FucyTech Tool

Table of Contents

1. Introduction

1.1 What is the TARA Tool?

The **TARA (Threat Analysis and Risk Assessment) Tool** by **Fucytech** is a powerful software solution designed to help organizations systematically assess and manage risks within their systems. It provides a comprehensive framework for:

- Identifying potential threats
- Evaluating their impact
- Developing mitigation strategies

Designed with a focus on automotive cybersecurity, TARA supports compliance with **ISO 21434** standards, helping organizations strengthen system security and reduce vulnerabilities throughout the development lifecycle.

1.2 Purpose of the Tool

The core purpose of the **TARA Tool** is to simplify and automate the risk management process, empowering organizations to take a proactive approach to cybersecurity. It enables teams to:

- Identify threats early
- Assess the severity and impact of risks
- Implement effective countermeasures
- Document compliance with **ISO 21434** requirements

By streamlining these processes, TARA enhances **security**, **reliability**, and **regulatory compliance**, making it an essential tool for teams managing **complex systems** or **critical infrastructure**—especially within the **automotive sector**, where ISO 21434 compliance is increasingly critical.

1.3 ISO 21434 Compliance Overview

ISO/SAE 21434 – *"Road Vehicles — Cybersecurity Engineering"* – defines a comprehensive framework for managing cybersecurity risks throughout the **automotive product lifecycle**.

The **FucyTech TARA Tool** is specifically designed to support and streamline compliance with this standard by:

- Providing structured workflows aligned with **ISO 21434 clauses**
- Supporting the four key risk assessment factors: **threat scenario**, **impact**, **attack path**, and **feasibility**
- Enabling thorough documentation of required cybersecurity activities
- Facilitating collaboration among stakeholders across the **automotive supply chain**
- Supporting cybersecurity efforts in both **development** and **post-production** phases

By integrating these capabilities, the TARA Tool helps organizations meet **ISO 21434** requirements efficiently, enhancing both the **effectiveness** and **traceability** of their cybersecurity engineering processes.

1.4 Key Use Cases

The **FucyTech TARA Tool** supports a wide range of cybersecurity and risk management applications across industries, with a focus on the automotive sector. Key use cases include:

- **Automotive cybersecurity compliance**
  Supporting compliance with **ISO 21434** and **UNECE WP.29** regulatory requirements for vehicle cybersecurity.

- **Risk assessment for critical infrastructure**
  Managing threats in systems that support essential and high-impact services.

- **Cybersecurity assessments**
  Evaluating vulnerabilities in **embedded systems**, **IoT devices**, and **networked environments**.

- **Compliance and regulatory risk analysis**
  Ensuring systems adhere to relevant **safety** and **security standards** across industries.

- **System design and testing**
  Identifying and mitigating risks throughout the entire **development lifecycle**, from concept to deployment.

- **Supply chain cybersecurity management**
  Coordinating cybersecurity activities and risk assessments across **multiple suppliers** and partners.

- **Post-production cybersecurity monitoring**
  Supporting ongoing cybersecurity efforts and **threat response** after product release.

2. System Overview

2.1 High-Level Architecture

The TARA Tool is modular, scalable, and secure, making it adaptable to industries like automotive, IoT, and smart home systems. It uses modern web technologies and cloud infrastructure for performance and reliability, with specific design considerations to support ISO 21434 compliance.

2.1.1 Frontend

- Developed with **React.js**
- Provides a dynamic, responsive UI
- Supports real-time project setup, risk modeling, threat analysis, and reporting
- Includes ISO 21434-specific dashboards and reporting templates

2.1.2 Backend

- Built using **Python Flask**
- Handles API requests and business logic
- Communicates securely with frontend via RESTful API
- Implements ISO 21434 workflows and data models

2.1.3 Database

- **MongoDB (NoSQL)**
- Flexible, document-based storage
- Stores complex project data: threats, risks, treatment actions
- Maintains traceability of cybersecurity activities as required by ISO 21434

2.1.4 Cloud Infrastructure

- Hosted on **Microsoft Azure**
- Ensures scalability, high availability, and security

- Supports automated backups and disaster recovery
- Provides secure access controls aligned with ISO 21434 requirements

2.2 Main Modules / Components

Each module supports a key stage of the threat and risk assessment process, aligned with ISO 21434 clauses:

2.2.1 Item Definition (Clause 9)

- Define assets, interfaces, and communication flows in the system
- Document system boundaries and cybersecurity properties
- Establish item definitions as the foundation for cybersecurity analysis

2.2.2 Damage Scenarios and Impact Ratings (Clause 15)

- Analyze the impact of cyber failures on safety, privacy, finances, and operations
- Document damage scenarios with clear traceability

  Assess impact ratings using ISO 21434 methodologies

2.2.3 Threat Scenarios (Clause 15)

- Document threats and vulnerabilities, identifying attack opportunities
- Link threats to damage scenarios
- Maintain comprehensive threat catalogs aligned with industry standards

2.2.4 Attack Path Analysis (Clause 15)

- Explore attacker paths to find weak points and attack surfaces
- Assess attack feasibility using ISO 21434 parameters
- Document attack paths with clear visualization

2.2.5 Goals, Claims, and Requirements (Clauses 7, 14, 15)

- Define security goals, link supporting claims, and identify needed requirements

- Ensure traceability between requirements and identified risks
- Support verification planning as required by ISO 21434

2.2.6 Risk Assessment and Treatment (Clause 15)

- Determine risk levels based on impact and attack feasibility
- Document risk treatment decisions
- Support risk management throughout the product lifecycle

2.2.7 Cybersecurity Verification (Clauses 10, 11)

- Plan and document verification activities
- Link verification results to requirements
- Support evidence collection for compliance demonstration

2.2.8 Post-Production Support (Clauses 7, 13)

- Monitor cybersecurity events
- Support incident response processes
- Facilitate vulnerability management

2.3 ISO 21434 Alignment

The TARA Tool has been specifically designed to align with ISO 21434 requirements:

2.3.1 Process Alignment

- Each module corresponds to specific clauses in ISO 21434, ensuring comprehensive coverage of the standard’s requirements.

2.3.2 Documentation Support

- Automatically generates documentation required for ISO 21434 compliance, including risk assessment reports, verification evidence, and traceability matrices.

2.3.3 Cybersecurity Assurance Levels

- Supports defining and managing Cybersecurity Assurance Levels (CALs) as outlined in ISO 21434.

2.3.4 Supply Chain Integration

- Features to support standardized communication and collaboration between different entities in the supply chain, as required by ISO 21434

2.3.5 Executive Reporting

- Dashboards and reports designed to provide executive management with visibility into cybersecurity status and compliance.

2.4 Technologies Used

- **Frontend:** React.js, Redux, Material-UI
- **Backend:** Python Flask, RESTful API
- **Database:** MongoDB
- **Cloud Infrastructure:** Microsoft Azure
- **Security:** OAuth 2.0, HTTPS, data encryption
- **Visualization:** D3.js, Cytoscape.js
- **Reporting:** PDF generation, Excel export
- **Integration:** REST APIs, webhook support

3. Accessing and Using the TARA Tool

The TARA (Threat Analysis and Risk Assessment) Tool is a structured, web-based platform that assists organizations in identifying, evaluating, and managing cybersecurity risks in alignment with ISO 21434 standards.

3.1 TARA Tool Workflow Overview

The TARA Tool integrates the ISO 21434 cybersecurity engineering process into a structured workflow. Below is the step-by-step workflow represented in block format:

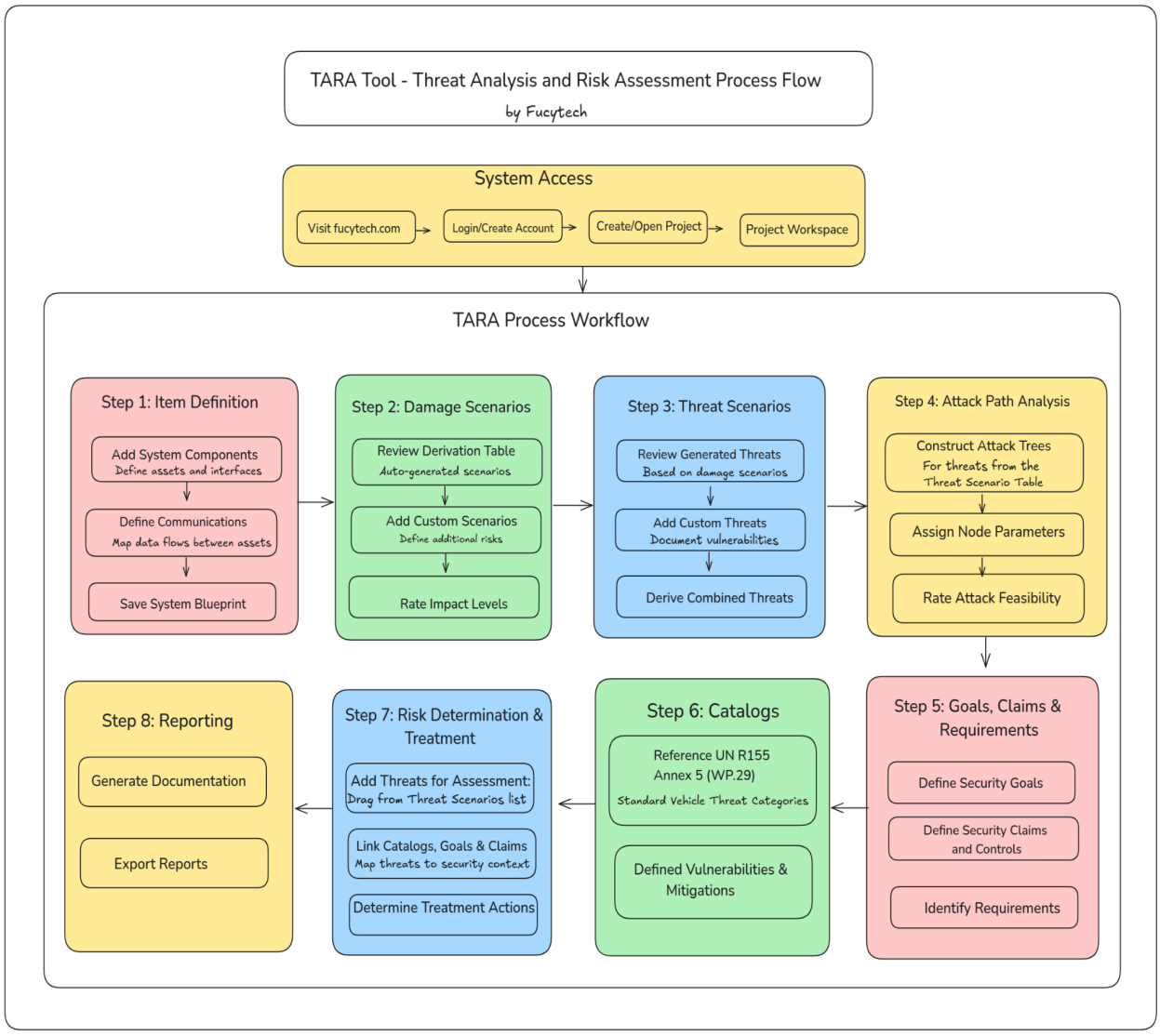


Figure 3.1: Workflow Block Diagram of the Tara Tool

3.2 Accessing the Tool

3.2.1 Visit the Official Website

- Go to: 👉 https://www.fucytech.com
- Upon accessing the link, you will be redirected to the **FucyTech Home Page**.

Home Page of FucyTech

3.2.2 Navigate to the TARA Tool

- From the Home Page, go to the top navigation bar
- Hover over "Products"
- Under the "Cyber Security" section, click on "TARA Tool"

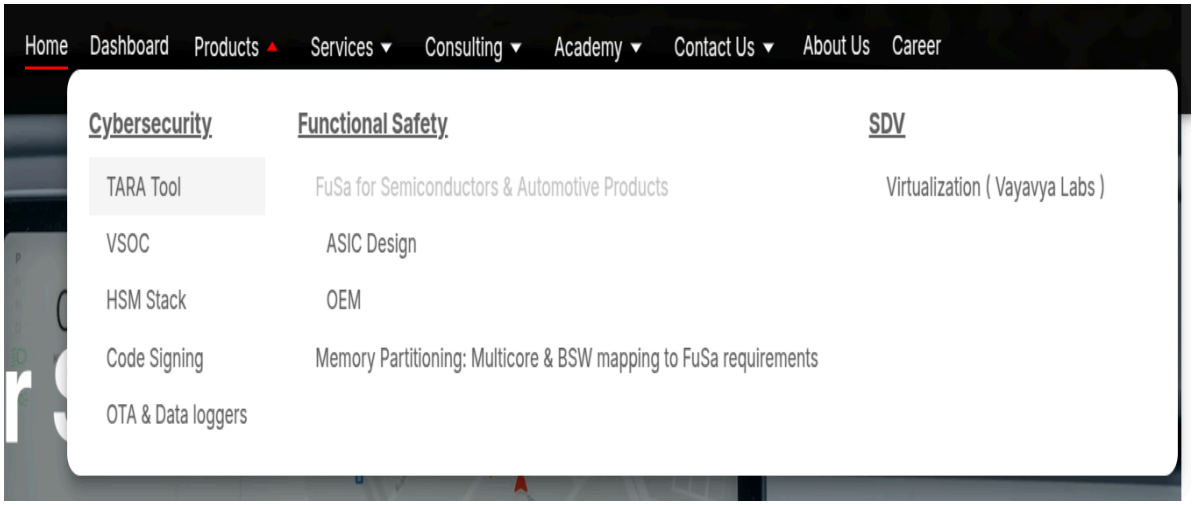
3.2.3 Login or Create an Account

a. If you already have an account:

- Enter your email and password
- Click Login

b. If you're a new user:

- Click "Sign Up" or "Create Account"
- Enter the required details (e.g., name, email, password)
- Submit the form to register
- You will be redirected to the login interface



Accessing the TARA Tool from the Home Page

3.3 Navigating the TARA Tool After Login

Once you have successfully logged in or registered, follow the steps below:

3.3.1 Project Options

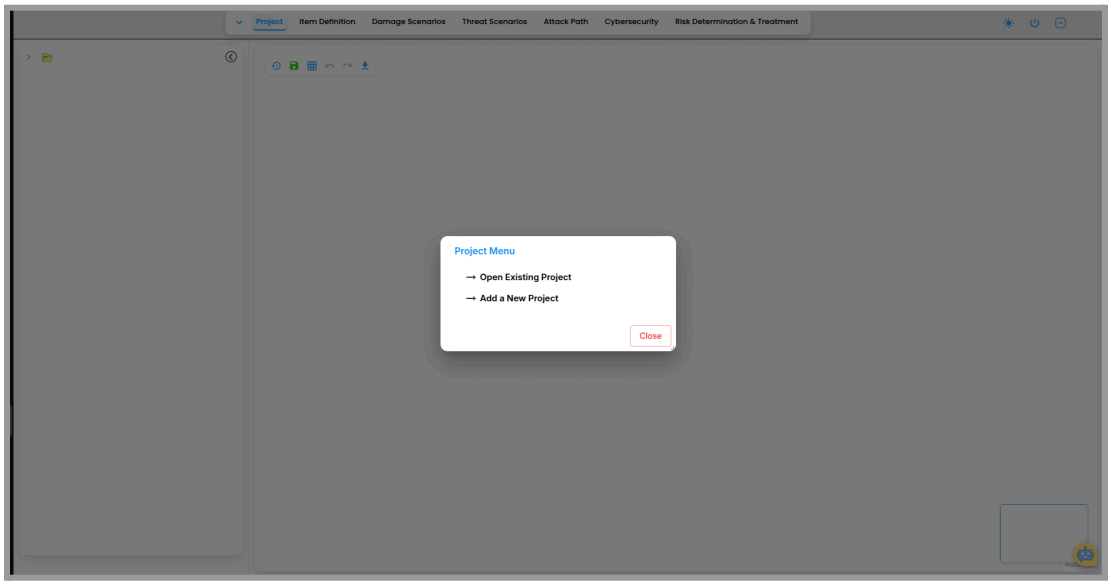
You will be prompted to choose between:

- Open Existing Project – to edit or update a project
- Create New Project – to initiate a new analysis

3.3.2 Creating a New Project

If you choose to create a new project:

- Enter the Project Name
- Click Next or Proceed



Navigating the TARA Tool After Login

3.3.3 Using the Project Workspace

Inside the project workspace, you can:

- Add system assets and interfaces
- Identify threats and attack paths
- Determine risks and define mitigations
- Generate reports and export findings

4. Working with the TARA Tool: Step-by-Step Process

Once you're inside a project, follow these key steps in the **TARA Risk Analysis Workflow** to define and build your system model.

4.1 Step-1 : Item Model and Definition

The **Item Model** is a blueprint that describes the components of a system, how they are interconnected, and how they collectively function as a complete system. It helps visualize the architecture, identify component relationships, and uncover potential security risks.

Example:

Consider a smart home system:

- Components: Smart Lock, Security Camera, Smart Lights
- Connected to: Central Hub (brain of the system)
- User Interface: Mobile App
- Data Storage: Cloud Server

This complete setup — with devices, their interconnections, and communication methods — constitutes the **Item Model**.

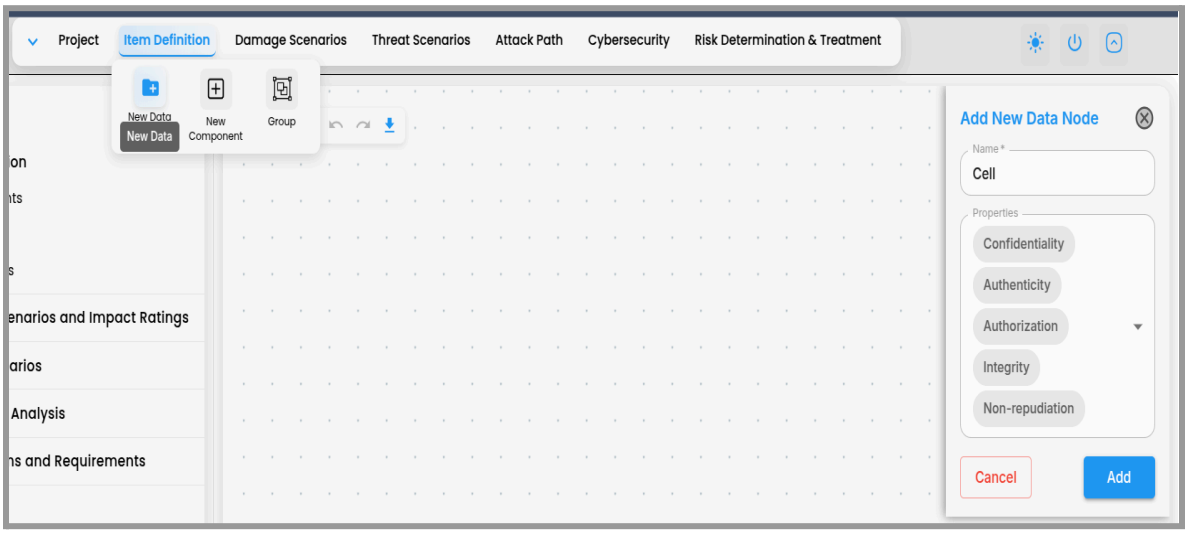
4.1.1 Building the Item Model in the TARA Tool

Step 1: Add New Nodes (System Components)

1. Navigate to **Item Definition** in the top navigation bar.
2. Click **New Data**.
3. In the "Add New Data Node" popup:
    - Enter the **component name** (e.g., Smart Lock).
    - Select **properties** from the dropdown.

- Click **Add** to place the node on the canvas.

4. Repeat for all system components.

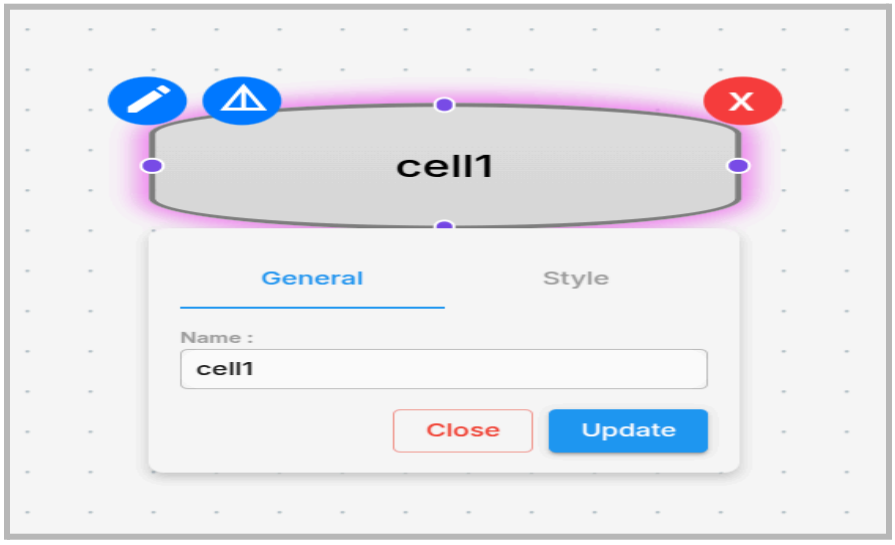


Adding New Nodes (System Components)

Edit Existing Nodes

Rename a Node:

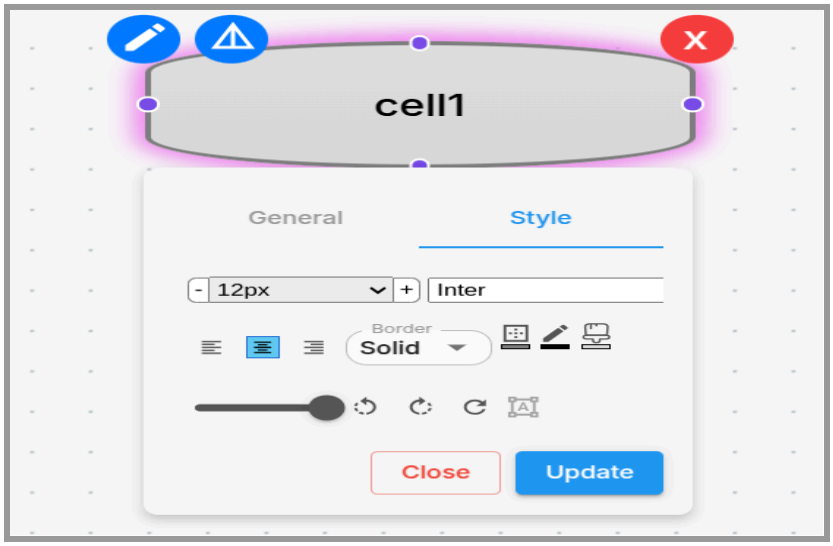
1. Click the node on the canvas.
2. Click the ✏️ (edit) icon at the top of the node.
3. In the popup under the **General** heading, rename the node.



FiEditing Existing Nodes

Edit Nod Style:

1. In the same popup, switch to the **Style** tab.
   to modify the following:
   - **Font size** and **font family**
   - **Text alignment**
   - **Connection type** (Solid, Dashed, etc.)
   - **Text color**
   - **Box color** and **opacity**

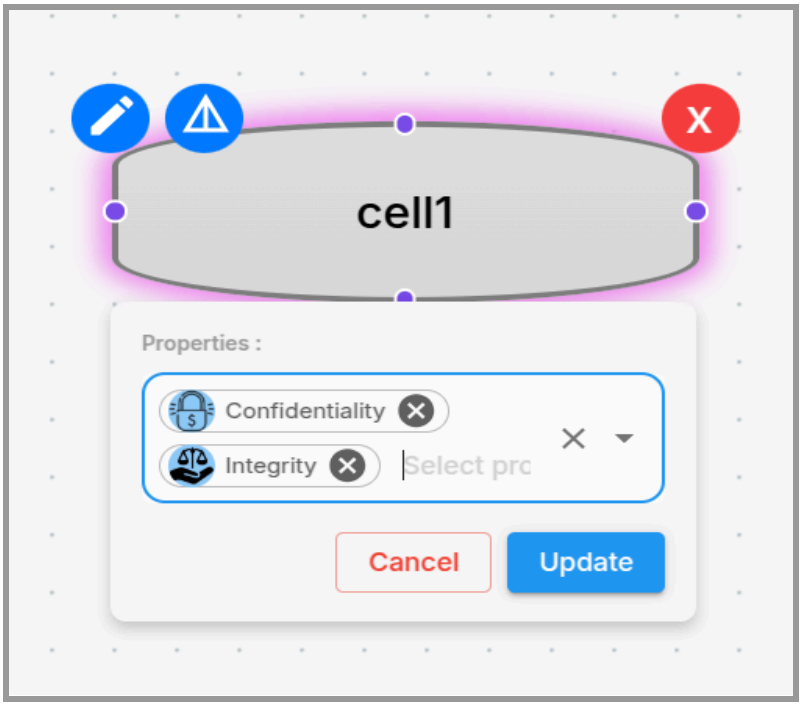


Editing Node Style

2. After making your changes, click **Update** to save them

Edit Node Properties:

1. To edit the properties, click the icon next to the **edit icon**.
2. Select the properties you want to modify or remove. Once you're done, click **Update** to save the changes.



Editing Node Properties

Delete a Node:

1. Click the ❌ (X) icon on the node.
2. Choose one of the options:
    - **Delete from Canvas** – removes node visually.

      Delete Permanently – removes node and data.

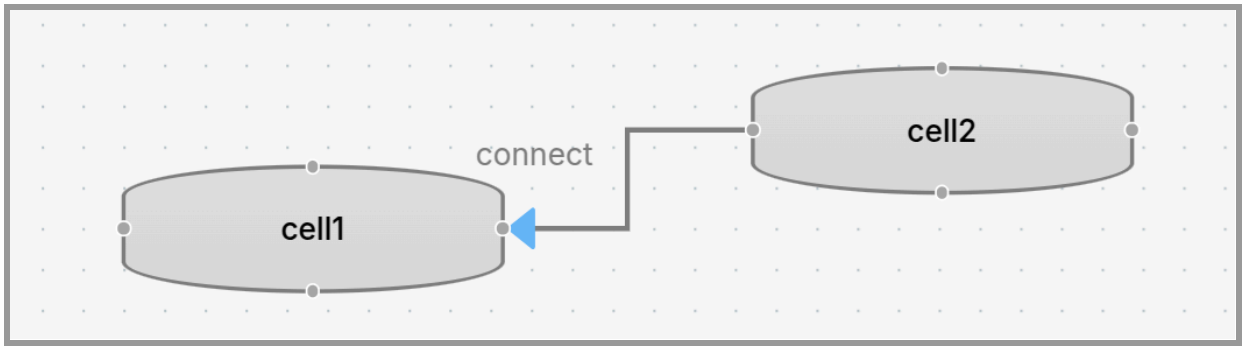
Additional Actions

- Right-click any node to access **Copy**, **Paste**, or **Duplicate** options.

Step 2: Connect Nodes

Create Connections:

1. Use connector dots on each node (top, bottom, left, right).
2. Click and drag from one dot to another node to establish a connection.



Creating Connections Between Nodes

Edit Connections:

1. Click on the connection line.
2. Use the icons:
    - **Direction Icon**: Set direction (e.g., uni- or bi-directional).
    - **Edit Icon (✏️)**:
        - Rename connection
        - Add/remove properties (e.g., communication protocol, data type)
        - Style (font, color, line type)
    - **Delete Icon (X)**: Remove the connection.

Step 3 : Group Nodes

A) Drag-and-Drop Grouping:

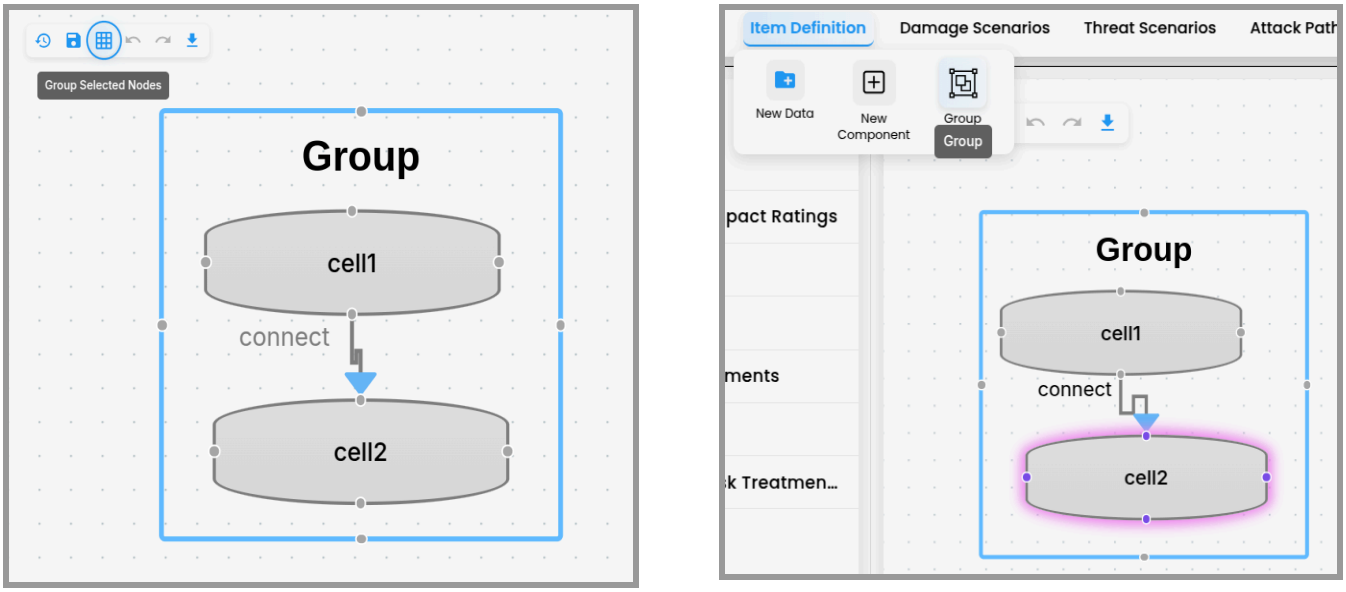
1. Click the **Group** icon (beside Save panel).
2. Drag it onto the canvas.
3. Move relevant nodes inside the group box.
4. Click the box to rename the group.

B) Group via Navigation Bar:

1. Navigate to **Item Definition**.
2. Drag and drop the **Group** option from the sidebar.

---

3. Create and manage groups from this interface.



Grouping Nodes Using Sidebar and Navigation Bar

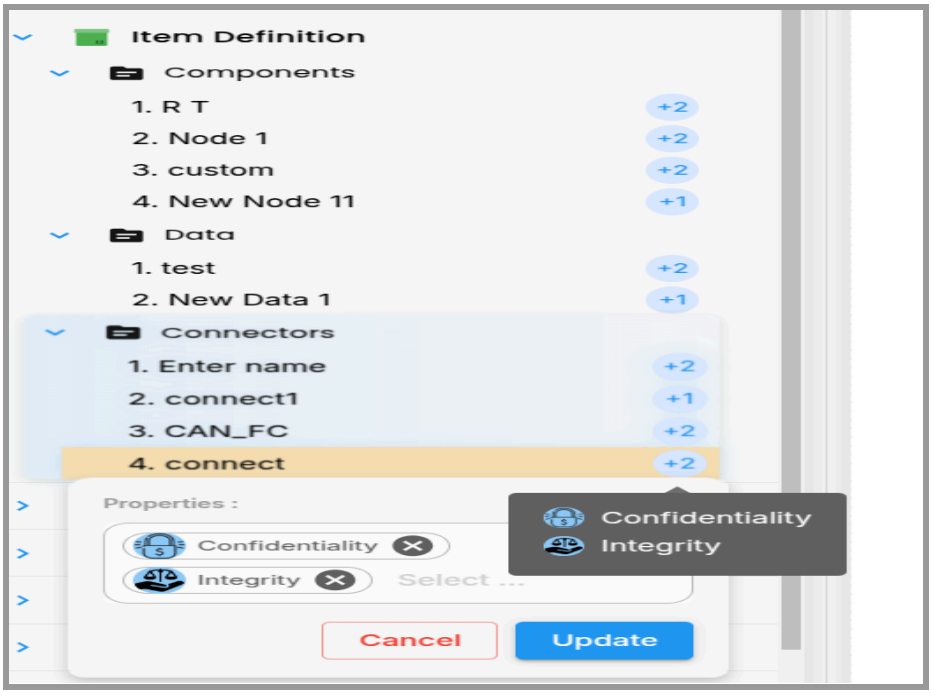
Access Existing Nodes and Connectors

1. Open the sidebar and click **Item Definition**.
2. A dropdown will display all existing nodes and connections.
3. Hover over a node to view attached properties (e.g., +4, +3).
4. Click the endpoints to edit node properties directly.

Step 4: Save Your Model

Once your nodes are added, styled, connected, and grouped:

- Click the **Save** icon in the toolbar.
- Your **Item Model** is now saved and ready for further TARA risk analysis.



Accessing Existing Nodes and Connectors

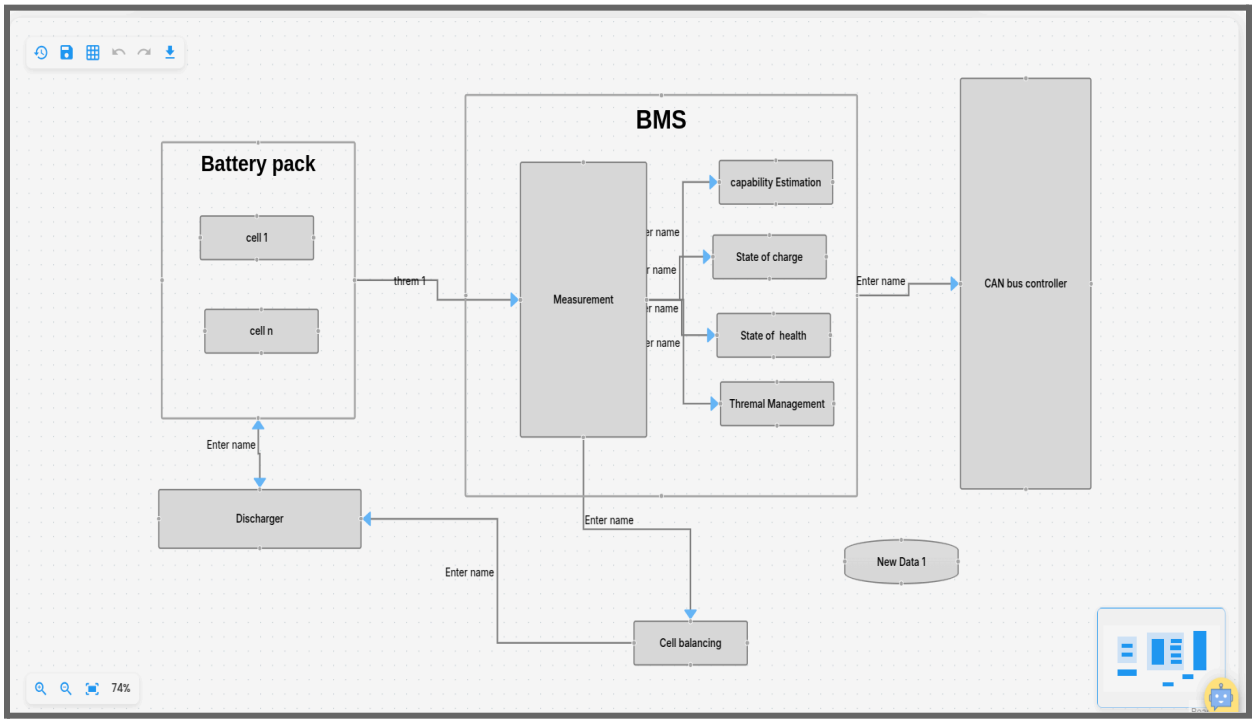


Figure 4.1: Complete Item Model for the Battery Management System (BMS)

4.2 Step 2: Damage Scenarios and Impact Ratings

Damage Scenario Identification is a key step in cybersecurity risk management. It helps organizations understand how different parts of a system might be harmed if a cyberattack or failure occurs. By recognizing potential failures and threats early, you can take action to minimize risk.

Example:
In a smart home security system, imagine a hacker gains access to the central hub. With control over the hub, they could unlock the smart lock, disable the security cameras, and turn off alarms. This creates a serious damage scenario where the safety of the home is at risk, personal privacy is violated, and there may be financial losses due to theft. Identifying this scenario helps prioritize actions like strengthening passwords, securing network connections, and monitoring system access.

Building the Damage Scenario in the TARA Tool

Follow these steps to define your system's damage scenario using the TARA Tool:
Navigate to **Damage Scenarios** via the sidebar or navbar. You will see two sub-items:

- **Damage Scenario Derivation Table**
- **Damage Scenarios – Impact Ratings**

4.2.1 Damage Scenario Derivation Table

Once the item model and system assets are defined, a **Damage Scenario Derivation Table** is automatically generated. This table outlines:

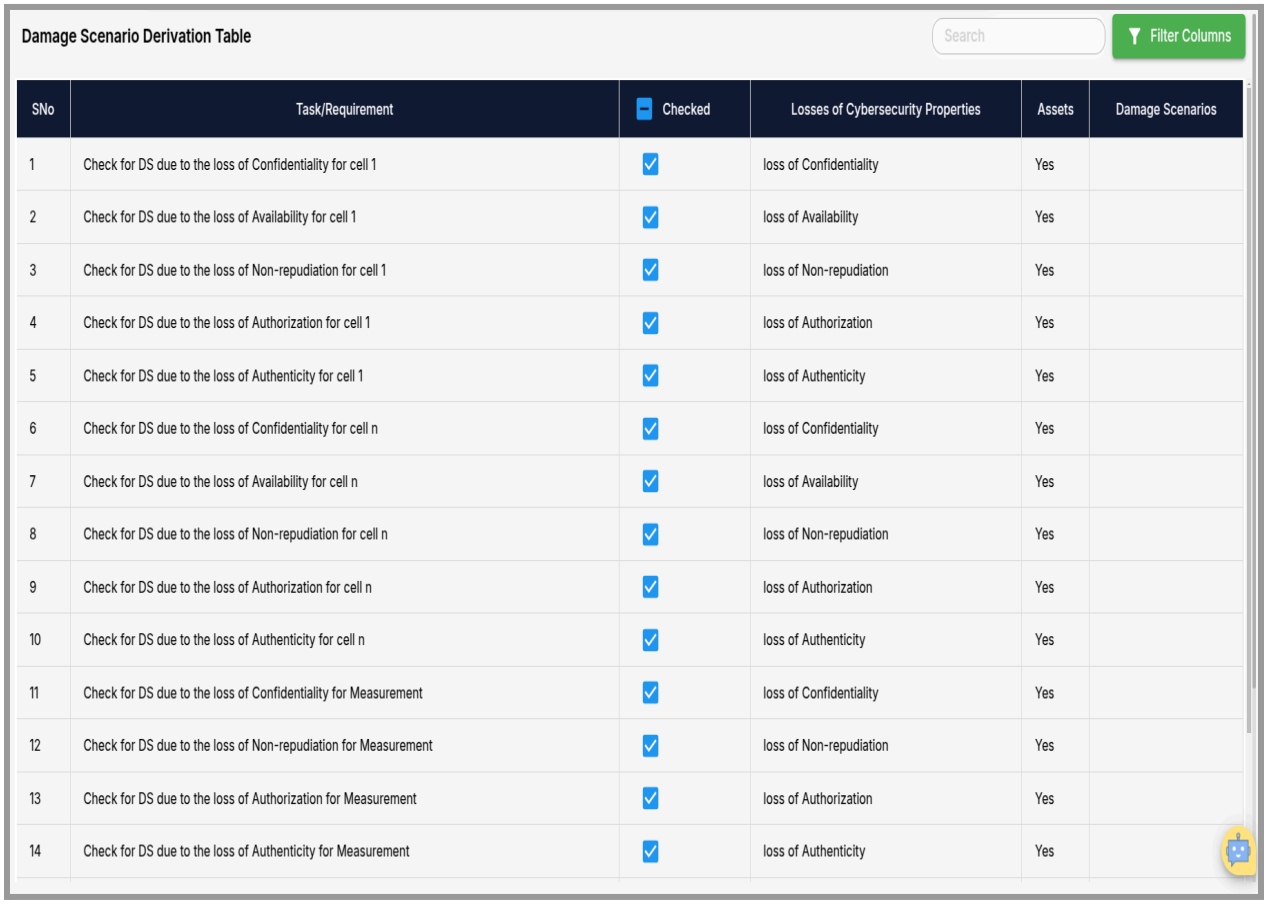
- Possible damage scenarios (ways the system might be harmed)
- The relationship between components and their vulnerabilities

Review each damage scenario listed.

- Check the box beside each scenario to validate and accept it.

- Your task is to review and verify the listed damage scenarios. Each should reflect realistic threats based on how your system is built and used.

Damage Scenario Derivation Table displaying potential system threats linked to specific components and vulnerabilities.



Damage Scenario Derivation Table

Search

Filter Columns

SNo	Task/Requirement	Checked	Losses of Cybersecurity Properties	Assets	Damage Scenarios
1	Check for DS due to the loss of Confidentiality for cell 1	☑	loss of Confidentiality	Yes	
2	Check for DS due to the loss of Availability for cell 1	☑	loss of Availability	Yes	
3	Check for DS due to the loss of Non-repudiation for cell 1	☑	loss of Non-repudiation	Yes	
4	Check for DS due to the loss of Authorization for cell 1	☑	loss of Authorization	Yes	
5	Check for DS due to the loss of Authenticity for cell 1	☑	loss of Authenticity	Yes	
6	Check for DS due to the loss of Confidentiality for cell n	☑	loss of Confidentiality	Yes	
7	Check for DS due to the loss of Availability for cell n	☑	loss of Availability	Yes	
8	Check for DS due to the loss of Non-repudiation for cell n	☑	loss of Non-repudiation	Yes	
9	Check for DS due to the loss of Authorization for cell n	☑	loss of Authorization	Yes	
10	Check for DS due to the loss of Authenticity for cell n	☑	loss of Authenticity	Yes	
11	Check for DS due to the loss of Confidentiality for Measurement	☑	loss of Confidentiality	Yes	
12	Check for DS due to the loss of Non-repudiation for Measurement	☑	loss of Non-repudiation	Yes	
13	Check for DS due to the loss of Authorization for Measurement	☑	loss of Authorization	Yes	
14	Check for DS due to the loss of Authenticity for Measurement	☑	loss of Authenticity	Yes	

Figure 4.2.1 :Damage Scenario Derivation Table

4.2.2 Damage Scenarios – Impact Ratings

In this section, users manually define new damage scenarios and evaluate their impact across multiple dimensions.

Step 1: Add a New Damage Scenario

- Click the **Add New Scenario** button in the top-right corner.
- A popup will appear. Fill in the following details:
    - **Name:** e.g., Unauthorized Access to Camera Feed
    - **Description:** Briefly explain what the scenario entails.
- Click **Create** to add the scenario to the table.

📌 **Note:** You can add as many damage scenarios as needed to accurately capture all relevant risks to your system.

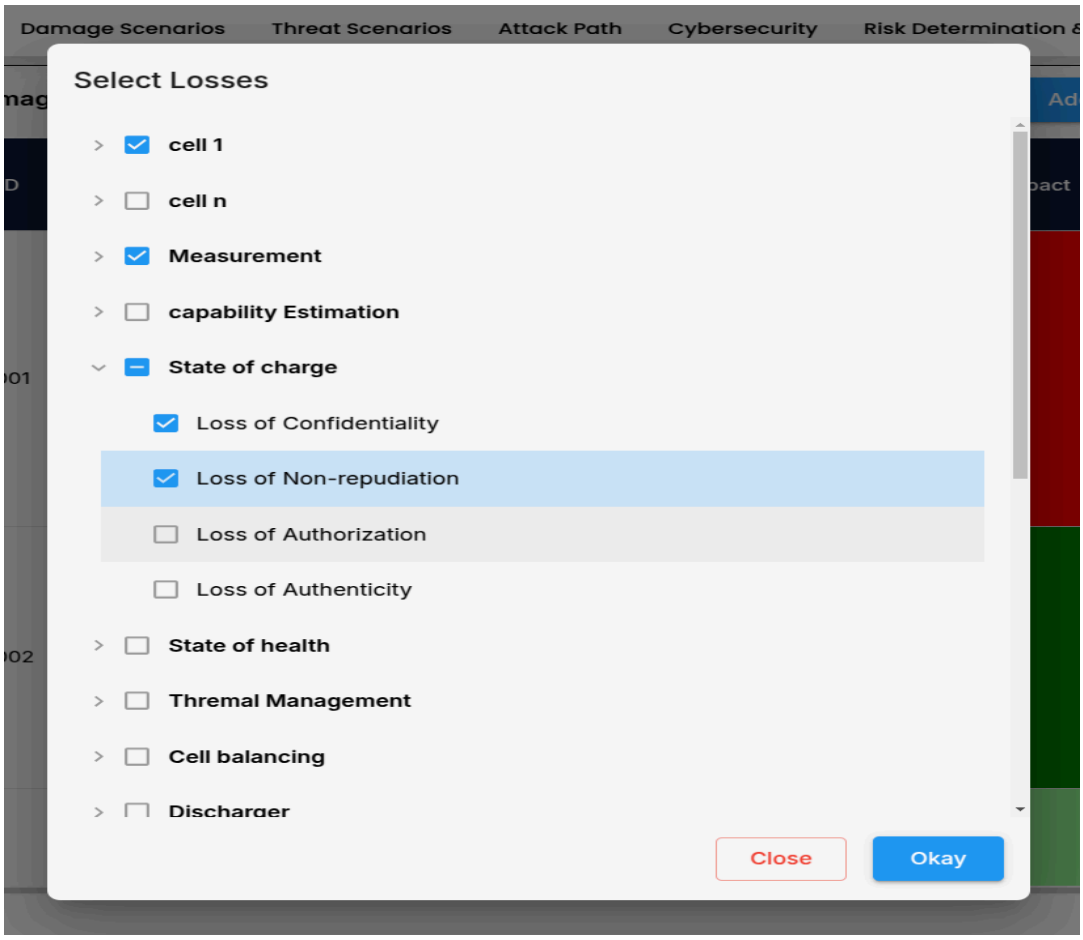
Step 2: Review the Table Structure

Once added, the new scenario appears in the table with the following columns:

- **ID**
- **Name**
- **Description** (pre-filled during scenario creation)

Step 3: Assign Losses of Cybersecurity Properties

- Under the **Select Losses** column, click to open a popup.
- A tree view of all system nodes and connectors will appear.
- You can:
    - Select all properties of a component, or
    - Expand a component (using the > icon) to choose specific properties (e.g., Wi-Fi credentials, live camera feed).
- Click **OKAY** to confirm.



Assigning Losses of Cybersecurity Properties

Step 4: Assess Impact Ratings

Each scenario must be evaluated across four key impact areas:

Impact Area	Question to Consider
Safety Impact	Could this scenario put physical safety at risk?
Financial Impact	Could it result in financial loss?

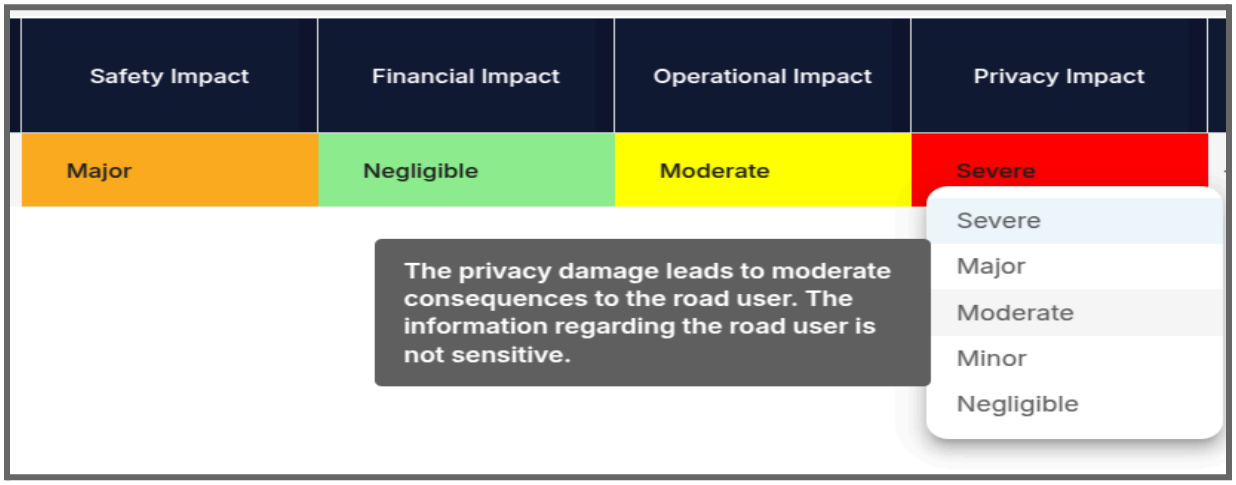
Operational Impact	Could it disrupt system functionality?
Privacy Impact	Could it lead to data breaches or leaks?

For each area:

Click the corresponding cell.

Select one of the following impact levels (color-coded for clarity):

- 🔴 **Severe**
- 🟠 **Major**
- 🟡 **Moderate**
- 🟢 **Minor**
- 🟢 **Negligible**



Impact Rating Assessment Interface

Step 5: Provide Impact Justification and Threat Scenarios

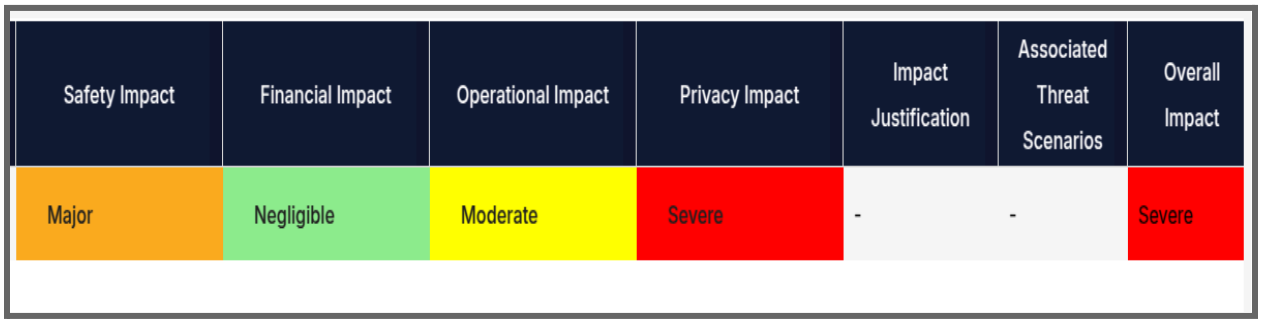
Use the **Impact Justification and Associated Threat Scenarios** column to briefly explain why each impact level was selected.

📌 **Note:** This field is currently empty. The relevant data will be added at a later stage.

Step 6: Review the Overall Impact

The **Overall Impact** is automatically calculated based on the four individual impact ratings.

This provides a quick summary of the scenario's total potential harm.



Safety Impact	Financial Impact	Operational Impact	Privacy Impact	Impact Justification	Associated Threat Scenarios	Overall Impact
Major	Negligible	Moderate	Severe	-	-	Severe

Overall Impact Calculation

Final Result

By completing this process, you will:

- Have a list of tailored damage scenarios for your system
- Clearly link each scenario to specific components and properties
- Understand the potential impact across safety, financial, operational, and privacy domains

Deleting Damage Scenarios

To delete a scenario:

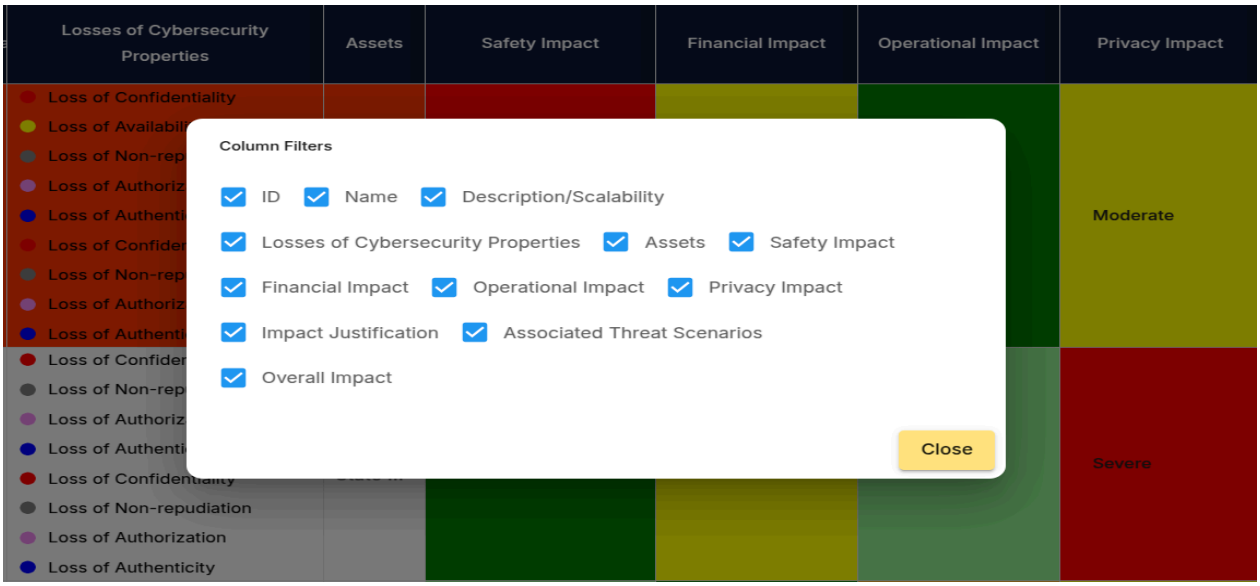
- Click on the corresponding **ID** (e.g., DS001).
- Once selected, click the **Delete** button at the top right.
- You can select multiple IDs and delete them simultaneously.

Deleting Damage Scenarios

Filtering Table Columns

Use the **Filter** option (top right) to customize the table view.

- You can choose which columns to show or hide based on your focus.



Filtering Table Columns

Figure 4.2.2: Structured View of Custom Damage Scenarios

4.3 Step 3: Threat Scenarios

Threat scenarios are created by examining how specific system vulnerabilities can be exploited to cause known types of damage—such as loss of **confidentiality**, **availability**, or **non-repudiation**.

The process begins with identifying potential damage impacts, then determining which attacks and threat actors could realistically cause them. Each threat scenario outlines a possible attack path, including the **method**, **target asset**, and the **compromised cybersecurity property**. This helps visualize how threats emerge and guides risk reduction strategies.

Example:

In a smart home system, unauthorized access to the central hub could lead to a loss of:

- **Confidentiality**
- **Availability**
- **Non-repudiation**

Threat scenarios include:

- **Phishing** to steal credentials (*loss of confidentiality*)
- **Tampering with logs** to hide actions (*loss of non-repudiation*)

  DoS attack on the hub (*loss of availability*)

Each path highlights a different way the same damage outcome can occur, helping organizations prepare effective defenses.

Working with Threat Scenarios in the TARA Tool

To define your system's threat scenarios using the **TARA Tool**, follow these steps:

Navigation:

Go to the Threat **Scenario** from the **sidebar** or **navbar**. You will find two sub-sections:

- **Threat Scenarios**
- **Derived Threat Scenarios**

4.3.1 Threat Scenarios

Accessing Threat Scenarios:

1. In the sidebar, click on **"Threat Scenarios"**.
2. A dropdown will appear. Select **"Threat Scenarios"**.
3. You will see a table containing **auto-generated threat scenarios** based on your earlier damage scenarios.

Understanding the Generated Threat Scenarios:

Each entry in the threat scenario table includes:

- **Name**: e.g., *TS001, TS002*
  Description: Brief explanation of the threat (e.g., *"Phishing attack to steal credentials"*)
  Linked Damage Scenario: The damage scenario this threat corresponds to
- **Cybersecurity Property Affected**: e.g., *confidentiality, availability, non-repudiation*
  Asset: System asset at risk (e.g., *smart lock, central hub*)

These details help track how specific attacks exploit vulnerabilities and their potential impact on the system.

Adding a New Threat Scenario:

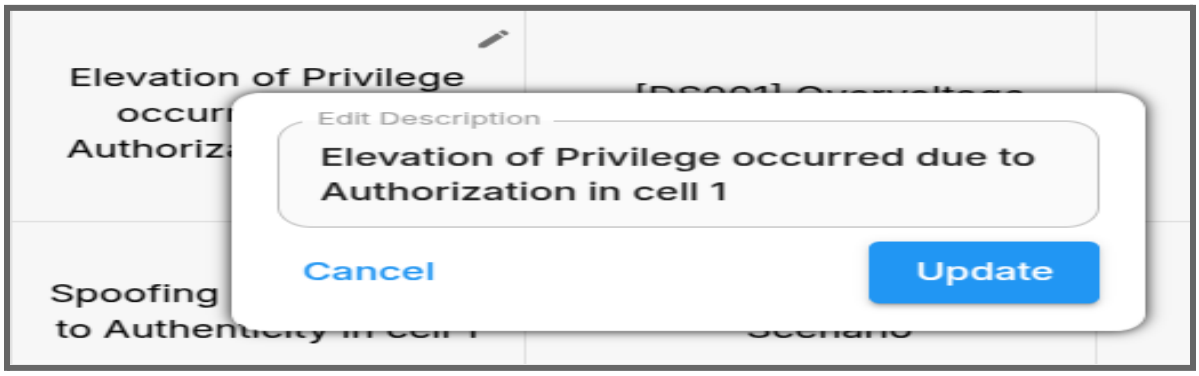
1. Click **"Add New Scenario"** in the top-right corner of the Threat Scenario section. A popup titled **"Add Threat Scenario"** will appear.
2. In the popup:

- Enter a **name** for the new scenario (e.g., *TS003: Brute Force Attack*)
- Provide a **description** of how the threat could occur
- Select the **linked damage scenario**
- Choose the **affected cybersecurity property**
- Assign the relevant **system asset**

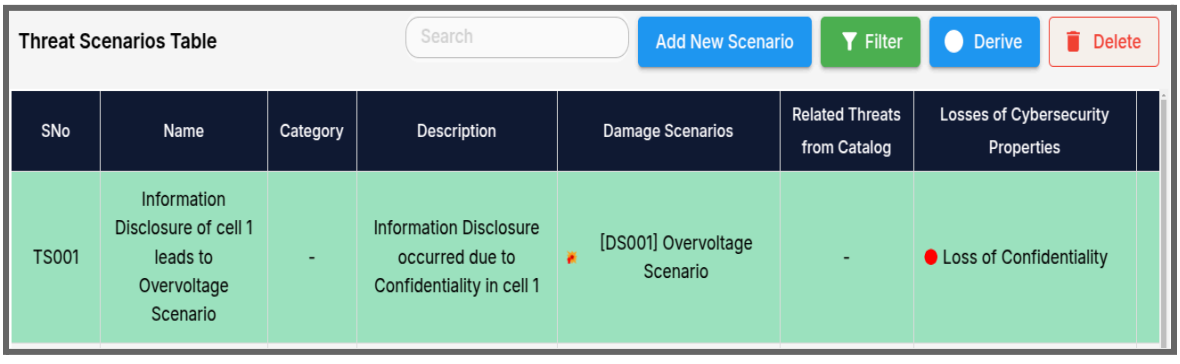
  Click **"Create"** to save the new scenario.
- It will now appear in the list of threat scenarios.

Editing or Removing a Scenario:

- **Edit**: Click an existing threat scenario. Hover over the description and click the **pencil icon** to update it.
- **Delete**: Click the scenario's serial number, then click **"Delete"** to remove it.



Editing a Threat Scenario Description

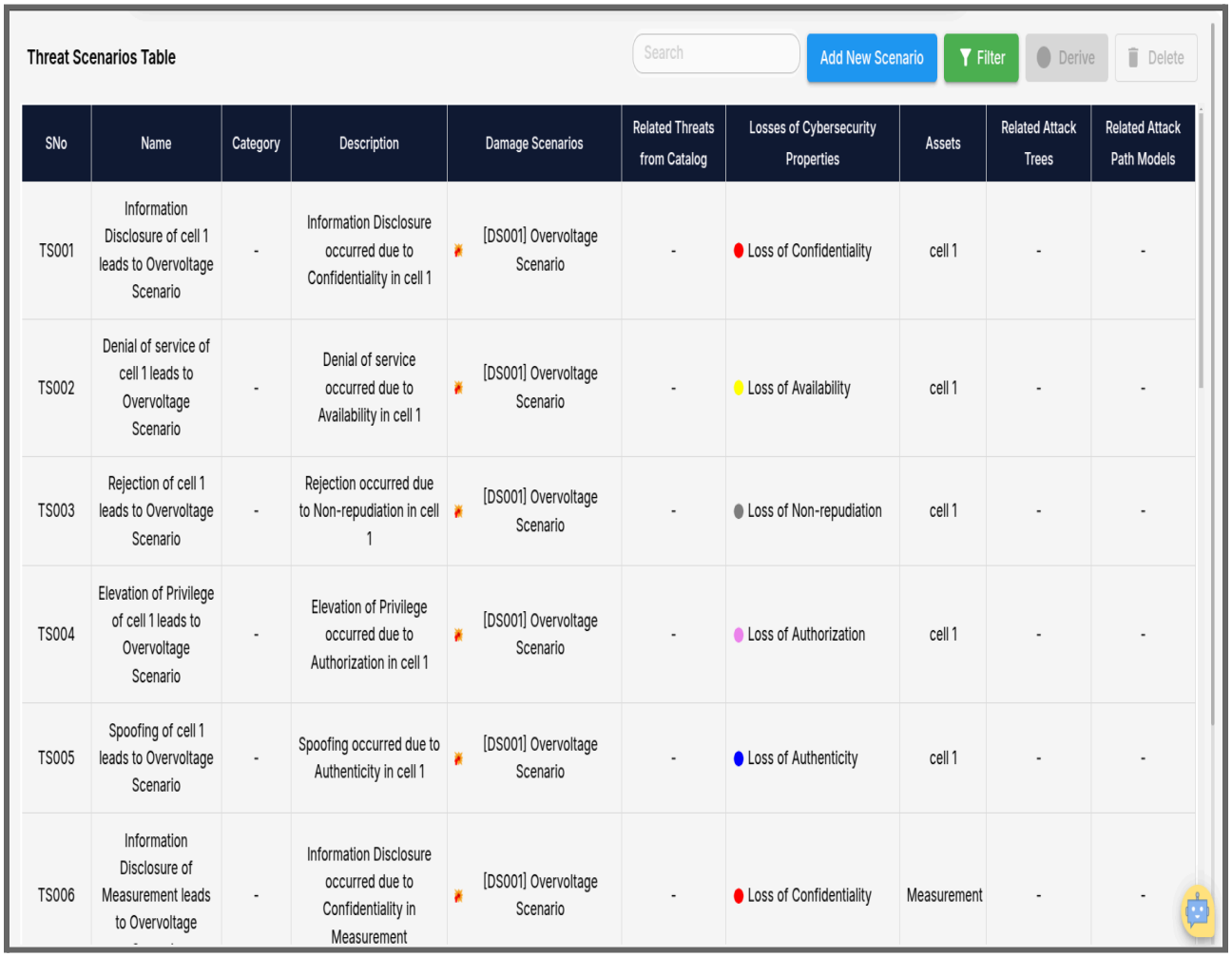


Deleting a Threat Scenario by Serial Number

📌 **Note:**

- Deleting a **damage scenario** will also delete all **linked threat scenarios**.
- Editing a **damage scenario** will update the related **threat scenarios** accordingly.

Example of threat scenarios derived from previously defined damage scenarios.



Threat Scenarios Table

Search | Add New Scenario | Filter | Derive | Delete

SNo	Name	Category	Description	Damage Scenarios	Related Threats from Catalog	Losses of Cybersecurity Properties	Assets	Related Attack Trees	Related Attack Path Models
TS001	Information Disclosure of cell 1 leads to Overvoltage Scenario	-	Information Disclosure occurred due to Confidentiality in cell 1	[DS001] Overvoltage Scenario	-	Loss of Confidentiality	cell 1	-	-
TS002	Denial of service of cell 1 leads to Overvoltage Scenario	-	Denial of service occurred due to Availability in cell 1	[DS001] Overvoltage Scenario	-	Loss of Availability	cell 1	-	-
TS003	Rejection of cell 1 leads to Overvoltage Scenario	-	Rejection occurred due to Non-repudiation in cell 1	[DS001] Overvoltage Scenario	-	Loss of Non-repudiation	cell 1	-	-
TS004	Elevation of Privilege of cell 1 leads to Overvoltage Scenario	-	Elevation of Privilege occurred due to Authorization in cell 1	[DS001] Overvoltage Scenario	-	Loss of Authorization	cell 1	-	-
TS005	Spoofing of cell 1 leads to Overvoltage Scenario	-	Spoofing occurred due to Authenticity in cell 1	[DS001] Overvoltage Scenario	-	Loss of Authenticity	cell 1	-	-
TS006	Information Disclosure of Measurement leads to Overvoltage	-	Information Disclosure occurred due to Confidentiality in Measurement	[DS001] Overvoltage Scenario	-	Loss of Confidentiality	Measurement	-	-

Figure 4.3: Threat Scenario Table

4.3.2 Derived Threat Scenarios

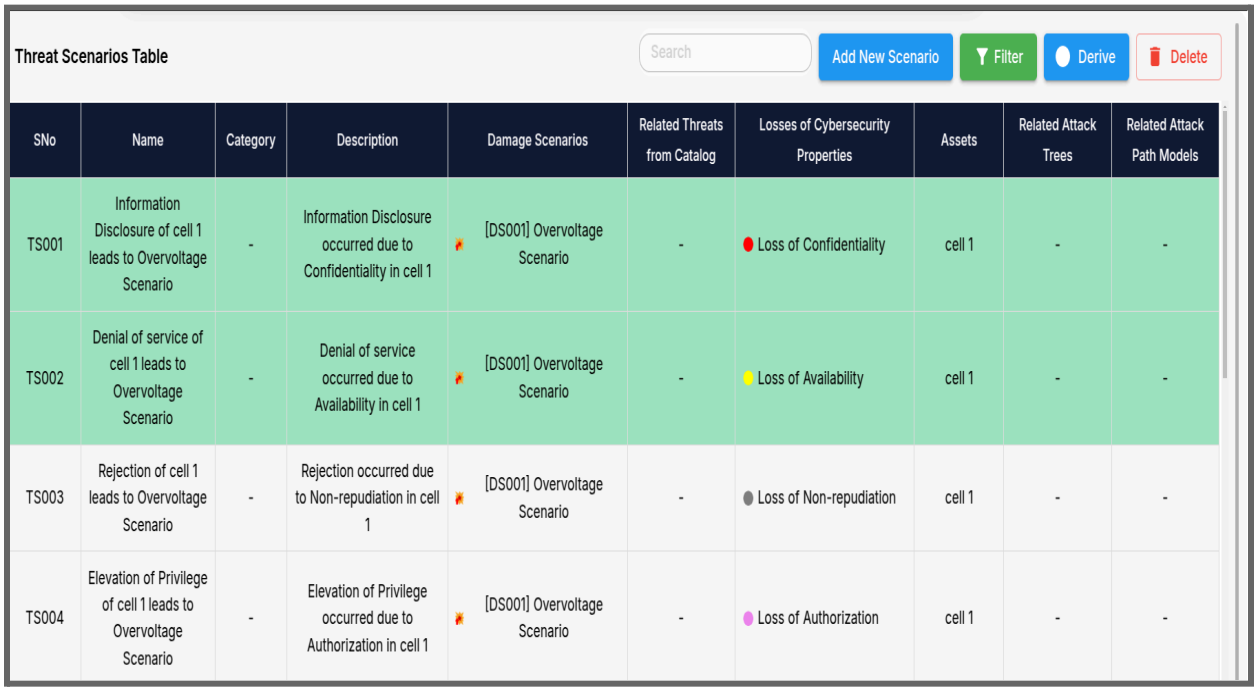
The **Derived Threat Scenarios Table** is created by **combining multiple related threat scenarios**. This helps streamline your threat landscape by grouping relevant scenarios into a more manageable set of **derived threats**.

Access the Threat Scenarios Table:

1. Go to the **Threat Scenarios** table you worked on earlier.

Select Threat Scenarios to Combine:

1. Identify the threat scenarios to combine (those sharing similar damage outcomes or attack methods).
2. Click on the corresponding scenario number (e.g., *TSD001*) for each scenario you want to combine.



Threat Scenarios Table

Search | Add New Scenario | Filter | Derive | Delete

SNo	Name	Category	Description	Damage Scenarios	Related Threats from Catalog	Losses of Cybersecurity Properties	Assets	Related Attack Trees	Related Attack Path Models
TS001	Information Disclosure of cell 1 leads to Overvoltage Scenario	-	Information Disclosure occurred due to Confidentiality in cell 1	[DS001] Overvoltage Scenario	-	Loss of Confidentiality	cell 1	-	-
TS002	Denial of service of cell 1 leads to Overvoltage Scenario	-	Denial of service occurred due to Availability in cell 1	[DS001] Overvoltage Scenario	-	Loss of Availability	cell 1	-	-
TS003	Rejection of cell 1 leads to Overvoltage Scenario	-	Rejection occurred due to Non-repudiation in cell 1	[DS001] Overvoltage Scenario	-	Loss of Non-repudiation	cell 1	-	-
TS004	Elevation of Privilege of cell 1 leads to Overvoltage Scenario	-	Elevation of Privilege occurred due to Authorization in cell 1	[DS001] Overvoltage Scenario	-	Loss of Authorization	cell 1	-	-

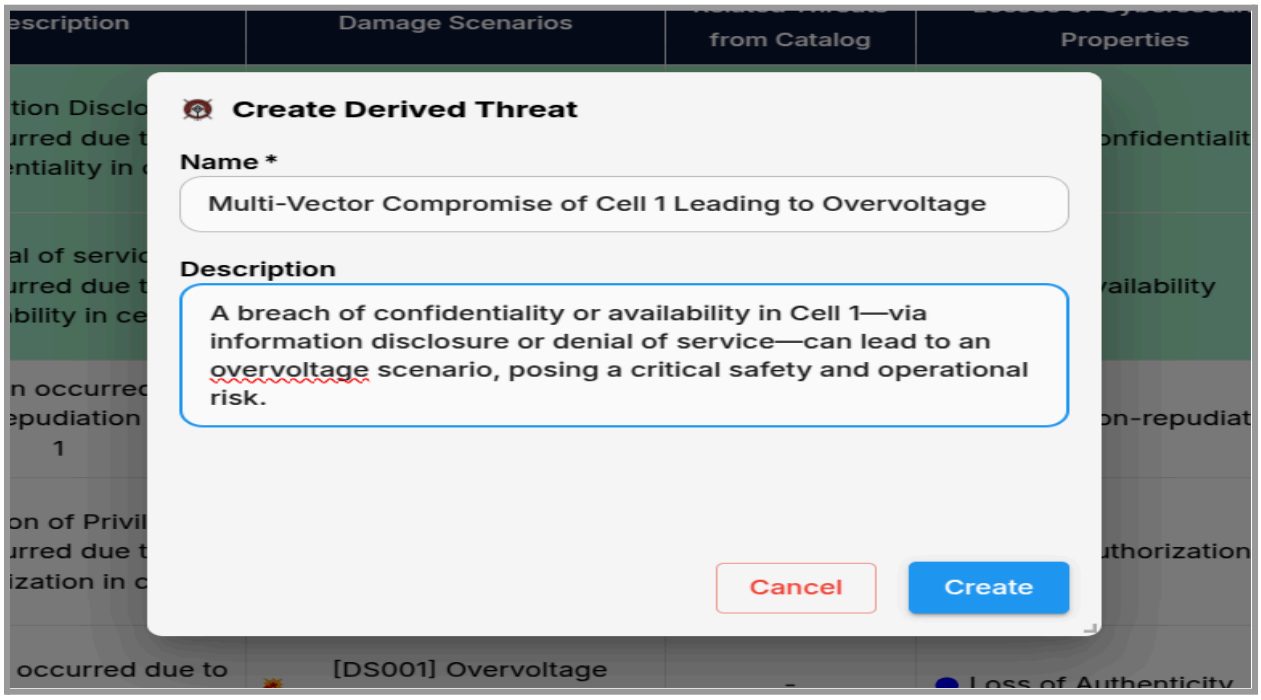
Accessing the Threat Scenarios Table and Identifying Scenarios for Combination

Create a Derived Threat:

1. After selection, look to the **top-right corner** of the screen.
2. Click the **"Derive"** button to start creating a derived threat scenario.

Fill in the Derived Threat Details:

1. A popup titled **"Create Derived Threat"** will appear.
2. Enter the following:
    - **Name** for the derived threat (e.g., *TSD002: Combined Phishing and DoS Attack*)
    - **Description** explaining the combination (e.g., *"A combination of phishing attack to steal credentials and denial-of-service attack targeting system availability"*)



Input Form for Creating a Combined Threat Scenario

Save the Derived Threat:

1. Click **"Create"**.
2. A confirmation will appear: *"Data added to Threat_Scenarios Details."*

View the Derived Threat Scenarios:

1. Navigate to the **Derived Threat Scenarios** section.
2. The newly created scenario will be listed with:
    - Corresponding **damage scenarios**

      Affected **cybersecurity properties**
    - Related **system assets**

Example:

You selected two scenarios:

- **TSD001**: Phishing attack to steal credentials (*loss of confidentiality*)
  TSD002: Denial-of-Service attack (*loss of availability*)

These are combined into:

- **TSD003: Combined Phishing and DoS Attack**, affecting both *confidentiality* and *availability*.

This simplifies threat scenario management and supports more efficient risk mitigation.

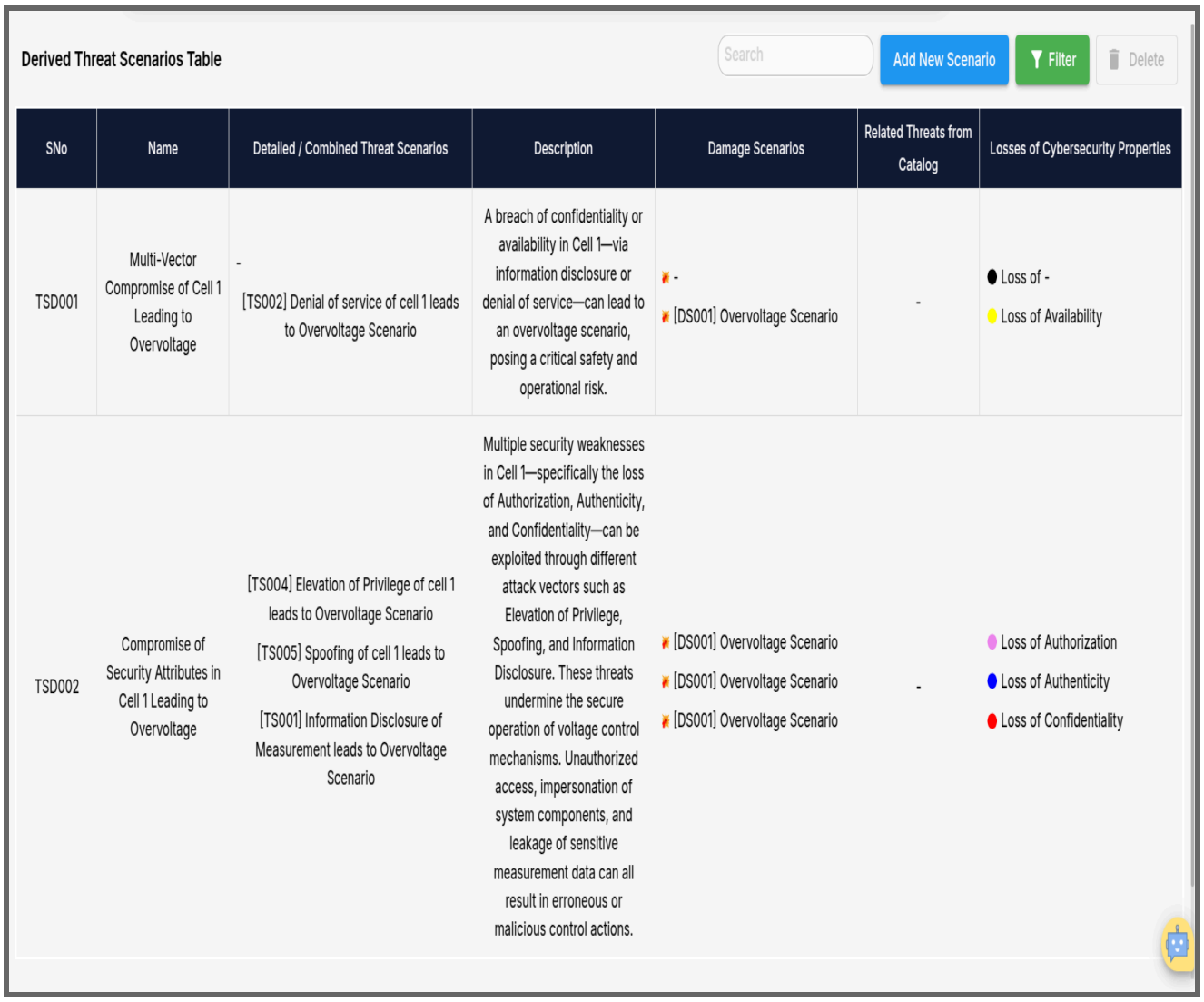


Figure 4.5: Input Form for Creating a Combined Threat Scenario

4.4 Step 4: Attack Path Analysis

Attack Path Analysis is a crucial technique in cybersecurity that maps out the possible steps an attacker might take to reach a valuable asset within a system. It helps in visualizing the sequence of events and decision points an attacker could exploit. By understanding these paths, security teams can break the chain of attack early by hardening vulnerable points, placing stronger controls, and monitoring high-risk steps.
Example

In a smart home security system, suppose an attacker starts by exploiting a weak password on a smart thermostat. From there, they move laterally through the network to access the central home hub. Once inside, they could gain control over smart locks, surveillance cameras, and lighting systems. This attack path shows how a small weakness can lead to full system compromise. Recognizing this path early allows homeowners to enforce strong authentication, isolate critical devices, and monitor unusual activity.

Working with Attack Path Analysis in the TARA Tool

To define and analyze attack paths using Attack Trees in the TARA Tool, follow these steps:

Navigate to **Attack Trees** from the **sidebar** or **navbar**. You will find two sub-sections:

- **Attack**
- **Attack Tree**

4.4.1 Step 4.1: Attack

This is the **Attack Table** in which the attacks from the Attack Tree are added. You need to assign the following values:

- Elapsed Time
- Expertise
- Knowledge of the Item

- Window of Opportunity
- Equipment

Once these values are filled in, the **Attack Feasibility Rating** will be calculated automatically.

Steps

1. First, go to Step 4.2 and build the complete attack tree.
2. Follow all steps up to **Step 6: Define Nodes (Attack or Requirement)**.
3. Specifically, complete **Step 3: Assign Attribute Values (Go to Step 4.1)**.
4. After that, come back to this Attack Table section.

Working with the Attack Table

- In the table, you will already see the added attack data based on what you defined in the tree.
- The columns include:
  SNO, Name, Category, Description, Elapsed Time, Expertise, Knowledge of the Item, Window of Opportunity, Equipment, and Attack Feasibility Rating.

Assigning Attribute Values

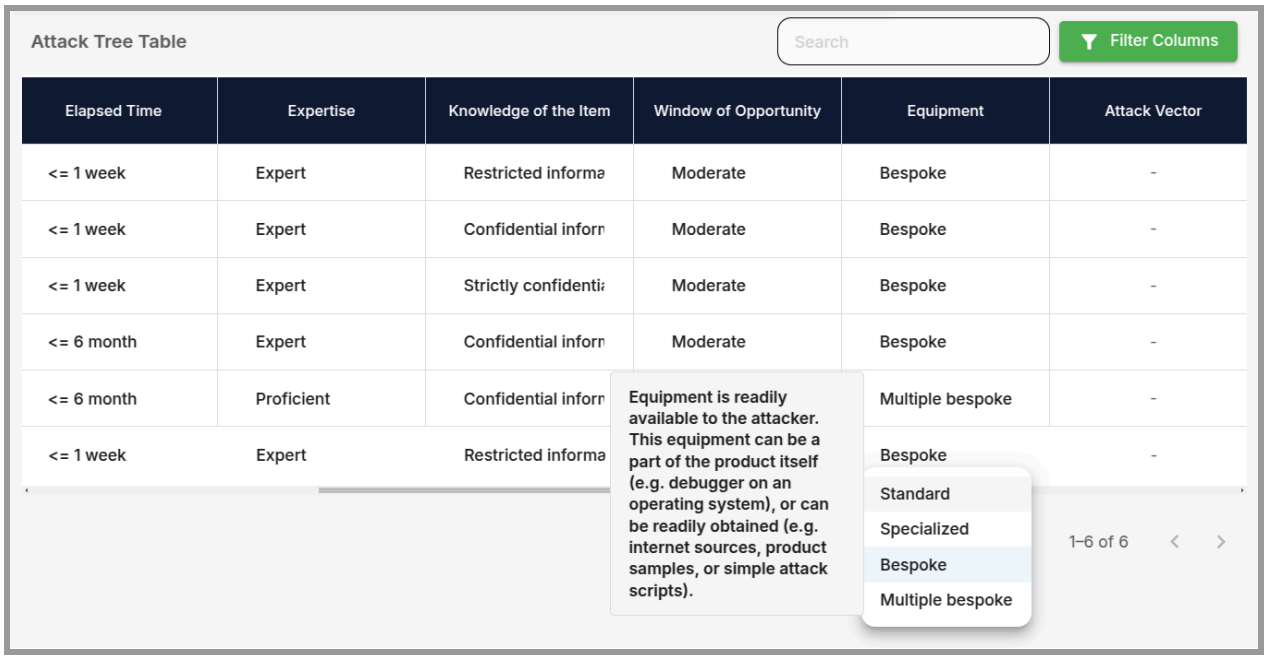
For each row, you will see the attack node and corresponding attributes
Below each of these columns:

- **Elapsed Time**
- **Expertise**
- **Knowledge of the Item**
- **Window of Opportunity**
- **Equipment**

You will see a **"Select Value"** option.

1. Click on **"Select Value"** → A dropdown will appear → Choose the correct value for each column.

2. After selecting, hover over the selected values to see a tooltip with an explanation of what each means.



Assigning Attribute Values to Attack Nodes

Automated Feasibility Calculation

Once all five values are filled, the last column **"Attack Feasibility Rating"** will automatically display the result:

- Very Low
- Low
- Medium
- High

This value is also visually represented using a background color for quick severity assessment.

After Completing

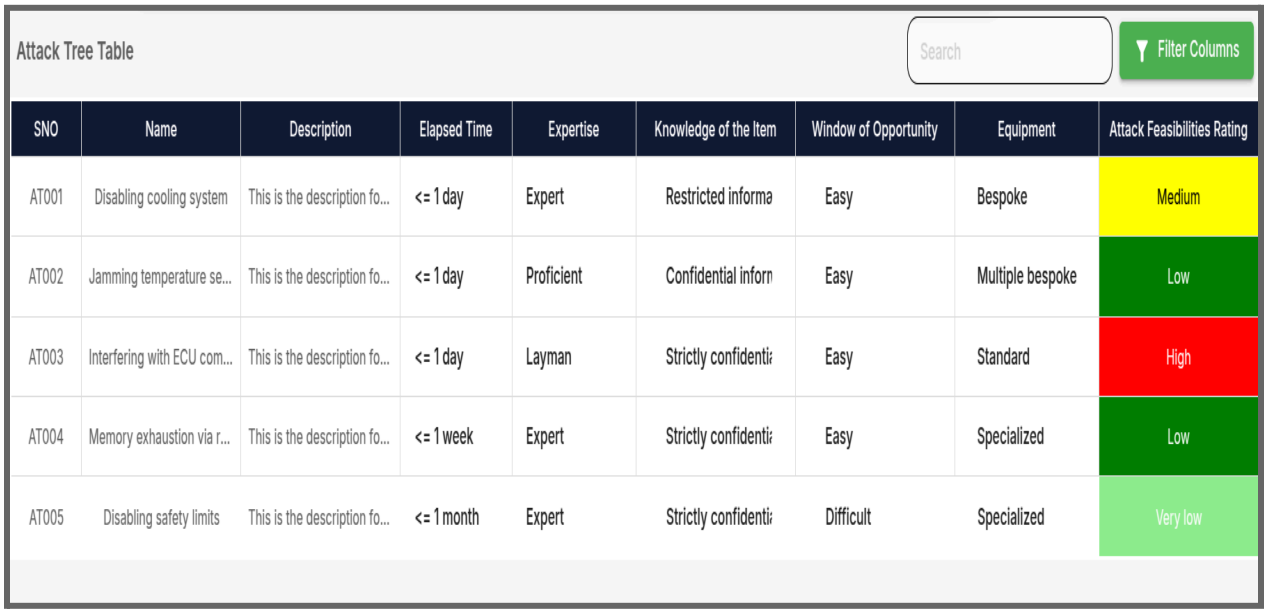
Once done with value selection, return to **Step 4.2** and continue from where you had stopped.

Additional Features

- You can filter columns by clicking on the **"Filter Columns"** button.
- Select which columns to show or hide.
- You can use the **Search Bar** to quickly locate specific attack nodes.

⚠️ Important Notes:

- There is no specific delete option for individual rows.
  If you want to remove attack data, go to the **Attack Tree** and delete the related event.
- It will be automatically removed from the Attack Table.



SNO	Name	Description	Elapsed Time	Expertise	Knowledge of the Item	Window of Opportunity	Equipment	Attack Feasibilities Rating
AT001	Disabling cooling system	This is the description fo...	<= 1 day	Expert	Restricted informa	Easy	Bespoke	Medium
AT002	Jamming temperature se...	This is the description fo...	<= 1 day	Proficient	Confidential inforn	Easy	Multiple bespoke	Low
AT003	Interfering with ECU com...	This is the description fo...	<= 1 day	Layman	Strictly confidentia	Easy	Standard	High
AT004	Memory exhaustion via r...	This is the description fo...	<= 1 week	Expert	Strictly confidentia	Easy	Specialized	Low
AT005	Disabling safety limits	This is the description fo...	<= 1 month	Expert	Strictly confidentia	Difficult	Specialized	Very low

Figure 4.4.1: Attack Tree Analysis Table

4.4.2 Attack Tree

The **Attack Tree** is a structured diagram that helps visualize all the potential ways an attacker might exploit your system's vulnerabilities. It allows you to break down each threat path into smaller, manageable nodes, making it easier to analyze risks and prioritize defenses.

Building the Attack Tree in the TARA Tool

Follow these steps to define your system's attack paths using the TARA Tool.

Step:1 Add a New Attack Tree

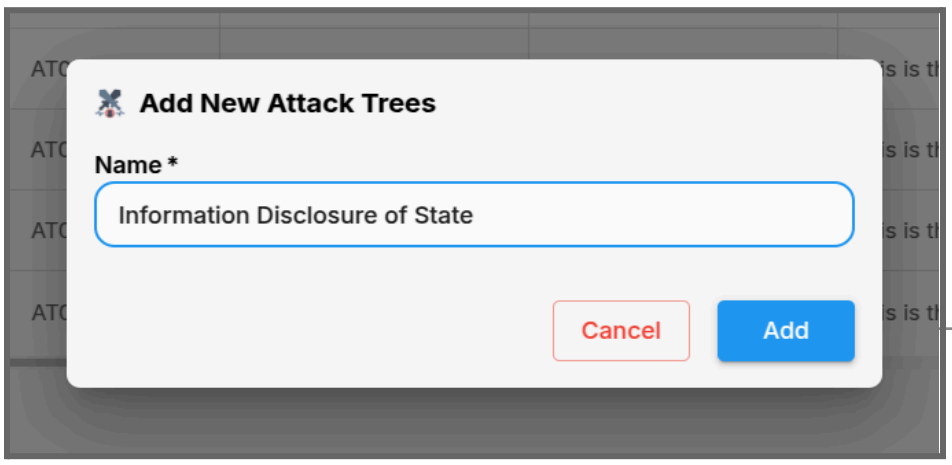
Option A: Using the Sidebar

1. Go to the left sidebar and click on **"Attack Tree"**.
2. Click the **"+" icon** next to Attack Tree. A popup titled **"Add Attack Tree"** will appear.
3. In the popup:

   a. Enter a suitable name (e.g., `SmartHome_Breach_Tree`)

      Click **"Add"**

   b. A confirmation message will appear: **"Added Successfully"**



Option B: Using the Top Navbar

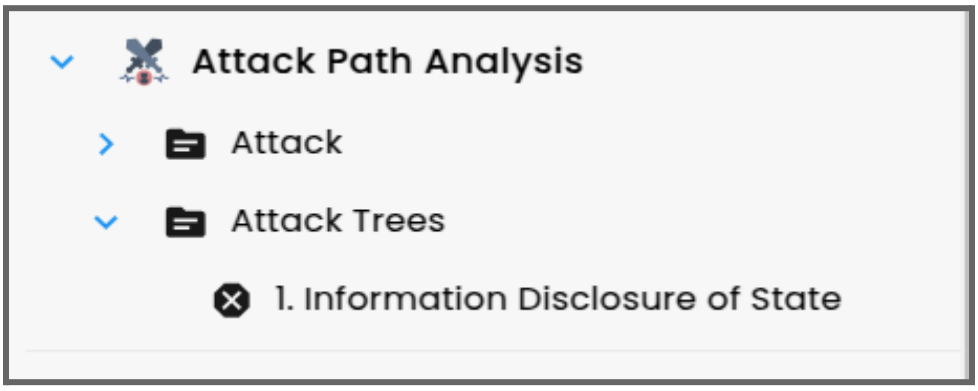
1. Click on **"Attack Path"** from the top navigation bar.
2. In the dropdown, click **"Add Attack"**.
3. Enter the tree name and click **"Add"**.
4. A confirmation message will appear: **"Added Successfully"**

---

step:2 Access and Open Attack Trees

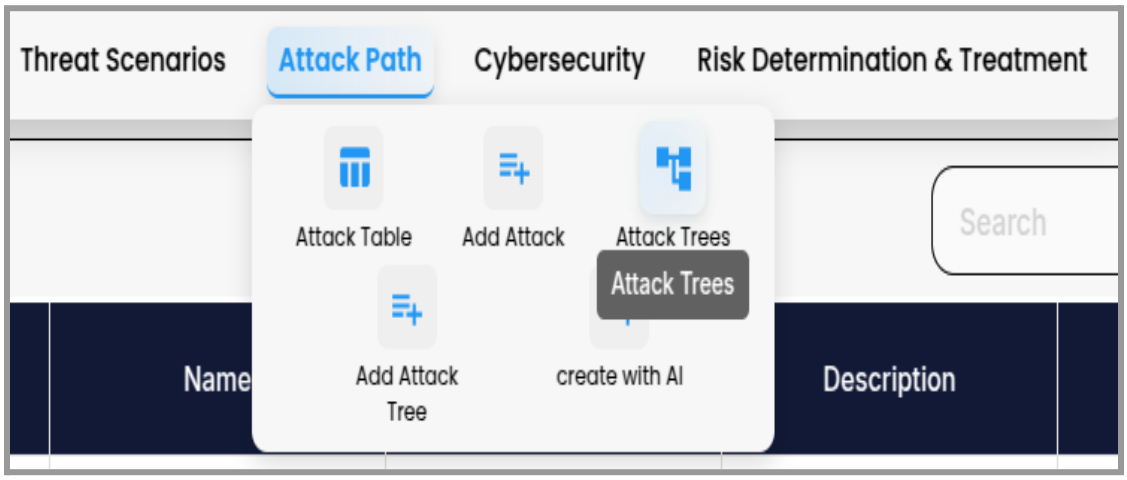
From the Sidebar

- Click the **">" icon** next to Attack Tree to expand the list.
- You will see all existing and newly added attack trees.
- Click a tree name to open the Attack Tree Canvas



From the Navbar

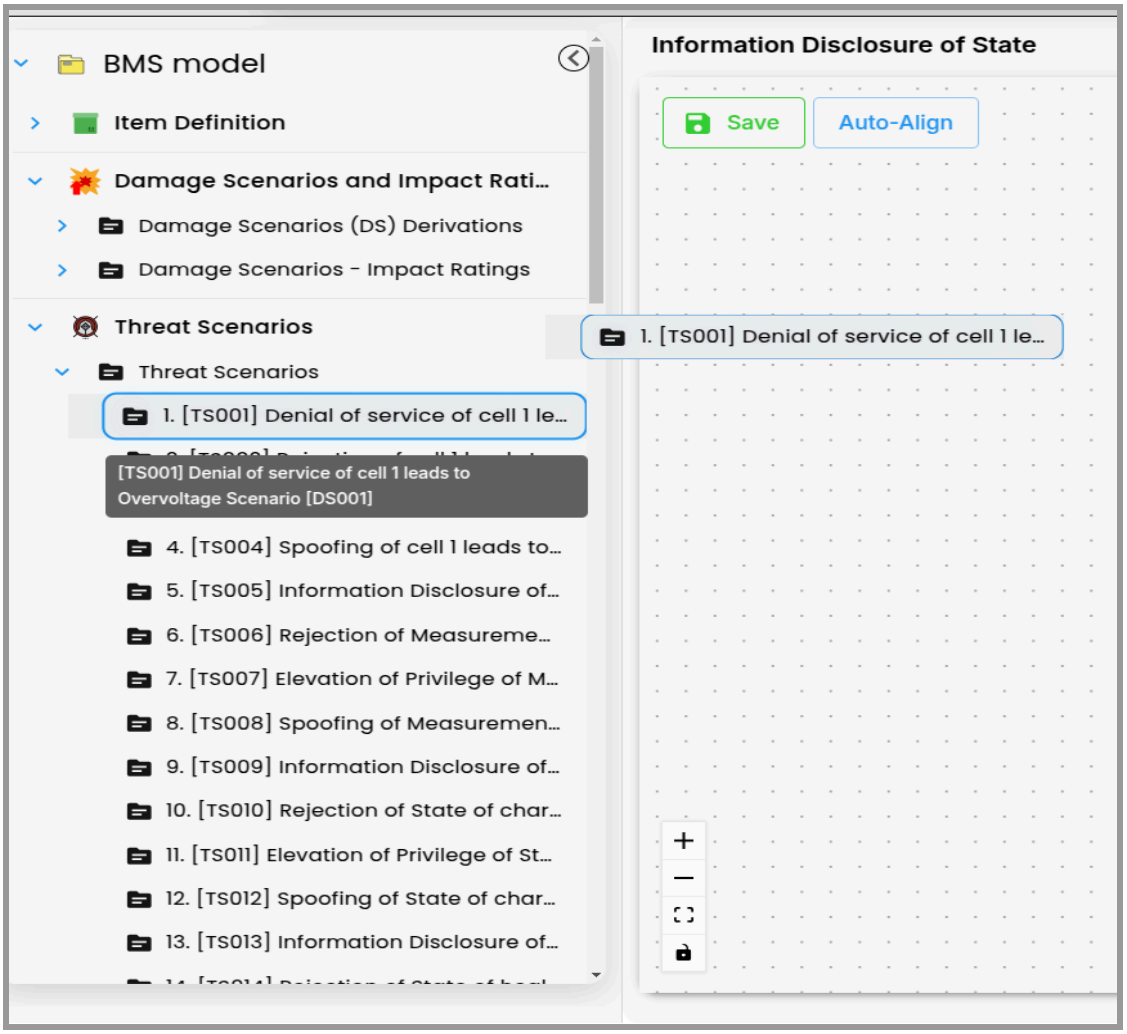
1. Click **"Attack Path"** → **"Attack Trees"**.
2. A popup will list all created trees.
3. Click on any tree to open the canvas for editing.



Step:3 Add Threats to the Attack Tree Canvas

1. In the sidebar, go to **"Threat Scenarios"**.
2. Click the **">" icon** to expand the section.
   You'll see two sub-sections:
   - **Threat Scenarios**
   - **Derived Threat Scenarios**
3. Expand **"Threat Scenarios"** to see all defined threats.
4. Drag and drop desired threats directly onto the canvas.

📌 **Note:** If a threat already exists in the tree, there's no need to add it again.

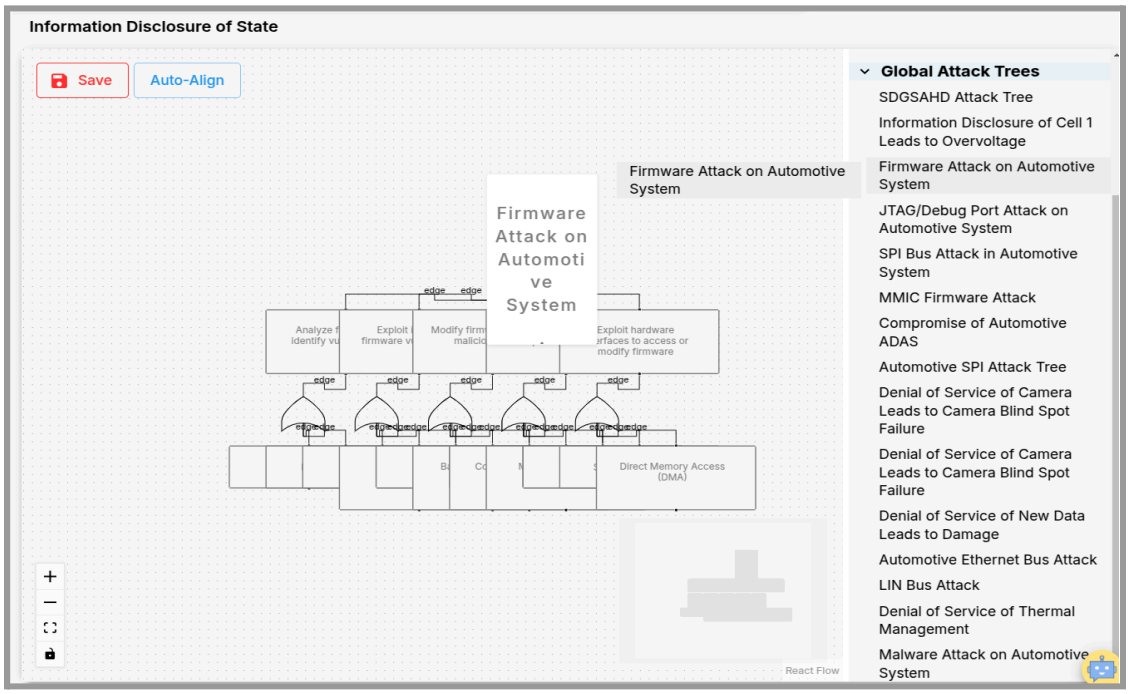


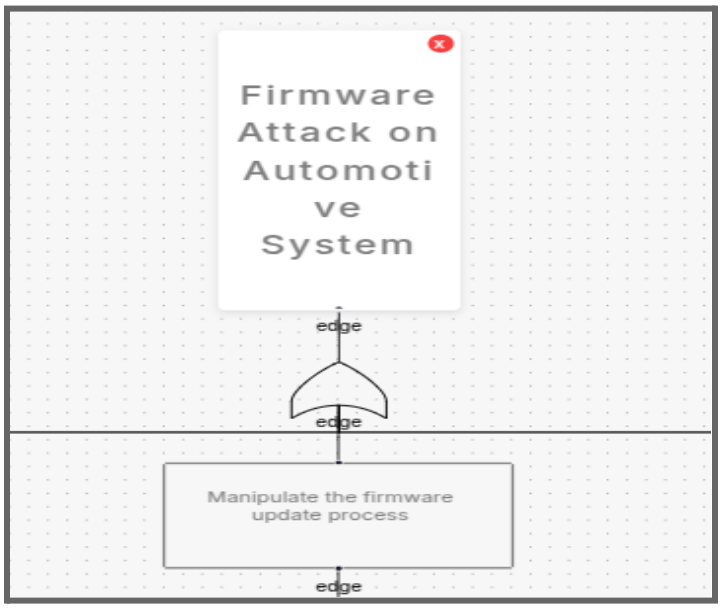
Step:4 Use Global Attack Trees

1. On the right side, under **Global Attack Tree**, you'll find a list of predefined global attack trees.
2. If a global attack tree already exists for the threat you're working on:
    - Drag and drop the global tree into your canvas.
    - This populates the tree with its components.
3. To replace the root node:
    - Hover over the default root node → Click red delete icon
    - Drag your own defined threat from **Threat Scenarios**

- Connect it to the gate

4. Use **"Auto Align"** (top-right) to organize elements.
5. Click **"Save"** (top-left) to store changes.





Step:5 Build a Custom Attack Tree (If Not Found in Global)

Step 1: Add the Threat to the Canvas

1. Go to **Threat Scenarios** in the left sidebar.
2. Drag and drop the desired threat to become the **root node**.

Step 2: Open the Attack Tree Library

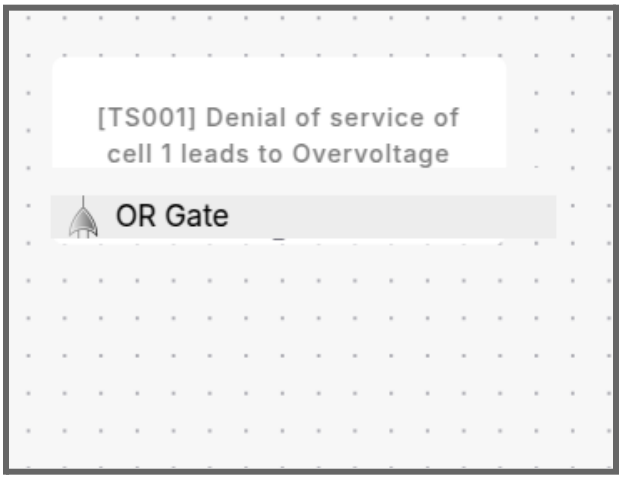
On the right side of the canvas, the library includes:

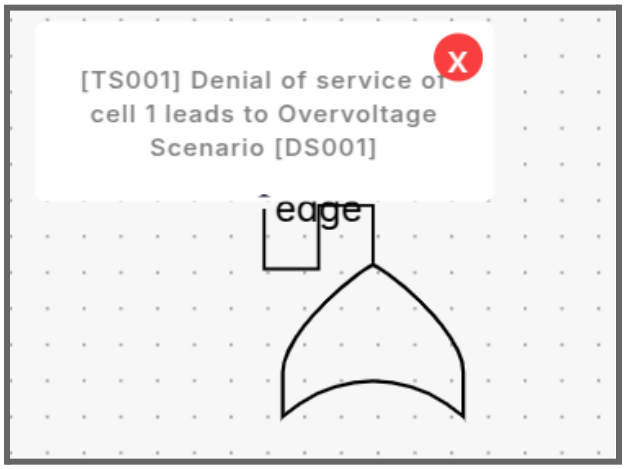
- **Events**
- **Gates** (OR, AND, Voting, Transfer)

Step 3: Build the Tree Structure

Add Gates:

1. Drag & drop a gate onto the threat node.
2. Gate connects automatically, or connect manually using endpoints.





Add Events:

1. Drag & drop events from the library and connect to the gate.
2. Or, drag directly onto the gate for auto-connection.

Step 4: Edit and Arrange the Tree

- Click inside any event to **edit its name**.
- Click **"Auto Align"** to organize layout.
- Click **"Save"** to store.

Step 5: Additional Actions

Copy & Paste:

- Right-click event/gate → Copy → Paste.

Delete Nodes:

- Hover and click the **X icon**, or press Backspace/Delete.

📌 **Important Notes:**

- Each Attack Tree links to **one Threat Scenario** only.
- No more than one root node is allowed.
- Threats and events **cannot connect directly**—use gates in between.

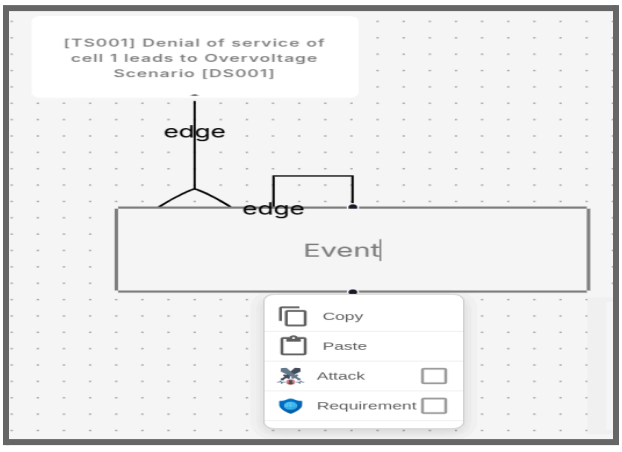
Step:6 Define Nodes (Attack or Requirement)

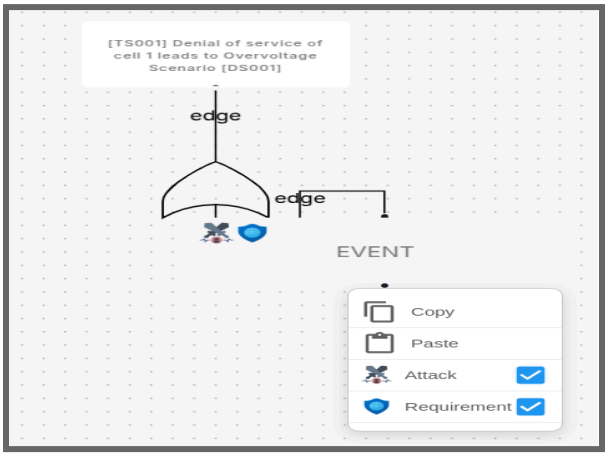
Step 1: Open Node Classification Options

- Right-click on an event node → Popup appears with checkboxes.

Step 2: Classify the Node

- **Attack**: Represents an attack step
- **Requirement**: Represents a security need
- **Both**: If applicable





These are reflected in:

- **Attack Table**
- **Cybersecurity Requirements Table**

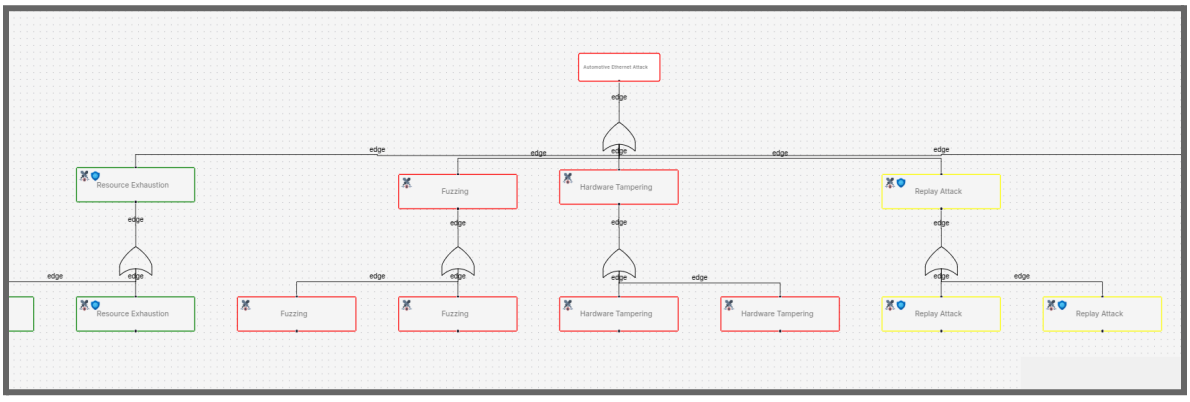
Step 3: Assign Attribute Values (Go to Step 4.1)

1. After classification, go to **Step 4.1**.
2. Assign attribute values → Return to canvas.

Step 4: Visual Feedback – Color Coding

- Nodes get colored by severity:
    - Very Low
    - Low
    - Medium
    - High

- The severity of the root node is calculated automatically based on the values of all connected nodes.
- You will see the severity represented visually by the **color of the root node's border (outline).**



Step 5: Save Your Progress

- Click **"Save"** at top-left to store changes

Step:6 Create an Attack Tree Using AI

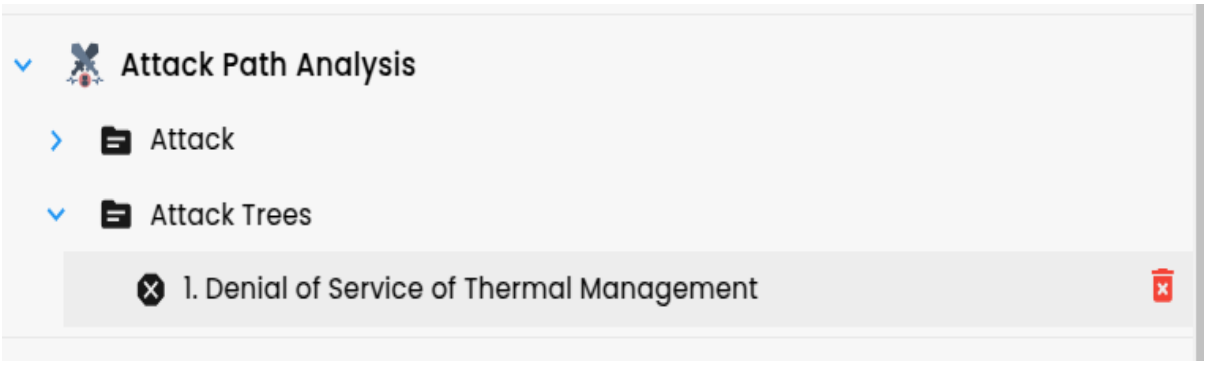
1. From the top navbar: **Attack Path** → **Create With AI**
2. Enter the **Threat Name** → Tree is generated
3. To change the threat name:
    - Follow Global Attack Tree editing steps

Deleting an Attack Tree

1. Hover over the attack tree in the sidebar.
2. Click the **delete button** when it appears.
3. Confirm the deletion when prompted.
4. A success message confirms removal.

If name is too long:

1. Stretch the sidebar.
2. Hover again to reveal the delete button.
3. Click to delete.



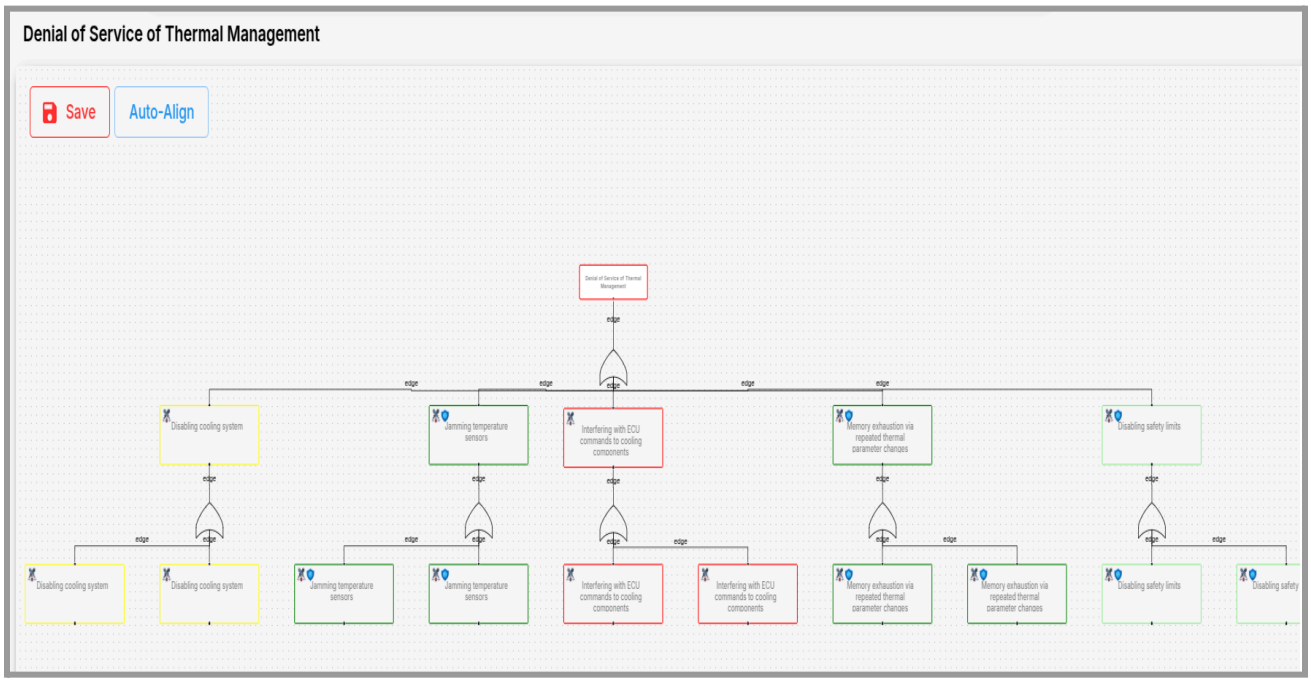


Figure 4.4.2: Structured Attack Tree Diagram

4.5 Step 5: Goals, Claims, and Requirements

This step involves defining and managing key cybersecurity components that outline a system's security objectives, actions, and validation. Cybersecurity Goals represent the desired security outcomes. Cybersecurity Requirements specify the necessary actions to achieve those goals. Cybersecurity Controls are the measures in place to enforce the requirements, and Cybersecurity Claims validate that the system meets specific security conditions.

Example

For a smart home security system, a goal could be "prevent unauthorized access." The requirement might be "implement multi-factor authentication (MFA)" for system access. A corresponding control would be the deployment of MFA as a safeguard. The claim would confirm that "MFA is enforced to block unauthorized entry."

Accessing the Section

From the Sidebar or Top Navbar, navigate to: **Goals, Claims, and Requirements**

Within this section, you will find the following subsections:

- Cybersecurity Goals
- Cybersecurity Requirements
- Cybersecurity Controls
- Cybersecurity Claims

4.5.1 Cybersecurity Goals

The Cybersecurity Goals table outlines the high-level security objectives for your system. These goals ensure the protection and integrity of the system by setting clear, measurable security outcomes.

Adding a New Goal

1. Click on the **"Add New"** button located at the top of the Cybersecurity Goals table.

---

2. In the popup window, provide the following details:
    - **Name**: A short, descriptive name for the goal.
    - **Description**: A detailed explanation of the goal.
3. Under the Related Cybersecurity Controls column, you will see a right and wrong mark. After entering the Name and Description, click the right mark to successfully add the goal.
4. Once you click the right mark, a confirmation message will appear indicating that the goal has been added successfully.
5. Repeat the process to add additional goals.

Editing a Goal

1. Hover over the Name or Description field you want to edit.
2. Click the edit icon (pencil) next to the field to open the editing window.
3. Make the necessary changes and click **Update** to save your edits.

Filtering or Searching Goals

- Click on the **Filter** icon to filter the table by specific columns.
- Use the **Search** bar to search for specific goals by their Name or Description.

Deleting a Goal

1. Click on the S.No (e.g., CG001) of the goal you wish to delete.
2. A red line will appear next to the selected goal.
3. The **Delete** button will become active in the top-right corner. Click the Delete button to delete the goal.

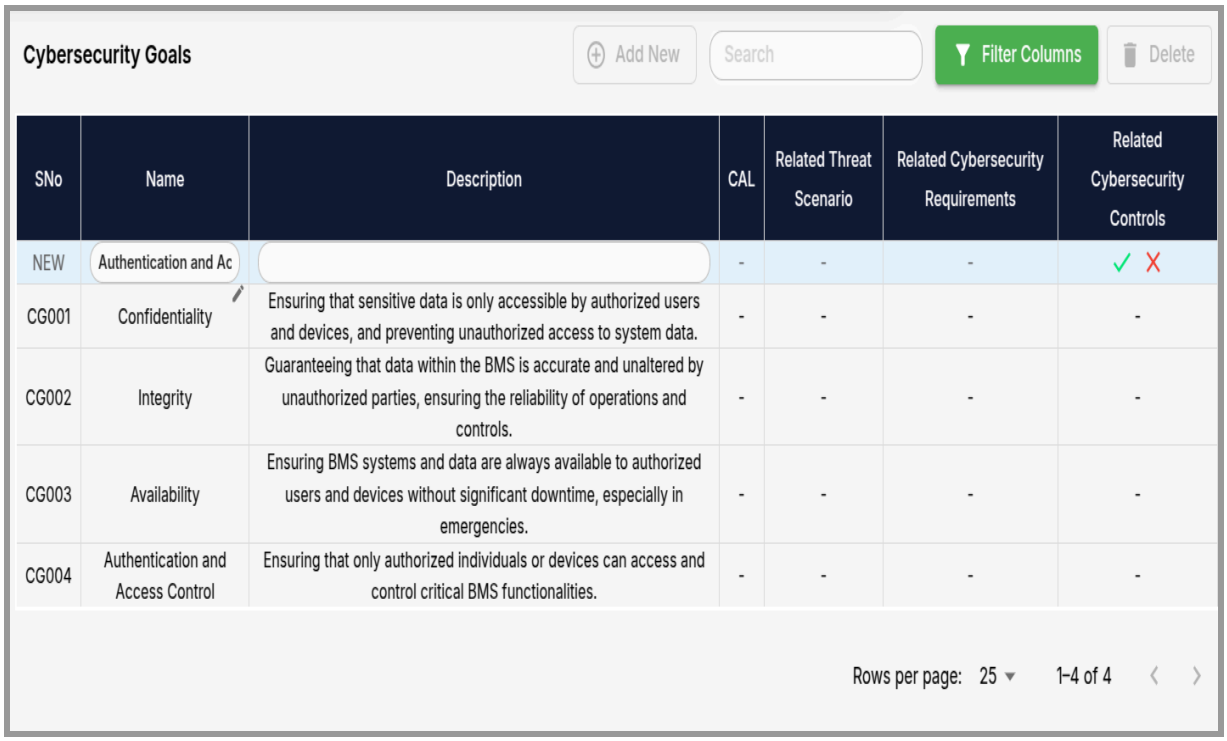


Figure 4.5.1: Sample Table Illustrating Cybersecurity Goals

4.5.2 Cybersecurity Requirements

Cybersecurity Requirements are specific actions or conditions necessary to achieve the cybersecurity goals and safeguard the system.

📌 **Note**: Any requirements defined in the Attack Tree Table (from Step 4) will automatically appear here.

Adding a New Requirement

1. Click on the **"Add New"** button located at the top of the table.
2. In the popup window, provide the following details:
    - **Name**: The name of the requirement.
    - **Description**: A brief explanation of the requirement.
3. Click **Add** to save the requirement.

Editing a Requirement

1. Hover over the Name or Description field you want to edit.
2. Click the edit icon (pencil) to open the editing window.
3. Make the necessary changes and click **Update** to save your edits.

Filtering or Searching Requirements

- Click on the **Filter** button to filter the table by specific columns.
- Use the **Search** bar to locate a specific requirement by its Name or Description.

Deleting a Requirement

1. Click on the S.No (e.g., CR001) of the requirement you wish to delete.
2. A red line will appear to the selected requirement.
3. Click the **Delete** button to remove the requirement.

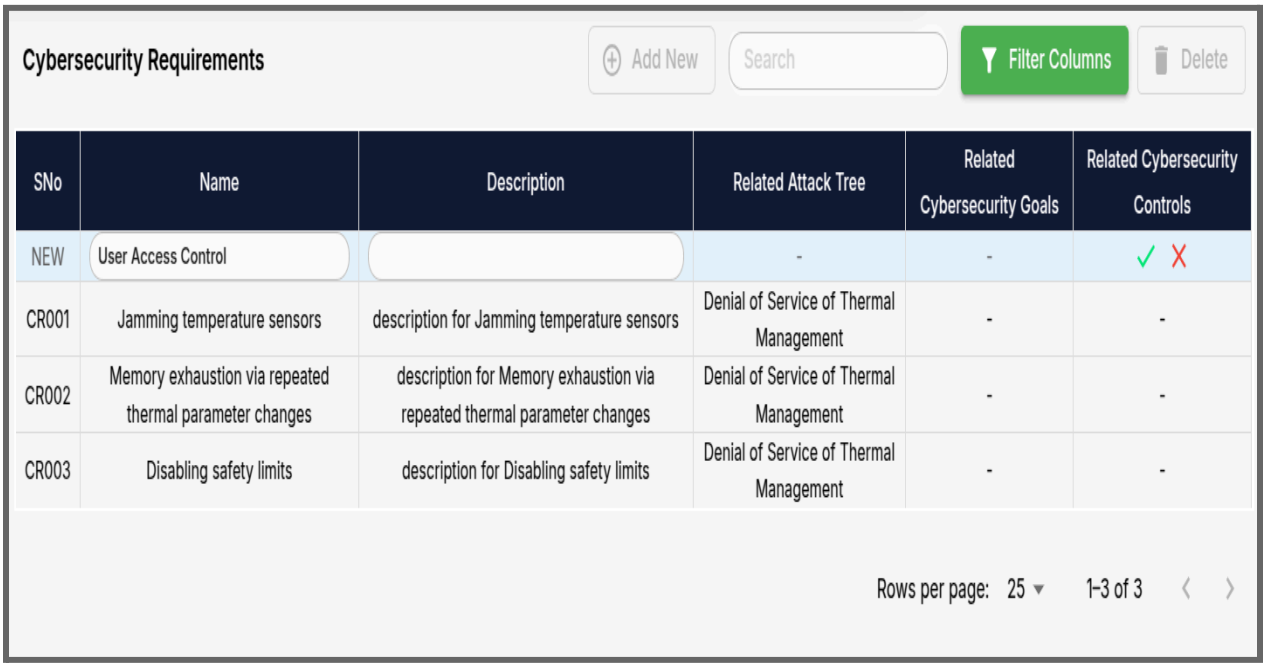


Figure 4.5.2: Sample Table Illustrating Cybersecurity Requirements

4.5.3 Cybersecurity Controls

Cybersecurity Controls are actions, processes, or tools used to enforce the cybersecurity requirements and mitigate risks.

Adding a New Control

1. Click the **"Add New"** button at the top of the table.
2. In the popup window, enter the following details:
    - **Name**: The name of the control.
    - **Description**: A detailed explanation of how the control will mitigate risk.
3. Click **Add** to save the control.

Editing a Control

1. Hover over the Name or Description field you want to edit.
2. Click the edit icon (pencil) to open the editing window.
3. Modify the fields as needed and click **Update** to save the changes.

Filtering or Searching Controls

- Use the **Filter** option to filter the controls by specific columns.
- Use the **Search** bar to find a specific control by Name or Description.

Deleting a Control

1. Click on the S.No (e.g., CL001) of the control you want to delete.
2. A red line will appear to the control.
3. Click the **Delete** button to remove the control.

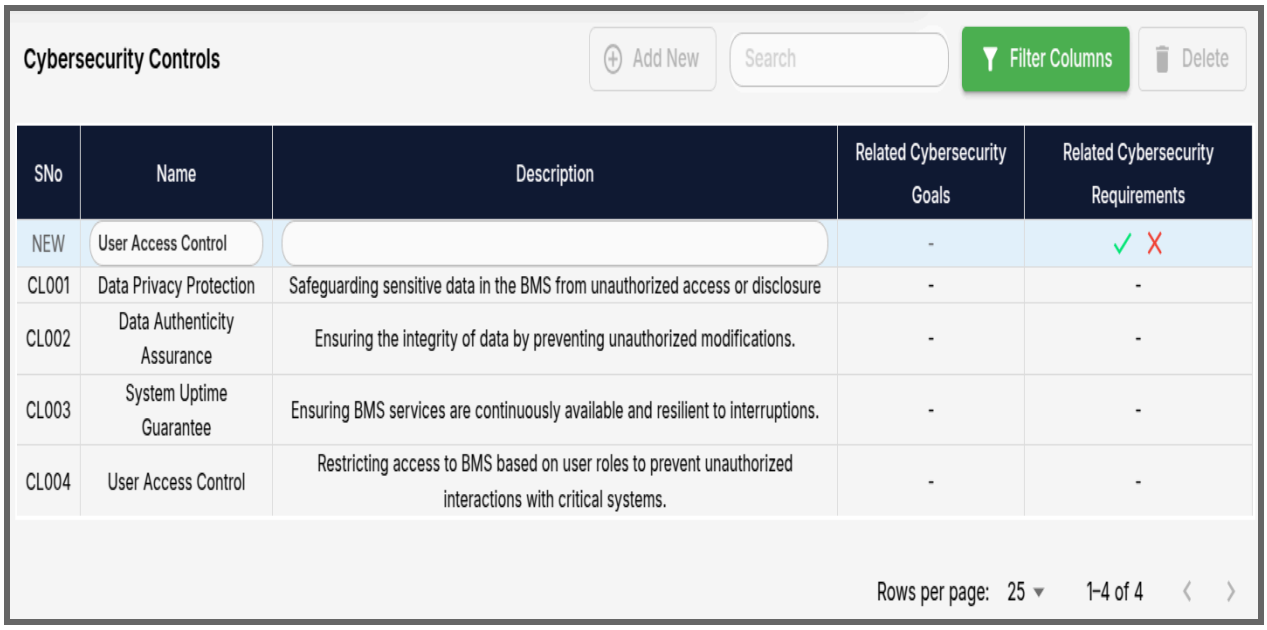


Figure 4.5.3: Sample Table Illustrating Cybersecurity Controls

4.5.4 Cybersecurity Claims

Cybersecurity Claims are statements made about the system's security posture. These claims are typically used for certification, validation, or assurance purposes.

Adding a New Claim

1. Click the **"Add New"** button to open the popup.
2. In the popup window, enter the following details:
    - **Name**: The name of the claim.
    - **Description**: A detailed description of the claim.
    - **Condition for Re-Evaluation**: A condition that may trigger a re-evaluation of the claim.
    - **Related Threat Scenario**: Select a relevant threat scenario from the list.
3. Click **Add** to save the claim

Editing a Claim

1. Hover over the Name or Description field you want to edit.

2. Click the edit icon (pencil) to open the editing window.
3. Modify the necessary details and click **Update** to save the changes.

Filtering or Searching Claims

- Use the **Filter** button to narrow down claims by specific criteria.
- Use the **Search** bar to find specific claims by Name or Description.

Deleting a Claim

1. Click on the S.No (e.g., CC001) of the claim you wish to delete.
2. A red line will appear next to the selected claim.
3. Click the **Delete** button to remove the claim.

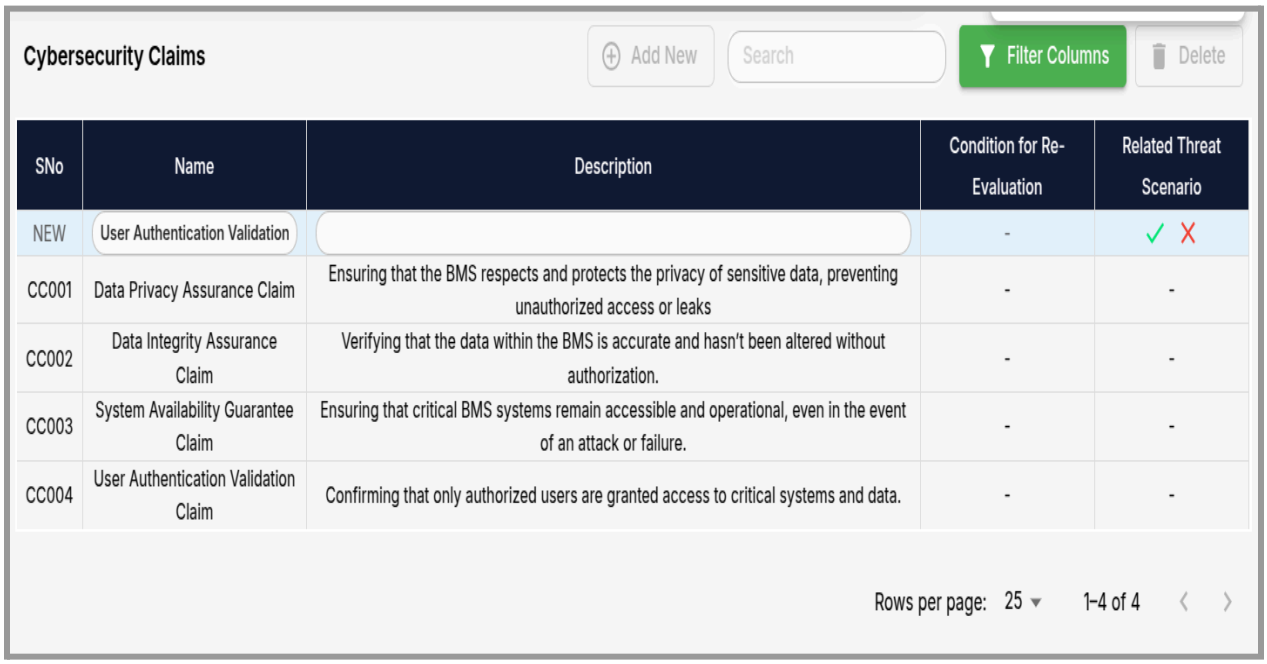


Figure 4.5.4: Sample Table Illustrating Cybersecurity Claims

4.6 Step 6: Catalogs

In this step, you'll explore standardized cybersecurity references defined under **UN Regulation No. 155 (Annex 5)**, which help identify typical threats, vulnerabilities, and mitigation strategies relevant to vehicle systems. This content is for **reference and understanding only** — you **do not need to make changes**, just review and take notes as needed.

4.6.1 Accessing the Catalogs

From the **sidebar**, click on: **Catalogs → UNICE R.155 Annex 5 (WP.29)**Under this section, you'll see multiple categorized reference catalogs:

4.6.2 Threat Categories

- **Threats – Back-end servers associated with vehicle field operations**
  Concerns potential risks associated with servers that support vehicle operations remotely.
- **Threats – Vehicle communication channel vulnerabilities**
  Addresses weaknesses in the communication pathways between vehicle components.
  Threats – Vehicle update procedures and their risks
  Highlights potential issues during the process of updating vehicle software or firmware.
- **Threats – Human actions unintentionally enabling cyberattacks on vehicles**
  Focuses on risks arising from human errors that might expose vehicles to cyber threats.
- **Threats – Vehicles from external connectivity and network connections**
  Pertains to vulnerabilities introduced through external connections like Wi-Fi or Bluetooth.
- **Threats – Vehicle data and software integrity**
  Concerns the preservation of data accuracy and software reliability within the vehicle.

Back-end Servers Associated with Vehicle Field Operations Table

Search

ID	Name	Category	Example
4.3.1.	Threats regarding back-end servers related to vehicles in the field	Vehicle related data held on back-end servers being lost or compromised	1. Abuse of privileges by staff (insider attack)
			2. Loss of information in the cloud due to attacks
4.3.1.	Threats regarding back-end servers related to vehicles in the field	Back-end servers used as a means to attack a vehicle or extract data	1. Abuse of privileges by staff (insider attack)
			2. Unauthorized internet access to the server
			3. Unauthorized physical access to the server
4.3.1.	Threats regarding back-end servers related to vehicles in the field	Services from back-end server being disrupted, affecting the operation of a vehicle	1. Attack on back-end server stops it functioning

Rows per page: 25 1–6 of 6

4.6.3 Vulnerability Category

- **Potential vulnerabilities in vehicles if not properly secured or hardened**
  Identifies weaknesses that could be exploited if vehicles are not adequately protected.

Vulnerability Table

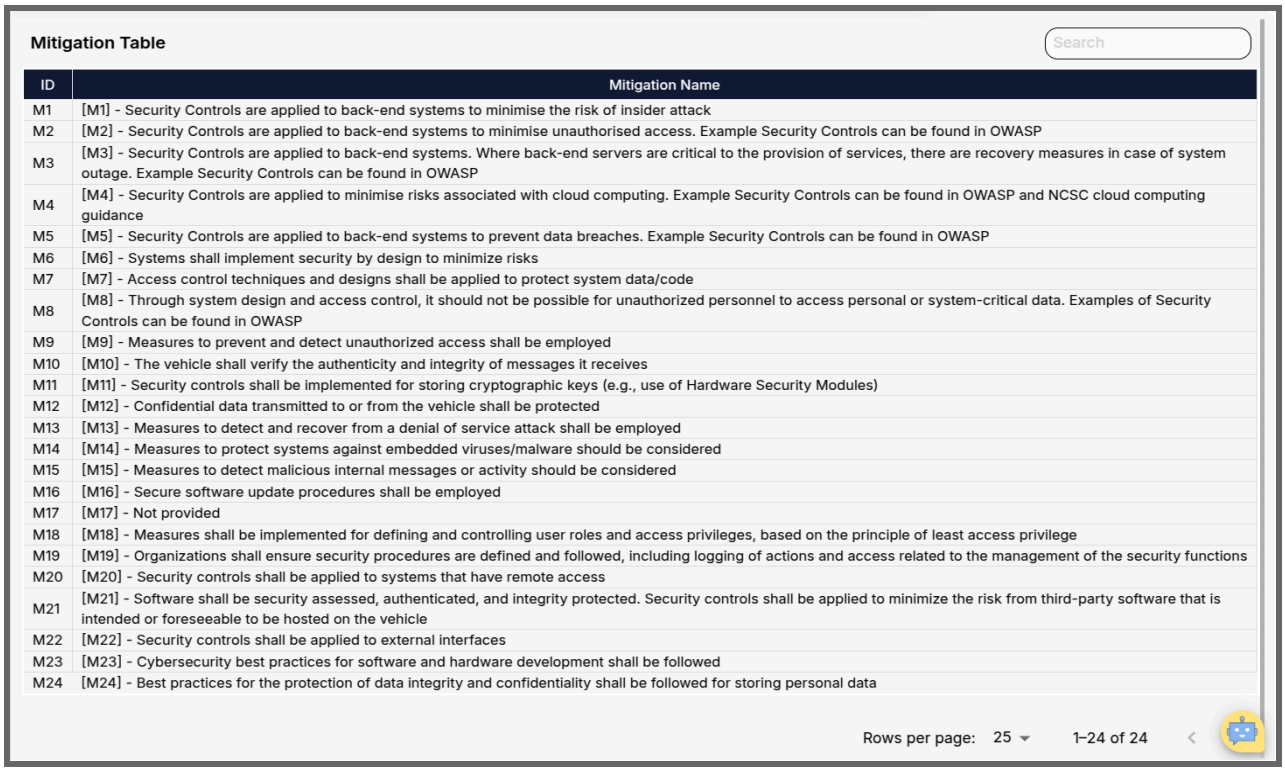
Search

Scene ID	Scene Name
[1.1]	[1.1] - Vehicle related data held on back-end servers being lost or compromised
[1.2]	[1.2] - Back-end servers used as a means to attack a vehicle or extract data
[1.3]	[1.3] - Services from back-end server being disrupted, affecting the operation of a vehicle
[2.1]	[2.1] - Spoofing of messages or data received by the vehicle
[2.2]	[2.2] - Communication channels used to conduct unauthorized manipulation, deletion or other amendments to vehicle held code/data
[2.3]	[2.3] - Communication channels permit untrusted/unreliable messages to be accepted or are vulnerable to session hijacking/replay attacks
[2.4]	[2.4] - Information can be readily disclosed. For example, through eavesdropping on communications or through allowing unauthorized access to sensitive files or folders
[2.5]	[2.5] - Denial of service attacks via communication channels to disrupt vehicle functions
[2.6]	[2.6] - An unprivileged user is able to gain privileged access to vehicle systems
[2.7]	[2.7] - Viruses embedded in communication media are able to infect vehicle systems
[2.8]	[2.8] - Messages received by the vehicle (for example X2V or diagnostic messages), or transmitted within it, contain malicious content
[3.1]	[3.1] - Misuse or compromise of update procedures
[3.2]	[3.2] - It is possible to deny legitimate updates
[4.1]	[4.1] - Legitimate actors are able to take actions that would unwittingly facilitate a cyberattack
[5.1]	[5.1] - Devices connected to external interfaces used as a means to attack vehicle systems
[5.2]	[5.2] - Manipulation of the connectivity of vehicle functions enables a cyberattack
[5.3]	[5.3] - Manipulation of the connectivity of vehicle functions enables a cyberattack
[6.1]	[6.1] - Extraction of vehicle data/code
[6.2]	[6.2] - Manipulation of vehicle data/code
[6.3]	[6.3] - Erasure of data/code
[6.4]	[6.4] - Introduction of malware
[6.5]	[6.5] - Introduction of new software or overwrite existing software
[6.6]	[6.6] - Disruption of systems or operations
[6.7]	[6.7] - Manipulation of vehicle parameters
[7.1]	[7.1] - Parts or supplies could be compromised to permit vehicles to be attacked

Rows per page: 25 1–25 of 30

4.6.4 Mitigation Category

- **Mitigations**
  Proposes strategies to reduce or eliminate identified threats and vulnerabilities.



Mitigation Table

Search

ID	Mitigation Name
M1	[M1] - Security Controls are applied to back-end systems to minimise the risk of insider attack
M2	[M2] - Security Controls are applied to back-end systems to minimise unauthorised access. Example Security Controls can be found in OWASP
M3	[M3] - Security Controls are applied to back-end systems. Where back-end servers are critical to the provision of services, there are recovery measures in case of system outage. Example Security Controls can be found in OWASP
M4	[M4] - Security Controls are applied to minimise risks associated with cloud computing. Example Security Controls can be found in OWASP and NCSC cloud computing guidance
M5	[M5] - Security Controls are applied to back-end systems to prevent data breaches. Example Security Controls can be found in OWASP
M6	[M6] - Systems shall implement security by design to minimize risks
M7	[M7] - Access control techniques and designs shall be applied to protect system data/code
M8	[M8] - Through system design and access control, it should not be possible for unauthorized personnel to access personal or system-critical data. Examples of Security Controls can be found in OWASP
M9	[M9] - Measures to prevent and detect unauthorized access shall be employed
M10	[M10] - The vehicle shall verify the authenticity and integrity of messages it receives
M11	[M11] - Security controls shall be implemented for storing cryptographic keys (e.g., use of Hardware Security Modules)
M12	[M12] - Confidential data transmitted to or from the vehicle shall be protected
M13	[M13] - Measures to detect and recover from a denial of service attack shall be employed
M14	[M14] - Measures to protect systems against embedded viruses/malware should be considered
M15	[M15] - Measures to detect malicious internal messages or activity should be considered
M16	[M16] - Secure software update procedures shall be employed
M17	[M17] - Not provided
M18	[M18] - Measures shall be implemented for defining and controlling user roles and access privileges, based on the principle of least access privilege
M19	[M19] - Organizations shall ensure security procedures are defined and followed, including logging of actions and access related to the management of the security functions
M20	[M20] - Security controls shall be applied to systems that have remote access
M21	[M21] - Software shall be security assessed, authenticated, and integrity protected. Security controls shall be applied to minimize the risk from third-party software that is intended or foreseeable to be hosted on the vehicle
M22	[M22] - Security controls shall be applied to external interfaces
M23	[M23] - Cybersecurity best practices for software and hardware development shall be followed
M24	[M24] - Best practices for the protection of data integrity and confidentiality shall be followed for storing personal data

Rows per page: 25 1–24 of 24

Glossary of Terms

Term	Meaning
Threat	Something that **could happen** and cause harm to your system or data.
Vulnerability	A **weakness** in the system that could be used by attackers.
Mitigation	A **protective measure** that reduces risk or impact of a threat.
Back-end servers	Servers used to support services like remote updates or diagnostics.
Communication channels	Ways devices in the vehicle talk to each other or the cloud.

What to Do Here

- Click each **catalog name** to **view its table**.
- Carefully **read** and **understand** the listed threats, vulnerabilities, and mitigations.
- **Make notes** of entries that may apply to your system (e.g., Smart Locks, CAN Bus, etc.).

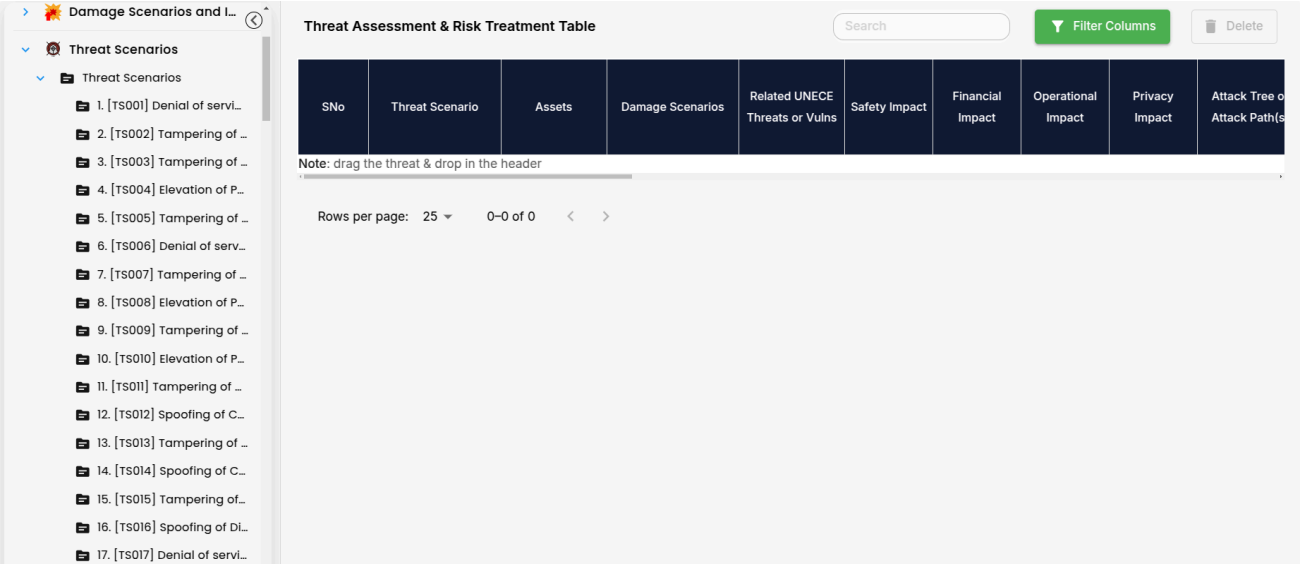
📌 **Note:** You **cannot add, edit, or delete** entries in these tables — they are global standards for reference only.

4.7 Step 7: Risk Determination and Risk Treatment Decision

In this step, you will assess the identified threats and determine appropriate actions to manage associated cybersecurity risks. This includes mapping each threat to system impacts, relevant catalogs, goals, and claims to ensure comprehensive risk evaluation and treatment.

4.7.1 Accessing the Threat Assessment & Risk Treatment Table

1. Navigate to the Sidebar or Navbar.
2. Click on **Risk Determination and Risk Treatment Decision**.
3. From the dropdown, select **Threat Assessment & Risk Treatment**.
4. You will see an empty table, which will populate once threats are added.



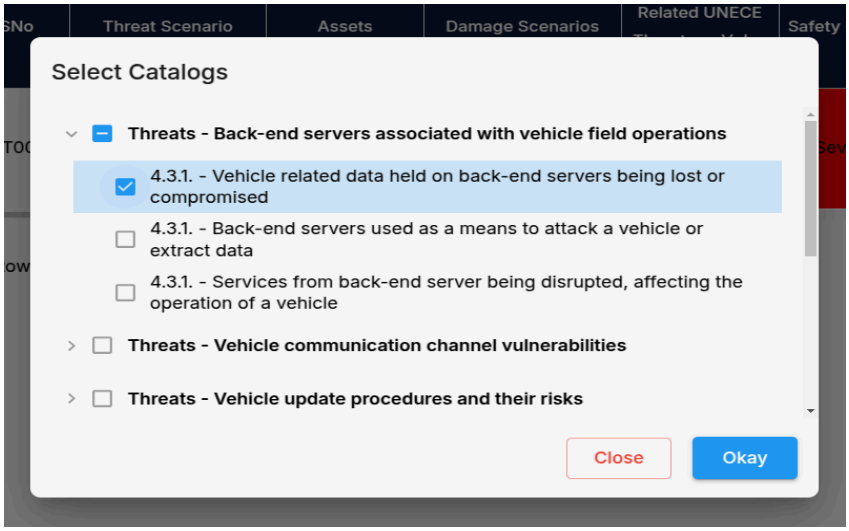
4.7.2 Adding Threats to the Table

1. In the Sidebar, expand the **Threat Scenarios** section by clicking the **>** icon.
2. You will see two categories:
    - Threat Scenarios
    - Derived Threat Scenarios
3. Click on **Threat Scenarios** to view all available threats.
4. Drag and drop the desired threat(s) onto the table header.

5. This action will auto-generate a new row for each threat with pre-filled data.

4.7.3 Catalog Selection

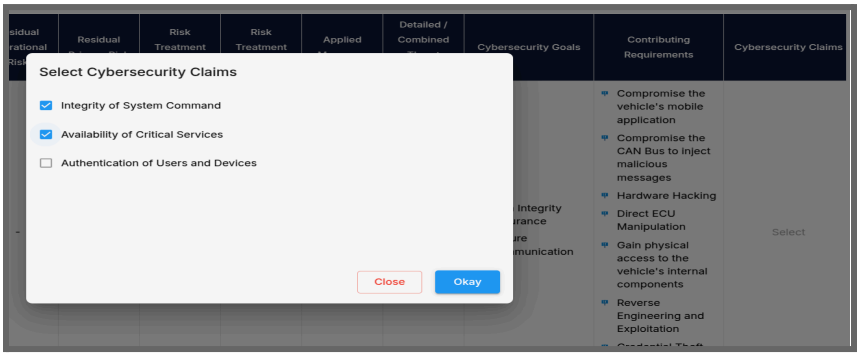
1. Under the **Catalog** column in the table, click on **Select Catalog**.
2. A dialog will appear with a list of catalog items.
3. Select the appropriate catalogs and click **OKAY**.
4. A success message will confirm: ✅ "Catalog added successfully."



4.7.4 Linking Goals and Claims

In the **Cybersecurity Goals** and **Cybersecurity Claims** columns:

1. Click to open a list of existing goals or claims.
2. Select the ones that apply to the threat.



3. These links provide traceability and context for risk treatment decisions.

Deleting a Threat

To remove a threat from the Threat Assessment & Risk Treatment table:

1. Click on the **S.No** of the threat row (e.g., RT001).
2. The entire row will be highlighted in gray.
3. The **Delete** button (located at the top-right corner) will now be enabled.
4. You can also select multiple rows the same way and delete them together.

Filtering Columns

To simplify your view or focus on specific data:

1. Click the **"Filter Columns"** button at the top of the table.
2. Select the columns you want to show or hide.
3. This helps customize your view for easier analysis.

📌 Important Notes

- You can only edit the **Catalog**, **Cybersecurity Goals**, and **Cybersecurity Claims** columns directly in this table.

- If any other data (e.g., threat description, impact details) needs changes, you must go to the original source column or module (e.g., Attack Tree or Threat Scenarios) to edit it. Changes will then automatically reflect here.
- You **cannot add the same threat more than once** to this table. Attempting to re-add an already added threat will be ignored.

- Ensure that relevant Catalogs, Goals, and Claims are properly linked to each threat scenario for complete and traceable risk treatment.

4.8 Step 8: Reporting

In this step, you will generate a report of your cybersecurity analysis and risk assessment. You can select the components you want to include in the report and download it in PDF format.

4.8.1 Accessing the Reporting Feature

1. Navigate to the Sidebar.
2. Click on **Reporting**.
3. A pop-up titled **Document Report** will appear.

4.8.2 Selecting Components for the Report

In the pop-up window, you will see a list of components you can include in the report. These components are:

- Item Definition
- Damage Scenarios and Impact Ratings
- Damage Scenarios - Impact Ratings
- Threat Scenarios
- Derived Threat Scenarios
- Attack Path Analysis and Attack Feasibility Rating
- Risk Determination and Risk Treatment Decision
- Threat Assessment & Risk Treatment

Select the items you want to include in your report.

4.8.3 Downloading the Report

1. After selecting the desired components, click on the **Download** button.
2. The document will be generated and opened in a new tab.
3. In the top-right corner of the document, you will see a **Download** icon.
4. Click on the **Download** icon to save the report in PDF format on your laptop.

Final Notes

- Ensure that you select the necessary components relevant to your analysis before downloading the report.
- After downloading, you can recheck the report or share it for further evaluation or review.