In this document

- we describe what is an assurance case and explain the notation used in NOR-STA,
- present a sample assurance case and discuss the steps of the argument,
- review the argument and improve it to make it complete.

There are a few publications which define assurance cases like ISO 15026 standard, GSN Community Standard, OMG SACM metamodel. Argevide NOR-STA implements a general metamodel of the argument which forms the basis for use of specific argument notations like GSN. In this document we present the general concept of an argument model and refer to specific notations when necessary.

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.

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 argument.

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.

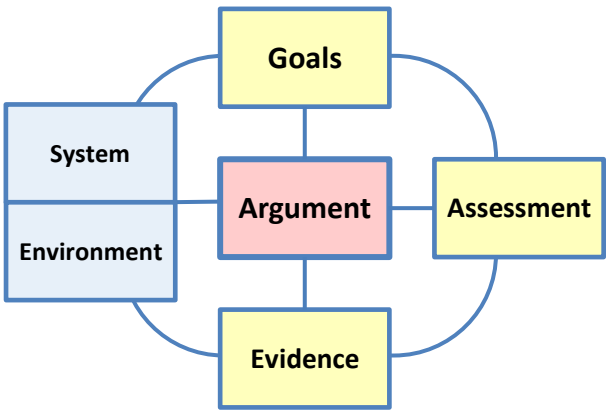


Figure 1. The component model of the assurance case

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 steps of the argument

The objective of the argument is to explicitly present the reasoning how the goal is supported by the evidence.

Simplified argument structure is presented in Figure 2. The argument starts with the goal “Device is adequately safe” which should be defined in the context of a specific device and its context of use but we will skip this for simplicity at the moment.

Goals and any statements in the argument are defined as **claims**. A claim is a true-false statement, a predicate. The sentence “Device is adequately safe” is a true-false statement as it can be true or it can be false. This requires a precise definition what is the system and what level of safety is adequate but we will ignore this issue at the moment. Each claim should be defined in an unambiguous way. We will describe how we define claims in the next section.

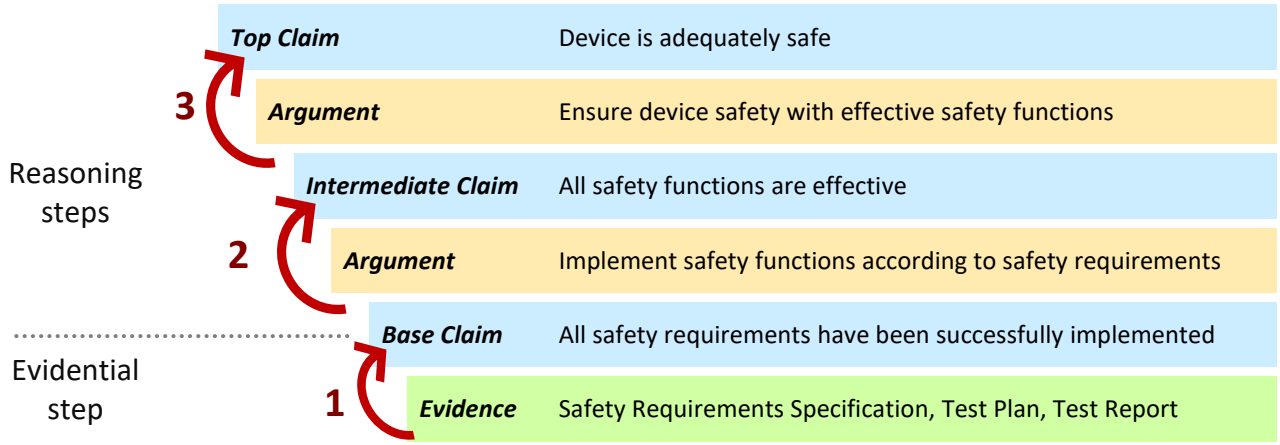


Figure 2. General argument structure and the flow of reasoning

The argument presents a line of reasoning from the evidence presented at the bottom of the diagram to the claim presented on the top. The reasoning is divided into steps and we distinguish two types of **argument steps**: reasoning steps and evidential steps.

The lowest level of the argument consists of **evidential steps**. The step number 1 is an example of an evidential step. The objective of this step is to establish **base claims** backed directly by evidence. In our example we use Safety Requirements Specification, Test Plan and Test Report as the evidence. The step is **valid** when, on the basis of the evidence, we can conclude that the base claim is correct. The base claim should be defined in a way that it is supported directly by the evidence. No reasoning should take place in the evidential step of the argument. The evidential step should be simple and straightforward.

Steps 2 and 3 are **reasonings steps** which describe the reasoning how a given claim can be inferred from its supporting claims. The supporting claims are presented in the lower part of the step. They form premises for a given reasoning step. The claim on the top is the conclusion. The relation between the premises and the conclusion is described by an argumentation strategy which described the line of reasoning.

We usually develop assurance cases top-down and the process is not completed until we define all the evidence to support the argument. When you analyze the reasoning you go bottom-up. You start with evidence and draw conclusions going up step by step. The final conclusion should be the top claim of the argument.

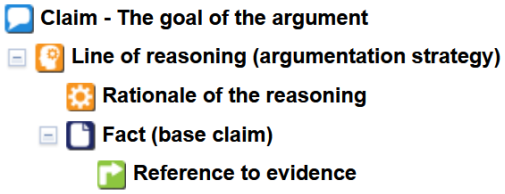
3 Argument notations – NOR-STA and GSN

There are many ways to present an argument. In NOR-STA we use a **hierarchical notation** to develop and manage the argument. The other way presenting the argument is **Goal Structuring Notation** (GSN). All GSN diagrams presented in this document have been generated by NOR-STA.

The hierarchical notation is also sometimes called a tree view of the argument. Indentations are used in this notation to represent the level of the argument hierarchy. The notation is intuitive and makes operation like adding or moving elements quick and easy as you do not have to rearrange the layout of any diagram. Therefore the notation is mainly used to work with the argument.

On the other hand graphical notation like GSN is better for presentations and discussions on assurance case. The notations are equivalent and NOR-STA generates GSN diagrams for any assurance case developed in the tool.

a) NOR-STA hierarchical notation
(argument tree view)



b) GSN notation

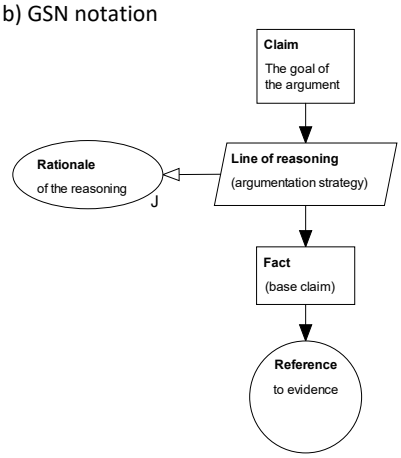


Figure 3. An argument in NOR-STA hierarchical notation (left) and a corresponding GSN diagram (right)

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

- The hierarchical notation has been developed at Gdańsk University of Technology, Poland and implemented in NOR-STA.
- GSN notation had been initially developed at the University of York and since 2018 it is maintained by Assurance Case Working Group (ACWG) at Safety-Critical Systems Club (SCSC). Version 3 of "Goal Structuring Notation Community Standard" was published in May 2021 (https://scsc.uk/gsn). You can refer to this standard to learn more about GSN.

To learn more about assurance cases you may also refer to ISO/IEC/IEEE 15026 series of standards "Systems and software assurance". Part 2 of the standard describes the structure of assurance cases.

4 The reasoning step

We will discuss the argument going top-down. That is the way we usually develop assurance cases.

The top fragment of the argument is presented in Figure 4. We add identifiers to all argument elements to make the referring to them easier. The argument starts with the top claim C1 “Device is adequately safe”.

Figure 4. The top-level reasoning step of the argument for device safety

In this reasoning step we argue that the device is adequately safe (the top claim C1) when all safety functions are effective (claim C2). The reasoning is defined by two elements: an argumentation strategy and a rationale.

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.

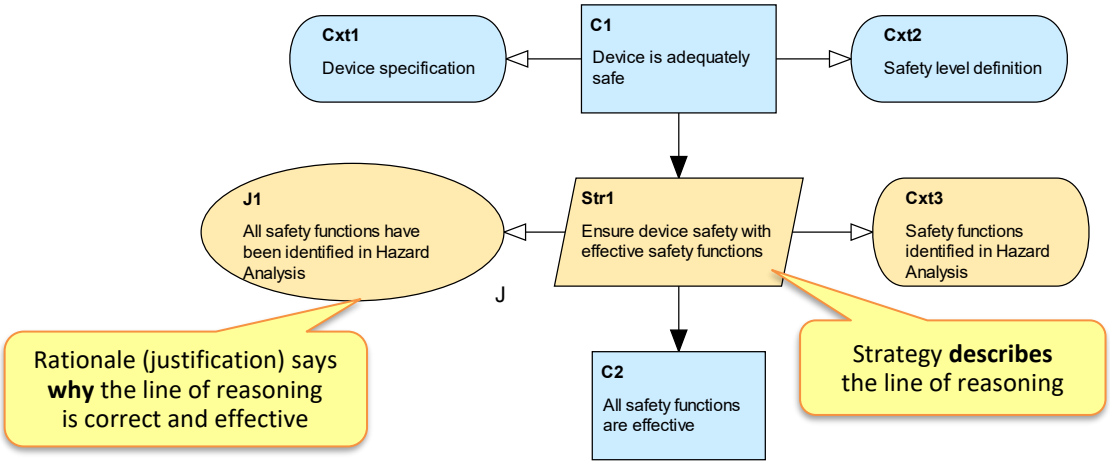


Figure 5. The reasoning step for the top claim (GSN)

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. The strategy says WHAT to do support a given claim.

It will not always be clear that the selected strategy is right for a given claim in its context or that the strategy was implemented in the right way, for example if all steps of the strategy have been implemented. Therefore we add a justification (or a rationale) to state WHY we think the strategy is applicable and implemented in the right way.

The top level reasoning step is presented using GSN notation in Figure 5, and using NOR-STA notation in Figure 6.

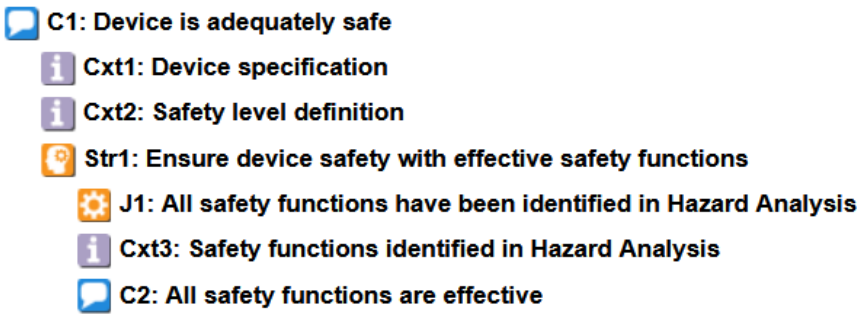


Figure 6. The reasoning step for the top claim (NOR-STA notation)

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. The assessment mechanism in NOR-STA is described in our other white paper.

The claim C2 is not supported on the presented diagram. It will be supported in the next reasonings step. We can develop any number of sequential reasoning steps until we reach the level of base claims (facts) supported directly by evidence. To keep our argument simple we will define base claims in the next reasoning step.

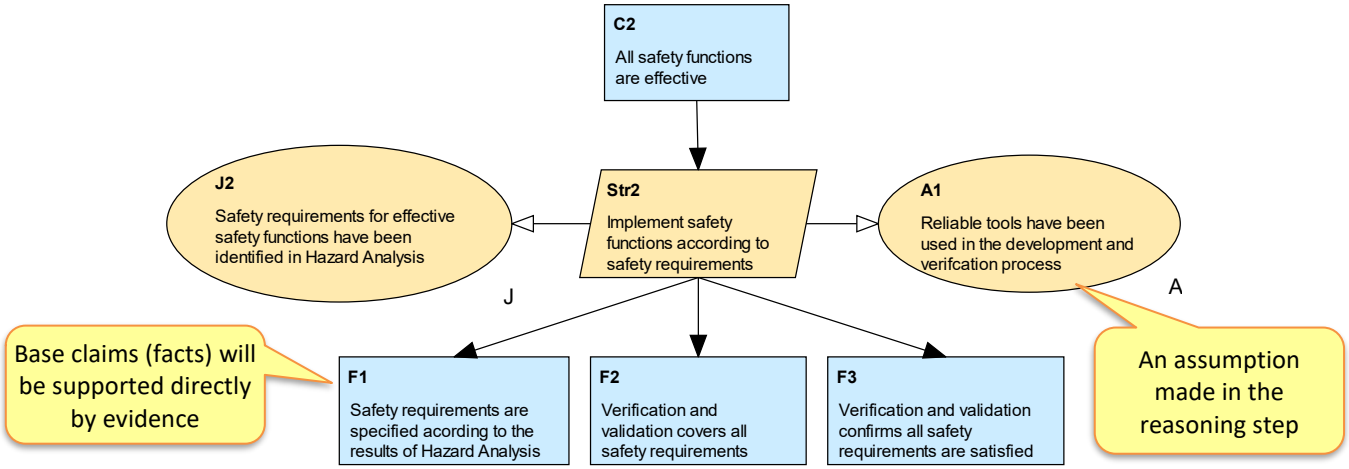


Figure 7. Argument for the implementation of safety functions (GSN notation)

We will demonstrate that the safety functions are effective by verification if they satisfy the allocated requirements. This will be done in steps: first we will demonstrate that we have a set of requirements for safety functions, then we plan V&V actions which will cover all the requirements and finally we will check if V&V results confirm the requirements are satisfied.

Sometimes in the argument we refer not only to claims we plan to be supported by evidence, but also some conditions which are **assumptions** for the reasoning. For example you may notice that the tools used in the development process may have impact on system safety and therefore we add assumption A1. You may also use assumptions to specify context in which assurance case goals are to be demonstrated.

Each reasoning step has three layers as presented with the use of colors in Figure 7. Starting from the top layer of the step we define:

- the conclusion – a claim and optionally related context or assumptions,
- the reasoning – a strategy, its justification and optionally related assumptions,
- the premises – claims which will be supported by further reasoning or evidential steps.

5 The evidential step

The reasoning steps of an assurance case describe the logic while the evidential steps describe relation to real world artifacts. All reasoning steps should finally be supported by evidential steps.

The basic schema of an evidential step consists of just two elements:

- a **base claim** (fact) which describes a required property of an object and
- a reference to **evidence** which directly supports the claim.

For the base claims presented in the previous section we can use the following documents produced in the device development process as evidence:

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

The evidential step for the device safety argument in presented in Figure 8.

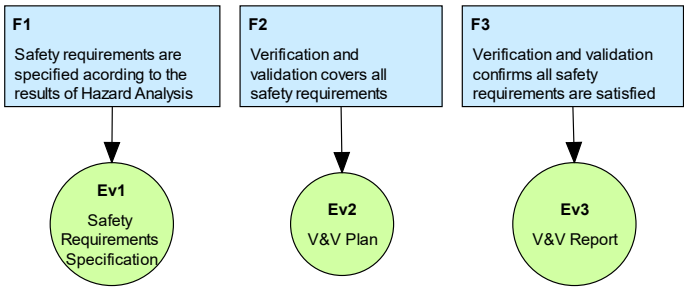


Figure 8. Evidential step for the device safety argument (GSN notation)

We may call elements on the diagram as “evidence” but in fact they are references to the evidence item. An **evidence item** is a piece of information represented in any form available for the assurance case users. In most of the cases it is an electronic document (like PDF file) but it can also be a paper document.

If the evidence item is available online the reference in the argument may contain an URL address to let the argument users open it. The other solution is just to describe where the evidence item is located. This approach is commonly used for paper documents. In same cases evidence may contain so sensitive information that it would not be included to the assurance case online and the reviewer has to get a physical access to it in order to make a review.

6 The complete sample argument model for device safety

We have discussed a sample assurance case for device safety step by step. In this section we present a complete argument using GSN and NOR-STA notation.

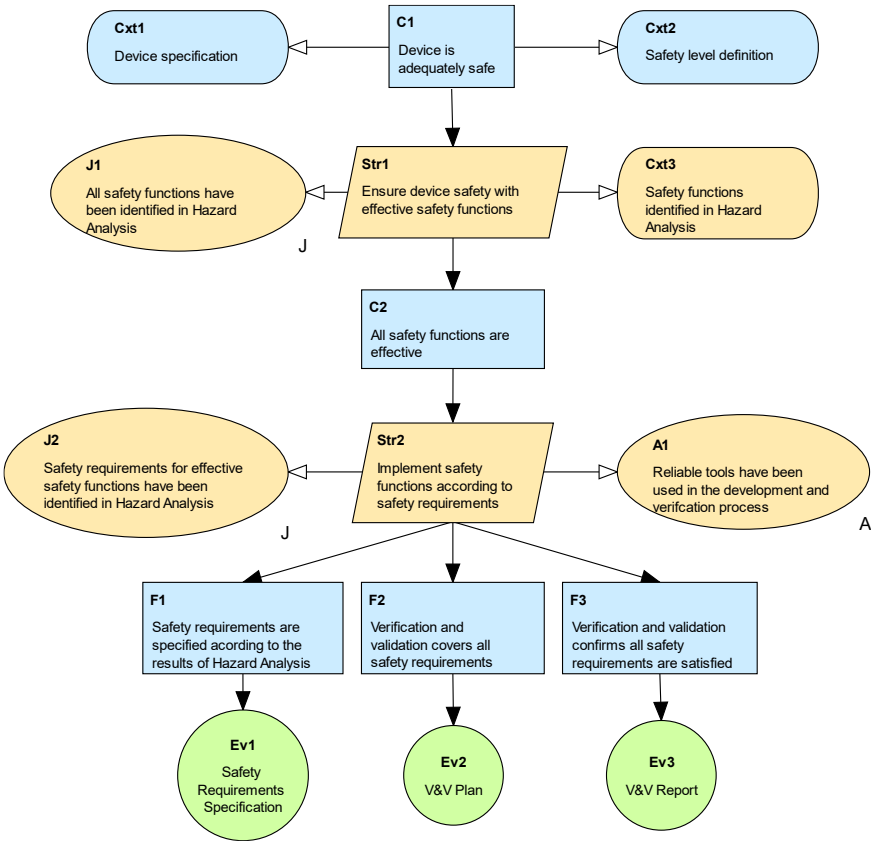


Figure 9. Complete argument for device safety (GSN notation)

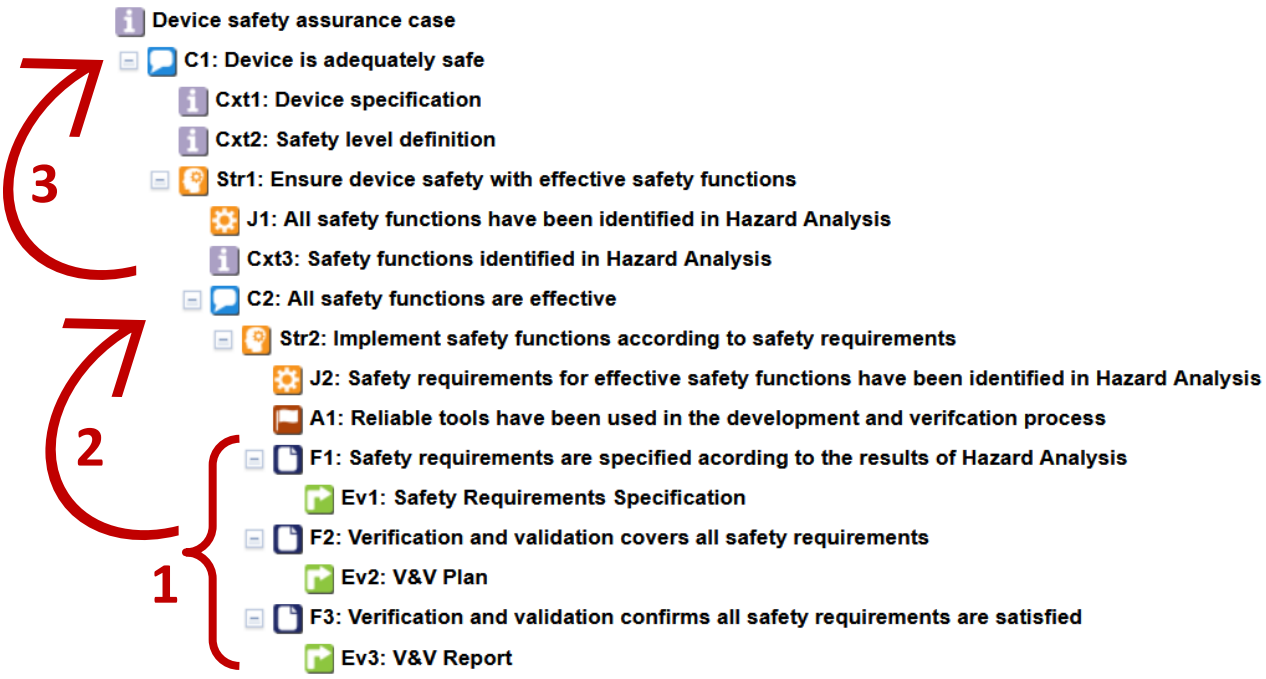


Figure 10. Complete argument for device safety (NOR-STA notation)

7 NOR-STA argument metamodel

The general metamodel of NOR-STA argument structure is presented in Figure 11.

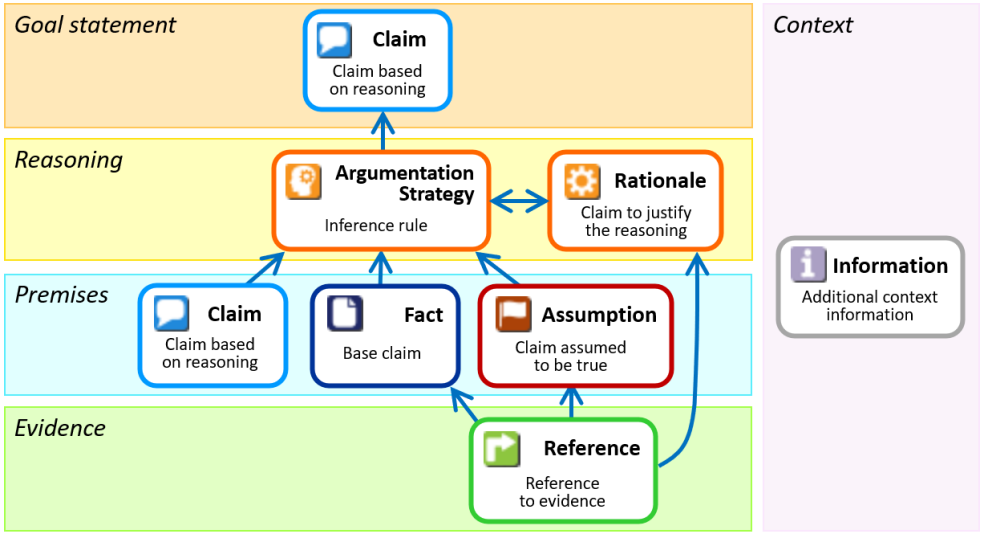


Figure 11. NOR-STA argument metamodel

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

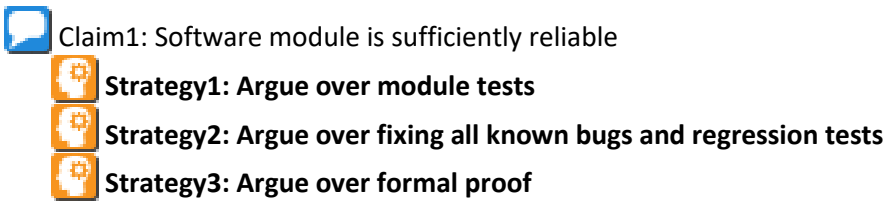
Icon	Name	Definition
	**Fact** (base claim)	A statement about some property supported directly by evidence Note: Facts are a type of claims that don't need any argumentation step and evidence is sufficient to demonstrate they are satisfied
	**Reference**	A reference to the evidence to support the argument.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

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

7.1 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.

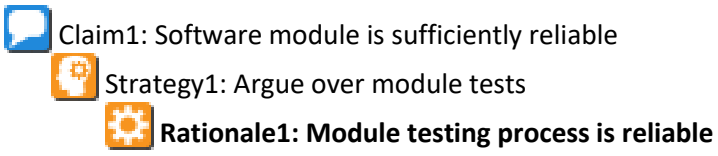
More than one strategy for a claim can be defined to represent independent argumentations.



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

7.2 A rationale is provided for each strategy

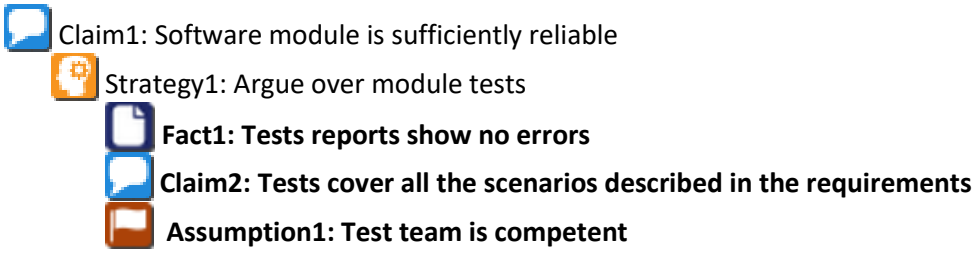
A rationale is to be specified for each strategy to justify that the strategy is correct and applicable for a given claim and also that it is was correctly applied.



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

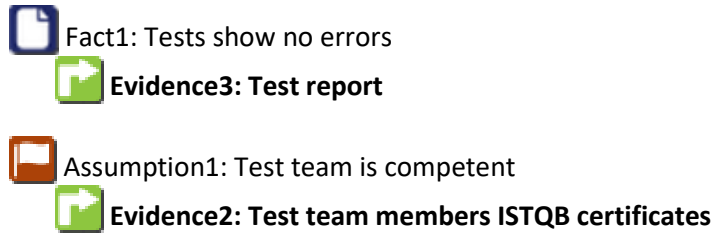
7.3 Argumentation strategy is supported by an arbitrary number of premises (facts, claims and/or assumptions)

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



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

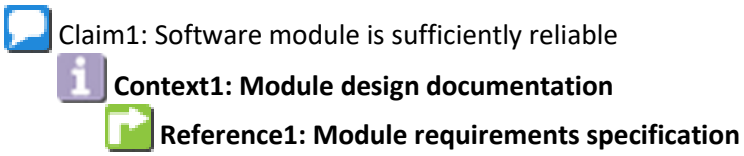
Facts and assumptions can be supported by evidence.



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

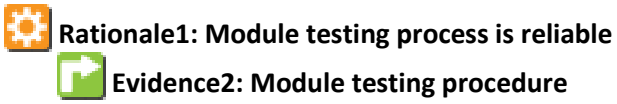
7.5 Information element can be attached to any element

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.



7.6 Rationale can be supported by evidence or an argument

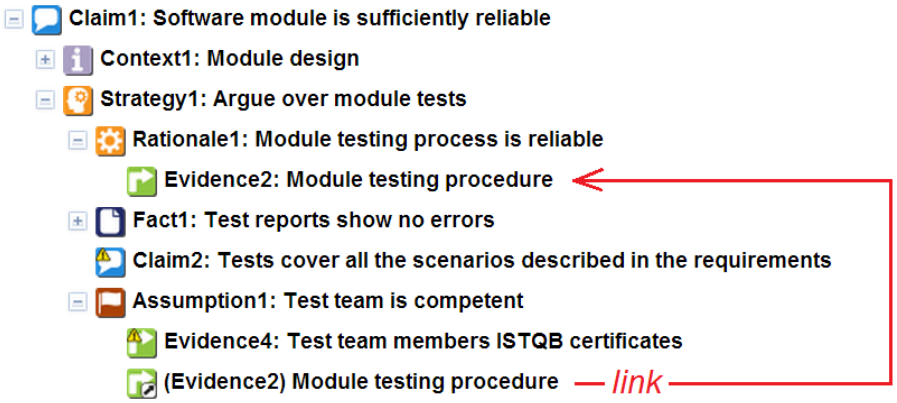
Rationale element can be supported either by an external evidence or by an explicit argument (a confidence argument) if a detailed argumentation is needed to build confidence in the rationale.



7.7 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.



8 Summary

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

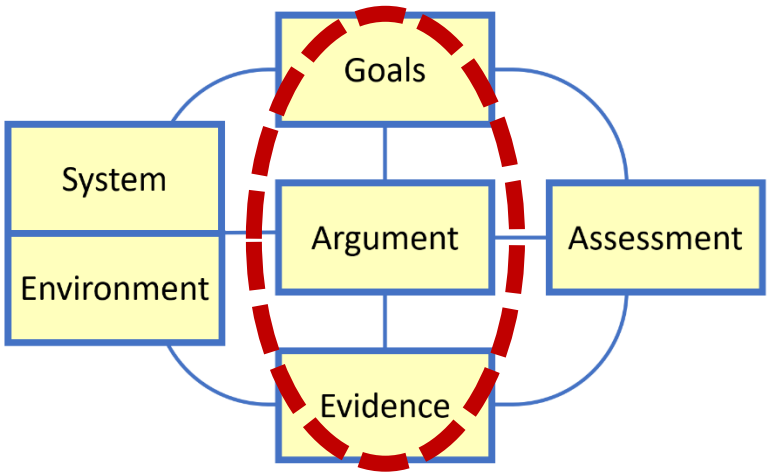


Figure 12. The main components of the assurance case

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.