ARGEVIDE

TRUST-IT Guide

Part 2. Argument Assessment

v1.0, 26.09.2022

1 Introduction

The definition of an assurance case says that it is a structured and **compelling** argument, supported by evidence, **justifying** that a system has some postulated properties in a specific context and environment. When we have an argument developed we should verify that it is "compelling" and that it "justifies" postulated properties. The way to achieve this goal is the argument assessment mechanism.

Argument assessment is a systematic and documented process of an argument review performed to verify its correctness and to guide the improvement process in order to produce an acceptably compelling argument.

The assessment process can be performed as self-assessment internally in the argument development team, by another division in the organization or by a third party, like a qualifier or certifier.

In this document we will describe:

- the main rules that drive the assessment process,
- the activities of the assessment process and
- argument quality checklist.

We recommend that you get familiar with the first part of TRUST-IT Guide which described the structure of an assurance case before reading this text. It would be great if you use NOR-STA when reading about the assessment and try the assessment yourself at once.

Figure 1. Visual presentation of the assessment on the argument diagram

2 What do we assess in the argument?

The main objective of the assessment is to determine if the top claim is satisfied or not. The top claim, like all claims in the argument, is a proposition. Each proposition is a false-true statement. An example of a top claim is “the device is adequately safe to use”. Each proposition in the argument is a natural object for the assessment.

An argument is a composition of three base types of elements:

- propositions (claims, assumptions, rationales),
- inference rules (argumentation strategies) and
- information artefacts (references to evidence, context elements).

Propositions are the elements we are focused on in the assessment process. Propositions depend on each other in the argument structure and the assessment process should take these dependencies into account. A simplified argument structure is presented in Figure 2. To get more information about the argument structure and elements please refer to the first part of TRUST-IT Guide.

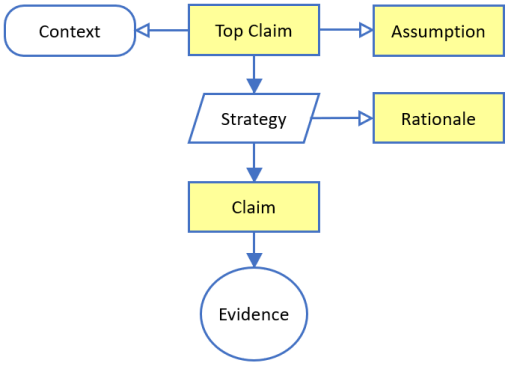


Figure 2. Main elements in the argument structure (rectangles are used for propositions in the argument)

The diagram presents a claim and other argument elements it depends on. There are three basic types of dependencies in the argument that affect the overall assessment result. They are defined by:

- **evidential steps** of the argument which demonstrate that base claims are correctly supported by evidence,
- **reasoning steps** of the argument which demonstrate that inferred claims are correctly supported by other claims,
- **assumptions** made in the argument which should be verified if they apply.

Note that TRUST-IT method advices to define an explicit strategy and rationale (justification) for each step of the reasoning in the argument. When higher confidence in the reasoning step is required a rationale can be supported with a confidence argument.

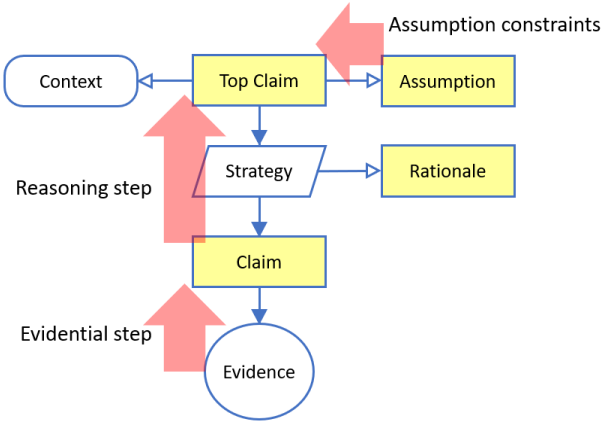


Figure 3. The main assessment points in the assurance case argument

3 What does the assessment mean?

The goal of the assessment is to give information if a given proposition is true or false. In the assessment process we should also allow that for some reason we are not able to make an assessment or the assessment is not made yet. This represents a situation we don't know if a given proposition is true or false. We call this state an uncertainty. Assurance cases are often developed in parallel with system life cycle activities and uncertainty may corresponds to tasks and work products which are not developed or not verified yet. Uncertainty is reduced with the progress in system development, verification and validation.

The base three values of the assessment are: "false", "true" and "uncertain". When the assessment is presented to the user we may use a color code to represent the values: red for false, green for true and yellow for uncertainty.

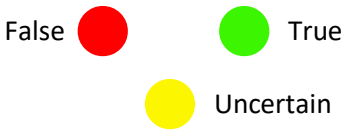


Figure 4. The main values of the assessment: false (red circle), true (green circle) and uncertainty (yellow circle)

The three-value assessment scale can be used in practice but it will not allow to give information how many of the supporting premises are satisfied. Using a single true/false scale it is not possible to distinguish if most of the premises are satisfied or maybe just a few of them.

To represent the extent of achievement of a given proposition we extend the false/true values with a continuous scale from 0 (which denotes "false") to 1 ("true"). The values can be represented with numbers (for example 0,85 or 85%) or graphically using scale marked with values from 0 to 1. Another way of graphical representation is a color bar with green, yellow and red segments corresponding to the assessment value. Both ways of assessment presentation are shown in Figure 5.

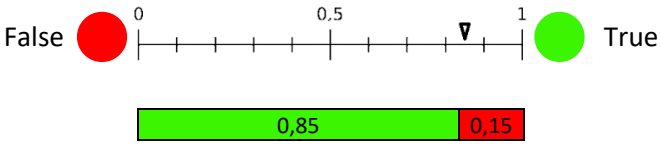


Figure 5. Assessment scale for a decision if proposition is true

Use of such a detailed scale raises some questions. What is the precise meaning of the assessment values? When a value like 0,85 should be used?

The assessment can be interpreted as a progress towards the goal. The value should not be interpreted as a metric for the goal. You cannot say that you have achieved 85% of system safety. The only reasonable statement is that according to the argument a given claim is true when it's fully assessed to be true (assessment value 100%). Any assessment different from full acceptance (below 100%) means that the claimed system properties are not certain.

When a lower safety level can be accepted for your system, you should define such goal in an explicit way and then demonstrate that it has been fully achieved.

The scale presented in Figure 5 is using one dimension for the assessment from 0 (false) to 1 (true). Value 0,85 can be interpreted as our opinion that a given proposition is true is 85% and 15% that it is false. This does not correspond to a situation when some evidence items are not available yet or we cannot interpret some elements in the argument.

To resolve the problem, a second dimension of the assessment is added for confidence in the argument. This is presented with a vertical axis on the assessment scale. The space of the assessment could be represented as a rectangle however when the assessment is "uncertainty" then we have no opinion about the proposition

to be false or true. With decreasing confidence the meaning of the assessment decision also decreases. This is represented with an opinion triangle[1].

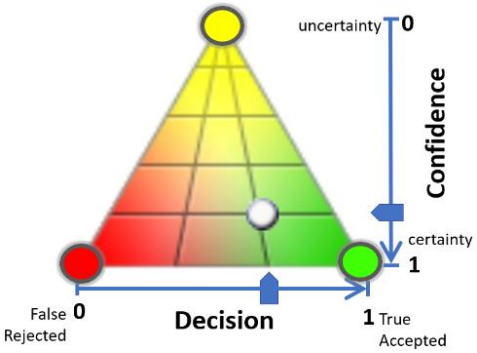


Figure 6. Opinion triangle used to represent proposition assessment

Any point in the triangle can be represented with two values which describe two dimensions of the assessor evaluation. The first dimension is used to say if a proposition is true or false. The second dimension is used to define the confidence level of the first assessment.

This way of the assessment representation with two values (decision, confidence) is formally defined by Dempster–Shafer theory as a pair (belief, plausibility).

Mathematical formulas are used to calculate the assessment point in the triangle depending on the assessor decision. The assessment can also be presented on the assessment bar where the width of green, red and yellow sections depends on the value of the assessment.

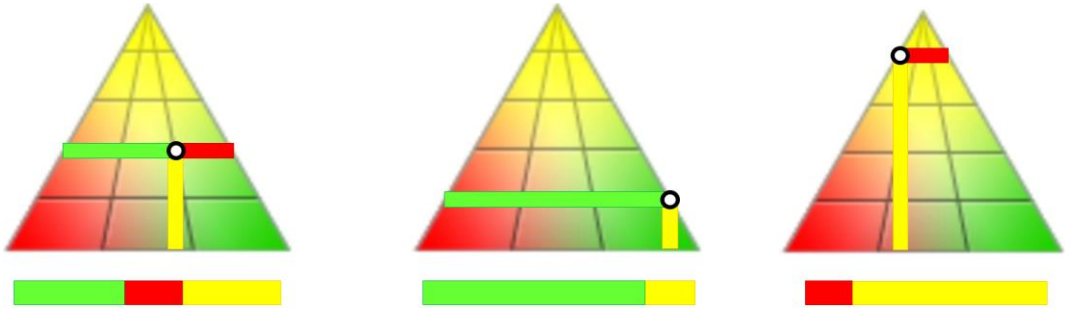


Figure 7. Examples of an assessment in the opinion triangle and presented in the assessment bar

The opinion triangle enables representation of uncertainty of the assessment, however simpler scales may also be used for the assessment of TRUST-IT assurance case. All scales use a subset of Dempster-Shafer assessment scale presented in Figure 6. Examples of simple assessment scales are:

- three-value assessment scale uses only three values as presented in Figure 4,
- SPICE scale defined by ISO 33000 standard with values from 0 to 100 divided into four ranges N-P-L-F: Not achieved (0–15%), Partially achieved (>15–50%), Largely achieved (>50–85%), Fully achieved (>85–100%).

[1] You can find description of the opinion triangle in: Josang A., Grandison T. Conditional inference in subjective logic. In: Proceedings of the 6th international conference on information fusion cairns, 2003, p. 471–8 (link)

4 Assessment in the argument structure

The argument assessment is a systematic process of the review of all evidential and reasoning steps is they provide sufficient support. The assessment of the top claim depends on the results of the review of the supporting argument steps according to the dependencies of the argument structure.

- Inferred claims are supported by **reasoning steps** and their assessment depends on the assessment of the inference rule and the premises. The inference rule for each reasoning step should be reviewed and assessed. The resulting assessment of the inferred claim can be calculated automatically.
- Base claims are supported directly by evidence. The **evidential steps** of the argument should be reviewed by the assessor to check if the available evidence satisfied the requirements specified by the base claim.
- Additionally the assessor should review and verify all **assumptions** in the argument if they apply.

The distinction between reasoning and evidential steps is the essential element of the assessment process. The assessment scenarios are different for these two types of argument steps.

- **Reasoning steps** contain claims supported by strategies and supporting premises while the premises are
  - inferred claims supported by further reasoning steps and
  - base claims supported by evidential steps,
- **Evidential steps** contain base claims supported directly by evidence and are not supported by any other claims. They form the bottom layer of the argument

The argument steps are not separable and they share elements, usually claims, on their boundaries. Figure 8 presents three argumentation steps which share two base claims.

TRUST-IT methods requires the claim are precisely defined and each argument step can be examined and assessed in separation from other steps except from inherited context and assumptions that apply to the whole branches of the argument.

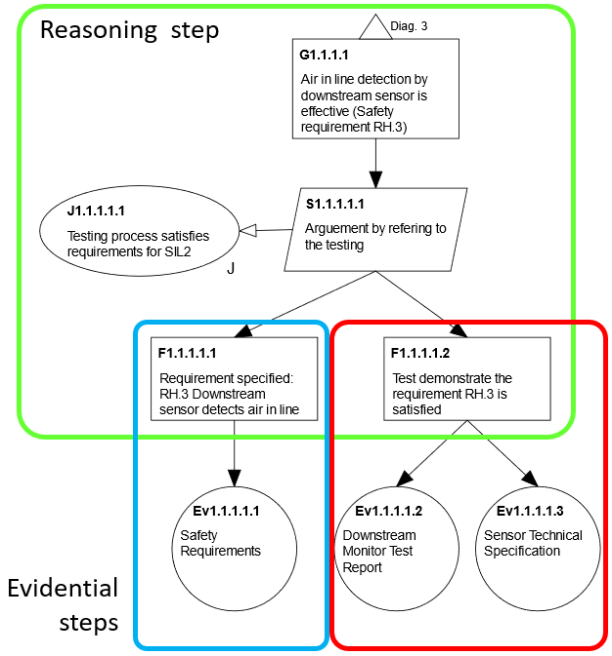


Figure 8. Boundaries of argumentation steps

Boundaries of an argumentation step are correctly defined when no other argument elements (except inherited context and assumption) are necessary to interpret the content of a given step. When you find any other information that has impact on the interpretation of an argument step then you should move this information into the scope of the argument step or define as an inherited context or assumption.

The logical separation of steps of the argument is also useful for the change management process. Impact analysis can be automated and this reduces the effort of the assessment in the argument evolution process.

5 Assessment of evidential steps

An evidential step consists of a base claim, supporting evidence and optionally direct or inherited context and assumptions.

There are to two main rules of the assessment of evidential steps:

1. The prerequisite is that the base claim provides a precise description of the required evidence and also acceptance criteria. The criteria should enable objective assessment if they are satisfied by the provided evidence.
2. The assessment of a base claim in manual. The assessor should review:
   a) the requirements defined by the base claim,
   b) the direct and inherited context and assumptions when applicable,
   c) evidence to check if it satisfies the specified requirements in a given context.

The scope of reviewed elements is presented in Figure 9.

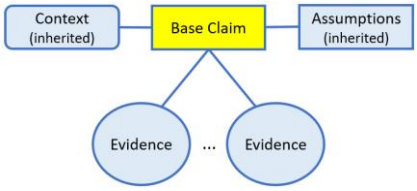


Figure 9. Elements that have impact on the assessment of the an evidential step marked with light blue background

Precise specification of requirements in base claims is essential to develop unambiguous assurance case. When the requirements are not precise the assessor should give uncertain assessment and comments to point out the problem and possibly suggest improvement.

Base claim F1.1.1.1.2 presented in Figure 8 refers to the tests of safety requirements for a component named Downstream Monitor. It should either refer to requirements for a test report (which are usually defined in the system development process) or specify these requirements directly or both when needed. Sample base requirements may be as follows:

> Downstream Monitor Test Report documents results of the test:
> - performed according to the Test Plan which includes requirement RH.3
> - where the test object if the sensor used in the pump specified in the inhered context
> - and the test results of all test cases relayed to the requirement RH.3 are positive
> - and the test process and tools satisfied the requirements of the development process.

The assessor also should not forget to check inherited context and assumptions if they are defined for some elements up the structure of the argument.

The assessment made by an assessor is valid as long as the related elements (Figure 9) are not modified. Evidence items are not a part of the argument but their modification should also invalidate assessment of all base claims that refer to them. The same problem relates to context documentation. When context elements refer to documents then their change should also invalidate assessment of the base claim. All referred document referred as evidence or context information should be under the configuration management to enable change management.

6 Assessment of reasoning steps

A reasoning step consists of:

- an inferred claim and optionally its context and assumptions (including inherited),
- supporting strategy and its premises, optionally you may define more than one strategy to support a claim,
- a rationale for each strategy to justify the reasoning step, which optionally can be supported by a confidence argument.

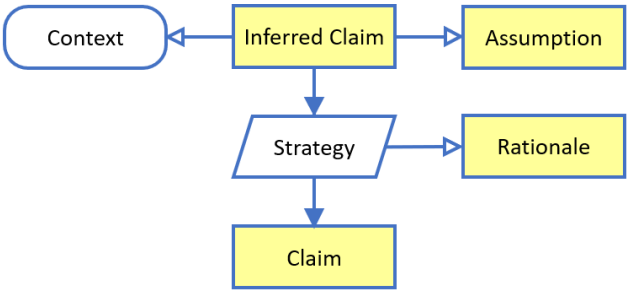


Figure 10. The scope of a reasoning step of the argument

Inferred claims are not assessed manually by the assessor but their assessment is calculated based on the assessment of other elements: assumptions, rationales and supporting claims.

The assessment of a reasoning argumentation step is divided into two activities:

The first activity is to provide assessment of the supporting elements: assumptions, rationales and the supporting claims. This can be performed manually by an assessor or automatically for element supported by a reasoning.

The second activity is automatic and is to be performed each time the first activity delivers update of any assessment. The activity consists of four automatic steps:

1. **Premises assessment aggregation** – when there is more than one premise under a strategy their assessments are to be merged into one aggregated assessment.
2. **Calculation of confidence of the reasoning** – confidence of the aggregated assessment is to be adjusted depending on the assessment of the rationale of the reasoning step.
3. **Merging the assessment of alternative strategies** – if more then one strategy supports the inferred claim the assessments of the strategies are to be merged.
4. **Assumption adjustment** – if an assumption is attached to the inferred claim it should be verified and possibly confidence of the inferred claim should be corrected.

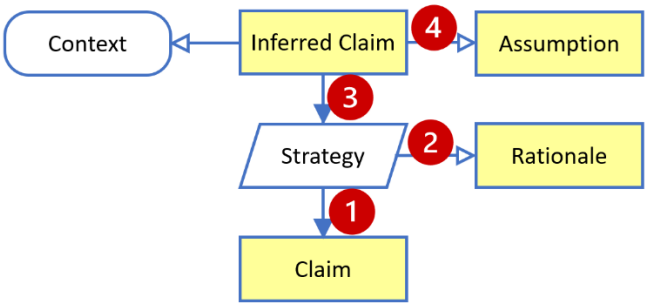


Figure 11. Steps to calculate the assessment of the inferred claim

The steps are assumed to be performed automatically when any of the input assessment is modified. If the inferred claim supports higher-level reasoning step, its assessment should be also updated in the same way. This process should be repeated up to the level of the top claim of the argument.

Depending on the assessment method used in the argument the details of the automatic steps may differ. The description in the following subsections presents the most advanced assessment calculation mechanism for Dempster-Shafer assessment method. Other assessment methods use simpler algorithms for assessment aggregation.

6.1 Premises assessment aggregation

When more then one premise is defined for a reasoning step their assessment has to be aggregated and the algorithm depends of the relations between them.

The argument developer may choose of three types of relations between premises:

- complementary premises,
- necessary and sufficient premises,
- sufficient premises.

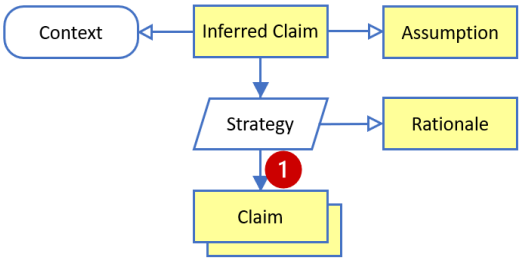
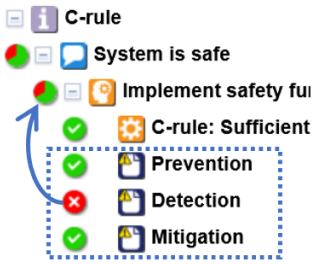
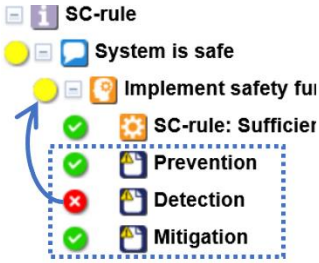


Figure 12. The step of assessment aggregation for multiple premises

The types of relations and corresponding calculation algorithms are presented in Table 1. Examples of a reasoning argumentation steps are presented with icons to present the assessment to illustrate how rejection of one premise affects the calculated result.

Table 1. Types of aggregation rules for multiple premises

Complementary premises	Necessary and sufficient premises	Sufficient premises
The premises support the conclusion in a complementary way. Every premise has its "share" in the conclusion assessment.	Every premise is required to be satisfied. When any of the premises is rejected, it entails rejection of the conclusion.	Every premise is required to be satisfied. A single premise, if rejected, leaves the conclusion uncertain.
		

6.2 Calculation of confidence of the reasoning

The next step is to assess if the way of reasoning is applicable and valid. The reviewer should evaluate if the strategy is applicable for a given claim and if it was correctly applied. If not the strategy should not be used to support a given claim. The rationale element is used to justify the strategy and when the reviewer does not agree with the way of reasoning it is the rationale to be rejected. Rejection of the rationale causes uncertainty of the inferred claim (Figure 13 on the right).

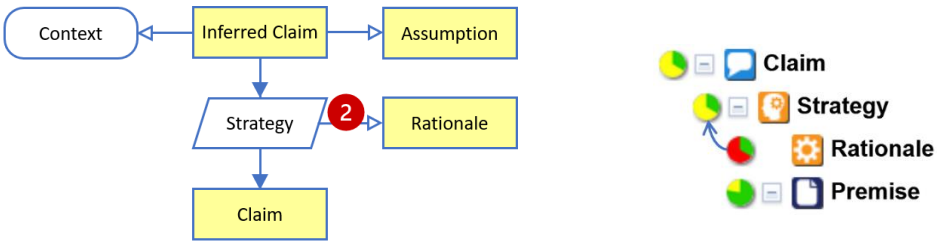


Figure 13. The step of the conclusion confidence assessment (left) and sample argument fragment (right)

6.3 Merging the assessment of alternative strategies

It may happen that several alternative strategies are defined to support the inferred claim.

Two strategies are alternative when two conditions are satisfied:

- they are independent of each other and
- each of them is sufficient itself to fully support a given claim.

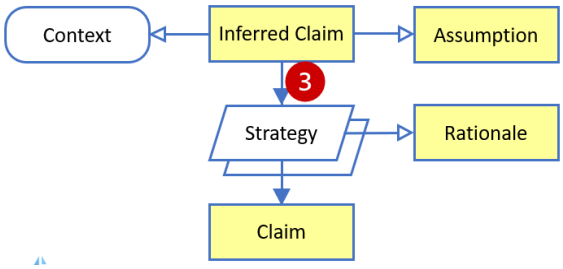


Figure 14. Use of alternative strategies

It should be checked if two strategies are alternative. In some cases two strategies may only seem to be alternative. For example static and dynamic testing may seem to be alternative approached but it should be demonstrated if each of them is sufficient to support the inferred claim. If you find out that there are some types of failures that cannot be detected by static testing then then this approach cannot be regarded an alternative strategy. The use of alternative strategies is to be considered individually for each assurance case.

When there are two alternative strategies the argument developer may select one of them to support it and ignore other strategies. This is presented in Figure 15 a).

Another solution is to implement both of them to achieve higher level of confidence. Figure 15 b) presents two strategies that are partially implemented. The resulting confidence in the inferred claim is higher than for each of the supporting strategies. This is a result of application of the belief matrix for alternative strategies shown in Figure 15 c).

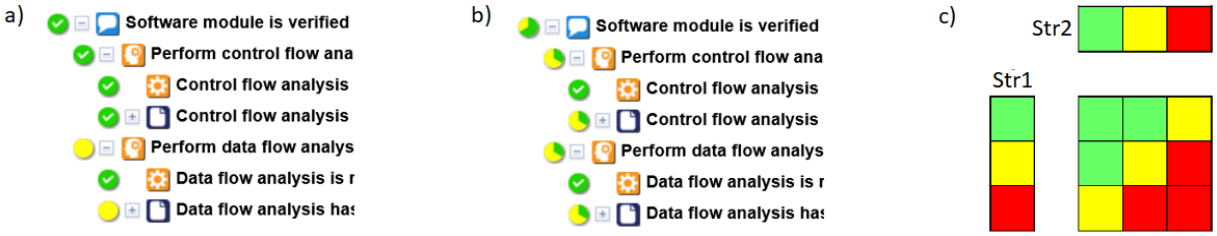


Figure 15. Use of alternative strategies (a and b), the belief matrix for alternative strategies (c)

6.4 Assumption adjustment

The last step is performed when an assumption is attached to the inferred claim. The assumption should be confirmed to be true. When the assumption is invalid then the whole argument may be also not valid and that causes uncertainty of the inferred claim.

Assumptions are generally assumed to be true but their verification is recommended for each assurance case, especially in case of argument reuse. It may happen that some assumptions are not valid when the argument is used in different context.

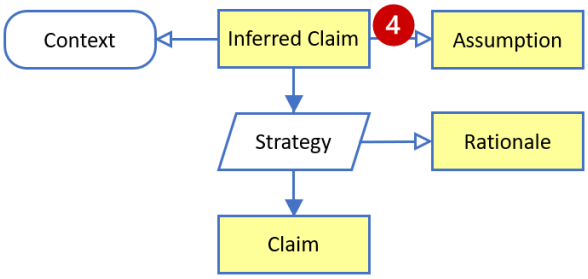


Figure 16. The step of assumption adjustment

7 Validity period of the assessment

Any assessment made in the argument is not valid indefinitely. The assessed assurance case may evolve and any change may invalidate some assessments. The affected assessment should be regarded as “outdated” and a re-assessment if a given argument step is required to confirm the assessment is still valid or it should be updated. The re-assessment is to be made by the assessor. The outdated assessments may be automatically reported for the assessors for review to reduce the effort of argument reviews.

The impact of a change on the argument assessment is determined based on the scope of argumentation steps. When any of the elements of an argumentation step is modified then the assessment of a given step becomes outdated. The scope of argumentation steps is presented in Figure 17.

- Assessment of a base claim becomes outdated when its context, assumptions, supporting evidence or the base claim itself is modified.
- Assessment of a rationale becomes outdated when the inferred claim, its context, assumptions, the strategy, premises or the rationale itself is modified.

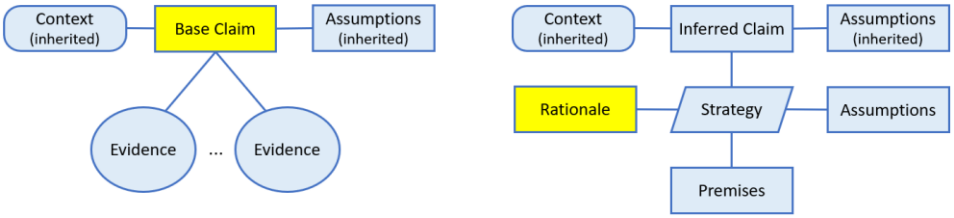


Figure 17. Scope for evidential step (left) and reasoning step (right)

The objective of tracking outdated assessment is to assist the assessor and alert them when a review is required to update the assessment.

It happens that during an assessment of a modified argumentation step the assessor finds any further inconsistencies or doubts caused by the change and to correct them next changes of the argument are required. These changes in turn cause other assessment to be outdated and the next argumentation steps have to be reviewed. This chain of argument and assessment changes will stop when a new consistent state of the argument is reached.

8 Argument quality checklist

A simple argument quality checklist given below can be used in the argument reviews when you perform the assessment.

1. Clear and unambiguous assurance case
   a) understandable – the goals, line of reasoning and context are clearly specified
   b) precise – descriptions are clear and the terms used are defined
   c) explicit – claims and argumentation strategies are explicitly defined
   d) restricted – the context and boundaries are clearly specified
2. Convincing arguments
   a) direct – reasoning should aim directly at the specific claim
   b) defensible – capable of being justified and defended
   c) comprehensive – reasoning should cover the full scope of the top claim, its context and the assumptions
   d) complete – containing all elements required to reason the conclusion but not redundant elements
   e) robust – not based on optimistic assessment and weak premises
3. Compelling evidence
   a) veracious – representing the truth and being accurate
   b) applicable – consistent with the goals and useful for the reasoning, adequate
   c) unambiguous – not open to more than one interpretation
   d) sufficient – containing all information required by the supported base claim
   e) up to date – representing the current state adequate for the goals

Points 1 and 2 of the checklist apply to reasoning steps of the argument and points 1 and 3 apply to evidential steps.