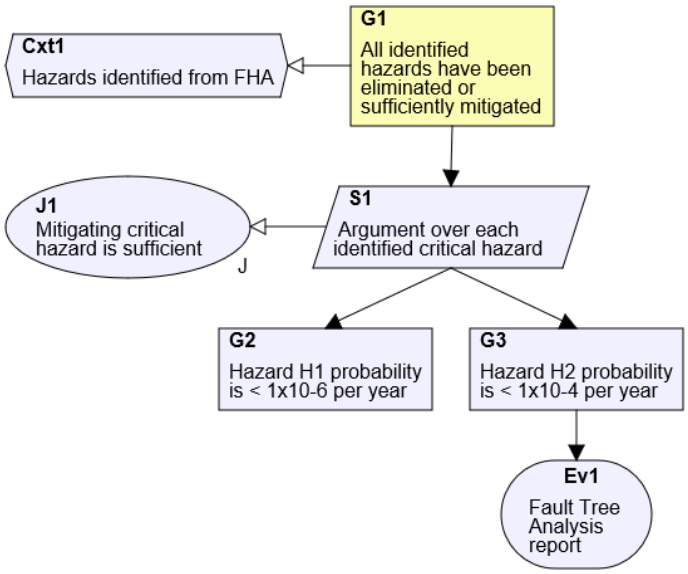
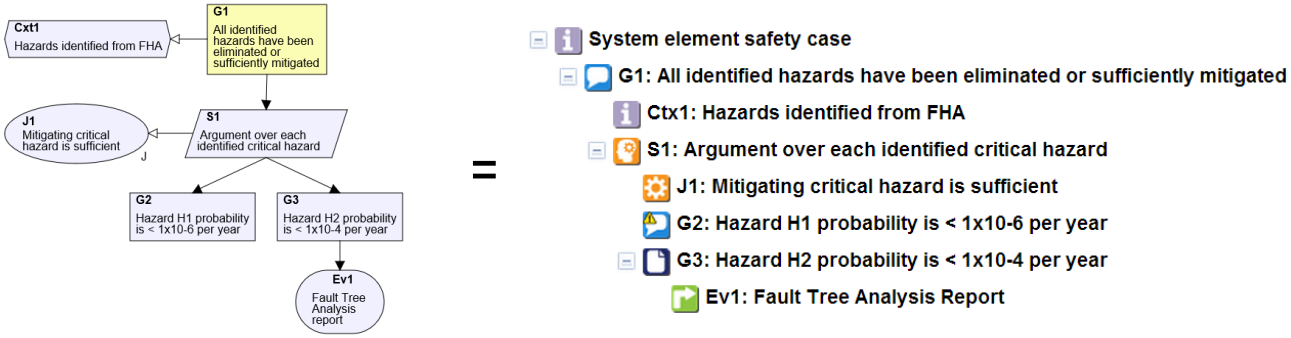
Building Safety Cases with NOR-STA
Step by Step Introduction

NOR-STA is a software tool dedicated for construction, assessment and maintenance of argument structures (assurance cases, safety cases etc.). To demonstrate this we will build a simple argument with NOR-STA. Let's build an argument presented in the figure:



First of all **NOR-STA is focused on the argument structure – it is not a graphics-oriented tool**. In NOR-STA your work will be focused on logical structure of the argument and NOR-STA provides features supporting effective management of large and complex assurance cases. If you need diagrams they can be generated by NOR-STA in reports.

Argument structure is presented in NOR-STA as a tree-like structure with the root element on the left and supporting elements expanding down and to the right. Type of each element is indicated by an icon.



I assume you are already familiar with the concept of safety cases (assurance cases). If you need some introduction to the subject you can refer to other publications.

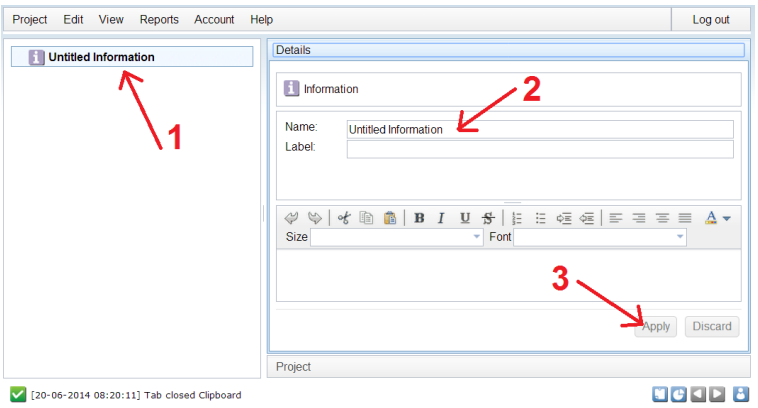
GSN is currently the most widely used notation for safety case argumentation. NOR-STA has been developed independently from GSN and you will find minor differences in the structure of an argument. We will go step by step through the process of creating an argument and I will explain the differences and how to manage it.

Now let's get to work and create the argument.

Step 1. Create your first claim

When you start working on a new project, you begin your work with a single information element – it is the root of your argument structure. Each time you want to add an element to the argument you have to attach it to an existing element. This approach suggests top-down approach, however working bottom-up is also possible.

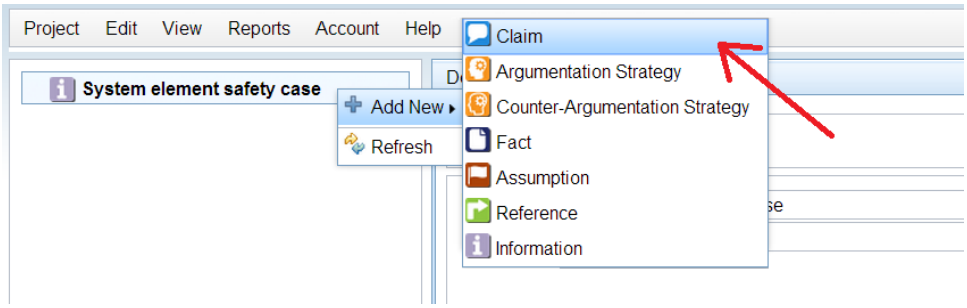
The root element is unnamed when we begin our work. Let's give it a name:



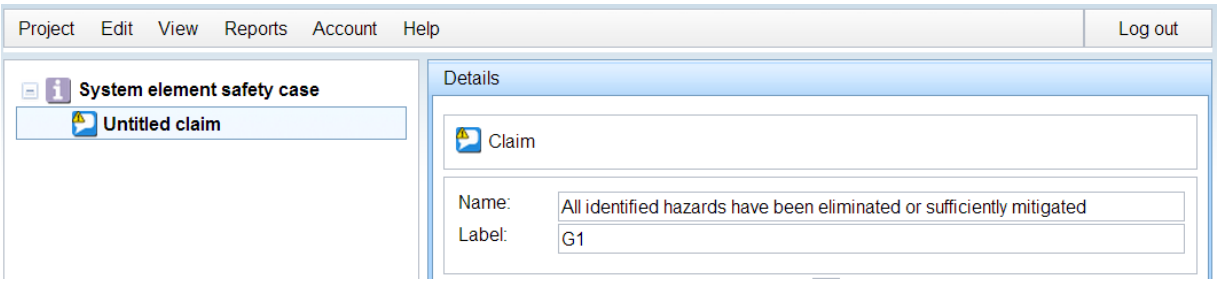
1) Click on the information element (follow action 1 on the figure above).
2) Click on the name field in the details panel and enter the name, for example "System element safety case".
3) Press enter or click on **`Apply`** button.

Now we are ready to create the first claim.

Right-click on the root node and select **`Add new`** → **`Claim`** action in the context menu:

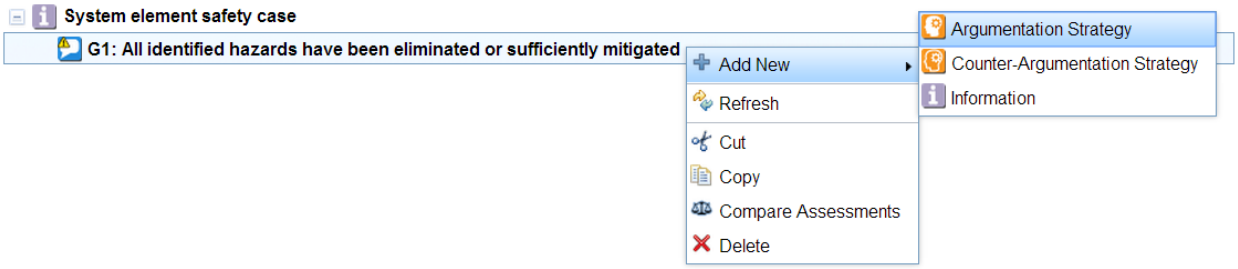


New claim element will appear in the argument on the left. Give it a name and a label in the details panel on the right.

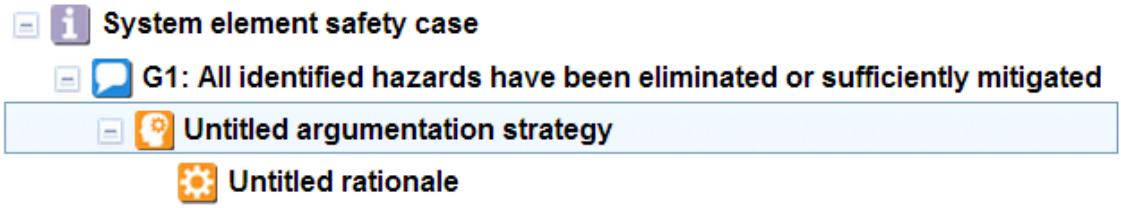


Step 2. Create argument

For now we have two element of our argument structure: the root node and the claim. Right-click on the claim and select **`Add new`** → **`Argumentation strategy`** action.

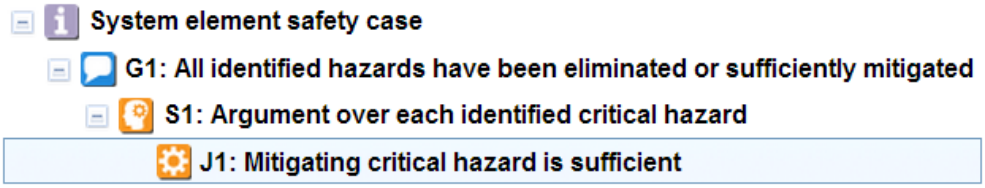


Please note that not one but two new elements have been created: argumentation strategy and its justification (called “rationale”).



Justification (rationale) for an argumentation strategy is obligatory in NOR-STA (not optional like in GSN).

We can give names and labels to the argumentation strategy and its justification to get argument like this:



NOR-STA argument tree has just one type of relation: ancestor-descendant. Each element (except the root element) has one parent. It is sufficient for representing any argument. GSN provides two types of links between elements: supported-by (rendered as a line with a solid arrowhead) and in-context-of (rendered as a line with a hollow arrowhead). The type of relation depends directly on the types of related elements..

Step 3. Add premises

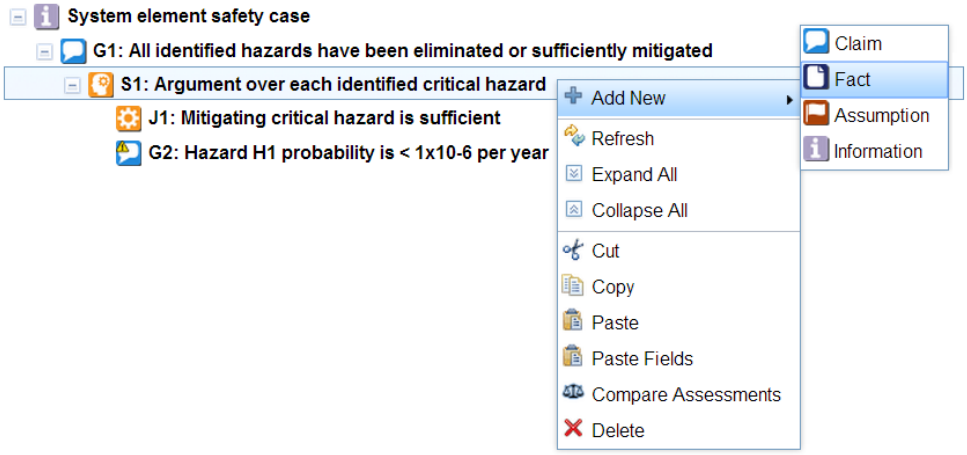
When specifying premises in NOR-STA you should be aware of strict distinction between two types of premises:

- **`fact`** is a premise supported directly by an evidence document and
- **`claim`** is a premise supported by its own argumentation strategy.

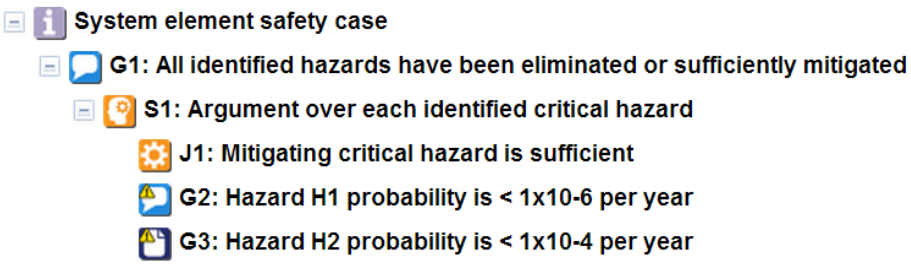
Premises supported directly by evidence are denoted as **`facts`** in NOR-STA.
It distinguishes them from **`claims`** which are to be backed by an argumentation strategy.

Let's assume that we have two hazards. One of them is more complex and we will use claim supported by an argumentation strategy how we mitigate it. We will add claim **G2**: **`Hazard H1 probability is less than 1×10`**$^{-6}$ **`per year`**.

The second hazard is simpler and not so severe. Let's say the FTA analysis report will be sufficient evidence for it. We will define the premise as a fact **`Hazard H2 probability is less than 1×10`**$^{-4}$ **`per year`**.



Now we have almost complete argument with two premises:

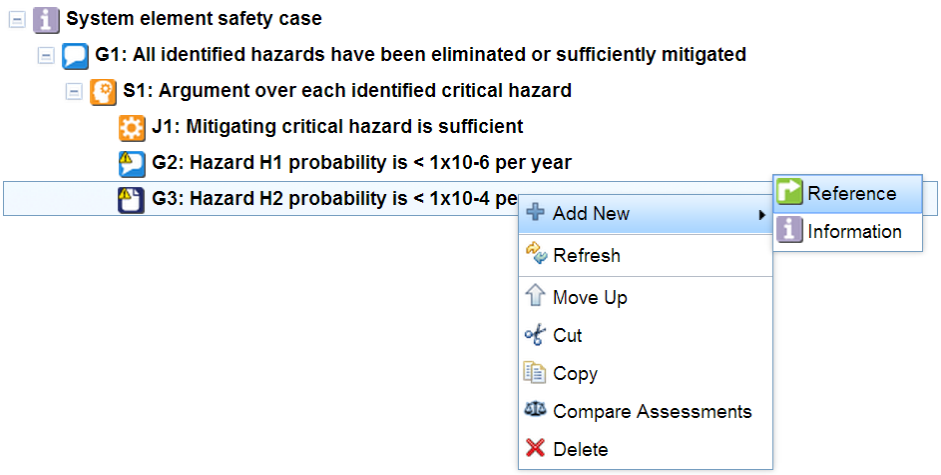


Please note yellow attention signs (⚠) displayed in two element icons to indicate that these two elements are not fully developed at the moment (missing evidence or argumentation strategy).

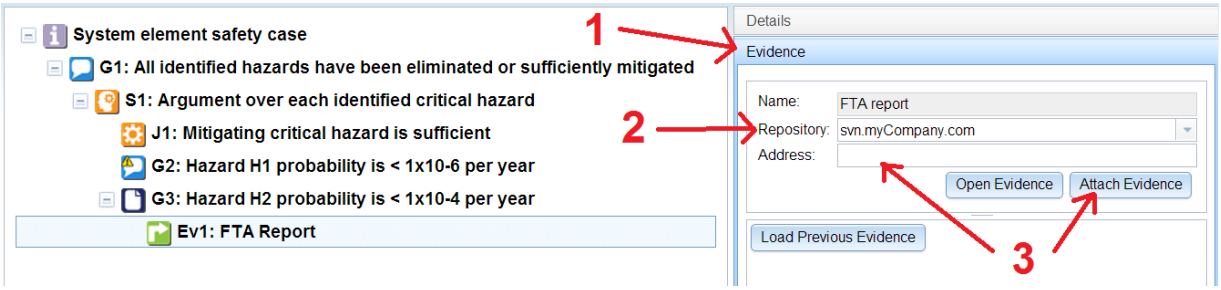
Step 4. Support premises with the evidence

I assume We have Fault Tree Analysis report ready to be used as evidence for G3. All the evidence is external to NOR-STA argument and the connection is defined as a **reference**.

Right-click on G3 element and select **Add new** → **Reference**:



Evidence documents can be stored in various repositories. You can use NOR-STA internal repository and put all the documents there. However, usually it is convenient to use references to documents in your own repository. This way you can be sure NOR-STA will refer always to current version of the document.



To set reference to the evidence document click on the element and follow action presented on the figure above:

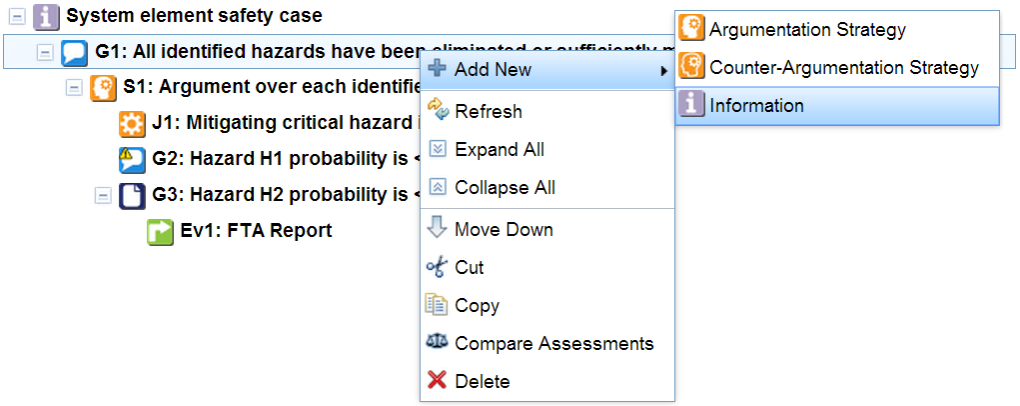
1) Open **Evidence** panel on the right side (find the title bar of the panel and click on it).
2) Chose repository name. If you need access to any new repository contact the system administrator.
3) Enter direct address of the evidence document (any http address will work) or use **Attach Evidence** button to add the document to NOR-STA repository manually.

NOR-STA argument can be supported by the evidence in its internal repository or stored in any external repository that is managed independently.
You do not need to store any repository passwords in NOR-STA.

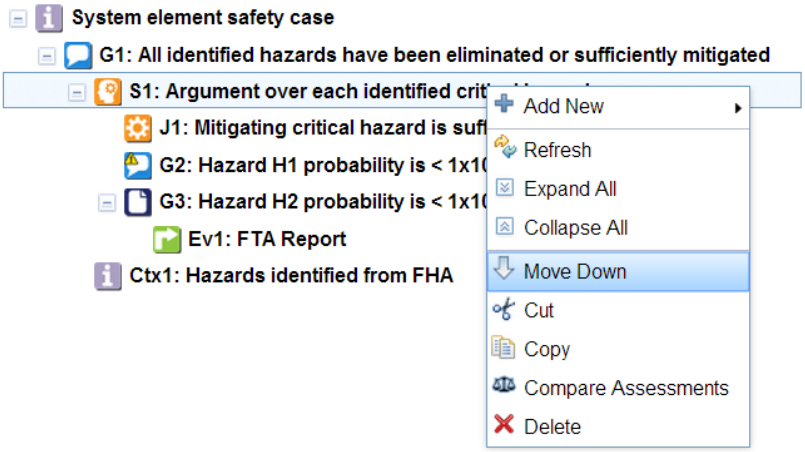
Step 5. Context

Our safety case is still incomplete. The whole argument depends on the hazard list but it's missing in our safety case. G1 claim refers to "all identified hazards" therefore the hazard log should be defined as a context for this claim. As the top claim context is inherited down the structure it will apply to all safety case elements below the claim.

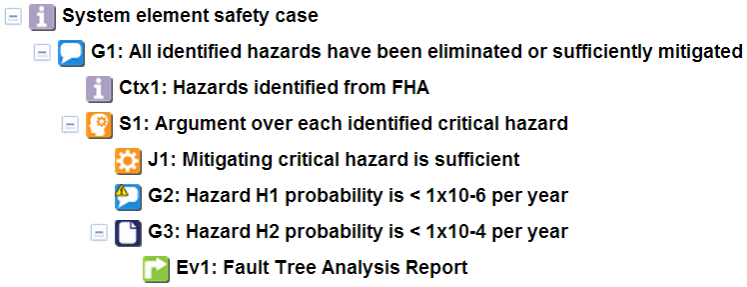
To add context to the claim right-click on the claim and select **`Add new → Information`** action. Then we define it as **`Ctx1`** named **`Hazards identified from FHA`**.



New element will be added at the bottom, below the existing elements. Context and argumentation strategy are linked directly to the claim. I want the context Ctx1 to be above the strategy S1. You can change the order of elements using **`move down`** and **`move up`** function in the context menu (right-click on the element to open the menu).



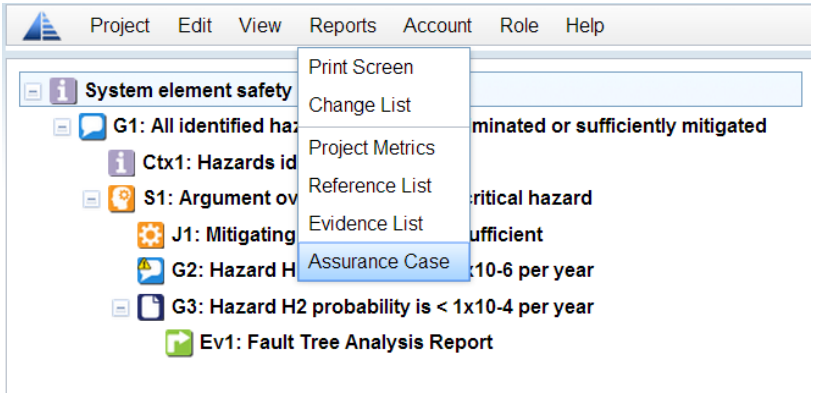
Now we have our final argument structure:



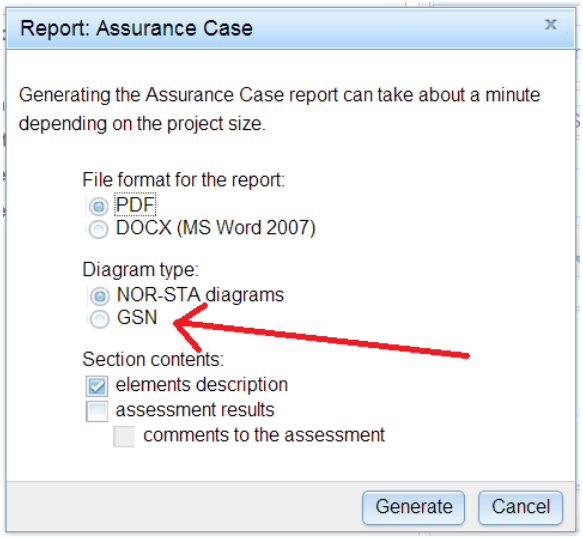
How you like this argument structure? Claim G1 with Cxt1 context supported by strategy S1 and then G2 and G3. Now the argument is complete and it's time to generate GSN diagram…

Step 6. Generate GSN report

You do not work with GSN directly in NOR-STA. As you have seen we created the whole argument without any reference to GSN. GSN diagrams are embedded in NOR-STA reporting tool.

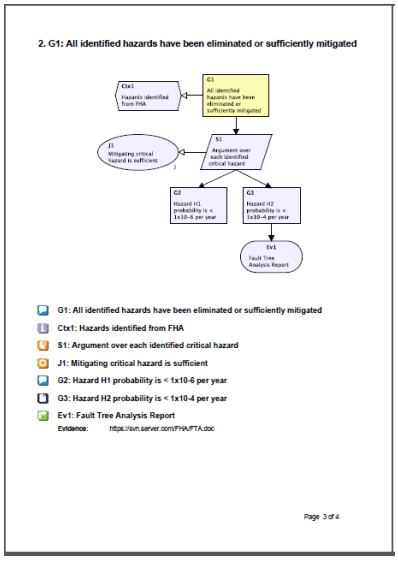


When you select Assurance Case report from the Report menu, you will be asked to set the report parameters. If you want GSN diagrams please select GSN option in the report parameters window.



The report will present the whole contents of the assurance case divided into section. Generally speaking, one section is based on one argument strategy. It contains claim and its supporting elements: argumentation strategy and premises. If any premise is a claim supported by another argumentation strategy it will be presented in a separate section in the report.

Each section in the assurance case report contains a diagram and descriptions of each element in the section. In our example we have not defined any description for the elements. It will be the next step and I will describe it in our next paper.



Our goal was to create a simple assurance case argument. We achieved this in six steps and it only takes two or three minutes.

You can easily create larger and more complex assurance cases in NOR-STA.

You can find more information on website: www.argevide.com.