In this document we describe the concept of an assurance case and give overview of the argument structure implemented in the Argevide NOR-STA platform.

You will find more information on our website www.argevide.com and in the NOR-STA manual.

1 The concept of an assurance case

An **assurance case** is a structured, compelling argument, supported by evidence, justifying that a system has some postulated properties in a specific context and environment.

An assurance case consists of main six components presented in Figure 1.

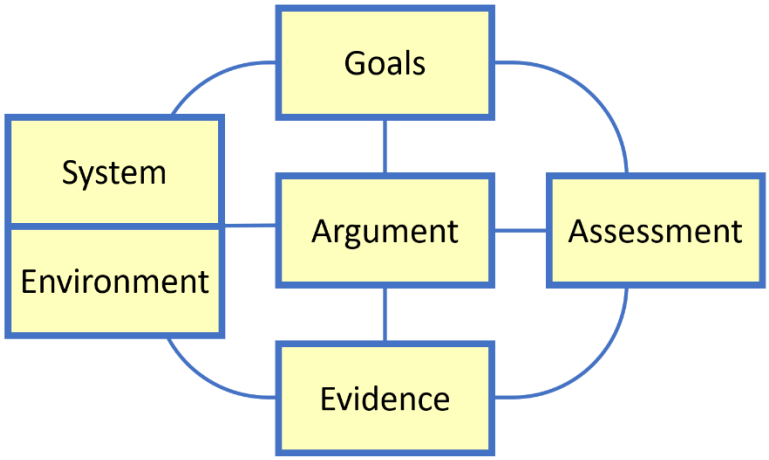


Figure 1. The main components of the assurance case

Goals specify properties of the system that are to be demonstrated by the assurance case. They have to be specified to start development of an assurance case.

The goals are specified in the context of the **system** and its **environment**. The system is the subject of assurance goals. It can be a simple device, a complex system or a set of integrated systems, an organization or a process. The system operates in the environment which covers operational physical objects, regulations and any information external to the system. Description of the system and the environment should be sufficiently detailed to allow for unambiguous interpretation of the goals, the argument and evidence.

The **Argument** contains an explicit and verifiable reasoning supported by evidence which demonstrates that the specified goals are achieved. It is the core element of an assurance case.

The argument is to be supported by **evidence**. Evidence is a verifiable and auditable information in any form (documents, data, photos, video, statistics) which describes the system, its components, characteristics, properties or events including data on the system operation. To be valid, the evidence needs to be consistent with the reality and up to date.

The last component of an assurance case is the **assessment**. The assessment is produced as a result of a systematic review of the argument and evidence. It gives information if the argument and evidence support the claims that the goals are achieved and that is the system has required properties.

2 The argument structure

The objective of the argument is to explicitly present the reasoning how the goal is supported by the evidence. This is achieved by reasoning steps and evidence support steps. This can be shown on the example of a simple argument of device safety (see Figure 2)

We will start with a goal “Device is adequately safe” which is defined in the context of a specific device and its context of use. Goals and any statements in the argument are defined as **claims** in the argument. There are several types of claims and we will present them in our case study.

A claim is a true-false statement, a predicate. Sentence “Device is adequately safe” is a true-false statement as it can be true or it can be false.

The argument presents a line of reasoning supported by evidence for the top claim. We will argue that the device is adequately safe by referring to the development process appropriate for safety-related systems. For example, we may follow the requirements of functional safety management according to the IEC 61508 standard.

The argument can be divided into steps. There are two types of **argument steps**: reasoning steps and evidence support steps.

A **reasoning step** describes the reasoning how a given claim can be inferred from its supporting claims. When we develop an argument for the device safety we can say the device “is adequately safe” because all safety functions are implemented. In the next step we demonstrate that all safety functions have been implemented. Our strategy of reasoning can be based on the use of a systematic development process. The reasoning steps are denoted with arrows in Figure 2. Indents indicate the hierarchy of argument elements. The direction of the reasoning is from the evidence to the claims as indicated by the direction of arrows.

Figure 2. General argument structure and the flow of reasoning

The whole reasoning is based on the evidence. The lowest level of the argument consists of a set of **evidence support steps**. The objective of this step is to establish claims backed directly by evidence. In our case study of a device safety argument, the documents like Test Plan and Test Report can be used to demonstrate that the required activities of the development process had been completed.

The claims supported directly by evidence are called **base claims** or **facts**. A fact is a statement (a claim) based directly on observation of real-world artefacts (the evidence). When I look at a thermometer and I see the temperature outside is 18 degrees Celsius then based on this evidence I can state a fact “the temperature outside is 18°C”. The statement of a fact usually requires some interpretation of the available artefacts, but not reasoning. For each fact a systematic way of determining if it is true for a given available evidence should be established.

3 Argument notations

There are many ways to present an argument. In NOR-STA we use a hierarchical notation to develop and manage the argument and additionally the Goal Structuring Notation (GSN diagrams) for reporting. All GSN diagrams presented in this document have been generated by NOR-STA. NOR-STA does not generate coloured diagrams and we have added colours following the schema of Figure 2 for easier viewing.

Indentation is used in NOR-STA notation to represent an argument hierarchy. The notation has been developed for use in the application and interaction with users. The plus and minus icons (like ⊟) are used in the tool to expand and collapse the argument elements below.

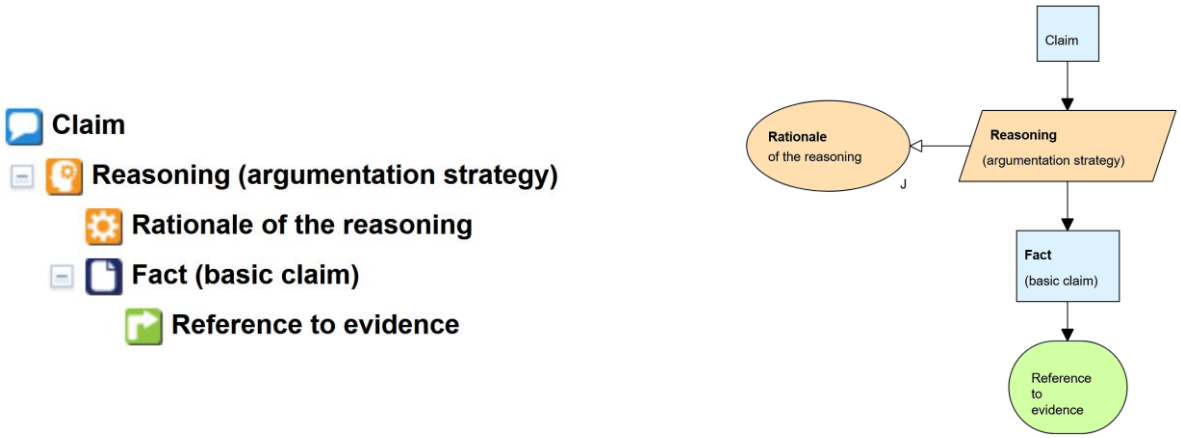


Figure 3. An argument in NOR-STA hierarchical notation (left) and a corresponding GSN diagram (right)

We will use both notations to present arguments and explain the argument structure.

The hierarchical notation has been developed at the Gdańsk University of Technology, Poland and implemented in NOR-STA. GSN notation had been initially developed at the University of York, UK and documented in "Goal Structuring Notation Community Standard" published in 2018 (https://scsc.uk/scsc-141B). You can refer to this standard to learn more about GSN.

4 Reasoning and evidence support steps of the argument

We will discuss the argument going bottom-up. The line of reasoning is based on the claim that all safety functions have been implemented and this can be demonstrated be presenting artefacts of the component development process.

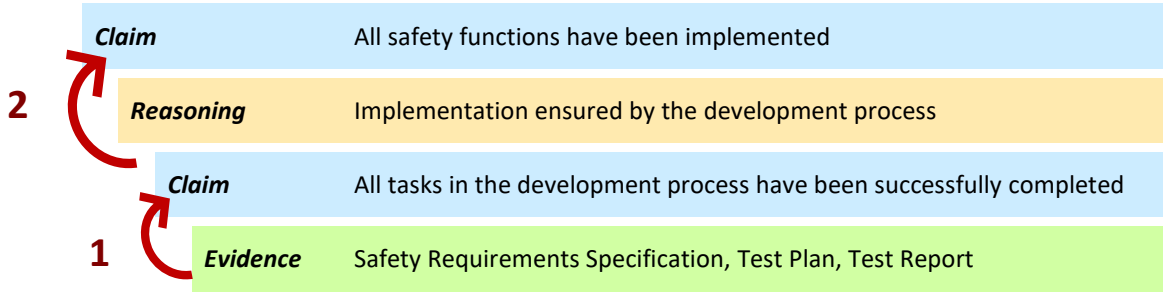


Figure 4. Steps 1 and 2 of the argument for device safety

We will develop a simple argument which will cover only three artefacts required by the development process: Safety Requirements Specification, Test Plan and Test Report.

In the first step we will define the claim and the related reasoning. In Figure 5 we present the claim "All safety functions have been implemented" supported by the reasoning. The reasoning is defined by two elements: an argumentation strategy and a rationale.

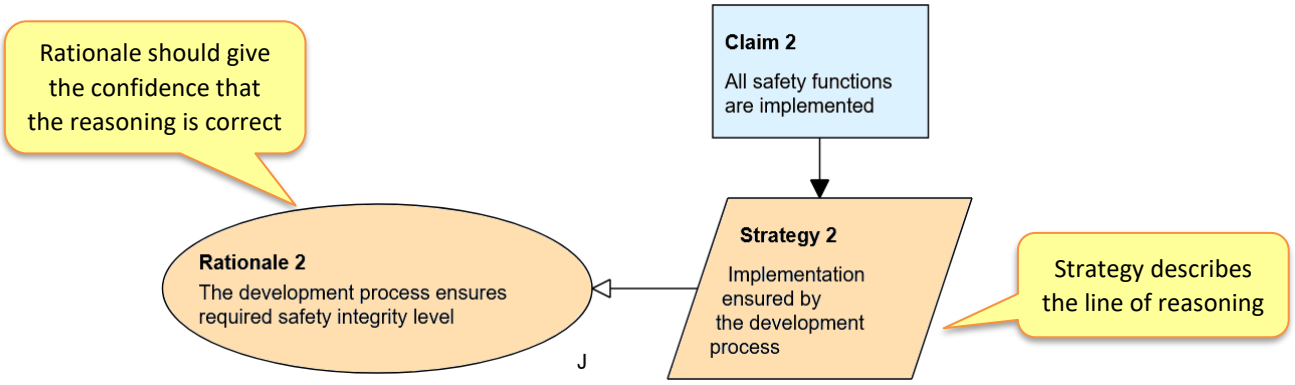


Figure 5. The reasoning step for a claim on safety functions implementation (GSN)

A **strategy** specifies the inference rule used to reason that the conclusion (the higher-level claim) is true when the premises (the lower-level claims) are true.

A strategy is not a statement and it is not a predicate. It just identifies a rule we use to reason. You can say a strategy is like a recipe telling you how to take ingredients and combine them to bake a cake. Or like a formula to calculate a result from the available data. Your strategy can be to use the Pythagoras's theorem to calculate the length of the hypotenuse in a right triangle.

When your strategy is the Pythagoras's theorem you have to use correctly the formula $a^2 + b^2 = c^2$. You have to select the right length values for a and b and then make a correct calculation. There are quite a lot of scenarios of mistakes. Maybe the triangle is not right-angled and the formula is not applicable? What if you make a mistake and use an incorrect formula like $A = (b \times h) / 2$? We need some safety mechanism to ensure we use the right inference rule and it is used in the right way. Therefore we add a rationale (see Figure 6).

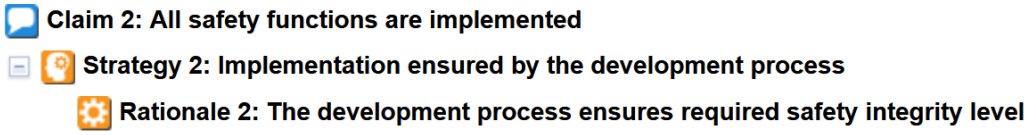


Figure 6. The reasoning step for a claim on safety functions implementation (NOR-STA notation)

A **rationale** is a statement which justifies that the right strategy is used to support a given claim and that it is used in the right way. It is a statement so technically a rationale is also a claim. A rationale does not have direct effect on the goal of the assurance case, that is in our example the rationale will not impact directly safety of the device. The role of the rationale is to provide confidence that the reasoning about device safety is correct.

Rationale has impact not on the goal of the argument, but on the **confidence** in the reasoning. The rationale will not say if the goal of the argument is achieved, for example if the system is adequately safe. It will say if we can trust the reasoning leading to the conclusion that the top claim of the argument is true. We will discuss this in detail in the section on argument assessment.

The same fragment of the argument as in Figure 5 is presented in NOR-STA hierarchical notation in Figure 6. No premises are defined yet for the argumentation strategy. We will add them in the next step.

The strategy requires to demonstrate that the development process has been applied to develop all safety functions of the system. As mentioned earlier we will demonstrate that three artifacts had been developed for the system:

- Safety Requirements Specification which covers the required safety functions,
- Test Plan that covers verification of the safety requirements and
- Test Report.

We will specify three claims (labelled 2.1, 2.2 and 2.3) supported directly by **evidence**. They are “base claims” and we distinguish this by labelling them as facts. Each of them is supported by a reference to corresponding document used as evidence. A document is a real-world artifact that you can review and check if a given base claim like “Test plan covers all safety requirements ” is satisfied.

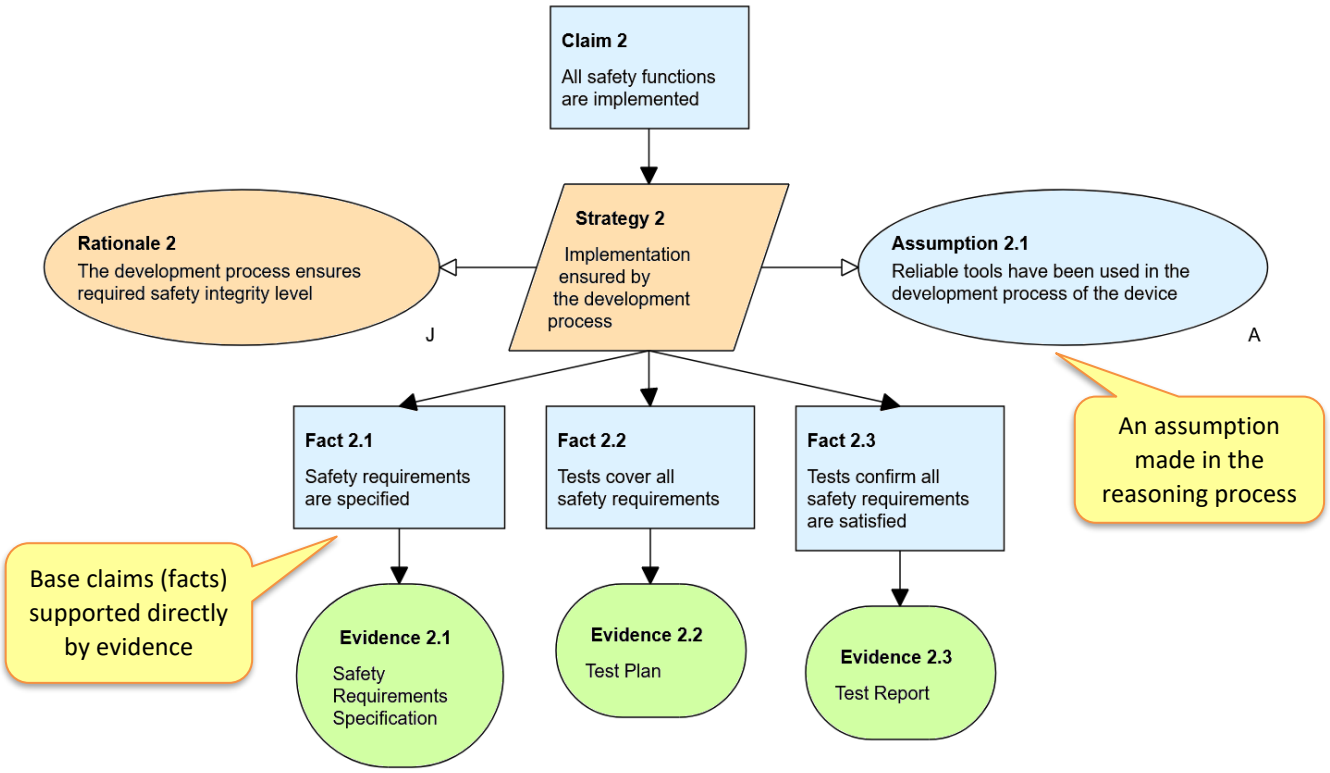


Figure 7. Argument for the implementation of safety functions in GSN

Sometimes in the argument we refer not only to available evidence but also to some assumptions we make without providing any evidence for them. For example you may notice that the tools used in the development process may have impact on the developed system and its safety. To point it out we add an **assumption** element to the argument.

Any time you see a gap in the reasoning you may consider if there are any hidden assumptions in the argument. When you identify them you should specify them in the argument. All assumptions should be explicitly specified to ensure the argument is complete.

You may also use assumptions to represent some knowledge you have about the system and assume it to be true without requesting any evidence. An assumption may describe the context of the system and its use. For example we may know that the system is intended to be used indoors and specify an assumption that the temperature during system operation will be above zero Celsius.

In Figure 8 we present the same argument using NOR-STA hierarchical notation. You may notice that the only relation in this type of diagram is the hierarchy. The specific properties of relations depend on the types of the related elements.

Figure 8. Argument step for implementation of safety functions (hierarchical notation)

The presented argument diagrams describe reasoning steps 1 and 2. Now we will extend this with step 3.

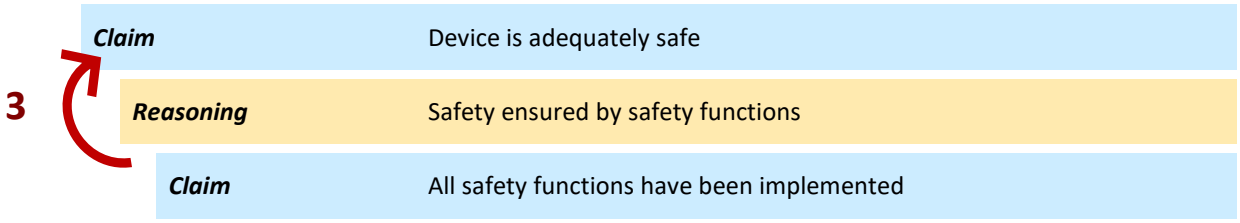


Figure 9. Step 3 of the argument for device safety

We will use this step of argument to add a new claim that all safety functions have been specified.

We also add a context information needed to precisely specify the top claim.

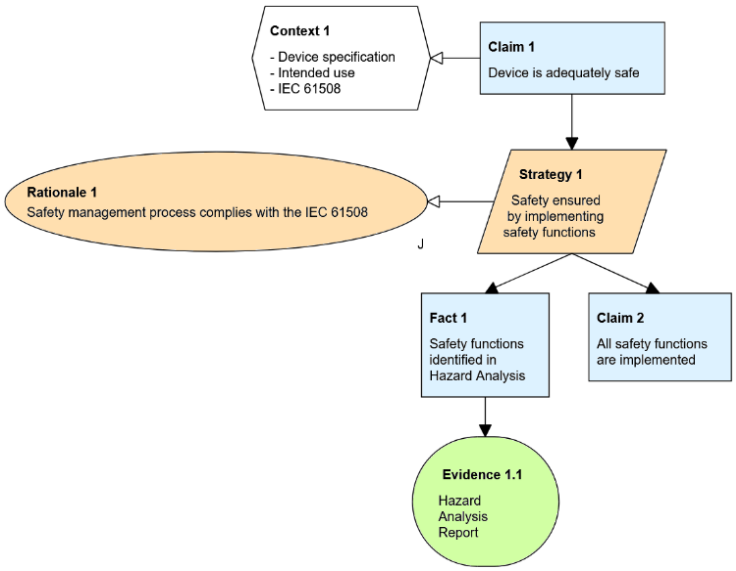


Figure 10. Step 3 of the reasoning on device safety (GSN)

The complete argument consisting all three steps of reasoning in NOR-STA hierarchical natation is presented in Figure 11.

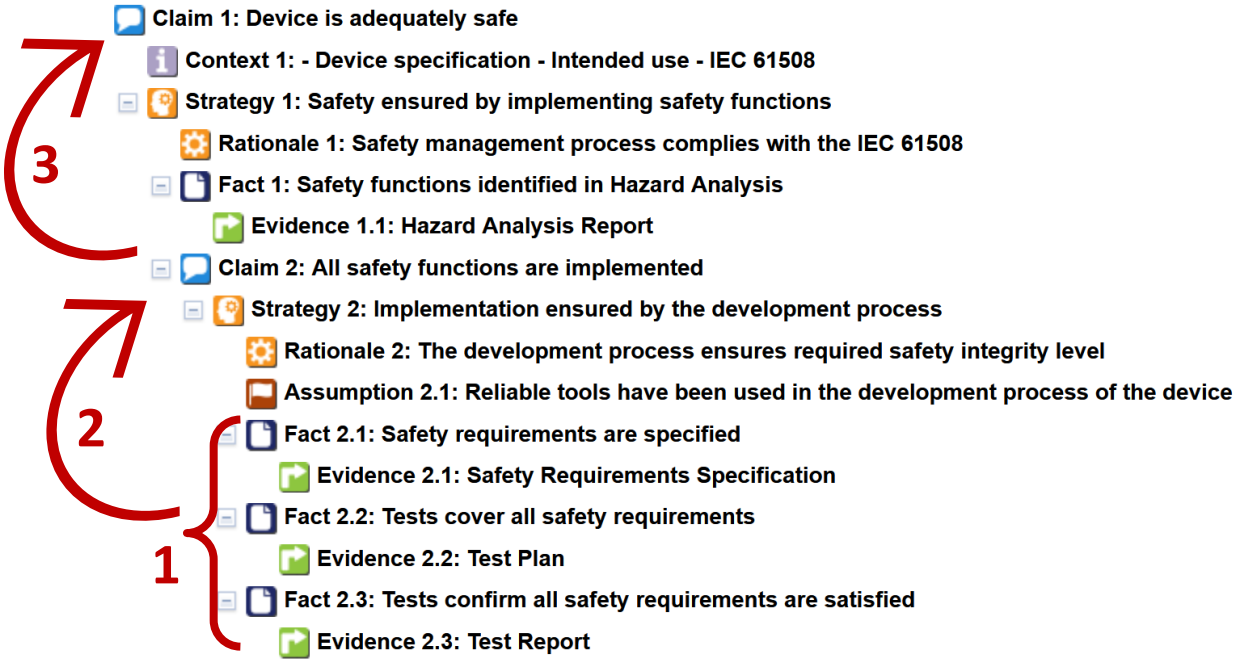


Figure 11. Complete argument for device safety in NOR-STA hierarchical notation

5 NOR-STA argument structure

The general metamodel of NOR-STA argument structure is presented in Figure 12.

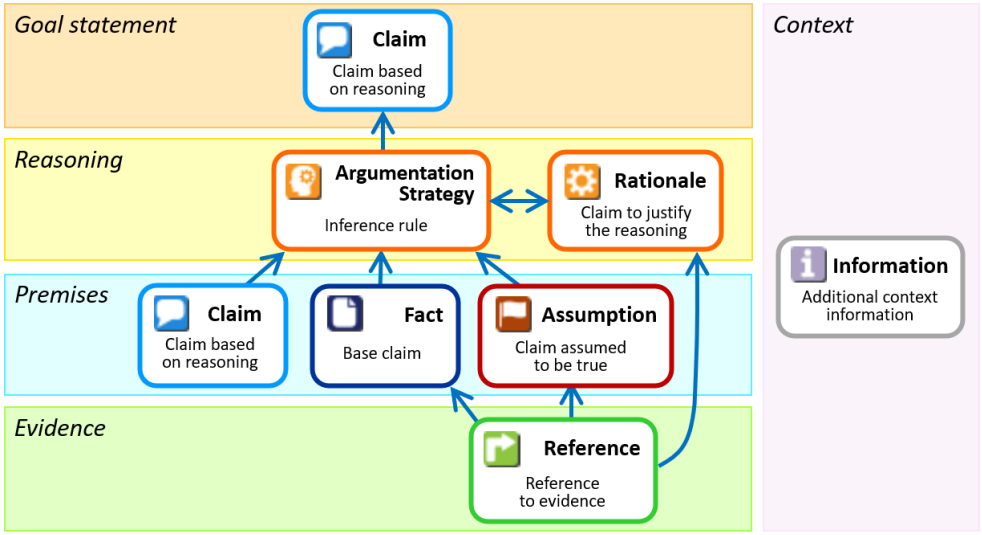


Figure 12. NOR-STA argument metamodel

Arrows on the diagram denote support. For example a claim is supported by a strategy. An element at the beginning of an arrow provides support for the element at its end.

1. The goal statement is a **claim**. It is a predicate (a true-false) statement which states the goal to be supported.
2. Reasoning is implemented by:
   a) an **argument strategy** which specifies the line of reasoning and
   b) **rationale** with justifies that the strategy is correct and applicable for a given claim and also that it is was correctly applied.
3. A premise can be:
   a) a **claim** that is to be supported by another argumentation strategy and further premises or
   b) a **fact** (base claim) supported directly by evidence, or
   c) an **assumption** that we make in the argument.
4. Evidence which supports the premises:
   a) **references** to evidence artefact, usually documents but other media like photos or measurement data may also be used.
5. The context **information** may be provided to ensure precise interpretation of argument elements.

All the NOR-STA assurance case elements are listed in the table below:

Icon	Name	Definition
	Claim	A statement about some property that requires argumentation and evidence to demonstrate that the system satisfies it
	Argumentation Strategy	Strategy specifies the inference rule that uses the supporting premises to conclude that the claim is satisfied. Note: Strategy used to refute a claim (to conclude that it is not satisfied) is called a counter-argumentation strategy.
	Rationale	A statement that justifies validity of the reasoning set down for a given claim by the argumentation strategy
	Assumption	A statement about some property, assumed to be true without any argument or evidence, usually assured by the environment

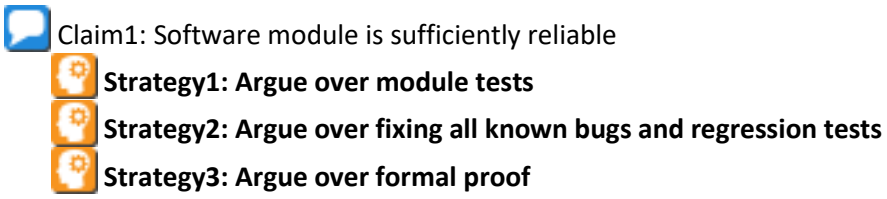
Icon	Name	Definition
	**Fact** (base claim)	A statement about some property supported directly by evidence Note: Facts are a type of claims that don't need any argumentation step and evidence is sufficient to demonstrate they are satisfied
	**Reference**	A reference to the evidence to support the argument.
	**Information**	Additional description for the argument element that supplements its definition

NOR-STA argument structure should follow the rules described in the following subsections.

5.1 Each claim is supported by one or more strategies

NOR-STA notation requires each claim to be supported by at least one argumentation strategy. You cannot support a claim directly with other claims. Each reasoning step should be defined with the use of argumentation strategy and justified with a rationale.

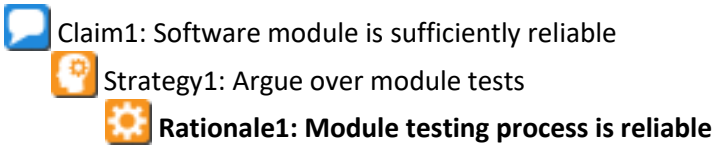
More than one strategy for a claim can be defined to represent independent argumentations.



Note: a base claim, that is, a claim supported directly by evidence is distinguished as a separate type “fact”.

5.2 A rationale is provided for each strategy

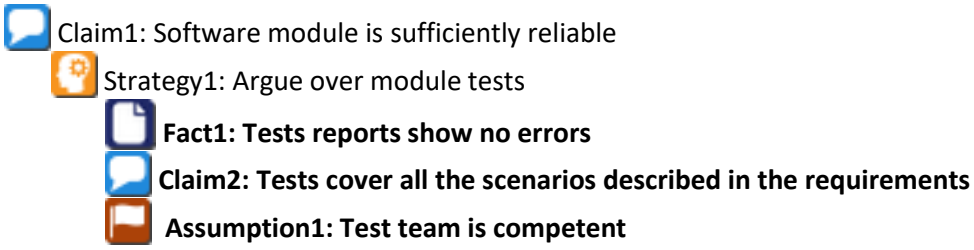
A rationale is to be specified for each strategy to justify that the strategy is correct and applicable for a given claim and also that it is was correctly applied.



A rationale is a predicate (a true/false statement) like a claim. It can be supported by evidence or by arguments when necessary.

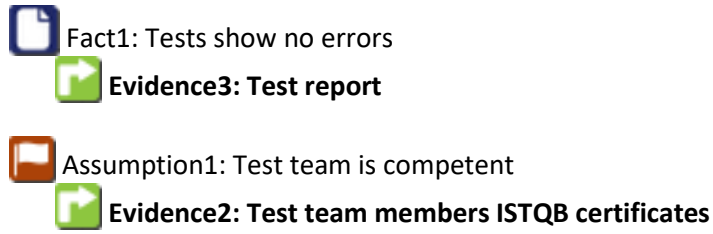
5.3 Argumentation strategy is supported by an arbitrary number of premises (facts, claims and/or assumptions)

A strategy should be supported by one or more premises. A premise can be a fact, an assumption or a claim.



5.4 Facts and assumptions are supported directly by references to the evidence

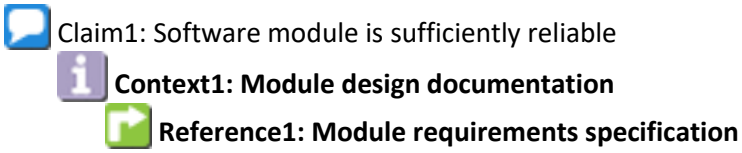
Facts and assumptions can be supported by evidence.



Providing evidence for facts is mandatory in NOR-STA, while evidence for assumptions is optional.

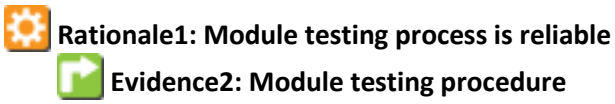
5.5 Information element can be attached to any element

Additional information like a context data can be attached to any element using an information element. Such information element can be supported by references to documentation when needed.



5.6 Rationale can be supported by evidence or an argument

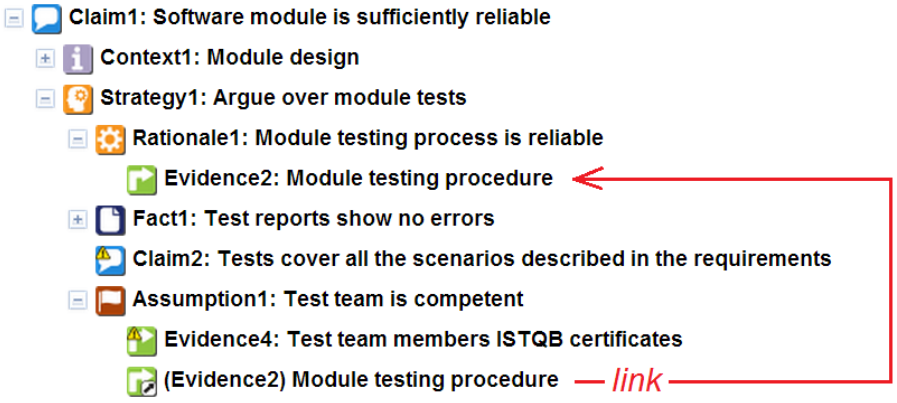
Rationale element can be supported either by an external evidence or by an explicit argument (a confidence argument) if a detailed argumentation is needed to build confidence in the rationale.



5.7 Linking argument elements

Some argument elements, for example references to evidence, can provide support for more than one argument element. Presenting assurance cases in a hierarchical way is a simplification and an argument is really a directed graph, not a hierarchical tree. We need a way to represent an element when it supports more than one element.

When one element is to be used more than once we can use links. Links are marked with a small black arrow in their icons:  . You can create links to any argument element except rationales.



6 Summary

In this guide we described the main elements of NOR-STA argument structure.

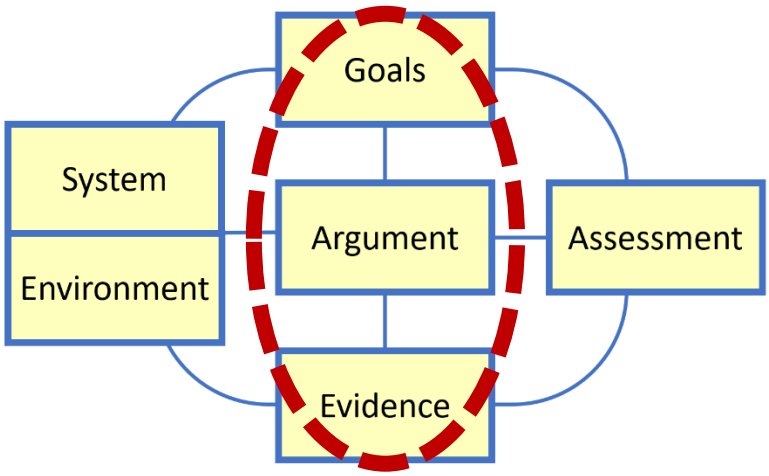


Figure 13. The main components of the assurance case

You can find more information on our website www.argevide.com and in the NOR-STA manual.

When you see any error or missing information in this guide please let us know at support@argevide.com.