuration folders.

3.3 Licensing

A valid license is required to use the software. You can obtain a license in one of the following ways:

- from your tool coordinator
- via the self-service portal on the ETAS website at www.etas.-com/support/licensing

- via the ETAS License Manager

To activate the license, you must enter the Activation ID that you received from ETAS during the ordering process.

For more information about ETAS license management, see the ETAS License Management FAQ or the ETAS License Manager help.

To open the ETAS License Manager help

The ETAS License Manager is available on your computer after the installation of any ETAS software.

1. From the Windows Start menu, select **E** > **ETAS** > **ETAS License Manager**.

   The ETAS License Manager opens.
2. Click in the ETAS License Manager window and press F1.

   The ETAS License Manager help opens.

3.4 Uninstalling

To uninstall CycurRISK

1. Close CycurRISK.
2. Go to the **Control Panel** on Windows **Start** menu.
3. Click **Programs**.
4. Click **Uninstall a program** in **Programs and Features**.
   The Uninstall or change a program window opens.
5. Select CycurRISK V2.31.10 and right-click.
   The context menu opens.
6. Click **Uninstall**.
   The "Uninstall CycurRISK 2.31.10" dialog box is displayed.

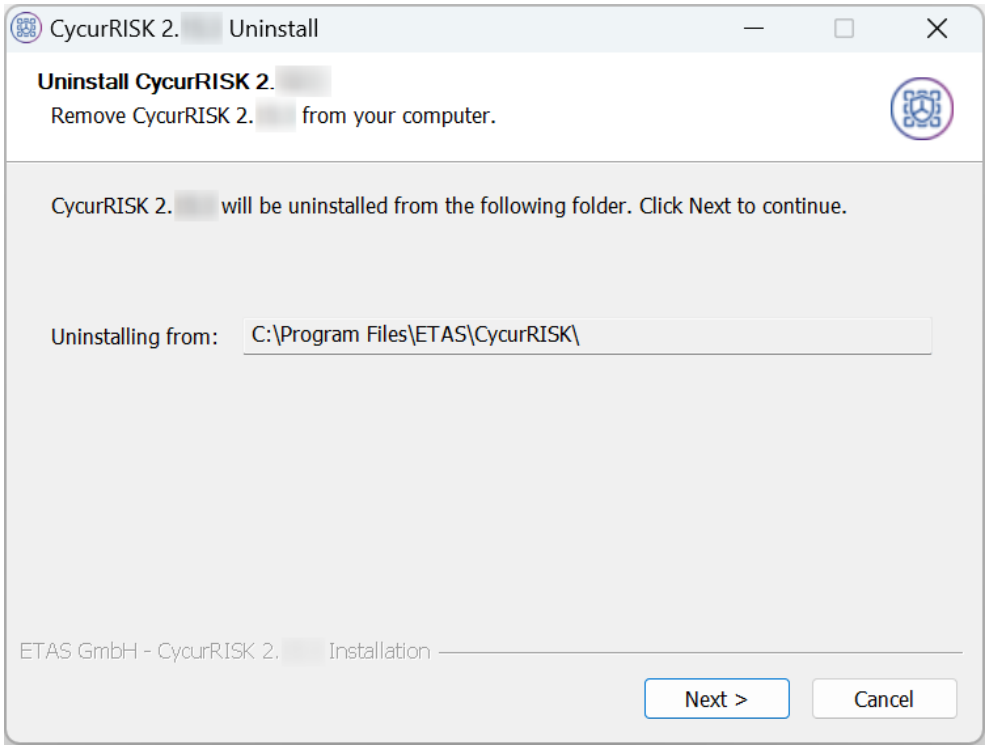


Fig. 3-8: The Uninstall CycurRISK 2.31.10 dialog box

7. Click **Next >** to proceed with the uninstallation process.
   Uninstallation process is initiated.

> **Note**
>
> A progress indicator shows the progress of uninstallation.

8. Click **Close** to complete the uninstallation process.

⇨ CycurRISK is uninstalled from your PC.

4 User Interface

4.1 Home

When you launch CycurRISK first time, the **Home** UI is displayed as shown in screen below.

The **Home** screen allows you to perform the following operations:

- Create a new project
  Refer to Creating a New Project for how to create a new project into CycurRISK.
- Open a local file
  Refer to Opening a Local File for how to open an existing project into CycurRISK.
- Import a project from different formats
  Refer to Importing a Project from Different Formats for how to import a project from different formats such as CSV, Excel, and Tra.

You can view the current and archived projects of the selected organizational unit from the **Projects** menu and the user rights for each project from the **Project rights** menu. See Projects for more information and Managing the Project Rights for how to manage the project rights.

You can manage the Methodologies, Methodology version mappings, Report templates, and Hierarchy definitions from the **OU resources** menu. See OU resources for more information. Also, you can manage and configure the server from the **Server management** menu. See Server management for more information.

The Home screen displays all recently worked projects sorted by the last saved time stamp.

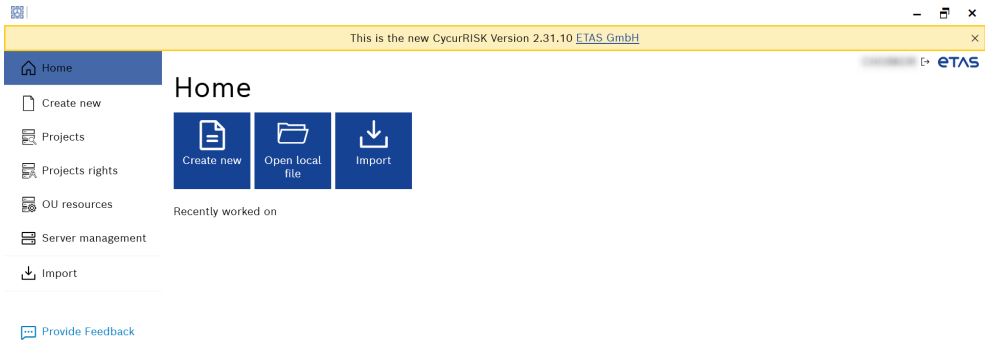


Fig. 4-1: Home

4.2 Projects

The **Projects** dashboard displays the Current and Archived projects and their versions. It helps to open and export projects. You can move projects to Archived or Current projects. You can compare it as a project and as a reference project. See Comparing a Project for more information on comparing the two different versions of the project.

You can select a organizational unit from the "Organizational unit" drop-down menu. You can lock or unlock a project to restrict other users for editing the project. See Adding or Removing a Project Lock for more information.

A filter can be applied to the elements listed under Current and Archived projects. You can publish the released libraries and unpublish the published libraries.

You can click **Copy a link to the newest or this project version into the clipboard** icon to copy the corresponding project version link to the clipboard. You can use the copied link when working with the API Client. For more information, refer to Working with the API-Client.

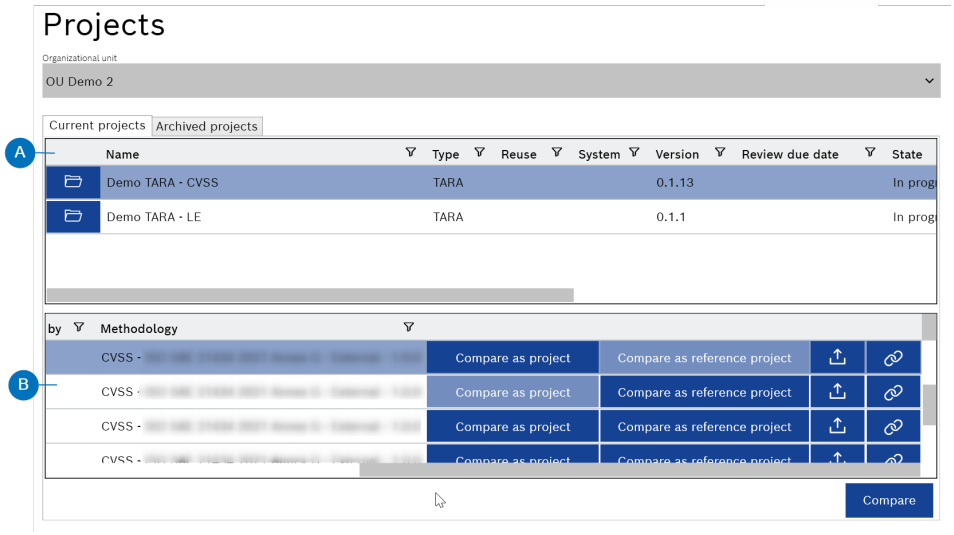


Fig. 4-2: Projects

A. Current projects list
B. Current project versions list

4.3 OU resources

The “OU resources” tab is visible only if you have the Product Security Officer role. With this role, you can manage the resources for the specific OU. See the Server management for more information about managing user rights.

You can select the OU and configure it with the following features:

- Methodologies
  You can upload or download the default methodology configuration files. Further, you can select this uploaded methodology when you create the new TARA project or library. A default file is provided with the delivery package (in ***.mdd** format). See Delivery Package for more information. You will also see the available versions of the selected methodology in the “Methodologies” tab.
- Methodology version mappings
  You can upload, download, or remove a mapping file (in ***.mmd** format) to transfer projects between configurations, where different attribute values need to be mapped.
- Report templates
  You can upload, download, or remove the LaTeX and HTML templates (in ***.zip** format). These report templates are part of the delivery package. You can customize and upload these templates for PDF report generation. See Generating a PDF for more information.
- Hierarchy definitions
  You can upload, download, or remove the configuration files (in ***.json** format) for the hierarchy for system TARAs (e.g., System > Features > Component).

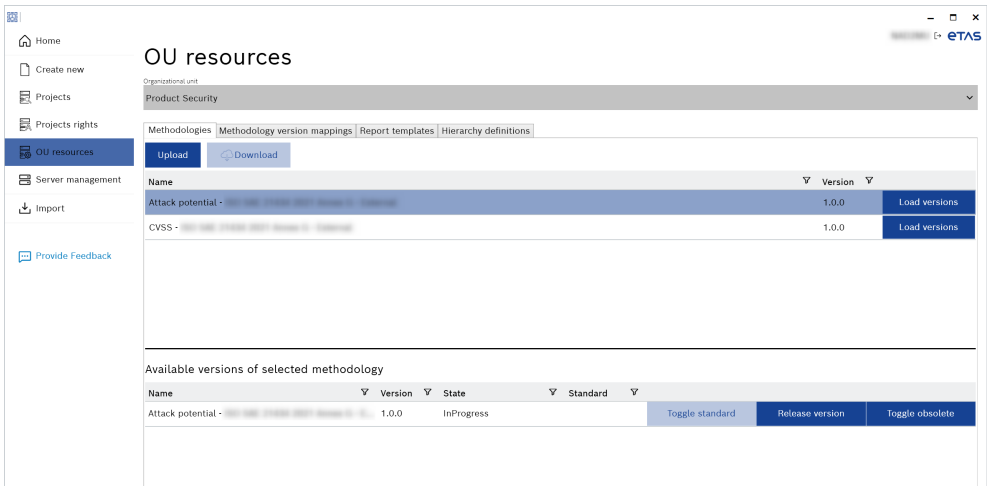


Fig. 4-3: OU resources

4.4 Server management

You will require administrator rights to access and configure the server. Refer to the server manual for more information about administrative rights. The Server manual is provided with the delivery package.

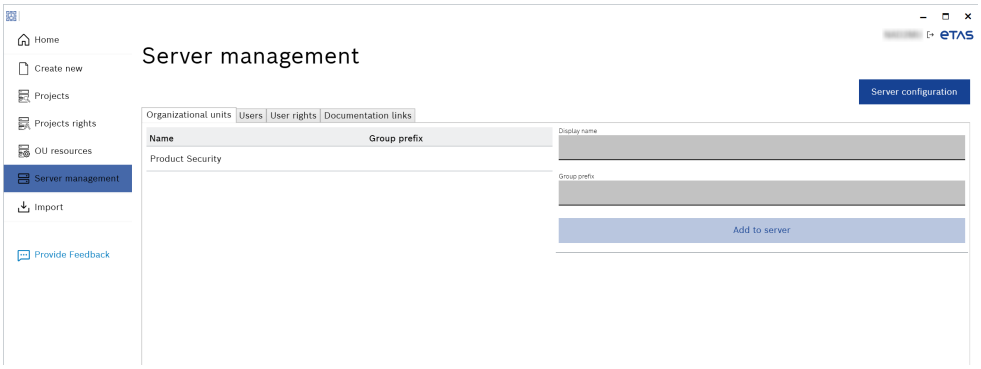


Fig. 4-4: Server management

It has the following features that you can manage:

A. Organizational units
   You can create and add a new organization unit to the server. Also, you can enter the group prefix. You allow to revise the name and group prefix of an existing OUs.
   - Group prefix
     The prefix of the Active Directory. All users of the active directory group get access to the organizational unit and are assigned the corresponding access rights.
     The corresponding suffix is defined in the “Server Configuration”. The users of the group prefix plus suffix are assigned the corresponding access rights. See the Server configuration below for more information.

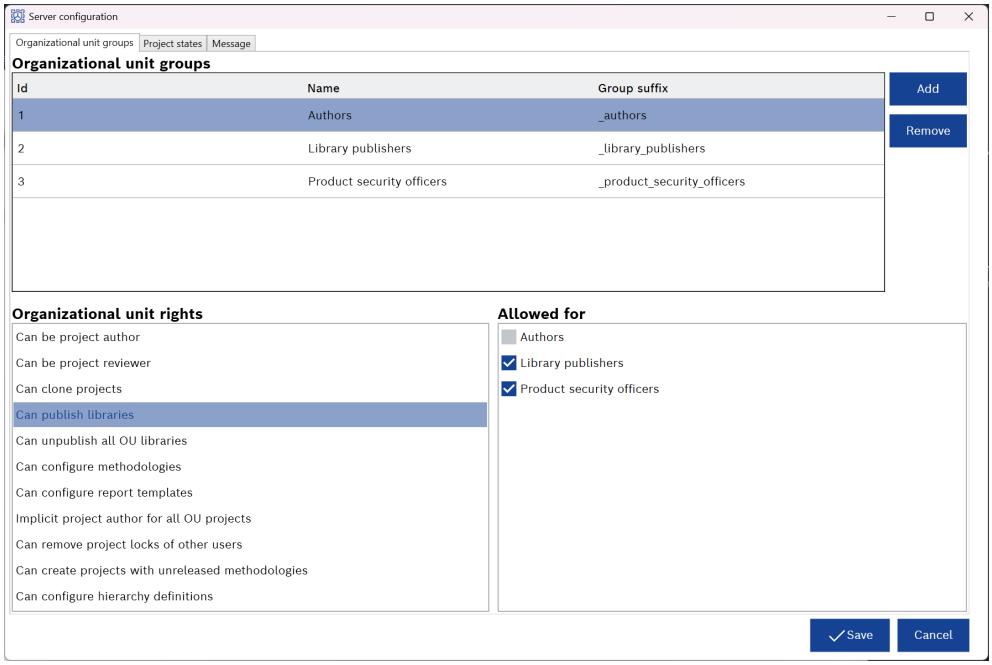
B. Users
   It displays the list of all users on the server and their assigned rights. Also, you can manually add a user to the server using the Active Directory or EntraID username.

C. User rights
   It displays all existing OUs and their respective users with all assigned access rights. You can assign or remove the access rights for each OU.

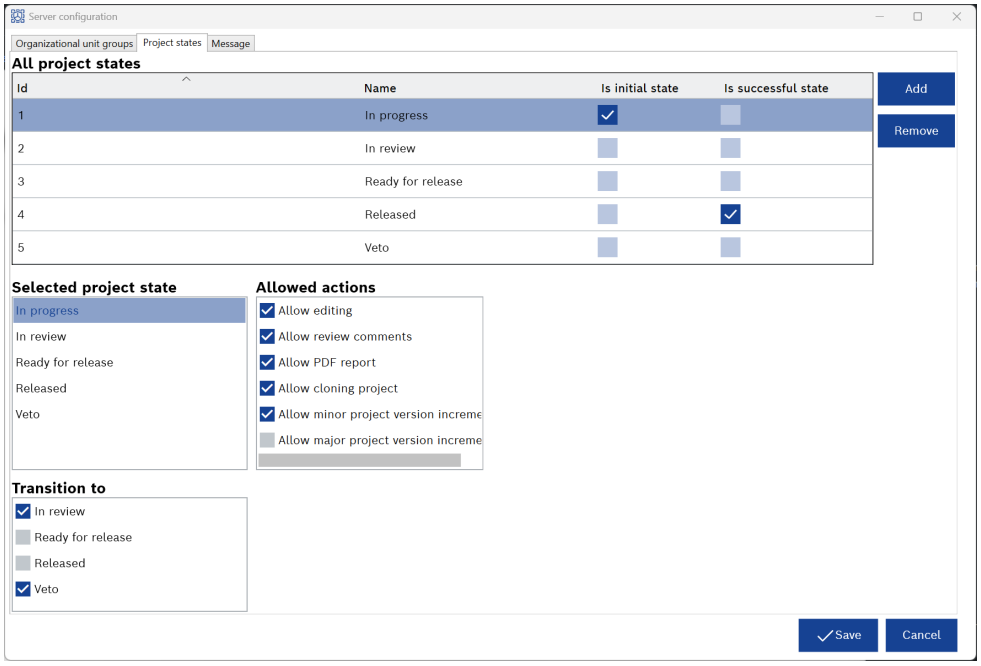
D. Documentation links
   You can upload or download the documentation links in ***.json** format. The **DocumentationLinks.json** file is provided with the delivery package. See Delivery Package for more information.

E. Server configuration
   It has the following features that you can manage:

– Organizational unit groups
  It displays the organizational unit groups and organizational unit rights. You can add, change, or remove the access rights groups. You can set up the name and active directory suffix of the group. You can assign the OU rights to the group.



– Project states
  It displays all and selected project states. You can add, change, or remove the project states. You can set the allowed actions for each project state and transition between states.



– Message
  You can set up a message to display as a banner to the user.

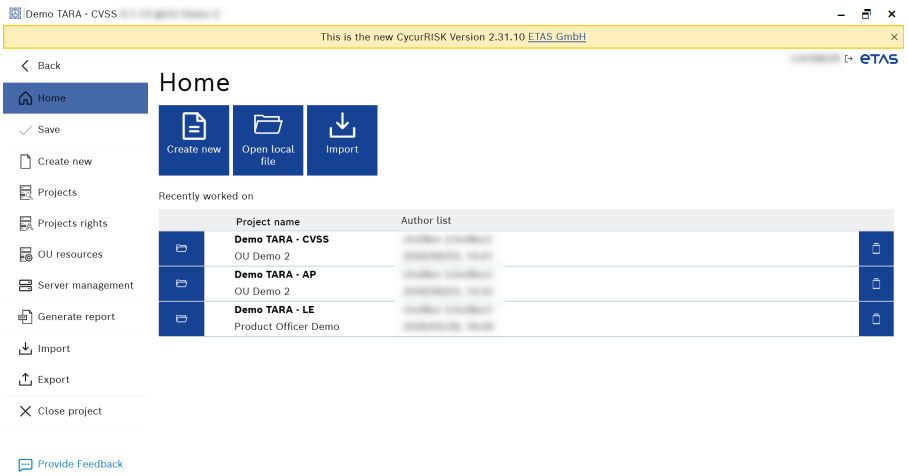
To configure the message

1. Perform one of the following steps:
   - Click **Server management** in the “Home” screen.
   - Go to the **File** menu > **Server management**.
     The “Server management” window appears.

2. Click the **Server configuration** button.
   The “Server configuration" window appears.

Fig. 4-5: Server configuration

3. Go to the “Message” tab.
   By default, the “Enabled” toggle button is disabled.
4. Enable the “Enabled” toggle button to display the message.
5. Enter the message text in the “Message text” field.
6. Enter an additional link to a website in the “Message link” field.
7. Enter a text to display instead of a website URL in the “Message link text” field.
8. Select the message banner color from the “Message color” drop-down list.
9. Decide whether you want to allow the user to close the message banner with the “Can be closed” toggle button.
   This step is optional.
10. Click **Save**.
    The message will take time to appear in the application just below the title bar.



4.5 Cockpit

As soon as you create or open a project, the **Cockpit** window is displayed.

The Cockpit is an environment that contains the project metadata. After creating a project, you can change its name and status.

You can document the necessary information in the "Comment" field. You can enter the project review due date, assign the project roles and rights, and see the project history in the Cockpit window. It has the following four project rights:

- None
- Project author
- Project reviewer
- Project reader

The menu bar is also available and contains all functions for file-specific actions.

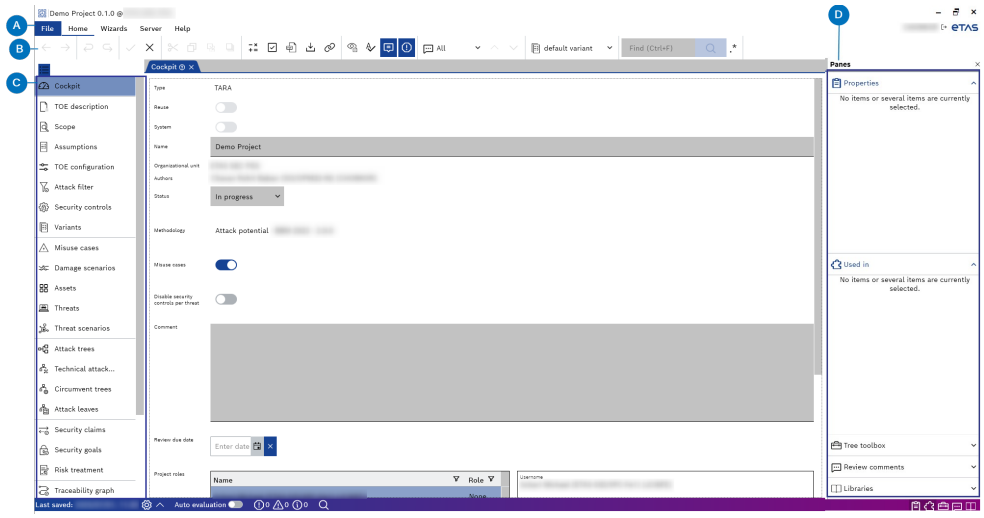


Fig. 4-6: Cockpit

A. Menus
B. Commands
C. TARA artifacts
D. Panes

The cockpit window has the following five statuses for projects:

- In progress
- In review
- Ready for release
- Released
- Veto

You can change the project status only if certain conditions are satisfied. Possible conditions are:

- No existing validation warnings and/or errors
- No open review comments

An overview of allowed status transitions and attached functionality is given in the figure below.

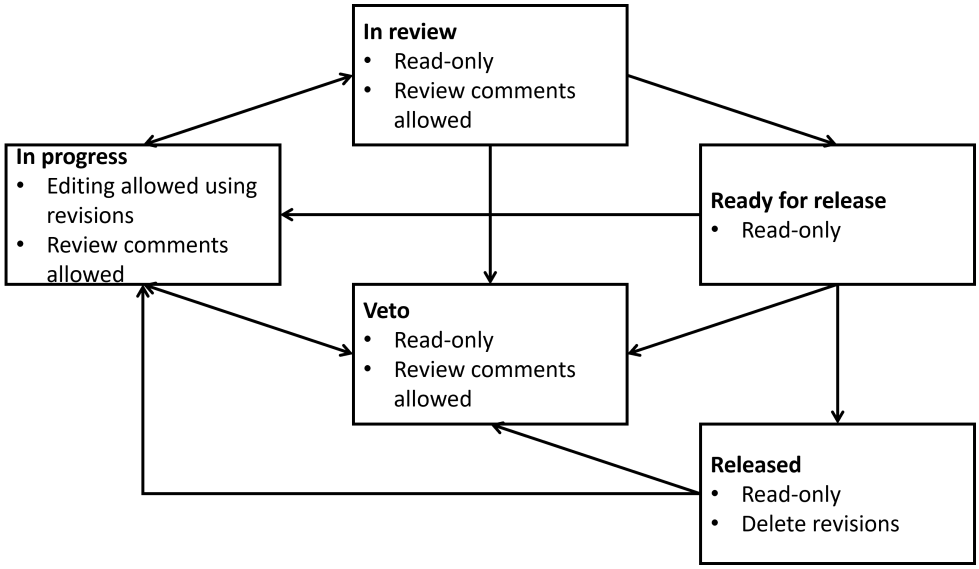


Fig. 4-7: Status model of CycurRISK

4.6 TOE Description

CycurRISK contains a dedicated page for the Target of Evaluation (TOE) description, which is a text field.

The TOE is the system or product analyzed by the TARA. A TARA always starts with a TOE description, which is a detailed technical description of the TOE including information as follows:

- Function
  - Intended behavior
  - Vehicle functionality realized by the TOE, etc.
- Architecture
  - Internal components
  - Data flow
  - Interfaces
  - Physical, and logical aspects, etc.
- Relevant constraints and compliance needs
  - Functional constraints
  - Technical constraints
  - Security standards, and norms etc.

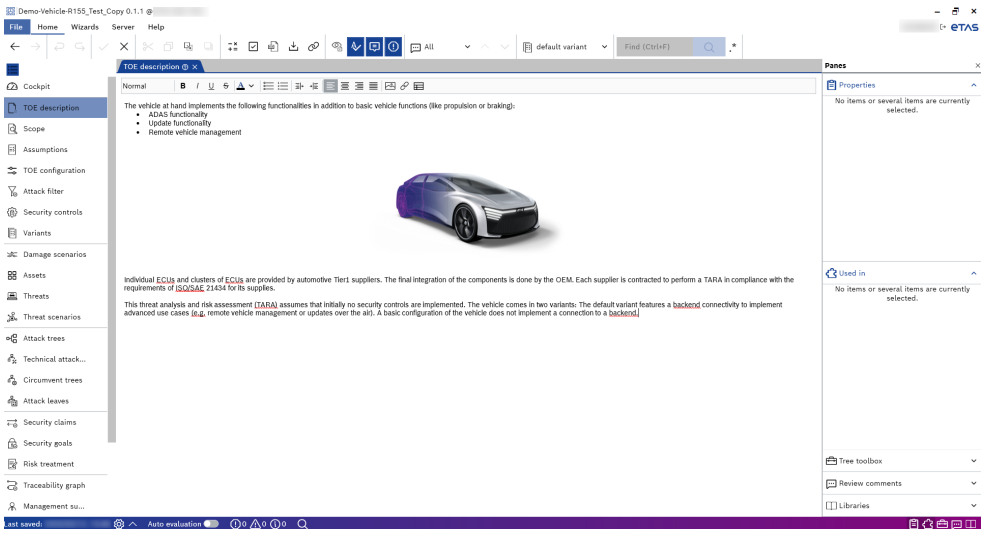


Fig. 4-8: TOE description

> **Note**
>
> CycurRISK provides basic formatting, tables, graphics, and links for the TOE description.

4.7 Scope

CycurRISK contains a separate page for the Scope, which works just exactly the same as the TOE description.

The Scope defines two things are as follows:

A. The boundary of the TOE itself for the purpose of the TARA. So it distinguishes the TOE from its operational environment. This should mostly follow from the TOE description, but you can use the scope to highlight some important points.

B. The boundaries of the analysis itself, e.g., which types of attacks and attackers are considered.

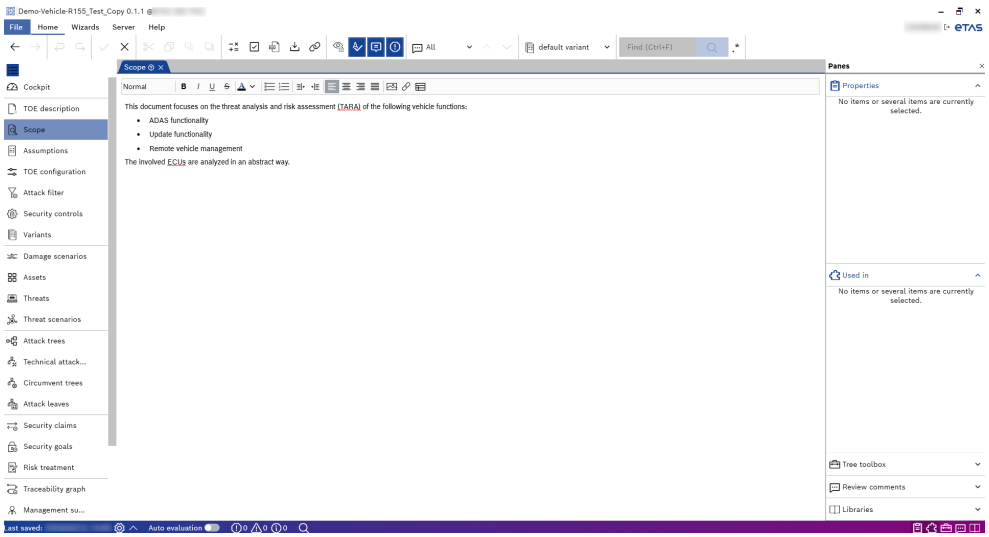


Fig. 4-9: Scope

> **Note**
>
> CycurRISK provides basic formatting, tables, graphics, and links for the scope.

4.8 Assumptions

You can create assumptions via CTRL+N, INSERT key, "Home" menu, or context menu.

The assumptions feature allows you to set the assumptions to "Enabled" or "Disabled" status, evaluate different scenarios from the project, and compute the corresponding risks.

The assumptions can only be linked to the attack trees nodes and they can not be linked to other artifacts. Changing the enabled status of an assumption has effects on the status of all linked artifacts (E.g., Attack tree nodes, Technical attack trees, Circumvent trees, Attack leaves, and Security claims). The disabled artifacts are excluded from the computations, which may influence the resulting AFR and risk values.

You can see, compare, and evaluate the influence of assumptions status on the risks in the "Management summary."

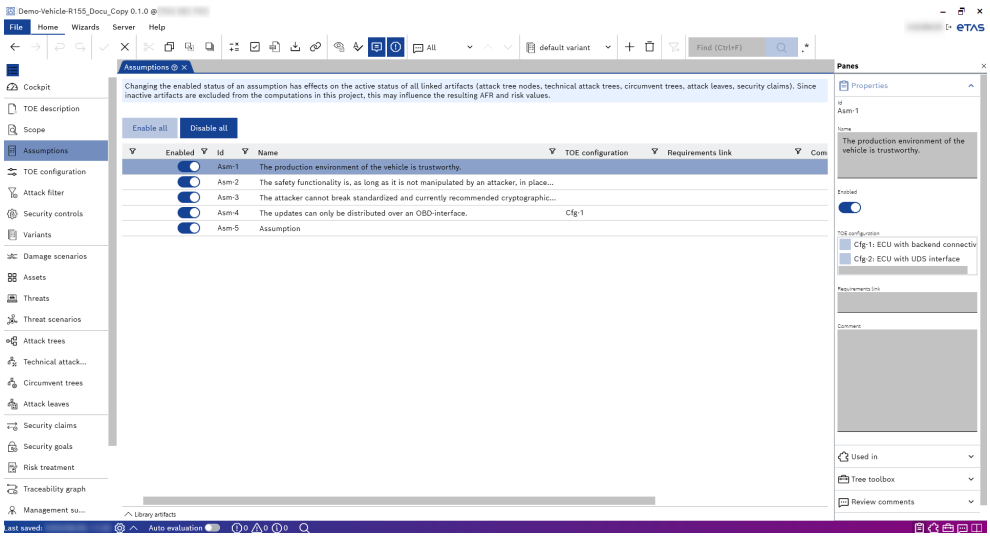


Fig. 4-10: Assumptions

4.9 TOE Configuration

The TOE configuration models different variants of the TOE. Individual configuration items may be enabled or disabled independently of each other, leading to the overall configuration of the TOE. This configuration is the basis for the AFR and risk computations. For this purpose, all relevant artifacts (E.g., Assumptions, Assets, Threats, Tree nodes, Security claims, and Security goals) must be linked with the appropriate TOE configuration items.

CycurRISK contains a dedicated page to add different TOE configurations. You can create TOE configurations via CTRL+N, INSERT key, "Home" menu, or context menu. Defining and using TOE configurations is an essential part of creating a TARA. The TOE configuration items represent things or elements or properties that differ between different TOE variants. All things or elements or properties that are shared or the same between TOE variants should not be listed as TOE configuration items.

When a TOE configuration item is disabled, the linked artifacts are excluded from the analysis and marked via shading. You can completely hide these linked artifacts with the "Hide inactive items (F8)" button in the "Home" menu.

> **Note**
>
> If an artifact is linked to multiple TOE configuration items, it is included in the analysis if all linked configuration items are enabled.

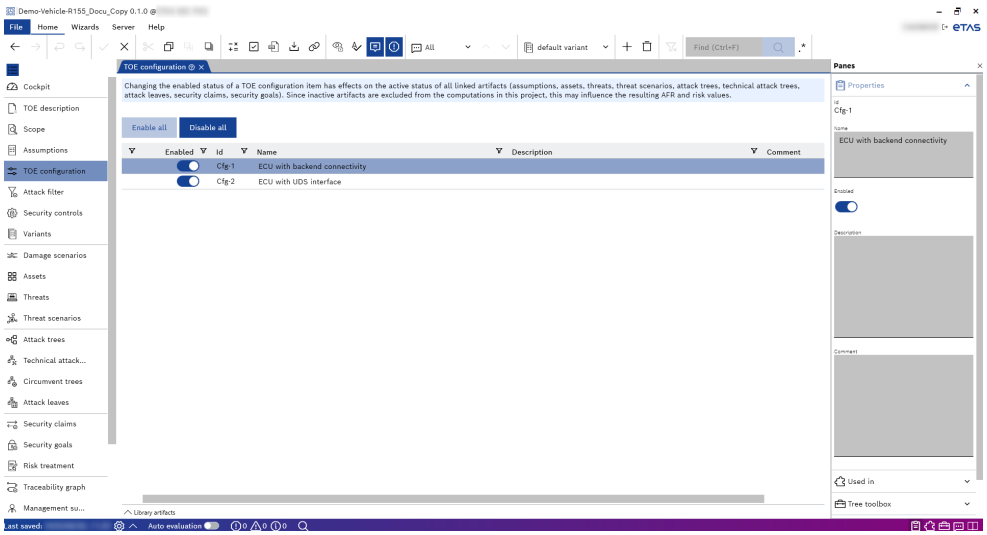


Fig. 4-11: TOE configuration

You can link the TOE configurations defined on this page to other pages. The following table provides an overview of where TOE configurations can be linked manually and where they are inherited from other pages.

Artifact type	Link to TOE configuration
Assumptions	Manual
Security controls	Manual
Assets	Manual
Threats	Inherited from Assets
Threat scenarios	Inherited from Threats/Assets
Attack trees	Inherited from Threats/Assets
Technical attack trees	Manual
Circumvent trees	Inherited from Security controls
Attack leaves	Manual
Security claims	Manual
Security goals	Manual

4.10 Attack Filter

The **Attack filter** feature enables you to filter the attacks considered in your analysis for certain properties. The selected values on the attack filter page are included in the AFR and risk computations and the deselected values are excluded from the analysis.

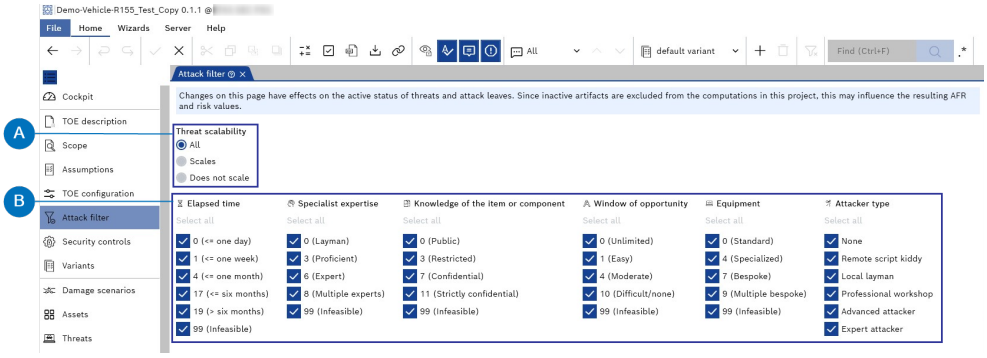


Fig. 4-12: Attack filter

A. Threat scalability filter
B. Attacker capability filter

You can filter for two things on the "Attack filter" page as follows:

A. Threat scalability filter
   You can set the threat scalability filter by choosing the three options below:
   a. All
      By default, it is set to "All," which includes all threats, regardless of whether they scale.
   b. Scales
      Deactivates all threats that do not scale.
   c. Does not scale
      Deactivates all threats that scale.
B. Attacker capability filter
   All available attacker capabilities are listed, including all possible values. All values are selected by default and will be included in the analysis. By deselecting a value, all attack leaves with this value and corresponding nodes connected via an AND node are excluded from the analysis.

4.11 Security Controls

The **Security controls** allows you to enable or disable the security controls for all TARA and RRA projects. Changing the enabled status of a security control has effects on the status of the corresponding circumvent tree. The disabled artifacts are excluded from the computations, which may influence the resulting AFR and risk values.

CycurRISK offers the "Threat-specific security controls" feature, with which you can either enable or disable the security controls per threat at once during the project creation.

To use this feature, the respective circumvent tree has to be embedded in the attack tree. When the control is disabled or enabled, the circumvent tree will be deactivated or activated in the attack tree, and the calculation will change.

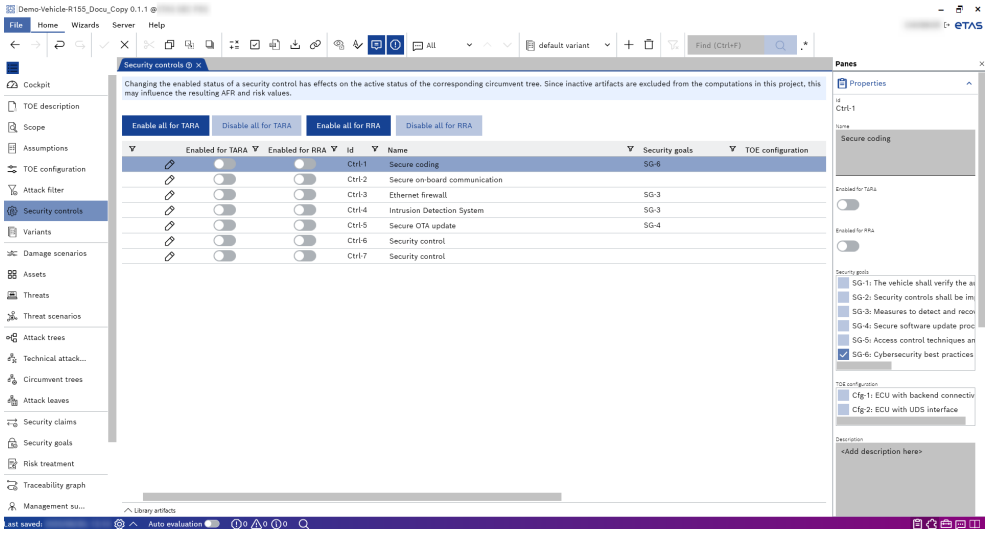


Fig. 4-13: Security controls

4.12 Variants

The Variants page is located below the "Security controls" in the Project Explorer. You can configure the variants on this page as follows:

- Duplicate an existing variant
- Delete a variant
- Add a new variant
- Similar to the functionality in the Management summary, the switches for the Security controls, TOE configuration, and Assumptions can be turned on and off.

If no variant has been added explicitly, the current status of Security controls, TOE configuration, and Assumptions is considered the default variant.

You can select only one configured variant from the "Select the active variant" drop-down field in the Home menu. The active variant is highlighted in blue. The active variant affects all of the project explorer's other pages. The Management summary shows only the active variant, and it is not possible to add other variants.

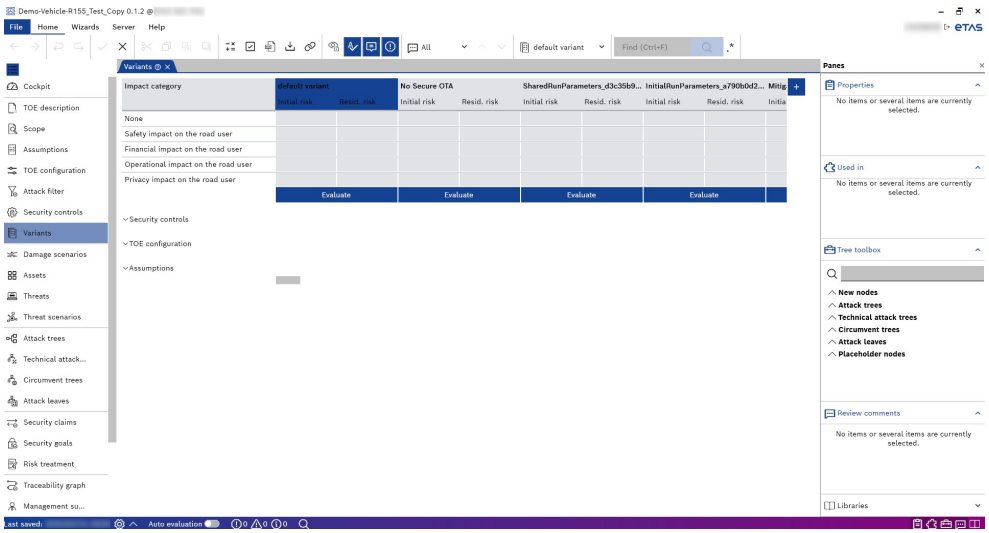


Fig. 4-14: Variants

4.13 Misuse Cases

CycurRISK contains a dedicated page for the Misuse cases.

Misuse cases are a collection of possible attacks, harms, or malfunctions that can lead to damage to the TOE, the road user, or a further stakeholder.

The misuse cases are optional. However, they are used as a brainstorming element and are often produced in a misuse case workshop with various stakeholders. They may be used to generate further content for the TARA, particularly assets and threats.

You can create misuse case via CTRL+N, INSERT key, **Add** icon from the **Home** menu, or context menu and enter the name of the misuse case.

Misuse cases ? ×

Id	Name	Comment
MUC-1	Send manipulated messages over the CAN bus.	
MUC-3	Steal privacy-relevant data.	
MUC-4	Flood the bus to launch a DoS attack.	
MUC-5	Manipulate HMI information.	
MUC-6	Suppress sensor data.	
MUC-7	Copy the firmware.	need to check this again
MUC-9	Steal intellectual property.	

Fig. 4-15: Misuse cases

4.14 Damage Scenarios

A damage scenario is an adverse consequence involving the TOE, a vehicle, or a vehicle function and affecting the road user. There are four impact categories concerning the road user, as given by ISO/SAE 21434:

- Safety
- Financial
- Operational
- Privacy

The impact describes the magnitude of damage or physical harm from a damage scenario. There are four impact ratings defined according to the impact category:

- Severe
- Major
- Moderate
- Negligible

The tables below show the definition of impact ratings:

Impact rating	Criteria for safety impact rating
Severe	S3: Life-threatening injuries (survival uncertain), fatal injuries
Major	S2: Severe and l life-threatening injuries (survival probable)
Moderate	S1: Light and moderate injuries
Negligible	S0: No injuries

Tab. 4-1: Example: Safety impact rating criteria

Impact rating	Criteria for financial impact rating
Severe	Catastrophic consequences which the affected road user might not overcome
Major	Substantial consequences which the affected road user will be able to overcome
Moderate	Inconvenient consequences which the affected road user will be able to overcome with limited resources
Negligible	No effect, negligible consequences or is irrelevant to the road user

Tab. 4-2: Example: Financial impact rating criteria

Impact rating	Criteria for operational impact rating
Severe	Loss or impairment of a core vehicle function. Example 1: Vehicle not working or showing unexpected behaviour of core functions such as enabling of limp home mode or autonomous driving to an unintended location.
Major	Loss or impairment of an important vehicle function. Example 2: Significant annoyance of the driver.
Moderate	Partial degradation of a vehicle function. Example 3: User satisfaction negatively affected.
Negligible	No impairment or non-perceivable impairment of a vehicle function.

Tab. 4-3: Example: Operational impact rating criteria

Impact rating	Criteria for privacy impact rating
Severe	Significant or even irreversible impact to the road user. The information regarding the road user is highly sensitive and easy to link to a PII principal.
Major	Serious impact to the road user. The information regarding the road user is: A. highly sensitive and difficult to link to a PII principal; or B. sensitive and easy to link to a PII principal.
Moderate	Inconvenient consequences to the road user. The information regarding the road user is: A. sensitive but difficult to link to a PII principal; or B. not sensitive but easy to link to a PII principal.
Negligible	No effect or, negligible consequences or is irrelevant to the road user. The information regarding the road user is not sensitive and difficult to link to a PII principal.

Tab. 4-4: Example: Privacy impact rating criteria

You must fill in the reasoning field. If you leave this field empty and do your project validation, it will eventually give you an error because you have not filled in your reasoning.

Each damage scenario must be assigned precisely with one impact category and impact. If a damage scenario has several relevant impact categories, you

should specify damage scenarios further to make them specific enough so that only one impact category applies. If you can not do that, you must assign the impact category that leads to the worst impact.

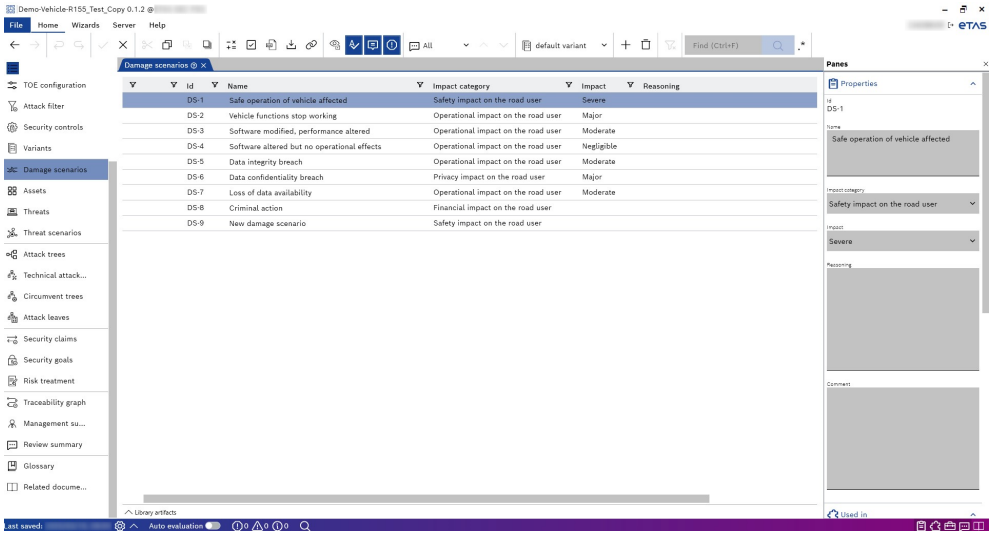


Fig. 4-16: Damage scenarios

4.15 Assets

CycurRISK provides a dedicated page for the Assets. The assets are any data, function, or resource of the TOE that must be protected to reduce the probability of a successful attack. You can add an asset to the list of assets and give a detailed description stating what it is. Then, you must specify which aspects of each asset must be protected. These are called as Security Properties.

A security property is an attribute of an asset that is worth protecting. ISO/SAE 21434 recommends using the following security properties:

- Confidentiality
- Integrity
- Availability

These properties are defined and used as follows:

Security Properties	**Definition**	**Threat Name**
Confidentiality	Information can not be accessed by unauthorized parties	Extraction of
Integrity	Information has not been altered and the source of the information is genuine	Manipulation of
Availability	Information is accessible by authorized users	Blocking

Tab. 4-5: Definition of security properties

> **Note**
>
> Adding and adapting security properties in a customized methodology is possible as needed.

Each asset may have one or several security properties. Each pair, which consists of an asset and a linked security property, is called a "Security Objective. " For example, an asset of ECU firmware is added and assigned the security property "Confidentiality", "Integrity", and "Availability" (CIA).

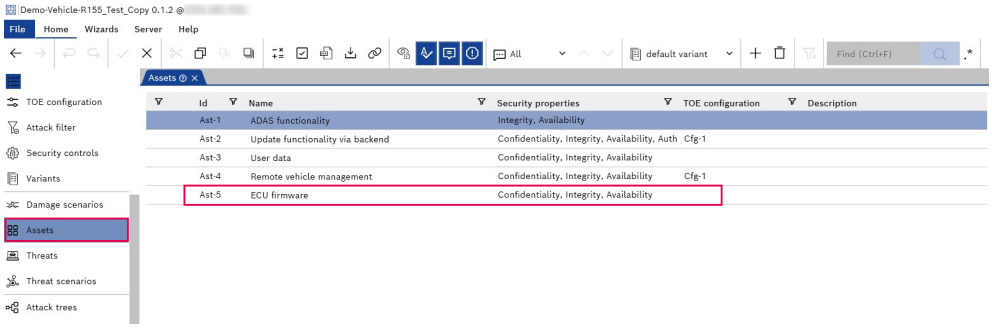


Fig. 4-17: Assets

4.16 Threats and Threat Scenarios

A threat is an action that violates a security objective, that leads to the non fulfillment of a security property regarding an asset. There must be one threat per security objective and no more.

The threats are automatically generated from the assets with their security properties. If you want a threat, you must go to your assets page, add an asset, and assign at least one security property, and that will automatically generate a threat for you on this page. For example, an asset of "ECU firmware" is added and assigned the security property "Confidentiality", "Integrity", and "Availability", which leads to the threat of "Extraction of ECU firmware", "Manipulation of ECU firmware", and "Blocking ECU firmware."

> **Note**
>
> You can not add threats manually. CycurRISK automatically generates threats from the security objective according to the naming scheme in Tab. 4-5.

You must link the threat to the relevant damage scenarios, i.e., all kinds of damages that can result from this threat. If you are using misuse cases, you can link the misuse cases related to this threat.

Once you build attack trees for your threats, CycurRISK shows you the AFR for the listed threats.

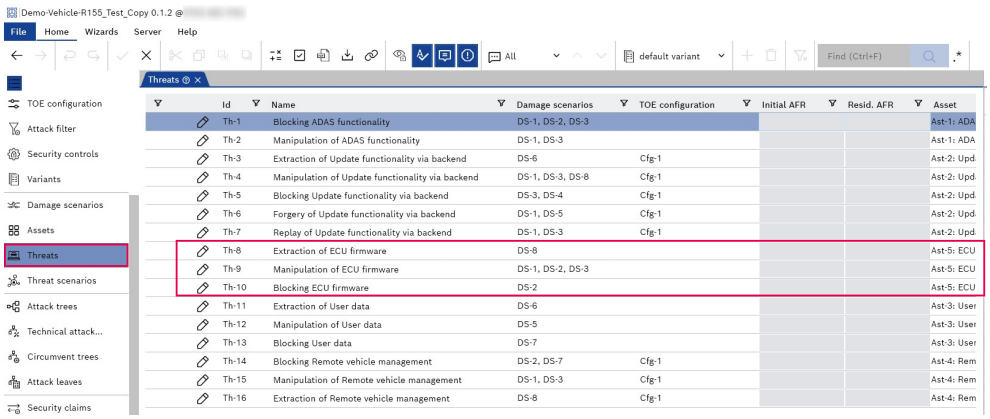


Fig. 4-18: Threats

Each pair of one threat and one linked damage scenario generates one threat scenario. If more than one damage scenario is linked to a threat, then there will be more or several damage scenarios per threat. So, typically, there are more threat scenarios than threats.

For example, the "Manipulation of ECU firmware" linked to three damage scenarios, i.e., DS-1, DS-2, and DS-3, means CycurRISK automatically generates three threat scenarios for this threat.

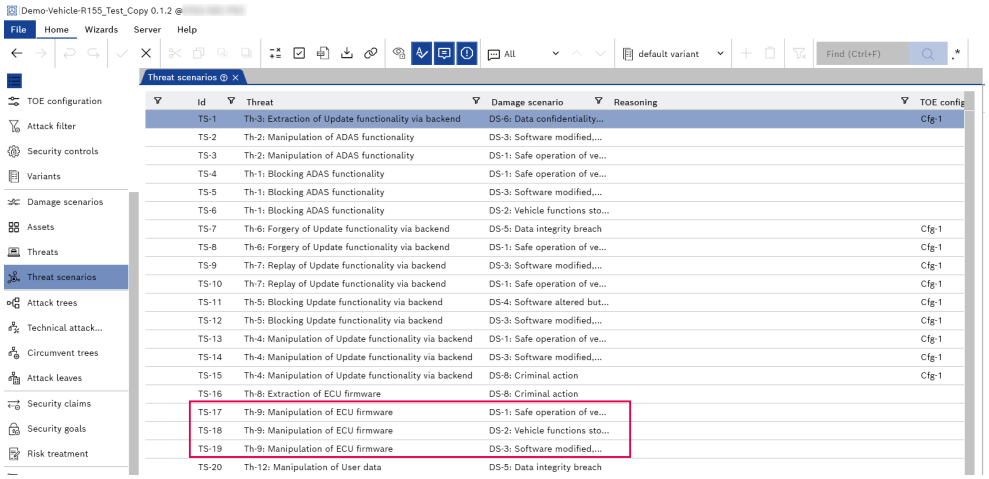


Fig. 4-19: Threat scenarios

> **Note**
>
> The "Threat Scenarios" are automatically generated from the information entered on the "Threats" page and can not be added manually.

4.17 CVSS score

This page displays the rating for each threat based on the CVSS scores. It is an alternative to attack potential rating and attack tree modeling.

The CVSS score refers to the Common Vulnerability Scoring System value assigned to a vulnerability. The CVSS score is a numeric value from 0 to 10, as defined in ISO/SAE 21434, where higher values indicate more critical vulnerabilities.

Severity Rating	CVSS Score
None	0.0
Low	0.1 – 3.9
Medium	4.0 – 6.9
High	7.0 – 8.9
Critical	9.0 – 10.0

You can configure the parameters below for each threat to measure the severity of software vulnerabilities:

- Attack Vector
- Attack Complexity
- Privilege Required
- User Interaction

The "CVSS" page removes the Attack trees, Technical attack trees, Circumvent trees, and Attack leaves tabs from the Attack potential method and the Likelihood estimation tab from the Likelihood estimation method.

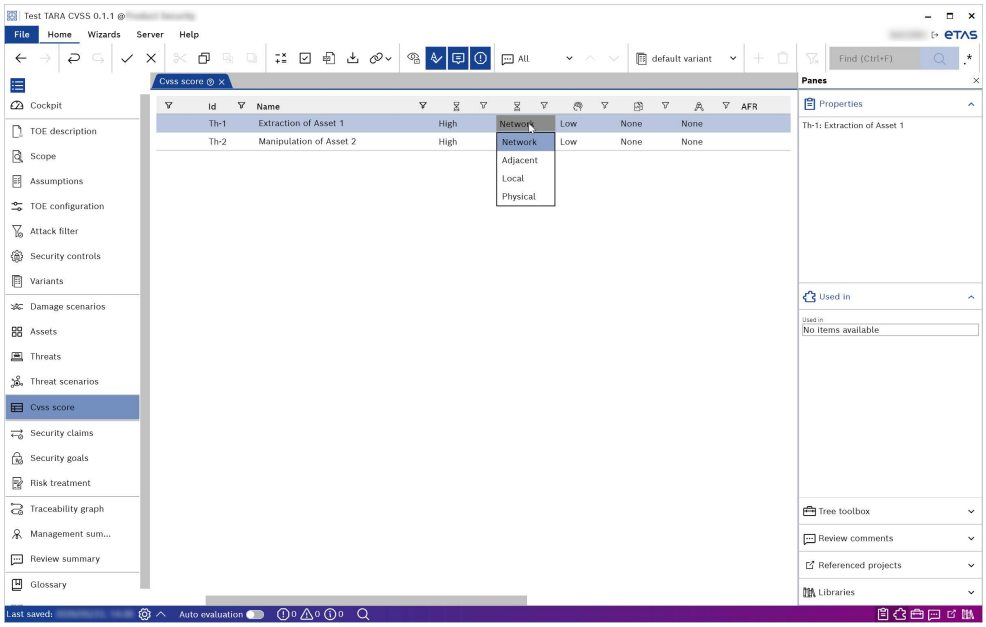


Fig. 4-20: CVSS score

4.18 Likelihood Estimation

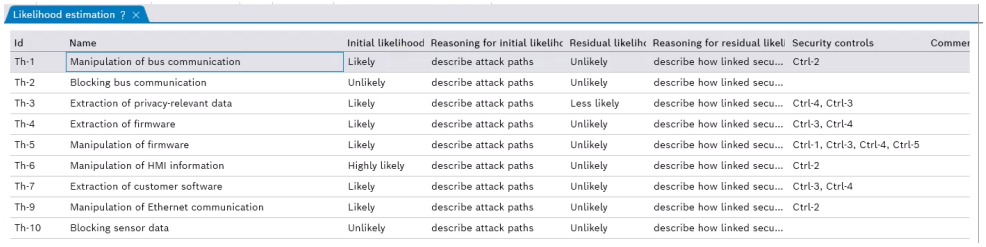
The "Likelihood estimation" method is an alternative to the "Attack potential" method used for the attack feasibility evaluation. It determines AFR without building attack trees. Instead of using such trees, the initial and residual likelihood is estimated and translated into the AFR, as shown in the table below. The likelihood is divided into four categories: highly likely, likely, less likely, and unlikely.

AFR	**Likelihood**
high	highly likely
medium	likely
low	less likely
very low	unlikely

As a consequence, this method is far less rigorous and detailed and should therefore only be used in certain use cases, e.g., high-level TARAs, SW-only projects, projects with unclear context (which HW is used, which signals are transferred, which data is stored, etc.).

You can select this method while creating a new project. On the likelihood estimation page, each threat is rated with an initial likelihood, and the reasoning for the rating is given.

- If only a TARA is done, all other columns will stay empty.
- If RRA is conducted, the residual likelihood is rated based on the linked security controls. Furthermore, reasoning for the residual likelihood is mandatory.


Likelihood estimation ? ×

Id	Name	Initial likelihood	Reasoning for initial likelihc	Residual likelihc	Reasoning for residual likeli	Security controls	Commer
Th-1	Manipulation of bus communication	Likely	describe attack paths	Unlikely	describe how linked secu...	Ctrl-2	
Th-2	Blocking bus communication	Unlikely	describe attack paths	Unlikely	describe how linked secu...		
Th-3	Extraction of privacy-relevant data	Likely	describe attack paths	Less likely	describe how linked secu...	Ctrl-4, Ctrl-3	
Th-4	Extraction of firmware	Likely	describe attack paths	Unlikely	describe how linked secu...	Ctrl-3, Ctrl-4	
Th-5	Manipulation of firmware	Likely	describe attack paths	Unlikely	describe how linked secu...	Ctrl-1, Ctrl-3, Ctrl-4, Ctrl-5	
Th-6	Manipulation of HMI information	Highly likely	describe attack paths	Unlikely	describe how linked secu...	Ctrl-2	
Th-7	Extraction of customer software	Likely	describe attack paths	Unlikely	describe how linked secu...	Ctrl-3, Ctrl-4	
Th-9	Manipulation of Ethernet communication	Likely	describe attack paths	Unlikely	describe how linked secu...	Ctrl-2	
Th-10	Blocking sensor data	Unlikely	describe attack paths	Unlikely	describe how linked secu...		

Fig. 4-21: Likelihood estimation

To differentiate the Likelihood estimation from the Attack potential method

The main differences to the attack potential method are:

- The "Assumptions" can not be enabled or disabled.
- The "Security controls" can not be enabled or disabled.
- The "Likelihood estimation" page removes the Attack trees, Technical attack trees, Circumvent trees, and Attack leaves tabs from the Attack potential method.

4.19 Attack Trees

An attack tree describes a set of attack paths that realize a given threat.

The goal of compiling an attack tree for a given threat is to systematically collect all possible and relevant attacks realizing that threat, i.e., achieving the attack goal described by the threat. For this purpose, the overall attack goal is broken down into sub-goals, and ultimately into elementary actions that must be performed in order to reach the goal.

An attack tree provides a structured way to compute the attack feasibility rating of a threat. Precisely one attack tree is designed for each threat. The nodes represent different actions that must be performed in order to carry out the attack and thus reach the attack goal.

Formally, an attack tree is a rooted tree (in the terminology of graph theory). The root node is the threat itself (recall that a threat is formulated as an action). Now consider any given node that has children. The action described by this node is decomposed into different steps and specified in more detail by the child nodes. Iterating this principle and decomposing each action further as we move away from the root, we see that the nodes describe more and more low level and elementary actions. Decomposition of a node stops when the author of the TARA decides that the node describes an action which is elementary and low level enough to be rated with an attack potential tuple; such a node is called a leaf.

In principle, an attack tree can have arbitrary depth, as the author deems appropriate, but as a general rule of thumb, three to five levels are often sufficient.

Any node that has children must be labeled either AND or OR.

- If a node is labeled AND, an attacker can perform the associated action by carrying out all actions described by its children.
- If a node is labeled OR, an attacker can perform the associated action by carrying out one of the actions described by its children.

Since all nodes that are not leaves are labeled either AND or OR, the attack tree describes a collection of attack paths, i.e., sets of elementary actions that can be carried out by an attacker in order to perform the action described by the root node (and the corresponding threat).

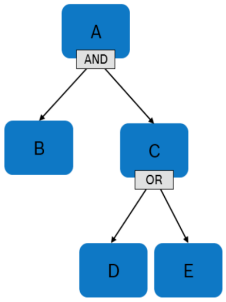


Fig. 4-22: Simplified attack tree

4.20 Technical Attack Trees

A technical attack tree is an isolated subtree of an attack tree that may be used as a subtree in many attack trees.

A technical attack tree is just like an attack tree, except that its root node does not represent a threat itself, but some lower level action.

It makes sense to outsource a collection of (partial) attack paths to a technical attack tree when they are part of many attacks. Any attack tree, technical attack tree, or circumvent tree may reference technical attack trees.

> **Note**
>
> Technical attack trees are included as references, and hence they cannot be edited within the including tree. Furthermore, technical attack trees exist only for convenience, their use is not required.

Technical attack trees

Id	Name	Used in Th
TAT-1	Backend servers used as a means to attack a vehicle or extract data	Th-7, Th-15
TAT-2	Services from backend server being disrupted, affecting the...	
TAT-3	Spoofing of messages or data received by the vehicle	
TAT-4	Denial of service attacks via communication channels to disrupt...	
TAT-5	Misuse or compromise of update procedures	Th-7, Th-9
TAT-6	Manipulation of vehicle data/code	
TAT-7	ATM-T0001: Downgrade to insecure protocols	Th-9
TAT-8	ATM-T0014: Malicious app	

Fig. 4-23: Technical attack trees

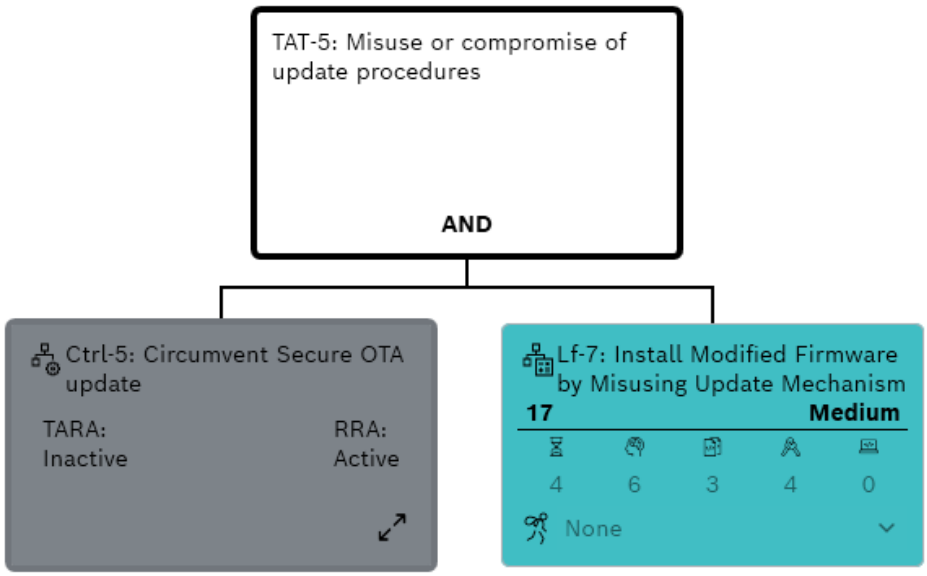


Fig. 4-24: Technical attack trees in the tree editor

4.21 Circumvent Trees

A circumvent tree corresponding to a given security control is an attack tree where the root node is the action of circumventing the security control.

A circumvent tree models the actions required to circumvent its corresponding security control. It is referenced in attack trees and technical attack trees to indicate where an enabled security control must be circumvented. Hence, this is relevant only when security controls are assumed to be enabled, particularly for the residual risk analysis.

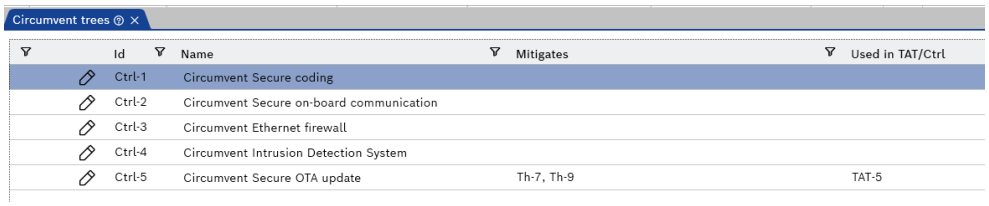


Fig. 4-25: Circumvent trees

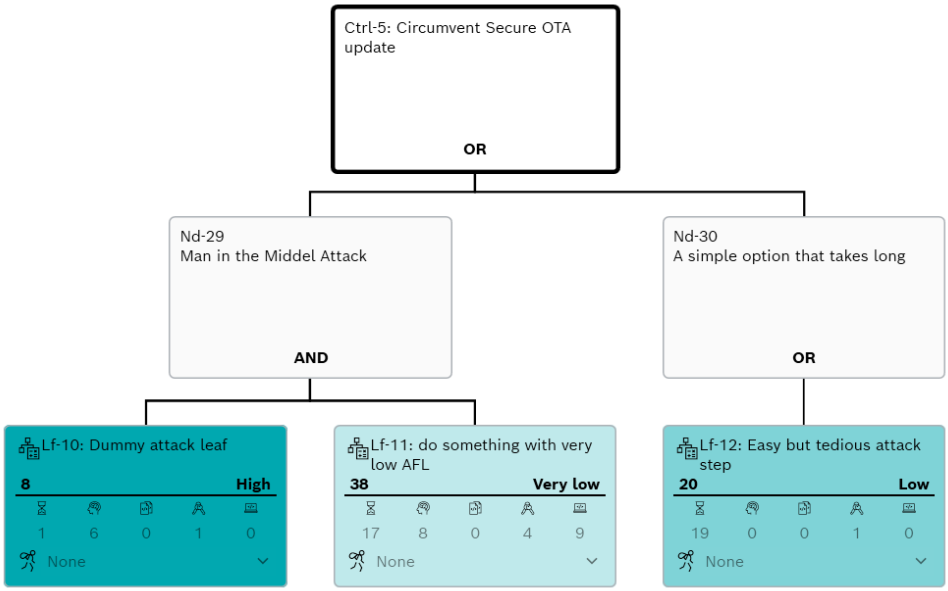


Fig. 4-26: Circumvent trees in the tree editor

4.22 Attack Leaves

An attack leaf is a leaf of an attack tree. Attack leaves represent the elementary actions that need to be taken in an attack path.

The attacks are broken down until the actions are elementary, when we stop, we have a leaf. Each leaf is rated with an attack potential tuple. An attack potential tuple rates the effort required to carry out an attack in the categories called attack capabilities i.e., time, expertise, knowledge, opportunity, and equipment.

The attack potential of each attack leaf is rated according to the tooltips available in the CycurRISK. You must provide a reason for the rating.

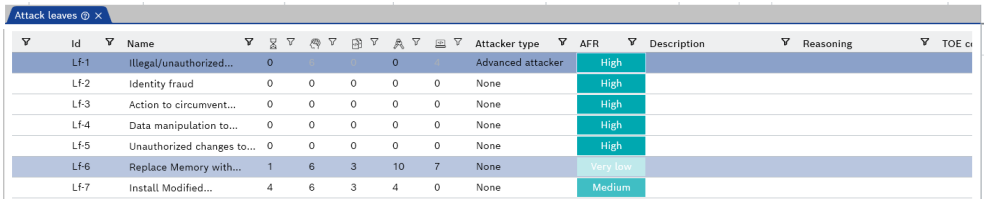


Fig. 4-27: Attack leaves

4.23 Risk Assessment and Treatment

A risk is the effect of uncertainty on road vehicle security, expressed in terms of attack feasibility and impact.

The risk for a given threat scenario is determined from the AFR of the associated threat and the impact of the associated damage scenario according to the risk matrix (see figure below) by a simple table look-up.

There are five risk levels, one is the lowest, and five is the highest risk level.

Inspecting the risks per threat scenario gives a maximally detailed view. For a shorter overview, risks may be aggregated by threat, damage scenario, or impact category. In such a case, the shown risk is the highest of all associated risks.

Attack Feasibility Rating	Risk Assessment				AP sum
high	1	3	4	5	0–13
medium	1	2	3	4	14–19
low	1	2	2	3	20–24
very low	1	1	1	2	>24
impact	negligible	moderate	major	severe	

Fig. 4-28: Risk matrix

4.23.1 Security Claims

A security claim is a statement about a risk, typically made to justify sharing or retaining a risk. In particular, one security claim must be formulated for each assumption within the TARA. For each risk with treatment share, at least one security claim must be linked on the risk treatment page, see Risk Treatment.

Security claims resulting from one or several assumptions must be linked with the corresponding assumption(s). Moreover, a responsible must be specified. This is typically a customer, or a supplier, further parties may be added.

Each security claim identified by the TARA shall be taken up in the security concept or considered with the relevant stakeholders.

For example,

- For security topics
  The security responsible for the OEM, component, SoS, and plant
- For safety topics
  Project safety manager

Fig. 4-29: Security claims

4.23.2 Security Goals

A security goal is a concept-level cybersecurity requirement associated with one or more threat scenarios.

Security goals are closely related to the technical measures designed within the security concept to mitigate the risks. At least one security goal must be linked on the risk treatment page for each risk with treatment reduction.

If a security goal is associated with a threat scenario, the corresponding requirement must be satisfied to mitigate the risk of the threat scenario. A responsibility must be specified for each security goal. This is typically a customer or a supplier; further parties may be added.

Each security goal identified by the TARA shall be taken up in the security concept or considered with the relevant stakeholders.

For example,

- For security topics
  The security responsible for the OEM, component, SoS, and plant
- For safety topics
  Project safety manager

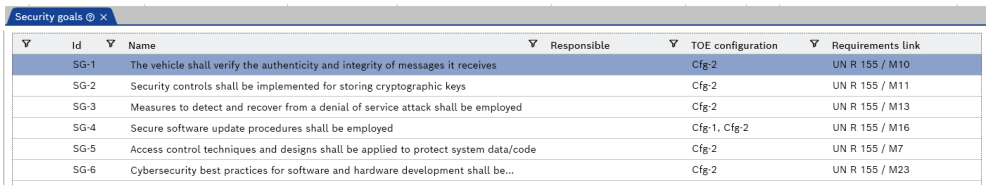


Fig. 4-30: Security goals

4.23.3 Risk Treatment

CycurRISK provides an overview of the risks on the "Risk Treatment" page. One risk is computed for each threat scenario, where the AFR is taken from the linked threat, the impact is taken from the linked damage scenario, and then the risk value between one and five is computed as specified in the Risk matrix.

When you click **Expand all**, you can see the risk for each threat scenario in the column called "Initial risk." Based on the above computation, you will get a risk value for each threat scenario and you need to make a risk treatment decisions.

A risk treatment decision for a given risk is one of the following.

- Reduce
  The risk is reduced by means of a technical measure specified in one or several security goals, which must be linked.
- Share
  The risk is shared with or transferred to one or several other parties. At least one corresponding security claim must be formulated and linked.
- Retain
  A reasoning must be given whenever a residual risk greater than one is accepted. Security claims and goals shall be linked.
- Avoid
  The risk is avoided by removing the risk sources or deciding not to start/-continue with the activity that gives rise to the risk. Notice that this often leads to a change in the target of evaluation, which in turn eliminates the corresponding risk from the final version of the TARA.

The risk treatment decision is made in the TARA and can be updated or supplemented for the RRA. A typical case would be that the decision reduce is made for the TARA, and once appropriate measures have been implemented, the risk is additionally retained in the RRA.

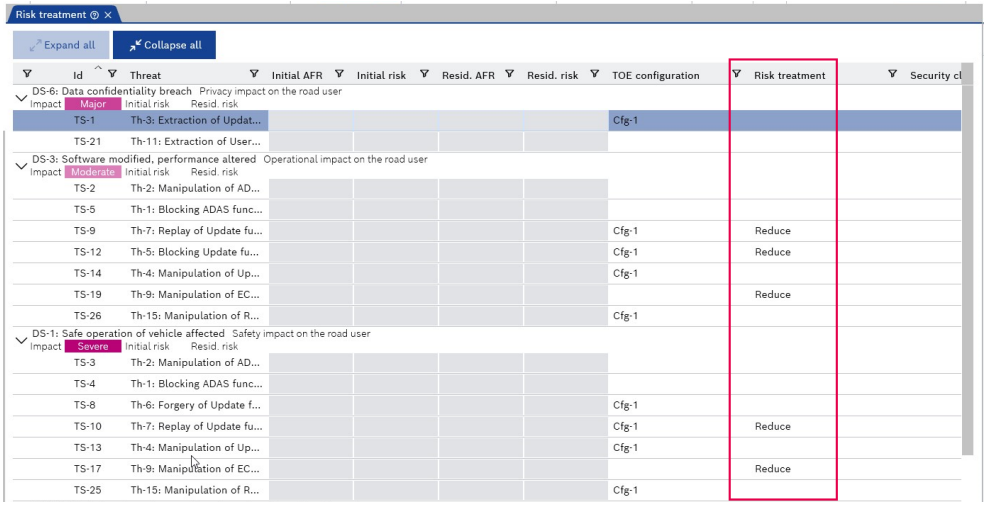


Fig. 4-31: Risk treatment

4.24 Traceability Graph

The Traceability Graph page overviews the traceability graph's functionality.

The traceability graph visualizes the relationship of the various TARA artifacts. Via highlighting, the complete relation is presented: Starting from the damage scenarios and the threats (including the assets and their properties) leading to the corresponding threat scenarios and their risks. These risks are then mitigated by linked security goals and claims, which further define the security controls.

You can choose the level of detail of information presented in the traceability graph.

The traceability graph shows the relationship between several artifacts of a TARA. From left to right, the TARA workflow is represented (similarly to the tabs in the project explorer). The relationships or links between the artifacts are shown via the gray connection lines. If one or multiple artifacts are selected, the linked artifacts are highlighted with gray backgrounds, the connection lines change the color from gray to blue.

For example, this may help you to understand which security controls mitigate which risks or which security goals are related to which threats in a TARA.

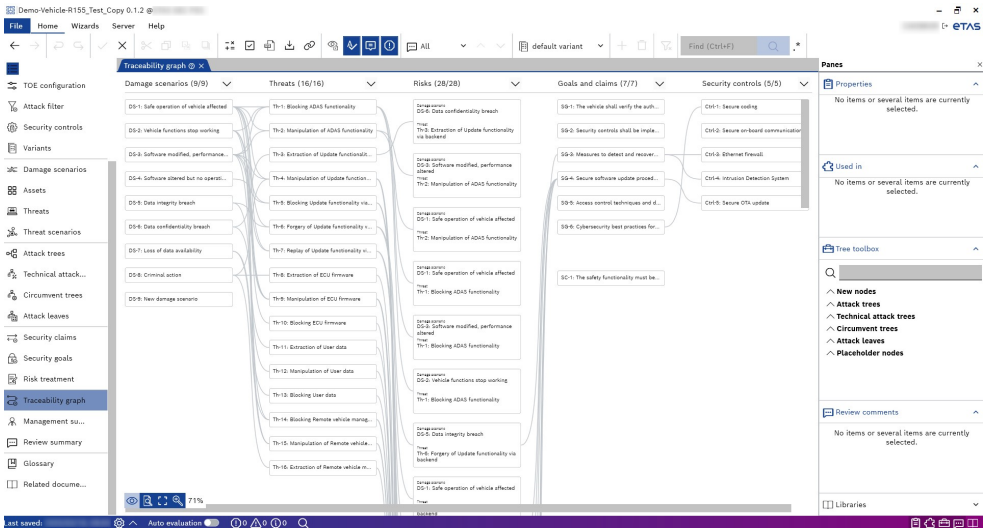


Fig. 4-32: Traceability graph

4.25 Management Summary

The Management summary page provides a brief summary of the TARA. It has three sections, where the first and the third section are filled automatically, and the second section is a text that should be written by you.

A. High level risks
B. Top findings
C. Risk matrices

4.25.1 High Level Risks

This section shows the initial and residual risks aggregated by impact category. In each case, this is the highest of all risks of threat scenarios linked to damage scenarios with the given impact category.

> **Note**
>
> The risks field will show empty if an impact category is not assigned to any damage scenario.

The first column shows the "Initial risk," i.e., the TARA risks. The initial risk can include enabled security controls, if these are already applicable for the TARA.

The second column shows the "Residual risk," i.e., the RRA risks, which are computed on the basis of the enabled security controls.

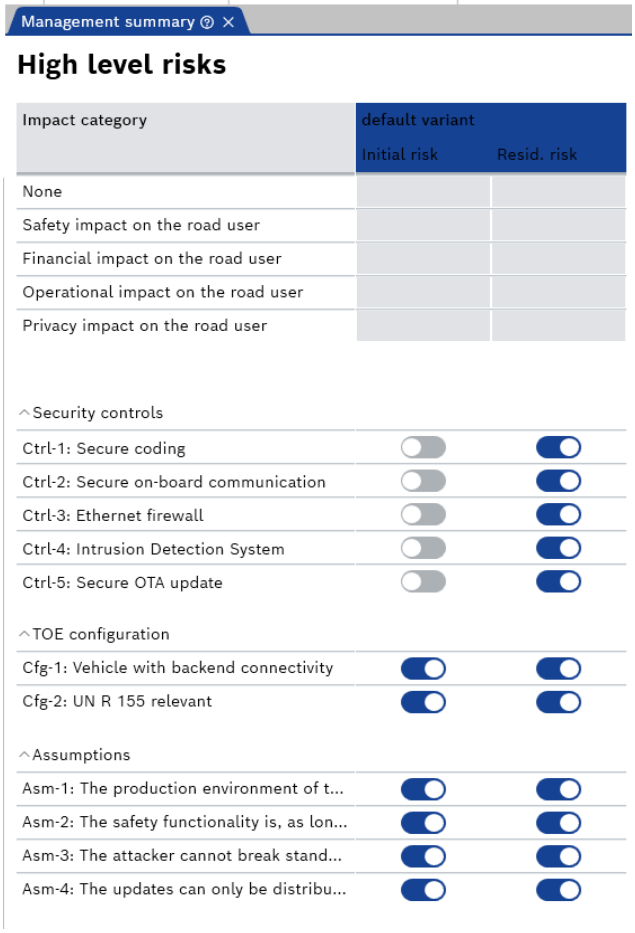


Fig. 4-33: Management summary - High level risks

4.25.2 Top Findings

This section provides a textual summary written by the author of the TARA.

The basic formatting options are provided, similar to the TOE description and Scope functionality. You can write and format the TARA's most important information or conclusions. The headlines are provided as hints on what information to include, but they may be changed or deleted as desired.

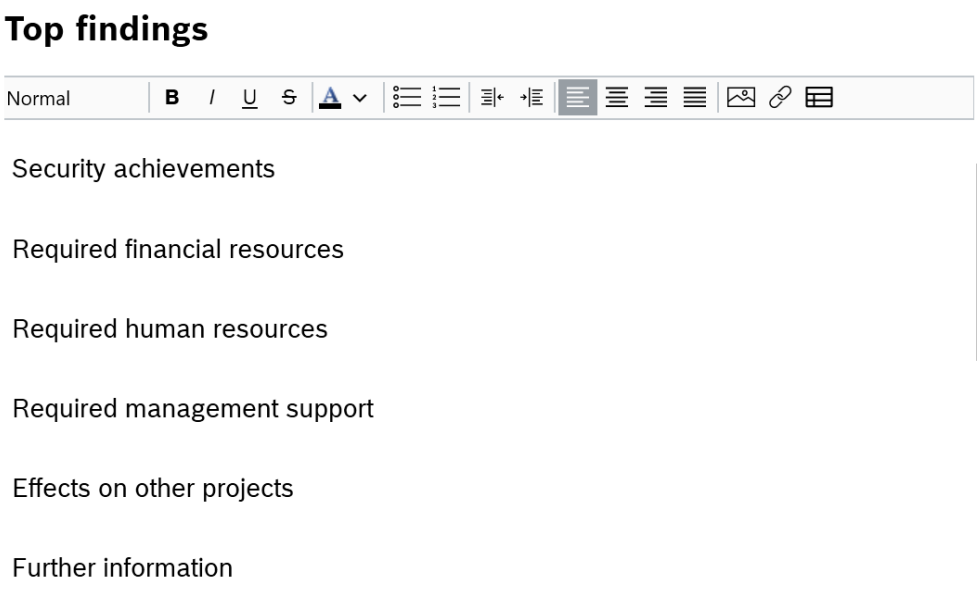


Fig. 4-34: Management summary - Top findings

4.25.3 Risk Matrices

For each initial and residual risk, matrices in the heat map style show a number of threat scenarios with that risk.

The number in each matrix cell indicates the number of threat scenarios with a corresponding risk value. A comparison of two matrices yields an overview of how the risks have shifted. The risks can only shift in the vertical direction (from top to bottom) since a security control can only influence the AFR, not the impact of a threat scenario.

By clicking on a risk field, the corresponding threat scenarios are listed with detailed information in the table below. The initial and residual risk columns compare and show each threat scenario's initial and residual risks.

4.26 Reuse Summary

The Reuse summary page summarizes the changes in a reuse TARA project with respect to the reference project. It is divided into two sections:

A. High level risks
B. Summary of changes

4.26.1 High Level Risks

The reference project is used as a base for creating the reuse project.

The **High level risks** provides a comparison of the reference project with the reuse project as follows:

- Column 1
  Initial risk of the selected variant in the reference project.
- Column 2
  Residual risk of the selected variant in the reference project.
- Column 3
  Initial risk of the currently active variant in the reuse project.
- Column 4
  Residual risk of the currently active variant in the reuse project.

It also shows the Security controls, TOE configuration, and Assumptions comparable to the Management summary or Variants pages.

Fig. 4-35: Reuse summary - High level risks

4.26.2 Summary of Changes

The **Summary of changes** shows all changes made within the reuse project compared to the reference project.

- Column 1
  Shows the known icon for the reuse project
  - Added
  - Modified
  - Removed
- Column 2
  Shows the ID and name of the artifacts
- Column 3
  Shows the type of the project item.

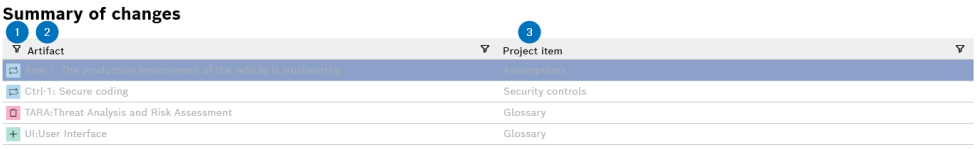


Fig. 4-36: Reuse summary - Summary of changes

4.27 Review Summary

The Review summary page shows all the review comments. It is divided into four sections mentioned below:

A. Review due date
B. Reviewer
C. Review summaries
D. Review comments

The project author can enter and add the review summary in the text field or finish the review without a summary. The table below the review summary lists all the review comments on the current project. It shows the following items:

- Artifact to which a comment is attached
- Review comment
- Author of the comment
- Detailed information about the state of the comment
- The time when it was created and edited for the last time.

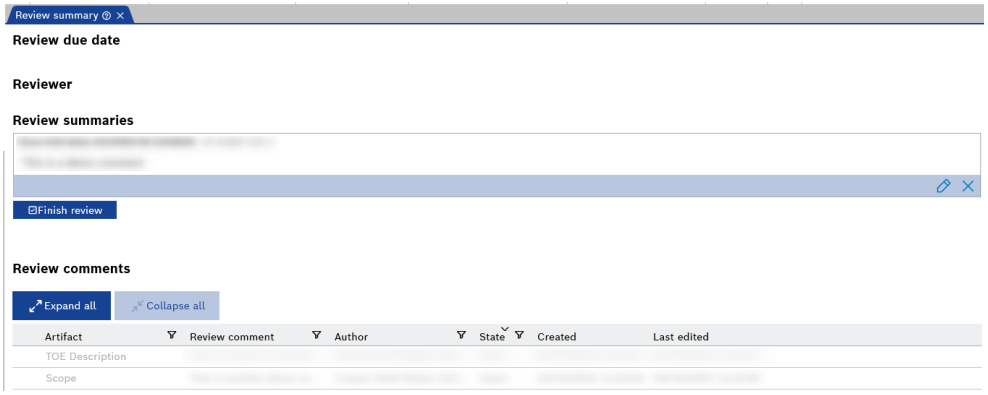


Fig. 4-37: Review summary

4.28 Glossary and Related Documents

CycurRISK provides the dedicated page for the Glossary where you can document the abbreviations used throughout the TARA.

The Related documents section is a bibliography containing a list of references used within the TARA.

You can add the glossaries and the related documents with one of the following options:

- Press CTRL+N
- Press INSERT
- Go to the **Home** menu > **Add**
- Right-click and go to the context menu > **Add**

4.29 Menus

CycurRISK comprises of the following menus:

- File
- Home
- Wizards
- Server
- Help

4.29.1 File

The **File** menu contains the following sub-menu items:

- Back
  Goes back to the current project.
- Home
  Goes back to the Home screen.
- Save
  Saves the modified changes in a current project.
- Create new
  Creates a new project.
- Projects
  Displays the current and archived projects.
- Project rights
  Displays the current and archived project rights.
- OU resources
  Displays the OU resources.
- Server management
  Displays the server management options.
- Generate report
  Shows the report creation dialog box.
- Import
  Imports a project from different formats.
- Export

Exports the current project.

- Close project
  Closes the current project.

4.29.2 Home

The **Home** menu contains the following commands:

- Backward
  Navigates backward.
- Forward
  Navigates forward.
- Undo
  Undo the last action.
- Redo
  Redo the last undo action.
- Save
  Saves the current project.
- Close project
  Closes the current project.
- Cut
  Removes the selection and adds it to the clipboard.
- Copy
  Copies the selection to a clipboard.
  - In tables
    Copies table cell contents as text.
  - In trees
    Copies nodes with substructure.
- Paste
  Inserts content from the clipboard.
- Duplicate
  Duplicates the selected item.
- Evaluate
  Triggers the evaluation for all attack trees.
- Validate
  Triggers the validation of project items.
- Generate report
  Shows the report creation dialog.
- Import
  Shows the import dialog.
- Create link to newest or this project version
  Puts a link to the newest or current project version into the clipboard.

- Hide inactive items
  Toggles the visibility of all inactive items. It will also toggle read-only mode since editing is only responsible with all items visible.
- Spell checking
  Enables or disables spell check indication and suggestions.
- Tooltip
  Shows or hides tooltip
- Status indicators
  Shows or hides errors and warnings next to the artifacts.
- Filter review comments
  Selects which review comments shall be visible. It has three options, i.e., All, All open, and None. You can jump to previous or next review comments.
- Select the active variant
  Select which variant is currently displayed and used in evaluations.
- Add
  Adds a new item.
- Remove
  Removes the selected item.
- Clear filters
  Clears all filters of the current view.
- Find
  Finds the elements in the project.
- Regex search
  Interprets the search string as a regular expression.

4.29.3 Wizards

The **Wizards** menu contains the following sub-menu items:

- Update methodology
  Select a methodology to which the current project shall be updated.
- Rebase reuse project
  Rebase this reuse project to the newest version of the reference project.
- Update project reference
  Update the artifacts that are copied from a referenced project with a newer version.
- Update library
  Update the artifacts that are copied from a library with a newer version.

4.29.4 Server

The **Server** menu contains the following sub-menu items:

- Upload a custom project
  Uploads a custom project version to the server, if the project is not yet managed by the server.
- Increment project version
  Increments the major or minor version of this project manually.
- Revert to previous project version
  Shows the available previous project versions.
- Browse projects on server
  Shows all the server projects within this OU.
- Lock/Unlock
  Locks the project and check it out for modifications. Unlocks the project and load it in the read-only mode.
- Lock project for offline mode
  Adds a lock to the project, so it can be edited even when you are not connected to the server.
- Refresh project permissions
  Checks whether the project is still locked by another user.

4.29.5 Help

The **Help** menu contains the following sub-menu items:

- User manual
  Shows tool documentation in a web browser.
- Methodology
  Shows methodology documentation in a web browser.
- Help
  Opens service desk in a web browser.
- About
  Shows the information about CycurRISK.

4.29.6 Icons

CycurRISK uses various icons or buttons for easy operation.

4.29.6.1 TARA Artifacts

Icons	Meaning
	Cockpit
	TOE description
	Scope

Icons	Meaning
	Assumptions
	TOE configuration
	Attack filter
	Security controls
	Variants
	Misuse cases
	Damage scenarios
	Assets
	Threats
	Threat scenarios
	CVSS score or Likelihood estimation
	Attack trees
	Technical attack trees
	Circumvent trees
	Attack leaves
	Security claims
	Security goals
	Risk treatment
	Traceability graph
	Management summary
	Review summary
	Glossary
	Related documents

4.29.6.2 File Menu

Icons	Meaning
	Back
	Home
	Save
	Create new
	Projects
	Project rights
	OU resources
	Server management
	Generate report
	Import
	Export
	Close project

4.29.6.3 Home Menu

Icons	Meaning
	Backward
	Forward
	Undo
	Redo
	Save
	Close project
	Cut

Icons	Meaning
	Copy
	Paste
	Duplicate
	Evaluate
	Validate
	Generate report
	Import
	Create link to newest or this project version
	Hide inactive items
	Spell checking
	Tooltip
	Status indicators
	Filter review comments
	Select the active variant
	Add
	Remove
	Clear filters
	Find
.*	Regex search

4.29.6.4 Wizards Menu

Icons	Meaning
	Update methodology
	Rebase reuse project
	Update project reference
	Update library

4.29.6.5 Server Menu

Icons	Meaning
	Upload a custom project
	Increment project version
	Revert to previous version
	Browse projects on server
	Lock
	Unlock
	Lock project for offline mode
	Refresh project permissions

4.29.6.6 Help Menu

Icons	Meaning
	User manual
	Methodology
	Help
	About

4.29.6.7 Rich Text Format Editor

Icons	Meaning
Normal	Paragraph settings
B	Bold
I	Italic
U	Underline
S	Strikethrough
A	Font color
	Bullets
	Numbering
	Decrease indent
	Increase indent
	Left
	Center
	Right
	Justify
	Picture
	Hyperlink
	Table

4.29.6.8 Attack Trees

Icons	Meaning
	Edit in tree editor
	Elapsed time
	Specialist expertise

Icons	Meaning
	Knowledge of the item or component
	Window of opportunity
	Equipment
	Show threat
	Collapse subtree
	Extend subtree
	Show referenced tree
	Hide referenced tree
	Toggle layout of tree (to horizontal view)
	Toggle layout of tree (to vertical view)
	Show/hide highlighting of critical path.
	Highlight cycles in tree

4.29.6.9 Traceability Graph

Icons	Meaning
	Show/hide items that are not affected by current selection
	Show details
	Auto fit
	Show/hide zoom panel

4.29.6.10 Context Menu

Icons	Meaning
	Show tree in tabular view
	Move left
	Move right
	Extract as technical attack tree
	Open in new window
	Open in new tab in left view
	Open in new tab in right view

4.29.6.11 Status Bar

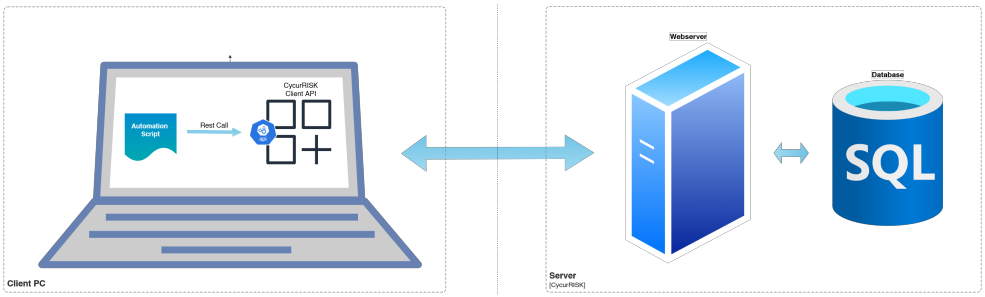
Icons	Meaning
	Auto save
	Set auto save time interval
	Show or hide the errors
	Show or hide the warnings
	Show or hide the info grid
	Show the properties grid
	Show where used in
	Show the tree toolbox
	Show the review comments
	Show the referenced projects
	Show libraries the libraries toolbox

5 Headless Mode

The CycurRISK API-Client is a stand-alone GUI-less version of CycurRISK GUI-Client. You can control the API-Client via REST API calls. All available rest endpoints of Client-API are documented via Swagger UI.

After startup, the API client starts a local web server that listens to REST calls on port 5160. You can set the port number via a command-line parameter.

See the API-Client architecture as shown in the image below.



For the restrictions and system requirements to install and run API-Client, see Restrictions and General respectively.

5.1 Download and Installation

The API-Client is integrated into the UI-Client installer. You can find the CycurRiskClientApi.exe in the installation folder.

> **Note**
>
> Windows 10 or higher version is required to install the API-Client.

5.2 Working with the API-Client

To work with the API-Client

1. Copy the CycurRISK installation path.
2. Open one of the following command-line interface and navigate to the copied CycurRISK installation path:
   - Disk Operating System (DOS) or Command Prompt
   - Windows PowerShell
   - Git Bash
3. Run the executable file:
   CycurRiskClientApi.exe

⇨ The API Client starts and launches CycurRISK.

You can also start the API Client using an existing project link to directly open the corresponding project. See Opening an Existing Project for more information.

5.2.1 Creating a New Project

You can run the program CycurRiskClientApi.exe with the commands below to create new projects:

Commands	Meaning
new-tara	Creates a new TARA projects
new-system-tara	Creates a new system TARA project
new-reuse-tara	Creates a reuse project
new-library	Creates a new library

Additionally, you require necessary attributes below:

Attributes	Meaning
--location <location>	Specifies the server and organisational unit where the project should be created
--name <name>	Specifies the name of the new project
--methodology-key <methodology-key>	Specifies the name of the methodology
--methodology-version <methodology-version>	Specifies the version of the methodology
--system-configuration <system-configuration>	Specifies the name of the system configuration
--misuse-cases	Specifies whether misuse cases should be supported in the project
--threat-specific-security-controls	Specifies whether threat specific security controls should be supported in the project
--reference-project <reference-project>	Specifies the project that should be referenced. This must be CycurRISK link

For more information, you can refer the “Help” menu.

5.2.2 Cloning a project

You can run the program CycurRiskClientApi.exe and pass the copied reference project link and the new project name as a parameters.

Example:

CycurRiskClientApi.exe clone --reference-project <project link> --name "My new project"

5.2.3 Opening an Existing Project

You can run the program **CycurRiskClientApi.exe** and pass the copied project link as a parameter. This will open the respective TARA or Library project.

Example:

CycurRiskClientApi.exe open --project <project link>

> **Note**
>
> CycurRISK TARA or Library-project link is a URL pointing to a TARA or Library project. You can copy this link using the GUI, go to the “Projects” menu, and click **Copy a link to the newest or this project version into the clipboard** icon on the desired project or library version. This will copy a link to the project or library version into the clipboard.

5.3 Accessing Swagger UI Rest-API Endpoint Documentation

Swagger is interactive API documentation that allows you to live test APIs in the browser.

You can go to the link http://localhost:5160/swagger/index.html to open the interactive Swagger API endpoint documentation. The link becomes available only after you start **CycurRiskClientApi.exe**.

6 System TARA

A System TARA is designed to model and analyze all parts of a system hierarchically based on the system architecture. It provides an easy way of evaluating risks for the entire system and various parts of the system, such as features, components, data points, interfaces, and the relationship between the corresponding TARA artifacts.

See Creating a New System TARA for information on creating a new System TARA project.

6.1 System Configuration

The System configuration structures the TOE and, therefore, the TARA in a hierarchical way. It generally works analogously to the TOE configuration.

You can create the system configuration items on the System configuration page. There are four hierarchy levels for the system configuration items as follows:

A. Product
B. Project
C. Data
D. Component

To create system configuration items

1. Go to the **Home** menu > Click **Add** icon.
   The drop-down menu is displayed.

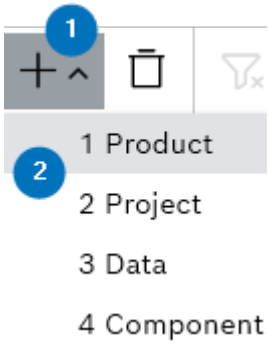


Fig. 6-1: Add node (+) drop-down

2. Select the configuration items.
   The system configuration item is created.

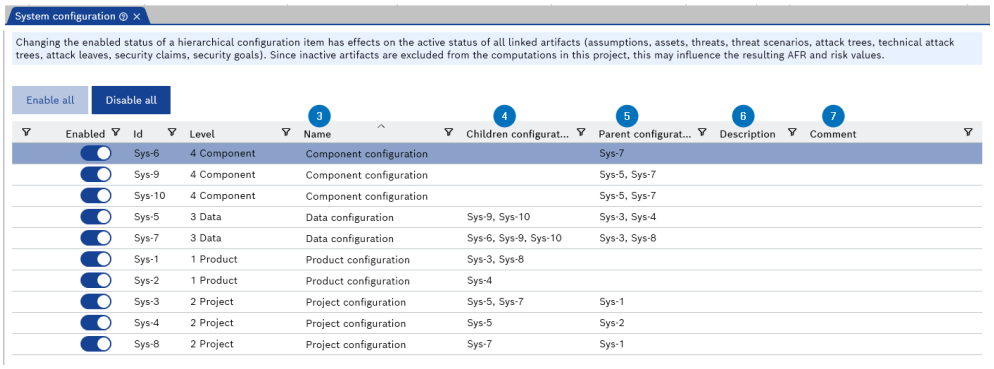


Fig. 6-2: System configuration

3. Enter **Name** of the item.
4. Select the child items from the **Children configurations** drop-down menu.

> **Note**
>
> The children configurations are automatically kept in sync with the parent configurations. You can select an item below the hierarchy level; the lowest hierarchy level does not have child items.

5. Select the parent items from the **Parent configurations** drop-down menu.

> **Note**
>
> The parent configurations are automatically kept in sync with the children configurations. You can select an item above the hierarchy level; the highest hierarchy level does not have parent items.

6. Enter **Description** of the item.
7. Enter **Comment** of the item. This step is optional.

.

6.2 System Graph

The System graph displays the hierarchy and connections between the system configuration items and gives a good overview of the system configuration. It is analogous to the Traceability graph.

The view depends on the active variant, and filters can be used to configure it further. You can enable or disable the configuration items on the System configuration page.

The system graphs are automatically created based on the system configuration items and their connection.

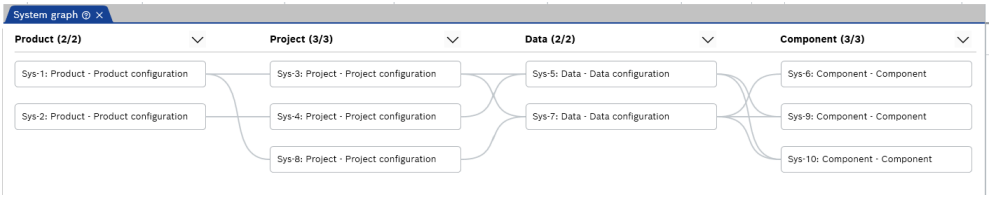


Fig. 6-3: System graph

7 Project Management

7.1 Creating a New Project

The Create new dashboard is an interface that allows you to create new TARA, new system TARA, new reuse TARA, and new library. It also provides an option to clone an existing TARA project, and convert it to a system TARA.

7.1.1 Creating a New TARA

To create a new TARA project

1. Perform one of the following steps:
   - Click **Create new** in the "Home" screen.
   - Go to the **File** menu > **Create new**.
     The New TARA is selected by default and a corresponding screen is displayed.

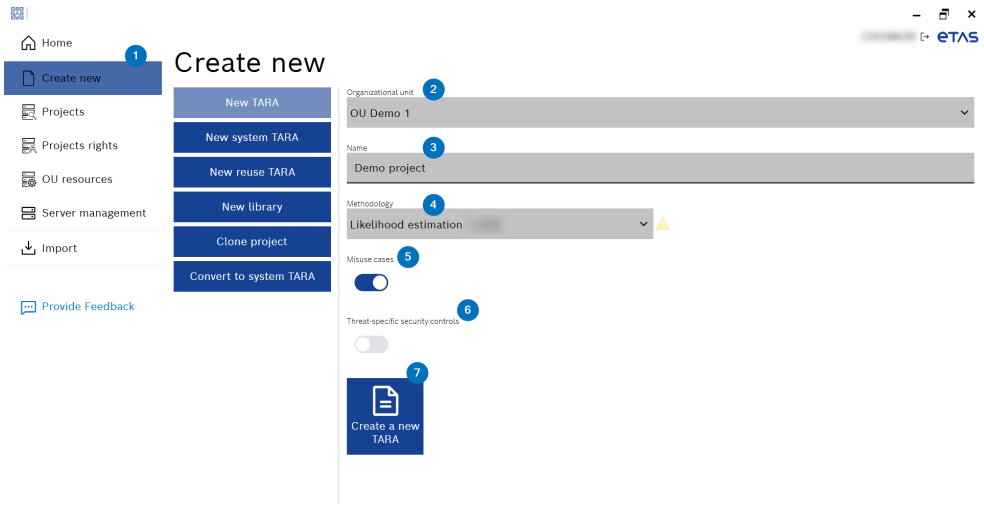


Fig. 7-1: New TARA

2. Select an organizational unit from the "Organizational unit" drop-down list.
3. Enter the "Name" of a project.
4. Select a methodology from the "Methodology" drop-down list.

> **Note**
>
> Using the methodology wizard, you can change the selected methodology again after the project creation.

5. Decide whether you want to use a misuse cases with the "Misuse cases" toggle button.
   This step is optional.

6. Decide whether you want to enable a security control for each thread with "Threat-specific security controls" toggle button.
   This step is optional.
   The "Create a new TARA" button is enabled.
7. Click **Create a new TARA**.
   The new TARA project is created and the Cockpit window is displayed with the metadata for the new TARA project.

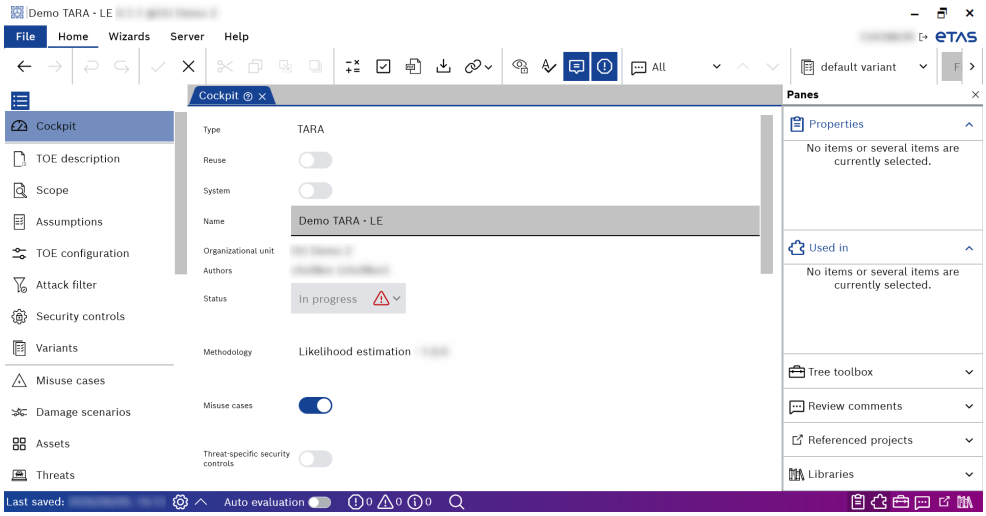


Fig. 7-2: TARA projects cockpit window

The Project Explorer window on the left corresponds to the "Methodology" selected for the TARA workflow. You can navigate it from top to bottom, guiding you through the various steps required to complete the TARA project.

7.1.2 Creating a New System TARA

To create a new system TARA project

1. Perform one of the following steps:
   - Click **Create new** in the "Home" screen.
   - Go to the **File** menu > **Create new**.
     The Create new screen is displayed.
2. Click **New system TARA**.
   The screen corresponding to new system TARA is displayed.

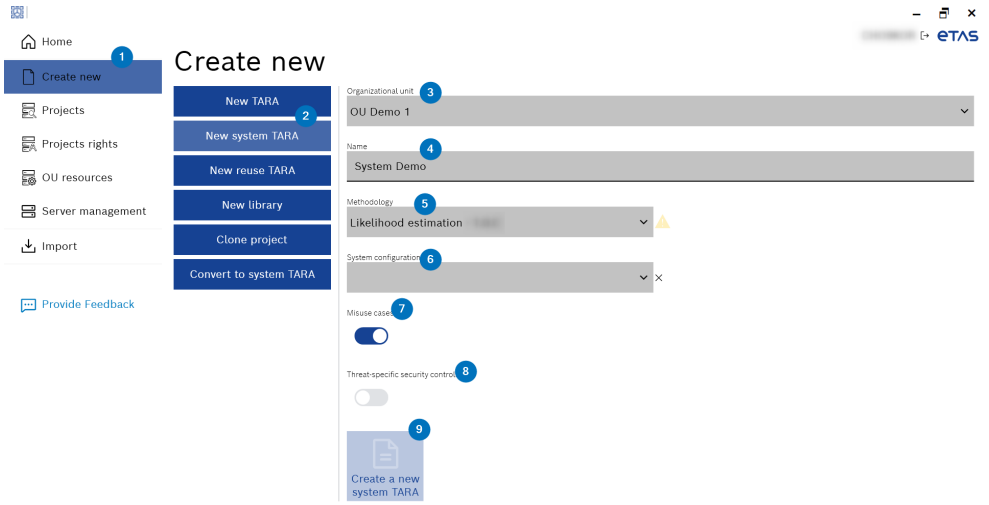


Fig. 7-3: New system TARA

3. Select an organizational unit from the "Organizational unit" drop-down list.
4. Enter the "Name" of a project.
5. Select a methodology from the "Methodology" drop-down list.
6. Select a system configuration from the "System configuration" drop-down list.
7. Decide whether you want to use a misuse cases with the "Misuse cases" toggle button.
   This step is optional.
8. Decide whether you want to enable a security control for each thread with "Threat-specific security controls" toggle button.
   This step is optional.
   The "Create a new system TARA" button is enabled.
9. Click **Create a new system TARA**.
   The new system TARA project is created and the "Cockpit" window is displayed with the metadata for the new system TARA.

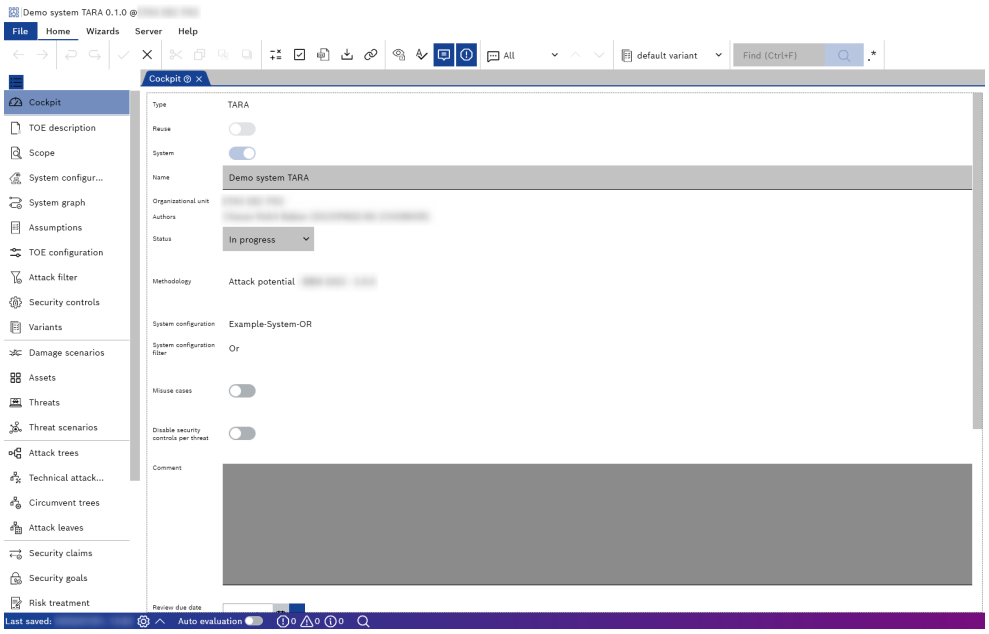


Fig. 7-4: System TARA projects cockpit window

The Project Explorer window on the left corresponds to the "Methodology" selected for the system TARA workflow. You can navigate it from top to bottom, guiding you through the various steps required to complete the system TARA project.

7.1.3 Creating a New Reuse TARA

You can reuse the TARA projects and libraries from other OUs. You will see the projects from other OUs in the **Reference project** › **Organizational unit** column.

> **Note**
>
> You allow to see and clone or reuse the libraries from other OUs only when you have an access to those libraries.

To create a new reuse TARA project

1. Perform one of the following steps:
   - Click **Create new** in the "Home" screen.
   - Go to the **File** menu › **Create new**.
     The "Create new" window is displayed.
2. Click **New reuse TARA**.
   The screen corresponding to new reuse TARA is displayed.

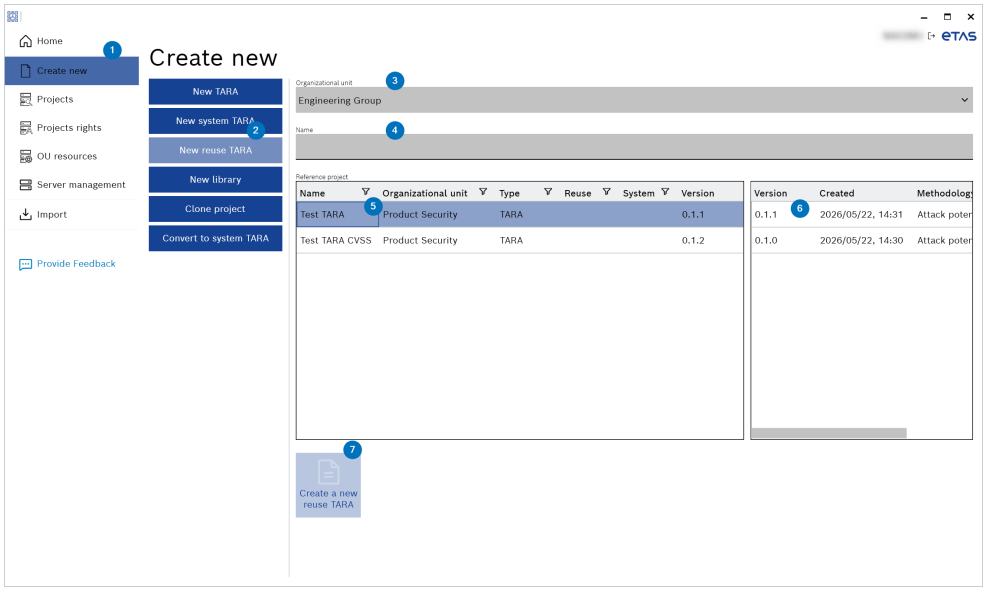


Fig. 7-5: New reuse TARA

3. Select an organizational unit from the "Organizational unit" drop-down list.
   The project list from other OUs are displayed in the "Reference project".
4. Enter the "Name" of a project.
5. Select a reference project from the list.
6. Select a version of the reference project from the list.
   The "Create a new reuse TARA" button is enabled.
7. Click **Create a new reuse TARA**.
   The selected reference project is cloned and a new reuse TARA project is created. The "Cockpit" window is displayed in the new window with the metadata for the new reuse TARA project.

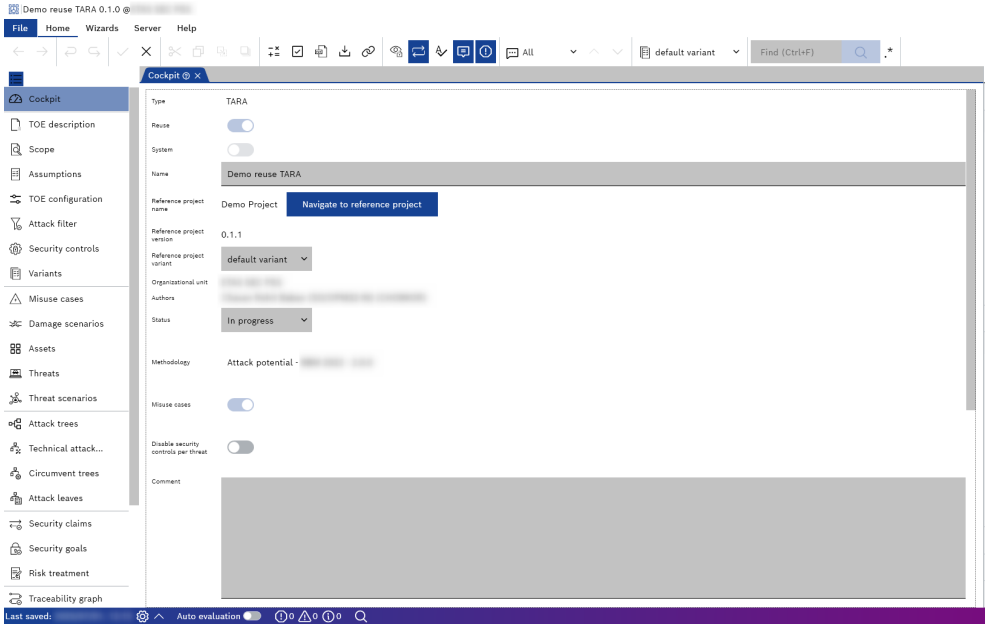


Fig. 7-6: Reuse TARA projects cockpit window

The Project Explorer window on the left corresponds to the reuse TARA workflow. You can navigate it from top to bottom, guiding you through the various steps required to complete the reuse TARA project.

7.1.4 Creating a New Library

To create a new library

1. Perform one of the following steps:
   - Click **Create new** in the "Home" screen.
   - Go to the **File** menu > **Create new**.
     The "Create new" window is displayed.
2. Click **New library**.
   The screen corresponding to new library is displayed.

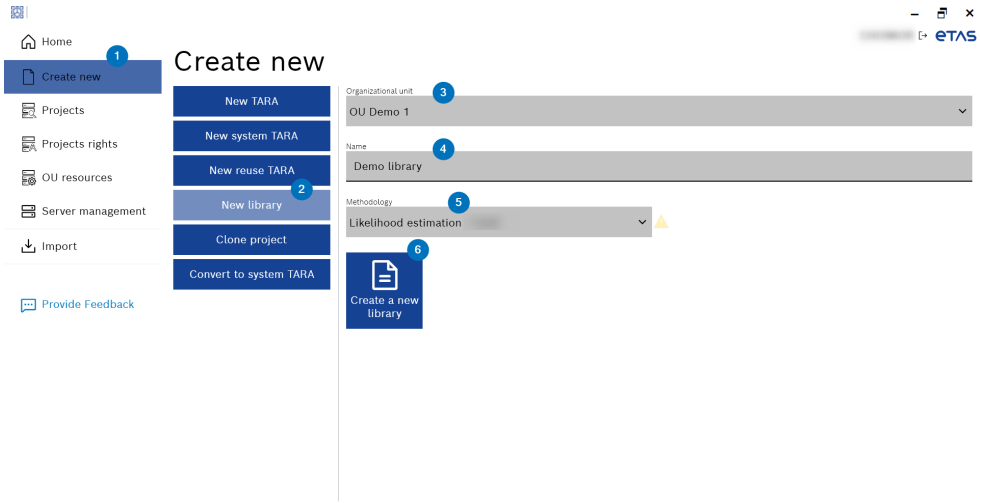


Fig. 7-7: New library

3. Select an organizational unit from the "Organizational unit" drop-down list.
4. Enter the "Name" of a project.
5. Select a methodology from the "Methodology" drop-down list.
   The "Create a new library" button is enabled.
6. Click **Create a new library**.
   The new library is created and the "Cockpit" window is displayed with the metadata for the new library.

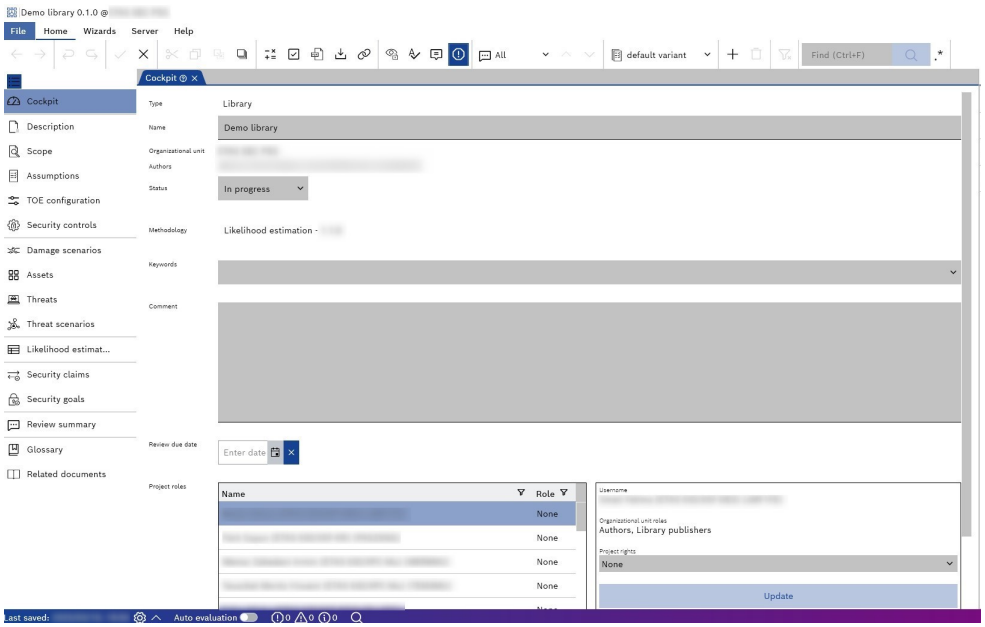


Fig. 7-8: Library cockpit window

The Project Explorer window on the left corresponds to the "Methodology" selected for the library workflow. You can navigate it from top to bottom, guiding you through the various steps required to complete the library.

7.1.5 Creating a New Clone Project

To create a new clone project

1. Perform one of the following steps:
   - Click **Create new** in the "Home" screen.
   - Go to the **File** menu > **Create new**.
     The "Create new" window is displayed.
2. Click **Clone project**.
   The screen corresponding to clone project is displayed.

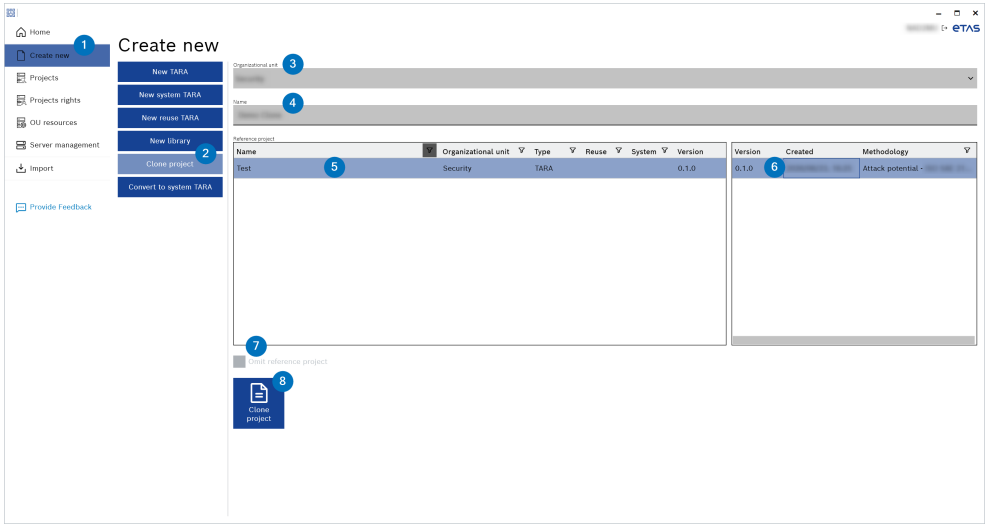


Fig. 7-9: Clone project

3. Select an organizational unit from the "Organizational unit" drop-down list.
4. Enter the "Name" of a project.
5. Select a reference project from the list.
6. Select a version of the reference project from the list.
   The "Clone project" button is enabled.
7. Decide whether you want to omit the reference project and activate or deactivate the "Omit reference project" check box. This step is optional.
8. Click **Clone project**.
   The new clone project is created and the "Cockpit" window is displayed with the metadata for the new clone project.

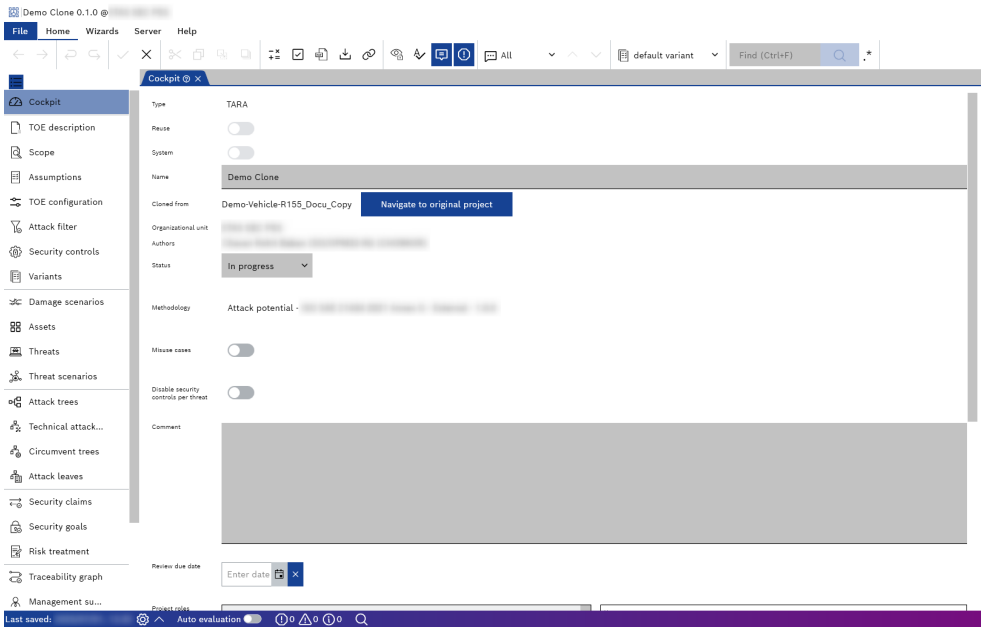


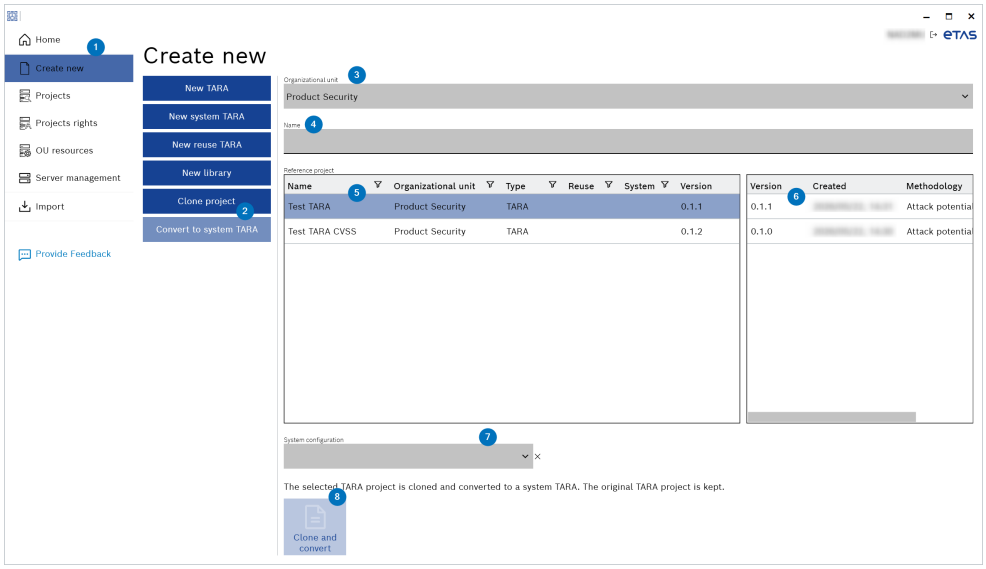
Fig. 7-10: New clone project cockpit window

The Project Explorer window on the left corresponds to the clone project workflow. You can navigate it from top to bottom, guiding you through the various steps required to complete the clone project.

7.1.6 Converting TARA to System TARA

To convert the TARA to the system TARA project

1. Perform one of the following steps:
   - Click **Create new** in the "Home" screen.
   - Go to the **File** menu > **Create new**.
     The “Create new” window appears.
2. Click **Convert to system TARA**.
   The corresponding screen appears.



3. Select an organizational unit from the "Organizational unit" drop-down list.
4. Enter the "Name" of a project.
5. Select a reference project from the list.
6. Select a version of the reference project from the list.
7. Select a system configuration from the "System configuration" drop-down list.
   The “Clone and convert” button is enabled.
8. Click **Clone and convert**.
   The selected TARA project is cloned and converted to a system TARA. The original TARA project is kept.

7.2 Opening a Local File

You can open an existing CycurRISK project (in *.tra or *.tralib formats) with the following methods.

- Opening a local project file from a specific location
- Opening a recent project from the Project List
- Browse and double-click a *.tra or *.tralib file to open.

7.3 Importing a Project from Different Formats

The "Import" option allows you to import old TARA projects into CycurRISK in different formats.

7.3.1 Importing from CSV

You can import the CycurRISK project from the CSV files. To export the project to CSV format, refer to Generating a CSV.

To import a project from CSV file

1. Go to the **File** menu > **Import**.
   The "Import" window is displayed.

Fig. 7-11: Import - CSV

2. Select **Csv** from the "Import format" drop-down list.
3. Enter the path of the CycurRISK project in the "Import path" field.
   or
   Click **...** to browse and select the CycurRISK project path.
   The "Import" button is enabled.
4. Click **Import**.

⇨ The CycurRISK project is imported.

7.3.2 Importing from Excel

> **Note**
>
> The import of a TARA project in Excel requires a proprietary template. If this import feature is required, you should contact ETAS via support. See Contact Information for more information.

To import a project from Excel

1. Perform one of the following steps:
   - Click **Import** in the "Home" screen.
   - Go to the **File** menu > **Import**.
     The "Import" window is displayed.

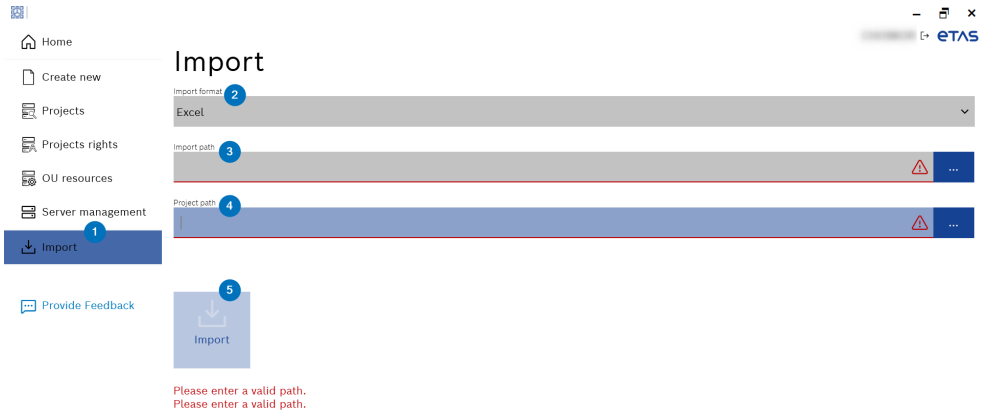


Fig. 7-12: Import - Excel

2. Select **Excel** from the "Import format" drop-down list.
3. Enter the path of the Excel TARA (*.xlsm or *.xlsx format) in the "Import path" field.
   or
   Click **...** to browse and select it.
4. Enter the path where the imported project should be saved in the "Project path" field.
   or
   Click **...** to browse and select it.
   The "Import" button is enabled.
5. Click **Import**.

⇨ The Excel TARA is imported.

7.3.3 Importing from Tra

You can import the CycurRISK project from the *.tra format files.

To import a project from Tra file

1. Go to the **File** menu › **Import**.
   The "Import" window is displayed.

2. Select **Tra** from the "Import format" drop-down list.
3. Enter the path where the imported project should be saved in the "Project path" field.
   or
   Click **...** to browse and select it.
   The "Import" button is enabled.
4. Click **Import**.

➪ The *.tra format TARA file is imported.

7.4 Saving a Project

Saves the modified changes in a project.

To save the modified changes

– Click **Save** icon on the **Home** menu.
  or
– Go to the **File** menu and click **Save**.

➪ The modified changes are saved.

7.5 Closing a Project

Closes an opened CycurRISK project.

To close a project

– Click **Close project** icon on the **Home** menu.
  or
– Go to the **File** menu and click **Close project**.

➪ An open project is closed.

7.6 Exporting a Report in CSV or Tra Format

You can export the analyzed content into CSV or Tra format. The CSV file contains all the raw data that you can use as a base for generating PDF reports.

To generate a CSV or Tra file

1. Perform one of the following steps:
   - Click the **Export** icon on the "Home" menu.
   - Go to the **File** menu > **Export**.
     The “Export” screen appears.

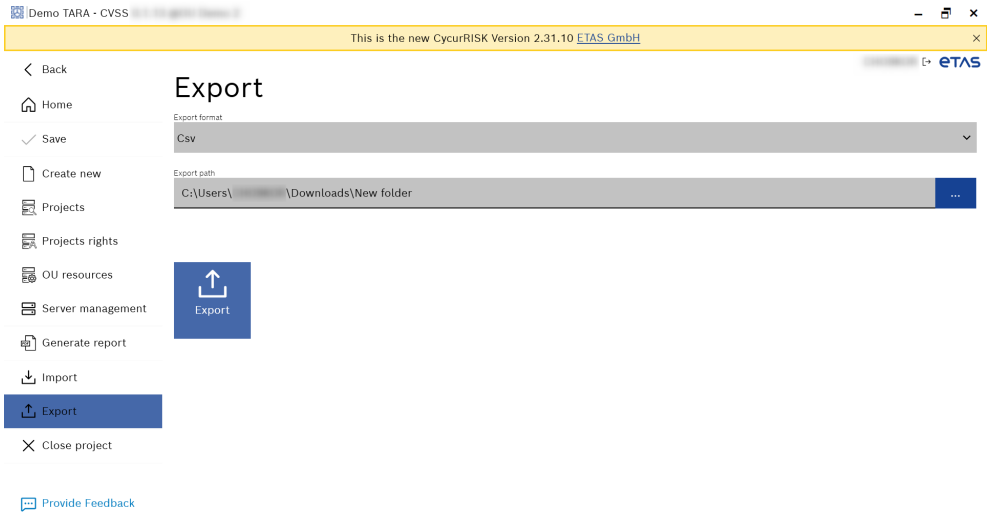


Fig. 7-13: The "Export" window

2. Select Csv or Tra from the “Export format” drop-down list.
3. Enter the valid export path in the "Export path" field or click **...** to browse and select it.
   The Export button is enabled.
4. Click **Export**.

⇨ The report is exported in the selected format.

7.7 Managing the Project Rights

You can manage the user rights to current and archived projects.

To manage the project rights

1. Go to the **File** menu > **Project rights**.
   The "Project rights" window is displayed.

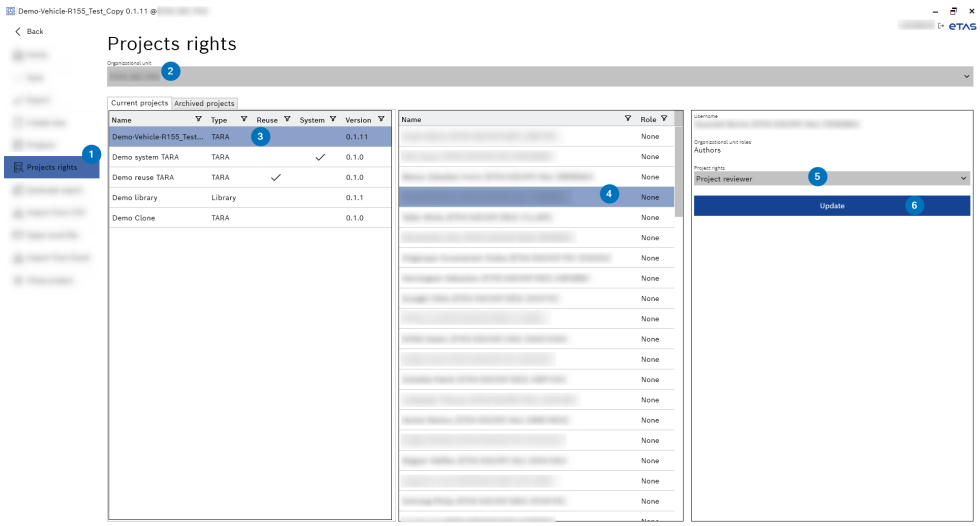


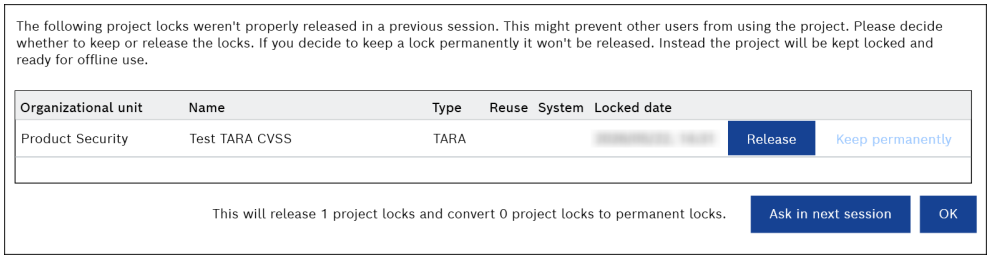
Fig. 7-14: Managing the project rights

2. Select an organizational unit from the "Organizational unit" drop-down menu.
3. Select the project from the Current or Archived projects list.
4. Select the user from the list.
5. Select the project rights from the "Project rights" drop-down menu.
6. Click **Update**.

⇨ The project rights are assigned.

7.8 Managing Project Locks

On startup of CycurRISK, the system displays a pop-up if one or more projects were not properly released in a previous session. This indicates that the projects are still locked by you or by other users, preventing access for others.



To manage project locks

- Click **Release**.
  To release the lock and make the project available for use.
- Click **Keep permanently**.
  To keep the lock and continue working on the project offline.
  In this case, the system retains lock until you release it within the project, preventing other users from accessing the project. See the Adding or Removing a Project Lock for more information.

7.9 Adding or Removing a Project Lock

You can lock or unlock the project automatically or manually so that another user can not edit it. When you open the project, it is automatically locked for editing by another user. However, this user can open the project in read-only mode.

To manually lock the project

1. Open the project and go to the **Server** menu.
   The server sub-menus are displayed.

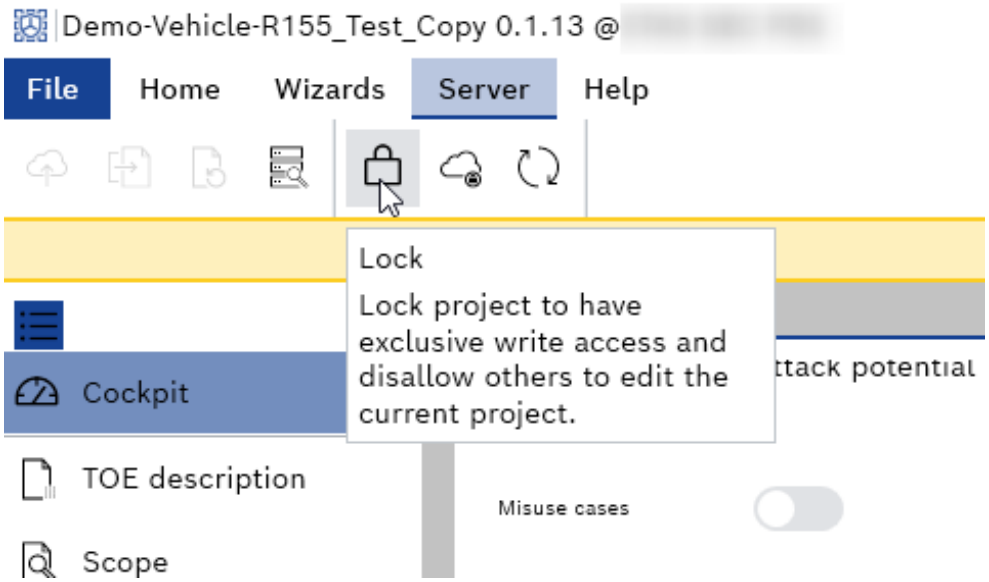


Fig. 7-15: Locking the project

2. Click **Lock** icon.

⇨ The project is locked.

To manually unlock the project

Perform the following steps:

1. Go to the **File** menu › **Projects**.
   The "Projects" window is displayed.

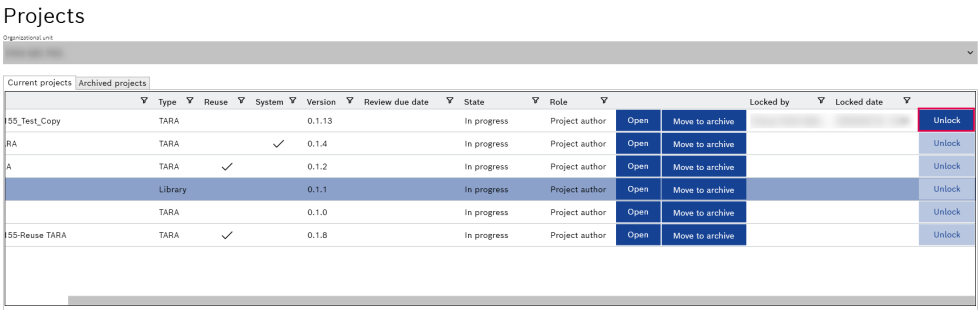


Fig. 7-16: The "Projects" window

2. Select the organizational unit from the "Organizational unit" drop-down menu.
3. Go to the locked project and click **Unlock**.

⇨ The project is unlocked.

or

1. Open the project and go to the **Server** menu.
   The server sub-menus are displayed.

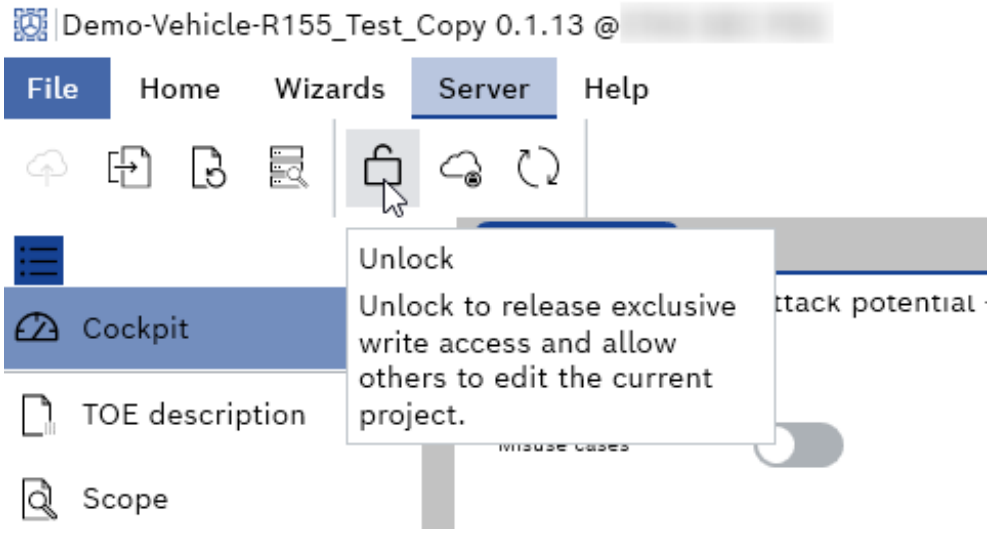


Fig. 7-17: Unlocking the project

2. Click **Unlock** icon.

⇨ The project is unlocked.

7.10 Comparing a Project

You can compare the two different versions of the project.

> **Note**
>
> Comparing project versions is only possible when both versions have the same methodology.

To compare a projects

1. Go to the **File** menu › **Projects**.
   The "Projects" window is displayed.

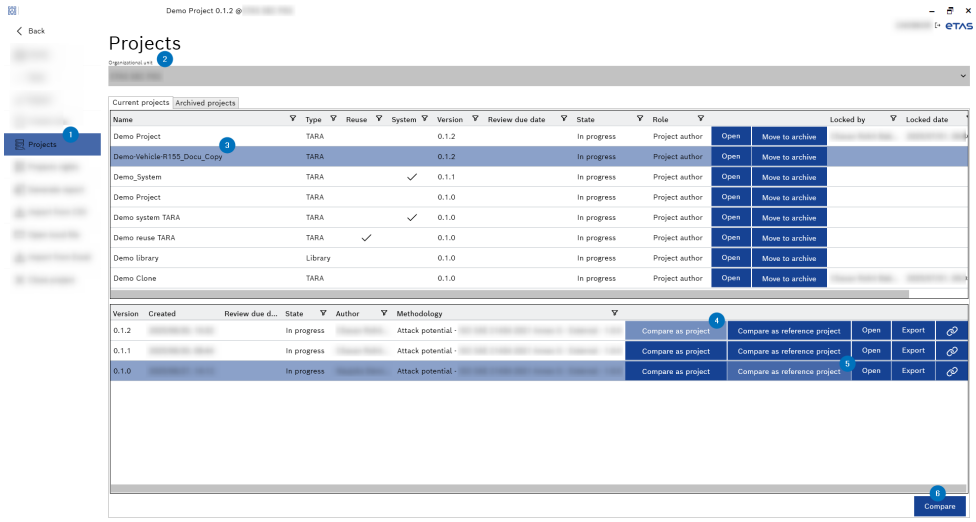


Fig. 7-18: Comparing a projects

2. Select the organizational unit from the "Organizational unit" drop-down menu.
3. Select the project from the Current or Archived projects window.
4. Click **Compare as project** to select the project version.
5. Click **Compare as reference project** to select the another project version.
6. Click **Compare**.

⇨ The project comparison is opened in a new CycurRISK instance as a read-only mode.

The visual indicators show the difference between the "Project" and the "Reference project." They highlight "Added," "Modified," and "Removed" artifacts compared to the reference project.

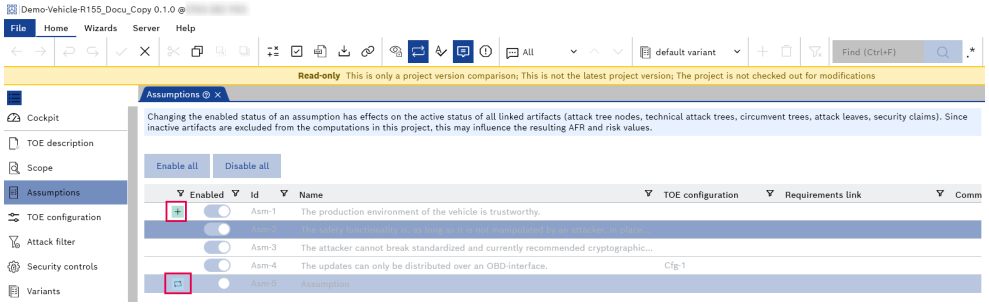


Fig. 7-19: Comparison of two project versions

7.11 Copy and Paste TARA Artifacts between and within Projects

You can copy and paste a single or multiple TARA artifacts along with all linked items from one project to another only if the methodologies are compatible. To multi-select several artifacts, use CTRL+CLICK for arbitrary artifacts and SHIFT+CLICK for a range of artifacts.

The copy and paste functionality helps to copy the following artifacts:

- TOE configuration
- Assumptions
- Security controls
- Security properties
- Attack trees
- Technical attack trees
- Circumvent trees
- Security claims

To copy the TARA artifacts

1. Perform one of the following steps:
   - Right-click the artifact and select **Copy** from the context menu.
   - Select the artifact and click **Copy** icon from the "Home" menu.
   - Press CTRL+SHIFT+C.

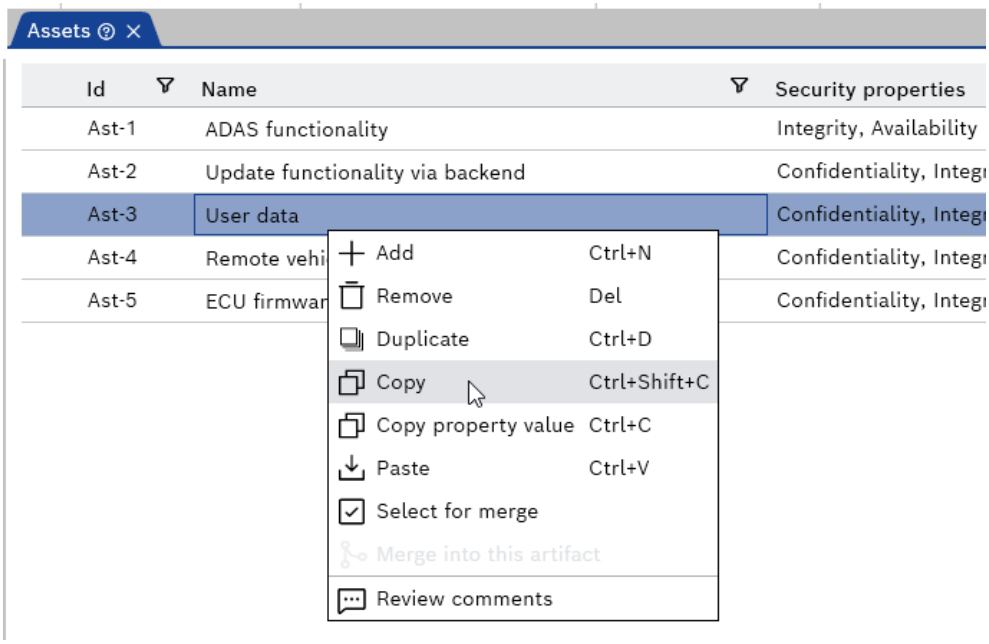


Fig. 7-20: Copying the artifact

The "Please select the linked item types to be copied:" pop-up is displayed.

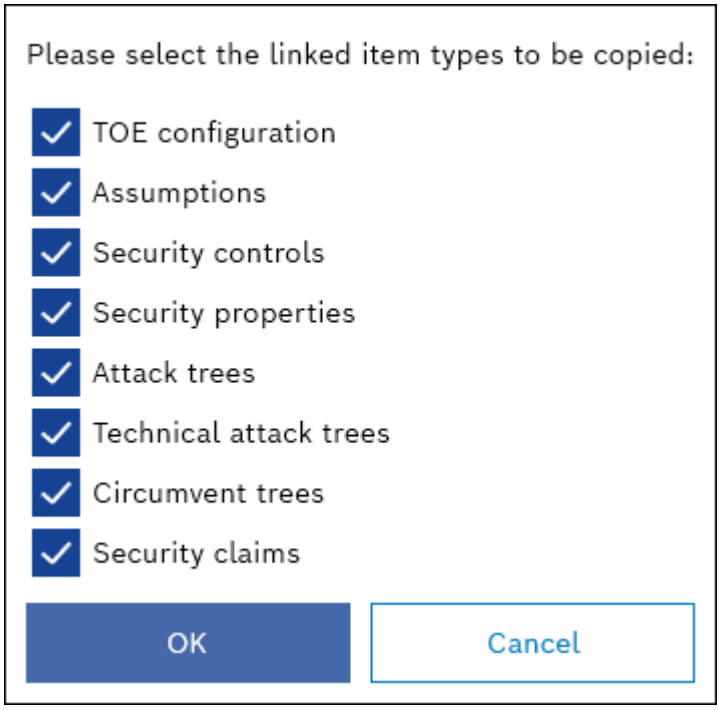


Fig. 7-21: Selecting the linked item types

2. Activate or deactivate the check boxes to copy the linked item types.
3. Click **OK**.
   The selected artifacts are copied.
4. Perform one of the following steps:
   - Right-click and select **Paste** from the context menu.
   - Click **Paste** icon from the "Home" menu.
   - Press CTRL+V.

⇨ The copied artifacts are pasted.

7.12 Generating a Report

7.12.1 Storing Template in a Custom Location

CycurRISK provides the functionality to store your template in a custom location.

You can copy your unzipped template folder into the folder, C:\Users\<UserName>\AppData\Local\ETAS\CycurRisk\Local\Templates. The copied template is automatically added to the "Template" drop-down menu, and you can select it while generating the PDF reports.

Note

The local templates are only available locally and not published on the server for the OU.

7.12.2 Generating a PDF

You can export the analyzed content into PDF format.

To generate a PDF

1. Perform one of the following steps:
   - Click **Generate report** icon on the **Home** menu.
   - Go to the **File** menu > **Generate report**.
   - Press F10.
     The "Generate report" window is displayed.

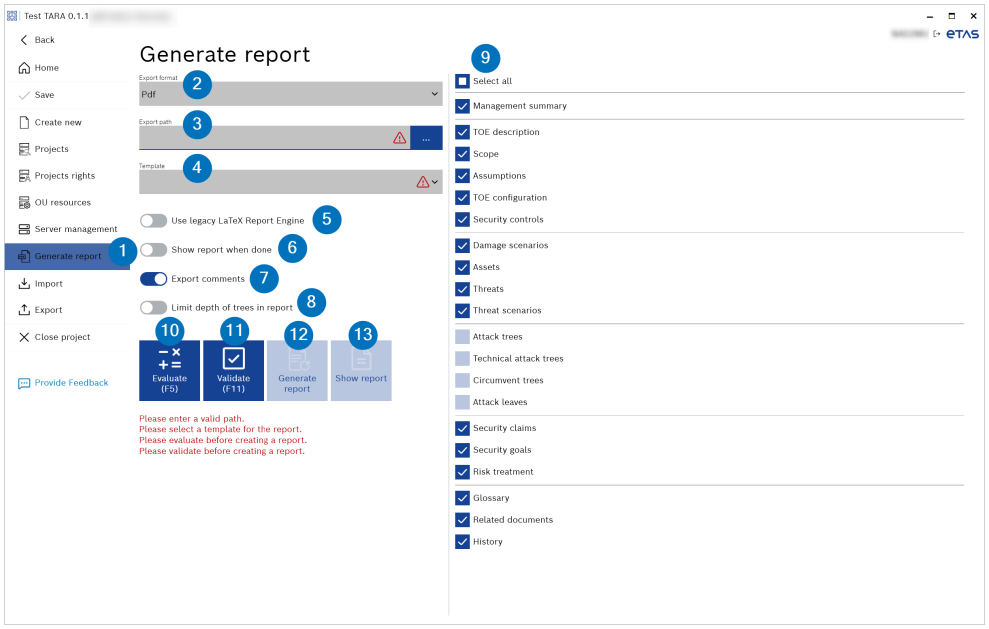


Fig. 7-22: The "Generate report" window - PDF

2. Select **pdf** from the "Export format" drop-down menu.
3. Enter the export path in the "Export path" field or click ... to browse and select it.
4. Select the template from the "Template" drop-down menu.

> **Note**
>
> You can customize the templates, but you must not modify the binding variables. The software uses these variables to fill content, and altering them results in erroneous behavior.

5. Decide whether you want to use legacy LaTeX report engine with the "Use legacy LaTeX Report Engine" toggle button.
   - If enabled, you can select LaTeX templates from the "Template" drop-down menu. It then uses the LaTeX engine to generate the PDF.
   - If disabled, you can select HTML templates from the "Template" drop-down menu. It does not use the LaTeX engine; instead, it uses the the HTML templates with values and convert them to PDF.

6. Decide whether you want to show the report when done with the "Show report when done" toggle button. This step is optional.
7. Decide whether you want to export comments with the "Export comments" toggle button. This step is optional.
8. Decide whether you want to limit depth of trees in report with the "Limit depth of trees in report" toggle button. This step is optional and only applicable for Attack Potential methodology.
9. Activate or deactivate the check boxes to configure the information to include in the report.

> **Note**
>
> You must evaluate and validate the project before generating a PDF report.

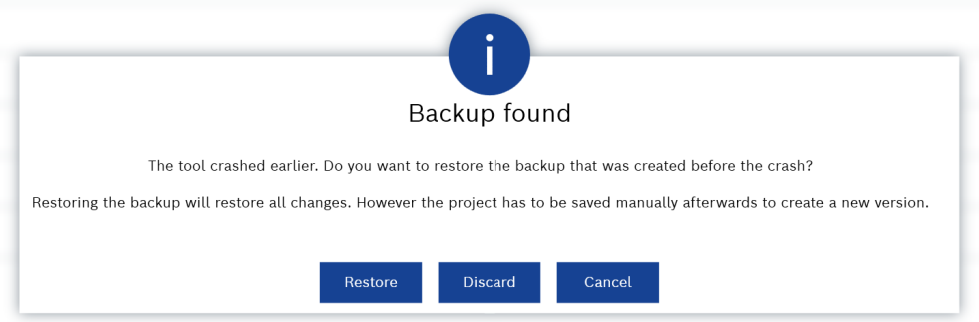
10. Click **Evaluate**.
    The report is evaluated, and the "Generate report" option is enabled.
11. Click **Validate**. It is not mandatory to solve errors and warnings when generating a report. This step is optional.
    The report is validated.
12. Click **Generate report**.
    The report is successfully generated.
13. Click **Show report**, if the "Show report when done" toggle button is not activated in Step 5.

⇨ The report is displayed.

7.13 Restoring a crashed project

The CycurRISK stores data locally on the client at regular intervals. In the event of an unexpected crash, the CycurRISK restores any data not stored on the server after restarting CycurRISK and reopening the project.

The CycurRISK will display the “Backup found” pop-up as shown below.



You can perform the following actions with the backup created before the crash:

- Restore
- Discard
- Cancel

8 Tree Editor

The tree editor features work similarly for creating attack trees, technical attack trees, and circumvent trees.

8.1 Opening the Tree Editor

To open the tree editor

1. Go to the **File** menu > **Attack trees** or **Technical attack trees** or **Circumvent trees**.
   The corresponding tree is opened.

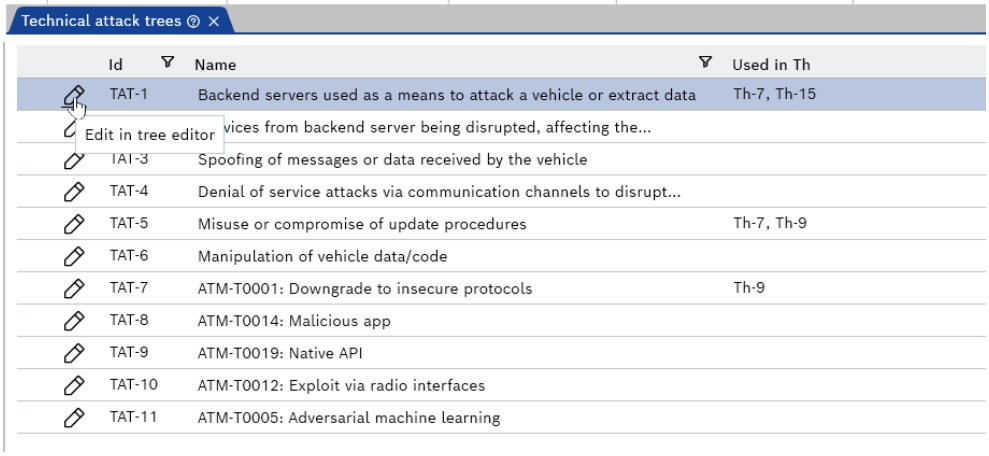


Fig. 8-1: For example - Technical attack trees

2. Click **Edit in tree editor** icon.
   The tree editor is opened.

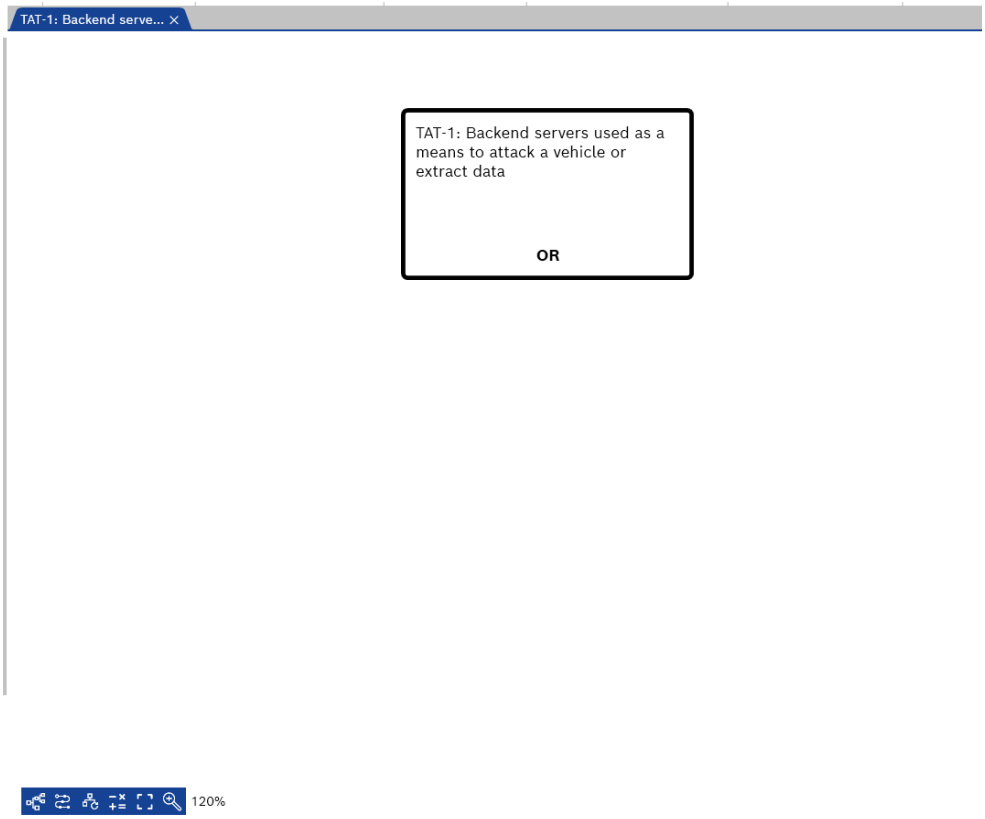


Fig. 8-2: Tree editor window

8.2 Editing the Tree Editor

Once you open a tree in the tree editor, only the root node appears if the trees are not built. The color of the root node is black.

8.2.1 Adding a Node

You can add the Intermediate node, Technical attack tree, Circumvent tree, Attack leaf, and Placeholder node to the tree. There are several ways to add a node to the tree.

To add a node

1. Perform one of the following steps:
   - Go to the **Home** menu › Click **Add** icon.
   - Right-click a node and select **Add node** from the context menu.
   - Press CTRL+N and select a node.
   - Drag and drop a node from the "Tree toolbox."

⇨ The selected node is added to the tree.

8.2.2 Editing the Node Properties

You can click the node shape to select it. The selection is usually shown via a gray color border.

To edit the node properties

1. Double-click the node shape.
   The node goes into the edit mode, and the edit mode is visualized via a blue border.

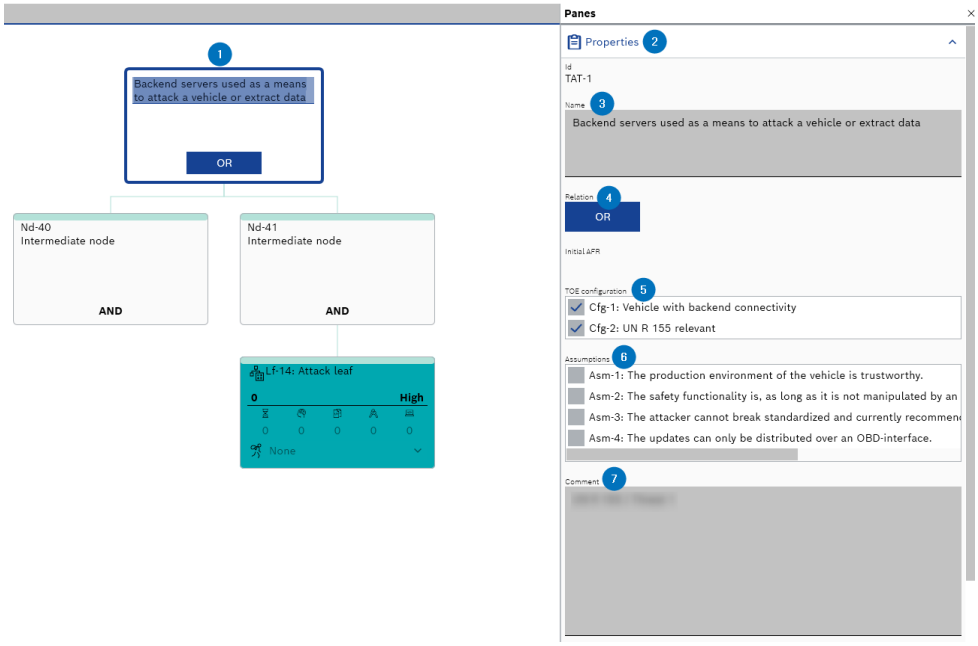


Fig. 8-3: Editing the node properties

2. Go to the **Panes** > **Properties**.
   The "Properties" pane is displayed.
3. Edit the node name in the "Name" field.
4. Click the **Relation** field to change the relation.
   The relation is changed.
5. Enable or disable the check boxes to configure the "TOE configuration" artifacts.
6. Enable or disable the check boxes to configure the "Assumptions" artifacts.
7. Enter or edit the information in the "Comment" field.

⇨ The node properties are edited.

8.2.3 Replacing a Placeholder Node

You can replace the placeholder node with a new TAT, new leaf, or Attack leaves. You can also replace it with an existing technical attack or circumvent tree.

To replace a placeholder node

1. Perform one of the following steps:
   - Drag and drop an artifact (New TAT or leaf, existing technical attack tree or circumvent tree, or Attack leaves) from the "Tree toolbox" onto the placeholder node.
   - Right-click a placeholder node.
     The context menu is displayed.

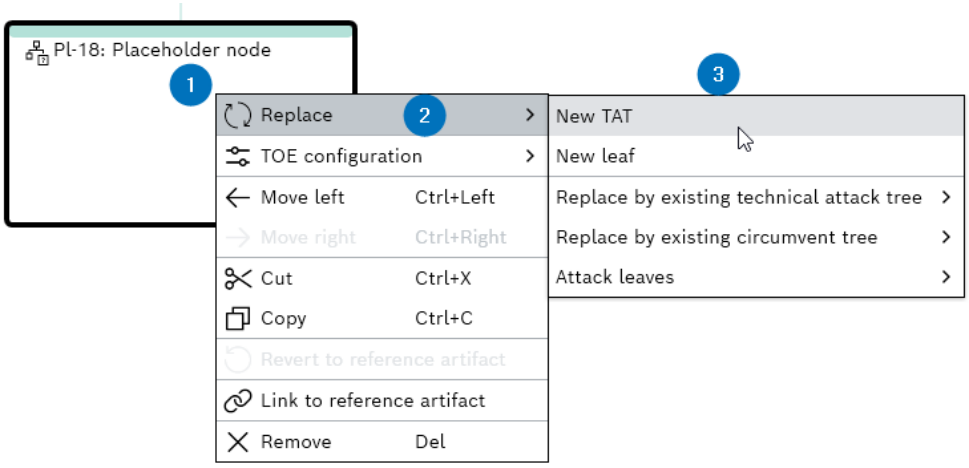


Fig. 8-4: Replacing a placeholder node

2. Click **Replace**.
   The context menu is displayed.
3. Select an artifact node from the list.

⇨ The placeholder node is replaced with the selected artifact node.

8.2.4 Removing a Node

When you remove an intermediate node, the nodes below are also removed. To keep them, drag and drop them to another node before removing them. There are several ways to remove a node from the tree.

To remove a node

1. Perform one of the following steps:
   - Select a node and click **Remove** icon from the **Home** menu.
   - Right-click a node and select **Remove** from the context menu.
   - Select a node and press DELETE.

⇨ The selected node is removed from the tree.

8.2.5 Structuring a Tree

By default, a new node is always added to the right of the existing node. However, you can change the tree structure by dragging and dropping a node to a different node to make a child.

To (Re-)structure a tree

Perform one of the following steps:

- Right-click a node and click **Move left** or **Move right** from the context menu.
- Select a node and press CTRL+LEFT or CTRL+RIGHT.

⇨ The selected node is moved.

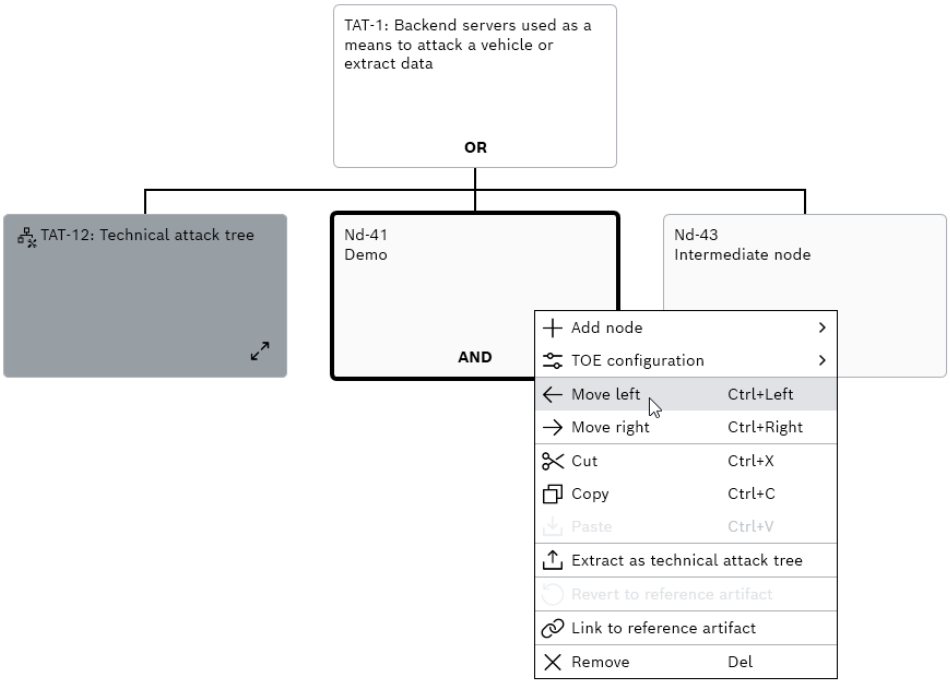


Fig. 8-5: Restructuring a tree

8.2.6 Extracting as Technical Attack Tree

If you require using a subtree in other trees, you can turn this subtree into a technical attack tree.

To extract as technical attack tree

1. Right-click a node.
   The context menu is displayed.

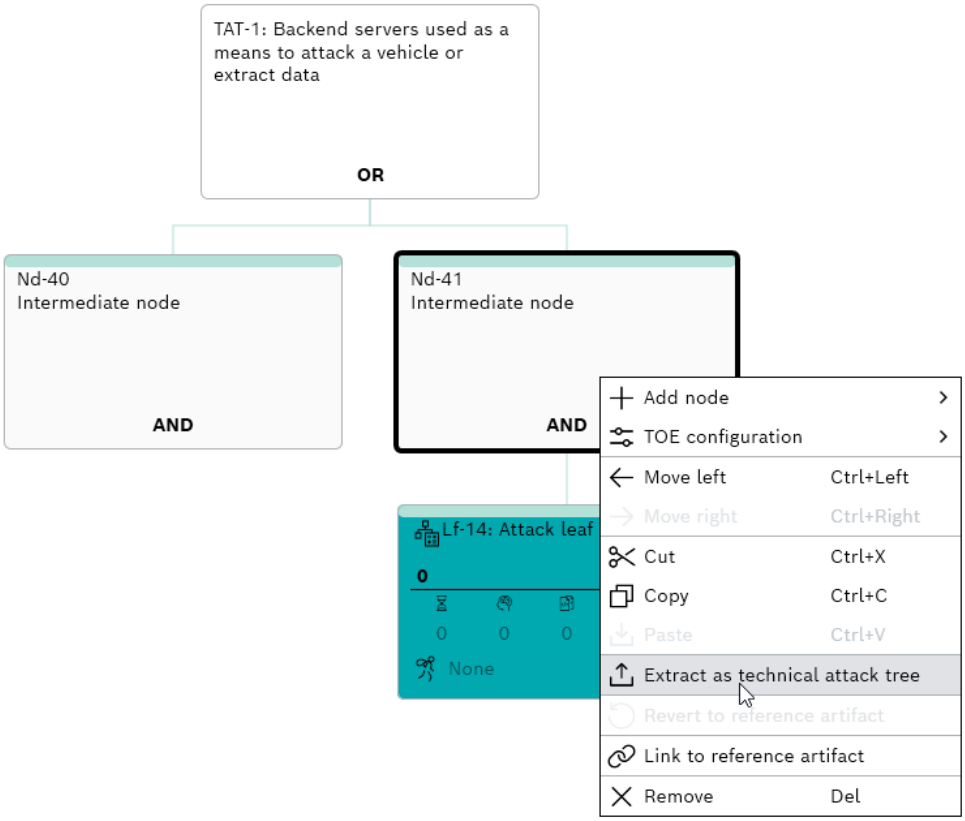


Fig. 8-6: Extracting as technical attack tree

2. Click **Extract as technical attack tree**.

⇨ The subtree is added to the list of technical attack trees as a new technical attack tree and receives an ID.

8.3 Evaluating a Tree

When the tree is structured, you can evaluate it to obtain the initial AFR, the critical path, and residual AFR.

The critical path highlights those leaves (and their path up to the root) that lead to the smallest attack potential sum. Only the leftmost path is highlighted if multiple critical attack paths lead to the same smallest sum. You can click **Show/hide highlighting of critical path** icon from the tree editor window to show or hide the critical path, which is highlighted with a yellow border.

The tree editor offers the "Auto evaluation" function. This function evaluates the project upon every relevant change. By default, it is inactive, but activating it may slow down large the projects.

To evaluate a tree

Perform one of the following steps:

- Go to the **Home** menu > Click **Evaluate** icon.
- Press F5.

➪ The current tree is evaluated.

9 Project References

It is possible to reference one project from another and use artifacts from the referenced project. It allows you to create a hierarchy of projects. This approach is similar to referencing libraries. See Libraries for more information.

Example:

Project A references projects B1, B2, and B3. Projects B1 and B2 each reference a library as shown in figure below.

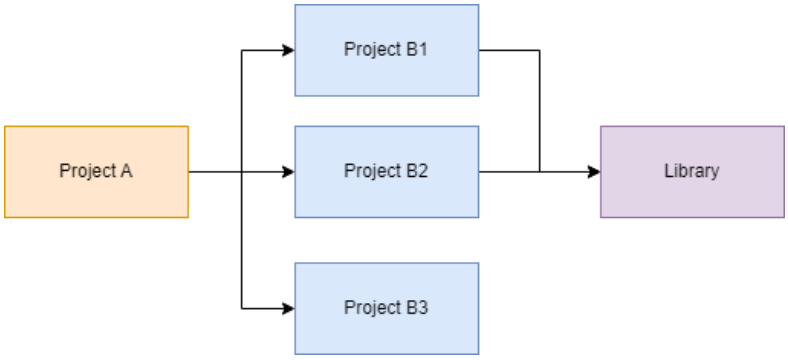


Fig. 9-1: Project references

> **Note**
>
> This feature behaves similarly to the library's feature. Where not explicitly specified, it mirrors the implementation of the library's feature.

The"Referenced projects" pane is located within the side panes, which lists all referenced projects. This pane displays the following properties for each project:

- Number in list
- Name
- Author
- Version
- Methodology
- Last edited
- Organizational unit

This is similar to how all referenced libraries are listed in the “Libraries” pane.

9.1 Adding a New Project Reference

To add a new project reference

1. Perform one of the following steps:

- Go to the **Panes** › **Referenced projects**.
- Go to the "Status" bar and click **Referenced projects** icon.

– Press CTRL+SHIFT+O.
The "Referenced projects" pane is opened.

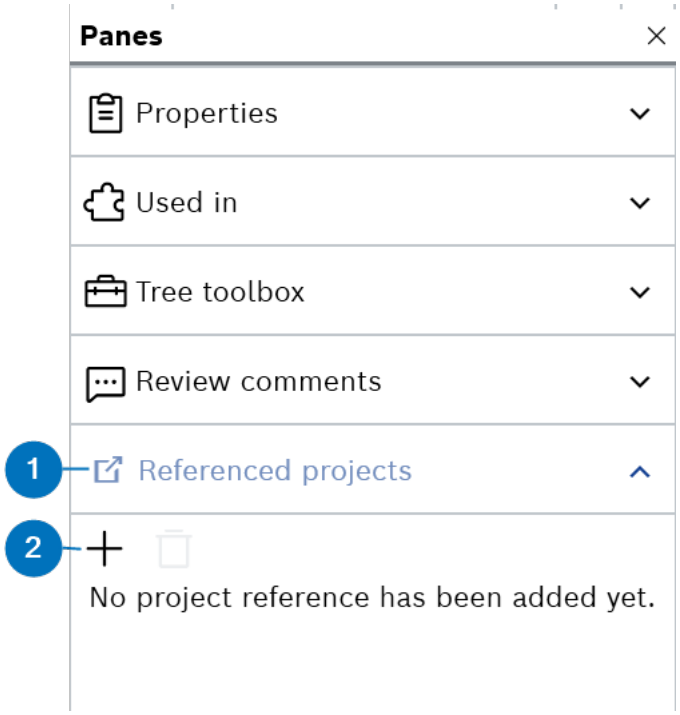


Fig. 9-2: The "Referenced projects" pane

2. Click **Add** icon.
The "Browse referenceable projects" dialog box is displayed.

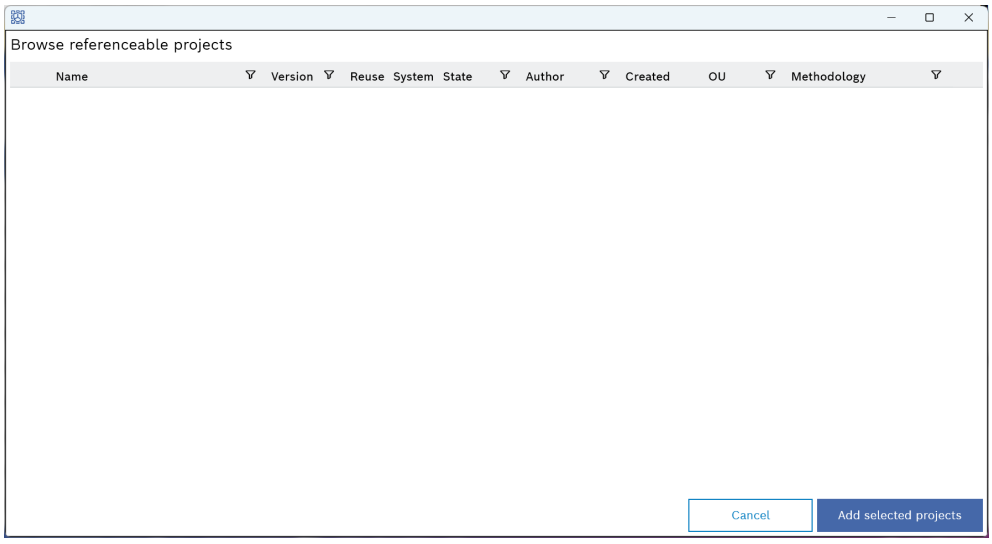


Fig. 9-3: The "Browse referenceable projects" window

> **Note**
>
> The **Add** icon is enabled only if the project has no unsaved changes.

3. Select the projects from the list.

Note

- You can select a project version only if you have read access to it.
- You have read access if the project belongs to an OU that you can access.
- You can select only released project versions. Unlike libraries, you cannot reference unpublished project versions.

4. Click **Add selected projects**.

➪ The selected projects are added to the "Referenced Projects" pane, but no artifacts are imported.

See Including Artifacts from the Referenced Project for more information. It does not matter whether you reference a reuse TARA or a system TARA. The methodology also does not matter, similar to libraries.

9.2 Removing a Project Reference

To remove a project reference

1. Go to the **Panes** > **Referenced projects**.
   The "Referenced projects" pane is opened.

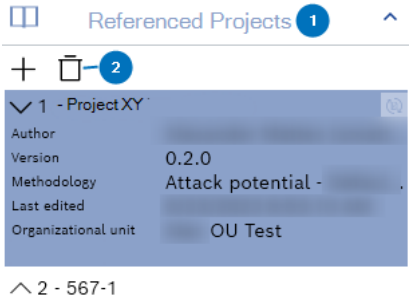


Fig. 9-4: Referenced projects

2. Click the **Remove** icon.

➪ The selected project reference is removed.

9.3 Including Artifacts from the Referenced Project

The CycurRISK displays the "Referenced project artifacts" panel at the bottom of the artifact pages. This panel lists all artifacts from the referenced projects and includes an additional project name column.

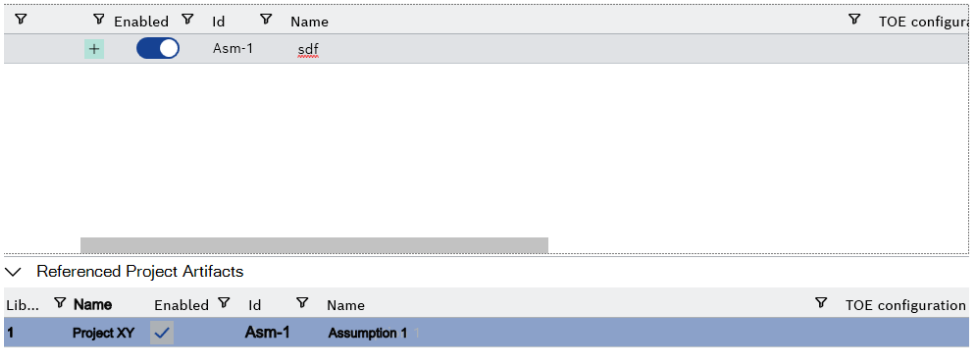


Fig. 9-5: The "Referenced Project Artifacts" window

You can copy artifacts from referenced projects into the current project. When you copy artifacts, the system opens a dialog box where you can select or deselect linked artifact types. Unless specified otherwise, the behavior matches that of libraries.

9.4 Updating a Project Reference

You can update the artifacts that are copied from a referenced project with a newer version.

To update the project reference

1. Go to the **Wizards** menu and click **Update project reference** icon. The wizard then guides you through all artifact pages.
2. You can review and apply the changes.

This behavior is the same as in the “Update Library” wizard. It includes all artifact types, including those not covered by the "Update Library " wizard.

The “Update project reference” wizard supports the following additional features:

- Updates all changes automatically without navigating through all pages.
- Updates all changes on the current page.
- Updates the entire tree structure instead of only the metadata.

10 Libraries

Library projects are handled like normal CycurRISK projects, i.e., TARA, Reuse TARA, and System TARA. The library project has the following differences to the normal projects:

- Libraries can not reference other libraries.
- A library does not contain the following pages:
  - Misuse cases
  - Risks
  - Risk treatment
  - Attack filter
  - Traceability graph
  - Management summary
- A library contains a field in the cockpit to specify keywords to describe the library content.
- The library projects can also be released with placeholder nodes in the attack trees.
- A library can be published.

> **Note**
>
> A user can reference a library even if it is not in a "Released" state, provided the same user created the library and references it within the project.

10.1 Uploading .tra Files as Library Project

You can change the project type from .tra to .tralib and upload it as a library project to the server.

To change the project type from .tra to .tralib

1. Select the .tra file and right-click.
   The context menu is displayed.
2. Click **7-zip** › **Extract to "projectname**."
   The file is extracted, and a new folder with the project name is created.
3. Open the newly created folder.
4. Open the CycurRISK.json file in the Visual Studio Code application.
5. Change "ProjectType" from 0 to 1 and save it.
6. Mark all the files included in the above newly created folder and right-click.
   The context menu is displayed.
7. Click **7-zip** › **Add to "ProjectName**."
   A new zip folder (file type: ".zip") has been created.

8. Rename the file or change the file type to ".tralib."

➪ The new library project is created.

10.2 Adding Libraries to a Project

To add libraries to a project

1. Perform one of the following steps:

– Go to the **Panes** > **Libraries**.

– Go to the "Status" bar and click **Libraries** icon.

– Press CTRL+SHIFT+L

The "Libraries" pane is opened.

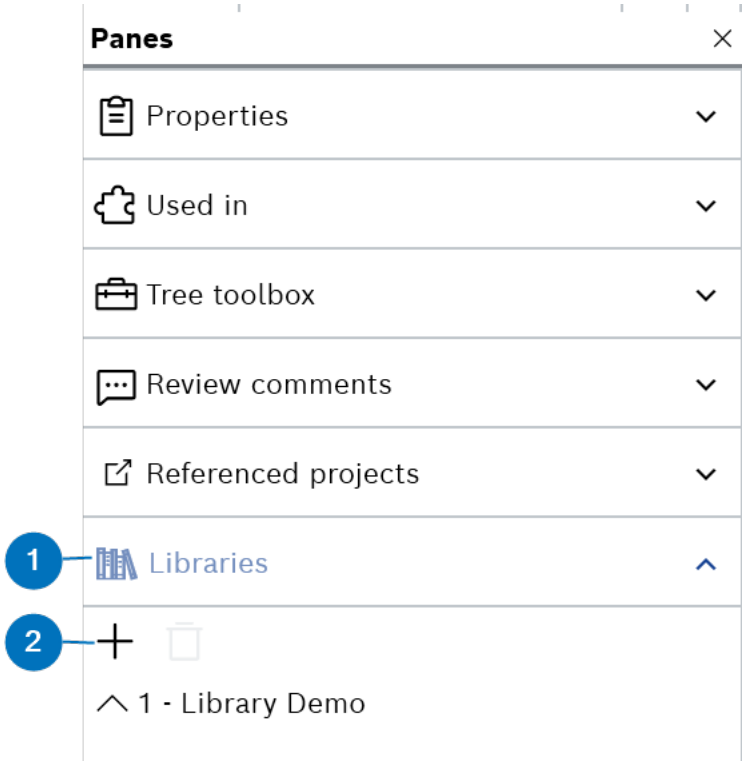


Fig. 10-1: The "Libraries" pane

2. Click **Add** icon.

The "Browse available libraries" dialog box is displayed.

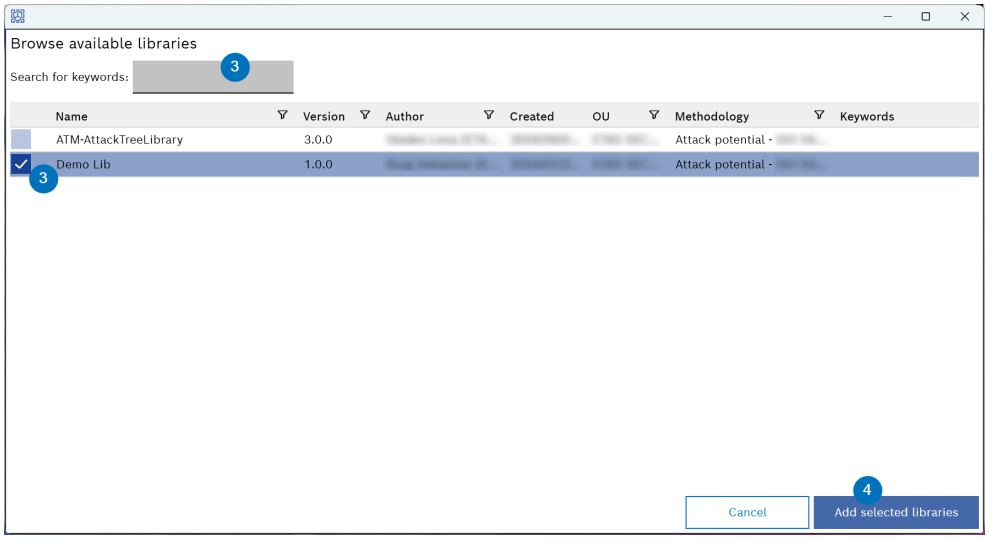


Fig. 10-2: The "Browse available libraries" window

3. Select the libraries from the list.
   or
   Search and select the available libraries with keywords from the "Search for keywords" field.
4. Click **Add selected libraries**.

⇨ The selected library is added to the "Libraries" pane and "Cockpit" page.

10.3 Removing Libraries from a Project

To remove libraries from a project

1. Go to the **Panes** > **Libraries**.
   The "Libraries" pane is opened.

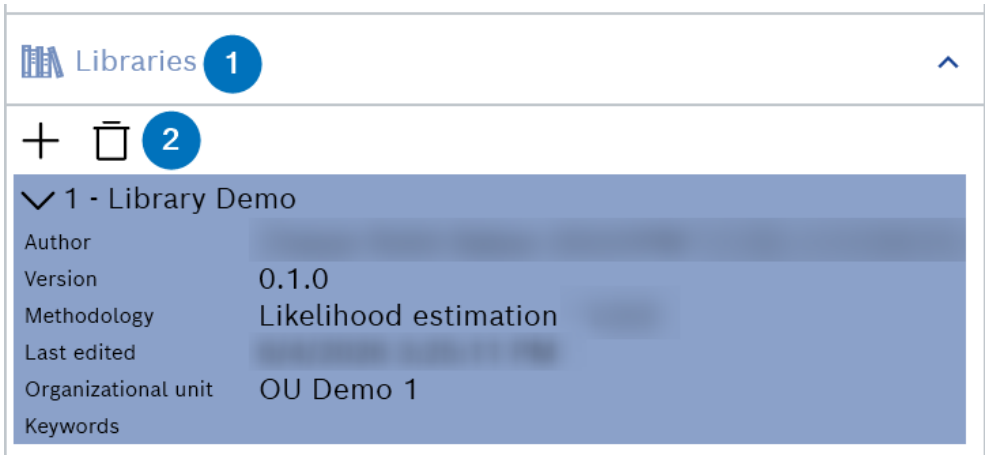


Fig. 10-3: Libraries

2. Click **Remove** icon.

⇨ The selected library is removed.

10.4 Updating a Library

You can update the artifacts that are copied from a library with a newer version.

To update a library

1. Go to the **Wizards** menu and click **Update library** icon.
   The “Update library" window appears.

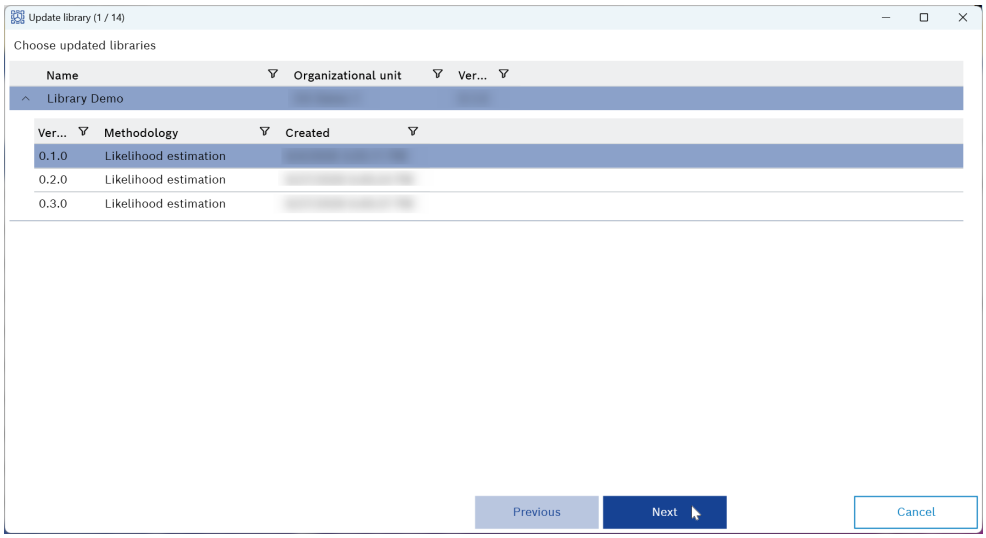


Fig. 10-4: The "Update library" window

2. Select the updated library version from the list.
3. Click **Next**.
   The “Update all artifacts?” pop-up appears.

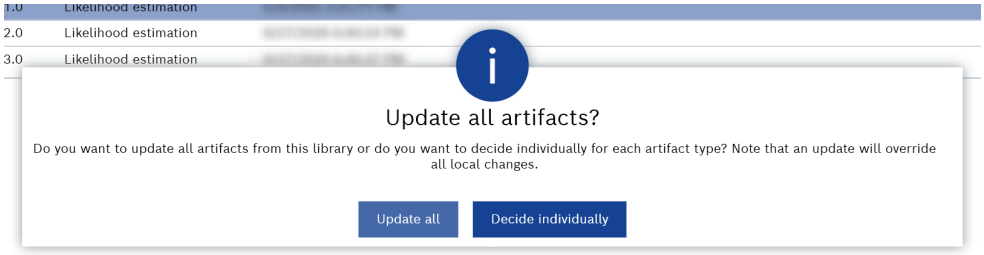


Fig. 10-5: The "Update all artifacts?" pop-up

4. Decide whether you want to update all or individual artifacts at once.

– Click **Update all** to update all artifacts from this library.
  The library update is finished.

– Click **Decide individually** to update each artifact individually.
  The wizard guides you through all artifact pages, where you can review and apply changes and click **Finish**

⇨ The library update is finished and the changes are applied.

10.5 Publishing a Library

You can publish a library project to make it available to other users in the organizational unit. They can embed this library into their project and use these artifacts for their project.

You can only publish the library when the project status is set to "Released " in the "Projects" window.

> **Note**
>
> You need the "Library publisher" role to publish libraries.

To publish a library project

1. Go to the **File** menu > **Projects**.
   The "Projects" window is displayed.
2. Select the "Released" state project.
3. Click **Publish**.

⇨ The selected project is published.

11 Navigation

11.1 Open Multiple Tabs

To open multiple tabs at the same time

1. Click one item in the Project Explorer.
   The selected item will open in a new tab.
2. Select another item in the project explorer and right-click.
   A context menu is displayed.
3. Click **Open in new tab in left view**.

➪ The selected item will open in another new tab.

> **Note**
>
> The selected item can only open in one tab; multiple instances of the selected item are not possible.

11.2 Side-by-Side View

To open two tabs alongside each other

1. Click one item in the Project Explorer.
   The selected item will open in a new tab.
2. Select another item in the project explorer and right-click.
   A context menu is displayed.
3. Click **Open in new tab in right view**.

➪ The selected item will open alongside the first opened item tab.

11.3 Tab Undocking or Docking

To undock the tabs:

1. Click and hold on to the tab.
2. Drag the tab away from its current position.

➪ The selected tab is undocked from the tab.

or

1. Right-click an item in the project explorer.
   A context menu is displayed.
2. Click **Open in new window**.

➪ The selected item is opened in a new window.

To dock the tabs:

1. Drag the undocked tab to the tab bar (left or right view).

⇨ The undocked tab is docked to the tab bar.

or

1. Right-click the undocked tab.
   A context menu is displayed.
2. Select "Move to left view" or "Move to right view."

⇨ The undocked tab is docked to the tab bar.

11.4 Internal Links

You can follow internal and external links (including links in the errors/warnings window) via CTRL+CLICK. For example, you can CTRL+CLICK an artifact to jump to where it is defined.

When the keyboard focus is set over an artifact link, you can follow the link with the hotkey, ALT+ENTER.

11.5 Navigate Search Results

Navigating search results is possible with the hotkeys, F3 (Forward) and SHIFT+F3 (Backward).

12 TARA Methodologies

CycurRISK currently offers three methodologies for creating a project.

A. Likelihood estimation
B. Attack potential
C. CVSS

> **Note**
>
> CycurRISK provides only the above three methodologies. However, you can modify methodology attributes.

12.1 Likelihood Estimation

Likelihood estimation provides a simplified methodology to evaluate the likelihood of a risk in CycurRISK. This methodology uses one likelihood dimension to perform the evaluation. You can use this approach when you require a clear and straightforward assessment.

This method estimates a threats initial and residual AFR as one of the four values: highly likely, likely, less likely, or unlikely. These values are then translated to an AFR, as shown in Tab. 12-1.

The likelihood estimation method does not use any attack trees but gives textual descriptions of the considered attack paths. Likelihood estimation is considered less rigorous than the attack potential method.

Likelihood	**AFR**
highly likely	high
likely	medium
less likely	low
unlikely	very low

Tab. 12-1: Example - Mapping of likelihood to AFR

12.2 Attack Potential

You can use this methodology to perform a detailed attack-feasibility-oriented assessment. You can configure this methodology to use a single or multi-impact category, depending on the assessment needs.

- Single impact category
  It has one impact category per damage scenario for the assessment.
- Multi-impact category
  It has multiple impact categories per damage scenario for the assessment.

This method analyzes attack paths using attack trees and rates them with a so-called attack potential, which is subsequently translated to an Attack Feasibility Rating (AFR). The attack potential is evaluated based on factors such as:

- Elapsed time
- Specialist expertise
- Knowledge of the item or component
- Window of opportunity
- Equipment

The difference between the Likelihood Estimation and Attack Potential methodologies is how a threat AFR is determined.

.

12.3 CVSS

A methodology configuration is based on CVSS-style likelihood factors and impact categories.

The methodology evaluates likelihood using the following categories:

- Attack Vector
- Attack Complexity
- Privileges Required
- User Interaction

13 Configuring TARA Methodology

You can configure the methodology to meet your specific requirements and test the functionality effectively.

> **Note**
>
> The report generation will works smoothly only if the changes in the methodology are also made to the LaTeX and HTML templates.

13.1 General Constraints

13.1.1 ID Handling

Description:

Define how identifiers are handled in the methodology configuration.

Requirements:

- IDs must be unique, stable, and deterministic.
- Do not use random IDs for elements referenced in:
  - Score mappings
  - Matrices
  - Categories
  - Attacker types
  - Imported project data

Effect:

Enables CycurRISK to correctly map categories, scores, and risks.

Constraints:

- Changing IDs without updating references may break calculations and imports.
- This is critical when objects are cross-referenced across multiple arrays.

13.2 Common JSON Structure and its Meaning

13.2.1 MethodologyDataHeader

Type: Object

Description: Contains metadata about the methodology configuration used such as the methodology name, type, and version.

Possible values:

Keys	Type	Description	Examples
MethodologyKey	String	A unique identifier for the methodology	Attack potential - ISO SAE 21434 2021 Annex G - External
MethodologyType	String	The type of methodology • AP for Attack Potential • LE for Likelihood Estimation • CVSS for CVSS-based methodology	AP, LE, CVSS
Version	String	The version of the methodology	1.0.0, 1.1.0, 1.2.0

Effect:

- Determines the calculation and display logic used by CycurRISK.
- Supports version traceability.

Constraints:

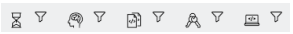
- MethodologyKey should be stable and unique.
- MethodologyType must match supported methodology (LE, AP, and CVSS).
- Should not change the methodology casually; switching a project to a different methodology requires a proper methodology mapping.
- Version should be updated when the methodology content changes.

13.2.2 LikelihoodCategories

Type: Array of Objects

Description: A list of categories used to calculate Likelihood or Attack Potential or CVSS in CycurRISK. Each entry defines one scoring dimension, such as attack vector, expertise, knowledge, or equipment.

Possible values:

Keys	Type	Description	Examples
Id	Integer	A unique identifier for the likelihood category (consistent sequence numbering)	Integer values such as 1, 2, 3, 4, 5
Name	String	The full name of the likelihood category	— LE Likelihood — AP • Elapsed time • Specialist expertise • Knowledge of the item or component • Window of opportunity • Equipment — CVSS • Attack Vector • Attack Complexity • Privileges Required • User Interaction
Description	String or Null	Description of the likelihood category	String or null
ShortName	String	A short representation of the category	— AP T, Ex, K, WoO, Eq — CVSS V, C, P, U
Icon	String	A code representing an icon	Icon codes such as e19f, e2ff, e419, e42e, e11e, e5b7, e4bb, e280 Icon display of AP in UI  Icon display of CVSS in UI 

Effect:

- Defines the factors used for scoring Likelihood, Attack Potential, or CVSS.
- Controls the labels displayed in the CycurRISK UI.
- Supports scoring and display behavior.

Constraints:

- IDs must be unique and stable.
- Category names must match the selected methodology.
- ShortName should be short and unambiguous.
- Icon must be a valid icon code recognized by CycurRISK.

13.2.3 LikelihoodRanges

Type: Array of Objects

Description: A list of ranges that define the final qualitative result after scoring Likelihood or Attack Potential or CVSS.

Possible values:

Keys	Type	Description	Examples
Id	Integer	A unique identifier for the likelihood range	Integer values such as 1, 2, 3, 4
Name	String	The name of the likelihood range	High, Medium, Low, Very low
Description	String or Null	A description of the range	String or null
NumericLowerLimit	Integer	The lower score limit for the range	Integer values such as, Name: Numer-icLowerLimit - Numer-icUpperLimit High: 0 - 13 Medium: 14 - 19 Low: 20- 24 Very low: 25- 1000
NumericUpperLimit	Integer	The upper score limit for the range	
ColorCode	String	A color code asso-ciated with the range	High: #FF00A8B0 High Medium: #FF40BEC4 Medium Low: #FF7FD3D7 Low Very Low: #FFBFE9EB Very low

Effect:

- Maps the calculated score to a final likelihood result.
- Drives the color and label shown in CycurRISK.

Constraints:

- Ranges must not overlap.
- All relevant score values must fall into one of the defined ranges.
- Color codes must be valid hex values.
- Range values must be consistent with the selected methodology.

13.2.4 LikelihoodScores

Type:

Array of Objects

Description:

A list of numeric scores for each likelihood category.

Possible values:

Keys	Type	Description	Examples
CategoryId	Integer	ID of the likelihood category	Must reference LikelihoodCategories.Id

Keys	Type	Description	Examples
Name	String	Name of the likelihood score	LE — Likelihood • Highly likely • Likely • Less likely • Unlikely
			AP — Elapsed time • < = one day • < = one week • < = two weeks • < = one month • < = two months • < = three months • < = four months • < = five months • < = six months • > six months • Infeasible
			— Specialist expertise • Layman • Proficient • Expert • Multiple experts • Infeasible
			— Knowledge of the item or component • Public • Restricted • Confidential • Strictly Confidential • Infeasible

Keys	Type	Description	Examples
			— Window of opportunity • Remote and unlimited • Remote and limited • Easy Physical acces • Medium Physical access • Difficult Physical access • Infeasible
			— Equipment • Standard • Specialized • Bespoke • Multi bespoke • Infeasible
			CVSS — Attack Vector • Network • Adjacent • Local • Physical
			— Attack Complexity • Low • High
			— Privileges Required • None • Low • High
			— User Interaction • None • Required

Keys	Type	Description	Examples
Value	Integer	Numeric score value of Name	LE — Likelihood • Highly likely = 0 • Likely = 1 • Less likely = 2 • Unlikely = 3
			AP — Elapsed time • < = one day = 0 • < = one week = 1 • < = two weeks = 2 • < = one month = 4 • .....
			CVSS — Attack Vector • Network = 85 • Adjacent = 62 • Local = 55 • Physical = 20 — .....
Description	String or Null	Description of the score	String or null

Effect:

- Used to calculate the final score for the methodology.
- The result based on AP or CVSS formula is later mapped to a range.

Constraints:

- CategoryId must refer to a valid category.
- Values must match the selected methodology.
- Score definitions must not conflict within the same methodology.

13.2.5 AttackerTypes

Type: Array of Objects

Description: A list of attacker profiles used to support Attack Potential or Likelihood Estimation or CVSS. Each attacker type describes a typical attacker capability and may predefine scoring assumptions.

Possible values:

Keys	Type	Description	Example
Id	Integer	A unique identifier for the attacker type (consistent sequence numbering)	Integer values such as 0, 1, 2, 3, 4, 5
Name	String	The name of the attacker type	None, Remote script kiddy, Local layman, Professional workshop, Advanced attacker, Expert attacker
ShortName	String or Null	Short representation of the attacker type	String or null
Definition	String	Detailed attacker profile description	Free text
Prerequisites	String	Conditions required for this attacker type	Free text
Examples	String	Example persons or groups matching this type	Free text
Scores	Object	Score mapping for category IDs	Object with numeric values

Effect:

- Defines attacker profiles used in the methodology.
- Can predefine scores for categories such as expertise, knowledge, and equipment.
- Supports consistent and repeatable scoring.

Constraints:

- IDs must be unique and stable.
- Scores must reference valid likelihood category IDs.
- Attacker type definitions must align with the selected methodology.

13.2.6 MultiCategoryImpact

Type: Boolean

Description: Indicates whether multiple impact categories considered for a single damage scenario.

Possible values:

- true
- false

Effect:

- If true, a damage scenario can use multiple impact categories.
- If false, only single impact category is intended.

Constraints:

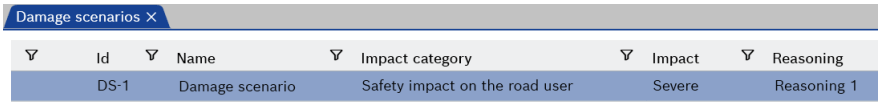
- If enabled, CycurRISK must support multiple impact categories in the UI and calculation flow.
- For more complicated changes such as multi-impact, see the example below displaying the effect in CycurRISK.

Example:

– Single-impact categories
  - Methodology configuration

```
"MultiCategoryImpact": false,
"ImpactCategories": [
  {
    "Id": 0,
    "Name": "",
    "Description": null,
    "ShortName": null,
    "Icon": null
  },
  {
    "Id": 1,
    "Name": "Safety impact on the road user",
    "Description": null,
    "ShortName": null,
    "Icon": null
  },
  {
    "Id": 2,
    "Name": "Financial impact on the road user",
    "Description": null,
    "ShortName": null,
    "Icon": null
  },
  {
    "Id": 3,
    "Name": "Operational impact on the road user",
    "Description": null,
    "ShortName": null,
    "Icon": null
  },
```

  - Impact categories in Damage scenarios

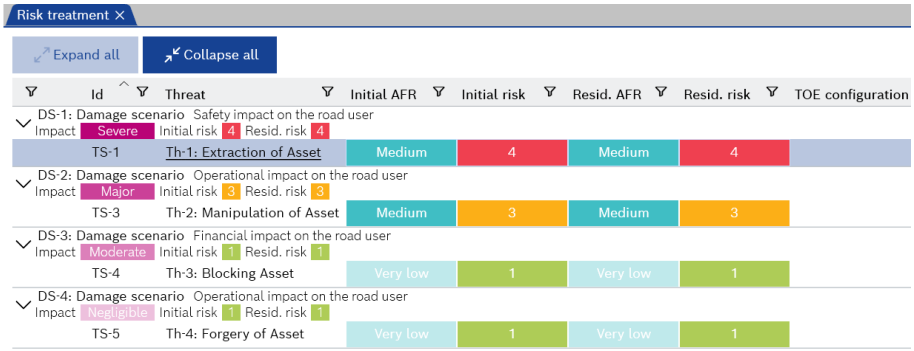


– Multi-impact categories
  - Methodology configuration

```
"MultiCategoryImpact": true,
"ImpactCategories": [
  {
    "Id": 1,
    "Name": "Safety",
    "Description": null,
    "ShortName": null,
    "Icon": null
  },
  {
    "Id": 2,
    "Name": "Financial",
    "Description": null,
    "ShortName": null,
    "Icon": null
  },
  {
    "Id": 3,
    "Name": "Operational",
    "Description": null,
    "ShortName": null,
    "Icon": null
  },
  {
    "Id": 4,
    "Name": "Privacy and Legislation",
    "Description": null,
    "ShortName": null,
    "Icon": null
  }
],
```

  - Impact categories in Damage scenarios

– Resulting impact score or risk output



13.2.7 ImpactCategories

Type: Array of Objects

Description: A list of categories used for impact assessment. Each category represents one consequence dimension, such as safety, financial, operational, privacy, or company impact.

Possible values:

Keys	Type	Description	Example
Id	Integer	A unique identifier for the impact category (consistent sequence numbering)	Integer values such as 0, 1, 2, 3, 4, 5, 6
Name	String	The full name of the impact category	Single-impact category: – Safety impact on the road user – Financial impact on the road user – Operational impact on the road user – Privacy impact on the road user – Financial impact on company – Operational impact on company Multi-impact category, typically: – Safety – Financial – Operational – Privacy – Legislation
Description	String or Null	Description of the impact category	String or null
ShortName	String or Null	Short representation of the impact category	String or null
Icon	String or Null	Icon code for the category	String or null

Effect:

- Defines which impact dimensions are available for evaluation.
- Determines what can be rated for each damage scenario.

Constraints :

- Category set must match the methodology type.
- If MultiCategoryImpact = true, multiple categories may be selected for one damage scenario.
- Category names should remain meaningful and consistent.

13.2.8 ImpactRanges

Type: Array of Objects

Description: A list of ranges used to classify impact severity levels.

Possible values:

Keys	Type	Description	Example
Id	Integer	A unique identifier for the impact range (consistent sequence numbering)	Integer values such as 1, 2, 3, 4
Name	String	The impact severity name	Negligible, Moderate, Major, Severe
Description	String or Null	Description of the impact range	String or null
NumericValue	Integer	Numeric value for the impact	0, 1, 2, 3
ColorCode	String	Color code for the range	#FFEDC0DD: Negligible #FFDC80BA: Moderate #FFCB4198: Major #FFB90276: Severe

Effect:

- Defines the severity classes for impact scoring.
- Used to classify each impact category.

Constraints:

- Numeric values must match the selected methodology.
- Range names must be consistent and meaningful.
- Color codes must be valid and consistent.

13.2.9 ImpactScores

Type:

Array of Objects

Description:

A list of numeric scores for each impact category.

Possible values:

Keys	Type	Description	Example
CategoryId	Integer	ID of the impact category	Must reference ImpactCategories.Id
Name	String	Impact score name	Negligible, Moderate, Major, Severe
Value	Integer	Numeric impact score	Standard: 0, 1, 2, 3
Description	String or Null	Description of the impact score	String or null

Effect:

- Used to determine the severity of each impact category.
- Supports final impact classification and risk determination.

Constraints:

- CategoryId must refer to a valid impact category.
- The numeric values must align with the selected methodology.
- When multi-impact is enabled, each selected category must be scored consistently.

13.2.10 SecurityProperties

Type: Array of Objects

Description: A list of security properties used for threat modeling and scenario classification.

Possible values:

Keys	Type	Description	Example
Value	Integer	Numeric value representing the security property	0 to 7
Name	String	Name of the security property	Confidentiality, Integrity, Availability, Authenticity, Correctness, Freshness, Authorization, Non-repudiation
PrefixForThreat	String	Prefix used to describe threats related to the property	Extraction of, Manipulation of, Blocking, Forgery of, Invalidation of, Replay of, Unauthorized access to, Repudiation of

Effect:

- Controls naming and classification of threat scenarios.
- Helps express the type of security property that may be compromised.

Constraints:

- For ISO/SAE 21434-oriented use, the primary focus shall be:
  - Confidentiality
  - Integrity
  - Availability
- Additional properties should be used only where necessary.

Example:

- Security properties in Assets

Assets

Id	Name	Security properties	TOE configuration
Ast-1	Asset	Confidentiality	
Ast-2	Asset	Integrity	
Ast-3	Asset	Availability	
Ast-4	Asset	Authenticity	
Ast-5	Asset	Correctness	
Ast-6	Asset	Freshness	
Ast-7	Asset	Authorization	
Ast-8	Asset	Non-repudiation	

- Name in Threats (PrefixForThreat)

Threats

Id	Name	Damage scenarios	TOE configuration
Th-1	Extraction of Asset	DS-1	
Th-5	Manipulation of Asset	DS-2	
Th-6	Blocking Asset	DS-3	
Th-7	Forgery of Asset	DS-4	
Th-8	Invalidation of Asset	DS-1	
Th-9	Replay of Asset	DS-2	
Th-10	Unauthorized access to Asset	DS-3	
Th-11	Repudiation of Asset	DS-4	

13.2.11 SecurityRisks

Type: Array of Objects

Description: A list of security risks.

Possible values:

Keys	Type	Description	Example
Id	Integer	A unique identifier for the risk level (consistent sequence numbering)	Integer values such as, 1, 2, 3, 4, 5
Value	Integer	Numeric representation of the risk severity	Example values 1 to 5
Name	String	Risk level name	Very low, Low, Medium, High, Very high
ColorCode	String	Color for the risk level	#FFAECC57: 1 #FFFDD78B: 2 #FFFCAF17: 3 #FFEF4050: 4 #FFB00010: 5

Effect :

- Represents the final risk result after combining impact and Likelihood or Attack feasibility.

Constraints:

- Risk IDs and values must match the configured matrix.
- Color codes must be valid hex values.
- Risk names must align with the methodology.

13.2.12 SecurityRiskMatrix

Type: Array of Objects

Description: A matrix that links impact ranges, likelihood ranges, and final risk classes.

Possible values:

Keys	Type	Description	Example
ImpactRangeId	Integer	ID of the associated impact range	Integer referencing ImpactRanges.Id
LikelihoodRangeId	Integer	ID of the associated likelihood range	Integer referencing LikelihoodRanges.Id
SecurityRiskId	Integer	ID of the associated security risk	Integer referencing SecurityRisks.Id

Effect:

- Determines the final risk result from impact and likelihood.

Constraints:

- All referenced IDs must exist.
- The matrix must cover all intended combinations.
- IDs must remain stable to avoid broken mappings.

13.2.13 ResponsibleDefaultValues

Type:

Array of Strings

Description:

A list of default values related to responsibility.

Possible values:

- Bosch
- Customer
- Supplier

Effect:

- Defines default responsibility ownership values.

Constraints:

- Shall contain only valid organizational values.
- This is typically a workflow attribute, not a scoring attribute.

13.2.14 ExtendedTreatments

Type:

Array of Objects

Description:

A list of additional treatment options that can be used in the methodology.

Possible values:

Keys	Type	Description	Example
Id	Integer	A unique identifier for the treatment	Integer values such as 1
Name	String	The treatment name	

Effect

- Adds additional risk treatment options.

Constraints

- IDs must be unique and stable.
- Only use if supported by the methodology and process.

14 Troubleshooting

This chapter describes some useful troubleshooting hints that might be helpful while working with CycurRISK.

14.1 Report Engine Not Working Even Though All Installation Steps Executed

In such a case, verify that the environment variable CYCURRISK_PDF_LATEX contains the path to the pdflatex.exe file given during installation.

For example, "C:\TCC\Tools\miktex\21.6_WIN64\-texmfs\install\miktex\bin\x64\pdflatex.exe."

If it does not, configure it manually.

> **Note**
>
> Make sure your LateX packages are complete and updated.

15 Contact Information

Technical Support

For details of your local sales office as well as your local technical support team and product hotlines, take a look at the ETAS website:

www.etas.com/hotlines

ETAS offers trainings for its products:

www.etas.com/academy

ETAS Headquarters

ETAS GmbH		
Borsigstraße 24	Phone:	+49 711 3423-0
70469 Stuttgart	Fax:	+49 711 3423-2106
Germany	Internet:	www.etas.com

16 Glossary

A

AFR

Attack Feasibility Rating

AP

Attack Potential

API

Application Programming Interface

B

BU

Business Unit

C

CSV

Comma-Separated Values - The file format stores the data in a tabular format, with values within each row are separated by commas.

CVSS

Common Vulnerability Scoring System

E

ETAS

Empowering Tomorrow's Automotive Software

G

GUI

Graphical User Interface

H

HW

Hardware

I

ID

Identification or Identity Document

ISO

International Organization for Standardization

K

KIR

Known Issue Reports - For severe Problem Reports which occur after a release, ETAS has introduced the Known Issue Report to inform affected customer immediately. The current Known Issues of former versions can be found on the ETAS website: www.etas.com/kir

L

LE

Likelihood Estimation

O

OEM

Original Equipment Manufacturer

OS

Operating System

P

PC

Personal Computer

PDF

Portable Document Format

PII

Personally Identifiable Information

R

RRA

Residual Risk Analysis

RTF

Rich Text Format

S

SoS

System of Systems

SW

Software

T

TARA

Threat Analysis and Risk Assessment

TAT

Technical Attack Trees

TCL

Tool Confidence Level

TOE

Target of Evaluation

U

UI

User Interface

17 Index

C

E